Network Monitoring System

Gutor Modular DC Charger

User Guide

With the network management card AP9643 with application firmware version 2.4.0.2
06/2023 Version 2

https://www.gutor.com

Schneider Electric

Legal Information

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this guide are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owners.

This guide and its content are protected under applicable copyright laws and furnished for informational use only. No part of this guide may be reproduced or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the prior written permission of Schneider Electric.

Schneider Electric does not grant any right or license for commercial use of the guide or its content, except for a non-exclusive and personal license to consult it on an "as is" basis. Schneider Electric products and equipment should be installed, operated, serviced, and maintained only by qualified personnel.

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

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

Table of Contents

Safety Information 4
Safety Precautions for the Network Management System 5
General Information 7
Network Monitoring System Overview 7
Hardware of the Network Management System 8
Front Panel on the NMC (AP9643) 8
Network Management Card Overview 10
Watchdog Timer 10
User Accounts 11
Default User and Network Settings 11
Change User Settings 12
Reset Password 12
Command Line Interface 13
How to Log in to the Command Line Interface 13
Overview of the Command Line Interface 14
Command Line Interface Commands 15
How to Change the IP Address from the CLI with Local Connection 16
Web Interface 17
How to Log in to the Web Interface 17
Overview of the Web Interface 18
Breaker Status Page 20
Module Overview Page 21
Mimic Diagram Page 22
Web Interface Menu Structure 22
Configure the IP Address from the Web Interface 25
File Transfer 26
How to Enable SCP and FTP 26
NMC Firmware 28
Download Logs 29
Modbus Access to the Network Management Card 30
Configure Modbus Access 30
Modbus Register List 34
Modbus Wiring Diagrams 42
SNMP Access to the Network Management Card 43
SNMPv1 Access 43
SNMPv3 Access 45
SNMP Trap Receiver 47
SNMP Trap OIDs 49
SNMP GET OIDs 49
SNMP Flags 52
Troubleshooting for the Network Management Card 55
Troubleshooting for NMC Access 55
Troubleshooting for NMC SNMP 56

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.

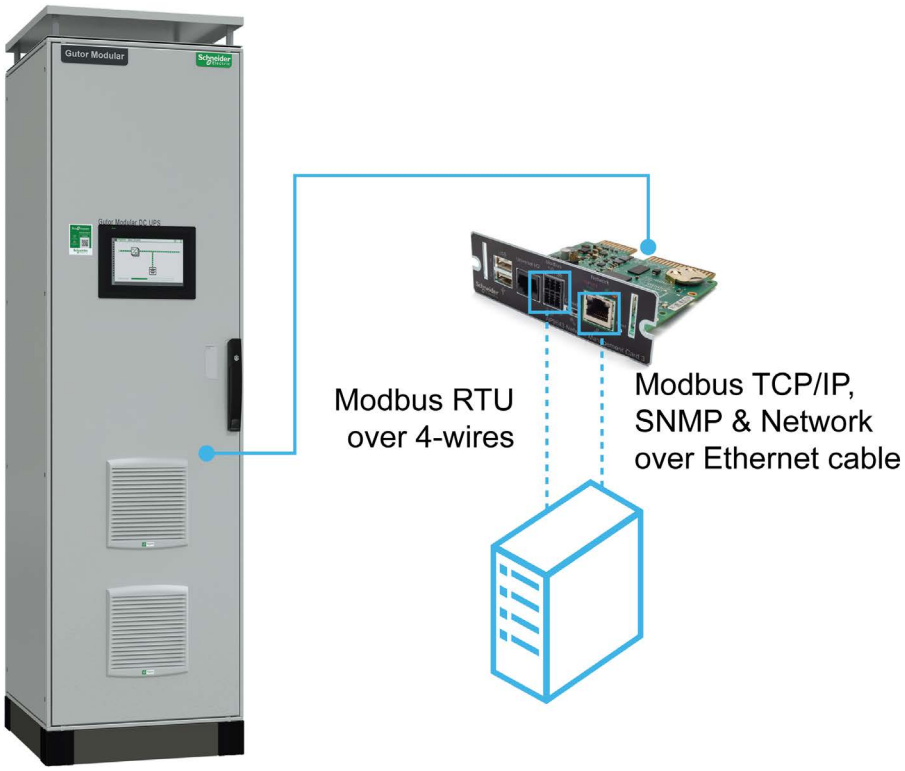
General Information

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

Network Monitoring System Overview

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

The network monitoring card (NMC) is a core component of the network monitoring system. The NMC is installed inside the Gutor system and allows for multiple connection options and protocols. As an option the NMC can be combined with additional gateways for additional protocols.

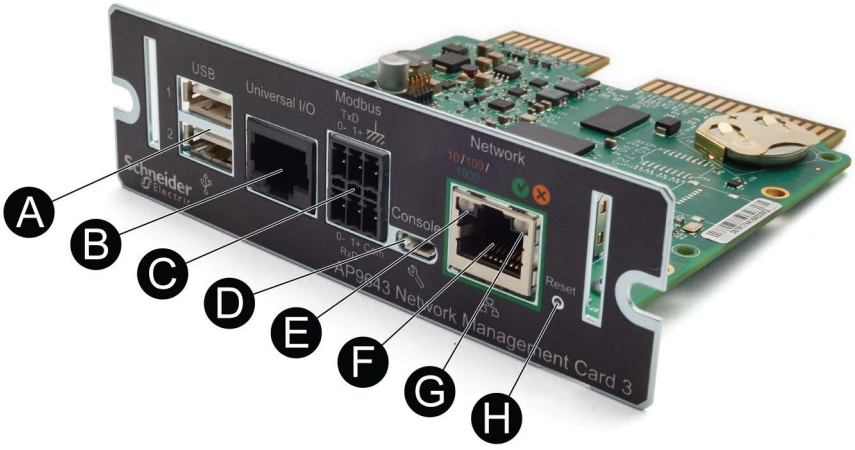


Hardware of the Network Management System

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

Front Panel on the NMC (AP9643)

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



Position	Part	Description
(A)	USB ports	(Not used)
(B)	Universal I/O sensor port	Can be used to connect a temperature sensor (AP9335T) or temperature and humidity sensor (AP9335TH).
(C)	Modbus connector	Can be used to connect the NMC to a 4-wire RS485 Modbus protocol network.
(D)	Micro-USB Console port	Can be used to connect the NMC directly to a computer with a micro-USB configuration cable. Used for a local connection to the command line interface (CLI) or for NMC firmware updates.
(E)	Link-RX/TX (10/100) LED	Indicates the status of the network. For details see section Link-RX/TX (10/100/1000) LED, page 9.
(F)	10/100/1000 Base-T connector	Can be used to connect the NMC to an Ethernet network.
(G)	Status LED	Indicates the status of the NMC. For details see section Status LED, page 9.
(H)	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 **(G)** 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 55 for more information.
Constant green	The NMC has valid TCP/IP settings.
Constant orange	One of the two reasons: • The NMC is in Bootmonitor mode. • A hardware issue has been detected on the NMC. Contact Gutor Service Center.
Flashing green	The NMC does not have valid TCP/IP settings.
Flashing orange	The NMC makes BOOTP requests.
Flickering orange	The NMC is in the boot monitor mode.
Flashing and alternating between green an orange	If the LED is flashing slowly, the NMC is making DCHP requests. If the LED is flashing quickly, the NMC is starting up.

Link-RX/TX (10/100/1000) LED

The Link-RX/TX (10/100/1000) LED **(E)** 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 55 for more information.
Constant green	The NMC is connected to a network operating at 1000 Megabits per second (Mbps).
Constant yellow	The NMC is connected to a network operating at 10-100 Mbps.
Flashing green	The NMC receives or transmits data packets at 1000 Mbps.
Flashing yellow	The NMC receives or transmits data packets at 10-100 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 a password is always required. Both the user name and the 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:

- 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:

- 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

To reset the password all the NMC must be reset to its default settings. This will remove all the configurations on the NMC, including the passwords.

To reset the NMC:

1. Hold down the **Reset button** for 20-25 seconds, as long as the status LED is green.
2. As soon as the status LED changes to orange release the **Reset button**.
3. Let the NMC reboot and start up again.
4. The IP address, network settings, user settings and any other settings will need to be configured again.

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 Micro-USB Console port on the NMC. It is also possible to connect remotely using SSH or Telnet.

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 two ways to connect to the command line interface (CLI):

- Connect and Configure Local Access to the CLI via the NMC, page 13
- Connect and Configure Remote Access to the CLI, page 14

NOTE: Remote access to the CLI requires that an IP address have already been configured. For initial setup of the NMC use local access to the CLI.

Connect and Configure Local Access to the CLI via the NMC

1. Connect the micro-USB configuration cable (Part number 960-0603) to the micro-USB console port on the NMC and a USB port on the computer.
2. On the computer open the **Device Manager**.
3. In the **Device Manager** select **Ports** and note the COM port (USB port) number the NMC was assigned.
4. Start a terminal application and configure the connected COM port (USB port) to:

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

5. Save the COM port (USB port) settings.
6. Press **Enter**, repeatedly if necessary, to open the prompt to enter the user name and password to login to the CLI.

   NOTE: On the first login the user name and password will be `apc` for the super user. You will be prompted to enter a new password after you log in.
7. For more information about the setting options in the CLI see, Overview of the Command Line Interface, page 14 and Command Line Interface Commands, page 15. For information on how to change the IP address see How to Change the IP Address from the CLI with Local Connection, page 16.
8. 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. If an IP address have not been configured for the NMC this needs to be done with local access to the NMC. 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 application from a computer on the same sub network as the NMC.
2. In the command line type `ssh <username>@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 Telnet, type `telnet xxx.xxx.xxx.xxx` instead of `ssh <username>@xxx.xxx.xxx.xxx` 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.X
(c) Copyright 2022 All Rights Reserved  Gutor Modular UPS DC&AC APP    vX.X.X.X
------------------------------------------------------------------------------
Name      : System name                                 Date : 06/21/2022
Contact   : Contact name                                Time : 11:00:45
Location  : Location name                               User : Super User
Up Time   : 0 Days 0 Hours 7 Minutes                    Stat : P+ N4+ N6+ A+
------------------------------------------------------------------------------
IPv4               : Enabled            IPv6               : Enabled
Ping Response      : Enabled
------------------------------------------------------------------------------
HTTP               : Disabled           HTTPS              : Enabled
FTP                : Disabled           Telnet             : Disabled
SSH/SCP            : Enabled            SNMPv1             : Disabled
SNMPv3             : Enabled
------------------------------------------------------------------------------
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
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      ssh         ssl         system
tcpip       tcpip6      user        userdflt    web         whoami
wifi        xferINI     xferStatus

