SPACE 42

COMMANDER NEO

User & Installation Manual

Document number: 98-188249-B

Release date: November 27, 2025

Disclaimer

Thrane & Thrane A/S disclaims any responsibility or liability for loss or damage in connection with the use of this product and the accompanying documentation. The information in this manual is provided “as is” for information purposes only, is subject to change without notice and may contain errors or inaccuracies. Manuals issued by Thrane & Thrane A/S are periodically revised and updated. Anyone relying on information in this manual should acquire the most current version e.g. from the partner portal at https://partnerportal.cobhamsatcom.com/eshop/downloads, or from the distributor. Thrane & Thrane A/S is not responsible for the content or accuracy of any translations or reproductions, in whole or in part, of this manual from any other source. In the event of any discrepancies, the English version shall be the governing text.

Thrane & Thrane A/S is trading as Cobham Satcom.

Copyright

Manufacturer address

Thrane & Thrane A/S, Lundtoftevej 160, DK-2800, Kgs. Lyngby, Denmark

Trademark acknowledgments

- **SPACE42** is a trademark of BAYANAT INVESTMENTS LTD.
- **Thuraya** is a registered trademark of Thuraya Satellite Telecommunications Company.
- Other product and company names mentioned in this manual may be trademarks or trade names of their respective owners.

Safety summary

The following general safety precautions must be observed during all phases of operation, service and repair of this equipment. Failure to comply with these precautions or with specific warnings elsewhere in this manual violates safety standards of design, manufacture and intended use of the equipment. Thrane & Thrane A/S assumes no liability for the customer's failure to comply with these requirements.

Intended use
The Commander NEO terminal is intended for land vehicular use.

Before installing this product, please contact the vehicle manufacturer to confirm details about the mounting, cabling and placement.

Observe marked areas
Under extreme heat conditions do not touch areas of the terminal that are marked with this symbol, as it may result in injury.

Microwave radiation hazards
During transmission the antenna in this system radiates microwave power. This radiation may be hazardous to humans close to the terminal. When the system is powered, make sure that nobody gets closer than the recommended minimum safety distance.

The minimum safety distance is 1 m to the side and above the terminal when the Commander NEO is powered. The safety distance does not apply directly below the terminal, as the radiation forms a hemisphere above the terminal.

La distance de sécurité minimale est de 1 m des parois ainsi que du haut de l'antenne lorsque le Commander NEO est allumé. La distance de sécurité minimale ne s'applique pas au-dessous de l'antenne car la radiation ne forme une sphère qu'au-dessus de l'antenne.

Install and use the terminal with care

WARNING! Failure to install and/or secure the Commander NEO properly on the vehicle in accordance with the instructions provided may result in detachment, and/or cause damage or injury. Thrane & Thrane A/S disclaims all responsibility and liability arising from improper installation.

WARNING! Only skilled persons may install the Commander NEO.

Service
User access to the interior of the system units is prohibited. Only an authorized technician may perform service - failure to comply with this rule will void the warranty.

Power supply
The voltage range is 12 - 24 VDC (MIL-STD 1275 28 Vnom), max. range 10.8 to 33.6 VDC.

Do not operate in an explosive atmosphere
Do not operate the equipment in the presence of flammable gases or fumes. Operation of any electrical equipment in such an environment constitutes a definite safety hazard.

Keep away from live circuits

WARNING! Do not install the Commander NEO or exchange cables with the engine running in the vehicle.

Operating personnel must not remove equipment covers. Do not replace components with the power cable connected. Under certain conditions, dangerous voltages may exist even with the power cable removed. To avoid injuries, always disconnect power and discharge circuits before you touch them.

Magnetic Mount Solution

WARNING! Do not place your fingers underneath the terminal when placing the terminal on the vehicle! The magnetic force is very powerful and your fingers may be hurt if they are caught between the terminal and the mounting surface.

Important

In order to provide sufficient airflow below the terminal in very high temperatures, there must be **30 mm** between the terminal and the mounting surface. The Magnetic Mount Solution only provides **10 mm** space between terminal and mounting surface, and thus **may not provide sufficient airflow to keep the terminal operational in high temperatures**.

Under normal driving circumstances the magnetic force of the Magnetic Mount Solution for the terminal should be sufficient to hold the terminal. However, the magnets may not be able to hold the terminal in place, if:

- the vehicle is involved in an accident or similar extreme conditions,
- the magnets are not mounted properly,
- the roof is not level or made of a material that will not stick properly to the magnets,
- the speed of the vehicle is too high.

We recommend mounting the terminal directly on the roof instead of using the Magnetic Mount Solution. Make sure that all mounting bolts and nuts are secured properly, and that the material of the mounting surface is strong enough to hold the terminal during the intended use.

Failure to comply with the rules above will void the warranty!

About this manual

Intended readers

This manual is a user manual for the Commander NEO. The manual is intended for anyone who is using or intends to use the Commander NEO. No specific skills are required to operate the Commander NEO. However, it is important that you observe all safety requirements listed in the **Safety summary** in the beginning of this manual, and operate the Commander NEO according to the guidelines in this manual.

Manual overview

This manual has the following chapters and appendices:

- *Introduction to Commander NEO*
- *To install the system*
- *To get started*
- *To use the Commander NEO*
- *Configuration*
- *Maintenance and troubleshooting*
- *Specifications*
- *Command reference*
- *List of default settings*
- *Conformity*

Related documents

The below list shows the documents related to this manual and to the Commander NEO system.

Title and description	Document number
Commander NEO Installation guide	98-188250
REST API documentation for Commander NEO	98-182365
Mobile Gateway M NEO Installation guide	98-188254
Mobile Gateway M NEO Installation & user manual	98-188253
Space42 IP Handset User manual	98-188255
Connection box for NEO and EXPLORER Terminals, Installation guide	98-186961

Typography

In this manual, typography is used as indicated below:

Bold is used for the following purposes:

- To emphasize words.
  Example: “Do **not** touch the terminal during transmission”.
- To indicate what the user should select in the user interface.
  Example: “Select **Terminal settings**”.

Italic is used to emphasize the paragraph title in cross-references.
Example: “For further information, see *Connecting Cables* on page...”.

COURIER is used for the following purposes:

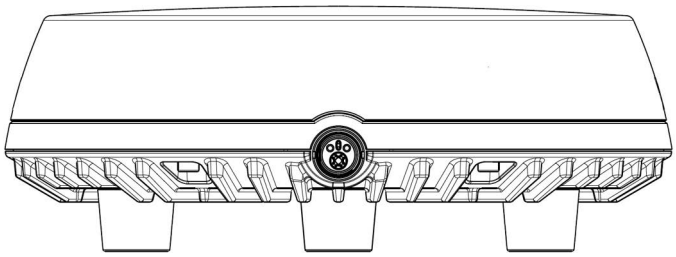
- To indicate text appearing in the display.
  Example: “the Main screen shows `READY`”.
- To indicate low level commands such as AT commands.
  Example: “In your terminal program, type **ATD**”.

Table of contents

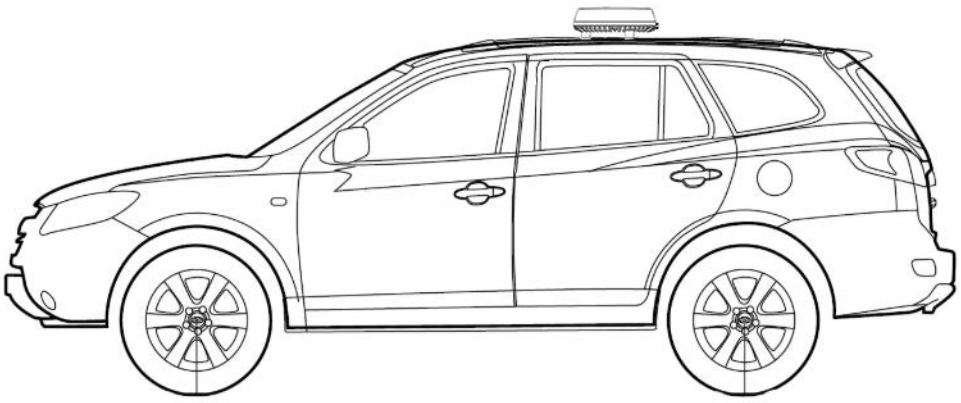
Introduction to Commander NEO

1.1 General description

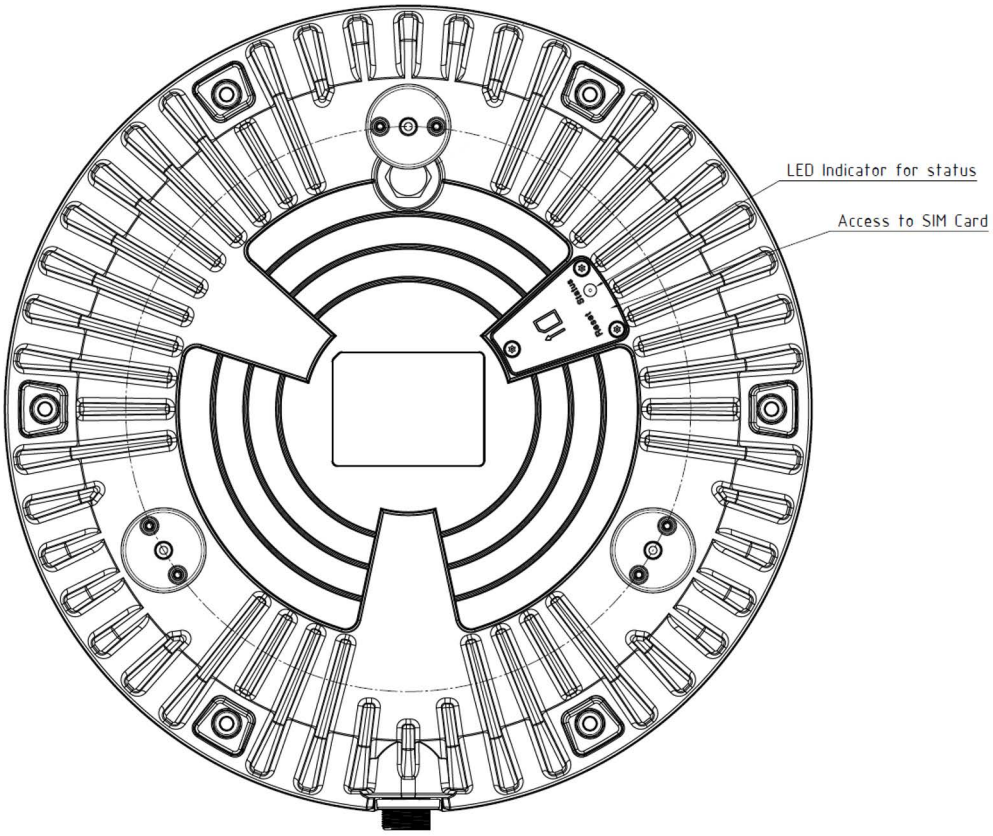
Commander NEO is a small and compact land-vehicular terminal that provides simultaneous high-speed data and voice communication via satellite through the Thuraya satellite network. You can access the terminal through an Ethernet connection or through a WLAN (Wi-Fi) connection.



