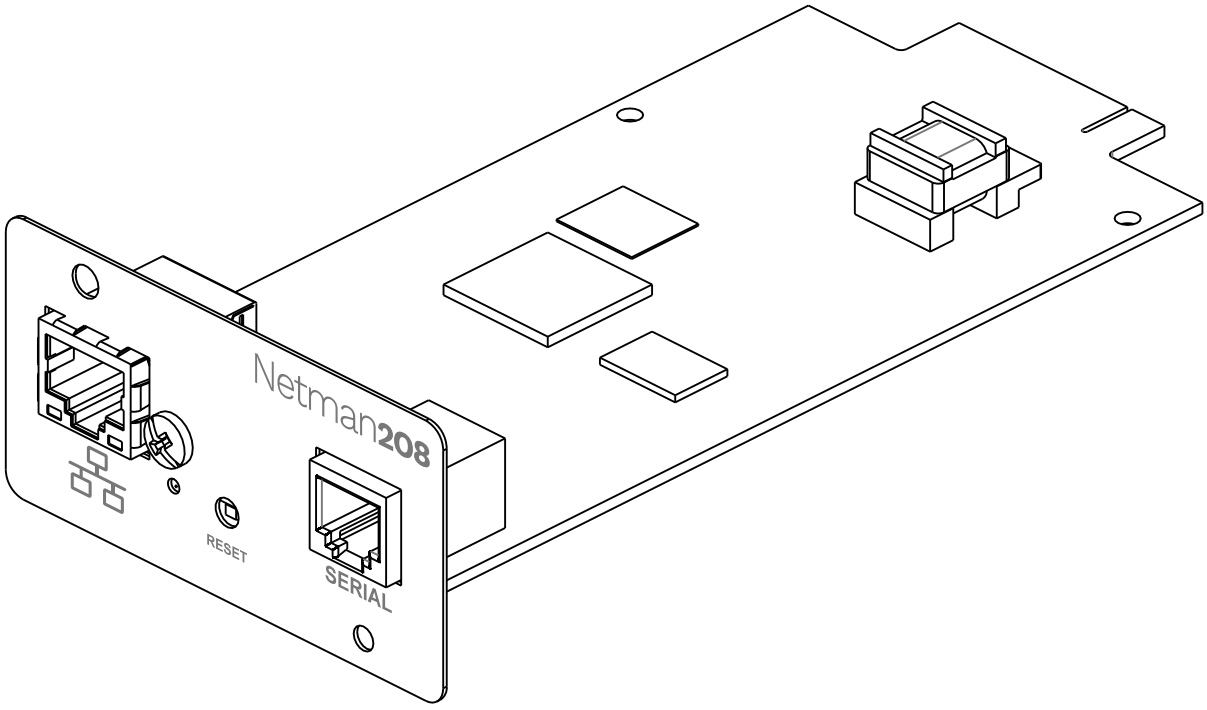
Netman208



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 <u>CONSULTED BEFORE USING THE DEVICE</u> 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.

CONTENTS

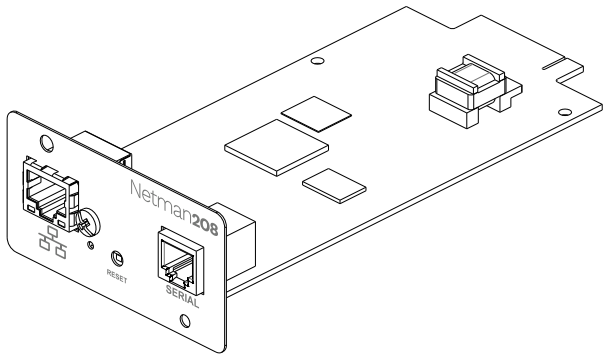
DESCRIPTION

OVERVIEW

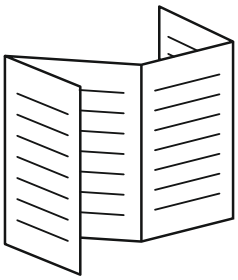
Netman 208 is an accessory that allows device management through a LAN (Local Area Network); the accessory supports all the main network protocols (SNMP v1, v2 and v3, TCP/IP, HTTP and MODBUS) and is compatible with Ethernet 10/100/1000 Mbps IPv4/6 networks. The device can therefore be integrated easily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

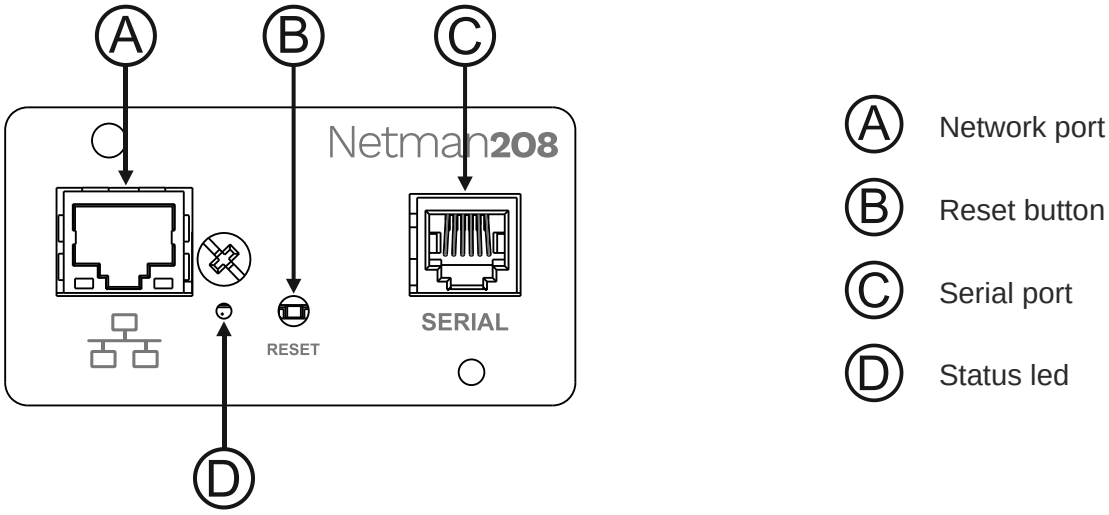
Netman 208



Quick start



FRONT PANEL



Network port

Netman 208 connects to 10/100/1000 Mbps Ethernet networks by means of connector RJ45. The LEDs built into the connector describe the status of the network:

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

Reset button

The reset button enables the user to execute a *system reboot* or enter the *recovery mode*.

- **System reboot**: keep the reset button pressed until the status led starts blinking and then release it.
- **Recovery mode:** keep the reset button pressed; first the status led starts blinking, then turns to solid green (approx. 5 seconds). When the led is solid green, release the reset button.

Serial port

Netman 208 makes available a RS232/RS485 serial communication port (for more details, see paragraph *"Technical data"*).

Status led

This led describes the status of *Netman 208*:

Led color	Description
SOLID GREEN	Normal operation
FAST BLINKING GREEN	Reset button pressed or Recovery mode running
SLOW BLINKING GREEN	Update mode running
FAST BLINKING RED	Network communication error
SOLID RED	UPS communication error or wrong PRTK code configured

USERS

It is possible to access to *Netman 208* with two different users:

Username	Default password	Privileges
admin	admin	user with right to modify the configuration (1)
power	No pre-set password (2)	user with right to modify the configuration (2)

(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 208 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 208* 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 208 can send “Wake-on-LAN” command for remote computers boot.

HTTP

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

SNMP

SNMP (Simple Network Management Protocol) is a communication protocol that allows a client (manager) to make requests to a server (agent). *Netman 208* 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 208* 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;

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

- Host: hostname or *Netman 208* 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 208*.

Syslog

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

Email

Netman 208 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 208 can send periodic e-mails with an attachment containing the files of the device values and events history log archive.
This service can be used to periodically save the history log archives.
The “Email” service must be enabled in order to send reports; the reports are sent to all the addresses configured for this service (for more details see paragraph “Configuration”).

SSH Client

When not feasible to operate on equipment by other means, 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 208 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:

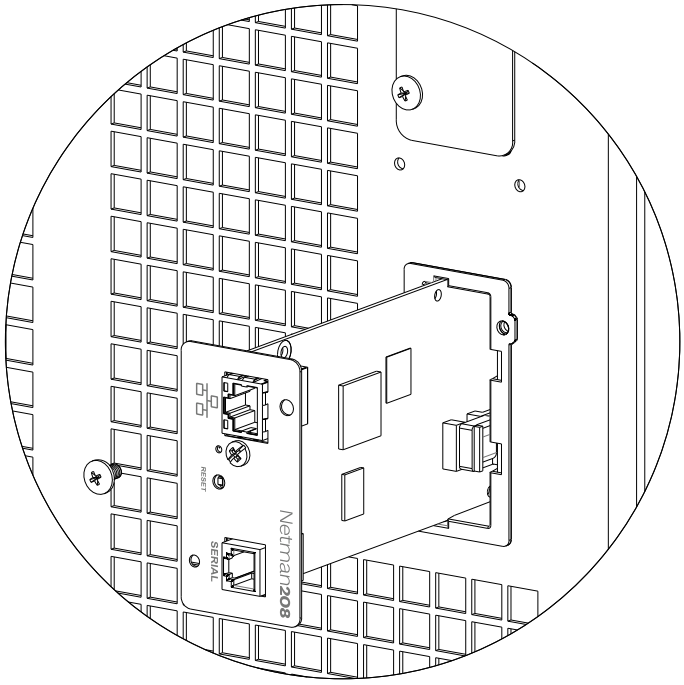
- A red dot if the event is the start of an alarm condition.
- A green dot if the event is the end of an alarm condition.
- A blue dot otherwise.

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.

INSTALLATION

1. Remove the cover of the COMMUNICATION SLOT by unscrewing the two retaining screws.
2. Carefully insert the *Netman 208* into the COMMUNICATION SLOT.
3. Secure the *Netman 208* in the COMMUNICATION SLOT using the two previously removed screws.
4. Connect the device to the network by means of an RJ-45 connection cable.



CONFIGURATION

Netman 208 can be configured via HTTP using the web browser interface.

Netman 208 is provided by default with the DHCP enabled.

Netman 208 requires approximately 2 minutes to become fully operational from when it is powered up or following a reboot; before this time the device may not respond to commands that are sent to it.

To configure the *Netman 208*, enter the IP address or the hostname into your web browser and then log in with the following username and default password:
Username: admin
Password: admin

At the first boot or if you don't know the IP address, you can use the Zero Configuration Networking (Zeroconf) as described below.
On the bottom side of the card, you can find the label reporting the mac address of your *Netman 208*.

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

00	02	63	XX	YY	ZZ
		63			

In the address bar of a web browser, enter:

http://netman63XXYYZZ.local

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

For example, if the mac address of your *Netman 208* is 00:02:63:08:03:1f, you must enter http://netman6308031f.local in the address bar of the web browser.

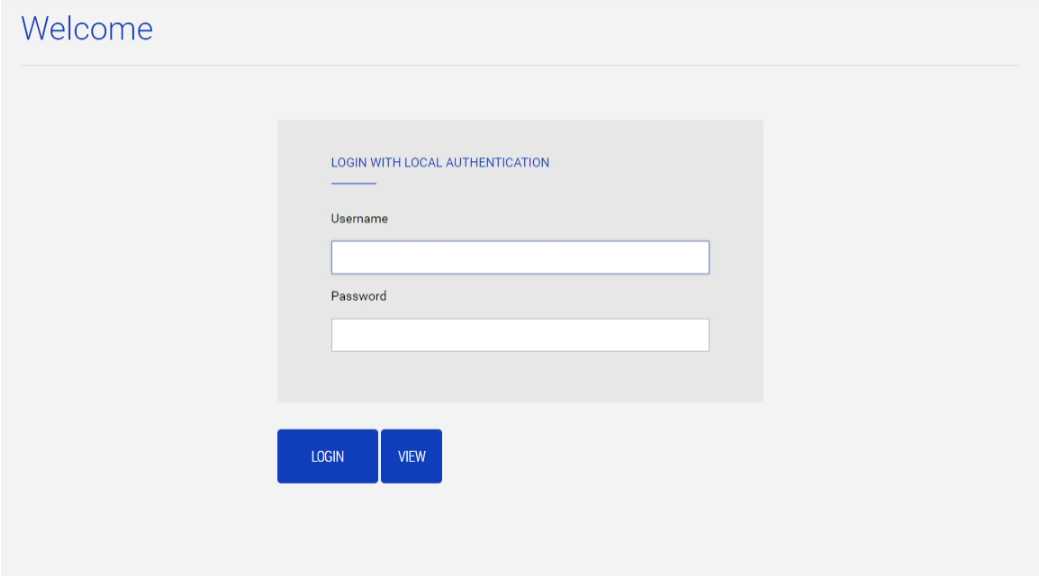
Then log in with the following username and default password:
Username: admin
Password: admin

For security reasons, we suggest the user changes the default password "admin" with a secure password.

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

LOGIN

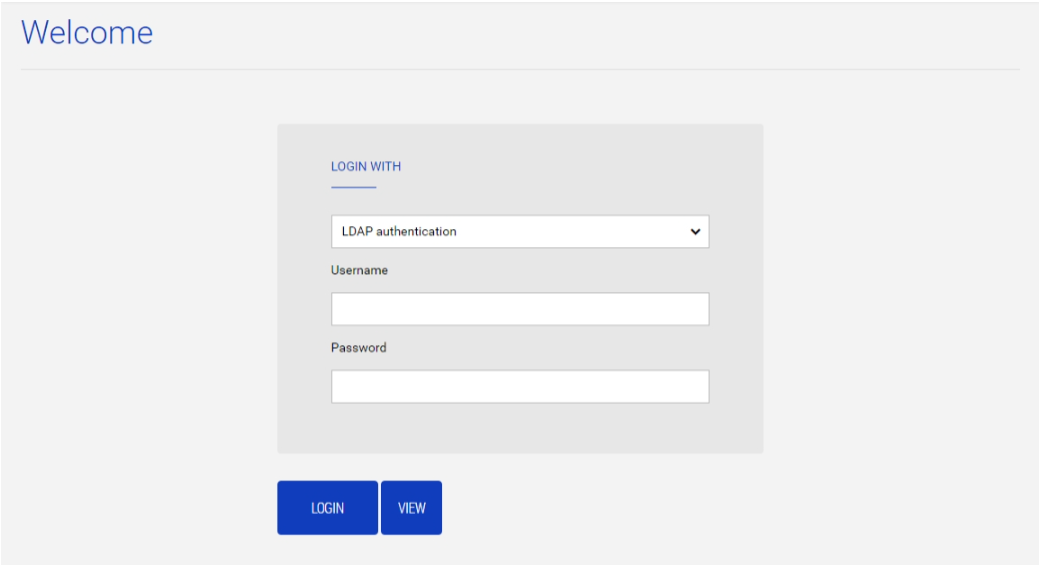
All the settings are available on the web configuration when logged is as “admin” or “power” user. It is not possible to have multiple concurrent sessions.



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

- 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
- Pressing the VIEW button, without inserting username and password, allows to view the status of the device; no other action is permitted.

It is possible to login with local authentication (managed by *Netman 208*) or centrally with LDAP or AD (more information at paragraph “Login access configuration”).



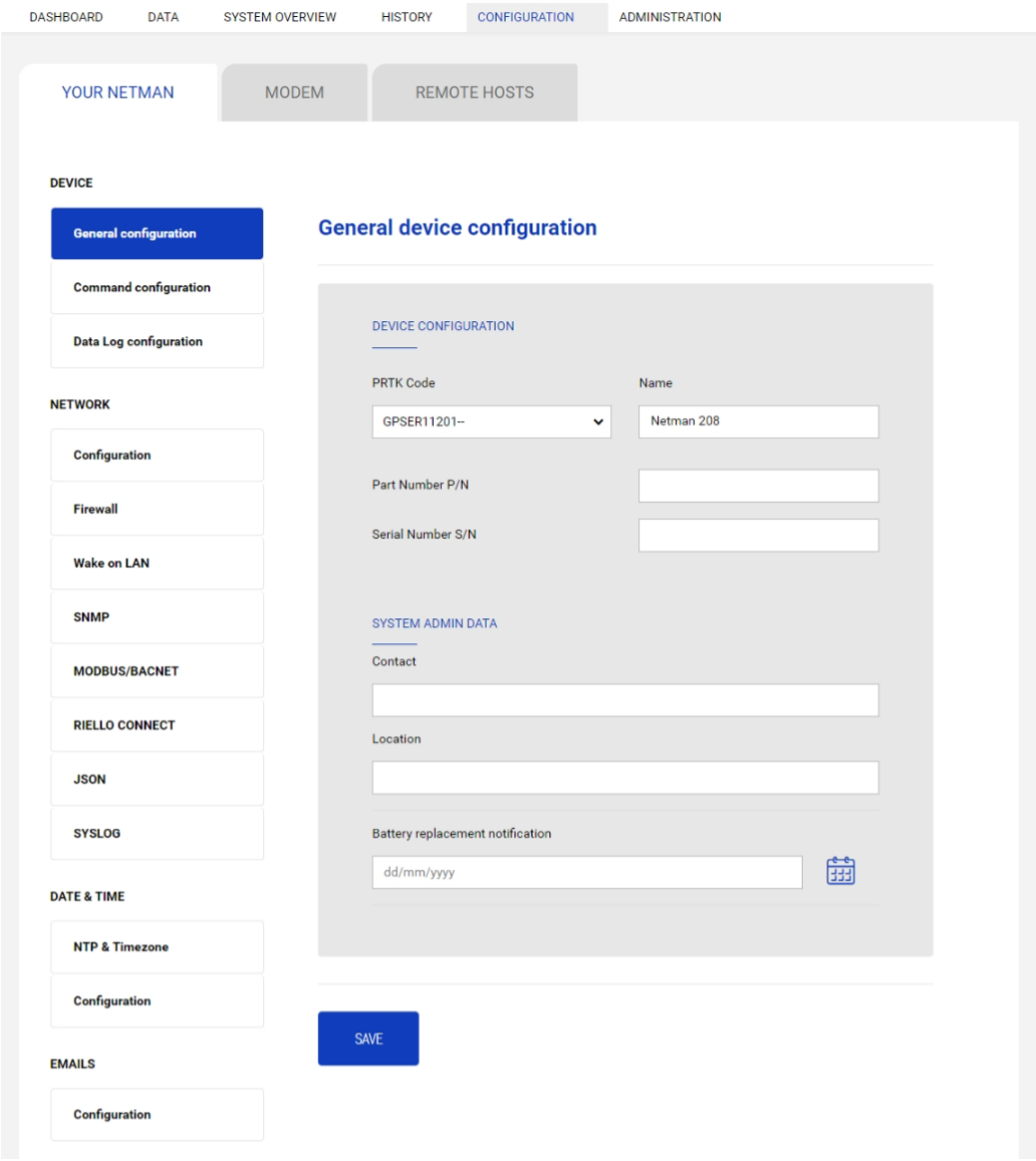
DASHBOARD

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.

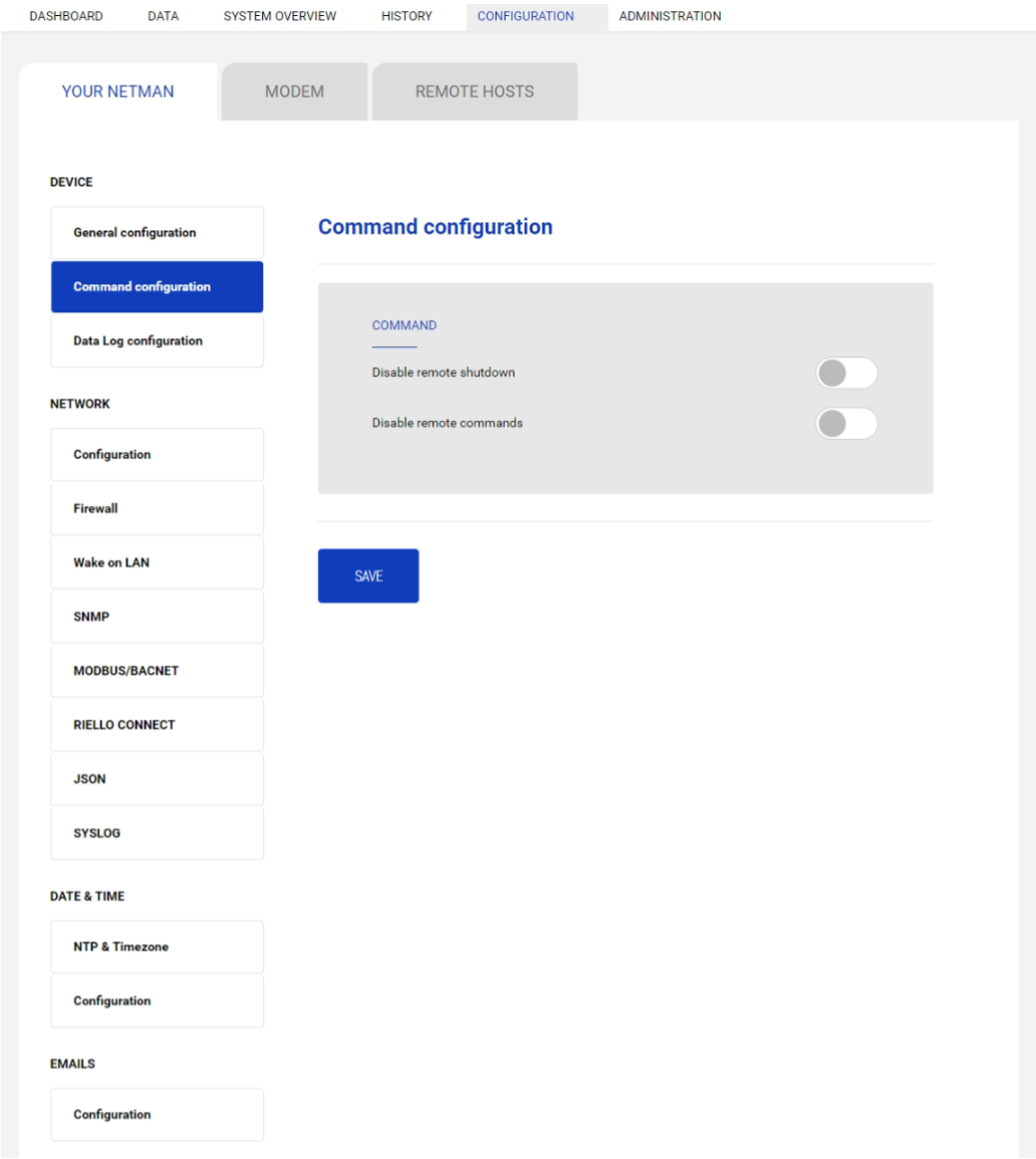
DEVICE

General configuration



Field	Description
PRTK Code	Enter the PRTK code indicated at the back of the device.
Name	Enter the identifying name of the device.
Part Number P/N	If empty, you must insert the value present in the device technical label.
Serial Number S/N	If empty, you must insert the value present in the device technical label.
Contact	Informational
Location	Informational
Battery replacement notification	To generate an alarm at the end of the set period.

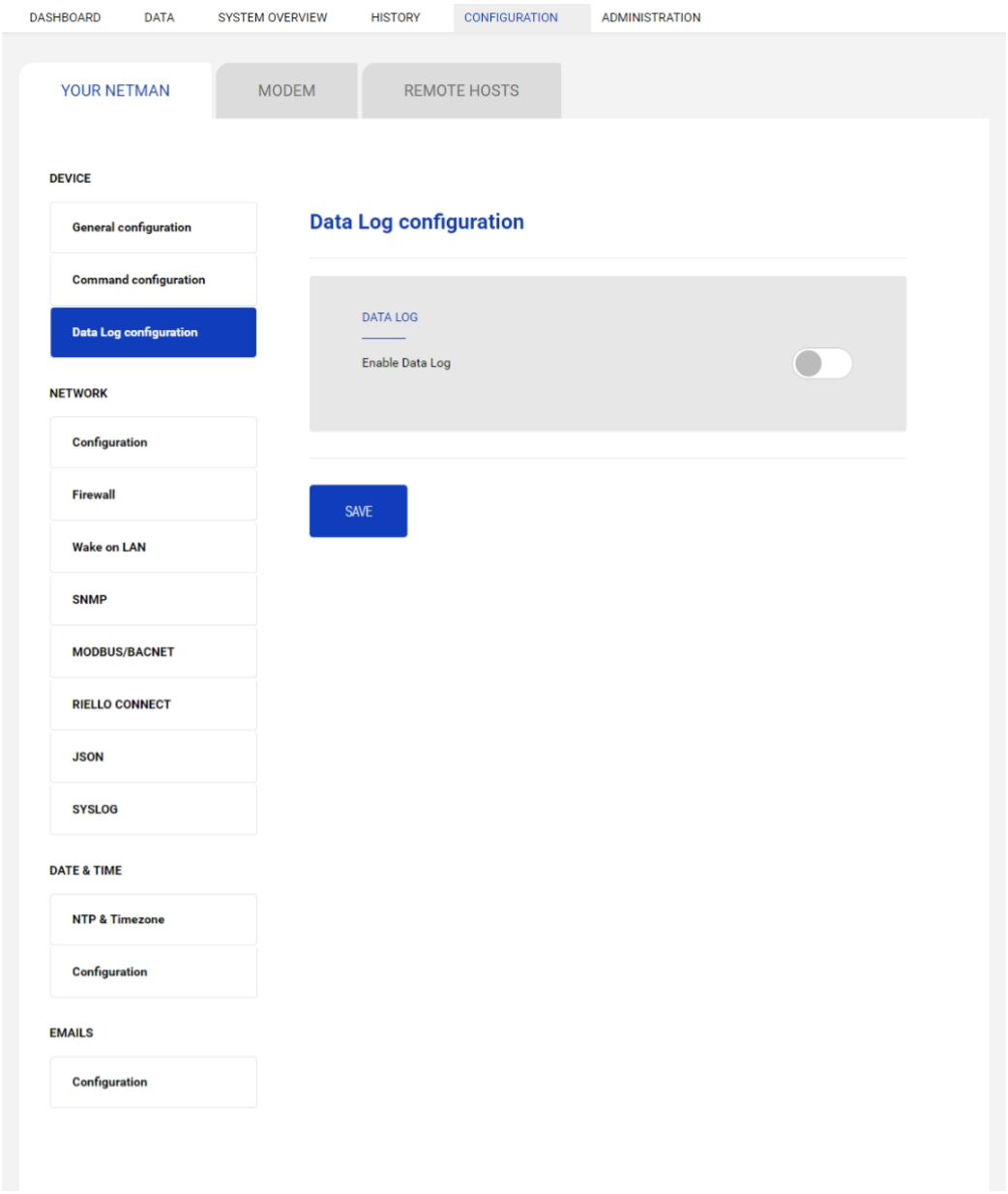
Command configuration



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

Field	Description
Disable remote shutdown	To disable the execution of shutdown commands
Disable remote commands	To disables the execution of the remaining commands

