www.AKCP.com

SecurityProbe 5E (SVA)
User Manual

Help Version updated till firmware 404u

Copyright © 2013, AKCess Pro Co., Ltd..

1) Introduction

1. What is securityProbe 5E Standard with Video?
2. How to use this manual
3. Package Contents
4. Front and Rear Panels

2) Installation

1. Setting the IP address
2. Testing the IP address
3. Firmware upgrade and creating a backup configuration
4. Multi User Groups and Management
5. Services and Security
6. Setting up a sensor
    - i) Notification thresholds
    - ii) Advanced sensor settings
7. Expansion Ports

3) Notifications

1. Adding a notification
2. SNMP trap
3. E Mail
4. SMS notification

4) Camera

1. Basic Setup
2. Pan / tilt functions
3. Automating camera movements
4. Recording from camera
5. Picture log

5) Mapping

1. Adding a map
2. Monitoring via map interface

6) Filters

1. Sensor filters

2. Syslog filters

7) Making my unit visible to the internet

8) FAQ and Troubleshooting

1) Introduction

What is securityProbe 5E Standard with Video?

The securityProbe 5E Standard with Video integrates over 10 years of environmental monitoring experience with the latest technology to push the boundaries of disaster protection. Now you can sense and see problems before they lead to business disruptions.

The SEC 5E is a high speed, accurate, intelligent monitoring device, featuring a completely embedded host and Linux Operating System. The design is based on our successful securityProbe 5ES, but with the camera inputs.

How to use this manual

This manual is meant to provide the user with a step by step guide on how to configure and set up their unit. It utilizes screen shots in an effort to make things simpler for the user to follow. It is split up into sections that form “mini tutorials”. These cover the basic set up and common configurations of the unit, and give an introduction to its most useful features.

At the end of the manual there is a FAQ section that provides some further in-depth information regarding specific set ups and answers some commonly asked questions. If you need any further information or help with using your unit then please contact us on support@akcp.com and one of our technical support staff will be only to pleased to help you with any information you require.

Package Contents

Your Securityprobe-5E package contains the following items:-

- 1x Product CD
- 1x 5ft Crossover cable
- 1x THS00 with 5 ft straight cable
- 1x 7.0 – 9 V, 2.5 A power supply
- 2x Brackets for rack mounting
- 1x Blue quick-start guide.

Front and rear panels

Fig 1. Front panel

The front panel has several LEDs which display the units status and notify you as to its activity.

1. **Power LED**

   When the unit is powered up the power LED will be lit continuously. If the power LED is flashing then it indicates a problem with the CPU. If you notice this then please contact us on support@akcp.com

2. **Ethernet LED**

   The ***Activity*** and ***Link*** LEDs indicate network connectivity and activity. The Link LED will light up when there is a network connection present. The activity LED will flash when there is network traffic being sent or received by the unit.

3. **Status / Online LEDs**

   These are numbered 1 – 8. They are used to indicate the connectivity status of the sensors connected to each port. These LEDs also can be used to indicate system status when undertaking various operations.

   A. The LEDs will indicate the progress of an upgrade. The red LEDs will move from left to right to indicate activity, and the green LEDs will indicate overall progress of the upgrade. When all the red lights are off and all green are on the upgrade / recovery process is complete.

   B. These lights will indicate if the unit is operating in safe mode. This is when the unit loads the Operating System (OS) with a minimal set of drivers. If your device enters safe mode after rebooting then please contact us on support@akcp.com

   C. The unit may enter recovery mode if a firmware upgrade has been incomplete. This will be indicated by the unit displaying a continuously lit row of red LEDs. If this happens please contact us on support@akcp.com

4. **Mic**

   The mic is a small hole for access to the internal microphone. This can be used as a sound sensor (or an external mic can be used)

5. **Removable SD slot**

   This slot is provided so you are able to add your own SD flash card to increase the storage space on the unit. You can install up to a 16GB SD card.

The on board memory on the SEC 5E is 128MB. This is where the operating system, sensor data, the unit's settings, picture and sound logs are all stored.

If the picture and sound logs become full they will then begin to be stored on your SD card (if one is installed on the unit) automatically.

6. Expansion Ports

There are two expansion ports numbered from E1 and E2. These are expansion Ports for connecting either the 8-sensor8 or the E-opto16 expansion units. These are also used for connecting the CCU or Cabinet Control Units. Please see each of these separate user manuals for each of these products.

Fig 2. Rear panel.

The rear panel of the unit is home to various ports and connections. The functions of these are as follows :-

1. **Safe Mode button.** ***(DOES NOT RESET THE UNIT)***

   The black tact switch button is used to perform the following functions

   A. A single press will announce the IP address of the unit. This is audible through the internal speaker. It also broadcasts the IP address to the IPset program.

   B. Turns off password checking when accessing the web based interface (hold down for 12 seconds)

   C. To reboot the unit into the firmware upgrade or "SAFE" mode press and hold in the button for more than 12 seconds.

2. **Sensor ports**

   There are 8 RJ45 ports numbered from 1 – 8. These are for connecting AKCP intelligent sensors to the unit.

3. **USB port**

   The unit is equipped with one USB 1.1 port. This can be used, for example, to connect a USB GPRS/GSM compatible modem, a USB WiFi dongle or USB Bluetooth dongle.

4. **Mic Out**

   This is used to connect an external microphone for voice modem applications.

5. Audio in / out

The in is used to connect an external microphone, the output for external speakers.

6. RS485 Port

Used for Modbus connectivity. We support Modbus master or slave.

7. Power Connector

This is a 7.5V DC plug. We recommend you using a 7.0 – 9 V, 2.5 A power supply.

8. Ethernet Port

This RJ45 port is used to connect your unit to the network.

9. External ground (Must Be Used)

The EXT. GND must be used to external ground the unit.

10. BNC Camera Inputs

The 4 BNC camera ports are where the cameras are connected.

11. High Definition Digital Pan Tilt Dome Controller Inputs

This is where you would connect each of the PTDC pan tilt controller cable inputs.

2) Installation

1. Setting up the IP address

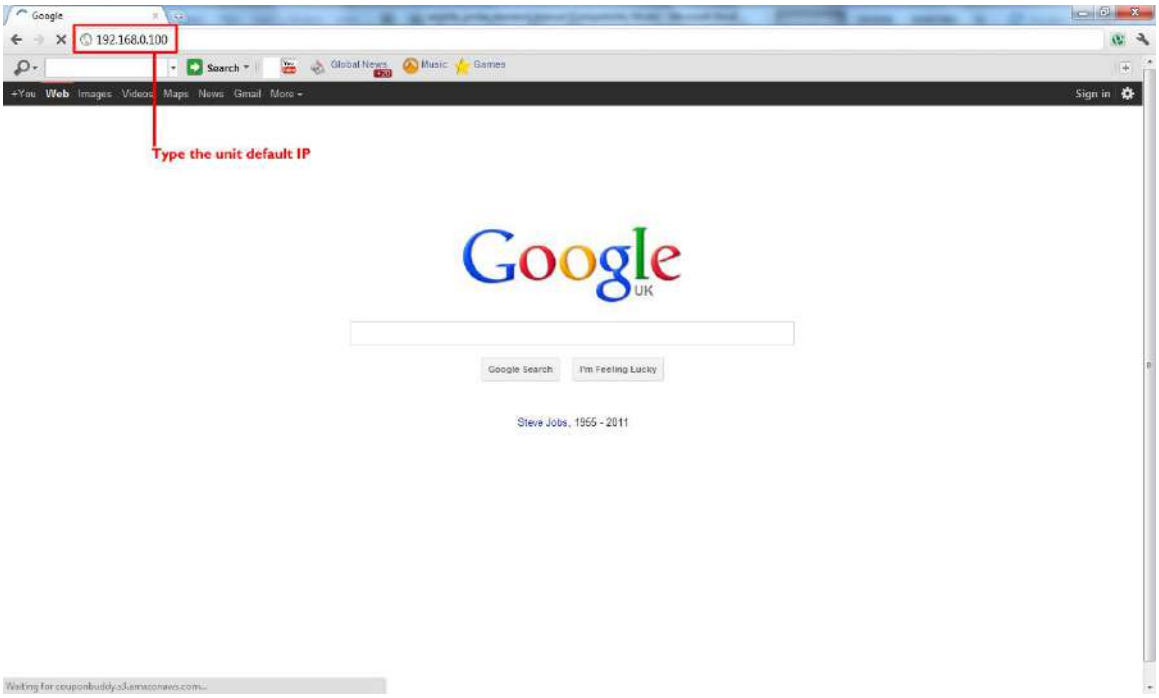
Every unit is shipped with the default IP address of **192.168.0.100** First we will go through the process of changing this IP address to fit your own network configuration.

Ensure the following items are available to you before starting:-

1. RJ45 CAT5 crossover cable with RJ45 male connection
2. A PC with Ethernet card or LAN socket.
3. Power socket for the unit to connect to

a) Connect the unit via the Ethernet port of the unit to your computers LAN or Ethernet port with a CAT5 crossover cable.

b) Open a web browser and type the default IP address, hit enter.



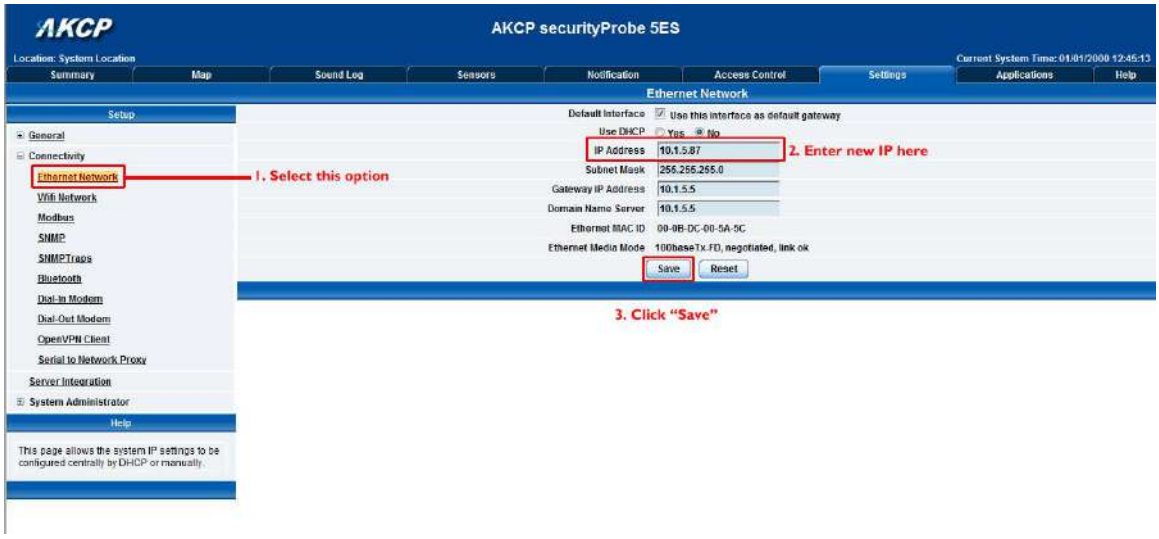
In some cases your computer might not be able to connect to this default IP address. In this situation you need to set up your computers routing table to allow access to this. See the appendix on how to setup this.

c) You will now be presented with the following screen. The default password for Admin is “public”. To make your unit secure and change the password.

d) Next the home page will be displayed. It will look similar to this.

e) Click on “Ethernet network” from the list on the left frame of the page.

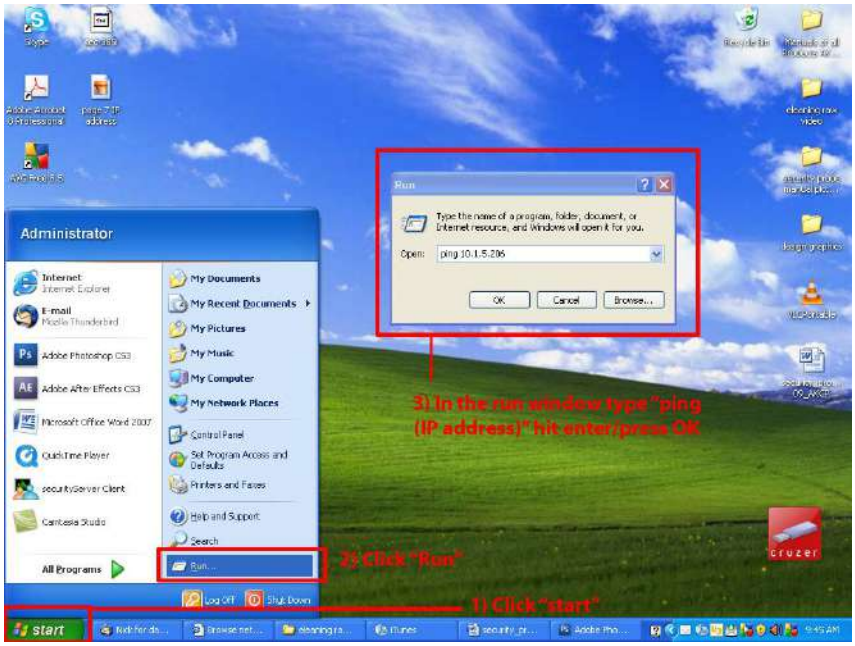
Please Note: Even though the screen shots included in this manual will display AKCP securityProbe 5ES, there are no differences between the securityProbe 5ES and the securityProbe 5E’s web interface as they are shown. If or when there are differences, these will be pointed out.



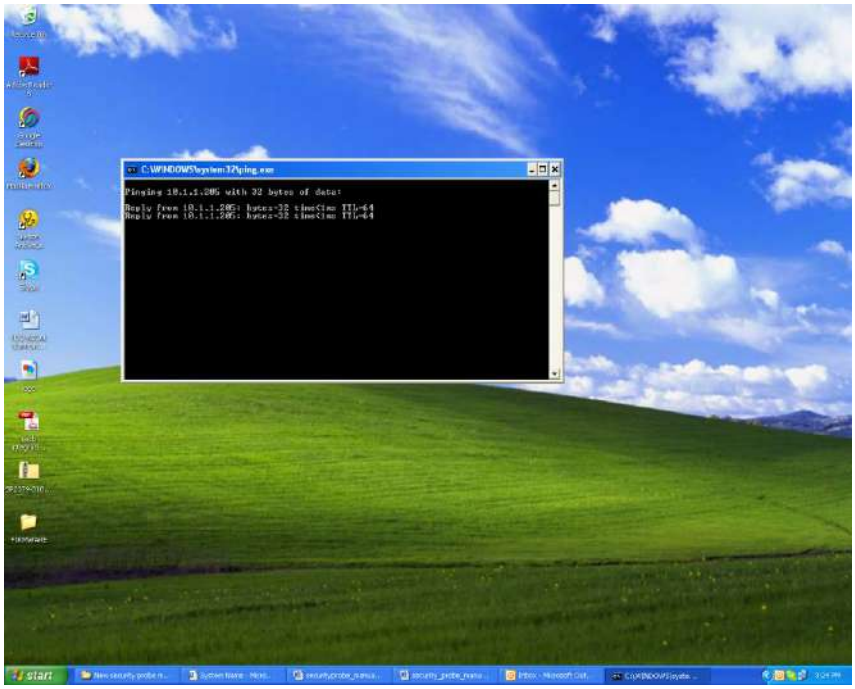
Note. The unit ships with DHCP disabled. If you wish to use a DHCP server to obtain the IP address then see the "Using DHCP" section of the FAQ>

2. Testing the new IP address with the “ping” command

Once you have assigned the new IP address use the “ping” command to test the unit. This can also be used as a diagnostic tool in order to check whether your unit is connected to the network.



After hitting “enter” you will get an MS DOS prompt window that will show the ping results (as below). If unsuccessful you will get a message saying “request timed out”. This indicates either an incorrect IP address or a unit that is not connected to the network.



3. Firmware upgrade

Ensure you are running the latest firmware. You will also need to download the latest firmware from our website (http://www.akcp.com/company/firmwareupdate.htm). Log into our webpage using your MAC address, this is found on a sticker on the base of the unit. After the download navigate back to the web based interface (units IP address. This manual will refer to the DEFAULT IP address, 192.168.0.1 you need to substitute this for your own IP address if you have changed it)

Please Note: The firmware file used for the securityProbe 5E is the same file used to update the securityProbe 5ES units as it uses the same iMX25 processor.

This tutorial provides you the information needed to upgrade the firmware.

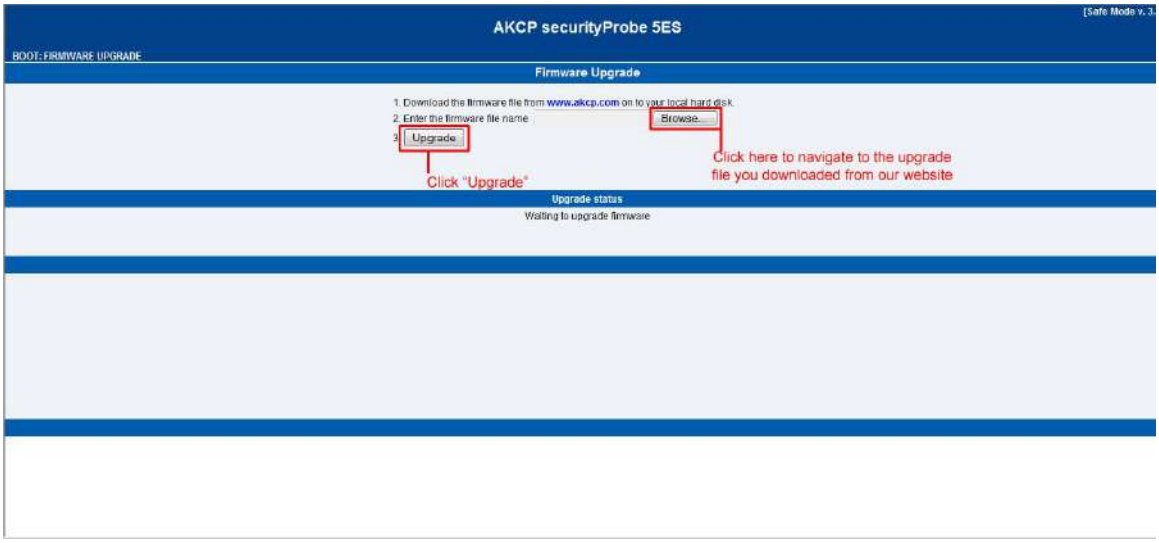
To get to the starting point of this tutorial:

- Log in as administrator
- Click on the settings tab

Go to the Settings page then >> System Administrator >> System Maintenance >> System Firmware Upgrade Click on the "Upgrade" button, this will reboot the unit into "safe" mode, or "upgrade" mode.

Click OK.. After reboot you will be redirected to the safe mode web interface. This can take some time, so please be patient. The page will display the following message while rebooting

Once the unit has rebooted you will be viewing the following page. Follow these instructions.



After clicking Next, you can browse to the firmware update file (xxxxxx.bin) and click on the "Upgrade" button on the Firmware Upgrade screen.

After clicking the Upgrade button, the unit will appear to sit and do nothing, please be patient. If you can see the "Elapsed Time" is still running and in the lower left hand corner of your browser you will see the "Sending Request" notices this means the first half of the update process is working properly.

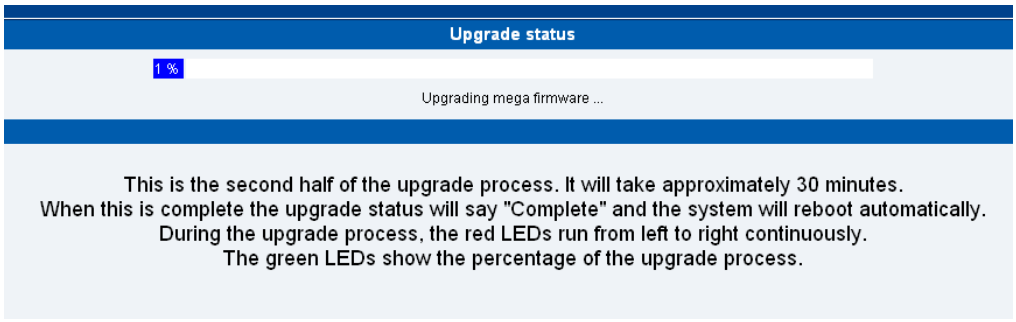
The second half of the update will begin in roughly 7 to 10 minutes. This will show the upgrade process bar and the percentage that has completed.

You will notice the RED sensor LED's on the front of the unit will be moving from left to right very quickly.

When the unit finishes updating, it will boot back to normal mode and the web interface will refresh back to normal after roughly 3 minutes.

You can check to be sure the unit has been upgraded by checking the version on the

Settings Page >> General >> System Description



The unit will then reboot. The process is complete when the LED's are back to their "normal" status.

Please Note: If the unit gets disconnected from the AC power or something else occurs during the firmware update to cause this from not being completed the unit should boot back to normal mode after leaving it powered on (NOT PUSHING THE SAFE MODE BUTTON ON THE BACK OF THE UNIT) and left alone for 30 minutes.

If the unit does not boot back to normal mode or remains with the LED's circling in a counter clockwise rotation after 30 minutes the unit is most likely stuck in safe mode.

If this is the case please **DO NOT CONTINUE TO PRESS THE SAFE MODE BUTTON ON THE BACK OF THE UNIT. This will only continue to keep the unit stuck in safe mode.**

If the unit does not boot back to normal mode after leaving powered on for 30 minutes then perform the following steps;

Firmware Update Mode Using LinuxIPSet

Note: Please always try to use the web interface when upgrading the firmware on the units, but if you are not able to access the web interface then use the LinuxIPSet.

Getting the unit unstuck or back to normal mode;

#1. Power OFF your device.

#2. Connect your securityProbe via crossover cable directly to your computer's network interface card.

#3. Reconfigure your network interface card's TCP/IP settings (IP Address: 192.168.0.2, Subnet Mask: 255.255.255.0, Default Gateway and DNS: Leave them blank)

#4. Make sure that firewall programs are temporarily turned OFF or make an exception for lnuxIPSet5.8.1.exe.

#5. Run lnuxIPSet5.8.1.exe which can be accessed from your product CD, or found within the firmware update compressed file.

#6. Click the "Firmware Upgrade" option mode in the LinuxIPSet.

#7. While pressing and holding in the reset button, power ON the unit. Remember not to let go until you see the text in the LinuxIPSet (Received a request of 'kernel-pxa.img' from 192.168.0.100).

#8. Check the Link LED. It should turn ON. Wait for the green bar to appear in the LinuxIPSet after a minute or two.

#9. Click on this bar to access the device's web interface and start uploading the new firmware to the SD card or to the unit is this is a 5ES.

Note: If your web browser displays "404 not found" or "page cannot be displayed" errors then try pasting http://192.168.0.100/index2.html directly to your browser's address bar.

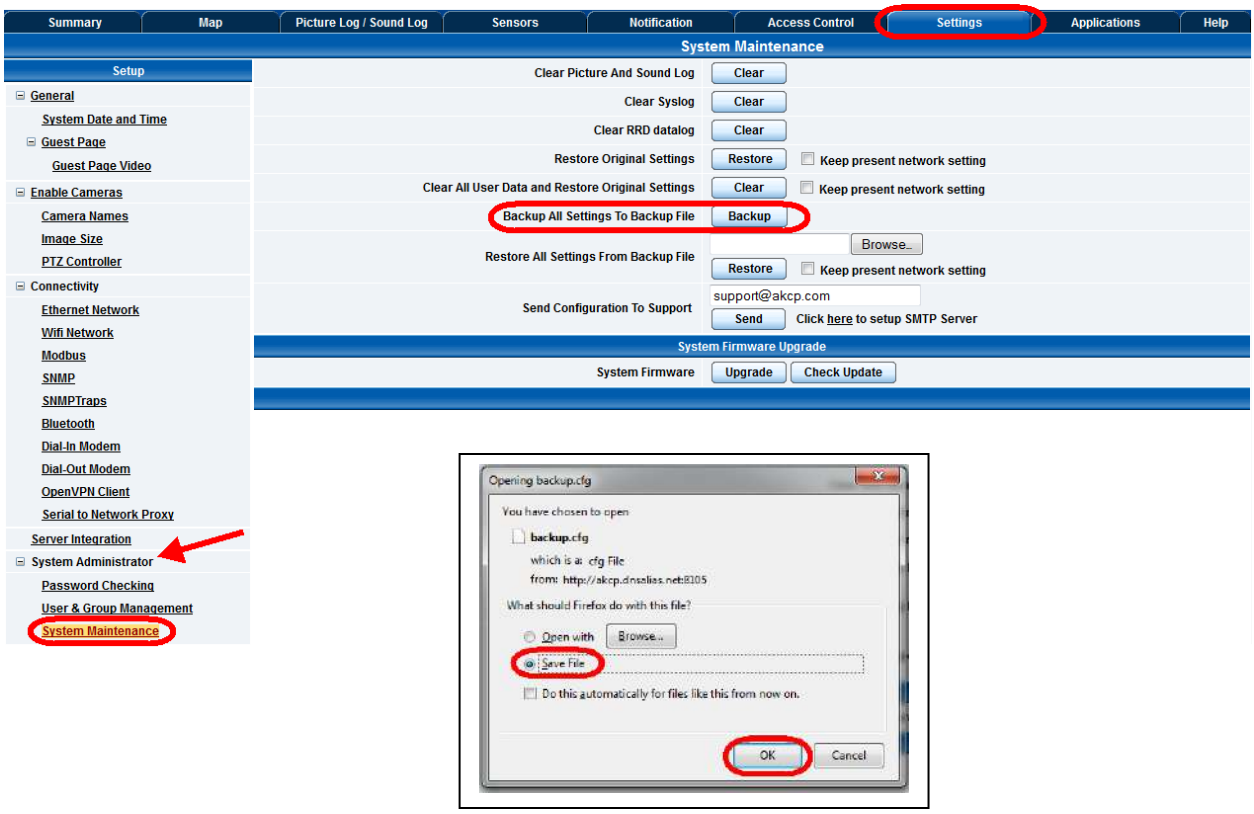
Note: If you still have a problem with the upgrade or the unit please contact AKCP support at **support@akcp.com**

Creating A Backup Configuration File

Keep in mind the after you set up your securityProbe unit and have all the settings and alerts completed you can create a backup configuration file. This file will contain the configuration of the units settings and also the sensor settings and notification alerts.

These backup configuration files can be loaded on other units as long as they are the same basic type. For example you can load a backup config file from a securityProbe 5E onto a securityProbe 5ES unit. You can also use the probeManager utility to push out the same configuration file to multiple units on your network simultaneously.

However it is not recommended to load a backup file from a securityProbe 5ES or 5E unit to a securityProbe 5ES-X20 or X60 or a 5E-X20 or X60 unit.



To create your backup config file, you first need to log in to the unit as an Administrator, then navigate to the Settings page >> System Administrator >> System Maintenance then click on the “Backup” button as shown in the screen shot above.

You will then browse to where you would like to store the backup file on the PC, making sure the Save is chosen then clicking the OK button.

You can restore this or another backup file using the Restore All Settings From Backup File.

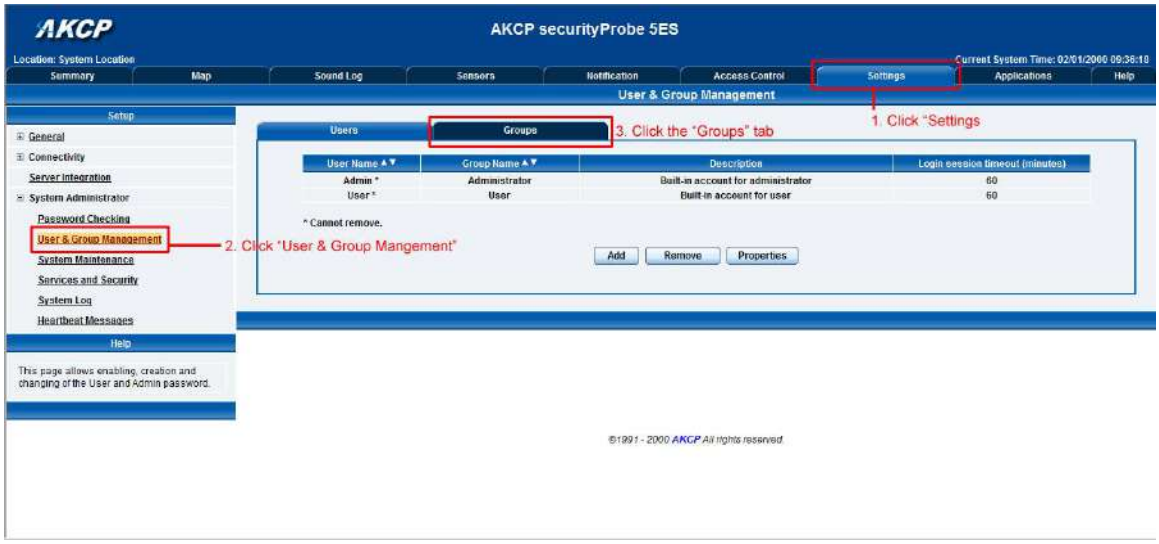
4. Multi-users and groups setup

Login to the securityProbe or securityProbe 5E with the Administrator password, the default will be “public” if you have not changed this yet.

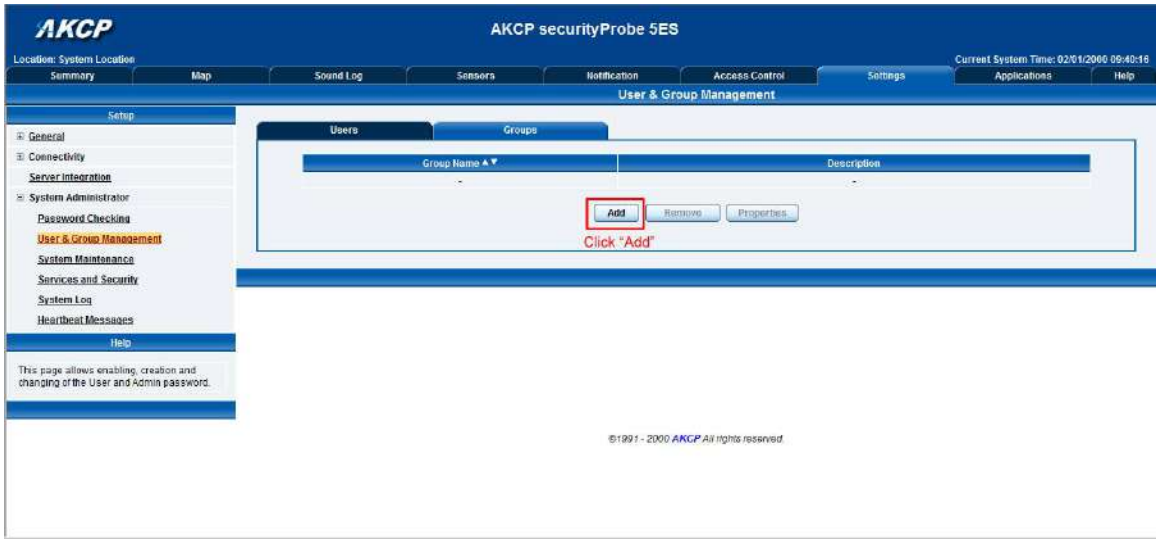
Click on the Settings page, then System Administrator then User & Group Management as shown in the screen shot below:

Note: *The following screen shots may appear small and hard to read. Please use the zoom feature in your PDF reader program to increase the size of the page to better view these screen shots.*

Group Setup



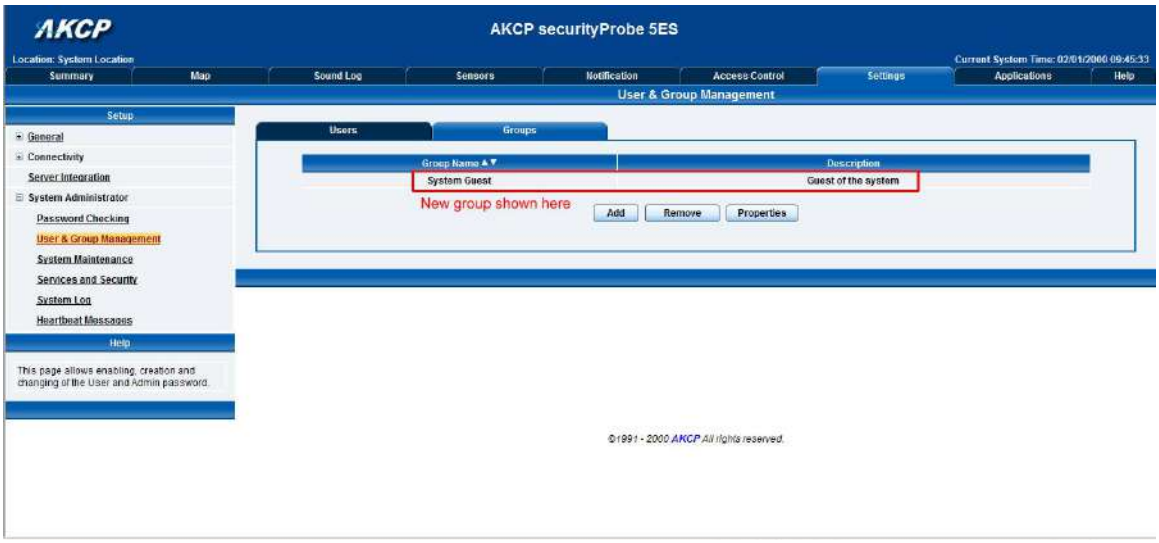
This will take you to the Groups page shown below:-



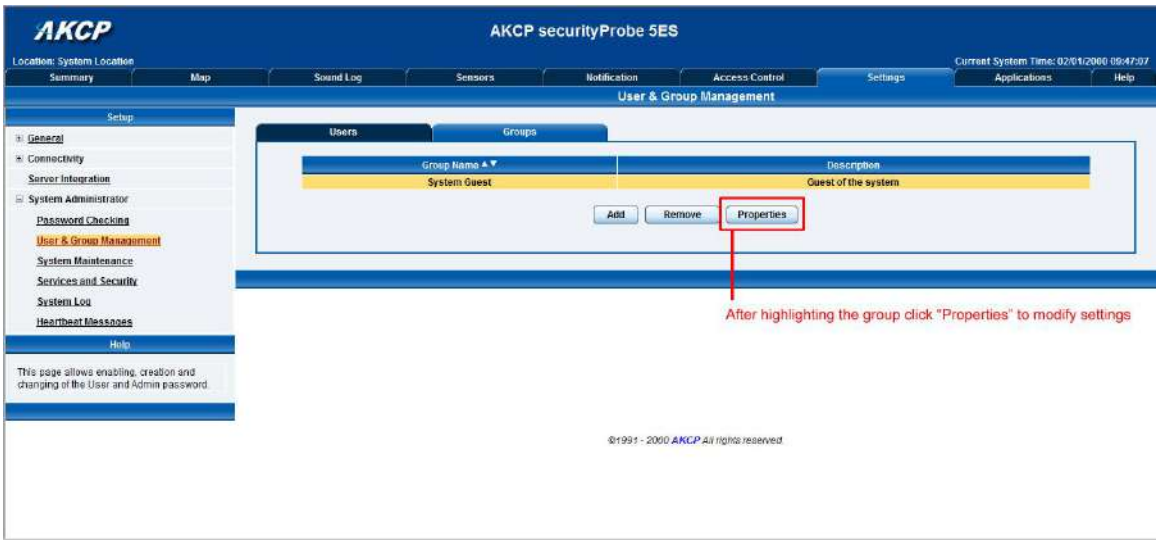
Now click on the “Add” button to add your groups as shown in the screen shot above.

Enter your group name for example we have added a group named “System Guest” and entered our description.

Now check the objects within the web interface that this group will be able to Modify and View. Then click the “Finish” button to save your group.

