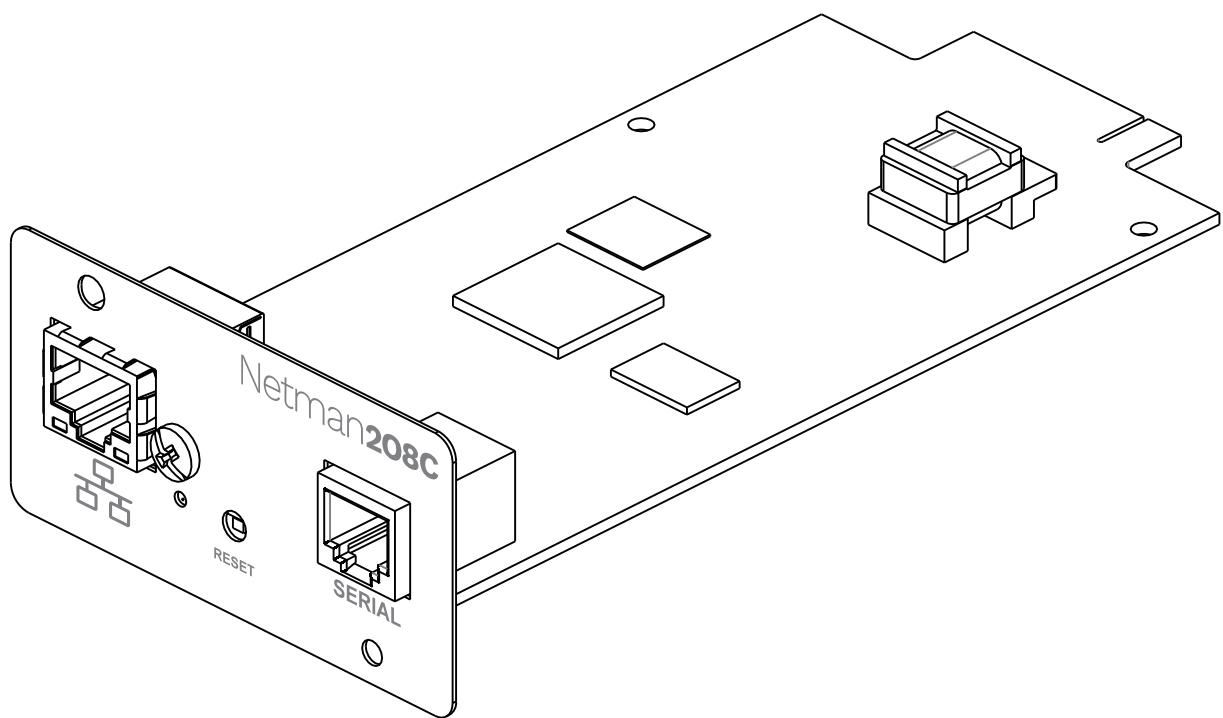


NetMan 208C



Installation and user manual

INTRODUCTION

Thank you for choosing our product.

The accessories described in this manual are of the highest quality, carefully designed and built in order to ensure excellent performance.

This manual contains detailed instructions on how to install and use the product.

This manual must be stored in a safe place and CONSULTED BEFORE USING THE DEVICE for proper usage instructions as well as maximum performance from the device itself.

NOTE: Some images contained in this document are for informational purposes only and may not faithfully demonstrate the parts of the product they represent.

Symbols used in this manual:



Warning

Indicates important information that must not be ignored.



Information

Provides notes and useful suggestions for the User.

SAFETY

This part of the manual contains SAFETY precautions that must be followed scrupulously.

- ❖ The device has been designed for professional use and is therefore not suitable for use in the home.
- ❖ The device has been designed to operate only in closed environments. It should be installed in rooms where there are no inflammable liquids, gas or other harmful substances.
- ❖ Ensure that no water or liquids and/or foreign bodies fall into the device.
- ❖ In the event of a fault and/or impaired operation of the device, do not attempt to repair it but contact the authorized service centre.
- ❖ The device must be used exclusively for the purpose for which it was designed. Any other use is to be considered improper and as such dangerous. The manufacturer declines all responsibility for damage caused by improper, wrong and unreasonable use.

ENVIRONMENTAL PROTECTION

Our company devotes abundant resources to analysing environmental aspects in the development of its products. All our products pursue the objectives defined in the environmental management system developed by the company in compliance with applicable standards.

Hazardous materials such as CFCs, HCFCs or asbestos have not been used in this product.

When evaluating packaging, the choice of material has been made favouring recyclable materials. Please separate the different material of which the packaging is made and dispose of all material in compliance with applicable standards in the country in which the product is used.

DISPOSING OF THE PRODUCT

The device contains internal material which (in case of dismantling/disposal) are considered TOXIC, such as electronic circuit boards. Treat these materials according to the laws in force, contacting qualified centres. Proper disposal contributes to respect for the environment and human health.

- © The reproduction of any part of this manual, even in part, is prohibited unless authorized by the manufacturer.
- The manufacturer reserves the right to change the product described at any time without prior notice for improvement purposes.

CONTENTS

| | |
|---|-----------|
| OVERVIEW | 9 |
| PACKAGE CONTENTS | 9 |
| FRONT PANEL | 10 |
| Reset button | 10 |
| Serial port | 11 |
| Status LED | 11 |
| NETWORK SERVICES | 12 |
| SSH | 12 |
| Serial network | 12 |
| Wake-on-LAN | 12 |
| HTTP / HTTPS | 12 |
| SNMP | 12 |
| UDP | 12 |
| Modbus TCP/IP | 12 |
| BACnet/IP | 13 |
| Syslog | 13 |
| Email | 13 |
| Reports | 13 |
| SSH Client | 13 |
| DEVICE VALUES AND EVENTS HISTORY LOG ARCHIVE | 14 |
| Eventlog | 14 |
| Datalog (only for UPS devices) | 14 |
| INSTALLATION | 15 |
| FIRST LOGIN | 16 |
| USERS | 18 |
| LOCAL Users | 18 |
| LDAP/AD Users | 18 |
| FALLBACK ADDRESS 169.254.1.208 | 19 |
| DEFAULT CONFIGURATION | 20 |
| MAIN PORTS AND SERVICES | 21 |
| GENERAL DESCRIPTION | 22 |
| DASHBOARD | 22 |
| DATA | 23 |
| SYSTEM OVERVIEW | 24 |
| HISTORY | 25 |

| | |
|------------------------------|-----------|
| Event Log | 25 |
| Data Log | 26 |
| CONFIGURATION | 27 |
| DEVICE | 27 |
| General configuration | 27 |
| Command configuration | 29 |
| Data log configuration | 30 |
| NETWORK | 31 |
| Configuration | 31 |
| IEEE 802.1x | 34 |
| Connectivity | 42 |
| Firewall | 45 |
| Wake-on-LAN | 50 |
| SNMP | 51 |
| MODBUS/BACNET | 56 |
| JSON | 57 |
| Syslog | 62 |
| DATE & TIME | 63 |
| NTP & Timezone | 63 |
| Configuration | 64 |
| EMAILS | 65 |
| Configuration | 65 |
| ADVANCED | 69 |
| Expert Shell | 69 |
| SENSORS | 71 |
| GSM MODEM | 72 |
| Configuration | 72 |
| REMOTE HOSTS | 74 |
| SSH | 74 |
| VMware ESXi | 79 |
| Nutanix | 85 |
| Syneto | 90 |
| ADMINISTRATION | 99 |
| Automatic Check for Updates | 99 |
| Firmware upgrade | 100 |
| Certificates | 101 |
| Backup/Restore Configuration | 104 |
| Reset to defaults | 111 |
| Reset Log | 111 |

| | |
|---|-----|
| Reboot | 111 |
| Change local password | 112 |
| Login access | 118 |
| Login rules | 137 |
| Web Login banner | 141 |
| DEVICE COMMANDS | 145 |
| Test battery | 145 |
| Shutdown | 145 |
| Shutdown / Restore | 146 |
| DIAGNOSTIC | 147 |
| Test COMM LOST | 148 |
| Test AUDIT FAILURE | 149 |
| Web Requests | 150 |
| PASSWORD RESET | 151 |
| CONFIGURATION VIA SSH | 154 |
| Main menu | 155 |
| Setup | 156 |
| IP config | 157 |
| Expert mode | 158 |
| UPLOAD / MAINTENANCE MODE | 159 |
| PROCEDURES | 168 |
| RESET BUTTON | 168 |
| CONFIGURATION OF SEVERAL DEVICES | 170 |
| MONITORING RESOURCES | 171 |
| INTERNAL LOGS | 172 |
| SERVICE LOG | 173 |
| SNMP CONFIGURATION | 174 |
| MODBUS TCP/IP PROTOCOL | 182 |
| BACNET/IP CONFIGURATION | 183 |
| EVENTLOG CODES | 185 |
| TECHNICAL DATA | 187 |
| SERIAL PORT PINOUT | 187 |
| NETWORK CABLE | 188 |
| OPERATING AND STORAGE CONDITIONS | 189 |

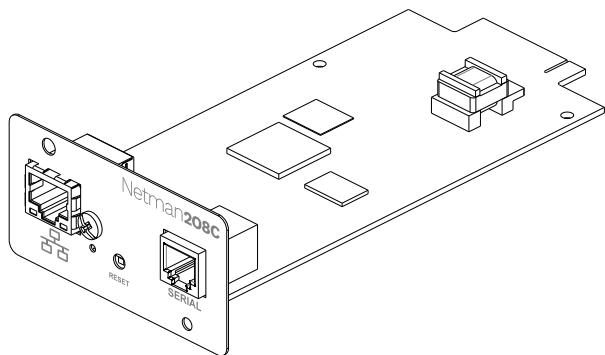
OVERVIEW

NetMan 208C is an accessory that allows the management of the UPS through a LAN (Local Area Network); the accessory supports all the main network protocols (SNMP v1, v2 and v3, TCP/IP, HTTP, HTTPS and MODBUS) and is compatible with Ethernet 10/100/1000 Mbps IPv4/6 networks. The device can therefore be integrated easily into medium and large-sized networks.

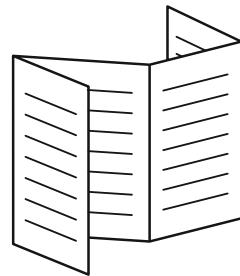
NetMan 208C also records device values and events in the history log archive and can manage optional environmental sensors (not supplied with the device but provided separately).

PACKAGE CONTENTS

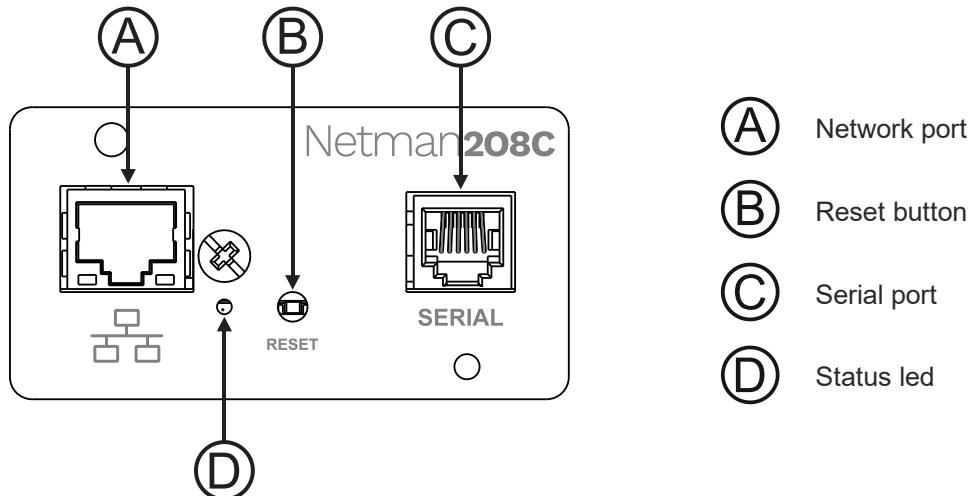
NetMan 208C



Quick start



FRONT PANEL



Network port

The LEDs built into the RJ45 connector describe the status of the network.

| Left LED (green) | Right LED (yellow) | Link / Activity |
|------------------|--------------------|-------------------------------|
| OFF | OFF | Link Off |
| ON | OFF | 1000 Link / No Activity |
| Blinking | OFF | 1000 Link / Activity (RX, TX) |
| OFF | ON | 100 Link / No Activity |
| OFF | Blinking | 100 Link / Activity (RX, TX) |
| ON | ON | 10 Link / No Activity |
| Blinking | Blinking | 10 Link / Activity (RX, TX) |

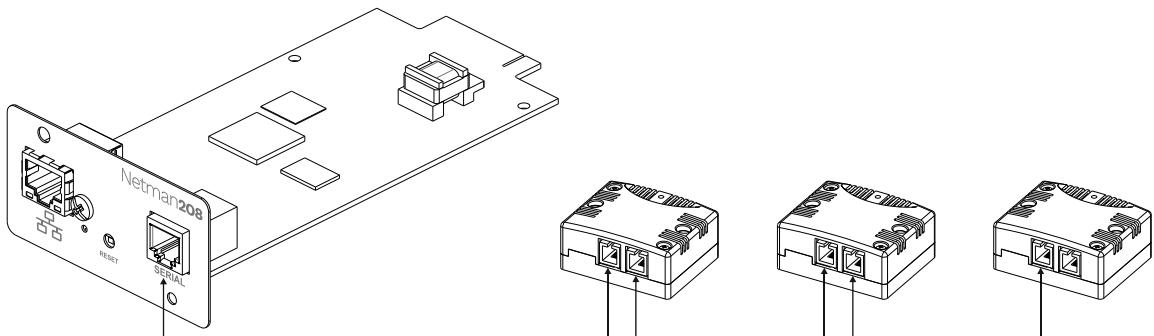
Reset button

The reset button enables the user to enter the Maintenance Mode. To boot into Maintenance Mode:

- If NetMan 208C is already powered and working, keep the reset button pressed for approximately 12 seconds; first the status LED starts blinking, then turns off. When the status LED turns off, release the reset button and wait for about 2 minutes. When the status LED blinks green, NetMan 208C is in Maintenance Mode with HTTP connection active (not HTTPS).
- Upon power on and/or within three seconds of inserting the NetMan 208C into the slot, keep the reset button pressed for approximately 12 seconds; first the status LED starts blinking, then turns off. When the status LED turns off, release the reset button and wait for about 2 minutes. When the status LED blinks green, NetMan 208C is in Maintenance Mode with HTTP connection active (not HTTPS).

Serial port

To connect up to three optional environmental sensors to NetMan 208C.



Status LED

This led describes the status of NetMan 208C:

| LED color | Description |
|---------------------|--|
| SOLID GREEN | <ul style="list-style-type: none">Normal operation |
| FAST BLINKING GREEN | <ul style="list-style-type: none">Reset button pressedUpdate mode running |
| SLOW BLINKING GREEN | <ul style="list-style-type: none">Recovery mode running |
| SOLID RED | <ul style="list-style-type: none">UPS communication errorWrong PRTK code configured |

NETWORK SERVICES

NetMan 208C implements a series of services based on the main network protocols. These services can be activated or deactivated according to requirements (see paragraph “Configuration”). A brief description for each of these is given below.

SSH

By means of a SSH client (available on all the main operating systems) a remote connection with NetMan 208C can be established to change its configuration (see paragraph “Configuration via SSH”).

Serial network

To emulate a point-to-point serial connection through the network (TCP/IP protocol) in order to use special function service software.

Wake-on-LAN

NetMan 208C can send the “Wake-on-LAN” command to boot remote computers.

HTTP / HTTPS

Using the HTTPS (Hyper Text Transfer Protocol Secure), it is possible to configure NetMan 208C and the status of the device can be monitored by means of a web browser without having to install additional software. All the most popular web browsers are supported; only most recent versions of browsers are supported.

HTTP is only used in Maintenance Mode, when no other access to NetMan 208C is possible and it is intended for emergency (it requires physical intervention by the operator on NetMan 208C itself, by pressing the reset button).

SNMP

SNMP (Simple Network Management Protocol) is a communication protocol that allows a client (manager) to make requests to a server (agent). NetMan 208C is an SNMP agent.

To exchange information, manager and agent use an addressing technique called MIB (Management Information Base). There is a MIB file for each agent, defining which variables can be requested and the respective access rights. The agent can also send messages (TRAP) without a prior request from the manager, to inform the latter of particularly important events. SNMPv3 is the evolution of SNMP and introduces important features related to security.

UDP

UDP (User Datagram Protocol) is a low-level network protocol that guarantees speed in the exchange of data and low network congestion. It is the protocol used by the UPSMon software for monitoring and control of the device.

The UDP connection uses the UDP 33000 port by default but can be configured on other ports according to requirements.

Modbus TCP/IP

The device status can be monitored by means of the standard network protocol MODBUS TCP/IP. Modbus TCP/IP is simply the Modbus RTU protocol with a TCP interface that runs on Ethernet.

BACnet/IP

The device status can be monitored by means of the standard network protocol BACnet/IP. BACnet (Building Automation and Control networks) is a data communication protocol mainly used in the building automation and HVAC industry (Heating Ventilation and Air-Conditioning).

Syslog

NetMan 208C can send events to a syslog server over UDP. This service allows the user to centralize the log of the IT infrastructure on a single server, in order consume them in the preferred way.

Email

NetMan 208C can send a notification e-mail if one or more alarm conditions occur. The e-mails can be sent to up to three recipients and for different kinds of alarms and notifications using SMTP protocol (Simple Mail Transfer Protocol). The port is configurable. For more details, see paragraph “Configuration”

Reports

NetMan 208C can send periodic e-mails with an attachment containing the files of the device values and events history log archive.

This service can be used to periodically save the history log archives.

The “Email” service must be enabled in order to send reports; the reports are sent to all the addresses configured for this service (for more details see paragraph “Configuration”).

SSH Client

When not feasible to operate on equipment by other means, it is possible to execute a script on a remote host over SSH. For more details, see paragraph “Configuration”.

DEVICE VALUES AND EVENTS HISTORY LOG ARCHIVE

NetMan 208C records the device values (Datalog) and events (Eventlog) in a history log database.

Eventlog

The Eventlog service is always active and records all relevant device events in the ‘event.db’ file. With the “Email report” service, is sent a .csv file with the event of the last day or week according to your setting. The data are saved in circular list mode; thus, the most recent data are saved by overwriting the oldest data.

On the web page, these icons will be shown on the “type” column:

- A red dot if the event is the start of an alarm condition.
- A green dot if the event is the end of an alarm condition.
- A blue dot otherwise.

Datalog (only for UPS devices)

The Datalog service records the main data of the UPS in the ‘datalog.db’ file.

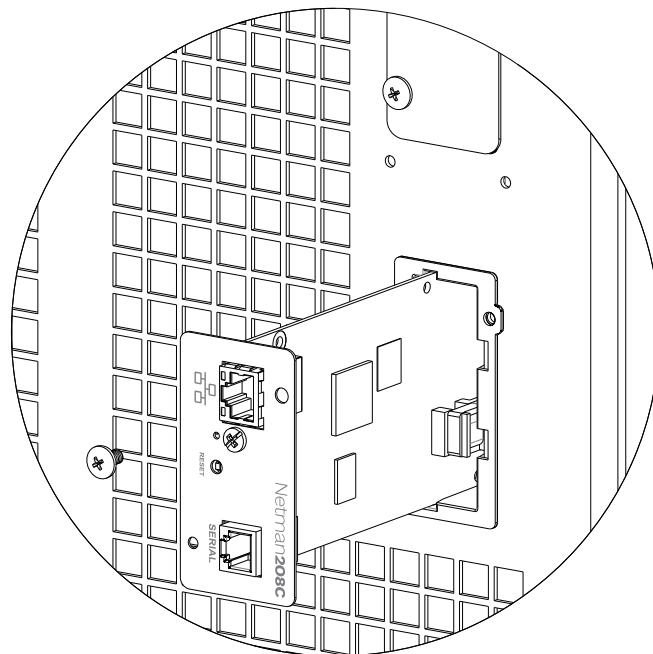
This service writes a record each hour at 00 minutes, which summarizes the data of the past hour: values are recorded at their minimum, maximum and average. Records older than one year are overwritten with new records.

The file can be viewed via the web page after login authentication (only the most important values are shown on the web page).

With the “Email report” service, the last records (last day or last 7 days according to your settings) will be sent in a .csv format.

INSTALLATION

1. Remove the cover of the COMMUNICATION SLOT by unscrewing the two retaining screws. Save the screws for later.
2. Carefully insert NetMan 208C into the COMMUNICATION SLOT.
3. Secure NetMan 208C in the COMMUNICATION SLOT using the two previously removed screws.
4. Connect to the network by means of an RJ45 connection cable.



FIRST LOGIN



By default, NetMan 208C has DHCP enabled.



NetMan 208C requires approximately 4 minutes to become fully operational from when it is powered up or following a reboot; before this time the device may not respond to commands that are sent to it.

To configure the NetMan 208C, enter the IP address or the hostname into your web browser and then log in with the following username and default password:

Username: **admin**

Password: **admin**

At the first boot or if you don't know the IP address, you can use the Zero Configuration Networking (Zeroconf) as described below.

On the bottom side of the card, you can find the label reporting the mac address.



00:02:63:XX:YY:ZZ

Take note of the last six characters of the mac address.

| | | | | | |
|----|----|----|----|----|----|
| 00 | 02 | 63 | XX | YY | ZZ |
| | 63 | | | | |

In the address bar of a web browser, enter:

https://netman63XXYYZZ.local

replacing **XXYYZZ** with the last six characters of the mac address.

For example, if the mac address is **00:02:63:a1:b2:c3**, you must enter

https://netman63a1b2c3.local

in the address bar of the web browser.

Then log in with the following username and default password:

Username: **admin**

Password: **admin**

LOGIN WITH LOCAL AUTHENTICATION

Username

Password 

LOGIN



For security reasons, at the first login the user must change the default password "admin" with a secure password.

ADMIN FIRST LOGIN

admin is using the default password.
A new password is required, different from the default password.

Current **admin** password 

NEW ADMIN PASSWORD RULES

Password length: **8-40 chars**
Min Lowercase chars requested (a,b,c,...,z): 1
Min Uppercase chars requested (A,B,C,...,Z): 1
Min digit chars requested (0-9): 1
Min special chars requested (.,_+:@%~-): 1

Type the new password 

Type again the new password 

BACK TO LOGIN **SET THE NEW PASSWORD**

The password can contain alphanumeric characters and only the following special characters:



* ! ? # \$ @ % & = < > () [] : . , ^ | _ - + (space)

No other characters are allowed.

The accepted username length ranges from 1 to 253 characters.



The password change is mandatory and must follow the complexity rules requested. Later, in the Configuration of accesses, it is possible to customize the password complexity rules for the local users ("admin", "power", "view").



After a reset to default, the default password "admin" is restored.

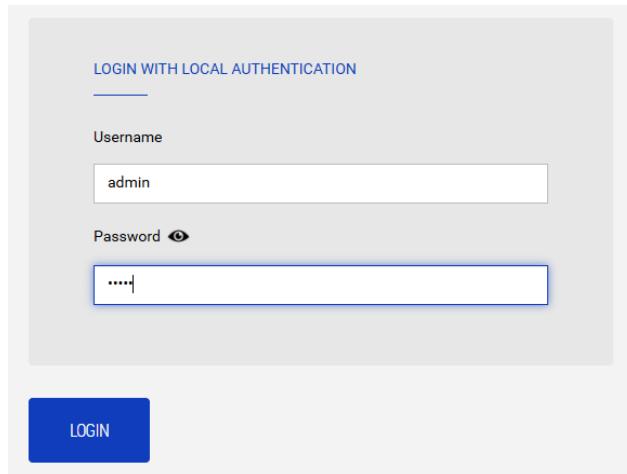
USERS

It is possible to access to NetMan 208C with three different users: “admin”, “power” and “view”. All the settings are available on the web configuration when logged in as “admin” or “power” user. It is not possible to have multiple concurrent sessions.

LOCAL Users

It is possible to login with local authentication (managed by NetMan 208C):

- “admin” user will be able to change the configuration and fully operate on the device.
- “power” user will be able to change some part of the configuration and limited operations on the device; the roles of the “power” user are configurable.
- “view” user will be able to monitor some states and perform very limited actions; the roles of the “view” user are configurable.



LOGIN WITH LOCAL AUTHENTICATION

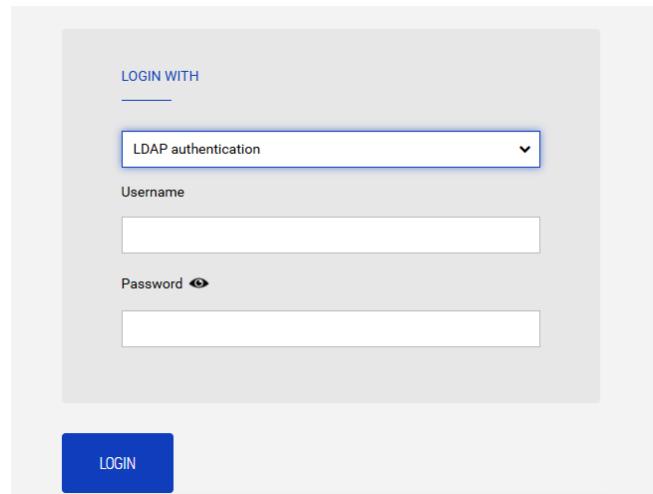
Username

Password 

LOGIN

LDAP/AD Users

It is possible to login with LDAP or AD (Active Directory). More information in paragraph “Login access configuration”.



LOGIN WITH

LDAP authentication

Username

Password 

LOGIN

FALLBACK ADDRESS 169.254.1.208

When NetMan 208C, during the boot sequence, requires address from DHCP Server and no DHCP is available in the connected network, the FALBACK ADDRESS 169.254.1.208 is auto set without gateway and without DNS:

| | | |
|--------------------|-------|----------------------|
| NetMan 208C | IP: | 169.254.1.208 |
| | Mask: | 255.255.0.0 |
| | Gw: | - |
| | DNS: | - |
| | DNS: | - |

The PC must be configured with:

| | | | |
|-----------|-------|------------------------------|--------------------------|
| PC | IP: | 169.254.1.<xyz> | <xyz> not equal to “208” |
| | Mask: | 255.255.0.0 | |
| | Gw: | - | |
| | DNS: | - | |
| | DNS: | - | |

In the address bar of a web browser type:

- <http://169.254.1.208>
- <https://169.254.1.208>



DEFAULT CONFIGURATION

| | |
|--------------------------|--|
| IP address | <p>IPv4:</p> <ul style="list-style-type: none"> - DHCP (if DHCP Server available). - 169.254.1.208/16 (auto-assigned after about 5 minutes if not available during the booting of the NetMan 208C). <p>IPv6:</p> <ul style="list-style-type: none"> - enabled, stateless. |
| Configuration interface | Web connection only. |
| Web connection details | HTTPS, signed certificate from external CA. |
| Date/time (NTP) | Date/time from common default external servers (Linux default NTP pool addresses). |
| First access | Web access only, login as “ admin ” and password “admin”, mandatory password change upon first login. |
| User roles | <p>Only local “admin” user accesses to all the functionalities and configuration.</p> <p>Users ‘power’ and ‘view’ are not enabled: must be activated later with a password, proposing the only minimal roles active</p> <p>LDAP users: disabled by default.</p> |
| Password strength | Set to common security level with uppercase, lowercase, numbers and punctuations. |
| Auto-logout sessions | <p>Web session:</p> <p>enabled by default,</p> <p>delay 1 hour,</p> <p>last warning 1 minute.</p> |
| Functionalities disabled | <p>SNMP, REMOTE COMMANDS, REMOTE HOSTS, SSH, SYSLOG, JSON, MODBUS, BACNET, EMAIL, FIREWALL, REMOTE HOSTS, SENSORS, LDAP, 802.1x, UDP/PowerShield, SERIAL NETWORK TUNNELING, WAKE ON LAN.</p> <p>(can be enabled later from the “admin” user with the related security requirements)</p> |

MAIN PORTS AND SERVICES

Services protocols and related ports:

| | |
|--|--|
| HTTPS | TCP/ 443 (default) or customizable |
| HTTP | TCP/ 80 (default) or customizable |
| MODBUS | TCP/ 502 (default only) |
| BACNET | UDP/ 47808 (default only) + BACNET #Address customizable |
| SSH | TCP/ 22 (default only) |
| SNMP | UDP/ 161 (default only) |
| POWERSHIELD | TCP/ 55300 (default only) UDP/ 33000 (default) or port customizable |
| TUNNELING / UPSTOOLS / GPDOWNLOAD | TCP/ 34000 (default only) |

System ports:

| | |
|--------------------------------------|--|
| DHCLIENT | UDP/ 68 |
| NTPD | "ntpd" (Time Server synchronization port) UDP/ 123 |
| NETWORK Avahi mDNS (Zeroconf) | UDP/ 5353 + UDPv4/ 37682 (*) + UDPv6/ 38971 (*) (*) <i>the port can change without notice</i> |

External remote protocols and ports queried by NetMan 208C services (when enabled):

| | |
|--------------------------|---|
| JSON | Remote Server: TCP/ customizable |
| SYSLOG | Remote Server: UDP/ 514 (default) or customizable |
| LDAP | Remote Server: TCP/ 389 (LDAP – STARTTLS) TCP/ 636 (LDAPS) TCP/ customizable |
| Nutanix / SSH | Remote Server: TCP/ 22 (SSH) |
| VMware / Syneto | Remote Server: TCP/ 443 |
| Connectivity Test | PING 8.8.8.8: ICMP/* PING / HTTP (www.google.com): TCP/ 80 |

GENERAL DESCRIPTION

DASHBOARD

The dashboard is divided into several sections:

- Top Bar:** Shows the device model (CSP21K0AA300RUA), system status (LOAD ON INVERTER), a warning icon with 'Alarm NONE', and a user icon for 'Welcome ADMIN'.
- Navigation:** Includes links for DASHBOARD, DATA, SYSTEM OVERVIEW, HISTORY, CONFIGURATION, and ADMINISTRATION.
- Central View:** A network diagram showing connections between a power source (transformer), a central unit (inverter), a factory, and a battery. Below the battery is a battery level gauge at 100%.
- Autonomy:** Displays the current autonomy time as 03:47.
- Output Load:** Shows values for L1 (0), L2 (-), and L3 (-).
- Input Voltage:** Shows values for L1 (228), L2 (-), and L3 (-).
- Environmental Sensors:** Details for three sensors:
 - SENSOR 1:** Temperature 25.5°C, Humidity 46%RH. Input 1 and Output 1 are both OPEN.
 - SENSOR 2:** Temperature 25.7°C, Humidity 46%RH. Input 2 and Output 2 are both OPEN.
 - SENSOR 3:** Temperature 25.4°C, Humidity 46%RH. Input 3 and Output 3 are both OPEN.
- Last Events / Timedate:** A table of recent events:

| Code | Type | Category |
|--|-------|----------|
| 2025/12/19 11:05:00 UTC Load on Bypass | Minor | |
| 2025/12/19 11:30:37 UTC Change Configuration | Info | |
| 2025/12/19 11:31:08 UTC START APPLICATION | Info | |
| 2025/12/19 11:33:31 UTC Change Configuration | Info | |
| 2025/12/19 11:34:06 UTC START APPLICATION | Info | |

At the top you can check the general status of the device, all active alarm conditions and notifications, and the user's privilege level.

Below the navigation area there is the current dashboard with a synthetic view of the device and the main operating values.

If optional environmental sensors are installed, their values are also displayed. Finally, there is a table with the latest events (from the event log).

DATA

Real time data from device UPS is displayed.

The screenshot shows the Netman208C UPS monitoring interface with the following data:

Device model: CSP21K0AA300RUA

System status: LOAD ON INVERTER

Alarms: Alarm NONE

Temperature: 28 °C

INPUT:

| | VOLTAGE [V] | CURRENT [A] | FREQUENCY [Hz] |
|----|-------------|-------------|----------------|
| L1 | 229 | - | 49.9 |
| L2 | - | - | |
| L3 | - | - | |

BYPASS:

| | VOLTAGE [V] | CURRENT [A] | FREQUENCY [Hz] |
|----|-------------|-------------|----------------|
| L1 | 229 | 0.0 | 49.9 |
| L2 | - | - | |
| L3 | - | - | |

OUTPUT:

| | VOLTAGE [V] | LOAD [%] | CURRENT [A] | FREQUENCY [Hz] |
|----|-------------|----------|-------------|----------------|
| L1 | 231 | 0 | 0.0 | 50.0 |
| L2 | - | - | - | |
| L3 | - | - | - | |

BATTERY:

| VOLTAGE [V] | CAPACITY [%] |
|-------------|--------------|
| 40.8 | 100 |

AUTONOMY [HH:MM]: 03:47

SYSTEM OVERVIEW

Useful information about NetMan 208C and UPS are displayed.

| Field | Description |
|----------------------|--|
| Download Service Log | Allows you to download the service log file. NetMan 208C saves the internal states and logs in this file, useful for technical support for checks and inspections of problems. |
| Read Manual | Click to show the online User Manual |
| Legal Information | Show the Legal information of modules referenced from NetMan 208C. |

HISTORY

Event Log

Event Log reports events from the system.

Netman208C

Device model
CSP21K0AA300RUA

System status
LOAD ON INVERTER

Alarm
NONE

Welcome
ADMIN

DASHBOARD DATA SYSTEM OVERVIEW HISTORY CONFIGURATION ADMINISTRATION

EVENT LOG DATA LOG

FILTER EVENT-LOG

From: 19/11/2025 14:19 To: 19/12/2025 14:20

Category: Any Type: Any

LOAD LOG DOWNLOAD EVENT LOG

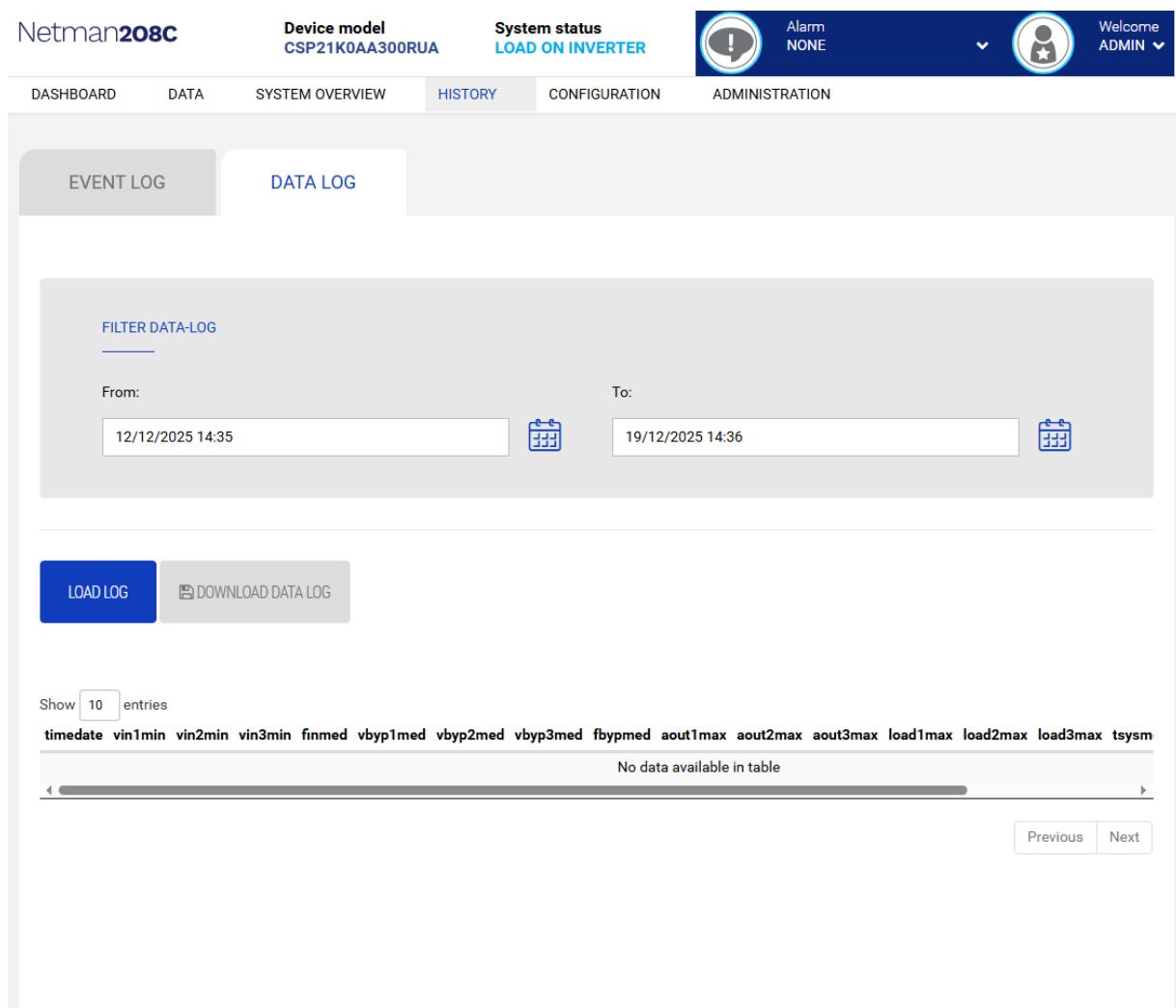
| Timedate | Code | Type | Category |
|-------------------------|----------------------|-------|----------|
| 2025/12/19 11:02:35 UTC | START APPLICATION | Info | |
| 2025/12/19 11:02:49 UTC | Output powered | Minor | |
| 2025/12/19 11:04:50 UTC | Output powered | Minor | |
| 2025/12/19 11:04:56 UTC | Load on Bypass | Minor | |
| 2025/12/19 11:05:00 UTC | Load on Bypass | Minor | |
| 2025/12/19 11:30:37 UTC | Change Configuration | Info | |
| 2025/12/19 11:31:08 UTC | START APPLICATION | Info | |
| 2025/12/19 11:33:31 UTC | Change Configuration | Info | |
| 2025/12/19 11:34:06 UTC | START APPLICATION | Info | |

Previous 1 Next

| Field | Description |
|--------------------|---|
| Filter event-log | Filters can be applied for the event search: <ul style="list-style-type: none">date from-tocategorytype |
| Load Log | Show the log in the bottom table |
| Download event log | Download the log in CSV format |

Data Log

Data Log reports data from the system.



| Field | Description |
|-------------------|---|
| Filter data-log | Filters can be applied for the event search: date from-to |
| Load Log | Show the log in the bottom table |
| Download data log | Download the log in CSV format |

Activation of Data Log

If not enable a banner is shown:

NOTICE: DATALOG IS DISABLED. TO VIEW DATA HERE PLEASE ENABLE IT IN THE ➤ CONFIGURATION MENU / DATA LOG

Follow the link or go to Configuration → Data Log configuration for enabling it.

CONFIGURATION



To make a new configuration active, it is necessary to save it. Some changes are applied immediately, while others require a reboot of the NetMan 208C.

DEVICE

General configuration

The screenshot shows the 'General configuration' section of the NetMan 208C configuration interface. The top navigation bar includes links for DASHBOARD, DATA, SYSTEM OVERVIEW, HISTORY, CONFIGURATION (which is highlighted in blue), and ADMINISTRATION. Below the navigation is a secondary navigation bar with tabs for YOUR NETMAN, SENSORS, MODEM, and REMOTE HOSTS, with 'YOUR NETMAN' currently selected. The main content area is titled 'General device configuration' and contains two main sections: 'DEVICE CONFIGURATION' and 'SYSTEM ADMIN DATA'. In the 'DEVICE CONFIGURATION' section, the 'PRTK Code' is set to 'GPSERI11201--' and the 'Name' is 'Netman 208C'. In the 'SYSTEM ADMIN DATA' section, there are fields for 'Contact' (empty), 'Location' (empty), and 'Battery replacement notification' (a date input field with a calendar icon). On the left side, a sidebar lists various configuration categories: NETWORK (Configuration, Connectivity, Firewall, Wake on LAN, SNMP, MODBUS/BACNET, JSON, SYSLOG), DATE & TIME (NTP & Timezone, Configuration), EMAILS (Configuration), and ADVANCED (Expert Shell). A large blue 'SAVE' button is located at the bottom of the configuration section.

| Field | Description | Default |
|----------------------------------|---|--------------|
| PRTK Code | Enter the PRTK code indicated at the back of the device (UPS or other). | GPSER11201-- |
| Name | Enter the identifying name of the device. (e.g. "NetMan 208C") | empty field |
| Part Number P/N | If empty, you must enter the value present in the device technical label. | empty field |
| Serial Number S/N | If empty, you must enter the value present in the device technical label. | empty field |
| Contact | Informational | empty field |
| Location | Informational | empty field |
| Battery replacement notification | The date from when NetMan 208C will starts to generate alarm notifications about the battery. | not set |

Command configuration

The screenshot shows the 'Command configuration' page within a web-based management interface. The top navigation bar includes links for DASHBOARD, DATA, SYSTEM OVERVIEW, HISTORY, CONFIGURATION (which is the active tab), and ADMINISTRATION. Below the navigation is a secondary navigation bar with tabs for YOUR NETMAN, SENSORS, MODEM, and REMOTE HOSTS, with SENSORS being the active tab. The main content area is titled 'Command configuration'. On the left, a sidebar lists various configuration sections: General configuration, Command configuration (which is selected and highlighted in blue), Data Log configuration, Configuration, Connectivity, Firewall, Wake on LAN, SNMP, MODBUS/BACNET, JSON, and SYSLOG. The 'Command configuration' section contains two settings under the 'COMMAND' heading: 'Disable remote shutdown' and 'Disable remote commands', each with a blue toggle switch that is currently set to 'on'. A large blue 'SAVE' button is located at the bottom of this section. The bottom of the sidebar also lists NTP & Timezone and Configuration.

These settings inhibit the execution of commands received from remote connectivity services: SNMP, MODBUS etc.

| Field | Description | Default |
|-------------------------|--|--|
| Disable remote shutdown | To disable the execution of shutdown commands | Enabled (i.e. shutdown command not accepted) |
| Disable remote commands | To disable the execution of the remaining commands | Enabled (i.e. remaining commands not accepted) |



By default, remote shutdown and commands are not accepted from the UPS. The user can modify the configuration so that they are accepted by the UPS, with suggestion of securing the network communication.

