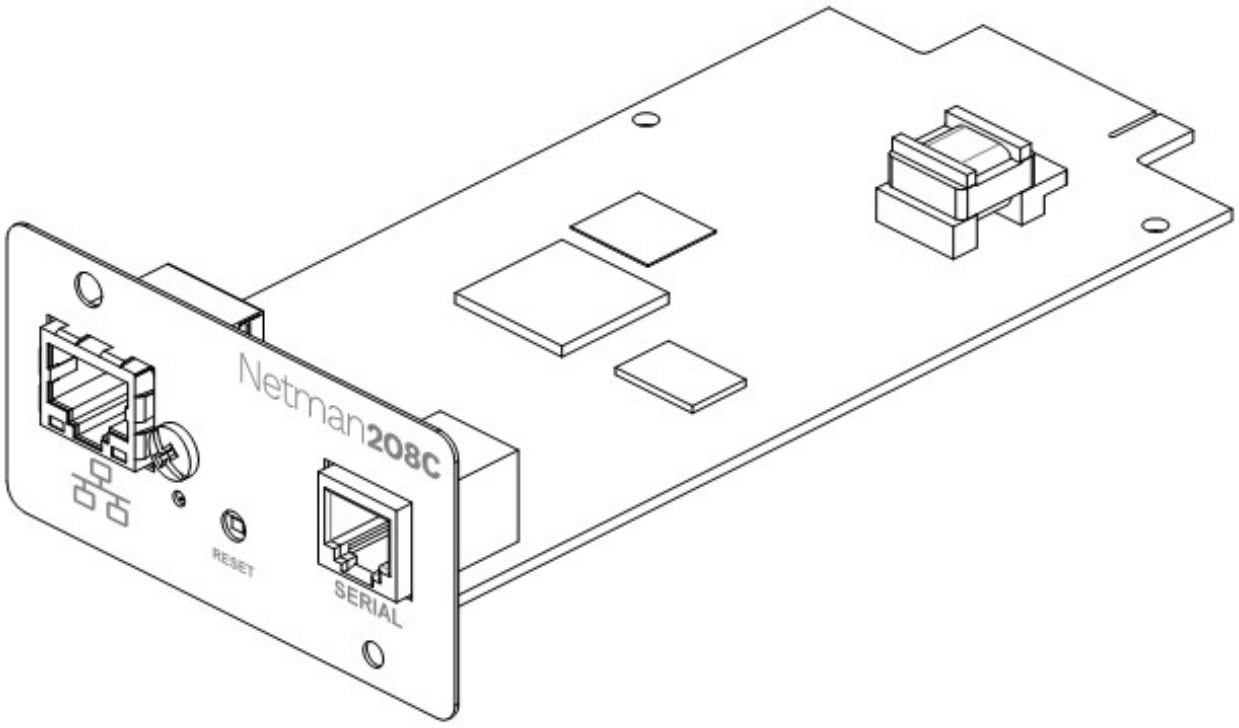
NetMan 208C



Security Guidelines

1. Introduction

This document is the Security Guidelines for NetMan 208C.

2. Defense in Depth requirements

Details of defence-in-depth REQUIREMENTS

>> **Enable internal and/or external firewall for limiting access**

- internal firewall can block and ignore unwanted incoming requests (blocking the sources)
- external firewalls can control and manage the data flow from/to the NetMan 208C in both directions (inbound/outbound)

>> **Isolate the physical access to the device**

Secure location in networking can be implemented as:

- secure locations network and other cables
- dedicated network cables only for the UPS/NetMan 208C area
- use of metal conduits for network cables protection
- isolate the NETWORK and SENSOR cables
- area with locked doors
- use a cage to protect the devices
- limited physical access to the device and the nearby
- area protecting the access to PHYSICAL CONNECTIONS and SENSORS of the NetMan 208C and cables related
- place signs for "*authorized only personnel*" or other generic warnings (not giving hints of the kind of devices installed)