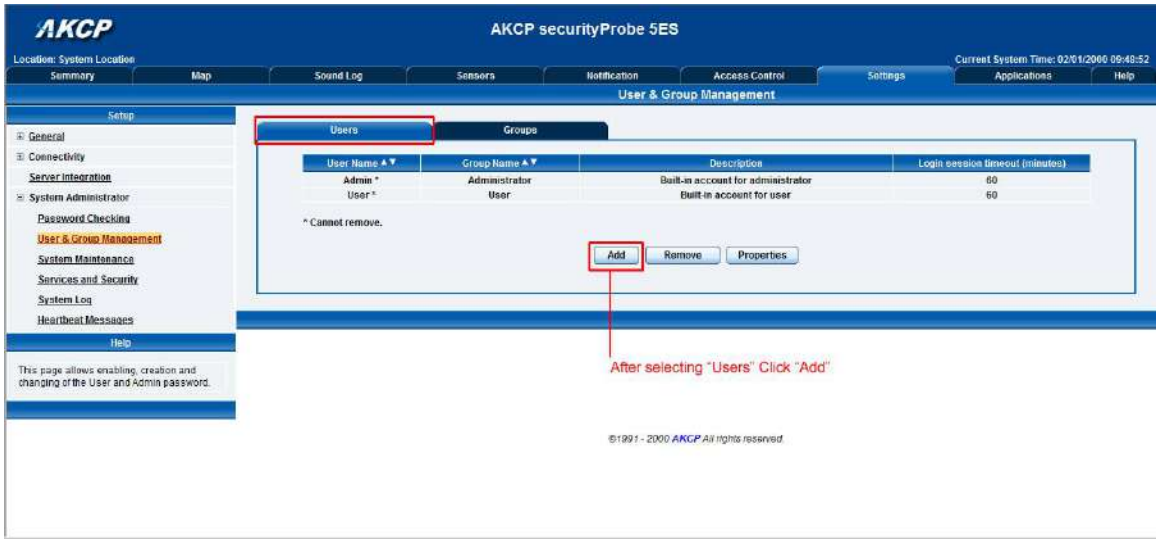


Now you can see the new group “System Guest” has been added to our group list as shown in the screen shot above.

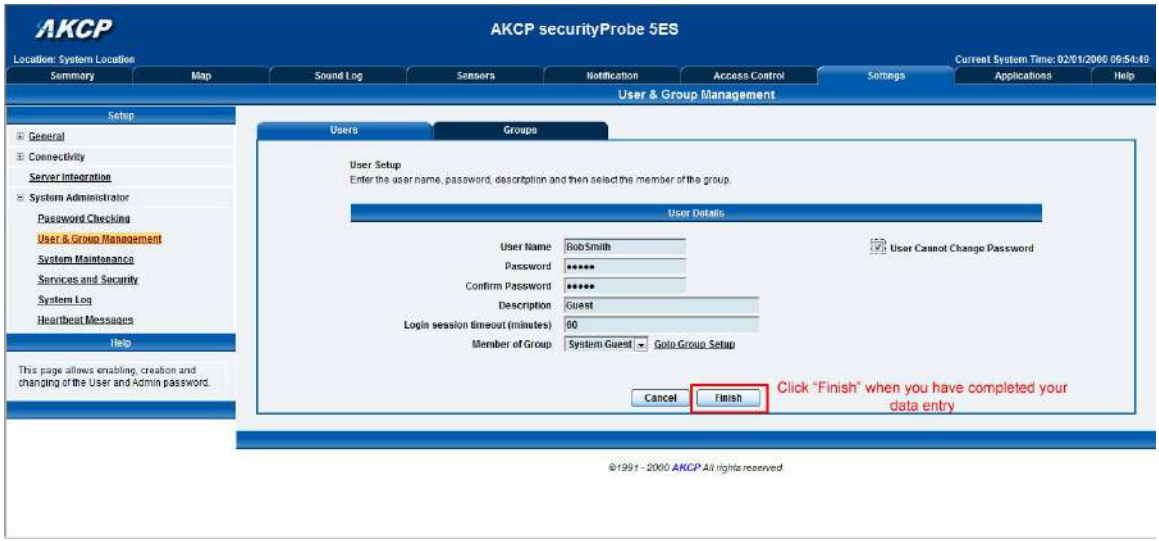


If you wish to modify your group settings, highlight the group you wish to modify by clicking on it, then click on the “Properties” button as shown in the screen shot above.

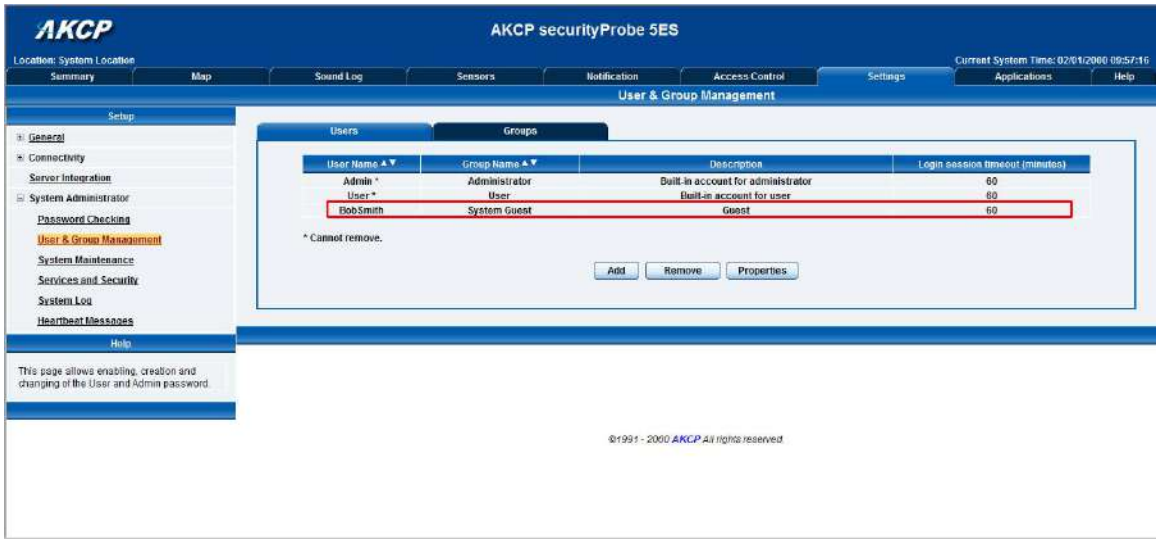
User Setup



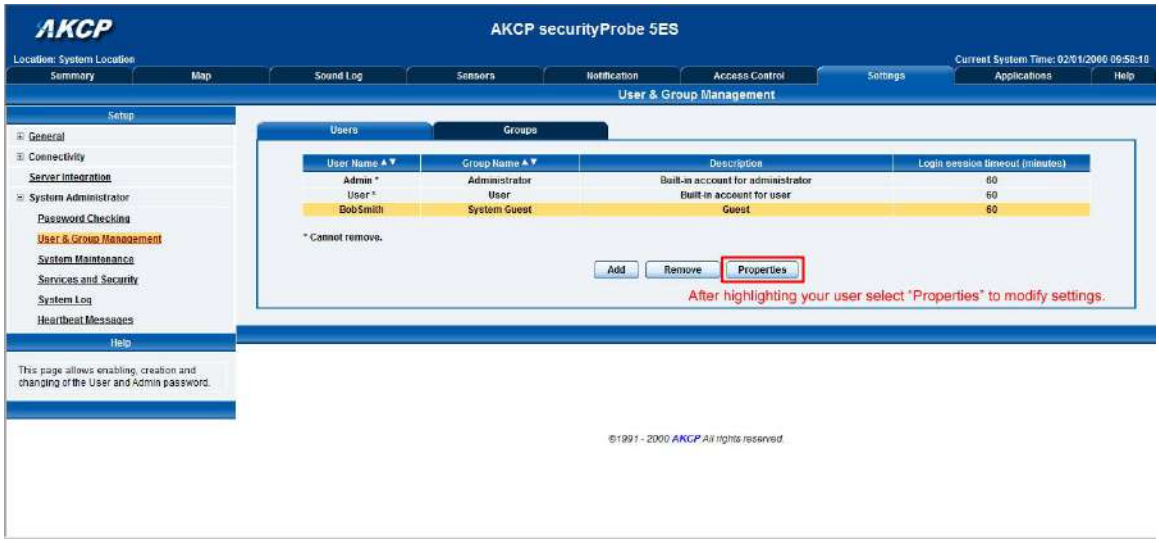
Click on the Users tab then click the “Add” button to add the new Users to your groups as shown above.



Now enter your User details as shown above. In our example we have entered Bob Smith as our Guest into our “System Guest” group. We have also added the option so that this user cannot change his login password. After addition your users for each group click the “Finish” button to save each user.



Now as you can see the new user has been entered into our list of Users.



To modify a users setting, first highlight the user by clicking on it, then click the " Properties" button as shown in the screen shot above.

5. Services and Security

Active Services Application (disabling)

You can enable or disable the Nagios, Video Conferencing, Secure Shell and Telnet applications running on the unit thus making the unit more secure as shown in the screen capture above.

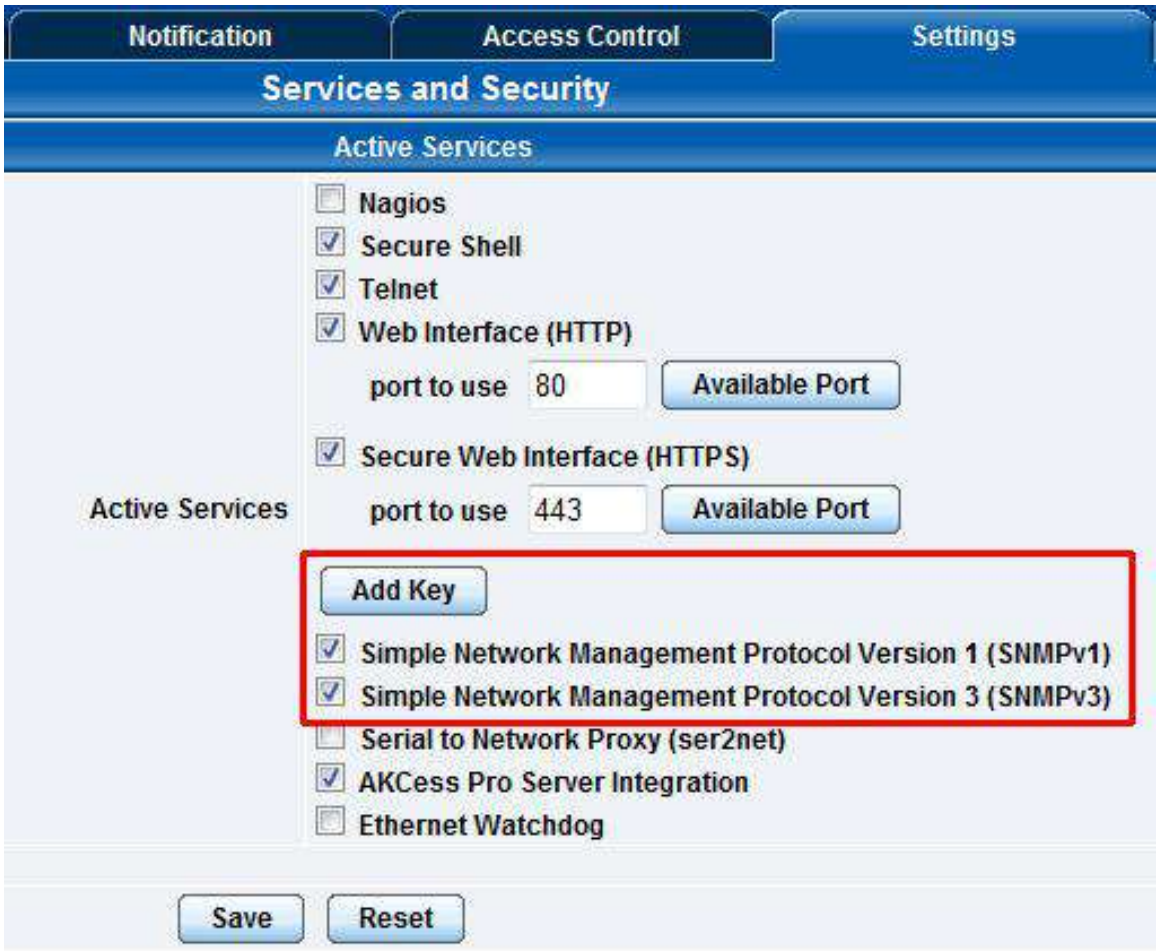
Closing or changing ports disabling HTTP and enabling HTTPS

You can also close or change the ports used to access the units web interface, disable HTTP and enable HTTPS only.

The "s" at the conclusion in HTTPS stands for secure. This SSL/TLS connection type is used primarily for high-value sites or ‘pages’, to elevate the potential of being unreadable by anyone but the end-points.

One benefit is the traffic between client and the securityProbe is not cached along the various units as it moves across the 'Net, and so can't be accessed by someone after the connection is terminated.

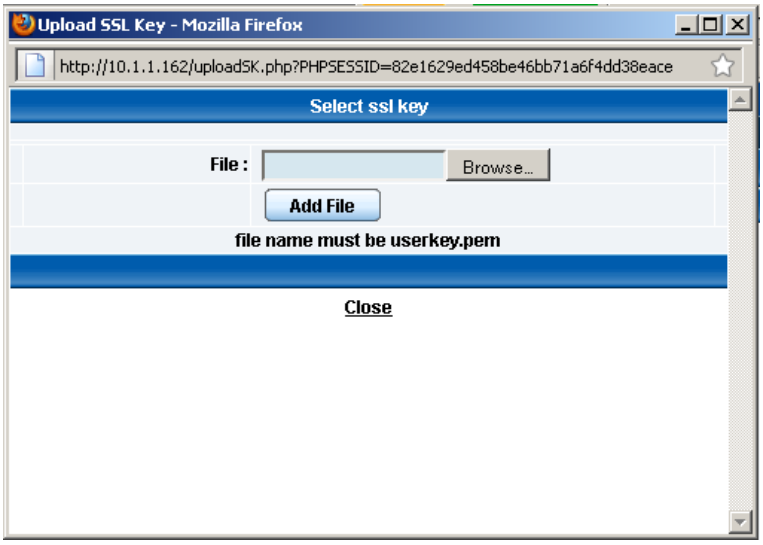
The SNMPv3 SSL security feature



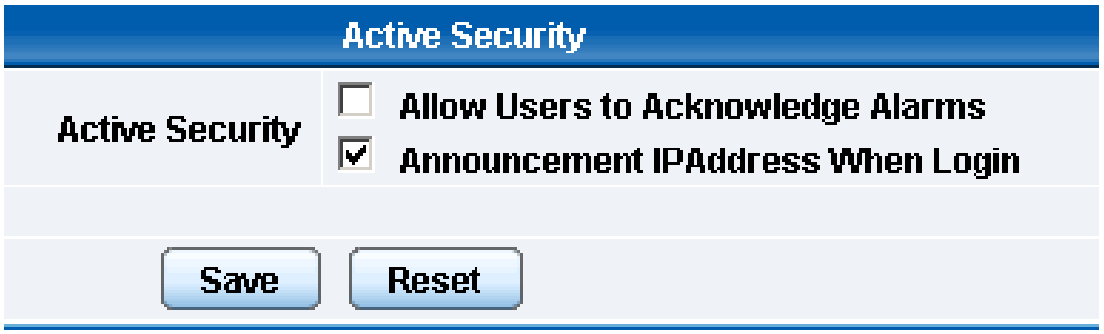
Use the SNMPv3 SSL (Secure Sockets Layer) which is the standard security technology for establishing the encrypted link between the securityProbe in our case and the web browser. This link ensures that all data passed between the securityProbe and the browser remains private and integral.

SNMPv3 provides important security features:

* Confidentiality - Encryption of packets to prevent snooping by an unauthorized source.
* Integrity - Message integrity to ensure that a packet has not been tampered with in transit.
* Authentication - to verify that the message is from a valid source.



Active Security



In the Active Security section you can allow Users who are logged into the units web interface to “Acknowledge” alarms, which is normally reserved only for the Administrator.

When the unit boots up, it will announce the IP address that it has been configured with. As an added security feature this announcement can be disabled in the above screen shot, so that the IP address remains unknown.

The NAC or Network Access Control security feature

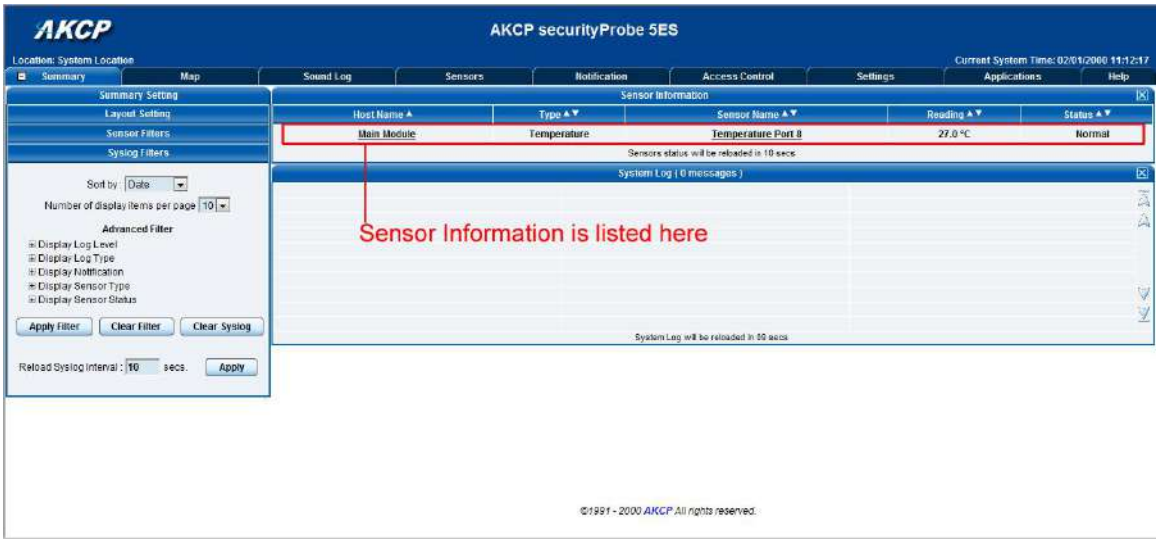
The NAC or Network Access Control feature allows you to restrict access to the web interface for only certain IP addresses, or deny access to the web interface for only certain IP addresses.

6. Setting up a sensor

In this section we will now go through the basic set up of a sensor. We will focus on the AKCP temperature sensor; however this basic set up process is applicable to all of our sensors. If you require information on specific functions of a particular sensor then please download the manual for that sensor from our website, or locate it on your product CD.

a) Plug the sensor into one of the RJ45 "intelligent sensor ports" on the rear panel of the unit. In this example we will use port 1.

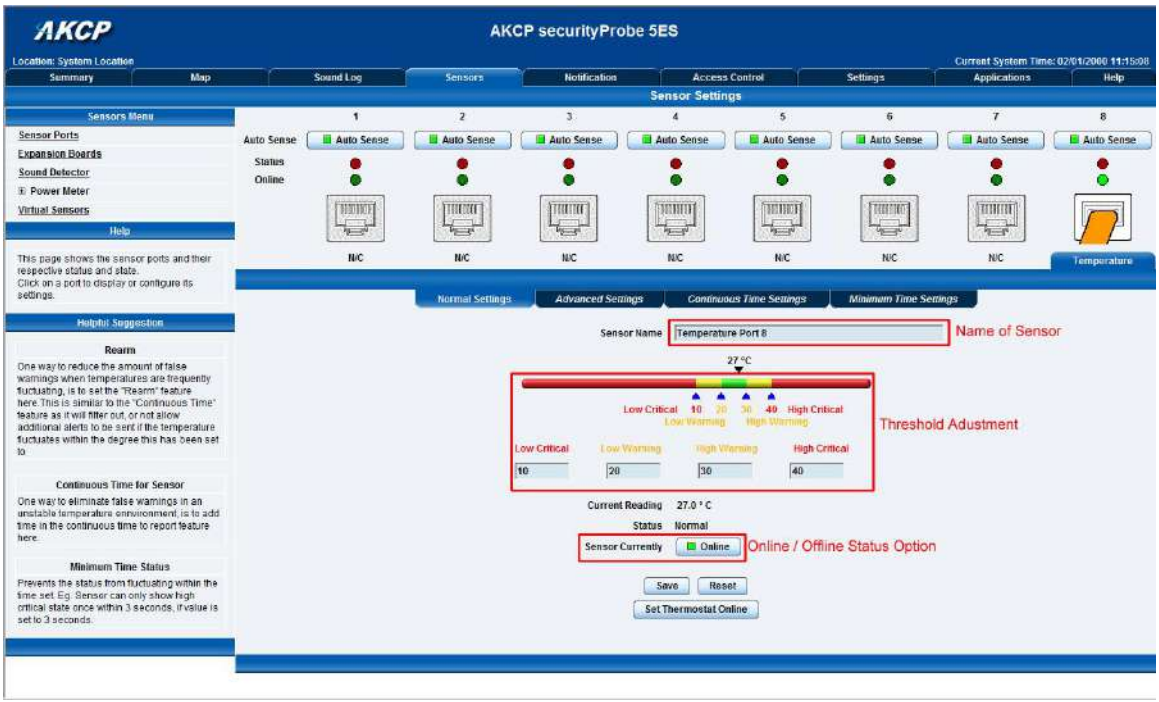
b) Now point your browser to the IP address of the unit (default, 192.168.0.100). Next you need to login as the administrator using your administrator password (default is "public"). You will then be taken to the summary page. This is shown below.



The temperature sensor should be listed, along with its current reading and status. If this is not shown please see refer to the FAQ.

This summary page allows you to quickly see which sensors are connected, their status, view the system log, and also view footage from any connected cameras. We will now go through some of the tools the web based interface provides for getting feedback from the sensors.

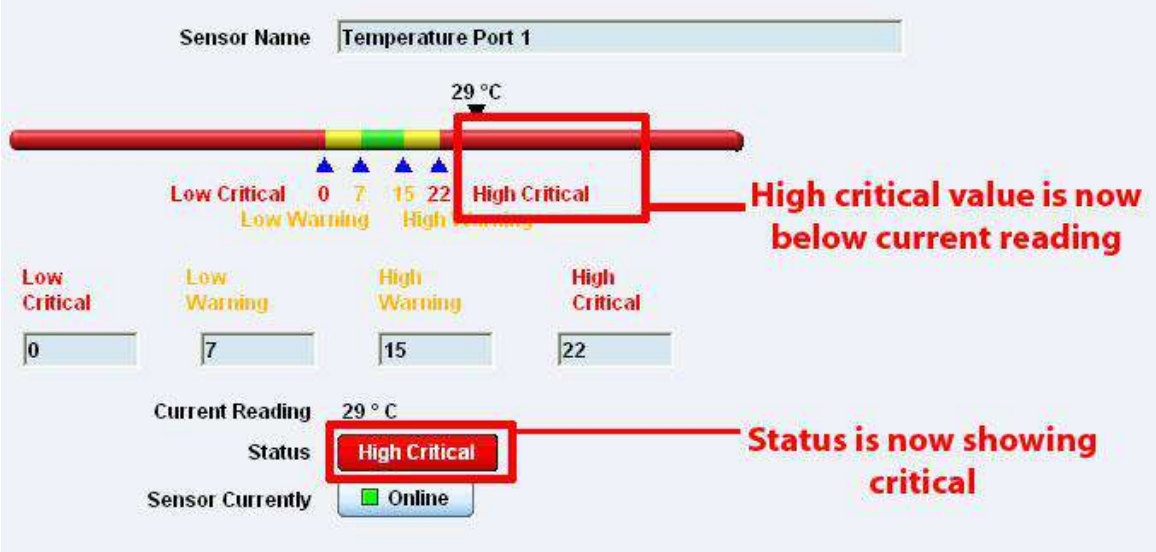
c) Now click on the temperature sensors name (indicated in previous screen shot). This will bring you to the following page, the sensors page:-



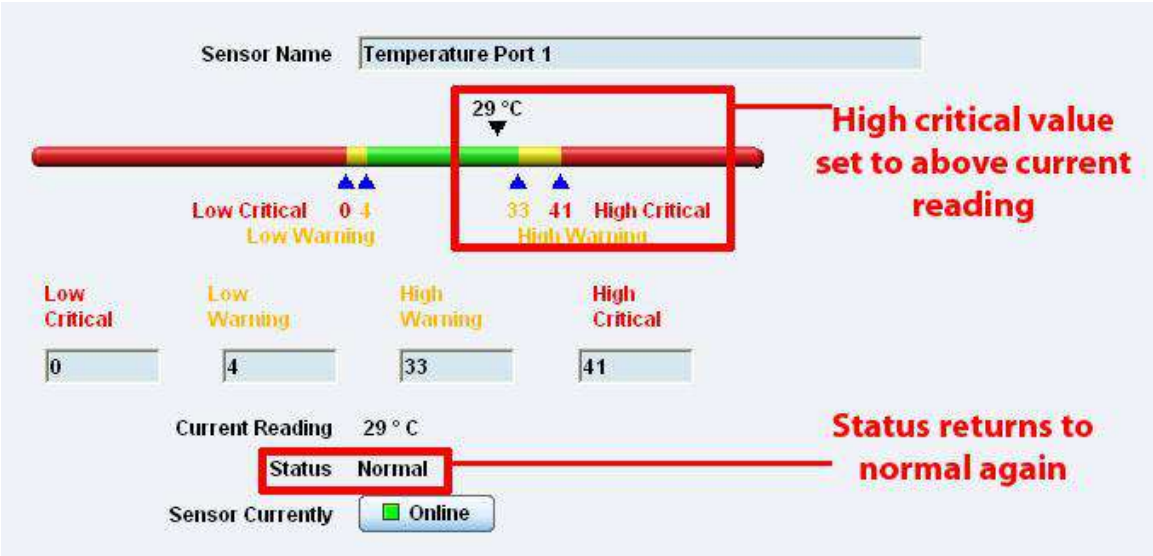
Note: another way of accessing this page is to click on the "sensors" tab at the top of the page.

I) Notification thresholds

From this page you can carry out various operations as indicated above. Also view the current status (normal, low critical, high critical etc). In the screen shot above you can see the sensor is indicating a temperature of 29 degrees F, and a status of Normal. If you click on the blue marker arrow indicated above by the “Set the required threshold” label you can drag this marker to re-configure the thresholds. After dragging the marker click “save” In the next screen shot you can see that this marker has been moved to make a new threshold, and along with it the sensor status has changed.



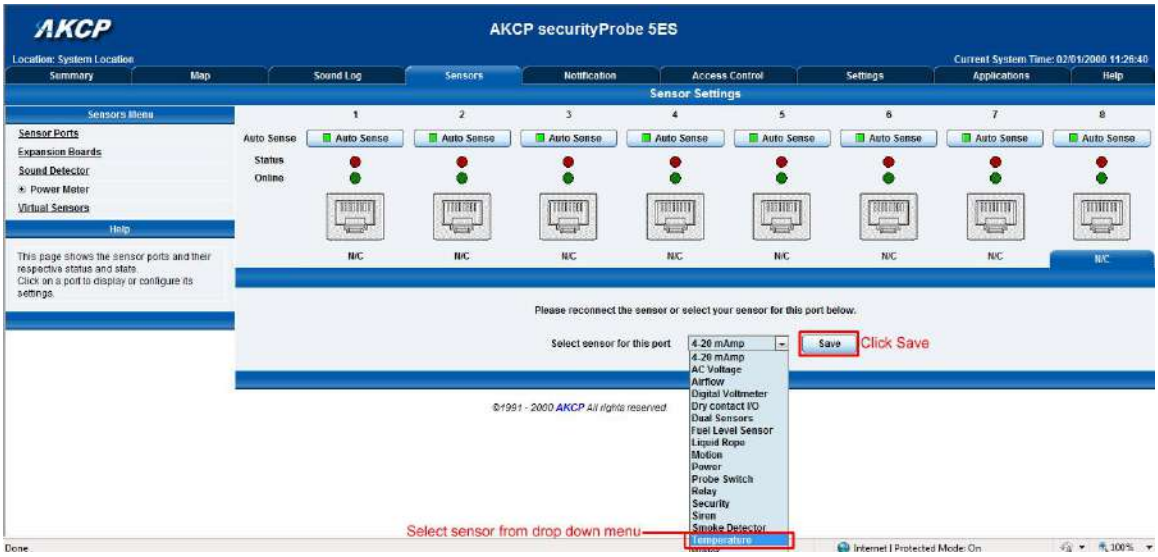
If the marker is then dragged back to above the current reading temperature you should see the status returns to a normal condition again. *Note: If this does not happen straight away press your browsers refresh button.*



If you wish to take a sensor offline then click on the “sensor currently” button. This will offline the sensor without the need for you to physically unplug it.

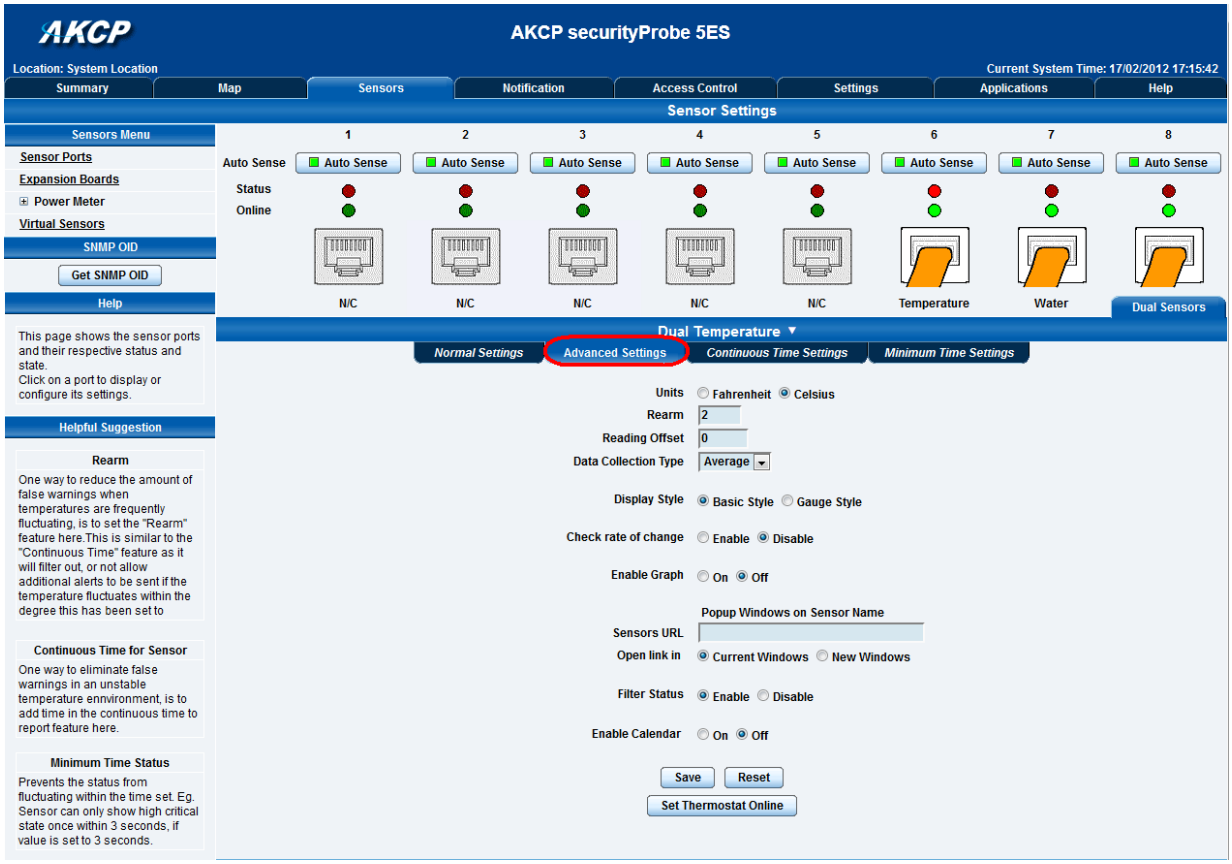
Now your page will look something like below after taking the sensor offline.

To bring a sensor back online, select your sensor type from the drop down menu and click “save”.

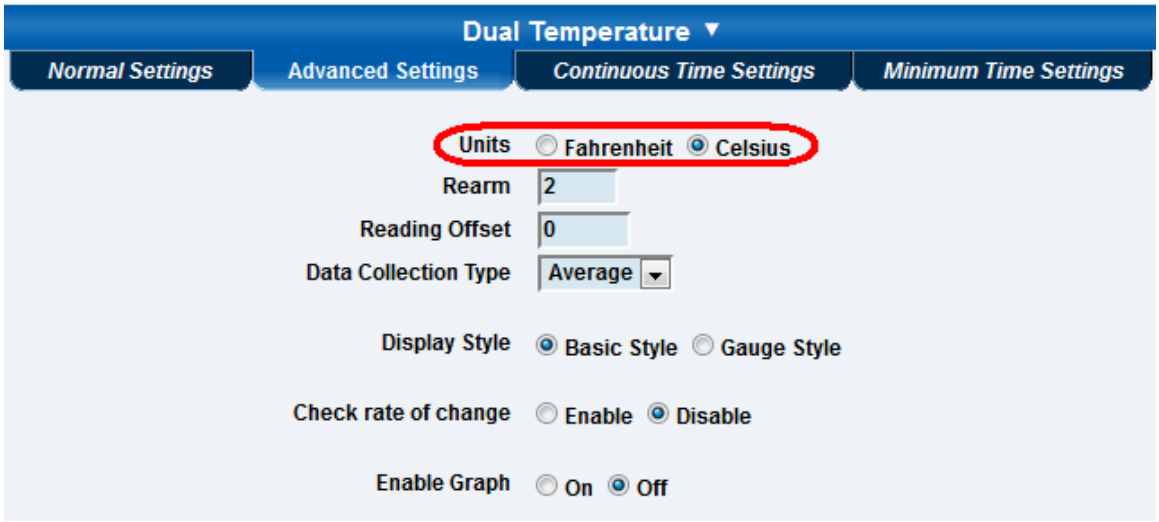


Advanced sensor settings

By clicking on the Advanced Settings tab you will then see the advanced settings for the sensor.

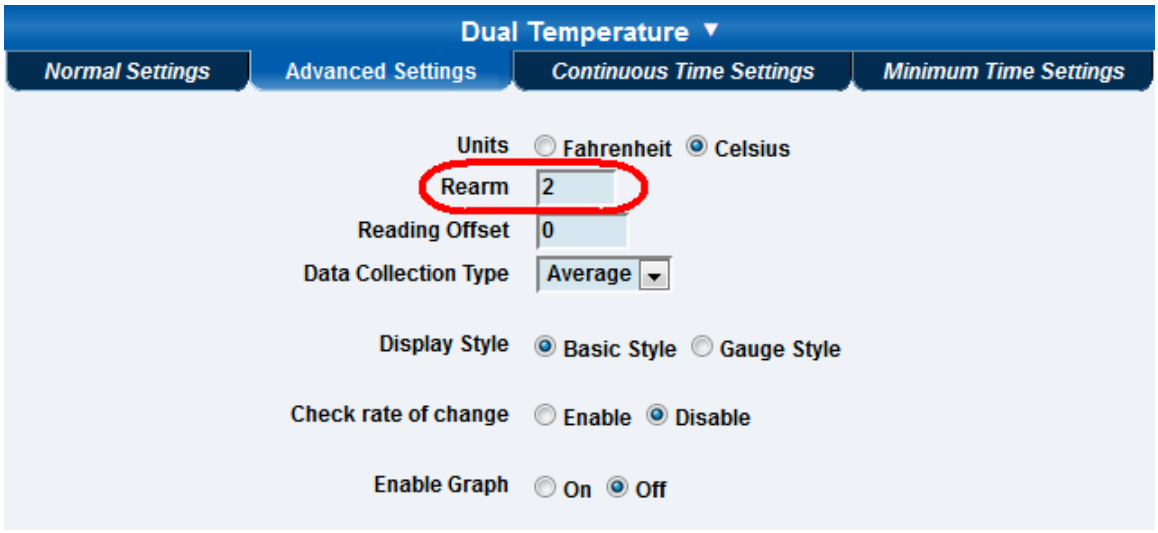


Advanced mode functions



Units: changes units from C to F or vice versa

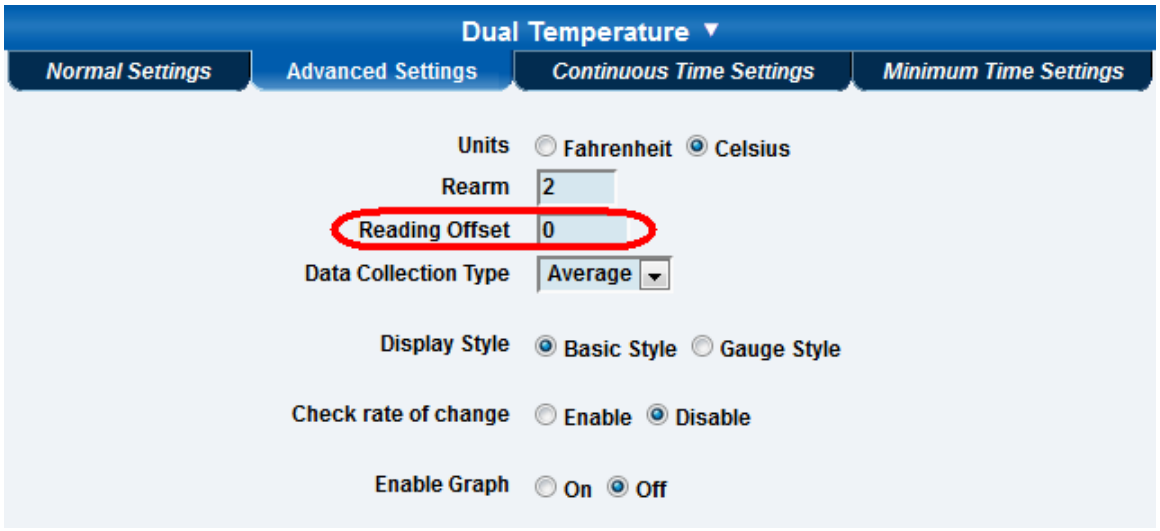
Rearm:



The Rearm parameter is useful for sensors whose values can vary such as the temperature and humidity sensors.

