SafetyNet Series 5 D40
User Manual

Document Revision CSSS5D40 04/10
SafetyNet Series 5 D40 Version 1.00

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
09/03/2010	CSSS5D40 03/10	NK Initial Release
20/04/2010	CSSS5D40 04/10	Updated digital connection type notes. RJ45 to 2 wire connection type. Add connection diagram

Declaration of Conformity

Manufacturer's Name & Address:

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

Product Name Model: SafetyNet Series 5 D40 Environmental Monitoring System. Models include ZSN5005, ZSN5005P & ZSN5005G

Warranty

Computer Support Systems warrants SafetyNet Series 5 D40

- 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 Series 5 D40 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.

SafetyNet Series 5 D40 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 Computer Support Systems 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 Series 5 D40

SafetyNet Series 5 D40 is modern network based Environmental Monitoring System (EMS).

It is capable of monitoring surrounding environment conditions using connected digital sensors. In alarm conditions, SafetyNet Series 5 D40 alerts notification via SNMP (Simple Network Management Protocol), email messaging (SMTP Protocol), via SMS messaging/ Pager notification and by its web interface. Blinking LED's, a buzzer and a strobe is also activated on alarm and will attract attention on error conditions.

The device is capable of activating relays on alarm activation to activate desired external peripheral. This product is ideal to monitor facility services and notify of potential environmental problems, which may impact on network operations. Additionally, the unit can monitor an IP address and enter into an alarm condition when the IP address does not respond to a ping command.

SafetyNet Series 5 D40 comprises an embedded web server and a powerful processor. An attractive, user friendly interface is used for viewing or configuring the device. This interface is accessible via a standard Java enabled web browser installed in almost all computers today.

Features

- Powerful embedded microprocessor driven, with networking feature
  - TCP/IP, UDP, DHCP, HTTP, SNMP, SMTP, ICMP protocols are supported
- Up to 2.5 hours of internal battery backed operation in power failures
- 19" inch rack mountable, compact size, light weight and sleek design
- SNMP (V1) features to notify error conditions via traps and allows polling data of sensors/relays
- Email messages up to three given email addresses notifying alarm conditions.
- SMS messaging or pager messaging via a network interface independent internal PSTN or GSM modem.*
- Remote configuration and monitoring capabilities via a web interface.
- User friendly and attractive user interface
- 40 user-configurable *digital* sensor inputs - Digital, Smoke, Fluid, Security etc
- Two individual relays, capable of being controlled manually via a web interface or by sensors upon alarms. Connection type is 2-wire directly run from the input.
- IP monitoring
- Optional strobe and a buzzer to indicate error conditions. Blinking LED on unit indicates alarm conditions
- Up to 40 entries on alarm and event logs
- Integrated Camera view on device with compatible IP cameras.
- Firmware upgrades over the network

* Only one type of modem can be ordered on one unit

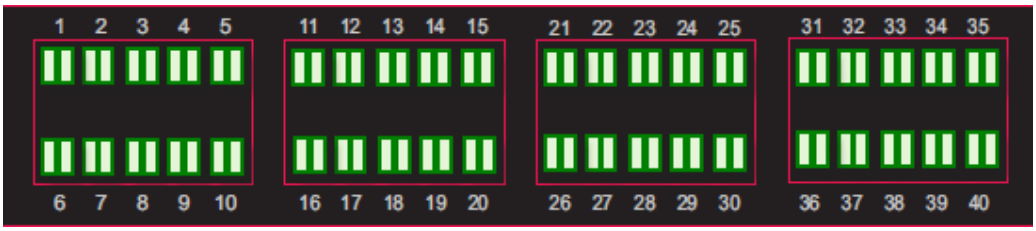
Applications

- Computer server room monitoring
- Computer rack monitoring and management
- Alarm consolidation from other network disabled systems
- Monitoring of other controlled environments
- Monitoring of servers or PCs

- Water monitoring systems
- Remote door controlling applications
- Remote PoP, data centers, co-locations, telecom switching facilities and utility site monitoring
- IP camera view via a single web interface on the monitoring system by using a compatible camera

Figure 1: SafetyNet Series 5 D40 Environmental Monitoring System

Note: rear of unit is displayed only for illustration purposes. Digital connections are 2 wire connection type as shown below:



1.1 Available SafetyNet Series 5 D40 Models

Model Number	Description
ZSN5005P	SafetyNet Series 5, 40 digital inputs, 2 Relay outputs, 240V input, battery backup, Network Viewer, Camera Viewer, SNMP, SMTP, Inbuilt PSTN modem
ZSN5005G	SafetyNet Series 5, 40 digital inputs, 2 Relay outputs, 240V input, battery backup, Network Viewer, Camera Viewer, SNMP, SMTP, Inbuilt GSM modem
ZSN5005	SafetyNet Series 5, 40 digital inputs, 2 Relay outputs, 240V input, battery backup, Network Viewer, Camera Viewer, SNMP, SMTP

1.2 SafetyNet Series 5 D40 Concept Diagram

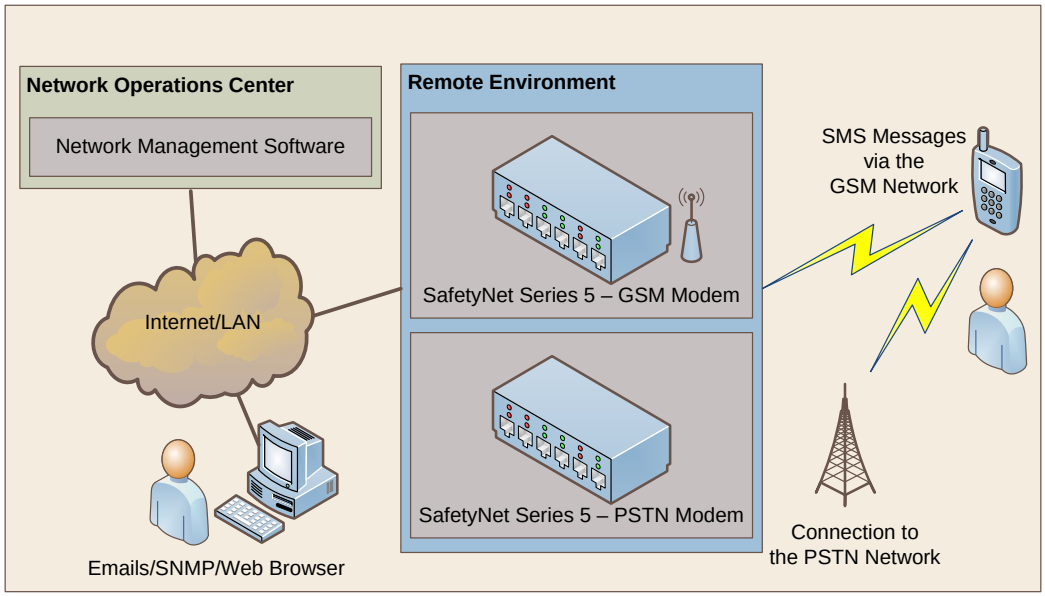


Figure 2: Network Concept

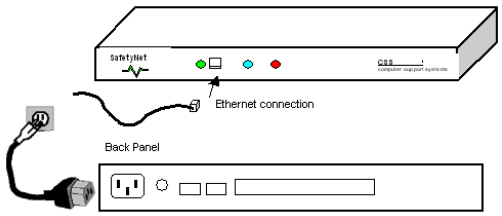
2 Quick Install Guide

2.1 Requirements for a successful Installation

- Access to the local area network & UDP port 30705 available for communication.
- Java enabled web browser. (Java™ 2 Runtime Environment, Standard Edition, Version 1.6.0. or higher)

2.2 Hardware Installation

1. SafetyNet Series 5 D40 should be **turned off**.
2. Connect the Ethernet cable to the interface located on the front panel.
3. Connect necessary inputs on to the back of SafetyNet.
4. Connect power cable and turn unit on.



2.3 Assigning an IP address

DHCP on the network interface is enabled by factory default. Upon non-detection of a DHCP server on the network the unit falls back to IP address 192.168.1.100 with a gateway of 255.255.255.0.

An IP address can be applied to the unit by:

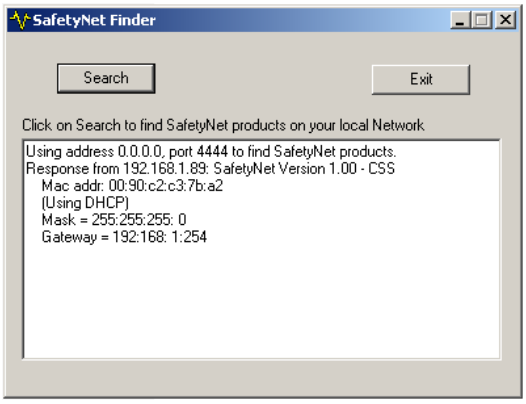
1. DHCP server automatic IP allocation. (factory default)
2. Web browser via the 'Settings' menu, ''Network Interface' panel

IP address allocation using DHCP

If your network is DHCP enabled, SafetyNet Series 5 D40 will be allocated with an automatic IP address, gateway address and a subnet mask when powered on.

Consult the network administrator for further details in finding the DHCP allocated IP address using the DHCP server. You may also use the tool "SafetyNetFinder.exe" [1]application provided by Computer Support Systems to find out the current IP address of the unit.

Once the IP address allocated by the DHCP server is found, use the web browser and point to the IP address to load the web interface.



Note: *The unit falls back to the IP address 192.168.1.100 with a subnet mask of 255.255.255.0 after 30 seconds if the network is DHCP disabled. If this is the case use a cross over cable on to a PC with an IP address of 192.168.1.xxx (except 100) and set the unit to a static IP address. Once done, turn off unit, connect the unit to the local network and then turn power on.*

[1] SafetyNetFinder.exe is a tool provided by CSS to locate SafetyNet products on the local network

IP address allocation using a Web Browser

Open a web browser and direct to the IP address of the unit. Use the tool "SafetyNetFinder.exe" to find out the IP address of the unit.

Chapter 6.1.2 Network Interface shall provide more information on setting up the network parameters. The factory default password to login to the device is 'password'.

IP address allocation when DHCP is disabled

If the network is DHCP disabled, SafetyNet Series 5 D40 will allocate itself a fallback IP address. You are advised to use a cross over cable to set a static IP address in this case.

Method:

A. Use a standalone PC with the IP address set to be of 192.168.1.xxx (xxx should not be 100), set the gateway to be 255.255.255.0

B. Connect SafetyNet Series 5 D40 using a crossover cable and wait for more than 30 seconds once turned on.

C. SafetyNet Series 5 D40 will be allocated 192.168.1.100 as its fallback IP address. Open a browser and point to the menu, where a desired static IP address can be set.

D. Disconnect SafetyNet Series 5 D40 and connect it back on the network and ping device in order to confirm the presence.

Important Tips

- Use the command "ping" to check if the allocated static IP address is a duplicate before you begin.
- Use the command "ping" to check if you are able to reach the unit once you have configured the unit.

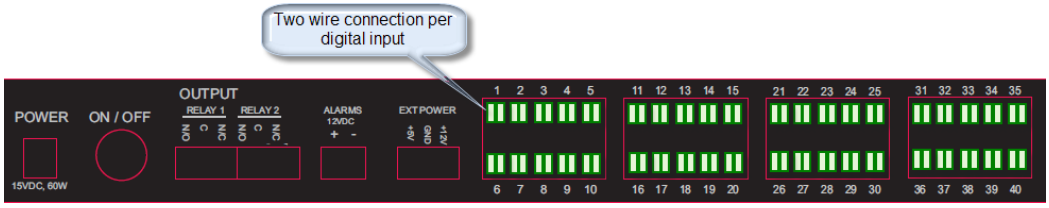
Read the trouble shooting section in the user manual for any additional tips.

Note: *Once the device is configured, please note the network parameters from the network administrator and note below.*

Serial No: ____ ____ ____ ____ ____ ___ (Rear label on SafetyNet)

IP Address: _____ _____ _____ _____
Subnet Mask: _____ _____ _____ _____
Gateway: _____ _____ _____ _____

2.4 Digital Input Connection



The rear of the device contains the 40 digital input connections. The connection type is a 2-wire connection type and can be run directly from the input/sensor.

