



# **Remote Watchman™ Enterprise 2020 User's Manual**

**Manual P/N 071-0146 Rev 11    July 3, 2023**

Copyright © 2002-2023, Sensorsoft Corporation, All rights reserved.  
Sensorsoft, Alert and Remote Watchman are trademarks of Sensorsoft Corporation.



# Table of Contents

About This Manual .....	6
Glossary of Acronyms .....	6
Overview .....	7
System Requirements for running RWME .....	8
System Requirements for the web browser .....	8
Specifications of RWME .....	9
Installation of RWME.....	11
Installing from a CD .....	11
Installing from a Download File.....	11
Removal of RWME .....	12
Using RWME.....	13
Logging in from web browser on computer where RWME is installed .....	13
Logging in from web browser on another computer on same network .....	13
Stopping and Starting the RWME service .....	15
Stop the RWME service with SCM/Services app .....	15
Start the RWME service with SCM/Services app .....	15
Controlling the RWME service from command line.....	16
Setting up Monitored Items/Nodes .....	17
Monitoring a Sensorsoft device .....	17
Monitoring security or safety devices on the SS6420 .....	18
Monitoring a TCP or Web server port .....	20
Monitoring a network camera.....	21
Monitoring a Sensorsoft Alert appliance .....	22
General Usage .....	24
Accounts and passwords.....	24
RWME administration.....	24
Address Book .....	26
The Monitor List .....	27
Reordering the Monitor List.....	28
Selecting variables to display on the Monitor List .....	29
Automatically refreshing the Monitor List page .....	30
Arranging Monitored Items/Nodes in Groups .....	31
Add a new monitor group.....	31
Renaming a monitor group .....	32
Selecting a monitor group to view in the Monitor List.....	32
Logging Data .....	33
Data file naming convention.....	33
Graphing data files.....	33
Viewing log files .....	34
Alerting .....	35
What are Scalar and Boolean variables .....	35
What are Scalar breach limits .....	35
What are Boolean breach limits.....	35
Setting up Alerts .....	36
Creating address book members.....	38
Adding a person to the address book.....	38

Adding a command line to the address book .....	39
Setting up SMTP host names .....	39
Sending a test email message .....	40
Sending a message to a pager device using a modem .....	40
Setting up the modem .....	40
Sending a test SMS message .....	41
Sending a test DTMF message to a numeric only pager .....	42
Setting up a command line .....	43
Sending a message to a Windows machine or user .....	43
Shutting down a Windows machine .....	44
Running multiple command lines .....	45
Additional information about command lines .....	46
Controlling Sensorsoft Devices .....	47
Customizing variable description and Boolean strings in the SS6420 .....	48
Security Considerations .....	49
IP blocking and trusting .....	49
Multi-Level user access .....	49
Password encryption .....	49
Inactive user logout timer .....	49
Logged in users count .....	49
Web access history .....	50
Admin use history .....	50
User executables .....	50
User definable web server port .....	50
Troubleshooting Guide .....	50
Web Server problems .....	51
Email problems .....	52
SMS problems .....	53
Common problems .....	55
Getting Help .....	58
Technical Support .....	58
30-day money back guarantee .....	58
Appendix A – SMS/Paging Dial-up Modem Requirements .....	59
DIP switches .....	59
Custom modem strings .....	59
Appendix B – SMS/Paging Tutorial .....	61
Appendix C – Making changes to setup files using a text editor .....	63
Appendix D – Using Dollar Variables in your messages .....	66
Appendix E – Running RWME Pipe Command Lines .....	67
Writing to a Sensorsoft device variable .....	67
Disable and enable alerts .....	68
Set Alert Breach Limits .....	69
Controlling a relay contact .....	69
Running RWME commands in alerting actions .....	69
Exit codes used by RWME .....	70
Appendix F – Running RWME command from Smart phone web browser .....	71
Appendix G – Using XML Output to share live data with other software Applications .....	75
Accessing the XML page .....	75
XML data organization .....	76

Appendix H – List of Breach Conditions and Device Errors that can be used to generate alerts .....77

Appendix J – Configuring the RWME Service to Log on with Administrative Account .78

## About This Manual

This document contains information about installing, configuring, using and troubleshooting Sensorsoft Remote Watchman Enterprise (RWME) 2020 software.

When other sections of this manual are referenced, *italics* are used.

The terms “**sensor**”, “**device**”, “**Sensorsoft device**” (and its acronym “**SSD**”) refer to devices whose model number appears in the section *Specifications and Requirements* under “Sensorsoft Protocol devices supported”.

The terms “**item**” or “**node**” refer to any Sensorsoft Device, TCP server port, network camera or Sensorsoft Alert appliance that is being monitored by the RWME software.

## Glossary of Acronyms

DTMF – **Dual Tone Multi-Frequency** – this is the technical terminology for Touch Tone™

DIP – **Dual Inline Package**

GSM – **Global System for Mobile Communications**

IANA – **Internet Assigned Numbers Authority**

RWME – **Remote WatchMan Enterprise** software

SGT – **Sensorsoft Graphing Tool** software

SCM – **Service Control Manager** for Windows

SMS – **Short Message Service** – defines any alphanumeric message that is sent to a mobile device

SIM – **Subscriber Identification Module** – a small chip card that plugs into a cell phone or modem to give it an identity (i.e. phone number) on a GSM/3G/LTE network

POTS – **Plain Old Telephone Service** – a wired telephone line using analog service

SMTP – **Simple Mail Transfer Protocol** – used to send email messages over a network

SSA – **Sensorsoft Alert** – a standalone network appliance

SSD – **Sensorsoft Device** – a device that incorporates the Sensorsoft Device Protocol

TAP – **Telocator Alpha-Paging Protocol** – used to send alphanumeric messages to a pager

## Overview

Sensorsoft Remote Watchman Enterprise 2020 is Windows based software that allows you to monitor network and environmental conditions, and send alerts or take action on problems. It permits you to monitor sensors, cameras and servers – remotely over any TCP/IP network. By employing a powerful integrated web server that runs as a Windows service, you can keep watch from anywhere in the world using a web browser.

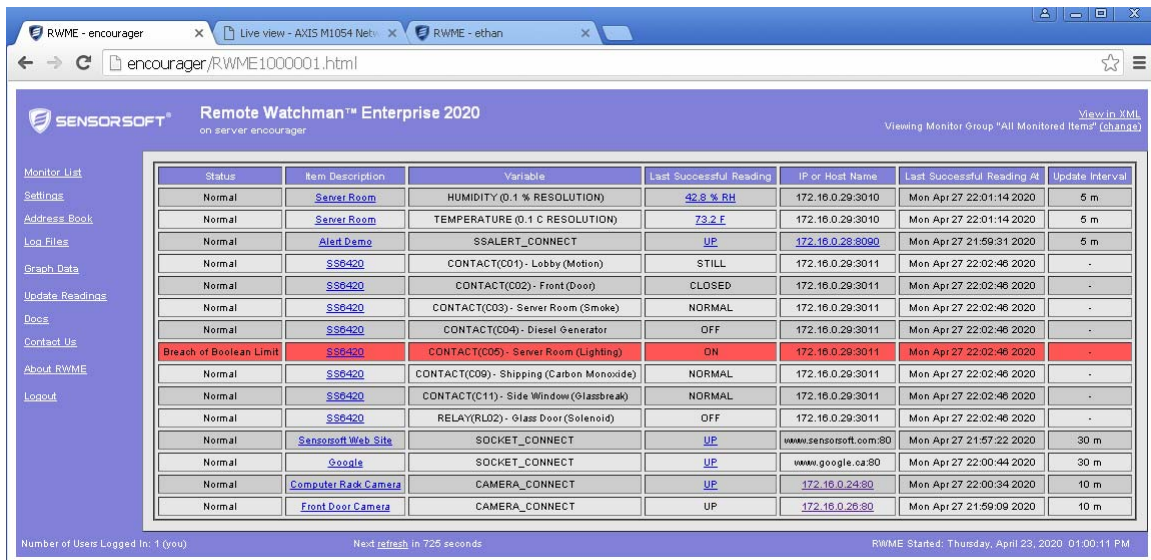


Figure 1(a): RWME Monitor List page

Remote Watchman Enterprise has the ability to issue email and SMS alerts and launch command lines, when the limits that you set become unacceptable.

The data logged by Remote Watchman Enterprise can be graphed using the integrated Sensorsoft Graphing Tool (SGT) software or exported to another application like Microsoft Excel.

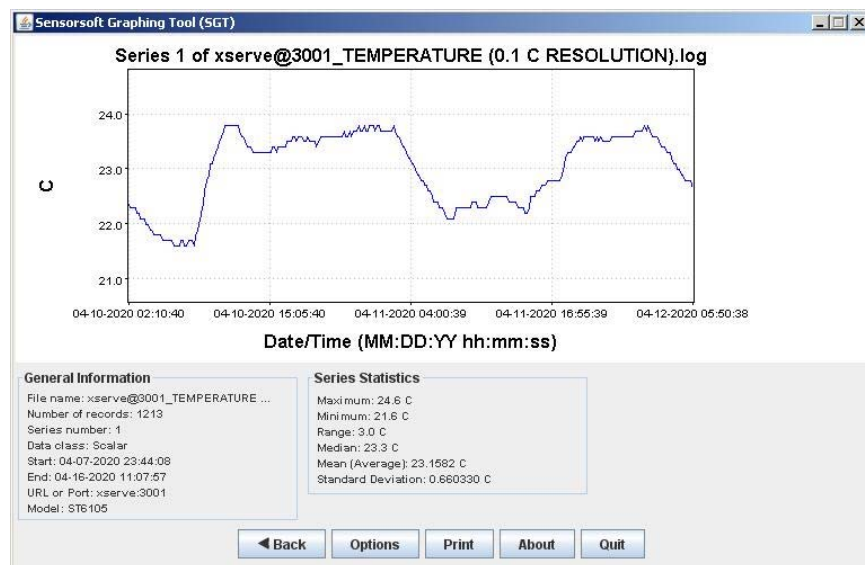


Figure 2: Sensorsoft Graphing Tool (SGT) app

## System Requirements for running RWME

**Operating System (OS):** Microsoft Windows 2000, XP, Vista, 7, 8, 10 or Windows Server 2000, 2003, 2008, 2012, 2016. When the number of monitored items/nodes is at or greater than 10 we recommend a Windows Server OS.

**CPU:** Intel Pentium II 300 MHz processor or greater

**Machine Form Factor:** Desktop, tower workstation or rack mount server designed to run continuously (24/7). Do not use a mobile computer like a laptop or notebook.

**RAM:** 256 MB (more is required as number of monitored items/nodes increase)

**Hard disk space:** 10 MB minimum for product install. Recommend 1 GB free space for log files. Installation program will take at least 25 MB of free space.

**CD-ROM drive:** If installing from CD media

Modem is required if SMS or DTMF numeric paging is used

**TCP/IP LAN or Internet connection** is required

**TCP/IP Services** must be installed

SMTP compliant mail server, if email alerts are required

## System Requirements for the web browser

**Minimum Graphics screen resolution:** 1024 × 768 pixels

**Java Runtime Environment (JRE):** Version 5.0 or later needs to be installed to use the Sensorsoft Graphing Tool (SGT) app software.

**Web Browser:** Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox, Google Chrome, and Apple Safari.



**IMPORTANT – JavaScript and cookies** must be enabled in your web browser to support many of the features in RWME.



## Specifications of RWME

**Monitored Item/Node Types:** Sensorsoft Devices, TCP Servers, Network Cameras (Axis, Panasonic and Canon), Sensorsoft Alert appliances

**Sensorsoft Protocol Devices Supported:** ST6105J/C; ST6154J/C; SM6204J/C; SM6201C/CP; SS6201J; SR6170J; SR6171J; SR6172J; SP6400J; SS6402J; SS6610J/C; SS6420E/J; SS8002 (Sensorsoft Device Protocol Version 2 and 3 are supported)

**Item/Node Polling Rate:** selectable from 1,2,3,4,5,10,15,20,25,30,35,40,45,55 minutes and 1,2,4,6,12,24 hours

**Maximum Number of Monitored Items/Nodes:** Depends on license level. The unlimited license will be limited by the machines performance (available RAM and CPU speed)

**Maximum Number of Monitor Groups:** Cannot exceed the number of monitored items/nodes

**Number of User Accounts:** Two, admin (administrator) and ruser (read-only)

**Number of Simultaneous Users:** No limit

**Login Authentication:** Two factor, Username and Password (clear text over http)

**Login IP Access List:** Trusting or blocking is supported; IP addresses must be entered individually.

**Inactive User Logout Timeout Range:** Never, 1 to 60 minutes

**Monitor List Page Automatic Refresh Rate:** Never, 1 to 2147483647 seconds

**Monitor List Page Columns:** Status, Description, Variable, Last Successful Reading, Location, Host:Port, Comments, Group, Last Successful Reading At, Last Attempted Reading At, No. of Successful Consecutive Readings, Update Interval, Estimated Uptime, Vendor, Model

**Monitor List Page Alert Colors:** User selectable from 13 pre-defined colors

**Monitor List Page Font Sizes:** Standard, Small

**Alerting Methods:** Email, SMS/Paging, command line execution

**Maximum Alerting Rate:** every five minutes for a single state change

**Email Protocol:** SMTP (client side only)

**SMTP Authentication:** Login (base64 encoded password)

**Definable SMTP Servers:** 2

**SMS and Paging Protocols:**

- SMS using TAP and a dial-up modem and POTS (wired) phone line
- SMS using a GSM/3G/LTE cellular radio modem, SIM card and a service provider. Supports PDU (Unicode) and Text modes
- DTMF numeric paging using dial-up modem and POTS (wired) phone line

**Modem Com Port:** 1 supported, can use COM 1 through 255

**Supported Modem Types:**

- US Robotics Sportster Voice 56K
- US Robotics Sportster
- U.S. Robotics 5633 56K USB Fax
- U.S. Robotics Courier V.Everything
- Hawkings USB
- Hayes
- Older Hayes
- Custom/User Definable
- Any GSM/GPRS/3G/LTE cellular radio modem with an RS232 serial or USB port
- USR3500 Courier M2M 3G Cellular Modem

**Web Server Protocol:** HTTP v1.1

**Default Web Server Port:** TCP Port 80 (user definable)

**Alert Limit Types:** Boolean, Warning, Critical, Return to Non-Alert State

**Temperature - Unit of Measures:** Celsius, Fahrenheit

**Alert Types:** Breach of Critical Limit, Breach of Warning Limit, Breach of Boolean Limit, Return to Non-Alert State (for Breach types only), Device Model Changed, COMM Corrupted, TIMEOUT, OFFLINE, ONLINE, EEPROM Failure, LOW SUPPLY VOLTAGE, TAMPER

**Alert Actions:** Email (SMTP), SMS (TAP or Cellular), Numeric DTMF and Command Line

**Alert Message \$ Variables:** Description (\$D), Comments (\$C), Location (\$L), Host:Port (\$P), Variable Name (\$V), Variable Value (\$R), Variable Description (\$Z), Alert Type Description (\$A), List Item/Node Variables and Values (\$X), New Line (\$N) and Date and Time (\$T).

**Alert Intervals:** Once only, repeat every 5 minutes to 24 hours

**Address Book Entries for Alerting:** People, Command Lines and Alert Groups

**Maximum Log File Size:** Limited by Windows Operating System and available disk space

**Log File Lines Viewable through Web Server:** May be set to unlimited or a finite number of most recent log entries

**XML Output:** Includes all data available in the monitor list. A schema file (xsd) is provided

**Graphing Software:** Sensorsoft Graphing Tool (SGT), signed Java Web Start app

## Installation of RWME

To install the RWME software you need to be logged into the target computer as the administrator. Administrative privileges are required in order to add the RWME service to your computer. Please carefully execute the following steps to install the RWME software:

### Installing from a CD

1. Log into the target computer as the Windows administrator, where you want to install the RWME software.
2. Close any open applications.
3. Place the Remote Watchman CD into the target computer's CD drive.
4. The autorun sequence of the CD should open a web page in your default web browser. If it does not, this file can be opened manually. The file that you should open is named **Version Index.html**, and can be found in the root directory of the CD.
5. From this web page you will find out what versions of software are contained on the CD. Follow the link under the Remote Watchman Enterprise 2020 heading. This will lead you to a file named setup.exe. Double-click this file to run the installer and wait for on screen instructions.
6. You must accept the license agreement before the installer will continue. PLEASE READ THIS AGREEMENT CAREFULLY.
7. Enter the required license key or serial number as printed on the front of your Remote Watchman CD jewel case.
8. After the installation has completed, you will be asked if you would like to start the Sensorsoft RWME service. If you would like to use a TCP port other than 80 for the web server, choose No, and refer to *Troubleshooting: Web Server Problems* for further instructions, otherwise, choose Yes.

### Installing from a Download File

1. Log into the target computer as the Windows administrator, where you want to install the RWME software.
2. Download the following file to the target computer;

<https://www.sensorsoft.com/download/rwme-v2020-b651-setup.exe>

3. Close any open applications.
4. Double click the download file to launch the installer.
5. You must accept the license agreement before the installer will continue. PLEASE READ THIS AGREEMENT CAREFULLY.
6. Enter the required license key or serial number provided to you electronically.
7. After the installation has completed, you will be asked if you would like to start the Sensorsoft RWME service. If you would like to use a TCP port other than 80 for the web server, choose No, and refer to *Troubleshooting: Web Server Problems* for further instructions, otherwise, choose Yes.

## Removal of RWME

During removal of RWME, you will need to be logged into the target computer as administrator. Administrative privileges are required in order to remove the RWME service. Please carefully execute the following steps to remove the RWME software:

1. Log into the target computer as the Windows administrator, where RWME was installed.
2. Close open applications.
3. From the Windows Start button choose **Settings->Control Panel->Add/Remove Programs**.
4. Select Sensorsoft Remote Watchman Enterprise 2020 from the list and click the Remove button.

## Using RWME

The RWME software starts automatically along with Windows operating system on the computer where it is installed. To use the RWME software you must login with a web browser as described below.

### Logging in from web browser on computer where RWME is installed

On the computer where RWME is installed, click the Windows Start button and choose:

```
All Programs->Sensorsoft Remote Watchman Enterprise (RWME) 2020
->Login to RWME
```

You should see your web browser start and the RWME login page appear as in Figure 3. Then type in the username and password in the appropriate fields. The admin and ruser accounts have a default password of **begin**.

Click the **Log In** button or press the Enter key. You should now see the monitor list page.

If you don't see the RWME login page it is likely that the URL shown for shortcut [Login to RWME] is set to a web port not being used by RWME. You can determine the web server port used by RWME after checking the records in the **rwme.log** file located in the Logs folder of the RWME installation directory. If this record shows the default port of 80, make sure the URL for [Login to RWME] is as follows:

```
http://localhost/RWME
```

If this log file shows RWME using another web server port, for example 8090, make sure the URL for [Login to RWME] is set as follows:

```
http://localhost:8090/RWME
```

You can edit the URL for [Login to RWME] by right clicking on it and choosing Properties. Make any changes required as above and click OK.

