Network Monitoring System

Gutor PxW

User Guide

With the network management card AP9635 with AOS v6.8.2 and APP v6.8.0
12/2019 Version 1

www.schneider-electric.com

Legal Information

As standards, specifications, and designs change from time to time, information contained in this guide may be subject to change without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this material or consequences arising out of or resulting from the use of the information contained herein.

Table of Contents

Safety Information

Read these instructions carefully and look at the equipment to become familiar with it before trying to install, operate, service or maintain it. The following safety messages may appear throughout this manual or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

IMPORTANT: Save the safety information for future reference.

⚡ The addition of this symbol to a “Danger” or “Warning” safety message indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

⚠ This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages with this symbol to avoid possible injury or death.

⚠DANGER

DANGER indicates a hazardous situation which, if not avoided, will result in death or serious injury.

Failure to follow these instructions will result in death or serious injury.

⚠WARNING

WARNING indicates a hazardous situation which, if not avoided, could result in death or serious injury.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

⚠CAUTION

CAUTION indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

Failure to follow these instructions can result in injury or equipment damage.

NOTICE

NOTICE is used to address practices not related to physical injury. The safety alert symbol shall not be used with this type of safety message.

Failure to follow these instructions can result in equipment damage.

Please Note

Electrical equipment should only be installed, operated, serviced, and maintained by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction, installation, and operation of electrical equipment and has received safety training to recognize and avoid the hazards involved.

Safety Precautions for the Network Management System

⚠⚠DANGER

HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH

- All safety information in this document must be read, understood and followed.
- Always use appropriate personal protective equipment (PPE).
- Hazardous voltages are present as soon as the cabinet door is opened. Only qualified electrical personnel are allowed to open the cabinet.
- Turn off all power supplying the system before connecting any cables to or between the network management system inside the cabinet.
- Always use isolated tools when removing the protection covers inside the cabinet (metal sheets and plastic covers).
- Replace all protective covers and close all doors before turning on power to the system.

Failure to follow these instructions will result in death or serious injury.

⚠WARNING

INACCURATE DATA RESULTS

- Do not use data displayed from the network management card (NMC) as a substitute for proper workplace practices or equipment maintenance.
- Always confirm that any active alarms from the NMC is also active on the system.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

⚠WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Always change the default passwords to help prevent unauthorized access.
- Disable unused network access option and accounts to minimize pathways for malicious attacks.
- Use multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection).
- Use cyber security best practices (for example: least privilege, separation of duties) to help prevent unauthorized exposure, loss, modification of data and logs, interruption of services, or unintended operation.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

NOTICE

LOSS OF OPERATION

When updating the firmware on the network management card (NMC) always ensure that the modules are updated in the correct order:

- First the boot monitor (BM)
- Then the APC operating system (AOS)
- Last the application module (APP)

Failure to follow these instructions can result in equipment damage.

NOTICE

DATA LOSS

When a hard reset is done (by pressing the reset button for a long time) on the network management card (NMC) all network configurations and user settings are reset to the default factory settings, also all logs and event lists are erased.

Failure to follow these instructions can result in equipment damage.

General Information

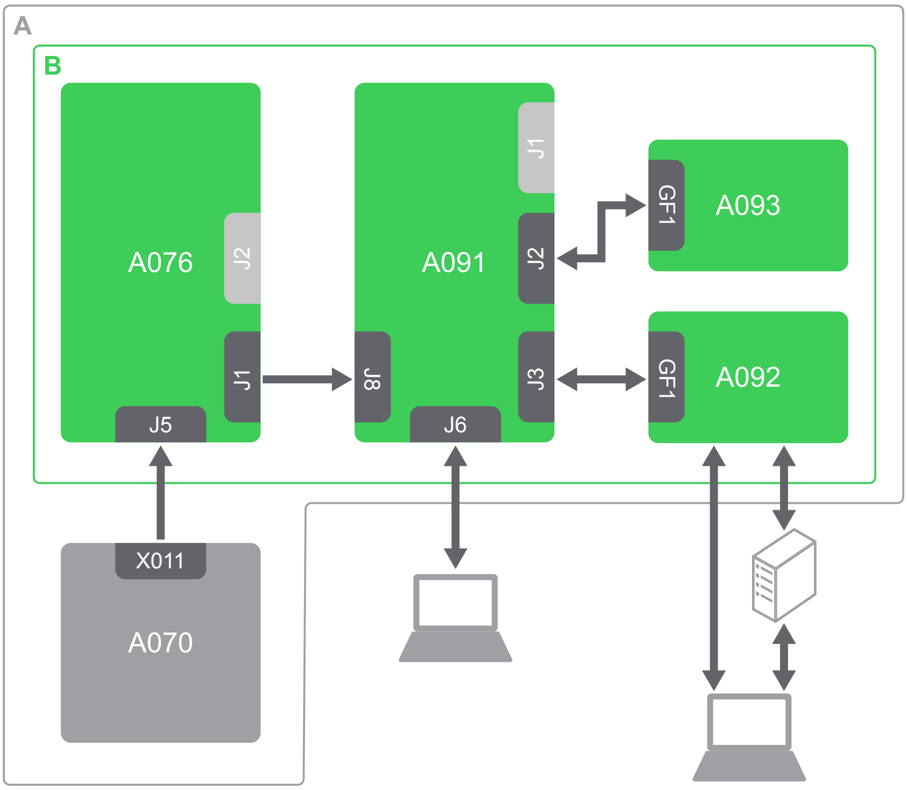
This user guide provides information about the network management system in Gutor systems.

In this manual “the system” refers to the complete single, redundant or dual system, and “the unit” refers to one of the units in a redundant or dual system. Also “the cabinet” refers to the mechanical frame of the system or unit.

NOTE: Always dispose of any waste in accordance with local regulations and rules.

Network Monitoring System Overview

The network monitoring system in Gutor UPSs provides the possibility to obtain readings, measurements, events and logs via a secure one-way communication from the controller board.



NOTE: The light grey ports are not connected.

Network Monitoring System Parts

Part	Name	Description
(A)	The UPS	Inside the system.
(B)	The network monitoring system	The parts of the network monitoring system placed in the low voltage section.
A070	Controller board	The controller board sends information and status changes in the system to the communication interface.
A076	Communication interface	Extends the signal from the controller board and to the smart slot translator.
A091	Smart slot translator	Converts the signal from the controller board to another type of protocol. Allows for local connection to the NMC.

Network Monitoring System Parts (Continued)

Part	Name	Description
A092	Network management card (NMC)	Offers secure local and/or remote monitoring of Gutor systems.
A093	Options slot	An additional slot for an optional second NMC card that can be used for: • Additional available ports with two NMCs. • A second NMC with different settings. • Redundant network communication. • Two digital inputs.

Hardware of the Network Management System

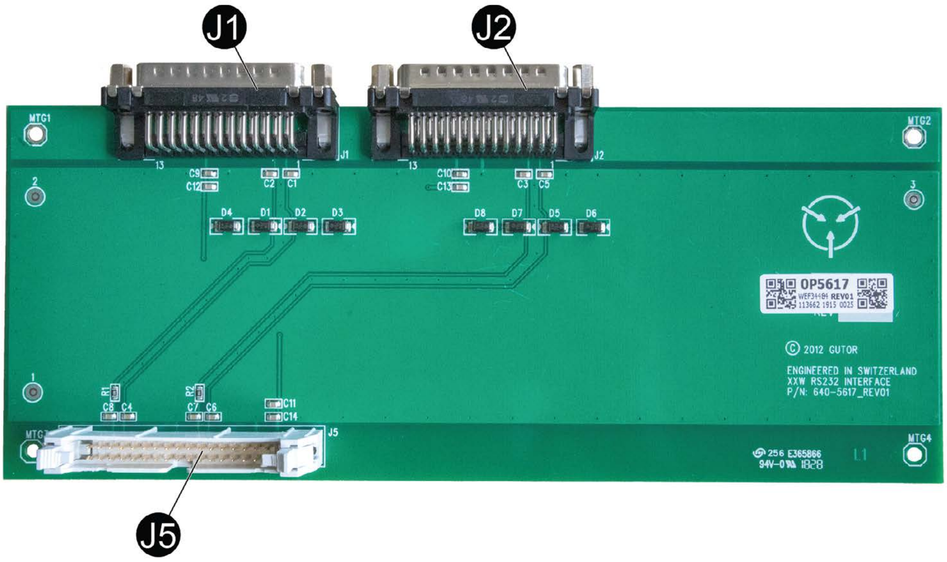
An overview of the connection options and available ports on the cards used in the network management system.

Connections on the Communication Interface

The communication interface makes it possible to connect the controller board to the smart slot translator. The communication interface has two RS-232 ports with DB-25 connector **J1** and **J2** and one RS-232 port with a 34 pin IDC-connector **J5** using the Silcon[1] protocol.

The Silcon protocol uses a Block Check Character (BCC) to acknowledge requests and to make sure the status messages does not contain any errors. Any other communication is ignored by the controller board without leading to any reaction from the system.

The connection between the communication interface and the smart slot translator is an extension of the one-way communication from the controller board. No conversion of the signal is done on the communication interface.



Ports	**Port Standard**	**Connector**	**Communication Protocol**
J1, **J2** (outputs)	RS-232	DB-25 (male)	Silcon[2]
J5 (input)	RS-232	34 pin IDC (male)	Silcon[2]

Pinout of **J1** and **J2**:

- Pin 2: RS-232 Tx
- Pin 3: RS-232 Rx
- Pin 9: 10 V (DC)
- Pin 7: GND

Other pins are not connected.

[1] The Silcon protocol is an internal Schneider Electric protocol.
[2] The Silcon protocol is a Internal Schneider Electric protocol.

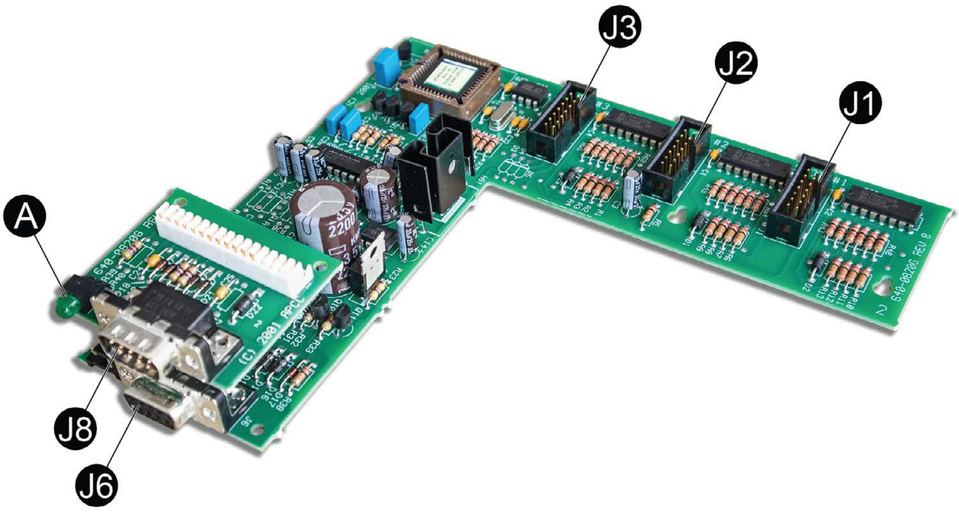
Connections on the Smart Slot Translator

The smart slot translator is used to convert the RS-232 signal from the Silcon[3] protocol to the UPS-link protocol. The connection from the communication interface is to a RS-232 port **J8** with a DE-9 connector (male), using the Silcon[4] protocol. The connections to the NMC and the options slot are from RS-232 ports **J3** and **J2** with 10 pin IDC-connectors, using the UPS-Link protocol[5].

The smart slot translator has a serial monitoring port **J6**, a RS-232 port with a DE-9 connector (female). With a serial cable it is possible to access the command line interface (CLI) from the **J6** port.

The green LED **(A)** indicates the status of the serial connection. A solid green light indicates normal operation and that the smart slot translator is receiving valid information from the system, else the LED is flashing with a green light.

The port **J1** is not used.



Ports	Port Standard	Connector	Communication Protocol
J1, **J2**, **J3** (outputs)	RS-232	10 pin IDC (male)	UPS-Link
J6 (output)	RS-232	DE-9 (female)	UPS-Link
J8 (input)	RS-232	DE-9 (male)	Silcon[3]

[3] The Silcon protocol is a Internal Schneider Electric protocol.

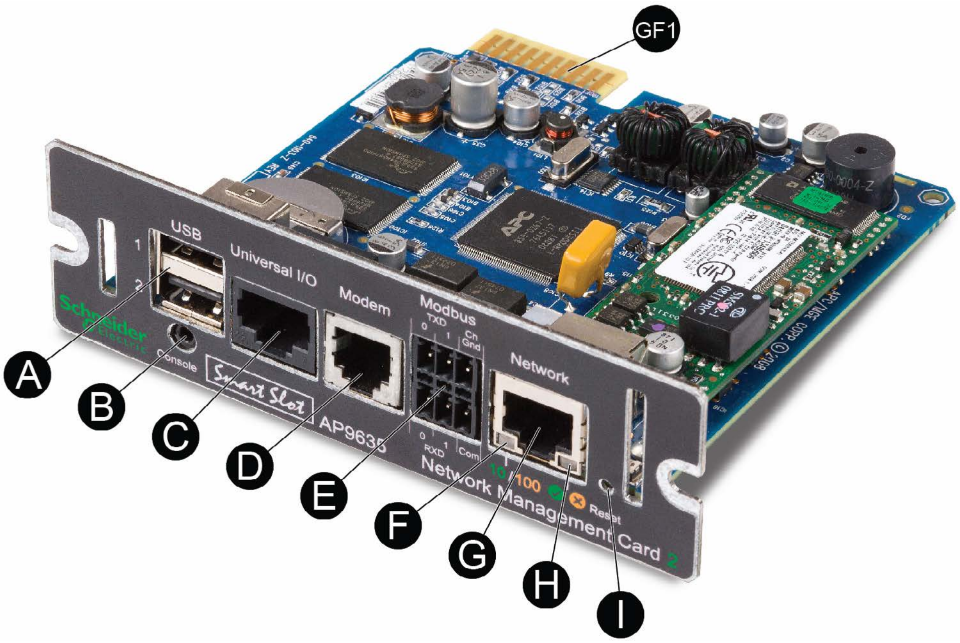
[4] The Silcon protocol is an Internal Schneider Electric protocol.

