UNIPOWER
POWERING TECHNOLOGY

SageNET User Manual for Sageon Power Systems

PM990.4035.00, Rev 5

UNIPOWER, LLC
65 Industrial Park Rd
Dunlap, TN 37327
Phone: +1-954-346-2442
Toll Free: 1-800-440-3504
Web site – www.unipowerco.com

RECEIVING INSTRUCTIONS
&
GENERAL EQUIPMENT INFORMATION

Please Note: For your protection, the following information and the product manual should be read and thoroughly understood before unpacking, installing, or using the equipment.

UNIPOWER, LLC presents all equipment to the delivering carrier securely packed and in perfect condition. Upon acceptance of the package from us, the delivering carrier assumed responsibility for its safe arrival to you. Once you receive the equipment, it is your responsibility to document any damage the carrier may have inflicted, and to file your claim promptly and accurately.

1. PACKAGE INSPECTION

1.1 Examine the shipping crate or carton for any visible damage: punctures, dents, and any other signs of possible internal damage.

1.2 Describe any damage or shortage on the receiving documents, and have the carrier sign their full name.

1.3 If your receiving freight bill notes that a Tip-N-Tell is attached to your freight, locate it. If the Tip-N-Tell arrow has turned even partially blue, this means the freight has been tipped in transport. Make sure the carrier notes this on your receipt before you sign for the freight.

2. EQUIPMENT INSPECTION

2.1 Within fifteen days, open the crate and inspect the contents for damages. While unpacking, be careful not to discard any equipment, parts, or manuals. If any damage is detected, call the delivering carrier to determine appropriate action. They may require an inspection.

***SAVE ALL SHIPPING MATERIAL FOR THE INSPECTOR TO SEE!**

2.2 After the inspection has been made, call UNIPOWER. We will determine if the equipment should be returned to our plant for repair, or if some other method would be more expeditious. If it is determined that the equipment should be returned to UNIPOWER, ask the delivering carrier to send the packages back to UNIPOWER at the delivering carrier's expense.

2.3 If repair is necessary, we will invoice you for the repair so that you may submit the bill to the delivering carrier with your claim form.

2.4 It is your responsibility to file a claim with the delivering carrier. Failure to properly file a claim for shipping damages may void warranty service for any physical damages later reported for repair.

3. HANDLING

Equipment can be universally heavy or top-heavy. Use adequate humanpower or equipment for handling. Until the equipment is securely mounted, be careful to prevent the equipment from being accidentally tipped over.

4. NAMEPLATE

Each piece of UNIPOWER equipment is identified by a part number on the nameplate. Please refer to this number in all correspondence with UNIPOWER.

5. INITIAL SETTINGS

All equipment is shipped from our production area *fully checked and adjusted*. Do not make any adjustments until you have referred to the technical reference or product manual.

6. SPARE PARTS

To minimize downtime during installation or operation, we suggest you purchase spare fuses, circuit boards and other recommended components as listed on the Recommended Spare Parts List in the back of the product manual. If nothing else, we strongly recommend stocking spare fuses for all systems.

REVISION HISTORY

Rev	Description	Checked & Approved by / Date
5	See PCO 45388	CJM 8/1/19

PROPRIETARY AND CONFIDENTIAL

The information contained in this product manual is the sole property of UNIPOWER, LLC. Reproduction of the manual or any portion of the manual without the written permission of UNIPOWER, LLC is prohibited.

DISCLAIMER

Data, descriptions, and specifications presented herein are subject to revision by UNIPOWER, LLC without notice. While such information is believed to be accurate as indicated herein, UNIPOWER, LLC makes no warranty and hereby disclaims all warranties, express or implied, with regard to the accuracy or completeness of such information. Further, because the product(s) featured herein may be used under conditions beyond its control, UNIPOWER, LLC hereby disclaims and excludes all warranties, express, implied, or statutory, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any implied warranties otherwise arising from course of dealing or usage of trade. The user is solely responsible for determining the suitability of the product(s) featured herein for user's intended purpose and in user's specific application.

Throughout the remainder of this manual, "UNIPOWER" will mean "UNIPOWER, LLC."

PERSONNEL REQUIREMENTS

Installation, setup, operation, and servicing of this equipment should be performed by qualified persons thoroughly familiar with this Product Manual and Applicable Local and National Codes. A copy of this manual is included with the equipment shipment.

Table of Contents

1 INTRODUCTION

The SageNET system is an embedded network server, attached to a Sageon Control Unit that allows the Sageon Power Plant to be accessed from anywhere in the world.

SageNET runs over any IP network, including the Internet, and allows monitoring of the site via the Sageon's proprietary SageView protocol, as well as SNMP and HTTP.

The SNMP interface allows alarm notification via traps, and read only access to all of the system controller parameters, with a remote Network Management System. The SageNET unit allows you to setup which alarms you want reported as SNMP traps.

Using the SageVIEW monitoring and control program, you may configure and monitor the system controller on up to 2 separate computers, at any given time. Alternatively, you can monitor the system controller's status via a web browser with no additional software required.

1.1 NOMENCLATURE

Throughout this manual the following styles are used to differentiate between pull-down menus and selections.

File Menu	Denotes a pull down menu from the menu bar at the top of the window
Print	Denotes a selection option within a pull down menu
SCU	Denotes a short-cut button on the toolbar below the menu bar

1.2 GETTING STARTED

1.2.1 Package Contents

- SageNET Hardware
  - SageNET Printed Circuit Board Assembly

- CD, containing
  - Installation & Operation Manual (this document);
  - Configuration Tool Installation; (SageNET Config)
  - SageNET MIB;
  - XPort Device Installer

1.2.2 Minimum Requirements

1.2.2.1 Minimum PC Requirements

The following equipment is required to establish a connection to a SCU:

- Computer running Windows 98/Me/2000/XP/7/8/8.1 with at least 10MB of disk space available. The SageNET Configuration program is best view at screen resolution of 1024x768 or higher. The minimum screen resolution required is 800x600.
- A network connection to the SageNET product
- For HTTP Interface users:
  - Internet Explorer 6.0, Netscape, Netscape 7 or Firefox 1.0 (or higher)
  - Java 1.4.2 (or higher) Runtime Engine

1.2.2.2 Minimum SCU Requirements

The following are the minimum requirements for the SCU

- SCU with BIOS revision '.3'. or any Micro Sageon SCU Controller. The revision is displayed when the

SCU is powered up or may be displayed at any time by selecting the ‘Test Indicators’ menu function on the front panel of the Sageon Power Plant.

1.2.2.3 Minimum User Requirements

- For installation of the SageNET unit, it is recommended that your have some working knowledge of general network settings, the TCP/IP and UDP/IP protocols, and also have access to network information Installation requires administrative privileges.
- If SNMP is to be installed it is highly recommended that your have knowledge of the Network Management System to be used.

2 INSTALLATION

2.1 INSTALLING SAGENET

2.1.1 Installing the SageNET Unit

There are two methods of setting your SageNET unit up on your network.

- ARP and Telnet
- XPort Installer

Each of these methods has its advantages, and you should choose the method that suits your particular needs.

2.1.1.1 Setting the IP Address using ARP and Telnet

Procedure described below is recommended for advanced users with understanding of operation of networks.

2.1.1.2 Preparations for local address set up

From your network administrator obtain a new static IP address. Also ask for your network class / subnet mask and default gateway. At the end of this manual you will find a sheet for SageNET setup data to record your settings.

Connect PC to the SageNET’s network interface (directly using a crossover Ethernet cable or via a network hub). **Note: The PC <u>must</u> be on the same physical network subnet as the SageNET being configured.**

Power-up the SageNET

2.1.1.3 Local IP address set up procedure

The following section is excerpted from Lantronix "Embedded Integration Kit" Revision D 06/03/02, Part Number 900-226.

The unit’s IP address must be configured before a network connection is available. If the unit has no IP address, you can use Address Resolution Protocol (ARP) method from Windows-based systems to assign a temporary IP address. If you want to initially configure the unit through the network, follow these steps:

1. On a Windows-based host, create an entry in the host's ARP table using the intended IP address and the hardware address of the unit, which is found on the product label on the bottom of the unit.

   ```
   arp -s 191.12.3.77 00-20-4A-xx-xx-xx
   ```

   Notes:

   i. The IP address used here is an example and a value within the range of allowable IP addresses in your network may need to be used. The DOS command *ipconfig* with display the IP address of the Windows-based host machine.

ii. For the ARP command to work on Windows 95 (and later) the ARP table on the PC must have at least one IP address defined other than its own.

2. If you are using Windows 95, type ARP -A at the DOS command prompt to verify that there is at least one entry in the ARP table. If the local machine is the only entry, ping another IP address on your network to build a new entry in the ARP table; the IP address must be a host other than the machine on which you are working. Once there is at least one additional entry in the ARP table, use the following command to ARP an IP address to the unit:
   ```
   arp -s 192.168.0.97 00-20-4a-xx-xx-xx
   ```

3. Open a Telnet connection to port 1. The connection will fail quickly, but the unit will temporarily change its IP address to the one designated in this step.

   ```
   telnet 192.168.0.97.1
   ```

4. Finally, open a Telnet connection to port 9999 and press Enter within three seconds to go into Setup Mode. If you wait longer than three seconds the unit will reboot.

   ```
   telnet 192.168.0.97 9999
   ```

5. Set all required parameters

Note: The IP address you just set is temporary and will revert to the default value when the unit 's power is reset unless you log into the unit and store the changes permanently. Refer to the chapter on configuration for instructions on permanently configuring the IP address. Telnet must be reenabled in Windows 7 or later.
� Lantronix, Inc, 2002, all rights reserved, used herein by permission from Lantronix.

