

# **MINUTE MAN<sup>®</sup>**

**Power Technologies**

---

*From Para Systems, Inc.*

## **SSL-Manager**

(SNMP-SSL Management Software)



## **User's Manual**

## Table of Contents

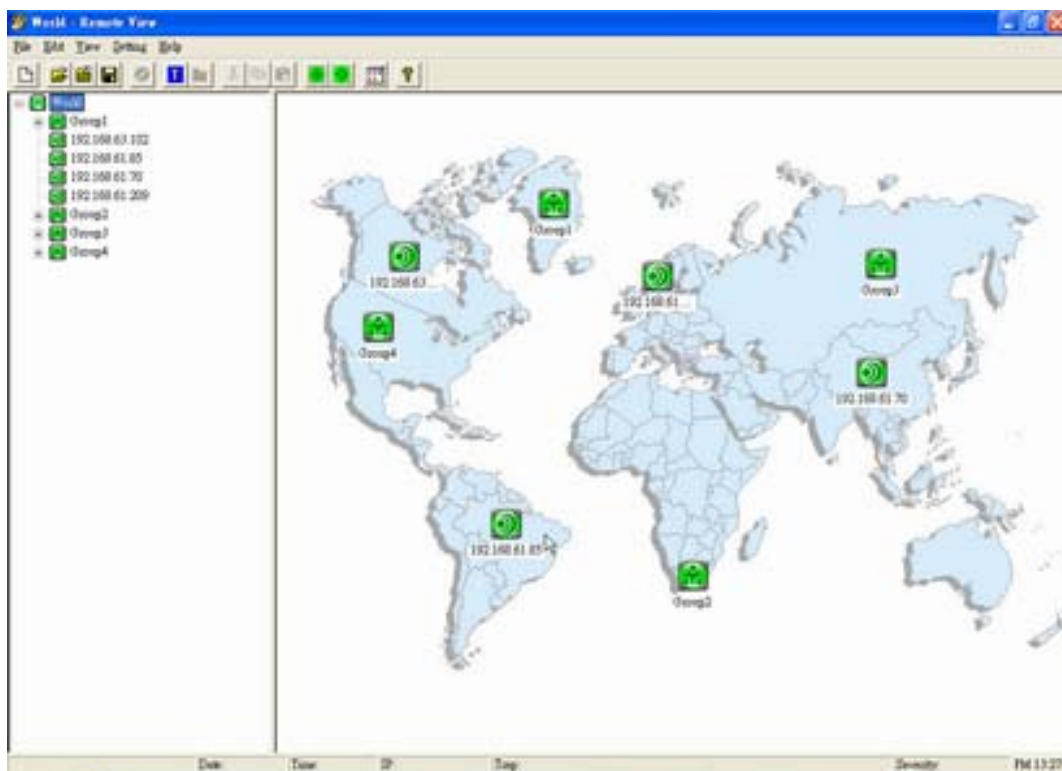
Chapter 1 Introduction .....	3
Chapter 2 Installation .....	4
Chapter 3 SSL-Manager Menus .....	8
Chapter 4 Setup .....	11
Chapter 5 Operation .....	18
Chapter 6 Upgrading the SNMP-SSL card .....	21
Chapter 7 Batch Configuration.....	22
Obtaining Technical Assistance .....	23
Limited Product Warranty .....	24

## Chapter 1 Introduction

SSL-Manager is an application running under Windows NT4.0/2000/XP/2003/Vista, used for monitoring the device equipped with an SNMP-SSL card on the Internet through SNMP protocol. The SSL-Manager supports HTTPS when monitoring the SNMP-SSL card's web pages for enhanced security. Before using the SSL-Manager install the SNMP protocol and start the SNMP service in your system. SSL-Manager can manage up to 3000 devices simultaneously and the hierarchy structure can have up to 8 levels.

The SSL-Manager is client software running on NMS (Network Management System). Users are provided with a Tree-View on the left hand side and a List-View (Icon style and Report style) on the right hand side to monitor the device in this software. When an event occurs, the icon will change colors according to the severity level, sending email to the address which has been set in E-mail Configuration window, calling a cell phone number which has been set in Short Message Service Configuration window.

**Note:** The SSL-Manager software only supports the SNMP-SSL card configured for SNMPv3. The SSL-Manager software does not support SNMPv1. See the SNMP-SSL User's Manual section "SNMP-SSL Control" for configuring the SNMP-SSL card for SNMPv3.



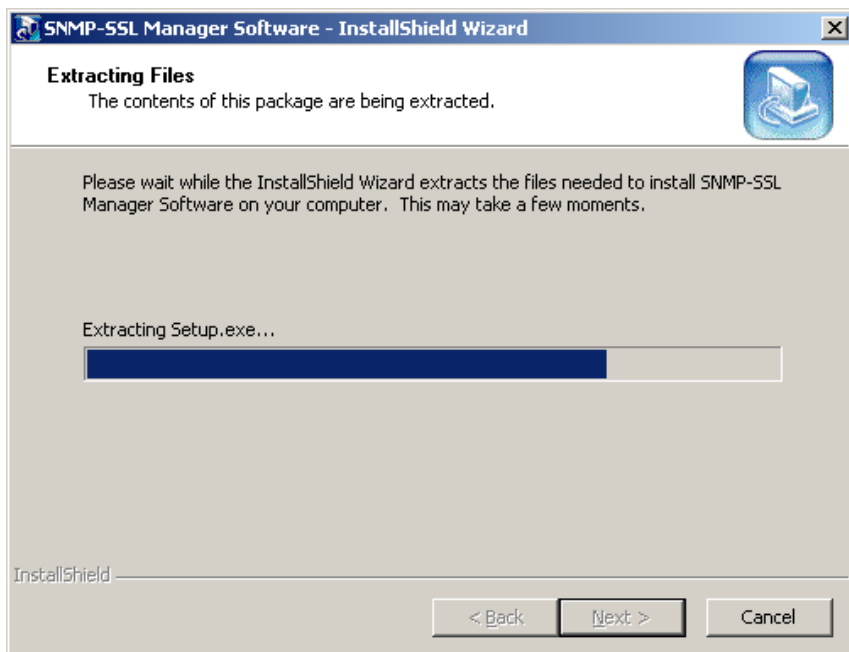
## Chapter 2 Installation

The SSL-Manager is quick and easy to install. The InstallShield Wizard will guide you through the installation.

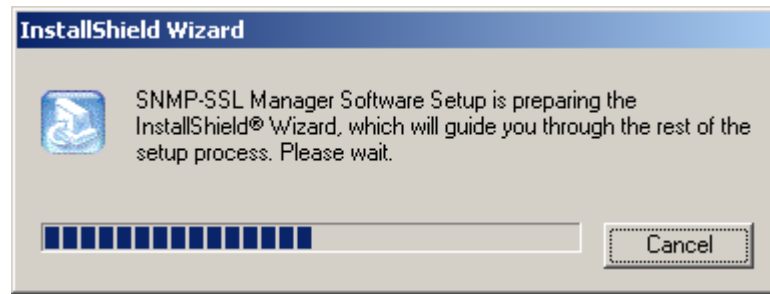
1. Insert the SNMP-SSL CD ROM into the CD ROM drive.
2. Run the SNMP-SSL Manager.exe.
3. Select Next to start the installation.



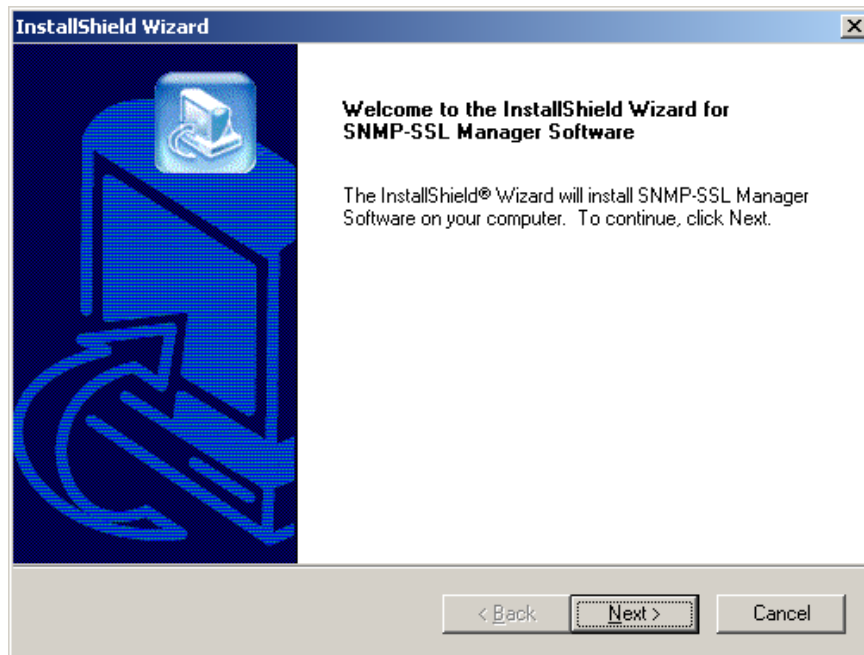
4. The files are being extracted.