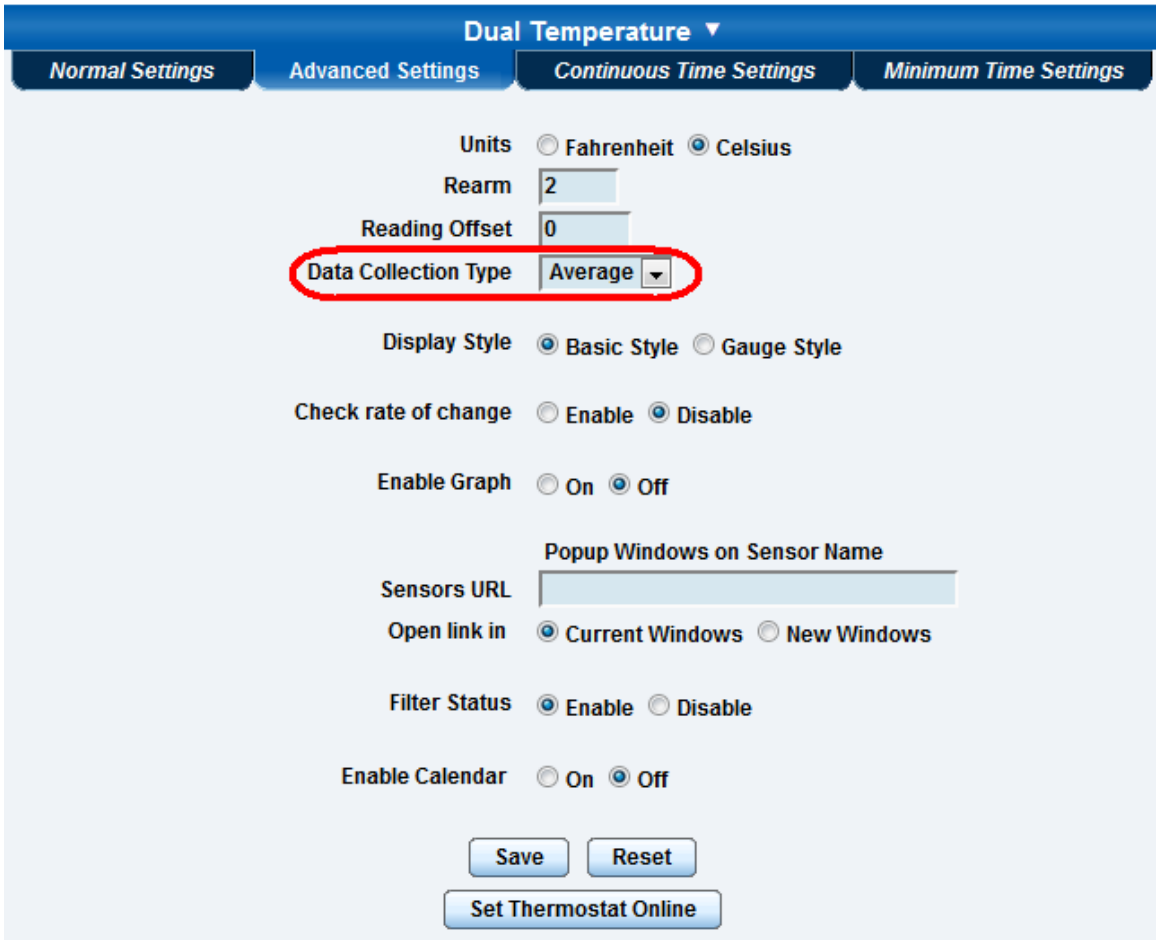
It is used to prevent the sensor from flickering between two states. For example if the **Warning High** threshold for the temperature sensor is set to 80 degrees and the sensor were to vary between 79 and 80 you could be faced with a very large number of emails, traps, and events logged. The Rearm parameter prevents this by forcing the temperature to drop by the Rearm value before changing the state back to normal. In this example, if Rearm is set to 2 then the sensor would have to drop from 80 down to 77 before the status would change from **Warning High** back to normal.

Reading Offset:



The Reading Offset feature Is a calibration tool. If you wish to calibrate the temperature sensor, for example, you could enter an offset value of 5. This would mean if the sensor reads 20 degrees then it would record as 25 degrees. This figure can also be a minus figure (e.g. -5 would show 15 degrees instead of 20)

Data Collection Type:



This refers to the data collection from the sensor and how the data is then displayed on the graphs.

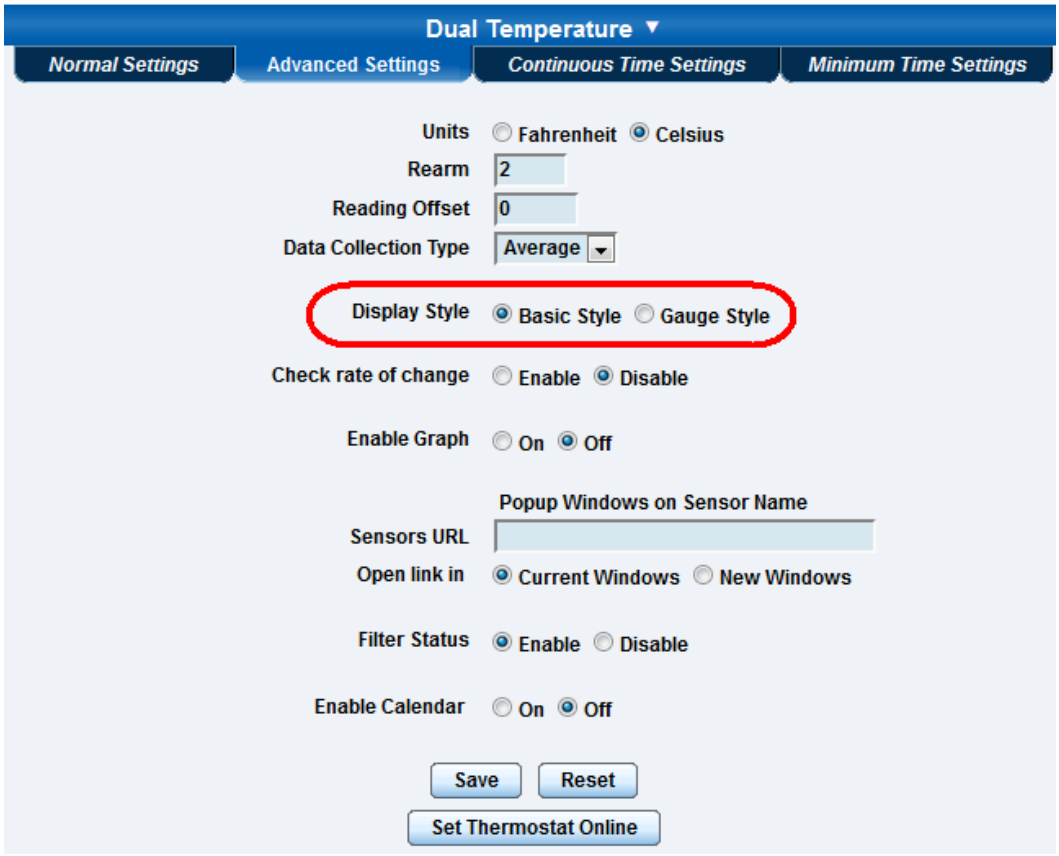
There are three options for the collection of data. Average, Highest and Lowest. The default setting is “Average”.

When the data collection type is set to “Average” the output graphs for the daily, monthly, and yearly all have the same size on the screen. For the daily graph, each data point on the graph is one data point collected from the sensor. But for the monthly and yearly graph, in order to display more data into the same size as the daily graph, some consolidation on the data is needed. One data point on the monthly and yearly graph is an average of the sensor data in a range.

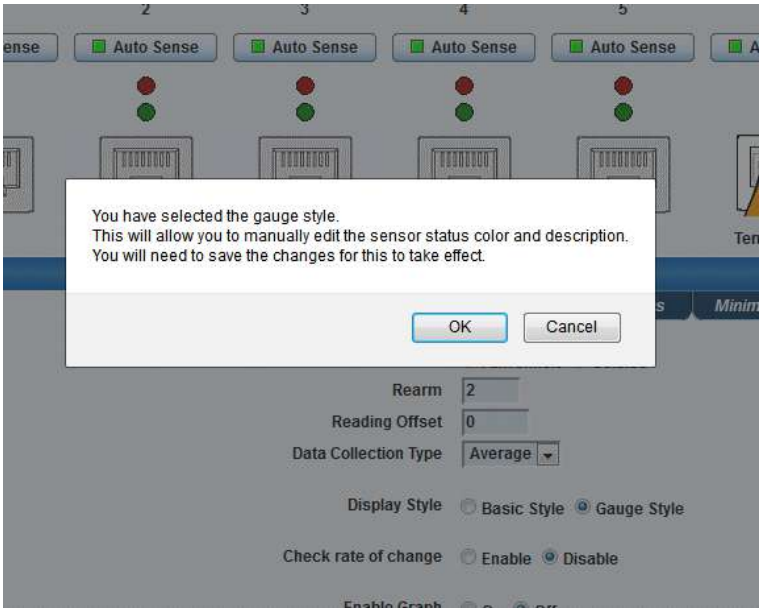
The maximum and minimum values showing on the monthly and yearly graphs are the value of this consolidated data and not the raw data over that period of that time.

The When the Data Collection Type is set to the Highest setting then you will get the graphing output displaying the sensors highest reading. This is the same for the Lowest setting.

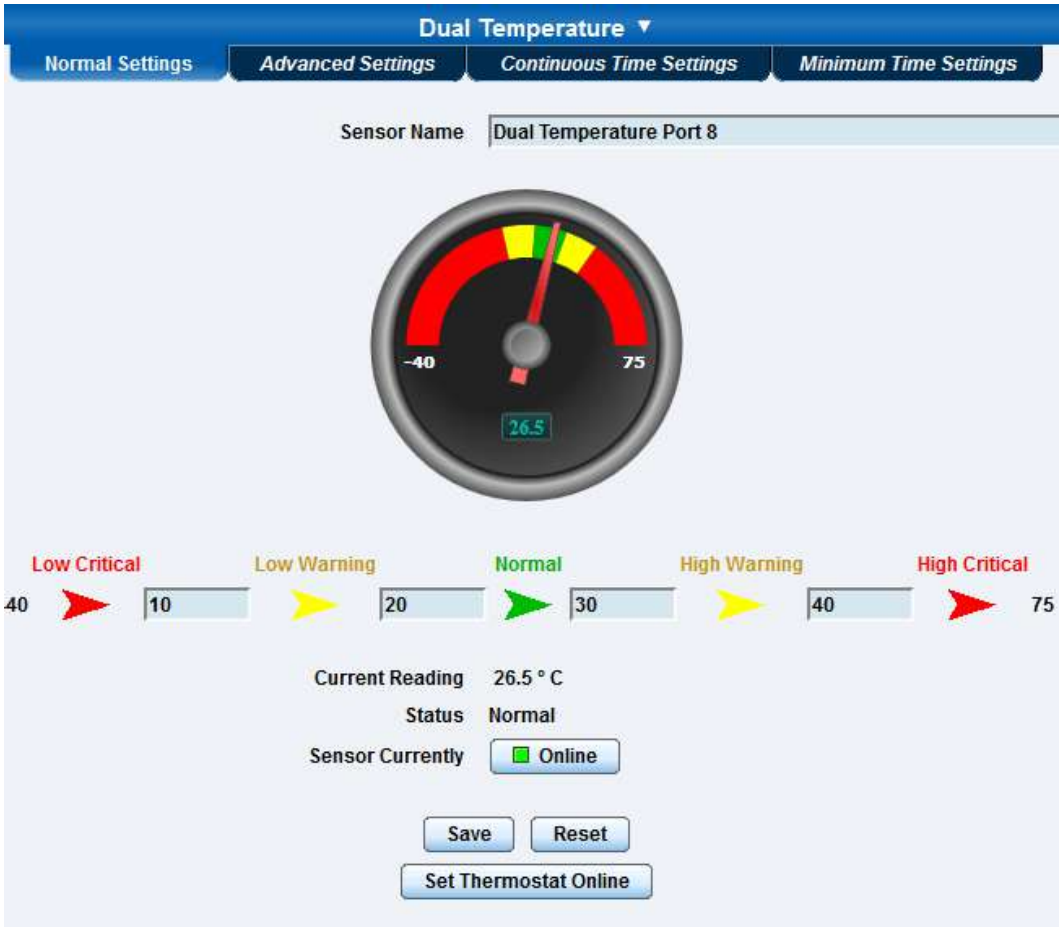
Display Style:



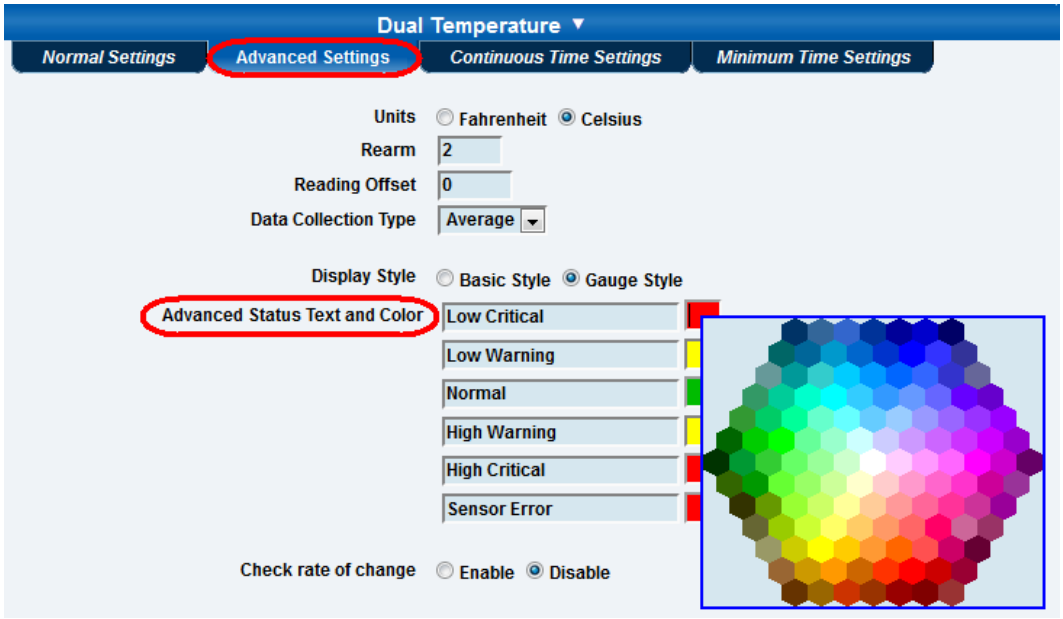
You can keep the sensors "Display Style" in the web interface as the Basic Style which will be the slide bar type or you can change it to the "Gauge Style" type.



When switching to the Gauge Style type you will first be prompted with the pop up dialog box show above.

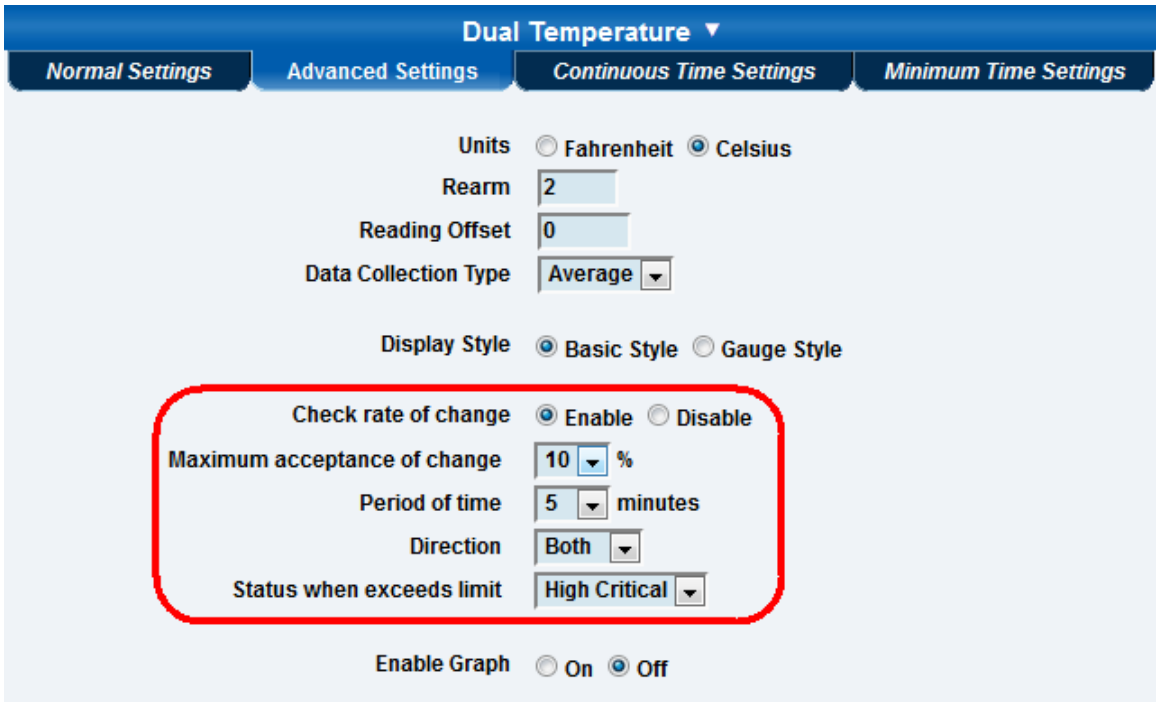


You will now see the new display where you can set the sensors threshold levels as shown above.



After clicking on the “Advanced Settings” tab, you can change the text and colors for each sensor threshold as shown in the screen shot above.

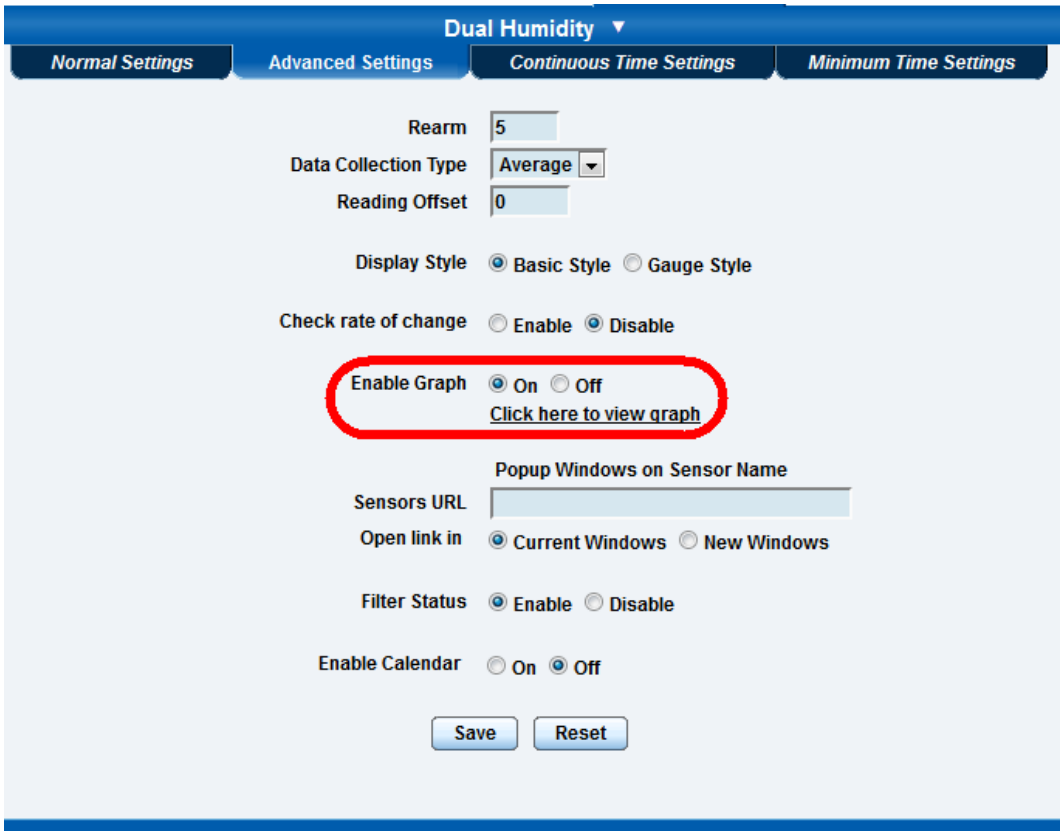
Check rate of change:



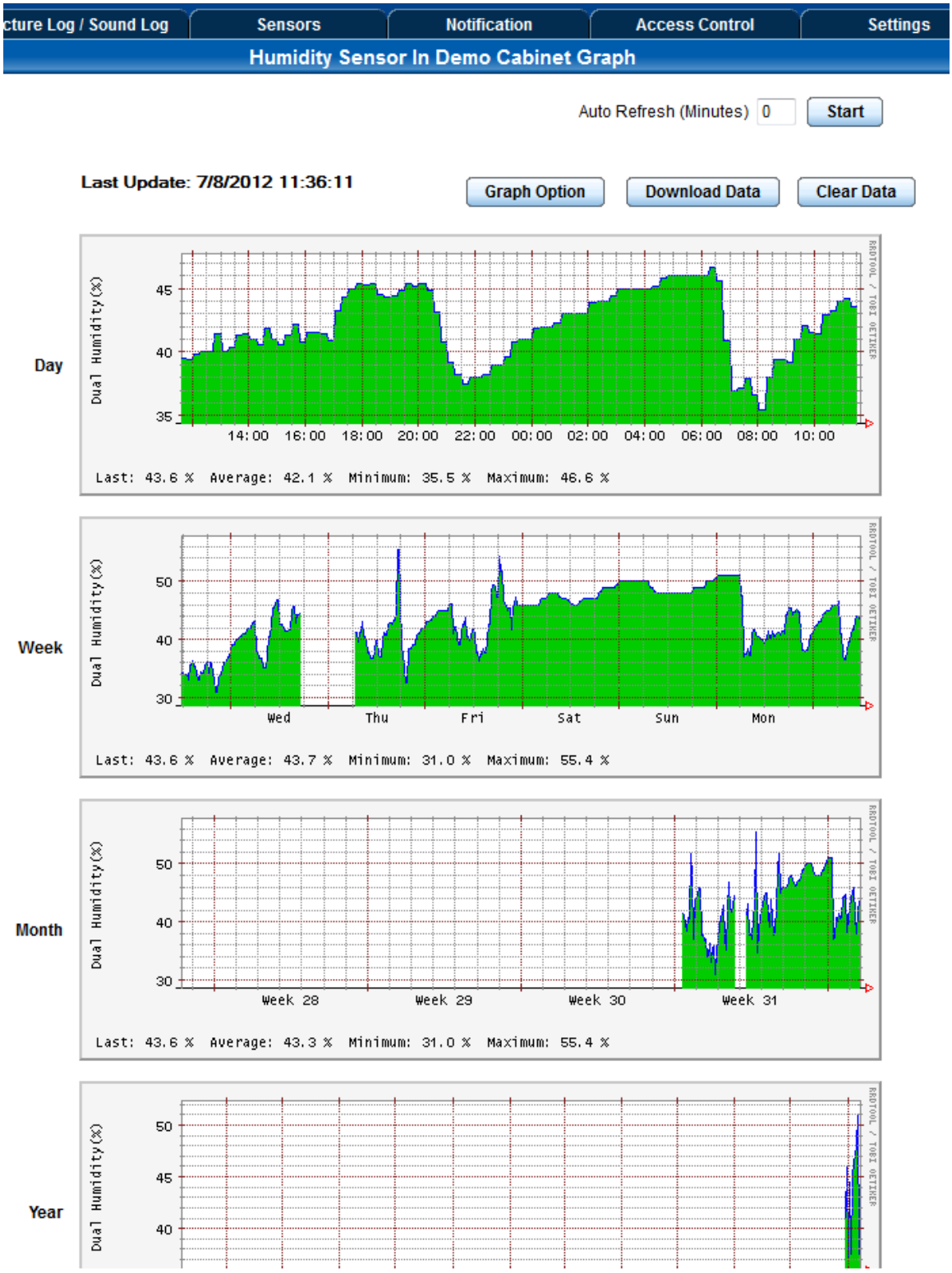
When enabling the “check rate of change” feature for this sensor, you can set the rate in a percentage from 1% to 50% over a period of time from 1 to 20 minutes. You can set the direction to Up, Down, or Both and you can set the Status when the limit is exceeded to show either High Critical or Low Critical.

Now you can tie this sensor alert to any notification. This feature is ideal for our Ultrasonic Fuel Level Sensor to prevent theft of fuel or be alerted to leaks in storage tanks for example.

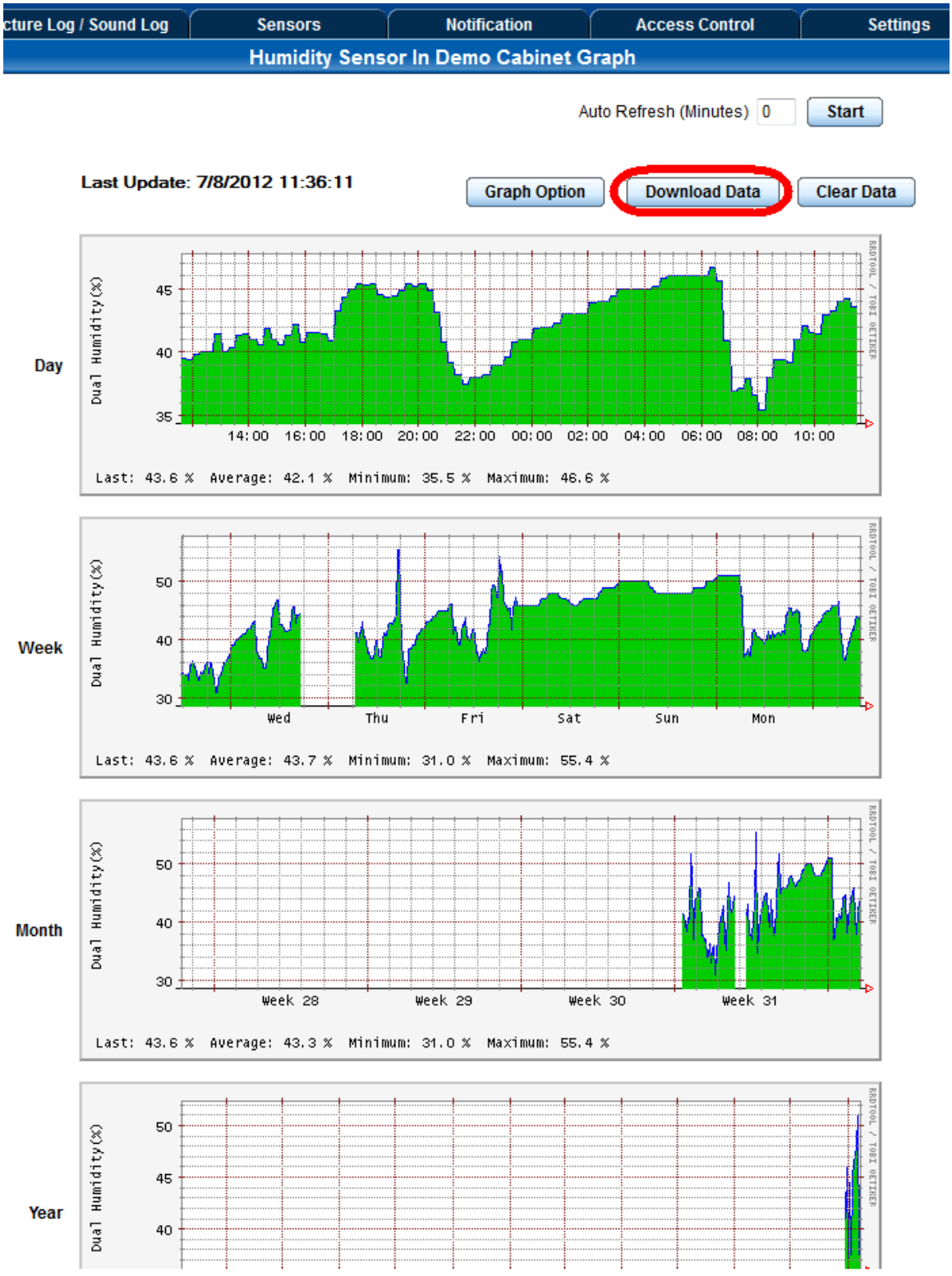
Graphing Sensor Data:



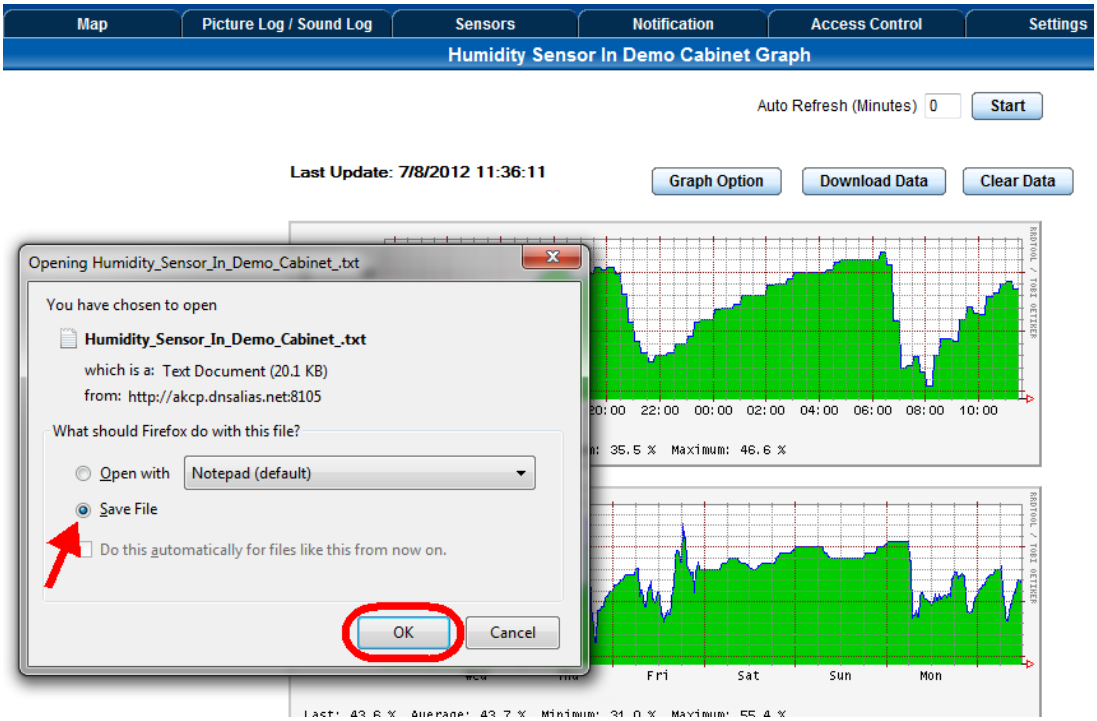
In order to save the data from the sensors on the securityProbe 5E you will need to enable the Graphing feature on the unit. You need to change the Enable Graph to the On position and click on the Save button to enable the graphing.



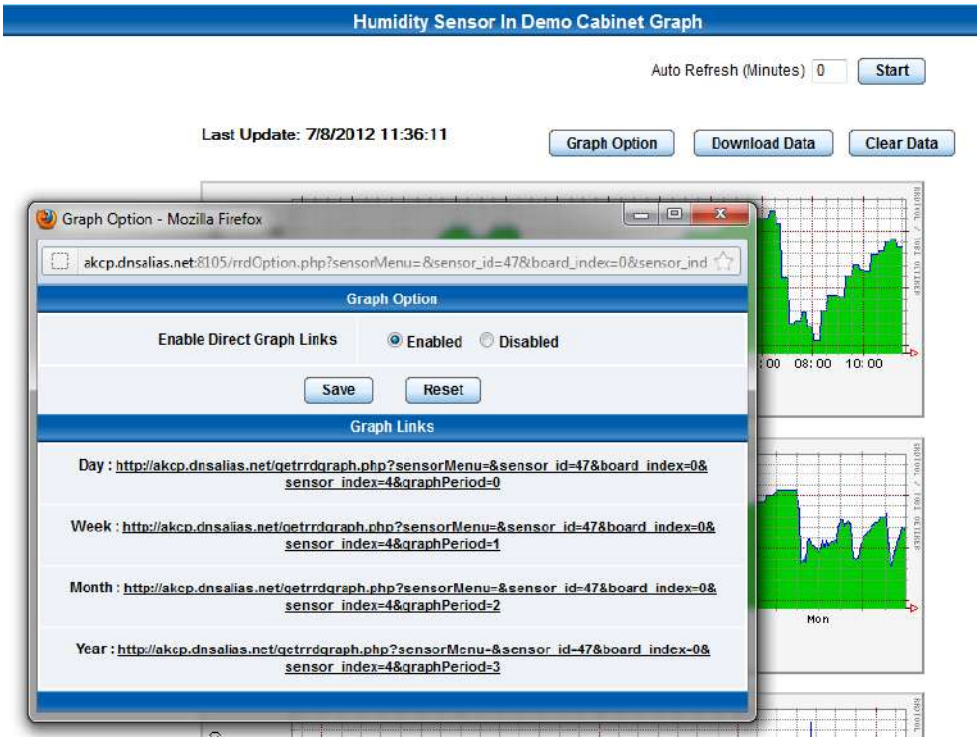
After clicking on the “Click Here to View Graph” link shown in the screen shot on the previous page you will then see the graphs for the sensor.



You can download the sensor data to a text file by clicking on the Download Data button shown in the screen shot above.

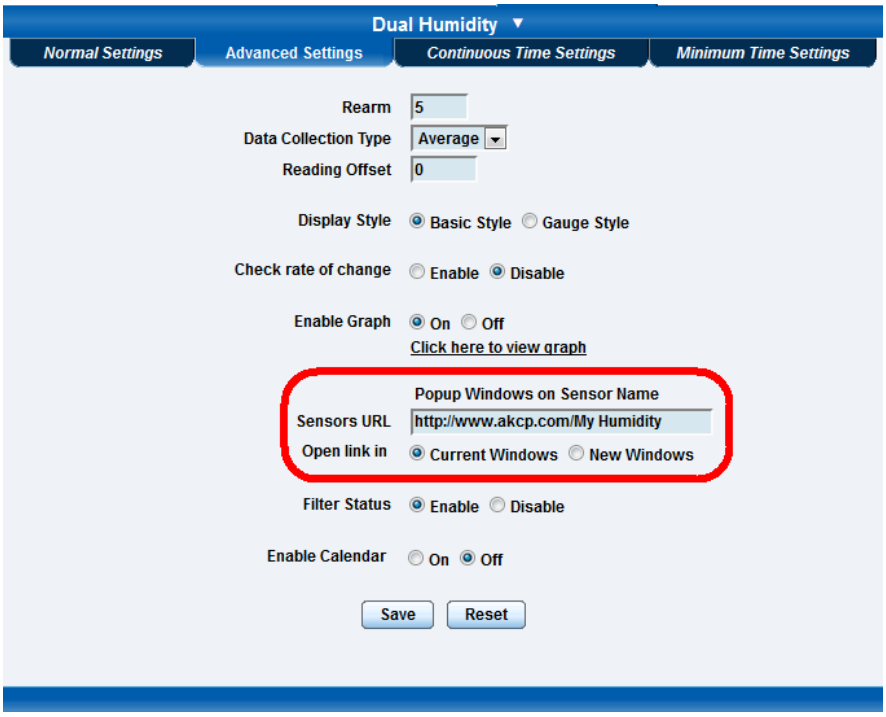


Which will display the pop up box as shown in the screen shot above.