Note:
On Windows 2000 1XP/7/8/8.1 systems equipped with multiple network interfaces, it is necessary to specify which physical network port the ARP command should use. Using the command-line program **ipconfig***, identify the IP address of the port on your computer that is connected to the SageNet. In the following example, assume* **ipconfig** *returns 192.168.0.22 as the IP address for your computer's port. The ARP command would then be:*

```
arp -s 192.168.0.97 00-20-4a-xx-xx-xx 192.168.0.22
```

2.1.1.4 XPort Installer

The XPort Installation tool is provided on the SageNET Installation CD in the \XPORT Installer subdirectory. Please run the Setup.exe program from that director to install XPort Installer. If your computer does not have Microsoft .NET Framework already installed, please install .NET Framework from the CD before installing the XPORT installer.

To configure your SageNET module's IP address using the XPort Installer, you will need to know the MAC address of your SageNET module.

2.1.1.5 Preparations for local address set up

- From your network administrator obtain new static IP address. Also ask for your network class / subnet mask.
- Retrieve the MAC address from the SageNET module (see label on RJ45 jack).

- Connect PC to the SageNET's network interface (directly using a crossover Ethernet cable or via a network hub). Note: The PC must be on the same physical & logical network subnet as the SageNET being configured.
- Power-up the SageNET
- Start Xport Installer Program

2.1.1.6 Local IP Address set up procedure

- On the XPort Installer toolbar, click the "Assign IP" button
- Enter the SageNET modules MAC address.
- Enter the assigned IP address for the SageNET module
- Click "OK" button.
- The program will then take a few seconds, and should return either a success message, or a failure message.
- If the program returns a failure message, check the details of the unit, (ie MAC address, and assigned IP address), and make sure there is no other device with the assigned IP address on the network..
- On the XPort Installer toolbar, you can now click "search", and a list of your SageNET units will be presented. Look for the unit you have just programmed, to ensure they unit is using the correct IP address.

2.1.2 Installing the SageNET Configuration Tool

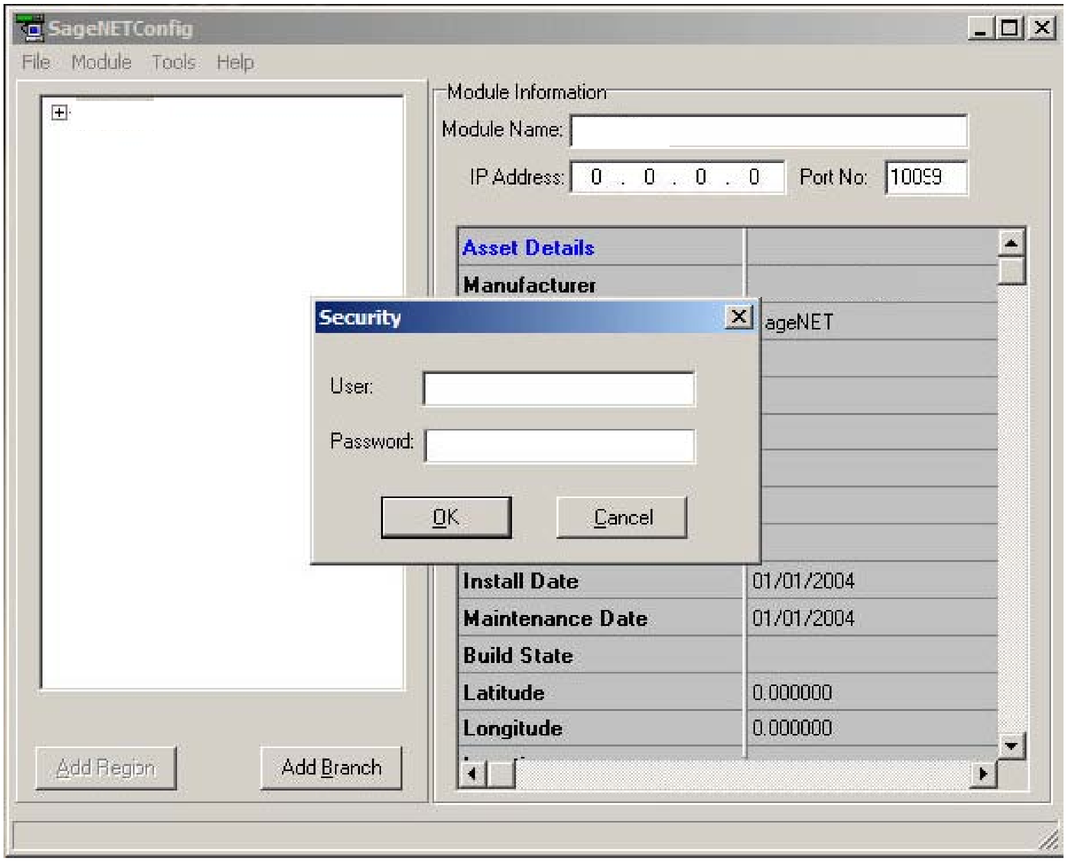
Please ensure you are logged into an account with dministrative access before installing. If you are not sure, please consult your network administrator.

- Insert the CD into the CD-ROM drive.
- The CD will auto-play to install the configuration software.
- Follow the prompts during the installation procedure.

At the completion of installation, a SageNET Configuration shortcut icon will be added to the Start/Program menu.

2.1.3 Installing the SageNET MIB

The SageNET MIB has been provided to allow integration into the your Network Management System. Please consult the network management system's help for directions on how to compile and install the MIB.



Module Information

Module Name:

IP Address: 0 . 0 . 0 . 0 Port No: 10099

Asset Details	
Manufacturer	
	ageNET
Install Date	01/01/2004
Maintenance Date	01/01/2004
Build State	
Latitude	0.000000
Longitude	0.000000

User:

Password:

2.2 DEFAULT PASSWORD

The default username is: Administrator and the defaultpassword is: configuration.This password screen will appear every time you run the configuration tool. It is to ensure that no unauthorised user can log in to the system. This prevents unauthorised users from making critical changes to any SageNET units.Please change the default password immediately. Accessing your ***Management*** option of the **Tools** menu (see …) can do this.

NOTE:

Every attempt to log in to the application is logged in the system event log, and also sent to a syslog server on the network. (see section Reporting Options).

2.3 NETWORK SETUP

DISCLAIMER

This section describes some tips and troubleshooting for the installation of a SageNET unit on a user's network. Each user's network is unique, and as such UNIPOWER cannot accept responsibility for any errors or problems that occur during the installation of a SageNET unit.

If you do not have experience maintaining and configuring your network, or do not have sufficient authorization, it is STRONGLY RECOMMENDED that you contact you network or systems administrator to either help, or configure this for you.

2.3.1 Network Protocols

SageNET is designed to allow a user to remotely monitor the system controller, over a IP based network. It uses 2 widely used protocols, known as the TCP and UDP protocols. Although it is not essential to understand these protocols in depth, a basic knowledge of these protocols is recommended, to assist your in the setup and any troubleshooting of network issues. The Transmission Control Protocol (TCP) and your Datagram Protocol (UDP) protocols are widely documented, on the Internet, and online tutorials are readily available for both protocols.

TCP and UDP are both IP based standards, defined under a global standards system, known as RFC (Request For Comments). TCP is defined under RFC 793 (http://www.faqs.org/rfcs/rfc793.html), the UDP is defined under RFC 768 (http://www.faqs.org/rfcs/rfc768.html), and the IP standard is available in RFC 791, (http://www.faqs.org/rfcs/rfc791.html).

The TCP and UDP standards are used as a method of encapsulating data from network applications for transport. The IP standard is essentially a method for addressing computers, and other network devices, using a standard addressing scheme. The combination of these standards allows every computer to allow simultaneous communications on each device, over different channels.

2.3.1.1 Addressing Schemes

A key notion of the TCP/IP and UDP/IP standards is the addressing scheme. An IPv4 address is a 32 bit address, broken up into 4 bytes. It is normally represented as 4 sub sections, and displayed as such: xxx.xxx.xxx.xxx, where each xxx is an integer in the range 0 – 255. Classless routing (CIDR) is now standard; however, the follow may still be useful.

There are 3 main classes of network addresses.

Class	Range Start	Range End	Subnet Mask
Class A	1.0.0.0	127.255.255.255	255.0.0.0
Class B	128.0.0.1	191.255.255.255	255.255.0.0
Class C	192.0.0.0	233.255.255.255	255.255.255

Class A networks are fairly major networks, and generally used by military or governments. Class B networks are normally used for large companies, with a lot of computers on the Internet. Class C networks are reserved for small – medium companies.

There are 4 exceptions to the above. The IP address 127.0.0.1 is used exclusively as a loopback address, also the following 3 ranges are used as internal network addresses only, and cannot be used on the Internet.

Class	Range Start	Range End
Class A	10.0.0.0	10.255.255.255
Class B	172.16.0.0	172.31.255.255
Class C	192.168.0.0	192.168.255.255

2.3.1.2 Ports

Ports are an integral component of the TCP and UDP standards. For each standard, there are 65535 ports that can be used to access the network device. Some of the ports are defined, (known as the 'Well Known Ports'), some are reserved, and some are free to be used.

An example of ports, is when an Internet browser, (such as Internet Explorer or Netscape), requests a web page, a TCP connection is established between the 2 computers. However, if the connection were established between the 2 computers, and not ports of the 2 computers, the computers would then be effectively closed to any other incoming connections. So, instead, the browser connects to a single port, (in the case of HTTP, this is port 80). This allows both computers to still accept any incoming connections on any of the other open ports they have.

One good way to look at these ports is doors to a building. You have an address for the building, which is your IP address, as described above. The ports then become the entries to the building. Without making a connection to the port, you cannot enter.

2.3.1.3 TCP versus UDP

TCP and UDP are the most commonly used IP based protocols in operation today. They are however, different in their basic makeup.