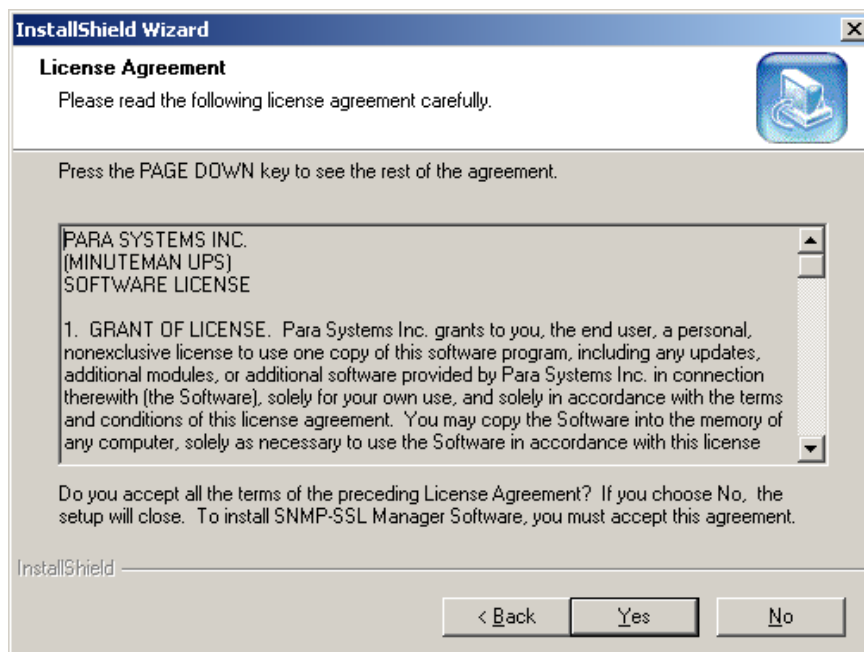
5. The setup of the InstallShield Wizard is in process.



6. The InstallShield Wizard is ready to complete the installation. Select Next to continue.

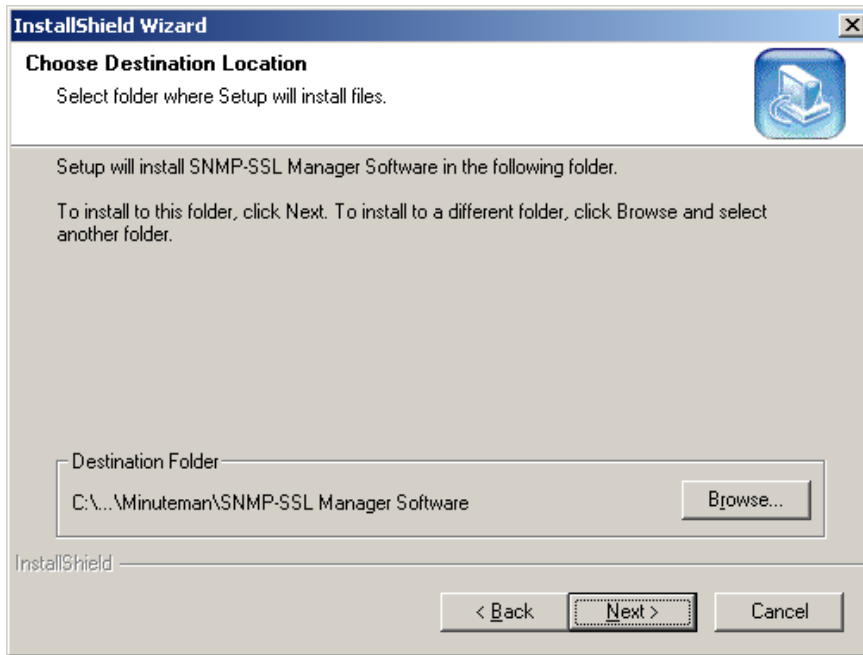


7. Please read the entire License Agreement and if you agree with the terms select Yes to continue.

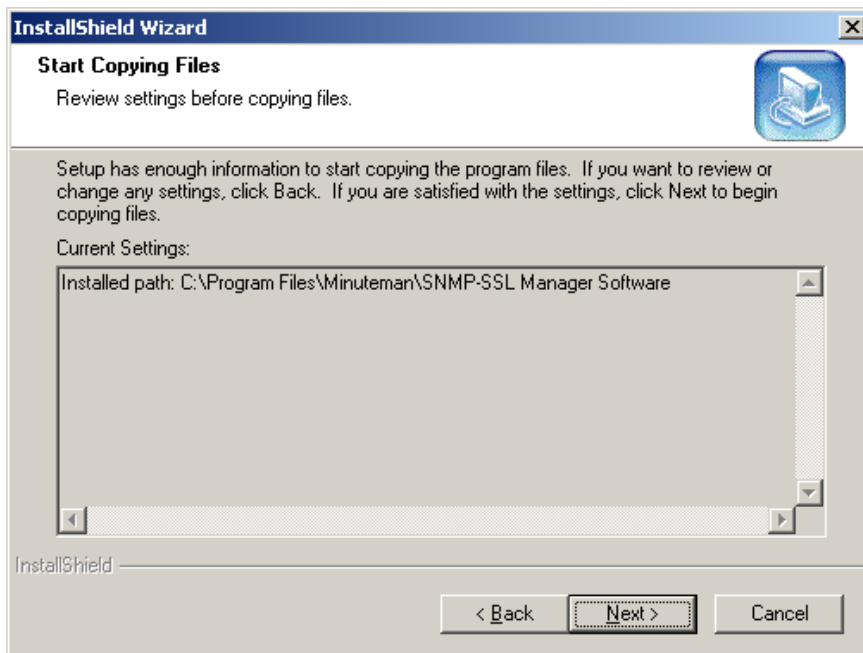


## SNMP-SSL

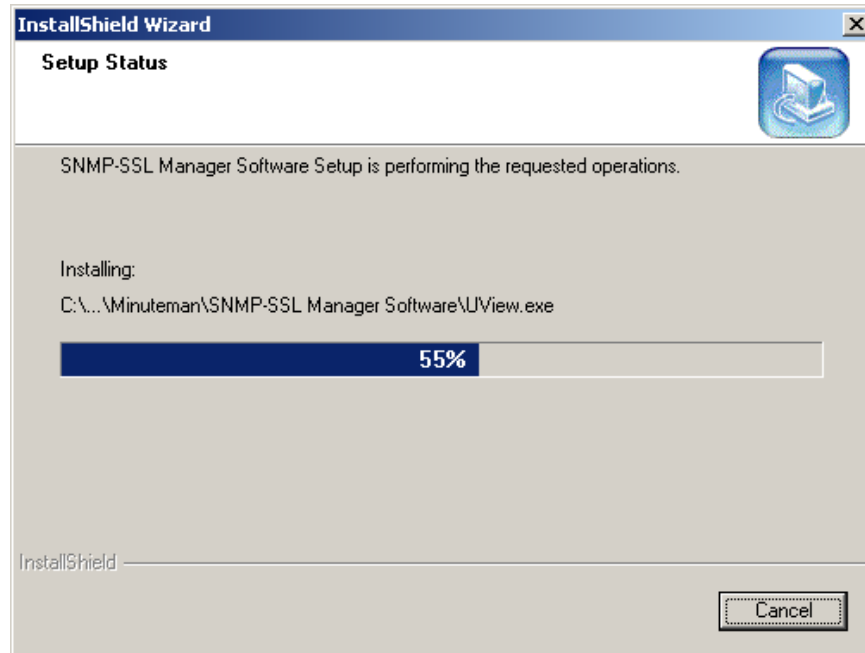
8. Select the desired location for the files by using the Browse button or use the default location. Select Next to continue.



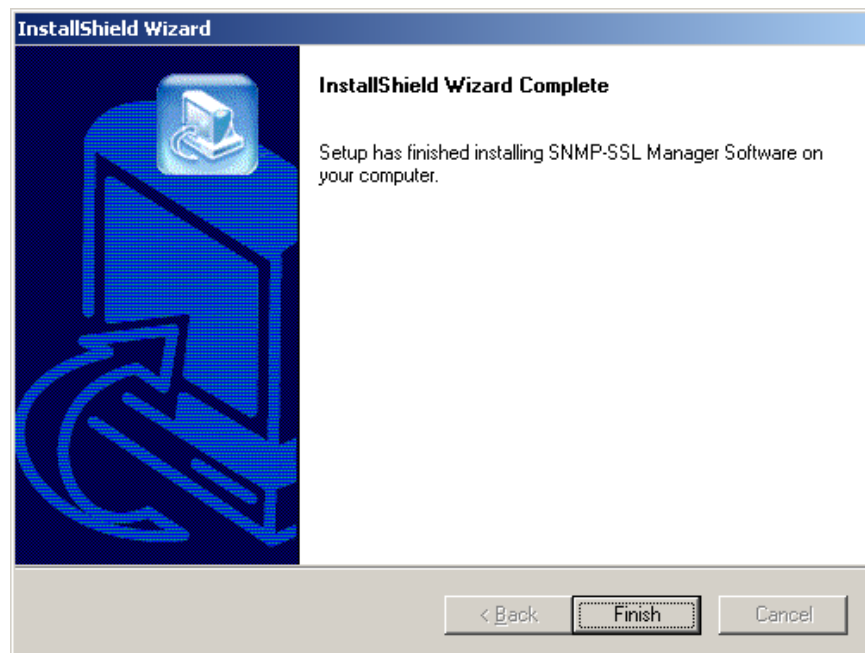
9. The InstallShield Wizard is coping the files to the selected location. Select Next to continue.



10. This screen shows the status of the setup. Any time during the installation if you choose not to complete the installation select Cancel.