Manage the accesses to authorized only personnel (maintainers):

- with physical or electronic checks
- preventing accidental or unwanted access to cables

>> Isolate the communication flow

Device isolation may be implemented as:

- secure locations for devices
- area with locked doors
- use of a physical cage for device protection
- protection the access to RESET BUTTON and SENSORS of the NetMan 208C
- placing signs for “unauthorized access” (not giving hints of the kind of devices installed)

Authorized only personnel (maintainers):

- limited physical access to the device and the nearby
- with physical or electronic checks
- preventing accidental or unwanted access to the device

>> Use strong Secure algorithm for LDAP

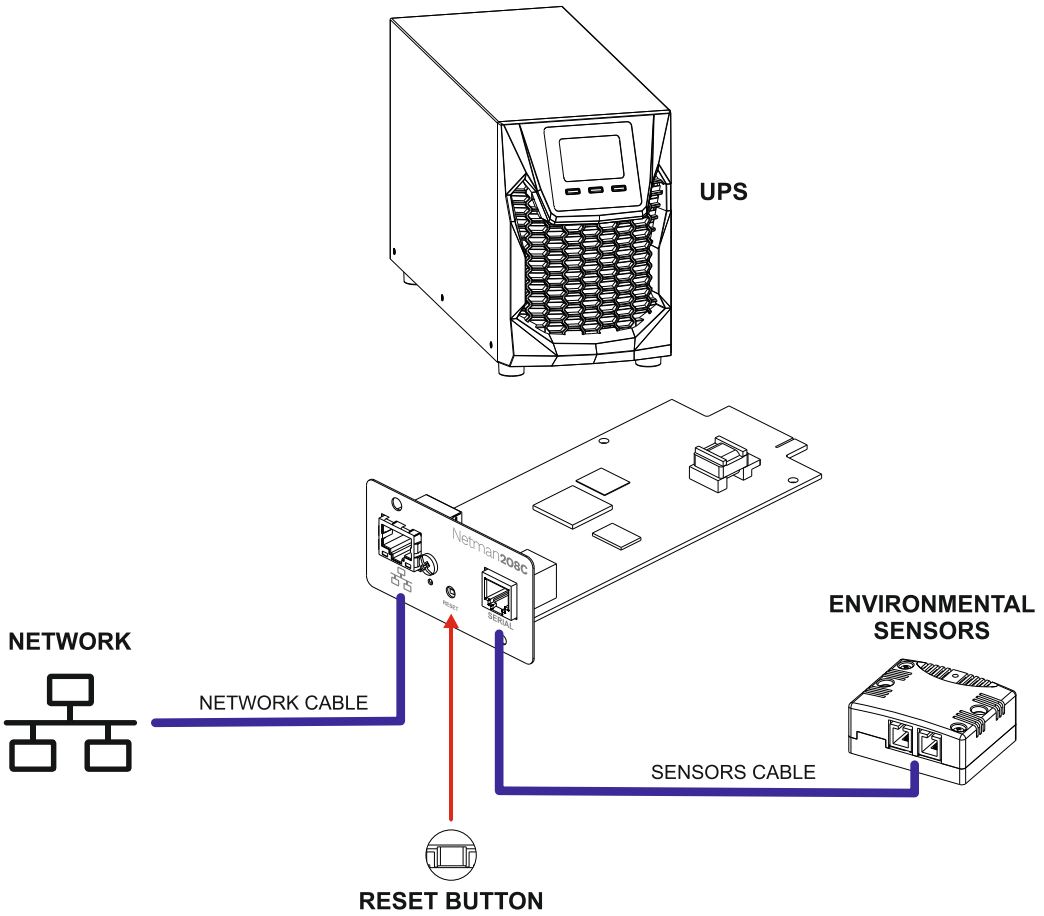
Check the usage of the local and LDAP credentials for login: prefer LDAP over local users and avoid credential account sharing.