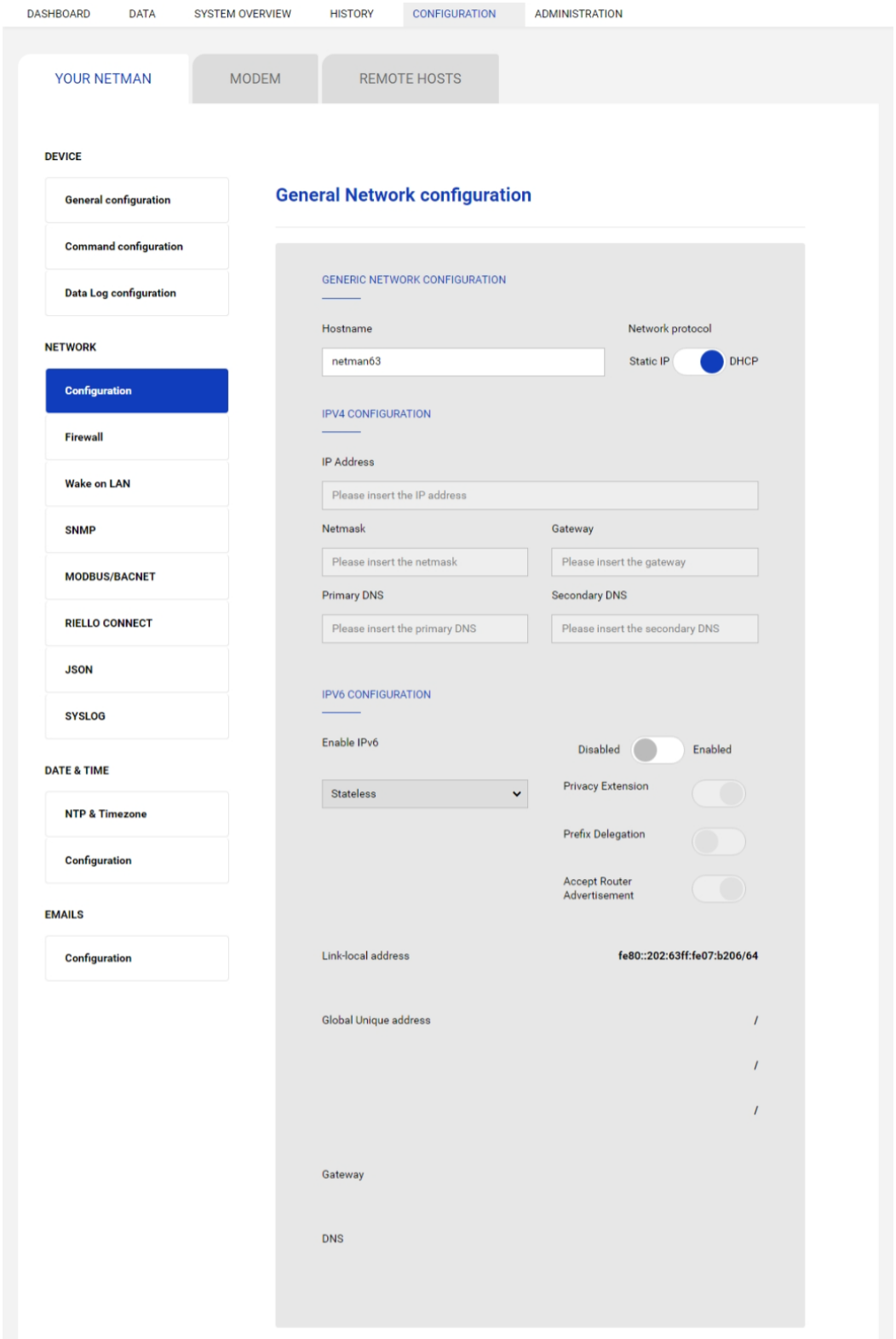
Data log configuration

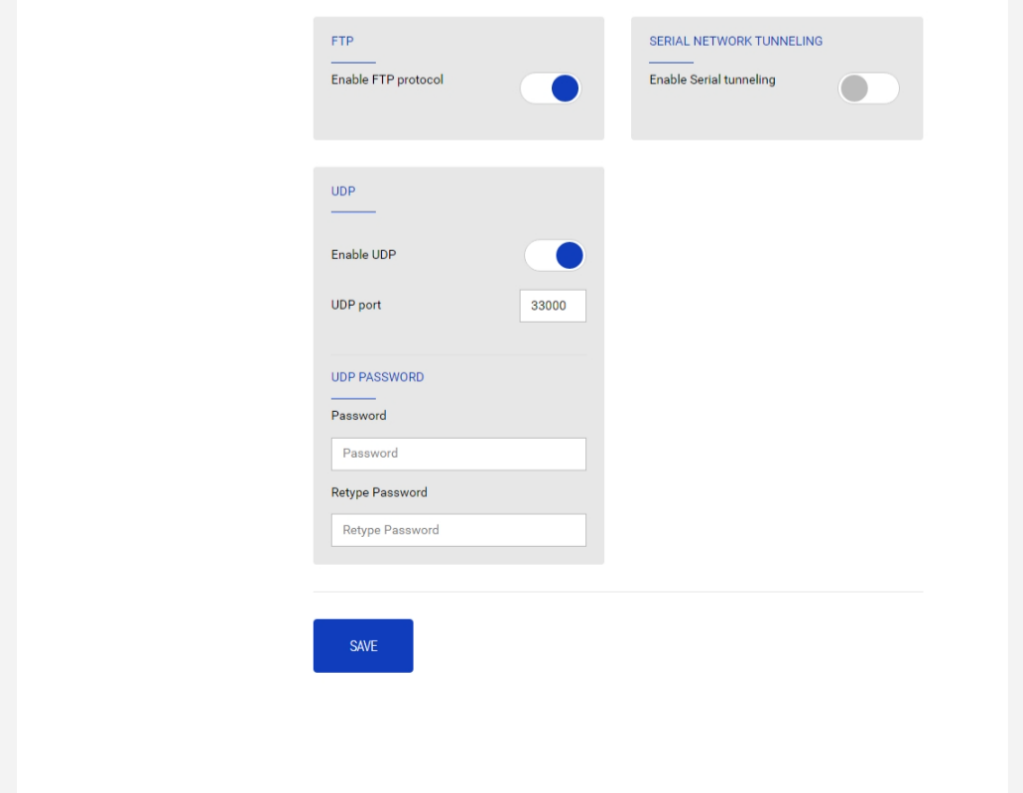


Field	Description
Enable Data log	To enables the datalog service

NETWORK

Configuration





Field	Description
Hostname	Enter the *Netman 208* 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 IPv6	Allow to enable IPv6 protocol
Method	Available method: *Stateless*
Privacy Extension	Option for requesting usage or random-generated IPv6 address instead of pre-defined address creation (related to MAC address)
Enable FTP protocol	To enable the FTP protocol
Enable Serial network tunneling	To enable the serial network tunnelling protocol
Enable UDP	To enable UDP/UPSMon service
UDP port	Enter the port where the UDP/UPSMon service is started [(1)]
UDP Password	To change the password used for UDP/UPSMon communication

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

How to access the Netman via Hostname.

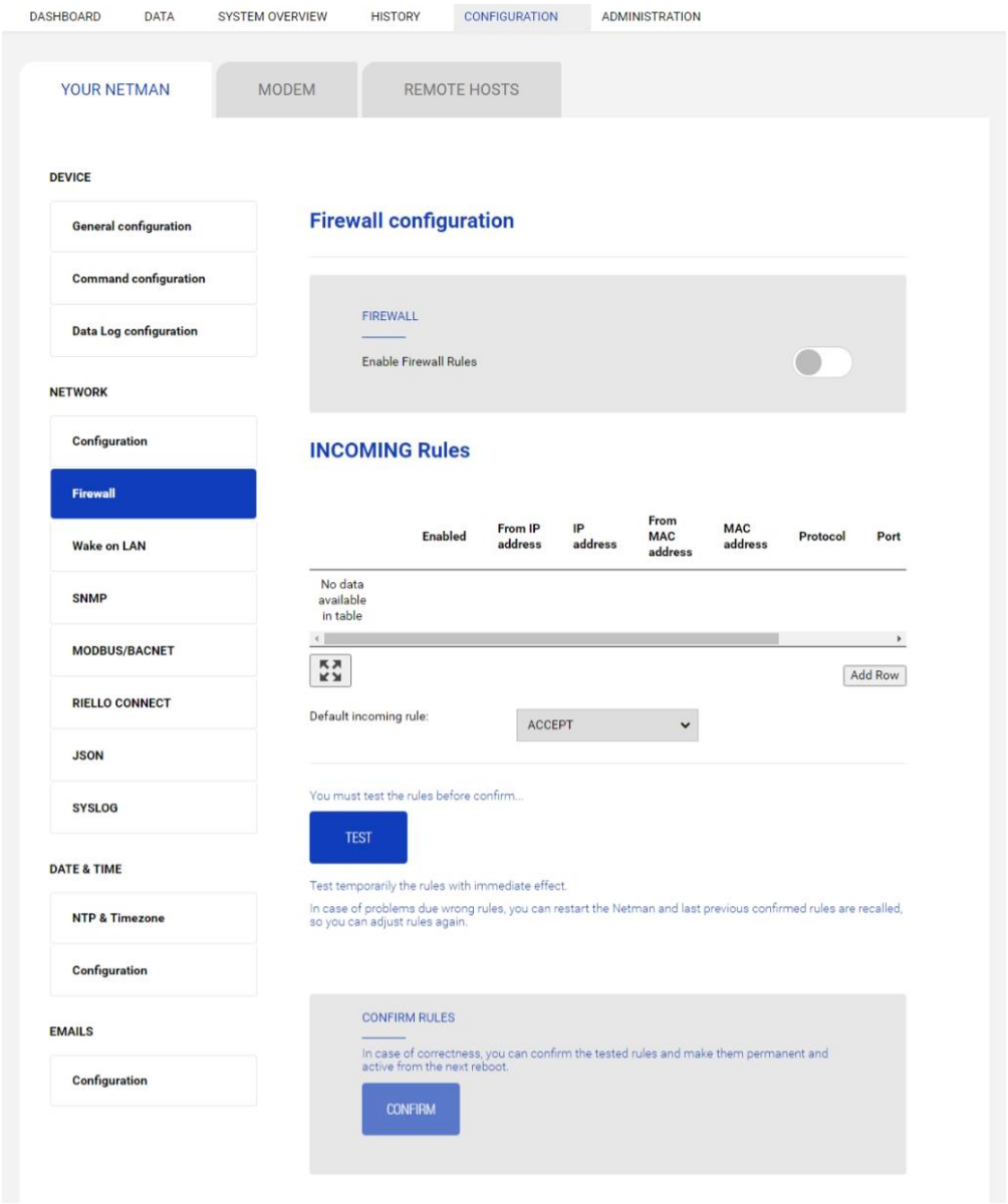
➔ By default, the Hostname is built from MAC address
*e.g., from Netman MAC Address: 00:02:**63**:**05**:**00**:**37*** ➔ ***http://netman63050037.local***

➔ If the User changes the Hostname the new hostname becomes active
*e.g., new Hostname "**servernetman**" ➔ **http://servernetman.local***

How to access the Netman via IPv6 address.

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

Firewall



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

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

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

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

and in addition, filtering the traffic incoming that requests:

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

where each rule obeys to one ACTION:

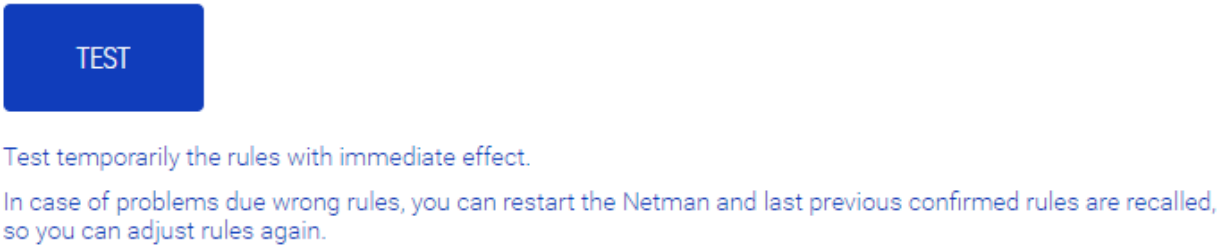
- **ACCEPT**: allows the traffic filtered by the rule
- **DROP**: lets drop the traffic request incoming due to the rule (no response is sent back to the Source of the connection)
- **REJECT**: refuses the connection (an answer of reject is sent back to the Source of the connection)

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

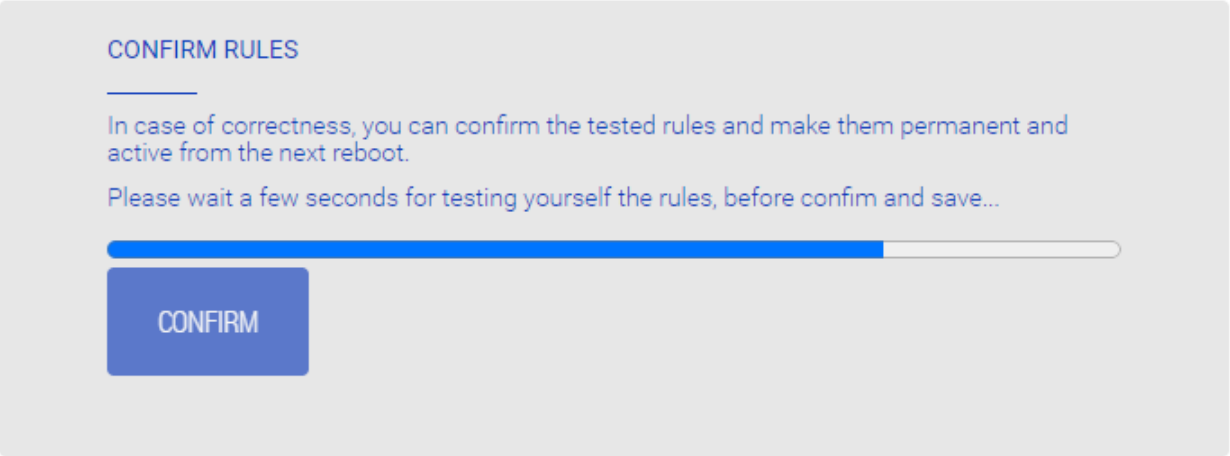
where options are:

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

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



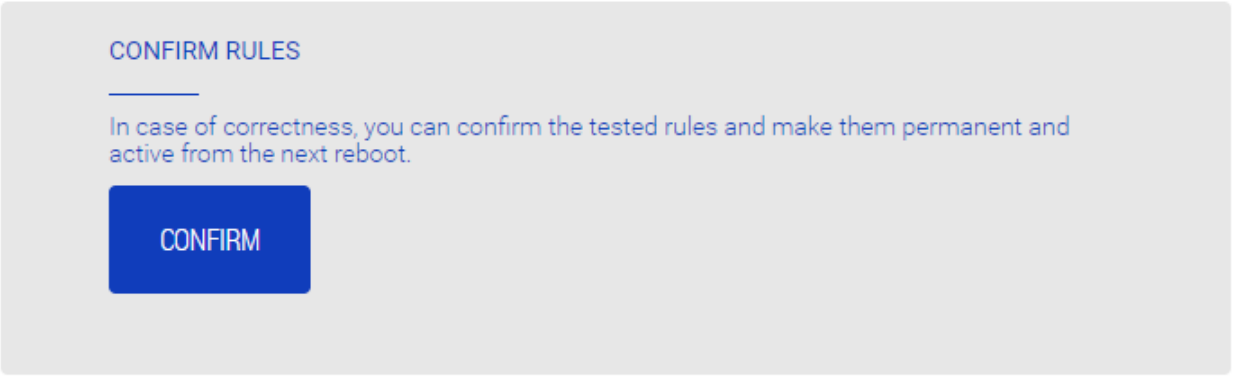
The TEST activates temporarily the rules forcing the user to wait some time before any CONFIRM action:



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

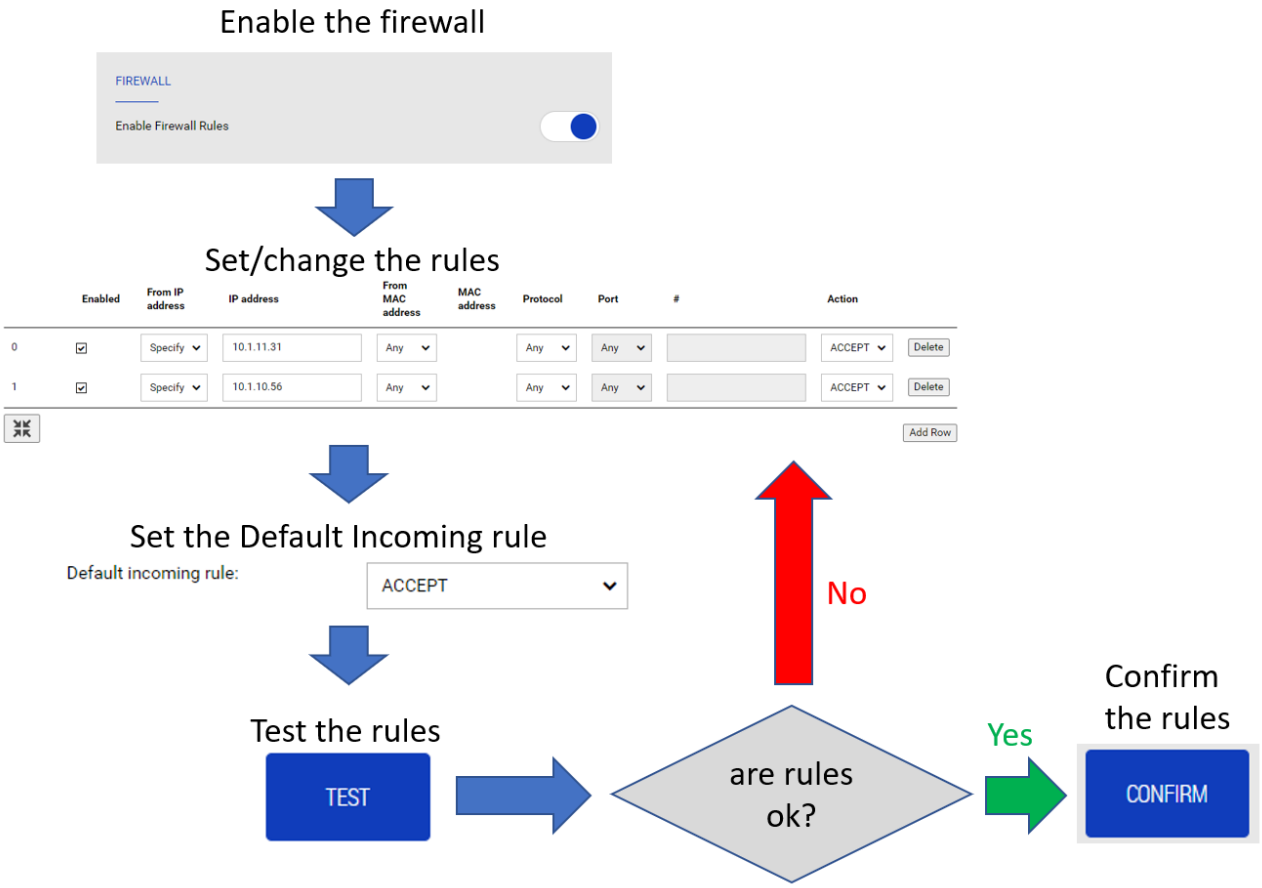
- in case of **connection lost** the User can reboot the *Netman 208* (physically un-plugging and re-plugging again in the slot) and connection is restored as it was before firewall TEST, so the User can re-check the rules and TEST again with the new rule changes

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



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

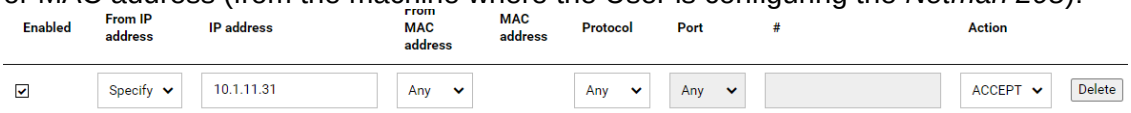
Workflow for a correct configuration



Notes and suggestions

Safe rule

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



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

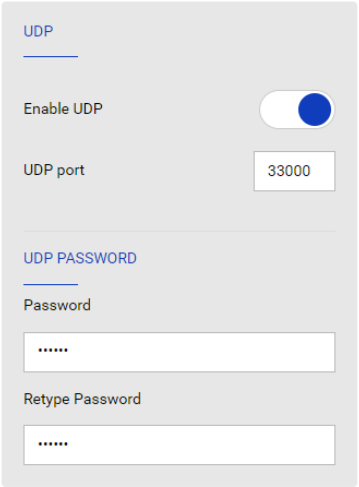
Without any "*safe rule*" the User risks to lose connection to the *Netman 208*, with unique solution of resetting to default (by physical button) losing any configuration previously applied.

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

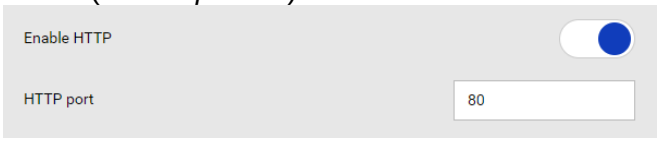
The worst condition possible is setting all the rules in the table with **DROP** and **Default Incoming Rule** as **DROP**: in this way the *Netman 208* will refuse any connection and becomes no more reachable: in this case, it must be reset to default by pressing the physical button, losing any configuration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

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

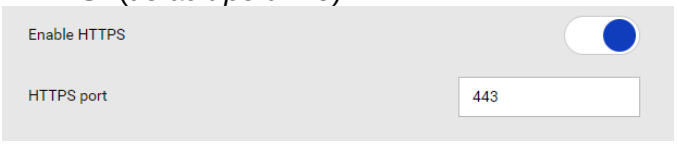
UPSMON* (*default port 33000*)



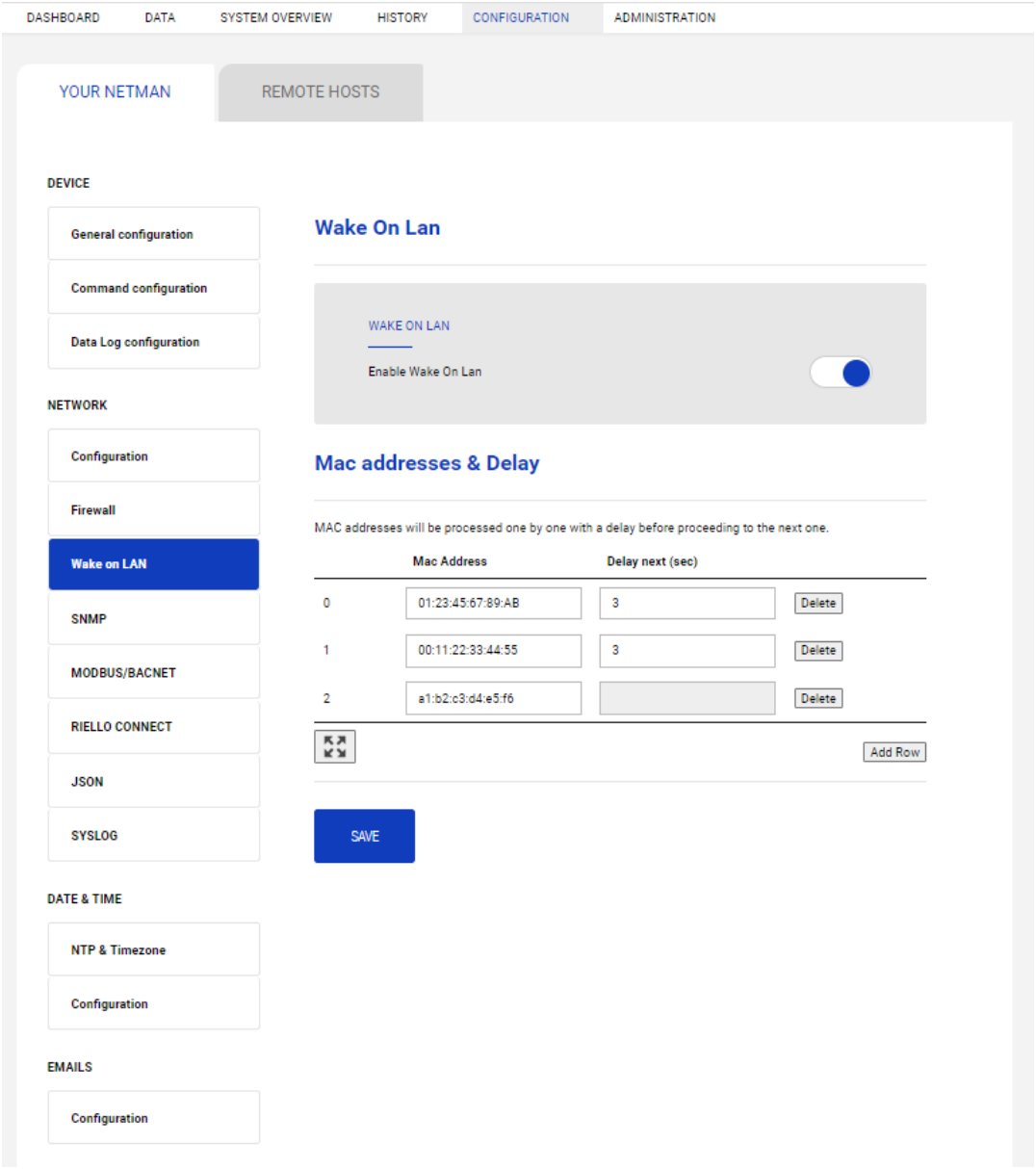
HTTP* (*default port 80*)



HTTPS* (*default port 443*)