TCP establishes a connection between 2 computers, which is held open for as long as the connection is needed. This is analogous to calling somebody on a telephone. Every packet is tracked through the network, and if any packets are lost, the protocol knows to request a resend of the packet immediately.

UDP sends a packet through the IP based network to the receiver, similar to sending a letter to somebody via postal mail. There is no connection made between the 2 computers, and no absolute assurance that the packet will reach the intended destination.

SageNET uses both of these protocols for different tasks.

2.3.2 Network Setup & Troubleshooting

When installing the SageNET unit onto your network, you should ask some basic questions before beginning, which will assist you with the installation.

- What static IP Address should the unit use?
- What is the Subnet mask?
- What is the default gateway’s IP address?
- Is there a firewall? Do I use a proxy server?

2.3.2.1 SageNET IP Address

The IP Address of each SageNET unit is static. This means it cannot be dynamically given an IP address on boot up, using a DHCP server. You need to assign an IP address to the unit, and ensure that the IP address you give it is unique on the network.

To assign an IP address to the SageNET unit, see section 2.1.1

2.3.2.2 Subnet Mask

Each IP based network has a subnet mask used on it. The subnet mask usually corresponds to the class of the network, as described in section 2.3.1.2. This will need to be changed to reflect the subnet mask used in your particular network..

TIP: Use the Windows™ command line tool ipconfig to discover your subnet mask.

2.3.2.3 Gateway IP Address

The gateway IP address is required, if you will be communicating with computers that are not on the same LAN segment. A gateway is generally a computer, router, or bridge, which in connects a PC, or network device to another network, for instance, the Internet.

TIP: Use the Windows™ command line tool ipconfig to discover your Gateway IP address.

2.3.2.4 Firewalls

Firewalls are devices that block incoming (and sometimes outgoing) packets from accessing your network. It is a method of stopping any network 'hacking'. In current day systems, firewalls are in common use with most Internet connections.

The way a firewall works, is it blocks any attempts to establish a connection with the network device. The connections are generally blocked when a PC or network device attempts to connect to the internal network from the Internet.

Many firewalls also provide security by for data which must pass across the Internet, this feature being referred to as virtual private networking (VPN). Using SageNET across the Internet without any form of encryption is NOT recommended. All data transfer is in an unprotected state, and is vulnerable to attack. Remote access across the Internet should be done via a virtual private network.

To use SageNET across the Internet, you must ensure that certain ports are available for connection. Most of these ports are configurable, such as the WinCSU-2 connection ports; the web interface connection port and the configuration and firmware upgrade ports. Some ports, are not configurable, such as the SNMP trap (UDP Port 162) and SNMP monitoring ports (UDP Port 161), and the HTTP connection ports (TCP Port 80).

To utilize the features of SageNET, you will need to ensure that all ports you decide to use are open to the Internet

For a full list of the TCP and UDP port assignments, please refer to:
http://www.iana.org/assignments/port-numbers

Each firewall has its own way of configuring ports for usage. Please refer to the firewall manuals for instructions on how to open ports.

2.3.2.5 Proxy Server

A proxy server is a method of speeding up the loading of web pages. It generally operates from an Internet Service Provider's network, and when a web page is loaded, it is cached into the proxy server. Then, if the same webpage is requested again within a certain time frame, the page from the proxy server is sent again, reducing the time to get the page.

You should avoid using a proxy server with the SageNET unit. This is because when a proxy server is used, some of the pre-processing that occurs before the page is returned does not get redone, and as such, some changes that may have occurred, may not be reflected in the reloaded web page.

TIP: Internet Explorer allows the proxy setting to be switched off or excluded for particular IP addresses, under the Tools Menu, Options, Connections Tab, LAN Settings, Advanced.

3 SAGENET CONFIGURATION TOOL OPERATION

The SageNET Configuration Tool allows you to review and change the configuration of each SageNET module, on one, or more PC's. This tool allows you to create regions and locations, and organise these units in a tree structure, for easy sorting and maintenance.

With this tool, you can download the configuration from, or upload the configuration to any SageNET module that it has network access to. This may range from a SageNET unit on your local area network (LAN) or using a wide area network (WAN) such as the Internet, access a module on the other side of the world.

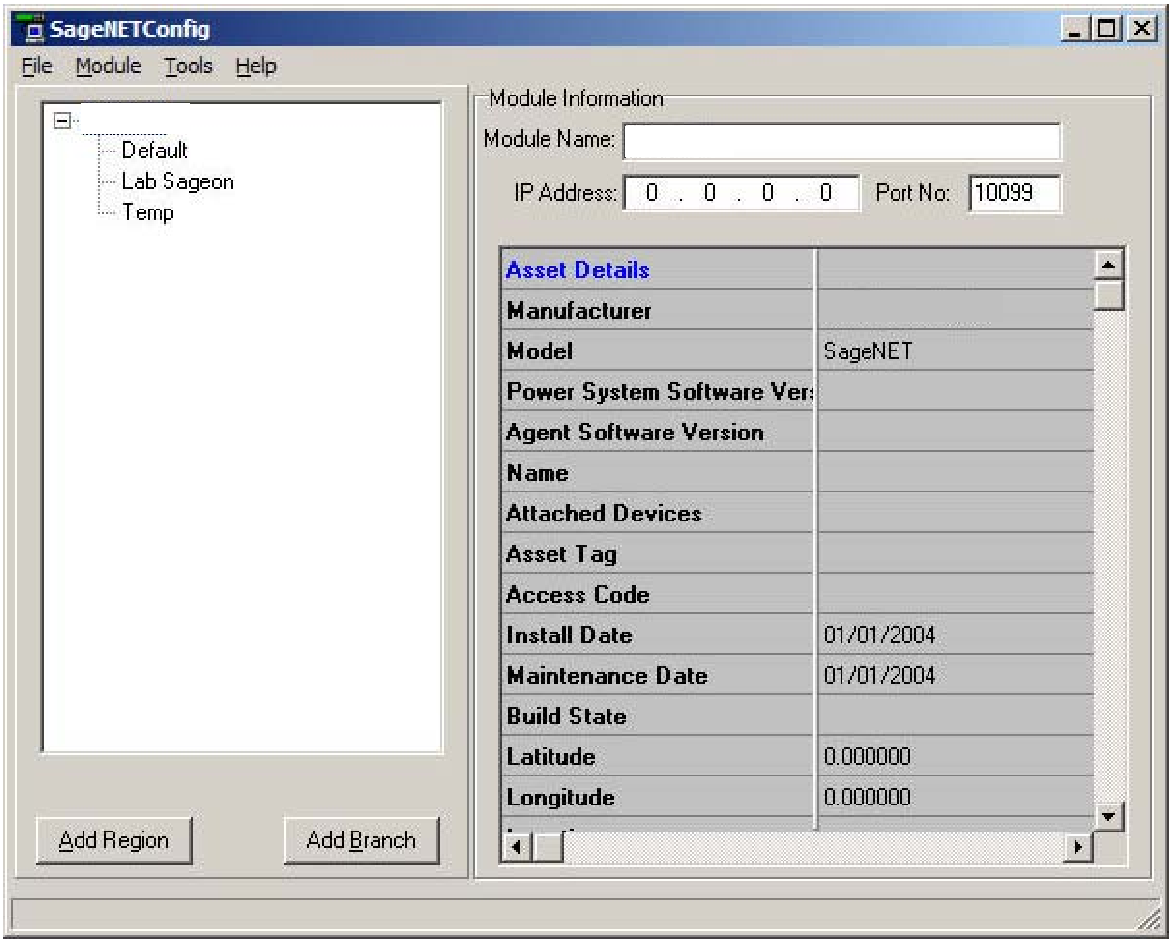
The tool also allows you to update the SageNET module with updated web page modules and firmware updates, and the SCU firmware from a remote location.

All the configuration information for each module is saved onto the local hard disk, and can be backed up accordingly.

The configuration utility also provides traceability, as it logs important information to the system event log, and also can be configured to send syslog messages to a network syslog server.

3.1 THE MAIN SCREEN

The main screen allows you to create and maintain many SageNET modules, in various locations. It can show the configuration for each module listed, and gives access to edit each modules setting's via the menu system.



Module Name:

IP Address: 0 . 0 . 0 . 0 Port No: 10099

Asset Details	
Manufacturer	
Model	SageNET
Power System Software Ver:	
Agent Software Version	
Name	
Attached Devices	
Asset Tag	
Access Code	
Install Date	01/01/2004
Maintenance Date	01/01/2004
Build State	
Latitude	0.000000
Longitude	0.000000

3.1.1 The Module Tree

The module tree allows you to define a organisational tree, listing all the SageNET modules that will be accessed by the configuration tool. Using the *Add Region* and *Add Branch* buttons, your can define regions based on geographical location, or logistical information.

3.1.2 The Module Information Area

There are 4 important sections of the Site Information area.

3.1.2.1 Module Name

The module name is configurable label, set by you, and allows the changes in how it appears in the Module Tree.

3.1.2.2 IP Address

The IP Address of the module that you wish to connect to, is set here.

TIP: If you wish to upload the same module configuration to more than one unit, create a template and upload to each unit by adjusting the IP Address each time.

3.1.2.3 Port No

The configuration port of the SageNET module will not normally require changing from the default value of 10099. This is the port that you wish to connect to during the next configuration upload or download.

3.1.2.4 Module Information Window

The module information window allows you to quickly view a module's settings. This section will give you a break down of all the settings that can be changed via the Module Properties menu. There is some additional data displayed in the site information window. These details are saved locally on the PC, and are not transferable between SageNET and the configuration tool.

The additional data includes;

3.1.2.4.1 <u>Last Configuration File Write Date</u>

Shows the last date the configuration was written to the SageNET module.

