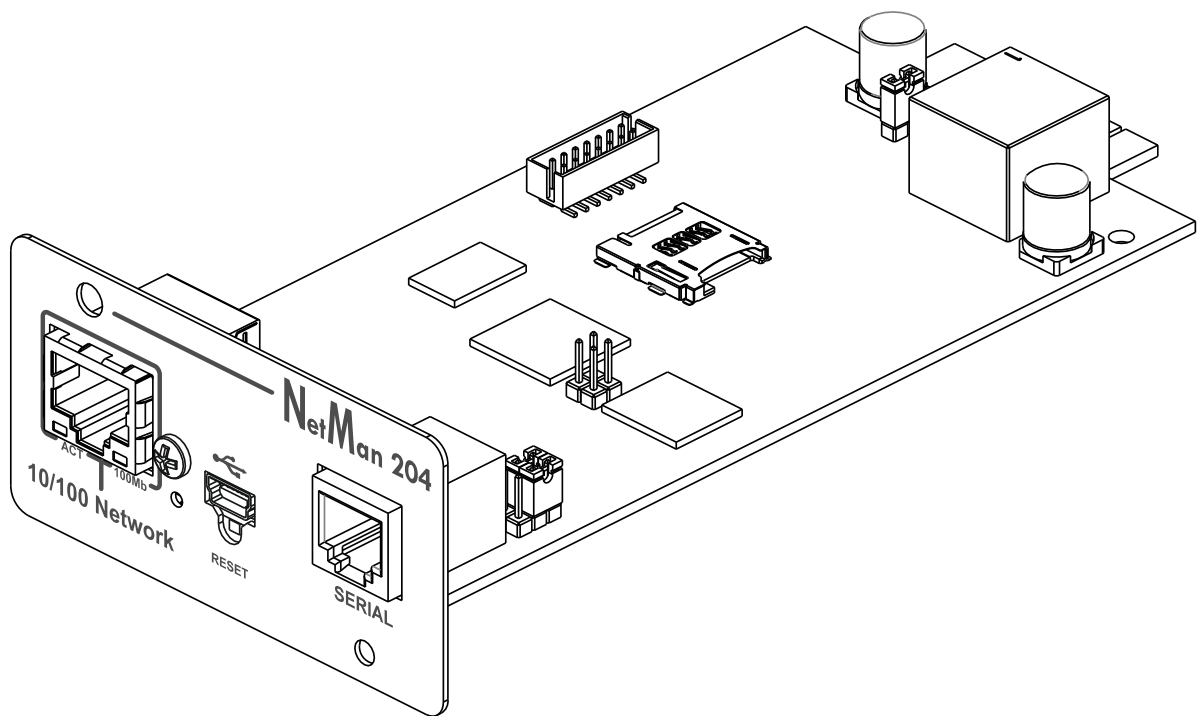


NETMAN 204

NETWORK ADAPTER



MANUALE d'INSTALLAZIONE ED USO

INTRODUZIONE

Vi ringraziamo per la scelta del nostro prodotto.

Gli accessori descritti nel presente manuale sono prodotti della massima qualità, attentamente progettati e realizzati per garantire le migliori prestazioni.

Questo manuale contiene istruzioni dettagliate per l'installazione e l'uso del prodotto.

Conservare il manuale in un luogo sicuro e CONSULTARLO PRIMA DI UTILIZZARE IL DISPOSITIVO per verificare le necessarie istruzioni e sfruttare al massimo le capacità del dispositivo.

NOTA: alcune immagini contenute nel presente documento vengono fornite a scopo informativo e potrebbero non illustrare esattamente le parti del prodotto che raffigurano.

Simboli usati in questo manuale:



Avvertenza

Indica informazioni importanti che non devono essere ignorate.



Informazioni

Segnala informazioni e suggerimenti utili per l'utente.

SICUREZZA

In questa parte del manuale sono fornite le precauzioni di SICUREZZA da seguire scrupolosamente.

- ❖ Il dispositivo è stato progettato per essere utilizzato in ambito professionale; pertanto non è idoneo a un utilizzo domestico.
- ❖ Il dispositivo è stato progettato per essere utilizzato soltanto in ambienti chiusi. Deve essere installato in ambienti privi di liquidi o gas infiammabili o altre sostanze nocive.
- ❖ Evitare che acqua o liquidi e/o altri oggetti estranei penetrino all'interno del dispositivo.
- ❖ In caso di guasto e/o funzionamento irregolare del dispositivo, non tentare di ripararlo e contattare il centro assistenza autorizzato.
- ❖ Il dispositivo deve essere utilizzato per le finalità per cui è stato progettato. Qualsiasi altro utilizzo è da considerarsi improprio e quindi pericoloso. Il produttore declina ogni responsabilità di eventuali danni causati da un utilizzo improprio, erraneo e irragionevole.

TUTELA AMBIENTALE

La nostra società dedica notevoli risorse all'analisi degli aspetti ambientali nello sviluppo dei prodotti. Tutti i nostri prodotti perseguono gli obiettivi definiti nel sistema di gestione ambientale sviluppato dalla società in conformità a tutti gli standard applicabili.

In questo prodotto non sono stati utilizzati materiali nocivi, quali CFC, HCFC o amianto.

Nella valutazione dell'imballo, è stata data preferenza ai materiali riciclabili. Separare i vari materiali di cui è composto l'imballo ed eliminarli tutti in conformità agli standard applicabili nel Paese in cui è stato utilizzato il prodotto.

SMALTIMENTO DEL PRODOTTO

Il dispositivo contiene materiale interno (ad esempio, schede elettroniche) considerato TOSSICO se smontato o smaltito. Smaltire questi materiali in base alle leggi in vigore, contattando i centri di raccolta specializzati. Lo smaltimento adeguato contribuisce alla tutela dell'ambiente e della salute dell'uomo.

© È vietata la riproduzione di qualsiasi parte del presente manuale, anche parziale, tranne se autorizzata dal produttore.

Il produttore si riserva il diritto di modificare il prodotto descritto per finalità migliorative in qualsiasi momento e senza preavviso.

SOMMARIO

DESCRIZIONE	8
PRESENTAZIONE	8
CONTENUTO DELL'IMBALLO	8
PANNELLO FRONTALE	9
Porta di rete	9
Porta micro-USB	9
Porta seriale	9
LED	9
Modem GSM (opzionale)	10
Pulsante di reset	10
UTENTI	10
SERVIZI DI RETE	11
SSH	11
Rete seriale	11
Wake-on-LAN	11
HTTP	11
SNMP	11
UDP	11
Modbus TCP/IP	11
BACnet/IP	12
FTP	12
Servizio syslog	12
Servizio Email	12
Servizio Reports	12
Client SSH (solo per sistema operativo W18-1 o successivo)	12
ARCHIVIO STORICO DEI VALORI E DEGLI EVENTI DEL DISPOSITIVO	13
Eventlog	13
Datalog (solo per dispositivi UPS)	13
SENSORI AMBIENTALI (OPZIONALE)	14
Sensori disponibili	14
INSTALLAZIONE	14
CONFIGURAZIONE	15
PRESENTAZIONE	15
Configurazione mediante HTTP/HTTPS	15
Configurazione mediante USB	16
Configurazione mediante SSH	16

DESCRIZIONI DEI MENU DI CONFIGURAZIONE	17
Menu iniziale	17
Setup	19
IP config	20
CONFIGURAZIONE WEB	21
Login	21
Dashboard	23
Configurazione di rete	24
Configurazione del dispositivo	25
Configurazione comandi remoti	26
Data log	27
Firewall UDP	28
Indirizzi Wake-On-LAN	29
SNMP	30
MODBUS/BACNET	33
JSON	34
Configurazione syslog	37
Configurazione client SSH (solo per sistema operativo W18-1 or successivo)	38
VMware ESXi	40
Nutanix	44
Syneto	48
Configurazione NTP & Timezone	57
Configurazione Date & Time	58
Configurazione email	59
Email logic	60
Modem GSM	61
Sensori	62
Installazione Sensori tramite SSH o USB	63
Installazione sensori tramite HTTP	65
Configurazione dell'accesso	67
Certificati	69
Recupero della password	79
Configurazione Wi-Fi (richiesta scheda opzionale)	80
Modalità Expert	81
CONFIGURAZIONE DI DIVERSI DISPOSITIVI	81
SERVICE LOG	82
AGGIORNAMENTO DEL FIRMWARE	83
AGGIORNAMENTO DEL FIRMWARE MEDIANTE HTTP	83
AGGIORNAMENTO DEL FIRMWARE MEDIANTE FTP	83

CONFIGURAZIONE DI SNMP	84
PROTOCOLLO MODBUS TCP/IP	87
CONFIGURAZIONE BACNET/IP	91
EVENTLOG CODES	93
CONFIGURAZIONE PORTA SERIALE	95
DATI TECNICI	96
CAVO DI RETE	96
CONDIZIONI DI FUNZIONAMENTO E CONSERVAZIONE	96
INFORMAZIONI LEGALI	97

DESCRIZIONE

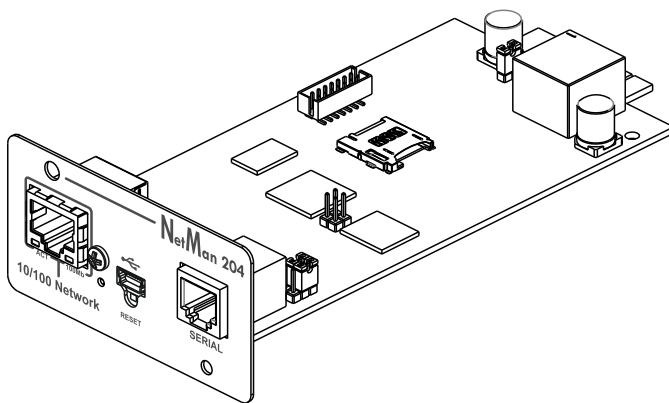
PRESENTAZIONE

Netman 204 è un accessorio che consente la gestione del dispositivo tramite una rete locale (LAN); supporta tutti i principali protocolli di rete (SNMP v1, v2 e v3, TCP/IP, http/HTTPS, MODBUS TCP e BacNet/IP) ed è compatibile con le reti Ethernet 10/100Mbps IPv4/6. Il dispositivo può pertanto essere integrato facilmente in reti di dimensioni medie e grosse.

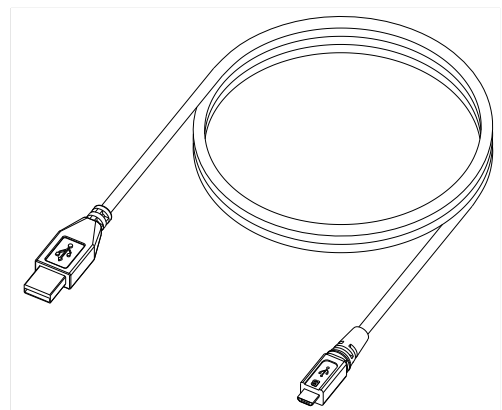
Netman 204 registra inoltre i valori e gli eventi del dispositivo nell'archivio storico ed è in grado di gestire sensori ambientali opzionali (non in dotazione con il dispositivo, forniti separatamente).

CONTENUTO DELL'IMBALLO

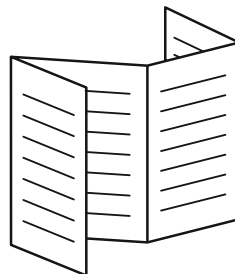
Netman 204



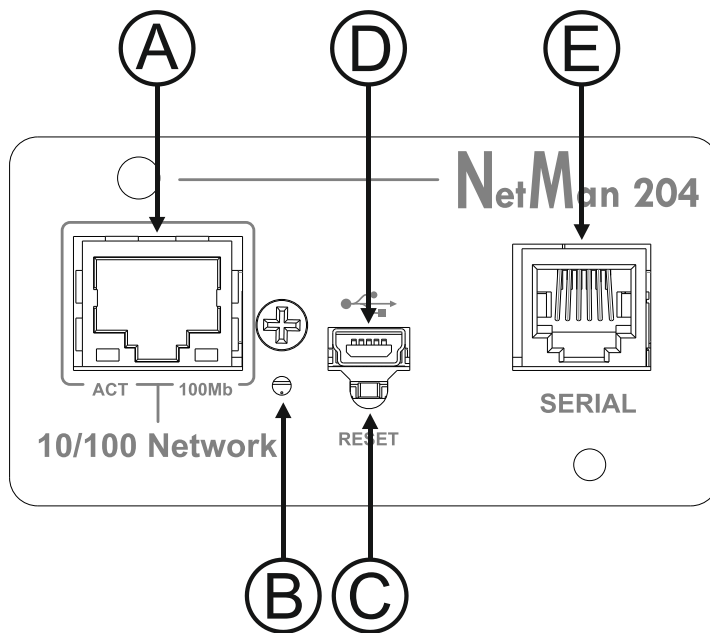
Cavo USB



Riferimento rapido



PANNELLO FRONTALE



- A: Porta di rete
- B: LED
- C: Pulsante di reset
- D: Porta micro-USB
- E: Porta seriale

Porta di rete

NetMan 204 viene collegato alle reti Ethernet 10/100 Mbps mediante connettore RJ45. Le spie luminose a LED integrate nel connettore descrivono lo stato della rete:

- LED a sinistra
GIALLO FISSO: *NetMan204* ha rilevato un collegamento valido.
GIALLO LAMPEGGIANTE: *NetMan204* sta ricevendo o trasmettendo pacchetti di dati.
- LED a destra
VERDE FISSO: *NetMan204* viene collegato a una rete funzionante alla velocità di 100 megabit al secondo.

Porta micro-USB

NetMan 204 dispone di una porta di comunicazione USB che permette di configurarlo (vedere la sezione "Configurazione mediante USB").

Porta seriale

NetMan 204 dispone di una porta di comunicazione seriale che consente di collegare sensori ambientali (non in dotazione con il dispositivo, forniti separatamente).

LED

Questo LED descrive lo stato di *NetMan 204*:

- ROSSO FISSO: *NetMan 204* non comunica con il dispositivo (verificare il codice PRTK).
- ROSSO LAMPEGGIANTE: il server DHCP non ha assegnato un indirizzo IP valido a *NetMan 204*.
- SPENTO: funzionamento regolare.

Modem GSM (opzionale)

NetMan 204 è in grado di inviare SMS di notifica al verificarsi di determinate condizioni. Gli SMS possono essere inviati a un massimo di tre destinatari per sette tipi diversi di allarme. Sono richiesti un modem GSM esterno (accessorio opzionale) e una SIM card. Per ulteriori dettagli, vedere la sezione "Modem GSM".

Pulsante di reset

Il pulsante di reset consente di riavviare *NetMan204* o di caricare una configurazione predefinita con un indirizzo IP statico prestabilito.

Per eseguire il reset di *NetMan204*: tenere premuto il pulsante di reset fino quando il LED rosso non inizia a lampeggiare (circa 2 secondi) e quindi rilasciarlo.

Per caricare una configurazione con un indirizzo IP statico prestabilito: tenere premuto il pulsante di reset; il LED inizia a lampeggiare, quindi emette una luce rossa fissa (circa 10 secondi). Quando la luce rossa del LED è fissa, rilasciare il pulsante di reset e attendere il riavvio di *NetMan 204* con:

- Indirizzo IP: 192.168.0.204
- Netmask: 255.255.0.0
- Servizio SSH attivato
- Servizio HTTP attivato



I servizi HTTP e SSH vengono attivati temporaneamente senza modifiche alla configurazione salvata nella memoria non volatile.

UTENTI

L'accesso a *Netman 204* può essere consentito a quattro utenti diversi:

Nome utente	Password predefinita	Privilegi
admin	admin	utente con diritto di modificare la configurazione ⁽¹⁾
power	N/D ⁽²⁾	utente con diritto di modificare la configurazione ⁽²⁾
fwupgrade	fwupgrade	utente con diritto di aggiornare il firmware
user	user	utente con diritto di leggere e scaricare gli archivi



- (1) L'utente "admin" può inoltre operare sul dispositivo e quindi comandare lo spegnimento.
- (2) L'utente "power" è disabilitato di default e ha il diritto di modificare la configurazione (solo tramite web) ma non ha il diritto di operare sul dispositivo. Per abilitare l'utente, si deve settarne la password sulla configurazione web.

SERVIZI DI RETE

NetMan 204 implementa una serie di servizi basati sui principali protocolli di rete. Tali servizi possono essere attivati o disattivati in base alle necessità (vedere la sezione "Configurazione"). Di seguito viene fornita una breve descrizione dei vari servizi.

SSH

Un client SSH (disponibile su tutti i principali sistemi operativi) consente di stabilire una connessione remota con *NetMan 204* per modificarne la configurazione (vedere la sezione "Configurazione mediante SSH").

Rete seriale

Emulazione di una connessione seriale punto-punto tramite la rete (protocollo TCP/IP) per consentire l'uso di uno speciale software di assistenza.

Wake-on-LAN

NetMan 204 è in grado di inviare un comando di attivazione LAN ("Wake-on-LAN") per l'avvio di computer remoti.

HTTP

Il protocollo HTTP (Hyper Text Transfer Protocol) consente di configurare *NetMan 204* e di monitorare lo stato del dispositivo mediante un browser web senza dover installare altro software. Sono supportati tutti i principali browser web; è supportata solo la versione più recente dei browser.

SNMP

SNMP (Simple Network Management Protocol) è un protocollo di comunicazione che consente a un client (gestore) di inviare richieste a un server (agente). *NetMan 204* è un agente SNMP. Gestore e agente utilizzano una tecnica di indirizzamento denominata MIB (Management Information Base) per permettere lo scambio di informazioni. Per ciascun agente è disponibile un file MIB che definisce le variabili che è possibile richiedere e i rispettivi diritti di accesso. L'agente può inoltre inviare messaggi (TRAP) senza precedente richiesta da parte del gestore, per informare quest'ultimo di eventi particolarmente rilevanti. SNMPv3 è la versione evoluta di SNMP che introduce nuove caratteristiche importanti relative alla sicurezza.

UDP

UDP (User Datagram Protocol) è un protocollo di rete di basso livello che garantisce velocità di scambio dei dati e congestione ridotta della rete. È il protocollo utilizzato dal software UPSMon per il monitoraggio e il controllo del dispositivo.

La connessione UDP utilizza la porta UDP 33000 per impostazione predefinita, ma può essere configurata su altre porte in base alle necessità.

Modbus TCP/IP

Lo stato del dispositivo può essere monitorato mediante il protocollo di rete standard MODBUS TCP/IP. Modbus TCP/IP non è che il protocollo Modbus RTU con un'interfaccia TCP eseguita su Ethernet.

BACnet/IP

Lo stato del dispositivo può essere monitorato mediante il protocollo di rete standard BACnet/IP. BACnet (Building Automation and Control networks) è un protocollo di comunicazione di dati utilizzato principalmente nel settore industriale dell'automazione e della climatizzazione degli edifici.

FTP

FTP (File Transfer Protocol) è un protocollo di rete utilizzato per lo scambio di file. *NetMan 204* utilizza questo protocollo per:

1. scaricare i file dell'archivio storico dei valori e degli eventi (Datalog e Eventlog) del dispositivo;
2. scaricare e caricare file di configurazione;
3. aggiornare il firmware.

In entrambi i casi è richiesto un client FTP configurato con i seguenti parametri:

- Host: nome host o indirizzo IP di *NetMan 204*;
- Utente: vedere il capitolo "Utenti";
- Password: password corrente.

La connessione può inoltre essere stabilita utilizzando un browser web (sono supportati tutti i principali browser web), specificando il nome host o l'indirizzo IP di *NetMan 204*.

Servizio syslog

Netman 204 può inviare eventi ad un server syslog tramite UDP. Questo servizio consente di centralizzare i log dell'infrastruttura IT in un unico server, per poi essere consumati nel modo che si preferisce.

Servizio Email

NetMan 204 è in grado di inviare e-mail di notifica al verificarsi di determinate condizioni. Le e-mail possono essere inviate a un massimo di tre destinatari per sette tipi diversi di allarme. SMTP (Simple Mail Transfer Protocol) è il protocollo utilizzato per inviare le e-mail. La porta è configurabile. Per ulteriori dettagli, vedere la sezione "Configurazione".

Servizio Reports

NetMan 204 consente di inviare e-mail periodiche contenenti un allegato con i file dell'archivio storico dei valori e degli eventi.

Questo servizio può essere utilizzato per salvare periodicamente gli archivi storici.

Per consentire l'invio dei rapporti, è necessario che il servizio "Email" sia attivato; i rapporti vengono inviati a tutti gli indirizzi configurati per questo servizio (per ulteriori dettagli, vedere la sezione "Configurazione").

Client SSH (solo per sistema operativo W18-1 o successivo)

Se non è fattibile operare sui dispositivi con altri mezzi, è possibile eseguire uno script su di un host tramite SSH. Per maggiori dettagli, vedere la sezione "Configurazione".

ARCHIVIO STORICO DEI VALORI E DEGLI EVENTI DEL DISPOSITIVO

Netman 204 registra i valori (Datalog) e gli eventi (Eventlog) del dispositivo in un archivio storico.

Eventlog

Il servizio Eventlog è sempre attivo e registra tutti gli eventi di rilievo del dispositivo nel file "event.db". Il file può essere scaricato tramite FTP o visualizzato tramite la pagina web senza credenziali. Con il servizio "Email report", viene inviato per e-mail un file .csv con gli eventi del giorno o della settimana precedente in base alla configurazione. I dati vengono salvati in una modalità di elencazione circolare, in base alla quale i dati più recenti vengono memorizzati sostituendo i dati meno recenti.

Nella visualizzazione web, viene mostrate le seguenti icone nella colonna "type":

- un pallino rosso se l'evento è l'inizio di una condizione di allarme;
- un pallino verde se l'evento è la fine di una condizione di allarme;
- un pallino azzurro altrimenti

Datalog (solo per dispositivi UPS)

Il servizio Datalog registra i principali dati dell'UPS nel file "datalog.db".

Il servizio scrive un record ogni ora al minuto 0, che riassume i dati dell'ora precedente: vengono salvati i valori minimi, medi e massimi. I record più vecchi di un anno vengono sovrascritti dai nuovi. Il file può essere scaricato tramite FTP o visualizzato tramite la pagina web senza credenziali (vengono mostrati solo i valori più significativi).

Con il servizio "Email report", i record del giorno oppure della settimana precedente (in base alla configurazione) vengono inviati in formato .csv.

SENSORI AMBIENTALI (OPZIONALE)

È possibile collegare sensori ambientali a *Netman 204* per il monitoraggio di temperatura, umidità e I/O digitale.

Le informazioni fornite da questi sensori possono essere visualizzate mediante il software di monitoraggio e controllo del dispositivo o con un browser web.

I valori forniti dai sensori possono inoltre essere richiesti con SNMP in base allo standard RFC 3433 (file MIB disponibile sul sito internet).

Sensori disponibili

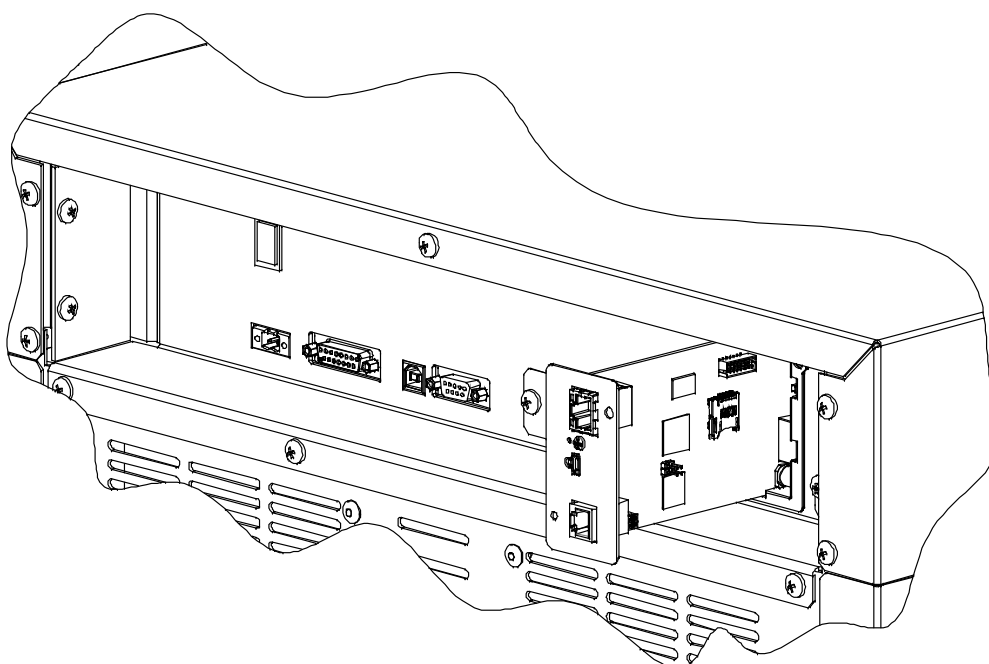
- **Temperatura:** rileva la temperatura ambientale in °C.
- **Umidità e temperatura:** rileva l'umidità relativa in % e la temperatura ambientale in °C.
- **I/O digitale e temperatura:** rileva la temperatura ambientale in °C e dispone di un ingresso e di un'uscita digitali.



È possibile collegare fino a 3 sensori ambientali a *Netman 204* (per l'installazione dei sensori, consultare il manuale dei sensori).

INSTALLAZIONE

1. Rimuovere il coperchio dello slot di espansione del dispositivo svitando le due viti di fissaggio.
2. Inserire *Netman 204* nello slot.
3. Fissare *Netman 204* nello slot con le due viti estratte in precedenza.
4. Collegare il dispositivo alla rete mediante il connettore RJ-45 (vedere "Specifiche di collegamento del cavo di rete").



CONFIGURAZIONE

PRESENTAZIONE

NetMan 204 può essere configurato mediante USB, SSH o HTTP.



Nella configurazione predefinita di fabbrica, *NetMan 204* viene fornito con DHCP attivato e con i seguenti servizi attivi: SSH, HTTP, SNMP, UDP e FTP.

Per modificare la configurazione di *NetMan 204*, è necessario accedere con il nome utente admin (password predefinita: "admin").

NetMan 204 richiede circa 2 minuti per diventare operativo dal momento in cui viene acceso o dopo un riavvio; durante questo tempo il dispositivo potrebbe non rispondere ai comandi impartiti.

Configurazione mediante HTTP/HTTPS

Per modificare la configurazione mediante HTTP/HTTPS, è necessario immettere nel browser web il nome host o l'indirizzo IP di *NetMan 204* e quindi accedere con il nome utente admin (password predefinita: "admin").



Il servizio HTTPS utilizza il protocollo TLS (Transport Layer Security) per fornire sicurezza mediante cifratura. Tuttavia, trattandosi di un'autocertificazione, il browser web potrebbe fornire un avviso di sicurezza; in questo caso, è possibile ignorare l'avviso e procedere alla configurazione di *NetMan 204*.

Al termine della procedura di accesso, è possibile spostarsi tra i menu per configurare *NetMan 204*.



Per rendere attiva la nuova configurazione, è necessario salvarla. Alcuni settaggi vengono applicati immediatamente, mentre altri richiedono un riavvio della *NetMan 204* (come suggerito dal popup sul web browser).

Configurazione mediante USB

Per configurare *NetMan 204* mediante USB, è necessario procedere come segue:

- Collegare con il cavo USB in dotazione la porta micro-USB alla porta USB di un PC dotato di sistema operativo Windows.
- Se non è stato installato in precedenza, installare il driver USB (dopo l'installazione del driver, il gestore del dispositivo presenta una porta COM virtuale denominata "NetMan 204 Serial").
- Eseguire un programma di emulazione di terminali con le seguenti impostazioni: COMn ⁽¹⁾, 115200 baud, nessuna parità, 8 bit di dati, 1 bit di stop, nessun controllo di flusso.

⁽¹⁾ COMn = porta COM assegnata a "NetMan 204 Serial" dal gestore del dispositivo.

- Premere il tasto "Invio" del PC.
- Alla richiesta del nome utente di accesso, immettere "admin".
- Alla richiesta della password, immettere la password corrente (password predefinita: "admin").



Durante la digitazione della password, non viene mostrato alcun carattere.

Al termine della procedura di accesso, viene visualizzata la schermata del menu iniziale. In questa schermata è possibile accedere ai vari menu per modificare le impostazioni di *NetMan 204* (vedere la sezione "Menu iniziale" e le sezioni successive).

Configurazione mediante SSH

Per configurare *NetMan 204* mediante SSH, è necessario procedere come segue:

- Eseguire un client SSH su un PC collegato in rete a *NetMan 204* impostato con l'indirizzo IP del dispositivo da configurare.
- Alla richiesta del nome utente di accesso, immettere "admin".
- Alla richiesta della password, immettere la password corrente (password predefinita: "admin").



Durante la digitazione della password, non viene mostrato alcun carattere.



Per una corretta configurazione di *Netman 204*, è necessario impostare il SSH in modo che il tasto Backspace invii "Control-H".
Verificare le opzioni di tastiera del client SSH.

Al termine della procedura di accesso, viene visualizzata la schermata del menu iniziale. In questa schermata è possibile accedere ai vari menu per modificare le impostazioni di *NetMan 204* (vedere la sezione "Menu iniziale" e le sezioni successive).

