

PowerNETGuard

User and Installation Manual

SUPPORT AND LIABILITY STATEMENT

The manufacturer does not accept liability for loss of data, productivity, equipment or any other associated damage or cost (direct or indirect) due to the failure of PowerNETGuard or related equipment.

A tremendous amount of effort has gone into making PowerNETGuard as easy to use as possible. However, should the user find that additional information or help is necessary, he/she should contact the local distributor/dealer who has access to the support centre.

It should be noted that technical support is not intended for general questions regarding the operating system.

© No part of this manual may be reproduced without the prior written permission of the manufacturer. The manufacturer reserves the right to modify the product described in this manual at any time and without notice.

SUMMARY

<i>WHAT IS SNMP?</i>	4
<i>HARDWARE REQUIREMENTS</i>	4
<i>INSTALLATION</i>	4
<i>UNINSTALLING</i>	5
<i>FUNCTION</i>	5
<i>WHAT'S NEW SINCE PREVIOUS VERSION</i>	5
SERVICES	6
<i>WEB CONNECTIVITY</i>	6
<i>SECURE SNMP</i>	10
<i>MULTIUSER</i>	11
<i>EVENT LOG</i>	12
<i>ADVANCED CONFIGURATION</i>	12
USER INTERFACE	13
<i>TOOLBAR STRUCTURE</i>	13
<i>NEW SNMP OBJECT</i>	14
<i>IDENTIFICATION DATA MODIFICATION</i>	14
NETWORK VISUALIZATION	15
<i>TREE STRUCTURE DISPLAY</i>	15
<i>INDEX DISPLAY</i>	16
<i>SCHEDULED MAINTENANCE DATABASE</i>	17
<i>DESKTOP</i>	18
<i>STANDARD DATA (UPS VERSION)</i>	19
<i>STANDARD DATA (IRMS VERSION)</i>	20
<i>DIAGRAM DATA (ONLY UPS)</i>	21
<i>LOG</i>	22
<i>GRAPHICS</i>	23
CONFIGURATION	25
<i>USER CONFIGURATION</i>	25
<i>GENERAL CONFIGURATION</i>	26
<i>SECURE SNMP CONFIGURATION</i>	27
<i>AUTO WALK CONFIGURATION</i>	28
<i>ALARMS CONFIGURATION</i>	29
<i>EMAIL CONFIGURATION</i>	30
<i>SMS CONFIGURATION</i>	31
<i>OTHER CONFIGURATION</i>	31

INTRODUCTION

Thank you for choosing PowerNETGuard!

PowerNETGuard is an UPS remote management program which utilises the SNMP protocol. In other words, it is an optimised SNMP manager for RFC 1628, the world standard in the management of UPSs. For this reason PowerNETGuard can be used with any agent that supports this standard. Versions for Windows (2000, XP, 2003, Vista, 2008, 7); as well as for Linux x86, Solaris 8, 9, 10 (x86 and SPARC) are available.

WHAT IS SNMP?

SNMP (Simple Network Management Protocol) is a communications protocol, a tool that allows the client (manager) to effect requests to a server (agent). This protocol is an international standard and so any SNMP manager can communicate with any SNMP agent.

To exchange information, the manager and agent utilise an addressing technique called MIB (Management Information Base). MIB defines which variables can be requested and the respective access rights. MIB is equipped with a tree structure (like the folders on a hard disk), through which manager and agent can use several MIB at the same time, as there is no overlap.

Each MIB is oriented to a particular sector; in particular RFC-1628, also called UPS-MIB, holds the data for UPS remote management.

Furthermore, the agent can submit data without a prior request to inform the manager about particularly important events. These messages are called traps.

For more information about SNMP visit this site: <http://www.snmp.com>.

HARDWARE REQUIREMENTS

The following are the minimum requirements to obtain an acceptable operating speed.

Intel systems require a PC with a Pentium III or an equivalent processor with 1GHz and 256 Mb RAM.

SPARC systems require a workstation with an UltraSPARC-IIe processor of 500MHz and 256 Mb RAM (for example, SunBlade 100).

Mac systems require a computer with a G3 processor 500MHz and 256 Mb RAM. For SGI systems a MIPS R4000 processor is required and for Compaq system a Alpha 21064 processor is required.

INSTALLATION

On Windows systems, open the "PowerNETGuard.exe" file in the "Windows" folder and follow the instructions.

On Linux and Solaris, open the "install.bin" file in the respective folders and follow the instructions.

On Mac systems, open the "PowerNETGuard.dmg" disk image in the "MacOSX" folder and then copy the application to the "Applications" folder.

On SGI Irix systems, open the "install.bin" file and follow the instructions.

On Tru64 systems, open the "install.bin" file and follow the instructions.

If the installation program shows that a Java Virtual Machine is not present (version 6 or higher is required), proceed with the installation as follows:

if you own the CD-ROM run the installation program contained in the "JavaVM" folder; otherwise download "Java software" from the website <http://www.java.com>.

On Mac system the Java Virtual Machine is distributed by Apple from this site:

<http://www.apple.com/macosx/features/java/>.

UNINSTALLING

For Windows systems, run the “Install applications” program from the Control Panel, select PowerNETGuard and click on “Remove”.

For Unix systems run the “Uninstall” program in the “PowerNETGuard/Uninstaller Data” directory.

For Mac systems drag the “PowerNETGuard” application contained in the “Application” folder to the trash.

FUNCTION

PowerNETGuard provides a visual display of UPSs managed through the medium of a folder structure. At the root there is the “Network” folder and each folder can contain other folders, UPSs and IRMSs.

The UPSs/IRMSs contained in the “UPS” folder, or in a sub-folder make up the cluster of objects that can be managed through the program and the folders serve to organise these objects according to various criteria. One example of a possible criterion is geographic. For instance, there could be a folder called “Europe” that contains “Italy” and “Germany” folders, which in turn contain UPSs.

Once the structure that represents the remotely managed objects has been created, it can be saved on the disk drive, or another structure that has been created beforehand can be loaded.

The UPS is an object that can be queried to supply operating status data. It can be selected to view data and in order to avoid unnecessary queries, the information retrieved is saved in the memory until the program is closed. This is valid also for IRMS.

When a UPS or a IRMS is selected, updated real-time status information can be obtained, data that is not yet updated can also be retained. In the first case the data viewed is more reliable, however it causes greater network traffic.

Even if it has not been selected, an object will show its status anyway through the colour of its icon. PowerNETGuard detects errors even when an UPS/IRMS is not selected thanks to the integrated trap management and to auto-walk.

PowerNETGuard is multi-user, where each user is identified by a password and personalised rights.

PowerNETGuard is able to react to UPSs/IRMSs status changes by giving a timely communication to the users by means of email and SMS. It is available a WAP connectivity in order to perform a “everywhere and 24 hours” alarm monitoring on the objects. Also WEB connectivity is available for UPS monitoring via web browser.

WHAT’S NEW SINCE PREVIOUS VERSION

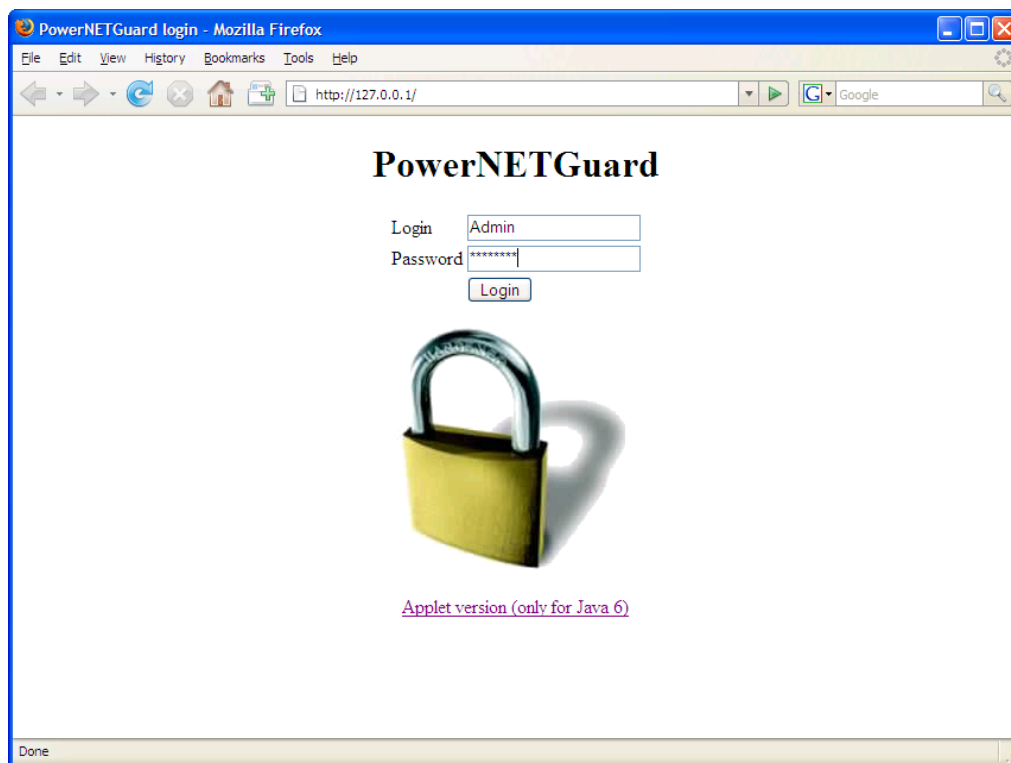
- 4.0 Renewed user interface, extended MAPI, more powerful scripts and new license scheme.
- 3.5 New auto-walk logic, applet, email with authentication
- 3.0 Secure SNMP support, controls for WakeOnLan, and scheduled maintenance
- 2.4 Multilanguage, controls for remote shutdown and reboot
- 2.1 WEB connectivity for state monitoring
- 2.0 IRMS support, event log.
- 1.2 WAP connectivity enables a “everywhere and 24 hours” alarm monitoring.
- 1.1 PowerNETGuard is able to react to UPSs status changes by giving a timely communication to the users by means of email and SMS.

SERVICES

Besides directly monitoring the devices, PowerNETGuard supports a wide range of tools and services that improves the devices management.

