interSeptor Pro

Environmental Monitoring System for Data Centers, Server Rooms, Racks

8-Port, 16-Port, 24-Port Versions

User Manual V1.1

Jacarta

T. +44 (0) 1672 511125

Email: support@jacarta.co.uk

www.jacarta.co.uk

Copyright

Trademarks
DOS, Windows 95, 98, ME, NT, 2000, XP are registered trademarks of Microsoft Corporation.
All other trademarks belong to their respective proprietors.

Electronic Emission Notice

Federal Communications Commission
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

CE Notice
This device complies with the EMC directive of the European Community and meets or exceeds the following technical standard:

- EN 55022:1998 – "Limits and Methods of Measurement of Radio interference Characteristics of information Technology Equipment." This device complies with the CISPR Class B standard.
- EN 55024:1998 –"Electromagnetic compatibility – Generic immunity standard Part1: Residential, and light industry."

RoHS
This device is RoHS compliant.

WEEE
In accordance with the European Directive 2002/96/EC on Waste Electrical and Electronic Equipment (WEEE) Jacarta will arrange for the appropriate disposal of the product (at the end of its serviceable life).

Safety Information

- To reduce the risk of fire or electric shock, install the unit in a temperature-controlled indoor area free of conductive contaminants. Do not place the unit near liquids or in an excessively humid environment.
- Do not allow liquids or foreign objects to enter the unit.
- The unit does not contain any user-serviceable parts. Do NOT open the unit.
- Before shipment the unit must be completely switched off and unplugged and all connections must be removed.
- Before connecting the interSeptor Pro to the power supply, make sure the rating of power source is consistent with the rating of the interSeptor Pro.

Table of Contents

1 Introduction

The interSeptor Pro is a Network device designed for remote monitoring of temperature, humidity, and status of up to 24 environmental monitoring devices (EMDs) via a standard web browser, Network Management System (NMS) and Telnet. Alerts can be provided via email, SNMP, and telephone voice & SMS via the Jacarta Alert Centre Service (registration required). Alternatively SMS alerts can also be transmitted using a GSM modem (not supplied).

1.1 Features

The interSeptor Pro supports the following features:

- **Temperature and Humidity monitoring**
  You can monitor the temperature and humidity of any desired environment to protect critical equipment.
- **Contact closure status monitoring**
  You can monitor the status of up to forty-eight (48) volt free dry contact devices to protect your critical equipment.
- **The interSeptor Pro functions can be configured from any client (password protected)**
  You can set the interSeptor Pro settings from any SNMP management station or by web browser using HTTP forms and objects.
- **E-mail notification**
  Supports e-mail notification through SMTP via e-mail client software, when alarms are triggered or contact status changes.
- **History logs and events**
  When the temperature and humidity values exceed the user-defined limits, or the status of the contact closure changes, the logs are recorded in the History Log of the interSeptor Pro.
- **Optional Sensors**
  A range of Jacarta Sensors including Smoke, Security, Water leak and Power are available for connection to the interSeptor Pro.
- **Hot-swapping**
  You can install the EMDs safely without powering down the InterSeptor Pro.
- **Telephone Voice & SMS Alerts available via Jacarta Alert Centre (UK only)**
- **SMS**
  This is an integrated facility that requires an additional external GSM modem, by connecting the GSM modem the interSeptor Pro SMS Messages can be sent to up to 12 contacts. Please refer to "3.*4.7 Sending SMS (Using GSM Modem)*" for more detailed information.

Note: There are currently 3 interSeptor Pro versions available. 8, 16 and 24 port.

1.2 Package Contents

interSeptor Pro

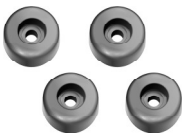
U-type handles (x 2)

Temperature/Humidity Probe (EMD) (x 8, 16, 24 version dependent)

19″ Bracket (x 2)

U-type handle screws (x 4)

RJ45 to RJ45 male cable for EMD connection (x 1,2 ,3 version dependant)



Feet (x 4)

Bracket screws (x 6)

Accessory Pack containing cable tie, velcro and screws for mounting EMD (quantity is version dependent)

Feet screws (x 4)

Quick Start Guide

AC power adapter

CD-ROM (containing MIB file for SNMP Network Management System (NMS), Quick Installation Guide, User Manual and Upgrade utility)

1.3 Front View

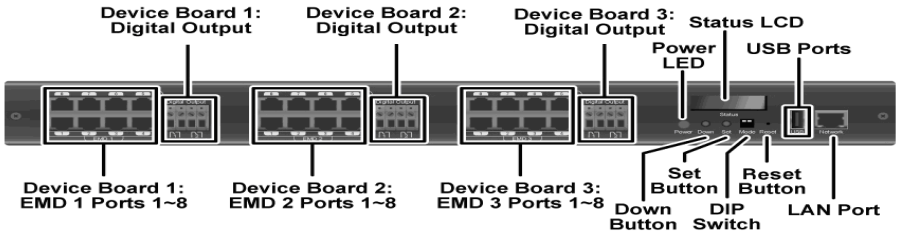


Figure 1-1 interSeptor Pro front view

Note: The USB 2.0 ports are standard interface connectors, designed primarily for use with an external keyboard or keypad.

1.4 Rear View

Figure 1-2 interSeptor Pro rear view

2 Installation

To install the interSeptor Pro on a network and change its configuration, you need a workstation running Microsoft Windows (9x, ME, NT4.0, 2000, XP or later). To configure the interSeptor Pro, connect it to your LAN and follow the instructions in the subsequent sections.

2.1 Installing the interSeptor Pro via LAN

Follow the steps below to install the interSeptor Pro via a LAN connection.

1. Ensure your workstation has a web browser installed and is connected to your LAN via a hub/router/Switch.
2. Connect one end of a network cable to the LAN port on the front of the interSeptor Pro and the other end to your hub.
3. Set the DIP switches of the interSeptor Pro to **OFF** by moving the switches upward.
4. Connect one end of the supplied CAT 5 network cable to any of the device board ports on the front of the interSeptor Pro and the other end to the RJ45 port on an EMD.
5. Insert one end of the power connector to the AC-In socket on the rear of the interSeptor Pro. Connect the other end to a power socket.

Upon successful connection, you can configure the interSeptor Pro via the web browser from any workstation connected to the same LAN as the interSeptor Pro. For further details, please refer to Chapter 3.

2.2 LED Overview

When you have successfully installed and powered on the interSeptor Pro, check the power LED and LCD screen to ensure it is operating properly. The power LED should be on (Green/Red depend on status) and “System Power On” should be displayed on the LCD screen.

The power LED is a bi-color LED, whose changes state depending on the alarm level.

1. Power LED Status

LED color	Blinking	Alarm Level
Green	No	None
Green	Yes	Informational
Red	Yes	Warning
Red	No	Critical

Note: If the sensor or output device is enabled from the Configuration page but the device is not connected, the LED will be red since the interSeptor Pro will treat this condition as a ‘communication loss ’.

2.3 LCD Screen Overview

You can view and configure the main system settings using the LCD screen and the **Down** and **Set** buttons on the front of the interSeptor Pro (see on page 8 for exact location of the switches). For additional security the LCD controls can be password protected with a default password of 0000.

The LCD screen operates in two modes: **idle** mode and **operation** mode.

2.3.1 LCD Screen in Idle Mode

When the system is started, the LCD screen is in idle mode. In this mode, system information, along with temperature and humidity alarm data for each connected EMD device is displayed. Press the **Down** button to scroll through the displayed information.

2.3.2 LCD Screen in Operation Mode

Press the **Set** button to enter operation mode. You can perform system configuration through the menus available in operation mode.

- Press the **Down** button to scroll through the settings menus.
- Press the **Set** button to enter settings menus and adjust values.
- To exit a settings menu without making any changes, press the **Set** and **Down** buttons simultaneously.

See the following for all available settings menus in operation mode.

No.	Setting Menu	Description	Default
1	IP Address	Set the IP address	192.168.001.001
2	Net Mask	Set the net mask	255.255.000.000
3	Gateway	Set the gateway	192.168.001.254
4	HTTP Security	Enable or disable login and password request for HTTP access	Enabled
5	Telnet Control	Enable or disable the TELNET protocol	Enabled
6	DHCP Function	Enable or disable the DHCP protocol	Disabled
7	Power Saving	Enable or disable the power saving function	00060
8	Back to Idle	Return to idle mode	N/A

Figure 2-1 LCD Screen: Operation mode menus

3 Managing interSeptor Pro via Web Browser

Open a web browser, enter the IP address of the interSeptor Pro and the **Comprehensive View** page is displayed.

Note: Click the **Help** icon located on the top right hand corner of each page for a detailed description. While navigating the screens, press the **Back** icon to return to the previously-viewed screen.

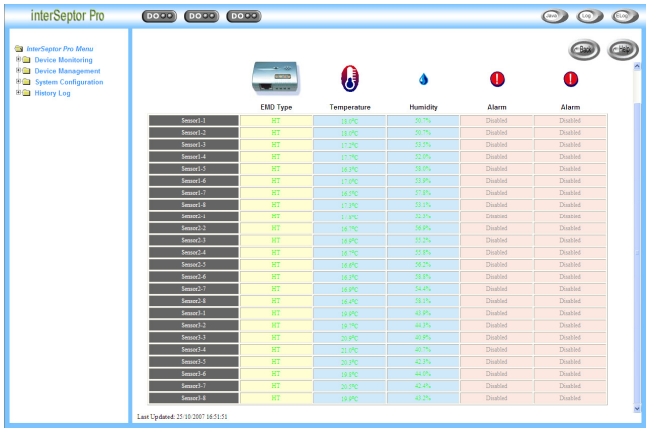


Figure 3-1 Use the Help and Back icons to navigate the pages

3.1 Initial Configuration

The first time you access the interSeptor Pro via the web browser, please follow the steps below to configure the basic settings.

1. Click the **Device Management** menu. Click the **Become Administrator** button at the bottom of the page. Enter the default login name (**iSPro**) and password (**admin**). The login name and password are case-sensitive.
2. Click the **System Configuration** menu, then do the following:
   - Click **System Configuration**. Modify the IP address, gateway, and subnet mask if necessary (see Chapter 3.4 System Configuration). Click the **Set Value** button to save the changes. (you may need to reconnect to the new IP address)
   - Click **Date and Time**. Enter the date and time settings (see Chapter 3.4.1 Date and Time). Click the **Set Value** button to save the changes.
3. Click **System Control** to enable or disable the network protocols (see Chapter 3.4.3).
4. Click the **Apply** button to save the changes.