Data log configuration

NAVIGATION: DASHBOARD | DATA | SYSTEM OVERVIEW | HISTORY | **CONFIGURATION** | ADMINISTRATION

YOUR NETMAN | SENSORS | MODEM | REMOTE HOSTS

DEVICE

- General configuration
- Command configuration
- Data Log configuration**

NETWORK

- Configuration
- Connectivity
- Firewall
- Wake on LAN
- SNMP
- MODBUS/BACNET
- JSON
- SYSLOG

DATE & TIME

- NTP & Timezone
- Configuration

EMAILS

- Configuration

ADVANCED

- Expert Shell

Data Log configuration

DATA LOG

Enable Data Log

SAVE

| Field | Description | Default |
|-----------------|--|----------|
| Enable Data log | To enable the datalog service shown in HISTORY -> Data Log | Disabled |

NETWORK

Configuration

DASHBOARD DATA SYSTEM OVERVIEW HISTORY **CONFIGURATION** ADMINISTRATION

YOUR NETMAN SENSORS MODEM REMOTE HOSTS

DEVICE

General configuration
Command configuration
Data Log configuration

NETWORK

Configuration (highlighted)
Connectivity
Firewall
Wake on LAN
SNMP
MODBUS/BACNET
JSON
SYSLOG

DATE & TIME

NTP & Timezone
Configuration

EMAILS

Configuration

ADVANCED

Expert Shell

General Network configuration

GENERIC NETWORK CONFIGURATION

Hostname: netman630a1373 Network protocol: Static IP DHCP

IPV4 CONFIGURATION

IP Address: Please insert the IP address
Netmask: Please insert the netmask Gateway: Please insert the gateway
Primary DNS: Please insert the primary DNS Secondary DNS: Please insert the secondary DNS

802.1X ON IPV4

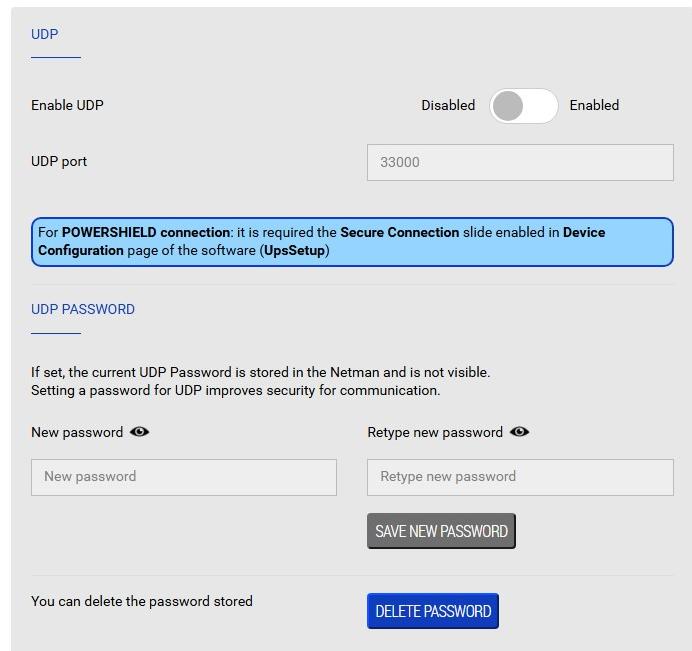
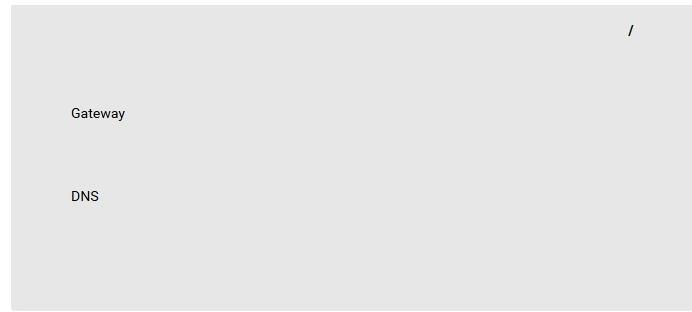
802.1x on IPv4: Disable Enable

IPV6 CONFIGURATION

Enable IPv6: Enabled
Stateless: Privacy Extension:
Prefix Delegation: Accept Router Advertisement:

Link-local address: fe80::202:63ff:fe0a:1373/64
Global Unique address: /

/



| Field | Description | Default |
|---------------------------------|--|--|
| Hostname | Enter the NetMan 208C host name | netman63XXYYZZ see also  below |
| Static IP/DHCP | Choose between static IP or dynamic IP (DHCP) | DHCP |
| IP Address | Enter the IP address | Not active / Empty |
| Netmask | Enter the netmask to be used together with the static IP address | Not active / Empty |
| Gateway | Enter the name or the address of the network gateway | Not active / Empty |
| Primary DNS | Enter the name or the address of the preferred DNS to be used | Not active / Empty |
| Secondary DNS | Enter the name or the address of the alternative DNS to be used | Not active / Empty |
| 802.1x on IPv4 | To enable the 802.1x protocol on IPv4 | Disabled (see also section “IEEE 802.1x”) |
| Enable IPv6 | Allow to enable IPv6 protocol | Enabled |
| Method | Available method: <i>Stateless</i> | Stateless |
| Privacy Extension | Option for requesting usage or random-generated IPv6 address instead of pre-defined address creation (related to MAC address) | Enabled |
| Enable Serial network tunneling | To enable the serial network tunnelling protocol | Disabled |
| Enable UDP | To enable UDP/UPSMon service | Disabled |
| UDP port | Enter the port where the UDP/UPSMon service is started ⁽¹⁾ Expected when UDP enabled: 33000 or as set in the UPDMon software | Not set / Empty |
| UDP Password | To change the password used for UDP/UPSMon communication | Not set / Empty |

⁽¹⁾ This port must be the same as configured in the UPDMon software

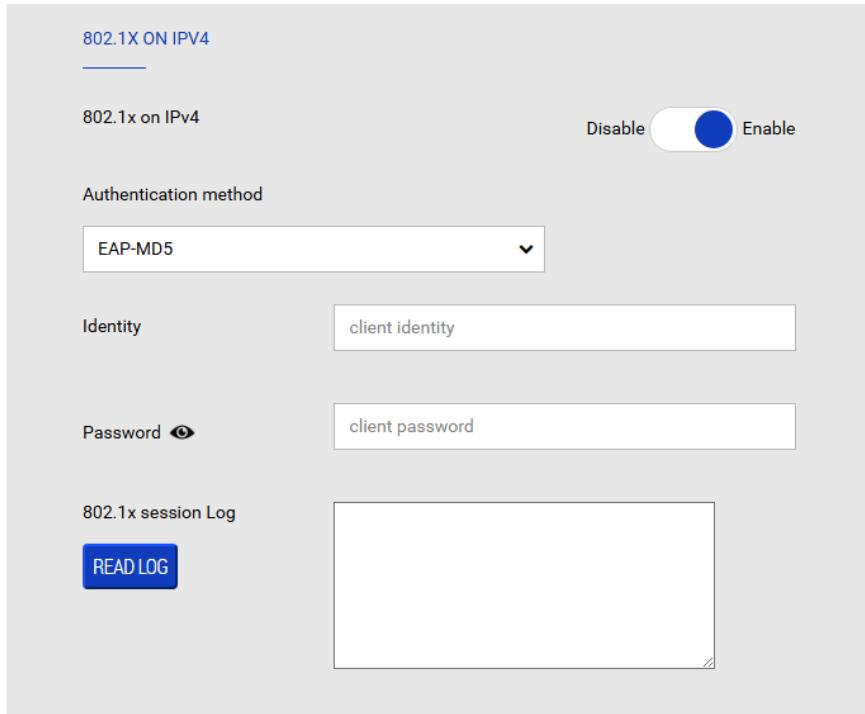
How to access NetMan 208C via Hostname.

- ➔ By default, the Hostname is built from MAC address
e.g., from NetMan MAC Address: 00:02:63:05:00:37 → <https://netman63050037.local>
- ➔ If the User changes the Hostname the new hostname becomes active
e.g., new Hostname “**servernetman**” → <https://servernetman.local>

How to access NetMan 208C via IPv6 address.

- ➔ With IPv6 active, one or more addresses are available. URL address is built with the structure **http://[ipv6address]** inside “[...]" (square brackets)
e.g., with assigned address fe80::202:63ff:fe07:b205 → [https://\[fe80::202:63ff:fe07:b205\]](https://[fe80::202:63ff:fe07:b205])

IEEE 802.1x



802.1x allows the setting of a security layer in LAN wired networks, able to implement a network access control and authentication protocol for preventing unauthorized clients connected to a LAN port inside an existing network.

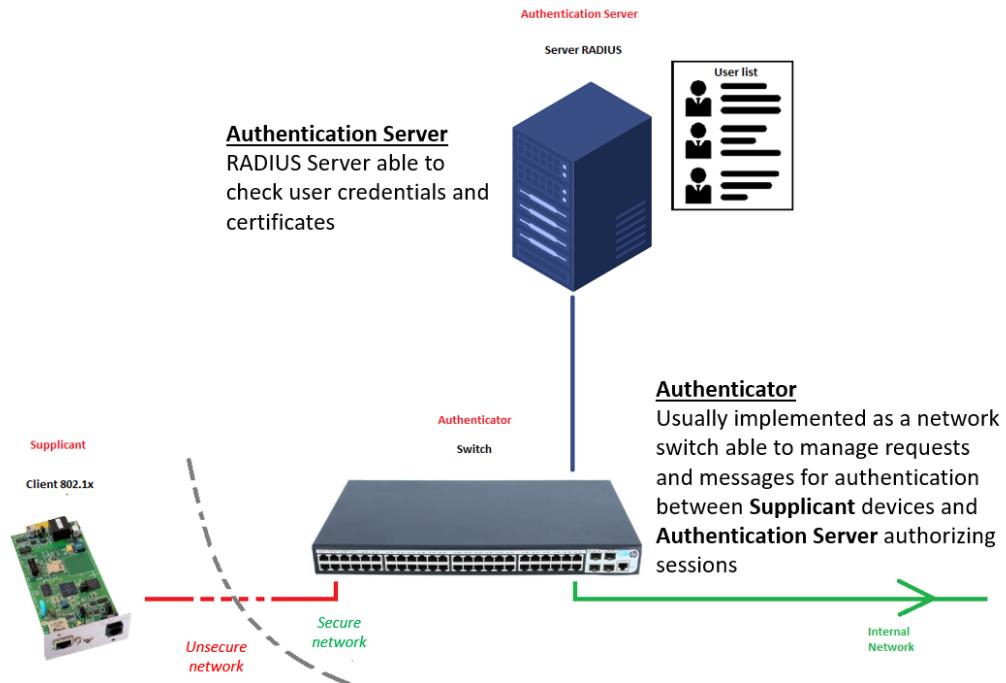
Inside a network, the NetMan 208C using the 802.1x has the role of:

- the **Supplicant**: the device asking for connection to an existing secure network, with its credentials and/or certificates within the authentication method chosen.

The existing network must have implemented the other roles:

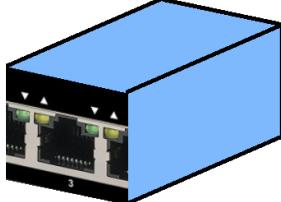
- the **Authenticator**: usually implemented as a Network switch able to implement/configure 802.1x control and authentication on its LAN ports, where the devices connect to
- the **Authentication Server**: usually implemented as RADIUS Server with EAP able to check credentials (usually LDAP) and certificates (for encryption)

EAP 802.1x

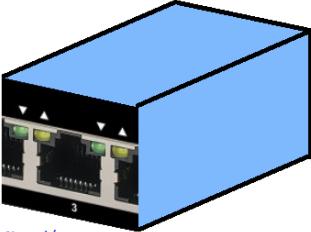


IEEE 802.1x behaviour vs common LAN connectivity

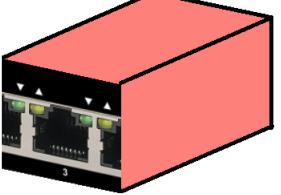
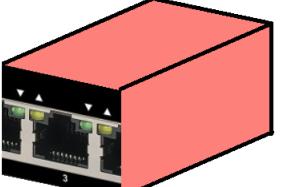
Usually, every common LAN port inside a network is a “ALWAYS AUTHORIZED” port: every device connected to it has rights to connect to the LAN without the need of any authentication:

| | | |
|---|--|--------------------------------------|
|  |  | Network connectivity: OK ✓ |
|---|--|--------------------------------------|

When a network device with IEEE 802.1x configuration active is plugged into the same port it gains the same rights to connect (its special 802.1x configuration is ignored):

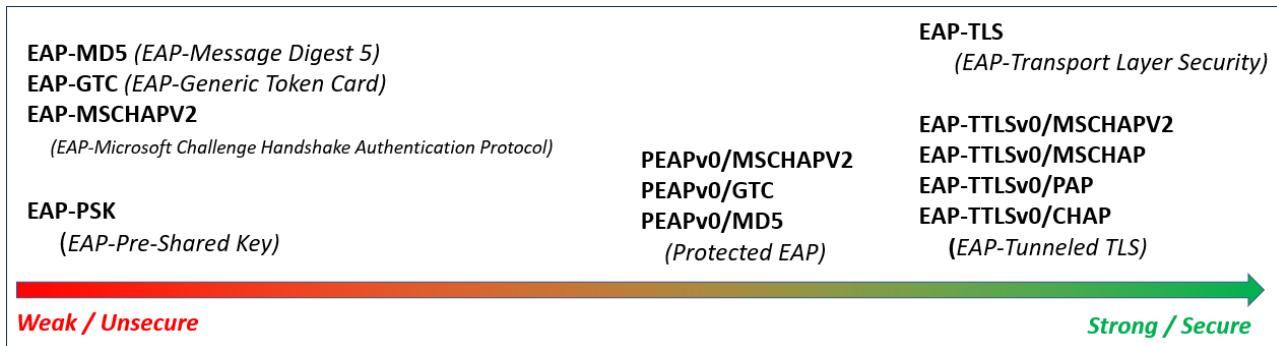
| | | |
|---|--|--------------------------------------|
|  |  | Network connectivity: OK ✓ |
|---|--|--------------------------------------|

On the opposite, when IEEE 802.1x is implemented in the network, the **Authenticator** switch accepts only **Supplicant** devices with valid IEEE 802.1x configuration and all the other devices are blocked:

| | | |
|---|--|---|
|  |  | Network connectivity: BLOCKED ✗ |
|  |  | Network connectivity: OK ✓ |

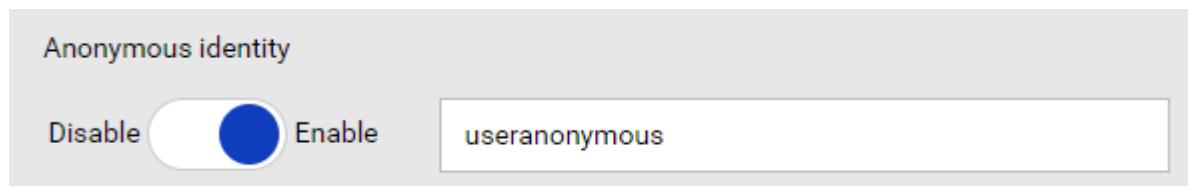
This is the aim and the security layer implemented at the **Authenticator** (the *network switch*) level. Behind the Authenticator must be implemented all the rest of 802.1x infrastructure supporting the Authenticator role as needed.

Authentication methods implemented in NetMan 208C



Even if introducing parameters for authentication, some methods may expose clear traffic that can be sniffed with a “man-in-the-middle” technique, other methods expose partially at first stage in clear traffic and then encrypt the rest of the traffic. The most secure methods allow the usage of encrypted secure traffic from the beginning for the communication, given by the usage of Certificates and Keys. The choice of the right method is the key for a secure IEEE 802.1x authentication but it may require more work and care for a correct implementation and configuration.

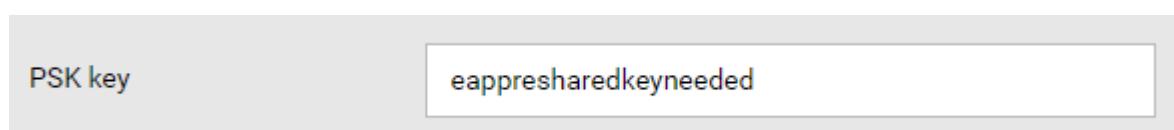
Due to the method chosen, the configuration of NetMan 208C may require parameters like:



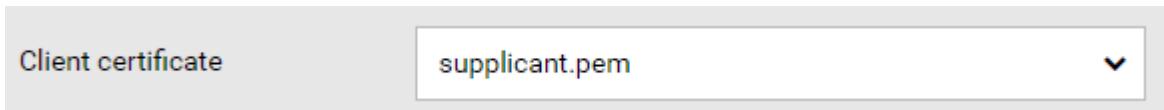
Anonymous identity: it covers the first credentials used for authentication, allowing the use of a custom “anonymous” user. This functionality is strongly depended on the **Authentication Server** (LDAP) implementation.



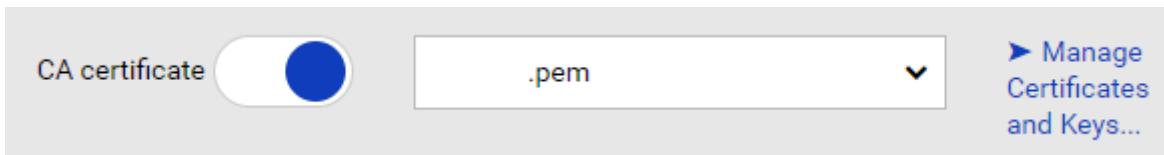
Identity and Password: used for authentication referring the users active in the **Authentication Server**. For some methods is only needed the *Identity* parameter, not the *Password*.



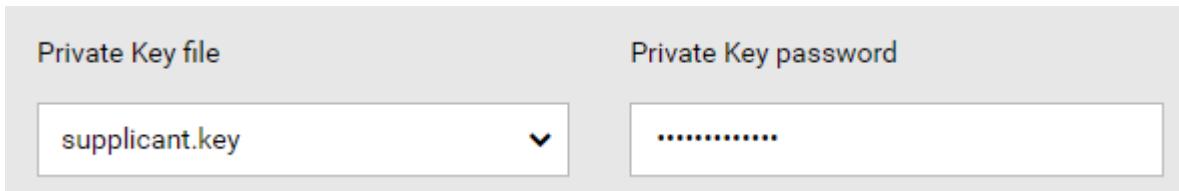
Pre-Shared Key: the pre-shared key defined for the connection.



Client Certificate: the Certificate generated for the device (NetMan 208C) that may be generated with *Openssl* procedures from network **CA Authority** or from the **Authentication Server**, with internal scripts.



CA certificate: can be *self-signed* (if generated from the **Authentication Server**) or *fully CA trusted* from a CA Authority (network or global): it is mandatory for some authentication methods and optional for others.



Private Key and Password: when needed it is required always with its Private Key password associated.

Log of authentications

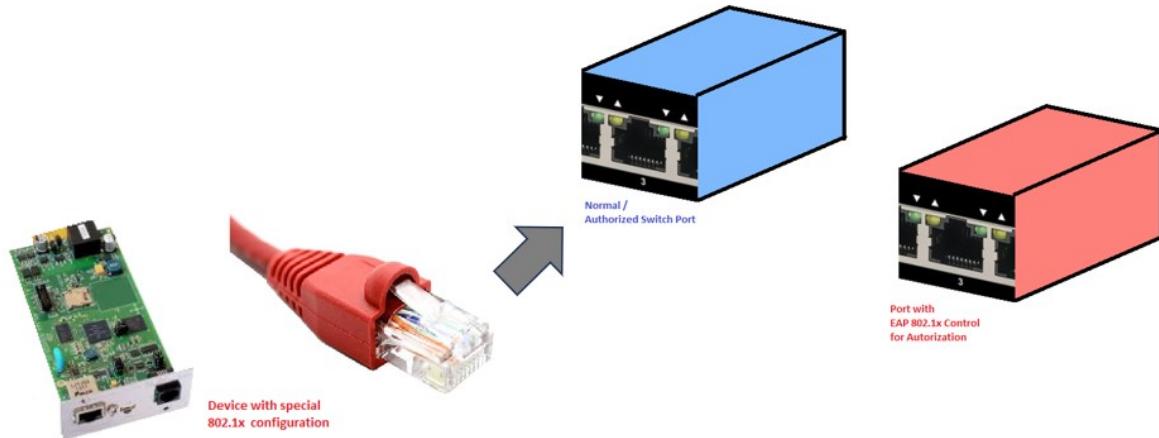
| 802.1x session Log | |
|--------------------|--|
| READ LOG | 12/9/2023 08:35:20 SUCCESS 12/9/2023 08:36:20 SUCCESS 12/9/2023 08:37:20 SUCCESS 12/9/2023 08:38:20 SUCCESS 12/9/2023 08:39:20 SUCCESS |

The web configuration page allows the user to check the **SUCCESS** or the **FAIL** of the authentication process, for a quick check. It is normal that the check is periodical (e.g. every minute). The aim of this log is to give feedback of the credentials/method/certificate authentication and configuration. When IEEE 802.1x is configured and enabled in NetMan 208C, the normal state is always **SUCCESS**.

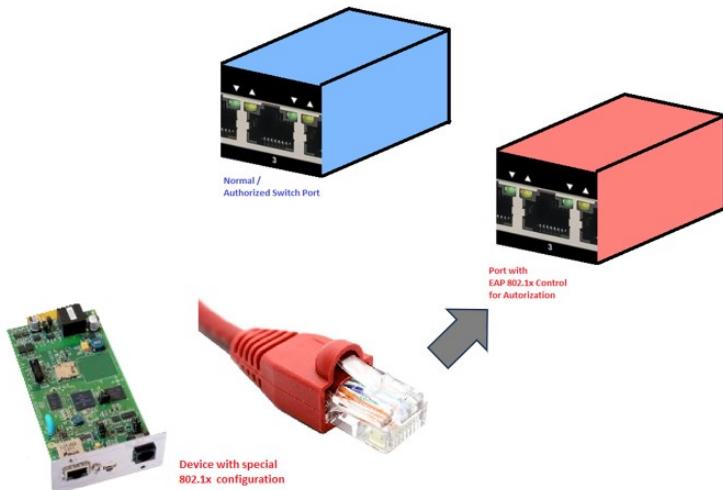
Troubleshooting 802.1x with NetMan 208C

IEEE 802.1x for NetMan 208C may consider many parameters and certificates: just one wrong parameter may cause NetMan 208C unreachable via network connection. In case of problems, follow these steps:

- ⇒ Unplug the NetMan 208C and connect its cable to a “normal” switch port



- ⇒ Now NetMan 208C comes reachable again: Login and change the 802.1x configuration in NetMan 208C.
- ⇒ Save new configuration.
- ⇒ now connect NetMan 208C LAN cable to the Port with 802.1x in the switch:



- ⇒ Check if NetMan 208C is reachable.
- ⇒ In case of other problems, it is possible to check the **Authenticator** (switch) or the **Authentication Server (RADIUS Server)** for any Logs or messages/feedback information useful, trying to understand what may be wrong.
- ⇒ if useful, crosscheck the same exact 802.1x configuration with another device.
- ⇒ Repeat the steps until you reach the desired configuration.

Complexity

When securing a network implementing IEEE 802.1x it is possible to reach a good level of safety:

- only the network devices (“**Supplicants**”) with the secure configuration have permission to connect to the internal LAN network, all the other devices cannot connect.

There are some drawbacks related to its complexity:

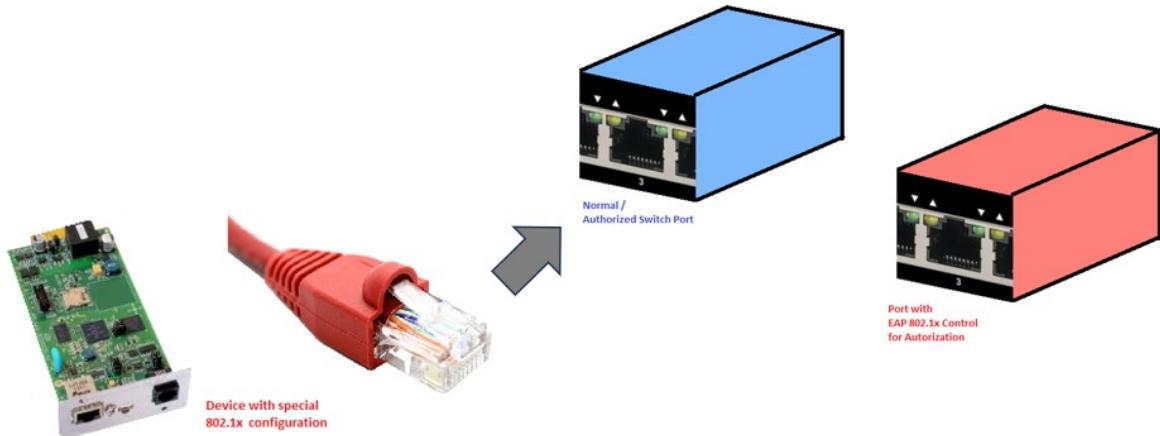
- **Authenticator** device (e.g. *network switch*) may not be so common to install and implement in small networks
- **Authentication Server** (e.g. *RADIUS Server*) must be implemented internally in the network (with roles as authentication LDAP and WPA/EAP service) and maintained with all credentials needed by devices and all certificates/keys always updated (both for Supplicants and Authentication Server).
- The **choice of the authentication methods** ranges from less secure to the more secure method: the more secure the method, the more care is required for its configuration for each **Supplicant** device.
- Difficult diagnostic and debugging in case of problems: in case of FAILURE or wrong parameters diagnostic and debug may be not so easy.
- Finally, the **Certificate and Keys** used must be generated, managed and maintained with care for its validity and then loaded into the **Supplicant** device and the **Authentication Server**.

Overall, besides its complexity, implementing a secure LAN network with 802.1x may help to avoid common weak situations as unwanted intrusions and network threats, especially in big networks.

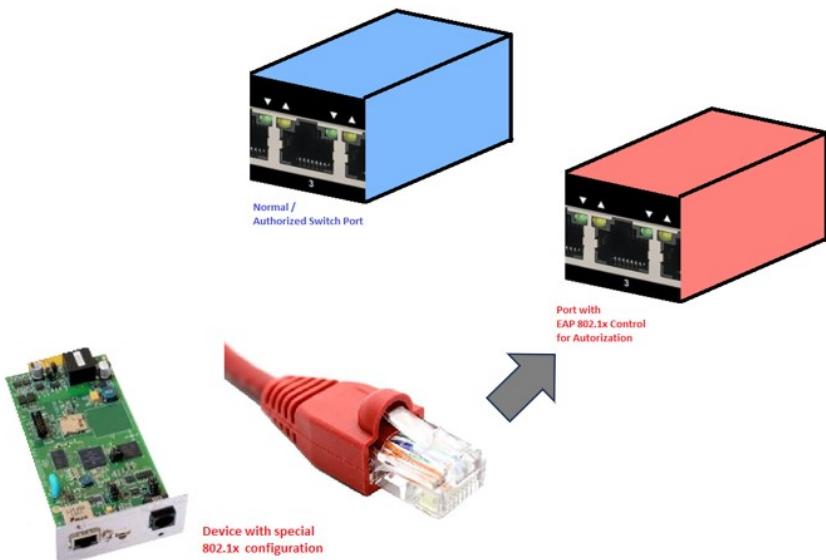
!!! Updating NetMan 208C and Update/Maintenance Mode

When the User must update NetMan 208C must leave normal Application of NetMan 208C and go to Update/Maintenance Mode. Update/ Maintenance Mode does use any 801.1x secure connection, so it is needed to:

- *unplug and reconnect NetMan 208C to a Normal LAN port in the Network so NetMan 208C is reachable during Update/Recovery.*



When finished and rebooting successfully, NetMan 208C can be reconnected back to the Secure 802.1x port network:



Connectivity

Connectivity menu allows the user to check Network states and connections active.

The screenshot shows the 'CONFIGURATION' tab selected in the top navigation bar. The main content area is divided into several sections:

- YOUR NETMAN** (selected)
- SENSORS**
- MODEM**
- REMOTE HOSTS**

DEVICE

- General configuration
- Command configuration
- Data Log configuration

NETWORK

- Configuration
- Connectivity** (selected)
- Firewall
- Wake on LAN
- SNMP
- MODBUS/BACNET
- JSON
- SYSLOG

DATE & TIME

- NTP & Timezone
- Configuration

EMAILS

- Configuration

ADVANCED

- Expert Shell

Internet Connectivity

Allows to check Internet Connectivity querying Gateway, DNS and network permissions. Press the button to start the check:

CHECK INTERNET CONNECTIVITY

Check Ping

Host to ping

host to ping

CHECK PING

Active Network Connections

Allows to check current Active Connections to the Netman. Press the button to check and show the connections:

CHECK ACTIVE NETWORK CONNECTIONS

| Protocol | Local | Remote | State |
|----------|-----------------|------------------|--------|
| TCPv4 | 127.0.0.1:53 | 0.0.0.0:* | LISTEN |
| TCPv4 | 10.1.10.240:53 | 0.0.0.0:* | LISTEN |
| TCPv4 | 0.0.0.0:80 | 0.0.0.0:* | LISTEN |
| TCPv4 | 0.0.0.0:443 | 0.0.0.0:* | LISTEN |
| TCPv4 | 127.0.0.1:953 | 0.0.0.0:* | LISTEN |
| TCPv4 | 10.1.10.240:443 | 10.1.10.88:59580 | ESTAB |
| UDPv4 | 0.0.0.0:68 | 0.0.0.0:* | UNCONN |
| UDPv4 | 127.0.0.1:53 | 0.0.0.0:* | UNCONN |

Internet Connectivity

Checks the state of internet connection from NetMan 208C.

During the connectivity test, the following network entities are checked:

- reachability and query of the User defined GATEWAY (Configuration -> Network)
- reachability of remote address 8.8.8.8
- reachability and query of remote www.google.com request (port 80) and ping

Status reported may be:

| Status | Issue | To do |
|---|--|--|
| OK, Full connectivity (Internet) allowed and working | OK, NetMan 208C has full access to internet | OK, nothing to do |
| ERR #0: No network interface active | Internal issue of NetMan 208C | Notify to the Service |
| ERR #1: No Gateway IP | No IP address gateway defined in the configuration | Set a Gateway IP address in the network parameters |
| ERR #2: Ping Gateway IP FAIL: please check the Gateway IP address and its reachability | IP address gateway not reachable | Check the Gateway IP address in the network parameters |
| ERR #3: Ping external IP FAIL: please check permissions to ping outside the network on the internet by simple IP address | Issue pinging external IP address | Check the access to external network (internet) |
| ERR #4: Query_DNS FAIL: please check permissions to ping the DNS resolver | Issue trying to resolve external hostname with DNS | Check the external DNS resolution (internet) |
| ERR #5 Ping DNS (Internet) FAIL: please check permissions to resolve hosts on the internet by simple host name resolution (DNS) | Issue trying to ping external hostname | Check the permission to ping external hostnames |

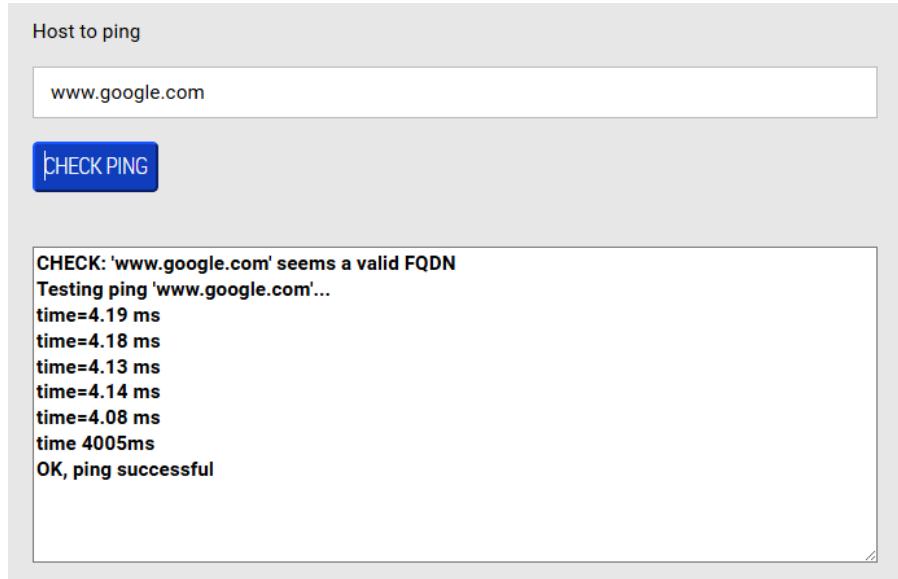
Check Ping

This operation checks the ping execution and IP/Hostname reachability from NetMan 208C.
Useful for:

- checking remote host reachability
- internal network server reachability

| Field | Description |
|--------------|--------------------------------------|
| Host to ping | Enter IP address or Hostname to ping |

Expected successful output:



The screenshot shows a user interface for performing a ping. At the top, there is a text input field labeled "Host to ping" containing "www.google.com". Below this is a blue button labeled "CHECK PING". To the right of the button, the output of the ping command is displayed in a text box. The output text is as follows:

```
CHECK: 'www.google.com' seems a valid FQDN
Testing ping 'www.google.com'...
time=4.19 ms
time=4.18 ms
time=4.13 ms
time=4.14 ms
time=4.08 ms
time 4005ms
OK, ping successful
```

Active Network Connections

It allows the user to check the current active network connections to NetMan 208C and listening ports.

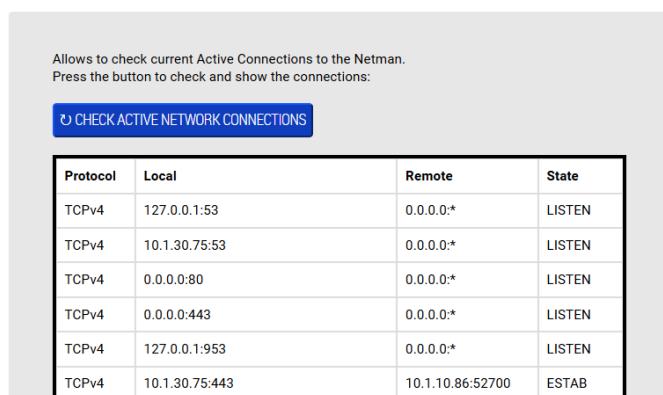
If a Service is enabled and not used, please consider disabling it.

If an active connection is detected and not expected, please consider creating a specific firewall rule for blocking that incoming connection (-> see Firewall configuration).

Notes:

- some ports must be opened and listening for system networking (e.g.: TCP/53 used for DNS resolution, UDP/68 used for DHCP)

[Active Network Connections](#)



The screenshot shows a table of active network connections. The table has four columns: "Protocol", "Local", "Remote", and "State". The data in the table is as follows:

| Protocol | Local | Remote | State |
|----------|----------------|------------------|--------|
| TCPv4 | 127.0.0.1:53 | 0.0.0.0:* | LISTEN |
| TCPv4 | 10.1.30.75:53 | 0.0.0.0:* | LISTEN |
| TCPv4 | 0.0.0.0:80 | 0.0.0.0:* | LISTEN |
| TCPv4 | 0.0.0.0:443 | 0.0.0.0:* | LISTEN |
| TCPv4 | 127.0.0.1:953 | 0.0.0.0:* | LISTEN |
| TCPv4 | 10.1.30.75:443 | 10.1.10.86:52700 | ESTAB |

Firewall

DASHBOARD DATA SYSTEM OVERVIEW HISTORY **CONFIGURATION** ADMINISTRATION

YOUR NETMAN SENSORS MODEM REMOTE HOSTS

DEVICE

General configuration
Command configuration
Data Log configuration

NETWORK

Configuration
Connectivity
Firewall
Wake on LAN
SNMP
MODBUS/BACNET
JSON
SYSLOG

DATE & TIME

NTP & Timezone
Configuration

EMAILS

Configuration

ADVANCED

Expert Shell

Firewall configuration

FIREWALL

Enable Firewall Rules

INCOMING Rules (IPv4 only)

| Enabled | From IP address | IP address | From MAC address | MAC address | Protocol | Port | # |
|----------------------------|-----------------|------------|------------------|-------------|----------|------|---|
| No data available in table | | | | | | | |

Default incoming rule: ACCEPT

You must test the rules before confirm...

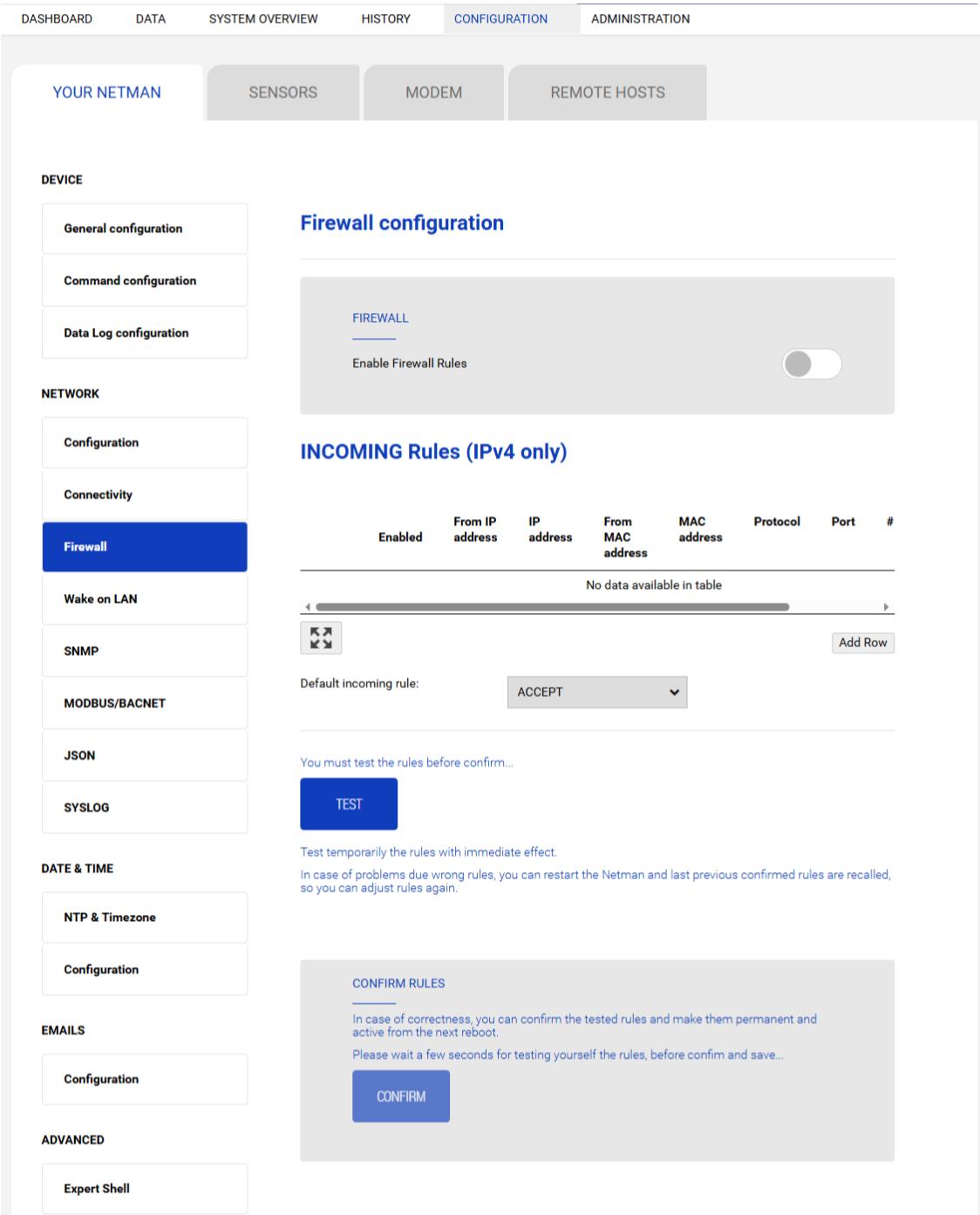
TEST

Test temporarily the rules with immediate effect.
In case of problems due wrong rules, you can restart the Netman and last previous confirmed rules are recalled, so you can adjust rules again.

CONFIRM RULES

In case of correctness, you can confirm the tested rules and make them permanent and active from the next reboot.
Please wait a few seconds for testing yourself the rules, before confirm and save...

CONFIRM



Firewall configuration can allow and/or block the traffic incoming to NetMan 208C due to the rules set with this configuration. It is disabled by default and must be enabled by the User.

Notes:

- please consider enabling the internal firewall for limiting access only to allowed remote hosts
- for a stronger security please consider adding an external physical firewall and limit the access to the network cables conduits

The basic firewall logic requires to set the custom **Incoming rules** desired:

| Enabled | From IP address | IP address | From MAC address | MAC address | Protocol | Port | # | Action |
|---------|-------------------------------------|------------|------------------|-------------|----------|------|---|--------|
| 0 | <input checked="" type="checkbox"/> | Any | Any | Any | WEB-HTTP | Any | | ACCEPT |
| 1 | <input checked="" type="checkbox"/> | Any | Any | Any | FTP | Any | | REJECT |

that filter the traffic incoming to NetMan 208C where each rule checks the *Source of connection*:

- by **IP Address** or **Netmask** (e.g., 10.2.30.5, 10.0.1.0/24) [default is **Any**]
- by **MAC address** (e.g., 00:50:56:00:C0:01) [default is **Any**]

and in addition, filtering the traffic incoming that requests:

- a specific protocol used by then NetMan 208C (**BACNET**, **MODBUS**, **PING**, **SNMP**, **SSH**, **UPSMON***, **WEB-HTTP***, **WEB-HTTPS***)
- a custom protocol set by user for **TCP/<portnumber>** or **UDP/<portnumber>**

where each rule follows one ACTION:

- **ACCEPT**: allows the traffic filtered by the rule
- **DROP**: lets drop the traffic request incoming due to the rule (no response is sent back to the Source of the connection)
- **REJECT**: refuses the connection (an answer of reject is sent back to the Source of the connection)

When a specific traffic does not match any rules in the rules table, the **Default Incoming rule** is applied:

Default incoming rule:

ACCEPT

▾

where options are:

- **ACCEPT**: allows the traffic
- **DROP**: lets drop the traffic incoming

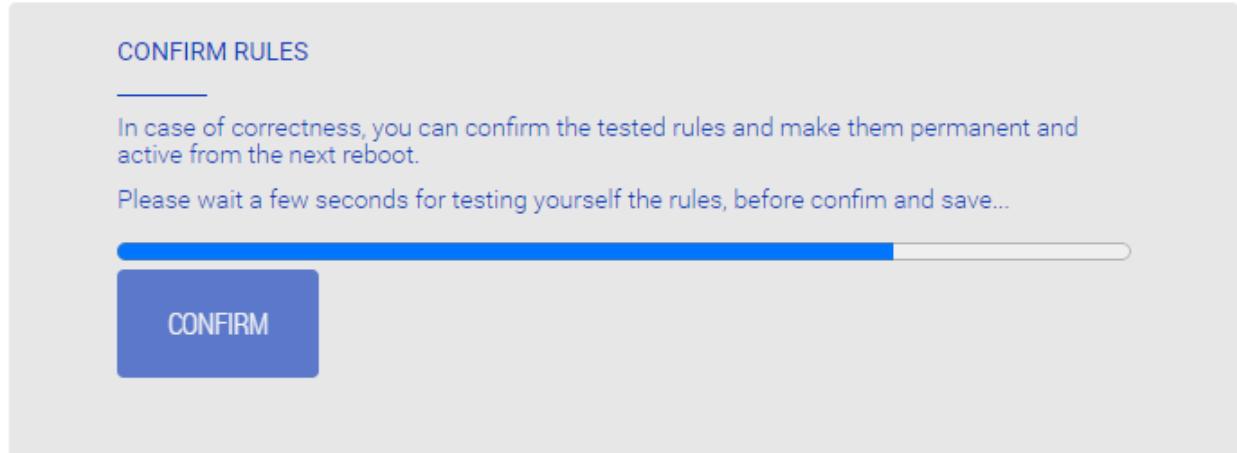
After setting all the **Rule Table** and the **Default Incoming rule**, it is possible to **TEST** the firewall logic immediately:

TEST

Test temporarily the rules with immediate effect.

In case of problems due wrong rules, you can restart the Netman and last previous confirmed rules are recalled, so you can adjust rules again.

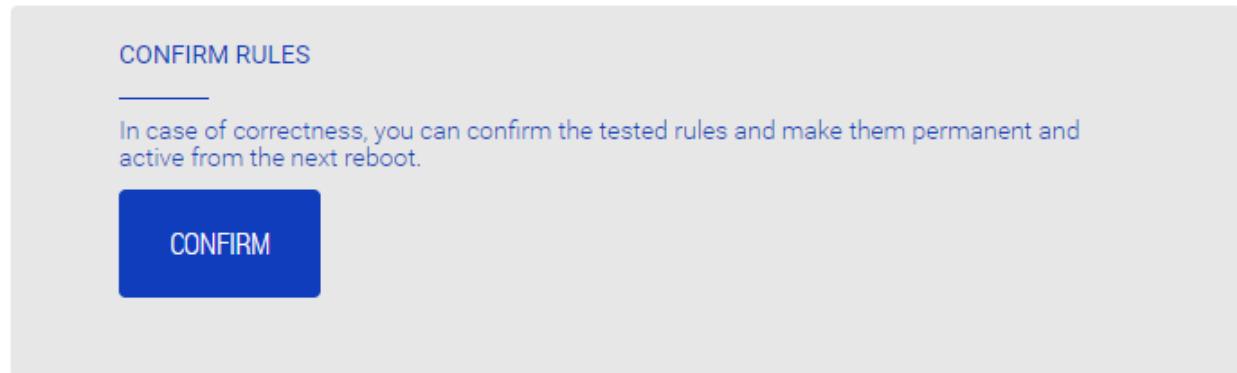
The TEST activates temporarily the rules forcing the user to wait some time before any CONFIRM action:



At this moment the rules are temporarily active, giving some time to the User to check them:

- in case of **connection lost** the User can reboot NetMan 208C (physically un-plugging and re-plugging again in the slot) and connection is restored as it was before firewall TEST, so the User can re-check the rules and TEST again with the new rule changes

Only after the forced count-down time, if behavior of the rules is validated the User can click on the **CONFIRM** button:



After CONFIRM button, the activated rules are written, saved, applied and ready for the next reboot. From now, in case of NetMan 208C not reachable, the only solution is to reset it to the default configuration, losing any configuration applied.

Workflow for a correct configuration

Enable the firewall

FIREWALL

Enable Firewall Rules



Set/change the rules

| Enabled | From IP address | IP address | From MAC address | MAC address | Protocol | Port | # | Action |
|---------|-------------------------------------|--|------------------|--------------------------------------|--------------------------------------|--------------------------------------|---|---|
| 0 | <input checked="" type="checkbox"/> | Specify <input type="button" value="▼"/> | 10.1.11.31 | Any <input type="button" value="▼"/> | Any <input type="button" value="▼"/> | Any <input type="button" value="▼"/> | | ACCEPT <input type="button" value="▼"/> <input type="button" value="Delete"/> |
| 1 | <input checked="" type="checkbox"/> | Specify <input type="button" value="▼"/> | 10.1.10.56 | Any <input type="button" value="▼"/> | Any <input type="button" value="▼"/> | Any <input type="button" value="▼"/> | | ACCEPT <input type="button" value="▼"/> <input type="button" value="Delete"/> |



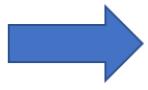
Set the Default Incoming rule

Default incoming rule:



Test the rules

TEST



No

Yes

Confirm
the rules

CONFIRM

Notes and suggestions



Safe rule

During first configuration/testing phase, please set a “**safe rule**” as 1st rule (at the top of the rule table) always allowing all traffic to NetMan 208C, incoming from a specific IP or MAC address (from the machine where the User is configuring NetMan 208C):

| Enabled | From IP address | IP address | From MAC address | MAC address | Protocol | Port | # | Action |
|-------------------------------------|-----------------|------------|------------------|-------------|----------|------|---|--------|
| <input checked="" type="checkbox"/> | Specify | 10.1.11.31 | Any | Any | Any | Any | | ACCEPT |

In this way, if some rules are set wrong, the User can always connect to NetMan 208C and adjust the wrong rules. Only after a successful test the User can remove this “**safe rule**” if no more needed.

Without any “**safe rule**” the User risks losing connection to NetMan 208C, with unique solution of resetting to default (by physical button) losing any configuration previously applied.



