Network Monitoring System

Gutor PXP

User Guide

With the network management card AP9635 with AOS v7.0.4 and APP v7.0.4
11/2021 Version 4

https://www.se.com/ww/en/brands/gutor/

Legal Information

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.

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.

NOTICE

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

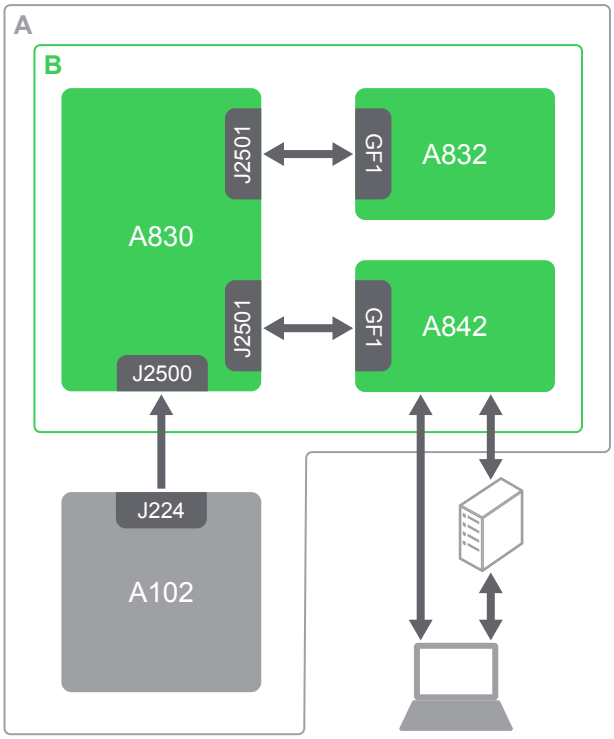
General Information

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.

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.



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.
A102	Controller box	The controller box sends information and status changes in the system to the communication interface.
A830	Communication interface	Connects directly to the network management cards.
A842	Network management card (NMC)	Offers secure local and/or remote monitoring of Gutor systems.
A832	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.

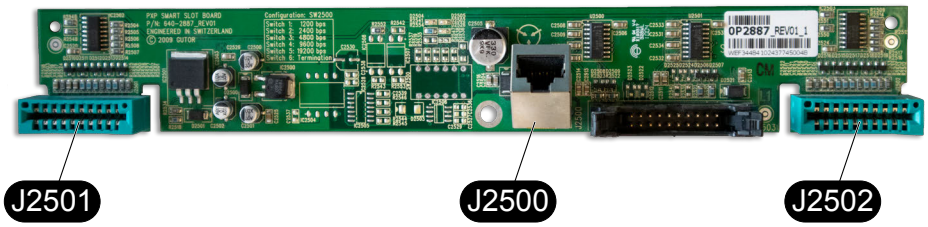
Hardware of the Network Management System

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 box to the network management cards. The communication interface has two edge connector slots **(J2501)** and **(J2502)** where the NMC edge connector **(GF1)** can be inserted.

The input port **(J2500)** connects to the port **(J224)** on the controller box **(A102)** with a 8P8C. Both the incoming and outgoing communication is according to the RS-232 standard using the UPS-Link protocol.

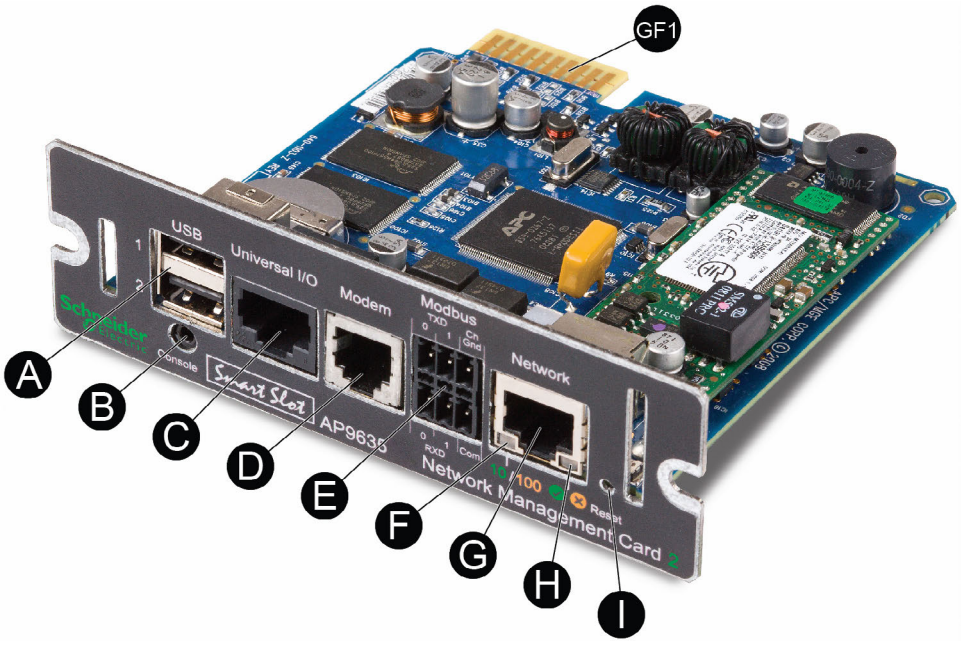


Ports	Port Standard	Connector	Communication Protocol
J2501, J2502 (outputs)	RS-232	Edge connector	UPS-Link[1]
J2500 (input)	RS-232	8P8C	UPS-Link[1]

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.



1. For more information about the UPS-link protocol see How to download and use the APC UPS-Link Protocol Language

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[2]	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 11.
(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 10.
(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.

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 57 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.

2. Gutor does not recommend using the port and does not provide support for the port/connection.

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 57 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 13.
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 serial port on the NMC or the serial port on an optional NMC 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.

NOTE: The CLI is only available in English.

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 15
- Remote access, page 16

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 16 and Command Line Interface Commands, page 17. For information on how to change the IP address see How to Change the IP Address from the CLI, page 19.
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 18. 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      vX.X.X
(c) Copyright 2019 All Rights Reserved  Gutor UPS PXP & PXC APP          vX.X.X
------------------------------------------------------------------------------
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 Minute                     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`[3].

   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.

3. 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.

NOTE: The web interface is only available in English.

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.

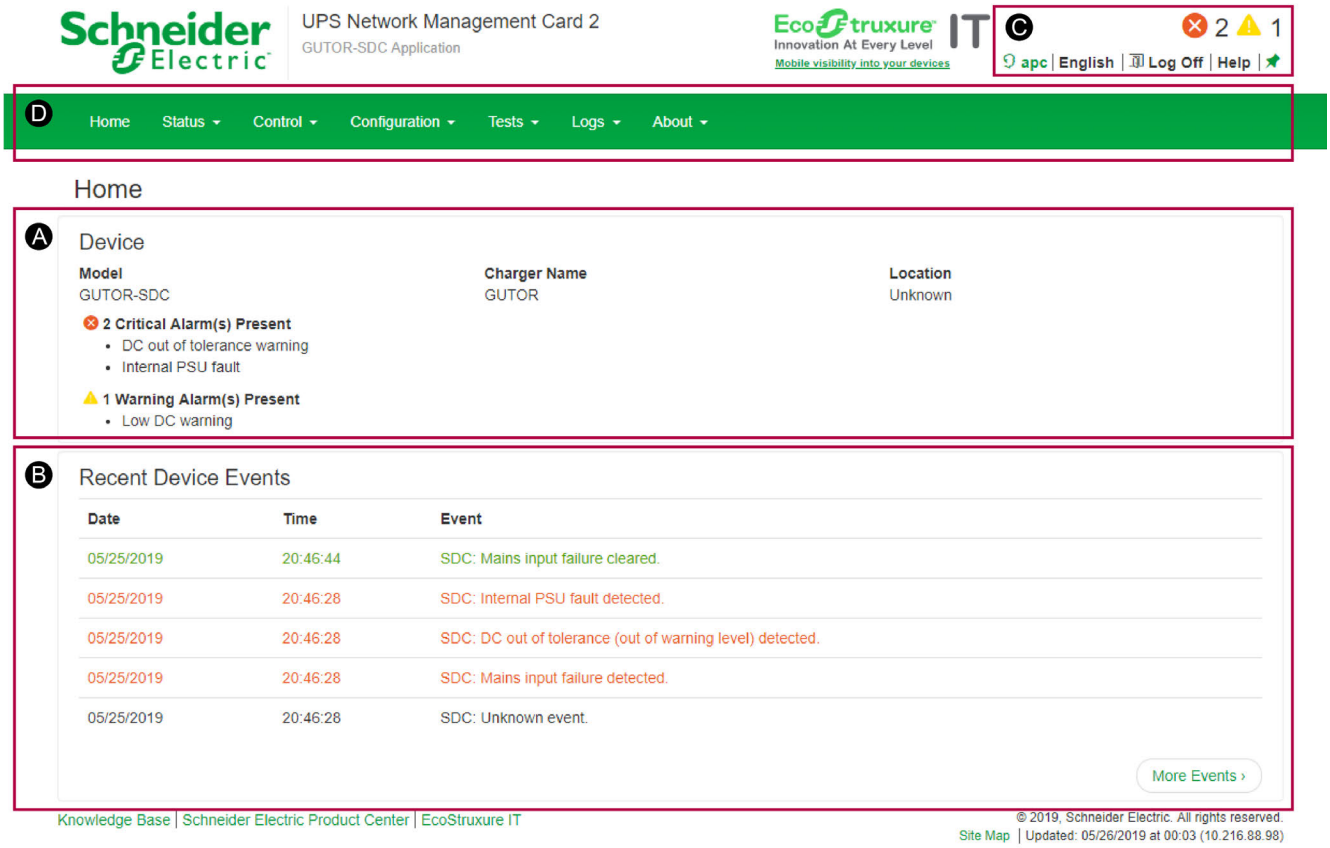
Example NMC Identifier	URL Example
With an NMC DNS name that is nmcdnsname	`https://nmcdnsname`
With an NMC IP address of 139.225.6.133	`https://139.225.6.133`
With an NMC IP address of 139.225.6.133 and specified port of :5000	`https://139.225.6.133:5000`
With an NMC IPv6 address of 2001:db8:1::2c0:b7ff:fe00:1100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