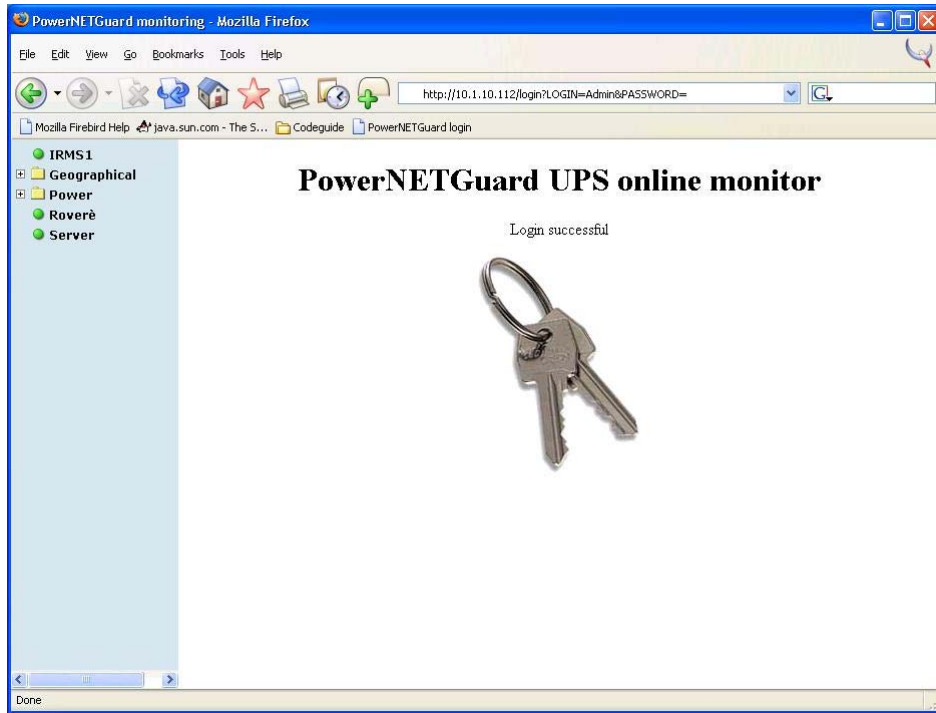
WEB CONNECTIVITY

In order to enable or disable the WEB connectivity select the panel “Preferences...→WEB” and then restart PowerNETGuard. This function obviously cannot coexist with other web servers running on the same port. From a client computer it is possible to connect with an internet browser by inserting as web address the host name or the IP address of the computer where PowerNETGuard is running.

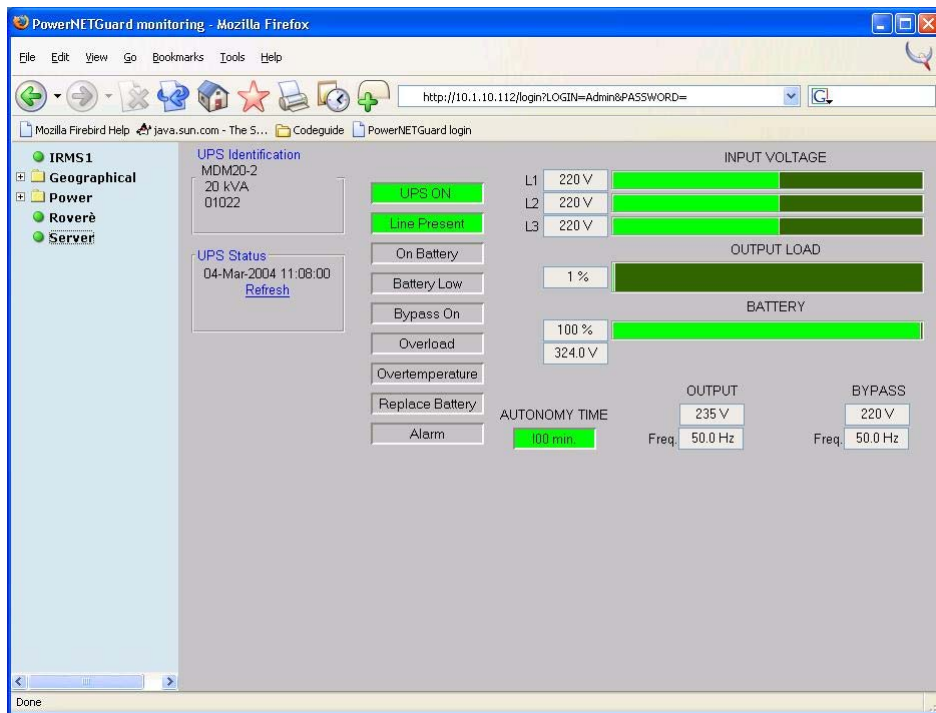


Insert login and password of a PowerNETGuard user; as an alternative, it is possible to use the applet version (functionally equivalent but with the application's graphics) by selecting the link on the bottom of the page.

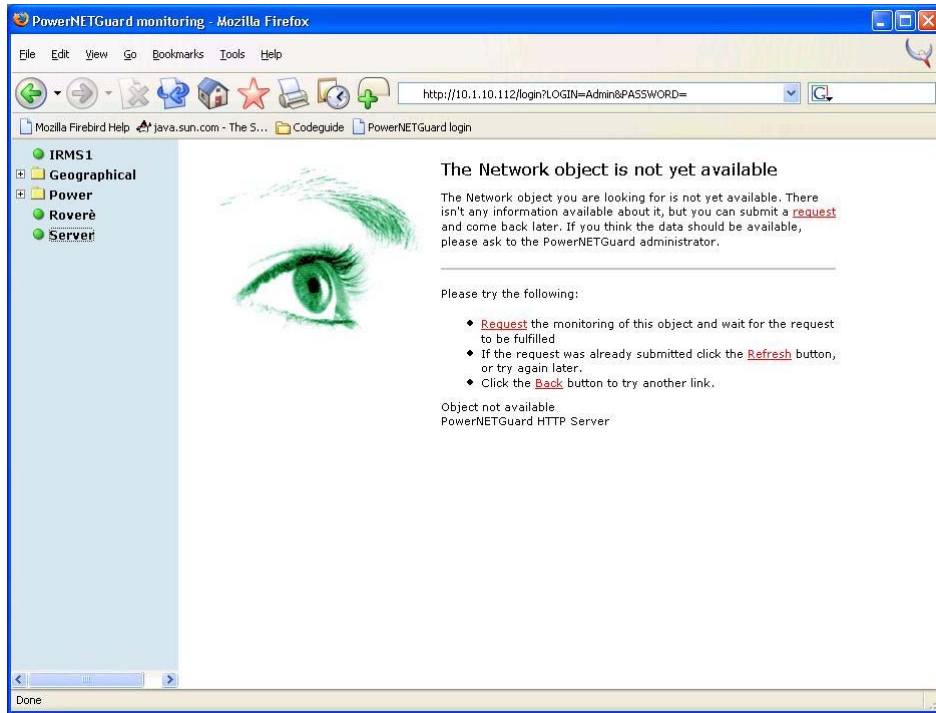
WARNING: if there is a completely different page instead of this then on the computer is running another web server; in that case please change PowerNETGuard's WEB port and when connecting from a client add the specified port number to the address (for example: `http://10.1.10.112:4000`).



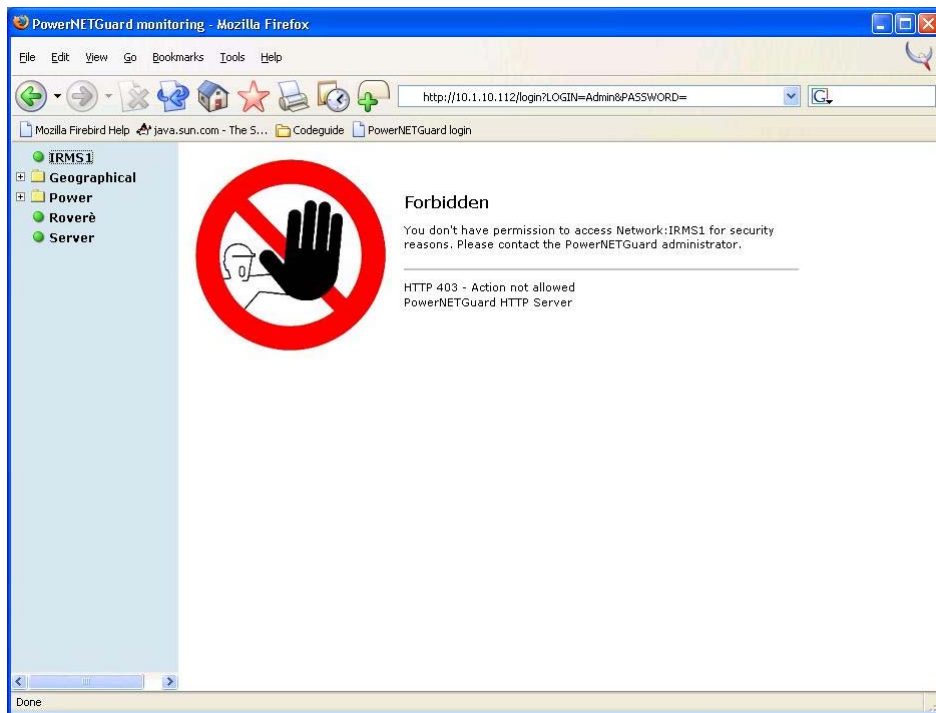
After that the access has been authenticated this page is shown. On the left side there is a tree structure that replicates that of the PowerNETGuard; by selecting a folder it is possible to view the objects and the subfolders contained, and by selecting an object it is possible to view the data monitored by PowerNETGuard.