- Keep strong password strength rules and login/lock rules.
- Maintain least-privilege rule for the functions active with "power" and "view" user profiles.

3. Security Hardening Guidelines

The protection of the NetMan 208C, can be hardened and customized for each use case and network environment following some suggestions given below, deploying a better defense-in-depth solution.
Many suggestions available here are technical, others concern the management and the physical installation of the NetMan 208C, the latter concern some suggestions specifically for the personnel and the rules for more secure management.
Beware that not all suggestions given below may fully fit your environment and installation. In case of doubts consult your technical department.

3.1. Product integration in its product security context



1. **UPS**: the physical device where the NetMan 208C is installed in the dedicated slot.
2. NetMan 208C: the physical device to secure.
3. Network: the dedicated network to which the NetMan 208C is connected.
4. Network cable: the physical cable for connecting to the network.
5. Reset button: the button to press to enter Maintenance Mode.
6. Sensor cable: the cable that connects the card to the optional Environmental Sensors.
7. Environmental sensor: the optional environmental sensors (temperature, humidity, I/O) that can be connected to the NetMan 208C.

3.2. Integration of APIs and interface protocols with user applications

Services and protocols listening on the NetMan 208C

HTTP	Internal web server
HTTPS	Internal web server
MODBUS	Modbus TCP for external communication
BACNET	Bacnet/IP for external communication
SSH	Secure shell for administration tasks
SNMP	SNMP for external communication
POWERSHIELD	Service for support of the remote software for UPS status control and shutdown actions (see the User Manual)
TUNNELING / UPSTOOLS / GPDOWNLOAD	Service for support of the download of log and configuration data (see the User Manual)

External remote protocols queried by the Services (when enabled)

JSON	Service for reporting data to external server as JSON data
SYSLOG	Service for reporting events to external SYSLOG server
LDAP	Service for authentication with external LDAP server
Nutanix / SSH	Service for shutting down external hosts via Nutanix protocol or SSH commands
VMware / Syneto	Service for shutting down external hosts via VMware API protocol

3.3. Usage and maintenance of the product's defense in depth strategy

Periodically check:

- internal and external firewall rules
- isolation and access to the dedicated network (logically and physically)
- isolation and access to the device
- HTTPS certificates validity and expirations
- user accesses and credentials of personnels

3.4. Configuration of security options and capabilities

- Generate and use a strong custom HTTPS certificate
- Password Strength and Complexity
- Login attempts
- Backup and device configuration

3.5. Usage of security-related tools delivered with the product

HTTPS / Internal HTTPS Certificate:

For fully verifying the internal certificate with the browser (*CA check*) there is the need of the CA certificate "**Netman208Secure_Https_CA.pem**" to be installed in the browser/computer as "*trusted root certificate*" for a full trust. Refer to the User Manual for the instructions.

3.6. Security maintenance activities

- periodically and regularly check for latest firmware updates: the device shall warn the user for available updates or periodically check the web site of the product.
- do not enable SSH and other protocols if not needed
- enable and secure reporting services (e.g. SYSLOG, emails)
- keep always auto-logout functionality active and checked
- periodically review the personnel authorized to access the area and the NetMan 208C
- periodically check and maintain least-privilege rule for the functions active with "power" and "view" user and profiles
- enforce periodically password change of the authorized users.
- check periodically the history of login accesses (Web->Administration->Login rules->Login History)
- check temporal validity of the certificates (Validity and Expiration) (Web->Administration->Certificates and Keys->View certificate)
- execute Diagnostics Operations available in Web->Administration->Diagnostics

3.7. Reporting of security incidents

The user can report vulnerabilities with online website:
https://www.riello-ups.it/pages/177-vulnerability-disclosure
Follow the instructions for a fully trusted report.

The web page above contains a clear indication of the email address to be contacted to report issues/incidents and a PGP key associated with this function, for the purpose of encrypting exchanged data.