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:

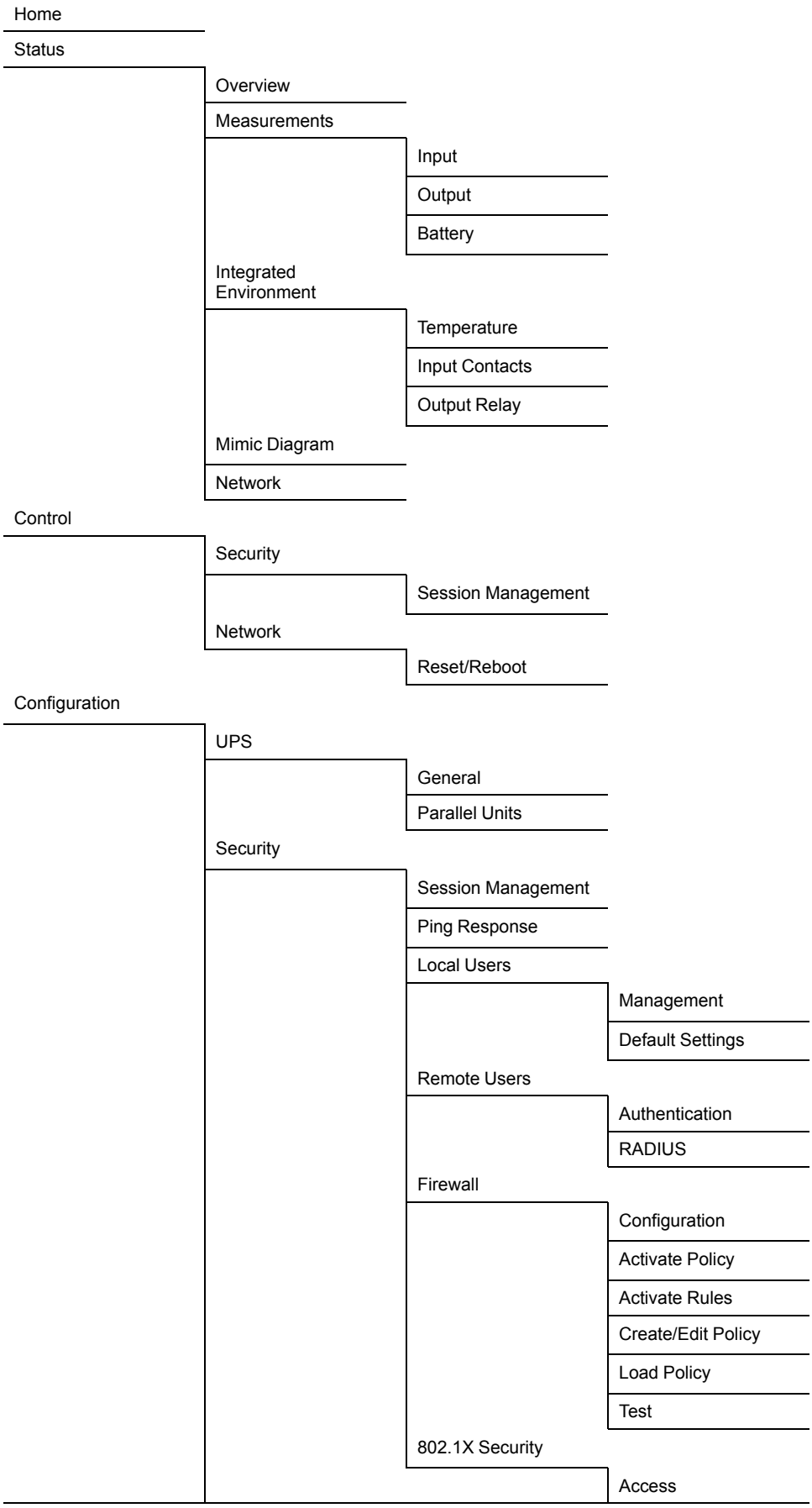
- **Home:** Returns the user to the **Home** page.
- **Status:** Sub menus for status and measurements from the system, sensors and network.
- **Control:** See current login sessions and reset network settings.
- **Configuration:** Configure system information and sensor, security, network and notification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

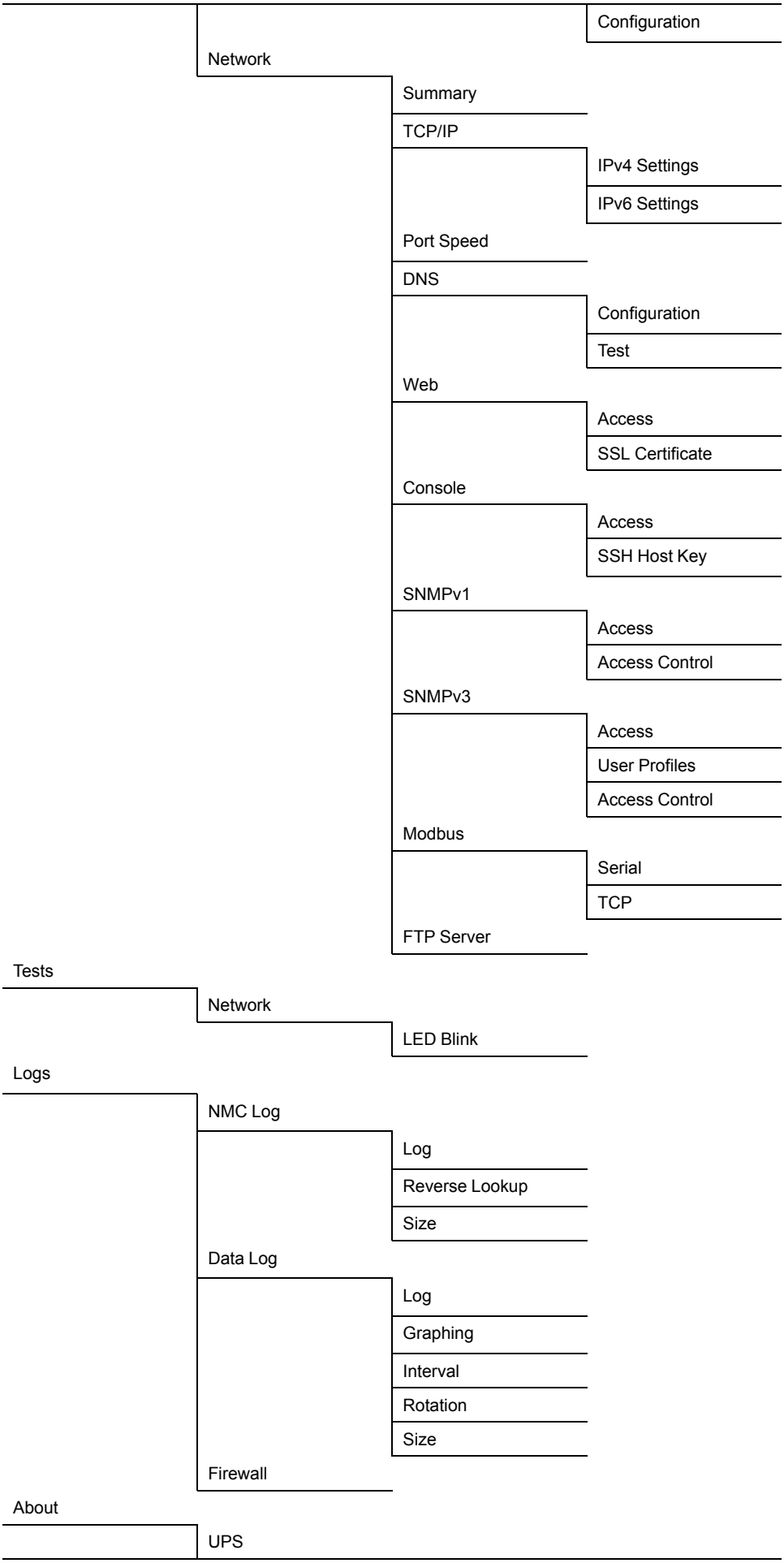
  NOTE: By default the size of the event log and data log is set to 400 entries (maximum 1500 entries).
- **About:** View the information about the system, network settings and firmware. Contains information for troubleshooting.

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.




Configuration
Network
Summary
TCP/IP
IPv4 Settings
IPv6 Settings
Port Speed
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 26
- Enable SCP from the CLI, page 26
- Enable FTP from the Web Interface, page 27
- Enable SCP from the Web Interface, page 27

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.