All parts are contained in a standalone unit that is roof-mounted on a vehicle. A single cable connects both power and data (LAN/Ethernet) to the Commander NEO from other equipment inside the vehicle.



In the bottom of the Commander NEO there is a SIM compartment containing the SIM, the Reset button and the Status LED.



1.2 Applications

Examples of applications for Commander NEO:

- E-mail.
- Phone services.
- File transfers.
- VPN (Virtual Private Network) access to corporate servers.
- PTT (Push To Talk), when used with Mobile Gateway M NEO.
- Network browsing.

1.3 Standard features

Commander NEO offers the following features:

- Compact standalone satellite terminal.
- Silent operation and high reliability (No moving parts).
- Single cable solution.
- Powered by vehicle battery, or optionally Power over Ethernet.
- Remote on/off option.
- Satellite voice support using VoIP/SIP handset via LAN or WLAN.[1]
- Over the Air software update (via the RTM/Restful API's).[1]
- Full duplex, single or multi-user, standard data up to 1 Mbps[2].
- Support for streaming data (symmetric or asymmetric) at 16, 32, 64, 128, 256, 384, 512, 768, and 1024 kbps[2].
- LAN port for IP connectivity and optional PoE power supply.
- WLAN interface.
- Support for Mobile Gateway M NEO[3].
- Remote management[1]
- IP68 protection (with the recommended connector housing and SIM cover properly closed).
- Built-in web interface for managing data sessions and configuring the terminal, using a computer, tablet or smartphone.
- Built-in SIP server managing voice communication.[1]
- Multilingual user interface (Arabic, Chinese, English, French, Japanese, Portuguese, Russian and Spanish).
- REST API for managing the terminal, getting status and configuring the terminal.

---

1. Only when connected to T4-NGS network.
2. For T2/T3 network, the max. Standard data speed is 444 kbps and max. Streaming rate is 384 kbps.
3. The Mobile Gateway M NEO is an IP-based communications device that supports integration of satellite/LTE/3G/LAN backhaul and Land Mobile Radio.

1.4 Available parts

1.4.1 System part numbers

Item	Part number
Commander NEO vehicular satellite terminal	408033A-42000

1.4.2 Options

The following options and accessories are available for the Commander NEO:

Item	Part number
Connection box	403706B-050
Hybrid DC/Ethernet connection cable (6m open ended)	408030A-931
Hybrid DC/Ethernet connection cable (25m open ended)	408030A-935
PoE connection cable (Cat6A), 6m open ended	408030A-941
PoE connection cable (Cat6A), 25m open ended	408030A-945
PoE connection cable (Cat6A), 50m open ended	408030A-948
Magnetic mounts (3 pcs. Set)[1]	403723B-009

1. Note that the magnetic mounts **do not provide 30 mm distance** between the terminal bottom and the mounting surface! This means there may not be sufficient airflow to keep the terminal operational in case of very high ambient temperatures. To maintain the distance below the terminal, mount the included standoffs as described in the installation guide for the Magnetic Mount.

To install the system

This chapter describes how to install the Commander NEO on a vehicle and connect cables. It has the following sections:

- *To unpack*
- *To insert the SIM card*
- *To place the terminal*
- *To install the terminal*
- *To connect cables*

2.1 To unpack

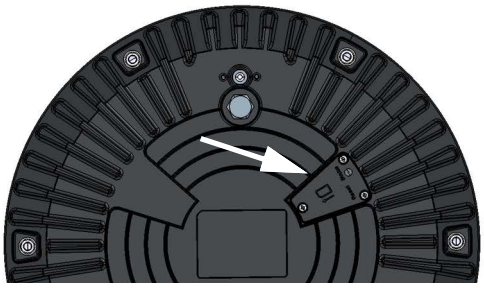
Unpack your Commander NEO and check that the following items are present:

- Commander NEO Terminal with plastic spacers mounted
- Hybrid DC/Ethernet connection cable (6m open ended)
- Torx bit for the screws for the cover of the SIM compartment
- Commander NEO Installation guide
- Production certificate

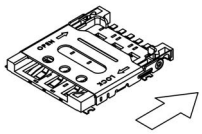
Inspect all units and parts for possible transport damage.

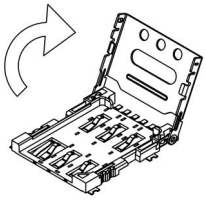
2.2 To insert the SIM card

The SIM card is placed in the SIM compartment in the bottom of the terminal.

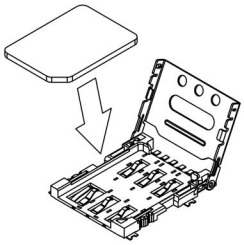


1. Use the included Torx bit to unscrew the 3 screws for the SIM compartment and remove the cover. Keep screws and cover for later.
2. Locate the SIM holder in the middle of the compartment.
3. Slide the metal lid to “Open” to relase it.
4. Lift the metal lid and insert the SIM card as shown.

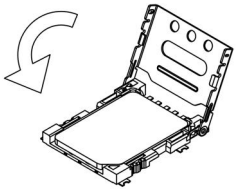




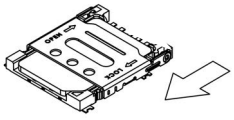
Open



Place SIM card, chip side facing down.



Close



Slide to “Lock”

5. Remount the cover for the SIM compartment and use the included Torx bit to fasten the 3 screws.

2.3 To place the terminal

2.3.1 Placement

For best performance, mount the terminal in the center of the vehicle roof and with free line of sight in all directions (no blocking objects).

2.3.2 Orientation

For best performance, mount the terminal reasonably leveled (not tilted) on a flat surface.

2.3.3 Obstructions

Obstructions can cause signal degradation. We recommend to avoid any blocking objects on the vehicle roof that may obstruct the satellite signal from/to the Commander NEO.

2.3.4 Radiation hazard

The Commander NEO antenna radiates microwave power when it is active. Make sure the terminal is placed where humans will normally not come closer than the minimum safety distance from the terminal while it is active. Refer to the *Safety summary* in the beginning of this manual. Note that the safety distance applies to a hemisphere above the terminal. The terminal does not radiate power directly below the terminal.

2.3.5 Interference

Do not place the terminal close to interfering signal sources or receivers. We recommend that other antennas, such as LTE or VHF antennas, are located as far as possible from the terminal. If other equipment is installed near the Commander NEO we recommend that you test the total system by operating all equipment simultaneously and verifying that there is no interference.

2.4 To install the terminal

CAUTION! Before installing this terminal, please contact the vehicle manufacturer to confirm details about the mounting, cabling and placement.

WARNING! It is the responsibility of the customer to ensure a safe installation! See guidelines in the *Safety summary* on page ii.

2.4.1 Important mounting notes

Line of sight

Place the terminal with free line of sight in all directions to ensure proper reception of the satellite signal. Do not place the terminal close to large objects that may block the signal.

Condensation and ventilation

In some cases there will be condensation inside the Commander NEO. A ventilation hole with a Goretex membrane in the bottom of the terminal is designed to lead any humidity away from the terminal.

Make sure the ventilation hole is not blocked.

Important Make sure there is always a distance of minimum 10 mm between **any part** of the terminal bottom and the mounting surface. **In very high temperatures, 30 mm space is required** to provide sufficient ariflow to keep the terminal operational. If you are not using the included plastic spacers nor the magnets, use spacers at each bolt.

See *To mount the terminal fixed on the vehicle roof (recommended)* on page 2-5.

2.4.2 To mount the Commander NEO

Important Before you install the Commander NEO, **make a note of the serial number** found on the label on the bottom of the terminal. The serial number must initially be used for two things:

- **Password** for accessing the **administrator** part of the web interface. See *To access and navigate the web interface* on page 5-2.
- **WLAN encryption key**. See *WLAN interface setup* on page 5-14.

The terminal can now be installed on the roof of the vehicle. You may choose between these methods:

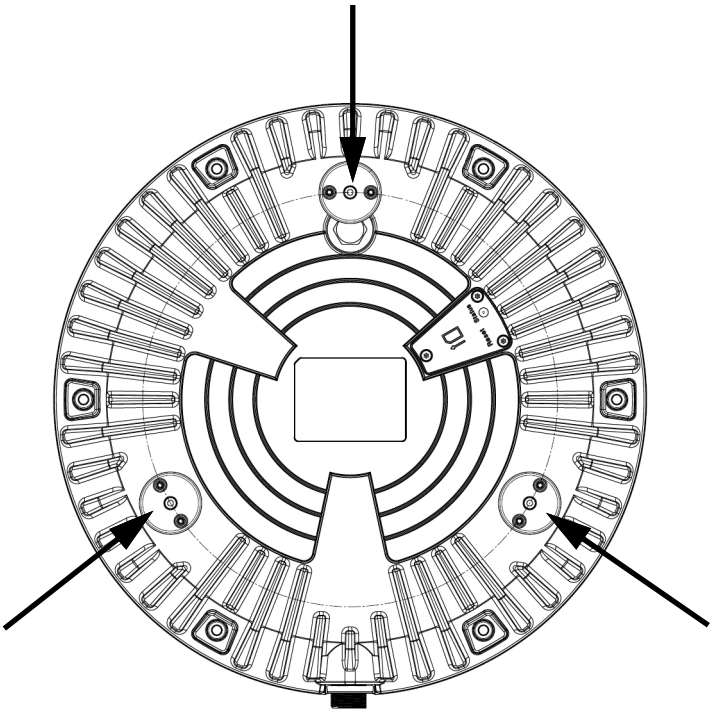
- *To mount the terminal fixed on the vehicle roof (recommended)*
- *Magnetic Mount Solution (optional)*. Attach the terminal using magnets underneath the terminal.

2.4.3 To mount the terminal fixed on the vehicle roof (recommended)

The terminal may be fixed on the roof of your vehicle using three M6 bolts and mounting spacers (already mounted). This solution requires that you drill three holes in the roof of the vehicle.