[5] For more information about the UPS-link protocol see *How to download and use the APC UPS-Link Protocol Language*

Connections on the Network Management Card (AP9635)

The NMC allows for multiple different remote and local connection options.

NOTE: Not all connection options are supported by Gutor.



Position	Part	Description
(A)	USB ports	Can only be used for NMC firmware updates.
(B)	Serial console port	Can be used to connect the NMC directly to a computer with a serial cable. Used for a local connection to the command line interface (CLI) or for NMC firmware updates.
(C)	Universal I/O sensor port	Can be used to connect a relay input/output accessory connector. The Dry Contact I/O Accessory (*AP9810*) has two input contacts and one output relay.
(D)	Modem Port[6]	Can be used to connect the NMC to a dial-up network.
(E)	Modbus connector	Can be used to connect the NMC to a 2-wire or 4-wire RS485 Modbus protocol network.
(F)	Link-RX/TX (10/100) LED	Indicates the status of the NMC. For details see section *Link-RX/TX (10/100) LED, page 13*.
(G)	10/100 Base-T connector	Can be used to connect the NMC to an Ethernet network.
(H)	Status LED	Indicates the status of the network. For details see section *Status LED, page 13*.
(I)	Reset button	Reboot/Reset: Press one time to reboot the NMC. Hard reset: Press and hold for a long time to reset the NMC to the default settings.

[6] Gutor does not recommend using the port and does not provide support for the port/connection.

Status LED

The status LED **(H)** indicates the status of the NMC by changing color and how it lights up (constant, flashing, flickering).

LED Light Condition	Description
Off	One of the two reasons: • The NMC does not receive any power. Make sure that the power is connected and on. • The NMC does not operate properly. Make sure that the NMC is installed correctly in the system. If the problem is still not resolved, see the chapter *Troubleshooting for the Network Management Card, page 54* for more information.
Constant green	The NMC has valid TCP/IP settings.
Constant orange	A hardware issue has been detected on the NMC. Contact *Gutor Service Center*.
Flashing green	The NMC does not have valid TCP/IP settings.
Flashing orange	The NMC makes BOOTP requests.
Flickering orange	The NMC is in the boot monitor mode.
Flashing and alternating between green an orange	If the LED is flashing slowly, the NMC is making DCHP requests. If the LED is flashing quickly, the NMC is starting up.

Link-RX/TX (10/100) LED

The Link-RX/TX (10/100) LED **(F)** indicates the status of the Ethernet network connection by changing color and how it lights up (constant, flashing, flickering).

LED Light Condition	Description
Off	One of the following reasons: • The NMC is not receiving any power. Make sure that the power is connected and on. • The NMC is not connected to the network. Make sure that the network cable is connected. • The device that connects the NMC to the network is turned off or inoperable. Check the network device. • The NMC is not operating properly. Make sure that the NMC is installed correctly in the system. If the problem is still not resolved, see the chapter *Troubleshooting for the Network Management Card, page 54* for more information.
Constant green	The NMC is connected to a network operating at 10 Megabits per second (Mbps).
Constant orange	The NMC is connected to a network operating at 100 Mbps.
Flashing green	The NMC receives or transmits data packets at 10 Mbps.
Flashing orange	The NMC receives or transmits data packets at 100 Mbps.

Network Management Card Overview

The network management card (NMC) makes it possible to access logs, status information and events from Gutor systems.

The information can be accessed with:

- Graphical user interface (GUI) also called the web interface, with remote access from a web browser
- Command line interface (CLI), with both local and remote access options
- Simple network management protocol (SNMP)
- Modbus

NOTE: A proxy server cannot be used to access the NMC.

Benefits of an NMC in a Gutor System

With an NMC you can:

- Monitor and manage your Gutor systems remotely over your own enterprise network.
- Identify trends and take preventive actions.
- Manage and maintain battery systems. See detailed battery information that can be used to plan preventive maintenance.
- Monitor external triggers that can initiate actions on other connected devices (for example air conditioning).
- Be ready to support the next generation of IP network.

Watchdog Timer

To detect internal problems and recover from unexpected inputs, the NMC uses a watchdog timer. If the NMC does not receive any network traffic for 9.5 minutes, the NMC assumes that there is a problem with its network interface and restarts. When the NMC restarts because of the watchdog timer it is recorded in the event log as “System: Network interface restarted”.

How to Reset the Watchdog Timer

To make sure that the NMC does not restart if the network is quite for 9.5 minutes the NMC attempts to contact the default gateway every 4.5 minute. If the default gateway is available and responds the watchdog timer is reset.

If your application does not have or does not require a default gateway it is possible to specify an IP address of a computer instead as the gateway. The computer needs to be on the same network and subnet as the NMC. In this case the network traffic from the computer will reset the watchdog timer on the NMC.

To change the default gateway:

- From the CLI type `-tcpip —g` or `-tcpip6 —g` followed by the computer’s IP address. Press **Enter** to confirm the change.
- From the web interface navigate to **Configuration > Network > TCP/IP > IPv4 (or IPv6)** and enter the computer’s IP address in the default gateway field. Click **Apply** to save the changes.

NOTE: The NMC needs to reboot before the default gateway change takes effect.

User Accounts

To access the NMC a login with a user name and password is always required. Both the user name and password are case sensitive and can consist of maximum 64 characters.

There are different user types with different access levels:

- **Super user:** Both CLI and GUI access. Full access to all menus and options. Can add new users and manage other users.
- **Administrator:** Both CLI and GUI access. Full access to all menus and options. Can add new users.
- **Device manager:** Both CLI and GUI access. Can only access the log options, event and system menu.
- **Read-only user:** Only GUI access. Can view the same menus as the device manager but cannot configure, delete data, or use FTP options.
- **Network-only user:** Only remote access to the CLI and GUI. Can only access the network settings.

NOTE: Menus and options that a user does not have access to will appear grayed out.

Default User and Password Settings

User Types	Default User Name	Default Password
Super user	apc	apc
Administrator	apc	apc
Device manager	device	apc
Read-only user	readonly	apc
Network-only user	–	–

NOTE: A user is automatically logged out after 3 minutes (default setting) of inactivity, this can be changed from the user settings.

Default User and Network Settings

Default user settings for NMC AOS v6.8.0 and higher:

- After the first log in the user is prompted and required to set a new password.
- All users except the super user is disabled and cannot be enabled until the super user password is changed.
- After changing the password first time the user will be directed to the network overview (path: **Configuration > Network > Summary**) to view the default network settings.
- After a new user type is enabled and after the first log in the user is prompted and required to set a new password.

Default network settings for NMC AOS v6.8.0 and higher:

- HTTPS and SSH are enabled.
- SCP is enabled but will not allow any file transfer until after the super user password has been changed from the default.
- All other protocols are disabled.

NOTE: If a hard reset is done on the NMC the user and network settings are restored to the default settings.

Change User Settings

Some user settings can be changed for all users of the same type, for example password strength requirements. Other settings are only done for a specific user, for example to change the password.

From the web interface:

- To make changes to a specific user follow the path: **Configuration > Security > Local Users > Management** and then click on the name of the specific user.
- To make changes to a type of users follow the path: **Configuration > Security > Local Users > Default Settings**

From the CLI type `user ?` to view the available options. For example, to set the password of a user, type `user -n <user name> -pw <new password>`.

Reset Password

1. Make sure you have a serial port on the local computer. Disable any services that uses that port.
2. Connect the serial cable (Gutor part number: 940-0299) to the serial port on the computer and the serial configuration port on the NMC.
3. Start a terminal emulator and configure the connected serial port on to:

Name	Value
Baud rate	9600 bps
Data	8 bit
Parity	None
Stop	1 bit
Flow control	None

4. Press the **Enter** repeatedly to get the user name prompt.
5. Press the **Reset** button on the front panel of the NMC to start the reboot sequence.
6. Press the **Reset** button again during the reboot just when the status LED starts to flash orange and green. This will temporary reset the user name and password to their default settings for 30 seconds, see table *Default User and Password Settings, page 15*.
7. Press the **Enter** repeatedly to get the user name prompt. Use the default user name and password `apc` to login.

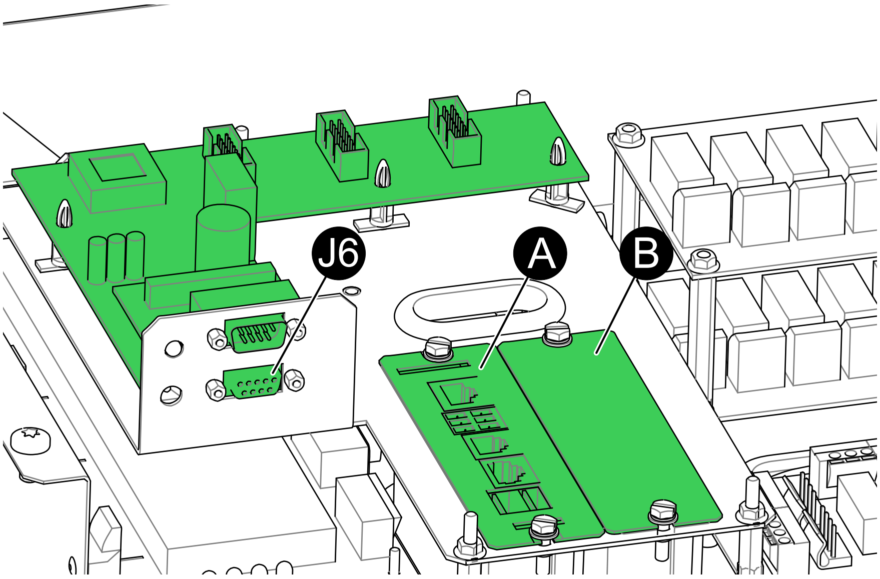
   NOTE: When the prompt is displayed you need to login within 30 seconds, else the password needs to be reset again.
8. To set a new password type `user —n <current user name> —pw <new user password>`. For example, to change the password to abcXYZ_!12 type `user —n apc —pw abcXYZ_!12`.
9. Type `quit` or `exit` to log out.
10. Press the **Reset** button on the front panel to reboot the NMC.

Command Line Interface

The command line interface (CLI) is one of the interfaces used to connect to the NMC.

The CLI can be accessed locally from the smart slot translator to port **J6**, the serial port on the NMC **(A)** or the serial port on an optional NMC **(B)** if installed. It is also possible to connect remotely using Telnet or SSH.

From the CLI a user can access the same information that is available from the web interface, but the settings options are slightly different.



How to Log in to the Command Line Interface

There are three ways to connect to the command line interface (CLI):

- *Local access via the network management card, page 18*
- *Local access via the smart slot translator, page 18*
- *Remote access, page 19*

Connect and Configure Local Access to the CLI via the NMC

1. Make sure you have a serial port on the local computer. Disable any services that uses that port.
2. Connect the serial cable (Gutor part number: 940-0299) to the serial port on the computer and the serial configuration port on the NMC.
3. Start a terminal emulator and configure the connected serial port on to:

Name	Value
Baud rate	9600 bps
Data	8 bit
Parity	None
Stop	1 bit
Flow control	None

4. Press **Enter**. When prompted enter the user name and password to login to the CLI.
5. For more information about the setting options in the CLI see, *Overview of the Command Line Interface, page 19* and *Command Line Interface Commands, page 20*. For information on how to change the IP address see *How to Change the IP Address from the CLI, page 22*.
6. To log out from the CLI type `exit` or `quit` and press **Enter**.

Connect and Configure Local Access to the CLI via the Smart Slot Translator

1. Make sure you have a serial port on the local computer. Disable any services that uses that port.
2. Connect a serial DB-9 cable to the serial port on the computer and the serial monitoring port **J6** on the smart slot translator.

Male Cable End	Female Cable End	Description
1	3	TXD
2	2	RXD
9	5	GND
–	1 connected to 4	DCD – DRT
–	7 connected to 8	shield

NOTE: Do not connect or use other pins!

3. Start a terminal emulator and configure the connected serial port on to:

Name	Value
Baud rate	2400 bps
Data	8 bit
Parity	None
Stop	1 bit
Flow control	None

4. Press **Enter**. When prompted enter the user name and password to login to the CLI.
5. For more information about the setting options in the CLI see, *Overview of the Command Line Interface, page 19* and *Command Line Interface Commands, page 20*. For information on how to change the IP address see *How to Change the IP Address from the CLI, page 22*.
6. To log out from the CLI type `exit` or `quit` and press **Enter**.

Connect and Configure Remote Access to the CLI

To access the CLI remotely an IP address or a DNS name must be configured for the NMC card, see *How to Set an Initial IP Address for the NMC, page 21*. The remote access can use Telnet for basic access or SSH for secure encrypted access.

NOTE: Without encryption the user name, password and data are transmitted as plain text. Plain text can be read by someone that monitors the network traffic.

1. Start a terminal emulator from a computer on the same sub network as the NMC.
2. In the command line type `telnet xxx.xxx.xxx.xxx` where xxx.xxx.xxx.xxx is the IPv4 address of the NMC.
3. Press **Enter**.
4. Enter your user name and press **Enter**.
5. Enter your password and press **Enter**.

   NOTE: For access with SSH, type `ssh` instead of `telnet` in the command line if configured.

   NOTE: If configured, the DNS or IPv6 name can be used instead of the IPv4 address of the NMC.

