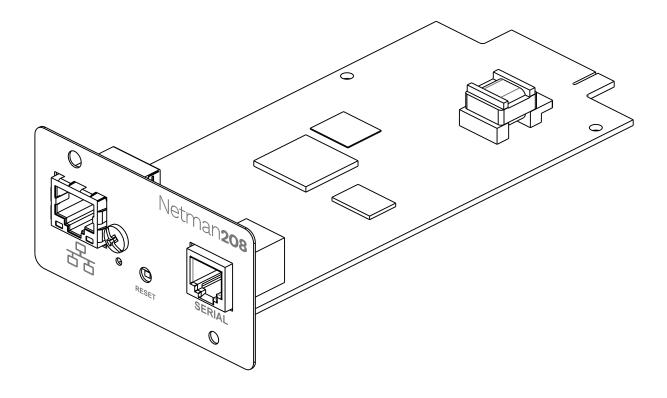
# Netman208



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:

WarningIndicates important information that must not be ignored.InformationProvides notes and useful suggestions for the User.

## SAFETY

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

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

## ENVIRONMENTAL PROTECTION

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

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

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

## DISPOSING OF THE PRODUCT

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

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

## CONTENTS

DESCRIPTION	8
Overview	
PACKAGE CONTENTS	
FRONT PANEL	
Network port	
Reset button	
Serial port	
Status led	
Users	10
Network services	11
SSH	
Serial network	
Wake-on-LAN	
НТТР	
SNMP	11
UDP	11
Modbus TCP/IP	11
BACnet/IP	12
FTP	
Syslog	
Email	
Reports	
SSH Client	
Device values and events history log archive	13
Eventlog	13
Datalog (only for UPS devices)	13
INSTALLATION	14
CONFIGURATION	15
Login	16
Dashboard	17
Device	18
General configuration	
Command configuration	
Data log configuration	
Network	21
Configuration	

Firewall	24
Wake-on-LAN	
SNMP	30
MODBUS/BACNET	33
JSON	34
Syslog	38
DATE & TIME	39
NTP & Timezone	39
Configuration	40
Emails	41
Configuration	41
GSM MODEM	43
Configuration	43
Remote hosts	45
SSH	45
VMware ESXi	49
Nutanix	54
Syneto	58
ADMINISTRATION	67
Automatic Check for Updates	
Firmware upgrade	
Reset to defaults	
Reset Log	
Reboot	79
Change local password	
Login access	74
Commands	79
Test battery	79
Shutdown	
Shutdown / Restore	80
PASSWORD RECOVERY	81
CONFIGURATION VIA SSH	82
Main menu	83
Setup	
IP config	
Expert mode	
CONFIGURATION OF SEVERAL DEVICES	88
SERVICE LOG	89

SNMP CONFIGURATION	90
MODBUS TCP/IP PROTOCOL	93
BACNET/IP CONFIGURATION	96
EVENTLOG CODES	98
TECHNICAL DATA	100
SERIAL PORT PINOUT	100
NETWORK CABLE	101
OPERATING AND STORAGE CONDITIONS	101
LEGAL INFORMATION	102

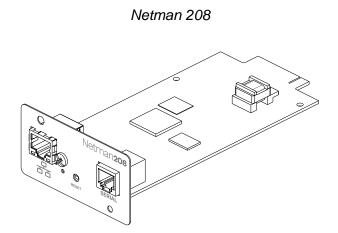
## DESCRIPTION

#### **O**VERVIEW

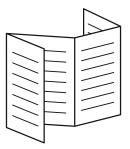
*Netman 208* is an accessory that allows device management through a LAN (Local Area Network); the accessory supports all the main network protocols (SNMP v1, v2 and v3, TCP/IP, HTTP and MODBUS) and is compatible with Ethernet 10/100/1000 Mbps IPv4/6 networks. The device can therefore be integrated easily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

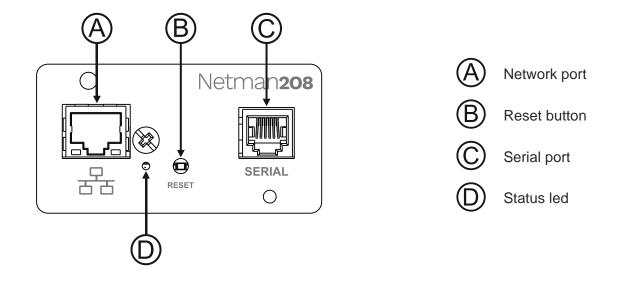
Netman 208 also records device values and events in the history log archive and can manage optional environmental sensors (not supplied with the device but provided separately).

#### PACKAGE CONTENTS



Quick start





#### **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 <sup>(2)</sup>	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.

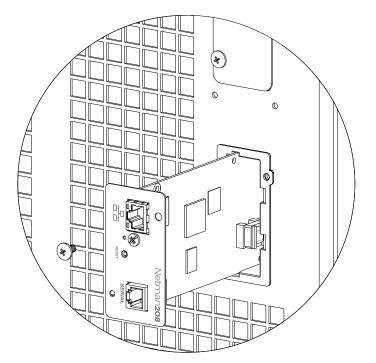
This service writes a record each hour at 00 minutes, which summarizes the data of the past hour: values are recorded at their minimum, maximum and medium. Records older than one year get overwritten with new records.

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	ΥY	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 <u>http://netman6308031f.local</u> 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.

Welcome	
	LOGIN WITH LOCAL AUTHENTICATION Username Password
	LOGIN VIEW



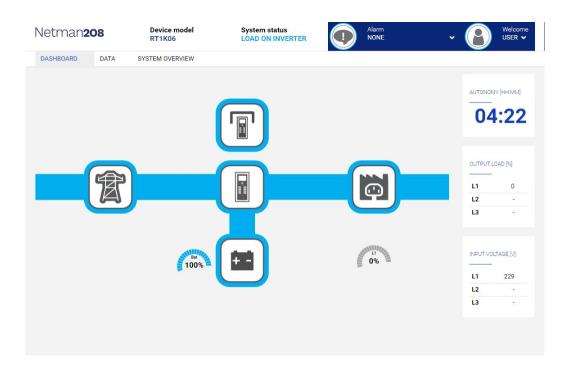
The login password can contain alphanumeric characters and these special characters only: , .\_+:@%/-. No other characters are allowed to avoid malicious script injections.

- 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").

Welcome	
	LOGIN WITH
	LDAP authentication
	Username
	Password
	LOGIN VIEW

#### 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**

DASHBOARD	DATA	SYSTEM OVERVIEW	HISTORY	CONFIGURATION	ADMINISTRATION	
YOUR NET	MAN	MODEM	REMOT	TE HOSTS		
DEVICE		_				
General cor	nfiguration	Gene	ral device	configuration		
Command	configuration					
Data Log co	onfiguration		DEVICE CONFIG	URATION		
NETWORK			PRTK Code GPSER11201	. <b>.</b>	Name Netman 208	
Configurati	on					
Firewall			Part Number P/N			
Wake on LA	AN .		Serial Number 5/	'N		
SNMP			SYSTEM ADMIN	DATA		
MODBUS/B	ACNET		Contact			
RIELLO CO	NNECT		Location			
JSON						
SYSLOG			Battery replacem	nent notification		
DATE & TIME			dd/mm/yyyy			
NTP & Time	ezone					
Configurati	on					
EMAILS		S	AVE			
Configurati	on					

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

DASHBOARD	DATA	SYSTEM OVERVIEW	HISTORY	CONFIGURATION	ADMINISTRATION	
YOUR NE	TMAN	MODEM	REMO	TE HOSTS		
DEVICE						
General c	onfiguration	Com	mand cont	figuration		
Command	l configuration					
Data Log	configuration		COMMAND  Disable remote a	shutdown		
NETWORK			Disable remote o			
Configura	tion					
Firewall						
Wake on I	AN	s	<b>WE</b>			
SNMP						
MODBUS/	BACNET					
RIELLO CO	DNNECT					
JSON						
SYSLOG						
DATE & TIME						
NTP & Tin	nezone					
Configura	tion					
EMAILS						
Configura	tion					

