SafetyNet Micro
User Manual

Document Revision CSSSN 01/09
SafetyNet Micro

Copyright and Trademark

Computer Support Systems Pty Ltd.

Head Office: 373 Johnston Street
Abbotsford
VICTORIA 3067
Australia

Telephone: - 61 3 9419 3955
Facsimile: - 61 3 9419 3509
Web Address: - www.csspl.com.au
sales@csspl.com.au
support@csspl.com.au

Disclaimer and Revisions

Operation of this equipment in a residential area may cause interference in which case the user, at his or her own expense, will be required to take whatever measures may be required to correct the interference.

Date	Revision	Comments
01/03/2005	CSSSN 03/05	NK Revision A
27/07/2005	CSSSN 07/05	NK Revision B
13/01/2009	CSSSN 01/09	NK Updated with Modem init strings introduction.

Declaration of Conformity

Manufacturer's Name & Address:

Computer Support Systems Pty Ltd, 373 Johnston Street, Abbotsford, Victoria 3067, Australia.

Product Name Model: SafetyNet Micro Environmental Monitoring

Warranty

Computer Support Systems warrants SafetyNet Micro

- If used in accordance with all applicable instructions
- To be free from defects in material and workmanship for a period of one year from the date of initial purchase.

This warranty is voided if the customer uses SafetyNet Micro in an unauthorized or improper way, or in an environment for which it was not designed. Warranty does not apply to normal wear or to damage resulting from accident, misuse, abuse or neglect.

Safety Instructions

When using this product, basic safety precautions should always be followed to reduce the risk of fire, electric shock, and injury to persons, including the following:

1. Read and understand all instructions.
2. Unplug this product from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.
3. Do not use this product in an outdoor environment or near water, for example, near a bathtub, washbowl, kitchen sink or laundry tub, in a wet basement, or near a swimming pool.
4. Do not place this product on an unstable surface. The product may fall, causing serious damage to the product.
5. This product should never be placed near or over a radiator or heat register. This product should not be placed in a built-in installation unless proper ventilation is provided.
6. Do not allow anything to rest on the power cord. Do not locate this product where the cord will be abused by walking on or over it.
7. Do not overload wall outlets and extension cords as this can result in the risk of fire or electric shock.
8. Never push objects of any kind into this product through the slots as they may touch dangerous voltage points or short out parts that could result in a risk of fire or electrical shock. Never spill liquid of any kind on the product.
9. To reduce the risk of electrical shock, do not disassemble this product. Opening or removing covers will expose you to dangerous voltages or other risks. Incorrect re-assembly can cause electric shock when the appliance is subsequently used.
10. Unplug this product from the wall outlet and return to CSS for repairs under the following conditions:
    a) When the power supply cord or plug is damaged.
    b) If liquid has been spilled into the product.
    c) If the product has been exposed to rain or water.
    d) If the product does not operate normally by following the operating instructions. Adjust only those controls that are covered by the operating instructions because improper adjustment of other controls may result in damage and will often require extensive work by a qualified technician to restore the product to normal operation.
    e) If the product has been dropped or has been damaged.
    f) If the product exhibits a distinct change in performance.
11. Do not use sensors that are not supplied by Computer Support Systems

Table of Contents

1 Introduction to SafetyNet Micro

SafetyNet Micro is modern network based Environmental Monitoring System (EMS). It is capable of notifying error conditions via SNMP (Simple Network Management Protocol), via SMS messaging or by a web page. A blinking LED is also activated on alarm and will attract attention on error conditions.

This product is ideal to monitor facility services and notify of potential environmental problems, which may impact on the network operations. The unit can monitor even an IP address and reboot servers if it stalls with appropriate accessories.

SafetyNet Micro comprises an embedded web server. With a standard Java enabled web browser installed in almost all computers today, you can easily view SafetyNet Micro web pages to monitor status and change settings remotely.

The option of having PPP allows to have monitoring perform when the network fails or at remote locations where there is no Ethernet. SafetyNet Micro is able to deliver SNMP Traps using PPP, when there is no network and notify of any potential issues.

Features

- Powerful embedded microprocessor driven, with networking features.
- 19” inch rack mountable and compact size. (1/3 RU)
- SNMP features to notify error conditions or to poll data.
- SMS messaging via the Internet, or the option of selecting a network independent internal PSTN modem to send SMS messages. *
- Remote configuration and monitoring capabilities via a Java enabled web browser.
- User friendly and an attractive user interface.
- Internal temperature & humidity sensor and two digital contact sensor inputs; also configurable as a smoke or a fluid sensor.
- Selectable power sources at ordering. I.e. 48V DC or 9-12V DC plug pack
- Remote IP monitoring feature with physical rebooting of servers/systems when failed or stalled. **
- A blue blinking LED to indicate error conditions.
- Graphical plotting for the internal analogue sensor. (Temperature and humidity)
- Up to 40 entries of alarm and event logs.
- Optional PPP features. Dial into SafetyNet Micro and auto dial out based on alarms. SNMP trap delivery even when there is no Ethernet connectivity or if the network fails. ***

* Optional & recommended. Applicable to models ZSN4001M & ZSN4001MD.
** With the option of using a SafetyBoot device.
*** Applicable to models ZSN4001MP & ZSN4001MDP.

Applications

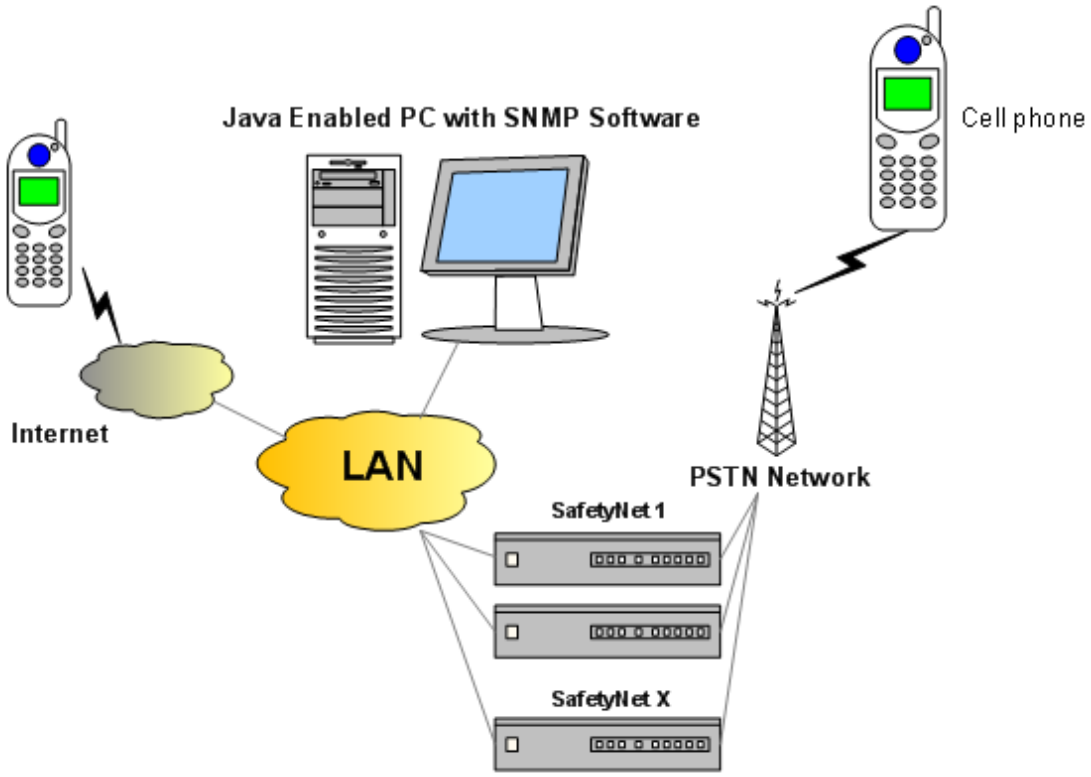
- Computer server room monitoring.
- Computer rack monitoring and management.
- Alarm consolidation from other non-net enabled systems.
- Monitoring of other controlled environments
- Monitoring of servers or PC’s and rebooting when stalled. ** (See above)
- Water monitoring systems.

SafetyNet Micro Environmental Monitoring System
ZSN4001

1.1 Available SafetyNet Micro Models

Model Number	Description
ZSN4001	SafetyNet Micro, 9 -12 Volt D.C plug pack input
ZSN4001D	SafetyNet Micro, 48 Volt D.C
ZSN4001M	SafetyNet Micro, 9 -12 Volt D.C plug pack input, PSTN modem
ZSN4001MD	SafetyNet Micro, 48 Volt D.C, PSTN modem
ZSN4001MP	SafetyNet Micro, 9 -12 Volt D.C plug pack input, PPP
ZSN4001MDP	SafetyNet Micro, 48 Volt D.C, PPP

1.2 SafetyNet Product Family Concept



2 Assumptions

We assume that you have: -

- Configured SafetyNet Micro network parameters according to the ***SafetyNet Quick Install Guide,*** and that the IP address of the device is known. This manual is to explain how to use SafetyNet Micro once successfully installed on the network. You can find information on how to get SafetyNet Micro on the network in the ***Quick Install Guide*** found on your product CD.
- An installed SafetyNet Micro with all necessary sensors supplied by Computer Support Systems.
- All requirements specified on the ***SafetyNet Micro Getting Started Manual*** are met.

3 Introduction to SafetyNet Micro Web Interface

SafetyNet Micro web interface is controlled by Java applets. The Java™ Runtime Environment version 1.4.2 or higher is required to be installed on the computer to load the applets. See section 2 (Requirements) under the ***SafetyNet Micro Getting Started Manual*** for further details.

The product uses applets to represent its Graphical User Interface (GUI). The user interface consists of a menu for easy navigation.

The SafetyNet Micro web interface is password protected and case sensitive. Factory default password is set to be "*password*".

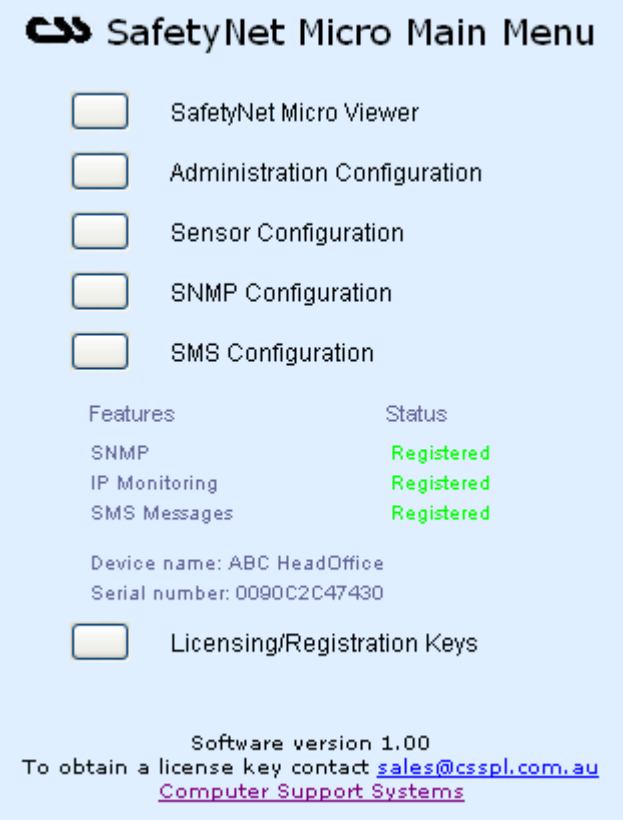
A simple description of each web interface is described below. Further details of each web interface and how to use them can be found under chapter 5, Configuring SafetyNet Micro.

The web interface is loaded simply using a Java enabled browser, and by pointing it to the IP address of SafetyNet Micro. Alternatively, configure the WINS (Windows Internet Name Service) to provide a name resolution for SafetyNet Micro from NetBIOS names to IP addresses for Windows PCs. This will enable to type the given name instead of the IP address.

3.1 SafetyNet Micro Main Menu

The SafetyNet Micro main menu controls the navigation. It shows the current software version, the unit name, the MAC address (serial number) and the features that are registered.

Features that are unregistered will have their configuration menu entry access denied or disabled.



3.1.1 Registering Features (Registration Keys)

SafetyNet Micro has the following features controlled by registration keys.

- SNMP
- IP monitoring
- SMS messages (Not available on models ZSN4001M & ZSN4001MD)

The product CD label on the provided CD-ROM will contain the appropriate registration key for each feature purchased.

To register features enter the registration keys on the registration control web page. Click on "*Licensing/Registration Keys*" under the main menu to enter this page.

Enter the correct registration keys and click on "*Update*". Any incorrect entry will be notified. Once updated with the correct keys the feature status will be updated to "*registered*". Click on main menu to exit.

Notice that you have access to the configuration settings of the features that are registered only. Features that are unregistered cannot be configured and access to the configuration web pages would be denied.

3.1.2 Introduction to SafetyNet Micro Viewer

This is the main remote web interface that allows viewing of the current sensor status.

The analogue and digital-alarm status are clearly indicated and any fault will attract attention by blinking indicators.

This interface also provides navigation shortcuts to view the analogue sensor graphs and the alarm & event logs.

Chapter 4, SafetyNet Micro Viewer discusses further about the Viewer features.

3.1.3 Introduction to Administration Configuration

Allows network interface setting changes, password changes, hardware resets, loading factory defaults, viewing the configuration summary and updating the time on SafetyNet Micro.

3.1.4 Introduction to Sensor, Ping & PPP Configuration

Allows installing sensors, making changes to sensor settings & configuring the IP monitoring. This interface also allows clearing existing data used for graphing purposes and the alarm & event log.

PPP settings are configured via this interface for models ZSN4001MP & ZSN4001MDP.

3.1.5 Introduction to SNMP Configuration

Allows SNMP configuration changes; such as the communities and the network manager IP address insertion.

3.1.6 Introduction to SMS Configuration

This interface is applicable to models ZSN4001, ZSN4001D, ZSN4001MP & ZSN4001MDP only. These models are capable of sending SMS messages via the network.

This interface allows configuring the SMS operation of SafetyNet Micro.

3.1.7 Introduction to Modem Configuration

This interface is applicable to models ZSN4001M & ZSN4001MD only. These models have an in-built PSTN modem that can send SMS messages independent of the network, when configured. These models use the standard telephone line to send SMS messages.

This interface allows configuring the modem and the SMS customisation of SafetyNet Micro.

3.2 Security on SafetyNet Micro

3.2.1 Password

A password secures entry to the important configuration pages of the SafetyNet Micro unit.

The factory default password is set to be "*password*". We recommend changing it to a desired password with at least four characters.
Note: *SafetyNet Micro password is case sensitive. The password is limited to a maximum number of eight characters.*

3.2.1.1 Changing the Password

A password change may be performed on the administration configuration web interface. Read section chapter 5.1 Administration Configuration to find out how to change the password.

3.2.2 Forgotten Password

Entering an incorrect password for more than three times on the web interface will direct to a web page where it provides details of how to re-enter a new password.

Upon a successful password unlock key submission it will then allow to enter a new password.

3.2.3 Inactivity Timed Redirection

If SafetyNet Micro configuration pages that are logged in are inactive for more than five minutes, it will automatically log out from the web interface and will direct back to the main menu. This feature will protect users from forgetting to logout from the configuration pages and will attempt to prevent unauthorised access to the configuration aspects of the unit.

This does not apply to the SafetyNet Micro Viewer, the analogue sensor graphs or the alarm & event log interfaces.

4 SafetyNet Micro Viewer

SafetyNet Micro viewer is the key remote interface that allows viewing the current status of the monitored environment.

It shows the label of each sensor, what type of a sensor it is, the current status or the reading of the sensor.

For the internal temperature and humidity sensor, it gives visual interpretation of the current level with respect to the upper and lower range settings of the sensor limits. This will enable an immediate impression of what level of threat you are in, if at an alarm stage.

IP monitoring errors, hardware errors, no dial tone detection* errors are also shows on the viewer if they occur.

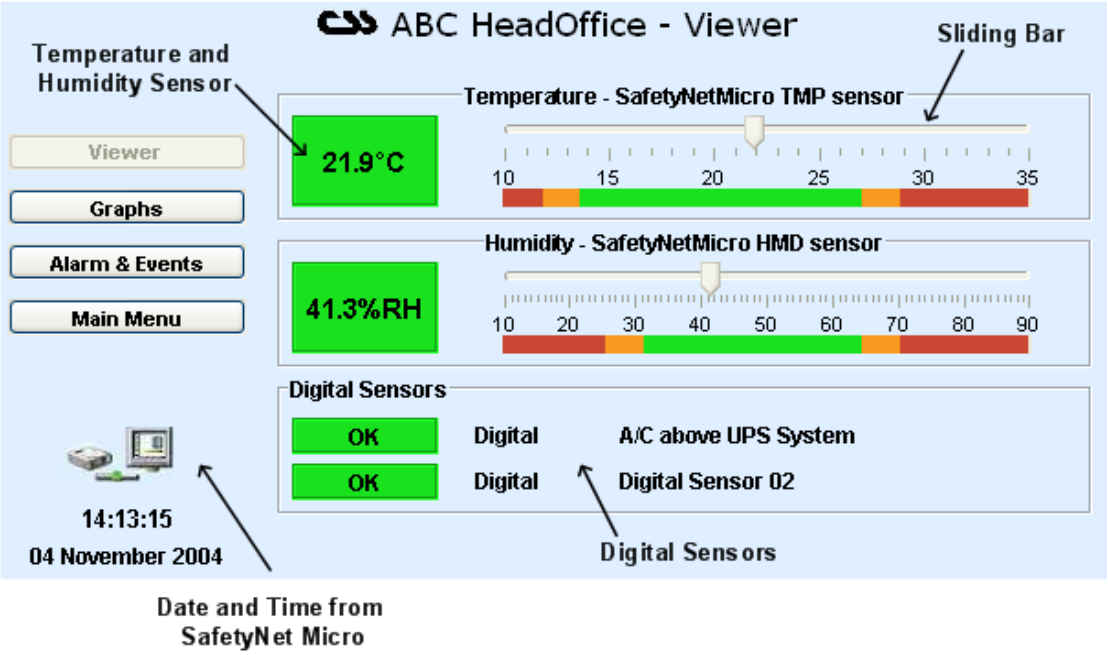
The time display on the left bottom of the viewer interface is the time extracted from SafetyNet Micro, updated every second.

The two alternating images at the bottom left corner is an indicator that the interface is communicating with the SafetyNet Micro via the network.

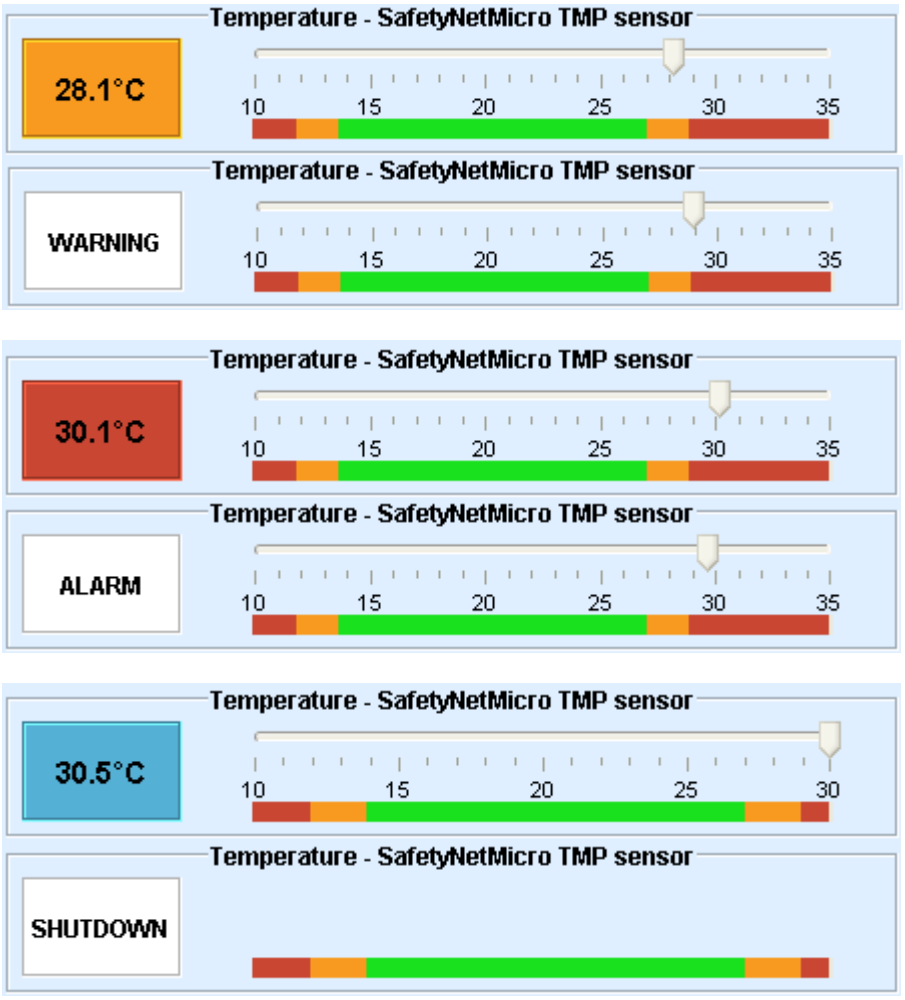
The sub-menu on the left will allow viewing the graphs for temperature/humidity type sensors and to view the alarm & event log.