3.8. Best practices for product maintenance and administration

Risk assessment / Updates / Checks
Periodically execute a Risk Assessment and verify that all the secure protections implemented are effective with the NetMan 208C and the environment related.
Check if firmware updates are available (both for SYS and APP).
Execute Diagnostics from the NetMan 208C (**Web->Administration->Diagnostics**) checking the effectiveness of the notifications and events.

Backup and device configuration
Provide a backup plan for the configuration of NetMan 208C (**Web->Administration->Backup/Restore Configuration**) and systems related to.
After the first configuration and installation in production (Web->Administration->Backup/Restore Configuration):

- execute a COMPLETE backup of the configuration
- store the backup in secure place
- allow only authorized personnel to access the backup and to restore procedure

Use HTTPS

- Prefer HTTPS with custom certificate over the default internal HTTPS certificate provided
- For fully verifying the internal certificate with the browser (*CA check*) there is the need of the CA certificate "**Netman208Secure_Https_CA.pem**" to be installed in the browser/computer as "*trusted root certificate*" for a full trust (every browser/computer may have a different procedure)

Generate and use a strong custom HTTPS certificate

- evaluate to generate your custom HTTPS certificate from your Certification Authority
- use 2048 bit or (better) 4096-bit RSA Private Key length: it has been predicted that 2048-bit key is enough strong for a few years but it is possible to choose 4096-bit in advance
- prefer **Certificate + CA** over a less secure **self-signed certificate (**may not be so easy)

Password Strength and Complexity

Password strength is set to default with the following rules:

Password length:	8-40 chars
Lowercase chars:	at least 1 char
Uppercase chars:	at least 1 char
Digit chars:	at least 1 char
Special chars:	at least 1 char

For better password strength, it is suggested to improve these basic rules by increasing the numbers of chars and extending password length (Web->Administration->Change local password->Password complexity).

Login attempts

A mechanism for login retries and user locked is enabled by default:

Login retry counter:	max 5 retries
Retry interval:	60 seconds

and can be customized (Web->Administration->Login rules->In case of login failure).
For better security:

- reduce the retry counter to 3 or less in critical environments
- increase the retry interval to 2-3 minutes or more

Login attempts save a log as history data (Web->Administration->Login rules->Login History): this log can be checked periodically reporting any event of login and user locked.
Remember to enable the Email Service: the critical login events release a notification when a user Is locked and retries to login unsuccessfully. This notification is sent to the Email recipients with the flag “Security alert” enabled (Web->Configuration->Emails->Configuration->Flag “Security alerts”). Keep always an email recipient with this flag able to receive this kind of notification. Periodically execute a test trying to login as a non-existent user and wrong password, verifying the correct send of the notification.

Network and Connectivity: IPv4, IPv6, 802.1x

Hardenings for IPv4:

- set a Static IPv4 address for each NetMan 208C
- choose a dedicated subnet in your network

Hardenings for IPv6:

- IPv6 network infrastructure is very sensible and if not well configured may expose the devices to other networks or the public internet via its IPv6 address
- Pros: IPV6 may be useful to ease the reachability of the NetMan 208C in the network with the simple hostname
- Cons: if not well configured and not well protected (e.g.: unwanted router advertisement flood attack) IPv6 can leave accessibility to the NetMan 208C from unwanted networks; please disable IPv6 on the NetMan 208C in not well configured in the network

Hardenings for 802.1x (Web->Configuration->Network):

- the NetMan 208C provides the optional configuration for IEEE 802.1x authentication in the Network for a more secure connectivity with the NetMan 208C
- due to its complexity the 802.1x is disabled by default but can be enabled anytime