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

DASHBOARD	DATA	SYSTEM OVERVIEW	HISTORY	CONFIGURATION	ADMINISTRATION	
YOUR NET	MAN	MODEM	REMO	TE HOSTS		
DEVICE						
General co	nfiguration	Data	a Log config	guration		
Command	configuration					
Data Log c	onfiguration		DATA LOG			
NETWORK			Enable Data Log			
Configurat	ion					
Firewall			SAVE			
Wake on L	AN					
SNMP						
MODBUS/	BACNET					
RIELLO CO	NNECT					
JSON						
SYSLOG						
DATE & TIME						
NTP & Tim	ezone					
Configurat	ion					
EMAILS						
Configurat	ion					

Field	Description
Enable Data log	To enables the datalog service

## NETWORK

## Configuration

DASHBOARD	DATA	SYSTEM OVERVIEW	HISTORY	CONFIGURATION	ADMINISTRAT	ION		
YOUR NET	TMAN	MODEM	REMO	TE HOSTS				
DEVICE								
General co	onfiguration	Gen	eral Netwo	rk configuratio	n			
Command	configuration							
Data Log o	configuration		GENERIC NETW	ORK CONFIGURATION				
NETWORK			Hostname			Network pr Static IP	DHCP	
Configurat	tion		IPV4 CONFIGUR	ATION				
Firewall			IP Address					
Wake on L	AN		Please insert 1	the IP address				
SNMP			Netmask		Gateway			
MODBUS/	BACNET		Please insert 1 Primary DNS	the netmask	Please in Secondary	sert the gatewa	У	
RIELLO CO	ONNECT		Please insert 1	the primary DNS	Please in	sert the second	ary DNS	
JSON			IPV6 CONFIGUR	ATION				
SYSLOG			Enable IPv6		Disab	led.	Enabled	
DATE & TIME			Stateless	~	Privoov F	Extension	Enabled	
NTP & Tim	nezone				Prefix De	legation		
Configurat	tion				Accept R			
EMAILS					Advertise	ement		
Configurat	tion		Link-local addre	SS		fe80::202:63	ff:fe07:b206/64	
			Global Unique a	ddress			1	
							/	
							1	
			Gateway					
			DNS					

FTP		SERIAL NETWORK TUNNELIN	IG
Enable FTP protocol		Enable Serial tunneling	
UDP			
Enable UDP			
UDP port	33000		
UDP PASSWORD			
Password			
Password			
Retype Password			
Retype Password			
SAVE			

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 <sup>(1)</sup>
UDP Password	To change the password used for UDP/UPSMon communication

<sup>(1)</sup> This port must be the same as configured in the UPSMon software

## i

#### How to access the Netman via Hostname.

- → By default, the Hostname is built from MAC address e.g., from Netman MAC Address: 00:02:<u>63:05:00:37</u> → <u>http://netman63050037.local</u>
- → 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 <u>fe80::202:63ff:fe07:b205</u> → http://[fe80::202:63ff:fe07:b205]

#### Firewall

SHBOARD DATA	SYSTEM OVERVIEW HISTORY CONFIGURATION ADMINISTRATION	
YOUR NETMAN	MODEM REMOTE HOSTS	
DEVICE		
General configuration	Firewall configuration	
Command configuration		
Data Log configuration	FIREWALL	
NETWORK	Enable Firewall Rules	
Configuration	INCOMING Rules	
Firewall		
Wake on LAN	Enabled From IP IP From MAC Protocol address address address address	Port
SNMP	No data available in table	
MODBUS/BACNET	K A Add	, Row
RIELLO CONNECT	Default incoming rule: ACCEPT	
JSON		
SYSLOG	You must test the rules before confirm TEST	
DATE & TIME	Test temporarily the rules with immediate effect.	
NTP & Timezone	In case of problems due wrong rules, you can restart the Netman and last previous confirmed rules are rec so you can adjust rules again.	alled,
Configuration		
EMAILS	CONFIRM RULES	
Configuration	In case of correctness, you can confirm the tested rules and make them permanent and active from the next reboot.	
	CONFIRM	

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:

	Enabled	From IP address	IP address	From MAC address	MAC address	Protocol	Port	•	Action
0		Any 🗸		Any 🗸		WEB-HTTP 🗸	Any 🗸		ACCEPT 🖌 Delete
1		Any 🗸		Any 🗸		FTP 🗸	Any 🗸		REJECT 🗸 Delete

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:

Default incoming rule:

where options are:

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

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



Test temporarily the rules with immediate effect.

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

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



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

- in case of **connection lost** the User can reboot 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

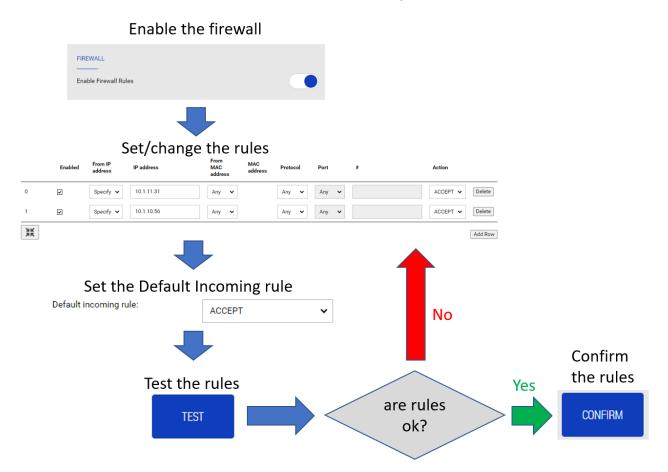
Only after the forced count-down time, if behavior of the rules is validated the User can click on the **CONFIRM** button:





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





#### 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*):

Enabled	From IP address	IP address	MAC address	MAC Protocol address	Port #	ŧ	Action
~	Specify 🗸	10.1.11.31	Any 🗸	Any 🗸	Any 🗸		ACCEPT V Delete

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)	
UDP	Enable HTTP	
Enable UDP	HTTP port	80
UDP port 33000		
UDP PASSWORD	HTTPS* (default port 443)	
Password	Enable HTTPS	
	HTTPS port	443
Retype Password		

#### Wake-on-LAN

SHBOARD	DATA	SYSTEM OVERVIEW	ISTORY	CONFIGURATION	ADMINISTRATION				
YOUR NE	TMAN	REMOTE HOSTS							
DEVICE									
General co	onfiguration	Wake O	n Lan						
Command	configuration								
Data Log o	configuration	-	KE ON LAN	n					
NETWORK		EI	Let the we on Le						
Configurat	tion	Mac ad	dresses 8	Delay					
Firewall		MAC addres	MAC addresses will be processed one by one with a delay before proceeding to the next one.						
Wake on LAN			Mac Addre	ss	Delay next (sec)				
SNMP		o	01:23:45:6	7:89:AB	3	Delete			
MODBUS/	BACNET	1	00:11:22:3		3	Delete			
RIELLO CO	NNECT	2	a1:b2:c3:d	4:e5:f6		Delete			
JSON		K.N.				L	Add Row		
SYSLOG		SAVE							
DATE & TIME									
NTP & Tim	iezone								
Configurat	tion								
EMAILS									
Configurat	tion								