A typical “All’s well” status will give you an interface such as.

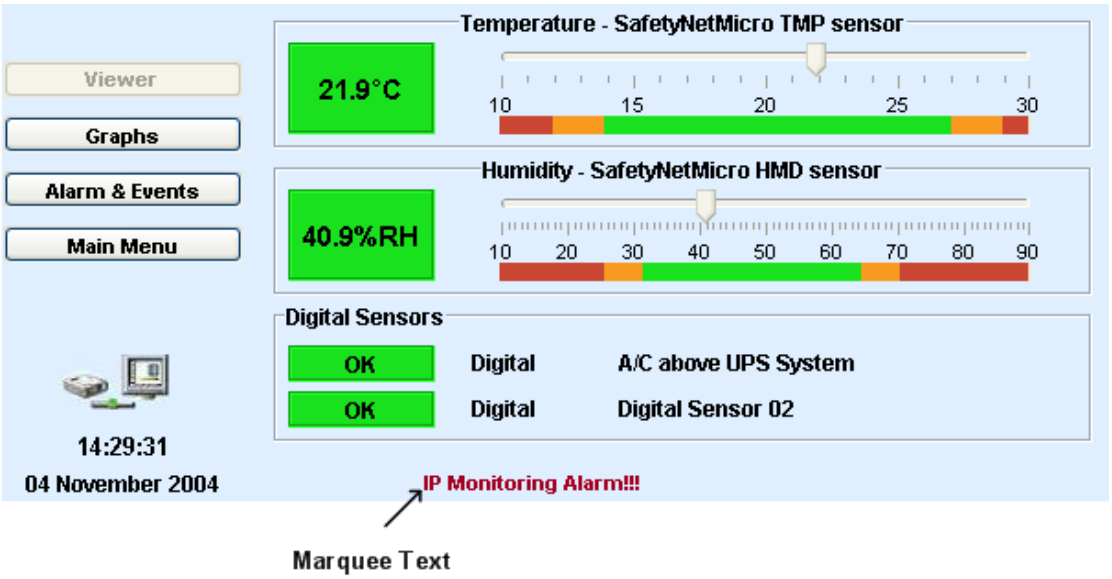
* Only on models ZSN4001M & ZSN4001MD



Any warning, alarm or a shutdown of an analogue sensor will be indicated on the screen as below.



If the internal analogue sensor is faulty, IP monitoring alarm has triggered or no dial tone is detected, notification is set by a text field describing the error as illustrated below.



4.1 Graphs

Click on the "*Graphs*" button on the left side of the viewer to view the internal analogue sensor data using line graphs. This allows viewing the temperature and humidity sensor values up to the last month. It is vital to view these graphs as an audit trail, as well as to analyse the trend of future data based on previous records.

There are four different graphs offered with SafetyNet Micro local graphing. They are:

- 2 Hour Graph (1 minute average)
- Daily Graph (6 minute average)
- Weekly Graph (1 hour average)
- Monthly Graph (3 hour average)

Read chapter 6 to learn more about graphs.

4.2 Alarm and Event Log

Click on the "*Alarm & Events*" to check the log entries. These log entries will allow to keep track of previous alarms and event entries.

Read chapter 7 to learn more about log entries.

5 Configuring SafetyNet Micro

Configuring SafetyNet Micro is purely done remotely using web interfaces that embed Java™ applets. Any configuration change does not reboot SafetyNet Micro. All configuration changes are performed at runtime.

Once all configuration aspects have been performed, we recommend initiating a hardware reset by clicking the "*Hardware Reset*" sub menu button found in the administration configuration interface on SafetyNet Micro.

As a **backup of the configuration**, we recommend keeping a listing of each of the settings stored elsewhere^. Viewing the summary of the complete settings can be obtained via the Administration Configuration page. **Retain a hardcopy of the settings as backup.**

^ This options is not available on models ZSN4001MP & ZSN4001MDP

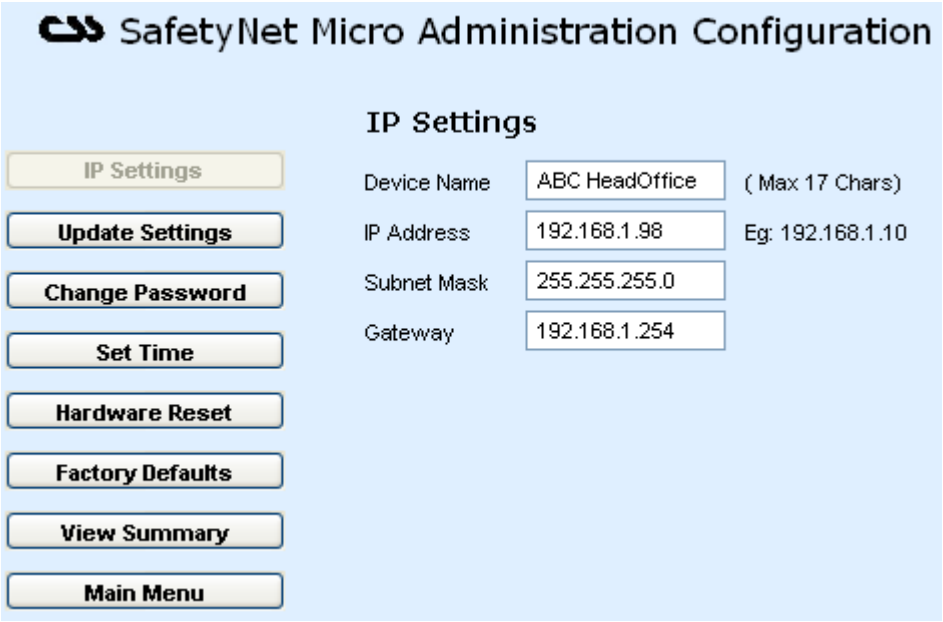
PPP users with SafetyNet Micro models ZSN4001MP & ZSN4001MDP please refer to "Appendix A – PPP Users" of this document on page XXX

5.1 Administration Configuration

To enter this configuration interface click on "*Administration Configuration*" button on the main menu of SafetyNet Micro.

Use this interface to

- Set network parameters
- Set a device name
- Set/Change the time on SafetyNet Micro
- Perform a hardware reset via software
- Load factory defaults of the product
- Change the current password
- View and store the current configuration settings as a backup



IP Settings

SafetyNet Micro Name: A 17-character device name to uniquely identify each SafetyNet Micro unit on the network.

IP Address: Enter new static IP address or 0.0.0.0 to enable DHCP. (No broadcast address or duplicate IP addresses to be inserted)

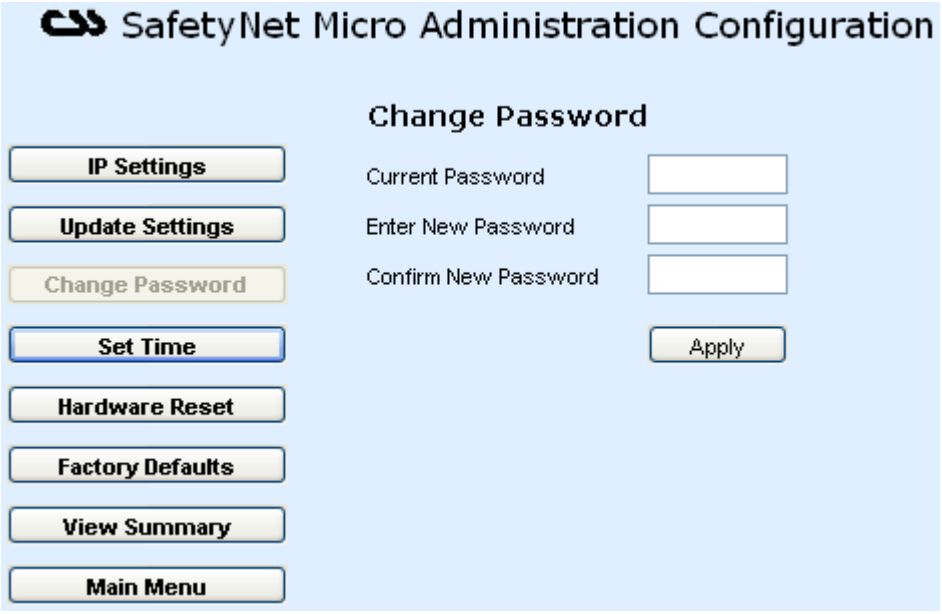
Subnet Mask*:* Indicates the number of subnets on the network. Contact your network administrator for further details on your subnet mask. DHCP will automatically allocate the subnet mask.

Gateway: Contact your network administrator for further details.

Update Settings

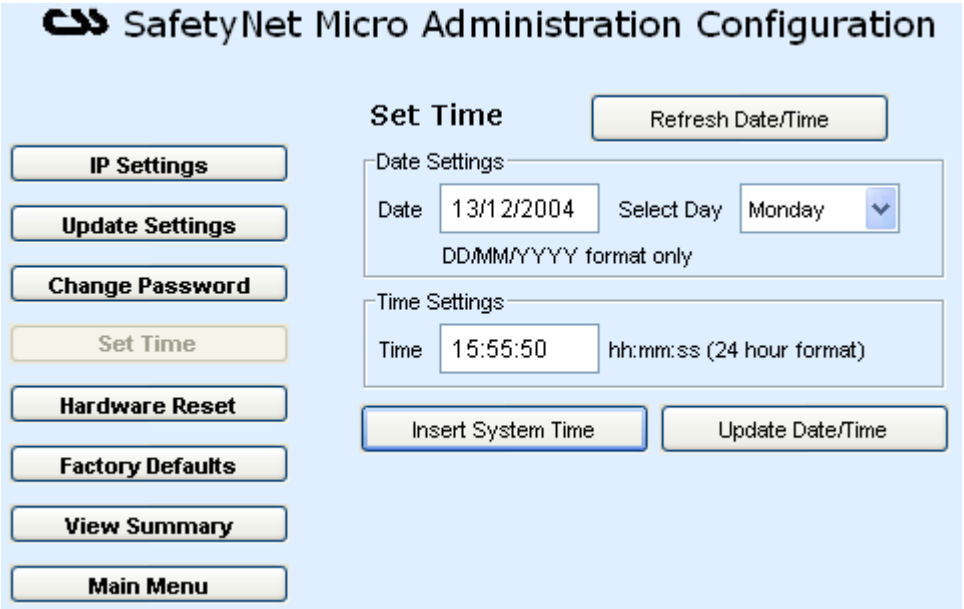
When clicked on "*Update Settings*" it will prompt a confirmation dialog box to proceed. Click "*Yes*" to apply your settings or click "*No*" or "*Cancel*" to cancel new settings.

If clicked "*Yes*", the new settings are applied to SafetyNet Micro. Updating settings take approximately about 10 seconds.



Change Password

Password Settings: Change the password here and click "*Apply*". It will automatically log you out from the device and the new password is required to log back in.



Set Time

This allows setting the real time clock on SafetyNet Micro. When the "*Set Time*" button is clicked, the time and date is extracted from SafetyNet Micro and displayed. When entering field values, the date format should be DD/MM/YYYY and the time format should be HH:MM:SS in 24-hour format.

Refresh Date/Time: The web interface will read the SafetyNet Micro current time and date updates the appropriate fields.

Insert System Time: This will extract the system time & date from your machine and place them on the appropriate fields.

Update Date/Time: Will confirm the update and set the current field time and date on to SafetyNet Micro. Once the update is completed, the time is refreshed on fields with the new time and date on SafetyNet Micro.

Hardware Reset

This is similar to toggling power to the unit and resetting the device. It will cause all alarms to be redetected if present, at start up.

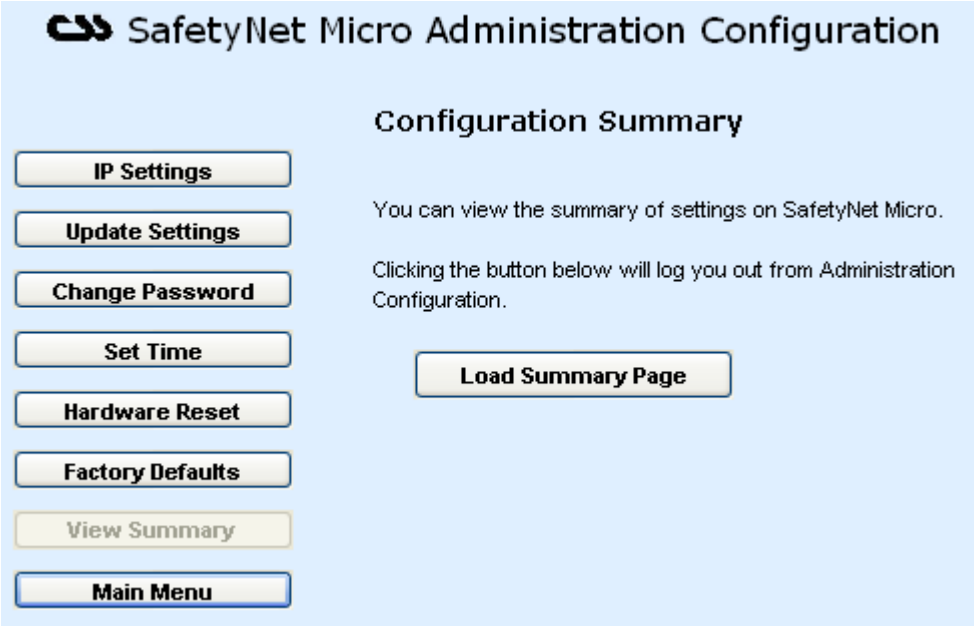
Factory Defaults

This will give a method to set factory defaults on SafetyNet Micro. The following will be applied on the product.

- All sensors will be set back to its original sensor types, labels & threshold values. Digital sensors will be disabled. IP monitoring cleared and disabled.
- All analogue-sensor related graph data would be cleared.
- Both alarm and event logs will be cleared.

- SMS configuration cleared.
- SNMP configuration cleared.

Click on "*Load Factory Defaults*" to set the above settings.



View Summary

Click on "*View Summary*" to view the current settings as a summary. It will prompt to refresh the page to prevent items loading from the cache memory. This page is for the purpose of keeping a backup of the configuration saved/printed elsewhere. In any circumstance, if the site is to be restored, having the summary page will assist to bring up the site in no time.

This is not available on models ZSN4001MP & ZSN4001MDP

Main Menu

The main menu can be reached by clicking "*Main Menu*" button at any given time.

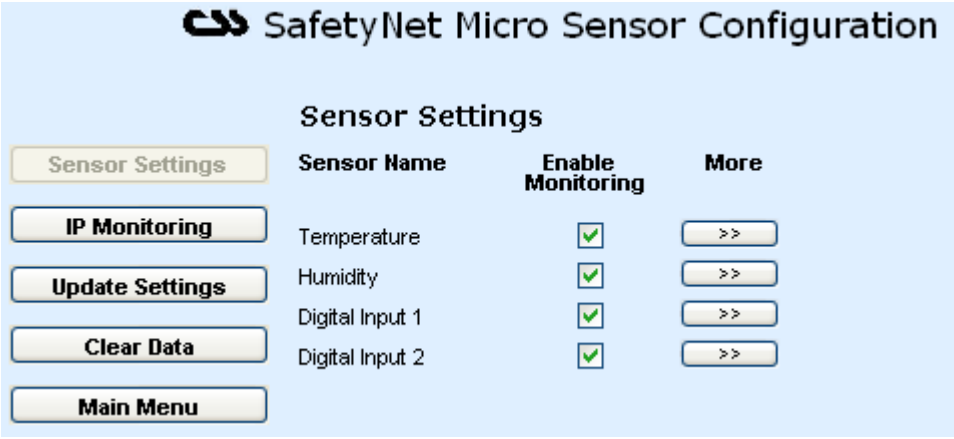
Staying inactive for over 5 minutes on any interface will automatically direct back to the main menu.

5.2 Sensor Configuration, PPP & IP Monitoring Configuration

To enter this configuration interface click on the "*Sensor Configuration*" button on the main menu of SafetyNet Micro.

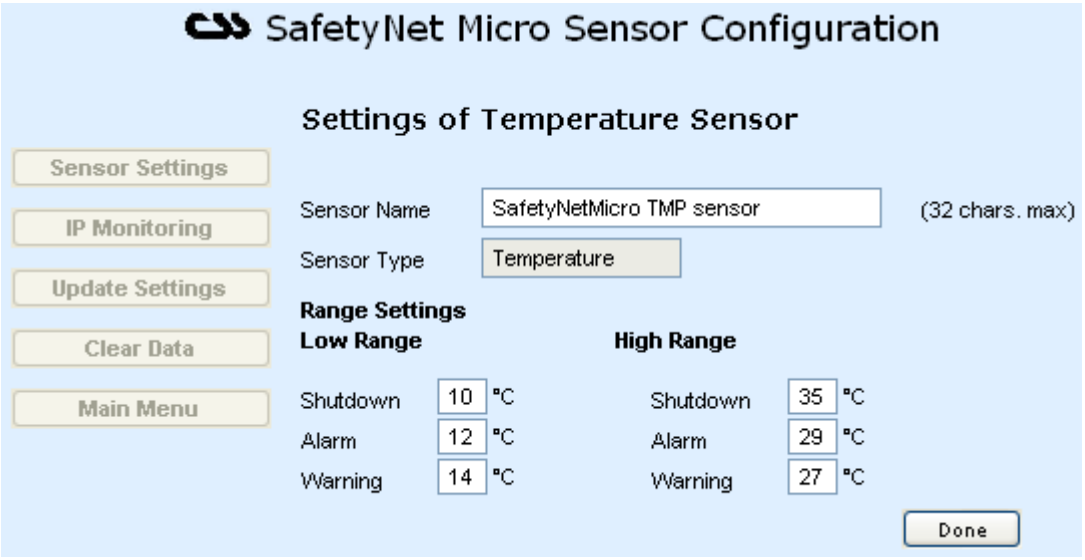
Use this interface to

- Enable or disable any sensor/s. (making sensors active or inactive)
- Change any of the sensor parameters, such as the trigger delay, temperature limits or the sensor label.
- Configure the IP monitoring parameters.
- Clear analogue sensor related data that plots graphs, or clear the alarm & event log.
- Configure incoming and outgoing PPP connections.



Sensor Settings

This section allows enabling sensors and setting its details. Click on the ">>" button to expand each sensor/s further setting.



Temperature or Humidity Sensor Detail Expansion

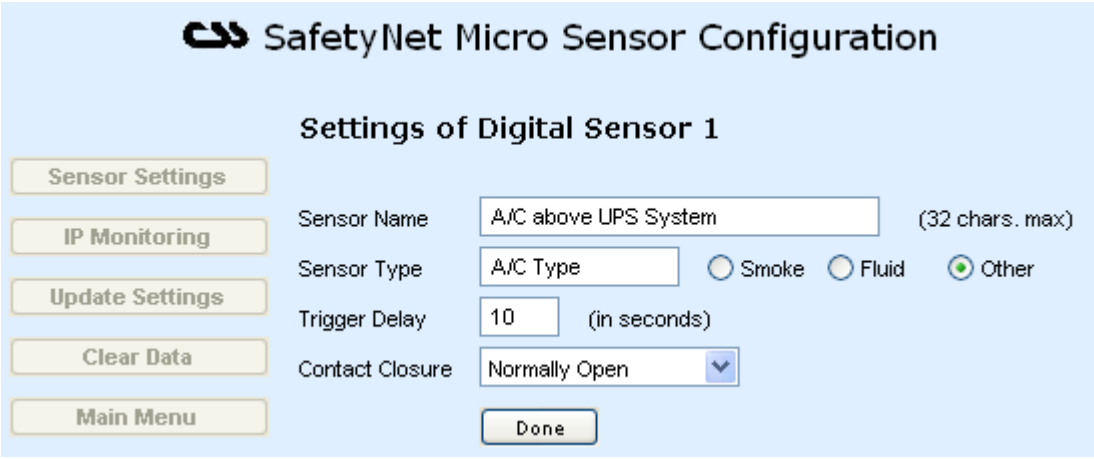
Sensor Name: A 32-character label for the sensor

Sensor Type: Temperature or humidity type

Range Settings: Insert the lower and higher end analogue sensor cutoff limits.

The preferred temperature or humidity range of the monitored environment should be between the low warning and high warning limits.

Click "*Done*" when finished configuring the sensor.



