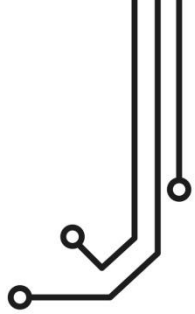
DIGITAL YACHT





IMPORTANT NOTE

Your NET Protect has a WiFi network name "**NETProtect-xxxx**" where **xxxx** is your unique 4 digit code. The default Password = "**PASS-xxxx**", where **xxxx** is the same unique four-digit code at the end of the WiFi network name.

To access the web interface, http://192.168.1.1 or http://netprotect.local

NET PROTECT
NMEA 2000 INTRUSION DETECTION SYSTEM

Installation and instruction Manual

Version 1.10

Tel: 01179 554 474
www.digitalyacht.co.uk

1. Introduction

Congratulations on the purchase of your NET Protect NMEA 2000 Intrusion Detection System. In addition to this quick start guide, we recommend watching our NET Protect video, simply scan the QR code to be taken to our YouTube video….

This product is designed for use by Technical Dealers and Installers with knowledge/experience of NMEA 2000, Digital Yacht cannot provide technical support or training on NMEA 2000 networking.

2. Before you start

To use your NET Protect you will need:

- A wireless device with web browser i.e. Smart Phone, Tablet or Laptop
- A spare "T-Piece" connection on a working/powered NMEA 2000 network.

3. Installation

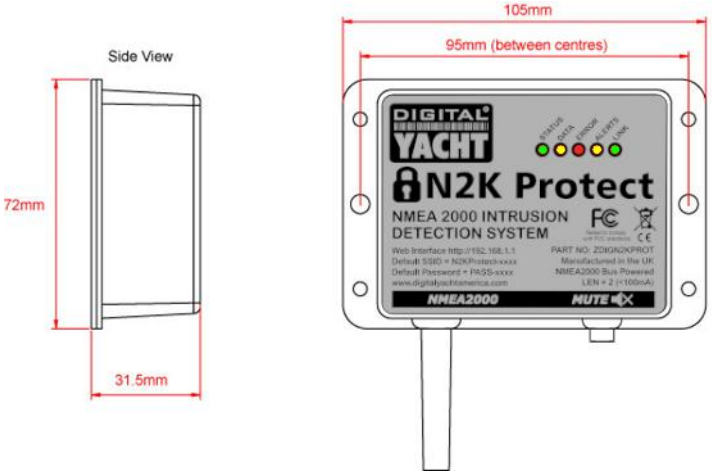
The NET Protect is IP54 rated (water resistant) and care should be taken when operating it, to ensure it is not submerged in water.

3.1 – Connecting to NMEA 2000 Network

- Connect the NET Protect cable, to a spare connector on the NMEA2000 network.
- NET Protect takes its power (LEN=2) from the NMEA2000 network so no additional connections are necessary.
- If you are connecting NET Protect to a non-standard NMEA2000 network, then a suitable adaptor cable will need to be sourced from the relevant manufacturer;
  - SeaTalkNG (Raymarine P/No A06045)
  - Simnet (Simrad P/No 24006199)

3.2 – Mounting and Location

- Install NET Protect to a flat bulkhead using suitable fixings (not supplied)
- NET Protect can be installed in any orientation.
- A location should be chosen for best WiFi performance, where its internal buzzer can be heard and where it cannot easily be tampered with.



3.3 – Powering NET Protect

- Apply power to the NMEA 2000 network, the NET Protect LEDs will illuminate in sequence, from left to right, and then they should behave, as per Table 1…

Condition	STATUS LED (Green)	DATA IN LED (Yellow)	ERROR LED (Red)	ALERTS LED (Yellow)	LINK LED (Green)
ON (Solid)	Wi-Fi STA Mode Connected		N2K Network Down	N2K Issues Alert State	Web Connection
Flashing	Wi-Fi AP-Mode Active	Data Received	N2K Issues High Risk	N2K Issues Low Risk	
OFF	Wi-Fi STA Mode Disconnected*	No Data From N2K	All OK	All OK	No Web Connection

Table 1

*** Note** – Short flash every 2 seconds indicates NET Protect cannot connect in STA Mode, check wireless network is visible and password is correct.

