ENGLISH
Ver. 2502.11

SNMP06 LAN CARD
&
SNMP WEB PRO COMMUNICATION INTERFACE

USER MANUAL

NOTE: NOT VALID FOR EQUIPMENT SUPERVISED VIA RS232/USB PORT.

TABLE OF CONTENTS

1. OVERVIEW.

1.1. Introduction.

SNMP LAN card and its **SNMP Web Pro** interface can monitor and control XMART UPS, Inverters, STA and XSI Solar inverters in network environment, including LAN and Internet. Also supports Xmart Environmental Monitoring Devices showing data and alarms, as well as sending SMS and e-mails.

This manual shows all information regarding installation and operation of SNMP card in Xmart UPS and Inverters. For STA, info is available in **APPENDIX A** of this manual, and regarding XSI Inverters, all necessary info is in in **APPENDIX B**.

EXTBOX-SNMP06 accessory (to communicate over the network with Xmart devices with RS232 ports) includes an SNMP card, so **SNMP Web Pro** is also its native interface and all information described in this manual is also valid for accessory EXTBOX-SNMP0.

Integrated with Shutdown Wizard, **SNMP Web Pro** can prevent data loss from power outage and safely shutdown systems, as well as store programming data and scheduled UPS shut down. All UPS warning and fault event records can be kept in **SNMP Web Pro**.

Along with Monitoring and Control Software, **SNMP** offers monitoring and remote access to all equipment with SNMP card in a LAN or INTERNET. For the detailed operations. Next table shows specific software for each product family:

Product Family	Software
Optima y XBU-SW-LCD	ViewPower Pro
XSI-120-1K a 3K // XSI-230-PWM-1K a 5K // XSI-230-MPP-1K a 5K	WatchPower
Inversores Solares (XSI) de Capacidad de 6KVA y Superior	SolarPower Pro
STA	ATS Monitor

References to Supervision Software will refer to the specific software for the supervised equipment and detailed information about handling of each software is in its User Manual, which can be downloaded from **Downloads** section of our website: **www.xmart- ups.com**.

1.2. Features.

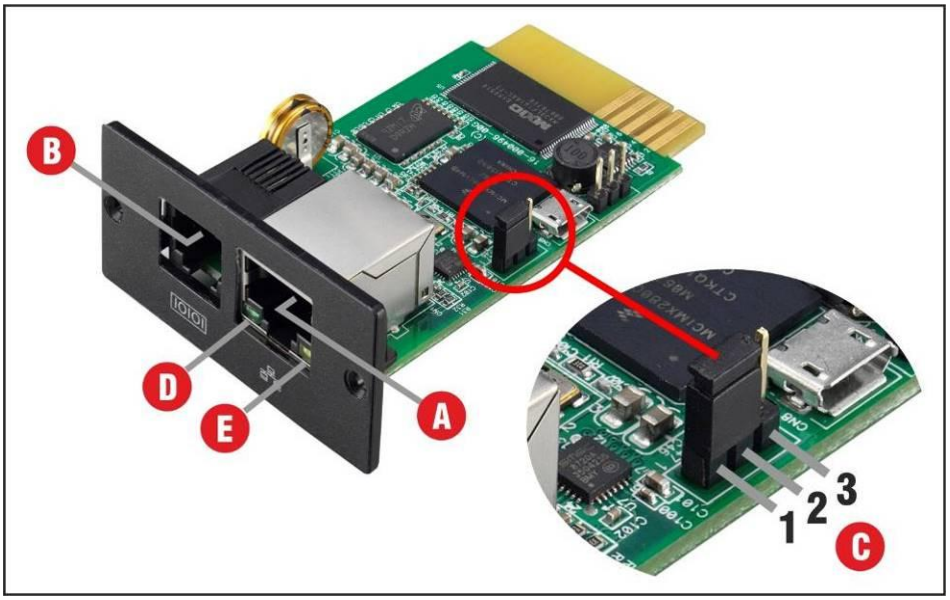
1. Device operation monitoring via Web Browser.
2. Offers SNMP MIB to monitor UPS status.
3. 10M/100M autodetection speed
4. Wake-On-LAN function Support.
5. Communication for LAN Ethernet under protocols TCP/IP, UDP, SNMP, SMTP, SNTP, HTTP, HTTPS, SSL, SSH, IPV4/IPV6, DHC, etc.
6. Safe shutdown of equipment and systems to prevent data loss on power outage, when integrated with Shutdown Wizard.
7. Connection to external XMART environmental sensor to acquire temperature/humidity data (RJ11).
8. Data logging up to 200.000 events/alarms, including warnings, faults, and XMART environmental sensor warnings, operations data logs from either **SNMP Web Pro** or software used. Stored date is safe even during power outage.
9. Daily reports for event log and data log.
10. Unit scheduled on/off and battery test.

1.3 Description.

SNMP Web Pro communicates with all monitored devices via SNMP Card, therefore, it is important to understand SNMP card in detail, to assure software proper operation and management.

SNMP is a powerful and versatile communication LAN card for XMART UPS, Inverters, STA, and Solar Inverters, including:

- Communication for LAN Ethernet under protocols TCP/IP, UDP, SNMP, SMTP, SNTP, HTTP, HTTPS, SSL, SSH, IPV4/IPV6, DHCP, etc.
- Connection to external XMART environmental sensor to acquire temperature/humidity data (RJ11).
- 10M/100M autodetection speed
- Internal data logging up to 200.000 events and alarms.
- Interface to monitor and control main parameters of UPS or STA.
- Equipped with real-time clock with 7 days runtime without power.
- Small size: 42x80mm



A: LAN Ethernet Connection (10/100MB)
B: Sensor TH / GSM Connection
C: Reset Jumper: To reestablish default values: (1-2): Normal / (2-3): Reset: Check **Note 1**
D: LED green = ON: 100MB / OFF: 10MB
E: LED yellow = ON: connection detected / OFF: connection not detected

NOTE 1 – RESET: Reset function restarts card to factory parameters and eliminates user passwords.
To apply a reset, follow this procedure:

1) Remove card from UPS and set jumper between pins 2 & 3 (see previous image)
2) Insert card into the UPS and **wait for 5 minutes** while reset is performed.
3) Remove card from the unit again and set jumper between pins 1 & 2.
4) Reinsert card into the unit and **wait for 5 minutes** while card restarts with factory setting.

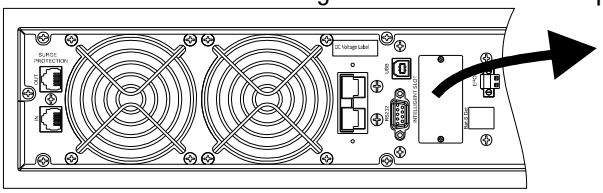
Factory setting after reset:
IP: 192.168.102.230 (STATIC IP) ;
Subnet Mask: 255.255.255.0 ;
Default gateway: 192.168.102.1
Password: 12345678

1.4. SNMP Card Installation.

This section describes installation and operation of SNMP Cards in UPS and inverters. For installation and y operation in STA, refer to **APPENDIX A** of manual. For installation and y operation in XSI Inverters, refer to **APPENDIX B** of this manual.

SNMP card must be correctly installed for **SNMP Web Pro** to operate properly, therefore please read, and understand carefully following procedure before installing SNMP Card.

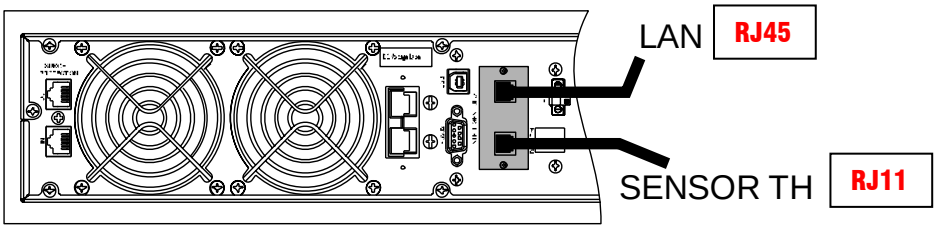
1: Remove cover from Intelligent Slot in the UPS rear panel, as shown in the next figure



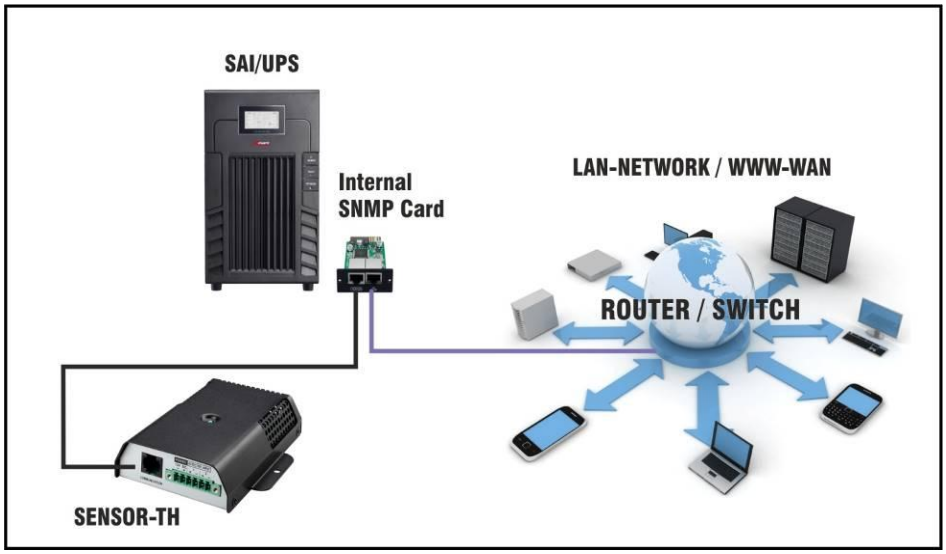
2: Check jumper "C" is between pins 1 & 2 in the card

3: Insert SNMP Card in Intelligent Slot and tight the screws to fix it to UPS rear panel.

4: Plug RJ45 cable in the Ethernet port of the card and connect other side to the network socket. Check if yellow LED lights as expected. See next figure as reference.



If there is a Sensor-TH to be installed, connect it to RJ11 port in the card according to previous figure.
We strongly suggest checking Sensor-TH manual.



1.5. Communication.

There are 2 ways to communicate with SNMP cards:

A. Using XMART UPS monitoring software (See section **1.1 Introduction**, in this manual)

B. From a WEB Browser (Explorer, Firefox, Chrome, etc.) typing IP address of SNMP card.

A. MONITORING AND CONTROL SOFTWARE

Monitoring software offers all kind of control and monitoring functionality for all XMART devices in the network. Software communicates any PC with any XMART device in the same network. It also provides functions to power off/on UPS in real time. Shutdown Wizard installed in PC allows controlled shutdown of PC when an event is detected by the software. Software also provides logging capabilities for data, events, and alarms. Monitoring software can be downloaded from our WEB Site **www.xmart-ups.com**, along with User Manual for more information.

B. COMMUNICATION FROM INTERNET WEB BROWSER

User can monitor and control any XMART device in the network from any PC installed in same network by contacting SNMP card from internet explorer. To do so, enter the SNMP card IP address in the WEB Browser Address Bar to open **SNMP Web Pro** interface. This is the way described and explained in this manual. SNMP card can storage data and events in its internal memory with external software. SNMP can also send messages and alarms by email if there is a router in the network with open access to internet.
If SNMP is installed in a DHCP network, it will receive dynamic IP address from the network.
If SNMP is installed in a static network, then network administrator must assign IP to the card. **Please check section "ESTABLISHING COMMUNICATION IN STATIC IP NETWORKS" further in this manual.**

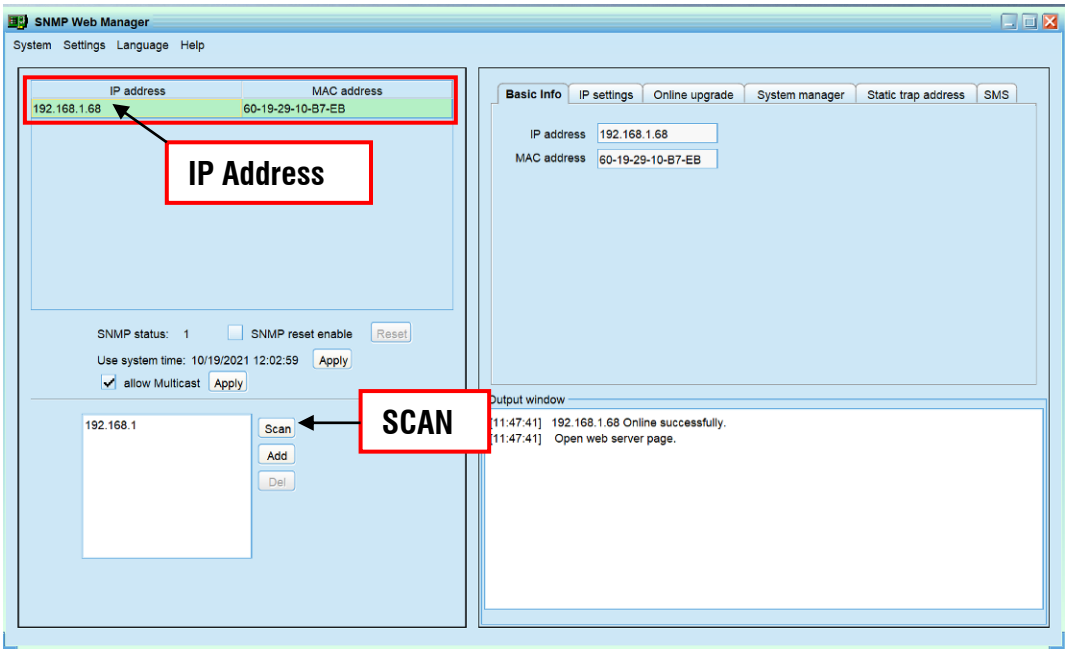
SNMP WEB MANAGER

SNMP Web Manager is a service software to scan and detect all SNMP Card in the network, it can be downloaded from Download\Software section in our web site: www.xmat-ups.com.

Once successfully installed, there will be a Shortcut Icon on your desktop, like the one on the right:

When executed, SNMP WEB Manager interface will show, as in the next figure:

SNMP WEB MANAGER INTERFACE



ESTABLISHING COMMUNICATION IN DHCP NETWORKS

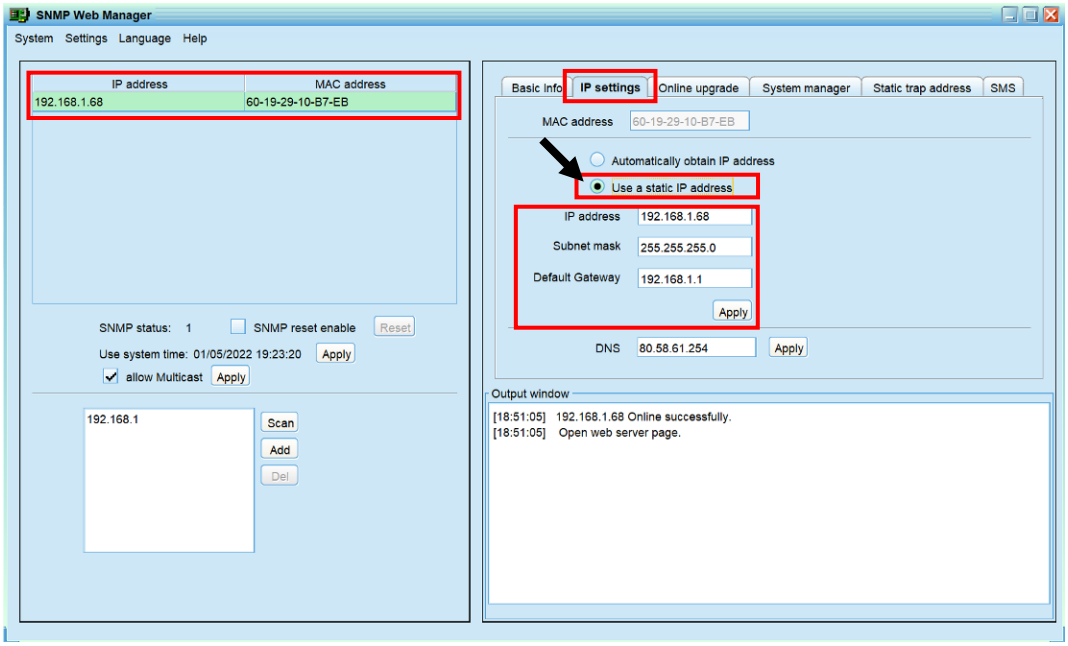
To know which IP address has been assigned to SNMP card by DHCP network, click "Scan" button. On the left area you will find IP and MAC addresses available in the network, as shown in previous image:

This process could take some minutes. Sometimes SCAN must be performed several times, to detect all cards.

ESTABLISHING COMMUNICATION IN STATIC IP NETWORKS

If the network where UPS is connected is static IP network, then Network Administrator must assign an IP to SNMP card, for being the one responsible for network safety restrictions. This is the Static IP Addresses assignation procedure:

1. UPS with SNMP card must be ON
2. One PC with **SNMP Web Manager** must be connected to the SNMP card directly by a RJ45 cable, without passing thru any router. There are recent SNMP cards that can be detected though the network. For those cards PC can be connected to the network and try to contact the SNMP card.
3. **SNMP Web Manager** must detect card automatically. If not, a manual SCAN must be done. This scan process could take between 2 to 5 minutes. Repeat scan if it is necessary.
4. Select the IP shown in the left area of the **SNMP Web Manager** screen. See next figure for reference.



5. Open IP SETTINGS tab and select option: “Use a Static Address”.

   NOTE: If system does not allow modifications, do SCAN again, and repeat previous steps.

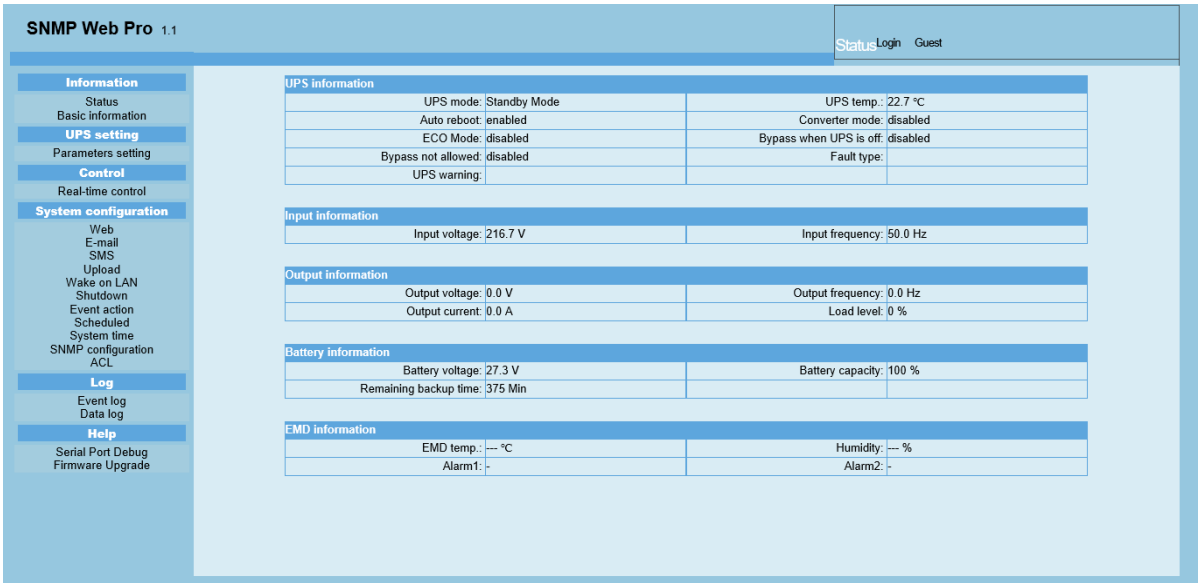
6. Manually enter static IP address, Subnet mask y Default Gateway.
7. Click on APPLY button to save modifications.

System could ask you a password. In that case introduce password: **12345678**. Then select APPLY again to save modifications. System must show following message: “OPERATION SUCCESSFULL”

Once you know SNMP Card IP Address, there are 2 ways to monitor it:

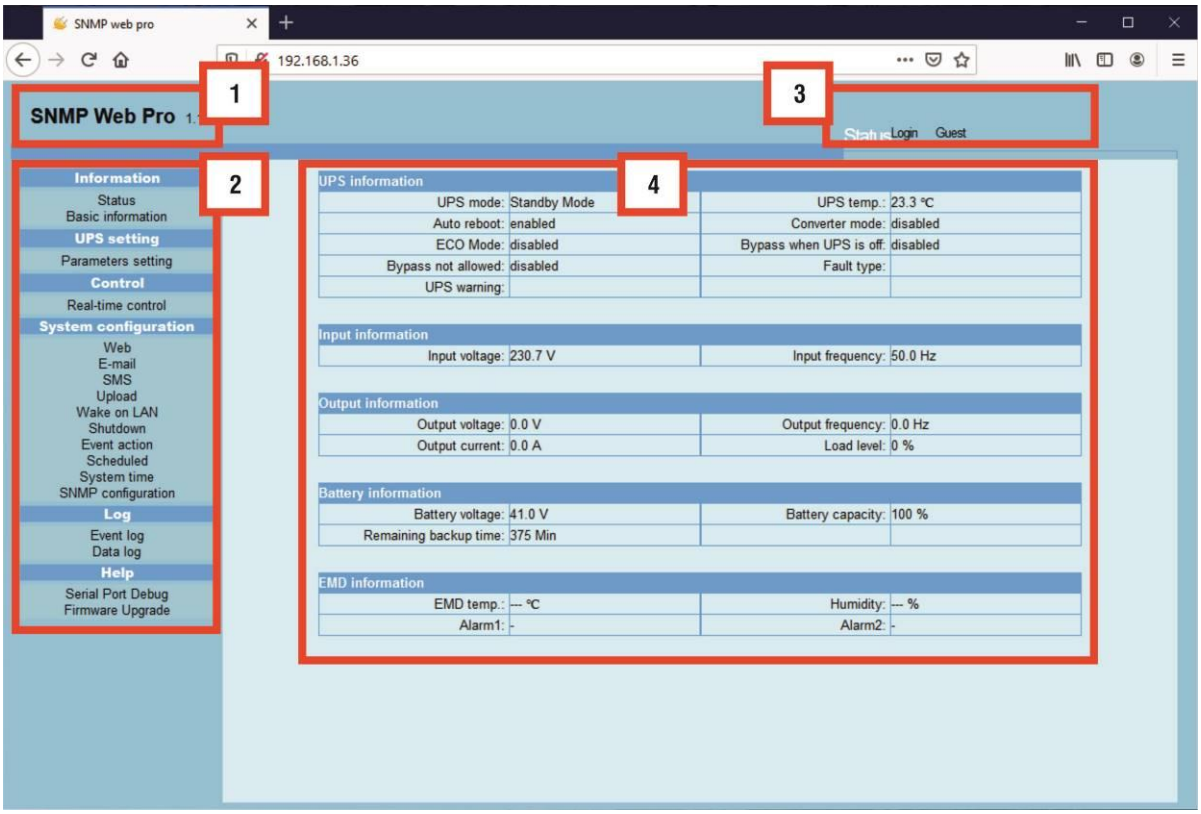
- Doble clicking selected IP Address on **SNMP Web Manager**.
- Entering IP Address in your WEB Browser Address Bar.

Either way your WEB Browser will open a WEB Page to show **SNMP Web Pro** interface, communicating with identified SNMP card. See next figure for reference.



2. SNMP WEB PRO INTERFACE.

SNMP Web Pro Interface allows you to access, monitor, configure, and control your UPS. Next figure shows each area location:

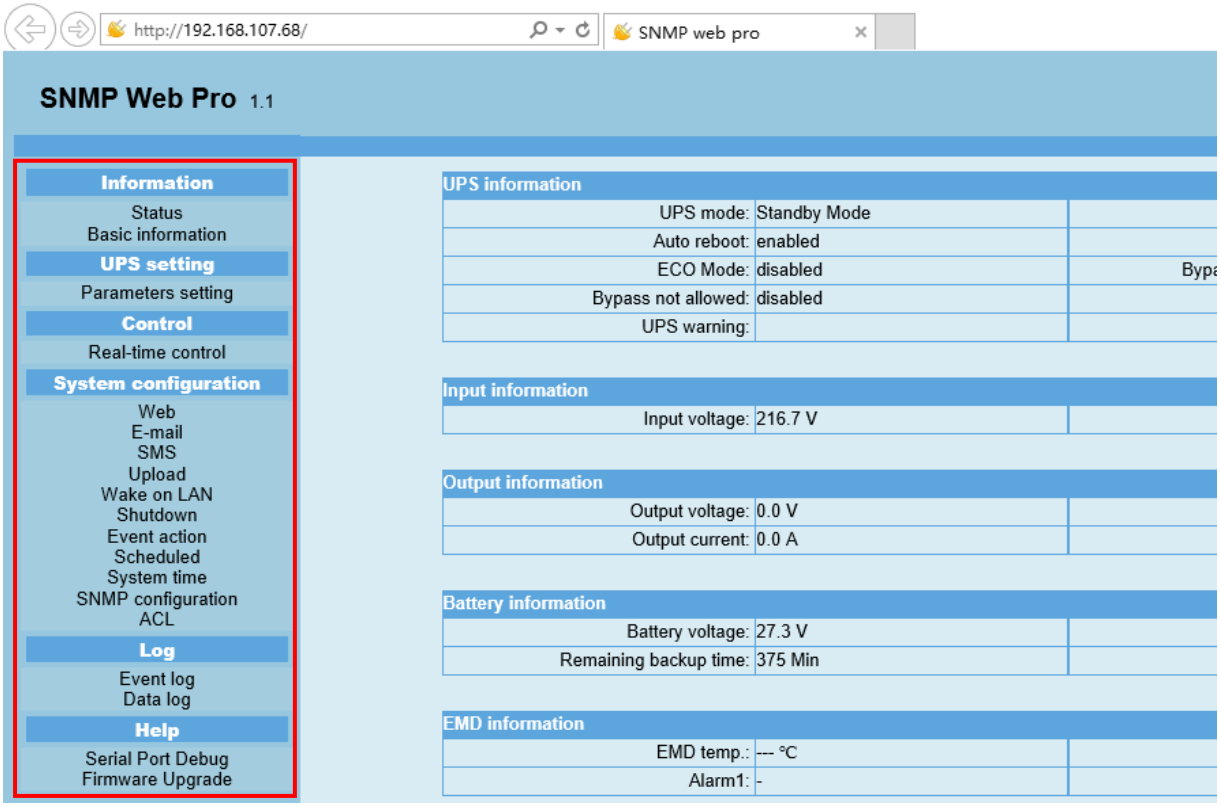


2.1 Interface Areas Identification

According to previous figure, these are interface operational areas:

1. **SNMP Web Pro** Version
2. Function Area
   In this area you can control and configure UPS, communication, and **SNMP Web Pro** parameters.
3. Login Area
   Here you can see the current user level. Administrator User is the highest priority level. Password to login as Administrator is **12345678.**
4. Information Area
   Sensitive area which shows a wide variety of data and fill-in fields, according to function selected in function area.

3. FUNCTION AREA.



Previous figure shows Function Area in SNMP Web Pro Interface. In this section you will find detailed information about each function.

3.1. INFORMATION

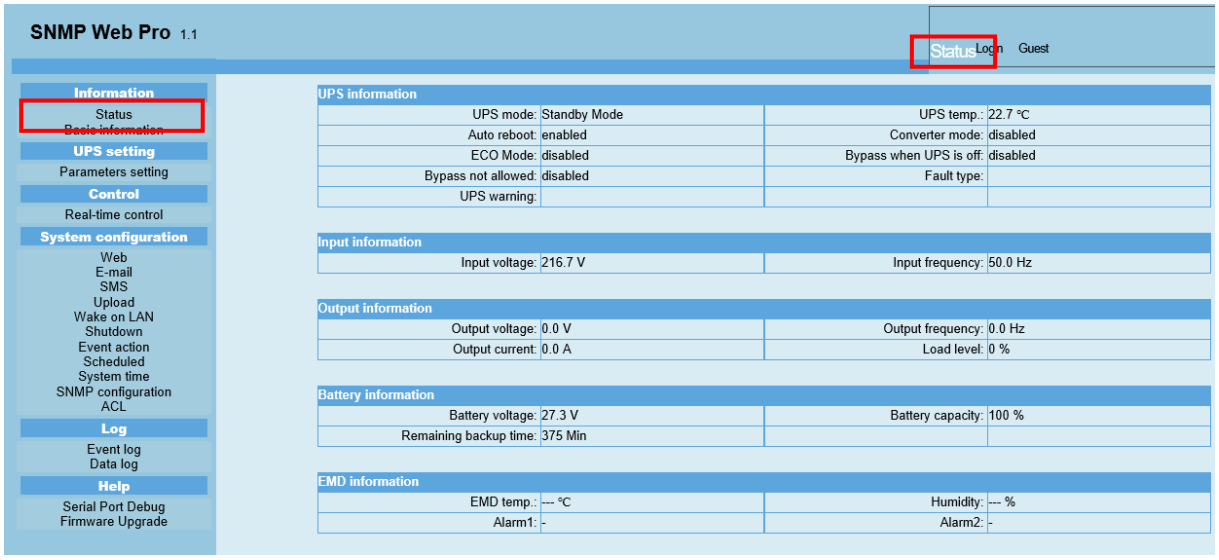
This function shows UPS operational data, separated in two groups.

3.1.1. STATUS

This section offers information about the UPS, such as:

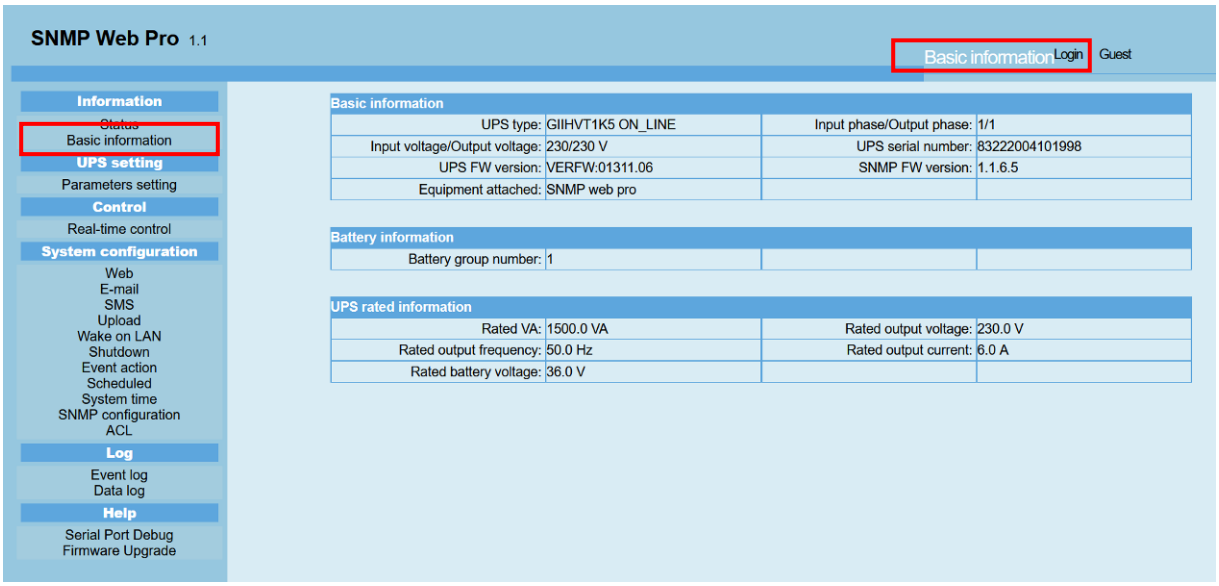
- Operation mode and main parameters
- Input values: Voltage and Frequency
- Output values: Voltage, Frequency, Current, Load connected to UPS, etc.
- Battery information
- Temperature and Humidity (only if Sensor-TH is connected to the SNMP card)

See next figure for reference:



3.1.2. BASIC INFORMATION

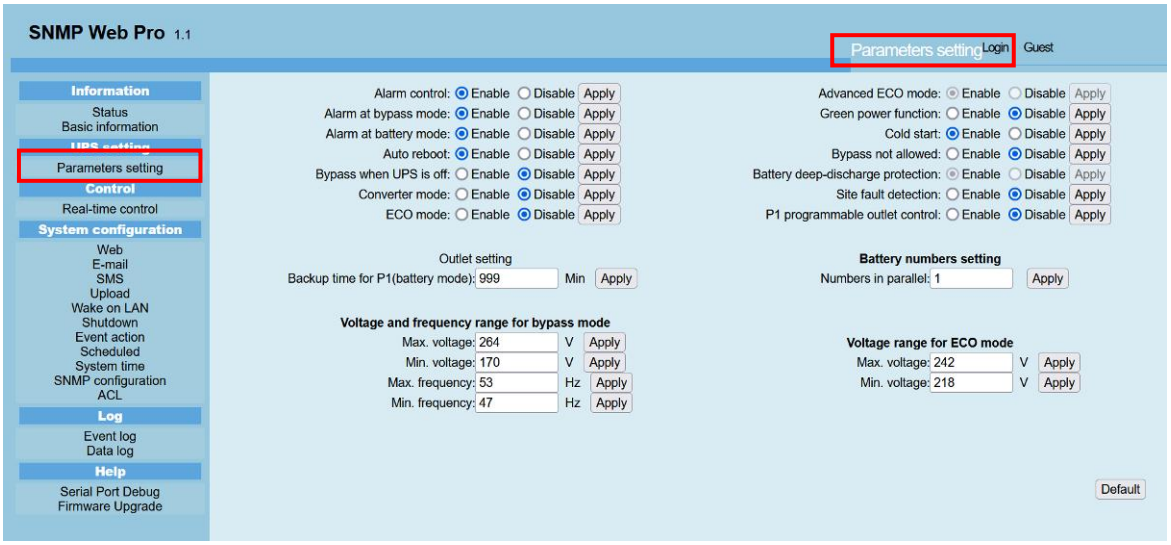
This section provides information about UPS technology, rated values (Capacity, Voltage, Frequency, Current), number of batteries, and the type of SNMP card connected to UPS. See next figure for reference:



3.2. UPS SETTINGS

Parameters Setting

UPS Parameters can be checked and modified in this function. See next figure:



We strongly recommend checking UPS manual, for detailed explanation about each parameter to be adjusted.

Parameters to be adjusted:

Alarm Control:
Enable/Disable audible alarm (beep)

Alarm At Bypass Mode:
Enable/Disable audible alarm (beep) for bypass mode.

Alarm At Battery Mode:
Enable/Disable audible alarm (beep) for battery mode.

Auto Reboot:
Enable/Disable auto-reboot function when AC service comes back from long blackout.

Bypass When UPS is OFF:
Enable/Disable bypass mode when UPS is OFF but connected to AC service.

Converter Mode:
Enable/Disable frequency converter function.

ECO Mode:
Enable/Disable ECO mode.

Battery Open Status Check:
If enabled, monitored UPS will check if the battery connection is ok upon power up.

Green Power:
Enable/Disable green-power function allowing UPS automatic shutdown when in battery mode and no load is connected to UPS outlets.

Cold Start:
Enable/Disable cold-start function to allow UPS to start-up in battery mode.

Bypass Not Allowed:
Enable/Disable BYPASS function. If activated (NOT ALLOWED), UPS never will switch to bypass mode. If inactive (ALLOWED) UPS will go to bypass mode depending on internal configuration.

Battery Deep-Discharge Protection:

If activated, UPS will shut down when Deep protection Battery level is reached. This level is usually configurable and higher than standard low battery level.

Site Fault Detection:

If activated, UPS will generate beep alarm if site wiring problem is detected. Usually, Line and neutral swapped.

P1 Programmable Outlet:

If activated, UPS will turn-off programable outlets according to internal configuration. See backup for P1 parameter.

Backup For P1:

Backup for programable outlets in minutes.

Battery Number in Parallel:

Allows user to fix the number of Battery Packs connected in parallel (internal + external batteries).

Voltage & Frequency Range for Bypass

MAX - MIN Voltage:

Acceptable voltage range for bypass mode. When UPS is in bypass mode and input is out of this range, UPS switches to battery mode.

MAX -MIN Frequency:

Configures frequency range for bypass mode. When UPS is in bypass mode and input is out of this range, UPS switch to battery mode.

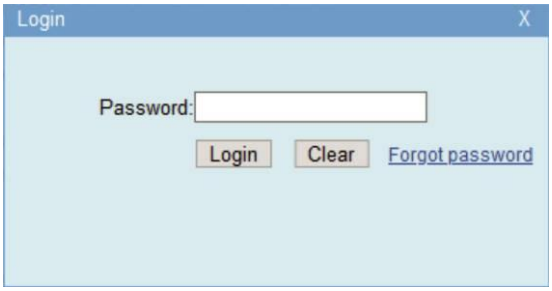
VOLTAGE RANGE ECO

MAX - MIN Voltage:

Configures voltage range for ECO mode. When UPS is in ECO mode and input is out of this range, UPS switches to online mode.

IMPORTANT NOTES:

- You will not be able to change parameters, unless logged in as Administrator. Trying to do so will show a dialog window like the following:



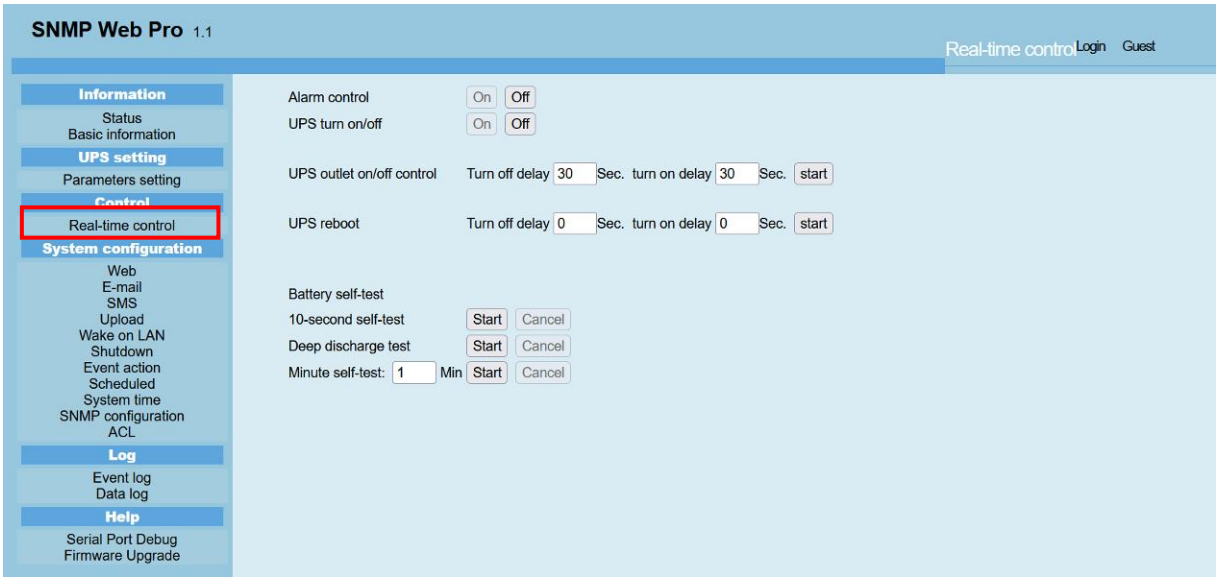
Enter your password (Default **12345678**) and click “Login” button.

- After each single change, click on “Apply” button to save changes, otherwise changes will be lost.
- Some parameters might not me available, according to UPS model.
- Numbers can be written directly in any field.
- Click on Default button to recover factory settings.

3.3. CONTROL

Real Time Control

Allows real time control. UPS can be turned-off and turned-on, alarm mute, battery tests, etc., see next figure for reference.



Alarm Control:

- On: Activates the UPS alarm immediately, in case it was previously deactivated, it works only if the unit is in Alarm Mode.
- Off: Disables the UPS alarm immediately, it works only if the unit is in Alarm Mode.

UPS Turn On/Off:

- On: Turn on the UPS immediately.
- Off: Turn off the UPS immediately.

UPS Reboot:

- Turn Off Delay: Time for the UPS to turn off, once the "Start" button has been pressed.

  Multiples of 60 Seconds should be used: 60, 120, 180, 240 and so on, until reaching the maximum, which varies depending on the UPS model. An intermediate value between 60 and 120 will be interpreted as 60, one between 120 and 180 will be interpreted as 120, and so on.

  - Up to 3KVA UPS: Maximum shutdown time is 10 min. (Up to 659 Sec.)
  - 6KVA UPS and above: Maximum shutdown time is 99 min. (Up to 5.999 Sec.)

- Turn On Delay: Time that must elapse for the UPS to turn on again, after having been turned off by the Turn Off Delay function.

  Multiples of 60 Seconds must be used: 60, 120, 180, 240 and so on, up to 599,940 seconds, equivalent to 9,999 minutes. An intermediate value between 60 and 120 will be interpreted as 60, one between 120 and 180 will be interpreted as 120, and so on.

  If the two values entered are valid for the equipment, after clicking the "Start" button, SNMP Web Pro will respond with the message "OPERATION SUCCESSFUL", otherwise it will respond with the message "OPERATION FAILURE".

BATTERY SELF TEST:

3 different immediate battery self-test are available:

- 10 seconds test
- Deep discharge test
- User defined test, running during selected minutes.

Either if a command is successfully done or if it fails, SNMP Web Pro confirms it with a message window.

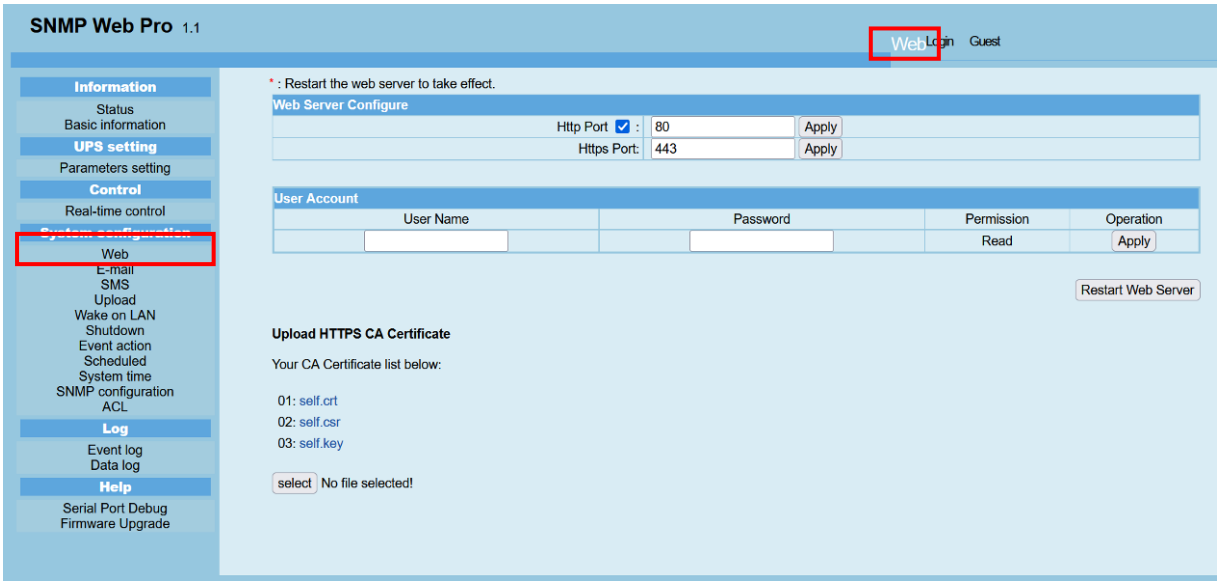
3.4. SYSTEM CONFIGURATION

Main system operating parameters are configured in this section, regarding communication, Shutdown, communications protocols, actions, logs, among others.

3.4.1. WEB

Adjustments here are significant, so after each change is made, Web Server must be restarted to activate modifications.