Wake-on-LAN

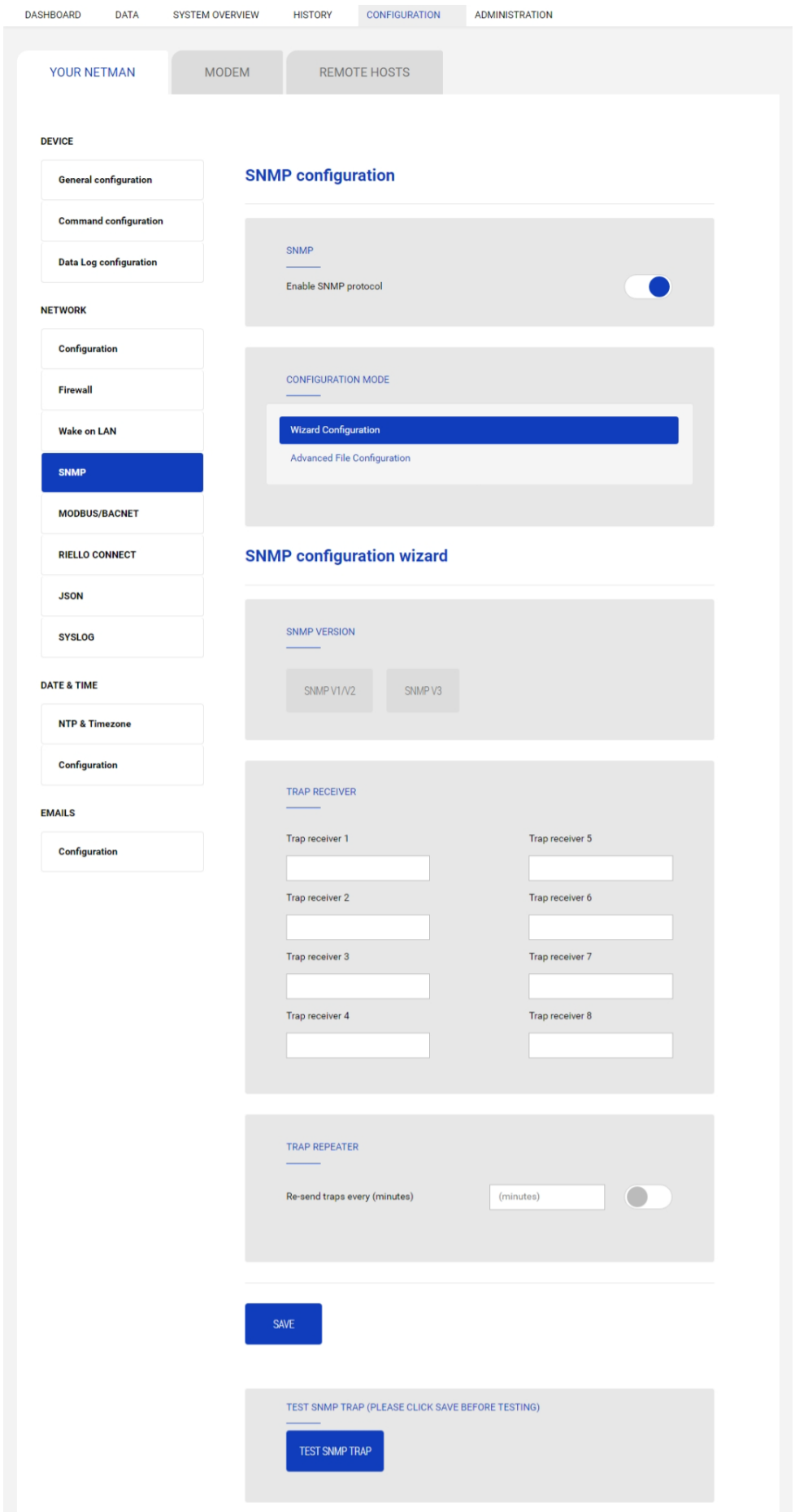


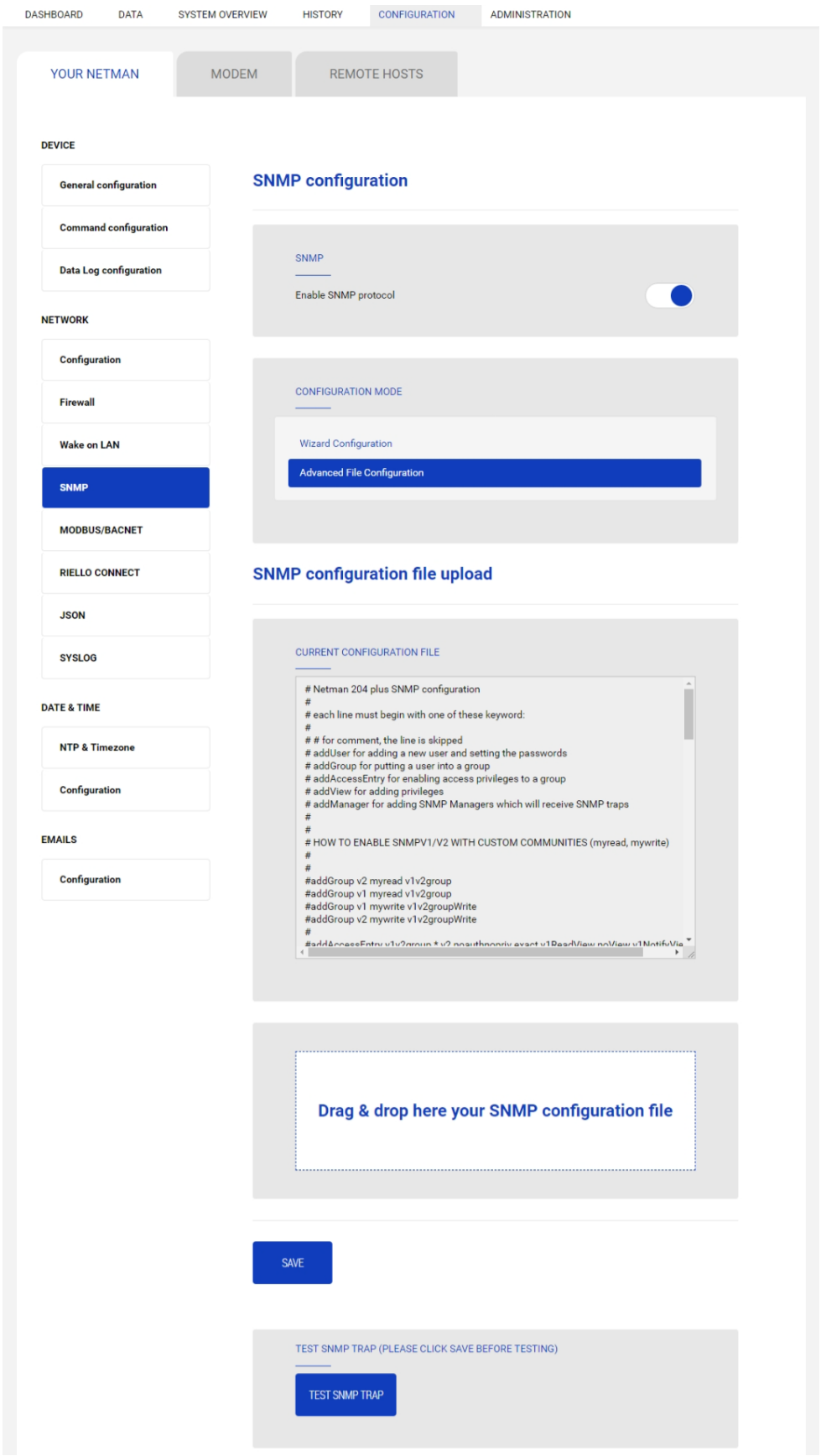
With this menu it is possible to populate a list of MAC addresses for executing Wake-on-LAN operation. Please remember to set the *Delay Next* time (in seconds) between each execution. The list order can be easily managed dragging up/down the rows by the “row number” on the left.

The Wake-on-LAN is sent at *Netman 208* boot and when the mains return from black-out.

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

SNMP


DASHBOARD
DATA
SYSTEM OVERVIEW
HISTORY
CONFIGURATION
ADMINISTRATION
YOUR NETMAN
MODEM
REMOTE HOSTS
DEVICE
General configuration
Command configuration
Data Log configuration
NETWORK
Configuration
Firewall
Wake on LAN
SNMP
MODBUS/BACNET
RIELLO CONNECT
JSON
SYSLOG
DATE & TIME
NTP & Timezone
Configuration
EMAILS
Configuration
SNMP configuration
SNMP
Enable SNMP protocol
CONFIGURATION MODE
Wizard Configuration
Advanced File Configuration
SNMP configuration wizard
SNMP VERSION
SNMP V1/V2
SNMP V3
TRAP RECEIVER
Trap receiver 1
Trap receiver 2
Trap receiver 3
Trap receiver 4
Trap receiver 5
Trap receiver 6
Trap receiver 7
Trap receiver 8
TRAP REPEATER
Re-send traps every (minutes)
(minutes)
SAVE
TEST SNMP TRAP (PLEASE CLICK SAVE BEFORE TESTING)
TEST SNMP TRAP


DASHBOARD
DATA
SYSTEM OVERVIEW
HISTORY
CONFIGURATION
ADMINISTRATION
YOUR NETMAN
MODEM
REMOTE HOSTS
DEVICE
General configuration
Command configuration
Data Log configuration
NETWORK
Configuration
Firewall
Wake on LAN
SNMP
MODBUS/BACNET
RIELLO CONNECT
JSON
SYSLOG
DATE & TIME
NTP & Timezone
Configuration
EMAILS
Configuration
SNMP configuration
SNMP
Enable SNMP protocol
CONFIGURATION MODE
Wizard Configuration
Advanced File Configuration
SNMP configuration file upload
CURRENT CONFIGURATION FILE
Netman 204 plus SNMP configuration
#
each line must begin with one of these keyword:
#
for comment, the line is skipped
addUser for adding a new user and setting the passwords
addGroup for putting a user into a group
addAccessEntry for enabling access privileges to a group
addView for adding privileges
addManager for adding SNMP Managers which will receive SNMP traps
#
#
HOW TO ENABLE SNMPV1/V2 WITH CUSTOM COMMUNITIES (myread, mywrite)
#
#
#addGroup v2 myread v1v2group
#addGroup v1 myread v1v2group
#addGroup v1 mywrite v1v2groupWrite
#addGroup v2 mywrite v1v2groupWrite
#
Drag & drop here your SNMP configuration file
SAVE
TEST SNMP TRAP (PLEASE CLICK SAVE BEFORE TESTING)
TEST SNMP TRAP

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 provides defaults that fit the needs of most use cases for SNMPv1/v2.

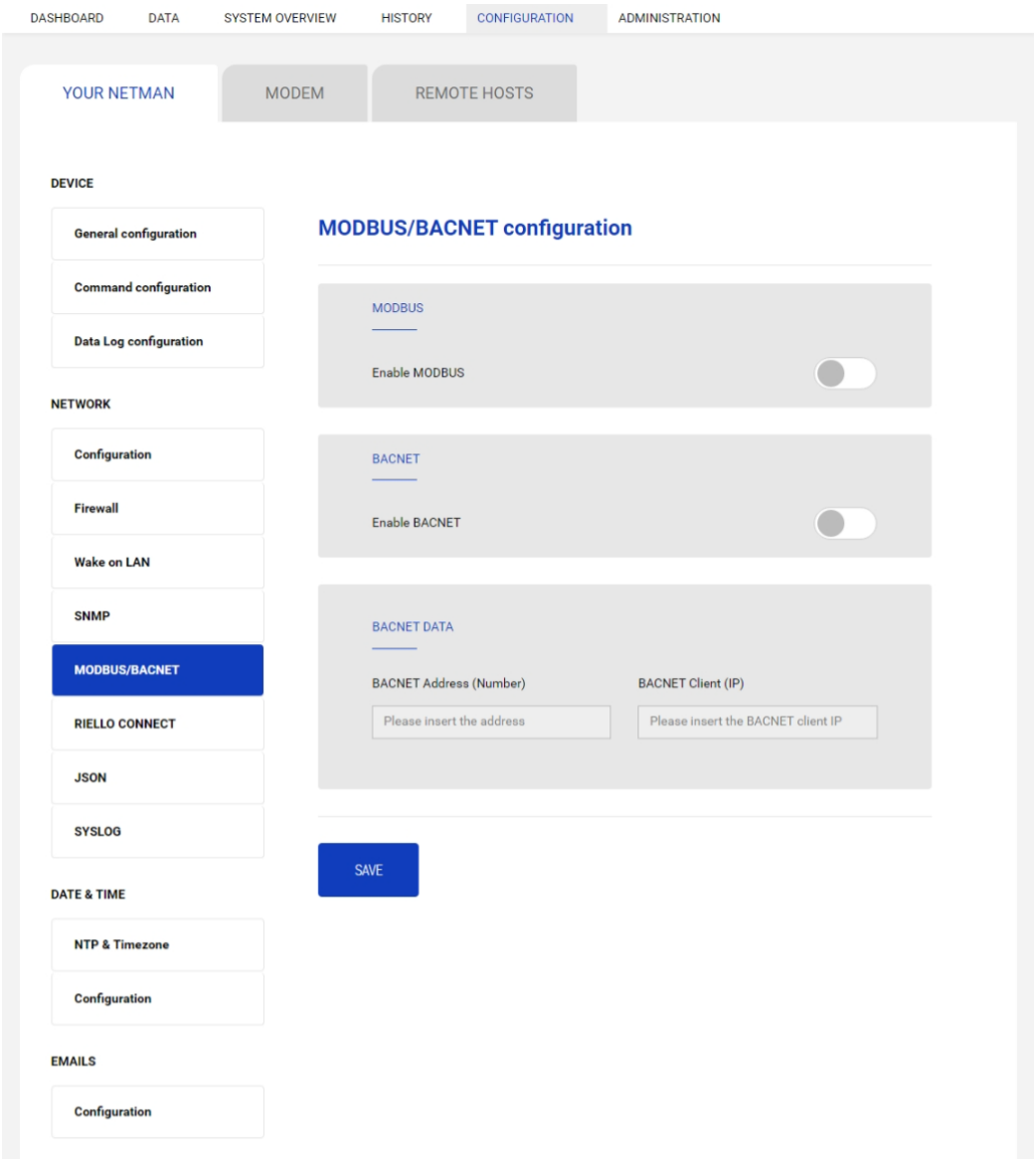
When is needed additional security by means of authentication and encryption, it is recommended to use SNMPv3 with the wizard configuration.

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

Advanced configuration requires to edit `snmp.conf` (please see chapter "*SNMP configuration*").

Field	Description
Enable SNMP protocol	To enable the SNMP service
Configuration mode	Choose between *wizard configuration* or to upload a *configuration file*
SNMP version	Choose between *SNMPv3* (strongly suggested) and *SNMPv1/v2*
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

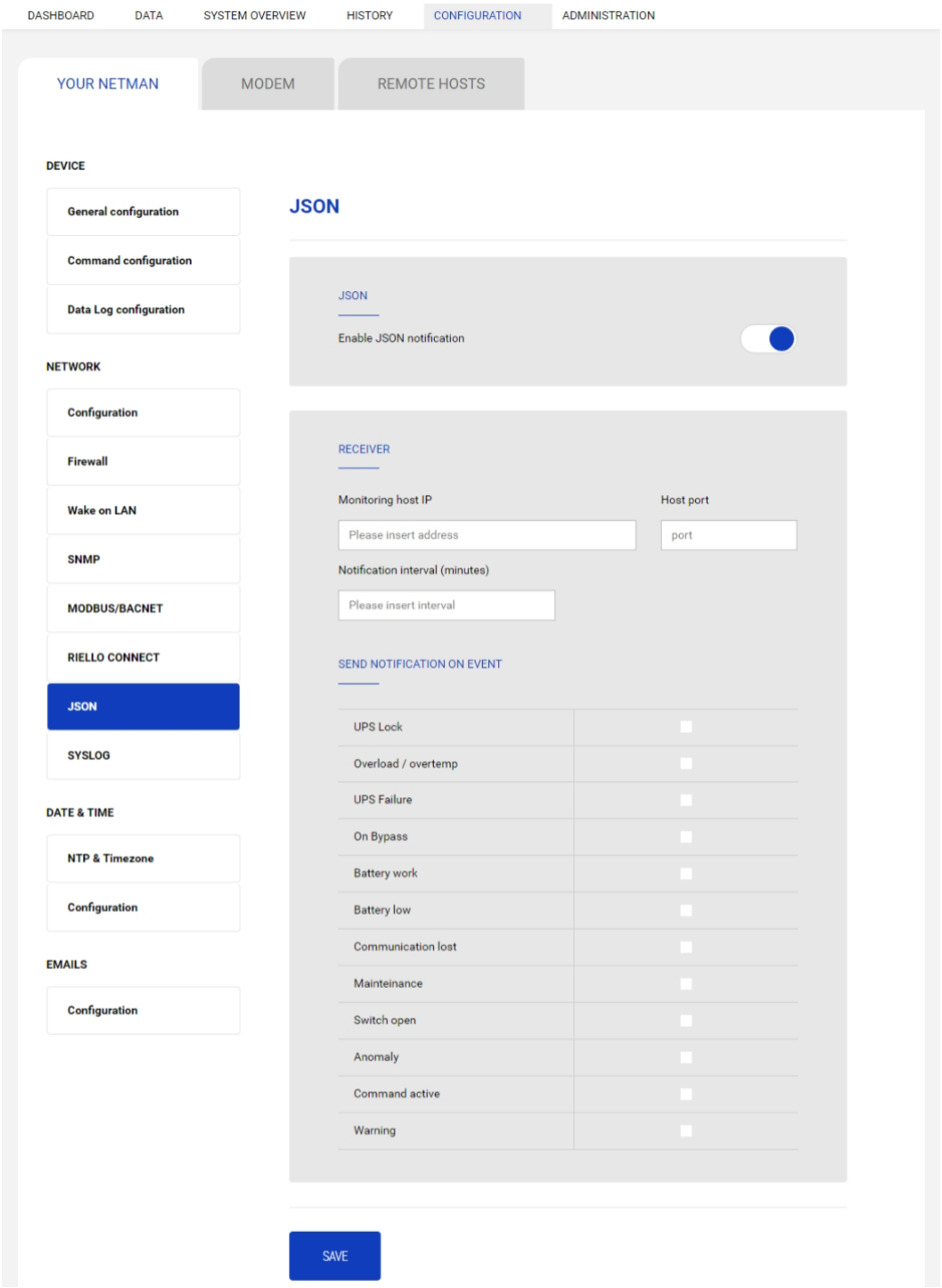
MODBUS/BACNET



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

Field	Description
Enable MODBUS	To enable the MODBUS protocol
Enable BACNET	To Enable 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 208 can send a periodic message in JSON trap format that contains the status and the values of the UPS. The trap can also be sent on the specified conditions.

Field	Description
Enable JSON	To enable 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 208*. 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.

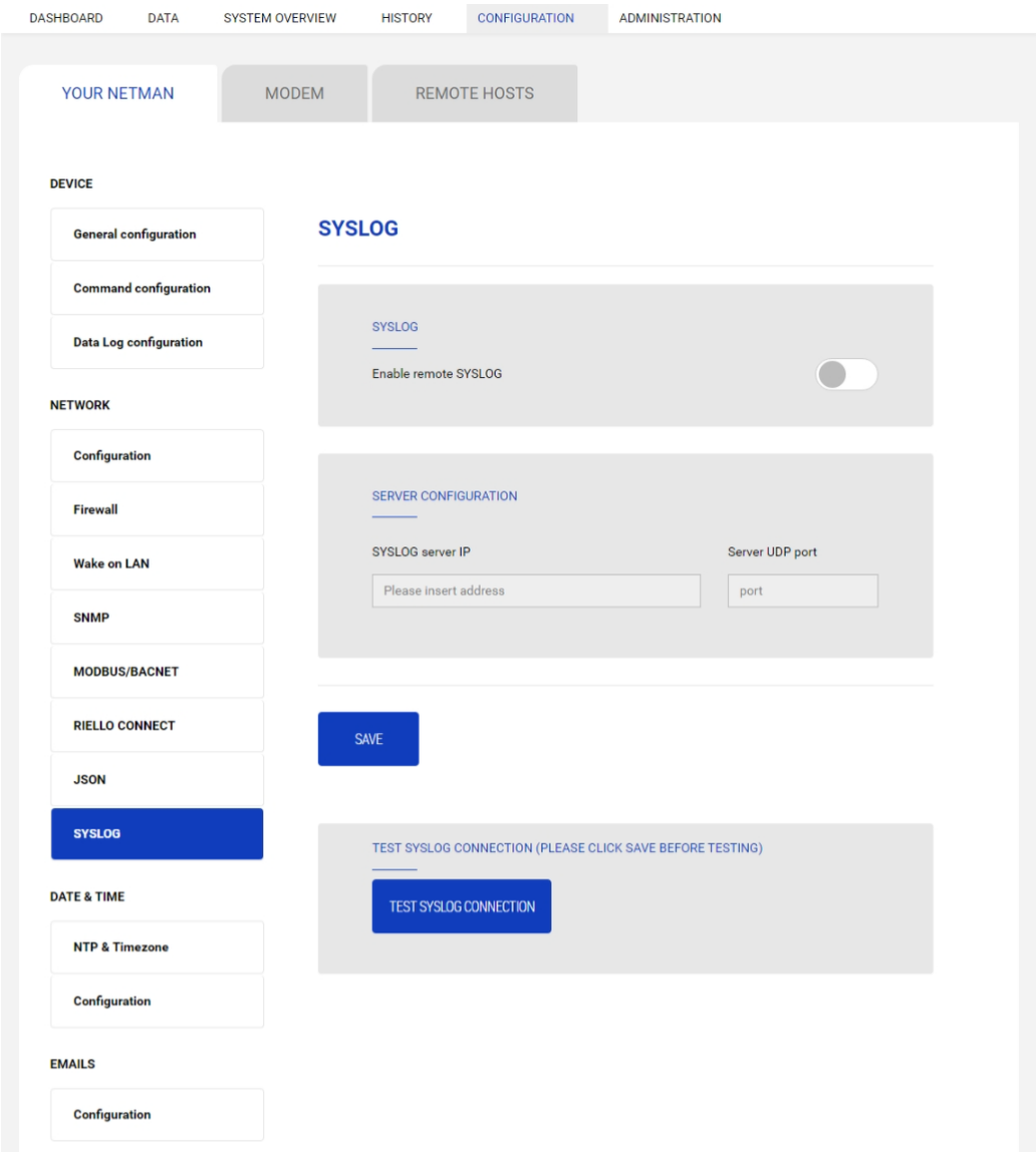
`status` is an array that must be interpreted as follows:

byte	bit	Description
0	0	UPS Mainteinance
	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



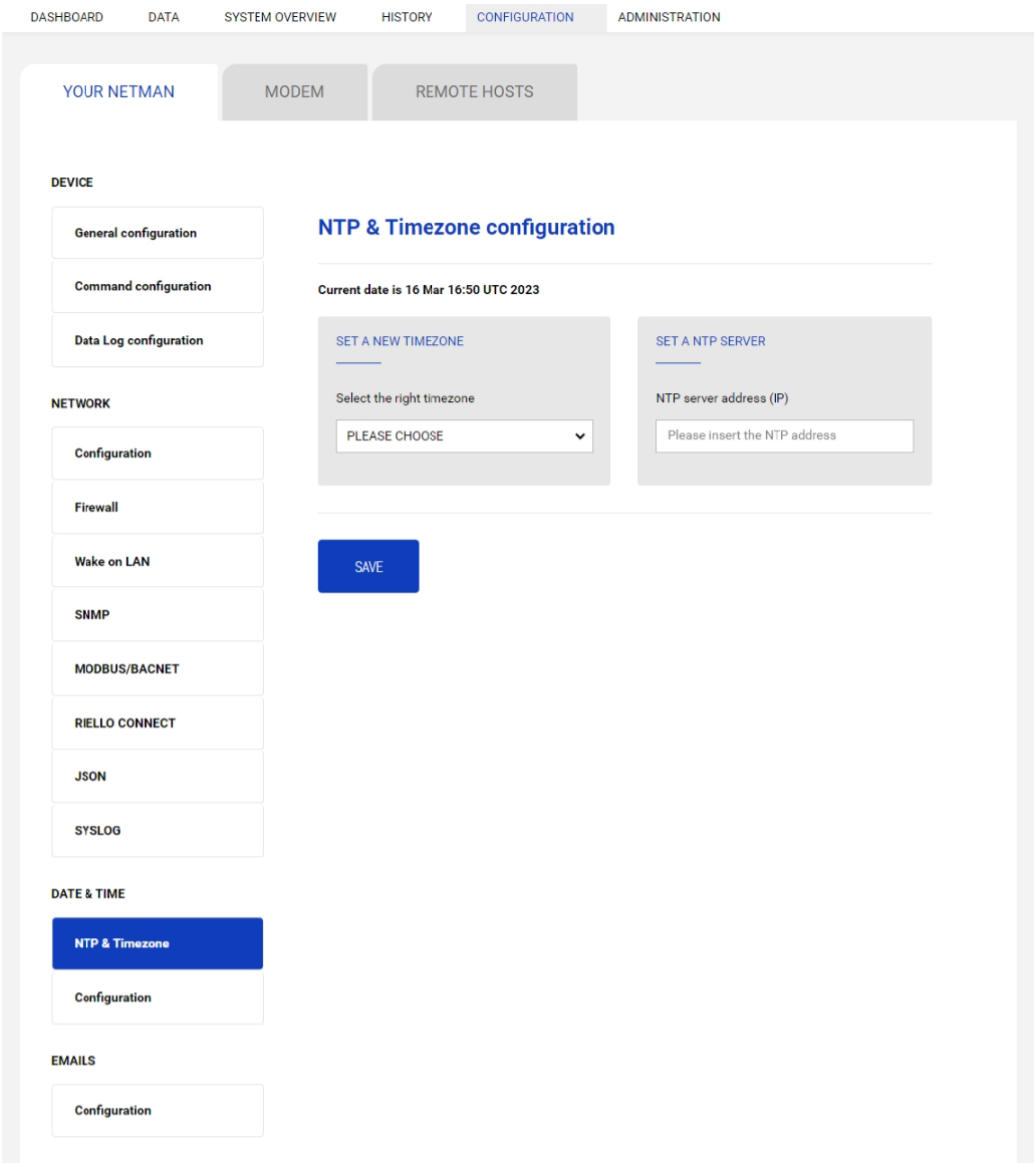
This menu allows to configure the syslog service over UDP port.

Field	Description
Enable remote syslog	To enable 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

DATE & TIME

NTP & Timezone

Some *Netman 208* 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.

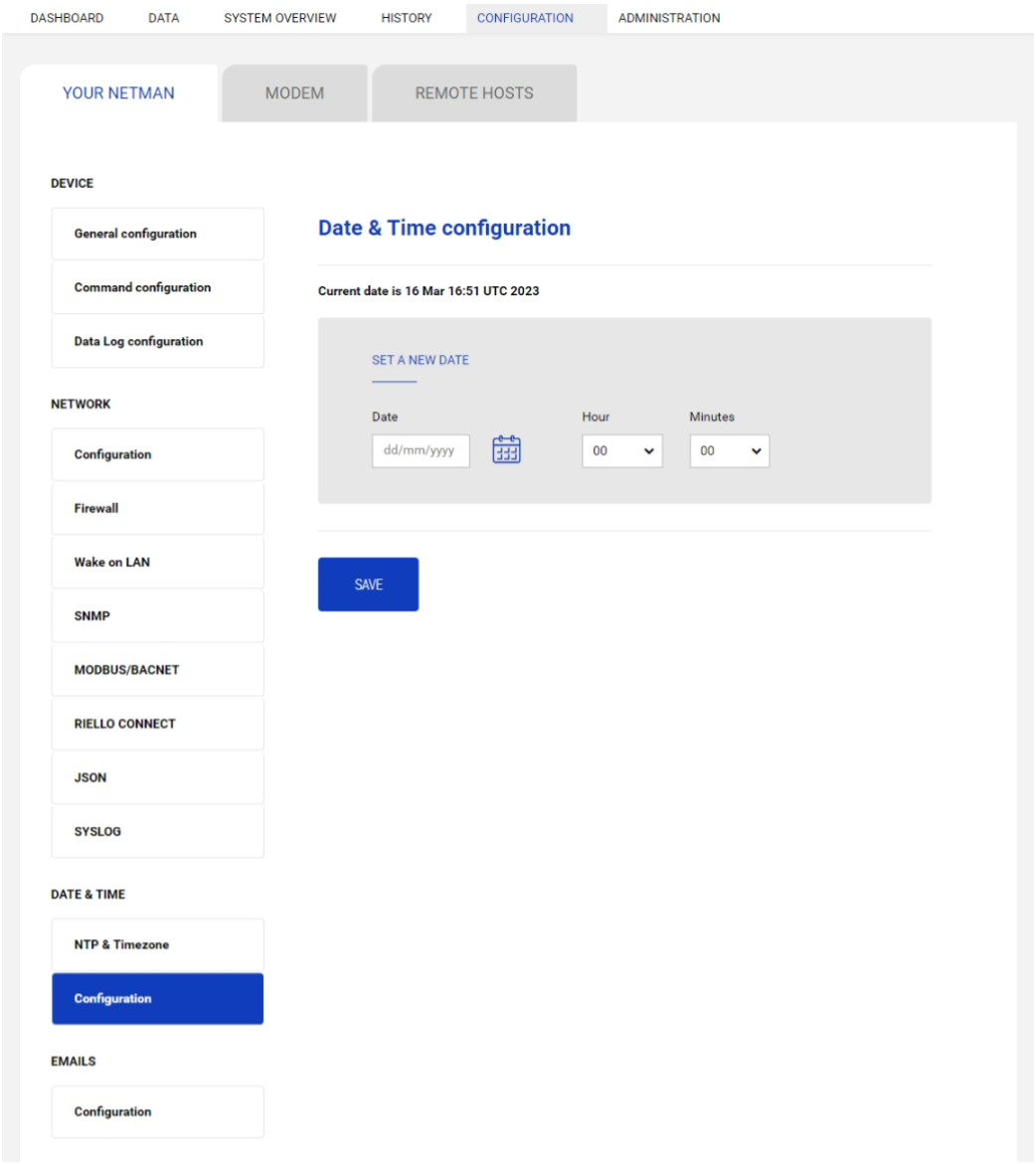


With this menu is possible to configure the NTP synchronization.