3.4 – Setting up the Wireless Network

- By default, NET Protect' creates a wireless network (Access Point), with Name (SSID) = "**NETProtect-xxxx**" and Password = "**PASS-xxxx**", where xxxx is a four digit code, unique to your device.
- To connect to NET Protect you need to scan for wireless networks, find it, select it and then enter the default password when prompted.
- As soon as a wireless connection is established, the Status LED will stop flashing and stay permanently ON, whilst a wireless device is connected.
- NET Protect is not a router/gateway, so when connected to it, you will not have an internet connection. Some operating system; Windows, iOS, Android, etc. may display "No Internet", which is normal and not a cause for concern.

3.5 – Accessing the Web Interface

- The NET Protect has a built-in web interface, consisting of a series of pages that provide key information on the status of the NMEA 2000 network.
- A wireless device, connected to NET Protect, can access its web interface in a browser at http://192.168.1.1 or http://netprotect.local which should bring up the NET Protect home page as shown in Figure 1.

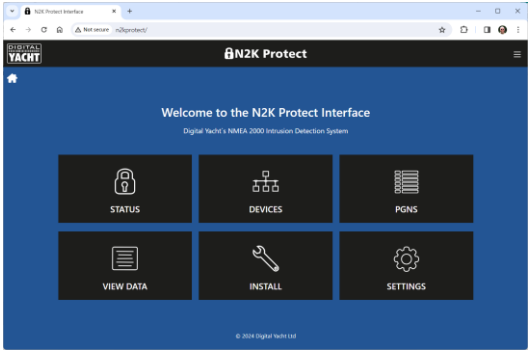


Figure 1

3.6 – Status “Dashboard” Page

- To display the current status of your NMEA 2000 network, click on the STATUS button on the home page and you will see a page similar to Fig 2.

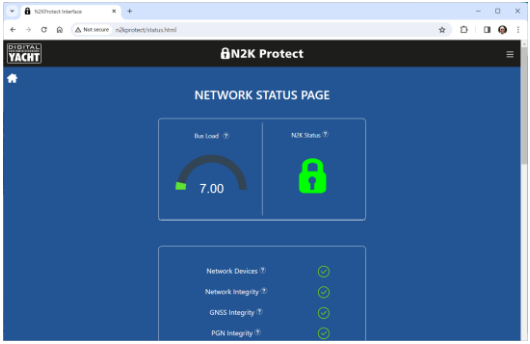


Figure 2

- On this page will are a series of key indicators that provide a good indication of how well your NMEA 2000 network is performing. If the real time tests are running and no threats are detected, then a green pulsing Padlock icon will be displayed. If there is a static Yellow (low risk issues detected) or a solid Red (high risk issues detected) Padlock icon shown then your NMEA 2000 network needs some immediate attention.
- Other indicators include (see Fig 3);
    1. Bus Load % - indicates how much data is on the network
    2. Real Time Test Status – series of Ticks and Crosses
    3. Number of Devices on Network
    4. Bus Errors – excessive errors reduce performance
    5. Global ISO Request Count – use of this PGN is discouraged
    6. RCA Group Function Count – used to control other devices
    7. Proprietary PGN Count – should be < 3% of network traffic
- At the bottom of the Status page is a logging window where any test failures or security alerts are displayed. The Log can be Cleared or Saved (Downloaded) by clicking the two buttons below the window.

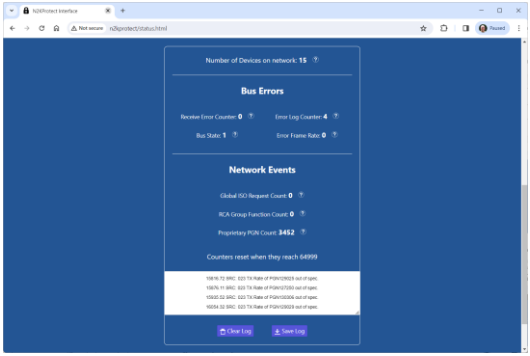


Figure 3

3.7 – Devices Page

- To display a list of all devices on the network, click on the **Devices** icon/button and you should see a page, similar to Figure 4.
- To access additional Product and/or Configuration information about a specific device, click the "Eye" icon at the end of its row.
- The green heart icon indicates that a device is active (transmitting PGNs) on the network – click the green heart icon to display the PGNs it is transmitting.