DESCRIZIONI DEI MENU DI CONFIGURAZIONE

Menu iniziale

Al termine della procedura di accesso tramite SSH o USB, viene visualizzata una schermata come la seguente:

```
Netman 204

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

inet 10.1.30.68 netmask 255.255.0.0 broadcast 10.1.255.255

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

Funzione	Descrizione
Setup	Per accedere al menu di configurazione principale
View status	Per verificare lo stato del dispositivo
Change password	Per modificare la password (vedere anche Recupero della password)
Service log	Per generare un file di registro della scheda (se richiesto dall'assistenza)
Wi-Fi setup	Per configurare la connessione Wi-Fi Per la connessione Wi-Fi, è richiesta una scheda opzionale. La scheda Wi-Fi non è fornita in dotazione con <i>NetMan 204</i> e deve essere acquistata separatamente.
Factory reset	Ripristino della configurazione di fabbrica
Expert mode	Per accedere alla modalità Expert (per ulteriori informazioni, vedere la sezione " <i>Modalità Expert</i> ")

Per spostarsi all'interno di questo menu e dei menu successivi, utilizzare i tasti indicati nella seguente tabella; la freccia o il cursore mostra la selezione corrente.

Tasto	Funzione
Tasti di direzione (freccia su, giù, destra, sinistra)	Per spostare il cursore all'interno dei menu
Tab	Per passare all'opzione successiva
Invio ⁽¹⁾	Per scegliere un sottomenu
	Per confermare i caratteri immessi
Esc ⁽¹⁾	Per uscire dal menu principale ⁽²⁾
	Per ritornare al menu precedente

⁽¹⁾ Alcuni tasti possono svolgere una funzione diversa a seconda del menu.

⁽²⁾ All'uscita da un menu, è richiesta una conferma ("Y" per sì o "N" per no) dopo avere premuto il tasto ESC.

Setup

Il menu di configurazione principale visualizza una schermata come la seguente:

```
Setup

IP config.....:<--
Wi-Fi setup....:
Enable Sensors.:
Sensors Config.:
Expert mode....:
Factory reset..:
Reboot.....:

Press [Esc] to quit
SysVer. S16-1 - AppVer. 02.01.000
```

In questo menu principale è possibile accedere a vari sottomenu, le funzioni di ciascuno dei quali sono illustrate nella seguente tabella.

Menu	Funzione
IP config	Per configurare i parametri di rete
Wi-Fi setup	Per configurare la connessione Wi-Fi Per la connessione Wi-Fi, è richiesta una scheda opzionale. La scheda Wi-Fi non è fornita in dotazione con <i>Netman 204</i> e deve essere acquistata separatamente.
Enable sensors	Per abilitare il servizio sensori ambientali
Sensors config	Per configurare i sensori ambientali
Expert mode	Per accedere alla modalità Expert (per ulteriori informazioni, vedere la sezione " <i>Modalità Expert</i> ")
Factory reset	Ripristino della configurazione di fabbrica
Reboot	Riavvia la <i>Netman 204</i>

IP config

```

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

IP config

Hostname.....:ups-server

IP address/DHCP:DHCP

Netmask.....:

Gateway.....:

Primary DNS...:

Secondary DNS..:

```

Questo menu consente di impostare i principali parametri di rete, come descritto nella seguente tabella.

Campo	Parametri da immettere
Hostname	Immettere il nome host <i>NetMan 204</i>
IP address/DHCP	Immettere l'indirizzo IP per un IP statico; immettere "DHCP" per un IP dinamico
Netmask	Immettere il netmask da usare insieme all'indirizzo IP statico
Gateway	Immettere il nome o l'indirizzo del gateway di rete
Primary DNS	Immettere il nome o l'indirizzo del DNS preferito da utilizzare
Secondary DNS	Immettere il nome o l'indirizzo del DNS alternativo da utilizzare



Se viene assegnato un indirizzo IP statico al dispositivo, è necessario configurare tutti i campi con i parametri di rete. Se viene assegnato un indirizzo IP dinamico, è sufficiente immettere "dhcp" nel campo "IP Address/DHCP" e indicare un nome host; ignorare tutte le altre opzioni, le quali vengono configurate automaticamente con DHCP.

Dopo avere premuto "ESC" e "Y" per confermare l'uscita dal menu, viene visualizzata una schermata come quella riportata qui sotto. Premere il tasto "INVIO" per ritornare al menu principale e la configurazione sarà resa efficace immediatamente.