Field	Description
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 208* will synchronize the clock of the UPS daily at 00:30.

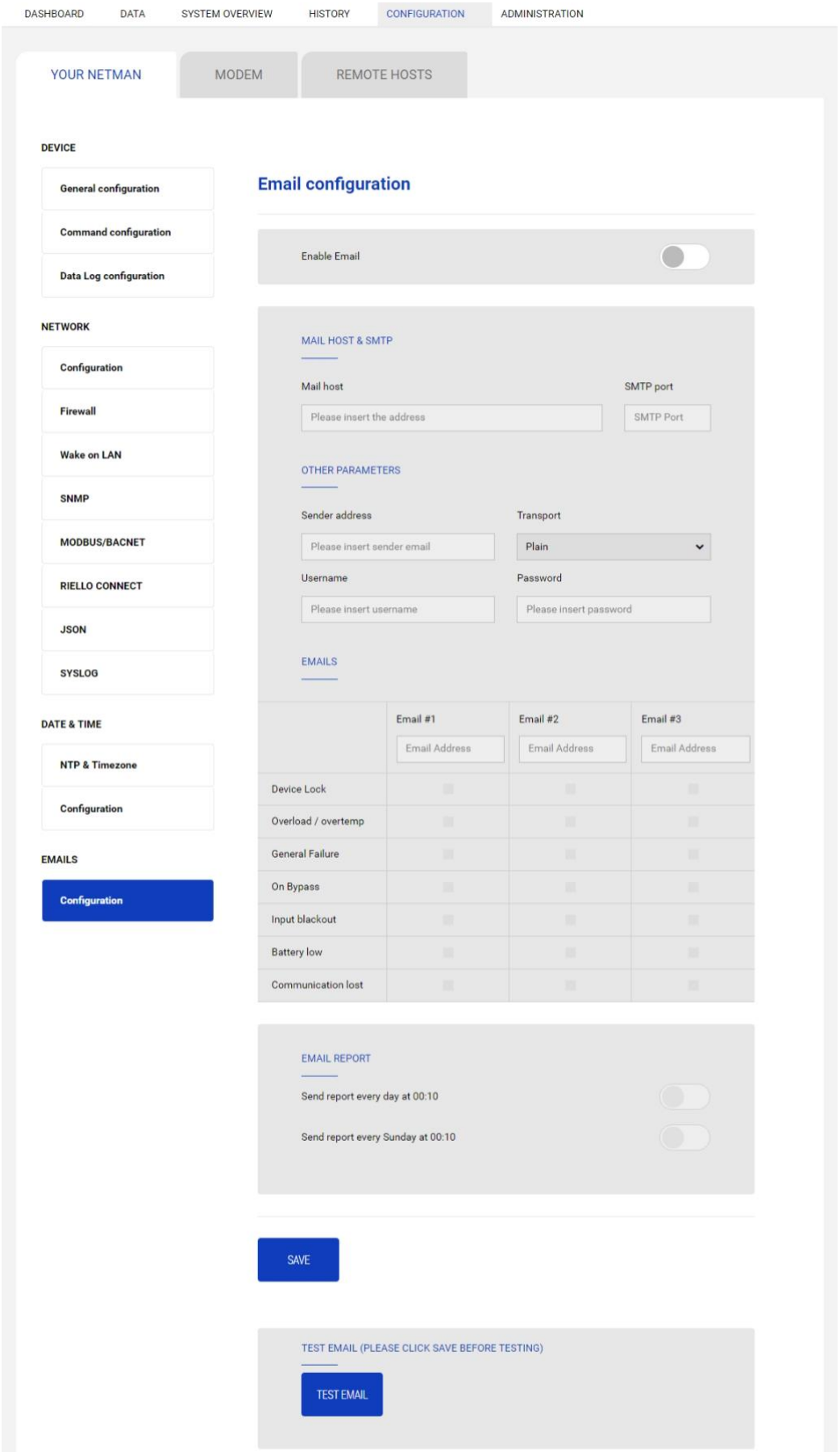
Configuration



Field	Description
Date	Enter the current date
Hour	Enter the current hour
Minutes	Enter the current minutes

EMAILS

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	Description
Enable Email	To enable 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 “Username”.
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	To send the email report every day at 00:00
Send report every week	To send 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.
Alarm notification e-mails are sent only to the selected addresses.

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

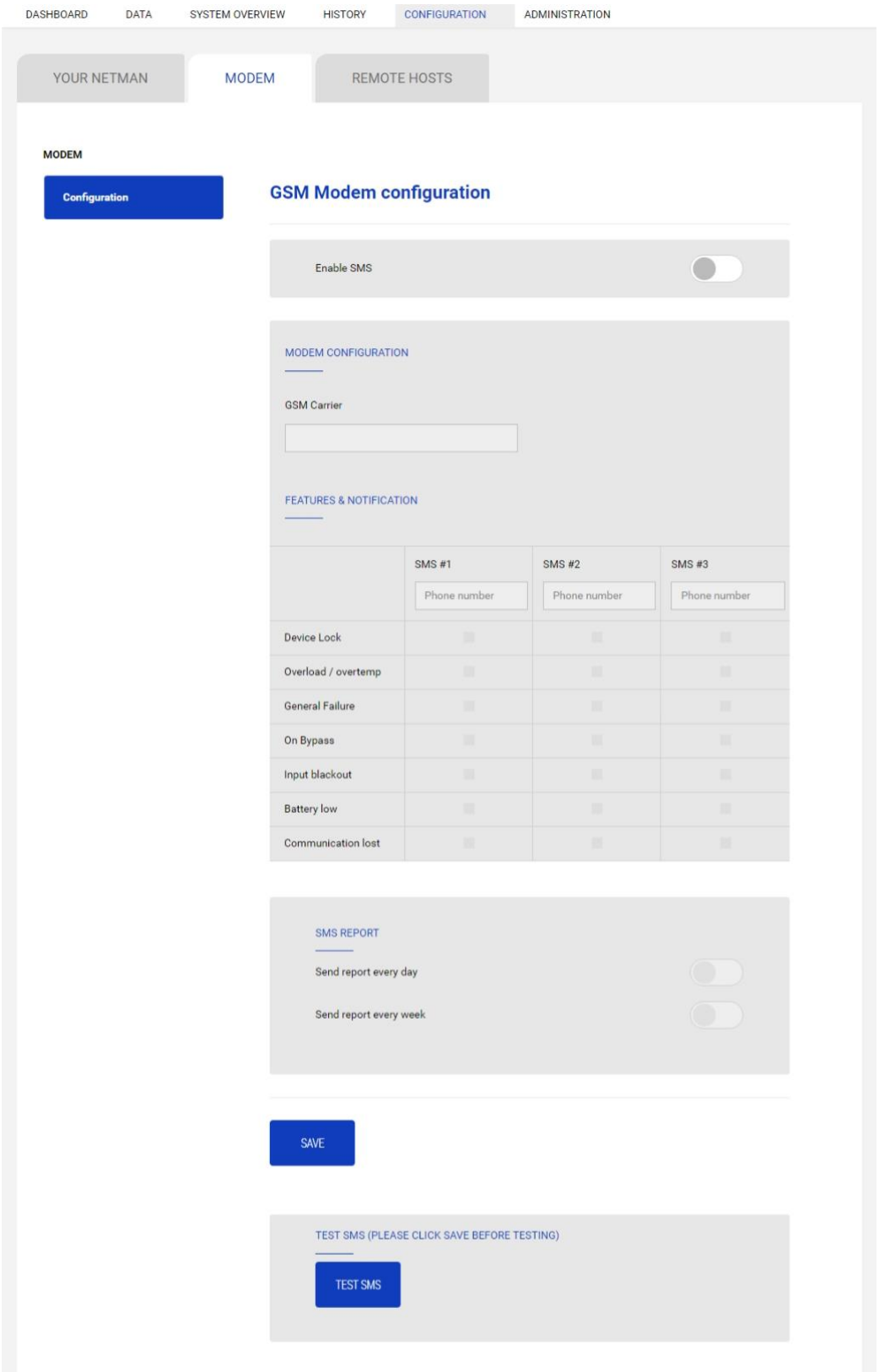
Event	Meaning
Device Lock	Device is locked or in a severe failure state
Ovrload/Ovrtemp	Device in overload or in overtemperature
General Failure	Failure of the device
On bypass	Operation from bypass
Input blackout	The input source is in blackout
Battery low	Battery low
Communic lost	Communication between the *Netman 208* and the device has been interrupted

GSM MODEM

Configuration

Netman 208 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.

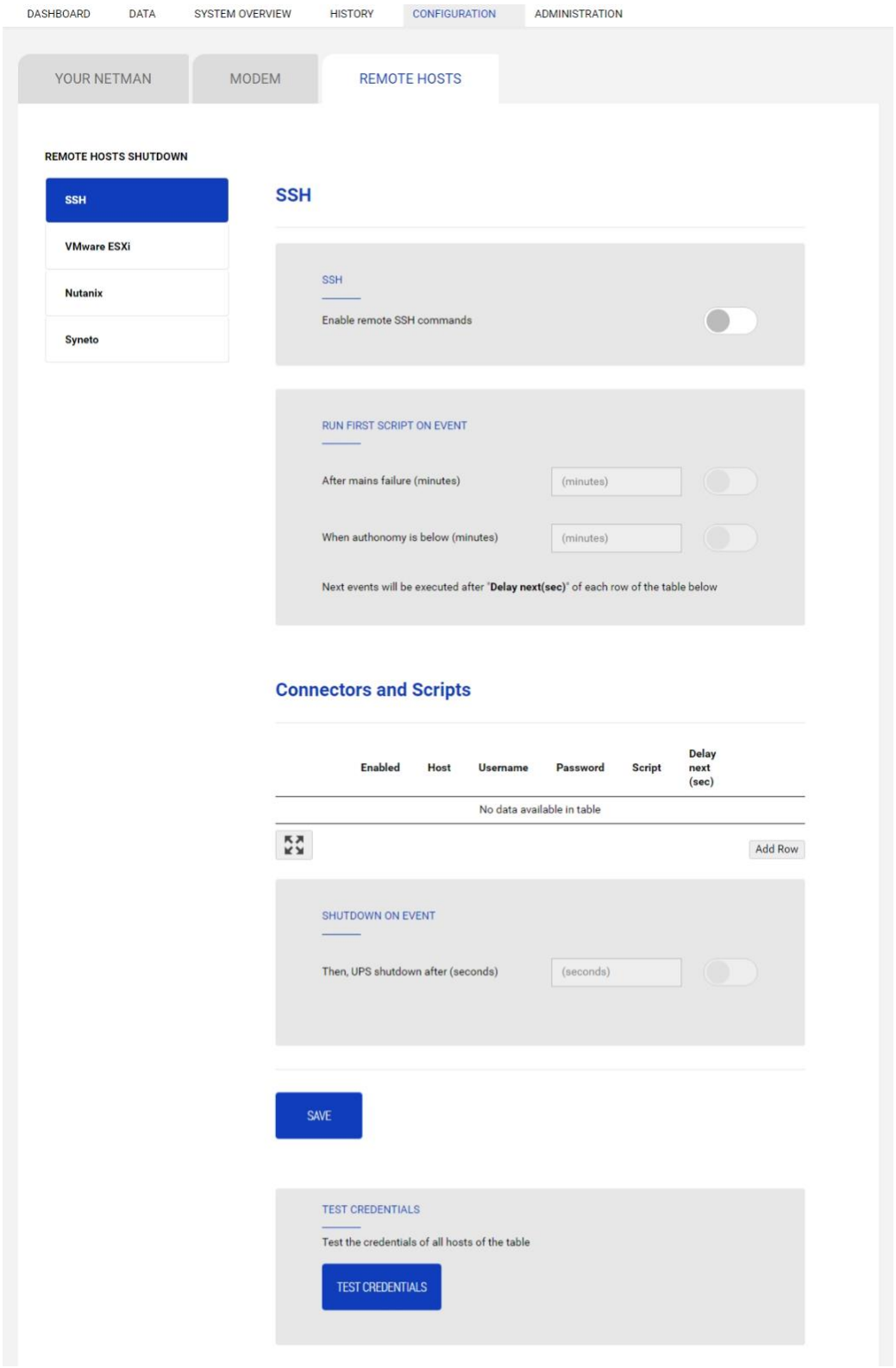


This menu may be used to configure the GSM modem in order to send SMS.

Field	Description
Enable SMS	To enable 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	To send the SMS report every day at 00:00
Send report every week	To send the SMS report every Monday at 00:00

REMOTE HOSTS

SSH



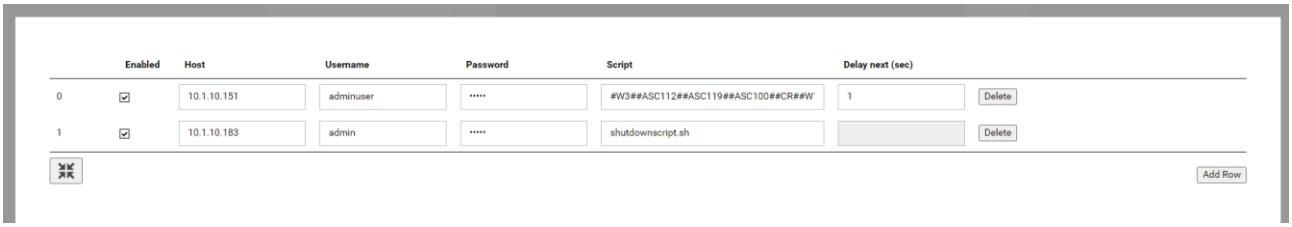
This section allows to configure the SSH client service.

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

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

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

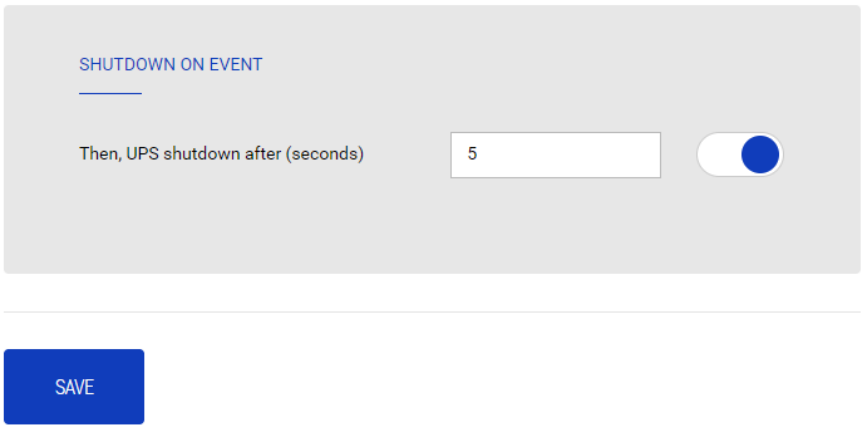
Actions to call must be configured in the table:



one action per row, with a "delay next" before executing the row below.
For each row, then fields are:

Row Field	Description
Enabled	Action enabled
Host	Host to connect to via SSH
Username	Username for login to SSH
Password	Password for login to SSH
Script	Command to execute after login (***simple command*** or ***multiple command string***)
Delay next (sec)	In case of multiple actions (rows) the delay (seconds) before executing the next action

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



Type of commands as action for Script: single command

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

Here some examples:

```
shutdown 5
```

```
/run/custom/switchchoff.sh
```

```
/run/myshutdownscript.sh
```

Type of commands as Action for Script: multiple command string

A more complete solution is using a ***multiple command string***: is written as single string data but it behaves as a multiple command as if the User were typing char after char the commands (with return keys and other characters including pauses).
This solution with “multiple command string” allow to shutdown a device via SSH when there is the need of some sort of interaction (delays, enter keys, special chars).

The list of tags accepted is:

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

Some examples here:

// Shutdown of QNAP

```
Q#CR#Y#CR#/sbin/poweroff#CR#
```

that is like typing manually:

```
Q (enter)
Y (enter)
/sbin/poweroff (enter)
```

// Shutdown commands for "NetApp OnTap 9.9.1"

```
system node halt -node * -skip-lif-migration-before-shutdown true -ignore-
quorum-warnings true -inhibit-takeover true -ignore-strict-sync-warnings
true#CR##W1#Y#CR##W1#Y#CR#
```

that is like typing manually:

```
system node halt -node * -skip-lif-migration-before-shutdown true -ignore-
quorum-warnings true -inhibit-takeover true -ignore-strict-sync-warnings true
(enter)
(wait 1 second)
Y (enter)
(wait 1 second)
Y (enter)
```

// Shutdown command for "Firewall CheckPoint"

```
halt#CR#Y#CR#
```

that is like typing manually:

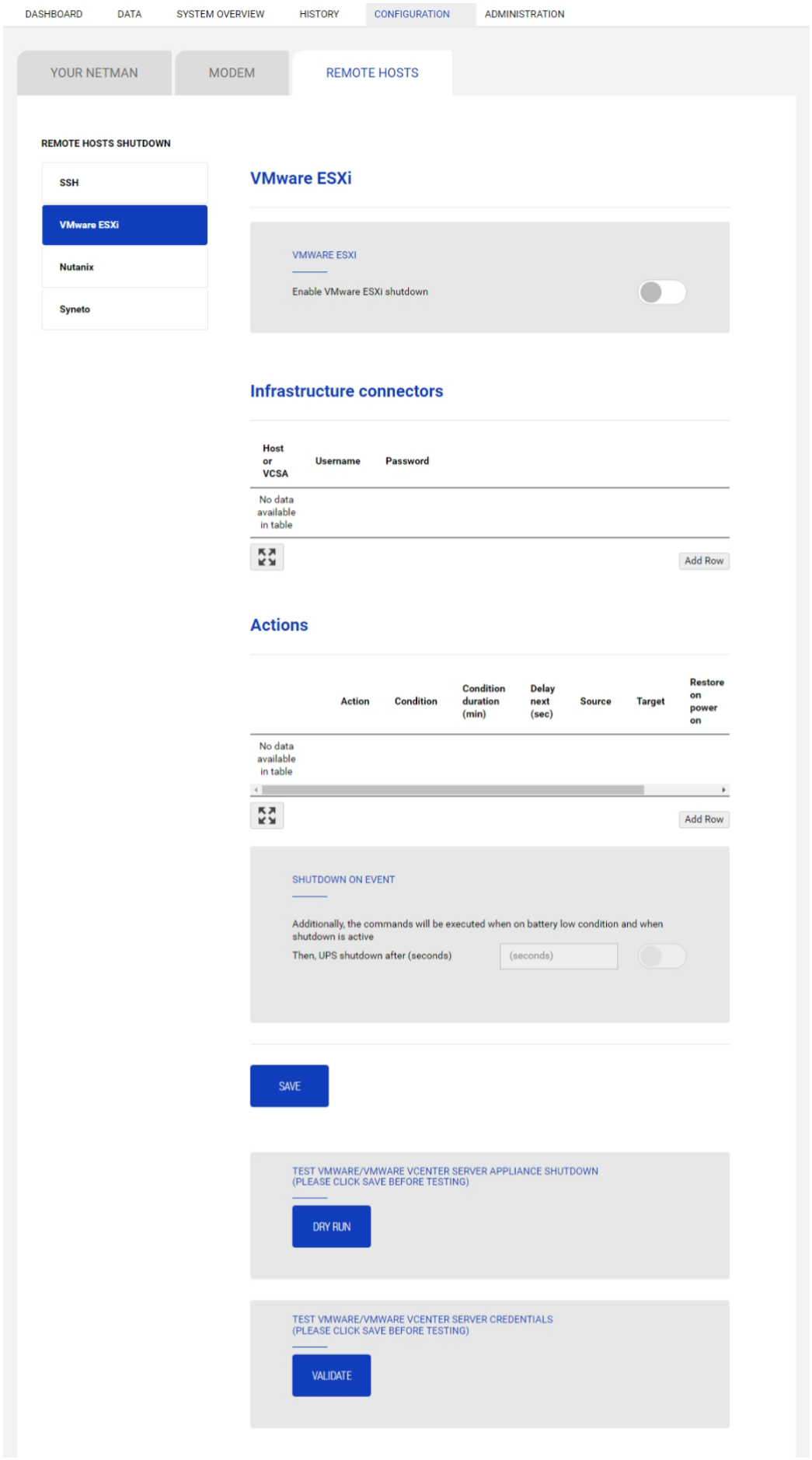
```
halt (enter)
Y (enter)
```

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

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

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

VMware ESXi


DASHBOARD
DATA
SYSTEM OVERVIEW
HISTORY
CONFIGURATION
ADMINISTRATION
YOUR NETMAN
MODEM
REMOTE HOSTS
REMOTE HOSTS SHUTDOWN
SSH
VMware ESXi
Nutanix
Syneto
VMware ESXi
VMWARE ESXI
Enable VMware ESXi shutdown
Infrastructure connectors
Host or VCSA
Username
Password
No data available in table
Add Row
Actions
Action
Condition
Condition duration (min)
Delay next (sec)
Source
Target
Restore on power on
No data available in table
Add Row
SHUTDOWN ON EVENT
Additionally, the commands will be executed when on battery low condition and when shutdown is active
Then, UPS shutdown after (seconds)
(seconds)
SAVE
TEST VMWARE/VMWARE VCENTER SERVER APPLIANCE SHUTDOWN (PLEASE CLICK SAVE BEFORE TESTING)
DRY RUN
TEST VMWARE/VMWARE VCENTER SERVER CREDENTIALS (PLEASE CLICK SAVE BEFORE TESTING)
VALIDATE

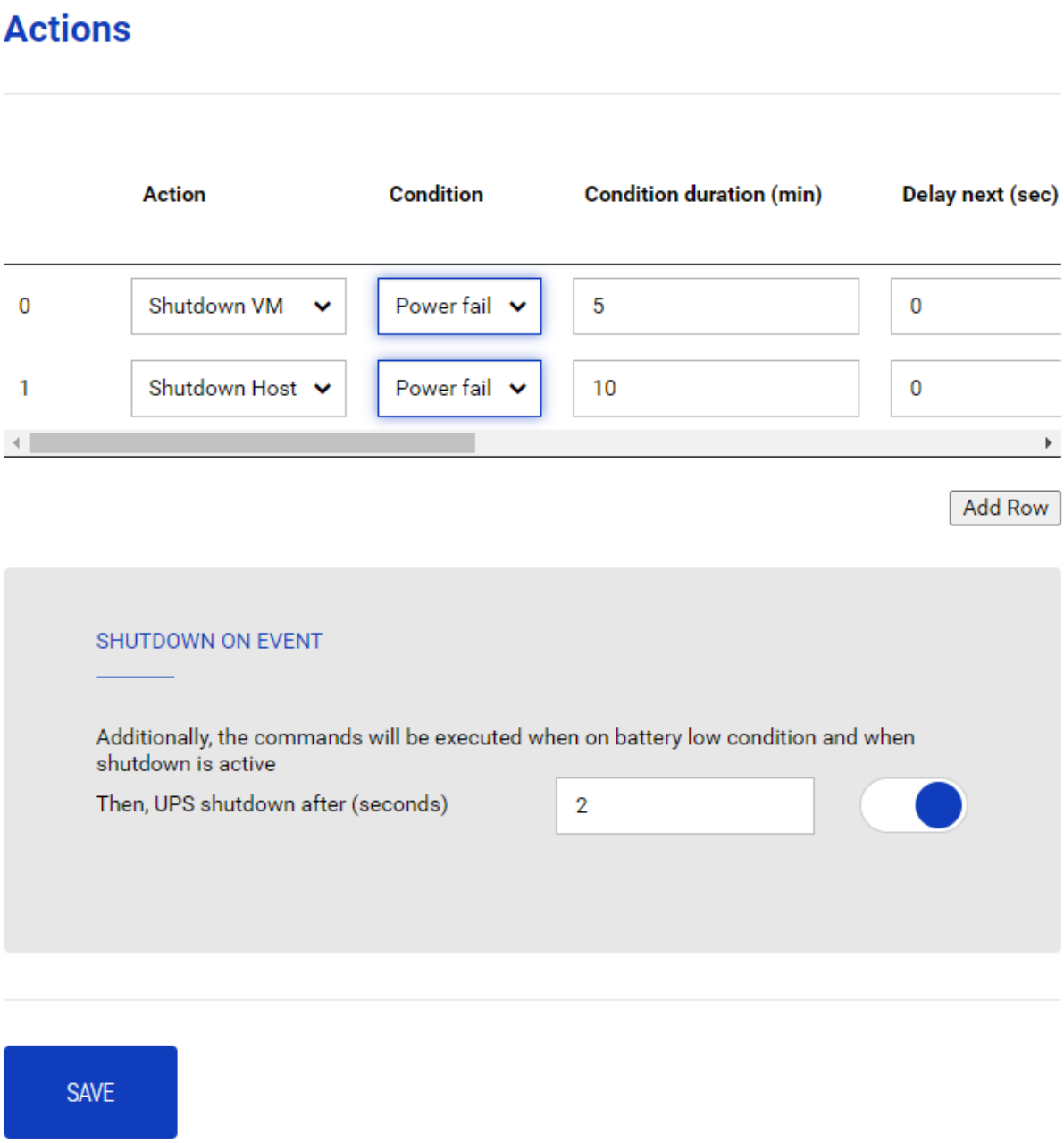
This menu enables the configuration of the VMware Esxi shutdown service. Any Esxi host or part of a vSphere infrastructure or the included vCenter server appliance can be shut down, it is possible execute a vMotion in order to move active VM from a host or Cluster to a specific target, each with their separate credentials, priority and delay.
The validity of the credentials is checked periodically and, if not valid, an alarm is generated.
It is also possible to shutdown the UPS at the end of the hosts shutdown process.

ATTENTION
The 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	Description
Host or VCSA	Enter the hostname or IP address of the ESXi host or VCSA
Username	Enter the username for ESXi or VCSA administrator
Password	Enter the password for ESXi or VCSA administrator



Actions

Field	Description
Action	The action that will be executed: **Shutdown VM** will shutdown the specific VM **Shutdown Host** will shutdown all the active VM on the specified host and finally the host itself **Shutdown Cluster** will shutdown all the active VM on the specified cluster and all hosts part of the cluster **VMotion** will move all the active VM from a source host to a target host **Maintenance** will force a host in maintenance mode

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 **Shutdown Host**, **VMotion** or **Maintenance**; an IP address or hostname of a present host or VCSA must be specified. If the action is **Shutdown VM** or **Shutdown Cluster** a valid VM name or Cluster name, present in the infrastructure must be specified.
Target	If the action is **VMotion**, a valid IP address or hostname must be specified
Restore on power on	In case of shutdown actions the *Netman 208* will restart automatically all the VMs that where shutdown. In case of Maintenance action the *Netman 208* will restore the host from maintenance. Please note that to restart the host the Wake on Lan feature must be used instead.
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.