Overview of the Command Line Interface

The CLI main menu provides some general information of the system and NMC:

- Firmware versions
- Name, contact and location of the system
- Date and time of the login
- Current status and up time of the NMC
- Model of the system
- Descriptions of a few commands

This is an example of a main menu that is shown when logging in to the CLI:

```
Schneider Electric                      Network Management Card AOS      v6.8.2
(c) Copyright 2019 All Rights Reserved  Gutor XXW & SDC APP              v6.8.0
-------------------------------------------------------------------------------
Name      : System name                                 Date : 07/23/2019
Contact   : Contact name                                Time : 00:01:17
Location  : Location name                               User : Super User
Up Time   : 0 Days 0 Hours 0 Minutes                    Stat : P+ N4+ N6+ A+
-------------------------------------------------------------------------------
IPv4               : Enabled            IPv6               : Enabled
Ping Response      : Enabled
-------------------------------------------------------------------------------
HTTP               : Disabled           HTTPS              : Enabled
FTP                : Disabled           Telnet             : Disabled
SSH/SCP            : Enabled            SNMPv1             : Disabled
SNMPv3             : Disabled
-------------------------------------------------------------------------------
Super User         : Enabled            RADIUS             : Disabled
Administrator      : Disabled           Device User        : Disabled
Read-Only User     : Disabled           Network-Only User  : Disabled


Type ? for command listing
Use tcpip command for IP address(-i), subnet(-s), and gateway(-g)
```

The `Stat:` field provides a quick overview of the status of the NMC. The table describes each status code.

Status Code:	Status Description:
P+	The AOS is functioning properly.
N+	The network is functioning properly.
N?	A BOOTP request cycle is in progress.
N-	The NMC failed to connect to the network.
N!	Another device is using the NMC’s IP address.
A+	The APP is functioning properly.
A?	The APP is initializing.
A-	The APP is initializing.
A!	The APP is not compatible with the AOS.

Command Line Interface Commands

The `System Commands` are general and the same for all Gutor systems. The `Device Commands` are specific for the system type.

The navigation in the CLI is the same for all systems, but the options available will depend on the system configuration and options selected.

Available Commands in the CLI

To view the available `System Commands` and `Device Commands` type `?` and press **Enter**.

This is an example of the available commands:

```
System Commands:
---------------------------------------------------------------------------
For command help: command ?

?           about       alarmcount  boot        bye         cd
cipher      clrrst      console     date        delete      dir
dns         eapol       email       eventlog    exit        firewall
format      ftp         help        lang        lastrst     ledblink
logzip      netstat     ntp         ping        portspeed   prompt
pwd         quit        radius      reboot      resetToDef  session
smtp        snmp        snmptrap    snmpv3      system      tcpip
tcpip6      user        userdflt    web         whoami      xferINI
xferStatus

Device Commands:
---------------------------------------------------------------------------
ups         modbus
```

Command Syntax and Navigation

To navigate in the CLI type a command and then press **Enter** to run the command. The command syntax is:

NOTE: Type `?` or `help` to view available commands.

Item	Description
–	Options are preceded by a hyphen.
< >	The definitions of options are enclosed in angle brackets. For example: `-pw <user password>`
[ ]	If a command accepts multiple options or an option accepts mutually exclusive arguments, the values may be enclosed in brackets.
|	A vertical line between items enclosed in brackets or angle brackets indicates that the items are mutually exclusive. You must use one of the items.

Some examples are:

- To view the event log type: `eventlog` and press **Enter**.
- To enable HTTP type: `web -h enable` and press **Enter**.
- To change to the metric temperature scale for the logged in user type: `user -ts metric` and press **Enter**.

How to Set an Initial IP Address for the NMC

When setting up a new NMC or if the NMC does not yet have an IP address defined it is necessary to define an IP address to be able to access the NMC.

To set the IP address the MAC address of the NMC is needed. The MAC address can be found on a label on the bottom of the card. The MAC address consists of 12 characters (only letters and numbers).

NOTE: Make sure to select a unique IP address for each NMC on the same network.

1. Start a terminal emulator from a computer on the same network or connected with a serial cable.
2. Type `arp -s xxx.xxx.xxx.xxx yy-yy-yy-yy-yy-yy`. Where xxx.xxx.xxx.xxx is the IPv4 address that you want to assign to the NMC card with a MAC address of yyyyyyyyyyyy[7].

   NOTE: Linux uses colon instead dashes in the MAC address, for Linux write the MAC address as `yy:yy:yy:yy:yy:yy`
3. Type `ping xxx.xxx.xxx.xxx -l 113` to ping 113 bytes to check that the new IPv4 address for the NMC is working.

   NOTE: For Linux write -s instead of -l.

NOTE: To assign an IPv6 address, choose an IPv6 address in the above example instead of an IPv4 address.

[7] Network devices from APC starts with a MAC address of “00C0B7” for older devices or “282986” for new devices.

How to Change the IP Address from the CLI

When connected and logged in to the CLI the IP address of the NMC can be changed.

To set a new IPv4 TCP/IP address:

1. Type `tcpip –i xxx.xxx.xxx.xxx` where xxx.xxx.xxx.xxx is the new IPv4 address.
2. Press **Enter**.
3. The IP address is now changed.

To set a new IPv6 TCP/IP address:

1. Type `tcpip6 –i xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx` where xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx is the new IPv6 address.
2. Press **Enter**.
3. The IP address is now changed.

   NOTE: Reboot the NMC to apply changes. From the web interface select **Control > Network > Reset/Reboot** for options.

Web Interface

The web interface also called the graphical user interface (GUI), provides an easy and user-friendly way to manage the NMC and view the status of the system.

How to Log in to the Web Interface

The web interface supports the latest versions of the browsers:

- Chrome®
- Edge®
- Firefox®
- Internet Explorer®

Other browsers might work but have not been fully tested.

NOTE: It is not possible to access the NMC with a proxy server. Make sure to disable the proxy server or configure it to not proxy the IP of the NMC.

Log in to the Web Interface

1. Check that HTTPS or HTTP access is enabled and configured correctly on the NMC card.

   NOTE: Only HTTPS is enabled by default.

2. Open a supported web browser on a computer.

   NOTE: The computer needs to be connected to the same local network as the NMC or the internet if the NMC is connected to the internet.

3. In the browser field type the URL to the IP address of the NMC (and web server port if changed) or the DNS name of the NMC.

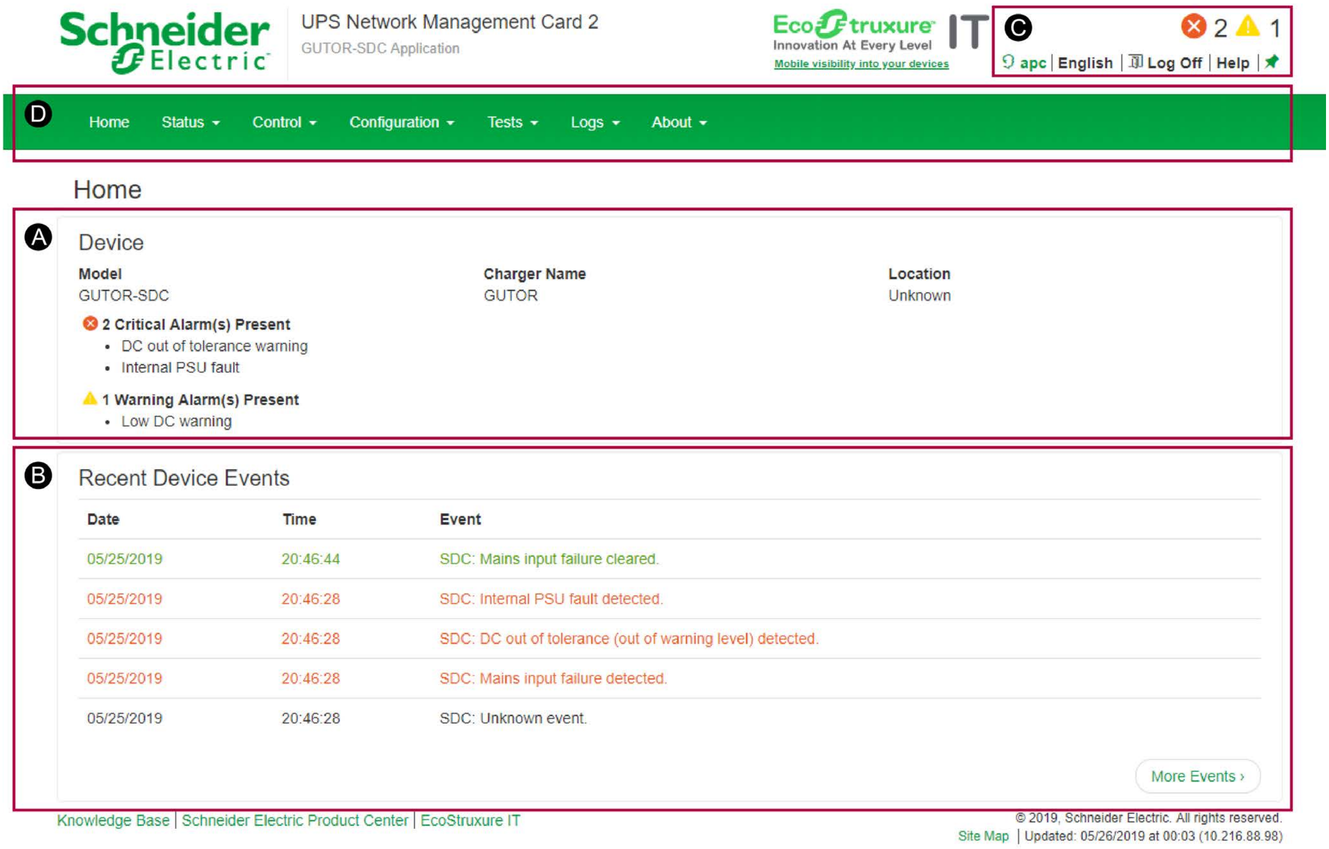
Example NMC Identifier	URL Example
With an NMC DNS name that is nmcdnsname	`https://nmcdnsname`
With an NMC IP address of 139.225.6.133	`https://139.225.6.133`
With an NMC IP address of 139.225.6.133 and specified port of :5000	`https://139.225.6.133:5000`
With an NMC IPv6 address of 2001: db8:1::2c0:b7ff:fe00:1100 and specified port of :5000	`https://[2001:db8:1::2c0:b7ff: fe00:1100]:5000`

   NOTE: Change `https` to `http` in the URL if HTTP is used instead of HTTPS.

4. Enter the user name and password to log in to the web interface.
5. To log out of the web interface, click **Log Off** in the top right corner of the window.

Overview of the Web Interface

The default **Home** page is shown when logged in to the web interface. This is an example of the default **Home** page:


Schneider Electric
UPS Network Management Card 2
GUTOR-SDC Application
EcoStruxure IT
Innovation At Every Level
Mobile visibility into your devices
C
2
1
apc | English | Log Off | Help
D
Home
Status
Control
Configuration
Tests
Logs
About
A
B
More Events ›
Knowledge Base | Schneider Electric Product Center | EcoStruxure IT
Site Map

Home

Device

Model
GUTOR-SDC

Charger Name
GUTOR

Location
Unknown

2 Critical Alarm(s) Present

- DC out of tolerance warning
- Internal PSU fault

1 Warning Alarm(s) Present

- Low DC warning

Recent Device Events

Date	Time	Event
05/25/2019	20:46:44	SDC: Mains input failure cleared.
05/25/2019	20:46:28	SDC: Internal PSU fault detected.
05/25/2019	20:46:28	SDC: DC out of tolerance (out of warning level) detected.
05/25/2019	20:46:28	SDC: Mains input failure detected.
05/25/2019	20:46:28	SDC: Unknown event.

© 2019, Schneider Electric. All rights reserved.
Updated: 05/26/2019 at 00:03 (10.216.88.98)

The default home page has two main sections, **Device** and **Recent Device Events**. The **Main Menu** and the **Quick Status Menu** are always displayed on all pages and subpages.

(A) Device: System status overview.

(B) Recent Device Events: Lists the latest events.

(C) Quick Status Menu: Quick overview and some common menu options.

(D) Main Menu: The main navigation menu.

Home Page: Device

The **Device** section shows the system or unit type, name and location. The section provides information on any alarms that are present in the system.

Home Page: Recent Device Events

The **Recent Device Events** contains a list of the latest events with the most recent at the top. Click **More Events >** to view the full list of events.

Each event contains a date, time and event description. The color of the event also gives a quick overview of the event type.

Event Text Color	Event Severity	Severity Description
Red	Critical	A critical alarm exists and requires immediate action.
Orange	Warning	An alarm exists and requires attention. If not addressed, it could damage data or equipment.
Green	Alarm Cleared	The alarm has been resolved and cleared.
Black	Normal	No alarms are present. The NMC and all connected devices are operating normally.
Blue	Informational	An event to provide information. The NMC and all connected devices are operating normally.

Quick Status Menu

The **Quick Status Menu** in the top right corner contains an overview of the alarms and some setting options:

- **System status:** Shows if the system operates as intended or the number of present alarms and warnings.
- **User name:** Click to configure the user preferences.
- **Language:** The current displayed language
- **Log Off:** Logs out the user from the web interface.
- **Help:** Opens a new window that provides help for the current page in the web interface. In the help window it is possible to navigate and view help for each page.
- **Pin:** Click to set the current page as the new home page, the icon will change to a pushed in pin (circle). Click again to reset to the default home page.