```

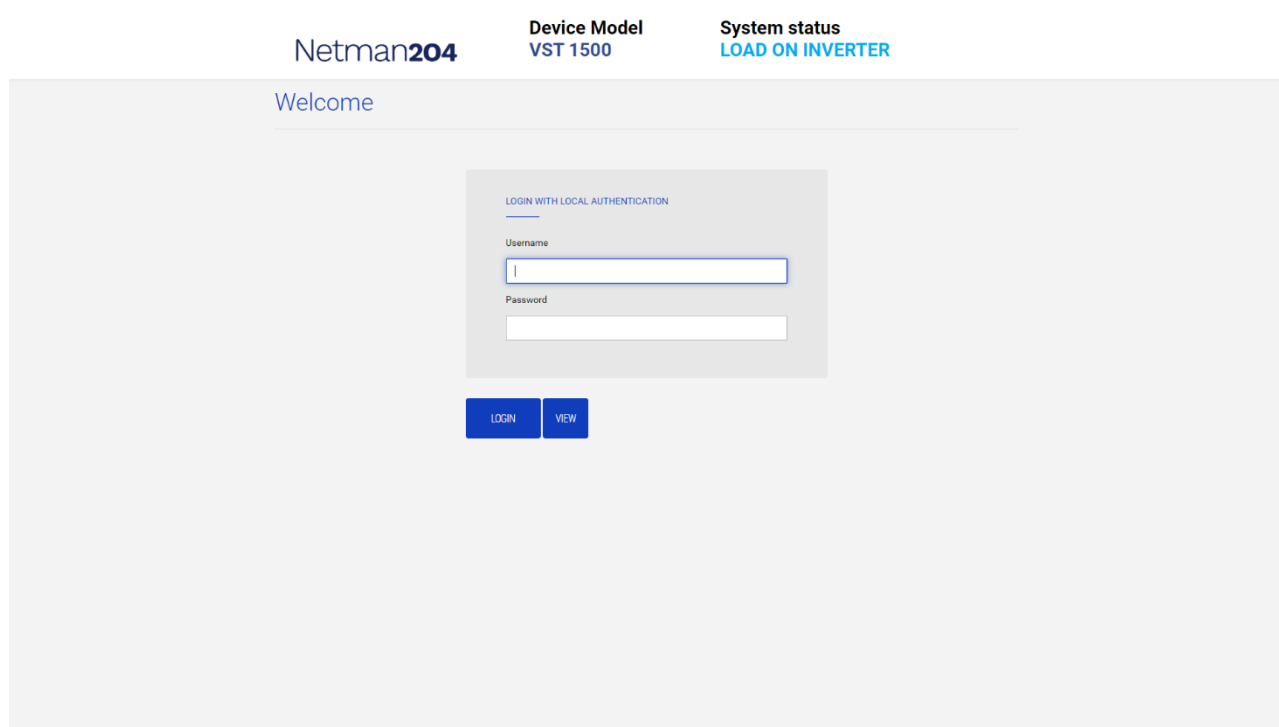
eth0      Link encap:Ethernet  Hwaddr 00:02:63:04:07:b1
          inet addr:10.1.11.19  Bcast:10.1.255.255  Mask:255.255.0.0
          inet6 addr: fe80::202:63ff:fe04:7b1/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:145877 errors:0 dropped:0 overruns:0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

```

CONFIGURAZIONE WEB

Login

Dopo aver configurato la rete, tutti i settaggi sono disponibili sulla configurazione web se viene effettuato l'accesso come utente "admin" oppure "power". Non è possibile avere più sessioni concorrenti.



The screenshot shows the Netman204 web interface. At the top, there is a header with 'Netman204' on the left, 'Device Model VST 1500' in the center, and 'System status LOAD ON INVERTER' on the right. Below the header, there is a 'Welcome' message. The main content area contains a login form titled 'LOGIN WITH LOCAL AUTHENTICATION'. The form has two input fields: 'Username' and 'Password'. Below the form are two buttons: 'LOGIN' and 'VIEW'.



La password di login deve essere contenere caratteri alfanumerici ed i seguenti caratteri speciali: `, . _ + : @ % / -`. Nessun altro carattere è consentito per evitare attacchi "script injection".

Si prega di notare che gli utenti "fwupgrade" e "user" non possono eseguire il login sulla pagina web. Si usi l'utente "admin", "power", oppure si entri senza password.

- L'utente admin può modificare la configurazione e operare sul dispositivo
- L'utente power può modificare la configurazione ma non può operare sul dispositivo
- Entrando senza password si può vedere lo stato del dispositivo; nessun'altra azione è consentita

Welcome

LOGIN WITH

LDAP authentication

Username

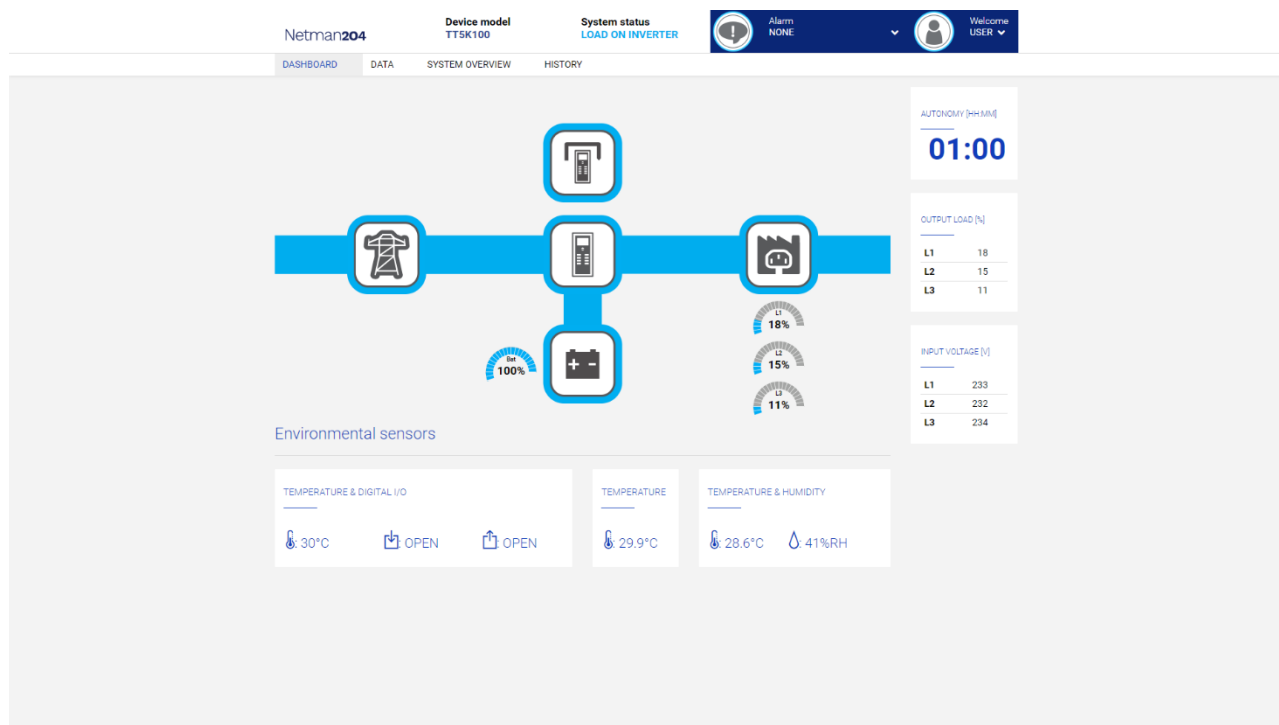
john

Password

LOGIN VIEW

E' possibile eseguire il login con l'autenticazione locale (gestita dalla *Netman 204*) oppure centralmente tramite LDAP o AD (maggiori informazioni al paragrafo "Autenticazione").

Dashboard

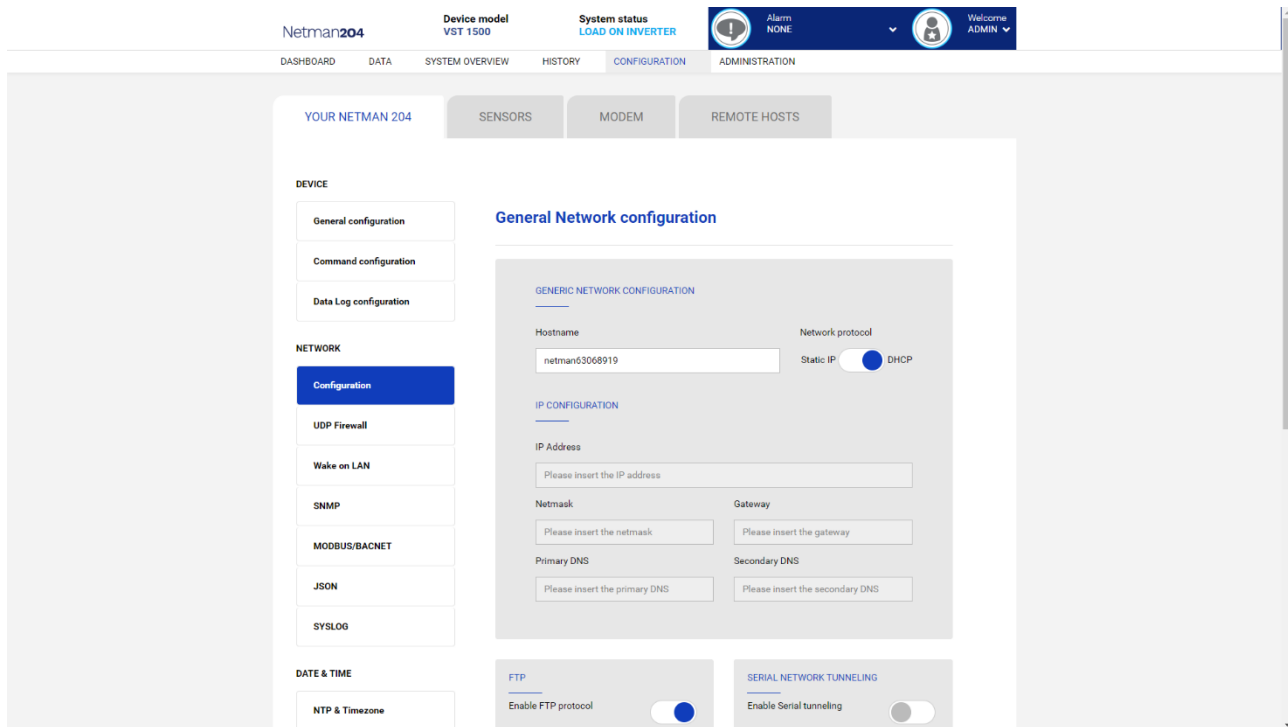


Nell'area in alto è possibile controllare lo stato generale del dispositivo, tutti le condizioni di allarme attive ed il livello di privilegio dell'utente.

Sotto l'area di navigazione è presente la dashboard vera e propria con uno schema sintetico del dispositivo ed i principali valori di funzionamento.

In basso, sono presenti i valori dei sensori ambientali (se installati e configurati).

Configurazione di rete

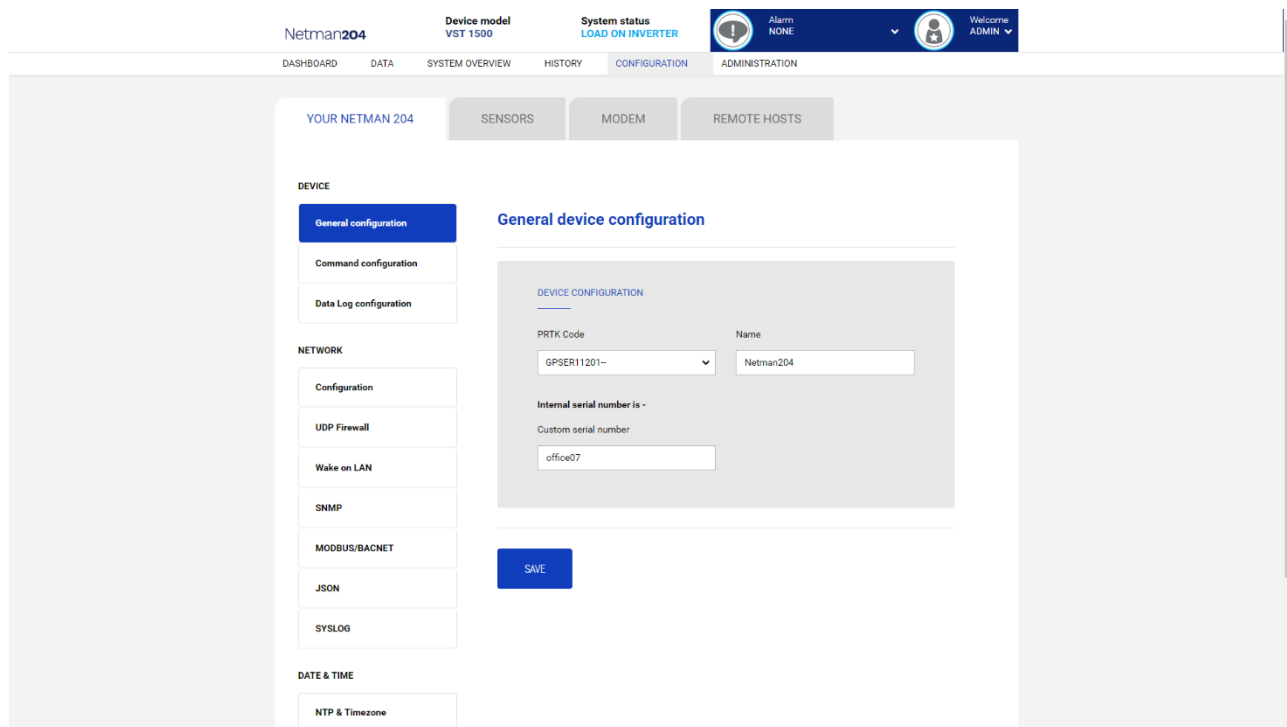


Sulla pagina web è possibile configurare tutti i servizi di rete della *Netman 204*.

Campo	Parametri da immettere
Hostname	Immettere il nome host <i>NetMan 204</i>
Static IP/DHCP	Scegliere tra indirizzo IP statico o dinamico
IP Address	Immettere l'indirizzo IP
Netmask	Immettere il netmask da usare insieme all'indirizzo IP statico
Gateway	Immettere il nome o l'indirizzo del gateway di rete
Primary DNS	Immettere il nome o l'indirizzo del DNS preferito da utilizzare
Secondary DNS	Immettere il nome o l'indirizzo del DNS alternativo da utilizzare
Enable FTP protocol	Abilita il servizio FTP
Enable Serial network tunneling	Abilita il protocollo serial network tunnelling
Enable UDP	Abilita il servizio UDP/UPSMon
UDP port	Immettere la porta per il servizio UDP/UPSMon ⁽¹⁾
UDP Password	Cambiare la password usata per la comunicazione UDP/UPSMon

⁽¹⁾ Questa porta deve corrispondere a quella configurata nel software UPSMon.

Configurazione del dispositivo



Campo	Parametri da immettere
PRTK Code	Immettere il codice PRTK indicato sul pannello posteriore del dispositivo
Name	Immettere il nome di identificazione del dispositivo
Custom serial number	Immettere un serial number che andrà a sovrascrivere il default

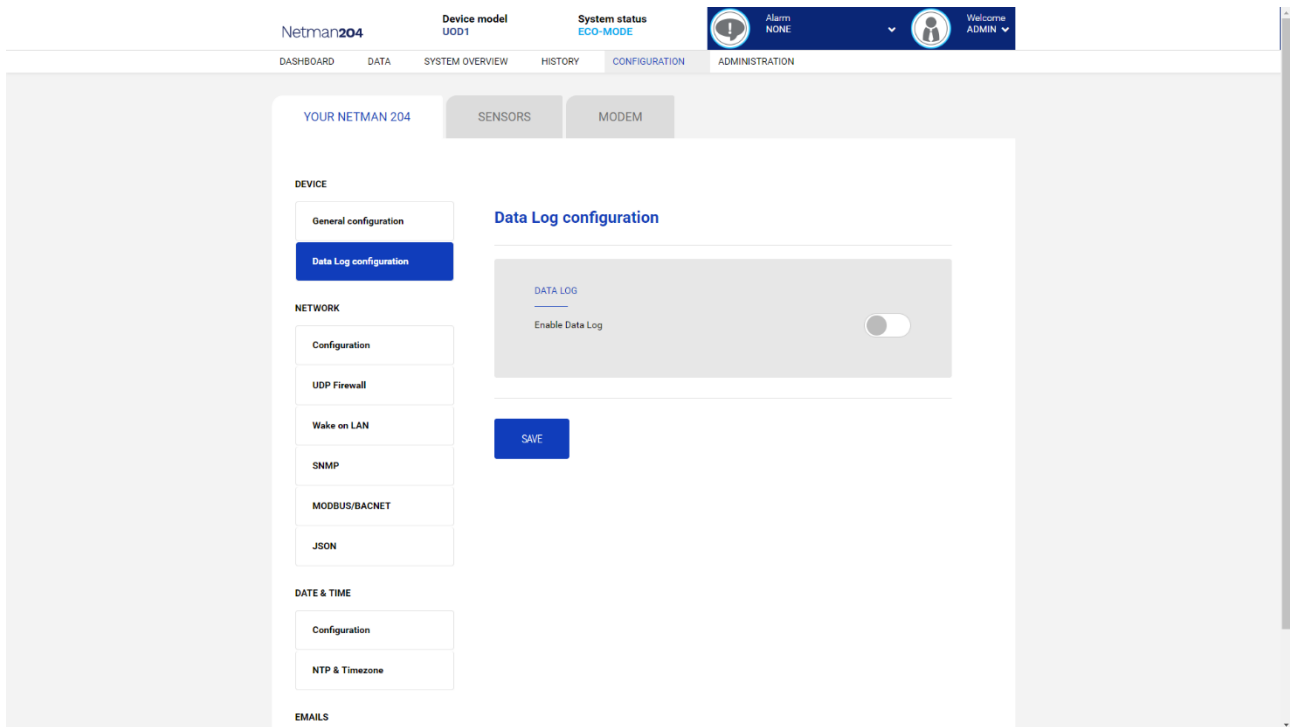
Configurazione comandi remoti

The screenshot displays the 'Command configuration' page in the Netman204 interface. The page is titled 'YOUR NETMAN 204' and has tabs for 'SENSORS' and 'MODEM'. The 'COMMAND' section contains two toggle switches: 'Disable remote shutdown' and 'Disable remote commands', both of which are currently turned off. A 'SAVE' button is located below the toggles. The left sidebar shows a navigation menu with categories: DEVICE (General configuration, Command configuration, Data Log configuration), NETWORK (Configuration, UDP Firewall, Wake on LAN, SNMP, MODBUS/BACNET, JSON, SYSLOG), and REMOTE HOSTS SHUTDOWN (SSH). The top navigation bar includes 'DASHBOARD', 'DATA', 'SYSTEM OVERVIEW', 'HISTORY', 'CONFIGURATION', and 'ADMINISTRATION'. The top right corner shows 'Alarm NONE' and 'Welcome ADMIN'.

Questi settaggi disabilitano l'esecuzione di comandi ricevuti dai servizi di connettività remota: SNMP, MODBUS ecc.

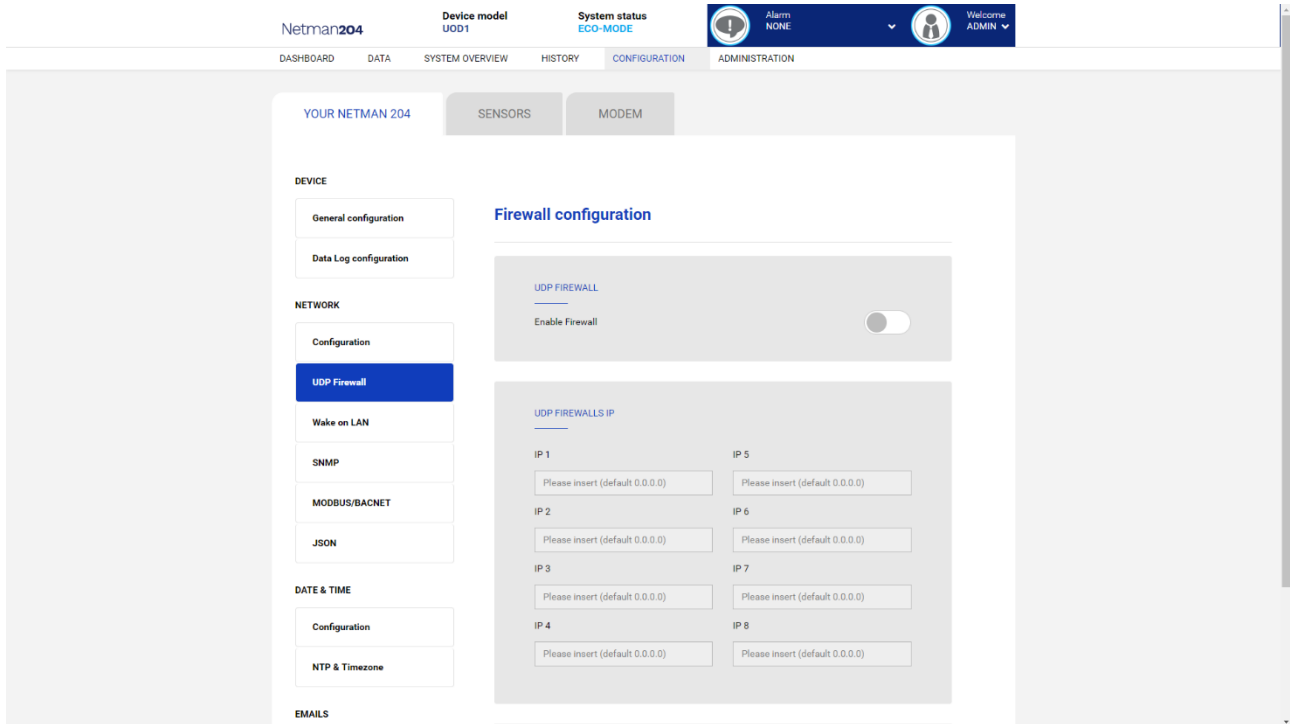
Campo	Parametri da immettere
Disable remote shutdown	Disabilita l'esecuzione di comandi shutdown
Disable remote commands	Disabilita l'esecuzione di tutti gli altri comandi

Data log



Campo	Parametri da immettere
Enable Data log	Abilita il servizio datalog
Backup UPS data log at boot	All'avvio <i>NetMan 204</i> scarica il datalog del dispositivo per un accesso veloce

Firewall UDP



Questo menu consente di configurare gli indirizzi IP o i nomi host dei dispositivi abilitati alla comunicazione con *Netman 204*. Il numero **255** può essere utilizzato per uno o più campi dell'indirizzo IP per indicare che tutti i valori compresi tra 0 e 255 sono accettati nel campo. Nella seguente tabella sono forniti alcuni esempi di configurazione possibile.

Accesso IP	Descrizione
255.255.255.255	Tutti i dispositivi presenti in rete sono abilitati alla comunicazione con <i>Netman 204</i> (configurazione predefinita)
10.1.10.255	I dispositivi con indirizzi compresi tra 10.1.10.0 e 10.1.10.255 sono abilitati alla comunicazione con <i>NetMan 204</i>
myserver.mydomain	Nome host del dispositivo abilitato alla comunicazione con <i>Netman 204</i>

Indirizzi Wake-On-LAN

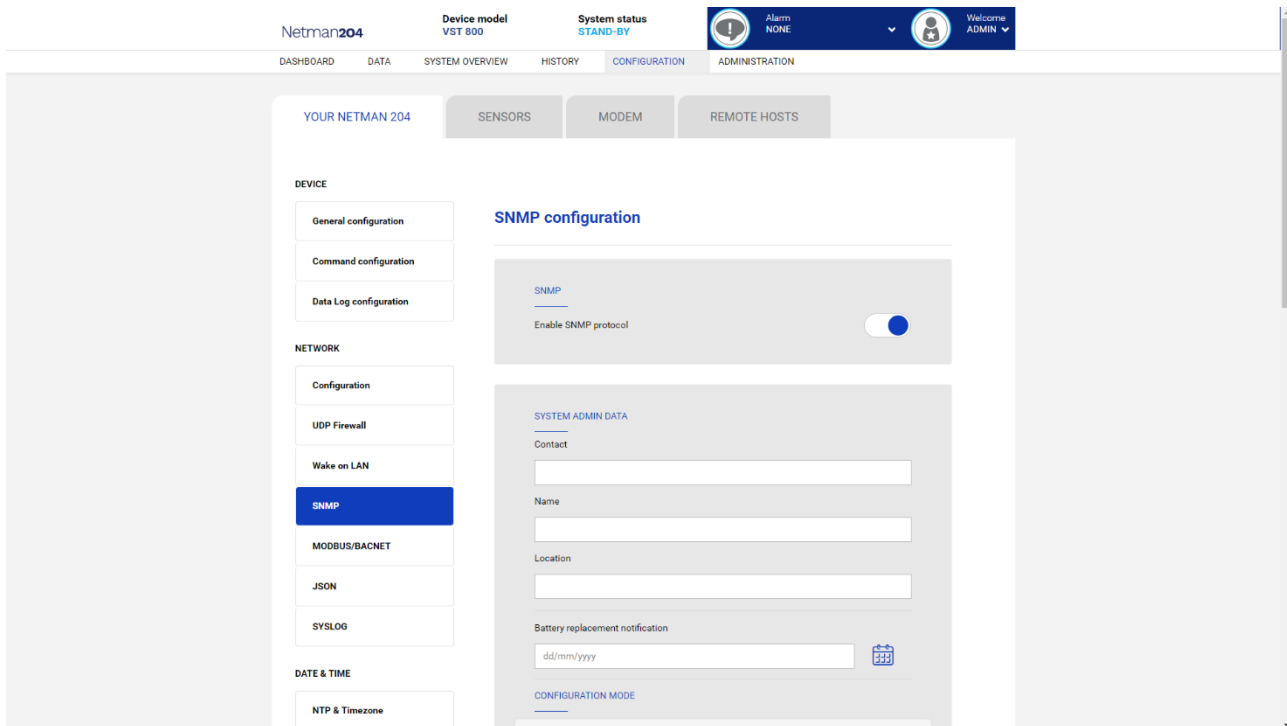
The screenshot shows the Netman204 configuration interface. The top navigation bar includes 'Netman204', 'Device model UOD1', 'System status ECO-MODE', and 'Alarm NONE'. The main menu includes 'DASHBOARD', 'DATA', 'SYSTEM OVERVIEW', 'HISTORY', 'CONFIGURATION', and 'ADMINISTRATION'. The left sidebar lists configuration categories: 'YOUR NETMAN 204', 'SENSORS', and 'MODEM'. Under 'YOUR NETMAN 204', there are sections for 'DEVICE' (General configuration, Data Log configuration), 'NETWORK' (Configuration, UDP Firewall, Wake on LAN, SNMP, MODBUS/BACNET, JSON), 'DATE & TIME' (Configuration, NTP & Timezone), and 'EMAILS'. The 'Wake on LAN' configuration page is active, showing a toggle for 'Enable Wake On Lan' and a table for 'MAC ADDRESSES & DELAY' with five rows for MAC addresses and their corresponding delays.

Questo menu consente di immettere fino a 8 indirizzi MAC per l'esecuzione di Wake-on-LAN, ed i tempi di ritardo per ciascun Wake-on-LAN. Il Wake-on-LAN è inviato all'avvio della *NetMan 204* e quanto la rete ritorna dal black-out.



Accertarsi che il PC utilizzato supporti questa funzione e che sia configurato correttamente.

SNMP



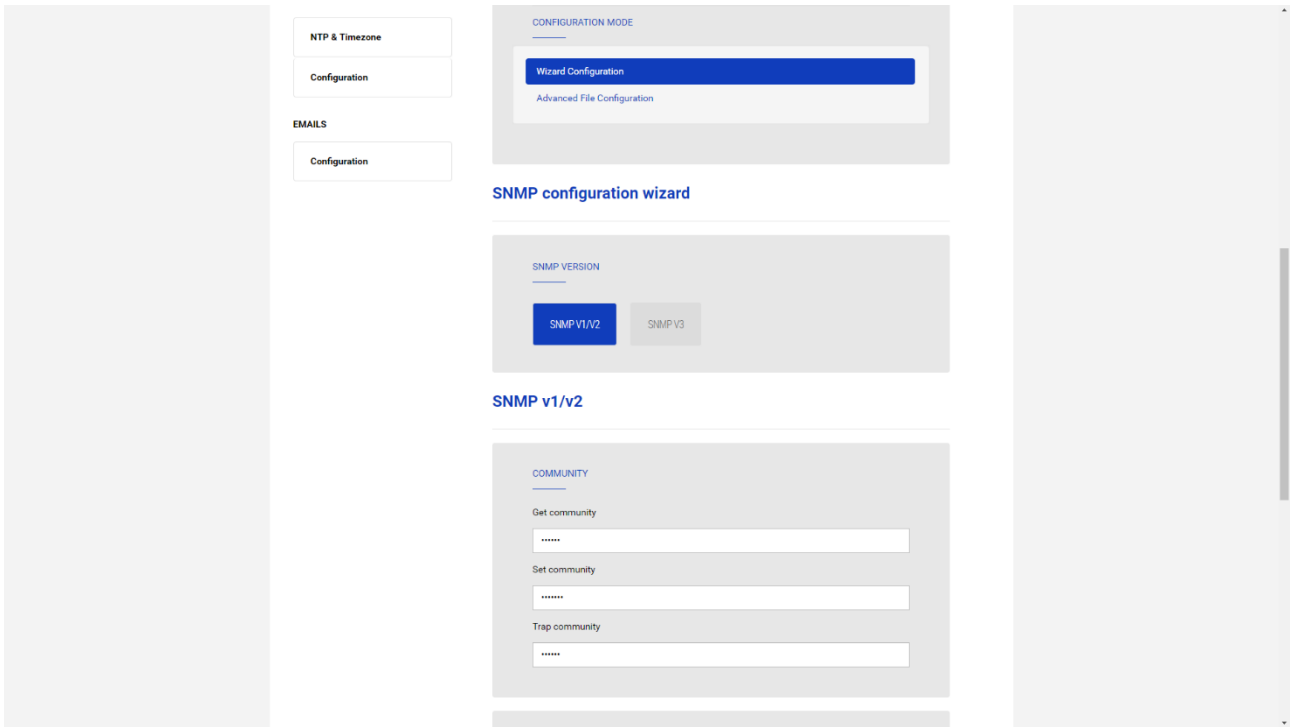
SNMP (Simple Network Management Protocol) è un protocollo di comunicazione, ovvero uno strumento che consente ad un client (manager) di effettuare richieste ad un server (agent). Questo protocollo è uno standard internazionale e per questo motivo qualunque manager SNMP può dialogare con qualunque agent SNMP.

Per scambiare informazioni manager e agent utilizzano una tecnica di indirizzamento che prende il nome di MIB (Management Information Base). Il MIB definisce quali variabili possono essere richieste e i rispettivi diritti di accesso. Il MIB è dotato di una struttura ad albero (come le cartelle presenti in un hard disk), per cui manager e agent possono usare contemporaneamente più MIB, in quanto non c'è alcuna sovrapposizione.

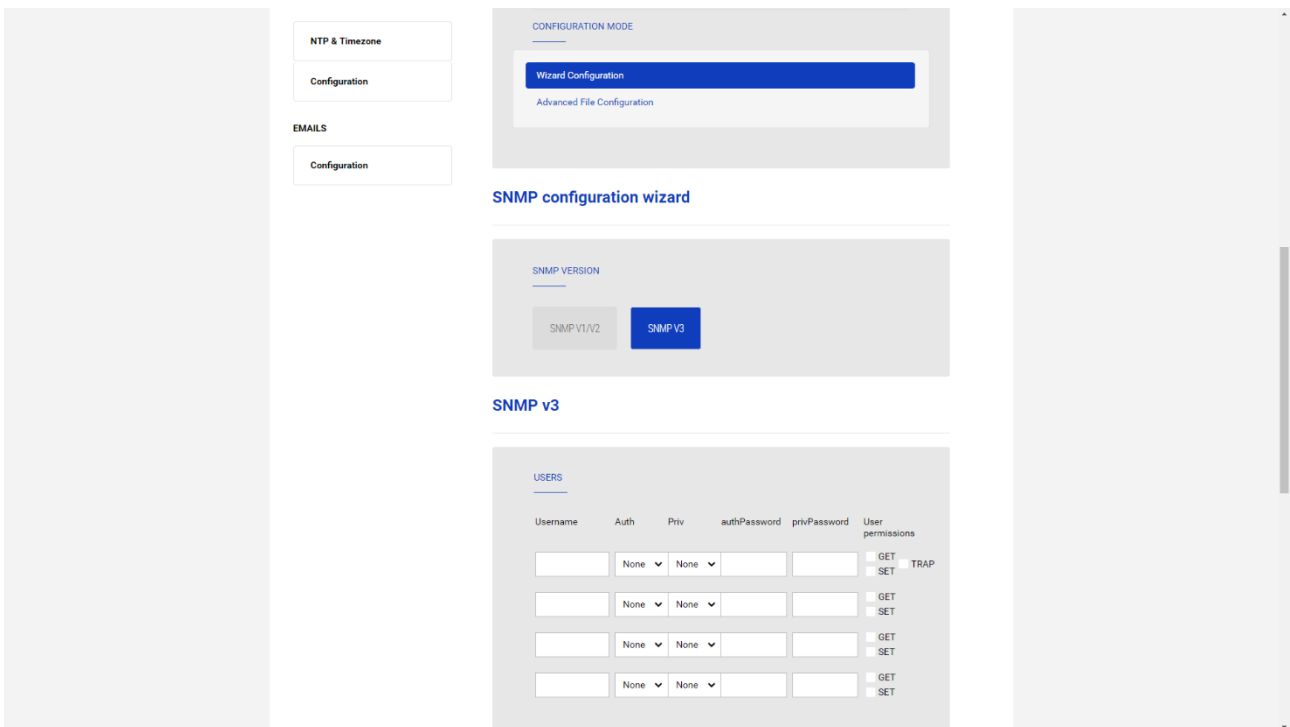
Ogni MIB è orientato ad un particolare settore, in particolare RFC-1628 detto anche UPS-MIB contiene i dati per la gestione remota di UPS.

L'agent può inoltre inviare informazioni senza una precedente richiesta, per informare il manager di eventi di particolare importanza. Tali messaggi si chiamano trap.

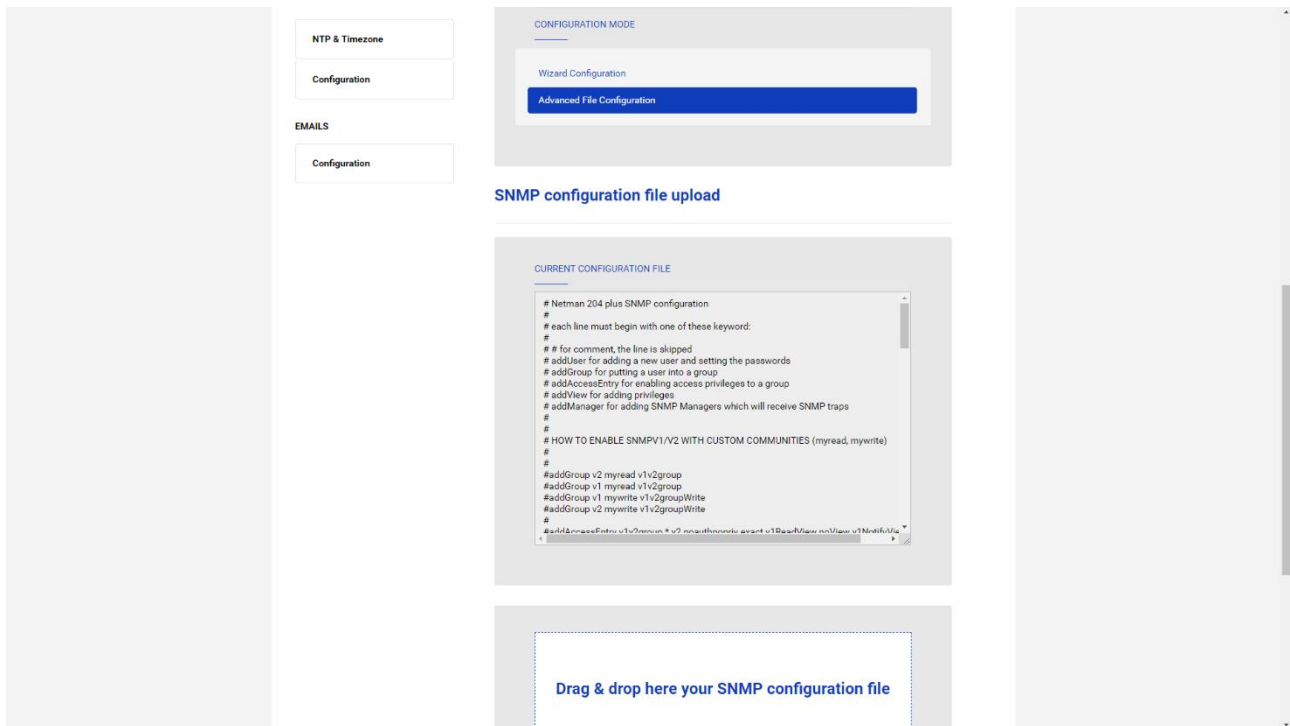
Per maggiori informazioni su SNMP si veda il sito <http://www.snmp.com>.



Per configurare SNMP è possibile usare il wizard da pagina web per una configurazione semplice. Il wizard fornisce una configurazione standard che copre la maggior parte dei casi d'uso per SNMPv1/v2.



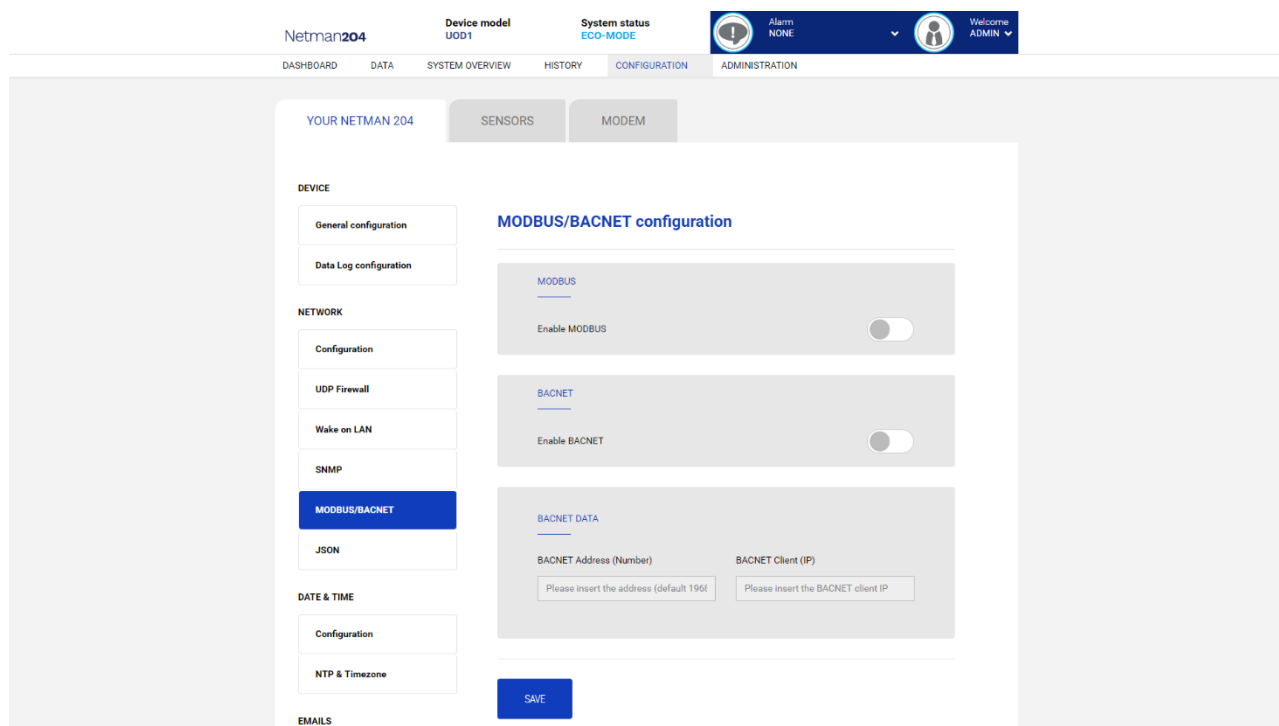
Quando è richiesta una sicurezza aggiuntiva attraverso l'autenticazione e la crittografia, è consigliabile usare SNMPv3 con la configurazione wizard.



Per la configurazione avanzata è necessario editare il file `snmp.conf` (maggiori informazioni al capitolo “Configurazione SNMP”).

Campo	Parametri da immettere
Enable SNMP protocol	Abilita il servizio SNMP
Contact	Immettere la stringa da associare a queste variabili SNMP
Name	Immettere la stringa da associare a queste variabili SNMP
Location	Immettere la stringa da associare a queste variabili SNMP
Battery replacement notification	Immettere la data in cui essere notificati che la batteria va sostituita
Configuration mode	Scelta tra la configurazione wizard oppure caricamento di un file di configurazione
SNMP version	Scelta tra SNMPv1/v2 o SNMPv3
Get community	Immettere la comunità per l'accesso alla lettura
Set community	Immettere la comunità per l'accesso alla scrittura
Trap community	Immettere la comunità per l'invio di trap
Trap receiver	Immettere l'indirizzo IP a cui inviare le trap
Username	Inserire lo username USM
Auth	Inserire l'algoritmo di autenticazione
Priv	Inserire l'algoritmo di privacy
AuthPassword	Inserire la password di autenticazione
PrivPassword	Inserire la password di privacy
Permissions	Scelta dei permessi per ciascun utente

MODBUS/BACNET

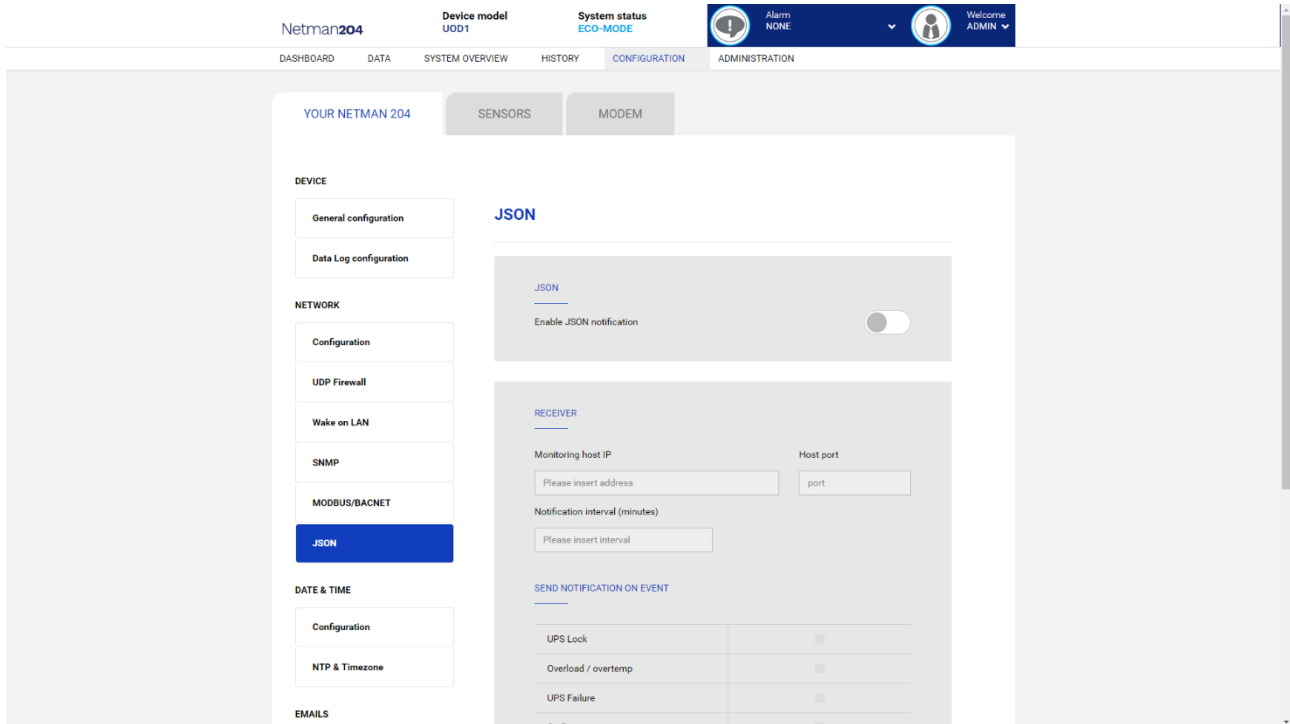


Per maggiori informazioni riguardo ai registri MODBUS, si rimanda alla sezione “Protocollo MODBUS TCP/IP”.

Per maggiori informazioni riguardo BACNET, si manda alla sezione “Configurazione BACNET/IP”.

Campo	Parametri da inserire
Enable MODBUS	Abilita il protocollo MODBUS
Enable BACNET	Abilita il protocollo BACNET
BACNET Address (Number)	Inserire l'indirizzo BACNET del dispositivo
BACNET Client (IP)	Inserire l'indirizzo IP del client BACNET

JSON



Netman 204 può inviare una trap periodica in formato JSON che contiene lo stato ed i valori dell'UPS. La trap può essere inviata nelle condizioni specificate.

Campo	Parametri da inserire
Enable JSON	Abilita il servizio notifiche JSON
Monitoring host IP	Inserire l'indirizzo IP a cui inviare le trap JSON
Host port	Inserire la porta a cui inviare le trap
Notification interval (minutes)	Inserire l'intervallo tra l'invio di trap JSON
Send notification on event	Scelta degli eventi per i quali viene inviata la trap

Richiede un file `license.txt` da caricare sulla *Netman 204*. Il contenuto del file sarà incluso nella trap.

Trap di esempio:

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

timestamp è l'istante della trap espresso come *Unix epoch*.

model è una stringa che identifica il modello dell'UPS.

io_conf è la configurazione dell'UPS; alcuni valori dipendono da essa (vedi note).

license è il contenuto del file di licenza.

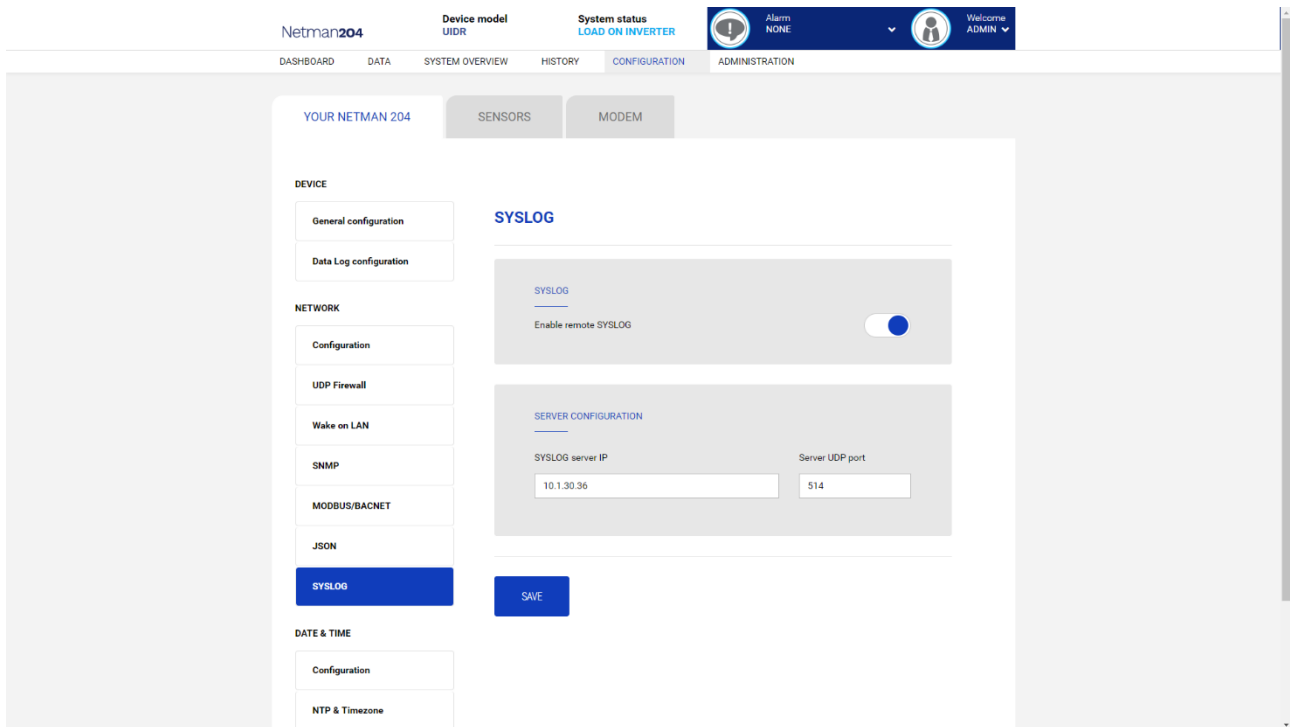
status è un array che va interpretato come segue:

byte	bit	Descrizione
0	0	UPS Maintenance
	1	Communication lost
	2	Battery low
	3	Battery working
	4	On bypass
	5	UPS Failure
	6	Overload/Overtemperature
	7	UPS Locked
1	0	SWIN Open/Battery Low
	1	SWBYP Open/Battery Working
	2	SWOUT Open/UPS Locked
	3	Output Powered
	4	SWBAT Open

	5	SWBAT_EXT Open
	6	Battery not present
	7	Battery overtemperature
2	0	Buck Active
	1	Boost Actived
	2	O.L./L.I. function