Beware the action defined by “**Default Incoming Rule**”: when is set to **DROP** only the traffic **ACCEPTED** by the custom rules in the table is allowed.



The worst condition possible is setting all the rules in the table with **DROP** and **Default Incoming Rule as DROP**: in this way NetMan 208C will refuse any connection and becomes no more reachable: in this case, it must be reset to default by pressing the physical button, losing any configuration applied to NetMan 208C configuration.



For the protocols labelled as **UPSMON***, **WEB-HTTP*** and **WEB-HTTPS***, firewall rules automatically follow the settings/port defined in the related configuration sections:

UPSMON* (default port 33000)

UDP

Enable UDP

UDP port 33000

UPD PASSWORD

Password

Retype Password

HTTP* (default port 80)

Enable HTTP

HTTP port 80

HTTPS* (default port 443)

Enable HTTPS

HTTPS port 443

Wake-on-LAN

DASHBOARD DATA SYSTEM OVERVIEW HISTORY **CONFIGURATION** ADMINISTRATION

YOUR NETMAN SENSORS MODEM REMOTE HOSTS

DEVICE

General configuration
Command configuration
Data Log configuration

NETWORK

Configuration
Connectivity
Firewall
Wake on LAN
SNMP
MODBUS/BACNET
JSON
SYSLOG

DATE & TIME

NTP & Timezone
Configuration

EMAILS

Configuration

ADVANCED

Expert Shell

Wake On Lan

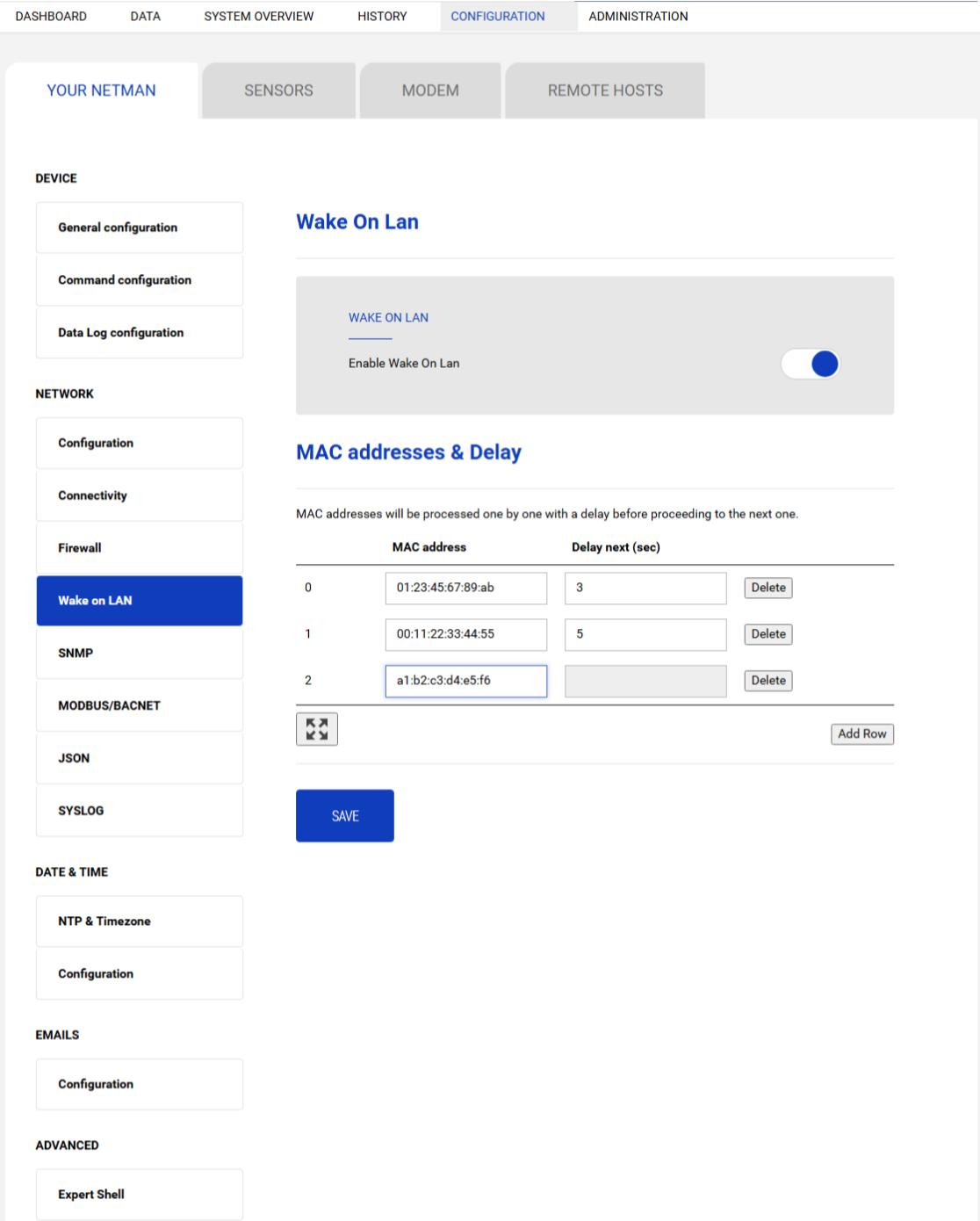
WAKE ON LAN

Enable Wake On Lan

MAC addresses & Delay

MAC addresses will be processed one by one with a delay before proceeding to the next one.

| | MAC address | Delay next (sec) | |
|---|-------------------|------------------|---------------------------------------|
| 0 | 01:23:45:67:89:ab | 3 | <input type="button" value="Delete"/> |
| 1 | 00:11:22:33:44:55 | 5 | <input type="button" value="Delete"/> |
| 2 | a1:b2:c3:d4:e5:f6 | | <input type="button" value="Delete"/> |



With this menu it is possible to populate a list of the MAC addresses for executing Wake-on-LAN operation. Please remember to set the *Delay Next* time (in seconds) between each execution. The list order can be easily managed dragging up/down the rows by the “row number” on the left.

The Wake-on-LAN is sent when NetMan 208C boots and when the mains power returns after a black-out.



Please make sure that the target PC supports this function and that is properly configured.

SNMP

DASHBOARD DATA SYSTEM OVERVIEW HISTORY **CONFIGURATION** ADMINISTRATION

YOUR NETMAN

SENSORS

MODEM

REMOTE HOSTS

DEVICE

General configuration

Command configuration

Data Log configuration

NETWORK

Configuration

Connectivity

Firewall

Wake on LAN

SNMP

MODBUS/BACNET

JSON

SYSLOG

DATE & TIME

NTP & Timezone

Configuration

EMAILS

Configuration

ADVANCED

Expert Shell

SNMP configuration

SNMP

Enable SNMP protocol



CONFIGURATION MODE

Wizard Configuration

[Advanced File Configuration](#)

SNMP configuration wizard

SNMP VERSION

SNMP V3

SNMP V1/V2

SNMP v3

USERS

| Username | Auth | Priv | authPassword | privPassword | User permissions |
|----------------------|----------------------------------|----------------------------------|----------------------|----------------------|--|
| <input type="text"/> | <input type="button" value="▼"/> | <input type="button" value="▼"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> GET <input type="checkbox"/> SET <input type="checkbox"/> TRAP |
| <input type="text"/> | <input type="button" value="▼"/> | <input type="button" value="▼"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> GET <input type="checkbox"/> SET |
| <input type="text"/> | <input type="button" value="▼"/> | <input type="button" value="▼"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> GET <input type="checkbox"/> SET |
| <input type="text"/> | <input type="button" value="▼"/> | <input type="button" value="▼"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> GET <input type="checkbox"/> SET |

TRAP RECEIVER

Trap receiver 1

Trap receiver 5

Trap receiver 2

Trap receiver 6

Trap receiver 3

Trap receiver 7

Trap receiver 4

Trap receiver 8

TRAP REPEATER

Re-send traps every (minutes)

2

SAVE

SEND SPECIFIC TRAP (PLEASE CLICK SAVE BEFORE TESTING)

Select the trap to send

SEND

YOUR NETMAN

SENSORS

MODEM

REMOTE HOSTS

DEVICE

General configuration

Command configuration

Data Log configuration

NETWORK

Configuration

Connectivity

Firewall

Wake on LAN

SNMP

MODBUS/BACNET

JSON

SYSLOG

DATE & TIME

NTP & Timezone

Configuration

EMAILS

Configuration

ADVANCED

Expert Shell

SNMP configuration

SNMP

Enable SNMP protocol



CONFIGURATION MODE

Wizard Configuration

Advanced File Configuration

SNMP configuration file upload

SAMPLE CONFIGURATION FILE

```
# Netman 208C SNMP configuration examples
#
# each line must begin with one of these keyword:
#
# for comment, the line is skipped
# addUser for adding a new user and setting the passwords
# addGroup for putting a user into a group
# addAccessEntry for enabling access privileges to a group
# addView for adding privileges
# addManager for adding SNMP Managers which will receive SNMP traps
#
#
# HOW TO ENABLE SNMPV1/V2 WITH CUSTOM COMMUNITIES (myread, mywrite)
#
#
#addGroup v2 myread v1v2group
#addGroup v1 myread v1v2group
#addGroup v1 mywrite v1v2groupWrite
#addGroup v2 mywrite v1v2groupWrite
#
```

UPLOAD NEW SNMP CONFIGURATION FILE (*.CONF)

Drag & drop here your SNMP configuration file

TRAP REPEATER

Re-send traps every (minutes)

2



SAVE

SNMP (Simple Network Management Protocol) is a communications protocol, a tool that allows the client (manager) to effect requests to a server (agent). This protocol is an international standard and so any SNMP manager can communicate with any SNMP agent.

To exchange information, the manager and agent utilise an addressing technique called MIB (Management Information Base). MIB defines which variables can be requested and the respective access rights. MIB is equipped with a tree structure (like the folders on a hard disk), through which manager and agent can use several MIB at the same time, as there is no overlap.

Each MIB is oriented to a particular sector; in particular RFC-1628, also called UPS-MIB, holds the data for UPS remote management.

Furthermore, the agent can submit data without a prior request to inform the manager about particularly important events. These messages are called traps.

For more information about SNMP visit this site: <http://www snmp com>.

Use of the Wizard

For configuring SNMP, it is possible to use the wizard web page for a simple configuration using SNMPv3 or SNMPv1/v2.

By default, the more secure SNMPv3 is proposed.



SNMPv3 is strongly suggested due to its better security and encryption algorithms.



If user chooses to set SNMPv1/v2 (very insecure protocol) should not set “public” / “private” for communities, well known as the basic first attack surface.

Use of Advanced configurations

Advanced configuration requires to customize the proposed snmp.conf sample configuration file (please see chapter “SNMP configuration”).

| Field | Description | Default |
|---------------------------------|--|----------------------|
| Enable SNMP protocol | To enable the SNMP service. | Disabled |
| Configuration mode | Choose between <i>wizard configuration</i> or to upload a <i>configuration file</i> (<i>configuration file</i> may result more complex to configure). | Wizard Configuration |
| SNMP version | Choose between <i>SNMPv3</i> (suggested, more secure) and <i>SNMPv1/v2</i> (less secure). | SNMPv3 |
| Get community | Enter the community for read access. If set: please avoid the commonly used “public” community. | Empty |
| Set community | Enter the community for write access. If set: please avoid the commonly used “private” community. | Empty |
| Trap community | Enter the community for traps If set: please avoid the commonly used “public” community. | Empty |
| Trap receiver (8 receivers) | Enter the IP addresses to which traps are sent. (e.g.: “10.1.51.3”) | Empty |
| Username | Enter the USM username. (username for SNMPv3) | Not set / Empty |
| Auth | Enter the authentication algorithm. (algorithm for SNMPv3 authentication) | Not set / Empty |
| Priv | Enter the privacy algorithm. (algorithm for SNMPv3 encryption) | Not set / Empty |
| AuthPassword | Enter the authentication password. (password for SNMPv3 authentication) | Not set / Empty |
| PrivPassword | Enter the privacy password. (password for SNMPv3 encryption) | Not set / Empty |
| Permissions GET / SET / TRAP | Choose the permissions for each user SNMPv3 Permissions: GET / SET / TRAP. | Not set |
| Send specific TRAP | Allow the user to send a TRAP for testing. | |

MODBUS/BACNET

The screenshot shows a configuration interface for a device. The top navigation bar includes links for DASHBOARD, DATA, SYSTEM OVERVIEW, HISTORY, **CONFIGURATION** (which is the active tab), and ADMINISTRATION. Below the navigation is a secondary navigation bar with tabs: YOUR NETMAN, SENSORS, MODEM, and REMOTE HOSTS. The main content area is divided into sections:

- DEVICE** section with sub-options: General configuration, Command configuration, Data Log configuration.
- MODBUS/BACNET configuration** section (active):
 - MODBUS** sub-section with an **Enable MODBUS** toggle switch (disabled).
 - BACNET** sub-section with an **Enable BACNET** toggle switch (disabled).
 - BACNET DATA** sub-section with a **BACNET Address (Number)** input field containing the value 1968.
- NETWORK** section with sub-options: Configuration, Connectivity, Firewall, Wake on LAN, SNMP, **MODBUS/BACNET** (highlighted in blue), JSON, SYSLOG.
- DATE & TIME** section with sub-options: NTP & Timezone, Configuration.
- EMAILS** section with sub-options: Configuration.
- ADVANCED** section with sub-options: Expert Shell.

A large blue **SAVE** button is located at the bottom of the configuration section.

For information about MODBUS **registers**, please check the “MODBUS TCP/IP protocol” section.
 For information about BACNET, please check “BACNET/IP configuration” section.

| Field | Description | Default |
|-------------------------|--|-----------------|
| Enable MODBUS | To enable the MODBUS protocol | Disabled |
| Enable BACNET | To Enable the BACNET protocol | Disabled |
| BACNET Address (Number) | Enter the BACNET address of the device | Not set / Empty |

JSON

DASHBOARD DATA SYSTEM OVERVIEW HISTORY **CONFIGURATION** ADMINISTRATION

YOUR NETMAN

SENSORS

MODEM

REMOTE HOSTS

DEVICE

General configuration

Command configuration

Data Log configuration

JSON

JSON

Enable JSON notification



NETWORK

Configuration

Connectivity

Firewall

Wake on LAN

SNMP

MODBUS/BACNET

JSON

SYSLOG

DATE & TIME

NTP & Timezone

Configuration

EMAILS

Configuration

ADVANCED

Expert Shell

JSON

RECEIVER

Monitoring host IP

Host port

Please insert address

port

Notification interval (minutes)

1

SEND NOTIFICATION ON EVENT

| | | | |
|--------------------|--------------------------|---------------------|--------------------------|
| UPS Lock | <input type="checkbox"/> | Overload / overtemp | <input type="checkbox"/> |
| UPS Failure | <input type="checkbox"/> | On Bypass | <input type="checkbox"/> |
| Battery work | <input type="checkbox"/> | Battery low | <input type="checkbox"/> |
| Communication lost | <input type="checkbox"/> | Mainteinance | <input type="checkbox"/> |
| Switch open | <input type="checkbox"/> | Anomaly | <input type="checkbox"/> |
| Command active | <input type="checkbox"/> | Warning | <input type="checkbox"/> |

CURRENT STATUS

Json Service **not enabled**.

LICENSE

License file

No license (default)

If this Netman is for a custom client, please upload your license:

Upload Custom license



SAVE

NetMan 208C can send a periodic message in JSON trap format that contains the status and the values of the UPS. The trap can also be sent on the specified conditions.

| Field | Description | Default |
|---------------------------------|---|--------------------|
| Enable JSON notification | To enable the JSON notification service | Disabled |
| Monitoring host IP | Enter the IP address to which the JSON traps will be sent. e.g. "10.1.55.3" when enabled | Not set / Empty |
| Host port | Enter the port where traps will be sent (port number chosen from the user) e.g. "4000" / user customized when enabled | Not set / Empty |
| Notification interval (minutes) | Enter the interval between JSON trap sending | 1 (minute) |
| Send notification on event | Choose the events upon which the trap will be sent | No events selected |

It requires a license.txt file to be uploaded on NetMan 208C. The content of the file will be included in the trap.

Examples of trap, depending on the usage of license or not:

| Standard (default, no license uploaded) | With license (custom file license uploaded) |
|--|--|
| <pre>[{ "timestamp": 1741960153, "model": "UOD2", "license": "no license", "name": "Netman 208", "location": "", "contact": "", "partnumber": "UOD2", "serialnumber": "ME39VOD20000018", "status": [32, 8, 0, 5, 0, 0], "measures": { "vin1": 229, "vin2": 0, "vin3": 0, "fin": 49.9, "vbyp1": 229, "vbyp2": 0, "vbyp3": 0, "fbyp": 49.9, "vout1": 231, "vout2": 0, "vout3": 0, "fout": 50.0, "load1": 0, "load2": 0, "load3": 0, "vbat": 40.7, "autonomy": 202, "batcap": 89, "tsys": 25 } }]</pre> | <pre>[{ "timestamp": 1741960472, "model": "UPS 6kVA", "license": "this_is_a_custom_license", "io_conf": 1, "status": [32, 8, 0, 5, 0, 0], "measures": { "vin1": 230, "vin2": 0, "vin3": 0, "fin": 499.0, "vbyp1": 230, "vbyp2": 0, "vbyp3": 0, "fbyp": 499.0, "vout1": 231, "vout2": 0, "vout3": 0, "fout": 500.0, "load1": 0, "load2": 0, "load3": 0, "vbat": 406, "autonomy": 202, "batcap": 89, "tsys": 25 } }]</pre> |

Some field contents:

`timestamp` is the instant of the trap in reference to *Unix epoch*.

`model` is the model of the UPS.

`io_conf` is the UPS configuration, some values depends on it (see notes).

`license` is the content of the license file

`status` is an array that must be interpreted as follows:

| byte | bit | Description |
|------|-----|-----------------------------------|
| 0 | 0 | UPS Maintenance |
| | 1 | Communication lost |
| | 2 | Battery low |
| | 3 | Battery work |
| | 4 | On bypass |
| | 5 | UPS Failure |
| | 6 | Overload/Overtemperature |
| | 7 | UPS Locked |
| 1 | 0 | SWIN Open/Battery Low |
| | 1 | SWBYP Open/Battery Working |
| | 2 | SWOUT Open/UPS Locked |
| | 3 | Output Powered |
| | 4 | SWBAT Open |
| | 5 | SWBAT_EXT Open |
| | 6 | Battery not present |
| | 7 | Battery overtemp |
| 2 | 0 | Buck Active |
| | 1 | Boost Activated |
| | 2 | O.L./L.I. function |
| | 3 | Load threshold exceeded/On Bypass |
| | 4 | EPO command active |
| | 5 | BYPASS command active |
| | 6 | Service UPS |
| | 7 | Service battery |
| 3 | 0 | Replace Battery |
| | 1 | Battery Charged |
| | 2 | Battery Charging |
| | 3 | Bypass Bad |
| | 4 | Low redundancy |
| | 5 | Lost redundancy |
| | 6 | System anomaly |
| | 7 | |
| 4 | 0 | Bypass backfeed/Beep On |
| | 1 | Test in progress |
| | 2 | Shutdown Imminent |
| | 3 | Shutdown Active |
| | 4 | PM1 fault/lock |

| | | |
|---|---|-----------------------|
| | 5 | PM2 fault/lock |
| | 6 | PM3 fault/lock |
| | 7 | PM4 fault/lock |
| 5 | 0 | PM5 fault/lock |
| | 1 | Alarm Temperature |
| | 2 | Alarm Overload |
| | 3 | PM6 fault/lock |
| | 4 | PM7 fault/lock |
| | 5 | BM fault/lock |
| | 6 | Power supply PSU fail |
| | 7 | Battery unit anomaly |

measures, contains the instant values of the UPS at the timestamp time. The measures with note **(1)** aren't meaningful when **io_conf** is 1, the measures with note **(2)** aren't meaningful when **io_conf** is 1 or 3.

JSON License

A specific **JSON file license** can be uploaded in the specific section:

LICENSE

License file
No license (default)

If this Netman is for a custom client, please upload your license:

Upload Custom license

(OPTIONAL) UPLOAD A NEW LICENSE FILE NAMED "LICENSE.TXT" FOR JSON (FILE .TXT)

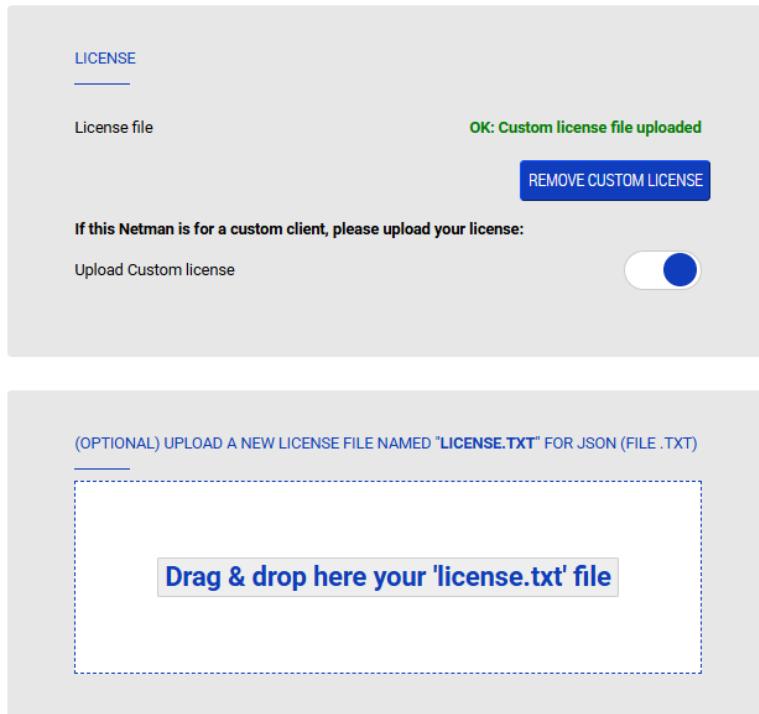
Drag & drop here your 'license.txt' file

The license file is a simple text file with a text string:
e.g.:

license.txt

License_00-AA-BB-CC-DD-EE-FF-1234-ABCDEFG

When JSON license is uploaded:



The following JSON data are sent:

| With custom file license upload |
|---|
| <pre>[{ "timestamp": 1741960472, "model": "UPS 6kVA", "license": "License_00-AA-BB-CC-DD-EE-FF-1234-ABCDEG", "io_conf": 1, "status": [32, 8, 0, 5, 0, 0], "measures": { "vin1": 230, "vin2": 0, "vin3": 0, "fin": 499.0, "vbyp1": 230, "vbyp2": 0, "vbyp3": 0, "fbyp": 499.0, "vout1": 231, "vout2": 0, "vout3": 0, "fout": 500.0, "load1": 0, "load2": 0, "load3": 0, "vbat": 406, "authonomy": 202, "batcap": 89, "tsys": 25 } }]</pre> |

The usage of the "license" field may be used from the remote Server as identification of which NetMan/UPS sending JSON traps.

Syslog

DASHBOARD DATA SYSTEM OVERVIEW HISTORY CONFIGURATION ADMINISTRATION

This menu allows the user to configure the syslog service over UDP port.

| Field | Description | Default |
|------------------------|---|-----------------|
| Enable remote syslog | To enable the syslog service | Disabled |
| Syslog server IP | Enter the IP address of the syslog server e.g. "10.11.51.23" when enabled | Not set / Empty |
| Server UDP port | Enter the UDP port where the events will be sent When enabled: 514 (standard) or user customized | No set / Empty |
| TEST SYSLOG CONNECTION | Allow to send a test message log to the syslog server set | |

DATE & TIME

NTP & Timezone

The screenshot shows the 'NTP & Timezone configuration' page within the 'CONFIGURATION' tab of the NetMan 208C interface. The left sidebar lists various configuration categories: 'YOUR NETMAN', 'SENSORS', 'MODEM', 'REMOTE HOSTS', 'DEVICE' (with 'General configuration', 'Command configuration', and 'Data Log configuration' sub-options), 'NETWORK' (with 'Configuration', 'Connectivity', 'Firewall', 'Wake on LAN', 'SNMP', 'MODBUS/BACNET', 'JSON', and 'SYSLOG' sub-options), and 'DATE & TIME' (with 'NTP & Timezone' and 'Configuration' sub-options). The 'NTP & Timezone' sub-option is highlighted with a blue background. The main content area displays the 'NTP & Timezone configuration' page. It shows the current date as '22 Dec 09:13 UTC 2025'. Two main configuration sections are present: 'SET A NEW TIMEZONE' (with a dropdown menu labeled 'PLEASE CHOOSE') and 'SET A NTP SERVER' (with a text input field labeled 'NTP server address (IP)'). A red warning box contains the text: 'WARNING: ! HTTPS PROTOCOL IS ENABLED AND ANY TIME CHANGE MAY COMPROMISE AND INVALIDATE THE CURRENT SESSION AND THE NEXT WEB ACCESS, DUE TO TIME MISMATCH.' A blue 'SAVE' button is located at the bottom of the configuration area.

With this menu it is possible to configure the NTP synchronization.

| Field | Description | Default |
|-------------------------|---|-----------------|
| Set a new Timezone | Time zone to set. e.g.: "ROME" when set | Not set |
| NTP server address (IP) | Enter the name or address of the NTP server If not set, by default a pool address set is used. e.g. 10.11.12.13 when set. | Not set / Empty |



NetMan 208C basic internal services (e.g. HTTPS, Certificate validations) require a correct date and time to work properly. It is therefore necessary to configure them always correctly for a correct logging event, reporting notifications and certificates validation in the System.



Only for some specific UPS models: if a valid time is received by the configured NTP server, NetMan 208C will synchronize the clock of the UPS daily (at 00:30).

Configuration

DASHBOARD DATA SYSTEM OVERVIEW HISTORY CONFIGURATION ADMINISTRATION

YOUR NETMAN

SENSORS

MODEM

REMOTE HOSTS

DEVICE

General configuration

Command configuration

Data Log configuration

NETWORK

Configuration

Connectivity

Firewall

Wake on LAN

SNMP

MODBUS/BACNET

JSON

SYSLOG

DATE & TIME

NTP & Timezone

Configuration

EMAILS

Configuration

ADVANCED

Expert Shell

Date & Time configuration

Current date is 22 Dec 09:15 UTC 2025

SET A NEW DATE

Date

dd/mm/yyyy



Hour

00

Minutes

00

WARNING: ! HTTPS PROTOCOL IS ENABLED AND ANY TIME CHANGE MAY COMPROMISE AND INVALIDATE THE CURRENT SESSION AND THE NEXT WEB ACCESS, DUE TO TIME MISMATCH.

SAVE

| Field | Description | Default |
|---------|---|-----------------|
| Date | Enter the current date. e.g. 19/11/2025 – format “dd/mm/yyyy” when set | Not set / Empty |
| Hour | Enter the current hour. | Not set / 00 |
| Minutes | Enter the current minutes. | Not set / 00 |

EMAILS

Configuration

DASHBOARD DATA SYSTEM OVERVIEW HISTORY **CONFIGURATION** ADMINISTRATION

YOUR NETMAN SENSORS MODEM REMOTE HOSTS

DEVICE

General configuration
Command configuration
Data Log configuration

NETWORK

Configuration
Connectivity
Firewall
Wake on LAN
SNMP
MODBUS/BACNET
JSON
SYSLOG

DATE & TIME

NTP & Timezone
Configuration

EMAILS

Configuration

ADVANCED

Expert Shell

Email configuration

Enable Email

MAIL HOST & SMTP

Mail host: Please insert the address
SMTP port: 25

OTHER PARAMETERS

Sender address: Please insert sender email
Transport: Plain

Username: Please insert username
Password: Please insert password

EMAILS

| | Email #1 | Email #2 | Email #3 |
|-----------------------------------|--------------------------|--------------------------|--------------------------|
| Device Lock | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Overload / overtemp | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| General Failure | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| On Bypass | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Input blackout | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Battery low | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Communication lost | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Ext. sensor Temp out of range | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Ext. sensor Humidity out of range | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Ext. sensor Input contact active | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Security alerts | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

EMAIL REPORT

Send report every day at 00:10
Send report every Sunday at 00:10

SAVE

To configure the email addresses to which alarm notifications and email reports are sent and other related parameters.

| Field | Description | Default |
|------------------------|---|--------------------|
| Enable Email | To enable the Email service. | Disabled |
| Mail host | Enter the name or the address of the SMTP server to be used to send e-mails. ⁽¹⁾ | Not set / Empty |
| SMTP port | The IP port used by the SMTP protocol (standard ports are: 25-PLAIN / 465-SSL / 587-STARTTLS). | Not set / Empty |
| Sender address | Enter the address from which the e-mails are sent. ⁽²⁾ | Not set / Empty |
| Username | If the server requires authentication, enter the "Username". | Not set / Empty |
| Password | If the server requires authentication, enter the password. | Not set / Empty |
| Transport | It is possible to choose between PLAIN, SSL or TLS. <ul style="list-style-type: none"> • PLAIN = None (not encrypted). • SSL = SSL/TLS (encrypted). • TLS = STARTTLS (starts not encrypted, then encrypted). | PLAIN |
| Email #1 | Enter the e-mail addresses (recipients) to which to send the alarm notifications and reports (see notes below). | Not set / Empty |
| Email #2 | | |
| Email #3 | | |
| Device events | Choose the event upon which the email will be sent. | No events selected |
| Send report every day | To send the email report every day at 00:00. | Disabled |
| Send report every week | To send the email report every Monday at 00:00. | Disabled |

⁽¹⁾ Ensure that the SMTP server accepts connections on the configured port

⁽²⁾ Do not use the "space" character in this field

After having set the data and saving, the service can be tested. If the test is performed, a test email is sent to all the configured email addresses.



Report e-mails are sent to all the addresses set.
Alarm notification e-mails are sent only to the selected addresses.

The following table describes the meaning of the events. These can vary depending on the device connected.

| Event | Meaning |
|---------------------------------------|---|
| Device Lock | Device is locked or in a severe failure state |
| Ovrlload/Ovrtemp | Device in overload or in overtemperature |
| General Failure | Failure of the device |
| On bypass | Operation from bypass |
| Input blackout | The input source is in blackout |
| Battery low | Battery low |
| Communic lost | No communication between NetMan 208C and the UPS. |
| Ext. sensor Temp out of range (*) | Events on temperature range, when Environmental Sensors are configured (high and low temperature threshold) As addition: - notification on sensor lost/disconnected/reconnected events |
| Ext. sensor Humidity out of range (*) | Events on humidity range, when Environmental Sensors are configured (high and low humidity value threshold) As addition: - notification on sensor lost/disconnected/reconnected events |
| Ext. sensor Input contact active (*) | Events on input I/O, when Environmental Sensors are configured (input contact changes) As addition: - notification on sensor lost/disconnected/reconnected events |
| Security alerts (**) | General Security notification when: - a user fails to login and is being blocked or retries - alert when too many requests are detected from internal web server |

Sensor Events (*)

Details of event notifications sent related to the Sensors:

| Events | Flags | | |
|---|-------------------------------|-----------------------------------|----------------------------------|
| | Ext. sensor Temp out of range | Ext. sensor Humidity out of range | Ext. sensor Input contact active |
| High temp alarm | Send email | - | - |
| High temp restore | ✓ Send email | - | - |
| Low temp restore | ✓ Send email | - | - |
| Low tempo alarm | ✓ Send email | - | - |
| High humidity alarm | - | ✓ Send email | - |
| High humidity restore | - | ✓ Send email | - |
| Low humidity restore | - | ✓ Send email | - |
| Low humidity alarm | - | ✓ Send email | - |
| Input contact alarm | - | - | ✓ Send email |
| Input contact restore | - | - | ✓ Send email |
| Sensor LOST alarm (sensor disconnected) | ✓ Send email | ✓ Send email | ✓ Send email |
| Sensor LOST restore (sensor reconnected) | ✓ Send email | ✓ Send email | ✓ Send email |

Security alerts (**)

Event “Security alerts” is recalled when:

- Web Login: a user exceeds failing login during the authentication: an email is sent to inform the Security alerts recipients
- Web requests: an excessive number of web pages/queries are received from NetMan 208C: an email is sent to inform the Security alerts recipients

ADVANCED

Expert Shell

DASHBOARD DATA SYSTEM OVERVIEW HISTORY **CONFIGURATION** ADMINISTRATION

YOUR NETMAN SENSORS MODEM REMOTE HOSTS

DEVICE

General configuration

Command configuration

Data Log configuration

NETWORK

Configuration

Connectivity

Firewall

Wake on LAN

SNMP

MODBUS/BACNET

JSON

SYSLOG

DATE & TIME

NTP & Timezone

Configuration

EMAILS

Configuration

ADVANCED

Expert Shell

Expert Shell

WARNING ! SOME PARAMETERS ARE CRITICAL AND MAY MIS-CONFIGURE THE NETMAN CHANGING ITS BEHAVIOUR OR WITH RISK OF LOSING CONNECTION WITH IT.

Parameter: (parameter name)

Value: (value)

GET SET DELETE



This menu is available only to “admin” user.

| Field | Description | Default |
|-----------|--|-----------------|
| Parameter | Name of the internal parameter | Not set / Empty |
| Value | Value of the internal parameter | Not set / Empty |
| GET | Reads the content of the internal parameter requested The value read is reported in the Value field | |
| SET | Writes the value in the Value field to the internal parameter set | |
| DELETE | Delete the parameter requested | |



Modifying these parameters may lead to a malfunction or critical states with NetMan 208C; please operate in this menu only when specifically requested by Thecnical Support or by following detailed instructions.

SENSORS

NAVIGATION: DASHBOARD DATA SYSTEM OVERVIEW HISTORY **CONFIGURATION** ADMINISTRATION ⌚ 26 NOV 13:17 UTC 2025

YOUR NETMAN SENSORS MODEM REMOTE HOSTS

SENSORS

Main

Scan the sensors

Events configuration

Environmental sensors configured (3)

SENSOR 1

TEST SENSOR

26°C 38%RH OPEN Input 1 OPEN Output 1

Sensor 1

SENSOR 2

TEST SENSOR

21°C 49%RH OPEN Input 2 OPEN Output 2

Sensor 2

SENSOR 3

TEST SENSOR

26°C 38%RH CLOSE Input 3 OPEN Output 3

Sensor 3

General Sensors configuration

SENSORS CONFIGURATION

Enable sensors

SAVE

To configure the **optional** environmental sensors connected to NetMan 208C.



Refer to the **ENVIRONMENTAL SENSOR User manual** for installation and configuration of the sensors.

GSM MODEM

Configuration

NetMan 208C can send as SMS notification if one or more alarm conditions occur. The SMS can be sent to up to three recipients and they can be sent for seven different kinds of alarm.



An external GSM modem (optional accessory) and a SIM card with pin request disabled are required.

The screenshot shows the 'Modem' configuration page within the NetMan 208C web interface. The top navigation bar includes links for DASHBOARD, DATA, SYSTEM OVERVIEW, HISTORY, CONFIGURATION (which is highlighted in blue), and ADMINISTRATION. Below the navigation is a secondary navigation bar with tabs for YOUR NETMAN, SENSORS, MODEM (which is highlighted in blue), and REMOTE HOSTS. The main content area is titled 'GSM Modem configuration'. It contains several sections: 'Enable SMS' (with a toggle switch), 'MODEM CONFIGURATION' (with a field for 'SMSC Short Message Service Center number'), 'FEATURES & NOTIFICATION' (a table with columns for SMS #1, SMS #2, and SMS #3, and rows for various alarm types like Device Lock, Overload / overtemp, General Failure, etc.), 'SMS REPORT' (with toggle switches for 'Send report every day' and 'Send report every week'), and a 'TEST SMS' button at the bottom. A 'SAVE' button is located at the bottom left of the configuration section.

This menu can be used to configure the GSM modem to send SMS.

| Field | Description | Default |
|--|--|--------------------|
| Enable SMS | To enable the SMS service | Disabled |
| SMSC Short Message Service Center number | Enter the phone number of the Short Message Service Center (e.g.: +3900112233445566) | Not set / Empty |
| SMS #1 | Phone numbers that will receive SMS | Not set / Empty |
| SMS #2 | | |
| SMS #3 | | |
| Device events | Choose the events upon which the SMS will be sent | No events selected |
| Send report every day | To send the SMS report every day at 00:00 | Disabled |
| Send report every week | To send the SMS report every Monday at 00:00 | Disabled |

REMOTE HOSTS

SSH

The screenshot shows the 'REMOTE HOSTS' configuration page. At the top, there is a navigation bar with tabs: DASHBOARD, DATA, SYSTEM OVERVIEW, HISTORY, **CONFIGURATION** (which is the active tab), and ADMINISTRATION. Below the navigation bar, there is a secondary navigation bar with tabs: YOUR NETMAN, SENSORS, MODEM, and **REMOTE HOSTS** (which is the active tab). The main content area is divided into several sections:

- REMOTE HOSTS SHUTDOWN**: A sidebar on the left lists supported hosts: **SSH** (selected), VMware ESXi, Nutanix, and Syneto. The main panel shows the **SSH** configuration with a toggle switch to "Enable remote SSH commands".
- RUN FIRST SCRIPT ON EVENT**: Configuration for running scripts after a mains failure or when autonomy is below a certain level. It includes input fields for minutes and toggle switches.
- Connectors and Scripts**: A table with columns: Enabled, Host, Username, Password, Script, and Delay next (sec). The table is currently empty and displays "No data available in table".
- SHUTDOWN ON EVENT**: Configuration for shutdown events, including a field for "Then, UPS shutdown after (seconds)" and a toggle switch.
- TEST CREDENTIALS**: A button to test the credentials of all hosts in the table.

At the bottom of the configuration area is a large blue **SAVE** button.

This section allows the user to configure the SSH client service: NetMan 208C can connect to remote servers with SSH protocol and execute commands and script in a remote server.



The SSH client service is not compatible with hosts with Windows operating systems. With these hosts, we recommend installing the communication and shutdown software, which has similar or superior functionality.

The main triggering event is configured **enabling** and setting the “On Event” run:

| Field | Description | Default |
|----------------------------------|---|----------|
| Enable remote SSH commands | To enable the SSH client service | Disabled |
| After mains failure | Scripts will be executed after the set minutes of delay after mains failure | Disabled |
| When autonomy is below (minutes) | Scripts will be executed when autonomy is below the minutes set | Disabled |

Actions to call must be configured in the table:

| | Enabled | Host | Username | Password | Script | Delay next (sec) |
|---|-------------------------------------|-------------|-----------|----------|-----------------------------------|------------------|
| 0 | <input checked="" type="checkbox"/> | 10.1.10.151 | adminuser | | #W3##ASC112##ASC119##ASC100#CR##W | 1 |
| 1 | <input checked="" type="checkbox"/> | 10.1.10.183 | admin | | shutdownscript.sh | |

one action per row, with a “delay next” before executing the row below.

For each row, then fields are:

| Row Field | Description | Default |
|------------------|--|-----------------|
| Enabled | Action enabled | Disabled |
| Host | Host to connect to via SSH | Not set / Empty |
| Username | Username for login to SSH | Not set / Empty |
| Password | Password for login to SSH | Not set / Empty |
| Script | Command to execute after login (simple command or multiple command string) | Not set / Empty |
| Delay next (sec) | In case of multiple actions (rows) the delay (seconds) before executing the next action | Not set / Empty |

When all the enabled rows in the table are processed, one by one, the event of “**Shutdown on Event**” may be executed if desired.

SHUTDOWN ON EVENT

SHUTDOWN ON EVENT

Then, UPS shutdown after (seconds)

SAVE

| Field | Description | Default |
|------------------------------|---|-----------------|
| UPS shutdown after (seconds) | Delay of the final action. After that all the defined script have been executed, the UPS will shutdown. | Not set / Empty |
| Slider | Enable/Disabled | Disabled |

Type of commands as action for Script: single command

The basic action can be called as a single command script: just a single command for invoking a sequence of actions desired.

Here some examples:

```
| shutdown 5
| /run/custom/switchchoff.sh
| /run/myshutdownscript.sh
```

Type of commands as Action for Script: multiple command string

A more complete solution is using a multiple command string: is written as single string data but it behaves as a multiple command as if the User were typing char after char the commands (with return keys and other characters including pauses).

This solution with “multiple command string” allow to shutdown a device via SSH when there is the need of some sort of interaction (delays, enter keys, special chars).

The list of tags accepted is:

| <i>TAG</i> | <i>Meaning</i> |
|------------|---|
| #CR# | → Enter key |
| #W1# | → Wait 1 second |
| #W2# | → Wait 2 seconds |
| #W3# | → Wait 3 seconds |
| #W4# | → Wait 4 seconds |
| #W5# | → Wait 5 seconds |
| #W6# | → Wait 6 seconds |
| #W7# | → Wait 7 seconds |
| #W8# | → Wait 8 seconds |
| #W9# | → Wait 9 seconds |
| #ASC001# | For special needs, it is possible to send single chars by its Ascii code: → Ascii(1) |
| #ASC002# | → Ascii(2) |
| #ASC003# | → Ascii(3) |
| ... | ... |
| ... | ... |
| #ASC253# | → Ascii(253) |
| #ASC254# | → Ascii(254) |
| #ASC255# | → Ascii(255) |

Some examples here:

// Shutdown of QNAP

```
| Q#CR#Y#CR#/sbin/poweroff#CR#
that is like typing manually:
| Q (enter)
| Y (enter)
| /sbin/poweroff (enter)
```

// Shutdown commands for “NetApp OnTap 9.9.1”

```
| system node halt -node * -skip-lif-migration-before-shutdown true -ignore-
| quorum-warnings true -inhibit-takeover true -ignore-strict-sync-warnings
| true#CR##W1#Y#CR##W1#Y#CR#
that is like typing manually:
| system node halt -node * -skip-lif-migration-before-shutdown true -ignore-
| quorum-warnings true -inhibit-takeover true -ignore-strict-sync-warnings true
| (enter)
| (wait 1 second)
| Y (enter)
| (wait 1 second)
| Y (enter)
```

// Shutdown command for “Firewall CheckPoint”

```
| halt#CR#Y#CR#
that is like typing manually:
| halt (enter)
| Y (enter)
```



Using ***multiple command string*** always write the correct TAGS, otherwise mis-type TAGs are sent as a command to the remote host/device with errors or unexpected answers (e.g.: do not forget to open and close the special TAGS with a "#").



The usage of ***single command*** and ***multiple command string*** is automatically detected by the presence of char "#": if found in the string is executed as *multiple command string*, otherwise is *single command*.



The ***single command*** is faster than the ***multiple command string***: the first is a simple command launched, the second one instead emulates an SSH session and involves some extra internal delays (few seconds).

VMware ESXi

DASHBOARD DATA SYSTEM OVERVIEW HISTORY CONFIGURATION ADMINISTRATION

YOUR NETMAN

SENSORS

MODEM

REMOTE HOSTS

REMOTE HOSTS SHUTDOWN

SSH

VMware ESXi

Nutanix

Syneto

VMware ESXi

VMWARE ESXI

Enable VMware ESXi shutdown



Infrastructure connectors

| Host or VCSA | Username | Password |
|--------------------|----------|----------|
|--------------------|----------|----------|

No data available in table



Add Row

Actions

| Action | Condition | Condition duration (min) | Delay next (sec) | Source | Target | Restore on power on | Tr... |
|--------|-----------|--------------------------|------------------|--------|--------|---------------------|-------|
|--------|-----------|--------------------------|------------------|--------|--------|---------------------|-------|

No data available in table



Add Row

SHUTDOWN ON EVENT

Additionally, the commands will be executed when on battery low condition and when shutdown is active

Then, UPS shutdown after (seconds)

1



SAVE

TEST VMWARE/VMWARE VCENTER SERVER APPLIANCE SHUTDOWN
(PLEASE CLICK SAVE BEFORE TESTING)

DRY RUN

TEST VMWARE/VMWARE VCENTER SERVER CREDENTIALS
(PLEASE CLICK SAVE BEFORE TESTING)

VALIDATE

This menu enables the configuration of the VMware Esxi shutdown service. Any Esxi host or part of a vSphere infrastructure or the included vCenter server appliance can be shut down, it is possible execute a vMotion in order to move active VM from a host or Cluster to a specific target, each with their separate credentials, priority and delay.

The validity of the credentials is checked periodically and, if not valid, an alarm is generated. It is also possible to shutdown the UPS at the end of the hosts shutdown process.



ATTENTION

The VMware infrastructure has to be installed with a valid license, a free of charge installation doesn't work properly, due to the API access limitation, the virtual machines and the physical servers cannot be shut down due this system limitation.

The slider “Enable ESXi shutdown” enable the ESXi shutdown service.