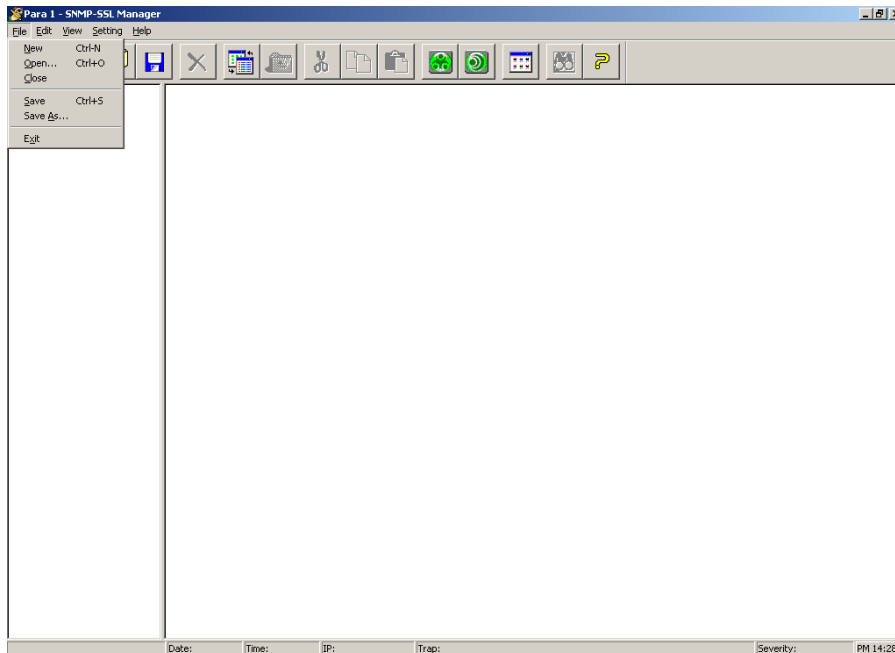


11. The Installation is complete, select Finish.



## Chapter 3 SSL-Manager Menus

Select the Start button in the system tray, then programs, then SNMP-SSL Manager and then Run SNMP-SSL Manager. The main screen of the SSL-Manager will be displayed. This chapter describes the Menu Options.



### 1. File:

- a. New: When selected a new map file is created. You can add groups, devices, and customize for your application.
- b. Open: Open an existing map file.

**Note:** The map file can only be opened by SSL-Manager.

- c. Close: Close the window. The program is still running. Right click on the Icon in the right hand side system tray to reopen the program.
- d. Save: Save new files and save the changes to existing files. If saving a new file, a standard file-save dialog box will popup, input file name, and the file will be saved. If the file already exists the changes will be saved.
- e. Save As: Save a file as another file name. When selected a standard file-save-as dialog will popup, input file name, and the file will be saved.
- f. Exit: Exit the program. If you have created a new map file or made changes to the existing map file, before the program closes, you will have the option to save or not save the changes.



**2. Edit:**

- a. Copy Device: This command and the Paste command allow you to copy and paste one or more devices from one group to another group.
- b. Cut Device: This is a standard Copy and Paste command. Cut a device from one group and paste it in another group.
- c. Paste: This is a standard Paste command. If you have executed the cut or the copy command, click the main menu or right click in the List-View window, and then paste the device.
- d. Delete: This is a standard Delete command. Before using this command, select a group or device in List-View window. You can use this command from the main menu or right click on the group or device icon in the Tree-View or List-View.
- e. Rename: This is a standard Rename command. You can rename a group or device. Select a group or a device icon, click the main menu or right click on the icon in the List-View window and then you can change the group or device name.

**Note:** The maximum character length is 16.

- f. Add Group: This command will allow you to add a new group to the List-View window. Default name is "Group1", you can change it by the "Rename" command.
- g. Add Device: This command will allow you to add a device. Select "Discovery" to search for the device. Select a device in list then select "Add", the device will be added to the List-View window.

**Note:** The maximum depth of the tree structure is 8.

**3. View:**

- a. Toolbar: The Toolbar's function is identical to that of main menu except the "Jump to parent group" command. The "Jump to parent group" command is used to return to the upper tree level of the map file.
- b. Status Bar: The Status bar is used to show the device's IP address, date, time, severity and the description of the trap once the event has occurred.
- c. Icon Style: Displays the device or group's icon in List-View window (right hand side).
- d. Report Style: Displays the devices in table format.
- e. Arrange Icon: Arranges the icons in List-View window.
- f. Browse: Select a device and then select Browse. This will open the default browser to view the SNMP card's web pages.
- g. Trap Log: This function allows you to view the trap logs for all of the devices. You can also search a specific device's trap log by right clicking on the device's icon and select "Trap History".

### 4. Setting:

- a. Background color: This command is used to set the background color of the List-View window. The color can be saved to the map file. The default background color of the List-View window is white.
- b. Cancel Background Color: This command is used to set the window's background color to the default color (white).
- c. Background Image: You can use this command to set the background image of List-View window. The setting can be saved to the map file.

**Note:** The Background image is saved in the map file. If the image file is moved to another directory, it will not be shown in List-View window.

- d. Cancel Background Image: This command is used to cancel the window's background image.
- e. Autoload Map: Select this setting and the last map file saved will be used when the program is restarted.
- f. e-Mail: This allows you to send and receive notifications of events via email. Select "Authentication", if the mail server requires authentication.
- g. Short Message Service: This allows you to send and receive notifications of events via phone. Connect a GSM modem to the Com port on the SNMP-SSL card. The maximum number of phones that can be notified is 8.
- h. Upgrade File: This allows you to upgrade the SNMP-SSL card's firmware.
- i. Set Discover IP Table: Set the IP Range for all of the SNMP-SSL cards in the LAN.

### 5. Help:

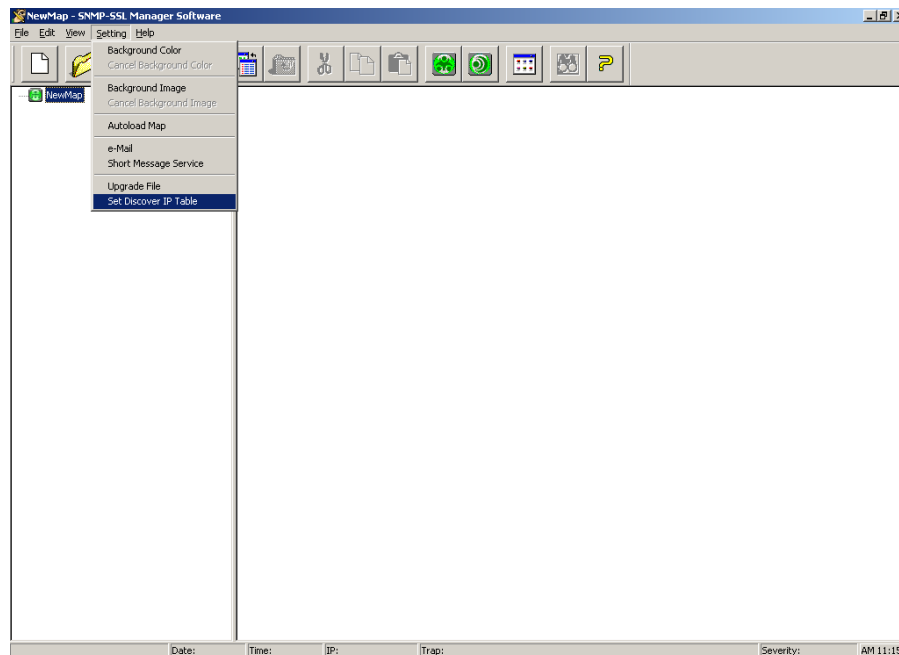
- a. Content: This opens the Help file.
- b. Status Legend: This shows the color associated with the severity level of the events. Severity levels are from high to low.
- c. Registration: The default number of devices that the SSL-Manager will support is 25. Registering the software will allow you to receive a Key Code to upgrade the Device Limit to 3000 devices. Select Register and complete the registration form. Shortly you will receive the Key Code (via email) to upgrade the Device Limit.
- d. Enter Key: Enter the information and select Apply. The Device Limit will be upgraded to 3000 devices.
- e. About SSL-Manager: Shows the version of SSL-Manager and the Device Limit.

## Chapter 4 Setup

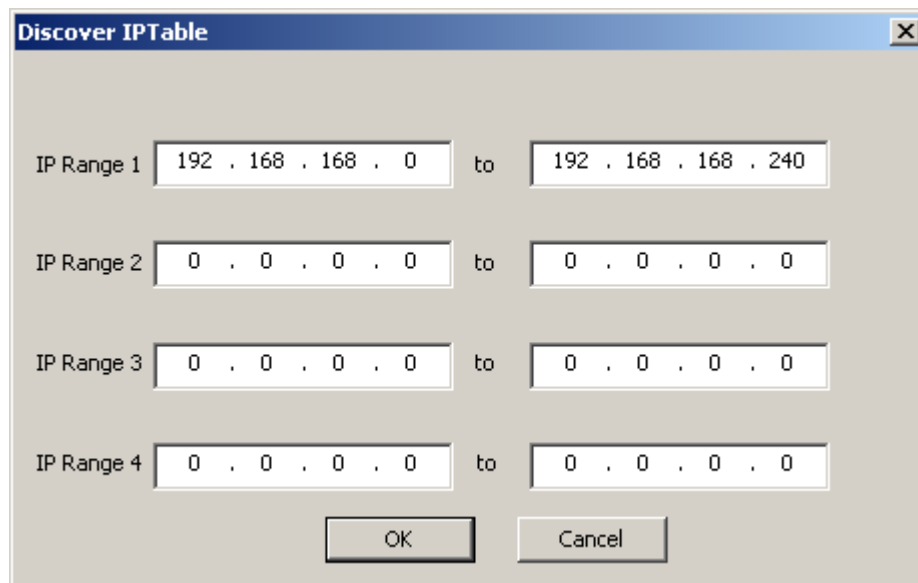
This chapter will guide you through the Setup of the SSL-Manager.

**Note:** The SSL-Manager software only supports the SNMP-SSL card configured for SNMPv3. The SSL-Manager software does not support SNMPv1. See the SNMP-SSL User's Manual section "SNMP-SSL Control" for configuring the SNMP-SSL card for SNMPv3.

