

RAMOS Ultra

User Manual



© 2012 CONTEG, spol. s r.o.

All rights reserved. No part of this publication may be used, reproduced, photocopied, transmitted or stored in any retrieval system of any nature, without the written permission of the copyright owner.

Although this manual was prepared and checked with the best care, CONTEG, spol. s r.o. cannot accept any liability for omissions or errors in this publication. Due to the continuous development and progress, CONTEG, spol. s r.o. also reserves the right to change details and technical specifications of the products described in this manual. Such changes along with eventual errors or printing errata shall not constitute grounds for compensation.

Content

1.	Introduction.....	4
1.1.	What is RAMOS Ultra?	4
1.2.	How to use this manual.....	4
1.3.	Package Contents	4
1.4.	Front panel	4
1.5.	Rear panel	6
2.	Installation.....	7
2.1.	Setting up the IP address.....	7
2.2.	Testing the new IP address with the “ping” command	8
2.3.	Firmware upgrade	9
3.	Multi-users and groups setup	12
3.1.	Group Setup.....	13
3.2.	User Setup	14
4.	Services and Security	16
4.1.	Setting up a sensor	18
4.2.	Notification thresholds.....	20
4.3.	Advanced sensor settings	22
4.4.	Continuous time sensor settings	23
5.	Expansion Ports.....	24
6.	Notifications	26
6.1.	Adding a notification.....	26
6.2.	SNMP trap	27
6.3.	E-mail.....	29
6.4.	SMS notification	31
7.	Mapping	35
7.1.	Adding a map.....	35
7.2.	Monitoring via the map interface.....	38
8.	Filters	39
8.1.	Sensor filters	39
8.2.	Syslog filters.....	40
9.	Making my unit visible on the internet	42
10.	FAQ.....	43

1. Introduction

1.1. What is RAMOS Ultra?

The RAMOS Ultra integrates the latest technology to push the boundaries of disaster protection. Now you can sense and see problems before they lead to business disruptions. It is a high speed, accurate, intelligent monitoring device, featuring a completely embedded host and Linux Operating System. This gives you everything you need and nothing you don't!

1.2. 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 ramos@conteg.com.

1.3. Package Contents

Your RAMOS Ultra package contains the following items:

- 1x Product CD
- 1x 1,5m Crossover or straight cable
- 1x 7,5 V, 3 A power supply
- 2x Brackets for rack mounting
- 1x First run manual

1.4. 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 ramos@conteg.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.

1. 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.
2. 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 ramos@conteg.com
3. 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 ramos@conteg.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) Expansion Ports

There are four expansion ports numbered from E1 – E4. These are expansion Ports for connecting either the 8port expansion or 16 dry contact expansion modules.

6) Removable SD slot

This slot so where you can place your SD card which can store data such as pictures taken from the CCTV camera, sounds recorded from the internal microphone, and also the current firmware of the unit. Supported card size is up to 32GB. SD card is not included.

1.5. Rear panel



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

1) Reset button

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

1. 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.
2. Turns off password checking when accessing the web based interface (hold down for 7 seconds)
3. To reboot the unit into the firmware upgrade mode (hold down for 12 seconds)

2) Sensor ports

There are 8 RJ45 ports numbered from 1 – 8. These are for connecting Conteg 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

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

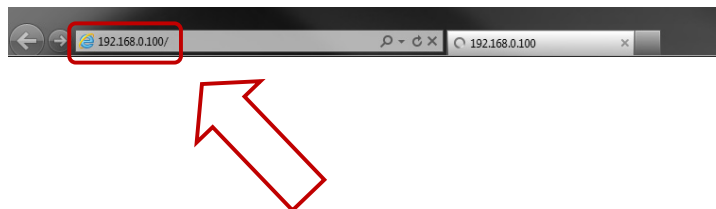
2. Installation

2.1. 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, and then press 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) On welcome "Log in" page enter username "Admin" and default password for Admin is "public". Change the password to make your unit secure!
- d) Next the home page will be displayed. It will look similar to this.

Host Name	Type	Sensor Name	Reading	Status
Main Module	Virtual Sensors	Temperature on RAMOS Mini	23.5 °C	Normal
	Temperature Array	Temperature Array Port 2.1	24.5 °C	Normal
	Temperature Array	Temperature Array Port 2.2	24.5 °C	Normal
	Temperature Array	Temperature Array Port 2.3	24.5 °C	Normal
RAMOS ULTRA-EX 0A000858	Temperature	Temperature Port 4	24.5 °C	Normal
	Dry contact I/O	Dry contact I/O Port 3	-	Critical
	4-20 mAmp	4-20 mAmp Port 1	0.1 kPa	Normal

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

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>

2.2. 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.

```

Správce: C:\Windows\system32\cmd.exe
Microsoft Windows [Verze 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Všechna práva vyhrazena.
C:\Users\tgraf>ping 192.168.168.168
Příkaz PING na 192.168.168.168 - 32 bajtů dat:
Odpověď od 192.168.168.168: bajty=32 čas=1ms TTL=64
Odpověď od 192.168.168.168: bajty=32 čas < 1ms TTL=64
Odpověď od 192.168.168.168: bajty=32 čas < 1ms TTL=64
Odpověď od 192.168.168.168: bajty=32 čas < 1ms TTL=64
Statistika ping pro 192.168.168.168:
Pakety: Odeslané = 4, Přijaté = 4, Ztracené = 0 (ztráta 0%),
Přibližná doba do přijetí odezvy v milisekundách:
Minimum = 0ms, Maximum = 1ms, Průměr = 0ms
C:\Users\tgraf>

```

2.3. Firmware upgrade

Ensure you are running the latest firmware. You will also need to download the latest firmware from our website www.conteg.com.

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

a)

The screenshot shows the CONTEG RAMOS ULTRA web interface. The 'Settings' tab is highlighted with a red box and a red arrow pointing to it. The interface displays sensor information for a 'Main Module' and 'RAMOS ULTRA-EX 0A000858'. The sensor data table is as follows:

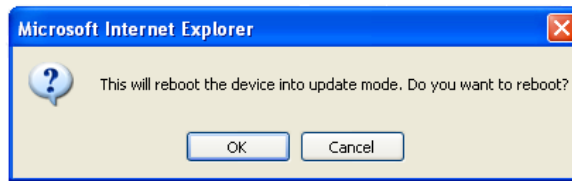
Host Name	Type	Sensor Name	Reading	Status
Main Module	Virtual Sensors	Temperature on RAMOS Mini	23.5 °C	Normal
	Temperature Array	Temperature Array Port 2.1	24.5 °C	Normal
	Temperature Array	Temperature Array Port 2.2	24.5 °C	Normal
	Temperature Array	Temperature Array Port 2.3	24.5 °C	Normal
	Temperature	Temperature Port 4	24.5 °C	Normal
RAMOS ULTRA-EX 0A000858	Dry contact I/O	Dry contact I/O Port 3	-	Critical
	4.20 mAmp	4.20 mAmp Port 1	0.1 kPa	Normal
	Module	RAMOS ULTRA-EX 0A000858	-	Critical

A red arrow points to the 'Settings' tab in the top navigation bar, with the text 'Select Settings tab' written below it.

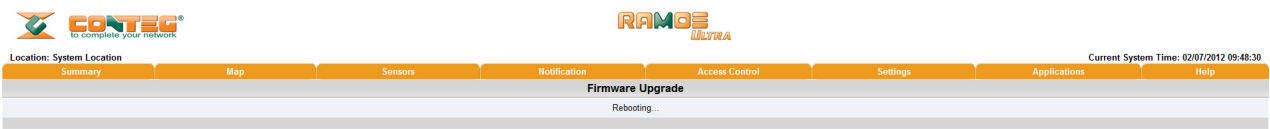
b)

The screenshot shows the CONTEG RAMOS ULTRA web interface. The top navigation bar includes 'Summary', 'Map', 'Sensors', 'Notification', 'Access Control', 'Settings', 'Applications', and 'Help'. The 'Settings' tab is active, and the 'System Maintenance' section is expanded. In the left sidebar, 'System Administrator' and 'System Maintenance' are highlighted with red boxes and arrows. Red text annotations indicate: '1) Click on „System Administrator“', '2) Click on „System Maintenance“', and '3) Click on „Upgrade“'. The 'Upgrade' button is also highlighted with a red box and arrow.

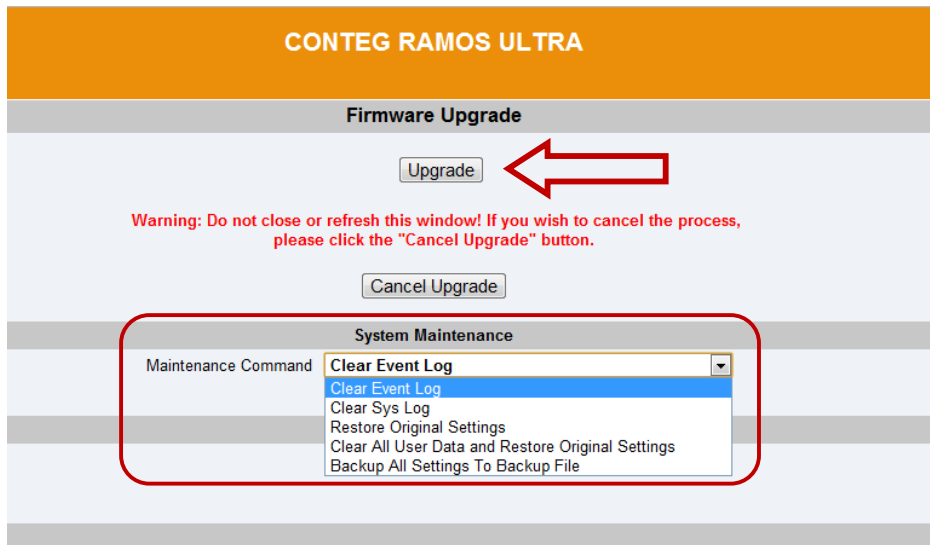
c) You will then be presented with this pop up:



Click OK. The unit will then reboot in safe mode. 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.



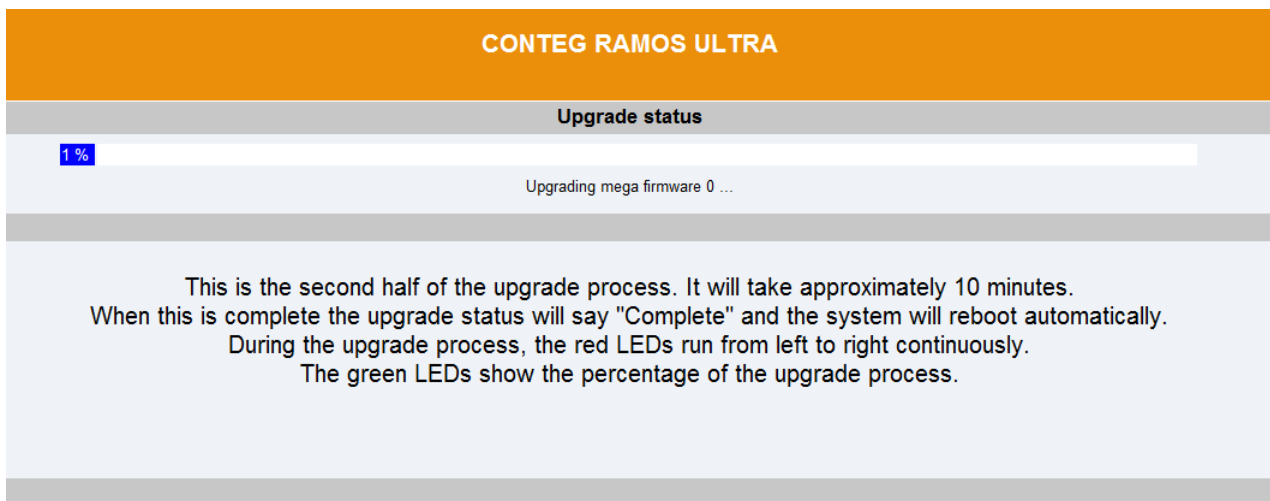
- d) Once the unit has rebooted you will see the following page where is presented Firmware upgrade and system maintenance options with backup for example. For upgrade press button “Upgrade”.