3 Assumptions

We assume that you have: -

- Configured SafetyNet Series 5 D40 network parameters according to the ***Quick Install Guide - Chapter 2,*** and that the IP address of the device is known. This manual explains how to operate SafetyNet Series 5 D40 once successfully installed on the network.
- An installed SafetyNet Series 5 D40 with all necessary sensors supplied by Computer Support Systems.
- All requirements specified below are met.
  - Access to the local area network
  - Java enabled web browser. (IE 6.0 or higher recommended)
  - UDP port 30705 available (firewall enabled) for communication on the network.
  - Java™ 2 Runtime Environment, Standard Edition, Version 1.6.0 or higher installed on viewing PC.(You may install this from http://java.sun.com)
  - SMS delivery
    - PSTN modem based SafetyNet Series 5 D40 requires Access Account from Telstra – (SMS Access Manager)
    - GSM modem based SafetyNet Series 5 D40 requires a post paid, PIN disabled GSM SIM card.

4 Introduction to SafetyNet Series 5 D40 Web Interface

SafetyNet Series 5 D40 web interface is controlled by Java applets. Java™ Runtime Environment version 1.6.0 or higher is required to be installed in order to load the applets on the browser.

The product uses applets to represent its Graphical User Interface (GUI). This user interface consists of a structural menu for easy navigation and an intuitive interface for setting up & viewing the status of sensors of the device.

The 'configuration elements' of SafetyNet Series 5 D40 web interface is password protected.

A brief description of each web interface menu item is described below. Additional details of each menu item and how to use them can be found under chapter 6, *Configuring SafetyNet Series 5 D40*.

The web interface is loaded simply using a Java enabled browser, and by pointing it to the IP address of SafetyNet Series 5 D40. Alternatively, configure the WINS (Windows Internet Name Service) to provide a name resolution for SafetyNet Series 5 D40 from NetBIOS names to IP addresses for Windows PCs. This will enable to use the given resource name instead of the IP address.

4.1 SafetyNet Series 5 D40 Web Interface – Main Page/Viewer

The SafetyNet Series 5 D40 web interface consists of a menu structure that is used for navigation. This menu panel is located on the left side of the diagram below.

Figure 3: SafetyNet Series 5 D40 Main Page

4.1.1 Menu Item – Viewer

This is the main interface which allows viewing of the current sensor and relay status. It also gives access to control the relays remotely if the relays are set for manual control. A few other monitored alarm status is also displayed. (e.g.: Low battery, mains failure, etc)

Digital-alarm status is clearly indicated and any fault will attract attention by blinking indicators.

Chapter 5 discusses further about the Viewer features/descriptions.

4.1.2 Menu Item – View Camera

View the IP 'camera view' if configured. This provides a link for accessing the camera view instead of requesting another webpage for the camera.

4.1.3 Menu Item – View Logs

View the alarm and event log on SafetyNet Series 5. There are up to 40 log entries for each log type.

4.1.4 Menu Item – Sensors & Action

Primary link to setup all parameters related to sensors and their associated actions. This includes sensor types; trigger delays, association of relay action to sensors, etc.

This menu item is password protected.

4.1.5 Menu Item – Relays & IP Monitoring

This menu item allows setting up Relays and IP monitoring settings.
This menu item is password protected.

4.1.6 Menu Item – Settings

Allows setting up the device settings such as network interface, password, system time, modem configuration, SNMP configuration, SMTP setup, Camera setup, hardware resets, loading factory defaults, etc on SafetyNet Series 5 D40.

This menu item is password protected.

4.1.7 Menu Item – Logout

Allows logging out if logged into the system.

4.2 Security on SafetyNet Series 5

4.2.1 Password Authentication

A password secures entry to the configuration menu items of the SafetyNet Series 5 D40.

The factory default password is set to be "*password*". We recommend changing the password to a desired password with at least six characters.
Note: *SafetyNet Series 5 D40 password is case sensitive. The password is limited to a maximum number of 12 characters.*

4.2.1.1 Changing the Password

A password change may be performed by navigating to the 'Settings' menu item and clicking on the 'Change Password' button of the 'Device Settings' Panel.

4.2.2 Forgotten Password

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

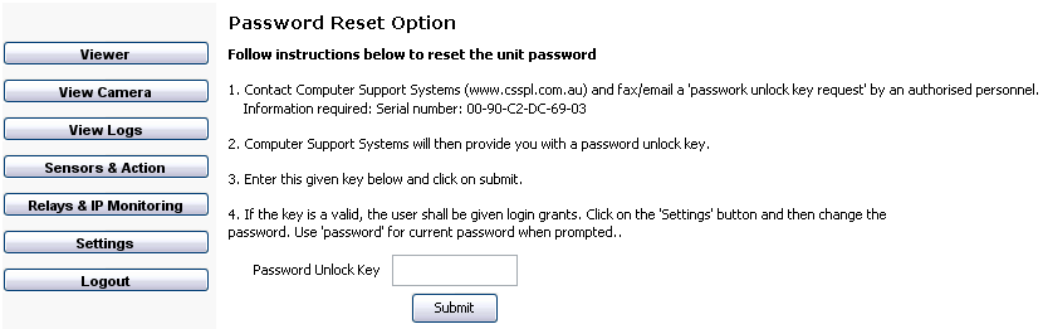


Figure 4: Forgotten Password

Upon a successful password unlock key submission the system will then allow entering logging the user in, so that a password change can be made. The default password is set to 'password' in such cases. It is expected that the user will change the password via the web interface.

4.2.3 Timed Redirection based on Inactivity

If a user logged into SafetyNet Series 5 D40 and been inactive for over five minutes, the user is automatically logged out and the screen will be navigated to the viewer menu item. This feature will protect users from forgetting to logout from the configuration menu items and will attempt preventing unauthorised access to the configuration aspects of the unit. It is recommended that the user clicks on the Logout button when the configuration tasks are complete.

5 SafetyNet Series 5 D40 Viewer

SafetyNet Series 5 D40 viewer is the key web graphical interface which allows viewing the current status of the monitored environment.

It gives an overall view of each sensor, its type and the status. Sensor name labels are displayed to identify the sensor clearly.

If sensors are in alarm conditions, blinking conditions provides an immediate impression of a situation.

The viewer also shows the current output status of each individual relay. If the relays are configured to be manually driven, the viewer allows controlling the relays via the interface. When relays are latched, and no alarms are active it is possible to reset the latched relays via the interface.

IP address monitoring errors, hardware errors such as mains failure type or low battery errors are also shows on the viewer if they occur.

The link status of the interface and the device is portrayed by a series of green moving indicators on the left side of the interface. These indicators turn red, if the link is broken and requires a refresh of the web interface via the browser.

A typical “All’s well” status snap shot is displayed below:

Figure 5: SafetyNet Series 5 D40 Viewer

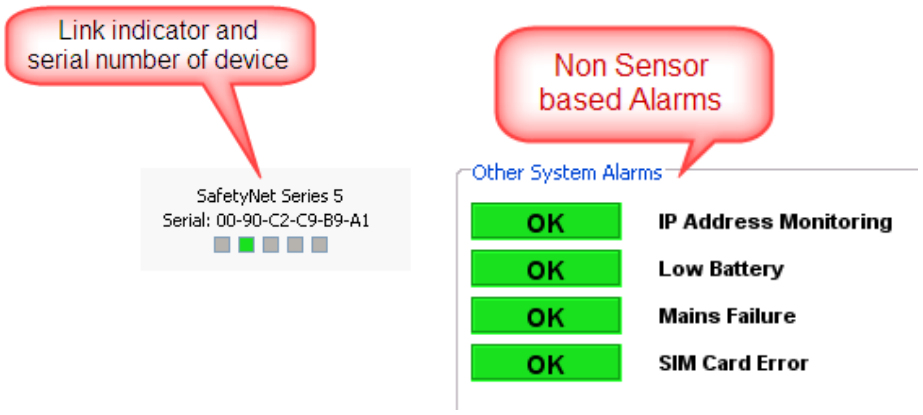


Figure 6: Features of the Viewer

Any alarm of a sensor will be indicated on the interface as below.

Figure 7: Alarm Condition

If IP monitoring alarm has triggered, no SIM present, 240V mains have failed, or the internal battery is low notification is provided on the 'Other System Alarms' panel.

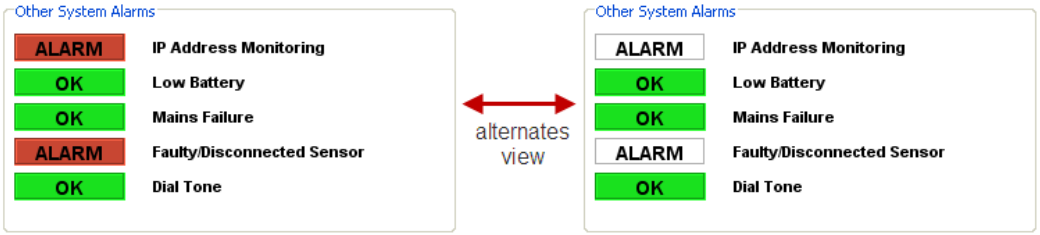


Figure 8: Other System Alarms

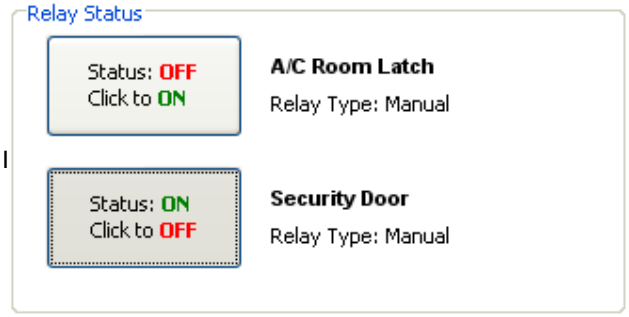
The signal strength of the GSM modem on version ZSN5005G of the device is also displayed on the Viewer.

The signal strength bars turn red when the GMS modem does not have sufficient signal strength.

5.1 Relay Status

SafetyNet Series 5 D40 relays can be setup to be driven by sensors and other system alarms on alarm conditions, manually operated via the web interface. Latching option is available when relays are driven via sensors or other system alarms.

When a relay is set to be controlled manually, buttons on the Viewer allows controlling the relays.

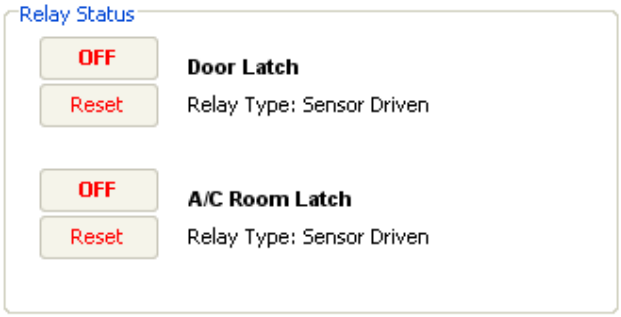


These buttons are toggle buttons. The text on the button describes the status of the relay.

If the status is ON, click the button to turn OFF and vice versa.

The above image describes that the relay at the "*Security Door*" is ON and the relay at the "*A/C Room Latch*" is OFF.

If sensors drive the relays the following is visible:



The "*Reset*" button would be disabled at all times in the case of sensors drive the relays, except: -

A. If latching were enabled and,
B. If there are no active alarms that drive relays.

6 Configuring SafetyNet Series 5 D40

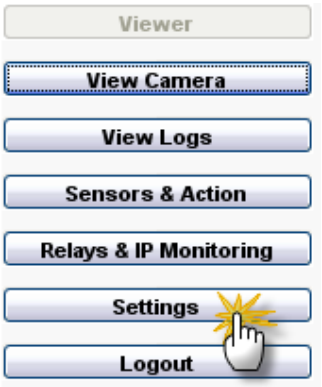
Configuring SafetyNet Series 5 D40 is performed remotely using the web interface that embeds a Java™ applet. Any configuration change does not reboot SafetyNet Series 5 D40. All configuration changes are performed at runtime.