Main Menu

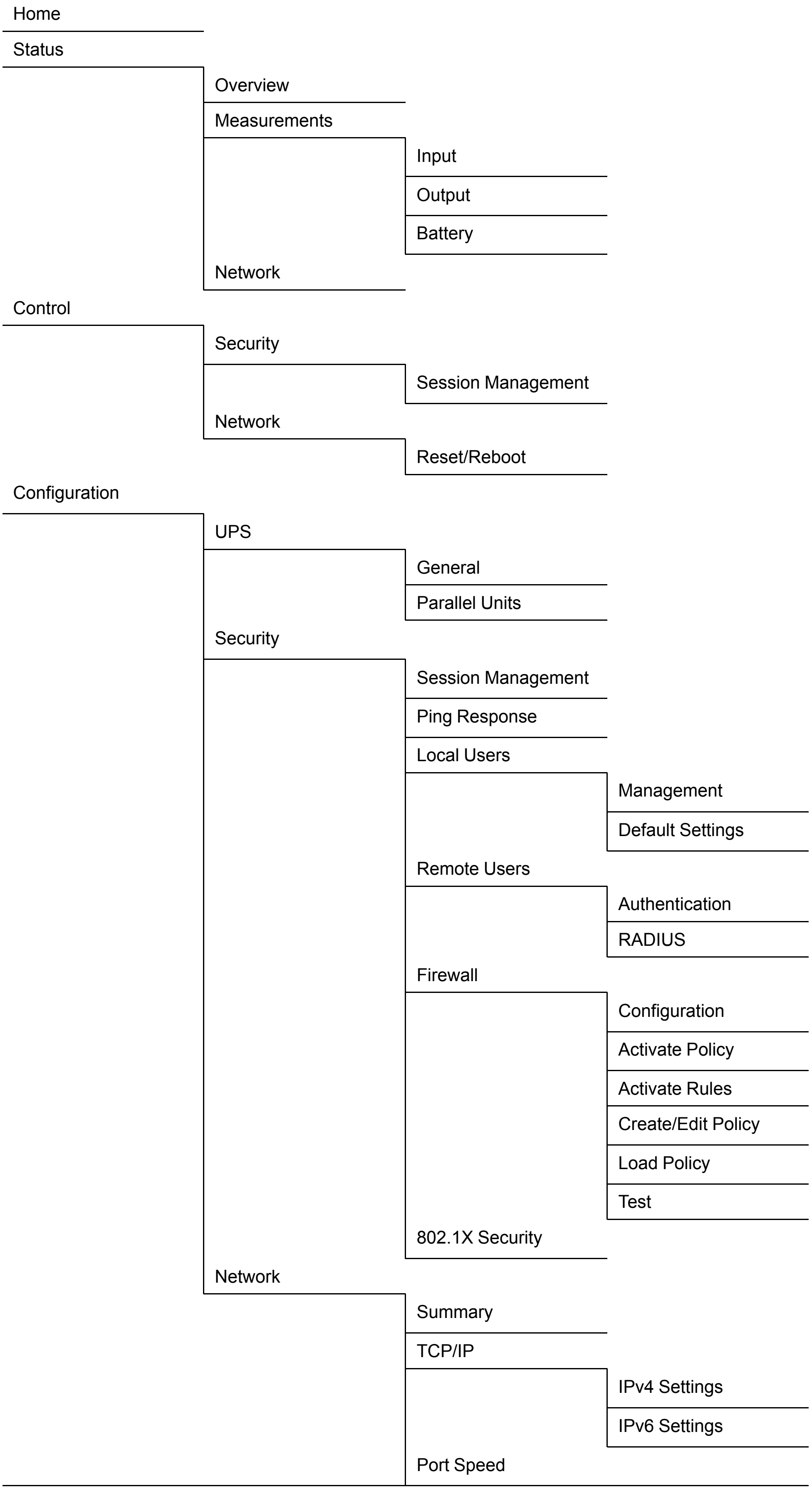
The **Main Menu** is used to navigate between the pages. The pages and navigation options are:

- **Home:** Returns the user to the **Home** page.
- **Status:** Sub menus for status and measurements from the system, sensors and network.
- **Control:** See current login sessions and reset network settings.
- **Configuration:** Configure system information and sensor, security, network and notification settings. Can also configure general settings for the interface and Syslog settings.
- **Test:** Test the LEDs on the NMC.
- **Logs:** Look at and download the event logs and the data logs. View the firewall policy log.
- **About:** View the information about the system, network settings and firmware. Contains information for troubleshooting.

For a detailed description of all pages and feature, please see the **Help** page available from the **Quick status Menu**.

Web Interface Menu Structure

The navigation from the main menu have the following structure. It is only possible to click on the lowest level of each branch, the other names are only for navigation and grouping.



- DNS
  - Configuration
  - Test
- Web
  - Access
  - SSL Certificate
- Console
  - Access
  - SSH Host Key
- SNMPv1
  - Access
  - Access Control
- SNMPv3
  - Access
  - User Profiles
  - Access Control
- Modbus
  - Serial
  - TCP
- FTP Server

- Tests
  - Network
    - LED Blink
- Logs
  - NMC Log
    - Log
    - Reverse Lookup
    - Size
  - Data Log
    - Log
    - Graphing
    - Interval
    - Rotation
    - Size
  - Firewall
- About
  - UPS
  - Network
  - Support

Configure the IP Address from the Web Interface

Log in to the web interface to change the IP address of the NMC.

To configure the TCP/IP IPv4 settings:

1. Navigate to **Configuration > Network> TCP/IP > IPv4 Settings**
2. Here you can:
   - Enable IPv4
   - Set a manual IP address, subnet mask and default gateway.
   - Enable BOOTP or DHCP
3. To enter a new manual IP address:
   a. Make sure IPv4 is enabled.
   b. Make sure **Manual** mode is selected.
   c. Enter the new IP address in the field **System IP**.
   d. Click **Apply**.
   e. The IP address is now changed.

   NOTE: Reboot the NMC to apply changes. From the web interface select **Control > Network > Reset/Reboot** for options.

To configure the TCP/IP IPv6 settings:

1. Navigate to **Configuration > Network> TCP/IP > IPv6 Settings**.
2. Here you can:
   - Enable IPv6
   - Enable IPv6 auto configuration
   - Set a manual IP address and default gateway.
   - Enable different DHCPv6 modes
3. To enter a new manual IP address:
   a. Make sure IPv6 is enabled.
   b. Make sure **Manual Configuration** is enabled and **Auto Configuration** is disabled.
   c. Enter the new IP address in the field **System IP**.
   d. Click **Apply**.
   e. The IP address is now changed.

   NOTE: Reboot the NMC to apply changes. From the web interface select **Control > Network > Reset/Reboot** for options.

File Transfer

File transfer is used both to update the firmware and to download logs. There are two different protocols that can be used with different security options:

- File transfer protocol (FTP): With FTP the information is transferred as plain text. Use SCP for increased security.
- Secure copy protocol (SCP): With SCP the information is encrypted. SCP is automatically used when the SSH protocol is enabled and configured and the FTP protocol is disabled.

How to Enable FTP and SCP

Both FTP and SCP can be enabled from the command line interface or the web interface. For information on how see each section:

- *Enable FTP from the CLI, page 29*
- *Enable SCP from the CLI, page 29*
- *Enable FTP from the Web Interface, page 30*
- *Enable SCP from the Web Interface, page 30*

Enable FTP from the CLI

1. Log in to the CLI.
2. To enable FTP type `ftp -s enable` and press **Enter** to confirm.
3. To set the FTP port to, for example 5001, type `ftp -p 5001`. Available ports are 21, 5001-32768.

   NOTE: Use a specified FTP port, instead of the default, to increase security.
4. FTP is now enabled.

   NOTE: Reboot the NMC to apply changes. From the web interface select **Control > Network > Reset/Reboot** for options.

Enable SCP from the CLI

To enable SCP, SSH needs to be enable and FTP needs to be disabled.

1. Log in to the CLI.
2. To disable FTP type `ftp -s disable` and press **Enter** to confirm.
3. To enable SSH type `ssh -s enable` and press **Enter** to confirm.
4. To set the SSH port, to for example 5000, type `ssh -p 5000`. Available ports are 22, 5000-32768.

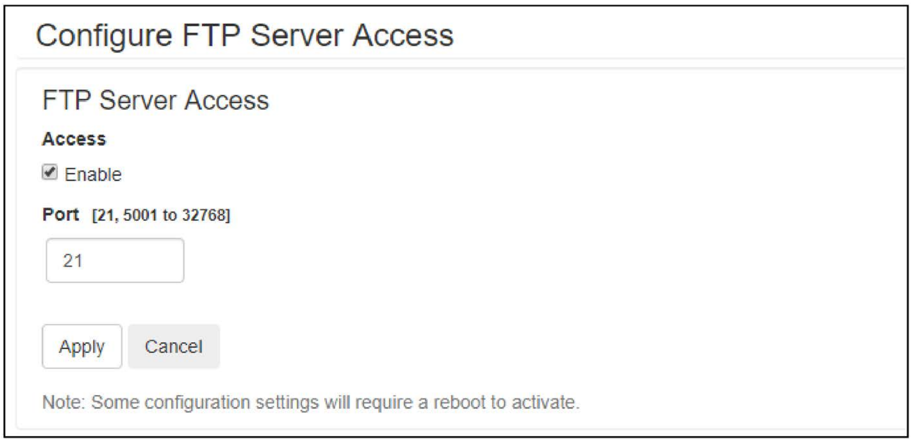
   NOTE: Use a specified SSH port, instead of the default, to increase security.
5. SCP is now enabled.

   NOTE: Reboot the NMC to apply changes. From the web interface select **Control > Network > Reset/Reboot** for options.

Enable FTP from the Web Interface

1. Log in to the web interface.
2. Navigate to **Configuration > Network > FTP server > Access**.
3. Check the FTP enable box. It is also possible to specify an FTP port. Click **Apply** to save the changes.

   NOTE: Use a specified FTP port, instead of the default, to increase security.



Configure FTP Server Access

FTP Server Access

Access

☑ Enable

Port [21, 5001 to 32768]

21

Note: Some configuration settings will require a reboot to activate.

4. FTP is now enabled.

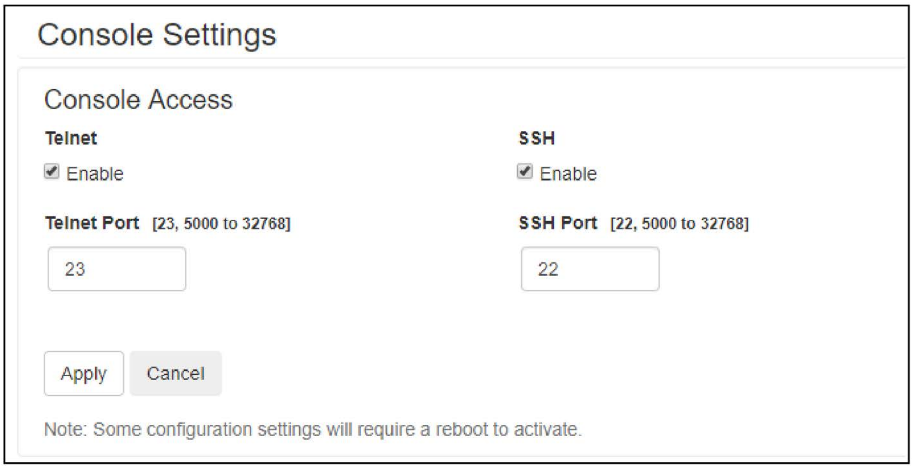
   NOTE: Reboot the NMC to apply changes. From the web interface select **Control > Network > Reset/Reboot** for options.

Enable SCP from the Web Interface

To enable SCP, SSH needs to be enable and FTP needs to be disabled.

1. Log in to the web interface.
2. Navigate to **Configuration > Network > Console > Access**.
3. Check the SSH enable box. It is also possible to specify an SSH port. Click **Apply** to save the changes.

   NOTE: Use a specified SSH port, instead of the default, to increase security.



Console Settings

Console Access

Telnet

☑ Enable

Telnet Port [23, 5000 to 32768]

23

SSH

☑ Enable

SSH Port [22, 5000 to 32768]

22

Note: Some configuration settings will require a reboot to activate.

4. Navigate to **Configuration > Network > FTP server > Access**.
5. Make sure that the FTP enable box is unchecked. Click **Apply** to save the changes.
6. SCP is now enabled.

   NOTE: Reboot the NMC to apply changes. From the web interface select **Control > Network > Reset/Reboot** for options.

NMC Firmware

The firmware for the NMC card in a Gutor system consists of three modules:

Module Name	Description	Example File Name
Application module (APP)	The Gutor specific application for Gutor systems	`apc_hw5_gutor_682.bin`
APC operating system (AOS)	Can be thought of as the operating system of the NMC	`apc_hw5_aos_680.bin`
Boot monitor (BM)	Can be thought of as the BIOS of the NMC	`apc_hw5_bootmon_108.bin`

IMPORTANT: To update the firmware correctly always update the BM first, then the AOS and the APP last.

Update the NMC Firmware with FTP

To update the firmware using FTP the NMC needs to have FTP enabled and an IP address, subnet mask and default gateway configured. The NMC and the computer also needs to be on the same network.

1. From a computer on the same network as the NMC open a command prompt window.
2. Go to the directory that contains the firmware files and list the files:
   `C:\>cd apc`
   `C:\apc>dir`
3. First update the BM:
   a. Type `C:\apc>ftp` to open an FTP session.
   b. Type `ftp> open xxx.xxx.xxx.xxx:xxxx` and press **Enter** to confirm.

      NOTE: Where `xxx.xxx.xxx.xxx` is the IP address of the NMC and `:xxxx` is the specified port if used. Some FTP clients might use a space instead of a colon.

   c. Log on as a super-user or administrator.
   d. Type `ftp> bin` and press enter
   e. Type `ftp> put apc_hw05_bm_`*`nnn`*`.bin`

      NOTE: Where *`nnn`* is the version number.

   f. Wait until there is a confirmation that the transfer is complete.
   g. Type `quit` to exit from the FTP session.
   h. Wait 20 seconds while the card is rebooting before proceeding with the AOS update.
4. Then update the AOS:
   a. Type `C:\apc>ftp` to open an FTP session.
   b. Type `ftp> open xxx.xxx.xxx.xxx:xxxx` and press **Enter** to confirm.