This section is divided in 3 areas, as follows (see next figure as reference):

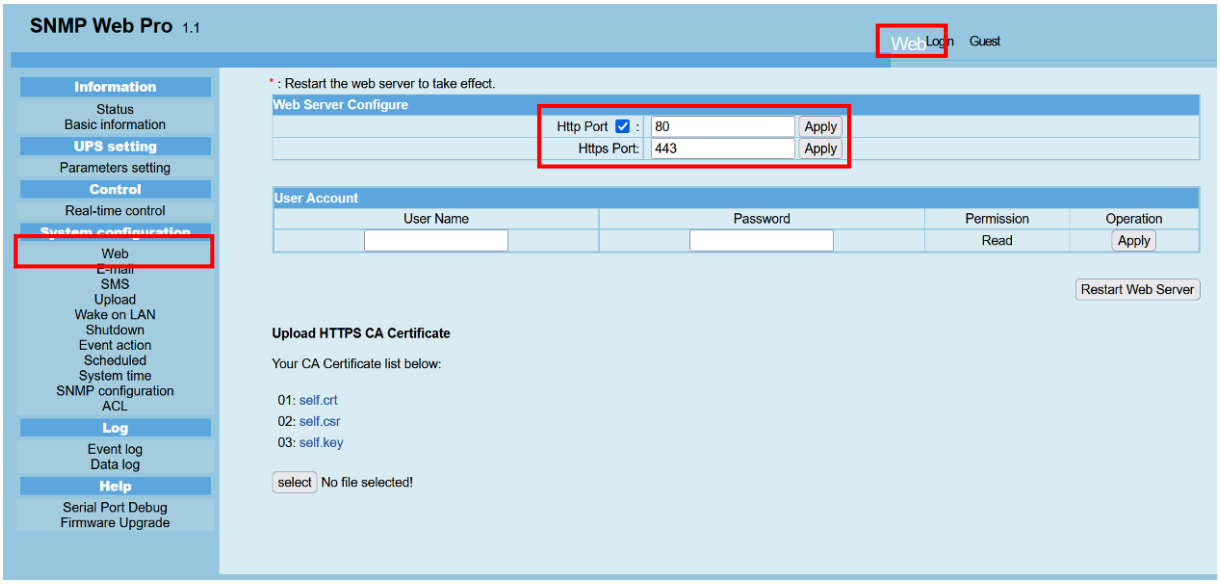


1. **Web Server Configure:** SNMP06 supports **Http** and **Https** protocols, and this can be configured in this section. This procedure will be explained later.
2. **User Account:** Configure authority to access **SNMP Web Pro**. Enter Username and password in each field, then select APPLY to save changes.

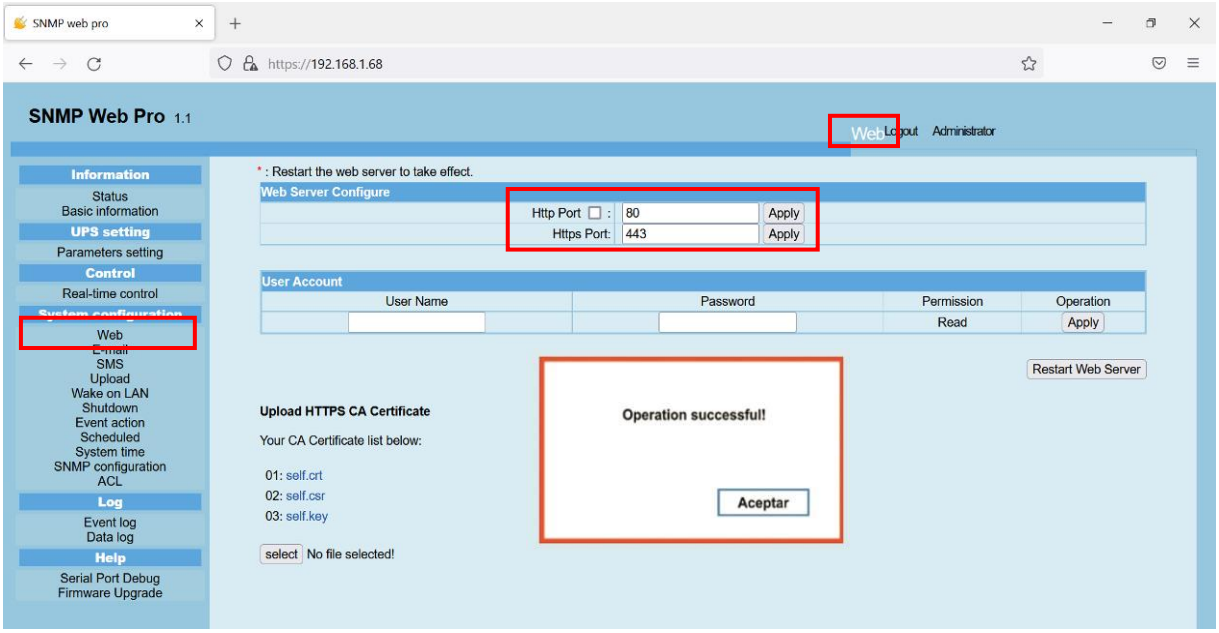
   After all information has been entered, click “Restart Web Server” button to restart web server and activate modifications.
3. **Upload HTTPS CA Certificate:** Click “Select” button to browse and look for HTTPS CA certificate directory and upload the files.

ACTIVATING HTTPS PROTOCOL:

Factory setting for SNMP06 is **Http**. To operate only under **Https** protocol, Http port 80 must be disabled. Otherwise, card would communicate under any of these 2 protocols. See next figure for your reference:

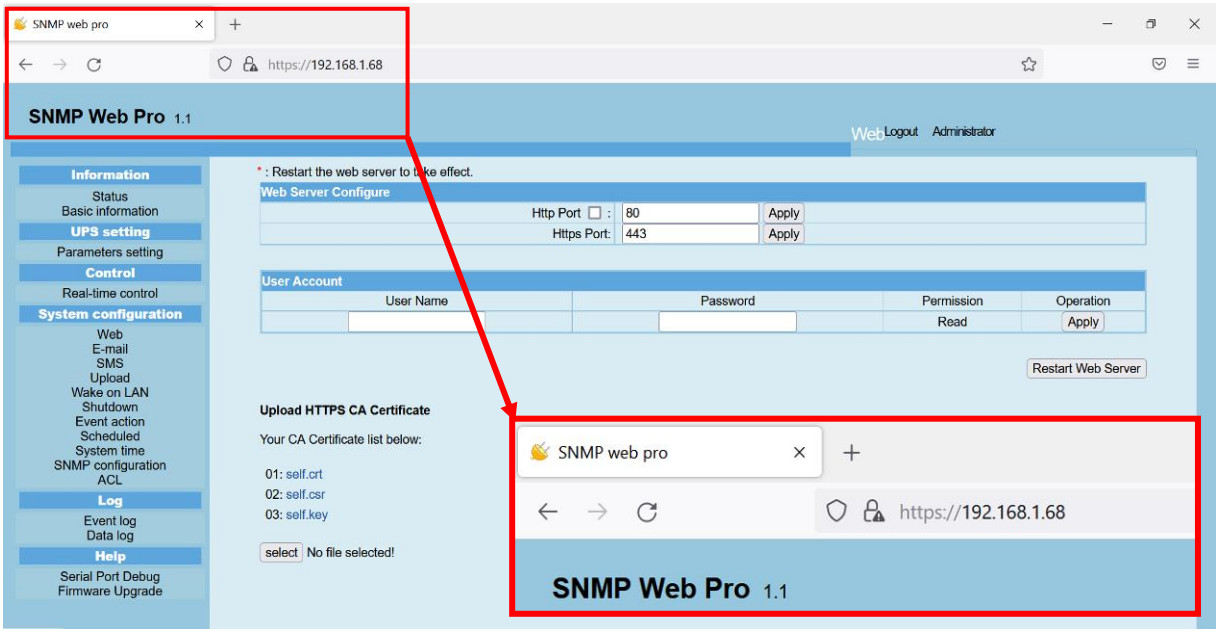


1. Make sure you have already logged in as administrator by introducing password: **12345678**. Otherwise, modifications are NOT allowed.
2. Uncheck option Http Port and select APPLY to disable port 80. Only if port 80 is disabled, card will be forced to communicate under Https protocol. A message OPERATION SUCCESSFUL must be shown. Select Accept button. See next figure as reference.



3. Click “Restart Web Server” button to restart web server and activate modifications.
4. **Wait about 30s to save changes** and update Web Browser with <F5> key (in Windows®). Web Browser must response with a message indicating communication is lost. This is because port 80 is disabled and HTTP communication is prohibited.
5. At this moment you can check if HTTPS protocol is active by introducing in the Web Browser bar address, the IP Address of the card preceded by https://

   For instance: **https://192.168.1.36**
6. Web Browser will open **SNMP Web Pro** interface under HTTPS as seen in the next figure

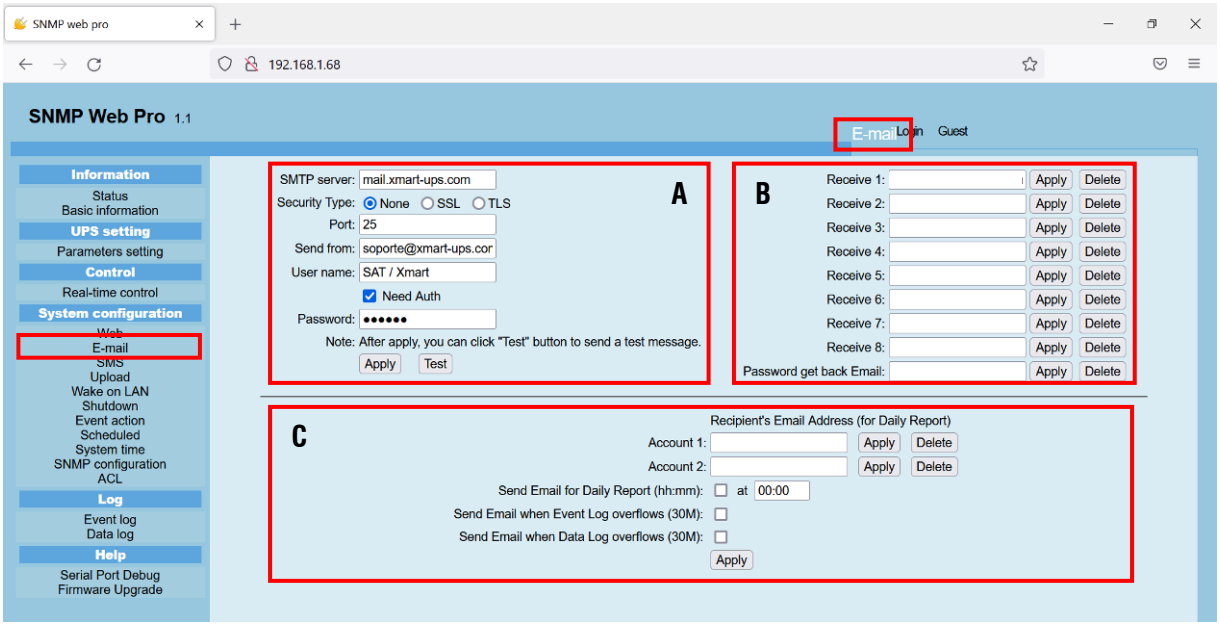


3.4.2. E-MAIL

SNMP card can send emails using accounts based on SNMP, SSL, or TTL servers. In this section all parameters can be configured, such as: email server, email account, password, receivers, etc.

If your mail server has a two-step verification method to access the account, go to **APPENDIX F** of this manual; otherwise, continue in this section.

All values are Default empty. See next figure as reference:



- **Area A**: E-mail sender account
- **Area B:** Up to 8 e-mail receiver accounts. After each entry, click Apply button to save data. "Delete" button eliminate selected Phone number.
- **Area C:** E-mail account to receive Daily Report, as well as Event Log Overflow and Data Log Overflow, clicking on respective check boxes.

Keep in mind that for each entry, you must click on Apply button, for changes to be saved, otherwise changes will lose.

CONFIGURING EMAIL SENDER:

SMTP server:	email server to be used to send emails. For instance: **smtp.gmail.com** for Gmail®
Security Type:	Type of email server to be used: **NONE:** Usually for web-domain email servers. **SSL:** For servers with security SSL like Gmail, Yahoo, etc. **TLS:** For emails servers with TLS security.
Port:	Depends on Server type. Usually: **NONE: 25** / **SSL: 465** / **TLS: 587**
Send from:	email account to send emails. E.g.: abc@xxxxxxxxxxx.com
Username:	Username of the email to send emails. This will be the email signature.
Need Authorization:	Check this option for accounts that require Authorization (“Need Auth”)
Password:	Email account password.
APPLY	Click APPLY button to save modifications.

DAILY REPORT (C):

Every day, SNMP can send an email reporting Daily Reports (Area tagged as **C**), here you can configure it:

Account 1: Account 2:	Email addresses to receive Daily report. Select “APPLY” on the right for each receiver added
Send email for daily report:	Mark checkbox to activate, also select the time.
Send email when Event Log overflows:	Mark checkbox to activate.
Send email when Data Log overflows:	Mark checkbox to activate.

IMPORTANT NOTES:

- **The email-sending firmware of the SNMP card has not been compatible with the security settings of Hotmail® and Microsoft® servers since September 2024, due to changes in their authentication system.**
- **If you have any questions, contact either your Internet/email provider or your IT administrator.**
- **After configuring the email section, we recommend testing it by clicking the "TEST" button.**

System will response with a message: “TEST SUCCESSFULL” when email has been sent without errors. In case email cannot be sent, system will show a failure message.

IMPORTANT: If SNMP Web Pro reports problems sending emails, it can be for one of these reasons:

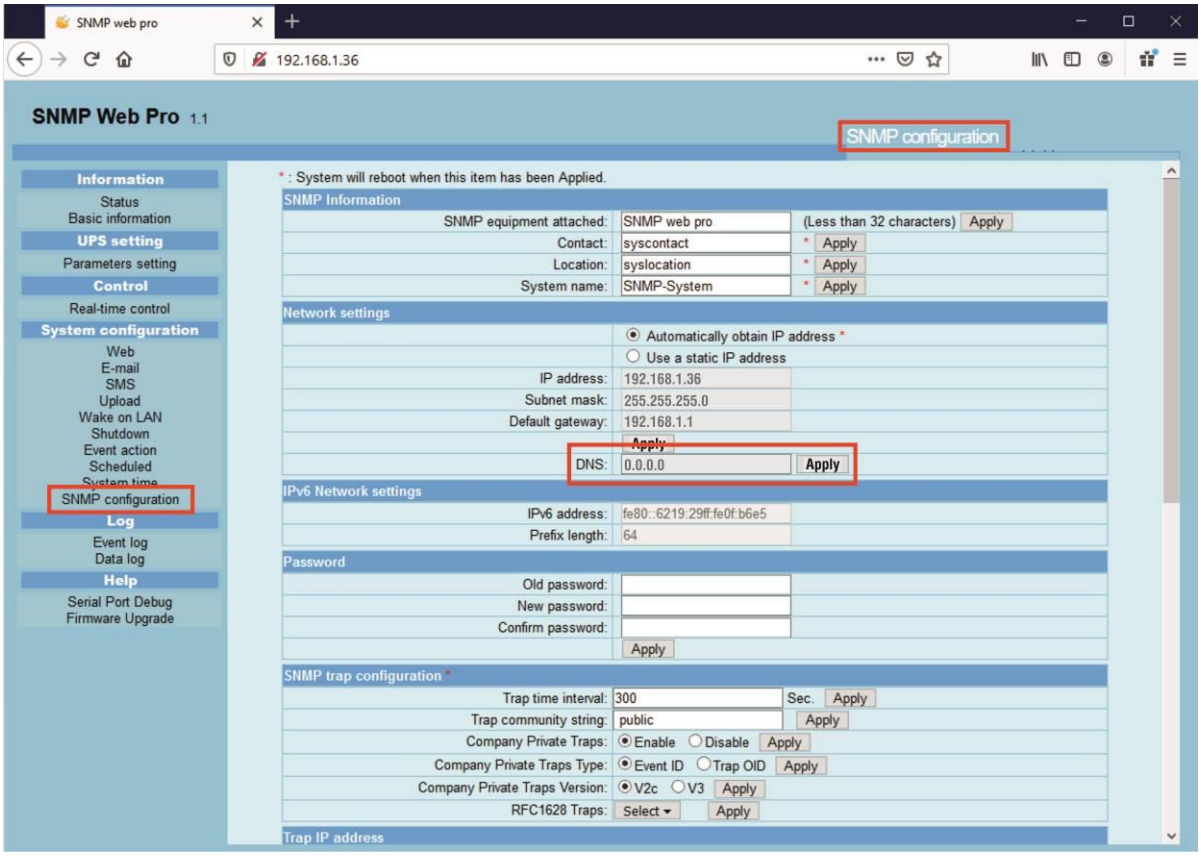
1.- A mistake in one or more data fields. Check and correct any wrong data.

2.- Check there is no firewall or any other security system blocking email delivery

3.- DNS has not been saved automatically in the card. In this case, follow this procedure:

a) Check **System Configuration** / **SNMP configuration** / network settings.

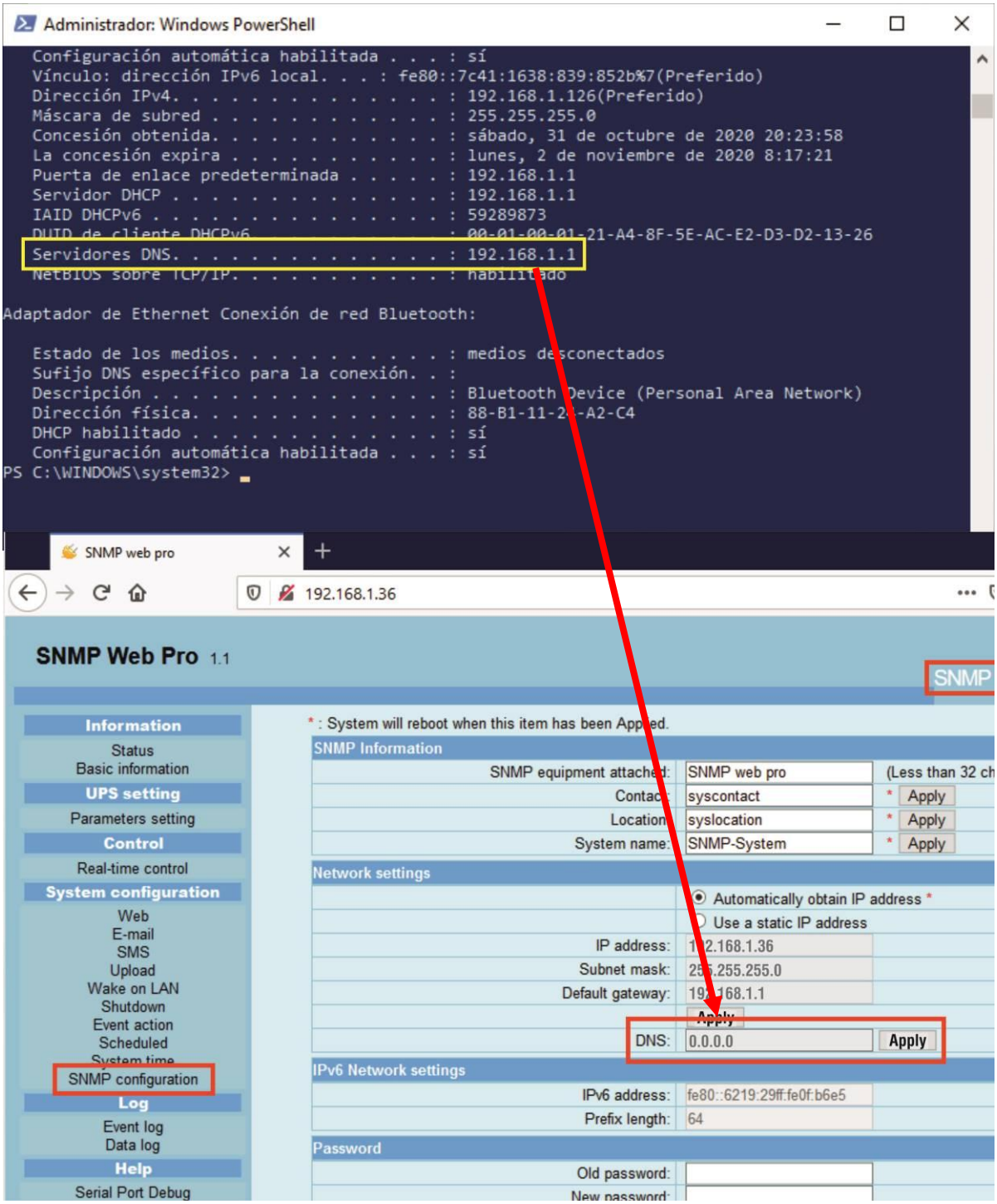
b) Check if DNS field shows appropriate DNS. If it shows 0.0.0.0, user must enter manually DNS of the network and select APPLY. See next figure for reference.



The way to find out DNS of your network, depends on your operating system. For instance, in windows you can go to system command line of your PC and execute this command:

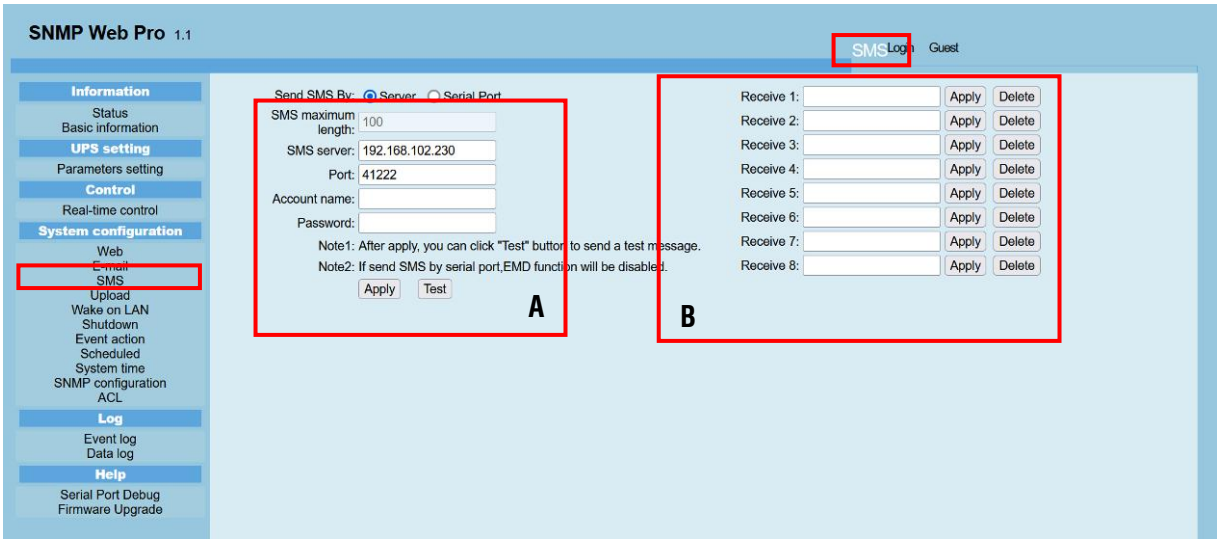
ipconfig -all

Your operating system will list several related parameters. Look for the line dedicated to DNS server. In the following example the value is: **192.168.1.1**. This is the address to be written in DNS Field. See next figure for reference:


Administrador: Windows PowerShell
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::7c41:1638:839:852b%7(Preferido)
Dirección IPv4. . . . . : 192.168.1.126(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : sábado, 31 de octubre de 2020 20:23:58
La concesión expira . . . . . : lunes, 2 de noviembre de 2020 8:17:21
Puerta de enlace predeterminada . . . . . : 192.168.1.1
Servidor DHCP . . . . . : 192.168.1.1
IAID DHCPv6 . . . . . : 59289873
DUID de cliente DHCPv6 . . . . . : 00-01-00-01-21-A4-8F-5E-AC-E2-D3-D2-13-26
Servidores DNS. . . . . : 192.168.1.1
NetBIOS sobre TCP/IP. . . . . : habilitado
Adaptador de Ethernet Conexión de red Bluetooth:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
Descripción . . . . . : Bluetooth Device (Personal Area Network)
Dirección física. . . . . : 88-B1-11-2
-A2-C4
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
PS C:\WINDOWS\system32>
SNMP web pro
192.168.1.36
SNMP Web Pro 1.1
SNMP
Information
Status
Basic information
UPS setting
Parameters setting
Control
Real-time control
System configuration
Web
E-mail
SMS
Upload
Wake on LAN
Shutdown
Event action
Scheduled
SNMP configuration
Log
Event log
Data log
Help
Serial Port Debug
* : System will reboot when this item has been Applied.
SNMP Information
SNMP equipment attached:
SNMP web pro
(Less than 32 ch
Contact:
syscontact
Apply
Location:
syslocation
Apply
System name:
SNMP-System
Apply
Network settings
Automatically obtain IP address *
Use a static IP address
IP address:
192.168.1.36
Subnet mask:
255.255.255.0
Default gateway:
192.168.1.1
Apply
DNS:
0.0.0.0
Apply
IPv6 Network settings
IPv6 address:
fe80::6219:29ff:fe0f:b6e5
Prefix length:
64
Password
Old password:
New password:

3.4.3. SMS

Some events can cause SNMP card to generate SMS (See section **3.4.7 EVENT ACTION** for more details). Thus, this section describes SMS parameters configuration. For configuration purposes, it is necessary to log in as administrator. See next figure as reference:



Send SMS By: This parameter selects one out of two ways to send SMS:

- **Server**: Mark this checkbox to use a SMS server using the configuration of the Zone **A**.
- **Serial Port**: Mark this checkbox to send SMS thru serial port (Secondary Port) of SNMP card.

ZONE A: CONFIGURATION TO SEND SMS VIA SMS SERVER

- **SMS SERVER:** IP address of SMS Server
- **Port**: SMS Server Port
- **Account Name**: Username of the account at SMS Server
- **Password**: Access password of the account at SMS Server
- **Apply**: Click this button to save entered information.
- **Test**: Click this button for testing new configuration.

ZONE B: SMS RECIPIENT PHONE NUMBER LIST

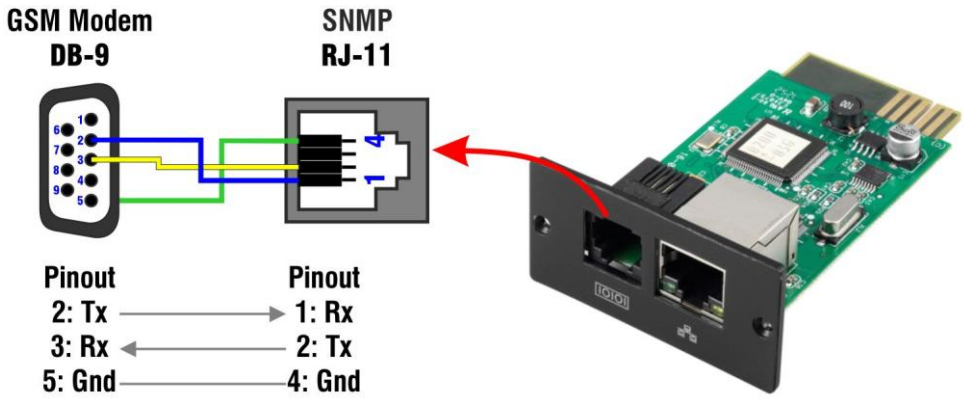
Parameters to set phone numbers to receive SMS:

- **RECEIVE** 1 to 8: These fields must contain phone numbers which will receive SMS.
- **Apply**: After each phone number has been entered, click this button to save data.
- **Delete**: This button deletes selected number, emptying the field.

CONFIGURATION TO SEND SMS VIA SERIAL PORT (SNMP PORT B)

To use this option, there must be a GSM Modem connected to the secondary port of SNMP Card (B Port). This is the same port to connect Environmental Measuring Devices (EMD), therefore sending SMS via serial port is not compatible with EMD.

Pin-out for GSM Modem connection to SNMP card is shown in the next figure:



RJ11 – DB9 Cable not included

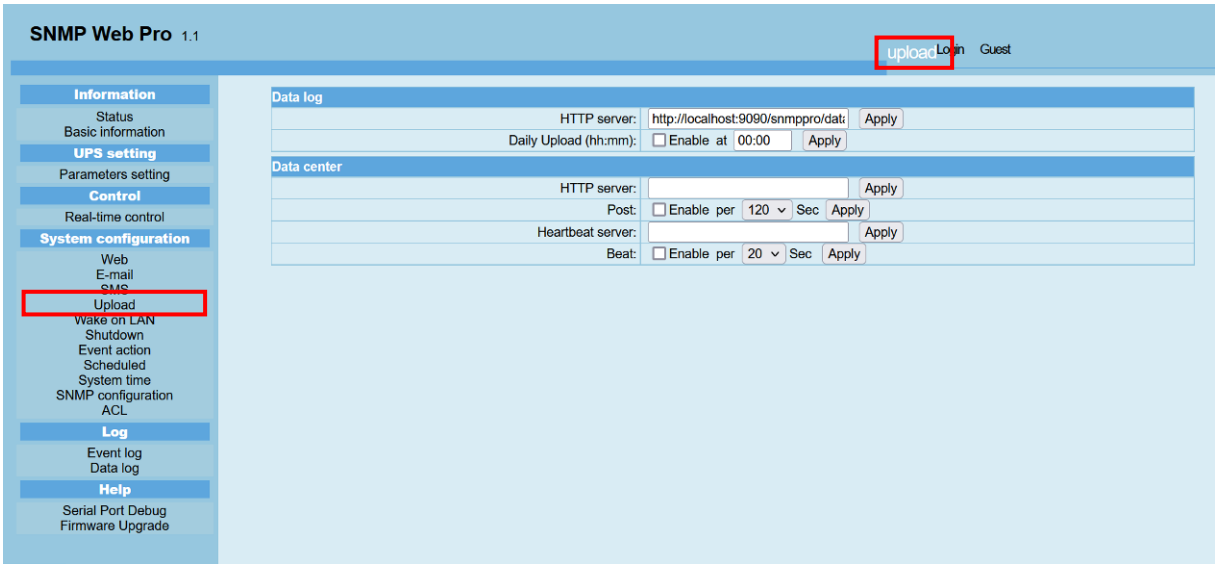
The GSM Modem configuration must be as follows:

- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: Hardware Flow control
- Rata de Baudio: 9600
- ECHO: Off

Additionally, in the **Event Action** configuration, "SMS Send when any event occurs" checkbox must be enabled, otherwise, SMS sending will not work, even using the **Test** button.

Finally, make sure the GSM Modem is properly connected to B Port of SNMP Card (RJ11 Port).

3.4.4. UPLOAD



This section allows to upload data to selected end user servers, and it is divided in 2 areas, as follows:

- **Data Log:**

  Enter HTTP server address to send Event and Data Logs. Click "Apply" to save changes.

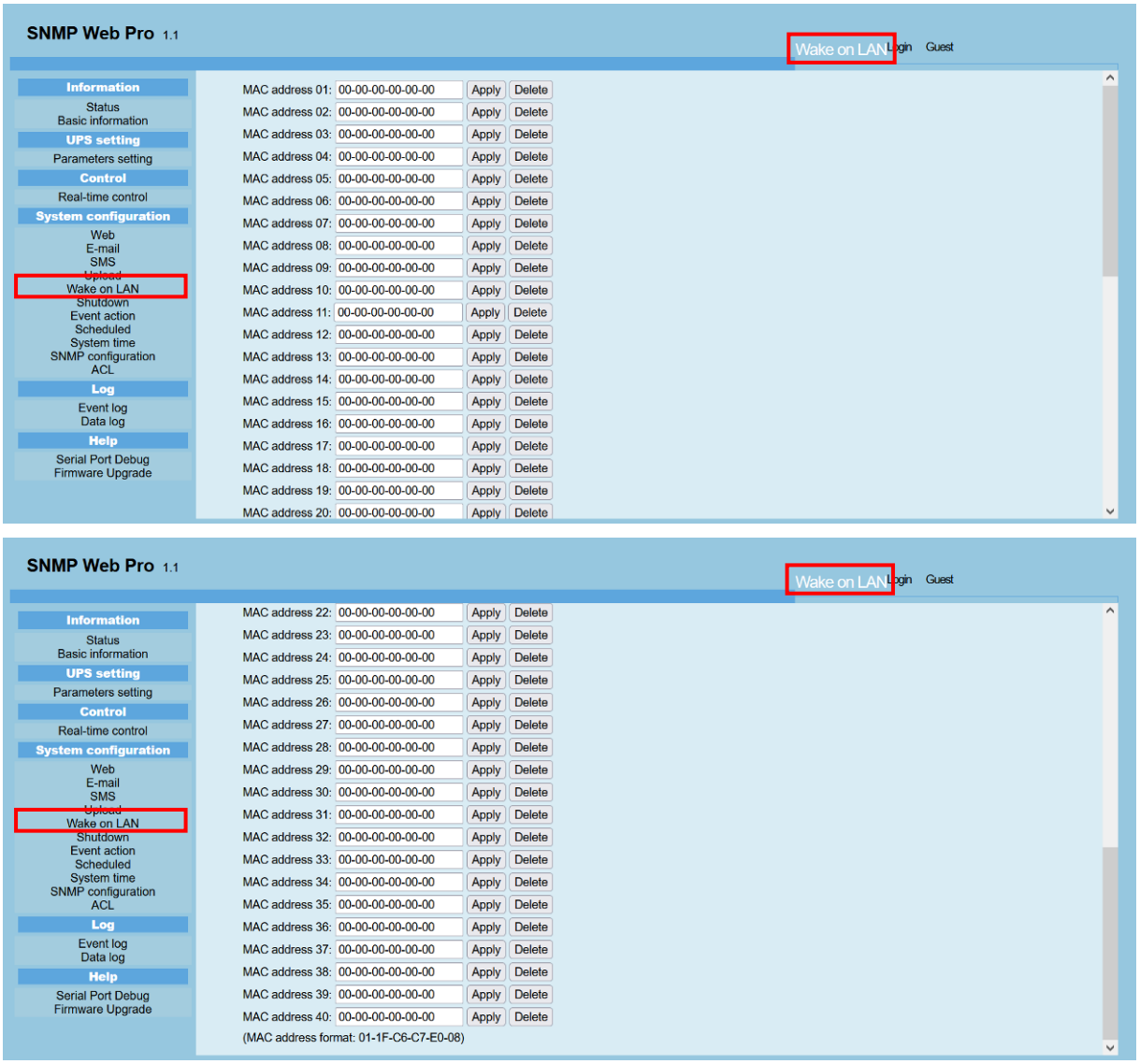
Enable data sending and enter the time when data should be sent every day. Click “Apply” to save changes.

- **Data Center:**

  Enter HTTP server address to send Real-time UPS data and alarms in JSON format. This is particularly helpful to integrate UPS data in end user web site. Click “Apply” to save changes. Enter the rest of details to upload data. Click “Apply” every time to save changes.

3.4.5. WAKE ON LAN (WOL)

This function allows remotely start a given computer in LAN via Magic Packet protocol. PC hardware and BIOS must support this feature. MAC address must be entered for each PC to work with WOL, up to 40, and "Apply" button must be clicked on to save changes after entering each line information. See next figures for reference.



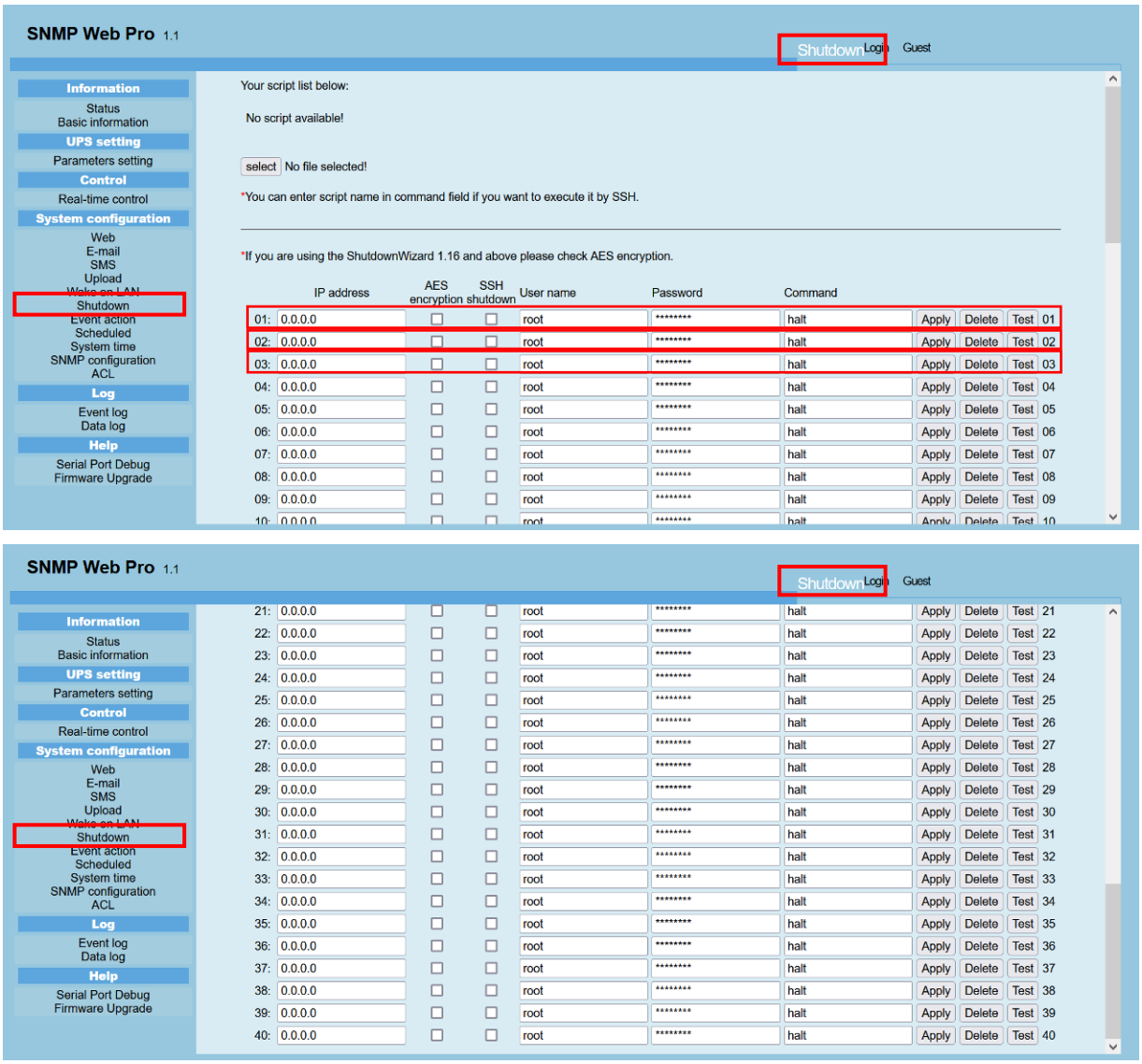
3.4.6. SHUTDOWN

In this section, PC to receive shutdown commands (identified by IP address) can be configured. Conditions that generate these commands should be configured in the following section: **EVENT ACTION**.

For information about finding out the IP Address of a given PC, please refer to **APPENDIX C** in this manual.

SNMP card, based on some events, can send commands to shutdown PC in the network before UPS runs out of batteries, after saving and closing all files to avoid data loss. PC to be shutdown must have Shutdown Wizard software installed, check Shutdown Wizard user manual for details.

Due to the windows size for this section, the screen has been separated in 2 images. See next images for reference:



Command Files:

Clicking “Select” button, located at the top left corner of the screen, user can browse and select script (Commands) files in case they are needed. Once selected, files will be listed under the phrase: “Your script list below:”.

Scripts files can be uploaded to SNMP card clicking “Upload” button to be permanently stored and used to generate shutdown commands.

Configuration To Generate Shutdown Commands

All devices requiring shutdown commands must be registered in the lines numbered from 01 up to 40 in this section, in previous image 3 first lines have been highlighted in red color.

The fields to be filled for each device are explained here:

- **IP Address**: IP Address of either PC or server to receive shutdown command.

- **AES Encryption**: Check this checkbox for compatibility with Shutdown Wizard. When using SSH, this is not necessary.
- **SSH Shutdown**: Some EXsi and Linux operating systems use SSH to manage remote commands, such as Shutdown using SSL clients, without Shutdown Wizard. To shut down this kind of device mark this checkbox. In these cases, you will need Username and Password to access the device, these are the following 2 fields to be filled.

  Note: **We strongly recommend checking APPENDIX D for details to avoid potential failures of shutdown command on Virtual Servers (VMWare).**
- **Username**: ID configured in the device to be shut down. For SSH commands only.
- **Password**: Security password to access the device to be shut down. For SSH commands only.
- **Command**: This is the command to be sent to the device with registered IP address. By default, it is set to "Halt", however it can be changed to another host specific command or to the name of one of the Script files stored in the SNMP, in case the user needs it.

  NOTA: We strongly recommend keeping the default value unless change is absolutely necessary.
- **Apply**: Click this button for each IP Address, after entering changes.
- **Delete**: Button to empty all fields related to selected IP Address.

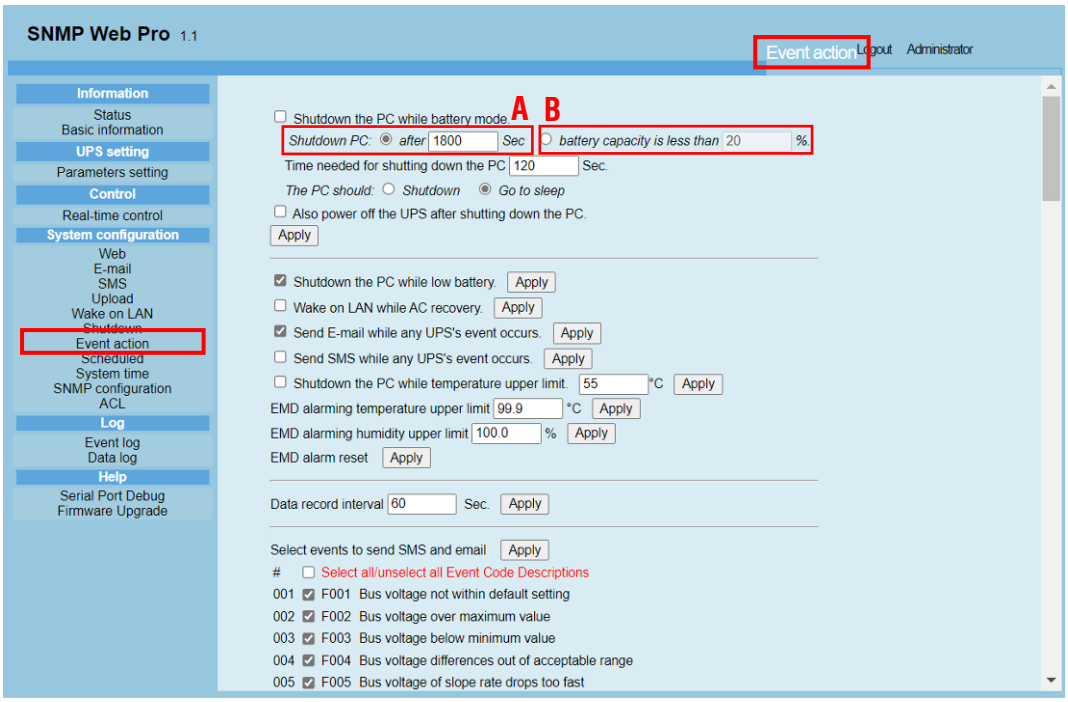
NOTE:

All PC to receive shutdown commands must have SHUTDOWN WIZARD auxiliary software installed for a successful shut down, otherwise the command will be ignored. Except for systems using SSH protocol, which should be configured as previously explained.

SCOPE AND RESPONSIBILITIES:
Installing software in End User terminals and/or servers, as well as finding out IP addresses and usernames in End User networks, and any other related issue, affects the security of the system, therefore it should be responsibility of the System Administrator and we strongly recommend being done by the System Administrator, not by the technical personnel installing the UPS arrangement.

3.4.7. EVENT ACTION

In previous section, we explained how to identify devices to receive shutdown commands. In this section we will explain the conditions that generate these commands and how to configure them, as well as some other actions such as emailing, SMS and alarms of Environmental Measuring devices (EMD). Next figure shows this section and how to select it.