Once all configuration aspects have been performed, it is recommended that a hardware reset is initiated by clicking the "*Hardware Reset*" button on the 'System Maintenance' panel found on the 'Settings' menu on SafetyNet Series 5 D40 or by physically turning the device off and then turning it back on using the button on the rear of the device.

As a **backup of the configuration**, we recommend keeping a listing of each of the settings stored elsewhere. **Retain a hardcopy of the settings as backup.**

6.1 Settings Menu Item

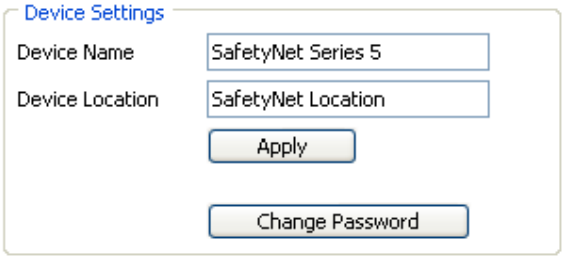
To enter this menu item click on "*Settings*" button on SafetyNet Series 5 D40 web interface. Please note that this is a password protected menu item.



Use this interface to configure:

- Device Settings
- Network parameters & boot up preference
- SMTP Configuration
- SNMP Configuration
- Modem/SMS Configuration
- System Clock Settings
- Camera Settings
- System Maintenance Options

6.1.1 Device Settings



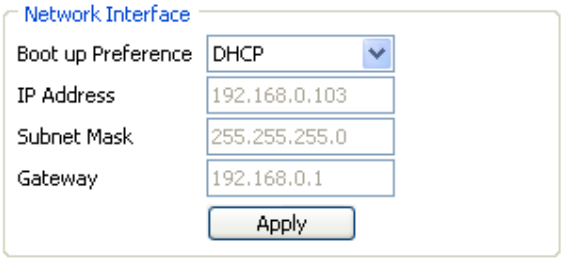
Device Name: Indentifies the device. This free form text tag is used on SMS and SNMP traps.

Device Location: This free form text tag can be used to indicate the location of the device. The tag is used in SMS and SNMP traps.

Apply Button: Checks validity of the available fields and updates 'Device Settings'

Change Password: Click to change the password on SafetyNet Series 5 D40. The existing password is required to change the new password.

6.1.2 Network Interface



Boot up Preference: Select DHPC or Static. If 'DHCP' selected, an IP address is issued by the DHCP server. If 'Static' is selected is expected the user to provide the interface IP address, Subnet Mask and the Gateway.

IP Address: IP address of the device.

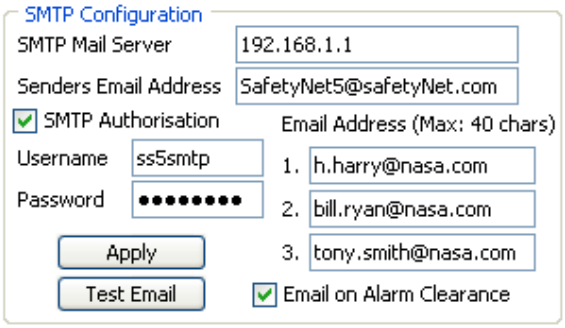
Subnet Mask: Subnet Mask of the device.

Gateway: Gateway of the device.

Apply Button: Checks validity of the available fields and updates 'Network Interface' panel settings.

PS: Please contact the network administrator for the appropriate settings for the network interface panel.

6.1.3 SMTP Configuration



SMTP Main Server: Address of the SMTP Mail server. This could be an IP address or a machine name with a domain address.

Senders Email Address: The emails are tagged by this email address as the senders address.

SMTP Authorisation: Select to enter the username and the password for the SMTP authentication for delivering emails. Contact the network administrator for details.

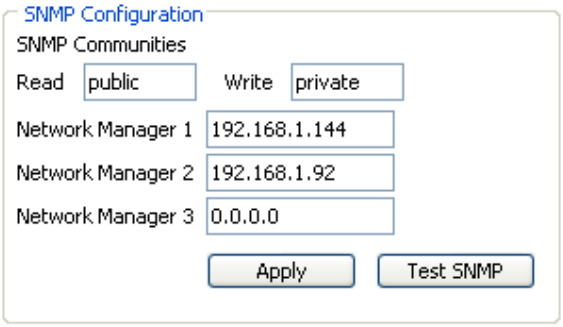
Email Addresses: SafetyNet Series 5 D40 shall attempt to deliver emails listed.

Email on Alarm Clearance: Select to receive emails when alarms are cleared.

Test Email: Upon applying settings, this button attempts to deliver a test email to ensure configuration is correct.

Apply Button: Checks validity of the available fields and updates 'SMTP Configuration' panel settings.

6.1.4 SNMP Configuration



Read SNMP Community: The read community setup by the network administrator for SNMP

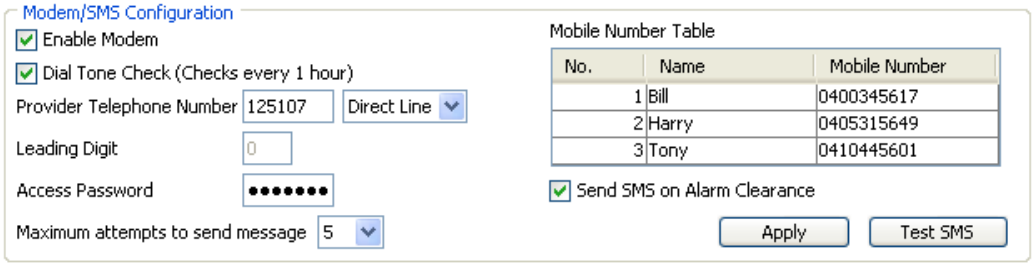
Write SNMP Community: The write community setup by the network administrator for SNMP. There are no writable attributes on SafetyNet Series 5 D40 at this stage.

Network Manager 1-3: IP addresses for delivery of SNMP traps. SafetyNet Series 5 D40 is able to deliver the same trap up to 3 network manager IP addresses.

Apply Button: Checks validity of the available fields and updates 'SNMP Configuration' panel settings.

6.1.5 Modem/SMS Configuration - PSTN Modem based units

Enable Modem: Select to enable modem. If modem is not enabled no SMS messages shall be delivered.



Dial Tone Check: Select to enable a dial tone check every hour. If the dial tone is not present, SafetyNet Series 5 D40 raises an alarm and then notifies via SNMP/SMTP and the web interface.

Provider Telephone Number & Line Type: Enter the dial out number for connecting to pager or SMS service (e.g.: SMS Access Manager).Configure the type of telephone line connected to SafetyNet Series 5 D40 by selecting 'Direct Line' or 'PABX'. If an analogue PABX line is connected, enter the leading digit to get an outside line under the '**Leading Digit**' field.

Access Password: Enter the access password provided by the paging or SMS service.

Maximum Attempts to Send Message: Select the maximum number of attempts so that a failing SMS/Pager message is kept trying until it is delivered by the unit. E.g.: line being busy or connection loss fails the delivery.

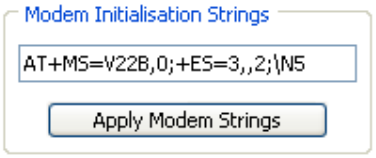
Mobile Number Table: Enter the mobile phone numbers along with names in this table. Names are not mandatory in this setting panel.

Send SMS on Alarm Clearance: Select to receive SMS messages when alarms are cleared.

Test SMS: Upon applying settings, this button attempts to deliver a test SMS message(s) to ensure configuration is correct.

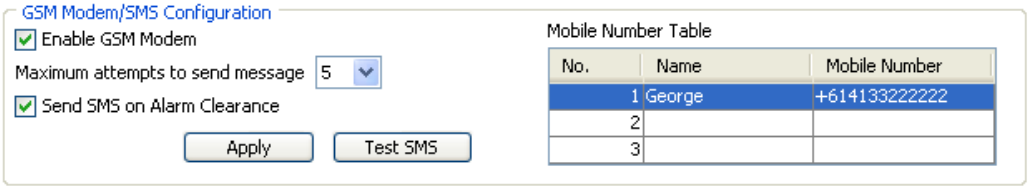
Apply Button: Checks validity of the available fields and updates 'Modem/SMS Configuration' panel settings.

Modem Initialisation Strings:



Modem initialization strings can be applied in sub panel 'Modem Initialisation Strings'. Enter the strings as necessary and click on 'Apply Modem Strings' button. It is assumed that the user is knowledgeable of the affect these strings have on the modem. The modem initialisation strings are further described in section 8.3.1 Modem Initialisation Strings.

6.1.6 GSM Modem/SMS Configuration – GSM Modem based units



Enable GSM Modem: Select to enable modem. If modem is not enabled no SMS messages shall be delivered.

Maximum Attempts to Send Message: Select the maximum number of attempts so that a failing SMS/Pager message is kept trying until it is delivered by the unit. E.g.: line being busy or connection loss fails the delivery.

Mobile Number Table: Enter the mobile phone numbers along with names in this table. Names are not mandatory in this setting panel.

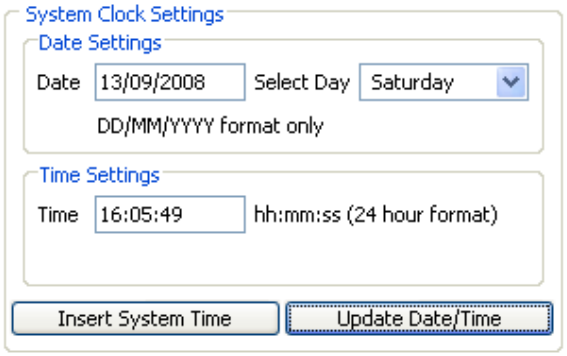
Send SMS on Alarm Clearance: Select to receive SMS messages when alarms are cleared.

Test SMS: Upon applying settings, this button attempts to deliver a test SMS message(s) to ensure configuration is correct.

Apply Button: Checks validity of the available fields and updates 'Modem/SMS Configuration' panel settings.

6.1.7 System Clock Settings

This panel allows setting the real time clock on SafetyNet Series 5. The date format should be DD/MM/YYYY and the time format should be HH:MM:SS in 24-hour format.



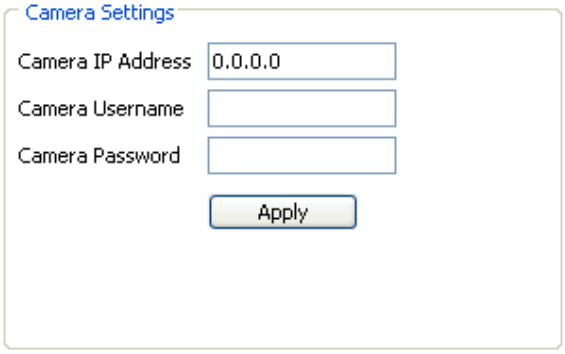
Insert System Time: Extracts the system time & date from the local machine and places them on the

appropriate fields. Optionally, SafetyNet Series 5 D40 has capability of using the NTP protocol to retrieve the time from services available on the Internet.

Update Date/Time*:* Updates the time and date on the fields on SafetyNet Series 5 D40.

6.1.8 Camera Settings

SafetyNet Series 5 D40 can be used to view IP Camera video page.



Enter the Camera IP address, username and the password to set up camera.

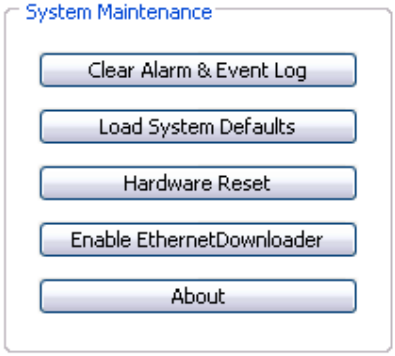
The camera view is accessed by clicking on the 'View Camera' button on the main menu.

Please note that the Camera feature required Active X components and DirectX to run on Internet Explorer, thus virtual machines cannot display the live view.

Apply Button: Checks validity of the available fields and updates 'Camera Settings' panel settings.