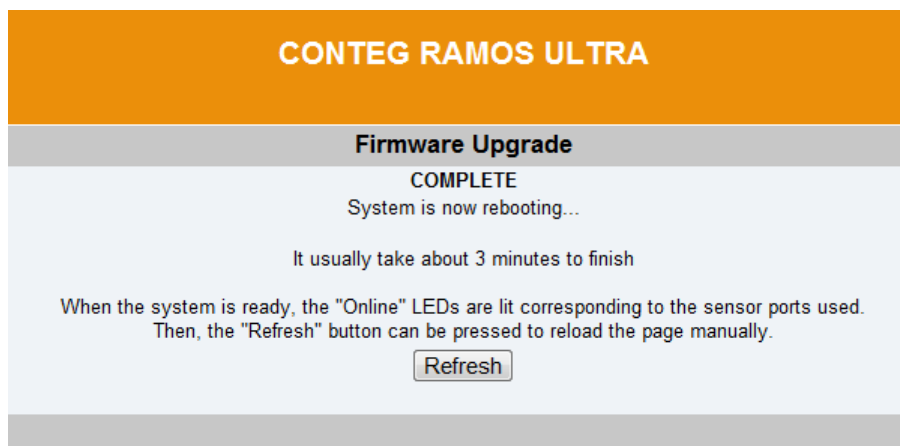
- e) On the next page follow these instructions.



f) During the process you will see the following messages:



g) The unit will then reboot. The process is complete when the LED's are back to their "normal" status. Then press button "refresh"



3. Multi-users and groups setup

Log in to the RAMOS Ultra with the Administrator password, the default will be "public" if you have not changed this yet.

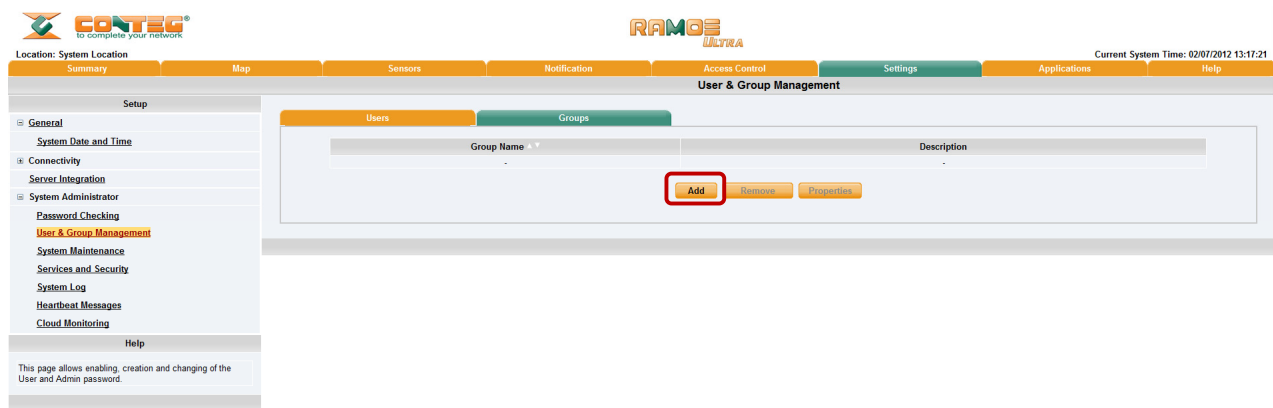
Click on the Settings page, then System Administrator then User & Group Management as shown in the screen shot below:

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.

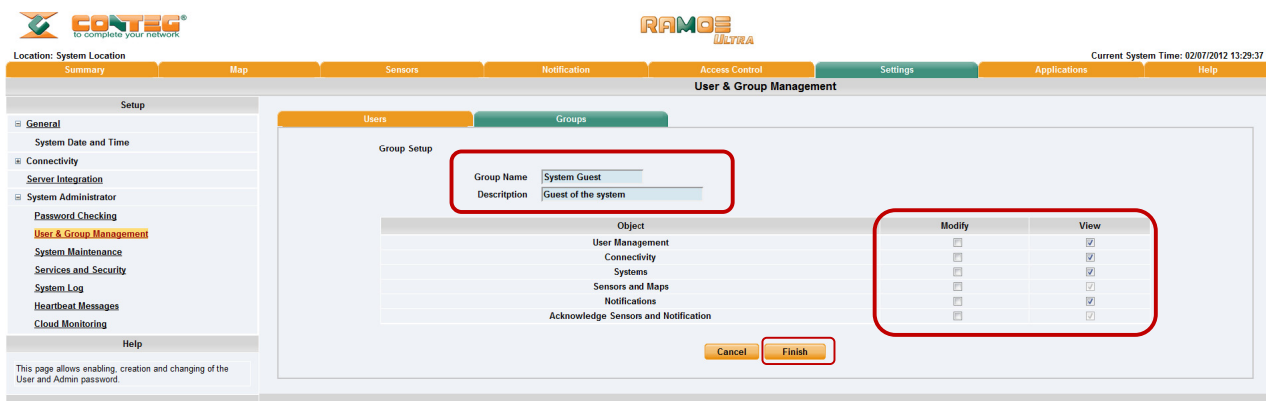
3.1. Group Setup



This will take you to the Groups page shown below:

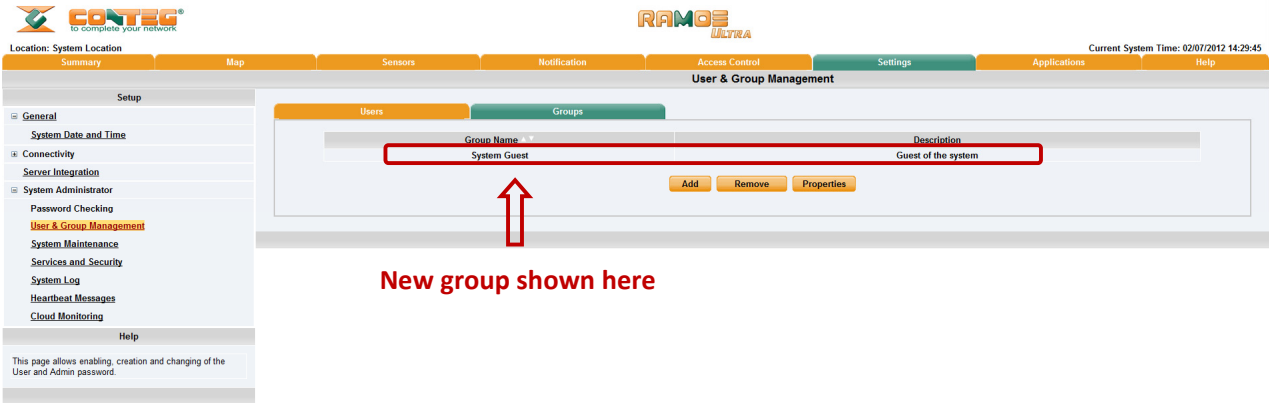


Now click on the "Add" button to add your groups as shown in the screen shot above.

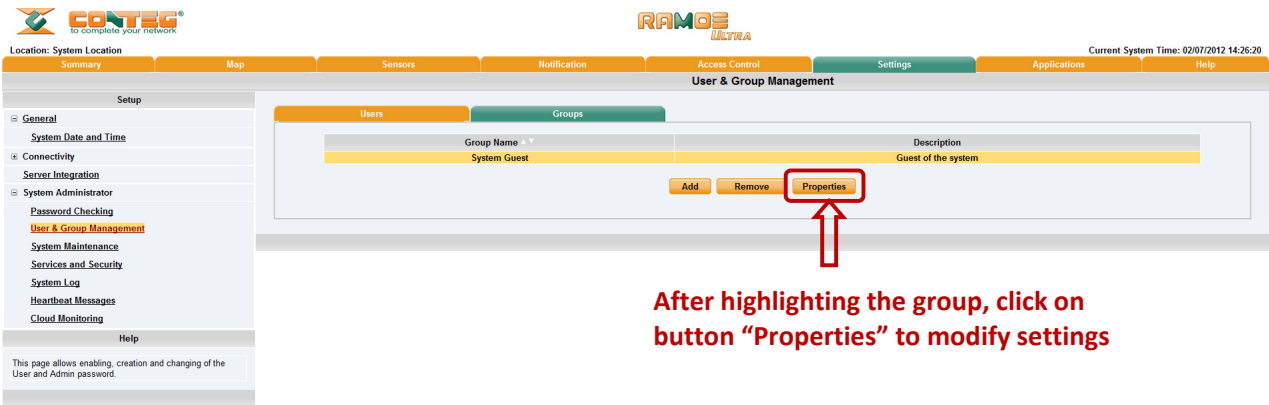


Enter your group name for example we have added a group named "System Guest" and entered our description.

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.

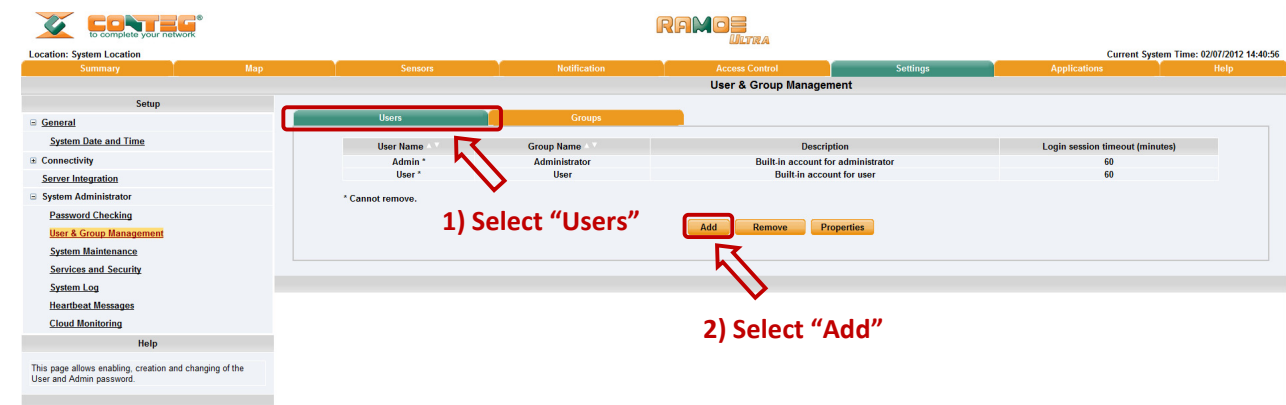


Now you can see the new group “System Guest” has been added to our group list as shown in the screen shot above.

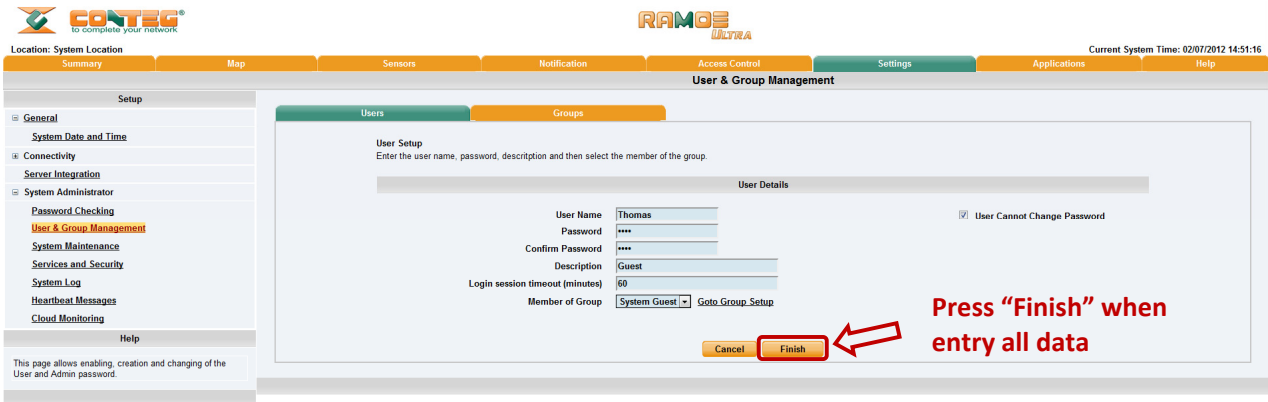


If you wish to modify your group settings, highlight the group you wish to modify by clicking on it, and then click on the “Properties” button as shown in the screen shot above.