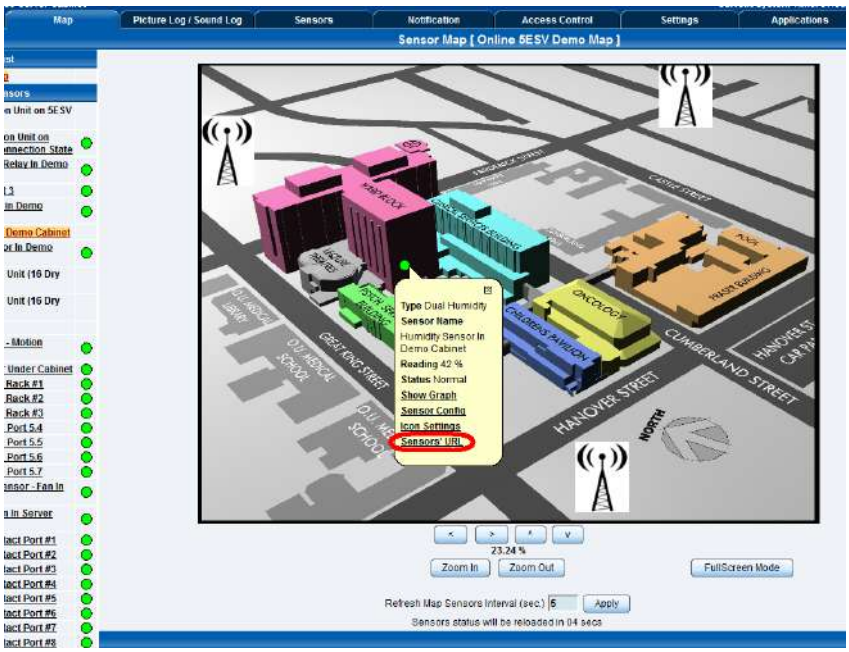
You can also set the Graph Options by clicking on that button then Enabling the graphing page URL's as shown in the screen shot above.

Sensors URL:

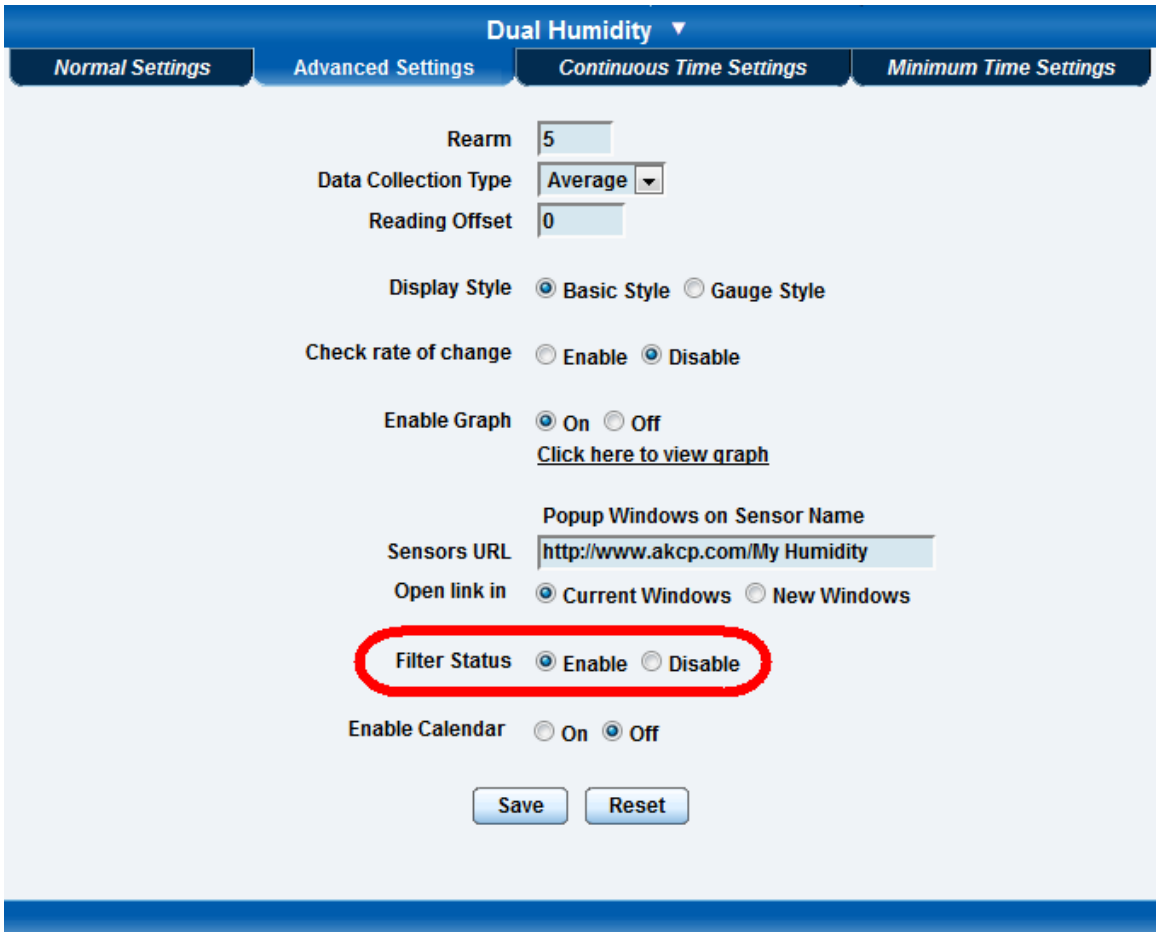


The Sensors URL feature in the Advanced Settings tab is the optional Hyperlink URL for each sensor.

What this feature does is allow you to add a Hyperlink to a sensor, then this link will be displayed in the securityProbe 5E's mapping feature for that sensor (see the screen shot below) that you can then click on to follow the link to say a picture on the web of where the sensor is exactly or whatever you wanted to link to.



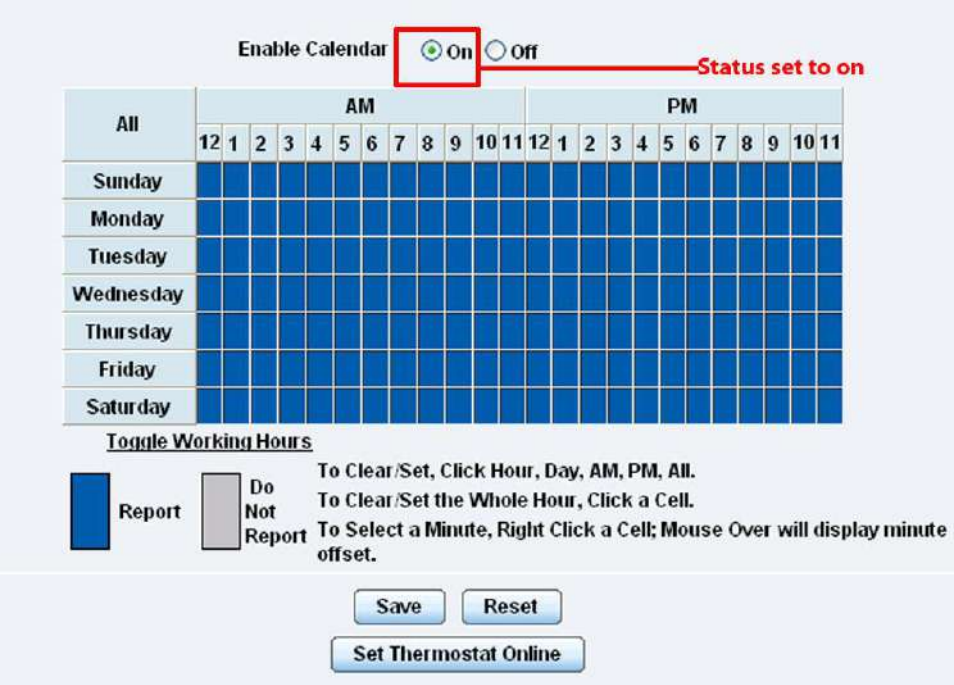
Sensor Filter Status:



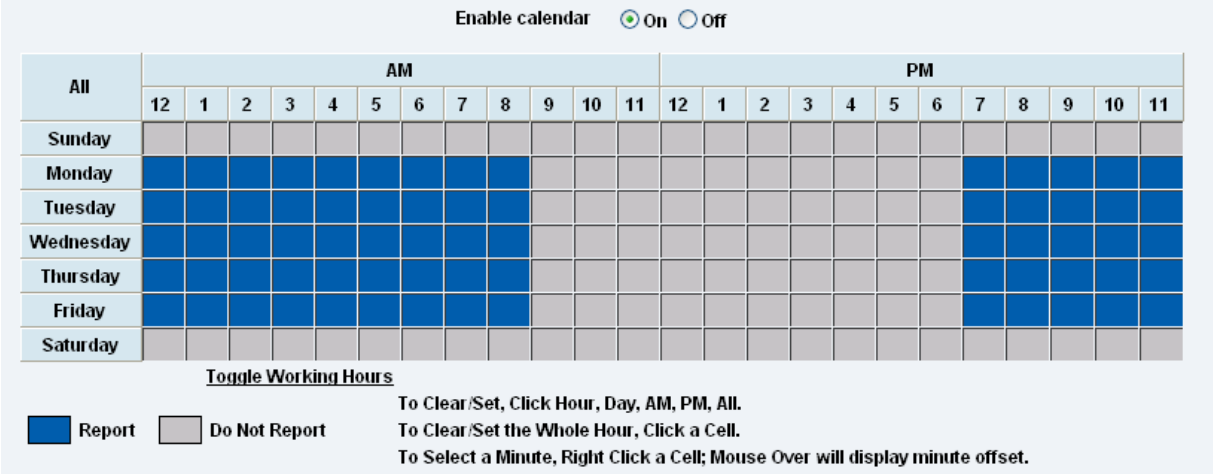
The Sensor Filter Status is a a feature that you can Enable or Disable and when enabled will check the sensor status. If the status of the sensor changes very rapidly, then it will report how many times the sensor status changed, instead of having 36 separate entries in the syslog entry.

For example this will report the changes and status once as shown below. Sensor Temperature port 1 status was Error 3 Times, Normal 2 Times. This reduces the writing to the flash and improves performance.

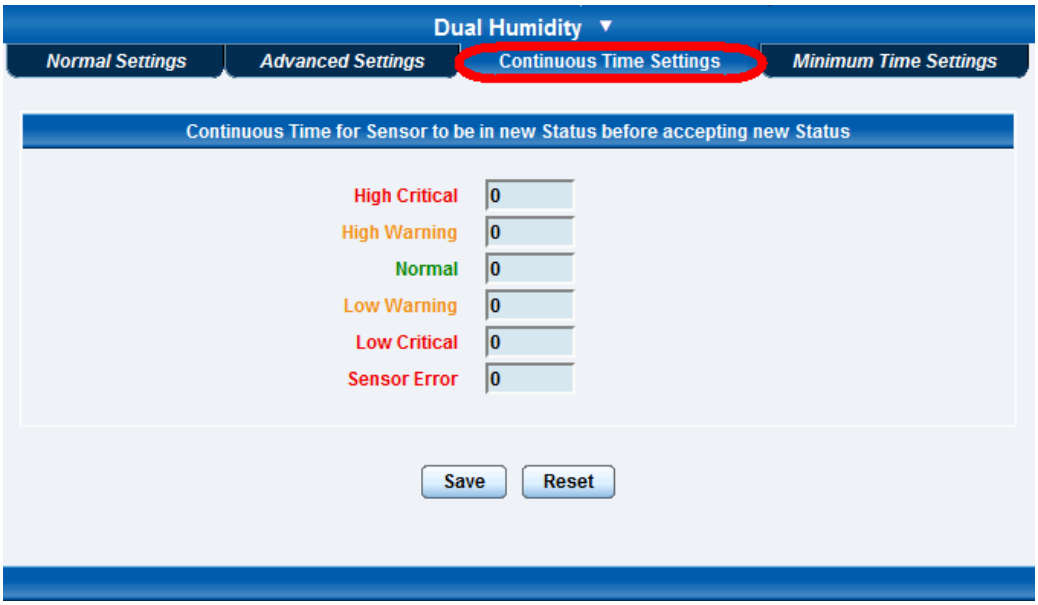
Enable Calendar: If you select this option then the following will be displayed:-



In our example we wish to monitor an office building between the hours of 7 PM – 9 AM Monday – Friday only. You can see in this picture we have selected the “Do Not Report” option for the hours in which we do not wish to receive any notifications or have any events logged. You change the status of that time frame (Report / Do Not Report) by simply clicking on the square. This will change it from blue to grey, a second click will return it to blue.



Continuous Time Settings Tab



The following advanced functions are for setting the time frame in which the system should delay a notification being triggered when a sensor gives a reading that exceeds the thresholds (high warning, normal, etc).

Continuous Time to Report High Critical: This helps to eliminate unnecessary messages during minor fluctuations. You can set the amount of time to delay a notification of a status change from high warning to high critical. Enter the time in seconds and press the "Save" button. The amount of time that can be entered is between 0 and 65535 seconds which equals approximately 18 hours

Continuous Time to Report High Warning: As above but delays notification for "High Warning"

Continuous Time to Report for Normal: As above but delays notification for return to "Normal" state

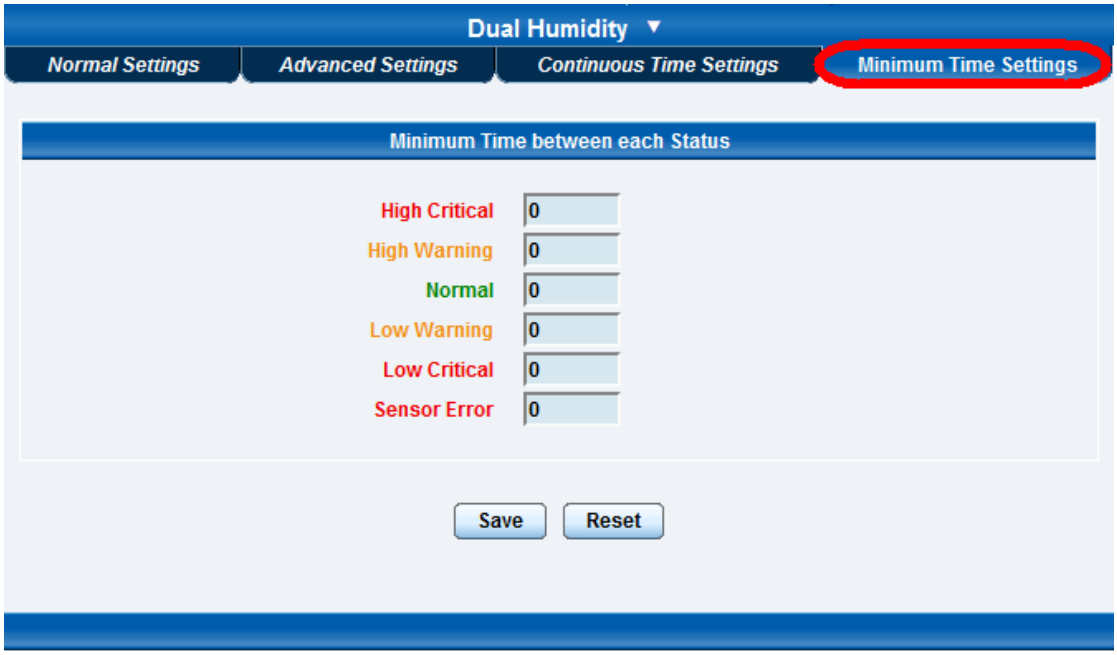
Continuous Time to Report for Low Warning: As above, but delays notification for "Low Warning" state.

Continuous Time to Report for Low Critical: As above but delays notification for "Low Critical" state.

Continuous Time to Report for Sensor Error: As above, but delays notification being sent for sensor going into an error state.

Example: An airflow sensor or humidity sensor may have temporary drops in readings which are normal operating characteristics; a logical time limit is set to show abnormal conditions.

Minimum Time Settings Tab



Minimum Time Status Prevents the status from fluctuating within the time set. For example, a sensor can only show high critical state once within 3 seconds, if value is set to 3 seconds.

Using internal Mic as a sound detection sensor

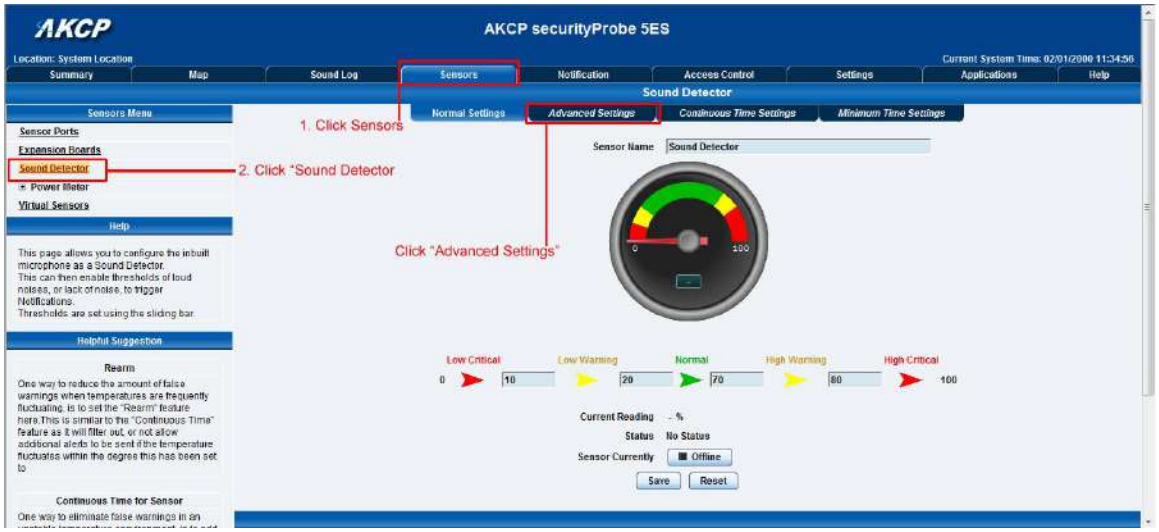
The internal microphone (or an external plugged into the line in jack) can be used as a sound detector.

This tutorial provides you the information needed to setup the internal Mic as a sound detection sensor.

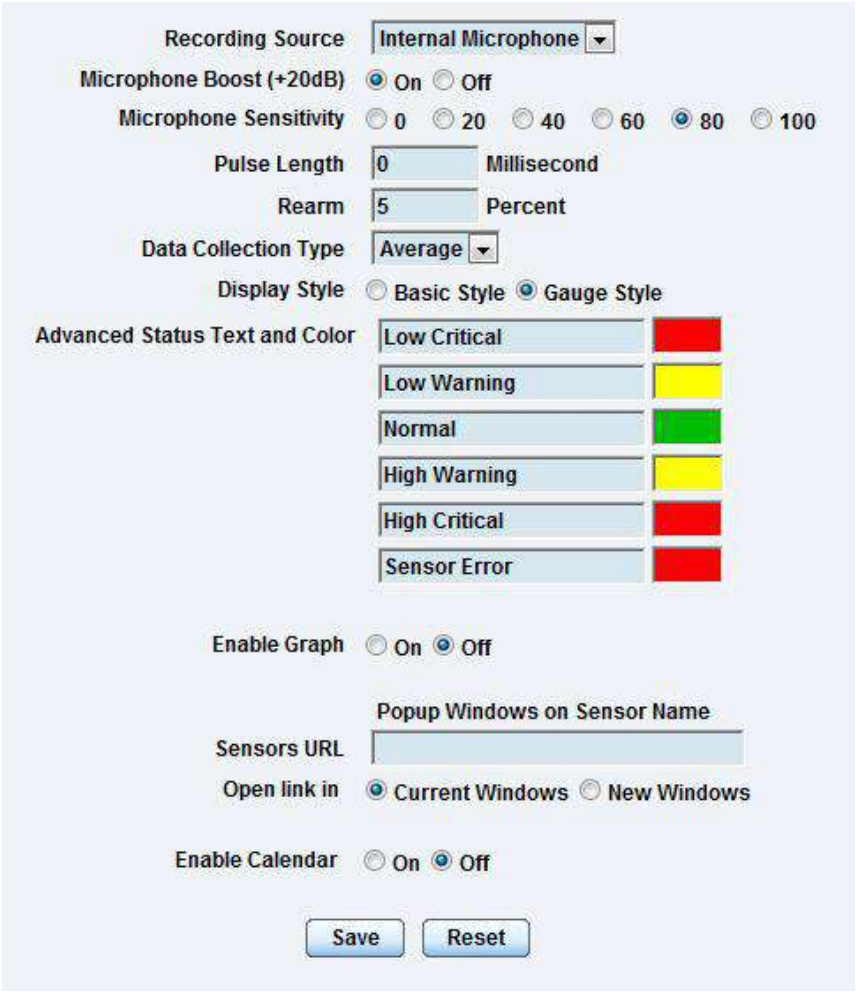
To get to the starting point of this tutorial:

- Log into the web based interface
- Click on the sensors tab

a) First navigate to the correct page in the web interface.



b) When you have clicked on the advanced settings tab you will see the advanced options presented to you.



Now lets look at what each of these settings does:-

Recording Source: Here you can choose either internal or external microphone.

Microphone boost (+20dB): Boosts the microphone by 20 dB

Microphone Sensitivity: The level of sensitivity that can be set. For example, if you set the level to 80, then the microphone will detect more sound if the level was set a 20.

Pulse Length: This defines the minimum duration of a sound to trigger an alert notification.

Rearm: The Rearm parameter is used to prevent the sensor from flickering between two states. For example if the **Warning High** threshold for the sound sensor is set to 80 and the sensor was to vary between 79 and 80, a very large number of emails, traps, and events would be logged. The Rearm parameter prevents this by forcing the signal level to drop by the Rearm value before changing the state back to normal. In this example, if Rearm is set to 2 then the sensor would have to drop from 80 down to 77 before the status would change from **Warning High** back to normal.

Data Collection Type: There are 3 settings for this parameter: lowest, highest, and average. Data will be collected for the lowest, highest, or average sound reading accordingly.

Display Style: Here you can choose the gauge style, or the classic bar style gauge.

Advanced Status Text and Color: Here you can select to change your display text and warning colors.

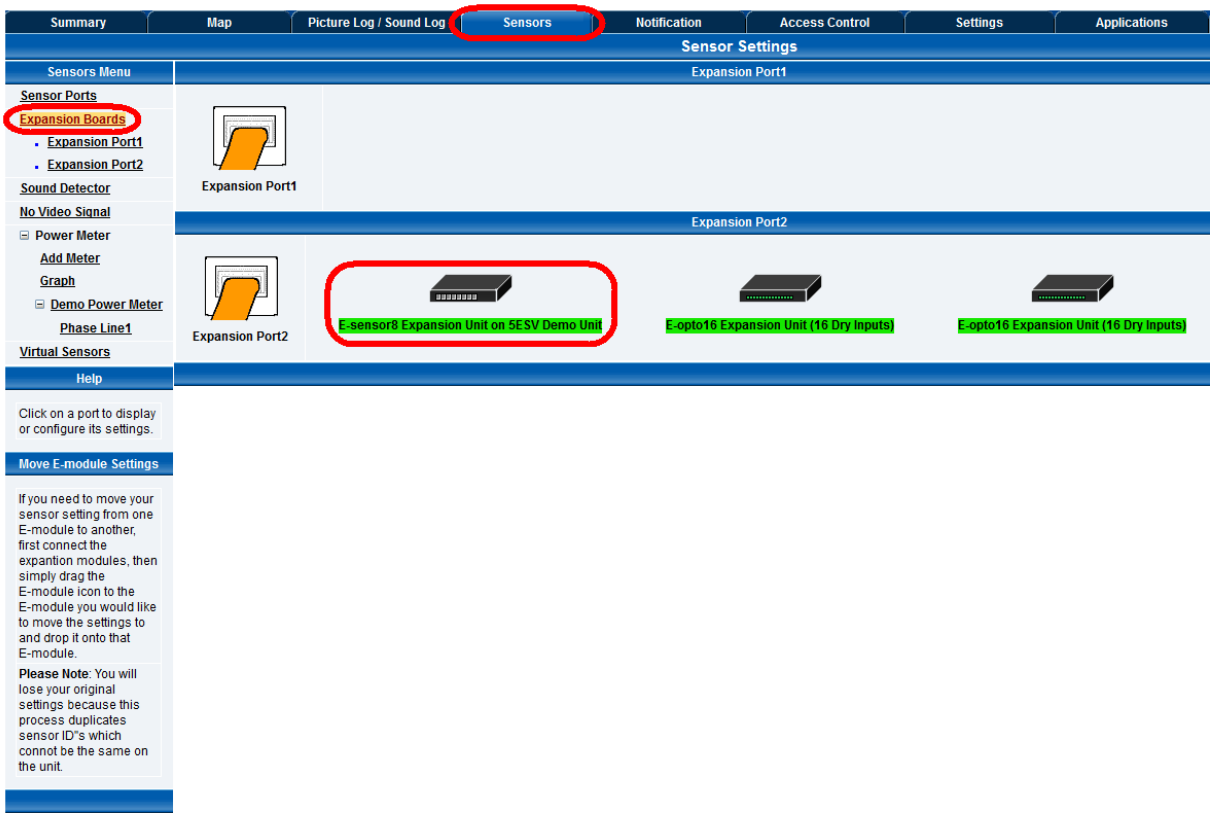
Note: As for all the other sensors you can now set up the sound detector to be attached to a notification. Then when your thresholds are broken it will trigger a specified type of notification.

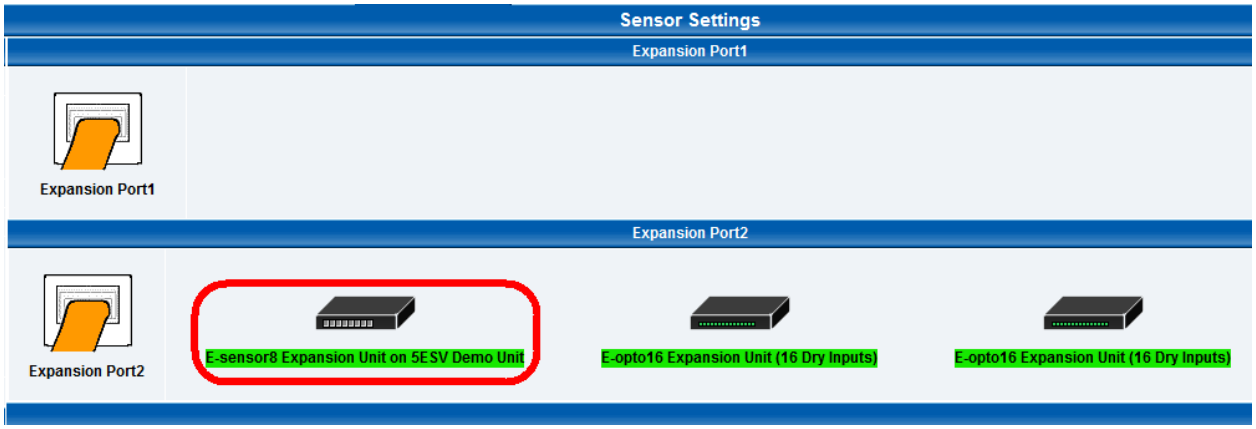
7. Expansion Ports

Your AKCP Securityprobe-5E is equipped with two expansion ports. This enables you connect up to four daisy chains of expansion modules. The available expansion modules are an eight port intelligent sensor board and an Opto-isolated sixteen dry contact expansion module. In this section we will go through the basic setup of the sensor. If you require information on specific functions of a particular sensor or expansion board then please refer to the relevant manual for that product.

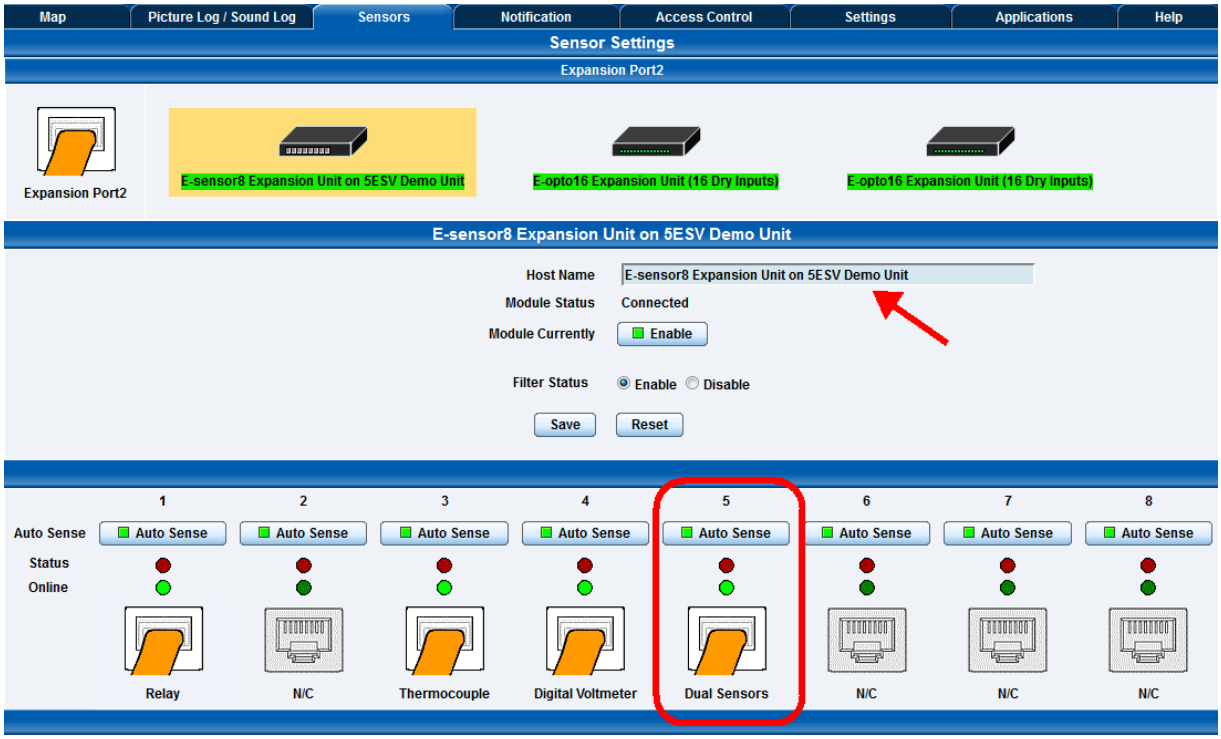
Plug the expansion unit into one of the two ports located on the front panel of the unit. These are numbered E1 and E2.

From the summary page, navigate to the “Sensors” tab. Then click “Expansion Units” as outlined in the image below:-





A list of all extended ports will be shown. Each port will display any available expansion units, these will be highlighted in green. Click the module to be taken to the sensor settings page.



This will bring you to the page shown above, the extended port sensors page. On this page you can change the name of the expansion module you can also disable it by clicking on the Enable / Disable button.

Once you have clicked on the “Dual sensors” tab you will be directed to the familiar looking notification thresholds page. From this page you can carry out various operations as indicated in the sensor settings tutorials found on page 42.

Please consult the Expansion Units separate product manual for more specific information such as the SNMP OID’s for checking sensors connected, how to transferring settings to additional units, setting up disconnect alerts etc.

3) Notifications

If you setup a notification you can define the action to take when the sensor gives a reading beyond your previously set thresholds. This allows you to determine how you will be notified that a sensors reading has reached the specified parameters (high warning, critical etc) that we looked at in the previous section.

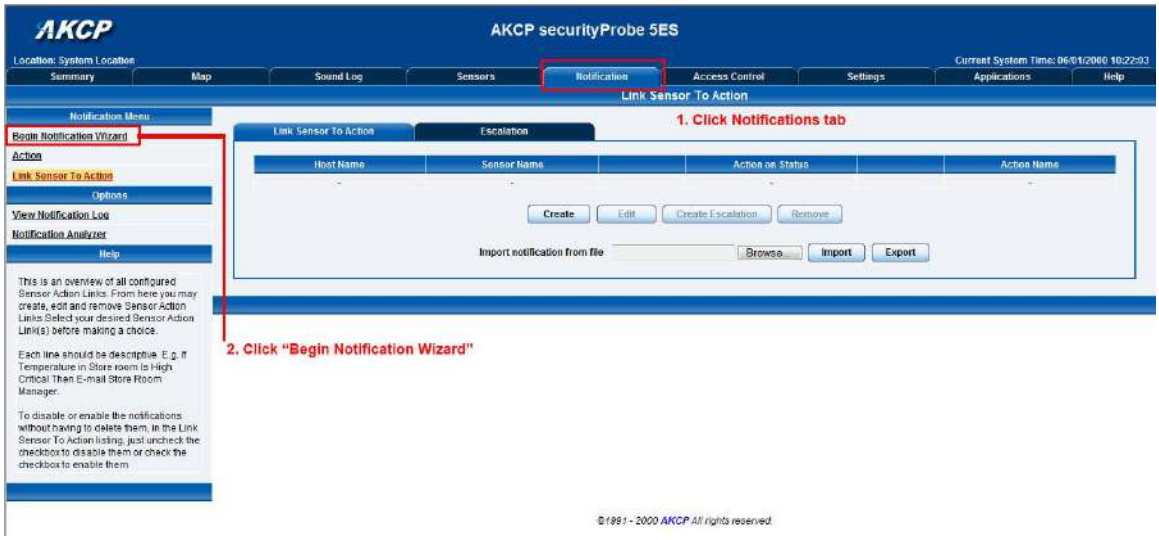
This tutorial provides you the information needed to setup a notification.

To get to the starting point of this tutorial:

- Login as administrator
- Click the “Notifications” tab

1. Adding a notification

a) First click on the “notification wizard”



b) You will now have the notification wizard page displayed, shown on the next page.

Please Note: We will now go through setting up a few different ways of notification step by step. To learn what the other types of notifications do refer to the separate notification manuals that can be found on your product CD.

2. SNMP trap

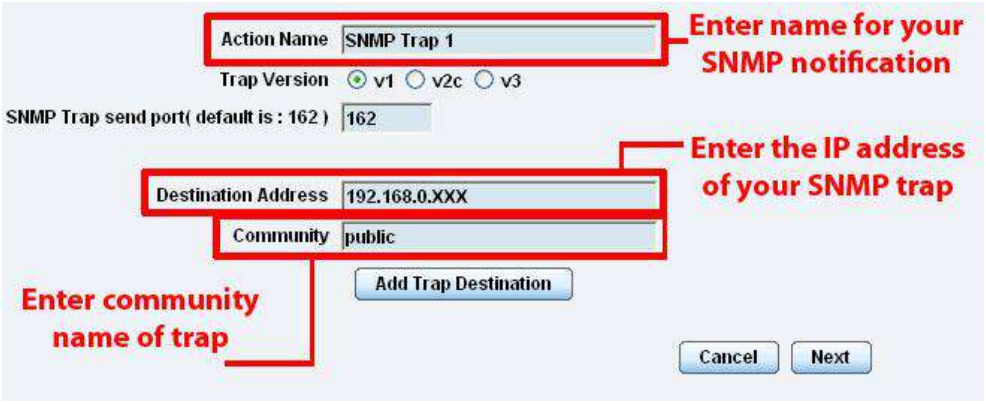
First we will set up a notification via SNMP trap, so that when your sensor reaches a certain threshold it will send a notification to your SNMP server.