Smoke, Fluid & Digital Sensor Detail Expansion

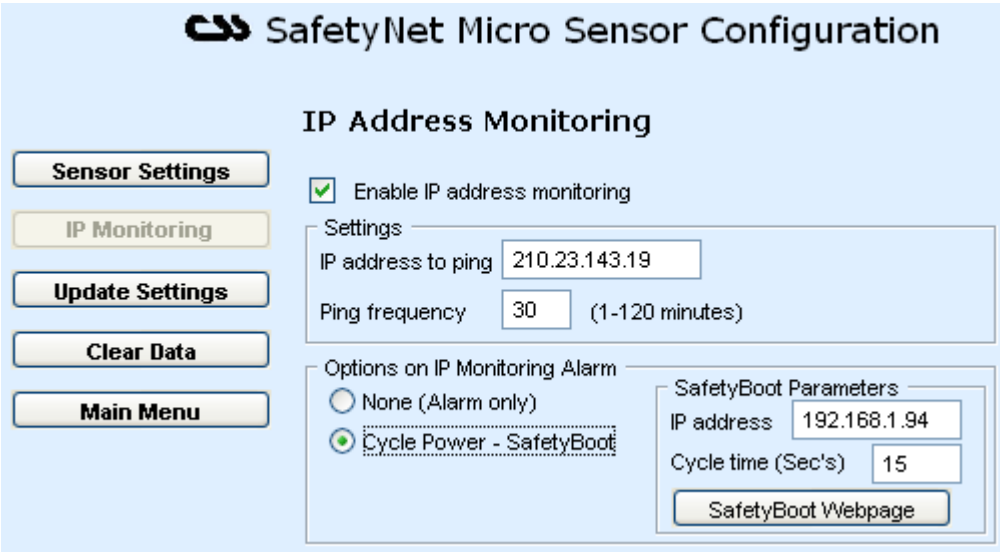
Sensor Type: a 10-character type label, e.g. A/C, External, Security, Lock, and Power, etc. If smoke or fluid type is selected Sensor 4 is de-activated.

Trigger Delay: Enter a trigger delay for digital type sensors. An actual alarm is raised only if the alarm was active for this period. The accepted range of values for this field is 0-120 seconds. Any sensor input that activates or deactivates before the trigger delay period is elapsed is not treated as an alarm. For immediate triggers of digital alarms set this value as zero.

If the sensor type is selected as smoke or fluid, the default value of 10 is inserted as the trigger delay. You may increase it accordingly if necessary.

Contact Closure: Digital sensors can be either "*Normally Open*" or "*Normally Closed*". If the sensor type is selected to be as smoke the contact closure type is automatically selected as "*Normally Closed*".

Click on "*Done*" when finished configuring the sensor.

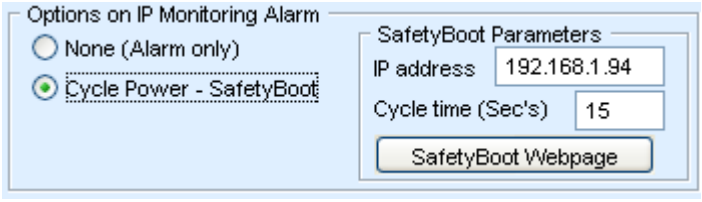


IP Monitoring

Settings: Insert the IP address that needs to be monitored and the frequency of the ICMP commands that are sent out. SafetyNet Micro will produce an ICMP request based on this frequency to monitor the specified network device.

Options: On IP Monitoring alarm, one of the options would be triggered as an action. It is able to

a) Trigger the alarm only
b) Cycle power of a specified SafetyBoot device.



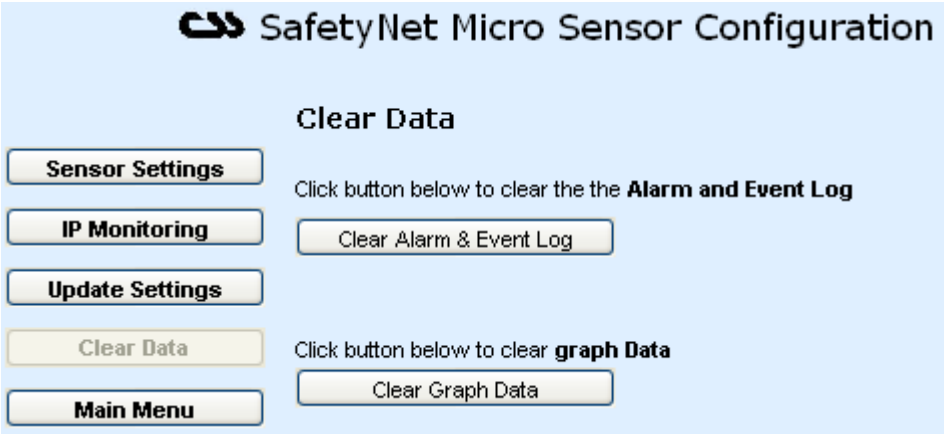
Update Settings

When clicked on "*Update Settings*" it will prompt a confirmation dialog box to proceed. Click "*Yes*" to apply settings or click "*No*" or "*Cancel*" to cancel new settings.

If clicked "*Yes*", the new settings are applied to SafetyNet Micro. Updating settings take approximately about 5 seconds.

Clear Data

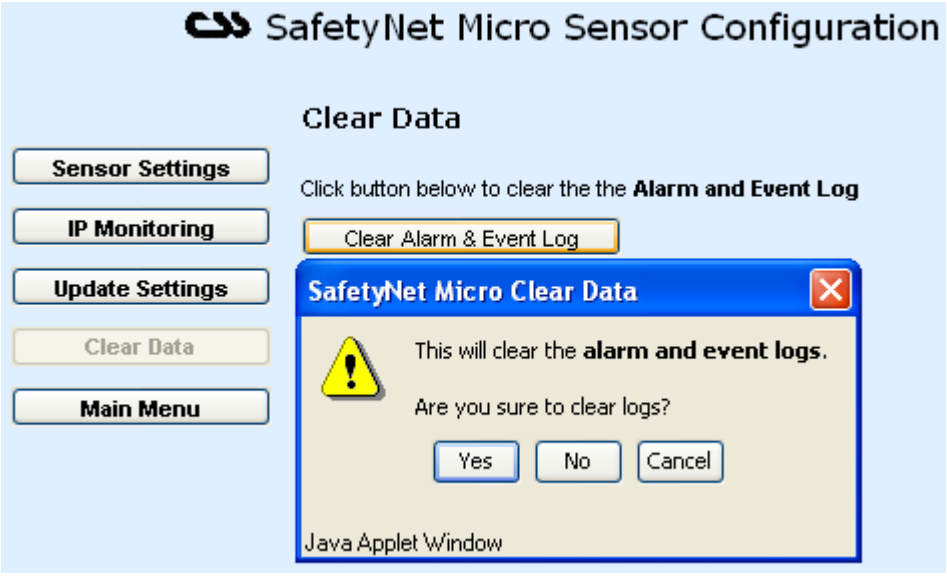
When clicked on "*Clear Data*", it gives the option to clear the analogue sensor related graph contents and the alarm & event log.



Click the appropriate button to clear data. A confirmation dialog box is prompted to proceed. Click on "*Yes*" to clear the relevant data.

Clearing the graph data will give a blank graph to start with. This is ideal if the product was moved to a new site.

Clearing the alarm & event log will wipe all entries in both logs and create a new event entry stating the clearance of the logs.



The action is performed immediately and a confirmation box will indicate the success of the command.

Main Menu

The main menu can be reached by clicking "*Main Menu*" button at any given time.

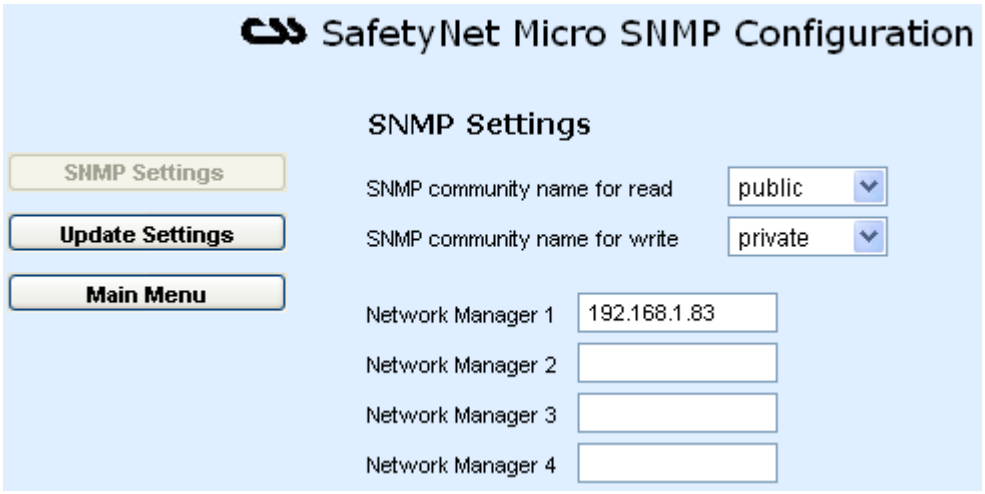
Staying inactive for over 5 minutes will automatically direct back to the menu page.

5.3 SNMP Configuration

Click on the "*SNMP Configuration*" button on the main menu of SafetyNet Micro to enter this configuration interface.

Use this interface to

- Configure the read and write SNMP communities.
- Configure the SNMP manager IP addresses.
  PS: Obtain these from your network administrator



SNMP Settings

SNMP Read Community: Select public, private or other (default: public). If other is selected, a field is displayed for entry of community type.

SNMP Write Community: Select public, private or other (default: private). If other is selected, a field is displayed for entry of community type.

Network Manager Addresses: Enter IP addresses (up to four) of the Network Management Software hosts. If no IP addresses are entered, SNMP traps are not sent.

Update Settings

Same as other configuration interfaces.

Main Menu

The main menu can be reached by clicking "*Main Menu*" button at any given time.

Staying inactive for over 5 minutes will automatically direct back to the menu page.

5.4 SMS Configuration (Models ZSN4001, ZSN4001D, ZSN4001MP & ZSN4001MDP only)

To enter this configuration interface click on the "*SMS Configuration*" button on the main menu of SafetyNet Micro.

This interface configures the sending of SMS messages through the network. The SMS server application at Computer Support Systems handles delivering the SMS message upon receiving the network traffic.

Use this interface to

- Configure the SMS receiving phone numbers.
- Associate sensors to send SMS messages.
- Customise additional SMS messages

Select SMS Inputs

This section selects which inputs are SMS message enabled. By selecting an alarm you are obliged to select up to three mobile phone numbers where the SMS is sent.

Make sure that correct details of the phone numbers are entered under "*Phone Number Settings*".

If you want to select all check boxes, select the appropriate 'select all' check box.

Phone Number Settings

Allows inserting or changing existing mobile telephone numbers.

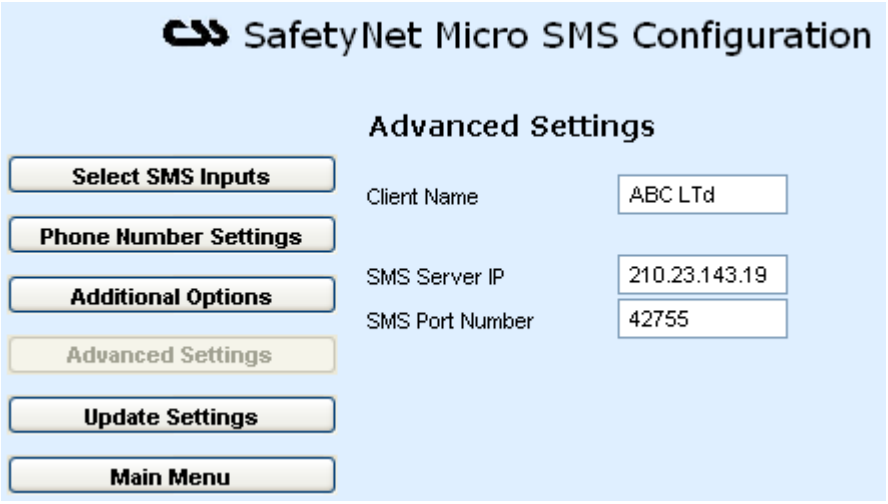
It is able to receive the same SMS message at, up to three different mobile phones. Priority is given to phone number 1, then 2 and finally 3 when delivering the SMS messages.

Additional SMS Options

This section allows customising additional SMS messages sent for notifications.

The warnings and shutdown messages for temperature or humidity type alerts are sent to the same phones selected for as the alarms, under "*Select SMS Inputs*"

The other alarms that are customisable are IP monitoring, mains failure/low battery alarms and faulty analogue sensor alerts.



Advanced Settings

This section allows to enter/change-advanced settings related to SMS messaging. The SMS Server IP address or the SMS port number should not be changed unless Computer Support Systems so advises.

Client Name: Enter your company name using 8-characters. If the space is insufficient, use initials to identify your company.

Update Settings

Same as other configuration interfaces.

Main Menu

The main menu can be reached by clicking "*Main Menu*" button at any given time.

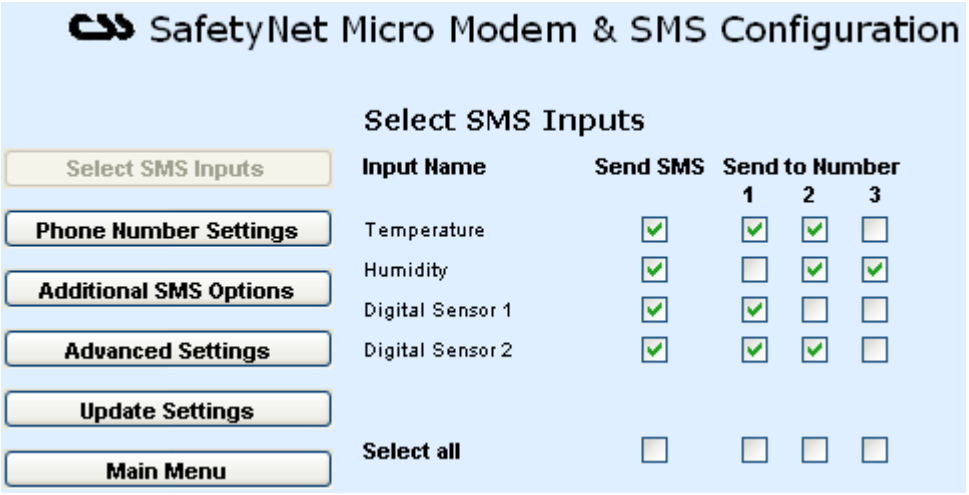
Staying inactive for over 5 minutes will automatically direct back to the menu page.

5.5 Modem/SMS Configuration (Models ZSN4001M & ZSN4001MD only)

To enter this configuration interface click on the "*Modem Configuration*" button on the main menu of SafetyNet Micro.

Use this interface to

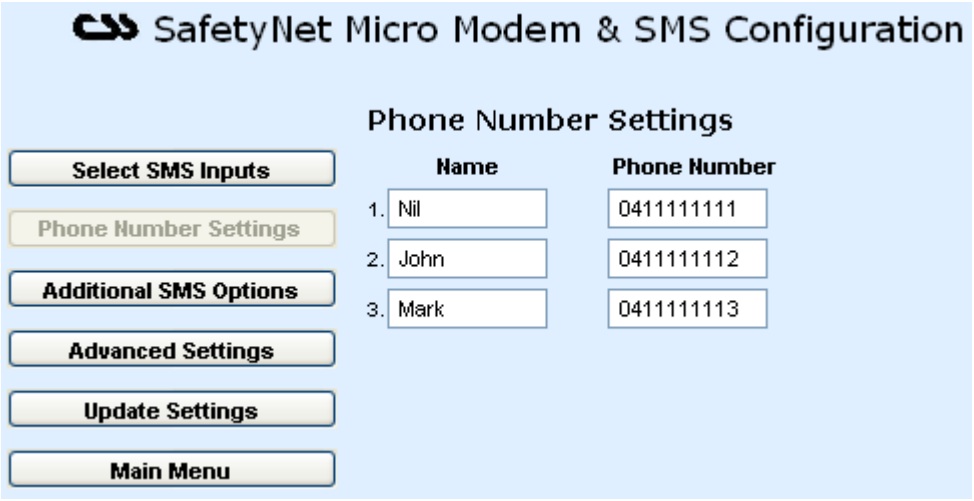
- Configure the SMS receiving phone numbers.
- Associate the sensor SMS alerts with the appropriate phone numbers.
- Configure the modem functions.
- Insert the dial up number and password
- Initiate a test alarm



Select SMS Inputs

This section selects which inputs are SMS message enabled. By selecting an alarm you are obliged to select up to three mobile phone numbers where the SMS is sent. Make sure that correct details of the phone numbers are entered under "*Phone Number Settings*".

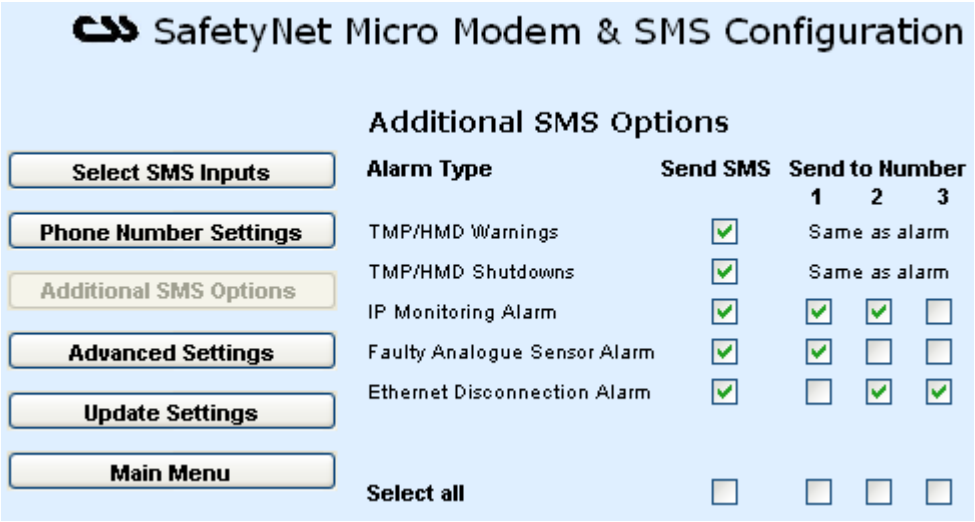
If you want to select all check boxes, select the appropriate 'select all' check box.



Phone Number Settings

Allows inserting or changing existing mobile telephone numbers.

It is able to receive the same SMS message at, up to three different mobile phones. Priority is given to phone number 1, then 2 and finally 3 when delivering the SMS messages.

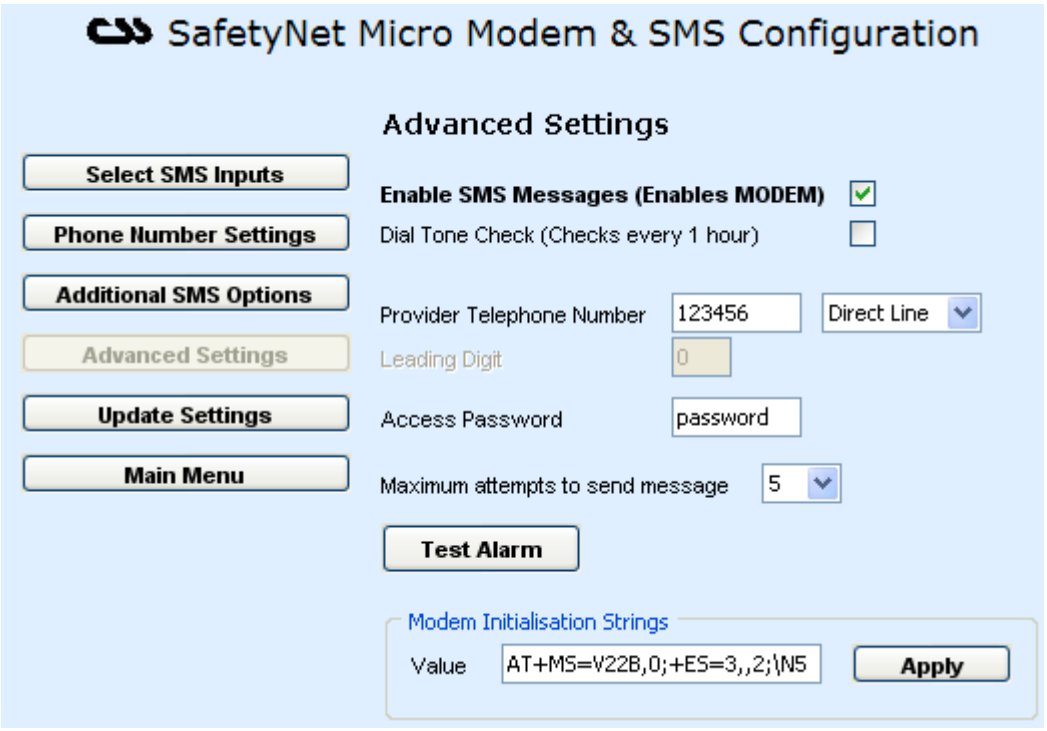


Additional SMS Options

This section allows customising SMS messages sent for additional notifications.

The warnings and shutdown messages for temperature or humidity type alerts are sent to the same phones selected for as the alarms, under "*Select SMS Inputs*"

The other alarms that are customisable are IP monitoring, faulty analogue sensor alert and Ethernet disconnection alert.



Advanced Settings

This section allows entering/changing-advanced settings related to modem, the telephone line connected and testing the SMS sending ability.

For the modem to be useful you need have it enabled.

The dial tone check is performed every hour. If there is no dial tone, an error will be prompted and logged. To disable the dial tone check, disable the dial tone detection check box.
Configure the type of line connected to SafetyNet Micro. If an analogue PABX line is connected, enter the leading digit to get an outside line. *(Note: If a PABX line is connected it needs to be an analogue PABX line. Digital PABX lines may damage the inbuilt modem)*

The maximum number of attempts is given so that a failing SMS is kept trying until it is delivered by the unit.

Test Alarm Button: After having all the parameters entered and updated, click the test alarm button to receive a test alarm on the phone numbers you have entered under "*Phone Number Settings*". An entry on the alarm log will be included and a SNMP trap is sent when a test alarm is initiated.