Note: These settings can also be set via the LCD screen on the front of the interSeptor Pro. See Chapter 2.3.2 LCD Screen in Operation Mode for more details.

3.2 Device Monitoring

There are six sub-menus in the **Device Monitoring** menu:

- **Comprehensive View**
- **Device Board-1 Web Pages**
- **Device Board-2 Web Pages**
- **Device Board-3 Web Pages**
- **Identification Web Pages**
- **Alarm Table Web Pages**

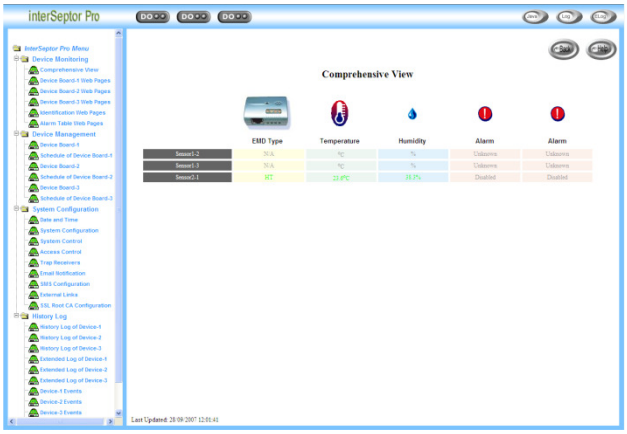


Figure 3-2 Device Monitoring-Comprehensive View

3.2.1 Comprehensive View

This page displays the information of all the sensors and output devices connected to the interSeptor Pro. It also provides an overview of alarm status.

This page is the default home page of the interSeptor. A summary of all the devices connected to the interSeptor Pro is presented. The parameters are updated automatically every 5 seconds.

Figure 3-3 Comprehensive View

The text color of each parameter indicates status:

Text Color	Status
Green	Normal
Yellow	Warning
Red	Critical
Grey	Unknown

The text color of the alarm columns also indicates status:

Text Color	Status
Red	Alarm is active
Green	Alarm is inactive

3.2.2 Device Board Web Pages

The **Device Board 1**, **2**, and **3 Web Pages** provide detailed information for all sensors or output devices connected to each device board. The parameters are updated automatically every 5 seconds.

Note: The following instructions apply for each of the **Device Board-1 Web Page**, **Device Board-2 Web Page**, and **Device Board-3 Web Page** screens.

Click the **Reset** button to reset data for a specific parameter, or the **Reset All** button reset data for all parameters for a specific sensor or output device.

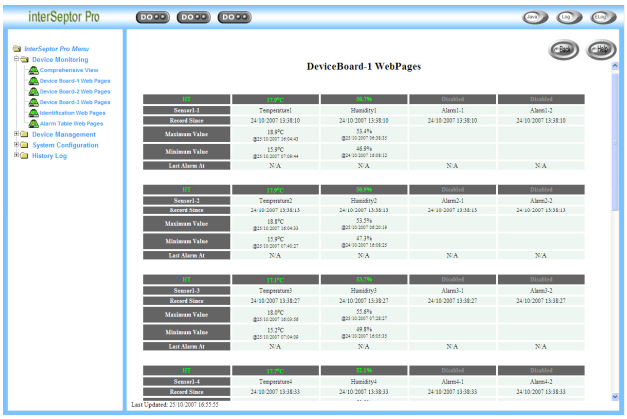


Figure 3-4 Device Board Web Page

3.2.3 Identification Web Pages

This page provides general interSeptor Pro identification information, including firmware version and the date and time. All the information in this page is read-only.

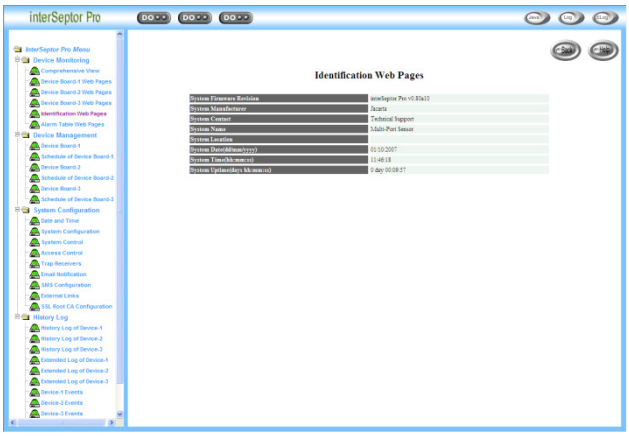


Figure 3-5 Identification Web Page

3.2.4 Alarm Table Web Pages

This page provides information on the number of currently active alarms, alarm ID, alarm time, and alarm description. All the information in this page is read-only. This page will refresh automatically after 5 seconds.

When an alarm is activated, you can access this screen from any page by clicking the alarm icon at the top of the screen.

Figure 3-6 Alarm Table Web Page

3.3 Device Management

The **Device Management** menu allows the configuration of EMD sensors, Dry contact sensors, and output controls connected to each of the device boards on the interSeptor Pro.

There are six sub-menus in the **Device Management** menu:

- **Device Board-1**
- **Schedule of Device Board-1**
- **Device Board-2**
- **Schedule of Device Board-2**
- **Device Board-3**
- **Schedule of Device Board-3**

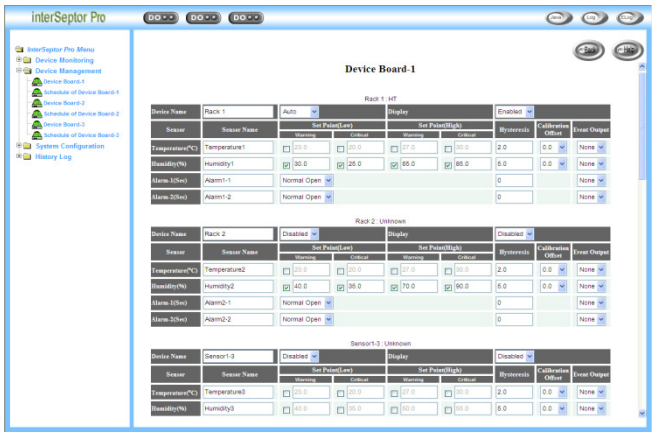


Figure 3-7 Device Management: Device Board 1

3.3.1 Device Board Screens

The **Device Board-1**, **Device Board-2**, and **Device Board-3** screens allow you (as administrator) to configure settings and alarm schedules for eight EMDs (maximum) on each device board.

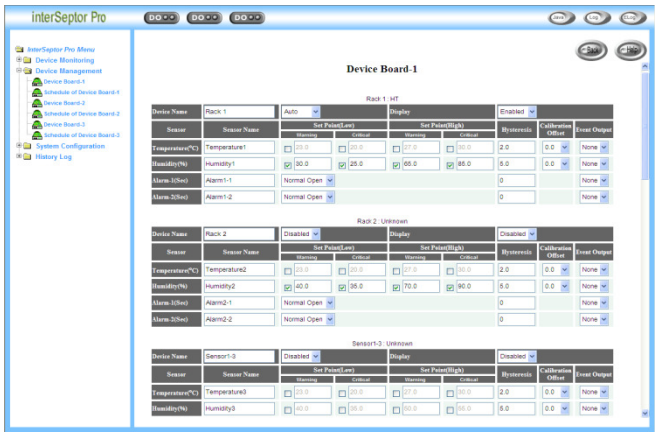


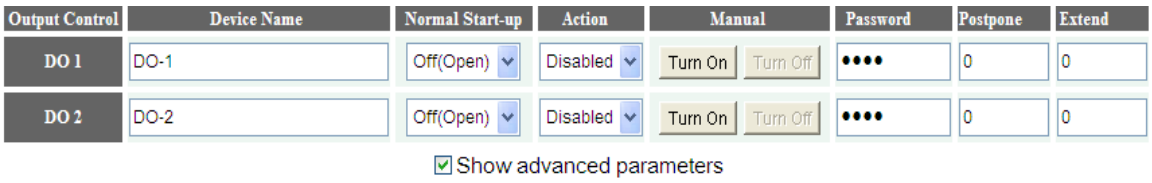
Figure 3-8 Device Board 1

Note: The following instructions apply for each of the **Device Board-1**, **Device Board-2**, and **Device Board-3** screens.

Configure the following settings for a new device:

- **Device Name**: Enter the device name.
- **Device Status**: Select **Auto** from the drop down menu to enable the device or **Disabled** to disable.
- **Display**: Select **Enable** from the drop down menu to display the device in the Comprehensive View and Java display or **Disabled** to disable.
- **Set Point**: Enter a temperature or humidity value over or under which an alarm will be triggered. You can enter values for warning or critical levels. The valid ranges are as follows:
  Temperature: -15℃ (5 ℉) to 65 ℃ (149 ℉)
  Humidity: 5% to 95%
- **Hysteresis**: A sensors value could be floating around the configured threshold, triggering multiple alarms. Setting the hysteresis will help to prevent the alarm being constantly activated and deactivated in this situation.
  For example, if the low warning threshold point is 20 and hysteresis is 3, then the alarm will activate when the value reaches 20 but will not deactivate until the value reaches 23.
  For the contact alarm sensors, the hysteresis can be used to adjust the sensitivity of an alarm. The alarm will be active or inactive only after the alarm stays in the same state of the hysteresis value (in seconds).
- **Calibration Offset**: If the measurement value of a sensor does not comply with the actual environment for whatever reason, a calibration offset value can be set to adjust the final sensor reading.
  For example, if a sensor reports 43% humidity in an environment where humidity is at 45%, you can set the humidity offset to 2% so the sensor can adjust its final reading.
- **Alarm Type**: If an alarm is connected to the interSeptor Pro, select from **Normal Open**, **Normal Close** or **Disabled**.

  Normal Open & **Normal Close** are used for a two wire detector that emulates an open/close state.
- **Event Output**: Select from **D01** or **D02** as the event output when a digital output is connected. Scroll down to the bottom of the screen to configure output control settings. Check **Show advanced parameters** and the following will display:



Configure the following settings:

- **Device Name**: Enter the device name.
- **Normal Start-up**: Select **On(Close)** or **Off(Open)** to configure the normal status of the device.
- **Action:** Select to **Enable** or **Disable** the digital output.
- **Manual Control**: Select **Turn On** to turn on a device manually or **Turn Off** to turn it off.