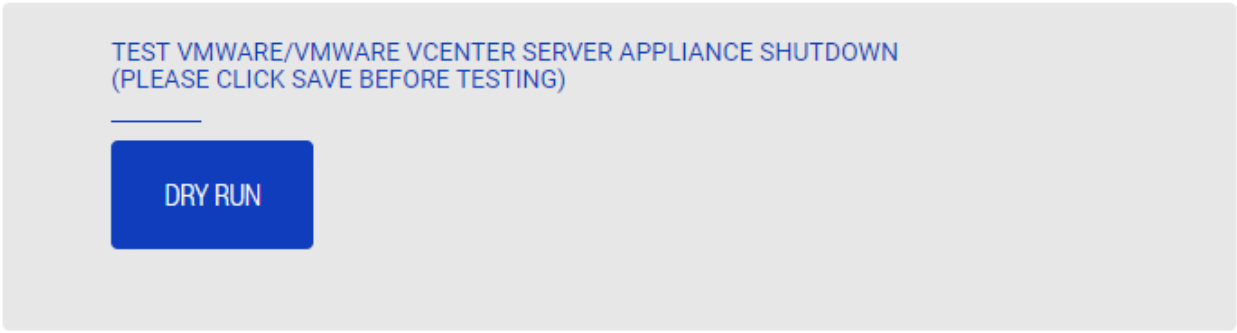
SHUTDOWN ON EVENT

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.

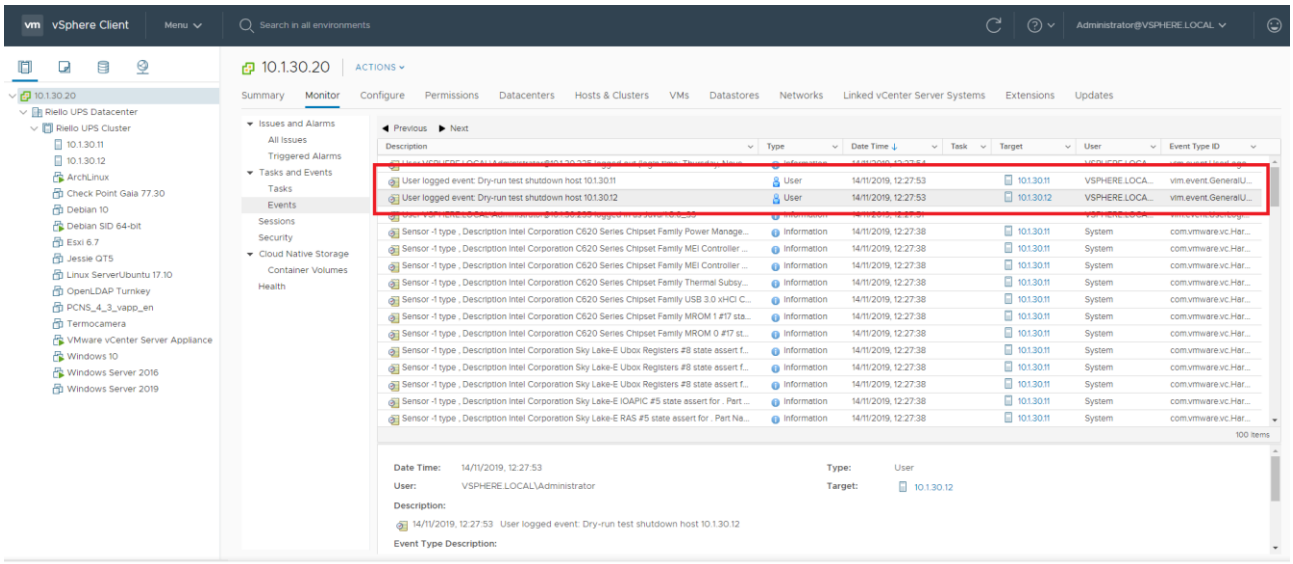
Additionally, the commands will be executed when on battery low condition and when shutdown is active.

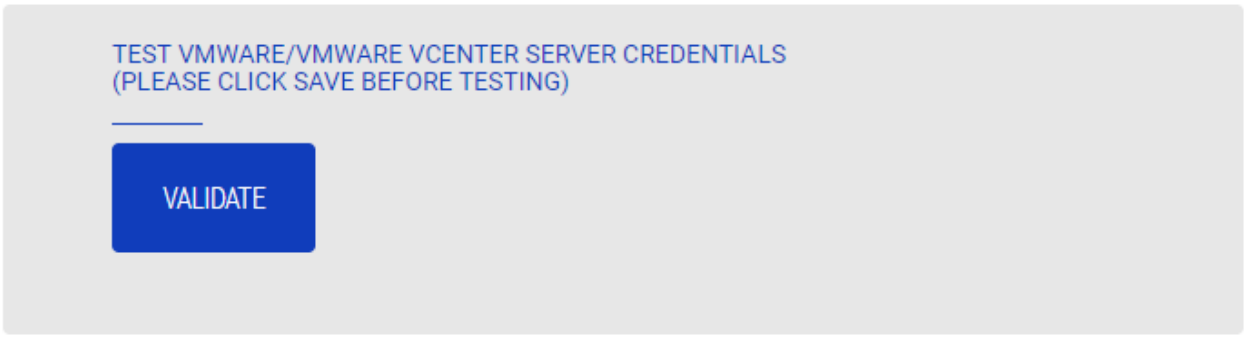
SAVE

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



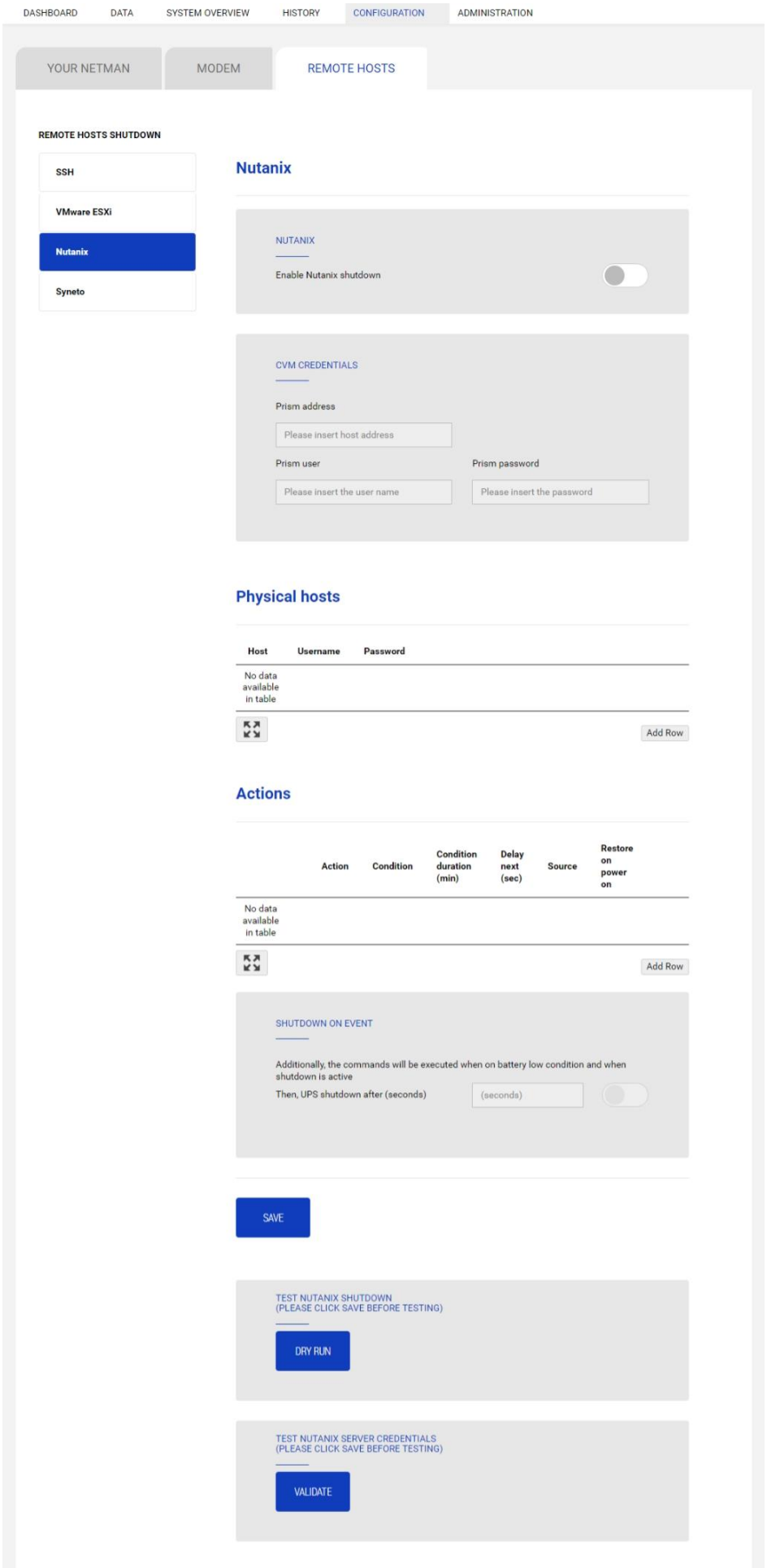
Testing the configuration
It is possible to test the procedure without performing a real shutdown by pressing “Dry Run”. The logs on the target host or vCenter Server Appliance will confirm the correctness of the configuration.





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.

Nutanix

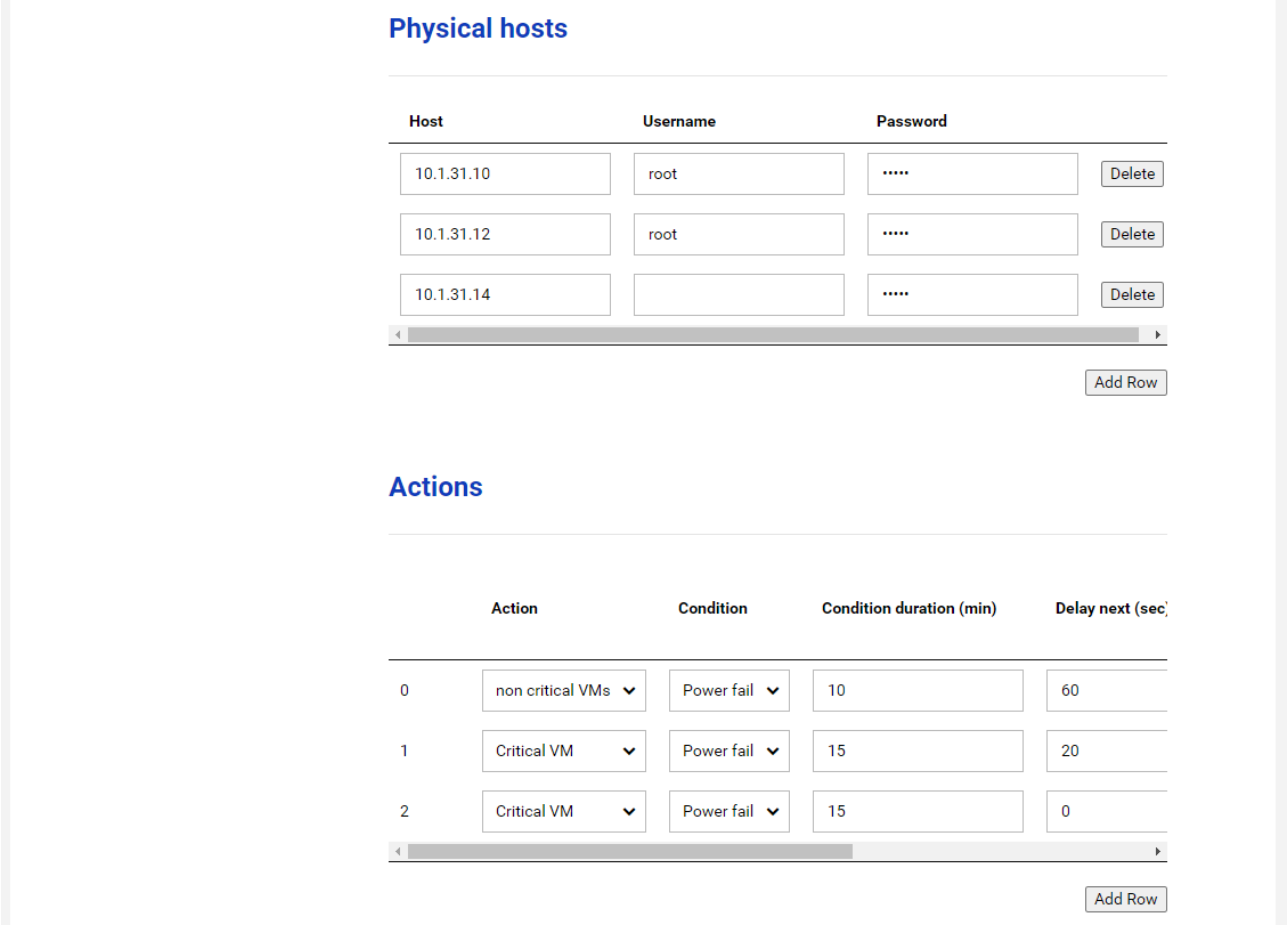

DASHBOARD
DATA
SYSTEM OVERVIEW
HISTORY
CONFIGURATION
ADMINISTRATION
YOUR NETMAN
MODEM
REMOTE HOSTS
REMOTE HOSTS SHUTDOWN
SSH
VMware ESXi
Nutanix
Syneto
Nutanix
NUTANIX
Enable Nutanix shutdown
CVM CREDENTIALS
Prism address
Please insert host address
Prism user
Please insert the user name
Prism password
Please insert the password
Physical hosts
Host
Username
Password
No data available in table
Add Row
Actions
Action
Condition
Condition duration (min)
Delay next (sec)
Source
Restore on power on
No data available in table
Add Row
SHUTDOWN ON EVENT
Additionally, the commands will be executed when on battery low condition and when shutdown is active
Then, UPS shutdown after (seconds)
(seconds)
SAVE
TEST NUTANIX SHUTDOWN
(PLEASE CLICK SAVE BEFORE TESTING)
DRY RUN
TEST NUTANIX SERVER CREDENTIALS
(PLEASE CLICK SAVE BEFORE TESTING)
VALIDATE

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

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

CVM credentials

Field	Description
Prism address	Enter the hostname or IP address of the Prism CVM
Username	Enter the username for CVM administrator
Password	Enter the password for CVM administrator



Actions

ıration (min)	Delay next (sec)	Source	Restore on power on	
	60		☑	Delete
	20	79ab502a-13ca-4162-8aa	☑	Delete
	0	568bd95a-af84-4510-bcb'	☑	Delete

Add Row

SHUTDOWN ON EVENT

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

Then, UPS shutdown after (seconds) 180

SAVE

TEST NUTANIX SHUTDOWN
(PLEASE CLICK SAVE BEFORE TESTING)

DRY RUN

TEST NUTANIX SERVER CREDENTIALS
(PLEASE CLICK SAVE BEFORE TESTING)

VALIDATE

Actions

Field	Description
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 *Netman 208* 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

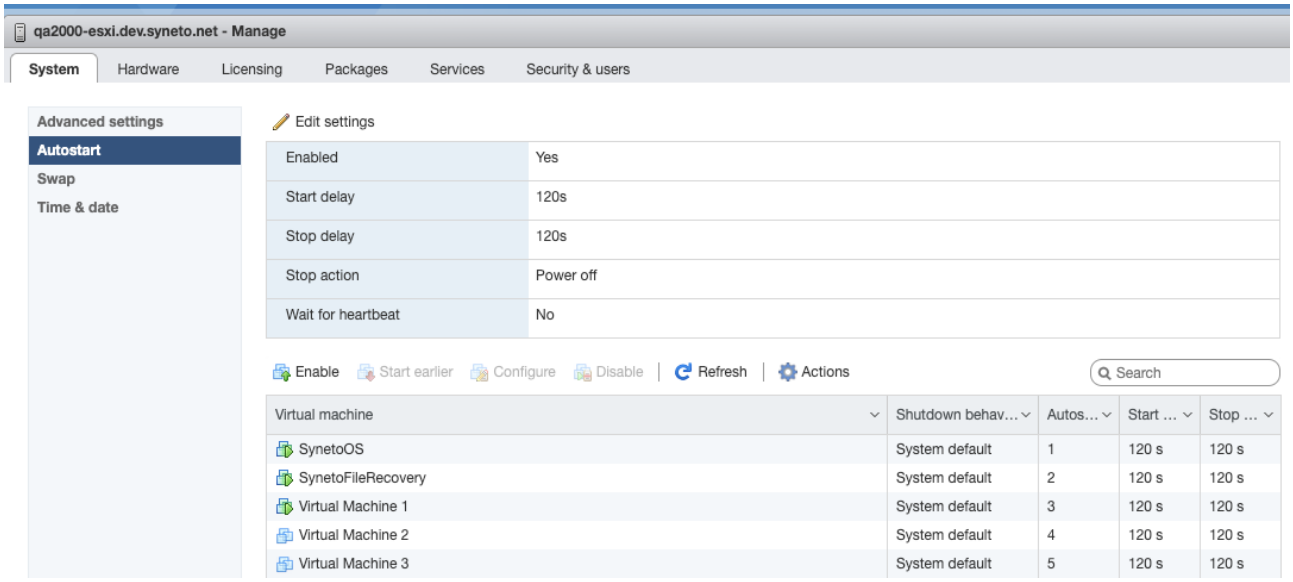
It is possible to test the procedure without performing a real shutdown by pressing “Dry Run”. The logs on the target Prism CVM will confirm the correctness of the configuration.

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.

CONFIGURE ESXI AUTOSTART FUNCTIONALITY

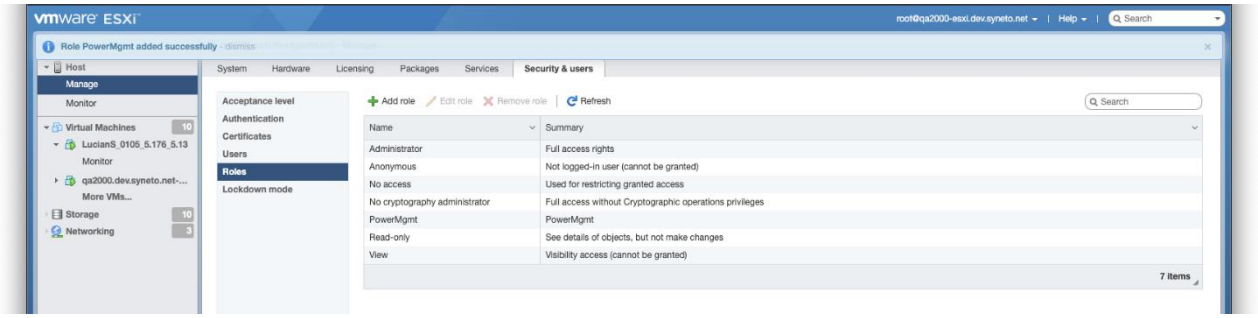
Syneto HYPER appliances have the Autostart functionalities enabled by default on the ESXi hypervisor. This is a mandatory prerequisite so that virtual machines can be powered on or off in the right order when the request is made from *Netman 208*.
Configure the virtual machines that must be powered on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

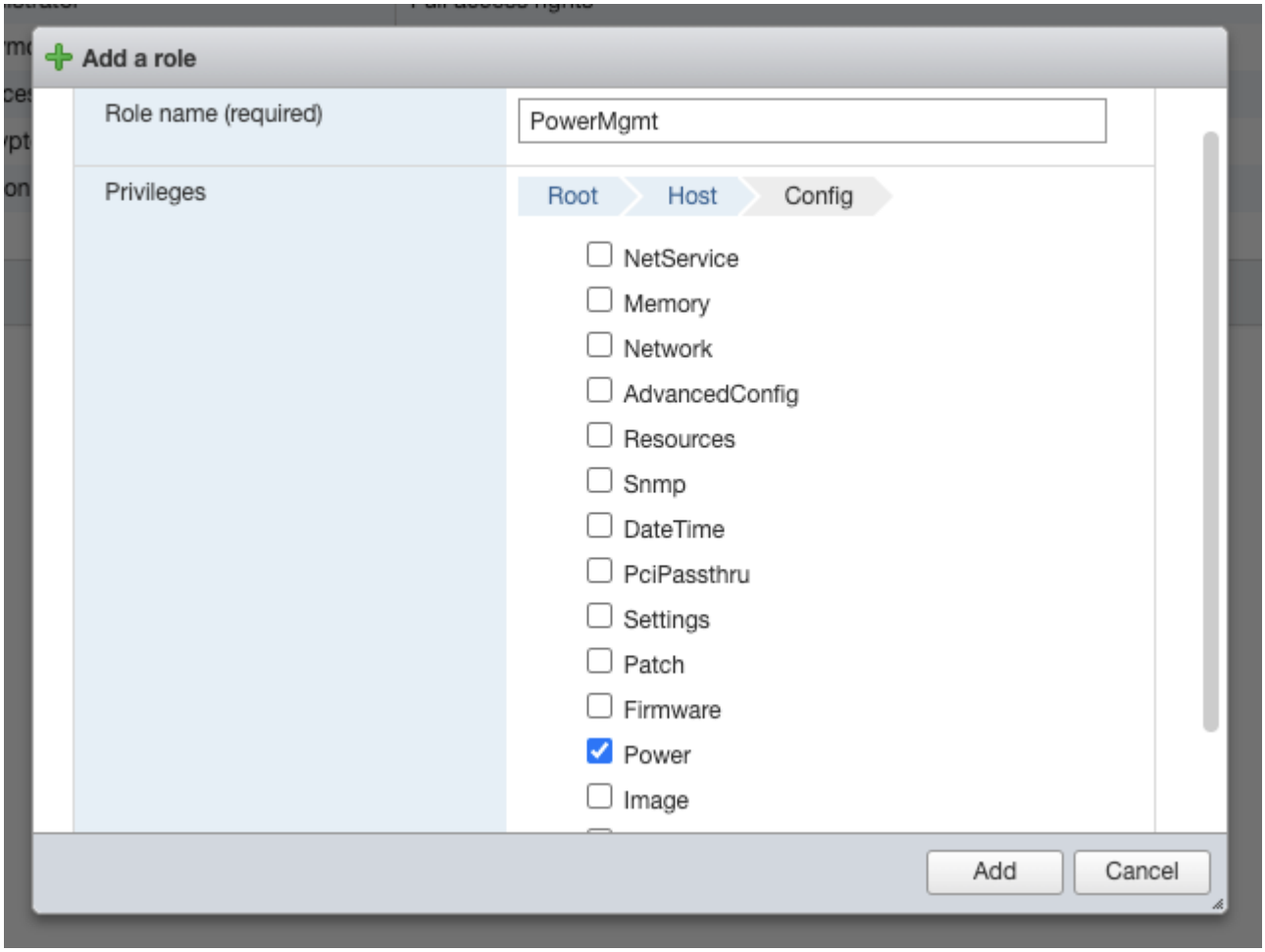
1. Create a new Role.
Go to Host -> Security and Users -> Roles.



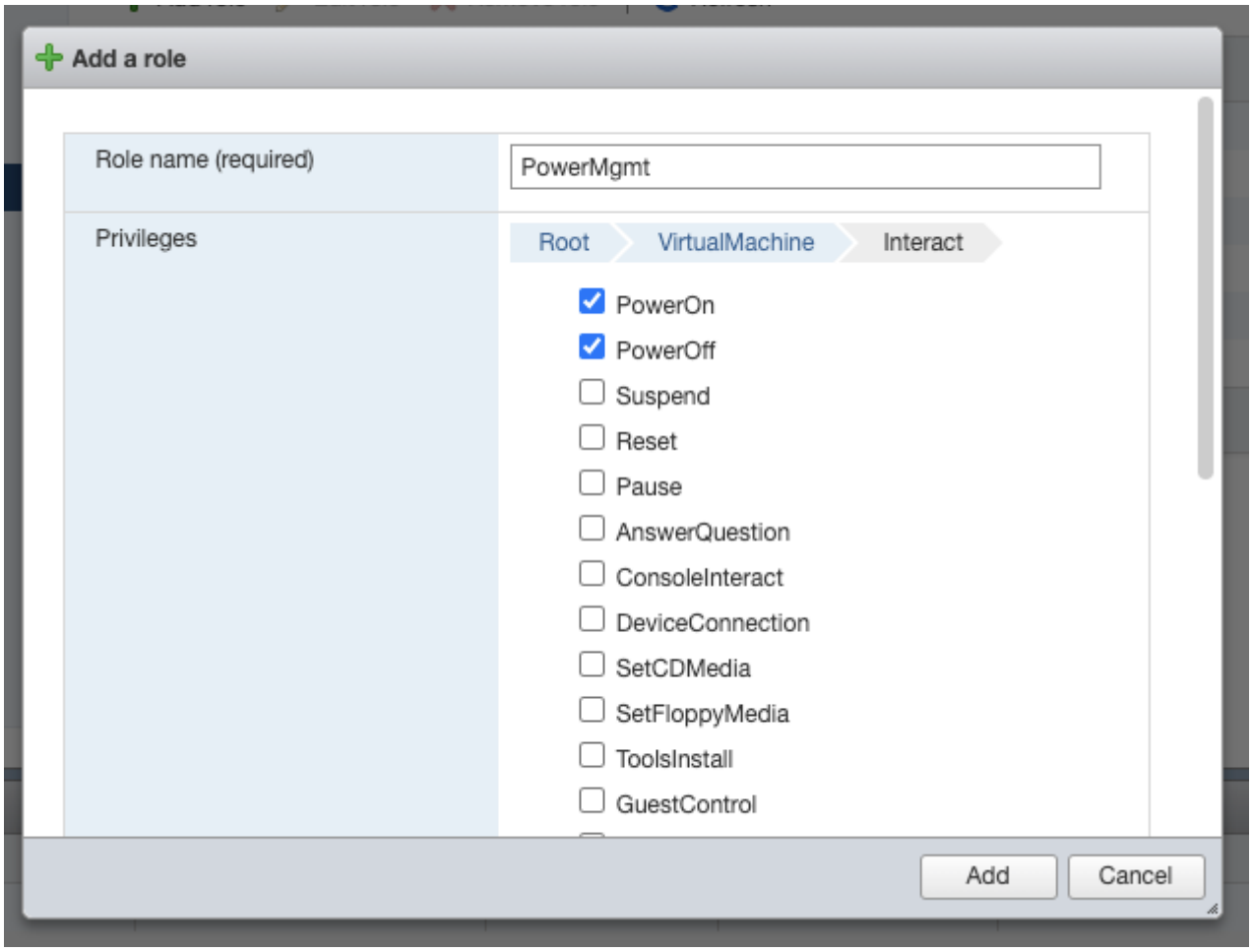
Click on Add Role. Give the new role a suggestive name, for example: PowerMgmt.

Choose the following from Privileges:

Root -> Host -> Config -> Power.



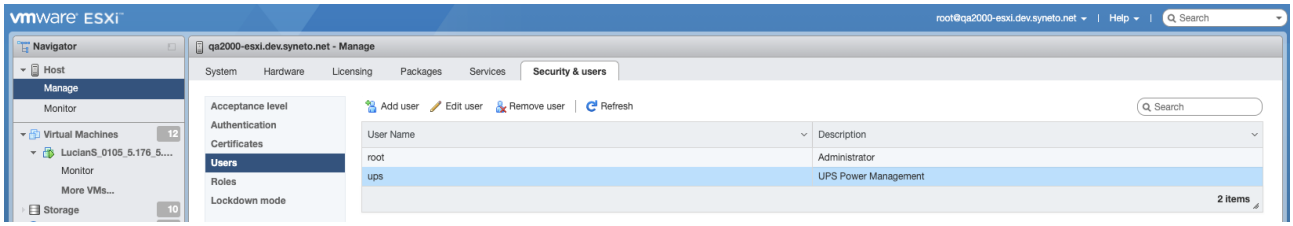
Root -> VirtualMachine -> Interact -> PowerOn, PowerOff



Click Add to create the new role.