- when enable please avoid less secure methods (“EAP-MD5”, “EAP-GTC”, “EAP-MSCHAPV2”, “EAP-PSK”), provided for compatibility and extreme needs
- prefer the authentication methods “EAP-TLS”, “EAP-TTLSv0/***” because their encryption algorithms
- even more prefer the secure authentication methods with the certificates (“EAP-TLS”, “EAP-TTLSv0/***”, “PEAPv0/***”)

Ping response

In some critical networks may be useful to disable the ping response with the NetMan 208C.
How to:

- add an internal firewall rule with DROP/REJECT action for PING requests (**Web->Configuration->Firewall**)

NTP Specific Vulnerability

A specific vulnerability can be identified for a possible hardening in the configuration but it must be activated by the administration user in the configuration.
This vulnerability (**CVE-2014-5209**) allows an external attacker to query the NTP of the NetMan 208C with the response of a hint of date/time set in the NetMan 208C:

```
                        :~$ sudo nmap -sU -p123                  --script ntp-info -Pn -n
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-24 10:42 CEST
Nmap scan report for                  (           )
Host is up (0.00054s latency).

PORT    STATE SERVICE
123/udp open  ntp
| ntp-info:
|_  receive time stamp: 2036-02-07T06:28:30
MAC Address: 00:02:63:        (UPS Manufacturing SRL)

Nmap done: 1 IP address (1 host up) scanned in 10.20 seconds
```

To block this kind of response a specific rule is needed in the NetMan 208C Firewall section (**Web->Configuration->Firewall**):

	Enabled	From IP address	IP address	From MAC address	MAC address	Protocol	Port	#	Action
0	☑	Specify	10.1.5.12	Any		UDP	Specify	123	ACCEPT
1	☑	Any		Any		UDP	Specify	123	DROP

This rule allows only answer to the NTP Server set (**Web->Configuration->Date/Time**, e.g.: 10.1.5.12) dropping the answer to all the others.
After the application of the rule all the other IP addresses receive no response with exception of the authorized IP set:

```
PORT    STATE         SERVICE
123/udp open|filtered ntp
MAC Address: 00:02:63:        (UPS Manufacturing SRL)

Nmap done: 1 IP address (1 host up) scanned in 20.39 seconds
```

Services – Services not used, custom ports

Any Service enabled provides a surface attack that can be compromised.

If a Service is not used, please disable it.

If it must be enabled, consider protecting the NetMan 208C by setting the internal firewall (accepting only trusted remote connections) and connecting the NetMan 208C in a secure dedicated network protected with dedicated firewall.

Another option for security hardening could be the change of the default ports to custom ports when possible.

SSH

As a surface attack, SSH is not immune to vulnerabilities (known or future).

If possible, disable the SSH Service if not strongly used. If it is used occasionally, leave it disabled when not needed.

Web Server HTTPS / HTTP

You can improve the security by requesting the technical department to provide and load a specific HTTPS certificate for the NetMan 208C under the network infrastructure or from an external certified SSL provider. The upload of custom certificates is executed via web (Web->Administration->Certificate and Keys).

For a little more improvement, a change of the port of Web Service port can be evaluated over some pros and cons ("*security through obscurity*").

For maintenance, keep checked periodically:

- the validity of the HTTPS certificates (expiration date, subject, issuer) (Web->Administration->Certificates and Keys->View certificate)
- always the correctness of the Date/Time reference and the NTP server if used (Web->Configuration->Date & Time)

SYSLOG

Customize the SYSLOG UDP port (different from the default UDP/514) (Web->Configuration->SYSLOG).

Certificates

Certificates and Keys are the roots for a secure trust infrastructure and have some features to be cared:

- temporal validity (Validity and Expiration)
- Subjects and Issuer of the Certificate
- Subjects and Issuer of the CA
- Private Key length (1024, 2048 and 4096 bit) for RSA
- the date/time correct synchronism given from NTP configuration of the NetMan 208C or the manual Date/Time settings possible with Web pages

Some suggestions for security hardening:

- avoid the use of Self-Signed certificates
- generate 2048 bit or (better) 4096-bit RSA Private Key length: it has been predicted that 2048-bit key is enough strong for a few years, but it is possible to choose 4096-bit in advance
- generate your custom certificates, strongly related to your network with Certificates and CAs even if their generation may not be so easy
- Prefer **Certificate + CA** over a less secure **self-signed certificate**

Email

The basic transport protocols are: Plain, SSL and START-TLS. Please prefer encrypted transport SSL or START-TLS when possible.