  Password: Enter a password for each digital output. It must be 4 digits long, within the range of **0000** – **9999**. The default password is 0000.
- **Postpone**: Enter a value in seconds by which the alarm trigger time can be postponed if necessary. If set to zero, the digital output will be activated as soon as an alarm is triggered.
- **Extend**: Enter a value in seconds before which the digital output changes back to start up status after an alarm is triggered. If set to zero, the digital output will be deactivated as soon as an alarm is triggered.

3.3.2 Schedule of Device Board Screens

The **Schedule of Device Board-1**, **Schedule of Device Board-2**, and **Schedule of Device Board-3** pages allow you (as administrator) to set a schedule by which alarms can be disabled.

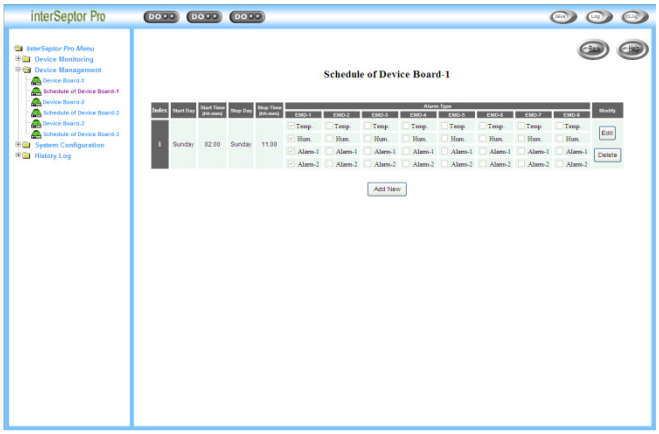


Figure 3-9 Schedule of Device Board 1 page

Note: The following instructions apply for each of the **Schedule of Device Board-1**, **Schedule of Device Board-2**, and **Schedule of Device Board-3** pages.

Click **Add New** to create a new schedule.

Configure the following settings:

- **Alarm Disable Start Day**: Select the day of the week on which the alarm will be deactivated.
- **Alarm Disable Start Time**: Enter the start time.
- **Alarm Disable Stop Day**: Select the day of the week on which the alarm will be reactivated.
- **Alarm Disable Stop Time**: Enter the stop time.
- **Alarm Type**: Select the alarm types to deactivate during the scheduled time. Only alarm types that are not selected will alarm if triggered.

Click **Set Value** to confirm and save the schedule.

The configured schedule will appear on the page. Click the **Edit** button to edit the schedule details or the **Delete** button to delete the schedule.

3.4 System Configuration

The **System Configuration** menu allows you to configure all system settings on the interSeptor Pro.

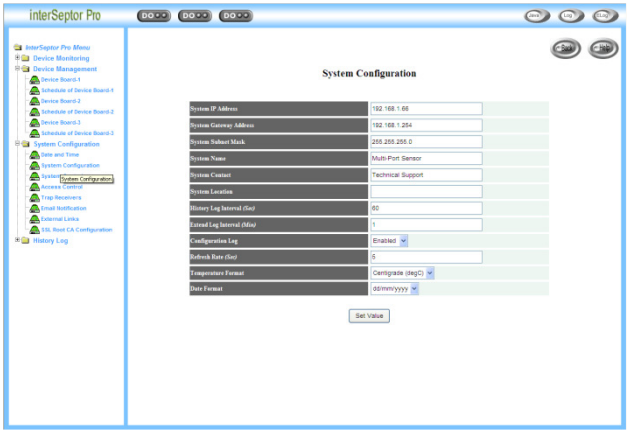


Figure 3-10 System Configuration: Date & Time

There are nine sub-menus in the **System Configuration** menu:

- **Date and Time**
- **System Configuration**
- **System Control**
- **Access Control**
- **Trap Receivers**
- **Email Notification**
- **External Links**
- **SMS Configuration**
- **SSL Root CA Configuration**

3.4.1 Date and Time

This page allows you (as administrator) to set the date and time of the interSeptor Pro manually or synchronize the settings with the computer time or an NTP (Network Time Protocol) server.

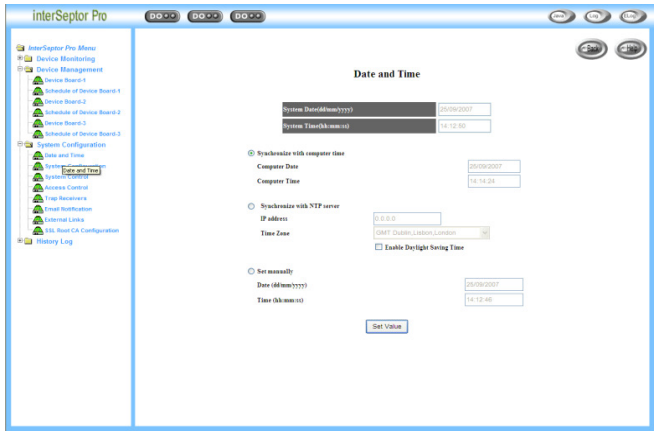


Figure 3-11 Date and Time

3.4.2 System Configuration

This page allows you (as administrator) to set all system configuration settings.

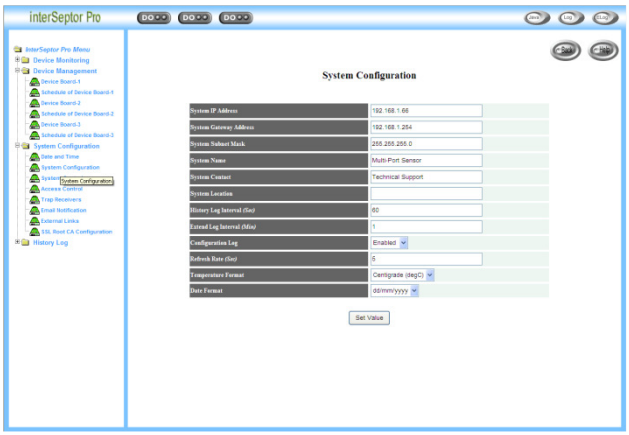


Figure 3-12 System Configuration

3.4.3 System Control

This page allows you (as administrator) to enable or disable the communication protocols available in the interSeptor Pro, or assign a different port number for the communication protocol. You can also click the **Reset to Default** button to reset all default configurations for the interSeptor Pro, or the restart **interSeptor Pro** button to restart the interSeptor Pro.

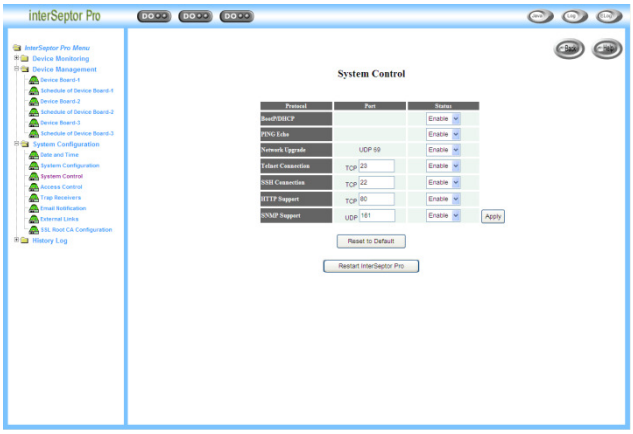


Figure 3-13 System Control

3.4.4 Access Control

This page allows you (as administrator) to add SNMP NMS stations specified for read-only, read/ write, or restricted access to the interSeptor Pro.

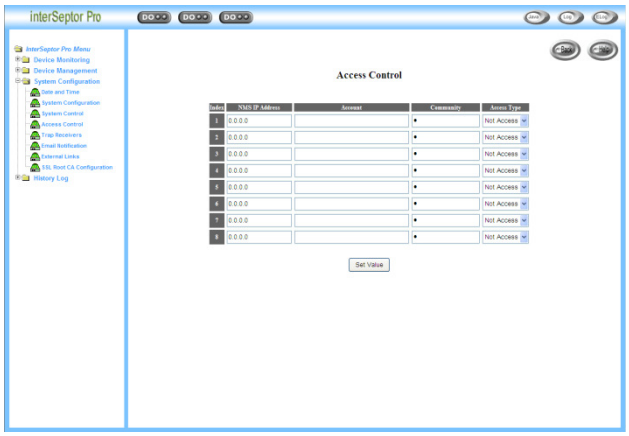


Figure 3-14 Access Control

3.4.5 Trap Receivers

This page allows you (as administrator) to modify the settings for SNMP trap receivers (for SNMP Network Management).

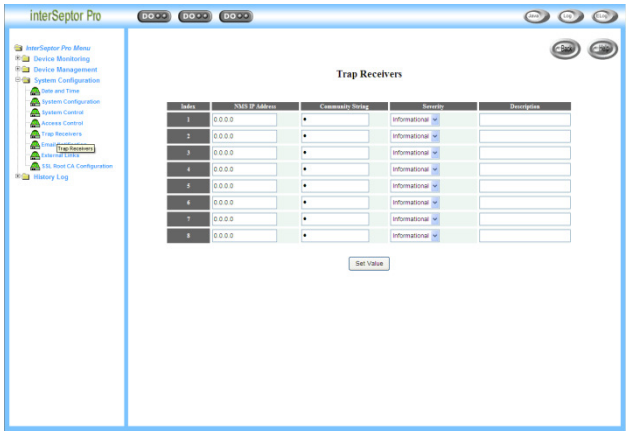


Figure 3-15 Trap receivers

3.4.6 Email Notification

This page allows you (as administrator) to configure the mail server and mail receiver settings to send alert emails when an event occurs.

After setting up the mail server and receiver, you can click the **Send Test** button to make sure your email system is working properly.

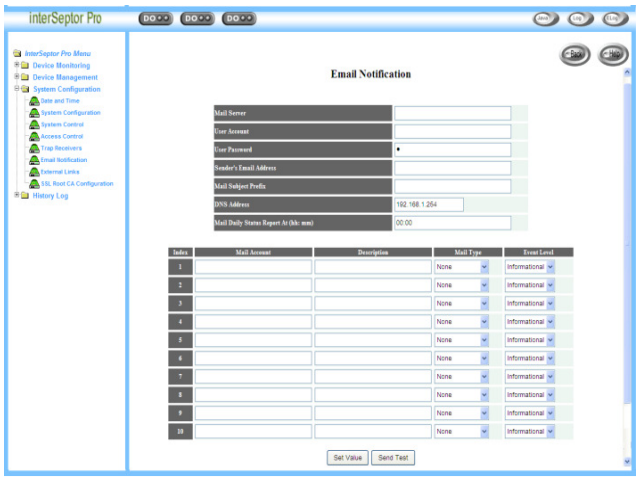


Figure 3-16 Email notification

3.4.7 Sending SMS (Using a GSM Modem)

This page allows you (as administrator) to configure the SMS settings for sending messages to recipients when events occur.