Device Commands:
------------------------------------------------------------------------
charger     modbus      uio
```

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 Change the IP Address from the CLI with Local Connection

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 changed. From the CLI type `reboot` and press **Enter**.

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®

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.

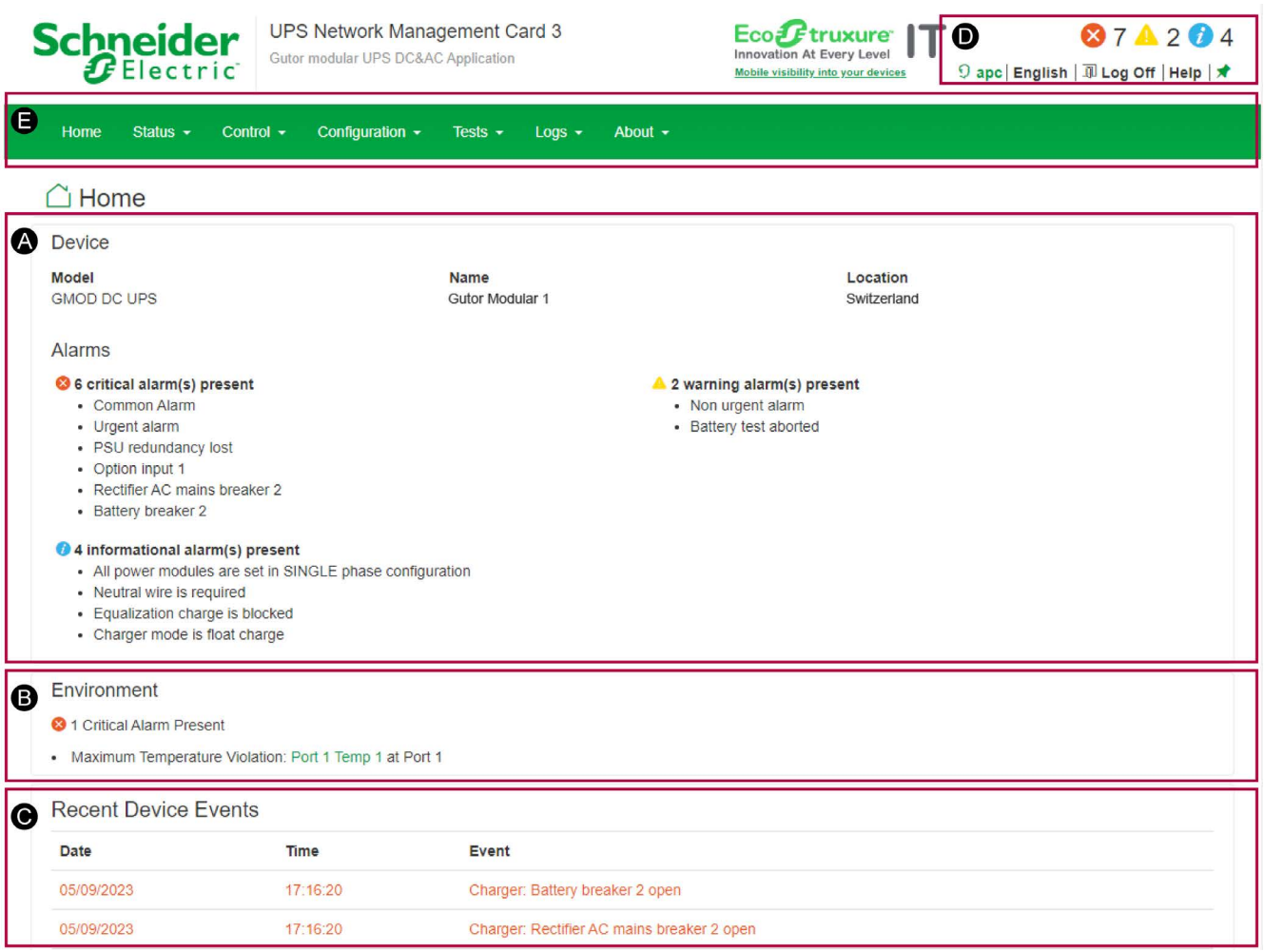
Example NMC Identifier	URL Example
With an NMC DNS name that is nmcdnsname	`https://nmcdnsname`
With an NMC IP address of 139.225.6.133	`https://139.225.6.133`
With an NMC IP address of 139.225.6.133 and specified port of :5000	`https://139.225.6.133:5000`
With an NMC IPv6 address of 2001:db8:1::2c0:b7ff:fe00:1100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

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

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

(E) 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: Environment

The **Environment** section shows a quick status of any connected temperature or temperature/humidity sensor, and if any alarm is active for the connected sensor.

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.

It is possible to enable/disable color coded events. To do that navigate to **Configuration > Security > Local Users > Default Settings**, then under **User Preferences** there is a check box for **Event Log Color Coding**.

Event Text Color	Event Severity	Severity Description
Red/Orange	Critical	A critical alarm exists and requires immediate action.
Yellow	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, modules, switchgear, sensors, network and mimic diagram.
- **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.

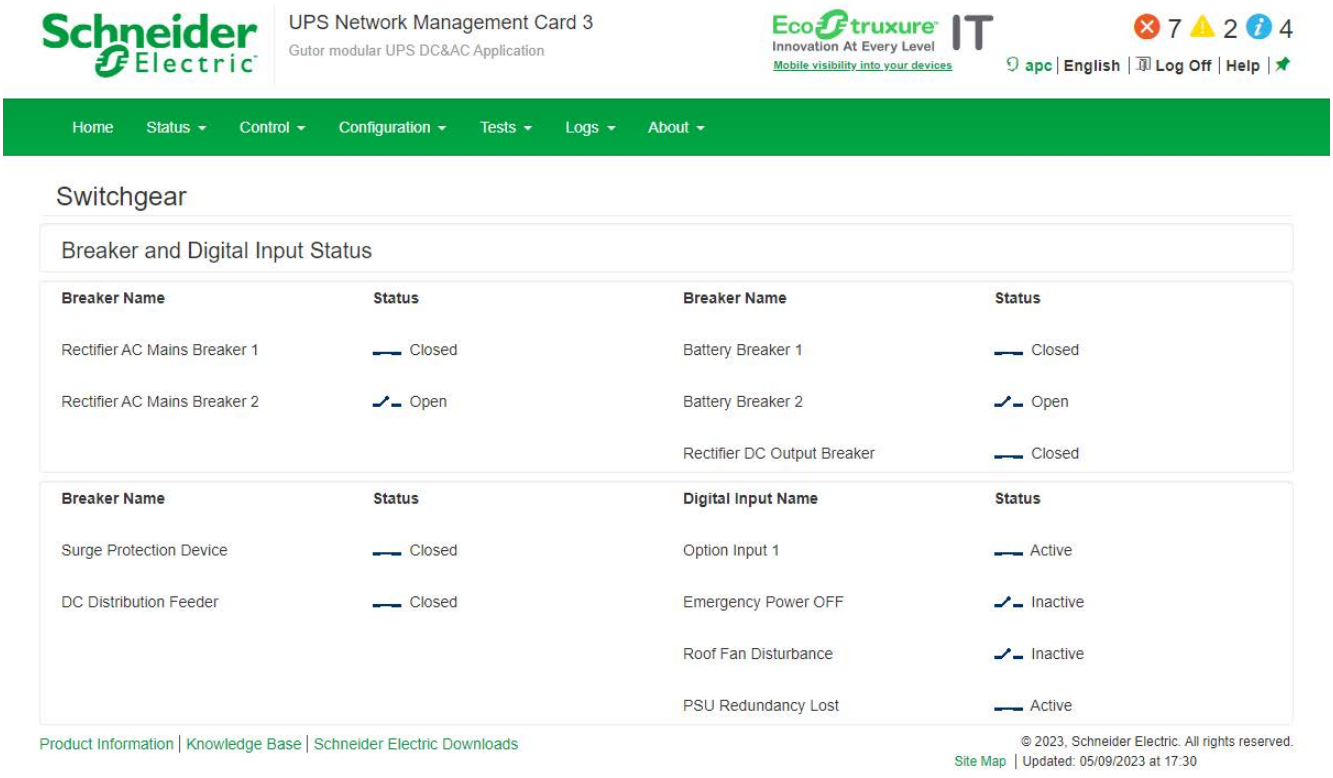
  NOTE: By default the size of the event log and data log is set to 1500 entries (maximum 30000 entries).
- **About:** View the information about the system, network settings and firmware. Contains information for troubleshooting.

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

Breaker Status Page

To view the breaker status page navigate to **Status > Switchgear**

NOTE: Some breakers are optional and might not be available in the system configuration. For the actual breakers used, position and reference designator of the breakers please see the *Drawings* for that specific system.



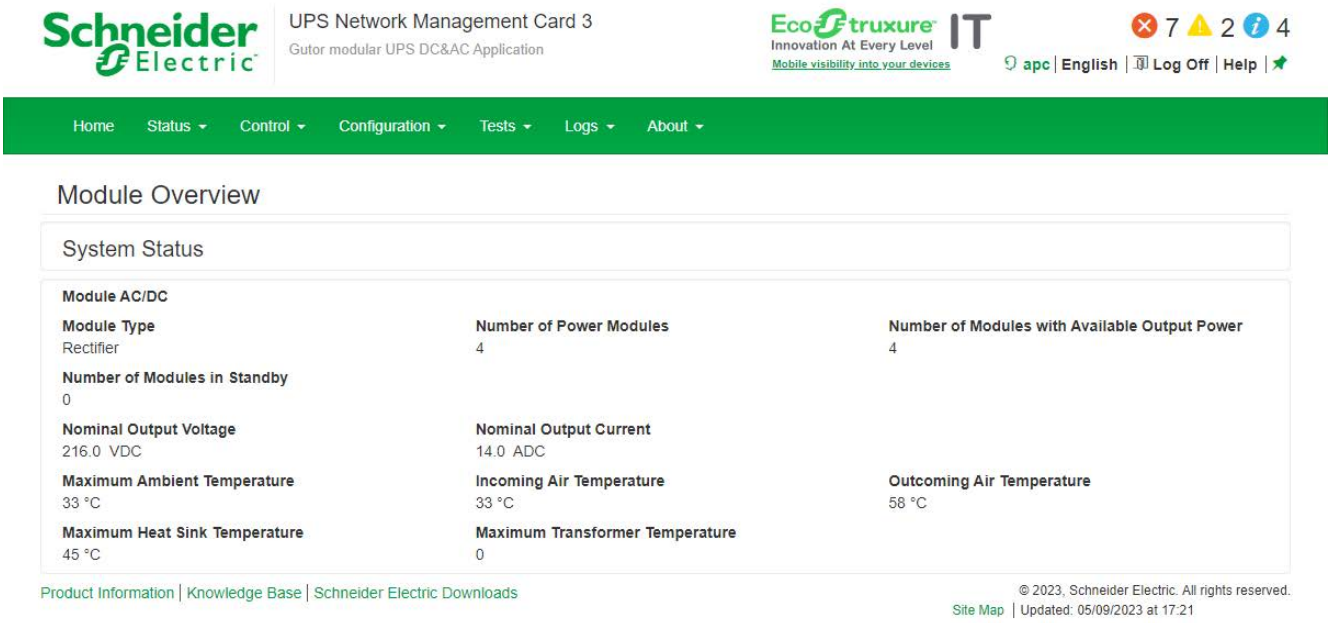
Breaker Name	Open Status	Closed Status
Rectifier AC mains breaker 1	The rectifier AC mains input breaker has been manually opened or has tripped.	The rectifier AC mains input breaker is closed.
Rectifier AC mains breaker 2	The rectifier AC mains input breaker has been manually opened or has tripped.	The rectifier AC mains input breaker is closed.

Breaker Name	Open Status	Closed Status
Battery breaker 1	One or both battery breakers have been manually opened or have tripped. Always monitors the internal battery breaker, as an option it can also monitor an external battery if the signal is wired in series.	All battery breakers are closed.
Battery breaker 2	One or both battery breakers have been manually opened or have tripped. Always monitors the internal battery breaker, as an option it can also monitor an external battery if the signal is wired in series.	All battery breakers are closed.
Rectifier DC output breaker	The rectifier DC output breaker is open.	The rectifier DC output breaker is closed.
Surge protection device	The AC input surge arrester has tripped.	The AC input surge arrester is closed.
DC distribution feeder	One or more distribution output feeders has tripped.	All output feeders are closed.

Digital Input Name	Inactive Status	Active Status
Option input 1	Digital input option 1 signal is inactive.	Digital input option 1 signal is active.
Emergency power OFF	The emergency power off (EPO) signal is inactive.	The emergency power off (EPO) signal is active.
Roof fan disturbance	Roof fan disturbance signal is inactive. The roof fans are operable.	Roof fan disturbance signal is active. One or more fans have the speed reduce, signal missing or is inoperable.
PSU redundancy lost	Power supply unit (PSU) redundancy lost signal is inactive.	Power supply unit (PSU) redundancy lost signal is active.

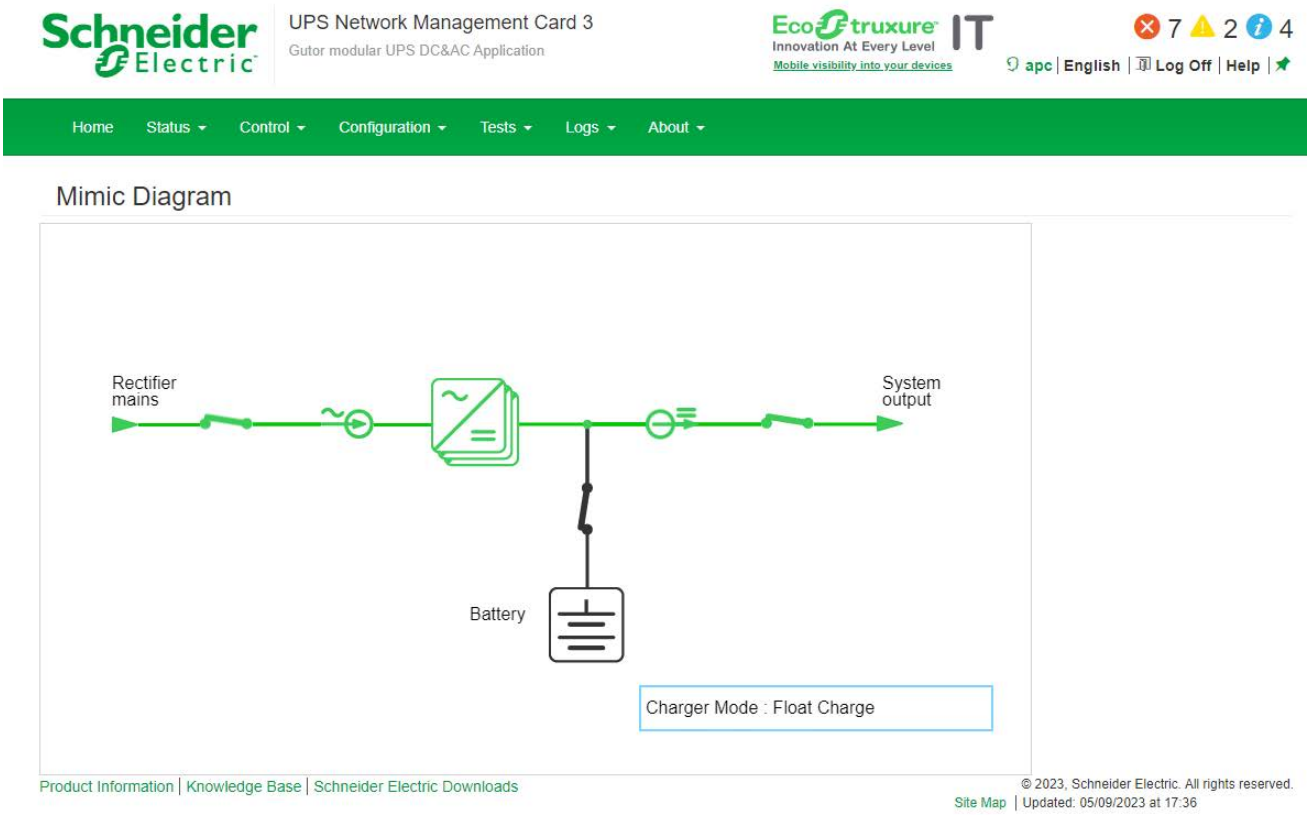
Module Overview Page

To view the module overview page navigate to **Status > Module Overview**.



Mimic Diagram Page

To view the mimic diagram page navigate to **Status > Mimic Diagram**.

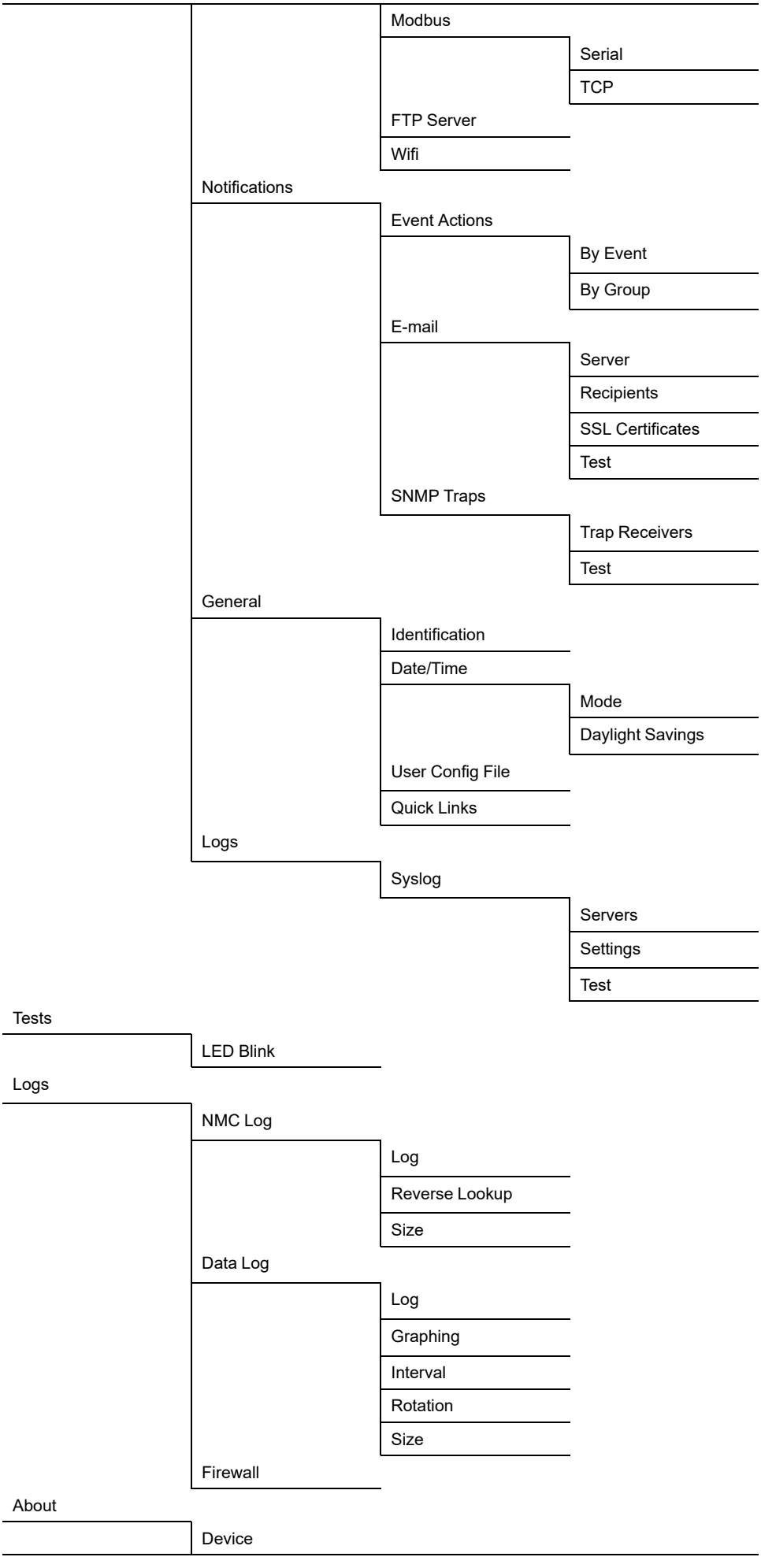


Web Interface Menu Structure

The navigation from the main menu has 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.

- Home
- Status
  - Overview
  - Measurements
    - Input
    - Output
    - Battery
  - Mimic Diagram
  - Switchgear
  - Network
  - Module Overview
- Control
  - Security
    - Session Management
  - Network
    - Reset/Reboot

- Configuration
  - Charger
    - Battery
  - Security
    - Session Management
    - Ping Response
    - Local Users
      - Management
      - Default Settings
    - Remote Users
      - Authentication
      - RADIUS
    - Firewall
      - Configuration
      - Activate Policy
      - Activate Rules
      - Create/Edit Policy
      - Load Policy
      - Test
    - 802.1X Security
      - Access
      - Configuration
    - SSL Certificates
  - 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
Wifi
Notifications
Event Actions
By Event
By Group
E-mail
Server
Recipients
SSL Certificates
Test
SNMP Traps
Trap Receivers
Test
General
Identification
Date/Time
Mode
Daylight Savings
User Config File
Quick Links
Logs
Syslog
Servers
Settings
Test
Tests
LED Blink
Logs
NMC Log
Log
Reverse Lookup
Size
Data Log
Log
Graphing
Interval
Rotation
Size
Firewall
About
Device

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 SCP and FTP

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

- Enable SCP from the CLI, page 26
- Enable FTP from the CLI, page 26
- Enable SCP from the Web Interface, page 27
- Enable FTP from the Web Interface, page 27

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 changed. From the CLI type `reboot` and press **Enter**.

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.

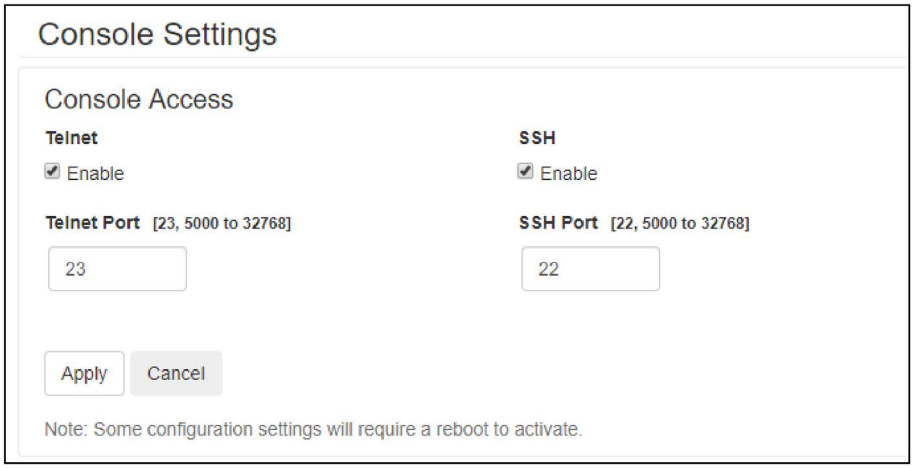
   NOTE: Reboot the NMC to apply changed. From the CLI type `reboot` and press **Enter**.

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.



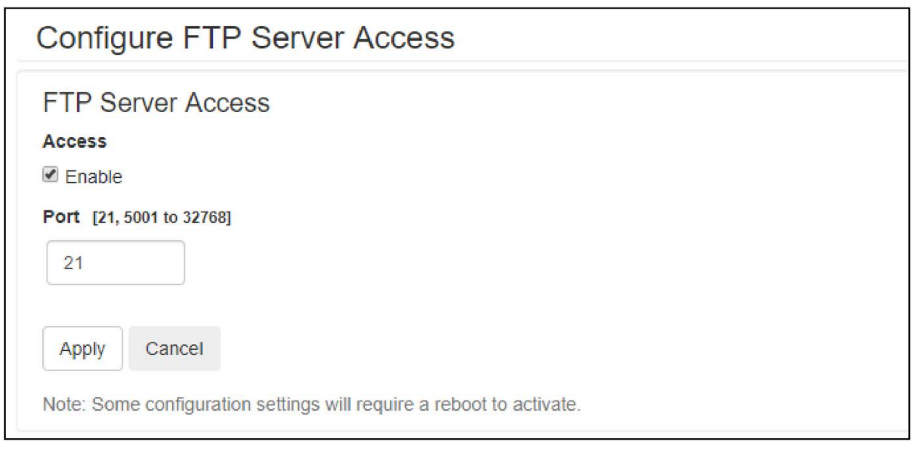
4. Navigate to **Configuration > Network > FTP server**.
5. Make sure that the FTP enable box is unchecked. Click **Apply** to save the changes.
6. SCP is now enabled.

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

Enable FTP from the Web Interface

1. Log in to the web interface.
2. Navigate to **Configuration > Network > FTP server**.
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.

NMC Firmware

The firmware for the NMC card in a Gutor system consists of one file. Examples of the file name are `apc_hw21_gmod_2-1-0-3.nmc3` or `apc_hw21_sxw_1-4-0-15.nmc3`.

Update the NMC Firmware with SCP

To update the firmware using SCP the NMC needs to have SCP enabled and configured network settings. 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: `scp apc_hw21_YYY_v-v-v-v.nmc3 apc@xxx.xxx.xxx.xxx:apc_hw21_YYY_v-v-v-v.nmc3` and press **Enter** to run.
3. Where `YYY` is the system type code, `v-v-v-v` is the version of the firmware file and `xxx.xxx.xxx.xxx` is the IP address of the NMC.
4. Wait 20 seconds while the card is rebooting.

Verify Firmware Update