6.1.9 System Maintenance

Several maintenance options are provided for management purposes.



All buttons have confirmation boxes prompted as accidental clicks may have severe impact on device configuration and data.

Clear Alarm & Event Log: This button clears both alarm and event logs on SafetyNet series 5.

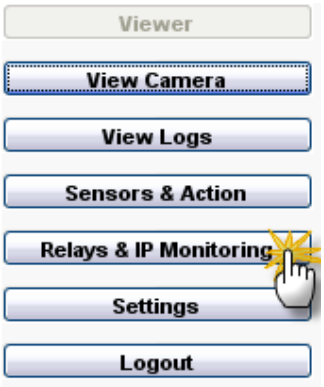
Load System Defaults: All settings excluding Network interface settings are set back to default. If there are active alarms on sensors, these shall be turned off as by default all sensors are disabled. If any relays are energized these will be turned off.
The alarm, event log and the graph data will be cleared.

Hardware Reset: Click to toggle power to the unit and resetting the device. It will cause all alarms to be redetected if present, and both relays to be turned off at start up.

Enable EthernetDownloader: Firmware upgrades on the device are carried through using an application named 'CSS Ethernet Downloader Utility' provided by Computer Support Systems. In order to download the binary image, it is necessary to authorize the device to receive this firmware file. Click this button to enable receiving new firmware. Please note that rebooting SafetyNet Series 5 D40 will default this option back to an off position.

About: Click on the about button to view the firmware version. The about box provides contact and model information.

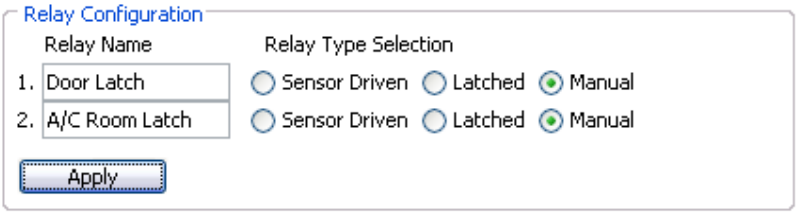
6.2 Relays & IP Monitoring Menu Item



To enter this menu item click on "*Relays & IP Monitoring*" button on SafetyNet Series 5 D40 web interface menu. Please note that this is a password protected menu item.

This interface allows configuring the two relays of the product & the IP monitoring settings.

6.2.1 Relay Configuration



Sensor Driven Option: Relays can be setup so that alarm activation causes relays to turn on or off.

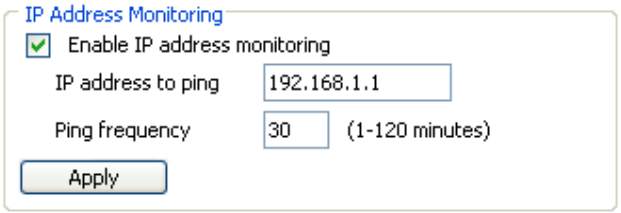
Latched: Additionally to 'Sensor Driven Option', relays can be set as latched, which allows a trigger of a relay to stay latched until such time it is released by a user via the web interface. The 'Reset' button on the 'Relay Status' turns active when a relay enters into such mode.

Manual: Relays can be setup, so that controlling is manual via the web interface.

Apply Button: Checks validity of the available fields/options and updates 'Relay Configuration' panel settings.

6.2.2 IP Address Monitoring

Enable IP Address Monitoring: Select this option to enable IP address monitoring.



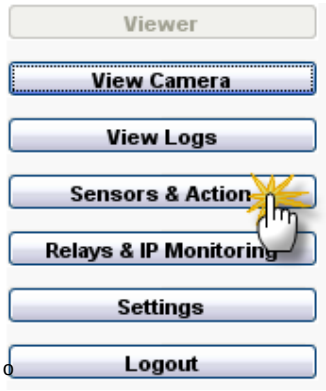
IP Address to Ping: A ping (ICMP) command is sent to the IP address provided in this field.

Ping Frequency: The frequency of the ICMP command is set via this field. Default is set to be 30 minutes.

Apply Button: Checks validity of the available fields/options and updates 'IP Address Monitoring' panel settings.

Please note that the monitored device should respond to ping commands. If ping (ICMP protocol) is disabled, SafetyNet Series 5 D40 may not receive a response, thus causing an IP Address Monitoring alarm.

6.3 Sensors & Action Menu Item

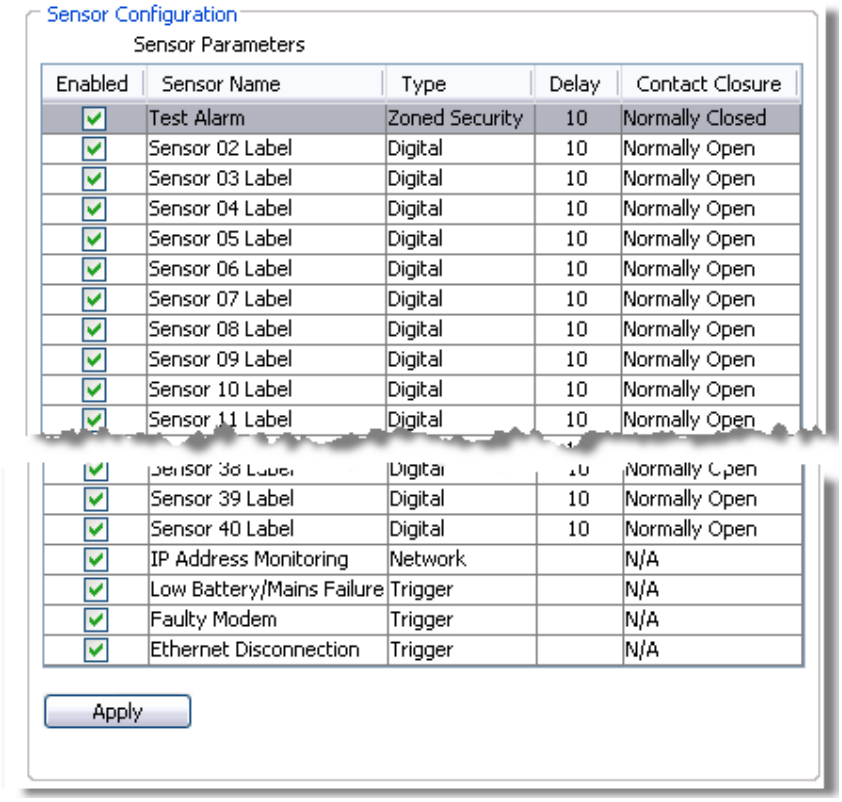


To enter this menu item click on "*Sensors & Relays*" button on SafetyNet Series 5 D40 web interface menu. Please note that this is a password protected menu item.

Use this interface to configure:

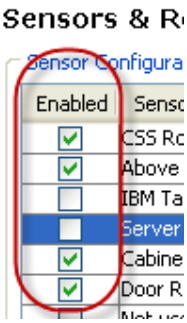
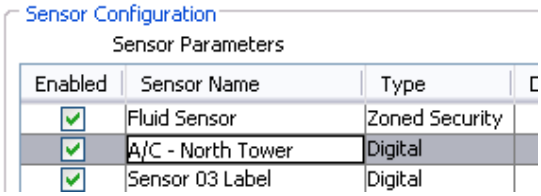
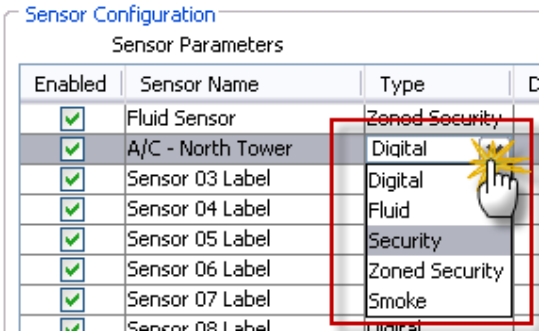
- Sensors
- Association of Relay action to Sensors state
- Association of SMS to Sensors/Alarms
- Association of Emails to Sensors/Alarms

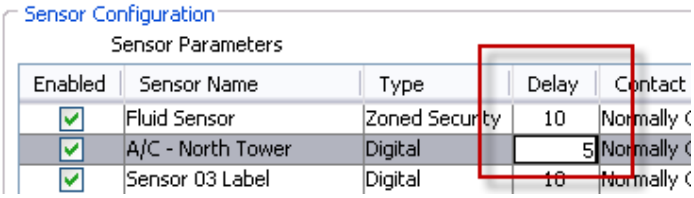
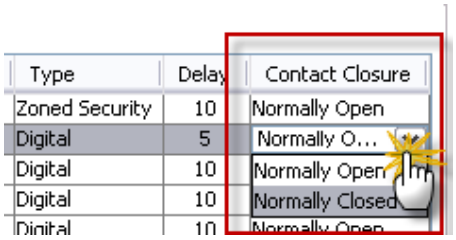
6.3.1 Sensor Configuration



This panel allows sensor configuration. Each row represents a sensor, where a user may configure appropriate settings such as the sensor label, sensor type, trigger delay and contact closure type.

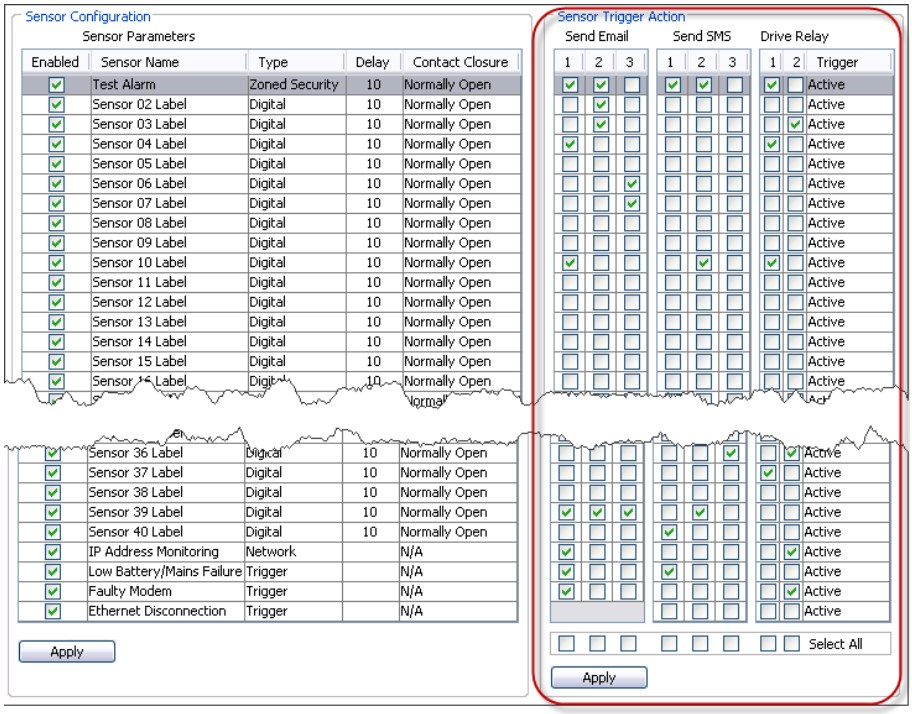
Sensor Settings - General:

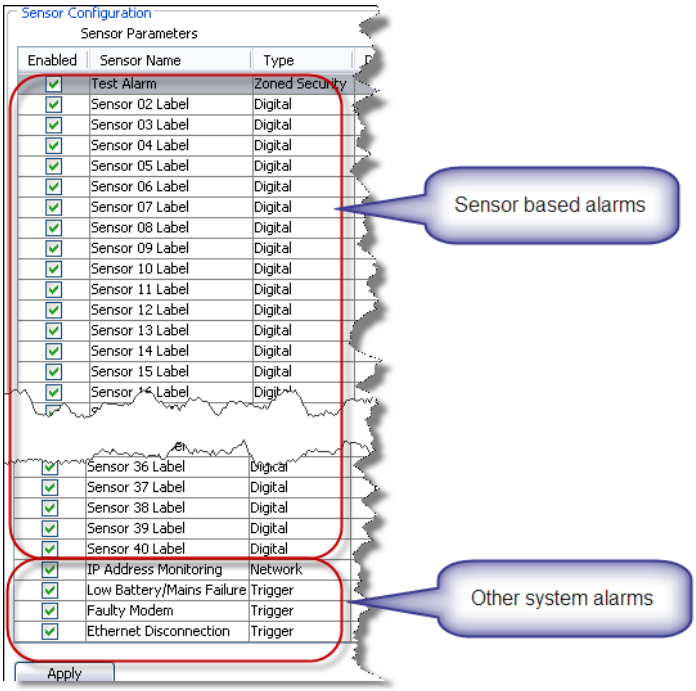
Column Name	Description
Enabled	To edit/configure a sensor, it has to be enabled first. All disabled sensors are not monitored by SafetyNet Series 5 D40. 
Sensor Name	A Sensor label can be given for identification of sensor: 
Type	Sensor Type can be selected by clicking on the drop down box in column 'Type' on the desired row. Sensor can be of type: o Smoke o Fluid o Digital o Zoned Security o Security 
Trigger Delay	A trigger delay for each sensor can be setup by entering a

	numeric value (in seconds) in column 'Trigger Delay'. This value is used to activate an alarm upon triggering and being active for the given duration specified. E.g.: A trigger delay of 20 causes the particular sensor to enter in to alarm mode, only if the alarm is active for 20 seconds. This shall eliminate spikes which may cause unnecessary alarms. 
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*" 

6.3.2 Sensor Trigger Action

This panel holds key mapping configuration settings for each sensor and other system alarms. The mapping allows setting up preference of delivery of emails, SMS messages and also setting up the relay action for relays when 'Sensor Driven' and 'Latched' selection is made.