1. Open the SSL-Manager program. Under Setting open Set Discover IP Table.

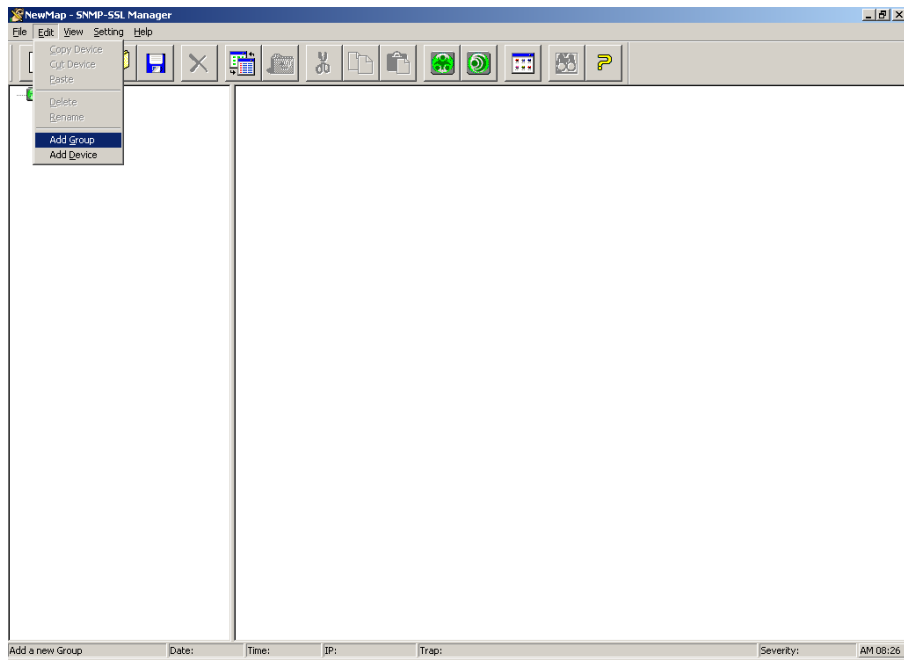


2. Set the IP Range for all of the SNMP-SSL cards in the LAN.

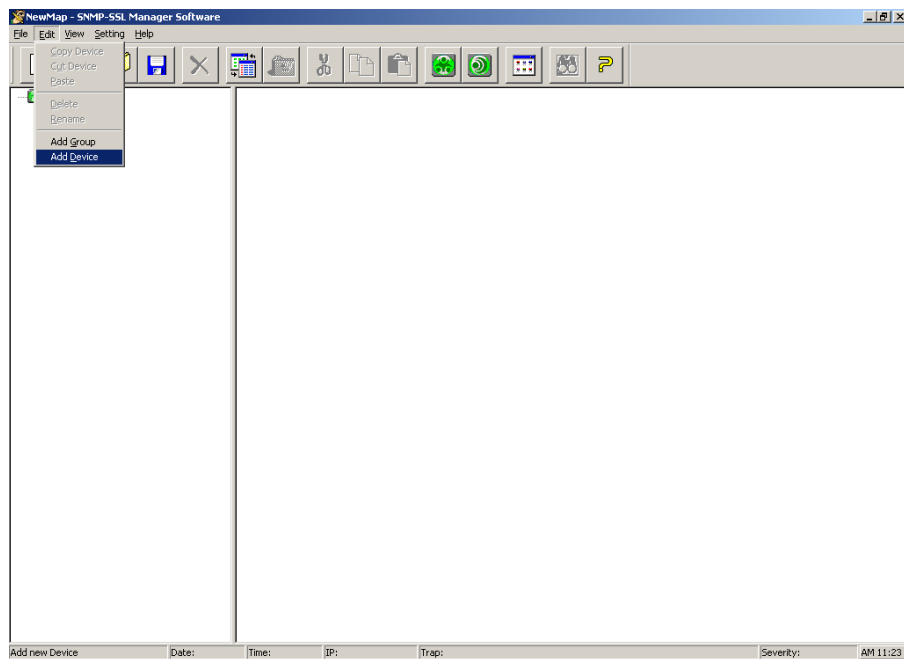


## SNMP-SSL

3. Under Edit open Add Group. This command will add a new group to the Tree-View window on the left hand side. The default name is "Group1". The default name can be changed by the "Rename" command. You can setup different groups for different locations.

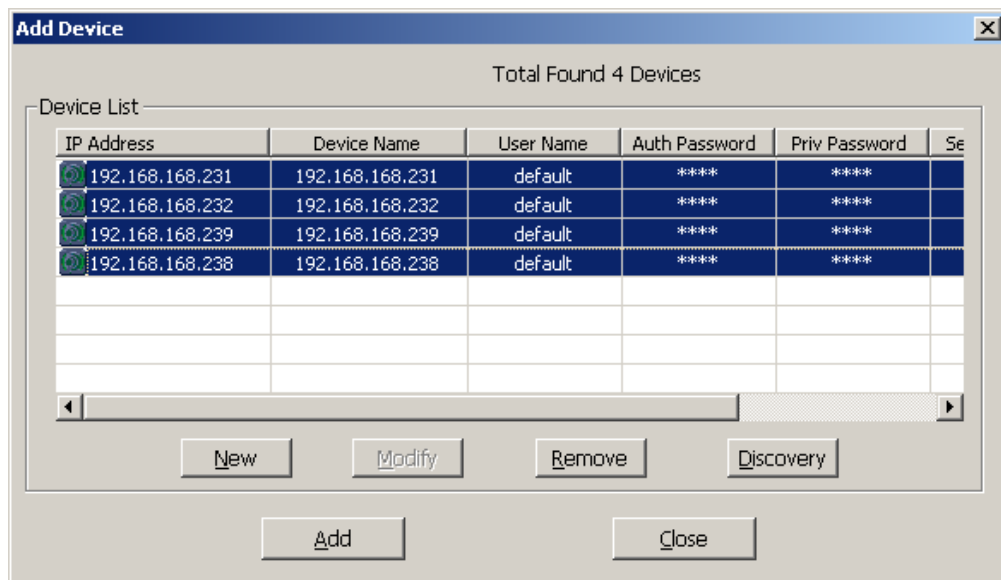


4. Select the New Group and then under Edit open Add Device.

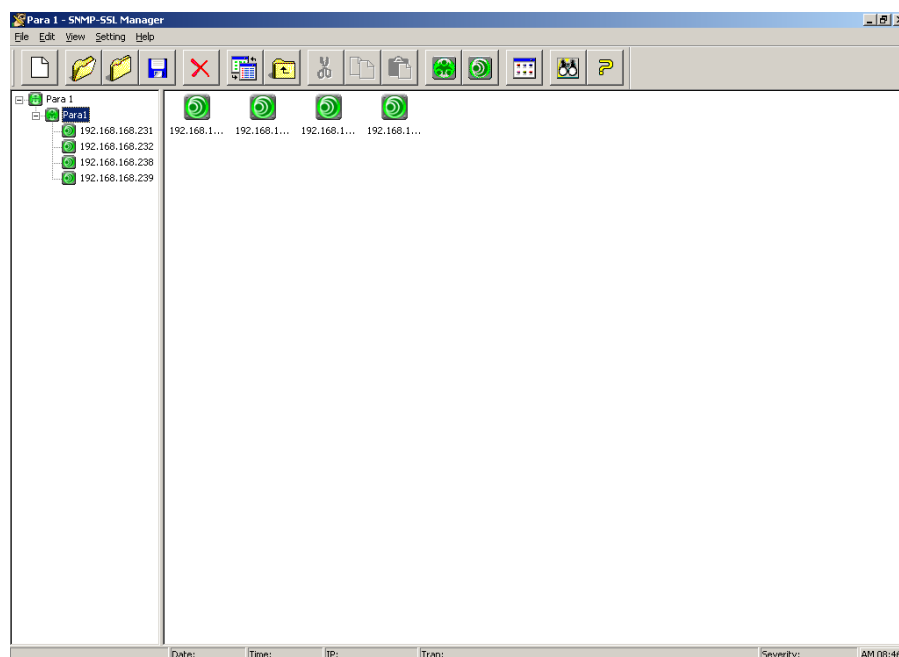


- Select "Discovery" to search for the devices on the LAN. The devices information will be shown in the list. The "Modify" button is for editing the information. The "New" button is for adding a new device to the list. The "Remove" button is for removing a device from the list. Select a device in list then select "Add", device will be added to the Tree-View and the List-View windows. Select the desired devices to add to a specific group.

**Note:** You must input the devices correct R-community and W-community or the device cannot be added. If the Trap Receiver table is full, SSL-Manager will pop-up a warning message that the device cannot be added.