To mount the terminal,:

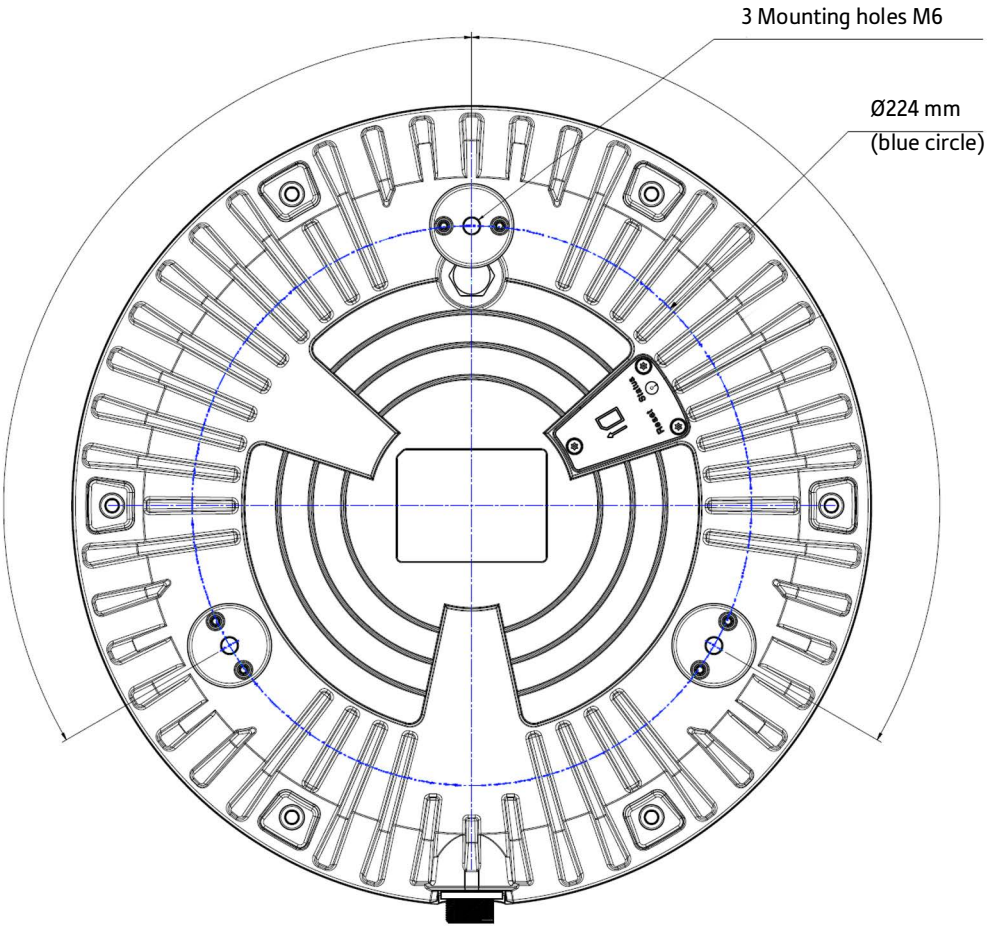
1. Use the already mounted plastic spacers or use similar mounting plates of 30 mm height. See the drawing below.



Important Do not mount the terminal without the spacers! If you mount the Commander NEO directly on a roof without the spacers, this will have a significant negative impact on antenna performance.

Also, free airflow under the terminal is necessary for the ventilation hole in the bottom of the terminal and to prevent over-heating.

2. Based on the dimensions of the mounting plates, calculate and mark up the position of the holes to be drilled in the roof of the vehicle. The drawing below shows the Drill Circle Diameter for the bushings in the terminal. The bushings are 120° apart.



3. Drill the 3 holes in the roof according to the previous step.
4. Mount the terminal with the spacers/mounting plates using 3 M6 bolts and washers. If the mounting plates are less than 30 mm thick, use spacers to obtain a distance of 30 mm between the roof and the terminal bottom. This is to ensure that the ventilation hole in the bottom of the terminal is not blocked, and to ensure free airflow under the terminal to prevent over-heating.

Important The bolts must **never** penetrate more than max. 10 mm into the bushings in the terminal! Make sure the bolts are not too long.

5. Connect the cable from the terminal to power and LAN equipment (if used).
Refer to *To connect cables* on page 2-8.

2.4.4 Magnetic Mount Solution (optional)

Overview

We recommend mounting the terminal with bolts through the roof instead of using magnets. However, a Magnetic Mount Solution for use in temporary installations is available from your supplier.

The Magnetic Mount Solution consists of 3 individual high intensity magnets with rubber coating. You can place the Commander NEO directly on the roof of the vehicle using these magnets.

Important In order to provide sufficient airflow below the terminal in very high temperatures, there must be **30 mm** between the terminal and the mounting surface. The Magnetic Mount Solution only provides **10 mm** space between terminal and mounting surface, and thus **may not provide sufficient airflow to keep the terminal operational in high temperatures**.

To install the terminal with the Magnetic Mount Solution

To mount the magnets on the Commander NEO:

1. Remove the 3 external plastic spacers and mount the magnetic feet in the 3 threaded holes as described in the installation guide included with the Magnetic Mount Solution. Use the included standoffs to provide 30 mm distance between the mounting surface and the

CAUTION! Refer to the *Safety summary* on page -ii before using the Magnetic Mount Solution.

2. Make sure the mounting place on the roof of the vehicle is level and made of a magnetizable material.
3. Wipe the surface clean before you place the terminal on the roof, in order to make a better connection between the magnets and the roof and to avoid scratches in the surface.
4. Place the terminal with magnets carefully on the roof of the vehicle.

WARNING! Do not place your fingers underneath the terminal when you place the terminal on the vehicle!
The magnetic force is very powerful and your fingers may be hurt if they are caught between the terminal and the mounting surface.

5. Connect the cable from the terminal to power and LAN equipment (if used).
Refer to *To connect cables* on page 2-8.

To detach the terminal

Grab the terminal near one of the magnets and lift it. When one magnet is off, the other two are easier to detach.

2.5 To connect cables

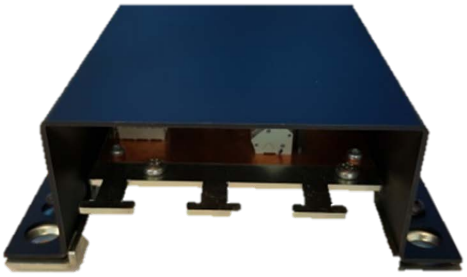
There are different options for power supply to the Commander NEO terminal.

- If you are using a 12-24 VDC supply, e.g. from a vehicle, use the included Hybrid DC/Ethernet cable.
- If you are using Power over Ethernet supply, you can acquire a PoE connection cable without the separate DC wires.

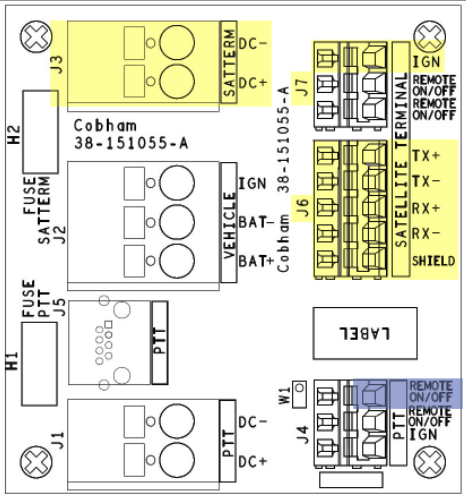
See *Options* on page 1-4 for available cables.

2.5.1 Using the connection box

You can use the **Connection box for NEO and EXPLORER Terminals** for making your connections to the Commander NEO.



Connect the open end of the Commander NEO cable to the connection box according to the highlighted parts of the figure and table below. For details, see the installation guide for the connection box (*98-186961*) and the following sections.



Empty, not connected

Fuse PTT: 4 A

Fuse SATTERM: 7.5 A for use with Voyager/Commander/Orion NEO

Voyager/Commander NEO	J3	DC-	NEO terminal cable	Black	Cable 4
		DC+	NEO terminal cable	Red	
	J7	IGN	NEO terminal cable	Blue	
		Remote On/Off	Not connected		
		Remote On/Off	Not connected		
	J6	Ethernet Tx+	NEO terminal cable	Orange/white	
		Ethernet Tx-	NEO terminal cable	Orange	
		Ethernet Rx+	NEO terminal cable	Green/white	
		Ethernet Rx-	NEO terminal cable	Green	
		Ethernet shield	NEO terminal cable	Silver	

Vehicle	J2	IGN	Typically yellow	Cable 3
		Bat-	Black	
		Bat+	Red	

Mobile Gateway Neo	J1	DC-	MG NEO power cable	Thick black	Cable 1
		DC+	MG NEO power cable	Thick red	
	J4	Remote On/Off	Future use (MG NEO power cable)	Thin black	
		Remote On/Off	Future use (MG NEO power cable)	Thin red	
		IGN	MG NEO power cable	Thin brown	
	J5	Ethernet	Ethernet cable		Cable 2
	W1	Ground jumper	Not connected for NEO terminals		

If used **without** a Mobile Gateway NEO, modify J4:

J4	Remote On/Off	Short circuit
	Remote On/Off	
	IGN	

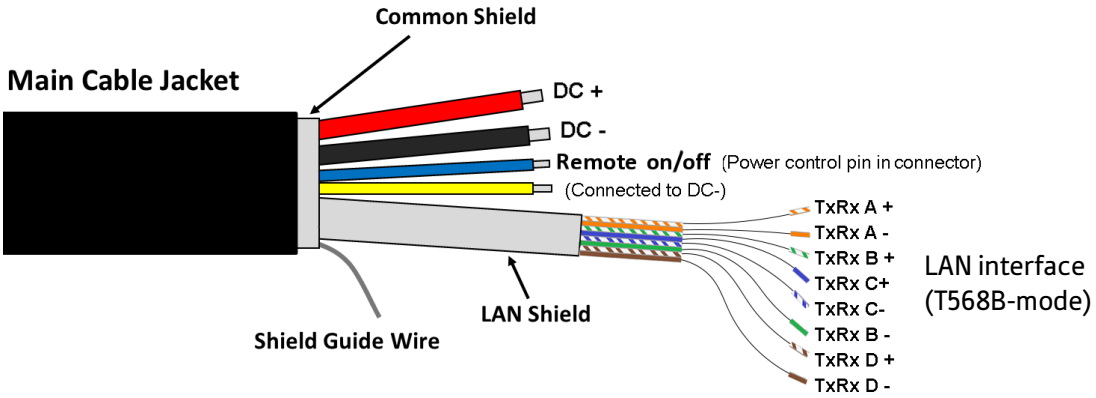
2.5.2 For 12-24 VDC power supply

Hybrid DC/Ethernet cable

A Hybrid DC/Ethernet 6 m cable for connection to power supply and Ethernet equipment comes with the system. If you need a longer cable, a 25 meter cable is also available.

Important The **25 m** cable requires **24 V (or 28 V) operation!**

Note The cable is open-ended to allow for various installation options. Depending on your installation you may use e.g. the Connection Box (previous section) to make the connections, connect the wires directly to vehicle power and other equipment, or mount connectors on the cable.



1. Connect the open end of the cable to the connection box or directly as described in the following sections.

CAUTION! This Hybrid DC/Ethernet cable is strictly for DC power supply. Do **not** connect this cable to both DC power supply and PoE.

CAUTION! Cut off and isolate unused wires in order to avoid short circuits.

2. Connect the cable connector to the circular connector on the Commander NEO.

To connect DC from vehicle

We recommend to use the included 6 m Hybrid DC/Ethernet cable if possible. If you need a longer cable, you can use the 25 meter cable available from your supplier (**only for 24 V or 28 V operation!**).

Important When used without the Mobile Gateway M NEO, the **Remote on/off function is disabled by default** in the Commander NEO. This means that when you have connected the Commander NEO to the battery power of the vehicle, the Commander NEO is always on, and can potentially drain the battery!

