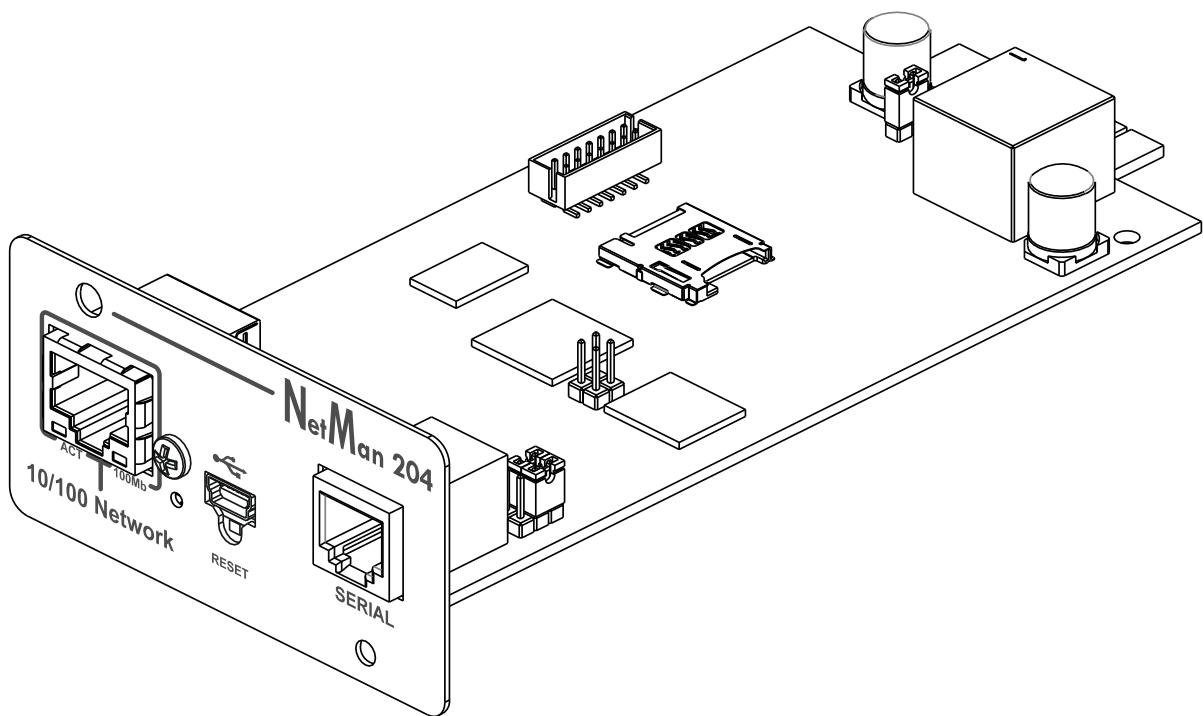


NETMAN 204

NETWORK ADAPTER



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.
- ❖ Take care 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 analyzing 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 favoring 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 centers. 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

DESCRIPTION	8
OVERVIEW	8
PACKAGE CONTENTS	8
FRONT PANEL	9
Network port	9
Micro-USB port	9
Serial port	9
LED	9
GSM Modem (optional)	10
Reset button	10
USERS	10
NETWORK SERVICES	11
SSH	11
Serial network	11
Wake-on-LAN	11
HTTP	11
SNMP	11
UDP	11
Modbus TCP/IP	11
BACnet/IP	12
FTP	12
Syslog	12
Email	12
Reports	12
SSH Client (only for operating system W18-1 or later)	12
DEVICE VALUES AND EVENTS HISTORY LOG ARCHIVE	13
Eventlog	13
Datalog (only for UPS devices)	13
ENVIRONMENTAL SENSORS (OPTIONAL)	14
Available sensors	14
INSTALLATION	14
CONFIGURATION	15
OVERVIEW	15
Configuration via HTTP/HTTPS	15
Configuration via USB	16
Configuration via SSH	16

CONFIGURATION MENU DESCRIPTION	17
Start menu	17
Setup	19
IP config	20
WEB CONFIGURATION	21
Login	21
Dashboard	23
Network configuration	24
Device configuration	25
Command configuration	26
Data log	27
UDP Firewall	28
Wake-on-Lan address	29
SNMP	30
MODBUS/BACNET	33
JSON	34
Syslog configuration	37
SSH client configuration (only for operating system W18-1 or later)	38
VMware ESXi	40
Nutanix	44
Syneto	48
NTP & Timezone configuration	57
Date & Time configuration	58
Email configuration	59
Email logic	60
GSM Modem	61
Sensors	62
Sensors Config over SSH or USB	63
Sensors Config over HTTP	65
Login access configuration	67
Certificates	69
Password recovery	79
Wi-Fi setup (optional card required)	80
Expert mode	81
CONFIGURATION OF SEVERAL DEVICES	81
SERVICE LOG	82
FIRMWARE UPGRADE	83
FIRMWARE UPGRADE VIA HTTP	83
FIRMWARE UPGRADE VIA FTP	83

SNMP CONFIGURATION	84
MODBUS TCP/IP PROTOCOL	87
BACNET/IP CONFIGURATION	91
EVENTLOG CODES	93
SERIAL PORT CONFIGURATION	95
TECHNICAL DATA	96
NETWORK CABLE	96
OPERATING AND STORAGE CONDITIONS	96
LEGAL INFORMATION	97

DESCRIPTION

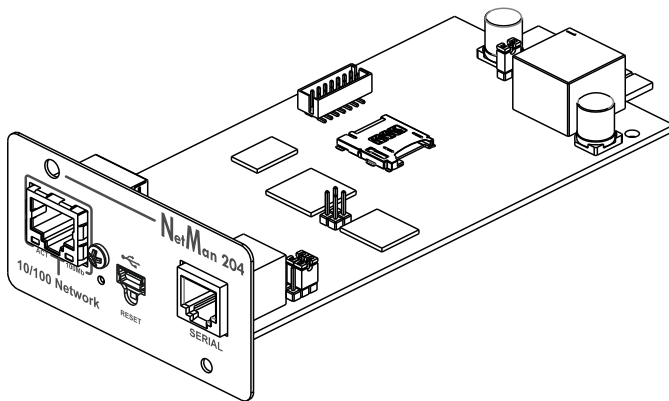
OVERVIEW

Netman 204 is an accessory that allows device management through a LAN (Local Area Network); the accessory supports all the main network protocols (SNMP v1, v2 and v3, TCP/IP, HTTP and MODBUS) and is compatible with Ethernet 10/100Mbps IPv4/6 networks. The device can therefore be integrated easily into medium and large-sized networks.

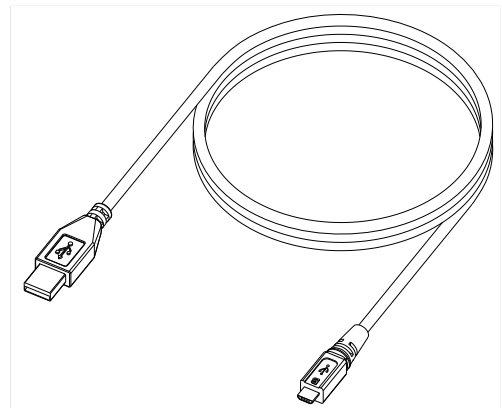
Netman 204 also records device values and events in the history log archive and can manage optional environmental sensors (not supplied with the device, but provided separately)

PACKAGE CONTENTS

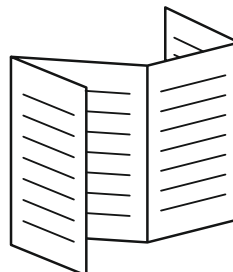
NetMan 204



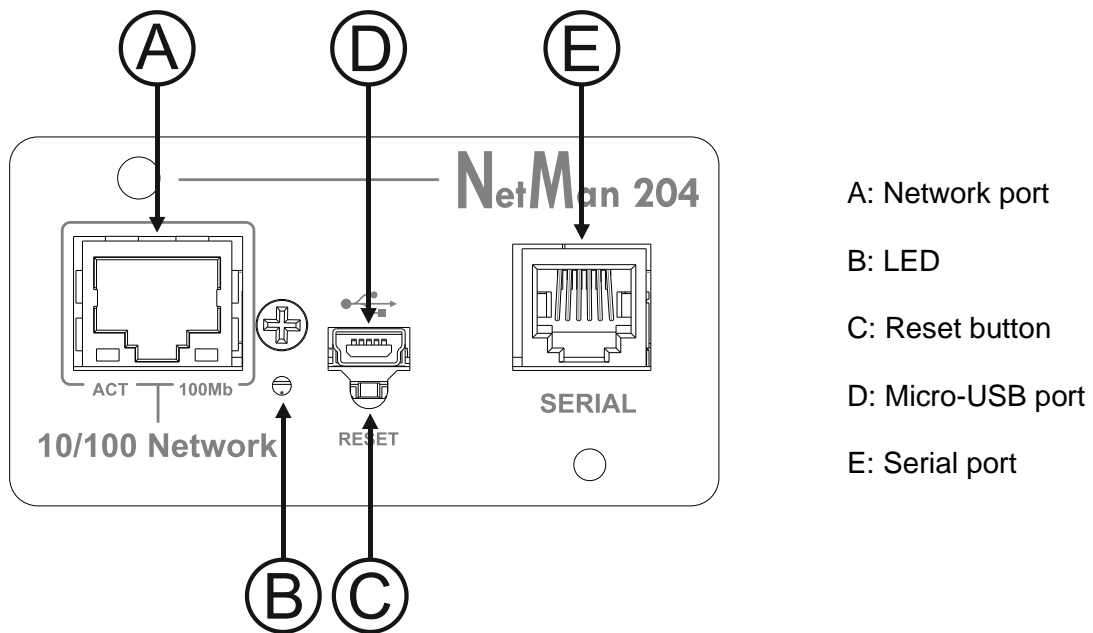
USB cable



Quick start



FRONT PANEL



Network port

Netman 204 connects to 10/100 Mbps Ethernet networks by means of connector RJ45. The LEDs built into the connector describe the status of the network:

- Left LED
SOLID YELLOW: *NetMan204* has detected a valid link.
FLASHING YELLOW: *NetMan204* is receiving or transmitting data packets.
- Right LED
SOLID GREEN: *NetMan204* is connected to a network operating at 100 Megabits per second.

Micro-USB port

NetMan 204 makes available an USB communication port through which it is possible to configure it (see paragraph "Configuration via USB").

Serial port

NetMan 204 makes available a serial communication port to which you can connect environmental sensors (not supplied with the device, but provided separately).

LED

This led describes the status of *NetMan 204*:

- SOLID RED: *NetMan 204* is not communicating with the device (verify PRTK Code).
- FLASHING RED: the DHCP server does not have assigned a valid IP address to *NetMan 204*.
- OFF: regular working.

GSM Modem (optional)

NetMan 204 can send a notification SMS 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 are required. For more details, see paragraph "GSM Modem"

Reset button

The reset button allows to restart the *NetMan204* or to load a default configuration with a predefined static IP address.

To reset *NetMan204*: keep press the reset button until the red led start flashing (ca. 2 seconds) and then release it.

To load a configuration with predefined static IP address: keep press the reset button; first the led starts flashing, then turns to solid red (ca. 10 seconds). When the led is solid red, release the reset button and the *NetMan 204* will reboot with:

- IP address: 192.168.0.204
- Netmask: 255.255.0.0
- SSH service enabled
- HTTP service enabled



HTTP and SSH service are enabled temporarily without changing the configuration saved in non-volatile memory.

USERS

It is possible to access to *Netman 204* with four different users:

Username	Default password	Privileges
admin	admin	user with right to modify the configuration ⁽¹⁾
power	N/A ⁽²⁾	user with right to modify the configuration ⁽²⁾
fwupgrade	fwupgrade	user with right to upgrade the firmware
user	user	user with right to read and download the log files



(1) Admin user can also operate on the device and therefore shutdown it.

(2) The user "Power" is disabled by default and has the right to modify the configuration (only via web) but not the right to operate on the device. To enable the user, you must set the password on the web configuration.

NETWORK SERVICES

Netman 204 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 204* 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 204 can send "Wake-on-LAN" command for remote computers boot.

HTTP

Using the HTTP (Hyper Text Transfer Protocol), is possible to configure the *NetMan 204* 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 version of browsers are supported.

SNMP

SNMP (Simple Network Management Protocol) is a communication protocol that allows a client (manager) to make requests to a server (agent). *NetMan 204* 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 new 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).

FTP

FTP (File Transfer Protocol) is a network protocol used for file exchange. *NetMan 204* uses this protocol for:

1. download of files of the device values and events history log archive (Datalog and Eventlog);
2. download and upload of configuration files;
3. firmware upgrade.

In both cases a client FTP is required, configured with these parameters:

- Host: hostname or *NetMan 204* IP address;
- User: see chapter “Users”;
- Password: current password.

The connection can also be established using a web browser (all the most popular web browsers are supported), by inserting the hostname or IP address of the *NetMan 204*.

Syslog

Netman 204 can send events to a syslog server over UDP. This service allow to centralize the log of the IT infrastructure on a single server, in order to have them consumed on the preferred way.

Email

Netman 204 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 they can be sent for seven different kinds of alarm. SMTP (Simple Mail Transfer Protocol) is the protocol used to send the e-mails. The port is configurable. For more details, see paragraph “Configuration”

Reports

Netman 204 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 (only for operating system W18-1 or later)

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

DEVICE VALUES AND EVENTS HISTORY LOG ARCHIVE

NetMan 204 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. The file can be downloaded via FTP or can be viewed through the web page without credentials. With the "Email report" service, is sent a .csv 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 medium. Records older than one year get overwritten with new records.

The file can be downloaded via FTP or can be viewed through the web page (only the most important values are shown on the web page) without credentials.

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.

ENVIRONMENTAL SENSORS (OPTIONAL)

It is possible to connect to *NetMan 204* the environmental sensors for monitoring temperature, humidity and digital input/output.

The information provided by these sensors can be showed with the device monitoring and control software or with a web browser.

The values provided by the sensors may also be requested with SNMP according to the RFC 3433 standard (MIB files on the download site).

Available sensors

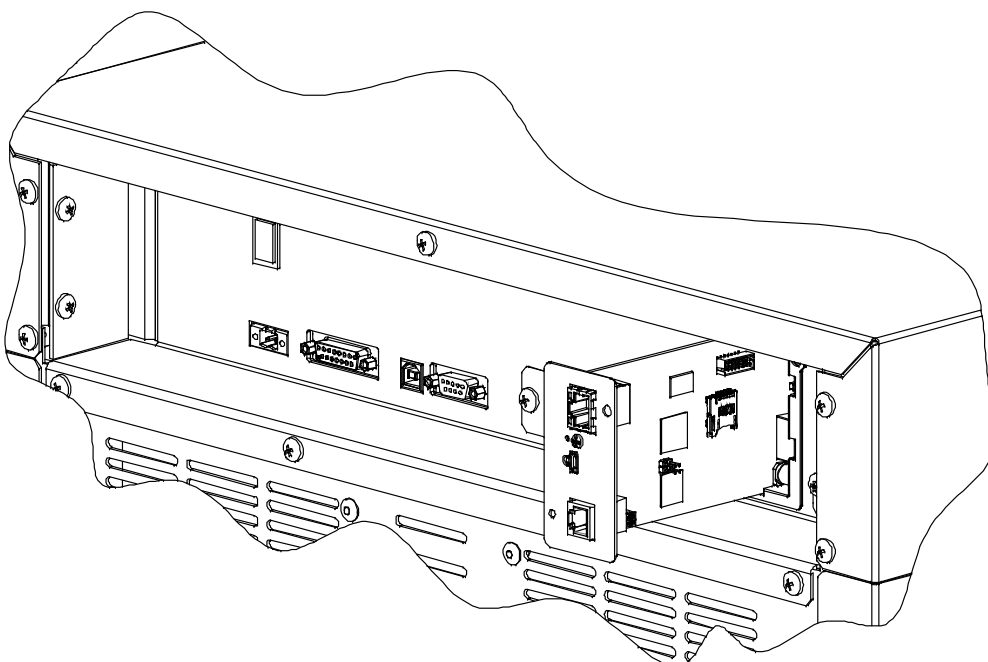
- **Temperature:** detects the environmental temperature in °C.
- **Humidity & Temperature:** detects the relative humidity in % and the environmental temperature in °C.
- **Digital I/O & Temperature:** detects the environmental temperature in °C and features a digital input and a digital output.



It is possible to connect up to 3 environmental sensor to a *NetMan 204* (for sensor installation please see the sensors' manual).

INSTALLATION

1. Remove the cover of the device expansion slot by removing the two retaining screws.
2. Insert *NetMan 204* in the slot.
3. Secure *Netman 204* in the slot using the two screws removed previously.
4. Connect the device to the network by means of connector RJ-45 (see "Specifications for the cabling of the network cable")



CONFIGURATION

OVERVIEW

NetMan 204 can be configured via USB, via SSH or via HTTP.



NetMan 204 comes provided as factory default with DHCP enabled and with the following services active: SSH, HTTP, SNMP, UDP and FTP.

In order to change the configuration of *NetMan 204*, you have to log in as admin (default password "admin").

NetMan 204 needs approx. 2 minutes to become operational from when it is powered up or after a reboot; before this time the device may not respond to commands that are sent to it.

Configuration via HTTP/HTTPS

In order to change the configuration via http/https, you have to insert in your web browser the hostname or IP address of the *NetMan 204* and then log in as admin (default password: "admin").



The HTTPS service uses TLS (transport layer security) in order to provide cryptographic security. However, the certificate used is self-signed and therefore the web browser may prompt a security alert; in this case you can ignore the alert and proceed with the configuration of *NetMan 204*.

Once login has been affected, you can browse through the menus to configure the *NetMan 204*.



In order to make a new configuration effective, it is necessary to save it. Some changes are applied immediately, while other require a reboot of the *NetMan 204* (as required with a pop-up by your web browser).

Configuration via USB

To configure *NetMan 204* via USB it is necessary to:

- Connect, with the USB cable provided, the micro-USB port with the USB port of a PC with Windows operating system.
- If not previously installed, install the USB driver (after driver installation, a virtual COM named "NetMan 204 Serial" will be present in device manager).
- Execute a terminal emulation program with the following settings:
COMn ⁽¹⁾, 115200 baud, no parity, 8 databits, 1 stop bit, no flow control.
(¹) COMn = COM port assigned to "NetMan 204 Serial" by device manager.

- Press the "Enter" key of the PC.
- At the login prompt, enter "admin".
- At the password prompt, enter the current password (default password: "admin").



During password's typing, no character is shown.

Once login has been affected, the screen of the start menu is displayed. From this screen it is possible to access the various menus to change *NetMan 204* settings (see paragraph "Start menu" and following paragraphs).

Configuration via SSH

To configure *NetMan 204* via SSH it is necessary to:

- Execute a SSH client on a PC connected in a network to *NetMan 204* set with the IP address of the device to be configured.
- At the login prompt, enter "admin".
- At the password prompt, enter the current password (default password: "admin").



During password's typing, no character is shown.



For proper configuration of *NetMan 204*, you must configure the SSH client so that the backspace key sends "Control-H".
Please verify the keyboard options of your SSH client.

Once login has been effected, the screen of the start menu is displayed. From this screen it is possible to access the various menus to change *NetMan 204* settings (see paragraph "Start menu" and following paragraphs).

CONFIGURATION MENU DESCRIPTION

Start menu

Once login has been effected via SSH or USB, a screen like the following is displayed:

```

  /-----/
 /         \
/           \
 \         /
  \-----/

Netman 204

Setup.....:<--
View status....:
Change password:
Service log....:
Wi-Fi setup....:no card installed
Factory reset..:
Expert mode....:

      inet 10.1.30.68 netmask 255.255.0.0 broadcast 10.1.255.255

Press [ESC] for logout
SysVer. S20-1 - AppVer. 03.14.000
  
```

Function	Description
Setup	To enter main configuration menu
View status	To see the status of the device
Change password	To modify the password (see also Password recovery)
Service log	To generate a log file of the card (when requested by the service)
Wi-Fi setup	To configure Wi-Fi connection For Wi-Fi connection, an optional card is required. The Wi-Fi card is not provided with <i>NetMan 204</i> but it has to be purchased separately.
Factory reset	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 (Arrow up, down, right, left)	To move the cursor within the menus
Tab	Goes on to next option
Enter ⁽¹⁾	Choice of submenu
	Confirmation of characters entered
Esc ⁽¹⁾	Exit main menu ⁽²⁾
	Return to previous menu

⁽¹⁾ Some keys can have a different function 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.....:<--
Wi-Fi setup....:
Enable Sensors.:
Sensors Config.:
Expert mode....:
Factory reset..:
Reboot.....:

Press [Esc] to quit
SysVer. S20-1 - AppVer. 03.14.000
```

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
Wi-Fi setup	To configure Wi-Fi connection For Wi-Fi connection, an optional card is required. The Wi-Fi card is not provided with <i>Netman 204</i> but it has to be purchased separately.
Enable Sensors	To enable the environmental sensors
Sensors Config	To configure the environmental sensors
Expert mode	To enter Expert mode (more information at paragraph “ <i>Expert mode</i> ”)
Factory reset	Restore factory configuration
Reboot	Reboots the <i>Netman 204</i>

IP config

```

  /-----/
 /         \
/           \
/           \
 \           /
  \         /
   \-----/

IP config

Hostname.....:ups-server

IP address/DHCP:DHCP

Netmask.....:

Gateway.....:

Primary DNS...:

Secondary DNS..:
```

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

Field	Parameters to be inserted
Hostname	Enter the <i>NetMan 204</i> host name
IP address/DHCP	Enter the IP address for a static IP; enter “DHCP” for a dynamic IP
Netmask	Enter the netmask to be used together with the static IP address
Gateway	Enter the name or the address of the network gateway
Primary DNS	Enter the name or the address of the preferred DNS to be used
Secondary DNS	Enter the name or the address of the alternative DNS to be used



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 and provide a hostname; all the other options should be ignored because these are automatically configured with DHCP

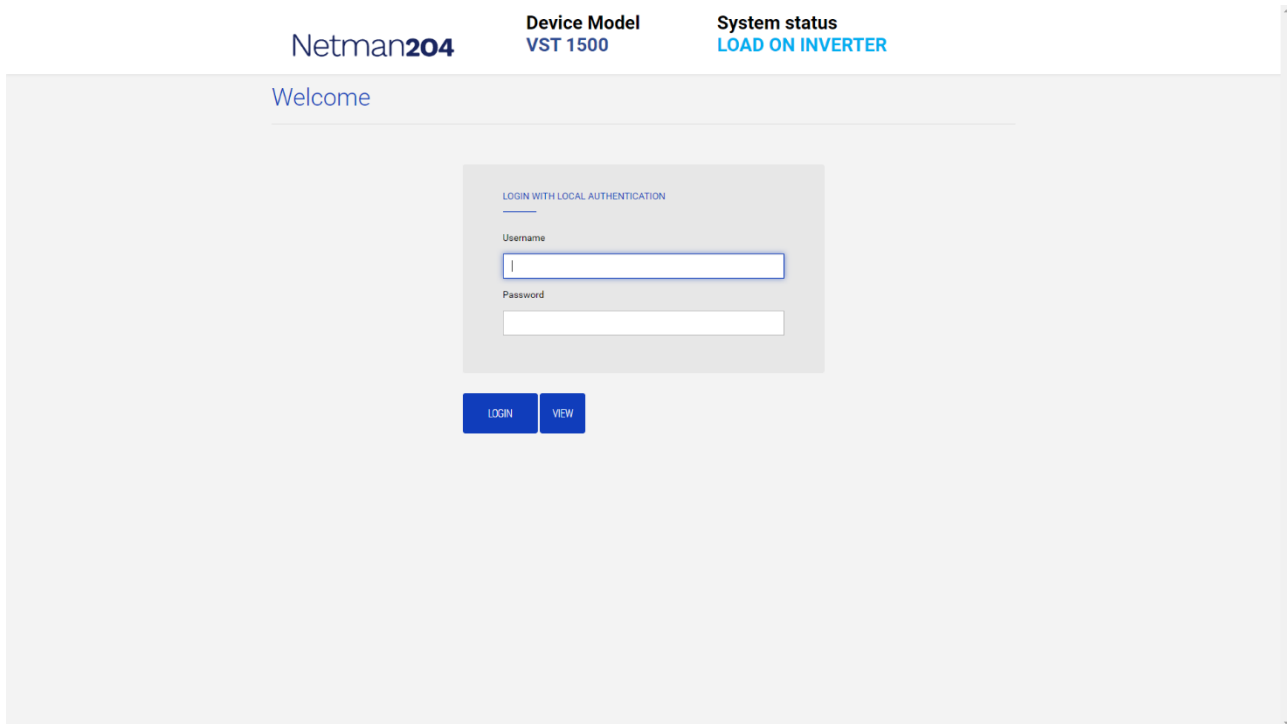
After pressing “ESC” and “Y” to confirm exit from the menu, a screen similar to the image below is displayed. Press the “ENTER” key to return to the main menu and the configuration will be immediately applied.

