

Release Notes for Netman 204-4GB

APP version 04.06 – OS version B24-1

(November 2024)

Brief

This update for Netman 204-4GB introduces some features from Cybersecurity policies and rules other than other fixes and improvements for the general behaviour of web interface and the system. Implementation of some new features may change deeply some previous habits and settings. The purpose of this Release Notes is to show the main changes with more impact for the users.

Update instructions

Application update only

A first level of update may be choosed for updating:

- only **the FW application 04.06**
- keepinge the current OS

This upload can be executed **via Web page**, with usual Web upload interface in the Netman 204.

By this choice:

- major functionalities **will be updated**
- some minor functionalities **will be not updated**
- OS security and CVEs **will be not updated**

For this update, some passwords and part of the configuration may be cleared and must re-written later.

Full update

A full update is strongly suggested and includes:

- **FW application 04.06**
- **OS update B24-1**

This upload can be executed **via the SD card**. In this way:

- major and minor functionalities **will be updated**
- OS security and CVEs **will be updated**

All the configuration and password will be lost.

!!! In both cases, please follow the suggestion to save the parameters of configuration before the update.

Brief list of New Features and changes

Here follows the list of the most impact changes for the user.

] Reset password from Service [

When “**admin**” tries to login with wrong password, a new RESET PASSWORD procedure is called:

The image shows two screenshots of the Netman interface. The left screenshot shows the login page with a 'LOGIN WITH' dropdown set to 'Local authentication'. The 'Username' field contains 'admin' and the 'Password' field is masked with dots. Below the login fields is a red error message box that says: '! LOGIN FAILED. CLICK [HERE](#) IF YOU FORGOT THE PASSWORD.' The right screenshot shows the 'Password Reset' page. It has an 'INSTRUCTION' section with a long, crypted 'REQUEST' code. Below this is an 'INSERT RESET CODE' section with a text area for pasting the code and a 'SUBMIT' button.

The User must copy and send (by email) the ciphered REQUEST CODE to the Service then wait for RESET CODE.

The new procedure implements a ciphered requests (more secure than before) that allows to reset the password restoring the default password (“**admin**”) for the “**admin**” user.

] HTTP / HTTPS [

When the Netman is configured with HTTPS web settings enabled, the browser searching for HTTP it will be redirected to the correct HTTPS web service and port.

e.g.:

`http://netman6306xxyy.local` → (auto-redirection) → `https://netman6306xxyy.local`

This redirection is available for both **IPv4** and **IPv6**.

] Users [

The local users are as before:

- **admin**
- **power**
- **view**

By default only “**admin**” user is active, “**power**” and “**view**” user must be activated.

The big difference is that now “**view**” user requires a password as well the other users:

Username: admin Password: admin (default)	Username: power Password: <the password set>	Username: view Password: <the password set>
--	---	--

	The previous “ View ” button (without password) has been removed indeed from the Login page.	
--	---	--

] User Roles [

User “**admin**” keeps always the full functionalities by default and is always available.

Users “**power**” and “**view**” are not available by default and must be enabled setting their password.

All the users “**admin**”, “**power**” and “**view**” needs a password.

The roles for these users now can be configured only after a “**admin**” user access and allows to select multiple specific functions for “**power**” and “**view**” users in a more flexible way. E.g.: the “**view**” user may be able to reboot the Netman with “*M-reboot*” function flagged.


Only the “**admin**” user has full power with all the functions enabled by default.

Change local password

ADMIN USER

Password

Retype Password




Admin credentials grant the right to manage Netman and also the device, including shutdown

SAVE

POWER USER

Password

Retype Password



Power credentials grant the right to manage Netman but may not full operate the device

SAVE

It is possible to revoke access to Power user just clicking the button. After this action, Power user can't login. For restoring the access a new password must be set.

Functions:

- ✓ A - General info (always active)
- ✓ B - Detail info
- ✓ C - Network status
- ✓ D - View/Download logs
- ✓ E - Service Log download
- ✓ F - Ups config
- ✓ G - Ups command config
- ✓ H - Ups command execution
- ✓ I - System/Network config
- ✓ J - Services/Functionalities config
- ✓ K - Advanced config
- ✓ M - Reboot


REVOKE ACCESS

SAVE

VIEW USER

Password

Retype Password



View credentials grant the right to only view some values of the Netman (no action is possible)

SAVE

It is possible to revoke access to View user just clicking the button. After this action, View user can't login. For restoring the access a new password must be set.

Functions:

- ✓ A - General info (always active)
- ✓ B - Detail info
- ✓ C - Network status
- ✓ D - View/Download logs
- ✓ E - Service Log download
- ✓ H - Ups command execution
- ✓ M - Reboot

REVOKE ACCESS

SAVE

] Stronger User Login check and retries [



A new mechanism for the login failed has been added: a User has limited retries before being locked and a certain customizable time to wait before any retry.

Default values for the retries are:

- max **5** retries
- **60** seconds between each retry

and can be customized.