### Logging in from web browser on another computer on same network

1. Determine the IP address or host name of the computer where you installed RWME.
2. From a web browser on another computer type the following into its address box replacing the <IP address> portion with the IP address or host name of the computer where RWME is installed:

```
http://<IP address>/RWME
```

3. If you don't see the RWME login page it is likely RWME is not using the default web server port of 80. You can determine the web server port used by RWME after checking the records in the **rwme.log** file located in the Logs folder of the RWME installation directory. If this log file shows RWME using another web server port, for example 8090, make sure to use the format shown below:

```
http://<IP address>:<port number>/RWME
```

4. When the login page appears as shown in Figure 3, type in the username and password in the appropriate fields. The admin and ruser accounts have a default password of **begin**.
5. Click the **Log In** button or press the Enter key.

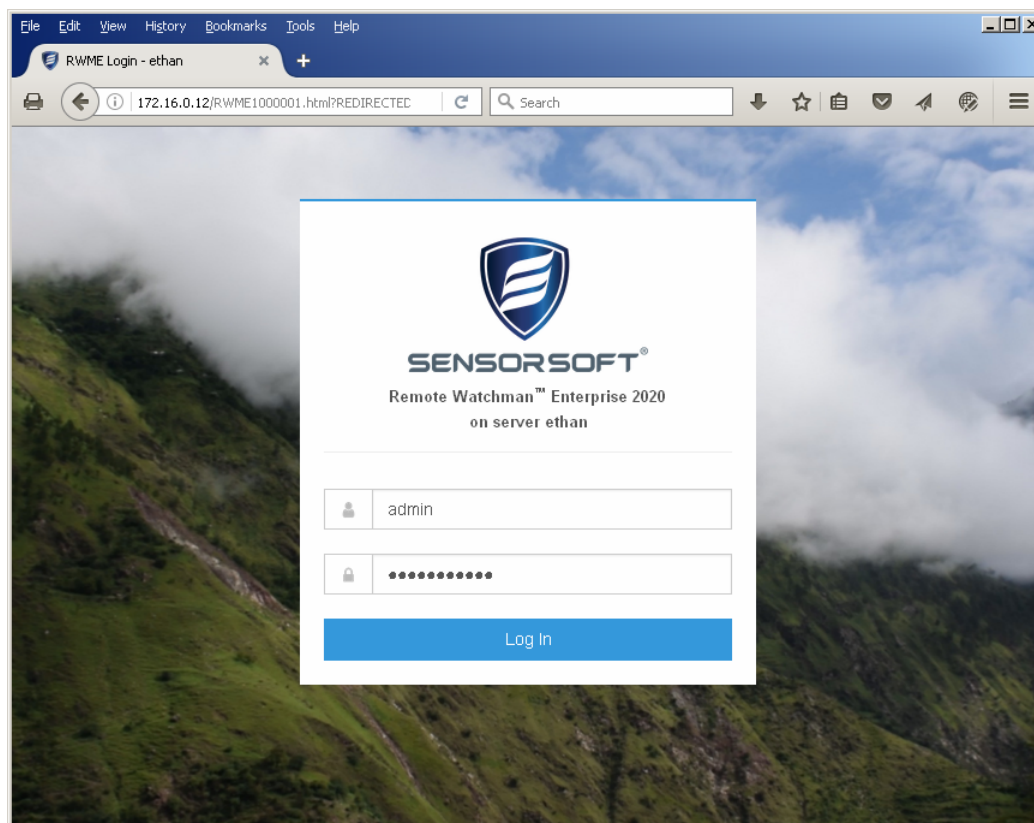


Figure 3: RWME Login page

## Stopping and Starting the RWME service

You might be required to start, stop or check status of the RWME service for maintenance purposes. The Windows Service Control Manager (SCM) or Services app as shown in Figure 4 is used for this purpose.

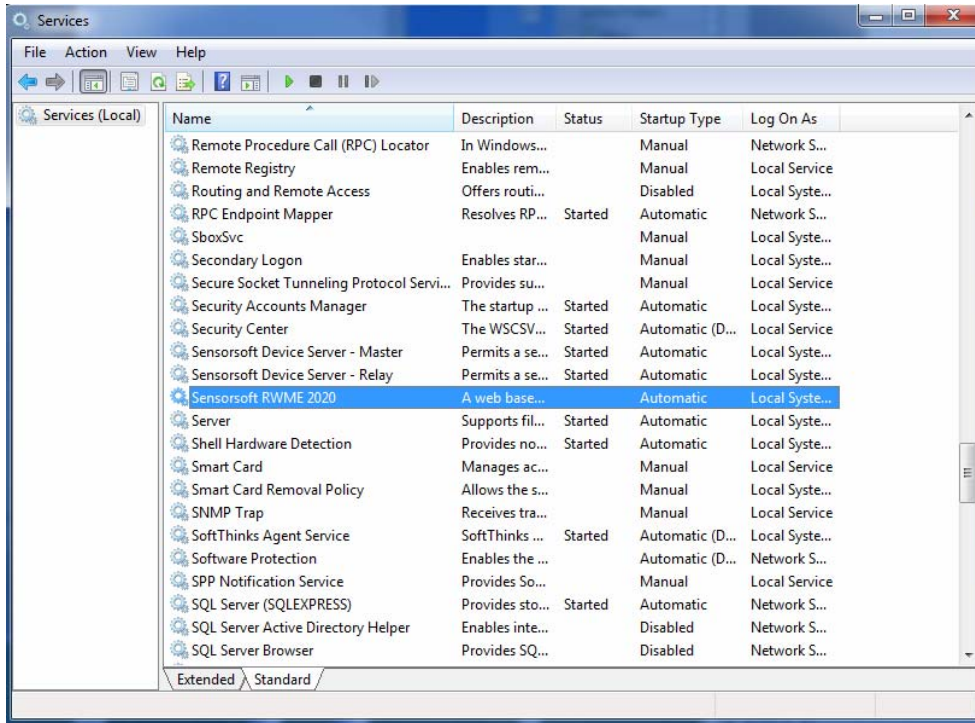


Figure 4: Using SCM or Services app to check status and control the RWME service

### Stop the RWME service with SCM/Services app

1. Log into the target computer (where you installed RWME) as the Windows administrator.
2. Click the Windows Start button and choose:

Settings->Control Panel->Administrative Tools->Services

3. Select the service display name **Sensorsoft RWME 2020** and double-click on it.
4. Click the Stop button.

### Start the RWME service with SCM/Services app

1. Log into the target computer (where you installed RWME) as the Windows administrator.
2. Click the Windows Start button and choose:

Settings->Control Panel->Administrative Tools->Services

3. Select the service display name **Sensorsoft RWME 2020** and double-click on it.
4. Click the Start button.

## **Controlling the RWME service from command line**

With RWME 2020 Build 694 and forward you can also start, stop and check status of the RWME service and for that matter any service from the command line. Administrator privileges are required to run these command lines:

```
RWME.exe -start Sensorsoft_RWME_2020  
or  
RWME.exe -start <service_name>
```

```
RWME.exe -stop Sensorsoft_RWME_2020  
or  
RWME.exe -stop <service_name>
```

```
RWME.exe -status Sensorsoft_RWME_2020  
or  
RWME.exe -status <service_name>
```

In the case of the -status command argument, it returns various exit codes and text output that relate to the service status:

<u>Exit Code</u>	<u>Service Status</u>
-1	Command failed with error
0	Not used
1	SERVICE_STOPPED
2	SERVICE_START_PENDING
3	SERVICE_STOP_PENDING
4	SERVICE_RUNNING
5	SERVICE_CONTINUE_PENDING
6	SERVICE_PAUSE_PENDING
7	SERVICE_PAUSED



## Setting up Monitored Items/Nodes

This section describes how to create and setup items/nodes in the Monitor List. These items/nodes can include Sensorsoft devices, TCP servers, network cameras and Sensorsoft Alert appliances.

If you have an item/node limited license, RWME will limit the number of items/nodes that can be monitored. After the number of monitored items/nodes has reached the license limit, you will not be allowed to add more until you upgrade. If you have the unlimited license, there is no limit on the number of monitor items/nodes. Your RWME license information can be found by clicking the **About RWME** link.

### Monitoring a Sensorsoft device

This section describes how to add an item/node for monitoring a Sensorsoft device (sensor). You will need to be logged in as admin user to follow this procedure.

1. Click the **Settings** link.
2. Under the Monitored Item/Node Management heading, click the link entitled – **Add a new Item/Node to Monitor List**.
3. Select “Sensorsoft Device” from the list and click the **Next** button.
4. Under the Administrative Information section, you are required to setup the following fields:
  - Description – enter a unique description for the device.
  - IP Address or Host Name – enter the address of the Sensorsoft device or device server/computer that is sharing the Sensorsoft device on the network.
  - TCP Port (This must be between 1 and 65535) – enter the TCP port number assigned to the Sensorsoft device. When the Sensorsoft device is connected to a Lantronix Device Server the port number is 3001-30xx. The xx is dependent on the physical port number where the Sensorsoft device is connected to the Lantronix Device Server. If the Sensorsoft device is connected to a Windows machine running Sensorsoft Device Server (SDS) software, the TCP port number is determined by the setting used in this software. The default TCP port number used by SDS software is usually 6101.
  - Update Interval – Select the interval that you want RWME to take readings from the device
5. Click the **Save** button. The device item/node is now added to the monitor list.
6. Click the link entitled **Monitor List** to see the device reading(s). If the status column shows an error for this item/node, you will need to more carefully check your settings.



**Important** – Device or terminal servers that are hosting Sensorsoft devices must be configured to use the correct serial port settings. The correct settings are 1200 bps (57,600 bps for SS6420J), 8 bits and no parity. In addition, set the device server's idle timeout value to at least 2 minutes to prevent RWME from being unexpectedly disconnected. Please consult your device/terminal server documentation to configure these setting. If you are using a Lantronix device server that you purchased from

Sensorsoft, consult the Sensorsoft documentation that came with the device server.

If the device being monitored is the Sensorsoft Contact & Voltage Sensor (SS6420), then continue to the following section *Monitoring Security or Safety Devices on the SS6420*.

## Monitoring security or safety devices on the SS6420

This section describes how to configure RWME to monitor security or safety devices connected to the Sensorsoft SS6420 Contact & Voltage Sensor. Such devices include but are not limited to door contacts, motion, glass-break, carbon monoxide and smoke detectors. This section assumes that the SS6420 and its security or safety devices have been properly installed. Please refer to the User Manual for the SS6420 for more instructions on installing these detectors.

After adding the SS6420 as a monitored item/node, as per the section *Monitoring a Sensorsoft device*, you will notice that the contact, voltage, and relay variables will appear on the Monitor List. In the example below we instruct you how to setup a door contact or sensor (with Sensorsoft Quick Connect (QC) feature) that is connected to C1 and C2 inputs of the SS6420. Eight of the variables as shown below are of interest:

```
CONTACT(C01)
CONTACT(C01)_DESCRIPTION
CONTACT(C01)_ZEROSTATE
CONTACT(C01)_ONESTATE

CONTACT(C02)
CONTACT(C02)_DESCRIPTION
CONTACT(C02)_ZEROSTATE
CONTACT(C02)_ONESTATE
```

CONTACT(C01) reports the door's position in Boolean terms (i.e. OPEN or CLOSED). CONTACT(C01)\_DESCRIPTION allows for a user defined string (up to 32 characters) that describes the function or application of CONTACT(C01) input. CONTACT(C01)\_ZEROSTATE and CONTACT(C01)\_ONESTATE are user defined strings (up to 8 characters) that define the two Boolean states used by CONTACT(C01) variable, that can be displayed on the Monitor List in the Last Successful Reading column.

CONTACT(C02) reports whether the door contact is properly connected to the SS6420 in Boolean terms (i.e. NORMAL or ALARM). CONTACT(C02)\_DESCRIPTION allows for a user defined string (up to 32 characters) that describes the function or application of CONTACT(C02) input. CONTACT(C02)\_ZEROSTATE and CONTACT(C02)\_ONESTATE are user defined strings (up to 8 characters) that define the two Boolean states used by CONTACT(C02) variable, that can be displayed on the Monitor List in the Last Successful Reading column.

Using the following procedure you will be instructed on how to give the above variables meaningful descriptions and suitable values for the Boolean state strings:

1. From the **Monitor List** page, click the link in the **Description** field of the SS6420. This will take you to the **Sensorsoft Device Details** page.
2. Scroll to the section **Sensorsoft Device Management**. At the bottom of this section, click the link, **View Tech Variables**. This will make all the Tech Variables visible in the **Sensorsoft**

**Device Readings** section. You will see that for each CONTACT(CXX) variable, there is a corresponding CONTACT(CXX)\_DESCRIPTION variable. By modifying the DESCRIPTION variable you can assign a meaningful description to the CONTACT (CXX).

3. Locate the CONTACT(C01)\_DESCRIPTION variable, and click on its *Modify Variable Value* link.
4. On the **Modify Variable Value** page, type in “Server Room (Door)” or another description that you prefer and click **Submit**.
5. Repeat steps 3 and 4 above, using the CONTACT(C02)\_DESCRIPTION variable. In this case type in “Server Room (Door disconnect)” or another description that you prefer and click **Submit**.
6. Repeat steps 3 and 4 above, using the CONTACT(C01)\_ZEROSTATE variable. In this case type in “OPEN” and click **Submit**.
7. Repeat steps 3 and 4 above, using the CONTACT(C01)\_ONESTATE variable. In this case type in “CLOSED” and click **Submit**.
8. Repeat steps 3 and 4 above, using the CONTACT(C02)\_ZEROSTATE variable. In this case type in “ALARM” and click **Submit**.
9. Repeat steps 3 and 4 above, using the CONTACT(C02)\_ONESTATE variable. In this case type in “NORMAL” and click **Submit**.

Your Monitor List should now look similar to the screen image below.

Normal	<a href="#">Contact &amp; Voltage Sensor</a>	CONTACT(C01) - Server Room (Door)	<a href="#">OPEN</a>
Normal	<a href="#">Contact &amp; Voltage Sensor</a>	CONTACT(C02) - Server Room (Door disconnect)	<a href="#">NORMAL</a>

Figure 5

The following table shows the recommended set-up for several types of security and safety devices that could be attached to the contact inputs of SS6420:

Security or Safety Detector	Sample Description	Zero State String Default is OPEN	One State String Default is CLOSED
<b>Motion Detector</b> <sub>1</sub>	Server Room (Motion)	MOTION	STILL
	Server Room (Motion tamper)	ALARM	NORMAL
<b>Glass-break Detector</b> <sub>1,3</sub>	Back Window (Glass-break)	ALARM	NORMAL
	Back Window (Glass-break tamper)	ALARM	NORMAL
<b>Carbon Monoxide Detector</b> <sub>2</sub>	Shipping (CO)	ALARM	NORMAL
	Shipping (CO disconnect)	ALARM	NORMAL

<b>Door Sensor</b> <sup>2</sup>	Server Room (Door)	OPEN	CLOSED
	Server Room (Door disconnect)	ALARM	NORMAL
<b>Smoke Detector</b> <sup>2,3</sup>	Server Room (Smoke)	ALARM	NORMAL
	Server Room (Smoke disconnect)	ALARM	NORMAL

<sup>1</sup> The Sensorsoft supplied motion and glass-break detectors have a normally-closed tamper switch that is wired separately from the alarm contact. If monitored, this can indicate if the detector's enclosure has been opened and that someone has perhaps made an attempt to disable or cut wires in the detector. This tamper switch can also be used to detect severed wires or accidental removal or disconnect from the SS6420 terminals.

<sup>2</sup> Sensorsoft supplied door contacts, CO and smoke detectors with the Sensorsoft Quick Connect (QC) feature can indicate when they are physically disconnected from the SS6420. This type of disconnect sensing is useful for detecting severed wires or accidental removal from the SS6420 terminals.

<sup>3</sup> Sensorsoft supplied glass-break and smoke detectors will hold an alarm state (latch) until their power is removed. The easiest way to reset them is to temporarily remove the peripheral power supply from the SS6420.

## Monitoring a TCP or Web server port

Many networked appliances and software applications have web based capability that can be monitored by RWME for their UP/DOWN status. The following is a list of common devices that can have web based capability:

- firewalls and VPN appliances
- laser printers
- routers, switches and other network equipment

This section describes how to add an item/node for monitoring a TCP or web server port. Any TCP server (mail, web, telnet, ftp, VNC etc.) that services a TCP socket port can be monitored. You will need to be logged in as admin to follow this procedure.

1. Click the **Settings** link.
2. Under the Monitored Item/Node Management heading, click the link entitled – **Add a new Item/Node to Monitor List**.
3. Select **TCP Server Port** from the list and click the **Next** button.
4. Under the Administrative Information section, you are required to setup the following fields:
  - Description – enter a unique description for the server.
  - IP Address or Host Name – enter the address of the server.
  - TCP Port (This must be between 1 and 65535) – enter TCP port of the server. For examples of typical TCP server ports, click the link entitled “Click here for a list of

well known TCP Ports”. If this is a web server or web appliance use 80 as the port number, unless otherwise specified by its documentation.

- Select the Update Interval that you want RWME to use for checking if the server is up and responding.
5. Select the appropriate filename from the drop down box near the check box “Send this File to the Host After Connection”. For web servers and appliances use HTTP.txt. For Telnet servers use Telnet.txt. These files are in the TCP Protocols folder of the RWME installation folder. RWME uses the contents of this file to check to see if the server is responding. Some servers (SMTP and FTP) do not require a file since they send a response immediately upon connection. In these cases clear the check box.
  6. Clear the check box entitled “Poll this item/node to verify the above configuration before adding to the Monitor List”.
  7. Click the **Save** button. The server item/node is now added to the monitor list.
  8. Click the link entitled **Monitor List** to see if the server is UP and responding. If the item/node shows incorrect readings you will need to check your item/node settings more carefully.

## **Monitoring a network camera**

This section describes how to add an item/node for monitoring a network camera. Canon, Panasonic and Axis web based network cameras are supported. RWME will allow you to view images from the camera using the link it creates in the “Host:Port” column. You will need to be logged in as admin to follow this procedure.

1. Click the **Settings** link.
2. Under the Monitored Item/Node Management heading, click the link entitled – **Add a new Item/Node to Monitor List**.
3. Select “Network Camera” from the list and click the **Next** button.
4. Under the Administrative Information section, you are required to setup the following fields:
  - Description – enter a unique description for the camera.
  - IP Address or Host Name – enter the address of the camera.
  - TCP Port (This must be between 1 and 65535) – enter the TCP Port of the camera’s web server. By default most network cameras are set to 80.
  - Update Interval – select the interval that RWME will check if the network camera is up and responding.
5. Under the Camera User Account Information, you should enter a username and password for your camera. If your camera does not use a username and password, leave these fields blank.
6. Clear the check box entitled “Poll this item/node to verify the above configuration before adding to the Monitor List”.
7. Click the **Save** button. The camera item/node is now added to the monitor list.