```
eth0      Link encap:Ethernet  Hwaddr 00:02:63:04:07:b1
          inet addr:10.1.11.19  Bcast:10.1.255.255  Mask:255.255.0.0
          inet6 addr: fe80::202:63ff:fe04:7b1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:145877 errors:0 dropped:0 overruns:0 frame:1
          TX packets:4899 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12740380 (12.1 MiB)  TX bytes:2115614 (2.0 MiB)
```

WEB CONFIGURATION

Login

After setting up the network, 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.



The screenshot displays the web configuration interface for Netman204. At the top, the device model is identified as 'VST 1500' and the system status is 'LOAD ON INVERTER'. A central login form titled 'LOGIN WITH LOCAL AUTHENTICATION' contains two input fields: 'Username' and 'Password'. Below the form are two buttons: 'LOGIN' and 'VIEW'.



The login password must contain alphanumeric characters and these special characters: `, . _ + : @ % / -`. No other characters are allowed to avoid malicious script injections.

Please note that user “fwupgrade” and “user” are not allowed to log in on the web page. Either use “admin”, “power” or enter without password.

- Admin user will be able to change the configuration and operate on the device
- Power user will be able to change the configuration but not operate on the device
- Entering without password allows to view the status of the device; no other action is permitted.

Welcome

LOGIN WITH

LDAP authentication

Username

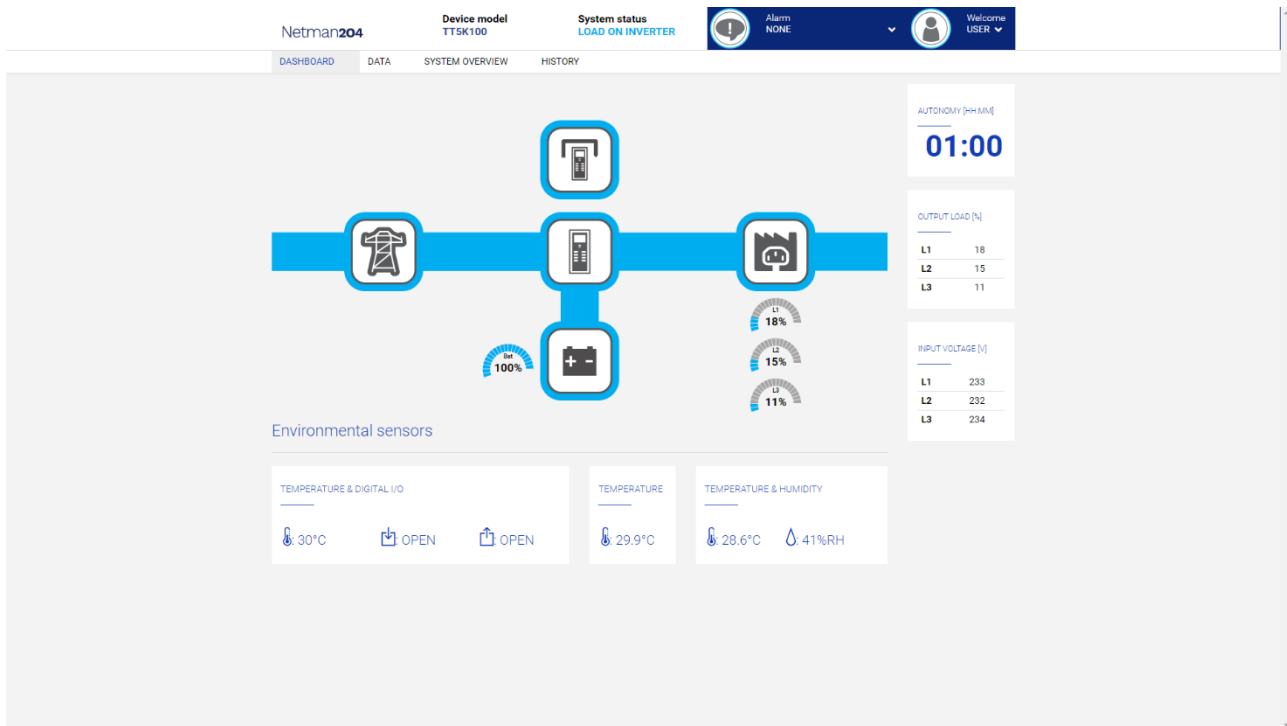
john

Password

LOGIN VIEW

It is possible to login with local authentication (managed by *Netman 204*) or centrally with LDAP or AD (more information at paragraph “Login access configuration”).

Dashboard

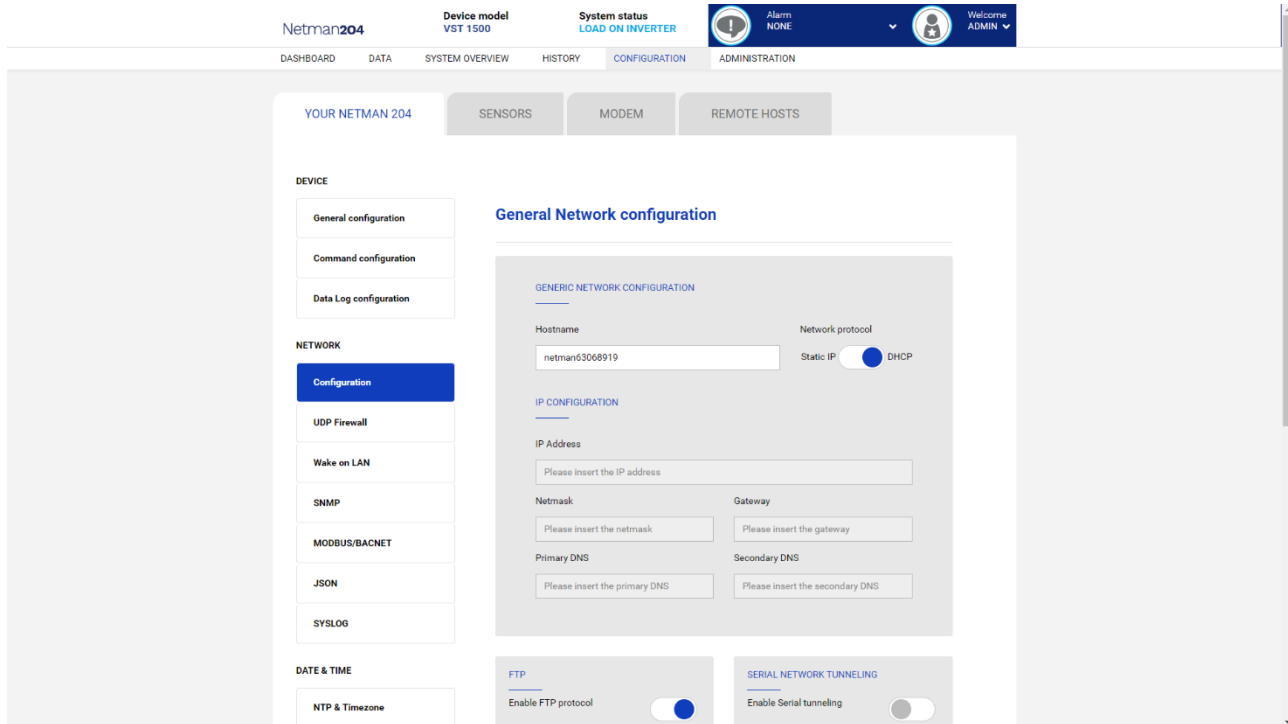


On the top area is possible to check the general status of the device, all the active alarm conditions and the privilege level of the user.

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

On the bottom, there are the values of the environmental sensors (if installed and configured).

Network configuration

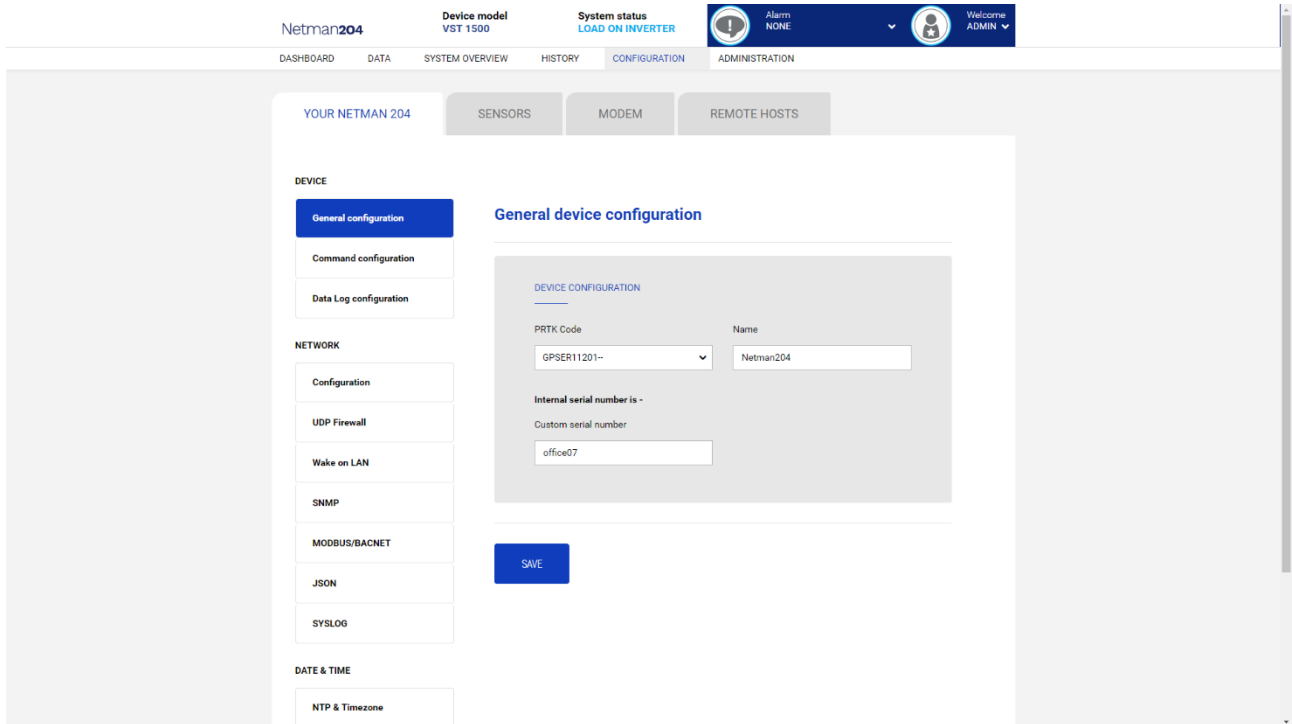


On the web page, is possible to configure in depth the network services of *Netman 204*.

Field	Parameters to be inserted
Hostname	Enter the <i>Netman 204</i> host name
Static IP/DHCP	Choose between static IP or dynamic IP
IP Address	Enter the IP address
Netmask	Enter the netmask to be used together with the static IP address
Gateway	Enter the name or the address of the network gateway
Primary DNS	Enter the name or the address of the preferred DNS to be used
Secondary DNS	Enter the name or the address of the alternative DNS to be used
Enable FTP protocol	Enables the FTP protocol
Enable Serial network tunneling	Enables the serial network tunnelling protocol
Enable UDP	Enables UDP/UPSMon service
UDP port	Enter the port where the UDP/UPSMon service is started ⁽¹⁾
UDP Password	Change the password used for UDP/UPSMon communication

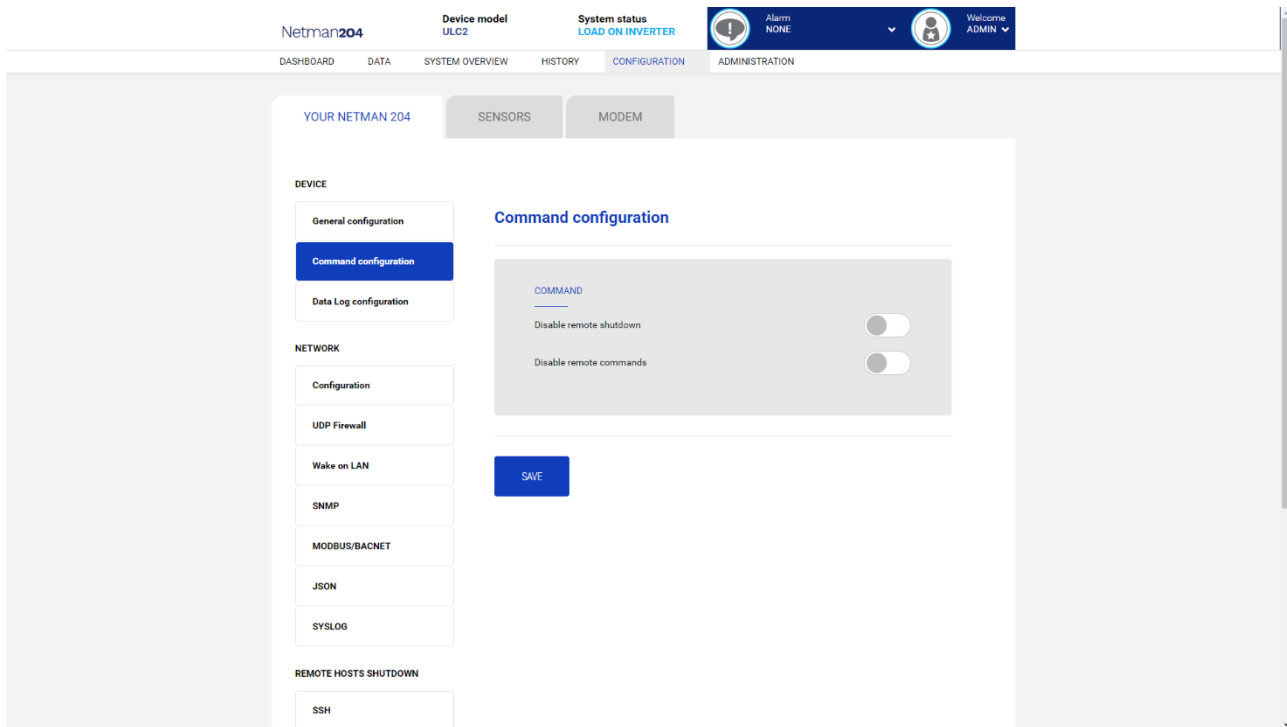
⁽¹⁾ This port must be the same as configured in the UPSMon software

Device configuration



Field	Parameters to be inserted
PRTK Code	Enter the PRTK code indicated at the back of the device
Name	Enter the identifying name of the device
Custom serial number	Enter a serial number that will override the default

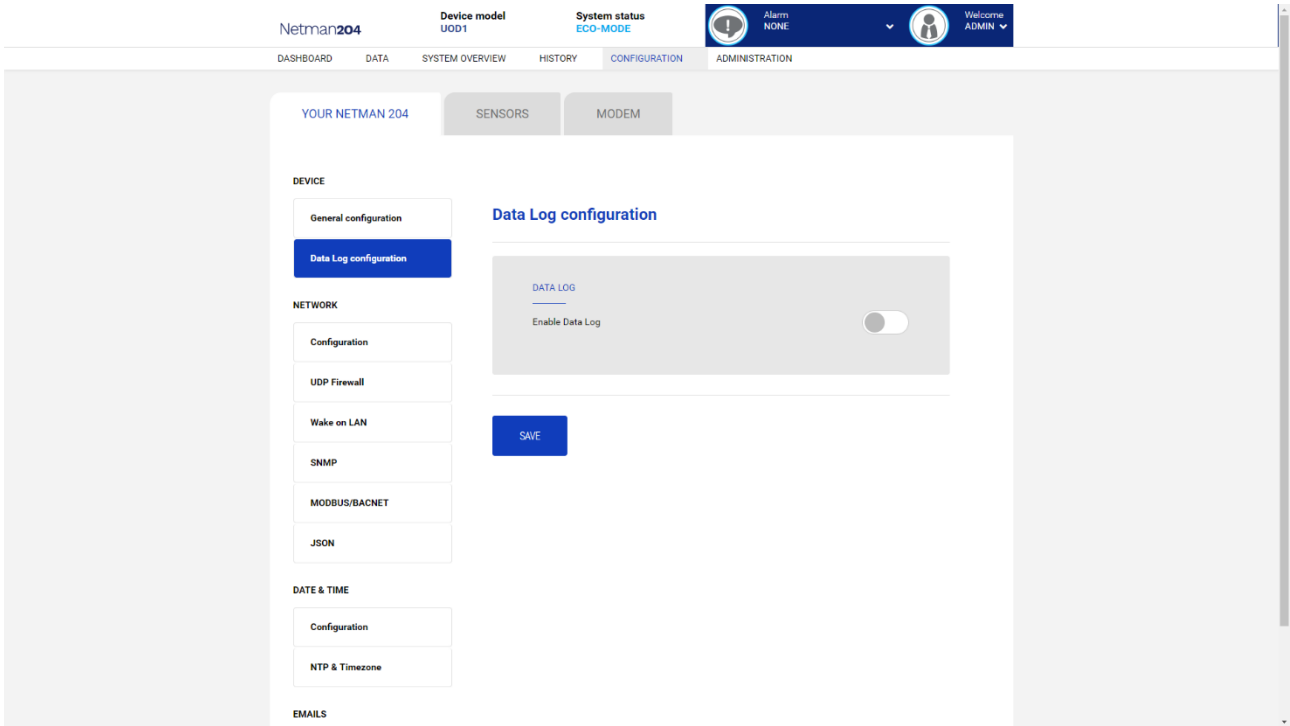
Command configuration



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

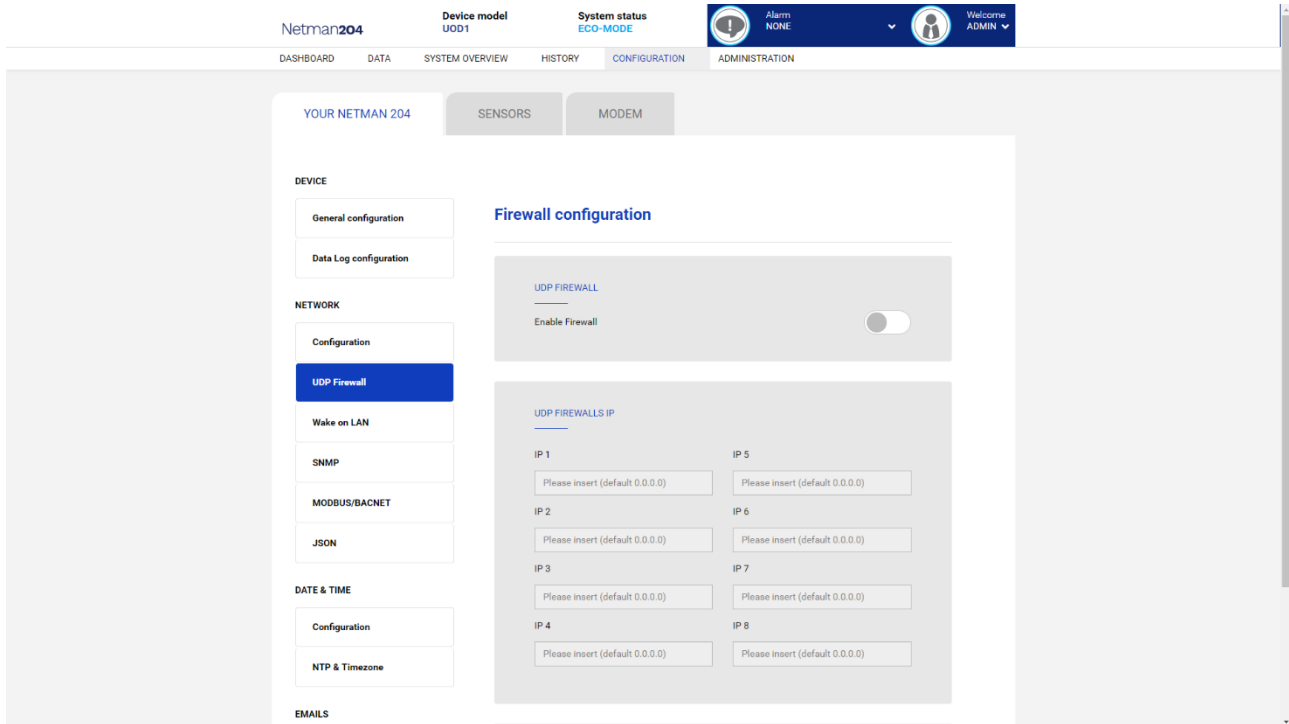
Field	Parameters to be inserted
Disable remote shutdown	Disables the execution of shutdown commands
Disable remote commands	Disables the execution of the remaining commands

Data log



Field	Parameters to be inserted
Enable Data log	Enables the datalog service
Backup UPS data log at boot	At boot <i>NetMan 204</i> downloads the data log of the device for quick access

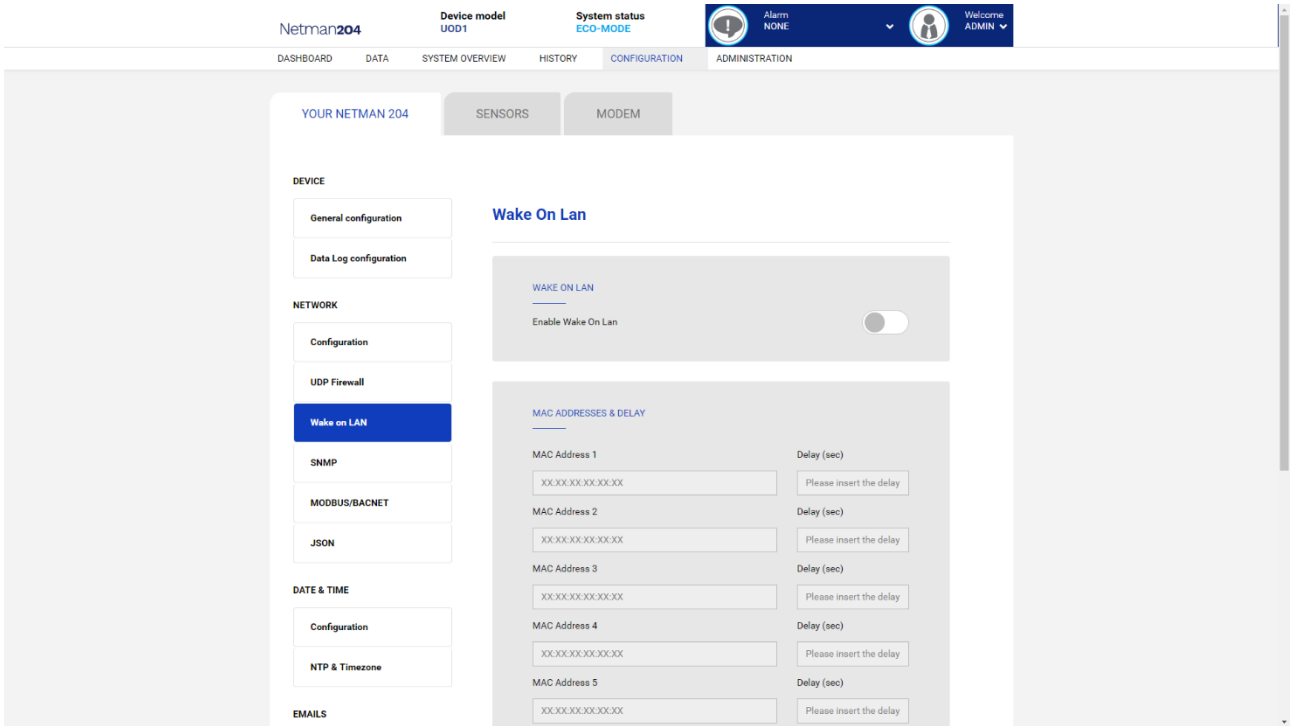
UDP Firewall