      NOTE: Where `xxx.xxx.xxx.xxx` is the IP address of the NMC and `:xxxx` is the specified port if used. Some FTP clients might use a space instead of a colon.

   c. Log on as a super-user or administrator.
   d. Type `ftp> bin` and press enter
   e. Type `ftp> put apc_hw05_aos_`*`nnn`*`.bin`

      NOTE: Where *`nnn`* is the version number.

   f. Type `quit` to exit from the FTP session.
   g. Wait 20 seconds while the card is rebooting with the APP update.
5. Lastly update the APP:
   a. Type `C:\apc>ftp` to open an FTP session.

b. Type `ftp> open xxx.xxx.xxx.xxx:xxxx` and press **Enter** to confirm.

   NOTE: Where `xxx.xxx.xxx.xxx` is the IP address of the NMC and `:xxxx` is the specified port if used. Some FTP clients might use a space instead of a colon.

c. Log in using the user name `apc` and the password `gutor`.

   NOTE: The AOS update have reset the user name to `apc` and the password to `gutor`.

d. Type `ftp> bin` and press enter

e. Type `ftp> put apc_hw05_app_nnn.bin`

   NOTE: Where *nnn* is the version number.

f. Type `quit` to exit from the FTP session.

g. Wait 20 seconds while the card is rebooting.

Verify Firmware Update

To verify that the firmware update succeeded, and no error occurred it is possible to:

- Type `xferStatus` in the CLI.
- Use a SNMP GET to the `mfiletransferStatusLastTransferResult` OID.

Download Logs

How to Retrieve Log Files with FTP from the CLI

With FTP it is possible to retrieve a copy of the data or event log.

1. Make sure that FTP is enabled.
2. From a computer on the same network as the NMC open a command prompt window.
3. Type `ftp <ip_address>` or `ftp>open <ip_address> <port_number>` if the port number have been changed from the default. Press **Enter**.

   NOTE: The command is for a windows FTP client, other FTP clients might work differently.
4. Log in with an administrator or device user.
5. To enable binary transfer mode type `ftp>bin`
6. To enable a progress bar for the file transfer type `ftp>hash`
7. To retrieve the event log file type `ftp>get event.txt`
8. To retrieve the data log file type `ftp>get data.txt`

   NOTE: It is possible to delete the log files on the NMC. The delete command do not have any confirmation prompt. A deletion of the data log is stored as an event in the event log. A deletion of the event logs is stored as an event in a new event log.
9. To delete the event log file type `ftp>del event.txt`
10. To delete the data log file type `ftp>del data.txt`
11. Type `ftp>quit` to exit.

How to Retrieve Log Files with SCP from the CLI

With SCP it is possible to retrieve a copy of the data or event log.

1. Make sure that SCP is enabled.
2. From a computer on the same network as the NMC open a command prompt window.

   NOTE: The commands bellow are only examples.
3. To retrieve the event log file type `scp <username@hostname>:event.txt /temp/event.txt` or `scp <ip_address>:event.txt /temp/event.txt`
4. To retrieve the data log file type `scp <username@hostname>:data.txt /temp/data.txt` or `scp <ip_address>:data.txt /temp/data.txt`

Modbus Access to the Network Management Card

Modbus is a serial communications protocol, the NMC supports Modbus RTU (also called Modbus serial) and Modbus TCP/IP (also called Modbus TCP). If using Modbus serial for the NMC, the RS-485 communication can be either with half-duplex over a 2-wire bus or with full duplex over a 4-wire bus.

For the wiring of the Modbus serial, see *Modbus Wiring Diagrams, page 41*.

Configure Modbus Access

Super users, administrators and device users can configure the settings for Modbus serial and TCP from the CLI or the web interface. The Modbus configuration options are the same in both interfaces. For more information see respective section:

- *Configure Modbus Serial and TCP from the CLI, page 34*
- *Configure Modbus Serial from the Web Interface, page 35*
- *Configure Modbus TCP from the Web Interface, page 36*

The recommended settings are 19200 baud rate, 8 bit data, even parity, 1 stop bit.

NOTE: Each NMC on a network needs to have a unique ID.

Configure Modbus Serial and TCP from the CLI

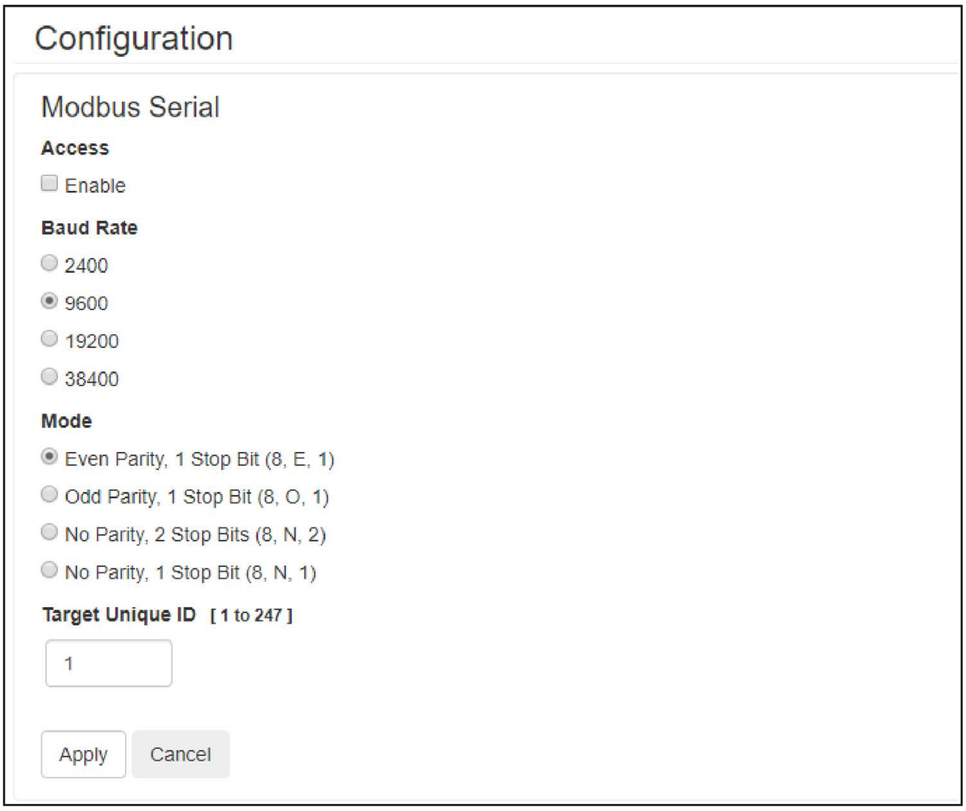
1. Log in to the CLI.
2. To see the configuration options type `modbus ?`.

Setting	Command	Argument	Description
Help	`?`		Shows the command help for Modbus.
Modbus serial status	`-a`	`enable | disable`	Enables or disables Modbus serial.
Baud rate	`-br`	`2400 | 9600 | 19200 | 38400`	The data transfer rate in bits per second.
Parity	`-pr`	`even | odd | none`	The parity bit or check bit.
Mode	`-m`	`8e1 | 8o1 | 8n2 | 8n1`	Default modes for the serial configuration: • **8o1**– 8 bit data, odd parity, 1 stop bit • **8e1**– 8 bit data, even parity, 1 stop bit • **8n1**– 8 bit data, no parity, 1 stop bit • **8n2**– 8 bit data, no parity, 2 stop bits
Slave address	`-s`	`1 - F7`	The slave address or unique ID of the target device in hexadecimal.
Reset settings	`-rDef`		Resets all the Modbus settings to default.
Modbus TCP status	`-tE`	`enable | disable`	Enables or disables Modbus TCP.
Modbus TCP port number	`-tP`	`502, 5000 – 32768`	Sets the Modbus TCP port number to the entered value.
Modbus TCP timeout	`-tTO`	`1 – 64800 seconds, 0 = never`	Set for how long the Modbus TCP communication can be active before timing out.

Configure Modbus Serial from the Web Interface

1. Log in to the web interface.
2. Navigate to **Configuration > Network > Modbus > Serial**.
3. Configure the Modbus serial settings:
   - **Access:** Enabled if box is checked.
   - **Baud Rate:** Select a baud rate [2400 | 9600 | 19200 | 38400].
   - **Mode:** Select a parity.
   - **Target Unique ID:** A unique number for the NMC, needs to be different for each NMC on a network [1 – 247].
4. Click **Apply** to save any changes.

   NOTE: Reboot the NMC to apply changes. From the web interface select **Control > Network > Reset/Reboot** for options.



Configuration

Modbus Serial

Access

□ Enable

Baud Rate

○ 2400

● 9600

○ 19200

○ 38400

Mode

● Even Parity, 1 Stop Bit (8, E, 1)

○ Odd Parity, 1 Stop Bit (8, O, 1)

○ No Parity, 2 Stop Bits (8, N, 2)

○ No Parity, 1 Stop Bit (8, N, 1)

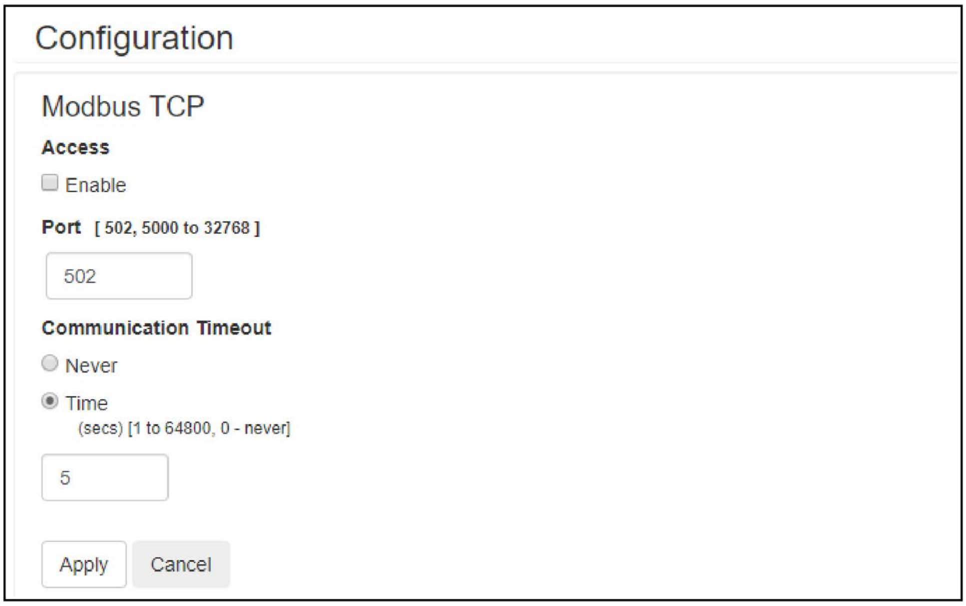
Target Unique ID [1 to 247]

1

Configure Modbus TCP from the Web Interface

1. Log in to the web interface.
2. Navigate to **Configuration > Network > Modbus > TCP**.
3. Configure the Modbus TCP settings:
   - **Access:** Enabled if box is checked.
   - **Port:** Enter port used [502, 5000 – 32768].
   - **Communication Timeout:** Enter a timeout time in seconds or select never (can also enter 0 seconds for never).
4. Click **Apply** to save any changes.

   NOTE: Reboot the NMC to apply changes. From the web interface select **Control > Network > Reset/Reboot** for options.



Configuration

Modbus TCP

Access

□ Enable

Port [502, 5000 to 32768]

502

Communication Timeout

○ Never

● Time

(secs) [1 to 64800, 0 - never]

5

Modbus Read Coil Register (Function Call 01)

The read coil register contains digital information, the parameters are either 1 (true) or 0 (false). True indicates that the alarm/indication is active and present in the system.

The data is stored as Boolean. This information can be used to trigger alarms, actions or other events.

NOTE: It is recommended that the delay poll is more than 10 seconds because the refresh rate of the register is about 10 seconds.

NOTE: All coil registers between 00001-00071 are reserved even if not listed in the table.

Modbus Read Coil Register List

Coil Register	Parameter	Description
00001	Output is out of tolerance detected	Indicates that the output voltage of the UPS is out of tolerance. The system will transfer to bypass if the bypass mains is within tolerance, if not the system will shut down.
00002	Battery operation	The system is in battery operation mode.
00003	Bypass operation	The system is in static bypass operation mode.
00004	Low DC shutdown	The supply to the inverter is too low and the inverter will turn off. The system will transfer to bypass if the bypass mains is within tolerance, if not the system will shut down.
00005	High DC shutdown	The output of the rectifier is too high, and the rectifier will turn off. The system will transfer to battery operation if possible. Else the system will transfer to bypass if the bypass mains is within tolerance, if not the system will shut down.
00006	Common alarm	The common alarm is active in the system.
00007	Overload > 100%	The system is overloaded. After some time, the system will transfer to bypass if the bypass mains is within tolerance, if not the system will shut down.
00008	SSW temp warning/ shutdown	One of the static switches are overheated. The system will transfer to an operating mode that does not use the overheated static switch if possible, or it will shut down.
00009	System pushed on	Indicates that the **ON button** was pushed.
00010	Inverter out of tolerance	
00011	Inverter not synchronized to bypass	
00012	Battery charge current is being limited by UPS	The battery current limiter is active. Does not trigger the common alarm.
00016	Battery test active	A battery monitor test or a battery capacity test is running.
00021	Low DC warning	Warning signal that shut down is imminent when running in battery operation.
00023	Inverter or output overload	The inverter is overloaded, the current limiter is active.
00025	Bypass voltage (average) is out of tolerance	
00027	Digital input 1	Restored the local network management interface-to-integrated environmental monitor (Universal I/O at Port 1) communication.
00028	Digital input 2	Restored the local network management interface-to-integrated environmental monitor (Universal I/O at Port 1) communication.
00035	Inverter fuse blown	One or more of the inverter fuses have blown (F021 on A071: X003:1). The inverter turns off. The system switches to bypass if possible or it shuts down.
00037	Aux 1 Error	Possibly one or more of the following: rectifier fuse blown, battery breaker (Q004) disconnected, DC earth fault (Option 1), Option 2..6, manual bypass switch.
00038	Fan inoperable	One or more fans are inoperable.
00039	High DC warning	The DC is above the high DC warning level.
00040	Inverter voltage out of tolerance	The inverter voltage before the static switch EA is about <85% of the reference voltage. If the inverter turns on or if system is in bypass operation the static switch EA is blocked.
00043	PSU1 AC/DC not working	A fault is detected in one of the two internal power supplies.