Configurable parameters:

- **Shutdown The PC While Battery Mode**: When selected, the Shutdown command will be generated if one of the following conditions occurs:
    1. With “after” checkbox selected (See Zone A previous figure) and UPS reaches the number of seconds entered in Battery Mode, in the figure time is 1800 sec.
    2. With “battery capacity is less than” checkbox selected, and remaining battery capacity is less than percentual value entered, with UPS in Battery Mode. It is 20% in previous figure.
- **Time Needed for Shutting Down The PC**: Delay time to shut down the operating system, after previously selected event. For previous example, this time is 120 Sec.
- **The PC Should**: Select what PC should do when receiving Shutdown command by clicking one of these checkboxes:
    1. **Shutdown**: Shut down device. This is default setting.
    2. **Sleep mode**: Suspend the system instead of shutdown, supported by Windows 2000® and above on supported hardware.
- **Also Power Off The UPS After Shutting Down The PC**: Click this checkbox to turn off monitored UPS after shutting down the local PC.
- **Shutdown The PC While Low Battery**: Click this checkbox to shut down local PC when monitored UPS batteries reach low level.
- **Wake On Lan While AC Recovery**: Click this checkbox to send a wake on LAN to the PC that was shut down when AC recovers.
- **Send E-Mail While Any UPS Event Occurs**: Click this checkbox, to send alarm E-mail when any of the events selected in the list occur in the UPS. The list is in the lower part of the screen.

- **Send SMS While Any UPS Event Occurs**: Click this checkbox, to send alarm SMS when any of the events selected in the list occur in the UPS. The list is in the lower part of the screen. This requires having a GSM Modem connected to SNMP Card's Port B.
- **Shutdown The PC While Temperature Upper Limit:** Click this checkbox to generate a Shutdown command when temperature reaches the value entered on the field on the right. After selecting this checkbox, two more parameters will be required:
    1. Selecting either this should be the UPS internal temperature or the EMD temperature.
    2. Selecting if the UPS should restart a given time after the shutdown. If so, time should be entered (in minutes) in the field on the right.
- **EMD Alarming Temperature Upper Limit**: Set up alarm for high temperature point. EMD measured temperature over this limit will cause an alarm message.
- **EMD Alarming Humidity Upper Limit**: Set up alarm for high humidity point. EMD measured humidity over this limit will cause an alarm message.
- **EMD Alarm Reset**: Clear all EMD alarms clicking on "Apply" button.
- **Data Record Interval XX Sec**: Time between samples for Data log. Default: 60 sec.
- **Select Events To Send SMS And Email**: In the lower side of the screen there is a list or alarms and UPS failures. Those selected will generate E-mails and SMS when happening. Once all desired conditions are either marked or unmarked, select "Apply" button to save changes.
- **Select All/Unselect All Event Code Descriptions**: Click in this checkbox to either select or unselect all Event Code Descriptions simultaneously. Select "Apply" button to save changes.

NOTES:

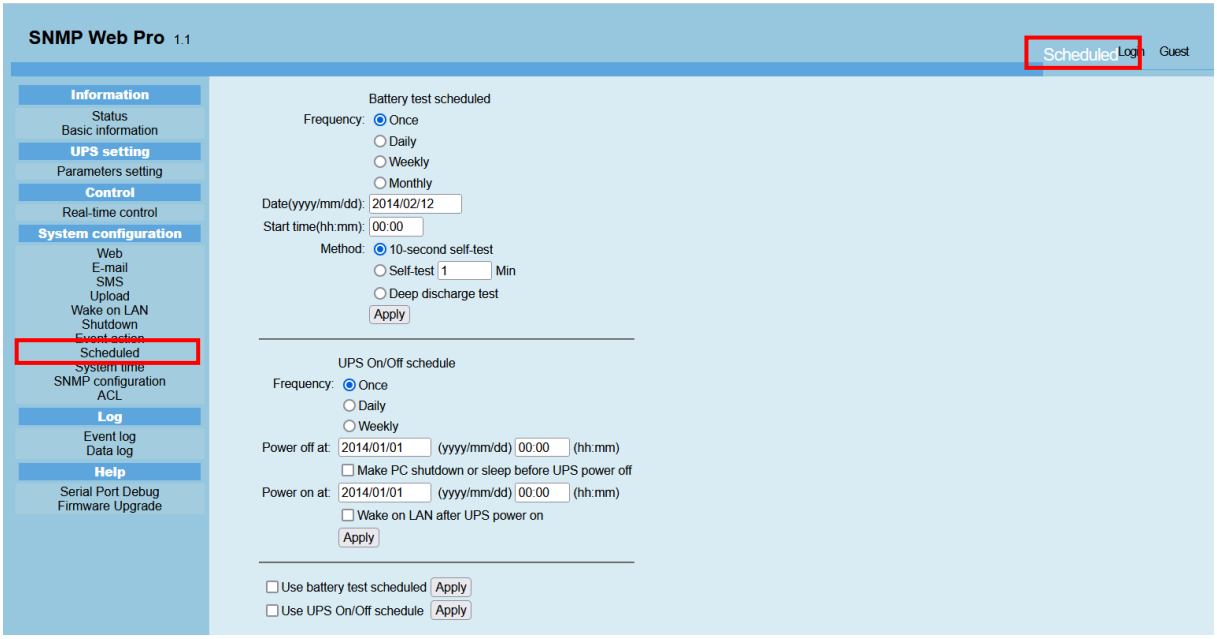
1. Shutdown commands generated by parameters configured in this section will be sent to devices whose IP addresses are configured in the previous section (3.4.6. SHUTDOWN).
2. For the devices to be able to execute these shutdown commands, it is required to have SHUTDOWN WIZARD auxiliary software installed, unless the devices can manage SSH protocol and have been properly configured in the former section (3.4.6. SHUTDOWN).
3. We strongly recommend reading **APPENDIX C**, for examples about Shutdown Commands Configuration.

SCOPE AND RESPONSIBILITIES:

Installing software in End User terminals and/or servers, as well as finding out IP addresses and usernames in End User networks, and any other related issue, affects the security of the system, therefore it should be responsibility of the System Administrator and we strongly recommend being done by the System Administrator, not by the technical personnel installing the UPS arrangement.

3.4.8. SCHEDULED

This section is for programming scheduled tasks, such as battery tests and UPS power On and Off. See next image for reference.



Battery Test Scheduled:

- **Frequency**: Adjust how often the test will be done (Once / Daily / Weekly / Monthly)
- Date and Time of battery test.
- **Method**: 10 Seconds test / Self defined Tests (In minutes) / Deep discharge test
- Once all data is entered, click “Apply” button to save changes.

UPS On/Off Scheduled:

- **Frequency**: adjust how often the UPS will be turned On/ Off (Once / Daily / Weekly)
- **Power Off At**: Time and date to power off the UPS.
- **Make PC Shutdown Or Sleep Before UPS Power Off**: Check this checkbox to safely shutdown local PC before turning off the UPS.
- **Power On At**: Time and date to power on the UPS.
- **Wake On LAN After UPS Power On**: Check this checkbox to start up local PC after turning on the UPS.
- Once all data is entered, click “Apply” button to save changes.

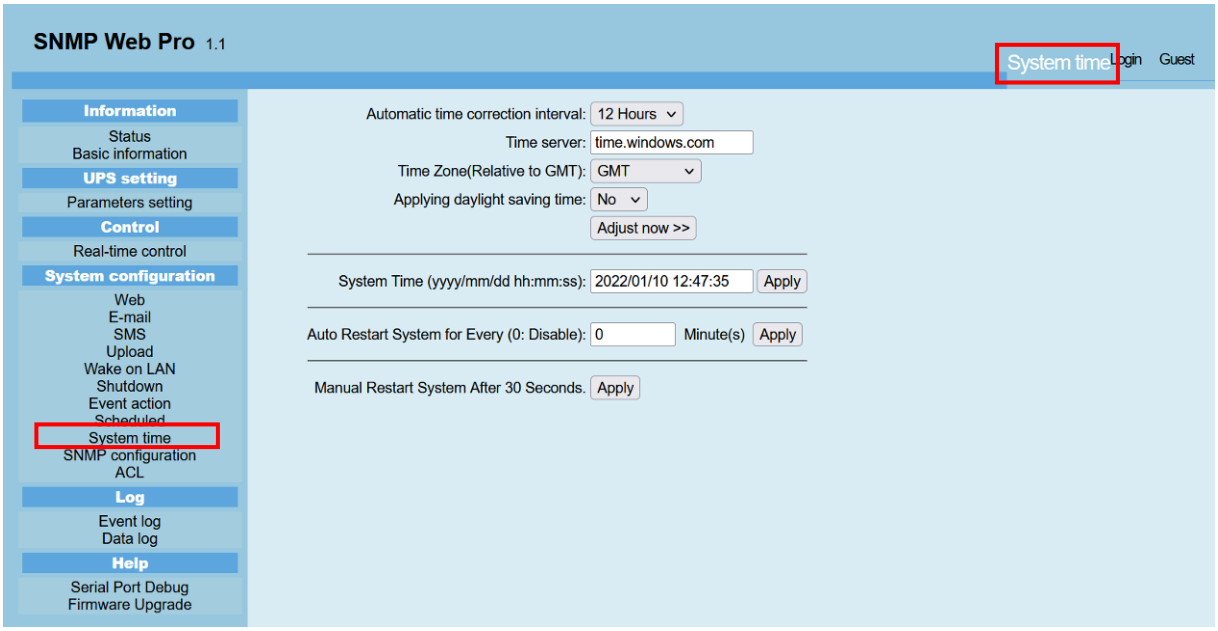
Enable Schedule Tasks:

- **Use Battery Test Scheduled**: Check this checkbox to activate scheduled battery test.
- **USE UPS ON/OFF SCHEDULE**: Check this checkbox to activate scheduled UPS operations.

Notes:

- We recommend not scheduling several actions to be executed at the same time. If several actions are running at the same time, some might be ignored.
- Any action not supported by the UPS will be ignored.

3.4.9. SYSTEM TIME



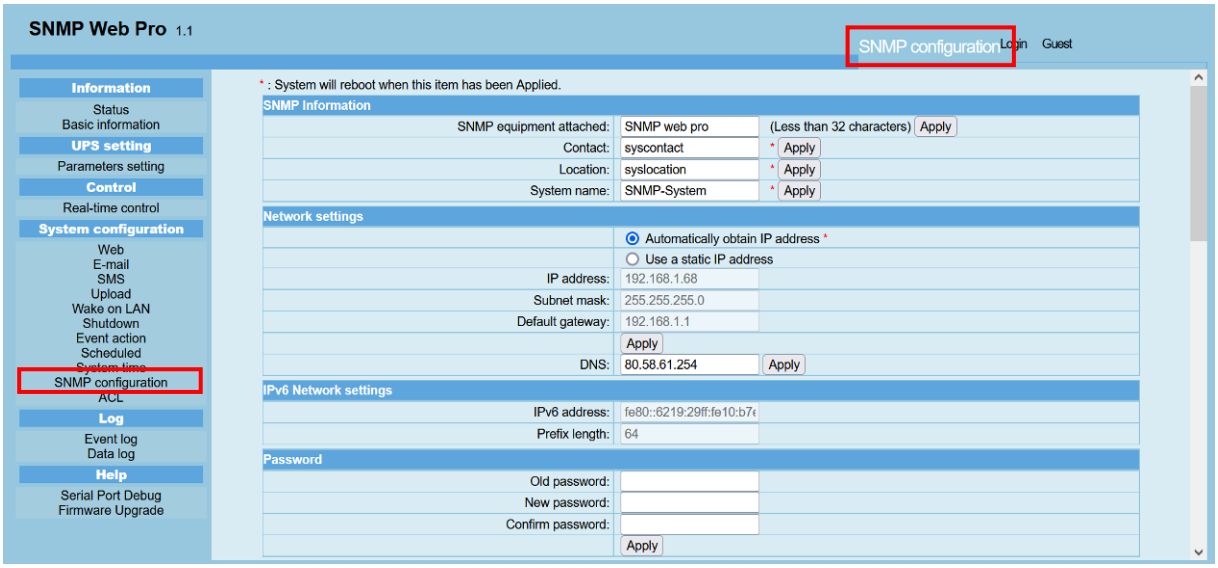
Adjustable Parameters:

- **Automatic time correction interval**
- **Time Server**: Reference server for time system.
- **Time Zone (Relative to GMT)**: Time Zone for system.
- **System Time** (mm/dd/yyyy hh:mm:ss): To set up **SNMP Web Pro** local time
- **Auto Restart System for Every**: Select time (in minutes) for automatic, repetitive restarts. 0 Disables this function.
- **Manual Restart System After 30 Seconds**: Clicking "Apply" button, restarts SNMP after 30 seconds. It requires waiting for 1 minute approximately, to reestablish communication.

3.4.10. SNMP CONFIGURATION

This section is for setting **SNMP Web Pro** basic information. This window is quite longer than the rest so it takes scrolling down to reach the end, therefore it will be shown in 2 different images within explaining texts.

The information is divided in areas, which will be separately explained, as follows:



Network Settings:

IP address configuration can be done here in two different ways:

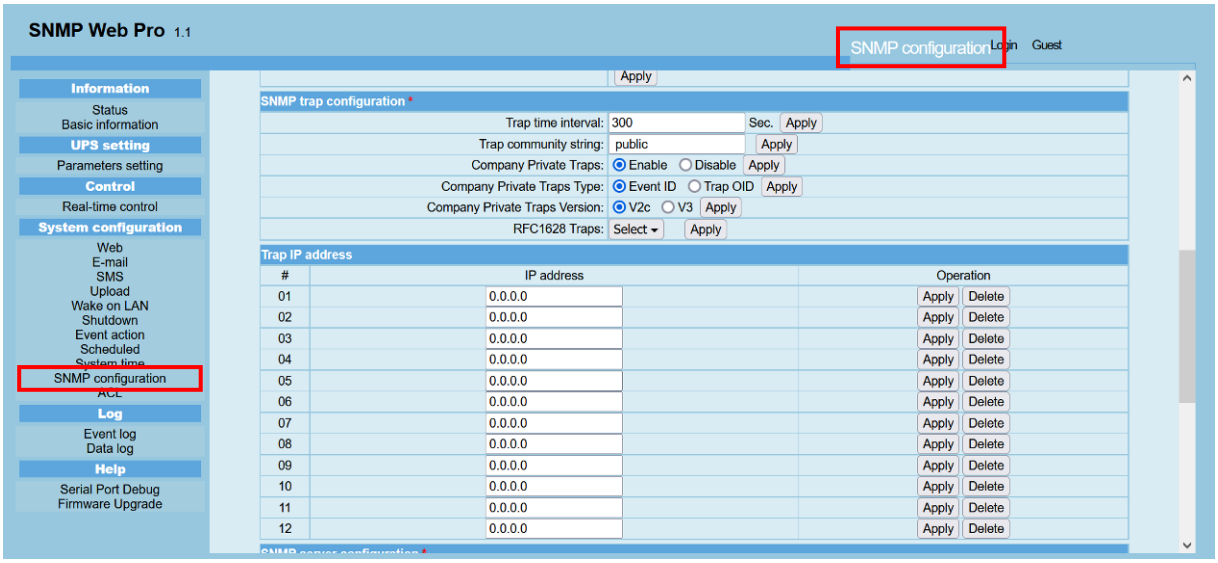
1. Automatically obtain IP address: Default option, it is for DHCP Networks.
2. Manually configure IP address: For Static IP Networks. In this case the IP Address will be shown as "**192.168.102.230**", Net mask as "**255.255.255.0**" and default gateway as "**0.0.0.0**" and values must be entered manually.

IPv6 Network Settings:

Parameters for IPv6 networks can be configured here, including IPv6 address and Prefix length of address format.

Password:

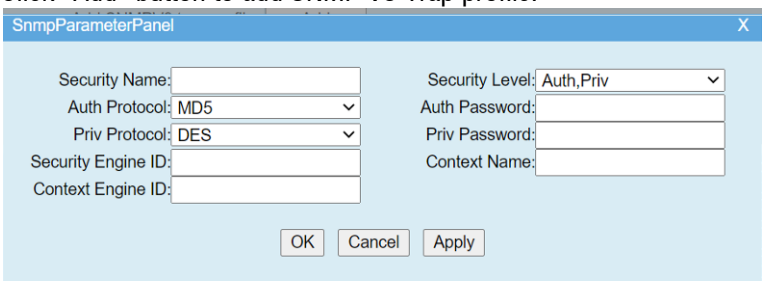
To change password, first enter old password, then new password, and new password again to confirm. Click on "Apply" button to save changes. Passwords must be 8 to 15 characters long.



SNMP Trap Configuration:

Configuration for Trap community string:

- Trap Time interval, in seconds
- Trap community string: “public” as default
- Company Private Traps: Click “Enable” or “Disable” checkbox. Default: Enable.
- Company Private Traps Type: Check your option either Event ID or OID (Object ID). Default Event ID.
- Company Private Traps Version: Check your option either V2c, or V3. Default V2c.
  To select V3 Version, please follow this procedure:
  a) Click V3 checkbox and click “Apply” button to save changes.
  b) Click “Add” button to add SNMP V3 Trap profile.



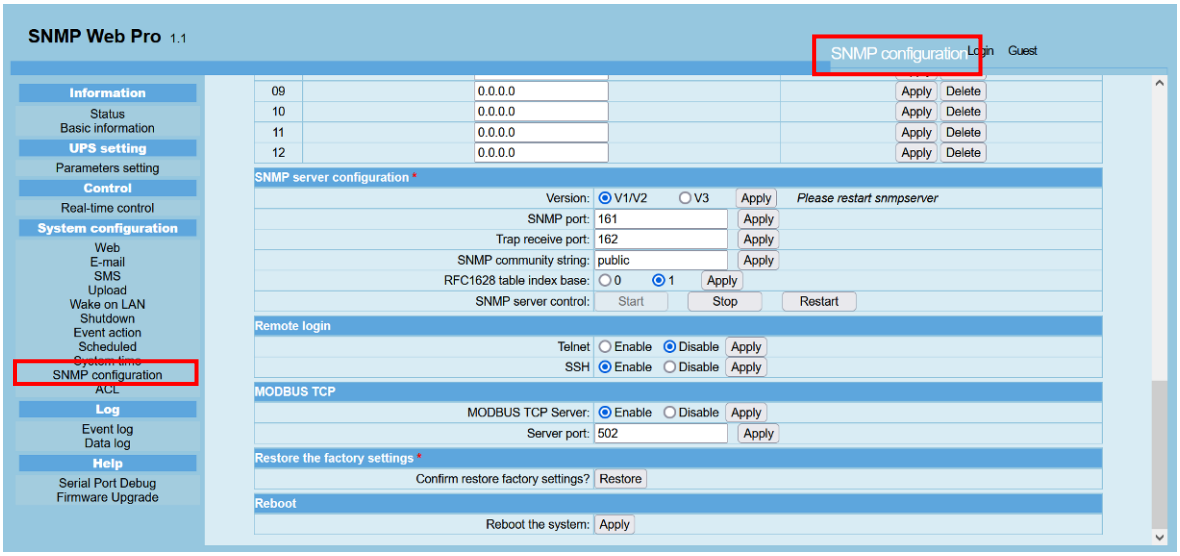
  c) Enter all required information.
  d) Click “Apply” button to save changes.
- RFC1628: Click “Select” button to deploy a list of UPS events to be included in Trap messages. Default: All options are checked.

Trap IP Address

As SNMP V3 Server Trap IP have already been described, this explanation corresponds to V2c.

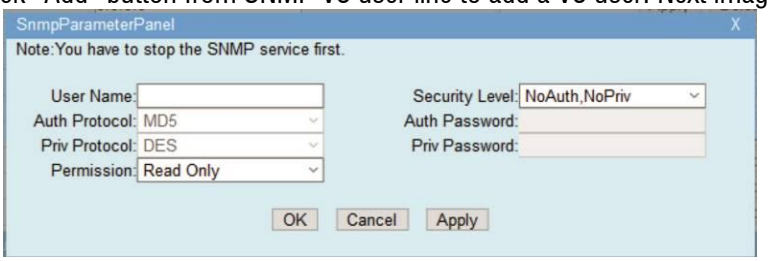
Enter up to 12 static Trap IP addresses, provided by SNMP device. After entering each IP address, click “Apply”, otherwise the changes will be lost. “Delete” button clears the fields.

Next figure shows bottom part of the window and includes all areas explained from here.



SNMP Server Configuration

- **Version**: Selection of SNMP Server version between V1/V2 (Default) and V3.
  To select V3 Version, please follow this procedure:
  a) Click "Stop" button to stop SNMP server.
  b) Click V3 checkbox and click "Apply" to save changes.
  c) Click "Add" button from SNMP V3 user line to add a V3 user. Next image should show up:



  d) Click "Apply" to save changes or "Cancel" to abort operation.
  e) Click "Restart" button to restart SNMP Server.
- **SNMP Port**
- **TRAP Receive Port**
- **SNMP Community String**. Default "public"
- **RFC1628 Table Index Base**: Select between "0" and "1" (Default).
- **Add SNMPV3 User**: if "V3" option has been selected, this line shows up, under "**RFC1628 table index base**" line. This entry was already explained in parameter "**Version**".
- **SNMP Server Control**: "Start" and "Stop" buttons start and stop SNMP server. "Restart" button restarts SNMP server.

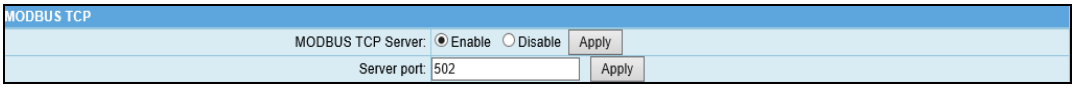
Remote Login:

- Telnet: Enable or Disable (Default) remote access to Telnet services.
- SSH: Enable (Default) or Disable remote access to SSH services.

ModBus TCP

This function enables or disables ModBus TCP service and defines ModBus TCP port (Default: 502).

If disabled, the service will stop and ModBus TCP information packets cannot be obtained. See next image for reference.



Once this option is configured, operation can be tested using ModBus Poll or ModScan software. Data acquisition parameters depend on address mapping and recording protocol, which may vary depending on the UPS model. Xmart offers protocols corresponding to the different models.

Restore The Factory Settings

Clicking on "Restore" button will restore all factory default settings. This means system will automatically try to obtain IP Address and password will be 12345678 again.

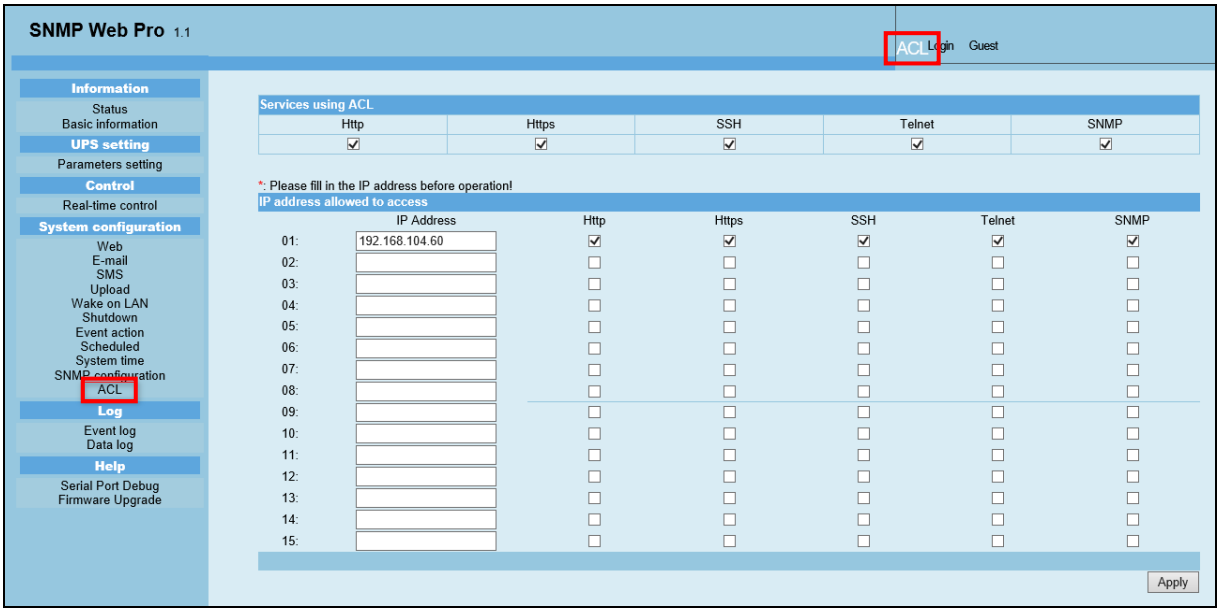
Reboot

Click "Apply" button to restart **SNMP Web Pro** interface.

3.4.11. ACL

ACL is the acronym for **Access Control List**.

This section is for protecting access security via Internet, identifying which IP addresses can effectively access **SNMP Web Pro** interface. See the following image for reference.



Services Using ACL

Check boxes of all types of services ACL system will allow: Http, Https, SSH. Telnet, & SNMP.

IP Address allowed to Access

Enter IP addresses of users ACL will allow access to. In IP Address column, specific IP addresses must be entered and in the boxes on the right, services allowed for each particular IP address must be marked.

Any IP address not configured in this table will be blocked from accessing **SNMP Web Pro**.

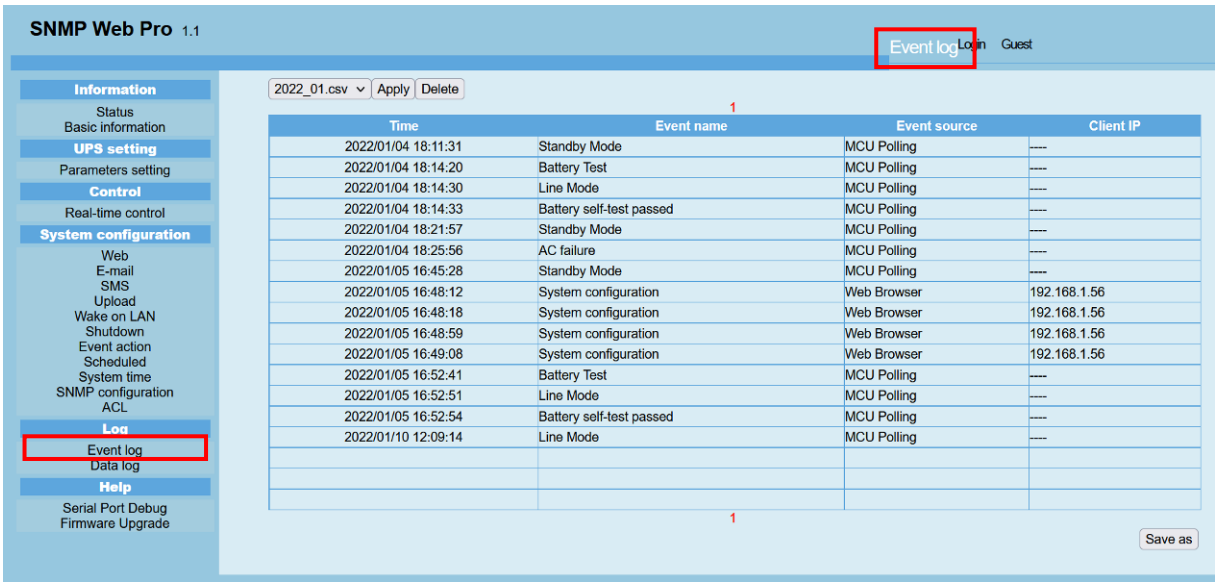
After all Data is configured, click on "Apply" button to save changes, otherwise, changes will be lost.

3.5. LOG.

UPS events and data are stored in SNMP flash memory for about a month, so information is safe even during long blackouts.

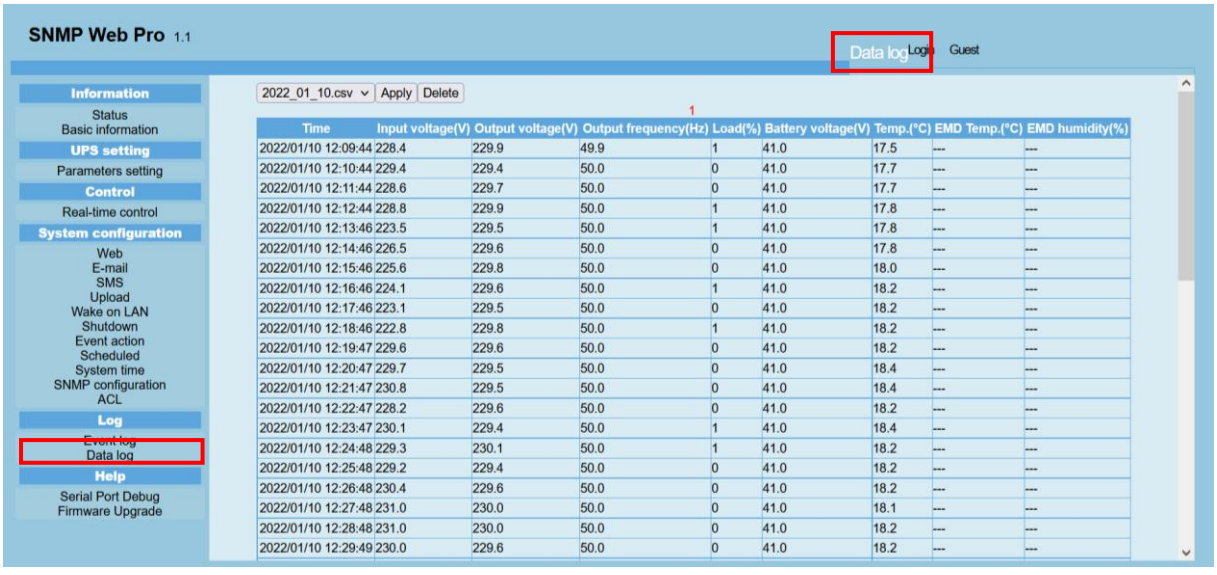
3.5.1. Event Log

Up to 200,000 event threads can be stored in Event Log and information can be downloaded as .csv File. The event Log includes UPS Warnings, Failure Information, Sensor-TH Warnings, UPS Operations commanded from either **SNMP Web Pro** or any of our Supervision and control software. See next image for reference:



3.5.2. Data Log

Up to 200,000 data threads can be stored in Data Log and information can be downloaded as .csv File. The Data Log includes values of input and output voltages, frequency, UPS load, Battery Voltage, UPS internal Temperature, Sensor-TH readings. See next figure for reference:

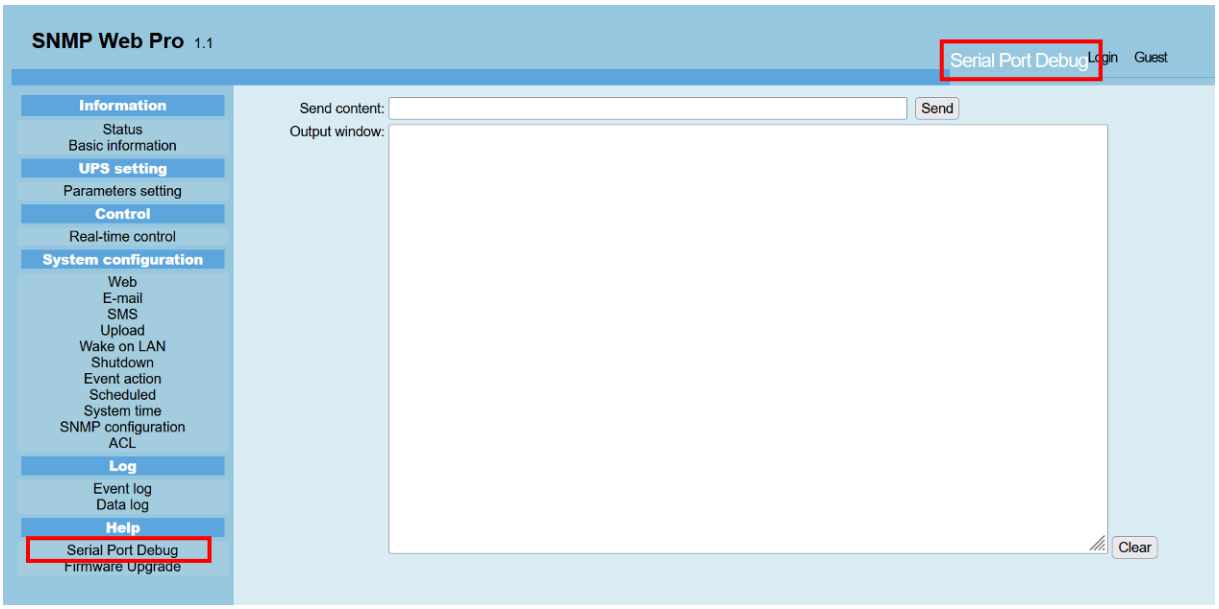


3.6. HELP.

This area is reserved for qualified personnel only and for SNMP maintenance purposes.

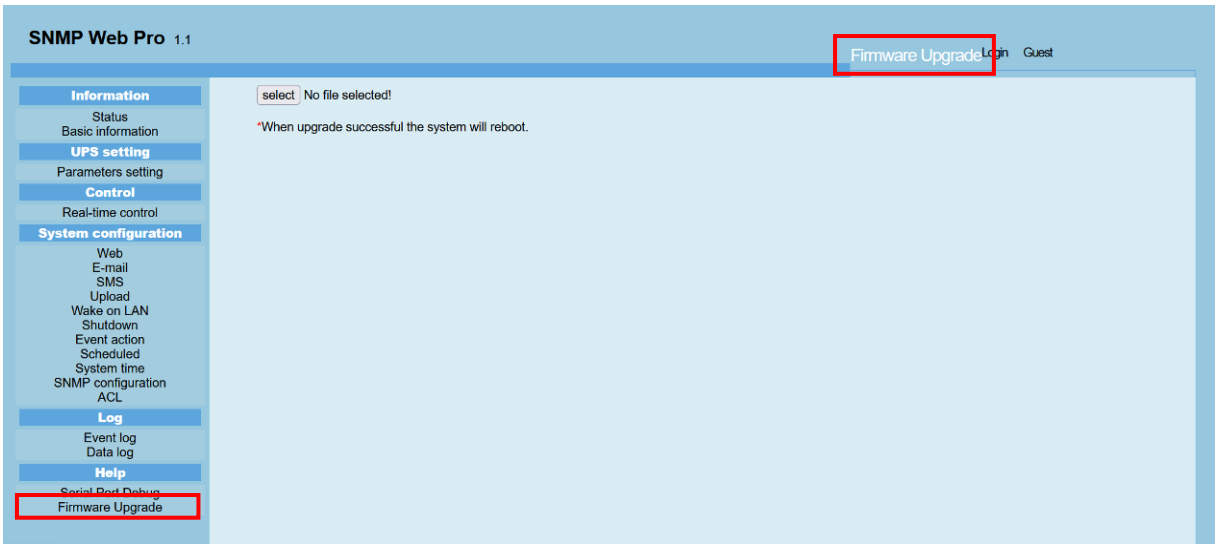
3.6.1. Serial Port Debug

This function is intended to test communication condition between SNMP card and testing device. See next figure for reference.



3.6.2. FIRMWARE UPGRADE

This function allows upgrading SNMP card firmware. See next figure for reference.

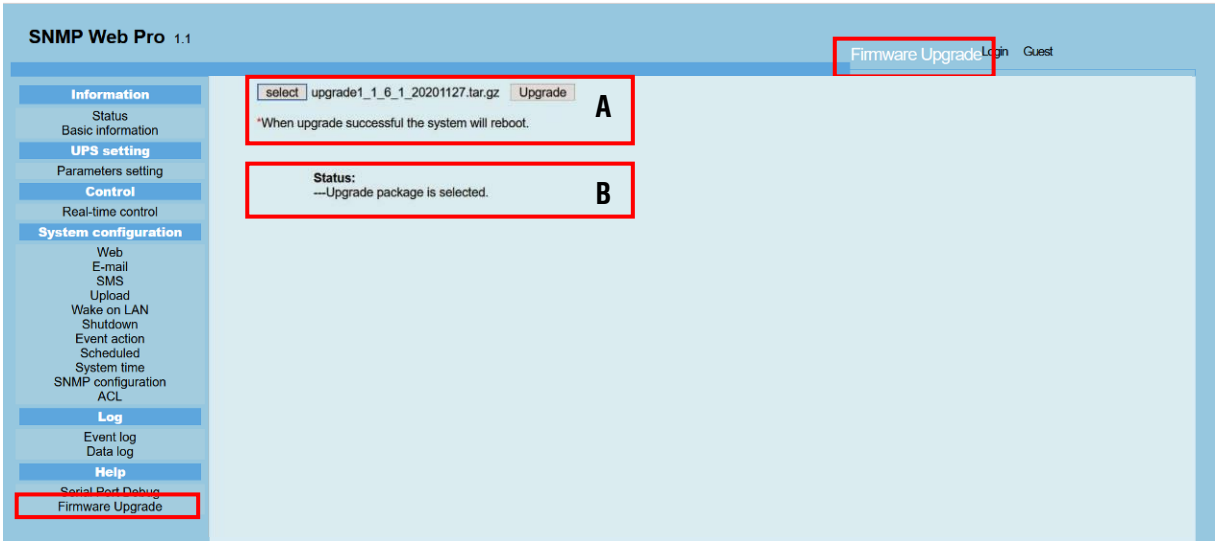


Button “Select” allows selecting, in your computer, the firmware file to be sent to SNMP card. Please keep this in mind:

- Firmware file must have this extension: **“.tar.gz”**
- IMPORTANT: Disable FIREWALL and antivirus since they could stop the download process and SNMP card would get damaged.

- Make sure you are communicating with the right SNMP card, confirming that IP address in your browser address bar corresponds to the card to be upgraded.
- To perform this process, you should log in as administrator.

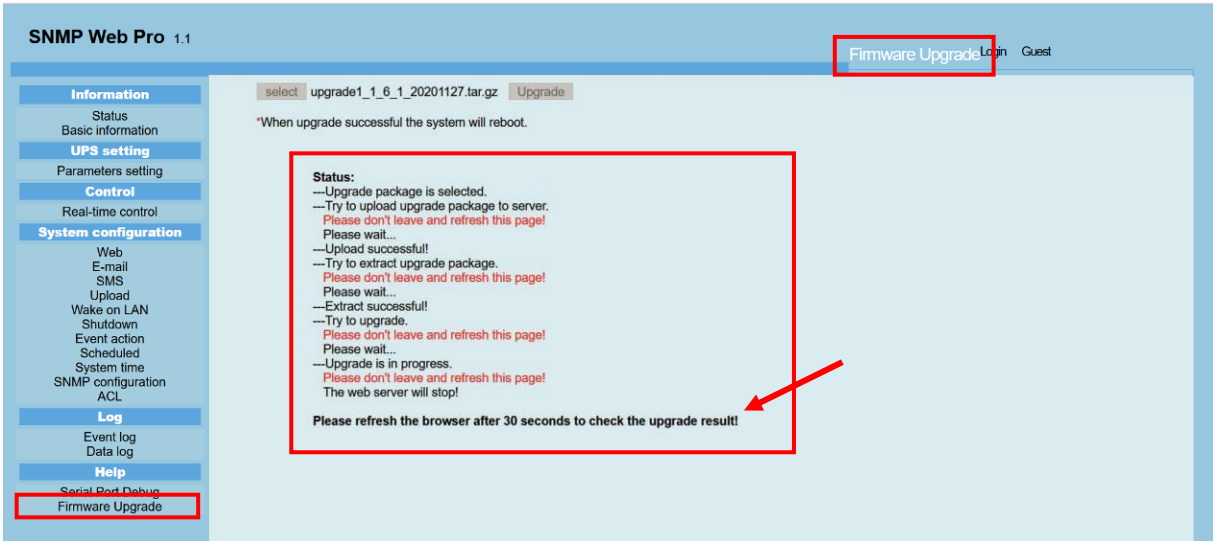
After selecting the firmware file, the window will look like the next image:



The name of the selected file appears as well as “Upgrade” button (Area “**A**”), clicking on this button the file will be sent to the card to be upgraded.

Also, the word **Status** is shown (Area ”**B**”) and below, in the messages zone, there is a confirmation about the firmware file been selected.

Click on “Upgrade” button to start the upgrade process. Advance messages will be shown sequentially to indicate the process steps, as shown in the next figure in the area marked in red.



When pointed text (with a red arrow) appears, means the firmware upgrading is successfully done. Wait about 30 seconds and refresh the browser, which should show **SNMP Web Pro** opening window.

APPENDIX A
SNMP: INSTALLATION AND OPERATION IN STA

STA-16A

INTRODUCTION

STA-16A is an automatic switch with 2 AC Inputs and AC Output. STA-16A keeps its output connected to preselected AC Input, until a failure is detected. At this moment STA-16 switched to connect its output to secondary AC Input to keep it powered. As soon as main AC Input recovers STA-16 switches back to normal primary input.

STA-16A is usually used for 2 main applications:

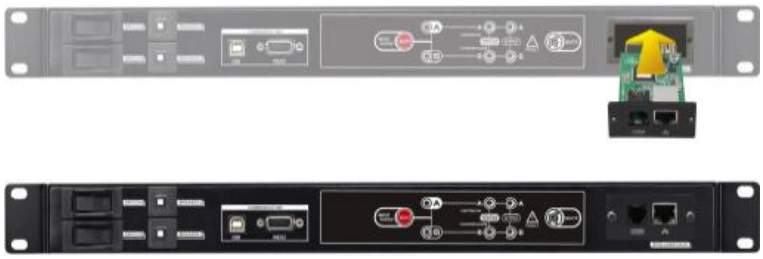
1.- Offering redundant inputs for one UPS.
2.- Redundancy with 2 UPS, as STA-16A can be powered by UPS #2, in case UPS #1 fails.

SNMP INSTALLATION IN STA:

1: Check jumper "C" is between pins 1 & 2 in the card

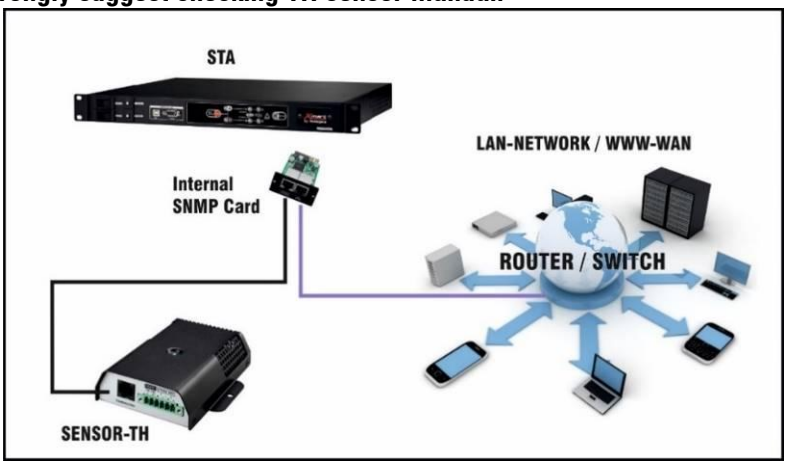
2: Remove cover from intelligent slot in the STA front panel

3: Insert SNMP Card into Intelligent Port as shown in next figure:



4: Plug RJ45 cable in the Ethernet port of the card and connect other side to the network socket. Check if yellow LED lights as expected.

If XMART TH sensor is available, connect it to RJ11 port of SNMP Card.
In this case we strongly suggest checking TH sensor manual.