With this menu the IP addresses or hostnames of the devices enabled for communication with *NetMan 204* can be configured. The number **255** can be used for one or more fields of the IP address to indicate that all values between 0 and 255 are accepted in that field. The following table provides some possible configuration examples.

IP Access	Description
255.255.255.255	All the devices present on the network are enabled to communicate with <i>NetMan 204</i> (default configuration)
10.1.10.255	The devices with addresses between 10.1.10.0 and 10.1.10.255 are enabled to communicate with <i>NetMan 204</i>
myserver.mydomain	Hostname of the device enabled to communicate with <i>NetMan 204</i>

Wake-on-Lan address

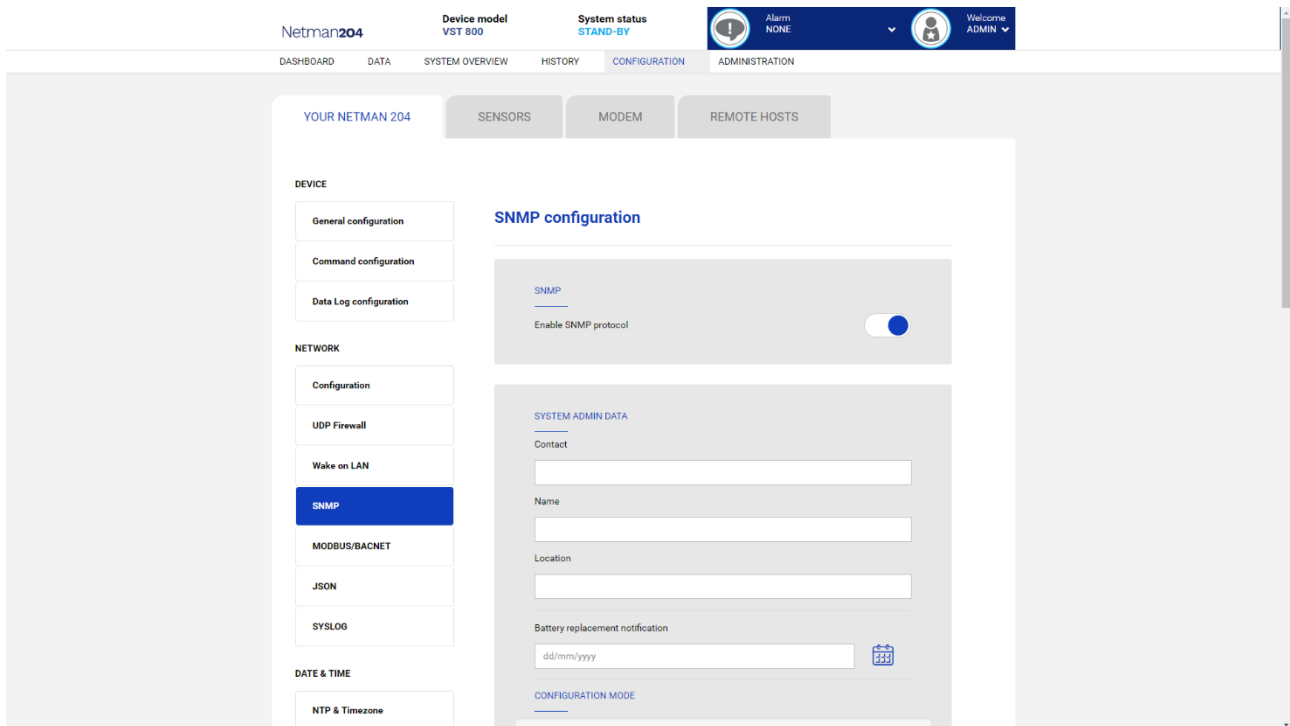


With this menu is possible to insert up to 8 MAC address to execute Wake-on-LAN, and the delay times for each Wake-on-LAN. The Wake-on-LAN is sent at *NetMan 204* boot and when the mains returns from black-out.



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

SNMP



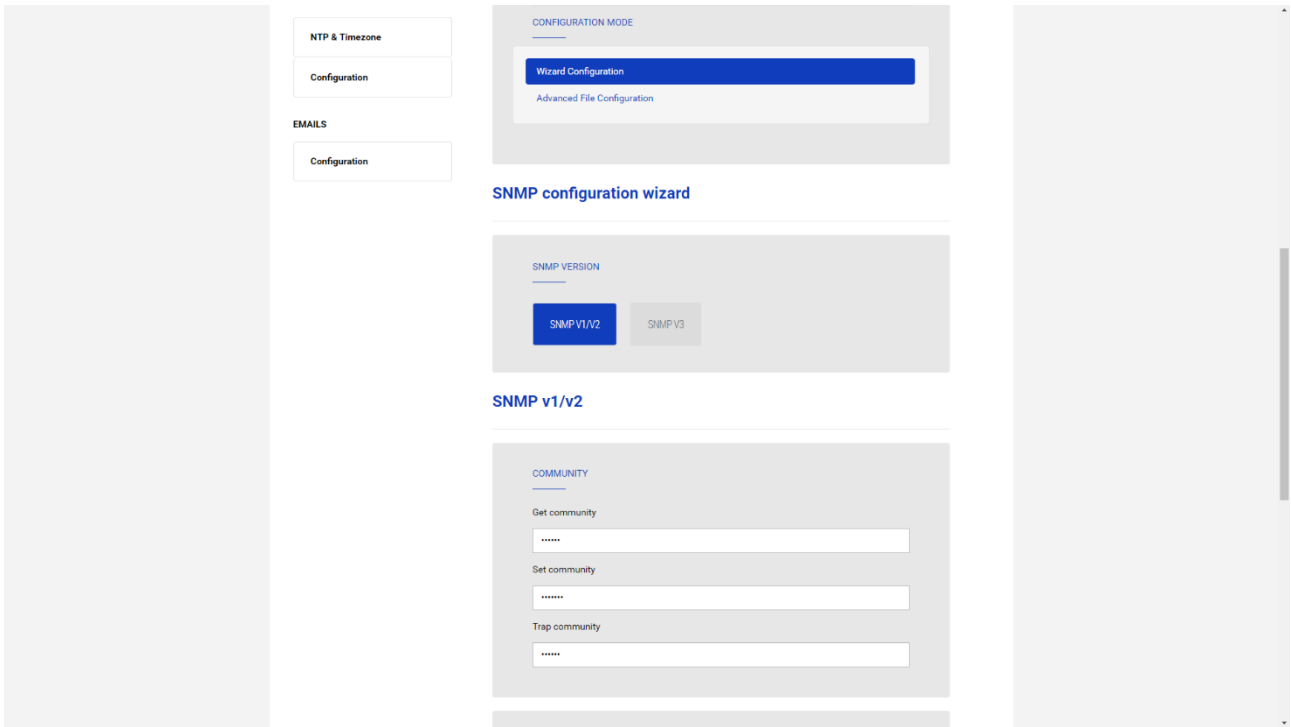
SNMP (Simple Network Management Protocol) is a communications protocol, a tool that allows the client (manager) to effect requests to a server (agent). This protocol is an international standard and so any SNMP manager can communicate with any SNMP agent.

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.

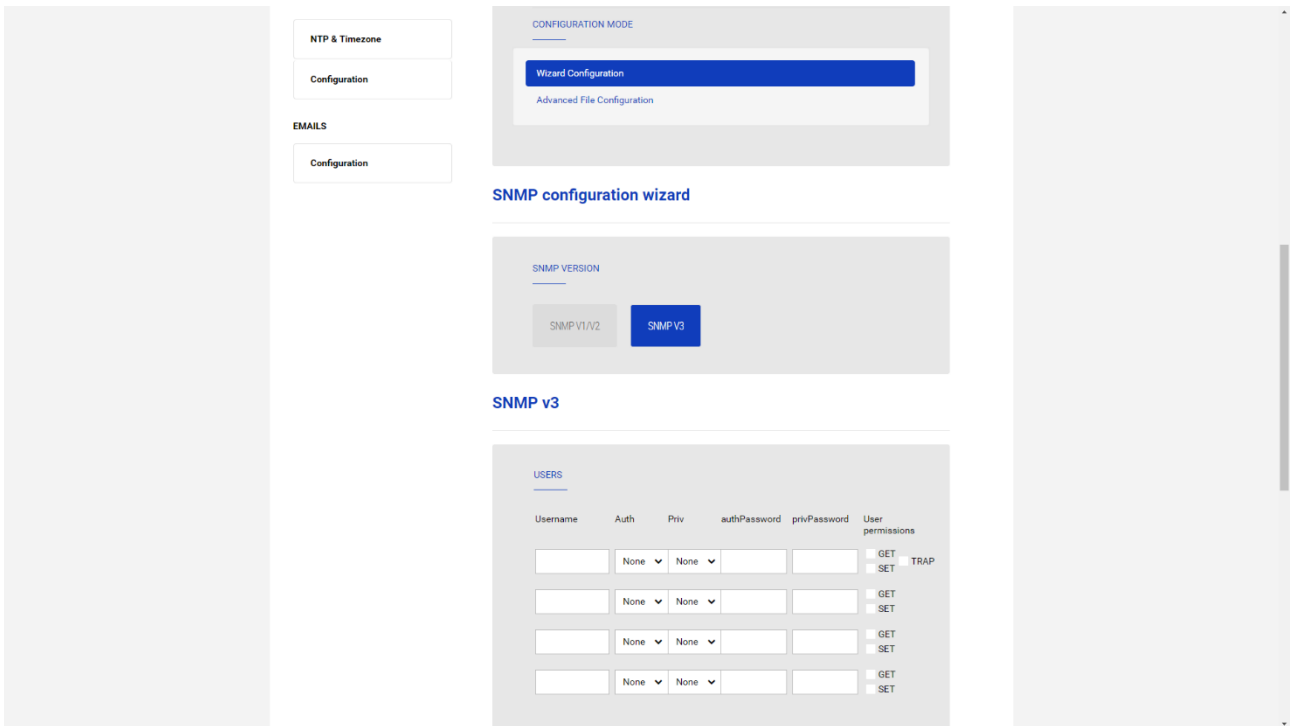
Each MIB is oriented to a particular sector; in particular RFC-1628, also called UPS-MIB, holds the data for UPS remote management.

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

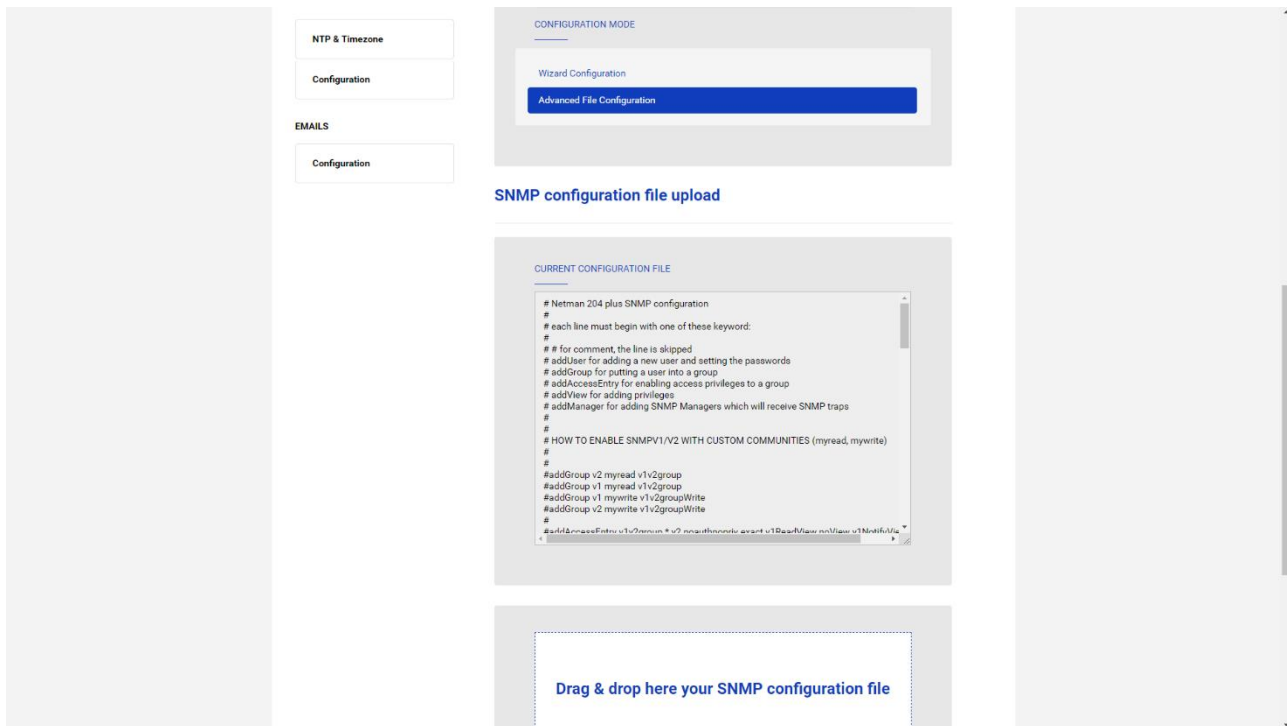
For more information about SNMP visit this site: <http://www.snmp.com>.



For configuring SNMP, is possible to use the wizard web page for a simple configuration. The wizard that provide defaults that fit the needs of most use cases for SNMPv1/v2.



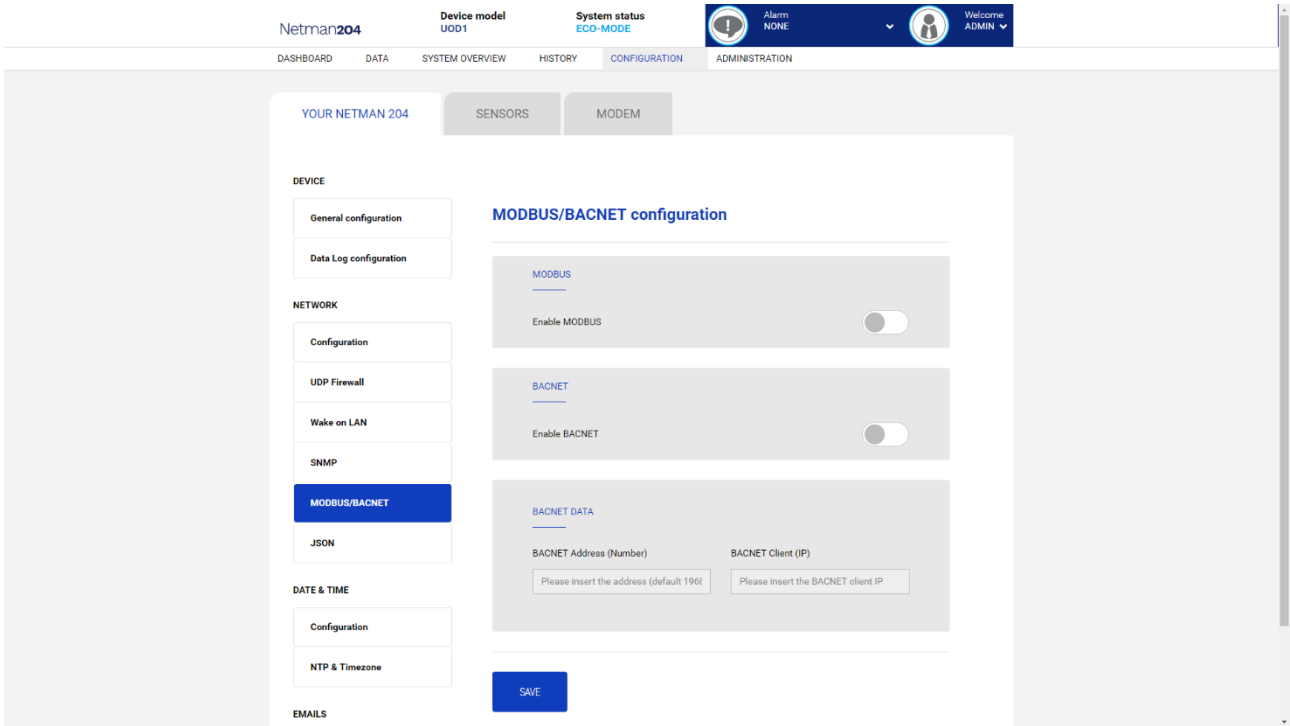
When is needed additional security by means of authentication and encryption, it is recommended to use SNMPv3 with the wizard configuration.



Advanced configuration requires to edit `snmp.conf` (please see chapter “SNMP configuration”).

Field	Parameters to be inserted
Enable SNMP protocol	Enables the SNMP service
Contact	Enter the string to be associated with these SNMP variable
Name	Enter the string to be associated with these SNMP variable
Location	Enter the string to be associated with these SNMP variable
Battery replacement notification	Enter the date to be notified when battery should be replaced
Configuration mode	Choose between wizard configuration or to upload a configuration file
SNMP version	Choose between SNMPv1/v2 or SNMPv3
Get community	Enter the community for read access
Set community	Enter the community for write access
Trap community	Enter the community for traps
Trap receiver	Enter the IP addresses to which traps are sent
Username	Enter the USM username
Auth	Enter the authentication algorithm
Priv	Enter the privacy algorithm
AuthPassword	Enter the authentication password
PrivPassword	Enter the privacy password
Permissions	Choose the permissions for each user

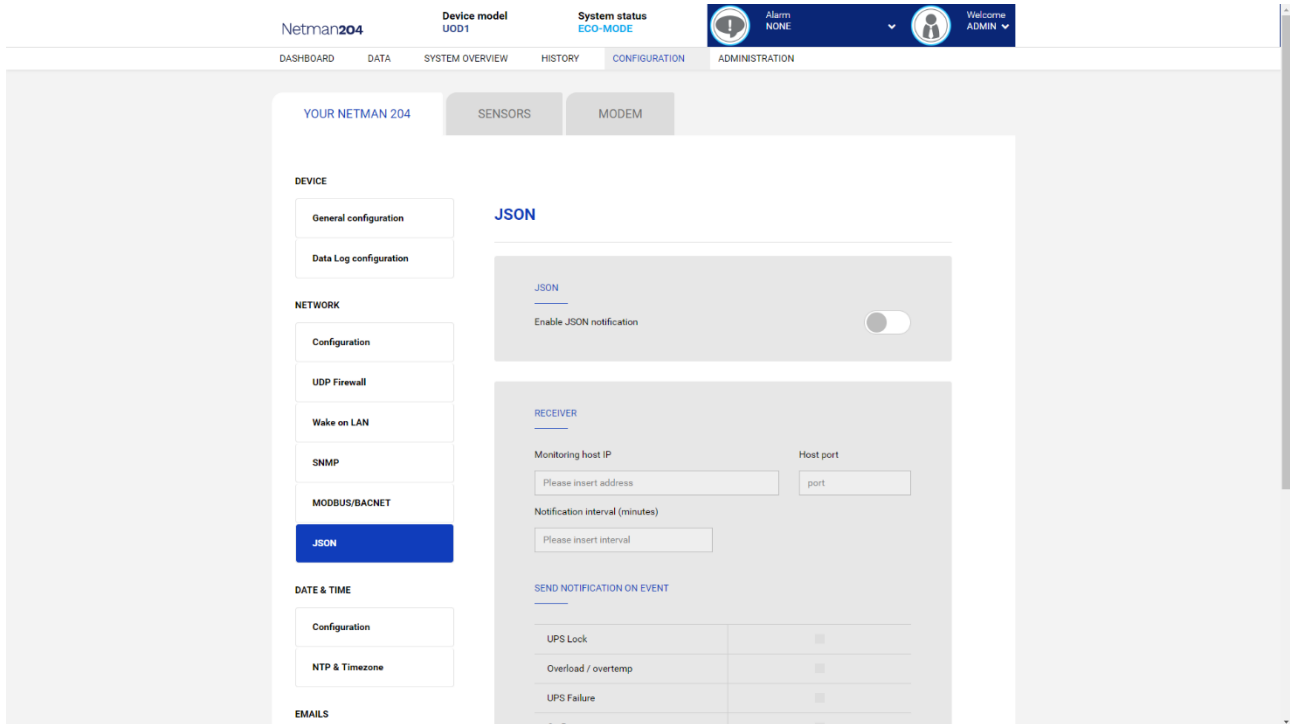
MODBUS/BACNET



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

Field	Parameters to be inserted
Enable MODBUS	Enables the MODBUS protocol
Enable BACNET	Enables the BACNET protocol
BACNET Address (Number)	Enter the BACNET address of the device
BACNET Client (IP)	Enter the IP address of the BACNET client

JSON



Netman 204 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	Parameters to be inserted
Enable JSON	Enables the JSON notification service
Monitoring host IP	Enter the IP address to which send the JSON traps
Host port	Enter the port where traps will be sent
Notification interval (minutes)	Enter the interval between JSON trap sending
Send notification on event	Choose the even upon which the trap will be sent

It requires a `license.txt` file to be uploaded on the *Netman 204*. The content of the file will be included in the trap.

Example trap:

```
[
  {
    "timestamp": 1464255869,
    "model": "UPS 6kVA",
    "license": "00-B3-74-98-ED-43=2D84-1234-9E4B-5FAD",
    "io_conf": 1,
    "status": [ 123, 255, 0, 97, 132, 12 ],
    "measures":
    {
      "vin1": 231,
      "vin2": 0,           // (1)
      "vin3": 0,           // (1)
      "fin": 499,          // Hz/10
      "vbyp1": 231,
      "vbyp2": 0,          // (2)
      "vbyp3": 0,          // (2)
      "fbyp": 499,        // Hz/10
      "vout1": 231,
      "vout2": 0,          // (2)
      "vout3": 0,          // (2)
      "fout": 499,
      "load1": 0,
      "load2": 0,          // (2)
      "load3": 0,          // (2)
      "vbat": 817,        // V/10
      "authonomy": 475,    // min
      "batcap": 100,
      "tsys": 33
    }
  }
]
```

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.

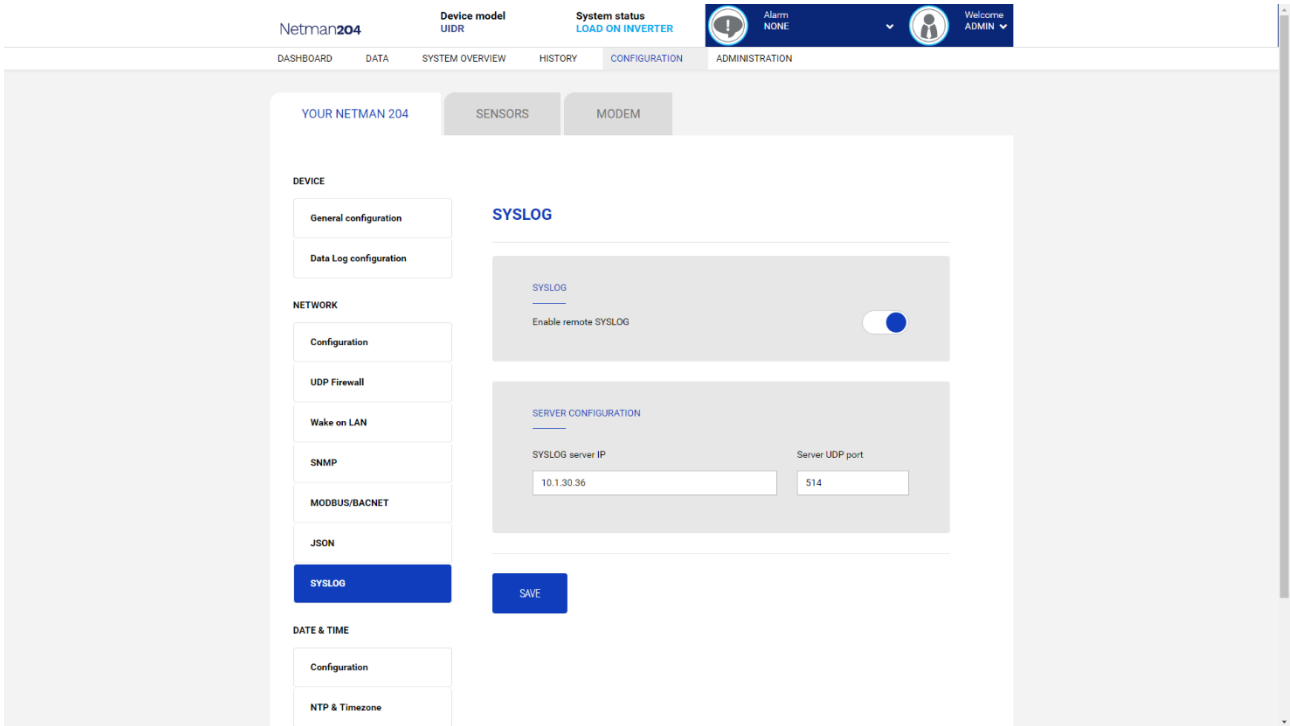
status is an array that must be interpreted as follows:

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 Actived
	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/Beeper 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.

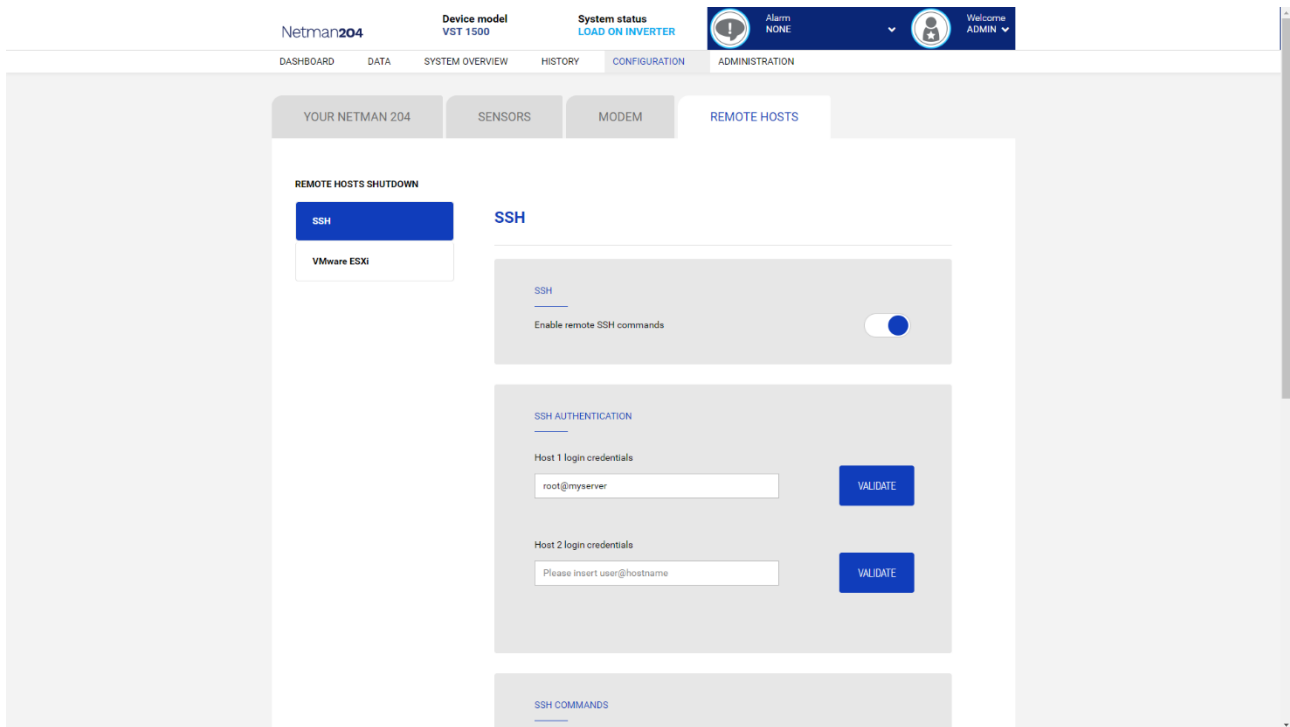
Syslog configuration



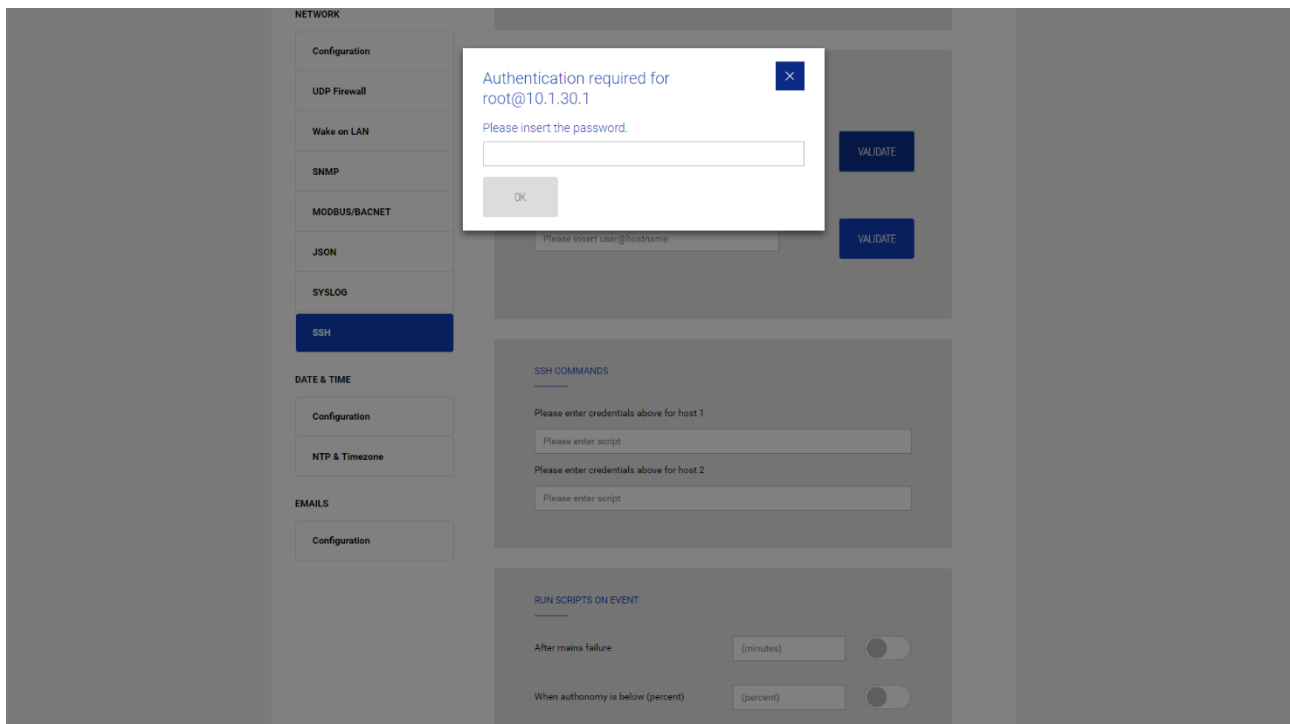
This menu allow to configure the syslog service over UDP port.

Field	Parameters to be inserted
Enable remote syslog	Enables the syslog service
Syslog server IP	Enter the IP address of the syslog server
Server UDP port	Enter the UDP port where the events will be sent

SSH client configuration (only for operating system W18-1 or later)



This menu allow to configure the SSH client service. After inserting the SSH credential for the first time you will be asked for the authentication password for the remote host.



After inserting a valid password, you will be able to execute scripts on the remote host with the authenticated user. This is confirmed by the “Validated” badge.



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.

Field	Parameters to be inserted
Enable remote SSH commands	Enables the ssh client service
Host 1 login credentials	Enter the ssh credentials for host 1
Host 2 login credentials	Enter the ssh credentials for host 2
SSH commands	Enter the script to be executed for each host
After mains failure	Scripts will be executed after the set minutes of delay after mains failure
When autonomy is below (percent)	Scripts will be executed when autonomy is below the set percent
Minimum delay between execution (minutes)	Cooldown for script execution to prevent script to be executed within the set time

VMware ESXi

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 Vmmware 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.

Infrastructure connectors

Field	Parameters to be inserted
Host or VCSA	Enter the hostname or IP address of the ESXi host or VCSA
User name	Enter the user name for ESXi or VCSA administrator
Password	Enter the password for ESXi or VCSA administrator

Actions

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

SHUTDOWN ON EVENT

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

Then, UPS shutdown after (seconds)

Actions

Field	Parameters to be inserted
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>

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>
Condition duration (minutes)	The duration that the selected condition (Power fail or Autonomy less) must be active for before the selected action starts.
Delay next (seconds)	Delay in seconds to execute the next action
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>
Target	If the action is VMotion , a valid IP address or hostname must be specified
Restore on power on	<p>In case of shutdown actions the <i>Netman 204</i> will restart automatically all the VMs that where shutdown.</p> <p>In case of Maintenance action the <i>Netman 204</i> 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>
Target Netman	For future use.

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.



NOTE

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

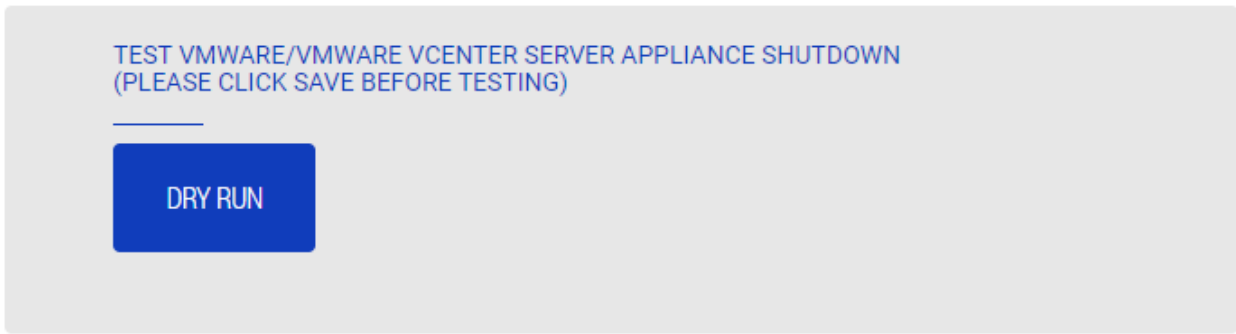
SHUTDOWN ON EVENT

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.

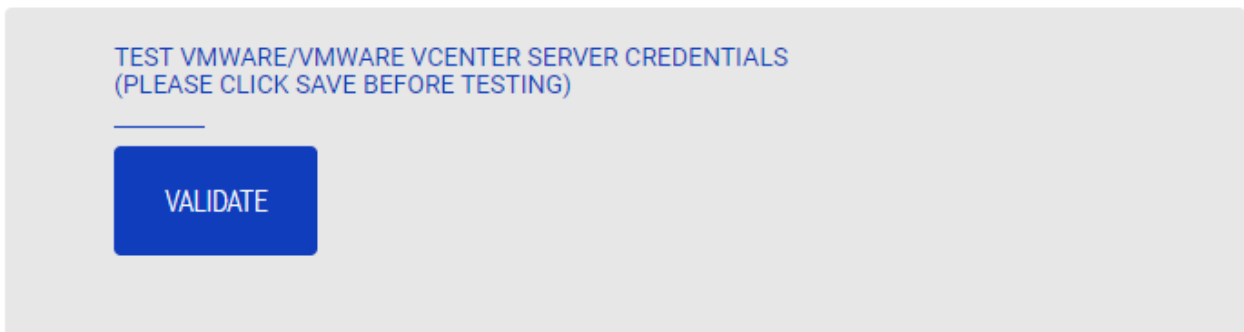
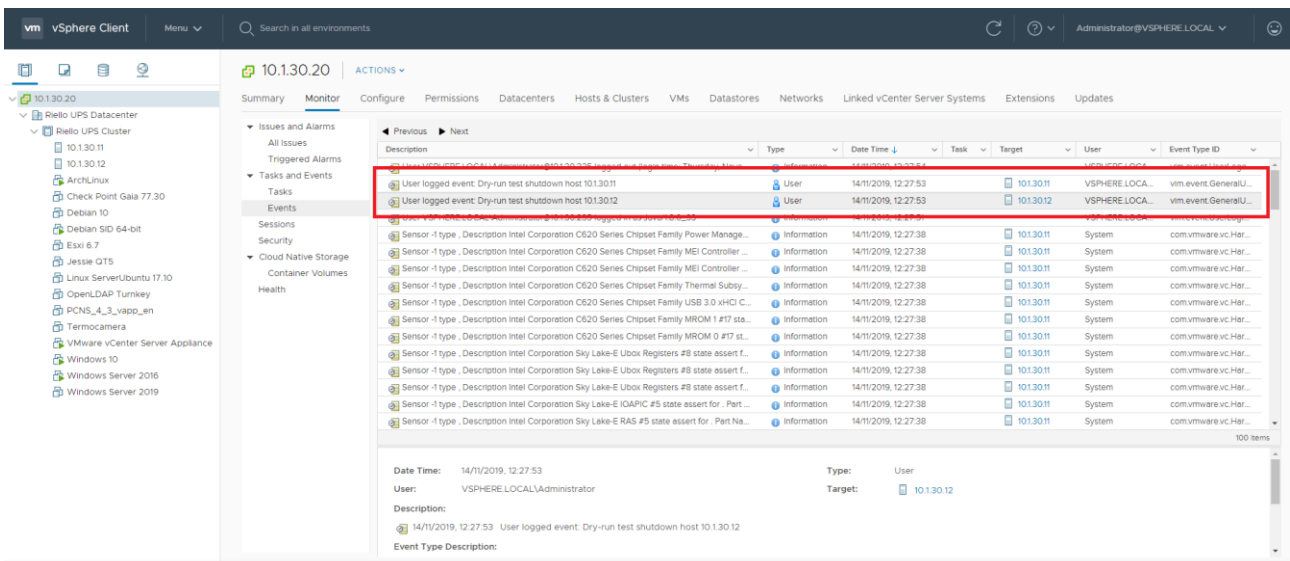
SAVE

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



Testing the configuration

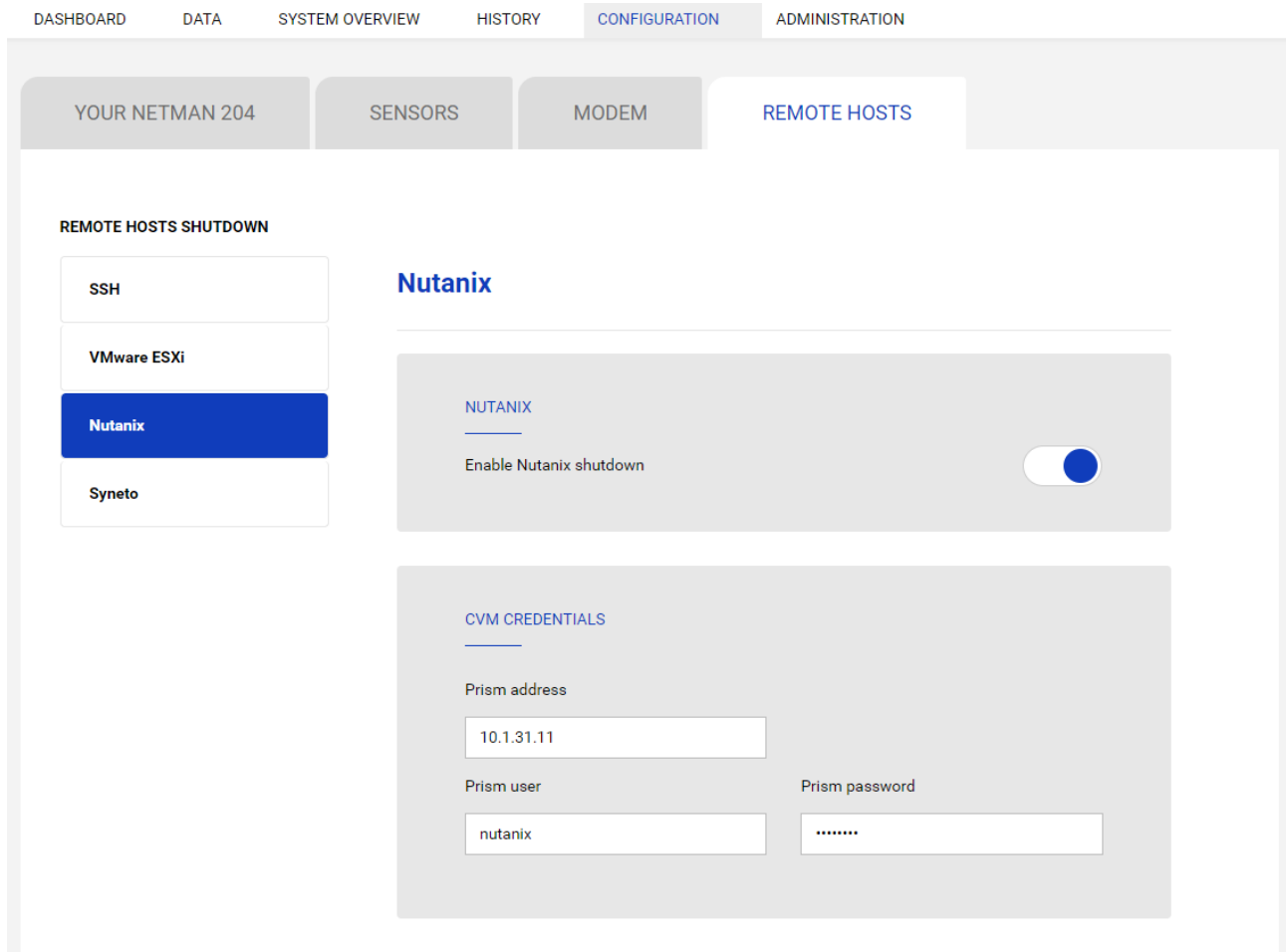
It is possible to test the procedure without performing a real shutdown by pressing “Dry Run”. The logs on the target host or vCenter Server Appliance will confirm the correctness of the configuration.



Validating the connections

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

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



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

CVM credentials

Field	Parameters to be inserted
Prism address	Enter the hostname or IP address of the Prism CVM
User name	Enter the user name for CVM administrator
Password	Enter the password for CVM administrator

Physical hosts

Host	Username	Password	
10.1.31.10	root	Delete
10.1.31.12	root	Delete
10.1.31.14		Delete

[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

[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)



SAVE

TEST NUTANIX SHUTDOWN
(PLEASE CLICK SAVE BEFORE TESTING)

DRY RUN

TEST NUTANIX SERVER CREDENTIALS
(PLEASE CLICK SAVE BEFORE TESTING)

VALIDATE

Actions

Field	Parameters to be inserted
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
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.
Condition duration (minutes)	The duration that the selected condition (Power fail or Autonomy less) must be active for before the selected action starts.
Delay next (seconds)	Delay in seconds to execute the next action
Source	If the action is Critical VM a valid VM UID, present in the infrastructure must be specified.

Restore on power on	In case of shutdown actions the <i>Netman 204</i> will restart automatically in reverse sequence all the VMs that where shutdown. Please note that to restart the host the Wake on Lan feature must be used instead.
---------------------	---

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

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

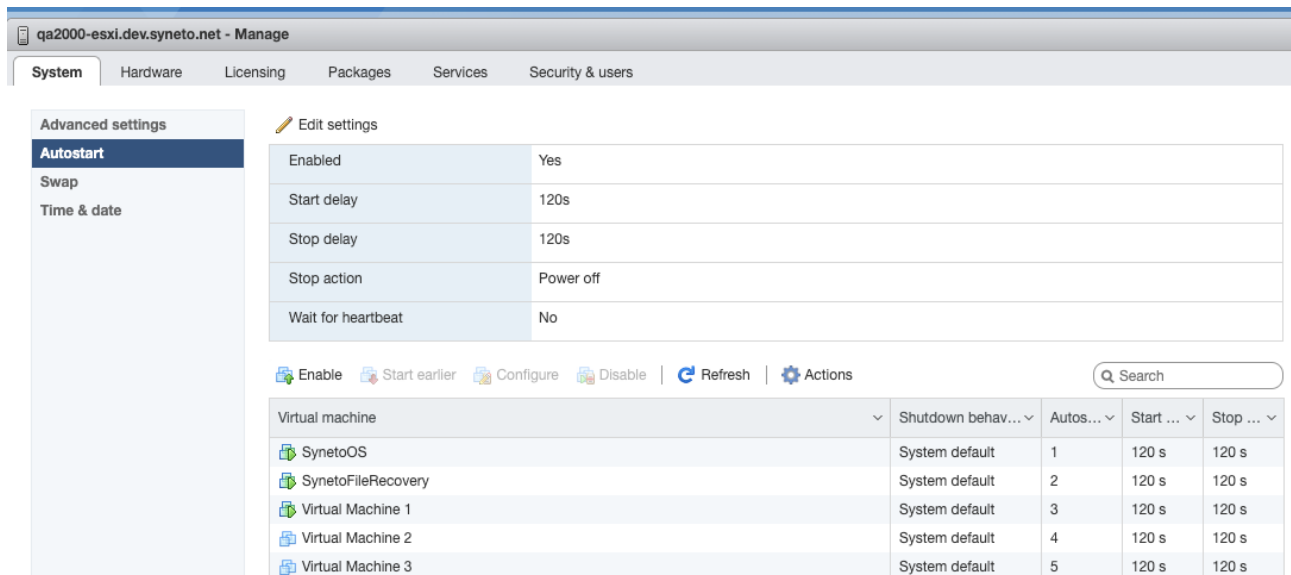