Follow the steps below to add/edit/delete a short message.

1. You have to connect the GSM modem to interSeptor Pro, as shown below:

Figure 3-17 Connect GSM modem to interSeptor Pro

2. Set the **GSM modem function** to ENABLE.

Figure 3-18 SMS configuration page

Configure the following settings to enable/disable the GSM modem:

- **GSM Modem Function**: Choose **Enable**/ **Disable** to enable or disable the **GSM Modem Function**. Up to twelve phone numbers maximum
- **Authentication and Pin Code**: If the SIM card is locked by PIN code, tick **Authentication** and enter the correct Pin Code into **Pin Code**.
- **Set Value**: Press the **Set Value** button to confirm.

Info: A GSM Modem is required for this functionality. Please ensure that the baud rate for the modem is 38400. Please see **Appendix C**

3. Add a new message for an SMS recipient.

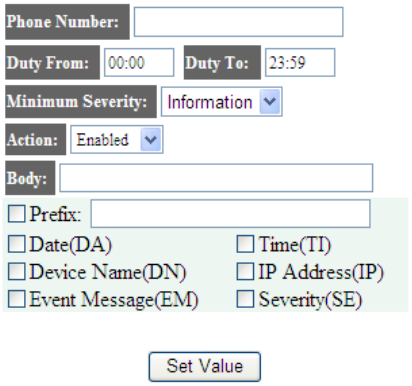


Figure 3-19 New SMS page

Configure the following settings for a new message:

- **Phone Number:** Enter a phone number to send the SMS to.
- **Duty From and Duty To:** Enter a start and end time and only during this period of time the SMS recipient will be sent SMS messages, when events occur.
- **Minimum Severity:** Choose the **Information**/ **Warning**/ **Severe** to set the minimum level of the event to be received.
- **Action:** Choose **Enable**/ **Disable** to enable/ disable sending the message to the SMS recipient.
- **Body:** Enter the content of the SMS.
- **Prefix:** Enter the title of the SMS message. 30 characters maximum.
- **Set Value**: Press **Set Value** to confirm and then the setting is listed on the **SMS configuration** screen.

4. If an SMS message needs to be edited then press **Edit** to configure the messages on the SMS configuration screen. To delete the message press **Delete** or alternatively **Delete All** to remove all recipients.

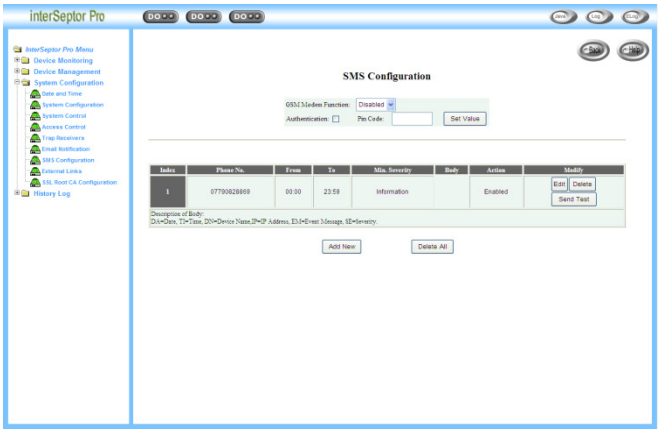


Figure 3-20 SMS configuration page with SMS list

3.4.8 External Links

This page allows you (as administrator) to specify up to ten links in this page. Each link can be configured to an external web page, such as another interSeptor Pro or Technical Support home page. The links will appear under the “External Links” menu on the left.

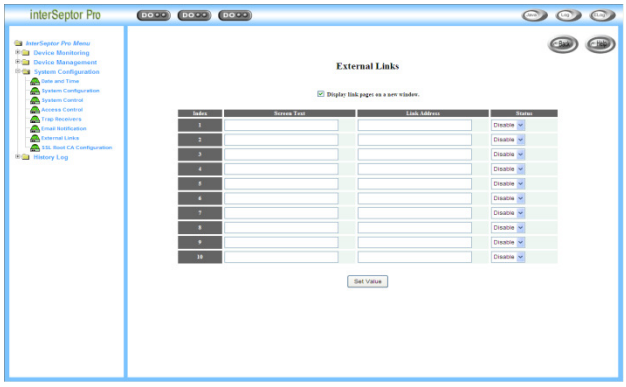


Figure 3-21 External links setup

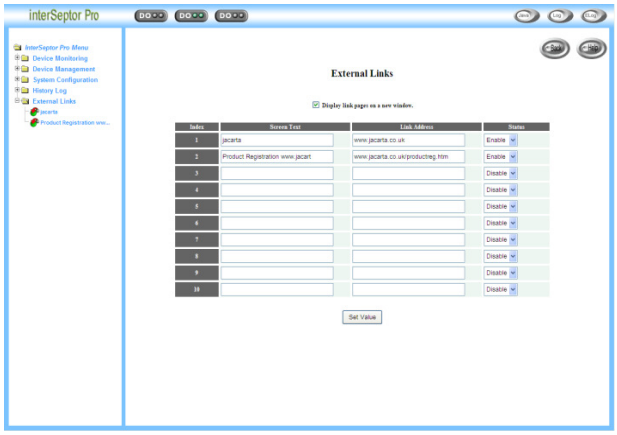


Figure 3-22 the links appear on the left of the page

3.4.9 SSL Root CA Configuration

You can download the Root CA certificate of the interSeptor Pro and the Root CA certificate of the interSeptor Pro for Java plug-in. The interSeptor Pro Root CA self-signed certificate contains the interSeptor Pro Root CA public key. Installing the interSeptor Pro Root CA prevents the browser from prompting for CA confirmation when opening the interSeptor Pro pages with HTTPS.

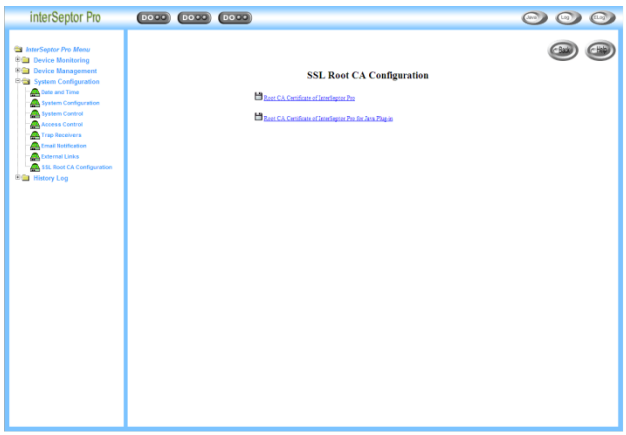


Figure 3-23 SSL Root CA Configuration

3.5 History Log

The **History Log** menu displays detailed past activity for each connected EMD sensor and the interSeptor Pro system as a whole.

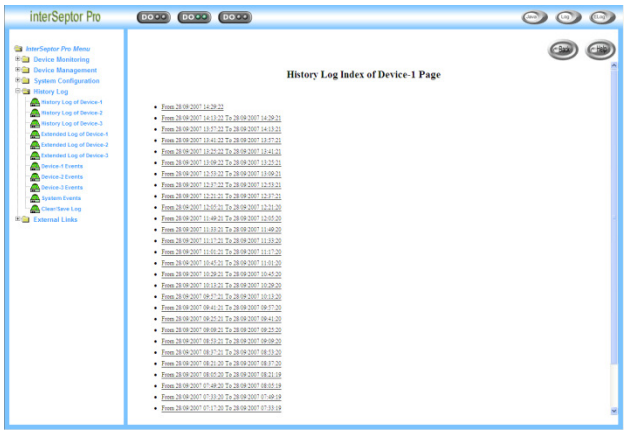


Figure 3-24 History: History Log Index of Device-1 Page

There are eleven sub-menus in the **History Log** menu:

- **History Log of Device-1**
- **History Log of Device-2**
- **History Log of Device-3**
- **Extended Log of Device-1**
- **Extended Log of Device-2**
- **Extended Log of Device-3**
- **Device-1 Events**
- **Device-2 Events**
- **Device-3 Events**
- **System Events**
- **Clear/Save Log**

3.5.1 History Logs of Devices

These pages give a snapshot of all the fundamental EMD parameters on each of the three device boards. The existing values will be overwritten when the maximum number of entries (rows) is reached. The administrator has the right to delete the table entries.

Note: To save the history log, please refer to Chapter 3.5.5.