8. Click the link entitled **Monitor List** to see if the camera is UP and responding. If the item/node shows incorrect readings you will need to check your item/node settings more carefully. You should also notice that the “Host:Port” column for this item/node has a link to the live camera.

## **Monitoring a Sensorsoft Alert appliance**

This section describes how to add an item/node for monitoring a Sensorsoft Alert appliance. A Sensorsoft Alert appliance must already be setup on your network. RWME will allow you to login to the Sensorsoft Alert appliance with one click. RWME will also monitor whether the Sensorsoft Alert appliance is online. You will need to be logged in as RWME admin to follow this procedure.

1. Click the **Settings** link.
2. Under the Monitored Item/Node Management heading, click the link entitled - **Add a new Item/Node to Monitor List**.
3. Select “Sensorsoft Alert Appliance” from the list and click the **Next** button.
4. Under the Administrative Information section, you are required to set-up the following fields:
  - Description – enter a unique description for the Sensorsoft Alert appliance.
  - IP Address or Host Name – enter the address of the Sensorsoft Alert appliance.
  - TCP Port (This must be between 1 and 65535) – enter the TCP Port of the Sensorsoft Alert’s web server. The default this is 80.
  - Update Interval – select the interval that RWME will check if the Alert appliance is online.
5. Under the Sensorsoft Alert Appliance Login Information, you should enter the **admin** and **ruser** passwords. If you enter the incorrect passwords, RWME will not be able to login to the Sensorsoft Alert appliance.
6. Click the **Save** button. The Sensorsoft Alert appliance item/node is now added to the monitor list.
7. Click the link entitled **Monitor List** to see if the Sensorsoft Alert appliance is UP and responding. If the item/node shows incorrect readings you will need to check your item/node settings more carefully. You should also notice that the “Host:Port” column for this item/node has a link to log you into the Sensorsoft Alert appliance.

When you start monitoring an Alert appliance, you will notice that four rows have been added to the Monitor List. The rows respectively contain information about the following variables:

### **SSALERT\_CONNECT**

This variable indicates whether Sensorsoft Alert is online. When the Alert appliance is online, this variable reads UP, otherwise, it would read DOWN.

### **SSALERT\_RESPOND**

This variable indicates whether the Sensorsoft Alert appliance is responding to queries.

### **SSALERT\_PASSWORD**

This variable indicates whether the admin account password that you have specified in step 5 is valid. It allows you to be notified if someone changes the Alert appliance password without your knowledge. The reading of this variable will be `PASSWORD_OK` when the Alert appliance is accepting the password and can be logged into, otherwise, the reading will be `PASSWORD_FAIL`. The reading of this variable can be obtained only when the `SSALERT_CONNECT` and `SSALERT_RESPOND` variables are `UP` and `RESPOND_OK`, respectively. In other words, the Alert appliance must be online and responding in order to validate the password. If the Alert appliance is either offline or is not responding, then the `SSALERT_PASSWORD` variable would not have a deterministic value. In turn, it would have a blank reading on the Monitor List, and would not be logged until the unit comes back online and responds.

### **SSALERT\_REMOTE**

This variable indicates whether an exception has occurred on the Alert appliance. An exception occurs when the Alert appliance is in an unusual state, for example, one of its sensors is breaching a limit. The following is a list of conditions that can cause an exception on Sensorsoft Alert:

- Monitored device in breach state
- Monitored device is OFFLINE
- Monitored device is in TIMEOUT
- Monitored device's model has changed
- Monitored device has a Low Voltage problem
- Monitored device has a Tamper condition

If an exception occurs, this variable's value will read `REMOTE_EXCEPTION`, otherwise, it reads `REMOTE_OK`. You can determine the exact cause of the exception by logging into the Sensorsoft Alert appliance by clicking the link under the **Host:Port** column.

The `SSALERT_REMOTE` variable's reading can be obtained only when all of the following conditions are true:

- `SSALERT_CONNECT` is `UP`
- `SSALERT_RESPOND` is `RESPOND_OK`
- `SSALERT_PASSWORD` is `PASSWORD_OK`

In other words, the Alert appliance must be online, responding, and accepting the admin account password before it can report the presence of an exception. If any of these conditions are not met, then the `SSALERT_REMOTE` variable would not have a deterministic value. In turn, it would have a blank reading on the Monitor List, and would not be logged.

## General Usage

### Accounts and passwords

RWME uses two levels of access rights. The administrator account or **admin** username provides full rights to change settings in RWME. The read-only account or **ruser**, only provides the rights to view the Monitor list, log files and to graph data files. The initial or default password for each username is **begin**. Please see the *Troubleshooting* section for information on how to reset a lost password.

### RWME administration

At any point after you have logged into RWME as the administrator, you can follow the link **Settings**. From this page you may add, remove or modify an item/node, and set some operational features of the software. Most of the advanced administration for RWME is performed by following the **Settings->Server Settings** link. The following are descriptions of the features that you will find on this page:

#### HTTP settings

- Inactive User Logout – This is the amount of time that must pass without web browser activity before a user is automatically logged out. Please note that any web browser that has a RWME page open will not appear to be logged out until after a RWME link has been clicked. See *Security Considerations* for more information.
- Refresh Period – This is the interval that the Monitor List page will be automatically refreshed. This allows you to keep watch on all of your current readings without having to click on the web browser's refresh button.
- HTTP Server Port – This is the TCP port that you must use when accessing RWME with your web browser. IANA has defined TCP port 80 as the international standard, but you may wish to change this value to add an increased layer of security, as indicated in *Security Considerations*.
- Temperature Unit of Measure – This is the unit of measure that RWME will use to display all temperature readings. The Celsius or Fahrenheit scale can be selected.

#### Changing login passwords

The Current Admin Password must be entered before you will be authorized to change either the admin password or the read-only user (ruser) password. If you want to change the ruser password, but not the admin password, you would enter the Current Admin Password, the New Read-Only User Password, and then Confirm the Read-Only User Password, leaving the new Admin Password and Confirm Admin Password fields empty.

#### SMTP settings

- Primary SMTP Server – This is the IP address or host name of the primary SMTP server that delivers the alert emails. If this server does not respond, or is experiencing problems,



the secondary SMTP server will be used for 15 minutes, and then the primary SMTP server will be tried again.

- **Secondary SMTP Server** – This is the IP address or host name of the secondary SMTP server. This server is used in the event that the primary SMTP server stops responding. Use of this field is optional.
- **Administrator Email** – This is the email address that RWME will use to indicate the sender of the email. Although you cannot send mail back to the RWME application, you may wish to use a valid address in this field to allow someone in your organization to monitor any emails that are being discarded by the SMTP server (i.e. to monitor that no emails are “bouncing back” to the sending address).
- **SMTP Server Max. Retries** – This is the number of times that RWME will retry sending Email alerts after encountering SMTP problems such as server offline or not responding.
- **SMTP Server Retry Interval** – This is the interval (in minutes) that Email alerts will be retried after encountering SMTP server problems such as server offline or not responding.

### **SMS Modem Settings**

- **COM Port** – This is the serial or USB port where the modem is connected.
- **Modem Type** – This is the type of modem that you have connected to your USB or COM port. This list is generated from the INI files in the Modems folder of RWME. Please see *Appendix A – SMS/Paging Dial-up Modem Requirements* for more information.
- **Lock Modem COM Port** – This will force RWME to dominate the modem, preventing other applications from using it. This improves the reliability that RWME will be able to access the modem when a pager alert is issued.

### **Sensorsoft Device Poll Settings**

These settings affect only Sensorsoft devices. Although these values may be modified, Sensorsoft recommends certain values for each field. Contact Sensorsoft Support if you feel the need to change these settings. The following should only be modified if device errors are frequently generated:

- **Wait For Active Connection** – This is the amount of time that RWME will wait for a TCP connection when polling a device.
- **Wait For Receive Data** – This is the amount of time that RWME will wait before abandoning the current device packet reception. If some or all of the data is missing or invalid, and the Max Function Retries has expired, an appropriate alert will be generated.
- **Max. Function Retries** – This is the number of times that RWME will attempt to resend a command to a device, after which, it will generate an appropriate alert.
- **Wait For Retry Function** – This is the amount of time RWME will wait before resending a command to the device after a failed communication.
- **Max. Connection Retries** – This is the number of times that RWME will attempt to establish a TCP connection before generating an offline alert.

- **Wait For Retry Connection** – This is the amount of time that RWME will wait before reattempting a TCP connection.

### **Incoming Web IP Access List**

The IP Access List allows you to protect RWME from unwanted users or hackers by denying them access, based on their IP address. If you choose to block IP addresses in the list, then everyone will have access to RWME, except those listed. If you choose to trust IP addresses in the list, then no one will have access to RWME, except those listed.

Please note that RWME can always be accessed from the computer that it is installed on, regardless of whether that IP address is specified as being blocked. This guarantees that you cannot be completely locked out of RWME for administration purposes. Please see *Security Considerations* for more information.

### **Address Book**

The RWME address book contains three different types of entries. These three types of entries can be used collectively to issue alerts.

#### **People**

These entries are used for email and SMS/pager alerts. They are much like any other address book entry that you might make in your typical email software (Microsoft Outlook etc). They contain the person's name, email address, phone number, pager type, SMS ID, etc.

#### **Command lines**

These entries are used to run other programs when an alert is issued. The type of command can vary from turning a relay contact on or off, to sending a message to someone's computer screen using Microsoft's NetBIOS Messenger Service. Please see *Security Considerations* for more information on running command lines.

#### **Alert Groups**

These entries are collections of People and Command Lines. These are the objects that are bound to an item/node's alerts.

## The Monitor List

The Monitor List page consists of a table that shows the monitored items/nodes that are currently under view. Each row in the table displays information about a variable that is being monitored. Some monitored items/nodes can have several variables each in subsequent rows. If the monitored items/nodes are arranged into groups, you can select which group of monitored items/nodes you view. The default is to view All Items-Nodes.

Status	Item Description	Variable	Last Successful Reading	IP or Host Name	Last Successful Reading At	Update Interval
Normal	<a href="#">Server Room</a>	HUMIDITY (0.1 % RESOLUTION)	42.8 % RH	172.16.0.29:3010	Mon Apr 27 22:01:14 2020	5 m
Normal	<a href="#">Server Room</a>	TEMPERATURE (0.1 C RESOLUTION)	73.2 F	172.16.0.29:3010	Mon Apr 27 22:01:14 2020	5 m
Normal	<a href="#">Alert Demo</a>	SSALERT_CONNECT	UP	172.16.0.28:8090	Mon Apr 27 21:59:31 2020	5 m
Normal	<a href="#">SS8420</a>	CONTACT(C01) - Lobby (Motion)	STILL	172.16.0.29:3011	Mon Apr 27 22:02:46 2020	-
Normal	<a href="#">SS8420</a>	CONTACT(C02) - Front (Door)	CLOSED	172.16.0.29:3011	Mon Apr 27 22:02:46 2020	-
Normal	<a href="#">SS8420</a>	CONTACT(C03) - Server Room (Smoke)	NORMAL	172.16.0.29:3011	Mon Apr 27 22:02:46 2020	-
Normal	<a href="#">SS8420</a>	CONTACT(C04) - Diesel Generator	OFF	172.16.0.29:3011	Mon Apr 27 22:02:46 2020	-
Breach of Boolean Limit	<a href="#">SS8420</a>	CONTACT(C05) - Server Room (Lighting)	DN	172.16.0.29:3011	Mon Apr 27 22:02:46 2020	-
Normal	<a href="#">SS8420</a>	CONTACT(C06) - Shipping (Carbon Monoxide)	NORMAL	172.16.0.29:3011	Mon Apr 27 22:02:46 2020	-
Normal	<a href="#">SS8420</a>	CONTACT(C11) - Side Window (Glassbreak)	NORMAL	172.16.0.29:3011	Mon Apr 27 22:02:46 2020	-
Normal	<a href="#">SS8420</a>	RELAY(RL02) - Glass Door (Solenoid)	OFF	172.16.0.29:3011	Mon Apr 27 22:02:46 2020	-
Normal	<a href="#">Sensorsoft Web Site</a>	SOCKET_CONNECT	UP	www.sensorsoft.com:80	Mon Apr 27 21:57:22 2020	30 m
Normal	<a href="#">Google</a>	SOCKET_CONNECT	UP	www.google.ca:80	Mon Apr 27 22:00:44 2020	30 m
Normal	<a href="#">Computer Rack Camera</a>	CAMERA_CONNECT	UP	172.16.0.24:80	Mon Apr 27 22:00:34 2020	10 m
Normal	<a href="#">Front Door Camera</a>	CAMERA_CONNECT	UP	172.16.0.26:80	Mon Apr 27 21:59:09 2020	10 m

Figure 1(b): The Monitor List page

The Monitor List page automatically refreshes itself to display the latest readings. You can manually refresh this page by clicking the **Monitor List** link on the left side of the page or by clicking the **refresh** link at the bottom of the page or using the keys **Ctrl R**.

The Monitor List consists of the following column headings:

- **Status:** This column indicates the status of the monitored item/node or variable.
- **Description:** This column contains a user-specified description of the monitored item/node. When logged into RWME as admin, this description will be a link. Clicking this link will take you to the Details page where you can view and configure the item/node's settings.
- **Variable:** This column contains the name of the variable. If the item/node is a Sensorsoft Device, then its variable name is defined in the device. If the item/node is a TCP Server Port, Camera, or Sensorsoft Alert unit, then the variable name is pre-defined by RWME. In any case, the variable name cannot be changed. If the variable supports custom description (see *section Custom Variable and Boolean String*), this field would show the description string concatenated to the variable name.
- **Last Successful Reading:** This column contains the last successful reading taken from the variable. If you have enabled logging for the variable, then you can click on the reading to graph its data file.
- **Location:** This column displays the user-specified physical location of the monitored item/node.

- **Host:Port:** This column contains the user-specified network IP or host name and port number to access the monitored item/node. If the item/node is set-up as a network camera or Sensorsoft Alert unit, this field will become a clickable link.
- **Comments:** This column contains a comment that the user can enter about the monitored item/node.
- **Group:** This column contains the name of the group that the monitored item/node that will belong to. This field is blank until the user adds a name. Adding a group name to each item/node can be useful if you have a number of items/nodes (> 25) that need to be organized by physical location or function. The word Group as explained here applies to how monitored items/nodes are organized and should not be confused with Alerting Groups mentioned in the Address Book.
- **Last Successful Reading At:** This column contains the time and date when the last successful reading was taken from the monitored item/node.
- **Last Attempted Reading At:** This column contains the time and date when RWME attempted to take a reading from the monitored item/node.
- **No. of Successful Consecutive Readings:** This column contains the number of consecutive readings taken from the item/node without encountering any communication or device related errors. Please note: readings that exceed breach limits are not considered errors.
- **Update Interval:** This column contains the user-selected interval that the item/node is being read or updated. If the item/node is a Real-Time Sensorsoft device, this field would be blank because Real-Time Sensorsoft devices are not polled by RWME, but rather, they would inform RWME immediately when their reading changes.
- **Estimated Uptime:** This column contains the estimated amount of time that the monitored item/node has been up and responding.
- **Vendor:** This column contains the name of the vendor that manufactured the Sensorsoft device or Sensorsoft Alert unit.
- **Model:** This column contains the model number of the Sensorsoft device or Sensorsoft Alert unit.

## Reordering the Monitor List

Monitored items/nodes on the Monitor List can be reordered or arranged, as you desire. For example, you can arrange similar nodes together. This is the procedure:

1. Click the **Settings** link.
2. Under the Settings and Management heading, click the **Monitor List Display Settings** link.
3. Under the **Display the monitor list in the following order** heading, there is a list box that looks like the one shown in Figure 6. This list box contains all of the monitored items/nodes. From the list box, select the item/node of interest and move it using the arrows buttons on the right. If your list is long (hundreds or thousands) additional radio button options will be displayed to allow you to move items/nodes fast and very fast through the list by holding down the up and down mouse buttons.

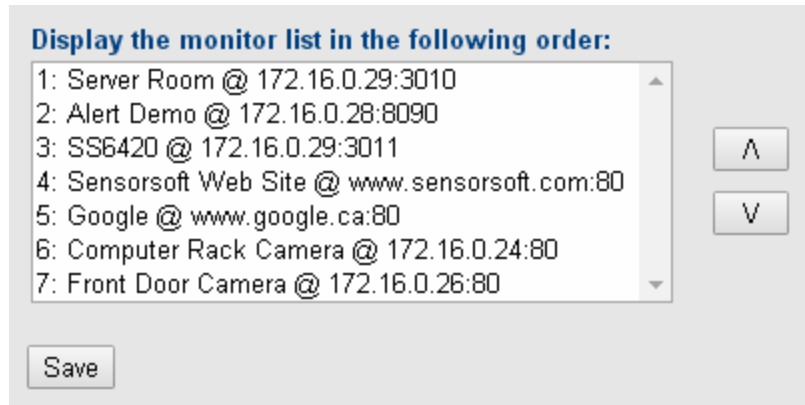


Figure 6: Reordering the Monitor List

- After reordering the items/nodes in the list, click the **Save** button to activate the changes.

## Selecting variables to display on the Monitor List

You can select which variables you want to have displayed on the Monitor List page. When you add a new item/node to be monitored, by default, all of its variables are displayed on the Monitor List (excluding tech variables). However, instead of seeing all of the variables on the Monitor List, you may only want to see the variables that you care about. For example in Figure 7, if you are monitoring a Sensorsoft SS6610J or SS6610C, you may want the Monitor List page to display just the high resolution and not the low resolution variables. To select the variable(s) to be displayed, do the following:

- From the Monitor List page, click the link in the **Description** field of the monitored item/node. This will take you to the Details page.
- On the Details page you will see a list of variables, as shown in Figure 7.
- Uncheck the box adjacent to TEMPERATURE (0.5 C RESOLUTION) and HUMIDITY (1 % RESOLUTION) and click the **Save – View on Monitor List** button.

**Sensorsoft Device Readings**

This device is operating normally.

View on Monitor List	Variable Index	Variable Name	Last Reading	Log Readings
<input type="checkbox"/>	1	HUMIDITY (1 % RESOLUTION)	51 % RH	No
<input checked="" type="checkbox"/>	2	HUMIDITY (0.1 % RESOLUTION)	51.3 % RH	Yes
<input type="checkbox"/>	3	TEMPERATURE (0.5 C RESOLUTION)	75.2 F	No
<input checked="" type="checkbox"/>	4	TEMPERATURE (0.1 C RESOLUTION)	75.5 F	Yes

[Save - View on Monitor List](#)

This will change the variable values displayed on the [Monitor List](#) page.