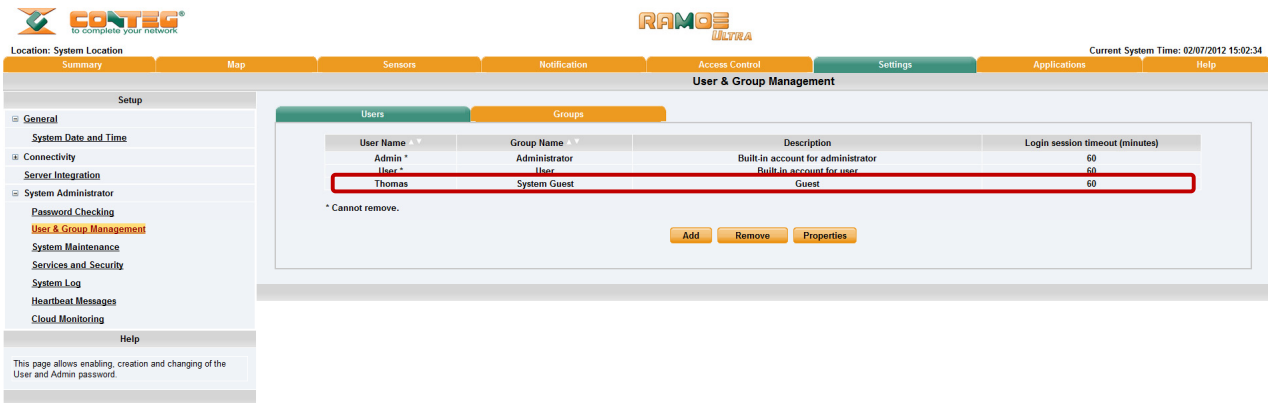
3.2. User Setup



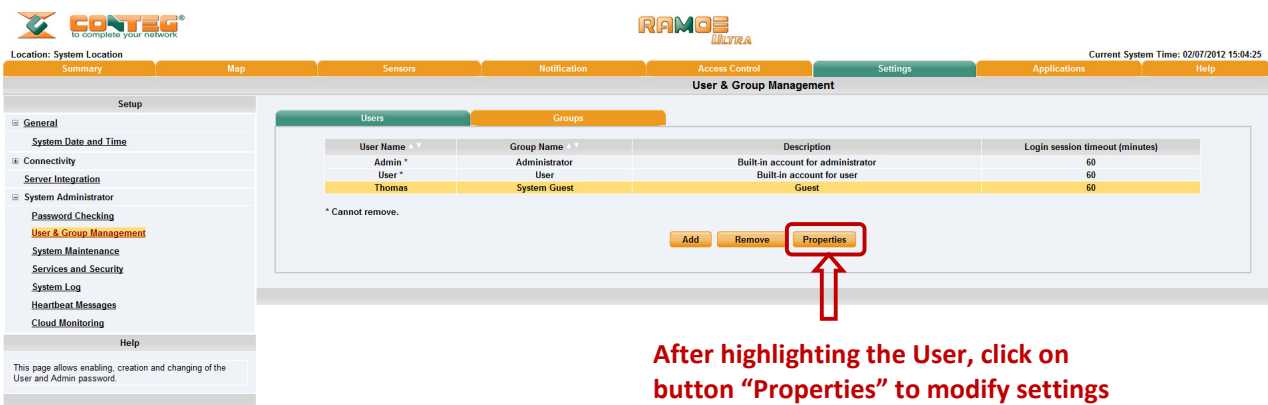
Click on the Users tab then click the “Add” button to add the new Users to your groups as shown above.



Now enter your User details as shown above. In our example we have entered Thomas as our Guest into our "System Guest" group. We have also added the option so that this user cannot change his Log in password. After adding your users for each group click the "Finish" button to save each user.



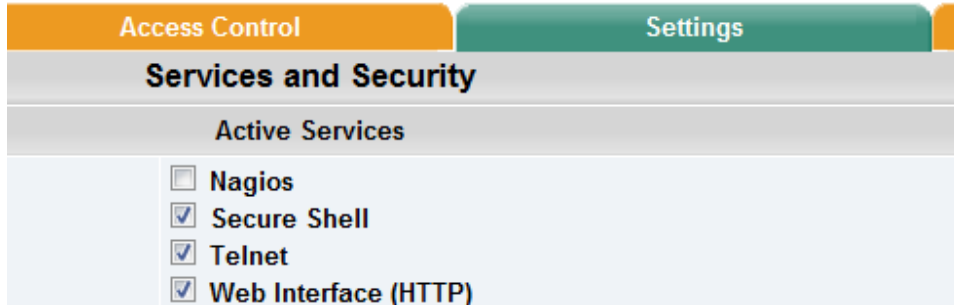
Now as you can see the new user has been entered into our list of Users.



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

4. 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 RAMOS Ultra 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

The screenshot shows the 'Services and Security' configuration page. The 'Active Services' section is expanded, showing a list of services with checkboxes. 'Simple Network Management Protocol Version 3 (SNMPv3)' is checked and highlighted with a red box. Other services include Nagios, Secure Shell, Telnet, Web Interface (HTTP), Secure Web Interface (HTTPS), Serial to Network Proxy (ser2net), AKCess Pro Server Integration, and Ethernet Watchdog. There are 'Save' and 'Reset' buttons at the bottom.

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

The screenshot shows the 'Select ssl key' dialog box. It contains a 'File' field with a 'Browse...' button, an 'Add File' button, and a message that says 'file name must be userkey.pem'. There is a 'Close' button at the bottom.

[Close](#)

Active Security

Active Security	
Active Security	<input type="checkbox"/> Allow Users to Acknowledge Alarms
	<input checked="" type="checkbox"/> Announce IP Address When Boots
<input type="button" value="Save"/> <input type="button" value="Reset"/>	

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

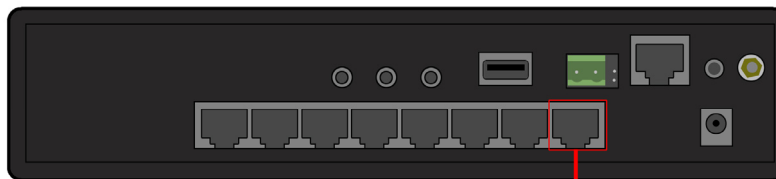
Network Access Control	
Network Access Control	<input type="radio"/> Off <input checked="" type="radio"/> On
Access Policy	<input checked="" type="radio"/> Only allow access to the host below <input type="radio"/> Only deny access to the host below
Address	<input type="text"/>
Allow List	<input type="text"/> <input type="button" value="Add"/>
<input type="button" value="Save"/> <input type="button" value="Reset"/>	

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.

4.1. Setting up a sensor

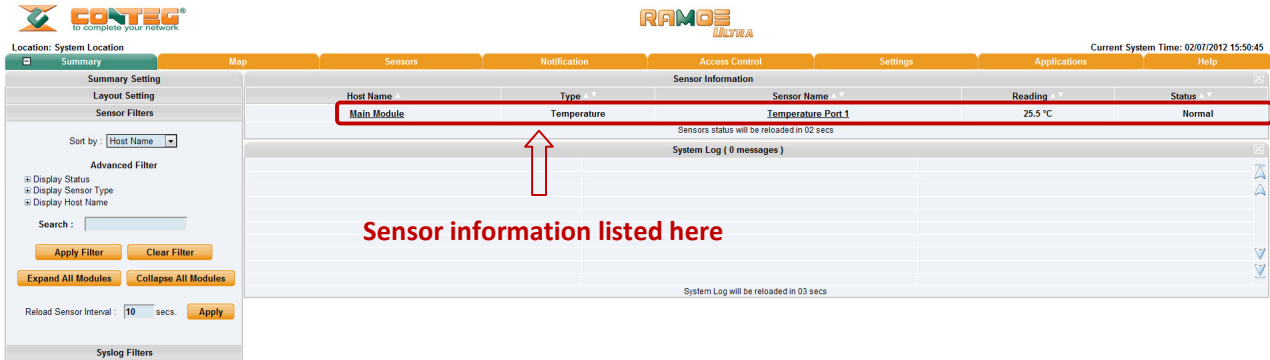
In this section we will now go through the basic set up of a sensor. We will focus on the CONTEG temperature sensor; however this basic set up process is applicable to all of our sensors. If you require information on specific functions of a particular sensor then please download the manual for that 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.



Connect Sensor to one of the ports on the rear of the unit

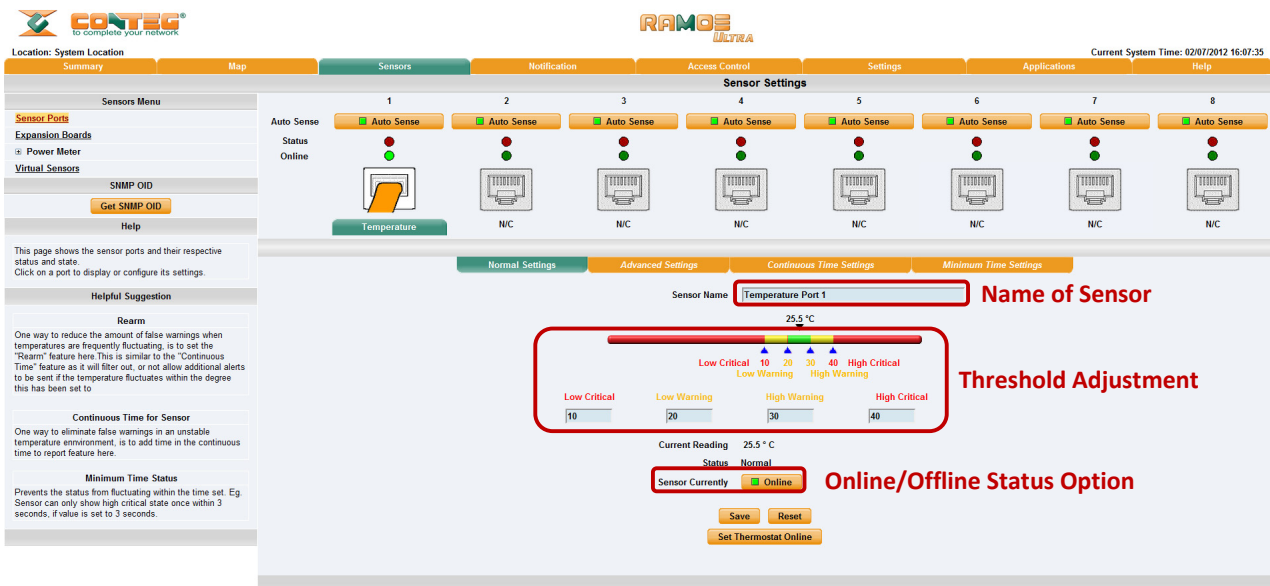
- b) Now point your browser to the IP address of the unit (default, 192.168.0.100). Next you need to log in as the administrator using your administrator password (default is “public”). You will then be taken to the summary page. This is shown below.



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.

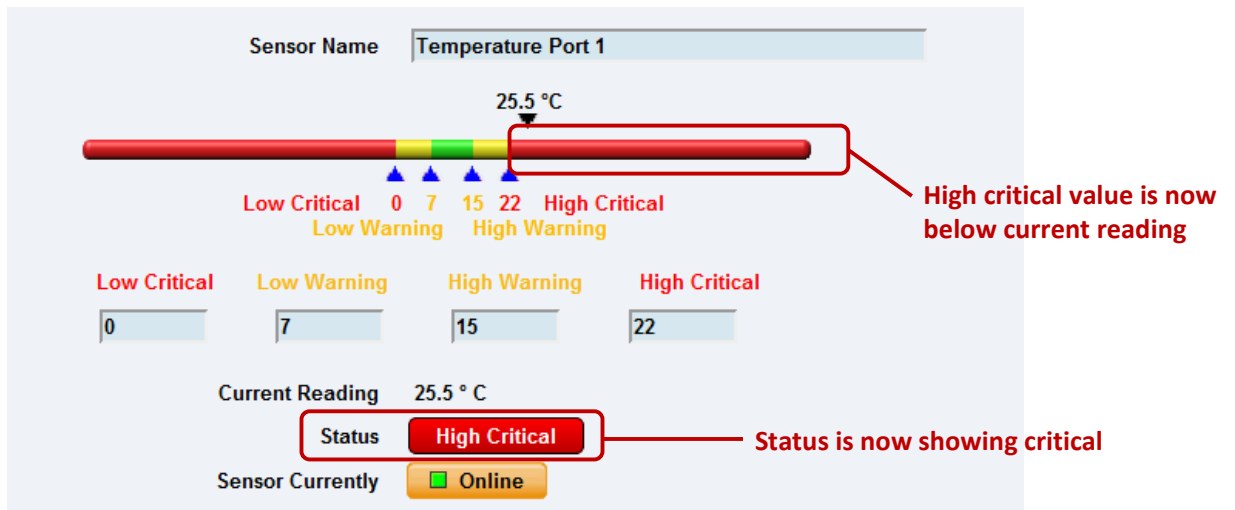
- c) Now click on the temperature sensors name (indicated in previous screen shot). This will bring you to the following page, the sensors page:



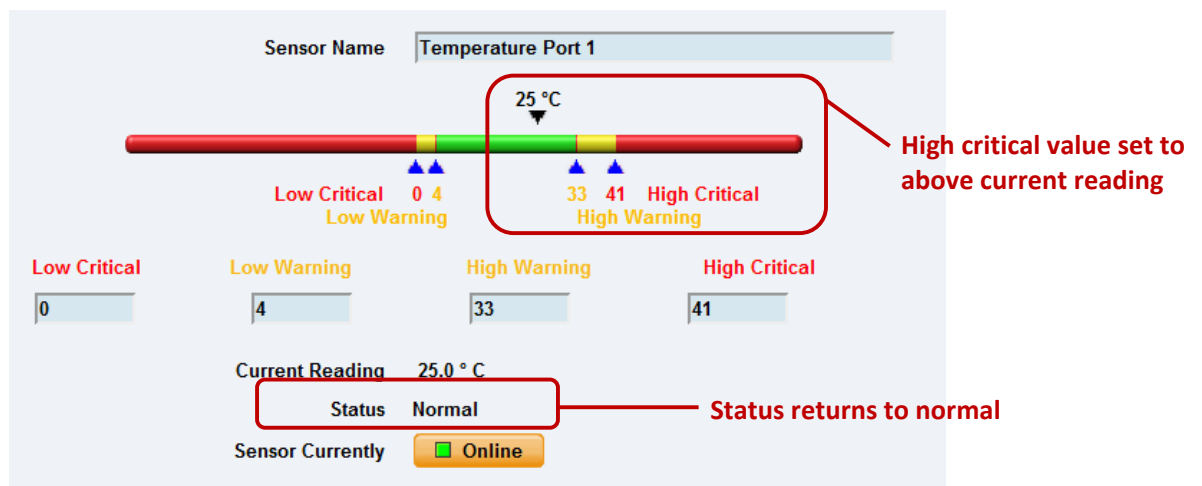
Note: another way of accessing this page is to click on the “sensors” tab at the top of the page.