The modem initialisation strings can be set if necessary to optimise the connection between the provider and SafetyNet Plus. This allows adjusting the modem link negotiation so that different speeds and different error correct modes and different compression methods can be applied. Please see section 8.4.1 for details of specific parameters.

Update Settings

Same as other configuration interfaces.

Main Menu

The main menu can be reached by clicking "*Main Menu*" button at any given time.

Staying inactive for over 5 minutes will automatically direct back to the menu page.

5.6 Feature Registration / Licensing on SafetyNet Micro

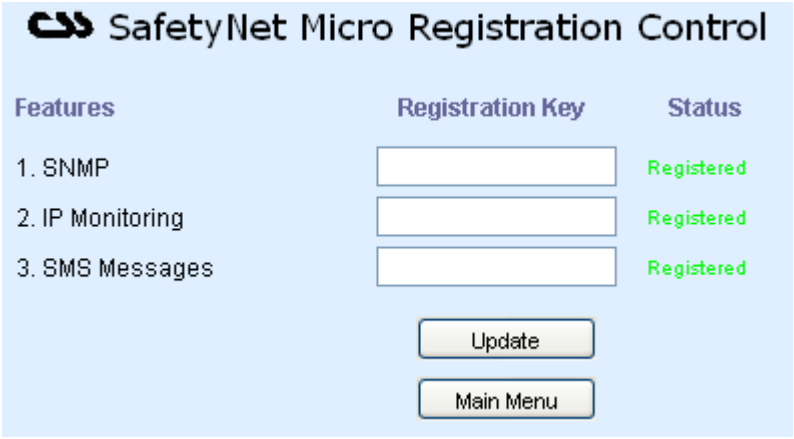
To enter this configuration interface click on "*Licensing/Registration Keys*" button on the main menu of SafetyNet Micro.

Use this interface to enter registration keys to register controlled features of SafetyNet Micro.

SafetyNet Micro has the following features.

1. SNMP
2. IP Monitoring
3. SMS Messaging for alerts/warnings & alarms (only on models ZSN4001 and ZSN4001D)

These individual features are registered only via a unique 9-character registration key supplied by Computer Support Systems. The supplied product CD contains a label with registration keys requested.



Enter the correct registration key(s) and click on "*Update*". Click on "*Main Menu*" to exit. The main menu will show what features have been registered or not.

6 Graphs on SafetyNet Micro

The graphs on SafetyNet Micro allow viewing the trend of the temperature and humidity sensor up to the last month. View these graphs as an audit trail as well as a tool to analyse the trend of future data based on the previous records.

There is no special requirement or third party applications involved in viewing these graphs. The data is stored locally in SafetyNet Micro and can be cleared whenever it is necessary.

The left Y-axis of the graph provides the range for the temperature sensor, where as the right Y-axis provides the range for the humidity sensor.

The X-axis displays the most recent time analogue data was updated and the gives timeline of the data records.

The following graphs are provided on SafetyNet Micro:

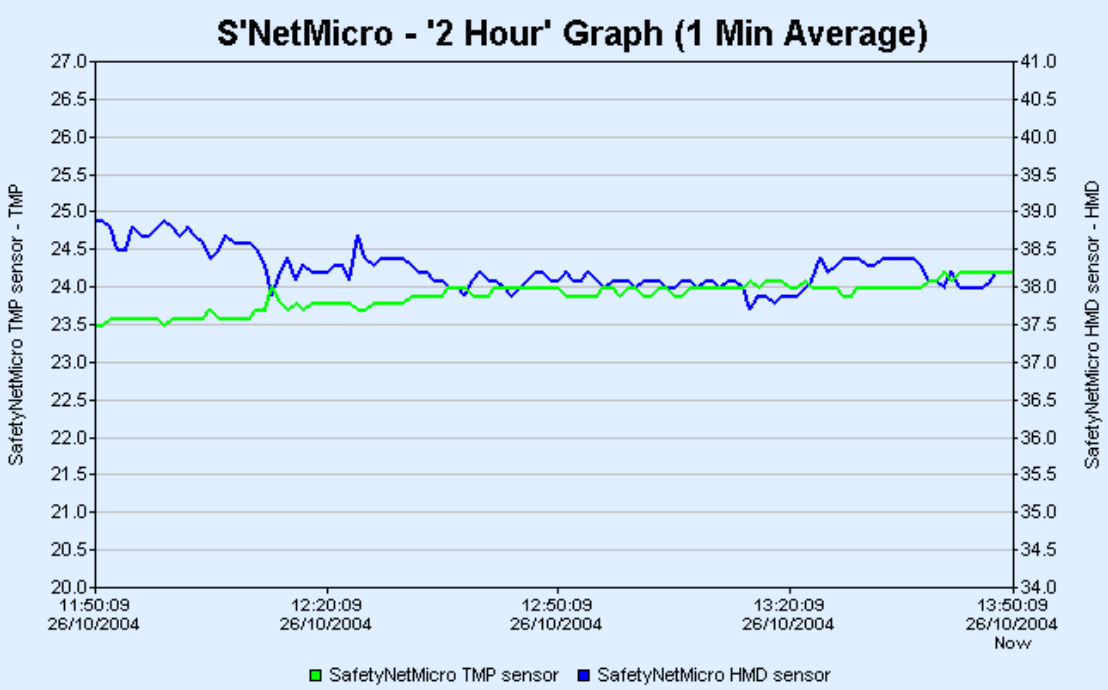
- 2 Hour Graph
- Daily Graph
- Weekly Graph
- Monthly Graph

6.1 2 Hour Graph (1 minute average)

Click on "*Two Hour Graph*" button to refresh data on this graph.

Temperature and humidity sensor data is recorded every 5 seconds; the average for every minute is calculated and then plotted for the last two hours. This graph is useful when immediate response to analogue sensor related alarms are required. For example, if you receive a SMS message stating the temperature or humidity sensor limits were exceeded, you could simply use a browser and view the sensor values noted for the last two hours.

This graph will plot 120 points of data records. (Every minute for 2 hours)

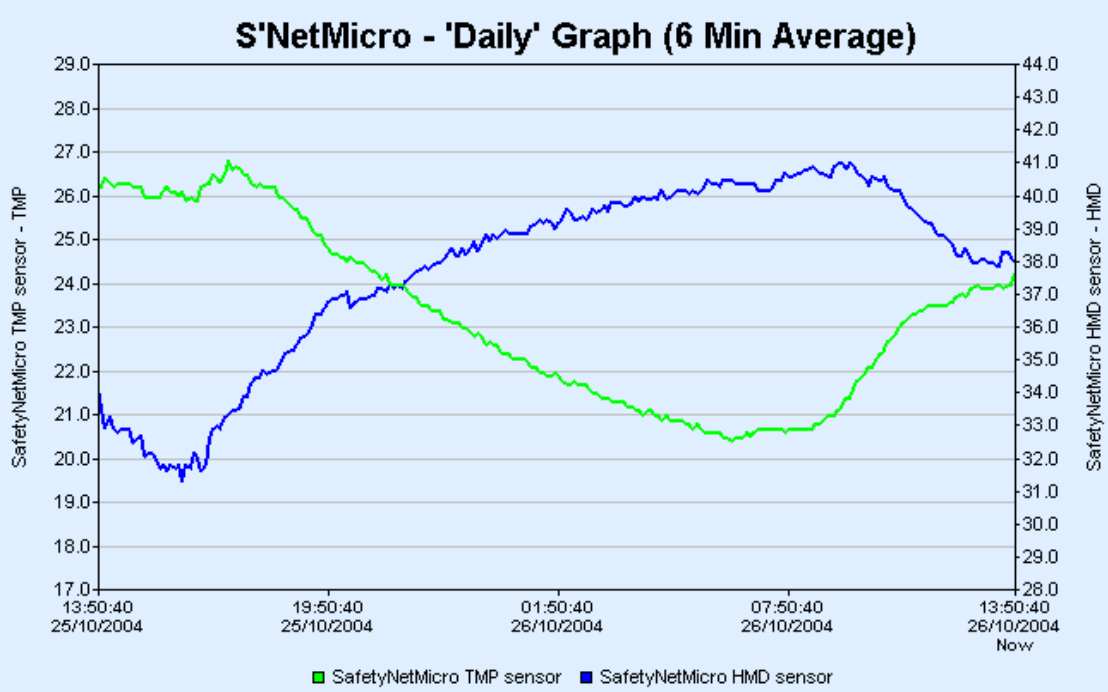


6.2 Daily Graph (6 minute average)

Click on "*Daily Graph*" button to refresh data on this graph.

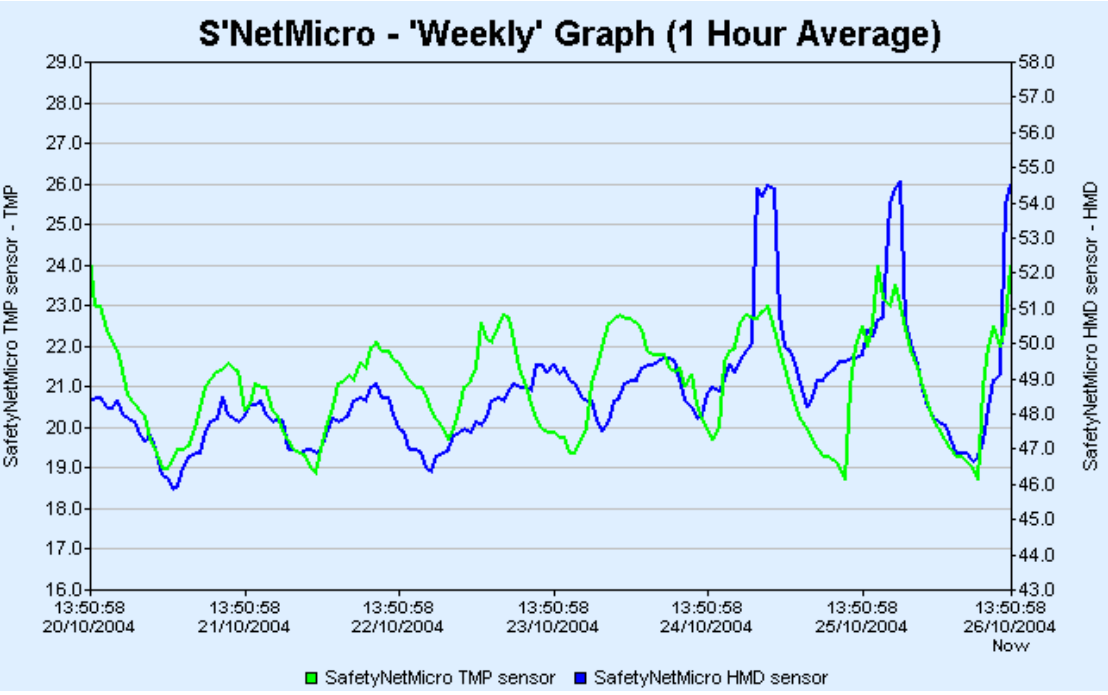
Analogue sensor data average of every 6 minutes is used and plotted for the last 24 hours. This graph is useful to get an overview of the daily temperature or humidity levels of the monitored environment.

This graph will plot 240 points of data records. (Every 6 minutes for 24 hours)



6.3 Weekly Graph (1 hour average)

Analogue sensor data average of every 1 hour is used to plot a graph for the last 7 days.

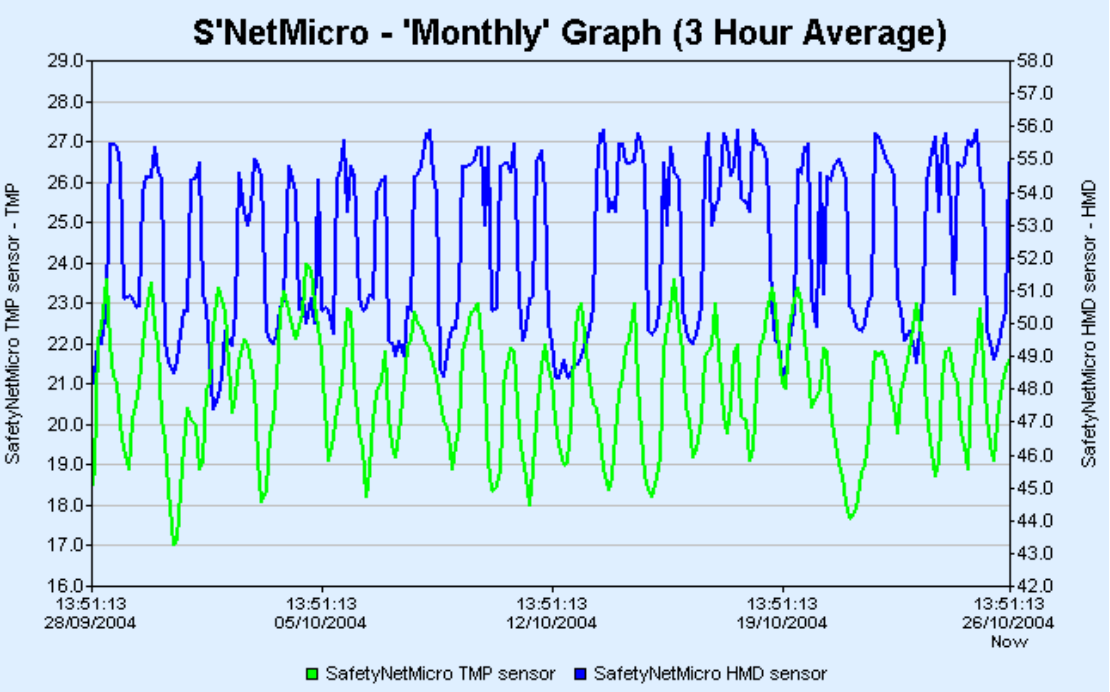


6.4 Monthly Graph (3 hour average)

Click on "*Monthly Graph*" button to refresh data on this graph.

Analogue sensor data average of every 3 hours is used to plot a graph for the last month. This graph is useful to get an overview of the monthly temperature or humidity levels of the monitored environment.

This graph will plot 248 points of data records. (Every 3-hours for 31 days)



7 Alarm and Event Logs on SafetyNet Micro

SafetyNet Micro stores internal log entries for each alarm and event that occurs. These are two separate logs with up to 20 entries of each. When the log reaches more than 20 entries, the oldest entry is removed and the latest entry is added. Therefore, at any given time it is able to review the last 20 entries of alarms and events. To keep a record of the alarms and events, we recommend a print of the table or copy and paste the table to a file (eg: to Notepad) frequently.

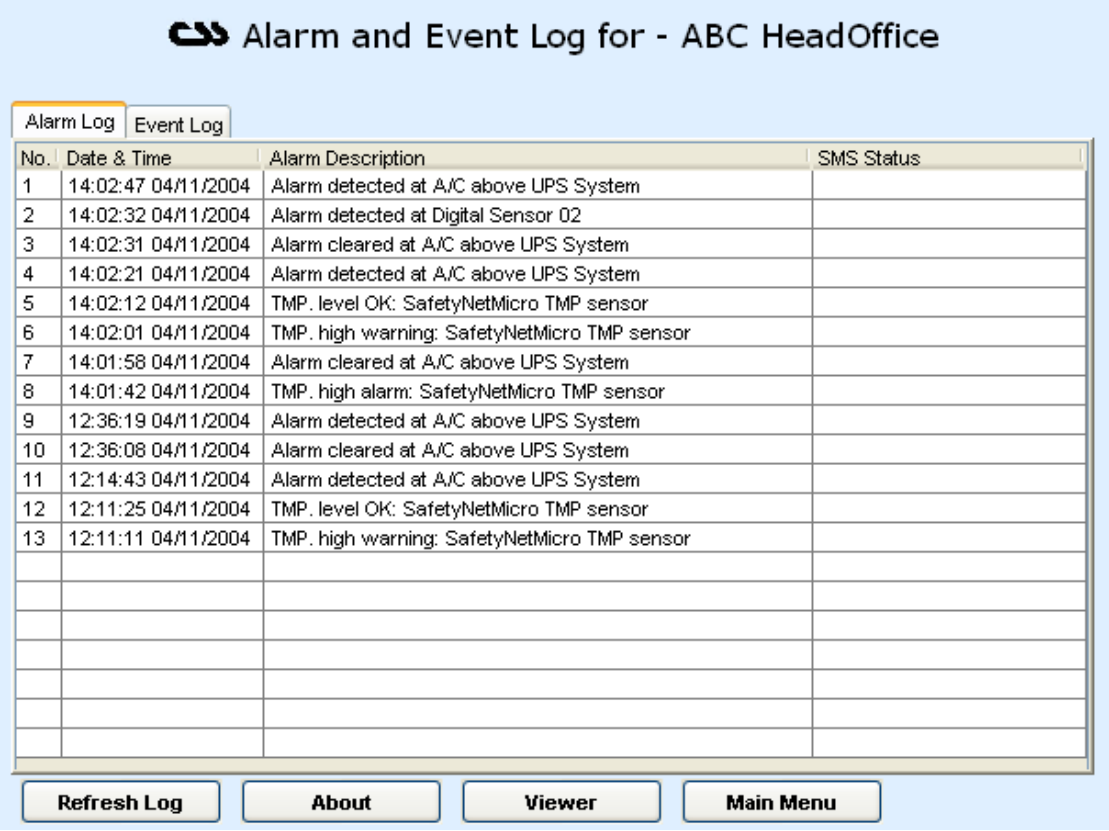
To view the alarm or event log click on "*Alarm & Events*" button given on the Viewer interface.

Each log entry consists a time stamp and a description of the alarm or the event. For sensor related alarms it will include the sensor label in its description for better identification.

7.1 Alarm Log

Any sensor related alarm activation or clearance would be logged in the alarm log. If the internal analogue sensor is installed, and was faulty it will also be logged in the alarm log.

Internal analogue sensor alarms will be logged indicating what threshold value it reached. IP monitoring alarm and the dial tone check error will be also logged in the alarm log.



Loss of Ethernet connection will be logged in the alarm log for models ZSN4001M and ZSN4001MD.

The alarm log contains a column for indicating the SMS status. This will indicate the status of the SMS related to that log entry.

Possible SMS status strings for models ZSN4001, ZSN4001D, ZSN4001MP and ZSN4001MDP are given in the table below. These models send the SMS message content using TCP/IP to a central server. The reliability depends on the networks until the packet reaches the central server and then on Telstra to deliver the message.

SMS Status	Description
SMS info. sent to CSS	SMS message information has successfully been sent to Computer Support Systems. SMS messages would be delivered as configured on the unit.
SMS link failed	SMS server is not active or routers did not allow TCP/IP packets to arrive at the correct destination. Check if the unit has rights to connect to SMS server IP on the SMS port number.
Failed opening TCP/IP link	Typically the firewall is blocking the destination. Check the gateway is correct & contact your Network Administrator. Make sure the firewall has been enabled. (See SMS requirements)
BLANK entry	SMS not to be sent (E.g. clearing of an alarm) or SMS messages are not configured for this type of alarm.

Table 1.0

Possible SMS status strings for models ZSN4001M and ZSN4001MD are given in the table below. These models use the internal PSTN modem to dial out and send SMS messages. The reliability depends on the telephone link provided to the unit. This allows getting notified when the network is down.

SMS Status	Description
SMS message(s) successful	The telephone network SMS gateway received the SMS request successfully. SMS message will be delivered if the mobile phone is turned on.
Failed - No reply from provider	Unit attempted to dial. No reply from the provider for all re-try attempts
Failed - No dial tone detected	Unit attempted to dial. There was no dial tone detected for all re-try attempts
Failed - Line BUSY status reported	Unit attempted to dial. The line was busy for all re-try attempts
Failed - No 'ID=' reply	When dialing up, upon connection the network should reply with ‘ID=”. Unit did not receive such message from the provider.
Failed - 'ID=' request timeout	While waiting for ‘ID=’ a time out occurred.
Failed - Incorrect password	The password sent from the unit is incorrect.
Failed - Password ACK timeout	While waiting for the password acknowledgement a timeout occurred.
Failed - Attempted to send. ACK/NAK timeout	The message content was sent, however a timeout occurred while waiting for the ACK or a NAK
Failed - Provider did not acknowledge msg	Message delivery failed. Message not acknowledged. Please check of phone number is correctly inserted.
Failed - Main time out occurred - max 3 mins	Only 3 minutes is given to send any messages. Message could not be sent due the elapse of 3 minutes
Modem is disabled. Cannot send message	The modem needs to be enabled for a message to be sent. The message sending will not be attempted.
Message in queue. To be sent	The message is currently in the queue. Dialing may have begun or is currently active.

Failed - Abandoned due to reset of unit	While a dial process is active the unit was turned off. The message has not been sent and will not be attempted to. If the alarm is still active after a reboot, the alarm will re-trigger and then a new message will be sent.
BLANK entry	SMS not to be sent (eg: clearing of an alarm) or SMS messages are not configured for this type of alarm.

Table 1.1

Models ZSN4001MP and ZSN4001MDP will have an additional column describing the PPP status for each alarm.