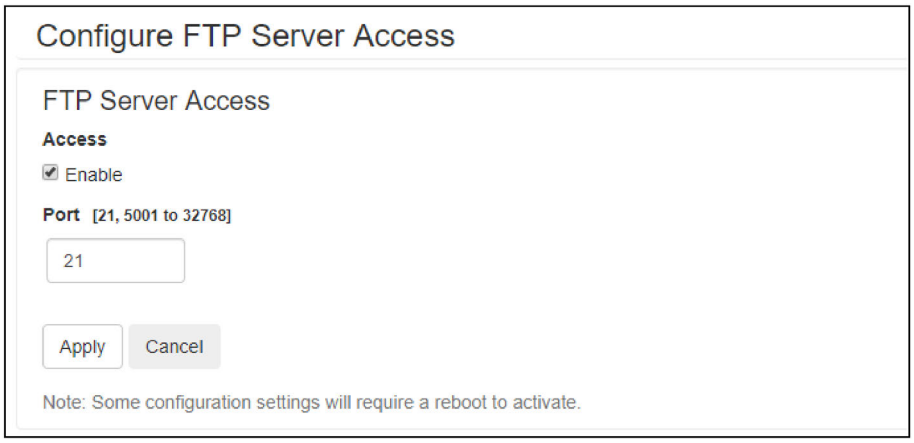
   NOTE: Use a specified SSH port, instead of the default, to increase security.
5. SCP is now enabled.

   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.



4. FTP is now enabled.

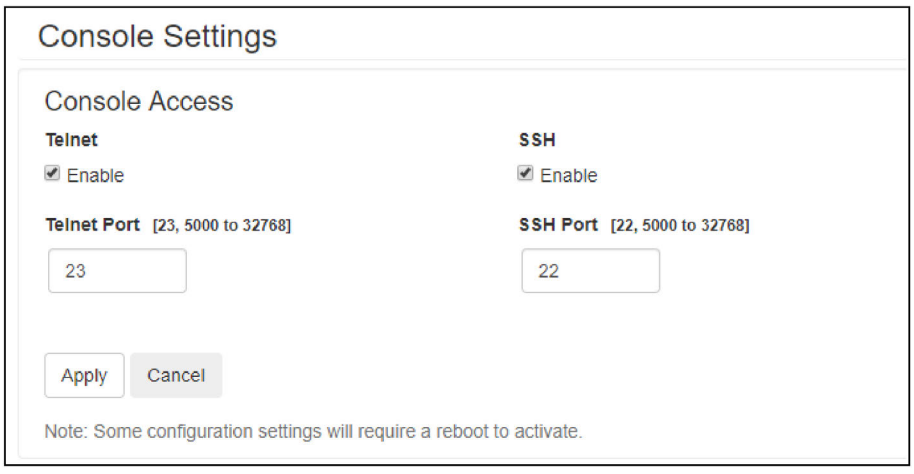
   NOTE: Reboot the NMC to apply changes. From the web interface select **Control > Network > Reset/Reboot** for options.

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.



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_pxc_692.bin`
APC operating system (AOS)	Can be thought of as the operating system of the NMC	`apc_hw5_aos_692.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_pxc_`*`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

There are two types of logs available, the event log (also called NMC log) and the data log. They can also be downloaded through the web interface.

NOTE: By default the size of the event log and data log is set to 400 entries (maximum 1500 entries).

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 should be wired with full duplex over a 4-wire bus.

For more details about the wiring of the Modbus serial, see Modbus Wiring Diagrams, page 39.

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 31
- Configure Modbus Serial from the Web Interface, page 32
- Configure Modbus TCP from the Web Interface, page 33

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

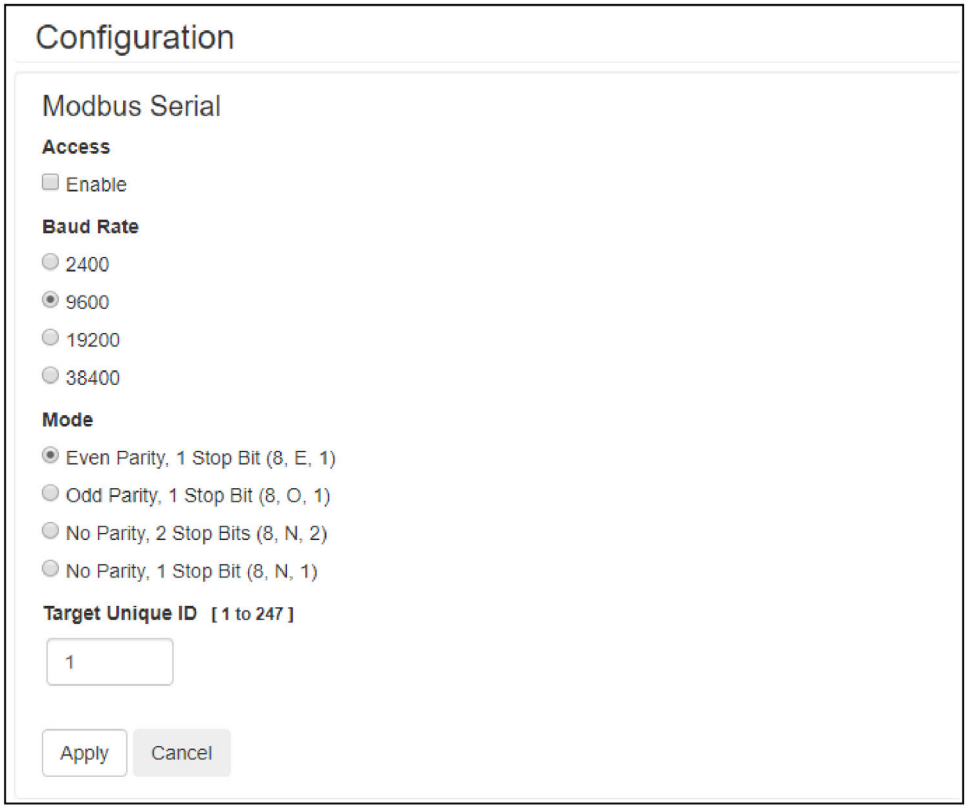
1. Log in to the CLI.
2. To see the configuration options type `modbus ?`.

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.

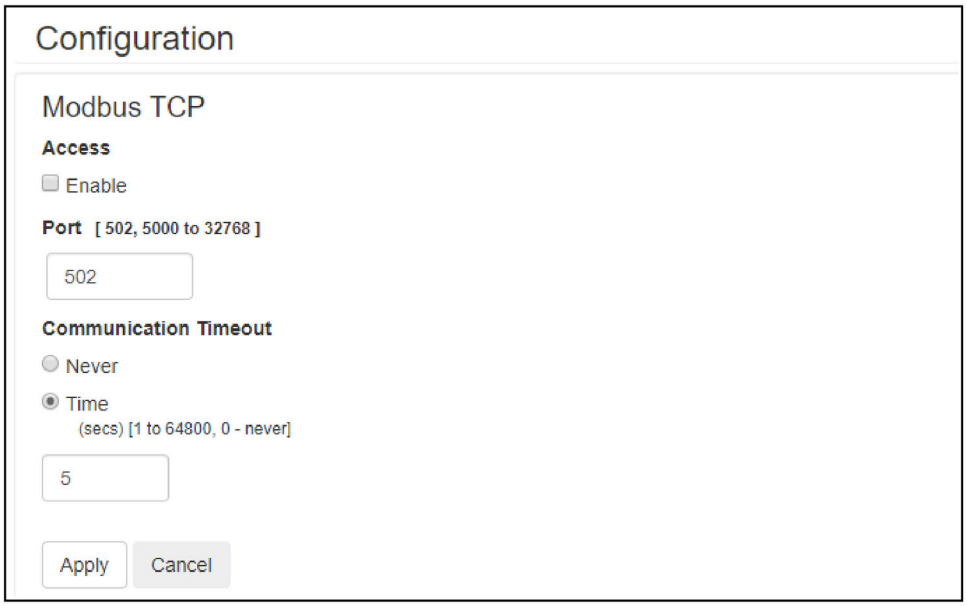
   NOTE: Reboot the NMC to apply changes. From the web interface select **Control > Network > Reset/Reboot** for options.



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.



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.

Modbus Read Coil Register List

Coil Register	Parameter	Description
00023	System switched on	The system is switched on.
00024	Standby	1 = the system is in standby operation.
00025	Normal operation	1 = the system is in normal operation.
00026	Battery operation	1 = the system is in battery operation.
00027	Bypass operation	Static bypass is switched on.
00028	Initial charge	The battery charger has been set to initial charge mode. The batteries are charged with an initial charge voltage.
00029	Float charge	The battery charger has been set to float charge state. The batteries are charged with a float charge voltage.
00030	Boost charge	The battery charger has been set to boost charge mode. The batteries are charged with a boost charge voltage.
00031	Cyclic charge	The battery charger has been set to cyclic charge mode. The batteries are charged with a cyclic charge voltage.
00039	Temporary static bypass	The system is in static bypass operation due to a fault.
00040	Requested static bypass	The system is in static bypass operation due to a user request.
00041	SBS inoperable	SBS inoperable.
00054	Q001 closed	The rectifier mains input switch Q001 is closed.
00056	Q201 closed	The battery switch Q201 is closed.
00057	Q501 closed	The bypass mains input switch Q501 is closed.
00058	Q502 closed	The bypass transformer output switch Q502 is closed.
00060	Q611 closed	The load output switch Q611 is closed.
00062	Q691 closed	The SBS input switch Q691 is closed.
00063	Q692 closed	The UPS output switch Q692 is closed.
00065	MBS: TEST	The manual bypass switch Q601 in the test position.
00066	MBS: BYPASS	The manual bypass switch Q601 in the bypass position.
00067	MBS: AUTO	The manual bypass switch Q601 in the auto position.
00068	Overtemperature	An overtemperature at a PM or a transformer is detected (if available).
00071	T001 overtemperature	An overtemperature at the rectifier mains transformer is detected.
00072	T401 overtemperature	An overtemperature at the output transformer is detected.
00073	T501 overtemperature	An overtemperature at the bypass transformer is detected.
00074	Battery temperature warning	The battery temperature exceeds the programmed warning level.
00075	Battery temperature shutdown	The battery temperature exceeds the programmed shutdown level.
00076	Temperature 1 warning	The temperature sensor, connected to the external connection board, is over the temperature warning level.