To verify that the firmware update succeeded and to check the firmware version it is possible to:

- From the NMC web interface navigate to **About > Network**.
- Use a SNMP GET to the MIB II `sysDescr` 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 1500 entries (maximum 30000 entries).

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`

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 has 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.

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 42.

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

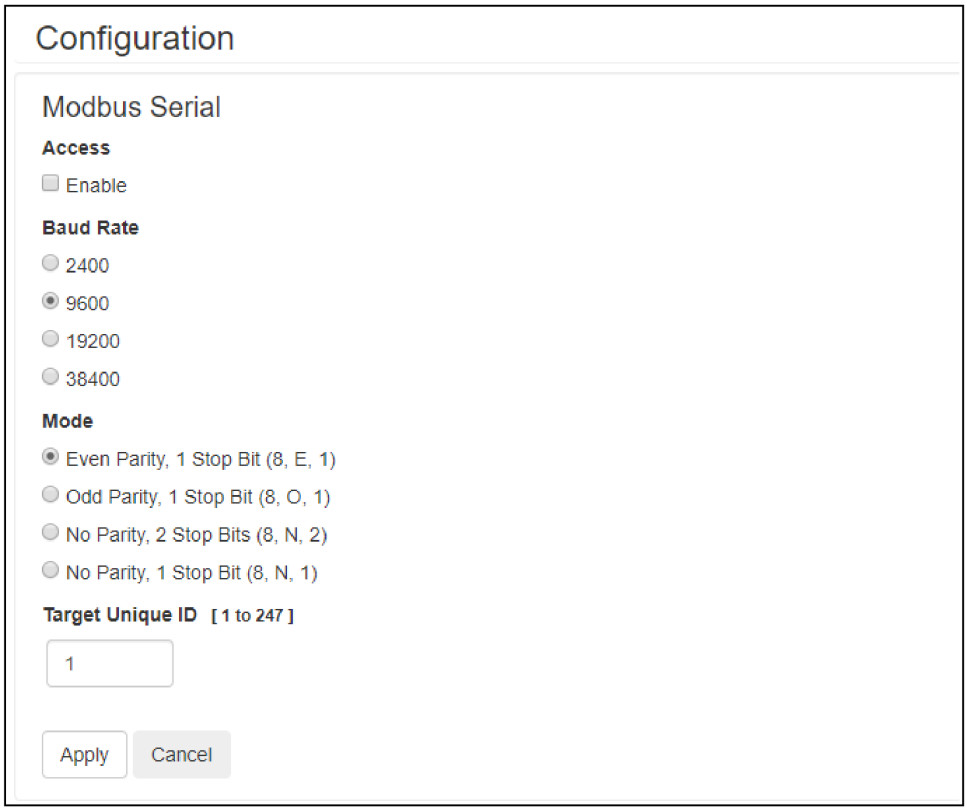
1. Log in to the CLI.
2. To see the configuration options type `modbus ?`.

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.
Modbus TCP keep-alive	`-ka`	`enable | disable`	Enables or disables Modbus TCP keep-alive.

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).
   - **Keep-Alive:** When enabled, an acknowledge request will be sent to any open connection that has been idle for a long time (2h). This option is independent of the communication timeout setting.
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 Register List

The Modbus register is supported both on function call 2 and function call 4. The data is stored as either:

- UINT32 (unsigned 32–bit integer), most significant word in n+0, least significant word in n+1, also known as big-endian.
- UINT16 (unsigned 16–bit integer), registers are transmitted as with the most significant bit (MSB) first, also known as big-endian.
- ASCII (the printable ASCII subset from 0x20 – 0x7E), strings with unused characters (length less than maximum) are filled with nulls. Strings are two characters per register, first character in high-order byte, second character in low-order byte.
- Boolean (a single bit, 0 or 1), 1 = alarm active, reserved or undefined registers will return an error. Blocked reads which begin with a valid register will not return an error but will return zeros for undefined registers.
- FP (floating point)

All registers are read only (RO). Bit 0 is the least significant bit.

NOTE: For the Modbus register the absolute starting register address is 0, this is equivalent to 40001 in Modicon terminology (address zero when transmitted over the wire).

Modbus Register	Name	Data Type (Length / Number of Registers)	Description [Unit of Measurement]
General status			
1	NMC model number	ASCII (9)	The model number of the NMC.
10	NMC serial number	ASCII (8)	The serial number of the NMC.
18	NMC firmware revision APP	ASCII (9)	The firmware revision of the Gutor application for the NMC.
27	NMC firmware revision	ASCII (9)	The firmware revision of the NMC.
36	NMC date of manufacture	ASCII (6)	The manufacturing date for the NMC.
42	NMC/UPS time (hh:mm: ss format)	ASCII (4)	The NMC/system time (hh:mm:ss format).
46	NMC/UPS date (mm/dd/ yyyy format)	ASCII (5)	The NMC/system date (mm/dd/yyyy format).
51	Product name	ASCII (40)	The name for the system entered in the NMC.
91	Probe 1 temperature	UINT16 (1)	The measured temperature from the optionally connected temperature and humidity sensor (AP9335TH) or the temperature sensor (AP9335T). Only available if the sensor is connected.
92	Probe 1 humidity	UINT16 (1)	The measured humidity from the optionally connected temperature and humidity sensor (AP9335TH). Only available if the sensor is connected.
108	UPS model	ASCII (16)	The model of the connected UPS or system.
124	UPS type	ASCII (16)	The type of the connected UPS or system.
140	UPS serial number	ASCII (8)	The serial number of the connected UPS or system.
148	UPS manufacturing date	ASCII (6)	The manufacturing date of the connected UPS or system.
201	MCU Modbus revision	UINT16 (1)	The Modbus revision of the UPS or system controller.
202	MCU part number	UINT32 (2)	The part number of the UPS or system controller.
204	Software version of MCU (Index)	UINT16 (1)	Software version of the UPS or system controller (Index).
206	MCU serial number word 1 (LB)	UINT16 (1)	The UPS or system controller’s serial number word 1 (LB).
207	MCU serial number word 2	UINT16 (1)	The UPS or system controller’s serial number word 2.

Modbus Register	Name	Data Type (Length / Number of Registers)	Description [Unit of Measurement]
208	MCU serial number word 3	UINT16 (1)	The UPS or system controller's serial number word 3.
209	MCU serial number word 4 (HB)	UINT16 (1)	The UPS or system controller's serial number word 4 (HB).
1000	**NMC Alarm - Alarm register 1**		
1000 (Bit 0)	Communication lost with MCU	Boolean	The communication between the NMC and the UPS or system controller is lost.
1000 (Bit 1)	Lost the management interface-to-UPS communication while the UPS was on battery	Boolean	The communication management interface-to-UPS between the NMC and the UPS or system controller is lost.
1000 (Bit 2)	Unknown system type	Boolean	Unknown system type is detected.
1000 (Bit 3)	Firmware incompatibility detected	Boolean	The Gutor NMC application firmware is incompatible with the system controller (MCU) firmware.
1001	**NMC Alarm - Alarm register 2**		
1001 (Bit 0)	Low temperature threshold violation at remote sensor	Boolean	The measured temperature is below the configured low temperature setting. Only available if (AP9335TH) or (AP9335T) is connected to the NMC.
1001 (Bit 1)	Minimum temperature threshold violation at remote sensor	Boolean	The measured temperature is below the configured minimum temperature setting. Only available if (AP9335TH) or (AP9335T) is connected to the NMC.
1001 (Bit 2)	High temperature threshold violation at remote sensor	Boolean	The measured temperature is above the configured high temperature setting. Only available if (AP9335TH) or (AP9335T) is connected to the NMC.
1001 (Bit 3)	Maximum temperature threshold violation at remote sensor	Boolean	The measured temperature is above the configured maximum temperature setting. Only available if (AP9335TH) or (AP9335T) is connected to the NMC.
1001 (Bit 4)	Low humidity threshold violation at remote	Boolean	The measured humidity is below the configured low humidity setting. Only available if (AP9335TH) is connected to the NMC.
1001 (Bit 5)	Minimum humidity threshold violation at remote sensor	Boolean	The measured humidity is below the configured minimum humidity setting. Only available if (AP9335TH) is connected to the NMC.
1001 (Bit 6)	High humidity threshold violation at remote sensor	Boolean	The measured humidity is above the configured high humidity setting. Only available if (AP9335TH) is connected to the NMC.
1001 (Bit 7)	Maximum humidity threshold violation at remote sensor	Boolean	The measured humidity is above the configured maximum humidity setting. Only available if (AP9335TH) is connected to the NMC.
1001 (Bit 8)	Lost communication to NMC integrated environmental sensor	Boolean	The communication to the temperature and humidity or the temperature sensor connected to the NMC card is interrupted. Only available if (AP9335TH) or (AP9335T) is connected to the NMC.
1002	**System main alarm - Alarm register 1**		
1002 (Bit 0)	Common alarm	Boolean	One or more alarms that are configured for the common alarm are present. The common alarm is mainly intended to be used for external signals.
1002 (Bit 1)	Urgent event	Boolean	One or more urgent alarms that require immediate actions are present.
1002 (Bit 2)	Non urgent alarm	Boolean	One or more non urgent alarms that require actions are present.
1002 (Bit 3)	HMI to MCU communication fault	Boolean	The communication between the display and the controller is interrupted or lost.