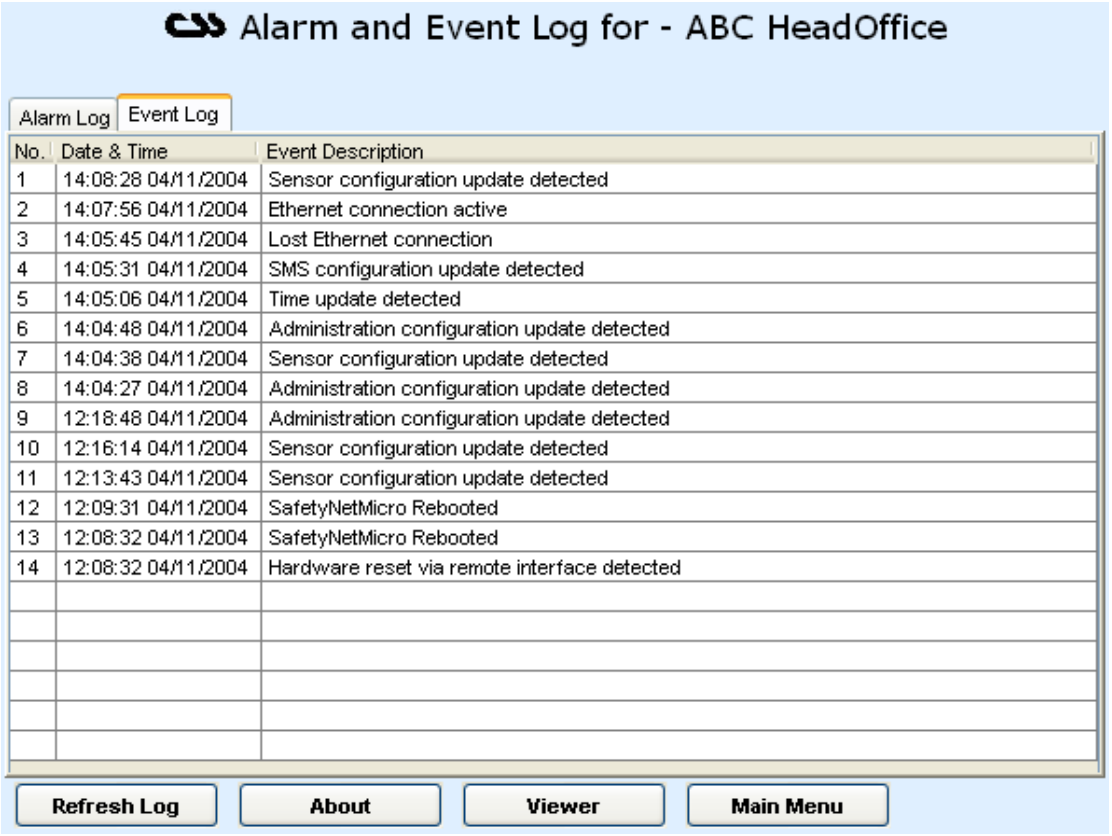
7.2 Event Log

The event log simply logs any internal event within SafetyNet Micro. To view the event log, click on the tab "*Event Log*" once the alarm log is displayed.

Current event entries consist of:

- SafetyNet Micro reboot
- Configuration updates
  - Real time clock on SafetyNet Micro updated.
  - Administration configuration
  - Sensor configuration
  - SMS/Modem configuration
  - SNMP configuration
  - License key registration updates
- Loading of factory defaults via the web interface.
- Hardware reset via the web interface
- Clearing of analogue sensor data for graphs via the web interface
- Clearing of alarm and event logs via the web interface
- Watchdog timer reset – Software error
- Ethernet link down indication *
- Ethernet link up indication *
- Details of driving SafetyBoot by the IP monitoring alarm.

* Only on models ZSN4001 and ZSN4001D

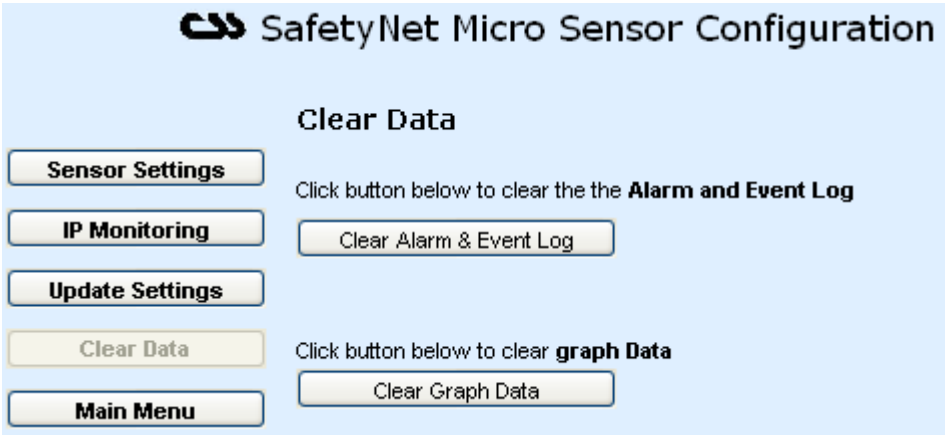


7.2.1 Clearing of Alarm and Event Logs

Logs can be cleared via two methods.

1. Choose to clear the log data only

Use the main menu and enter Senor Configuration. Then select the menu button, “Clear Data”. Now click “Clear Alarm & Event Log”. Upon success, confirmation is given



2. Load factory defaults. (Read section 5.1 on Administration Configuration on what loading factory defaults resets back to defaults)

Both these events will make an entry indicating the clearance of the logs as an event in the event log just after they have been cleared.

8 Operation of SafetyNet Micro

8.1 Basic Operation

SafetyNet Micro will constantly monitor '*enabled*' sensors. It is able to notify any alarm condition via several notification methods those being; SNMP traps, SMS messages, visually on the web interface and a blinking blue LED on the unit.

Any alarm or event will be logged, as an entry in the alarm and event log viewable at any given time. These logs can be cleared upon request by the web interface.

SafetyNet Micro will work out the average analogue sensor data for data plotting. This data is stored locally up to a month and is shown when the required graph is requested. Data can be cleared upon request by the web interface.

Any sensor that is not "*enabled*" under the Sensor Configuration will not be monitored. To disable an existing sensor simply set it as **not** "*enabled*", which will then be disregarded as an active sensor.

It is possible to monitor a particular IP address using the registered feature of IP monitoring. An alarm is indicated if the IP address fails and the administrator could get notified using one of the notifying methods. Read the IP Monitoring section of the manual on chapter 10 for further details on IP monitoring.

PPP is optional on SafetyNet Micro. PPP allows establishing a network connection to the unit via a PSTN telephone line. It will give you access to the web pages of SafetyNet Micro. This will give the opportunity to engage in monitoring in situations where there is no network connection or at remote sites where there is simply no network.

Outgoing PPP allows notification of alarms via an auto PPP dialer. A RAS (Remote Access Server) can be configured to receive SafetyNet Micro PPP connection and deliver the SNMP Traps to the relevant destination. For specific details of PPP, its configuration and operation please refer to appendix A of this document.

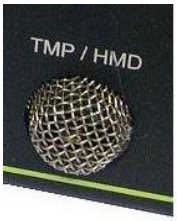
8.2 Sensors

Only sensors supplied by Computer Support Systems may be used with SafetyNet Micro. The types of sensors that are allowed are: -

1 x analogue sensor (temperature and humidity combined - inbuilt)
1 x digital sensor (configurable as a fluid, smoke or a dual contact input sensor)

The digital sensor is a standard RJ45 connection type sensor and connected to the rear panel of SafetyNet Micro.

8.2.1 Temperature and Humidity Sensors



The sensor is inbuilt within the unit and sits behind the tiny wire mesh located on the front of the unit. The ambient temperature and the humidity are reported to the unit via this sensor.

- Low power consumption
- High accuracy and long-term reliability.
- Excellent noise immunity.
- Robust, sealed construction.
- Self-testing; SafetyNet Micro raises an alert of sensor is faulty.
- Immune to most airborne industrial contaminants.

8.2.2 Fluid Detectors

These sensors are intended to be used anywhere where water or moisture can intervene normal operation of the environment. Features of fluid sensors are

- Exclusive mat design for detecting surface water on floors, cabinet bases, etc
- Self-resets once fluid is removed.
- Excellent electrical noise immunity and long term reliability.
- Beep sound when fluid is detected from the sensor itself.
- An option of having a hard metal cover installed for industrial safety.

Only one of these fluid sensors could be installed on SafetyNet Micro.

8.2.3 Smoke Detectors

These sensors will constantly monitor any smoke presence on the premises. LED indication is activated when smoke is present. A manual acknowledgement of the sensor is required if triggered. This is performed by simply turning the sensor anti-clock wise, and un-latching the situation.

The smoke sensor works on a “Normally Closed” (closed circuit) methodology. Hence, if disconnected from SafetyNet Micro, an alarm is raised.

Only one of these fluid sensors could be installed on SafetyNet Micro.

8.2.4 Digital Sensors

SafetyNet Micro allows connecting a dual digital sensor. This is a contact closure sensor, and is capable of detecting open circuits or closed circuits. At the time of configuring digital sensors it is able to specify the sensor be “Normally Open” or “Normally Closed”.

Each of the digital sensors of the dual-sensor carries a trigger delay up to 120 seconds. This is set at the time of installing the digital sensor on the Sensor Configuration Interface. For example, if you set the trigger delay to be 30 seconds, an alarm is raised only if the digital sensor is active for 30 seconds or more. This feature eliminates any spikes that could occur in the monitored environment.

If sensor 3 is selected to be a smoke or a fluid sensor, usage of sensor 4 is not possible.

8.3 Alarms and Alerts

The types of alarms and alerts could be any of the following.

- Alarm trigger (smoke, fluid or digital).
- Exceeding a lower or higher set threshold of the temperature/humidity sensor.
- IP monitoring alarm.
- Dial tone detection failure or modem detection error. *
- Faulty internal analogue sensor.
- Ethernet connection loss. *

* Applicable to models ZSN4001M & ZSN4001MD only

Alarms are triggered only if they are "*enabled*" via the Sensor Configuration web interface. SafetyNet Micro will not monitor non-enabled/disabled sensors. The viewer web interface will indicate a disabled sensor as "spare".

Temperature, humidity, smoke & fluid sensors have a trigger delay of 15 seconds embedded within the software. This will prevent any alarm spikes being treated as an alarm. If the alarms were active for more than 15 seconds they would be triggered. This value is not user-configurable.

The digital sensor trigger delay is variable up to 120 seconds and can be set via software using the web interface.

The remote viewer always shows *almost* real time data, therefore if an alarm threshold is exceeded, it will be shown immediately on the remote viewer. However the actual trigger of alarm occurs only if the trigger delay elapses.

Alarms can be delivered via a PPP link to a specific Network Manager System using SNMP traps with the optional PPP SafetyNet Micro.

8.4 All About the Inbuilt Modem

This applies to models ZSN4001M and ZSN4001MD only.

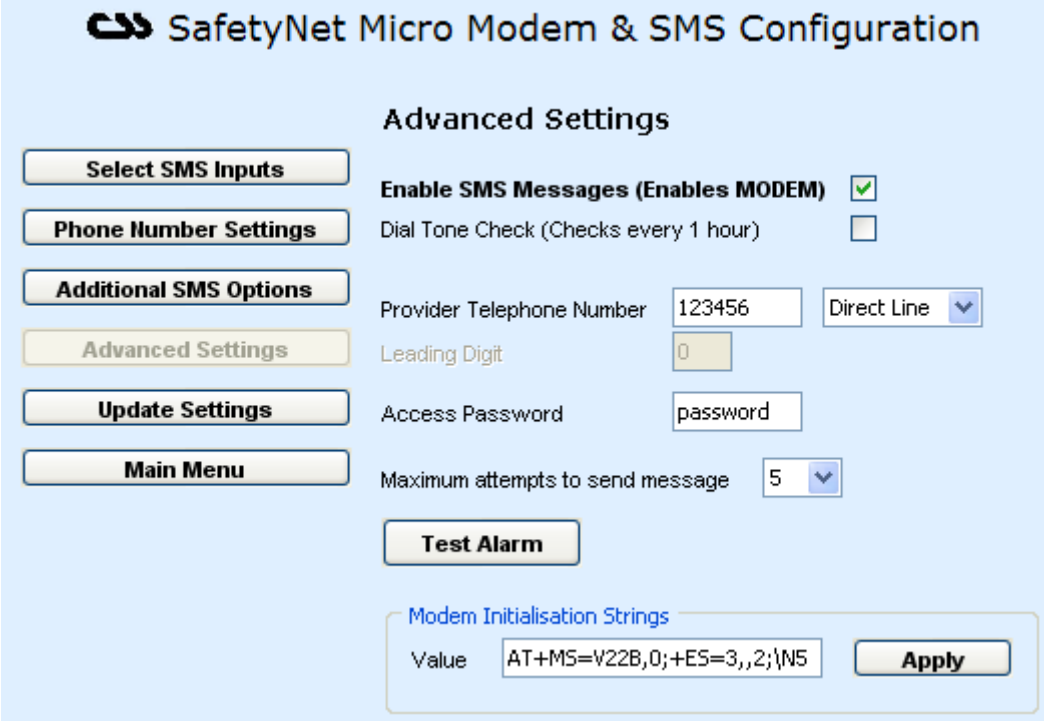
The inbuilt modem is capable of notifying a mobile phone when an alarm condition occurs, even when the network is down. This makes SafetyNet Micro a reliable device even when the network is down.

To activate the modem, it has to be enabled. The Modem Configuration web interface will allow configuring the modem and to test its functionality.

The modem is able to check for the dial tone every hour to ensure that there is a reliable telephone connection. On a dial tone failure after three consecutive checks the unit will log an entry in the alarm log indicating the failure. Despite having this alarm active if a new SMS is to be sent, the unit will still attempt to send the message.

The connected telephone line type has to be notified to SafetyNet Micro. The types that are allowed are a direct line or an **analogue** PABX line with a leading digit in front. These parameters can be entered on the Modem Configuration interface.

By clicking the "Test Alarm" button, it is able to test the delivery of the SMS messages to all the numbers entered in the interface. Ensure that the latest configuration is **updated** on the interface with the latest phone numbers before proceeding with this option.



8.4.1 Modem Initialisation Strings

The modem initialization strings are expected to be set as default, unless connection issues persist between the provider and SafetyNet Micro.

The current default setting value is:
AT+MS=V22B,0;+ES=3,,2;\N5

It is recommended that the user is familiar with Hayes AT commands (both basic and extended.
The basic set of modem init strings can be set as per guide below.

Generic Modem Commands

Command: \N		**Operating Mode – Error Correction**
Description:		Controls the preferred error-correcting mode to be negotiated in a subsequent data connection.
Default:		5
Defined Values:	\N0	Selects normal speed buffered mode (Disables error- correction mode). (Forces &Q6.)
	\N1	Serial interface selected: Selects direct mode and is equivalent to&M0, Q0 mode of operation. (Forces &Q0.) Parallel interface selected: Same as \N0.
	\N2	Selects reliable (error-correction) mode. The modem will first attempt a LAPM connection and then an MNP connection. Failure to make a reliable connection results in the modem hanging up. (Forces &Q5, S36=4, and S48=7.)
	\N3	Selects auto-reliable mode. This operates the same as \N2 except failure to make a reliable connection results in the modem falling back to the speed buffered normal mode. (Forces &Q5, S36=7, and S48=7.)
	\N4	Selects LAPM error-correction mode. Failure to make an LAPM error-correction connection results in the modem hanging up. (Forces &Q5 and S48=0.) Note: The -K1 command can override the \N4 command.

\N5 Selects MNP error-correction mode. Failure to make an MNP errorcorrection connection results in the modem hanging up. (Forces &Q5, S36=4, and S48=128.)

Modulation Control Commands

Command: +MS — Modulation Selection

Description: This extended-format compound parameter controls the manner of operation of the modulation capabilities in the modem. It accepts six subparameters.

Syntax:
+MS=[<carrier>
[,<automode>
[,<min_tx_rate>
[,<max_tx_rate>
[,<min_rx_rate> ,<max_rx_rate>]]]]]
Where possible <carrier>, <min_tx_rate>, <max_tx_rate>, min_rx_rate>, and <max_rx_rate> values are listed in table below

Modulation	<carrier>	Possible (<min_rx_rate>, <min_rx_rate>, (<min_tx_rate>), and <max_tx_rate>) Rates (bps)
Bell 103	B103	300
Bell 212	B212	1200 Rx/75 Tx or 75 Rx/1200 Tx
V.21	V21	300
V.22	V22	1200
V.22 bis	V22B	2400 or 1200
V.23	V23C	1200
V.32	V32	9600 or 4800
V.32 bis	V32B	14400, 12000, 9600, 7200, or 4800
V.34	V34	33600, 31200, 28800, 26400, 24000, 21600, 19200, 16800, 14400, 12000, 9600, 7200, 4800, or 2400
56K	K56	56000, 54000, 52000, 50000, 48000, 46000, 44000, 42000, 40000, 38000, 36000, 34000, 32000
V.90	V90	56000, 54667, 53333, 52000, 50667, 49333, 48000, 46667, 45333, 44000, 42667, 41333, 40000, 38667, 37333, 36000,34667, 33333, 32000, 30667, 29333, 28000
V.92 downstream	V92	56000, 54667, 53333, 52000, 50667, 49333, 48000, 46667, 45333, 44000, 42667, 41333, 40000, 38667, 37333, 36000,34667, 33333, 32000, 30667, 29333, 28000
V.92 upstream	V92	48000, 46667, 45333, 44000, 42667, 41333, 40000, 38667, 37333, 36000, 34667, 33333, 32000, 30667, 29333, 28000, 26667, 25333, 24000

Defined Values: <carrier> A string that specifies the preferred modem carrier to use in originating or answering a connection. <carrier> values are strings of up to eight characters, consisting only of numeric digits and upper case letters. <carrier> values for ITU standard modulations take the form: <letter><1-4 digits><other letters as needed>. Defined values are listed in Table above.

<automode> A numeric value which enables or disables automatic modulation negotiation (ITU-T V.32*bis* Annex A or V.8).
0 = Automode disabled.
1 = Automode enabled. (Default.)

<min_rx_rate> and <max_rx_rate>
Numeric values which specify the lowest (<min_rx_rate>) and highest (<max_rx_rate>) rate at which the modem may establish a receive connection. May be used to condition distinct limits for the receive direction as distinct from the transmit direction. Values for this

subparameter are decimal encoded, in units of bit/s. The possible values for each modulation are listed in Table above. Actual values will be limited to possible values corresponding to the entered <carrier> and fallback <carrier> as determined during operation. (Default = lowest (<min_rx_rate>) and highest (<max_rx_rate>) rate supported by the selected carrier.)

<min_tx_rate> and <max_tx_rate>

Numeric values which specify the lowest (<min_tx_rate>) and highest (<max_tx_rate>) rate at which the modem may establish a transmit connection. Non-zero values for this subparameter are decimal encoded, in units of bit/s. The possible values for each modulation are listed in Table above. Actual values will be limited to possible values corresponding to the entered <carrier> and fall-back <carrier> as determined during operation. (Default = lowest (<min_tx_rate>) and highest (<max_tx_rate>) rate supported by the selected carrier.).

Error Control Commands

Command: +ES — Modulation Selection

Description: This extended-format command specifies the initial requested mode of operation when the modem is operating as the originator. Optionally specifies the acceptable fallback mode of operation when the modem is operating as the originator, and optionally specifies the acceptable fallback mode of operation when the modem is operating as the answerer. Accepts three numeric subparameters.

Default: Varies by request

Defined Values:

<orig_rqst>

Decimal number specifies the initial requested mode of operation when the modem is operating as the originator. The options are:

+ES0 Initiate call with Direct Mode.
+ES1 Initiate call with Normal Mode (also referred to as Buffered Mode) only.
+ES2 Initiate V.42 without Detection Phase. If V.8 is in use, disable V.42 Detection Phase.
+ES3 Initiate V.42 with Detection Phase. (Default.)
+ES4 Initiate MNP.
+ES6 Initiate V.80 Synchronous Access Mode when connection is completed, and Data State is entered. (See +ESA and +ITF commands.)
+ES7 Initiate Frame Tunneling Mode when connection is complete, and Data Mode is entered.

<orig_fbk>

Decimal number specifies the acceptable fallback mode of operation when the modem is operating as the originator.

+ES0 LAPM, MNP, or Normal Mode error control optional. (Default)
+ES1 LAPM, MNP, or Direct Mode error control optional.
+ES2 LAPM or MNP error control required; disconnect if error control is not established.
+ES3 LAPM error control required; disconnect if error control is not established.
+ES4 MNP error control required; disconnect if error control is not established.

<ans_fbk>

Decimal number specifies the acceptable fallback mode of operation when the modem is operating as the answerer or specifies V.80 Synchronous Access Mode.

+ES0 Direct Mode.
+ES1 Error control disabled, use Normal Mode.
+ES2 LAPM, MNP, or Normal Mode error control optional. (Default)
+ES3 LAPM, MNP, or Direct Mode error control optional.

+ES4 LAPM or MNP error control required; disconnect if error control is not established.
+ES5 LAPM error control required; disconnect if error control is not established.
+ES6 MNP error control required; disconnect if error control is not established.
+ES8 Initiate V.80 Synchronous Access Mode when connection is completed and Data State is entered (see +ESA and +ITF).
+ES9 Initiate Frame Tunneling Mode when connection is complete, and Data Mode is entered.