[View Tech Variables](#)

Figure 7: Selecting Variables to display on the Monitor List

## Automatically refreshing the Monitor List page

You can set the Monitor List page to automatically refresh itself in the browser at a regular interval. After installing RWME, the refresh rate is set to once every 60 seconds by default. You can change this interval to suit your preference. For example, if you have a real-time device such as the SS6420, you may wish to speed up the refresh rate to once per 5 seconds to see the real-time readings change. To change the Monitor List refresh interval, do the following:

1. Click the link **Settings**.
2. Click the link **Server Settings**.
3. Under the section **Web Server (HTTP) Settings**, set the field **Refresh Period (seconds)** to your desired refresh interval.
4. Scroll to the bottom of the page, and click the **Submit** button.

## Arranging Monitored Items/Nodes in Groups

For customers with many monitored items/nodes (> 25) that extend beyond the web browser's current view it is possible to arrange these items/nodes in logical groups. Monitor groups can greatly simplify viewing of hundreds or thousands of monitored items/nodes by arranging them in the same way that you organize business assets or properties. Here are some examples:

By function (sensors, cameras, servers, workstations, routers, printers)

By physical locale (country, region, state, city, store/hotel number, lab, room)

RWME supports one tier or level for monitor group names. If you need multiple tiers for group naming you can work around this by using aggregated names as shown below:

Region 1 – Hotel 556

California – Campus A Bldg 24 – Curtis Smith Lab

Canada – Alberta – Store # 1524

Sensors with multiple variables, like the Sensorsoft SS6420, appear as one item/node in the monitor list and cannot be split into separate groups.

## Add a new monitor group

You can create a monitor group by modifying a monitored item/node and adding a new group:

1. Click the **Description** link of the item/node where you want to assign a group
2. Click the **Modify this Item/Node** link.
3. Select CREATE NEW GROUP from the Group Name drop-down menu and the Add New Monitor Group window should pop-up as in Figure 8
4. Type in the new group name you want to assign to this item/node and click the Create button.



Figure 8: Adding a new Monitor Group



**Important** – Monitor group names that you create are dynamic and only exist as long as they are assigned to at least one item/node. Monitor group names must be between 1 and 50 characters.

## Renaming a monitor group

A monitor group can be renamed so that all items/nodes assigned to it will reference the new group name. To rename:

1. Click the **Settings** link.
2. Click the **Rename a Monitor Group** link.
3. Select the group name you want to rename
4. In the New Monitor Group Name text box enter the new name and click the **Save** button

The default groups **\*\*\*All Items-Nodes\*\*\*** and **\*\*\*Ungrouped Items-Nodes\*\*\*** cannot be renamed.

## Selecting a monitor group to view in the Monitor List

To select a monitor group for viewing:

1. Click the **Viewing Monitor Group “All Items-Nodes” (change)** link in the upper right corner of the Monitor List. A window should pop up with the name **Select a Monitoring Group to View** as shown in Figure 9.
2. Select the group you want to view from the drop-down list. The monitored item/node(s) of the group you selected should now be displayed in the Monitor list.

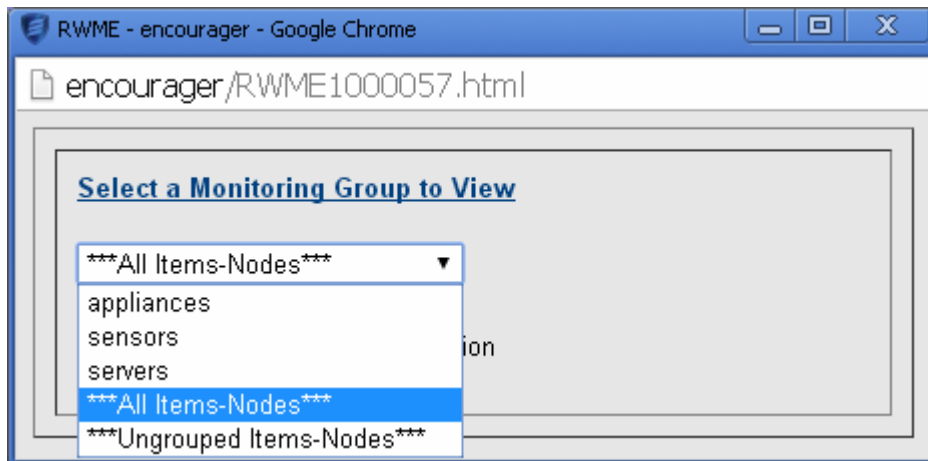


Figure 9: Selecting a Monitoring Group to View

RWME stores the name of the last group you viewed, in a web browser cookie. For this reason when you log back into RWME using the same web browser (on the same machine), the last group you selected will be recalled for viewing. Many people in your organization can use



RWME to view a group of their own choice. Cookies must be enabled in the web browser for this functionality to work.

## Logging Data

RWME records two types of log files: data files, and status, error and debug files.

Data files contain readings collected from monitored items/nodes. This information is suitable for graphing and viewing in textual format.

Status, error and debug logs contain information that is only suitable for viewing in textual format. These cannot be graphed.

Both of these log file types are recorded in text-delimited format with date and time stamps.

### Data file naming convention

RWME uniquely names data files using a combination of the following information:

- IP address or Host name
- @ character
- TCP Port number
- Underscore character
- Variable name
- .log** extension

The following are examples of data file names:

- ets16@3001\_TEMP\_C.log.
- www.google.com@80\_SOCKET\_CONNECT.log
- 173.16.8.10@21\_SOCKET\_RESPONSE.log

### Graphing data files

The data logged by RWME for monitored items/nodes can be graphed using the integrated Sensorsoft Graphing Tool (SGT) app software.

There are two methods to graph data files:

- a) The easiest way to graph a data file is to click on the variable's reading (link) in the Monitor List page. This will launch SGT and offer a single series that can be graphed. You will only be able to do this, if RWME is logging the data for this variable.
- b) If the variable that you want to graph is NOT displayed on the Monitor List page, then it can be graphed by clicking the link entitled **Graph Data Files**. This will launch SGT where you can select the name of data file to graph.

For information on how to use the Sensorsoft Graphing Tool (SGT), see the Sensorsoft Graphing Tool User's Manual. This can be found by clicking the Docs link on the monitor list.

## Viewing log files

There are two methods we suggest for viewing data or log files:

- a) The easiest way to view a data file is to allow your mouse pointer to hover over the variable's reading (link) in the Monitor List page. A menu will then be displayed, where you can select the **View Data File** option. The data file will then be displayed in text format in your browser window. You will only be able to do this, if RWME is logging the data for this variable.
- b) If the variable is NOT displayed on the Monitor List page, or it is an error/status log, then it can be viewed by clicking the link entitled **Log Files** on the Monitor list. This will display all log files available where you can select the name of the file that you wish to view.

## Alerting

Alerting action in RWME is always bound to changes in state that occur on a particular item/node variable or device error (OFFLINE, TIMEOUT). Since a monitored item/node can have several variables, each of these variables has its own user-defined limits. When the value of a variable reaches or exceeds the user-defined limit, it changes state causing an event to occur that can launch a user-defined alerting action. This action is bound to an alert group, which may contain one or more user-defined actions.

### What are Scalar and Boolean variables

There are two main types of variables that RWME uses; Scalar or Boolean. Scalar variables take on numeric values (i.e. 0 to 100, -40 to +125) and often have units of measure (i.e. °F or %RH). Boolean variables can only take on values of zero or one and are represented by opposing states (i.e. WET/DRY, OPEN/CLOSED, ON/OFF). Boolean variables and device errors support the option for delayed alerting instead of issuing the alert immediately.

### What are Scalar breach limits

A scalar variable in RWME can be in one of five possible states based on its numeric value. When the value of a scalar variable reaches or exceeds a user-defined breach limit it changes state. This change of state creates an event that can trigger or launch an alerting action:

#### **Breach of Critical High Limit**

A scalar variable goes into this state when its value becomes greater than or equal to the Critical High Limit.

#### **Breach of Warning High Limit**

A scalar variable goes into this state when its value becomes greater than or equal to the Warning High Limit but less than the Critical High Limit.

#### **Breach of Warning Low Limit**

A scalar variable goes into this state when its value becomes less than or equal to the Warning Low Limit.

#### **Breach of Critical Low Limit**

A scalar variable goes into this state when its value becomes less than or equal to the Critical Low Limit.

#### **Normal**

A scalar variable is in this state when its value is less than the Warning High Limit and greater than the Warning Low limit.

### What are Boolean breach limits

A Boolean variable in RWME can be in one of two possible states based on its value. When the value of a Boolean variable is at a user defined breach limit it will change state. This change of state creates an event that can be used to trigger an alerting action:

#### **Breach of Boolean Critical Limit**

A Boolean variable goes into this state when its value is equal to the Boolean Critical Limit.

### **Normal**

A Boolean variable is in this state when its value is not equal to the Boolean Critical Limit.

## **Setting up Alerts**

To setup alerts for a variable, follow the steps below:

1. Login to RWME using the **admin** username.
2. From the **Monitor List** page, click the link in the **Description** field of the monitored item/node. This will take you to the **Details** page.
3. From the Details page, click the link **Modify this Item/Node**. This will take you to the **Update Existing** page
4. Scroll to the section, **Alerts, Limits and Logging for Variables**. There you will see the monitored item/node's variables that can be alerted on.
5. If you are setting up alerts for a scalar variable, then you need to set the appropriate breach limits and enable the checkbox for each of the breach conditions that you would like to be alerted on. Please note that **as long as the variable breaches one of the breach limits, the Monitor List page will show that it is in a breach state, even if all checkboxes (breach limits) have been disabled for alerting**. If you do not want the Monitor List to show breach states that have been disabled for alerting, then simply set the breach limit to a value that can never be exceeded. For example, if you do not want to see nor alert on the Breach of Warning Low Limit State, then simply set the Breach of Warning Low Limit to -100000.



**IMPORTANT** – Setting a breach limit to zero will not cause the breach condition to be disabled. Just like any other scalar value, zero will be treated as a legitimate breach limit by RWME.

6. If you are setting up alerts for a Boolean variable then you need to set the Boolean Critical Limit to the desired state string (i.e. DOWN vs. UP, CLOSED vs. OPEN) and enable the checkbox for each of the conditions that you would like to be alerted on. Please note that **as long as the variable breaches the Boolean Critical State, the Monitor List page will show that it is in a breach state, even if the checkbox for Boolean Critical Limit has been disabled for alerting**.
7. From the **Alert Group** selection box, select the alert group that will receive alerts, and skip to step 9. If you have not yet created an alert group, you can create one by selecting **CREATE NEW GROUP** in the selection box. This will open the **Add New Alert Group** page as in Figure 10.

**Add New Alert Group**

Group Name

Comments

Alert Interval

☒ Enable email alerts to these group members.

☒ Enable SMS alerts to these group members (modem and setup required).

☒ Enable command line alerts to these group members.

Address Book Members		Selected Alert Group Members
John Smith (Person)	<input type="button" value=""/> >>  <input type="button" value=""/> >  <input type="button" value=""/> <  <input type="button" value=""/> <<	John Smith (Person)
Send Message to Computer (Command Line)		Send Message to Computer (Command Line)

Figure 10: Adding a new Alert Group

8. From the Add New Alert Group page, enter the **Alert Group Name**. The group name will be used to identify the group in the **Address Book**. The **Alert Interval** is the interval at which alerts will be sent until the breach condition is clear. The **Address Book Members** list shows all of the current existing persons and command lines in the Address Book. Using the arrow buttons, select the persons who will receive the alert, and select the command lines to be executed. If you have not yet created any Address Book members, you can create an empty group for now by leaving the **Selected Alert Group Members** list blank, and clicking **Save** to close the Add New Alert Group window. Later, you can always create new Address Book members to populate the empty group.
9. If you are setting up an alert for a Boolean variable or device error, then for each alert condition, you can also specify a delayed alerting value. This delay, depending on node, is the length of time or the number of readings that the variable or device error has to continuously stay in breach condition before the alert is acted upon. If for example, you want to be alerted only when a particular variable has continuously been in Boolean Breach condition for two readings, then you need to set the delay to 2 readings as shown in Figure 11. Alternately, Figure 12 shows setting the alert delay to 2 minutes for a device error condition. This delay prevents alerts from being generated by short duration or intermittent breach events. If you do not use this delay, then the alert will be acted upon as soon as the variable goes into the breach condition.

**Alerts, Limits and Logging for Variables**

Please note that "Non-Alert State Restored Notifications" will only be issued if Boolean alerts are generated.

**Variable Name:** SOCKET\_CONNECT      **Breach Limits**      **Alert Group**

☒ Send Boolean Alerts      DOWN ▼      Boolean Alerts ▼

☒ Delay alerting until 2 consecutive readings in Breach State

☐ Send Non-Alert State Restored Notifications      None ▼

☒ Log Readings

Figure 11: Delayed alerting in number of readings for an item/node variable

**Send Alerts for the following Device Error Conditions**

☐ **Device Model Changed** - Indicates that the device model has changed. **Delayed alerting not supported**

☐ **COMM Corrupted** - Indicates that RWME can establish a TCP Connection, but the data from the device is unrecognized or corrupted.

☒ **TIMEOUT** - Indicates that RWME can establish a TCP Connection, but the device is not responding.

☒ **OFFLINE** - Indicates that RWME cannot establish a TCP Connection.

☐ **ONLINE** - Indicates that RWME has re-established a TCP Connection, after the connection was lost. **Delayed alerting not supported**

☐ **EEPROM Failure** - Indicates that the device cannot access its EEPROM.

☐ **LOW SUPPLY VOLTAGE** - Indicates that the device has low power supply voltage.

☐ **TAMPER** - Indicates that the device enclosure has been opened or the device may be damaged.

**Alert Group:** Boolean Alerts ▼

☒ Delay alerting until 2 minute(s) in Device Error condition.

Since alerting occurs at the time the device is read/updated a delayed alert with a period less than update interval will actually be sent/executed at next update interval.

Figure 12: Delayed alerting in minutes for Sensorsoft Device Errors

10. After the correct alert settings have been entered, click the **Save** button at the bottom of the **Update Existing** page.
11. If you have created any empty groups, you can go to the Address Book to create new persons or command lines to populate the empty groups.

## Creating address book members

The Address Book has three types of members: persons, command lines, and groups. **To create members you must be logged in as the admin user.** Persons are used to send email and pager alerts. Command lines are used to run executable files. A group may contain any number of persons and/or command lines.

### Adding a person to the address book

1. Click the **Address Book** link.
2. Click the **Add a new Person** link at the bottom of the page.
3. Enter the first and last name of the person.
4. If this person has a cell phone or pager with ability to receive SMS text messages, then in the **SMS Type** field, select **SMS (TAP)**. In the **SMS Number/ID** field, enter the cell phone number or pager ID. In the **Service Center Number** field, enter the modem pool phone

number that was provided by the person's service provider. Before RWME can send SMS alerts, you must attach a modem to the computer where RWME is installed, as well as configure the **SMS Modem Settings** in RWME (see section *Sending a Message to a Pager Device*).

5. If the person has a numeric pager, then in the **SMS Type** field, select **Numeric (DTMF)**. In the **SMS Number/ID** field, enter the pager phone number or ID. Before RWME can send these alerts, you must attach a modem to the computer where RWME is installed, as well as configure the **SMS Modem Settings** in RWME (see section *Sending a Message to a Pager Device*).
6. If this person has an Email address, enter it in the **Email Address** field. Before RWME can send Email alerts, you need to configure the **Email Alert (SMTP) Settings** in RWME (see section *Sending an Email Message*).
7. Click the **Save** button to add this person in the address book.

## Adding a command line to the address book

1. Click the **Address Book** link.
2. Click the **Add new Command Line** link at bottom of the page.
3. Click on the command name you want to use in the command line. If the command name you wish to use does not appear, you will need to place the command file in the **User Executables** directory of your RWME installation and repeat the above steps.
4. In the **Friendly Name** box, type in the name you desire for the command line.
5. In the **Parameters** box add the command line arguments if any are required.
6. Click the **Save** button to add this command line to the address book.
7. Verify that this command line works properly by clicking, **Test this Command Line**.
8. To check on the execution status of this message open **Log Files-->commandline\_exec.log** to see if the command was executed successfully, or if problems were encountered. If it shows that a problem occurred, you should refer to the *Troubleshooting* section of this manual.
9. Once you have successfully tested the command, you can add this command line to an Alert Group and bind it to a variable's breach limit. To do this, refer to the instructions in section entitled, *Setting up Alerts*.

## Setting up SMTP host names

1. Click the **Settings->Server Settings** link.
2. Scroll down to the SMTP Settings section, and enter the IP address or host name of your primary SMTP server. If you have a secondary SMTP server, you may enter its IP address or host name as well.
3. Type in the email address of the RWME administrator in the **Administrator Email** field. This email address must be a valid and working address. The mail server will use this email address to inform you if an alert message is undeliverable.

4. If your SMTP mail server requires authentication, click the check box named Use SMTP authentication and type the password in the text field below. RWME uses only LOGIN authentication and does not support SSL (secure socket layer) encryption. Some mail servers such as Google Gmail require SSL.
5. Click the **Save** button or the **Test SMTP Settings** button.

## **Sending a test email message**

1. Click the **Address Book** link.
2. You will now either need to modify an existing person from the address book, or create a new person for the address book. To create a new person, click on the **Add a new Person** link at the bottom of the page, and then skip to step 4. To modify an existing person, click on the name of the person to whom the email should be sent. This will open the **View Member Details** page.
3. From the **View Member Details** page, click on the **Modify this Member** link to open the **Update Existing Person** page.
4. Type in the person's first and last name, and an email address.
5. Click the **Save** button
6. On the next page, click the **Send a Test Email to this Person** link. A new window will open with the information for this person. You should verify this information and then click the **Send Now** button.
7. This email message will be added to the RWME email queue. You will need to wait for the RWME email queue to process the message. The RWME queue operates on a First-In First-Out (FIFO) manner, therefore if other alert messages are also waiting in the RWME queue, then this message may take a few minutes to be sent. To check on the delivery status of this message open **Log Files-->smtp-email.log** to see if the message was sent successfully, or whether problems were encountered. If it shows that a problem occurred, you should refer to the *Troubleshooting* section of this manual.
8. Once you have successfully tested the email, you can configure RWME to send alerts via email to this person upon breach conditions. Please follow the instructions in section *Setting up Alerts* to do this.

## **Sending a message to a pager device using a modem**

If you are new to the Sensorsoft Remote Watchman line of products, we suggest that you read *Appendix B – SMS/Paging Tutorial* before continuing.

## **Setting up the modem**

1. If you are using an external modem, you will need to ensure that it is turned on and connected to an available COM port on the computer where RWME is installed. You will also need to ensure that if your modem has DIP switches, which are set according to *Appendix A, SMS/Paging Modem Requirements*.



2. If you are using a dial-up modem, skip to step 5. If you are using a GSM modem, you will need to configure the modem COM Port settings. This is done by first stopping the RWME software (see Stopping RWME Software), and then editing the file RWME.ini in your RWME installation directory using a text editor. In the editor, change the lines

```
ModemPortBitRate=%1200  
ModemPortDataBits=%7  
ModemPortParity=$even  
ModemPortStopBits=$1
```

to

```
ModemPortBitRate=%9600  
ModemPortDataBits=%8  
ModemPortParity=$none  
ModemPortStopBits=$1
```

and then save the file.