STA COMMUNICATION

There are 2 ways to communicate with STA via SNMP06 cards:

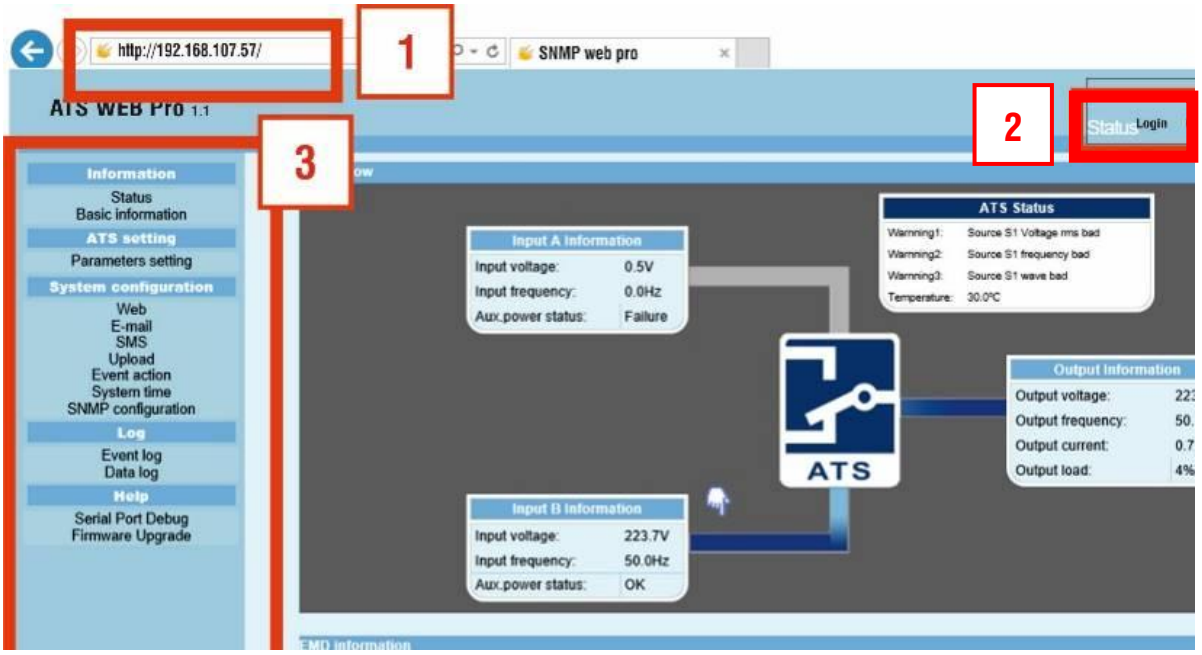
A) MONITORING SOFTWARE: ATS MONITOR

ATS MONITOR software offers all kind of control and monitoring functionality for all STA in the LAN. Software communicates any PC with any of the STA. Software also provides logging capabilities, as well as a configurable e-mail system. Install **ATS MONITOR** software in the PC from which STA will be monitored. **ATS MONITOR** is available in www.xmart-ups.com. For more information download and check user manual for **ATS MONITOR** software.

B) COMMUNICATION THRU WEB BROWSER – ATS WEB PRO INTERFACE

User can monitor any STA in the LAN from any PC in same LAN accessing SNMP06 card from Web Browser by introducing IP address of the SNMP06 to open **ATS Web Pro** interface. SNMP06 card can storage data and events in its internal memory, without depending on external software. It can also send messages and alarms by email if there is a router in the network with open access to internet. If network is DHCP, card will receive dynamic IP address installed in STA and connected to network. If network uses static IP, network administrator must assign IP for the card, refer to section dedicated to this subject in this manual, for details.

WEB BROWSER COMMUNICATION INTERFACE: ATS WEB PRO.



This operator interface is divided in different areas:

1) ADDRESS BAR: Where card IP address must be introduced

2) LOGGIN: To login as administrator introduce password: 12345678

3) FUNCTIONS MENU

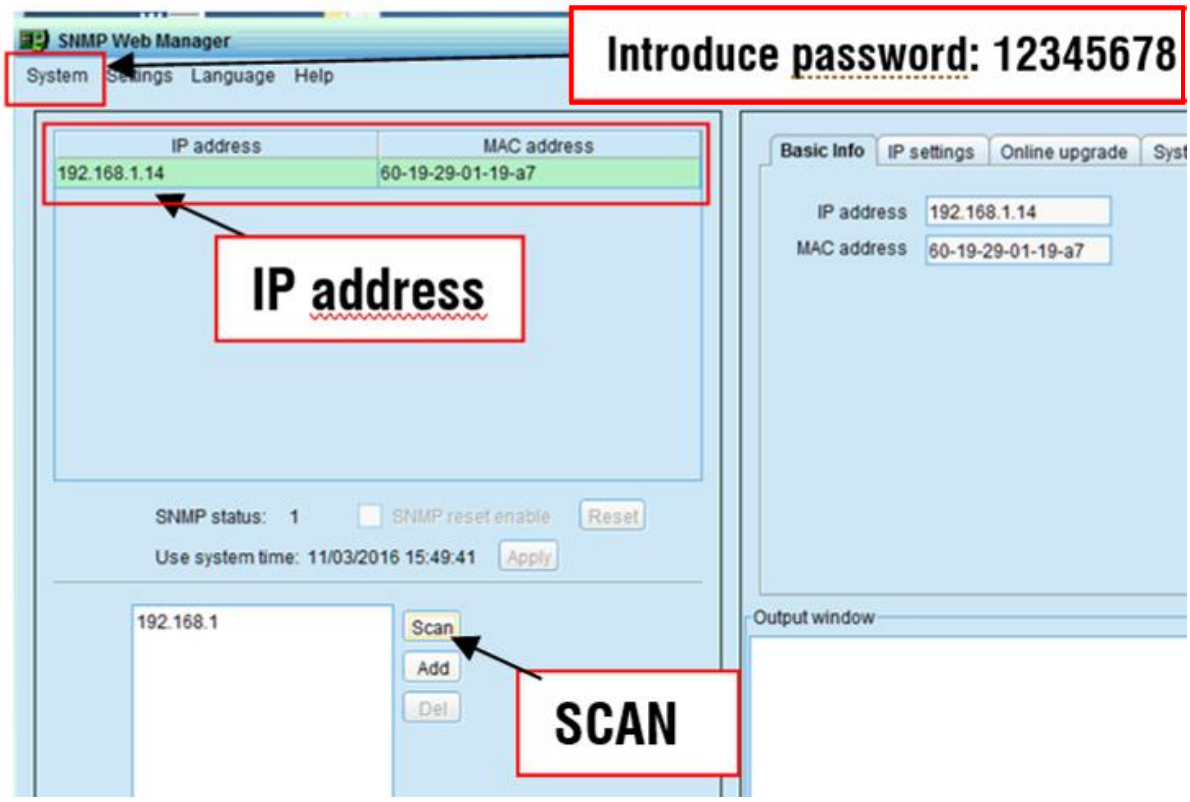
DHCP NETWORKS

To know which IP has been assigned to the card by DHCP network, user can run SNMP Manager software to perform scan. SNMP Manager is available as separate software in the CD, or it can be run from ATS Monitor Software (as indicated in software manual).

Install and execute SNMP Manager to open interface window as next figure shows:

We suggest to login as administrator in the System section with password: 12345678

SNMP WEB MANAGER:



Press SCAN to show all cards with dynamic IP available in the network. **This process could take some minutes. Sometimes this SCAN process must be performed more than once, until detecting cards.**

Take note of the IP for the card and type it in the address bar in the Web Browser. You can also simply double click over IP address listed in the SNMP Manager window. System will open Web Browser with **ATS WEB Pro** interface.

STATIC IP NETWORKS

If the network where STA will be connected is static IP network, the network administrator must assign an IP to the STA LAN card. This can be done by following procedure:

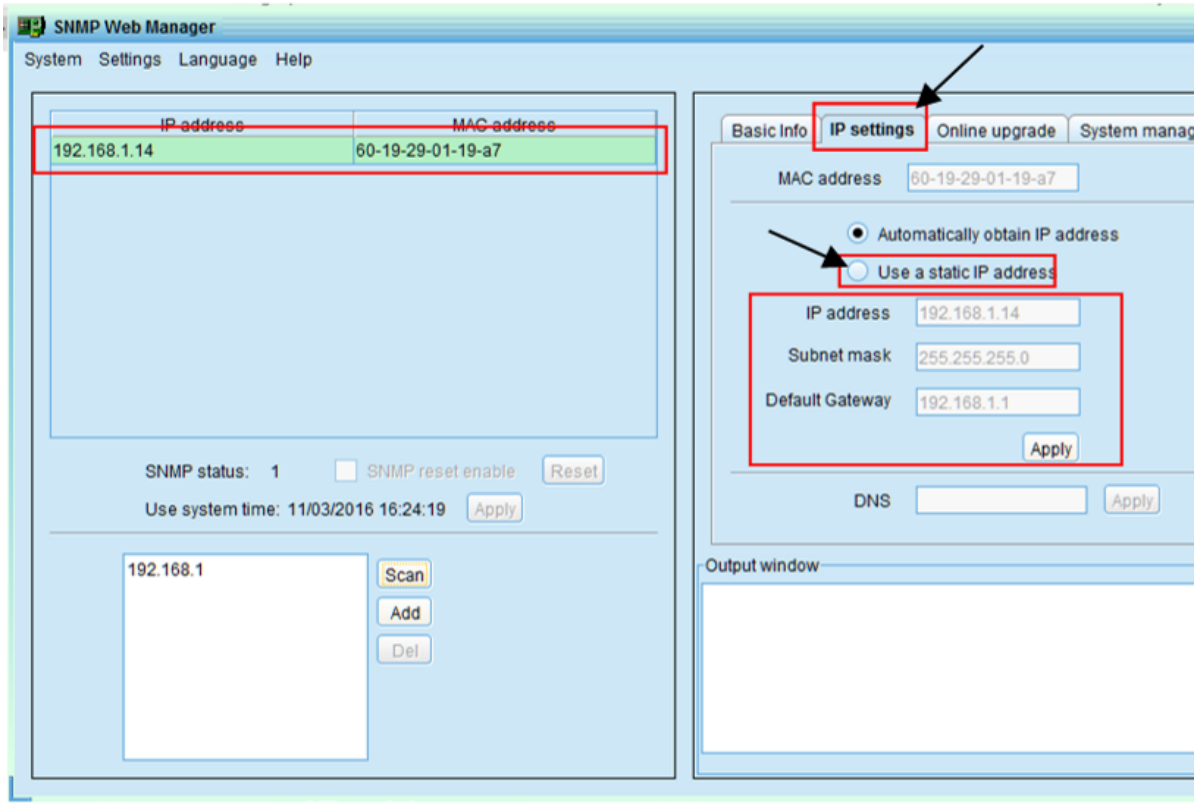
1.- STA with SNMP card must be ON

2.- One PC with SNMP MANAGER or ATS Monitor software must be connected to the SNMP card directly by a RJ45 cable. There are new SNMP cards that can be detected though the network. For those cards PC can be connected to the network and try to contact SNMP card.

3.- SNMP MANAGER must detect card automatically. If not, a manual SCAN must be done. **This scan process could take about 2 to 5 minutes. Do several scans if necessary**.

4.- Select the IP shown in the left area of the SNMP Manager screen. As shown in the figure

SNMP WEB MANAGER:



5.- Open IP SETTINGS tab and select option: “Use a Static Address”.

NOTE: If system does not allow modifications do SCAN again and repeat previous steps.

6.- Enter static IP address, Subnet mask y Default Gateway.

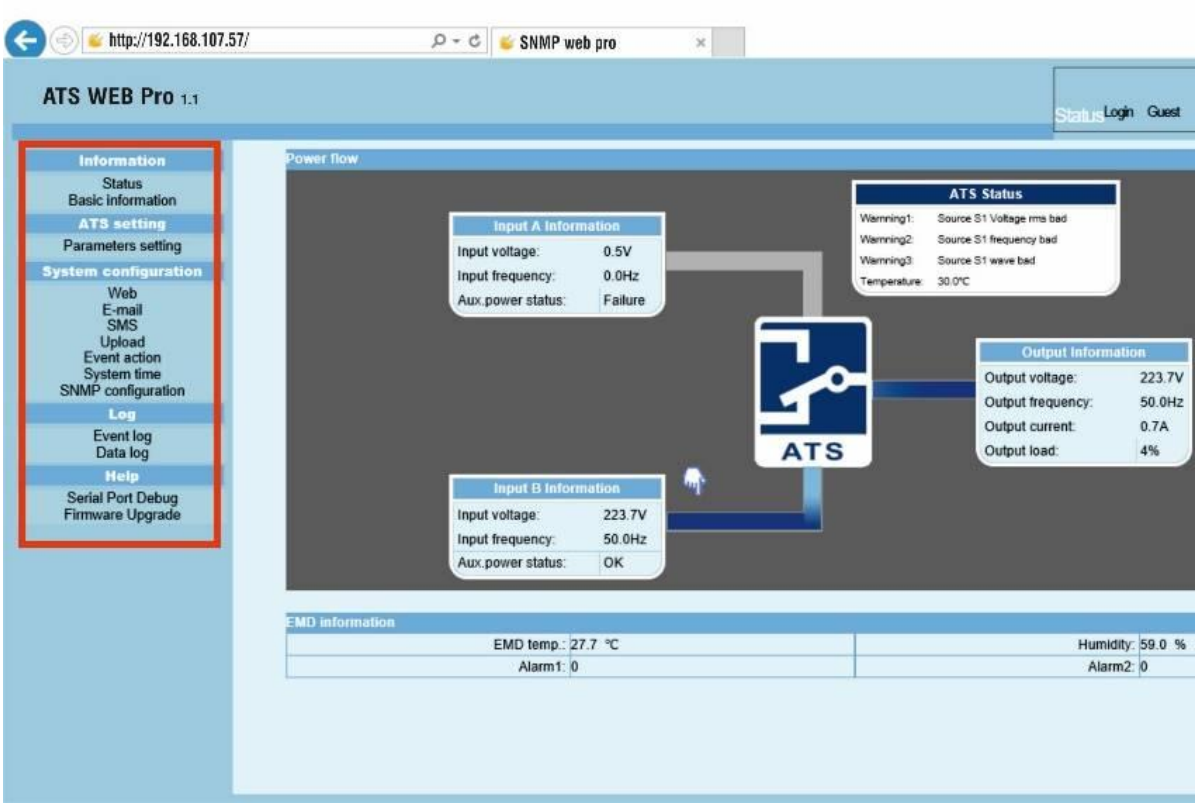
7.- Select APPLY command key to save modifications.

System could require you a password. In that case introduce password: **12345678**. Then select APPLY again to save modifications. System must show a message:

“OPERATION SUCCESSFULL”

ATS WEB PRO INTERFACE

In the following image you will find Functions Menu area:



INFORMATION:

STATUS:

This section offers information about the STA including:

- Values of A and B Inputs: Voltage, Frequency, and Line Status
- Output values: Voltage, Frequency, Current, and Load connected to STA (%).
- Temperature and Humidity values and alarms. Only if Sensor-TH is connected to the SNMP card

BASIC INFORMATION:

Provides information about STA technology: CPU Firmware version, STA Serial Number, STA Ratings (Voltage, Current, Frequency), SNMP Firmware version.

ATS SETTINGS: Parameters Settings

In this area operating parameters can be configured:

- Maximum and minimum admissible voltage values for Inputs A & B.
- Maximum and minimum frequency values admissible for Inputs A & B.
- Suitable values of voltage and frequency to come back to normal, after an Input AC range failure.
- Overload alarm point and fault point

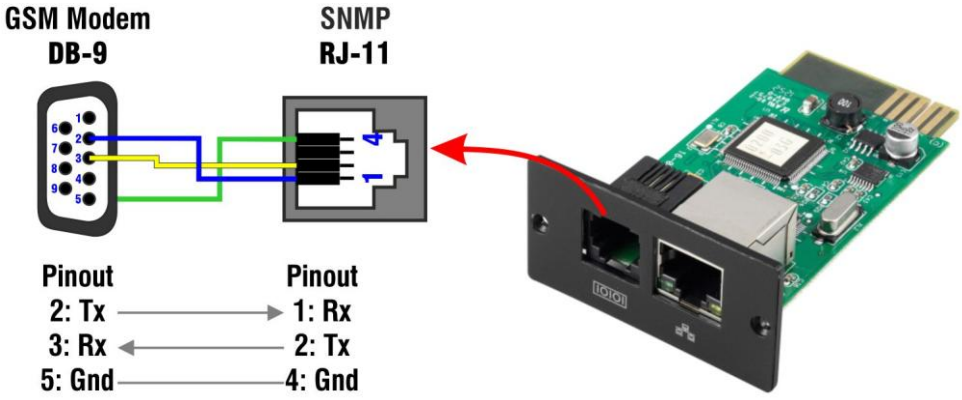
SYSTEM CONFIGURATION:

In this area important functions can be configured. For example:

- Usernames and passwords to access **ATS WEB Pro**.
- Selecting HTTP & HTTPS Protocols

- Emails configuration
- SMS sending (it requires external GSM connected to port B of the card, Check figure below).

GSM Connection Pin-Out



RJ11 – DB9 Cable not included

The GSM Modem configuration must be as follows:

- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: Hardware Flow control
- Rata de Baudio: 9600
- ECHO: Off

Additionally, in the **Event Action** configuration, "SMS Send when any event occurs" checkbox must be enabled, otherwise, SMS sending will not work, even using the **Test** button.

Finally, make sure the GSM Modem is properly connected to B Port of SNMP Card (RJ11 Port).

- Upload: Parameters to upload data to servers. It is divided in 2 sections:
  Data Log: Configuration to upload Event and Data Logs data to a server.
  Data Center: Reserved for future use.
- Event Action: When there are events in STA, SNMP card can send emails or SMS, according to configuration in this section.
- System Time: To configure date and time.
- SNMP Configuration: To configure LAN parameters for the SNMP card.

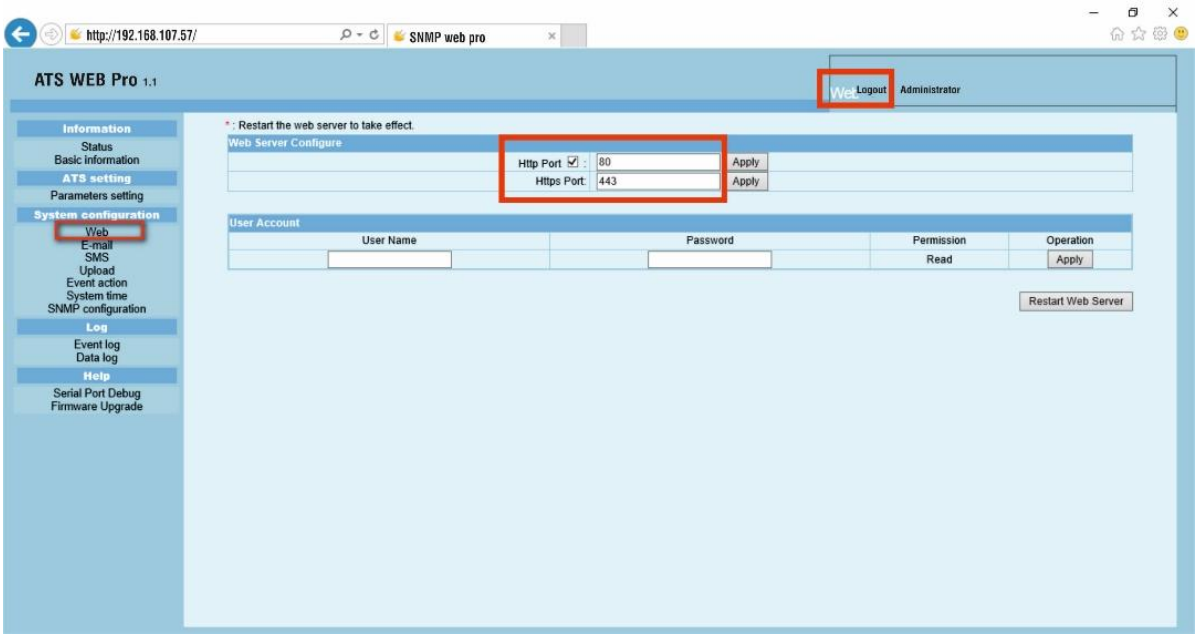
LOG: Event and data logs can be checked in this section

HELP: Serial Port Debugging: Only for service purposes. Allows to check communication between card and external device.

WEB CONFIGURATION

Http & Https Ports

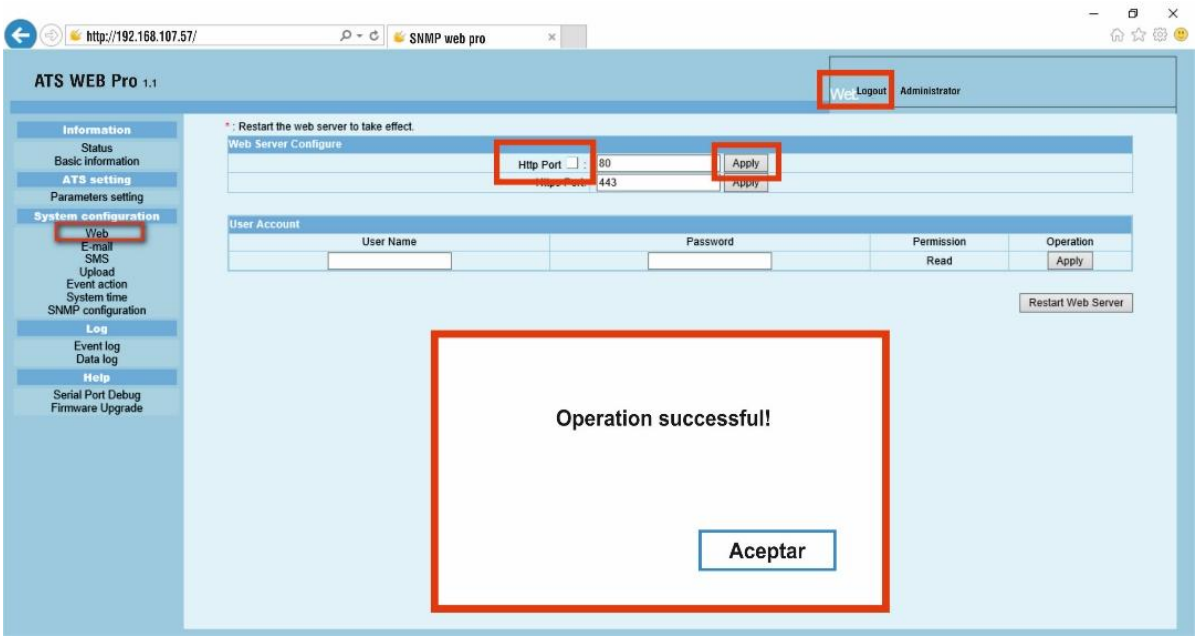
SNMP06 supports both **http** and **https** communication protocols, as seen in the following figure:



Factory set is Http communication. To operate **only** under **https** protocol, http port 80 must be disabled. Otherwise, card would communicate under any of these 2 protocols.

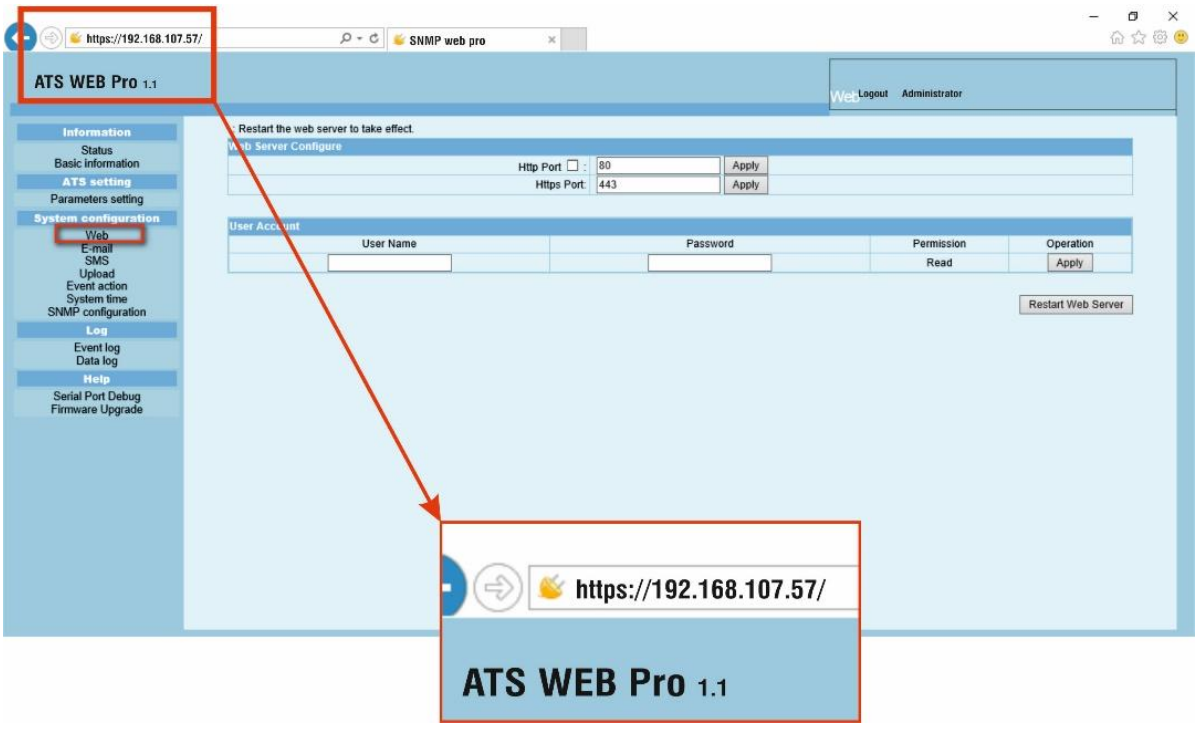
To activate Https protocol, follow this procedure:

1. Make sure you have already logged in as administrator by introducing password: “12345678”. If you do not enter as administrator, modifications will NOT be saved.
2. Check option Https Port and select APPLY.
3. Uncheck option Http Port and select APPLY to disable port 80. Only if port 80 is disable, card will be forced to communicate under Https protocol. A message OPERATION SUCCESSFUL must be shown. Select Accept button. See next figure as reference.



4. Click “Restart Web Server” button to restart web server and activate modifications.
5. **Wait about 30s to save changes** and update Web Browser with F5 key (in Windows). Web Browser must response with a message indicating communication is lost. This is because port 80 is disabled and HTTP communication is prohibited.
6. At this moment you can check if HTTPS protocol is active by introducing in the Web Browser bar address, the IP Address of the card preceded by https://
   For instance: **https://192.168.1.18**

7. Web Browser will open **ATS WEB Pro** interface under HTTPS as seen in the next figure.



Configuring access to ATS WEB Pro

In this window you can also configure authority to access **ATS Web Pro**. Please enter access ID and password in each column. After each entry, select APPLY to save changes.

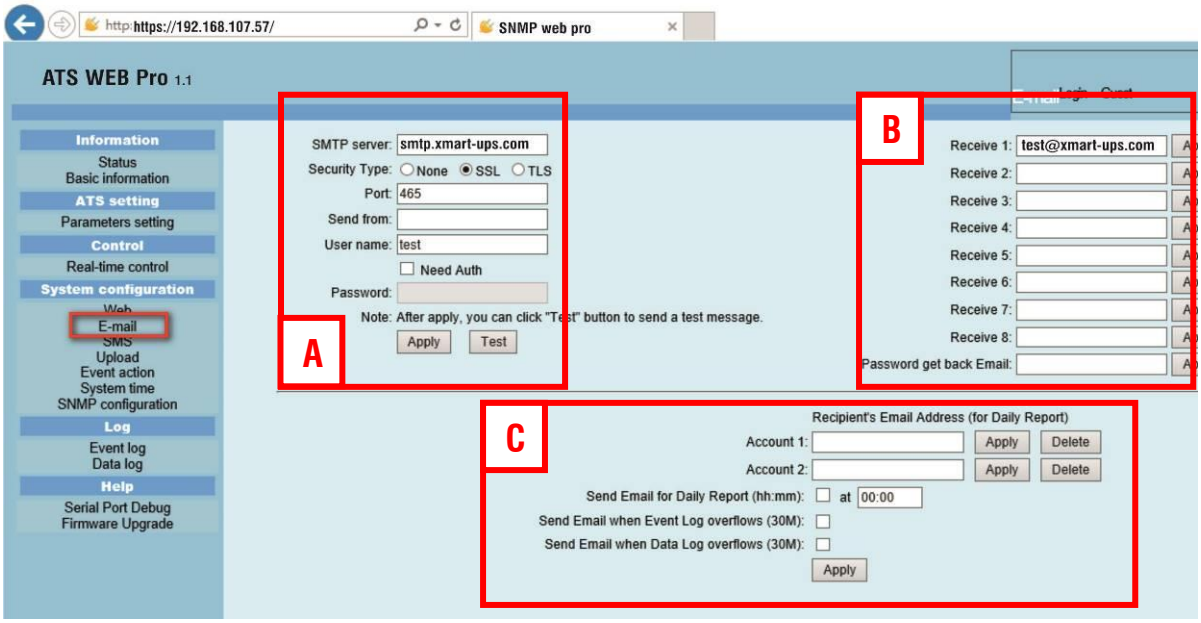
After all information has been entered, click “Restart Web Server” button to restart web server and activate modifications.

EMAILS CONFIGURATION

SNMP card can send emails using accounts based on SNMP, SSL or TTL servers.

If your mail server has two-step verification method to access the account, go to **APPENDIX F** of this manual; otherwise, continue in this section. All values are Default empty.

Check **SYSTEM CONFIGURATION** / **E-mail** to configure parameters like email server name, email account name & password (Area tagged as **A**), up to 8 receivers (Area tagged as **B**), etc. See next figure for reference:



CONFIGURING EMAIL SENDER:

SMTP server:	email server to be used to send emails. For instance: **smtp.gmail.com** for Gmail
Security Type:	Type of email server to be used: **NONE:** Usually for web-domain email servers. **SSL:** For servers with security SSL like Gmail, Yahoo, etc. **TLS:** For emails servers with TLS security.
Port:	Depends of the type of server. Usually: **NONE: 25** / **SSL: 465** / **TLS: 587**
Send from:	Name of the email account to send emails. E.g.: abc@xxxxxxxxxxx.com
Username:	Username of the email to send emails. Usually same email account name.
Need Authorization:	Check this option for accounts that require Authorization (“Need Auth”)
Password:	Email account password.
APPLY	Click APPLY button to save modifications.

EMAIL RECEIVERS:

On the right side of the screen (Area tagged as **B**) there are 8 fields to configure destination email addresses. Select APPLY for each receiver added.

DAILY REPORT:

Every day, SNMP can send an email reporting Daily Reports (Area tagged as **C**), here you can configure it:

Account 1: Account 2:	Email addresses to receive Daily report. Select "APPLY" on the right for each receiver added
Send email for daily report:	Mark checkbox to activate, also select the time.
Send email when Event Log overflows:	Mark checkbox to activate.
Send email when Data Log overflows:	Mark checkbox to activate.

IMPORTANT NOTES:

- **The email-sending firmware of the SNMP card has not been compatible with the security settings of Hotmail® and Microsoft® servers since September 2024, due to changes in their authentication system.**
- **If you have any questions, contact either your Internet/email provider or your IT administrator.**
- **After configuring the email section, we recommend testing it by clicking the "TEST" button.**

System will response with a message: "TEST SUCCESSFULL" when email has been sent without errors. In case email cannot be sent, system will show a failure message.

IMPORTANT: If SNMP Web Pro reports problems sending emails, it can be for one of 2 reasons:

1.- A mistake in one or more data fields. Check and correct any wrong data.

2.- DNS has not been saved automatically in the card. In this case, follow this procedure:

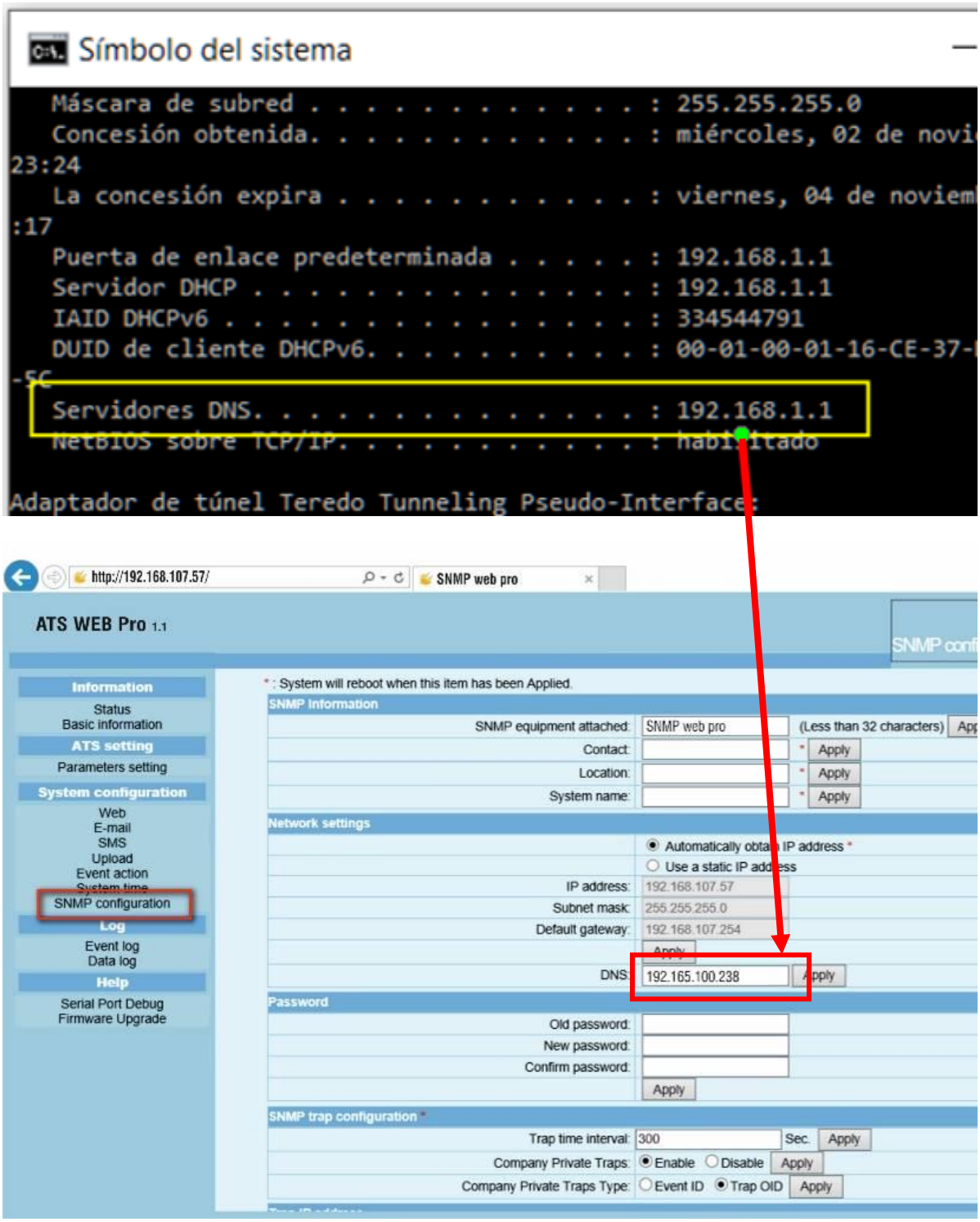
a) Check **System Configuration** / **SNMP configuration** / network settings.

b) Check if DNS field shows appropriate DNS. If it shows 0.0.0.0, user must enter manually DNS of the network and select APPLY. See next figure for reference.

The way to find out DNS of your network depends on your operating system. For instance, in windows you can go to system command line of your PC and execute this command:

ipconfig -all

Your operating system will list several related parameters. Look for the line dedicated to DNS server. In the below example the value is: 192.168.1.1. (See the next figure)



Go to **System Configuration** / **SNMP configuration** to mark option: “Use a static IP address”. Enter DNS value and select APPLY. Wait for some seconds.

Mark again option: “Automatically obtain IP address” (for DHCP networks) and select APPLY. Wait some seconds during card restarts to recover communication.

Go back to the **Configuration** / **E-mail** section and test again.

APPENDIX B
SNMP: INSTALLATION AND OPERATION IN XSI INVERTERS

INTRODUCTION

XMART XSI inverters are high-tech equipment for power generation from solar energy. These kinds of installations are usually unattended, so remote supervision and control are of vital importance.

The way for remote communication with the inverter is through a network with an SNMP card, which must be installed in the equipment. The installation instructions for the SNMP card can be found in the inverter User Manual, in the section dedicated to Inverter installation.

The SNMP card can store events and data in its internal memory without relying on external monitoring software. It can also send emails with alarm messages if the LAN has a router with internet access.

COMMUNICATION WITH XSI INVERTERS

There are 2 ways to communicate with SNMP06 cards:

A) MONITORING SOFTWARE

Software for monitoring and controlling the inverter depends on the model, as shown in the following table:

Models	Software
XSI-B-120-MPP – 1K to 3K XSI-B-230-MPP – 1K to 5K	WatchPower
Solar Inverters (XSI) 6KVA y Higher	SolarPower Pro

Both software are available in Download section of our website (**www.xmart-ups.com**), as well as their respective manuals where their instructions for installation, use, features and functionalities can be found. Install appropriate software on the PC from which the inverter will be monitored and operate it as explained in the respective User Manual.

B) COMMUNICATION THRU WEB BROWSER – SNMP WEB PRO INTERFACE

User can monitor any inverter in the LAN from any PC in same LAN, accessing SNMP06 card from Web Browser by introducing IP address of the SNMP06 to open SNMP Web Pro interface. Browser will contact SNMP06 card and open SNMP Web Pro interface from where inverter can be configured and monitored.

NOTE:

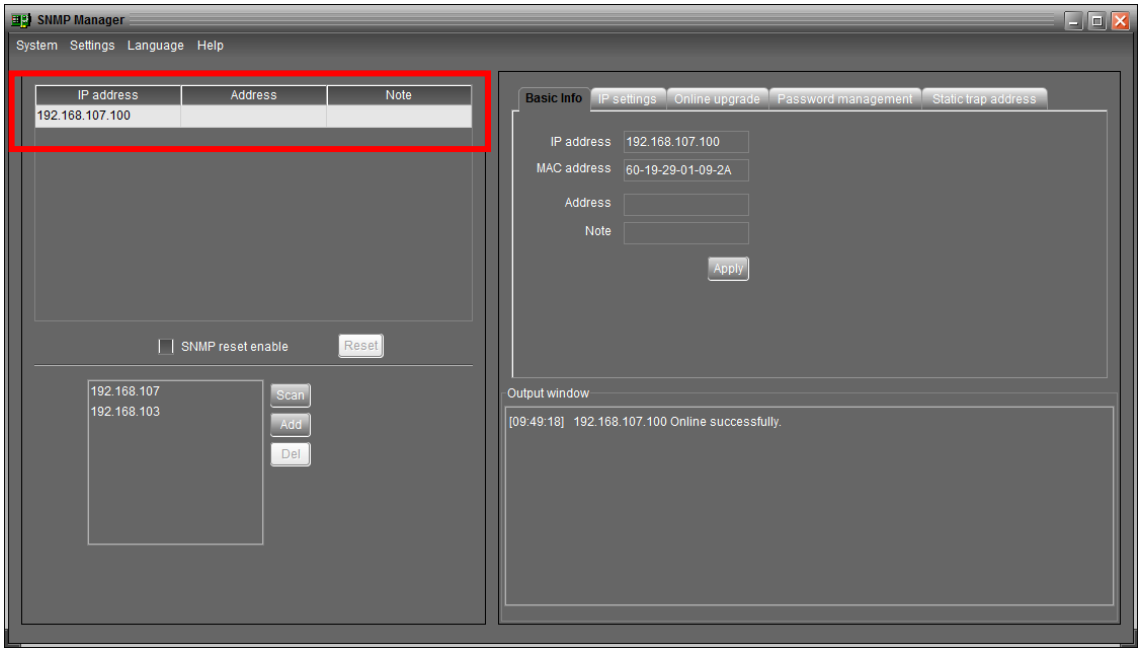
In the case of the **XSI-230-OGP – 3K to 5K** family, communication via the network through the SNMP card can only be done through SNMP Web Pro interface, from the PC browser. Neither **WatchPower** nor **SolarPower Pro** are compatible with this family of solar inverters.

If **WatchPower** or **SolarPower Pro** has been installed, there is a second way to communicate with SNMP card, using the following procedure:

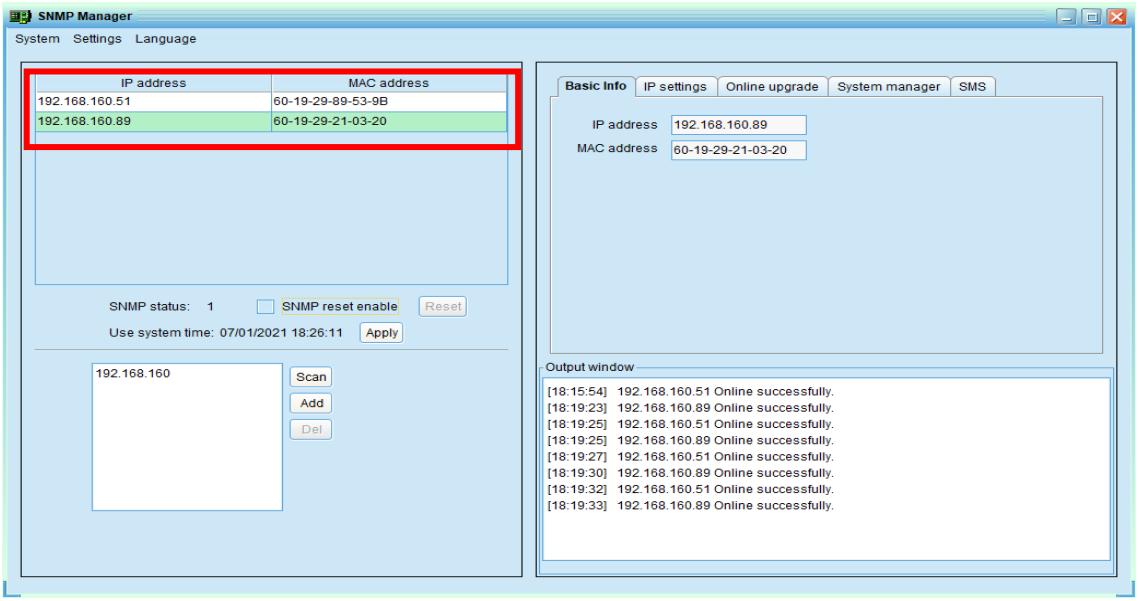
- Open the **SNMP Manager** Plug-in. The procedure is explained in the manual of each software.
- Enter the IP address of the SNMP card of the inverter you want to monitor. If you don't know the address, enter the network segment you are in (for example: 192.168.0) and scan for units in the network with SNMP card. The procedure is also explained in the manual of each software.

The SNMP Manager interface varies depending on the installed software.

SNMP Manager for WatchPower



SNMP Manager for SolarPower Pro



- Red box shows the IP addresses of the devices detected on the LAN.
- Double click on the IP address you want to work with. This will open the **SNMP Web Pro** interface from where inverter can be configured and monitored.

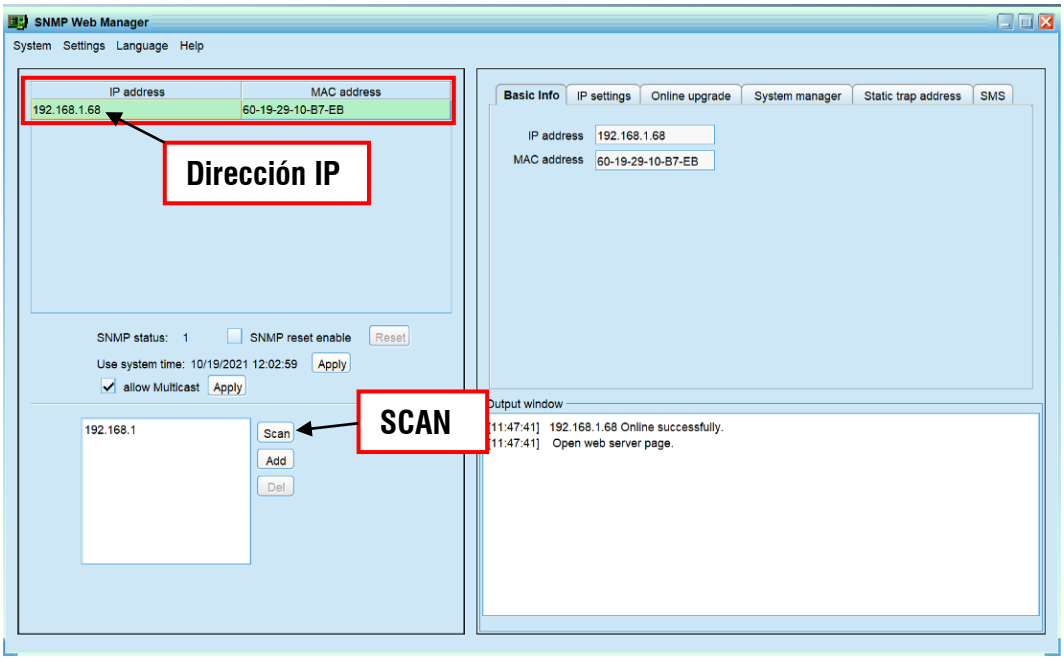
If the inverter with SNMP card is in a DHCP network, it will receive a dynamic IP address from the network. If it is connected to a static network, then network administrator will need to assign an IP address to SNMP device. Please check "Network Settings" section later in this manual.
If neither **WatchPower** nor **SolarPower Pro** have been installed, there is an additional way to establish contact with the SNMP card: **SNMP WEB MANAGER**.