VMware ESXi

| Field | Description | Default |
|-----------------------------|---|----------|
| Enable VMware ESXi shutdown | Enable or disable the VMware ESXi service | Disabled |

Infrastructure connectors

| Field | Description | Default |
|--------------|---|-----------------|
| Host or VCSA | Enter the hostname or IP address of the ESXi host or VCSA | Not set / Empty |
| Username | Enter the username for ESXi or VCSA administrator | Not set / Empty |
| Password | Enter the password for ESXi or VCSA administrator | Not set / Empty |

Actions

| | Action | Condition | Condition duration (min) | Delay next (sec) |
|---|---------------|------------|--------------------------|------------------|
| 0 | Shutdown VM | Power fail | 5 | 0 |
| 1 | Shutdown Host | Power fail | 10 | 0 |

[Add Row](#)

SHUTDOWN ON EVENT

Additionally, the commands will be executed when on battery low condition and when shutdown is active

Then, UPS shutdown after (seconds)

2



[SAVE](#)

Actions

| Field | Description | Default |
|------------------------------|--|-----------------|
| Action | <p>The action that will be executed:</p> <p>Shutdown VM will shutdown the specific VM</p> <p>Shutdown Host will shutdown all the active VM on the specified host and finally the host itself</p> <p>Shutdown Cluster will shutdown all the active VM on the specified cluster and all hosts part of the cluster</p> <p>VMotion will move all the active VM from a source host to a target host</p> <p>Maintenance will force a host in maintenance mode</p> | Not set / Empty |
| Condition | <p>Power fail: When the UPS detects a main failure, the configured condition duration time (minutes) will begin to countdown. Once the timer has elapsed the selected action will start. If the main returns within this time, then the action will be cancelled.</p> <p>Autonomy less: When the calculated battery autonomy of the UPS falls below the configured condition duration time(minutes) the selected action will start. If main returns within this time, then the action will be cancelled.</p> | Not set / Empty |
| Condition duration (minutes) | The duration that the selected condition (Power fail or Autonomy less) must be active for before the selected action starts. | Not set / Empty |
| Delay next (seconds) | Delay in seconds to execute the next action. | Not set / Empty |
| Source | <p>If the action is Shutdown Host, VMotion or Maintenance; an IP address or hostname of a present host or VCSA must be specified.</p> <p>If the action is Shutdown VM or Shutdown Cluster a valid VM name or Cluster name, present in the infrastructure must be specified.</p> | Not set / Empty |
| Target | If the action is VMotion , a valid IP address or hostname must be specified. | Not set / Empty |
| Restore on power on | <p>In case of shutdown actions, NetMan 208C will restart automatically all the VMs that were shutdown.</p> <p>In case of Maintenance action, NetMan 208C will restore the host from maintenance.</p> <p>Please note that to restart the host the Wake on Lan feature must be used instead.</p> | Not set / Empty |
| Target Netman | For future use. | Not set / Empty |

The priority order of the actions in the action list can be changed, selecting and moving the action row up or down with the mouse.



The vSphere DRS automation function can be used by forcing the target host in Maintenance mode.

SHUTDOWN ON EVENT

| Field | Description | Default |
|------------------------------|---|-----------------|
| UPS shutdown after (seconds) | Delay for UPS shutdown after event occurs | Not set / Empty |
| Shutdown on event | Action of shutdown UPS after all previous actions | Disabled |

It is possible configure the UPS shutdown delay in seconds, this counter will start at the same time of the shutdown actions listed on the Action list.

Additionally, the commands will be executed when on battery low condition and when shutdown is active.

SAVE

This button SAVE the configuration, please note that the service will be restarted.

TEST VMWARE/VMWARE VCENTER SERVER APPLIANCE SHUTDOWN
(PLEASE CLICK SAVE BEFORE TESTING)

DRY RUN

Testing the configuration

It is possible to test the procedure without performing a real shutdown by pressing “Dry Run”. The logs on the target host or vCenter Server Appliance will confirm the correctness of the configuration.

| Description | Type | Date Time | Task | Target | User | Event Type ID |
|---|-------------|----------------------|------|------------|------------------------------|----------------------|
| User logged event: Dry-run test shutdown host 10.1.30.11 | User | 14/11/2019, 12:27:53 | | 10.1.30.11 | VSPPHERE.LOCAL\administrator | vim.event.General |
| User logged event: Dry-run test shutdown host 10.1.30.12 | User | 14/11/2019, 12:27:53 | | 10.1.30.12 | VSPPHERE.LOCAL\administrator | vim.event.General |
| Sensor-1-type : Description Intel Corporation C620 Series Chipset Family Power Manage... | Information | 14/11/2019, 12:27:38 | | 10.1.30.11 | System | com.vmware.vc.Har... |
| Sensor-1-type : Description Intel Corporation C620 Series Chipset Family MEI Controller ... | Information | 14/11/2019, 12:27:38 | | 10.1.30.11 | System | com.vmware.vc.Har... |
| Sensor-1-type : Description Intel Corporation C620 Series Chipset Family MEI Controller ... | Information | 14/11/2019, 12:27:38 | | 10.1.30.11 | System | com.vmware.vc.Har... |
| Sensor-1-type : Description Intel Corporation C620 Series Chipset Family Thermal Subsys... | Information | 14/11/2019, 12:27:38 | | 10.1.30.11 | System | com.vmware.vc.Har... |
| Sensor-1-type : Description Intel Corporation C620 Series Chipset Family USB 3.0 xHCI_C... | Information | 14/11/2019, 12:27:38 | | 10.1.30.11 | System | com.vmware.vc.Har... |
| Sensor-1-type : Description Intel Corporation C620 Series Chipset Family MROM 1 #17 sta... | Information | 14/11/2019, 12:27:38 | | 10.1.30.11 | System | com.vmware.vc.Har... |
| Sensor-1-type : Description Intel Corporation C620 Series Chipset Family MROM 0 #17 sta... | Information | 14/11/2019, 12:27:38 | | 10.1.30.11 | System | com.vmware.vc.Har... |
| Sensor-1-type : Description Intel Corporation Sky Lake-E Ubox Registers #8 state assert f... | Information | 14/11/2019, 12:27:38 | | 10.1.30.11 | System | com.vmware.vc.Har... |
| Sensor-1-type : Description Intel Corporation Sky Lake-E Ubox Registers #8 state assert f... | Information | 14/11/2019, 12:27:38 | | 10.1.30.11 | System | com.vmware.vc.Har... |
| Sensor-1-type : Description Intel Corporation Sky Lake-E Ubox Registers #8 state assert for ... | Information | 14/11/2019, 12:27:38 | | 10.1.30.11 | System | com.vmware.vc.Har... |
| Sensor-1-type : Description Intel Corporation Sky Lake-E RAS #5 state assert for... Part... | Information | 14/11/2019, 12:27:38 | | 10.1.30.11 | System | com.vmware.vc.Har... |

TEST VMWARE/VMWARE VCENTER SERVER CREDENTIALS
(PLEASE CLICK SAVE BEFORE TESTING)

VALIDATE

Validating the connections

It is also possible to test the correct user account and password to login on an ESXi host or vSphere VCSA.

The test will return the result with a pop-up screen.

Nutanix

DASHBOARD DATA SYSTEM OVERVIEW HISTORY **CONFIGURATION** ADMINISTRATION

YOUR NETMAN SENSORS MODEM **REMOTE HOSTS**

REMOTE HOSTS SHUTDOWN

Nutanix

NUTANIX

Enable Nutanix shutdown

CVM CREDENTIALS

Prism address Please insert host address

Prism user Please insert the user name

Prism password Please insert the password

Physical hosts

| Host | Username | Password |
|----------------------------|----------|----------|
| No data available in table | | |

Add Row

Actions

| Action | Condition | Condition duration (min) | Delay next (sec) | Source | Restore on power | Note |
|----------------------------|-----------|--------------------------|------------------|--------|------------------|------|
| No data available in table | | | | | | |

Add Row

SHUTDOWN ON EVENT

Additionally, the commands will be executed when on battery low condition and when shutdown is active

Then, UPS shutdown after (seconds) 1

SAVE

TEST NUTANIX SHUTDOWN (PLEASE CLICK SAVE BEFORE TESTING)

DRY RUN

TEST NUTANIX SERVER CREDENTIALS (PLEASE CLICK SAVE BEFORE TESTING)

VALIDATE

This menu enables the configuration of the Nutanix shutdown service. Any host or part of a Nutanix cluster infrastructure can be shut down, it is possible execute a priority and non-priority VMs shutdown, each with their separate credentials, priority and delay. The validity of the credentials is checked periodically and, if not valid, an alarm is generated. It is also possible to shutdown the UPS at the end of the hosts shutdown process.

The slider “Enable Nutanix shutdown” enable the Nutanix shutdown service

Nutanix

| Field | Description | Default |
|-------------------------|---------------------------------------|----------|
| Enable Nutanix shutdown | Enable or disable the Nutanix service | Disabled |

CVM credentials

| Field | Description | Default |
|---------------|---|-----------------|
| Prism address | Enter the hostname or IP address of the Prism CVM | Not set / Empty |
| Username | Enter the username for CVM administrator | Not set / Empty |
| Password | Enter the password for CVM administrator | Not set / Empty |

Physical hosts

| Host | Username | Password | |
|--|----------|----------|---------------------------------------|
| 10.1.31.10 | root | | <input type="button" value="Delete"/> |
| 10.1.31.12 | root | | <input type="button" value="Delete"/> |
| 10.1.31.14 | | | <input type="button" value="Delete"/> |
| <input type="button" value="Add Row"/> | | | |

Actions

| Action | Condition | Condition duration (min) | Delay next (sec) | |
|--|------------------|--------------------------|------------------|----|
| 0 | non critical VMs | Power fail | 10 | 60 |
| 1 | Critical VM | Power fail | 15 | 20 |
| 2 | Critical VM | Power fail | 15 | 0 |
| <input type="button" value="Add Row"/> | | | | |

Actions

| Duration (min) | Delay next (sec) | Source | Restore on power on |
|----------------|------------------|-------------------------|--|
| | 60 | | <input checked="" type="checkbox"/> Delete |
| | 20 | 79ab502a-13ca-4162-8aa | <input checked="" type="checkbox"/> Delete |
| | 0 | 568bd95a-af84-4510-bcb' | <input checked="" type="checkbox"/> Delete |

[Add Row](#)

SHUTDOWN ON EVENT

Additionally, the commands will be executed when on battery low condition and when shutdown is active

Then, UPS shutdown after (seconds)

180



[SAVE](#)

TEST NUTANIX SHUTDOWN (PLEASE CLICK SAVE BEFORE TESTING)

[DRY RUN](#)

TEST NUTANIX SERVER CREDENTIALS (PLEASE CLICK SAVE BEFORE TESTING)

[VALIDATE](#)

Actions

| Field | Description | Default |
|------------------------------|--|---------|
| Action | The action that will be executed: Non critical VM will shutdown all non-critical VMs Critical VM will shutdown the specified UID critical VM | Not set |
| Condition | Power fail: When the UPS detects a main failure, the configured condition duration time(minutes) will begin to countdown. Once the timer has elapsed the selected action will start. If the main returns within this time, then the action will be cancelled. Autonomy less: When the calculated battery autonomy of the UPS falls below the configured condition duration time(minutes) the selected action will start. If main returns within this time, then the action will be cancelled. | Not set |
| Condition duration (minutes) | The duration that the selected condition (Power fail or Autonomy less) must be active for before the selected action starts. | Not set |
| Delay next (seconds) | Delay in seconds to execute the next action. | Not set |
| Source | If the action is Critical VM a valid VM UID, present in the infrastructure must be specified. | Not set |
| Restore on power on | In case of shutdown actions, NetMan 208C will restart automatically in reverse sequence all the VMs that were shutdown. Please note that to restart the host the Wake on Lan feature must be used instead. | Not set |

The priority order of the actions in the action list can be changed, selecting and moving the action row up or down with the mouse.

SHUTDOWN ON EVENT

| Field | Description | Default |
|------------------------------|---|-----------------|
| UPS shutdown after (seconds) | Delay for UPS shutdown after event occurs | Not set / Empty |
| Shutdown on event | Action of shutdown UPS after all previous actions | Disabled |

It is possible configure the UPS shutdown delay in seconds, this counter will start after the shutdown actions listed on the Action list.

Additionally, the commands will be executed when on battery low condition and when shutdown is active.

SAVE

This button SAVE the configuration, please note that the service will be restarted.

DRY-RUN

Testing the configuration

It is possible to test the procedure without performing a real shutdown by pressing “Dry Run”. The logs on the target Prism CVM will confirm the correctness of the configuration.

Validating the connections

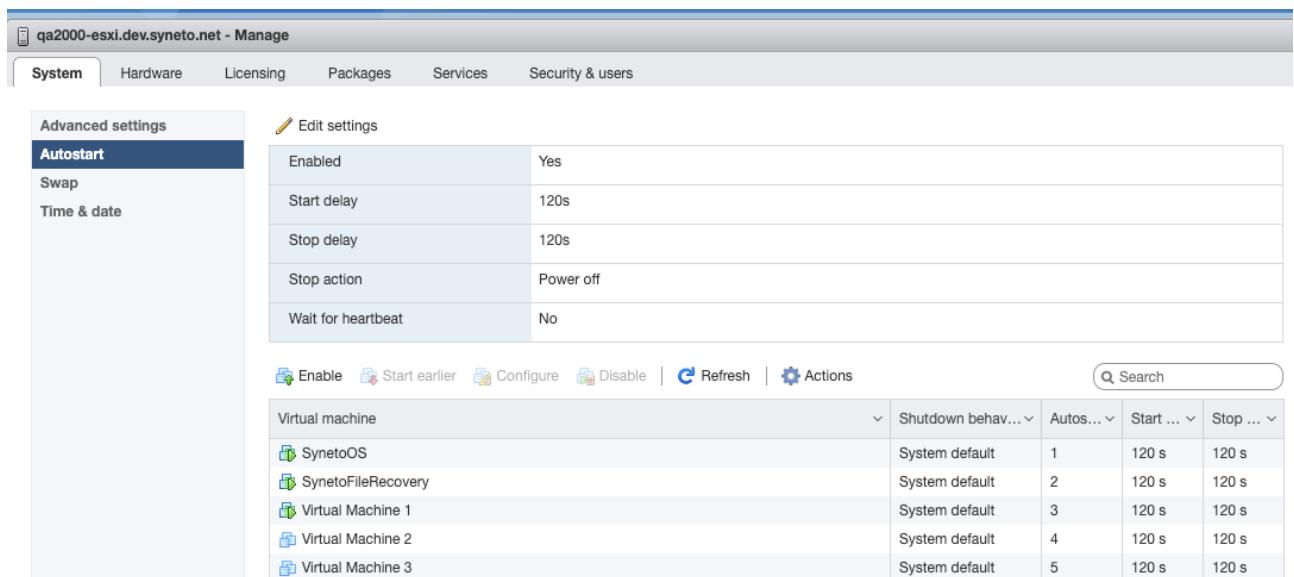
It is also possible to test the correct user account and password to login on a Prism CVM. The test will return the result with a pop-up screen.

Syneto

CONFIGURE ESXI AUTOSTART FUNCTIONALITY

Syneto HYPER appliances have the Autostart functionalities enabled by default on the ESXi hypervisor. This is a mandatory prerequisite so that virtual machines can be powered on or off in the right order when the request is made from NetMan 208C.

Configure the virtual machines that must be powered on the hypervisor in their desired order. SynetoOS and SynetoFileRecovery are always first and second in the list.



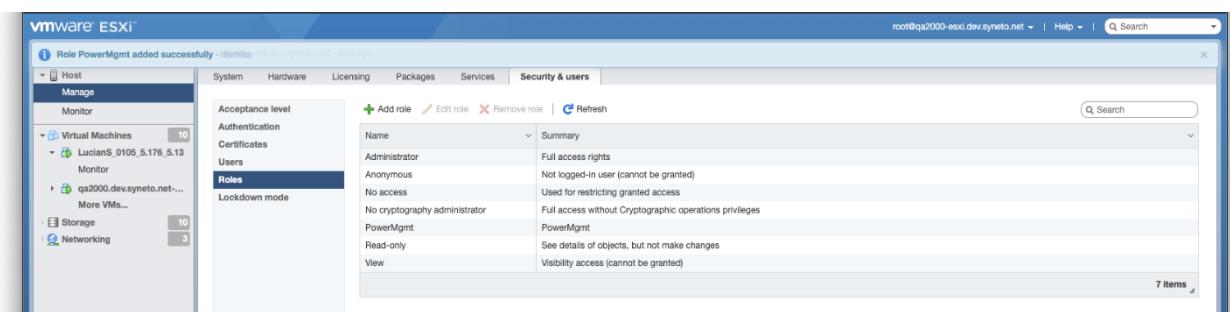
| Virtual machine | Shutdown behav... | Autos... | Start ... | Stop ... |
|--------------------|-------------------|----------|-----------|----------|
| SynetoOS | System default | 1 | 120 s | 120 s |
| SynetoFileRecovery | System default | 2 | 120 s | 120 s |
| Virtual Machine 1 | System default | 3 | 120 s | 120 s |
| Virtual Machine 2 | System default | 4 | 120 s | 120 s |
| Virtual Machine 3 | System default | 5 | 120 s | 120 s |

CONFIGURE ESXI USER & ROLE FOR REMOTE POWER MANAGEMENT

Syneto recommends to configure an ESXi user to be used especially for power management duties by the UPS. This provides a level of security that limits potential attack vectors. Connect to your ESXi host with the Web client.

1. Create a new Role.

Go to Host -> Security and Users -> Roles.

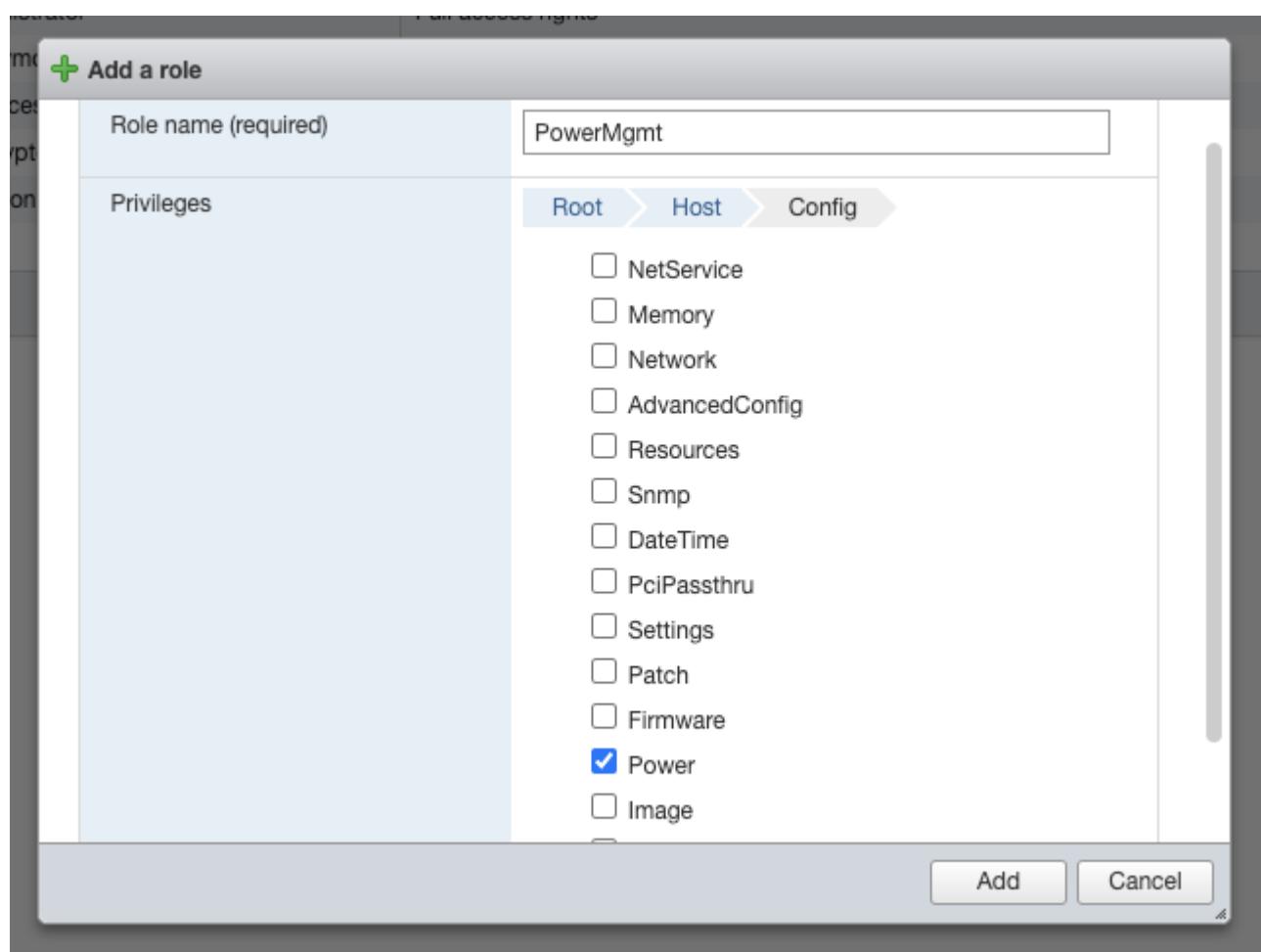


| Name | Summary |
|-------------------------------|---|
| Administrator | Full access rights |
| Anonymous | Not logged-in user (cannot be granted) |
| No access | Used for restricting granted access |
| No cryptography administrator | Full access without Cryptographic operations privileges |
| PowerMgmt | PowerMgmt |
| Read-only | See details of objects, but not make changes |
| View | Visibility access (cannot be granted) |

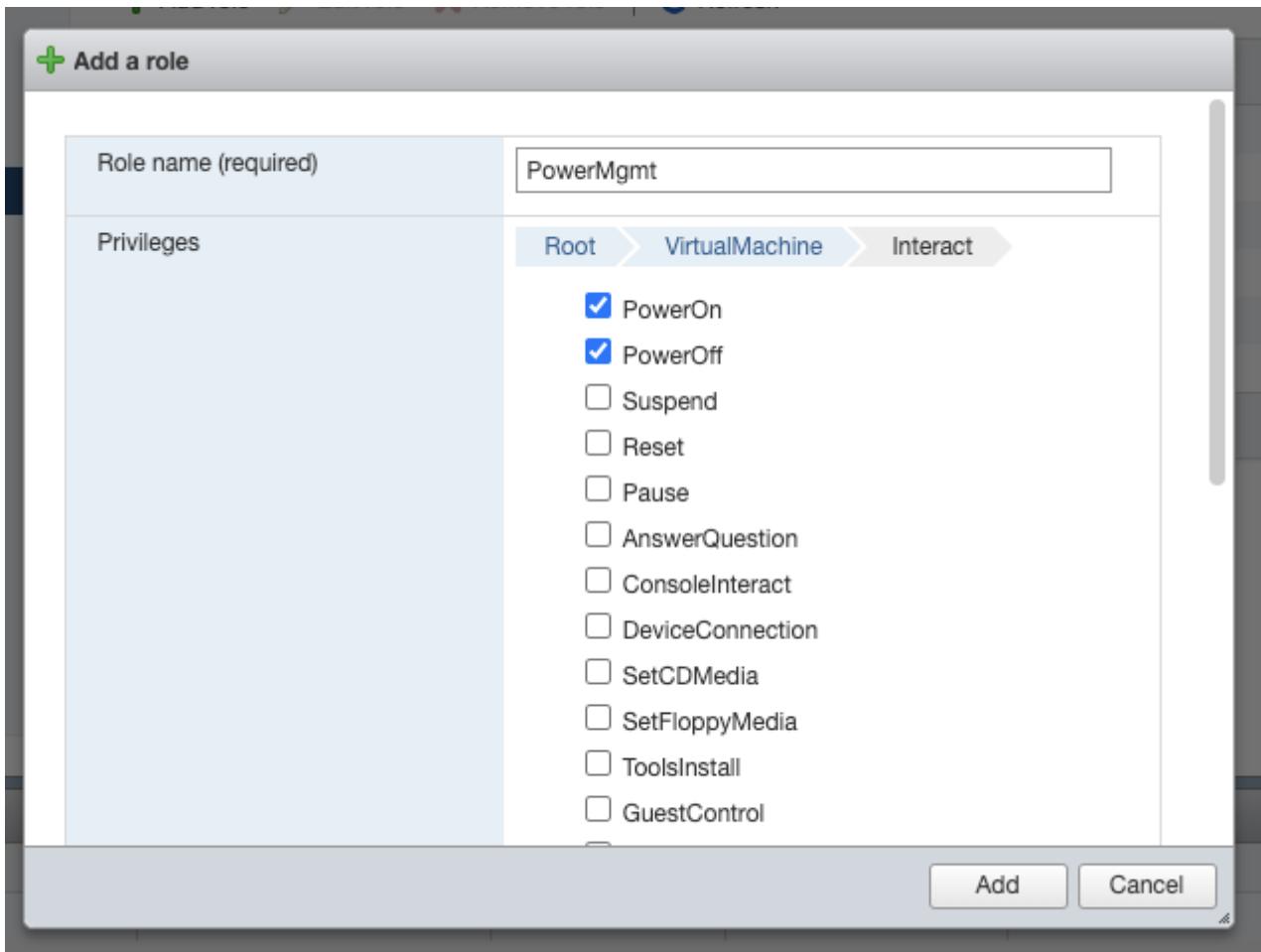
Click on Add Role. Give the new role a suggestive name, for example: PowerMgmt.

Choose the following from Privileges:

Root -> Host -> Config -> Power.



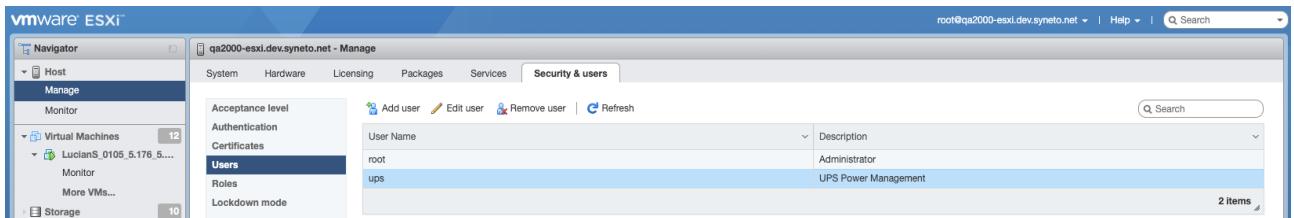
Root -> VirtualMachine -> Interact -> PowerOn, PowerOff



Click Add to create the new role.

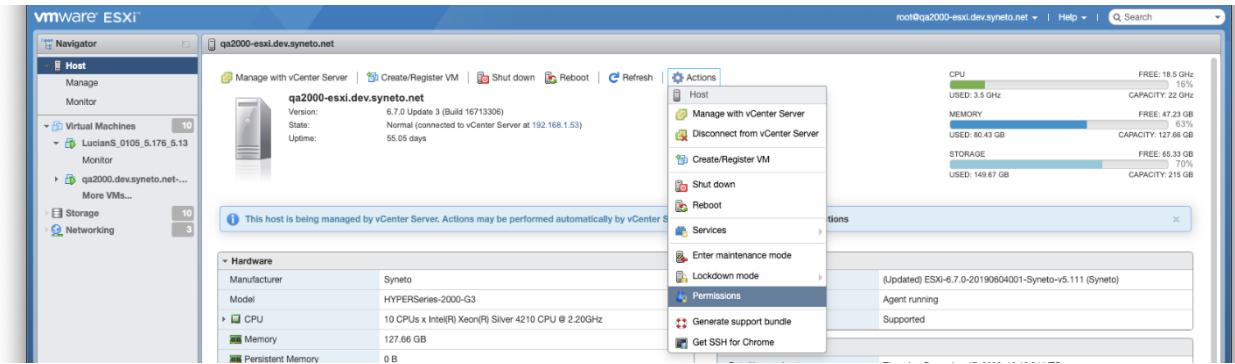
2. Create a new user.

Go to Host -> Manage -> Security & users -> Users. Click on Add user to create a new user. Call it for example ups.



3. Assign the role PowerMgmt to the newly created user ups on the ESXi host.

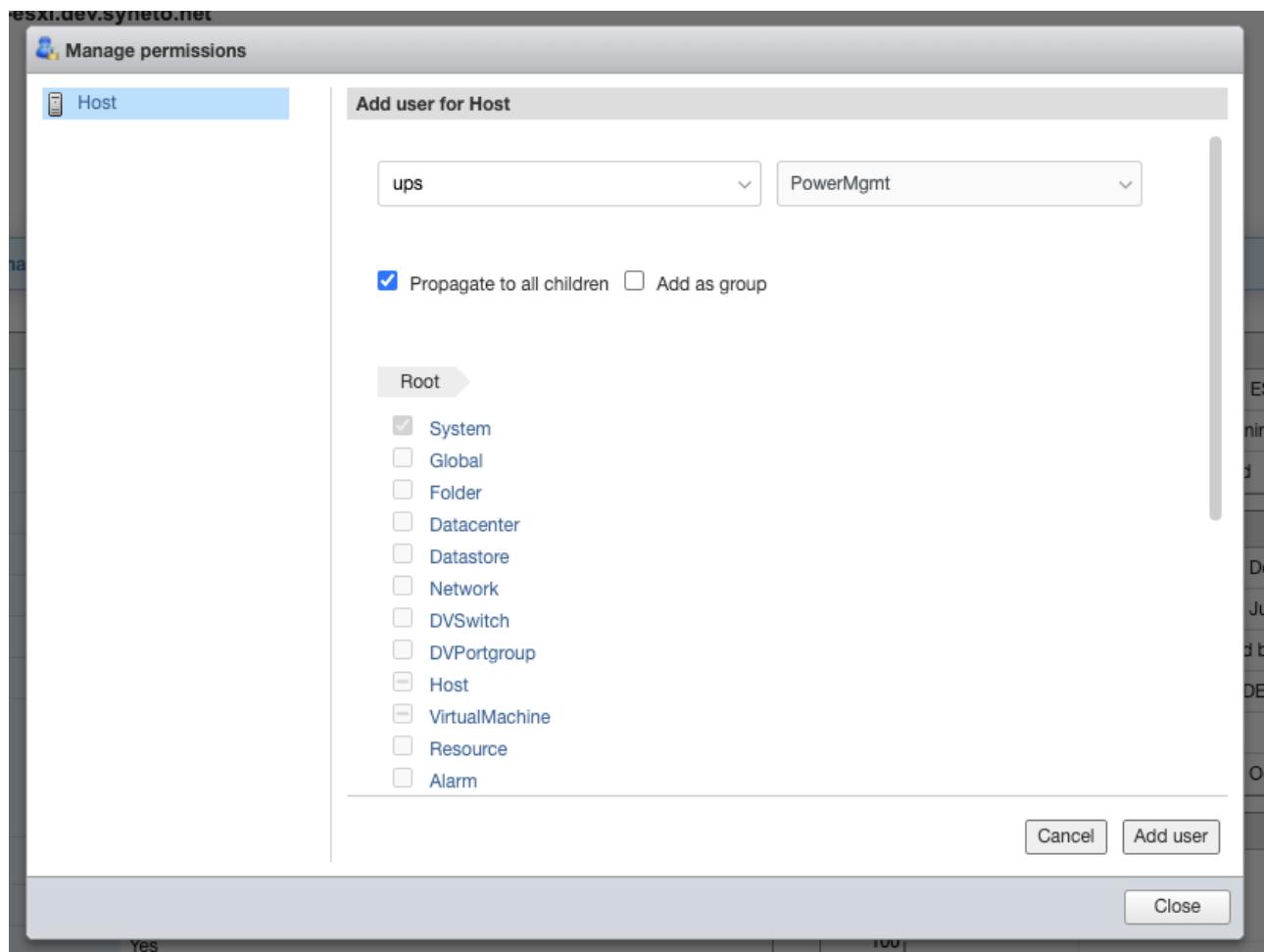
Go to Host -> Actions -> Permissions.



Click on Add user to assign the user and the role to the ESXi host.

| User | Role |
|---------|---------------|
| dcui | Administrator |
| root | Administrator |
| vpxuser | Administrator |

Type the username in the field, select the appropriate role for power management. For this example, *ups* and *PowerMgmt*.



Click Add user. You have now setup a user which can be used for power management on the ESXi host.

CONFIGURE NETMAN 208C FOR HOST SHUTDOWN

Connect to NetMan 208C via the web interface. Go to Configuration -> Remote Hosts -> Syneto

The screenshot shows the NetMan 208C configuration interface for 'REMOTE HOSTS' under the 'SYNETO' section. It includes sections for 'REMOTE HOSTS SHUTDOWN' (with a list of supported hosts like SSH, VMware ESXi, Nutanix, and Syneto), 'Infrastructure connectors' (empty table), 'Actions' (empty table), 'SHUTDOWN ON EVENT' (with a note about battery low and active shutdown, and a field for UPS shutdown delay), and two test buttons: 'DRY RUN' and 'VALIDATE'.

REMOTE HOSTS SHUTDOWN

- SSH
- VMware ESXi
- Nutanix
- Syneto**

Syneto

SYNETO

Enable Syneto shutdown

Infrastructure connectors

| ESXi Hypervisor | Username | Password |
|----------------------------|----------|----------|
| No data available in table | | |

Actions

| Action | Condition | Condition duration (min) | Delay next (sec) | Source | Restore on power on |
|----------------------------|-----------|--------------------------|------------------|--------|---------------------|
| No data available in table | | | | | |

SHUTDOWN ON EVENT

Additionally, the commands will be executed when on battery low condition and when shutdown is active

Then, UPS shutdown after (seconds)

SAVE

TEST SYNETO SHUTDOWN (PLEASE CLICK SAVE BEFORE TESTING)

DRY RUN

TEST SYNETO SERVER CREDENTIALS (PLEASE CLICK SAVE BEFORE TESTING)

VALIDATE

- Check the box for Enable Syneto shutdown

Syneto

| Field | Description | Default |
|------------------------|--------------------------------------|----------|
| Enable Syneto shutdown | Enable or disable the Syneto service | Disabled |

- In the section Infrastructure connectors, click on the Add Row button. You will connect NetMan 208C to the ESXi host.

- Enter the following:

| ESXi Hypervisor | The ip address of your ESXi host or Vcenter | Default |
|-----------------|---|-----------------|
| Username | The username you created for power management. e.g. "ups" when set | Not set / Empty |
| Password | The username you created for power management. e.g. "ups" when set | Not set / Empty |

- In the section Actions, click on the Add Row button. You will define the action to take on the ESXi host.

- Enter the following:

| Action: Shutdown host | Shutdown the host | Default |
|-------------------------------|---|-----------------|
| Condition: | <p>Power fail: When the UPS detects a main failure, the configured condition duration time(sec) will begin to countdown. Once the timer has elapsed the selected action will start. If the main returns within this time, then the action will be cancelled.</p> <p>Autonomy less: When the calculated battery autonomy of the UPS falls below the configured condition duration time(sec) the selected action will start. If main returns within this time, then the action will be cancelled.</p> | Not set / Empty |
| Condition duration (minutes): | <p>The duration that the selected condition (Power fail or Autonomy less) must be active for before the selected action starts.</p> <p>We recommend at least 15 minutes.</p> | Not set / Empty |

Actions

| Action | Condition | Condition duration (min) | Delay next (s) |
|---------------|---------------|--------------------------|----------------|
| 0 Shutdown VM | Autonomy less | 15 | |

Actions

| Delay next (sec) | Source | Target | Restore on power on |
|------------------|--------|--------|------------------------------|
| | | | <input type="checkbox"/> |

[Add Row](#)

SHUTDOWN ON EVENT

Additionally, the commands will be executed when on battery low condition and when shutdown is active

Then, UPS shutdown after (seconds)

120



[SAVE](#)

The device with NetMan 208C will shut down all virtual machines that are included in the AutoStart functionality in the inverse order: last virtual machine in the list will be shutdown first.

SHUTDOWN ON EVENT

| Field | Description | Default |
|------------------------------|---|-----------------|
| UPS shutdown after (seconds) | Delay for UPS shutdown after event occurs | Not set / Empty |
| Shutdown on event | Action of shutdown UPS after all previous actions | Disabled |

It is possible to configure the UPS shutdown delay in seconds, this counter will start after the shutdown actions listed on the Action list.

Additionally, the commands will be executed when on battery low condition and when shutdown is active.

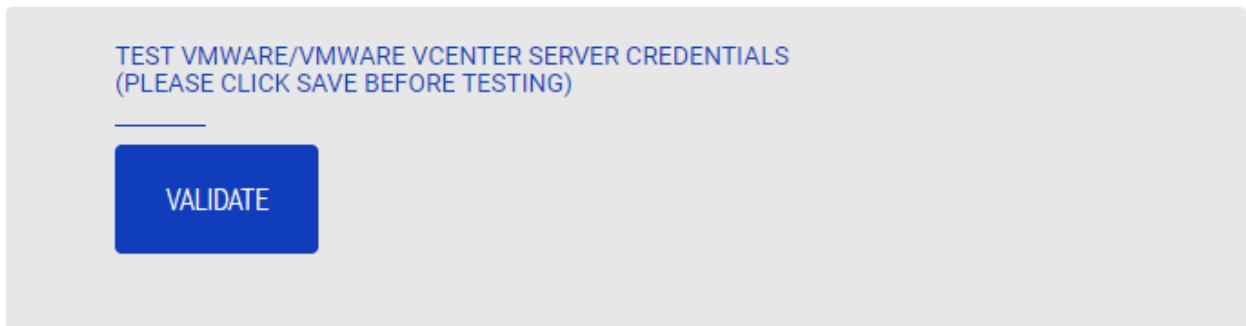
SAVE

This button SAVE the configuration, please note that the service will be restarted.



Testing the configuration

It is possible to test the procedure without performing a real shutdown by pressing "Dry Run". The logs on the target host or vCenter Server Appliance will confirm the correctness of the configuration.

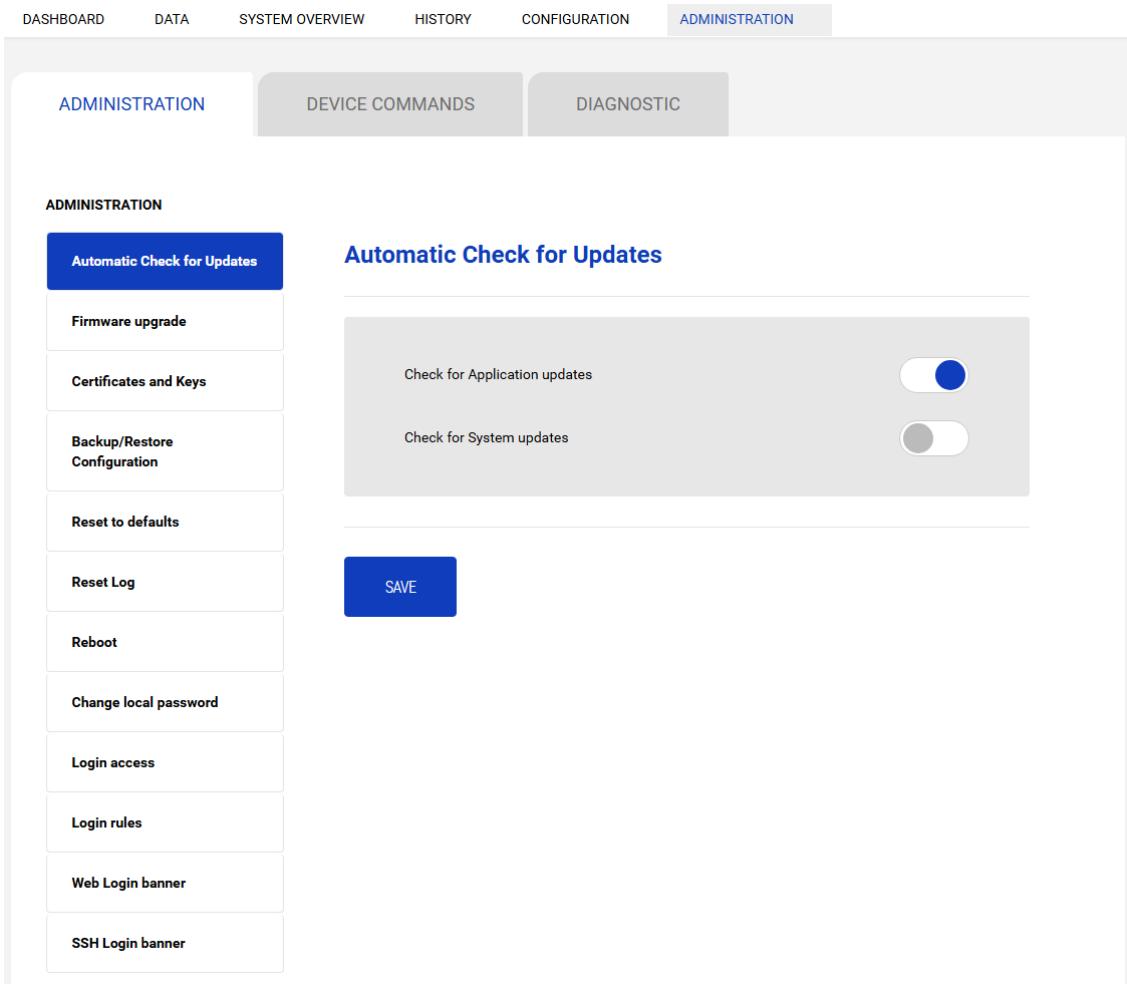


Validating the connections

It is also possible to test the correct user account and password to login on the VSphere VCSA. The test will return the result with a pop-up screen.

ADMINISTRATION

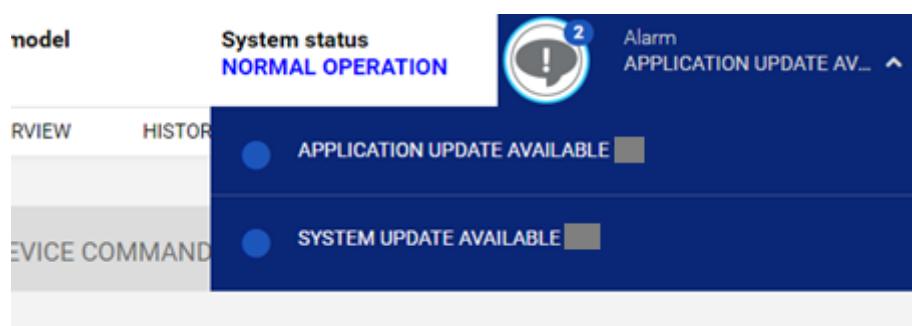
Automatic Check for Updates



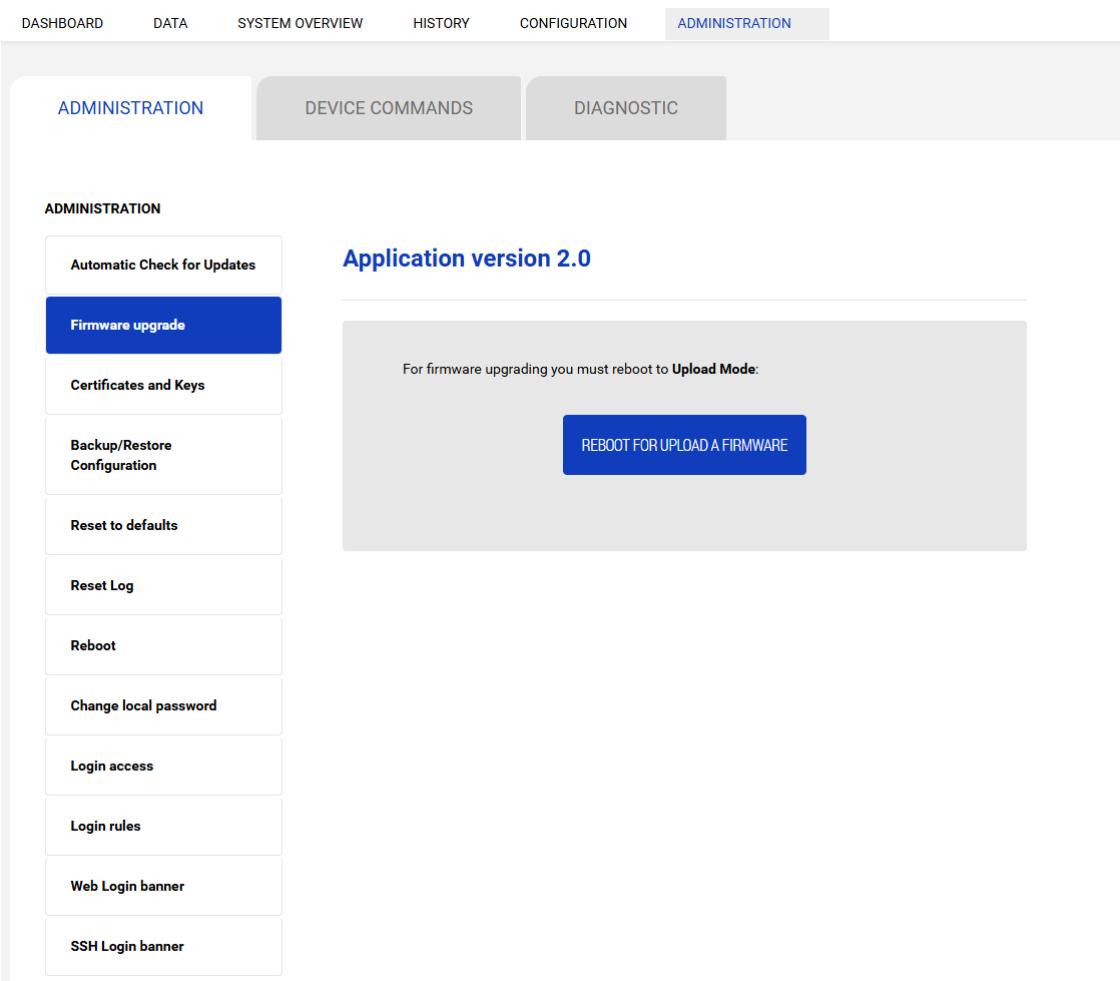
The screenshot shows the 'Automatic Check for Updates' configuration page. On the left, a sidebar lists various administration options: Firmware upgrade, Certificates and Keys, Backup/Restore Configuration, Reset to defaults, Reset Log, Reboot, Change local password, Login access, Login rules, Web Login banner, and SSH Login banner. The main panel is titled 'Automatic Check for Updates' and contains two toggle switches: 'Check for Application updates' (which is enabled, indicated by a blue switch) and 'Check for System updates' (which is disabled, indicated by a grey switch). At the bottom of the main panel is a 'SAVE' button.

| Field | Description | Default |
|-------------------------------|--------------------------------------|----------|
| Check for Application updates | Checks for APP (Application) updates | Enabled |
| Check for System updates | Checks for SYS (System) updates | Disabled |

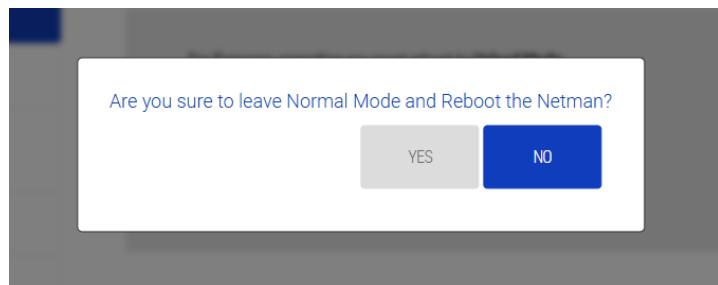
NetMan 208C automatically checks for updates available on the official server ONLINE. It is possible to check only for Application updates, for System updates or both. When an update is available, it is shown in the "Alarm" area.