3. If you are using a GSM modem, and wish to include international characters (e.g. Thai) in the alert messages, then you will need to set your modem to use PDU mode. This is done by manually editing the Generic\_cellular.ini file in the **Modems** directory of your RWME installation using a text editor. In the editor, change the line

```
MODEM_SMSTYPE=AT+CMGF=1
```

to

```
MODEM_SMSTYPE=AT+CMGF=0
```

and then save the file.



Please be aware that PDU mode supports no more than 30 characters per message, whereas the default Text mode supports up to 160 characters per message. If you choose PDU mode, RWME will truncate all SMS messages to fit the 30 character maximum limit.

4. Restart RWME (see Starting RWME Software).
5. Click the **Settings** link, and then the **Server Settings** link.
6. Scroll down to the SMS Modem Settings section. Select the COM port and your modem type from the list. If you are using a GSM modem, select Generic GSM GPRS Modem from the list. You should also select the Lock Modem Port checkbox for increased reliability. Doing so will prevent other software applications from access the COM port. If your modem is not on the list, you may need to have a custom modem file created. Please refer to *Appendix A, SMS/Paging Modem Requirements* for more information or contact Sensorsoft Technical Support.
7. Click the **Save** button. If any error messages are returned, then you should correct them now.

## **Sending a test SMS message**

1. Click the **Address Book** link.
2. You will now either need to modify an existing person from the address book, or create a new person for the address book. To create a new person, click on the **Add a new Person** link at the bottom of the page, and then skip to step 4. To modify an existing person, click on the

name of the person to whom the SMS should be sent. This will open the **View Member Details** page.

3. From the **View Member Details** page, click on the **Modify This Member** link to open the **Update Existing Person** page.
4. Type in the person's first and last name, if adding a new person.
5. Select SMS (TAP) from the SMS Type combo box if you are using a dial-up modem. Select SMS (GSM) if you are using a GSM modem.
6. Enter your pager number (ID) or cell phone number. You will need to enter this number without dashes or spaces for your service provider to accept it.
7. Enter the Modem Number, also known as the modem pool phone number or service center number for your service provider. You will need to ask your service provider for this phone number.
8. Click the **Save** button. If any error messages are returned, then you should correct them now.
9. On the next screen, click the **Send a Test SMS to this Person** link. A new window will open with the information for this person. You should verify this information and then click the send now button.
10. This message will be added to the RWME SMS queue. You will need to wait for the RWME queue to process the message. The RWME SMS queue operates on a First In First Out (FIFO) manner, therefore if other alert messages are also waiting in the RWME queue, then this message may take a few minutes to be delivered. To check on the delivery status of this message open **Log Files-->SMS.log** to see if the message was sent successfully, or whether problems were encountered. If it shows a problem occurred, then you should refer to the *Troubleshooting* section of this manual.
11. Once you have successfully tested the SMS, you can configure RWME to send alerts via SMS to this person upon breach conditions. Please follow instructions in section *Setting up Alerts* on how to do this.

## **Sending a test DTMF message to a numeric only pager**

1. Click the **Address Book** link.
2. You will now either need to modify an existing person from the address book, or create a new person for the address book. To create a new person, click on the **Add a new Person** link at the bottom of the page, and then skip to step 4. To modify an existing person, click on the name of the person to whom the message should be sent. This will open the **View Member Details** page.
3. From the **View Member Details** page, click on the **Modify this Member** link to open the **Update Existing Person** page.
4. For this person, you will need to enter the following:
  - The person's first and last name if adding a new person
  - Select Numeric (DTMF) from the SMS Type combo box
  - Enter your ID number

- Enter the number of seconds that RWME should wait for the voice announcement to end, before issuing the numeric message
5. Click the **Save** button. If any error messages are returned, then you should correct them now.
  6. On the next screen, click the **Send a Test SMS to this Person** link. A new window will open with the information for this person. You should verify this information and then click the **Send Now** button.
  7. This page message will be added to the RWME queue. You will need to wait for the RWME queue to process the message. The RWME queue operates on a First In First Out (FIFO) manner, therefore if other alert messages are also waiting in the RWME queue, then this message may take a few minutes to be delivered. To check on the delivery status of this message open **Log Files-->SMS.log** to see if the message was sent successfully. If it shows that a problem occurred, then you should refer to the *Troubleshooting* section of this manual.
  8. Once you have successfully tested the SMS, you can configure RWME to send alerts via SMS to this person upon breach conditions. Please follow the instructions in the section *Setting up Alerts* on how to do this.

## Setting up a command line

For the following sections, you will need to be logged into RWME using the admin account.

When you are setting up command lines to be run from within RWME, you will need to ensure that any programs that you want to execute reside within the User Executables sub-folder of the RWME installation. Only files in this folder will be executed by RWME. Please see the *Security Considerations* section for more information.

## Sending a message to a Windows machine or user

This example demonstrates how to send a message to a Windows machine or user on your network using the Microsoft NetBIOS Messenger Service. This procedure only works on Windows 2000, XP and Server 2003 and only with the Messenger service running. This must be done on the RWME machine and the remote machine(s) where the message is destined.

1. Click the **Address Book** link.
2. Click the **Add new Command Line** link at the bottom of the page.
3. Click on the command **NET.EXE**.
4. In the **Friendly Name** box, type in the name you desire for the command line.
5. In the **Parameters** box add the arguments or parameters. This command line uses three parameters to make it run. These parameters are separated by a space. If you wish to use a space in the parameter list and you would like it to be represented as a space, then that single parameter must be enclosed in double quotation marks. For this command line, you should modify the example below to be applicable on your network;

send computer\_name "\$D in \$L is \$R"

The first parameter is **send**

The second parameter is **computer\_name** or **/DOMAIN:computer\_name**

The third parameter is **"\$D in \$L is \$R"**

You will need to change the value of the second parameter to the name of the computer where the message will be sent. You should only enter the host name of the computer and not the fully qualified host name. For example, if the fully qualified host name is computer1.yourcompany.com, you should only enter computer1 as the parameter or alternatively /DOMAIN:computer1.

6. Click the **Save** button to add this command line to the address book.
7. Verify that this command line works properly by clicking, **Test this Command Line**.
8. You should now see a message pop up on the target computer's screen. If this command is bound to a group and run during an actual alert, the \$ variables will be filled in with the proper values for the item/node being monitored. If you did not see the message pop up on the target computer's screen, this could result if NetBIOS is disabled on your network or machine or RWME is outside of the NetBIOS domain. In this case, you can test the command from a command prompt window on the machine where RWME is installed. In addition make sure that the Messenger Service is started on the RWME machine and the remote machine.
9. Once you have successfully tested the command, you can add this command line to an alerting group and bind it to a variable's breach limit. To do this, refer to the instructions in section entitled, *Setting up Alerts*.

## Shutting down a Windows machine

You can configure RWME to shutdown a Windows machine on your local network as an alert action. To do this, RWME needs to use Sysinternals' free software utility **PSShutdown**. This is part of Sysinternals' PsTools suite, and is not packaged with RWME. The PsTools suite can be downloaded from the following URL:

<https://live.sysinternals.com/>

Before using the procedure below, we suggest testing that the RWME machine has connectivity to the remote machine you want to shutdown. You can do this using the Windows Start-Run command window on the RWME machine and the following syntax:

```
\\remote_computer_name
```

The remote Windows machine should respond by providing a window of available shares (disk drives, folders or printers) or perhaps a login username and password dialog. If an error message appears you will need to do some troubleshooting to determine the cause. Do not proceed without success.

The next step is to test the psshutdown command from a win32 command prompt window. Make sure you are logged in as Windows Administrator on the RWME machine before attempting this test, or it will not work. Type the following command in a command prompt window on the RWME machine (to reboot the remote machine as a test):

```
psshutdown -r -t 60 -m "this is a test" -u administrator -p <password>  
\\remote_computer_name
```

Substitute the remote machine's correct administrator password for the <password> syntax shown above. Also replace remote\_computer\_name with the actual network name of the machine (usually the DNS name). You should see the remote machine reboot successfully. If not, observe the error message and correct the problem. Do not proceed until you have success.

To have RWME shutdown a Windows machine as an alert event:

1. Configure the RWME service to log on with a network administrative account (see *Appendix H – Configuring RWME Service to Log On with an Administrative Account*).
2. Place **psshutdown.exe** command file in the **User Executables** directory of your RWME installation.
3. Click the **Address Book** link.
4. Click the **Add new Command Line** link at the bottom of the page.
5. Click on the command **psshutdown.exe**.
6. In the **Friendly Name** box, type in the name you desire for the command line.
7. In the **Parameters** box add the arguments you need using the syntax definition below.
8. Click the **Save** button to add this command line to the address book.
9. Verify that this command line works by clicking the link, **Test this Command Line**. The web interface always reports success, even if the command fails to shutdown the remote machine. So verify the remote machine is in fact shutting down. If it is not, you did not successfully complete this procedure or the pre-testing procedure.
10. Once you have successfully tested the command, you can add this command line to an alerting group and bind it to a variable's breach limit. To do this, refer to the instructions in section entitled, *Setting up Alerts*.

#### Syntax for the PsShutdown command:

```
psshutdown -t <countdown> -m "<message>" -u <user> -p <password> \\<computer>
```

where

<countdown> is the time in seconds until the shutdown.  
<message> is the message to display to logged-on users when a shutdown countdown commences  
<user> is the username of the administrative account on the target computer  
<password> is the administrative account password  
<computer> is the remote computer or computers specified. If you omit the computer name the command runs on the local system, and if you specify a wildcard (\\\*), the command runs on all computers in the current domain.

## Running multiple command lines

If you need to execute several command lines in sequence you have two ways:

- Add these commands to a batch file (.bat) and in the sequence you need them to execute. Then create a command line in the Address Book that executes this batch file.

- Add several separate command lines in the Address Book and add each of these command lines to a single Alert Group. The order of the command lines you see in the Alert Group is the order in which they are executed. You can only change this order by editing each command line or creating them in the order you desire.

### **Additional information about command lines**

To learn about useful command line functions that are integrated into RWME, see *Appendix E – Running RWME Pipe Command Lines*.

## Controlling Sensorsoft Devices

Some Sensorsoft devices (SSD's) contain variables that can be written or modified. RWME can be used to modify these values in two ways:

- Using Pipe commands (*Appendix E – Running RWME Pipe Command Lines*)
- Using the Web interface

We will discuss here how to use the web interface method. In the example of Figure 13 we see RELAY\_BIT, for a Sensorsoft SR6171J Relay, can be modified. We know this because it has a link called Modify Variable Value. By clicking on this link you will be shown a page like that in Figure 14.



Figure 13: Link to Modifying a Variable Value page

Here you are shown the current state of the relay (OFF) with the possibility to change it to the opposite state (ON) as also shown. When you click Submit it changes the relay to the ON state.

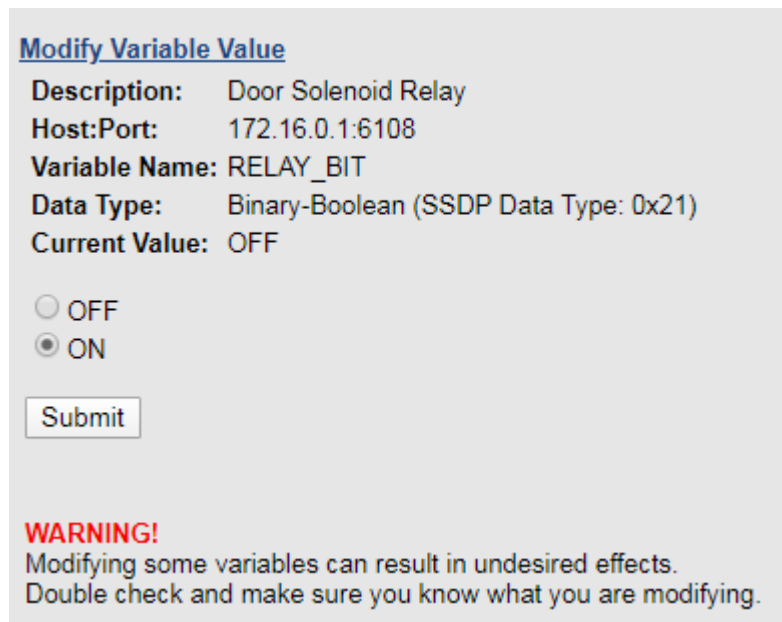


Figure 14: Modify a Variable Value

## Customizing variable description and Boolean strings in the SS6420

Customization of variable descriptions and Boolean strings are supported by the Sensorsoft Real-Time Contact and Voltage Sensor (Model SS6420). The variable descriptions and Boolean strings are stored in non-volatile memory in the device. This means that if the device is powered off, or if RWME is reinstalled, these custom strings will still remain in the device.

The variable description is a custom description that you can add to a particular variable to describe it in more detail. For example, if you are using the SS6420, then you would notice there are 12 contact variables with names CONTACT(C01) – CONTACT(C12), respectively. You can add a description to each of these contact variables to describe how each contact is being used. So if CONTACT(C01) is connected to a motion detector in the lobby, then you may want to give it the description “Motion Detector in Lobby”. This description would then appear in the **Variable column** of the Monitor List, making the field read “CONTACT(C01) – Motion Detector in Lobby”.

You can also customize a Boolean variable’s Boolean strings. Each Boolean variable has two Boolean strings: the zero-state string and the one-state string. The best way to demonstrate the usefulness of custom Boolean strings is with an example. Suppose the CONTACT(C01) of your SS6420 is connected to a motion detector, and when the motion detector sees motion, it closes its contact output, and when it sees no motion, it opens its contact output. You may find it much more user friendly if CONTACT(C01) reported STILL/MOTION rather than the default OPEN/CLOSED.

To customize a variable’s description and Boolean strings, do the following:

1. Click the link in the **Description** field of the target device. This will take you to the **Sensorsoft Device Details** page.
2. Scroll to the section titled **Sensorsoft Device Readings**. At the bottom of this section, click the link **View Tech Variables**. If this link does not exist, it means that the Sensorsoft Device does not support the customization of variable description and Boolean strings.
3. After clicking the **View Tech Variables** link, additional variables will be visible in the variable list as in Figure 15. In the list, locate the variable that you would like to customize. Going back to the above example, you would look for the variable CONTACT(C01). If the variable is customizable, then below it, you will see the variables CONTACT(C01)\_DESCRIPTION, CONTACT(C01)\_ZEROSTATE and CONTACT(C01)\_ONESTATE.

View on Monitor List	Variable Index	Variable Name	Last Reading	Log Readings
<input checked="" type="checkbox"/>	1	CONTACT(C01)	OPEN	No
	2	CONTACT(C01)_SETTINGS	6	<a href="#">Modify Variable Value</a>
	3	CONTACT(C01)_DESCRIPTION	-	<a href="#">Modify Variable Value</a>
	4	CONTACT(C01)_ZEROSTATE	OPEN	<a href="#">Modify Variable Value</a>
	5	CONTACT(C01)_ONESTATE	CLOSED	<a href="#">Modify Variable Value</a>

Figure 15: Viewing Tech Variables

4. To add a custom description to the variable CONTACT(C01), click the link **Modify Variable Value** next to CONTACT(C01)\_DESCRIPTION. Enter your custom variable description and then click the **Submit** button.
5. To customize CONTACT(C01)’s Boolean strings, modify the variable values of CONTACT(C01)\_ZEROSTATE and CONTACT(C01)\_ONESTATE. Going back to the previous example, you would change CONTACT(C01)\_ZEROSTATE’s value from OPEN to STILL, and change CONTACT(C01)\_ONESTATE’s value from CLOSED to MOTION.



## Security Considerations

### IP blocking and trusting

This security feature allows you to restrict the computers that can log in to RWME by denying access to specified IP addresses. This feature is useful if you are exposing your RWME web server port to the Internet. RWME can be configured to allow your residential IP address to access RWME, while blocking the rest of the Internet.



**IMPORTANT** – If you are planning to expose RWME to the Internet, Sensorsoft recommends that you do so through a separate firewall device that is capable of protecting your network from various hacker attacks, including SYN flooding, Ping of Death, IP Spoofing, etc. These types of attacks may cause RWME to respond unexpectedly, or can cause it to fail.

### Multi-Level user access

RWME offers two levels of user access to allow some users to view only current monitored item/node information, while allowing other users to fully administer RWME.



**IMPORTANT** – Sensorsoft recommends that you only log into RWME using the ruser account when accessing RWME over the Internet. This will protect your admin password from being sent as clear text, as described in the next section.

### Password encryption

RWME encrypts both its admin and ruser passwords and stores them in the passwords.dat file to ensure that the passwords cannot be easily read without the use of the decryption algorithm.



**IMPORTANT** – Passwords are not encrypted as they are traversing the network from your web browser to RWME. An individual or hacker that is sniffing the network will be able to read this information as clear text.

### Inactive user logout timer

The inactive user logout timer ensures that a login to RWME is logged out after a period of no use. By default this setting is disabled.



**IMPORTANT** – For the inactive user logout timer to work correctly make sure that the refresh period for the Monitor List page is set to slightly longer period. For example, if you want a 30 minute (1800 sec) inactive logout timer, use a (monitor list) refresh period of 1810 second.

### Logged in users count

RWME displays the number of users that are logged in on the bottom left corner of the page.

## Web access history

RWME records all web access login and logout events in the file **webaccess.log**. These events include both successful and failed login attempts. A logout event occurs when the user clicks the **Logout** link. Closing the browser or a tab will not result in a logout event. The **webaccess.log** can only be viewed by the admin user. To view this file, see section *Viewing Log Files*.

## Admin use history

RWME records important administrator's actions in a file called **admin\_audit.log**. This includes:

- adding, removing or modifying an item/node
- adding or removing an Alert Group, Person or Command Line
- upgrading the license key item/node limit
- changing Alert Message Definitions
- changing Monitor List Display Settings
- reordering the Monitor List
- renaming a monitor group
- requested update of all node readings
- lost/forgotten password reset
- changing admin or ruser passwords

## User executables

When you are setting up Command Line alerts with RWME, only programs that exist in the User Executables folder can be run. This ensures that potentially harmful commands cannot be run on your system.



**IMPORTANT** – When you place a file in this folder it can be run by anyone with RWME admin privileges. Please be sure that any files that you place in this folder cannot inadvertently harm your system.

## User definable web server port

Although the Internet Assigned Numbers Authority (IANA) has defined TCP port 80 as the international standard TCP port for web browsers and servers, you may wish to change this value to add an increased layer of security to RWME. You have the option to set this port from 1 to 65535, but Sensorsoft recommends that you choose a port between 1024 and 65535, as ports 1 through 1023 are reserved for “well known” protocols.

## Troubleshooting Guide

The troubleshooting guide is designed to help you in the event that you should have trouble with RWME. In order to make effective use of this guide (and Sensorsoft technical support, should it be necessary) it is beneficial that you attempt to determine the precise nature of the problem.