3.1.2.4.2 <u>Last SageNET Firmware Write Date</u>

Shows the last date the SageNET firmware was updated.

3.1.2.4.3 <u>Last SageNET Firmware Filename</u>

Shows the filename of the last SageNET firmware file that was uploaded.

3.1.2.4.4 <u>Last SageNET Webpage Write Date</u>

Shows the date of the last webpage update on the SageNET.

3.1.2.4.5 <u>Last SageNET Webpage Filename</u>

Shows the last webpage file to be uploaded to the SageNET Module.

3.1.2.4.6 <u>Last SCU Firmware Write Date</u>

Shows the date of the last SCU Firmware Update.

3.1.2.4.7 <u>Last SCU Firmware Filename</u>

Shows the last firmware filename that was uploaded to the SCU.

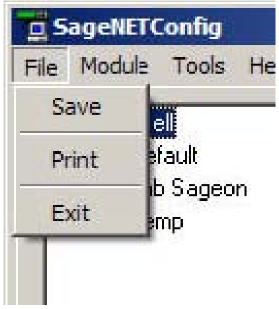
This information is logged in the system event log, and reported to a syslog server, if configured.

3.2 PULL-DOWN MENUS

The pull-down menus provide access to all your selectable functions of the SageNET configuration tool. This section describes the function of each pull-down menu and its sub-items.

3.2.1 File Menu

The File menu provides the ability to print hardcopies of module settings, saving the configuration information, and exiting the program. The functions available in the **<u>File Menu</u>** in listed order are as follows:



3.2.1.1 Save

Saves any changes to a module configurations to the local disk for future reference. You will be asked to save on exit, but to safe guard change in the meantime, they should use the save menu option.

3.2.1.2 Print

Prints the currently selected window. The Print Dialogue appears, allowing you to select the appropriate printer and properties.

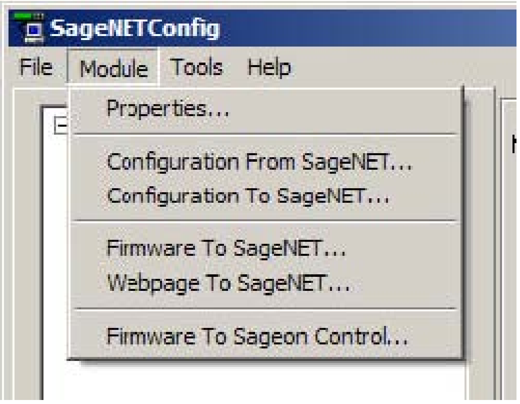
3.2.1.3 Exit

Exits the SageNET programs and returns to the operating system.

3.2.2 Module Menu

The Module menu provides access to the configuration properties and functions of the SageNET Module selected.

The functions available in the **Module Menu** in listed order are as follows:



3.2.2.1 Properties

Opens the module parameters window that displays and allows editing of the currently selected SageNET module parameters.

3.2.2.2 Configuration From SageNET

Creates a connection to the currently selected SageNET module, and downloads the live configuration information from the module.

3.2.2.3 Configuration To SageNET

Creates a connection to the currently selected SageNET module, and uploads the configuration information to the module.

This operation will result in the SageNET module resetting, and is logged in the system event log, and to the syslog server, if configured.

3.2.2.4 Firmware To SageNET

Allows you to upload the latest firmware provided by UNIPOWER to the SageNET module.

This operation will result in the SageNET module resetting, and is logged in the system event log, and to the syslog server, if configured.

When selected, a dialog box will open, requesting the file to be uploaded, which will be of type .rom

WARNING *This function affects the SageNET firmware and as such, may cause malfunctions of the SageNET unit. Please ensure the correct software is uploaded to the SageNET module, and that UNIPOWER has provided the software. UNIPOWER accepts no responsibility for any errors caused by uploading incorrect firmware files.*

3.2.2.5 Webpage to SageNET

Allows you to update the web page files on the SageNET module.

When selected, a dialog box will open, searching for .cob files, which may be uploaded to the SageNET unit. The cob file is a special file that packages all the html files and java files into one file.

3.2.2.6 Firmware to SCU

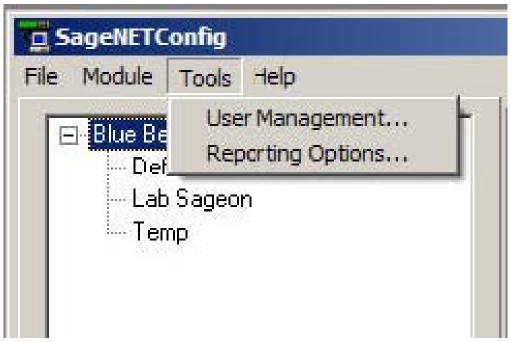
Allows you to update the SCU firmware from a remote location.

This operation will result in the SageNET module resetting, and is logged in the system event log, and to the syslog server, if configured.

****WARNING**** *This function effects the SCU firmware and as such, may cause malfunctions of the SCU unit. Please ensure the correct software is uploaded to the SCU, and that UNIPOWER has provided the software. UNIPOWER accepts no responsibility for any errors caused by uploading incorrect firmware files.*

3.2.3 Tools Menu

The **Tools Menu** provides access to the program options of the SageNET configuration tool.



3.2.3.1 User Management

Opens the User Management window. This window allows you to add or delete users, and edit user information.

3.2.3.2 Reporting Options

Opens a window that allows you to set the syslog reporting address. This should be the address of a syslog server on the network. The syslog server will then receive notifications of events, such as opening and closing of the program, user login's, changing of user information, changing of module configurations, uploads and downloads of configurations, and uploads of firmware.

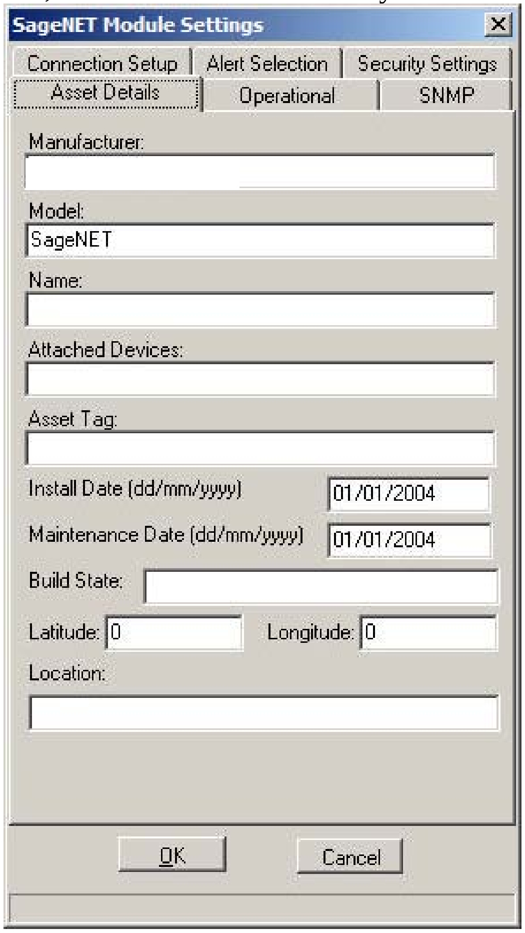
4 OPERATION

Several parameter windows have been mentioned in the previous sections where system-operating parameters are displayed and able to be edited. Each time a parameter is modified, it is highlighted in yellow and will be reset to white when the *Write to* function is used within the parameters window. The parameter windows and the function of their listed parameters are described in this section.

4.1 SAGENET MODULE PARAMETERS WINDOW

4.1.1 Asset Details Tab

The asset details tab provides the ability to change any details that may be required by your to assist with asset tracking. The asset tracking details are reported via SNMP, and allow your to discover information about the unit, such as it's physical location, that can be accessed directly via the unit, and no external source.



Manufacturer:

Model: SageNET

Name:

Attached Devices:

Asset Tag:

Install Date (dd/mm/yyyy) 01/01/2004

Maintenance Date (dd/mm/yyyy) 01/01/2004

Build State:

Latitude: 0 Longitude: 0

Location:

4.1.2 Manufacturer

This is the manufacturer of the SageNET Unit. It corresponds to the manufacturer variable in the SNMP MIB, allowing you to configure each SageNET unit's manufacturer name.

4.1.3 Model

The model corresponds to the model type of the SageNET unit. Typically, this will be SageNET, however this may change for your unit, if you wish to rename the model.

4.1.4 Name

The name of the system in your power network may be stored here, for usage in the SageNET SNMP MIB.

4.1.5 Attached Devices

This is the area where you may describe any attached devices for reporting via SNMP. For instance, you may wish to show that it is a system equipped with a Site Monitor or Battery Monitor, or note how many rectifiers are installed.

4.1.6 Asset Tag

The asset tag area is a place to keep track of the asset tag of the SageNET unit. It may be up to 15 alphanumeric characters.

4.1.7 Install Date

The install date allows you to keep track of when the power system or SageNET unit was installed.

4.1.8 Maintenance Date

The Maintenance date allows you to keep track of the last time any maintenance was performed on the SageNET unit, or on the power supplies.

4.1.9 Build State

The build state allows you to describe what release version and patches that have been uploaded to the SageNET module.