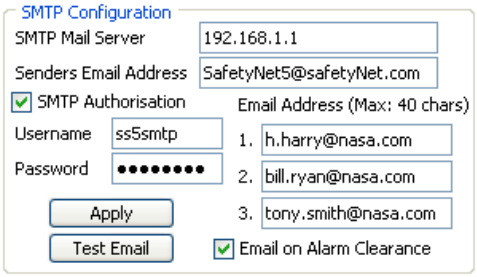




Send Emails based on Alarm:
It is required to set which alarms need to send emails to which email address in the matrix given below. (Note: Email addresses are set up as described by section 6.1.3 in this document.

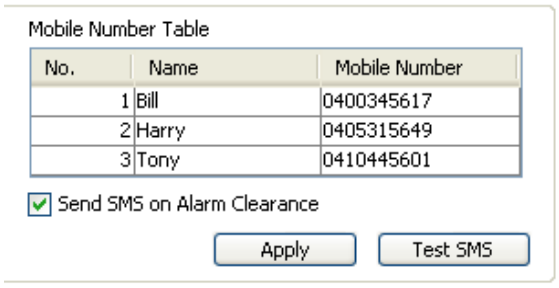
Follow each row and mark the columns 1, 2 or 3 with a tick to enabled emails for the email addresses 1, 2 or 3.

E.g.: Row 1 indicates that on alarm, sensor 1 (Label: CSS Room) shall deliver messages to email addresses at 1 & 2. From SMTP configuration (section 6.1.3) it is clear that emails addresses 1 & 2 are addressed to h.harry@nasa.com & bill.ryan@nasa.com respectively.



PS: emails are not available for 'Ethernet Disconnection' error.

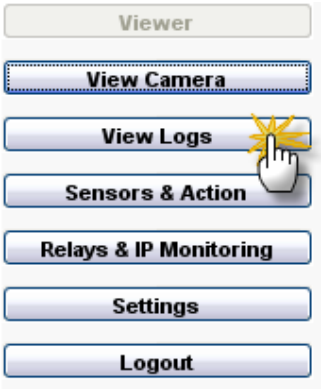
Send SMS messages based on Alarm:
The set up is similar to above email setup where instead of emails, SMS messages are delivered to recipients denoted by the 'Modem/SMS Configuration' described in section 6.1.5.



Drive Relays based on Alarm:
Relays can be driven on or off based on an alarm being active or inactive.

Select the relay which you wish to operate by following the sensor/trigger row and click on column 1 or 2. Then select the operation of the relay; i.e.: relay to be active when the alarm is active/inactive

7 Alarm and Event Logs on SafetyNet Series 5



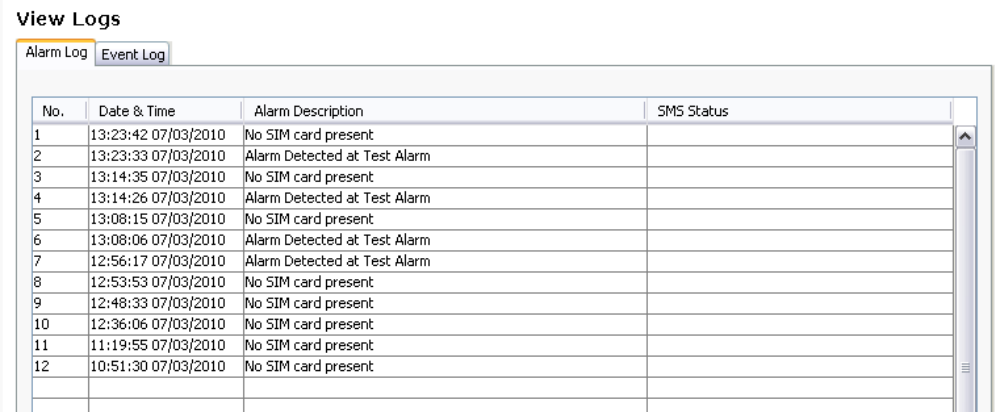
SafetyNet Series 5 D40 stores internal log entries for each alarm and event that occurs. These are two separate logs with up to 40 entries of each. When the log reaches more than 40 entries, the oldest entry is removed and the latest entry is added. Therefore, at any given time it is able to review the last 40 entries of alarms and events. To keep a record of the alarms and events, it is recommended to print the table or copy and paste the table to a file and save (e.g.: to Notepad/Excel) frequently.

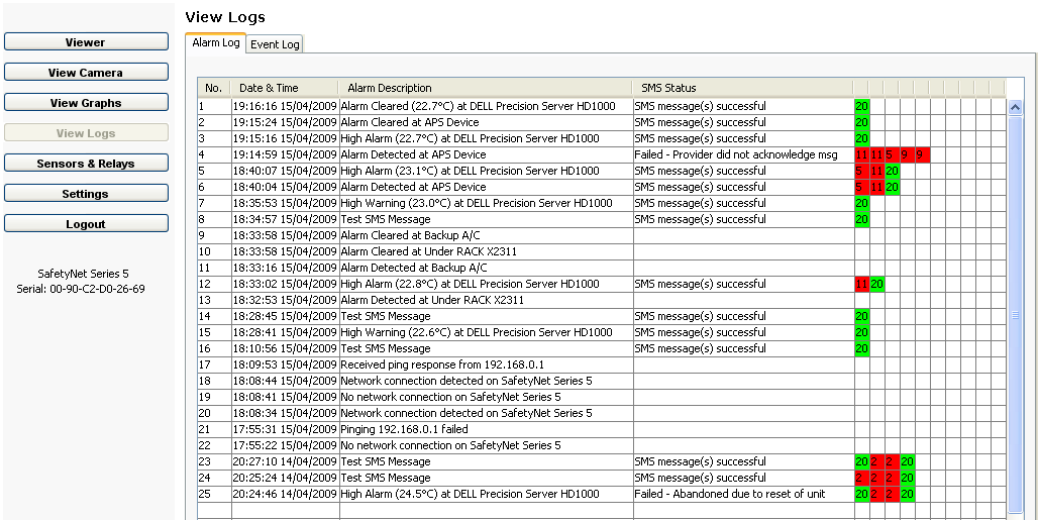
To view the alarm and event logs click on "*View Logs*" button on the main menu.

Each log entry consist 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. Additionally, IP monitoring alarm and the dial tone check error will be also logged in the alarm log.





No.	Date & Time	Alarm Description	SMS Status
1	19:16:16 15/04/2009	Alarm Cleared (22.7°C) at DELL Precision Server HD1000	SMS message(s) successful
2	19:15:24 15/04/2009	Alarm Cleared at APS Device	SMS message(s) successful
3	19:15:16 15/04/2009	High Alarm (22.7°C) at DELL Precision Server HD1000	SMS message(s) successful
4	19:14:59 15/04/2009	Alarm Detected at APS Device	Failed - Provider did not acknowledge msg
5	18:40:07 15/04/2009	High Alarm (23.1°C) at DELL Precision Server HD1000	SMS message(s) successful
6	18:40:04 15/04/2009	Alarm Detected at APS Device	SMS message(s) successful
7	18:35:53 15/04/2009	High Warning (23.0°C) at DELL Precision Server HD1000	SMS message(s) successful
8	18:34:57 15/04/2009	Test SMS Message	SMS message(s) successful
9	18:33:58 15/04/2009	Alarm Cleared at Backup A/C	
10	18:33:58 15/04/2009	Alarm Cleared at Under RACK X2311	
11	18:33:16 15/04/2009	Alarm Detected at Backup A/C	
12	18:33:02 15/04/2009	High Alarm (22.8°C) at DELL Precision Server HD1000	SMS message(s) successful
13	18:32:53 15/04/2009	Alarm Detected at Under RACK X2311	
14	18:28:45 15/04/2009	Test SMS Message	SMS message(s) successful
15	18:28:41 15/04/2009	High Warning (22.6°C) at DELL Precision Server HD1000	SMS message(s) successful
16	18:10:56 15/04/2009	Test SMS Message	SMS message(s) successful
17	18:09:53 15/04/2009	Received ping response from 192.168.0.1	
18	18:08:44 15/04/2009	Network connection detected on SafetyNet Series 5	
19	18:08:41 15/04/2009	No network connection on SafetyNet Series 5	
20	18:08:34 15/04/2009	Network connection detected on SafetyNet Series 5	
21	17:55:31 15/04/2009	Pinging 192.168.0.1 Failed	
22	17:55:22 15/04/2009	No network connection on SafetyNet Series 5	
23	20:27:10 14/04/2009	Test SMS Message	SMS message(s) successful
24	20:25:24 14/04/2009	Test SMS Message	SMS message(s) successful
25	20:24:46 14/04/2009	High Alarm (24.5°C) at DELL Precision Server HD1000	Failed - Abandoned due to reset of unit

Alarm log entries can be delivered via SMS messages when appropriate settings are configured in the 'Sensor Action Panel'. SMS attempt status is indicated by red or green colours. The SMS attempt status is provided by a number. Click on the 'Legend' button on the alarm log screen. Please note that attempt statuses are displayed only on the PSTN modem based version of SafetyNet Series 5.

Other items that are logged in the alarm log are mains failure, low battery warning and Ethernet disconnection errors.

Possible SMS status strings for the PSTN version are given in the table below.