Modbus Read Coil Register List (Continued)

Coil Register	Parameter	Description
00077	Temperature 2 warning	The temperature sensor, connected to the external connection board, is over the temperature warning level.
00078	Temperature 3 warning	The temperature sensor, connected to the external connection board, is over the temperature warning level.
00079	T001 temperature sensor fault	The mains input transformer temperature sensor PT100 is not connected or shorted.
00080	T401 temperature sensor fault	The output transformer temperature sensor PT100 is not connected or shorted.
00081	T501 temperature sensor fault	The bypass transformer temperature sensor PT100 is not connected or shorted.
00082	Fan inoperable	The transformer, SBS or power module fan is inoperable.
00089	Emergency power off (EPO)	The digital input of emergency power off (EPO) is activated (contact open) or the EPO wiring is disconnected.
00091	PSU fault	One or more PSU faults are detected.
00092	General mains fault	One or more mains faults are detected.
00093	Mains RMS fault	The rectifier mains voltage is out of tolerance.
00094	Mains input RMS fault	The rectifier mains voltage on primary side of the input transformer is out of tolerance. This event is only active if a transformer is installed.
00101	General bypass fault	One or more bypass faults are detected.
00102	Bypass RMS fault	The bypass voltage is out of tolerance.
00103	Bypass input RMS fault	The bypass mains voltage on the primary side of bypass transformer is out of tolerance. This event is only active if a transformer and the bypass measurement is installed.
00108	General output fault	One or more output faults are detected.
00109	Output RMS fault	The output voltage on the secondary side of the output transformer is out of tolerance.
00110	Inverter output RMS fault	The UPS output voltage is out of tolerance.
00116	Output overloaded	The UPS output is overloaded (>100%) or the inverter current limiter is active.
00119	Battery current positive	0 = the battery is discharged. 1 = the battery is charged.
00121	Battery warning or error	The battery voltage is out of tolerance or the runtime is too short.
00122	Battery earth fault	The interface has detected a battery earth fault (if available).
00123	High battery shutdown	Battery voltage above the high battery shutdown level.
00124	High battery warning	Battery voltage above the high battery warning level (no warning in battery operation).
00125	Low battery warning voltage	Battery voltage below the low battery warning level.
00126	Battery discharged (Low battery shutdown voltage)	Battery voltage below low battery shutdown level.
00127	Battery earth fault positive	The interface has detected a battery positive earth fault (if available).
00128	Battery earth fault negative	The interface has detected a battery negative earth fault (if available).
00140	Rectifier fault / error	The rectifier turned off because a fault was detected.
00141	Inverter fault / error	The inverter turned off because a fault was detected.
00154	Input closed Ecb 1	
00155	Input closed Ecb 2	
00156	RB1.1 input closed	
00157	RB1.2 input closed	
00158	RB1.3 input closed	
00159	RB1.4 input closed	

Modbus Read Coil Register List (Continued)

Coil Register	Parameter	Description
00160	RB1.5 input closed	
00161	RB1.6 input closed	
00162	RB1.7 input closed	
00163	RB1.8 input closed	
00172	HMI alarm LED 1 active	
00173	HMI alarm LED 2 active	
00174	HMI alarm LED 3 active	
00175	HMI alarm LED 4 active	
00176	HMI alarm LED 5 active	
00177	HMI alarm LED 6 active	
00178	HMI alarm LED 7 active	
00179	HMI alarm LED 8 active	
00180	HMI alarm LED 9 active	
00181	HMI alarm LED 10 active	
00182	HMI alarm LED 11 active	
00183	HMI alarm LED 12 active	
00184	HMI alarm LED 13 active	
00185	HMI alarm LED 14 active	
00186	HMI alarm LED 15 active	
00187	ECB common alarm active	
00188	ECB output 1 closed	
00189	ECB output 2 closed	
00190	RB1.1 output closed	
00191	RB 1.2 output closed	
00192	RB 1.3 output closed	
00193	RB 1.4 output closed	
00194	RB 1.5 output closed	
00195	RB 1.6 output closed	
00196	RB 1.7 output closed	
00197	RB 1.8 output closed	
00198	RB 1.9 output closed	
00199	RB 1.10 output closed	
00200	RB 1.11 output closed	
00201	RB 1.12 output closed	
00202	RB 1.13 output closed	
00203	RB 1.14 output closed	
00204	RB 1.15 output closed	
00205	RB 1.16 output closed	

Modbus Read Holding Register (Function Call 03)

The read holding register contains analog 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.

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.

Modbus Read Holding Register List

Holding Register	Parameter [Unit of Measure]	Factor[4]	Description
40001	System load [% of VA]	10	
40002	System load [% of W]	10	
40003	Apparent system load [kVA]	10	
40004	Real system load [kW]	10	
40005	Output apparent power L1 [kVA]	10	
40006	Output apparent power L2 [kVA]	10	
40007	Output apparent power L3 [kVA]	10	
40008	Output real power L1 [kW]	10	
40009	Output real power L2 [kW]	10	
40010	Output real power L3 [kW]	10	
40011	Output power factor L1	100	
40012	Output power factor L2	100	
40013	Output power factor L3	100	
40015	Total output load [% of VA]	10	Only for redundant systems.
40016	Total output load [% of W]	10	Only for redundant systems.
40017	Total output load [VA]	10	Only for redundant systems.
40018	Total Output load [W]	10	Only for redundant systems.
40019	Output frequency [Hz]	10	
40020	Output voltage L1 [V]	10	
40021	Output voltage L2 [V]	10	
40022	Output voltage L3 [V]	10	
40023	Output current L1 [A]	10	
40024	Output current L2 [A]	10	
40025	Output current L3 [A]	10	
40035	Input frequency [Hz]	10	
40036	Input voltage L1 [V]	10	
40037	Input voltage L2 [V]	10	
40038	Input voltage L3 [V]	10	
40045	Input current L1 [A]	10	
40046	Input current L2 [A]	10	
40047	Input current L3 [A]	10	

4. The actual measured value is multiplied with a factor.

Modbus Read Holding Register List (Continued)

Holding Register	Parameter [Unit of Measure]	Factor[5]	Description
40057	Input bypass frequency [Hz]	10	
40058	Input bypass voltage L1 [V]	10	Phase L1 to Phase L2. 0 if not available.
40059	Input bypass voltage L2 [V]	10	Phase L2 to Phase L3. 0 if not available.
40060	Input bypass voltage L3 [V]	10	Phase L3 to Phase L1. 0 if not available.
40061	Input bypass current L1 [A]	10	Measured before the bypass transformer. 0 if not available.
40062	Input bypass current L2 [A]	10	Measured before the bypass transformer. 0 if not available.
40063	Input bypass current L3 [A]	10	Measured before the bypass transformer. 0 if not available.
40071	Battery current [A]	10	
40072	Battery voltage [V]	10	
40075	Battery temperature [°C or °F]	1	Only available if optional Gutor battery ABM is installed in the system.
40076	Expected battery runtime [minutes]	1	Only available if optional Gutor battery ABM is installed in the system.
40077	Percentage of battery capacity [%]	10	Only available if optional Gutor battery ABM is installed in the system.
40090	Temperature sensor 1 [°C or °F]	1	The temperature sensor needs to be installed.
40091	Temperature sensor 2 [°C or °F]	1	The temperature sensor needs to be installed.
40092	Temperature sensor 3 [°C or °F]	1	The temperature sensor needs to be installed.
40093	Temperature T001 [°C or °F]	1	The temperature sensor needs to be installed.
40094	Temperature T401 [°C or °F]	1	The temperature sensor needs to be installed.
40095	Temperature T501 [°C or °F]	1	The temperature sensor needs to be installed.
40245	Read coil register 001-016	—	The registers are lined up the following way: 16-13 12-9 8-5 4-1.
40246	Read coil register 017-032	—	
40247	Read coil register 033-048	—	
40248	Read coil register 049-064	—	
40249	Read coil register 065-080	—	
40250	Read coil register 081-096	—	
40251	Read coil register 097-112	—	
40252	Read coil register 113-128	—	
40253	Read coil register 129-144	—	
40254	Read coil register 145-160	—	
40255	Read coil register 161-176	—	
40256	Read coil register 177-192	—	
40257	Read coil register 193-208	—	

5. The actual measured value is multiplied with a factor.

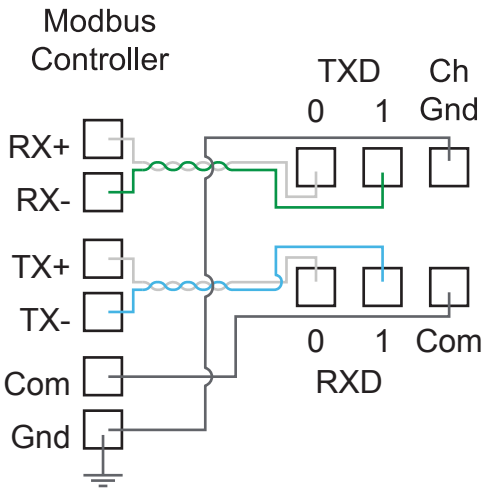
Modbus Wiring Diagrams

The Modbus wiring for the NMC in a Gutor system is done with 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.