We recommend that you use the Remote on/off function as described in the next sections.

Note Do not use the cigarette lighter socket in the vehicle to supply power for the Commander NEO. Connect directly to the 12 or 24 VDC supply instead.

Connect the wires from the Hybrid DC/Ethernet cable:

1. Connect the thick black wire (DC-) to negative (-) in the vehicle.
2. Connect the thick red wire (DC+) to positive (+) in the vehicle.

To connect Ignition

You can use the Ignition system of the vehicle to switch the Commander NEO on and off.

1. Connect the power wires from the Hybrid DC/Ethernet cable to positive (+, thick red wire) and negative (-, thick black wire) in the vehicle as described above in *To connect DC from vehicle*.
2. Connect the blue wire from the cable (Remote on/off) to the ignition signal of the vehicle. Refer to the vehicle manual for information on where and how to connect to the Ignition signal in your vehicle. Also refer to the next section for connection examples for the Power control pin.

   Note The yellow wire is connected to DC- internally in the Commander NEO.

3. Make sure the Commander NEO is switched on.

   Note If the Remote on/off function has already been enabled in the web interface, you can skip the next steps and go straight to step 7 below.

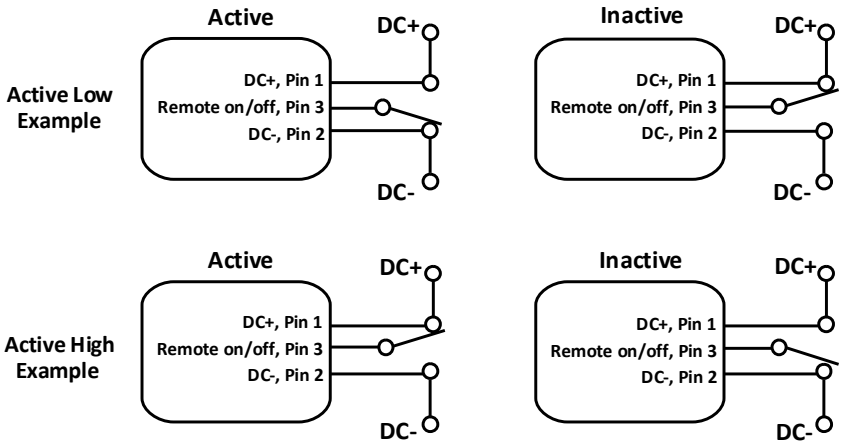
4. Connect a computer, either with the Ethernet interface as described in the next section, or via WLAN as described in *To connect your WLAN-enabled device* on page 3-4.
5. On the connected computer, open your browser and access the web interface by typing the local IP address in the address bar (default IP address: 192.168.0.1).
6. Select **Advanced** › **Power control** and enable the Remote on/off function as described in *Power control* on page 5-26.
7. Verify the Remote on/off function by starting and stopping the ignition of the vehicle and observing the Commander NEO switching on and off (check LED on the Commander NEO).

The Remote on/off signal (Power control pin)

The blue wire in the Hybrid DC/Ethernet cable is the Remote on/off signal, which is connected to the Power control pin in the Commander NEO connector. See *To connect Ignition* on page 2-10. The yellow wire is connected to DC- internally in the Commander NEO.

Connection examples for the Remote on/off signal:

Important The Power control pin in the Commander NEO connector is internally pulled down, so when it is not connected it **will always be in Low state**. However, the state of the Power control pin is only used if **Remote on/off** is selected as power save mode (see *Power control* on page 5-26).



Pin numbers in the Commander NEO connector: see *General specifications* on page A-1.

- If you have configured the input to be Active low (default):
  To deactivate: Connect Remote on/off (blue wire) to DC+ (*High: 2.8 - 32 VDC*).
  To activate: Connect Remote on/off (blue wire) to GND (*Low: 0 - 0.8 VDC*).
- If you have configured the input to be Active high:
  To deactivate: Connect Remote on/off (blue wire) to GND (*Low: 0 - 0.8 VDC*).
  To activate: Connect Remote on/off (blue wire) to DC+ (*High: 2.8 - 32 VDC*).

2.5.3 For PoE power supply

PoE from Mobile Gateway M NEO

The **LAN 1 PoE Ant** output from the Mobile Gateway M NEO meets the specifications for supplying the Commander NEO with Power over Ethernet (see note in next section).

1. Acquire a PoE connection cable for the Commander NEO terminal (see *Options* on page 1-4).
2. Mount an RJ-45 connector at the open end of the cable, matching the **LAN 1 PoE Ant** connector on the Mobile Gateway M NEO.[4]
3. Connect the PoE connection cable between the Commander NEO terminal and the **LAN 1 PoE Ant** connector on the Mobile Gateway M NEO.

For details on installation of the Mobile Gateway M NEO, refer to the manual for the Mobile Gateway M NEO.

PoE from other PoE supplying device

If you do not have a Mobile Gateway M NEO you can connect another PoE supplying device instead, e.g. a PoE injector.

Note A PoE supplying device used with the Commander NEO must comply with minimum Type 4 Class 8 (IEEE802.3bt), capable of supplying 52-57 VDC, 90 W.

1. Acquire a dedicated PoE connection cable for the Commander NEO terminal.
2. Mount an RJ-45 connector at the open end of the cable, matching the PoE injector.
3. Connect the PoE connection cable between the Commander NEO terminal and the PoE injector.

For details on installation of the PoE injector, refer to the manual for the PoE injector.

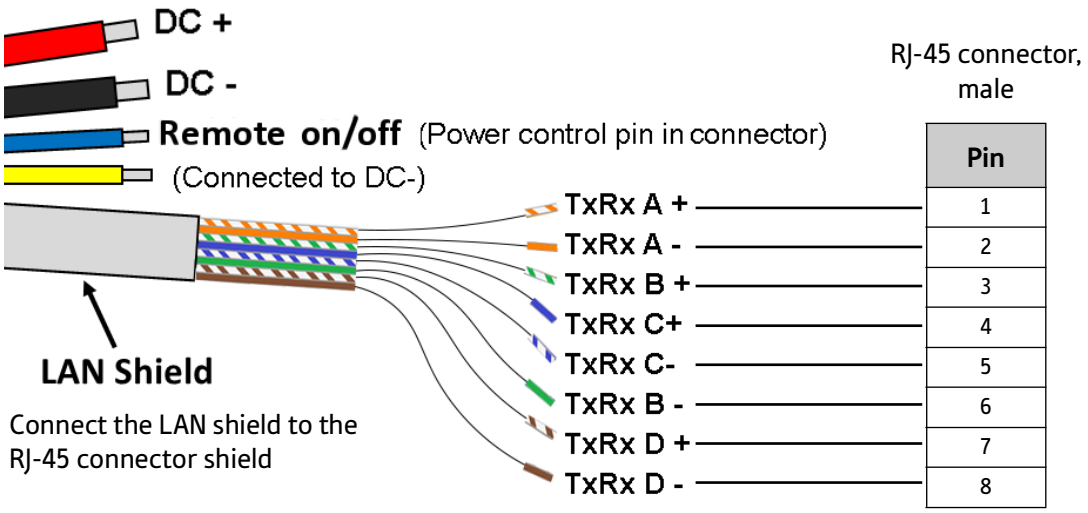
4. For ingress protection, the cable must have special protective connector housings at both ends of the cable. The dedicated cables available for Commander NEO are already protected at one end. Contact your supplier for separate protective connector housings matching the connector at the other end of the cable.

2.5.4 To connect Ethernet

Without PoE

Depending on your configuration, you can connect the Ethernet wires from the Hybrid DC/Ethernet cable to a switch or directly to a PC (using an RJ-45 connector).

1. Connect the DC power wires from the Hybrid DC/Ethernet cable according to the pinout shown in the previous section *For 12-24 VDC power supply* on page 2-9.
   If you prefer to mount an RJ-45 connector for the Ethernet wires, connect the wires as shown below.

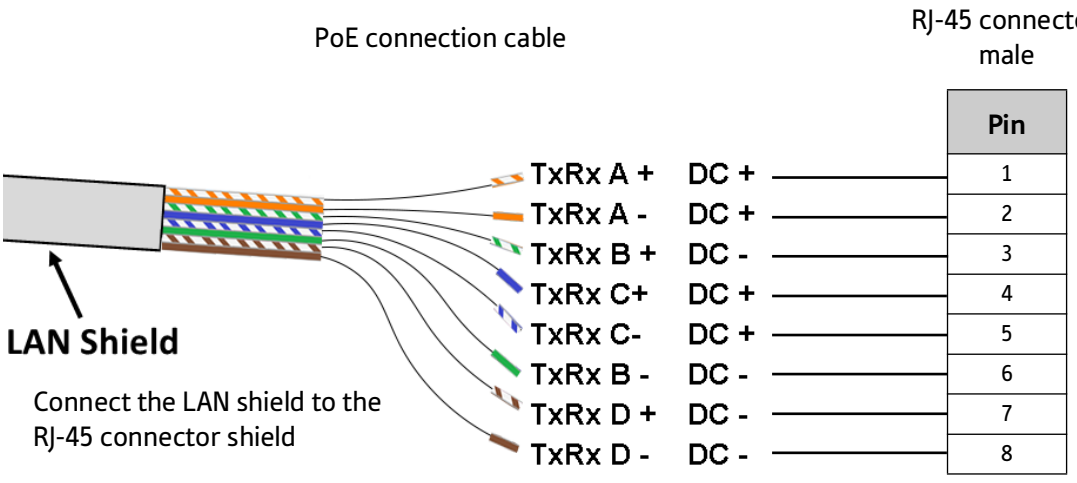


2. For further details on how to connect the LAN interface, see *To connect to the LAN interface* on page 3-3.

With PoE

If the Commander NEO is powered with PoE, there are no separate power wires, power is included in the Ethernet wires in the PoE connection cable.

This means that with the PoE connection cable you can connect directly to the Mobile Gateway M NEO[5] (**LAN1 PoE Ant** connector) or to another PoE supplying device that meets the specifications stated in *PoE from other PoE supplying device* on page 2-12.



5. Note that if the Commander NEO is used with the Mobile Gateway M NEO, the DHCP server in the Commander NEO must be disabled. See*To set up the connection mode* on page 5-20.

To get started

This chapter describes how to start up the system and make the first call or data session. It has the following sections:

- *Before you start*
- *To switch on the Commander NEO*
- *To connect to the LAN interface*
- *To connect your WLAN-enabled device*
- *The SPACE42Connect app*
- *To access the web interface*
- *To enter the SIM PIN for the terminal*
- *Mounting calibration*
- *To register with the satellite network*
- *To start and stop data connections*
- *To enable phone calls over satellite*

3.1 Before you start

3.1.1 Operation at high temperatures

WARNING! In very high ambient temperatures, do not touch areas of the terminal that are marked with this symbol.

3.1.2 Connector

There is only one connector on the terminal, placed on the side of the terminal. This connector is used for both DC power and Ethernet. A dedicated cable is included with the terminal. For details, see *To connect cables* on page 2-8.