## Web Server problems

RWME can take between five seconds and two minutes to start the web server. This is because it is loading the monitoring.ini file, and this can take quite a bit of time depending on how many items/nodes you are monitoring and how many address book entries you have.

To verify that the web server is running, go to the Logs folder in the RWME installation folder and open the **rwme.log** file. Scroll to the bottom of this file, and check to see if there is an entry that says “Web Server Started on Port *TCP\_Port*”. If you do not see this message, you may need to wait longer for the web server to start. If you see a message that says “Error Starting Web Server on Port *TCP\_Port* – *Err\_Code*”, then there has been a problem starting the web server. In both cases, *TCP\_Port* is the TCP port number that RWME attempted to start the web server on. In the latter case, *Err\_Code* is the operating system error code that was returned. The most common error codes are listed below.

You may wish to change the TCP port that the RWME web server uses, and this can be done by modifying the **rwme.ini** file. This file can be found in the RWME installation folder. The variable that needs to be modified is HTTPServerPort, and this can be found in the MISC section. Please choose an alternate value, between 1024 and 65535.

If *TCP\_Port* is not 80, this means that the web server attempted to start on a port that is different from the IANA standard. You will need to access RWME by using an address style that is similar to this in your web browser:

```
http://rwme_computer:TCP_Port
```

where *rwme\_computer* is the IP address or host name of the computer that RWME is installed on, and *TCP\_Port*, is the port that is specified in the rwme.ini file. Please note that you must include the *http://* so that your web browser knows that it is attempting to communicate with a web server. This addressing style will work with both Microsoft Internet Explorer and Mozilla Firefox. If you are using a different web browser, then your addressing style may differ from that shown above.

If you have verified that the Sensorsoft RWME 2020 service is running, and that the **rwme.log** file indicates that the web server has successfully started, the problem could lie with your web browser. You may try holding down the shift key and pressing the Refresh or Reload button. This will force your web browser to stop pulling information from its cache, and attempt to contact the web server again. If this does not solve the problem, you should restart your computer and try again, or try to connect to RWME using a different computer.

## Common error codes and solutions

**10048** – The TCP Port specified is already being used by another application. You will need to stop the offending application from using this TCP Port, or modify the rwme.ini file to use a different TCP Port.

**10013** – The TCP Port specified is being blocked by security software. Temporarily stop the security software from running to see if RWME will start without error. You should be able to configure your security software to make an exception for the RWME software.

**10049** – The requested address is not valid. You will need to ensure that the TCP Port number that is specified in `rwme.ini` is between 1 and 65535.

**10050** – A socket operation encountered a dead network. You will need to verify that your network is functioning properly. Performing a full shutdown and reboot of your system may be required. This error can indicate either a physical or logical failure in your computer's operating system or hardware or in the attached network.

**10091** – The underlying networking system that is used to provide network services is currently unavailable. You will need to ensure that TCP services have been installed in your Network Neighborhood properties.

**10092** – The version of Winsock that you have installed on your system is not sufficient. You will need to ensure that your Windows system, where RWME is installed, is running the latest service pack.

## Email problems

If you are experiencing problems sending an email, you should in all cases find out what error message is being sent to your **smtp-email.log** file. The following is a list of common errors and their solutions.

### **SMTP Error: Timed out waiting for mail server <>**

The IP address or host name for your primary or secondary mail server is empty. Please refer to *Sending an Email Message*.

### **SMTP Error: Timed out waiting for mail server <IP\_ADDRESS>**

The remote mail server was contacted but did not respond to the SMTP request in a timely manner.

### **SMTP Error: Timed out while attempting to connect to mail server**

Your primary or secondary SMTP server could not be contacted. Verify that the proper SMTP host address is entered in the **Settings->Server Settings** page.

### **Winsock Error 11001: No such host is known. <HOST\_NAME>**

Your primary or secondary SMTP server's host name could not be found. Verify that the proper SMTP host address is entered in the **Settings->Server Settings** page.

### **SMTP Error: Unexpected disconnect from mail server**

The remote mail server closed the socket connection unexpectedly. It is possible that the remote mail server was shutdown, or that the network between the RWME installation computer and the SMTP server has been disconnected. The email will be held in the RWME email queue and sent out again later.

### **SMTP Service Not Available**

The SMTP server was unable to accept messages for delivery. This may be due to the SMTP server being overwhelmed by large volumes of outgoing mail.

### **SMTP Transmission Error**

An unexpected response was received from the SMTP server. Double check the server address you have specified, and make sure the server is an SMTP server.

**Unable to relay or invalid E-mail Address: <RECIPIENT\_ADDRESSES>**

The given recipient email addresses may be invalid. Make sure multiple email addresses for the same person are delimited with semicolons. Another possibility is that relaying on the SMTP server has been disabled. If this is the case, the SMTP administrator should be contacted for assistance.

**SMS problems**

If you are experiencing problems sending an SMS message, you should in all cases find out what error message is being sent to your **SMS.log** file. If your modem has DIP switches, insure that they reflect the settings shown in *Appendix A*. The following is a list of common errors and their solutions:

**Received COM error code 2 – The Com Port does not exist.**

The com port that you have specified for the modem on the **Settings->Server Settings** page does not exist.

**Received COM error code 5 – The Com Port is in use.**

The modem's com port is being used by another application. You may wish to consider locking the modem's com port with the check box on the **Settings->Server Settings** page to prevent future errors.

**A modem error has been detected.**

The modem is returning an error message. You should verify that you have the proper modem type selected on the **Settings->Server Settings** page. If your modem has DIP switches, insure that they reflect the settings shown in *Appendix A*. If you are using a cellular modem, ensure that your SIM Card has been activated by a service provider and that it is securely plugged into your modem.

**No carrier signal could be detected.**

The modem dialed but did not connect to another modem at the destination phone number. You should verify the modem phone number for your service provider.

In rare cases, you may also need to increase the value of the **ConnectTimeout** in the **rwme.ini** file, and modify the appropriate variable in the modem setup string. You will have to restart the Sensorsoft RWME 2020 service for this change to take effect.

If you still receive this error message after trying the above, you should contact your service provider to report a problem.

**No dial tone was detected.**

You should verify that the phone line is securely plugged into the proper jack on the modem and the wall. You should also verify that the dial tone is steady. An intermittent dial tone can be caused by a message indication from your call answer service. You may wish to disable the call answer service feature.

**Received <CR><RS><CR> from the service provider - invalid ID number: <invalid ID>**

The pager ID is invalid, is no longer in use, or has been entered incorrectly. Verify the pager ID number with your service provider or try altering the format, by removing dashes, spaces or the area code.

**The modem did not respond to the reset command.**

You should verify that the modem is properly connected and that you have the proper modem type selected on the **Settings->Server Settings** page. If your modem has DIP switches, insure that they reflect the settings shown in *Appendix A*.

You should also check your modem com port settings in **rwme.ini** to make sure that they match your service provider's requirements. The variables that define the modem com port settings are **ModemPortBitRate**, **ModemPortDataBits**, **ModemPortParity** and **ModemPortStopBits**. For more information about these variables and how to change their values, see *Appendix C – Useful Variables in Rwme.ini*. You should also contact your service provider to find out what modem com port settings they require.

**The modem did not respond to the modem setup command.**

You should verify that the modem is properly connected and that you have the proper modem type selected on the **Settings->Server Settings** page. If your modem has DIP switches, insure that they reflect the settings shown in *Appendix A*.

**Modem Setup String Error**

You should verify that the modem is properly connected and that you have the proper modem type selected on the **Settings->Server Settings** page. If your modem has DIP switches, insure that they reflect the settings shown in *Appendix A*.

**Modem did not send a connect response within the timeout period.**

The modem dialed but did not connect to another modem at the destination phone number. You should verify the modem phone number for your service provider.

You may also need to increase the value of the **ConnectTimeout** in the **rwme.ini** file, and modify the appropriate variable in the modem setup string. You will have to restart the Sensorsoft RWME 2020 service for this change to take effect.

If you still receive this error message after trying the above, you should contact your service provider to report a problem.

**The service provider did not send ID= within the timeout period.**

If you receive this message once, you may need to increase the value of the **ResponseTimeout** in the **rwme.ini** file under the heading [SMS TIMEOUTS]. You should also check your modem com port settings in **rwme.ini** to make sure they match your service provider's requirements. The variables that define the modem com port settings are **ModemPortBitRate**, **ModemPortDataBits**, **ModemPortParity** and **ModemPortStopBits**. For more information about these variables and how to change their values, see *Appendix C – Useful Variables in Rwme.ini*. You should also contact your service provider to find out what modem com port settings they require. If you choose to increase the value of the **ResponseTimeout** or change your modem com port settings, you will have to restart the Sensorsoft RWME 2020 service for the changes to take effect.

If you continue to receive this error message after trying the above, you should contact your service provider to report a problem.

**The service provider did not send <ESC>[p<CR> within the timeout period.**

If you receive this message once, you may need to increase the value of the **ResponseTimeout** in the **rwme.ini** file. You will have to restart the Sensorsoft RWME 2020 service for this change to take effect.

If you receive this error message after trying the above, you should contact your service provider to report a problem.

**The service provider did not send <CR><ACK><CR> within the timeout period.**

If you receive this message once, you may need to increase the value of the **ResponseTimeout** in the **rwme.ini** file. You will have to restart the Sensorsoft RWME 2020 service for this change to take effect.

If you receive this error message after trying the above, you should contact your service provider to report a problem.

**Modem did not send an OK response within the timeout period for message send.**

You should verify that your DTMF alert messages do not contain any characters other than 0 - 9, '#' and '\*'. Dollar (\$) variables are also not allowed in DTMF messages, and using them can cause the DTMF paging routine to function improperly and generate the above error message.

**Unexpected response from modem**

You should verify that the modem is properly connected and that you have the proper modem type selected on the **Settings->Server Settings** page. If your modem has DIP switches, insure that they reflect the settings shown in *Appendix A*.

You should also check your modem com port settings in **rwme.ini** to make sure they match your service provider's requirements. The variables that define the modem com port settings are **ModemPortBitRate**, **ModemPortDataBits**, **ModemPortParity** and **ModemPortStopBits**. For more information about these variables and how to change their values, see *Appendix C – Useful Variables in Rwme.ini*. You should also contact your service provider to find out what modem com port settings they require.

**Message not accepted by provider.**

You should verify that the length of your message does exceed the maximum allowed message length of your service provider.

You should also check your modem com port settings in **rwme.ini** to make sure they match your service provider's requirements. The variables that define the modem com port settings are **ModemPortBitRate**, **ModemPortDataBits**, **ModemPortParity** and **ModemPortStopBits**. For more information about these variables and how to change their values, see *Appendix C – Useful Variables in Rwme.ini*. You should also contact your service provider to find out what modem com port settings they require.

## **Common problems**

**I have forgotten my ruser password.**

If you know the admin password, you can log in to RWME using the admin account and change the ruser password. This page is found by clicking on **Settings->Server Settings**.

**I have forgotten my admin password.**

The admin password can only be reset from the computer that RWME is installed on. To reset the password, you will need to stop the **Sensorsoft RWME 2020 service**. Once the service is completely stopped, you must delete the **passwords.dat** file from the RWME installation directory. Restart the **Sensorsoft RWME 2020 service** from the SCM. You may need to wait for

up to two minutes for the RWME web server to be started, while RWME is loading the information in your monitoring.ini file. Once the RWME web server is restarted, you may attempt to access RWME with your web browser. You will be asked to enter a new admin password. Please note that this procedure also resets the ruser password to **begin**.

**I am receiving the message “Your IP has been blocked by the administrator.”**

This means that the RWME administrator has blocked your IP address from accessing RWME. You should ask them to modify this setting by logging in and following the **Settings->Server Settings** link. Please note that you cannot block the IP address of the computer that RWME is installed on, even if this IP address is specified in the IP access list. You may need to modify the IP access list from this computer if all IP addresses have been blocked.

**Some log entries are missing from a log file.**

This can happen if you frequently view or graph log files from the RWME web server. When a file is being downloaded for viewing or graphing, it cannot be updated by RWME, and so no new log entries can be made to it. One way to adjust for this is to set the value of the variable LogFileLinesToReturn in rwme.ini to a positive whole number that is less than 5000 (see *Appendix C – Useful Variables in Rwme.ini* for how to change a variable value in rwme.ini). This will limit the number of lines that the web server returns to be less than 5000, and thus the length of time that the file will be opened will be shortened.

Another possible cause of this problem is that you may have opened the log file with a software program that locked the file. Examples of such software programs are Microsoft Word and Microsoft Excel. As long as the file is opened by such a program, the file would be locked, which means RWME would not be able to update it. If you really need to edit a log file, or view it without the use of RWME, we recommend that you use Microsoft Notepad or WordPad, because these editors will only lock the file briefly when the file is being loaded into memory or saved.

**My alert and log settings for a device have been disabled, unexpectedly.**

This could happen if you swapped out an ST6105 or ST6154 Sensorsoft Thermometer for one that has newer firmware (from v1.51 to v2.02 or greater). Earlier firmware such as v1.51 has only one temperature variable. Later firmware such as v2.02 or greater has two temperature variables. The RWME software reacts to this radical change in variables by disabling the log and alert settings and sending a warning email to the RWME Administrator.

**Monitor List shows a monitored item/node to be in breach state even though the item/node has not been assigned an alert group or breach limit.**

In RWME Build 94 or higher, the Monitor List will show an item/node (color change) to be in breach state as long as the item/node's reading has exceeded its breach limits. This allows users to see if an item/node has exceeded defined limits without having to setup an alert group. If you do not want the Monitor List to display the breach state for an item/node, simply modify the breach limits of the item/node to be well beyond any normal scalar reading. See the following example:

Critical High Limit = 100000  
Warning High Limit = 10000



Warning Low Limit = -10000  
Critical Low Limit = -100000

**Sensors reporting Timeout or false temperature readings of 85° Celsius (185 Fahrenheit).**

If you are using a device server that asserts RTS/DTR only when a TCP connection is made to that port, then the cause may be insufficient sensor power-up delay. The power-up delay is used to give a sensor sufficient time to energize before RWME begins to communicate with it. By default, the power-up delay for every sensor is zero, but you can change these values by modifying them in monitoring.ini. Simply add the following line to the file:

SensorPowerUpDelay<X>=%3

where <X> is the index of the sensor for which you want to apply the delay. The delay is specified in seconds. The above example would add a 3 second delay.

**I want to check the accuracy of some Sensorsoft temperature or humidity sensors. How do I get live (up to the second) readings of these scalar type sensors?**

RWME's quickest Update Interval setting for scalar Sensorsoft Devices is once per minute. If you need faster updates use the following procedure:

1. Expand your web browser to full screen mode.
2. In the Monitor List click the Description link for the scalar sensor in question.
3. Click the link "Update this Item/Node's Reading" in the Sensorsoft Device Management section.
4. Wait for the page to refresh and notice that the scalar values change in the Last Reading column of the Device Readings section.

## Getting Help

### Technical Support

Should you have problems installing or using Sensorsoft Remote Watchman Enterprise 2020 we offer technical support to help you overcome your difficulties for a one-year period.

You will receive support incidents (telephone calls or emails) with your purchase of a Sensorsoft Remote Watchman Enterprise 2020 license. The number of incidents depends on the item/node level of your license. See the following URL for more details:

<https://www.sensorsoft.com/rwme.html>

After these incidents expire you can choose to purchase a support package or pay a charge-per-incident fee for technical support. The RWME software license is **perpetual**; you **do not** have to pay a periodic subscription fee.

#### Before contacting Sensorsoft Technical Support:

Go through the *Troubleshooting Guide* in the previous sections of this manual. Even if a direct answer to your question is not found there, it will be helpful for the support technician if you are able to provide information obtained from the diagnostic and troubleshooting process. Please ensure the problem is directly related to the Sensorsoft Remote Watchman Enterprise 2020 software.

**World Wide Web:** <https://www.sensorsoft.com>

### 30-day money back guarantee

If for any reason you want to return a Sensorsoft product for a refund, you can do so within 30 days (calendar days) of your purchase. The refund does not include shipping or brokerage fees you may have incurred or paid.

## Appendix A – SMS/Paging Dial-up Modem Requirements

This section does not apply to GSM/3G/LTE modems.

### DIP switches

If you have a 3Com or U.S. Robotics modem with DIP switches, please make sure they reflect the required settings shown below. If you have another brand of modem which has DIP switches, please make sure they reflect the settings shown in the Function column:

#### DIP Switches (External Modems with DIP Switches Only)

Switch	Position	Function
1	OFF - UP	Normal DTR operations
2	OFF - UP	Result codes are words
3	ON - DOWN	Enable result codes
4	ON - DOWN	Echo disabled
5	ON - DOWN	Auto Answer disabled
6	OFF - UP	CD reflects state of carrier
7	OFF - UP	On power-up load user definition
8	ON - DOWN	Modem operates in smart mode

### Custom modem strings

Although Sensorsoft has found that most organizations are using one of our supported modem types, there are instances when your organization will be using a modem that is not supported. In this case, you may need to create your own modem file. If you are creating your own custom modem file, you should make a copy of the custom\_page.ini file in the Modems folder of your product installation folder.

You will need to obtain a list of AT commands for your particular brand of modem. This can generally be found on the modem manufacturer's web site, or in your modem's user manual.

You will need to modify the custom\_page.ini file to reflect the settings for your modem. The required settings for each string are listed below. Please note that not all AT command sets will support all of the settings listed below, and as such you may not be able to find a code for all of the following requirements:

#### MODEM\_SETUP

- Disable Echo
- Return Result Codes

- Use Verbal (Text) Result Codes
- Use All Result Codes
- Turn Speaker on Until Connect
- Error Control Disabled
- Connect Speed of 300 bps to 1200 bps
- Software Flow Control Disabled
- Hardware Flow Control Disabled
- Normal DTR (Data Terminal Ready) Operations
- Normal CD (Carrier Detect) Operations
- Disable Auto Answer
- Disable Compression
- Set the number of seconds to wait for a carrier to 30

#### **MODEM\_RESET**

- Disable Echo
- Return to Factory Default Settings

#### **Other Strings**

String	Description	Common Values
MODEM_DIALCMD	Command used to dial	ATDT
MODEM_ESCAPE	Character escape sequence used to terminate the connection	+++
MODEM_HANGUP	Command used to hang up	ATH0
MODEM_OK	Verbal success indicator	OK
MODEM_NOCARR	Verbal no carrier detect indicator	NO CARRIER
MODEM_ERROR	Verbal error indicator	ERROR
MODEM_NOTONE	Verbal no dial tone indicator	NO TONE
MODEM_BUSY	Verbal busy signal indicator	BUSY
MODEM_NOANS	Verbal no answer indicator	NO ANSWER
MODEM_CONNECT	Verbal connection established indicator	CONNECT

## Appendix B – SMS/Paging Tutorial

RWME supports three methods that can be used to issue alerts to your mobile device. The following section will help you determine what method of delivery you can use:

### What type of mobile device do you have?

There are four main types of mobile devices:

1. Cell phones with SMS text messaging service
2. Alphanumeric pagers
3. Numeric pagers
4. Smart phone

### What delivery method does your service provider use to send messages to your mobile device?

There are five main methods that are used to deliver messages to your mobile device:

- A. I have software for my computer that sends messages to my mobile device using my modem.
- B. I use one paging device to send messages to a second paging device.
- C. I dial the pager's phone number and wait for a voice that tells me to punch-in my call-back phone number with a Touch Tone™ (DTMF) key pad.
- D. I send an email to the device using an email address that was given to me by my service provider.
- E. I go onto my service provider's web site and send a message using a web page.