Modbus Read Coil Register List (Continued)

Coil Register	Parameter	Description
00048	Rectifier magnetics temp warning	The charger magnetic temperature is too high.
00049	High battery temperature[8]	The battery temperature is too high.
00050	Battery monitor warning[9]	
00051	Battery monitor alarm[9]	
00052	System locked in operation mode	The system is locked in an operation mode. The system was changing operation mode too frequently.
00054	Calibration stack entered by user	A login to the level 2 (configuration stack) occurred. Will not trigger a common alarm.
00055	Inverter PM block 1 (L1, L2, L3) temperature shutdown	A temperature shutdown alarm is active in one of the system inverter power modules.
00056	Charger temperature warning	A temperature warning is active in one of the system charger modules.
00057	Charger temperature shutdown	A temperature shutdown alarm is active in one of the system charger modules.
00058	Output voltage is out of tolerance	
00059	Static switch EA temperature warning or static switch EN temperature warning detected	One of the system static switch modules (EA or EN) has a temperature warning signal pending.
00060	Total DC current limit	The system charger operates in total DC current limit mode.
00061	AC capacitors CB03 current warning	The current in the AC capacitors is below the low warning limit value.
00063	No redundancy operation[10]	
00065	AC capacitors CB03 current shutdown	The current in the AC capacitors is below the low shutdown limit value.
00066	Mains out of tolerance	The rectifier mains is out of tolerance.
00068	Total DC current limit	The system charger is operating in total DC current limit mode.
00069	Charger temperature warning or shutdown	The temperature is to high in one of the system charger modules.

[8] Only available if optional battery temperature sensor is installed at the battery

[9] Only available if optional Gutor battery ABM is installed in the system.

[10] Only available for redundant systems.

Modbus Read Holding Register (Function Call 03)

The read holding register contains analogue information, the measured value from the parameters.

The data is stored as 16-bit unsigned integer, with the hexadecimal format FFFF of 4 digits. This corresponds to a numeric value between 0-65535.

The factor for all values is 1. This information can be used to trigger alarms, actions or other events.

NOTE: It is recommended that the delay poll is more than 10 seconds because the refresh rate of the register is about 10 seconds.

NOTE: All holding registers between 40001-40047 are reserved even if not listed in the table.

Modbus Read Holding Register List

Holding Register	Parameter [Unit of Measure]	Description
40001	**1–phase:** Output voltage L1 [V]	**1–phase:** Phase L1 to neutral.
	3–phase: Output voltage L1 [V]	**3–phase:** Phase L1 to phase L2.
40002[11]	**3–phase:** Output voltage L2 [V]	**3–phase:** Phase L2 to phase L3.
40003[11]	**3–phase:** Output voltage L3 [V]	**3–phase:** Phase L3 to phase L1.
40004	Input voltage L1 [V]	Phase L1 to phase L2.
40005	Input voltage L2 [V]	Phase L2 to phase L3.
40006	Input voltage L3 [V]	Phase L3 to phase L1.
40007	**1–phase:** Bypass voltage L1 [V]	**1–phase:** Phase L1 to neutral.
	3–phase: Bypass voltage L1 [V]	**3–phase:** Phase L1 to phase L2.
40008[11]	**3–phase:** Bypass voltage L2 [V]	**3–phase:** Phase L2 to phase L3.
40009[11]	**3–phase:** Bypass voltage L3 [V]	**3–phase:** Phase L3 to phase L1.
40010	Input current L1 [A]	
40011	Input current L2 [A]	
40012	Input current L3 [A]	
40013	Output current L1 [A]	
40014[11]	**3–phase:** Output current L2 [A]	
40015[11]	**3–phase:** Output current L3 [A]	
40016	Output peak current L1 [A]	
40017[11]	**3–phase:** Output peak current L2 [A]	
40018[11]	**3–phase:** Output peak current L3 [A]	
40019	Total DC current [A]	
40020	Battery current [A]	
40022	System operation mode	Value reflects the actual operation mode of the system: 1 = Standby. 2 = Charger only. 3 = Normal operation. 4 = Battery operation. 5 = Bypass operation. 6 = Hot standby. 7 = Economy operation. 8 = Battery test active.

[11] Only for three phase systems.

Modbus Read Holding Register List (Continued)

Holding Register	Parameter [Unit of Measure]	Description
40029	Battery voltage [V]	
40031	Active systems	1 = Single. 2 = Parallel.
40035	Battery temperature[12] [°C or °F]	Optional temperature sensor. Shows Fahrenheit or Celsius value depending on firmware setting. If the temperature sensor is not mounted this field will show a value of around 226!
40038	Output frequency [Hz]	The phase output frequency of the system.
40040	System load [%]	Percent of the output power capacity currently used.
40041	Battery time left[12] [minutes]	
40045	Firmware version first digit	The first digit in the firmware version for the NMC.
40046	Firmware version second digit	The second digit in the firmware version for the NMC.
40047	Firmware version third digit	The third digit in the firmware version for the NMC.

[12] Only available if optional Gutor battery ABM is installed in the system.

Modbus Wiring Diagrams

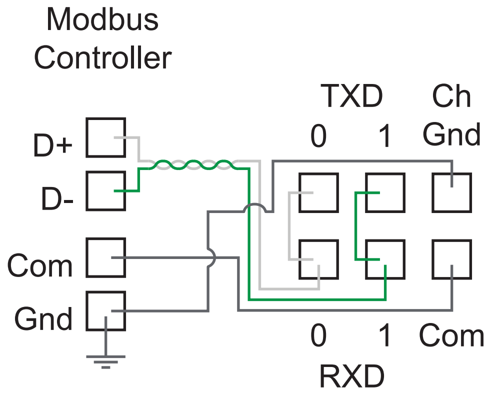
The Modbus wiring for the NMC in a Gutor system can be done either with a 2-wire or a 4-wire configuration.

IMPORTANT: Always follow local wiring codes.

NOTE: It is recommended to use 150 Ohm resistors at each end of the Modbus bus cable if the cable is over 300 m (1000 feet) using 19200 as baud rate or over 600 m (2000 feet) using 9600 as baud rate.

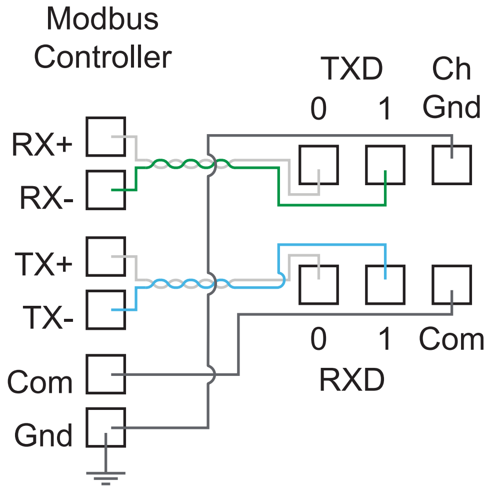
2-Wire Configuration

NOTE: Use shielded twisted pair cables.



4-Wire Configuration

NOTE: Use shielded twisted pair cables.



SNMP Access to the Network Management Card

SNMP is an internet standard protocol for IP networks. The NMC supports SNMPv1, SNMPv3 and SNMPv2c over SNMPv1.

With SNMP a Network Management System (NMS) can access the NMC by configuring a community (SNMPv1) or a user profile (SNMPv3). To view the traps a trap receiver also needs to be configured for the NMS.

Super users, administrators and network only users can configure the settings for SNMPv1 and SNMPv3 from the CLI or the web interface.

NOTE: Gutor system ignores any SET commands, only GET commands and traps can be used.

NOTE: Only for NMC AOS v6.8.0 and higher: Both SNMPv1 and SNMPv3 are disabled by default. There are no default settings available. The settings need to be defined before it is possible to enable the protocols.

SNMPv1 Access

SNMPv1 uses access communities to define what IP addresses on the network have access to the SNMP communication from the NMC.

SNMPv1 Access Communities

To use SNMPv1 an access community is used. Each access community has a community name, IP name or host name and an access type. It is possible to defined up to four different access communities.

- **The community name:** Used for access by a network management station (NMS). The maximum length of a community name is 15 ASCII characters.
- **The NMS IP/host name:** The IPv4 or IPv6 address, IP address mask, or host name that controls access by NMSs. A host name or a specific IP address (for example, 149.225.12.1) allows access only by the NMS at that location. IP addresses that contain 255 restrict access as follows:
  - 149.225.12.255: Access by NMS on the 149.225.12 segment.
  - 149.225.255.255: Access by NMS on the 149.225 segment.
  - 149.255.255.255: Access by NMS on the 149 segment.
  - 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by NMS on any segment.
- **The access type:** There are four different access types:
  - Read: GETS only, at any time
  - Write: GETS at any time, and SETS when no user is logged onto the UI or command line interface.
  - Write+: GETS and SETS at any time.
  - Disable: No GETS or SETS at any time.

Configure SNMPv1 from the CLI

1. Log in to the CLI.
2. To see the configuration options type `snmpV1 ?`.

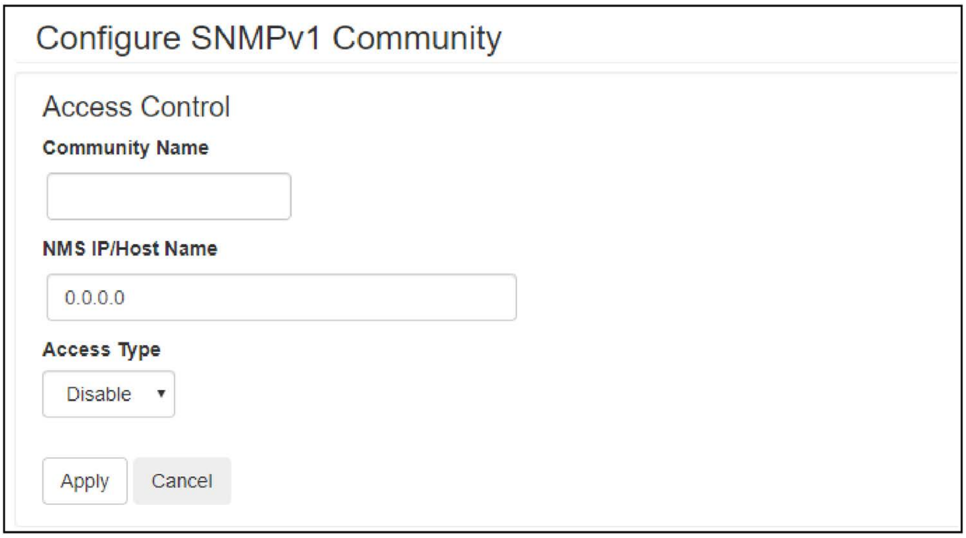
   NOTE: In the table `[n]` is the access community number 1, 2, 3 or 4.

Setting	Command	Argument	Description
Help	`?`		Shows the command help
SNMPv1 access	`-s`	`enable | disable`	Enables or disables SNMP version 1
Community name	`-c[n]`	`<Comunity Name>`	Specify a community name.
Community access type	`-a[n]`	`read | write | writeplus | disable`	Set the access type of a community.
Community IPv4/IPv6 address or host name	`-n[n]`	`<IP address> or <Host Name>`	Specify the IPv4/IPv6 address or the host name of community.

Configure SNMPv1 from the Web Interface

1. Log in to the web interface.
2. Navigate to **Configuration > Network > SNMPv1 > Access Control**.
3. Click on a community name to configure **Community Name**, **NMS IP/Host Name** and **Access Type**.
4. Click **Apply** to save any changes.

   NOTE: Reboot the NMC to apply changes. From the web interface select **Control > Network > Reset/Reboot** for options.



Configure SNMPv1 Community

Access Control

Community Name

NMS IP/Host Name: 0.0.0.0

Access Type: Disable

SNMPv3 Access

SNMPv3 uses user profiles to define what IP addresses on the network has access to the SNMP communication from the NMC. The settings for SNMPv3 can be configured from the CLI or the web interface.

SNMPv3 User Profiles

To use SNMPv3 a user profile needs to be defined. Each user profile has a user name, authentication setting and encryption setting. It is possible to defined up to four different user profiles.

- **The user name:** Used to identify the user profile. SNMPv3 checks that the user name is the same in the user profile and the data package being transmitted. The maximum length of a user name is 32 ASCII characters.
- **Authentication passphrase:** Provides the SNMPv3 communication with authentication. Checks that the NMS that communicates with the device is the NMS it claims to be. The authentication passphrase verifies that the message has not been changed during transmission. It also verifies that the transmission was not delayed, copied and then sent again. The length of a passphrase can be between 15-32 ASCII characters.
- **Privacy passphrase:** Provides the SNMPv3 communication with encryption. Ensures the privacy of the data sent with to and from an NMS. The length of a privacy passphrase can be between 15-32 ASCII characters.
- **Authentication protocol:** Use either SHA or MD5 as an authentication protocol.
- **Privacy protocol:** Use either AES or DES as a privacy protocol. For encryption of the SNMPv3 requests it is required to use both an authentication and a privacy protocol. To set a privacy protocol an authentication protocol must be selected.