	3	Load threshold exceeded/On Bypass
	4	EPO command active
	5	BYPASS command active
	6	Service UPS
	7	Service battery
3	0	Replace Battery
	1	Battery Charged
	2	Battery Charging
	3	Bypass Bad
	4	Low redundancy
	5	Lost redundancy
	6	System anomaly
	7	
4	0	Bypass backfeed/Beeper On
	1	Test in progress
	2	Shutdown Imminent
	3	Shutdown Active
	4	PM1 fault/lock
	5	PM2 fault/lock
	6	PM3 fault/lock
	7	PM4 fault/lock
5	0	PM5 fault/lock
	1	Alarm Temperature
	2	Alarm Overload
	3	PM6 fault/lock
	4	PM7 fault/lock
	5	BM fault/lock
	6	Power supply PSU fail
	7	Battery unit anomaly

measures, contiene i valori delle misure analogiche dell'UPS al momento del timestamp. Le misure con nota (1) non sono significative se **io_conf** vale 1, quelle con nota (2) non sono significative se **io_conf** vale 1 o 3.

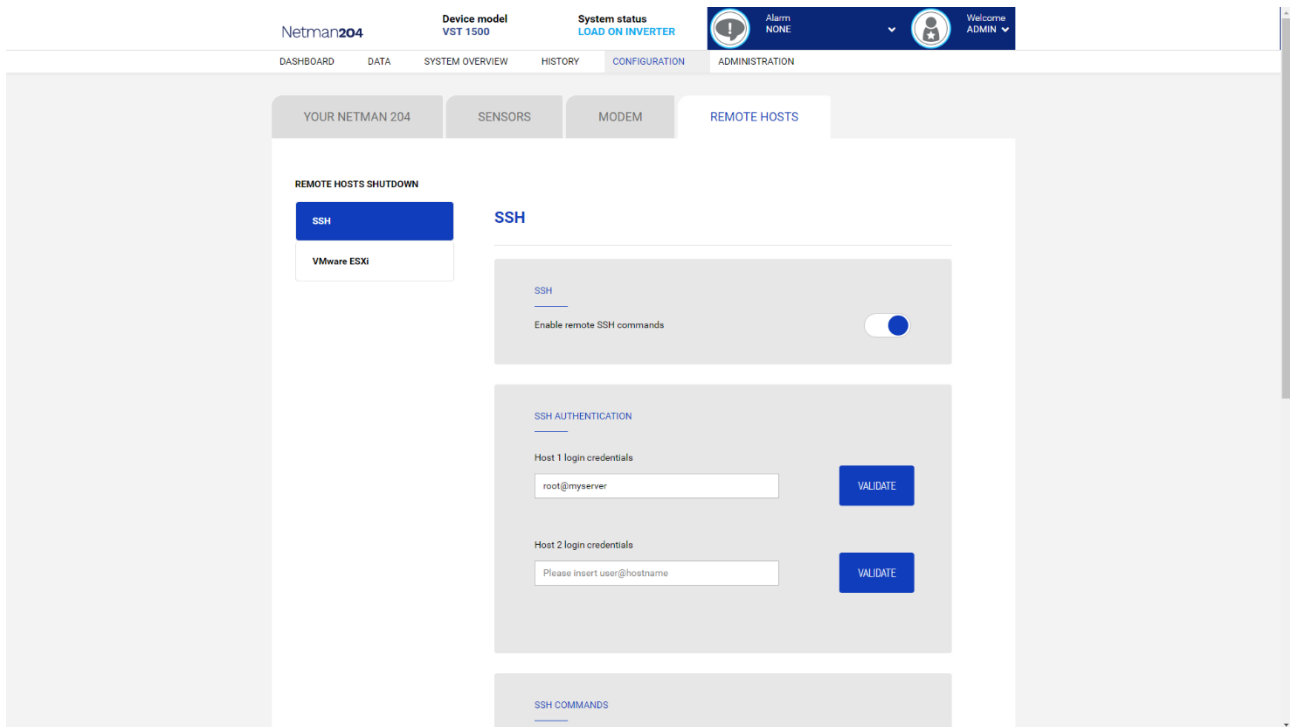
Configurazione syslog



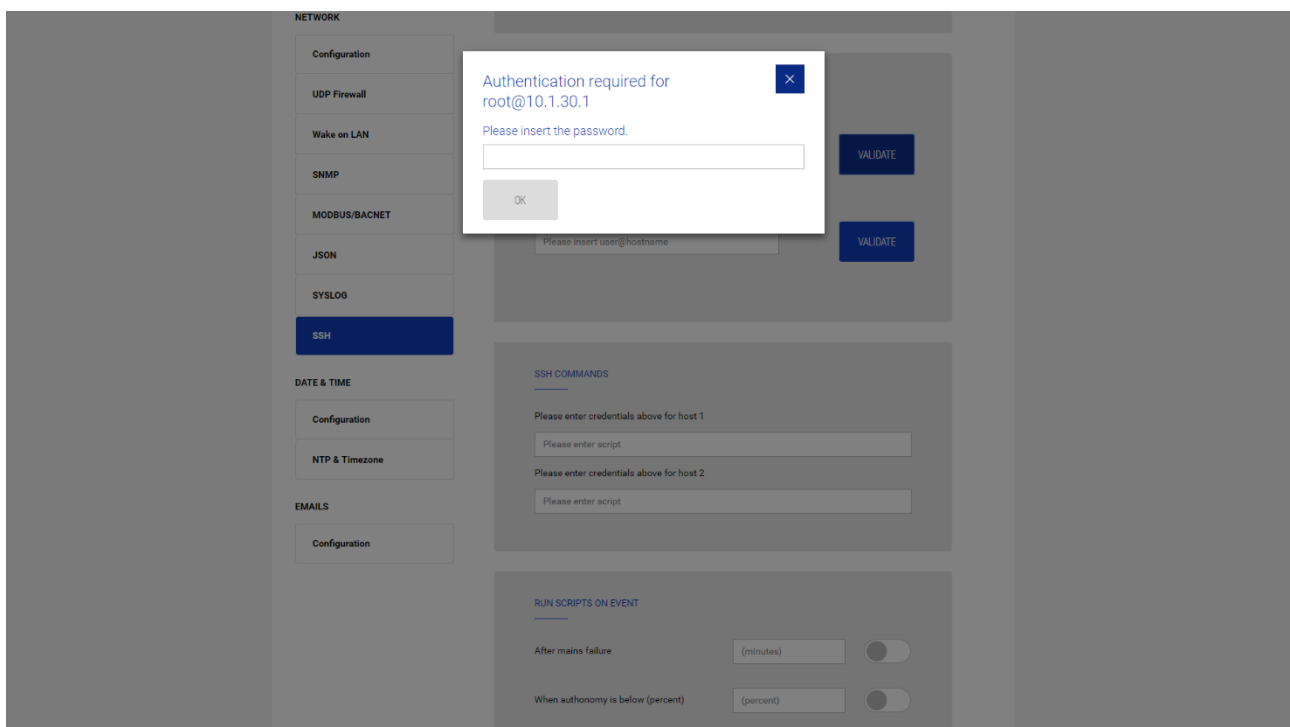
Questo menu consente di configurazione il servizio syslog su porta UDP.

Campo	Parametri da inserire
Enable remote syslog	Abilita il servizio syslog
Syslog server IP	Inserire l'indirizzo IP del server syslog
Server UDP port	Inserire la porta UDP a cui inviare gli eventi

Configurazione client SSH (solo per sistema operativo W18-1 or successivo)



Questo menu consente di configurare il servizio client SSH. Dopo aver inserito le credenziali SSH per la prima volta verrà chiesta la password di autenticazione per l'host remoto.



Dopo aver inserito una password valida, sarà possibile eseguire script sull'host remoto con l'utente autenticato. A titolo di conferma viene mostrato il badge "Validated".



Il servizio client SSH non è compatibile con gli host dotati di sistemi operativi Windows. Con questi host consigliamo l'installazione del software di comunicazione e shutdown, dotato di funzionalità simili o superiori.

Campo	Parametri da inserire
Enable remote SSH commands	Abilita il servizio client SSH
Host 1 login credentials	Inserire le credenziali SSH per l'host 1
Host 2 login credentials	Inserire le credenziali SSH per l'host 2
SSH commands	Inserire lo script da eseguire per ciascun host
After mains failure	Gli script saranno eseguiti dopo i minuti settati dopo un blackout in ingresso
When autonomy is below (percent)	Gli scripts saranno eseguiti quando l'autonomia è al di sotto della percentuale settata
Minimum delay between execution (minutes)	Cooldown per l'esecuzione degli script per prevenire l'esecuzione di script entro il periodo inserito

VMware ESXi

Host or VCSA	Username	Password	
vcsa.local	Administrator@vsphere.lc	Delete
hostbk.local	root	Delete

[Add Row](#)

Questo menu permette di configurare lo shutdown sui sistemi VMware Esxi. Qualunque host ESXi o parte di una infrastruttura vSphere o il vCenter server appliance incluso possono essere spenti; è possibile eseguire una vMotion per muovere VM attive da un host oppure un Cluster verso un target specifico ciascuno con le proprie credenziali, priorità e ritardo.

La validità delle credenziali è testata periodicamente e, se non valida, viene presentato un allarme. E' inoltre possibile eseguire lo shutdown dell'UPS alla fine.



ATTENZIONE

L'infrastruttura VMware deve essere installata con una licenza valida; una licenza gratuita non funzionerà in modo appropriato: a causa di limitazioni di accesso delle API le macchine virtuali ed i server fisici non possono essere spenti per limiti del sistema.

Lo slider "Enable ESXi shutdown" abilita il servizio shutdown ESXi.

Infrastructure connectors

Campo	Parametri da inserire
Host or VCSA	Inserire l'hostname dell'host ESXi o della VCSA
Username	Inserire lo user name dell'amministratore ESXi
Password	Inserire la password dell'amministratore ESXi

Actions

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

Add Row

SHUTDOWN ON EVENT

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

Then, UPS shutdown after (seconds)

2



SAVE

Azioni

Campo	Parametri da inserire
Action	<p>L'azione da eseguire:</p> <p>Shutdown VM eseguirà lo shutdown della VM specifica</p> <p>Shutdown Host eseguirà lo shutdown di tutte le VM attive nell'host specificato e poi sull'host stesso</p> <p>Shutdown Cluster eseguirà lo shutdown di tutte le VM attive nel cluster specificato e degli host che ne fanno parte</p> <p>VMotion farà una "move" delle VM attive da un host sorgente ad un host target</p> <p>Maintenance forzerà l'host in modalità maintenance</p>

Condition	<p>Specifica l'evento scatenante:</p> <p>Power fail: quando l'UPS rileva una mancanza rete, inizierà il conto alla rovescia con il tempo configurato (minuti). Una volta trascorso il tempo, verrà avviata l'azione selezionata. Se la rete ritorna entro questo tempo, l'azione verrà annullata.</p> <p>Autonomy less: quando l'autonomia calcolata della batteria dell'UPS scende al di sotto del tempo configurato (minuti) si avvia l'azione selezionata. Se la rete ritorna entro questo tempo, l'azione verrà annullata.</p>
Condition duration (minutes)	Il tempo per il quale la condizione selezionata (Interruzione di alimentazione o Autonomia inferiore) attiva l'azione selezionata.
Delay next (seconds)	Ritardo in secondi prima di eseguire l'azione successiva
Source	<p>Se selezionato Shutdown host, VMotion oppure Maintenance: va specificato un hostname o indirizzo IP raggiungibili</p> <p>Se selezionato Shutdown VM oppure Shutdown Cluster: va specificato un nome valido parte dell'infrastruttura</p>
Target	Se selezionato VMotion: va specificato un hostname o indirizzo IP
Restore on power on	<p>Nel caso di azioni di shutdown se abilitato, al ritorno rete la <i>Netman 204</i> riavvierà automaticamente le VM che ha spento.</p> <p>Nel caso di azione maintenace se abilitato, al ritorno rete la <i>Netman 204</i> toglierà l'host dallo stato di maintenace.</p> <p>Si prega di notare che per riavviare gli host è necessario invece usare Wake-on-Lan (maggiori informazioni al capitolo Wake-on-Lan)</p>
Target Netman	Per usi futuri.

La sequenza delle azioni nella lista può essere cambiata selezionando e muovendo la riga in alto oppure in basso con il mouse.



NOTA

La funzione vSphere DRS automation può essere usata forzando l'host target in modalità manutenzione.

SHUTDOWN SU EVENTO

E' possibile configurare il ritardo dello shutdown UPS in secondi; questo contatore partirà allo stesso tempo delle azioni shutdown nella lista Action.

Inoltre, i comandi verranno eseguiti in condizione di battery low e quando lo shutdown è attivo.

SAVE

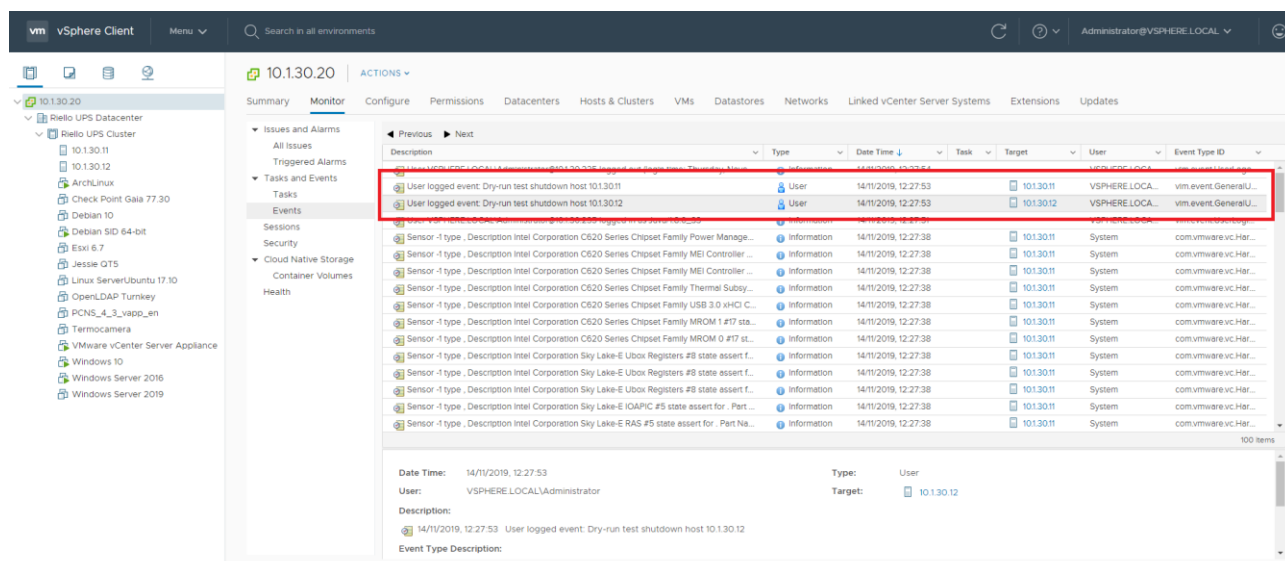
Questo pulsante SALVA la configurazione, si prega di notare che il servizio va riavviato.

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

DRY RUN

Test della configurazione

E' inoltre possibile testare la procedura senza eseguire un vero shutdown premendo "Dry Run". I log sull'host o vCenter Server Appliance confermeranno la correttezza della configurazione.



The screenshot shows the vSphere Client interface with the 'Monitor' tab selected. The event log table is highlighted, showing two 'User logged event: Dry-run test shutdown' entries for hosts 10.130.11 and 10.130.12. Below the table, the details for the selected event are shown.

Description	Type	Date Time	Task	Target	User	Event Type ID
User logged event: Dry-run test shutdown host 10.130.11	User	14/11/2019, 12:27:53		10.130.11	VSPHERE.LOCAL\Administrator	vim.event.GeneralU...
User logged event: Dry-run test shutdown host 10.130.12	User	14/11/2019, 12:27:53		10.130.12	VSPHERE.LOCAL\Administrator	vim.event.GeneralU...

Date Time: 14/11/2019, 12:27:53
User: VSPHERE.LOCAL\Administrator
Type: User
Target: 10.130.12
Description:
14/11/2019, 12:27:53 User logged event: Dry-run test shutdown host 10.130.12
Event Type Description:

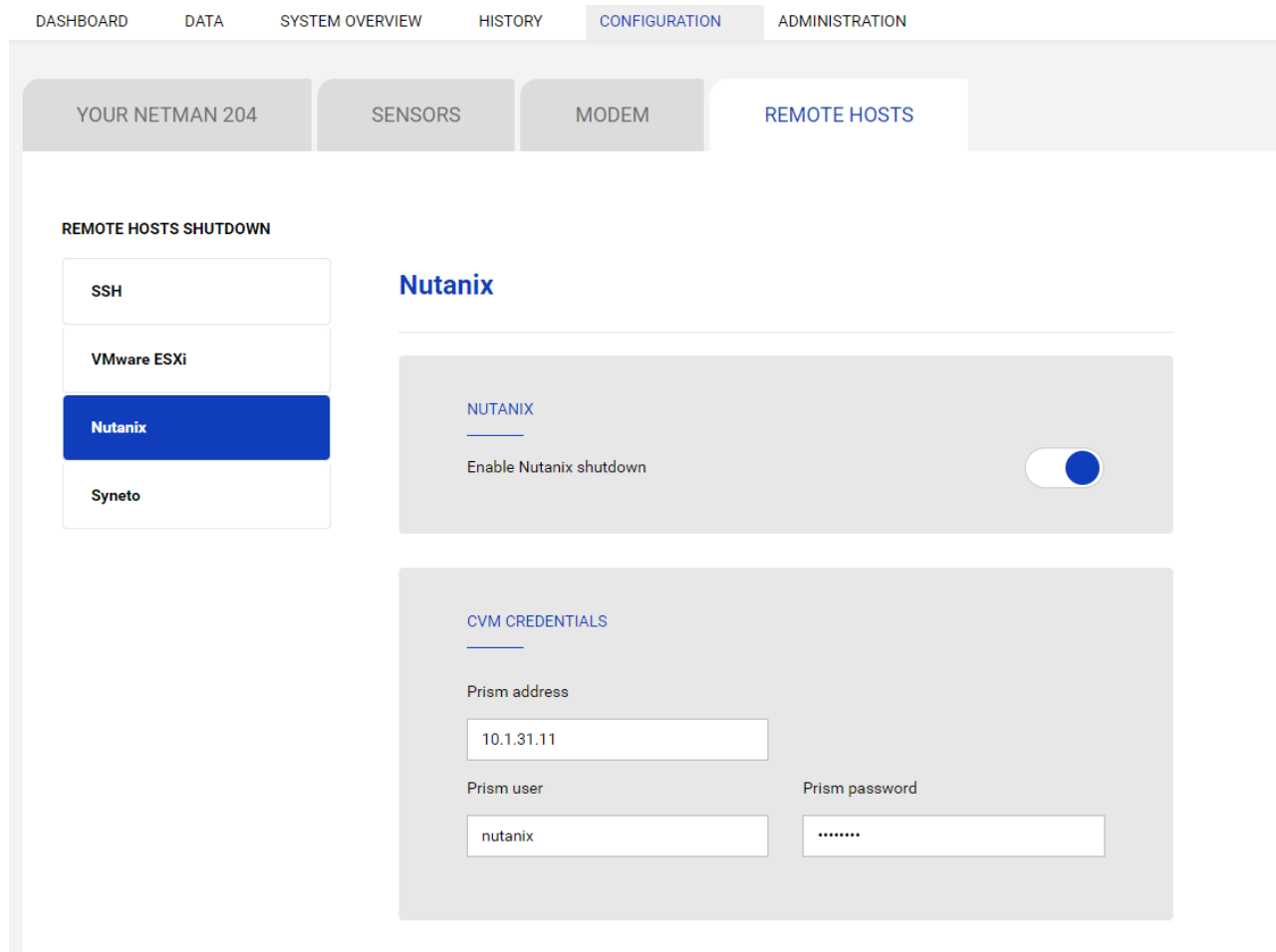
TEST VMWARE/VMWARE VCENTER SERVER CREDENTIALS (PLEASE CLICK SAVE BEFORE TESTING)

VALIDATE

Validazione delle connessioni

La validità delle credenziali può essere testata premendo "Validate". Ogni credenziale salvata verrà testata.

Dopo il test verrà mostrato il risultato con un messaggio pop-up.



Questo menu permette di configurare il servizio shutdown Nutanix. Qualunque host o parte di una infrastruttura cluster Nutanix può eseguire lo spegnimento; è possibile spegnere delle virtual machine sia con priorità che senza priorità, ciascuna con le proprie credenziali, priorità e ritardo. La validità delle credenziali è testata periodicamente e, se non valida, viene presentato un allarme. E' inoltre possibile eseguire lo shutdown dell'UPS alla fine.

Lo slider "Enable Nutanix shutdown" abilita il servizio Nutanix shutdown.

CVM credentials

Campo	Parametri da inserire
Prism address	Inserire l'hostname o indirizzo IP del CVM Prism
User name	Inserire lo user name dell'amministratore CVM
Password	Inserire la password dell'amministratore CVM

Physical hosts

Host	Username	Password	
10.1.31.10	root	Delete
10.1.31.12	root	Delete
10.1.31.14		Delete

[Add Row](#)

Actions

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

[Add Row](#)

Actions

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

[Add Row](#)

SHUTDOWN ON EVENT

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

Then, UPS shutdown after (seconds)



SAVE

TEST NUTANIX SHUTDOWN
(PLEASE CLICK SAVE BEFORE TESTING)

DRY RUN

TEST NUTANIX SERVER CREDENTIALS
(PLEASE CLICK SAVE BEFORE TESTING)

VALIDATE

Actions

Campo	Parametri da inserire
Action	L'azione da eseguire: Non critical VM eseguirà lo shutdown di tutte le VM non-critiche Critical VM eseguirà lo shutdown della VM con UID specificato
Condition	Specifica l'evento scatenante: Power fail: quando l'UPS rileva una mancanza rete, inizierà il conto alla rovescia con il tempo configurato (minuti). Una volta trascorso il tempo, verrà avviata l'azione selezionata. Se la rete ritorna entro questo tempo, l'azione verrà annullata. Autonomy less: quando l'autonomia calcolata della batteria dell'UPS scende al di sotto del tempo configurato (minuti) si avvia l'azione selezionata. Se la rete ritorna entro questo tempo, l'azione verrà annullata.
Condition duration (minutes)	Il tempo per il quale la condizione selezionata (Interruzione di alimentazione o Autonomia inferiore) attiva l'azione selezionata.
Delay next (seconds)	Ritardo in secondi prima di eseguire l'azione successiva
Source	Se Action è Critical VM , va specificata una VM UID presente nell'infrastruttura.

Restore on power on	Al ritorno rete la <i>Netman 204</i> riavvierà automaticamente le VM che ha spento. Si prega di notare che per riavviare gli host è necessario invece usare Wake-on-Lan (maggiori informazioni al capitolo Wake-on-Lan)
---------------------	--

La sequenza delle azioni nella lista può essere cambiata selezionando e muovendo la riga in alto oppure in basso con il mouse.

SHUTDOWN SU EVENTO

E' possibile configurare il ritardo dello shutdown UPS in secondi; questo contatore partirà allo stesso tempo delle azioni shutdown nella lista Action.

Inoltre, i comandi verranno eseguiti in condizione di battery low e quando lo shutdown è attivo.

SAVE

Questo pulsante SALVA la configurazione, si prega di notare che il servizio va riavviato.

DRY-RUN

Test della configurazione

E' inoltre possibile testare la procedura senza eseguire un vero shutdown premendo "Dry Run". I log sul Prism CVM destinazione confermeranno la correttezza della configurazione.

Validazione delle connessioni

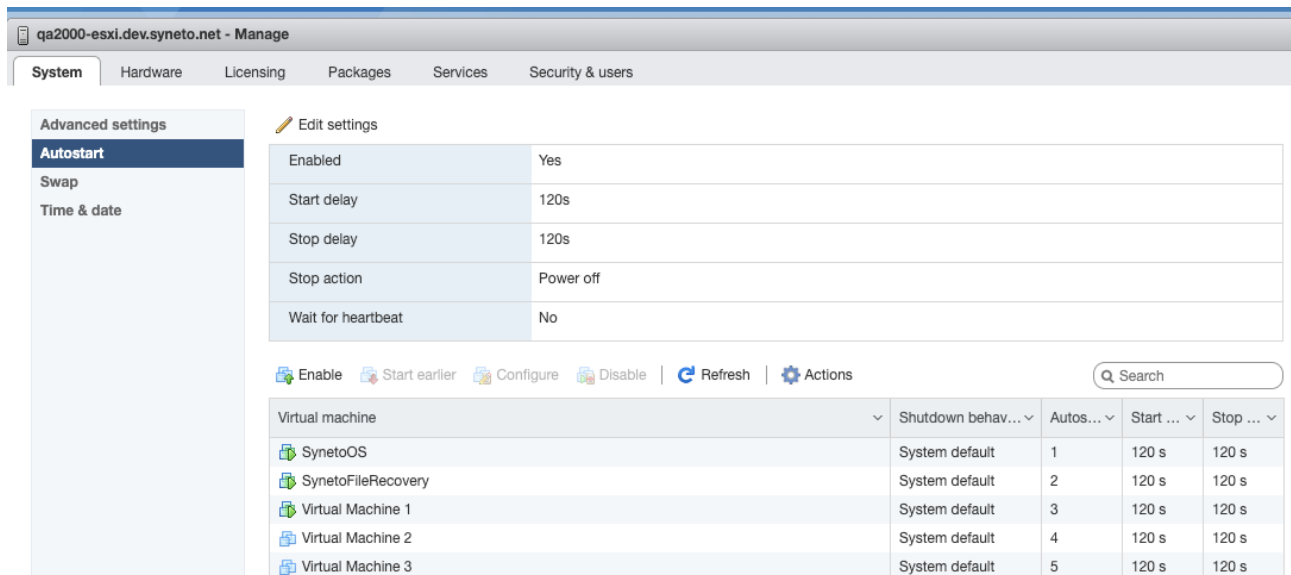
La validità delle credenziali può essere testata premendo "Validate". Dopo il test verrà mostrato il risultato con un messaggio pop-up.

Syneto

CONFIGURARE LA FUNZIONALITA' AUTOSTART ESXi

Le appliances Syneto HYPER hanno la funzionalità Autostart abilitata di default sull'hypervisor ESXi. Questo è un prerequisito obbligatorio in modo che le virtual machine si possano accendere o spegnere nell'ordine corretto quando viene richiesto dalla *Netman 204*.