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 ?`.

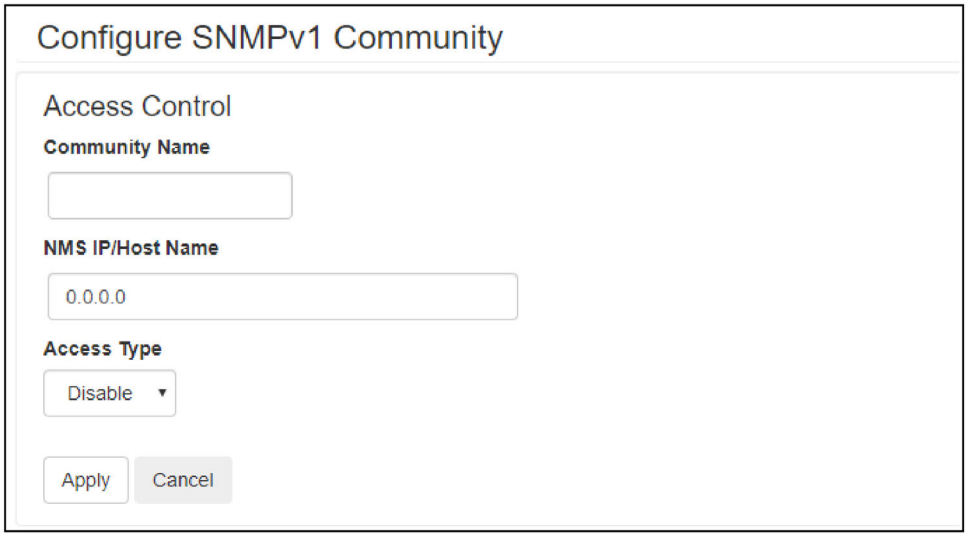
   NOTE: In the table `[n]` is the access community number 1, 2, 3 or 4.

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> | <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.



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

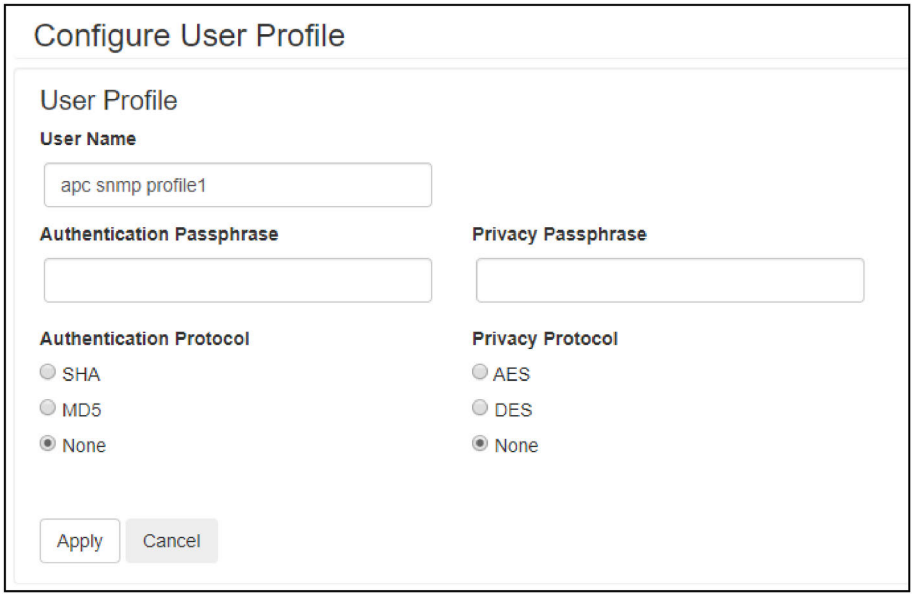
1. Log in to the CLI.
2. To see the configuration options type `snmpV3 ?`.

   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]`	`<Authenti-cation 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> | <Host Name>`	Set the IPv4/IPv6 address or the host name of the network management station.

Configure SNMPv3 from the Web Interface

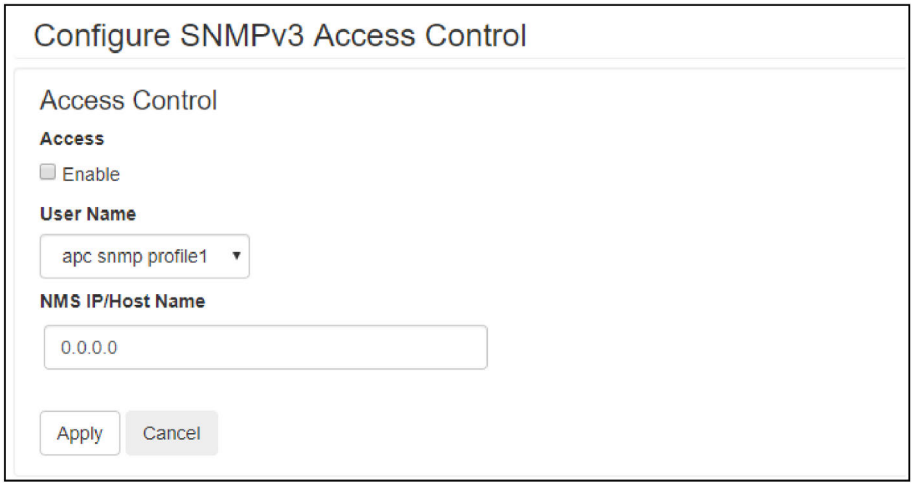
1. Log in to the web interface.
2. Navigate to **Configuration > Network > SNMPv3 > User Profile**.
3. Click on a user name to view the settings for it.
4. Here it is possible to configure the **User Name**, **Authentication Passphrase**, **Authentication Protocol**, **Privacy Passphrase** and **Privacy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



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.



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 ?`.

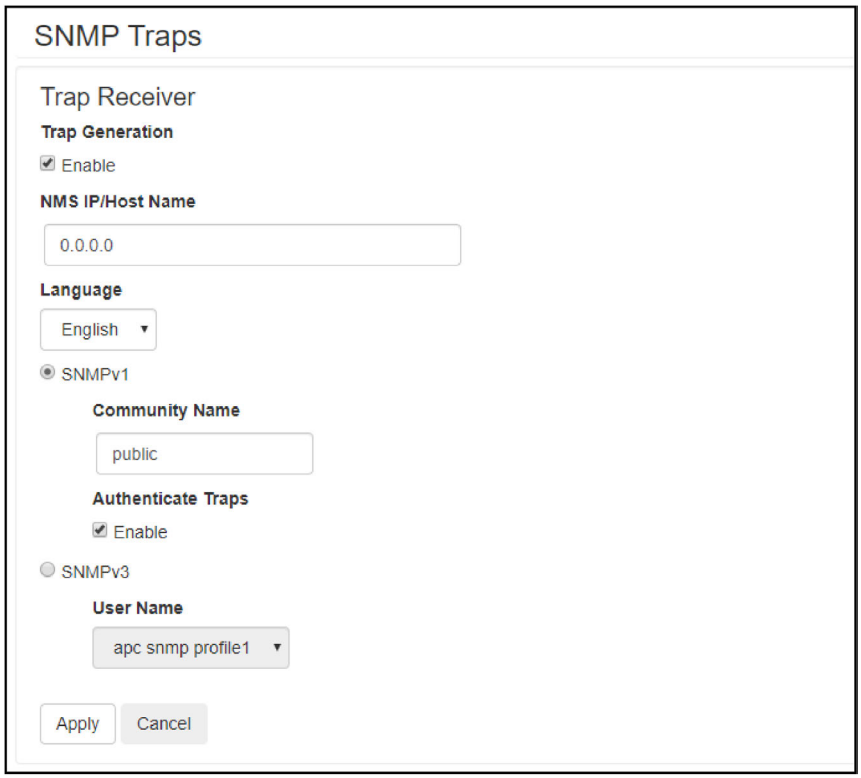
   NOTE: In the table `[n]` is the number of the trap receiver (1–6).

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.