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	ADMINISTR	ATION	
YOUR	NETMAN	MODEM	REMOT	E HOSTS			
DEVICE	l configuration	SNMF	<sup>o</sup> configura	ation			
Comm	and configuration						
Data Lo	og configuration		SNMP Enable SNMP pro	tocol			
NETWORK							
Config	uration						
Firewa	I	_	CONFIGURATION	MODE			
Wake o	on LAN	_	Wizard Configura				
SNMP							
MODB	JS/BACNET						
RIELLO	CONNECT	SNM	P configura	ation wizard			
JSON							
SYSLO	G		SNMP VERSION				
DATE & TIN	ΛE		SNMP V1/V2	SNMP V3			
NTP &	Timezone						
Config	uration		TRAP RECEIVER				
EMAILS			Trap receiver 1			Trap receiver 5	
Config	uration						
			Trap receiver 2			Trap receiver 6	
			Trap receiver 3			Trap receiver 7	
			Trap receiver 4			Trap receiver 8	
			TRAP REPEATER				
			Re-send traps eve	ery (minutes)	(minut	tes)	
		SA	/E				
			TEST SNMP TRAF	P (PLEASE CLICK SAVE BE	FORE TESTI	NG)	

DASHBOARD	DATA	SYSTEM OVERVIEW	HISTORY	CONFIGURATION	ADMINISTRATION					
YOUR NE	TMAN	MODEM	REMOT	E HOSTS						
DEVICE General c	onfiguration	SNM	P configur	ation						
	d configuration		SNMP							
	configuration		Enable SNMP protocol							
NETWORK										
Configura Firewall	ition		CONFIGURATION	MODE						
Wake on I	LAN		Wizard Configur	ation						
SNMP			Advanced File C	configuration						
MODBUS	/BACNET									
RIELLO C	ONNECT	SNM	P configur	ation file uplo	ad					
JSON										
SYSLOG			CURRENT CONFI							
DATE & TIME			# # each line mu #	plus SNMP configuratio st begin with one of the						
NTP & Tir	NTP & Timezone		## 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							
Configura	ition		# addView for	adding privileges	agers which will receive SNMP traps					
EMAILS	ation		# HOW TO EN/ # #	ABLE SNMPV1/V2 WITH	1 CUSTOM COMMUNITIES (myread, mywrite)					
			#addGroup v1 #addGroup v1 #addGroup v2 #	myread v1v2group mywrite v1v2groupWrite mywrite v1v2groupWrite						
			•		• A					
			Drag &	drop here you	ur SNMP configuration file					
		SA	VE							
			TEST SNMP TRA	P (PLEASE CLICK SAVE	BEFORE TESTING)					

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: <u>http://www.snmp.com</u>.

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**

DASHBOARD	DATA	SYSTEM OVERVIEW	HISTORY	CONFIGURATION	A	DMINISTRATION
YOUR NET	ΓΜΑΝ	MODEM	REMO	TE HOSTS		
DEVICE						
General co	onfiguration	MOD	BUS/BACI	NET configur	atior	1
Command	configuration		MODBUS			
Data Log c	onfiguration					
NETWORK			Enable MODBUS	5		
Configurat	ion		BACNET			
Firewall			Enable BACNET			
Wake on L	AN					
SNMP			BACNET DATA			
MODBUS/8	BACNET		BACNET Addres	s (Number)		BACNET Client (IP)
RIELLO CO	NNECT		Please insert 1	he address		Please insert the BACNET client IP
JSON						
SYSLOG			AVE			
DATE & TIME			AVL			
NTP & Tim	ezone					
Configurat	ion					
EMAILS						
Configurat	ion					

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

DASHBOARD [	DATA	SYSTEM OVERVIEW	HISTORY	CONFIGURATION	ADMINISTRATIC	IN	
YOUR NETM	AN	MODEM	REMO	TE HOSTS			
DEVICE General config	guration	JSO	N				
Command cor	nfiguration						
Data Log configuration			JSON				
NETWORK			Enable JSON notification				
Configuration							
Firewall			RECEIVER				
Wake on LAN			Monitoring host IP Please insert address			Host port	
SNMP			Notification interval (minutes)				
MODBUS/BAC			Please insert i				
JSON			SEND NOTIFICA	TION ON EVENT			
SYSLOG			UPS Lock Overload / ov	retemo			
DATE & TIME			UPS Failure				
NTP & Timezo	one		On Bypass				
Configuration			Battery work Battery low				
EMAILS			Communicati				
Configuration			Mainteinance Switch open	2			
			Anomaly				
			Command ac	stive			
		s	AVE				

*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:

```
Γ
  {
    "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,
                       // (1)
// (1)
// Hz/10
      "vin2": 0,
      "vin3": 0,
      "fin": 499,
      "vbyp1": 231,
      "vbyp2": 0,
"vbyp3": 0,
                         // (2)
// (2)
      "fbyp": 499, // Hz/10
"voutl": 231,
                       // (2)
      "vout2": 0,
                          // (2)
      "vout3": 0,
      "fout": 499,
      "load1": 0,
                           // (2)
      "load2": 0,
                           // (2)
      "load3": 0,
      "vbat": 817, // V/10
"authonomy": 475, // min
      "batcap": 100,
      "tsys": 33
    }
  }
1
```

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	UPS Mainteinance						
0	1	Communication lost						
	2	Battery low						
	3	Battery work						
	4	On bypass						
	5	UPS Failure						
	6	Overload/Overtemperature						
	7	UPS Locked						
	0	SWIN Open/Battery Low						
	1	SWBYP Open/Battery Working						
	2	SWOUT Open/UPS Locked						
	3	Output Powered						
1		SWBAT Open						
	5	SWBAT_EXT Open						
	6	Battery not present						
	7	Battery overtemp						
	0	Buck Active						
	1	Boost Actived						
	2	O.L./L.I. function						
	3	Load threshold exceeded/On Bypass						
2	4	EPO command active						
	5	BYPASS command active						
	6	Service UPS						
	7	Service battery						
	0	Replace Battery						
	1	Battery Charged						
	2	Battery Charging						
0	3	Bypass Bad						
3	4	Low redundancy						
	5	Lost redundancy						
	6	System anomaly						
	7							
	0	Bypass backfeed/Beeper On						
	1	Test in progress						
	2	Shutdown Imminent						
4	3	Shutdown Active						
4	4	PM1 fault/lock						
	5	PM2 fault/lock						
	6	PM3 fault/lock						
	7	PM4 fault/lock						
5	0	PM5 fault/lock						
5	1	Alarm Temperature						

	2	Alarm Overload
	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

DASHBOARD	DATA	SYSTEM OVERVIEW	HISTORY	CONFIGURATION	ADMINISTRATION	I.	
YOUR NET	YOUR NETMAN MC		REMOT	TE HOSTS			
DEVICE							
General co	nfiguration	SYSL	.0G				
Command	configuration						
Data Log co	onfiguration		SYSLOG				
NETWORK			Enable remote S	YSLOG			
Configurati	on						
Firewall			SERVER CONFIG	URATION			
Wake on LA	N		SYSLOG server If			Server UDP port	
SNMP			Please insert a	laaress		port	
MODBUS/B	ACNET						
RIELLO CO	NNECT	SA	WE				
JSON							
SYSLOG			TEST SYSLOG CO	ONNECTION (PLEASE CLI	CK SAVE BEFORE TE	ESTING)	
DATE & TIME			TEST SYSLOG	CONNECTION			
NTP & Time	ezone						
Configurati	on						
EMAILS							
Configurati	on						

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.