Configurare le virtual machine che devono essere gestite nell'hypervisor nell'ordine desiderato. SynetoOS e SynetoFileRecovery sono sempre la prima e la seconda della lista.



The screenshot shows the vSphere Client interface for a host named 'qa2000-esxi.dev.syneto.net'. The 'System' tab is selected, and the 'Advanced settings' section is expanded to 'Autostart'. The 'Autostart' settings are as follows:

Setting	Value
Enabled	Yes
Start delay	120s
Stop delay	120s
Stop action	Power off
Wait for heartbeat	No

Below the settings, there is a table listing the virtual machines and their autostart configurations:

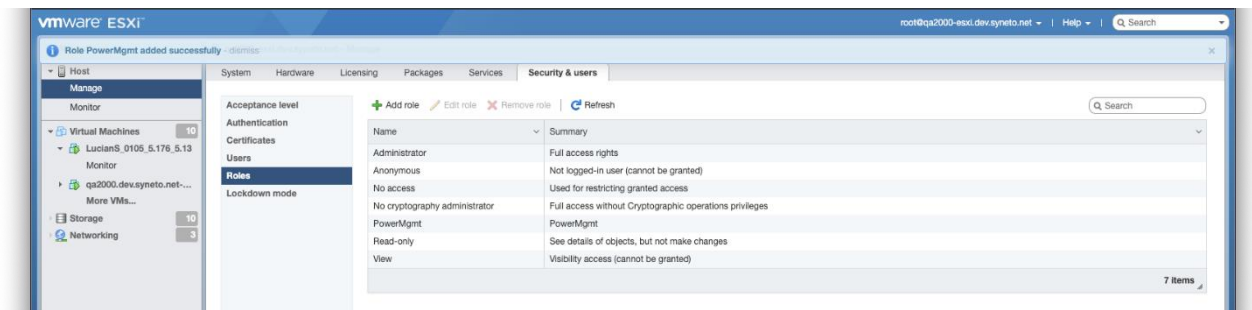
Virtual machine	Shutdown behavior	Autostart order	Start delay	Stop delay
SynetoOS	System default	1	120 s	120 s
SynetoFileRecovery	System default	2	120 s	120 s
Virtual Machine 1	System default	3	120 s	120 s
Virtual Machine 2	System default	4	120 s	120 s
Virtual Machine 3	System default	5	120 s	120 s

CONFIGURARE ESXi USER & RUOLO PER GESTIONE REMOTA ALIMENTAZIONE

Syneto consiglia di configurare un utente ESXi da usare appositamente per le funzioni power management dell'UPS. Questo consente un livello di sicurezza che limita la superficie di attacco. Collegarsi al vostro host ESXi tramite il Web client.

1. Creare un nuovo Ruolo.

Andare su Host -> Security and Users -> Roles.



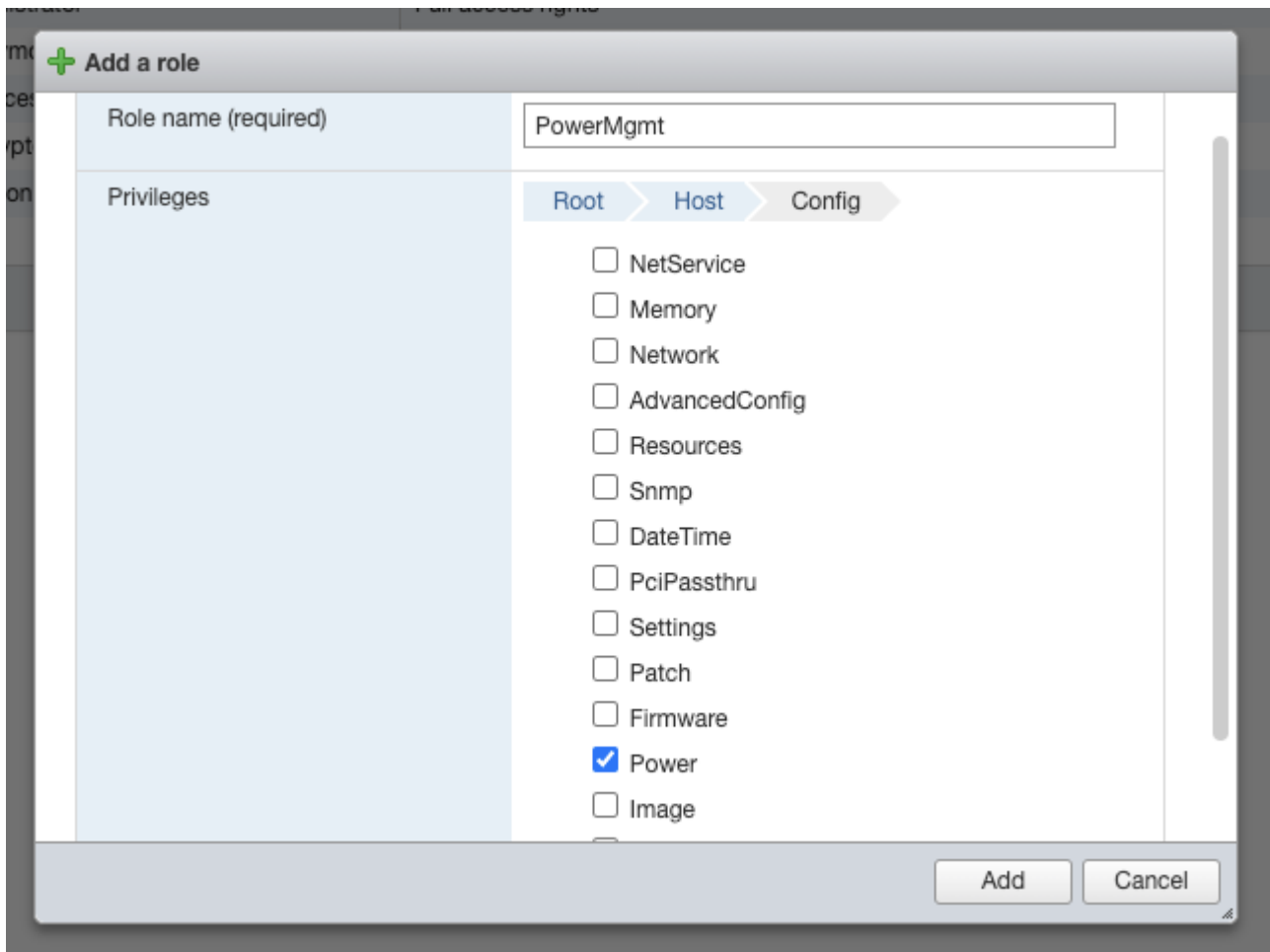
The screenshot shows the vSphere Client interface for a host named 'qa2000-esxi.dev.syneto.net'. The 'Security & users' tab is selected, and the 'Roles' section is expanded. The 'Roles' table is as follows:

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

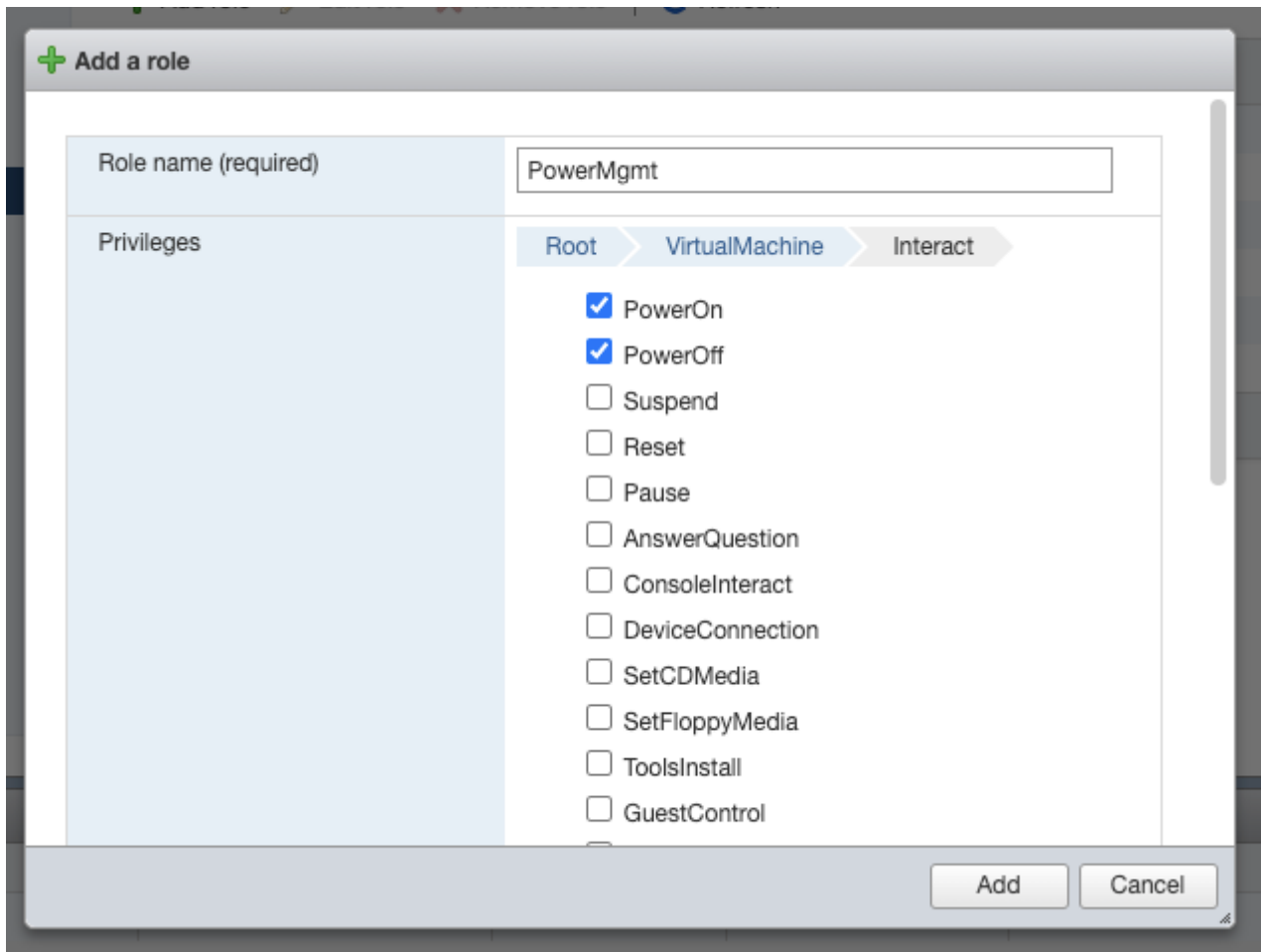
Fare click su Add Role. Dare al nuovo ruolo un nome idoneo, per esempio: "PowerMgmt".

Scegliere i seguenti da Privileges:

Root -> Host -> Config -> Power.



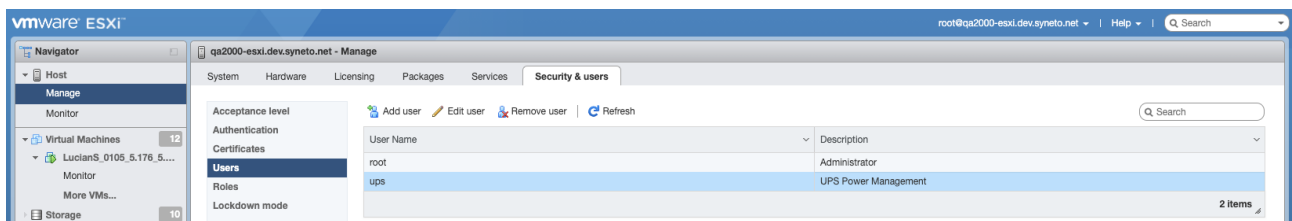
Root -> VirtualMachine -> Interact -> PowerOn, PowerOff



Fare click su Add per creare il nuovo ruolo.

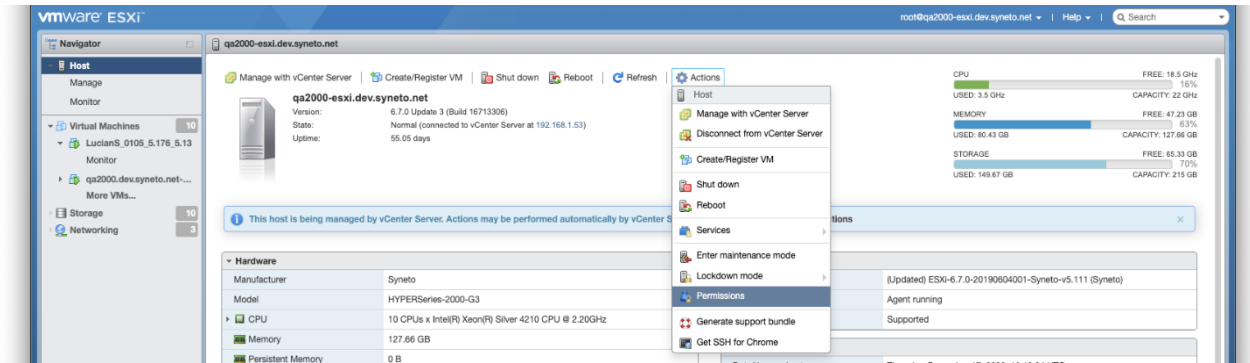
2. Creare un nuovo utente.

Andare su Host -> Manage -> Security & users -> Users. Fare click su Add user per creare un nuovo utente. Dare un nome ad esempio "ups".

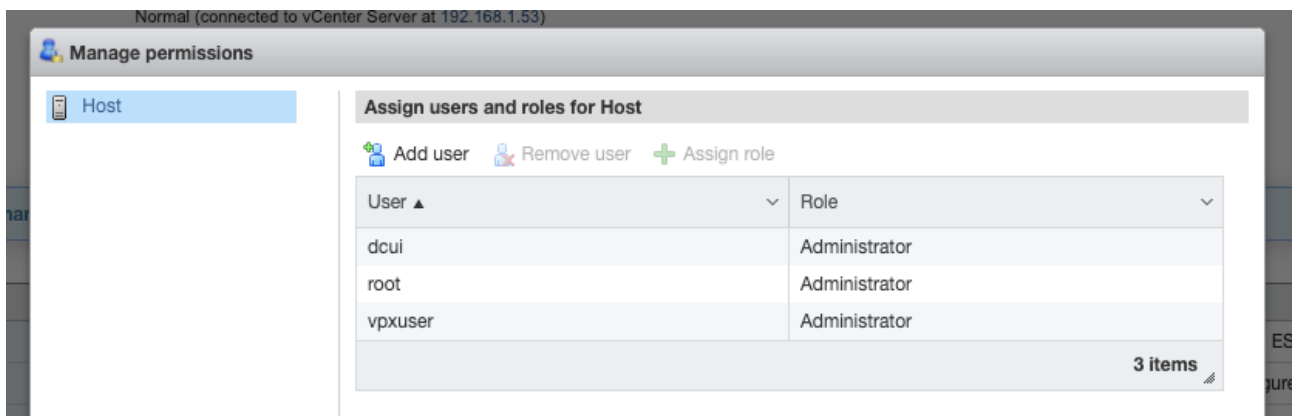


3. Assegnare il ruolo PowerMgmt al nuovo utente ups sull'host ESXi.

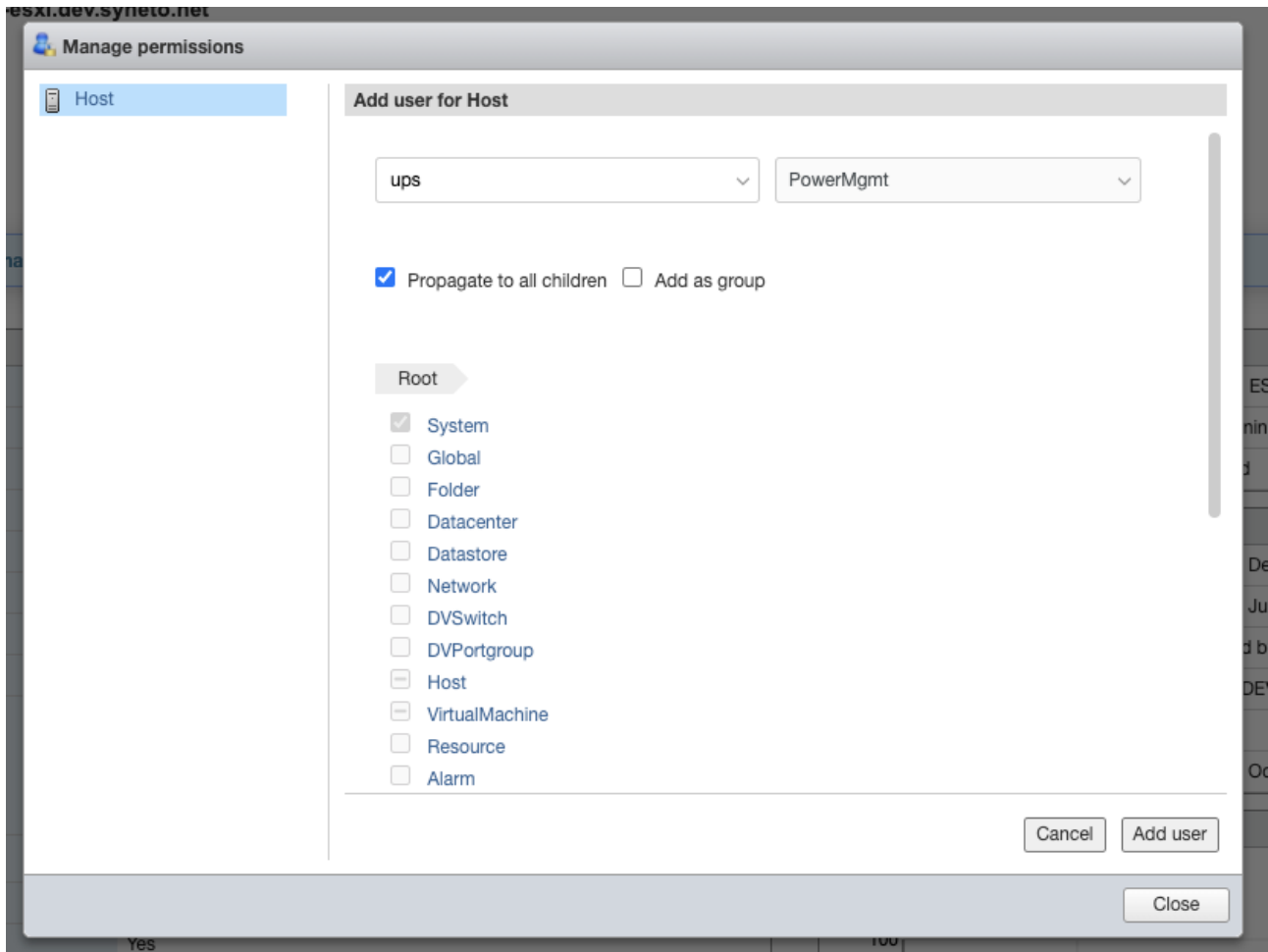
Andare su Host -> Actions -> Permissions.



Fare click su Add user per assegnare l'utente e il ruolo sull'host ESXi.



Inserire lo username, scegliere il ruolo appropriato per il power management. In questo esempio, *ups* e *PowerMgmt*.



Fare click su Add user. Adesso hai configurato un utente che può essere usato per il power management sull'host ESXi.

CONFIGURARE LA NETMAN 204 PER LO SHUTDOWN HOST

Collegarsi alla *Netman 204* tramite interfaccia web. Andare su Configuration -> Remote Hosts -> Syneto

YOUR NETMAN 204 SENSORS MODEM REMOTE HOSTS

REMOTE HOSTS SHUTDOWN

- SSH
- VMware ESXi
- Nutanix
- Syneto**

Syneto

SYNETO

Enable Syneto shutdown

Infrastructure connectors

ESXi Hypervisor	Username	Password	
192.168.1.27	ups	Delete

Add Row

- Fare click sul box Enable Syneto shutdown
- Nella sezione Infrastructure connectors, fare click sul tasto Add Row. Verrà collegata la *Netman 204* all'host ESXi.
- Inserire quanto segue:

ESXi Hypervisor	Indirizzo IP dell'host ESXi o Vcenter
Username	Username creato per il power management (esempio: ups)
Password	Password dell'utente di cui sopra

- Nella sezione Actions, fare click sul tasto Add Row. Definire l'azione da eseguire sull'host ESXi.

- Inserire quanto segue:

Azione: Shutdown host	Shutdown dell'host
Condition: Power Fail or Autonomy less .	<p>Power fail: quando l'UPS rileva una mancanza rete, inizierà il conto alla rovescia con il tempo configurato (minuti). Una volta trascorso il tempo, verrà avviata l'azione selezionata. Se la rete ritorna entro questo tempo, l'azione verrà annullata.</p> <p>Autonomy less: quando l'autonomia calcolata della batteria dell'UPS scende al di sotto del tempo configurato (minuti) si avvia l'azione selezionata. Se la rete ritorna entro questo tempo, l'azione verrà annullata.</p>
Condition duration (minutes):	Il tempo per il quale la condizione selezionata (Interruzione di alimentazione o Autonomia inferiore) attiva l'azione selezionata. Consigliamo almeno 15 minuti

Actions

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

Actions

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

SHUTDOWN ON EVENT

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

Then, UPS shutdown after (seconds)

L'UPS con *Netman 204* eseguirà lo shutdown di tutte le virtual machine che sono incluse nella funzione Autostart nell'ordine inverso: l'ultima virtual machine nella lista verrà spenta per prima.

SHUTDOWN ON EVENT

E' possibile configurare il ritardo UPS shutdown delay in secondi, questo contatore partirà dopo l'azione shutdown elencata in Action list.

Inoltre, i comandi saranno eseguiti ogni qualvolta si verifichi la condizione di battery low e quando lo shutdown è attivo.

SAVE

Questo tasto SALVA la configurazione, si prega di notare che il servizio va riavviato per diventare effettivo.

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

DRY RUN

Testare la configurazione

E' possibile testare la procedura senza eseguire un vero shutdown premendo "Dry Run". I log sull'host target o sulla vCenter Server Appliance daranno conferma della correttezza della configurazione.

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

VALIDATE

Validazione delle connessioni

E' possibile testare la correttezza del nome utente e password per eseguire il login su VSphere VCSA.

Dopo il test verrà mostrato il risultato con un messaggio pop-up.

Configurazione NTP & Timezone



Alcuni servizi della *Netman 204* richiedono ora e data corrette per funzionare. E' necessario configurarle appena possibile per evitare dei malfunzionamenti.

The screenshot shows the 'NTP & Timezone configuration' page in the Netman204 web interface. The page is divided into several sections:

- Navigation:** Includes 'YOUR NETMAN 204', 'SENSORS', 'MODEM', and 'REMOTE HOSTS' tabs.
- DEVICE Configuration:** A sidebar with options for 'General configuration', 'Command configuration', and 'Data Log configuration'.
- NETWORK Configuration:** A sidebar with options for 'Configuration', 'UDP Firewall', 'Wake on LAN', 'SNMP', 'MODBUS/BACNET', 'JSON', and 'SYSLOG'.
- DATE & TIME Configuration:** A sidebar with an option for 'NTP & Timezone'.
- Main Content Area:**
 - Current date:** 13 Nov 15:35 UTC 2019
 - SET A NEW TIMEZONE:** A dropdown menu with 'ROME' selected.
 - SET A NTP SERVER:** A text input field with the placeholder 'Please insert the NTP address'.
 - SAVE:** A blue button to save the configuration.

Questo menu consente di configurare la sincronizzazione con il server NTP.

Campo	Parametri da immettere
NTP server address (IP)	Immettere il nome o l'indirizzo del server NTP



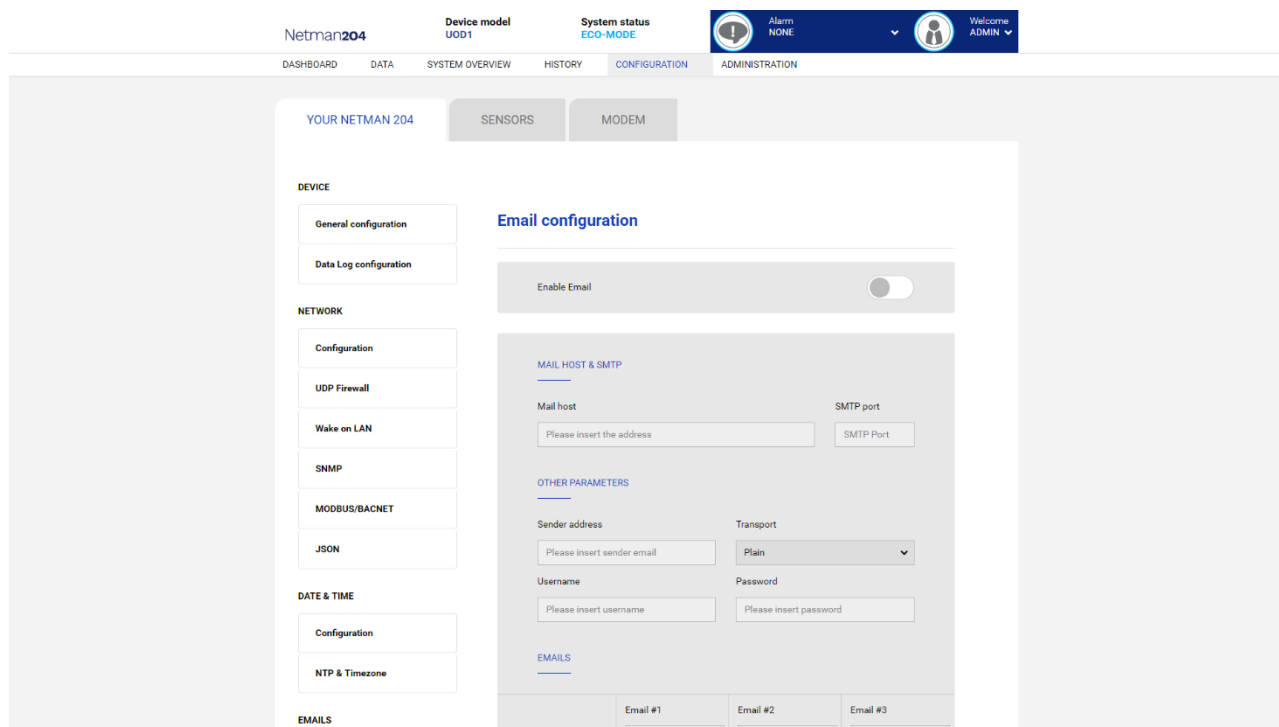
Solo per alcuni modelli di UPS; se si riceve un'ora valida dal server NTP configurato, *Netman 204* sincronizza l'orologio dell'UPS ogni giorno alle 00:30.

Configurazione Date & Time

The screenshot shows the Netman204 web interface. At the top, there is a navigation bar with 'Netman204', 'Device model VST 800', 'System status STAND-BY', and an 'Alarm NONE' indicator. Below this is a menu with 'DASHBOARD', 'DATA', 'SYSTEM OVERVIEW', 'HISTORY', 'CONFIGURATION', and 'ADMINISTRATION'. The main content area is titled 'YOUR NETMAN 204' and has tabs for 'SENSORS', 'MODEM', and 'REMOTE HOSTS'. On the left, there is a sidebar with configuration categories: 'DEVICE' (General configuration, Command configuration, Data Log configuration), 'NETWORK' (Configuration, UDP Firewall, Wake on LAN, SNMP, MODBUS/BACNET, JSON, SYSLOG), and 'DATE & TIME' (NTP & Timezone). The 'Date & Time configuration' page is active, showing the current date as '13 Nov 15:36 UTC 2019'. There is a 'SET A NEW DATE' section with a 'Date' input field (dd/mm/yyyy), a calendar icon, and 'Hour' and 'Minutes' dropdown menus (both set to 00). A blue 'SAVE' button is located below the input fields.

Campo	Parametri da inserire
Date	Inserire la data odierna
Hour	Inserire l'ora corrente
Minutes	Inserire il minuto corrente

Configurazione email



Questo menu può essere utilizzato per configurare gli indirizzi a cui inviare le notifiche degli allarmi e le e-mail con i rapporti e altri parametri del servizio Email, come descritto nella seguente tabella.

Campo	Parametri da immettere
Enable Email	Abilita il servizio Email
Mail host	Immettere il nome o l'indirizzo del server SMTP da utilizzare per inviare le e-mail. ⁽¹⁾
SMTP port	Porta IP utilizzata dal protocollo SMTP
Sender address	Immettere l'indirizzo da cui devono essere inviate le e-mail. ⁽²⁾
Username	Se il server richiede l'autenticazione, immettere il nome utente.
Password	Se il server richiede l'autenticazione, immettere la password.
Transport	È possibile scegliere tra normale, SSL o TLS.
Email #1	Immettere gli indirizzi e-mail a cui inviare le notifiche degli allarmi e i rapporti (vedere nota).
Email #2	
Email #3	
Device events	Scelta degli eventi per i quali verrà inviata l'email
Send report every day	Invia l'email report ogni giorno alle 00:00.
Send report every week	Invia l'email report ogni lunedì alle 00:00.

⁽¹⁾ Accertarsi che il server SMTP accetti connessioni sulla porta 25

⁽²⁾ Non utilizzare il carattere di "spazio" in questo campo

Dopo avere immesso i dati e avere salvato, è possibile eseguire un test del servizio. Se il test viene eseguito, viene inviata un'apposita e-mail a tutti gli indirizzi e-mail configurati.



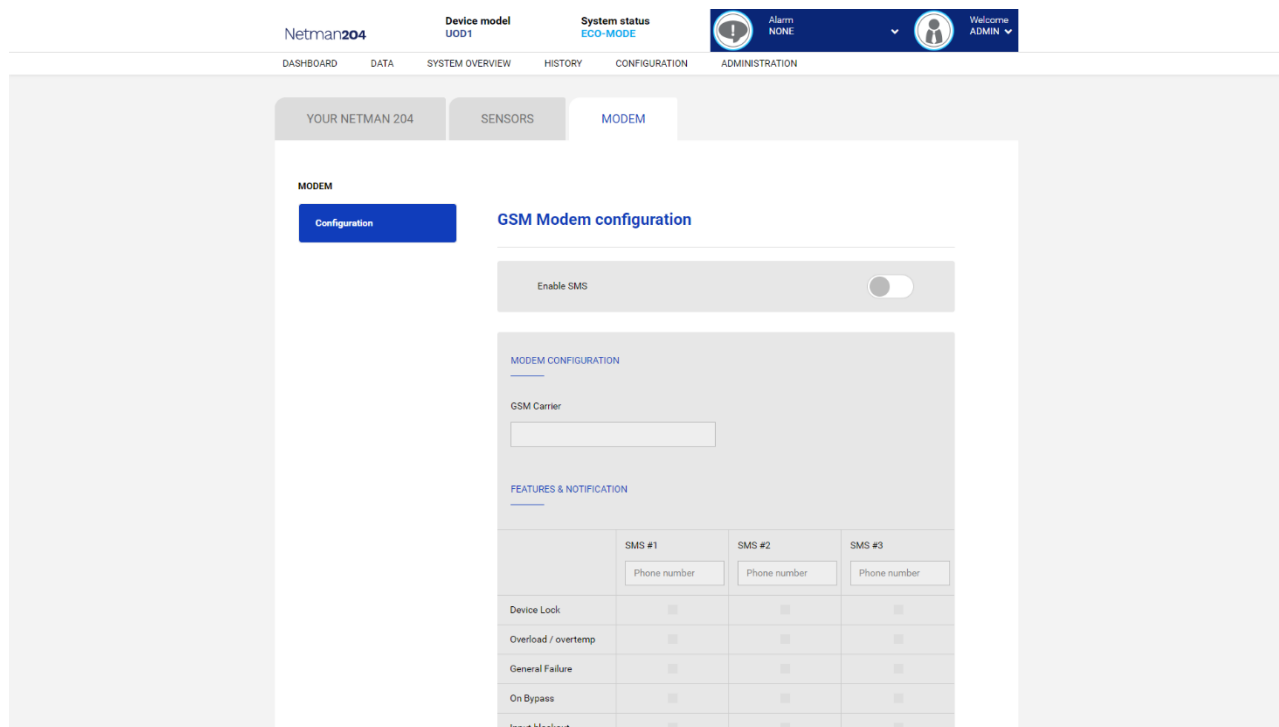
Le e-mail con rapporto vengono inviate a tutti gli indirizzi indicati; per le e-mail di notifica degli allarmi, vedere la sezione "*Email logic*".

Email logic

Nella seguente tabella viene descritto il significato degli eventi, i quali possono variare a seconda del dispositivo collegato.

Evento	Significato
Device Lock	Il dispositivo è bloccato o presenta un guasto grave
Ovrload/Ovrtemp	Il dispositivo è in sovraccarico o è surriscaldato
General Failure	Malfunzionamento del dispositivo
On bypass	Funzionamento da bypass
Input blackout	La sorgente di ingresso è in blackout
Battery low	Batteria quasi scarica
Communic lost	La comunicazione tra la <i>Netman 204</i> e il dispositivo è stata interrotta

Modem GSM



Tramite questo menu è possibile configurare il modem GSM per l'invio di SMS.

Campo	Parametri da immettere
Enable SMS	Abilita il servizio SMS
GSM carrier	Inserire il numero di telefono del carrier
SMS #1	Immettere i numeri di telefono che riceveranno le notifiche SMS
SMS #2	
SMS #3	
Device events	Scelta degli eventi per i quali verranno inviati gli SMS
Send report every day	Invia un SMS report ogni giorno alle 00:00
Send report every week	Invia un SMS report ogni lunedì alle 00:00

Sensori

Campo	Parametri da inserire
Enable sensors	Abilita il servizio sensori ambientali
Contact logic	Scelta tra normalmente aperto e normalmente chiuso
Output contact	Scelta del contatto di uscita da attivare con l'evento
Temperature high [°C]	Immettere la soglia di temperatura alta
Temperature low [°C]	Immettere la soglia di temperatura bassa
Temperature hysteresis [°C]	Immettere l'isteresi di temperatura
Humidity high [%RH]	Immettere la soglia di umidità alta
Humidity low [%RH]	Immettere la soglia di umidità bassa
Humidity hysteresis [%RH]	Immettere l'isteresi di umidità



Oltre a essere configurati, i servizi devono essere anche attivati per consentirne il corretto funzionamento (vedere la sezione "Installazione sensori").

Installazione Sensori tramite SSH o USB



Per accedere al menu "Sensors Config" è necessario prima attivare il servizio "Sensors" e riavviare la *Netman 204*.