4.2. 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 25.5 degrees C, 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 browser's refresh button.*



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

Current Reading 25.0 ° C
 Status Normal
 Sensor Currently **Online**

Click on this button to take a sensor offline

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

The screenshot shows the 'Sensor Settings' page for 'Main Module'. It displays eight sensor ports, each with an 'Auto Sense' button and a status indicator. The first port, labeled 'NIC', has a red dot above it, indicating it is offline. A red box highlights this port, and a red arrow points to it from the text below.

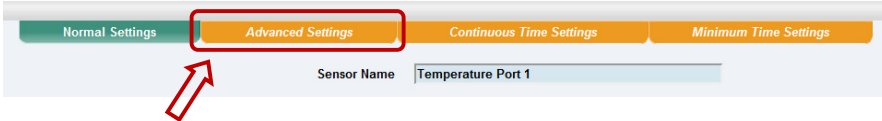
The shades sensor icon indicates that the sensor is offline

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

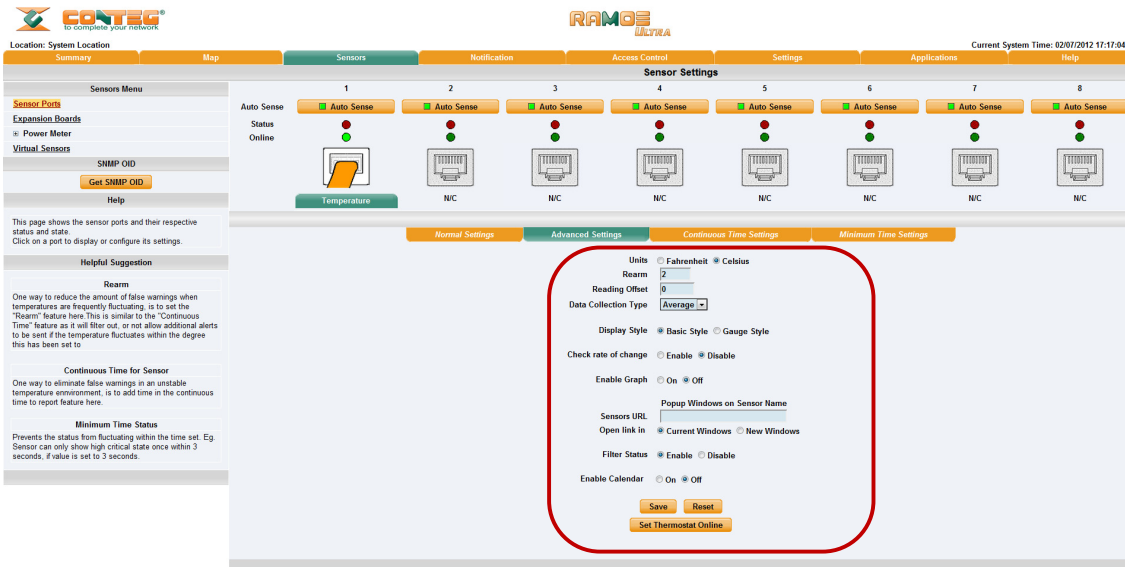
The screenshot shows the 'Sensor Settings' page with a dropdown menu open for port 1. The menu lists various sensor types, and 'Temperature' is highlighted. A red box highlights the 'NIC' icon, and a red arrow points to it from the text '1) Click on picture of sensor socket'. Another red box highlights the 'Save' button, and a red arrow points to it from the text '3) Click "Save"'. A third red box highlights the 'Temperature' option in the dropdown menu, with a red arrow pointing to it from the text '2) Select "Temperature"'. The status of port 1 is now 'Online'.

4.3. Advanced sensor settings

Near the bottom of the sensors page you will see the advanced mode button



By clicking this you will get the following options:



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: 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)

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

Enable Calendar On Off Status set to on

All	AM											PM											
	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10
Sunday	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report
Monday	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report
Tuesday	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report
Wednesday	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report
Thursday	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report
Friday	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report
Saturday	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report

Toggle Working Hours

Report Do Not Report

To Clear/Set, Click Hour, Day, AM, PM, All.
 To Clear/Set the Whole Hour, Click a Cell.
 To Select a Minute, Right Click a Cell; Mouse Over will display minute offset.

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.

Enable calendar On Off

All	AM											PM											
	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10
Sunday	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report
Monday	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Do Not Report	Do Not Report	Do Not Report	Report	Report
Tuesday	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Do Not Report	Do Not Report	Do Not Report	Report	Report
Wednesday	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Do Not Report	Do Not Report	Do Not Report	Report	Report
Thursday	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Do Not Report	Do Not Report	Do Not Report	Report	Report
Friday	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Do Not Report	Do Not Report	Do Not Report	Report	Report
Saturday	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report	Report

Toggle Working Hours

Report Do Not Report

To Clear/Set, Click Hour, Day, AM, PM, All.
 To Clear/Set the Whole Hour, Click a Cell.
 To Select a Minute, Right Click a Cell; Mouse Over will display minute offset.

4.4. Continuous time sensor settings

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).

Normal Settings	Advanced Settings	Continuous Time Settings	Minimum Time Settings
Continuous Time for Sensor to be in new Status before accepting new Status			
High Critical		0	
High Warning		0	
Normal		0	
Low Warning		0	
Low Critical		0	
Sensor Error		0	
<input type="button" value="Save"/> <input type="button" value="Reset"/> <input type="button" value="Set Thermostat Online"/>			

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.

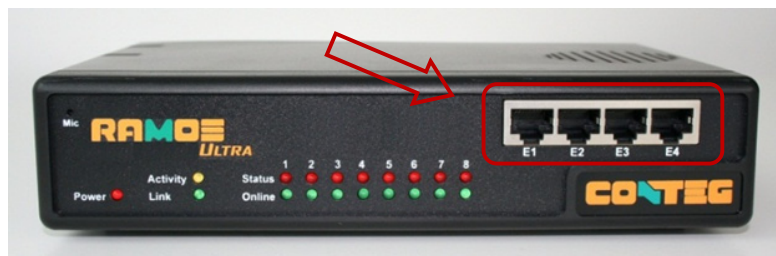
Continuous Time to Report for Sensor Error: As above, but delays notification being sent for sensor going into an error state.

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.

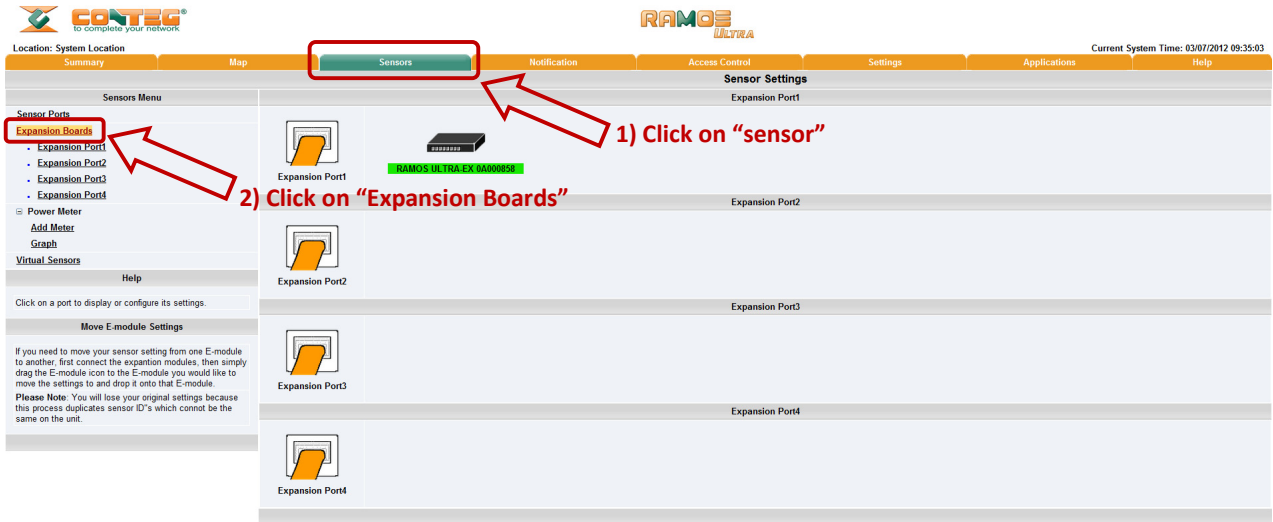
5. Expansion Ports

The RAMOS Ultra is equipped with four expansion ports. This enables you to 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.

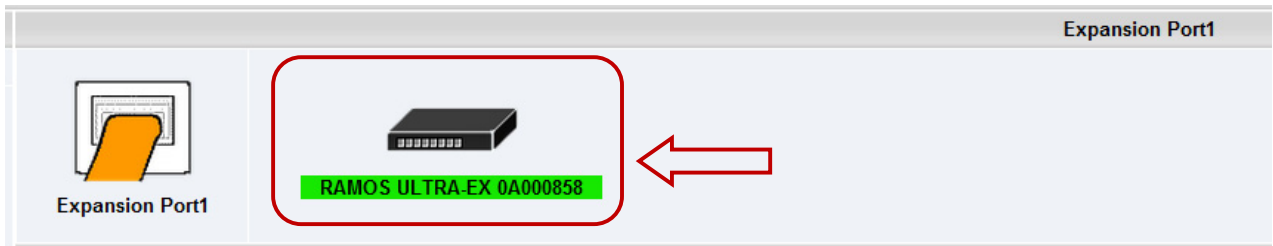
- a) Plug the expansion board into one of the four ports located on the front panel of the unit. These are numbered E1-E4.



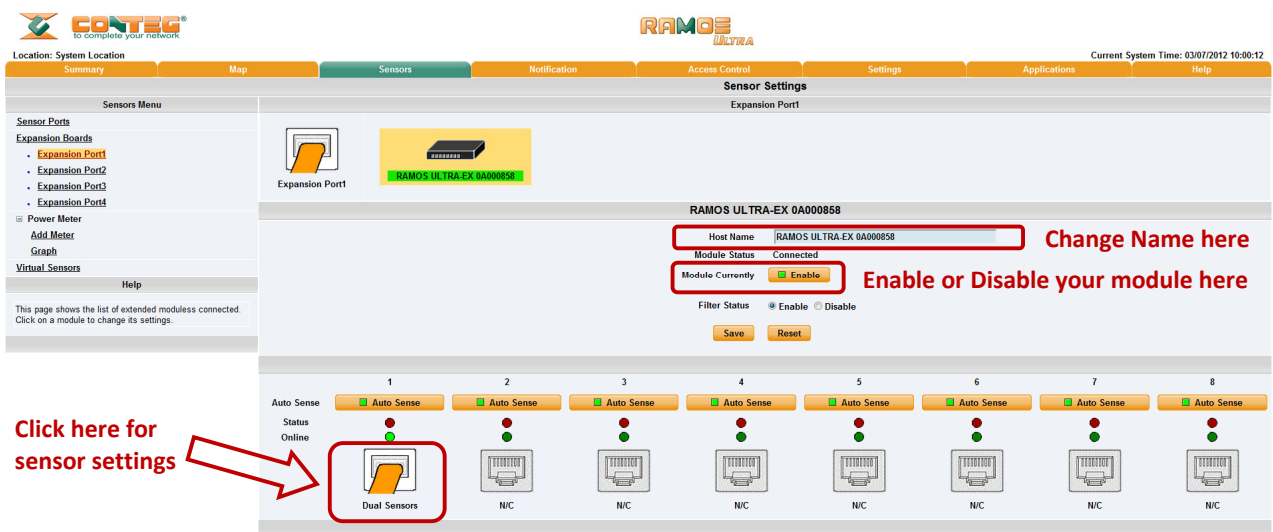
b) From the summary page, navigate to the "Sensors" tab. Then click "Expansion Boards" as outlined in the image below:



c) A list of all extended ports will be shown. Each port will display any available extension modules; these will be highlighted in green. Click the module to be taken to the sensor settings page.



d) This will bring you to the following page, the extended port sensors page:



- e) 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 16.