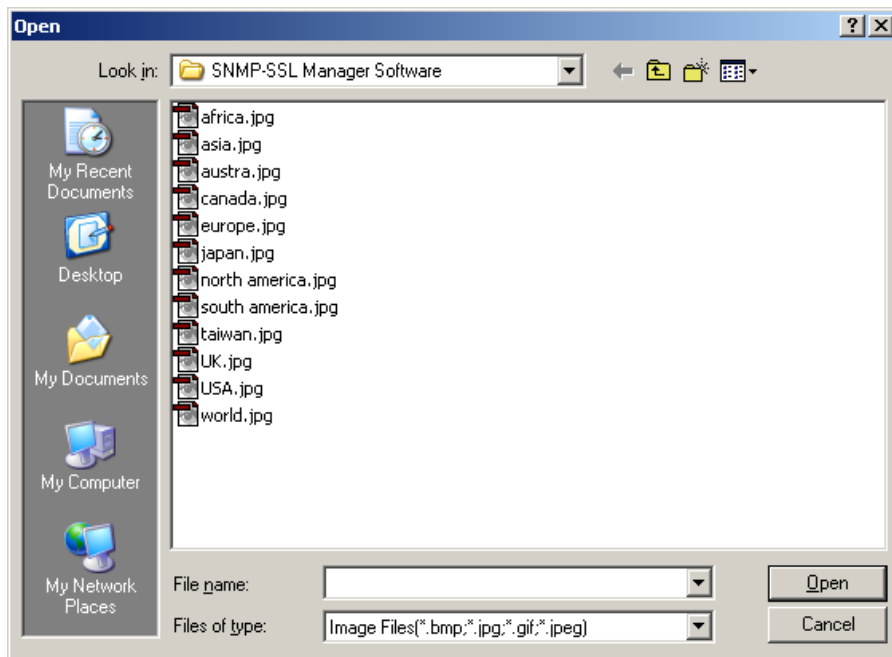


- The devices have been added to the Tree-View (left hand side) and the List-View (right hand side) window.

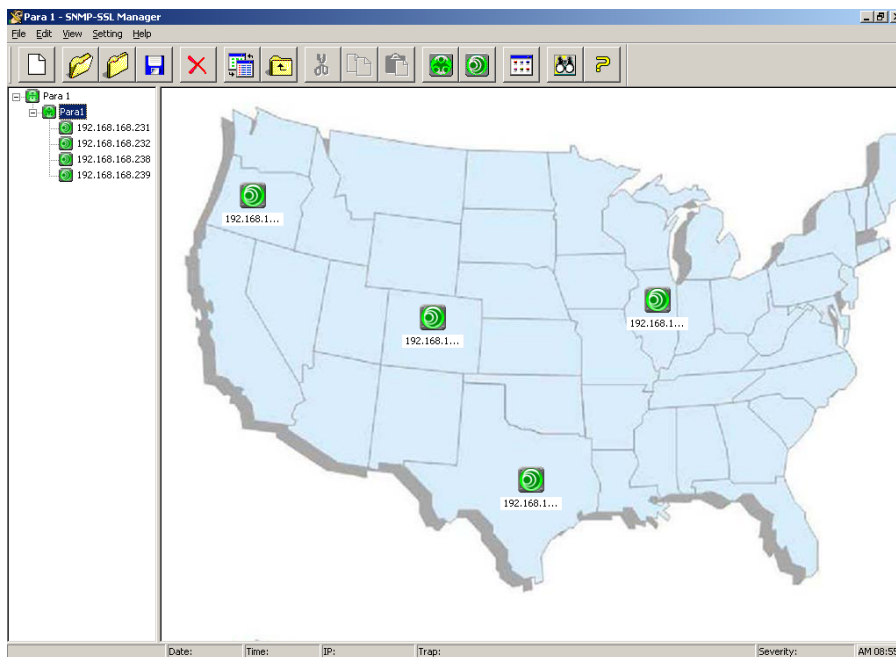


## SNMP-SSL

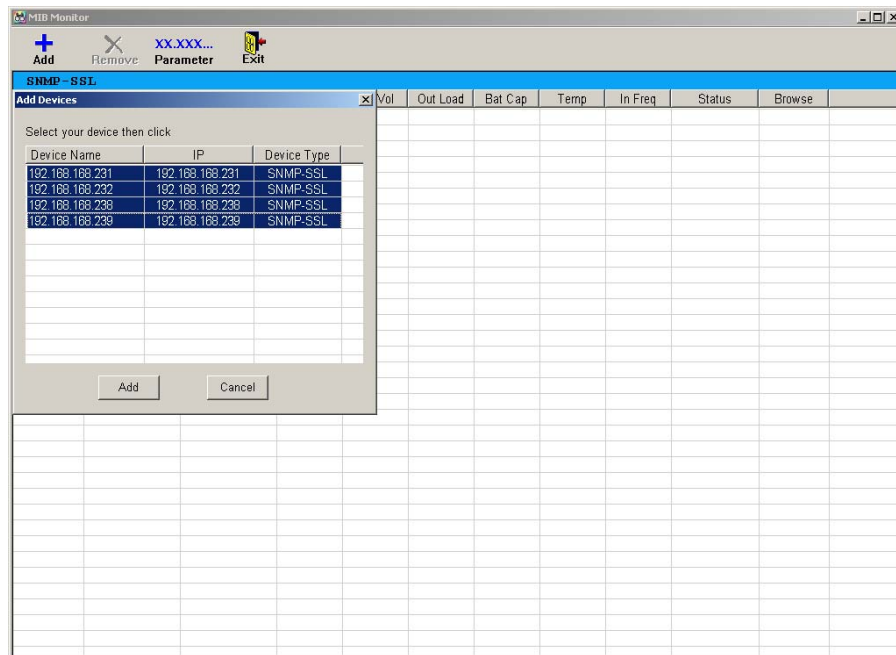
- Under Setting, select the Background Image. Select the appropriate image to be added to the window. These are the default images. You can add your own image using the following types of files: .bmp, .jpg, .gif, .jpeg.



- The icons can be arranged on the image to specify different locations.



9. Under View, select Open MIB Monitor. Select Add to open the Add Device window. Select the devices and then select Add.



10. The devices have been added to the MIB Monitor list. The MIB Monitor displays the operating parameters and the status of the device. Selecting Browse allows you to view the SNMP card's Web pages.

The screenshot shows the main window of the MIB Monitor application. The title bar is 'MIB Monitor' and the toolbar contains 'Add', 'Remove', 'Parameter', and 'Exit' buttons. The main area displays a table with the following data:

Group	Device Name	IP	In Vol	Out Vol	Out Load	Bat Cap	Temp	In Freq	Status	Browse
Para1	192.168.168.231	192.168.168.231	121.3	120.6	0.0	100.0	39.0	60.0	Normal	Browse
Para1	192.168.168.232	192.168.168.232	122.2	122.5	0.0	100.0	31.0	60.0	Normal	Browse
Para1	192.168.168.238	192.168.168.238	121.6	120.0	0.0	100.0	25.0	58.9	Normal	Browse
Para1	192.168.168.239	192.168.168.239	120.7	120.0	0.0	100.0	24.0	58.9	Normal	Browse

## SNMP-SSL

11. Select Parameter. The thresholds can be changed or disabled.

The Parameters Configuration dialog box displays the following settings for SNMP-SSL Parameters:

Parameter	Critical	Warning	Unit	Direction
Input Voltage	85.0	95.0	Vrms	Below
Battery Capacity	20.0	40.0	%	Below
Output Voltage	90.0	100.0	Vrms	Below
Temperature	45.0	38.0		Above
Output Load	110.0	105.0	%	Above
Input Frequency	53.0	56.0	Hz	Below

Buttons: OK, Cancel

12. Under Setting, open e-Mail. This allows you to send and receive notifications of events via email.

The E-Mail Configuration dialog box includes the following fields and options:

- Public Authentication:  User: [ ] Password: [ ] [Apply]
- Mail Server: [ ] => Your Mail Server's Domain or IP address
- Sender Name: [ ] => Sender name on the mail
- Sender e-mail box: [ ] => A valid e-mail address in your Mail Server

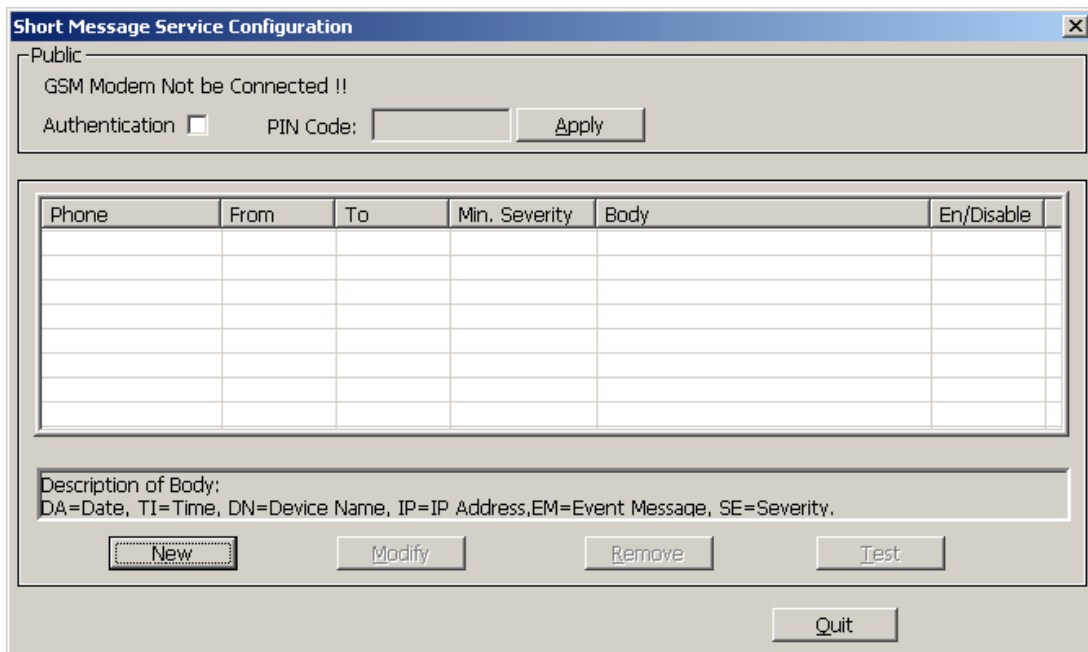
Receiver	Min. Seve...	Subject	En/Disable

Description of Subject:  
DN=Device Name, IP=IP Address, EM=Event Message, SE=Severity.