   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	Severity	Event Text
communicationLost	1	Critical	UPS: Lost the local network management interface-to-UPS communication.
upsDiagnosticsFailed	3	Critical	UPS: Self-test failed.
communicationEstablished	8	Informational	UPS: Restored the local network management interface-to-UPS communication.
upsDiagnosticsPassed	10	Informational	UPS: Passed a self-test.
abnormalCondition	77	Critical	UPS: 2: Hardware inoperable or wrong configuration file loaded.
abnormalCondition	77	Critical	UPS: 11: The system is in standby.
abnormalCondition	77	Critical	UPS: 15: The system is in battery operation.
abnormalCondition	77	Critical	UPS: 16: Normal operation.
abnormalCondition	77	Critical	UPS: 17: Requested bypass operation.
abnormalCondition	77	Critical	UPS: 18: Temporary bypass operation.
abnormalCondition	77	Critical	UPS: 20: Bypass charge operation.
abnormalCondition	77	Critical	UPS: 40: Charger off.
abnormalCondition	77	Critical	UPS: 41: Float charge.
abnormalCondition	77	Critical	UPS: 42: Boost charge.
abnormalCondition	77	Critical	UPS: 43: Initial charge.
abnormalCondition	77	Critical	UPS: 44: Cyclic charge.
abnormalCondition	77	Critical	UPS: 45: Boost / Init blocked.
abnormalCondition	77	Critical	UPS: 79: Parallel master has changed.
abnormalCondition	77	Critical	UPS: 102: Powermodule hardware failure (PFC).
abnormalCondition	77	Critical	UPS: 110: Powermodule hardware failure (CH).
abnormalCondition	77	Critical	UPS: 132: Powermodule hardware failure (INV).
abnormalCondition	77	Critical	UPS: 146: Inverter asynchronous.
abnormalCondition	77	Critical	UPS: 161: Static bypass on.
abnormalCondition	77	Critical	UPS: 162: SBS fault.
abnormalCondition	77	Critical	UPS: 163: SBS independent fired.
abnormalCondition	77	Critical	UPS: 164: SBS DC fault.
abnormalCondition	77	Critical	UPS: 165: Q601: TEST.
abnormalCondition	77	Critical	UPS: 166: Q601: BYPASS.
abnormalCondition	77	Critical	UPS: 167: Q601: AUTO.
abnormalCondition	77	Critical	UPS: 181: Powermodule temperature warning.
abnormalCondition	77	Critical	UPS: 182: Powermodule overtemperature.
abnormalCondition	77	Critical	UPS: 183: T001 overtemperature.
abnormalCondition	77	Critical	UPS: 184: T401 overtemperature.
abnormalCondition	77	Critical	UPS: 185: T501 overtemperature.

SNMP Trap OID List (Continued)

SNMP Trap OID Name	Trap ID	Severity	Event Text
abnormalCondition	77	Critical	UPS: 186: Battery temperature warning.
abnormalCondition	77	Critical	UPS: 187: Battery temperature shutdown.
abnormalCondition	77	Critical	UPS: 189: Temperature sensor 1 warning.
abnormalCondition	77	Critical	UPS: 190: Temperature sensor 2 warning.
abnormalCondition	77	Critical	UPS: 191: Temperature sensor 3 warning.
abnormalCondition	77	Critical	UPS: 192: T001 sensor fault.
abnormalCondition	77	Critical	UPS: 193: T401 sensor fault.
abnormalCondition	77	Critical	UPS: 194: T501 sensor fault.
abnormalCondition	77	Critical	UPS: 200: Powermodule fan failure.
abnormalCondition	77	Critical	UPS: 201: SBS fan failure.
abnormalCondition	77	Critical	UPS: 202: Transformer fan failure.
abnormalCondition	77	Critical	UPS: 220: Mains RMS fault.
abnormalCondition	77	Critical	UPS: 221: Mains input RMS fault.
abnormalCondition	77	Critical	UPS: 222: Mains FAST fault.
abnormalCondition	77	Critical	UPS: 223: Mains frequency fault.
abnormalCondition	77	Critical	UPS: 224: Mains phase missing.
abnormalCondition	77	Critical	UPS: 225: Mains input phase missing.
abnormalCondition	77	Critical	UPS: 228: Mains synchronisation fault.
abnormalCondition	77	Critical	UPS: 229: Mains neutral lost.
abnormalCondition	77	Critical	UPS: 240: Bypass RMS fault.
abnormalCondition	77	Critical	UPS: 241: Bypass input RMS fault.
abnormalCondition	77	Critical	UPS: 242: Bypass FAST fault.
abnormalCondition	77	Critical	UPS: 243: Bypass frequency fault.
abnormalCondition	77	Critical	UPS: 244: Bypass phase missing.
abnormalCondition	77	Critical	UPS: 245: Bypass input phase missing.
abnormalCondition	77	Critical	UPS: 260: Inverter output RMS fault.
abnormalCondition	77	Critical	UPS: 261: Output RMS fault.
abnormalCondition	77	Critical	UPS: 262: Output FAST fault.
abnormalCondition	77	Critical	UPS: 263: Output frequency fault.
abnormalCondition	77	Critical	UPS: 264: Output phase missing.
abnormalCondition	77	Critical	UPS: 266: High output voltage.
abnormalCondition	77	Critical	UPS: 267: High load warning.
abnormalCondition	77	Critical	UPS: 268: Current limitation.
abnormalCondition	77	Critical	UPS: 269: Overload.
abnormalCondition	77	Critical	UPS: 271: Output FAST fault.
abnormalCondition	77	Critical	UPS: 301: High Battery voltage shutdown.
abnormalCondition	77	Critical	UPS: 304: High Battery voltage.
abnormalCondition	77	Critical	UPS: 305: Low Battery voltage.
abnormalCondition	77	Critical	UPS: 306: Battery discharged.
abnormalCondition	77	Critical	UPS: 307: Battery earth fault positive.
abnormalCondition	77	Critical	UPS: 308: Battery earth fault negative.
abnormalCondition	77	Critical	UPS: 312: Battery weak.

SNMP Trap OID List (Continued)

SNMP Trap OID Name	Trap ID	Severity	Event Text
abnormalCondition	77	Critical	UPS: 313: Battery defect.
abnormalCondition	77	Critical	UPS: 314: Low runtime warning.
abnormalCondition	77	Critical	UPS: 315: Low runtime alarm.
abnormalCondition	77	Critical	UPS: 319: Battery collapsed.
abnormalCondition	77	Critical	UPS: 330: Q001: open.
abnormalCondition	77	Critical	UPS: 331: Q201 / Q211: open.
abnormalCondition	77	Critical	UPS: 332: Q501: open.
abnormalCondition	77	Critical	UPS: 333: Q502: open.
abnormalCondition	77	Critical	UPS: 334: Q611: open.
abnormalCondition	77	Critical	UPS: 335: Q691: open.
abnormalCondition	77	Critical	UPS: 336: Q901: open.
abnormalCondition	77	Critical	UPS: 337: Q692: open.
abnormalCondition	77	Critical	UPS: 338: K401: open.
abnormalCondition	77	Critical	UPS: 351: ABUS termination fault.
abnormalCondition	77	Critical	UPS: 370: Parallel configuration fault.
abnormalCondition	77	Critical	UPS: 371: No parallel master.
abnormalCondition	77	Critical	UPS: 374: Parallel load alarm.
abnormalCondition	77	Critical	UPS: 375: Redundancy alarm.
abnormalCondition	77	Critical	UPS: 397: PBUS 1 communication fault.
abnormalCondition	77	Critical	UPS: 398: PBUS 2 communication fault.
abnormalCondition	77	Critical	UPS: 399: PBUS 1 termination fault.
abnormalCondition	77	Critical	UPS: 400: PBUS 2 termination fault.
abnormalCondition	77	Critical	UPS: 440: EPO active.
abnormalCondition	77	Critical	UPS: 447: Internal error.
abnormalCondition	77	Critical	UPS: 448: Locked in bypass.
abnormalCondition	77	Critical	UPS: 650: LCM Start-Up Alert.
abnormalCondition	77	Critical	UPS: 653: LCM End of Warranty.
abnormalCondition	77	Critical	UPS: 658: LCM Technical Check.
abnormalCondition	77	Critical	UPS: 663: LCM Alert 1.
abnormalCondition	77	Critical	UPS: 668: LCM Alert 2.
abnormalCondition	77	Critical	UPS: 673: LCM Alert 3.
abnormalCondition	77	Critical	UPS: 678: LCM Alert 4.
abnormalCondition	77	Critical	UPS: 683: LCM Alert 5.
abnormalCondition	77	Critical	UPS: 722: Relayboard input 1.1.
abnormalCondition	77	Critical	UPS: 723: Relayboard input 1.2.
abnormalCondition	77	Critical	UPS: 724: Relayboard input 1.3.
abnormalCondition	77	Critical	UPS: 725: Relayboard input 1.4.
abnormalCondition	77	Critical	UPS: 726: Relayboard input 1.5.
abnormalCondition	77	Critical	UPS: 727: Relayboard input 1.6.
abnormalCondition	77	Critical	UPS: 728: Relayboard input 1.7.
abnormalCondition	77	Critical	UPS: 729: Relayboard input 1.8.
abnormalCondition	77	Critical	UPS: 730: Relayboard input 2.1.

SNMP Trap OID List (Continued)