Firmware upgrade



The screenshot shows the 'ADMINISTRATION' tab selected in the top navigation bar. Below it, the 'ADMINISTRATION' sub-tab is also selected. The main content area displays a sidebar with various administration options: 'Automatic Check for Updates', 'Firmware upgrade' (which is highlighted in blue), 'Certificates and Keys', 'Backup/Restore Configuration', 'Reset to defaults', 'Reset Log', 'Reboot', 'Change local password', 'Login access', 'Login rules', 'Web Login banner', and 'SSH Login banner'. To the right of the sidebar, the text 'Application version 2.0' is displayed. Below this, a message states 'For firmware upgrading you must reboot to **Upload Mode**'. A blue button labeled 'REBOOT FOR UPLOAD A FIRMWARE' is present. The entire interface is contained within a light gray box.



To upgrade the firmware, you must reboot NetMan 208C to **Upload Mode**.

Please follow the "**UPLOAD / MAINTENANCE MODE**" section instruction for executing operations as:

- upload firmware
- update firmware certificates
- change network compatibility
- other maintenance operations

Anytime, from "**UPLOAD / MAINTENANCE MODE**", it is always possible to reboot to "Normal Mode" to run NetMan 208C as normal usage.

Certificates

By default, NetMan 208C provides an HTTPS connection covered by an internal certificate that may be of two types:

| | |
|--------------------------------|--|
| signed by external CA | This HTTPS certificate can be verified by downloading the relative CA certificate from the manufacturer's web site and must be installed in the system/browser for a full trusted validation. |
| self-signed certificate | This HTTPS does not need external CA, it must be accepted. |

In both cases, the User can load and set:

- a **Custom certificate**
- a **CA certificate**

as optional for a more secure and customized HTTPS connection.

Before any configuration the User must load its certificates in the menu:

The screenshot shows the NetMan 208C Administration interface. The top navigation bar includes links for DASHBOARD, DATA, SYSTEM OVERVIEW, HISTORY, CONFIGURATION, and ADMINISTRATION. The ADMINISTRATION tab is selected, showing sub-links for ADMINISTRATION, DEVICE COMMANDS, and DIAGNOSTIC. The ADMINISTRATION section on the left contains links for Automatic Check for Updates, Firmware upgrade, Certificates and Keys (which is selected and highlighted in blue), Backup/Restore Configuration, Reset to defaults, Reset Log, Reboot, Change local password, Login access, Login rules, Web Login banner, and SSH Login banner. The main content area is divided into three sections: Certificates, Keys, and Jks (KeyStore). The Certificates section displays a message about HTTPS and EAP 802.1x, a 'No certificate available' message, a 'VIEW CERTIFICATE' button, a 'DELETE CERTIFICATE' button, and a 'UPLOAD NEW CERTIFICATE' button. The Keys section displays a message about EAP 802.1x, a 'No key available' message, a 'VIEW KEY' button, a 'DELETE KEY' button, and a 'UPLOAD NEW KEY' button. The Jks (KeyStore) section displays a message about LDAP, a 'No jks keystore available' message, a 'DELETE KEYSTORE JKS' button, and a 'UPLOAD NEW KEYSTORE JKS' button.

The only permitted operations are:

| | Certificate file | Key file | Jks File |
|---|---------------------|-------------|-------------|
| upload into NetMan 208C | ✓ | ✓ | ✓ |
| view from NetMan 208C | ✓ | ✓ | ✗ |
| delete from NetMan 208C | ✓ | ✓ | ✓ |
| Extraction/download from NetMan 208C | ✗ | ✗ | ✗ |

📄 Certificates

Certificates may be requested by **HTTPS** (CUSTOM-WEB-SERVER certificates and CA certificates) and **EAP 802.1x**.

Certificates must meet certain requirements:

📄 **Custom certificate:**

- generated as PEM file (base64 format)
- File extension **.pem**
- Generated from CA Authority as "Web Server" and joined with its "Private Key"

📄 **CA certificate:**

- generated as PEM file (base64 format)
- File extension **.pem**
- downloaded from the CA Authority

For deeper explanation, please check for the section "Certificate generation" in Appendix

🔑 Keys

Keys may be requested by **EAP 802.1x**.

Keys are used only for IEEE 802.1x / EAP.

The file format is:

- Generated from standard **openssl** command using a *password* for secret
- File extension (suggested): **.key**

Jks (KeyStore)

Jks Keystores may be requested by **LDAP**.

Jks is a certificate-bundle used only from LDAP configuration.

The file format is:

- File extension (mandatory): “**.jks**”
- obtained from a chained process using first standard **openssl** and then **keytool**

Please check the LDAP section and the Appendix section for more details about generating **.jks** certificates for LDAP both manually and with request automation.

Backup/Restore Configuration

Backup/Restore configuration menu allows the user to keep a save of NetMan 208C configuration as external file, ready to be uploaded again to restore part of, or the entire, configuration.

The screenshot shows the 'ADMINISTRATION' tab selected in the top navigation bar. Under 'ADMINISTRATION', the 'Backup/Restore Configuration' option is highlighted in blue. The main content area is titled 'Restore Configuration' with a sub-instruction: 'Click the button and select the configuration file to Restore'. A blue button labeled 'RESTORE FROM FILE' with a file icon is present. Below it, a note states: 'It is possible to restore the *Common configuration* or the *Complete configuration* saved before.' The 'Backup Configuration' section contains two options: 'BACKUP COMMON CONFIGURATION' and 'BACKUP COMPLETE CONFIGURATION', each with a blue button labeled 'BACKUP COMMON CONFIGURATION' or 'BACKUP COMPLETE CONFIGURATION' with a file icon. Descriptions for each are provided: 'Save this file for a backup of the common configuration parameters; it can be used to restore or copy the **common parameters** to **this or other Netman 208 cards**' for the common backup, and 'Save this file for a full backup of **this Netman 208**; this backup can restore the **full configuration** only for **this Netman 208** (and not for others)' for the complete backup.

The configuration can be saved as:

| | |
|---|---|
| COMMON configuration: ⬇ BACKUP COMMON CONFIGURATION | COMMON CONFIGURATION can be RESTORED later to other NetMan 208C setting all the non-confidential data, functionalities and settings; this operation allows you to quickly configure basic common settings to other NetMan 208C at once. |
| COMPLETE configuration: ⬇ BACKUP COMPLETE CONFIGURATION | COMPLETE CONFIGURATION can be RESTORED later only from this NetMan 208C (not for others) allowing a full restore of the whole configuration including all network, confidential data, critical and customized parameters. <i>Note: for future RESTORE configuration from COMPLETE take note of the Hostname and the network IP address and network set.</i> <i>Note: this COMPLETE CONFIGURATION can be restored only from this NetMan 208C and not from others.</i> |

Both type of backups are encrypted and signed ensuring confidentiality.

Once a configuration is saved as a backup file, it can be easily restored from the button:

| | |
|---|--|
| <p>RESTORE configuration</p> <div style="background-color: #0070C0; color: white; padding: 5px; border-radius: 5px; text-align: center; width: fit-content; margin: auto;"> ↑ RESTORE FROM FILE </div> | <p>It will manage the file and proceed to RESTORE the expected parameters.</p> <p>After RESTORE operation please proceed to a REBOOT of NetMan 208C.</p> <p>!!! When a COMPLETE configuration is restored please remember that the network configuration (IP, hostname, ...) may be changed (due to the restored) and the last known connection can be lost.</p> |
|---|--|

The full details of the COMMON and COMPLETE restore parameters are available in this table:

| | Restore COMMON | Restore COMPLETE |
|----------------------------|------------------------|------------------|
| LOCAL USER ACCESSES | | |
| admin | IGNORED - PASSWORD (*) | RESTORED |
| power | IGNORED - PASSWORD (*) | RESTORED |
| view | IGNORED - PASSWORD (*) | RESTORED |

| ACTIVE SERVICES | | |
|------------------------|---|---|
| SSH admin | IGNORED - PASSWORD (*) | RESTORED |
| SNMP | RESTORED WITHOUT PASSWORD (*) | RESTORED |
| SYSLOG | RESTORED | RESTORED |
| Email | RESTORED WITHOUT PASSWORD (*) | RESTORED |
| BACNET | RESTORED | RESTORED |
| Modbus | RESTORED | RESTORED |
| SENSORI | RESTORED | RESTORED |
| DATALOG | RESTORED | RESTORED |
| Firewall | RESTORED | RESTORED |
| Wake on LAN | RESTORED | RESTORED |
| JSON | RESTORED WITHOUT CUSTOM LICENSE (**) | RESTORED (WITH ITS CUSTOM LICENSE IF USED) |

| WEB CONFIGURATION | | |
|--|--------------------------------|----------|
| CONFIGURATION - General configuration | | |
| PRTK Code | IGNORED - OTHER SECRETS (****) | RESTORED |
| Name | IGNORED - OTHER SECRETS (****) | RESTORED |
| P/N | IGNORED - OTHER SECRETS (****) | RESTORED |
| S/N | IGNORED - OTHER SECRETS (****) | RESTORED |
| Contact | IGNORED - OTHER SECRETS (****) | RESTORED |
| Location | IGNORED - OTHER SECRETS (****) | RESTORED |
| Battery Replacement | IGNORED - OTHER SECRETS (****) | RESTORED |

| CONFIGURATION - Command configuration | | |
|---|--------------------------|----------|
| Disable remote shutdown | RESTORED | RESTORED |
| Disable remote commands | RESTORED | RESTORED |
| CONFIGURATION - Data Log configuration | | |
| Enable Data Log | RESTORED | RESTORED |
| CONFIGURATION - NETWORK - Configuration | | |
| Hostname | IGNORED - NETWORK (****) | RESTORED |
| Network protocol | IGNORED - NETWORK (****) | RESTORED |
| IP | IGNORED - NETWORK (****) | RESTORED |
| Netmask | IGNORED - NETWORK (****) | RESTORED |
| Gateway | IGNORED - NETWORK (****) | RESTORED |
| Primary DNS | IGNORED - NETWORK (****) | RESTORED |
| Secondary DNS | IGNORED - NETWORK (****) | RESTORED |
| 802.1x on IPv4 | RESTORED | RESTORED |
| 802.1x - Authentication method | RESTORED | RESTORED |
| 802.1x - Identity | RESTORED | RESTORED |
| 802.1x - Password | IGNORED - PASSWORD (*) | RESTORED |
| IPv6 | RESTORED | RESTORED |
| Stateless | RESTORED | RESTORED |
| Privacy Extension | RESTORED | RESTORED |
| Serial Network Tunneling | RESTORED | RESTORED |
| UDP - Enabled | RESTORED | RESTORED |
| UDP - Port | RESTORED | RESTORED |
| UDP - Password | IGNORED - PASSWORD (*) | RESTORED |
| CONFIGURATION - NETWORK - Firewall | | |
| Enable Firewall Rules | RESTORED | RESTORED |
| Rule - Enabled | RESTORED | RESTORED |
| Rule - From IP address | RESTORED | RESTORED |
| Rule - IP address | RESTORED | RESTORED |
| Rule - Action | RESTORED | RESTORED |
| Default incoming rule | RESTORED | RESTORED |
| CONFIGURATION - NETWORK - Wake on LAN | | |
| Enable Wake On Lan | RESTORED | RESTORED |
| Mac address | RESTORED | RESTORED |
| CONFIGURATION - NETWORK - SNMP | | |
| Enable SNMP protocol | RESTORED | RESTORED |
| Versione | RESTORED | RESTORED |
| v3 User | RESTORED | RESTORED |
| v3 Auth | RESTORED | RESTORED |
| v3 Priv | RESTORED | RESTORED |
| v3 authPassword | IGNORED - PASSWORD (*) | RESTORED |
| v3 privPassword | IGNORED - PASSWORD (*) | RESTORED |
| v3 permissions | RESTORED | RESTORED |
| Trap receiver | RESTORED | RESTORED |
| Trap repeater | RESTORED | RESTORED |
| CONFIGURATION - NETWORK - MODBUS/BACNET | | |
| Enable MODBUS | RESTORED | RESTORED |

| | | |
|---|------------------------|----------|
| Enable BACNET | RESTORED | RESTORED |
| BACNET Address (Number) | RESTORED | RESTORED |
| CONFIGURATION - NETWORK - JSON | | |
| Enable JSON notification | RESTORED | RESTORED |
| Monitoring host IP | RESTORED | RESTORED |
| Host port | RESTORED | RESTORED |
| Notification interval (minutes) | RESTORED | RESTORED |
| Send notification on event | RESTORED | RESTORED |
| License file | IGNORED - LICENSE (**) | RESTORED |
| CONFIGURATION - NETWORK - SYSLOG | | |
| Enable remote SYSLOG | RESTORED | RESTORED |
| SYSLOG server IP | RESTORED | RESTORED |
| Server UDP port | RESTORED | RESTORED |
| CONFIGURATION - DATE & TIME - NTP & Timezone | | |
| Select the right timezone | RESTORED | RESTORED |
| NTP server address (IP) | RESTORED | RESTORED |
| CONFIGURATION - DATE & TIME - Configuration | | |
| Date | RESTORED | RESTORED |
| Hour | RESTORED | RESTORED |
| Minutes | RESTORED | RESTORED |
| CONFIGURATION - NETWORK - EMAILS | | |
| Enable Email | RESTORED | RESTORED |
| Mail host | RESTORED | RESTORED |
| SMTP port | RESTORED | RESTORED |
| Sender address | RESTORED | RESTORED |
| Transport | RESTORED | RESTORED |
| Username | RESTORED | RESTORED |
| Password | IGNORED - PASSWORD (*) | RESTORED |
| Email #1 | RESTORED | RESTORED |
| Flags | RESTORED | RESTORED |
| Send report every day at 00:10 | RESTORED | RESTORED |
| Send report every Sunday at 00:10 | RESTORED | RESTORED |
| CONFIGURATION - SENSORS | | |
| Enable sensors | RESTORED | RESTORED |
| Sensor #1 | RESTORED | RESTORED |
| Sensor #2 | RESTORED | RESTORED |
| Sensor #3 | RESTORED | RESTORED |
| Sensor labels - Sensor 1 description | RESTORED | RESTORED |
| Sensor labels - Input 1 | RESTORED | RESTORED |
| Sensor labels - Output 1 | RESTORED | RESTORED |
| Sensor labels - Sensor 2 description | RESTORED | RESTORED |
| Sensor labels - Input 2 | RESTORED | RESTORED |
| Sensor labels - Output 2 | RESTORED | RESTORED |
| Sensor labels - Sensor 3 description | RESTORED | RESTORED |
| Sensor labels - Input 3 | RESTORED | RESTORED |
| Sensor labels - Output 3 | RESTORED | RESTORED |
| Sensor Logic | RESTORED | RESTORED |

| | | |
|---|------------------------|----------|
| Device event - Output contact | RESTORED | RESTORED |
| Sensor event - Output contact | RESTORED | RESTORED |
| Sensors threshold - Temperature high | RESTORED | RESTORED |
| Sensors threshold - Temperature low | RESTORED | RESTORED |
| Sensors threshold - Temperature hysteresis | RESTORED | RESTORED |
| Sensors threshold - Humidity high | RESTORED | RESTORED |
| Sensors threshold - Humidity low | RESTORED | RESTORED |
| Sensors threshold - Humidity hysteresis | RESTORED | RESTORED |
| CONFIGURATION - MODEM | | |
| Enable SMS | RESTORED | RESTORED |
| SMSC Short Message Service Center number: | RESTORED | RESTORED |
| SMS #1 | RESTORED | RESTORED |
| Flags | RESTORED | RESTORED |
| Send report every day | RESTORED | RESTORED |
| Send report every week | RESTORED | RESTORED |
| CONFIGURATION - REMOTE HOST - SSH | | |
| Enable remote SSH commands | RESTORED | RESTORED |
| Run first script on event - After mains failure (minutes) | RESTORED | RESTORED |
| Run first script on event - When authonomy is below (minutes) | RESTORED | RESTORED |
| Connectors and Scripts | | |
| Enabled | RESTORED | RESTORED |
| Host | RESTORED | RESTORED |
| Username | RESTORED | RESTORED |
| Password | IGNORED - PASSWORD (*) | RESTORED |
| Script | RESTORED | RESTORED |
| Delay next (sec) | RESTORED | RESTORED |
| Shutdown on event | | |
| Shutdown on event | RESTORED | RESTORED |
| CONFIGURATION - REMOTE HOST - VMWARE | | |
| Enable VMware ESXi shutdown | RESTORED | RESTORED |
| Infrastructure connectors | | |
| Host or VCSA | RESTORED | RESTORED |
| Username | RESTORED | RESTORED |
| Password | IGNORED - PASSWORD (*) | RESTORED |
| Actions | | |
| Action | RESTORED | RESTORED |
| Condition | RESTORED | RESTORED |
| Condition duration (min) | RESTORED | RESTORED |
| Delay next (sec) | RESTORED | RESTORED |
| Source | RESTORED | RESTORED |
| Target | RESTORED | RESTORED |
| Restore on power on | RESTORED | RESTORED |
| Target Netman | RESTORED | RESTORED |
| Shutdown on event | | |
| Then, UPS shutdown after (seconds) | RESTORED | RESTORED |

| CONFIGURATION - REMOTE HOST - NUTANIX | | |
|--|-------------------------------|----------|
| Enable Nutanix shutdown | RESTORED | RESTORED |
| CVM credentials | | |
| Prism address | RESTORED | RESTORED |
| Prism user | RESTORED | RESTORED |
| Prism password | IGNORED - PASSWORD (*) | RESTORED |
| Physical hosts | | |
| Host | RESTORED | RESTORED |
| Username | RESTORED | RESTORED |
| Password | IGNORED - PASSWORD (*) | RESTORED |
| Actions | | |
| Action | RESTORED | RESTORED |
| Condition | RESTORED | RESTORED |
| Condition duration (min) | RESTORED | RESTORED |
| Delay next (sec) | RESTORED | RESTORED |
| Source | RESTORED | RESTORED |
| Restore on power on | RESTORED | RESTORED |
| Shutdown on event | | |
| Then, UPS shutdown after (seconds) | RESTORED | RESTORED |
| CONFIGURATION - REMOTE HOST - SYNETO | | |
| Enable Syneto shutdown | RESTORED | RESTORED |
| ESXi Hypervisor | RESTORED | RESTORED |
| Username | RESTORED | RESTORED |
| Password | IGNORED - PASSWORD (*) | RESTORED |
| Actions | | |
| Action | RESTORED | RESTORED |
| Condition | RESTORED | RESTORED |
| Condition duration (min) | RESTORED | RESTORED |
| Delay next (sec) | RESTORED | RESTORED |
| Source | RESTORED | RESTORED |
| Restore on power on | RESTORED | RESTORED |
| Shutdown on event | | |
| Then, UPS shutdown after (seconds) | RESTORED | RESTORED |
| ADMINISTRATION - Check for Updates | | |
| Check for Application updates | RESTORED | RESTORED |
| Check for System updates | RESTORED | RESTORED |
| ADMINISTRATION - Certificates & Keys | | |
| Certificates | IGNORED - OTHER SECRETS (***) | RESTORED |
| Keys | IGNORED - OTHER SECRETS (***) | RESTORED |
| Jks | IGNORED - OTHER SECRETS (***) | RESTORED |
| ADMINISTRATION - Change local password | | |
| Admin user | RESTORED | RESTORED |
| Power user | IGNORED - OTHER SECRETS (***) | RESTORED |
| View user | IGNORED - OTHER SECRETS (***) | RESTORED |
| Password complexity | RESTORED | RESTORED |
| ADMINISTRATION - Login access | | |
| Enable Auto Logout | RESTORED | RESTORED |

| | | |
|--|--------------------------------|----------|
| Auto Logout due to user inactivity after (seconds) | RESTORED | RESTORED |
| Auto Logout Warning message when are left | RESTORED | RESTORED |
| Enable SSH | RESTORED | RESTORED |
| HTTP | RESTORED | RESTORED |
| HTTP port | RESTORED | RESTORED |
| HTTPS | RESTORED | RESTORED |
| HTTPS port | RESTORED | RESTORED |
| Custom Cert: | IGNORED - OTHER SECRETS (****) | RESTORED |
| CA Cert: | IGNORED - OTHER SECRETS (****) | RESTORED |
| Enable Local authentication | RESTORED | RESTORED |
| Enable AD/LDAP authentication | RESTORED | RESTORED |
| LDAP | RESTORED | RESTORED |
| LDAP - Passwords | IGNORED - PASSWORD (*) | RESTORED |
| ADMINISTRATION - Login rules | | |
| Login retry max | RESTORED | RESTORED |
| Login min interval before retry | RESTORED | RESTORED |
| ADMINISTRATION - Web Login Banner | | |
| Show Pre-Login banner | IGNORED - OTHER SECRETS (****) | RESTORED |
| Title | IGNORED - OTHER SECRETS (****) | RESTORED |
| Message | IGNORED - OTHER SECRETS (****) | RESTORED |
| Show Post-Login ADMIN banner | IGNORED - OTHER SECRETS (****) | RESTORED |
| Title | IGNORED - OTHER SECRETS (****) | RESTORED |
| Message | IGNORED - OTHER SECRETS (****) | RESTORED |
| Show Post-Login POWER banner | IGNORED - OTHER SECRETS (****) | RESTORED |
| Title | IGNORED - OTHER SECRETS (****) | RESTORED |
| Message | IGNORED - OTHER SECRETS (****) | RESTORED |
| Show Post-Login VIEW banner | IGNORED - OTHER SECRETS (****) | RESTORED |
| Title | IGNORED - OTHER SECRETS (****) | RESTORED |
| Message | IGNORED - OTHER SECRETS (****) | RESTORED |
| ADMINISTRATION - SSH Login Banner | | |
| Show Pre-Login banner | IGNORED - OTHER SECRETS (****) | RESTORED |
| Message | IGNORED - OTHER SECRETS (****) | RESTORED |

Notes:

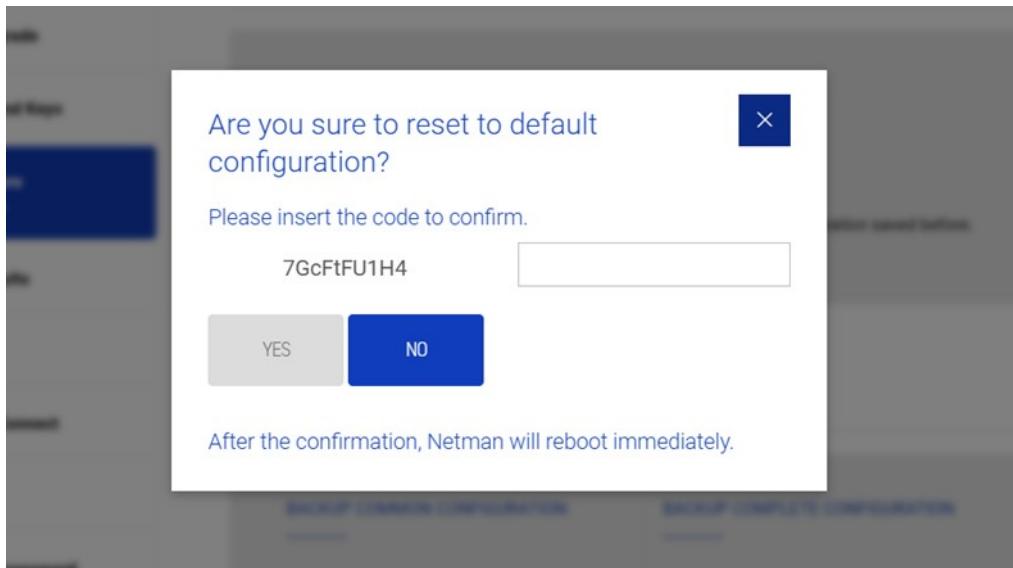
(*) IGNORED because PASSWORDS are not RESTORED from COMMON configuration

(**) IGNORED because SENSIBLE CUSTOM DATA is not RESTORED from COMMON configuration

(***) IGNORED because OTHER SECRETS are not RESTORED from COMMON configuration

(****) IGNORED because NETWORK CONFIGURATION is not RESTORED from COMMON configuration

Reset to defaults



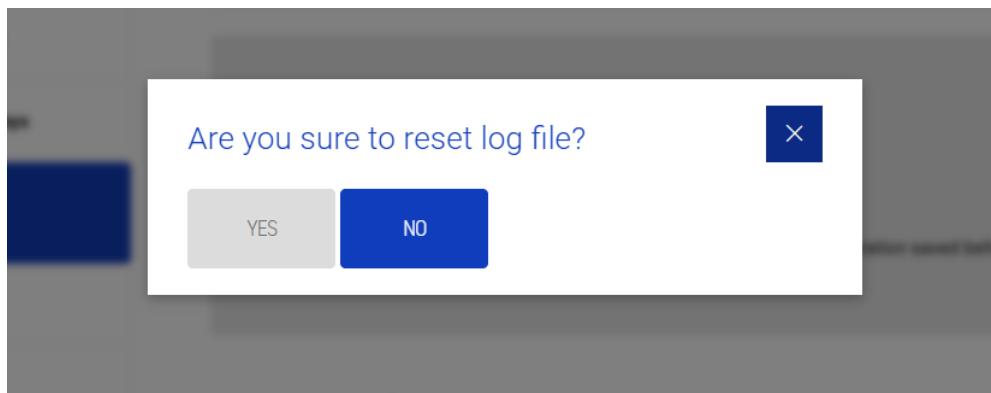
By writing the security code reported, NetMan 208C will reset to the default configuration.



Operation strongly suggested in case of decommissioning NetMan 208C.

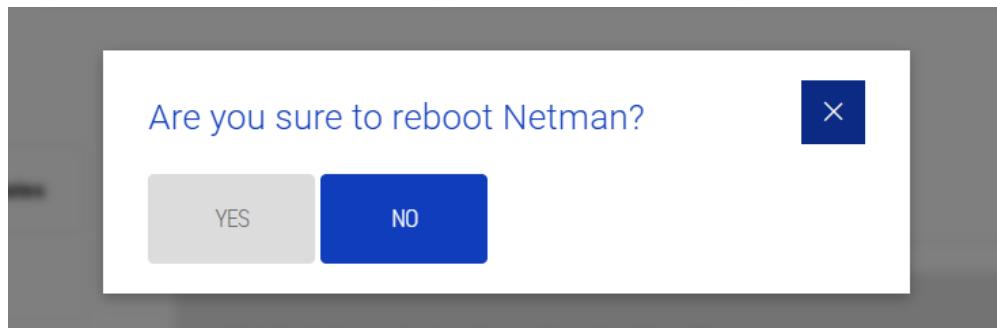
Reset Log

To reset all the log files of NetMan 208C.



Reboot

To reboot NetMan 208C.



Change local password

DASHBOARD DATA SYSTEM OVERVIEW HISTORY CONFIGURATION ADMINISTRATION

ADMINISTRATION DEVICE COMMANDS DIAGNOSTIC

ADMINISTRATION

- Automatic Check for Updates
- Firmware upgrade
- Certificates and Keys
- Backup/Restore Configuration
- Reset to defaults
- Reset Log
- Reboot
- Change local password**
- Login access
- Login rules
- Web Login banner
- SSH Login banner

Change local password

ADMIN USER

Admin credentials grant the right to manage Netman and also the device, including shutdown

Password  Retype Password 

 **SAVE**

POWER USER

Power credentials grant the right to manage Netman but may not full operate the device

Local **power** user is not enabled.
Please set a password for enable it.

Functions:

- A - General info (always active)
- B - Detail info
- C - Network status
- D - View/Download logs
- E - Service Log download
- F - Ups config
- G - Ups command config
- H - Ups command execution
- I - System/Network config
- J - Services/Functionalities config
- K - Advanced config
- M - Reboot

SAVE

VIEW USER

Password

View credentials grant the right to only view some values of the Netman (no action is possible)

Retype Password

Local **view** user is not enabled.
Please set a password for enable it.

Functions:

- A - General info (*always active*)
- B - Detail info
- C - Network status
- D - View/Download logs
- E - Service Log download
- H - Ups command execution
- M - Reboot

Password complexity

RULES

Min password length

chars

Max password length

chars

Min Lowercase chars requested
(**a,b,c,...,z**)

chars

Min Uppercase chars requested
(**A,B,C,...,Z**)

chars

Min digit chars requested
(**0-9**)

chars

Min special chars requested
(**, . _ + : @ % -**)

chars

To change local user “admin”, “power” and “view” passwords. By default, only “admin” user is available. Local users “power” and “view” must be activated by the “admin” user setting their password.

The password must meet the following requirements:

| | | |
|---|-------------|-------------------------|
| Min password length: | 0..40 chars | (<i>default = 8</i>) |
| Max password length: | 0..40 chars | (<i>default = 40</i>) |
| Min Lowercase chars requested (a,b,c,...,z): | 0..10 chars | (<i>default = 1</i>) |
| Min Uppercase chars requested (A,B,C,...,Z): | 0..10 chars | (<i>default = 1</i>) |
| Min digit chars requested (0-9): | 0..10 chars | (<i>default = 1</i>) |
| Min special chars requested (, . _ + : @ % -): | 0..10 chars | (<i>default = 1</i>) |

Functions:

the type of operations permitted and assignable to the users of NetMan 208C.

| | | |
|--------------|---|--|
| admin | local user “admin” LDAP users with “admin” profile | Can execute any operation on NetMan 208C. |
| power | local user “power” LDAP users with “power” profile | By default, starts with basic operations permitted. Can be customized adding other functionalities. |
| view | local user “admin” LDAP users with “view” profile | By default, starts with basic operations permitted. Can be customized adding a few limited functionalities. |

Complete function description map is available in this table:

Functions assignable to the users are listed in the table:

| | Admin | Power | View |
|-------------------------------------|--------------|--------------|-------------|
| A - General info | ✓ | ✓ | ✓ |
| B - Detail info | ✓ | ○ | ○ |
| C - Show network status | ✓ | ○ | ○ |
| D - View/Download logs | ✓ | ○ | ○ |
| E - Service Log download | ✓ | ○ | ○ |
| F - Ups config | ✓ | ○ | ✗ |
| G - Ups command config | ✓ | ○ | ✗ |
| H - Ups command execution | ✓ | ○ | ○ |
| I - System/Network config | ✓ | ○ | ✗ |
| J - Services/Functionalities config | ✓ | ○ | ✗ |
| K - Advanced config | ✓ | ○ | ✗ |
| L - Users config | ✓ | ✗ | ✗ |
| M - Reboot | ✓ | ○ | ○ |

| | |
|---|-------------------------|
| ✓ | Enabled |
| ○ | Optional |
| ✗ | Denied (not accessible) |

The menu in the Web are related to the functions in this list; just find which menu is needed and find the role necessary for its usage:

| DASHBOARD | |
|------------------------|-------------------------|
| show DASHBOARD diagram | A - General info |
| show SENSOR data | B - Detail info |
| show EVENTS data | B - Detail info |

| DATA | |
|-----------------|-------------------------|
| show UPS values | A - General info |

| SYSTEM OVERVIEW | |
|---------------------------|---------------------------------|
| show UPS DEVICE data | A - General info |
| show DEVICE configuration | A - General info |
| download SERVICE LOG | E - Service Log download |
| show NETWORK CARD data | C - Show network status |

| | |
|----------------------------|-------------------------|
| show NETWORK CONFIGURATION | C - Show network status |
| allow READ MANUAL | A - General info |
| allow LEGAL INFORMATION | A - General info |

| HISTORY | |
|--------------------|------------------------|
| event log FILTER | D - View/Download logs |
| event log LOAD | D - View/Download logs |
| event log DOWNLOAD | D - View/Download logs |
| datalog FILTER | D - View/Download logs |
| datalog LOAD | D - View/Download logs |
| datalog DOWNLOAD | D - View/Download logs |

| CONFIGURATION | |
|--|-------------------------------------|
| #YOUR NETMAN | |
| DEVICE - General configuration | F - Ups config |
| DEVICE - Command configuration | G - Ups command config |
| DEVICE - Data Log configuration | F - Ups config |
| NETWORK - Configuration - IPv4 configuration | I - System/Network config |
| NETWORK - Configuration - 802.1x configuration | I - System/Network config |
| NETWORK - Configuration - IPv6 configuration | I - System/Network config |
| NETWORK - Configuration - Serial Network Tunneling | I - System/Network config |
| NETWORK - Configuration - UDP configuration | I - System/Network config |
| Connectivity - Internet Connectivity check | C - Show network status |
| Connectivity - Check Ping | C - Show network status |
| Connectivity - Active Network Connections | C - Show network status |
| Firewall - Firewall configuration | I - System/Network config |
| Firewall - TEST action | I - System/Network config |
| Firewall - CONFIRM action | I - System/Network config |
| Wake On Lan configuration | J - Services/Functionalities config |
| SNMP - SNMP configuration | J - Services/Functionalities config |
| SNMP - SNMP test trap | J - Services/Functionalities config |
| Modbus/Bacnet configuration | J - Services/Functionalities config |
| JSON configuration | J - Services/Functionalities config |
| SYSLOG configuration | J - Services/Functionalities config |
| SYSLOG test connection | J - Services/Functionalities config |
| DATE & TIME - NTP & Timezone configuration | I - System/Network config |
| DATE & TIME - Date & Time configuration | I - System/Network config |
| EMAILS - EMAIL configuration | J - Services/Functionalities config |
| EMAILS - EMAIL test | J - Services/Functionalities config |
| ADVANCED - Expert Shell - GET parameter | K - Advanced config |
| ADVANCED - Expert Shell - SET parameter | K - Advanced config |
| ADVANCED - Expert Shell - DELETE parameter | K - Advanced config |

| #SENSORS | |
|----------------------|-------------------------------------|
| SENSOR activation | J - Services/Functionalities config |
| SENSOR scanning | J - Services/Functionalities config |
| SENSOR configuration | J - Services/Functionalities config |

| #MODEM | |
|---------------------|---------------------------|
| MODEM configuration | I - System/Network config |
| MODEM test | I - System/Network config |

| #REMOTE HOSTS | |
|-----------------------|---------------------------|
| SSH configuration | I - System/Network config |
| SSH test | I - System/Network config |
| VMware configuration | I - System/Network config |
| VMware dryrun | I - System/Network config |
| VMware validate | I - System/Network config |
| Nutanix configuration | I - System/Network config |
| Nutanix dry run | I - System/Network config |
| Nutanix validate | I - System/Network config |
| Syneto configuration | I - System/Network config |
| Syneto dry run | I - System/Network config |
| Syneto validate | I - System/Network config |

| ADMINISTRATION | |
|---|---------------------------|
| #ADMINISTRATION | |
| Automatic Check for Updates - Check for updates configuration | I - System/Network config |
| Firmware upgrade - Reboot action to Upload Mode | I - System/Network config |
| Certificates and Keys - Certificates management | I - System/Network config |
| Certificates and Keys - Keys management | I - System/Network config |
| Certificates and Keys - Jks management | I - System/Network config |
| Backup/Restore - Restore action | I - System/Network config |
| Backup/Restore - Backup common action | I - System/Network config |
| Backup/Restore - Backup complete action | I - System/Network config |
| Reset to defaults action | I - System/Network config |
| Reset Log action | I - System/Network config |
| Reboot action | M - Reboot |
| Change local password (*** only "admin") | L - Users config |
| ADMIN USER - Change password action | L - Users config |
| POWER USER - Change password action | L - Users config |
| POWER USER - Revoke access action | L - Users config |
| VIEW USER - Change password action | L - Users config |
| VIEW USER - Revoke access action | L - Users config |
| Password complexity - configuration | L - Users config |
| Password complexity - Clear rules to default action | L - Users config |
| Login access - Autologout action | I - System/Network config |
| Login access - SSH configuration | I - System/Network config |
| Login access - HTTP/HTTPS configuration | I - System/Network config |
| Login access - Local auth activation | I - System/Network config |
| Login access - AD/LDAP activation | I - System/Network config |
| Login access - AD/LDAP parameters | I - System/Network config |
| Login access - AD/LDAP certificate request | I - System/Network config |
| Login access - AD/LDAP configuration | I - System/Network config |
| Login access - AD/LDAP test | I - System/Network config |

| | |
|---|----------------------------------|
| Login Rules - Login failure configuration | L - Users config |
| Login Rules - Unlock users action | L - Users config |
| Login Rules - Login History check | L - Users config |
| Web Login banner configuration | I - System/Network config |
| SSH banner configuration | I - System/Network config |

| #DEVICE COMMANDS | |
|---|----------------------------------|
| COMMANDS - Test battery - UPS Test battery action | H - Ups command execution |
| COMMANS - Shutdown - UPS Shutdown action | H - Ups command execution |
| COMMANDS - Shutdown / Restore - UPS Shutdown / Restore action | H - Ups command execution |

| #DIAGNOSTIC | |
|-----------------------------------|----------------------------------|
| Test COMM LOST - test action | I - System/Network config |
| Test AUDIT FAILURE - test action | I - System/Network config |
| Web Requests - Check Web requests | I - System/Network config |

Login access

DASHBOARD DATA SYSTEM OVERVIEW HISTORY CONFIGURATION ADMINISTRATION

ADMINISTRATION DEVICE COMMANDS DIAGNOSTIC

ADMINISTRATION

- Automatic Check for Updates
- Firmware upgrade
- Certificates and Keys
- Backup/Restore Configuration
- Reset to defaults
- Reset Log
- Reboot
- Change local password
- Login access**
- Login rules
- Web Login banner
- SSH Login banner

Login access

AUTO LOGOUT

Enable Auto Logout

Auto Logout due to user inactivity after (seconds)

Warning message when are left (seconds) before logout (message 'Session is about to expire...')

SSH

Enable SSH

WARNING! IT IS NOT SUGGESTED TO KEEP ENABLED THE SSH PROTOCOL. WITH SSH ENABLED PLEASE CONSIDER TO IMPLEMENTED RESTRICTION METHODS FOR ITS ACCESS (E.G.: FIREWALL RULES, DEDICATED NETWORK CONNECTION, OTHERS...)

HTTP

Enable HTTP

HTTP port

HTTPS

Enable HTTPS

HTTPS port

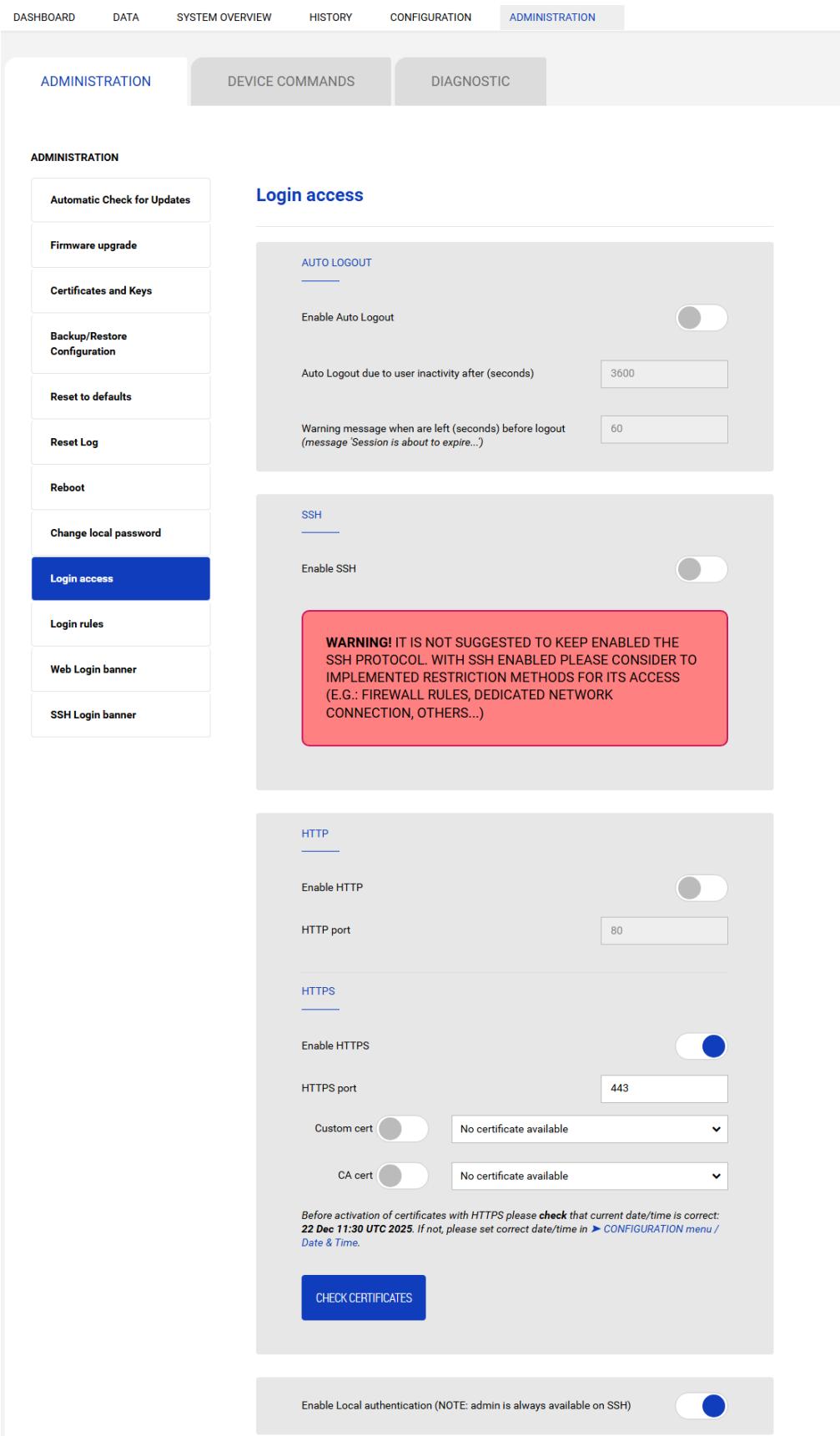
Custom cert No certificate available

CA cert No certificate available

Before activation of certificates with HTTPS please [check](#) that current date/time is correct: **22 Dec 11:30 UTC 2025**. If not, please set correct date/time in [CONFIGURATION menu / Date & Time](#).

CHECK CERTIFICATES

Enable Local authentication (NOTE: admin is always available on SSH)



Enable AD/LDAP authentication

LDAP

Connection Type

Host

Port

Certificate

!!! No jks keystore available

Password

Base DN/LDAP Users folder

Scope Auth method

BIND ACCESS

Bind User

Password

USER SEARCH

User Search Object Class

User Search Attribute

User Search Result / Groups

User Search Result / Auth

GROUP DEFINITIONS

Group Search DN Admin

Group Search DN Power

Group Search DN View

GROUP SEARCH

Group Search Object Class

Group Search Attribute

Group Member Attribute

LOGIN SESSION

Autocomplete Login with Base DN

HELP (WHAT IT DOES)

(click on the button for the complete description)

Auto Logout

AUTO LOGOUT

Enable Auto Logout

Auto Logout due to user inactivity after (seconds)

Warning message when are left (seconds) before logout
(message 'Session is about to expire...')

| Field | Description | Default |
|---|---|--------------|
| Enable Auto Logout | To enable Auto Logout | Enabled |
| Auto Logout due to user inactivity after (seconds) | After this inactivity time (no mouse clicks) NetMan 208C logout losing any unsaved configuration made | 3600 seconds |
| Warning message when are left (seconds) before logout | When inactivity time left is less than this value, a warning message is shown to alert of the next due logout | 60 seconds |

The Auto Logout function allows the user to logout automatically from Web Configuration (as “Admin” or “Power” credentials) after an inactivity time defined. While the User clicks and moves the mouse and interacts with Web configuration the session is kept alive.

Procedure allows the user to set:

- **“Autologout time”** (e.g.: 3600 seconds = 1 hour): after this time from last action, NetMan 208C logs out automatically the User freeing the Admin/Power session allowing another User to log in
- **“Warning time”** (e.g.: 60 seconds): when inactivity time left is less than this time, a Warning message is shown, so the User can continue and stay inside renewing the session or clicking somewhere

i This function solves the problem when a User logs in as Admin (or Power) and forgets the Web session open locking out any other Admin (or Power) User who wants to login. Enabling the Auto Logout function, after the defined time of inactivity, the User is automatically logout and the session is freed for any other User to login.