Examples:

+ES=6 Enable V.80 Synchronous Access Mode originator.
+ES=6 Enable V.80 Synchronous Access Mode originator.
+ES=,,8 Enable V.80 Synchronous Access Mode answerer.
+ES=6,,8 Enable V.80 Synchronous Access Mode.
+ES=3 Enable V.42 with Detection Phase originator. Disable V.80 Synchronous Access Mode originator.
+ES=,,2 Allow LAPM, MNP, or Normal Mode connection answerer. Disable V.80 Synchronous Access Mode answerer.
+ES=3,,2 Enable V.42 with Detection Phase originator, allow LAPM, MNP, or Normal Mode connection answer. Disable Synchronous Access Mode originator and answerer.

To apply the appropriate modem initialisation sting (commands separated by ;) enter value in the value field and click on the 'Apply' button.

8.5 Network Interface and Traffic from SafetyNet Micro

SafetyNet Micro network interface connects the unit to the local network. The connection is a RJ45 Ethernet 10Base-T connector. Network compatibility is Ethernet version 2.0/IEEE 802.3.

The type of traffic on SafetyNet Micro is mainly TCP/IP and UDP. UDP packets are sent back and forth when the user interfaces are active. There are no UDP packets sent on to the network when the user interface is not loaded except for the SNMP information. The IP monitoring feature sends ICMP packets based on the frequency specified. SNMP operates on UDP on ports 161 and 162.

If the device is DHCP enabled, at boot up the unit configures its network interface after obtaining the network parameters from the DHCP server using UDP.

SafetyNet Micro has a TCP/IP, HTTP web server that hosts the user interface on port 80.

The models without the modem uses TCP/IP in sending the SMS information to a central server hosted by Computer Supported Systems. The current destination for this service is at 210.23.143.19. The port used is 42755. If you have selected to send SMS messages using this option, please configure our firewall, thus allowing a successful connection.

9 SMS Messages from SafetyNet Micro

9.1 Introduction to SMS Messages from SafetyNet Micro

SafetyNet Micro is capable of sending SMS messages via two methods depending on the model.

1. Using the network connection and by connecting with a SMS server application hosted on the Internet by Computer Support Systems.
2. Using the internal PSTN modem and sending the SMS independent of the network. (Reliable when the network is down)

9.2 SMS Messages using the Network Interface

This applies to models ZSN4001 and ZSN4001D.

SafetyNet Micro converts any warning, alarms or shutdown messages into TCP/IP packets and transmits them over the Internet to a predetermined IP address. The server at this IP address handles sending the SMS to predetermined numbers set by SafetyNet Micro.

9.2.1 Requirements for SMS Messages via the Network

The requirements to successfully send SMS messages via the network are

- Access to the external machine with IP address 210.23.143.19 on port 42755 from SafetyNet Micro to establish a TCP/IP link. (Active Internet connection / a configured firewall)
- SMS features turned on by using the appropriate registration key for SMS software.
- Correct configuration on the SMS configuration web interface. (Sensors associated with SMS messages and correct phone numbers entered)

9.2.2 Limitations

- The SMS message is sent only up to the three mobile phone numbers entered on the SMS configuration web interface.
- Clearing of an alarm is not notified via SMS messages.
- The time stamp noted on the SMS message is extracted from SafetyNet Micro.
- SMS messages rely on the PSTN (Public Switched Telephone Network) and the Internet on distribution.
- SMS messages are delivered only when the mobile phone is switched on.

9.3 SMS Messages using the internal PSTN Modem

This applies to models ZSN4001M and ZSN4001MD.

SafetyNet Micro has an inbuilt modem that is able to dial out when an alarm condition is triggered. The operation of the modem and associating the alarms to mobile phone numbers are performed on the Modem Configuration web interface.

SafetyNet Micro converts any warning, alarms or shutdown messages, dials the telephone provider on the given number and sends the SMS messages via the PSTN (Public Switched Telephone Network).

9.3.1 Requirements for SMS Messages using the Modem

The requirements to successfully send SMS messages via the inbuilt modem are

- An active telephone line provided to the unit.
- Correct configuration on the Modem Configuration web interface. (Sensors associated with SMS messages and correct phone numbers entered)
- Subscribe to a telephone network provider for paging services. (Described in detail on 9.3.2)

9.3.2 Subscribing to a Paging Service to Receive SMS Messages

There are several network providers that allow sending SMS messages via a dial up process. SafetyNet Micro uses this service to send SMS messages on alarm activation.

To successfully send SMS messages via the modem the requirements are to have the dialup number and a password configured along with a telephone line connected to the back of the unit. Information to subscribe can be obtained by the telephone network provider. SafetyNet Micro has been tested with the following telephone network providers.

9.3.2.1 Telstra

Telstra provides a product named as "SMS Access Manager". Subscribing to this service will provide the necessary password and the dialup number.

More information about "***Telstra mobile SMS Access Manager***" can be found at http://www.telstra.com.au/mobile/business/products/sms.htm#manager

The cost involved per SMS message is given on this website.

The application forms to subscribe to ***Telstra mobile SMS Access Manager*** can be retrieved from the link below

For companies, associated incorporations and other body corporate institutions
http://www.telstra.com.au/mobile/business/products/pdf/smsbody.pdf

For partnership, sole traders, individuals and other non-body corporate institutions
http://www.telstra.com.au/mobile/business/products/pdf/smsnonb.pdf

For more information contact Telstra on 1800 200 010.

Please note: Chapter 9.3.2.1 information has be retrieved by Telstra's website at http://www.telstra.com.au/mobile/business/products/sms.htm#manager as at 24/02/2005. Information may change due to modifications by Telstra at any given time. Always refer to the current website for the latest information.

9.3.2.2 Orange (Hutchison Telecommunications (Aust) Limited)

To enquire about accessing the SMS gateways of Orange, contact Orange on 1300 133 585 (Australia wide) and speak to a customer care team member.

Orange will assist to set up and subscribe for the service by giving further details on the product. Upon receiving the dialup number and the password SafetyNet Micro will use Orange's service to deliver SMS messages.

Use Mr. Steve Hristofski as a reference at the time of communicating with Orange.

9.3.3 Limitations

- The SMS message is sent only up to the three mobile phone numbers entered on the Modem configuration web interface.
- Clearing of an alarm is not notified via SMS messages.
- The time stamp noted on the SMS message is extracted from SafetyNet Micro.
- SMS messages rely on the PSTN (Public Switched Telephone Network) on distribution.
- SMS messages are delivered only when the mobile phone is switched on.

9.4 Sample Messages

Some of the sample SMS messages would look like: (Unit name: MY SAFETYNET)

Sensor Alarms

SafetyNet message from MY SAFETYNET. Msg content: Low temperature warning detected at: Internal Temperature Sensor 18:04:56 21/09/2004

SafetyNet message from MY SAFETYNET. Msg content: High temperature alarm detected at: Internal Temperature Sensor 14:03:45 20/09/2004

SafetyNet message from MY SAFETYNET. Msg content: Alarm detected at: General UPS alarm 19:17:45 02/10/2004

General alerts

SafetyNet message from MY SAFETYNET. Msg content: Hardware error detected: Internal TMP/HMD sensor faulty 13:44:37 02/04/2004

SafetyNet message from MY SAFETYNET. Msg content: Lost Ethernet connection 10:33:06 27/05/2004

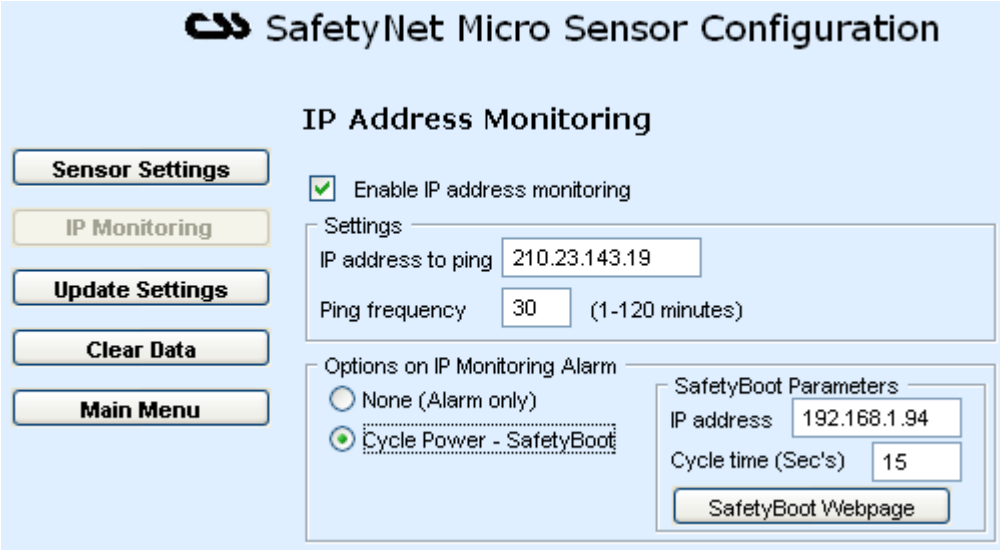
10 IP Monitoring on SafetyNet Micro

10.1 Introduction to IP Monitoring on SafetyNet Micro

SafetyNet Micro is capable of pinging any ICMP enabled network device. Upon ICMP receipts, SafetyNet Micro can monitor the presence and activity of the remote network device. This feature is a registered option on SafetyNet Micro.

The IP address to monitor, frequency of monitoring and the action to be taken is configured at Sensor Configuration under the sub menu *IP Monitoring.*

If the physical Ethernet connection is not present, IP monitoring halts until connection is detected.



If the monitored IP address goes down, or a router in between goes down, causing a non-reply to the ICMP request (Ping request). SafetyNet Micro issues two consecutive ping commands a minute apart for clarification to detect of the device has failed. After three consecutive reply failures an alarm is triggered and the action to be taken will be executed. The following options of action are available.

1. Alarm only.

2. Alarm and drive SafetyBoot.

   SafetyBoot is a product by Computer Support Systems that operates as a remote online 240V A/C power switch. By entering the parameters of SafetyBoot on SafetyNet Micro and the period to cycle power, SafetyNet can issue commands to trigger a power cycle thus causing 240V to be turned off and then on for the duration specified. Effectively this will reboot any remote device that could be in a *stalled* situation.

   For SafetyBoot to successfully cycle power, it has to be in a turned ON situation. Any error condition will be logged on SafetyNet Micro event log on this action.

11 SNMP on SafetyNet Micro

11.1 Introduction to SNMP Features on SafetyNet Micro

SafetyNet Micro is a SNMP (Simple Management Network Protocol) agent. The current status of any sensor including the current temperature or humidity values from the internal analogue sensor can be retrieved via SNMP polling techniques.

On alarm or on clearance of an alarm, SafetyNet Micro sends SNMP trap notifications up to four dedicated network managers. On boot up and on any configuration update, SafetyNet Micro will send a trap indicating the update to these network managers.

We assume that you are familiar with SNMP to use SNMP features and to feel comfortable with the rest of this chapter. SafetyNet Micro uses SNMP V1 standards.

11.2 SNMP Implementation

Computer Support Systems enterprise ID is 14748.

SafetyNet Micro supports the SNMP System group in the MIB-II Objects SysDescr, sysObjectID, sysUpTime, sysContact & sysName.

The private MIB (Management Information Base) implements the following objects.

Object	Description
snMicroTemperatureReading OID: 1.3.6.1.4.1.14748.1.5.1.1	Current SafetyNet Micro Temperature Reading (use multiplier 0.1 for actual reading)
snMicroHumidityReading OID: 1.3.6.1.4.1.14748.1.5.1.2	Current SafetyNet Micro Humidity Reading (use multiplier 0.1 for actual reading)
snMicroDigitalSensorOneReading OID: 1.3.6.1.4.1.14748.1.5.1.3	SafetyNet Micro Digital Sensor 01 Status (0 = OFF, 1 = ON)
snMicroDigitalSensorTwoReading OID: 1.3.6.1.4.1.14748.1.5.1.4	SafetyNet Micro Digital Sensor 02 Status (0 = OFF, 1 = ON)
safetyNetMicroTemperature OID: 1.3.6.1.4.1.14748.1.5.2.2 safetyNetMicroHumidity OID: 1.3.6.1.4.1.14748.1.5.2.3	An integer that describes which region temperature or humidity sensor is currently at. Alarm for temperature or humidity at 0 = level OK 1 = level at high warning limit 2 = level at high alarm limit 3 = level at high shutdown limit 4 = level at low warning limit 5 = level at low alarm limit 6 = level at low shutdown limit
safetyNetMicroAlarmSensor OID: 1.3.6.1.4.1.14748.1.5.2.4	An integer that describes which alarm is active. Alarm/Alert on Sensor 1 = Temperature 2 = Humidity 3 = Digital 01 4 = Digital 02 5 = IP Monitoring
safetyNetMicroSensorCleared OID: 1.3.6.1.4.1.14748.1.5.2.5	An integer that describes which alarm is cleared. Alarm cleared on Sensor 3 = Digital 01 4 = Digital 02 5 = IP Monitoring
safetyNetMicroSWNotification OID: 1.3.6.1.4.1.14748.1.5.2.6	An integer that describes a software notification. Software Notification 0 = Software watchdog timer reset 1 = Device reset manually via software 2 = Memory self-check failed, contact CSS 3 = Administration configuration (device settings/ password) update detected

	4 = Sensor configuration update detected 5 = Time update detected 6 = SMS/Modem configuration detected 7 = SNMP configuration detected 8 = Graph data cleared via web interface 9 = Alarm and event log cleared via web interface 10 = Firmware update detected 11 = Factory defaults loaded 12 = IP monitoring alarm activated SafetyBoot power cycle command 13 = IP monitoring alarm attempted to activate SafetyBoot power cycle command, aborted due to SafetyBoot being OFF 14 = IP monitoring alarm attempted to communicate with SafetyBoot. No response from SafetyBoot. Please check IP address of SafetyBoot 15 = Test alarm initiated via the web interface. 16 = License/Registration key(s) updated 17 = PPP Session established by an external user 18 = PPP Session auto initiated by SafetyNet Micro
safetyNetMicroHWNotification OID: 1.3.6.1.4.1.14748.1.5.2.7	An integer that describes a hardware notification. Hardware Error 1 = Temperature/Humidity sensor faulty or disconnected 2 = Temperature/Humidity sensor back in order 3 = Modem not detected. Modem initialisation error. SMS messages will fail. 4 = No response over 45 seconds. Abandoned SMS 5 = No dial tone. Abandoned sending SMS 6 = BUSY tone. Abandoned sending SMS 7 = Time out on receiving 'ID ='. Abandoned SMS 8 = Service provider did not respond with 'ID='. Abandoned sending SMS 9 = Password ACK timeout. Abandoned sending SMS 10 = Service provider did not acknowledge SMS password. Abandoned sending SMS 11 = Message attempted to be sent. ACK or NAK timeout. Abandoned sending SMS 12 = Message NAK by service provider. Abandoned sending SMS 13 = Service provider dropped call due to length of call exceeded maximum time. Abandoned sending SMS 14 = Routine dial tone check failed. Please check if telephone cable is connected to the modem 15 = Dial tone detected by modem 16 = Ethernet disconnection notified via PPP
safetyNetMicroMsgString OID: 1.3.6.1.4.1.14748.1.5.2.1	A trap will contain this object. It will give more detailed information on alarms/alerts/notifications.

Table 2.0

CSS.MIB implements TRAP-TYPE objects defined by RFC-1215.

Trap Number	Trap-Type	Description
2	hardwareErrorNotification	A hardware error notification trap is sent when any of the hardware goes into an alarm stage.
3	AlarmNotification	An alarm notification trap is sent when any of the monitored inputs go into an alarm stage.
4	AlarmClearNotification	An alarm clear notification trap is sent when any of the monitored inputs go into an alarm clear stage after being at an alarm stage.
5	softwareNotificationUpdate	A software notification update trap is sent when any an update or configuration change is detected on a unit.
6	softwareErrorNotification	A software error notification trap is sent when

		some kind of unwanted software error occurs within the unit.

Table 2.1

Refer to the file CSS.MIB under the SafetyNet Micro product CD-ROM under the folder MIB for further details on the Management Information Base. The latest CSS.MIB is also available at http://www.csspl.com.au

11.3 Requirements

- Registration key for SNMP software.
- A Network Manger System installed on your network or a SNMP sniffer program installed on your PC to detect SNMP traps.
- A correct SNMP configuration web interface setting.

11.4 How to Receive Traps

If the read community is set according to the local network SNMP read community, on alarm, SafetyNet Micro will send a trap out to each network manager IP address defined on its SNMP web interface.

SafetyNet Micro sends a “cold start” trap at a boot up. Upon a configuration update it also sends an update notification as a trap.

11.5 Setting the MIB

Use the CSS.MIB file given on the CD-ROM for SafetyNet Micro to set the MIB structure settings. The latest MIB file is also located at http://www.csspl.com.au. The SNMP software will allow to configure/add paths to where the MIB file is. Read the SNMP software help files to find out how to apply MIB paths.

Once the MIB path is effectively applied the trap bindings will indicate the details of the trap message.

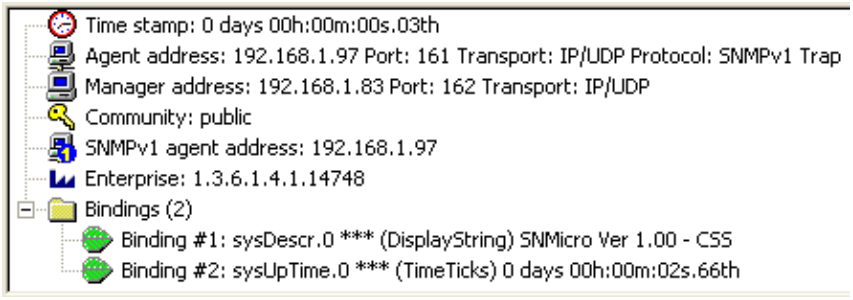
11.6 Interpreting SafetyNet Micro Traps

Every SNMP trap is accompanied by a string, which describes the notification in plain simple English.

In most cases there is another object that holds an integer value(s) that gives indication to which sensor is involved or what type of an alarm it is. Based on this integer value, it is possible to set the network manager software to perform any other third party action as desired. It is also possible to get the network manger software to poll the current sensor status periodically, and to check if there are any alarms active.

A few samples of the SNMP traps detect on a SNMP sniffer programs is depicted below.

Coldstart trap

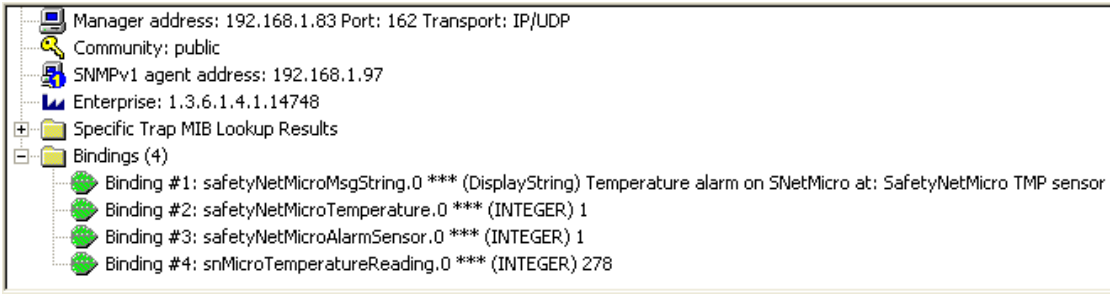


The bindings in the above image give indication of

1. System description: Gives the software version and manufacturer name.
2. System up time: How long the device has been up for.

The above bindings are objects on the MIB-II implementation.

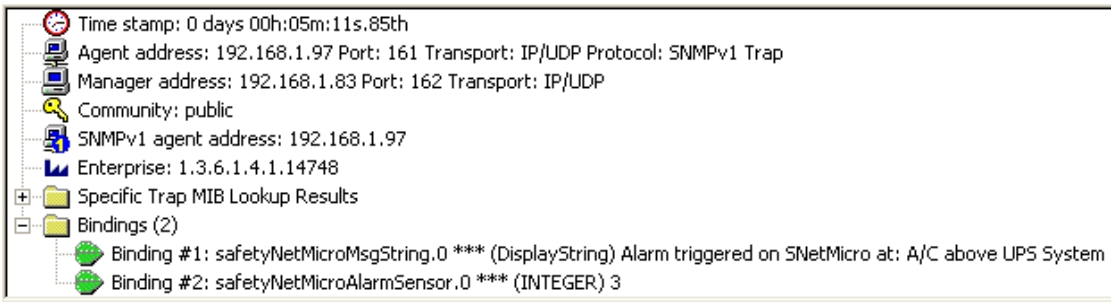
Temperature alarm trap



The bindings in the above image give indication of

1. Message string
2. Which region the analogue sensor value falls to (1 = Analogue sensor one at high warning limit, see table 2.0 under section 11.2 for details)
3. What sensor it arrived from; in the above case, temperature sensor one.
4. The reading of the sensor value; 27.8 degrees.