This tutorial provides you the information needed to setup an SNMP trap.

To get to the starting point of this tutorial:

- Log in as administrator
- Click the “Notifications” tab
- Choose “Notifications wizard”
- Choose SNMP trap

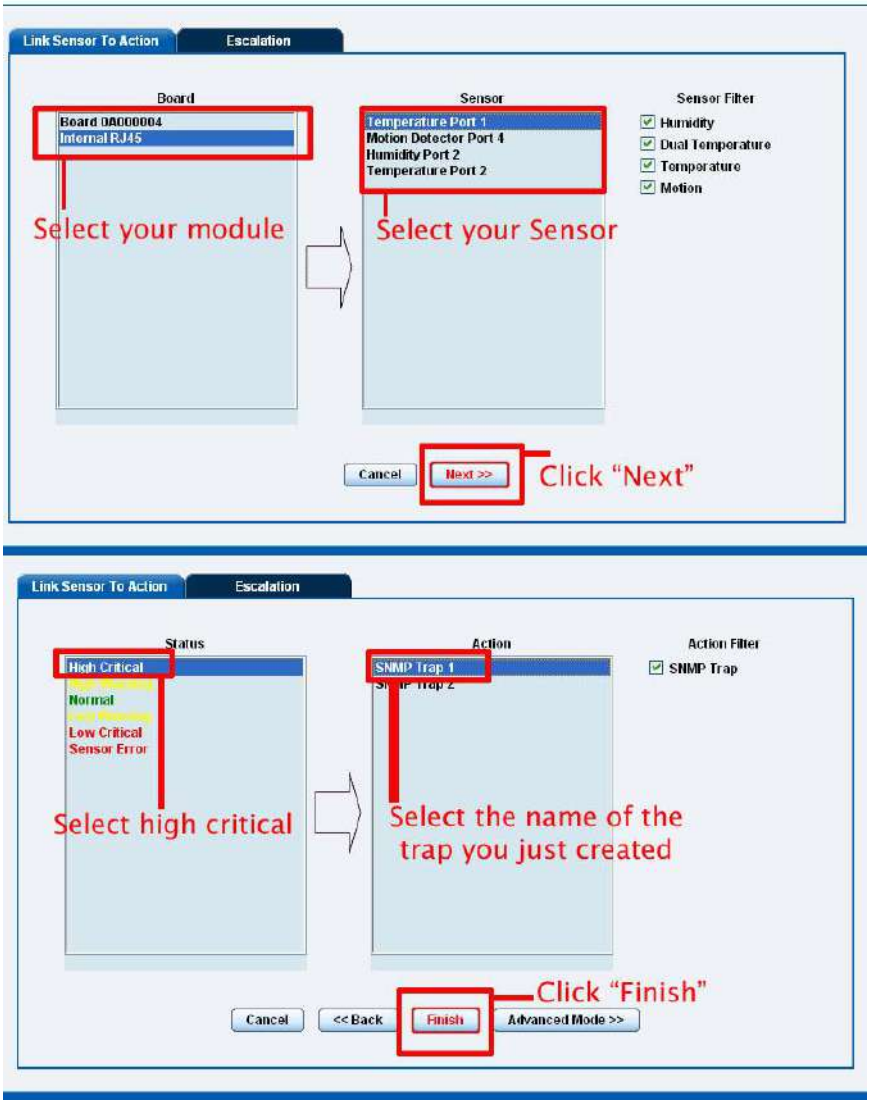
a) After selecting to add an SNMP trap you will need to fill in the following information



b) Once this information is correct you can press the “Add Trap Destination” button. After clicking this you have the option of inputting another trap, or clicking on “Next”. Now you can enter the following parameters:-

These parameters set the maximum number of times to send the trap notification and the time interval between each notification.

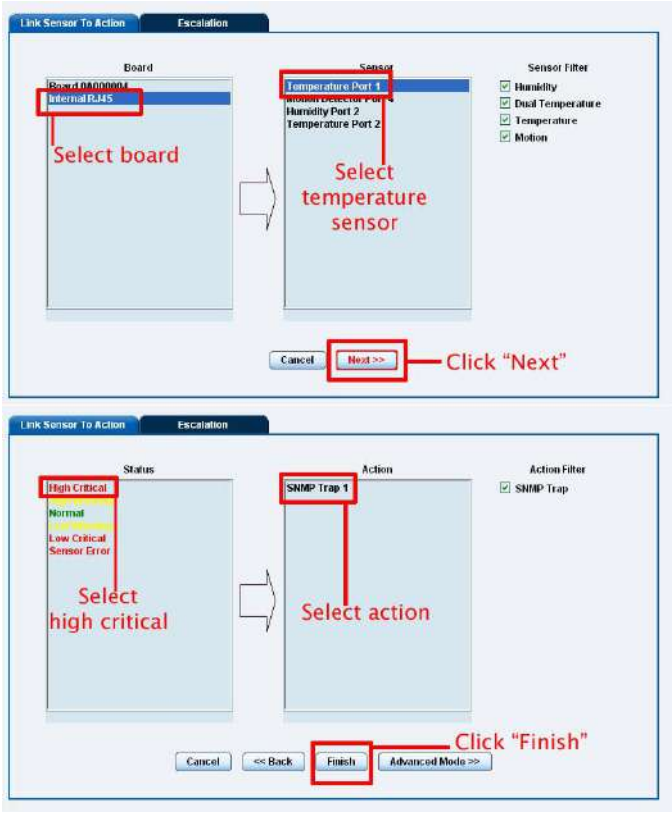
c) After clicking next you will be presented with the following screens:-



On these screens you can select the parameters for when to send the SNMP trap notification. In our example we have selected to bind the SNMP trap to the temperature sensor we have connected on port 1. The trap will be sent when the sensor reads a "High Critical" and we bind this to the SNMP trap we just created and named "SNMP Trap 1"

d) Once we have created the parameters for the SNMP trap, we need to make it active. To do this go back to the notifications tab and it should look like the following:-

e) Select the sensor and SNMP trap parameters as before



f) Now you will see the SNMP trap has been added to our notifications page:-

Note: To remove this trap and make it inactive, highlight the notification and click remove.

You can repeat this process to set up multiple SNMP traps for different sensors, or for multiple SNMP servers etc.

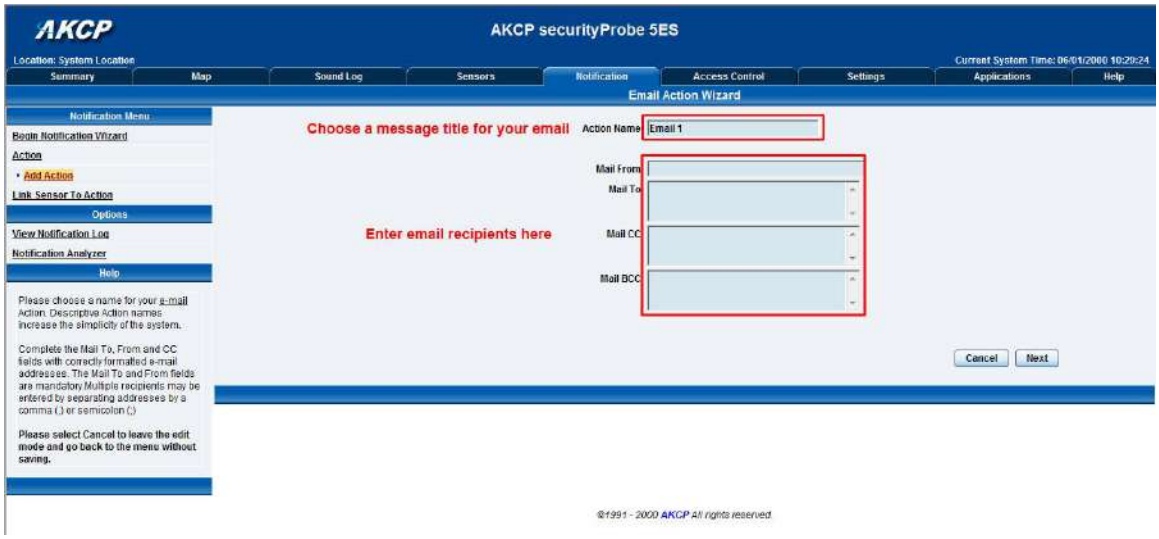
3. E-mail

This tutorial provides you the information needed to setup an E-Mail Notification.

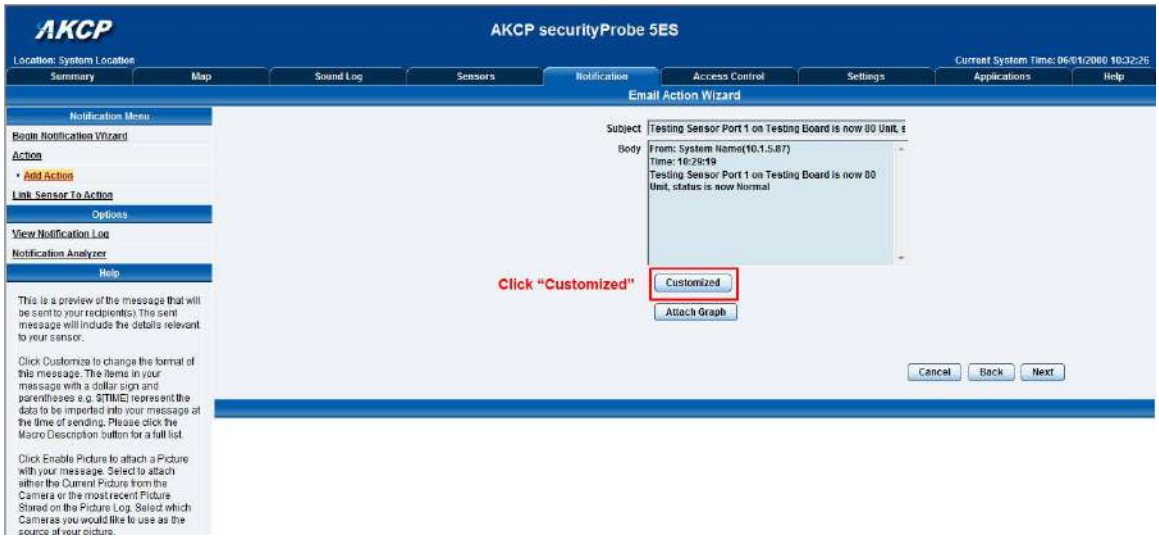
To get to the starting point of this tutorial:

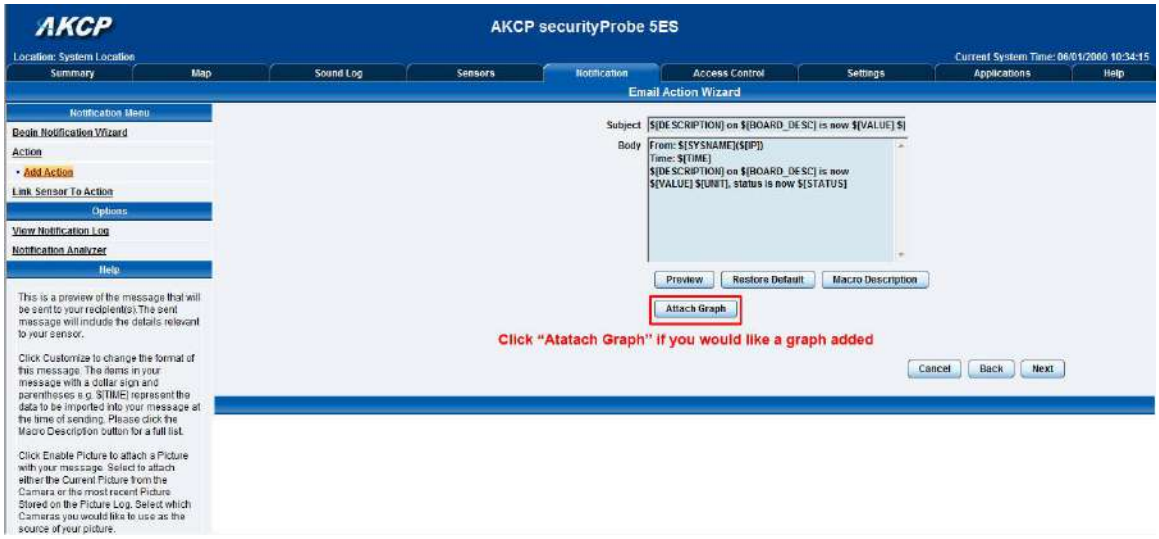
- Log in as administrator
- Select the “Notifications” tab
- Click “Notification Wizard”

a) If you select to set up an E-mail notification you will be shown the following page



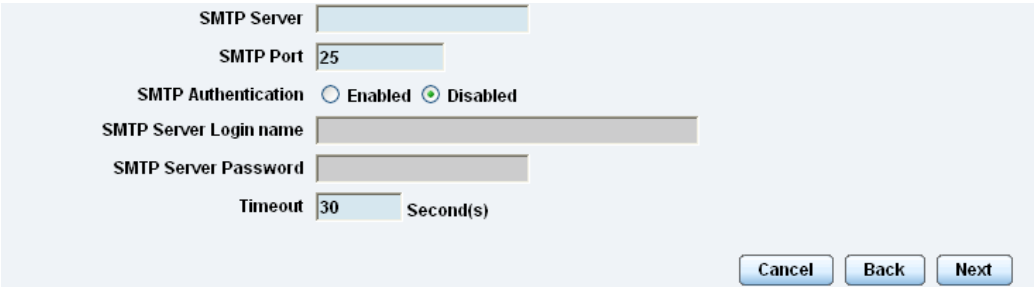
b) After clicking “Next” you will get a page where you can input the e-mail name and message. Press the “Customize” button and the fields will re-write in a format that will allow for an automated e-mail that will display the sensor information.





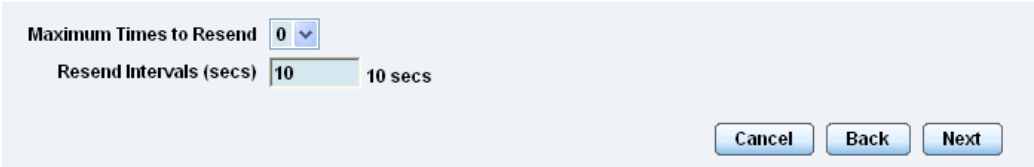
After this click “Next”

c) Now you need to input your SMTP server address for your e-mail account.



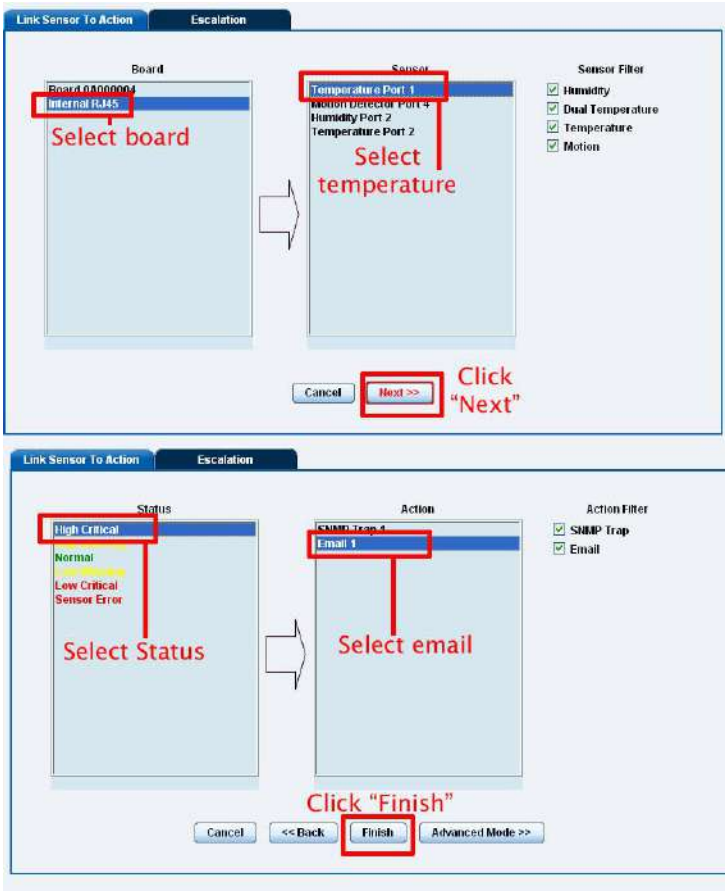
Once this is correct, click next.

d) Now, as with the SNMP trap you can select how many times to attempt to resend the e-mail, and the time elapsed between each attempt.



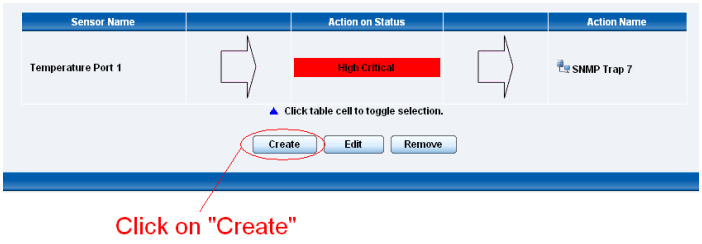
Click next when you have filled in your parameters.

e) Now link the e-mail we just created to the temperature sensor on port 1.

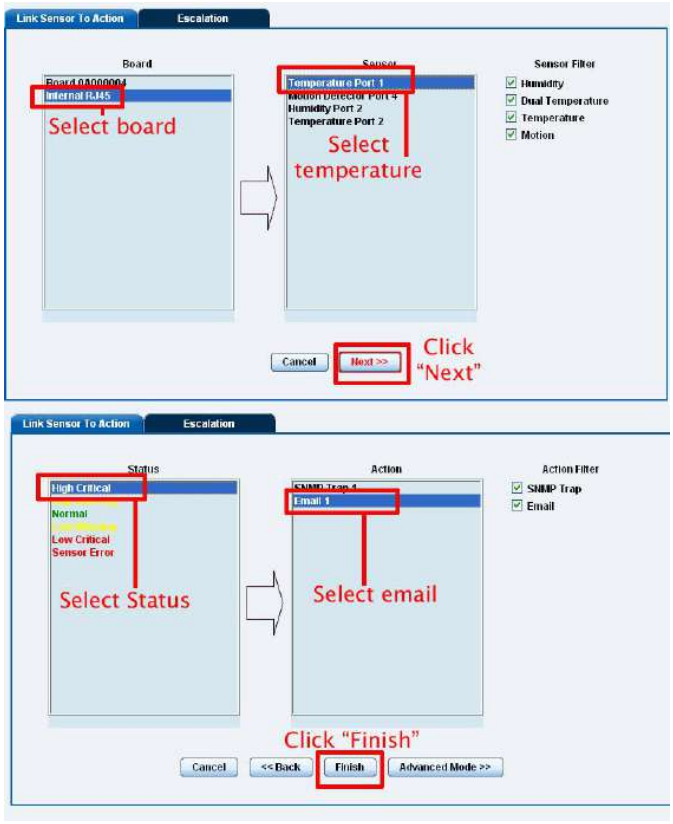


Click on “Finish”. You will now be taken back to the main Notification tab.

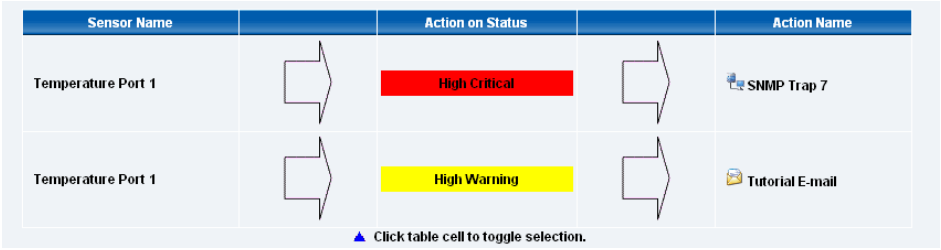
f) Click on create



g) Create the notification link as before. Then click finish



h) You will now be back at the main notification page. You should now see listed our two notifications, the SNMP trap and the e-mail.



As you can see from this page, we now have an SNMP trap set up not give us notification of a "High Critical", and an E-mail notification that will activate on a "High Warning"

4. SMS notification

Now, we will set up a notification so that you will be sent an SMS message. This message can be sent via a GSM/GPRS mobile phone connected via a Bluetooth connection or the USB port.

This tutorial provides you the information needed to setup a SMS notification.

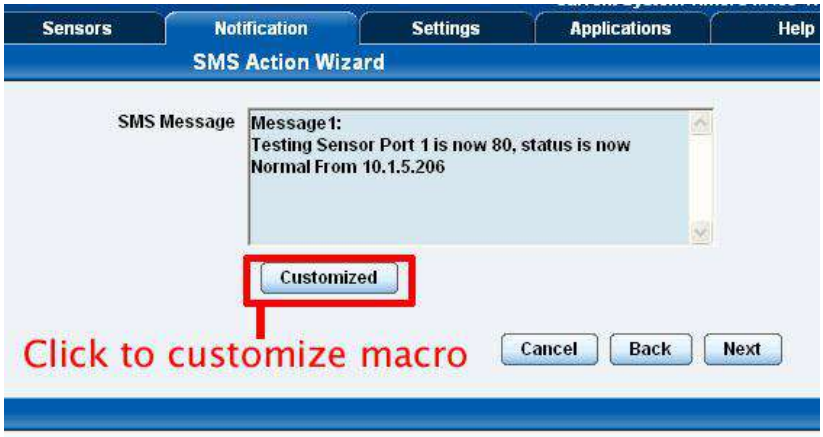
To get to the starting point of this tutorial:

- Log in as administrator
- Select the "Notifications" tab
- Click "Notification Wizard"

a) From the list of notification types select SMS and click next. You will then be presented with this :-

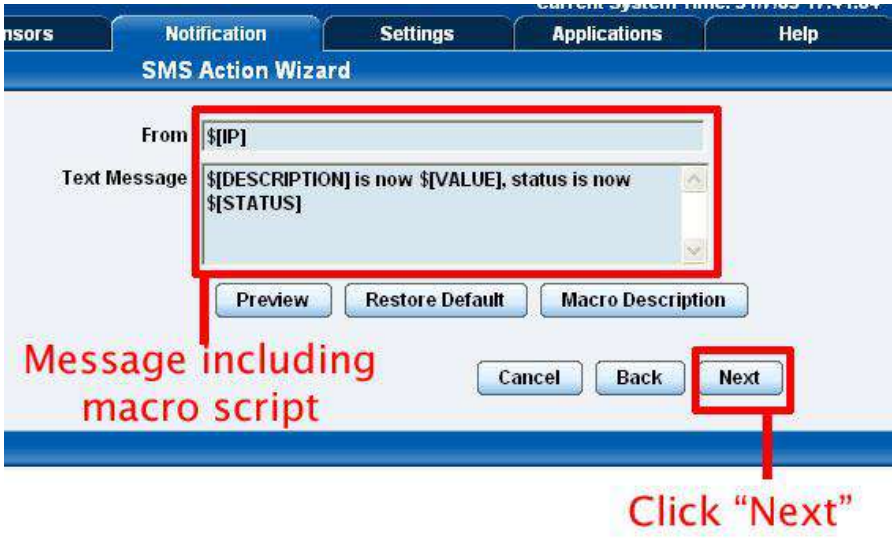
b) You can now either add multiple numbers, or click next. In our case we will click next.

c) Now we will set up the message that will be sent to the phone. You will see the following screen.

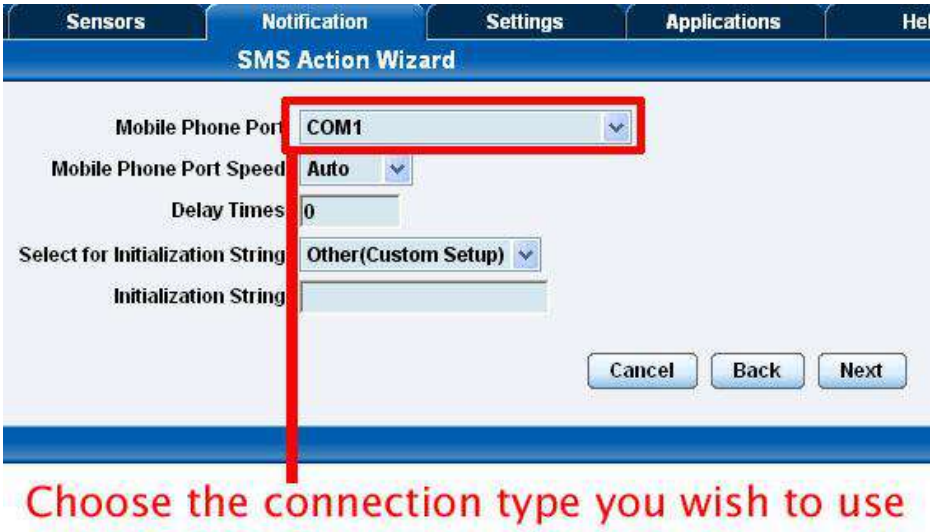


Note: A macro is a script that returns specific data collected by the unit. In our example here the macro will tell the notification to contain the "description" (sensor name), the value (current sensor reading) and the status (high/low warning etc) these macros are common to all sensor notifications.

d) You will now see that the SMS message has changed its format to include the Macro script.

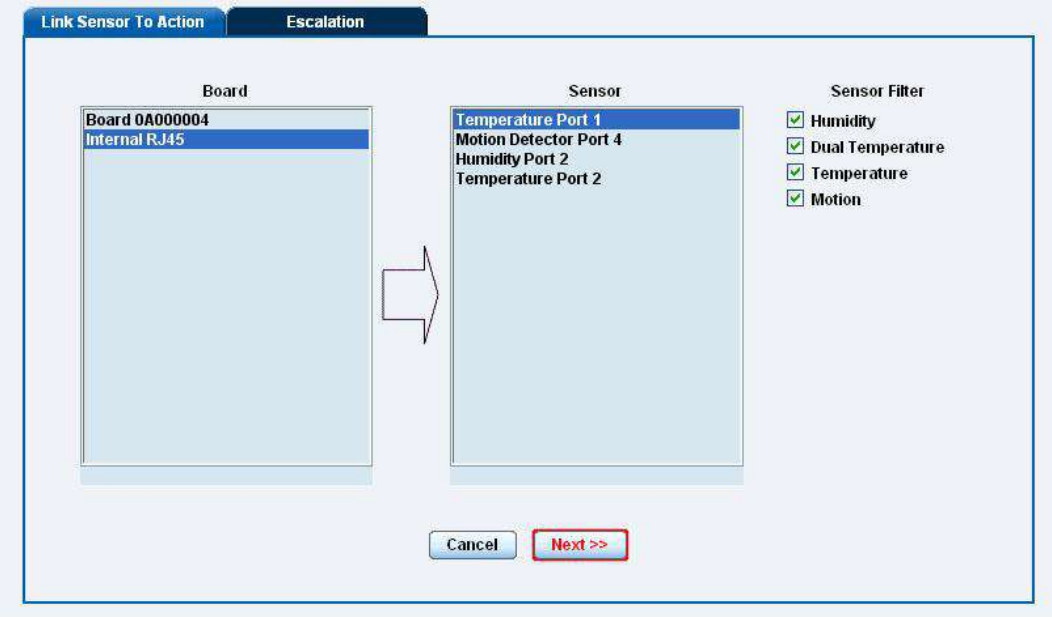


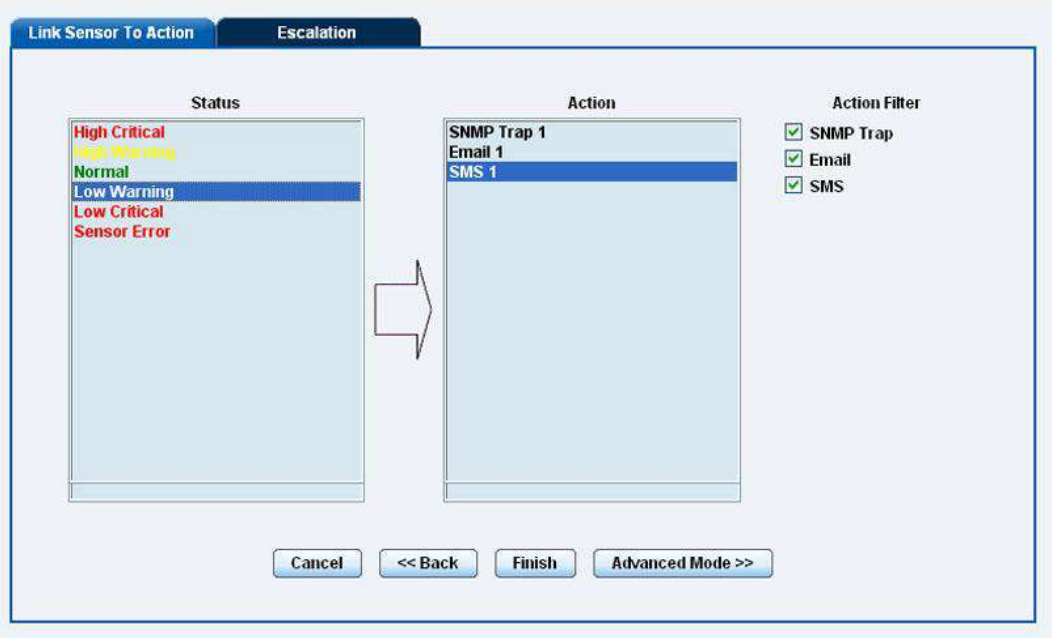
e) Next we will choose to set up the type of connection. This will depend on the type of modem you are connecting. For the purpose of this tutorial we will assume you are connecting a GSM/GPRS enabled modem to the serial port. Therefore we will select COM1 from the list.



f) You will now be able to select the number of times you wish the SMS to be resent and the interval between sending them.

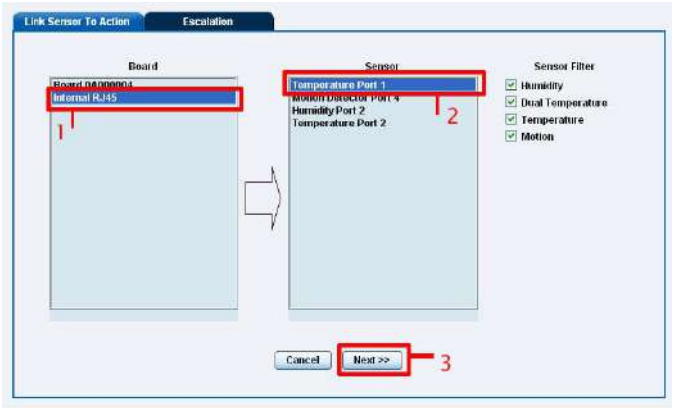
g) Again we now select the sensor to which to bind this notification too.



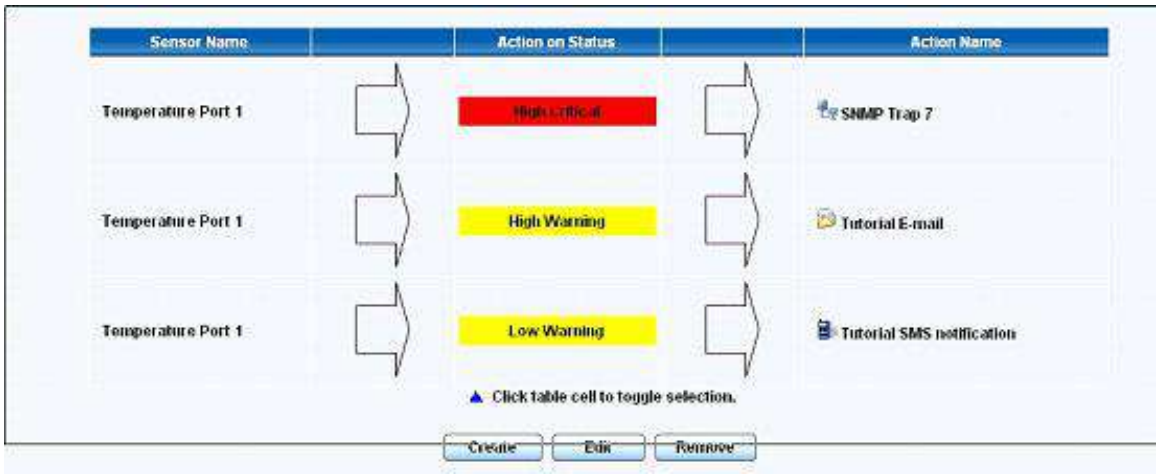


As before, select the Temperature sensor on port 1. This time we will use this notification for a low critical. Then select the notification name we assigned, in this case we chose “SMS 1”. Click Finish to finalize this.

h) Now we will add the SMS notification to our active list. This is the same process as for the others, simply click on create and then select the appropriate parameters.



j) You will now be back at the main notification page. Now the page should display three types of notifications, the SNMP trap, E-mail and SMS.



For the purposes of this tutorial we will not cover the set up of every type of notification. However, with this information you should be able to follow the procedure for the other types of notifications easily, as they all follow a similar format. If you still encounter difficulties with this then please contact us on support@akcp.com.

4) Camera

1. Basic setup

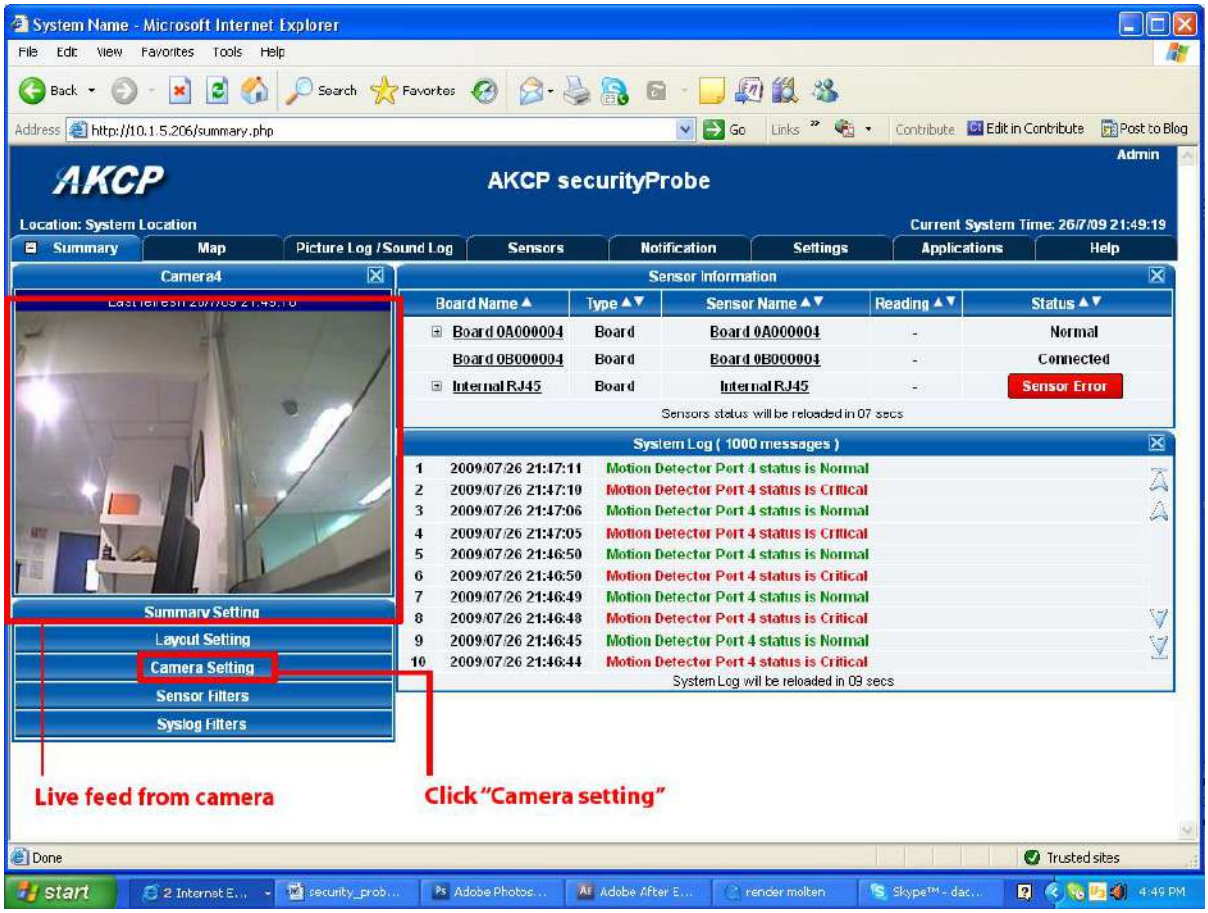
The unit will allow for connection of up to 4 cameras through the video inputs (V1 – V4). In this tutorial we are going to assume you are connecting an AKCP pan/tilt PTDC camera, and we are connecting it to port number V4.