1002 (Bit 4)	ADBUS communication is lost	Boolean	The communication with one or more optional ADBUS cards are interrupted or lost.
1002 (Bit 5)	Battery symmetry error	Boolean	The battery symmetry is out of tolerance.

Modbus Register	Name	Data Type (Length / Number of Registers)	Description [Unit of Measurement]
1002 (Bit 6)	Battery current-limiting is active	Boolean	The battery charging current has reached its maximum limit. The rectifier will regulate the DC output current to not overcharge the batteries with a too high charging current.
1002 (Bit 7)	High DC warning alarm	Boolean	The system output voltage is above the set high warning voltage level.
1002 (Bit 8)	High DC shutdown alarm	Boolean	The system output voltage is above the set high shutdown voltage level.
1002 (Bit 9)	Low DC warning alarm	Boolean	The system output voltage is below the set low warning voltage level.
1002 (Bit 10)	Low DC shutdown alarm	Boolean	The system output voltage is below the set low shutdown voltage level.
1002 (Bit 11)	Number of rectifier modules is below warning limit	Boolean	Only for redundant N+x and N+N module configurations. The number of redundant rectifier modules is currently below the warning limit because of some inoperable rectifier modules. (Calculated based on number of modules).
1002 (Bit 12)	Number of rectifier modules is below critical limit	Boolean	Only for redundant N+x and N+N module configurations. The number of redundant rectifier modules are currently below the critical limit because of some inoperable rectifier modules. (Calculated based on number of modules).
1002 (Bit 13)	Power module current reserve is lost	Boolean	Only for redundant N+x and N+N module configurations. The output current redundancy is currently not available because of some inoperable rectifier modules. (Calculated based on output current).
1002 (Bit 14)	One or more modules are inoperable	Boolean	One or more rectifier modules are inoperable. Depending on the module configuration this might be a warning or a critical alarm. If the system has no redundant rectifier modules, immediate action is required.
1002 (Bit 15)	One or more modules in over temperature warning	Boolean	One or more rectifier modules are above the high temperature level.
1007	**Main controller (MCU) main alarm - Alarm register 1**		
1007 (Bit 0)	MCU hard reset summary warning	Boolean	The MCU (controller) has detected a hard reset.
1007 (Bit 1)	MCU system errors summary alarm	Boolean	The MCU (controller) has detected a system error, for example with the real time clock (RTC), EEPROM, filesystem or task timed out.
1007 (Bit 2)	MCU memory errors summary alarm	Boolean	The MCU (controller) is out of memory, for example for the filter or heap.
1007 (Bit 3)	MCU Modbus errors summary alarm	Boolean	The MCU (controller) has detected a Modbus server error, for example with Modbus TCP/serial server communication.
1007 (Bit 4)	MCU initialization is in progress	Boolean	The MCU (controller) is initializing.
1007 (Bit 5)	MCU soft reset is active	Boolean	The MCU (controller) is performing a software reset.
1007 (Bit 6)	MCU watchdog reset summary alarm	Boolean	The MCU (controller) has detected a watchdog reset, for example in the MCU (controller), or in one or more modules.
1007 (Bit 7)	MCU temperature is too high	Boolean	The MCU (controller) temperature is above the set high temperature level.
1009	**System main configuration - Alarm register 1**		
1009 (Bit 0)	All power modules are set in SINGLE phase configuration	Boolean	The rectifier modules are configured for a 1-phase input.
1009 (Bit 1)	All power modules are set in THREE phase configuration	Boolean	The rectifier modules are configured for a 3-phase input.
1009 (Bit 2)	Neutral wire is required	Boolean	The neutral on the input must be wired. Only for systems with a 1-phase input.
1009 (Bit 3)	One of the power modules is in DC-DC mode	Boolean	One of the rectifier/DC–DC modules is configured for DC-DC conversion.

Modbus Register	Name	Data Type (Length / Number of Registers)	Description [Unit of Measurement]
1012	**System main operation modes - Alarm register 1**		
1012 (Bit 0)	Charger mode is boost-charge	Boolean	Boost charge mode is active in the rectifier modules. The rectifier DC output voltage is higher than float charge voltage.
1012 (Bit 1)	Boost charge is blocked	Boolean	Switch to boost charge mode is blocked. The mode can be blocked by an external/internal signal.
1012 (Bit 2)	Charger mode is float-charge	Boolean	Float charge mode is active in the rectifier modules.
1012 (Bit 3)	Charger mode is direct feed, no batt	Boolean	The direct feed mode is active in the rectifier modules. Caution, batteries might not be charged anymore.
1012 (Bit 6)	On battery	Boolean	Battery operation mode is active (manually or automatically). The batteries are being discharged to supply the load.
1012 (Bit 7)	Battery equalizing charging	Boolean	Equalizing charge mode is active in the rectifier modules. The rectifier DC output voltage is higher than float and boost charge voltage.
1012 (Bit 8)	Battery equalizing charging is blocked	Boolean	Switch to equalizing charge mode is blocked. The mode can be blocked by an external/internal signal.
1016	**System breaker status - Alarm register 1**		
1016 (Bit 0)	Rectifier AC mains breaker 1	Boolean	The rectifier AC mains input breaker is open.
1016 (Bit 1)	Battery breaker 1	Boolean	The internal battery breaker and/or the external battery breaker is open.
1016 (Bit 2)	Rectifier DC output breaker	Boolean	The rectifier DC output breaker is open.
1016 (Bit 3)	PSU redundancy lost	Boolean	Power supply unit (PSU) redundancy lost signal is inactive.
1016 (Bit 4)	DC distribution feeder	Boolean	One or more distribution output feeders has tripped.
1016 (Bit 5)	Surge protection device	Boolean	The AC input surge arrester has tripped.
1016 (Bit 6)	Option input 1	Boolean	Digital input option 1 signal is inactive.
1016 (Bit 7)	Emergency power OFF	Boolean	The emergency power off (EPO) signal is active.
1016 (Bit 12)	Rectifier AC mains breaker 2	Boolean	The dual rectifier AC mains input breaker is open.
1016 (Bit 13)	Battery breaker 2	Boolean	The internal battery breaker and/or the external battery breaker is open.
1016 (Bit 15)	Roof fan disturbance	Boolean	One or more fans have the speed reduce, signal missing or is inoperable.
1018	**Battery status/alarm - Alarm register 1**		
1018 (Bit 0)	Battery test running	Boolean	The system is running a battery capacity probe.
1018 (Bit 1)	A weak battery exists	Boolean	The result of a battery capacity probe shows that the battery capacity is too low.
1018 (Bit 2)	Battery test aborted	Boolean	A battery capacity probe was interrupted.
1018 (Bit 3)	Battery test configuration error	Boolean	The battery capacity probe is not configured correctly.
1018 (Bit 4)	Battery circuit test failed	Boolean	The battery circuit test showed that the battery is not available to take over the load if needed.
1018 (Bit 5)	Battery circuit test configuration error	Boolean	The battery circuit test is not configured correctly.

Modbus Register	Name	Data Type (Length / Number of Registers)	Description [Unit of Measurement]
1018 (Bit 6)	Battery temperature measurement invalid	Boolean	The battery temperature sensor is returning an invalid value (NaN or <-90°C). The sensor might not be configured correctly or is not operating correctly.
1018 (Bit 7)	Battery current-limiting configuration error	Boolean	The battery current limiting is not configured correctly.
1020	**Charger detailed alarm - Alarm register 1**		
1020 (Bit 0)	Module configuration mismatch is detected	Boolean	One or more rectifier modules mismatch configuration are detected.