The special “Security alerts” flag events intercepts:

- a user trying to login to the NetMan 208C but failing
- a user being locked after some failed login and then retrying
- excessive number requests for the Web server signaling possible DoS attack or over usage of Web server

Consider the “Security alerts” events as highly important notification: enable the related flag for some email recipients (at least one).

Verify periodically that the email recipients receive the expected alerts (e.g.: try to login with a non-existent user until the user is locked and notifications are sent).

4. Secure Disposal Guidelines

For a correct disposal procedure of the NetMan 208C:

- go to MAINTENANCE MODE (Web->Administration->Firmware upgrade->Reboot for upload a firmware or press the physical Reset Button for 12+ seconds)
- execute “Reset to default” procedure wiping all the logs, data and configuration
- reboot to Normal mode
- extract NetMan 208C from the physical UPS and proceed to its physical disposal
- place the device in a safe location

For any trouble with the disposal procedure please get in touch with your RPS (Riello UPS) point of contact (or eventually write an email to info@riello-ups.com, with subject “Product Disposal”) and you will be contacted to discuss further options.

5. Secure Operation Guidelines

MAINTENANCE MODE / Firmware update

When:

- updating Firmware of the NetMan 208C (APP, JVM, SYS)
- accessing the UPLOAD / MAINTENANCE mode

during maintenance the NetMan 208C is not protected without all secure components:

- be sure to keep UPLOAD / MAINTENANCE mode only when needed
- as soon as possible reboot to “Normal Mode” for restoring normal secure behavior of the NetMan 208C

6. Account Management Guidelines

The NetMan 208C allows the authentication of **three local users**:

- local user “admin”: the default user, full access to all the functionalities
- local user “power”: disabled by default, can access to a limited (customizable) configuration, mainly for normal management, least functionalities allowed by default
- local user “view”: disabled by default, can access to a few configuration (customizable) parameters, mainly as viewer role or very basic actions

The first time the “admin” user logon with the default “admin” password, a password change is mandatory following the strong rules given.

After the first configuration with the local “admin” user, it is suggested to change its password and avoid to login with this local “admin” user on the NetMan 208C: use this account only for critical actions (**Web->Administration->Change local password**).

Single user authentication can be enabled with LDAP Service: any single authentication ca be checked against the membership to three profiles:

- “admin” profile: access to all the functionalities

- “power” profile: same functionalities of the local “power” user defined above
- “view” profile: same functionalities of the local “view” user defined above

LDAP configuration is available in: Web->Administration->Login access->LDAP

	full access to all the functionalities	access to a limited (customizable) configuration	access to a few configuration (customizable) parameters/actions
local user “admin”	✓		
local user “power”		✓	
local user “view”			✓
LDAP “admin” profile	✓		
LDAP “power” profile		✓	
LDAP “view” profile			✓

The daily management should be executed as LDAP user with “admin” profile” or, as better option, using a LDAP “power” or “view” profile users when possible.
As general behavior, prefer to access with lower profiles with LDAP following the least-priviledge rule: only the necessary functionalities/roles needed (**Web->Administration->Change local password**). When necessary, access with local users (“view”, “power” or “admin” in the worst case).

ERRATA MANAGEMENT

RPS (Riello UPS) strives for continuous improvement of all product documentation material: in case errors or omissions are found in this document, please report them by contacting us at the email address doc_errata@riello-ups.com. Please include as subject of your email the name of the product and the version number of the security guidelines to which the report applies.