3.1.3 SIM card

The Commander NEO requires a SIM card to go online with the satellite network. Without a SIM card you can still configure the terminal, but you cannot access the external network.

There are two options for the SIM:

- A physical SIM card: Nano SIM card (4FF) from your IP NEO C supplier
- An electronic SIM card: eSIM preinstalled in the terminal

Note Before you can use the SIM, the SIM type (eSIM or USIM) must be selected in the web interface. See *To select the SIM mode* on page 5-27.

For details on how to insert the USIM card, see *To insert the SIM card* on page 2-2.

3.2 To switch on the Commander NEO

To use the ignition system

If you have connected the ignition system of your vehicle to the Remote on/off wire (blue wire in cable) and enabled the Remote on/off function in the web interface, the terminal will switch on/off when you start/stop the ignition of your vehicle.

When the ignition is switched off, the terminal is in power save state, unless other conditions keep the Commander NEO from going into power save state. see *Power mode functions* on page 4-8. For information on how to connect Ignition to the Commander NEO cable, refer to *To connect Ignition* on page 2-10.

If you are not using the Mobile Gateway M NEO, you must enable the Remote on/off function in the web interface. For further information, see *Power control* on page 5-26.

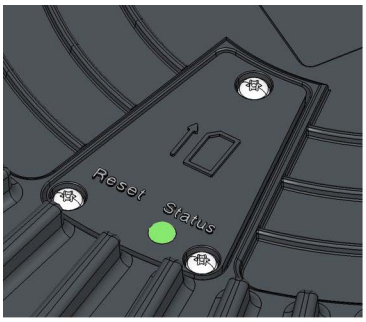
Note In some cases, the system may reboot after power-on because of the high start-up current.

To use a remote on/off switch

If an external switch is connected to the remote on/off signal (Power control pin in the connector), you may use the remote switch to turn the terminal on and off. When the remote switch is off, the terminal is in power save state, same function as with the Ignition described above.

Power up completed

When the terminal is switched on and ready, the LED in the bottom of the terminal lights steady green. By default, the LED stays on for 5 minutes and is then turned off. However, this is configurable in the web interface, see *To configure the LED mode* on page 5-26.



If the LED is flashing green it has started up but is not yet ready to communicate on the network. You can access the terminal settings, but the terminal is not ready to make calls or run data sessions until the system is registered on the satellite network. You may have to enter a SIM PIN before the system can register. For further information, see *To enter the SIM PIN* on page 5-6.

3.3 To connect to the LAN interface

There is only one wired LAN interface in the Commander NEO, so you may want to connect a switch in order to connect more devices. If you want to use a wired VoIP/SIP handset you may need to connect to a PoE switch for power; the Commander NEO LAN interface **does not supply PoE**.

3.3.1 Before you connect to the LAN interface

For the LAN interface to work without any further setup, the connected device must be set up to **obtain an IP address and a DNS server address automatically**.

3.3.2 To connect a computer to the LAN interface

Note This section only describes a Standard data connection with default settings on the terminal. For information on other scenarios, see *To control data connections from web interface* on page 5-7.

To connect a computer to the LAN interface:

1. Power up your computer.
2. Connect your LAN cable between the network connector on your computer and the LAN interface on the terminal (or a switch or Mobile Gateway M NEO connected to the terminal). For details on the physical LAN interface, see *To connect Ethernet* on page 2-13.
3. When the computer and the terminal are ready and the terminal is registered on the satellite network, you can start a data connection, e.g. from the web interface. See *To start and stop data connections* on page 3-10.
4. When you have started a data connection, you are ready to access the network over the satellite Standard data connection.

For information on how to configure the LAN interface on the terminal, see *LAN interface setup* on page 5-14, *Terminal settings* on page 5-19 and *Advanced LAN* on page 5-23.

3.4 To connect your WLAN-enabled device

3.4.1 Prepare the WLAN interface

The WLAN interface is disabled by default, so you must first access the Commander NEO using the LAN interface and then enable the WLAN interface in the web interface.

1. Connect a computer to the LAN interface as described in the previous section.
2. Open your browser and access the web interface as described in *To access the web interface* on page 3-7.
3. Click ⚙ from the bottom right corner of the web interface to access the Control panel.

1. Click the **WLAN** icon at the top of the page.
2. To enable the WLAN interface, select **Enable.**
   For details on WLAN configuration, see *WLAN interface setup* on page 5-14.

3.4.2 Connect your device

1. Switch on the Commander NEO.
2. Place your WLAN-enabled device (computer, tablet or smartphone) close to the Commander NEO.
3. On your device, search for available WLAN networks.
4. Select the Commander NEO WLAN access point when it appears in your list of available wireless networks.
   The default name is **Commander-NEO_<last four digits in serial number>**.

Note You must enter a password. By default the password is the serial number[1] of your Commander NEO and the encoding type is **WPA2-AES**.

1. You find the serial number on the label on the bottom side of the Commander NEO.

Your device is now connected to the Commander NEO. In the web interface, the WLAN icon shows the number of devices connected to the Commander NEO via WLAN.

For information on how to configure the WLAN interface in the Commander NEO, see *WLAN interface setup* on page 5-14.

For information on how to set up the LAN network, see *LAN interface setup* on page 5-14 and *Advanced LAN* on page 5-23.

3.5 The SPACE42Connect app

The SPACE42Connect app allows for configuration of supported NEO satellite terminals and enables satellite calls via Android or iOS smartphones. The app is available for Android phones at the Google Play store and for iPhones at the App Store.

3.5.1 First time app use

Permissions

When you start the app, some of these permissions may be required for optimal functionality (depending on your phone OS and version):

Android:	
Phone	Enables native phone controls while in a call and integration with top bar and background calls.
Calling account	Uses the SPACE42Connect app to make calls via the native phone application.
Microphone	Enables microphone for use in phone calls.
Contacts	Enables access to phone contacts.
iOS:	
Microphone	Enables microphone for use in phone calls.
Contacts	Enables access to phone contacts.
Local network	Enables access to the terminal which is required for using and configuring the terminal (Wi-Fi).

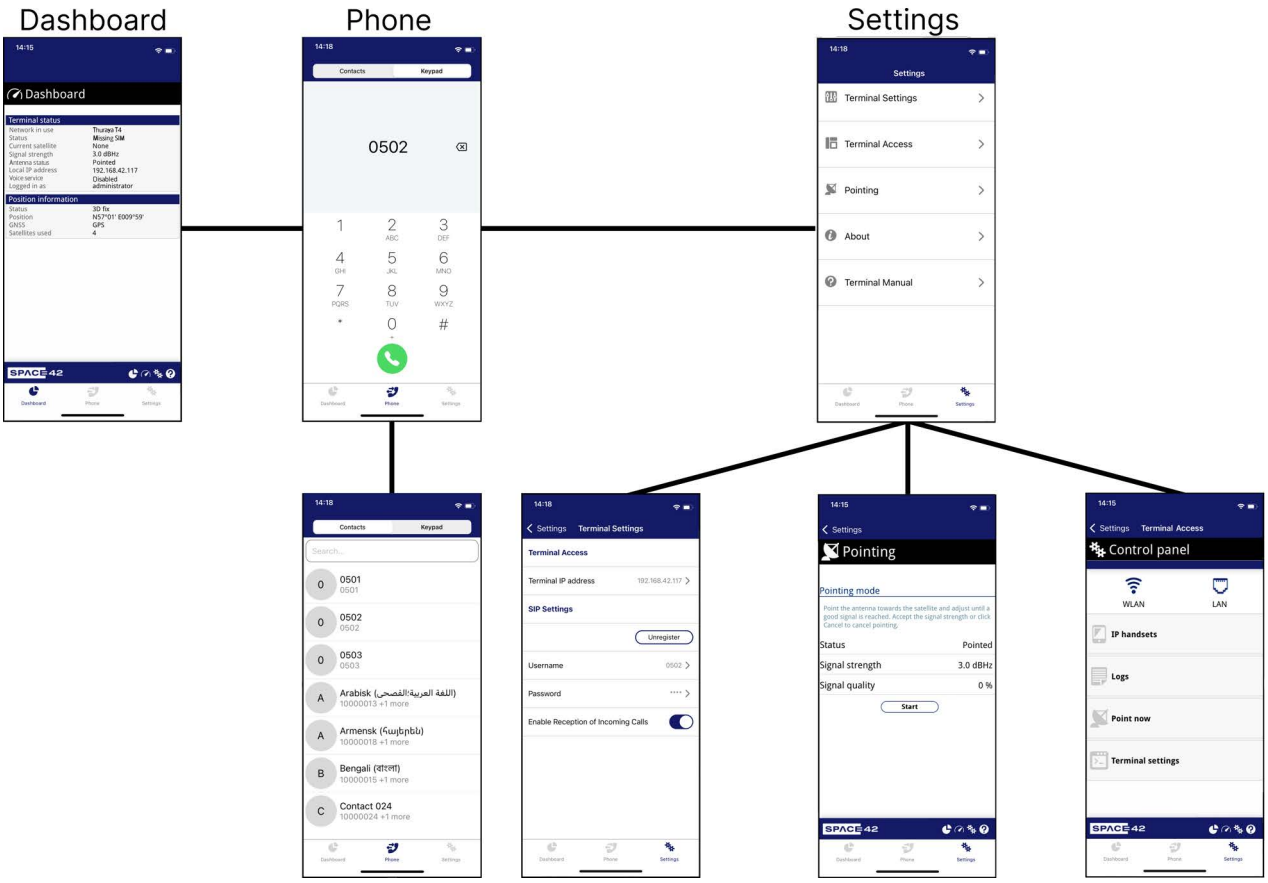
Note iOS does not support background calls. To receive a call on an iPhone, the app must be open and visible on the screen.

Menu overview of SPACE42Connect app

There are 3 main screens in the SPACE42Connect app: Dashboard, Phone and Settings, selectable from the icons at the bottom of the screen.

- **Dashboard**: shows status of the terminal and connections.
- **Phone**: Is used for making calls.
- **Settings**: Has a submenu with the following options:
  - Terminal Settings: Holds the IP address of the terminal and the SIP settings for connecting the SIP client in the phone with the SIP server in the terminal.
  - Terminal Access: Gives access to all configuration settings and status in the terminal (same as in the terminal's web interface).
  - Pointing: Antenna pointing. Not applicable for the Commander NEO.
  - About: Shows the App version of the SPACE42Connect app and the Helpdesk information entered in the terminal's web interface (Advanced › Help desk).
  - Terminal Manual: Accesses the user manual for the Commander NEO (this manual).