This tutorial provides you the information needed to setup the camera functions.

To get to the starting point of this tutorial:

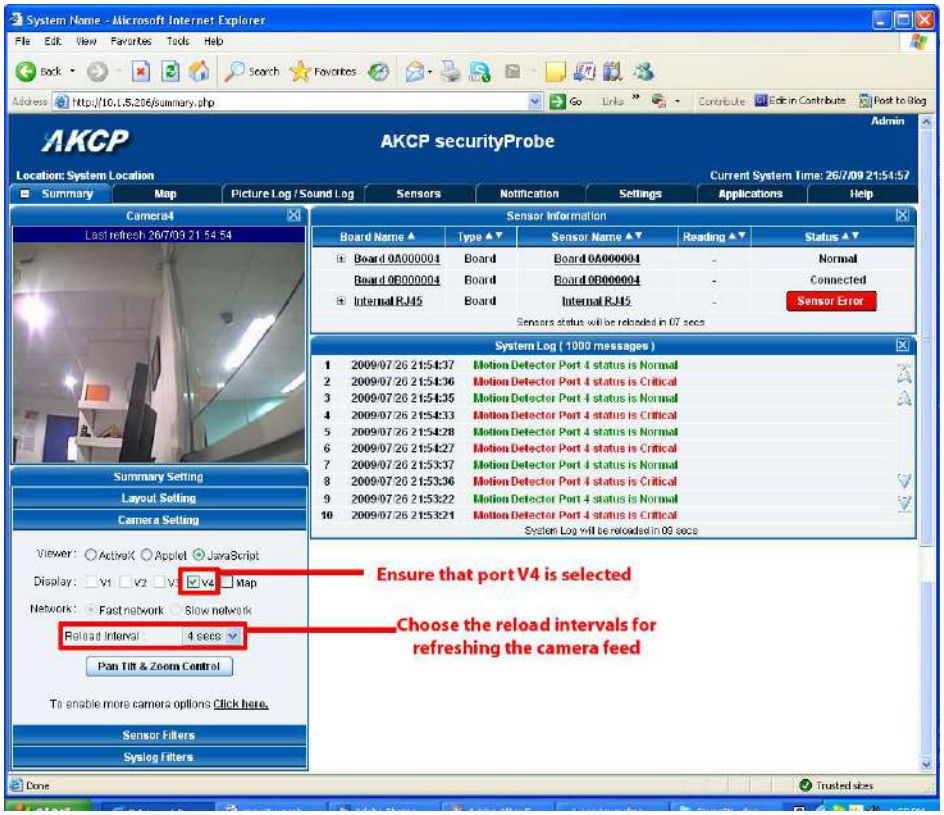
- Connect camera to a video ("V") port
- Log into web based interface as administrator

a) Once you are logged in you will be taken to the default "summary page".



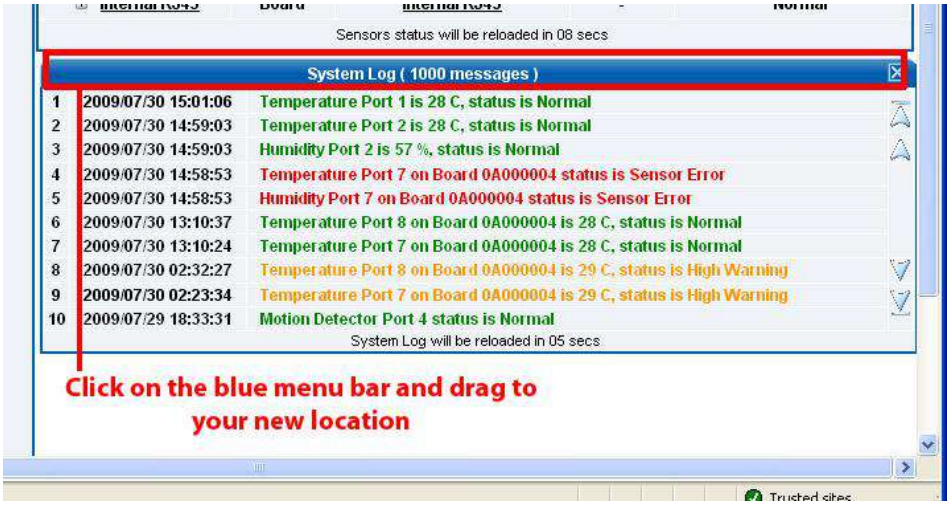
b) You may, or may not see the live image from the camera already. If not then click on Camera setting and follow the instructions below.

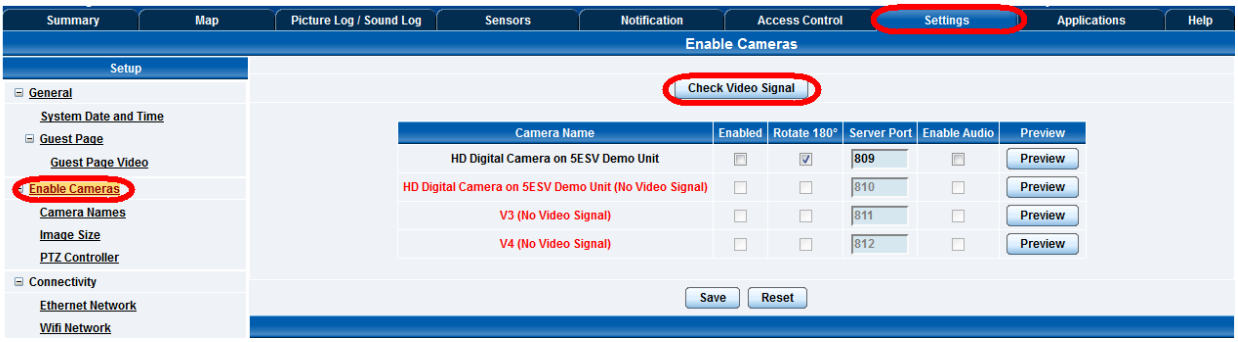
PLEASE NOTE: The ActiveX has been recently removed from the Camera Settings options in the Summery page, so your screen may appear differently.



Helpful hint

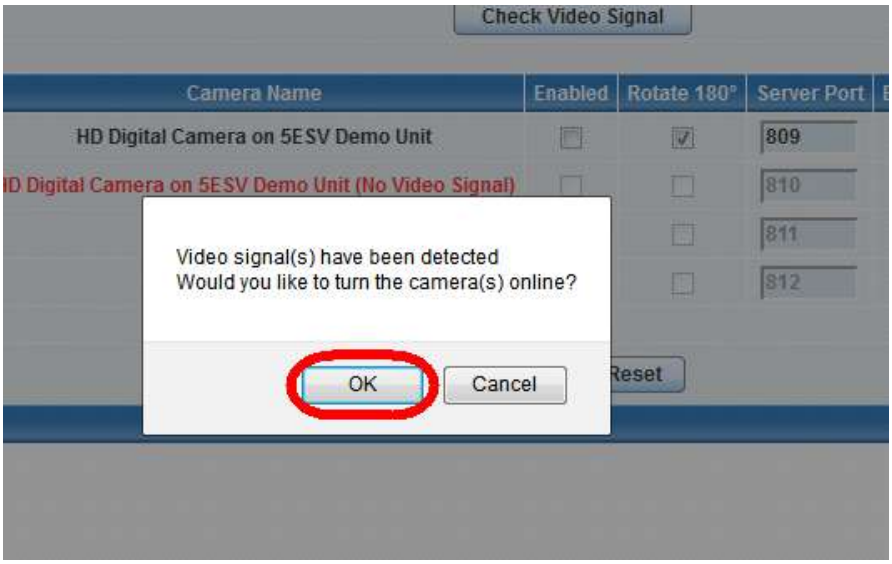
At this stage you will begin opening up multiple windows which my obscure valuable information displayed on the summary page. To prevent this from happening, each window can be dragged to a new position to accommodate your preferred layout. To achieve this follow the directions below.



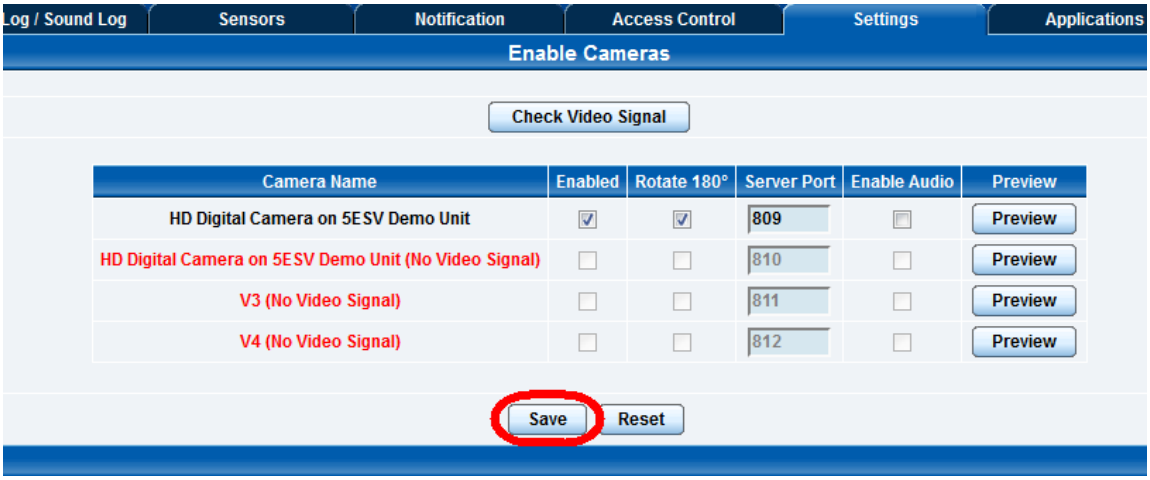


To check the cameras settings in the web interface you first need to go to the Settings page, then the Enable Cameras page.

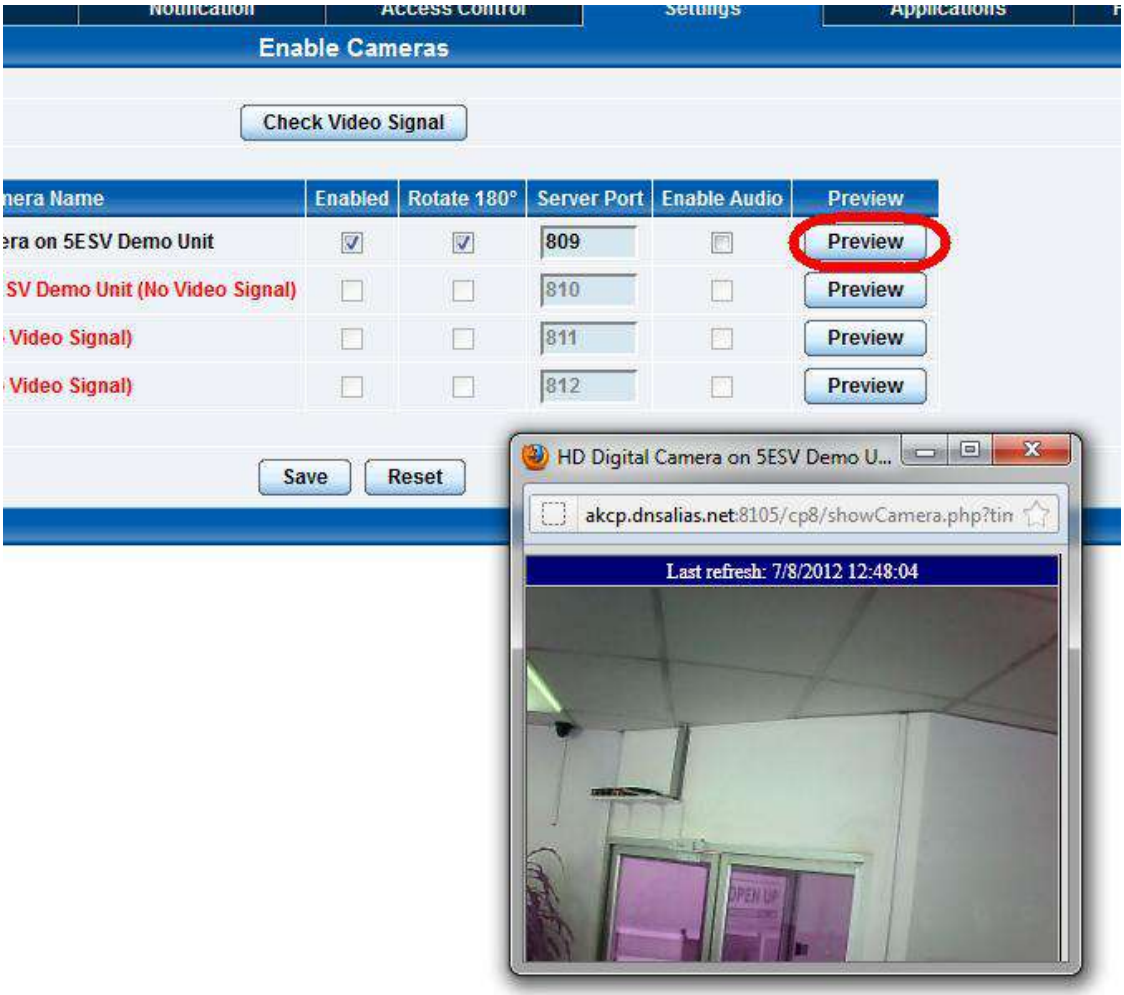
You can then press the Check Video Signal button to scan the camera ports on the unit for connected cameras.



After the camera or cameras are detected you will then see this pop-up message shown in the screen shot above. You can then click on the OK button.

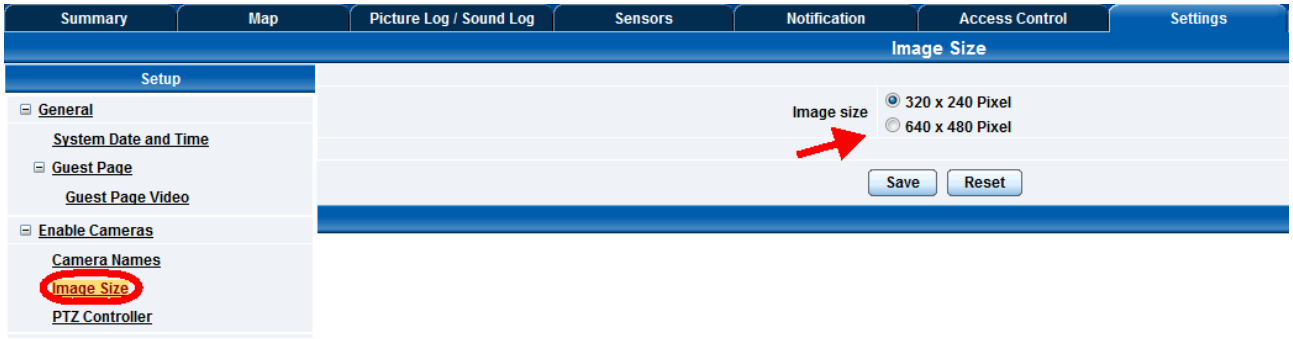


The cameras connected to the securityProbe 5E base unit will now show the check in the Enabled box as shown in the screen shot above.

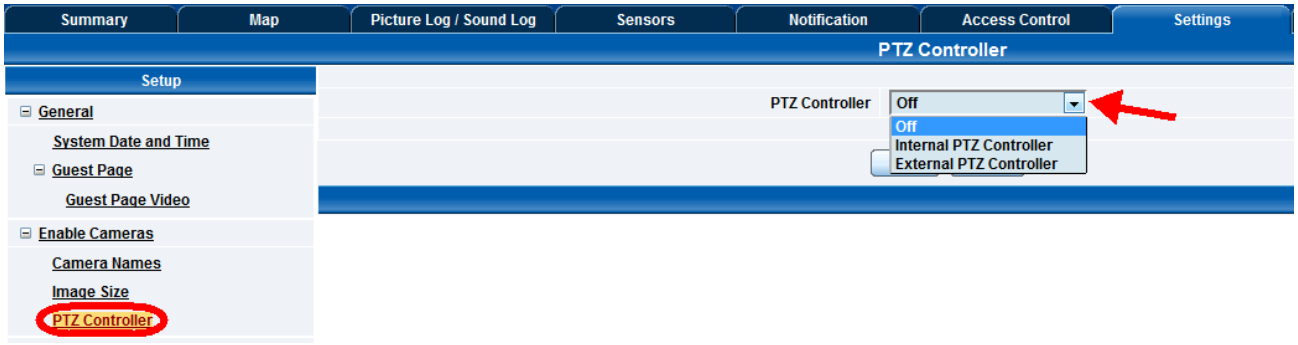


You can then check to make sure the video stream is working by clicking on the "Preview" button. If the image appears upside down, you can enable the "Rotate 180" setting to correct the image depending on how the camera is mounted.

After your cameras are enabled you can then name then as you require by first selecting the “Camera Names” link from the Setup column, then renaming the test in each of the V1-V4 description fields as shown in the screen shot above.

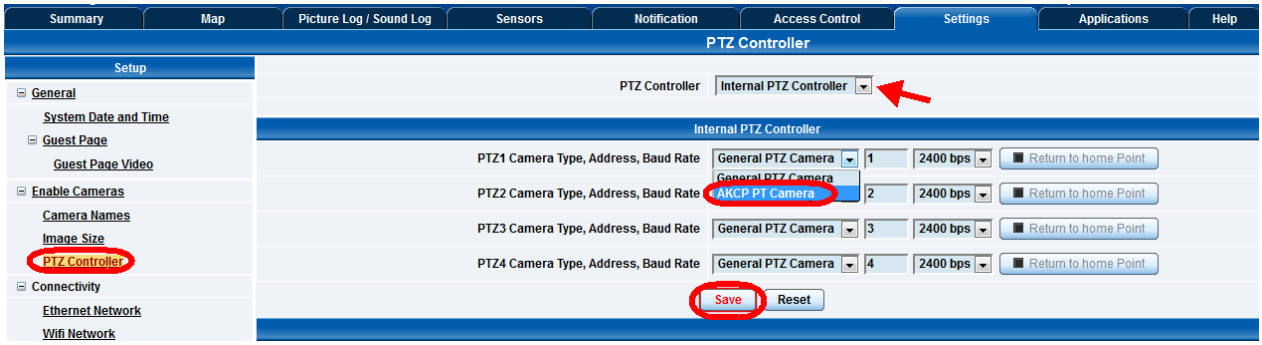


By clicking on the “Image Size” link in the Setup column you can then change the Image Size of the streaming video from your cameras to either 320 x 240 or 640 x 480. The streaming video Image Size will be displayed on the Summery page as shown in pages 61 and 62 above.



If you are using pan tilt cameras or other third party Pelco-D cameras then you will need to enable the PTZ Controller from the PTZ Controller page as shown above. You will always normally choose the “Internal PTZ Controller”

Note: The External PTZ Controller refers to an obsolete option where an external controller could be connected to the unit.



Now that the Internal PTZ controller is set, you need to select the correct camera type from the drop down list as shown in the screen shot above. If the cameras is an AKCP branded camera you will choose the AKCP PT Camera, if it is another third party Pelco-D type camera you will select the “General PTZ Camera”.

Note: For more information on the cameras, cable run lengths etc., please refer to the FAQ section at the end of this manual.

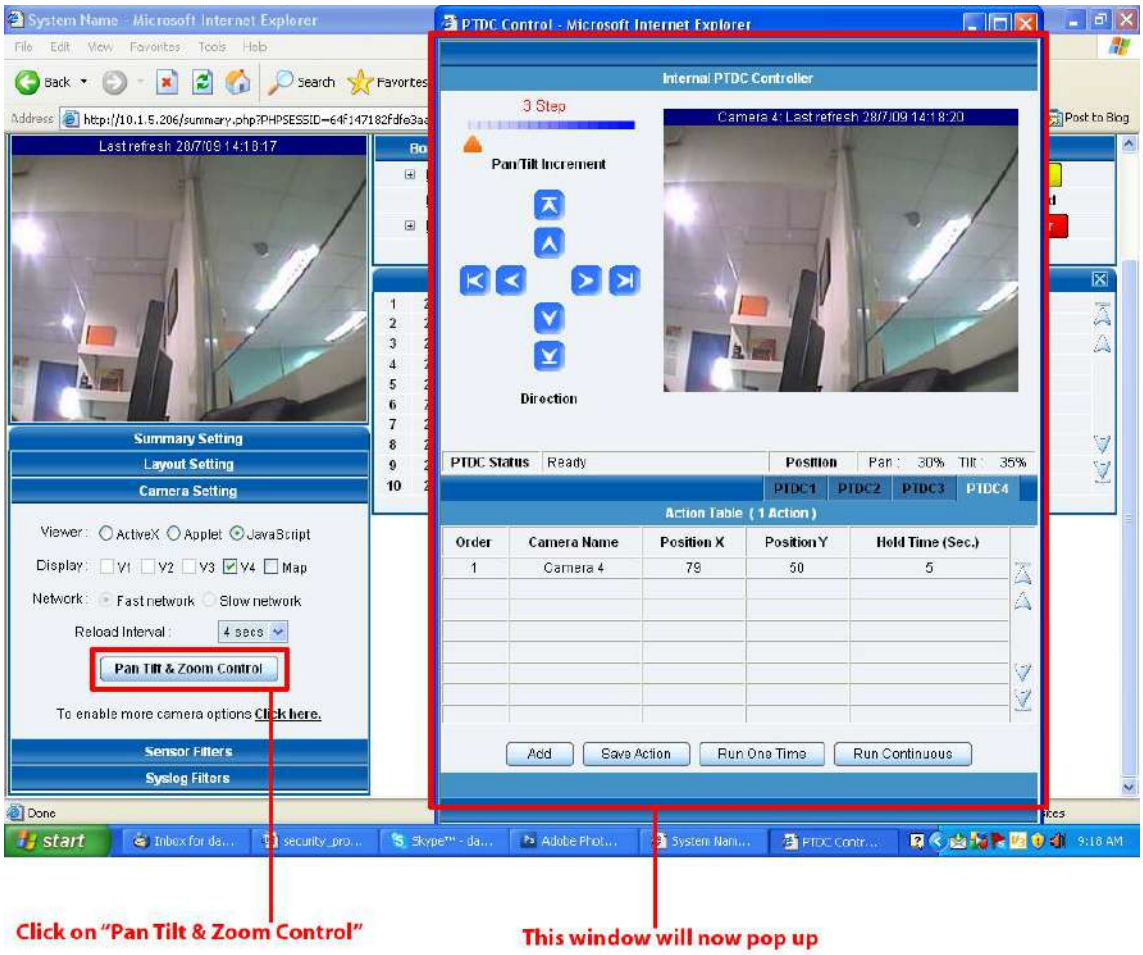
2. Pan / tilt functions of the camera.

This tutorial provides you the information needed to setup an MMS Notification.

To get to the starting point of this tutorial:

- Log in as administrator
- From summary page select options

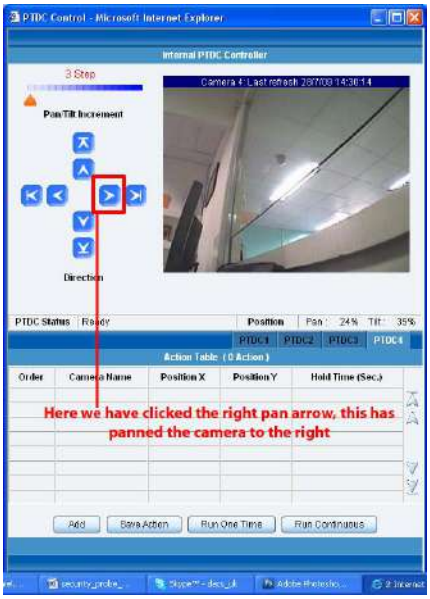
a) First, click on the “PTZ Control” button.



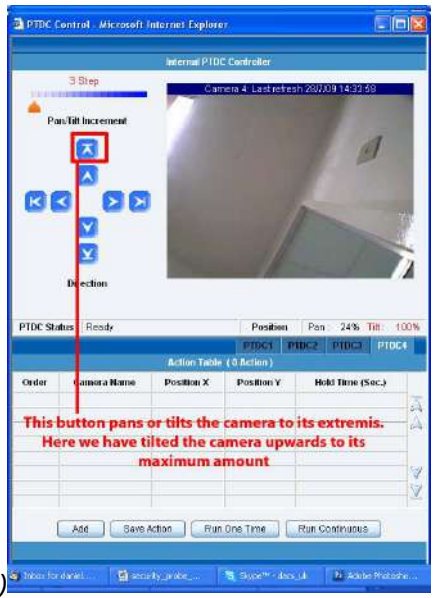
b) Now we can pan and tilt the camera by way of the pan / tilt arrows.

1)

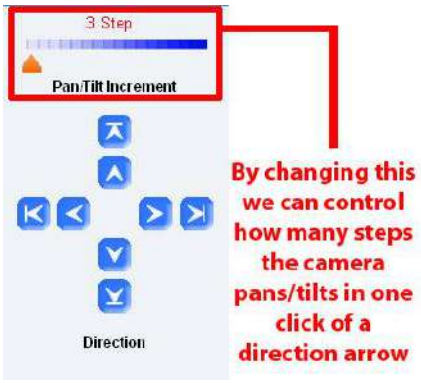
2)



3)



4)



Helpful Hint

You can also pan and tilt the camera by placing your mouse on the video image and clicking the position in which you would like the camera to face. This is useful when you want to enter the values for automated camera movements.

3. Automating camera movements

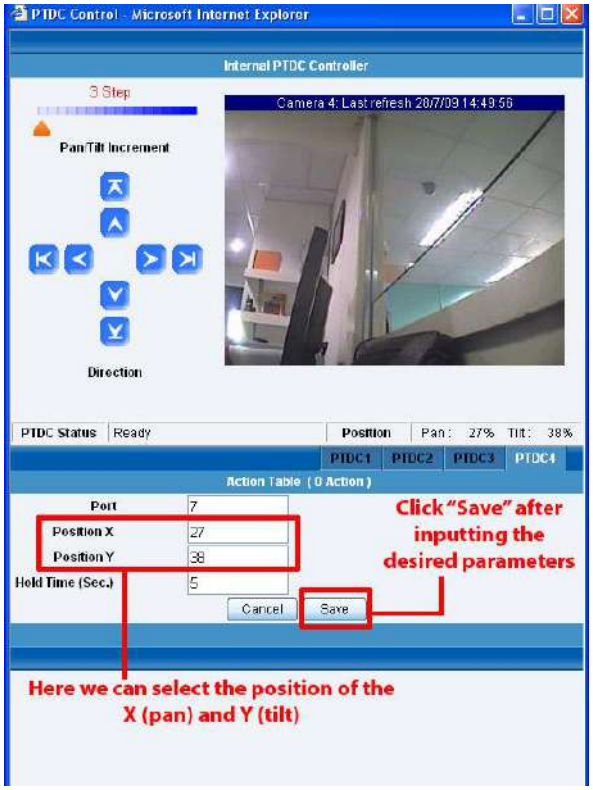
This tutorial provides you the information needed to setup automated camera movements.

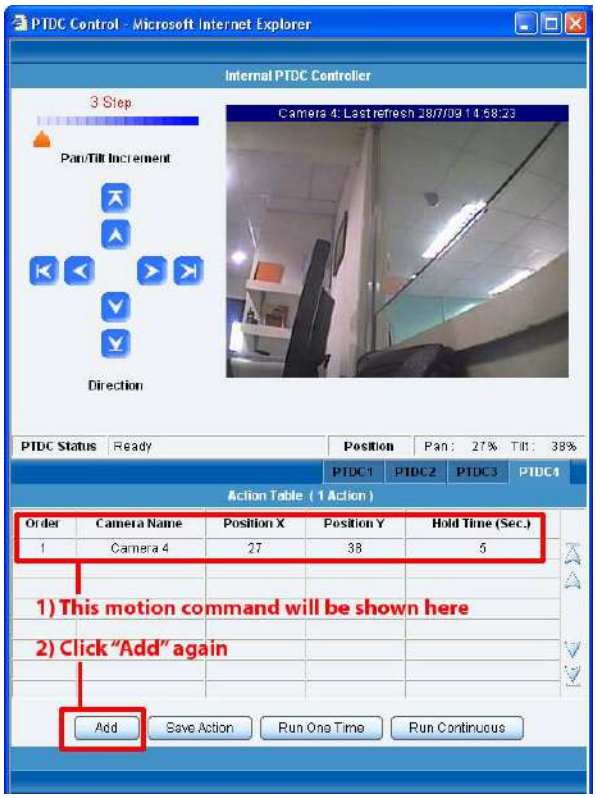
To get to the starting point of this tutorial:

- Log in as administrator
- Select options from the summary page
- Click Pan Tilt and Zoom control

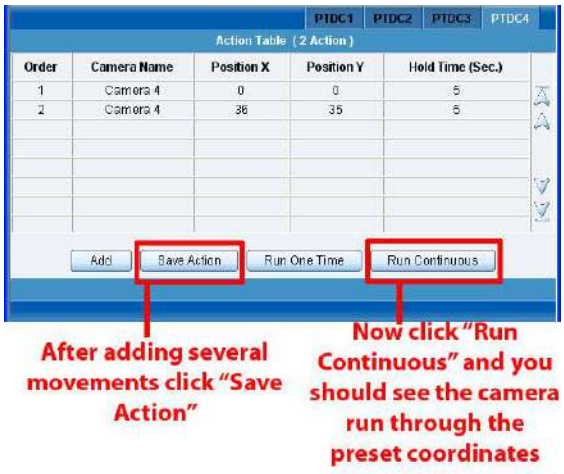
We will now look at creating an automated camera movement. This will make the camera automatically pan or tilt at preset intervals.

b) After clicking on the add button you will be met with the following pages





Repeat this process as many times as you wish to automate the cameras movement so that it covers the area you require too monitor. In this example we have added three different positions.



After clicking "Save Action", click on "Run Continuous". This will start the script running. You should then see instant feedback from the live stream in the camera window as the camera pans through these positions.

4. Recording from the camera

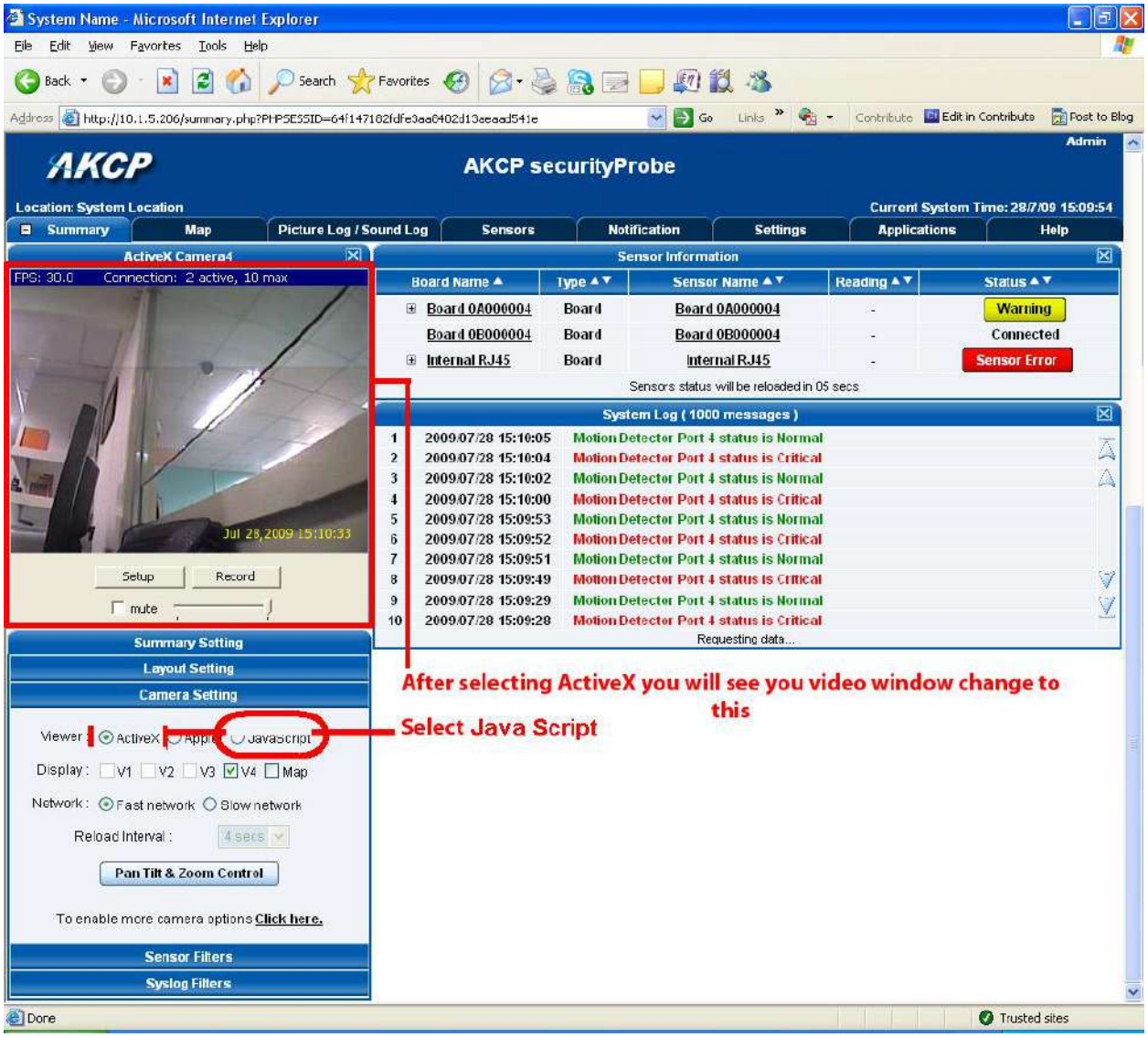
As the ActiveX has been removed from the Camera Settings page, to record from the camera please use the Java option. The web interface will direct you on how to do this. For this tutorial we will assume this is done.

This tutorial provides you the information needed to setup the recording from the camera.

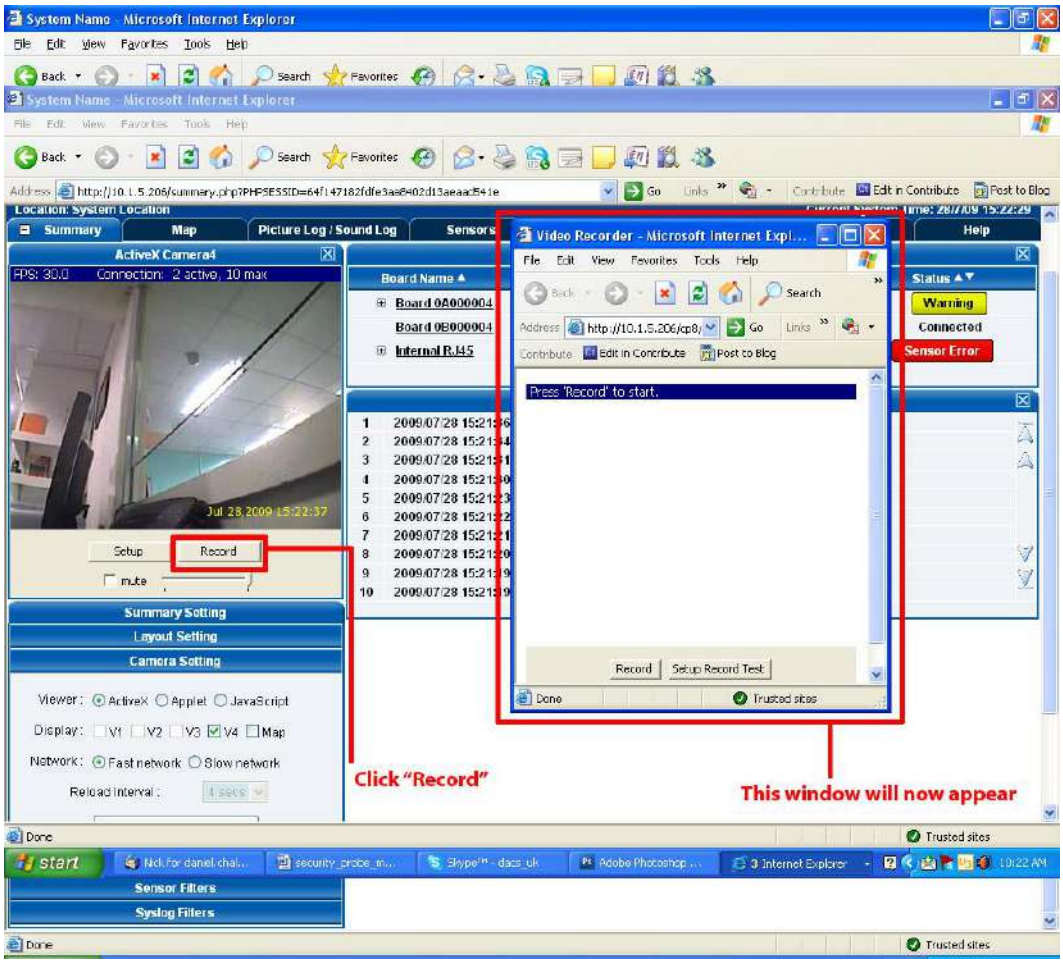
To get to the starting point of this tutorial:

- Log in as administrator
- From summary page select options

a) Select the Java Script as the mode of display.