ASHBOARD	DATA	SYSTEM OVERVIEW	HISTORY	CONFIGURATION	ADM	INISTRATION
YOUR NETM	IAN	MODEM	REMO	TE HOSTS		
DEVICE						
General confi	guration	NTP	& Timezo	ne configuratio	on	
Command co	nfiguration	Current	date is 16 Mar 16	50 UTC 2023		
Data Log con	figuration	SET	A NEW TIMEZONI	E		SET A NTP SERVER
NETWORK			t the right timezo	ne		NTP server address (IP)
Configuration	1	PLI	EASE CHOOSE	~		Please insert the NTP address
Firewall						
Wake on LAN	I	s	AVE			
SNMP						
MODBUS/BA						
JSON	NEC I					
SYSLOG						
DATE & TIME						
NTP & Timez	one					
Configuration	1					
EMAILS						
Configuration						

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

ASHBOARD DATA	SYSTEM OVERVIEW HISTORY CONFIGURATION ADMINISTRATION
YOUR NETMAN	MODEM REMOTE HOSTS
DEVICE	
General configuratio	Date & Time configuration
Command configurat	ion Current date is 16 Mar 16:51 UTC 2023
Data Log configuration	SET A NEW DATE
NETWORK	Date Hour Minutes
Configuration	dd/mm/yyyy 🚟 00 ▾ 00 ▾
Firewall	
Wake on LAN	SAVE
SNMP	
MODBUS/BACNET	
RIELLO CONNECT	
JSON	
SYSLOG	
DATE & TIME	
NTP & Timezone	
Configuration	
EMAILS	
Configuration	

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

# **E**MAILS

# Configuration

SHBOARD DATA	SYSTEM OVERVIEW	HISTORY	CONFIGURATION	ADMINISTRATION			
YOUR NETMAN	MODEM	REMOT	REMOTE HOSTS				
		NEWOLE HOSTO					
DEVICE							
General configuration	Emai	l configura	tion				
Command configuration		Enable Email					
Data Log configuration							
NETWORK		MAIL HOST & SM	ITP				
Configuration							
Firewall		Mail host Please insert th	ne address		SMTP port		
Wake on LAN							
			TERS				
SNMP		Sender address		Transport			
MODBUS/BACNET		Please insert se	ender email	Plain	~		
RIELLO CONNECT		Username Please insert u	samama	Please insert pas	bowe		
JSON		Frease insert u	sword				
SYSLOG		EMAILS					
DATE & TIME			Email #1	Email #2	Email #3		
NTP & Timezone			Email Address	Email Address	Email Address		
Configuration	Devic	e Lock					
		oad / overtemp					
EMAILS		ral Failure					
Configuration	On By	blackout					
		ry low					
	Comr	nunication lost					
	S	EMAIL REPORT Send report every Send report every WE TEST EMAIL (PLE		E TESTING)			

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 emails. $^{(1)}$			
SMTP port	The IP port used by the SMTP protocol			
Sender address	Enter the address from which the e-mails are sent. <sup>(2)</sup>			
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				
Email #2	Enter the e-mail addresses to which to send the alarm notifications and reports (see note).			
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			

<sup>(1)</sup> Ensure that the SMTP server accepts connections on the configured port

<sup>(2)</sup> 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 <i>Netman 208</i> 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.

DASHBOARD	DATA	SYSTEM OVERVIEW	HISTORY	CONFIGURATION	ADMINISTRATION	
YOUR NE	ETMAN	MODEM	REMO	TE HOSTS		
MODEM						
Configur	ration	GS	M Modem c	onfiguration		
		_				
			Enable SMS			
		N	ODEM CONFIGURAT	ION		
		-	SM Courses			
		G	SM Carrier			
		F	EATURES & NOTIFICA	ATION		
		-				
				SMS #1	SMS #2	SMS #3
				Phone number	Phone number	Phone number
		D	evice Lock			
		0	verload / overtemp			
		G	eneral Failure			
		0	n Bypass			
		In	put blackout			
		В	attery low			
		C	ommunication lost			
			SMS REPORT			
			Send report even	ry day		
			Send report even	ry week		
			SAVE			
			TEST SMS (PLE	ASE CLICK SAVE BEFORE	TESTING)	

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				
SMS #2	Phone numbers that will receive SMS			
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**

SH										
	DASHBOARD	DATA	SYSTEM O	VERVIEW	HISTORY	CONFIGURATION	ADMINISTRATION			
	YOUR NET	TMAN	МС	DEM	REMOTI	E HOSTS				
	REMOTE HOST	rs shutdow	'N							
	SSH			SSH						
	VMware E	SXi								
	Nutanix				SSH Enable remote SS	H commands				
	Syneto									
					RUN FIRST SCRIP	PT ON EVENT				
					After mains failure	e (minutes)	(minutes)			
					When authonomy	is below (minutes)	(minutes)			
						e executed after " <b>Delay</b>		w of the table b	pelow	
				Conr	nectors and	Scripts Host Usernan	ne Password	Script r	Delay text sec)	
				Conr		Host Useman	e Password available in table	Script r		_
				Conr		Host Useman		Script r	next	-
						Host Usernan No data		Script r	sec)	-
					Enabled SHUTDOWN ON E	Host Usernan No data		Script r	sec)	-
					Enabled SHUTDOWN ON E	Host Useman No data	available in table	Script r	Add Row	-
					Enabled SHUTDOWN ON E	Host Useman No data	available in table	Script r	Add Row	
				53	Enabled SHUTDOWN ON E	Host Useman No data	available in table	Script r	Add Row	
				53	Enabled	Host Useman No data	available in table	Script r	Add Row	
				53	Enabled SHUTDOWN ON E Then, UPS shutdo AVE TEST CREDENTIA	Host Usernan No data	available in table (seconds)	Script r	Add Row	
				53	Enabled SHUTDOWN ON E Then, UPS shutdo AVE TEST CREDENTIA	Host Usernan No data	available in table (seconds)	Script r	Add Row	

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:

	Enabled	Host	Username	Password	Script	Delay next (sec)
0	⊻	10.1.10.151	adminuser		#W3##ASC112##ASC119##ASC100##CR##W	1 Delete
1	•	10.1.10.183	admin		shutdownscript.sh	Delete

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:

SHUTDOWN ON EVENT	
Then, UPS shutdown after (seconds)	5
SAVE	

## 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 a	
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
	For special needs, it is possible to send single chars by its Ascii code:
#ASC001#	$\rightarrow$ Ascii(1)
#ASC002#	$\rightarrow$ Ascii(2)
#ASC003#	→ Ascii(3)
•••	
•••	
#ASC253#	$\rightarrow$ Ascii(253)
#ASC254#	$\rightarrow$ Ascii(254)
#ASC255#	→ Ascii(255)

The list of tags accepted is:

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)
(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 <u>presence of char "#"</u>: 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	ADMINIST	TRATION		
YOUR NE	TMAN	MODEM	REMOT	TE HOSTS				
REMOTE HOS SSH VMware	STS SHUTDOWN		are ESXi					
Nutanix Syneto			VMWARE ESXI	ESXI shutdown				
		Host or	Username	connectors Password				
		VCSA No dat availab in tabl	ta Ile					
		***						Add Row
		Actic	ons					
			Actio	n Condition	duration	Delay next So (sec)	ource Target	Restore on power on
		No da availab in tabl ∢	ble					,
		K7 K7						Add Row
			shutdown is activ	commands will be ex		battery low cor onds)	ndition and when	
		S	AVE					
			TEST VMWARE/ (PLEASE CLICK S	VMWARE VCENTER S	SERVER APPLIAN 4G)	ICE SHUTDOW	'n	
			TEST VMWARE/ (PLEASE CLICK S	VMWARE VCENTER	ERVER CREDEN	TIALS		

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

	Action	Condition	Condition duration (min)	Delay next (sec)
0	Shutdown VM 🗸	Power fail 🗸	5	0
1	Shutdown Host 🗸	Power fail 🗸	10	0
	SHUTDOWN ON EVENT  Additionally, the commands shutdown is active	will be executed wh	en on battery low condition and v	Add Row
	Then, UPS shutdown after (	seconds)	2	

SAVE

### Actions

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

Condition	<ul> <li>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.</li> <li>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 duration time(minutes) the selected action will start. If main returns within this time, then the action will be cancelled.</li> </ul>
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 <b>Shutdown Host</b> , <b>VMotion</b> or <b>Maintenance</b> ; an IP address or hostname of a present host or VCSA must be specified. If the action is <b>Shutdown VM</b> or <b>Shutdown Cluster</b> a valid VM name or Cluster name, present in the infrastructure must be specified.
Target	If the action is <b>VMotion</b> , a valid IP address or hostname must be specified
Restore on power on	In case of shutdown actions the <i>Netman 208</i> will restart automatically all the VMs that where shutdown. In case of Maintenance action the <i>Netman 208</i> 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

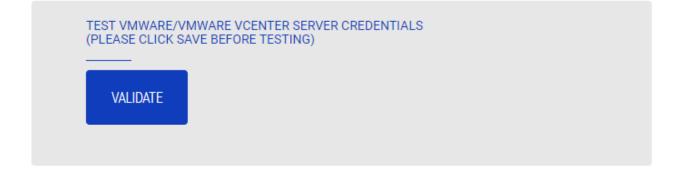
This button SAVE the configuration, please note that the service will be restarted.