1020 (Bit 4)	All rectifier modules switched off	Boolean	All rectifier modules are switched off from the display or through an external signal.
1020 (Bit 5)	Some rectifier modules switched off	Boolean	Some rectifier modules are switched off from the display or through an external signal.
1020 (Bit 6)	Some rectifier modules in current limitation	Boolean	One or more rectifier modules have reached current limitation (modules are overloaded).
1020 (Bit 7)	Some rectifier modules shutdown for overvoltage	Boolean	One or more rectifier modules have switched OFF because of too high output voltage. (The red LED will flash fast 3 times.)
1020 (Bit 8)	Rectifier output voltage out of range	Boolean	The rectifier modules output voltage is above or below the tolerance level.
1020 (Bit 9)	Mains input in fault condition	Boolean	The rectifier mains input is not available. The rectifier modules cannot operate.
1020 (Bit 10)	One or more modules with input voltage out of range	Boolean	The rectifier mains input is out of tolerance for one or more rectifier modules. Depending on the cause the rectifier modules might not run.
1020 (Bit 12)	One or more modules have an inoperable fan	Boolean	At least one of the fans is rotating too slowly or is inoperable.
1020 (Bit 14)	One or more modules in overtemperature shutdown	Boolean	One or more rectifier modules are above the temperature shutdown level. The rectifier modules will run with reduced output power.
1020 (Bit 15)	One or more modules with defective temperature sensor	Boolean	One or more rectifier modules have a temperature sensor that is inoperable.
1021	**Charger detailed alarm - Alarm register 2**		
1021 (Bit 0)	Load sharing error in all power modules	Boolean	The active load sharing between all the rectifier modules is not functioning correctly.
1021 (Bit 1)	Fan warning in all power modules	Boolean	The fans in all rectifier modules are rotating too slowly.
1021 (Bit 2)	Fan fault in all power modules	Boolean	The fans in all rectifier modules are inoperable.
1021 (Bit 3)	Input voltage out of range in all power modules	Boolean	Input voltage out of range in all rectifier modules.
1021 (Bit 4)	Output voltage out of range in all power modules	Boolean	The rectifier mains input is out of tolerance for all rectifier modules.
1021 (Bit 5)	Power module bus error	Boolean	There is a communication bus error between all rectifier modules and the controller (MCU).
1026	**Charger filter logic alarm - Alarm register 1**		
1026 (Bit 0)	Logic Gate - Option 1 alarm	Boolean	Customized (programmable) alarm on request, see system settings or drawings if used.
1026 (Bit 1)	Logic Gate - Option 2 alarm	Boolean	Customized (programmable) alarm on request, see system settings or drawings if used.
1026 (Bit 2)	Logic Gate - Option 3 alarm	Boolean	Customized (programmable) alarm on request, see system settings or drawings if used.
1027	**Charger filter delay alarm - Alarm register 1**		

Modbus Register	Name	Data Type (Length / Number of Registers)	Description [Unit of Measurement]
1027 (Bit 0)	Delay Gate - Option 1 alarm	Boolean	Customized (programmable) alarm on request, see system settings or drawings if used.
1028	**Charger filter set-reset gate alarm - Alarm register 1**		
1028 (Bit 0)	Filter Set-Reset Gate option 1 alarm	Boolean	Customized (programmable) alarm on request, see system settings or drawings if used.
1028 (Bit 1)	Filter Set-Reset Gate option 2 alarm	Boolean	Customized (programmable) alarm on request, see system settings or drawings if used.
1028 (Bit 2)	Filter Set-Reset Gate option 3 alarm	Boolean	Customized (programmable) alarm on request, see system settings or drawings if used.
1029	**Earth fault monitoring module alarm (IMDC) - Alarm register 1**		
1029 (Bit 0)	IMD 1 - Earth fault positive resistance warning	Boolean	Insulation resistance from the positive pole below the warning level detected by the optionally connected GUMD-ADB-IMD. Requires a connected GUMD-ADB-IMD.
1029 (Bit 1)	IMD 1 - Earth fault negative resistance warning	Boolean	Insulation resistance from the negative pole below the warning level detected by the optionally connected GUMD-ADB-IMD. Requires a connected GUMD-ADB-IMD.
1029 (Bit 2)	IMD 1 - Earth fault positive resistance alarm	Boolean	Insulation resistance from the positive pole below the alarm level detected by the optionally connected GUMD-ADB-IMD. Requires a connected GUMD-ADB-IMD.
1029 (Bit 3)	IMD 1 - Earth fault negative resistance alarm	Boolean	Insulation resistance from the negative pole below the alarm level detected by the optionally connected GUMD-ADB-IMD. Requires a connected GUMD-ADB-IMD.
1031	**Batter supervision module alarm (BM60) - Alarm register 1**		
1031 (Bit 0)	BM60 1 - Battery measurement out of range on channel 1	Boolean	The measurement on channel 1 from the optionally connected GUMD-ADB-BM60 is out of tolerance of the specified range. Requires a connected GUMD-ADB-BM60.
1031 (Bit 1)	BM60 1 - Battery measurement out of range on channel 2	Boolean	The measurement on channel 2 from the optionally connected GUMD-ADB-BM60 is out of tolerance of the specified range. Requires a connected GUMD-ADB-BM60.
1031 (Bit 2)	BM60 1 - Battery measurement out of range on channel 3	Boolean	The measurement on channel 3 from the optionally connected GUMD-ADB-BM60 is out of tolerance of the specified range. Requires a connected GUMD-ADB-BM60.
1031 (Bit 3)	BM60 1 - Battery measurement out of range on channel 4	Boolean	The measurement on channel 4 from the optionally connected GUMD-ADB-BM60 is out of tolerance of the specified range. Requires a connected GUMD-ADB-BM60.
1031 (Bit 4)	BM60 1 - Battery supervision module type mismatch	Boolean	The optionally connected GUMD-ADB-BM60 card settings is not matching the battery configuration. Requires a connected GUMD-ADB-BM60.
1033	**Battery supervision module alarm (BM300) - Alarm register 1**		
1033 (Bit 0)	BM300 1 - Battery measurement out of range on channel 1	Boolean	The measurement on channel 1 from the optionally connected GUMD-ADB-BM300 is out of tolerance of the specified range. Requires a connected GUMD-ADB-BM300.
1033 (Bit 1)	BM300 1 - Battery measurement out of range on channel 2	Boolean	The measurement on channel 2 from the optionally connected GUMD-ADB-BM300 is out of tolerance of the specified range. Requires a connected GUMD-ADB-BM300.
1033 (Bit 2)	BM300 1 - Wrong battery monitoring card detected	Boolean	The optionally connected GUMD-ADB-BM300 card settings is not matching the battery configuration. Requires a connected GUMD-ADB-BM300.
Charger - Dynamic data register 1			
5000	Rectifier module nominal voltage (output)	FP (2)	The nominal voltage of the rectifier modules in the system. [V]
5002	Rectifier module nominal current (output)	FP (2)	The nominal current of the rectifier modules in the system. [A]
5004	Number of power modules	UINT16 (1)	The number of rectifier modules connected and installed in the system.
5005	Modules with available output power	UINT16 (1)	The number of rectifier modules with an output power available.

Modbus Register	Name	Data Type (Length / Number of Registers)	Description [Unit of Measurement]
5006	Number of modules in standby	UINT16 (1)	The number of rectifier modules currently in standby.
5009	DC Rectifier output voltage	FP (2)	The DC output voltage of the rectifier modules in the system. [V]
5011	DC Rectifier output current	FP (2)	The total DC output current of the rectifier modules in the system. [A]
5013	Load current	FP (2)	The DC current used by the load. [A]
5015	Output power	FP (2)	The total output power of the system. [kW]