After the max retries with login failed the user is being locked and only the admin user can unlock it from its web configuration. Remember that the the “**admin**” user will never be locked.

Login rules

IN CASE OF LOGIN FAILURE

Login retry max

5

retry

Login min interval before retry

60 seconds

When USER exceeds all the retries with wrong password, it will be locked: only the ADMINISTRATOR can unlock the user again.

SAVE

CLEAR LOGIN RULES TO DEFAULT

UNLOCK USERS

Administrator can reactivate user locked because wrong password retries.

CHECK LOCKED USERS

Locked users:	Locked at time:	
power	04/09/2024, 14:14:55	UNLOCK

] Password complexity [



New custom definition for Password Complexity for the “**admin**”, “**power**” and “**view**” users: by default the complexity is set with the following settings (but I can be customized):

Password complexity

RULES

Min password length

8

chars

Max password length

40

chars

Min Lowercase chars requested
(a,b,c,...,z)

1

chars

Min Uppercase chars requested
(A,B,C,...,Z)

1

chars

Min digit chars requested
(0-9)

1

chars

Min special chars requested
(, . _ + : @ % / -)

1

chars

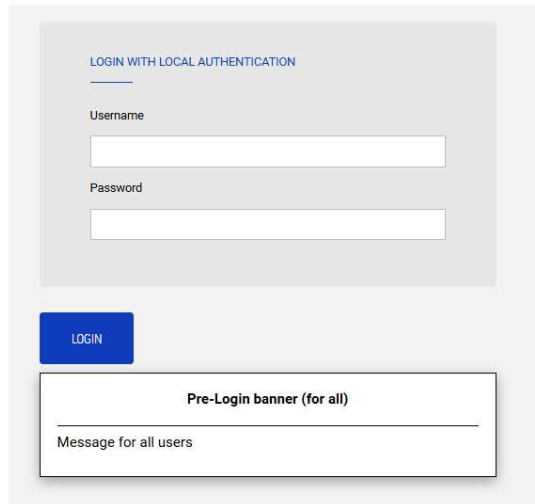
SAVE

CLEAR RULES TO DEFAULT

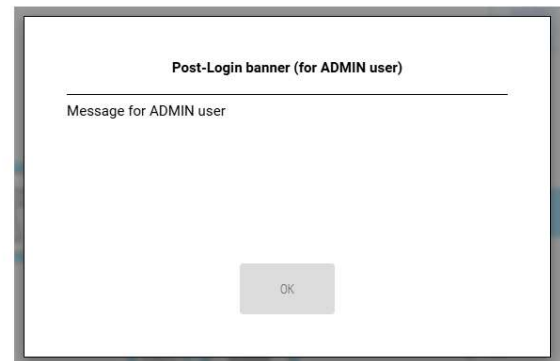
] Banner messages [

Banner messages Pre- and Post-Login are available:

- 1 Pre-login message visible for every user before login
- 3 Post-login messages each for every Admin/Power/View user, show after their login



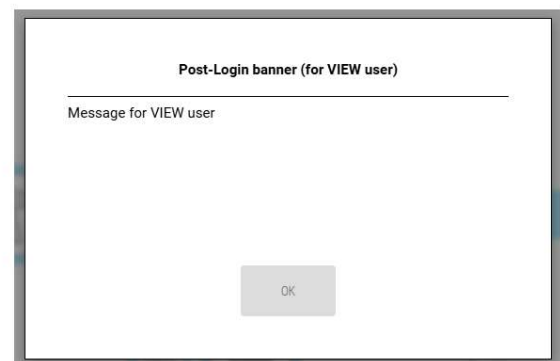
The login form is titled "LOGIN WITH LOCAL AUTHENTICATION". It contains two input fields: "Username" and "Password". Below the password field is a blue "LOGIN" button. At the bottom of the form, there is a "Pre-Login banner (for all)" box with a line for a message and the text "Message for all users".



This is a "Post-Login banner (for ADMIN user)" dialog box. It has a title bar and a line for a message, with the text "Message for ADMIN user". At the bottom right, there is an "OK" button.



This is a "Post-Login banner (for POWER user)" dialog box. It has a title bar and a line for a message, with the text "Message for POWER user". At the bottom right, there is an "OK" button.



This is a "Post-Login banner (for VIEW user)" dialog box. It has a title bar and a line for a message, with the text "Message for VIEW user". At the bottom right, there is an "OK" button.

] Expert Shell via Web [



Now the previous “SSH Expert Shell” is available in the Web section (only for “**admin**” user). It allows to manage the internal parameter from the Web, without accessing the SSH command line interface.

Expert Shell

WARNING ! SOME PARAMETERS ARE CRITICAL AND MAY MIS-CONFIGURE THE NETMAN CHANGING ITS BEHAVIOUR OR WITH RISK OF LOSING CONNECTION WITH IT.

Parameter:

Value:

↔ GET
↔ SET
✖ DELETE

This section is available only from the “**admin**” user and is used only rarely with special configurations. Please remember that managing the parameters without any reason may lead to malfunctions with the Netman.