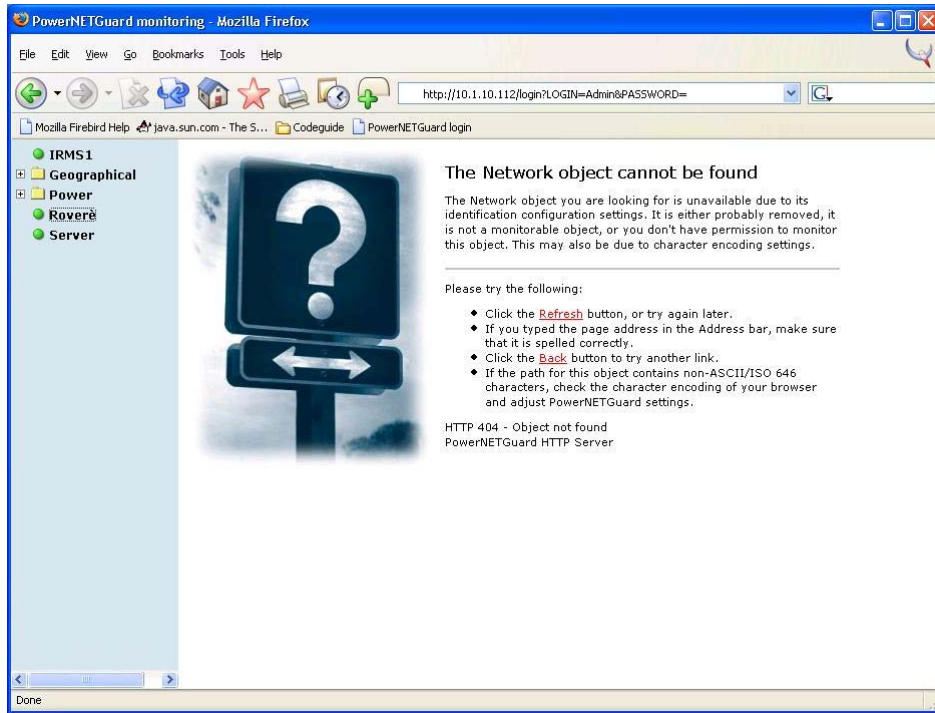
The data is shown only if before PowerNETGuard connected to the device. In particular, on "UPS Status" it is visible the time of the last refresh and by clicking on "Refresh" it is possible to request a refresh of the data.



If the data isn't available this page is shown, and from here it is possible to request a refresh of the data.



When the user does not have the right or when a non monitorable object is selected this page is shown.



The selected object might be unavailable due to removal or renaming and in that case this page is shown. It is also possible that the address of the object contains character non contained in standard ASCII and that the encoding of the browser is different from that used by PowerNETGuard: in that case it is necessary to modify the character encoding from the panel "Preferences...→ WEB" (for example, Microsoft Internet Explorer uses "UTF-8" encoding and Mozilla Firefox uses "ISO-8859-1").









SECURE SNMP

Secure SNMP is an innovation introduced for improving the security on the IRMS management; it features in particular authentication and authorization with the possibility to configure the granted privileges.

On the IRMS configuration it is possible to set 3 passwords and to bind to each one different privileges: when a user authenticates, these privileges will be granted. In particular, for each output socket it is possible to define the privilege to turn it on or off, to perform the reset (shutdown and restart), and to perform the source power switch (from line A to line B and vice versa).

Irms V.3.0 05/2004 □ Network card v. 01.01

Input lines OK

 Adm terminal	 Mail server	 WEB server	 FTP server	 Gateway	 Laboratory	 Office 1	 Office 2
---------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------






Output load

0.0 A	0.0 A	0.0 A	0.0 A	0.0 A	0.0 A	0.0 A	0.0 A
0 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %

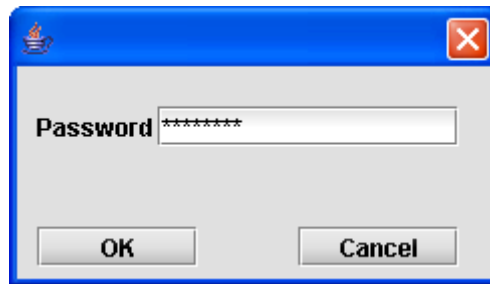
Input voltage

Line A	226 V	Line B	227 V
---------------	-------	---------------	-------

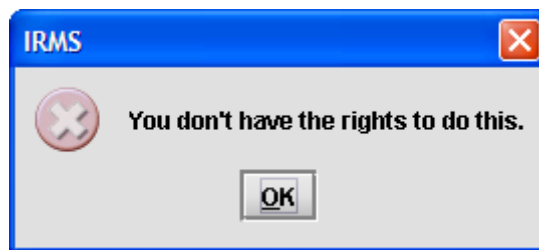
Command



At first PowerNETGuard locks all actions (padlock closed), but after clicking on a socket the password will be requested.



After inserting the password PowerNETGuard allows to send commands. The commands are sent together with the password inserted by the user: if the password is recognized by the IRMS and is granted the privilege to perform the operation then the request is fulfilled; otherwise PowerNETGuard shows an alert.



As a further level of security the functions unlocked becomes locked again after 1 minute. This amount can be configured on the preferences.

WARNING: Secure SNMP is not available for obsolete IRMS models.

However, PowerNETGuard is able to recognize these models and unlocks the supported functions without requiring a password.

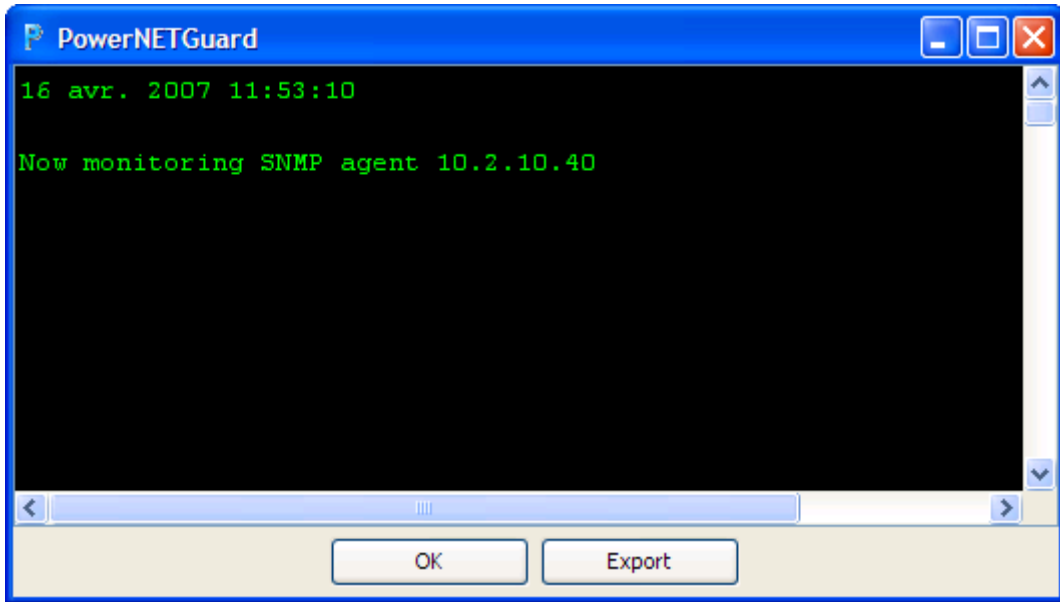
MULTIUSER

Every PowerNETGuard user has a login and password that are required for accessing the software functions. Every user has a different set of privileges which are defined by the administrator. In particular:

- ✍ Control UPSs: the right to perform maintenance operations like UPS shutdown and reboot;
- ✍ Monitor UPSs: the right to set up a connection to a device and to view data;
- ✍ Define UPSs and locations: the right to add new UPSs and new folders;
- ✍ Show logs and graphs: the right to view past data;
- ✍ Clear log database: the right to overwrite preceding logs;
- ✍ User administration: the right to create new users and modify the existing ones;
- ✍ Administrator: right to close the program down.

The default user is whom the automatic login is performed, when active.

EVENT LOG



By selecting "Event log" on the File menu it is possible to view the debug events that were registered by PowerNETGuard. This displays information about communication, such as the agent selected, timeout, the presence of request errors and the traps received. It is possible to export these events to a text file.

ADVANCED CONFIGURATION



It is also possible to perform remote maintenance operation on the UPS, like shutdown and reboot, by pressing the "Advanced configuration" button. PowerNETGuard will ask the seconds of delay for shutdown or reboot according to the requested operation. It is also possible to send WakeOnLan packets. To perform this function on a device it is required to know its MAC address and it is necessary that that device is compatible and correctly configured for using this function.

USER INTERFACE

TOOLBAR STRUCTURE



The «new folder» icon creates a new folder within the current folder.



The «delete» icon eliminates the selected item and any items it contains.



The «new object» icon creates an object inside the current folder.



The «open» icon loads the tree structure from the previously saved file.



The «save» icon saves the tree structure onto the hard disk so that it can be reloaded.



The «configure» icon to configure MIB variables.



The «advanced configuration» icon for maintenance operation like WakeOnLan, UPS shutdown and reboot.



The «load log file» icon loads the log files previously saved.



The «exit» icon exits PowerNETGuard.

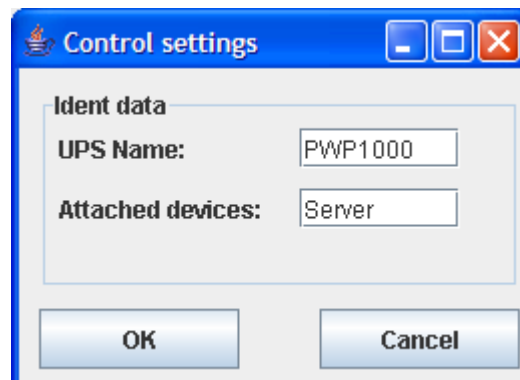
There is also an address bar that displays the path of the selected folder or UPS. A folder or a device are selected by entering an address and pressing Enter.

NEW SNMP OBJECT



When a new object is inserted to be monitored, this screen will appear, so that it can be given a name (it can be changed by clicking on the name in the tree structure display), an object type, a IP address (alternatively the name that is displayed on the network can be used), the SNMP communities and the SNMP communication port (the standard is 161 but this can be changed).

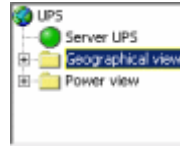
IDENTIFICATION DATA MODIFICATION



By pressing the "Configuration" button it is possible to set the UPS name and the attached devices. These values are used only for giving a SNMP identification and in particular the UPS name must not be confused with the identification code of the UPS.

NETWORK VISUALIZATION

TREE STRUCTURE DISPLAY



The tree structure displays the items managed. By selecting an item the communication is established; it can also be renamed, or a menu can be displayed (right-hand mouse button for Windows) for modify its data or show the maintenance database. UPSs and the IRMSs are displayed with an icon which shows the symbol of their status:

	Device not yet monitored.
	Normal status condition.
	"Minor" alarm present.
	Receipt of a trap, or "major" or "critical" alarm present.
	Communication lost.