Buttons: New, Modify, Remove, Test, Quit

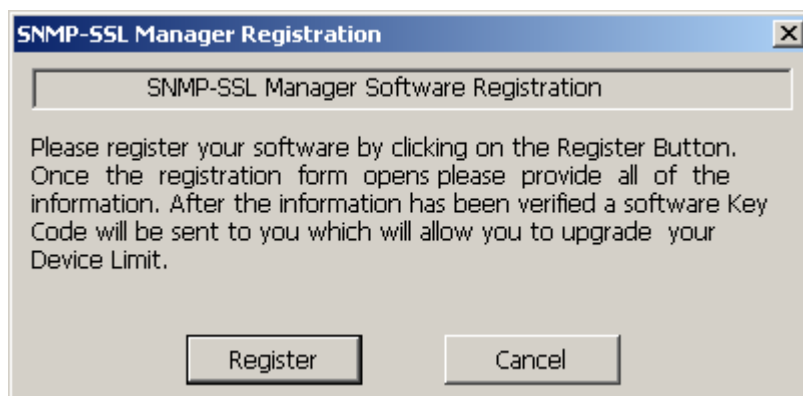


13. Under Setting, open Short Message Service. This allows you to send and receive notifications of events via phone. Connect a GSM modem to the Com port on the SNMP-SSL card.



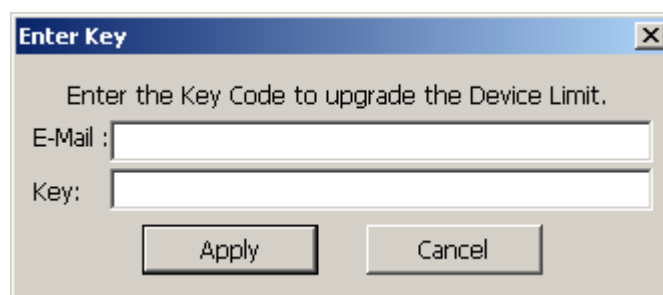
The dialog box is titled "Short Message Service Configuration". It has a "Public" section with the text "GSM Modem Not be Connected !!". Below this, there is an "Authentication" checkbox (unchecked) and a "PIN Code:" label followed by a text input field and an "Apply" button. The main area contains a table with the following columns: "Phone", "From", "To", "Min. Severity", "Body", and "En/Disable". The table is currently empty. Below the table is a "Description of Body:" section with the text "DA=Date, TI=Time, DN=Device Name, IP=IP Address, EM=Event Message, SE=Severity.". At the bottom, there are four buttons: "New", "Modify", "Remove", and "Test". A "Quit" button is located at the very bottom right.

14. The default number of devices that the SSL-Manager will support is 25. Registering the software will allow you to receive a Key Code to upgrade the Device Limit to 3000 devices. Select Register and complete the registration form. Shortly you will receive the Key Code (via email) to upgrade the Device Limit.



The dialog box is titled "SNMP-SSL Manager Registration". It contains the text "SNMP-SSL Manager Software Registration" in a header box. Below this, there is a paragraph of text: "Please register your software by clicking on the Register Button. Once the registration form opens please provide all of the information. After the information has been verified a software Key Code will be sent to you which will allow you to upgrade your Device Limit." At the bottom, there are two buttons: "Register" and "Cancel".

15. Enter the information and select Apply. The Device Limit will be upgraded to 3000 devices.

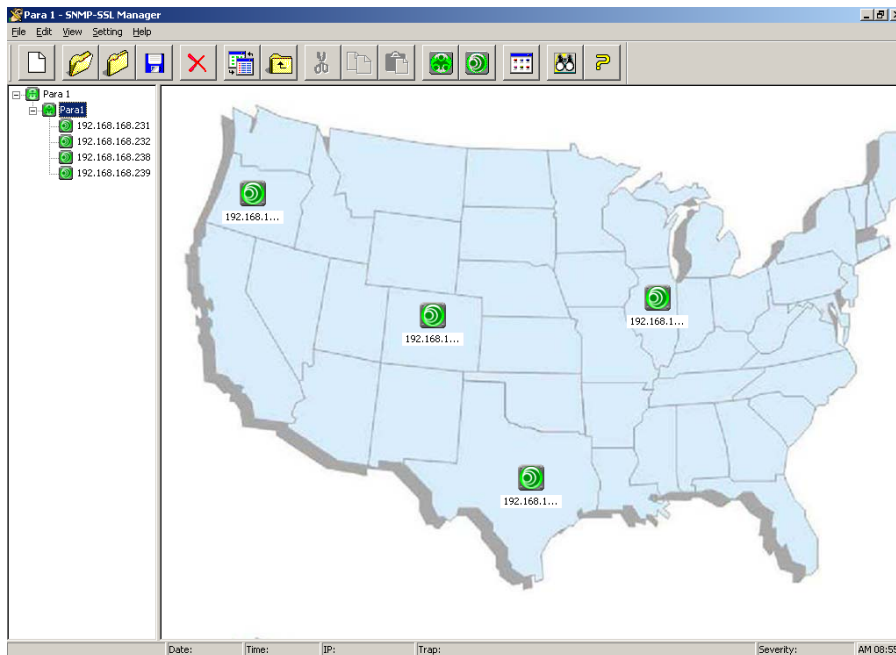


The dialog box is titled "Enter Key". It contains the text "Enter the Key Code to upgrade the Device Limit." Below this, there are two text input fields: "E-Mail:" and "Key:". At the bottom, there are two buttons: "Apply" and "Cancel".

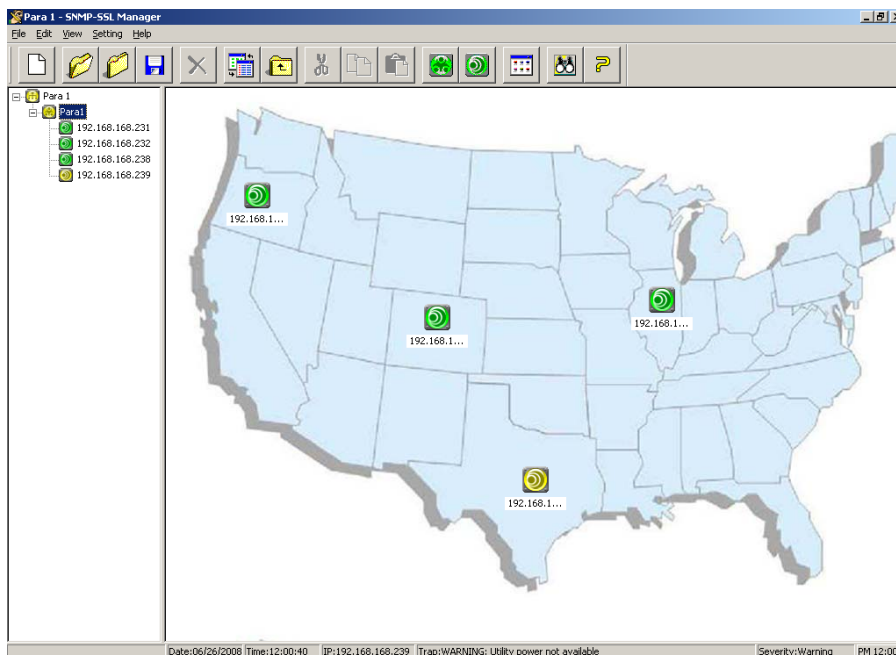
## Chapter 5 Operation

The SSL-Manager is client software running on NMS (Network Management System). Users are provided with a Tree-View on the left hand side and a List-View (Icon style and Report style) on the right hand side to monitor the device in this software. When an event occurs, the icon will change colors according to the severity level, sending an email to the address, which has been set in the e-Mail Configuration window, calling a cell phone number, which has been set in the Short Message Service Configuration window.

1. The SSL-Manager Main screen with all of the devices operating normally.



2. The icon color has changed to advise the user that an event has occurred. Under the Help menu the Status Legend describes the severity level colors.



3. There are several ways to check the status of the device.
  - a. Right click on the device and select Browse. This is the web page of the device, which shows that the UPS is operating on Battery Power.

The screenshot shows the 'Comprehensive View' of the UPS Monitor web interface. The status is 'On Battery'. The following table represents the data shown in the interface:

UPS Status	On Battery
Current Utility Line Voltage (Volt)	0.0
Output Voltage (Volt)	120.0
Output Current (A)	0.0
Output Power (Watts)	0
Output Load (%)	0
Battery Runtime Remaining (minutes)	1167
Battery Capacity Remaining (%)	99
Current Battery Voltage (Volt)	50.0
UPS Temperature (°C)	23.0
Input Frequency (Hertz)	0.0
Output Frequency (Hertz)	59.9
UPS Next Off Time (hh:mm mm/dd/yyyy)	
UPS Next On Time (hh:mm mm/dd/yyyy)	
SNMP-SSL System Date (mm/dd/yyyy)	06/26/2008
SNMP-SSL System Time (hh:mm:ss)	12:01:47
SNMP-SSL Up Time (days hh:mm:ss)	0day 02:13:33

- b. Right click on the device and select Trap History or under View select Trap Log. This shows that the UPS is operating on Battery Power.