SNMP Trap OID Name	Trap ID	Severity	Event Text
abnormalCondition	77	Critical	UPS: 731: Relayboard input 2.2.
abnormalCondition	77	Critical	UPS: 732: Relayboard input 2.3.
abnormalCondition	77	Critical	UPS: 733: Relayboard input 2.4.
abnormalCondition	77	Critical	UPS: 734: Relayboard input 2.5.
abnormalCondition	77	Critical	UPS: 735: Relayboard input 2.6.
abnormalCondition	77	Critical	UPS: 736: Relayboard input 2.7.
abnormalCondition	77	Critical	UPS: 737: Relayboard input 2.8.
abnormalCondition	77	Critical	UPS: 738: External connection board input 1.
abnormalCondition	77	Critical	UPS: 739: External connection board input 2.
abnormalCondition	77	Critical	UPS: 800: Common alarm.
abnormalConditionCleared	78	Informational	UPS: 243: Bypass frequency OK.
abnormalConditionCleared	78	Informational	UPS: 244: Bypass phases OK.
abnormalConditionCleared	78	Informational	UPS: 245: Bypass input phases OK.
abnormalConditionCleared	78	Informational	UPS: 260: Inverter output RMS OK.
abnormalConditionCleared	78	Informational	UPS: 261: Output RMS OK.
abnormalConditionCleared	78	Informational	UPS: 262: Output FAST OK.
abnormalConditionCleared	78	Informational	UPS: 263: Output frequency OK.
abnormalConditionCleared	78	Informational	UPS: 264: Output phases OK.
abnormalConditionCleared	78	Informational	UPS: 266: The UPS output voltage (RMS) is normal.
abnormalConditionCleared	78	Informational	UPS: 268: No limitation.
abnormalConditionCleared	78	Informational	UPS: 269: No overload.
abnormalConditionCleared	78	Informational	UPS: 301: Battery voltage OK.
abnormalConditionCleared	78	Informational	UPS: 304: Battery voltage OK.
abnormalConditionCleared	78	Informational	UPS: 305: Battery voltage OK.
abnormalConditionCleared	78	Informational	UPS: 306: Battery OK.
abnormalConditionCleared	78	Informational	UPS: 307: No battery earth fault.
abnormalConditionCleared	78	Informational	UPS: 308: No battery earth fault.
abnormalConditionCleared	78	Informational	UPS: 313: Battery OK.
abnormalConditionCleared	78	Informational	UPS: 314: Runtime OK.
abnormalConditionCleared	78	Informational	UPS: 315: Runtime OK.
abnormalConditionCleared	78	Informational	UPS: 319: Battery OK.
abnormalConditionCleared	78	Informational	UPS: 330: Q001: closed.
abnormalConditionCleared	78	Informational	UPS: 331: Q201 / Q211: closed.
abnormalConditionCleared	78	Informational	UPS: 332: Q501: closed.
abnormalConditionCleared	78	Informational	UPS: 333: Q502: closed.
abnormalConditionCleared	78	Informational	UPS: 334: Q611: closed.
abnormalConditionCleared	78	Informational	UPS: 335: Q691: closed.
abnormalConditionCleared	78	Informational	UPS: 336: Q901: closed.
abnormalConditionCleared	78	Informational	UPS: 337: Q692: closed.
abnormalConditionCleared	78	Informational	UPS: 339: Q528 SBS Input close.
abnormalConditionCleared	78	Informational	UPS: 447: No internal error.
abnormalConditionCleared	78	Informational	UPS: 448: Bypass unlocked.

SNMP Trap OID List (Continued)

SNMP Trap OID Name	Trap ID	Severity	Event Text
abnormalConditionCleared	78	Informational	UPS: 162: SBS OK.
abnormalConditionCleared	78	Informational	UPS: 242: Bypass FAST OK.
abnormalConditionCleared	78	Informational	UPS: 399: PBUS 1 OK.
abnormalConditionCleared	78	Informational	UPS: 400: PBUS 2 OK.
abnormalConditionCleared	78	Informational	UPS: 271: Output FAST OK.
abnormalConditionCleared	78	Informational	UPS: 440: EPO cleared.
abnormalConditionCleared	78	Informational	UPS: 163: SBS OK.
abnormalConditionCleared	78	Informational	UPS: 2: System configuration is OK.
abnormalConditionCleared	78	Informational	UPS: 397: PBUS 1 OK.
abnormalConditionCleared	78	Informational	UPS: 398: PBUS 2 OK.
abnormalConditionCleared	78	Informational	UPS: 351: ABUS termination OK.
abnormalConditionCleared	78	Informational	UPS: 374: Parallel load OK.
abnormalConditionCleared	78	Informational	UPS: 370: Parallel configuration is OK.
abnormalConditionCleared	78	Informational	UPS: 102: Powermodule hardware OK (PFC).
abnormalConditionCleared	78	Informational	UPS: 110: Powermodule hardware OK (CH).
abnormalConditionCleared	78	Informational	UPS: 132: Powermodule hardware OK (INV).
abnormalConditionCleared	78	Informational	UPS: 146: The UPS is unable to synchronise to the bypass source.
abnormalConditionCleared	78	Informational	UPS: 164: SBS DC OK.
abnormalConditionCleared	78	Informational	UPS: 182: Powermodule temperature OK.
abnormalConditionCleared	78	Informational	UPS: 183: T001 temperature OK.
abnormalConditionCleared	78	Informational	UPS: 184: T401 temperature OK.
abnormalConditionCleared	78	Informational	UPS: 185: T501 temperature OK.
abnormalConditionCleared	78	Informational	UPS: 187: Battery temperature OK.
abnormalConditionCleared	78	Informational	UPS: 192: T001 sensor OK.
abnormalConditionCleared	78	Informational	UPS: 193: T401 sensor OK.
abnormalConditionCleared	78	Informational	UPS: 194: T501 sensor OK.
abnormalConditionCleared	78	Informational	UPS: 200: Powermodule fans OK.
abnormalConditionCleared	78	Informational	UPS: 201: SBS fan OK.
abnormalConditionCleared	78	Informational	UPS: 202: Transformer fans OK.
abnormalConditionCleared	78	Informational	UPS: 220: Mains RMS OK.
abnormalConditionCleared	78	Informational	UPS: 221: Mains input RMS OK.
abnormalConditionCleared	78	Informational	UPS: 222: Mains FAST OK.
abnormalConditionCleared	78	Informational	UPS: 223: Mains frequency OK.
abnormalConditionCleared	78	Informational	UPS: 224: Mains phases OK.
abnormalConditionCleared	78	Informational	UPS: 225: Mains input phases OK.
abnormalConditionCleared	78	Informational	UPS: 228: Mains synchronisation OK.
abnormalConditionCleared	78	Informational	UPS: 229: Mains neutral OK.
abnormalConditionCleared	78	Informational	UPS: 240: Bypass RMS OK.
abnormalConditionCleared	78	Informational	UPS: 241: Bypass input RMS OK.
apcInternalCommunicationFault	730	Critical	UPS: An internal UPS communication fault exists.
apcInternalCommunicationFault-Cleared	731	Informational	UPS: An internal UPS communication fault no longer exists.
upsWarningCondition	736	Warning	UPS: 267: The load is above the configured load alarm level.

SNMP Trap OID List (Continued)

SNMP Trap OID Name	Trap ID	Severity	Event Text
upsWarningCondition	736	Warning	UPS: 722: Relay board 1 input 1 open / close.
upsWarningCondition	736	Warning	UPS: 723: Relay board 1 input 2 open / close.
upsWarningCondition	736	Warning	UPS: 724: Relay board 1 input 3 open / close.
upsWarningCondition	736	Warning	UPS: 725: Relay board 1 input 4 open / close.
upsWarningCondition	736	Warning	UPS: 726: Relay board 1 input 5 open / close.
upsWarningCondition	736	Warning	UPS: 727: Relay board 1 input 6 open / close.
upsWarningCondition	736	Warning	UPS: 728: Relay board 1 input 7 open / close.
upsWarningCondition	736	Warning	UPS: 729: Relay board 1 input 8 open / close.
upsWarningCondition	736	Warning	UPS: 730: Relay board 2 input 1 open / close.
upsWarningCondition	736	Warning	UPS: 731: Relay board 2 input 2 open / close.
upsWarningCondition	736	Warning	UPS: 732: Relay board 2 input 3 open / close.
upsWarningCondition	736	Warning	UPS: 733: Relay board 2 input 4 open / close.
upsWarningCondition	736	Warning	UPS: 734: Relay board 2 input 5 open / close.
upsWarningCondition	736	Warning	UPS: 734: Relay board 2 input 5 open / close.
upsWarningCondition	736	Warning	UPS: 736: Relay board 2 input 7 open / close.
upsWarningCondition	736	Warning	UPS: 737: Relay board 2 input 8 open / close.
upsWarningCondition	736	Warning	UPS: 738: External connection board input 1 open / close.
upsWarningCondition	736	Warning	UPS: 739: External connection board input 2 open / close.
upsWarningCondition	736	Warning	UPS: 650: LCM alert indicate that a proper start-up of the system is required.
upsWarningCondition	736	Warning	UPS: 653: The life cycle monitoring end of warranty alert.
upsWarningCondition	736	Warning	UPS: 658: The life cycle monitoring technical check alert.
upsWarningCondition	736	Warning	UPS: 663: The life cycle monitoring recommends to replace the fan modules.
upsWarningCondition	736	Warning	UPS: 668: The life cycle monitoring recommends to replace the battery.
upsWarningCondition	736	Warning	UPS: 673: The life cycle monitoring recommends to replace the power modules.
upsWarningCondition	736	Warning	UPS: 678: The life cycle monitoring recommends to replace the air filters.
upsWarningCondition	736	Warning	UPS: 683: The life cycle monitoring recommends to do the 10 year component replacement.
upsWarningCondition	736	Warning	UPS: 312: The advanced battery monitoring test has detected a weak battery.
upsWarningCondition	736	Warning	UPS: 186: The battery temperature is above the configured warning level.
upsWarningCondition	736	Warning	UPS: 375: At least one UPS is isolated or turned off.
upsWarningCondition	736	Warning	UPS: 371: No master is present in the redundant system.
upsWarningCondition	736	Warning	UPS: 146: Inverter synchronous.
upsWarningCondition	736	Warning	UPS: 161: The system is in static bypass operation.
upsWarningCondition	736	Warning	UPS: 181: The power module temperature is above 90 C.
upsWarningCondition	736	Warning	UPS: 189: The Temperature sensor 1 measures a temperature above the configured warning level.
upsWarningCondition	736	Warning	UPS: 190: The Temperature sensor 2 measures a temperature above the configured warning level.