5017	Charger output load (% kVA)	FP (2)	The relative output power of the system. [%]
5019	Maximum rectifier ambient temperature	FP (2)	Maximum rectifier ambient temperature [°C]
5021	ACM 1 - AC Voltage L1-N	FP (2)	The measured AC voltage on L1-N from the optionally connected GUMD-ADB-ACM to rectifier system 1. Requires a connected GUMD-ADB-ACM. [V]
5023	ACM 1 - AC Voltage L2-N	FP (2)	The measured AC voltage on L2-N from the optionally connected GUMD-ADB-ACM to rectifier system 1. Requires a connected GUMD-ADB-ACM. [V]
5025	ACM 1 - AC Voltage L3-N	FP (2)	The measured AC voltage on L3-N from the optionally connected GUMD-ADB-ACM to rectifier system 1. Requires a connected GUMD-ADB-ACM. [V]
5027	Relative output power low-pass filtered	FP (2)	The relative output power low-pass is filtered.
Battery - Dynamic data register 1			
5095	Battery voltage 1	FP (2)	The total measured battery voltage of string 1. [V]
5097	Battery current 1	FP (2)	The total measured battery current of string 1. [C]
5099	Nominal battery capacity 1	FP (2)	The available nominal battery capacity of string 1. [Ah]
5101	Final discharge voltage battery 1	FP (2)	The battery discharge voltage of string 1. [V]
5103	Battery capacity withdrawn 1	FP (2)	The amount of used battery capacity of string 1. [Ah]
5115	Battery temperature	FP (2)	The measured battery temperature by the system's battery temperature sensor. The temperature unit depends on the NMC setting. Temperatures below zero reads as 0. [°C or °F]
5117	Battery test duration	FP (2)	The duration of the latest battery capacity probe. [s]
5119	Last battery test (time stamp)	UINT32 (2)	The time stamp of the last battery capacity probe.
5121	Last battery circuit test (time stamp)	UINT32 (2)	The time stamp of the last battery capacity probe.
5123	Last battery replacement	UINT32 (2)	The time stamp of the last battery replacement.
Charger algebra - Dynamic data register 1			
5157	Input power	FP (2)	The system input power. [kW]
5165	Mains frequency (Max of first 30 modules)	FP (2)	The calculated maximum mains frequency of the first 30 rectifier modules. [Hz]
5167	Mains frequency (Min of first 30 modules)	FP (2)	The calculated minimum mains frequency of the first 30 rectifier modules. [Hz]
5169	Module incoming air temperature (Max of first 30 modules)	FP (2)	The calculated maximum incoming air temperature of the first 30 rectifier modules. [°C]
5171	Module outgoing air temperature (Max of first 30 modules)	FP (2)	The calculated maximum outgoing air temperature. [°C]

Modbus Register	Name	Data Type (Length / Number of Registers)	Description [Unit of Measurement]
5173	Module temperature heat sink (Max of first 30 modules)	FP (2)	The calculated maximum heat sink temperature of the first 30 rectifier modules. [° C]
5175	Module transformer temperature (Max of first 30 modules)	FP (2)	The calculated maximum transformer temperature of the first 30 rectifier modules. [°C]
5177	Battery capacity	FP (2)	The calculated relative available battery capacity (of nominal battery capacity). This value will only show a useful value if the battery capacity test is started with the batteries fully charged. [%]
5179	Charger algebra filter – Option 1	FP (2)	Customized (programmable) alarm on request, see system settings or drawings if used.
Earth fault monitoring module measurement (ESU) - Dynamic data register 1			
5285	IMD 1 - DC Voltage — ground fault monitoring	FP (2)	The measured value of the monitored ground earth fault. Requires a connected GUMD-ADB-DCM. [V]
5287	IMD 1 - Earth resistance positive pole R+	FP (2)	The measured value of the monitored earth resistance on the positive (+) pole. Requires a connected GUMD-ADB-DCM. [kOhm]
5289	IMD 1 - Earth resistance negative pole R-	FP (2)	The measured value of the monitored earth resistance on the negative (-) pole. Requires a connected GUMD-ADB-DCM. [kOhm]
Battery supervision module measurement (BATT60) - Dynamic data register 1			
5349	BM60 1 - Measurement input L1–N	FP (2)	The measured value on L1-N from the optionally connected GUMD-ADB-BM60. Requires a connected GUMD-ADB-BM60. [V]
5351	BM60 1 - Measurement input L2–N	FP (2)	The measured value on L2-N from the optionally connected GUMD-ADB-BM60. Requires a connected GUMD-ADB-BM60. [V]
5353	BM60 1 - Measurement input L3–N	FP (2)	The measured value on L3-N from the optionally connected GUMD-ADB-BM60. Requires a connected GUMD-ADB-BM60. [V]
5355	BM60 1 - Measurement input L4–N	FP (2)	The measured value on L4-N from the optionally connected GUMD-ADB-BM60. Requires a connected GUMD-ADB-BM60. [V]
5357	BM60 1 - Measurement input L5–N	FP (2)	The measured value on L5-N from the optionally connected GUMD-ADB-BM60. Requires a connected GUMD-ADB-BM60. [V]
Battery supervision module measurement (BATT300) - Dynamic data register 1			
5413	BM300 1 – Measurement input L1–N	FP (2)	The measured value on L1-N from the optionally connected GUMD-ADB-BM300. Requires a connected GUMD-ADB-BM60. [V]
5415	BM300 1 – Measurement input L2–N	FP (2)	The measured value on L2-N from the optionally connected GUMD-ADB-BM300. Requires a connected GUMD-ADB-BM60. [V]
5417	BM300 1 - Measurement input L3–N	FP (2)	The measured value on L3-N from the optionally connected GUMD-ADB-BM300. Requires a connected GUMD-ADB-BM60. [V]

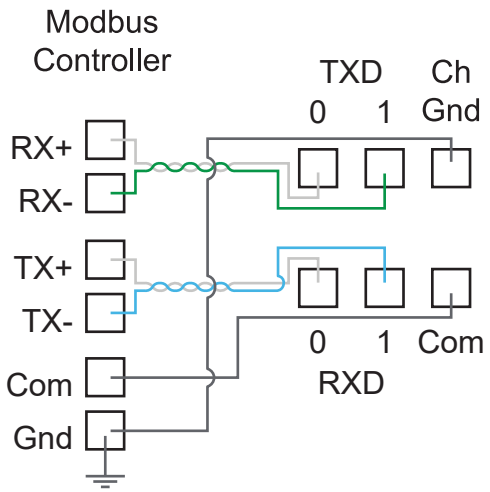
Modbus Wiring Diagrams

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

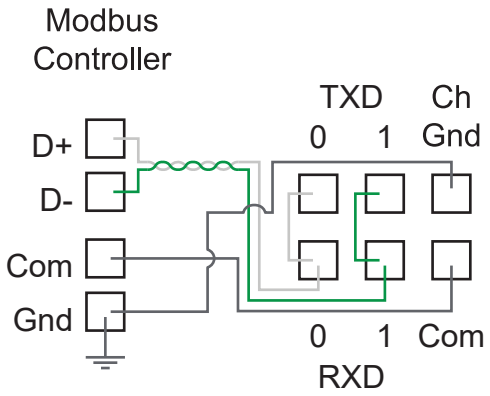
IMPORTANT: Always follow local wiring codes.

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



2-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 SNMPv3, SNMPv2c over SNMPv1 and SNMPv1.

With SNMP a Network Management System (NMS) can access the NMC by configuring a user profile (SNMPv3) or a community (SNMPv1). 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 SNMPv3 and SNMPv1 from the CLI or the web interface.

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

NOTE: Both SNMPv3 and SNMPv1 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, an IP name or a 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 `snmp ?`

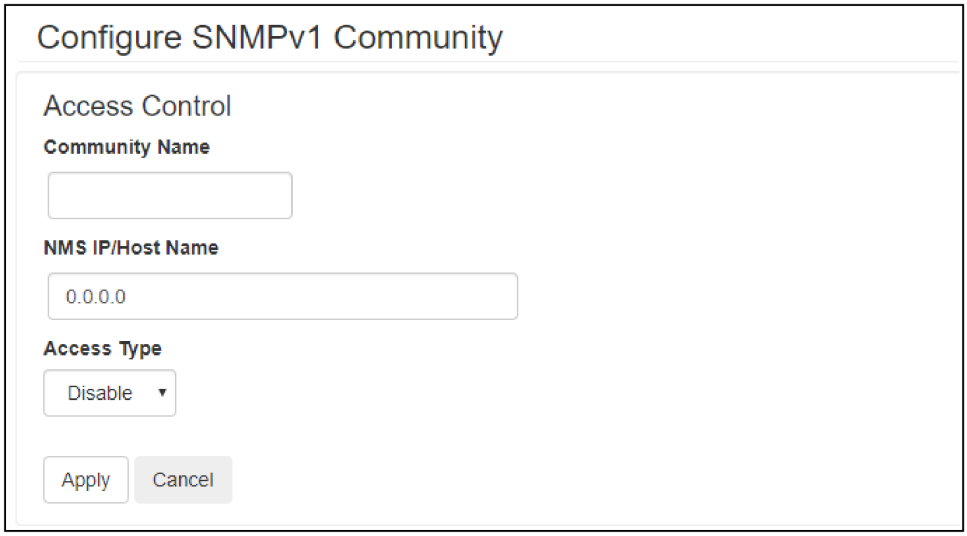
   NOTE: In the table `[n]` is the access community number 1, 2, 3 or 4.

Setting	Command	Argument	Description
Help	`?`		Shows the command help.
SNMPv1 access	`-S`	`enable | disable`	Enables or disables SNMP version 1.
Community name	`-c[n]`	`<Community 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

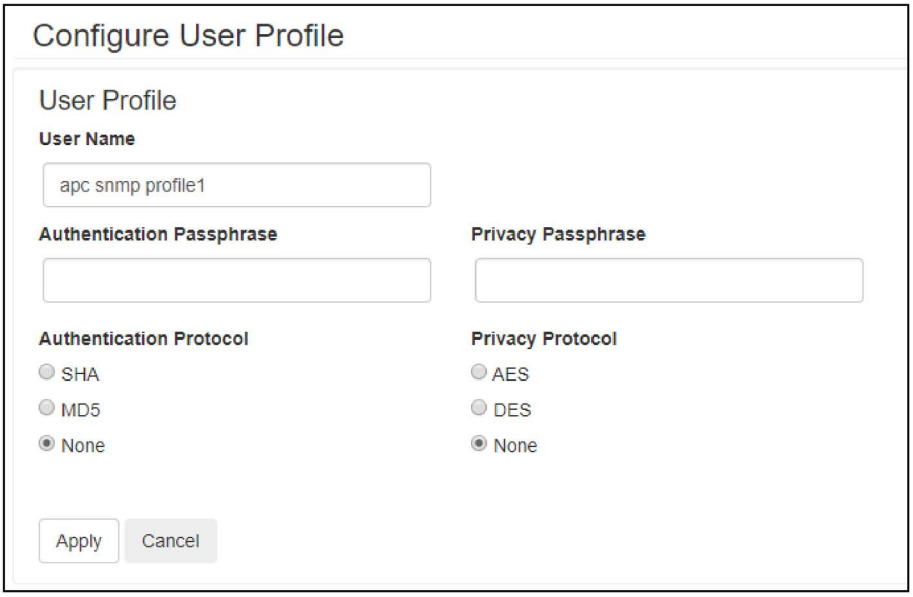
1. Log in to the CLI.
2. To see the configuration options type `snmpV3 ?`.

   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]`	`<Authentication Phrase>`	Set an authentication phrase.
Encryption phrase	`-c[n]`	`<Crypt Phrase>`	Set an encryption phrase.
Authentication protocol	`-ap[n]`	`sha | md5 | none`	Set the type of authentication protocol.
Privacy (encryption) protocol	`-pp[n]`	`eas | des | none`	Set the privacy (encryption) protocol.
Slave address	`-ac[n]`	`enable | disable`	Enable or disable access.
User access	`-au[n]`	`<User Name>`	Give access to a user.
Set IPv4/IPv6 address or host name	`-n[n]`	`<IP address> | <Host Name>`	Set the IPv4/IPv6 address or the host name of the network management station.

Configure SNMPv3 from the Web Interface

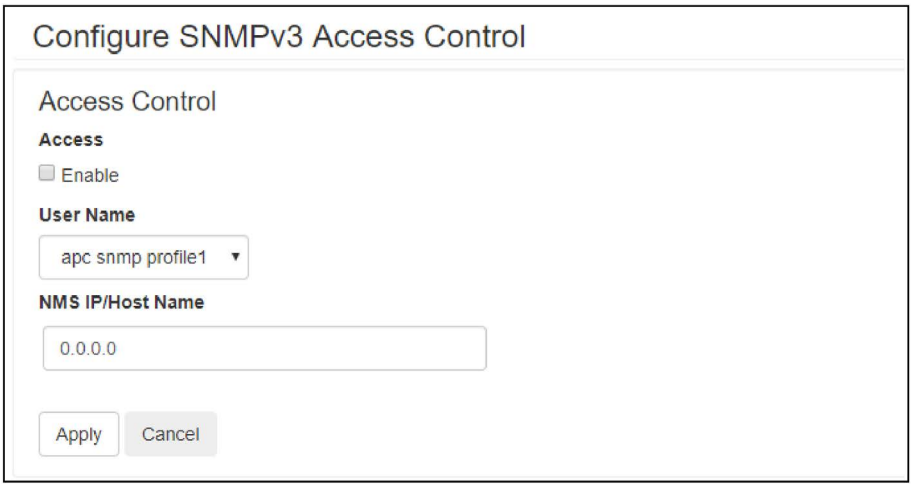
1. Log in to the web interface.
2. Navigate to **Configuration > Network > SNMPv3 > User Profile**.
3. Click on a user name to view the settings for it.
4. Here it is possible to configure the **User Name**, **Authentication Passphrase**, **Authentication Protocol**, **Privacy Passphrase** and **Privacy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