4.1.10 Latitude/Longitude

The Latitude and Longitude sections allow you to keep track of the co-ordinates of the system, for mapping to a larger system. These values are presented in GPS format, and to convert to degrees, need you need to follow the following instructions:

For Latitude:

Latitude in Degrees = (gpsLatitude * 90) / ((2^31)-1)

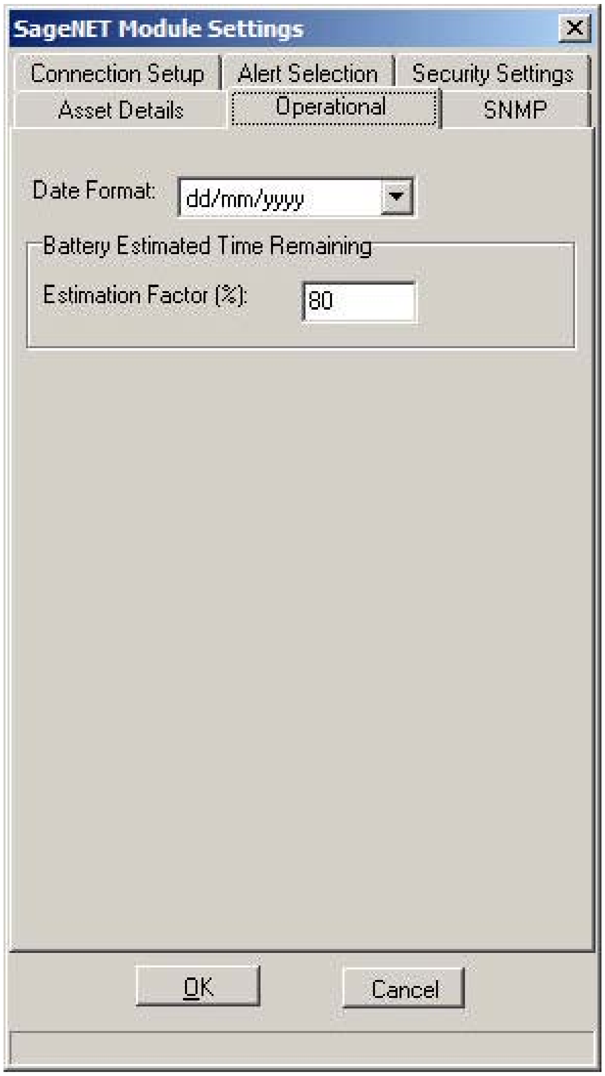
For Longitude:

Longitude in Degrees = (gpsLongitude * 180) / ((2^31)-1)

4.1.11 Location

Location allows you to describe where to module or power supply is situated. This could be an address, or an office, etc.

4.1.12 Operation Tab



Date Format: dd/mm/yyyy

Battery Estimated Time Remaining

Estimation Factor (%): 80

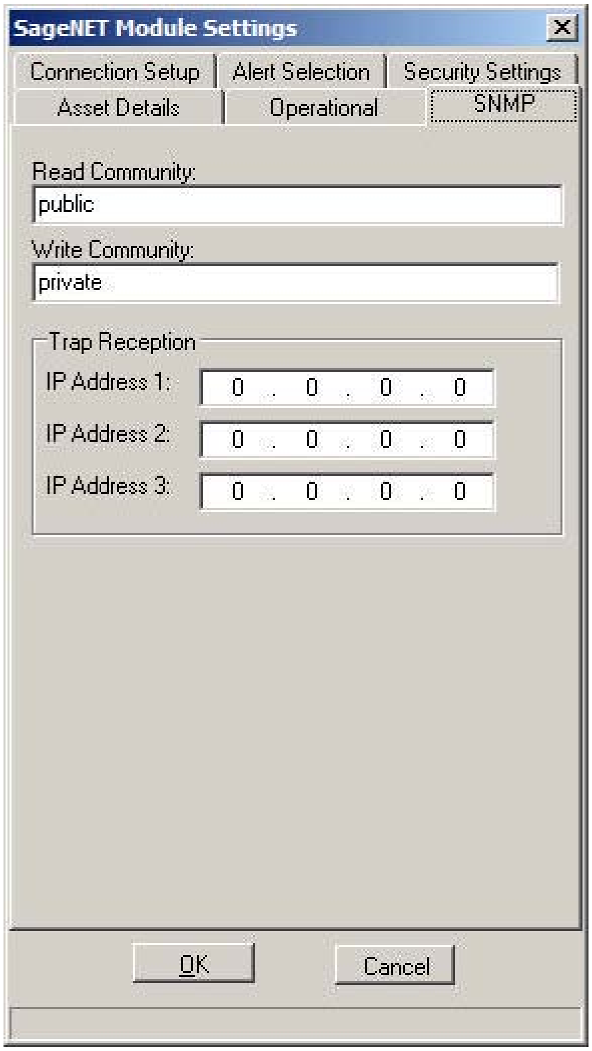
4.1.12.1 Date Format

The Date Format allows you to select how the date should be displayed for the SageNET module.

4.1.12.2 Estimation Factor

The Estimation Factor is a percentage operator. It can be used to adjust how correct the battery time remaining estimates calculated is. For instance, if there is 20 minutes battery charge remaining, the estimation factor will allow you to reduce, that to 15 minutes by changing it to 75%. This allows you to ensure that there is error allowed for in the estimated time remaining.

4.1.12.3 SNMP Tab



Read Community: public

Write Community: private

Trap Reception

IP Address 1: 0 . 0 . 0 . 0

IP Address 2: 0 . 0 . 0 . 0

IP Address 3: 0 . 0 . 0 . 0

4.1.12.4 Read Community

The read community allows you to set the SNMP read community name. This community name is used by SNMP monitoring software, to access the SNMP variables. As a default, this value is set to public.

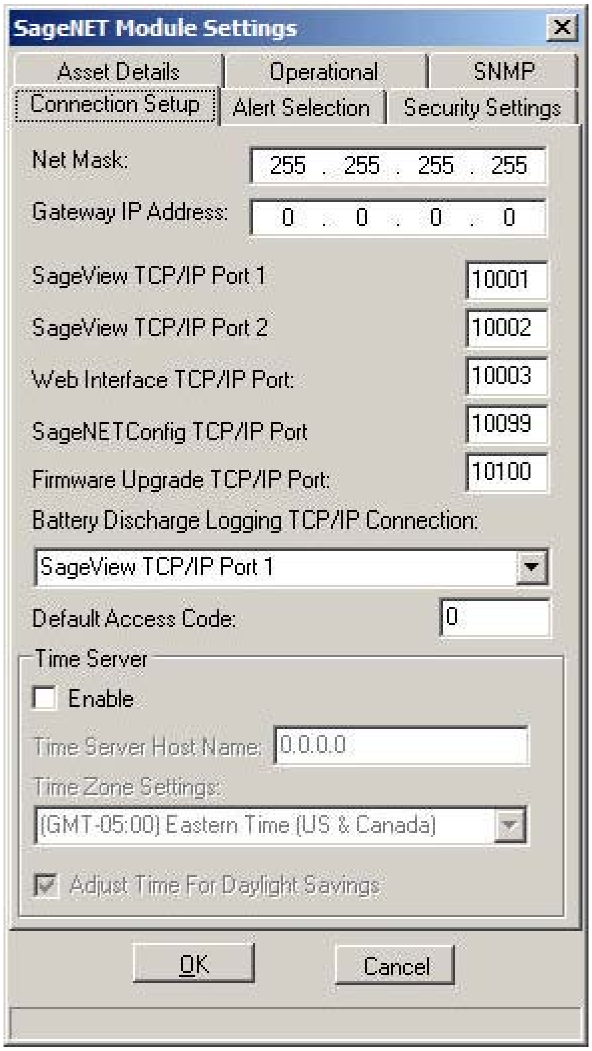
4.1.12.5 Write Community

The write community gives access to change the SNMP write community. Once again, it is used in SNMP monitoring software, to allow access to variables to be set. Since SageNET does not implement any writing of parameters, this community value is not used in this release.

4.1.12.6 *Trap Reception Section*

The trap reception section is where you can configure what IP addresses the traps for system should be sent to.

4.1.13 Connection Setup



Net Mask: 255 . 255 . 255 . 255

Gateway IP Address: 0 . 0 . 0 . 0

SageView TCP/IP Port 1: 10001

SageView TCP/IP Port 2: 10002

Web Interface TCP/IP Port: 10003

SageNETConfig TCP/IP Port: 10099

Firmware Upgrade TCP/IP Port: 10100

Battery Discharge Logging TCP/IP Connection: SageView TCP/IP Port 1

Default Access Code: 0

Time Server

□ Enable

Time Server Host Name: 0.0.0.0

Time Zone Settings: (GMT-05:00) Eastern Time (US & Canada)

☑ Adjust Time For Daylight Savings

4.1.13.1 Net Mask

The net mask is used by the network device to determine what computers/network devices are on the same subnet. This allows the SageNET module to determine what packets need to be sent to the gateway, and what packets can be directly addressed.

4.1.13.2 Gateway IP Address

A gateway device is used to route packets between two networks, for instance, the LAN and the Internet. The IP address of this device is important when a SageNET unit will be sending packets to computers or devices that are not on the same subnet as the unit.

4.1.13.3 SageView TCP/IP Port 1 & 2

The SageView TCP/IP port settings allow you to configure which ports the SageNET should listen for a connection from the SageView program on. These are configurable, so that you can set these to match ports that can be opened on any firewall(s) between the SageNET module and the monitoring PC. At the present time, SageView only supports communications on port 10001, so it is recommended that you leave these port numbers unchanged.

4.1.13.4 Web Interface TCP/IP Port

The SageNET's web page uses an embedded Java applet to monitor the power systems information. This connects to the SageNET unit via a specified TCP port (similar to the SageView connection). Once again, this is configurable, to allow easy port opening on any firewalls.

4.1.13.5 SageNET Configuration Tool TCP/IP Port

This port allows you to change what port the configuration tool should connect to the next time it connects to the SageNET module. This is configurable, to allow for firewalls.

4.1.13.6 Firmware Upgrade TCP/IP Port

The firmware upgrade port describes which port will be utilized to remotely upgrade the firmware of the SCU/MicroCSU unit. It may need to be changed, depending on the firewall settings.