It is also possible to test the correct user account and password to login on a Prism CVM. The test will return the result with a pop-up screen.

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 204.

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.

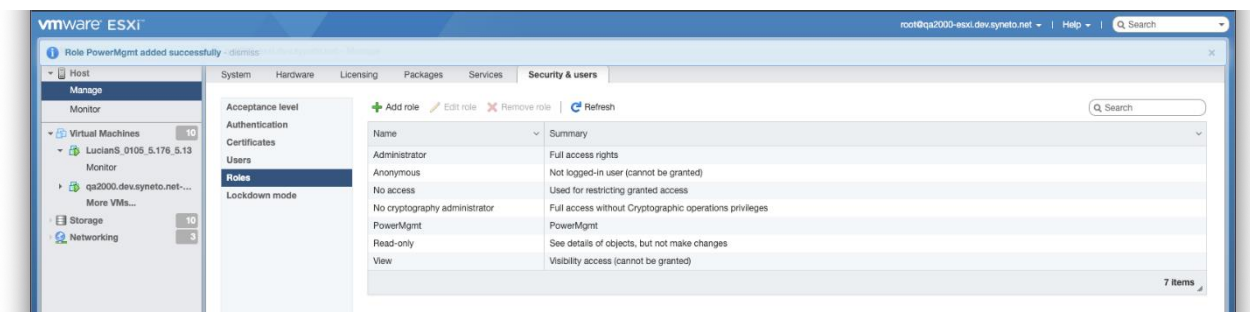


CONFIGURE ESXI USER & ROLE FOR REMOTE POWER MANAGEMENT

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.

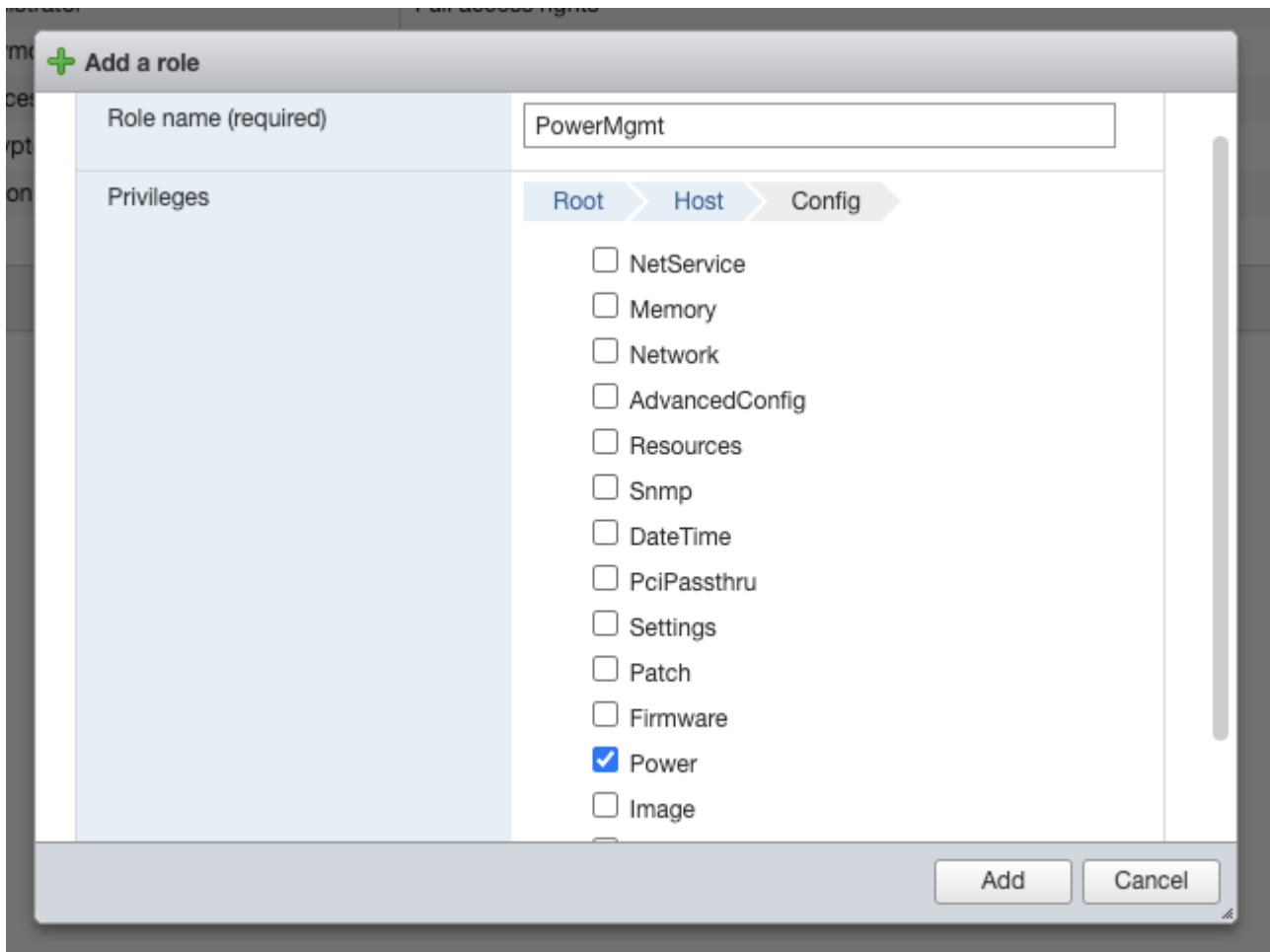
Go to Host -> Security and Users -> Roles.



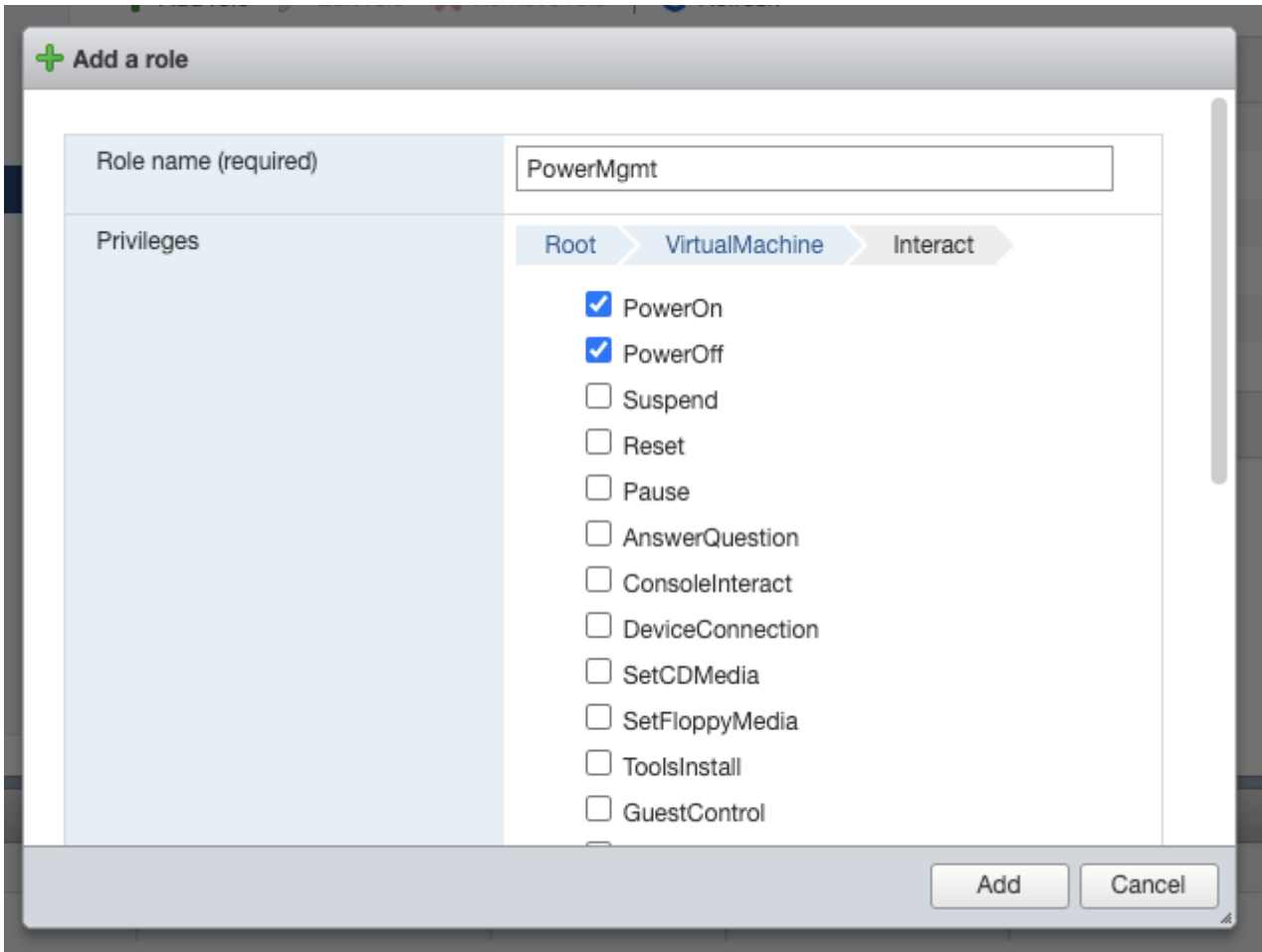
Click on Add Role. Give the new role a suggestive name, for example: PowerMgmt.

Choose the following from Privileges:

Root -> Host -> Config -> Power.



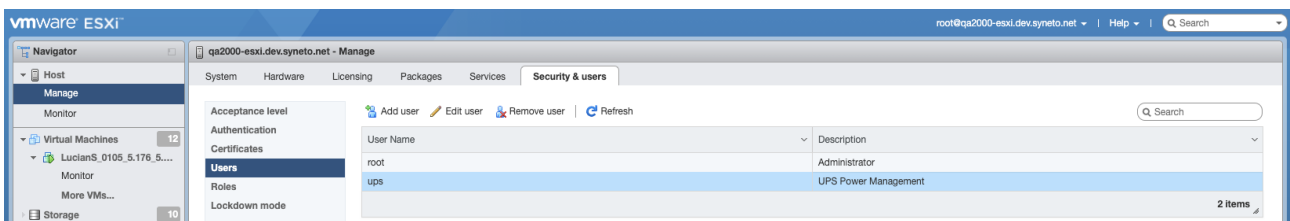
Root -> VirtualMachine -> Interact -> PowerOn, PowerOff



Click Add to create the new role.

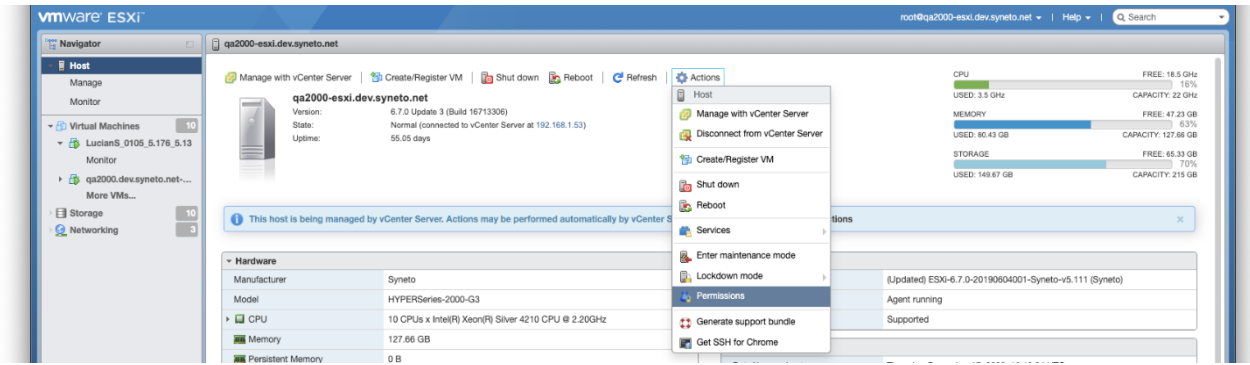
2. Create a new user.

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

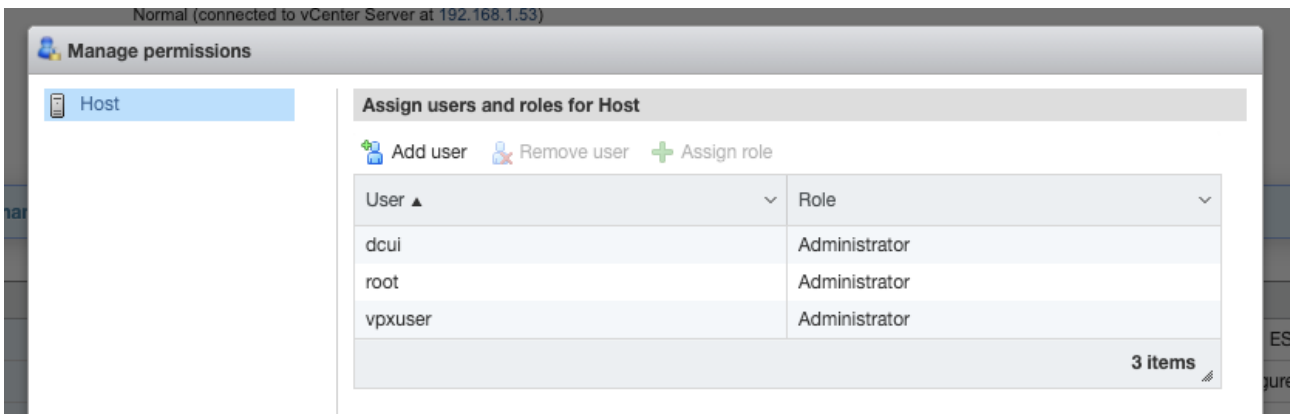


3. Assign the role PowerMgmt to the newly created user ups on the ESXi host.

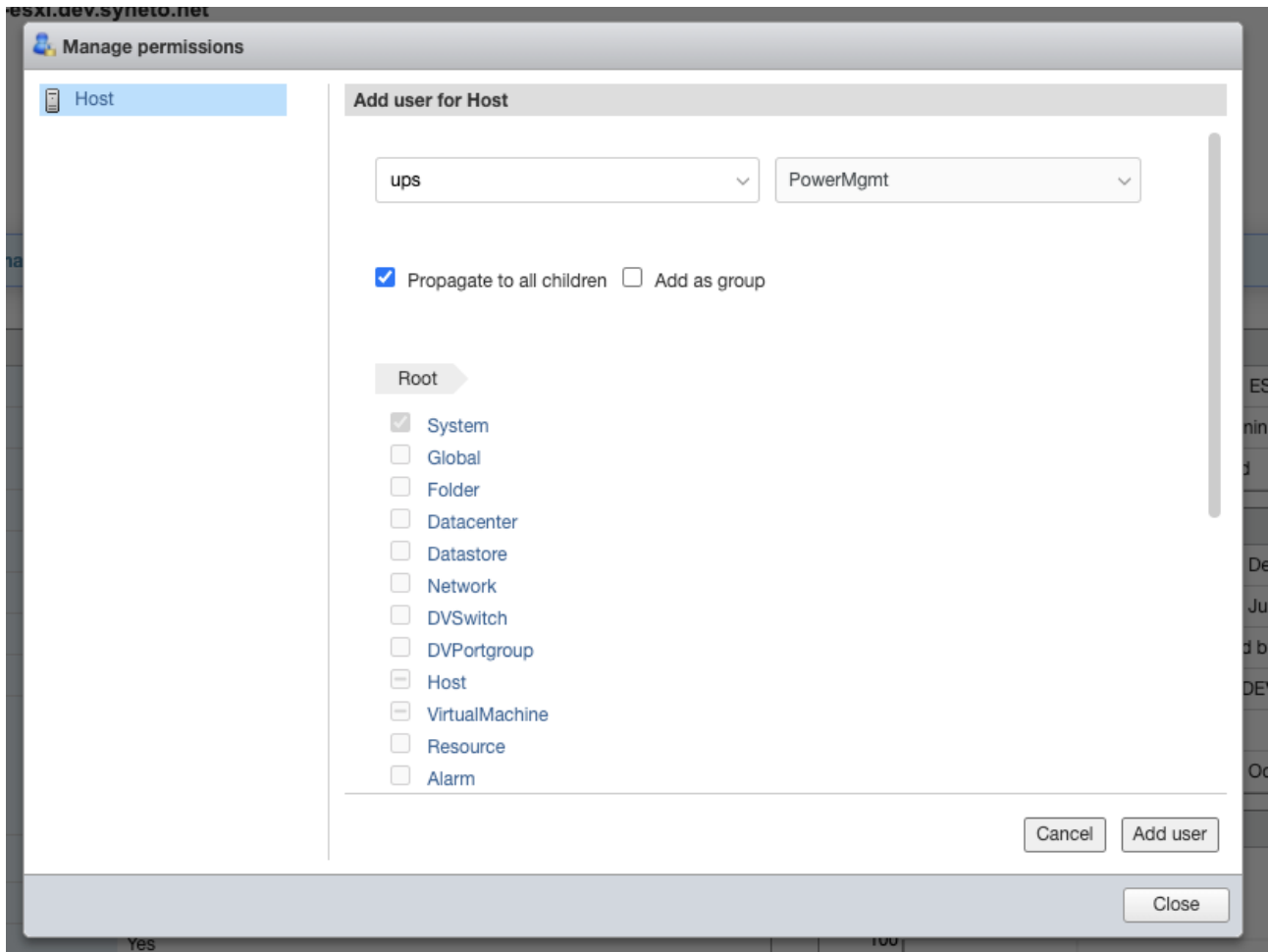
Go to Host -> Actions -> Permissions.



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



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 204 FOR HOST SHUTDOWN

Connect to Riello UPS Netman 204 via the web interface. Go to Configuration -> Remote Hosts -> Syneto

YOUR NETMAN 204 SENSORS MODEM REMOTE HOSTS

REMOTE HOSTS SHUTDOWN

- SSH
- VMware ESXi
- Nutanix
- Syneto**

Syneto

SYNETO

Enable Syneto shutdown

Infrastructure connectors

ESXi Hypervisor	Username	Password	
192.168.1.27	ups	Delete

Add Row

- Check the box for Enable Syneto shutdown
- In the section Infrastructure connectors, click on the Add Row button. You will connect *Netman 204* to the ESXi host.
- Enter the following:

ESXi Hypervisor	The ip address of your ESXi host or Vcenter
Username	The username you created for power management (eg: ups)
Password	The username you created for power management (eg: ups)

- 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
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>
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>

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="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

SHUTDOWN ON EVENT

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

Then, UPS shutdown after (seconds)

The Riello UPS with *Netman 204* will shutdown 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

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.

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.

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

NTP & Timezone configuration



Some *Netman 204* services require a correct date and time in order to work properly. It is therefore necessary to configure them as soon as possible to avoid malfunctions.

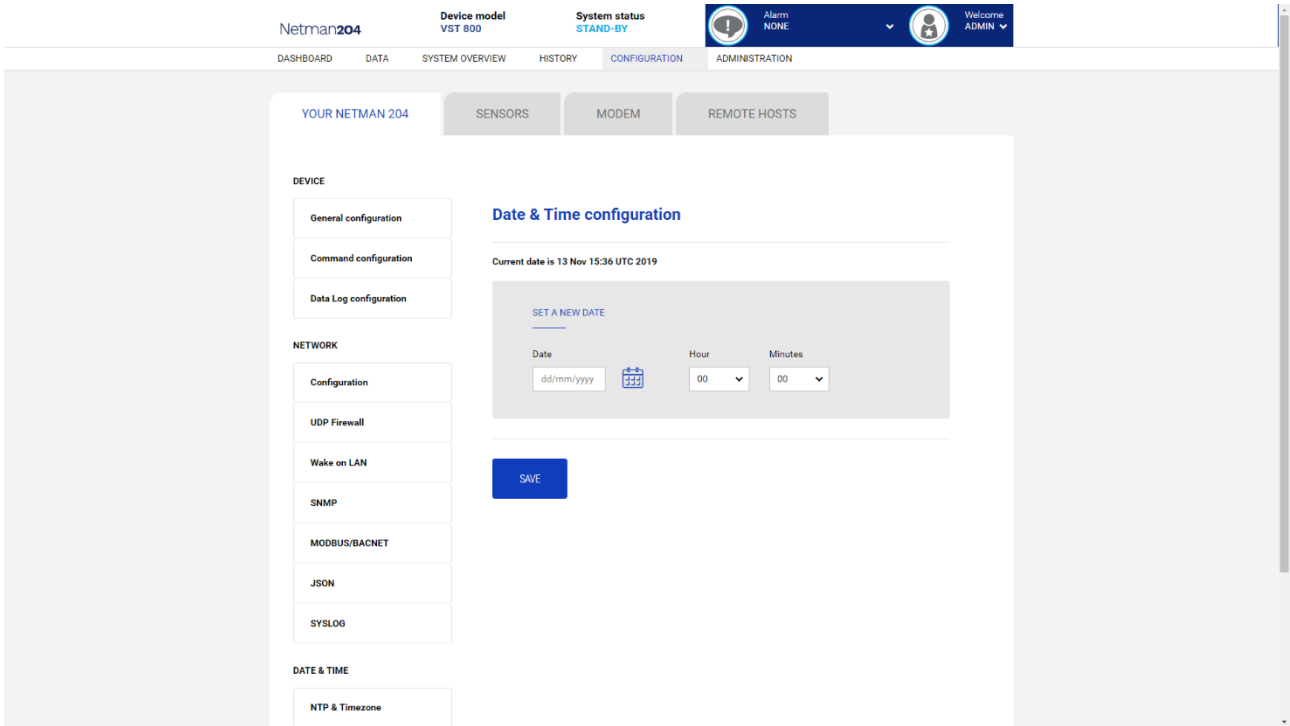
With this menu is possible to configure the NTP synchronization.

Field	Parameters to be inserted
NTP server address (IP)	Enter the name or address of the NTP server



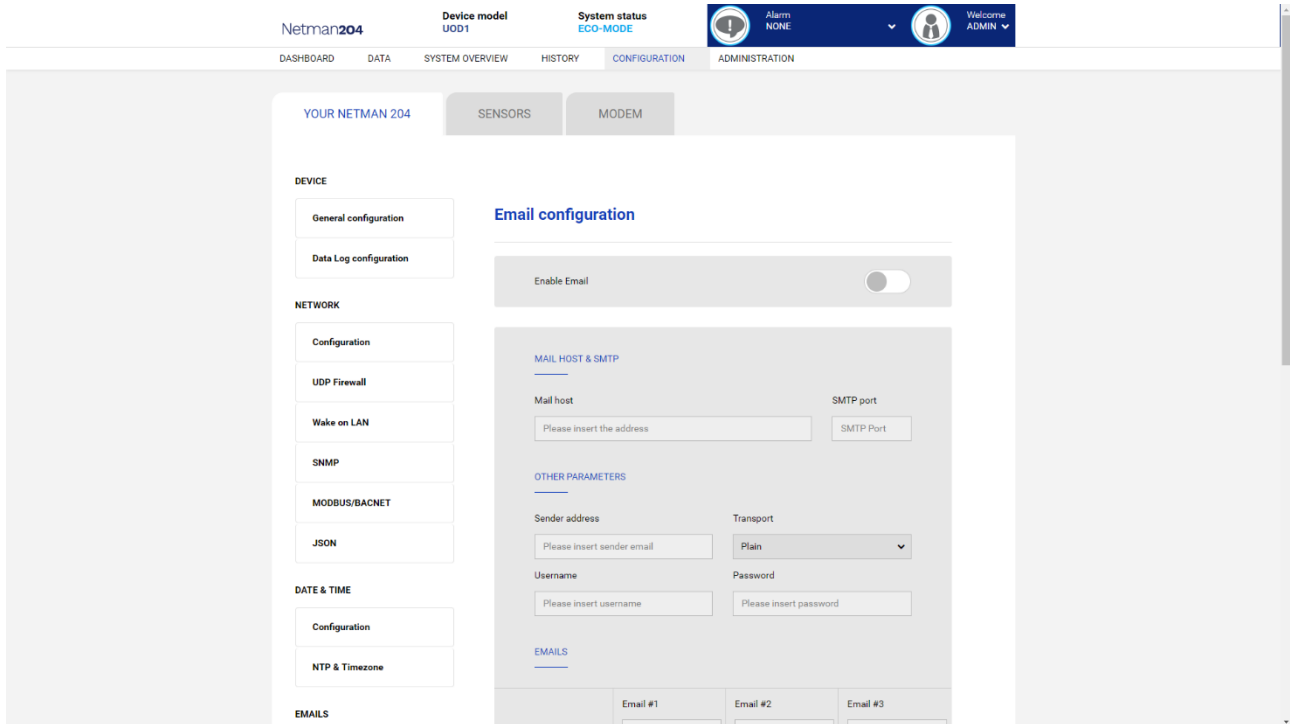
Only for some UPS models; if a valid time is received by the configured NTP server, *Netman 204* will synchronize the clock of the UPS daily at 00:30.

Date & Time configuration



Field	Parameters to be inserted
Date	Enter the current date
Hour	Enter the current hour
Minutes	Enter the current minutes

Email configuration



This menu may be used to configure the addresses to which to send the alarm notification and report e-mails and other parameters of the e-mail service as described in the following table.

Field	Parameters to be inserted
Enable Email	Enables the Email service
Mail host	Enter the name or the address of the SMTP server to be used to send e-mails. ⁽¹⁾
SMTP port	The IP port used by the SMTP protocol
Sender address	Enter the address from which the e-mails are sent. ⁽²⁾
Username	If the server requires authentication, insert the "User name".
Password	If the server requires authentication, insert the password.
Transport	It is possible to choose between plain, SSL or TLS.
Email #1	Enter the e-mail addresses to which to send the alarm notifications and reports (see note).
Email #2	
Email #3	
Device events	Choose the event upon which the email will be sent
Send report every day	Sends the email report every day at 00:00
Send report every week	Sends the email report every Monday at 00:00

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

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

After inserting 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.



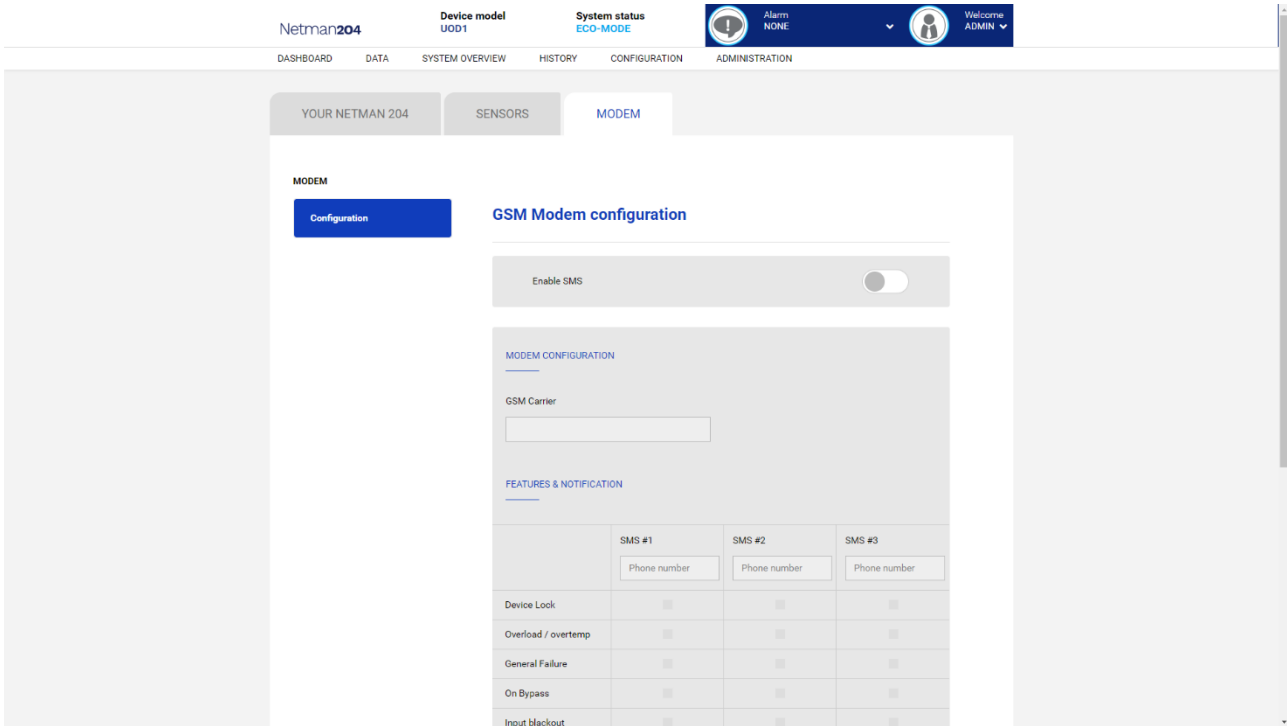
Report e-mails are sent to all the addresses inserted; for alarm notification e-mails see paragraph “*Email logic*”.

Email logic

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
Ovrload/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	Communication between the <i>Netman 204</i> and the device has been interrupted

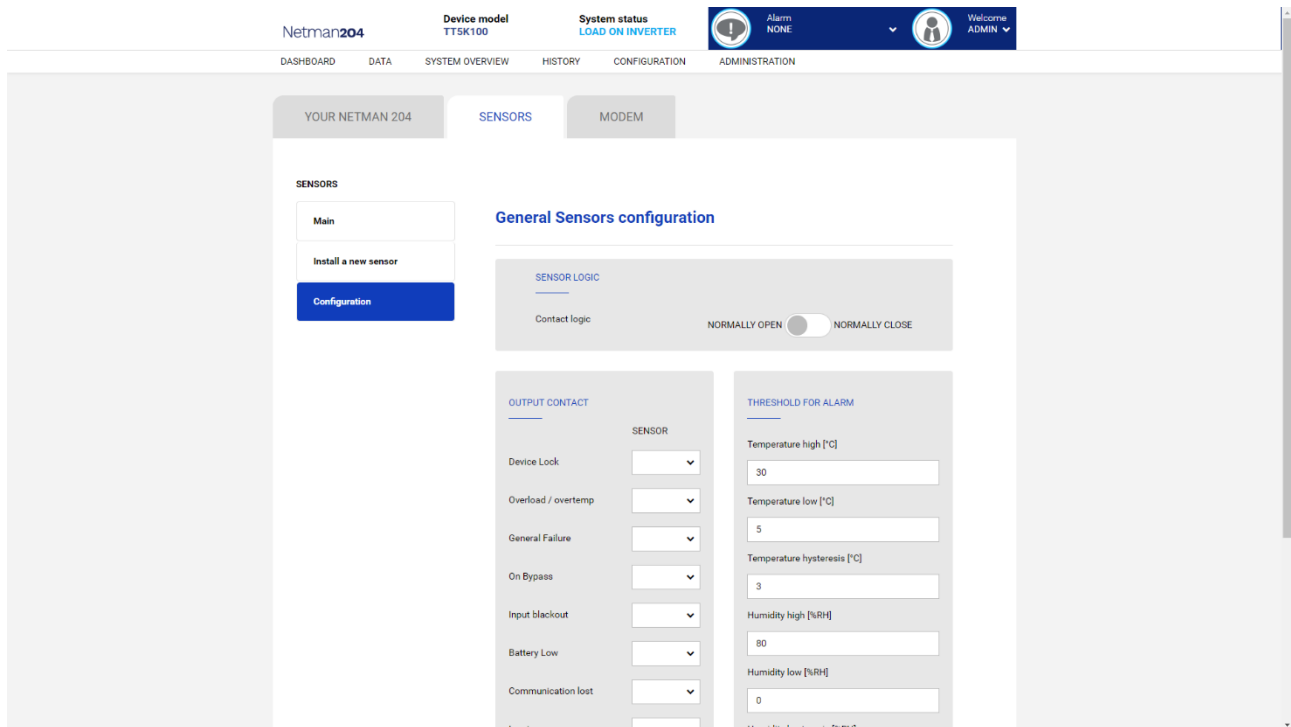
GSM Modem



This menu may be used to configure the GSM modem in order to send SMS.

Field	Parameters to be inserted
Enable SMS	Enables the SMS service
GSM carrier	Enter the phone number of the carrier
SMS #1	Phone numbers that will receive SMS
SMS #2	
SMS #3	
Device events	Choose the events upon which the SMS will be sent
Send report every day	Sends the SMS report every day at 00:00
Send report every week	Sends the SMS report every Monday at 00:00

Sensors



Field	Parameters to be inserted
Enable sensors	Enables the sensor service
Contact logic	Choose between normally open or normally closed
Output contact	Choose the output signal to be activated on event
Temperature high [°C]	Enter the high temperature threshold
Temperature low [°C]	Enter the low temperature threshold
Temperature hysteresis [°C]	Enter the temperature hysteresis
Humidity high [%RH]	Enter the high humidity threshold
Humidity low [%RH]	Enter the low humidity threshold
Humidity hysteresis [%RH]	Enter the humidity hysteresis



As well as being configured, the sensors must also be activated to function correctly (see paragraph “Sensors config”).

Sensors Config over SSH or USB



To enter on the “Sensors config” menu is necessary to enable the “Sensors” service and to reboot the *NetMan 204*.