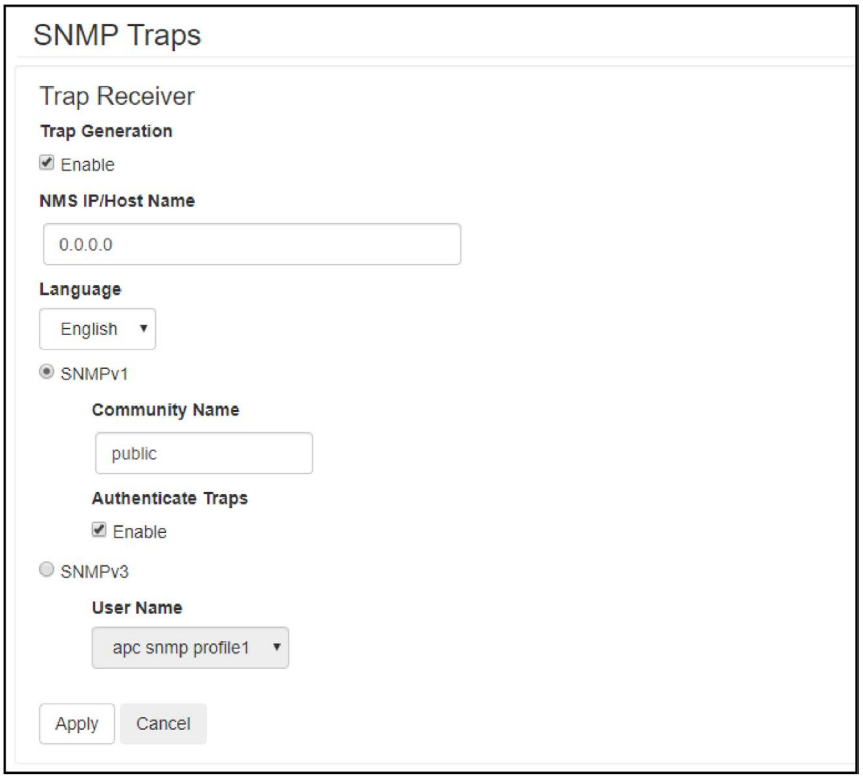
   NOTE: In the table `[n]` is the number of the trap receiver (1–6).

Setting	Command	Argument	Description
Community	`-c[n]`	`<Community Name>`	Select what SNMPv1 community name to use.
Receiver NMS IP	`-r[n]`	`<IP address>`	Set the IP address for the trap receiver.
Language	`-l[n]`	`<Language>`	Select language code.
Trap Type	`-t[n]`	`snmpV3 | snmpV1`	Select if the trap receiver should use SNMPv3 or SNMPv1.
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 SNMPv3 or SNMPv1 to use. For SNMPv3 select the user name that should be used. For SNMPv1 select the community name to use and select if the traps should use authentication.
   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. Make sure that the MIB is used so that the traps can be identified.

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	Description
communicationLost (1)	Communication to the system has been lost. Steps to reestablish communication are in progress.
upsCriticalCondition (734)	A critical condition that requires immediate action is detected. The first variable is the critical condition text message. The second variable is the critical condition number.
upsWarningCondition (736)	A warning condition that requires action is detected. The first variable is the warning condition.
upsInformationalCondition (738)	An informational condition is detected. The first variable is the informational condition.

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 it will return “No data available in this sub-tree” or “There is no such object in this MIB”.

APC / Gutor OID Address	SNMP OID Name	Description
1.1.1.1.1.1	upsBasicIdentModel	The system model name.
1.1.1.1.1.4	upsBasicIdentModelType	The detailed model information of the system used by the NMC.
1.1.1.1.2.1	upsAdvIdentFirmwareRevision	The firmware revision of the system controller (MCU).
1.1.1.1.2.2	upsAdvIdentDateOfManufacture	The date when the system was manufactured. In the format mm/dd/yy or yyyy.
1.1.1.1.2.3	upsAdvIdentSerialNumber	A unique identifying number for the system controller (MCU) set at the factory, the number is not related to any number on the system rating plate.
1.1.1.2.1.1	upsBasicBatteryStatus	Indicates the status of the battery. 1 = Unknown 2 = Normal 3 = Low capacity 4 = Fault condition 5 = Battery not present
1.1.1.2.1.3	upsBasicBatteryLastReplaceDate	The date when the battery were last replaced. In the format mm/dd/yy or mm/dd/yyyy.

APC / Gutor OID Address	SNMP OID Name	Description
1.1.1.2.2.1	upsAdvBatteryCapacity	The calculated relative available battery capacity (of nominal battery capacity). This value will only show a useful value if the battery capacity test is started with the batteries fully charged. [%]
1.1.1.2.2.2	upsAdvBatteryTemperature	The measured battery temperature by the system's battery temperature sensor. The temperature unit depends on the NMC setting. Temperatures below zero reads as 0. [°C or °F]
1.1.1.2.2.8	upsAdvBatteryActualVoltage	The battery bus voltage. [V]
1.1.1.2.2.9	upsAdvBatteryCurrent	The battery current. [A]
1.1.1.2.2.27	upsAdvBatteryBreakerStatus	Indicates the status of the battery breaker(s) in the system. 1 = All battery breakers are open 2 = At least one of the battery breakers are closed 3 = Breaker status is not present
1.1.1.2.3.2	upsHighPrecBatteryTemperature	The measured battery temperature by the system's battery temperature sensor. The temperature unit depends on the NMC setting. Value is with one decimal (tenths), temperatures below zero reads as 0. [°C / °F]
1.1.1.2.3.5	upsHighPrecBatteryCurrent	The measured battery current with one decimal (tenths). [A]
1.1.1.2.3.7.1.3.1	upsHighPrecBatteryVoltage	The measured battery bus voltage with one decimal (tenths). [V]
1.1.1.3.2.4	upsAdvInputFrequency	The measured frequency of the system input. [Hz]
1.1.1.3.2.12	upsAdvInputTotalActivePower	The total active input power (sum of all three phases) of the system. [kW]
1.1.1.3.3.4	upsHighPrecInputFrequency	The measured frequency with one decimal (tenths). [Hz]
1.1.1.4.2.8	upsAdvOutputActivePower	The total active output power (sum of all three phases) of the system. [W]
1.1.1.5.2.17	upsAdvConfigBattCabAmpHour	The configured maximum ampere hours of the battery bank. The value shows the maximum battery capacity configured for the system regardless of the breaker positions. [Ah]
1.1.1.7.2.13	upsAdvTestBatteryLastDate	The date of the latest performed battery diagnostic test. In the format YYYY-MM-DD.
1.1.1.7.2.14	upsAdvTestBatteryProcessStatus	The result of the latest performed battery discharge test. 1 = Successful 2 = Precondition not meet 3 = In progress 4 = Refused 5 = Manually/Automatically cancelled 6 = Pending 7 = Unknown 8 = No battery present
1.1.1.7.2.15	upsAdvTestBatteryConditionStatus	The result of the latest successful battery discharge test. 1 = Unknown 2 = Battery OK 3 = Battery capacity lower 4 = Battery defect
1.1.1.8.1.0	upsCommStatus	The status of the communication from the SNMP agent to the system.
1.1.1.11.2.16	upsAdvStateGutorModularSpecificFaults	An ASCII string containing the 64 flags representing the active specific alarms for Gutor Modular. For more information about the flags see the chapter SNMP Flags, page 52.
1.1.1.13.4.26.1.2	upsDiagSubSysNetworkComCardModel-Number	The model number of the NMC.
1.1.1.13.4.26.1.3	upsDiagSubSysNetworkComCardSerial-Number	The serial number of the NMC.
1.1.1.13.4.26.1.4	upsDiagSubSysNetworkComCardDateOf-Manufacture	The manufacturing date for the NMC.

APC / Gutor OID Address	SNMP OID Name	Description
1.1.1.13.4.26.1.5	upsDiagSubSysNetworkComCardHardwareRev	The hardware revision of the NMC.
1.1.1.13.4.26.1.6	upsDiagSubSysNetworkComCardFirmwareAppRev	The firmware revision of the Gutor application for the NMC.
1.1.1.17.1.2.1.2	upsDCOutputStatusVoltageNominal	The set nominal DC output voltage of the system with one decimal (tenths). [V]
1.1.1.17.1.2.1.3	upsDCOutputStatusCurrentRating	The set output current rating of the system with one decimal (tenths). [A]
1.1.1.17.1.2.1.4	upsDCOutputStatusVoltage	The measured DC output voltage of the system with one decimal (tenths). [V]
1.1.1.17.1.2.1.5	upsDCOutputStatusCurrent	The measured output current of the system with one decimal (tenths). [A]
1.1.25.1.2.1.1	uioSensorStatusPortID	The assigned ID of the port on the NMC where the temperature (or temperature and humidity) sensor is attached.
1.1.25.1.2.1.2	uioSensorStatusSensorID	The assigned ID of the temperature (or temperature and humidity) sensor connected to the NMC.
1.1.25.1.2.1.3	uioSensorStatusSensorName	The entered name of the temperature (or temperature and humidity) sensor connected to the NMC. Can be changed from the NMC interface.
1.1.25.1.2.1.4	uioSensorStatusSensorLocation	The entered location of the temperature (or temperature and humidity) sensor connected to the NMC. Can be changed from the NMC interface.
1.1.25.1.2.1.5	uioSensorStatusTemperatureDegF	The measured temperature by the temperature (or temperature and humidity) sensor in Fahrenheit. [°F]
1.1.25.1.2.1.6	uioSensorStatusTemperatureDegC	The measured temperature by the temperature (or temperature and humidity) sensor in Celsius. [°C]
1.1.25.1.2.1.7	uioSensorStatusHumidity	The measured relative humidity by the temperature and humidity sensor in percent. [%]