SNMP WEB MANAGER

It is a service software to scan and detect all SNMP cards in the network. It can be downloaded from **Download\Software** section of our WEB page: **www.xmart-ups.com**.

Once installed, there will be a Shortcut icon on your desktop, like the one on the right:

When executed, the **SNMP Web Manager** interface is displayed, as in the following figure:



COMMUNICATION IN DHCP NETWORKS (DYNAMIC IP)

To know which IP has been assigned to the card by DHCP network, click on "Scan" button on screen. On the left IP and MC addresses will be displayed.

SCAN could take some minutes. Sometimes scanning must be done several times to detect all cards.

COMMUNICATION IN STATIC IP NETWORKS

If the inverter will operate in a static IP network, then network administrator must assign an IP to the inverter's LAN card. This can be done as follows:

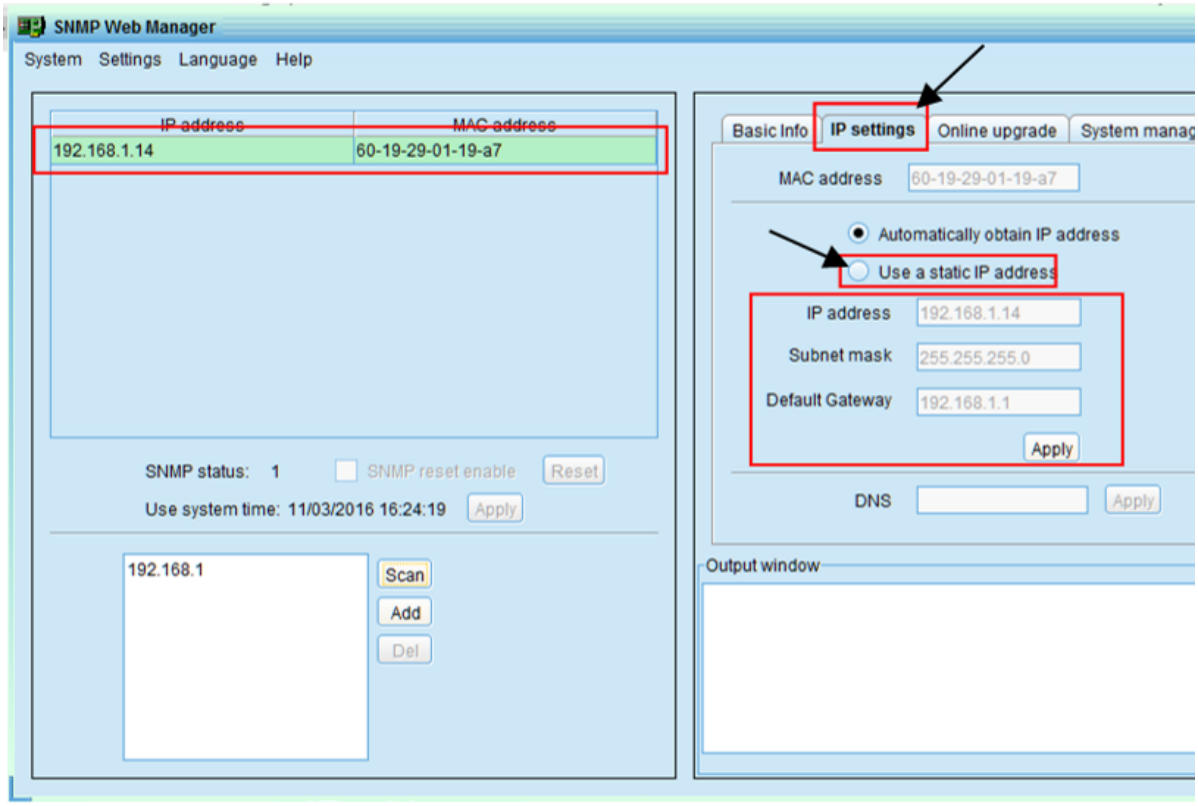
1.- Inverter with installed SNMP card must be ON

2.- One PC with **SNMP Web Manager** installed must be connected to the SNMP card directly by a RJ45 cable, without passing thru any router or switch. There are new SNMP cards that can be detected though the network. For those cards PC can be connected to the network and try to contact SNMP card.

3.- **SNMP Web Manager** should detect card automatically. Otherwise, a manual SCAN must be done.

This scan process could take about 2 to 5 minutes. Do several scans if necessary.

4.- Select the IP shown in the left area of the **SNMP Web Manager** screen. As shown in the figure



5.- Open IP SETTINGS tab and select option: “Use a Static Address”.

NOTE: If system does not allow modifications do SCAN again and repeat previous steps.

6.- Enter static IP address, Subnet mask y Default Gateway.

7.- Select APPLY command key to save modifications.

System could require you a password. In that case type in password: **12345678**. Then select APPLY again to save modifications. System must show a message:

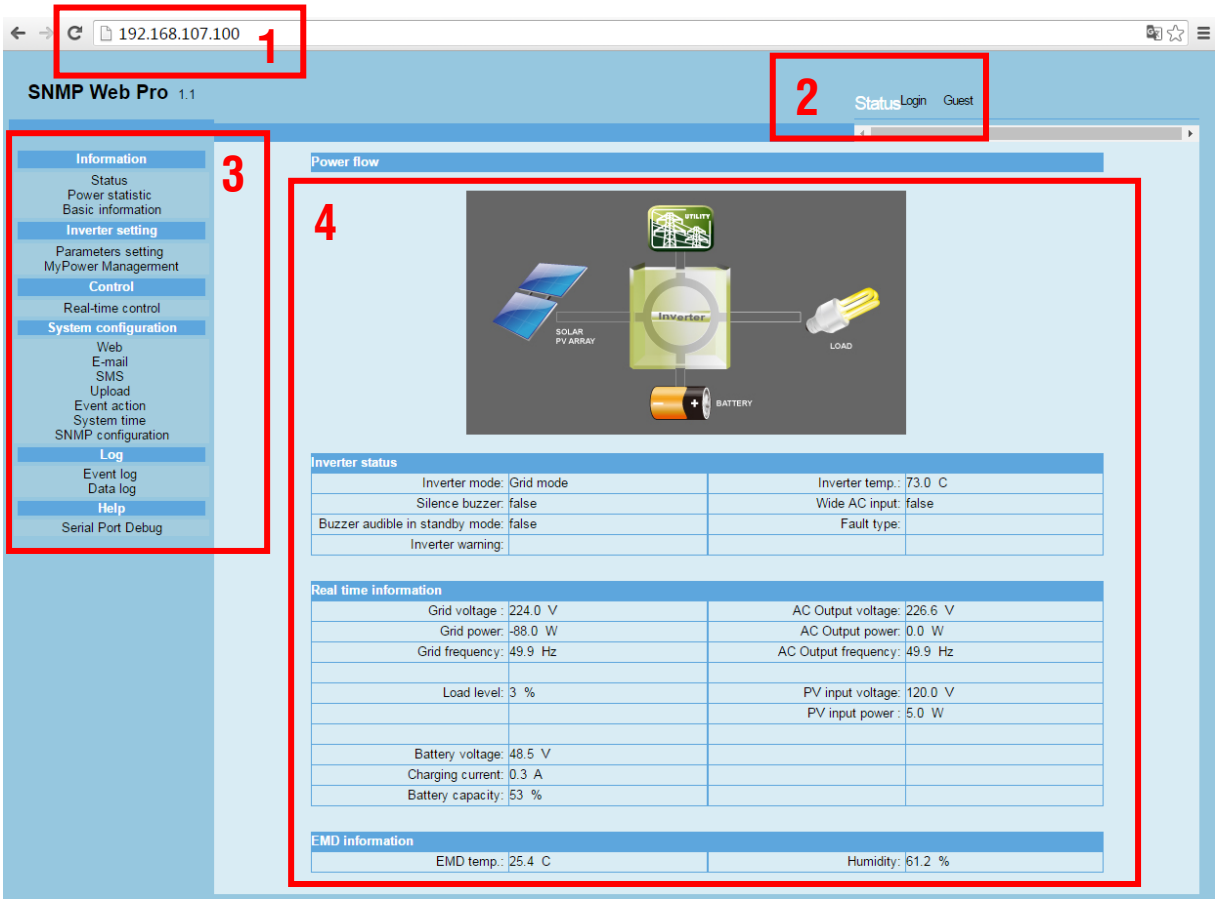
“OPERATION SUCCESSFULL”

Once you know the IP address of the SNMP card you are interested in, there are 2 ways to access it:

- Double click on the selected IP address in the **SNMP Web Manager** interface, upper left area.
- Enter the IP address in the Address Bar of your internet browser.

Both will open the **SNMP Web Pro** interface in the browser, communicating with specific SNMP card. See the following figure for reference.

WEB BROWSER COMMUNICATION INTERFACE: SNMP WEB PRO.



This interface is divided in different sections:

1) ADDRESS BAR: Where card IP address must be introduced

2) LOGGIN: Shows the user type and allows changing it. Password to login as administrator is: 12345678.

3) FUNCTIONS MENU: Tools for interface and inverter settings.

4) MAIN SECTION: Information and control area, according to selection in Functions Menu.

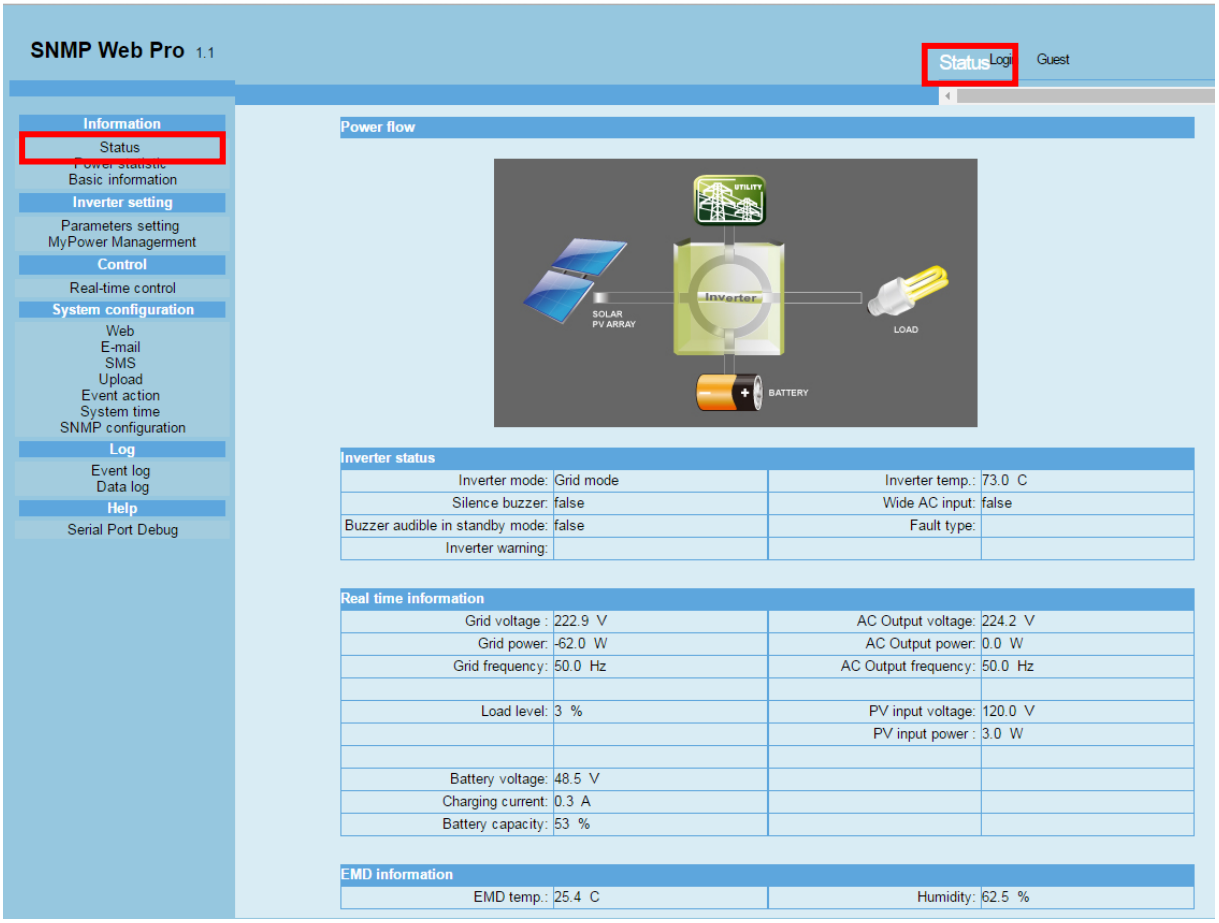
SNMP WEB PRO INTERFACE

This section explains the Function Menu area, by sections. Shown windows may vary, depending on the supervised inverter model.

INFORMATION

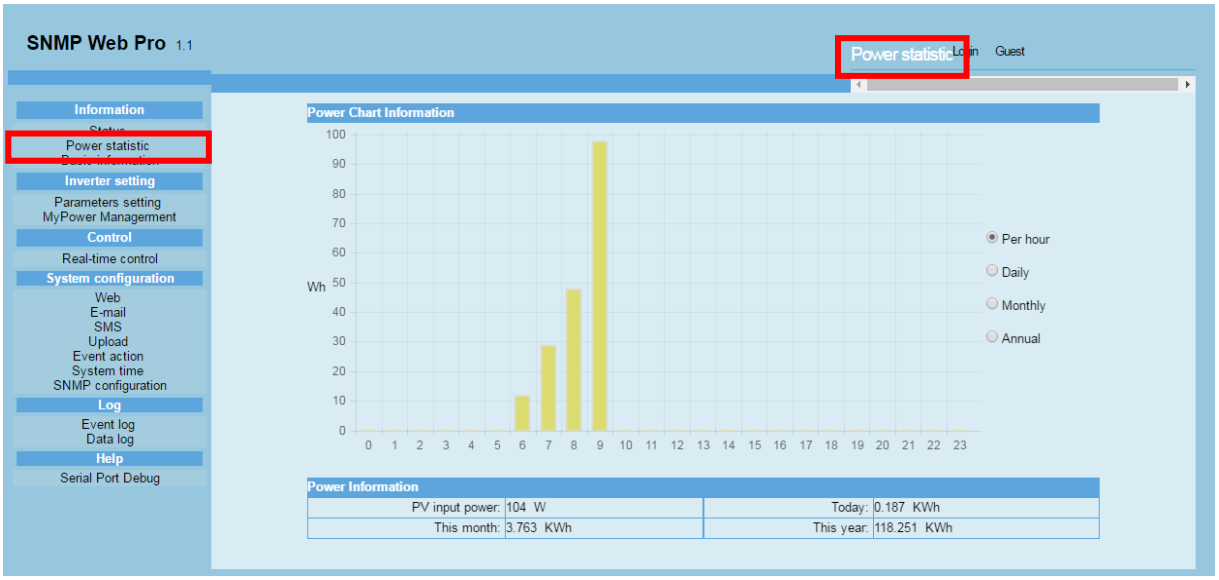
Displays wide information about monitored unit. It consists of the following sections:

Status:



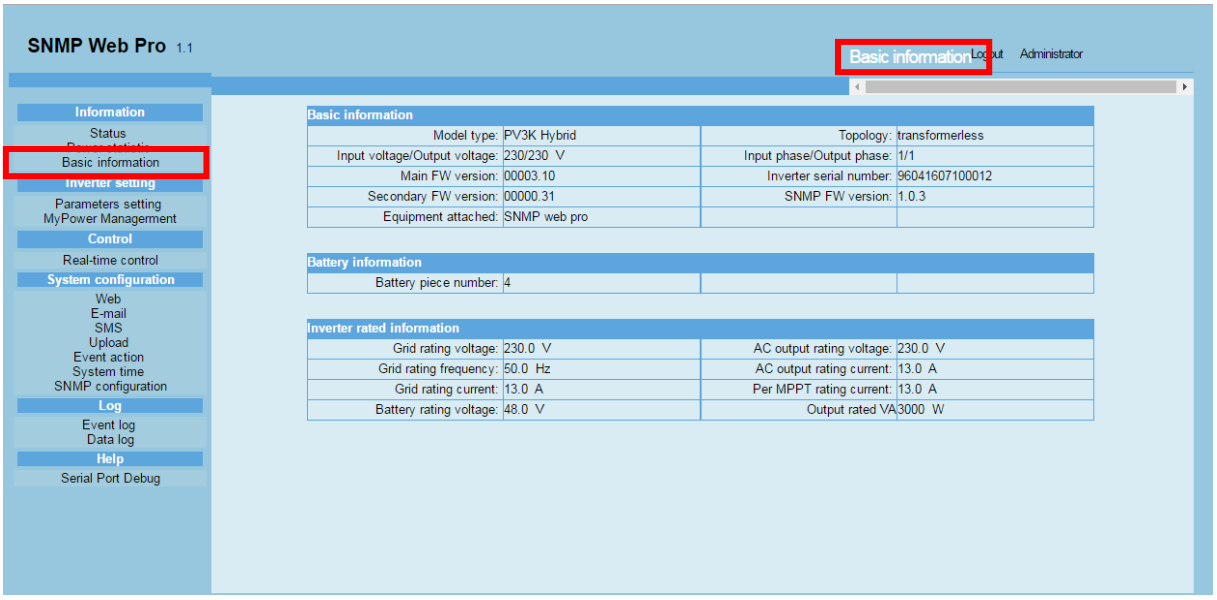
This section offers inverter information, in real time, such as: Power flow and status of the inverter, Voltage, frequency and power of the line and at the output of the inverter, Voltage, capacity and charging current of the batteries, Values and Alarms of temperature and humidity (ONLY if an optional TH-Sensor is connected).

Power Statistic:



This window shows the power generated by Hour, Day, Month or Year, in graph form.

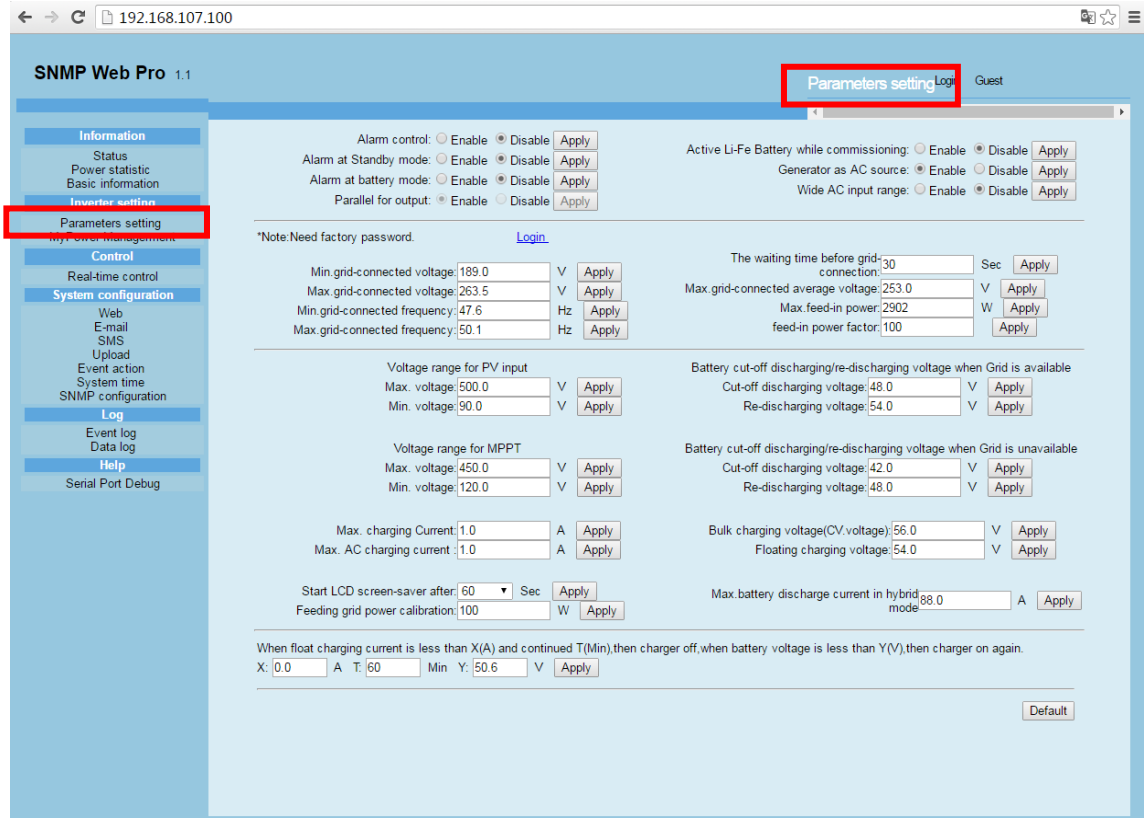
Basic Information:



This window offers the inverter design and technology values, such as: CPU firmware version, Serial Number, topology, Nominal Values (Voltage, Current, Frequency), SNMP Firmware version. As well as the number of batteries.

INVERTER SETTINGS:

Parameters Settings



In this area, all operative parameters adjustable from the software, can be adjusted. The parameters and values may vary depending on the inverter model.

Notes:

- Functions are either enabled or disabled, with the "Enable" or "Disable" buttons respectively.
- To change quantities, use up/down arrows or modify the values directly in the field to be changed.
- After changing any function, click “Apply” button to save changes. Otherwise, changes will be lost.
- Select “Default” button to load default parameters of the inverter.
- Functions not supported by the inverter will not be accessible in the interface.

Adjustable Parameters:

Alarm Control:

If enabled, silences audible alarm in general.

Alarm at Standby mode:

If enabled, silences the Standby Mode audible alarm.

Alarm at battery mode:

If enabled, silences the Battery Mode audible alarm.

Parallel Output:

If enabled, the inverter can be installed in parallel with other compatible units, allowing the connection and synchronization of their outputs. Please check details of parallel connection and operation in the inverter manual.

If not enabled, the inverter can only be installed individually.

Generator as AC source:

If enabled, it makes inverter's AC input more compatible with the output of a generator.

Activate Li-Fe battery while commissioning:

If enabled, the Li-Fe batteries will be activated at start-up.

Wide AC input range:

If it is not enabled, acceptable voltage and frequency ranges of AC input will be set by values configured in the equipment, through the following 4 adjustable parameters.

If enabled, the acceptable input ranges are the following:

- Voltage: 170V to 280V.
- Frequency: 40Hz to 55Hz for 50 Hz systems and 55Hz to 65Hz for 60 Hz systems.

When Grid voltage or frequency is out of these ranges, inverter is not allowed to feed the Grid, only supply power for the installation and charge the batteries.

Min. grid-connected voltage:

Minimum AC line voltage, for the inverter to remain connected to the line.

Max. grid-connected voltage:

Maximum AC line voltage, for the inverter to remain connected to the line.

Min. grid-connected frequency:

Minimum AC line frequency, for the inverter to remain connected to the line.

Max. grid-connected frequency:

Minimum AC line frequency, for the inverter to remain connected to the line.

The waiting time before grid-connection:

Waiting time to connect to the AC Line, once all the requirements have been met.

Max. grid-connected average voltage:

Average line voltage higher than this value is considered abnormal and alarm code 05 is activated.

Max. feed-in grid power:

Maximum power to feed the AC Line.

Feed-in power factor:

Adjustment range: -0.99 to -0.80 and 0.80 to 1.00

Max. PV input voltage:

Maximum acceptable voltage at the Solar input when AC Line is connected.

Min. PV input voltage:

Minimum acceptable voltage at the Solar input when AC Line is connected.

Max. MPP voltage:

Maximum acceptable voltage from solar panels, for MPP system.

Min. MPP voltage:

Minimum acceptable voltage from solar panels, for MPP system.

Max. charging current:

Maximum batteries charging current, includes solar power and AC input.

Max. AC charging current:

Maximum charging current coming from the AC line. If this value is higher than previous parameter, the Maximum Charge Current will be used also as the Maximum AC Charge Current.

Start LCD screen saver after:

After this time, the LCD backlight will turn off.

The value 00 means LCD Always on. Default option: 02.

Feeding grid power calibration:

Calibration of power sent to Grid, in watts.

Adjustment range: -300 to 300.

Battery cut-off discharging voltage when Grid is available:

Minimum battery discharge voltage when AC line is available. At this point battery discharge stops.

Battery re-discharging voltage when Grid is available:

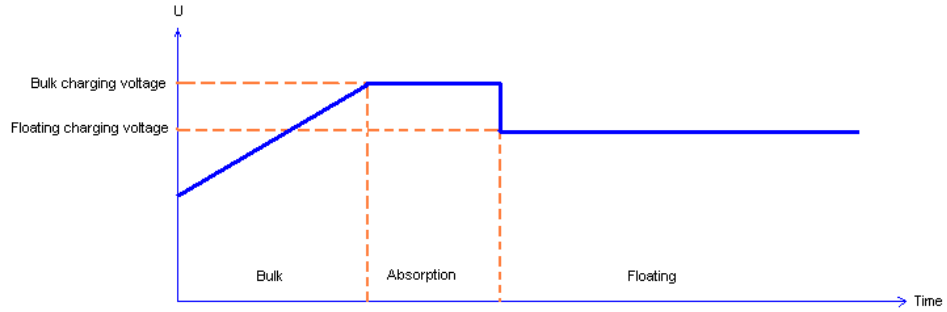
Battery recharge voltage, after having reached the End of Discharge Voltage, when the AC Line is available. When this voltage is reached, the batteries are enabled to be discharged again.

Battery cut-off discharging voltage when Grid is unavailable:

Minimum battery discharge voltage when AC line is not available. At this point battery discharge stops.

Battery re-discharging voltage when Grid is unavailable:

Battery recharge voltage, after having reached the "**Battery cut-off discharging voltage when Grid is unavailable**". When this voltage is reached, the batteries are again enabled to be discharged.



Bulk charging voltage (Max. Charging Voltage, Constant Current and Constant Voltage Stages)

Max. battery charging voltage in Constant Current and Constant Voltage stages. See previous figure.

Floating charging voltage:

Battery charging voltage in maintenance stage (Floating). See previous figure.

Max. battery discharge current in hybrid mode:

Maximum battery discharge current for Grid-Tie and Grid-Tie with backup modes.

When float charging current is less than X (A) and lasts T (Min), and then charger is off. When battery voltage is less than Y (V), and then charger is on again:

This function allows configuring inverter power-on and power-off, as follows:

- When the charging current is less than the value of the X (Amps) field, for a time equal to that of the T (Min) field, the charger turns off.
- When the battery voltage is less than the value of field Y (V), the charger is turned on again.

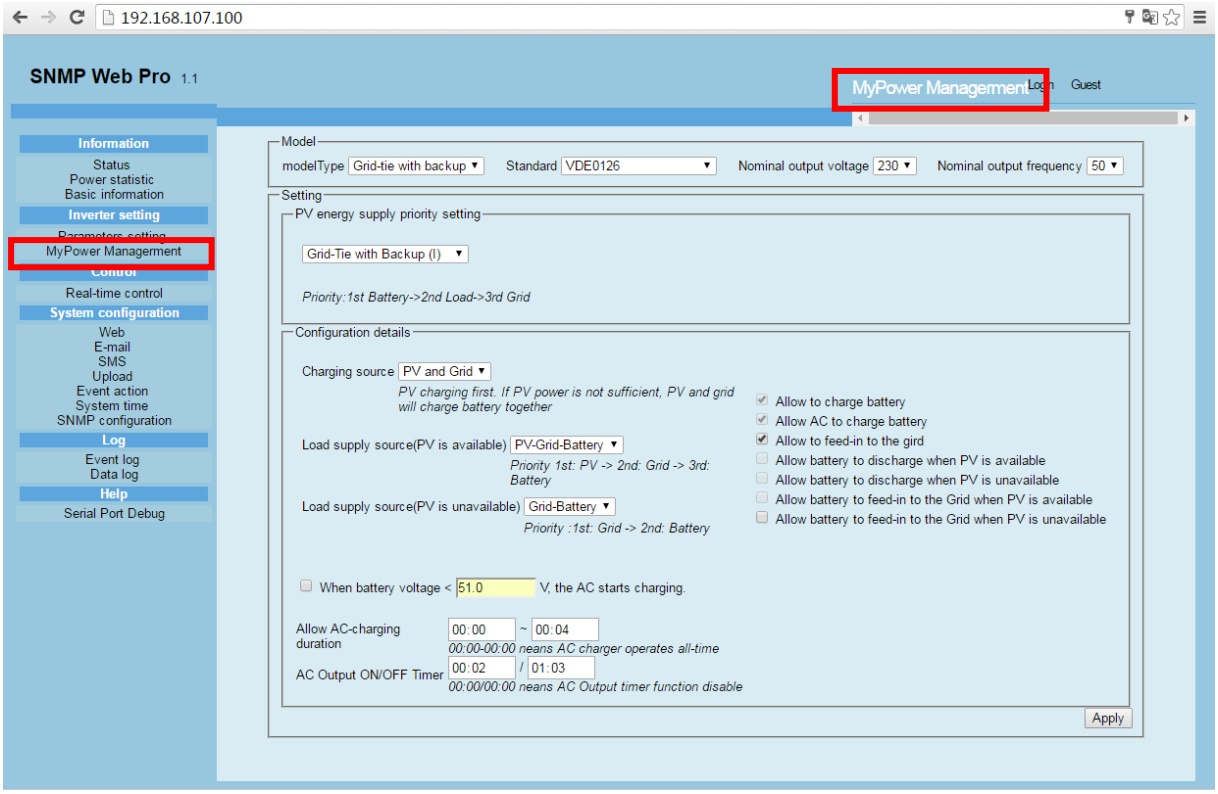
After making a change, "Apply" button must be selected to save it, otherwise modifications will be lost.

System time:

Represents inverter's system time. Any changes could affect generation calculations, so changes should be made with caution and certainty.

NOTE: All parameter setting must be made with inverter in Standby mode.

MyPower Management:



In this area, inverter operation mode and interface are configured in a personalized way.
It counts on the following sections:

Model:

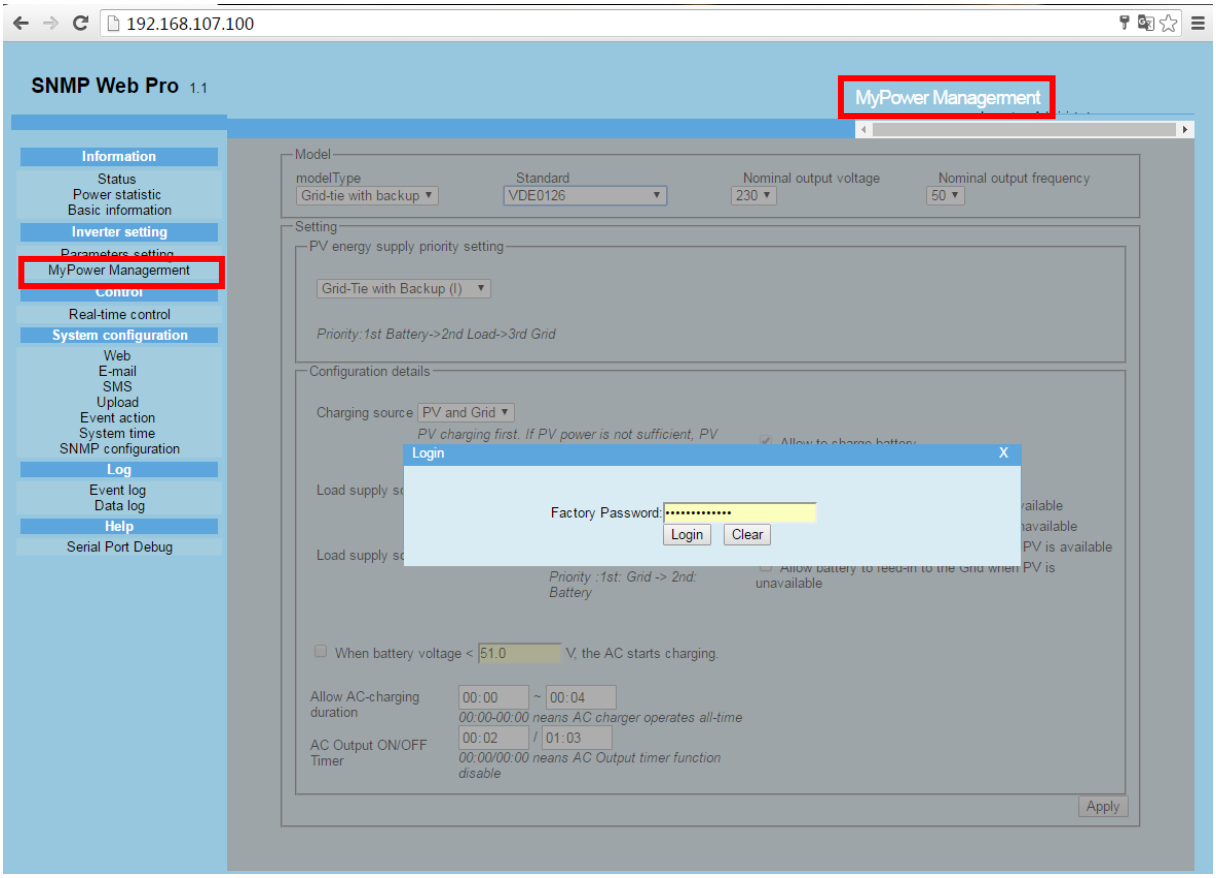
Model Type: There are 3 operation options for the inverter:

A. **Grid-Tie with Backup:**
   Power from solar panels can be sent to the Main AC Line (Grid), power the load, and charge batteries. In this mode there are 4 available options: I, II, III and IV, with which the user defines priority of solar power, source priority to charge the batteries, and priority to power the load. When option Grid-Tie with Backup IV is selected, inverter only operates between two work logics based on Peak Hour and Valley Hour of power consumption, previously defined for optimal use.

B. **Grid-Tie:**
   Power from solar panels can only be sent to the Main AC Line (Grid).

C. **Off-Grid:**
   Power from solar panels powers the load and recharges the batteries, sending energy to the Main AC Line (Grid) is not allowed.

Standard: Electrical standard used by the inverter. If you try to change it, software asks for factory password, not available for general use. Only factory can make this change. See following figure:



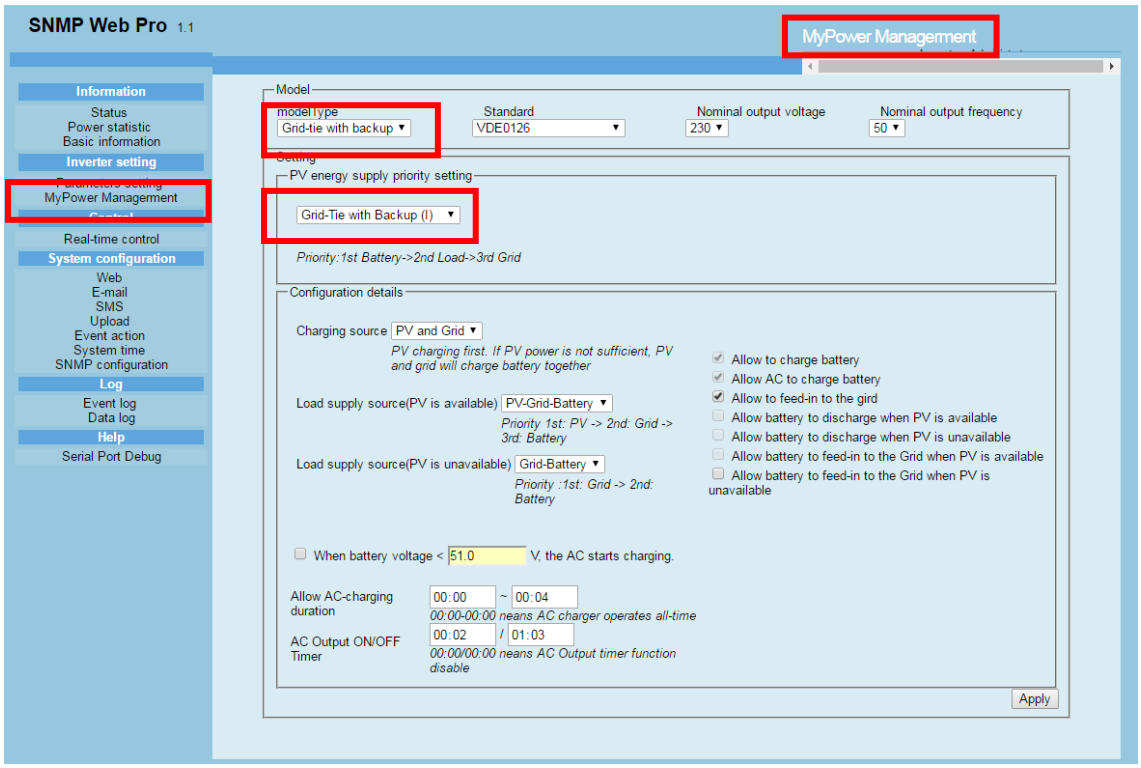
NOTE: This is a very sensitive technical issue that can cause malfunction or permanent damage to the equipment in case of errors, so it must be dealt with only by qualified personnel.

- Nominal Output Voltage. The available options are:
  - 220V models: 240V, 230V, 220V, 208V, 202V
  - 120V models: 127V, 120V, 110V and 101V.
- Nominal Output Frequency. Options available 50Hz and 60Hz.

Settings

Operation mode and parameters can be adjusted in this section:

GRID-TIE WITH BACKUP – Option: Grid-Tie with Backup I

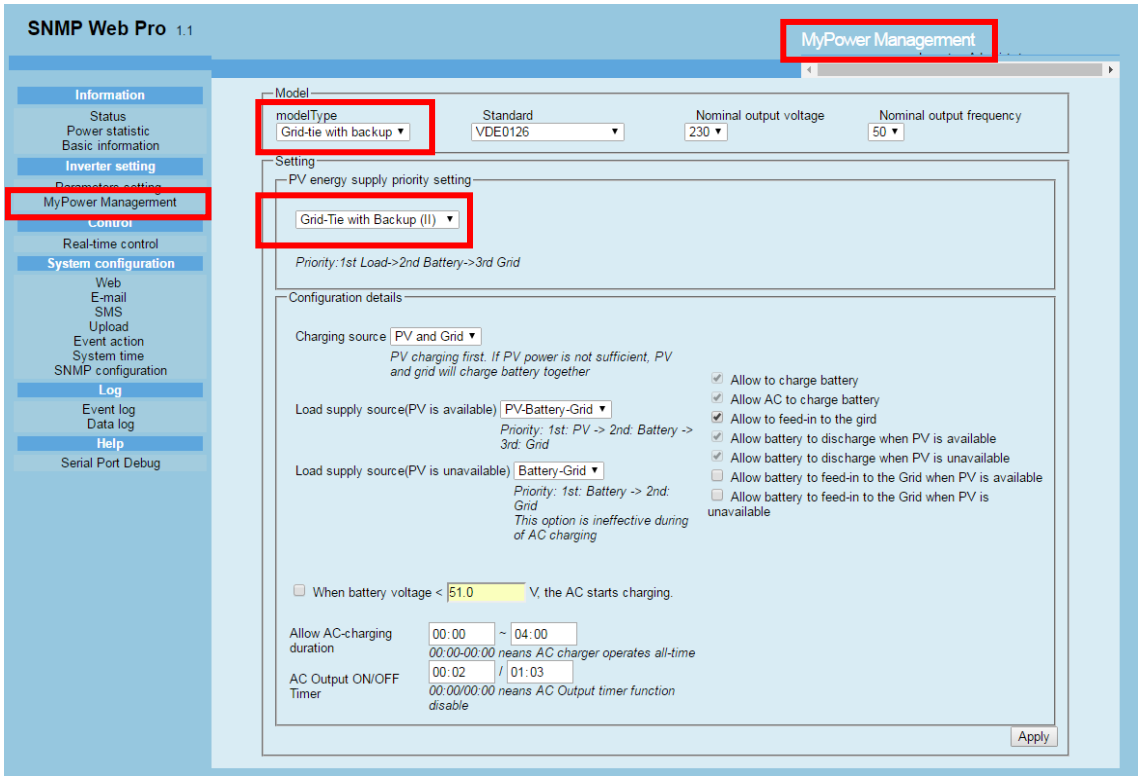


Parameters Setting:

- **PV Power supply priority setting: 1st Battery**, **2nd Load**, **3rd Grid**.
  Solar power will charge batteries first, then power the load and, if still available, feed the Grid.
- **Charging source**:
  Defines sources priority to charge batteries. Options:
  1. PV and Grid (Default Value): Solar Power will charge batteries and if it is not enough, Grid will co-charge.
  2. PV only: Only Solar Power will charge batteries.
  3. None: Battery charge is not allowed for any of inverter inputs.
- **Load supply source (PV is available)**
  1st PV (Solar Power), **2nd Grid** (AC Line), **3rd Battery.**
  With Solar power available, it is the first to feed load, then AC line and finally batteries. When batteries are not fully charged, then solar input will charge the batteries first and remaining power will be sent to the load, if it is not enough, Grid will feed the load simultaneously. If AC line is not present, batteries will power the load that cannot be covered by solar power.
- **Load supply source (PV is unavailable)**
  Priority to power the load when solar power is not available. Options:
  1. **1st Grid** (AC Line), **2nd Battery** (Factory Default)
     AC Line will power the load, if it is not available, the batteries will power the load.
  2. **1st Battery**, **2nd Grid** (AC Line),
     Batteries will power the load, if they are discharged, AC Line will power the load.

  Note: This option is ineffective during the AC Charging period and priority will automatically go to 1st Grid, 2nd Battery. Otherwise, batteries would be damaged.

GRID-TIE WITH BACKUP – Option: Grid-Tie with Backup II



Parameters Setting:

- **PV Power supply priority setting: 1st Load**, **2nd Battery**, **3rd Grid**.
  Solar power will power load first, then charge batteries and, if still available, feed the Grid.

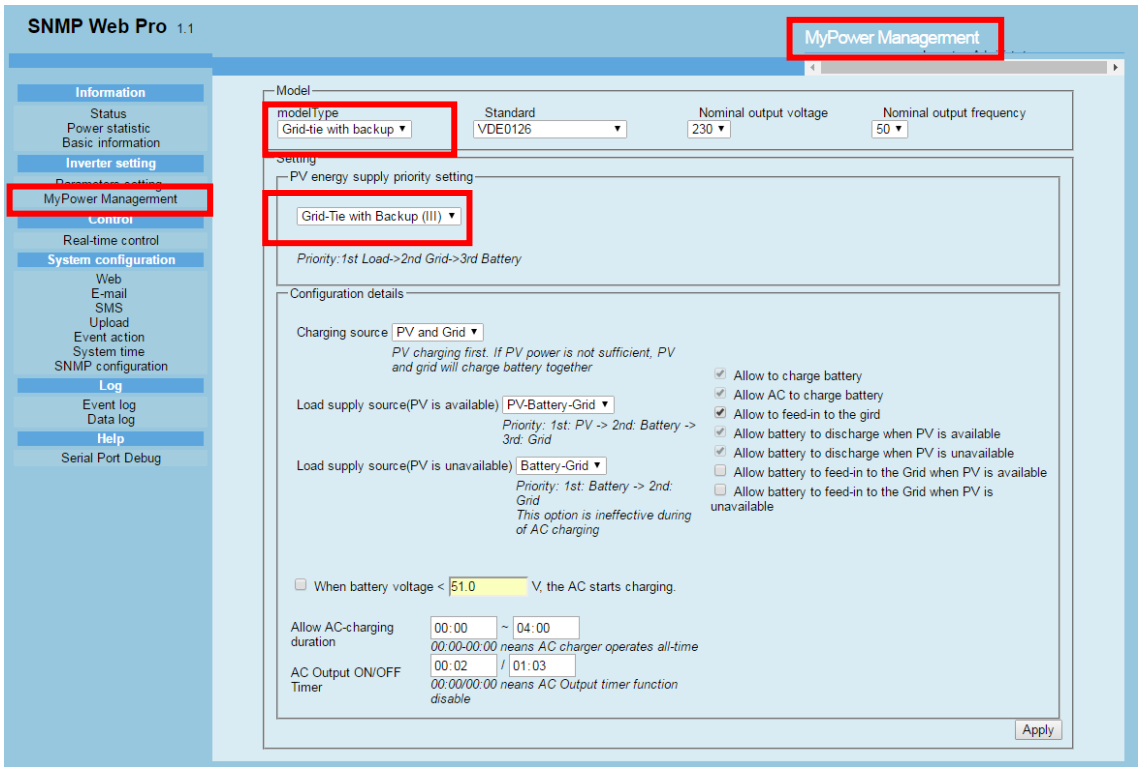
- **Charging source**:
  Defines sources priority to charge batteries. Options:
  1. PV and Grid: Solar Power will charge batteries and if it is not enough, Grid will co-charge them.
  2. PV only: Only Solar Power will charge batteries.
  3. None: Battery charge is not allowed for any of inverter inputs.