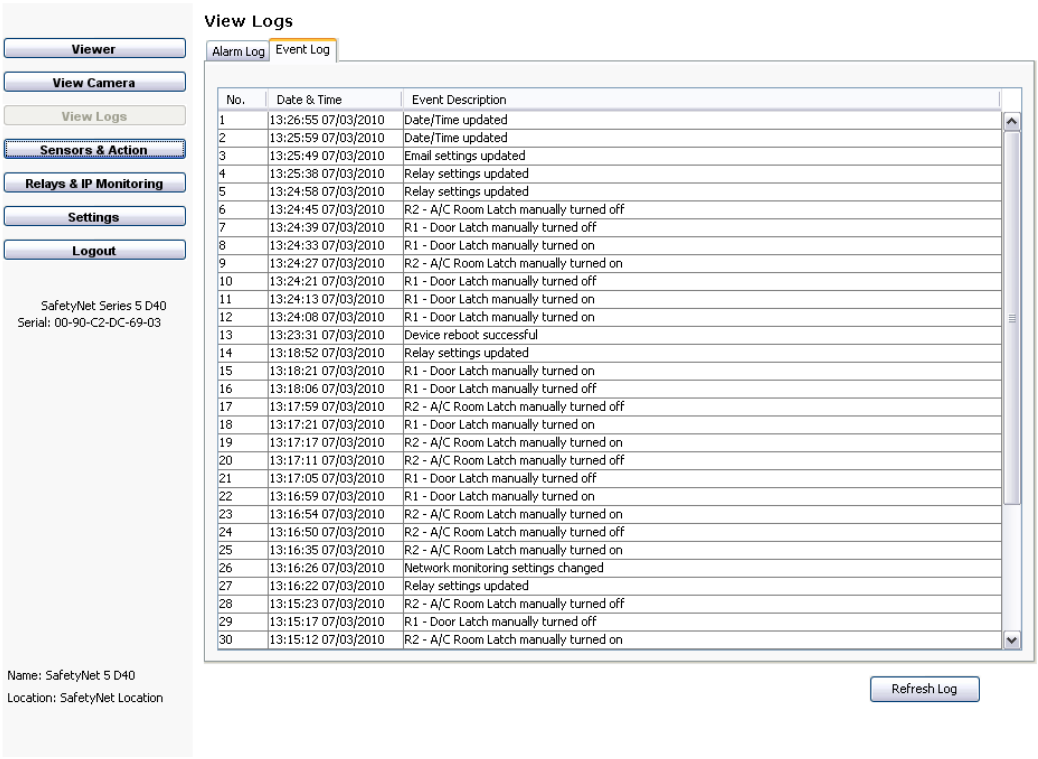
SMS Status	Description
SMS message(s) successful	The telephone network SMS gateway/Pager Service provider received the SMS/Pager request successfully. SMS/Pager message will be delivered if the mobile phone/Pager is turned on.
Failed - No reply from provider	Unit attempted to dial. No reply from the 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 - 'NO CARRIER' response	The modem responded with 'No Carrier'
Failed - 'CONNECT' not received	The modem dialed. Expected a 'CONNECT' status, however did not get connected with the destination modem.
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	Message not to be sent (eg: clearing of an alarm) or messages are not configured for this type of alarm.

Table 1.1

7.2 Event Log

The event log simply logs any internal event within SafetyNet Series 5. To view the event log, click on the tab "*Event Log*" once the alarm log is displayed.



7.2.1 Clearing of Alarm and Event Logs

Logs can be cleared by clicking the 'Clear Alarm & Event Log' button on the System Maintenance panel on 'Settings' menu. See section 6.1.9 for further details.

Note that loading factory defaults shall also clear the alarm and event log.

8 Operation of SafetyNet Series 5

8.1 Basic Operation

SafetyNet Series 5 D40 will constantly monitor '*enabled*' sensors. It is able to notify any alarm condition via several notification methods those being; SNMP traps, Email Messages, SMS messages, visually on the web interface, activation of relays, blinking LED on the unit, an optional strobe and an optional buzzer.

SafetyNet Series 5 D40 supports up to 40 external digital sensors. They can be Smoke, fluid, security and contact closure based sensors with on/off properties. SafetyNet Series 5 D40 has internal sensors for monitoring anti-tampering, mains failure, low battery, dial tone for PSTN modem and IP address monitoring sensors via software.

Any alarm or event will be logged, as an entry in its alarm and event log viewable at any given time.

SafetyNet Series 5 D40 is backed by an internal battery, which lasts for approximately 2.5 hours if main A/C power is not present. The internal battery is capable of running the sensors, the strobe and the buzzer at 12V DC. Users must not attempt to replace this battery at any stage. SafetyNet Series 5 D40 relays are driven at 12V DC.

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

8.2 External Sensors

Only sensors supplied by Computer Support Systems should be used with SafetyNet Series 5. Available sensor types are:

- Digital (contact closure based)
- Smoke
- Fluid
- Zoned Security
- Security
- PIR

All sensors are connected to the rear panel of SafetyNet Series 5.

8.2.1 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.

8.2.2 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 Series 5, an alarm is raised.

8.2.3 Digital Sensors

Digital sensors are contact closure sensors, and are capable of detecting open circuits or closed circuits. At the time of configuring digital sensors the system allows specifying the sensor be “Normally Open” or “Normally Closed”.

Each digital sensor carries a trigger delay up to 120 seconds. 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.
These digital sensors are 2-wire connection type which runs directly from the input.

8.2.4 PIR Motion Detector

Dual Sensor PIR with Pulse Count
This advanced design incorporates Motion Signal Discretion (MSD) processing to distinguish between motion and non-motion signals as well as pulse width analysis to ensure fast detection and superior detection performance. Pulse counting technology is utilised to virtually eliminate false detections and provide trouble free operation. This is an ideal PIR to expand your existing alarm system or for new installations that require good performance.

Features:
* 100 degree angle
* Intelligent Pulse Count
* Coverage of up to 15m
* Simple installation

8.3 Inbuilt PSTN Modem

This section applies to model ZSN5005P only.

The inbuilt modem is capable of notifying a mobile phone or a pager device when an alarm condition occurs, even when the network is down. This makes SafetyNet Series 5 D40 a reliable device even when power is completely down as the internal batteries will continue the operation of the unit for a further 2.5 hours and continue in notifying.

To activate the modem, it has to be enabled. The *Modem/SMS Configuration* panel under settings will allow configuring the modem and testing 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 and also notify via its user interface. Despite having this alarm active if a new message is to be sent, the unit will still attempt to send the message.
The connected telephone line type has to be configured within SafetyNet Series 5 D40 settings. The types that are allowed are a direct line or an analogue PABX line with a leading digit in front. By clicking the “*Test Alarm*” button on the *Modem/SMS Configuration* panel under settings, it is possible testing the delivery of the messages to all the numbers entered. Ensure that the latest configuration is updated on the interface with the latest phone numbers by clicking ‘Apply’ before proceeding with this option.

8.3.1 Modem Initialisation Strings

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

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.3*2bis* 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.

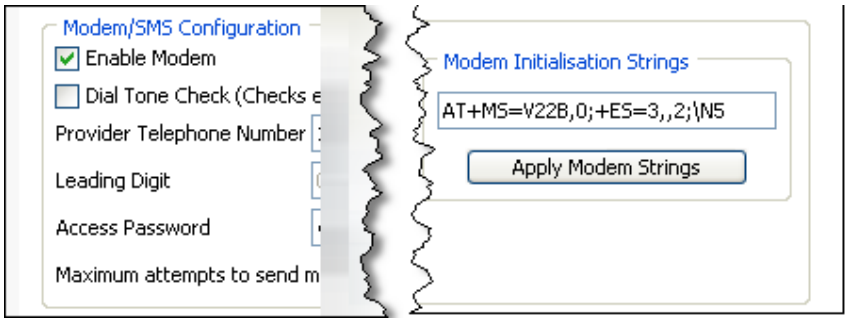
<ans_fbk>
Decimal number specifies the acceptable fallback mode of operation when the modem is operating as the answerer or specifies V.80 Synchronous Access Mode.

+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 Modem Strings' button.

8.4 Inbuilt GSM Modem

The GSM modem in SafetyNet Series 5 D40 requires a valid, post paid, PIN free GSM SIM card along with sufficient signal strength to deliver SMS messages. When in alarm conditions (also when network has failured including power) SafetyNet Series 5 D40 will operate and deliver SMS messages up to three mobile phone numbers.

8.5 Email Messaging from SafetyNet Series 5

The unit can send email messages when an alarm(s) is triggered or cleared up to three email addresses.

The unit requires a SMTP mail server address. Enter the SMTP mail server address, a valid senders email address, SMTP authentication details, an email address(es) and click on the 'Test Email' button in the email setup page (*Settings → SMTP Configuration Panel*) for testing the units functionality to ensure the unit performs this feature prior to setting up device in the field.

8.6 Network Interface and Traffic from SafetyNet Series 5

SafetyNet Series 5 D40 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 is TCP/IP and UDP. UDP packets are sent back and forth when the user interface is active on port 30705. The IP monitoring feature sends ICMP packets based on the frequency specified. SNMP operates on UDP on ports 161 and 162.

If the boot up preference is set to DHCP, at boot, up the unit configures its network interface after obtaining the network parameters from the DHCP server using UDP on standard ports used for DHCP/BOOTP protocols.

SafetyNet Series 5 D40 has a TCP/IP, HTTP web server that hosts the user interface on port 80.

SafetyNetFinder.exe is a tool provided by CSS to locate SafetyNet Family products on the local network. When running this tool please ensure the firewall is not preventing the communication. SafetyNetFinder.exe uses UDP for communications and allocates the next available port.

9 SMS/Pager Messages from SafetyNet Series 5

9.1 Introduction to SMS/Pager Messages from SafetyNet Series 5

SafetyNet Series 5 D40 is capable of sending SMS messages via two methods depending on the model:

1. Using the internal GSM Modem which requires a GSM SIM card independent of the network interface
2. Using the internal PSTN modem dialer and sending the SMS/Pager message independent of the network interface

9.2 SMS Messages using the GSM Modem

This section applies to model ZSN5005G only.

SafetyNet Series 5 D40 uses a SIM card and the internal GSM Modem to deliver SMS messages independent from the network interface. The reliability is increased of the transmission as even during network failures or power failure SafetyNet Series 5 D40 shall operate using the internal batteries.

9.2.1 Requirements for SMS Messages via the GSM Modem

The requirements to successfully send SMS messages via the GSM modem are:

- A valid GSM SIM card
- If SIM card is prepaid, sufficient credit
- Sufficient signal strength
- Appropriate configuration for GSM modem within SafetyNet Series 5
- 'Sensor Trigger Action' panel configured appropriately

9.2.2 Limitations

- The SMS message is sent only up to the three mobile phone numbers
- The time stamp noted on the SMS message is extracted from SafetyNet Series 5.
- SMS messages rely on the GSM Network
- SMS messages are delivered only when the mobile phone is switched on.

9.3 SMS/Pager Messages using the internal PSTN Modem

This section applies to model ZSN5005P only.

This particular model of SafetyNet Series 5 D40 has an inbuilt modem that is capable dialing out & delivering SMS/Pager messages when an alarm condition is triggered.

SafetyNet Series 5 D40 in alarm conditions dials the telephone/pager provider on a given number to a service provider and delivers the SMS/Pager messages via the PSTN (Public Switched Telephone Network).

The unit uses the TAP (Telocater Alphanumeric Protocol) protocol to communicate with the service provider.

9.3.1 Requirements for SMS Messages using the Modem

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

- An active PSTN telephone line provided to the unit.
- Correct configuration on the Modem/SMS Configuration on the Settings menu
- 'Sensor Trigger Action' panel configured appropriately
- 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/Pager messages via a dial up process. SafetyNet Series 5 D40 uses this service to send SMS/Pager 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 Series 5 D40 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.telstraenterprise.com/productsservices/mobility/messagingsolutions/Pages/SMSAccessManager.aspx

Please note: Chapter 10.3.2.1 information has be retrieved by Telstra's website at as at 24/04/2009. 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 Link Pager Service

SafetyNet Series 5 D40 has been tested with services from Link Pager Service. Contact Computer Support Systems for details in subscribing for this service.

9.3.3 Limitations

- The message is sent only up to the three mobile phone
- The time stamp noted on the message is extracted from SafetyNet Series 5.
- Messages rely on the PSTN (Public Switched Telephone Network) on distribution.
- Messages are delivered only when the mobile phone is switched on.

9.4 Sample Messages

Some of the sample messages would look like: (Unit name: 'Melbourne Unit', Unit Location 'Queens St')

Sensor Alarms

Message from Melbourne Unit, Queens St. Msg content: Alarm Detected at Fluid sensor under Server 11:21:19 29/04/2009

General alerts

Message from Melbourne Unit, Queens St. Msg content: Mains failure detected 12:41:15 12/02/2009

Message from Melbourne Unit, Queens St. Msg content: Low battery detected 23:18:01 03/01/2009

Message from Melbourne Unit, Queens St. Msg content: Lost Ethernet connection 10:33:06 27/03/2009

10 SNMP on SafetyNet Series 5

10.1 Introduction to SNMP Features on SafetyNet Series 5

SafetyNet Series 5 D40 is a SNMP (Simple Network Management Protocol) agent using SNMP Version 1. The type of sensor, the name and the current reading from any of the digital sensors and relay status can be retrieved via SNMP polling methods (GET commands).