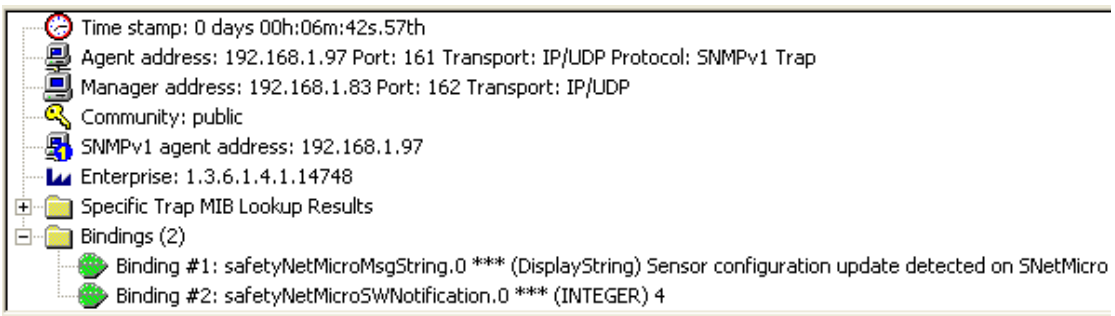
A digital sensor alarm trap (A/C alarm)



The bindings in the above image give indication of

1. Message string
2. It is arriving from sensor number 3, which has been configured as an A/C type alarm.

A configuration update notification



The bindings in the above image give indication of

1. Message string

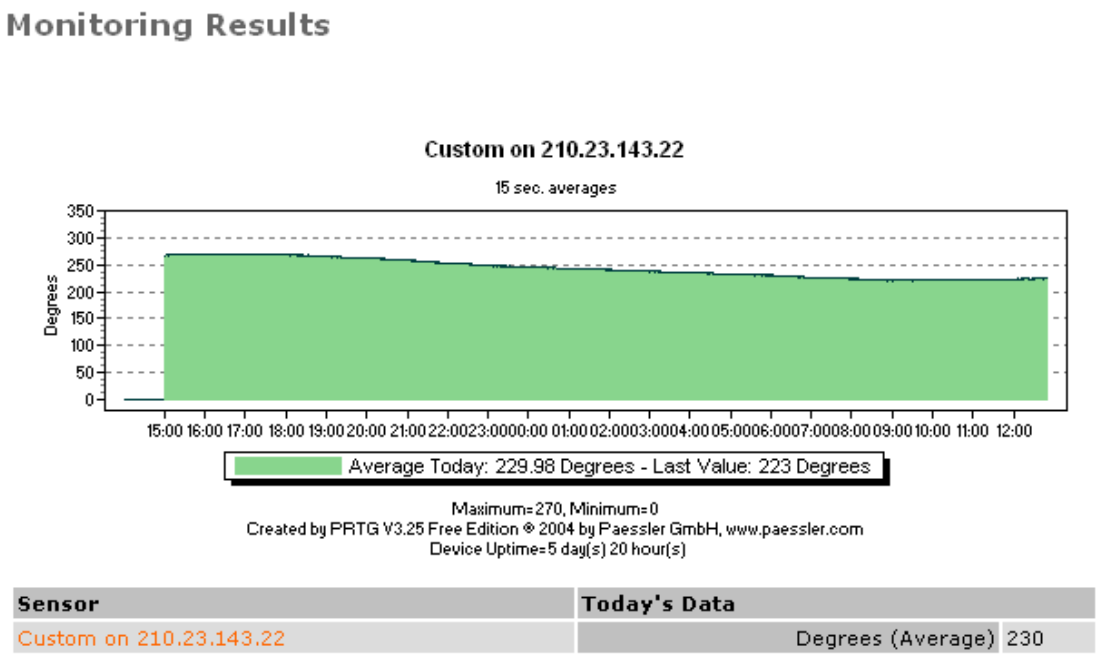
2. Software notification number 4, which is interpreted as Sensor configuration change detection on SafetyNet Micro.

11.7 SNMP Polling

It is possible for the Network Manager Software (NMS) to poll the current sensor status and values of analogue sensors periodically and store for graphing purposes. SafetyNet Micro updates the SNMP objects under snmReadings (OID: 1.3.6.1.4.1.14748.1.5.1.X) every second with its current values. For digital alarms the poll reply will indicate 1 or 0, where 1 is interpreted as an active alarm and 0 as an inactive alarm. If sensors are disabled, polled reply will indicate a zero value.

The value retrieved for temperature or humidity sensors is an integer hence a temperature or humidity value is shown as a multiplication of 10. Most SNMP graphing tools provide a method to view the graph by using a customised multiplier. In this case, use the multiplier 0.1 to retrieve the exact value. For example, temperature value 25.6°C is retrieved as 256 & humidity value 60.4% is retrieved as 604.

Below is sample screen shot of a temperature sensor graph polled via SNMP using a tool named as Paessler Router Traffic Grapher. (http://www.paessler.com)



12 Hardware Specifications

Device Model: SafetyNet Micro Version 1.00 & Version 1.00M

Physical Dimensions

- Dimensions: 135 mm W X 43 mm H (1 RU) X 108 mm D (1/3 RU unit)
- Weight: Models ZSN4001M, MP, MD & MDP 0.95 kg
  Models ZSN4001 & ZSN4001D 0.75 kg

Network Interface

- RJ45 Ethernet 10Base-T, Realtek Semiconductors
- LED indication: 10Base-T TX Activity, Full/half duplex.
- Network Compatibility: Ethernet: Version 2.0/IEEE 802.3

Inbuilt Modem (Socket Optional)

- Data format: V.32bis/14.4K data rates
- Error correction: V.42 (LAP-M or MNP 2-4)
- Data compression: V.42bis, MNP 5
- Power consumption: Typical 117mA (.58W @ 5V DC); Maximum 118mA (0.61W @ 5.25V DC)
- Operational temperature: 0 to +70°C
- Humidity range: 20 - 90%, non condensing

Inbuilt Modem (RJ45 for PPP - Optional)

- Data format: V.92bis/28.8K data rates
- Error correction: V.42 (LAP-M or MNP 2-4)
- Data compression: V.42bis, MNP 5
- Power consumption: Typical 117mA (.58W @ 5V DC); Maximum 118mA (0.61W @ 5.25V DC)
- Operational temperature: 0 to +70°C
- Humidity range: 20 - 90%, non condensing

Inbuilt Analogue Sensor

- Humidity Accuracy ±3.5,
- Temperature Accuracy ±0.5 @ 25°C
- Range –20°C to 100°C and 0 to 100%
- Power consumption 28µA

SafetyNet Micro Operating Conditions

- Temperature range: -20°C to +70°C; Resolution: 0.1°C
- Humidity range: 5 - 95%, non condensing; Resolution: 0.1%RH

Total Unit Power Requirements

- Operating voltage: 9 - 12V
- Input power: 9 - 12V DC Plug pack or 48V DC supply
- Current usage: Models ZSN4001M & ZSN4001MD 250-270mA @12V DC
  Models ZSN4001 & ZSN4001D 150 @12V DC

13 Troubleshooting

This section of this manual will give tips to troubleshoot SafetyNet Micro without having to contact technical support staff from Computer Support Systems.

When troubleshooting the following problems, make sure that the SafetyNet Micro is powered on. Confirm that you are using a good network connection.

Note: *Some unexplained errors might be caused by duplicate IP addresses on the network. Make sure that your unit's IP address is unique.*

Problem/Message	Reason	Solution
When you load the IP address on your browser, get an error message.	Your computer is not able to connect to port 30705 (77F1h) on the unit or your PC could not allocate a port to connect to SafetyNet Micro.	Make sure that port 30705 (77F1h) is not blocked with any router that you are using on the network. Close your browser, wait for a few minutes and try again.
Your password is not accepted any more or you have forgotten the correct password	Caps lock may be on.	The SafetyNet Micro passwords are case sensitive. Make sure you are entering the correct password. Keep a note of your current password in a secure place. Change your password periodically. 3 consecutive entries will give you instructions on resetting the password.
There is no response when you type the IP address on the browser address bar.	The SafetyNet Micro may not have rebooted properly. The device may not be powered on. The device may have its main connection fail and its internal battery life may have run out.	Ping the IP address for a response to detect if the device is active Make sure the product is active. The red led indicator shows the power status. The Ethernet link activity cable shows that the unit is up and running on the network.
You are unable to find what the IP address of the unit is, or you have forgotten the IP address of the unit.	A new DHCP lease may have been issued.	Use the SafetyNet Micro Finder Application provided by Computer Support Systems to locate your unit on the local network. If the product is not shown it may be behind a router. Make sure that you are on the same local network and that the unit is turned on.
When you type the IP address on the browser the menu is not loaded.	You may not have the Java™ Runtime Environment 1.4.2 or higher installed on your PC.	Install the Java™ Runtime Environment on your PC. This environment is a requirement of this product.
When loading the menu, you are receiving a prompt box saying "Time out in retrieving Menu information. Make sure device is active or network congestion is not present."	The congestion on your network is too high. UDP response was not received for over a period of 1.5 seconds. This is a great amount of time for packet data to come through the network.	Close browser and retry. Make sure that the device is powered on. It may have got turned off in the interim process of replying to your response. Occasionally, the menu will load up using cache memory of the browser even when the device is turned off. Make sure the device is active by pinging the unit.

Problem/Message	Reason	Solution
When the Viewer is active you are prompted with the message "Could not communicate with SafetyNet Micro. Timeout occurred. Possibly a Network delay or an inactive SafetyNet Micro device."	The congestion on the network is too high. UDP response was not received for over a period of 1 second over 5 seconds. This is a great amount of time for packet data to come through the network. Or the product is not active anymore.	Click OK. If you keep getting this message every 5 seconds thereon, the product is no longer active. Check power to the unit. Close browser and re-try again.
No SNMP traps are sent out	SNMP license may not have been entered. Network Manager IP addresses may have not been set. SNMP community access level may not acceptable on your SNMP community.	Make sure the main menu displays that SNMP traps are registered. Contact your network administrator to check the SNMP communities on your network. Contact your network administrator to check your SNMP settings on the network
SNMP polling shows values more that 100 for temperature or humidity sensors.	Temperature values and humidity values are represented by Integers.	Use a multiplier of 0.1 to get the correct analogue sensor value. E.g.: 257 is 257*0.1 = 25.7 degrees
SNMP traps are sent, detected but SNMP bindings are not shown.	CSS.MIB may not have been configured on your SNMP sniffer/detector	Configure the MIB file on your Network Management System. Read on help files of your software & follow steps on how to insert MIB files.
No SMS Messages are sent (On models ZSN4001 & ZSN4001D)	SMS configuration page settings may not be correct. Correct target IP address or/and ports are not used as advice by the CSS technical staff. Sensors may not be associated with sending SMS messages SafetyNet Micro is not able to make a direct TCP/IP connection to the target IP address on the destination port. Refer to your network administrator on setting these parameters	Check the SMS Configuration page settings. Check if the correct target IP address and ports are used as advice by the CSS technical staff. Check if sensors enabled to send SMS messages. Make sure that your unit is able to make a direct TCP/IP connection to the target IP address on the destination port. Refer to your network administrator on setting these parameters The target IP is 210.23.143.19 on port 42755.
No SMS Messages are sent (On models ZSN4001M & ZSN4001MD)	Modem configuration page settings may not be correct. Ensure the Provider number and access passwords are correct The modem may not have the dial tone	Check the Modem Configuration page settings. Initiate a test alarm on the Modem configuration and check if you receive the message. Make are the telephone line connected has the dial tone and the line type to be configured clearly as to a direct line or an analogue PABX line.
The temperature or humidity sensor did not send SMS	Sending SMS messages for warnings and shutdowns are	Make sure that you have ticked to send warnings and shutdown

messages for warnings or shutdown limit alarms.	optional and has to be specified under SMS/Modem configuration.	SMS's under additional settings under SMS/Modem configuration.
Incoming PPP connections are not successful	Incoming PPP username/password may have not been set correctly. PPP enable has not been ticked	Sensor and PPP configuration interface will allow changes to the PPP settings. Make sure PPP is enabled on the unit and ensure that the username and password is correctly set.
Outgoing PPP failure	Ensure that SafetyNet Micro attempts to establish connection with correct credentials.	Ensure the RAS server is configured correctly. Do not force RAS server to connect devices that uses encryption only. SafetyNet Micro PPP communication is not encrypted.

13.1 Technical Support

If unable to troubleshoot SafetyNet Micro using the above table, or if the FAQ section does not provide a solution, or if you cannot fix the error, you may contact CSS technical support at

Email: support@csspl.com.au

Telephone: +613-9419 3955
Fax: +613-9419 3509

Please have the following details when you contact CSS technical staff

- Model of product with software version.
- Serial number (Label on back panel or from the main menu display)
- Date of purchase
- Clear definition of problem
- Steps taken so far to fix problem

14 Appendix A – PPP Users

Table of contents for PPP on SafetyNet Micro

14.1 Introduction

This appendix applies only to SafetyNet Micro models ZSN4001MP and ZSN4001MDP. These models have PPP facilities on to facilitate an alternative path to establishing a network connection.

Incoming PPP connections allow viewing & configuring the SafetyNet Micro web interface by dialing in using the connected modem. This will allow installing SafetyNet Micro at locations where there is no active network that can be compromised via the PSTN.

Outgoing PPP is capable of initiating a PPP connection and delivering SNMP traps even when there is no Ethernet connectivity. This guarantees notifications even if the main network elements of yours are down.

All PPP settings are performed at the sub menu "*Sensor & PPP Configuration*" available under the main Menu. Select the sub menu "*PPP Settings*" within this interface to make any appropriate change.

14.2 Incoming PPP Connections

When an Incoming connection is made to SafetyNet Micro, SafetyNet Micro delivers an IP address to the PC network connection. The relevant IP addresses of SafetyNet Micro and of the PC can be configured on SafetyNet Micro before dialing in.

The network connection needs to be established with the V.90 or better type modem for an effective link.

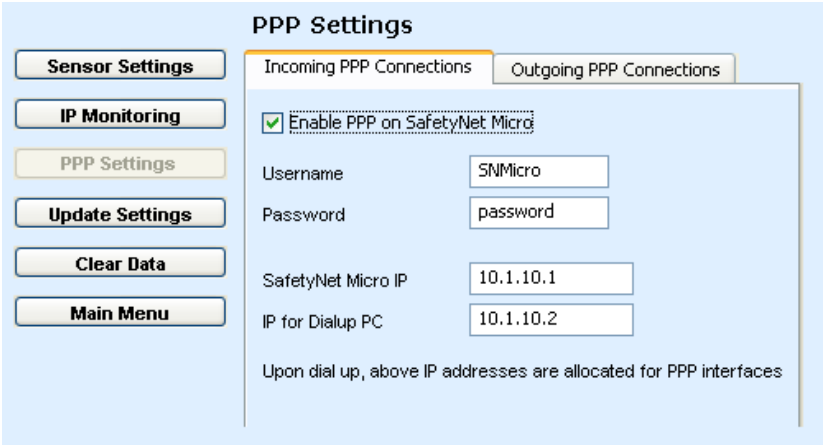
By default when SafetyNet Micro accepts an incoming connection it becomes the server and the PC that dials in becomes the client. Default server IP address is 10.1.10.1 and the client IP address is 10.1.10.2. These can be adjusted at the PPP configuration interface.

Once the connection is successful use your browser and point to the server IP address.

14.2.1 How to configure SafetyNet Micro for Incoming Connections

Click on "*Sensor & PPP Configuration*" under the main menu. Enter password and click on "*PPP Settings*". Make sure the "*Incoming PPP Connections*" tab is selected.

Ensure that PPP is enabled via selection on the screen as shown below.



Username: SafetyNet Micro accepts connections made with this username only. The dialing PC will use this username when dialing in. The factory default username is *SNMicro.*

Password: SafetyNet Micro accepts connections made with this password only. The dialing PC will use this password when dialing in. The factory default password is *password.*

SafetyNet Micro IP: Upon an incoming connection the PPP interface of SafetyNet Micro will be set to this IP address. This is the IP address the browser should point to.

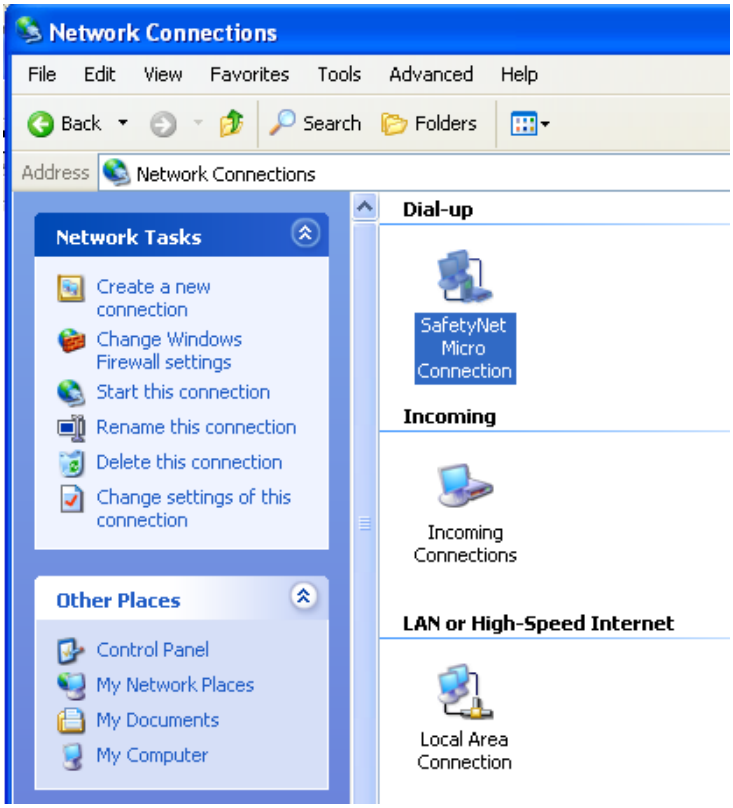
IP for Dialup PC: IP address allocated to the dial in PC upon establishing an incoming connection.

14.2.2 How to configure PC to dial SafetyNet Micro

A network connection has to be made on PC to be able to dial in to SafetyNet Micro. Your PC should be equipped with a v.90 or better modem to establish a successful connection. Please refer to your operating system documentation on help in setting up a network connection.

The following screen steps are for a machine running Windows XP™.

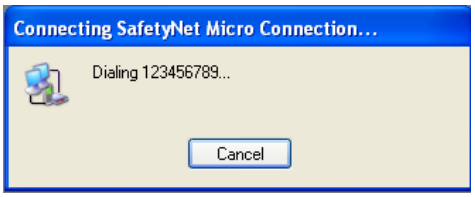
1. Click on *Start* and open *Control Panel*
2. Double Click on *Network Connections*
3. Select *Create New Network Connection* from the *Network Tasks* displayed on the top left corner.
4. The wizard will guide you to make a new network connection.
5. Select "*Connect to the Internet*". Click next. Select "*Set up my Connection Manually*" and click next. Select "*Connect Using a Dial up modem*" then click next. Give a name: Eg: "*SafetyNet Micro Connection*" and click next. *Enter Phone Numbe*r of the telephone line connected to SafetyNet Micro and click next.
6. As the username and password enter what is entered on SafetyNet Micro when configuring the Incoming PPP connection. Click finish and complete the network connection.



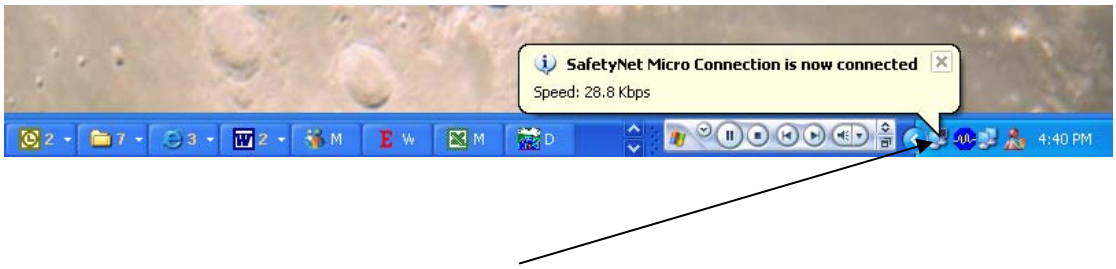
14.2.3 Viewing SafetyNet Micro Web pages Remotely

Double click on the network connection you made on your PC and establish connection.

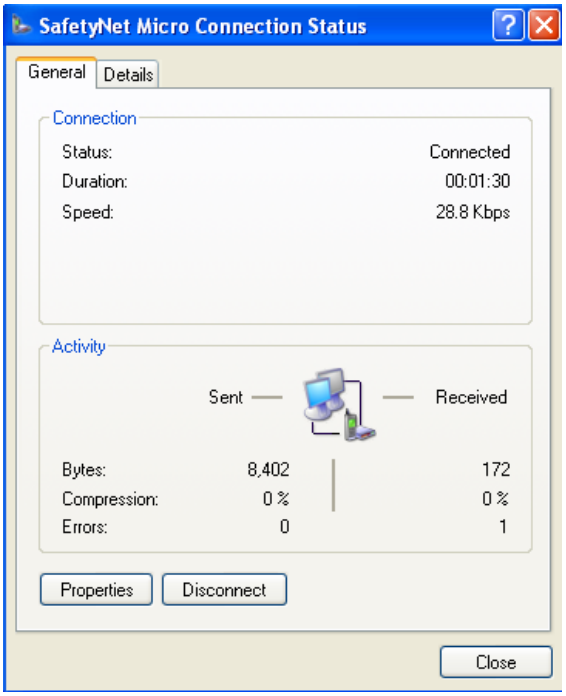
When dialing SafetyNet Micro you will see the following on your screen.