- **Load supply source (PV is available)**
  1. **1st PV** (Solar Power), **2nd Battery**, **3rd Grid** (AC Line)
     With Solar power available, it is the first to feed load, if it is not enough batteries will power the load. When batteries are discharged, AC input will power the load.
  2. **1st PV** (Solar Power), **2nd Grid** (AC Line), **3rd Battery**
     With Solar Power available, it is the first to feed load. If it is not enough AC input will co-power the load. If AC Line is not available, batteries will power the load consumption not covered by Solar Power.

- **Load supply source (PV is unavailable)**
  Priority to power the load when solar power is not available. Options:
  1. **1st Grid** (AC Line), **2nd Battery** (Factory Default)
     AC Line will power the load, if it is not available, the batteries will power the load.
  2. **1st Battery**, **2nd Grid** (AC Line),
     Batteries will power the load, if they are discharged, AC Line will power the load.

  Note: This option is ineffective during the AC Charging period and priority will automatically go to 1st Grid, 2nd Battery. Otherwise, batteries would be damaged.

GRID-TIE WITH BACKUP – Option: Grid-Tie with Backup III

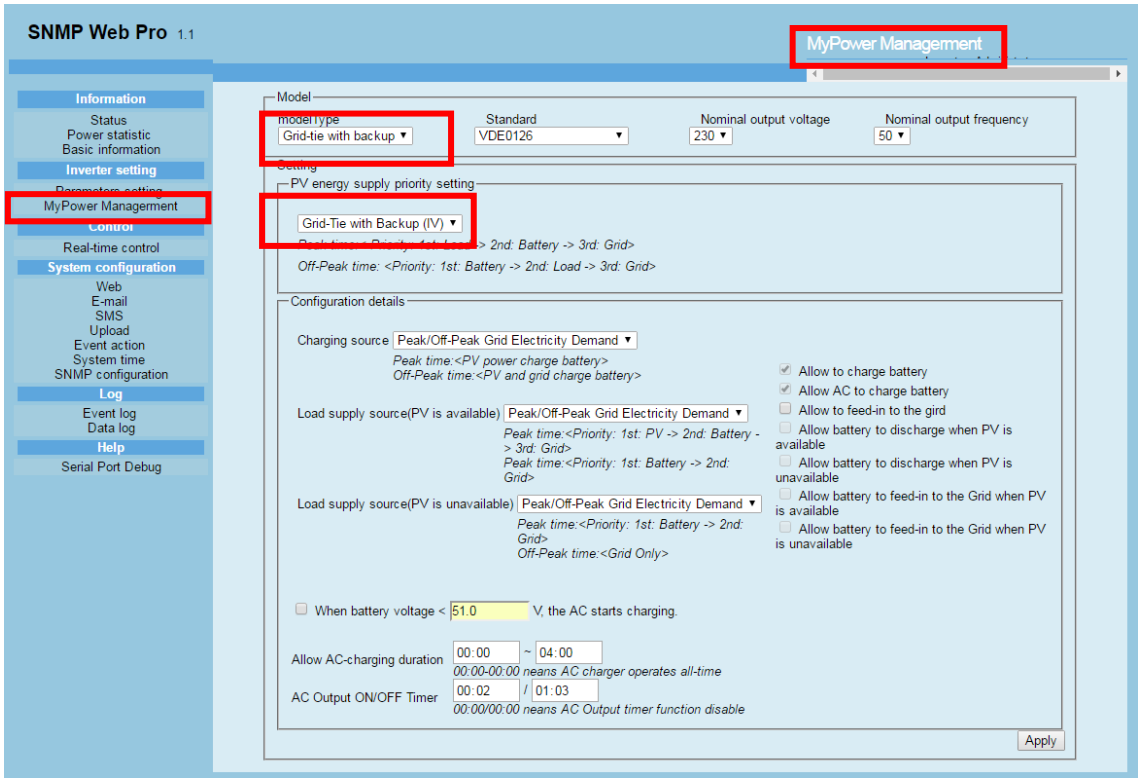


Parameters Setting:

- **PV Power supply priority setting: 1st Load**, **2nd Grid**, **3rd Battery.**
  Solar energy will power the load first, then if there is still available it will feed the Grid. When feed-in power reaches **Max. feed-in power** setting, remaining power will charge batteries. **Max. feed-in power** limit is available in software Parameter Setting. Refer to the manual for more details.
- **Charging source**:
  Defines sources priority to charge batteries. Options:
  1. PV and Grid: Solar Power will charge batteries and if it is not enough, Grid will co-charge them.
  2. PV only: Only Solar Power will charge batteries.
  3. None: Battery charge is not allowed for any of inverter inputs.
- **Load supply source (PV is available)**
  1. **1st PV** (Solar Power), **2nd Battery**, **3rd Grid** (AC Line)
     If Solar power available, it is the first to feed load, if it is not enough batteries will power the load. When batteries are discharged, AC input will power the load.
  2. **1st PV** (Solar Power), **2nd Grid** (AC Line), **3rd Battery**
     With Solar Power available, it is the first to feed load. If it is not enough AC input will co-power the load. If AC Line is not available, batteries will power the load consumption not covered by Solar Power.
- **Load supply source (PV is unavailable)**
  Priority to power the load when solar power is not available. Options:
  1. **1st Grid** (AC Line), **2nd Battery** (Factory Default)
     AC Line will power the load, if it is not available, the batteries will power the load.
  2. **1st Battery**, **2nd Grid** (AC Line),
     Batteries will power the load, if they are discharged, AC Line will power the load.

  Note: This option is ineffective during the AC Charging period and priority will automatically go to 1st Grid, 2nd Battery. Otherwise, batteries would be damaged.

GRID-TIE WITH BACKUP – Option: Grid-Tie with Backup IV



In this mode, user can only set Peak Hours (Peak Time) and Valley Hours (Off-Peak Time) periods, marking the inverter behavior.

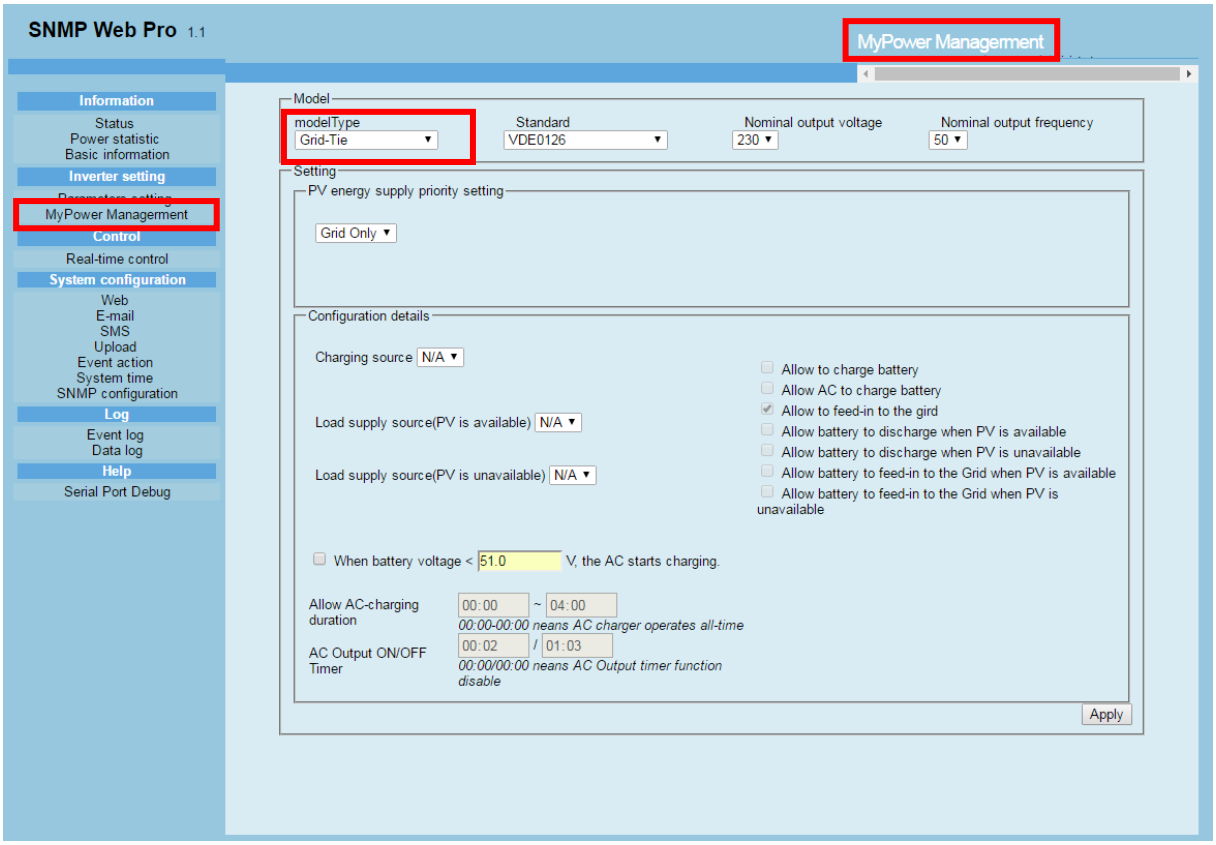
Operational Logic during Peak Hours:

- **PV energy supply priority setting**: 1st Load, 2nd Batteries and 3rd Main AC Line
  Solar power will first power the load, then remaining power will charge batteries. If there is still power remaining it feeds the grid. Grid feeding is originally disabled (Default).
- **Charging source**: Source priority to charge batteries. Option:
  PV only: Solar Power feeds the load, remaining power can charge batteries during peak hours.
- **Load supply source (PV is available):** Priority to power the load.
  1st PV (Solar Power), **2nd Battery**, **3rd Grid** (AC Line)
  Solar Power feeds the load, if it is not enough, batteries will supply missing power, when they are discharged, AC line will power the load.
- **Load supply source (PV is unavailable):** Priority to power the load when solar energy is not available.
  1º Battery, **2º Grid** (AC Line)
  Batteries power the load, in case of being discharged, AC Line will power the load.

Operational Logic during Off-peak Hours:

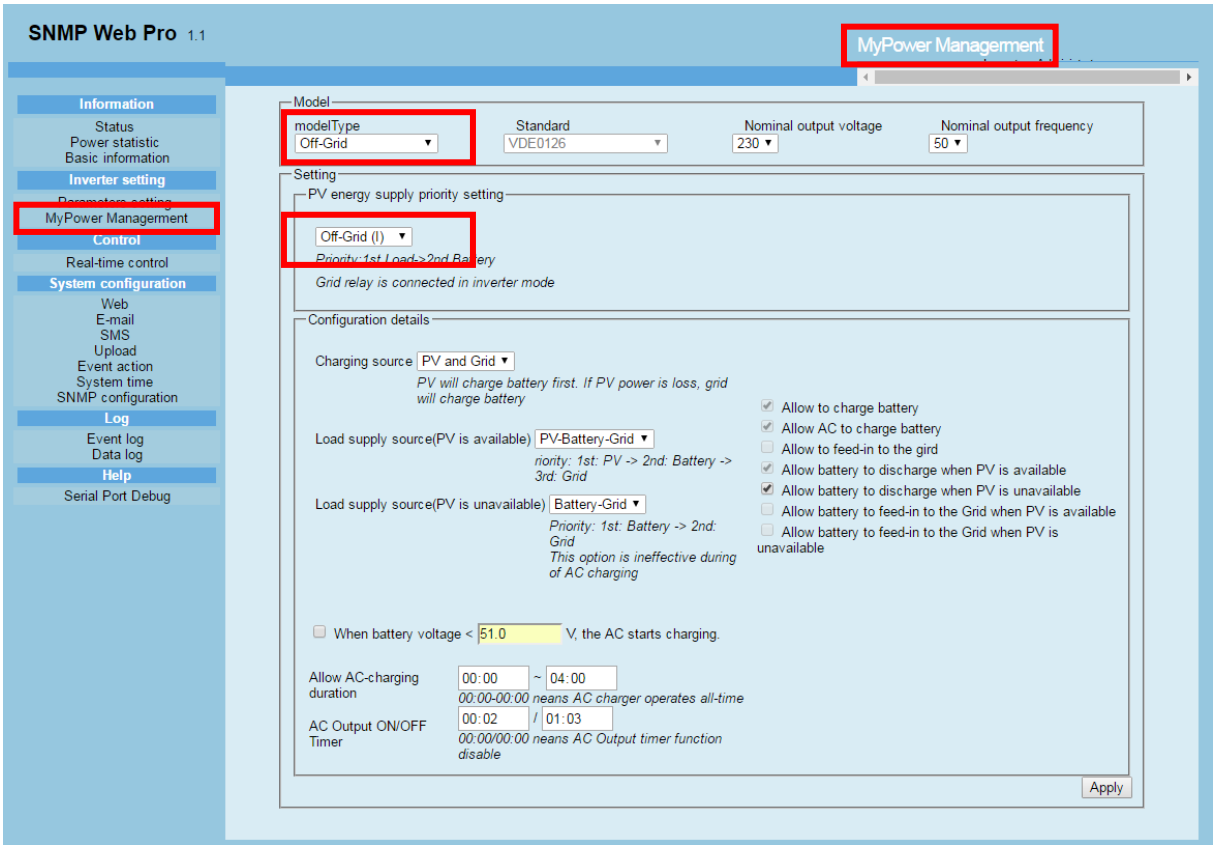
- **PV energy supply priority setting: 1st Batteries**, **2nd Load**, **3rd Main AC Line**
  Solar power will charge batteries first, remaining power will feed the load. Still remaining power will feed the Grid. **Max. feed-in power** limit is available in software Parameter Setting. Refer to the manual for more details.
- **Charging source**: Sources priority to charge the batteries. Option.
  PV and Grid (Solar Power and Main AC Line)
  Solar Power charges the batteries first, if it is not enough, Main AC Line will also charge batteries.
- **Load supply source (PV is available**): Defines priority when powering the inverter load. Operation:
  1st PV (Solar Energy), **2nd Grid** (AC Line), **3rd Battery.**
  When batteries are fully charged, Solar Energy power the load, if not enough, Grid powers the load. If the AC line is not available, batteries will supply the load.

GRID-TIE.



Inverter only sends Solar Power to the Main AC Line (Grid). There is no priority setting.

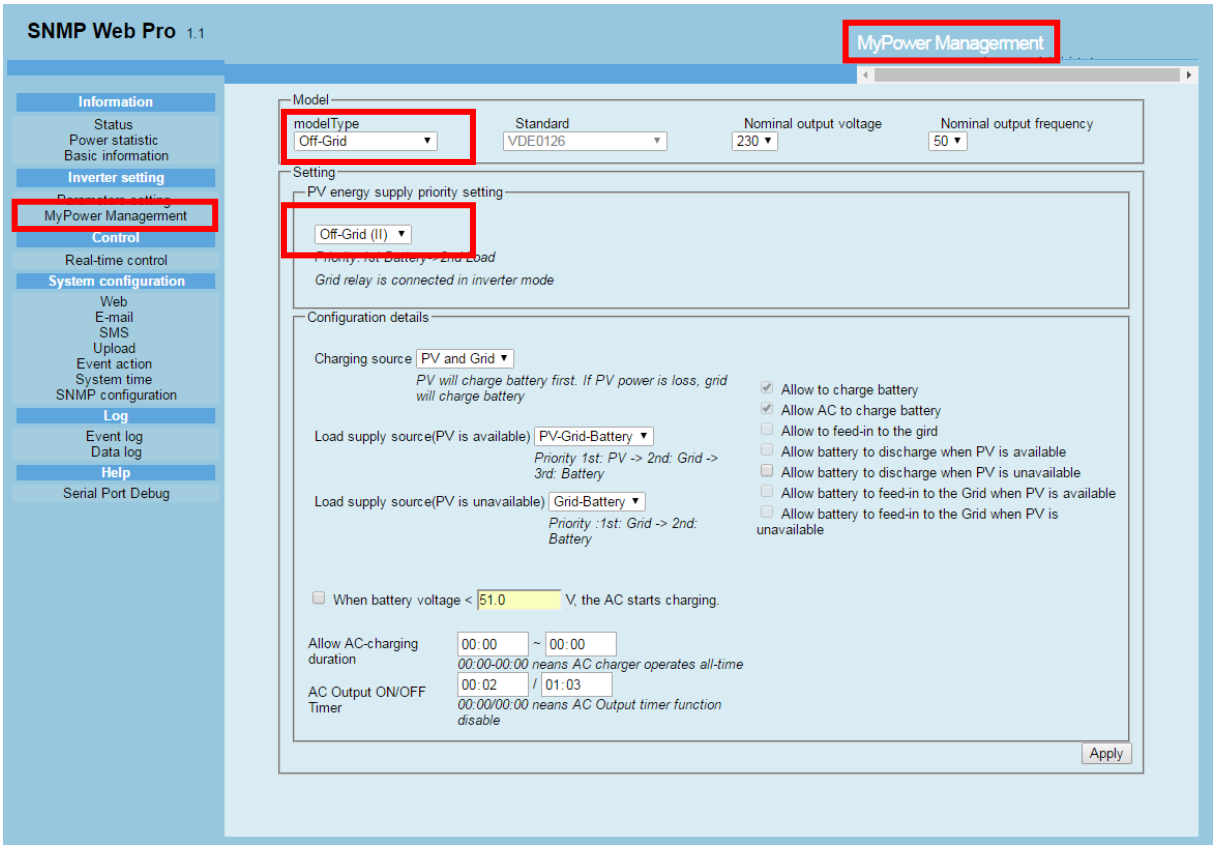
OFF GRID – Option: Off-Grid I.



- **PV energy supply priority setting**: **1º Load, 2º Battery**
  Solar power will power load first, remaining power will charge batteries. Grid feeding is not possible in this mode. Line Relay is positioned in Inverter mode, which means transfer from Inverter Mode to Battery Mode will take less than 15 mSec. This mode reduces overload faults since Grid can power load if it exceeds inverter capacity.
- **Charging source:** Defines sources priority to charge batteries. Options:
  1. **PV or Grid**: After powering the load, remaining Solar Power will charge batteries. Only when Solar Power is not available, Grid will charge batteries. Default setting.
  2. **PV only**: Only Solar Power is allowed to charge batteries.
  3. **None**: Battery charging is not allowed from any power source.
- **Load supply source (PV is available)**. Options:
  1. **1º PV, 2º Battery, 3º Grid**:
     Solar Power is first to feed the load, if it is not enough batteries would collaborate feeding the load. If batteries get discharged or become unavailable, Grid will feed the load simultaneously.
  2. **1º PV, 2º Grid**, **3º Battery**:
     Solar Power is first to feed the load. If it is not enough, Grid will also feed he load, in case Grid is not available, batteries will co-power the load.
- **Load supply source (PV is unavailable).** Options:
  1. **1º *Grid***, **2º Battery**: Grid Will power the load, if it is not available, batteries will power the load.
  2. **1º Battery**, **2º Grid**: Batteries power the load, if they get discharged, Grid will power the load.

  Note: This option is ineffective during the AC Charging period and priority will automatically go to 1st Grid, 2nd Battery. Otherwise, batteries would be damaged.

OFF GRID – Option: Off-Grid II.

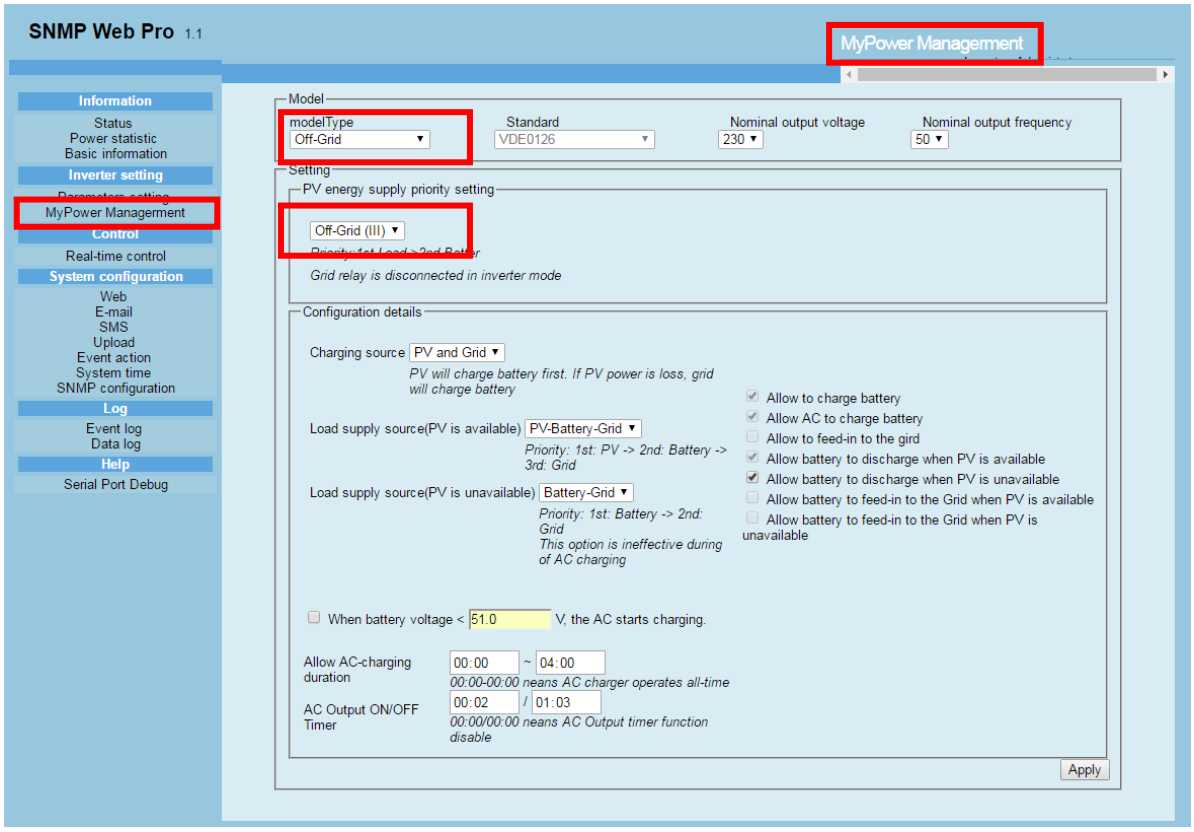


- **PV energy supply priority setting**: **1º Battery, 2º Load**
  Solar power will charge batteries first, remaining power will power load. Grid feeding is not allowed in this mode. Line Relay is positioned in Inverter mode, which means transfer from Inverter Mode to Battery Mode will take less than 15 mSec. This mode reduces overload faults since Grid can power load if it exceeds inverter capacity.
- **Charging source:** Defines sources priority to charge batteries. Options:
  1. **PV or Grid**: After powering the load, remaining Solar Power will charge batteries. Only when Solar Power is not available, Grid will charge batteries. Default setting.
  2. **PV only**: Only Solar Power is allowed to charge batteries.
  3. **None**: Battery charging is not allowed from any power source.

  Note: It is possible to configure **AC Charging Duration** parameter, that is, the Start and End Time of the period during which Grid is allowed to recharge the batteries.
- **Load supply source (PV is available)**. Options:
  1º PV, 2º Grid, **3º Battery**:
  Solar Power is first to feed the load. If it is not enough, Grid will also feed he load, in case Grid is not available, batteries will co-power the load.
- **Load supply source (PV is unavailable).** Options:
  1. **1º Grid**, **2º Battery**: Grid Will power the load, if it is not available, batteries will power the load.
  2. **1º Battery**, **2º Grid**: Batteries power the load, if they get discharged, Grid will power the load.

  Note: This option is ineffective during the AC Charging period and priority will automatically go to 1st Grid, 2nd Battery. Otherwise, batteries would be damaged.

OFF GRID – Option: Off-Grid III.



- **PV energy supply priority setting**: **1º Load, 2º Battery**
  Solar Power will power the load first, remaining power will charge batteries. Grid feeding is not allowed in this mode. Line Relay IS NOT POSITIONED in Inverter mode, transfer from Inverter Mode to Battery Mode will take approximately 15 mSec.
  In case of overload, Grid is allowed to power the load and Solar Input will be able to charge the batteries. If Grid is not available, inverter will go to Fault Mode due to overload.
- **Charging source:** Defines sources priority to charge batteries. Options:
  1. **PV or Grid**: After powering the load, remaining Solar Power will charge batteries. Only when Solar Power is not available, Grid will charge batteries. Default setting.
  2. **PV only**: Only Solar Power is allowed to charge batteries.
  3. **None**: Battery charging is not allowed from any power source.
     Note: It is possible to configure **AC Charging Duration** parameter, that is, the Start and End Time of the period during which Grid is allowed to recharge the batteries.
- **Load supply source (PV is available)**. Options:
  1º PV, 2º Battery, 3º Grid:
  Solar Power is first to feed the load, if it is not enough batteries would collaborate feeding the load. If batteries get discharged or become unavailable, Grid will feed the load simultaneously.
- **Load supply source (PV is unavailable).** Options:
  1. **1º Grid**, **2º Battery**: Grid Will power the load, if it is not available, batteries will power the load.
  2. **1º Battery**, **2º Grid**: Batteries power the load, if they get discharged, Grid will power the load.

  Note: This option is ineffective during the AC Charging period and priority will automatically go to 1st Grid, 2nd Battery. Otherwise, batteries would be damaged.

Other Configurable Parameters:

When battery voltage <:

Checking this box, AC charger will start charging batteries, when their voltage reaches the value entered in the available field. If check box is not selected, the field will not be available, entering any value will not be possible.

Allow AC charging duration:

Start and End times of the period during which the Main AC Line (grid) can charge batteries. Setting 0:00 – 00:00 (Default) means the function is not used.

AC output ON/Off Timer:

Time to Power-On and Power-Off the inverter's AC output.

Setting 0:00 – 00:00 (Default) means the function is not being used.

Allow to charge battery:

This option is automatically set when selecting "**Load Source**", no modifications are allowed here. Selecting "None" makes this option gray and unchecked.

Allow AC to charge battery:

This option is automatically set when selecting "**Load Source**", no modifications are allowed here. When selecting "Grid and PV" or "Grid or PV", this option is selected.

Selecting Grid-tie Mode disables this option.

Allow to feed-in to the Grid:

This option is available only in Grid-tie and Grid-tie with backup IV modes. User can decide if the inverter can feed the grid.

Allow battery to discharge when PV is available:

This option is set automatically when selecting "**Load supply source (PV is available)**".

If batteries have a higher priority than the Grid, this option is selected.

In Grid-tie Mode, this option is not available.

Allow battery to discharge when PV is unavailable:

This option is set automatically when selecting "**Load supply source (PV is unavailable)**".

If batteries have a higher priority than the Grid, this option is selected.

In Grid-tie Mode, this option is not available.

Allow battery to feed-in to the Grid when PV is available:

This option only valid in Grid-tie with backup II or Grid-tie with backup III modes.

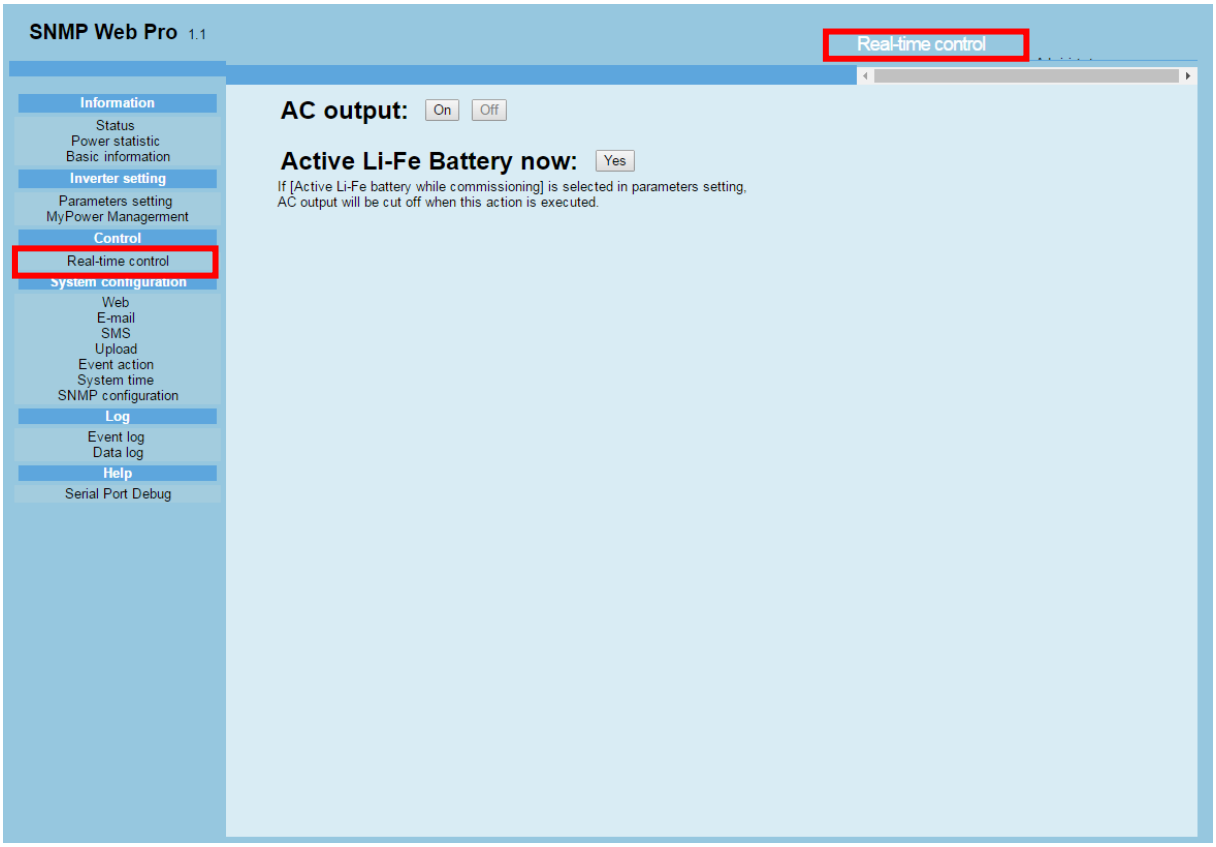
Allow battery to feed-in to the Grid when PV is unavailable:

Option is only valid in all Grid-tie with backup modes.

CONTROL

Allows real time control actions on the inverter.

Real Time Control:



AC Output:

"On" and "Off" buttons turn on and off, respectively, the inverter's AC output. Command is immediately executed when the button is clicked.

Activate Li-Fe battery Now:

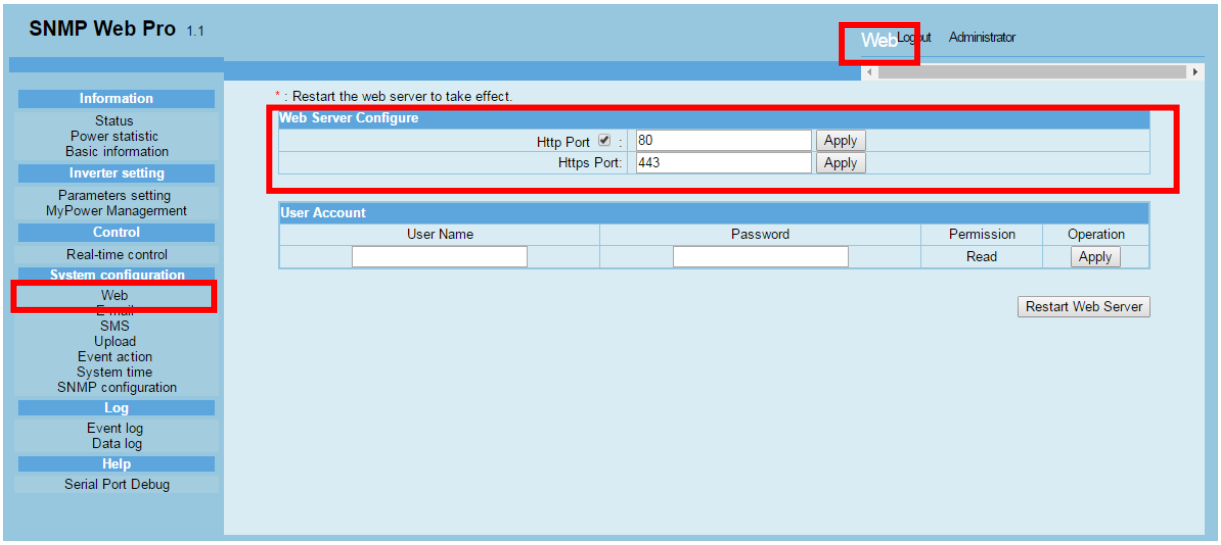
If **Activate Li-Fe battery while commissioning** parameter in the **Parameter Setting** section is enabled, clicking "Yes" button will activate the Li-Fe batteries. While this command is executed, Inverter's AC output will be off.

SYSTEM CONFIGURATION:

This section allows to configure parameters related to communication and operation of SNMP Web Pro.

WEB

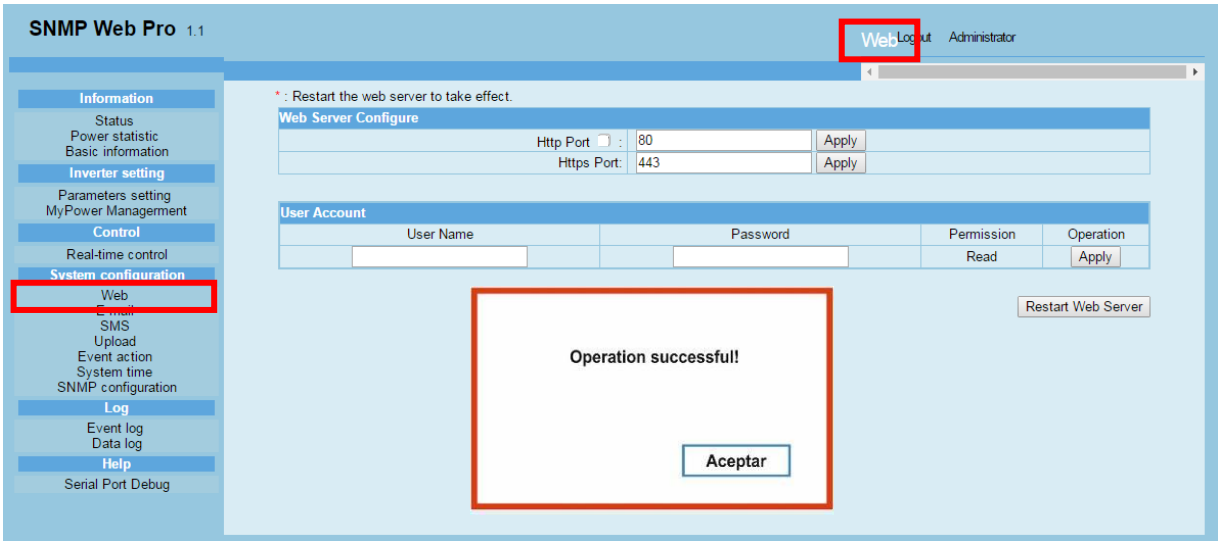
Web Server Configure



SNMP card allows communication via http as well as via secure https protocol, as previous figure shows. Factory setting is Http. To operate **ONLY** under secure https protocol, it is necessary to disable http port (80). Otherwise, the card could communicate using either of the 2 protocols.

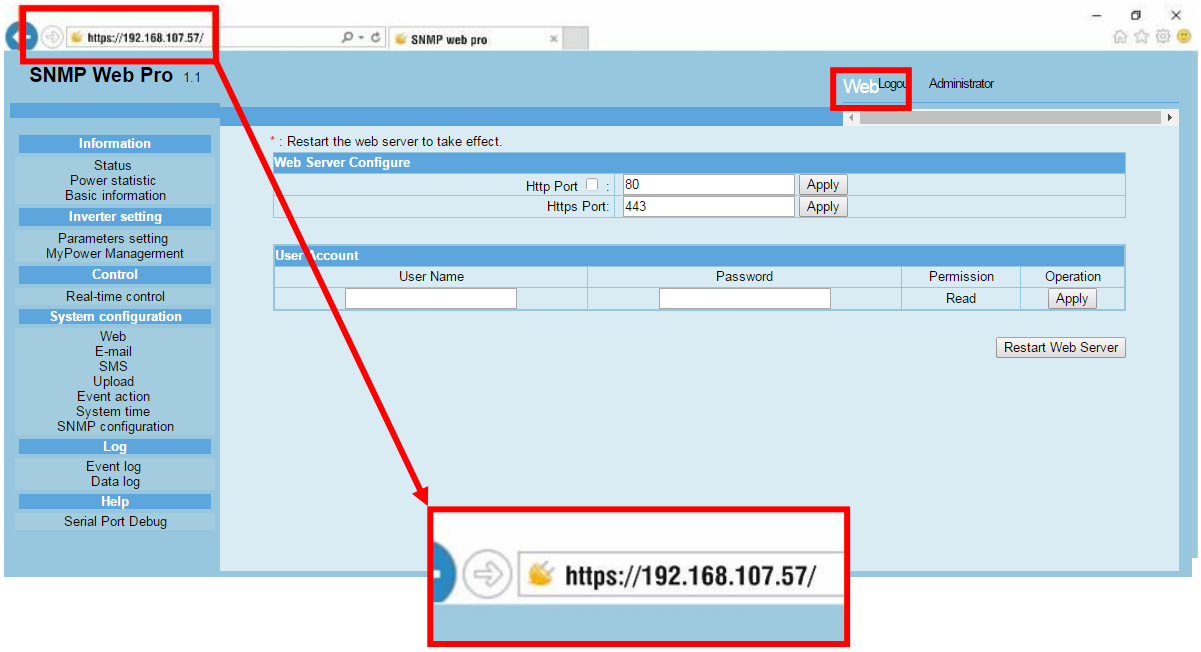
To activate Https protocol, follow this procedure:

1. Log in as Administrator (password “12345678”), otherwise you will not be able to save changes.
2. HTTP port must be disabled to force communication to be only via HTTPS protocol. Uncheck "Http Port (80)" option and check APPLY, otherwise changes will not be saved. A window should appear confirming the change with the message: OPERATION SUCCESSFUL!
3. Click ACCEPT. See next figure for reference.

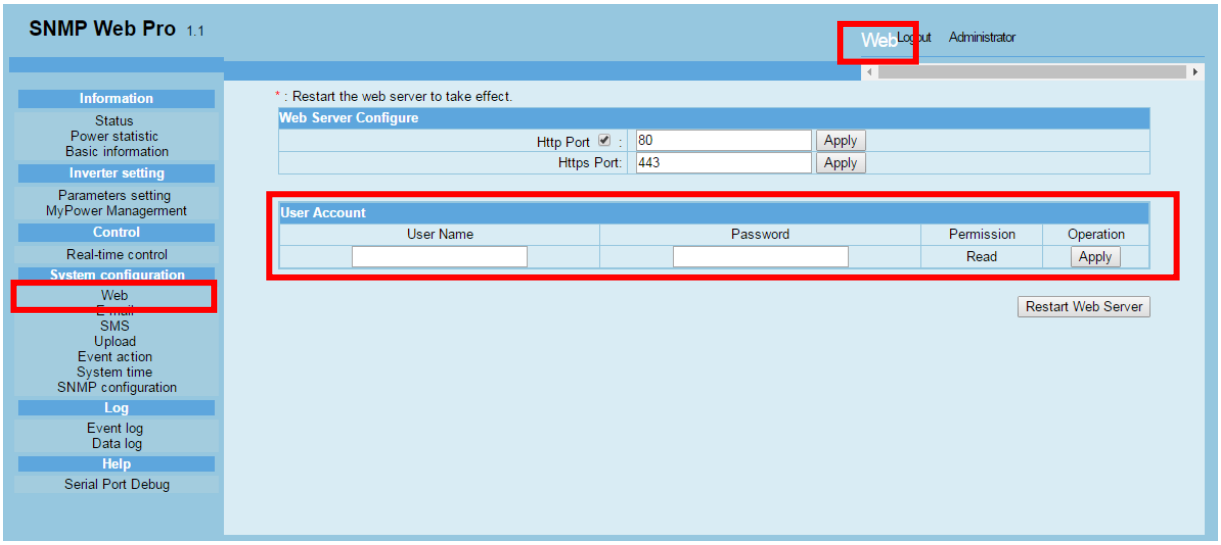


4. Click “Restart Web Server” button, to activate modifications.

5. **Wait about 30 seconds for changes to be saved**, refresh the browser with the <F5> key (for Windows®). Browser should reply with a message indicating that communicate with that IP is not possible. This is because http port (80) has been disabled and http communication is inhibited.
6. You can now verify that secure communication via HTTPS is active.
7. Write the IP of the card preceded by https:// in the browser. For example: **https://192.168.1.18**
8. Browser should open SNMP Web Pro interface using secure https protocol, as in the figure below.



User Account



In this window you can also configure access to **SNMP Web Pro**, ENTERING the name of each user and their respective access codes. After each entry, you must click "APPLY" button, to save each change. See previous figure for reference.

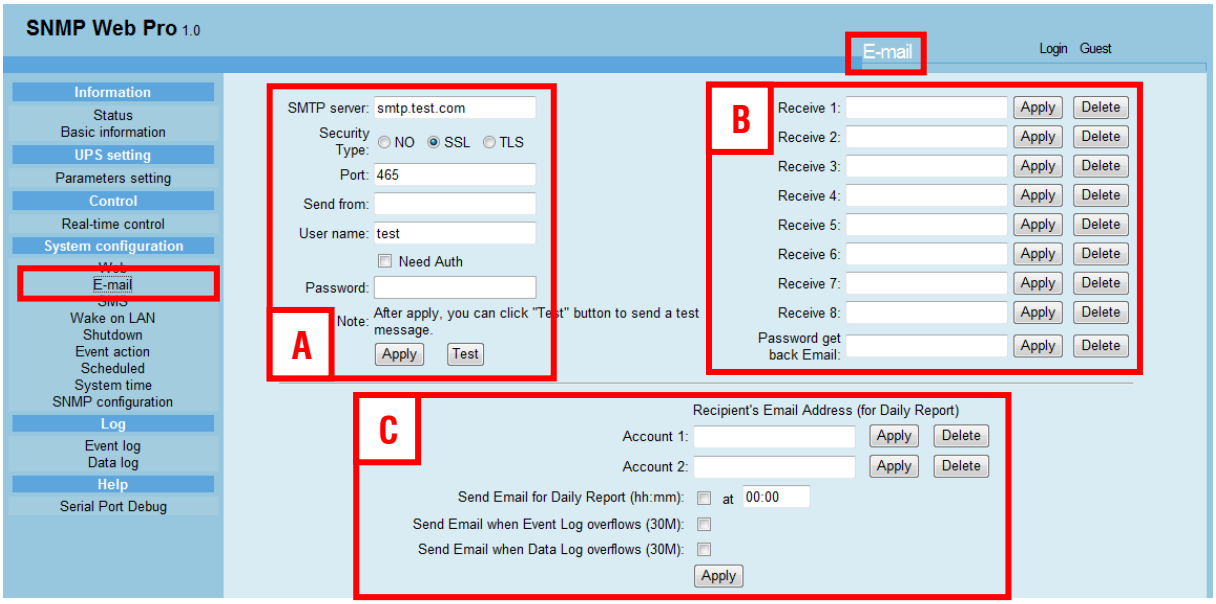
After all the information has been entered, click the "Restart Web Server" button to restart the WEB server and activate the modifications.

E-mail

SNMP card can send emails using accounts based on SNMP, SSL or TTL servers.