1.1.25.1.2.1.8	uioSensorStatusViolationStatus	Indicates the reason for why an alarm is active for the sensor. Should be read as a bit map, where each bit represents if the alarm condition is active = 1 or inactive = 0. Bit 1 = Maximum temperature exceeded Bit 2 = High temperature exceeded Bit 3 = Low temperature exceeded Bit 4 = Minimum temperature exceeded Bit 5 – Bit 8 = (Not used) Bit 9 = Maximum humidity exceeded Bit 10 = High humidity exceeded Bit 11 = Low humidity exceeded Bit 12 = Minimum humidity exceeded.
1.1.25.1.2.1.9	uioSensorStatusAlarmStatus	The alarm status of the temperature (or temperature and humidity) sensor connected to the NMC. 1 = Normal 2 = Warning 3 = Critical 4 = N/A
1.1.25.1.2.1.10	uioSensorStatusCommStatus	The status of the communication between the NMC and the connected temperature or temperature and humidity sensor. 1 = Not installed 2 = Communication OK 3 = Communication lost
1.1.29.1.1	chargerIdentModel	The model of the connected UPS or system.
1.1.29.1.3	chargerIdentSerialNumber	The serial number of the connected UPS or system.
1.1.29.1.4	chargerIdentModelType	The type of the connected UPS or system.
1.1.29.2.1.1.1.1	chargerInputPhaseTableIndex	Index for the first phase (L1) for the rectifier input.

APC / Gutor OID Address	SNMP OID Name	Description
1.1.29.2.1.1.1.2	chargerInputPhaseTableIndex	Index for the first phase (L2) for the rectifier input.
1.1.29.2.1.1.1.3	chargerInputPhaseTableIndex	Index for the first phase (L3) for the rectifier input.
1.1.29.2.1.1.2.1	chargerInputPhaseVoltage	The measured AC voltage on L1-N from the optionally connected GUMD-ADB-ACM to rectifier system 1. Requires a connected GUMD-ADB-ACM. [V]
1.1.29.2.1.1.2.2	chargerInputPhaseVoltage	The measured AC voltage on L2-N from the optionally connected GUMD-ADB-ACM to rectifier system 1. Requires a connected GUMD-ADB-ACM. [V]
1.1.29.2.1.1.2.3	chargerInputPhaseVoltage	The measured AC voltage on L3-N from the optionally connected GUMD-ADB-ACM to rectifier system 1. Requires a connected GUMD-ADB-ACM. [V]
1.1.29.3.1	chargerOutputStatus	The current state or operation mode of the system. 1 = Unknown 2 = Initializing 3 = Standby 4 = Battery operation 5 = Float charge 6 = Boost charge 7 = Equalizing (initial) charge 8 = Direct feed
1.1.29.3.3	chargerOutputTotalCurrent	The total DC output current of the rectifier modules in the system. [A]
1.1.29.3.4	chargerOutputLoad	The relative output power of the system. [%]

SNMP Flags

There are 64 flags representing active specific alarms for Gutor Modular. The ASCII string is read from left to right.

NOTE: Flags that are not listed are reserved. If the NMC can't get the value for a flag from the system it is set to "UNKNOWN". If the connected system does not use a specific flag it is set to "NOT SUPPORTED".

Breaker Flags (1–16)

Flag Number	Flag Name	Flag Description
Flag 1	Rectifier AC mains breaker 1	The rectifier AC mains input breaker is open.
Flag 2	Battery breaker 1	The internal battery breaker and/or the external battery breaker is open.
Flag 3	Rectifier DC output breaker	The rectifier DC output breaker is open.
Flag 4	DC distribution feeder	One or more distribution output feeders has tripped.
Flag 6	Surge protection device	The AC input surge arrester has tripped.

Module Flags (17–32)

Flag Number	Flag Name	Flag Description
Flag 18	Load sharing error in all power modules	The active load sharing between all the rectifier modules is not functioning correctly.
Flag 19	Fan fault in all power modules	The fans in all rectifier modules are inoperable.
Flag 20	Output voltage out of range in all power modules	The rectifier mains input is out of tolerance for all rectifier modules.
Flag 21	Input voltage out of range in all power modules	Input voltage out of range in all rectifier modules.
Flag 23	Number of rectifier modules is below warning limit	Only for redundant N+x and N+N module configurations. The number of redundant rectifier modules is currently below the warning limit because of some inoperable rectifier modules. (Calculated based on number of modules).
Flag 24	Number of rectifier modules is below critical limit	Only for redundant N+x and N+N module configurations. The number of redundant rectifier modules are currently below the critical limit because of some inoperable rectifier modules. (Calculated based on number of modules).
Flag 25	Power module current reserve is lost	Only for redundant N+x and N+N module configurations. The output current redundancy is currently not available because of some inoperable rectifier modules. (Calculated based on output current).

Charger Flags (33–44)

Flag Number	Flag Name	Flag Description
Flag 33	Common alarm	One or more alarms that are configured for the common alarm are present. The common alarm is mainly intended to be used for external signals.
Flag 34	Urgent event	One or more urgent alarms that require immediate actions are present.
Flag 35	Non urgent alarm	One or more non urgent alarms that require actions are present.
Flag 36	HMI to MCU communication fault	The communication between the display and the controller is interrupted or lost.
Flag 37	Battery equalizing charging is blocked	Switch to equalizing charge mode is blocked. The mode can be blocked by an external/internal signal.
Flag 38	Boost charge is blocked	Switch to boost charge mode is blocked. The mode can be blocked by an external/internal signal.
Flag 39	High DC warning alarm	The system output voltage is above the set high warning voltage level.
Flag 40	High DC shutdown alarm	The system output voltage is above the set high shutdown voltage level.
Flag 41	Low DC warning alarm	The system output voltage is below the set low warning voltage level.
Flag 42	Low DC shutdown alarm	The system output voltage is below the set low shutdown voltage level.

Charger Flags (45–54)

Flag Number	Flag Name	Flag Description
Flag 45	Battery symmetry error	The battery symmetry is out of tolerance.
Flag 46	Battery current-limiting is active	The battery charging current has reached its maximum limit. The rectifier will regulate the DC output current to not overcharge the batteries with a too high charging current.
Flag 48	Battery temperature measurement invalid	The battery temperature sensor is returning an invalid value (NaN or <-90°C). The sensor might not be configured correctly or is not operating correctly.

Charger Flags (55–64)

Flag Number	Flag Name	Flag Description
Flag 55	MCU temperature is too high	The MCU (controller) temperature is above the set high temperature level.

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.
Cannot access the NMC from EcoStruxture or another asset software	• Make sure that EcoStruxture (or asset software) is correctly configured for the NMC. • Check that the **About > Charger** page displays the correct information for the system.

Troubleshooting for NMC SNMP

Problem	Solution
Unable to perform a GET	• Check the user profile configuration (SNMPv3) or the read (GET) community name (SNMPv1). • Use the CLI or the web interface to make sure that the NMS has access.
Unable to perform a SET	• Check the user profile configuration (SNMPv3) or the read/write (SET) community name (SNMPv1). • Use the command line interface or UI to ensure that the NMS is granted access to the target IP address through the access control list (SNMPv3) or has write (SET) access (SNMPv1).
Unable to receive traps at the NMS	• Make sure the trap type (SNMPv3 or SNMPv1) is correctly configured for the NMS as a trap receiver. • For SNMPv3, check the user profile configuration for the NMS, and run a trap test. • 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.
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.

© 2022 – 2023 Schneider Electric. All rights reserved.

0000649741_01_en