4.1.13.7 Battery Discharge Logging TCP/IP Connection

The Battery Discharge Logging TCP/IP connection describes which SageView port will be used to report any discharge logs. Since SageView presently only supports communications on port 10001, this setting should be left at its default value (TCP/IP Port 1).

4.1.13.8 Default Access Code

To provide security for remote access to the Sageon Control Unit (plant controller), a unique access code may be entered into the plant controller. This code defaults to 000000 from the factory . If the access code for the power plant has been changed from the factor default, it should be entered here so that SageNET may gain remote access to the SCU.

4.1.14 Time Server

The time server details allow you to set the SageNET unit to use either a local SNTP time server, or a world SNTP time server.

4.1.14.1 Enabled

The first option is whether the SNTP protocol will be used. If it is not enabled, the SCU will use the time that it currently has, until it is updated by SageView. If it is enabled, the SNTP client running on the SageNET module will update the SCU time on boot up and every 24 hours thereafter.

4.1.14.2 Time Server Host Name / IP Address

The time server host name or IP address should be set with care. If an incorrect time server is given, the SNTP lookup will fail, and the time will not be updated on the SCU.

IMPORTANT NOTE

> When you insert a host name in this section, upon closing the Module settings dialog box, the host name is resolved to an IP address. The IP address is then saved, not the host name. If the host name changes IP address, there may be an address resolution problem later.

4.1.14.3 Time Zone Settings

The time zone settings describe what time zone the SageNET unit should use.

4.1.14.4 Adjust Time for Daylight Savings

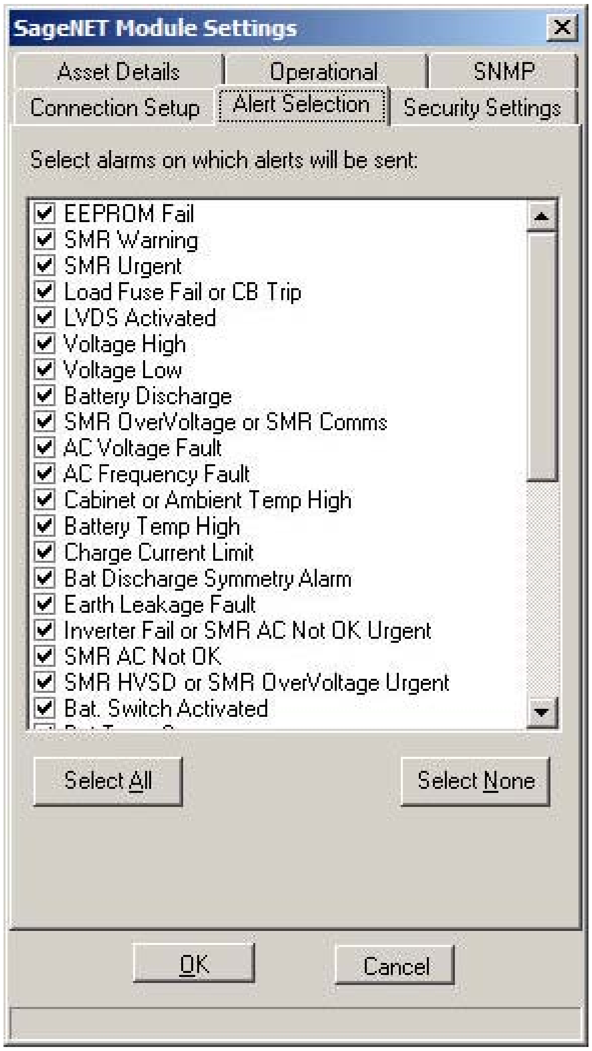
If you want to the unit to use daylight savings time for the local time zone, you need to check this option. Otherwise, the standard time zone information will be used.

NOTE

The unit WILL NOT automatically update for daylight savings.

4.1.14.5 Alert Selection Section

The alert selection section allows you to choose which of the available alarms will be reported via SNMP traps. If the alarm is unselected, it will still be available via the alarm logs of the SNMP monitoring and the SageView monitoring, but it will not have an SNMP trap generated for it.



Select alarms on which alerts will be sent:

- ☑ EEPROM Fail
- ☑ SMR Warning
- ☑ SMR Urgent
- ☑ Load Fuse Fail or CB Trip
- ☑ LVDS Activated
- ☑ Voltage High
- ☑ Voltage Low
- ☑ Battery Discharge
- ☑ SMR OverVoltage or SMR Comms
- ☑ AC Voltage Fault
- ☑ AC Frequency Fault
- ☑ Cabinet or Ambient Temp High
- ☑ Battery Temp High
- ☑ Charge Current Limit
- ☑ Bat Discharge Symmetry Alarm
- ☑ Earth Leakage Fault
- ☑ Inverter Fail or SMR AC Not OK Urgent
- ☑ SMR AC Not OK
- ☑ SMR HVSD or SMR OverVoltage Urgent
- ☑ Bat. Switch Activated

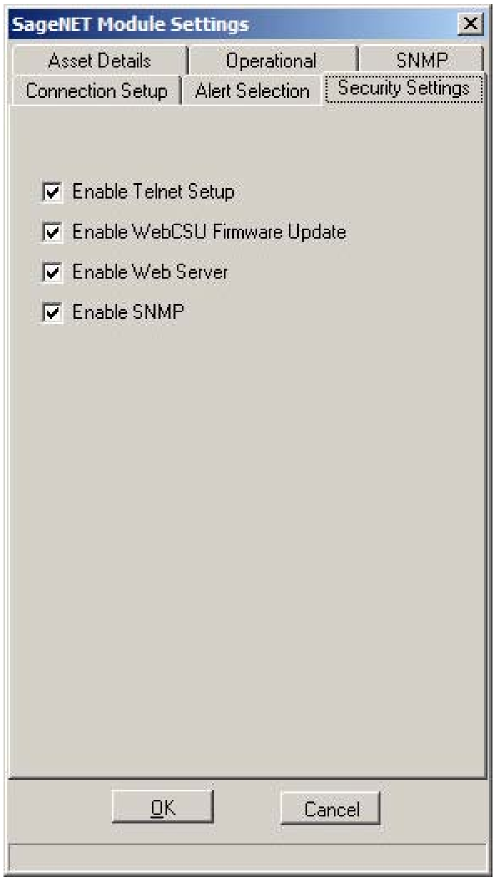
4.1.14.6 Select All

The select all button will quickly select all of the alarms to be reported.

4.1.14.7 Select None

The select none button will quickly remove all alarms from reporting.

4.1.15 Security Settings



☑ Enable Telnet Setup

☑ Enable WebCSU Firmware Update

☑ Enable Web Server

☑ Enable SNMP

4.1.15.1 Enable Telnet Setup

Enable Telnet Setup allows you to enable or disable the ability to establish a telnet connection with the unit. The telnet connection is a method of changing some basic parameters, such as the configuration port and the IP address of the unit.

4.1.15.2 Enable SageNET Firmware Update

Enable SageNET Firmware Update allows you to disable or enable the ability to update the SageNET firmware.

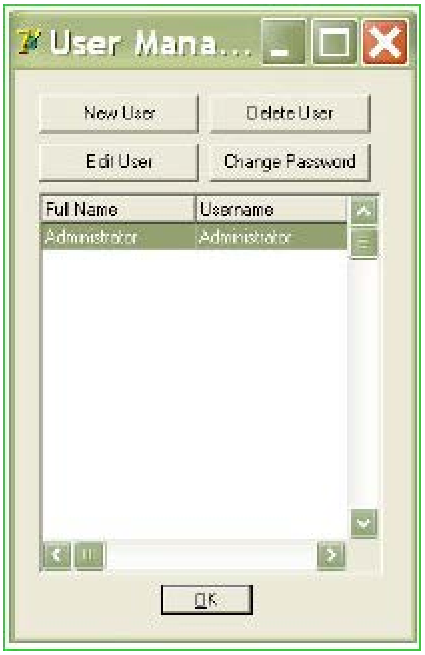
4.1.15.3 Enable Web Server

The web server may be shut down using this option. This will stop any users from accessing the SageNET web page, and monitoring without any security.

4.1.15.4 Enable SNMP

You can shut down the SNMP traps and monitoring ports using this option.

4.2 USER MANAGEMENT WINDOW



Full Name	Username
Administrator	Administrator

The user management window is used to maintain the users allowed to access the configuration tool. After the initial installation of the program, it is highly recommended that you change the administrator password from the default.

Any changes made to the users database is automatically logged in the system event logs, and if configured, is logged using the syslog protocol, to the set up syslog server.

4.2.1 Full Name

The full name of the user is inserted here.

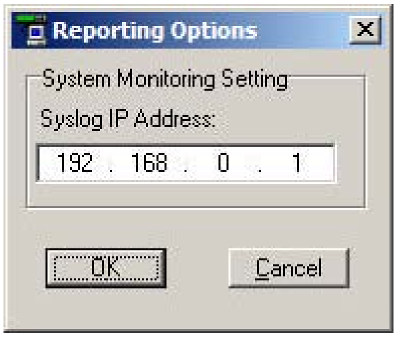
4.2.2 User Name

The name of the user who will log into the configuration tool.

4.2.3 Password / Confirmation Password

You need to type the user’s password into these sections to set the password for the user.

4.3 REPORTING OPTIONS



Syslog IP Address: 192 . 168 . 0 . 1

You may insert the IP address of a computer that runs a syslog daemon here. This allows you to monitor changes made to SageNET configurations, and your management of the configuration software from a remote computer.

5 SNMP

5.1 SNMP MIB STRUCTURE

The SNMP MIB has a tree structure to group and describe the variables available to you.

5.1.1 psIdent

The psIdent section contains all the system identification fields. These are all the fields that pertain to the asset management of the SageNET module.