6. 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:

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

6.1. Adding a notification

- a) First click on the “notification wizard”

The screenshot shows the CONTEG RAMOS ULTRA web interface. The top navigation bar includes 'Summary', 'Map', 'Sensors', 'Notification', 'Access Control', 'Settings', 'Applications', and 'Help'. The 'Notification' tab is highlighted. On the left, a sidebar contains a 'Notification Menu' with 'Begin Notification Wizard' highlighted. The main content area shows a table for 'Link Sensor To Action' with columns for 'Host Name', 'Sensor Name', 'Action on Status', and 'Action Name'. Below the table are buttons for 'Create', 'Edit', 'Create Escalation', and 'Remove'. There are also 'Import' and 'Export' buttons at the bottom.

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

The screenshot shows the 'Create Action' wizard page. The top navigation bar is the same as in the previous screenshot. The main content area has a heading 'Create Action' and a sub-heading 'The Notification Wizard will guide you step by step through the process of selecting a sensor, creating an action and defining the criteria under which the Notification will be sent.' Below this, there is a prompt 'Please select an Action Type' followed by a dropdown menu. The dropdown menu is open, showing a list of action types: 'SNMP Trap', 'Email', 'SMS', 'Relay', 'FTP', 'Custom Script', 'Fax', 'Siren', 'Wake Up / Shutdown', 'Windows Alert', 'Skype Call/SMS', 'Dry contact', 'Enable/Disable Sensor To Action', 'Modbus', 'Alarm Sound', 'Speech', 'Sound Log', and 'Telephone Call'. The 'SNMP Trap' option is selected. To the right of the dropdown are 'Cancel' and 'Next >' buttons. Red arrows point from the text '1) Select action' to the dropdown and from '2) Select "Next"' to the 'Next >' button.

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.

6.2. 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

Notification Access Control Settings Applications

SNMP Trap Action Wizard

Action Name Enter name for your SNMP notification

Trap Version v1 v2c v3

SNMP Trap send port(default is : 162)

Destination Address Enter the IP address of your SNMP trap

Community Enter community name of trap

Use Sensor Name

Add Trap Destination

Cancel Next

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:

Notification Access Control Settings Applications

SNMP Trap Action Wizard

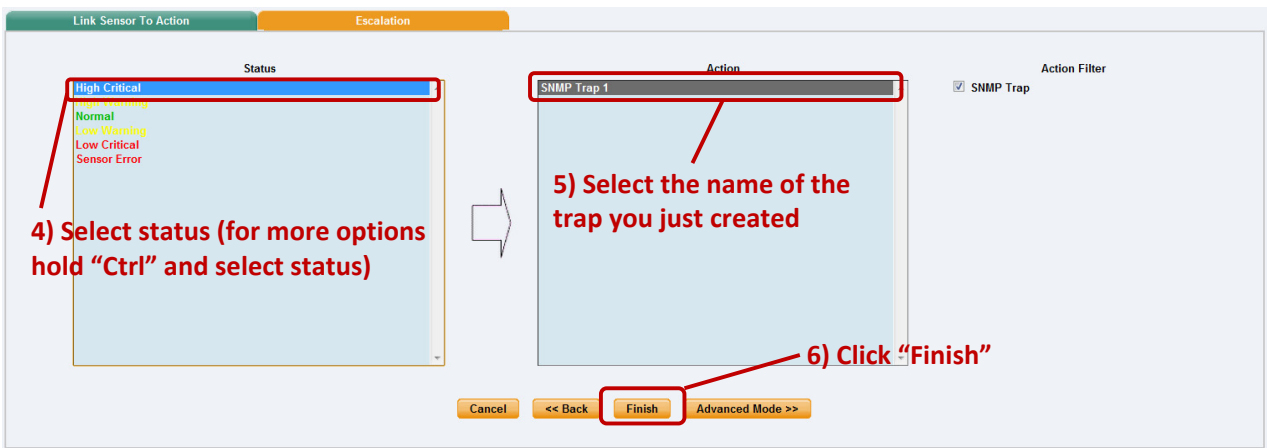
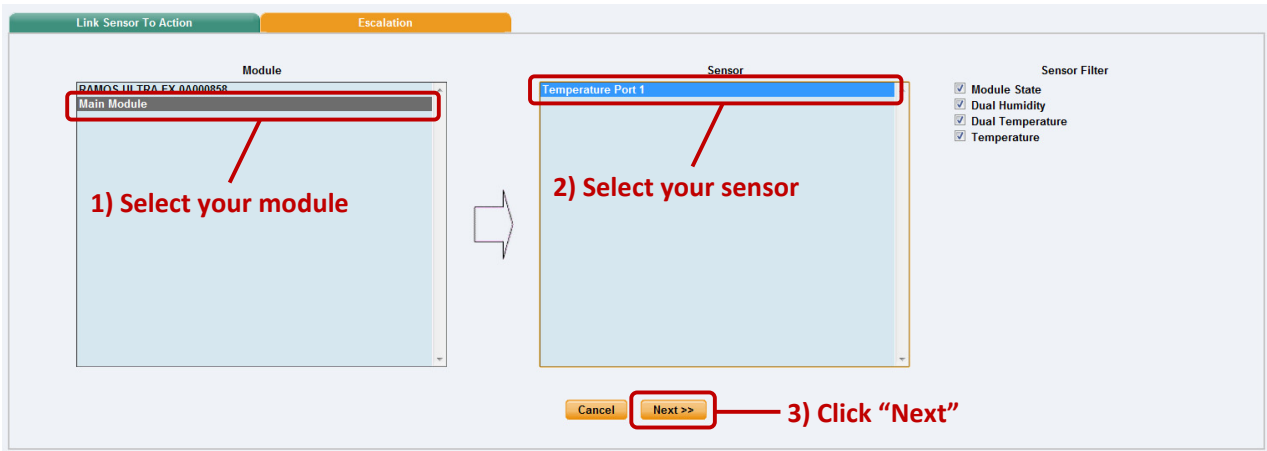
Maximum Times to Resend

Resend Intervals (secs) 10 secs

Cancel Back Next

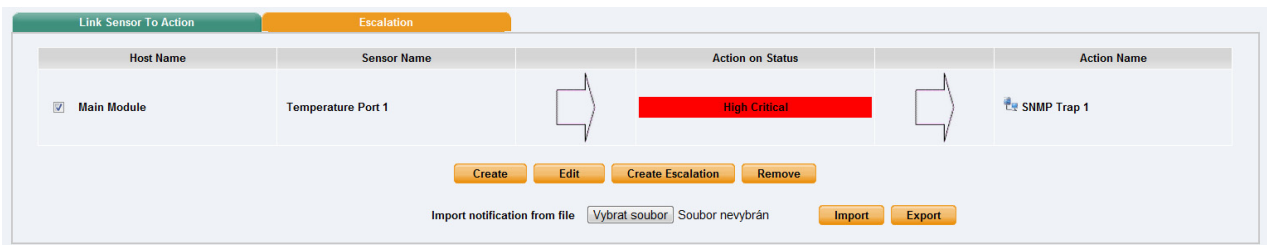
These parameters set the maximum number of times to send the trap notification and the time interval between each notification.

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) 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.

6.3. 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

Location: System Location
Summary Map Sensors Notification Access Control Settings Applications Help
Current System Time: 03/07/2012 13:18:44

Notification Menu
Begin Notification Wizard
Action
• Add Action
Link Sensor To Action
Options
View Notification Log
Notification Analyzer
Help

Please choose a name for your email Action. Descriptive Action names increase the simplicity of the system.

Complete the Mail To, From and CC fields with correctly formatted e-mail addresses. The Mail To and From fields are mandatory. Multiple recipients may be entered by separating addresses by a comma (,) or semicolon (;).

Please select Cancel to leave the edit mode and go back to the menu without saving.

Write a name of email action
Action Name: Email 1

Write a recipient
Mail From
Mail To
Mail CC
Mail BCC

Cancel Next

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.

Location: System Location
Summary Map Sensors Notification Access Control Settings Applications Help
Current System Time: 03/07/2012 13:26:34

Notification Menu
Begin Notification Wizard
Action
• Add Action
Link Sensor To Action
Options
View Notification Log
Notification Analyzer
Help

This is a preview of the message that will be sent to your recipient(s). The sent message will include the details relevant to your sensor.

Click Customize to change the format of this message. The items in your message with a dollar sign and parentheses e.g. \${TIME} represent the data to be imported into your message at the time of sending. Please click the Macro Description button for a full list.

Click Enable Picture to attach a Picture with your message. Select to attach either the Current Picture from the Camera or the most recent Picture Stored on the Picture Log. Select which Cameras you would like to use as the source of your picture.

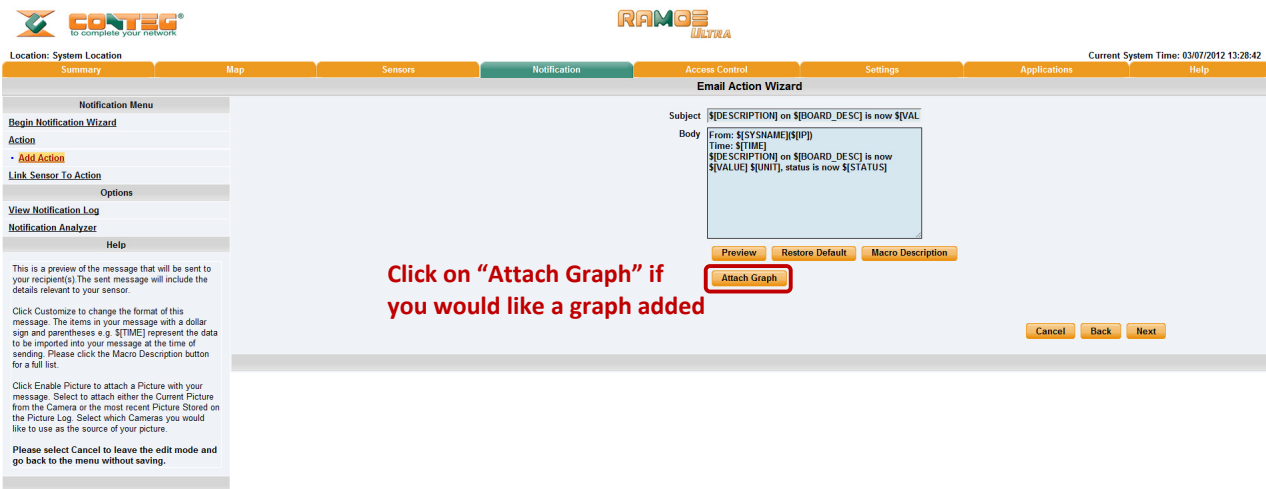
Please select Cancel to leave the edit mode and go back to the menu without saving.

Click on “customized”
Customized

Attach Graph

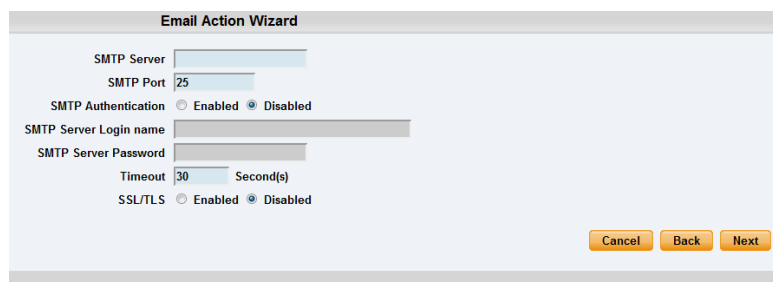
Cancel Back Next

Subject: Testing Sensor Port 1 on \${BOARD_DESC} is now 0
Body: From: System Name(192.168.161.237)
Time: 13:14:43
Testing Sensor Port 1 on \${BOARD_DESC} is now 80 Unit, status is now Normal



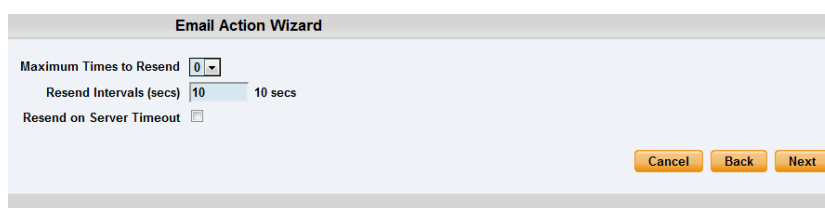
After this click “Next”