The Warning message allows the user to renew the session just clicking over “HERE TO RENEW” and User can continue to stay logged.

i Auto Logout ignores any unsaved change in the configuration.

SSH

SSH

Enable SSH



WARNING! IT IS NOT SUGGESTED TO KEEP ENABLED THE SSH PROTOCOL. WITH SSH ENABLED PLEASE CONSIDER TO IMPLEMENTED RESTRICTION METHODS FOR ITS ACCESS (E.G.: FIREWALL RULES, DEDICATED NETWORK CONNECTION, OTHERS...)

| Field | Description | Default |
|------------|--------------------------|----------|
| Enable SSH | To enable login over SSH | Disabled |

SSH service allow to connect to NetMan 208C via SSH protocol.

For a stronger security ensure the SSH protocol being disabled if not used.

HTTPS / HTTP

HTTP

Enable HTTP

HTTP port

HTTPS

Enable HTTPS

HTTPS port

Custom cert

CA cert

*Before activation of certificates with HTTPS please **check** that current date/time is correct: **19 Nov 15:13 UTC 2025**. If not, please set correct date/time in ➤ **CONFIGURATION** menu / **Date & Time**.*

CHECK CERTIFICATES

| Field | Description | Default |
|--------------|--|----------|
| Enable HTTP | To enable the HTTP service. | Disabled |
| HTTP port | Enter the port where HTTP service is started. | 80 |
| Enable HTTPS | To enable the HTTPS service. | Enabled |
| HTTPS port | Enter the port where HTTPS service is started. | 443 |
| Custom Cert | If uploaded and enabled, the HTTPS certificate to use for the HTTPS Web server connection | |
| CA Cert | If uploaded and enabled, the CA certificate to use for the HTTPS Web server connection | |

HTTPS certificates check

As option available to the user, HTTPS configuration can be tested before its effective usage:

- 1) just set the configuration without saving it:

Enable HTTPS

HTTPS port

Custom cert netman6309603e.pem

CA cert Riello_CA_signer.pem

*Before activation of certificates with HTTPS please **check** that current date/time is correct:
19 Nov 15:18 UTC 2025. If not, please set correct date/time in > CONFIGURATION menu / Date & Time.*

- 2) click to “CHECK CERTIFICATES” and wait for the quick testing:



- 3) after few seconds obtain the result of the correct (or wrong) certificate chain verification:

Enable HTTPS

HTTPS port

Custom cert netman6309603e.pem

CA cert Riello_CA_signer.pem

*Before activation of certificates with HTTPS please **check** that current date/time is correct:
19 Nov 15:20 UTC 2025. If not, please set correct date/time in > CONFIGURATION menu / Date & Time.*

CHECK CERTIFICATES

OK, CA file and CERTIFICATE file seems ok and valid for HTTPS

Warnings

Changing the Web settings **HTTP/HTTPS/ports** may lead to issues with the web browser.

Issue #1: use of HTTP

Some browsers can always try to reach the device with “<https://...>” even if the user write “<http://...>” as url requested. In this case, retry again, clear the Web browser history or change web browser

Issue #2: HTTPS connection lost

HTTPS web connection requires date/time set correctly. When switching to HTTPS or changing the date/time beware to set always the correct time or the correct existing timeserver.

When connection is lost and the web browser denies the access to the web page, fix the issue going to RECOVERY and execute “Restore Network” operation. SSH operations are allowed setting the correct parameters for date/time NTP server in the configuration via SSH Expert Shell or restoring HTTP connection for rescue the Web access.

Issue #3: cached web pages in the browser

Every web browser may keep saved in cache the previous version of a web page.

Effects of this browser behaviour may be:

- Web buttons (login) or links not working as expected
- Old or wrong web page shown instead of the new one expected

For solving this temporary issue, in the Web Browser the User can:

- press key **F5**
- press key **Shift + F5**
- press key **Control + F5**
- close and re-open the web browser
- change web browser

Local user authentication

Enable Local authentication (NOTE: admin is always available on SSH)



| Field | Description | Default |
|-----------------------------|--------------------------------|---------|
| Enable local authentication | To enable local authentication | Enabled |

Local user authentication allows the local users of NetMan 208C:

- “admin”
- “power”
- “view”

To login to NetMan 208C with Web Login.

By default, only “admin” user is available.

Local users “power” and “view” must be activated by the “admin” user (see “Change local password” section menu).

LDAP Configuration

| Field | Description | Default |
|----------------|-------------------------------|----------|
| Enable AD/LDAP | To enable LDAP authentication | Disabled |

LDAP

Connection Type: STARTTLS (LDAP with TLS)

Host: Debian11LdapServer.local, Port: 389

Certificate: Debian11LdapServer.local.jks

Password:

X REQUEST CERTIFICATE TO SERVER

Base DN/LDAP Users folder: dc=testdomain,dc=local

Scope: Subtree, Auth method: Anonymous

USER SEARCH

User Search Object Class: posixAccount

User Search Attribute: cn

User Search Result / Groups: uid

User Search Result / Auth: dn

GROUP DEFINITIONS

Group Search DN Admin: cn=GruppoAdmin,dc=testdomain,dc=local

Group Search DN Power: cn=GruppoPower,dc=testdomain,dc=local

GROUP SEARCH

Group Search Object Class: posixGroup

Group Search Attribute: dn

Group Member Attribute: memberUid

LOGIN SESSION

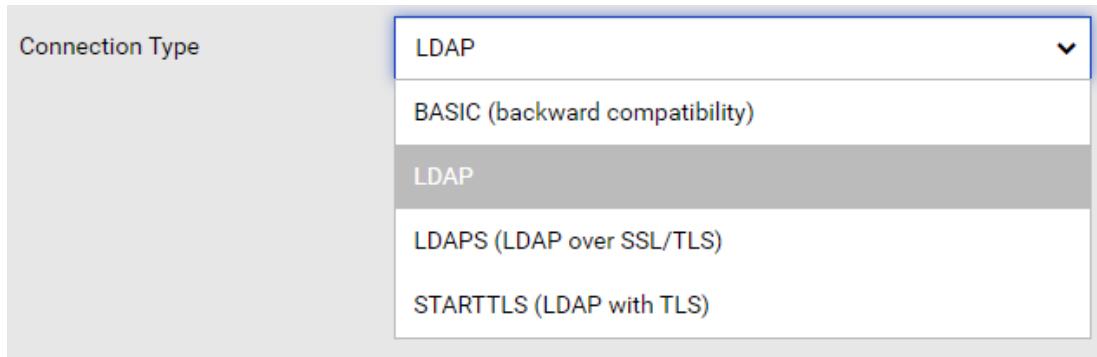
Autocomplete Login with Base DN: No

HELP (WHAT IT DOES)

UPDATE HELP DESCRIPTION (click on the button for the complete description)

This set of LDAP configuration parameters allows the user to connect both to LDAP and Active Directory for User Login authentication. The LDAP Configuration implemented allows the user to specify many credentials check behaviours: from *Anonymous* to *Regular* schemas and *Certificates*.

LDAP Connection Types



| Field | Description |
|-----------------|-------------------------|
| Connection Type | Type of LDAP connection |

There are four LDAP connection types:

| Connection Type | Description | Standard Port |
|---------------------------------------|---|--|
| BASIC (backward compatibility) | this mode replicates the previous LDAP method of NetMan 208C (Simple Authentication mode with some specific search of LDAP attributes both for AD and LDAP); if NetMan 208C was previously using LDAP successfully with old configuration, choosing this connection type all the parameters used before are still valid | port 389 or 636 (autodetected) |
| LDAP | implements a more complete way to connect via LDAP connection allowing exact specifications of Scope, Auth method, User Search attributes, Group search attribute specifications | port 389 |
| LDAPS (LDAP over SSL/TLS) | this connection type adds the usage of encryption with certificate from connection | port 636 |
| STARTTLS (LDAP with TLS) | this connection type allows encryption with TLS using the schema of STARTTLS (first connection then channel encryption with certificate) | port 389 |

Request of certificate to the Remote Server

When the remote Server Certificate is needed and queried port **636** is usually queried (→ see “Request certificate to server” procedure).

Host, Port, Certificate and Password

Host: Debian11LdapServer.local

Port: 389

Certificate: servertruststore.jks

Password:

REQUEST CERTIFICATE TO SERVER

| Field | Description |
|-----------------------------------|---|
| Host | Hostname or IP of the remote LDAP/AD Server |
| Port | Port used from remote LDAP/AD Server. (E.g.: 389, 636 or custom port) |
| Certificate | If available, select the JKS certificate to use for LDAP/AD connection |
| Password | <p>Password related to the JKS Certificate used. It must be ≥ 6 chars.</p> <p>For a successful connection to the server the Password field must be:</p> <ul style="list-style-type: none"> - left empty (normal usage, more secure) - the correct password related to the .JKS certificate used <p>When a wrong password the LDAP/AD connections is not established.</p> |
| REQUEST CERTIFICATE TO THE SERVER | Automatic procedure for requesting the correct certificate from the desired Server. |

LDAP/AD Certificate

When using LDAPS or STARTTLS connection type the LDAP Server may require use of a Certificate as mandatory showing the choice of the Certificate to use.

For LDAP the certificate is of **.JKS** type and it can be created and loaded: please check the configuration section “**Certificates and Keys**” under “**Administration**” menu.

REQUEST CERTIFICATE TO THE SERVER

For LDAP, instead of manually operate and then load the new certificate, it is offered a simpler way but is strongly dependant from the LDAP Server permissions: requesting directly the correct certificate to the LDAP Server.

How to do it?

Just filling the correct fields (Server hostname, Server Port, Password) and pressing the button “**Request Certificate to Server**” an internal procedure tries to Connect to the Server and download and save internally the certificate needed. If success, the final **.JKS** certificate is automatically saved and notified as available in NetMan 208C.

=> Please check then “**Technical Chapter**” for deeper understanding and how-to.

Base DN

Base DN/LDAP Users folder

OU=NoDomain Policy,OU=Utenti,OU=RPS,OU=GRUPPO RIELLO,DC=riello,DC=group

| Field | Description |
|--------------------------|---|
| Base DN/LDAP User folder | The Base DN for User Search / Auth in the LDAP Tree |

Scope and Authentication method

| | |
|---------|-------------|
| Scope | Auth method |
| Subtree | Simple |

| Field | Description |
|-------------|---|
| Scope | All the non-BASIC methods allow the choices of the Scope for the searches in the LDAP tree: <ul style="list-style-type: none">- Base: only objects of the Base DN- One level: only objects of 1st sub-level under the Base DN set- Subtree: all the objects found in the Base DN set and all subtree |
| Auth method | Authentication method: <ul style="list-style-type: none">- Anonymous: no need for credentials, just anonymous connection able to search every object in the LDAP tree- Simple: after the User authentication, NetMan 208C is allowed to search in the LDAP tree- Regular: a first Bind Authentication is needed for searching in LDAP tree, then the User that requests the Login must authenticate |

User Search parameters

| USER SEARCH | |
|-----------------------------|--------------|
| User Search Object Class | posixAccount |
| User Search Attribute | cn |
| User Search Result / Groups | uid |
| User Search Result / Auth | dn |

With these parameters, NetMan 208C is able to search the User in the Groups and to try to authenticate.

| Field | Description |
|------------------------------------|---|
| User Search Object Class | The object class to search in the LDAP tree (usually “posixAccount” for LDAP and “organizationalPerson” for AD). |
| User Search Attribute | The attribute to check for “Username” comparison (usually “cn” both for LDAP and AD). |
| User Search Result / Groups | The attribute to extract from object class found for searching membership the “groups” next (usually “uid” for LDAP and “dn” for AD). |
| User Search Result / Auth | The attribute to extract from object class found for next User authentication (usually “dn” for both LDAP and AD). |

Group definitions

GROUP DEFINITIONS

Group Search DN Admin

cn=administrators,ou=Groups,dc=yourrdomain,dc=com

Group Search DN Power

cn=powerusers,ou=Groups,dc=yourrdomain,dc=com

Group Search DN View

cn=viewusers,ou=Groups,dc=yourrdomain,dc=com

Here are defined the three groups where to search the User Membership:

| Field | Description |
|------------------------------|---|
| Group Search DN Admin | if User belongs to this group is recognized as an “admin” user. |
| Group Search DN Power | if User belongs to this group is recognized as a “power” user. |
| Group Search DN View | if User belongs to this group is recognized as a “view” user. |

Group Search

| GROUP SEARCH | |
|---------------------------|------------|
| Group Search Object Class | posixGroup |
| Group Search Attribute | dn |
| Group Member Attribute | memberUid |

| Field | Description |
|---------------------------|---|
| Group Search Object Class | Class to search for locating the user groups (e.g. “posixGroup”) |
| Group Search Attribute | Attribute to extract from object class for reading the group DN (e.g. “dn” can return “cn=GruppoAdmin,dc=testdomain,dc=local” that must match the group searched) |
| Group Member Attribute | Attribute to analyse for searching a specific user (e.g. memberUid) |

Example

With these parameters is checked the membership of the User to a Group:

- 1) NetMan 208C search for all the Object Class “posixGroup” in the LDAP tree
- 2) when find an Object with attribute “dn” equals to a group (e.g. “cn=GruppoAdmin,dc=testdomain,dc=local”) NetMan 208C lists all the members reading the attribute “memberUid”
- 3) the presence of the User (using its “uid” attribute) is checked in the list of members of the Group

If the User is found in the “Group Search DN Admin” group field set above, search stops and User is identified as “admin” user.

If not, the User is found in the “Group Search DN Power” group field set above, search stops and User is identified as “power” user.

If not, the User is found in the “Group Search DN View” group field set above, search stops and User is identified as “view” user.

If not found in any group, the User has no access, even if exists in the LDAP Server.

Auto-complete Login DN

LOGIN SESSION

Autocomplete Login with Base DN

| Field | Description | Default |
|--|--|-------------------------------|
| Autocomplete Login with Base DN | Some LDAP/AD servers may require to complete the simple username (e.g. “ alice ”) with its Full DN format (e.g. “ cn=alice,dc=testdomain,dc=local ”) for a correct authentication. | No (completion not needed) |

!!! General advice about the configuration parameters

All these parameters can show a strong variety due to all possible different implementations of attributes allowed in the LDAP Servers and Active Directory Servers.

⇒ Please read the “Technical Chapter” for deeper understanding and behaviour.

Preview of NetMan actions set by the parameters

When all parameters of LDAP are configured, it is possible to check the detailed operations that will be executed:

HELP (WHAT IT DOES)

↻ UPDATE HELP DESCRIPTION

(click on the button for the complete description)

just clicking over the button “**UPDATE HELP DESCRIPTION**” that shows a full explanation of the single actions executed:

Connection is executed as LDAPS (LDAP over SSL) to Hostname get from '**Debian11LdapServer.local**' and port '389' (default is 636).

For connection is used the certificate '**Debian11LdapServer.local.jks**' with password '#####' for data encryption. Referrals are followed.

Every search in the tree is executed with the search scope '**Subtree**' (all the subtree levels under '**dc=testdomain,dc=local**').

During Login, user must type its '**USERNAME_REQUESTING_LOGIN**' and password '**PASSWORD_REQUESTING_LOGIN**' for login into the system.

Authentication is done as ANONYMOUS, without any credentials.

Once connected, it must be possible to operate searches in the LDAP tree.

User (from Login credentials '**USERNAME_REQUESTING_LOGIN**' with password '**PASSWORD_REQUESTING_LOGIN**') must be searched in the LDAP tree: all objects with Class

'**posixAccount**' are searched, when object found is read the attribute '**cn**' and check for matching with username requested at login '**USERNAME_REQUESTING_LOGIN**'. If user match found, are extracted the attributes '**uid**' (for searching user in Groups) and '**dn**' (a full DN of User, for user authentication).

Checking if user '**USERNAME REQUESTING LOGIN**' belongs to Admin group

'**cn=GruppoAdmin,dc=testdomain,dc=local**'

all the objects with Class '**posixGroup**' are scanned and their attribute '**dn**' is compared with the Admin Group DN '**cn=GruppoAdmin,dc=testdomain,dc=local**'; if match is found, are extracted all the attributes '**memberUid**' as list; if user '**USERNAME_REQUESTING_LOGIN**' by its attribute '**uid**' (the full DN found as Result/Group before) is found in this list it gains 'Admin' rights in the Netman and search ends with success.

(If not found) Checking if user '**USERNAME REQUESTING LOGIN**' belongs to Admin group

'**cn=GruppoPower,dc=testdomain,dc=local**'

all the objects with Class '**posixGroup**' are scanned and their attribute '**dn**' is compared with the Admin Group DN '**cn=GruppoPower,dc=testdomain,dc=local**'; if match is found, are extracted all the attributes '**memberUid**' as list; if user '**USERNAME_REQUESTING_LOGIN**' by its attribute '**uid**' (the full DN found as Result/Group before) is found in this list it gains 'Power' rights in the Netman and search ends with success.

Now user requesting the access must authenticate: user DN '**USERNAME_REQUESTING_LOGIN**' by its attribute '**dn**' (the full DN found as Result/Auth before) test the binding with the password '**PASSWORD_REQUESTING_LOGIN**'; if binding fails, user authentication fails. If binding is correct,

user is authenticated and group membership is reported as **Admin** (if recognized before)

or **Power** group (if recognized before); if user has no membership, it is reported as '**No user found**'.

Testing the LDAP configuration with a Login Test

For a simpler check, after any “SAVE” action button, it is possible to test the LDAP configuration easily typing Username and Password of Users:

TEST AD/LDAP AUTHENTICATION (PLEASE CLICK SAVE BEFORE TESTING)

| | |
|------------|-------|
| Test User: | alice |
| Password | |

TEST AD/LDAP

Ok, User recognized as **ADMIN** User

| Field | Description |
|------------------|-------------------------------|
| Test user | User to test |
| Password | Password (it may be empty) |

This test can help to identify problems with configuration by some error messages:

TEST AD/LDAP

ERR-22: Wrong user credentials

TEST AD/LDAP

ERR-45: LDAPS - Server has not SSL/TLS certificates installed correctly: check server certificate configuration

TEST AD/LDAP

ERR-63: STARTTLS / Certificate error (CN different from Hostname, wrong password, certificate format wrong)

LDAP Error List

The first group of errors (from **ERR-20** to **ERR-98**) are strongly related to the NetMan 208C algorithm implemented. Then second group of errors (from **ERR-99** to the **ERR-223**) is based on the COMMON LDAP STANDARD ERRORS: then index of error is incremented by 100.

| | |
|----------------|---|
| ERR-20 | Unknown error |
| ERR-21 | Wrong bind or user credentials |
| ERR-22 | Wrong user credentials |
| ERR-23 | Server requires bind authentication credentials (Anonymous not allowed) |
| ERR-24 | User is not present in the ADMIN or POWER groups |
| ERR-25 | Server connection not successful (port or hostname wrong) |
| ERR-26 | Server connection not successful (hostname wrong) |
| ERR-41 | LDAPS - Certificate error (CN different from Hostname) or wrong Server port |
| ERR-42 | LDAPS - TLS handshake failed or Certificate CN different from Hostname or Server does not support certificates (check Server configuration): check certificate or Server certificate management |
| ERR-43 | LDAPS - Wrong Certificate (CN different from Hostname) |
| ERR-44 | LDAPS - Certificate error (CN different from Hostname, password wrong, certificate format wrong) or wrong certificate type or wrong port or Server does not support certificates (check Server configuration) |
| ERR-45 | LDAPS - Server has not SSL/TLS certificates installed correctly: check server certificate configuration |
| ERR-61 | STARTTLS - Certificate error (CN different from Hostname), during STARTTLS negotiation after the bind |
| ERR-62 | STARTTLS - TLS negotiation failed or CN different from Hostname or Server does not support certificates (check Server configuration) |
| ERR-63 | STARTTLS / Certificate error (CN different from Hostname, wrong password, certificate format wrong) |
| ERR-99 | COMMON - Undefined |
| ERR-100 | COMMON - Success |
| ERR-101 | COMMON - Operations Error |
| ERR-102 | COMMON - Protocol Error |
| ERR-103 | COMMON - Time Limit Exceeded |
| ERR-104 | COMMON - Size Limit Exceeded |
| ERR-105 | COMMON - Compare False |
| ERR-106 | COMMON - Compare True |
| ERR-107 | COMMON - Authentication Method Not Supported |
| ERR-108 | COMMON - Stronger Authentication Required |
| ERR-110 | COMMON - Referral |
| ERR-111 | COMMON - Admin Limit Exceeded |
| ERR-112 | COMMON - Unavailable Critical Extension |
| ERR-113 | COMMON - Confidentiality Required |
| ERR-114 | COMMON - SASL Bind In Progress |
| ERR-116 | COMMON - No Such Attribute |
| ERR-117 | COMMON - Undefined Attribute Type |
| ERR-118 | COMMON - Inappropriate Matching |
| ERR-119 | COMMON - Constraint Violation |
| ERR-120 | COMMON - Attribute or Value exists |
| ERR-121 | COMMON - Invalid Attribute Syntax |
| ERR-132 | COMMON - No such Entry |
| ERR-133 | COMMON - Alias Problem |
| ERR-134 | COMMON - Invalid DN Syntax') |

| | |
|----------------|---|
| ERR-135 | COMMON - Object is a Leaf |
| ERR-136 | COMMON - Alias Dereferencing Problem |
| ERR-148 | COMMON - Inappropriate Authentication |
| ERR-149 | COMMON - Invalid Credentials |
| ERR-150 | COMMON - Insufficient Access Rights |
| ERR-151 | COMMON - Busy |
| ERR-152 | COMMON - Unavailable |
| ERR-153 | COMMON - Unwilling to Perform |
| ERR-154 | COMMON - Loop Detected |
| ERR-160 | COMMON - Sort Control Missing |
| ERR-161 | COMMON - Offset Range Error |
| ERR-164 | COMMON - Naming Violation |
| ERR-165 | COMMON - Object Class Violation |
| ERR-166 | COMMON - Not Allowed On Non-Leaf |
| ERR-167 | COMMON - Not Allowed On RDN |
| ERR-168 | COMMON - Entry Already Exists |
| ERR-169 | COMMON - Object Class Modifications Prohibited |
| ERR-170 | COMMON - Results Too Large |
| ERR-171 | COMMON - Affects Multiple DSAs |
| ERR-176 | COMMON - Virtual List View Error or Control Error |
| ERR-180 | COMMON - Other |
| ERR-181 | COMMON - Server Down |
| ERR-182 | COMMON - Local Error |
| ERR-183 | COMMON - Encoding Error |
| ERR-184 | COMMON - Decoding Error |
| ERR-185 | COMMON - Client-Side Timeout |
| ERR-186 | COMMON - Unknown Authentication Mechanism |
| ERR-187 | COMMON - Filter Error |
| ERR-188 | COMMON - Cancelled by User |
| ERR-189 | COMMON - Parameter Error |
| ERR-190 | COMMON - Out of Memory |
| ERR-191 | COMMON - Connect Error |
| ERR-192 | COMMON - Operation not Supported |
| ERR-193 | COMMON - Control Not Found |
| ERR-194 | COMMON - No Results Returned |
| ERR-195 | COMMON - Unexpected Results Returned |
| ERR-196 | COMMON - Referral Loop Detected |
| ERR-197 | COMMON - Referral Hop Limit Exceeded |
| ERR-200 | COMMON - Invalid Response |
| ERR-201 | COMMON - Ambiguous Response |
| ERR-212 | COMMON - TLS Not Supported |
| ERR-213 | COMMON - Intermediate Response |

| | |
|----------------|----------------------------|
| ERR-214 | COMMON - Unknown Type |
| ERR-218 | COMMON - Cancelled |
| ERR-219 | COMMON - No Such Operation |
| ERR-220 | COMMON - Too Late |
| ERR-## | Unknown error |

| | |
|----------------|-------------------------------|
| ERR-221 | COMMON - Cannot Cancel |
| ERR-222 | COMMON - Assertion Failed |
| ERR-223 | COMMON - Authorization Denied |

Login rules

DASHBOARD DATA SYSTEM OVERVIEW HISTORY CONFIGURATION ADMINISTRATION

ADMINISTRATION DEVICE COMMANDS DIAGNOSTIC

ADMINISTRATION

Automatic Check for Updates

Firmware upgrade

Certificates and Keys

Backup/Restore Configuration

Reset to defaults

Reset Log

Reboot

Change local password

Login access

Login rules

Web Login banner

SSH Login banner

Login rules

IN CASE OF LOGIN FAILURE

Login retry max: 5 retry

Login min interval before retry: 60 seconds

When USER exceeds all the retries with wrong password, it will be locked: only the ADMINISTRATOR can unlock the user again.

SAVE **CLEAR LOGIN RULES TO DEFAULT**

UNLOCK USERS

Administrator can reactivate user locked because wrong password retries.

CHECK LOCKED USERS

| Locked users: | Locked at time: |
|------------------|-----------------|
| (No user locked) | - |

LOGIN HISTORY

UPDATE LOGIN HISTORY

Show 10 entries Search:

| Date/Time | Event |
|-------------------------|---|
| 2025/12/19 14:29:09 UTC | LOGIN - LOCAL user 'admin' (ADMIN user) logged from 10.1.10.88 |
| 2025/12/22 08:09:57 UTC | LOGIN - LOCAL user 'admin' (ADMIN user) logged from 10.1.10.88 |
| 2025/12/22 08:27:26 UTC | LOGIN - LOCAL user 'admin' (ADMIN user) logged from 10.1.10.88 |
| 2025/12/22 09:07:15 UTC | LOGIN - LOCAL user 'admin' tried to login from 10.1.10.88 but failed (access denied) |
| 2025/12/22 09:07:28 UTC | LOGIN - LOCAL user 'admin' tried to login from 10.1.10.88 but failed [Please wait before try again (47 seconds...)] |
| 2025/12/22 09:08:01 UTC | LOGIN - LOCAL user 'admin' tried to login from 10.1.10.88 but failed [Please wait before try again (14 seconds...)] |
| 2025/12/22 09:08:12 UTC | LOGIN - LOCAL user 'admin' tried to login from 10.1.10.88 but failed [Please wait before try again (3 seconds...)] |
| 2025/12/22 09:08:18 UTC | LOGIN - LOCAL user 'admin' (ADMIN user) logged from 10.1.10.88 |
| 2025/12/22 10:46:06 UTC | LOGIN - LOCAL user 'admin' (ADMIN user) logged from 10.1.10.88 |
| 2025/12/22 11:20:35 UTC | LOGIN - LOCAL user 'admin' (ADMIN user) logged from 10.1.10.88 |

<<< **1** **2** **>>>**

IN CASE OF LOGIN FAILURE

This menu section allows the user to define the rules of Web login authentications.

IN CASE OF LOGIN FAILURE

Login retry max retry

Login min interval before retry 60 seconds

When USER exceeds all the retries with wrong password, it will be locked: only the ADMINISTRATOR can unlock the user again.

SAVE **CLEAR LOGIN RULES TO DEFAULT**

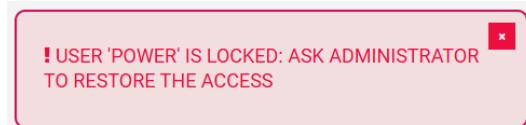
| Field | Description | Default |
|--|---|------------|
| Login retry max | The maximum number of retries permitted before a user is locked | 5 retries |
| Login min interval before retry | Time to wait for user authentication for retry again | 60 seconds |

By default:

- after a failed login the user must wait 60 seconds before retrying again.
- after 5 consecutive failed login the user is blocked.

When a user fails to login due to wrong username or password, the event is recorder and checked.

As unique exception, only the local “admin” user is never blocked and can retry indefinitely.

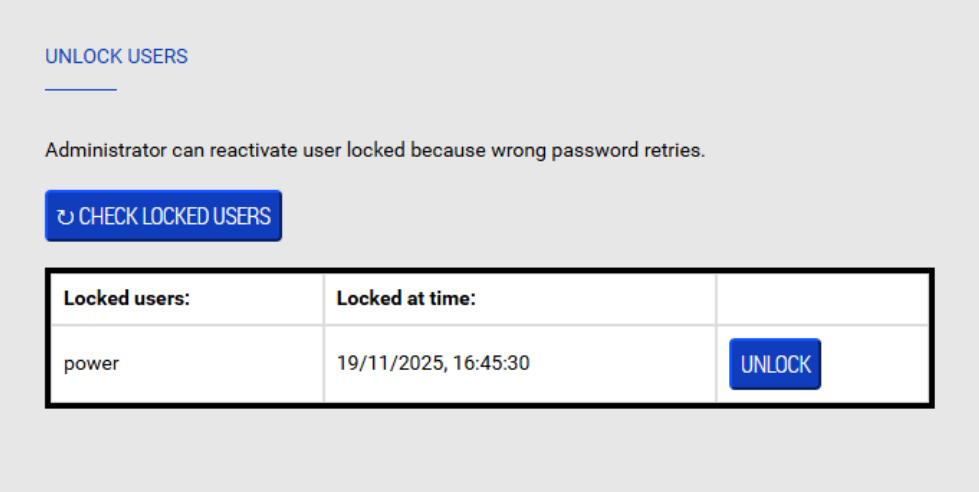


If Email service is enabled with “Security alerts” flags, an email notification is sent to all the “Security alerts” flagged recipients notifying this user locked event (-> see “Email” configuration).

Anytime the locked user retry to login other notifications are sent again to all the “Security” flagged recipients.

UNLOCK USERS

When a user is locked, only the “admin” user can unlock it:



UNLOCK USERS

Administrator can reactivate user locked because wrong password retries.

↻ CHECK LOCKED USERS

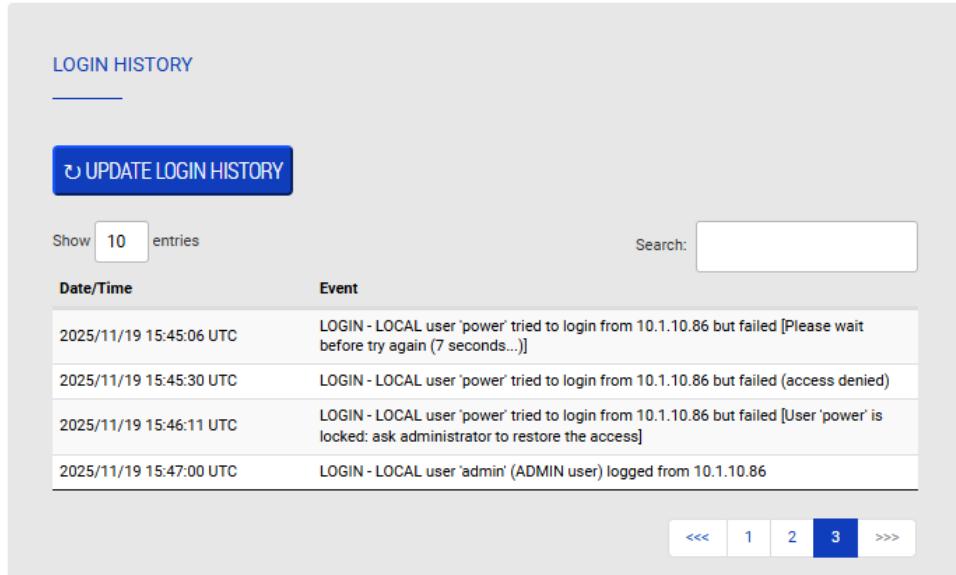
| Locked users: | Locked at time: | |
|---------------|----------------------|---------------|
| power | 19/11/2025, 16:45:30 | UNLOCK |

| Field | Description |
|---------------------------|--|
| CHECK LOCKED USERS | Manually updates the table of locked users |
| UNLOCK | Unlock the single user in the table |

Date and time reported in the Locked table refers to when the user has been blocked.

LOGIN HISTORY

Every login session is recorded in the Login history for a quick review and a search filter is available:



The screenshot shows a 'LOGIN HISTORY' page. At the top, there is a blue button labeled 'UPDATE LOGIN HISTORY' with a circular arrow icon. Below the button, there are two input fields: 'Show 10 entries' and a 'Search:' input box. The main area is a table with two columns: 'Date/Time' and 'Event'. The table contains four rows of login events. At the bottom, there is a navigation bar with buttons for '<<<', '1', '2', '3' (which is highlighted in blue), and '>>>'.

| Date/Time | Event |
|-------------------------|--|
| 2025/11/19 15:45:06 UTC | LOGIN - LOCAL user 'power' tried to login from 10.1.10.86 but failed [Please wait before try again (7 seconds...)] |
| 2025/11/19 15:45:30 UTC | LOGIN - LOCAL user 'power' tried to login from 10.1.10.86 but failed (access denied) |
| 2025/11/19 15:46:11 UTC | LOGIN - LOCAL user 'power' tried to login from 10.1.10.86 but failed [User 'power' is locked: ask administrator to restore the access] |
| 2025/11/19 15:47:00 UTC | LOGIN - LOCAL user 'admin' (ADMIN user) logged from 10.1.10.86 |

| Field | Description |
|-----------------------------|--|
| UPDATE LOGIN HISTORY | Manually updates the table of login events history. |
| Search | Filter field available to the user for searching specific words in the table events. |

Web Login banner

DASHBOARD DATA SYSTEM OVERVIEW HISTORY CONFIGURATION ADMINISTRATION

ADMINISTRATION

DEVICE COMMANDS

DIAGNOSTIC

ADMINISTRATION

Automatic Check for Updates

Firmware upgrade

Certificates and Keys

Backup/Restore Configuration

Reset to defaults

Reset Log

Reboot

Change local password

Login access

Login rules

Web Login banner

SSH Login banner

Web Login banner

!!! Please do not show sensible informations in the Banner text (e.g. usernames or passwords) when in production or not safe environment.

PRE-LOGIN BANNER



This banner is shown to all users of the Netman before every login.

Show Pre-Login banner

hide show

Title

Message

POST-LOGIN ADMIN USER



This banner is shown after ADMIN user login.

Show Post-Login ADMIN banner

hide show

Title

Message

POST-LOGIN POWER USER



This banner is shown after POWER user login.

Show Post-Login POWER banner hide show

Title

Message

POST-LOGIN VIEW USER



This banner is shown after VIEW user login.

Show Post-Login VIEW banner hide show

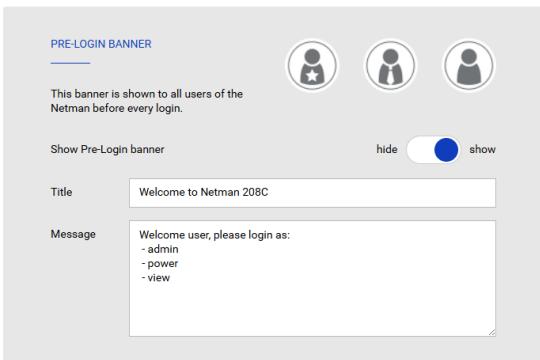
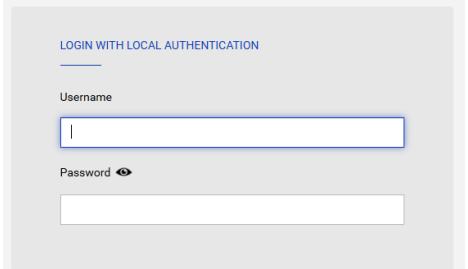
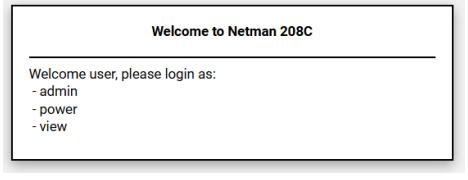
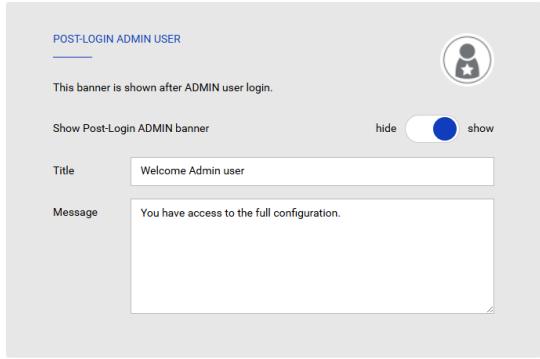
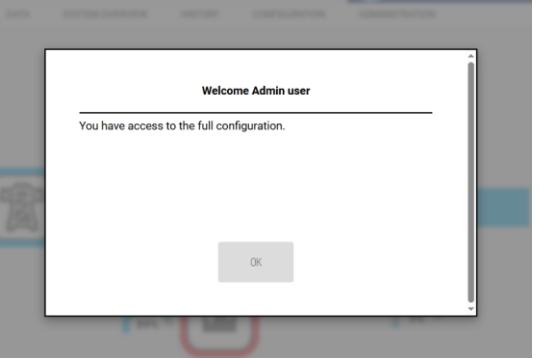
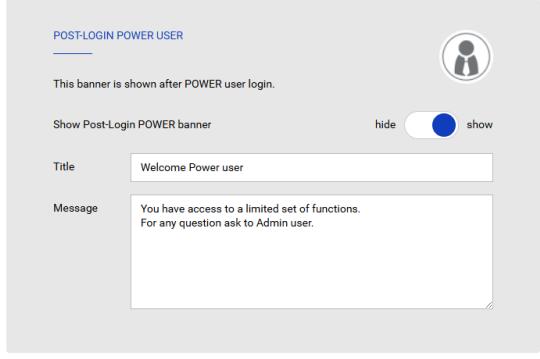
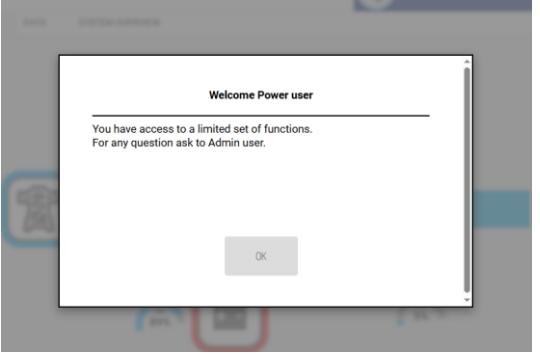
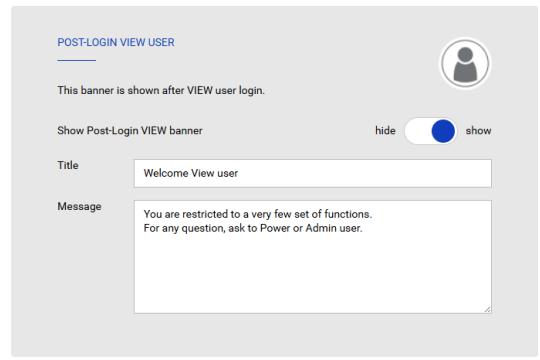
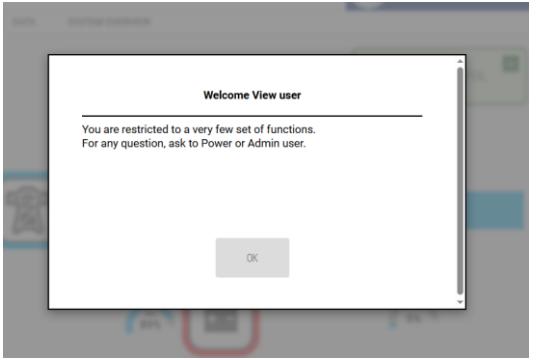
Title

Message

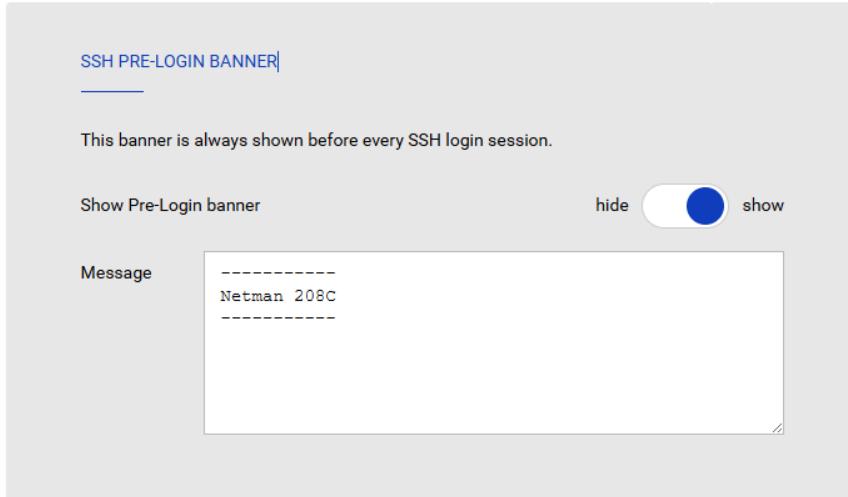
It is possible to define:

- **Pre-login** banner → shown with Web login page.
- Post-login **admin** user → shown after the Web login with “**admin**” (local or LDAP user)
- Post-login **power** user → shown after the Web login with “**power**” (local or LDAP user)
- Post-login **view** user → shown after the Web login with “**view**” (local or LDAP user)

| Field | Description | Default |
|--|--|----------|
| Show Pre-Login banner Show Post-Login ADMIN banner Show Post-Login POWER banner Show Post-Login VIEW banner | Enable / Disable the display of the message | Disabled |
| Title | Message to show as title | Empty |
| Message | Message to show as text (it accepts multi-line text) | Empty |

| Configuration | Result (before/after Web login) |
|---|---|
| <p>PRE-LOGIN BANNER</p>  <p>This banner is shown to all users of the Netman before every login.</p> <p>Show Pre-Login banner <input type="checkbox"/> <input checked="" type="checkbox"/> show</p> <p>Title: Welcome to Netman 208C</p> <p>Message: Welcome user, please login as: - admin - power - view</p> |   |
| <p>POST-LOGIN ADMIN USER</p>  <p>This banner is shown after ADMIN user login.</p> <p>Show Post-Login ADMIN banner <input type="checkbox"/> <input checked="" type="checkbox"/> show</p> <p>Title: Welcome Admin user</p> <p>Message: You have access to the full configuration.</p> |  |
| <p>POST-LOGIN POWER USER</p>  <p>This banner is shown after POWER user login.</p> <p>Show Post-Login POWER banner <input type="checkbox"/> <input checked="" type="checkbox"/> show</p> <p>Title: Welcome Power user</p> <p>Message: You have access to a limited set of functions. For any question ask to Admin user.</p> |  |
| <p>POST-LOGIN VIEW USER</p>  <p>This banner is shown after VIEW user login.</p> <p>Show Post-Login VIEW banner <input type="checkbox"/> <input checked="" type="checkbox"/> show</p> <p>Title: Welcome View user</p> <p>Message: You are restricted to a very few set of functions. For any question, ask to Power or Admin user.</p> |  |

SSH Login banner



| Field | Description |
|-----------------------|---|
| Show Pre-Login banner | Enable / Disable the display of the message when client connect to the SSH of NetMan 208C |
| Message | Message to show as text (it accepts multi-line text) |

When SSH service is enabled the message set is shown before the SSH Login password request:

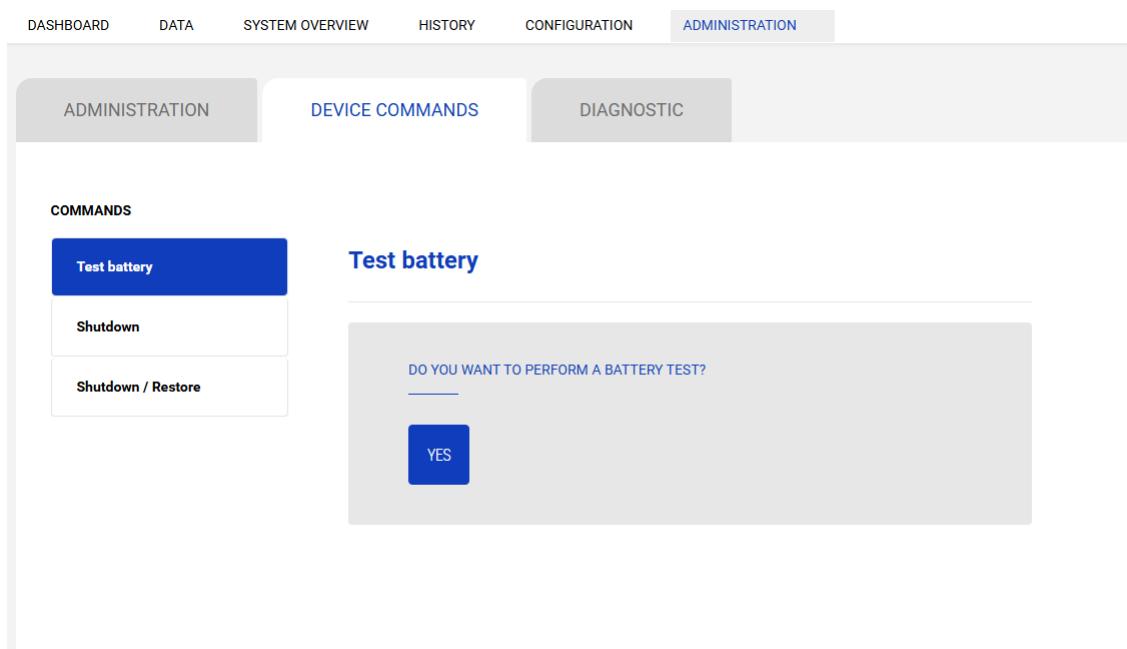
```
-----  
Netman 208C  
-----  
admin@netman [REDACTED].local's password:
```

Notes:

- some SSH clients *may not* show the Pre-banner text.
- example shown here is executed with command-line SSH command (Linux and Windows).