If a closed folder contains one or more devices in alarm status, the folder will display the alarm symbol.

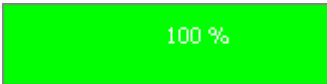
INDEX DISPLAY

Name	Last update	IP Address, Port	Communication bar	Status
Net4	n/a	10.1.10.219, 161		
Net2	3/10/07 2:08 PM	10.1.10.199, 161	100 %	
Net6	n/a	10.1.10.143, 161		
Netman plus	n/a	10.1.10.181, 161		
MDT60	n/a	10.1.10.128, 161		
Netman TT1	n/a	10.1.10.196, 161		
Net7	n/a	10.2.10.40, 161		

This displays a list of the objects in the current folder and sub-folders. The name, time of last query, address and agent port as well as the current status will be displayed. By clicking on an object this will be selected and polled automatically if necessary.



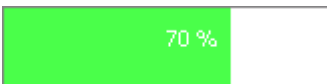
If the status is white, there is no information available and a query must be started.



If the status is bright green marked «100%» it has been polled and the data is available and the information displayed is updated in real time.

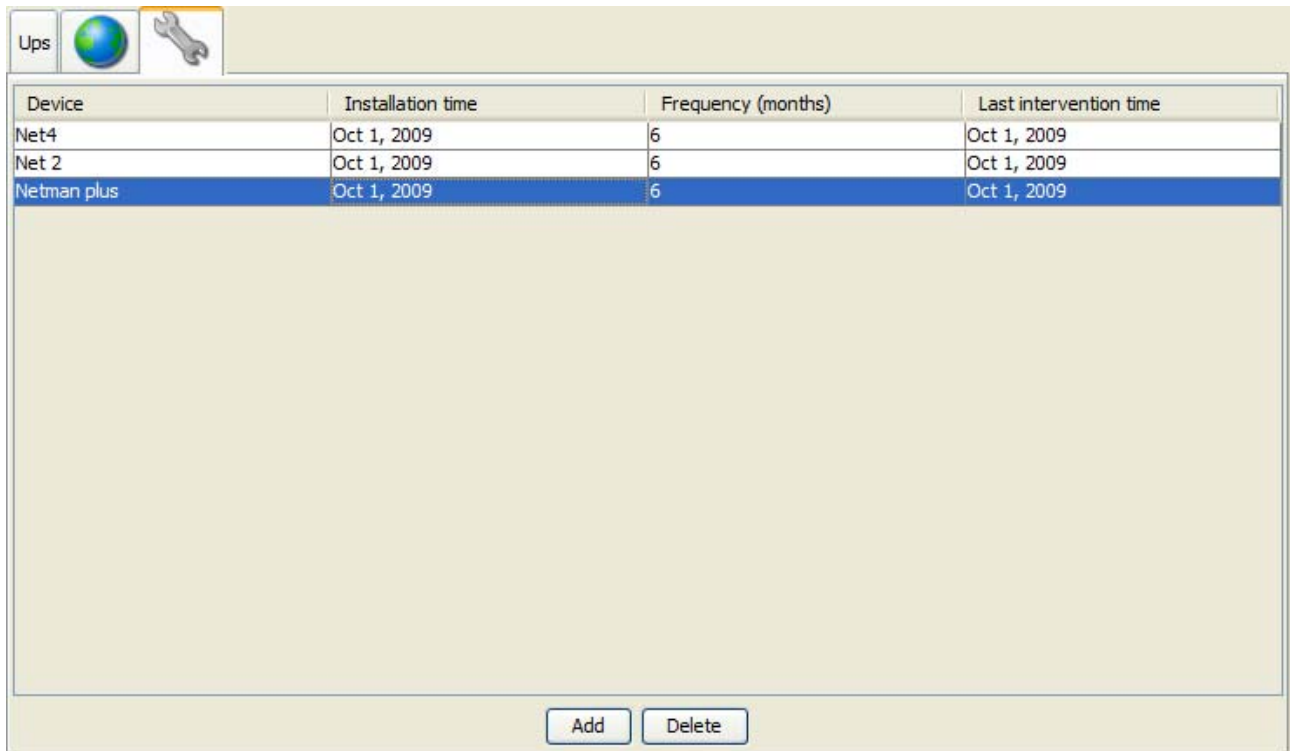


If the status is grey and marked «100%» it has been polled and the data is available, but it is not a current selection.



During the query, the bar grows and changes colour from white to green.

SCHEDULED MAINTENANCE DATABASE



Device	Installation time	Frequency (months)	Last intervention time
Net4	Oct 1, 2009	6	Oct 1, 2009
Net 2	Oct 1, 2009	6	Oct 1, 2009
Netman plus	Oct 1, 2009	6	Oct 1, 2009

Buttons: Add, Delete

Shows the scheduled maintenance database for the devices. For each device it is possible to insert a custom scheduled maintenance frequency; and at the fixed date the configured actions are performed (please see section “Alarm configuration”).

DESKTOP



This displays the UPSs/IRMSs contained in the current folder following the desktop metaphor. UPSs/IRMSs can be moved by clicking and dragging while holding the button down. A menu can be displayed on the (right-hand mouse button for Windows) UPSs/IRMSs or on the background.

In particular, the object can be selected, queried or eliminated, while on the desktop a new folder or a new object can be created, the background can be changed, or the user can browse among folders that stem from one folder or define an active area.

An active area is a desktop zone that when clicked, downloads a folder. For instance, the "Europe" folder can have a "France" sub-folder. In this case the "Europe" background could be a map of Europe, while the "France" background could be a map of France. In this case, it is worth defining the active area "France" in the section of the "Europe" background that coincides with France. So by clicking on France on the map of Europe the "France" folder will open.

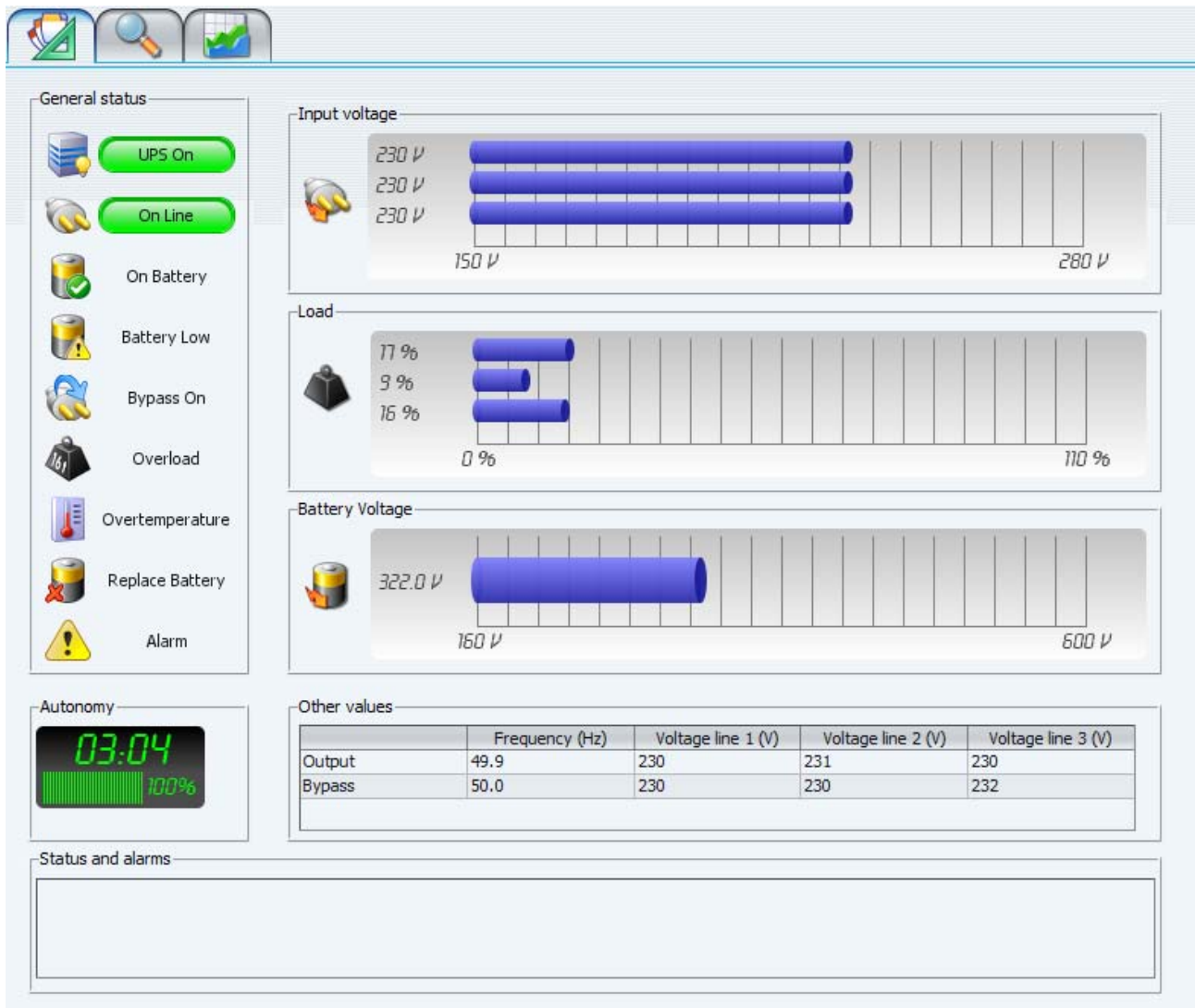
To define the active area:

1. Select the "define active area" entry from the menu;
2. Choose the area to be made active from the index;
3. Draw a rectangle to encompass the active area.

When the mouse passes over an active area this will turn:

- green if there are no UPS with alarm status inside;
- red if there are "major" or "critical" alarm status;
- yellow if there are "minor" alarm status;
- blue if the communication is lost.

STANDARD DATA (UPS VERSION)











This displays the machine status with LED lamps and graphic bars.