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



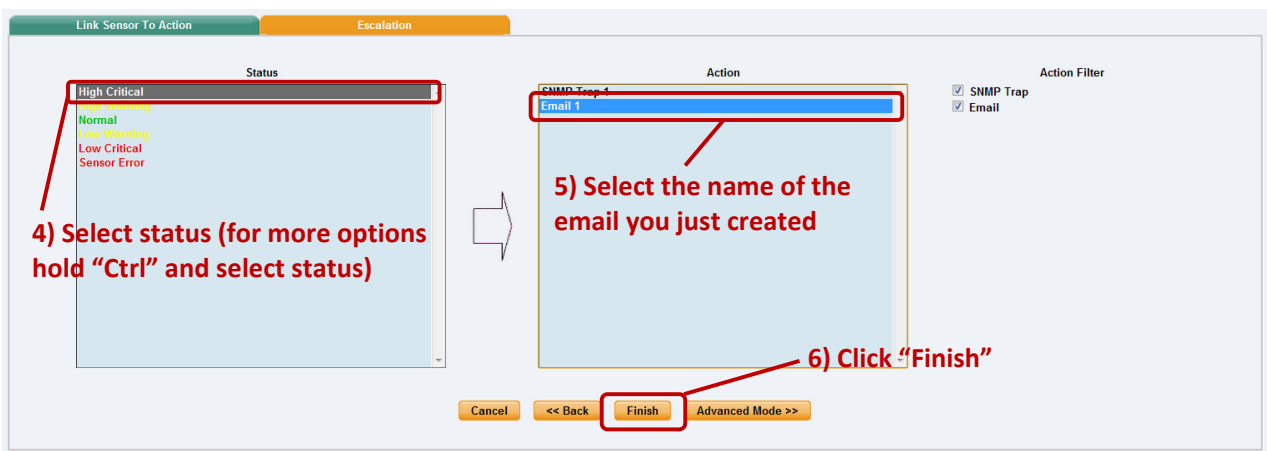
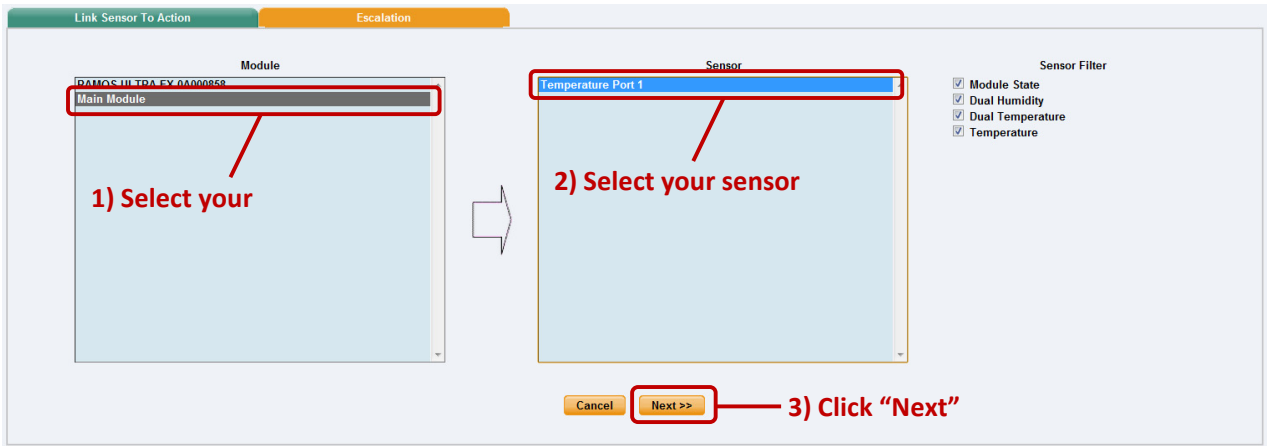
Once this when is correct, click next.

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) At the main notification page you should now see listed our two notifications, the SNMP trap and the e-mail.

Host Name	Sensor Name	Action on Status	Action Name
<input checked="" type="checkbox"/> Main Module	Temperature Port 1	High Critical	SNMP Trap 1
<input checked="" type="checkbox"/> Main Module	Temperature Port 1	High Critical	Email 1

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 Critical"

6.4. 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.

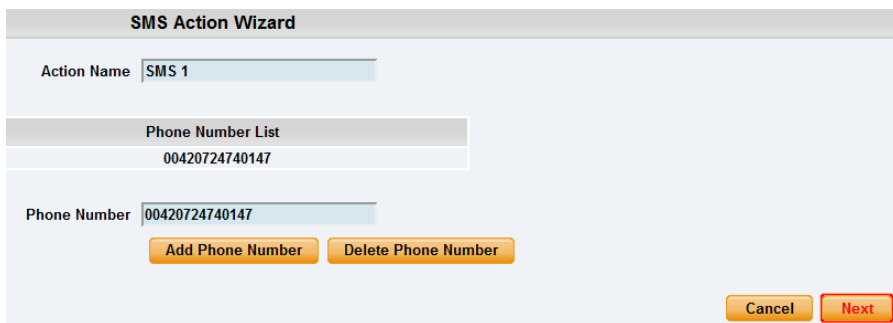
To get to the starting point of this tutorial:

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

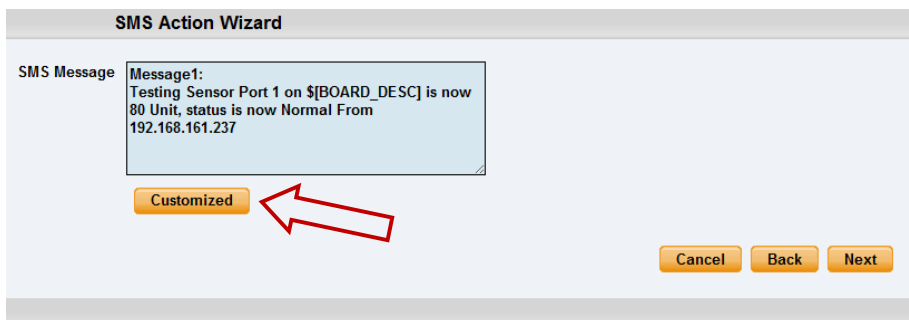
a) From the list of notification types select SMS and click next. You will then be presented with this:



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

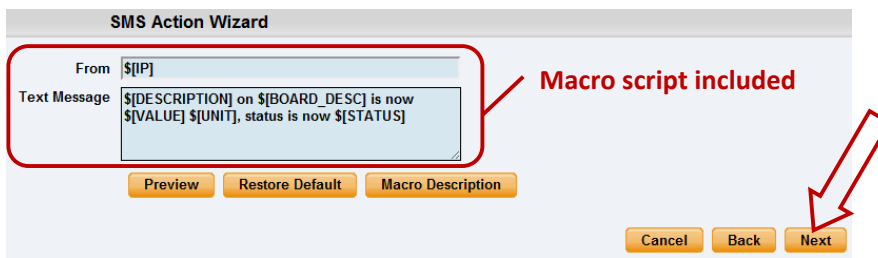


c) Now we will set up the message that will be sent to the phone. You will see the following screen.

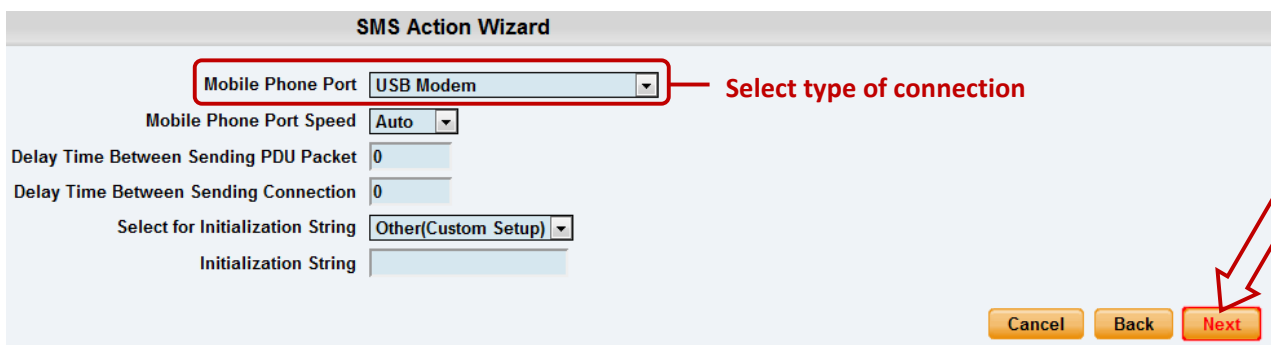


Note: A macro is a script that returns specific data collected by the unit. In our example here the macro will tell the notification to contain the “description” (sensor name), the value (current sensor reading) and the status (high/low warning etc.) these macros are common to all sensor notifications.

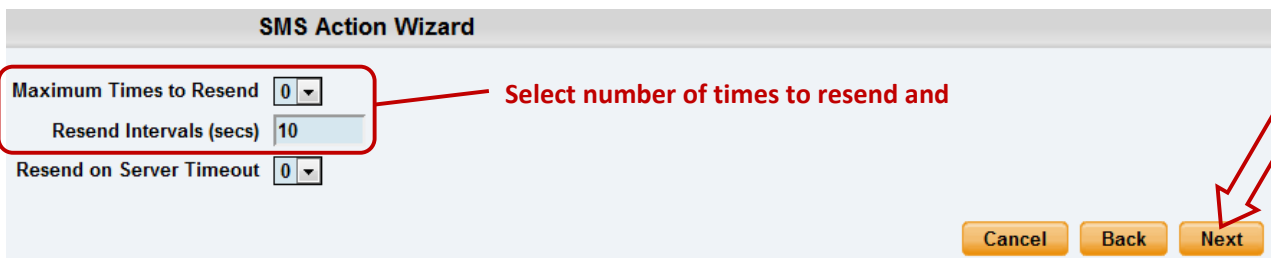
d) You will now see that the SMS message has changed its format to include the Macro script.



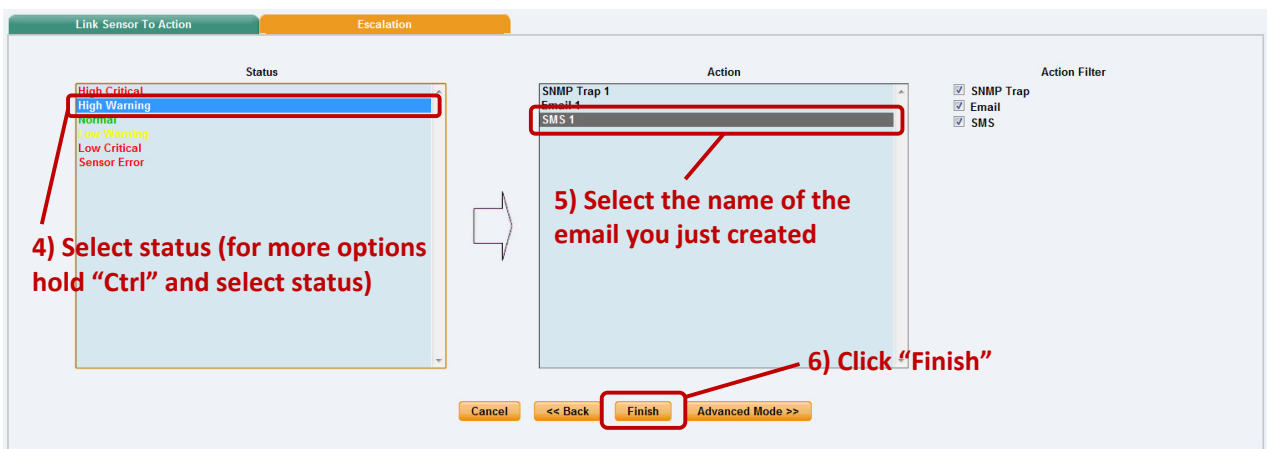
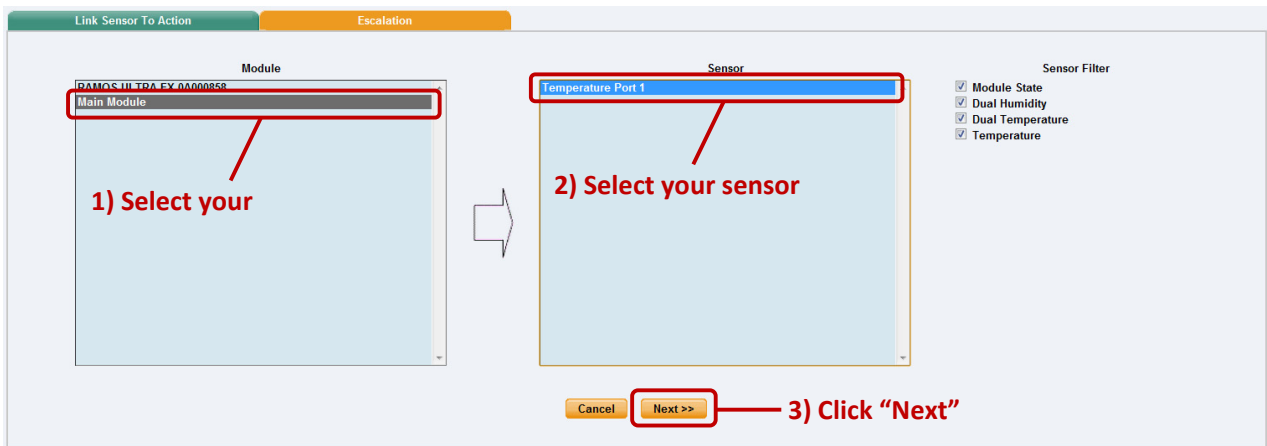
e) Next we will choose to set up the type of connection. This will depend on the type of modem you are connecting. For the purpose of this tutorial we will assume you are connecting a GSM/GPRS enabled modem to the USB port. Therefore we will select "USB Modem" from the list.