SNMP Trap OID List (Continued)

SNMP Trap OID Name	Trap ID	Severity	Event Text
upsWarningCondition	736	Warning	UPS: 191: The Temperature sensor 3 measures a temperature above the configured warning level.
upsWarningConditionCleared	737	Informational	UPS: 267: Load OK.
upsWarningConditionCleared	737	Informational	UPS: 312: Battery OK.
upsWarningConditionCleared	737	Informational	UPS: 186: Battery temperature OK.
upsWarningConditionCleared	737	Informational	UPS: 375: Redundancy OK.
upsWarningConditionCleared	737	Informational	UPS: 371: Parallel master selected.
upsWarningConditionCleared	737	Informational	UPS: 161: Static bypass OFF.
upsWarningConditionCleared	737	Informational	UPS: 181: Powermodule temperature OK.
upsWarningConditionCleared	737	Informational	UPS: 189: Temperature sensor 1 OK.
upsWarningConditionCleared	737	Informational	UPS: 190: Temperature sensor 2 OK.
upsWarningConditionCleared	737	Informational	UPS: 191: Temperature sensor 3 OK.

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 analog and digital values, see respective section.

Analog 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			
UPS model	upsBasicIdentModel	1.1.1.1.1.1	
User system name	upsBasicIdentName	1.1.1.1.1.2	
System firmware version	upsAdvIdentFirmwareRevision	1.1.1.1.2.1	
Date of manufacturing	upsAdvIdentDateOfManufacture	1.1.1.1.2.2	
Serial number	upsAdvIdentSerialNumber	1.1.1.1.2.3	
System SKU number	upsAdvIdentSkuNumber	1.1.1.1.2.5	
Input			
Input frequency [Hz]	upsAdvInputFrequency	1.1.1.3.2.4	
Input frequency [Hz]	upsHighPrecInputFrequency	1.1.1.3.3.4	Factor 10. The actual measured value is multiplied with a factor 10.
Number of input feeds	upsPhaseNumInputs	1.1.1.9.2.1	
Input voltage orientation	upsPhaseInputVoltageOrientation	1.1.1.9.2.2.1.3	
Input phase frequency [Hz]	upsPhaseInputFrequency	1.1.1.9.2.2.1.4	Index based (1.1.1 – 1.1.3)
Bypass input frequency [Hz]	upsPhaseInputFrequency	1.1.1.9.2.2.1.4	Index based (2.1.1 – 2.1.3)
Number of input feeds	upsPhaseInputName	1.1.1.9.2.2.1.6	
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 (2.1.1 – 2.1.3)
Input current (phase-to-neutral) [A]	upsPhaseInputCurrent	1.1.1.9.2.3.1.6	Index based (1.1.1 – 1.1.3)
Input maximum voltage [V]	upsPhaseInputMaxVoltage	1.1.1.9.3.3.1.4	
Input minimum voltage [V]	upsPhaseInputMinVoltage	1.1.1.9.3.3.1.5	
Output			
Output phase	upsBasicOutputPhase	1.1.1.4.1.2	
Output frequency [Hz]	upsAdvOutputFrequency	1.1.1.4.2.2	
Number of output feeds	upsPhaseNumOutputs	1.1.1.9.3.1	
Output voltage orientation	upsPhaseOutputVoltageOrientation	1.1.1.9.3.2.1.3	
Output voltage (phase-to-phase) [V]	upsPhaseOutputVoltage	1.1.1.9.3.3.1.3	Index based (1.1.1 – 1.1.3)
Current (phase-to-neutral) [A]	upsPhaseOutputCurrent	1.1.1.9.3.3.1.4	Index based (1.1.1 – 1.1.3)
Output apparent power [VA]	upsPhaseOutputLoad	1.1.1.9.3.3.1.7	Index based (1.1.1 – 1.1.3)
Output active power [W]	upsPhaseOutputPower	1.1.1.9.3.3.1.13	Index based (1.1.1 – 1.1.3)

Parameter [Unit of Measure]	SNMP OID Name	APC / Gutor OID Address	Notes
Output power factor [W]	upsPhaseOutputPowerFactor	1.1.1.9.3.3.1.19	
Battery			
Battery time Left [minutes]	upsAdvBatteryRunTimeRemaining	1.1.1.2.2.3	Only available if optional Gutor battery ABM is installed in the system.
Battery voltage [V]	upsAdvBatteryActualVoltage	1.1.1.2.2.8	
Battery current [A]	upsAdvBatteryCurrent	1.1.1.2.2.9	
Battery voltage [V]	upsHighPrecBatteryActualVoltage	1.1.1.2.3.4	Factor 10. The actual measured value is multiplied with a factor 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 '0000000000 0000000000 0000000000 0000000000 0001000000 0000000000 0000' it would indicate that the relay board 1, input 5 is closed, since the character position 44 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
4	Inverter output RMS fault	The UPS output voltage is out of tolerance.
5	Output RMS fault	The output voltage on the secondary side of the output transformer is out of tolerance.
12	Output overloaded	The UPS output is overloaded (>100%) or the inverter current limiter is active.
13	High battery shutdown	Battery voltage above the high battery shut-down level.
14	High battery warning	Battery voltage above the high battery warning level (no warning in battery operation).
15	Battery discharged	Battery voltage below the low battery warning level.
16	Low battery shutdown	Battery voltage below low battery shut-down level.
17	Battery earth fault positive	The interface has detected a battery positive earth fault (if available).
18	Battery earth fault negative	The interface has detected a battery negative earth fault (if available).
29	Q001 closed	The rectifier mains input switch Q001 is closed.
30	Q201 closed	The battery switch Q201 is closed.
31	Q501 closed	The bypass mains input switch Q501 is closed.
32	Q502 closed	The bypass transformer output switch Q502 is closed.
33	Q611 closed	The load output switch Q611 is closed.
34	Q691 closed	The SBS input switch Q691 is closed.

OID Address: 1.1.1.11.2.1 / OID Name: upsAdvStateAbnormalConditions (Continued)

Character Position	Parameter	Notes
36	Q692 closed	The UPS output switch Q692 is closed.
40	RB1.1 input closed	
41	RB1.2 input closed	
42	RB1.3 input closed	
43	RB1.4 input closed	
44	RB1.5 input closed	
45	RB1.6 input closed	
46	RB1.7 input closed	
47	RB1.8 input closed	
60	General bypass fault	One or more bypass faults are detected.
61	General mains fault	One or more mains faults are detected.
62	General output fault	One or more output faults are detected.
63	Overtemperature	Overtemperature in PM or transformers detected (if available).
64	Battery warning or error	The battery voltage is out of tolerance or the runtime is too short.

OID Address: 1.1.1.11.2.5 / OID Name: upsAdvStateSmartUPSSpecificFaults

Character Position	Parameter	Notes
1	Emergency power off (EPO)	The digital input of emergency power off (EPO) is activated (contact open) or the EPO wiring is disconnected.
6	Battery temperature warning	The battery temperature exceeds the programmed warning level.
18	Standby	1 = the system is in standby operation.
19	Battery operation	1 = the system is in battery operation.
20	Normal operation	1 = the system is in normal operation.
21	Requested static bypass	The system is in static bypass operation due to a user request.
22	Temporary static bypass	The system is in static bypass operation due to a fault.
25	Float charge	The battery charger has been set to float charge state. The batteries are charged with a float charge voltage.
26	Boost charge	The battery charger has been set to boost charge mode. The batteries are charged with a boost charge voltage.
27	Initial charge	The battery charger has been set to initial charge mode. The batteries are charged with a initial charge voltage.
28	Cyclic charge	The battery charger has been set to cyclic charge mode. The batteries are charged with a cyclic charge voltage.
35	Bypass operation	Static bypass is switched on.
37	MBS: TEST	The manual bypass switch Q601 in the test position.
38	MBS: BYPASS	The manual bypass switch Q601 in the bypass position.

OID Address: 1.1.1.11.2.5 / OID Name: upsAdvStateSmartUPSSpecificFaults (Continued)

Character Position	Parameter	Notes
42	T001 overtemperature	An overtemperature at the rectifier mains transformer is detected.
43	T401 overtemperature	An overtemperature at the output transformer is detected.
44	T501 overtemperature	An overtemperature at the bypass transformer is detected.
45	Battery temperature shutdown	The battery temperature exceeds the programmed shutdown level.
46	Temperature 1 warning	The temperature sensor, connected to the external connection board, is over the temperature warning level.
47	Temperature 2 warning	The temperature sensor, connected to the external connection board, is over the temperature warning level.
48	Temperature 3 warning	The temperature sensor, connected to the external connection board, is over the temperature warning level.
49	T001 temperature sensor fault	The mains input transformer temperature sensor PT100 is not connected or shorted.
50	T401 temperature sensor fault	The output transformer temperature sensor PT100 is not connected or shorted.
51	T501 temperature sensor fault	The bypass transformer temperature sensor PT100 is not connected or shorted.
55	Mains RMS fault	The rectifier mains voltage is out of tolerance.
56	Mains input RMS fault	The rectifier mains voltage on primary side of the input transformer is out of tolerance. This event is only active if a transformer is installed.
63	Bypass RMS fault	The bypass voltage is out of tolerance.
64	Bypass input RMS fault	The bypass mains voltage on the primary side of bypass transformer is out of tolerance. This event is only active if a transformer and the bypass measurement is installed.

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 Asia Pacific Sdn Bhd
No. 19, Jln Juruukur U1/19, Seksyen U135
Hicom Glenmarie Industrial Park,
40150 Shah Alam, Selangor, Malaysia
+ 60 (0) 3 5569 0331

Gutor Electronic LLC
Hardstrasse 72–74
5430 Wettingen
Switzerland

+41 (0) 56 437 34 34

https://www.se.com/ww/en/brands/gutor/gutor-service-centers.jsp

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

0000381324_04_en