STANDARD DATA (IRMS VERSION)

Irms V.3.0 05/2004 □ Network card v. 01.01

Input lines OK

 Adm terminal	 Mail server	 WEB server	 FTP server	 Gateway	 Laboratory	 Office 1	 Office 2
------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------






Output load

0.0 A	0.0 A	0.0 A	0.0 A	0.0 A	0.0 A	0.0 A	0.0 A
0 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %

Input voltage

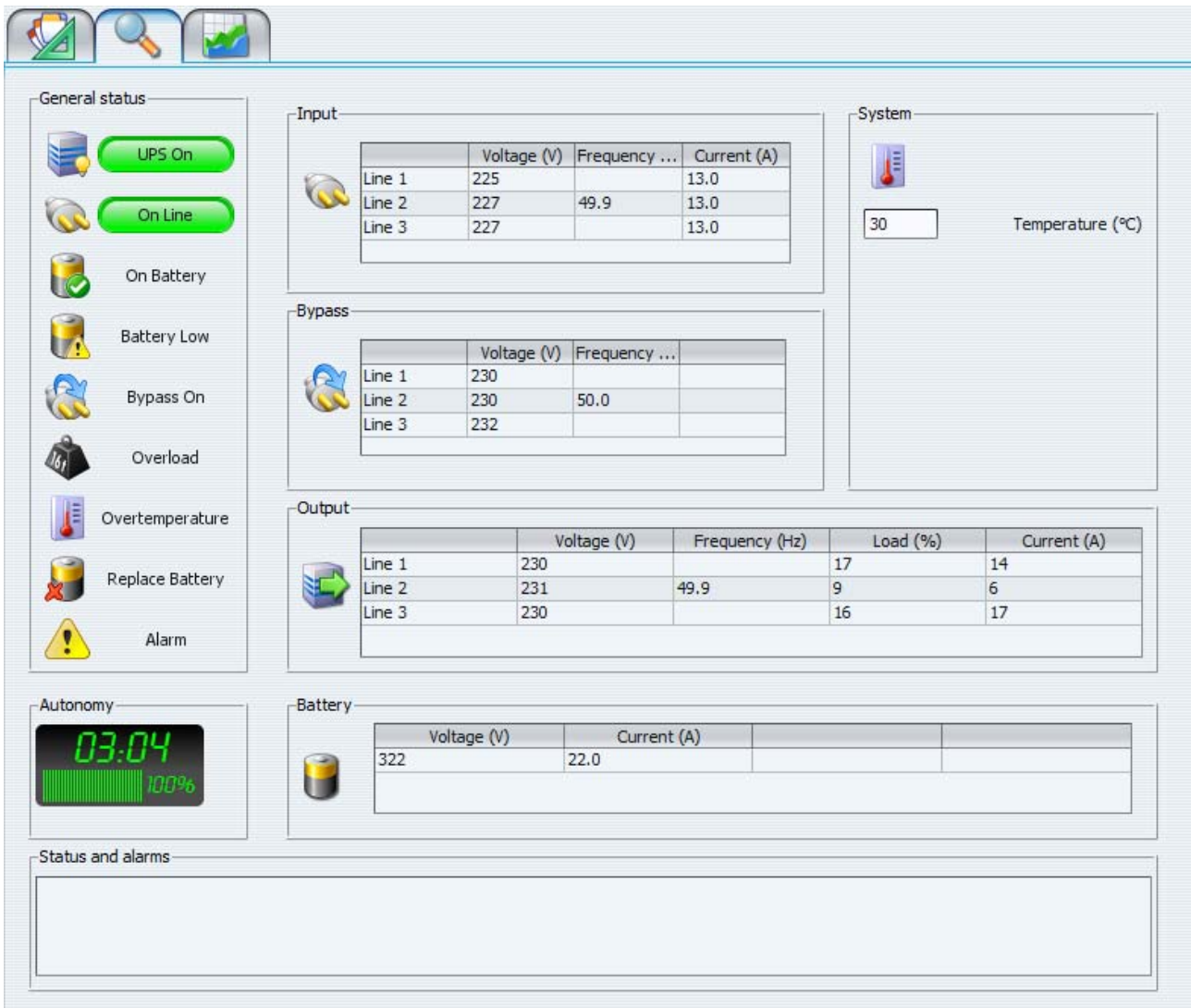
Line A	224 V	Line B	225 V
---------------	-------	---------------	-------

Command

If the monitored object is an IRMS this display will be shown. Each socket shows its current state by changing its color: it may be off (gray), active and connected to the A input line (green), or active and connected to the B input line (blue). The display shows the status of the two input lines: *Input lines OK* = line good, *Blackout A/B* = line not good, and *Phase shift* = A and B lines have their phases shifted. It is also showed the load and the input voltage. The state of the socket can be changed with the button on the bottom, after the specified socket is selected. In particular, A and B buttons changes power source line, OFF button turn the socket off, and the RST button turn the socket off for a set time (configured on the IRMS) and then turn it back on.

DIAGRAM DATA (ONLY UPS)



This displays the detailed status of the UPS.

LOG

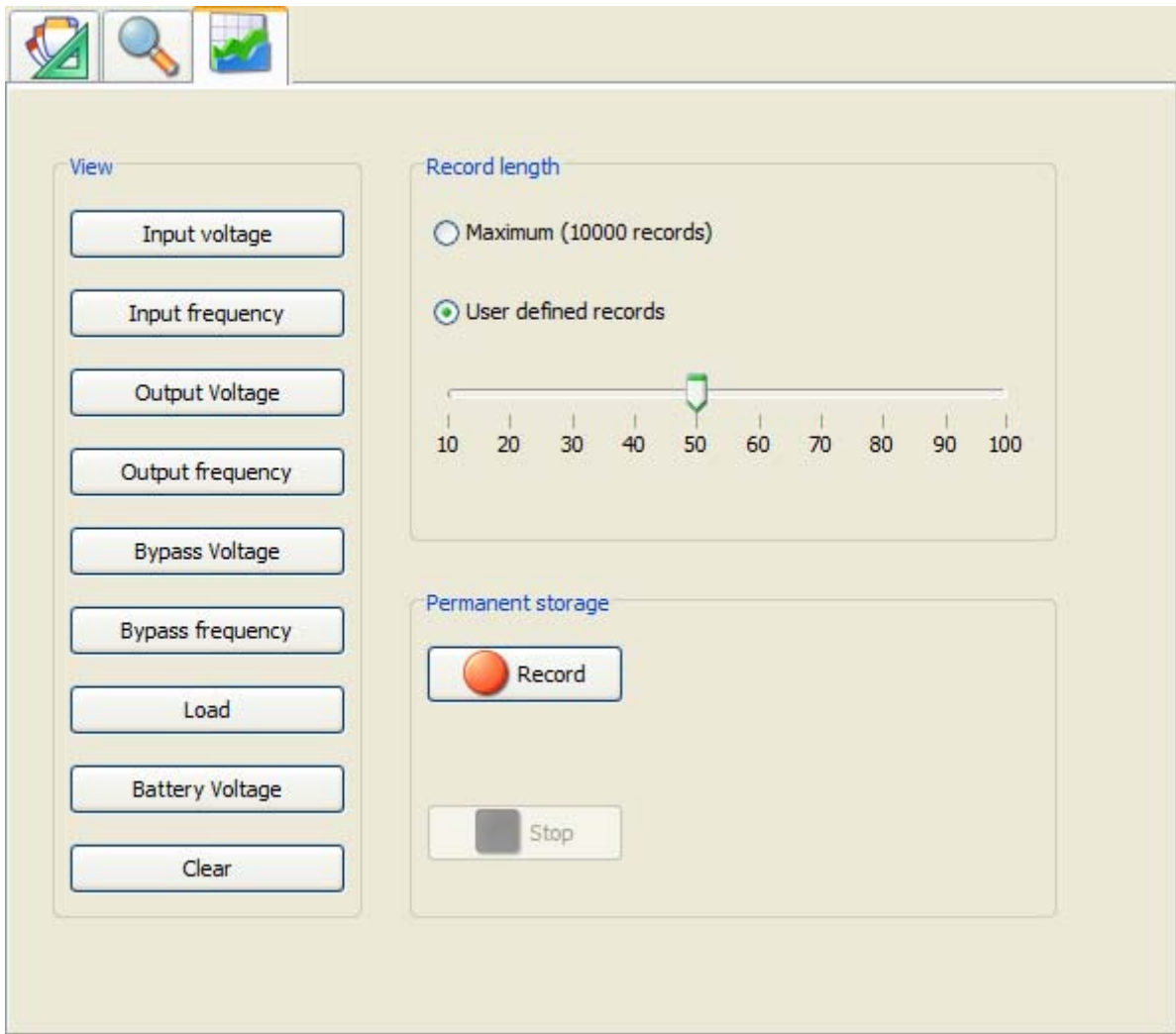
+/-	Gravity	Time	Device	Event
		Friday, September 4, 2009 11:33:03 AM		Event log started
		Friday, September 4, 2009 11:33:26 AM		Event log stopped
		Friday, September 4, 2009 11:33:40 AM		Event log started
		Friday, September 4, 2009 11:33:54 AM		Event log stopped
		Friday, September 4, 2009 11:33:57 AM		Event log started
		Friday, September 4, 2009 11:34:02 AM		Event log stopped
		Friday, September 4, 2009 11:57:29 AM		Event log started
		Friday, September 4, 2009 11:57:57 AM		Event log stopped
		Thursday, October 1, 2009 3:11:13 PM		Event log started
		Thursday, October 1, 2009 3:11:40 PM		Event log stopped
		Thursday, October 1, 2009 3:12:03 PM		Event log stopped
	Critical	Thursday, October 1, 2009 3:12:23 PM	Net4	Ups system off
		Thursday, October 1, 2009 3:12:29 PM		Event log stopped
	Critical	Thursday, October 1, 2009 3:13:23 PM	Netman plus	Device timeout
		Thursday, October 1, 2009 3:21:02 PM		Event log stopped
		Thursday, October 1, 2009 3:21:28 PM		Event log stopped
		Thursday, October 1, 2009 3:22:44 PM		Event log stopped
		Thursday, October 1, 2009 3:22:46 PM		Event log stopped
		Thursday, October 1, 2009 3:22:48 PM		Event log stopped
		Thursday, October 1, 2009 3:23:00 PM		Event log stopped
		Thursday, October 1, 2009 3:23:03 PM		Event log stopped
		Thursday, October 1, 2009 3:23:06 PM		Event log stopped
		Thursday, October 1, 2009 3:23:17 PM		Event log stopped
		Thursday, October 1, 2009 3:23:19 PM		Event log stopped
	Critical	Thursday, October 1, 2009 3:23:24 PM	Netman plus	Device timeout
		Thursday, October 1, 2009 3:23:35 PM		Event log stopped
		Thursday, October 1, 2009 3:23:36 PM		Event log stopped
		Thursday, October 1, 2009 3:23:40 PM		Event log stopped
	Critical	Thursday, October 1, 2009 3:23:43 PM	New object	Ups system off
		Thursday, October 1, 2009 3:23:55 PM		Event log stopped
		Thursday, October 1, 2009 3:24:10 PM		Event log stopped
		Thursday, October 1, 2009 3:24:38 PM		Event log stopped

Clear Export

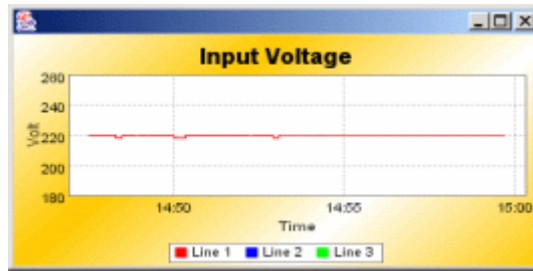
This shows the events of PowerNETGuard.