If your mail server has two-step verification method to access the account, go to **APPENDIX F** of this manual; otherwise, continue in this section. All values are Default empty.

Check **SYSTEM CONFIGURATION** / **E-mail** to configure parameters like email server name, email account name & password (Area tagged as **A**), up to 8 receivers (Area tagged as **B**), etc. See next figure for reference:



CONFIGURING EMAIL SENDER (A):

SMTP server:	email server to be used to send emails. For instance: **smtp.gmail.com** for Gmail
Security Type:	Type of email server to be used: **NO:** Usually for web-domain email servers. **SSL:** For servers with SSL security like Gmail, Yahoo, etc. **TLS:** For emails servers with TLS security like Hotmail.
Port:	Depends on the server type. Usually: **NO: 25** / **SSL: 465** / **TLS: 587**
Send from:	email account to send emails from. For instance.: abc@xxxxxxxxxxx.com
Username:	Username of the email to send emails. This is the email signature.
Need Authorization:	Check this option for accounts that require Authorization (“Need Auth”)
Password:	Email account password.
APPLY	Click APPLY button to save modifications.

EMAIL RECEIVERS (B):

On the right side of the screen (Area tagged as **B**) there are 8 fields to configure destination email addresses. Select APPLY for each receiver added.

DAILY REPORT (C):

Every day, SNMP can send an email reporting Daily Reports (Area tagged as **C**), here you can configure it:

Account 1: Account 2:	Email addresses to receive Daily report. Select “APPLY” on the right for each receiver added
Send email for daily report:	Mark checkbox to activate, also select the time.
Send email when Event Log overflows:	Mark checkbox to activate.
Send email when Data Log overflows:	Mark checkbox to activate.

IMPORTANT NOTES:

- **The email-sending firmware of the SNMP card has not been compatible with the security settings of Hotmail® and Microsoft® servers since September 2024, due to changes in their authentication system.**
- **If you have any questions, contact your Internet/email provider or your IT administrator.**
- **After configuring the email section, we recommend testing it by clicking the "TEST" button.**

System will response with a message: “TEST SUCCESSFULL” when email has been sent without errors. In case email cannot be sent, system will show a failure message.

IMPORTANT: If SNMP Web Pro reports problems sending emails, it can be for one of 2 reasons:

1.- A mistake in one or more data fields. Check and correct any wrong data.

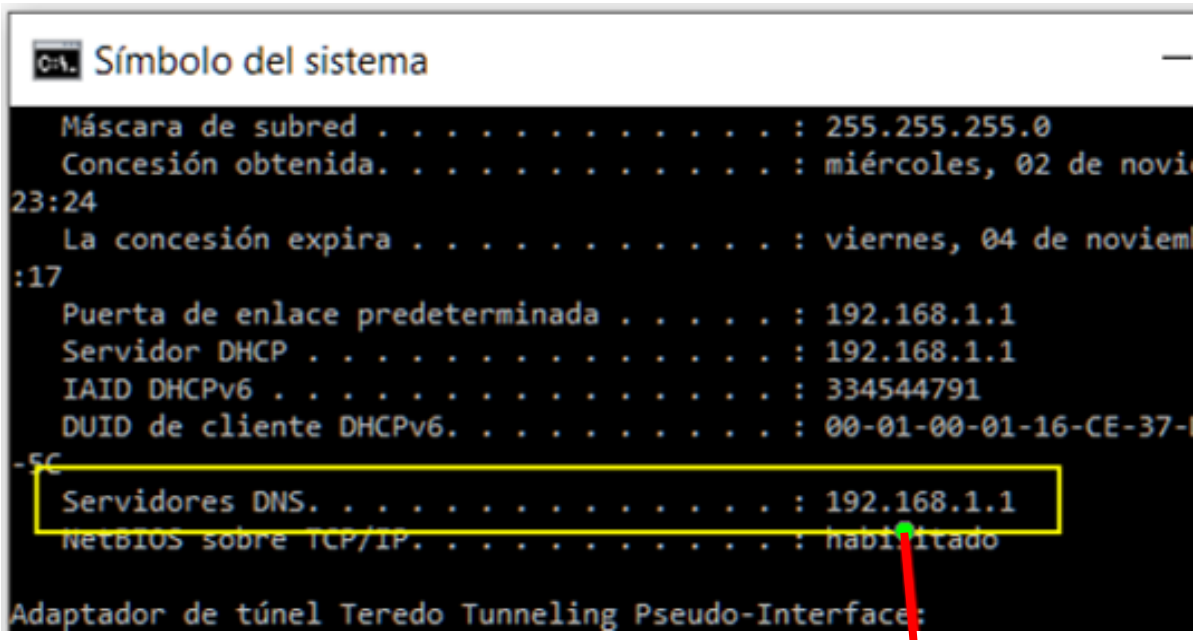
2.- DNS has not been saved automatically in the card. In this case, follow this procedure:

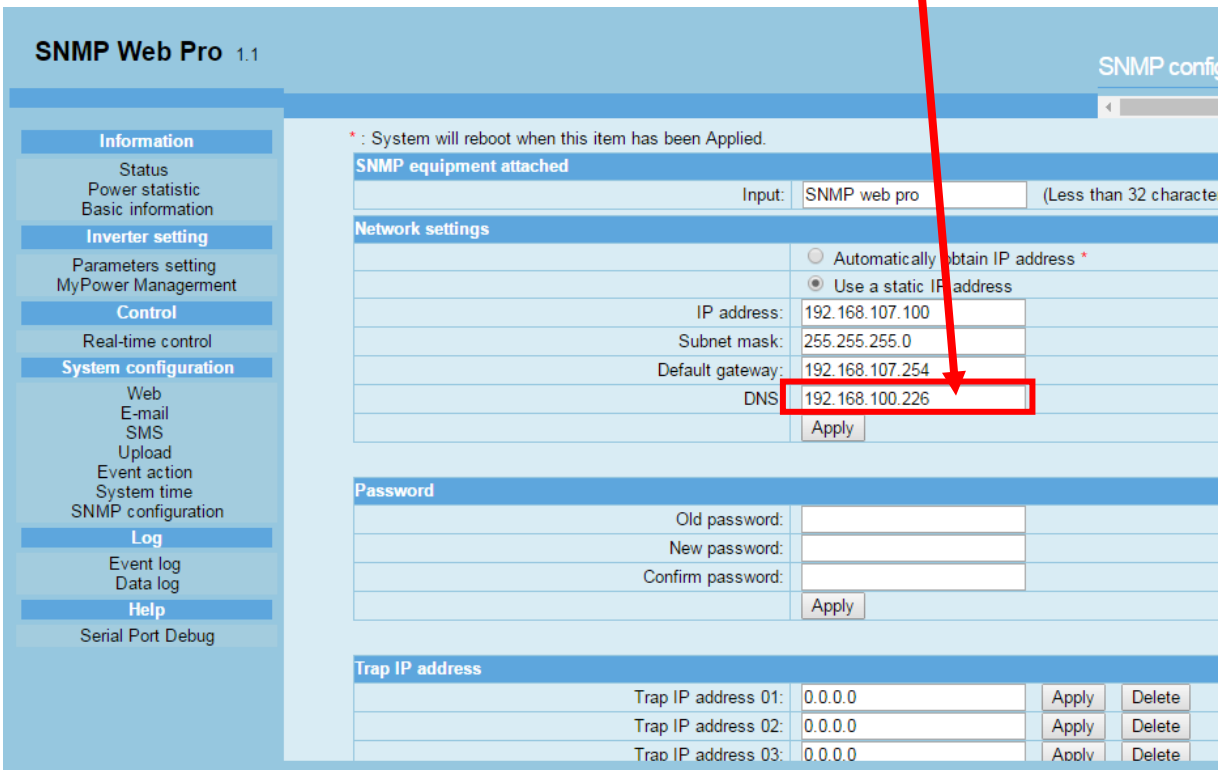
a) Check **System Configuration** / **SNMP configuration** / network settings.
b) Check if DNS field shows appropriate DNS. If it shows 0.0.0.0, user must enter manually DNS of the network and select APPLY. See the next figure for reference.

The way to find out DNS of your network depends on your operating system. For instance, in windows you can go to system command line of your PC and execute this command:

ipconfig -all

Your operating system will list several related parameters. Look for the line dedicated to DNS server. In the below example the value is: 192.168.1.1. (See the next figure)





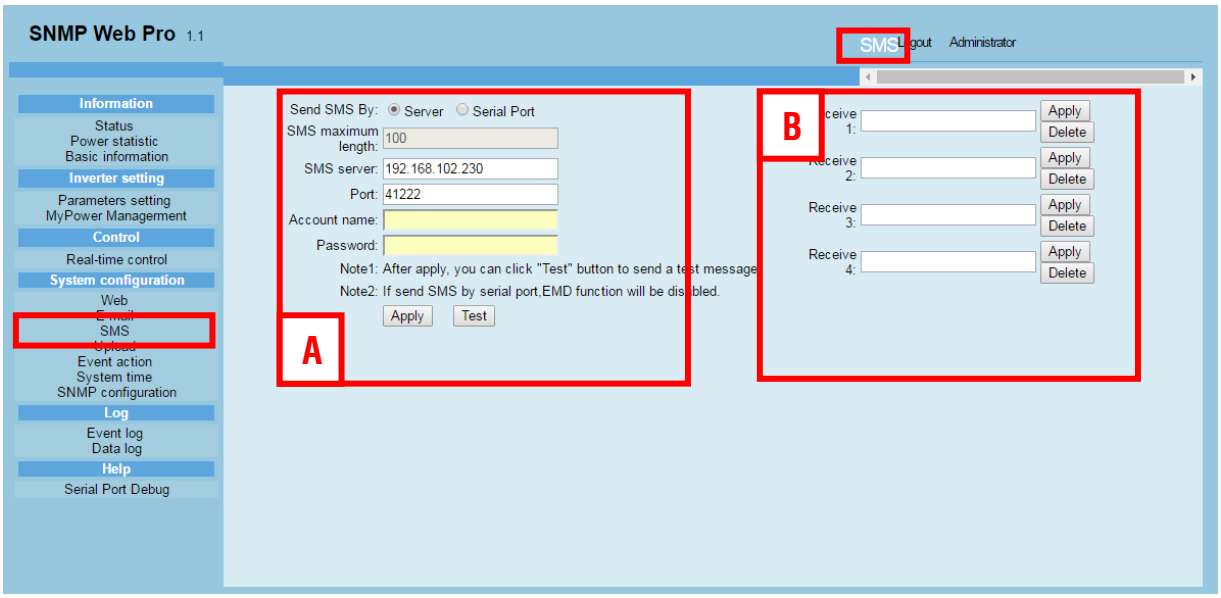
Go to **System Configuration** / **SNMP configuration** to mark option: “Use a static IP address”. Enter DNS value and select APPLY. Wait a few seconds.

Mark again option: “Automatically obtain IP address” (for DHCP networks) and select APPLY. Wait some seconds during card restarts to recover communication.

Go back to the **Configuration** / **E-mail** section and test again.

SMS

Some events can cause SNMP to generate SMS (See section **Event Action** in this appendix). Thus, this section describes configuration for SMS. For configuration purposes, it is necessary to log in as an administrator. See next figure as reference:



Send SMS By: This parameter selects one out of two ways to send SMS:

- **Server**: Mark this checkbox to use a SMS server using the configuration of Zone **A**.
- **Serial Port**: Mark this checkbox to send SMS through serial port (Secondary Port) of SNMP card.

ZONE A: CONFIGURATION TO SEND SMS VIA SMS SERVER

- **SMS SERVER:** IP address of SMS Server
- **Port**: Port of SMS Server
- **Account Name**: Username of the account at SMS Server
- **Password**: Access password of the account at SMS Server
- **Apply**: Click this button to save the information entered.
- **Test**: Click this button to test the new configuration.

ZONE B: SMS RECIPIENT PHONE NUMBER LIST

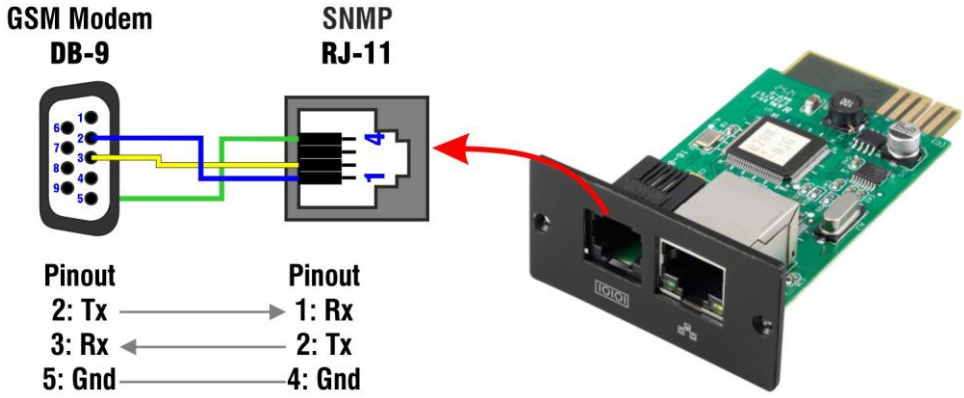
Parameters to set phone numbers to receive SMS:

- **RECEIVE** (up to 4): These fields must contain phone numbers which will receive SMS.
- **Apply**: After each phone number has been entered, click this button to save data.
- **Delete**: This button deletes selected number, emptying the field.

CONFIGURATION TO SEND SMS VIA SERIAL PORT (SNMP PORT B)

To use this option, there must be a GSM Modem connected to the secondary port of SNMP Card (B Port). This is the same port to connect Environmental Measuring Devices (EMD), therefore sending SMS via serial port is not compatible with EMD.

Pin-out for GSM Modem connection to SNMP card is shown in the next figure:



RJ11 – DB9 Cable not included

The GSM Modem configuration mus be as follows:

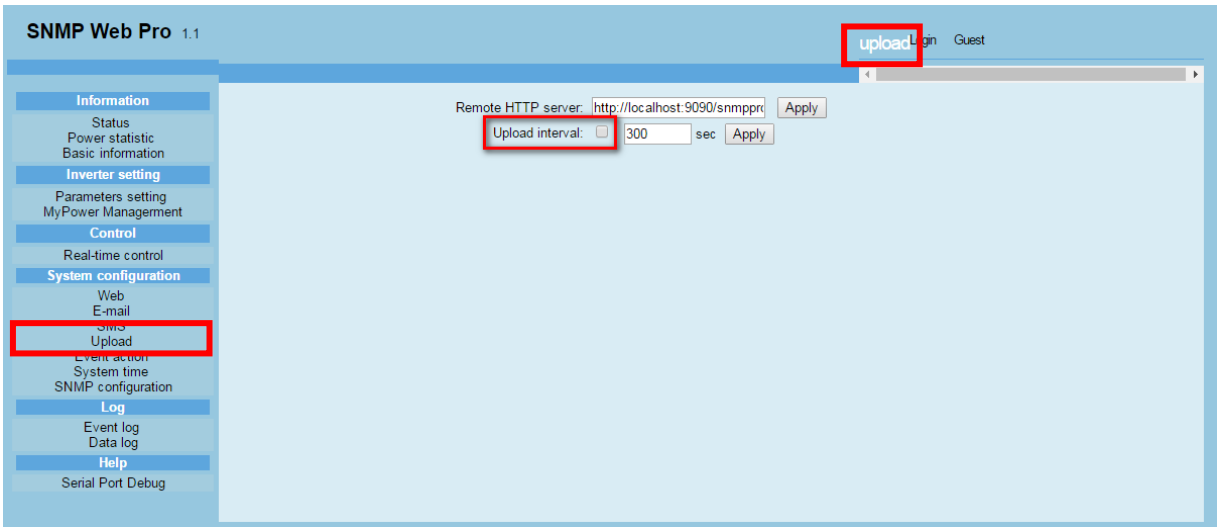
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: Hardware Flow control
- Rata de Baudio: 9600
- ECHO: Off

Additionally, in the **Event Action** configuration (See **Event Action** section, further ahead), "SMS Send when any event occurs" checkbox must be enabled, otherwise, SMS sending will not work, even using the **Test** button.

Finally, make sure the GSM Modem is properly connected to B Port of SNMP Card (RJ11 Port).

Upload

This section allows to upload data to selected end user servers, see next figure as reference:



Configurable parameters:

Remote HTTP Server:

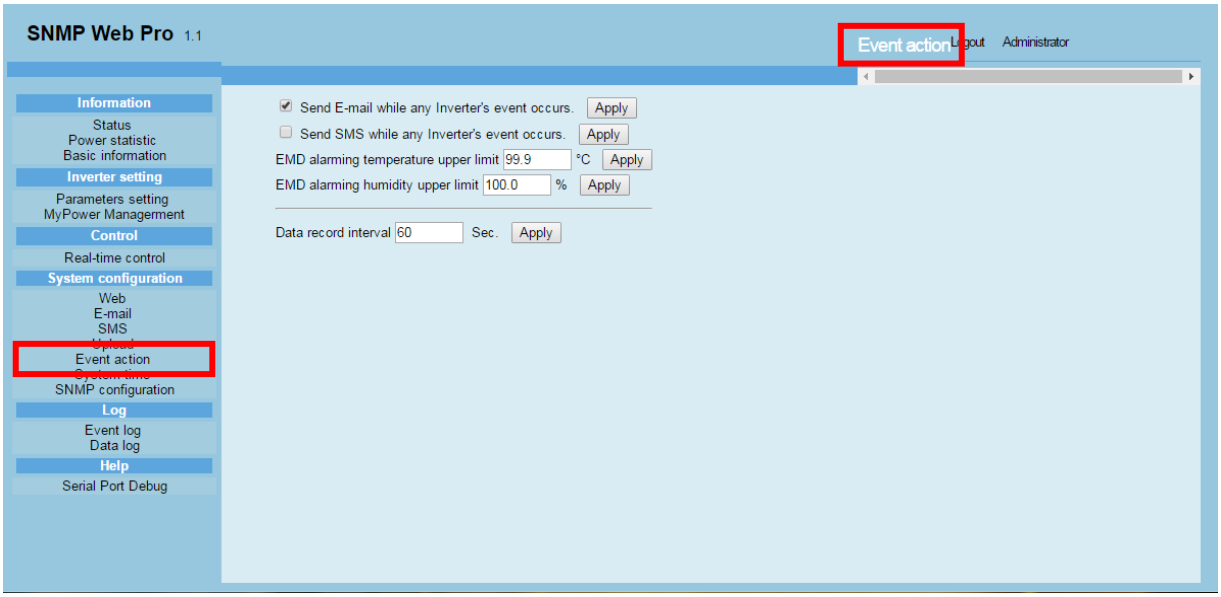
Enter HTTP server address to send Event and Data Logs. Click Apply to save changes.

Upload Interval:

Enter time between upload sessions and then click Apply to save changes. Default: 300 Sec.

Event Action

This section is to configure actions SNMP cards will perform due to events on the inverter it is installed into, as shown in next figure.



Configurable parameters:

Send E-mail while any Inverter event occurs:

Click this checkbox, to send alarm E-mail when any event occurs in the inverter.

Send SMS while any Inverter event occurs:

Click this checkbox, to send alarm SMS when any occurs in the inverter. This requires having a GSM Modem connected to SNMP Port B.

EMD alarming temperature maximum limit:

Set up alarm for high temperature point. Temperature over this limit will cause an alarm message.

EMD alarming humidity maximum limit:

Set up alarm for high humidity point. Humidity over this limit will generate an alarm message.

EMD ALARM RESET:

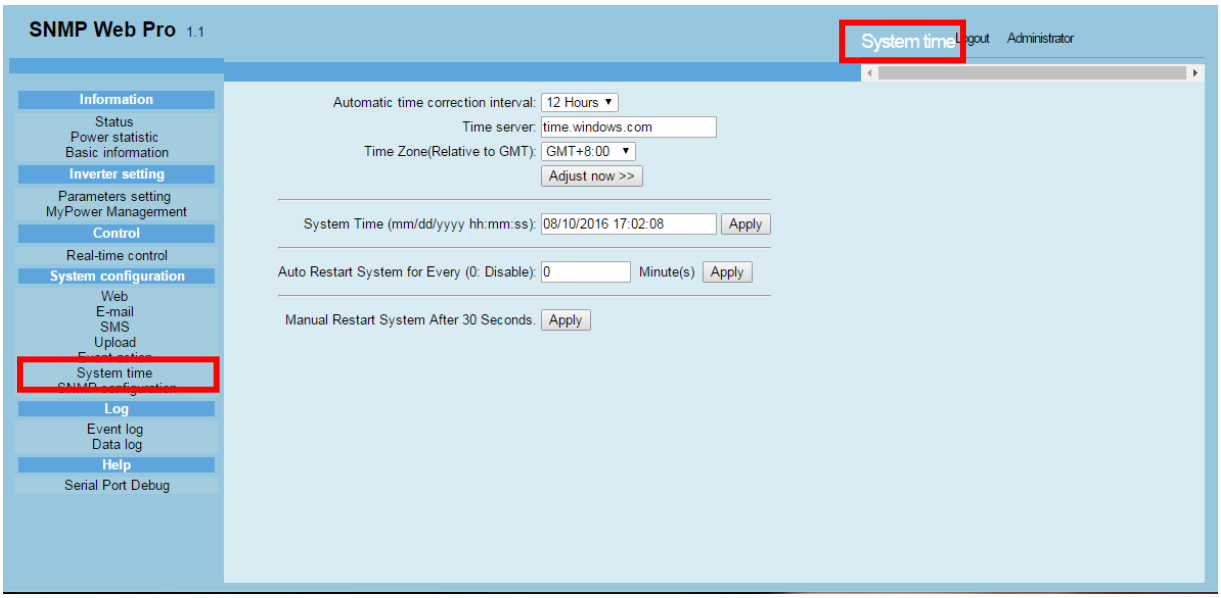
Clear all EMD alarms.

Data record interval xx sec:

Time between samples for Data log. Default: 60 sec.

System Time

Time and date configuration for SNMP Card. See next figure as reference.



Automatic time correction interval

Time server:

Reference server for time system (IP Address or Domain).

Time Zone (Relative to GMT):

Time Zone (Relative to GMT).

System Time (mm/dd/yyyy hh:mm:ss):

To set up SNMP Web local time.

Auto Restart System for Every (0: Disable):

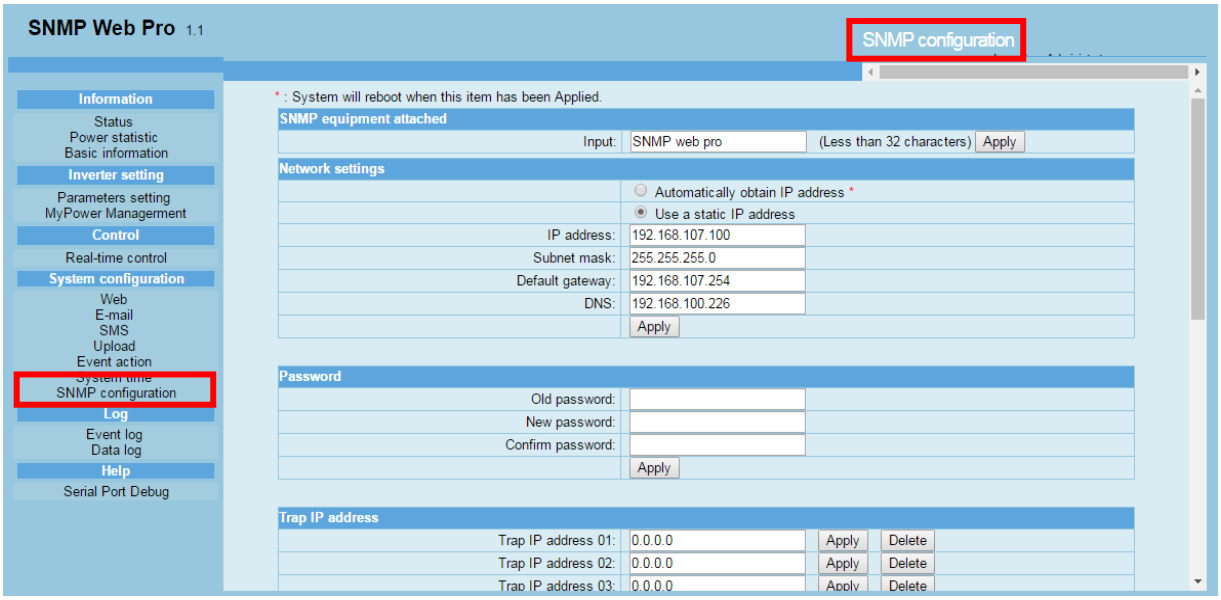
Select time (in minutes) for automatic, repetitive restarts. 0 Disables this function.

Manual Restart system after 30 Seconds:

Clicking “Apply” button, restarts SNMP after 30 seconds. It requires about 1 minute waiting, for communication reestablishing.

SNMP Configuration

This section is for setting **SNMP Web Pro** basic information. This window is quite longer than the rest so it takes scrolling down to reach the end, therefore it will be shown in 2 different images within explaining texts.



Network Settings:

IP address configuration can be done here in two different ways:

1. Automatically obtain IP address: Default option, it is for DHCP Networks.
2. Manually configure IP address: For Static IP Networks. In this case the IP Address will be shown as "**192.168.102.230**", Net mask as "**255.255.255.0**" and default gateway as "**192.168.107.254**". Values must be manually entered.

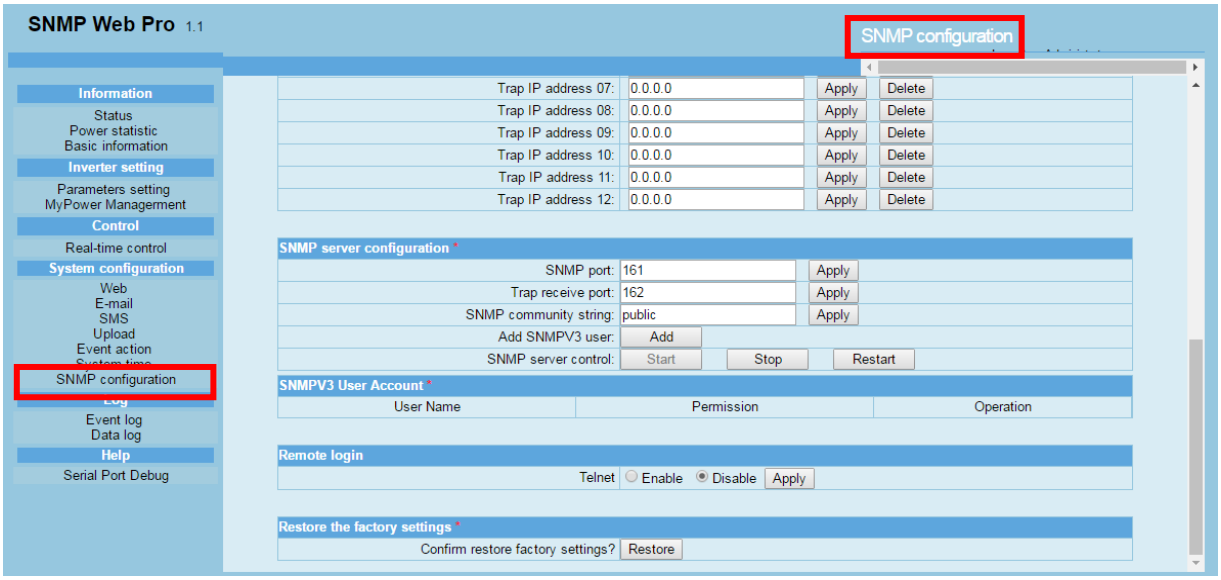
Password:

To change password, first enter old password, then new password, and new password again to confirm. Click on "Apply" button to save changes. Passwords must be 8 to 15 characters long.

Trap IP Address

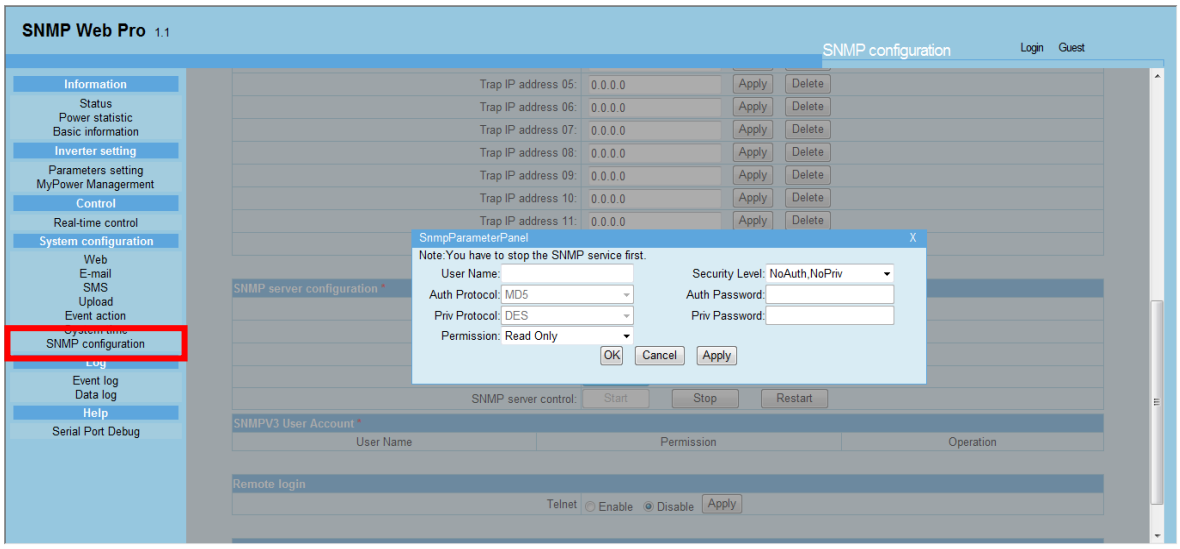
Enter up to 12 Static Traps IP addresses, provided by SNMP device. Once you enter one IP address, click on "Apply" button to save changes, otherwise the information will be lost. "Delete" button clears the fields.

Next figure shows bottom section of the windows. It includes setting explained from here.



SNMP Server Configuration

- **SNMP Port:** Click on "Apply" button to save changes.
- **Trap Receive Port**: Click on "Apply" button to save changes.
- **SNMP Community String**. Default "public". Click on "Apply" button to save changes.
- **Add SNMPV3 User**: Clicking on "Add" button a pop-up window will show-up asking for new user information. "Cancel" button closes the pop-up window and returns to previous one. When all information is entered, click on "Apply" button to save changes. See next figure for reference.



SNMP Server Control:

"Start" and "Stop" buttons start and stop SNMP server. "Restart" button restarts SNMP server.

Remote Login:

Enable or Disable (Default) remote access to Telnet services.

Restore The Factory Settings

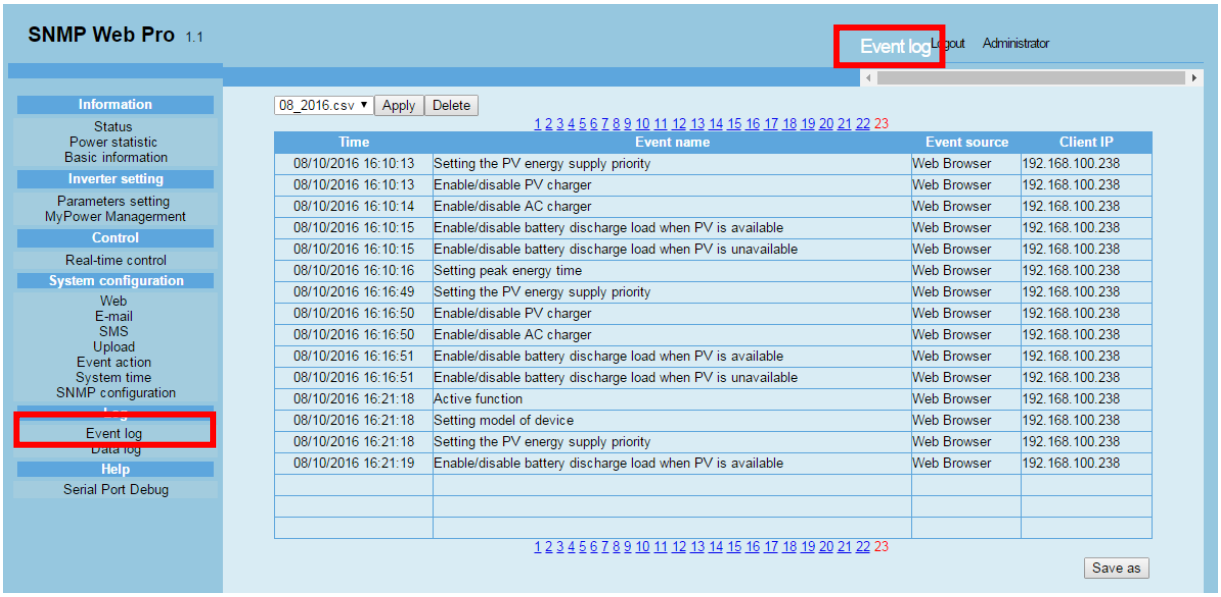
Clicking on "Restore" button will restore all factory default settings. This means system will automatically try to obtain IP Address and password will be 12345678 again.

LOG:

Events and data are stored in SNMP06 flash memory for about a month, so information is safe even during long power loss. This section allows reviewing both Logs.

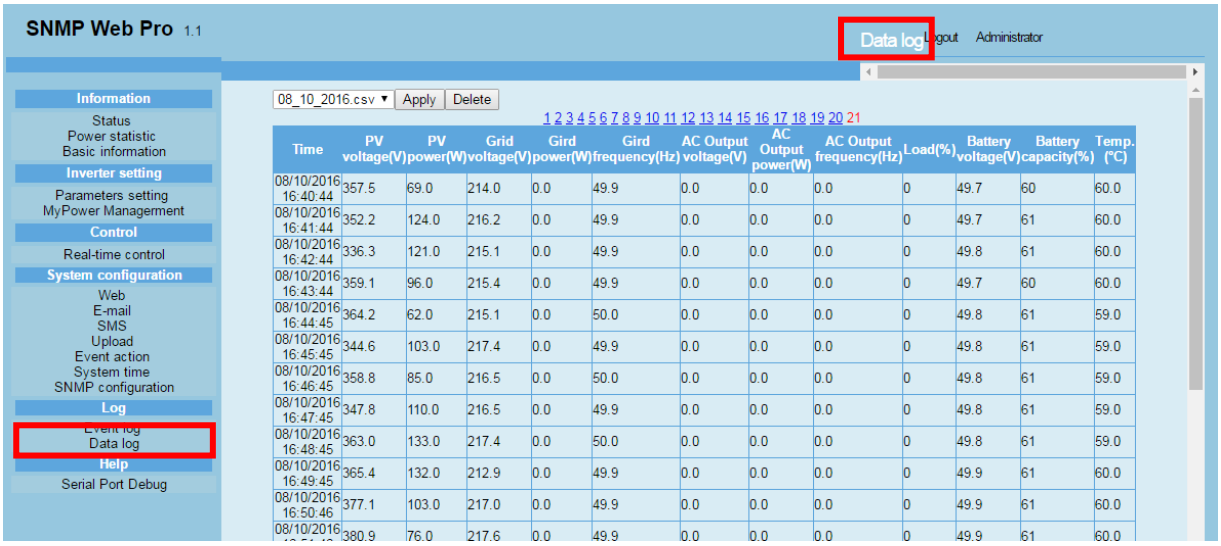
Event Log

Up to 200,000 event threads can be stored in Event Log and information can be downloaded as ".csv" Files. Event Log includes inverter Warnings, Failure Information, Sensor-TH Warnings, Operations controlled by either **SNMP Web Pro** or Monitoring/Control Software. See next figure for reference:



Data Log

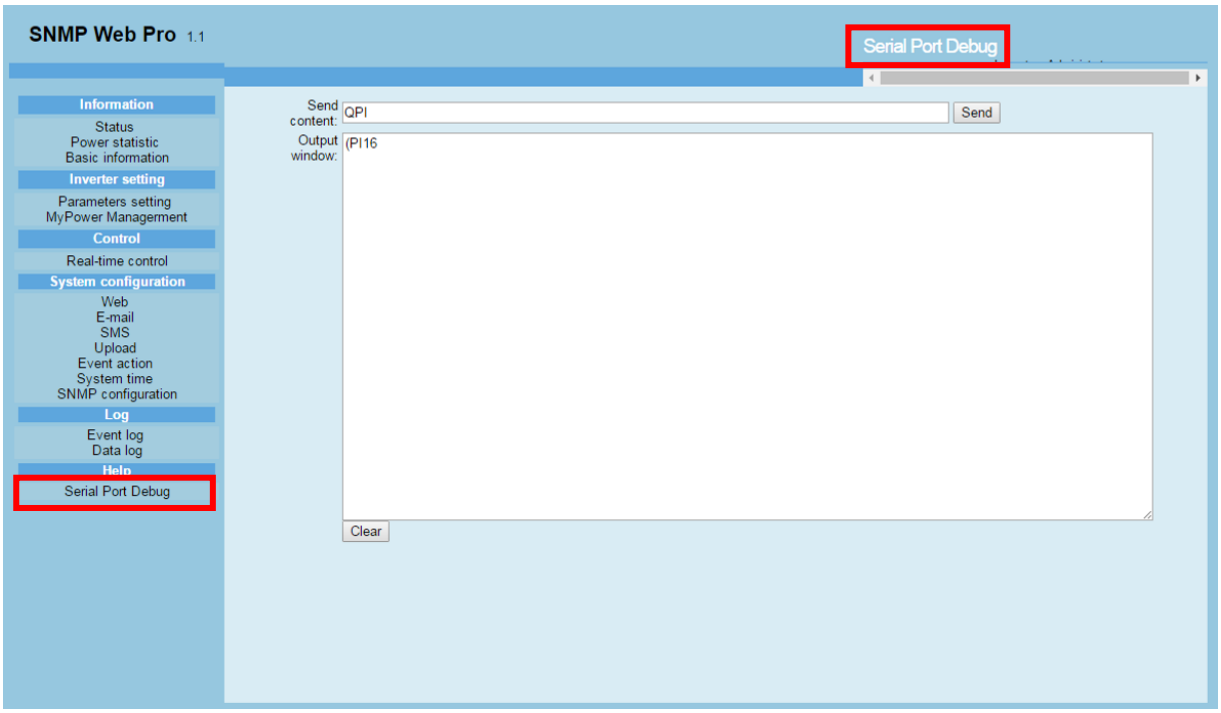
Up to 200,000 data threads can be stored in Data Log and information can be downloaded as ".csv" Files. Data Log includes values of input and output voltages, frequency, load, battery voltage, inverter internal temperature, Sensor-TH readings, etc. Log Is stored in SNMP's flash memory, daily and without risks of data loss for blackouts. See next figure for reference:



HELP:

Serial Port Debug

This function is intended to test communication condition between SNMP card and an external testing device. This function is for exclusive for authorized technical service personnel. See next figure for reference.



COMUNICATION WITH XSI INVERTERS OPERATING IN PARALLEL SYSTEMS

When monitoring over the network a group of inverters running in parallel, the look of **SNMP Web Pro** GUI changes to display serial numbers of all inverters in the parallel system. In addition, once the connection with one of the inverters has been established, any of the devices in the parallel array can be monitored in real time and parameters can be configured as well.

Following image shows an example of **SNMP Web Pro** GUI, monitoring 2 inverters operating in parallel. **Parallel Information** section and Inverter Setting section show Serial Numbers of both units working in parallel.

Parallel Information:

This section shows real-time information of the inverter whose Serial Number has been selected.

Inverter Setting:

This section is for configuring operating parameters of the inverter whose Serial Number has been selected.

APPENDIX C
PC & UPS SHUTDOWN CONFIGURATION

PC SHUTDOWN IN NETWORK:

Multiple PC (in the same network) can be shut down by remote commands generated by SNMP card. All PC to receive shutdown commands must have SHUTDOWN WIZARD auxiliary software installed except when it is not necessary, as in some specific EXsi and Linux systems which use SSH protocol for remote commands.

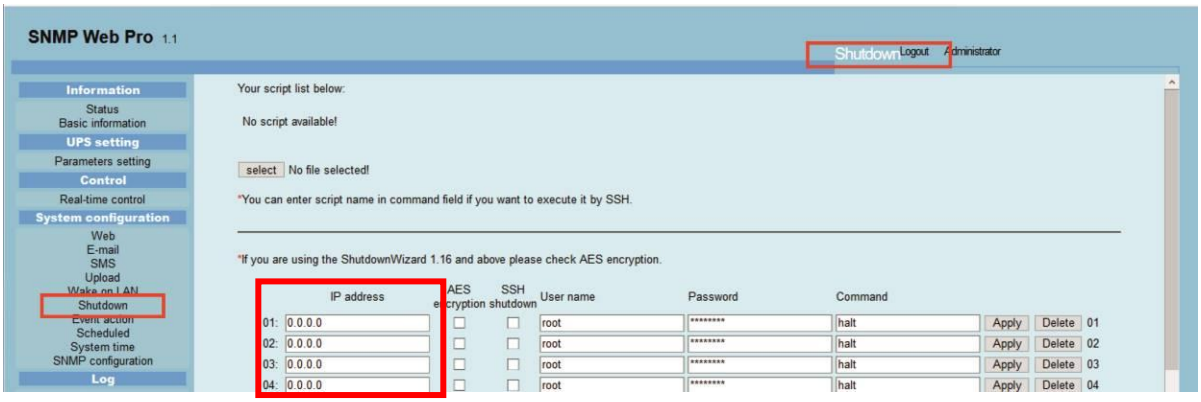
Even the PC in which **SNMP Web Pro** is configured, must have SHUTDOWN WIZARD auxiliary software installed. IF a shutdown command is sent to a PC without SHUTDOWN WIZARD, the command will be ignored.

SNMP card must be properly configured, through **SNMP Web Pro**, to send shutdown commands, referring to each single remote PC to which the command will be sent, by its IP address.

Shutdown commands are generated because of some events, such as power failure. Once the event is detected, SNMP card sends a command through the network to those PC whose IP addresses have been configured in **SYSTEM CONFIGURATION** / **SHUTDOWN** section of this manual.

Shutdown commands must be configured through 2 different sections of **SNMP Web Pro**, as follows:

SHUTDOWN: in this section can be registered the IP address of ALL PC to which shutdown commands will be sent. See section 3.4.6 **SYSTEM CONFIGURATION** / **SHUTDOWN** of this manual.
NOTE: The way to determine the IP Address of a PC will be explained later.

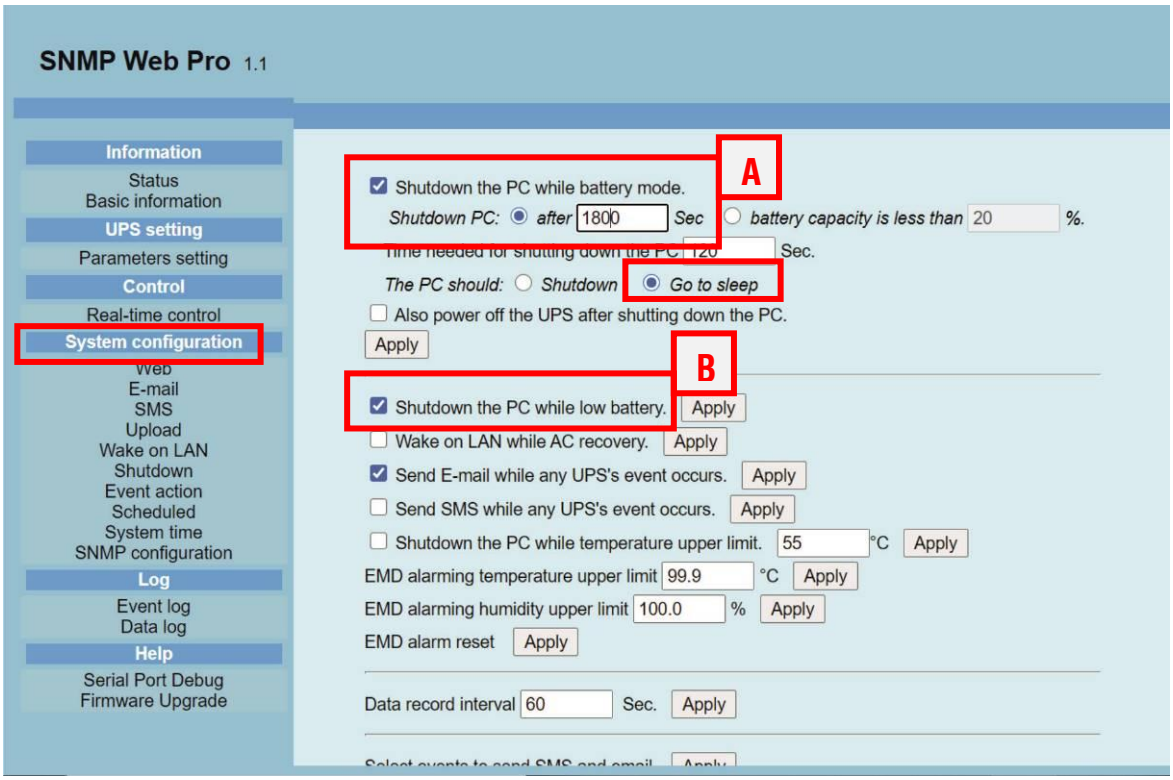


EVENT ACTION: In this section can be configured the kind of event which cause the shutdown commands. See section 3.4.7 **SYSTEM CONFIGURATION** / **EVENT ACTION** in this manual.