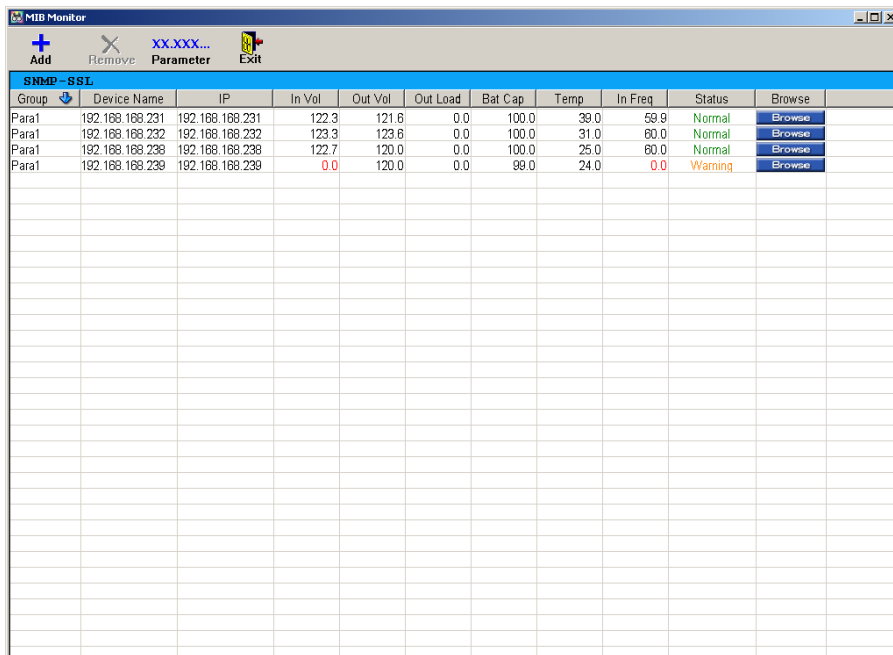
The screenshot shows the 'Trap List' window with a search filter set to 'ALL'. The following table represents the data shown in the window:

Date(M/D/...	Time(H:...	Device Name	IP Address	Event Trap	Severity
06/26/2008	09:22:27	192.168.16...	192.168.168.239	WARNING: The UPS has switched to battery back...	Warning
06/26/2008	09:23:27	192.168.16...	192.168.168.239	WARNING: The UPS has switched to battery back...	Warning
06/26/2008	09:24:27	192.168.16...	192.168.168.239	WARNING: The UPS has switched to battery back...	Warning
06/26/2008	09:25:27	192.168.16...	192.168.168.239	WARNING: The UPS has switched to battery back...	Warning
06/26/2008	09:26:28	192.168.16...	192.168.168.239	WARNING: The UPS has switched to battery back...	Warning
06/26/2008	09:27:28	192.168.16...	192.168.168.239	WARNING: The UPS has switched to battery back...	Warning
06/26/2008	09:28:28	192.168.16...	192.168.168.239	WARNING: The UPS has switched to battery back...	Warning
06/26/2008	09:28:58	192.168.16...	192.168.168.239	INFORMATION: Utility power has been restore	Information
06/26/2008	09:28:58	192.168.16...	192.168.168.239	INFORMATION: The UPS is not on battery power	Information
06/26/2008	12:00:40	192.168.16...	192.168.168.239	WARNING: The UPS has switched to battery back...	Warning
06/26/2008	12:00:40	192.168.16...	192.168.168.239	WARNING: Utility power not available	Warning
06/26/2008	12:01:40	192.168.16...	192.168.168.239	WARNING: The UPS has switched to battery back...	Warning
06/26/2008	12:02:40	192.168.16...	192.168.168.239	WARNING: The UPS has switched to battery back...	Warning
06/26/2008	12:03:40	192.168.16...	192.168.168.239	WARNING: The UPS has switched to battery back...	Warning
06/26/2008	12:04:31	192.168.16...	192.168.168.239	INFORMATION: Utility power has been restore	Information
06/26/2008	12:04:31	192.168.16...	192.168.168.239	INFORMATION: The UPS is not on battery power	Information

## SNMP-SSL

- c. Right click on the device and select Append to MIB Monitor. This shows that the Input voltage to the device is zero.

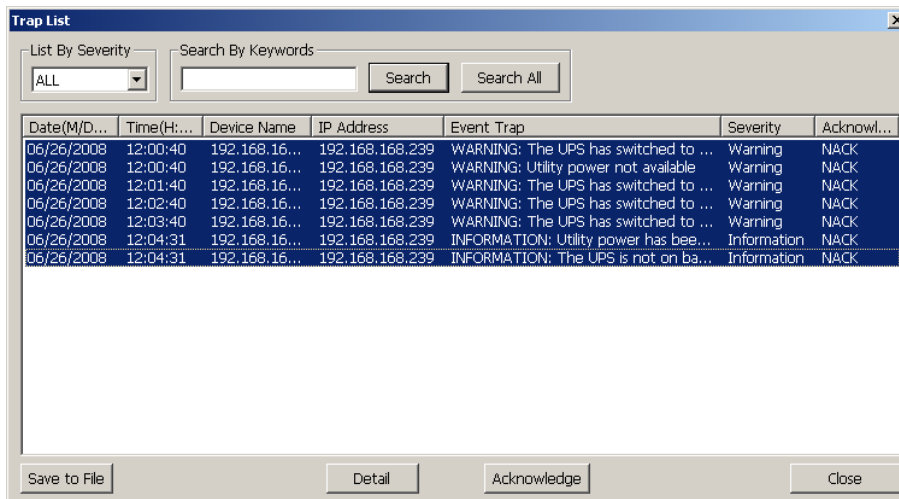
**Note:** To use the Append to MIB Monitor function the MIB Monitor must be running.



The screenshot shows the MIB Monitor application window. The title bar reads "MIB Monitor". Below the title bar is a menu bar with "Add", "Remove", "Parameter", and "Exit". The main area contains a table titled "SNMP-SSL". The table has the following columns: Group, Device Name, IP, In Vol, Out Vol, Out Load, Bat Cap, Temp, In Freq, Status, and Browse. The data rows are as follows:

Group	Device Name	IP	In Vol	Out Vol	Out Load	Bat Cap	Temp	In Freq	Status	Browse
Para1	192.168.168.231	192.168.168.231	122.3	121.6	0.0	100.0	39.0	59.9	Normal	Browse
Para1	192.168.168.232	192.168.168.232	123.3	123.6	0.0	100.0	31.0	60.0	Normal	Browse
Para1	192.168.168.238	192.168.168.238	122.7	120.0	0.0	100.0	25.0	60.0	Normal	Browse
Para1	192.168.168.239	192.168.168.239	0.0	120.0	0.0	98.0	24.0	0.0	Warning	Browse

4. Once the event is over and the device is operating normally the icon will retain the color of the last event. To reset the color to normal the events must be acknowledged. Right click on the device and select Acknowledge. This is a list of the events that have occurred. Select the events and then select Acknowledge.



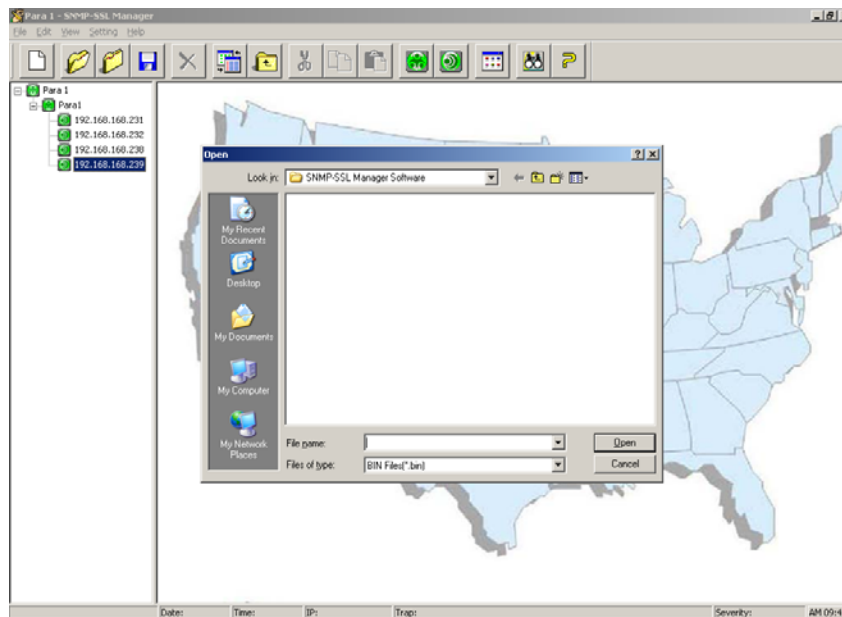
The screenshot shows the Trap List application window. The title bar reads "Trap List". Below the title bar is a menu bar with "List By Severity" and "Search By Keywords". The "List By Severity" dropdown is set to "ALL". The "Search By Keywords" field is empty. The main area contains a table with the following columns: Date(M/D/..., Time(H:...), Device Name, IP Address, Event Trap, Severity, and Acknowl... The data rows are as follows:

Date(M/D/...	Time(H:...	Device Name	IP Address	Event Trap	Severity	Acknowl...
06/26/2008	12:00:40	192.168.16...	192.168.168.239	WARNING: The UPS has switched to ...	Warning	NACK
06/26/2008	12:00:40	192.168.16...	192.168.168.239	WARNING: Utility power not available	Warning	NACK
06/26/2008	12:01:40	192.168.16...	192.168.168.239	WARNING: The UPS has switched to ...	Warning	NACK
06/26/2008	12:02:40	192.168.16...	192.168.168.239	WARNING: The UPS has switched to ...	Warning	NACK
06/26/2008	12:03:40	192.168.16...	192.168.168.239	WARNING: The UPS has switched to ...	Warning	NACK
06/26/2008	12:04:31	192.168.16...	192.168.168.239	INFORMATION: Utility power has bee...	Information	NACK
06/26/2008	12:04:31	192.168.16...	192.168.168.239	INFORMATION: The UPS is not on ba...	Information	NACK

## Chapter 6 Upgrading the SNMP-SSL card

The SNMP-SSL card's firmware can be upgraded individually or in a batch process from the SSL-Manager software.