SPACE42Connect app screens (example):



To set up the SPACE42Connect app for making calls

To set up the system to make calls through the terminal using WLAN, follow these steps:

1. Start up the terminal.
2. Connect to the terminal WLAN as described in the **Getting Started** chapter of this manual.
3. Open the SPACE42Connectapp and grant any required permissions, if any (see *First time app use* in the previous page).
4. If the terminal is password protected, log in to the terminal[1]:
   - Default for normal user: username= **user**, password= ‹**empty, no password**›.
   - Default for administrator: username= **administrator**, password= ‹**serial number of the Commander NEO**›
5. Go to **Settings** › **Terminal settings** › **SIP settings** and enter:
   - **Terminal IP Address** (SIP server address and port): Default address: **192.168.0.1**, Port: **5060**.
   - **Username** (handset user name): Default range **0501** to **0516** .
   - **Password** (handset password): Default same as username.

Note The handset username and password must match the IP handset settings in the web interface of the terminal, see the Configuration chapter, Voice setup.

1. To log out of the terminal select **Dashboard** and tap **log out**.

6. Make sure **Enable Reception of Incoming Calls** is selected.
   This is to prevent your smartphone from closing the WLAN connection when not in use. This is necessary in order to be able to receive calls on your smartphone.
7. Tap **Register** to complete the SIP registration.

With the SPACE42Connectapp open and visible on the screen, your smartphone should now be ready for making a call over satellite using the Commander NEO.

To configure the Commander NEO using the SPACE42Connect app

The SPACE42Connect app provides access to all terminal settings that are available in the web interface. To configure the terminal from the app, navigate to **Settings › Terminal Access**. For details on configuration, see the **Configuration** chapter.

3.6 To access the web interface

You can use the built-in web interface for configuration and operation of the Commander NEO. To access the web interface:

1. Start up the terminal.
   For details, see *To switch on the Commander NEO* on page 3-2.
2. Connect your computer or smartphone to the terminal, using LAN or WLAN as described in the previous sections.
3. Open your browser and enter the IP address of the terminal in the address bar. The default IP address of the terminal is 192.168.0.1.
4. Enter user name and password. You can log in as user or as administrator.
   - Default for **user**: User id = user, Password = ‹empty›
   - Default for **administrator**: User id = administrator, Password = ‹serial number of the Commander NEO›

   Important | For security reasons, change the passwords after first login.

The web interface opens on the dashboard. For more information on the web interface, see *The web interface* on page 5-2.

3.7 To enter the SIM PIN for the terminal

3.7.1 Do you need a SIM PIN?

To avoid having to enter a PIN at startup, you can disable the use of a SIM PIN. See *To enable or disable the use of a SIM PIN* on page 5-27. When the SIM PIN is disabled, the SIM can be used by other terminals without a PIN.

If you are using a SIM PIN in your system, you can enter the SIM PIN from the built-in web interface. For details, see the next section.

Note If you are asked for a PIN in the web interface and you select **Cancel**, you cannot communicate on the network, but you can access all settings.

For information on how to connect your computer, see *To connect a computer to the LAN interface* on page 3-3 or *To connect your WLAN-enabled device* on page 3-4

3.7.2 To enter the SIM PIN using the web interface

To enter the SIM PIN

Do as follows:

1. On a computer connected to the terminal, open your browser and enter the IP address of the terminal in the address bar (default IP address: **http://192.168.0.1**).
   If your SIM card uses a PIN and the PIN has not yet been entered, the web interface will open with an **Enter SIM PIN** popup.
2. Type in the PIN and click **OK**.
   When the PIN is accepted, the web interface opens the Dashboard and is ready for use. If the PIN is not accepted, see the next section *Wrong PIN*.

For further information on the web interface refer to *To use the web interface* on page 45.

Wrong PIN

You have 3 attempts to enter the PIN in the web interface, before you are asked to enter the PUK (Pin Unblocking Key). The PUK is supplied with your SIM card.
Enter the PUK followed by a new PIN of your own choice. The PIN must be 4 to 8 digits long.

If you enter a wrong PUK 10 times, the SIM card will no longer be functional, and you have to contact your Airtime Provider for a new SIM card.

3.8 To register with the satellite network

Note The terminal must have free line of sight to the satellite.

The correct satellite network must be selected in the web interface (T2/T3 or T4-NGS), see *To select the satellite network* on page 5-12.

When the terminal is started up, the Commander NEO System automatically starts the registration procedure on the satellite network.

To monitor the registration procedure, connect a computer, access the internal web interface of the terminal and watch the **Terminal status** field.

Normal startup procedure:

1. **Initializing** - The terminal is starting up.
2. **Acquiring position** - The terminal is trying to get a position fix.
3. **Scanning** - The terminal is scanning to find the satellite.
4. **Channel search** - The terminal is searching for the best channel.
5. **Registering** - The terminal is registering on the network.
6. **Ready** - The terminal is ready to set up data connections.

Note that the registration procedure may take several minutes.

The **Terminal status** in the web interface also shows the status during and after registration.

When the system is ready, the **Antenna status** field shows **Tracking** (or **Pointed** if not moving) and the **Status** field shows **Ready** (unless a call or data session is active).

Important The terminal may not be able to stay locked to the satellite signal if the vehicle moves very slowly, especially if it turns or goes backwards at a very slow pace. When the vehicle moves normally, the antenna status will show **Tracking**, but when it stops or moves very slowly it enters a different state and the status shows **Pointed**. In the Pointed state, the terminal assumes that it is stationary and not moving. As the vehicle picks up speed it will find the satellite signal and eventually show **Tracking** again.

Note The Commander NEO needs information on its mounting orientation in relation to the vehicle. To obtain or verify this information it runs a calibration or validation process when moving after restart. For details, see the next section, *Mounting calibration*.

3.9 Mounting calibration

Every time you start up the Commander NEO and move the vehicle, the Commander NEO will try to detect how it is oriented in relation to the vehicle (Mounting calibration). This is necessary in order to obtain and maintain the best possible signal strength when the vehicle is moving.

After a restart, the Commander NEO will run a calibration process, which may take a couple of minutes.

In most cases the terminal will be calibrated by normal driving in urban areas for a few minutes (normal accelerating, braking and turning).

For optimal calibration, drive two or three times a route in the shape of figure 8, at speeds above 20 km/h (12 mph) when possible.

Status of the mounting calibration

You can see the status of the mounting calibration in the **Terminal status** field in the web interface. The status can be:

- **Calibrating**: Shown after first installation or factory reset. The Commander NEO runs a complete calibration process and goes directly to status **Completed** when done. When moving in this state the terminal is **not** able to track the satellite.
- **Validating**: Shown after restart of the Commander NEO. The Commander NEO validates the mounting information from previous startup and goes directly to status **Completed** when done. When moving in this state the terminal will attempt to track the satellite using the previous mounting information.
- **Completed**: Shown when the calibration (or validation) process has finished. The Commander NEO now has the correct information of its mounting orientation in relation to the vehicle and is able to track the satellite while moving.

3.10 To start and stop data connections

By default, you have to start a data connection manually when the terminal is ready and connected to the satellite network. However, you can enable automatic activation of a data connection. See *Internet and LAN connection modes* on page 5-20.

To start and stop data connections on your Commander NEO:

1. On the connected device, open your browser and access the web interface, or
   On your smartphone, start the **SPACE42Connect** app and select **Settings** › **Terminal access**.
2. Locate the connection package you want to start.

   Note The icons for starting ▶ and stopping ■ connections are only active if the terminal is ready and registered on the network. Otherwise you cannot start data connections.

3. Click ▶ to start the connection.
4. Click ■ to stop the connection.

For details, see *To control data connections from web interface* on page 5-7.

3.11 To enable phone calls over satellite

Your smartphone or IP handset can be set up to make and receive calls over the satellite network, using the terminal's phone number.

Note Make sure your phone has an integrated SIP client. The Commander NEO has an integrated SIP server.

By default, one SIP client is enabled in the Commander NEO with the user name 0501. Additional phones (SIP clients) must first be set up inthe web interface and enabled before you can use them,

3.11.1 To connect your smartphone for making calls

Space42 offers the **SPACE42Connect** app with a built-in SIP client that is ready to use with the Commander NEO. You can also find other SIP applications on the Internet

1. Start up the Commander NEO terminal.
2. Connect your smartphone to the wireless access point of the Commander NEO.
   See *To connect your WLAN-enabled device* on page 3-4.
3. Open the SPACE42Connect app or start another SIP client.
4. Set up your smartphone for use with the Commander NEO.
   - SPACE42Connect app: See *To set up the SPACE42Connect app for making calls* on page 3-6.
   - If you have a 3rd party SIP client, see
   - To set up the Commander NEO for use with your smartphone, see *To manage phones in your Commander NEO* on page 5-16.
5. In the SPACE42Connect app select Phone, or start your 3rd party SIP client.

You should now be ready to make and receive calls over satellite with your smartphone.

For details on calls, see *To make phone calls over satellite (only with T4-NGS)* on page 4-6.

3.11.2 To connect a wired IP handset for making calls

Space42 offers the Space42 IP Handset with a built-in SIP client ready for use with the Commander NEO.

Note The Commander NEO does not supply PoE, so if your IP handset requires PoE you must connect a PoE switch or similar to supply power for the IP handset.

Note If you are using the Space42 IP Handset, no initial configuration is necessary.

1. Start up the Commander NEO terminal.
2. Connect your PoE switch or similar to the LAN interface in the Commander NEO cable (see *To connect Ethernet* on page 2-13).
3. Connect the IP handset to a PoE output on the PoE switch.
4. Set up the handset for use with the Commander-NEO.
   - Space42 IP Handset: Is ready for use with the Commander-NEO.
   - If you have a 3rd party IP Handset: see *First time SIP setup* on page 3-12 and the documentation for your handset.

- To set up the Commander NEO for use with your IP Handset, see *To manage phones in your Commander NEO* on page 5-16.

When the IP handset is powered and ready, you should now be able to make and receive calls over satellite.

3.11.3 First time SIP setup

If it is the first time you connect your phone to the Commander NEO for making calls, you must first set up the SIP server details in your phone. For information how, see the user documentation for your phone and for the SIP application. You may be asked to enter some of the following details (the SPACE42Connect app and the Space42 IP Handset are preconfigured with the below default settings):

- SIP server address and port: Default address: 192.168.0.1, Port: 5060
- User name: Local number in Commander NEO (0501 to 0504, by default 0501)
- Password: Create a four-digit password for the IP handset (by default 0501).
- Codec priority: Highest priority codec type: G.711.

Note The user name and password must match the IP handset settings in the Commander NEO. See *Voice setup* on page 5-16.