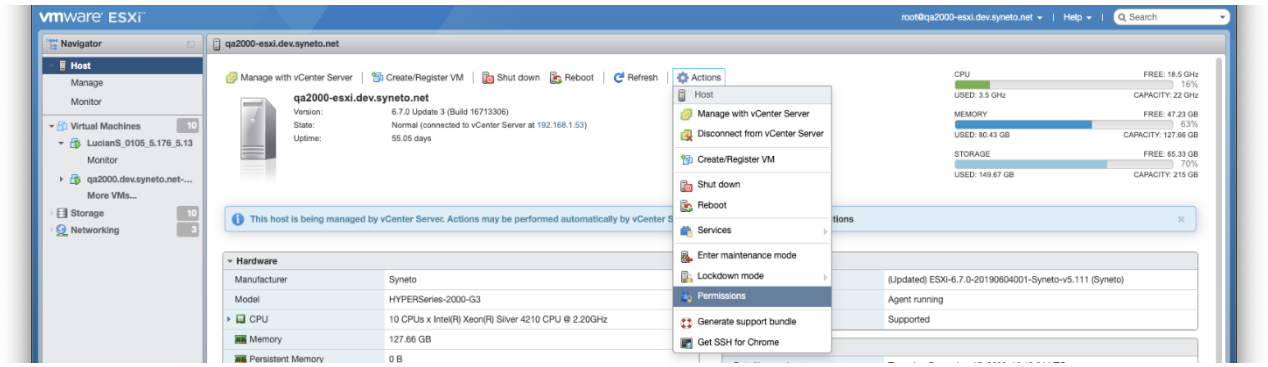
2. Create a new user.

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

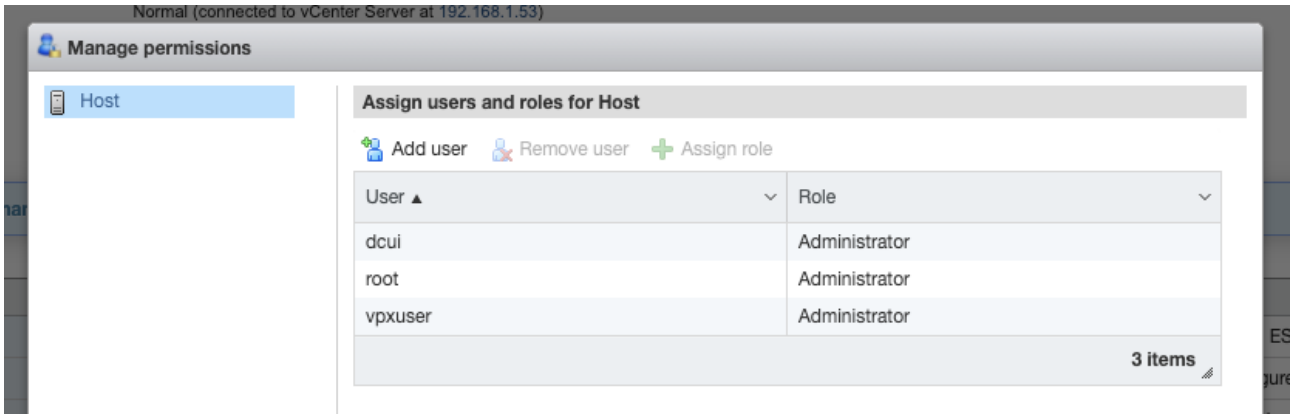


3. Assign the role PowerMgmt to the newly created user ups on the ESXi host.

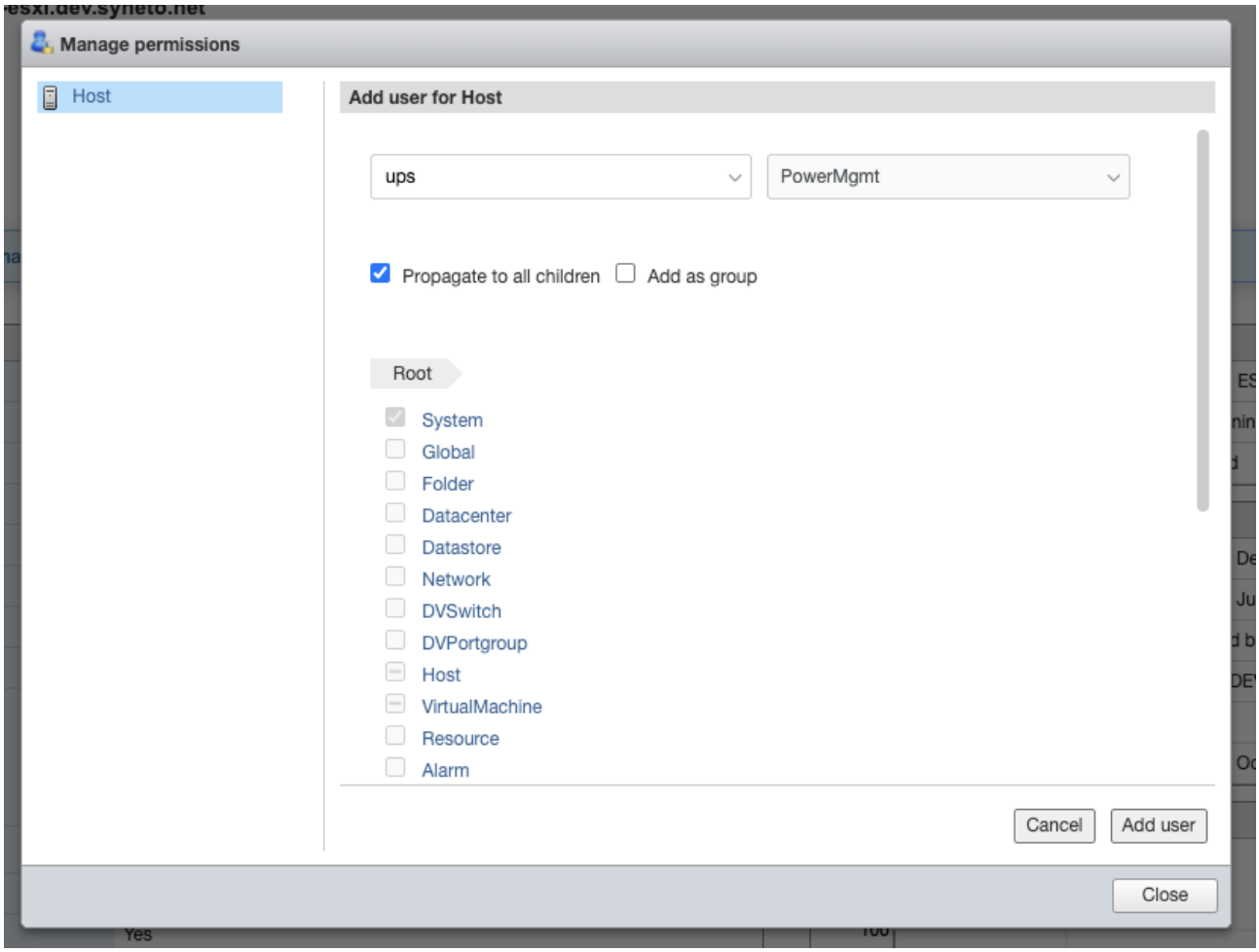
Go to Host -> Actions -> Permissions.



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



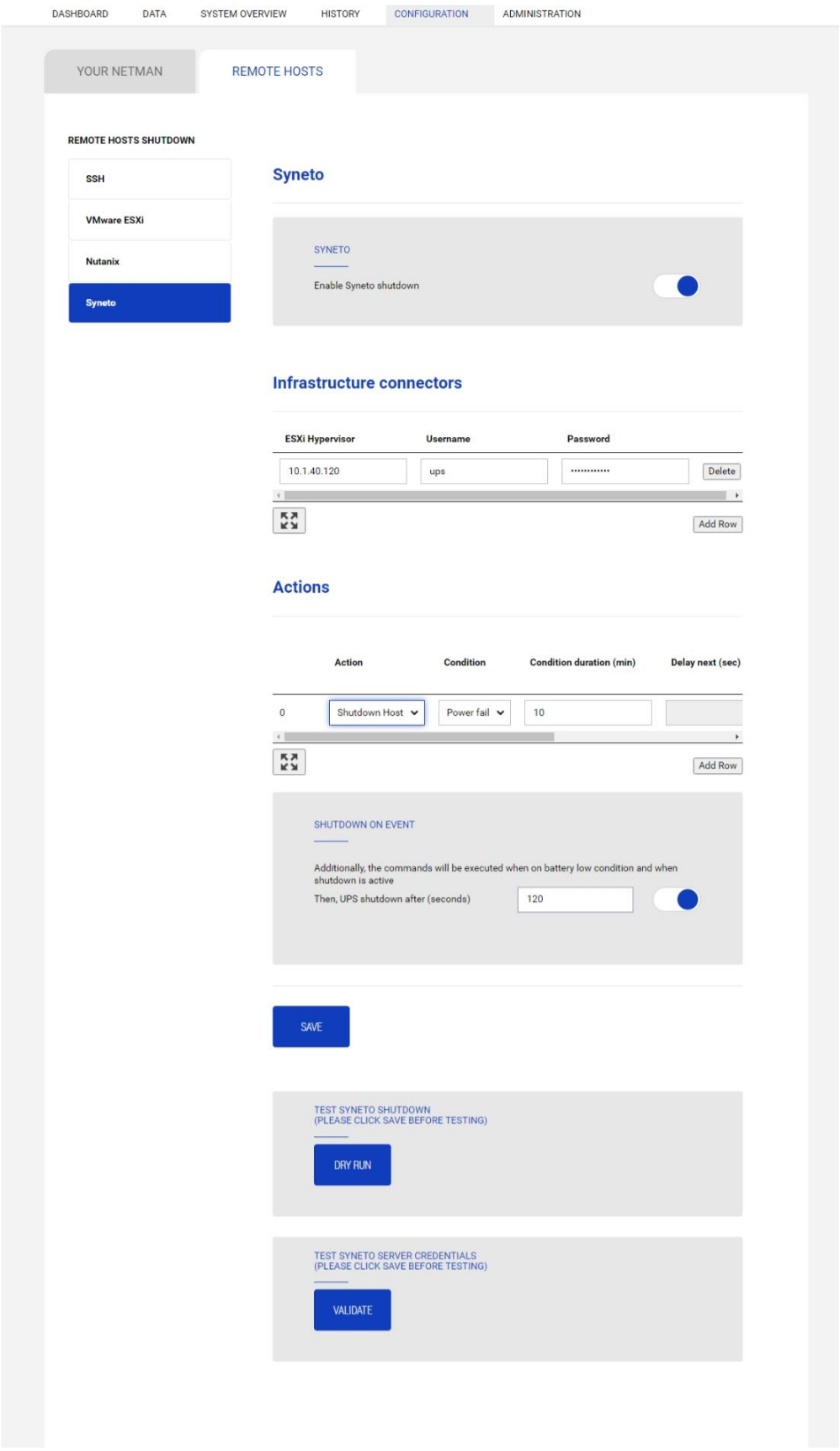
Type the username in the field, select the appropriate role for power management. For this example, *ups* and *PowerMgmt*.



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

CONFIGURE NETMAN 208 FOR HOST SHUTDOWN

Connect to *Netman 208* via the web interface. Go to Configuration -> Remote Hosts -> Syneto

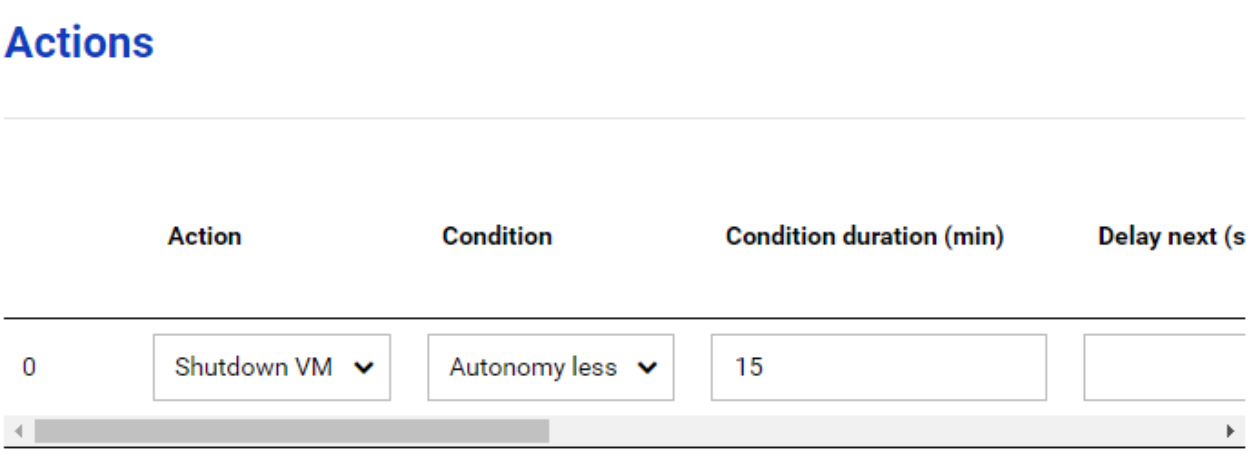


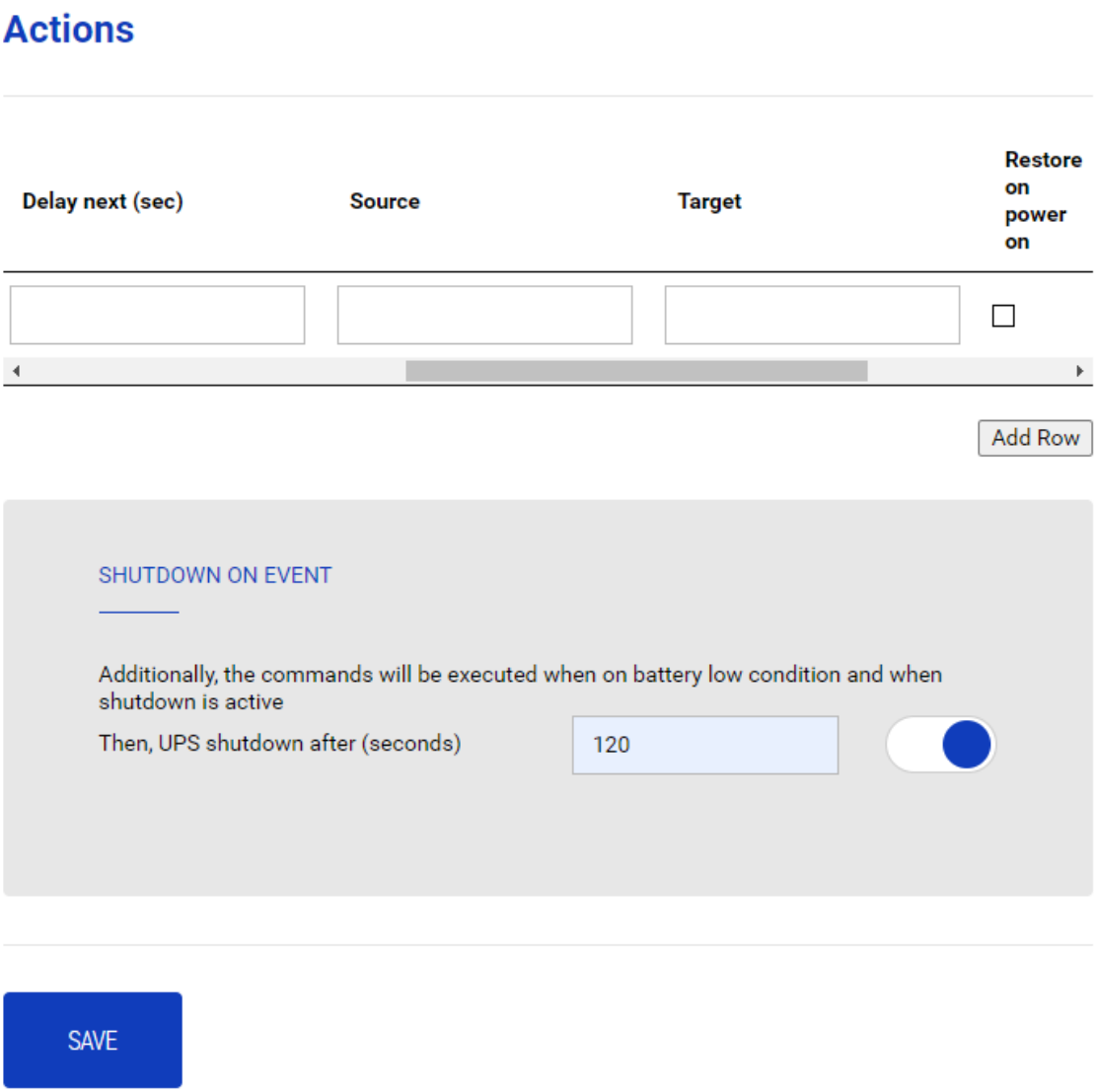
- Check the box for Enable Syneto shutdown
- In the section Infrastructure connectors, click on the Add Row button. You will connect *Netman 208* to the ESXi host.
- Enter the following:

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:	**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. **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.
Condition duration (minutes):	The duration that the selected condition (Power fail or Autonomy less) must be active for before the selected action starts. **We recommend at least 15 minutes.**





The device with *Netman 208* 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.

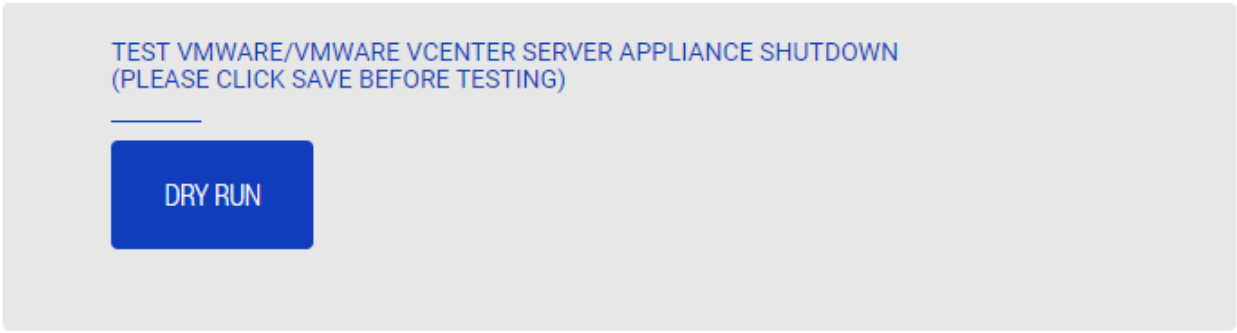
SHUTDOWN ON EVENT

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.

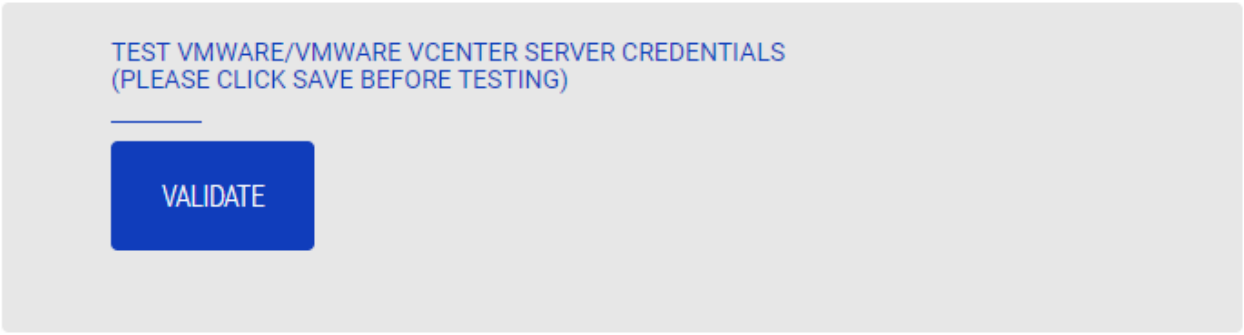
SAVE

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



Testing the configuration

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

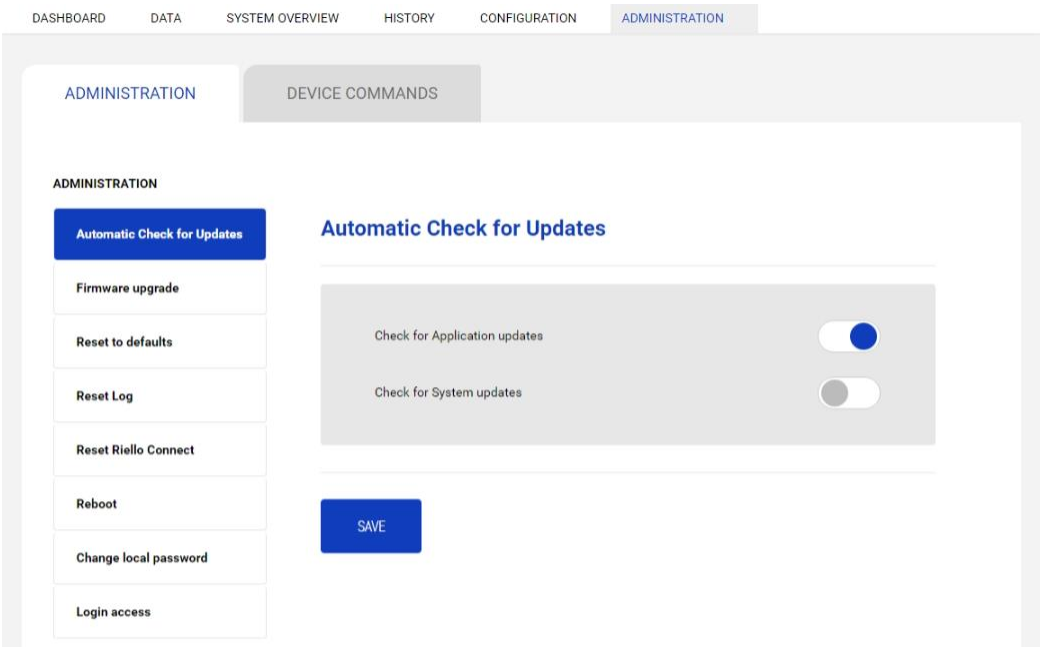


Validating the connections

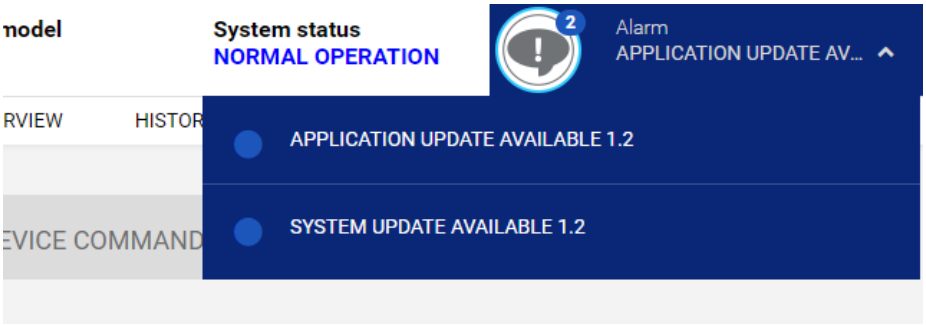
It is also possible to test the correct user account and password to login on the VSphere VCSA. The test will return the result with a pop-up screen.

ADMINISTRATION

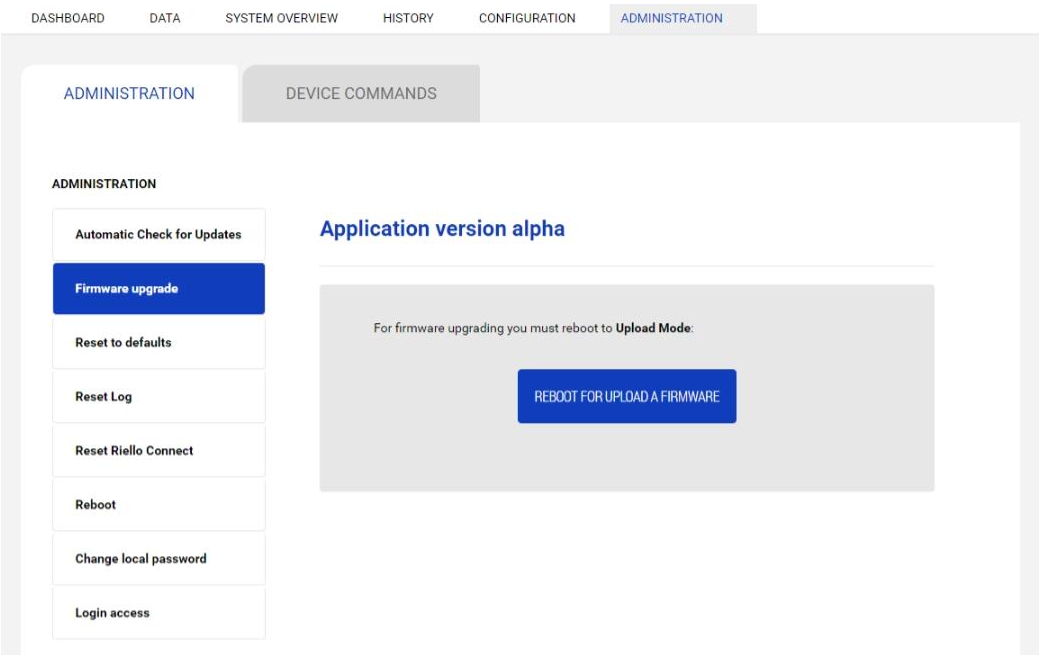
Automatic Check for Updates



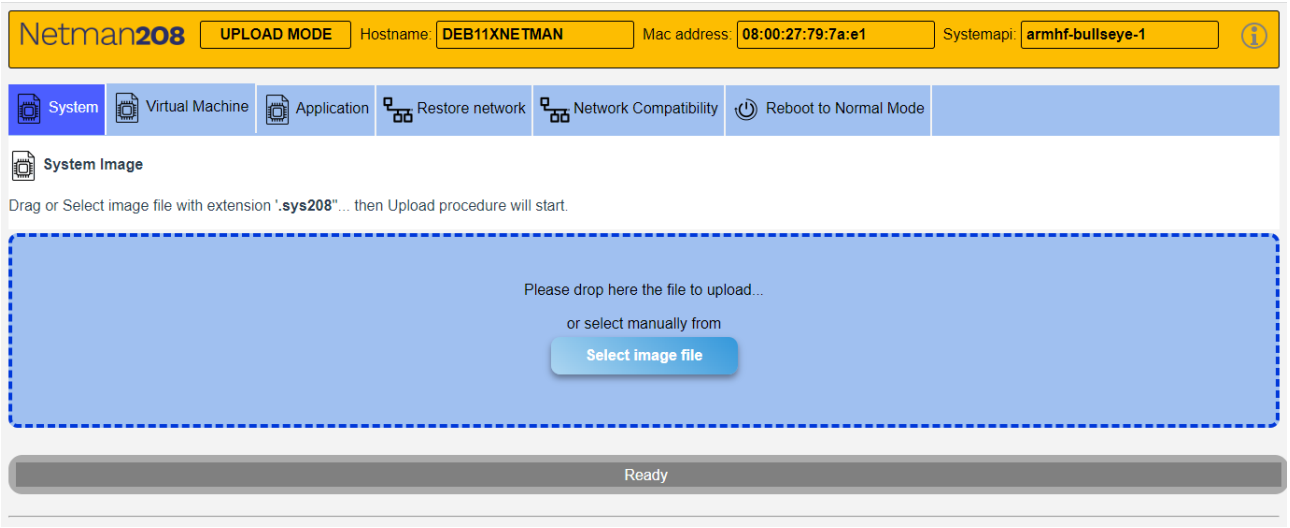
Netman 208 automatically checks for updates available on the official server ONLINE. It is possible to check only for Application updates, for System updates or both.
When an update is available, it is shown in the “Alarm” area.