### What method should RMWE use to send messages to my mobile device?

Using your answers from the last two questions, you can find out what method you should be using to send messages to your mobile device. Your service provider may not make all of the above methods available to you.

	A	B	C	D	E
1 Digital Phone	SMS	SMS	N/S	SMTP	SMS
2 Alphanumeric Pager	SMS	SMS	DTMF	SMTP	SMS
3 Numeric Pager	SMS or DTMF	SMS	DTMF	SMTP	SMS
4 Smart phone	SMS	SMS or Other	N/S	SMTP	SMS

N/S – Not Supported

### **SMS through a dial-up modem**

RWME can use the TAP protocol to send SMS messages to your mobile device using your computer's dial-up modem and a telephone line. **In order to setup SMS in RWME, you will need to call your service provider and ask them for the following:**

- Their modem pool phone number.
- Your device's ID or phone number and any special formatting that is required.

The formatting of the ID varies from provider to provider. In most cases, you will find that your ID is the device's phone number. The format of the ID also varies. Some service providers will not accept the ID if the area code is missing, while others will not accept the ID if dashes are used to separate the numbers. You will need to enter the ID into RWME exactly as your service provider requires.

### **SMS through a cellular modem**

RWME can send SMS messages if you have a cellular modem. This modem must be directly connected to a USB or serial port on the computer that is running the RWME software. **In order to setup SMS in RWME, you will need to call your mobile service provider and ask them for their SMS service center phone number.** The advantage of using cellular modem for SMS is that you do not need a dedicated telephone line. Cellular modems are wireless and use the cellular phone network.

### **SMTP SMS Gateway**

If your SMS service provider uses the SMTP protocol to send messages to your cell phone or pager device, then you do not need to configure the SMS portions of RWME. In this case, we recommend using the email messaging feature of RWME. Use the SMS gateway email address that can be provided by your service provider.

### **DTMF paging**

RWME can dial your paging device's phone number to send it a numeric page. When you are setting up the message, you will need to specify the amount of time that RWME should wait for the voice announcement to finish before issuing the DTMF message tones. This may require several attempts to determine the optimal time to wait for the voice announcement to finish.

It is also possible that your numeric pager can receive SMS messages (numeric only). You may wish to contact your service provider to find out about this. SMS is a more reliable method of delivery that includes confirmation. DTMF paging provides no confirmation of message delivery.

## Appendix C – Making changes to setup files using a text editor

The more common method of changing settings in RWME is to use the web interface. You can also change settings by editing the files `rwme.ini` and `monitoring.ini` located in RWME's root installation directory. Both text files contain many of RWME's settings. Each keyword in the files corresponds to a setting. To change a setting, one can edit the value of the corresponding keyword. The procedure below describes how to change a setting:

1. Stop the RWME service. (Refer to *Stop the RWME Software*)
2. Open the `rwme.ini` or `monitoring.ini` file using notepad or another text editor.
3. Locate the keyword associated with the desired setting to configure (see the table below for a list of commonly used keywords). If you are unable to locate one of the keywords shown below, in the file, you can also add it to the end of the file.
4. Set the keyword to the desired value (see the table below for allowable values).
5. Save the file and restart the RWME service (Refer to *Start the RWME Software*). The new settings will now take effect.

Keyword	Description	File	Possible values
HTTPServerPort	Defines the TCP port number of RWME's web server. The default is 80.	rwme.ini	%1 to %65535
AlternateHTTPServerPort	Defines the beginning of a range of TCP port numbers that RWME can use as an alternate web server port if the desired one, HTTPServerPort, is not available.	rwme.ini	%1 to %65535
SMTPServerPort1	Defines the TCP port number used by the remote primary mail server. The default is 25.	rwme.ini	%1 to %65535
SMTPServerPort2	Defines the TCP port number used by the remote secondary mail server. The default is 25.	rwme.ini	%1 to %65535
LogFileLinesToReturn	Defines the maximum number lines in a log file that a user can view through the web server. By setting this variable to a positive whole number, N, the web server will return the N most recent entries. By setting this variable to zero, the web server will return the entire log file.	rwme.ini	%0 to %2147483647
ConnectTimeout	Defines the number of seconds to wait for the service provider to answer the modem's call before timing out. This value should be at least two seconds greater than the time out period specified in the modem ini file so that RWME will always wait long enough to receive the no carrier signal from the modem before timing out.	rwme.ini	%3 or greater
ModemPortBitRate	Defines the bit rate to be used by the modem com port. Most North American TAP service providers require this to be 1200. GSM modems use 9600 (8N1) by default.	rwme.ini	%110, %300, %600, %1200, %2400, %4800, %9600,

			%14400, %19200, %38400, %56000, %57600, %115200, %128000, %256000
ModemPortDataBits	Defines the data bits to be used by the modem com port. Most North American TAP service providers require this to be 7. GSM modems use 8 bits by default.	rwme.ini	%5, %6, %7, %8
ModemPortParity	Defines the type of parity to be used by the modem com port. Most North American TAP service providers require this to be even. GSM modems use no parity by default.	rwme.ini	\$even, \$odd, \$none, \$mark, \$space
ModemPortStopBits	Defines the stop bits to be used by the modem com port. Most North American TAP service providers require this to be 1. GSM modems use 1 stop bit by default.	rwme.ini	\$1, \$1.5, \$2
StartupDelay	Defines the number of seconds that RWME should delay before starting up. This can be used to delay until the computer has acquired network access after booting up, so that the first few readings taken by RWME will not result in TCP Connection Errors.	rwme.ini	%0 to %2147483647
IRQTimeBetweenReconnections	Defines the number of milliseconds that RWME should wait between disconnecting from a Real-Time sensor and reconnecting to it. If your Real-Time sensor frequently reports TCP Offline or Timeout errors, then you may be able to reduce these errors by setting this variable's value to 2000 (2 seconds).	rwme.ini	%0 to %2147483647
LoginBackgroundImageFile	Selects the image to use for login screen. If you don't like our supplied images you can add your own image to the Web Images subdirectory and specify its filename. If you set the filename to none it uses a purple colored background.	rwme.ini	\$filename
BackgroundPageColor	Sets the color of web page background. By default it is purple or #8080D8 for hex_color. If you want a blue color use #0040FF for hex_color. You can lookup or test various hex color codes using a search engine.	rwme.ini	\$hex_color
SensorPowerUpDelay	Defines the amount of delay (in seconds) between opening the socket port and the start of communications. If the sensor is powered by RTS/DTR and these lines are not asserted until the socket is opened, then the sensor will need some time to energize before communications will be error free. This is the case when SSD's with older firmware (1.X) are used with Perle or Cyclades TS series device servers. By default, this keyword does not exist in monitoring.ini, and can therefore be assumed to be zero. This setting is sensor specific, meaning that each SSD can have a different value for SensorPowerUpDelay. A value of 0 disables this delay. Use a value of 2 for device servers that drop RTS/DTR between connections.	monitoring.ini	%0 to %2147483647
DeviceDebugEnabled	Controls whether communications between RWME and Sensorsoft device is recorded in a file. Do not keep this setting enabled for long periods of time as it can produce a huge file.	monitoring.ini	#TRUE# or #FALSE#
SMSPDUTruncateLength	Defines the maximum number of characters that are allowed by your GSM mobile service provider when sending SMS messages in PDU mode. This variable is defined so that any message with a length greater	rwme.ini	%1 to %2147483647



	than the maximum limit will be truncated to fit this limit. If an over sized message is sent without truncation, then the message may be rejected entirely by your mobile service provider. By default this variable is set to 30, which means RWME truncates all messages to fit a 30 character limit.		
SMSTextTruncateLength	Defines the maximum number of characters that are allowed by your GSM mobile service provider when sending SMS messages in text mode. This variable is defined so that any message with a length greater than the maximum limit will be truncated to fit this limit. If an over sized message is sent without truncation, then the message may be rejected entirely by your mobile service provider. By default this variable is set to 160, which means RWME truncates all messages to fit a 160 character limit.	rwme.ini	%1 to %2147483647

## Appendix D – Using Dollar Variables in your messages

Dollar (\$) variables can be used in SMS, email and command line alerting actions. During an actual alert the dollar variable is substituted with live data from the monitored item/node. The following are the supported dollar variables:

Variable	RWME 2002 Build 76 and earlier	RWME 2002 Build 94 to Build 150	RWME 2005 Build 200 forward
Location	\$SL	\$L	\$L
Date and Time	\$DT	\$T	\$T
Variable Value or Reading	\$VV	\$R	\$R
Description	\$SD	\$D	\$D
Comments	\$SC	\$C	\$C
Alert Type	\$AD	\$A	\$A
Host:Port	\$IP	\$P	\$P
All Variable Names and Readings	\$AV	\$X	\$X
Variable Name	\$VN	\$V	\$V
Variable Description	Not Supported	Not Supported	\$Z
New Line	\$N	\$N	\$N

RWME Build 94 and forward, continue to support older dollar variables used by RWME Build 76 and earlier.

## Appendix E – Running RWME Pipe Command Lines

As an alternative to interacting with RWME through its web interface, the command line method features built-in support for automating useful and repetitive application specific tasks. These commands may be used to do the following:

- controlling relays (SR6171J, SR6172J, SS6420)
- changing Sensorsoft device variable description/state strings (SS6420)
- schedule the enabling or disabling of alerts
- arm/disarm a security system
- turning ON or OFF beacons, sirens, solenoids or lights
- shutdown or reboot computers
- set alert breach limits

These RWME commands can be used in RWME command line alerting actions and interactively from a command prompt window.



**For an RWME pipe command to function you must have the RWME service running.**

To run RWME pipe commands, interactively, from a command prompt window you must be logged in as the Windows administrator on the machine where RWME is installed and running as a service. To run RWME pipe commands as alerting actions the Windows service can be logged in with LocalSystem (default) credentials or with network administrator credentials as described in *Appendix H - Configuring the RWME Service to Log on with an Administrative Account*.

### Writing to a Sensorsoft device variable

To write to a Sensorsoft device variable, the variable inside the device must have write capability. Attempting to write to a read-only variable would return an error on the command line. You can determine if a Sensorsoft device variable has write-capability, by going to its Device details page, scrolling down to the heading Device Readings and clicking View Tech Variables. A variable with write-capability will always have a link entitled, Modify Variable Value. In order to write to a variable, you must first setup RWME to monitor the device (see section *Monitoring a Sensorsoft device*). The following shows the command line syntax for writing to a Sensorsoft device variable:

```
<RWME Dir>\rwme.exe -writevar <Host:Port> <Variable Index> <Variable Data>
```

where;

<**RWME Dir**> the full path of the directory where RWME has been installed.

<**Host:Port**> is the IP address or host name used by RWME to access the device and the port number. This must exactly match the text in the Monitor List page from the Host:Port column.

<**Variable Index**> is the target device's variable index. To determine the variable index of the target variable, open the **Device Details** page of the target device, scroll to the section **Device Readings**, and then locate the column **Variable Index**.

<**Variable Data**> is the data to write to the target variable. If the target variable is type Boolean, then <Variable Data> must be either 1 or 0. If the target variable is of type string or text, then <Variable Data> must be enclosed in double quotes.

The `-set` argument has been deprecated in RWME 2020 Build 694, however it still works the same as the `-writevar` argument shown above.

## Disable and enable alerts

This section describes how to disable and enable alerts through command lines as an alternative to the web interface. A practical usage of this functionality is where the user wants to disable alerts for a whole group of monitored items/nodes, to prevent false alarms and later re-enable the alerts.

This command line syntax is for disabling an alert:

```
<RWME Dir>\rwme.exe -alertoff <Host:Port> <Variable Index> <Alert Code>
```

This command line syntax is for enabling an alert:

```
<RWME Dir>\rwme.exe -alerton <Host:Port> <Variable Index> <Alert Code>
```

where;

<**RWME Dir**> the full path of the directory where RWME has been installed.

<**Host:Port**> is the IP address or host name used by RWME to access the device and the port number. This must exactly match the text in the Monitor List page from the Host:Port column.

<**Variable Index**> is the target variable index. To determine the variable index of the target variable, open the **Details** page of the target item/node, scroll to the section **Readings**, and then locate the column **Variable Index**.

<**Alert Code**> is the alert state code. It must be one of the following two letter codes:

CH	Critical High
WH	Warning High
WL	Warning Low
CL	Critical Low
BC	Boolean Critical
RN	Return to Normal

## Set Alert Breach Limits

This section describes how to set alert breach limits through command lines as an alternative to the web interface. This command line syntax is as follows:

```
<RWME Dir>\rwme.exe -setlimit <Host:Port> <Variable Index> <Alert Code> <Breach Limit>
```

where;

**<RWME Dir>** the full path of the directory where RWME has been installed.

**<Host:Port>** is the IP address or host name used by RWME to access the device and the port number. This must exactly match the text in the Monitor List page from the Host:Port column.

**<Variable Index>** is the target variable index. To determine the variable index of the target variable, open the **Details** page of the target item/node, scroll to the section **Readings**, and then locate the column **Variable Index**.

**<Alert Code>** is the alert state code. It must be one of the following two letter codes:

CH	Critical High
WH	Warning High
WL	Warning Low
CL	Critical Low
BC	Boolean Critical
RN	Return to Normal

**<Breach Limit>** must be an integer number. Use 0 or 1 for a Boolean value.

## Controlling a relay contact

The following is a practical example of writing to a Sensorsoft device for controlling an access door solenoid or switching a warning lamp.

This command example turns ON relay1 in a SS6420:

```
"C:\Program Files\Sensorsoft\Remote Watchman Enterprise 2020\rwme.exe"  
-writevar 127.0.0.1:3001 77 1
```

This command example turns OFF relay1 in a SS6420:

```
"C:\Program Files\Sensorsoft\Remote Watchman Enterprise 2020\rwme.exe"  
-writevar 127.0.0.1:3001 77 0
```

If you are using the Sensorsoft SS6420, then **<Variable Index>** is 77 for RELAY1, and is 81 for RELAY2. If you are using the Sensorsoft SR6171 or SR6172J, the **<Variable Index>** is 1.

## Running RWME commands in alerting actions

To have RWME execute a command in an alert action, you can use a single command line inside an RWME Address Book Command line. If you need several commands executed at the same

time you can include these commands in a batch file and call the batch file from the RWME Address Book Command line.



**NEW in RWME 2020** – We have created a shortcut to the `rwme.exe` executable called `RWME_EXE_shortcut` in the User Executables subdirectory. You can reference this shortcut without including the full RWME executable path. This can be done in command lines that you create within RWME's Address Book.

For security reasons a batch (.bat) file must be located in the **User Executables** subdirectory. Command lines in the batch file must reference the full RWME executable path and do so with double quotes as shown below:

```
@echo off
"C:\Program Files\Sensorsoft\Remote Watchman Enterprise 2020\rwme.exe"
-writevar 172.17.0.12:3001 77 1
"C:\Program Files\Sensorsoft\Remote Watchman Enterprise 2020\rwme.exe"
-alertoff 172.17.0.12:3005 1 WH
"C:\Program Files\Sensorsoft\Remote Watchman Enterprise 2020\rwme.exe"
-writevar 172.17.0.12:3001 77 0
```

### Exit codes used by RWME

A successful RWME command exits with 0 and fails with -1.

## Appendix F – Running RWME command from Smart phone web browser

The smart phone is a preferred choice for controlling modern IT systems where mobility is a must. Many of the RWME commands you run automatically as an alert or pipe command can also be run from a smart phone web browser. This method should only be used on a private WiFi network that you know is safe and secure. Do not use this method over public networks as our software does not use encryption.

This procedure will setup login and run command bookmarks on your Smart phone:

1. On your Smart phone web browser type in the RWME URL in its address bar †:

`http://encourager/RWME`

2. When the RWME login page is displayed login with the admin username and password.
3. When the browser asks to remember the login, answer Yes or Remember ††
4. Once you see the Monitor List, choose to bookmark this page and name it:

**RWME – encourager – Login**

5. Tap the Address Book link as in Figure 16.



Figure 16: Smart phone screen with Address Book link shown

6. Tap the RWME command line name you want to add as in Figure 17.

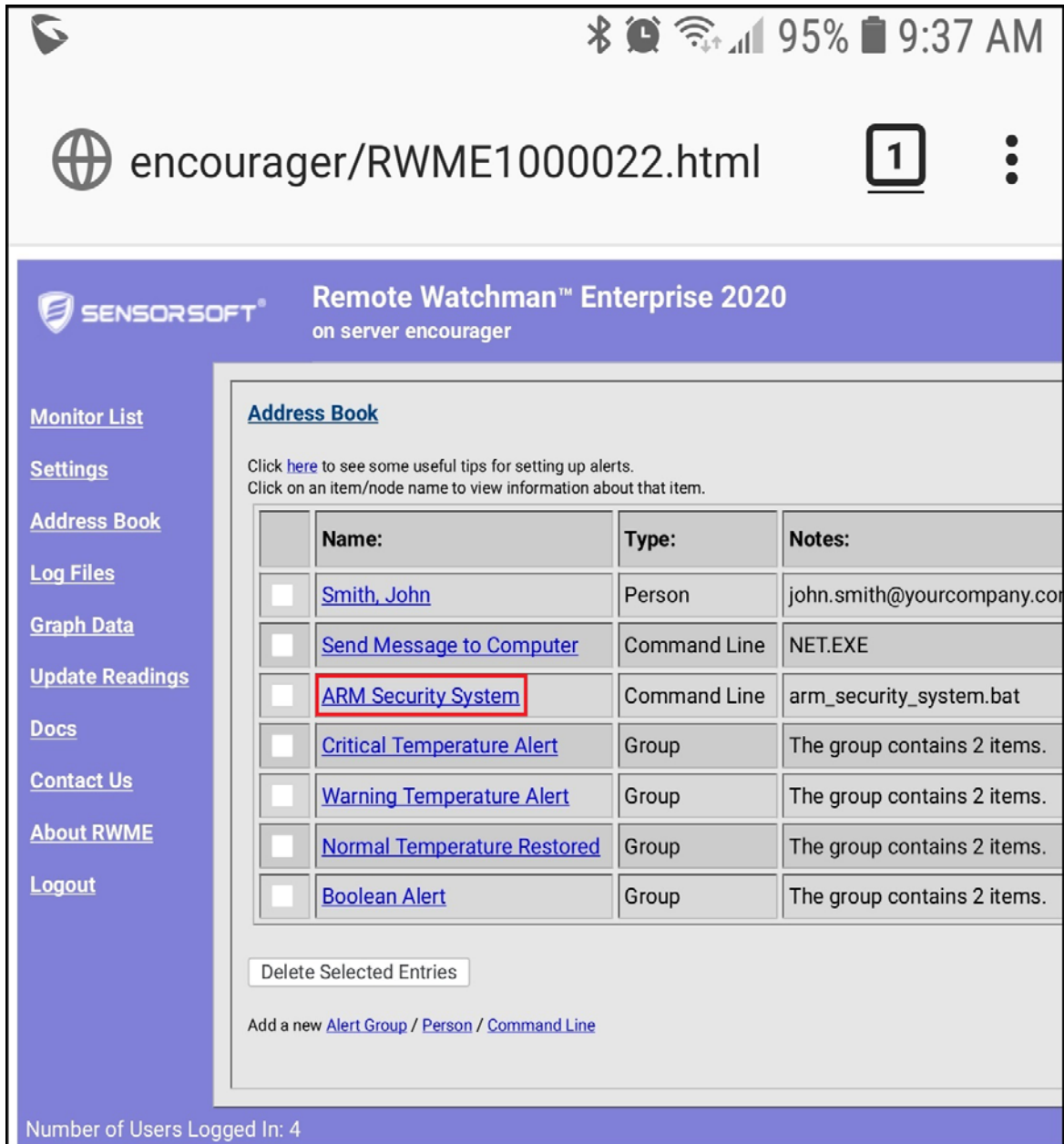


Figure 17: Smart phone screen with Command Line link shown

7. Hold your finger over the link Test this Command Line as in Figure 18 until it offers an option to copy the link/address.