To use the Commander NEO

This chapter describes how to use the Commander NEO. It has the following sections:

- *Tools for setup and use*
- *Data connection with computer, smartphone or tablet*
- *To control data connections*
- *To make phone calls over satellite (only with T4-NGS)*
- *Power mode functions*
- *Stealth mode*
- *Alerts*
- *Status of the Commander NEO*

4.1 Tools for setup and use

- The **web interface** is a built-in web interface for easy configuration. The web interface is accessed from a computer connected to the Commander NEO, using a browser. No installation of software is needed on the computer. For further information on the web interface, see *The web interface* on page 5-2.
- A smartphone app, **SPACE42Connect**, is also available for iPhone and for Android phones. The app includes a **satellite phone** function that enables you to make calls to and from your smartphone over the satellite network using the Commander NEO terminal. It also includes the complete feature set from the built-in web interface of the terminal, allowing you to **set up and use the terminal** with your smartphone.
- With **AT commands** you can configure and control the Commander NEO from a computer using an ssh session, or from other connected equipment. For further details see *To access the terminal using AT commands* on page 4-5 and Appendix B, *Command reference*.
- With a **Space42 IP Handset** you can enter PIN/PUK for the terminal, view pending alarms, view event log, view current satellite status and signal strength, and start/stop connection packages. For details, see *Commander NEO functions in the Space42 IP Handset* on page 4-7.
- With the **REST API** you can use your own application to configure and get the state of the terminal. For details on the REST API, see the REST API documentation for the Commander NEO (doc. number *98-182365*) attached to this PDF file.

Note Not all browsers support attachments in pdf files. If you cannot see and open the attachment in your browser, use the Firefox browser, or download and open this manual in a PDF reader such as Adobe Acrobat.

In addition to the above, you may have the **Remote Terminal Manager (RTM)**, used for remote configuration and management of several NEO terminals (only supported in T4-NGS network):

4.2 Data connection with computer, smartphone or tablet

4.2.1 Interfaces

The following interfaces are available for connecting computers, smartphones or tablets:

- LAN
- WLAN

4.2.2 Router function

The terminal has a router function which routes traffic between the local network connected to the terminal and up to 11 satellite network connections (also called PDP contexts on the satellite network).

The router contains NAT (Network Address Translation) which allows sharing of a public IP address between a number of local network users.

4.2.3 Standard or Streaming data

The satellite network supports different classes of data connection to the network. The main classes are **Standard data** and **Streaming data**.

- Using a **Standard data** connection, several users can share the data connection simultaneously. This type of connection is ideal for TCP/IP traffic such as e-mail, file transfer, and Internet and intranet access.

  The user pays for the amount of data sent and received.
- Using a **Streaming data** connection, you get an exclusive, guaranteed bit rate connection, ensuring seamless transfer of data. This type of connection is ideal for time critical applications like live video over IP.

  The user pays for the duration of the connection (per minute charge).

4.3 To control data connections

4.3.1 Automatic Connection Activation (ACA)

In the web interface you can set up the Commander NEO to automatically establish a data connection when it is registered on the satellite network. See *Enable Automatic Connection Activation* on page 5-9. Automatic Connection Activation also applies to the “wake up” after power save (see *Power mode functions* on page 4-8) and by recovery after e.g. loss of power. This means when ACA is enabled, your data connection will automatically be reestablished when the terminal “wakes up” and registers on the network after power save, loss of power, or loss of the network connection.

4.3.2 Manual activation of data connections

You can manually activate a data connection by connecting to the LAN or WLAN interface and then do one of the following:

- Access the web interface locally and click the tile for the data connection on the dashboard, see *To start and stop data connections* on page 5-7, or
- Send an AT command to the terminal. See *To configure the connected equipment for PPPoE* on page 4-4, *To access the terminal using AT commands* on page 4-5 and *Context management AT commands* on page B-4.

4.3.3 PPPoE (Point-to-Point Protocol over Ethernet)

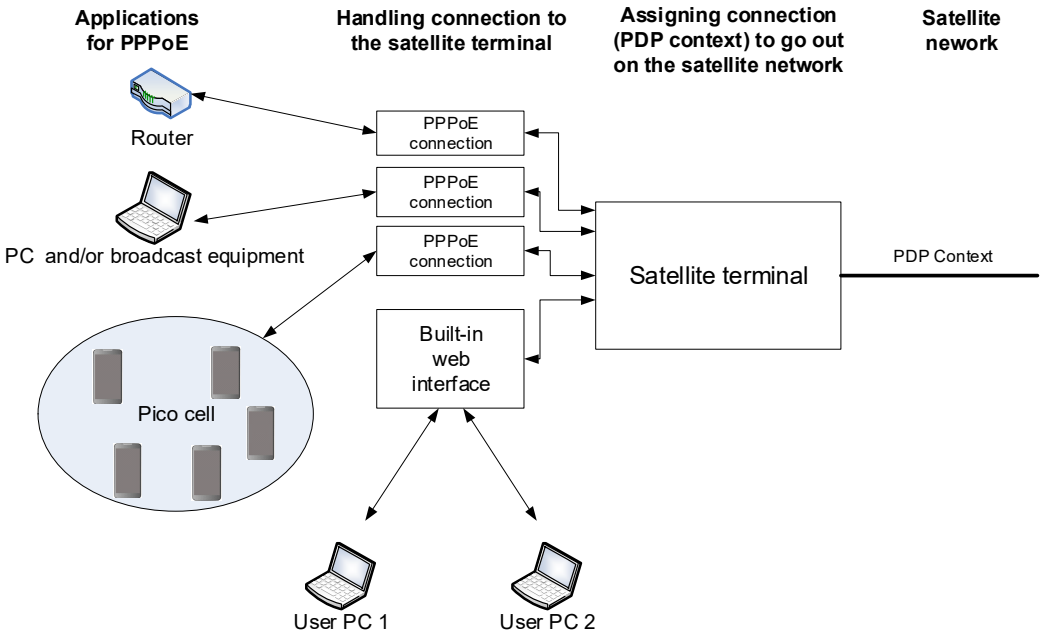
Overview

You can establish a PPPoE connection to the satellite network using the Commander NEO system. Use PPPoE if you want to control your connection independently of the web interface.

Possible applications are:

- Connect a Mobile Gateway M NEO.
- Connect a router.
- Connect broadcast equipment, optionally through a PC.
- Establish a Picocell for the use of cell phones.

The drawing shows connections managed through PPPoE and web interface respectively.



To configure the connected equipment for PPPoE

How to configure your equipment depends on the type of equipment. Refer to the user documentation of the equipment. As a minimum, you need to configure the following parameters in your equipment in order to make PPPoE work with the terminal:

- User name and password.

  The user name and password can be left blank (or insert user name: void and password: void). Then the registration on the Access Point is most commonly done in such a way that the data connection is established with a dynamic IP address from the airtime provider.

  To request a static IP (if subscribed to) from the Access Point you must type in the user name and password from your airtime subscription.

  Note for MAC OS: User name and password are required. Use user name void and password void. This works for some ISPs. Contact your airtime provider for further information.
- For setups that have a check box for “Enable LCP extensions”, deselect this.

No further configuration is needed to make a Standard IP data connection to the network.

See the table below for information on how to configure specific services for your PPPoE connection.

If you need a certain service, for example a Streaming class, you must type in a specified text string when asked for a service name.

The following table shows the service names supported by the terminal.

Text to type in the Service Name field	Function
(Blank)	Initiates a Primary Standard Data connection (default)
XBB:BACKGROUND	Initiates a Primary Standard Data connection (same as blank)
XBB:STREAM16K	Initiates a Primary Streaming 16 kbps connection
XBB:STREAM32K	Initiates a Primary Streaming 32 kbps connection
XBB:STREAM64K	Initiates a Primary Streaming 64 kbps connection
XBB:STREAM128K	Initiates a Primary Streaming 128 kbps connection
XBB:STREAM256K	Initiates a Primary Streaming 256 kbps connection
XBB:STREAM384K	Initiates a Primary Streaming 384 kbps connection
XBB:STREAM512K	Initiates a Primary Streaming 512 kbps connection
XBB:STREAM768K	Initiates a Primary Streaming 768 kbps connection
XBB:STREAM1024K	Initiates a Primary Streaming 1024 kbps connection

4.3.4 To access the terminal using AT commands

1. Make sure that AT shell is enabled and the AT shell password is set up in the web interface, see *To set up AT shell* on page 5-29.
2. Connect your computer to the Commander NEO terminal.
3. On the connected computer, start an SSH connection using the local IP address of the Commander NEO (default is 192.168.0.1). Use "atshell" as user.

   `Example: ssh atshell@192.168.0.1`

4. When prompted, enter the AT shell password you defined in the web interface (step 1).
5. When the connection is established, type in your AT commands.

   For information on supported AT commands, see *Command reference* on page B-1.

4.4 To make phone calls over satellite (only with T4-NGS)

Your IP handset or smartphone can be set up to make and receive calls over the satellite network, using the terminal's phone number.

Connect and configure your phone and the Commander NEO as described in *To enable phone calls over satellite* on page 3-11.

When the phone and Commander NEO are powered and ready, you are able to make and receive calls over the satellite connection.

4.4.1 To make or receive a phone call with Commander NEO

To make a call from the Commander NEO

If you are using a smartphone with the **SPACE42Connect** app, first start the app and select **Phone** from the main menu.

To make a call, dial

+ <country code> <phone number> followed by off-hook key.

Example: To call Cobham Satcom in Denmark (+45 39558800), dial **+45 39558800 or 00 45 39558800**

If you are calling with the **SPACE42Connect** app, you may also select a number from the **Contacts** list (icon in bottom right corner from the dial page). Note that the contacts found here are the contacts of your smartphone, **not** of the Commander-NEO.

If there was an error establishing the connection, the web interface of the Commander NEO shows an error message.

To receive a call

By default, all phones connected to the Commander NEO will ring when the mobile number of the Commander NEO is called.

Information on missed calls is stored in the call log. You can see the call log in the web interface (**Control panel** ⚙ › **Logs** › **Call log**).

To make a call to the Commander NEO

To make a call to a phone connected to the Commander NEO, dial **+ <Mobile number>**

- **+** is the prefix used in front of the country code for international calls. This is **00** when calling from countries in Europe and from many other countries.
- **Mobile number.** For information on the mobile number, refer to your airtime subscription.

4.4.2 Local numbers and special functions

There are a number of local numbers and dialing functions available in the Commander NEO.

The following list shows the allocated local numbers and special-purpose numbers for the Commander NEO.

Number	Function
0 followed by one of the numbers 501-504 and off-hook key	Local call to one smartphone or IP handset connected to the same Commander NEO terminal.
0500 followed by off-hook key	Local call broadcast to all locally connected phones.

Apart from the numbers above, the Commander NEO uses the following dialing prefixes:

- #31# before the phone number will hide the callers phone number to the recipient.
- *31# before the phone number will show the callers phone number to the recipient where it would otherwise be hidden, e.g. because the number is an ex-directory number.

To make local phone calls

You can make local calls between phones connected to the Commander NEO. For an overview of the available numbers, see the table in the previous section.

To make a local call, dial **<local number>** followed by **#** or **off-hook key**.

4.4.3 Commander NEO functions in the Space42 IP Handset

In addition to making calls over the T4-NGS network, the Space42 IP Handset offers some functions for use with the Commander NEO terminal.

Note If you want to use the Commander NEO functions of the Space42 IP Handset you must log in using the same user or administrator account used for the the web interface.

If you have Space42 IP Handset connected to the terminal and you are logged into the Commander NEO, you can use the handset to:

- Make calls over the Thuraya T4-NGS network.
- Enter PIN/PUK for the terminal.
- View alarms and event log.
- View current satellite status and signal strength
- Start and stop data connections over satellite.
- Set up PTT function and use as PTT handset with Mobile Gateway M NEO and Commander NEO.