Configure SNMPv3 from the CLI

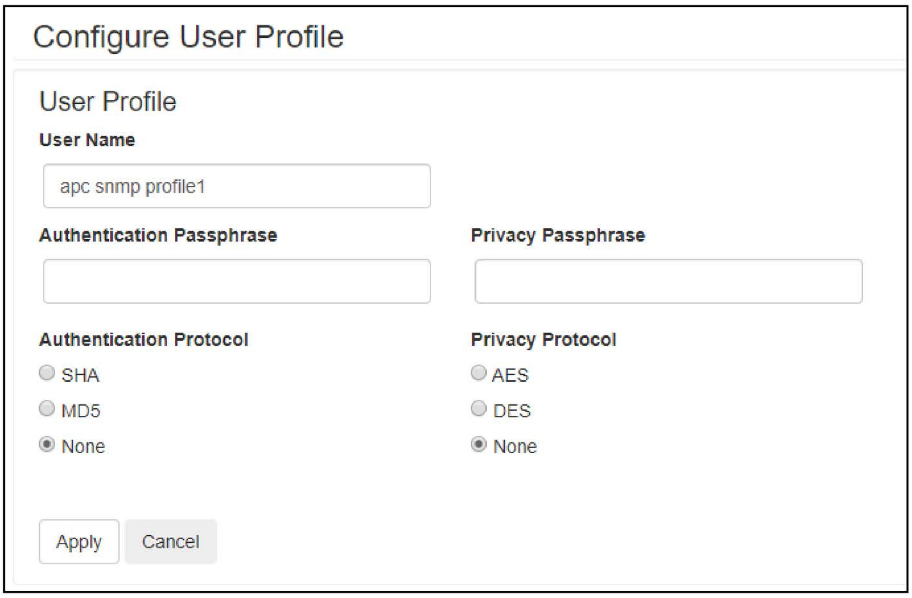
1. Log in to the CLI.
2. To see the configuration options type `snmpV3 ?`.

   NOTE: In the table `[n]` is the user name number 1, 2, 3 or 4.

Setting	Command	Argument	Description
Help	`?`		Shows the command help
SNMPv3 access	`-s`	`enable | disable`	Enables or disables SNMP version 3
User name	`-u[n]`	`<User Name>`	Set a user name.
Authentication phrase	`-a[n]`	`<Authentication Phrase>`	Set an authentication phrase.
Encryption phrase	`-c[n]`	`<Crypt Phrase>`	Set an encryption phrase.
Authentication protocol	`-ap[n]`	`sha | md5 | none`	Set the type of authentication protocol.
Privacy (encryption) protocol	`-pp[n]`	`eas | des | none`	Set the privacy (encryption) protocol.
Slave address	`-ac[n]`	`enable | disable`	Enable or disable access.
User Access	`-au[n]`	`<User Name>`	Give access to a user.
Set IPv4/IPv6 address or host name	`-n[n]`	`<IP address> or <Host Name>`	Set the IPv4/IPv6 address or the host name of the network management station.

Configure SNMPv3 from the Web Interface

1. Log in to the web interface.
2. Navigate to **Configuration > Network > SNMPv3 > User Profile**.
3. Click on a user name to view the settings for it.
4. Here it is possible to configure the **User Name**, **Authentication Passphrase**, **Authentication Protocol**, **Privacy Passphrase** and **Privacy Protocol**.



Configure User Profile

User Profile

User Name

apc snmp profile1

Authentication Passphrase

Privacy Passphrase

Authentication Protocol

○ SHA
○ MD5
● None

Privacy Protocol

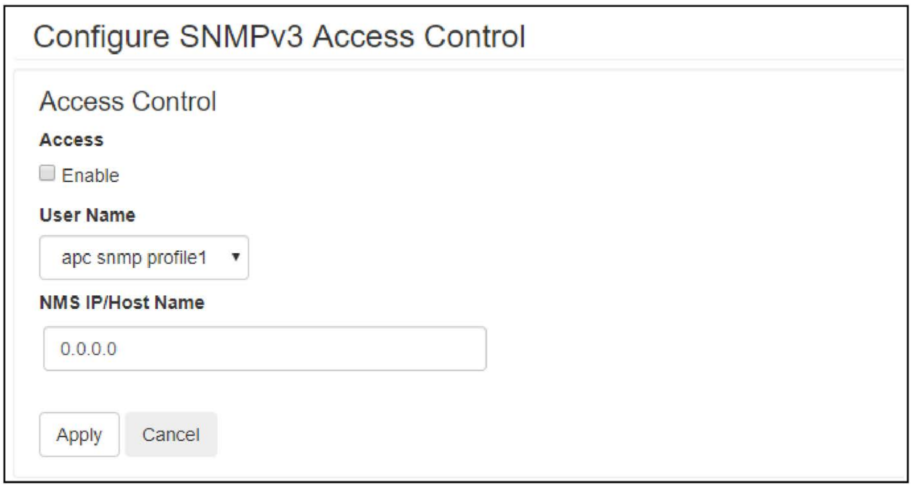
○ AES
○ DES
● None

Apply Cancel

5. Click **Apply** to save any changes.

   NOTE: Reboot the NMC to apply changes. From the web interface select **Control > Network > Reset/Reboot** for options.

6. Navigate to **Configuration > Network > SNMPv3 > Access Control**.
7. Click on a user name to view the settings for it.
8. Here it is possible to enable **Access** and configure the **NMS IP/Host Name** for the selected **User Name**. Use the drop-down menu to change **User Name** to configure.



Configure SNMPv3 Access Control

Access Control

Access

□ Enable

User Name

apc snmp profile1 ▾

NMS IP/Host Name

0.0.0.0

Apply Cancel

9. Click **Apply** to save any changes.

   NOTE: Reboot the NMC to apply changes. From the web interface select **Control > Network > Reset/Reboot** for options.

SNMP Trap Receiver

A SNMP trap receiver needs to be configured to receive the SNMP traps from the NMC in a Gutor system. Up to six trap receivers can be added for each NMC.

Super users, administrators and device users can add and configure SNMP traps from the CLI and the web interface.

Add and Configure SNMP Trap Receivers from the CLI

1. Log in to the CLI.
2. To see the configuration options type `snmptrap ?`.

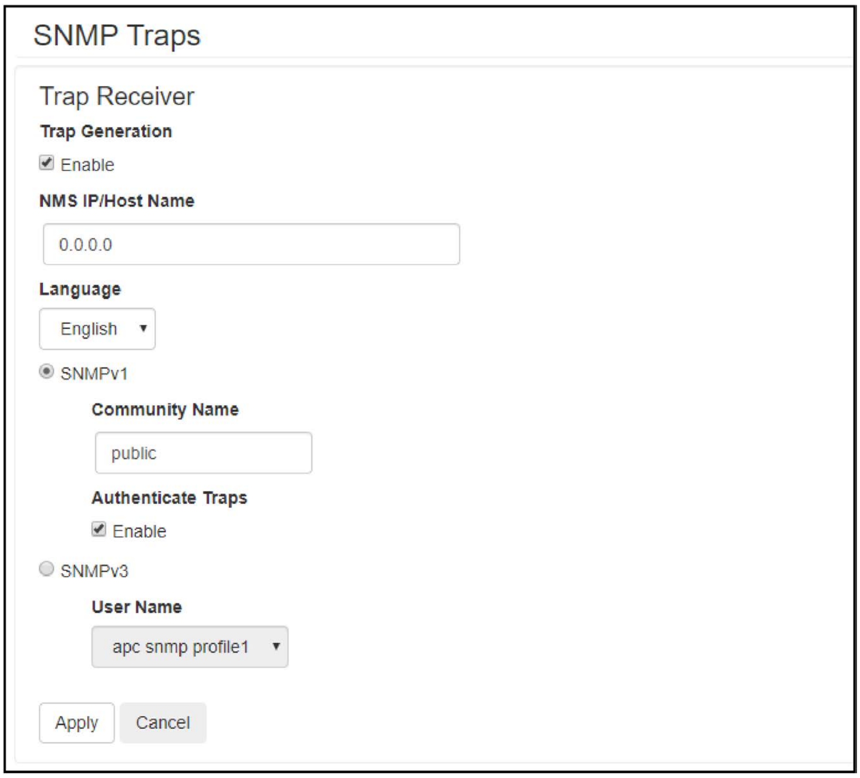
   NOTE: In the table `[n]` is the number of the trap receiver (1–6).

Setting	Command	Argument	Description
Community	`-c[n]`	`<Comunity Name>`	Select what SNMPv1 community name to use
Receiver NMS IP	`-r[n]`	`<IP address>`	Set the IP address for the trap receiver
Trap Type	`-t[n]`	`snmpV1 | snmpV3`	Select if the trap receiver should use SNMPv1 or SNMPv3
Generation	`-g[n]`	`enable | disable`	Enable or disable trap generation
Auth Traps	`-a[n]`	`enable | disable`	Enable or disable trap authentication for SNMPv1
User Name	`-u[n]`	`profile1 | profile2 | profile3 | profile4`	Select what SNMPv3 user name to use

3. For example, to set the trap receiver number 1 to an IP address of 255.255.255.255 using SNMPv3 and the user name for profile1 type: `snmptrap -r1 255.255.255.255 -t1 snmpV3 -u1 profile1 -g1 enable` and press **Enter**.
4. If the SNMP trap command was entered correctly a `Success` response is displayed, indicating that the SNMP trap was created with the chosen settings.

Add and Configure SNMP Trap Receivers from the Web Interface

1. Log in to the web interface.
2. Navigate to **Configuration > Notification > SNMP Traps > Trap Receivers**.
3. Here a list of the current trap receivers is displayed, if there are any. To configure an existing trap receiver, click on the NMS IP/host name.
4. To add a new trap receiver:
   a. Click **Add Trap Receiver**. Here the settings for the SNMP trap can be configured.



SNMP Traps

Trap Receiver

Trap Generation

☑ Enable

NMS IP/Host Name: 0.0.0.0

Language: English ▾

● SNMPv1

Community Name: public

Authenticate Traps

☑ Enable

○ SNMPv3

User Name: apc snmp profile1 ▾

   b. Check the **Enable** box under trap generation.
   c. Specify the IP address of the trap receiver under **NMS IP/Host Name**.
   d. Select either SNMPv1 or SNMPv3 to use. For SNMPv1 select the community name to use and select if the traps should use authentication. For SNMPv3 select the user name that should be used.
   e. Click **Apply** to save any changes.

SNMP Trap OIDs

Any active traps can be view from a management information base (MIB) browser with correctly configured trap receiver connected to the NMC.

The following table shows the different traps that can be sent out from the NMC when triggered. The NMC will only send out the traps that are currently triggered in the system.

NOTE: Base OID Address for APC / Gutor: 1.3.6.1.4.1.318.

SNMP Trap OID List

SNMP Trap OID Name	Trap ID	Specific Sub Trap ID	Severity	Event Text
communicationLost	1	—	Informational	UPS: Lost the local network management interface-to-UPS communication.
upsOverload	2	—	Critical	UPS: Inverter overload or output overload detected.
upsOnBattery	5	—	Warning	UPS: Battery operation detected.
lowBattery	7	—	Critical	UPS: Low DC voltage warning detected.
communicationEstablished	8	—	Informational	UPS: Communication established.
powerRestored	9	—	Informational	UPS: Utility power restored.
returnFromLowBattery	11	—	Informational	UPS: Low DC voltage warning cleared.
upsBatteryNeedsReplacement	17	—	Critical	UPS: Battery needs replacement.
switchedBypass	22	—	Warning	UPS: Static bypass operation or system set to manual bypass detected.
returnFromBypass	23	—	Informational	UPS: Static bypass operation or system set to manual bypass cleared.
upsOverloadCleared	33	—	Informational	UPS: Inverter overload or output overload cleared.
upsBatteryReplaced	36	—	Informational	UPS: Bad battery condition cleared.
abnormalCondition	77	15	Critical	UPS: Bypass is out of tolerance detected.
abnormalCondition	77	43	Critical	UPS: Output is out of tolerance detected.
abnormalCondition	77	45	Critical	UPS: Inverter not synchronized to bypass line detected.
abnormalCondition	77	47	Critical	UPS: Battery breaker open detected.
abnormalCondition	77	49	Critical	UPS: High DC voltage shutdown detected.
abnormalCondition	77	71	Critical	UPS: Fan inoperable detected.
abnormalCondition	77	73	Critical	UPS: High DC voltage warning detected.
abnormalCondition	77	75	Critical	UPS: Inverter voltage is out of tolerance detected.
abnormalCondition	77	81	Critical	UPS: PSU1 AC or DC is not working detected.
abnormalCondition	77	93	Critical	UPS: Battery temperature warning detected.
abnormalCondition	77	99	Critical	UPS: System is locked in operation mode detected.
abnormalCondition	77	129	Critical	UPS: Inverter fuse blown detected.
abnormalCondition	77	133	Critical	UPS: Aux 1 error detected.
abnormalCondition	77	155	Critical	UPS: Rectifier magnetics temperature warning detected.
abnormalCondition	77	159	Critical	UPS: Battery monitor warning detected.
abnormalCondition	77	161	Critical	UPS: Battery monitor alarm detected.
abnormalCondition	77	169	Critical	UPS: Inverter PM block 1 (L1, L2 or L3) temperature shutdown detected.
abnormalCondition	77	171	Critical	UPS: Charger 0 degree or 30 degrees temperature warning detected.