```
Sensor list
```

```
Press [C] to change sensors, [E] to exit
```

Enter on the “Config sensor” menu, connect the first sensor and press “C”. After some instants the device will be recognized and the device will be given an identifier number [1]. Connect the next sensor, if present, and press “N”. After some instants the device will be recognized and the device will be given an identifier number [2]. Repeat the procedure for all the sensors and when the configuration is finalized press “Y”.

```
Sensor list
```

```
1) Temperature [F100000013BE0628]  
2) Humidity & Temperature [4D00000083FF3326]  
3) Digital I/O & Temperature [BB0000003BA2FF12] [510000009A154228]
```

```
Press [Y] to confirm, [N] to insert a new sensor
```



For proper working of the devices, it is necessary to add just one device for each iteration and wait that it is recognized by *NetMan 204*.

Example: how to connect a *Temperature* sensor, a *Humidity & Temperature* sensor and a *Digital I/O & Temperature* sensor in exactly this order.

```
Sensor list
```

```
Press [C] to change sensors, [E] to exit
```

Connect the first sensor (*Temperature*), and press “C”.

```
Sensor list
```

```
1) Temperature [F100000013BE0628]
```

```
Press [Y] to confirm, [N] to insert a new sensor
```

Wait until the first sensor is identified and then connect the second sensor (*Humidity & Temperature*), and press “N”.

```
Sensor list
1) Temperature [F100000013BE0628]
2) Humidity & Temperature [4D00000083FF3326]

Press [Y] to confirm, [N] to insert a new sensor
```

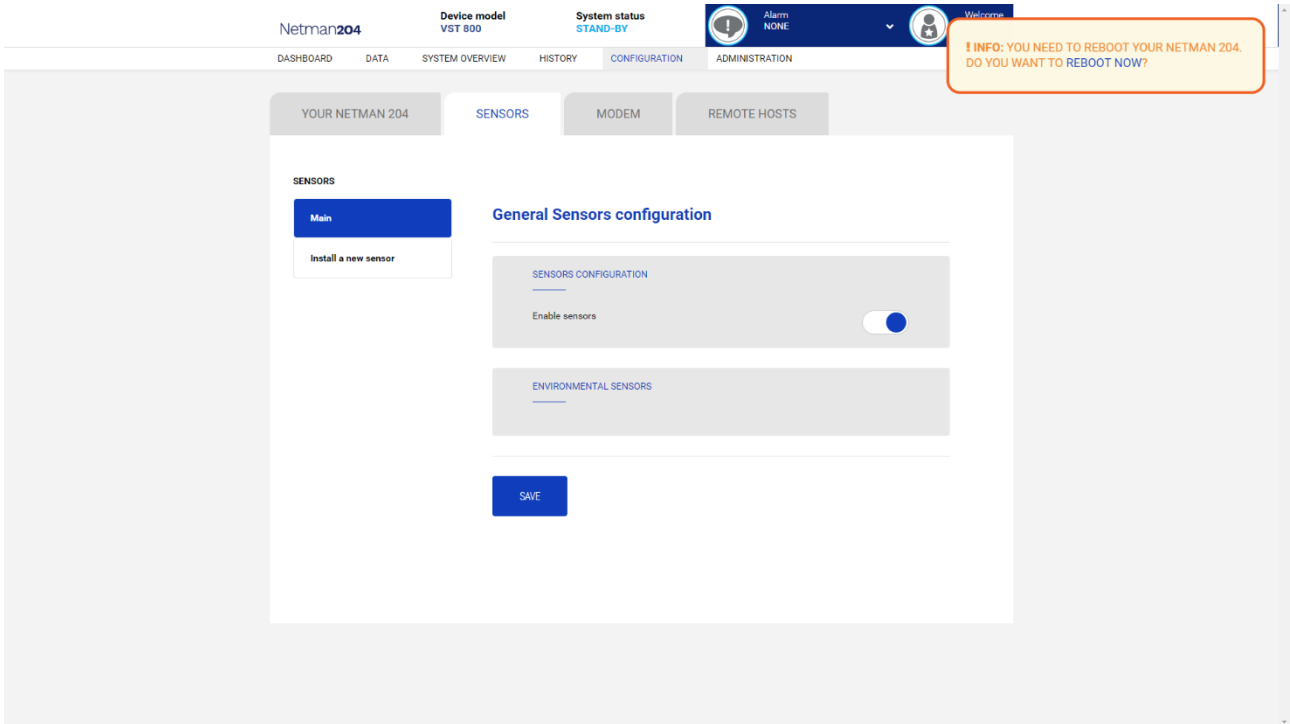
Wait until the second sensor is identified and then connect the third sensor (*Digital I/O & Temperature*), and press “N”.

```
Sensor list
1) Temperature [F100000013BE0628]
2) Humidity & Temperature [4D00000083FF3326]
3) Digital I/O & Temperature [BB0000003BA2FF12] [510000009A154228]

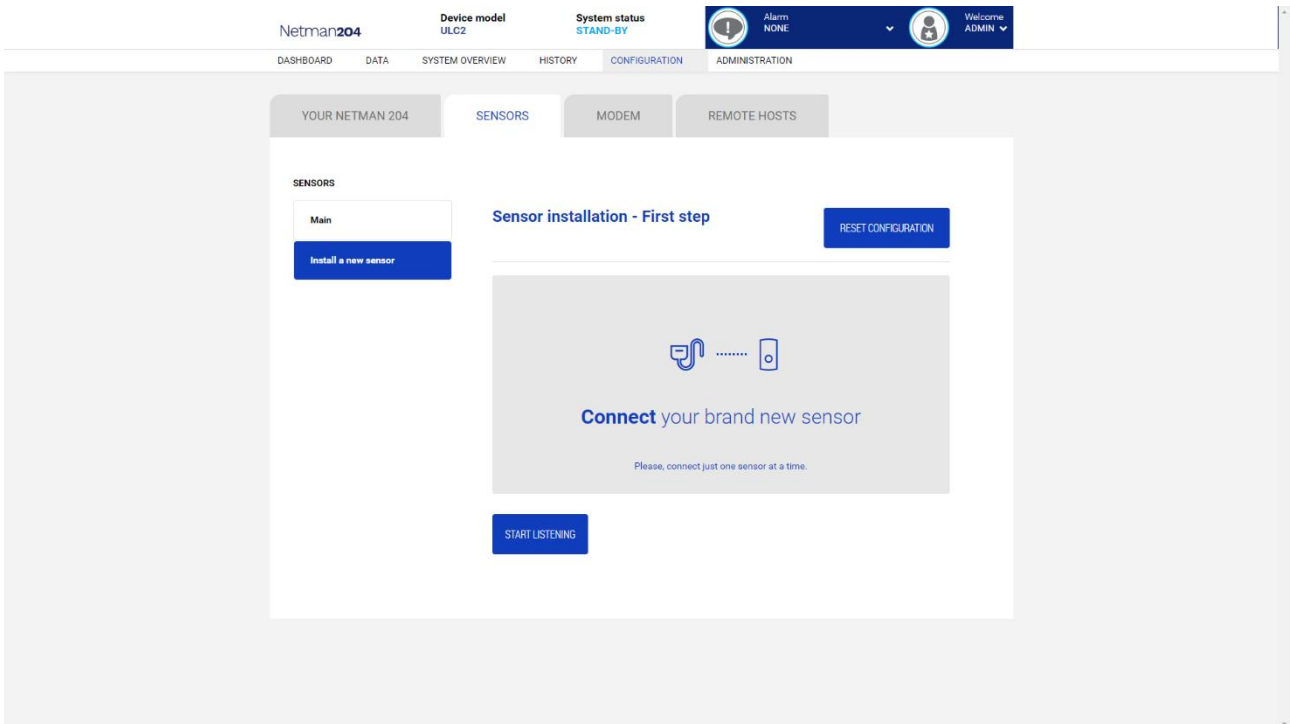
Press [Y] to confirm, [N] to insert a new sensor
```

Press “Y” to confirm.

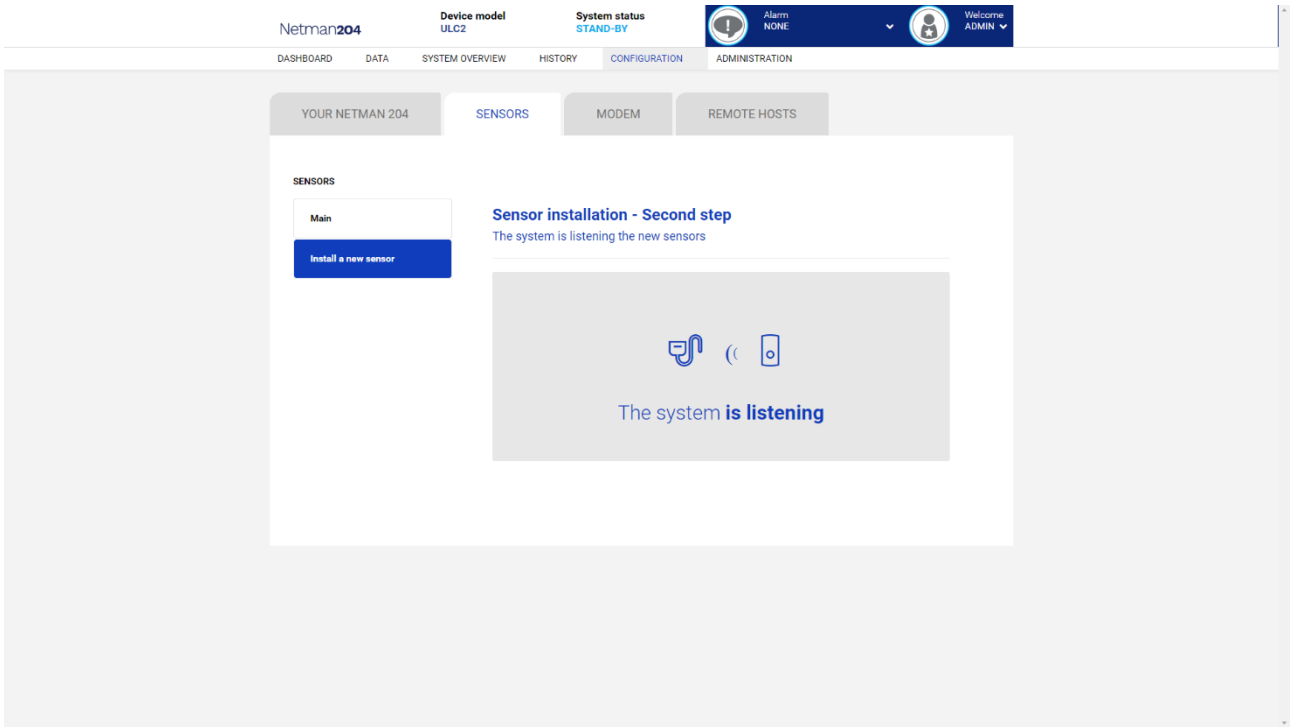
Sensors Config over HTTP



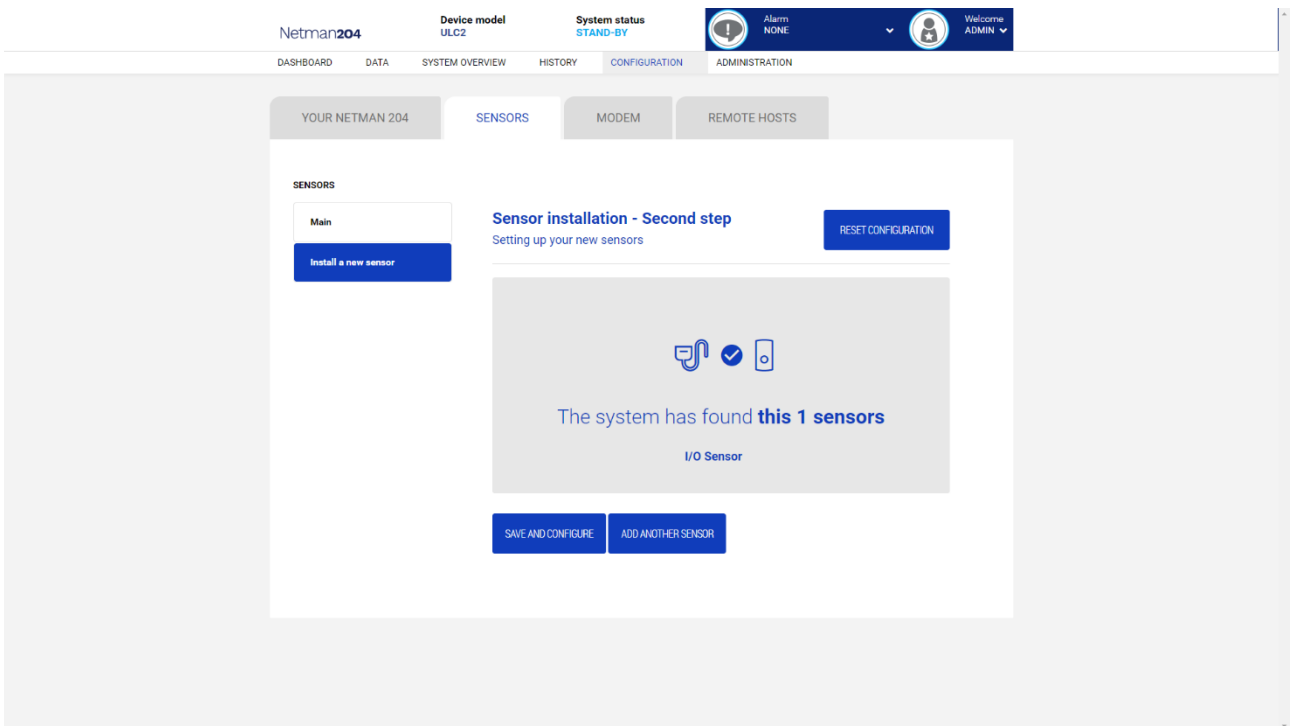
Enable the “Sensors” service and to reboot the *Netman 204*.



Click “Install a new sensor” to access the sensor installation page. Click “Reset configuration” and then connect the first sensor and click “Start listening”.

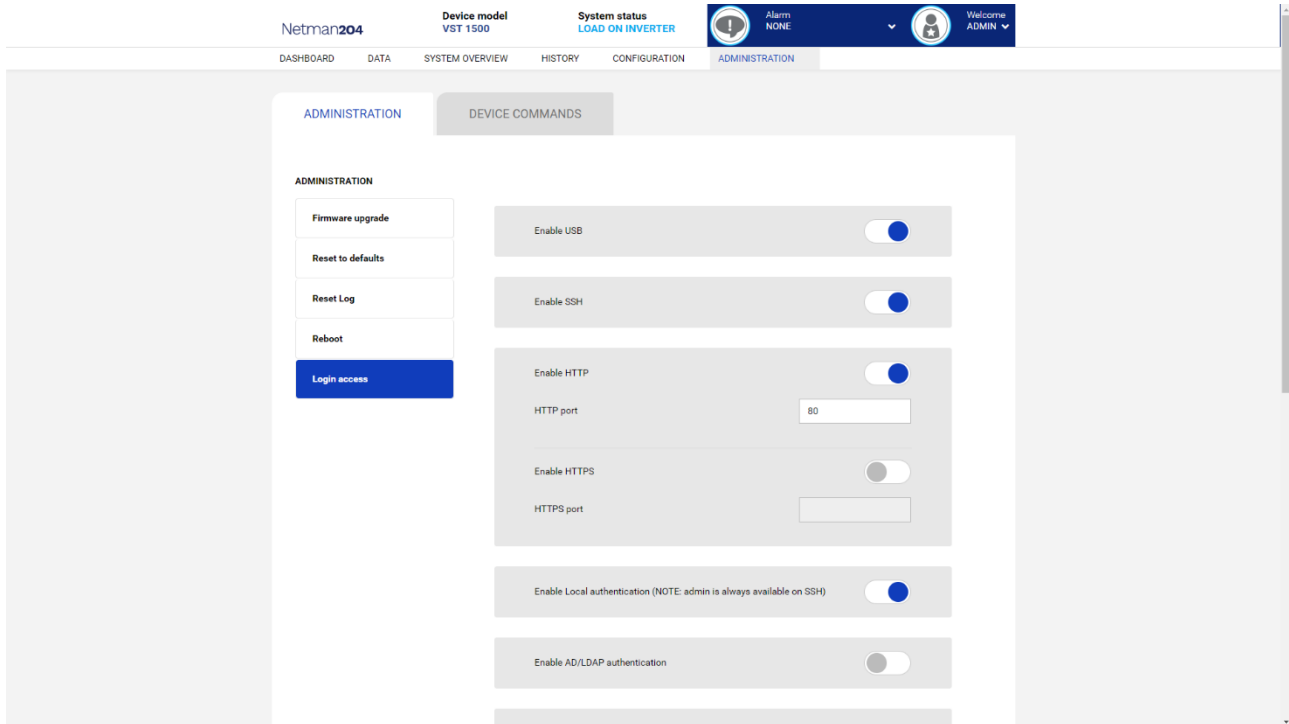


After some instant, the sensor will be detected



Click “Add another sensor” if another sensor needs to be installed, or “Save and configure” to complete the installation.

Login access configuration



It is possible to manage the login via LDAP or AD. The user must be present on the server and must belong to a specified group. If the group is the “Admin group” then the user will be granted the “admin” privileges. If the group is the “Power group” then the user will be granted the “power” privileges (i.e. without the privilege of performing shutdown on the device). After configuration, on the login screen it must be inserted only the username (instead of the full Distinguished Name) and the password.

Field	Parameters to be inserted
Enable USB	Enables login over USB cable
Enable SSH	Enables login over SSH
Enable HTTP	Enables the HTTP service
HTTP port	Enter the port where HTTP service is started (default: 80)
Enable HTTPS	Enables the HTTPS service
HTTPS port	Enter the port where HTTPS service is started (default: 443)
Enable local authentication	Enable local authentication
Enable LDAP/AD authentication	Enables login via LDAP or AD
Server address	The address of the server, can be either ldap:// or ldaps://
LDAP users folder	The folder of users allowed to log in
Admin group name	The group with “Admin” privileges
Power group name	The group with “Power” privileges

Examples of LDAP server addresses:

```
ldap://myserver:389/  
ldap://10.1.10.99:389/
```

Over secure socket:

```
ldaps://myserver:636/  
ldaps://10.1.10.99:636/
```

If the user "john" is present on the LDAP server and it belongs to the configured groups, it will be possible to login with username "john" and its LDAP password.

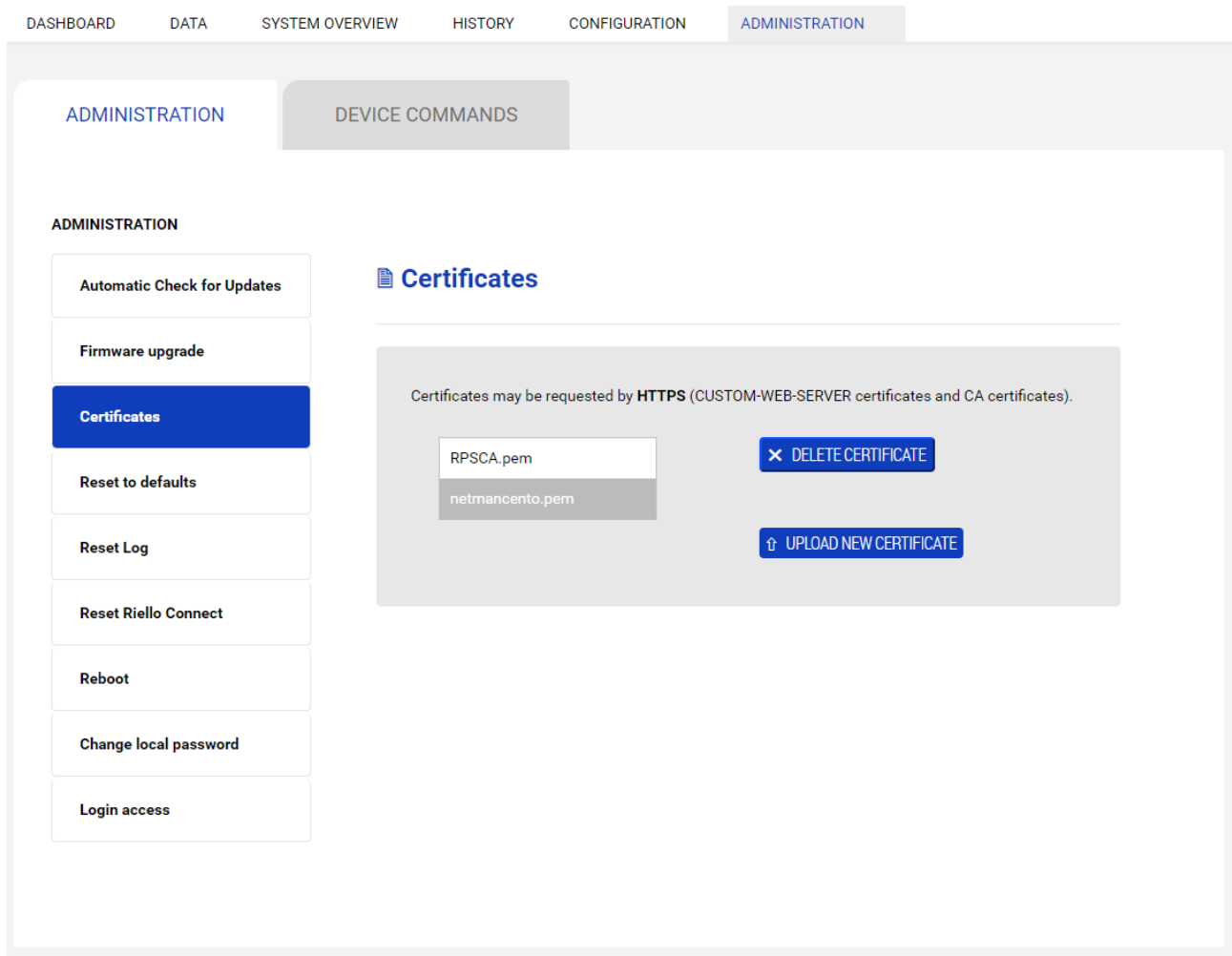
Certificates

For HTTPS the *Netman 204* provides an internal self-signed certificate, covering the basic usage. The User can load and set:

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

as optional for a more secure HTTPS connection.

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



where the certificates can be only:

- **uploaded** into the *Netman 204*
- **deleted** from the *Netman 204*

In no way the certificates can be viewed or downloaded.

Certificates must follow some 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.

After the proper certificate upload, the certificates can be set in the HTTPS configuration:

The screenshot displays the Administration menu on the left, with 'Login access' selected. The main content area is divided into two sections: 'Login access' and 'HTTPS'.

ADMINISTRATION

- Automatic Check for Updates
- Firmware upgrade
- Certificates
- Reset to defaults
- Reset Log
- Reset Riello Connect
- Reboot
- Change local password
- Login access**

Login access

- 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...'):
- Enable USB:
- Enable SSH:

HTTP

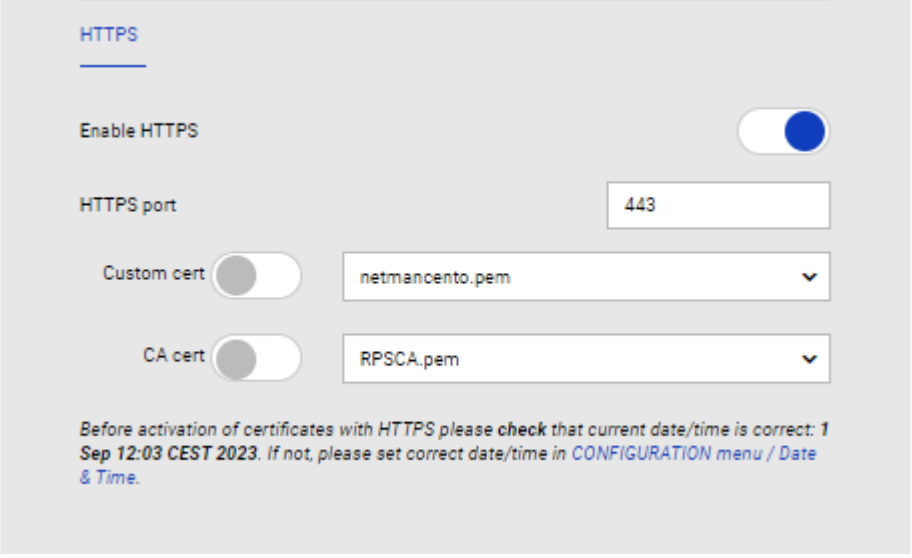
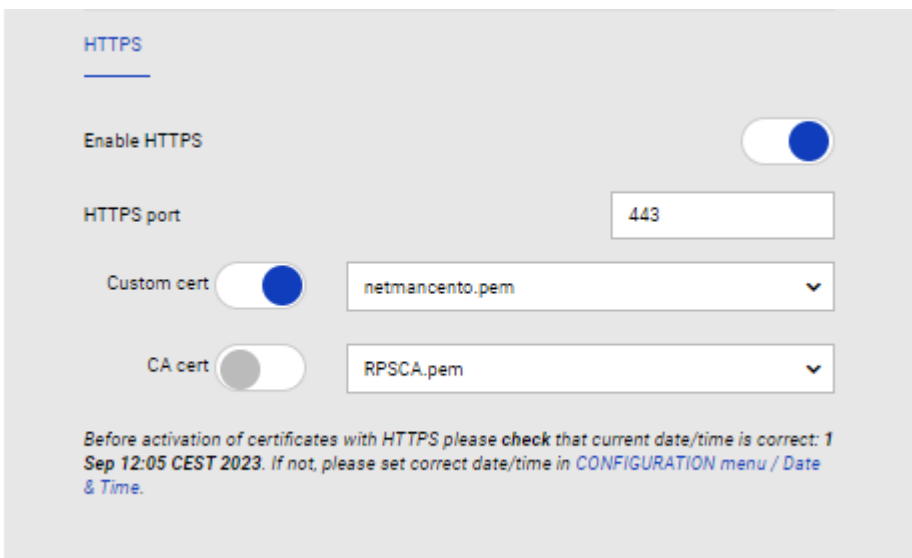
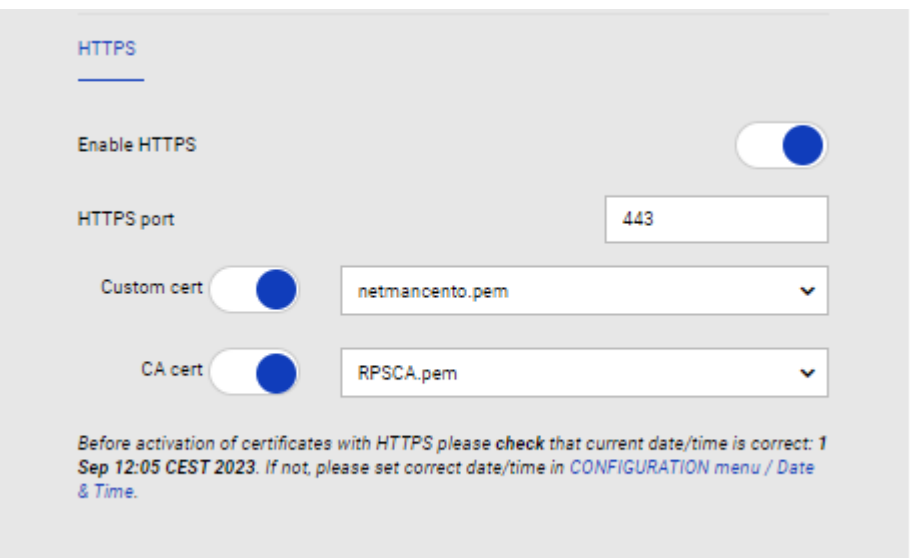
- Enable HTTP:
- HTTP port:

HTTPS

- Enable HTTPS:
- HTTPS port:
- Custom cert:
- CA cert:

Before activation of certificates with HTTPS please check that current date/time is correct: 1 Sep 12:01 CEST 2023. If not, please set correct date/time in CONFIGURATION menu / Date & Time.

where possible configurations can be set:

<p>only internal self-signed certificate</p>	 <p>The screenshot shows the 'HTTPS' configuration panel. The 'Enable HTTPS' toggle is turned on. The 'HTTPS port' is set to 443. The 'Custom cert' toggle is turned off, and the 'CA cert' toggle is also turned off. Both dropdown menus show 'netmancento.pem' and 'RPSCA.pem' respectively. A warning message at the bottom states: 'Before activation of certificates with HTTPS please check that current date/time is correct: 1 Sep 12:03 CEST 2023. If not, please set correct date/time in CONFIGURATION menu / Date & Time.'</p>
<p>Only custom certificate</p>	 <p>The screenshot shows the 'HTTPS' configuration panel. The 'Enable HTTPS' toggle is turned on. The 'HTTPS port' is set to 443. The 'Custom cert' toggle is turned on, and the 'CA cert' toggle is turned off. Both dropdown menus show 'netmancento.pem' and 'RPSCA.pem' respectively. A warning message at the bottom states: 'Before activation of certificates with HTTPS please check that current date/time is correct: 1 Sep 12:05 CEST 2023. If not, please set correct date/time in CONFIGURATION menu / Date & Time.'</p>
<p>Custom certificate with CA certificate</p>	 <p>The screenshot shows the 'HTTPS' configuration panel. The 'Enable HTTPS' toggle is turned on. The 'HTTPS port' is set to 443. Both the 'Custom cert' and 'CA cert' toggles are turned on. Both dropdown menus show 'netmancento.pem' and 'RPSCA.pem' respectively. A warning message at the bottom states: 'Before activation of certificates with HTTPS please check that current date/time is correct: 1 Sep 12:05 CEST 2023. If not, please set correct date/time in CONFIGURATION menu / Date & Time.'</p>

Date and time

Using the certificates for HTTPS the Date and Time of the *Netman 204* must be set correct, otherwise the HTTPS verification fails.

Possible problem with wrong date/time:

- web pages with HTTPS are not responding and the *Netman 204* is no more reachable via Web

The only solution is:

- ⇒ restore the original HTTP connection and then reconfigure the HTTPS again. Please see “**Troubleshooting**” section below for the procedure description.

Certificate validity

Even when date/time is correct:

- certificates outdated are used
- certificates generated with future date/time Start validation are used

then the HTTPS Web pages will not response anymore.

The only solution is:

- ⇒ restore the original HTTP connection and then reconfigure the HTTPS again setting the correct certificates. Please see “**Troubleshooting**” section below for the procedure description.

Changing certificates

With some browsers, changing the configuration of the certificates in the *Netman 204* it may require closing and re-opening the browser window itself for using the new certificates.

CA certificate for Browser

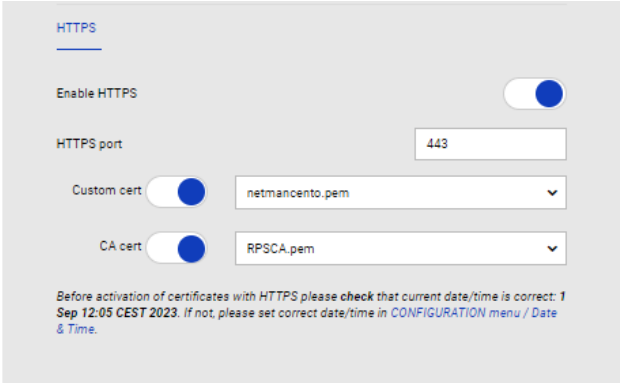
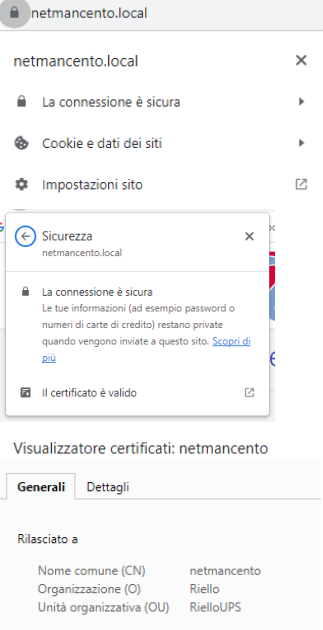
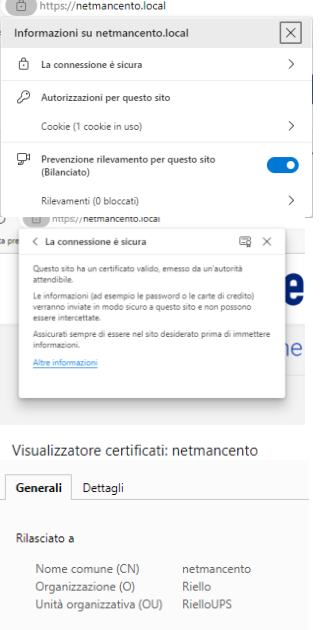
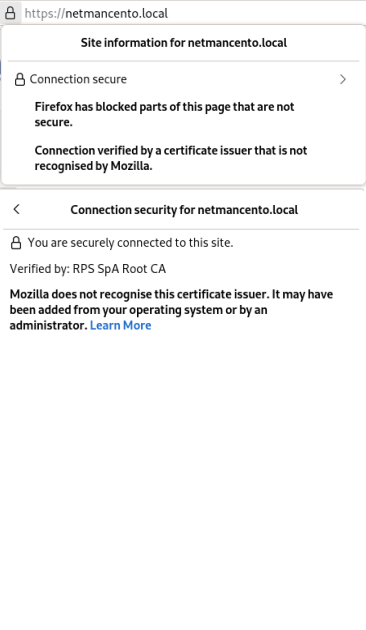
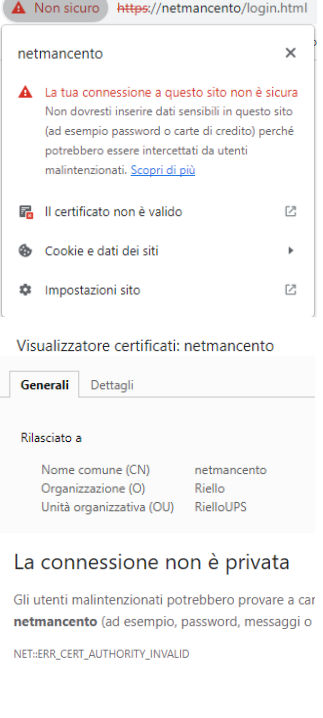
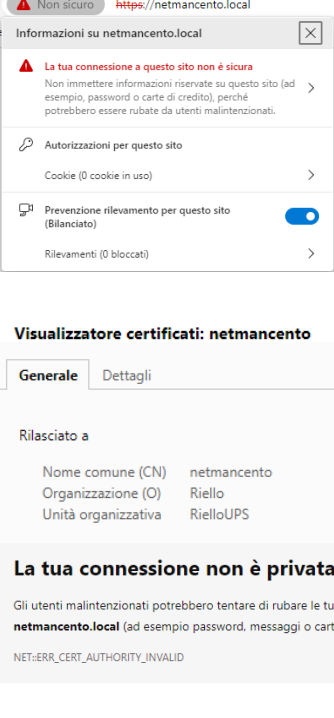
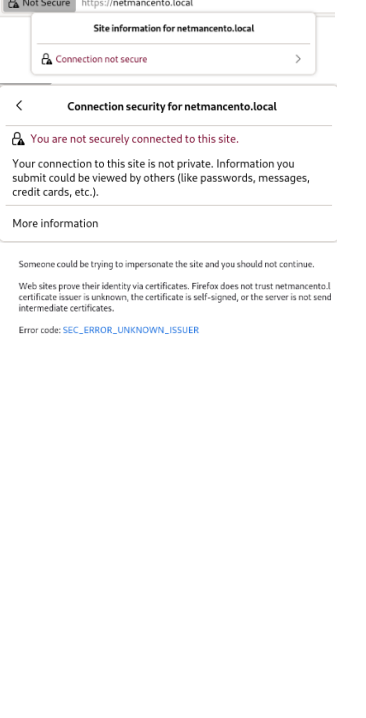
Usually, a well-structured Local Network should set and provide “as ready” the correct CA certificate to any client Web browser in its network.

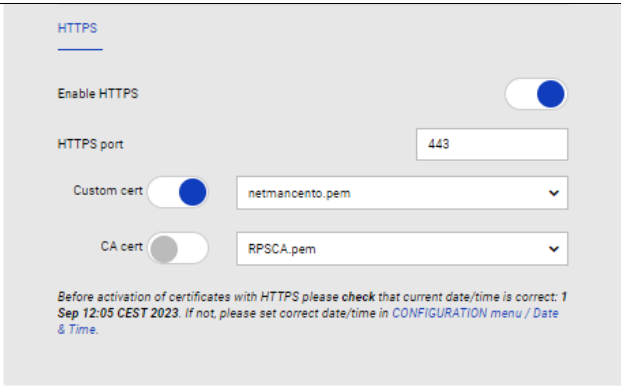
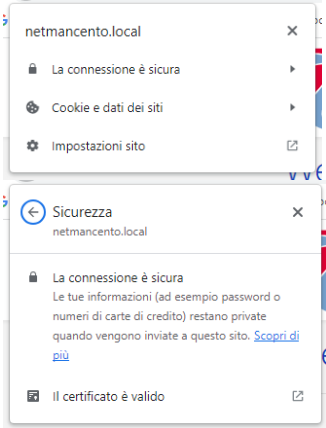
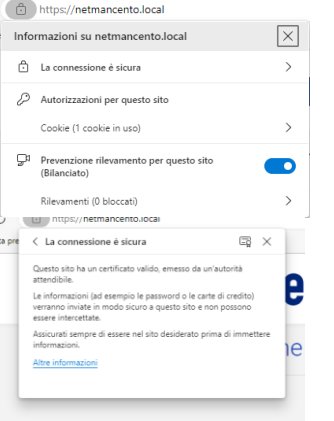
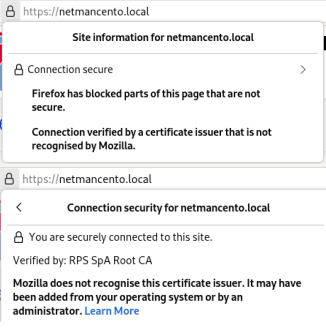
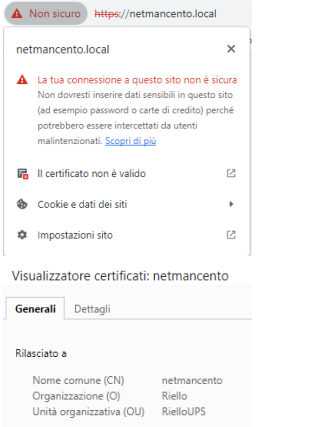
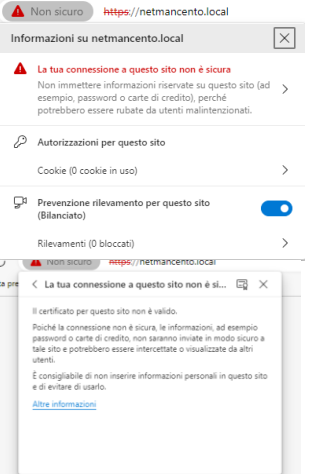
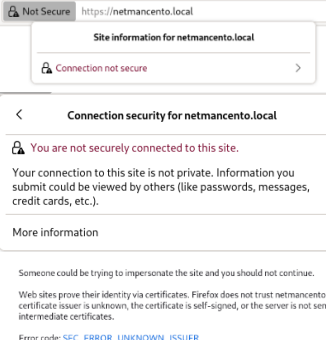
When the client Web browser does not know the CA issuer the Custom Certificate of the *Netman 204*, the User must import the CA certificate of the CA Issuer into its client Web browser as “trusted certification authority”. The procedure of importing the CA root/intermediate certificate is different depending on the browser used.

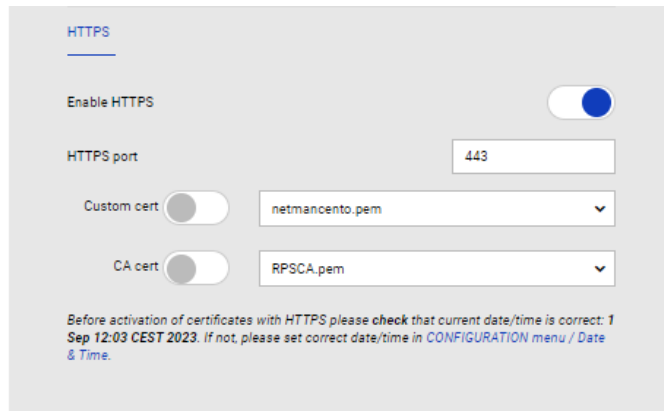
When is needed:

- when CA authority is a secondary server inside the local network
- when an external client must connect to the *Netman 204* from outside and it must know the original CA signing the *Netman 204* certificate.

Test cases (different configurations with different Web browsers)

Chrome	Edge	Firefox	Status
			<p>Netman 204: + HTTPS + custom cert + CA cert</p>
			<p>✓ CA known by the browser (cert installed in the browser)</p>
			<p>✗ CA not known by the browser (cert installed in the browser)</p>

		<p>Netman 204: + HTTPS + custom cert</p>	
			<p>✓ CA known by the browser (cert installed in the browser)</p>
			<p>✗ CA not known by the browser (cert installed in the browser)</p>



Netman 204:
+ HTTPS
+ self-signed cert

			<p>✘</p>
--	--	--	----------

Troubleshooting Web browser errors

With wrong certificates, browsing web pages with *Netman 204* can show various messages that hide many reasons. Here some messages to know:

NET::ERR_CERT_COMMON_NAME_INVALID

Custom Certificate set for HTTPS is valid for a different hostname/FQDN. If the User encounters this message means that the active Custom Certificate covers a different *Netman 204* hostname, not the hostname of the running *Netman 204*.

The User can continue the Web activity but is unsecure because wrong certificate.

E.g.:

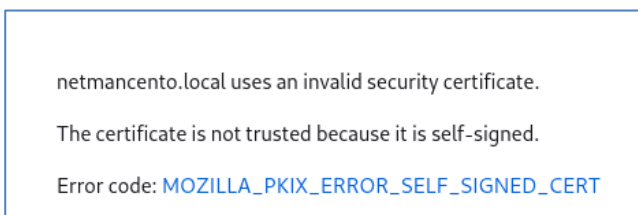
Active Netman 204 hostname: **netmanmille.local**
 Certificate for FQDN/hostname: **netmancento.local**



NET::ERR_CERT_AUTHORITY_INVALID

This message mainly suggests the **CA certificate is wrong**.

Other times can mean that the certificate is a **self-signed certificate** (e.g. in Chrome).

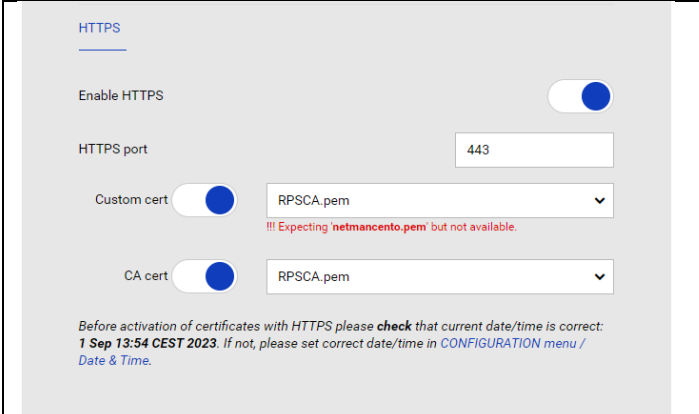


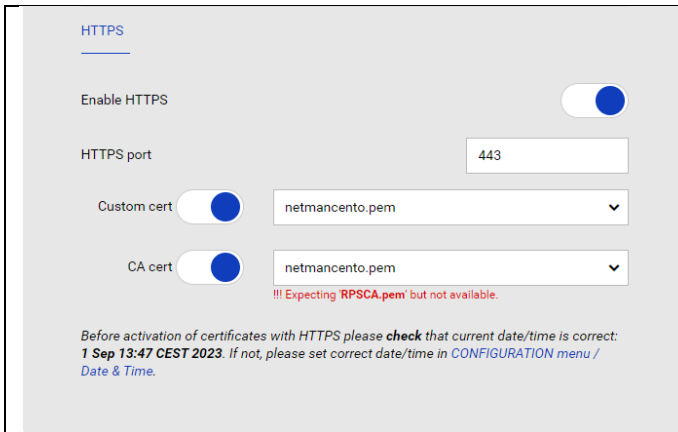
MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT

This message is clearly related to a Custom Certificate **self-signed**.

Missing certificates

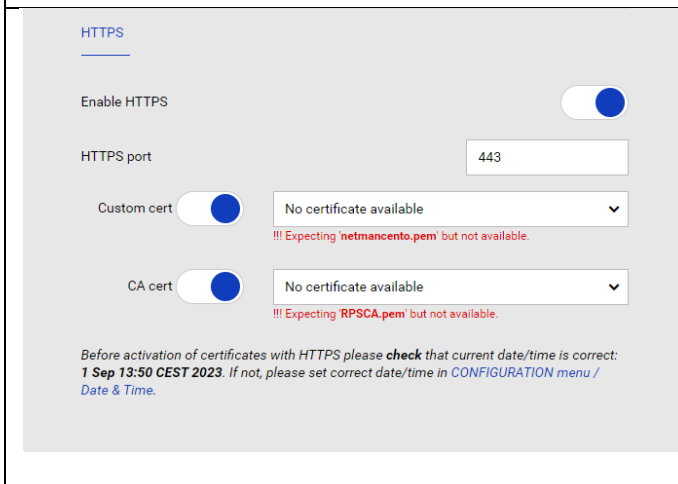
If custom & CA certificates are set in the configuration, but they are not available (maybe deleted), some warnings are shown and actions taken:

Warnings	Action taken
	<p>The configuration for HTTPS, at next reboot, it will use the default: SELF_SIGNED CERTIFICATE ignoring the custom cert “netmancento.pem” missing and ignoring the still available CA “RPSCA.pem”</p> <p><i>Reason: the CA cert is strongly related to the missing custom cert.</i></p>



The configuration for HTTPS, at next reboot, it will use only the:
CUSTOM CERT
 ignoring the missing CA “RPSCA.pem”.

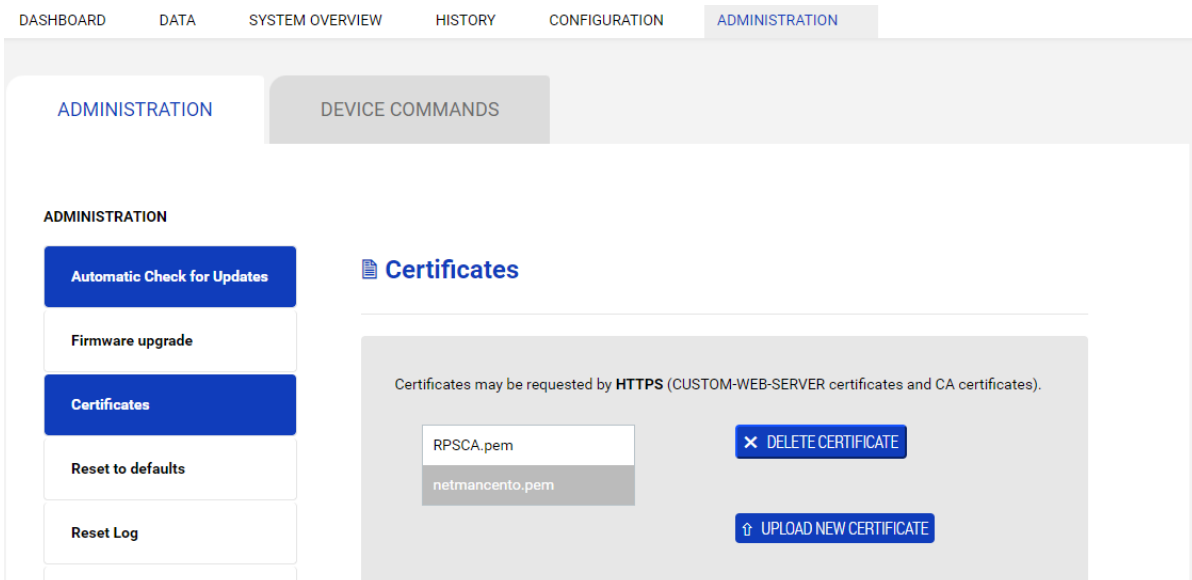
Reason: without CA the HTTPS is still reachable, other than the warnings.



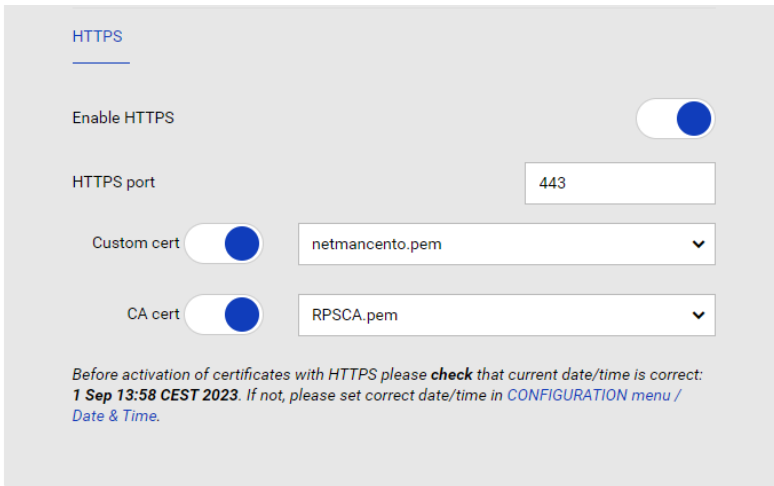
Both Custom and CA cert missing, then it will be used the default:
SELF_SIGNED CERTIFICATE
 only.

Reason: without the certificates the HTTPS is still reachable with internal self-signed cert, other than the warnings.

In any case of missing certificates, the User must upload the correct certificates in the dedicated menu:



and restore the correct behaviour without the red warnings:



HTTPS Web non reachable:

- Netman 204 Web is not responding.
- Web browser is reporting errors with Netman 204 Web

Possible causes:

- malformed certificate (CUSTOM and/or CA)
- expired certificate (CUSTOM and/or CA)
- wrong date/time in the Netman 204

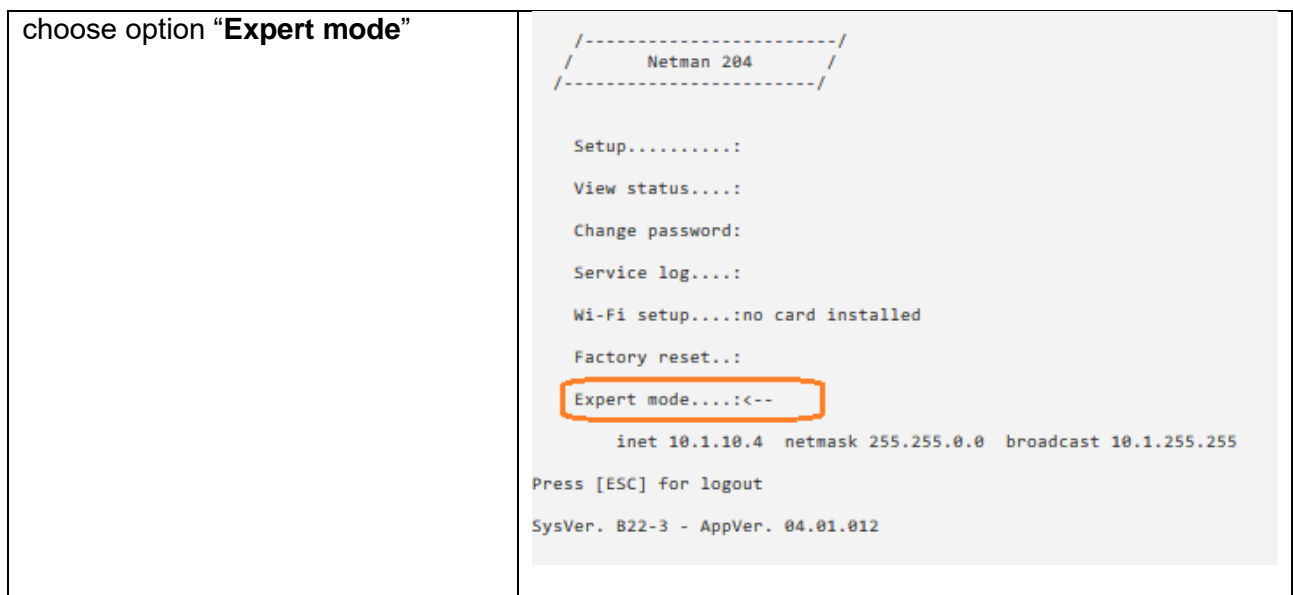
How to solve:

Via SSH command (network):