5.1.2 csuStatus

The csuStatus section contains the current status of the controller, and overall system. These fields are information about the system voltage, the total load current, and information about the incoming mains power.

It also contains a table, describing the status of the batteries. This table will always contain four rows, but the validity of the rows is dependant on the csNumBats variable, as this tells us how many batteries there are.

The table contains the following information:

- Battery number
- Battery current
- The estimated battery charge remaining
- The estimated battery time remaining (*NOTE: This only provides a crude indication of battery time remaining and its reliability is heavily reliant on the data your provides. The Battery Rating and the Estimation Battery Time Remaining Factor are key pieces of information that your provides).*

NOTE: The table always contains 4 rows; the relevancy of the data is dependant upon the number of batteries in the system.

5.1.3 csuTest

The csuTest section holds the information about the last battery discharge test. It holds information about the time and date, length, and result of the battery discharge test.

This section also contains a table that holds the estimated battery charge remaining after the completion of the battery discharge test.

5.1.4 csuSysConfig

The csuSysConfig holds the information about the configuration of the controller, which includes the options the controller has been configured with. This is presented as a table, which lists all configuration settings as SNMP objects in the range from scSysConfigSiteMonitor to scSysConfigTemperatureUnitFahrenheit.

5.1.5 csuParam

csuParam holds all the information about the controller parameters. All values are read only, and include such parameters as, number of rectifiers, number of batteries, AC voltage high and low alarms settings.

5.1.6 csuAlarmLog

The csuAlarmLog section holds the information of all currently active controller alarms. It does so using a table, with links to identity nodes. The first readable variable is alLogSize, which contains the number of active alarms, and also csuAlarmLogTable, which contains four sub-sections to be filled:

- The log index;
- The alarm code;
- The descriptions as SNMP objects in the range from alAlarmEEPROMFail to alAlarmLogAlarm7Bit7;

and

- The time the alarm was set.

NOTE: The alarm time is the point in time the alarm was triggered, relative to the uptime of the module. This is not the SNTP synchronised time, but the value in seconds that the module has been powered up for.

5.1.7 smrStatus

smrStatus contains information about the status of all the rectifiers in the power system. It contains the information for each rectifier, and the overall alarm log for the rectifiers. Both of these are presented in tables. Each line of the table for the status information includes:

- Rectifier index;
- Rectifier number for the entry;
- Rectifier current being used;
- Rectifier float voltage;
- Rectifier heat sink temperature; and
- Number of alarms active in the rectifier.

The alarm log table has 3 fields:

- The Alarm log index for the table;
- The Rectifier number that each arlarm corresponds to; and
- The Rectifier alarm description as SNMP objects in the range from ssAlarmOutputVoltHigh to ssAlarmRectifierIoutHighResFlag.

5.1.8 smrParam

smrParam contains information about the parameters of the rectifiers connected to the system.

5.1.9 cellVoltages

The cellVoltages section all the battery information is reported via variables and a table. The overall system information, such as Cell Voltage High alarm, and configuration information are all leaves of the cellVoltages branch.

Actual cell voltage information for each cell in the system is reported as a table including:

- The block index;
- The battery number;
- The block number;
- The cell voltage.

5.1.10 siteMonitorStatus

siteMonitorStatus covers all the site monitor status information for the power system. It reports back:

- Site Monitor analog channels current status table size;
- A table that contains:
  - Site Monitor analog channel number;
  - Site Monitor analog channel current value;

- Site Monitor digital channels current values table size;
- A table that contains:
  - Site Monitor digital channel number;
  - Site Monitor digital channel current value;
- The status of Site Monitor Output Relay control 1 to 4;

- The Site Monitor Alarm Log Size;
- A table for the Site Monitor Alarm Log containing:
  - Site Monitor alarm index;
  - Site Monitor alarm code;

- Site Monitor alarm description as SNMP objects in the range from smsSMAlarmAnalogChan1 to smsSMAlarmDigitChan12.

5.1.11 siteMonitorParam

The siteMonitorParam branch contains the set-up and configuration information for the site monitor peripherals. It includes the following information:

- Site Monitor Enabled;
- Site Monitor Analog Parameters Size;
- A table to describe the site monitor analog parameters, containing:
  - Site Monitor analog channel number;
  - Site Monitor analog channel alarm enable;
  - Site Monitor analog channel full scale rating;
  - Site Monitor analog channel upper alarm threshold;
  - Site Monitor analog channel lower alarm threshold;
  - Site Monitor user description label for this analog channel;
  - Site Monitor unit label for this analog channel;
  - Site Monitor output relay control 1 to 4 for this analog channel;
- Site Monitor digital channel parameter values table size;
- A table of the Site Monitor digital channel parameters, containing:
  - Site Monitor digital channel number;
  - Site Monitor digital channel alarm enable;
  - Site Monitor user description label for this digital channel;
  - Site Monitor normal state for this digital channel;
  - Site Monitor output relay control 1 to 4 set-up for this digital channel.

5.1.12 csuTraps

SageNET implements 6 traps, which notify a NMS of alarms in the power system. An explanation of each of these traps is detailed below.

5.1.12.1 csuTrapOnBattery

This trap is a notification that the system is operating on battery power. This trap is persistent and is resent at one minute intervals until either the batteries are discharged or the system is no longer running on battery. It reports the number of batteries present in the system (up to 4) and the charge remaining for all 4 possible batteries. The charge remaining for non-existent batteries should be ignored.

5.1.12.2 csuTrapOnBDTCompleted

This trap is a notification that a Battery Discharge Test has been completed. It reports the test results as an integer (see ctLastDischargeTestResult variable):

1. ldtFailed(1)
2. ldtPassed(2)
3. ldtNotAvailable(3)
4. ldtLowLoad(4)
5. ldtRectifierOverload(5)
6. ldtNoControl(6)

7. ldtUserTerminated(7)
8. ldtACLost(8)
9. ldtCellVoltageLow(9)
10. ldtBatteryCTFailed(10)
11. ldtUnknown(11)

5.1.12.3 csuTrapAlarmLogEntryAdded

This trap is a notification that an alarm has been inserted into the alarm table (see csuAlarmLog variable). It reports the alarm code and description as an SNMP object in the range from alAlarmEEPROMFail to alAlarmLogAlarm7Bit7. Only the alarms selected by your using the configuration tool are reported.

5.1.12.4 csuTrapAlarmLogEntryRemoved

This trap is a notification that an alarm has been removed from the alarm table (see csuAlarmLog variable). It reports the alarm code and description as an SNMP object in the range from alAlarmEEPROMFail to alAlarmLogAlarm7Bit7.

5.1.12.5 csuTrapCSUParameterChange

This trap is a notification that a SCU parameter has been changed from the front panel. It reports 2 variables that are current not used cpCSUParameterUserName and cpCSUParameterChangedDesc.

5.1.12.6 csuTrapCSUOffline

This trap is a notification that the SNMP interface has lost contact with the SCU (power system monitoring unit). This trap is persistent and is resent at one-minute intervals until communications has been restored.

NOTE: SageNET implements SNMPv1 traps.

5.1.13 Release

The release branch contains all the current release information of the SNMP MIB tree. It contains contact information and version information of the MIB.

6 SNTP

The SNTP server allows the SageNET module to automatically calibrate the controller’s time according to an extremely accurate Internet time source, (see http://www.ntp.org/ for listings of some time servers, and more information about the NTP protocol). When the time server is enabled, and the host name or IP address in the configuration tool (see ….), is set up to point to an internet time server, the SageNET module will get an update of the UTC time on boot-up and every 24 hours thereafter, which is used to update the SCU internal clock.

7 SAGEVIEW CONNECTIVITY

SageNET allows you to connect 2 copies of SageView to each SCU. The ports that SageView connect to are configurable via the configuration tool’s connection options. Default ports are 10001 and 10002.

***** Note ***

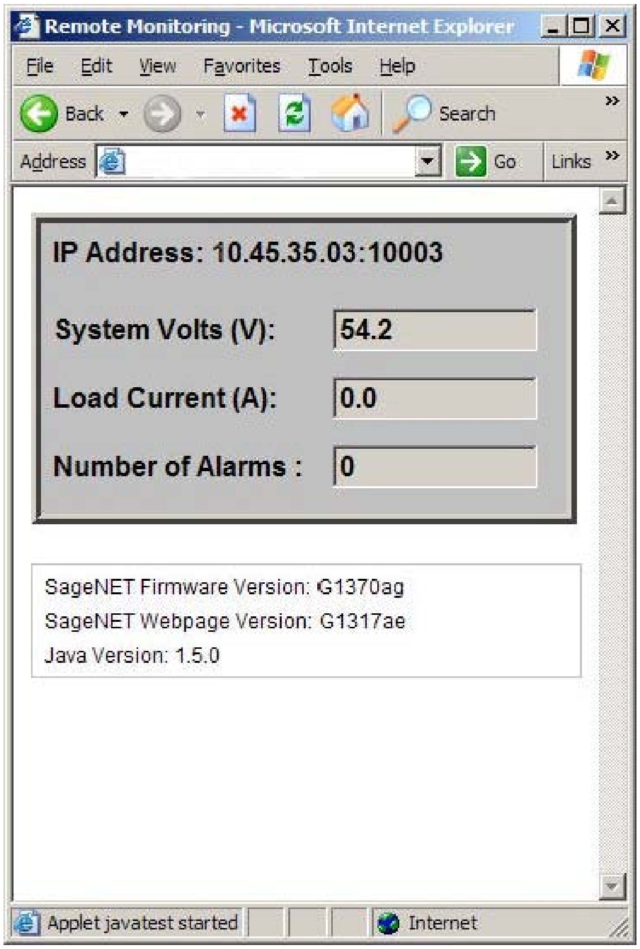
> *The Sageon Power Systems supports concurrent access via the front panel serial port and the network port (i.e. SageNET). Since SageNET can support two simultaneous connections, it is theoretically possible for three users to be accessing the Sageon plant at the same time. The possibility exists that all three users may try changing the Sageon’s configuration at the same time, to prevent possible corruption of configuration information that may be caused by such a simultaneous change, the Sageon Plant Controller employs a write-lockout feature.*
>
> *When the first attempt is made to change the Sageon’s configuration via Sagenet, the Sagenet connection*

making the change is awarded Write-Access privileges. Once this occurs, this connection is the only one that can make configuration changes, the other connections will receive a busy message if they attempt to change configuration. When the connection with Write-Access privileges is done making changes, it must log off (i.e. disconnect SageView from the power plant). When the connection is disconnected, the Write-Access privilege is cancelled after 20 seconds. At this time, any other connection (including a new SageView connection on the same port) can gain Write-Access.