Firmware upgrade



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



From here it is possible to:

- Upload the firmware (with "**System**", "**Virtual Machine**" and "**Application**" file images).

and, as operations:

- "**Restore Network**": restore the network configuration to the Default.
- "**Network Compatibility**": set special network settings (speed compatibility) for solving network problems.
- "**Reboot to Normal Mode**": reboot to Normal Mode.

Netman 208 has three firmware components:
- "**System**" component: the basic Operating System.
- "**Virtual Machine**" component: needed by "System" and "Application" components.
- "**Application**" component: what the User really use and interacts with (Web application.

The *Netman 208* receives more often updates for “Application” component and so the User has usually to update only one firmware. However, it is possible to update all three firmware.

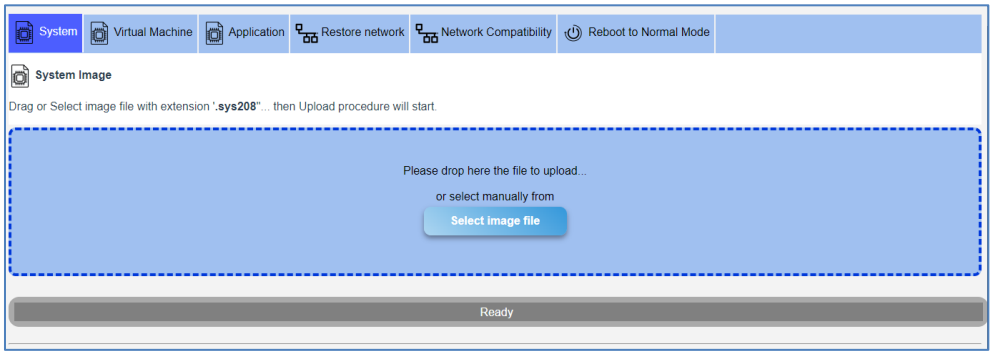
Every firmware component comes with 2 files and both files are needed for every single component upload:
- **Image** data file (FW108-vvrr.**app208** / FW107-vvrr.**jvm208** / FW109-vvrr.**sys208**)
- **JSON** file with **checksum** (FWxyz-vvrr-**JSON.json**)

System	**FW109-vvrr.sys208** **FW109-vvrr-JSON.json**
Virtual Machine	**FW107-vvrr.jvm208** **FW107-vvrr-JSON.json**
Application	**FW108-vvrr.app208** **FW108-vvrr-JSON.json**

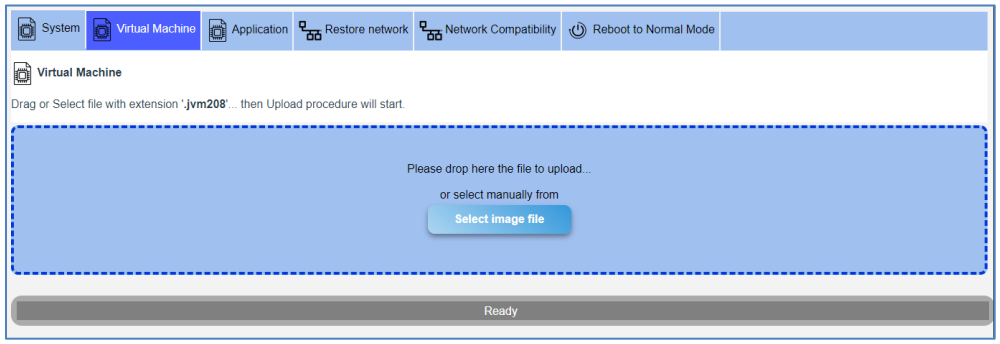
Uploading image files involves the reading and the transmission of huge data, therefore is strongly suggested to not loading the image file from the network / local network but to copy locally the image files on the computer

Every firmware component must be loaded from their specific tab:

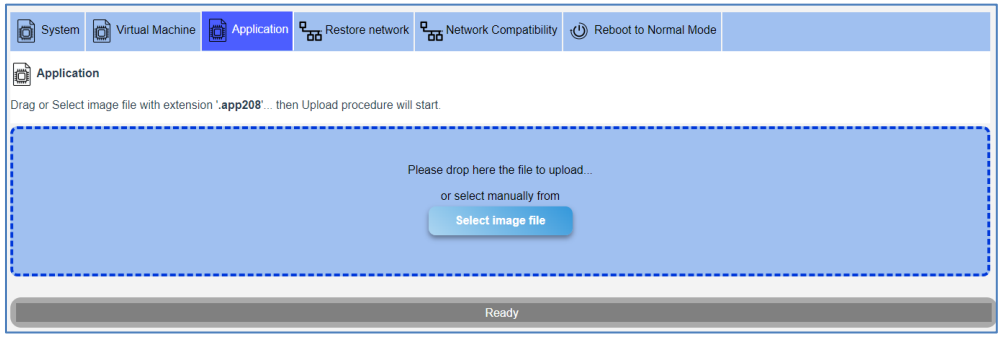
System



Virtual Machine



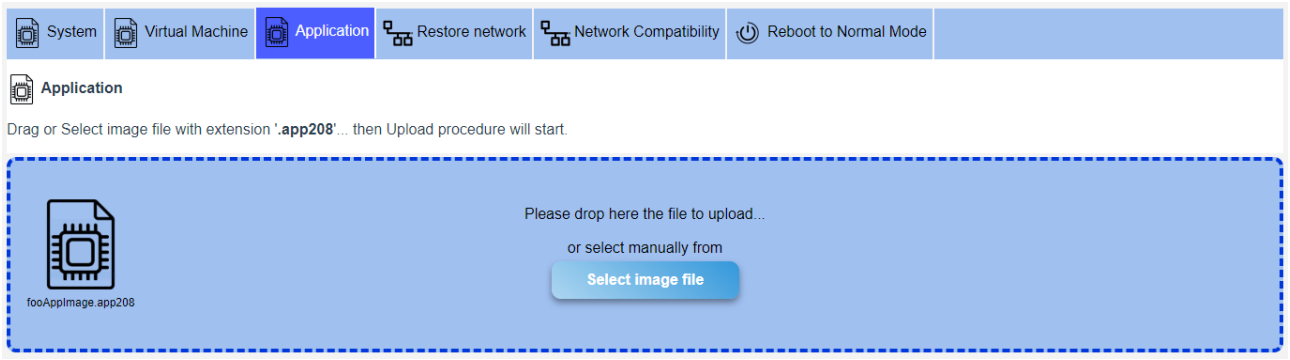
Application



Upload process is similar for “System”, “Virtual Machine” and “Application”.

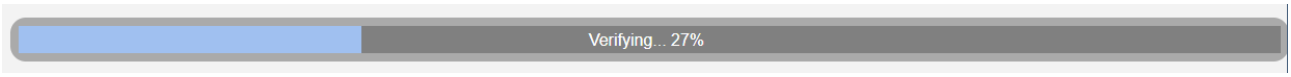
For example, for “Application” you have to go through the following stages:

1) Select the image file.

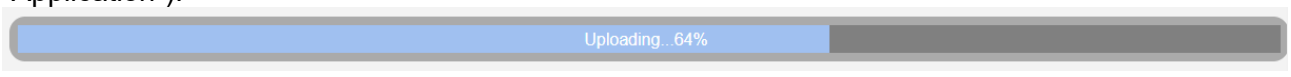


2) Select the json checksum file.

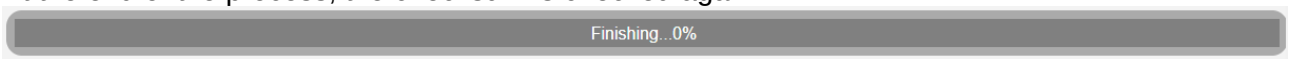
3) After upload the Checksum file, in case of no error, the Web page proceeds to calculate the Checksum of the file.



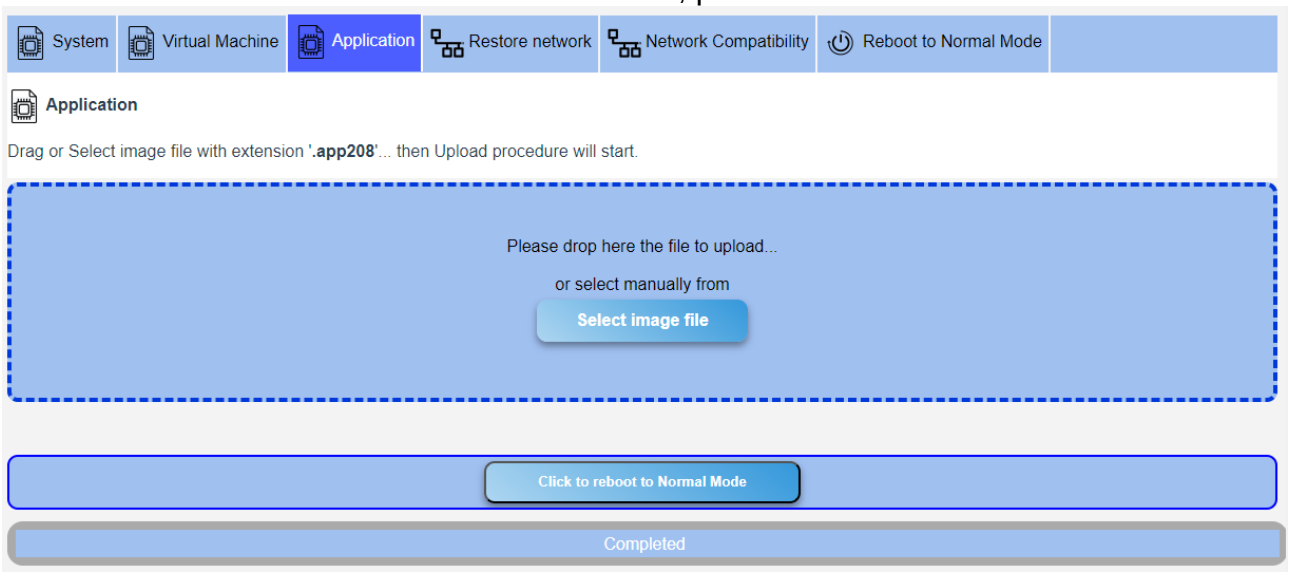
4) Checksum calculated is compared to the checksum loaded from JSON file: if it matches proceeds to upload the Image file overwriting existing image in the *Netman 208* (e.g. old “Application”).



5) At the end of the process, the checksum is checked again.

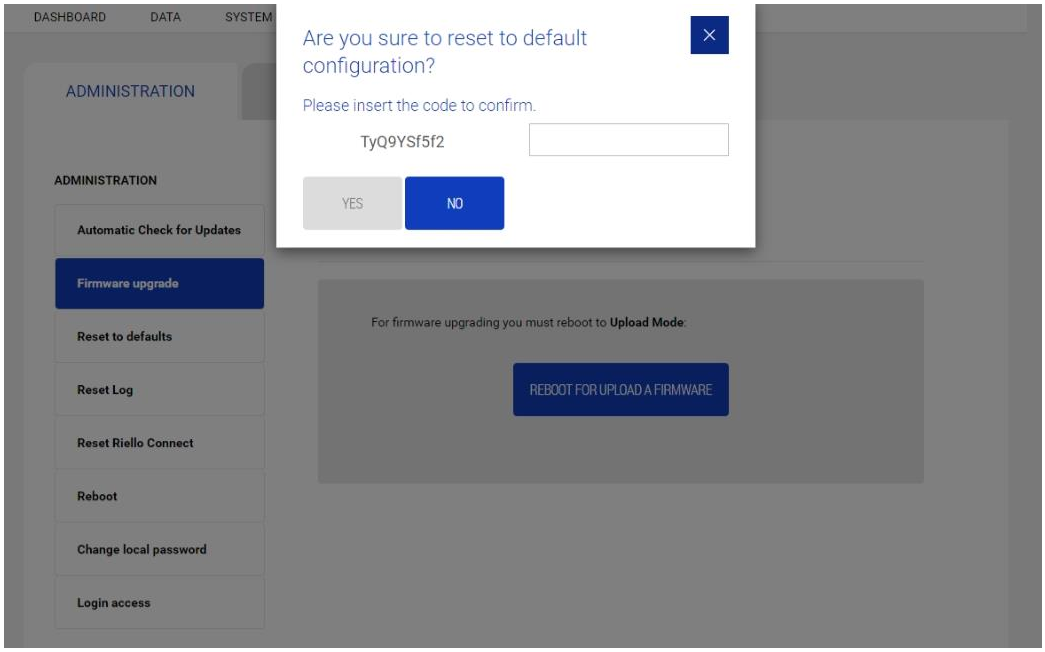


6) If checksum calculated matches the correct one, process confirm with success.



7) At the end, you must reboot the *Netman 208* to Normal Mode

Reset to defaults



By inserting the security code, the *Netman 208* will reset to the default configuration.

Operation strongly suggested in case of decommissioning the *Netman 208*.

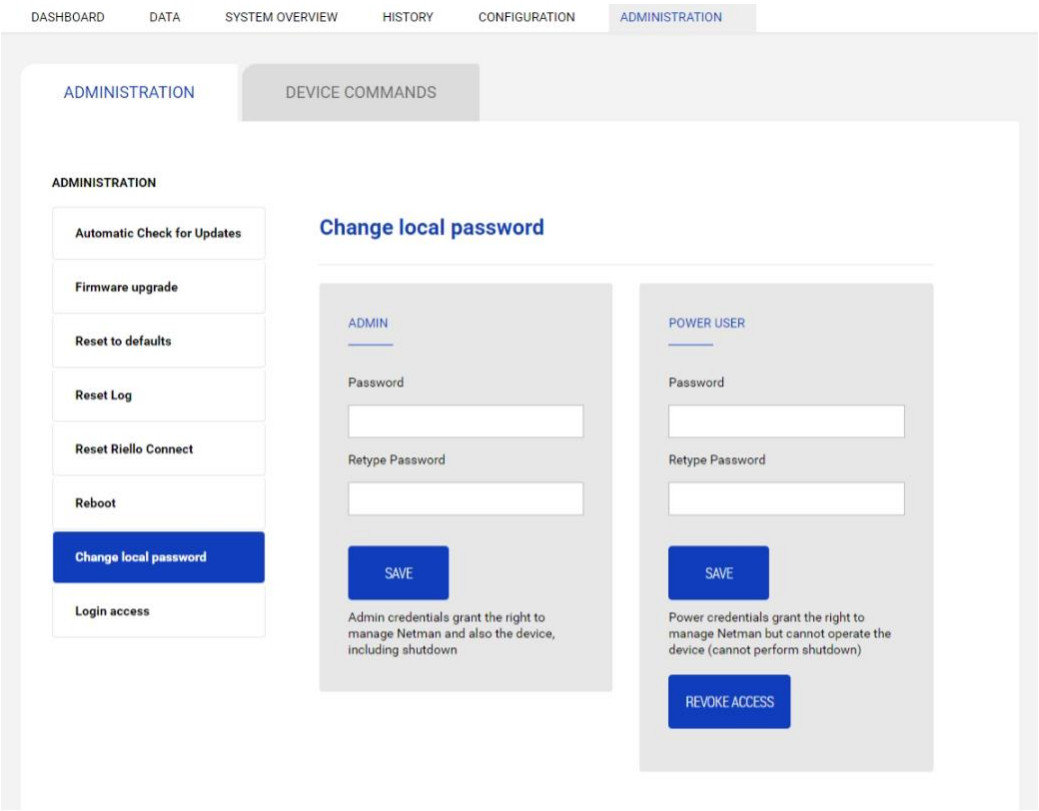
Reset Log

To reset all the log files of *Netman 208.*

Reboot

To reboot the *Netman 208.*

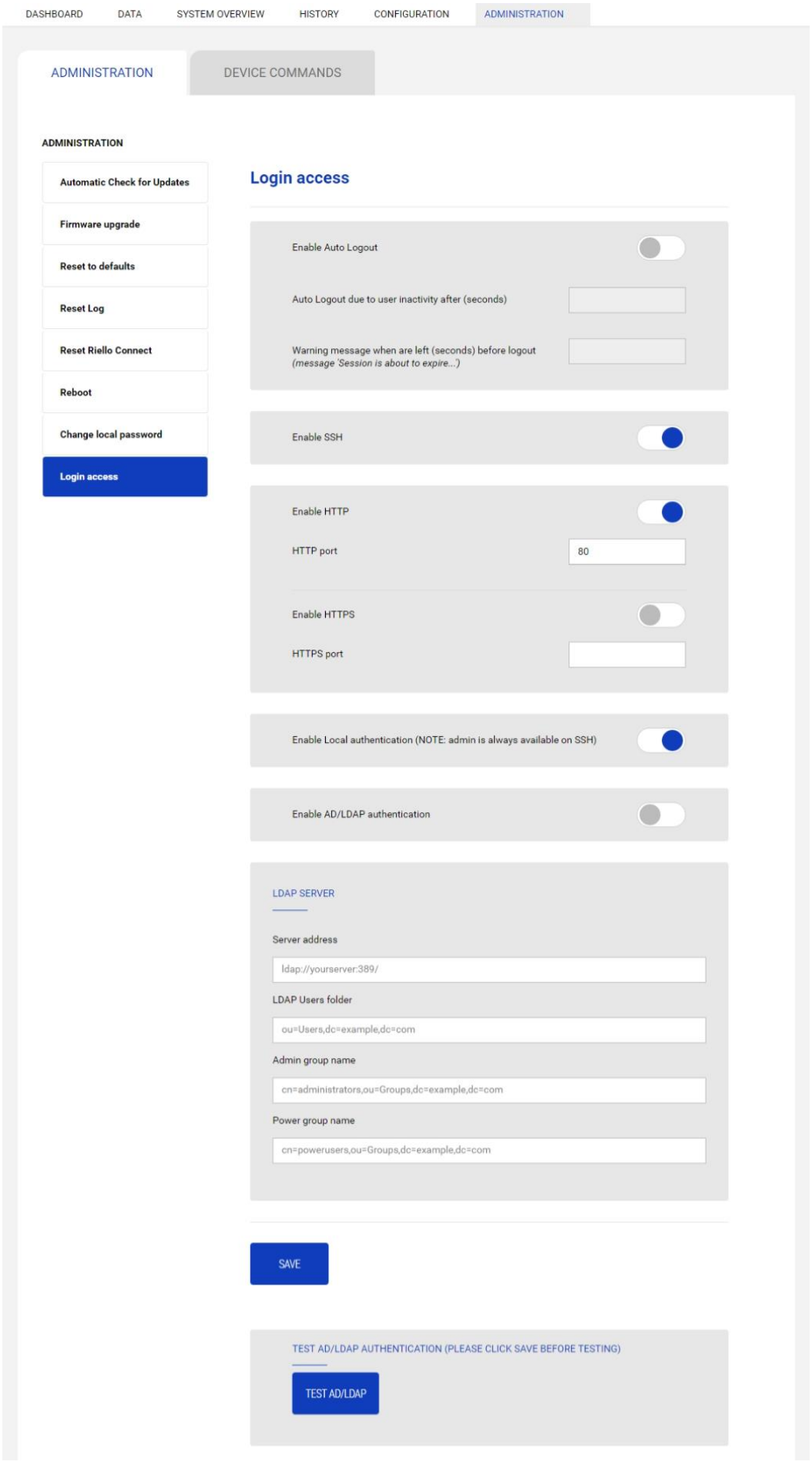
Change local password



To change “Admin” and “Power User” password.

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

Login access



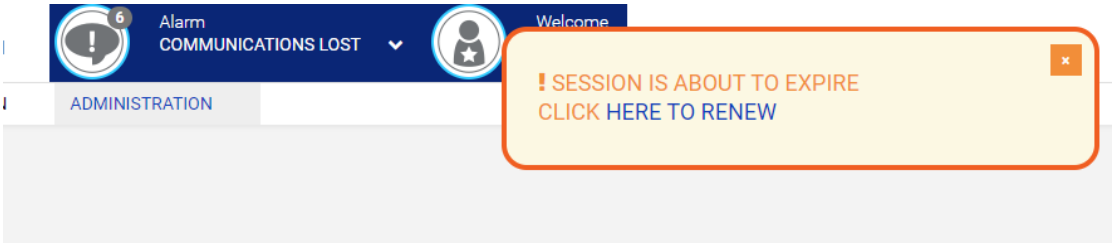
Field	Description
Enable Auto Logout	To enable Auto Logout
Auto Logout due to user inactivity after (seconds)	After this inactivity time (no mouse clicks) *Netman 208* logout losing any unsaved configuration made
Warning message when are left (seconds) before logout	When inactivity time left is less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

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

Procedure allows to set:

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

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



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

Auto Logout ignores any unsaved change in the configuration.

Field	Description
Enable SSH	To enable login over SSH
Enable HTTP	To enable the HTTP service
HTTP port	Enter the port where HTTP service is started (default: 80)
Enable HTTPS	To enable the HTTPS service
HTTPS port	Enter the port where HTTPS service is started (default: 443)
Enable local authentication	To enable local authentication

Field	Description
Enable LDAP/AD authentication	To enable 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

It is possible to manage the login via LDAP or Active Directory. 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).

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.

Specific example and how it works:

Considering these parameters:

Server address

ldap://10.1.10.150

LDAP Users folder

ou=ORGANIZATION,dc=example,dc=com

Admin group name

cn=sys.ups.sysadmins,ou=UPS,ou=SYS,ou=STRUCTURE_MANAGED,ou=ORGANIZATION,dc=example,dc=com

Power group name

cn=sys.ups.powerusers,ou=UPS,ou=SYS,ou=STRUCTURE_MANAGED,ou=ORGANIZATION,dc=example,dc=com

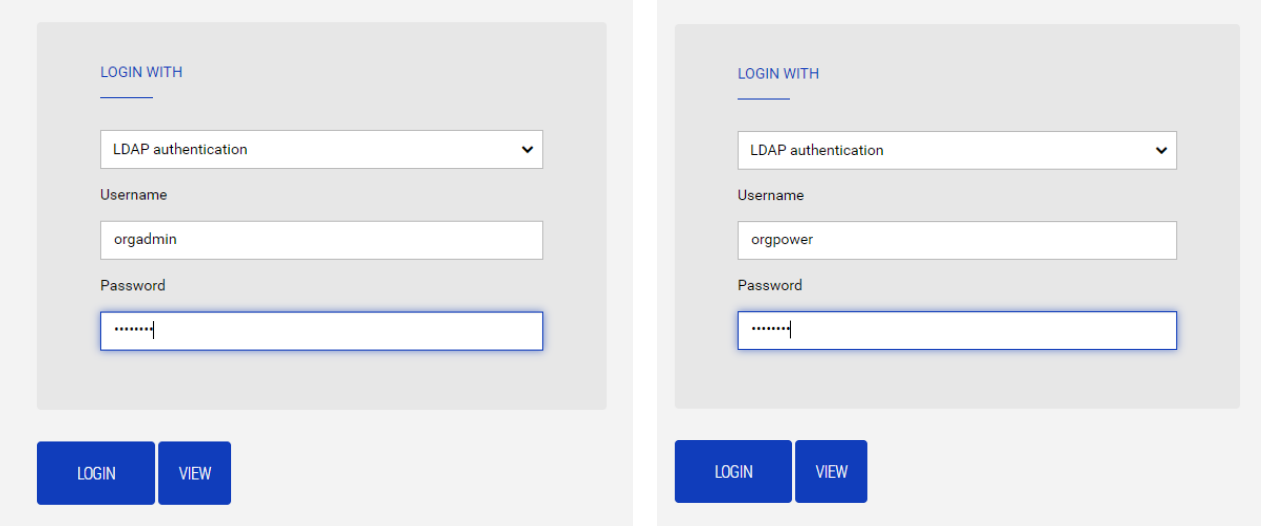
The given LDAP Server allows to access following credentials:

Username: **orgadmin** / Password: **orgadmin** (member of “**Admin**” grop)

Username: **orgpower** / Password: **orgpower** (member of “**Power**” group)

The action executed are:

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



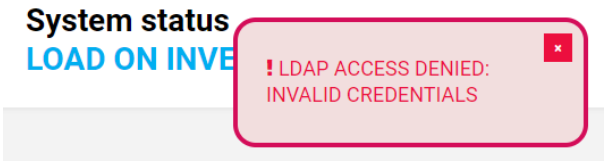
The *Netman 208* connects to host '**ldap://10.1.10.150**' as **LDAP**.
Authentication is checked binding with username '**CN=USERNAME_REQUESTING_LOGIN,ou=ORGANIZATION,dc=example,dc=com**' and password '**PASSWORD_REQUESTING_LOGIN**' with correct credentials.
Once connected, user must have rights to operate searches in the LDAP tree (as the 'Simple authentication method' in LDAP standard).

Checking if user '**USERNAME_REQUESTING_LOGIN**' belongs to Admin group '**cn=sys.ups.sysadmins,ou=UPS,ou=SYS,ou=STRUCTURE_MANAGED,ou=ORGANIZATION,dc=example,dc=com**':
At first get all the attributes of group '**cn=sys.ups.sysadmins,ou=UPS,ou=SYS,ou=STRUCTURE_MANAGED,ou=ORGANIZATION,dc=example,dc=com**',
then tries to read the attribute '**memberUid**': if it is found then Server is recognised as '**LDAP**' and user '**USERNAME_REQUESTING_LOGIN**' is searched in the list of the '**memberUid**' of the group.
Otherwise tries to read the attribute '**member**': if it is found then Server is recognised as '**Active Dirctory**' and username '**USERNAME_REQUESTING_LOGIN**' is searched in the list of the '**member**' of the group.
If user '**USERNAME_REQUESTING_LOGIN**' is found it gains **'Admin'** rights in the *Netman 208* and search ends with success.

(If not found) checking if user '**#USERNAME#**' belongs to Power group '**cn=sys.ups.powerusers,ou=UPS,ou=SYS,ou=STRUCTURE_MANAGED,ou=ORGANIZATION,dc=example,dc=com**':
At first get all the attributes of group '**cn=sys.ups.sysadmins,ou=UPS,ou=SYS,ou=STRUCTURE_MANAGED,ou=ORGANIZATION,dc=example,dc=com**',
then tries to read the attribute '**memberUid**': if it is found then Server is recognised as '**LDAP**' and username '**USERNAME_REQUESTING_LOGIN**' is searched in the list of the '**memberUid**' of the group.

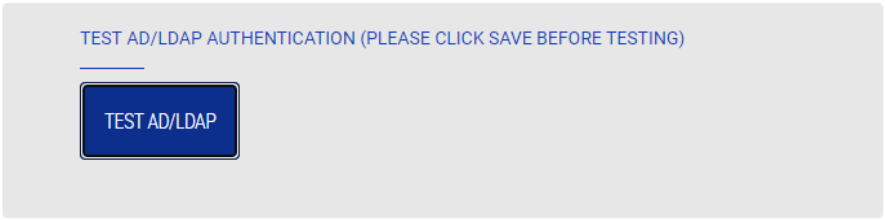
Otherwise tries to read the attribute '**member**': if it is found then Server is recognised as '**Active Dirctory**' and username '**USERNAME_REQUESTING_LOGIN**' is searched in the list of the '**member**' of the group.
If user '**USERNAME_REQUESTING_LOGIN**' is found it gains **'Power'** rights in the *Netman 208* and search ends with success.