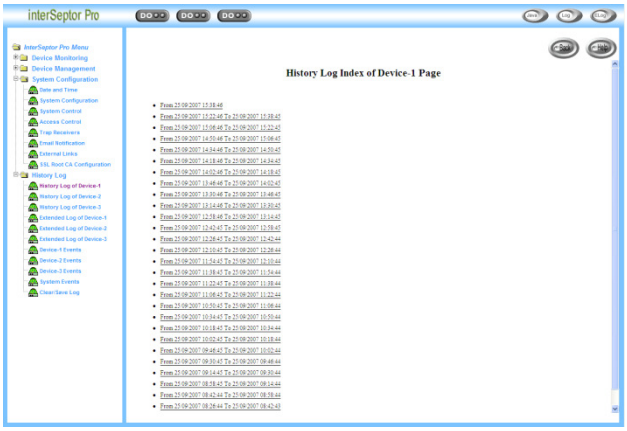


Figure 3-25 History Log Index of Device-1 Page

History Log Data of Device-1

Log Date (dd/mm/yyyy)	Log Time (hh:mm:ss)	Temp-1 (°C)	Temp-2 (°C)	Temp-3 (°C)	Temp-4 (°C)	Temp-5 (°C)	Temp-6 (°C)	Temp-7 (°C)	Temp-8 (°C)	Hum-1 (%)	Hum-2 (%)	Hum-3 (%)	Hum-4 (%)	Hum-5 (%)	Hum-6 (%)	Hum-7 (%)	Hum-8 (%)
25/09/2007	15:38:46	24.6	N/A	N/A	N/A	N/A	N/A	N/A	N/A	40.7	N/A	N/A	N/A	N/A	N/A	N/A	N/A
25/09/2007	15:39:46	24.6	N/A	N/A	N/A	N/A	N/A	N/A	N/A	40.8	N/A	N/A	N/A	N/A	N/A	N/A	N/A
25/09/2007	15:40:46	24.6	N/A	N/A	N/A	N/A	N/A	N/A	N/A	40.8	N/A	N/A	N/A	N/A	N/A	N/A	N/A
25/09/2007	15:41:46	24.6	N/A	N/A	N/A	N/A	N/A	N/A	N/A	40.8	N/A	N/A	N/A	N/A	N/A	N/A	N/A
25/09/2007	15:42:46	24.6	N/A	N/A	N/A	N/A	N/A	N/A	N/A	40.8	N/A	N/A	N/A	N/A	N/A	N/A	N/A
25/09/2007	15:43:46	24.6	N/A	N/A	N/A	N/A	N/A	N/A	N/A	40.8	N/A	N/A	N/A	N/A	N/A	N/A	N/A
25/09/2007	15:44:46	24.6	N/A	N/A	N/A	N/A	N/A	N/A	N/A	40.8	N/A	N/A	N/A	N/A	N/A	N/A	N/A
25/09/2007	15:45:46	24.6	N/A	N/A	N/A	N/A	N/A	N/A	N/A	40.9	N/A	N/A	N/A	N/A	N/A	N/A	N/A
25/09/2007	15:46:46	24.6	N/A	N/A	N/A	N/A	N/A	N/A	N/A	40.9	N/A	N/A	N/A	N/A	N/A	N/A	N/A
25/09/2007	15:47:46	24.6	N/A	N/A	N/A	N/A	N/A	N/A	N/A	40.9	N/A	N/A	N/A	N/A	N/A	N/A	N/A
25/09/2007	15:48:46	24.6	N/A	N/A	N/A	N/A	N/A	N/A	N/A	40.9	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Figure 3-26 History Log Data of Device-1

3.5.2 Extended Logs of Devices

These pages give a consolidated view of the EMD parameters taken over a period on each of the three device boards. The minimum, maximum and the average values of temperature and humidity are shown.

Note: The administrator can change the consolidation interval by changing the value of the Extended Log Interval in “System/ Configuration” page. The existing logs will be overwritten when the maximum number of entries is reached.

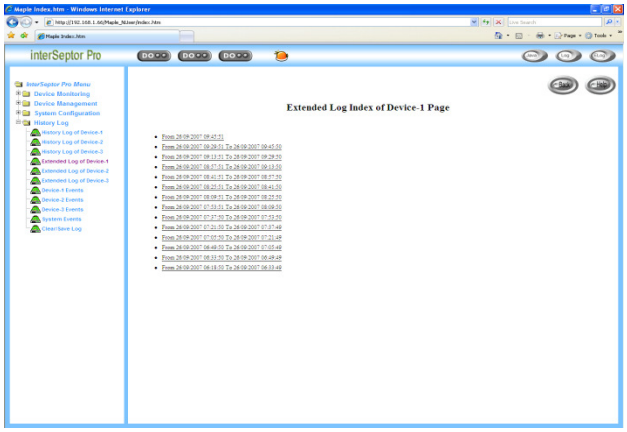


Figure 3-27 Extended Log Index of Device-1 Page

Extended Log Data of Device-1

Start Date (dd/mm/yyyy)	Start Time (hh:mm:ss)	End Date (dd/mm/yyyy)	End Time (hh:mm:ss)	Temp-1 (°C)			Temp-2 (°C)			Temp-3 (°C)			Temp-4 (°C)			Temp-5 (°C)			Temp-6 (°C)			Temp-7 (°C)			Temp-8 (°C)			hum-1 (%)		
				min	avg	max	min	avg	max	min	avg	max	min	avg	max	min	avg	max	min	avg	max	min	avg	max	min	avg	max	min	avg	max
29/04/2008	14:06:05	29/04/2008	14:16:04	25.5	25.5	25.5	27.7	27.7	27.8	28.0	28.1	28.1	39.6	39.8	40.0	32.1	32.2	32.2	25.9	25.9	25.9	N/A	N/A	N/A	N/A	N/A	N/A	35.5	35.7	35.8
29/04/2008	14:16:05	29/04/2008	14:26:04	25.5	25.5	25.5	27.7	27.7	27.7	28.0	28.0	28.1	39.6	39.8	39.9	32.1	32.1	32.2	25.9	25.9	25.9	N/A	N/A	N/A	N/A	N/A	N/A	35.8	35.9	35.9
29/04/2008	14:26:05	29/04/2008	14:36:04	25.5	25.5	25.5	27.7	27.7	27.7	28.0	28.0	28.1	39.7	39.8	40.0	32.1	32.1	32.2	25.9	25.9	25.9	N/A	N/A	N/A	N/A	N/A	N/A	35.9	35.9	36.0
29/04/2008	14:36:05	29/04/2008	14:46:04	25.5	25.5	25.5	27.7	27.7	27.8	28.0	28.0	28.1	39.7	40.1	40.7	32.1	32.1	32.2	25.9	25.9	25.9	N/A	N/A	N/A	N/A	N/A	N/A	36.0	36.0	36.0
29/04/2008	14:46:05	29/04/2008	14:56:04	25.5	25.5	25.5	27.7	27.7	27.8	28.0	28.0	28.1	39.8	40.1	40.7	32.1	32.1	32.2	25.9	25.9	25.9	N/A	N/A	N/A	N/A	N/A	N/A	36.0	36.1	36.1
29/04/2008	14:56:05	29/04/2008	15:06:04	25.5	25.5	25.5	27.7	27.7	27.8	28.0	28.1	28.1	39.8	40.1	40.4	32.1	32.1	32.2	25.9	25.9	25.9	N/A	N/A	N/A	N/A	N/A	N/A	36.1	36.1	36.2
29/04/2008	15:06:05	29/04/2008	15:16:04	25.5	25.5	25.6	27.7	27.8	27.8	28.0	28.1	28.1	39.9	40.3	40.6	32.1	32.1	32.2	25.9	25.9	25.9	N/A	N/A	N/A	N/A	N/A	N/A	36.1	36.2	36.2
29/04/2008	15:16:05	29/04/2008	15:26:04	25.5	25.5	25.6	27.7	27.8	27.8	28.0	28.1	28.1	39.8	40.1	40.6	32.1	32.2	32.2	25.9	25.9	25.9	N/A	N/A	N/A	N/A	N/A	N/A	36.1	36.2	36.2
29/04/2008	15:26:05	29/04/2008	15:36:04	25.5	25.5	25.5	27.7	27.8	27.8	28.0	28.1	28.1	39.7	39.9	40.5	32.1	32.1	32.2	25.9	25.9	26.0	N/A	N/A	N/A	N/A	N/A	N/A	36.0	36.1	36.1
29/04/2008	15:36:05	29/04/2008	15:46:04	25.3	25.5	25.5	27.6	27.7	27.8	28.0	28.0	28.1	34.9	38.0	39.7	32.1	32.1	32.2	25.8	25.9	25.9	N/A	N/A	N/A	N/A	N/A	N/A	35.8	35.8	36.0

Figure 3-28 Extended Log Data of Device-1

3.5.3 Device Events

This page lists all the device events. The logs will be overwritten when the maximum number of entries (rows) is reached.

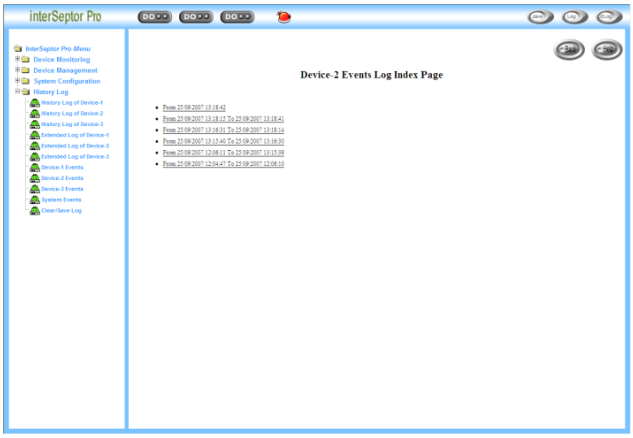


Figure 3-29 Device-2 Events Log Index page

Events Log Data of Device-1

Date (dd/mm/yyyy)	Time (hh:mm:ss)	Event Description
25/09/2007	13:30:41	Rack 2 communication lost
25/09/2007	13:30:41	Sensor1-3 communication lost
25/09/2007	13:44:30	Rack 2 communication restored
25/09/2007	13:44:30	Sensor1-3 communication restored
25/09/2007	17:04:27	Rack 1 communication lost

Figure 3-30 Events Log Data of Device-1

3.5.4 System Events

This page lists all the system events. The administrator has the right to delete the entries.

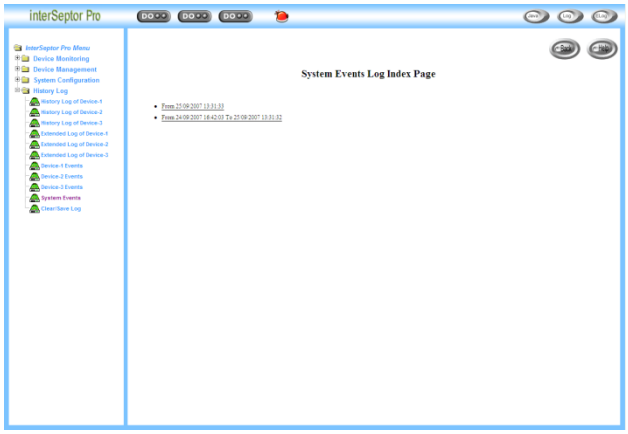


Figure 3-31 interSeptor Pro events page

System Events Log Data

Date (dd/mm/yyyy)	Time (hh:mm:ss)	Event Description
25/09/2007	13:31:33	Dev-3 EMD-1 EMD status had changed from HTTP by 192.168.1.87
25/09/2007	13:31:33	Dev-3 EMD-1 EMD display had changed from HTTP by 192.168.1.87
25/09/2007	13:31:33	Dev-3 EMD-2 EMD status had changed from HTTP by 192.168.1.87
25/09/2007	13:31:33	Dev-3 EMD-2 EMD display had changed from HTTP by 192.168.1.87
25/09/2007	13:31:34	Dev-3 EMD-3 EMD status had changed from HTTP by 192.168.1.87
25/09/2007	13:31:34	Dev-3 EMD-3 EMD display had changed from HTTP by 192.168.1.87
25/09/2007	13:44:29	Dev-1 EMD-2 EMD status had changed from HTTP by 192.168.1.87
25/09/2007	13:44:29	Dev-1 EMD-2 EMD display had changed from HTTP by 192.168.1.87
25/09/2007	13:44:30	Dev-1 EMD-3 EMD status had changed from HTTP by 192.168.1.87
25/09/2007	13:44:30	Dev-1 EMD-3 EMD display had changed from HTTP by 192.168.1.87
25/09/2007	13:44:48	Dev-3 EMD-1 EMD status had changed from HTTP by 192.168.1.87

Figure 3-32 interSeptor Pro events log data

3.5.5 Clear & Save

To save the interSeptor Pro log data to a file in Microsoft Excel format, click the links under the **Save Log Data** section. You can also clear the log data in this page.