```
ssh -l admin netmancento.local
>>>> admin
```

or via USB cable connection:

```
COMx / 115200
>>>> admin
```



<p>and set Netman 204 to basic HTTP manually:</p> <pre>set http_enable true set http_port 80 set https_enable false</pre> <p>then reboot the Netman 204:</p> <pre>reboot</pre>	<pre>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 erasefram erase the FRAM module clearlog clear data log and event log exit closes the connection netman>set http_enable true netman>set http_port 80 netman>set https_enable false netman>reboot Connection to netmancento.local closed.</pre>
--	---

After reboot, the *Netman 204* will allow **connection via HTTP** basic mode ignoring any HTTPS or certificate settings, keeping all other configuration as it was.

Password recovery

If the default password for the admin user is changed and forgotten, it is possible to recover it with the unlock key provided by the service department of the manufacturer.

To obtain the unlock key, you must send to the service department the service code of your *NetMan 204*. This code can be read via USB or via HTTP.

Via USB log in to *NetMan 204* with user "user" and password "user".

Via HTTP when you insert an incorrect password you are offered a link to a password recovery. Click the link to start the recovery.

In both case a message like this will be shown:

To restore the default password, please enter the unlock key.

If you don't know it, please send to service this code:

204:XX:XX:XX:XX:XX:XX



Please note that the unlock key is valid only for the corresponding service code which is specific for every *NetMan 204*.

Wi-Fi setup (optional card required)



For Wi-Fi connection, an optional card is required. The Wi-Fi card is not provided with *NetMan 204* but it has to be purchased separately.

After installing the optional Wi-Fi card, you can access to the "Wi-Fi setup" menu.



For *NetMan 204*, Wi-Fi is an exclusive alternative to cabled Ethernet: only one at time can be used. Therefore, after enabling Wi-Fi, it is not more possible to use cabled Ethernet.

After selecting Wi-Fi setup you get this prompt:

```
Wi-Fi Configuration
Do you want to use Wi-Fi instead of Ethernet [y/n]?
```

Insert 'n' to use Ethernet or 'y' to use Wi-Fi. In the latter case, a list of available Wi-Fi access points will be shown with the following request:

```
Please insert the SSID you want to connect without quotes
```

Type the SSID of the desired Wi-Fi access point.

```
Please insert the password for <wi-fi access point>
```

Here you insert the authentication password for Wi-Fi.

```
OK, you want to connect to <wi-fi access point> with password <wi-fi
password>.
Confirm [y/n]? >
```

After confirmation, you will return to the Main setup. At the next boot the *NetMan 204* will use Wi-Fi instead of Ethernet.

Expert mode

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

help	prints the 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
reboot	reboot the <i>NetMan 204</i>
erasefram	erase the FRAM module
clearlog	clear data log and event log
exit	closes the connection

CONFIGURATION OF SEVERAL DEVICES

If several *NetMan 204* have to be configured with similar parameters, you can configure the first *NetMan 204*, then connect via FTP with the admin user, download all the configuration files in the folder /cfg, and upload all them via FTP in the folder /cfg of all devices to be configured.

SERVICE LOG

The screenshot shows the Netman204 web interface. At the top, there is a navigation bar with tabs for DASHBOARD, DATA, SYSTEM OVERVIEW (selected), HISTORY, CONFIGURATION, and ADMINISTRATION. The main content area is divided into several sections:

- DEVICE:** Model: VST 1500, Serial number: -, Power [kVA]: 1.5, Power [kW]: 1.2, Battery capacity [Ah]: 7, Battery voltage [Vdc]: 48, Firmware version: SWM039-01-03.
- DEVICE CONFIGURATION:** PRTK code: GPSE11201--, Name: Netman204????.
- NETWORK CARD:** Card version: e3300003 (4GB), Serial Number: 62B9CFBC, MAC Address: 00:02:63:06:3a:75, Application version: 03.11, System version: S20-1, Kernel: 4.9.78-EK20200805, Current date: 1 Oct 09:27 CEST 2020.
- SERVICE LOG:** A button labeled 'DOWNLOAD SERVICE LOG' is present.
- NETWORK CONFIGURATION:** Hostname: netman63063a75, IPv4 Address: 10.1.10.230, Gateway: 10.1.1.1, DHCP enabled: yes, Netmask: 255.255.0.0, Primary DNS: 10.1.5.10, IPv6 Address: fe80::202:63ff:fe06:3a75, Secondary DNS: 10.3.5.3.

At the bottom of the page, there are two buttons: 'READ MANUAL' and 'LEGAL INFORMATION'.

In case of problem or If *Netman 204* 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”
2. Click on “System overview”
3. Click “Download service log”

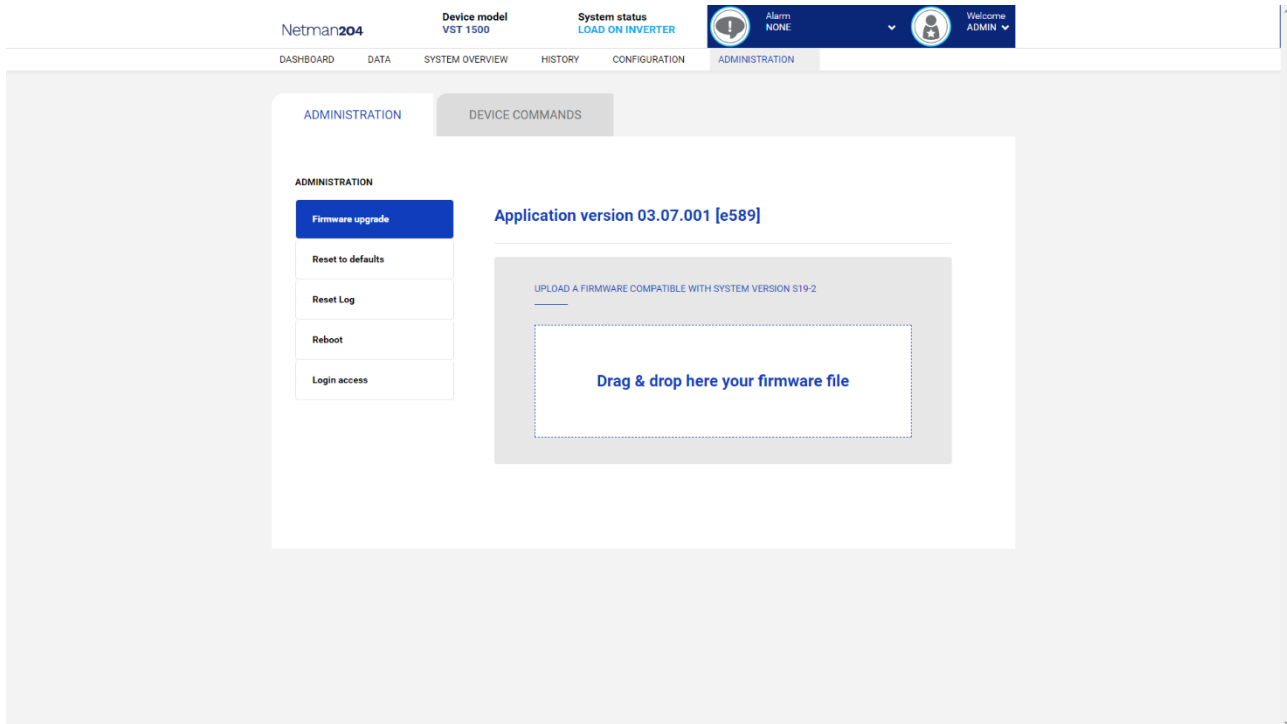
The service log will be downloaded in a few seconds. It must be sent to your local authorized service center to properly diagnose the problem.

FIRMWARE UPGRADE

The *Netman 204* firmware can be updated via HTTP or via FTP.

A valid upgrade file is named fwapp.204. If you downloaded a .zip file, you need to extract a fwapp.204 from the folder that matches the operating system of the *Netman 204*.

FIRMWARE UPGRADE VIA HTTP



Connect via HTTP to the *Netman 204* to be upgraded inserting in your web browser the hostname or IP address and then log in as admin (default password: “admin”). Then click on the “Administration” page.

Drag and drop the upgrade file. When the upgrade file is uploaded, the *Netman 204* will reboot automatically.

FIRMWARE UPGRADE VIA FTP

Connect via FTP with the user “fwupgrade” (default password “fwupgrade”) and copy the updated firmware on the /fwupgrade folder. Then restart the card by pressing the reset button.

SNMP CONFIGURATION

For configuring SNMP, is possible to use the wizard web page for a simple configuration. Advanced configuration requires to edit `snmp.conf`. This file can be downloaded and uploaded from the web page or via FTP with user "admin" (default password: "admin").

Each line of the file is parsed by *NetMan 204* and 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 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)

`<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 user name (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 minutes 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.

MODBUS TCP/IP PROTOCOL

This service is active on the TCP port 502. The supported function are listed below, together with the accessible registers.

SUPPORTED FUNCTION

SUPPORTED FUNCTION	FUNCTION DESCRIPTION	ACCESSIBLE DATA AREA
1 (0x01)	BIT READING	STATES
2 (0x02)		STATES
3 (0x03)	REGISTERS READING	ALL
4 (0x04)		ALL
6 (0x06)	SINGLE REGISTER WRITING	COMMANDS
16 (0x10)	MULTIPLE REGISTER WRITING	COMMANDS

UPS: TABLES OF STATES, MEASUREMENTS, NOMINAL DATA AND COMMANDS

REGISTER ⁽¹⁾		UPS - STATES	BIT ⁽²⁾	
NUMBER	ADDRESS		NUMBER	ADDRESS
1	0		1	0
		Test in progress [0=No / 1=YES]	2	1
			3	2
		Shutdown active [0=No / 1= YES]	4	3
			5	4
		Battery charged [0=No / 1= YES]	6	5
		Battery charging [0=No / 1= YES]	7	6
		Bypass bad [0=No / 1= YES]	8	7
			9	8
		Normal operation [0=No / 1= YES]	10	9
			11	10
		On bypass [0=No / 1= YES]	12	11
		Battery low [0=No / 1= YES]	13	12
		Battery working [0=No / 1= YES]	14	13
		UPS locked [0=No / 1= YES]	15	14
		Output powered [0=No / 1= YES]	16	15
		17÷28	16÷27	
2	1	Input Mains present [0=No / 1= YES]	29	28
		Alarm temperature [0=No / 1= YES]	30	29
		Alarm overload [0=No / 1= YES]	31	30
		UPS failure [0=No / 1= YES]	32	31
3	2		33÷48	32÷47
4	3		49÷63	48÷62
		Communication lost with UPS [0=No / 1= YES]	64	63
5÷8	4÷7		65÷128	64÷127

(1) The register number *n* must be addressed *n-1* in the data packet

(2) The bit number *n* must be addressed *n-1* in the data packet.

REGISTER ⁽¹⁾		UPS - MEASUREMENTS	UNIT
NUMBER	ADDRESS		
9÷11	8÷10		
12	11	Input mains star voltage V1	V
13	12	Input mains star voltage V2	V
14	13	Input mains star voltage V3	V
15	14	Input current phase L1	0.1*A
16	15	Input current phase L2	0.1*A
17	16	Input current phase L3	0.1*A
18	17	Input frequency	0.1*Hz
19÷21	18÷20		
22	21	Bypass mains star voltage V1	V
23	22	Bypass mains star voltage V2	V
24	23	Bypass mains star voltage V3	V
25	24	Bypass frequency	0.1*Hz
26	25	Output star voltage V1	V
27	26	Output star voltage V2	V
28	27	Output star voltage V3	V
29÷31	28÷30		
32	31	Output current phase L1	0.1*A
33	32	Output current phase L2	0.1*A
34	33	Output current phase L3	0.1*A
35	34	Output peak current phase L1	0.1*A
36	35	Output peak current phase L2	0.1*A
37	36	Output peak current phase L3	0.1*A
38	37	Load phase L1	%
39	38	Load phase L2	%
40	39	Load phase L3	%
41	40	Output active power phase L1	0.1 kW
42	41	Output active power phase L2	0.1 kW
43	42	Output active power phase L3	0.1 kW
44	43	Output frequency	0.1*Hz
45÷47	44÷46		
48	47	Battery voltage	0.1*V
49	48	Positive battery voltage	0.1*V
50	49	Negative battery voltage	0.1*V
51	50	Battery current	0.1*A
52	51	Remaining Battery Capacity	%
53	52		
54	53	Remaining back-up time	Minutes
55÷58	54÷57		
59	58	Total output energy (32 bit)	Least Significant Register
60	59		Most Significant Register
61	60		
62	61	Internal UPS temperature	°C
63	62	Sensor 1 temperature	°C
64	63	Sensor 2 temperature	°C
65÷72	64÷71		

⁽¹⁾ The register number *n* must be addressed *n-1* in the data packet.



Some measures may not be available for all the UPS. In this case, the relative register remains at 0xFFFF value.

REGISTER ⁽¹⁾		UPS – NOMINAL DATA	UNIT
NUMBER	ADDRESS		
73÷77	72÷76		
78	77	Output nominal voltage (star)	V
79	78	Output nominal frequency	0.1*Hz
80	79	Output nominal power	100*VA
81÷83	80÷82		
84	83	Battery nominal capacity (battery expansion included)	Ah
85	84	Battery benches	(1 or 2)
86	85	Battery type	Integer
87÷112	86÷111		

REGISTER ⁽¹⁾		UPS - COMMANDS	UNIT
NUMBER	ADDRESS		
113	112	Command code ⁽²⁾	Integer
114	113	Shutdown delay time	Seconds
115	114	Restore delay time	Minutes
116	115		
117	116	Command result ⁽³⁾	Integer
118	117		

REGISTER ⁽¹⁾		DIAGNOSTIC	UNIT
NUMBER	ADDRESS		
119	118	Counter of processed correct messages	Integer
120	119	Counter of processed NOT correct messages	Integer

⁽¹⁾ The register number **n** must be addressed **n-1** in the data packet.

⁽²⁾ Refer to “Command codes” paragraph

⁽³⁾ Command result = Command code if command is handled from the UPS

Command result = Command code + 100 if command is NOT handled from the UPS

Command result = 0 if Command code is wrong

REGISTER ⁽¹⁾		SPECIAL FLAGS (SENTR UPS)	UNIT
NUMBER	ADDRESS		
121	120	Byte 1 of "s = xx.." code / Byte 2 of "s = ..xx" code	Flag
122	121	Byte 1 of "c = xx.." code / Byte 2 of "c = ..xx" code	Flag
123	122	Byte 1 of "b = xx.." code / Byte 2 of "b = ..xx" code	Flag
124	123	Byte 1 of "r = xx-.." code / Byte 2 of "r = ..xx-.." code	Flag
125	124	Byte 3 of "r =-xx" code / Byte 1 of "i = xx-.." code	Flag
126	125	Byte 2 of "i = ..xx-.." code / Byte 3 of "i =-xx" code	Flag
127	126	Byte 1 of "a = xx-...." code / Byte 2 of "a = ..xx-...." code	Flag
128	127	Byte 3 of "a =-xx.." code / Byte 4 of "a =-..xx" code	Flag

REGISTER ⁽¹⁾		NETMAN DATA	UNIT
NUMBER	ADDRESS		
129	128	Firmware version	Integer
130÷131	129÷130		

⁽¹⁾ The register number **n** must be addressed **n-1** in the data packet.

⁽²⁾ In order to decode these registers, please refer to the UPS manual.

UPS: COMMANDS CODES

CODE	COMMAND
1 (0x0001)	Command Shutdown
2 (0x0002)	Command Shutdown and Restore
3 (0x0003)	Delete Command (code 1, 2, 12)
12 (0x000C)	UPS on Bypass
20 (0x0014)	Test Battery
22 (0x0016)	Test Panel

Please refer to the Modbus table document for additional information about registers for other devices.

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
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
Analog Input 33	System status group 1	
Analog Input 34	System status group 2	

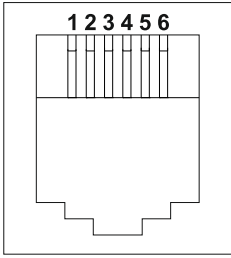
Analog Input 35	System status group 3	
Analog Input 36	Bypass module alarms	
Analog Input 37	Power module 1 alarms	
Analog Input 38	Power module 2 alarms	
Analog Input 39	Power module 3 alarms	
Analog Input 40	Power module 4 alarms	
Analog Input 41	Power module 5 alarms	
Analog Input 42	Power module 6 alarms	
Analog Input 43	Power module 7 alarms	
Analog Input 44	Bypass module status	
Analog Input 45	Power module 1 status	
Analog Input 46	Power module 2 status	
Analog Input 47	Power module 3 status	
Analog Input 48	Power module 4 status	
Analog Input 49	Power module 5 status	
Analog Input 50	Power module 6 status	
Analog Input 51	Power module 7 status	

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	Temperature 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	Temperature 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	Temperature 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	Temperature 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	Temperature 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	Temperature high sensor 6
TMIN6	Temperature low sensor 6
Input6	Input contact sensor 6
Hum6	Humidity high sensor 6
Hum low6	Humidity low sensor 6

SERIAL PORT CONFIGURATION

RJ-12 – SERIAL port	
	
POSITION	DESCRIPTION
1	+5V _{DC}
2	GND
3	Environmental sensors bus
4	GND
5	RXD
6	TXD

NetMan 204		LEAVE UNCONNECTED	Modem		
RJ-12			DB-25	DB-9	DESCRIPTION
POSITION	DESCRIPTION		POSITION	POSITION	
1	+5V _{DC}				
2	GND				
3	Environmental sensors bus				
4	GND	← CONNECT TO →	7	5	GND
5	RXD	← CONNECT TO →	3	2	TXD
6	TXD	← CONNECT TO →	2	3	RXD

TECHNICAL DATA

NETWORK CABLE

To connect the device to the Ethernet (10Base-T) or Fast Ethernet (100Base-T) network, a UTP (Unshielded Twisted Pair) or STP (Shielded Twisted Pair) cable with RJ45 connectors is required. The cable must conform to the standard IEEE 802.3u 100Base-T with 2 pairs of UTP cables 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.

NETWORK CABLE CONNECTIONS	
Signal	Pin # to Pin #
TX+	1 ← → 1
TX-	2 ← → 2
RX+	3 ← → 3
RX-	6 ← → 6



Pins 1 and 2 must be connected to one twisted pair, pins 3 and 6 to another.

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 204* includes some open source components. For more information please visit the website of the manufacturer.