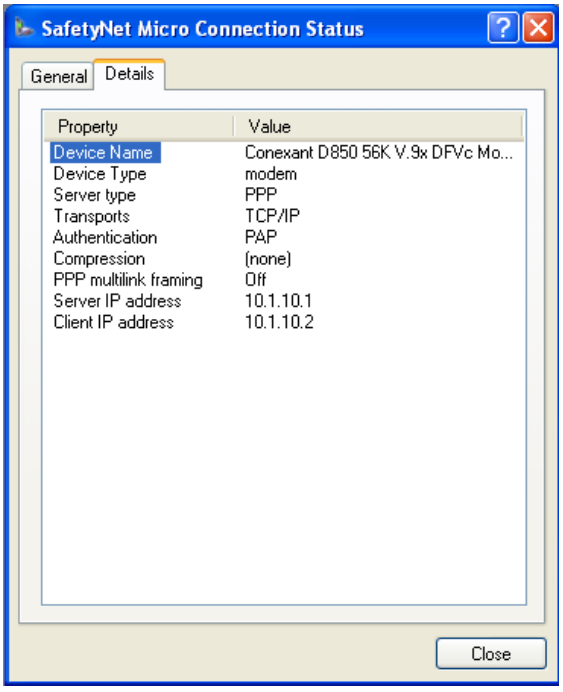


Once a successful connection is made your PC will indicate the success as show in the screen shot below.



Double clicking on the connection (2 PC icon) will bring you the window with details of the connection as shown below





The above image shows the Server IP address and the Client IP address.

Open the default browser and point to the IP address of the Server. This will bring up the SafetyNet Micro Main Menu.

You can disconnect the connection by clicking Disconnect as shown on the above image for terminating the connection.

14.3 Outgoing PPP Connections

SafetyNet Micro makes outgoing PPP connections when it meets certain criteria.

1. When there is no Ethernet present and when a SNMP trap has to be delivered upon an alarm being triggered.

2. SafetyNet Micro can be configured to ping a certain IP address just before it delivers a SNMP trap. This is to ensure that the network is present and in order. In such cases where the network has failed this Ping command will fail and would indicate to SafetyNet Micro that there is a potential network failure. This will trigger an Outgoing PPP connection that will attempt to deliver the SNMP trap via an alternative path.

An outgoing connection can be made when one or both of the above criterions are made.

Upon a successful outgoing PPP connection, SafetyNet Micro will deliver the SNMP traps via the PPP network connection.

To enable Outgoing PPP connections, PPP has to be enabled on the device under the "*Incoming PPP Connections*" tab.

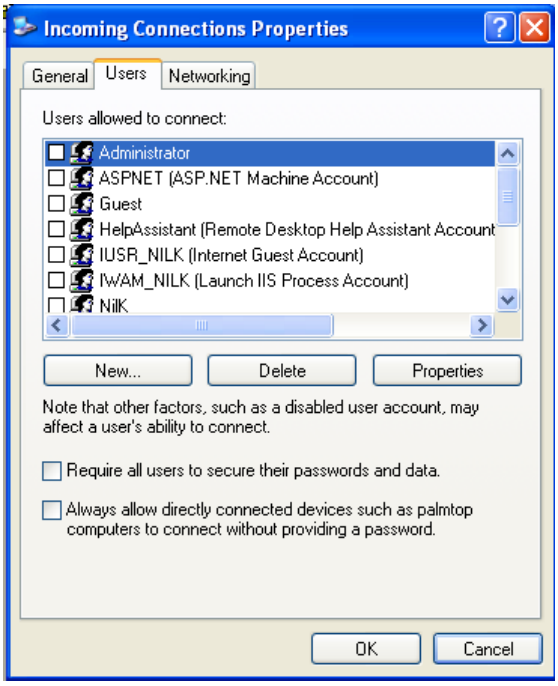
14.3.1 How to configure PC to accept incoming connections

PPP Server Software has to be installed on your PC to accept incoming connections. Windows NT based machines can be configured to have incoming network connections. Please refer to your operating system help files in configuring an incoming network connection.

RAS (Remote Access Server) is included in the Windows XP™ professional operating system.

The following example is setting up an incoming connection for a machine installed with Windows XP™ professional edition. If your operating system is different please use the help files to determine how to set up a RAS server.

1. Click on *Start* and open *Control Panel*
2. Double Click on *Network Connections*
3. Select *Create New Network Connection* from the *Network Tasks* displayed on the top left corner.
4. The wizard will guide you to make a new incoming network connection.
5. Select "*Setup an advanced connection*". Click next. Select "*Accept Incoming Connections*" Click next.
6. Select the modem installed on your PC that you want the incoming connection to come through.
7. Select "*Do not allow virtual private networks*". Click next.
8. Select users that can connect using this incoming connection. SafetyNet Micro has to be configured to use one of these usernames and passwords to establish the connection. (More on 14.3.2 How to configure SafetyNet Micro to auto establish PPP Connections will discuss this matter)
9. Use the default protocols displayed in the next wizard window. Click next.
10. Click finish.
11. Now select the "Incoming Connection" on control panel and right click on it. Then select properties.
12. Now select the users tab.
13. Make sure that "Require all users to secure their passwords and data" has been unchecked. Now click ok.



14. Your PC is now configured to accept incoming connections.

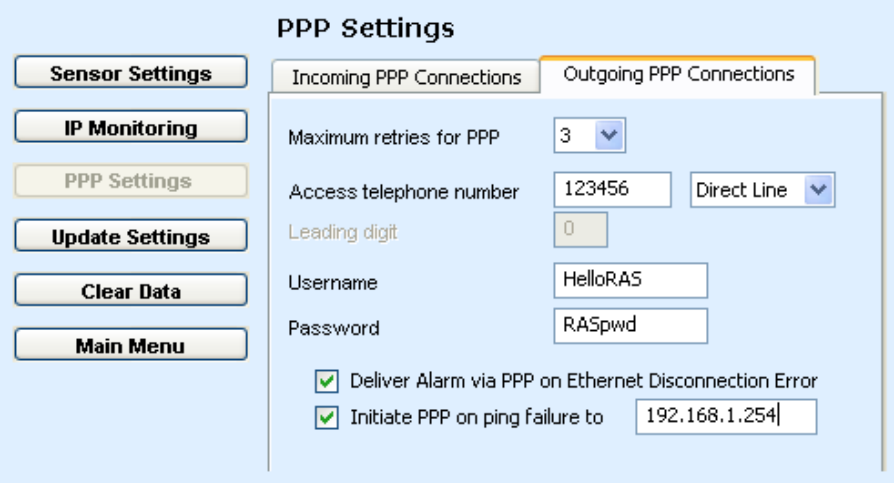
To receive SNMP traps this PC has to have a Network Manager System (NMS) installed, or should be able to route packets to the appropriate IP address from the incoming connections.

E.g.:
SafetyNet Micro → Connects to PC 1 and delivers SNMP trap addressed to PC2 on the network. PC1 has to be able to route the packet content to PC2 for successful delivery. If PC1 has no routing capability the SNMP trap capturing software has to be installed on PC1.

SafetyNet Micro needs to know the RAS Server, PPP incoming connection IP address to deliver the SNMP trap packet. You could statically set this in your PC or have a DHCP based address. Look up on the DHCP list to find out your RAS server interface IP address and set SafetyNet Micro NMS IP address to be able to send traps out on SNMP settings.

14.3.2 How to configure SafetyNet Micro to auto establish PPP Connections

Click on "*Sensor & PPP Configuration*" under the main menu. Enter password and click on "*PPP Settings*". Make sure the "*Outgoing PPP Connections*" tab is selected.



Maximum retries for PPP: SafetyNet Micro will attempt this many times to make a successful outgoing PPP connection.

Access Telephone Number: SafetyNet Micro uses this telephone number to dial up. Select the line type connected to SafetyNet Micro. If connected via a PABX, select the leading digit to get an outside line.

Username: SafetyNet Micro uses this username to get connected to the RAS server.

Password: SafetyNet Micro uses this password to get connected to the RAS server.

Deliver Alarm via PPP on Ethernet Disconnection Error: When the Ethernet connection on SafetyNet Micro is removed an alarm is logged after 25-second duration. This alarm can be used to initiate an outgoing PPP connection if this selection is made. If this selection has not been made, an Ethernet disconnection error will not initiate a PPP session.

Initiate PPP on ping failure: Each time an alarm occurs and when a SNMP trap needs to be delivered SafetyNet can ping the given IP address to ensure that there is network connectivity. On a ping failure to the given IP address SafetyNet will assume the network has failed for some reason and will auto initiate a PPP session to deliver the SNMP traps.

Please note: If there is no physical Ethernet connection present on SafetyNet Micro, on alarm or clearance of an alarm, the device will establish a PPP session to notify the alarm status. This will only occur if SNMP has been enabled via the registration key on the unit as PPP delivers an SNMP trap.

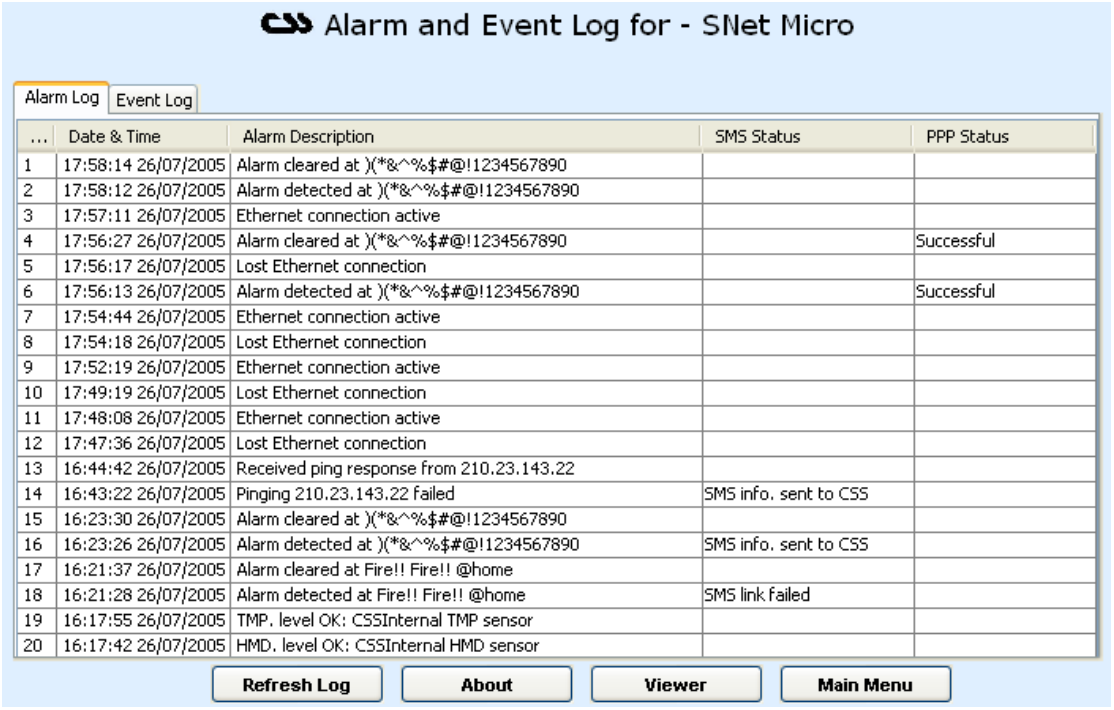
14.4 Alarm and Event Log related to PPP

The alarm and event log has an extra column to indicate the PPP status of the SNMP trap status.

The possible PPP status string descriptions could be

PPP Status	Description
Queued	Alarm is queued to be sent via PPP. This could be because the Ethernet physical connection is not present or it could because a ping failed just before delivering the SNMP trap as configured for outgoing PPP connections.

Successful	A successful connection was made and the SNMP traps were delivered to the respective Network Manager IP addresses. Please note that SNMP works on UDP and hence packet delivery is not guaranteed. Also if the RAS server is unable to route packets correctly SNMP traps may not be delivered. “Successful” status is displayed upon anticipation only.
Max. retries reached	Attempted to establish an outgoing PPP connection, but failed as maximum retry number was reached in connections.
Abandoned - Reboot	This status will only be displayed if the alarm was queued, but SafetyNet Micro was rebooted before it established a successful PPP connection. Upon reboot the alarm will not be sent. If the alarm is still active a new alarm will be triggered and will be notified accordingly.
PPP Disabled	No PPP sessions will be attempted. Ethernet connection was physically not present, yet PPP was disabled on settings.



...	Date & Time	Alarm Description	SMS Status	PPP Status
1	17:58:14 26/07/2005	Alarm cleared at)(*&^%$#@!1234567890		
2	17:58:12 26/07/2005	Alarm detected at)(*&^%$#@!1234567890		
3	17:57:11 26/07/2005	Ethernet connection active		
4	17:56:27 26/07/2005	Alarm cleared at)(*&^%$#@!1234567890		Successful
5	17:56:17 26/07/2005	Lost Ethernet connection		
6	17:56:13 26/07/2005	Alarm detected at)(*&^%$#@!1234567890		Successful
7	17:54:44 26/07/2005	Ethernet connection active		
8	17:54:18 26/07/2005	Lost Ethernet connection		
9	17:52:19 26/07/2005	Ethernet connection active		
10	17:49:19 26/07/2005	Lost Ethernet connection		
11	17:48:08 26/07/2005	Ethernet connection active		
12	17:47:36 26/07/2005	Lost Ethernet connection		
13	16:44:42 26/07/2005	Received ping response from 210.23.143.22		
14	16:43:22 26/07/2005	Pinging 210.23.143.22 failed	SMS info. sent to CSS	
15	16:23:30 26/07/2005	Alarm cleared at)(*&^%$#@!1234567890		
16	16:23:26 26/07/2005	Alarm detected at)(*&^%$#@!1234567890	SMS info. sent to CSS	
17	16:21:37 26/07/2005	Alarm cleared at Fire!! Fire!! @home		
18	16:21:28 26/07/2005	Alarm detected at Fire!! Fire!! @home	SMS link failed	
19	16:17:55 26/07/2005	TMP. level OK: CSSInternal TMP sensor		
20	16:17:42 26/07/2005	HMD. level OK: CSSInternal HMD sensor		

14.5 Further Help on PPP connections

Please contact Computer Support Systems to enquire details of PPP on SafetyNet Micro if you still have any questions. Refer to the frequently asked questions and the trouble shooting section of this manual before contacting Computer Support Systems to find out a solution.

15 Glossary

SNMP – Simple Network Management Protocol

Simple Network Management Protocol is used for internetwork management. More information can be obtained from http://www.snmplink.org/ (link active as at 22/06/2004)

MIB – Management Information Base
This is an important component of SNMP. Contains information for Network Managers interpretation.

WINS - Windows Internet Name Service
Windows Internet Name Service (WINS) provides a distributed database for registering and querying dynamic NetBIOS names to IP address mapping in a routed network environment for name resolution.

SafetyNet Micro Registration License Keys
Unique keys that enables certain features on SafetyNet Micro. Provided at the time of purchasing a SafetyNet Micro unit. Additional keys can be obtained from Computer Support Systems by emailing at sales@csspl.com.au

SafetyNet Micro Password Unlock Key
A specific key that allows entering a new password at the time of forgetting the SafetyNet Micro password. This key is only valid for a day. In order to obtain this key it is required to request this key officially from Computer Support Systems on a company letterhead, authorised by an authorised personnel.

DHCP - Dynamic Host Configuration Protocol
The *Dynamic Host Configuration Protocol* (DHCP) is an Internet protocol for automating the configuration of computers that use TCP/IP. DHCP can be used to automatically assign IP addresses, to deliver TCP/IP stack configuration parameters such as the subnet mask and default router, and to provide other configuration information such as the addresses for printer, time and news servers.

UDP - User Datagram Protocol
The User Datagram Protocol belonging to the TCP/IP family offers only a minimal transport service -- non-guaranteed datagram delivery -- and gives applications direct access to the datagram service of the IP layer. UDP is used by applications that do not require the level of service of TCP or that wish to use communications services (e.g., multicast or broadcast delivery) not available from TCP.

PPP – Point- to- Point Protocol
T The *Point-to-Point Protocol (PPP)* originally emerged as an encapsulation protocol for transporting IP traffic over point-to-point links.

16 Frequently Asked Questions (FAQ's)

FAQ 1. My product is connected to the network and turned on. Now what do I do?

Answer: Use the application "SafetyNetFinder.exe" provided by Computer Support Systems in the CD-ROM of SafetyNet Micro to detect the IP address of the unit. Alternatively, get your network administrator to look up the DHCP leases on your server and try to locate the device by using the MAC address of the unit. The MAC address can be found on the back of the unit on a label attached to it.

FAQ 2. My Java™ applets do not load up or my interface does not show up any buttons to click. What am I doing wrong?

Answer: Your system may not have the Java™ Runtime Environment (JRE) version 1.4.2 or higher installed. Check the requirements on the Getting Started Manual and install the JRE. Use control panel to check what version you have currently installed.

FAQ 3.What type of sensors and how many of them can I connect?

Answer: SafetyNet Micro supports one dual digital sensor. This digital sensor can be configured as fluid, smoke or as contact input sensor types. SafetyNet Micro has an inbuilt temperature and humidity sensor.

FAQ 4. What trigger delays are associated with sensors?

Answer: The temperature/humidity type sensor, smoke and fluid sensors have a 15 second trigger delay, where as the digital sensors provide a trigger delay that could be customised up to 120 seconds.

FAQ 5. How long can I run my sensor cables from SafetyNet Micro?

Answer: We recommend up to 60m of distance from the sensor to SafetyNet Micro using CAT 5 type cables. The applicable sensors are the dual digital sensor, fluid or a smoke sensor.

FAQ 6. Occasionally when the Viewer is active I am prompted with the message "Could not communicate with SafetyNet Micro. Timeout occurred. Possibly a Network delay or an inactive SafetyNet Micro device." Why is this happening?

Answer: The viewer did not receive an answer from SafetyNet Micro for more than 7.5 seconds. Click OK and try again. If you keep getting this message your network has a high volume of congestion or SafetyNet Micro is no longer active. Ensure that UDP port 30705 is open for communication and that the network setting on SafetyNet Micro has been entered correctly. Ping the unit to check its activity.

FAQ 7. How can I clear my graph data?
Answer: You can clear all related graph data by going in Sensor Configuration and then clicking "Clear Graph Data" button. Note: This will clear all analogue sensor related data.

FAQ 8. I have received a SNMP trap but I did not receive a SMS for a further 2 hours. I have enabled SMS registration and configured this particular sensor to send a SMS. What happened to the SMS? (On models ZSN4001 and ZSN4001D only)

Answer: Computer Support Systems cannot guarantee the time, delivery or reliability of SMS delivery as SMS relies on the Public Switched Telephone Network (PSTN) and the receiving mobile being switched and attended.

FAQ 9. My network is not DHCP enabled. Because the device is set by factory default to have DHCP when shipped, what IP address does it load up with?

Answer: If your network is not-DHCP enabled, after a timeout of 15 seconds the device will fall to IP address 192.168.1.100 (DHCP fall back IP address) with a subnet mask of 255.255.255.0.

The best way to allocate a preferred static IP address is to connect the device direct to a PC using a crossover cable. Set the PC IP address to 192.168.1.xxx (excluding 192.168.1.100) with a subnet mask of 255.255.255.0 and try to ping SafetyNet Micro on the fallback DHCP IP address. Once you are able to communicate with the device, then you may set the preferred static IP address and connect SafetyNet Micro on the network.

FAQ 10. I have set a static IP address on my product, but now I want to set it back so that DHCP is enabled. How can I set SafetyNet Micro with DHCP enabled?

Answer: Set the IP address in the Administration Configuration page to be 0.0.0.0 where DHCP will be activated. To find the DHCP enabled IP address, look up on your server DHCP leases or use the tool SafetyNet MicroFinder.exe application provided by CSS included the SafetyNet Micro CD under the tools directory.

FAQ 11. How can I load factory defaults on SafetyNet Micro?

Answer: Go to administration configuration settings and click on "*Factory Defaults*" menu. Then click on "*Load Factory Defaults*" button to clear current settings and load defaults on SafetyNet Micro.

If you are no longer able to access the device on the network the unit may have to be loaded with defaults physically. To do this, you will have to consult Computer Support Systems.

FAQ 12. How can I clear the alarm & events log or the graph data on SafetyNet Micro?

Answer: Go to Sensor Configuration from the main menu and then select "*Clear Data*". You can then clear the graph data or the alarm log as desired.

FAQ 13. I have forgotten my password on my SafetyNet Micro system. How can I access the product now?

Answer: SafetyNet Micro provides a secure method to re-enter a new password if you have forgotten the existing password. If attempted to login to SafetyNet Micro more than three times with an incorrect password it will redirect to a webpage where specific instructions are given on how to obtain a password unlock key to access the product.

FAQ 14. Can I get SNMP packets delivered when there is no Ethernet?

Answer: SafetyNet Micro has PPP as an option. This will allow notifying of any alarms via PPP by establishing connection to a Remote Access Server. All you have to do is set up the RAS server, the SNMP Manager and set rules on SafetyNet Micro to when and how to dial to make a PPP connection.

FAQ 15. If my network is down can I still view SafetyNet Micro web pages?

Answer: Yes you can. The optional PPP feature allows dialing into the SafetyNet Micro unit and view its web pages. You can perform any action as you are connected via the Ethernet interface via the PPP network link.