DEVICE COMMANDS

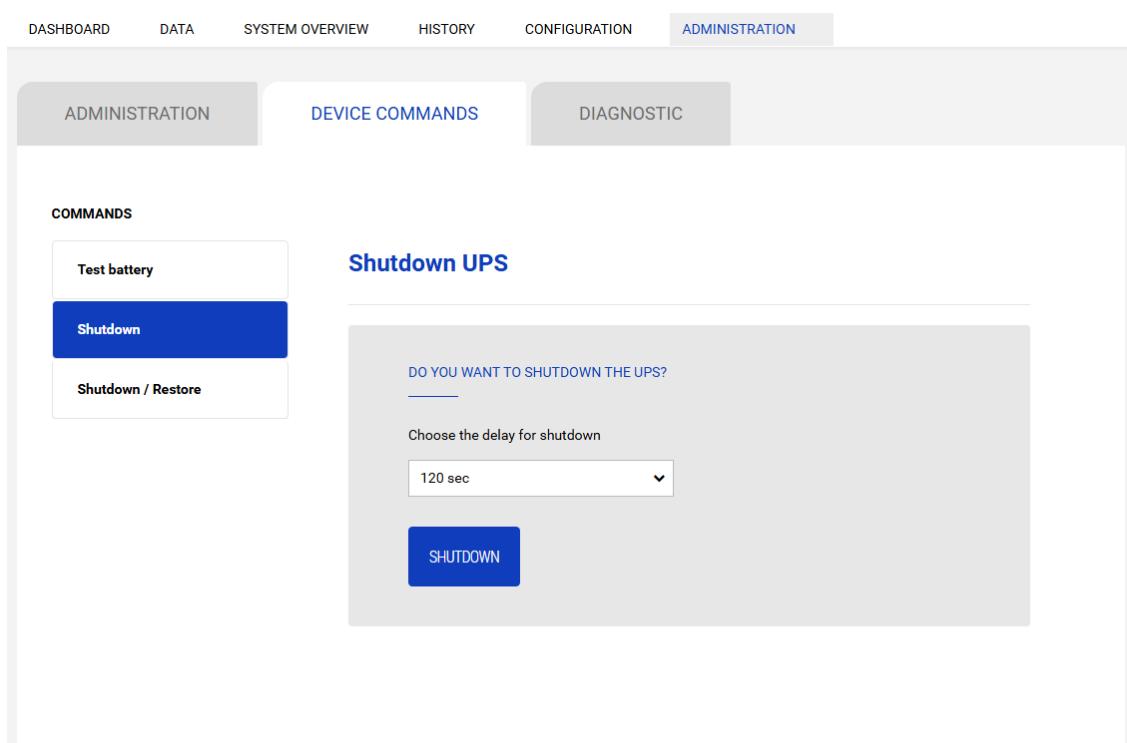
Test battery



The screenshot shows the 'DEVICE COMMANDS' section of the interface. On the left, a sidebar lists 'Test battery', 'Shutdown', and 'Shutdown / Restore'. The 'Test battery' option is highlighted with a blue background. The main area is titled 'Test battery' and contains the question 'DO YOU WANT TO PERFORM A BATTERY TEST?'. A blue 'YES' button is visible at the bottom.

To execute a test of the batteries.

Shutdown



The screenshot shows the 'DEVICE COMMANDS' section of the interface. On the left, a sidebar lists 'Test battery', 'Shutdown', and 'Shutdown / Restore'. The 'Shutdown' option is highlighted with a blue background. The main area is titled 'Shutdown UPS' and contains the question 'DO YOU WANT TO SHUTDOWN THE UPS?'. Below this, it says 'Choose the delay for shutdown' and shows a dropdown menu set to '120 sec'. A blue 'SHUTDOWN' button is visible at the bottom.

To execute a shutdown of the device.

Shutdown / Restore

The screenshot shows a web-based interface for device administration. At the top, there is a navigation bar with tabs: DASHBOARD, DATA, SYSTEM OVERVIEW, HISTORY, CONFIGURATION, and ADMINISTRATION. The ADMINISTRATION tab is currently selected. Below the navigation bar, there is a secondary navigation bar with three tabs: ADMINISTRATION, DEVICE COMMANDS (which is currently selected), and DIAGNOSTIC. On the left side, there is a sidebar titled 'COMMANDS' containing three buttons: 'Test battery', 'Shutdown', and 'Shutdown / Restore'. The 'Shutdown / Restore' button is highlighted with a blue background. The main content area is titled 'Shutdown and restore UPS'. It contains a sub-section titled 'DO YOU WANT TO SHUTDOWN AND RESTORE THE UPS?'. Below this, there are two dropdown menus: 'Choose the delay for shutdown' (set to '60 sec') and 'Choose the delay for restore' (set to '1 hour'). At the bottom of this section is a large blue button labeled 'SHUTDOWN AND RESTORE'.

To execute a shutdown and restore of the device.

DIAGNOSTIC

The diagnostic menu allows the user to test some NetMan 208C functionality as periodic check.

DASHBOARD DATA SYSTEM OVERVIEW HISTORY CONFIGURATION **ADMINISTRATION**

ADMINISTRATION DEVICE COMMANDS **DIAGNOSTIC**

DIAGNOSTIC

General

Test COMM LOST

Test AUDIT FAILURE

Web Requests

Diagnostic



This section allows to test some specific sections and functionalities of the Netman card.
Please be carefull with the tests and their effects on warnings / errors / messages as side effect.

Test COMM LOST

DASHBOARD DATA SYSTEM OVERVIEW HISTORY CONFIGURATION ADMINISTRATION

ADMINISTRATION DEVICE COMMANDS DIAGNOSTIC

DIAGNOSTIC

Test COMM LOST

This test will interrupt the communication with the UPS with these effects:

- no communication with the UPS
- warning messages in the web page as COMM LOST
- other warnings and messages sent via SNMP / Email / SYSLOG / etc... when set

Testing time: 1 minute

After the test the communication with the UPS will be restored to normal.

START THE TEST

| Field | Description |
|----------------|-----------------------|
| START THE TEST | Test COMM LOST starts |

The aim of this test is to interrupt the communication to the UPS for one minute and check

- warnings
- notification
- alerts

shown and sent in case of this type of event.

After one minute the UPS communication is restored.

Test AUDIT FAILURE

DASHBOARD DATA SYSTEM OVERVIEW HISTORY CONFIGURATION ADMINISTRATION

ADMINISTRATION DEVICE COMMANDS DIAGNOSTIC

DIAGNOSTIC

General

Test COMM LOST

Test AUDIT FAILURE

Web Requests

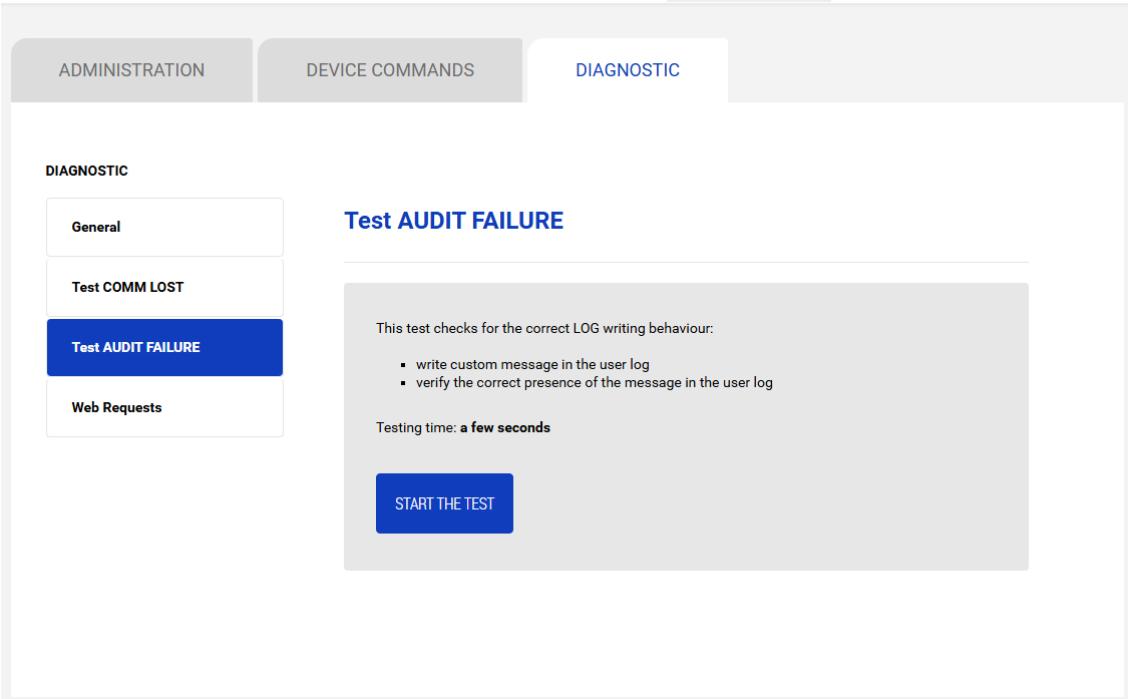
Test AUDIT FAILURE

This test checks for the correct LOG writing behaviour:

- write custom message in the user log
- verify the correct presence of the message in the user log

Testing time: **a few seconds**

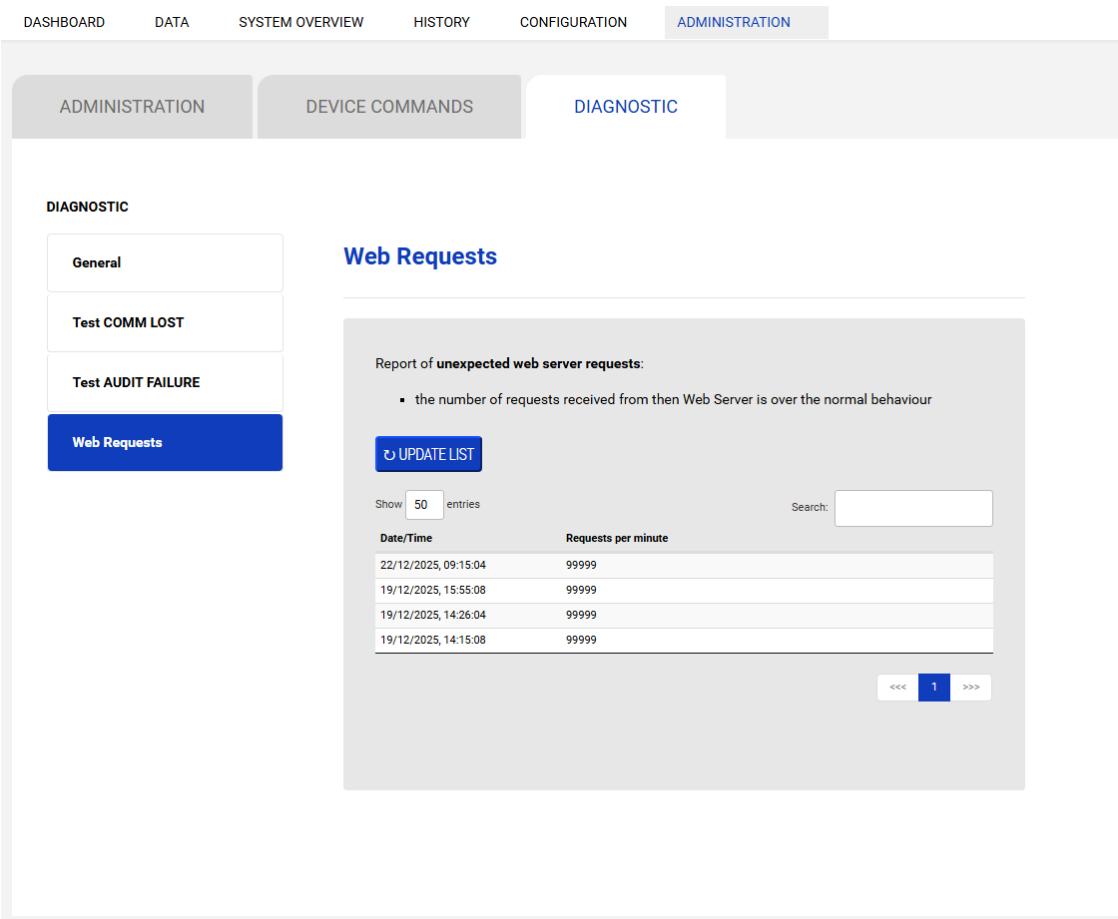
START THE TEST



| Field | Description |
|----------------|-------------------------------|
| START THE TEST | Starts the AUDIT FAILURE test |

The aim of this test is to check the capability of writing an event in the log.

Web Requests



Report of unexpected web server requests:
the number of requests received from then Web Server is over the normal behaviour

| Date/Time | Requests per minute |
|----------------------|---------------------|
| 22/12/2025, 09:15:04 | 99999 |
| 19/12/2025, 15:55:08 | 99999 |
| 19/12/2025, 14:26:04 | 99999 |
| 19/12/2025, 14:15:08 | 99999 |

| Field | Description |
|-------------|------------------------------------|
| UPDATE LIST | Update the list of recorded events |

This menu allows the user to check the events related to the unexpected high number or requests received from the Web server of the NetMan 208C (*number of requests per minute*). A number is shown when the requests per minute are over a predefined threshold. If number 99999 is reported the internal Web server has become out-of-service due to an excessive number of requests.

Causes of high request numbers reported:

- More than one user is requesting and updating heavily some web resources from the NetMan 208C.
- If more events like this are reported, a possible DoS attack has acted to the NetMan 208C from the Network.

Notes:

- Besides the Web pages are not accessible due to high requests, all the other services of the NetMan 208C keep working.
- If Email service is enabled, the email recipients with flag “Security alerts” enabled receives an email notification related to the event of excessive requests (-> See Email configuration).

PASSWORD RESET

If the default password for the local “admin” user is lost, it is possible to reset to default password with an authorization code from the Service department of the manufacturer.

The User can click on the link “HERE” to reset the password:



A “Password Reset” page will be displayed:

Password Reset

INSTRUCTION

Please send the following **REQUEST** to the Service via email and wait for the **RESET CODE**:

[COPY REQUEST TO CLIPBOARD](#)

```
MIIETwYJKoZIhvcNAQcCoIIEQDCCBDwCAQExDzANBglghkgBZQMEAqEFADAvBqkqhkiG9w0BBwGg
IgQgMDA6MDI6NjM6MDk6NjA6M2U6MDI6MDA6MDg6NTM6ND0ggI3MIICMzCCAdqgAwIBAgIUCu+v
vf3brwIXh6tSIm/Cd90vPDYwCgYIKoZIzj0EAwIwITELMAkGA1UEBhMCSVQxJzA1BgNVEAoMH1JQ
```

```
DzFsmGowCwYJYI2IAWUDBAEqMAsGCWCGSAF1AwQBFjALBglghkgBZQMEAQIwCgYIKoZIhvcNAwcw
DgYIKoZIhvcNAwICAgCAMA0GCCqGSIB3DQMCAgFAMAcGEss0AwIHMA0GCCqGSIB3DQMCAGeoMAoG
CCqGSM49BAMCBEYwRAIgVX5etj4MnBRQ4SPRuUmVg5TQJeelAw8nHyYBzz0XNQCIFUc0oj0bH5O
owFjJypTw2wZAAK1V8jgxAcmHYZPzKQA
```

INSERT RESET CODE

When you receive the **RESET CODE** from the Service paste here below, then press **SUBMIT**.
(You can close this page and come back later when you will receive the code)

The password reset procedure implies:

1) Copy the REQUEST CODE:

MIIEITwYJKo2IhvNAQcCoIIEQDCBCDwCAQExDzANBg1ghkgBZQMEAgsEFADAvBgkqhkiG9w0BBwGgIgQgMDA6MDI6NjM6MDk6NjA6M2U6MDI6MDA6MDg6NTM6ND0gggI3MIIICMzCCAdggAwIBAgIUCu+vvf3brwIXh6tSTM/Cd90vPDYwCgYIKoZIzj0EAwIwTTELMAkGA1UEBhMCsvQxJzA1BgNVBAoMH1JQ

DzFsMGowCwYJYIZIAWDBAEqMAsGCWCGSAF1AwQBFjALBglghkgBZQMEAQIwCgYIKoZIhvCNawcw
DgYIKoZIhvCNawICAqCAMA0GCCqGSIB3DQMCAGFAMACGBSsOAwIHMA0GCCqGSIB3DQMCAGEoMAoG
CCqGSM49BAMCBEYwRAIgVX5Zetj4MnBRQ4SPRuUmVg5TQJee1Aw8nHyYBzoXNQCIFUc0oj0bH50
owFjJypTw2wZAAK1V8jgxAcMHyZPzKQA

- 2) Send the REQUEST CODE copied to the Service via email.
- 3) Wait for the RESET CODE from the Service; the User can return to this page later with another failed login with “admin” user (e.g. login: “admin” / password: “wrongpassword”).
- 4) When Service sends the RESET CODE, please paste in the “INSERT RESET CODE” field.

INSERT RESET CODE

When you receive the **RESET CODE** form the Service paste here below, then press **SUBMIT**.
(You can close this page and come back later when you will receive the code)

```
MIIEtAYJKoZIhvcNAQcCoIIEPCCBDkCAQExDzANBg1ghkgBZQMEAgEFADA7BgkqhkiG9w0BBwGg
LgQsMDA6MDI6NjM6MDk6NjA6M2U6MDI6MDA6MDg6NTM6NDM6NGU6NTQ6NGQ6NGWgggIIMIICITCC
AciegAwIBAgIUVt/i0ju5D+4TPZ0+2PGS2PqLgcowCgYIKoZIzj0EAwIwTzELMAkGA1UEBhMCSVQx
JzA1BgNVBAoMh1JQUyBEZXZpY2VzIERpZ210YWwgSWRlbnRpG11czEXMBUGA1UEawwOaW50Q0FF
```

```
9w0BCQQxIgQgWpEUA4Cjq1EN7LbHh2sGQwOS/bSkidN0lp+Yk+CAGFgweQYJKoZIhvcNAQkPMWww
ajALBglhkgBZQMEA$owCwYJYIzIAWUBAEWMA$GCWCSSAFlAwQBAjAKBggqhkiG9w0DBzAOBggq
hkiG9w0DAgICAIAwDQYIKoZIhvcNAwICAUAwBwYFkW4DAgcwDQYIKoZIhvcNAwICASgwCgYIKoZI
zj0EAwIERzBFaiBp2nEiDUiYBJ6ZjjAnHXD1Y0o8MoGYaXr+XBaw1PkyQIhAnNnAW+MTq5AxJwIV
1XoTX96b/IFBHVgg6MYjB7JXQQWB
```

SUBMIT

5) then click SUBMIT button and wait for the message:



6) Now the local user "admin" can access with default password "admin" again (-> a new password set will be requested at next login)



Please note that the RESET CODE sent is valid only for this specific NetMan 208C and not others.



Only the local "admin" password is reset to default, the other local users ("power" and "view") keep the same password if are enabled.

CONFIGURATION VIA SSH



By default, SSH is disabled on the NetMan 208C. The SSH client service can be enabled/disabled only via http.

To configure NetMan 208C via SSH it is necessary to:

- Execute an SSH client on a PC connected in a network to NetMan 208C set with the IP address of the device to be configured.
- At the login prompt, enter “admin” for user.
- At the password prompt, enter the current password of “admin” user.

```
-----  
netmannicola.local - Netman 208C  
-----  
admin@netman [REDACTED].local's password:
```



No characters are displayed while typing the password.



For proper configuration of NetMan 208C, you must configure the SSH client so that the backspace key sends "Control-H".
Please verify the keyboard options of your SSH client.

After login with correct password, the screen of the start menu is displayed. From this screen it is possible to access to the “Main Menu” to change NetMan 208C settings.

Main menu

```

/-----/
|       Netman      |
/-----/
```

Setup.....: <--

View status....:

Change password:

Factory reset...:

Expert mode....:

hostname netman [REDACTED]

Press [ESC] for logout

SysVer. 2.0 - AppVer. [REDACTED]

| Function | Description |
|-----------------|---|
| Setup | To enter IP configuration menu |
| View status | To see the status of the device |
| Change password | To modify the password of "admin" user |
| Factory reset | To restore factory configuration |
| Expert mode | To enter Expert mode (more information at paragraph " <i>Expert mode</i> ") |

To move within this menu and the following menus, use the keys as described in the following table the arrow or the cursor shows the current selection.

| Key | Function |
|---|-------------------------------------|
| Direction keys (arrows: up ↑, down ↓, left ←, right →) | To move the cursor within the menus |
| Tab | Goes on to next option |
| Enter ⁽¹⁾ | Choice of submenu |
| | Confirmation of characters entered |
| Esc ^{(1) (2)} | Exit main menu ⁽²⁾ |
| | Return to previous menu |

⁽¹⁾ Some keys may have different functionality depending on the menu.

⁽²⁾ To exit from a menu a confirmation ('Y' or 'N') is required after pressing the ESC key.

Setup

The main configuration menu displays a screen like the following:

```
/-----/  
|       Setup       |  
/-----/  
  
IP config.....:<--  
Reboot.....:  
  
Press [Esc] to quit  
SysVer. 2.0 - AppVer. [REDACTED] - Data from flash
```

From this main menu it is possible to access the various submenus, the function of each of which is shown in the table below.

| Menu | Function |
|-----------|-------------------------------------|
| IP config | To configure the network parameters |
| Reboot | Reboots the NetMan 208C |

IP config

```
/-----/  
/      IP config      /  
/-----/  
  
IP address/DHCP:DHCP  
  
Netmask.....:  
  
Gateway.....:  
  
Primary DNS....:  
  
Secondary DNS...:  
  
  
Press [Esc] to quit  
SysVer. 2.0 - AppVer. [REDACTED] - Data from flash
```

With this menu the main network parameters can be set as described in the following table.

| Field | Parameters to be entered |
|-----------------|--|
| IP address/DHCP | Enter the IP address for a static IP (e.g. “10.1.50.27”) Enter “DHCP” for a always requesting dynamic IP from a DHCP Server (-> “DHCP”) |
| Netmask | Enter the netmask to be used together with the static IP address (e.g. “255.255.255.0”) |
| Gateway | Enter the name or the address of the network gateway (e.g. “10.1.50.1”) |
| Primary DNS | Enter the name or the address of the preferred DNS to be used (e.g. “10.1.50.252”) |
| Secondary DNS | Enter the name or the address of the alternative DNS to be used (e.g. “10.1.50.253”) |



If a static IP address is assigned to the device, all the fields must be configured with the network parameters. If a dynamic IP address is assigned, just enter ‘DHCP’ in the “IP Address/DHCP” field; all the other options should be ignored because these are automatically configured with DHCP.

Expert mode

Expert mode enables the configuration of advanced parameters that should be set by skilled technicians. These commands are supported:

```
Netman maintenance console
Available commands:
help           prints this help
get            shows all values
set <VAR> <VALUE>    set VAR to VALUE
delete <VAR>       removes VAR
sendtrap + <TRAPCODE> send a test SNMP trap (alarm added)
sendtrap - <TRAPCODE> send a test SNMP trap (alarm removed)
testemail      send a test email
testwol        send the wake-on-lan packets
reboot         reboot the Netman
clearlog       clear data log and event log
exit           closes the connection

netman>
```



Any operation in Expert Mode may lead to malfunction or critical states with the NetMan 208C; please operate in this menu only when specifically requested from the Service of by detailed instructions given

UPLOAD / MAINTENANCE MODE

Netman208 UPLOAD MODE Hostname: netman6309603e 19-11-2025 13:00

MAC Address: 00:02:63:09:60:3e Systemapi: armhf-bullseye-2

System Virtual Machine Application Restore network Network Compatibility Certificates User Code

Activations System Integrity Reset to Default Reboot to Normal Mode

System Image

Drag or Select image file with extension ".sys208"... then Upload procedure will start.

Please drop here the file .sys208 to upload...
or select manually from

Select image file

Ready

Upload / Maintenance Mode is meant:

- Upload firmware to the NetMan 208C
- Network settings operations (restoring network and compatibility)
- Firmware certificate update
- Other special operations



As a maintenance mode, it should be used only when strictly necessary and then return to NORMAL MODE.

How to access to **UPLOAD MODE**:

- from NORMAL MODE, menu ADMINISTRATION → Firmware Upgrade → Reboot for UPLOAD a FIRMWARE

How to access to **MAINTENANCE MODE**:

- press physical RESET BUTTON on the NetMan 208C for >12 seconds

or:

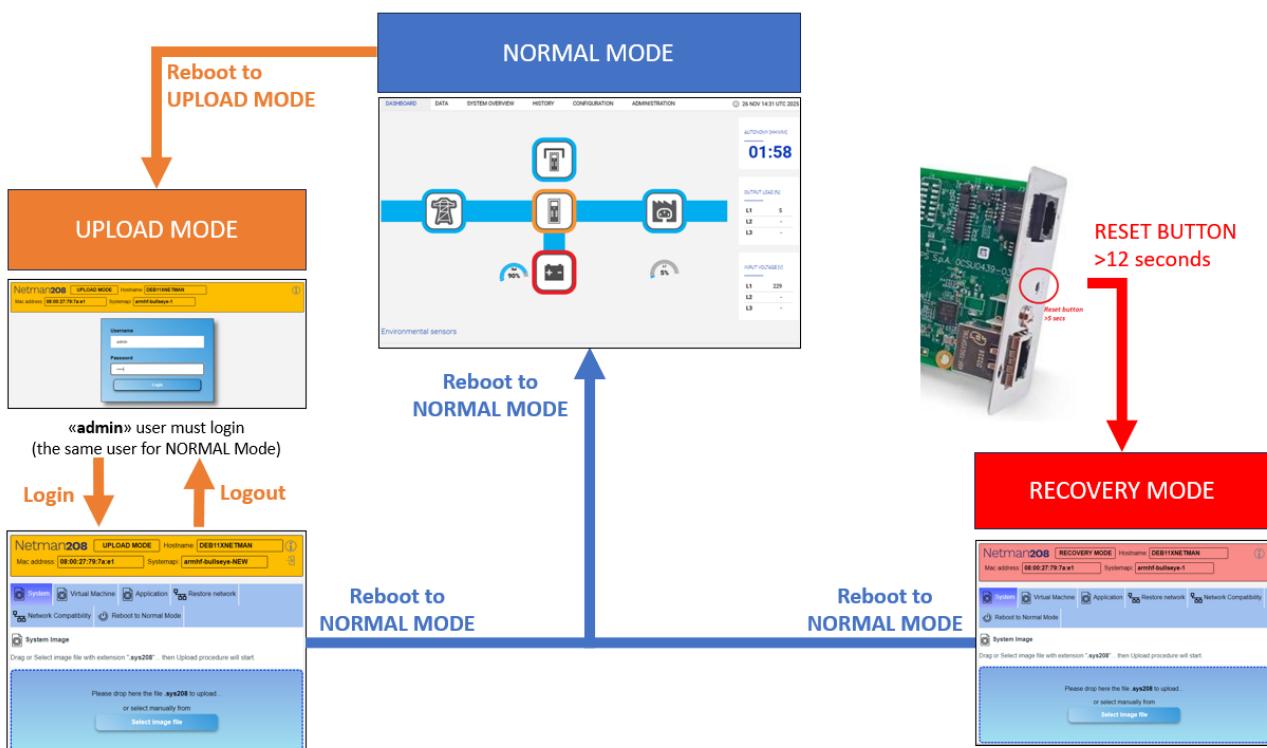
- when NORMAL APPLICATION detects issues on booting, it jumps to MAINTENANCE MODE

How to access to **NORMAL MODE**:

- From UPLOAD/RECOVERY: menu “Reboot to Normal Mode” → Click to reboot to Normal Mode

The main differences between UPLOAD MODE and MAINTENANCE MODE:

| MODE | Parameters to be entered |
|------------------|--|
| UPLOAD MODE | A login is required with “admin” user and its password. Web connection: HTTP or HTTPS (the same set in the NORMAL MODE). |
| MAINTENANCE MODE | No login requested, direct access to menu. The reset button pressing required must be executed physically by user action on the NetMan 208C device. Web connection: only HTTP. |



From UPLOAD/MAINTENANCE MODE it is possible to:

- Upload a new firmware (with “System”, “Virtual Machine” and “Application” file images)

| MODE | Parameters to be entered |
|-----------------|---------------------------|
| System | Upload a new SYS firmware |
| Virtual Machine | Upload a new JVM firmware |
| Application | Upload a new APP firmware |

It is also possible to execute other maintenance operations:

| MODE | Parameters to be entered |
|------------------------------|---|
| Restore Network | restore the network configuration to the Default |
| Network Compatibility | set for special network settings (speed compatibility 10/100/1000 Mbps) for solving network problems |
| Certificates | load new signer certificates for validation of the firmware |
| User Code | enter codes for custom operations (when needed, it requires <i>Service support</i>) |
| Activations | activate specific functionalities (when needed, it requires <i>Service support</i>) |
| System Integrity | check the integrity and the authenticity of NetMan 208C firmware |
| Reset to default | reset to default NetMan 208C deleting any configuration and parameters restoring NetMan 208C to its default status (in case of emergency or for disposal) |
| Reboot to Normal Mode | reboot to Normal Mode |

Firmware update

NetMan 208C has three different types of firmware:

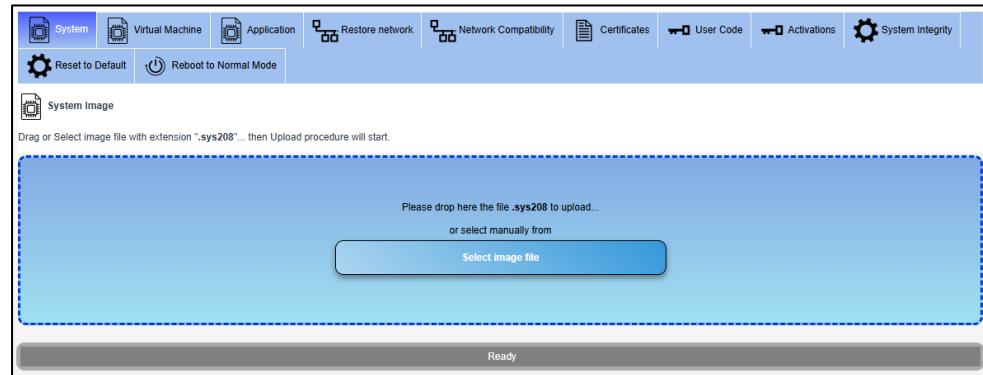
| Firmware type | Description | Normal updates availability |
|------------------------|--|-----------------------------|
| Application | What the User really use and interacts with (Web application). | More frequent updates |
| System | The basic Operating System. | Less frequent updates |
| Virtual Machine | Required for both the "System" and "Application" components. | Rarely or never |

Each firmware component is provided with two files, both of which are required for update.

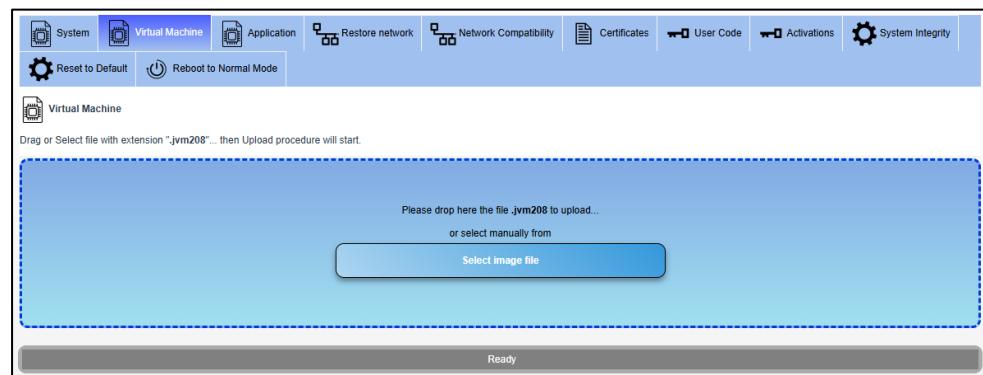
| Firmware type | Provided files |
|------------------------|---|
| Application | fw208-vvrr.app208 fw208-vvrr-JSON.json |
| System | fw208-vvrr.app208 fw208-vvrr-JSON.json |
| Virtual Machine | fw208-vvrr.jvm208 fw208-vvrr-JSON.json |

Every firmware component must be loaded from their specific tab:

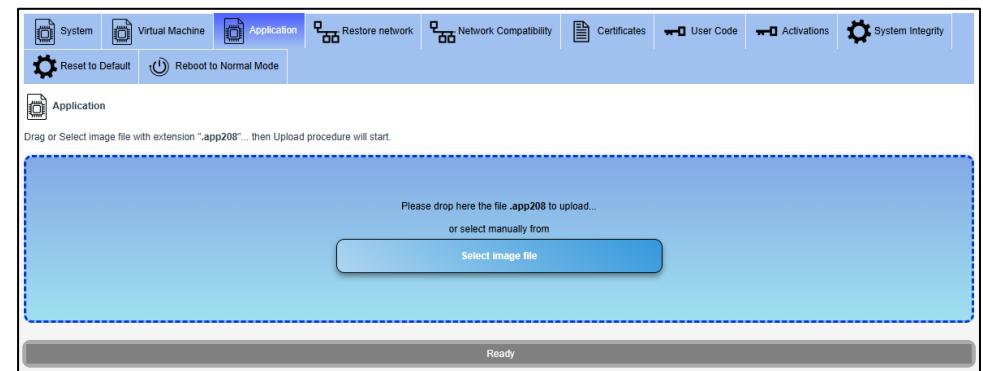
System



Virtual Machine



Application



It is recommended to avoid uploading the firmware directly from a network server.
How to proceed:

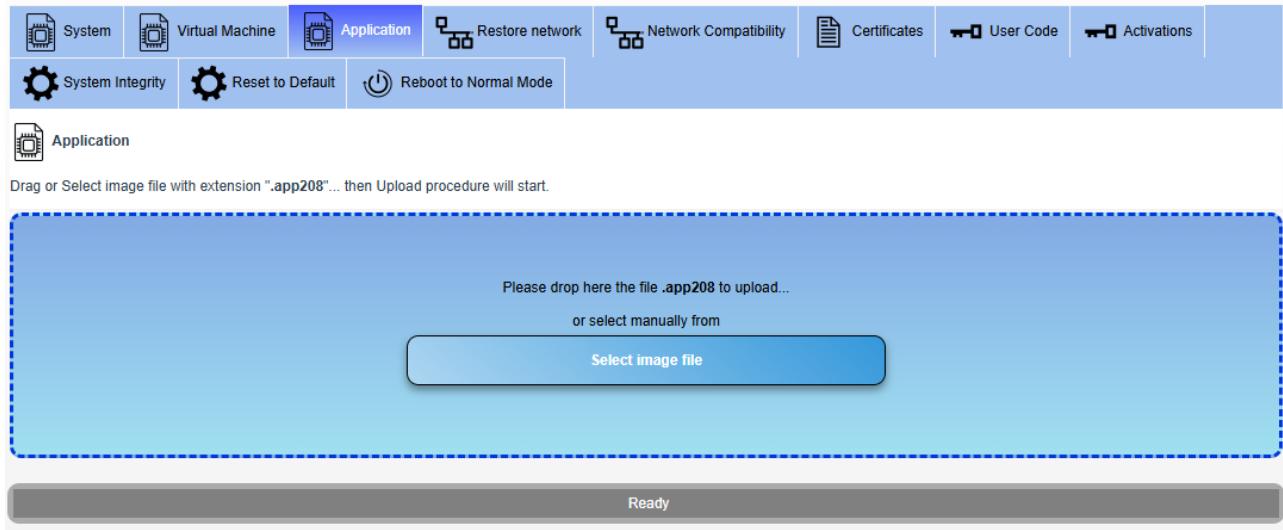


- First copy the image firmware file to a local storage on the computer.
- Then upload the file to NetMan 208C.

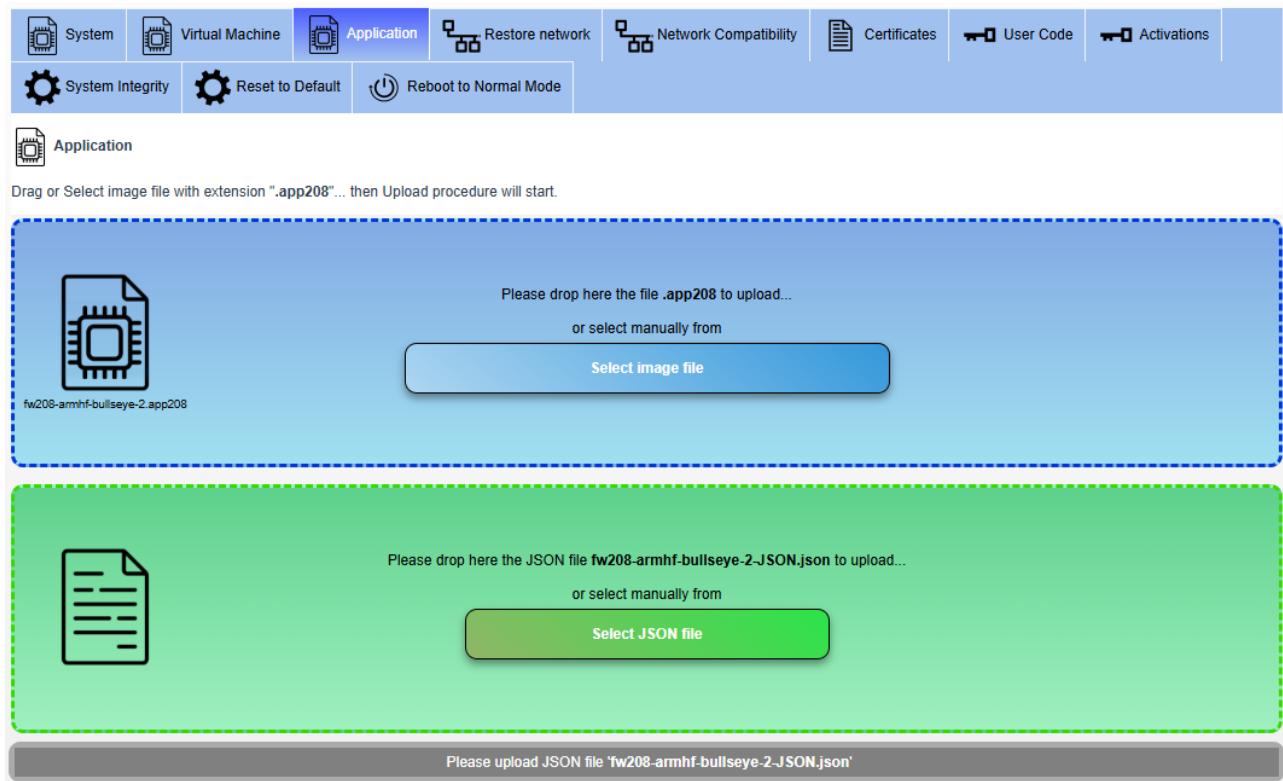
The upload process is the same for **“System”**, **“Virtual Machine”** and **“Application”**.

E.g.: upload a new firmware “Application”

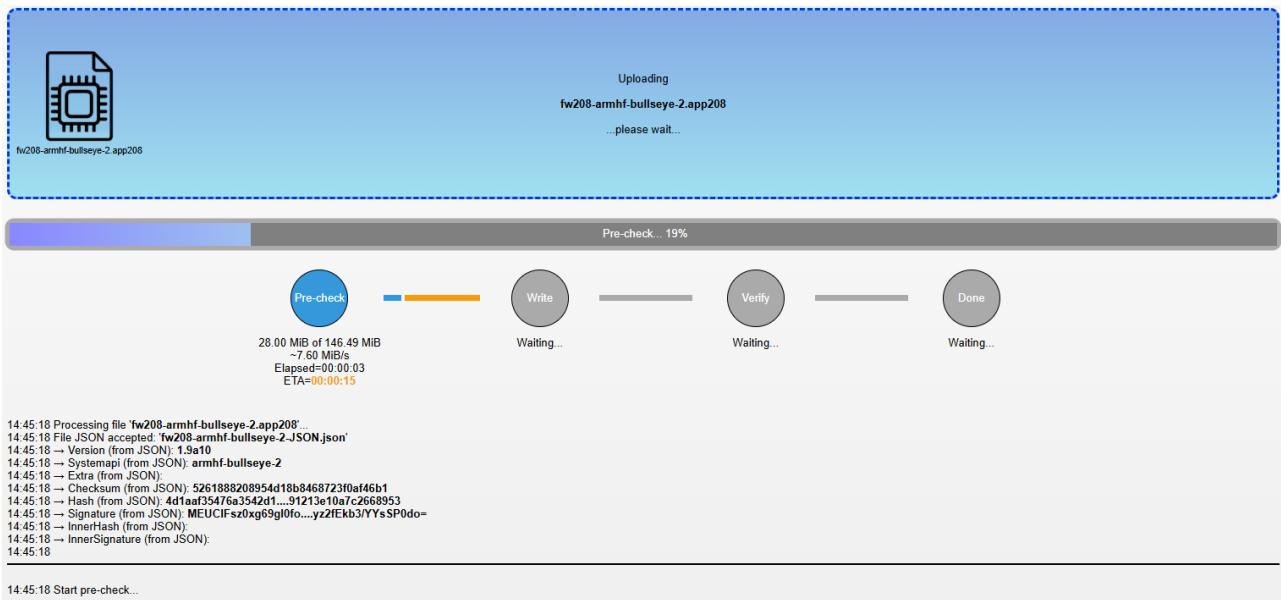
- 1) Select the firmware image file to upload (e.g.: “fw208-vvrr.app208”):



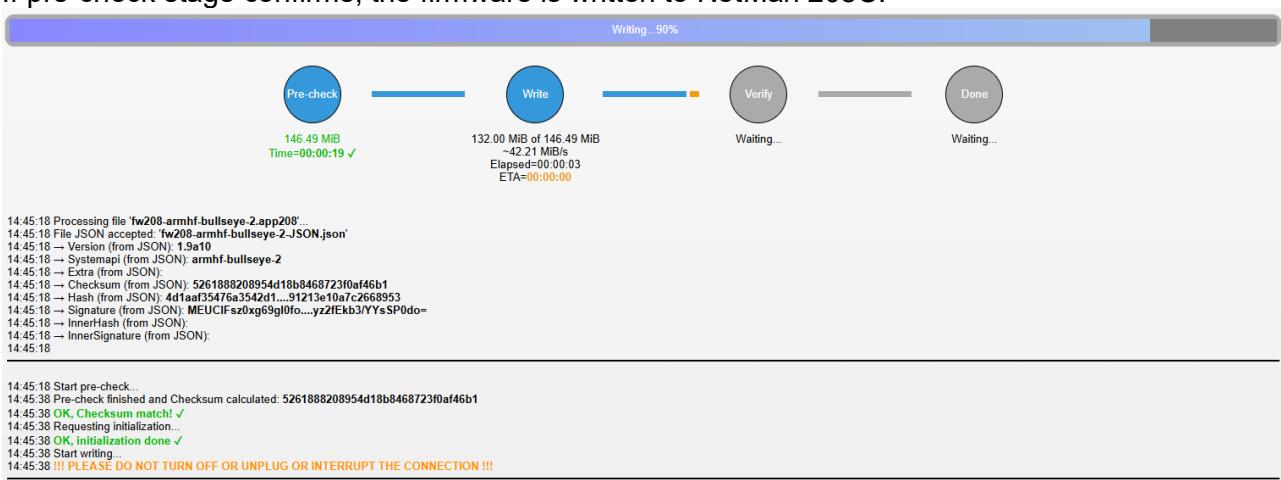
- 2) if requested select the JSON file (e.g.: “fw208-vvrr-JSON.json”):



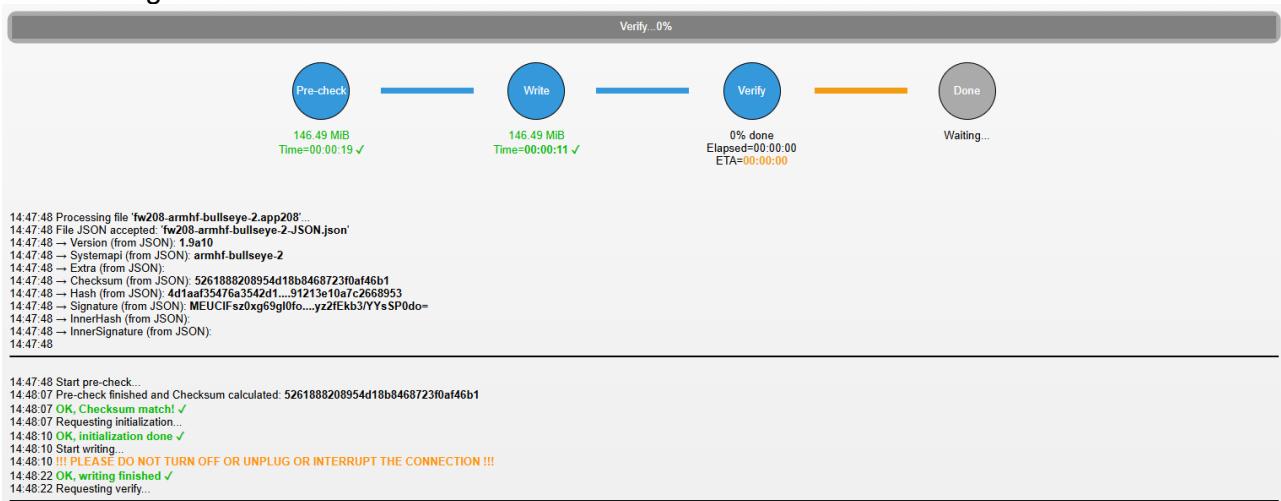
3) After the upload, the web page proceeds to pre-check the firmware:



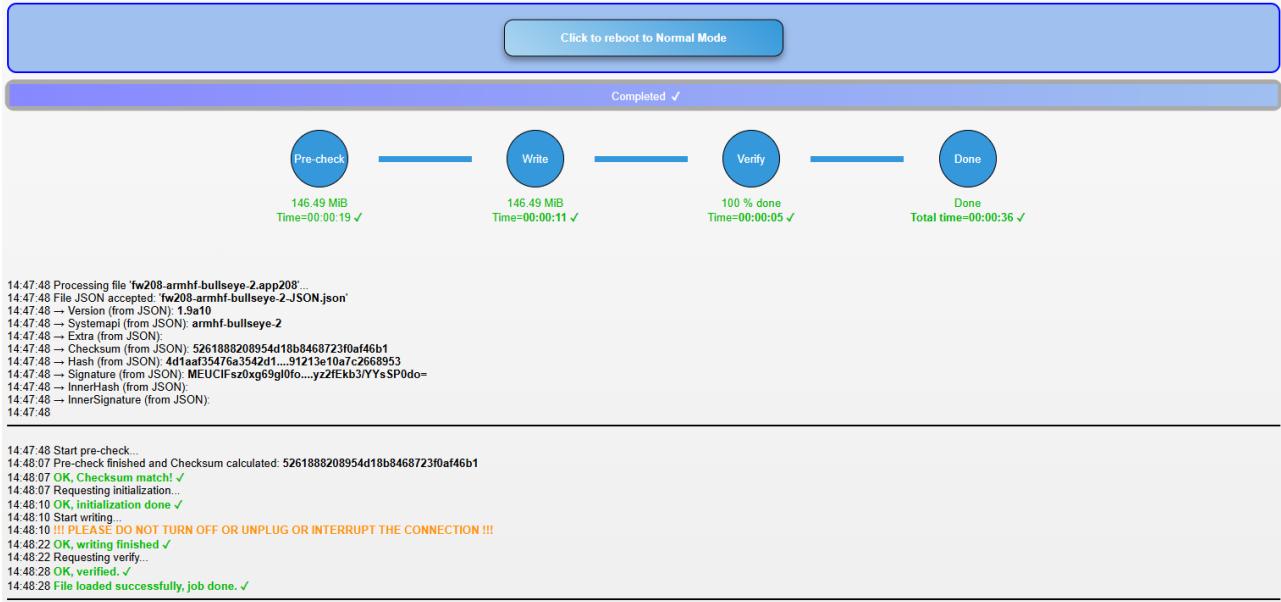
4) If pre-check stage confirms, the firmware is written to NetMan 208C:



5) As final stage the firmware is validated:

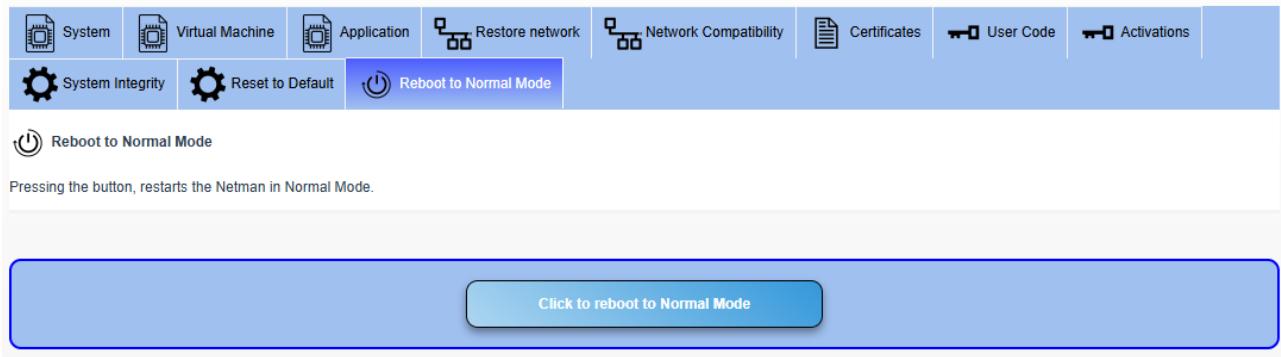


6) After all the verifications, the process confirms with success:



7) At the end, the User can upload other firmwares.