In order to have the events correctly registered it is necessary to configure this action.

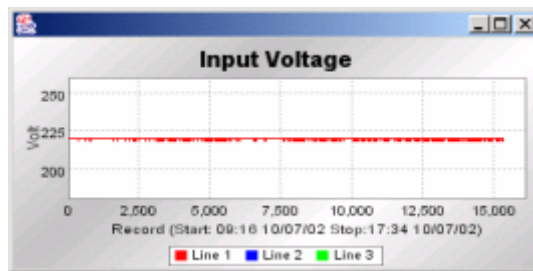
GRAPHICS



From this display the status history of the device being monitored can be analysed. During the “updated” visual display mode, PowerNETGuard gathers data on device status, especially the input/output/bypass/battery voltage, the load, and the input/output/bypass frequency. By pressing the buttons on the left the graphics that display the data gathered can be viewed. The number of data gathered is limited and old data is removed. This limit can be configured. These graphics have a gold background and are designed to display the recent history of the device. By making the menu appear (right-hand mouse button for Windows) one can zoom, save, or print the image.

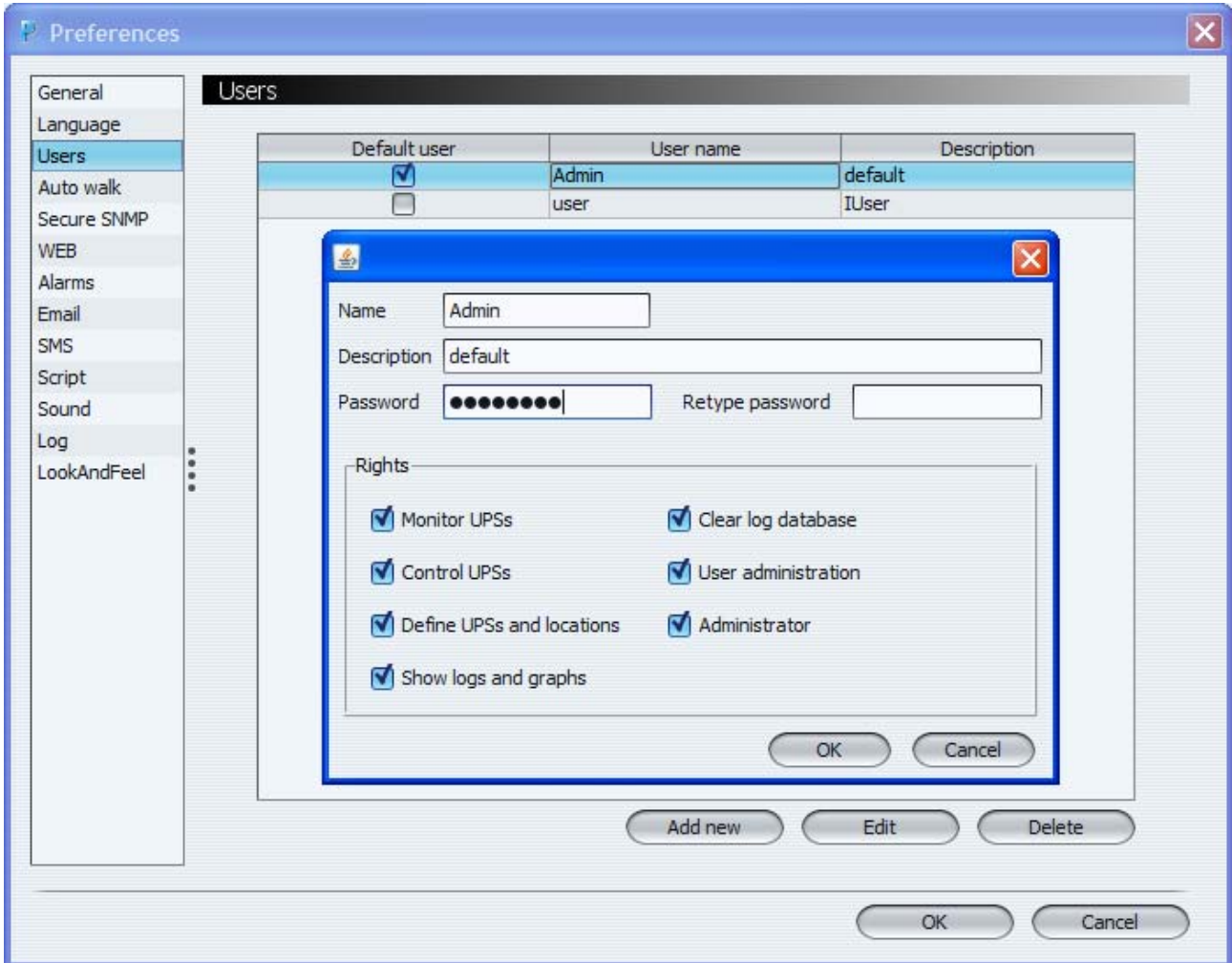


To monitor a long-term time interval the data can be saved on the hard disk so that it can be uploaded again later on. Recording can be started by pressing "Record" and stopped by pressing "Stop". It is worth noting that every time the record function starts, the data stored in the memory previously will be overwritten. Clicking on "Play" will load and display data. These graphics have a silver background.



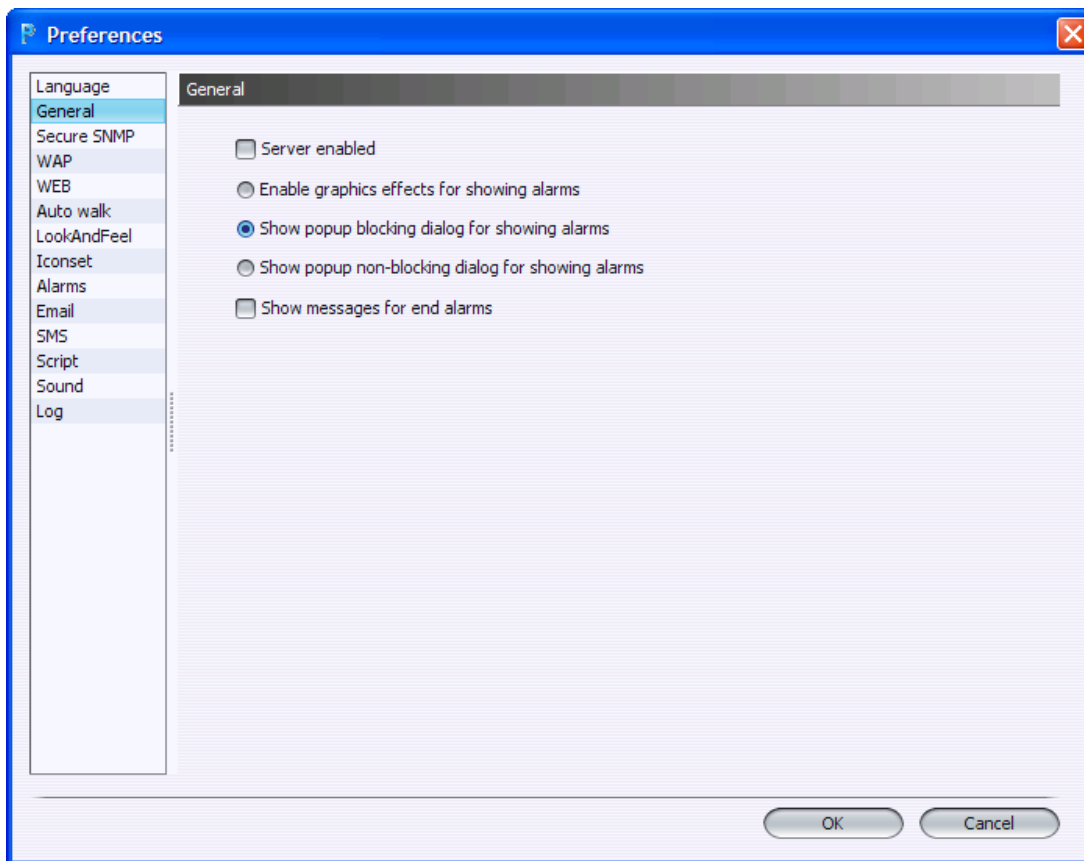
CONFIGURATION

USER CONFIGURATION



Here users and their rights can be configured by entering names, a brief description, and password and selecting the rights the user can be assigned: The user flagged as "Default user" is used during server mode. NOTE: if changes are made to user rights while in use, the changes will not become effective until after the user has logged out.