	/MWARE VCENTER SERVER AVE BEFORE TESTING)	APPLIANCE SHUTDOW	N
DRY RUN			

#### Testing the configuration

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

	10.1.30.20 ACTI	ions ~					
10:130:20         Summ           IP: Relio UPS Datacenter         Iss           IP: Relio UPS Datacenter         Iss           ID: 10:30:10         Iss           ID: 10:30:12         Iss           IP: ArchLmux         Ta           ID: Debans 10         Iss           ID: Debans 10         Iss           ID: Exsis 5D: 64-bit         Se           ID: Exsis 5D: 75         Iss           ID: Liss ServerUbuntu 17:10         Inc.		figure Permissions Datacenters Previous Nets Percipain User logged event Dry-un test shutdow User logge devent Dry-Une test shutdow User logge devent Dry-Une test shutdow User User User logge devent Dry-Une test shutdow User User VSPHERE LOCAL\Andre Description:	n host 10.13012	pe         V         Date Till           User         141102           User         141102           User         141122           User         141122           Information         141122	Center Server Systems	Updates Usrousnot Jood VSPHERELOCA VSPHERELOCA VSPHERELOCA VSPHERELOCA System System System System System System System System System System System System System	Event Type ID v vm event Generallu vm event Generallu vm event Generallu vm event Generallu vm event General com vmware vc Har com vmware vc Har



#### 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

		STEM OVERVIEW	HISTORY	CONFIGURATION	AD	OMINISTRATION		
YOUR NE	TMAN	MODEM	REMOT	TE HOSTS				
REMOTE HOS	TS SHUTDOWN	Nutar	nix					
331								
VMware I Nutanix	ESXi			be defense				
Syneto			Enable Nutanix s	hutdown				
			CVM CREDENTIA Prism address Please insert h Prism user Please insert th	iost address		Prism password Please insert the password		
		Physi	cal hosts <sub>Username</sub>	Password				
		No data availabl in table	e					
		Actio	ns				Add Row	
			Actio	n Condition de	onditio uratior nin)	n next Source	Restore on power on	
		No data availabh in table	Actio	n Condition de	uration	n next Source	on power	
		availabl	Actio	n Condition de	uration	n next Source	on power	
		availabi in table	Action	n Condition dr (n EVENT	uratior nin)	hen on battery low condition and	n power on Add Row	
		availabi in table	Action	n Condition dr (n EVENT commands will be execu	uratior nin)	hen on battery low condition and	Add Row	
		availabi in table	Action	n Condition dr (n EVENT commands will be execu	ated wi	hen on battery low condition and	Add Row	

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

#### **Physical hosts**

Host	Username	Password	
10.1.31.10	root		Delete
10.1.31.12	root		Delete
10.1.31.14			Delete
			)

Add Row

#### Actions

	Action	Condition	Condition duration (min)	Delay next (sec)
0	non critical VMs 🗸	Power fail 🗸	10	60
1	Critical VM 🗸 🗸	Power fail 🗸	15	20
2	Critical VM 🗸 🗸	Power fail 🗸	15	0
4				4

#### Actions

uration (min)	Delay next (sec)	Source	Restore on power on	
	60		•	Delete
	20	79ab502a-13ca-4162-8aa	•	Delete
	0	568bd95a-af84-4510-bcb'	•	Delete
4				

ally, the commands will be exe n is active	cuted when on batte	ry low conditi	ion and when
 S shutdown after (seconds)	180		

#### SAVE

TEST NUTANIX SHUTDOWN (PLEASE CLICK SAVE BEFORE TES  DRY RUN	STING)	
TEST NUTANIX SERVER CREDENT (PLEASE CLICK SAVE BEFORE TES  VALIDATE		

#### Actions

Field	Description
Action	The action that will be executed: <b>Non critical VM</b> will shutdown all non-critical VMs <b>Critical VM</b> will shutdown the specified UID critical VM
Condition	<ul> <li>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.</li> <li>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 duration time(minutes) the selected action will start. If main returns within this time, then the action will be cancelled.</li> </ul>
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 <b>Critical VM</b> a valid VM UID, present in the infrastructure must be specified.
Restore on power on	In case of shutdown actions the <i>Netman 208</i> will restart automatically in reverse sequence all the VMs that where shutdown. Please note that to restart the host the Wake on Lan feature must be used instead.

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

#### SHUTDOWN ON EVENT

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

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

#### SAVE

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

#### DRY-RUN

#### Testing the configuration

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

#### Validating the connections

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

## Syneto

#### **CONFIGURE ESXI AUTOSTART FUNCTIONALITY**

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

a2000-esxi.dev.syneto.net - Mana	age						
System Hardware Licens	ing Packages Services	Security & users					
Advanced settings	🖋 Edit settings						
Autostart	Enabled	Yes					
Swap Time & date	Start delay	120s					
	Stop delay	120s					
Stop action		Power off					
	Wait for heartbeat	No					
	🕞 Enable 🛛 🙀 Start earlier 🖓 Confi	gure 👸 Disable   🧲 Refresh   🏟 Actions		Q :	Search		
	Virtual machine	~	Shutdown behav ~	Autos ~	Start ~	Stop ~	
	SynetoOS		System default	1	120 s	120 s	
	SynetoFileRecovery		System default	2	120 s	120 s	
	b Virtual Machine 1		System default	3	120 s	120 s	
	First Virtual Machine 2		System default	4	120 s	120 s	
	Virtual Machine 3		System default	5	120 s	120 s	

#### **CONFIGURE ESXI USER & ROLE FOR REMOTE POWER MANAGEMENT**

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

1. Create a new Role.

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

Role PowerMgmt added success Host			Security & users		
Manage	System Hardware	Licensing Packages Services	Security & users		
Monitor	Acceptance level	🕂 Add role 🧪 Edit role 💥 Remo	ve role   C Refresh	Q Search	
🔁 Virtual Machines 🚺 10	Authentication Certificates	Name	~ Summary		~
<ul> <li>LucianS_0105_5.176_5.13</li> <li>Users</li> </ul>	Administrator	Full access rights			
Monitor	Roles	Anonymous	Not logged-in user (cannot be granted)		
F 🚯 qa2000.dev.syneto.net	Lockdown mode	No access	Used for restricting granted access		
More VMs		No cryptography administrator	Full access without Cryptographic operations privileges		
Storage 10 Networking 3		PowerMgmt	PowerMgmt		
Networking		Read-only	See details of objects, but not make changes		
		View	Visibility access (cannot be granted)		

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

Choose the following from Privileges:

Root -> Host -> Config -> Power.

n 🕂 Add a role		
e: Role name (required) pt	PowerMgmt	
n Privileges	Root Host Config	18
	NetService	18
	Memory	- 18
	Network	- 18
	AdvancedConfig	- 18
	Resources	- 18
	Snmp	- 11
	DateTime	- 18
	PciPassthru	- 18
	Settings	- 11
	Patch	- 18
	Firmware	- 18
	Power	- °
	Add Cance	
		h.