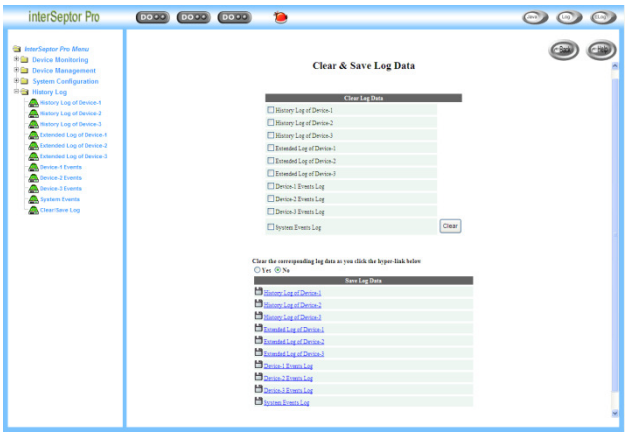


Figure 3-33 Clear and save log data page

4 Monitoring interSeptor Pro via Java Monitor

The interSeptor Pro provides three real-time graphical user interfaces, **Java Monitor**, **History Log Monitor**, and **Extended History Log Monitor**, written in Java applet to give user an alternative way to monitor the sensors or output devices via a browser.

4.1 Java Monitor

Click the Java button 

in the top right-hand corner of the interSeptor Pro home page to display the Java Monitor. The Java Monitor provides a graphical view of all the principle sensor parameters for the sensor being monitored.

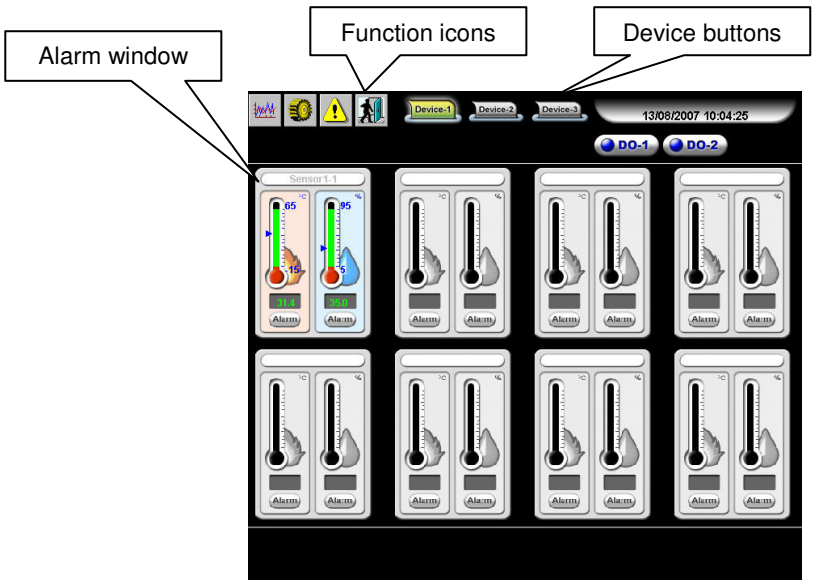


Figure 4-1 Java Monitor page

Function Icons

	**Display switch**-Two display styles (gauge or overall chart presentation) can be selected. This icon is used to switch the display of the device parameters from gauge presentation to chart presentation and vice versa.
	**Poll Rate**- Configure the time interval that the Java Monitor retrieves the value of the devices. The default setting is 5 seconds.
	**Event Message**- Enable and disable the pop-up display of the warning messages.
	**Exit**- Exit the Java Monitor.

Alarm Window

When changes are detected in the system configuration or in the status of the connected sensors, the interSeptor Pro displays a specific message in the Alarm Window. This type of status change message is an alarm.

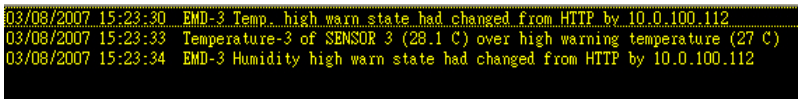


Figure 4-2 Alarm Window

4.2 History Log Monitor

Click the  button in the top right-hand corner of the interSeptor Pro home page to display the EMD History Log Monitor. The EMD history log is presented in line graph. By default, all the EMD parameters will be shown on the same graph. You can select any combination of the parameters to be displayed by checking the check box next to each parameter on the monitor screen. Click the **Refresh** button at the bottom of the page to apply the changes.

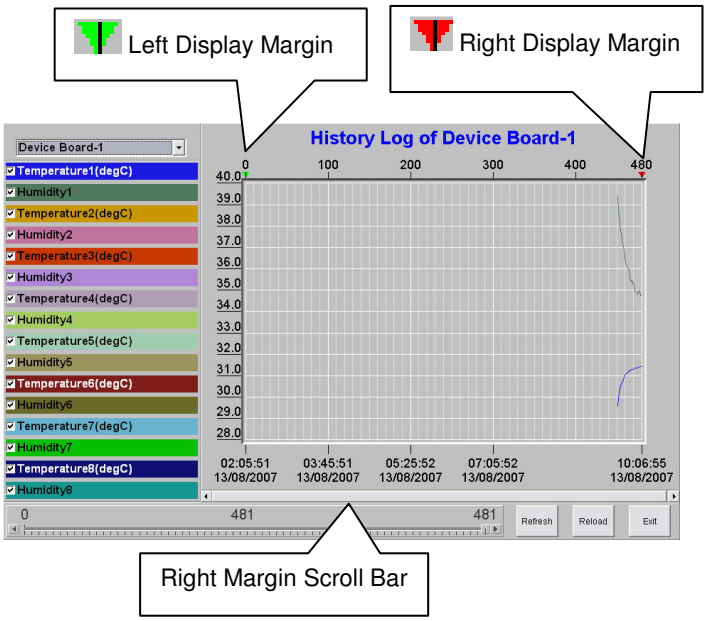


Figure 4-3 History Log Monitor page

Refresh	Click the **Refresh** button to apply the changes made to the parameters.
Reload	Update the monitor and reset the right display margin.
Exit	Close the window.

4.3 Extended History Log Monitor

Click the  button in the top right-hand corner of the interSeptor Pro home page to display the EMD Extended History Log Monitor. This monitor shows the EMD extended history log in line graph. By default, all the EMD parameters will be shown on the same graph. You can select any combination of the parameters to be displayed on the graph by checking the check box next to each parameter on the monitor screen. Click the **Refresh** button to apply the changes.

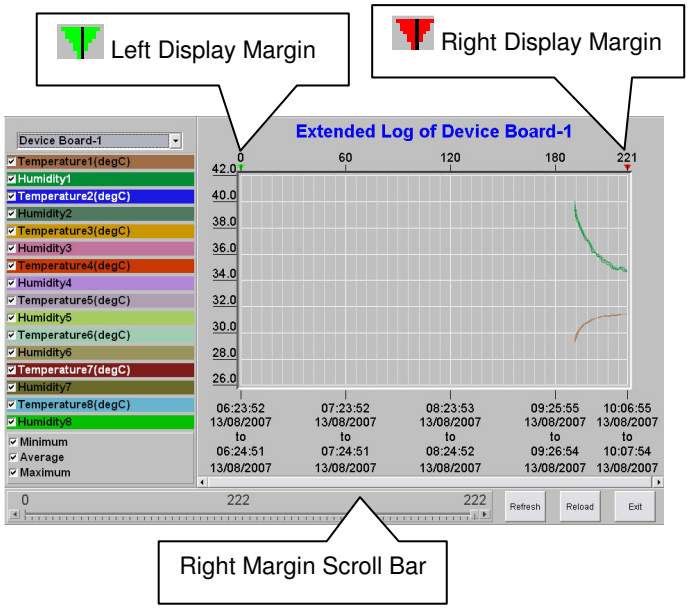


Figure 4-4 Extended History Log Monitor

Minimum	Display the minimum values of the temperature, humidity, or voltage of the EMDs, sensors, and the output devices.
Average	Display the average values of the temperature, humidity, or voltage of the EMDs, sensors, and the output devices.
Maximum	Display the maximum values of the temperature, humidity, or voltage of the EMDs, sensors, and the output devices.
Refresh	Click the **Refresh** button to apply the changes made to the parameters.
Reload	Update the monitor and reset the right display margin.
Exit	Close the window.

5 Managing the interSeptor Pro via SNMP

To manage your interSeptor Pro via SNMP, you may want to customize some of the SNMP settings (such as system name, system contact and system location).

Note: Before using the interSeptor Pro in an SNMP environment, the IP address and the gateway must be configured properly. See Chapter 6 for details.

5.1 Setting SNMP Access Control

The interSeptor Pro supports SNMP. You can use SNMP to manage the interSeptor Pro through the network. The IP address of the workstation must be entered in the interSeptor Pro write access table to prevent unauthorized users from configuring the interSeptor Pro via HTTP or SNMP.

Note: If you do not specify the IP address of the workstation in the Access Control Table (via Telnet) or the SNMP/HTTP Access Control (via web browser) in the interSeptor Pro, you can only view the interSeptor Pro status from SNMP, and will not be able to perform any configuration on the interSeptor Pro. (See Chapter6, and Chapter3, for details.)

5.2 Setting the SNMP Trap Receiver

To configure the SNMP trap receiver setting, please access the interSeptor Pro via a web browser and go to the “System/ Trap Receivers” page (see Chapter 3.4.5).