1. Individually Upgrading. Select the devices in the List-View window (left hand side). Under Setting select Upgrade File or right click on the device's icon (right hand side), select Upgrade Firmware. Browse for the location of the upgrade file (.BIN) and then select Open. The upgrading process will take approximately two minutes per device. Once the upgrade is complete the SNMP-SSL card will reboot.



2. Batch Process Upgrading. Under View, select Report Style. Select all of the devices in the list. Under Setting, select Upgrade File. Browse for the location of the upgrade file (.BIN) and then select Open. The upgrading process will take approximately two minutes per device. Once the first device is complete the software will automatically start upgrading the next device in the list. This will continue until all of the selected devices have been upgraded. Once the upgrade is complete the SNMP-SSL cards will reboot.

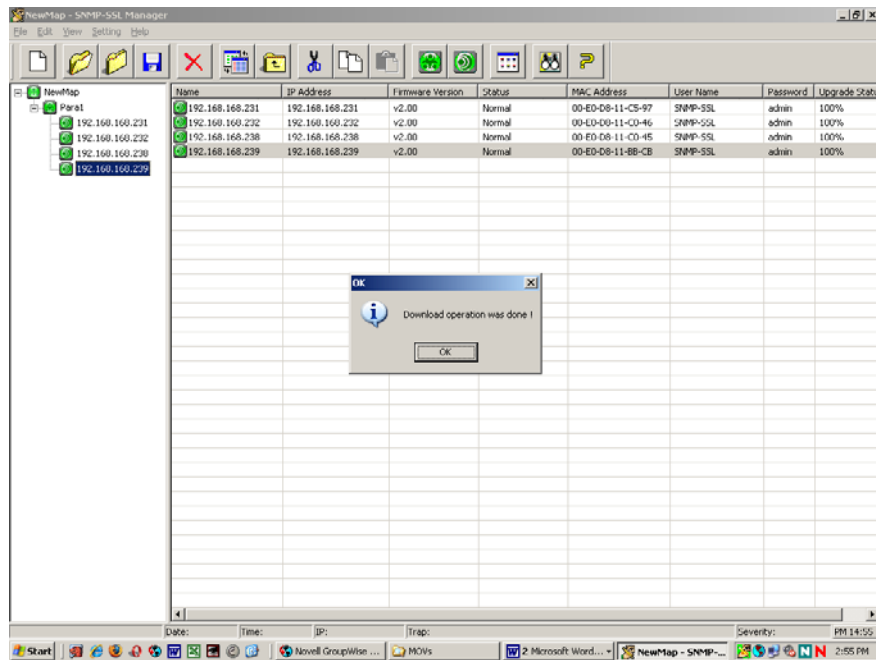
The screenshot shows the 'SNMP-SSL Manager' application window displaying a table of upgrade progress. The table has the following columns: Name, IP Address, Firmware Version, Status, MAC Address, User Name, Password, and Upgrade Si. The data rows are as follows:

Name	IP Address	Firmware Version	Status	MAC Address	User Name	Password	Upgrade Si
192.168.168.231	192.168.168.231	v2.00	Normal	00-E0-0B-11-C5-97	SNMP-SSL	admin	100%
192.168.168.232	192.168.168.232	v2.00	Normal	00-E0-0B-11-C0-46	SNMP-SSL	admin	100%
192.168.168.233	192.168.168.233	v2.00	Normal	00-E0-0B-11-C0-45	SNMP-SSL	admin	100%
192.168.168.234	192.168.168.234	v2.00	Normal	00-E0-0B-11-8B-C8	SNMP-SSL	admin	44%

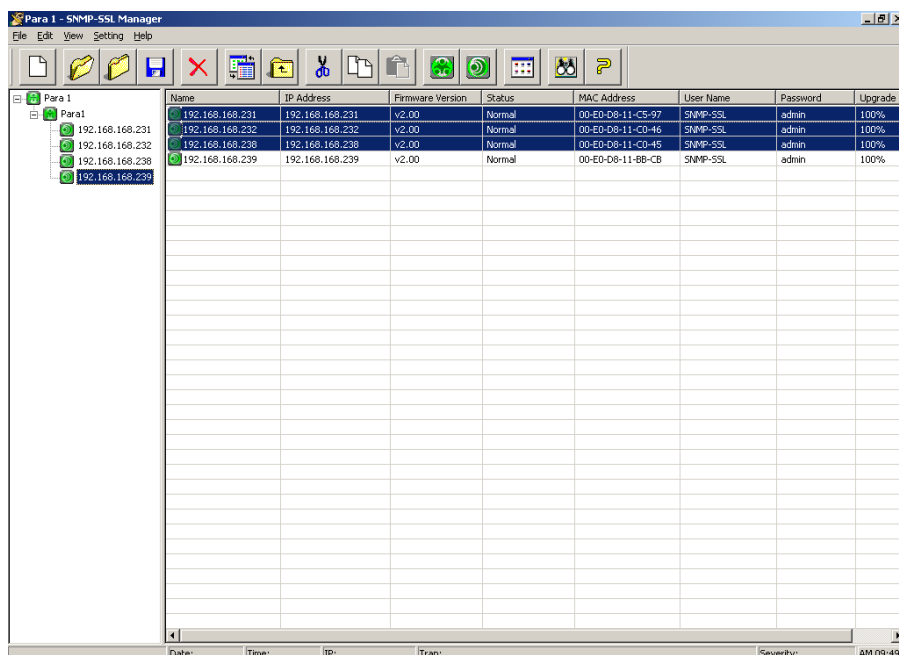
## Chapter 7 Batch Configurations

The SNMP-SSL card's Configuration can be copied (Downloaded) from one SNMP-SSL card and transferred (Uploaded) to another SNMP-SSL card from the SSL-Manager software. The configuration file will have all of the information from the SNMP-SSL web page, except the IP address, the Gate Way address, the SNMPv3 USM Table, or the log files.

1. Under View, select Report Style. Select the device from the list to download the conformation. Right click and select Download Configuration. When the download is complete the following screen will appear, click OK.



2. Select the devices from the list that you want to upload the Configuration to. Right click and select Upload Configuration. Once the upload is complete the SNMP-SSL cards will reboot.



## Obtaining Technical Assistance

For Technical Support on the Web, please visit the Support section of our Web site or visit our online Discussion Forum.

In order to diagnose the problem you are having, our technicians need the following information from you.

### Installation Site:

Company Name: \_\_\_\_\_

Address: \_\_\_\_\_

City: \_\_\_\_\_ State: \_\_\_\_\_ ZIP code: \_\_\_\_\_

Contact Person's Name: \_\_\_\_\_

Phone Number: \_\_\_\_\_

### If you are a consultant,

Consultant Name: \_\_\_\_\_

Phone Number: \_\_\_\_\_ Fax Number: \_\_\_\_\_

### Computer System:

Operating System and version: \_\_\_\_\_

System Manufacturer: \_\_\_\_\_

System Model Number: \_\_\_\_\_

NMS name and revision number: \_\_\_\_\_

### UPS:

Model Name/Number: \_\_\_\_\_

Serial Number: \_\_\_\_\_

### What are the symptoms?

---



---



---



---

Please have the information listed above ready when you contact us.

Contact Technical Support By:

Phone: 1-800-238-7272 / 1-972-446-7363

Fax: 1-972-446-9011

Web: [www.minutemanups.com/support/index.php](http://www.minutemanups.com/support/index.php) (Technical Support)  
[www.minutemanups.com/phpBB2/index.php](http://www.minutemanups.com/phpBB2/index.php) (Discussion Board)  
[www.minutemanups.com](http://www.minutemanups.com) (Home Page)

## Limited Product Warranty

Para Systems Inc. (Para Systems) warrants this equipment, when properly applied and operated within specified conditions, against faulty materials or workmanship for a period of three years from the date of original purchase by the end user. For equipment sites within the United States and Canada, this warranty covers repair or replacement of defective equipment at the discretion of Para Systems. Repair will be from the nearest authorized service center. Replacement parts and warranty labor will be borne by Para Systems. For equipment located outside of the United States and Canada, Para Systems only covers faulty parts. Para Systems products repaired or replaced pursuant to this warranty shall be warranted for the remaining portion of the warranty that applies to the original product. This warranty applies only to the original purchaser who must have properly registered the product within 10 days of purchase.

The warranty shall be void if (a) the equipment is damaged by the customer, is improperly used, is subjected to an adverse operating environment, or is operated outside the limits of its electrical specifications; (b) the equipment is repaired or modified by anyone other than Para Systems or Para Systems-approved personnel; or (c) has been used in a manner contrary to the product's operating manual or other written instructions.

Any technical advice furnished before or after delivery in regard to use or application of Para Systems's equipment is furnished without charge and on the basis that it represents Para Systems's best judgment under the circumstances, but it is used at the recipient's sole risk.

**EXCEPT AS PROVIDED HEREIN, PARA SYSTEMS MAKES NO WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.** Some states do not permit limitation of implied warranties; therefore, the aforesaid limitation(s) may not apply to the purchaser.

**EXCEPT AS PROVIDED ABOVE, IN NO EVENT WILL PARA SYSTEMS BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS PRODUCT, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.** Specifically, Para Systems is not liable for any costs, such as lost profits or revenue, loss of equipment, loss of use of equipment, loss of software, loss of data, cost of substitutes, claims by third parties, or otherwise. The sole and exclusive remedy for breach of any warranty, expressed or implied, concerning Para Systems's products and the only obligation of Para Systems hereunder, shall be the repair or replacement of defective equipment, components, or parts; or, at Para Systems's option, refund of the purchase price or substitution with an equivalent replacement product. This warranty gives you specific legal rights and you may also have other rights, which vary from state to state.