8) After all firmware updates the User can reboot the NetMan 208C to Normal Mode



After new firmware upload: web browser cache issues

Each web browsers may keep the previous version of a web page of the NetMan 208C saved in cache.

Effects of this browser behaviour may be:

- Web buttons (login) or links not working as expected
- Old or wrong web page shown instead of the new one expected

For solving this temporary issue, in the Web Browser the User can:

- press key **F5**
- press key **Shift + F5**
- press key **Control + F5**
- close and re-open the web browser
- change web browser

Firmware updates order

Firmware update usually requires updating only APPLICATION firmware:

| <i>Update order</i> | <i>Type</i> | <i>File</i> |
|---------------------|--------------------|---|
| 1 | Application | fw208-vvrr.app208 fw208-vvrr-JSON.json |

Less frequent update requires the upload of SYS + APP firmware with specific order:

| <i>Update order</i> | <i>Type</i> | <i>File</i> |
|---------------------|--------------------|---|
| 1 | System (*) | fw208-vvrr.sys208 fw208-vvrr-JSON.json |
| 2 | Application | fw208-vvrr.app208 fw208-vvrr-JSON.json |

(*) uploading

In case of boot issues, can be requested to upload the Virtual Machine:

| <i>Update order</i> | <i>Type</i> | <i>File</i> |
|---------------------|------------------------|---|
| 1 | Virtual Machine | fw208-vvrr.jvm208 fw208-vvrr-JSON.json |

In the worst scenario, a full upload of all the three firmware is required:

| <i>Update order</i> | <i>Type</i> | <i>File</i> |
|---------------------|------------------------|---|
| 1 | System | fw208-vvrr.sys208 fw208-vvrr-JSON.json |
| 2 | Application | fw208-vvrr.app208 fw208-vvrr-JSON.json |
| 3 | Virtual Machine | fw208-vvrr.jvm208 fw208-vvrr-JSON.json |

PROCEDURES

RESET BUTTON

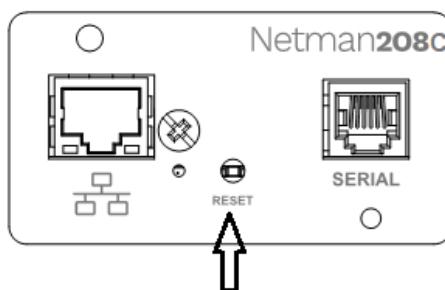
When the NetMan 208C:

- is no more reachable (due to wrong configuration).
- does not respond to web or to other requests (e.g. SSH).

it is possible to recall the safe “MAINTENANCE MODE” of the NetMan 208C trying to solve the issue and/or the network connection.

How to put the NetMan 208C in MAINTENANCE MODE:

- press the physical RESET BUTTON for 12 seconds



Effects:

- NetMan 208C saves logs that normally would be lost
- then NetMan 208C will reboot to the safe MAINTENANCE MODE where some rescue/reset operations are possible
- MAINTENANCE MODE does not require login access and is reachable with HTTP connection (not HTTPS)

A screenshot of the Netman208 web interface. The top bar is red and displays the device name 'Netman208', 'RECOVERY MODE', 'Hostname: netmannicola', 'MAC Address: 00:02:63:09:60:3e', and the date '25-11-2025 14:43'. Below this is a blue navigation bar with icons for System, Virtual Machine, Application, Restore network, Network Compatibility, Certificates, User Code, Activations, System Integrity, Reset to Default, and Reboot to Normal Mode. A gear icon is also present. The main content area is light blue and contains a 'System Image' section with a note to drag or select an image file. A dashed blue box highlights a central upload area with the text 'Please drop here the file .sys208 to upload...' and 'or select manually from'. A 'Select image file' button is shown. At the bottom of the page, a grey bar displays the word 'Ready'.

Possible rescue operations:

| | |
|-------------------------------------|---|
| <i>Upload a new firmware</i> | Firmware for System / Virtual Machine / Application can be uploaded for fixing some issues. |
| <i>Restore network</i> | Restore/set the network to DHCP. Useful when NetMan 208C network address is unknown. |
| <i>Network compatibility</i> | For some network switches can be useful to lower the network speed of NetMan 208C to 100 Mbps or 10 Mbps. |
| <i>Reset to Default</i> | Reset the whole NetMan 208C configuration to the default: any user setting is lost. |

After the rescue operations:

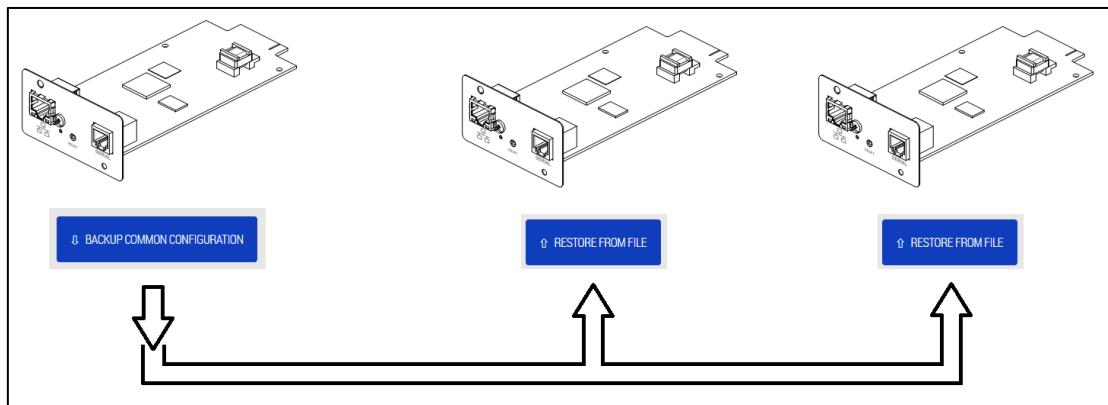
→ Reboot to Normal Mode to restart the normal Application execution.

CONFIGURATION OF SEVERAL DEVICES

If several NetMan 208C must be configured with similar parameters, you can configure the first NetMan 208C with all basic common parameters, then backup the COMMON configuration and finally RESTORE the saved configuration to other NetMan 208C: the common parameters are restored. Only the critical parameters are not restored (e.g. network configuration, passwords, critical data, ...) due to protect the confidential data saved in NetMan 208C.

Please follow the upper section menu in the manual for more details:

ADMINISTRATION -> BACKUP/RESTORE CONFIGURATION



DASHBOARD DATA SYSTEM OVERVIEW HISTORY CONFIGURATION **ADMINISTRATION**

ADMINISTRATION DEVICE COMMANDS DIAGNOSTIC

ADMINISTRATION

- Automatic Check for Updates
- Firmware upgrade
- Certificates and Keys
- Backup/Restore Configuration**
- Reset to defaults
- Reset Log
- Reboot
- Change local password
- Login access
- Login rules
- Web Login banner
- SSH Login banner

Restore Configuration

Click the button and select the configuration file to Restore

RESTORE FROM FILE

It is possible to restore the *Common configuration* or the *Complete configuration* saved before.

Backup Configuration

BACKUP COMMON CONFIGURATION

BACKUP COMPLETE CONFIGURATION

BACKUP COMMON CONFIGURATION

Save this file for a backup of the common configuration parameters; it can be used to restore or copy the **common parameters** to **this or other Netman 208 cards**.

BACKUP COMPLETE CONFIGURATION

Save this file for a full backup of **this Netman 208**; this backup can restore the **full configuration** only for **this Netman 208** (and not for others).

MONITORING RESOURCES

During normal execution the system is monitored from dedicated internal processes. When normal conditions are not met, some messages are shown to the User.

System Storage and Memory

Messages as warnings shown on the Web page:

| | Monitoring rule | Web Message |
|-----------------------|---------------------------------|--|
| System Storage | Storage space left < 5% |  LOW SPACE LEFT ON DEVICE |
| | Storage space left < 2% |  VERY LOW SPACE LEFT ON DEVICE |
| System Memory | Memory free left < 10 Mb |  LOW FREE MEMORY LEFT ON DEVICE |
| | Memory free left < 5 Mb |  VERY LOW FREE MEMORY LEFT ON DEVICE |

INTERNAL LOGS

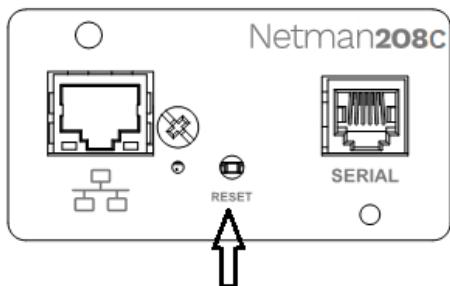
NetMan 208C manages different kinds of logs:

| | |
|--|--|
| Runtime logs | These logs are kept in memory and are lost when NetMan 208C is rebooted or powered off. |
| Static logs (with log rotation) | <p>These logs are saved in static internal files and are <u>not lost</u> when NetMan 208C is rebooted or powered off.</p> <p>Log rotation</p> <p>Static logs are rotated to keep a maximum value of storage size; in case of huge log data written, please download or check the logs more frequently avoiding the loss of the oldest data.</p> |
| Latest logs | <p>Latest logs (last hours events) are managed in a mixed mode:</p> <ul style="list-style-type: none">- for the first hours or day are saved as Runtime logs: latest events are kept only in memory.- after predefined time the Runtime logs are saved as Static logs. |

In case of NetMan 208C is no more responding, before rebooting or powering off, it is possible to save the **Runtime logs**, useful for issue analysis.

How to save the Runtime logs:

- Press the physical RESET BUTTON for 12 seconds.



This action from the User executes some actions:

- The Runtime logs in memory are saved as Static logs.
- Then the NetMan 208C reboots to "Maintenance mode" for restoring operations.
- From Maintenance Mode, the user can retry to "Reboot to Normal Mode".
- After a successful reboot to Normal Mode the User can manage the Logs available (check or Service Log download and analysis).

SERVICE LOG

DASHBOARD DATA SYSTEM OVERVIEW HISTORY CONFIGURATION ADMINISTRATION 21 NOV 17:11 UTC 2025

| DEVICE | | DEVICE CONFIGURATION | | NETWORK CARD | |
|-----------------------|------------------------|----------------------|---------------------|---------------------|--------------------------|
| Model | UOD2 | PRTK code | GPSER11201-- | Model | NetMan 208C |
| Part Number | - | Name | Netman 208C | Card version | e4400001 |
| Serial number | ME39VOD20000018 | | | Serial Number | 12345768 |
| Power [kVA] | 1.0 | | | MAC Address | 00:02:63:09:60:3e |
| Power [kW] | 0.9 | | | Application version | 1.92b4 |
| Battery capacity [Ah] | 9 | | | VM version | 2.0 |
| Battery voltage [Vdc] | 36 | | | System version | 2.0 |
| Firmware version | SWM073-01-01 | | | Recovery version | 2.0 |

| NETWORK CONFIGURATION | | | | | |
|-----------------------|--------------------------------|--------------|---------------------------------|---------------|------------------|
| Hostname | netmannicola | IPv4 Address | 10.1.11.84 | Gateway | 10.1.1.1 |
| DHCP enabled | yes | Netmask | 255.255.0.0 | Primary DNS | 10.1.5.10 |
| Network speed | 1000 Mbps (full-duplex) | IPv6 Address | fe80::202:63ff:fe09:603e | Secondary DNS | 10.3.5.3 |

[READ MANUAL](#) [LEGAL INFORMATION](#)

In case of problem or if NetMan 208C does not behave as you would expect, it is recommended to download the **service log**.

To create and download the service log do the follow:

1. Log in as “admin” user
2. Click on “System overview”
3. Click “Download service log”

SERVICE LOG

[DOWNLOAD SERVICE LOG](#)

The service log will be downloaded in a few seconds. It must be sent to your local authorized service centre to properly diagnose the problem.

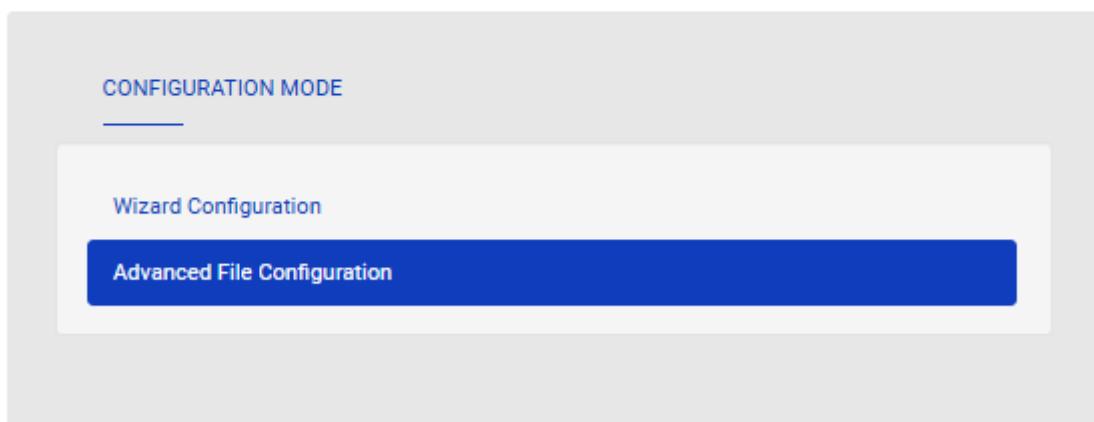
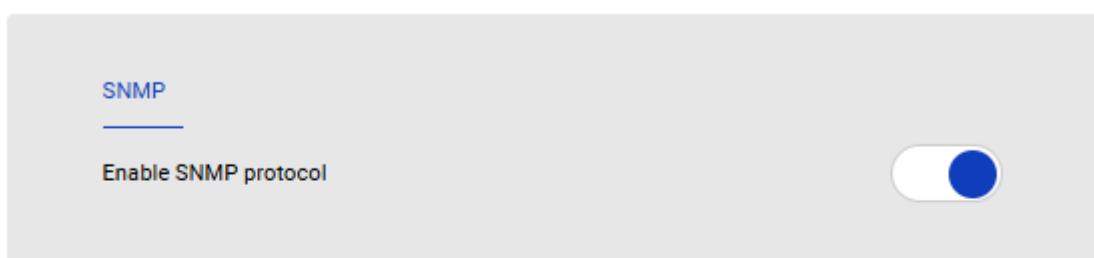
SNMP CONFIGURATION

For configuring SNMP, it is possible to use the wizard web page for a simple configuration. SNMPv3 is strongly suggested, due the weakness and vulnerabilities of the older SNMPv1/v2c version.

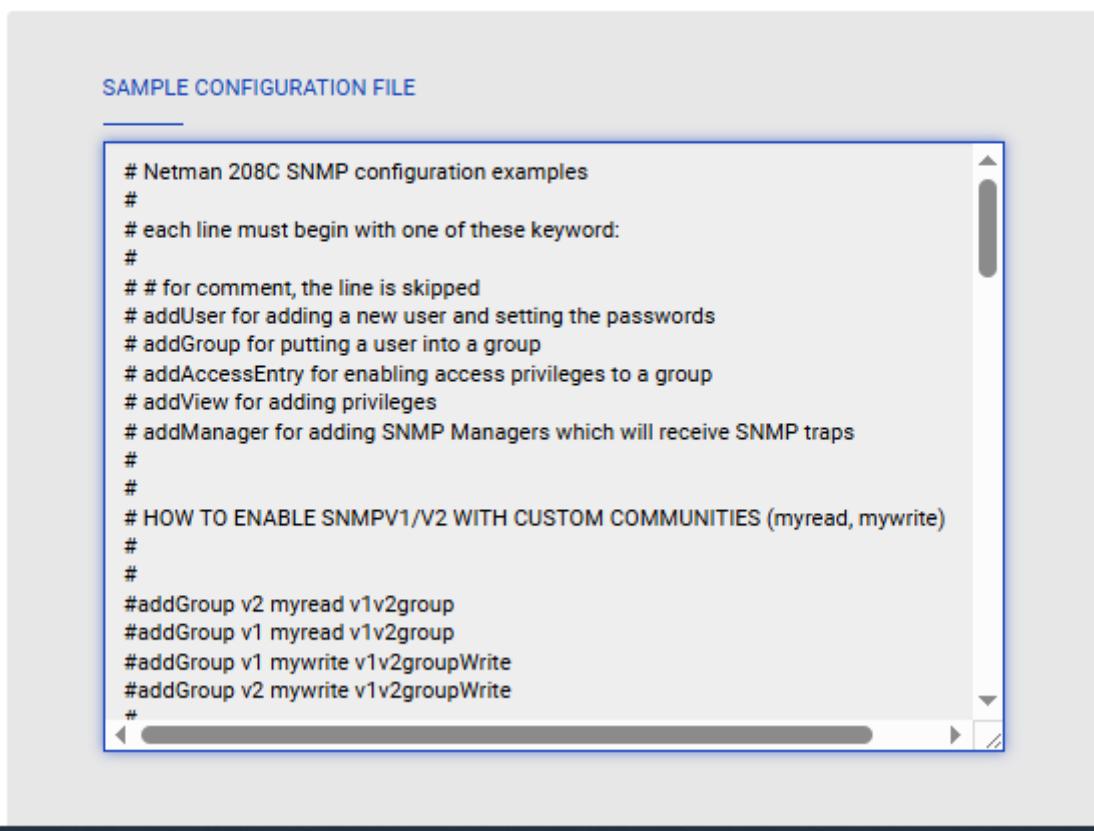
The screenshot shows a web-based configuration interface for a device. The top navigation bar includes links for DASHBOARD, DATA, SYSTEM OVERVIEW, HISTORY, **CONFIGURATION** (which is the active tab), and ADMINISTRATION. Below the navigation is a secondary navigation bar with tabs: YOUR NETMAN, SENSORS, MODEM, and REMOTE HOSTS. The main content area is divided into sections: DEVICE, NETWORK, DATE & TIME, EMAILS, and ADVANCED. The **SNMP** tab under the NETWORK section is selected. The **SNMP configuration** section contains a toggle switch for "Enable SNMP protocol" which is turned on. Below this is a "CONFIGURATION MODE" section with "Wizard Configuration" (which is highlighted in blue) and "Advanced File Configuration". The **SNMP configuration wizard** section shows the "SNMP VERSION" as "SNMP V3" (which is highlighted in blue). The **SNMP v3** section displays a table for "USERS" with columns: Username, Auth, Priv, authPassword, privPassword, and User permissions. The table contains four rows, each with a set of input fields for these parameters. To the right of the table are checkboxes for "GET", "SET", and "TRAP".

Advanced configuration is possible and requires editing `snmp.conf`. This file content can be copied from example in the web page (SNMP menu) and then the file can be uploaded to the web page.

SNMP configuration



SNMP configuration file upload



Each line of the file is parsed by NetMan 208C and must begin with one of these keywords:

- `#`: for comment, the line is skipped.
- `addUser`: for adding a new user and setting the passwords

- *addGroup*: for putting a user into a group
- *addAccessEntry*: for enabling access privileges to a group
- *addView*: for adding privileges
- *addManager*: for adding SNMP Manager which will receive SNMP traps.

The correct syntax for *addUser* is:

addUser <userName> <authProtocol> <privProtocol> <authPassword> <privPassword>

<userName> is the name of the user.

<authProtocol> is the protocol for authentication of this user during SNMP sessions.

Possible values are:

- *noauth* (no authentication will be used)
- *md5* (MD5 will be used for authentication)
- *sha* (SHA will be used for authentication)

<privProtocol> is the protocol for privacy of this user during SNMP sessions. Possible values are:

- *nopriv* (no privacy will be used)
- *des* (DES will be used for privacy)
- *aes128* (AES with 128-bit key)
- *aes192* (AES with 192-bit key)
- *aes256* (AES with 256-bit key)

<authPassword> is the password for authentication; it must be set to * when not used.

<privPassword> is the password for privacy; it must be set to * when not used.

The correct syntax for *addGroup* is:

addGroup <securityModel> <userName> <groupName>

<securityModel> is the security model. When using authentication and/or privacy, *securityModel* must be USM. Possible values are:

- *USM* (User-based Security Model with SNMPv3)
- *v2* (SNMPv2)
- *v1* (SNMPv1)

<userName> is the name of the user, must match one of the user name defined with *addUser*.

<groupName> is the name of the group.

Please note that a username can be assigned to only one group.

The correct syntax for *addAccessEntry* is:

addAccessEntry <groupName> <contextName> <securityModel> <securityType> <contextMatch> <readView> <writeView> <notifyView>

<groupName> is the name of the group to which this access right applies, must match one of the group name defined with *addGroup*.

<contextName> is the name of the context.

<securityModel> is the security model that must be used in order to gain access to this access right, must match the security model defined with *addGroup*.

<securityType> is the minimum security level that must be used to gain access to this access right. Possible values are:

- *noauthnopriv* (no authentication and no privacy)
- *authnopriv* (authentication but no privacy)
- *authpriv* (authentication and privacy)

<contextMatch> the type of match required. Possible values are:

- *exact* (the context name must exactly match the value in contextName)
- *prefix* (the context name must match the first few starting characters of the value in contextName)

<readView> the authorized MIB view name used for read access, must match one of the view name.

<writeView> the authorized MIB view name used for write access, must match one of the view name.

<notifyView> the authorized MIB view name used for notify access, must match one of the view name.

The correct syntax for addView is:

addView <viewName> <subtree> <mask> <included>

<viewName> is the name of the view.

<subtree> is the OID subtree which when combined with the corresponding instance of MASK defines a family of view subtrees.

<mask> the mask for filtering OID.

<included> the OID can be included or excluded. Possible values are:

- *included* (for including)
- *excluded* (for excluding)

The correct syntax for addManager is:

addManager <security> <ipAddress> <credentials> <securityType>

<security> is the security type for the notification. Possible values are:

- *USM* (User-based Security Model with SNMPv3)
- *v2* (SNMPv2)
- *v1* (SNMPv1)

<ipAddress> is the IP address of the SNMP manager.

<credentials> is either the username (when using USM security) or the trap community (when using v1 security)

<securityType> is either:

- *noauthnopriv* (for SNMPv1 and SNMPv2)
- *authpriv* (for SNMPv3)

addManager do not allow duplicate entries (one ipAddress can receive only one trap).

A sample *snmp.conf* is provided; the default users authorized are:

| Name | Auth protocol | Priv protocol | Auth password | Priv password |
|--------------|---------------|---------------|------------------------|------------------------|
| unsecureUser | Noauth | nopriv | | |
| MD5 | md5 | nopriv | MD5UserAuthPassword | |
| SHA | Sha | nopriv | SHAUserAuthPassword | |
| MD5DES | md5 | des | MD5DESUserAuthPassword | MD5DESUserPrivPassword |
| SHADES | Sha | des | SHADESUserAuthPassword | SHADESUserPrivPassword |

Trap explanation:

| OID | Description |
|----------------------|---|
| 1.3.6.1.2.1.33.2.0.1 | Sent whenever the UPS transfers on battery, then sent every minute until the UPS Comes back to AC Input |
| 1.3.6.1.2.1.33.2.0.3 | Sent whenever an alarm appears, the matching alarm oid is added as binded variables in the alarm table |
| 1.3.6.1.2.1.33.2.0.4 | Sent whenever an alarm disappears, the matching alarm oid is added as binded variables in the alarm table |

NetMan 208C Specific Traps oIDs

Single oID sent from the NetMan 208C:

| OID | Description |
|--|-----------------------|
| 1.3.6.1.2.1.1.3.0 = 0:12:40.96 | Time |
| 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.2.1.33.2.3 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.4.1.5491.10.2.3 | Alarm add (3) |
| 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.2.1.33.2.4 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.4.1.5491.10.2.4 | Alarm removed (4) |
| 1.3.6.1.2.1.33.1.6.2.1.1 = 0 1.3.6.1.4.1.5491.10.1.6.2.1.1 = 0 | upsAlarmld |
| 1.3.6.1.2.1.33.1.6.2.1.2 = 1.3.6.1.2.1.33.1.6.3.# 1.3.6.1.4.1.5491.10.1.6.2.1.2 = 1.3.6.1.4.1.5491.10.1.6.3.# | Trap number # (1..24) |

Complete Trap oIDs table:

| Trap | Alarm ADD (oIDs) | Alarm REMOVED oIDs |
|-------------------------|---|---|
| TRAP 1 (Battery Bad) | 1.3.6.1.2.1.1.3.0 = 0:12:40.96 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.4.1.5491.10.2.3 1.3.6.1.4.1.5491.10.1.6.2.1.1 = 0 1.3.6.1.4.1.5491.10.1.6.2.1.2 = 1.3.6.1.4.1.5491.10.1.6.3.1 | 1.3.6.1.2.1.1.3.0 = 0:14:03.78 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.4.1.5491.10.2.4 1.3.6.1.4.1.5491.10.1.6.2.1.1 = 0 1.3.6.1.4.1.5491.10.1.6.2.1.2 = 1.3.6.1.4.1.5491.10.1.6.3.1 |
| | 1.3.6.1.2.1.1.3.0 = 0:12:40.95 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.2.1.33.2.3 1.3.6.1.2.1.33.1.6.2.1.1 = 0 1.3.6.1.2.1.33.1.6.2.1.2 = 1.3.6.1.2.1.33.1.6.3.1 | 1.3.6.1.2.1.1.3.0 = 0:14:03.78 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.2.1.33.2.4 1.3.6.1.2.1.33.1.6.2.1.1 = 0 1.3.6.1.2.1.33.1.6.2.1.2 = 1.3.6.1.2.1.33.1.6.3.1 |
| TRAP 2 (On Battery) | 1.3.6.1.2.1.1.3.0 = 0:10:50.61 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.4.1.5491.10.2.3 1.3.6.1.4.1.5491.10.1.6.2.1.1 = 0 1.3.6.1.4.1.5491.10.1.6.2.1.2 = 1.3.6.1.4.1.5491.10.1.6.3.2 | 1.3.6.1.2.1.1.3.0 = 0:15:26.86 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.4.1.5491.10.2.4 1.3.6.1.4.1.5491.10.1.6.2.1.1 = 0 1.3.6.1.4.1.5491.10.1.6.2.1.2 = 1.3.6.1.4.1.5491.10.1.6.3.2 |
| | 1.3.6.1.2.1.1.3.0 = 0:10:50.61 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.2.1.33.2.3 1.3.6.1.2.1.33.1.6.2.1.1 = 0 1.3.6.1.2.1.33.1.6.2.1.2 = 1.3.6.1.2.1.33.1.6.3.2 | 1.3.6.1.2.1.1.3.0 = 0:15:26.86 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.2.1.33.2.4 1.3.6.1.2.1.33.1.6.2.1.1 = 0 1.3.6.1.2.1.33.1.6.2.1.2 = 1.3.6.1.2.1.33.1.6.3.2 |
| TRAP 3 (Low Battery) | 1.3.6.1.2.1.1.3.0 = 0:07:49.43 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.4.1.5491.10.2.3 1.3.6.1.4.1.5491.10.1.6.2.1.1 = 0 1.3.6.1.4.1.5491.10.1.6.2.1.2 = 1.3.6.1.4.1.5491.10.1.6.3.3 | 1.3.6.1.2.1.1.3.0 = 0:22:10.20 1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.4.1.5491.10.2.4 1.3.6.1.4.1.5491.10.1.6.2.1.1 = 0 1.3.6.1.4.1.5491.10.1.6.2.1.2 = 1.3.6.1.4.1.5491.10.1.6.3.3 |

MODBUS TCP/IP PROTOCOL

This service is active on the TCP port 502.



The specific modbus tables reporting alarms and measurements related to your UPS family, can be downloaded from the manufacturer's website.

BACNET/IP CONFIGURATION

| OBJECT | DESCRIPTION | UNIT |
|-------------------|----------------------------|-----------------------|
| Analogue Input 0 | Input voltage line 1 | V |
| Analogue Input 1 | Input voltage line 2 | V |
| Analogue Input 2 | Input voltage line 3 | V |
| Analogue Input 3 | Input current line 1 | A |
| Analogue Input 4 | Input current line 2 | A |
| Analogue Input 5 | Input current line 3 | A |
| Analogue Input 6 | Input frequency | Hz |
| Analogue Input 7 | Bypass voltage line 1 | V |
| Analogue Input 8 | Bypass voltage line 2 | V |
| Analogue Input 9 | Bypass voltage line 3 | V |
| Analogue Input 10 | Bypass frequency | Hz |
| Analogue Input 11 | Output voltage line 1 | V |
| Analogue Input 12 | Output voltage line 2 | V |
| Analogue Input 13 | Output voltage line 3 | V |
| Analogue Input 14 | Output current line 1 | A |
| Analogue Input 15 | Output current line 2 | A |
| Analogue Input 16 | Output current line 3 | A |
| Analogue Input 17 | Output peak current line 1 | A |
| Analogue Input 18 | Output peak current line 2 | A |
| Analogue Input 19 | Output peak current line 3 | A |
| Analogue Input 20 | Output power line 1 | W |
| Analogue Input 21 | Output power line 2 | W |
| Analogue Input 22 | Output power line 3 | W |
| Analogue Input 23 | Output frequency | Hz |
| Analogue Input 24 | Output load line 1 | % |
| Analogue Input 25 | Output load line 2 | % |
| Analogue Input 26 | Output load line 3 | % |
| Analogue Input 27 | Battery voltage | V |
| Analogue Input 28 | Battery current | A |
| Analogue Input 29 | Battery capacity | % |
| Analogue Input 30 | UPS temperature | °C |
| Analogue Input 31 | Autonomy | min |
| Analogue Input 32 | Nominal power | VA |
| Analogue Input 33 | Temperature sensor 1 | °C |
| Analogue Input 34 | Humidity sensor 1 | % |
| Analogue Input 35 | Temperature sensor 2 | °C |
| Analogue Input 36 | Humidity sensor 2 | % |
| Analogue Input 37 | Temperature sensor 3 | °C |
| Analogue Input 38 | Humidity sensor 3 | % |
| Analogue Input 39 | --- NOT USED --- | --- NOT USED --- |
| Analogue Input 40 | --- NOT USED --- | --- NOT USED --- |
| Analogue Input 41 | --- NOT USED --- | --- NOT USED --- |
| Analogue Input 42 | --- NOT USED --- | --- NOT USED --- |
| Analogue Input 43 | --- NOT USED --- | --- NOT USED --- |
| Analogue Input 44 | --- NOT USED --- | --- NOT USED --- |
| Binary Input 0 | Mains status | Present / Not present |
| Binary Input 1 | Bypass status | Active / Not active |
| Binary Input 2 | Battery status | Working / Not working |

| | | |
|-----------------|----------------------|--------------------------|
| Binary Input 3 | Battery level | Low / Not low |
| Binary Input 4 | UPS locked | Locked / Not locked |
| Binary Input 5 | UPS fail | Fail / Not fail |
| Binary Input 6 | Load | Overload / Normal |
| Binary Input 7 | Temperature | Overtemperature / Normal |
| Binary Input 8 | Bypass bad | Bad / Not bad |
| Binary Input 9 | Replace battery | Replace / Not replace |
| Binary Input 10 | Shutdown | Active / Not active |
| Binary Input 11 | Shutdown imminent | Imminent / Not imminent |
| Binary Input 12 | Communication status | Lost / OK |
| Binary Input 13 | Digital input 1 | 0/1 |
| Binary Input 14 | Digital output 1 | 0/1 |
| Binary Input 15 | Digital input 2 | 0/1 |
| Binary Input 16 | Digital output 2 | 0/1 |
| Binary Input 17 | Digital input 3 | 0/1 |
| Binary Input 18 | Digital output 3 | 0/1 |
| Binary Input 19 | --- NOT USED --- | --- NOT USED --- |
| Binary Input 20 | --- NOT USED --- | --- NOT USED --- |
| Binary Input 21 | --- NOT USED --- | --- NOT USED --- |
| Binary Input 22 | --- NOT USED --- | --- NOT USED --- |
| Binary Input 23 | --- NOT USED --- | --- NOT USED --- |
| Binary Input 24 | --- NOT USED --- | --- NOT USED --- |

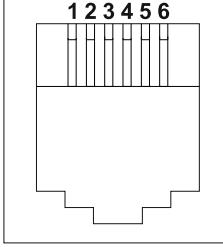
EVENTLOG CODES

| EVENT | DESCRIPTION |
|----------------------------|-----------------------------------|
| Battery low | Battery Low or Shutdown imminent |
| On battery | On battery |
| On bypass | On bypass |
| UPS lock | UPS lock |
| UPS fail | UPS failure |
| Overload | Overload |
| Overtemperature | Overtemperature |
| Output off | Output off |
| Bypass bad | Bypass bad |
| Comm lost | Communication lost |
| Battery bad | Battery bad |
| UPS generic alarm (SENTR) | UPS generic alarm (SENTR) |
| UPS internal alarm (SENTR) | UPS internal alarm (SENTR) |
| IRMS blackout | IRMS blackout |
| IRMS overload | IRMS overload |
| Synchro bad | Synchronisation wrong |
| Overload/overtemp | Overload/Overtemperature |
| xTS failure | ATS/STS failure |
| transfer active | Load Transfer active |
| source S1 bad | Source S1 bad |
| source S2 bad | Source S2 bad |
| MANUAL_BYPASS_ACTIVE_C01 | Manual bypass active |
| LOW_INPUT_VOLTAGE_A01 | Low input voltage |
| HIGH_INPUT_VOLTAGE_A02 | High input voltage |
| OVERLOAD1_F01 | Overload output 1 |
| OVERLOAD2_F02 | Overload output 2 |
| OVERLOAD3_F03 | Overload output 3 |
| OVERLOAD4_F04 | Overload output 4 |
| OVERLOAD5_F05 | Overload output 5 |
| OVERLOAD6_F06 | Overload output 6 |
| OVERLOAD7_F07 | Overload output 7 |
| OVERLOAD8_F08 | Overload output 8 |
| LOW_INPUT_CURRENT_F09 | Low input current |
| HIGH_INPUT_CURRENT_F10 | High input current |
| POWERFAIL_AUX1_F11 | Powerfail auxiliary powersupply 1 |
| POWERFAIL_AUX2_F12 | Powerfail auxiliary powersupply 2 |
| OVERLOAD_LOCK1_L01 | Lock due Overload output 1 |
| OVERLOAD_LOCK2_L02 | Lock due Overload output 2 |
| OVERLOAD_LOCK3_L03 | Lock due Overload output 3 |
| OVERLOAD_LOCK4_L04 | Lock due Overload output 4 |
| OVERLOAD_LOCK5_L05 | Lock due Overload output 5 |
| OVERLOAD_LOCK6_L06 | Lock due Overload output 6 |
| OVERLOAD_LOCK7_L07 | Lock due Overload output 7 |
| OVERLOAD_LOCK8_L08 | Lock due Overload output 8 |
| TMAX1 | Temerature high sensor 1 |
| TMIN1 | Temperature low sensor 1 |
| Input1 | Input contact sensor 1 |
| Hum1 | Humidity high sensor 1 |

| | |
|----------|--------------------------|
| Hum low1 | Humidity low sensor 1 |
| TMAX2 | Temerature high sensor 2 |
| TMIN2 | Temperature low sensor 2 |
| Input2 | Input contact sensor 2 |
| Hum2 | Humidity high sensor 2 |
| Hum low2 | Humidity low sensor 2 |
| TMAX3 | Temerature high sensor 3 |
| TMIN3 | Temperature low sensor 3 |
| Input3 | Input contact sensor 3 |
| Hum3 | Humidity high sensor 3 |
| Hum low3 | Humidity low sensor 3 |
| TMAX4 | Temerature high sensor 4 |
| TMIN4 | Temperature low sensor 4 |
| Input4 | Input contact sensor 4 |
| Hum4 | Humidity high sensor 4 |
| Hum low4 | Humidity low sensor 4 |
| TMAX5 | Temerature high sensor 5 |
| TMIN5 | Temperature low sensor 5 |
| Input5 | Input contact sensor 5 |
| Hum5 | Humidity high sensor 5 |
| Hum low5 | Humidity low sensor 5 |
| TMAX6 | Temerature high sensor 6 |
| TMIN6 | Temperature low sensor 6 |
| Input6 | Input contact sensor 6 |
| Hum6 | Humidity high sensor 6 |
| Hum low6 | Humidity low sensor 6 |

TECHNICAL DATA

SERIAL PORT PINOUT

| RJ-12 – SERIAL port | |
|---|-------------------|
|  | |
| POSITION | DESCRIPTION |
| 1 | +5V _{DC} |
| 2 | GND |
| 3 | RS232 TXD |
| 4 | RS232 RXD |
| 5 | RS485 A |
| 6 | RS485 B |

| NetMan 208C | | | Modem | | | |
|-------------|-------------------|-------------------|----------|----------|-------------|--|
| RJ-12 | | | DB-25 | DB-9 | DESCRIPTION | |
| POSITION | DESCRIPTION | | POSITION | POSITION | | |
| 1 | +5V _{DC} | LEAVE UNCONNECTED | | | | |
| 2 | GND | ← CONNECT TO → | 7 | 5 | GND | |
| 3 | RS232 TXD | ← CONNECT TO → | 2 | 3 | RXD | |
| 4 | RS232 RXD | ← CONNECT TO → | 3 | 2 | TXD | |
| 5 | RS485 A | LEAVE UNCONNECTED | | | | |
| 6 | RS485 B | | | | | |

NETWORK CABLE

To connect the device to the Ethernet (10Base-T), Fast Ethernet (100Base-T) or Gigabit Ethernet (1000Base-*) network, a cable with RJ45 connectors is required. The cable must conform to the standard IEEE 802.3* of category 5 or higher. The cable between the adaptor and the hub must not be more than 100m and not less than 2.5m.

OPERATING AND STORAGE CONDITIONS

| | | |
|-------------------------------------|------|----------|
| Operating temperature range | [°C] | 0 ÷ +40 |
| Storage temperature range | [°C] | -5 ÷ +50 |
| Maximum operating relative humidity | [%] | 80 |
| Maximum storage relative humidity | [%] | 90 |

LEGAL INFORMATION

The firmware of NetMan 208C includes some open-source components. For more information, please visit the website of the manufacturer.

The warranty for NetMan 208C firmware is subject to the correct use of the product as intended.

Manufacturer warrants during the warranty period that the firmware will function materially as described in the accompanying user documentation when given normal, proper, and intended usage.

This product uses the GNU/Debian operating system.

This product uses the Linux kernel version 5.15.5 under the terms of the GNU GPLv2.

This product includes Eclipse Temurin under the terms of the GNU GPLv2 with classpath exception.

This product includes SNMP++ software.

This product includes AGENT++ software.

This product includes Logback software under the terms of the GNU LGPLv2.1.

This product includes Google GSON software under the terms of the Apache license 2.0.

This product is based in part on the work of the Qwt project (<http://qwt.sf.net>).

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes a modified Qt library under the terms of the GNU LGPLv3; click here to get the source.

This product includes Apache Commons Lang under the terms of the Apache license 2.0.

This product includes DOM4J.

This product includes jSSC under the terms of the GNU LGPLv3.

This product includes Apache Log4j under the terms of the Apache license 2.0.

This product includes Eclipse Paho Client Mqttv3 under the terms of the Eclipse Public License v2.0.

This product includes SLF4J under the terms of the MIT license.

This product includes YAVI Java.

This product includes Astarte under the terms of the Apache license 2.0.

This product includes Apache MINA SSHD.

This product includes SQLite JDBC.

This product includes JSON.

This product includes Bouncy Castle Crypto APIs.

This product includes Joda Time under the terms of the Apache license 2.0.

This product includes ORMLite. Click here to read the license.

This product includes BSON under the terms of the Apache license 2.0.

This product includes JAXB API. Click here to read the license.

This product includes JavaBeans Activation Framework API under the terms of the GNU GPLv2.

This product includes Xerces2 under the terms of the Apache license 2.0.

This product includes Apache XML Commons under the terms of the Apache license 2.0.

This product includes OkHttp under the terms of the Apache license 2.0.

This product includes Okio under the terms of the Apache license 2.0.

This product includes Java Hamcrest. Click here to read the license.

This software contains unmodified binary redistributions for H2 database engine (<https://h2database.com/>), which is dual licensed and available under the MPL 2.0 (Mozilla Public License) or under the EPL 1.0 (Eclipse Public License). An original copy of the license agreement can be found at: <https://h2database.com/html/license.html>

This product includes MD5sum Calc from crypto-js.

This product includes FastCGI Application Library.

This product includes Roboto font.

This product includes Font Awesome font.

This product includes IcoMoon.

This product includes Bootstrap 3 for Sass under the terms of the MIT license.

This product includes include-media under the terms of the MIT license.

This product includes Moment.js under the terms of the MIT license.

This product includes jQuery under the terms of the MIT license.
This product includes jQuery Validation Plugin under the terms of the MIT license.
This product includes lunar.js under the terms of the MIT license.
This product includes favico.js under the terms of the MIT license.
This product includes Bootstrap Notify under the terms of the MIT license.
This product includes DataTables under the terms of the MIT license.
This product includes JCF under the terms of the MIT license.
This product includes Lodash under the terms of the MIT license.
This product includes Modernizr under the terms of the MIT license.
This product includes Zxcvbn under the terms of the MIT license.