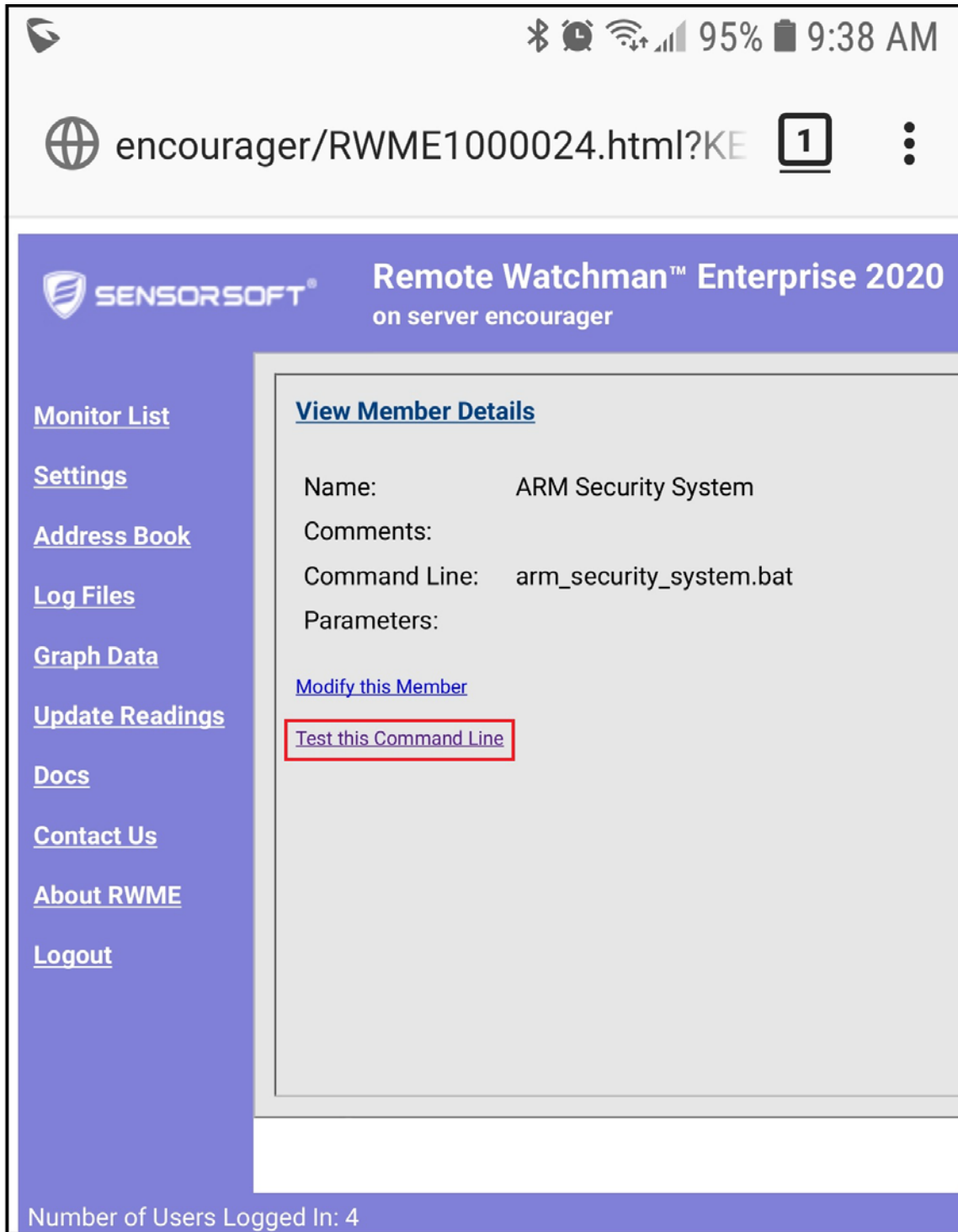


Figure 18: Smart phone screen with Test this Command Line link shown

8. Copy the address or link into your clipboard.
9. Paste this link into a new browser window and save it as another bookmark with a name similar to: **RWME – encourager – Command: Arm Security System**

10. You should now have two bookmarks on your smart phone, one to login to RWME and another to run a command. Test both, to verify that they work as expected.

† You can use a domain name or IP address in the URL. In cases where a web server port other than the default of 80 is used you will also have to include the alternate port number. The following example shows use of IP address and alternate port number:

`http://192.168.0.12:8090/RWME`

†† As an alternative to being prompted by web browser to recall saved login details you can use a more direct method to login as the URL example below:

`http://rwmehostname/RWME1000001.html?Username=admin&Password=mypassword`

Be sure to substitute `mypassword` with the actual admin password.

## Appendix G – Using XML Output to share live data with other software Applications

### Accessing the XML page

This section describes how to use the XML output capability of RWME to share live data with other software applications.

To view the XML page, login to RWME as **ruser** or **admin**. From the Monitor List page, click the link **View XML**. This will open a new web browser window containing the XML page.

An XML schema (XSD) page is also available. The XML schema defines the XML's hierarchy and data types. The schema file is used by automated readers to validate the XML output. Once you are logged into RWME you can access the XML schema (XSD) page using the following URL:

```
http://<RWME_ServerAddress>/RWME1000001.xsd
```

To access the XML page from another software application:

1. Send the following HTTP GET request to RWME's web server port:

```
GET /RWME1000001.html?Username=ruser&Password=<password> HTTP/1.1
```

Replace **<password>** string with RWME's ruser password.

2. RWME will then respond with the following headers:

```
HTTP/1.1 302 Redirect
Server: Sensorsoft-Remote-Watchman-Enterprise/1.0
Allow: GET,POST
Content-Length: 0
Set-Cookie: sessionID=<SessionIDValue>
Content-Type: text/html
Location: /RWME1000001.html
```

3. Your application is now logged in. **<SessionIDValue>** is the session cookie passed back from the web server. Your application must remember the **<SessionIDValue>** string.
4. To request the XML page, send the following HTTP GET request:

```
GET /RWME1000001.xml HTTP/1.1
Cookie: sessionID=<SessionIDValue>
```

Replace **<SessionIDValue>** string with the value you remembered in step 3. The web server in response will then send the XML page to your application.

## XML data organization

This following tree diagram illustrates how data is organized in the XML page:

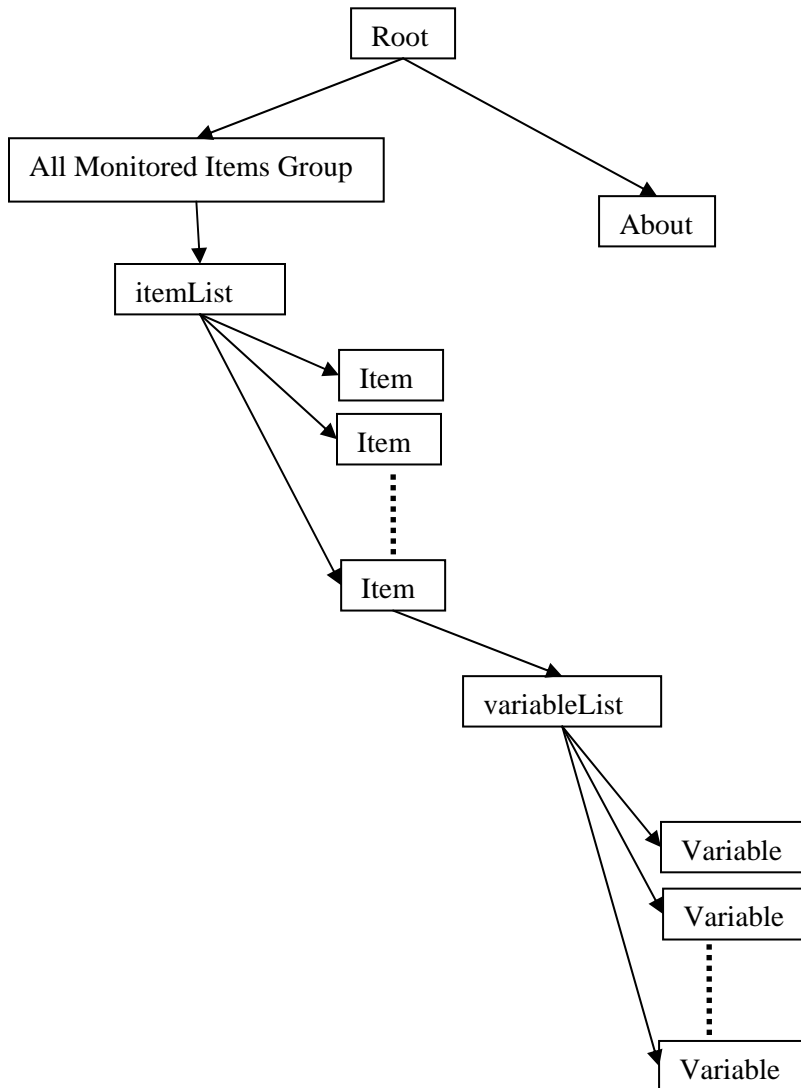


Figure 19: Organization of XML page output

Data pertaining to each monitored item/node is located in a separate **Item** sub-tree under `\root\group\itemList\`. Each **Item** sub-tree has a **variableList** sub-tree that contains the item/node's variable information. The data for each monitored variable is located in a separate **Variable** sub-tree under **variableList**. Please note that only variables that are shown on the **Monitor List** page will be listed under **variableList**. To select which item/node variables are to be shown on the Monitor List page, please refer to the section *Selecting Variables to Display on the Monitor List*.

## Appendix H – List of Breach Conditions and Device Errors that can be used to generate alerts

Event Type	Description
Breach of Warning Limit	This is generated when the device's reading moves to or beyond the limits specified, but stays inside the limits specified for the Breach of Critical Limits. These alerts are related to devices that contain scalar variables (e.g. temperature or humidity).
Breach of Boolean Limit	This is generated when the item/node's reading changes to the Boolean value that is designated as actionable. These alerts are related to items/nodes that contain Boolean variables (e.g. WET/DRY, ON/OFF, UP/DOWN).
Breach of Critical Limit	This is generated when the device's reading moves to or beyond the limits specified. These alerts are related to devices that contain scalar variables (e.g. temperature or humidity).
Non-Alert State Restored	This is generated when the device's reading is back to normal after breaching a limit.
Device Model Changed	This is generated when the model number of the monitored SSD changes between readings. You may want to use these alerts to notify you if someone switches devices. For example, let's say that you are monitoring two SSD's, a temperature device and a humidity meter. If someone were to come along and swap these two devices, you would no longer receive alerts for high or low temperature or humidity readings for either device, because all of the alerts are bound to the original configuration. If you were to receive a device model changed alert, you would have an opportunity to correct the situation.
COMM Corrupted	This is generated when RWME receives corrupted or unexpected data from a device during polling. If you are receiving numerous alerts, of this type, it can be an indication that there is a physical problem with the device or its cabling.
TIMEOUT - Device not responding	This is generated when RWME can establish a TCP connection with the remote host, but the device is not responding to commands. This can be an indication that there is a physical problem with the device, its cabling or an incorrect bit rate setting of the device server.
OFFLINE - TCP connection problem	This is generated when RWME cannot establish a TCP connection with the remote host or device or the connection was interrupted.
ONLINE - TCP connection restored	This is generated when RWME has been able to establish a TCP connection with the remote host, after issuing an OFFLINE alert. This alert is issued only once after returning from an OFFLINE alert state.
EEPROM Failure	This is generated when the device cannot read from its internal EEPROM memory. This indicates that the device has physical damage and should be repaired.
LOW SUPPLY VOLTAGE	This is generated when the device does not have enough voltage to ensure proper, uninterrupted operation. This can be an indication that the serial port that is powering the device does not have enough output voltage for proper operation.
TAMPER	This is generated when the device cannot read its sensing element or its enclosure is opened. This could be an indication that the probe or sensing element is damaged.

## Appendix J – Configuring the RWME Service to Log on with Administrative Account

To have RWME execute command lines that require administrative access to the network, for example to perform a remote shutdown of a machine, you must first configure its Windows service to log on with an administrative user account. The instructions below are based on RWME installed on a Windows 2000 domain controller or a workstation with domain access to the network. Note that for various Windows operating systems the way you select the administrative account will differ.

1. From the Windows Start button, choose Settings – Control Panel – Administrative Tools – Services.
2. Select the service named **Sensorsoft RWME 2020**.
3. Select **Action->Properties**. This will open the **Service Properties** window.
4. Click the **Log On** tab.

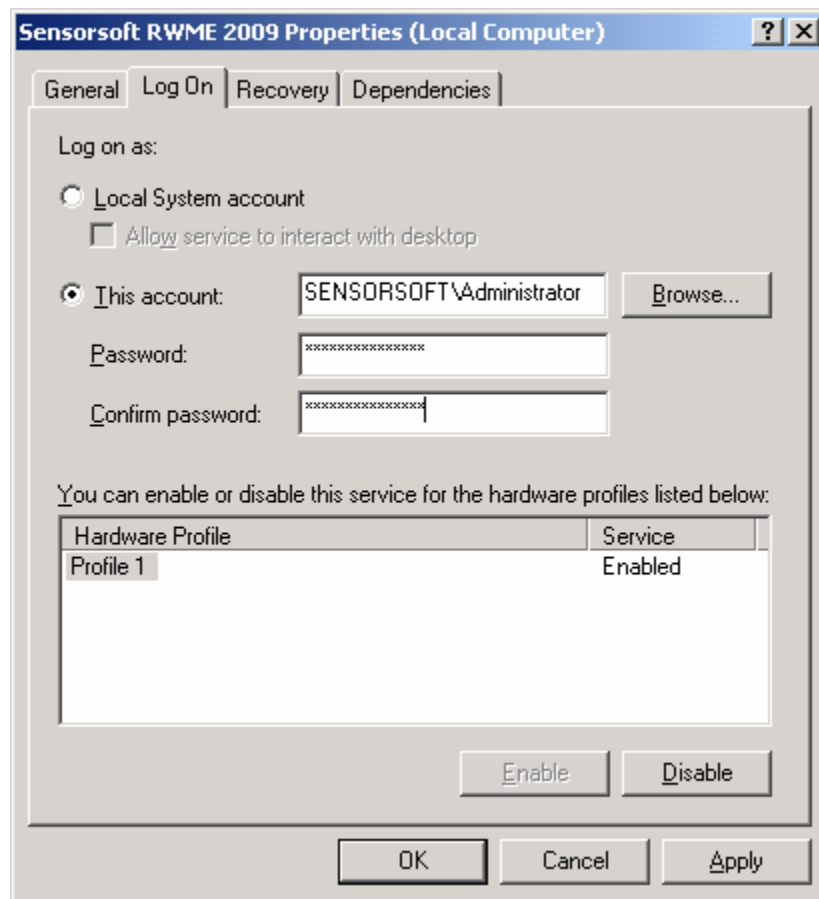


Figure 20: Log On Tab of Service Properties

5. Under the section “**Log on as:**”, select **This account**, and click the **Browse** or **Choose User** button. This will open the **Select User** window.

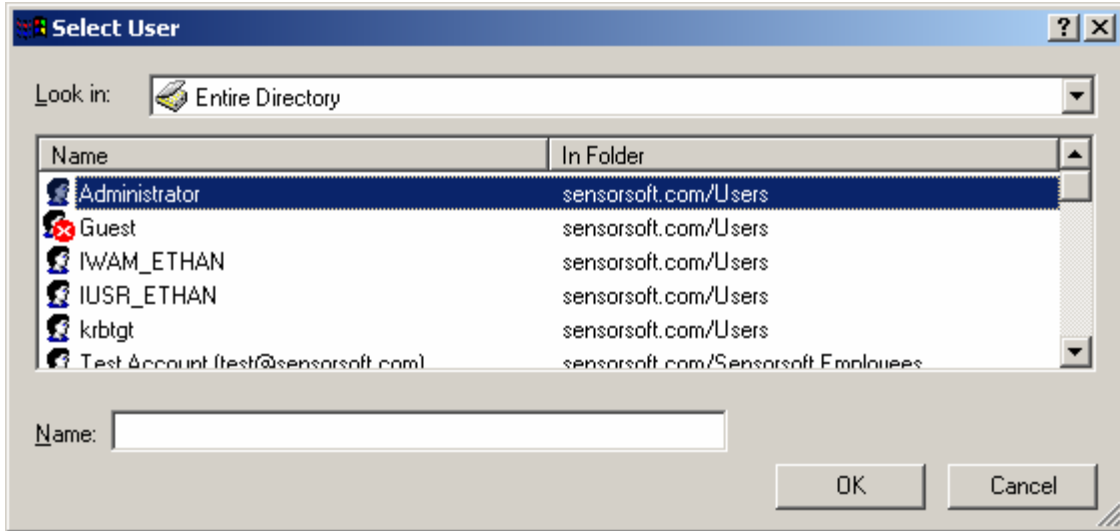


Figure 21: Selecting User for Log On

6. In the **Look in** selection box, choose **Entire Directory**. This will list all of the accounts on your network.
7. From the list of accounts, choose one with network administrative privilege (i.e. Administrator), and click **OK**.
8. In the Service Properties window, enter the password of the account you have selected. Click **OK**.
9. Restart the RWME service (see section *Starting and Stopping RMWE*).