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 High Warning. Then select the notification name we assigned, in this case we chose "SMS 1". Click Finish to finalize this.

h) 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.

Host Name	Sensor Name	Action on Status	Action Name
<input checked="" type="checkbox"/> Main Module	Temperature Port 1	High Critical	SNMP Trap 1
<input checked="" type="checkbox"/> Main Module	Temperature Port 1	High Critical	Email 1
<input checked="" type="checkbox"/> Main Module	Temperature Port 1	High Warning	SMS 1

Import notification from file Soubor nevybran

For the purposes of this tutorial we will not cover the setup 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 ramos@conteg.com.

7. 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

7.1. 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.

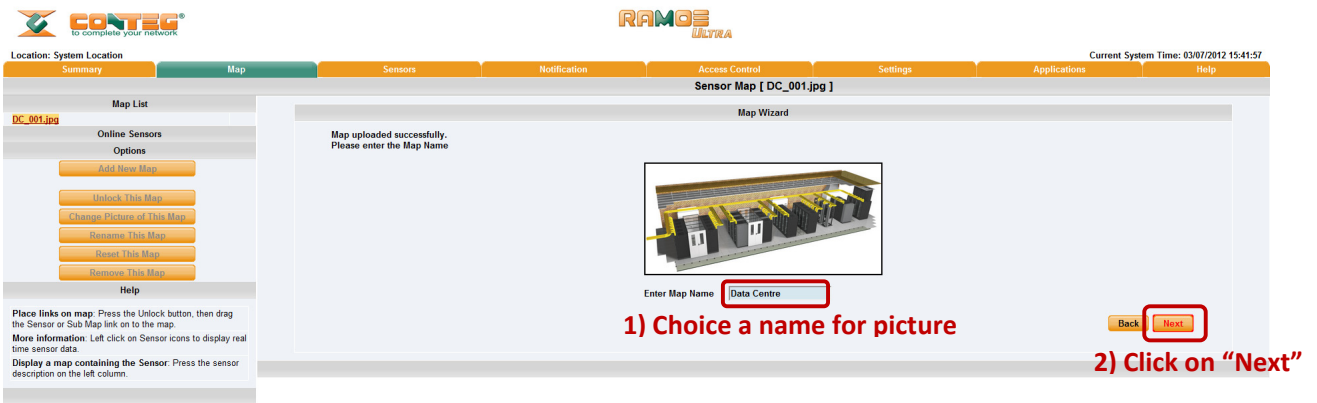
1) Click on “Map” tab

2) Click on “Add New Map”

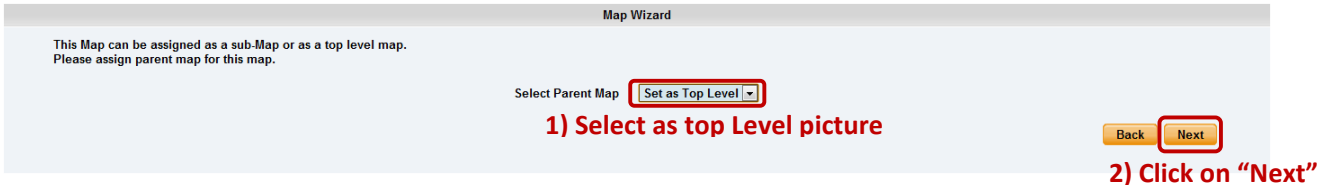
b) Now you can browse to the file on your HDD you wish to use.



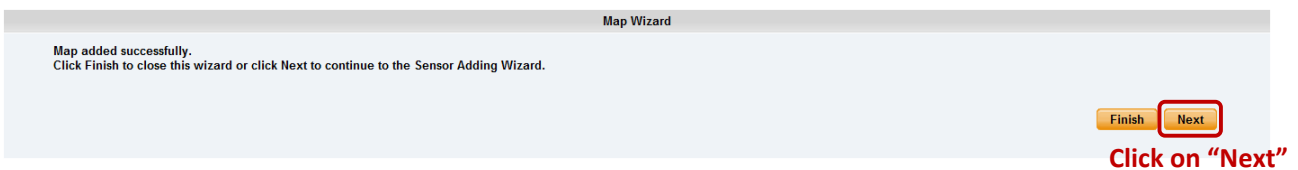
c) In this tutorial we are going to use a 3D map of a data centre we are monitoring.



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.



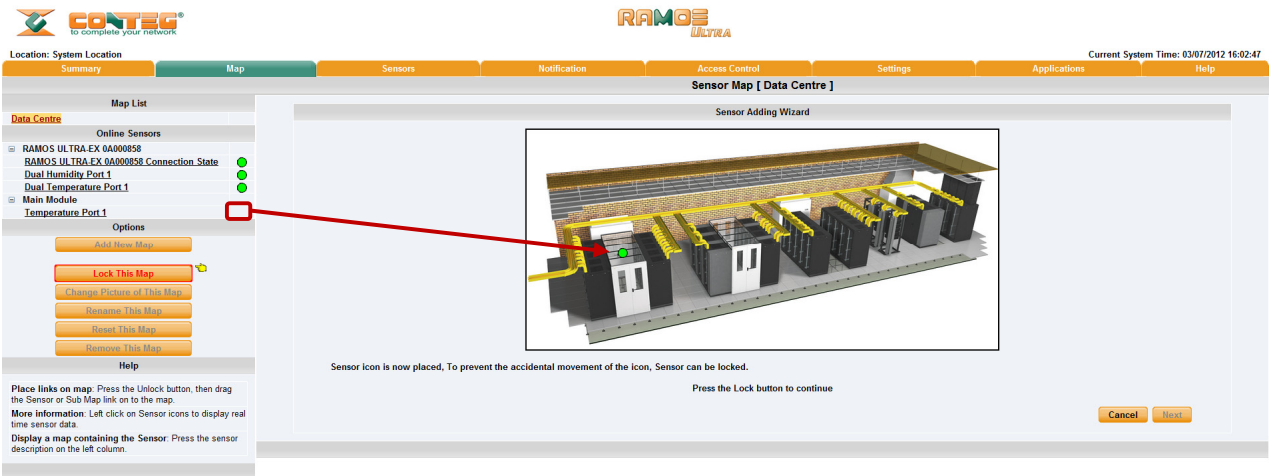
f) You will now be taken to the map page where it will display your map. To continue adding the sensors click next.



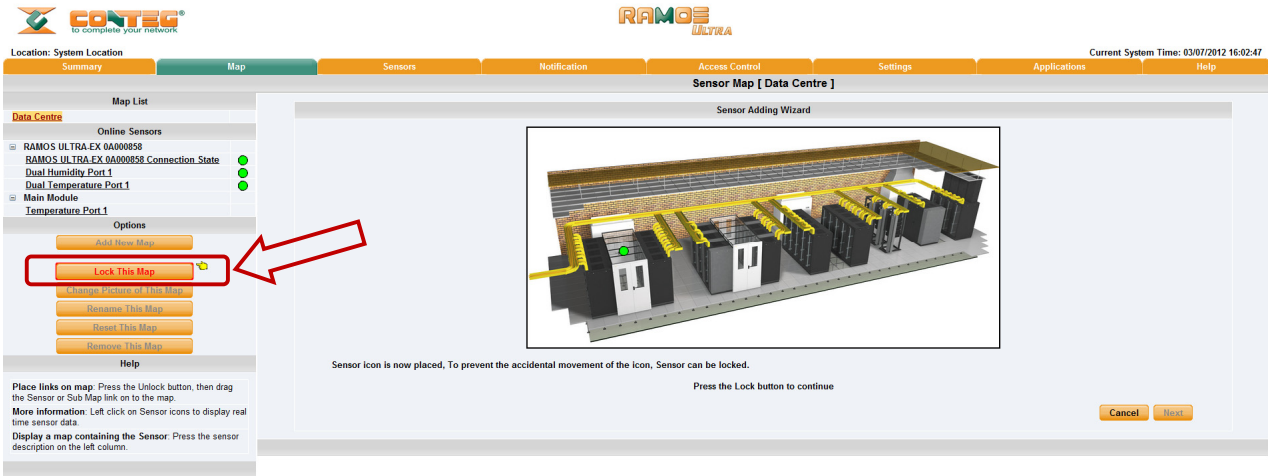
g) After clicking next you will be directed to click the "Unlock" button.



h) 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 “Lock This Map”



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

7.2. Monitoring via the map interface

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

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

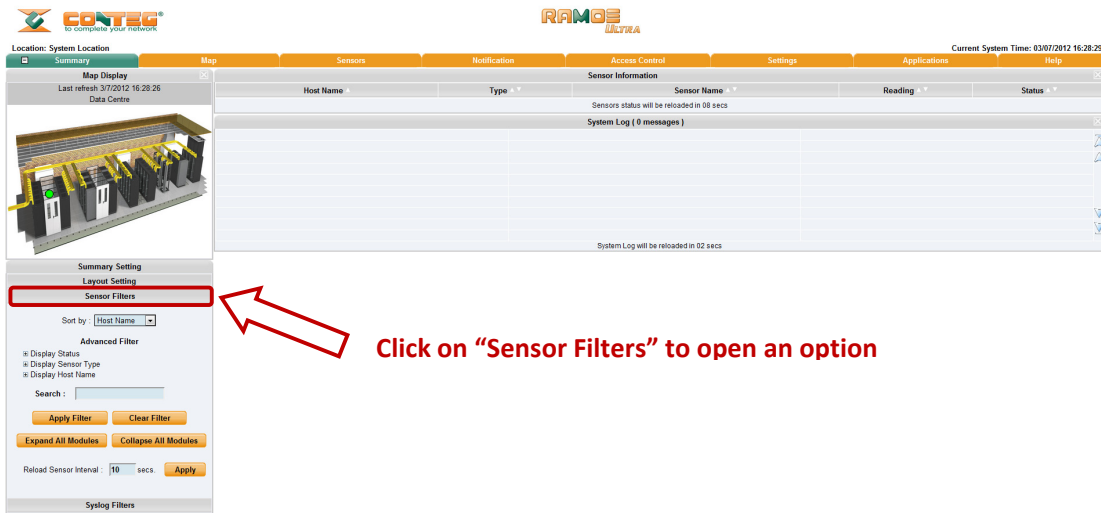


If you connect other sensors, these too can be dragged and positioned on the map.

8. Filters

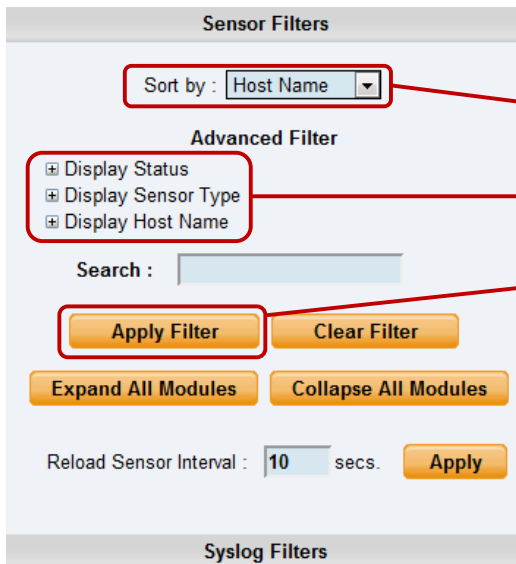
8.1. Sensor filters

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:



Click on "Sensor Filters" to open an option

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:

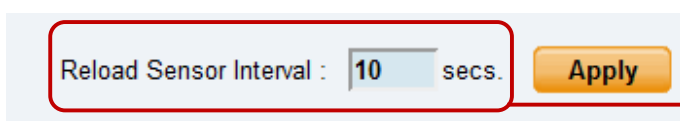


Sorting options are found here

Select various options to customize your viewing window data

Click here to save your changes

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



To alter your reload time, enter a new value here

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

The screenshot shows the 'Sensor Information' window in the CONTEG RAMOS ULTRA interface. The window displays a table with the following data:

Host Name	Type	Module	Sensor Name	Reading	Status
RAMOS ULTRA-EX 0A000858	Temperature	Main Module	RAMOS ULTRA-EX 0A000858 Temperature Port 1	23.5 °C	Normal

Below the table, there are status messages: 'Sensors status will be reloaded in 07 secs' and 'System Log (0 messages)'. A red box highlights the table, and a red arrow points to it with the text 'Your changes are display here'.