On alarm or on clearance of an alarm, SafetyNet Series 5 D40 sends SNMP trap notifications up to three dedicated network managers. On boot up and on any configuration update, SafetyNet Series 5 D40 will send a trap indicating the update to these network managers.

Upon configuration of the SNMP parameters, SafetyNet Series 5 D40 allows to deliver a 'test' trap to verify trap delivery.

It is assumed that the reader is familiar with SNMP to use SNMP features and to feel comfortable with the rest of this chapter. SafetyNet Series 5 D40 uses SNMP V1 standards.

Computer Support Systems shall provide the CSS-TRAPS-MIB.MIB file for SNMP purposes.

10.2 SNMP Implementation

Computer Support Systems enterprise ID is 14748.

SafetyNet Series 5 D40 supports the SNMP System group and the Interfaces (no packet count information) in the MIB-II – System Objects defined by RFC1213. The following objects are implemented

MIB-II System - OID Name	OID
sysDescr	1.3.6.1.2.1.1.1
sysObjectID	1.3.6.1.2.1.1.2
sysUpTime	1.3.6.1.2.1.1.3
sysName	1.3.6.1.2.1.1.5
sysLocation	1.3.6.1.2.1.1.6

SafetyNet Series 5 D40 product OID is set as: 1.3.6.1.4.1.14748.1.10 also named as safetynetseries5D40 in CSS-TRAPS-MIB.MIB file.

The following implementation is made for the safetynetseries5D40 OID tree:

Object	Description
ss5D40Sensor01Type to ss5D40Sensor40Type OID: 1.3.6.1.4.1.14748.1.10.1.1.1 to 1.3.6.1.4.1.14748.1.10.1.40.1 Eg: ss5D40Sensor01Type, ss5D40Sensor02Type, … … ss5D40Sensor40Type Numerical syntax: Integer (32 bit) Base syntax: INTEGER Composed syntax: INTEGER Status: mandatory Max access: read-only	Provides an identification for the sensor/input type 0 = Digital 1 = Fluid 2 = Security 3 = Zoned Security 4 = Smoke

Size list: 1: 0..4	
ss5D40Sensor01Name to ss5D40Sensor40Name OID: 1.3.6.1.4.1.14748.1.10.1.1.2 to 1.3.6.1.4.1.14748.1.10.1.40.2 Numerical syntax: Octets Base syntax: OCTET STRING Composed syntax: DisplayString Status: mandatory Max access: read-only Size list: 1: 0..42	Sensor Name of SafetyNet Series 5
ss5D40Sensor01Reading to ss5D40Sensor40Reading OID: 1.3.6.1.4.1.14748.1.10.1.1.3 to 1.3.6.1.4.1.14748.1.10.1.40.3 Numerical syntax: Integer (32 bit) Base syntax: INTEGER Composed syntax: INTEGER Status: mandatory Max access: read-only Size list: 1: 0..1	SafetyNet Series 5 sensor reading. If sensor is Digital 1 = sensor in alarm condition 0 = sensor not in alarm condition
ss5D40IpMonitoringReading OID: 1.3.6.1.4.1.14748.1.10.1.41 Numerical syntax: Integer (32 bit) Base syntax: INTEGER Composed syntax: INTEGER Status: mandatory Max access: read-only Size list: 1: 0..1	SafetyNet Series 5 D40 IP Monitoring Alarm. 1 = alarm condition 0 = not in alarm condition
ss5D40LowBatteryReading OID: 1.3.6.1.4.1.14748.1.10.1.42 Numerical syntax: Integer (32 bit) Base syntax: INTEGER Composed syntax: INTEGER Status: mandatory Max access: read-only Size list: 1: 0..1	SafetyNet Series 5 D40 Low Battery. 1 = alarm condition 0 = not in alarm condition
ss5D40MainsFailureReading OID: 1.3.6.1.4.1.14748.1.10.1.43 Numerical syntax: Integer (32 bit) Base syntax: INTEGER Composed syntax: INTEGER Status: mandatory Max access: read-only Size list: 1: 0..1	SafetyNet Series 5 D40 Mains Failure Alarm. 1 = alarm condition 0 = not in alarm condition
OID: 1.3.6.1.4.1.14748.1.10.1.44	Unused. This is intentional.
ss5D40DialToneOrSIMErrorReading OID: 1.3.6.1.4.1.14748.1.10.1.45 Numerical syntax: Integer (32 bit) Base syntax: INTEGER Composed syntax: INTEGER Status: mandatory Max access: read-only Size list: 1: 0..1	SafetyNet Series 5 D40 Dial Tone Alarm for PSTN Modem Version. SafetyNet Series 5 D40 GSM SIM Card Error Alarm for GSM Modem Version. 1 = alarm condition 0 = not in alarm condition
ss5D40RelayOne OID: 1.3.6.1.4.1.14748.1.10.2.1 Numerical syntax: Integer (32 bit) Base syntax: INTEGER Composed syntax: INTEGER Status: mandatory Max access: read-only Size list: 1: 0..1	SafetyNet Series 5 D40 Relay One Status. 0 = Relay active 1 = Relay inactive
ss5D40RelayTwo OID: 1.3.6.1.4.1.14748.1.10.2.2 Numerical syntax: Integer (32 bit) Base syntax: INTEGER Composed syntax: INTEGER Status: mandatory	SafetyNet Series 5 D40 Relay Two Status. 0 = Relay active 1 = Relay inactive

Max access: read-only Size list: 1: 0..1	

Table 2.0

The above table provides information of OIDs to perform certain GET commands to retrieve SafetyNet Series 5 D40 related sensor readings from a given NMS.

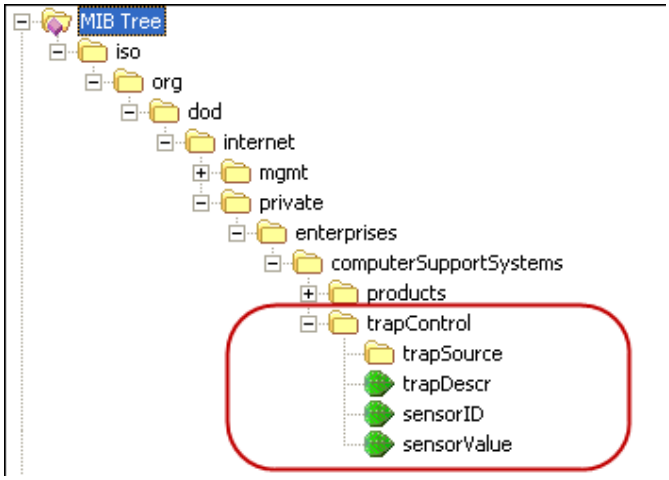
10.3 SNMP TRAP Implementation

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

Trap types for SafetyNet Series 5 D40 can be categorized in to four types:
1. Alarm type traps – for digital type sensors
2. Clear type traps – clearance of an alarm digital or other type (system alarms)
3. Event type traps – Event Notifications.

The trap types can be recognized from the prefix of the trap type name. All trap types have its Enterprise type set as 'trapControl' (1.3.6.1.4.1.14748.4)

The trapControl OID and the trap-type together has all information to capture and display traps and its relevant bind information



Name	OID	Description
trapSource	OID: 1.3.6.1.4.1.14748.4.1 Type: OBJECT-IDENTIFIER	points to the product the trap originates from - i.e.: safetynetseries5
trapDescr	OID: 1.3.6.1.4.1.14748.4.2 Numerical syntax: Octets Base syntax: OCTET STRING Composed syntax: DisplayString Status: mandatory Max access: read-only Size list: 1: 0..80	provides a textual description of the particular trap
sensorID	OID: 1.3.6.1.4.1.14748.4.3 Numerical syntax: Integer (32 bit) Base syntax: INTEGER Composed syntax: INTEGER Status: mandatory Max access: read-only Size list: 1: 0..16	allows identifying the sensor number the trap originates from

Table 2.1

Trap-Type table is listed below. Based on the alarm/warning/clearance or event on SafetyNet Series 5, the below trap types are used.

Trap Number	Trap-Type	Description
35	alarmSmokeSensor	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr, sensorID} DESCRIPTION Trap origin is from trapSource. Smoke sensor sensorID has triggered an alarm
36	clearSmokeSensor	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr, sensorID} DESCRIPTION Trap origin is from trapSource. Smoke sensor sensorID has cleared an alarm
37	alarmFluidSensor	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr, sensorID} DESCRIPTION Trap origin is from trapSource. Fluid sensor sensorID has triggered an alarm
38	clearFluidSensor	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr, sensorID} DESCRIPTION Trap origin is from trapSource. Fluid sensor sensorID has cleared an alarm
39	alarmDigitalSensor	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr, sensorID} DESCRIPTION Trap origin is from trapSource. Digital sensor sensorID has triggered an alarm
40	clearDigitalSensor	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr, sensorID} DESCRIPTION Trap origin is from trapSource. Digital sensor sensorID has cleared an alarm
41	alarmZonedSecuritySensor	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr, sensorID} DESCRIPTION Trap origin is from trapSource. Zoned Security sensor sensorID has triggered an alarm
42	clearZonedSecuritySensor	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr, sensorID} DESCRIPTION Trap origin is from trapSource. Zoned Security sensor sensorID has cleared an alarm

43	alarmSecuritySensor	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr, sensorID} DESCRIPTION Trap origin is from trapSource. Security sensor sensorID has triggered an alarm
44	clearSecuritySensor	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr, sensorID} DESCRIPTION Trap origin is from trapSource. Security sensor sensorID has cleared an alarm
45	alarmIPMonitoring	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. IP monitoring alarm has been triggered
46	clearIPMonitoring	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. IP monitoring alarm has been cleared
47	alarmLowBattery	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Low Battery alarm has been triggered
48	clearLowBattery	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Low Battery alarm has been cleared
49	alarmMainsFailure	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Mains Failure alarm has been triggered
50	clearMainsFailure	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Mains Failure alarm has been cleared
51	alarmDialTone	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Dial tone failure alarm has been triggered
52	clearDialTone	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Dial tone has been restored. Alarm has been cleared

55	alarmModemInitialisationError	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Modem initialisation caused an error
56	alarmSimCardError	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. SIM card caused an error
57	clearSimCardError	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. SIM card error cleared
58	clearEthernetConnection	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Ethernet Connection error is cleared
101	eventSNMPUpdate	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Event 'SNMP settings updated' triggered
102	eventEmailUpdate	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Event 'Email settings updated' triggered
103	eventSensorSettingsUpdate	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Event 'Sensor settings updated' triggered
104	eventDeviceRebootSuccessful	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Event 'Device reboot successful' occurred
105	eventDefaultsLoad	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Event 'Defaults loaded' triggered
106	eventFlashCorruptionDetection	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Event 'Falsh Corruption discovered. Loaded defaults' triggered

107	eventPasswordUpdate	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Event 'Password changed' triggered
108	eventDeviceReset	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Event 'Device reset via web interface' triggered
109	eventTimeDateUpdate	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Event 'Date/Time updated' triggered
110	eventDeviceParamsUpdate	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Event 'Device name/location updated' triggered
111	eventNetworkParamsUpdate	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Event 'Network parameters changed' triggered
112	eventModemUpdate	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Event 'SMS/Modem parameters changed' triggered
113	eventIPMonitoringUpdate	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Event 'Network monitoring settings changed' triggered
114	eventRelayUpdate	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Event 'Relay settings updated' triggered
115	eventSensorTriggerActionUpdate	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Event 'Sensor trigger action settings updated' triggered
116	eventLogCleared	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Event 'Alarm and Event log cleared' triggered

119	eventCameraUpdate	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Event 'Camera settings updated' triggered
120	eventRelayTurnedOn	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Event 'Relay turned on' triggered
121	eventRelayTurnedOff	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Event 'Relay turned off' triggered
122	eventRelayLatchReset	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Event 'Relay latch reset' triggered
123	eventTestSNMP	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Event 'Test SNMP Traps' triggered
124	eventTestSMS	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Event 'Test SMS' triggered
125	eventTestEmail	ENTERPRISE trapControl VARIABLES {trapSource, trapDescr} DESCRIPTION Trap origin is from trapSource. Event 'Test Email' triggered

Refer to the file CSS-TRAPS-MIB.MIB provided in the SafetyNet Series 5 D40 product CD-ROM for further details on the Management Information Base. The latest CSS-TRAPS-MIB.MIB is also available at http://www.csspl.com.au

10.4 Prerequisites

- A Network Manger System installed on your network or a SNMP sniffer program installed on your PC to detect SNMP traps.
- Correct SNMP configuration panel settings.