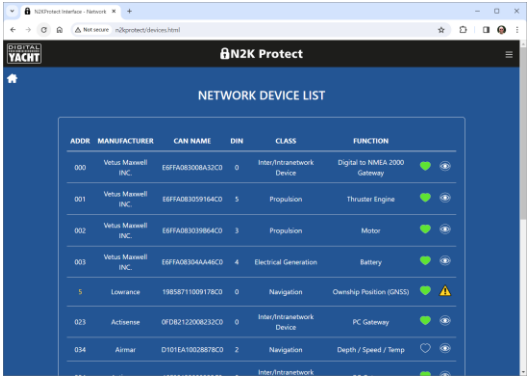


Figure 4

3.8 – PGNS Page

- To display all the PGNs being received, click on the **PGNS** icon/button and the table in Figure 5 will be displayed.
- To view specific PGN data, click on the "Info" icon on that PGN's row.

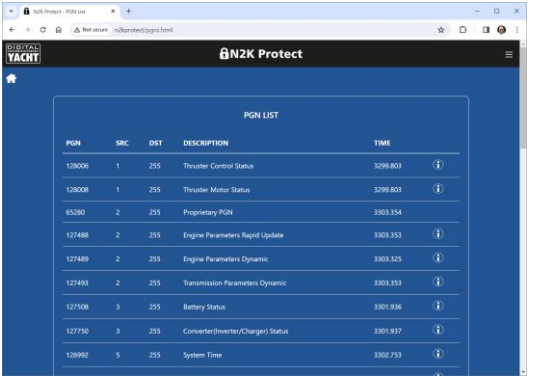


Figure 5

3.9 – View Data Page

- To display and log the raw NMEA 2000 data being received, click on the **View Data** icon/button and the page in Figure 6 will be displayed.

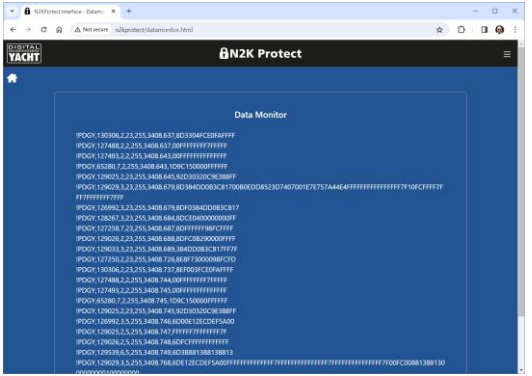


Figure 6

3.10– Install Page

- NET Protect provides a series of tests and tools for the marine electronics installer. To access them, click on the Install button of the home page and a similar screen to Figure 7 will be displayed.



Figure 7

- One of the prime functions of the NET Protect is to allow an Installer to test and validate the NMEA 2000 Network as part of their installation and commissioning process.
- The **Device Certification Tests** identify the devices on the network that are in the NMEA 2000 Certified Products database – maintained by the NMEA organization.
- The **Network Topography Tests** identify duplicate devices that have not had their Device Instance correctly set, devices that are sending out duplicate PGNs and data sources whose priority is wrong.
- The **Device Configuration Tools** allow the Installer to set the two text fields in a device's Configuration Info PGN, change a device's Device Instance or command a device to have a particular CAN address.
- The **Miscellaneous Tests** identify devices that are outputting important navigational PGNs with "no data" in key fields, extract the Firmware Versions of all devices on the network and add up the total LEN values of the physical devices on the network.
- The final tool at the bottom of the Install page, **CANShot™** is a key function of NET Protect and is covered in detail in section 3.10.

3.11– Creating the CANShot™ and securing NET Protect

- NET Protect is designed to monitor and protect the NMEA 2000 network 24/7, by constantly checking that the devices and data on the network are the same as when the network was installed and commissioned.
- After the Installer has finished commissioning the NMEA 2000 network and whilst all of the network devices are turned on and working normally, the Network Snapshot tool should be run.
- CANShot™ scans every device on the network, creating a network index file which can be downloaded for the Installer's records and also stored in NET Protect. This snapshot is then used in the Realtime tests to constantly check for "unknown" new devices or unusual, potentially malicious behaviour.
- When you start the **CANShot™** you are asked if you wish to "lock down" NET Protect by creating a "Super User" password (see Figure 8). This ensures that only someone with the Super User password can make changes to the NMEA 2000 network.
- It is only possible to take future, new **CANShots™** by first entering the Super User password, so it is very important that this password not lost or forgotten. If this happens contact support@digitalyacht.co.uk

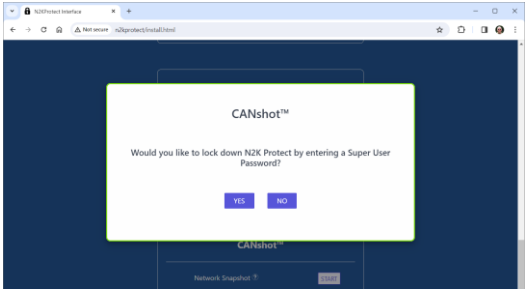


Figure 8

- If you click NO, then the **CANShot™** will be taken as normal, but anyone can take a subsequent **CANShot™** without entering a password. This is fine when familiarising yourself with the process but we strongly recommended securing NET Protect with a Super User password once the testing and commissioning of the network has been completed.
- The time that it takes for a **CANShot™** to be taken, depends upon the size of the network. A status bar is displayed showing the progress.