SNMP Trap OID List (Continued)

SNMP Trap OID Name	Trap ID	Specific Sub Trap ID	Severity	Event Text
abnormalCondition	77	173	Critical	UPS: Charger 0 degree or 30 degrees temperature shutdown detected.
abnormalCondition	77	175	Critical	UPS: High output voltage detected.
abnormalCondition	77	177	Critical	UPS: Static switch EA temperature warning or static switch EN temperature warning detected.
abnormalCondition	77	181	Critical	PS: AC capacitors CB03 current warning detected.
abnormalCondition	77	185	Critical	UPS: No redundancy operation detected.
abnormalCondition	77	187	Critical	UPS: FPU-MPU communication inoperable detected.
abnormalCondition	77	189	Critical	UPS: AC capacitors CB03 current shutdown detected.
abnormalConditionCleared	78	16	Informational	UPS: Bypass is out of tolerance cleared.
abnormalConditionCleared	78	44	Informational	UPS: Output is out of tolerance cleared.
abnormalConditionCleared	78	46	Informational	UPS: Inverter not synchronized to bypass line cleared.
abnormalConditionCleared	78	48	Informational	UPS: Battery breaker open cleared.
abnormalConditionCleared	78	50	Informational	UPS: High DC voltage shutdown cleared.
abnormalConditionCleared	78	72	Informational	UPS: Fan inoperable cleared.
abnormalConditionCleared	78	74	Informational	UPS: High DC voltage warning cleared.
abnormalConditionCleared	78	76	Informational	UPS: Inverter voltage is out of tolerance cleared.
abnormalConditionCleared	78	82	Informational	UPS: PSU1 AC or DC is not working cleared
abnormalConditionCleared	78	94	Informational	UPS: Battery temperature warning cleared.
abnormalConditionCleared	78	100	Informational	UPS: System is locked in operation mode cleared.
abnormalConditionCleared	78	130	Informational	UPS: Inverter fuse blown cleared.
abnormalConditionCleared	78	134	Informational	UPS: Aux 1 error cleared.
abnormalConditionCleared	78	156	Informational	UPS: Rectifier magnetics temperature warning cleared.
abnormalConditionCleared	78	160	Informational	UPS: Battery monitor warning cleared.
abnormalConditionCleared	78	162	Informational	UPS: Battery monitor alarm cleared.
abnormalConditionCleared	78	170	Informational	UPS: Inverter PM block 1 (L1, L2 or L3) temperature shutdown cleared.
abnormalConditionCleared	78	172	Informational	UPS: Charger 0 degree or 30 degrees temperature warning cleared.
abnormalConditionCleared	78	174	Informational	UPS: Charger 0 degree or 30 degrees temperature shutdown cleared.
abnormalConditionCleared	78	176	Informational	UPS: High output voltage cleared.
abnormalConditionCleared	78	178	Informational	UPS: Static switch EA temperature warning or static switch EN temperature warning cleared.
abnormalConditionCleared	78	182	Informational	UPS: AC capacitors CB03 current warning cleared.
abnormalConditionCleared	78	186	Informational	UPS: No redundancy operation cleared.
abnormalConditionCleared	78	188	Informational	UPS: FPU-MPU communication inoperable cleared.
abnormalConditionCleared	78	190	Informational	UPS: AC capacitors CB03 current shutdown cleared.
upsInternalOverTemperature	353	—	Warning	UPS: Over temperature violation on inverter magnetics, inverter power modules or static switches EA or EN detected.
upsInternalOverTemperatureCleared	354	—	Informational	UPS: Over temperature violation on inverter magnetics, inverter power modules or static switches EA or EN cleared.

SNMP Trap OID List (Continued)

SNMP Trap OID Name	Trap ID	Specific Sub Trap ID	Severity	Event Text
upsWarningCondition	736	—	Warning	UPS: Shutdown condition.
upsWarningConditionCleared	737	—	Informational	UPS: Shutdown condition cleared.
upsInformationalCondition	738	—	Informational	UPS: In hot standby mode.
upsInformationalConditionCleared	739	—	Informational	UPS: No longer in hot standby mode.

SNMP GET OIDs

There are several object identifiers (OID) available from the system via SNMP from the network management card (NMC). The OIDs needs to be requested with a GET from a MIB browser with correctly configured access to the NMC. The OIDs can show both analogue and digital values, see respective section.

Analogue Values from OIDs

The following table shows the analog values that are available as GET requests.

NOTE: Base OID Address for APC / Gutor: .1.3.6.1.4.1.318.

NOTE: If an OID is not supported for the system the displayed value will be -1 (or if the OID returns a string instead of an integer it will display "NOT SUPPORTED").

Parameter [Unit of Measure]	SNMP OID Name	APC / Gutor OID Address	Notes
General			
Model name	upsBasicIdentModel	1.1.1.1.1.1	
System name	upsBasicIdentName	1.1.1.1.1.2	
Model type	upsBasicIdentModelType	1.1.1.1.1.4	
Serial number	upsAdvIdentSerialNumber	1.1.1.1.2.3	
Last battery replacement	upsBasicBatteryLastReplaceDate	1.1.1.2.1.3	
System mode	upsBasicOutputStatus	1.1.1.4.1.1	
Number of parallel units	upsParallelSysRemoteAddress	1.1.1.14.2	
Input			
Input voltage orientation	upsPhaseInputVoltageOrientation	1.1.1.9.2.2.1.3	
Input type	upsPhaseInputType	1.1.1.9.2.2.1.5	
Input voltage (phase-to-phase) [V]	upsPhaseInputVoltage	1.1.1.9.2.3.1.3	Index based (1.1.1-1.1.3)
Bypass input voltage (phase-to-phase) [V]	upsPhaseInputVoltage	1.1.1.9.2.3.1.3	Index based for three phase systems (2.1.1-2.1.3)
Input maximum voltage (phase-to-phase) [V]	upsPhaseInputMaxVoltage	1.1.1.9.2.3.1.4	Index based (1.1.1-1.1.3)
Input minimum voltage (phase-to-phase) [V]	upsPhaseInputMinVoltage	1.1.1.9.2.3.1.5	Index based (1.1.1-1.1.3)
Input current (phase-to-neutral) [A]	upsPhaseInputCurrent	1.1.1.9.2.3.1.6	Index based (1.1.1-1.1.3)
Output			
System load [%]	upsAdvOutputLoad	1.1.1.4.2.3	
Peak current (phase-to-neutral) [A]	upsAdvOutputPeakCurrent	1.1.1.4.2.10.1.2	Index based for three phase systems (1.1.1-1.1.3)
Output frequency [Hz]	upsPhaseOutputFrequency	1.1.1.9.3.2.1.4	
Output voltage (phase-to-neutral/phase) [V]	upsPhaseOutputVoltage	1.1.1.9.3.3.1.3	Index based for three phase systems (1.1.1-1.1.3)
Current (phase-to-neutral) [A]	upsPhaseOutputCurrent	1.1.1.9.3.3.1.4	Index based for three phase systems (1.1.1-1.1.3)
Battery			
Battery status	upsBasicBatteryStatus	1.1.1.2.1.1	
Battery temperature [°C or °F]	upsAdvBatteryTemperature	1.1.1.2.2.2	
Battery time left [minutes]	upsAdvBatteryRunTimeRemaining	1.1.1.2.2.3	
Battery voltage [V]	upsAdvBatteryActualVoltage	1.1.1.2.2.8	

Parameter [Unit of Measure]	SNMP OID Name	APC / Gutor OID Address	Notes
Battery current [A]	upsAdvBatteryCurrent	1.1.1.2.2.9	
Total DC current [A]	upsAdvTotalDCCurrent	1.1.1.2.2.10	

Digital Values from OIDs

There are some specific OIDs that generate a string of zeros and ones, where certain positions in the string indicates an alarm. For details see the table for the respective OID.

The first (left most) character have the position 1, the last (right most) character have the position 64. For example, if the OID 1.1.1.11.2.1 have the string ‘0000000100 0000000000 0000000000 0000000000 0000000000 0000000000 0000’ it would indicate that the bypass voltage out of range, since the character position 8 has the value 1.

> **NOTE:** The spaces in the string is only shown to make it easier to read in the example, the string value from the SNMP OID does not contain any spaces.
>
> **NOTE:** Only the descriptions for the character positions that are relevant for the system type are shown. The same OID can be used for multiple systems types.

OID Address: 1.1.1.11.2.1 / OID Name: upsAdvStateAbnormalConditions

Character Position	Parameter	Notes
8	Bypass voltage (average) is out of tolerance	
22	Output is out of tolerance detected	Indicates that the output voltage of the UPS is out of tolerance. The system will transfer to bypass if the bypass mains is within tolerance, if not the system will shut down.
23	Inverter not synchronized to bypass	
25	High DC warning	The DC is above the high DC warning level.
26	Common alarm	The common alarm is active in the system.

OID Address: 1.1.1.11.2.3 / OID Name: upsAdvStateDP300ESpecificFaults

Character Position	Parameter	Notes
1	Mains out of tolerance	The rectifier mains is out of tolerance.
2	AC capacitors CB03 current shutdown	The current in the AC capacitors is below the low shutdown limit value.
3	Internal serial error	An internal serial error within the systems control electronic has occurred.
4	No redundancy operation	
6	AC capacitors CB03 current warning	The current in the AC capacitors is below the low warning limit value.
7	Total DC current limit	The system charger is operating in total DC current limit mode.
8	Static switch EA temperature warning or static switch EN temperature warning detected	One of the system static switch modules (EA or EN) has a temperature warning signal pending.
9	Output voltage is out of tolerance	
10	Charger temperature shutdown	A temperature shutdown alarm is active in one of the system charger modules.

OID Address: 1.1.1.11.2.3 / OID Name: upsAdvStateDP300ESpecificFaults (Continued)

Character Position	Parameter	Notes
11	Charger temperature warning	A temperature warning is active in one of the system charger modules.
12	Inverter PM block 1 (L1, L2, L3) temperature shutdown	A temperature shutdown alarm is active in one of the system inverter power modules.
16	Battery monitor alarm[13]	
17	Battery monitor warning[13]	
19	Rectifier magnetics temp warning	The temperature on the charger magnetic is too high.
30	Aux 1 Error	Possibly one or more of the following: rectifier fuse blown, battery breaker (Q004) disconnected, DC earth fault (Option 1), Option 2..6, manual bypass switch.
32	Inverter fuse blown	One or more of the inverter fuses have blown (F021 on A071: X003:1). The inverter turns off. The system switches to bypass if possible or it shuts down.
47	System locked in operation mode	The system is locked in an operation mode. The system was changing operation mode too frequently.
50	High battery temperature	The battery temperature is too high.
56	PSU1 AC/DC not working	One of the two internal power supplies has a fault.
59	Inverter voltage out of tolerance	The inverter voltage before the static switch EA is about <85% of the reference voltage. If the inverter turns on or if system is in bypass operation the static switch EA is blocked.
61	Fan inoperable	One or more fans are inoperable.

[13] Only available if optional Gutor battery ABM is installed in the system.

Troubleshooting for the Network Management Card

Troubleshooting for NMC Access

Problem	Solution
Unable to ping the NMC	If the NMC's status LED is green and the link LED is flashing, try to ping another node on the same network segment as the NMC. If that does not work, try the following: • Verify if the TCP/IP setting configuration of the NMC is set manually or obtained through DHCP or BOOTP. • Verify the number of the subnet bits set for the NMC's subnet mask. • Check any VLAN, firewall, or proxy configurations. Check the NMC status and system info through the local serial interface. If the NMC's status LED is not solid green and/or the link LED is not flashing, perform the following checks: • Verify that the NMC is properly connected in the system. • Check that the Ethernet cable is connected securely to your network and the NMC. If there is an issue with the Ethernet cable, try a second cable. • Verify that the network device (switch) port the NMC is connected to is not disabled, or that the port speed is set incorrectly. • Check that your network DHCP or BOOTP server is active.
Cannot allocate the communications port through a terminal program	Before you can use a terminal program to configure the NMC, you must shut down any application, service, or program using the communications port.
Cannot access the command line interface through a serial connection	• Verify that the NMC LEDs are illuminated and the NMC is powered on. • Make sure that you did not change the baud rate. Try 2400, 9600, 19200, or 38400. • Check your PC's COM port configuration. • Make sure the port is not already in use. • Verify that the serial cable is firmly attached to the NMC and PC. • Verify that the cable part number being used is compatible. • Verify that **Scroll Lock** is not disabled on your keyboard.
Cannot access the command line interface remotely	• Make sure you are using the correct access method, Telnet or Secure SHell (SSH). An Administrator can enable these access methods. By default, Telnet is disabled. • For SSH, the NMC may be creating a host key. The NMC can take up to one minute to create the host key, and SSH is inaccessible for that time.
Cannot access the web interface	• Verify that HTTP or HTTPS access is enabled and configured correctly. • Make sure you are specifying the correct URL, that is consistent with the security system used by the NMC. SSL requires HTTPS, not HTTP, at the beginning of the URL. • Verify that you can ping the NMC. • Verify that you are using a supported web browser. • If the NMC has just restarted and SSL security is being set up, the NMC may be generating a server certificate. The NMC can take up to one minute to create this certificate, and the SSL server is not available during that time.

Troubleshooting for NMC SNMP

Problem	Solution
Unable to perform a GET	• Check the read (GET) community name (SNMPv1) or the user profile configuration (SNMPv3). • Use the CLI or the web interface to make sure that the NMS has access.
Unable to perform a SET	• Check the read/write (SET) community name (SNMPv1) or the user profile configuration (SNMPv3). • Use the command line interface or UI to ensure that the NMS has write (SET) access (SNMPv1) or is granted access to the target IP address through the access control list (SNMPv3).
Unable to receive traps at the NMS	• Make sure the trap type (SNMPv1 or SNMPv3) is correctly configured for the NMS as a trap receiver. • For SNMP v1, query the mconfigTrapReceiverTable MIB OID to verify that the NMS IP address is listed correctly, and that the community name defined for the NMS matches the community name in the table. If either is not correct, use SETs to the mconfigTrapReceiverTable OIDs, or use the CLI or web interface to correct the trap receiver definition. • For SNMPv3, check the user profile configuration for the NMS, and run a trap test.
Traps received at an NMS are not identified	See your NMS documentation to verify that the traps are properly integrated in the alarm/trap database.

Printed in:
Gutor Electronic LLC
Hardstrasse 72–74
5430 Wettingen, Switzerland
P +41 (0)56 437 34 34
F +41 (0)56 437 34 21

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.schneider-electric.com

As standards, specifications, and design change from time to time,
please ask for confirmation of the information given in this publication.