If user is not found neither in Admin neither in Power group, procedure ends signaling '**No user found**'.

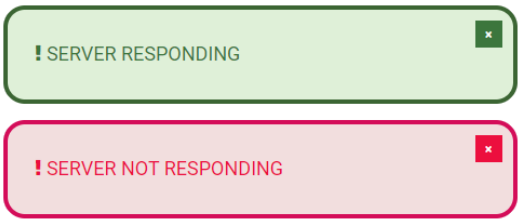


Test connection

It is possible check the connection to the Server:



checking the simple connection to the server, without any authentication.
The result is a message of success or error:

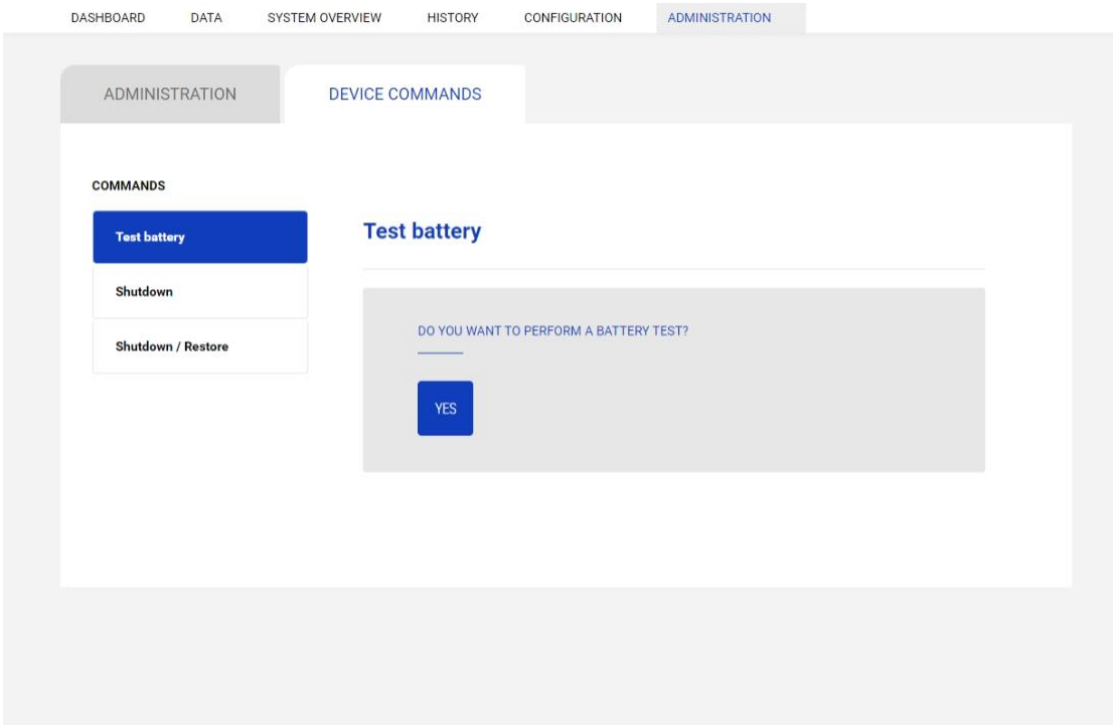


"Simple" Method Authentication: Authentication used by the *Netman 208* follows the "Simple" Method Authentication of LDAP where the User logging (with Username and Password) is able to check its membership to the groups.

Active Directory user's attribute: in case of Active Directory, login session can accept both "displayName" and "User logon Name" attributes of the Windows server in the User attributes.

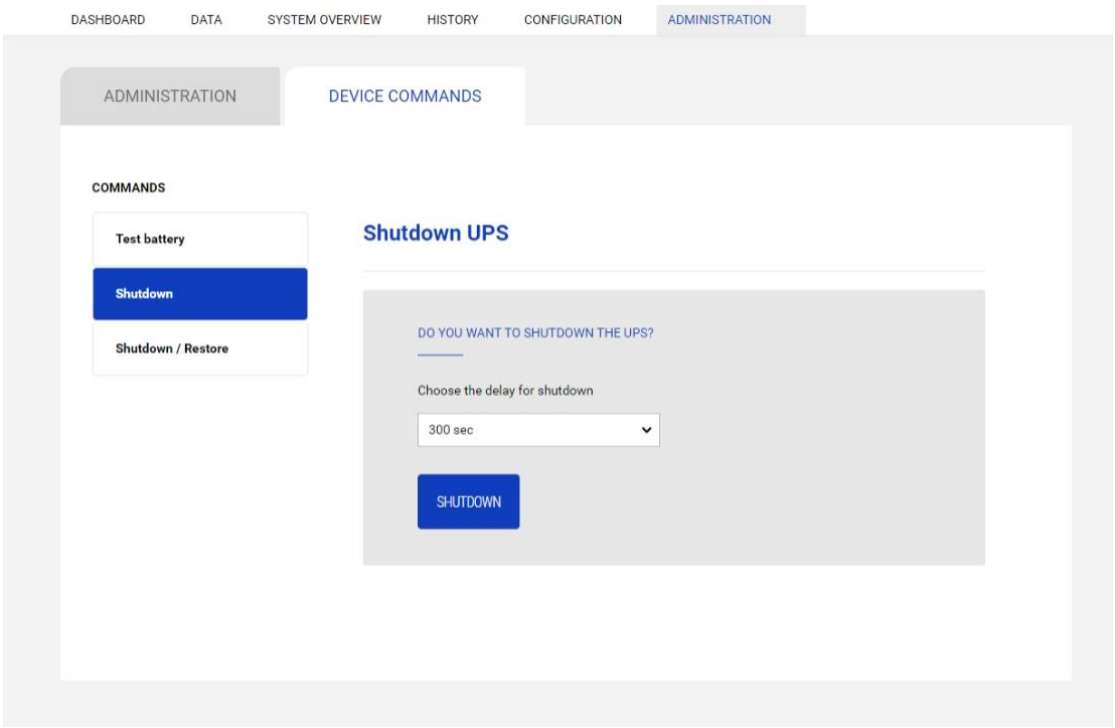
COMMANDS

Test battery



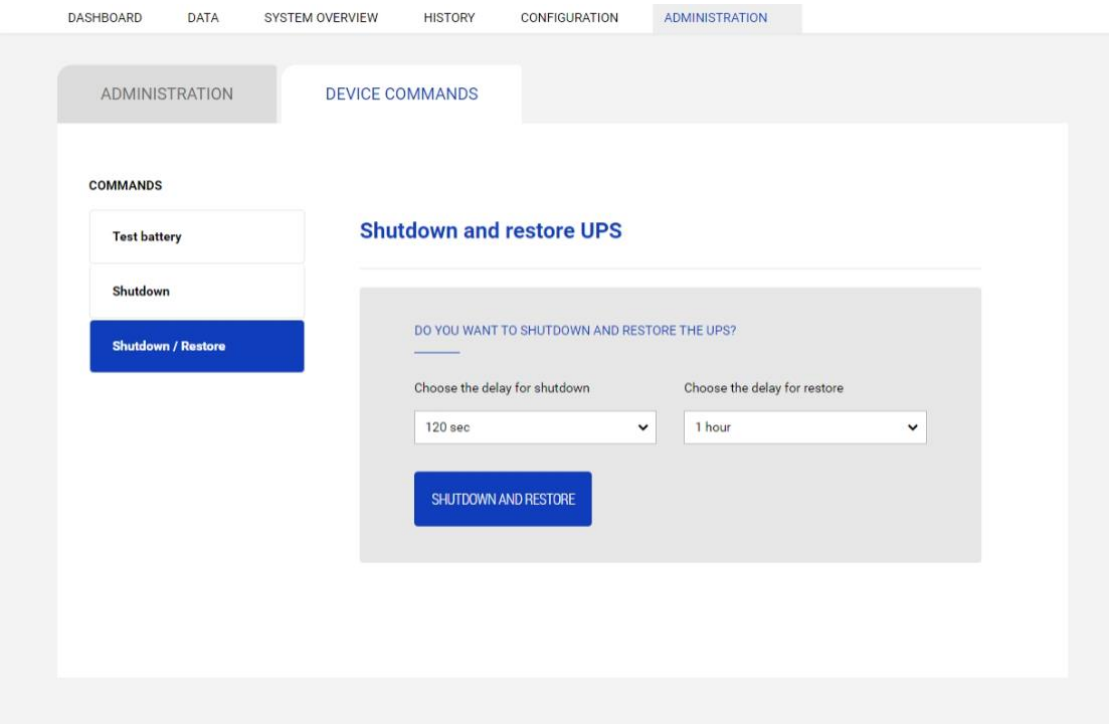
To execute a test of the batteries.

Shutdown



To execute a shutdown of the device.

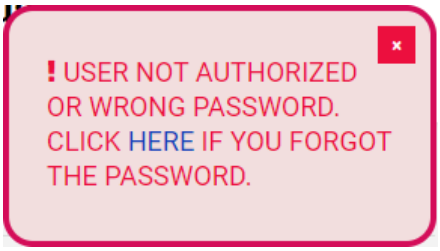
Shutdown / Restore



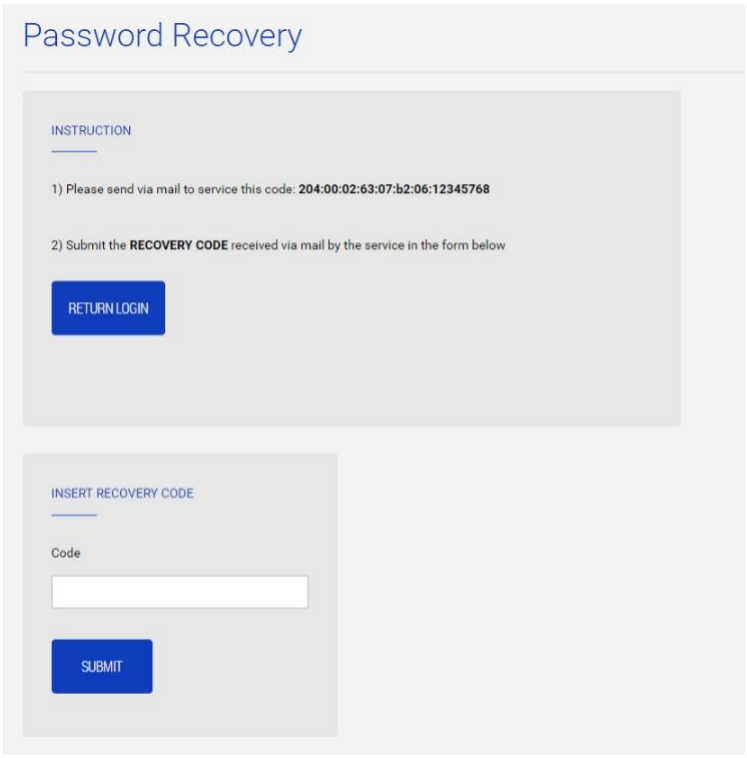
To execute a shutdown and restore of the device.

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 208*.
If you insert an incorrect password, you are offered a link to a password recovery. Click the link to start the recovery.



A window like the following will be shown:



Please note that the unlock key is valid only for the corresponding service code which is specific for every *Netman 208*.

CONFIGURATION VIA SSH

Netman 208 is provided by default with the SSH disabled. The SSH client service can be enabled/disabled only via http.

To configure *Netman 208* via SSH it is necessary to:

- Execute a SSH client on a PC connected in a network to *Netman 208* 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").

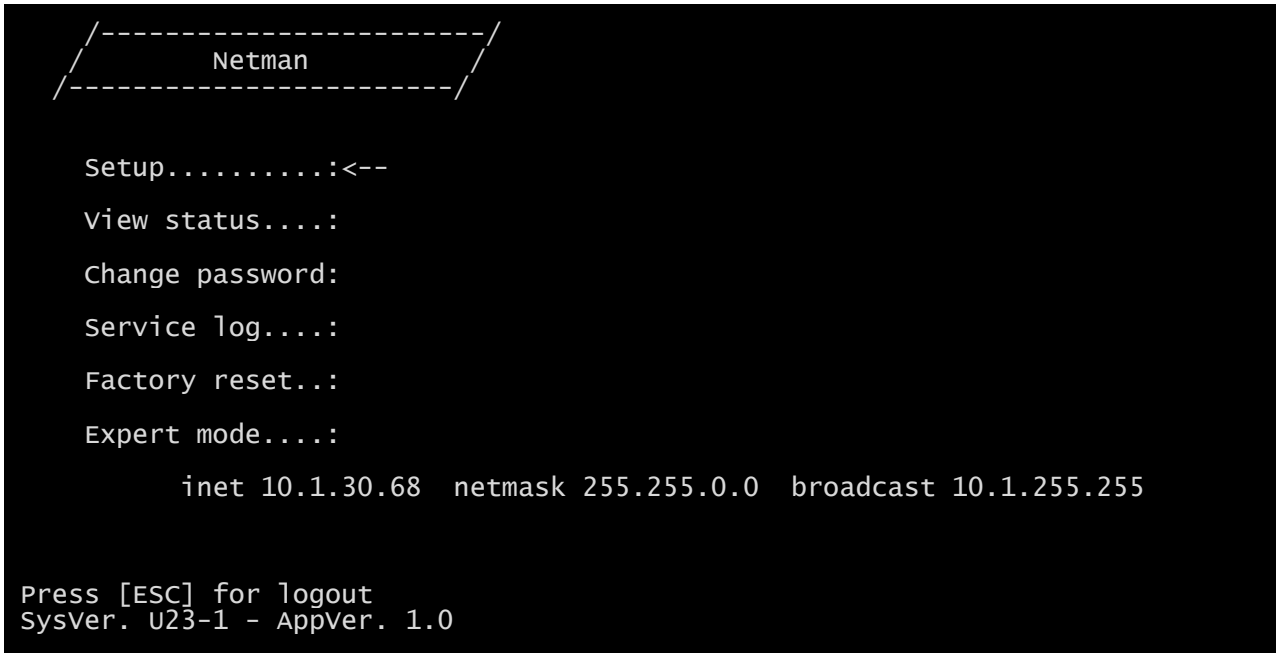
During password’s typing, no character is shown.

For proper configuration of *Netman 208*, 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 208* settings.

Main menu

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



Function	Description
Setup	To enter IP configuration menu
View status	To see the status of the device
Change password	To modify the password
Service log	To generate a log file of the card (when requested by the service)
Factory reset	To restore factory configuration
Expert mode	To enter Expert mode (more information at paragraph “*Expert mode*”)

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.

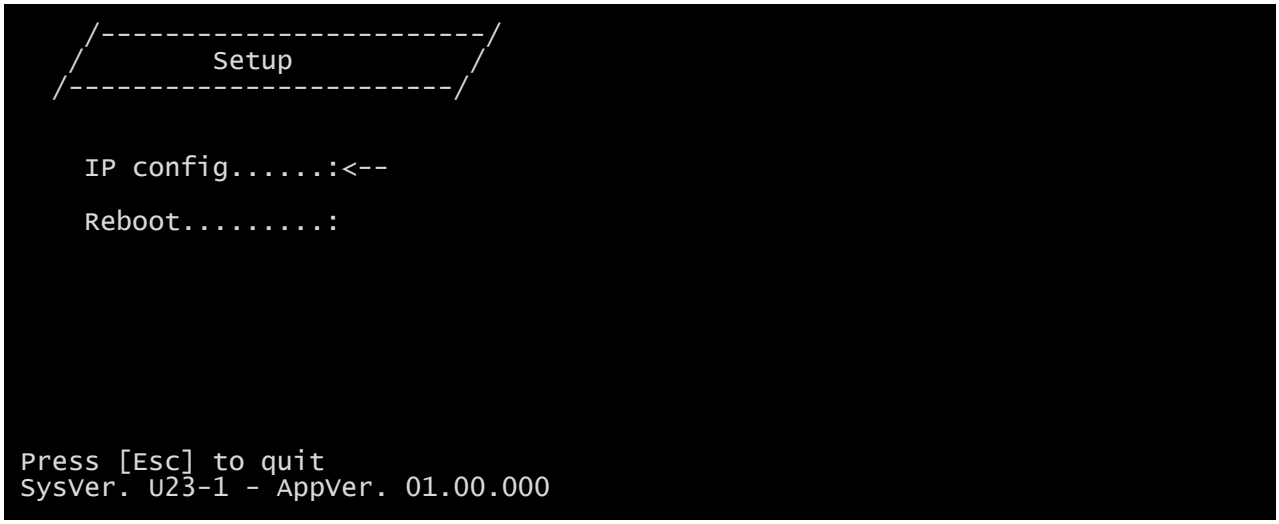
Key	Function
Direction keys (Arrow up, down, right, left)	To move the cursor within the menus
Tab	Goes on to next option
Enter [1]	Choice of submenu
	Confirmation of characters entered
Esc [1]	Exit main menu [2]
	Return to previous menu

[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:



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
Expert mode	To enter Expert mode (more information at paragraph “*Expert mode*”)
Reboot	Reboots the *Netman 208*

IP config

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

Field	Parameters to be inserted
Hostname	Enter the *Netman 208* 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.

Expert mode

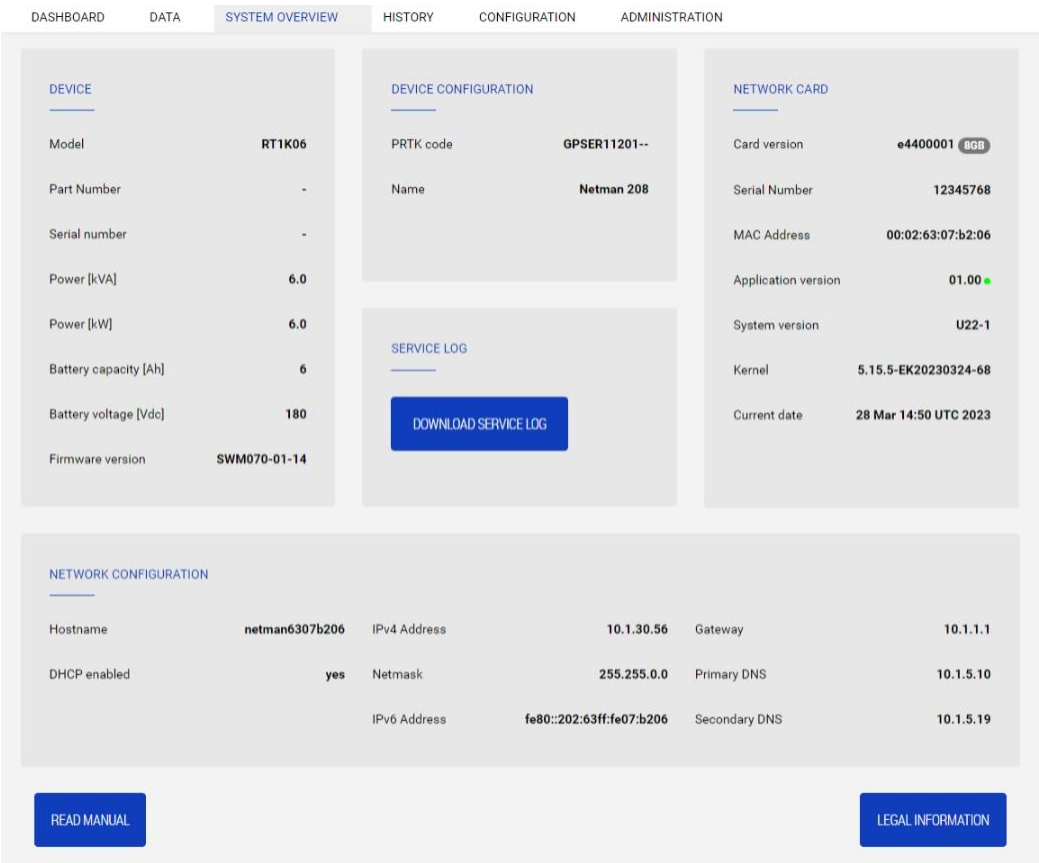
Expert mode enables the configuration of advanced parameters that should be set by skilled technicians. These commands are supported:

`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 *Netman 208*
`clearlog`	clear data log and event log
`exit`	closes the connection

CONFIGURATION OF SEVERAL DEVICES

If several *NetMan 208* have to be configured with similar parameters, you can configure the first *NetMan 208*, 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



In case of problem or if *Netman 208* 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 centre to properly diagnose the problem.

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, in the FTP folder `/cfg/`, with user "`admin`" (default password: "`admin`").
Each line of the file is parsed by *NetMan 208* and must begin with one of these keywords:

- *#*: for comment, the line is skipped.
- *addUser*: for adding a new user and setting the passwords
- *addGroup*: for putting a user into a group
- *addAccessEntry*: for enabling access privileges to a group
- *addView*: for adding privileges
- *addManager*: for adding SNMP Manager which will receive SNMP traps.

The correct syntax for addUser is:

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

<userName> is the name of the user.
<authProtocol> is the protocol for authentication of this user during SNMP sessions. Possible values are:

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

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

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

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

The correct syntax for addGroup is:

addGroup <securityModel> <userName> <groupName>

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

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

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

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

The correct syntax for addAccessEntry is:

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

<groupName> is the name of the group to which this access right applies, must match one of the group name defined with addGroup.
<contextName> is the name of the context.
<securityModel> is the security model that must be used in order to gain access to this access right, must match the security model defined with addGroup.
<securityType> is the minimum security level that must be used to gain access to this access right. Possible values are:

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

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

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

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

The correct syntax for addView is:

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

<viewName> is the name of the view.
<subtree> is the OID subtree which when combined with the corresponding instance of MASK defines a family of view subtrees.
<mask> the mask for filtering OID.
<included> the OID can be included or excluded. Possible values are:

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

The correct syntax for addManager is:

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

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

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

<ipAddress> is the IP address of the SNMP manager.
<credentials> is either the username (when using USM security) or the trap community (when using v1 security)
<securityType> is either:

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

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

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

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

Trap explanation:

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

MODBUS TCP/IP PROTOCOL

This service is active on the TCP port 502.
Below are the basic Modbus tables reporting main alarms and measurements compatible with all devices. For more information about alarms and measurements available on your device, refer to the specific extended Modbus table of the product family that can be downloaded from the manufacturer's website.

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

REGISTER [1]		STATES/ALARMS		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
				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
2	1			17	16
				…	…
				28	27
		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	32
				…	…
				48	47
4	3			49	48
				…	…
				63	62
		Communication lost with UPS	[0=NO / 1=YES]	64	63

[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]		MEASUREMENTS	UNIT
Number	Address		
9	8		
10	9		
11	10		
12	11	Input voltage (Ph-N) V1	V
13	12	Input voltage (Ph-N) V2	V
14	13	Input voltage (Ph-N) V3	V
15	14		
16	15		
17	16		
18	17	Input frequency	Hz/10
19	18		
20	19		
21	20		
22	21	Bypass voltage (Ph-N) V1	V
23	22	Bypass voltage (Ph-N) V2	V
24	23	Bypass voltage (Ph-N) V3	V
25	24	Bypass frequency	Hz/10
26	25	Output voltage (Ph-N) V1	V
27	26	Output voltage (Ph-N) V2	V
28	27	Output voltage (Ph-N) V3	V
29	28		
…	…		
37	36		
38	37	Load phase L1	%
39	38	Load phase L2	%
40	39	Load phase L3	%
41	40		
42	41		
43	42		
44	43	Output frequency	Hz/10
45	44		
46	45		
47	46		
48	47	Battery voltage	V/10
49	48		
50	49		
51	50		
52	51	Charge%	%
53	52		
54	53	Autonomy	Minutes
55	54		
…	…		
61	60		
62	61	Internal UPS temperature	°C
63	62		
…	…		
72	71		

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

For single-phase systems, the value 0xFFFF is reported in the registers relating to L2 and L3.

REGISTER [1]		NOMINAL DATA	UNIT
Number	Address		
73	72		
…	…		
77	76		
78	77	Output nominal voltage	V
79	78	Output nominal frequency	Hz/10
80	79	Output nominal power	kVA/10
81	80	Output nominal power	kW/10
82	81		
83	82		
84	83	Battery nominal capacity (battery expansion included)	Ah
85	84	Battery benches	(1 or 2)
86	85		
…	…		
112	111		

REGISTER [1]		COMMANDS	UNIT
Number	Address		
113	112	Command Code: 1 (0x0001) UPS Shutdown (see also register 114) 2 (0x0002) UPS Shutdown & Restore (see also register 114/115) 3 (0x0003) Delete Command (code 1 – 2) 20 (0x0014) Test Battery	Integer
114	113	Shutdown delay time	Seconds
115	114	Restore delay time	Minutes
116	115	RESERVED	
117	116	Command result: = Command code if command is handled from the UPS = Command code + 100 if command is NOT handled from the UPS = 0 if Command code is wrong	Integer
118	117	RESERVED	

[1] *The register number **n** must be addressed **n-1** in the data packet.*

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	

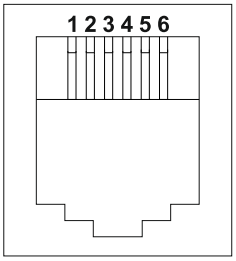
EVENTLOG CODES

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	Temerature high sensor 1
TMIN1	Temperature low sensor 1
Input1	Input contact sensor 1
Hum1	Humidity high sensor 1

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

TECHNICAL DATA

SERIAL PORT PINOUT

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

Netman 208			**Modem**		
RJ-12			**DB-25**	**DB-9**	**DESCRIPTION**
POSITION	**DESCRIPTION**		**POSITION**	**POSITION**	
1	$+5V_{DC}$	**LEAVE UNCONNECTED**			
2	GND	**← CONNECT TO →**	7	5	GND
3	RS232 TXD	**← CONNECT TO →**	2	3	RXD
4	RS232 RXD	**← CONNECT TO →**	3	2	TXD
5	RS485 A	**LEAVE UNCONNECTED**			
6	RS485 B				

NETWORK CABLE

To connect the device to the Ethernet (10Base-T) 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 208* includes some open-source components. For more information, please visit the website of the manufacturer.

The warranty for *Netman 208* firmware it is relative to the correct use to which the product has been sold.
Manufacturer warrants during the warranty period that the firmware will function materially as described in the accompanying user documentation when given normal, proper, and intended usage.

This product uses the GNU/Debian operating system.

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

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

This product includes SNMP++ software.

This product includes AGENT++ software.

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

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

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

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

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

This product includes a modified Qt library under the terms of the GNU LGPLv3.

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

This product includes DOM4J.

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

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

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

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

This product includes YAVI Java.

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

This product includes Apache MINA SSHD.

This product includes SQLite JDBC.

This product includes JSON.

This product includes Bouncy Castle Crypto APIs.

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

This product includes ORMLite.

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

This product includes JAXB API.

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

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

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

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

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

This product includes Java Hamcrest.

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

This product includes MD5sum Calc from crypto-js.

This product includes FastCGI Application Library. This product includes Roboto font. This product includes Font Awesome font.

This product includes IcoMoon.

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

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

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

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

This product includes jQuery Validation Plugin under the terms of the MIT license.

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

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

This product includes Bootstrap Notify under the terms of the MIT license.

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

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

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

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