8.2. Syslog filters

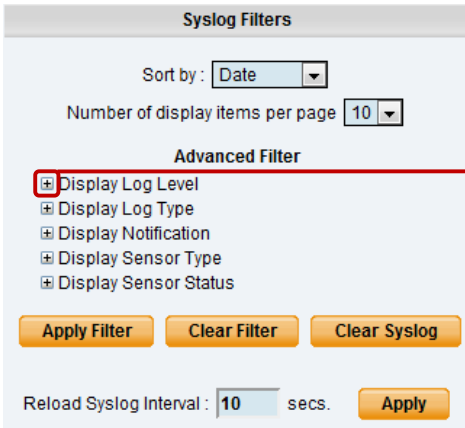
Syslog filters enable you to customize your syslog window. To begin select the “Syslog filter” tab found on the summary page:

The screenshot shows the 'Syslog Filters' window in the CONTEG RAMOS ULTRA interface. The window displays the following settings:

- Sort by:
- Number of display items per page:
- Advanced Filter:
 - Display Log Level
 - Display Log Type
 - Display Notification
 - Display Sensor Type
 - Display Sensor Status
- Buttons:
- Reload Syslog Interval: secs.

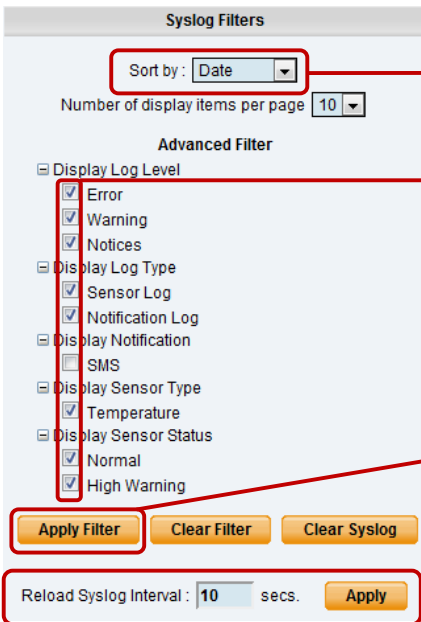
A red box highlights the 'Syslog Filters' section, and a red arrow points to it with the text 'Syslog filters are here'.

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 become available

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



Sorting options are found in the drop down menu

Various check boxes can be picked and unpicked to customize your filter window

Click here to save your selection

To change your reload interval enter a new value here and click “Apply”

Altering your reload interval can be achieved by using the options shown above:

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:

The screenshot shows the CONTEG RAMOE ULTRA web interface. The top navigation bar includes tabs for Summary, Map, Sensors, Notification, Access Control, Settings, Applications, and Help. The current system time is 04/07/2012 09:38:02. The main content area is divided into several sections:

- Map Display:** Shows a 3D perspective view of a data center with server racks.
- Sensor Information Table:**

Host Name	Type	Sensor Name	Reading	Status
RAMOS ULTRA EX 0A000858	Dual Humidity	Dual Humidity Port 1	55 %	Normal
Main Module	Dual Temperature	Dual Temperature Port 1	24.2 °C	Normal
	Temperature	Temperature Port 1	25.5 °C	Normal
- Syslog Log (2 of 10 messages):** A table showing log entries:

1	2012/07/04 09:37:43	Temperature Port 1 is 27.5 °C; status is Normal
2	2012/07/04 09:36:58	Temperature Port 1 is 30.0 °C; status is High Warning
- Summary Setting:** Includes options for Layout Setting, Sensor Filters, and Syslog Filters. The Syslog Filters section has a 'Sort by' dropdown set to 'Date' and a 'Number of display items per page' set to '10'. There are checkboxes for various log levels (Error, Warning, Notices) and types (Sensor Log, Notification Log, SMS, Sensor Type, Temperature, Sensor Status, Normal, High Warning). Buttons for 'Apply Filter', 'Clear Filter', and 'Clear Syslog' are present.

9. 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.

Simple setup:

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

Your unit's IP address is the default 192.168.0.100.

Your computer's IP address is 192.168.0.200

Your router's IP address is 192.168.0.300

- b) b) To find out your routers external IP address, go to www.seemyipaddress.com

Let's imagine your router's external IP address is 278.67.04.09

- c) You now need to setup port forwarding on your router. This varies depending on your routers model. Generally you need to point your browser to your router's IP address (in this case 192.168.0.300). This will then allow you to log into your router's administration interface. You can find how to go about doing this for your router on www.portforward.com.

For 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 that when you access your router using the external IP address you will be forwarded to your unit's internal IP address.

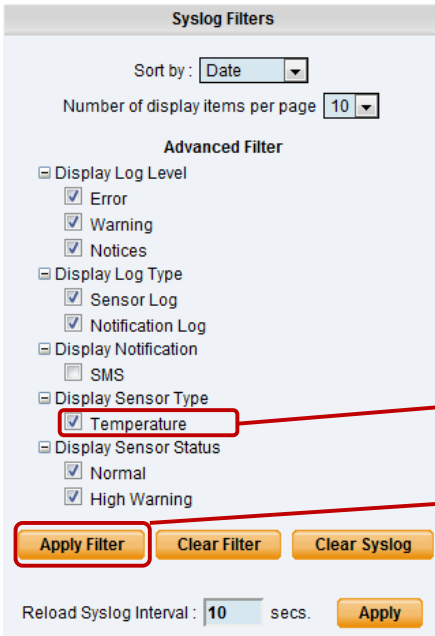
- d) To test this, open your web browser, and go to your external IP address (in our example 278.67.04.09). If you using a dynamic IP address, its best to check it again before doing this as it may have changed since the start of this tutorial.
- e) To make this easier you could use a dynamic DNS (Dynamic Name Server). This means you no longer need to remember IP addresses or use www.seemyipaddress.com to find out your IP address. You will instead register a domain name (for example myRamosUltra.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.
- 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.

10. FAQ

- a. [I cannot see the temperature sensor displayed on summary page](#)
- b. [I cannot access my unit's web based interface](#)
- c. [What do my LED lights mean?](#)
- d. [I have forgotten my unit's IP address](#)
- e. [I have forgotten the password for my unit](#)
- f. [Can I use DHCP to assign my units IP address?](#)
- g. [How do I set up my routing table?](#)
- h. [How can I change my administrator password?](#)
- i. [What functions do different types of notifications provide?](#)
- j. [Can I connect my unit via WiFi?](#)
- k. [What is the heartbeat message?](#)
- l. [What is the Network Sniffer?](#)

a) 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:



Click on “Display sensor type” and check the box marked “Temperature”

click on “Apply Filter”

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

b) I cannot access my units web interface

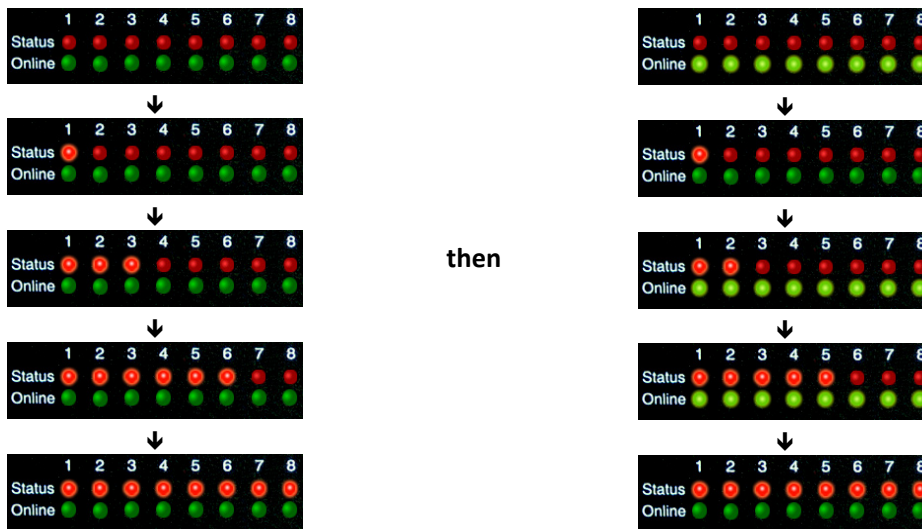
If you are having issues with network connectivity, first ensure that the link100 LED is lit on the front display of the unit. If this is not lit then you have no network connection present. If this is the case then ensure the following:

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

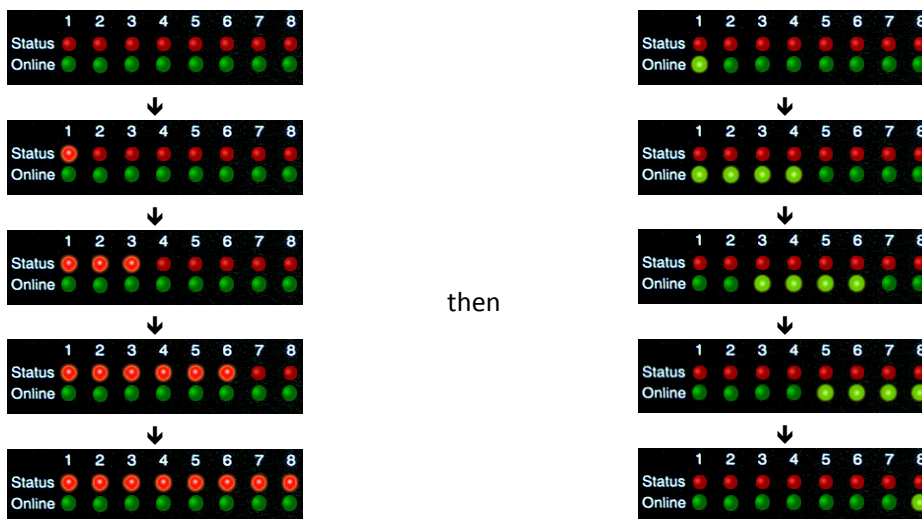
c) What do my LED lights mean?

The following diagrams show what the various LED displays mean.

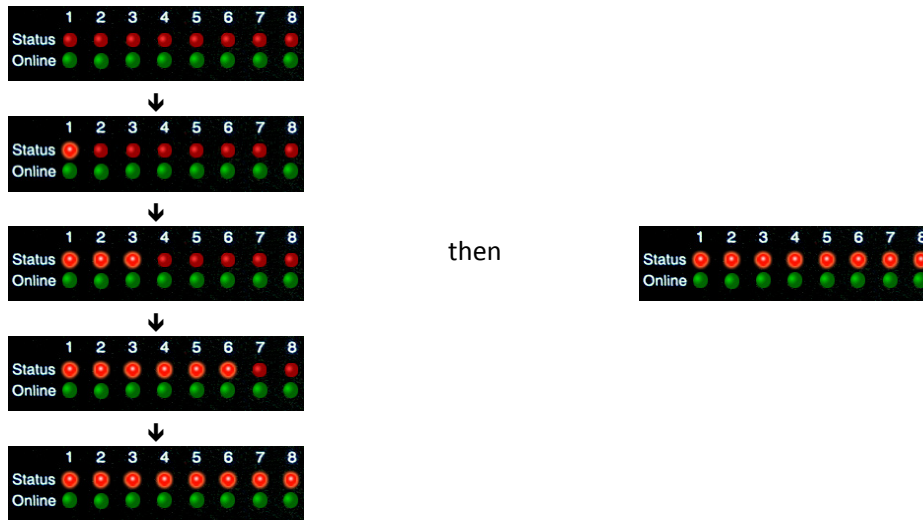
LED patterns in **Normal mode**



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 on-board 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.

d) I have forgotten my unit's IP address

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

e) I have forgotten the password for my unit.

Hold down the reset button for 7 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 7 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.

f) Can I use DHCP to assign my unit's 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.

g) 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 in with the crossover cable.

Now ping* 192.168.0.100 to see if the connection was successful.

h) 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:

- 1) Log into your unit using the default password.

2) Point towards the settings tab.

1) Click on "Settings"

2) Click on "System Administrator" and then on "User & Group management"

3) Select the User "Administrator"

4) Click on "Properties"

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

1) Input a new passwords

2) Press "Finish"

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

The notifications are used to notify you when a sensor reading has hit a certain pre-set "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.

Alarm sound: This notification will sound an alarm.

Speech: Creates a text to speech notification.

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.

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 ramos@conteg.com

j) Can I connect my unit via Wi-Fi?

Yes, you can connect the unit via Wi-Fi. 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 Wi-Fi is shown below.

Wifi Network	
Wireless Adapter Status	Not Found (Device is not connected or cannot be initialized)
Wireless Adapter	<input checked="" type="radio"/> On <input type="radio"/> Off
Default Interface	<input type="checkbox"/> Use this Interface as the Default Gateway.
Use DHCP	<input type="radio"/> Yes <input checked="" type="radio"/> No
IP Address	192.168.0.10
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.161.250
Domain Name Server	192.168.161.5
Wireless SSID	
Encryption Mode	<input checked="" type="radio"/> Disabled <input type="radio"/> 64bit WEP
Link Status	Not connected
Signal Strength	0%
<input type="button" value="Save"/> <input type="button" value="Reset"/>	

k) What is the Heartbeat message?

This setting is to have the RAMOS Ultra notify you it is still running. You can be notified by either traps 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.*

I) What is the network sniffer

The Network Sniffer application can be used to capture network packets running to and from the RAMOS Ultra, 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.