5.3 Setting up SNMP Manager Software

Follow the steps below to set up SNMP management software:

1. Add the **MIB** file in the interSeptor Pro CD-ROM to the MIB database of the SNMP manager.
2. Search for the interSeptor Pro in the network.
3. To access the interSeptor Pro SNMP agent, use ‘**public**’ for the GET community string, and use the read/ write password (default is **admin**) for the SET community string.

GET community string: **public** SET community string: **admin**

For more information, please refer to the MIB file on the interSeptor Pro CD-ROM.

6 Configuration

6.1 Configuring network settings for the interSeptor Pro

You must set an IP address, Subnet mask, and gateway via the LCD screen on the front of the interSeptor Pro to connect it to your network before you can begin using the system.

1. Press the **Set** button on the front of the interSeptor Pro so **System Config** displays on the LCD screen.
2. Press the **Set** button.
3. Press the **Down** button until **IP Address** displays on the LCD screen.
4. Press the **Set** button.
5. Enter the IP address given to you by your network administrator. Press the **Set** button to cycle the number, and the **Down** button to move to the next number.
6. Press the **Set** and **Down** buttons simultaneously to exit the setting menu once you have entered the IP address.
7. Repeat steps 1-5 above to enter the net mask and gateway (listed as **Net Mask** and **Gateway** in the system configuration menu).
8. Configure any of the other system configurations you require (see figure 2-1 LCD Screen: Operation mode menus for details), then select **Back to Idle** to complete the system setup.
9. Protect future unauthorized access to network settings by inputting a 4 digit password via the telnet menu.

6.2 Configuring interSeptor Pro via Telnet

When you have installed the interSeptor Pro via network, you can configure the interSeptor Pro via Telnet by the following steps.

1. Make sure you have a PC with the TCP/IP network installed.
2. Run command shell (i.e. Windows MS-DOS prompt).
3. By default DHCP is disabled, but if enabled the interSeptor Pro will try to acquire and IP address via DHCP on the network.
4. Type “Telnet *< interSeptor Pro IP address>*” and press **Enter**.

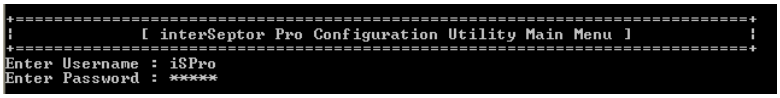


Figure 6-1 Connectivity Page

Note: If there is no DHCP network service on the network, contact your network administrator to get an IP address for your interSeptor Pro and set the IP address manually.

6.2.1 System Group Configuration

From the configuration menu, press "*1*" to select this function and set the IP address, gateway address and other group parameters. The definitions of these parameters are listed below (see Figure 6-2).

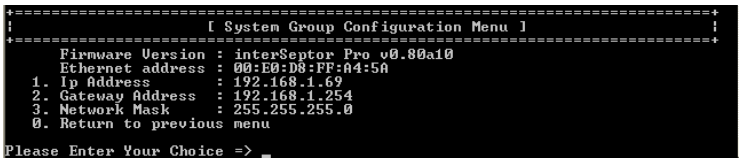


Figure 6-2: System Group Configuration Menu.

No	Function	Description	Example/Remark
1.	IP Address	The interSeptor IP address.	192.168.1.69
2.	Gateway Address	The network default gateway.	192.168.1.254
3.	Network Mask	The sub-net mask setting.	255.255.255.0

After completing these settings, press "0" to return to the configuration menu.

6.2.2 Control Group Configuration

From the configuration menu, press "2" to modify the access password and enabled/disabled status of the available network protocols (see Figure 6-3)

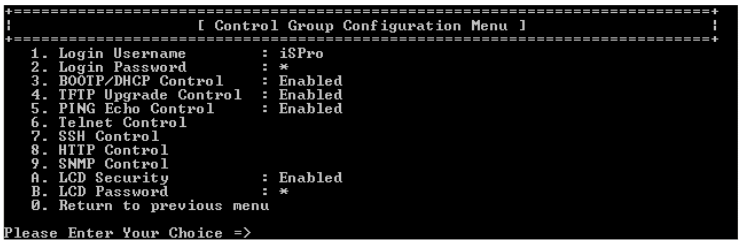


Figure 6-3: Control group Configuration menu

No.	Function	Description	Example/Remark
1.	HTTP Login Username	HTTP access login string	“iSPro”
2.	Login Password	Administrator password for read and write access	“admin”
3.	BOOTP/DHCP Control	Enable/disable the BOOTP/DHCP Protocols	Enabled
4.	TFTP Upgrade Control	Enable/disable the TFTP protocol for firmware upgrades through the local network	Enabled
5.	PING Echo Control	Enable/disable ping echo responses.	Enabled
6.	Telnet Control	Opens the telnet control settings menu.	
7.	SSH Control	Opens the SSH control settings menu.	
8.	HTTP Control	Opens the HTTP security control menu.	
9.	SNMP Control	Opens the SNMP control menu.	
A.	LCD Security	Enable or Disable LCD security. This is disabled by default.	Disable
B.	LCD Password	LCD Password for security. The default password is 0000.	0000

After completing these settings, press “0” to return to the configuration menu.

6.2.3 Telnet Control

From the control group menu, enter 6 to access the telnet configuration.

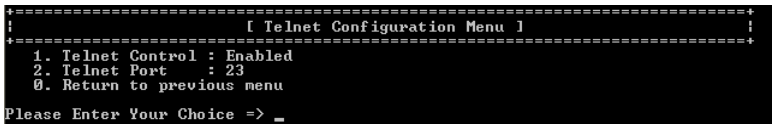


Figure 6-4 Telnet Configuration Menu

No	Function	Description	Example/Remark
1.	Telnet Control	Enable/disable the telnet connectivity.	Enable
2.	Telnet Port	Configure port for telnet connections.	23

After completing these settings, press “0” to return to the configuration menu

6.2.4 SSH Control

From the control group menu, enter 7 to access the SSH configuration.

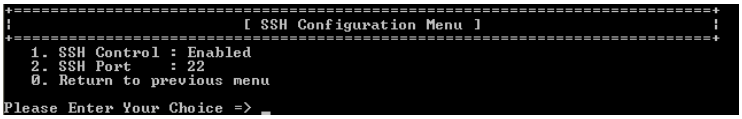


Figure 6-5 SSH Configuration Menu

NO.	Function	Description	Example
1.	SSH Control	Enable/Disable the SSH Control	Enabled
2.	SSH Port	Configuration Port for SSH connections	22

6.2.5 HTTP Control

From the control group menu, enter 8 to access the HTTP configuration

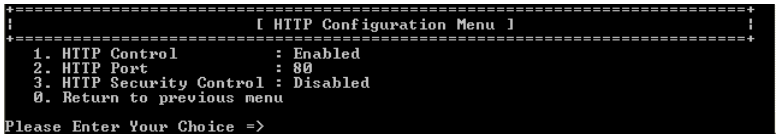


Figure 6-6 HTTP Configuration Menu

After completing these settings, press “0” to return to the configuration menu.

No	Function	Description	Example/Remark
1.	HTTP Control	Enable/disable HTTP Connectivity.	Enable
2.	HTTP Port	Configure port for HTTP Connections.	80
3.	HTTP Security Control	Enable/disable whether HTTP access is subject to access control settings.	Disable

6.2.6 SNMP Control

From the control group menu, enter 9 to access the SNMP configuration

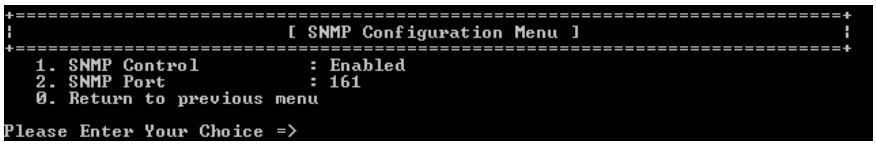


Figure 6-7 SNMP Configuration Menu

No.	Function	Description	Example/Remark
1.	SNMP Control	Enable/disable SNMP access.	Enable
2.	SNMP Port	Configure port for SNMP access.	161

After completing these settings, press “0” to return to the configuration menu.

NOTE: The SNMP port applies to the SNMP management port to be used. SNMP traps are not affected using this setting and always use UDP port 162.

6.2.7 Parameter Group Configuration

From the configuration menu press “3” to modify the SNMP identification information and the speed of reading data from interSeptor Pro (see Figure 6-8)

Figure 6-8 Parameter Configuration Menu

No	Function	Description	Example/Remark
1.	sysContact	Alphanumeric string	Technical Support Team
2.	sysName	Alphanumeric string	Multi-Port Sensor
3.	System Location	Alphanumeric string	Technical Support Lab.
4.	Poll Rate	Amount of time in seconds between sensor polls.	1

6.2.8 EMD Configuration

Use the EMD Configuration and Monitoring option to configure sensor related information to the interSeptor Pro.

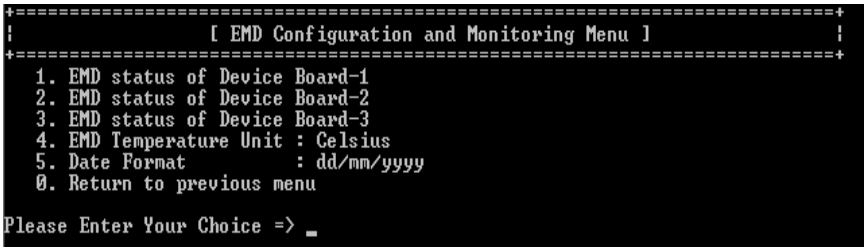


Figure 6-9 EMD Configuration and Monitoring Menu

No	Function	Description	Example/Remark
1.	EMD status of Device Board-1	Access Device Board-1 monitoring menu	
2.	EMD status of Device Board-2	Access Device Board-2 monitoring menu	
3.	EMD status of Device Board-3.	Access Device Board-3 monitoring menu	
3.	EMD Temperature Unit	Celsius / Fahrenheit	Celsius
4.	Date Format	dd/mm/yyyy or mm/dd/yyyy	dd/mm/yyyy

6.2.9 EMD of Device Board Monitoring

Shows the monitoring screen which will give the current values of the Sensors connected to that Device Board (See Figure 6-10)

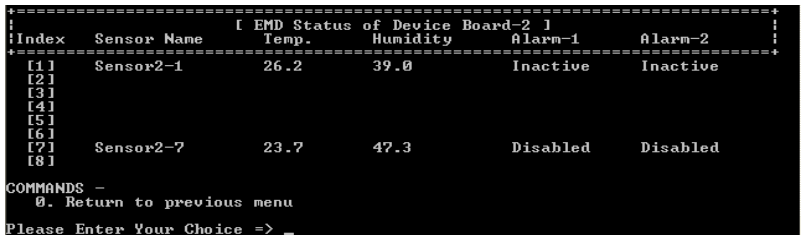


Figure 6-10 EMD Status Table

6.2.10 Digital Output control

Shows the digital output control screen this displays the current state of each output which can be changed manually using option ‘1. Modify’. (See Figure 6-11)

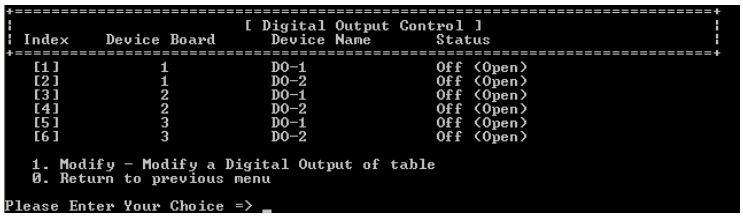


Figure 6-11 Digital Output Control Table

6.2.11 Access Control Table Configuration

If you wish to use a workstation with an SNMP manager installed, or if you wish to set more restrictive interSeptor Pro access, you can use the access table to add the IP addresses of the PC’s on which you wish to modify the access permissions (see Figure 6-12).