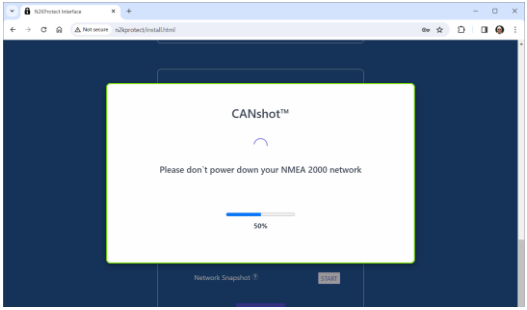


Figure 9

- Once completed, a "success" pop-up will be displayed and the **CANShot™** will be stored in the NET Protect's secure memory. The Installer can download a copy of the **CANShot™** by clicking the "Save CSV File" button.
- NET Protect will now start monitoring and protecting the NMEA 2000 network.

4. Settings

By default, NET Protect creates a wireless network (Access Point), with Name (SSID) = "**NETProtect-xxxx**" and Password = "**PASS-xxxx**", where **xxxx** is a four digit code, unique to your device – see example in Figure 10.

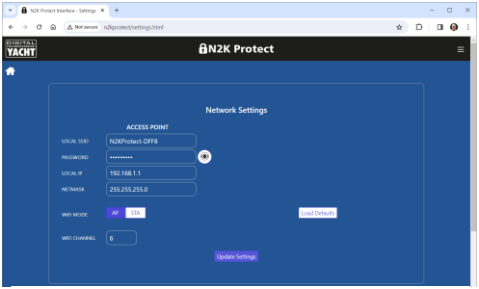


Figure 10

As NET Protect is a security device, we strongly recommend that you change the default wireless Password and/or the SSID (network name). Even though these are unique to you, anyone can read the online copy of this manual and work out what your password is once then can scan and see your wireless network.

It is much more secure to make NET Protect join the vessel's main wireless network, particularly if it is protected with the latest WPA3 encryption. To do this, from the Home page, click on the **Settings** icon/button and in the Network Settings section at the top of the page change WiFi Mode to **STA**, see Figure 11.

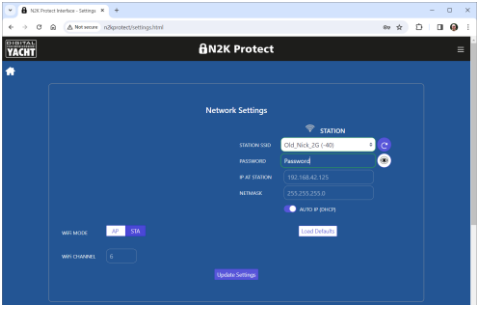


Figure 11

Click the **Scan** button to scan for available wireless networks, select the network you want to join from the drop-down list, enter the wireless password and click the **Update Settings** button.

NET Protect will now display a window saying that the Wi-Fi settings have been changed and the unit will now reboot. On rebooting it will try to join the selected wireless network and if successful the Status LED will stop flashing a few seconds after booting up and stay permanently ON.

If the Status LED is OFF with a short flash every two seconds, then NET Protect has failed to connect to the selected network. Wait 30-45secs for NET Protect to revert to AP mode or press and hold the reset button for >10secs for a factory reset.

Also, on the Settings page is the Gateway firmware version – see Figure 12. Updates to the firmware can be done via the web interface. It is expected that there will be numerous and frequent updates for NET Protect. Please regularly monitor the dedicated https://n2kprotect.com website that we have setup for NET Protect.