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

+	Add a role		
			- 18
	Role name (required)	PowerMgmt	-11
	Privileges	Root VirtualMachine Interact	-11
		PowerOn	- 18
		PowerOff	- 18
		Suspend	- 18
		Reset	- 18
		Pause	- 11
		AnswerQuestion	- 1
		ConsoleInteract	- 1
		DeviceConnection	- 1
		SetCDMedia	- 1
		SetFloppyMedia	- 1
		ToolsInstall	- 1
		GuestControl	- 1
		Add Canc	el

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.

<b>m</b> ware <sup>,</sup> ESXi <sup>-</sup>			root@qa2000-esxi.dev.syneto.net 👻   He	elp - I Q Search
🖥 Navigator 👘	a2000-esxi.dev.syneto.net - Mar	age		
🕶 🗐 Host	System Hardware Licen:	sing Packages Services Security & users		
Manage Monitor	Acceptance level	🐕 Add user 🥒 Edit user 🛛 🔒 Remove user 📔 🤁 Refresh		Q Search
Virtual Machines	Authentication Certificates	User Name	Description	~
<ul> <li>LucianS_0105_5.176_5</li> <li>Monitor</li> </ul>	Users	root	Administrator	
More VMs	Roles	ups	UPS Power Management	2 items
Storage 10	Lockdown mode			2 items

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

Go to Host -> Actions -> Permissions.

Navigator	] qa2000-esxi.dev.syneto.net					
Host         Manage           Monitor         10           Virtual Machines         10           - Virtual Machines         10           - Virtual Machines         10           - Constantiation         10           - Monitor         10           - Storage         10           - Storage         10           - Q. Networking         10	Manage with vCenter Server qa2000-esxi.de Version: State. Uptime:	CreaterRegister VM I Shut down Reboot I C Refresh exsyncto.net 6.7.0 Update 3 (Build 16713366) Normal (connected to vCenter Server at 192.168.1.53) 55.65 days  vv vCenter Server. Actions may be performed automatically by vCenter	Actions Host Host Host Center Server Disconnect from VCenter Server CesterRegister VM CesterRegister VM Shut down Shut down Reboot Secol	tions	CPU USED: 3.5 GHz MIKNORY USED: 10.43 GB STORAGE USED: 149.47 GB	FREE: 13.504 15% CAPACITY: 23.00 55% CAPACITY: 2154 00 FREE: 63.306 70% CAPACITY: 215 00
	* Hardware		Enter maintenance mode			
	Manufacturer	Syneto	Lockdown mode		(Updated) ESXi-6.7.0-20190604001-Syneto-v5	i.111 (Syneto)
	Model	HYPERSeries-2000-G3	b Permissions		Agent running	
	> 🔲 CPU	10 CPUs x Intel(R) Xeon(R) Silver 4210 CPU @ 2.20GHz	Generate support bundle		Supported	
	Memory	127.66 GB	Get SSH for Chrome			
	Persistent Memory	0.8				

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

ľ	Normal (connected to vCen	ter Server at 192.168.1.53)		
I	Host	Assign users and roles for Host		
l		ង Add user 🛛 🌡 Remove user 🛛 🕂 Assign role		
nar		User 🛦	Role ~	
		dcui	Administrator	
		root	Administrator	- 8
		vpxuser	Administrator	Б
			3 items	ju
				jui

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

esxi.dev.syneto.net				
4 Manage permissions				
Host	Add user for Host			
	ups	~	PowerMgmt	~
	Propagate to all childr Root	en 🗋 Add as group		E
	System Global Folder Datacenter			nir 3
	Datacenter Datastore Network DVSwitch			D Ju Jit
	<ul> <li>DVPortgroup</li> <li>Host</li> <li>VirtualMachine</li> <li>Resource</li> </ul>			d t
	Alarm			Cancel Add user
Yes			1001	Close

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

DASHBOARD	DATA	SYSTEM OVERVIEW	HISTORY	CONFIGURATION	ADMINISTRATION	1	
YOUR NE	TMAN	REMOTE F	IOSTS				
REMOTE HOS	STS SHUTDOWN		neto				
VMware	ECVI						
	LJAI		SYNETO				
Nutanix		- 1	Enable Syneto	shutdown		<u></u>	•
Syneto							
		In	frastructure	connectors			
		E	SXi Hypervisor	Username	Pa	ssword	
			10.1.40.120	ups			Delete
		5					Add Row
		Ac	tions				
			Action	Condit	ion Condition d	luration (min) De	elay next (sec)
		0		n Host 🗸 Powe	r fail 🖌 10		
		< K					Add Row
			SHUTDOWN O	N EVENT			
			Additionally, th shutdown is ac	e commands will be e tive	ecuted when on battery l	ow condition and when	
			Then, UPS shu	tdown after (seconds)	120		
			SAVE				
			TEST SYNETO	SHUTDOWN K SAVE BEFORE TESTI			
			_	SAVE BEFORE TEST	NG)		
			DRY RUN				
			TEST SYNETO (PLEASE CLICI	SERVER CREDENTIAL SAVE BEFORE TESTI	S NG)		
			VALIDATE				

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:	<ul> <li>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.</li> <li>Autonomy less: When the calculated battery autonomy of the</li> </ul>
	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. <b>We recommend at least 15 minutes.</b>

# Actions

	Action	Condition	Condition duration (min)	Delay next (s
0	Shutdown VM 🖌	Autonomy less 🗸	15	
•				Þ

## Actions

Delay next (sec)	Source		Target	o	ower
4					×.
				Ad	d Row
SHUTDOWN ON EVER Additionally, the comm shutdown is active	mands will be execute		ttery low conditior	n and when	
Then, UPS shutdown	after (seconds)	120			
SAVE					

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.

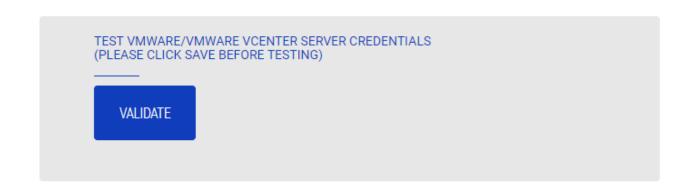
Additionally, the commands will be executed when on battery low condition and when shutdown is active.

#### 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

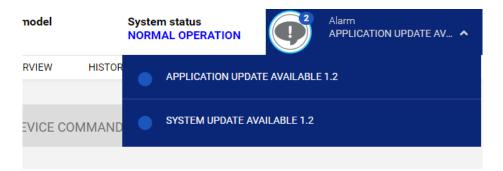
It is also possible to test the correct user account and password to login on the VSphere VCSA. The test will return the result with a pop-up screen.

# **ADMINISTRATION**

## **Automatic Check for Updates**

SHBOARD DATA SYSTEI	M OVERVIEW HISTORY	CONFIGURATION	ADMINISTRATION	
ADMINISTRATION	DEVICE COMMANDS			
ADMINISTRATION				
Automatic Check for Updates	Automatic Che	ck for Update	S	
Firmware upgrade				
Reset to defaults	Check for Applic	ation updates		
Reset Log	Check for System	m updates		
Reset Riello Connect				
Reboot	SAVE			
Change local password				
Login access				

*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

DASHBOARD DATA SYST	M OVERVIEW HISTORY CONFIGURA	ATION ADMINISTRATION
ADMINISTRATION	DEVICE COMMANDS	
ADMINISTRATION		
Automatic Check for Updates	Application version alph	ha
Firmware upgrade		
Reset to defaults	For firmware upgrading you mu	ust reboot to <b>Upload Mode</b> :
Reset Log	RE	EBOOT FOR UPLOAD A FIRMWARE
Reset Riello Connect		
Reboot		
Change local password		
Login access		

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

Netman208 UPLOAD MOD	DE Hostname: DEB11XNETMAN	Mac address	08:00:27:79:7a:e1	Systemapi: armhf-bullseye-1		
System Virtual Machine App	pplication 🖧 Restore network 🧏	Network Compatibility	Reboot to Normal Mode			
System Image						
Drag or Select image file with extension '.sys208" then Upload procedure will start.						
Please drop here the file to upload						
or select manually from Select image file						
Ready						