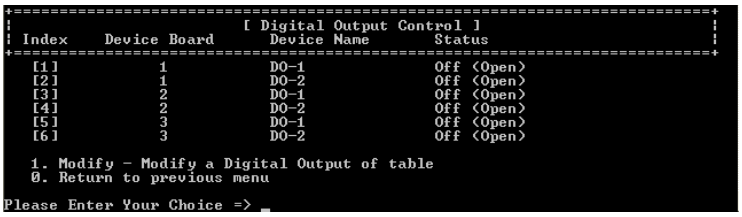


Figure 6-12 Access Control table

NOTE: The configuration of Access Control Table is configured for SNMP and HTTP Network Management. Access through TELNET is permitted only when using the “Community Read/Write” password in Control Group.

NOTE: If a “NotAccess” access right is associated with an IP address, the associated workstation will not be able to display any information regarding the interSeptor, even if the Community Read-Only string is entered.

6.2.12 Trap Receiver Configuration

If you want to send SNMP traps from the interSeptor Pro to an SNMP network management system, the IP address of the management station must be added to the interSeptor Pro list (see Figure 6-13).

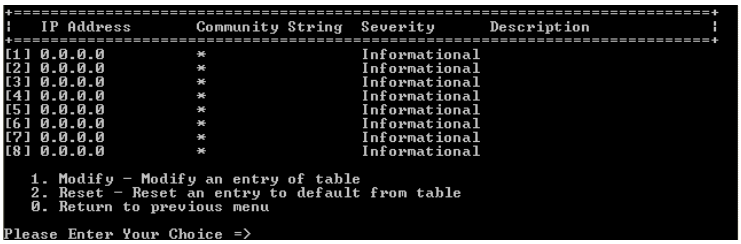


Figure 6-13 Access Control Table

6.2.13 Back to Main Menu

Press “0” to return to the main menu.

6.2.14 End of interSeptor Pro Configuration

When configuration is complete press “0” to terminate the console connection

NOTE: After completing all the settings, press “0” to terminate the connection without starting interSeptor Pro again or “6” to terminate the connection forcing the interSeptor Pro internal program to start again. At this point, the initial interSeptor Pro configuration is complete.

NOTE: If you want to restore the default interSeptor Pro configuration data set in the factory, press “5”: Reset Configuration to Default.

Appendix A. Technical Information

A1 DIP Switch Definition

Figure A-1 DIP switch

SW1	SW2	Function Mode
ON	ON	Manufacture Diagnostic Mode
ON	OFF	Reserved
OFF	ON	Reserved
OFF	OFF	Operating Mode

A2 EMD Cable Definition

The cable for EMD ports of the InterSeptor Pro (straight-through CAT5 network cable).

RJ45	RJ45	Color
1	1	White/ Orange
2	2	Orange
3	3	White/ Green
4	4	Blue
5	5	White/ Blue
6	6	Green
7	7	White/ Brown
8	8	Brown

Note: The maximum length of the cable is 20m/ 65.6ft.

Appendix B. Firmware Upgrade

B1 General Information

To perform firmware upgrade, the InterSeptor Pro must be connected to the same network as the workstation from which the file is to be sent. You must have administrator status and have the read/ write authority for the interSeptor Pro.

B2 Updating interSeptor Pro firmware via Upgrade.exe

1. Open the **upgrade.exe** from the upgrade folder on the CD provided with the interSeptor Pro pack.
2. Click the **Discover** button to discover the interSeptor pro installed on the network.

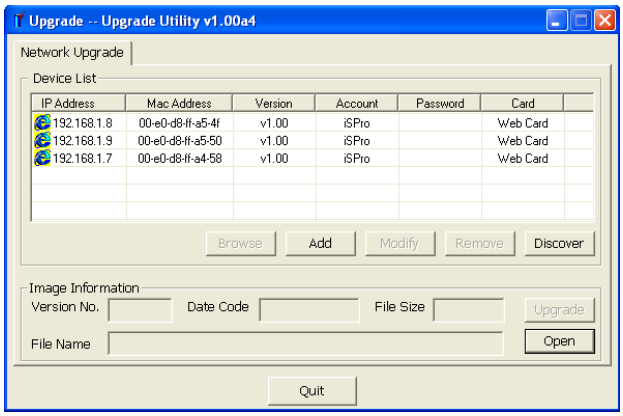


Figure B-1 upgrade.exe page

3. Click the **open** button and select the firmware to be upgraded.

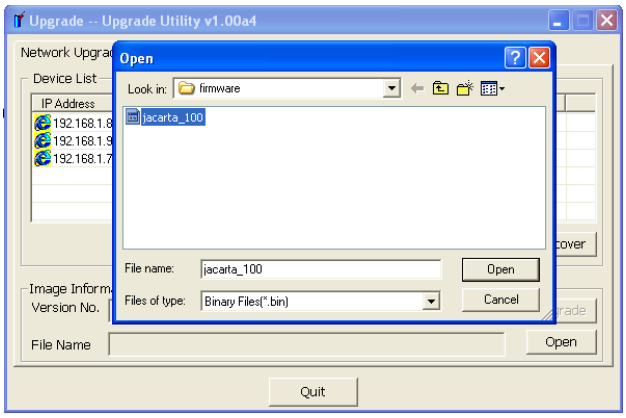


Figure B-2 upgrade.exe open page

4. Select the interSeptor Pro from the **Device List** and then click the **modify** button enter the **User name** and **Password** of the interSeptor Pro to be upgraded.

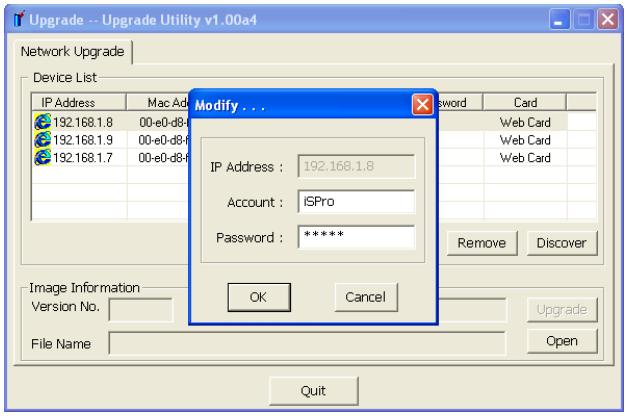


Figure B-3 upgrade.exe modify page

5. Then click the **upgrade** button, click **ok** at the end of the upgrade process.

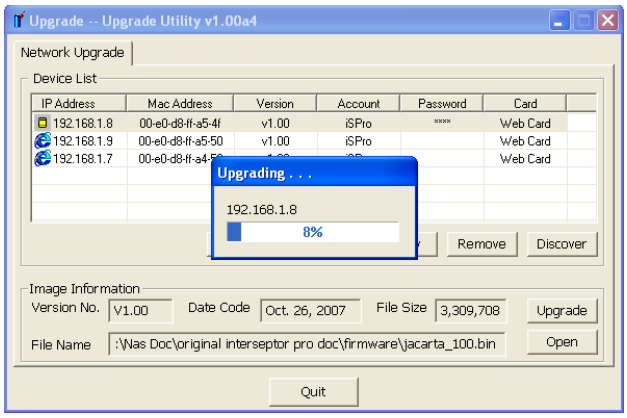


Figure B-4 upgrade.exe progress bar page

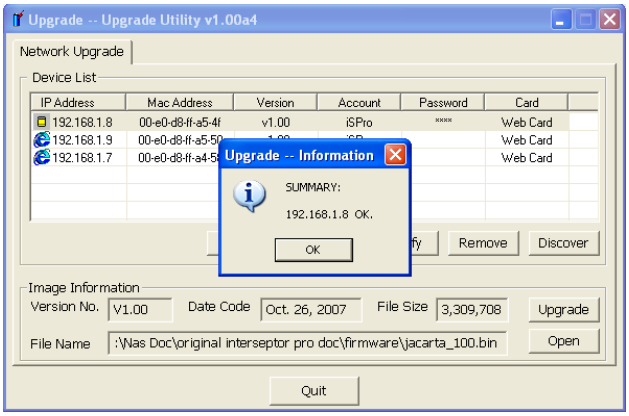


Figure B-5 upgrade.exe Summary page

Appendix C. Changing Baud rate for GSM modem

Most of the external GSM modems should auto detect the baud rate to use. If not please follow these steps:

- Connect your external GSM modem to a PC through the serial cable.
- Access the external GSM modem via HyperTerminal on your PC (instructions will come with the modem).
- Set the desired baud rate with the following command:

  at + ipr = 38400 (press enter)

- Then reconnect HyperTerminal using the new baud rate.
- Now make the changes permanent with the following command.

  at&w (press enter)

You should now be able to send SMS messages from your interSeptor Pro using your external GSM modem.

If you require any assistance please contact support@jacarta.co.uk.

Jacarta Ltd

Wagon Yard, London Road

Marlborough, Wiltshire

SN8 1LH

United Kingdom

Tel: +44(0)1672 511125

www.jacarta.co.uk