Here we have 2 examples:

SHUTDOWN BY TIME:

In area tagged as "A" (See next figure), there is a configuration to send a shutdown command after 1800 sec (30 minutes) for the UPS running on batteries, i.e.: AC Line Failure, putting the PC on SLEEP Mode. When the programmed time is reached, SNMP card will send a shutdown command to all PC which IP address has been configured in SHUTDOWN section.



Please note that marking on the checkbox "Also Power off the UPS after shutting down the PC", will shut down the UPS after configured PC, protecting the UPS, as well as the PC.

SHUTDOWN BY BATTERY ALARM:

In area tagged "B", same figure, a shutdown command can be a configured to be generated when UPS reach a Low Battery alarm. When this battery charge level is reached, the SNMP card will send a shutdown command to all PC which IP address has been configured in SHUTDOWN section.

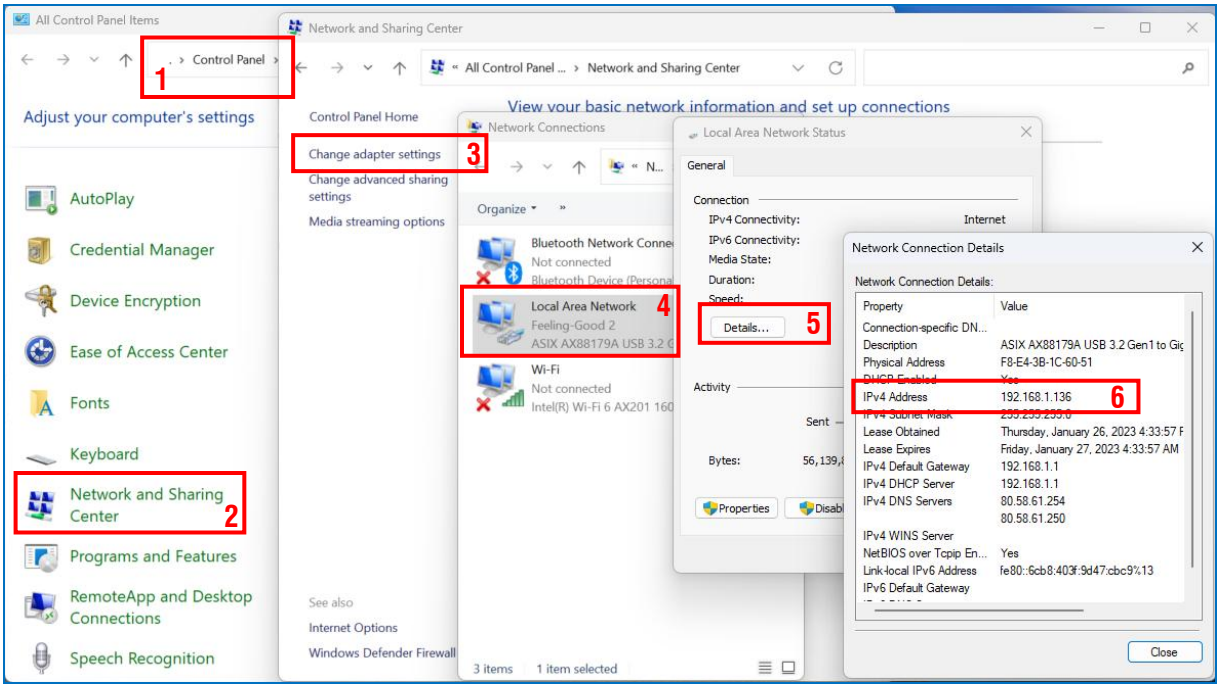
These configurations do not contradict each other, as they will execute when their respective conditions are reached.

It is important to note that the IP addresses of all PCs that should receive shutdown commands must have been configured in SHUTDOWN section.

NOTE:
HOW TO KNOW MY PC'S IP

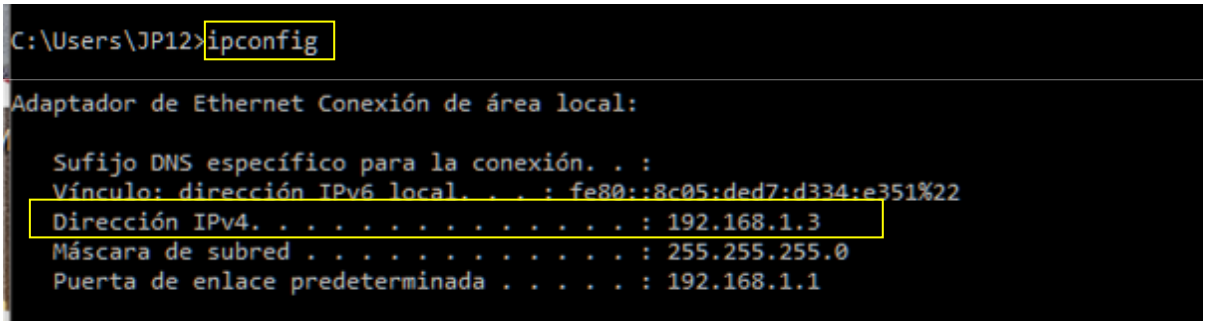
In **Windows 11**® you can quickly check the IP address of a PC as follows:

1. Open "**Control Panel**".
2. Choose "**Network and Sharing Center**".
3. Click option "**Change Adapter Settings**" for the network in use by the PC.
4. Double click on this network.
5. The connection status window will be displayed. Select "**Details**" button.
6. Network Connections Details windows will pop-up showing IP address (IPv4 Address). In the image below IP is 192.168.1.136.



IP can also be read by cmd.exe command line of the system.

Run "**cmd.exe**" and then execute command "**ipconfig**".
This command will list information for all network adapters available. Please take note of IPv4.



For more information about Shutdown Command Configuration, please refer to sections 3.4.6 and 3.4.7 in this manual.

SCOPE AND RESPONSIBILITIES:
Installing software in End User terminals and/or servers, as well as finding out IP addresses and usernames in End User networks, and any other related issue, affects the security of the system, therefore it should be responsibility of the System Administrator and we strongly recommend being done by the System Administrator, not by the technical personnel installing the UPS arrangement.

IMPORTANT INFORMACION:
If selected event disappears with enough time before shutdown command has been sent, shutdown process will be cancelled. For example, if software has been configured to shutdown UPS 5 minutes after detecting AC FAILURE event but AC main service comes back 2 minutes before sending shutdown command, software will reset event to inform UPS to eliminate shutdown action. If AC service is reestablished just few seconds before shutdown is completed, probably software will not have enough time to detect new event and inform UPS to stop shutdown process.
On the other hand, if selected event was configured to shutdown PC where software is installed and event is reestablished after PC has been shut down, there will be no way to warn UPS to stop shutdown process since PC is already powered off.

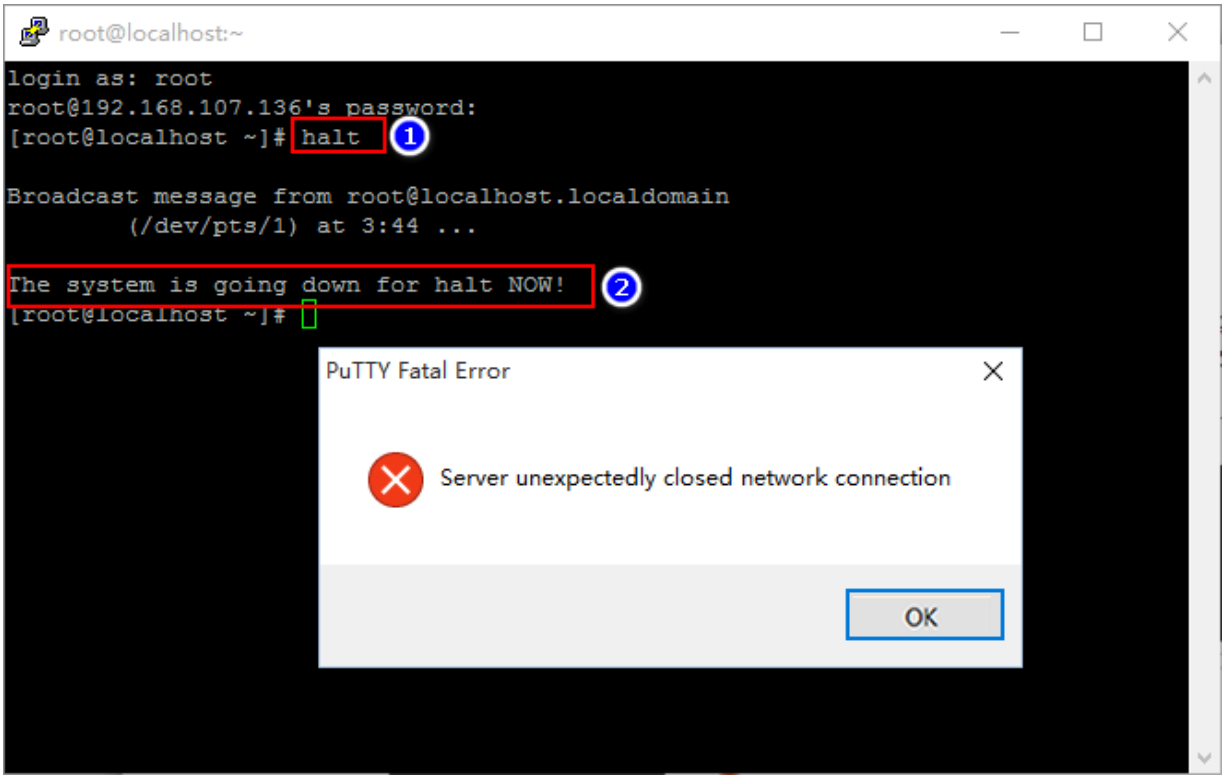
APPENDIX D
SHUTTING DOWN EXSI OS

REVISION AND TESTS PROCEDURE:

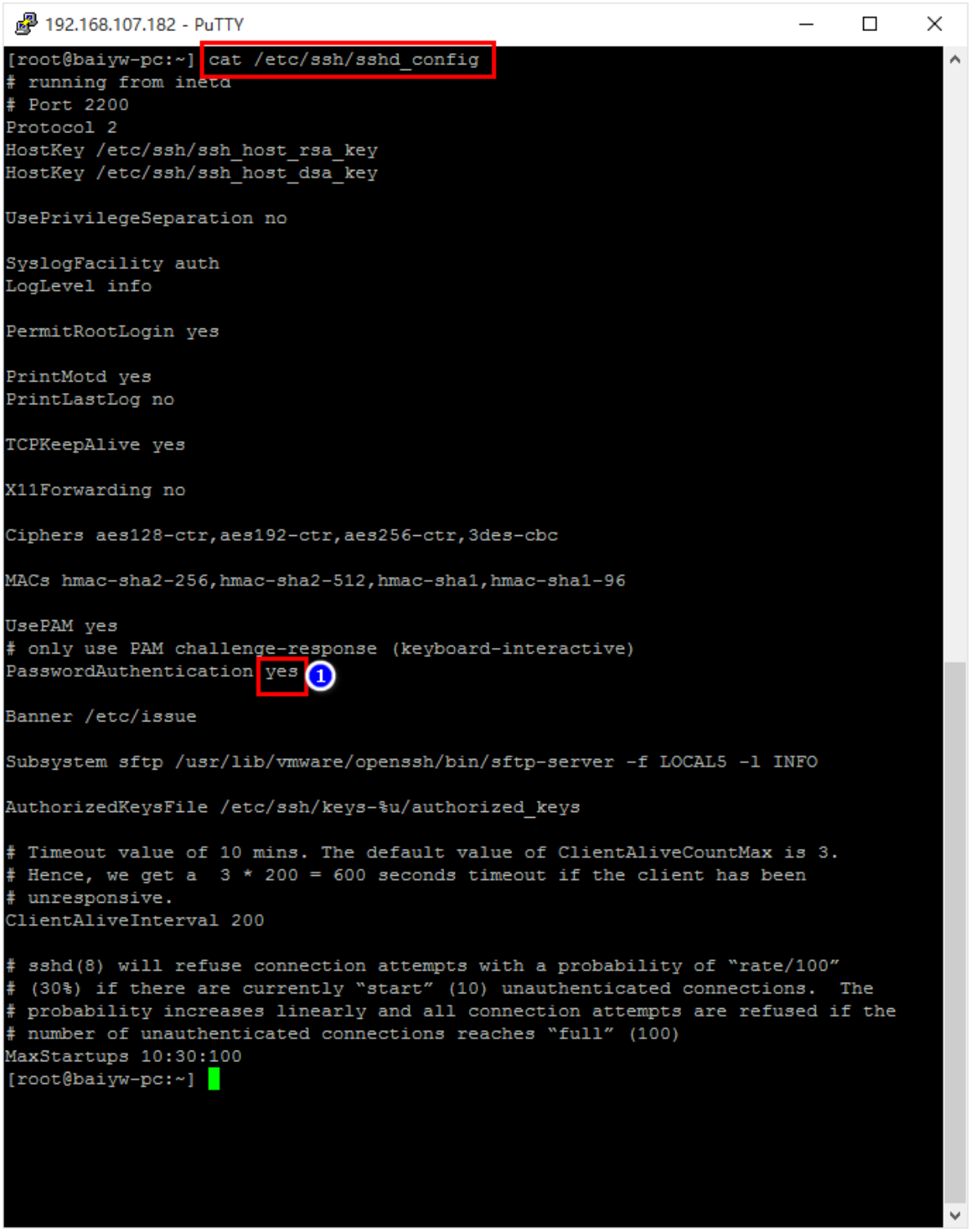
Shutdown commands generated by either **SNMP Web Pro** or Monitoring and Control Software are external commands for ESXI OS, therefore, to assure they will work, please check these two matters:

1. **SSH Shutdown function revision.**
   Try to communicate with the load to be shutdown via SSH tool (such as "putty", "Secure Shell Client", etc.). See the image below as reference:
   - Login as the remote system, as **root**
   - Execute command "halt" for shutdown (See Tag **1** in the image below)

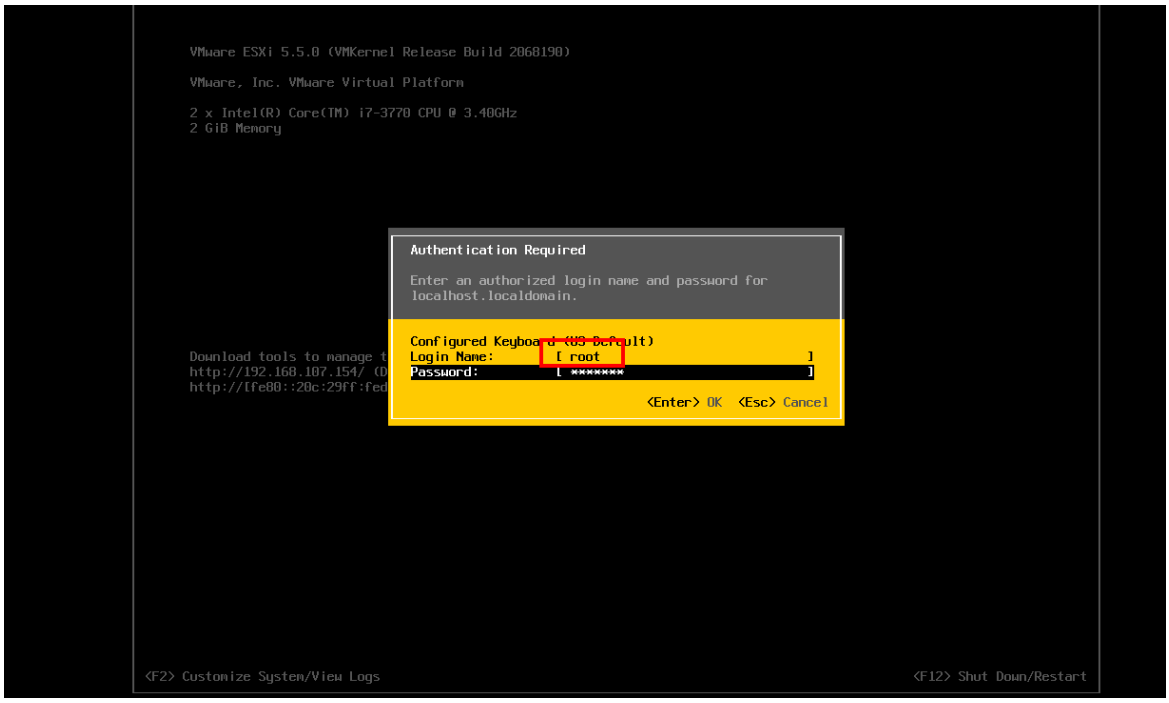
If remote system shutdowns and the tool shows the right message (See Tag **2** in the image below), this means the remote SSH shutdown function works fine, therefore shutdown commands generated from **SNMP Web Pro** or Monitoring and Control Software should work fine on this remote system.



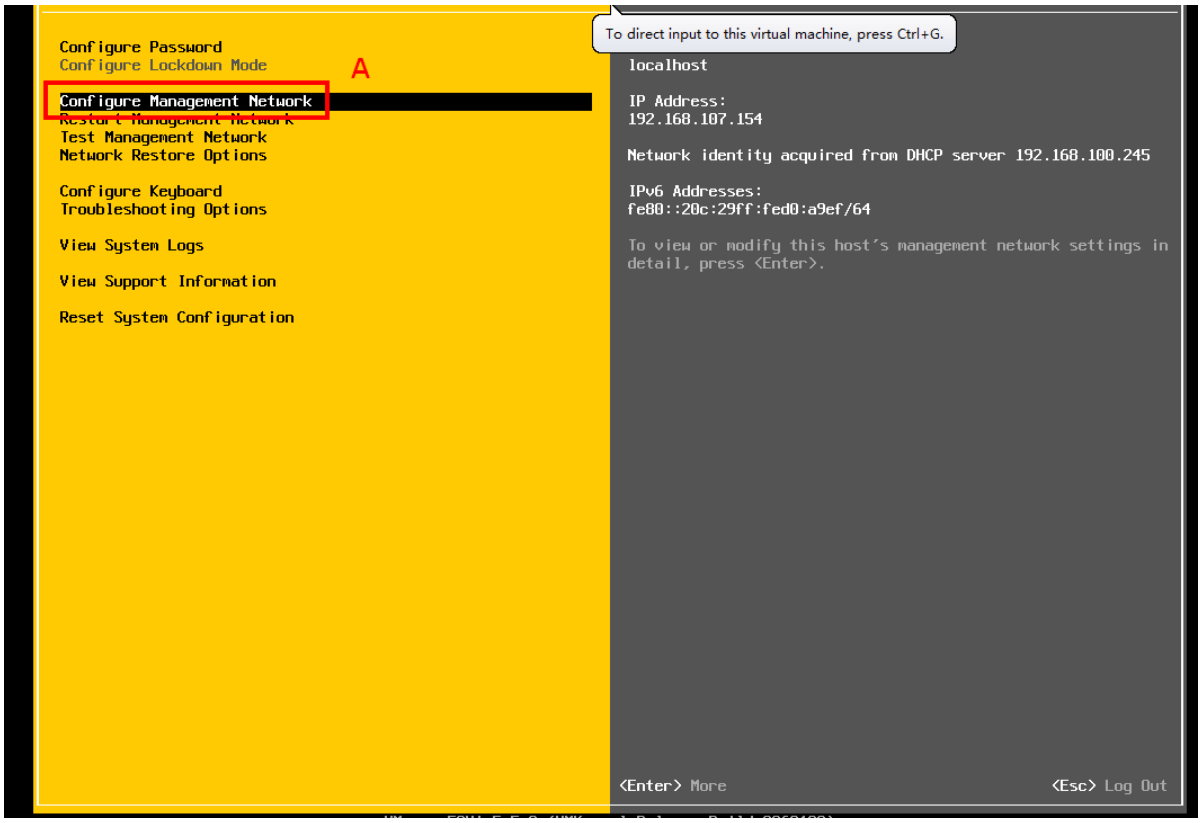
2. **If you can´t communicate with remote system, please check the following procedure:**
   - Make sure your ESXI OS allows the Password Authentication.
   - Please check as below: **cat /etc/ssh/sshd_config**.
   - If the status of **PasswordAuthentication** is “no” (See Tag **1**), change it to “yes”.
   - Restart the SSH server by **/etc/init.d/SSH restart**



3. Log in to your system on root

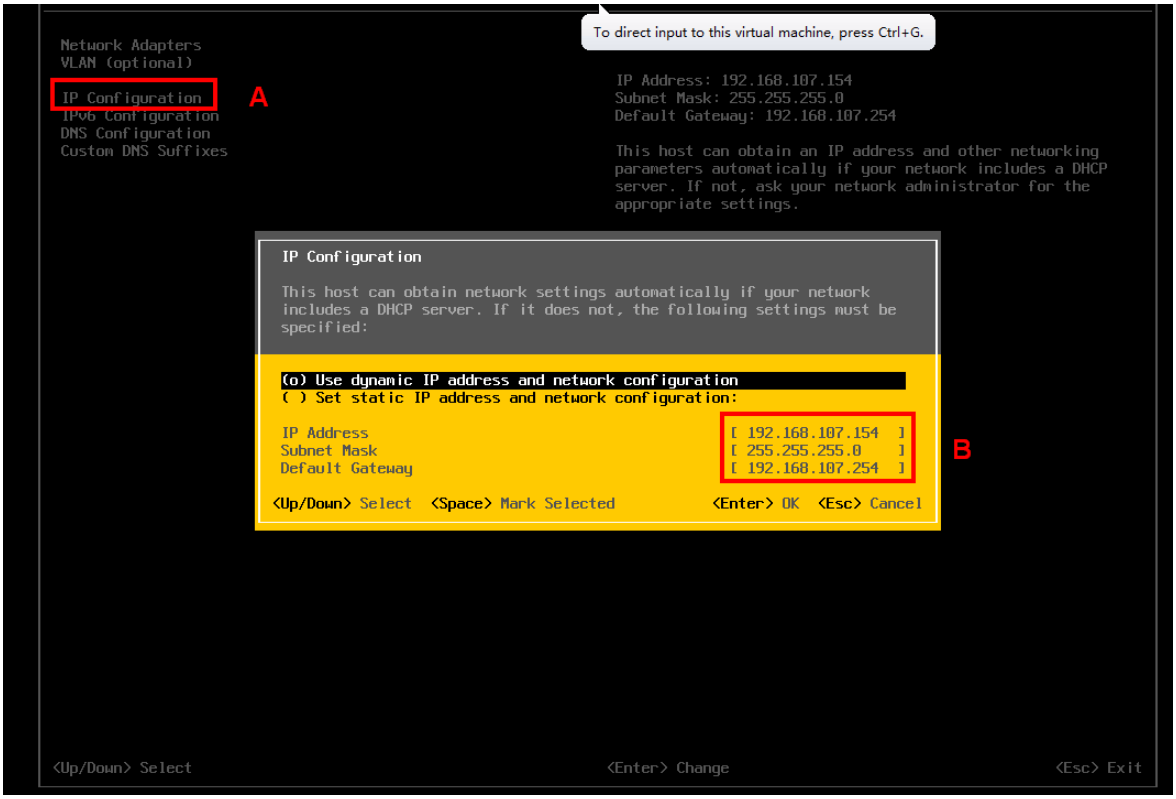


4. **Press F2 key and then select CONFIGURE MANAGEMENT NETWORK (See tag A in next figure).**
Enter as shown below to set **Network Config**, it is necessary for SSH remote shutdown.



5. NETWORK CONFIG

Choose **IP Configuration**, to see the **IP Configuration Panel** y set IP info to make sure the ESXI can be found by the host.



6. Return to step 4 (Interface) and select Troubleshooting Options

7. **Enable SSH**
   - If the screen shows “Enable SSH” means it is disabled. Press ENTER key to enable SSH.
   - If the screen shows “Disable SSH” means it is enabled. Do not do anything else.

   See next figure as reference.

After all previous settings, your ESXI system can accept shutdown commands from Monitoring and Control Software and/or **SNMP Web Pro** through SSH.

APPENDIX E
RECOVERING NOT RESPONDING SNMP06 CARDS.

When an SNMP06 card stops communicating, even though it seems to continue operating, it is usually due to a configuration change, which makes it no longer reachable for the software.

For these cases, the procedure described below can be followed for an operational recovery of the card.

1. On a PC connected to the same LAN as the card, install service software **SNMP WEB MANAGER.** Download it from **Download\Software** section of our WEB page: **www.xmart-ups.com**.

2. Since status of SNMP06 card is unknown, apply a RESET as described in ***NOTE 1 – RESET***, section **1.3 Description** of this manual, so it loads Default Configuration, including fixed IP address, as shown below:
   IP: 192.168.102.230 (STATIC IP)
   Subnet Mask: 255.255.255.0
   Default gateway: 192.168.102.1
   Default Password: 12345678

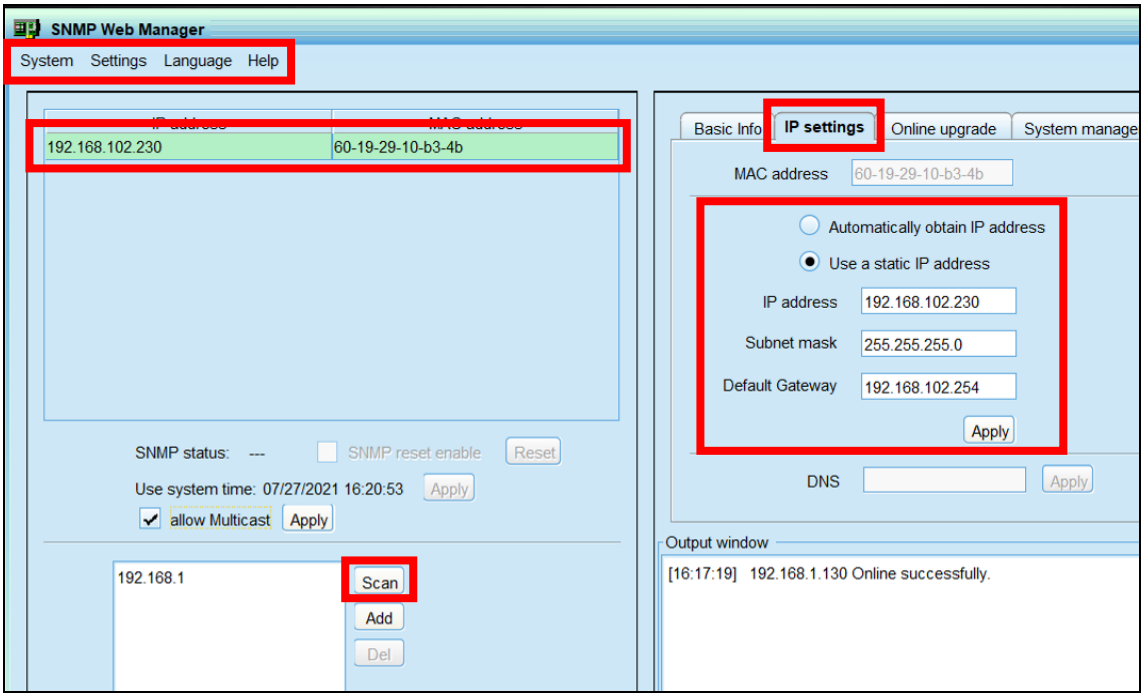
3. SNMP card should be detected by **SNMP WEB MANAGER** in LAN, as long as PC and SNMP card are both connected to same network switch.

4. Make sure the unit is connected to the AC Line, that it is turned on and LCD is illuminated.

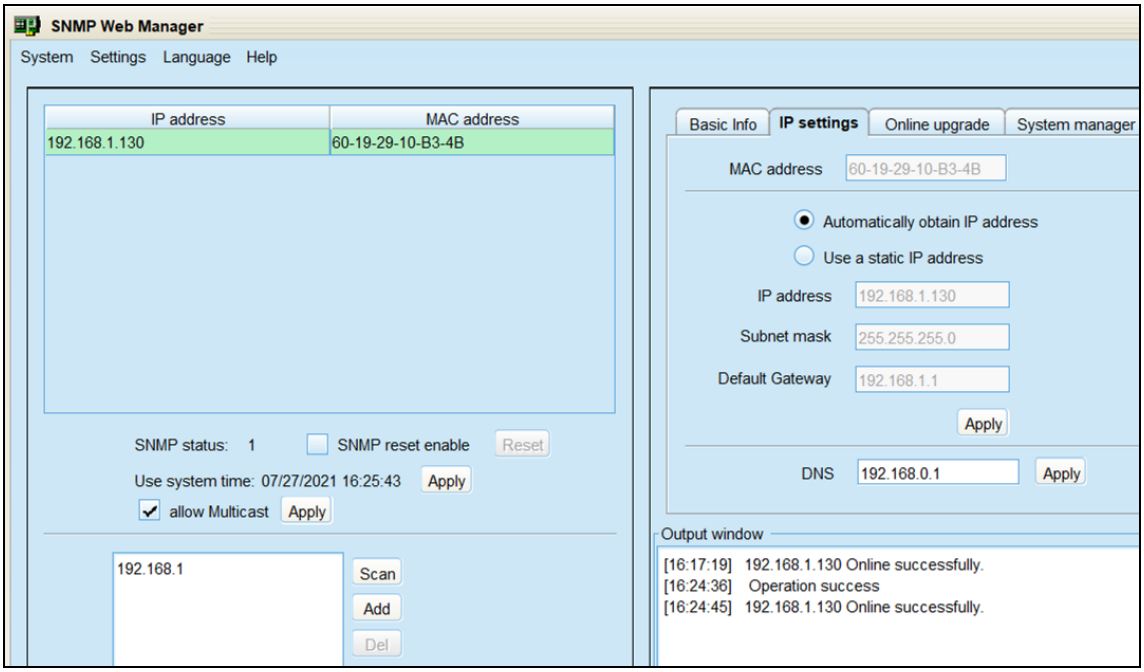
5. Run **SNMP WEB MANAGER** by double clicking the icon which should be installed on the desktop.

6. First try to scan the card from **SNMP WEB MANAGER** leaving it connected to the network switch. For this, press "SCAN" button of **SNMP WEB MANAGER**.

   - When detecting the card, it's IP and MAC will be displayed in the upper left area
   - Click once on the IP and select "IP Settings" tab to see the static IP due to previous RESET.



7. Set all parameters to the desired ones as shown in the previous figure or change the IP to dynamic, as shown in the following image. When asked for the password, enter: 12345678 and login. If the IP SETTINGS tab does not allow changes, do a new “SCAN” and try again.



A few seconds later, SNMP card will change its configuration. If it is not displayed, “SCAN” again.

NOTE:

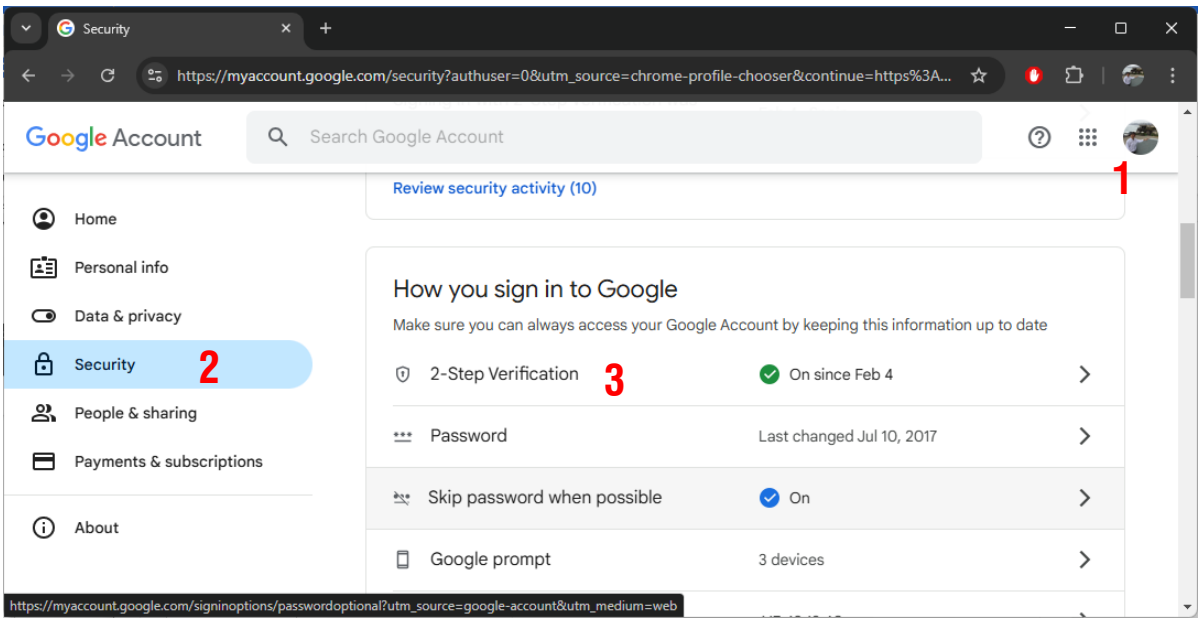
If SNMP card is not recent and **SNMP WEB MANAGER** does not detect it, connect the PC directly to SNMP card using a standard network cable (RJ45) and perform steps 6 and 7.

APPENDIX F
ACTIVATING TWO-STEP VERIFICATION AND SECURITY KEY

If your mail server has a two-steps verification system, the configuration of the SNMP card for sending emails is the one explained in this annex, where we will use a Gmail® account as an example. This procedure applies to any mail server with a two-steps verification service which doesn't use OAuth 2.0 as an authentication method.

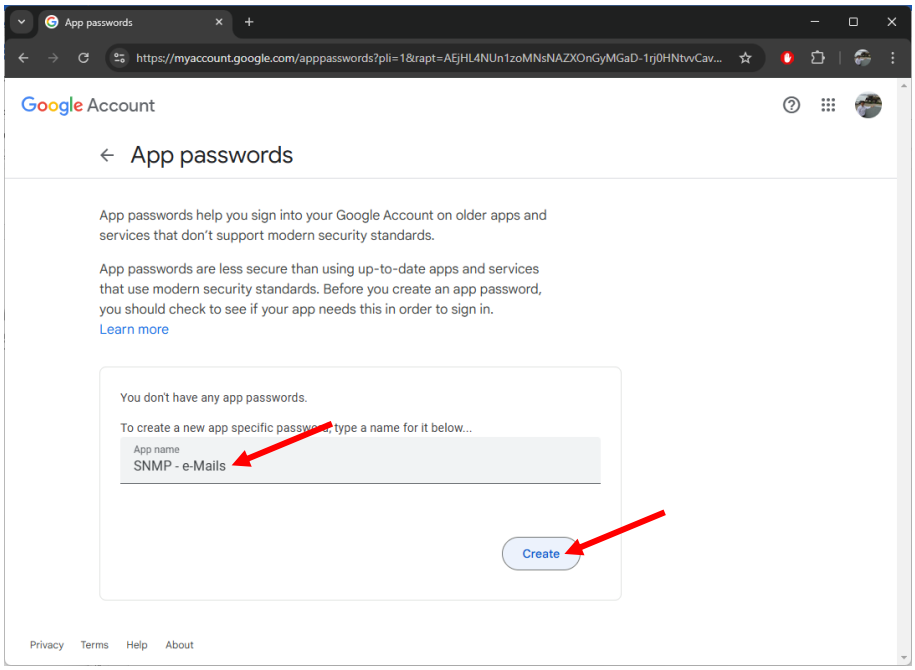
To configure the account from which the SNMP card will send emails, an **App Password** is required, which will be used as the password in the setup. In the case of Gmail® accounts, two-step verification must first be enabled, and then the **App Password** can be generated.

Below, you will find a reference screen, followed by the steps to complete the process.

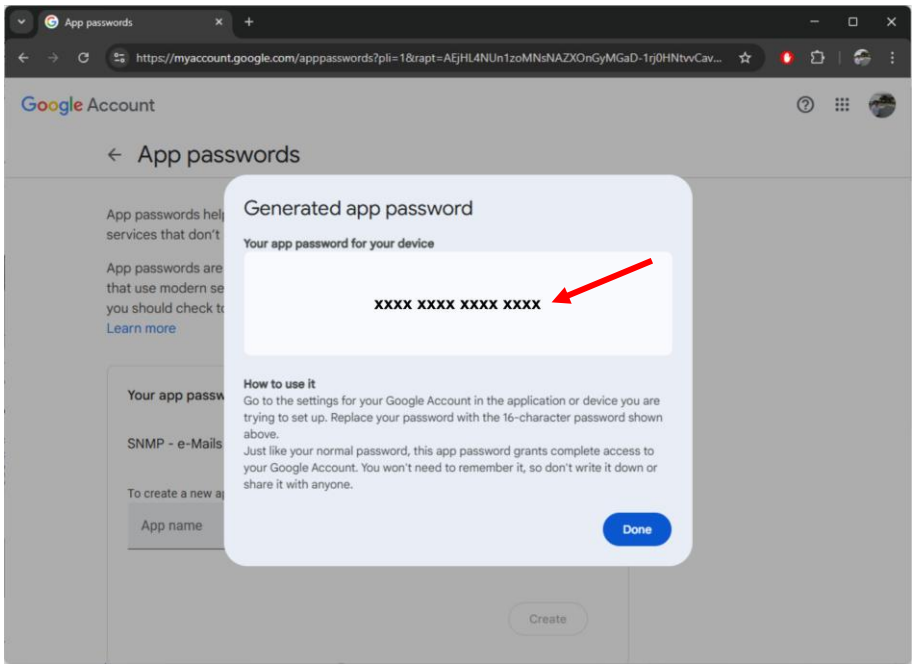


1. Open your Google account.
2. Go to the Security section.
3. Enable the Two-Step Verification option.
4. To do this, you will need a phone number through which Google will complete the verification process.
5. Once Two-Step Verification is enabled, go to the following address:

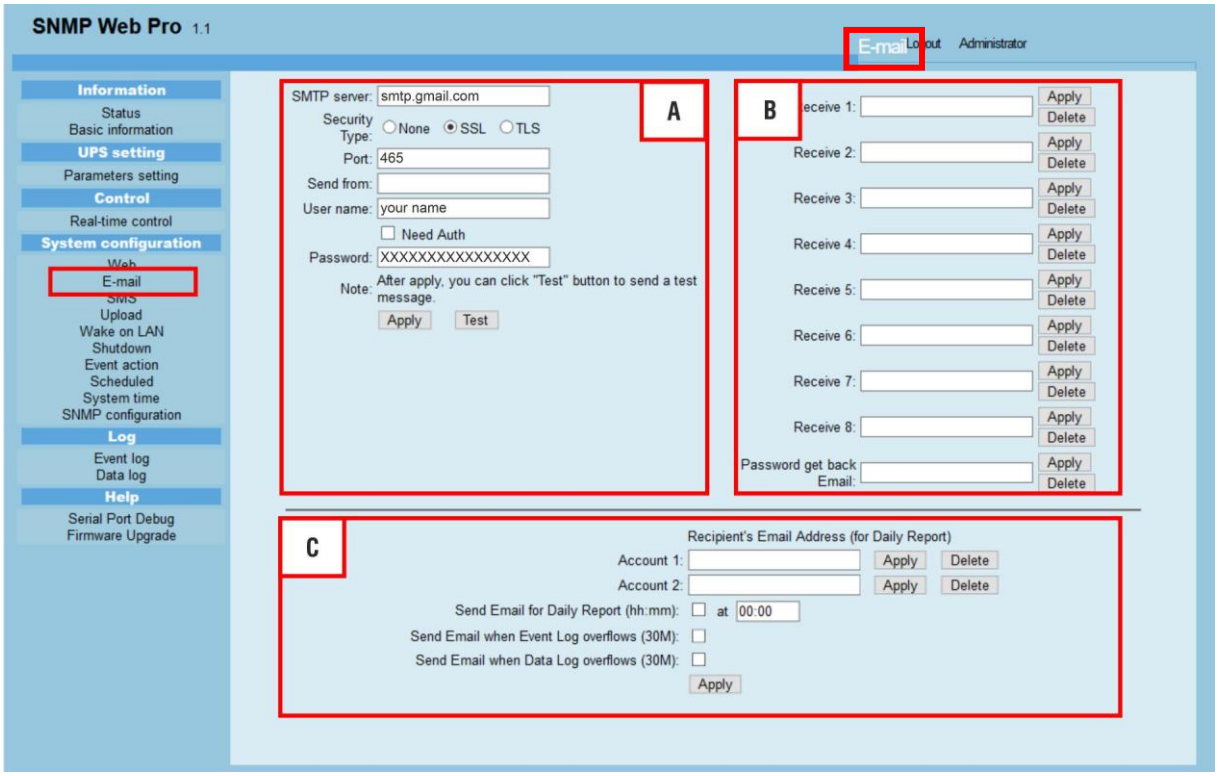
   https://security.google.com/settings/security/apppasswords
6. In the next window that appears, enter a name of your choice and then click the "Create" button, as shown in the image below.



7. A pop-up window will appear, as shown in the following image, displaying the **App Password**. This password will only be shown **once**, so make sure to copy it and save it in a secure place.



Open the **SNMP Web Pro** interface in your browser, connect to the SNMP card you want to configure, log in as the system administrator, and go to the **E-mail** section, as shown in the following figure.



Area A: Enter the server details and the sender's email account.
Area B: Enter the email accounts of the message recipients, up to a maximum of 8.

Email Sender Information (A):

SMTP server:	Mail server used to send emails. In this example: **smtp.gmail.com**
Security Type:	Select the security type of the server to be used. **NONE:** For web domain-based servers, such as emails associated with a website. **SSL:** For email servers with SSL security, such as Gmail, Yahoo, etc. **TLS:** For email servers with TLS security.
Port:	Depending on the server type, the usual ports are: **NONE: 25** / **SSL: 465** / **TLS: 587**
Send from:	Email account used to send emails. For example: *******@gmail.com
User name:	username of the sender's email account. This serves as the email signature.
Need Authorization:	If the outgoing email server requires authentication to send emails, check the **"Need Auth"** box. For Gmail, authentication is required.
Password:	Enter the **Application Password** generated in the previous procedure for your Gmail account, removing any spaces. All characters should be entered together.
APPLY	Once finished, click **APPLY** to save the configuration; otherwise, the data will be lost.

DAILY REPORT (C):

Every day, SNMP can send an email reporting Daily Reports (Area tagged as **C**), here you can configure it:

Account 1: Account 2:	Email addresses to receive Daily report. Select “APPLY” on the right for each receiver added
Send email for daily report:	Mark checkbox to activate, also select the time.
Send email when Event Log overflows:	Mark checkbox to activate.
Send email when Data Log overflows:	Mark checkbox to activate.

IMPORTANT NOTES:

- **The email-sending firmware of the SNMP card has not been compatible with the security settings of Hotmail® and Microsoft® servers since September 2024, due to changes in their authentication system.**
- **If you disable Two-Step Verification on your Gmail account, the generated password will also be deactivated, so it will no longer work.**
- **If you have any doubts, contact your Internet/email provider or your IT administrator.**
- **After configuring the email section, we recommend testing it by clicking the "TEST" button.**

System will response with a message: “TEST SUCCESSFULL” when email has been sent without errors. In case email cannot be sent, system will show a failure message.

If something prevents the email from being sent, the system will display a message indicating that the test has failed. In this case, you should check the configuration parameters of the email sending account and correct any possible errors.