10.5 How to Receive Traps

If the read community is set according to the local network SNMP read community, on alarm, SafetyNet Series 5 D40 will send a trap out to each network manager IP address defined on its SNMP web interface.

SafetyNet Series 5 D40 sends a “cold start” trap at boot-up. In addition, upon a configuration updates a trap notification is sent.

10.6 Setting the MIB File

Use the CSS-TRAPS-MIB.MIB file and make it available for the Network Manager Software. The latest MIB file is also located at http://www.csspl.com.au. The SNMP software will allow 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.

10.7 Interpreting SafetyNet Series 5 D40 Traps

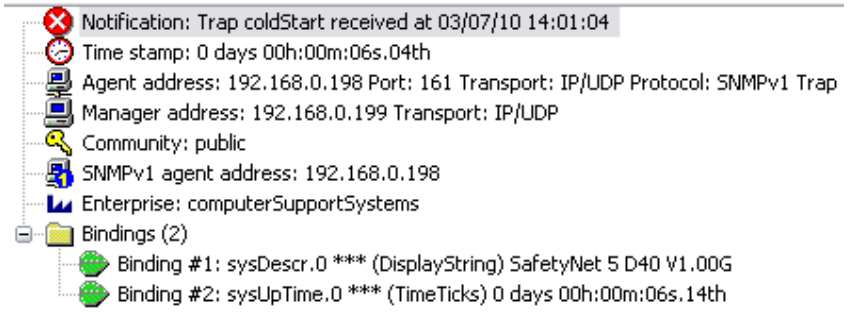
Every SNMP trap is accompanied by an OID indicating the device of the trap origin. This is provided by OID 1.3.6.1.4.1.14748.4.1 or 'trapSource' object in the MIB File. The 'trapSource' will point at 'safetynetseries5D40' (1.3.6.1.4.1.14748.1.10) at all times for this product.

Every trap also binds a string, which describes the notification in plain simple English. The OID of the message string is 'trapDescr' (1.3.6.1.4.1.14748.4.2).

In most alarm cases, more binding are attached to the trap, so that the alarm can be handled by the network manager software.

A few samples of the SNMP traps detect on a SNMP sniffer programs is depicted below using the SafetyNet Series 5 D40 product.

Coldstart trap

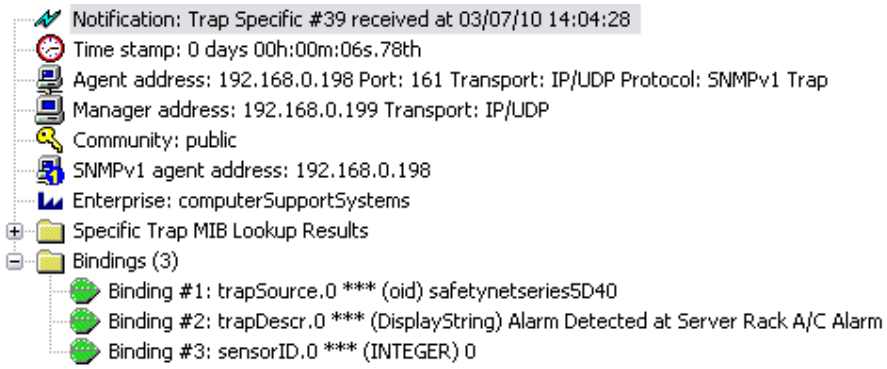


The bindings in the above image give indication of:

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

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

A digital sensor alarm trap (A/C alarm)

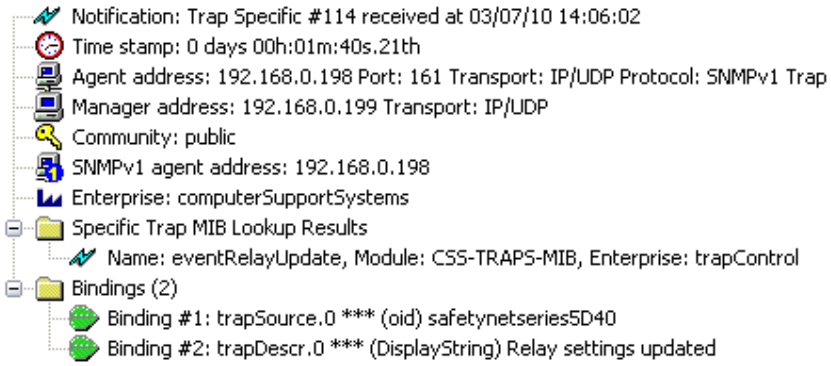


The bindings in the above image give indication of:

1. Trap Origin from SafetyNet Series 5 D40
2. Message string
3. Alarm trap is generated from Sensor Zero (first port on the sensor ports)

Also note the 'Specific' trap lookup is set as type #39, alarmDigitalSensor, Module: CSS-TRAPS-MIB, Enterprise: trapControl, indicating that it is a digital sensor that is in alarm condition.

A configuration update notification

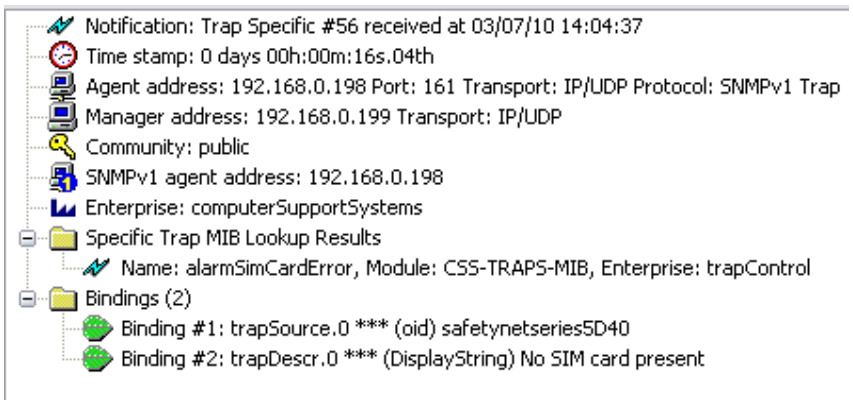


The bindings in the above image give indication of:

1. Trap Origin from SafetyNet Series 5 D40
2. Message string

Note the specific trap type is eventRelayUpdate, #114 indicating that the relay settings have been updated.

SIM card error notification trap



The bindings in the above image give indication of:

1. Trap Origin from SafetyNet Series 5
2. Message string

Note the specific trap type is alarmSimCardError, #56 indicating that SIM card is faulty or not present.

10.8 SNMP Polling

It is possible for the Network Manager Software (NMS) to poll the current sensor status periodically and store for various purposes. SafetyNet Series 5 D40 updates the SNMP objects under ss5D40Readings and ss5D40Relays 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.

Please note that the relay readings are inverted. 1 = relay is not energized and 0 = relay is energized.

11 Hardware Specifications

Device Model: SafetyNet Series 5 D40, ZSN5005, ZSN5005G, ZSN5005P

Physical Dimensions

- Dimensions: 480 mm L X 45 mm H (1 RU) X 107 mm W
- Weight: 1.55 kg
- Complies to IP 42

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 PSTN Modem (Optional - RJ45)

- 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 GSM Modem (Optional)

- Cellular Radio Global operation (quad GSM band: 800/900/1800/1900 MHz)
- Cellular Data GSM standard SMS, Fax, CSD (circuit), GPRS cl 10 (packet)

SafetyNet Series 5 D40 Operating Conditions

- Temperature range: -5°C to +55°C
- Humidity range: 5 - 95%, non condensing

Power Supply

- Operating voltage: 15VDC
- Input via plug pack: 90 – 264 VAC, 47-63Hz
- Meet energy star level (CEC) for 12~48V
- Meet EISA 2007(Energy Independence and Security Act)
- 3poleACinletIEC320-C14
- Class I power (with earth pin)
- Protections: Short circuit / Overload / Over voltage / Over temperature
- Class power (with earth pin)
- Protections: Short circuit / Overload / Over voltage / Over temperature
- Fully enclosed plastic case
- LED indicator for power on
- Approvals: UL / CUL / TUV / BSMI / CCC / CB / FCC / CE
- Current usage: 300 -1000 mA (high when battery is charging)
- Internally battery backed up to 2.5 to 3 hours of operation
- Safety Standards:- UL60950-1, TUV EN60950-1, BSMI CNS14336, CCC GB4943 approved
- Withstand Voltage:- I/P-O/P:3KVAC I/P-FG:1.5KVAC O/P-FG:0.5KVAC
- Isolation Resistance:- I/P-O/P, I/P-FG, O/P-FG/25/70%RH:100M Ohms/500VDC RH

- EMI Conduction& Radiation :- Compliance to EN55022 class B, FCC PART 15 / CISPR22 class B, CNS13438 class B, GB9254 class B
- Harmonic Current:- Compliance to EN61000-3-2,3, GB17625.1
- EMS Immunity:- Compliance to EN61000-4-2,3,4,5,6,8,11, light industry level, criteria A

PIR Motion Detector

- Dual element sensor
- 13mA current draw
- Selectable pulse count 2-3
- Tamper switch
- Walk test LED
- RFI immunity Ave. 30V/m (10-1000 MHz)
- Detectable speed range 0.3 - 1.5m/sec
- Dimensions 100(H) x 60(W) x 40(D)mm

12 Troubleshooting

This chapter provides troubleshooting tips for SafetyNet Series 5 D40 without having to contact technical support staff from Computer Support Systems.

When troubleshooting the following problems, make sure that the SafetyNet Series 5 D40 is powered on. Confirm that you are using an active 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 Series 5.	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. Make sure the Java Runtime environment is installed and the browser is configured to use the JRE.
There is no response when you type the IP address on the browser address bar.	The SafetyNet Series 5 D40 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 Series 5 D40 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 web interface is not loaded.	You may not have the Java™ Runtime Environment 1.6.0 or higher installed on your PC.	Install the Java™ Runtime Environment on your PC. This environment is a requirement of this product.
SNMP traps are sent, detected but SNMP bindings are not shown.	CSS-TRAPS-MIB.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.

12.1 Technical Support

If unable to troubleshoot SafetyNet Series 5 D40 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

13 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 Series 5 D40 Password Unlock Key
A specific key that allows entering a new password at the time of forgetting the SafetyNet Series 5 D40 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.

14 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/website (www.csspl.com.au) of SafetyNet Series 5 D40 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. Disable the firewall when the SafetyNet Finder application is used.

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 1.6.0 or higher installed.

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

Answer: SafetyNet Series 5 D40 supports up to 10 universal sensors. These sensors can be configured as temperature, humidity, fluid, smoke or as contact input sensor types. SafetyNet Series 5 D40 also supports a dual temperature/humidity sensor, however when used, the system utilizes two 'soft' ports and one 'physical' port. Ie: the second physical port cannot be used. The dual sensor type can be connected only to odd sensor numbers.

FAQ 4. What trigger delays are associated with sensors?

Answer: All sensor types have default trigger delays based on the sensor type. The user may adjust the trigger delay as required.

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

Answer: We recommend up to 60m of distance from the sensor to SafetyNet Series 5 D40 using CAT 5 type cables.

FAQ 6. 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 30 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 method 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 attempt pinging SafetyNet Series 5 D40 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 Series 5 D40 on the network.

FAQ 7. I have forgotten my password on my SafetyNet Series 5 D40 system. How can I access the product now?

Answer: SafetyNet Series 5 D40 provides a secure method to re-enter a new password if you have forgotten the existing password. If attempted to login to SafetyNet Series 5 D40 more than three times with an incorrect password it will provide specific instructions on how to obtain a password unlock key to access the product.