8 WEB INTERFACE

The web interface may be accessed via the web address: http://<ip-address-of-module>/ .

It requires the Java Runtime engine (plug-in) be installed on the browers system and be allowed to run. It also requires the Web Interface port be open on any firewall between the 2 systems. Please see your network administrator for help with these requirements.


Remote Monitoring - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Address
Go
Links
Applet javatest started
Internet

IP Address: 10.45.35.03:10003

System Volts (V): 54.2

Load Current (A): 0.0

Number of Alarms : 0

SageNET Firmware Version: G1370ag
SageNET Webpage Version: G1317ae
Java Version: 1.5.0

The web page has 2 main sections. The first (in grey), includes all the status information, read from the SageNET module. It shows the system voltage, the load current and the number of alarms. This is updated every 5 seconds.

The second section shows all of the version information from the SageNET unit, and the Java version information.

Important Note: Certain Internet Security programs which implement software firewalls (such as McAfee Security Center and Norton Person Firewall) may prevent the Java applet from loading the Webpage and

Firmware Versions. If you see <NotDetected> for these values, please check your computer for such software and disable it while accessing SageNET.

9 TELNET

SageNET provides telnet capability, to control the basic parameters of the system. You can access the telnet system by typing:

```
telnet <ip-address-of-unit> 9999
```

You will then be asked to 'Press Enter to go into Setup Mode'

If you press Enter, you will be presented with a menu. This menu will contain 3 options.

- Server Configuration
- Exit without save
- Save and Exit

9.1 SERVER CONFIGURATION (NETWORK CONFIGURATION)

The server configuration section allows you to change many of the basic network settings of the SageNET unit including,

- IP Address
- Gateway Address
- Net Mask
- Configuration Port
- Refresh Rate

9.1.1 IP Address

The IP address must be set to a unique value in your network. See Appendix A for more information about IP Addressing.

Note: *SageNET module cannot connect to the network if the assigned IP address is already in use by another device.*

9.1.2 Gateway Address

The gateway address, or router, allows communication to other LAN segments. The gateway address should be the IP address of the router connected to the same LAN segment as the *SageNET module*.

Note: *The gateway address must be within the local network segment.*

9.1.3 Net Mask

A netmask defines the number of bits taken from the IP address that are assigned for the host section.

Note: *Class A: 24 bits; Class B: 16 bits; Class C: 8 bits.*

The *SageNET module* prompts for the number of host bits to be entered then calculates the netmask, which is displayed in standard decimal-dot notation when the saved parameters are displayed (for example, 255.255.255.0).

9.1.4 Configuration Port

This is the port that the configuration tool will talk to.

9.1.5 Refresh Rate

The refresh rate is how often the SageNET module will update the data it stores from the SCU or MicroCSU. This is measured in milliseconds.   The default value is 5 seconds (i.e. 5000 ms), but the minimum value is 150ms.

9.2 EXIT WITHOUT SAVE

The Exit without save option allows you to discard any changes you've made while logged into the telnet interface.

9.3 SAVE AND EXIT

Save and exit saves any changes made in the telnet interface, and then reset's the unit, forcing a reloading of the configuration. This means all changes are stored, and reloaded for immediate use.

10 TCP/IP PORTS

The SageNET uses the following TCP/IP ports for its communications interfaces:

PORT	PROTOCOL
TCP Port 80	HTTP
TCP Port 9999	Telnet, non-standard port
TCP Port 1	Telnet, non-standard port
TCP Port 10001*	SageView software
TCP Port 10002*	SageView software (secondary connection)
TCP Port 10003*	Java applet embedded in SageNet
TCP Port 10099*	SageNETConfig access to SageNET
TCP Port 10100*	SageNETConfig firmware update of SageNet
TCP Port 37	Time server
TCP Port 161	SNMP
TCP Port 162	SNMP
UDP Port 162	SNMP

Note: *Ports marked with an asterisk may be re-configurable using the SageNET Configuration Program should a port conflict be encountered.*

In order for a computer to access the SageNET remotely, any networking equipment (routers, firewalls, proxy servers, etc.) between the two must configured to pass data on the appropriate TCP/IP port. If the SageNET can be accessed via web brower (HTTP is the most univeral TCP/IP protocol) but fails for one of the other protocols, then you should suspect a firewall or proxy server blocking TCP/IP prots to be the cause.

11 SAGENET QUICK START GUIDE

11.1 MATERIALS REQUIRED

- SageNET board and installation CD
- Computer running Windows 98 or higher operating system
- CAT5 network cable for SageNET connection to your network
- #1 Phillips Screwdriver

11.2 ADVANCE PREPARATIONS

Verify the SCU (plant controller) in your Sageon Power System is equipped with revision .3 or higher software. This may be verified by scrolling through the front panel menus on the controller and selecting the 'Test Indicators' function. This function will flash the revision level of the software. If the revision displayed ends in '.3' or higher, the SCU is acceptable for use with a SageNET.

You will need the following network information to configure the SageNET.

- Static IP Address for SageNET
- Subnet Mask
- IP Address of network gateway
- IP Address of SNMP Monitoring (to receive SNMP traps)
- IP Address of SNTP time server (optional)
- IP Address of system log server (optional)
- MAC address from label on SageNET board

A configuration check sheet for recording these values is included at the end of the User's Manual.

If your computer does not have Sun Java loaded, please install Java from the SageNET installation CD.

You may configure the IP address of the SageNET by using the ARP & Telnet protocol tools available from Windows or by using the XPORT configuration tool. Details of both procedures may be found in section 2.1.1 of the SageNET Manual. If you choose to use the XPORT configuration tool, it must be installed from the SageNET installation CD.

To configure the IP address of the SageNET device, the computer being used must be on the same physical network segment. This means that there should be no network segmenting equipment between the two devices (such as firewalls, gateways or filtering routers).

If the SageNET device is to be accessed from another network segment (for monitoring or remote programming), certain TCP/IP ports must be accessible from the other network segment. In many installations only the commonly used TCP/IP prots such as HTTP, FTP, POP3, etc. are allowed to pass through the network segmenting equipment. It may be necessary to configure the netowrk segmenting equipment to pass the unique TCP/IP ports required by SageNET. A more detailed discussion of TCP/IP ports may be found in section 2.3 of the SageNET Manual.

11.3 SAGENET INSTALLATION OVERVIEW

- Confirm firmware revision level of Sageon Plant Controller.
- Install SageNET board and connect Ethernet cable.
- Using ARP/Telnet or XPORT Configuration Tool, configure the IP address, subnet
- mask and gateway for the SageNET board.
- Using the SageNET Configuration Program, configure the IP address, subnet mask, gateway and network monitoring system.

- Test access to SageNET by directing a web browser to http://<ip-address-ofmodule>/. The SageNET status summary web page should be seen.

Note:
Due to the compact size of the XPORT connector on the SageNET board, it is necessary to use an Ethernet cable constructed with premium quality RJ45 connectors. Poor connections have been observed when using cables constructed from discount or generic RJ45 connectors. Brand name connectors such as those from AMP� will assure proper operation of your SageNET.

If you are experiencing problems with your SageNET board when it is properly installed, please check the link status LEDs on the RJ45 connector. If no LEDs are illuminated, a poor cable connection should be investigated.

11.4 SAGENET SETUP DATA WORKSHEET

Name of Installation:

____

SageNET MAC Number:

_00 - _20 - _4a - ___ - ___ - ___ (ex: 00-20-4a-xx-xx-xx)

SageNET Static IP:

_____ . _____ . _____ . _____ (ex: 192.168.0.11)

SageNET Network Mask:

_____ . _____ . _____ . _____ (ex: 255.255.0.0)

SageNET Network Gateway:

_____ . _____ . _____ . _____ (ex: 192.168.0.1)

Network Monitoring System: (where to send SNMP traps)

_____ . _____ . _____ . _____ (ex: 192.168.0.121)

Network Time Server: (optional)

_____ . _____ . _____ . _____ (ex: 192.168.0.209)

12 PRODUCT SUPPORT

Product support can be obtained using the following addresses and telephone numbers.

Corporate office:
UNIPOWER, LLC
210 N University Dr
Coral Springs, FL 33071
United States

Manufacturing facility:
UNIPOWER, LLC
65 Industrial Park Rd
Dunlap, TN 37327
United States

Manufacturing facility:
UNIPOWER Slovakia SRO
ZLATOVSKA 1279
Business Center 22
91105 Trencin, Slovakia

Phone: +1-954-346-2442
Toll Free: 1-800-440-3504
Web site – www.unipowerco.com

When contacting UNIPOWER, please be prepared to provide:

1. The product model number, spec number, S build number, and serial number - see the equipment nameplate on the front panel
2. Your company’s name and address
3. Your name and title
4. The reason for the contact
5. If there is a problem with product operation:
    - Is the problem intermittent or continuous?
    - What revision is the firmware?
    - What actions were being performed prior to the appearance of the problem?
    - What actions have been taken since the problem occurred?