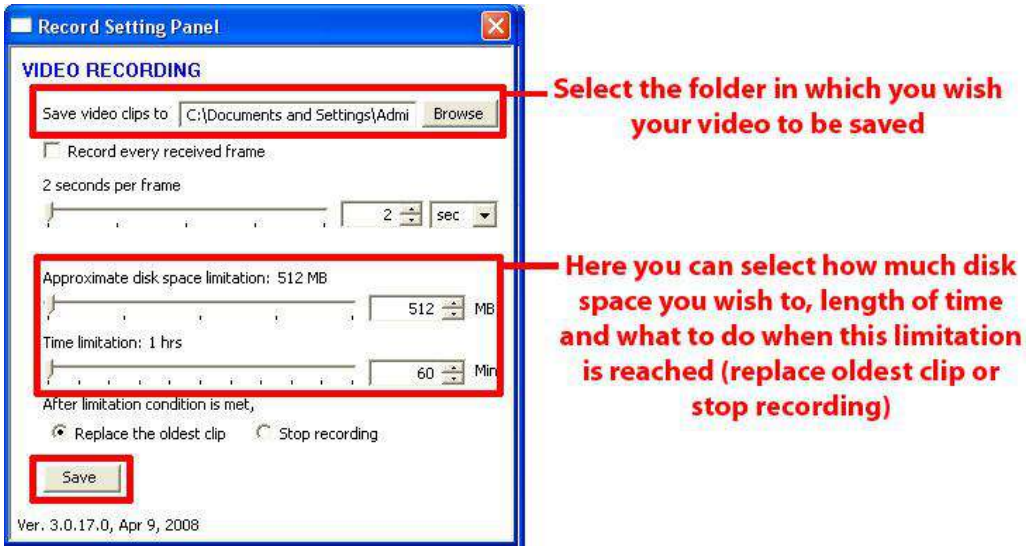
b) Click “Record” and the camera record window will now open.



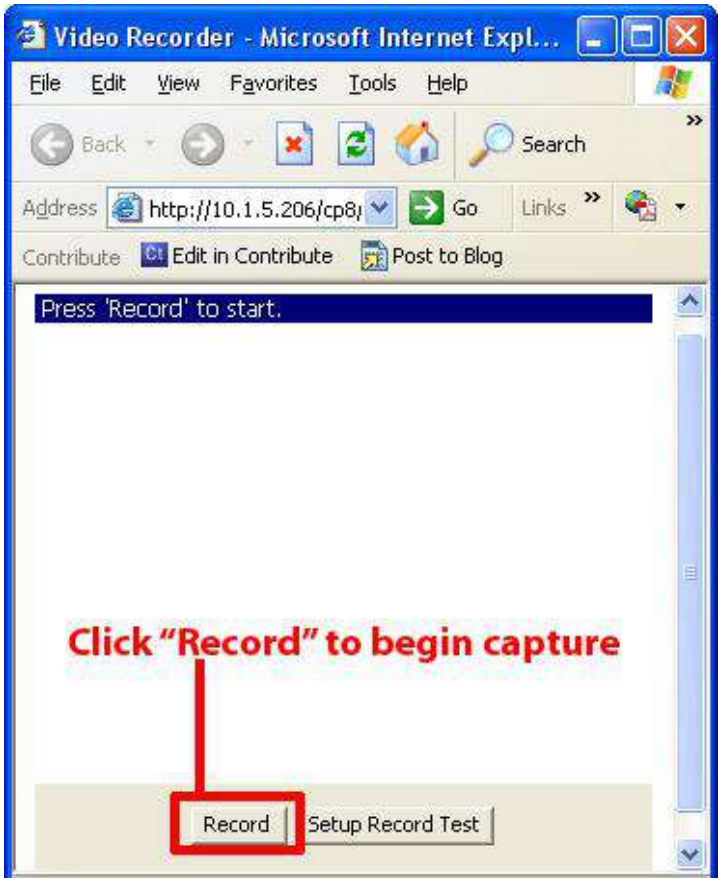
c) Now we need to set up the capture parameters. Click on “Setup Record Test”

1)

2)



d) To begin capture, simply click on “Record”.



Note: If you wish to record, and run the automated camera movement sat the same time, start the automated camera movements from the “PTZ Control”

5. Picture Log

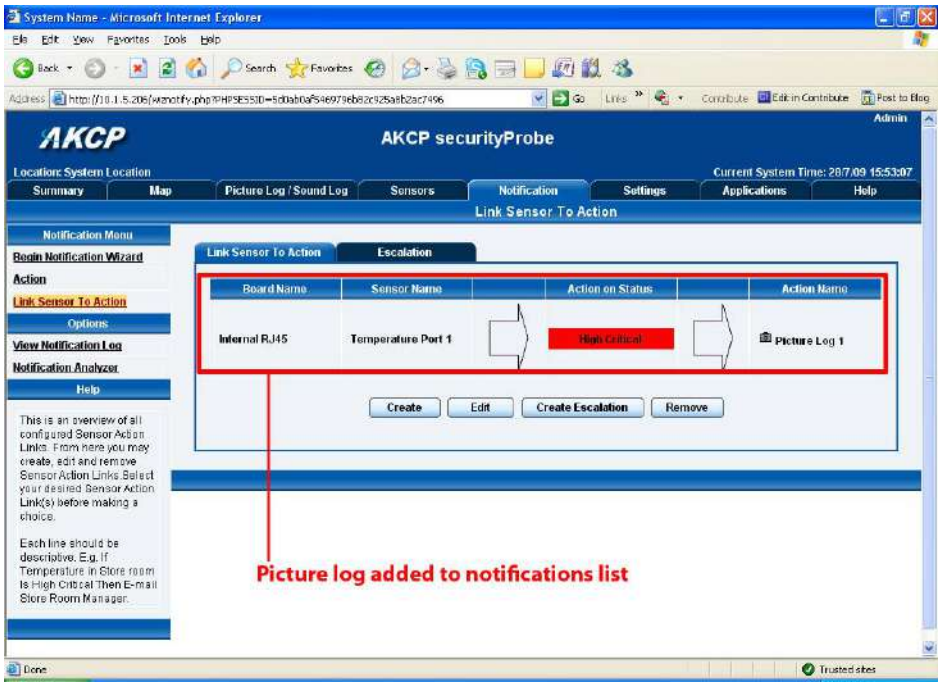
The camera can be used to automatically log a photo and send it as part of a notification. Continuing our example of setting up the temperature sensor in this part of the tutorial we are going to use the camera to capture an image from 2 seconds and 1 second before and 2 seconds after the event. The event will be when the temperature sensor reading is at “High Critical”.

This tutorial provides you the information needed to setup an MMS Notification.

To get to the starting point of this tutorial:

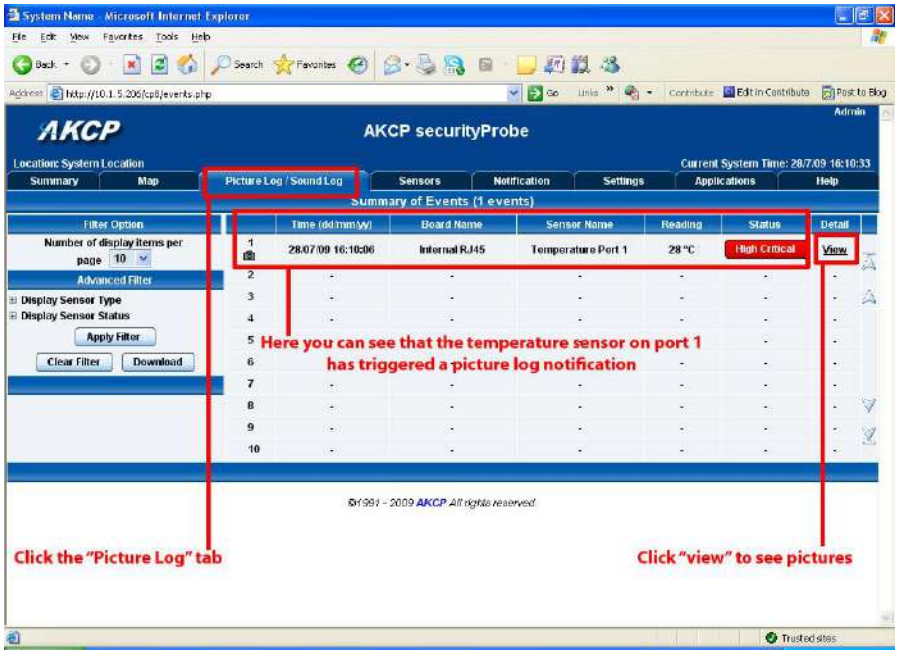
- Log in as administrator
- Select the notifications tab
- Select notification wizard
- Choose picture log as the notification type (follow previous notifications wizard instructions)

a) Once this is done you can add it to the active notifications so your page should now look like this:-

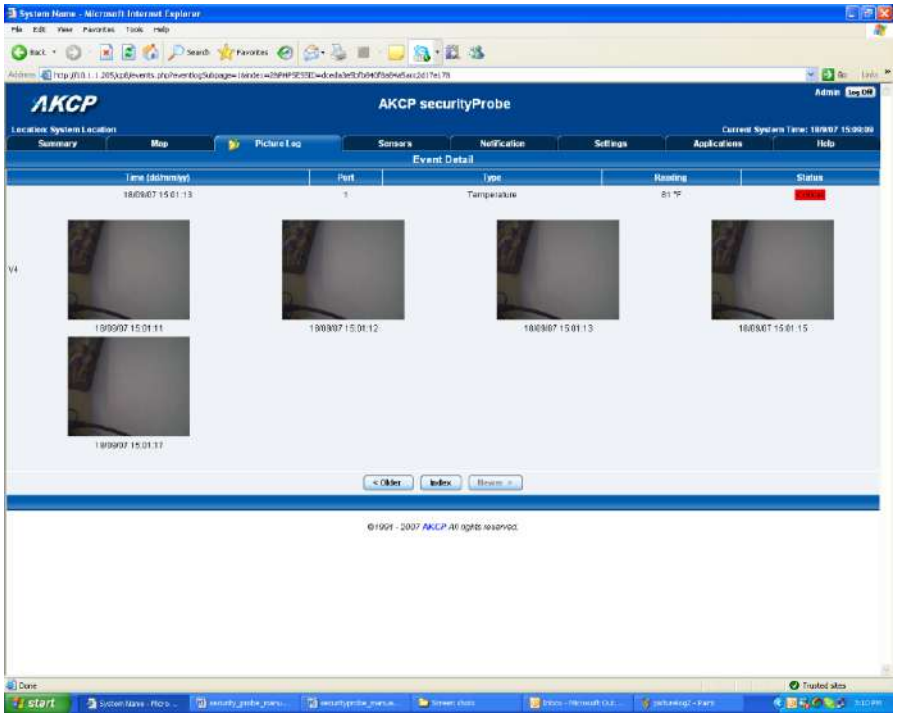


As you can see from the screen shot above, we have set the picture log to be created when the temperate sensor is at a “High Critical” state.

b) Adjust the notification thresholds in order to trigger a response. This has triggered the picture log notification.



c) Viewing the logged pictures.



Form here you can see there is a series of images. These have been taken at the preset time intervals, before and after the event. These parameters were set up in the notification wizard previously.

6) Mapping

The mapping feature allows for an instant visual feedback as to a sensors position, and status. It is a useful monitoring tool for a set up with several sensors in different positions.

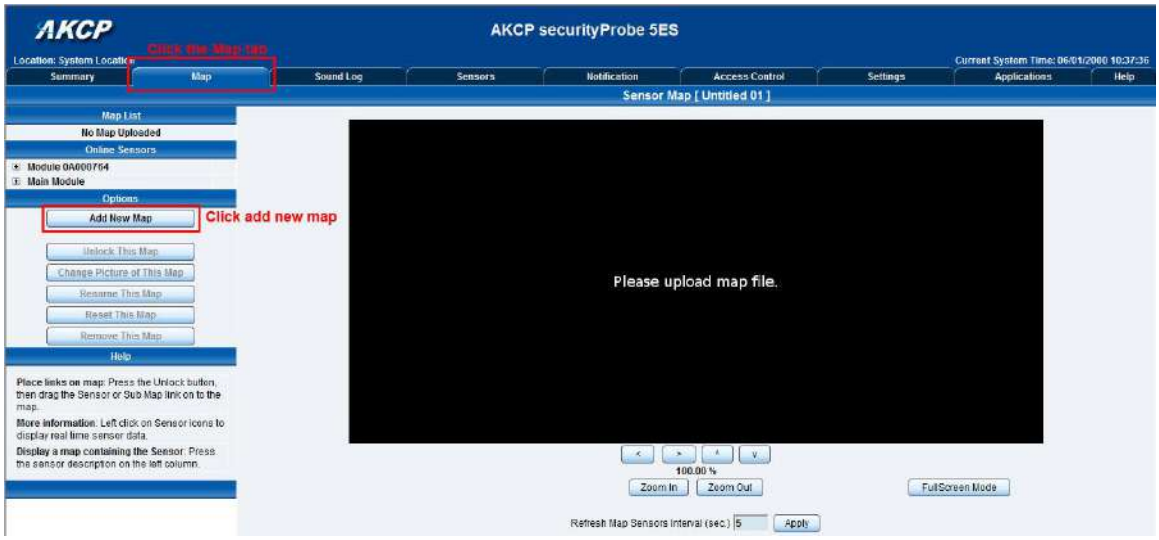
This tutorial provides you the information needed to setup the mapping feature.

To get to the starting point of this tutorial:

- Log in as administrator
- Click the “map” tab

1. Adding a map

a) First we need to add a picture file to be used as the map. This can be a blueprint of your office, a 3D picture of your office/site being monitored, or a photo of the wiring closet you are monitoring.

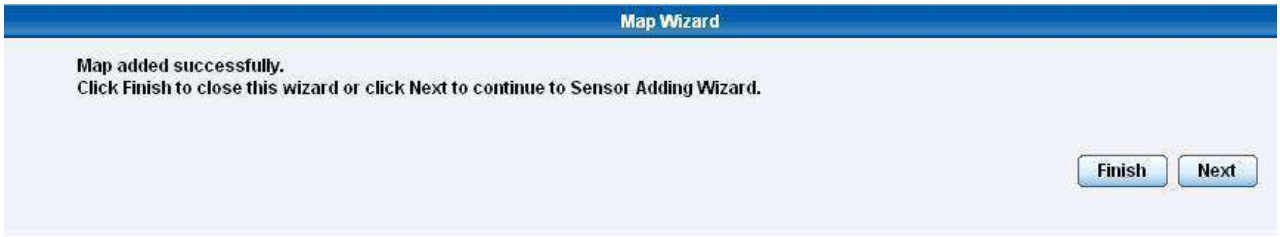


b) Now you can browse to the file on your HDD you wish to use.

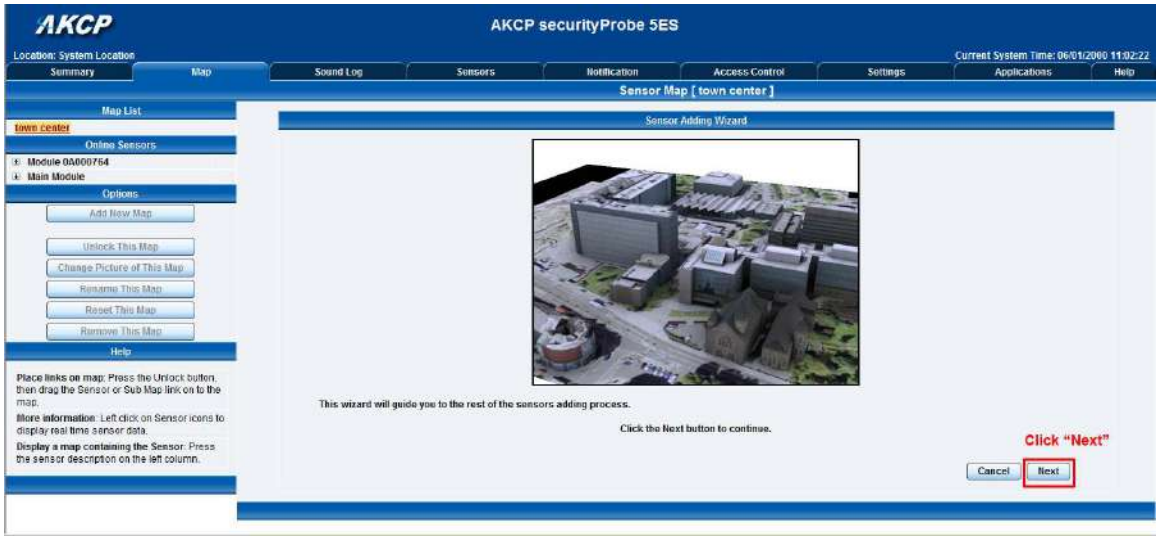
c) In this tutorial we are going to use a 3D map of a town center we are monitoring.

d) Choose to have the map as a top level map.

e) You will now have the option to finish or to continue adding your sensors to the map. For this tutorial, click next.

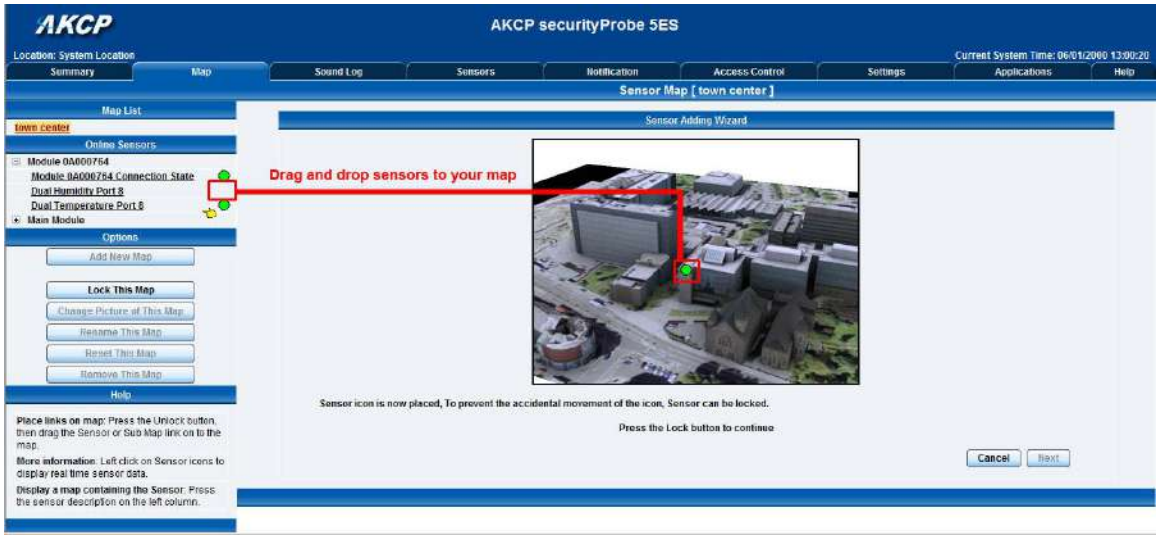


f) You will now be taken to the map page where it will display your map. To continue adding the sensors click next.

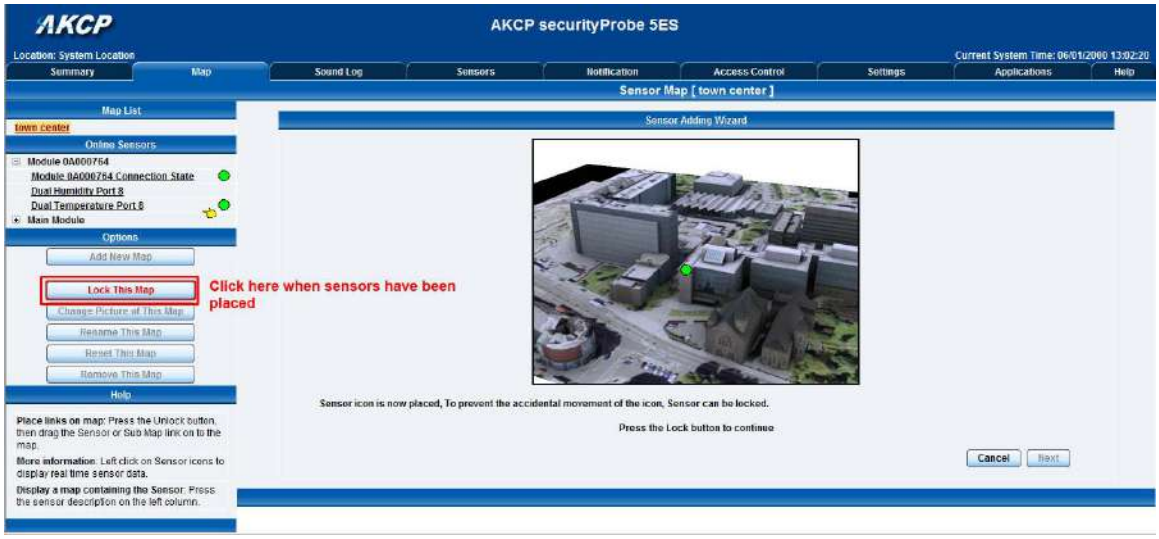


g) After clicking next you will be directed to click the "Unlock" button.

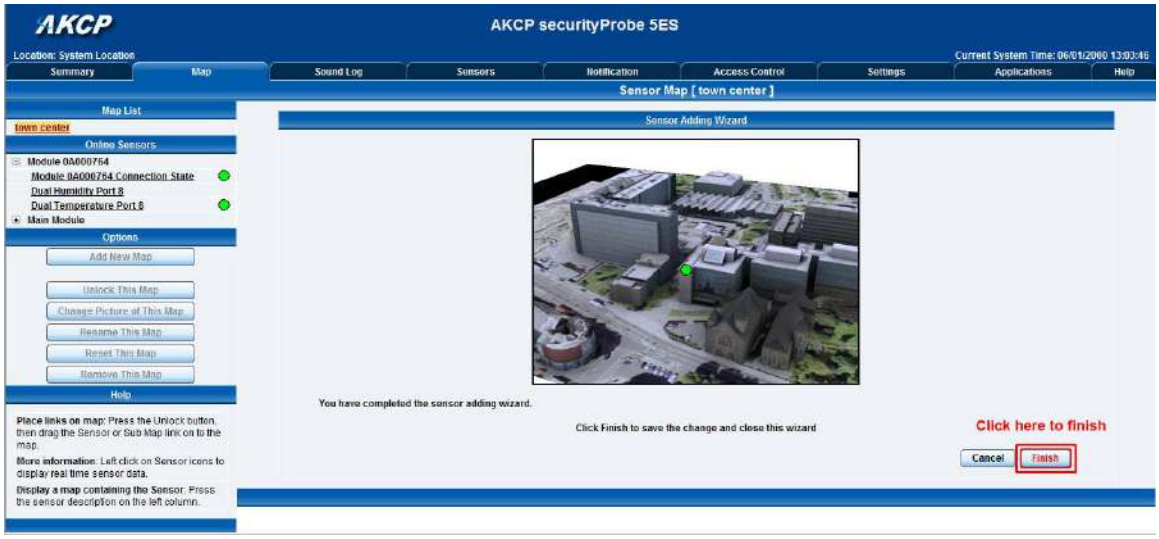
You can now drag sensor icons and position them on the map



i) After you have positioned the sensors in the correct location of your map click on “Unlock”



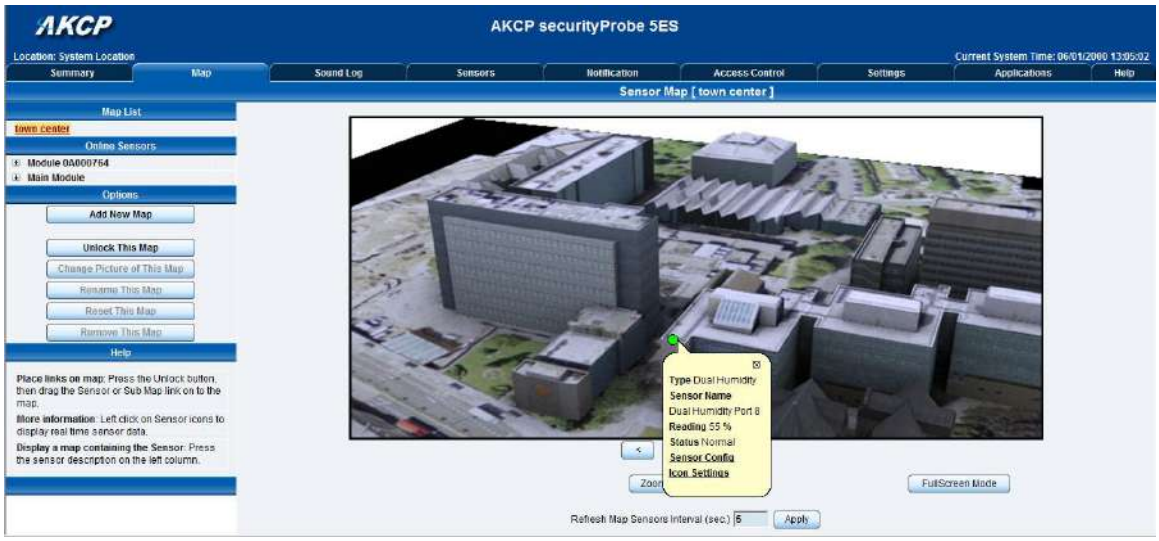
j) Finally you click on the “Finish: button to save your changes



2. Monitoring via the map interface

Now we are going to look at how to monitor the sensor status and use the map interface.

a) To see further information regarding a sensor you can click on its icon. First you must click on the “Lock Icons” button.



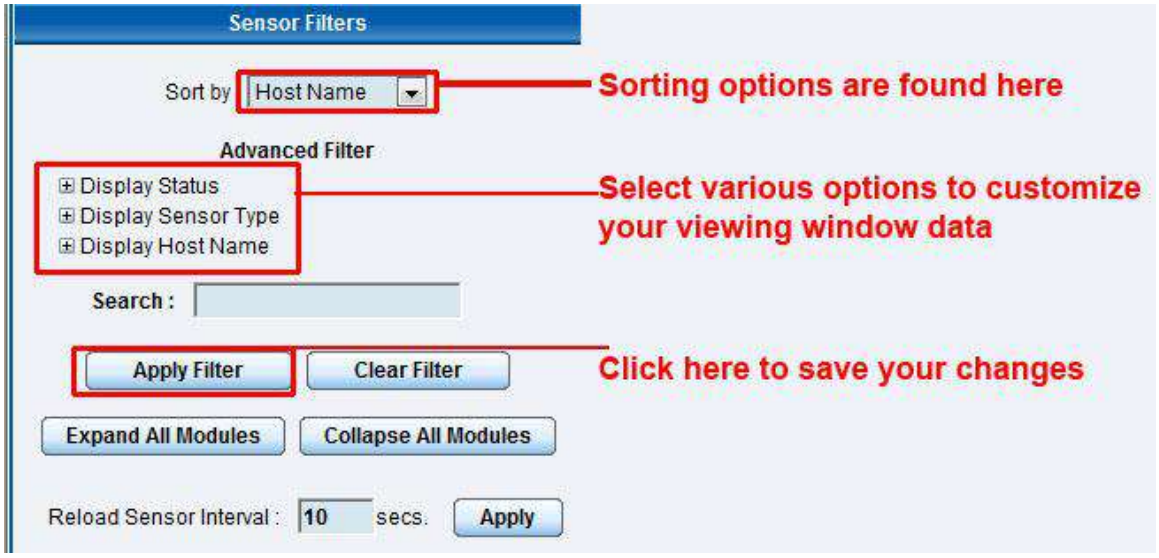
If you connect other sensors, these too can be dragged and positioned on the map.

6) Filters

1) Sensor filters

The module now comes equipped with the option to filter your sensor information which is displayed within the summary page. To enter the filter menu, select “Sensor Filters” from the dropdown tab on the left of the page:-

Once you have clicked the tab you will be able to select your filter results by altering various fields of information contained within sensor filter window:-

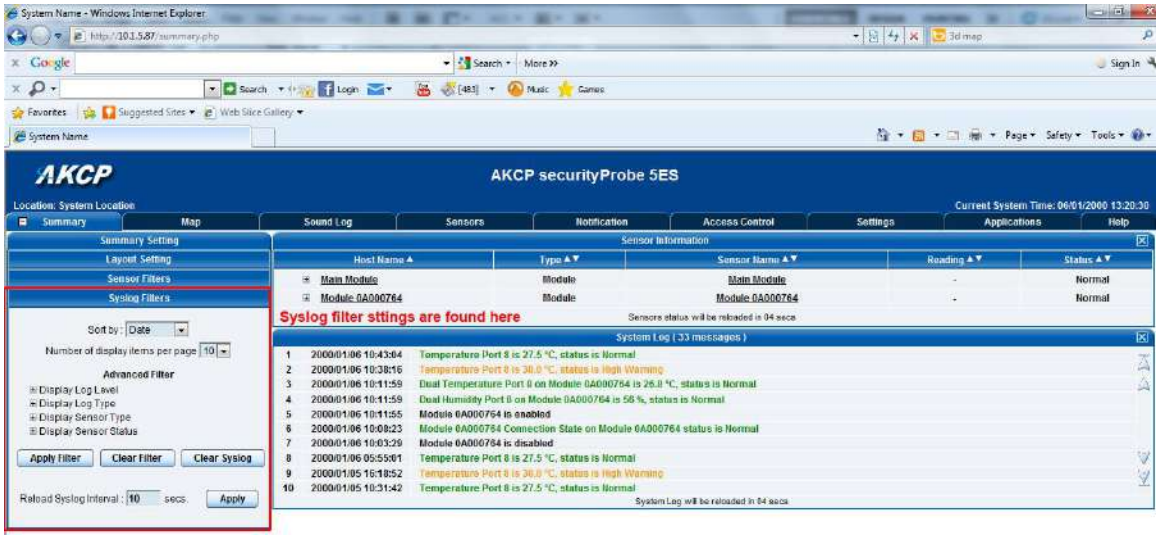


Altering your page reload interval can be achieved by using these options shown below:-

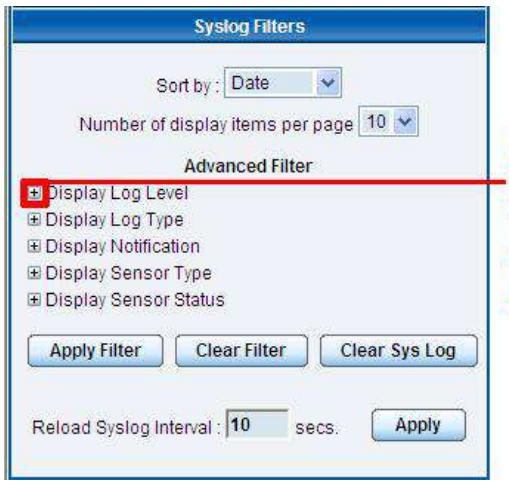
Once you have selected your preferred filter options, your new settings will be displayed in the "Sensor Information" window found on the summary page:-

2) Syslog filters

Syslog filters enable you to customize your syslog window. To begin select the “Syslog filter” tab found on the summary page:-



Once you have clicked the tab you will be able to select your filter results by altering various fields of information contained within syslog filter window:-

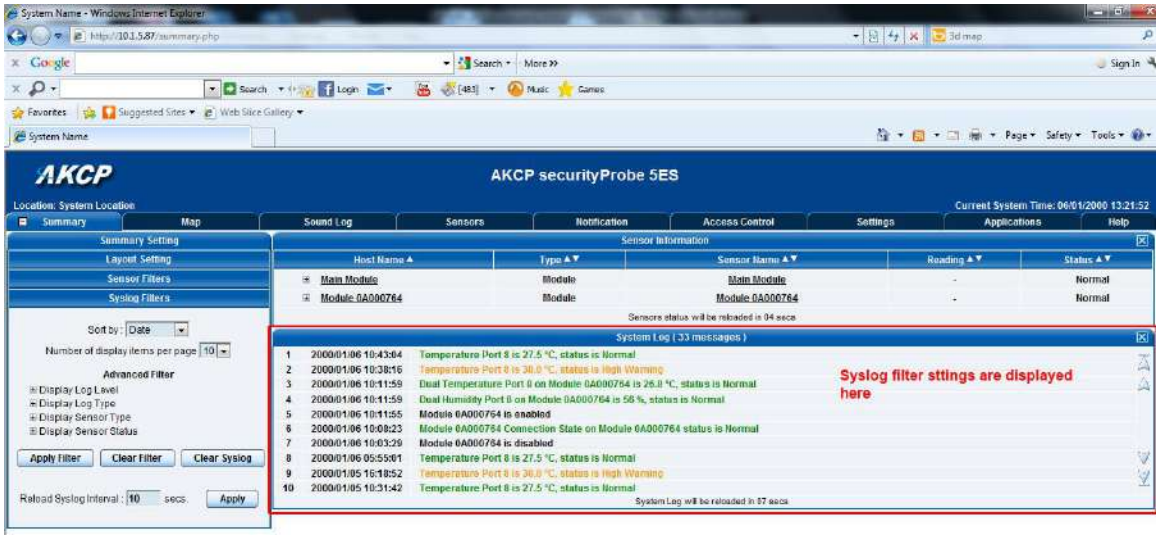


By clicking on the “+” sign, a drop down list of options will be come available.

By checking and un-checking various boxes within the Syslog filter window you can customize your displayed results contained within the syslog filter.

Altering your reaload interval can be achieved by using the options shown below:-

Once you have selected your preferred filter options, your new settings will be displayed in the "System log Information" window found on the summary page:-


AKCP securityProbe 5ES
Location: System Location
Current System Time: 06/01/2000 13:21:52
Summary
Map
Sound Log
Sensors
Notification
Access Control
Settings
Applications
Help
Summary Setting
Layout Setting
Sensor Filters
Syslog Filters
Sort by : Date
Number of display items per page 10
Advanced Filter
Display Log Level
Display Log Type
Display Sensor Type
Display Sensor Status
Apply Filter
Clear Filter
Clear Syslog
Reload Syslog Interval : 10 secs.
Apply
Sensor Information
Host Name
Type
Sensor Name
Reading
Status
Main Module
Module
Main Module
Normal
Module 0A000764
Module
Module 0A000764
Normal
Sensors status will be reloaded in 04 secs
System Log (33 messages)
1 2000/01/06 10:43:04 Temperature Port 8 is 27.5 °C, status is Normal
2 2000/01/06 10:38:16 Temperature Port 8 is 30.0 °C, status is High Warning
3 2000/01/06 10:11:59 Dual Temperature Port 8 on Module 0A000764 is 26.8 °C, status is Normal
4 2000/01/06 10:11:59 Dual Humidity Port 8 on Module 0A000764 is 56 %, status is Normal
5 2000/01/06 10:11:55 Module 0A000764 is enabled
6 2000/01/06 10:09:23 Module 0A000764 Connection State on Module 0A000764 status is Normal
7 2000/01/06 10:03:29 Module 0A000764 is disabled
8 2000/01/06 05:55:01 Temperature Port 8 is 27.5 °C, status is Normal
9 2000/01/05 16:18:52 Temperature Port 8 is 30.0 °C, status is High Warning
10 2000/01/05 10:31:42 Temperature Port 8 is 27.5 °C, status is Normal
System Log will be reloaded in 57 secs
Syslog filter sttings are displayed here

7) Making my unit visible on the internet

So far the manual has simply covered the basic set up. The setup we have just created will allow you to access your unit on a Local Area Network (LAN), monitor via the web based interface or with SNMP traps.