GENERAL CONFIGURATION



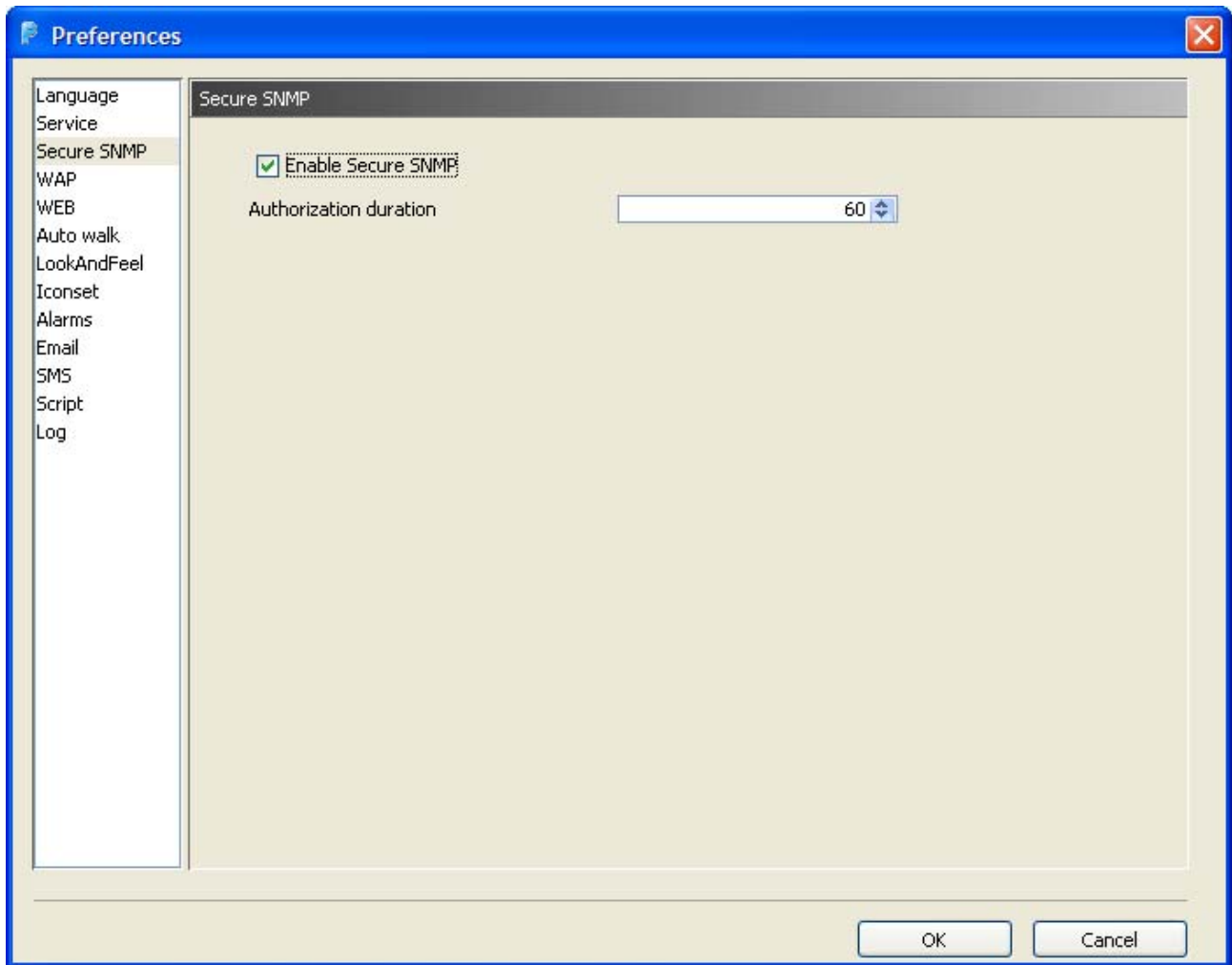
This panel allows to configure general parameters.

With the option “Server enabled” the logon is performed automatically with the default user; i.e. it is no longer necessary to insert the password at PowerNETGuard start. The default user owns the rights defined on the user configuration.

With the “Enable graphics effects for showing alarms” option enabled, the alarms are displayed by means of a prominent screen. With the option “show popup”, a popup notification window is showed (either blocking or not blocking the graphical interface).

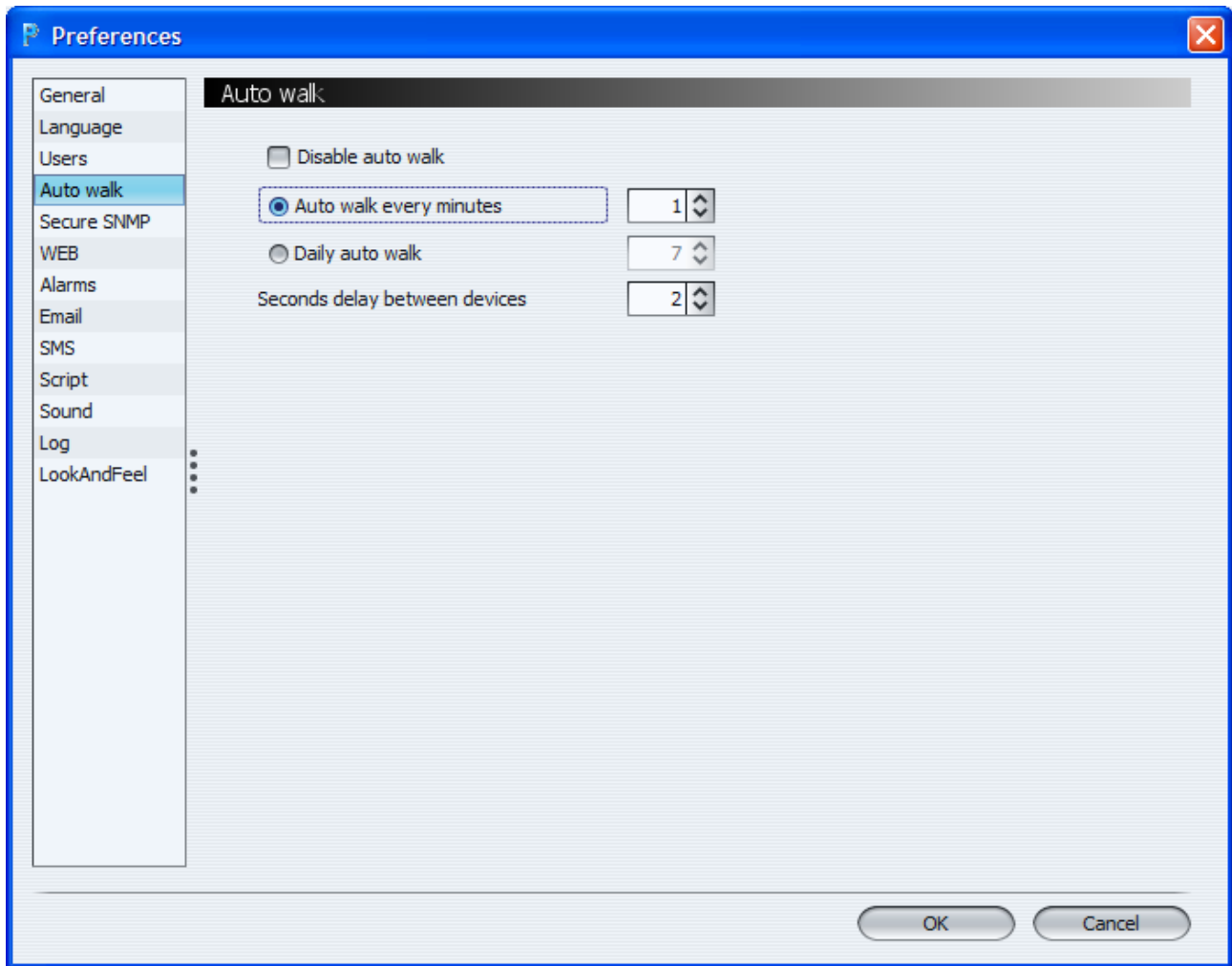
With the option “Show message for end alarms” also the end alarms will be showed.

SECURE SNMP CONFIGURATION



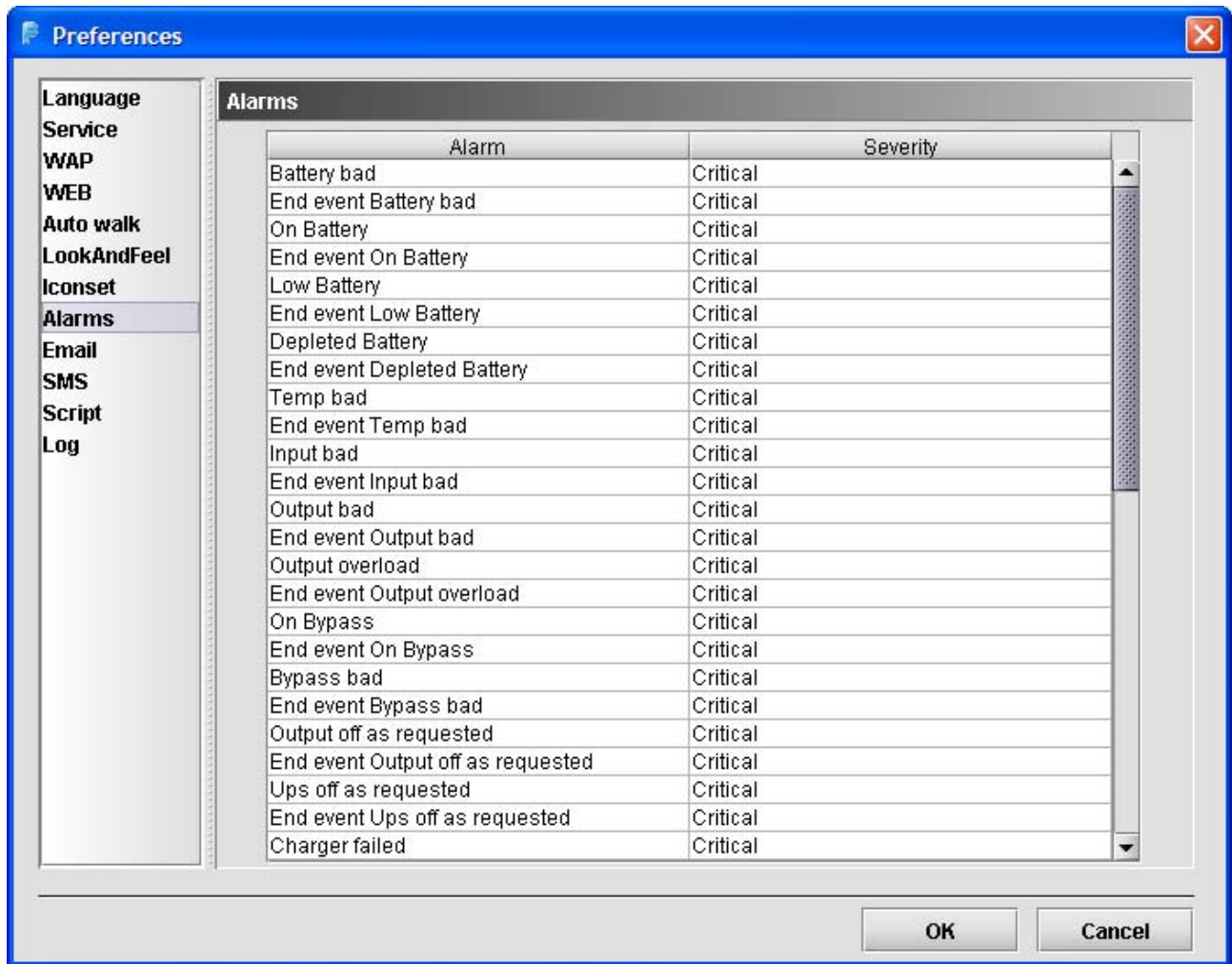
This panel allows to configure Secure SNMP. When disabled, PowerNETGuard will not lock the SNMP command but will use the predefined password for the selected object (SET Community). However, both the authentication and the authorization are performed on the remote host, therefore if Secure SNMP is enabled on remote but PowerNETGuard has this option disabled then the predefined password will not grant the required privileges.