] Network connections [



A new section in Web is now available for checking the **Internet Connectivity** and some socket **Connections Active** in the Netman understanding the services and the connections.

Internet Connectivity

Allows to check Internet Connectivity querying Gateway, DNS and network permissions.
Press the button to start the check:

CHECK INTERNET CONNECTIVITY

OK, Full connectivity (Internet) allowed and working

Active Network Connections

Allows to check current Active Connections to the Netman.
Press the button to check and show the connections:

CHECK ACTIVE NETWORK CONNECTIONS

Protocol	Local	Remote	State
TCPv4	0.0.0.0:21	0.0.0.0:*	LISTEN
TCPv4	0.0.0.0:22	0.0.0.0:*	LISTEN
TCPv4	0.0.0.0:443	0.0.0.0:*	LISTEN
TCPv4	0.0.0.0:502	0.0.0.0:*	LISTEN

*** **Internet Connectivity:** will report wrong check status if Netman 204 is not updated via SD card (it requires **OS version B24-1**).

] JSON file upload via Web [

CONFIGURATION → YOUR NETMAN → JSON

For the JSON configuration, now the “**licence file**” of the JSON service can be uploaded via web.

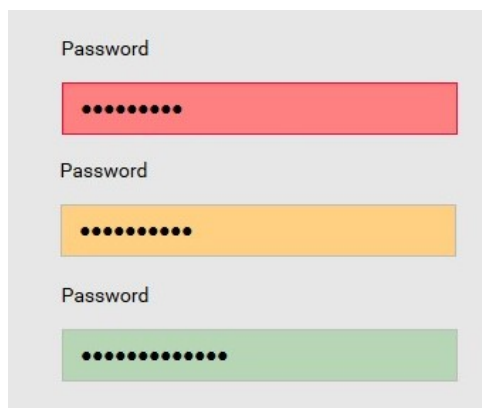


User can drop a file via web with some text data (<CONTENT_OF_LICENSE_FILE>); the content of this file will be written in the JSON field “**license**” as simple text:

```
[{
  "timestamp": 1682497583,
  "license": "<CONTENT_OF_LICENSE_FILE>",
  "io_conf": 1,
  "status": [0, 8, 0, 6, 0, 0],
  "measures": {
    "vin1": 230,
    ...
    "tsys": 23
  }
}]
```

] Password strength suggestions with colors (red, orange, green) [

Some password fields are checked against common passwords usage: **red** is very common or guessable, **green** is a good password.



] View Certificates [

It shows some data of the loaded certificates.

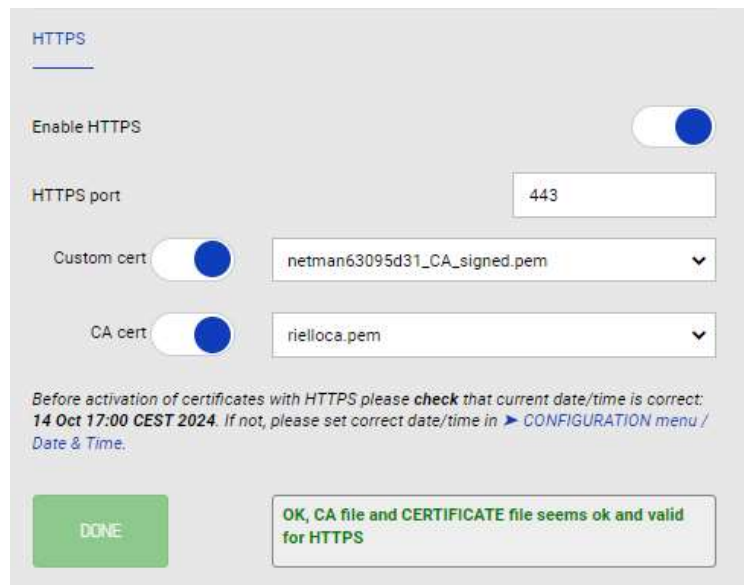
It allows to check some data and validity of each certificate loaded.



] HTTPS Certificate test [

Added a manual pre-check for HTTPS certificates before application and Save operation.

It allows to check the HTTPS configuration checking for its validity, both with single certificate and with CA. This is only an *on-the-fly* check with certificates currently selected in the lists. When certificate set is valid it can be activated with the “Save” operation at the bottom of the page as usual.



] Others minor improvements [

- Auto-logout improved (time of autologout showed)
- BACNET address range extended to 4194302
- General system and user messages improvement

] Various Security improvements [

The security of the Netman 204 has been improved with:

- HTTP/HTTPS security improvements (cookies/sessions)
- Fields in the Web pages (input check validation with only allowed chars and length validation)
- SSH Service warning if active (SSH can be used but is no more a full-safe service - *please consider to disable it if not necessary*)
- “admin” default password warning if the password is left as default (it should be changed after first login)
- Other bugs and a lot of CVEs has been fixed (both for Application and OS)