However, what if you wish to be able to remotely access your unit from anywhere in the world? This is possible; however, the following steps are only an outline guide. Your exact setup and configuration will often depend on your network equipment. You are going to need access to your router, if you are using one, and knowledge of whether your IP address is static or dynamic.

1) Simple setup

a) Lets imagine that your unit is connected to a router on your network, and the following IP addresses are assigned.

Your units IP address is the default 192.168.0.100.

Your computers IP address is 192.168.0.200

Your routers IP address is 192.168.0.300

b) To find out your routers external IP address go to www.whatsmyip.com

Lets imagine your routers external IP address is 278.67.04.09

c) You now need to setup port forwarding on your router. This varies depdning on your routers model. Generaly you need to point your browser to your routers IP address (in this case 192.168.0.300). This will then allow you to log into your routers administration interface. You can find how to go about doing this for your router on www.portforward.com For an example of how to do this for a commonly used router follow this link :- http://www.portforward.com/english/routers/port_forwarding/Linksys/WRT54G/HTTP.htm

You need to setup your routers HTTP forwarding to port 80. This will then mean when you access your router using the external IP address you will be forwarded to your units internal IP address.

d) To test this, open your web browser, and go to your external IP address (in our example 278.67.04.09). If your using a dynamic IP address, its best to check it again before doing this as it may have changed since the start of this tutorial.

e) To make this easier you could use a dynamic DNS (Dynamic Name Server). This means you no longer need to remember IP address's or use www.whatsmyip.com to find out your IP address. You will instead register a domain name (for example mysensorProbe2.homeip.com). This will then automatically point your routers external IP address (e.g. 278.67.04.09). This will require you to register the domain name and open an account with a DNS server provider. We recommend www.dyndns.com as they allow up to 5 free domain names to be registered.

f) If you have set everything up correctly you will now be able to access your unit from anywhere in the world by simply pointing your web browser to your DNS address.

FAQ & Trouble Shooting

1) I cannot see the temperature sensor displayed on summary page

2) I can not access my units web based interface

3) What do my LED lights mean?

4) I have forgotten my units IP address

5) I have forgotten the password for my unit

6) Can I use DHCP to assign my units IP address?

7) How do I set up my routing table?

8) How can I change my administrator password?

9) What functions do different types of notifications provide?

10) Can I connect my unit via WiFi?

11) What is the heartbeat message?

12) What is the Network Sniffer?

13) Can I use the unit to make video conferencing calls?

14) My securityProbe unit will not seem to boot up normally and the LED's are circling around counter clockwise what should I do?

15) After I finished the firmware upgrade I don't see any sensors connected to my unit in the web interface any longer. What could be the problem?

16) I just noticed this "Mega SPI Error" in my securityProbe's web interface. What is the problem? How do I clear this?

17) I am seeing "Database Locked" errors entries in the syslog on my securityProbe unit, what should I do?

18) My securityProbe unit keeps rebooting after I updated a firmware update failure. What happened and what can I do?

19) I have some problems with securityProbe. The following things are not working: When setting a virtual sensor online, the „Configuration "button is missing (several browsers tested) The Restore Original Settings" is not working Clear All User Data and Restore Original Settings" is not working

20) I am having problems with the unit but not sure what to do next?

21) On your specs it shows the same resolution on both HD and non HD camera's. What is the difference?

22) What are the differences between the securityProbe 5E, the securityProbe 5ES and the securityProbe 5E?

23)How long can the cameras be extended?

24) ~~Does the new camera have the cable incorporated into it and what is the length of that cable?~~ (not applicable to this model)

25~~) What if I need to extend the cameras further than 5 meters? Can I purchase what I need from you?~~ (not applicable to this model)

~~26) What if I need to extend the cameras further than 15 meters? Can I use the older digital cameras you offered before that connect to the SEC-5E BNC/RG-6 connectors? Can I use BNC-to-USB adapters?~~ (not applicable to this model)

27) Is this option a separate board or unit similar to your expansion units?

28) If I order this option will I be able to connect other types of third party cameras as I did with my SEC-5E?

29) I noticed on the data sheet the 5ESV now ships with 2 expansion ports instead of 4. Does reducing the expansion ports also reduce the total number of sensors that can be connected to the SEC-5E?

30) Can I add my own SD flash card to the unit? If so how large can I use and what is then stored on the SD card?

31) I noticed you have a different firmware for the securityProbe 5E and the SEC-5ES base units, will there be another separate firmware for the SEC-5E?

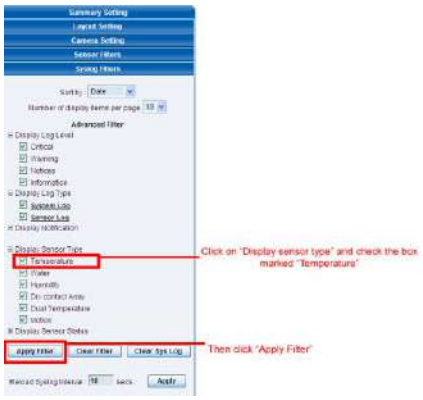
32) Speaking of firmware, do I need a separate firmware version or file if my unit has the X20 or X60 dry contact inputs? For example my SEC-5ES-X20 or my SEC-5E-X60?

33) Can I still use the same USB modems that worked or work on my securityProbe, my SEC- 5E and 5ES base units?

34) Will all the sensors that work on my SEC, SEC-5E, SEC-5ES work on the new SEC-5E base unit?

1) I cannot see the temperature sensor displayed on summary page

If after logging in for the first time with the temperature sensor connected, you may need to do the following:-



Next click on apply filter. The temperature sensor should then be displayed in the list of connected sensors.

2) I cannot access my units web interface

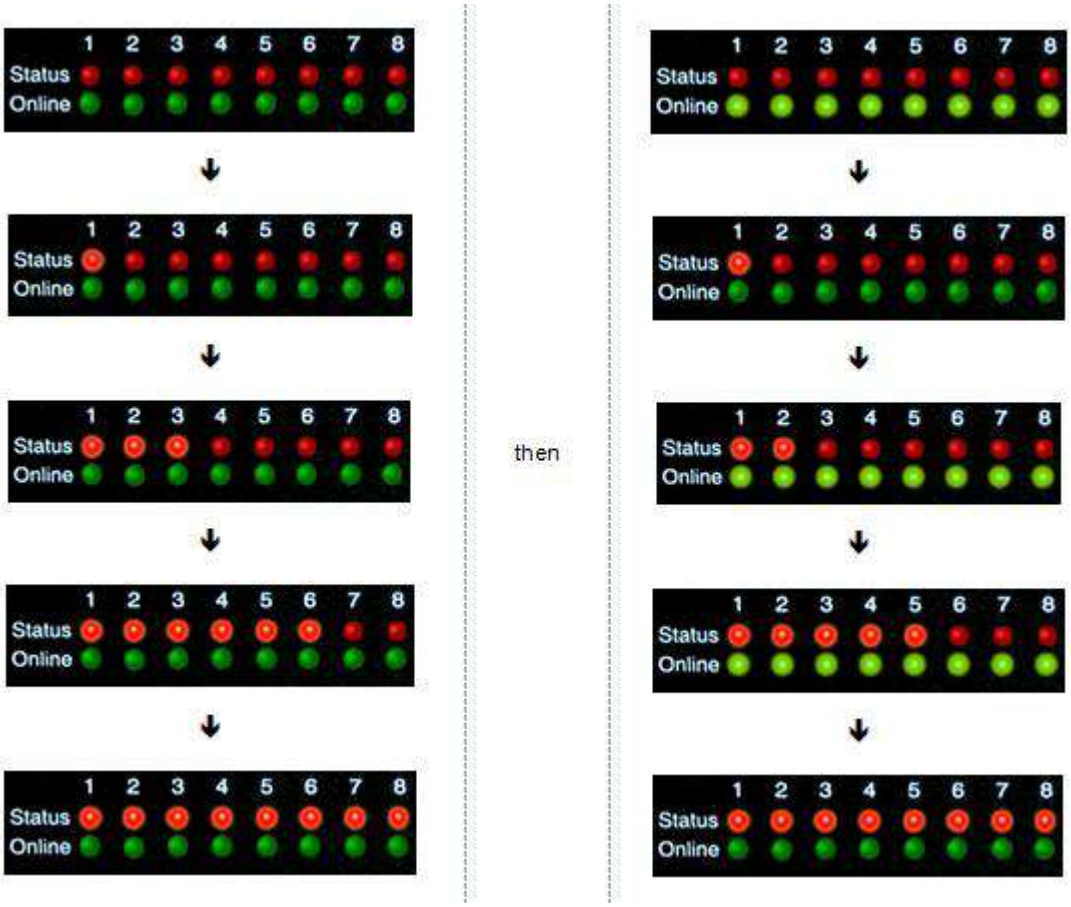
If you're having issues with network connectivity, first ensure that the link100 LED is lit on the front display of the unit. If this is not lit then you have no network connection present. If this is the case then ensure the following :-

1. If connected directly to a PC ensure a good quality crossover cable is being used
2. Ensure a standard CAT5 Ethernet cable is being used to connect to your network
3. See below for more trouble shooting on this.

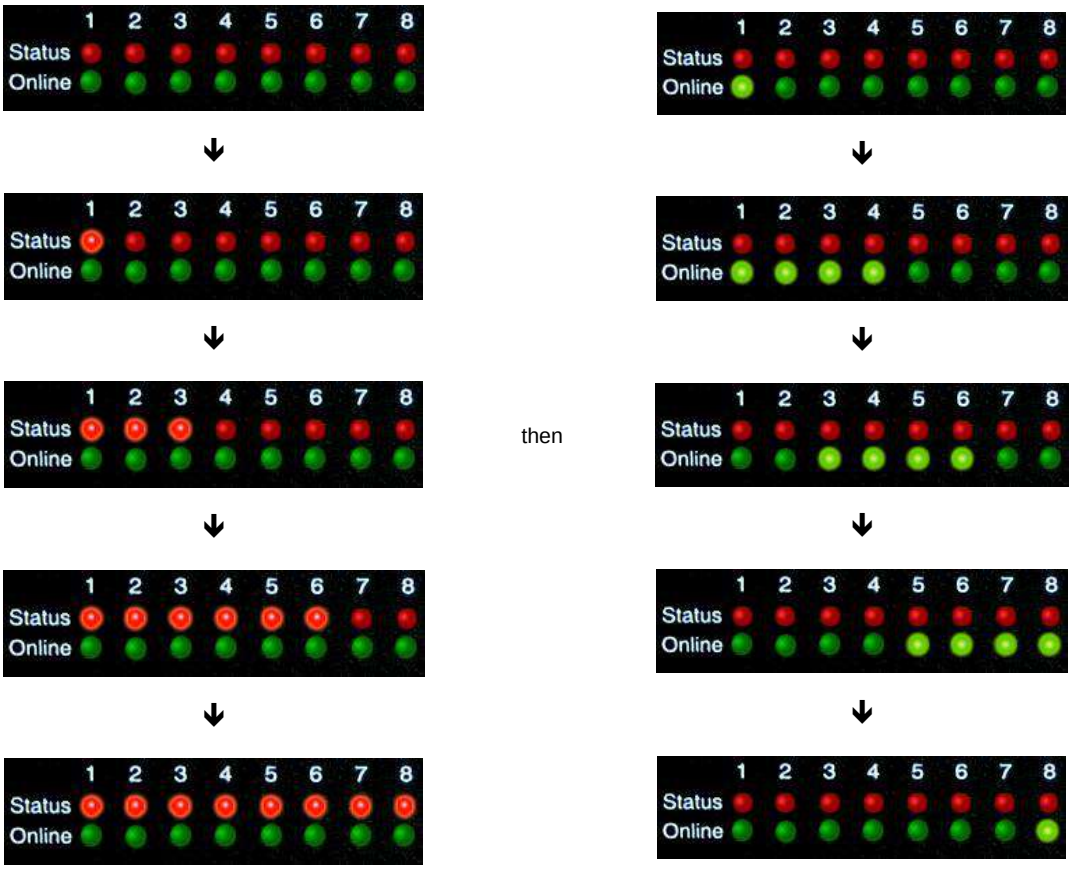
3) What do my LED lights mean?

The following diagrams show what the various LED displays mean.

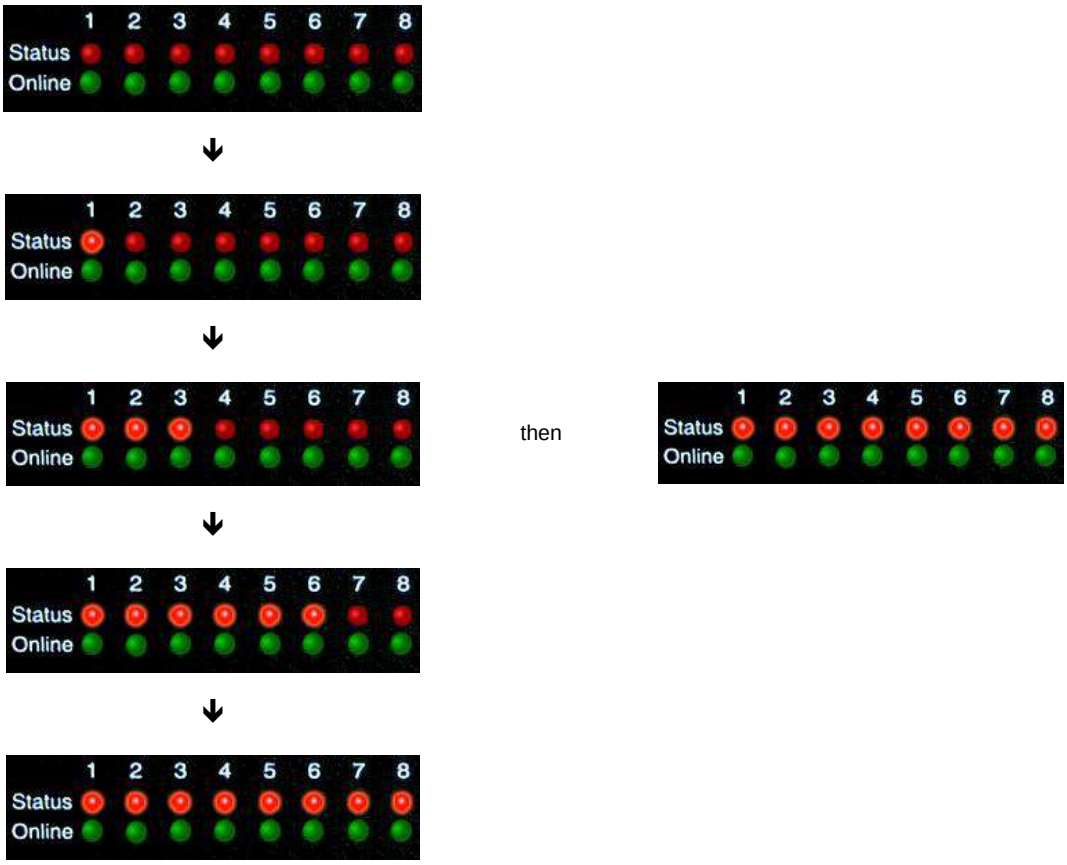
LED patterns in Normal Mode



LED patterns in Safe mode



LED patterns in **Recovery mode**



LEDs run clockwise after the power is connected.

From left to right each LED indicates

1st LED: U-Boot init
2nd LED: Kernel loaded with good CRC
3rd LED: Board init
4th LED: Serial port
5th LED: Ethernet
6th LED: NOR Flash
7th LED: NAND Flash
8th LED: Root file-system mounted. Starting init process

After the root file-system is mounted, all green LEDs will be flashing, and red LEDs light increasingly from left to right. The onboard web-server can be accessed during this time and shows a splash screen with boot details. After the boot process is finished the LEDs show the status of the online sensors.

4) I have forgotten my units IP address

If you have forgotten the IP address of your unit then you can simply press the rest button on the back of the unit. This will then announce the IP address through the units internal speaker.

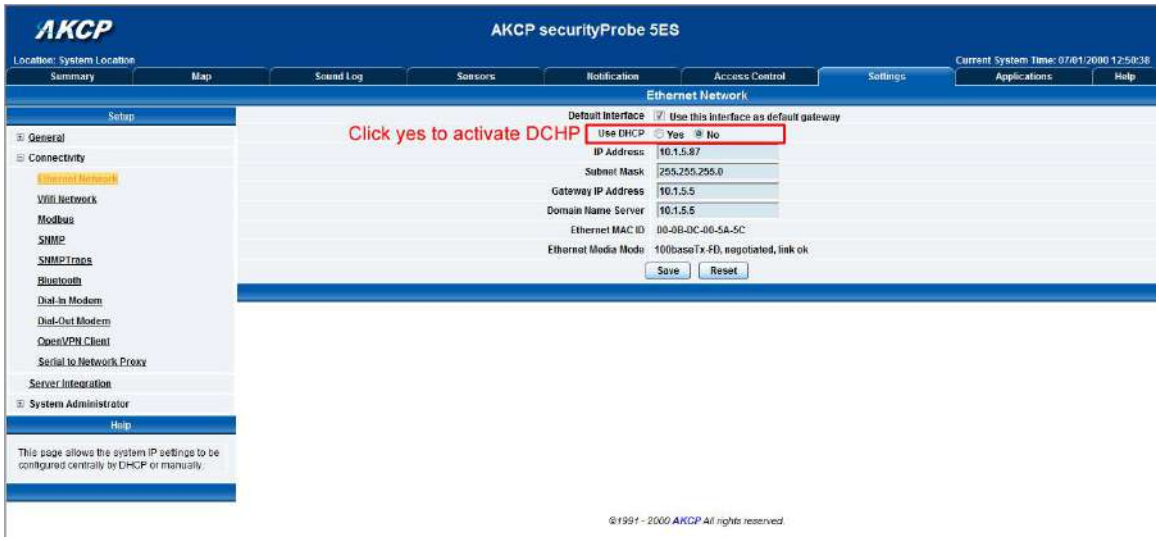
5) I have forgotten the password for my unit.

Hold down the reset button for 12 seconds. This will turn off the use password feature for the web based interface. This will remain turned off until you hold the button down for a further 12 seconds, or the unit announces *"Now turning off password checking"*.

Note: This will turn off the password checking for accessing the web interface only; you still have to enter the password when access the system via telnet.

6) Can I use DHCP to assign my units IP address?

Yes, you can use DHCP to assign the IP address. The unit ships with this disabled. Therefore to turn it on you need to log into the web interface and navigate to the Ethernet settings by way of clicking the "security" tab, "Ethernet Network" and then clicking on the YES button for "Use DHCP".



Note: If the unit has a static IP address assigned it will no longer send out DHCP requests. If you later wish to turn DHCP back on you can do that using the Web based interface.

7) How do I set up my routing table?

*To set up the routing table, open a DOS window (start, run type *command* press enter) and at the command prompt enter.

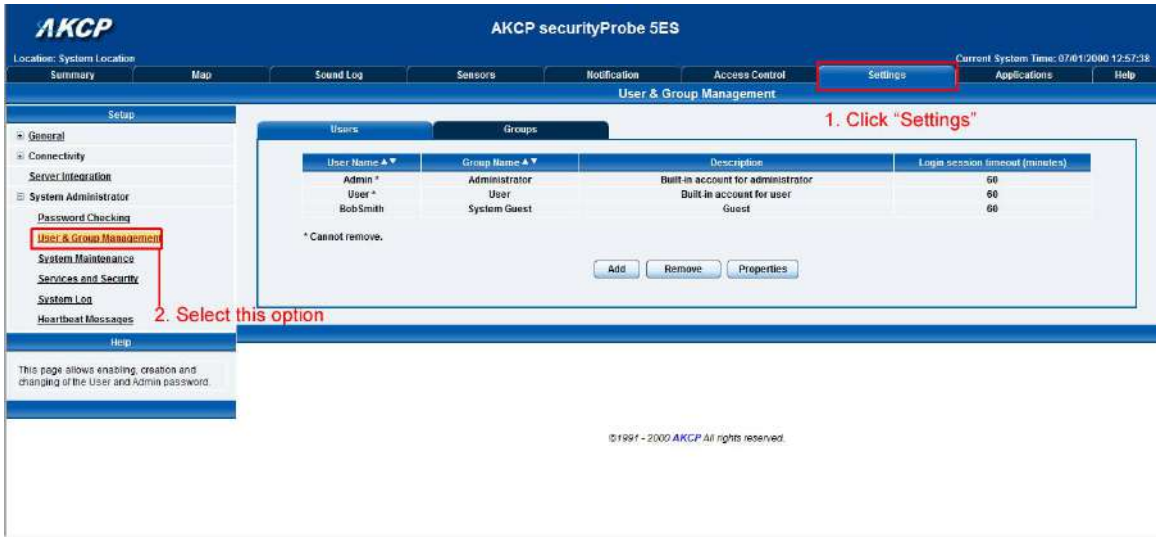
```
>route add 192.168.0.100 10.1.1.20
```

Where `10.1.1.20` is the IP address of the Ethernet interface on the PC that the unit is plugged into with the crossover cable.
Now ping* 192.168.0.100 to see if the connection was successful.

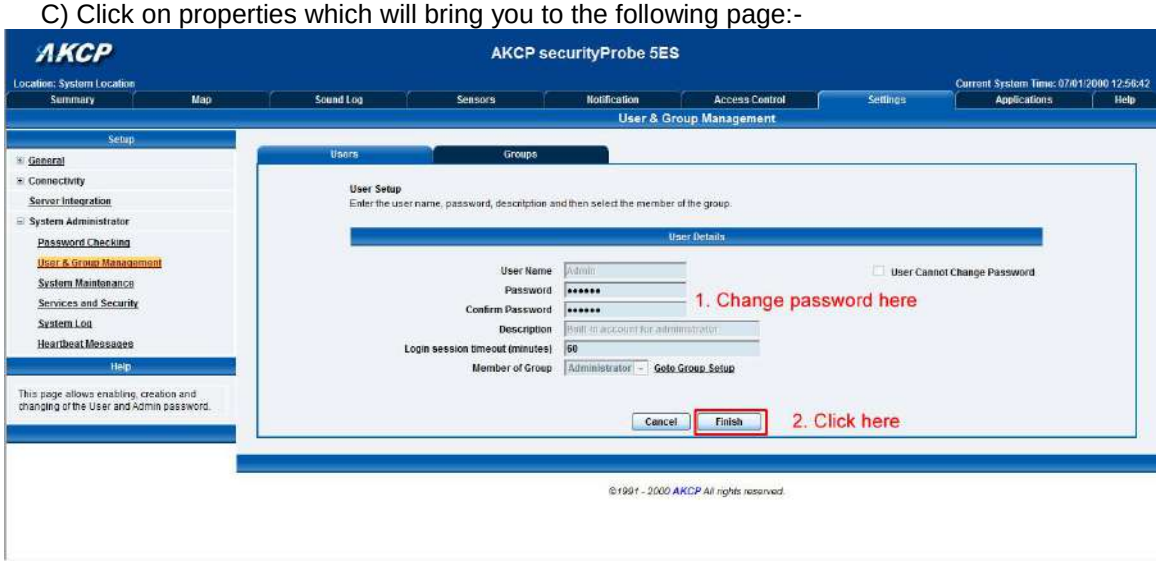
8) How can I change my administrator password?

If you wish to make your unit more secure and change the administrator password from the default (public) to your own choice follow these steps :-

A) Log into your unit using the default password.
B) Point towards the settings tab.



C) Click on properties which will bring you to the following page:-



9) What function do the different types of notifications provide?

The notifications are used to notify you when a sensor reading has hit a certain preset "critical" threshold. There are many ways you can be notified. They are as follows :-

SNMP Trap: This form of notification sends out a signal to your SNMP server.

E-Mail: This sends a notification via e-mail.

SMS: This sends an SMS message to your mobile phone.

MMS: This will send you a multimedia message to your mobile phone. This can include an image captured from one of the sensor probes cameras.

Relay: The relay is used as a switch, for example it could switch on an air con unit if the temperature reading of a temperature sensor reaches a certain threshold.

Alarm sound: This notification will sound an alarm.

Speech: Creates a text to speech notification.

Picture log: Creates an action where the camera logs a series of images when a certain event happens.

Telephone call: Will call you and play a pre recorded message or a text to speech message.

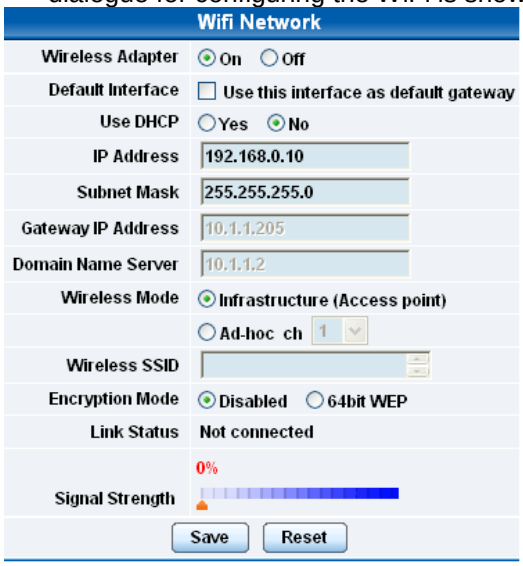
Custom script: Allows you to load a custom script that runs on a sensor reading a pre set parameter.

Fax: Will send a Fax to you with a notification message.

Sound log: creates a log of sound captured with the internal / external microphone.
Siren and strobe: will activate a siren and strobe light.
Mobile access: Gives you the function of viewing the camera attached to your security probe via your mobile phone.
Wake up / Shutdown: This will send a signal to wake or shut down a server.
If you require any assistance in setting up of these please contact us on support@akcp.com

10) Can I connect my unit via WiFi?

Yes you can connect the unit via WiFi. Simply plug a USB dongle into the USB port on the rear of the unit. You then need to configure your connection type, and encryption key etc. You do this from the web based interface in the settings tab and the connectivity option. The dialogue for configuring the WiFi is shown below.



11) What is the Heartbeat message?

This setting is to have the securityProbe notify you it is still running. You can be notified by either SMS, traps, Custom Scripts or by e-mail:
Alive Trap settings: *Send Keep Alive Traps (Default Off): Select on if you want the system to send Alive Traps.*
Destination: *enter the IP address of the server to send traps to.*
Community: *SNMP community string.*
Resend Interval (mins): *The period of time between each keep-alive trap. Values range from 1 to 65535 minutes.*

12) What is the network sniffer

The Network Sniffer application can be used to capture network packets running to and from the securityProbe, and all the network traffic. You can then import the captured file into Ethereal or TCP dump for details of these network packets. The network trace will help in debugging any network problems; for example, if e-mail cannot be sent.

13) Can I use the camera for a video conferencing call?

Yes it is perfectly possible to use the camera and the integrated microphone to make a video conferencing calls. To do this you need the software called “OpenPhone” running on your computer. This is included on the CD ROM that came with your unit. (Look for OpenPhone.exe). Next follow these steps:-

1. Initiate connection from OpenPhone (PC) to securityProbe.
    a) Open the program by double clicking "openphone.exe"

b) Click the "Make Call" button, enter the IP address of the sensorProbe8Linux/cameraProbe8 to initiate a call in the "Address" field. Then, click "Ok"
c) The unit will automatically respond to a call and establish the connection. You will then see the video, and hear sound from the unit.

2. Initiate connection from a securityProbe to OpenPhone (PC)
   a) Open the program by double clicking "openphone.exe"
   b) On the web interface, click on the ***Applications*** tab, and click on ***Video Conferencing.***
   c) select the **"*Call to*"** option and enter the IP address of the PC running OpenPhone. Click **"*Save*".** to discover your computers IP address in the command prompt type "*ipconfig"*
   d) On the OpenPhone application, click **"*Answer*"** to accept the call.
3. Connection between two sensorProbe8Linux/cameraProbe8 (only voice conference).
   a) On the web interface of the calling sensorProbe8Linux/cameraProbe8, click on the ***Applications*** tab, and click ***Video Conferencing***.
   b) On the right pane, select the "**Call to**" field and enter the IP address of the receiving sensorProbe8Linux/cameraProbe8 into this field. Click *"**Save**"*
   c) The connection should automatically establish.

You can end the video conference call by doing the following:-

1. End the call on OpenPhone (PC): to end call, click the ***"Hang Up"*** button on the OpenPhone. This method can be used to end the call between the system and OpenPhone.
2. End the call on the unit: From the web interface, click on the ***Applications*** tab and click on ***Video Conferencing***. On the right pane, select *"End call and wait for a new incoming call"* option. Then, click ***"Save"***

14) My securityProbe unit will not seem to boot up normally and the LED's are circling around counter clockwise what should I do?

Leave the power connected to the unit and let it sit for 30 minutes without pressing the safe mode button and it should boot back to normal mode. If it does not then please follow the instructions on page #16 of this manual.

15) After I finished the firmware upgrade I don't see any sensors connected to my unit in the web interface any longer. What could be the problem?

Ether the update did not completely finish for some reason or your browser has a java script error. First try to clear your cache on your browser, then do a Ctrl + F5 (refresh).
If the sensors still do not show then re-run the firmware update once more.

16) I just noticed this "Mega SPI Error" in my securityProbe's web interface. What is the problem? How do I clear this?

The Mega SPI Error is caused by a faulty connection between the main board and the Mega SPI board that is mounted underneath the mainboard and has the sensor ports.
This error can cause the sensors to not be visable as well.
The first thing to try is to re-flash the unit with the latest firmware on our web site, then power cycle the unit. If the unit still has this problem, then you can remove the power from the unit, open the case and re-seat the cables that connect the main board to the Mega IO board. If you still have the same error please contact support and provide the MAC ID of the unit.

17) I am seeing "Database Locked" errors entries in the syslog on my securityProbe unit, what should I do?

First navigate to the Settings >> System Administrator >> System Maintenance page, then run the "Backup All Settings To Backup File". Now run the "Clear All User Data and Restore Original Settings" keeping the network settings. After the unit has been reset you can upload the backup config file using the "Restore All Settings From Backup File".

18) My securityProbe unit keeps rebooting after I updated a firmware update failure. What happened and what can I do?

It sounds like the data base on the unit has been corrupted. Please use this version of firmware to update the unit. Which updating the unit please use the following procedures;
Do a complete reset back to factory default settings and a firmware re-flash.
First download the latest version of the firmware from our web site.
Here are the procedures:
First create a backup config file on the unit from the web interface.
Then run the firmware update and choosing the "Clear All User Data and Restore Original Settings" from the "System Maintenance" drop down menu.
After the firmware update is completed they can restore the backup config file.

19) I have some problems with securityProbe
The following things are not working:
When setting a virtual sensor online, the „Configuration“ button is missing (several browsers tested) The Restore Original Settings“ is not working
„Clear All User Data and Restore Original Settings“ is not working
The problem is most likely some files are missing or have been corrupted on the unit. Please try the following stepst;

1. backup the settings buy creating the backup config file
2. boot to recovery mode. Push and hold in the reset button while powering up the unit.
3. Choose the “clear all setting in recovery mode”
4. install the firmware again.
5. restore with the backup file in normal mode.

20) I am having problems with the unit but not sure what to do next?

Please email support@akcp.com and include the following detailed information in your email;
Note: The more details you can provide the easier and faster we can provide you with a resolution, so please be as detailed ad possible.

1. The details of the problem, condition of the LED’s etc.
2. What you did to determine the unit has this problem
3. Was there anything done to the unit prior to having the problem?
4. Did the unit always have this problem, if not when did this start?
5. Do you have more than one unit having the same problem?
6. What did you do to try and fix the problem?
7. What version of firmware is running on the unit? Did you try and upgrade it?
8. Include the backup configuration file from the unit.
9. If you can put the unit online this would be the fastest way for us to solve the problem.
10. What is the MAC ID of the unit.

21) On your specs it shows the same resolution on both HD and non HD camera’s. What is the difference?

The difference is the HD Cameras provide a a true digital image with enhanced clarity of the overall image. Resolutions are set to 640x480 to carefully balance image resolution and network bandwidth usage.

22) What are the differences between the securityProbe 5E, the securityProbe 5ES, the 5ESV and the securityProbe 5E?
The securityProbe 5E has all the features of the previous generation SEC-5E base unit. The main differences are:

- It uses a newer and better design that is less susceptible to EMI interference.

- It uses a newer and better processor than the 5E, the iMX25.
- It is configured with the NAND flash on board instead of the SD flash for its main Operating System memory. But still has the SD flash for extended picture and sound storage.
- The difference between the 5ESV and the 5ESVA unit is the 5E uses the BNC type coaxial camera connection where the 5ESV units use the USB type.
- The new PTDC is IR or night vision capable

The difference between the lower cost SEC-5ES and the SEC-5E is the 5ES unit does not include video where the 5E unit does support video. The 5E does not support software camera motion detection. Please use the IR motion sensor for motion detection.

~~**23) How long can the cameras be extended?**~~
~~You can extend the cameras both the UMC and the PTDC up to 5 meters. You cannot extend the cable more than 5 meters without active extenders – See FAQ #6 on the next page~~. (not applicable to this model)

~~**Does the new camera have the cable incorporated into it and what is the length of that cable?**~~
~~Yes, the cameras have the cable that attaches to the 5E unit incorporated in the camera and this cable comes in a 5 meter length.~~ (not applicable to this model)

~~**24) What if I need to extend the cameras further than 5 meters? Can I purchase what I need from you?**~~
~~You can use the active cable extenders to extend the run length of the camera cables to 10 meters. We don't currently offer these active extenders, however you should be able to source these in your local area quite easily.~~ (not applicable to this model)

25) Is this option a separate board or unit similar to your expansion units?
No this is not be a separate module, this is the same unit and case only the main board and back panel are different to provide the RG-6 BNC Digital camera connection inputs.

26) If I order this option will I be able to connect other types of third party cameras as I did with my SEC-5E?
Yes, the SEC-5E unit with the RG-6 BNC option will continue to support other third party cameras as long as they use the standard PELCO-D protocol and are within the previous specifications that worked with the SEC-5E base units.

27) I noticed on the data sheet the 5E now ships with 2 expansion ports instead of 4. Does reducing the expansion ports also reduce the total number of sensors that can be connected to the SEC-5ESV?
No, the SEC-5E unit will still support 500 sensors with the 2 expansion ports.

28) I noticed the the 5ES and 5E unit are now shipping without the SD cards inserted in the slot on the front panel. Did you forget to include them?
No, the units are now shipped as the NAND type setup where the operating system, settings, sensor data and other information is now stored on board in the NAND flash memory instead of the SD flash cards.

29) Can I add my own SD flash card to the unit? If so how large can I use and what is then stored on the SD card?
Yes, you can add your own SD flash card up to a 16GB. The picture and sound logs are stored on the SD flash. There is no setting that needs to be done, you can just insert the card and when the 128MB memory on the unit is full it will automatically begin storing the picture and sound logs on the SD flash.

30) I noticed you have a different firmware for the securityProbe 5E and the SEC-5ES base units, will there be another separate firmware for the SEC-5E?
No, the SEC-5ES and the SEC-5E units both use the same iMX25 processor so they will use the same firmware update file.

31) Speaking of firmware, do I need a separate firmware version or file if my unit has the X20 or X60 dry contact inputs? For example my SEC-5ESA-X20 or my SEC-5E-X60?
No, since all the units with the extra X20 and X60 dry contact inputs use the same iMX25 processor they use the same firmware update file.

32) Can I still use the same USB modems that worked or work on my securityProbe, my SEC- 5E and 5ES base units?
Yes, as long as your firmware is updated on the unit, the SEC-5E will support all the same modem types as the previous generation of units.

33) Will all the sensors that work on my SEC, SEC-5E, SEC-5ES work on the new SEC-5E base unit?
Yes, all the sensors are supported on the previous generation of SEC and SEC-5E base units will continue to be supported on the new 5E base units.

This concludes the securityProbe 5E User Manual.

Please contact support@akcp.com if you have any further technical questions or problems setting up your modem or your alerts.

Thanks for Choosing AKCess Pro!