AUTO WALK CONFIGURATION



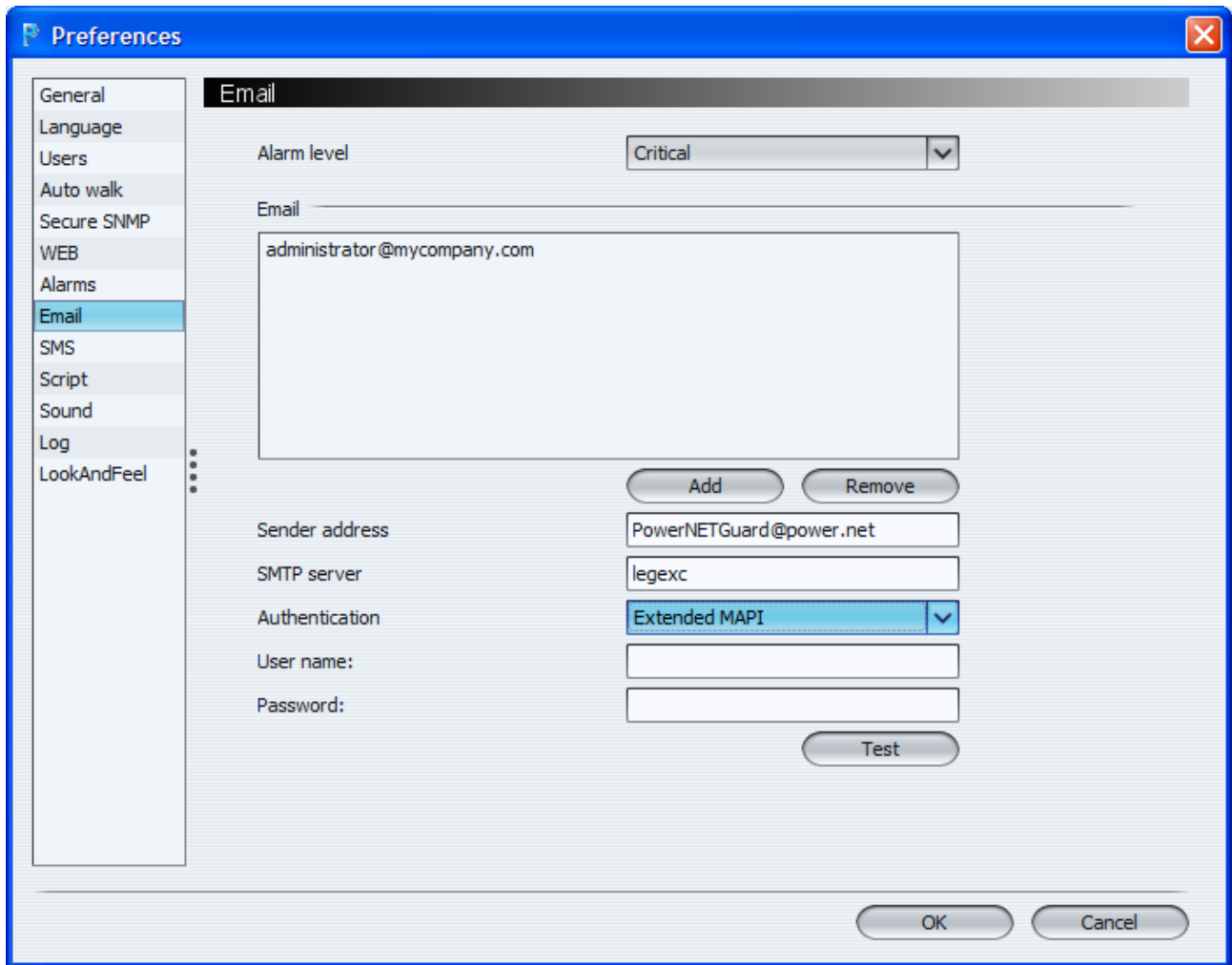
This panel allows to configure Auto walk. The devices are monitored automatically on the time interval defined and with the defined delay between the devices. It is also possible to disable this function.

ALARMS CONFIGURATION



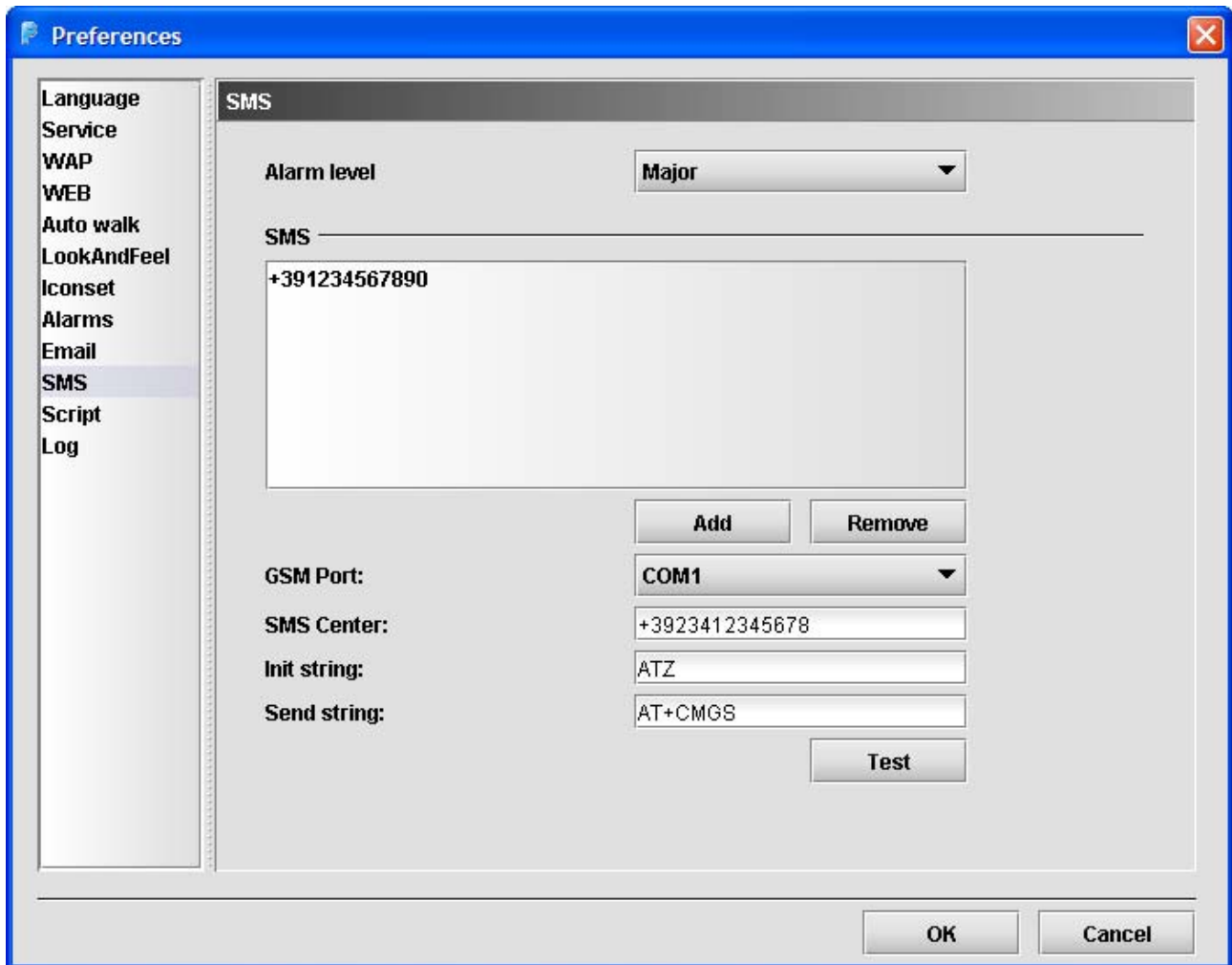
On this screen the alarm priority can be set. Then, for each priority level it will be possible to define the actions to be performed.

EMAIL CONFIGURATION



On this screen the email service can be configured. In particular for each priority level it is possible to define an address list for sending event notification emails. It is possible to configure the sender's email address and lastly it is possible to insert the address of the SMTP server used for sending emails. When required by the server, it is possible to insert the authentication data (username and password). Alternatively, is possible to use "Extended MAPI" for connecting to Microsoft Exchange servers. For testing the correctness of these settings, it is possible to send a test email.

SMS CONFIGURATION



On this screen the SMS service can be configured. In particular for each priority level it is possible to define a cell phone number list for sending event notification SMS. It is also possible to insert the serial port on which a GSM modem is present, the SMS centre number used for message sending and the init and send strings. For testing the correctness of these settings, it is possible to send a test SMS.

OTHER CONFIGURATION

For each alarm level, it is possible to execute a script, an audio file (MP3 or WAV) or register it on the log. The scripts are called with the parameters in this order:

1. Device name
2. IP Address
3. Type of alarm
4. Date and time
5. Estimated autonomy