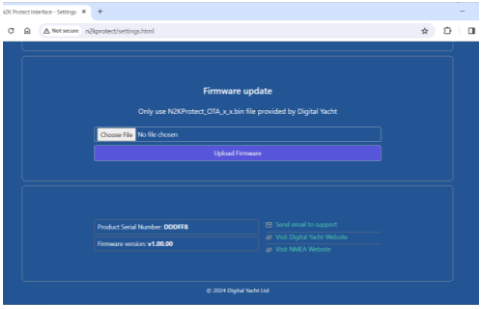


Figure 12

This Quick Start Manual just covers the very basic operation of NET Protect and a more detailed description is given in the training video at…

5. Garmin OneHelm Addendum

At the end of 2025, NET Protect was approved by Garmin as being OneHelm compatible. Unlike most OneHelm devices, NET Protect connects to the Garmin MFD via WiFi, rather than a wired Ethernet connection.

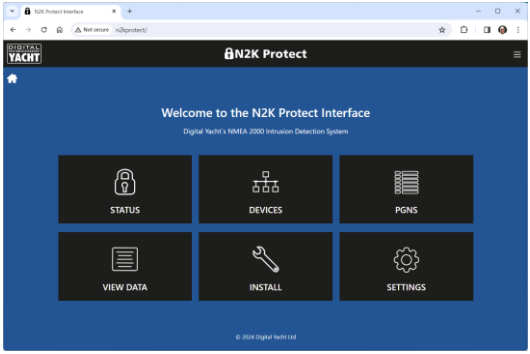
If you wish to connect your NET Protect to a Garmin MFD that supports OneHelm, please ensure you have the latest NET Protect firmware and then follow the instructions below…

5.1 Wi-Fi Connection

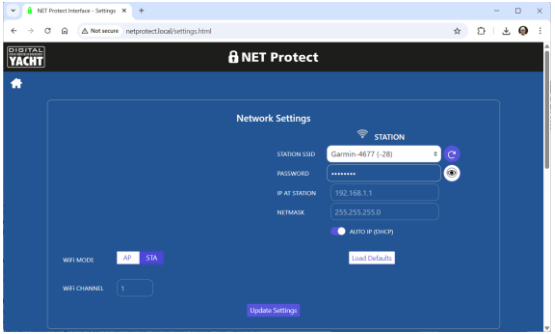
By default, Garmin do not enable the wireless interface in their units. If you cannot see a Garmin wireless network when you scan for networks, go to the MFD's ***SETTINGS>COMMUNICATIONS>Wi-Fi NETWORK*** menu and enable the wireless network. You will be prompted to accept or change the default SSID and then to enter a wireless password.

Once this is setup and saved, you should be able to see the Garmin Wi-Fi network when you scan for networks.

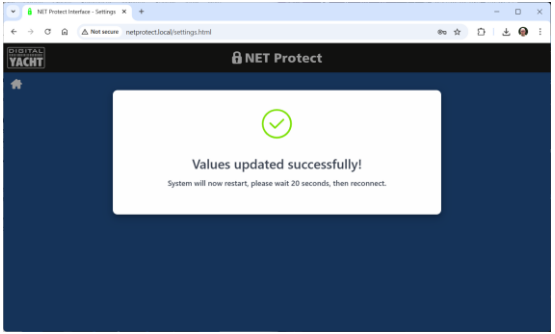
Wirelessly connect your mobile device to NET Protect's wireless network and using the device's web browser, bring up the NET Protect web interface.



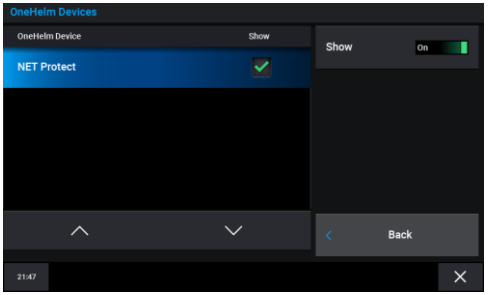
Go to the SETTINGS page, select STATION mode (STA), choose the Garmin wireless network from the drop down list, type in the wireless password and then click the "UPDATE SETTINGS" button ….



NET Protect should now display the following page and reboot. When it restarts, it will no longer create its own wireless network, but join the Garmin network. If it is successful, the STATUS LED will be permanently ON. If it is still flashing, then factory reset the NET Protect and repeat the process again, paying particular attention to enter the wireless password correctly.



The Garmin MFD should auto-discover the NET Protect and list it in the OneHelm Devices, ***SETTINGS>COMMUNICATIONS>ONEHELM DEVICES*** page…



Also you will see the NET Protect icon in the HOME>VESSEL page …



Click on this icon to access and operate the NET Protect web interface…