```
Sensor list
```

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

Accedere al menu "Config sensor", collegare il primo sensore e premere "C". Dopo alcuni istanti, il dispositivo viene riconosciuto e gli viene assegnato un numero di identificazione [1]. Collegare il sensore successivo, se presente, e premere "N". Dopo alcuni istanti, il dispositivo viene riconosciuto e gli viene assegnato un numero di identificazione [2]. Ripetere la procedura per tutti i sensori e al termine della configurazione premere "Y".

```
Sensor list
```

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

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



Per il corretto funzionamento dei dispositivi, è necessario aggiungere soltanto un dispositivo per ciascuna iterazione e attendere che venga riconosciuto da *Netman 204*.

Esempio: come collegare un sensore *Temperature*, un sensore *Humidity & Temperature* e un sensore *Digital I/O & Temperature* in questo ordine esatto.

```
Sensor list
```

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

Collegare il primo sensore (*Temperature*) e premere "C".

```
Sensor list
```

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

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

Attendere che il primo sensore venga identificato, collegare il secondo sensore (*Humidity & Temperature*) e premere "N".

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

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

Attendere che anche il secondo sensore venga identificato, collegare il terzo sensore (*Digital I/O & Temperature*) e premere "N".

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

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

Premere "Y" per confermare.

Installazione sensori tramite HTTP

Netman204 Device model VST 800 System status STAND-BY Alarm NONE Welcome ADMIN

DASHBOARD DATA SYSTEM OVERVIEW HISTORY CONFIGURATION ADMINISTRATION

YOUR NETMAN 204 SENSORS MODEM REMOTE HOSTS

SENSORS

Main

Install a new sensor

General Sensors configuration

SENSORS CONFIGURATION

Enable sensors

ENVIRONMENTAL SENSORS

SAVE

! INFO: YOU NEED TO REBOOT YOUR NETMAN 204. DO YOU WANT TO REBOOT NOW?

Abilitare il servizio “Sensors” e riavviare la *Netman 204*.

Netman204 Device model ULC2 System status STAND-BY Alarm NONE Welcome ADMIN

DASHBOARD DATA SYSTEM OVERVIEW HISTORY CONFIGURATION ADMINISTRATION

YOUR NETMAN 204 SENSORS MODEM REMOTE HOSTS

SENSORS

Main

Install a new sensor

Sensor installation - First step

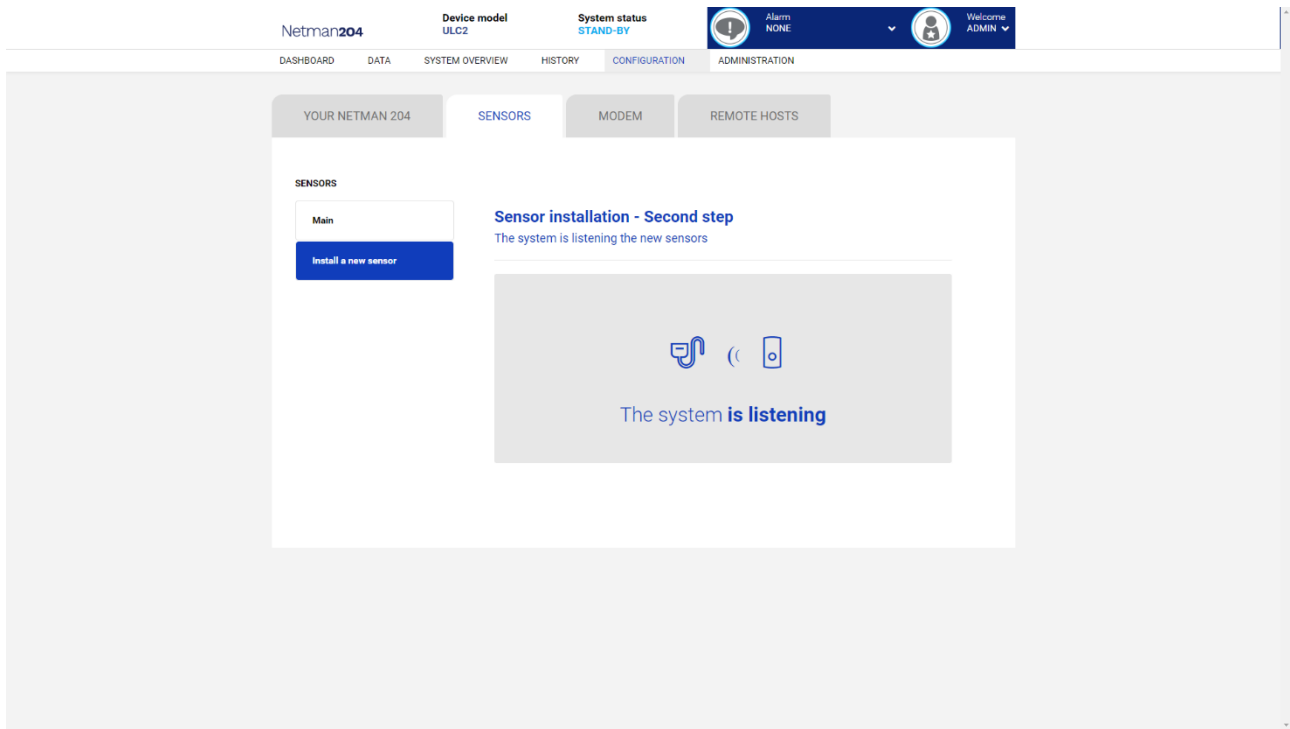
RESET CONFIGURATION

Connect your brand new sensor

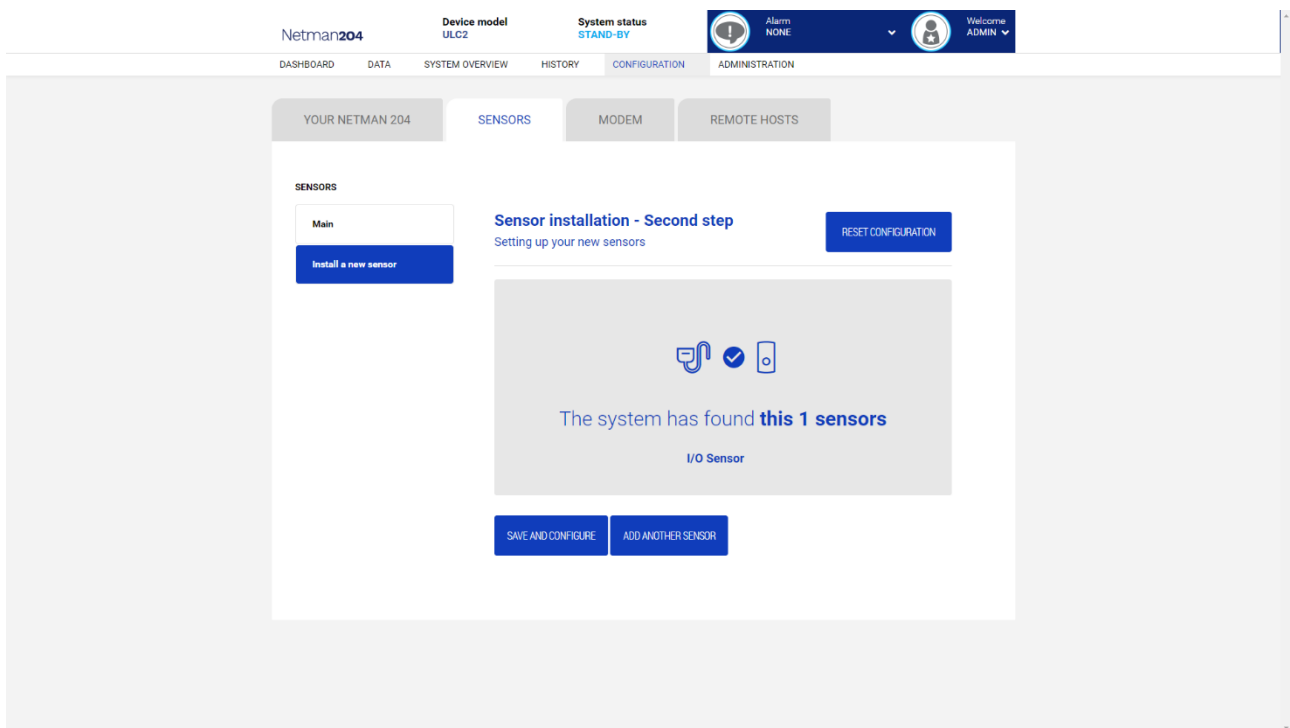
Please, connect just one sensor at a time.

START LISTENING

Premere “Install a new sensor” per accedere alla pagina di installazione sensori. Fare click su “Reset configuration” e poi connettere il primo sensore e fare click su “Start listening”.

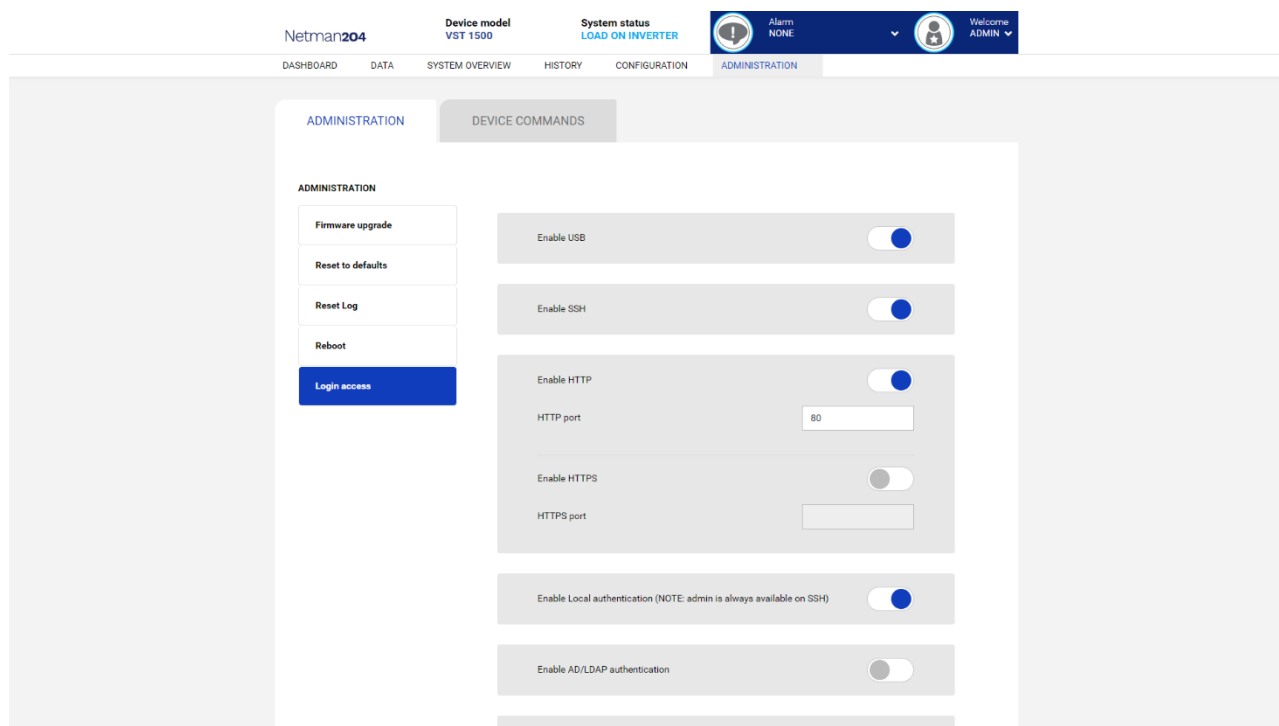


Dopo alcuni istanti il sensore verrà individuato.



Selezionare "Add another sensor" se necessario installare un altro sensore, oppure "Save and configure" per completare l'installazione.

Configurazione dell'accesso



E' possibile gestire la login tramite LDAP oppure AD. L'utente deve essere presente sul server e deve appartenere ad un gruppo specificato. Se il gruppo è il "gruppo Admin" allora l'utente otterrà i privilegi di "admin". Se il gruppo è il "gruppo Power" allora l'utente riceverà i privilegi "power" (ovvero non può eseguire lo shutdown sul dispositivo). Dopo la configurazione, nella videata di login va inserito solo lo username (invece del "Distinguished Name" completo) e la password.

Campo	Parametri da inserire
Enable USB	Abilita il login tramite cavo USB
Enable SSH	Abilita il login tramite SSH
Enable HTTP	Abilita il servizio HTTP
HTTP port	Inserire la porta dove gira il servizio HTTP (default: 80)
Enable HTTPS	Abilita il servizio HTTPS
HTTPS port	Inserire la porta dove gira il servizio HTTPS (default: 443)
Enable local authentication	Abilita l'autenticazione locale (interna alla <i>Netman 204</i>)
Enable LDAP/AD authentication	Abilita il login tramite LDAP oppure AD
Server address	L'indirizzo del server può essere ldap:// oppure ldaps://
LDAP users folder	La cartella degli utenti cui è consentito l'accesso
Admin group name	Il gruppo con privilegi "Admin"
Power group name	Il gruppo con privilegi "Power"

Esempi di indirizzi server LDAP:

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

Tramite secure socket:

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

Se l'utente "john" è presente sul server LDAP e appartiene ai gruppi configurati, sarà possibile eseguire il login con username "john" e la sua password LDAP.

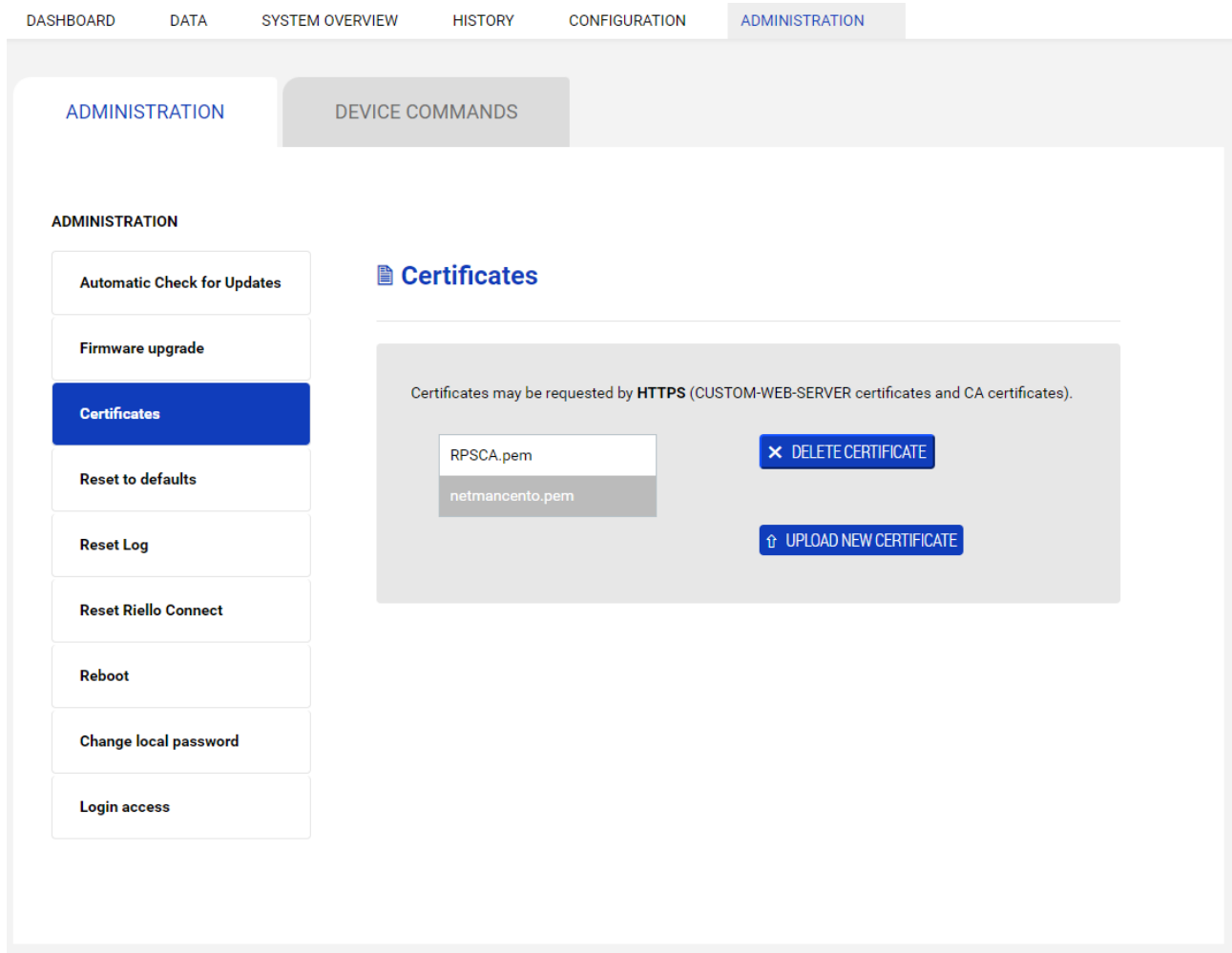
Certificati

Per HTTPS Netman 204 fornisce un certificato interno autofirmato, che copre l'utilizzo di base. L'utente può caricare e impostare:

- un **certificato Custom**
- un **certificato CA**

come opzionale per una connessione HTTPS più sicura.

Prima di qualsiasi configurazione l'Utente deve caricare i propri certificati nel menu:



Dove i certificati possono essere solo:

- **uploaded** nella *Netman 204*
- **deleted** (cancellati) dalla *Netman 204*

In nessun modo i certificati potranno essere visualizzati o scaricati.

I certificati devono seguire alcuni requisiti:

📄 Custom certificate:

- generato come file PEM (formato base64)
- Estensione del file ".pem"
- Generato dall'Autorità CA come "Web Server" e unito con la sua "Chiave privata"

📄 CA certificate:

- generato come file PEM (formato base64)
- Estensione del file ".pem"
- scaricato dall'Autorità CA

Per una spiegazione più approfondita, consultare la sezione "**Generazione del certificato**" nell'Appendice.

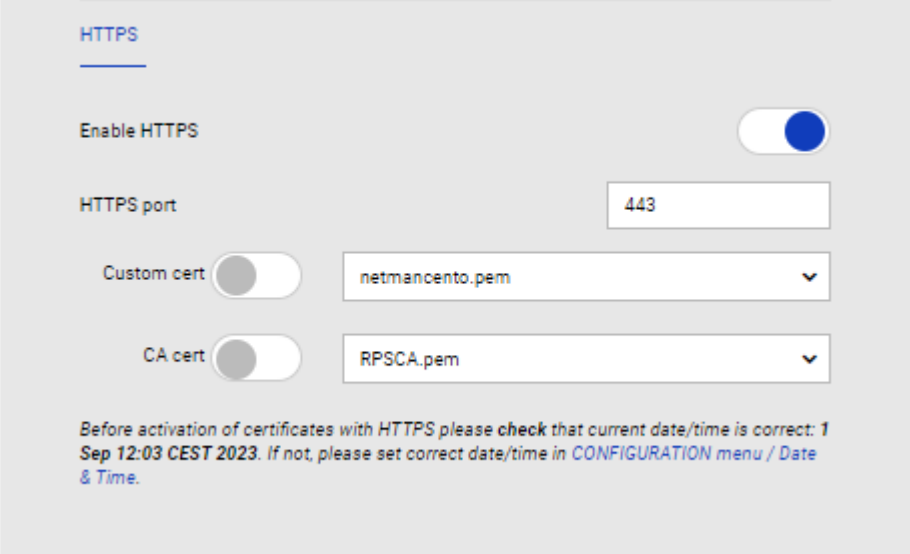
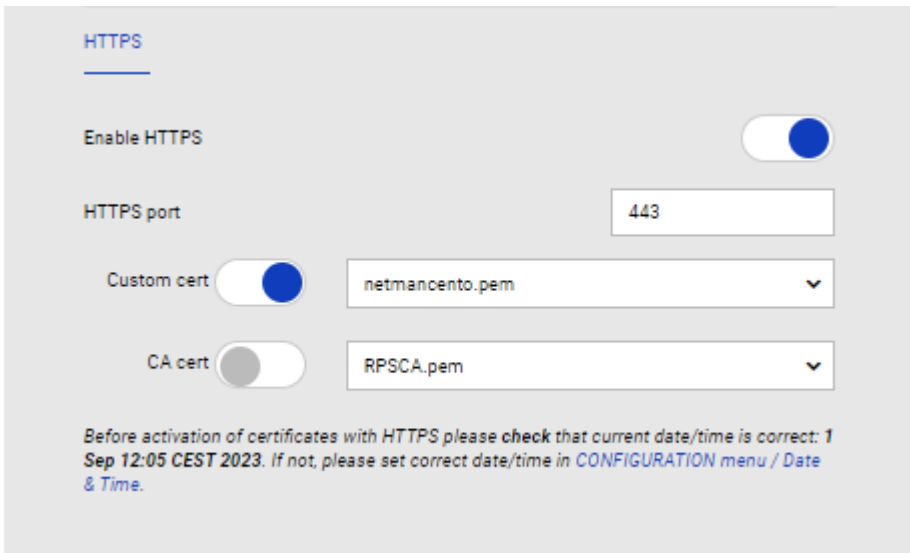
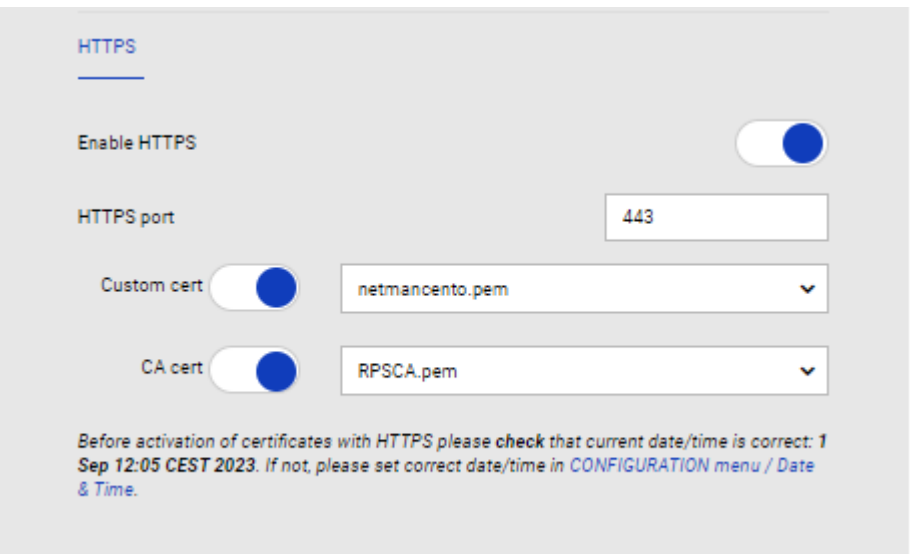
Dopo il corretto caricamento dei certificati, i certificati possono essere impostati nella configurazione HTTPS:

The screenshot displays the 'ADMINISTRATION' section of the Riello Connect interface. On the left, a sidebar lists various administrative tasks: Automatic Check for Updates, Firmware upgrade, Certificates, Reset to defaults, Reset Log, Reset Riello Connect, Reboot, Change local password, and Login access (highlighted in blue). The main content area is titled 'Login access' and is divided into several sections:

- Auto Logout:** Includes a toggle for 'Enable Auto Logout' (disabled), a text input for 'Auto Logout due to user inactivity after (seconds)', and another text input for 'Warning message when are left (seconds) before logout (message 'Session is about to expire...')'.
- Enable USB:** A toggle switch that is currently turned on.
- Enable SSH:** A toggle switch that is currently turned on.
- HTTP:** Includes a toggle for 'Enable HTTP' (disabled) and a text input for 'HTTP port'.
- HTTPS:** Includes a toggle for 'Enable HTTPS' (checked), a text input for 'HTTPS port' (value: 443), a 'Custom cert' toggle (checked) with a dropdown menu showing 'netmancento.pem', and a 'CA cert' toggle (checked) with a dropdown menu showing 'RPSCA.pem'.

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

dove possibile si possono impostare configurazioni:

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

Data e ora

Utilizzando i certificati per HTTPS la data e l'ora del *Netman 204* devono essere impostate correttamente, altrimenti la verifica HTTPS fallisce.

Possibile problema con data/ora sbagliata:

- le pagine web con HTTPS non rispondono e il *Netman 204* non è più raggiungibile via WEB

L'unica soluzione è:

⇒ ripristinare la connessione HTTP originale e quindi riconfigurare nuovamente HTTPS.

Consultare la sezione "Risoluzione dei problemi" di seguito per la descrizione della procedura.

Validità del certificato

Anche quando la data/ora è corretta:

- Vengono utilizzati certificati obsoleti
- Vengono utilizzati i certificati generati con data/ora futura

Avvio convalida quindi le pagine Web HTTPS non risponderanno più.

L'unica soluzione è:

⇒ ripristinare la connessione HTTP originale e quindi riconfigurare nuovamente HTTPS

impostando i certificati corretti. Consultare la sezione "**Risoluzione dei problemi**" di seguito per la descrizione della procedura.

Modifica dei certificati

Con alcuni browser, modificando la configurazione dei certificati nel *Netman 204* potrebbe essere necessario chiudere e riaprire la finestra del browser stesso per utilizzare i nuovi certificati.

Certificato CA per il browser

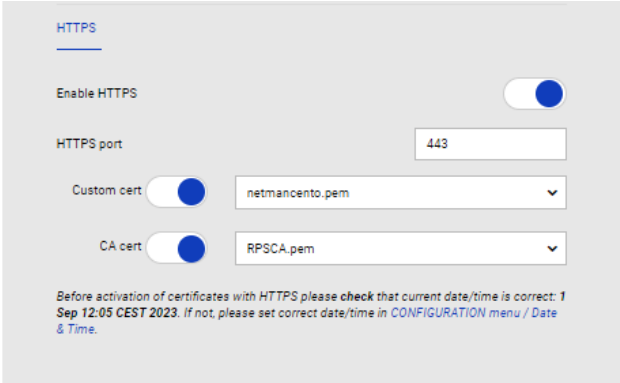
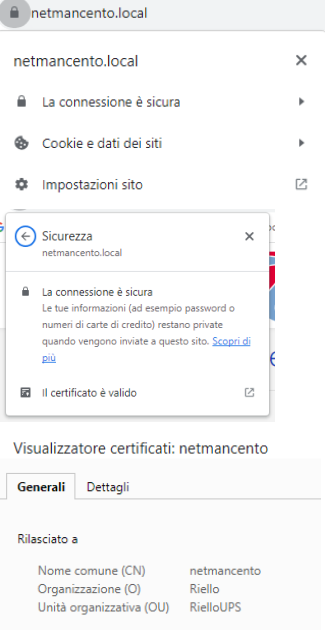
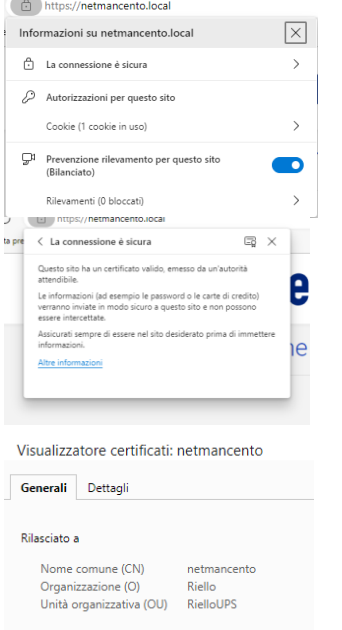
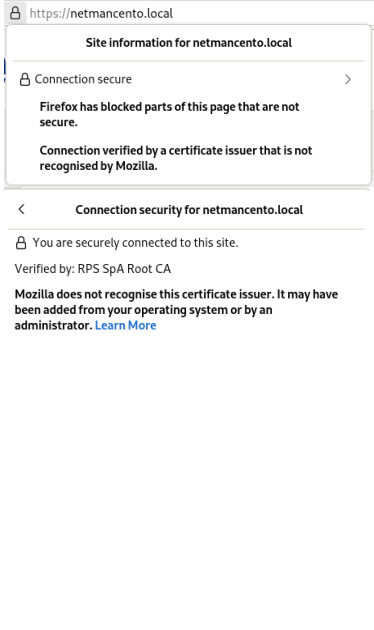
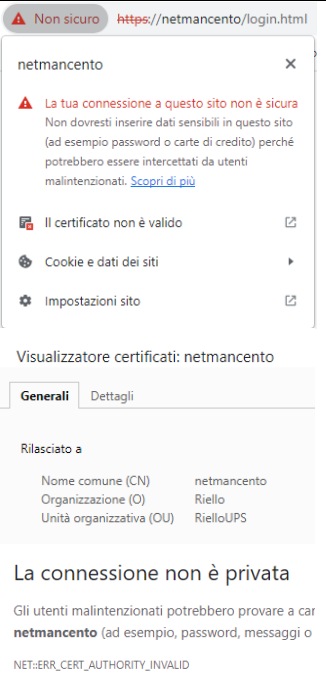
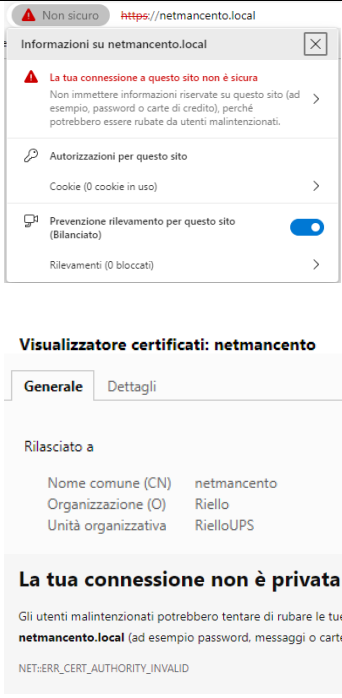
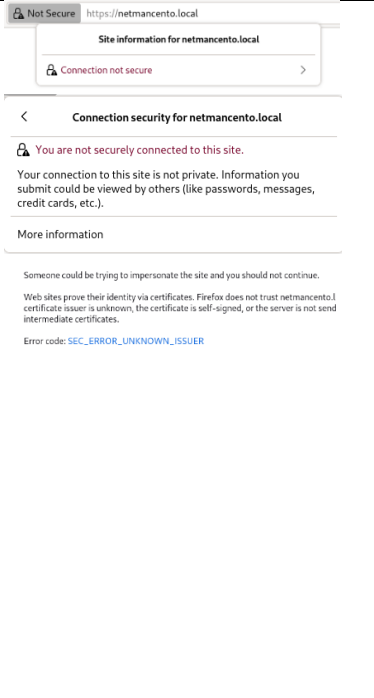
Di solito, una rete locale ben strutturata dovrebbe impostare e fornire "non appena pronto" il certificato CA corretto a qualsiasi browser Web client nella sua rete.

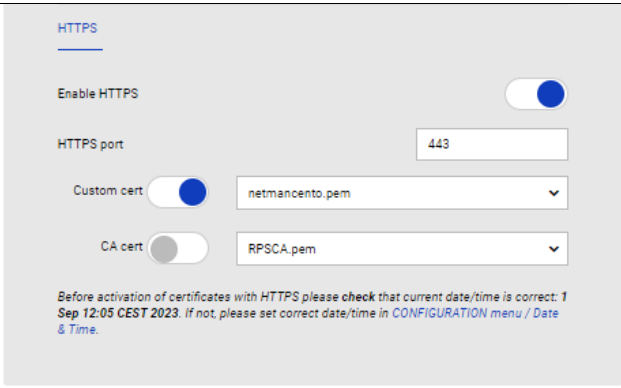
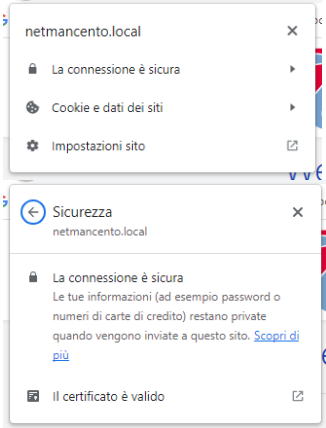
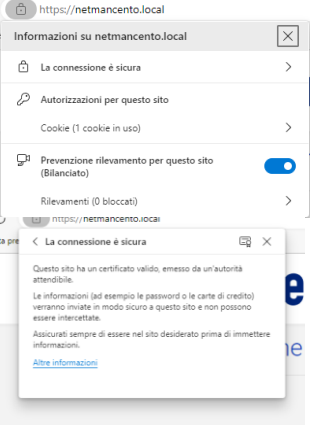
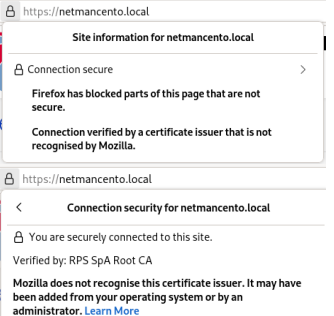
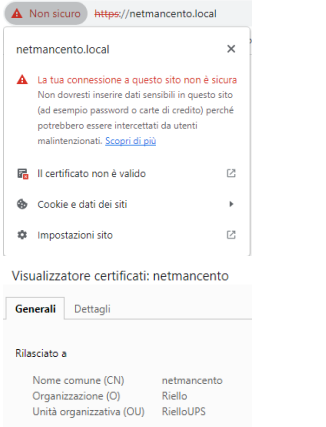
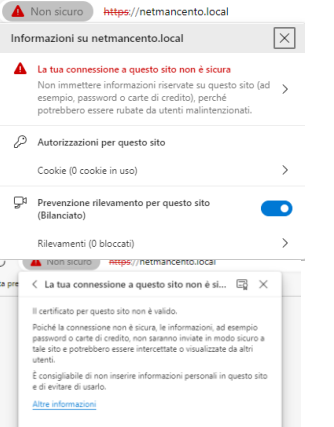
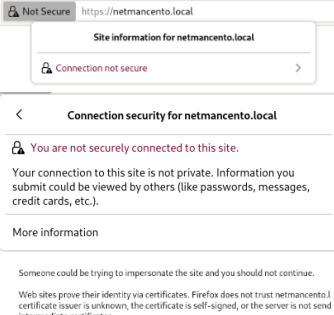
Quando il browser Web del client non riconosce l'emittente CA del certificato personalizzato del *Netman 204*, l'utente deve importare il certificato CA dell'emittente CA nel proprio browser Web client come "autorità di certificazione attendibile". La procedura di importazione del certificato CA root/intermedio è diversa a seconda del browser utilizzato.

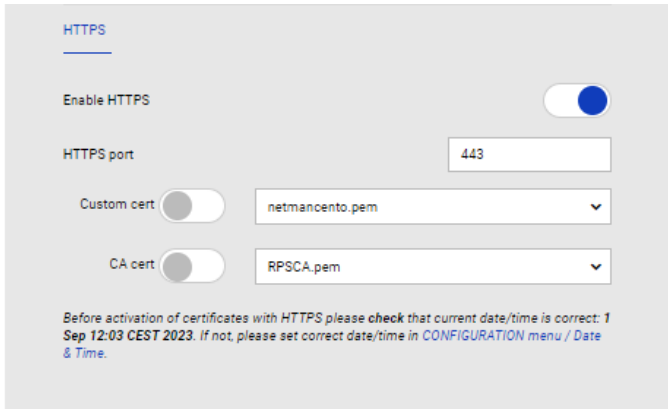
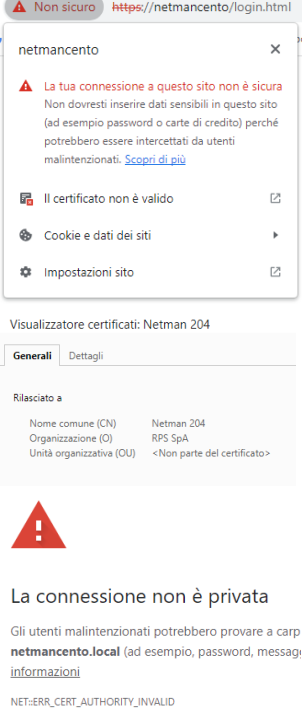
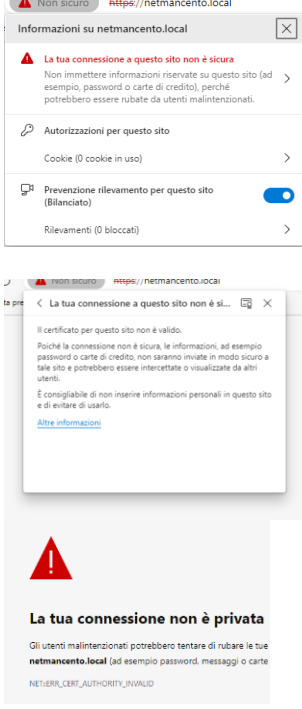
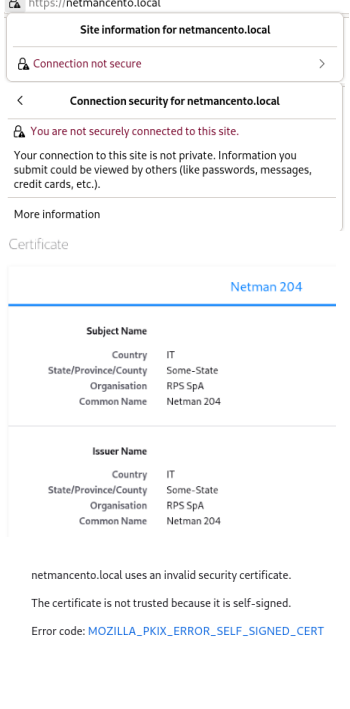
Quando è necessario:

- quando l'autorità CA è un server secondario all'interno della rete locale
- quando un client esterno deve connettersi al *Netman 204* dall'esterno e deve conoscere la CA originale che firma il certificato *Netman 204*.

Casi di test (diverse configurazioni con diversi browser Web)

Chrome	Edge	Firefox	Stato
			<p>Netman 204: + HTTPS + certificato custom + certificato CA</p>
			<p>✓ CA conosciuta dal browser (certificato installato nel browser)</p>
			<p>✗ CA non conosciuta dal browser (certificato installato nel browser)</p>

 <p>Enable HTTPS <input checked="" type="checkbox"/></p> <p>HTTPS port <input type="text" value="443"/></p> <p>Custom cert <input checked="" type="checkbox"/> netmancento.pem</p> <p>CA cert <input type="checkbox"/> RPSCA.pem</p> <p><small>Before activation of certificates with HTTPS please check that current date/time is correct: 1 Sep 12:05 CEST 2023. If not, please set correct date/time in CONFIGURATION menu / Date & Time.</small></p>		<p>Netman 204: + HTTPS + certificato custom</p>													
 <p>netmancento.local</p> <p>La connessione è sicura</p> <p>Cookie e dati dei siti</p> <p>Impostazioni sito</p> <p>Sicurezza netmancento.local</p> <p>La connessione è sicura Le tue informazioni (ad esempio password o numeri di carte di credito) restano private quando vengono inviate a questo sito. Scopri di più</p> <p>Il certificato è valido</p> <p>Visualizzatore certificati: netmancento</p> <p>Generali Dettagli</p> <p>Rilasciato a</p> <table border="1"> <tr><td>Nome comune (CN)</td><td>netmancento</td></tr> <tr><td>Organizzazione (O)</td><td>Riello</td></tr> <tr><td>Unità organizzativa (OU)</td><td>RielloUPS</td></tr> </table>	Nome comune (CN)	netmancento	Organizzazione (O)	Riello	Unità organizzativa (OU)	RielloUPS	 <p>https://netmancento.local</p> <p>Informazioni su netmancento.local</p> <p>La connessione è sicura</p> <p>Autorizzazioni per questo sito</p> <p>Cookie (1 cookie in uso)</p> <p>Prevenzione rilevamento per questo sito (Bilanciato)</p> <p>Rilevamenti (0 bloccati)</p> <p>Questo sito ha un certificato valido, emesso da un'autorità attendibile. Le informazioni (ad esempio le password o le carte di credito) verranno inviate in modo sicuro a questo sito e non possono essere intercettate. Assicurati sempre di essere nel sito desiderato prima di immettere informazioni. Altre informazioni</p> <p>Visualizzatore certificati: netmancento</p> <p>Generali Dettagli</p> <p>Rilasciato a</p> <table border="1"> <tr><td>Nome comune (CN)</td><td>netmancento</td></tr> <tr><td>Organizzazione (O)</td><td>Riello</td></tr> <tr><td>Unità organizzativa (OU)</td><td>RielloUPS</td></tr> </table>	Nome comune (CN)	netmancento	Organizzazione (O)	Riello	Unità organizzativa (OU)	RielloUPS	 <p>https://netmancento.local</p> <p>Site information for netmancento.local</p> <p>Connection secure</p> <p>Firefox has blocked parts of this page that are not secure.</p> <p>Connection verified by a certificate issuer that is not recognised by Mozilla.</p> <p>https://netmancento.local</p> <p>Connection security for netmancento.local</p> <p>You are securely connected to this site.</p> <p>Verified by: RPS SpA Root CA</p> <p>Mozilla does not recognise this certificate issuer. It may have been added from your operating system or by an administrator. Learn More</p>	<p>✓</p> <p>CA conosciuta dal browser (certificato installato nel browser)</p>
Nome comune (CN)	netmancento														
Organizzazione (O)	Riello														
Unità organizzativa (OU)	RielloUPS														
Nome comune (CN)	netmancento														
Organizzazione (O)	Riello														
Unità organizzativa (OU)	RielloUPS														