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.

i

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:

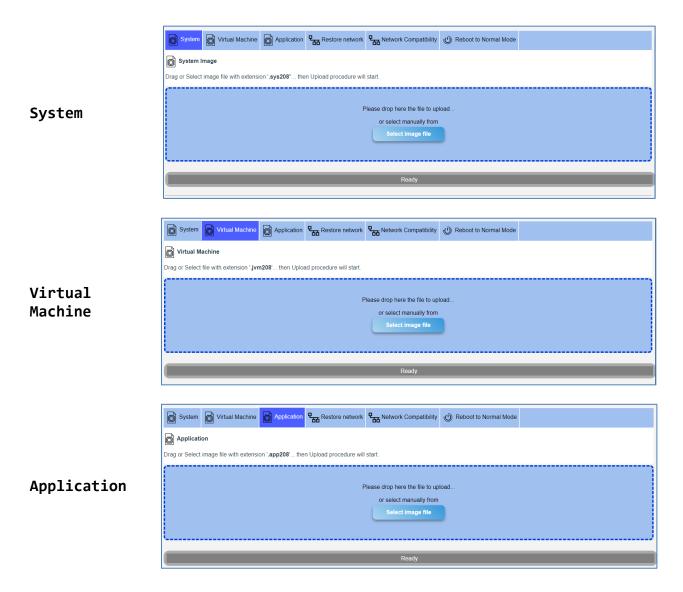
- Image data file (FW108-vvrr.app208 / FW107-vvrr.jvm208 / FW109-vvrr.sys208) - JSON file with checksum (FWxyz-vvrr-JSON.json)

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

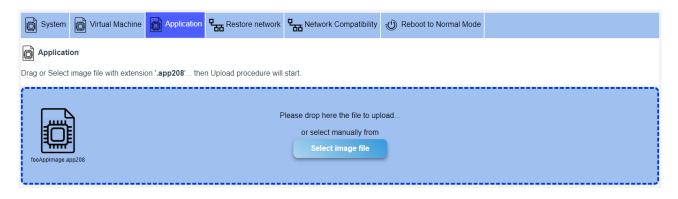
Every firmware component must be loaded from their specific tab:



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

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

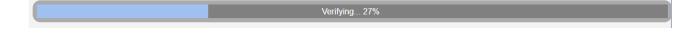
1) Select the image file.



2) Select the json checksum file.

Netma	11208 UPL		ostname: DEB11XNET	MAN Mac addre	ss: 08:00:27:79:7a:e1	Systemapi: armhf-bullseye-1	
System	Virtual Machine	Application	Restore network	Par Network Compatibility	Reboot to Normal Mode		
Applicatio	n						
Drag or Select in	mage file with extensi	on ' <b>.app208</b> ' the	n Upload procedure will	start.			
fooAppimage.app	5208		F	Please drop here the file to or select manually fro Select image file			
			Plea	se drop here the JSON file or select manually fro Select JSON file			
			Please	load JSON file ' <b>fooAppIm</b> a	ge-JSON.json'		

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.

Syste	em 👔 Virtual Mach	nine Application	Restore network	Post Network Compatibility	D Reboot to Normal Mode		
Appli	Application						
Drag or Se	ect image file with ext	tension ' <b>.app208</b> ' the	n Upload procedure will	start.			
			or sel	here the file to upload ect manually from lect image file			
			Click to r	reboot to Normal Mode			
	Completed						

Finishing...0%

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

## **Reset to defaults**

ASHBOARD DATA SYSTEN	Are you sure to reset to default × configuration?
ADMINISTRATION	Please insert the code to confirm. TyQ9YSf5f2
ADMINISTRATION	YES NO
Automatic Check for Updates	YES NO
Firmware upgrade	
Reset to defaults	For firmware upgrading you must reboot to <b>Upload Mode</b>
Reset Log	REBOOT FOR UPLOAD A FIRMWARE
Reset Riello Connect	
Reboot	
Change local password	

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

ADMINISTRATION	DEVICE COMMANDS	
ADMINISTRATION		
Automatic Check for Updates	Change local password	
Firmware upgrade		
Reset to defaults	ADMIN	POWER USER
Reset Log	Password	Password
Reset Riello Connect	Retype Password	Retype Password
Reboot		
Change local password	SAVE	SAVE
Login access	Admin credentials grant the right to manage Netman and also the device,	Power credentials grant the right to manage Netman but cannot operate the
	including shutdown	device (cannot perform shutdown) REVOKE ACCESS

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

DASHE	BOARD	DATA	SYSTEM OVERVIEW	HISTORY	CONFIGURATION	ADMINISTRATION		
	ADMINIST	TRATION	DEVICE	COMMANDS				
AD	MINISTRAT	ION Check for Upd	ates Log	gin access				
	Firmware							
				Enable Auto Log	out			
	Reset to de	efaults						
	Reset Log			Auto Logout due	e to user inactivity after (se	conds)		
	Reset Riel	lo Connect		Warning messag (message 'Sessio	ge when are left (seconds) on is about to expire')	before logout		
	Reboot							
	Change loo	cal password		Enable SSH				
	Login acce	955		Enable HTTP HTTP port			80	
				Enable HTTPS HTTPS port				
				Enable Local aut	thentication (NOTE: admin	is always available on	SSH)	
				Enable AD/LDAP	<sup>a</sup> authentication			
				LDAP SERVER				
				Server address	-			
				Idap://yourserver:3	04/			
				ou=Users,dc=exam	nple,dc=com			
				Admin group name				
				cn=administrators,	ou=Groups,dc=example,dc	≃com		
				Power group name				
				cn=powerusers,ou	=Groups,dc=example,dc=c	om		
				SAVE				
				TEST AD/LDAP /	AUTHENTICATION (PLEAS	E CLICK SAVE BEFORE	E TESTING)	

Field	Description
Enable Auto Logout	To enable Auto Logout
Auto Logout due to user inactivity after (seconds)	After this inactivity time (no mouse clicks) <i>Netman 208</i> 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 Idap:// or Idaps://
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

Idap://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=ORGANIZATIO N,dc=example,dc=com