 <p>Non sicuro https://netmancento.local</p> <p>netmancento.local</p> <p>La tua connessione a questo sito non è sicura. Non dovresti inserire dati sensibili in questo sito (ad esempio password o carte di credito) perché potrebbero essere intercettati da utenti malintenzionati. Scopri di più</p> <p>Il certificato non è valido</p> <p>Cookie e dati dei siti</p> <p>Impostazioni sito</p> <p>Visualizzatore certificati: netmancento</p> <p>Generali Dettagli</p> <p>Rilasciato a</p> <table border="1"> <tr><td>Nome comune (CN)</td><td>netmancento</td></tr> <tr><td>Organizzazione (O)</td><td>Riello</td></tr> <tr><td>Unità organizzativa (OU)</td><td>RielloUPS</td></tr> </table> <p>La connessione non è privata</p> <p>Gli utenti malintenzionati potrebbero provare a carpire informazioni da netmancento.local (ad esempio, password, messaggi).</p> <p>NET:ERR_CERT_AUTHORITY_INVALID</p>	Nome comune (CN)	netmancento	Organizzazione (O)	Riello	Unità organizzativa (OU)	RielloUPS	 <p>Non sicuro https://netmancento.local</p> <p>Informazioni su netmancento.local</p> <p>La tua connessione a questo sito non è sicura. Non immettere informazioni riservate su questo sito (ad esempio, password o carte di credito), perché potrebbero essere rubate da utenti malintenzionati.</p> <p>Autorizzazioni per questo sito</p> <p>Cookie (0 cookie in uso)</p> <p>Prevenzione rilevamento per questo sito (Bilanciato)</p> <p>Rilevamenti (0 bloccati)</p> <p>La tua connessione a questo sito non è sicura. Il certificato per questo sito non è valido. Poiché la connessione non è sicura, le informazioni, ad esempio password o carte di credito, non saranno inviate in modo sicuro a tale sito e potrebbero essere intercettate o visualizzate da altri utenti. È consigliabile di non inserire informazioni personali in questo sito e di evitare di usarlo. Altre informazioni</p> <p>La tua connessione non è privata</p> <p>Gli utenti malintenzionati potrebbero tentare di rubare le tue informazioni da netmancento.local (ad esempio password, messaggi o carte di credito).</p> <p>NET:ERR_CERT_AUTHORITY_INVALID</p>	 <p>Not Secure https://netmancento.local</p> <p>Site information for netmancento.local</p> <p>Connection not secure</p> <p>Connection security for netmancento.local</p> <p>You are not securely connected to this site.</p> <p>Your connection to this site is not private. Information you submit could be viewed by others (like passwords, messages, credit cards, etc.).</p> <p>More information</p> <p>Someone could be trying to impersonate the site and you should not continue.</p> <p>Web sites prove their identity via certificates. Firefox does not trust netmancento.local certificate issuer is unknown, the certificate is self-signed, or the server is not send intermediate certificates.</p> <p>Error code: SEC_ERROR_UNKNOWN_ISSUER</p>	<p>✗</p> <p>CA non conosciuta dal browser (certificato installato nel browser)</p>						
Nome comune (CN)	netmancento														
Organizzazione (O)	Riello														
Unità organizzativa (OU)	RielloUPS														

	<p>Netman 204: + HTTPS + certificato autofirmato</p>	
		

Risoluzione dei problemi
Errori del Web browser

Con certificati errati, la navigazione di pagine web con *Netman 204* può mostrare diversi messaggi che nascondono molte ragioni. Ecco alcuni messaggi da sapere:



La connessione non è privata

Gli utenti malintenzionati potrebbero provare a carpire le tue informazioni da **netmanmille.local** (ad esempio, password, messaggi o carte di credito). [Ulteriori informazioni](#)

NET::ERR_CERT_COMMON_NAME_INVALID

NET::ERR_CERT_COMMON_NAME_INVALID

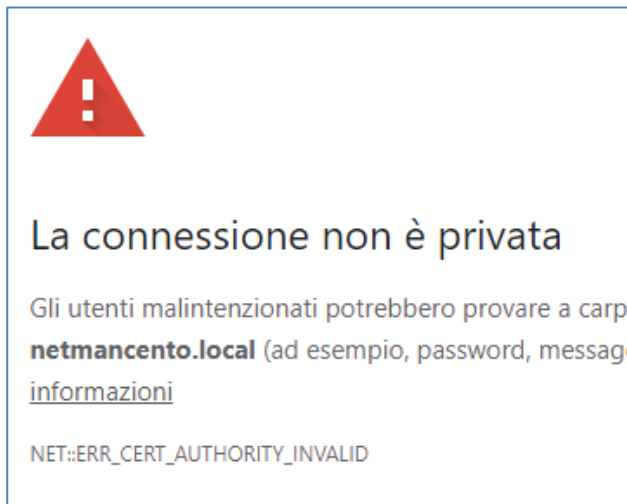
Il certificato personalizzato impostato per HTTPS è valido per un nome host/FQDN diverso. Se l'utente incontra questo messaggio significa che il certificato personalizzato attivo copre un nome host Netman 204 diverso, non il nome host della *Netman 204* in esecuzione.

L'utente può continuare l'attività Web ma non è sicura a causa del certificato errato.

E.g.:

Hostname Netman 204 attivo: **netmanmille.local**

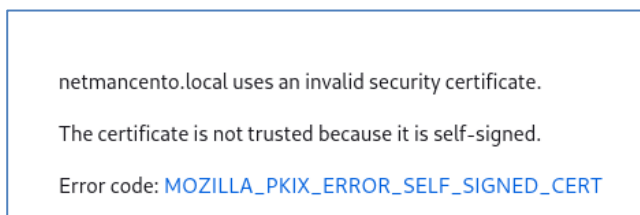
Certificato per FQDN/hostname: **netmancento.local**



NET::ERR_CERT_AUTHORITY_INVALID

Questo messaggio suggerisce principalmente che il **certificato CA è sbagliato**.

Altre volte può significare che il certificato è un **certificato autofirmato** (ad esempio in Chrome).

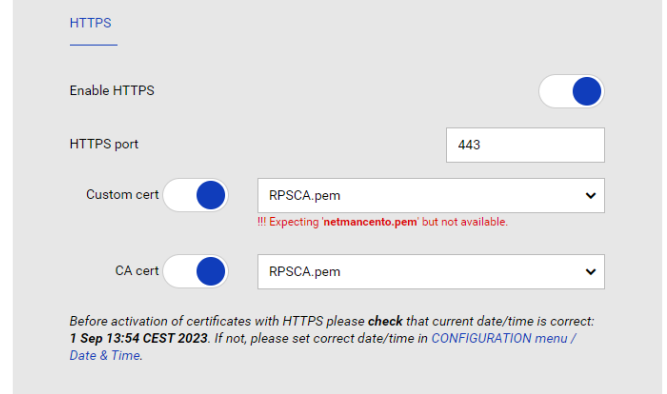


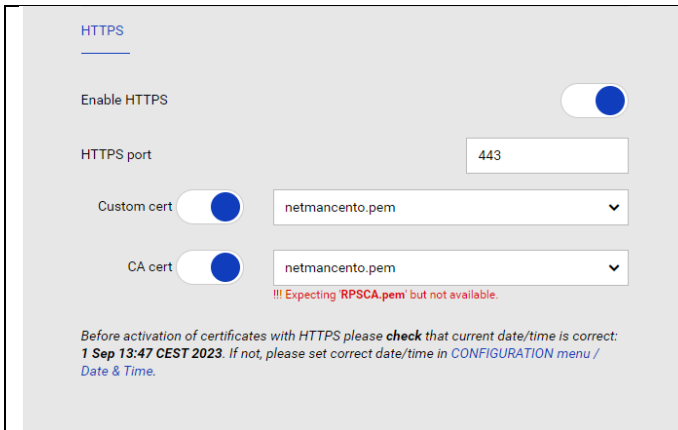
MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT

Questo messaggio è chiaramente correlato a un certificato personalizzato **autofirmato**.

Certificati mancanti

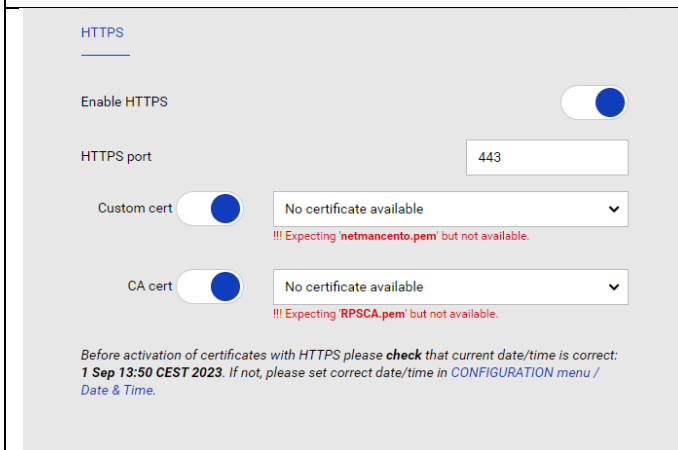
Se nella configurazione sono impostati certificati personalizzati e CA, ma non sono disponibili (magari eliminati), vengono visualizzati alcuni avvisi e vengono intraprese azioni:

Avviso	Azione effettuata
	<p>La configurazione per HTTPS, al prossimo riavvio, utilizzerà il valore predefinito: CERTIFICATO AUTOFIRMATO ignorando il certificato personalizzato "netmancento.pem" mancante e ignorando la CA ancora disponibile "RPSCA.pem"</p> <p><i>Motivo: il certificato CA è fortemente correlato al certificato personalizzato mancante.</i></p>



La configurazione per HTTPS, al prossimo riavvio, utilizzerà solo:
CUSTOM CERT
 ignorando la CA mancante
 “RPSCA.pem”.

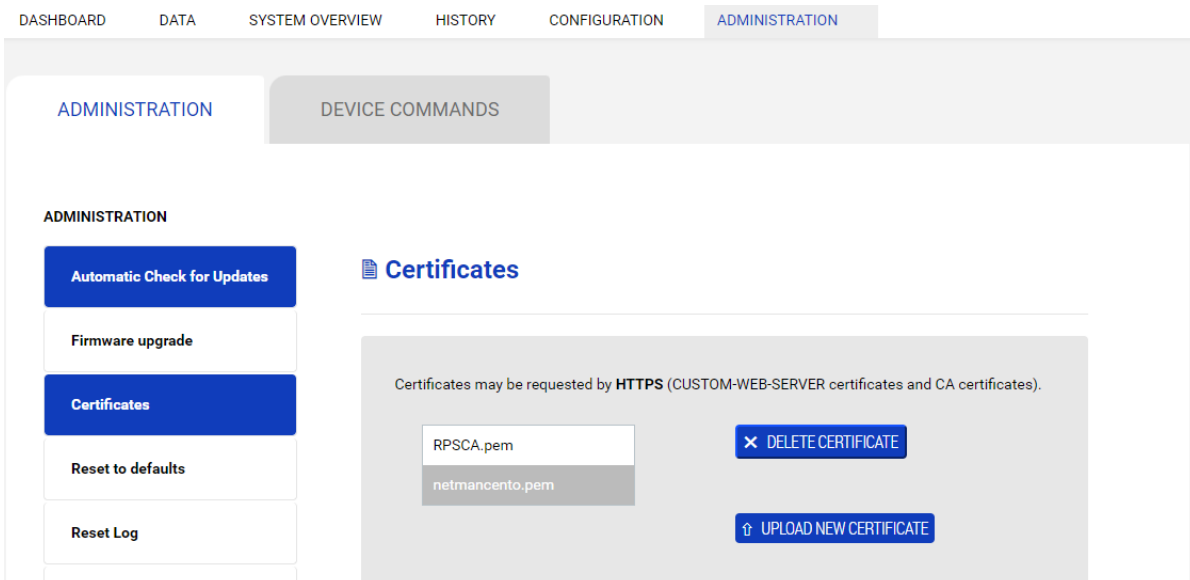
Motivo: senza CA l'HTTPS è ancora raggiungibile, a parte gli avvisi.



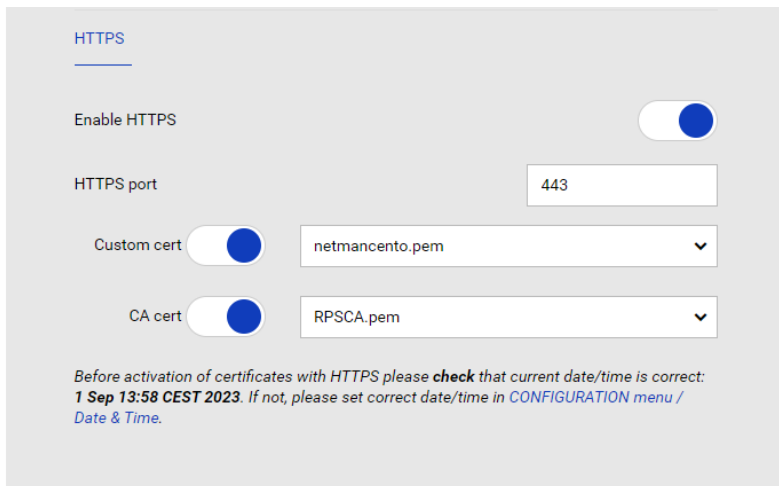
Mancano sia il certificato personalizzato che quello CA, verrà utilizzato soltanto il valore predefinito:
SELF_SIGNED CERTIFICATE

Motivo: senza i certificati HTTPS è ancora raggiungibile con certificato interno autofirmato, a parte gli avvisi.

In ogni caso di certificati mancanti, l'utente dovrà caricare i certificati corretti nel menu dedicato:



e ripristinare il comportamento corretto senza gli avvisi in rosso:



HTTPS Web non raggiungibile:

- Netman 204 Web non sta rispondendo.
- Web browser riporta errori collegandosi alla Netman 204

Cause possibili:

- Certificate malformato (CUSTOM e/o CA)
- Certificato scaduto (CUSTOM e/o CA)
- Errata data/ora nella Netman 204

Come risolvere:

Via comandi SSH (rete):

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

o via connessione con cavo USB:

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

<p>Scegliere l'opzione "Expert mode"</p>	<pre> /-----/ / Netman 204 / /-----/ Setup.....: View status....: Change password: Service log....: Wi-Fi setup....:no card installed Factory reset..: Expert mode....:←- inet 10.1.10.4 netmask 255.255.0.0 broadcast 10.1.255.255 Press [ESC] for logout SysVer. B22-3 - AppVer. 04.01.012 </pre>
--	---

<p>E configurare a HTTP base la Netman 204 manualmente:</p> <pre>set http_enable true set http_port 80 set https_enable false</pre> <p>quindi riavviare la Netman 204:</p> <pre>reboot</pre>	<pre>Netman maintenance console Available commands: help prints this help get shows all values set <VAR> <VALUE> set VAR to VALUE delete <VAR> removes VAR sendtrap + <TRAPCODE> send a test SNMP trap (alarm added) sendtrap - <TRAPCODE> send a test SNMP trap (alarm removed) testemail send a test email testwol send the wake-on-lan packets reboot reboot the Netman erasefram erase the FRAM module clearlog clear data log and event log exit closes the connection netman>set http_enable true netman>set http_port 80 netman>set https_enable false netman>reboot Connection to netmancento.local closed.</pre>
--	---

Dopo il riavvio, *Netman 204* consentirà la **connessione tramite la modalità base HTTP** ignorando qualsiasi impostazione HTTPS o certificato, mantenendo tutte le altre configurazioni invariate.

Recupero della password

Se la password dell'utente admin viene modificata o dimenticata, è possibile recuperarla utilizzando la chiave di sblocco fornita dal servizio assistenza del produttore.

Per ottenere la chiave di sblocco, è necessario inviare il codice di assistenza di *Netman 204* al servizio assistenza. Il codice può essere letto mediante USB o HTTP.

Per la lettura mediante USB, accedere a *Netman 204* con il nome utente "user" e la password "user".

Per la lettura mediante HTTP, quando si immettono credenziali non valide nella pagina di login viene offerto un link che conduce al recupero della password. Cliccare il link per iniziare la recovery.

In entrambi i casi viene visualizzato un messaggio come il seguente:

To restore the default password, please enter the unlock key. (Per ripristinare la password predefinita, immettere la chiave di sblocco.)

If you don't know it, please send to service this code: (Se non si dispone della chiave, inviare questo codice all'assistenza:)

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



Notare come la chiave di sblocco sia valida soltanto per il codice di assistenza specifico di ogni *Netman 204*.

Configurazione Wi-Fi (richiesta scheda opzionale)



Per la connessione Wi-Fi, è richiesta una scheda opzionale. La scheda Wi-Fi non è fornita in dotazione con *Netman 204* e deve essere acquistata separatamente.

Dopo avere installato la scheda Wi-Fi opzionale, è possibile accedere al menu "Wi-Fi setup".



Per *Netman 204*, la connessione Wi-Fi è un'alternativa a Ethernet con cavo e le due opzioni si escludono a vicenda. Pertanto, dopo avere attivato la connessione Wi-Fi, non è più possibile utilizzare Ethernet con cavo.

Dopo aver selezionato Wi-Fi setup viene visualizzato il seguente messaggio:

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

Immettere "n" per utilizzare Ethernet o "y" per utilizzare la connessione Wi-Fi. Nel secondo caso, viene visualizzato un elenco dei punti di accesso Wi-Fi disponibili con la seguente richiesta:

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

Digitare il codice SSID del punto di accesso Wi-Fi desiderato.

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

Nella seguente schermata è possibile immettere la password di autenticazione della connessione Wi-Fi.

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

Dopo la conferma, viene nuovamente visualizzata la schermata di configurazione principale. Al successivo riavvio, *NetMan 204* utilizzerà la connessione Wi-Fi, anziché Ethernet.

Modalità Expert

La modalità Expert consente di attivare la configurazione dei parametri avanzati riservata ai tecnici esperti. Vengono supportati i seguenti comandi:

help	stampa la guida
get	mostra tutti i valori
set <VAR> <VALUE>	imposta VAR su VALUE
delete <VAR>	rimuove VAR
sendtrap + <TRAPCODE>	invia una trap SNMP di test (allarme aggiunto)
sendtrap - <TRAPCODE>	invia una trap SNMP di test (allarme tolto)
testemail	invia una email di test
reboot	riavvia <i>NetMan 204</i>
erasefram	cancella il modulo FRAM
clearlog	cancella data log e event log
exit	chiude la connessione

CONFIGURAZIONE DI DIVERSI DISPOSITIVI

Se occorre configurare diversi dispositivi *NetMan 204* con parametri analoghi, è possibile configurare il primo *NetMan 204*, quindi collegarsi mediante FTP con il nome utente admin, scaricare tutti i file di configurazione contenuti nella cartella /cfg e caricarli tutti mediante FTP nella cartella /cfg di tutti i dispositivi da configurare.

SERVICE LOG

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

- DEVICE**: A table with the following data:

Model	VST 1500
Serial number	-
Power [kVA]	1.5
Power [kW]	1.2
Battery capacity [Ah]	7
Battery voltage [Vdc]	48
Firmware version	SWM039-01-03
- DEVICE CONFIGURATION**: A table with the following data:

PRTK code	GPSE11201--
Name	Netman204????
- NETWORK CARD**: A table with the following data:

Card version	e3300003 4GB
Serial Number	62B9CFBC
MAC Address	00:02:63:06:3a:75
Application version	03.11
System version	S20-1
Kernel	4.9.78-EK20200805
Current date	1 Oct 09:27 CEST 2020
- SERVICE LOG**: A section with a blue button labeled "DOWNLOAD SERVICE LOG".
- NETWORK CONFIGURATION**: A table with the following data:

Hostname	netman63063a75	IPv4 Address	10.1.10.230	Gateway	10.1.1.1
DHCP enabled	yes	Netmask	255.255.0.0	Primary DNS	10.1.5.10
		IPv6 Address	fe80::202:63ff:fe06:3a75	Secondary DNS	10.3.5.3

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

In caso di problemi oppure se la *Netman 204* non si comporta come ci si aspetterebbe, è consigliato lo scaricamento del service log.

Per creare e scaricare il service log seguire questi passaggi:

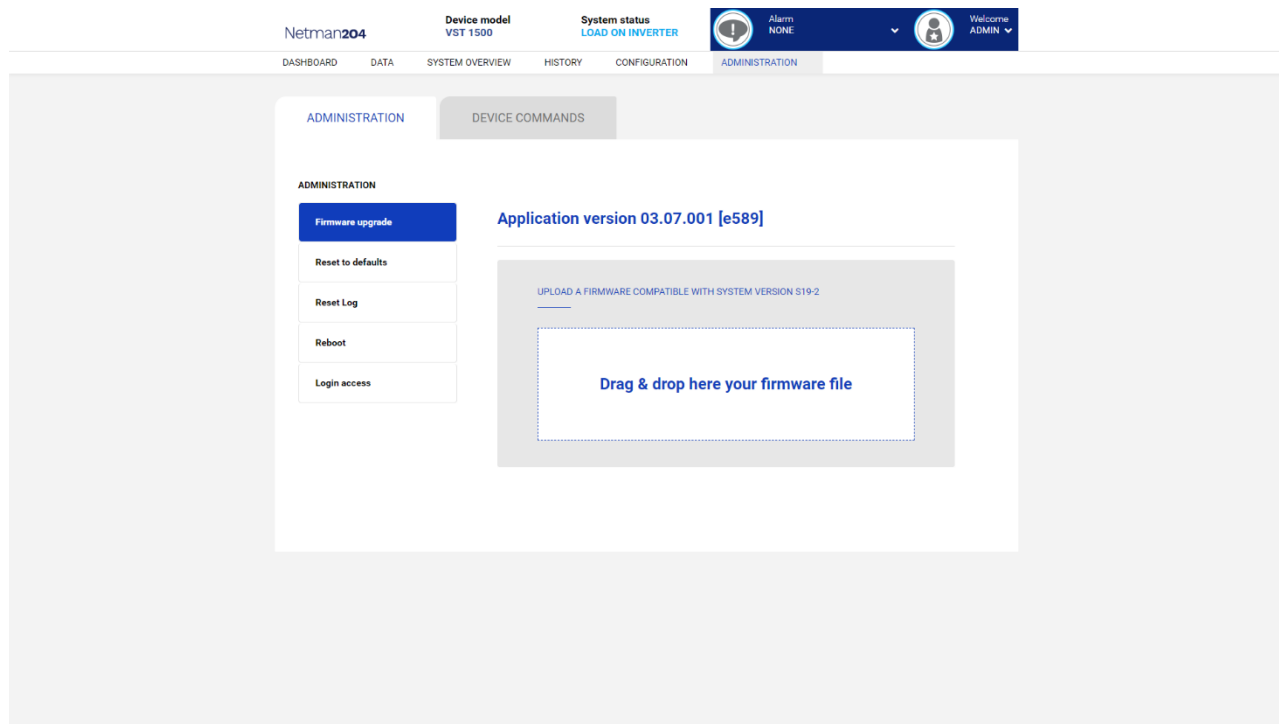
1. Eseguire il login come "admin"
2. Fare click su "System overview"
3. Fare click su "Download service log"

Il service log verrà scaricato in pochi secondi. Deve essere inviato al centro service autorizzato locale per diagnosticare adeguatamente il problema.

AGGIORNAMENTO DEL FIRMWARE

È possibile aggiornare il firmware di *Netman 204* mediante HTTP o FTP.
Un file di upgrade valido ha nome `fwapp.204`. Se si scarica un file `.zip`, è necessario estrarre un `fwapp.204` dalla cartella con un nome che corrisponde al sistema operativo della *Netman 204*.

AGGIORNAMENTO DEL FIRMWARE MEDIANTE HTTP



Collegarsi mediante HTTP al dispositivo *Netman 204* da aggiornare immettendo nel browser web il nome host o l'indirizzo IP e accedendo con il nome utente admin (password predefinita: "admin"). Quindi cliccare sul link "Administration".
Trascinare il file di upgrade nell'area indicata. Al termine del caricamento del file di aggiornamento, viene eseguito il riavvio automatico di *Netman 204*.

AGGIORNAMENTO DEL FIRMWARE MEDIANTE FTP

Collegarsi mediante FTP con il nome utente "fwupgrade" (password predefinita: "fwupgrade") e copiare il firmware aggiornato nella cartella /fwupgrade. Riavviare quindi la scheda premendo il pulsante di reset.

CONFIGURAZIONE DI SNMP

Per configurare l'accesso a SNMP, è possibile usare la pagina web wizard per una configurazione semplice. Per la configurazione avanzata è necessario modificare `snmp.conf`. Questo file può essere scaricato e caricato mediante dalla pagina web oppure tramite FTP utilizzando il nome utente "admin" (password predefinita: "admin").

Netman 204 analizza ciascuna riga del file per verificare che inizi con una delle seguenti parole chiave:

- `#`: riservata ai commenti, questa riga viene ignorata.
- `addUser`: per aggiungere un nuovo utente e impostare le password
- `addGroup`: per inserire un utente in un gruppo
- `addAccessEntry`: per attivare i privilegi di accesso a un gruppo
- `addView`: per aggiungere privilegi
- `addManager`: per aggiungere il gestore SNMP che riceverà trap SNMP.

La sintassi corretta di `addUser` è:

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

<userName> è il nome dell'utente.

<authProtocol> è il protocollo per l'autenticazione di questo utente durante le sessioni di SNMP. I valori consentiti sono i seguenti:

- `noauth` (non verrà utilizzata alcuna autenticazione)
- `md5` (verrà utilizzato MD5 per l'autenticazione)
- `sha` (verrà utilizzato SHA per l'autenticazione)

<privProtocol> è il protocollo per la privacy di questo utente durante le sessioni di SNMP. I valori consentiti sono i seguenti:

- `nopriv` (non verrà utilizzata alcuna privacy)
- `des` (verrà utilizzato DES per la privacy)

<authPassword> è la password per l'autenticazione. Deve essere impostata su * quando non viene utilizzata.

<privPassword> è la password per la privacy. Deve essere impostata su * quando non viene utilizzata.

La sintassi corretta di `addGroup` è:

```
addGroup <securityModel> <userName> <groupName>
```

<securityModel> è il modello di sicurezza. Se viene utilizzata l'autenticazione e/o la privacy, questo valore deve essere impostato su USM. I valori consentiti sono i seguenti:

- `USM` (modello di sicurezza basato sull'utente con SNMPv3)
- `v2` (SNMPv2)
- `v1` (SNMPv1)

<userName> è il nome dell'utente; deve corrispondere a uno dei nomi di utenti definiti con `addUser`.

<groupName> è il nome del gruppo.

Notare come ciascun nome utente possa essere assegnato soltanto a un gruppo.

La sintassi corretta di `addAccessEntry` è:

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

<groupName> è il nome del gruppo a cui è applicato questo diritto di accesso; deve corrispondere a uno dei nomi di gruppo definiti con `addGroup`.

<contextName> è il nome del contesto.

<securityModel> è il modello di sicurezza che deve essere utilizzato per ottenere questo diritto di accesso; deve corrispondere al modello di sicurezza definito con addGroup.

<securityType> è il livello minimo di sicurezza che deve essere utilizzato per ottenere questo diritto di accesso. I valori consentiti sono i seguenti:

- *noauthnopriv* (nessuna autenticazione e nessuna privacy)
- *authnopriv* (autenticazione, ma nessuna privacy)
- *authpriv* (autenticazione e privacy)

<contextMatch> tipo di corrispondenza richiesto I valori consentiti sono i seguenti:

- *exact* (il nome del contesto deve corrispondere esattamente al valore di contextName)
- *prefix* (il nome del contesto deve corrispondere ai caratteri iniziali del valore di contextName)

<readView> nome di visualizzazione MIB autorizzato utilizzato per l'accesso alla lettura; deve corrispondere a uno dei nomi di visualizzazione.

<writeView> nome di visualizzazione MIB autorizzato utilizzato per l'accesso alla scrittura; deve corrispondere a uno dei nomi di visualizzazione.

<notifyView> nome di visualizzazione MIB autorizzato utilizzato per l'accesso alla notifica; deve corrispondere a uno dei nomi di visualizzazione.

La sintassi corretta di addView è:

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

<viewName> è il nome della visualizzazione.

<subtree> è la sottostruttura OID che definisce una famiglia di sottostrutture di visualizzazione se combinata all'istanza di MASK corrispondente.

<mask> mask per filtrare l'OID.

<included> l'OID può essere inclusa o esclusa. I valori consentiti sono i seguenti:

- *included* (per l'inclusione)
- *excluded* (per l'esclusione)

La sintassi corretta di addManager è:

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

<security> è il tipo di sicurezza per la notifica. I valori consentiti sono i seguenti:

- *USM* (modello di sicurezza basato sull'utente con SNMPv3)
- *V2* (SNMPv2)
- *v1* (SNMPv1)

<ipAddress> è l'indirizzo IP del gestore SNMP.

<credentials> può essere il nome utente (se viene utilizzata la sicurezza USM) o la comunità di trap (se viene utilizzata la sicurezza v1)

<securityType> può essere:

- *noauthnopriv* (per SNMPv1 e SNMPv2)
- *authpriv* (per SNMPv3)

addManager non consente l'uso di valori doppi (un indirizzo IP può ricevere soltanto un trap).

Viene riportato un esempio di snmp.conf; gli utenti predefiniti autorizzati sono indicati come segue:

Nome	Protocollo aut.	Protocollo priv.	Password aut.	Password priv.
unsecureUser	Noauth	nopriv		
MD5	md5	nopriv	MD5UserAuthPassword	
SHA	Sha	nopriv	SHAUserAuthPassword	
MD5DES	md5	des	MD5DESUserAuthPassword	MD5DESUserPrivPassword
SHADES	Sha	des	SHADESUserAuthPassword	SHADESUserPrivPassword

Descrizione trap:

OID	Descrizione
1.3.6.1.2.1.33.2.0.1	Inviata ogni volta che l'UPS va da batteria, poi inviata ogni minuto finché l'UPS ritorna su rete.
1.3.6.1.2.1.33.2.0.3	Inviata ogni volta che appare un allarme. L'OID che corrisponde all'allarme è aggiunto alla varbind.
1.3.6.1.2.1.33.2.0.4	Inviata ogni volta che scompare un allarme. L'OID che corrisponde all'allarme è aggiunto alla varbind.

PROTOCOLLO MODBUS TCP/IP

Questo servizio è attivo sulla porta TCP 502. Di seguito viene fornito un elenco delle funzioni supportate e dei registri accessibili.

FUNZIONI SUPPORTATE

FUNZIONE SUPPORTATA	DESCRIZIONE FUNZIONE	AREA DATI ACCESSIBILE
1 (0x01)	LETTURA BIT	STATI
2 (0x02)		STATI
3 (0x03)	LETTURA REGISTRI	TUTTE
4 (0x04)		TUTTE
6 (0x06)	SCRITTURA REGISTRO SINGOLO	COMANDI
16 (0x10)	SCRITTURA REGISTRI MULTIPLI	COMANDI

UPS: TABELLE DI STATI, MISURE, VALORI NOMINALI E COMANDI

REGISTRO ⁽¹⁾		UPS - STATI	BIT ⁽²⁾	
NUMERO	INDIRIZZO		NUMERO	INDIRIZZO
1	0		1	0
		Test in esecuzione [0=No / 1=Si]	2	1
			3	2
		Shutdown attivo [0=No / 1= Si]	4	3
			5	4
		Batteria carica [0=No / 1= Si]	6	5
		Batteria in carica [0=No / 1= Si]	7	6
		Bypass non buono [0=No / 1= Si]	8	7
			9	8
		Funzionamento normale [0=No / 1= Si]	10	9
			11	10
		Da bypass [0=No / 1= Si]	12	11
		Batteria quasi scarica [0=No / 1= Si]	13	12
		Batteria in funzione [0=No / 1= Si]	14	13
		UPS in blocco [0=No / 1= Si]	15	14
		Uscita alimentata [0=No / 1= Si]	16	15
		17÷28	16÷27	
2	1	Rete di ingresso presente [0=No / 1= Si]	29	28
		Allarme sovratemperatura [0=No / 1= Si]	30	29
		Allarme sovraccarico [0=No / 1= Si]	31	30
		UPS in anomalia [0=No / 1= Si]	32	31
3	2		33÷48	32÷47
4	3		49÷63	48÷62
		Perdita di comunicazione con UPS [0=No / 1= Si]	64	63
5÷8	4÷7		65÷128	64÷127

⁽¹⁾ Il registro numero *n* deve essere indirizzato *n-1* nel pacchetto dati

⁽²⁾ Il bit numero *n* deve essere indirizzato *n-1* nel pacchetto dati.

REGISTRO ⁽¹⁾		UPS - MISURE	UNITÀ
NUMERO	INDIRIZZO		
9÷11	8÷10		
12	11	Tensione di rete di ingresso V1 (stellata)	V
13	12	Tensione di rete di ingresso V2 (stellata)	V
14	13	Tensione di rete di ingresso V3 (stellata)	V
15	14	Corrente di ingresso fase L1	0,1*A
16	15	Corrente di ingresso fase L2	0,1*A
17	16	Corrente di ingresso fase L3	0,1*A
18	17	Frequenza di ingresso	0,1*Hz
19÷21	18÷20		
22	21	Tensione di rete di bypass V1 (stellata)	V
23	22	Tensione di rete di bypass V2 (stellata)	V
24	23	Tensione di rete di bypass V3 (stellata)	V
25	24	Frequenza di bypass	0,1*Hz
26	25	Tensione di uscita V1 (stellata)	V
27	26	Tensione di uscita V2 (stellata)	V
28	27	Tensione di uscita V3 (stellata)	V
29÷31	28÷30		
32	31	Corrente di uscita fase L1	0,1*A
33	32	Corrente di uscita fase L2	0,1*A
34	33	Corrente di uscita fase L3	0,1*A
35	34	Corrente di picco di uscita fase L1	0,1*A
36	35	Corrente di picco di uscita fase L2	0,1*A
37	36	Corrente di picco di uscita fase L3	0,1*A
38	37	Carico fase L1	%
39	38	Carico fase L2	%
40	39	Carico fase L3	%
41	40	Potenza attiva in uscita fase L1	0,1 kW
42	41	Potenza attiva in uscita fase L2	0,1 kW
43	42	Potenza attiva in uscita fase L3	0,1 kW
44	43	Frequenza di uscita	0,1*Hz
45÷47	44÷46		
48	47	Tensione di batteria	0,1*V
49	48	Tensione positiva di batteria	0,1*V
50	49	Tensione negativa di batteria	0,1*V
51	50	Corrente di batteria	0,1*A
52	51	Capacità residua di batteria	%
53	52		
54	53	Tempo residuo di autonomia	Minuti
55÷58	54÷57		
59	58	Energia totale in uscita (32 bit)	Registro meno significativo
60	59		Registro più significativo
61	60		
62	61	Temperatura interna UPS	°C
63	62	Temperatura sensore 1	°C
64	63	Temperatura sensore 2	°C
65÷72	64÷71		

⁽¹⁾ Il registro numero *n* deve essere indirizzato *n-1* nel pacchetto dati.



Alcune misure potrebbero non essere disponibili per tutti gli UPS. In questo caso, il relativo registro continua a riportare il valore 0xFFFF.

REGISTRO ⁽¹⁾		UPS – VALORI NOMINALI	UNITÀ
NUMERO	INDIRIZZO		
73÷77	72÷76		
78	77	Tensione nominale (stellata) di uscita	V
79	78	Frequenza nominale di uscita	0,1*Hz
80	79	Potenza nominale di uscita	100*VA
81÷83	80÷82		
84	83	Capacità nominale di batteria (incluse espansioni di batteria)	Ah
85	84	Rami di batteria	(1 o 2)
86	85	Tipo di batteria	Intero
87÷112	86÷111		

REGISTRO ⁽¹⁾		UPS - COMANDI	UNITÀ
NUMERO	INDIRIZZO		
113	112	Codice comando ⁽²⁾	Intero
114	113	Tempo di ritardo spegnimento (shutdown)	Secondi
115	114	Tempo di ritardo accensione (restore)	Minuti
116	115		
117	116	Esito comando ⁽³⁾	Intero
118	117		

REGISTRO ⁽¹⁾		DIAGNOSTICA	UNITÀ
NUMERO	INDIRIZZO		
119	118	Contatore di messaggi corretti elaborati	Intero
120	119	Contatore di messaggi NON corretti elaborati	Intero

⁽¹⁾ Il registro numero **n** deve essere indirizzato **n-1** nel pacchetto dati.

⁽²⁾ Vedere la sezione "Codici comandi"

⁽³⁾ Esito comando = Codice comando se il comando è gestito dall'UPS

Esito comando = Codice comando + 100 se il comando NON è gestito dall'UPS

Esito comando = 0 se il Codice comando è errato

REGISTRO ⁽¹⁾		FLAG SPECIALI (UPS SERIE SENTR)	UNITÀ
NUMERO	INDIRIZZO		
121	120	Byte 1 of "s = xx.." code / Byte 2 of "s = ..xx" code	Flag
122	121	Byte 1 of "c = xx.." code / Byte 2 of "c = ..xx" code	Flag
123	122	Byte 1 of "b = xx.." code / Byte 2 of "b = ..xx" code	Flag
124	123	Byte 1 of "r = xx-.." code / Byte 2 of "r = ..xx-.." code	Flag
125	124	Byte 3 of "r =-xx" code / Byte 1 of "i = xx-.." code	Flag
126	125	Byte 2 of "i = ..xx-.." code / Byte 3 of "i =-xx" code	Flag
127	126	Byte 1 of "a = xx-...." code / Byte 2 of "a = ..xx-...." code	Flag
128	127	Byte 3 of "a =-xx.." code / Byte 4 of "a =-..xx" code	Flag

REGISTRO ⁽¹⁾		DATI DI NETMAN	UNITÀ
NUMERO	INDIRIZZO		
129	128	Versione firmware	Intero
130÷131	129÷130		

⁽¹⁾ Il registro numero **n** deve essere indirizzato **n-1** nel pacchetto dati.

⁽²⁾ Per decodificare questi registri, fare riferimento al manuale dell'UPS.

UPS: CODICI COMANDI

CODICE		COMANDO
1	(0x0001)	Spegnimento (Shutdown)
2	(0x0002)	Spegnimento e riaccensione (shutdown e restore)
3	(0x0003)	Cancellazione (codice 1, 2, 12)
12	(0x000C)	UPS da bypass
20	(0x0014)	Test batteria
22	(0x0016)	Test pannello

Fare riferimento al documento tabella Modbus per informazioni aggiuntive riguardo ai registri per altri dispositivi.

CONFIGURAZIONE BACNET/IP

OGGETTO	DESCRIZIONE	UNITÀ
Analogue Input 0	Tensione di ingresso linea 1	V
Analogue Input 1	Tensione di ingresso linea 2	V
Analogue Input 2	Tensione di ingresso linea 3	V
Analogue Input 3	Corrente di ingresso linea 1	A
Analogue Input 4	Corrente di ingresso linea 2	A
Analogue Input 5	Corrente di ingresso linea 3	A
Analogue Input 6	Frequenza di ingresso	Hz
Analogue Input 7	Tensione di bypass linea 1	V
Analogue Input 8	Tensione di bypass linea 2	V
Analogue Input 9	Tensione di bypass linea 3	V
Analogue Input 10	Frequenza di bypass	Hz
Analogue Input 11	Tensione di uscita linea 1	V
Analogue Input 12	Tensione di uscita linea 2	V
Analogue Input 13	Tensione di uscita linea 3	V
Analogue Input 14	Corrente di uscita linea 1	A
Analogue Input 15	Corrente di uscita linea 2	A
Analogue Input 16	Corrente di uscita linea 3	A
Analogue Input 17	Corrente di picco di uscita linea 1	A
Analogue Input 18	Corrente di picco di uscita linea 2	A
Analogue Input 19	Corrente di picco di uscita linea 3	A
Analogue Input 20	Potenza di uscita linea 1	W
Analogue Input 21	Potenza di uscita linea 2	W
Analogue Input 22	Potenza di uscita linea 3	W
Analogue Input 23	Frequenza di uscita	Hz
Analogue Input 24	Carico in uscita linea 1	%
Analogue Input 25	Carico in uscita linea 2	%
Analogue Input 26	Carico in uscita linea 3	%
Analogue Input 27	Tensione di batteria	V
Analogue Input 28	Corrente di batteria	A
Analogue Input 29	Capacità di batteria	%
Analogue Input 30	Temperatura UPS	°C
Analogue Input 31	Autonomia	min
Analogue Input 32	Potenza nominale	VA
Binary Input 0	Stato dell'energia di rete	Present / Not present
Binary Input 1	Stato del bypass	Active / Not active
Binary Input 2	Stato della batteria	Working / Not working
Binary Input 3	Livello della batteria	Low / Not low
Binary Input 4	UPS in blocco	Locked / Not locked
Binary Input 5	UPS in anomalia	Fail / Not fail
Binary Input 6	Carico	Overload / Normal
Binary Input 7	Temperatura	Overtemperature / Normal
Binary Input 8	Bypass non buono	Bad / Not bad
Binary Input 9	Sostituzione della batteria	Replace / Not replace
Binary Input 10	Spegnimento (shutdown)	Active / Not active
Binary Input 11	Spegnimento (shutdown) imminente	Imminent / Not imminent
Binary Input 12	Stato della comunicazione	Lost / OK
Analog Input 33	System status gruppo 1	
Analog Input 34	System status gruppo 2	

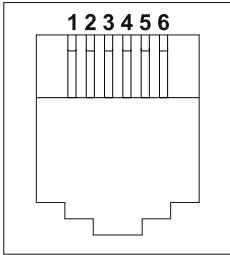
Analog Input 35	System status gruppo 3	
Analog Input 36	Allarmi modulo Bypass	
Analog Input 37	Allarmi Power module 1	
Analog Input 38	Allarmi Power module 2	
Analog Input 39	Allarmi Power module 3	
Analog Input 40	Allarmi Power module 4	
Analog Input 41	Allarmi Power module 5	
Analog Input 42	Allarmi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

EVENTLOG CODES

EVENTO	DESCRIZIONE
Battery low	Battery Low oppure Shutdown imminent
On battery	Da batteria
On bypass	Da bypass
UPS lock	UPS in blocco
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)	Allarme generico UPS (SENTR)
UPS internal alarm (SENTR)	Allarme interno UPS (SENTR)
IRMS blackout	IRMS blackout
IRMS overload	IRMS sovraccarico
Synchro bad	Synchronisation wrong
Overload/overtemp	Overload/Overtemperature
xTS failure	ATS/STS failure
transfer active	Trasferimento del carico attivo
source S1 bad	Sorgente S1 non buona
source S2 bad	Sorgente S2 non buona
MANUAL_BYPASS_ACTIVE_C01	Bypass manuale attivo
LOW_INPUT_VOLTAGE_A01	Tensione bassa di ingresso
HIGH_INPUT_VOLTAGE_A02	Tensione alta di ingresso
OVERLOAD1_F01	Sovraccarico uscita 1
OVERLOAD2_F02	Sovraccarico uscita 2
OVERLOAD3_F03	Sovraccarico uscita 3
OVERLOAD4_F04	Sovraccarico uscita 4
OVERLOAD5_F05	Sovraccarico uscita 5
OVERLOAD6_F06	Sovraccarico uscita 6
OVERLOAD7_F07	Sovraccarico uscita 7
OVERLOAD8_F08	Sovraccarico uscita 8
LOW_INPUT_CURRENT_F09	Corrente di ingresso bassa
HIGH_INPUT_CURRENT_F10	Corrente di ingresso alta
POWERFAIL_AUX1_F11	Powerfail auxiliary powersupply 1
POWERFAIL_AUX2_F12	Powerfail auxiliary powersupply 2
OVERLOAD_LOCK1_L01	Blocco per sovraccarico uscita 1
OVERLOAD_LOCK2_L02	Blocco per sovraccarico uscita 2
OVERLOAD_LOCK3_L03	Blocco per sovraccarico uscita 3
OVERLOAD_LOCK4_L04	Blocco per sovraccarico uscita 4
OVERLOAD_LOCK5_L05	Blocco per sovraccarico uscita 5
OVERLOAD_LOCK6_L06	Blocco per sovraccarico uscita 6
OVERLOAD_LOCK7_L07	Blocco per sovraccarico uscita 7
OVERLOAD_LOCK8_L08	Blocco per sovraccarico uscita 8
TMAX1	Temperatura alta sensore 1
TMIN1	Temperatura bassa sensore 1
Input1	Contatto di ingresso sensore 1
Hum1	Umidità alta sensore 1

Hum low1	Umidità bassa sensore 1
TMAX2	Temperatura alta sensore 2
TMIN2	Temperatura bassa sensore 2
Input2	Contatto di ingresso sensore 2
Hum2	Umidità alta sensore 2
Hum low2	Umidità bassa sensore 2
TMAX3	Temperatura alta sensore 3
TMIN3	Temperatura bassa sensore 3
Input3	Contatto di ingresso sensore 3
Hum3	Umidità alta sensore 3
Hum low3	Umidità bassa sensore 3
TMAX4	Temperatura alta sensore 4
TMIN4	Temperatura bassa sensore 4
Input4	Contatto di ingresso sensore 4
Hum4	Umidità alta sensore 4
Hum low4	Umidità bassa sensore 4
TMAX5	Temperatura alta sensore 5
TMIN5	Temperatura bassa sensore 5
Input5	Contatto di ingresso sensore 5
Hum5	Umidità alta sensore 5
Hum low5	Umidità bassa sensore 5
TMAX6	Temperatura alta sensore 6
TMIN6	Temperatura bassa sensore 6
Input6	Contatto di ingresso sensore 6
Hum6	Umidità alta sensore 6
Hum low6	Umidità bassa sensore 6

CONFIGURAZIONE PORTA SERIALE

RJ-12 – Porta SERIALE	
	
POSIZIONE	DESCRIZIONE
1	+5 V _{cc}
2	GND
3	Bus sensori ambientali
4	GND
5	RXD
6	TXD

NetMan 204			Modem		
RJ-12			DB-25	DB-9	DESCRIZIONE
POSIZIONE	DESCRIZIONE		POSIZIONE	POSIZIONE	
1	+5 V _{cc}	LASCIARE SCOLLEGATO			
2	GND				
3	Bus sensori ambientali				
4	GND	← COLLEGARE A →	7	5	GND
5	RXD	← COLLEGARE A →	3	2	TXD
6	TXD	← COLLEGARE A →	2	3	RXD

DATI TECNICI

CAVO DI RETE

Per collegare il dispositivo a una rete Ethernet (10Base-T) o Fast Ethernet (100Base-T), è necessario utilizzare un cavo UTP (Unshielded Twisted Pair) o STP (Shielded Twisted Pair) dotato di connettori RJ45. Il cavo deve essere conforme allo standard IEEE 802.3u 100Base-T con 2 coppie di cavi UTP di categoria 5 o superiore. La lunghezza del cavo che collega l'adattatore all'hub non deve superare 100 m e non può essere inferiore a 2,5 m.

CONNESSIONI DI RETE CON CAVO	
Segnale	Da pin n. a pin n.
TX+	1 ← → 1
TX-	2 ← → 2
RX+	3 ← → 3
RX-	6 ← → 6



I pin 1 e 2 devono essere collegati a una coppia intrecciata e i pin 3 e 6 a un'altra.

CONDIZIONI DI FUNZIONAMENTO E CONSERVAZIONE

Intervallo di temperature di funzionamento	[°C]	0 ÷ +40
Intervallo di temperature di conservazione	[°C]	-5 ÷ +50
Umidità relativa massima di funzionamento	[%]	80
Umidità relativa massima di conservazione	[%]	90

INFORMAZIONI LEGALI

Il firmware della *Netman 204* include alcuni componenti open source. Per maggiori informazioni visitare il sito del produttore.