Power group name

```
cn=sys.ups.powerusers,ou=UPS,ou=SYS,ou=STRUCTURE_MANAGED,ou=ORGANIZATI
ON,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:

LDAP authentication	~	LDAP authentication	
Username		Username	
orgadmin		orgpower	
Password		Password	

The Netman 208 connects to host 'Idap://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

<u>cn=sys.ups.sysadmins,ou=UPS,ou=SYS,ou=STRUCTURE\_MANAGED,ou=ORGANIZATION,</u> <u>dc=example,dc=com</u>:

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 <u>'Admin'</u> rights in the *Netman 208* and search ends with success.



(If not found) checking if user '#USERNAME#' belongs to Power group

<u>cn=sys.ups.powerusers,ou=UPS,ou=SYS,ou=STRUCTURE\_MANAGED,ou=ORGANIZATION</u>,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 <u>'Power'</u> 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'.

System status LOAD ON INVE	
	)

#### Test connection

It is possible check the connection to the Server:

TEST AD/LDAP AUTH	NTICATION (PLEASE (	CLICK SAVE BEFORE T	ESTING)	
TEST AD/LDAP				
TEST AD/LDAP				

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.

### **C**OMMANDS

## **Test battery**

DASHBOARD	DATA	SYSTEM OVERVIEW	HISTORY	CONFIGURATION	ADMINISTRATION	
ADMIN	ISTRATION	DEVICE CO	MMANDS			
COMMAND	IS					
Test be	ittery	Test	battery			
Shutdo	wn					
Shutdo	wn / Restore		DO YOU WANT	TO PERFORM A BATTERY	TEST?	
			YES			

To execute a test of the batteries.

### Shutdown

DASHBOARD	DATA SYST	EM OVERVIEW	HISTORY	CONFIGURATION	ADMINISTRATION	
ADMINIST	TRATION	DEVICE CO	OMMANDS			
COMMANDS						
Test batte	ry	Shut	tdown UPS			
Shutdown	1					
Shutdown	/ Restore			TO SHUTDOWN THE UPS	?	
			Choose the dela	y for shutdown		
			SHUTDOWN	I		

To execute a shutdown of the device.

### Shutdown / Restore

DASHBOARD	DATA SYST	EM OVERVIEW	HISTORY	CONFIGURATION	ADMINISTRATION	
ADMINISTRA	ATION	DEVICE CON	MMANDS			
COMMANDS						
Test battery		Shute	own and i	restore UPS		
Shutdown						
Shutdown / Re	estore		DO YOU WANT T	O SHUTDOWN AND REST	ORE THE UPS?	
		-	Choose the delay	for shutdown	Choose the delay for restore	
			120 sec	~	1 hour	~
			SHUTDOWN AI	ND 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:

assw	ord Recov	very			
	0N				
1) Please se	nd via mail to service th	iis code: <b>204:00</b> :	02:63:07:b2:06:123	45768	
2) Submit th	e RECOVERY CODE rece	eived via mail by	the service in the fo	rm below	
RETURN	OGIN				
INCEPT DEC	OVERY CODE				
	OVERY CODE				
Code					
SUBMI					

i

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.

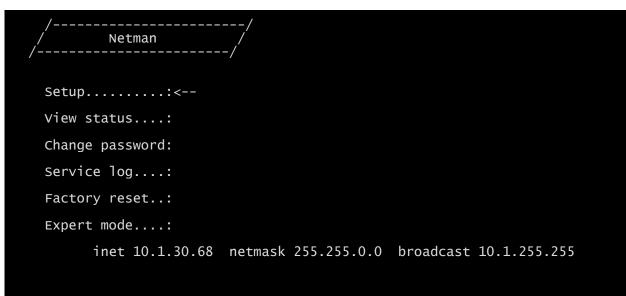


For proper configuration of *Netman 208*, you must configure the SSH client so that the backspace key sends "Control-H". Please verify the keyboard options of your SSH client.

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:



#### Press [ESC] for logout SysVer. U23-1 - AppVer. 1.0

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.

Кеу	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	
Enter	Confirmation of characters entered	
Esc <sup>(1)</sup>	Exit main menu <sup>(2)</sup>	
	Return to previous menu	

<sup>(1)</sup> Some keys can have a different function depending on the menu.

 $^{(2)}\,$  To exit from a menu a confirmation ('Y' or 'N') is required after pressing the ESC key.

## Setup

The main configuration menu displays a screen like the following:

// / Setup / //
IP config:<
Reboot:
Press [Esc] to quit SysVer. U23-1 - AppVer. 01.00.000

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

Menu	Function
IP config	To configure the network parameters
Expert mode	To enter Expert mode (more information at paragraph "Expert mode")
Reboot	Reboots the Netman 208

### **IP config**

// / IP config / //	
Hostnameups-server	
IP address/DHCP:DHCP	
Netmask	
Gateway	
Primary DNS:	
Secondary DNS:	

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

Field	Parameters to be inserted	
Hostname	Enter the 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></value></var>	set VAR to VALUE
delete <var></var>	removes VAR
sendtrap + <trapcode></trapcode>	send a test SNMP trap (alarm added)
sendtrap - <trapcode></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

### **C**ONFIGURATION 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

DEVICE		DEVICE CONFIGUR	ATION	NETWORK CARD	
Model	RT1K06	PRTK code	GPSER11201	Card version	e4400001 (8G)
Part Number	•	Name	Netman 208	Serial Number	1234576
Serial number	-			MAC Address	00:02:63:07:b2:0
Power [kVA]	6.0			Application version	01.00
Power [kW]	6.0	0759 HOT 1 00		System version	U22-
Battery capacity [Ah]	6	SERVICE LOG		Kernel	5.15.5-EK20230324-6
Battery voltage [Vdc]	180	DOWNLOAD SE	IVICE LOG	Current date	28 Mar 14:50 UTC 202
Firmware version	SWM070-01-14				
NETWORK CONFIGURATIO	N				
Hostname	netman6307b206	IPv4 Address	10.1.30.56	Gateway	10.1.1.
DHCP enabled	yes	Netmask	255.255.0.0	Primary DNS	10.1.5.1
		IPvő Address	fe80::202:63ff:fe07:b206	Secondary DNS	10.1.5.1
READ MANUAL					LEGAL INFORMATION

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 <sup>(1)</sup>		STATES/ALARMS		BIT <sup>(2)</sup>	
Number	Address	STATES/ALAP	IVIS	Number	Address
				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
1	0	Bypass bad	[0=NO / 1=YES]	8	7
T	0			9	8
		Normal operation	[0=NO / 1=YES]	10	9
				11	10
		On bypass	[0=NO / 1=YES]	12	11
		Battery low	[0=NO / 1=YES]	13	12
		Battery working	[0=NO / 1=YES]	14	13
		UPS locked	[0=NO / 1=YES]	15	14
		Output powered	[0=NO / 1=YES]	16	15
				17	16
				28	27
2	1	Input Mains present	[0=NO / 1=YES]	29	28
		Alarm temperature	[0=NO / 1=YES]	30	29
		Alarm overload	[0=NO / 1=YES]	31	30
		UPS failure	[0=NO / 1=YES]	32	31
				33	32
3	2				
				48	47
				49	48
4	3				
7	5			63	62
		Communication lost with UPS	[0=NO / 1=YES]	64	63

<sup>(1)</sup> The register number n must be addressed n-1 in the data packet.

<sup>(2)</sup> The bit number n must be addressed n-1 in the data packet.

REGIS	TER <sup>(1)</sup>		
Number	Address	MEASUREMENTS	UNIT
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	20	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	20	Output voltage (Ph-N) V3	V
29	28	Output voltage (FII-N) v5	V
 37	 36		
37	37	Load phase 11	%
38	37	Load phase L1	%
40	38	Load phase L2	%
	40	Load phase L3	70
41			
42	41		
43	42	Output fragmann	11-/10
44	43	Output frequency	Hz/10
45	44		
46	45		
47	46	Detter weltere	2////
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		

<sup>(1)</sup> 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 <sup>(1)</sup>			UNIT
Number	Address	- NOMINAL DATA	UNIT
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 <sup>(1)</sup>		COMMANDS		
Number	Address	COMMANDS	UNIT	
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		

<sup>(1)</sup> 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	А
Analogue Input 5	Input current line 3	А
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	А
Analogue Input 15	Output current line 2	А
Analogue Input 16	Output current line 3	А
Analogue Input 17	Output peak current line 1	А
Analogue Input 18	Output peak current line 2	А
Analogue Input 19	Output peak current line 3	А
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	
Analog Input 50	Power module 6 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 <sub>DC</sub>			
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	DESCRIPTION
1	+5V <sub>DC</sub>	LEAVE UNCONNECTED			
2	GND	$\leftarrow$ CONNECT TO $\rightarrow$	7	5	GND
3	RS232 TXD	$\leftarrow$ CONNECT TO $\rightarrow$	2	3	RXD
4	RS232 RXD	$\leftarrow \text{CONNECT TO} \rightarrow$	3	2	TXD
5	RS485 A	LEAVE UNCONNECTED			
6	RS485 B				

### **N**ETWORK 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+	$1 \leftarrow \rightarrow 1$		
TX-	$2 \leftrightarrow 2$		
RX+	$3 \leftrightarrow 3$		
RX-	$6 \leftrightarrow 6$		



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 (<u>http://qwt.sf.net/</u>).

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

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 (<u>https://h2database.com/</u>), 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: <u>https://h2database.com/html/license.html</u>

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.

#### 0MNACCSA8ENUA