For details on how to set up IP handsets connected to the Commander NEO, see *Voice setup* on page 5-16.

For details on the Space42 IP Handset, see the user manual for the Space42 IP Handset (doc. no. *98-188255*).

4.5 Power mode functions

You can configure the power mode options with the web interface. For details, see *Power control* on page 5-26.

You can choose between two modes:

- **Always on**. This is the default setting. The terminal will never go into power save state but will always be on when connected to power.
- **Remote on/off**. The terminal will go into power save state when the Power control pin (Remote on/off signal) is inactive. For details, see the following section *Remote on/off*.

4.5.1 Always on

Always on is the default mode where the terminal stays on as long as power is connected.

Important When the Commander NEO is powered from the vehicle battery there is a risk of draining the battery if you use this method! We recommend to use the Remote on/off method instead.

4.5.2 Remote on/off

When Remote on/off is selected in the web interface, you can control the power save function using the Power control pin (Remote on/off signal). See the next section for details.

You can configure the function in the web interface (see *Power control* on page 5-26).

Note To use the Remote on/off function you must first connect the blue Remote on/off wire to the ignition of your vehicle (or to another remote on/off switch) as described in *To connect Ignition* on page 2-10.

Power control pin function when Remote on/off is selected

You can set the polarity of the Power control pin, that is whether the pin should be active high or low. **Default is active low**.

The function of the Power control pin in Remote on/off mode is:

Power control pin is active: The terminal is on and will stay on as long as the pin is active.

Power control pin is inactive: The terminal will attempt to go into power save state. However, a number of conditions may keep the terminal awake even if the Power control pin is inactive:

- Optional shut-down delay period ongoing.
  This is a configurable delay period between deactivating the Power control pin and entering power save state.
- The terminal is in the process of updating software or downloading software for installation.
- Terminal was started by connecting power and 3 minute grace period is still ongoing.
  To avoid the terminal going into power save state immediately at power-up, the terminal stays awake for 3 minutes after power-up, to allow for reconfiguration of the terminal if wanted.

4.6 Stealth mode

If Stealth mode is supported by the SIM, you can put the Commander NEO in Stealth mode. When the Commander NEO is in Stealth mode, **WLAN, LED and system sounds are disabled**.

Important Note that this setting **only applies to the Commander NEO** terminal. Connected equipment must be put into Stealth mode individually.

To activate Stealth mode in the terminal:

1. Connect a computer and access the web interface at http:**192.168.0.1** as described in *To access the web interface* on page 3-7.
2. Select (Control panel).
3. Click the **Stealthmode** tile.
   When Stealth is activated, the tile image is red, and a red Stealth icon appears in the status bar at the top of the page.
4. To exit Stealth mode, click the **Stealthmode** tile again. The text and image on the tile becomes gray and the Stealth icon disappears from the status line at the top.

4.7 Alerts

When an alert is registered, the web interface shows a warning icon in the icon bar as long as the alert is active. The **Alerts** list only shows alerts that are currently active.

To view the Alerts list, click from the icon bar at the top of the page, or select **Alerts** from the **Support** page.

For more information on the alert messages, refer to *List of alert messages* on page 6-10.

4.8 Status of the Commander NEO

Web interface: If the screen for the web interface is large enough, it shows a status field at the bottom of the page or in the right side of the page. If not, click to show the status page. Click again to return to the previous page.

The Status page shows information such as terminal status, network status, position status and ongoing communication.

Configuration

This chapter describes how to use the **web interface** to operate, set up and configure your system.

The Configuration chapter has the following sections:

- *The web interface*
- *To enter the SIM PIN in the web interface*
- *To control data connections from web interface*
- *Status information*
- *The Control panel*
- *To select the satellite network*
- *To activate Stealth mode*
- *To use the logs*
- *To set up the interfaces*
- *Voice setup*
- *Support features*
- *Terminal settings*
- *Advanced LAN*
- *Advanced settings*

5.1 The web interface

5.1.1 What is the web interface?

The web interface is built into the terminal and is used for operating, setting up and configuring the system.

You can access the web interface from a computer with a standard browser.

5.1.2 Access levels for the web interface

There are two levels of access to the web interface:

user has access to the following:

- Start and stop data connections
- Read main configuration parameters.
- Generate and download diagnostics report.
- Embedded user manual.

administrator has access to the same as **user**, plus the following:

- Read and write all main configuration parameters.
- Upload software.
- Change password for “user” and “administrator”.
- Enable AT shell access and change password for AT shell.

5.1.3 To access and navigate the web interface

To access the web interface

To access the web interface:

1. Start up the terminal.
   For details see *To switch on the Commander NEO* on page 3-2.
2. Connect your computer to the terminal.
   For details see *To connect to the LAN interface* on page 3-3 or *To connect your WLAN-enabled device* on page 3-4.
3. Open your browser and enter the IP address of the terminal in the address bar.
   The default IP address of the terminal is **192.168.0.1**.
4. When prompted, enter user ID and password. Default values are:
   - Standard user:
     user ID: **user**
     Password: <empty>
   - administrator user
     User ID: **administrator**
     Password: <serial number of your Commander NEO>

Note You are prompted to change the administrator password after first logon. For details, see *To change the administrator password* on page 5-25.

To change the language

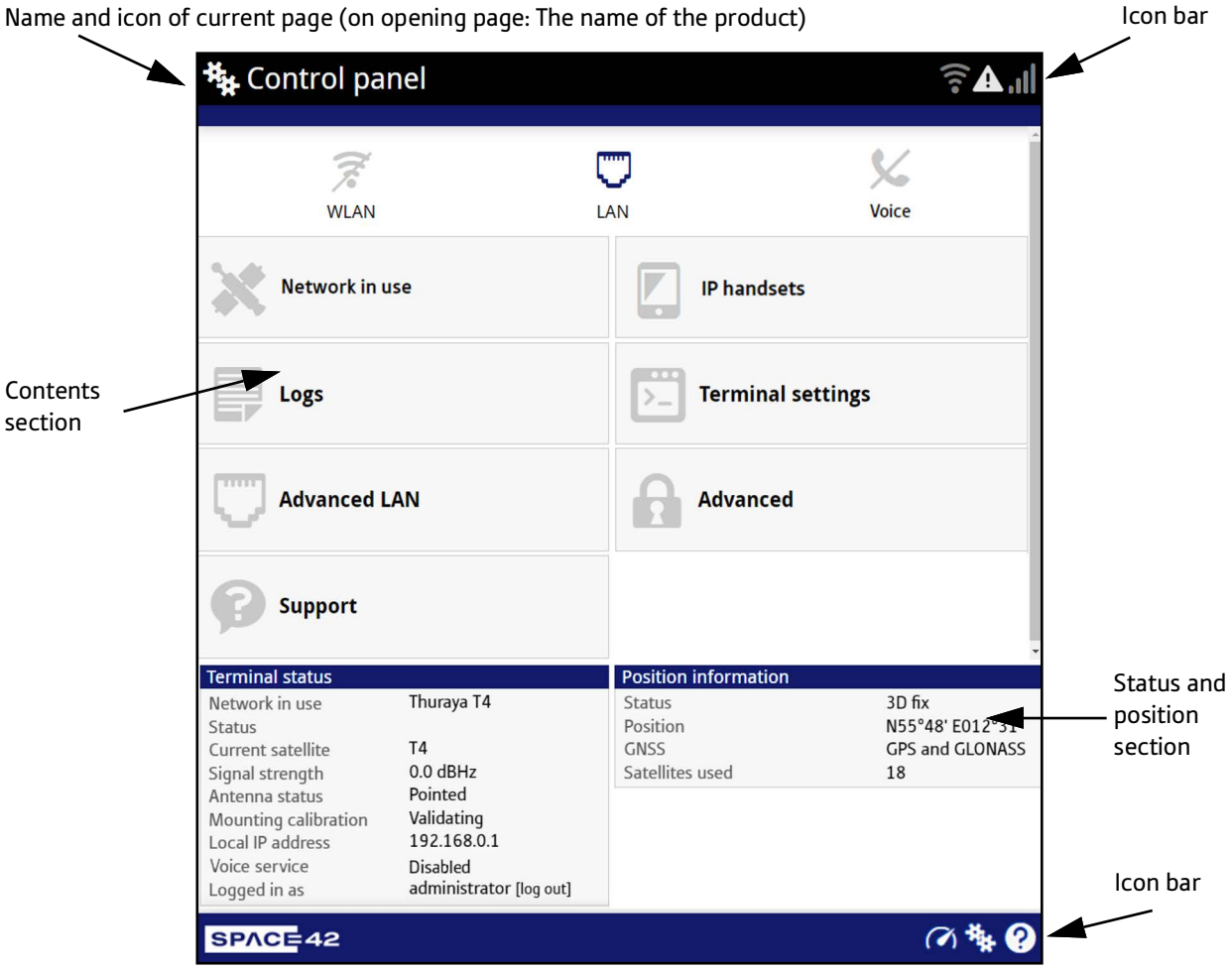
When you have access to the web interface, if you want to display a different language than English:

1. Select the Control panel in the bottom right corner.
2. Select **Terminal settings**.
3. At **Language**, select a language from the drop-down list and click **Apply**.

You can change the language to **Arabic, Chinese, French, Japanese, Portuguese, Russian** or **Spanish.**

Overview of the web interface

When the web interface opens, the title bar shows the name of the product. The example below shows the **Control panel** page.



The web interface consists of the following sections.

- **Name** of current page. Tap or click to refresh the page.
- **Icon bars** at the top and bottom are present on all pages and hold icons that give access to status such as signal level as well as active alerts when relevant. It also holds the icon for the Control panel. For explanations of the icons, see the next section, *Icons in the icon bars*.
- **Contents section** shows the contents of the selected page. This section is used for viewing or changing settings, or for performing actions. On the opening page, this section is used to start and stop data connections.
- **Status and position section** shows the status of the terminal and the network connection, position information, ongoing calls and data sessions etc. The Status section is not shown on

small screens. If the screen is small (e.g. on a smartphone), you can show/hide the status by clicking at the bottom of the page.

Icons in the icon bars

The icon bars are always available at the top and bottom of the web interface. Some of the icons are permanent while others are temporary.

Icon	Explanation
	Signal level of the external network (satellite network).
 2	WLAN interface. Bright when WLAN is enabled, grayed when it is disabled. Click to access WLAN settings. The WLAN icon shows the number of connected devices.
	An alert is active. Click the icon to see a list of active alerts. Note that this icon will remain in the icon bar as long as the alert is still active.
	Help. Click to get context-sensitive help for the current page (in this manual).
	Control panel. Click to access the settings.
 1	Startup page where you can start and stop data connections. Click to go to the startup page. The "1" at the icon shows that a satellite data connection is running.
	Status. If the screen is not large enough to show the status field, this icon appears at the bottom of the page. Click the icon to see status of the terminal and satellite connection. Click again to exit the status page.

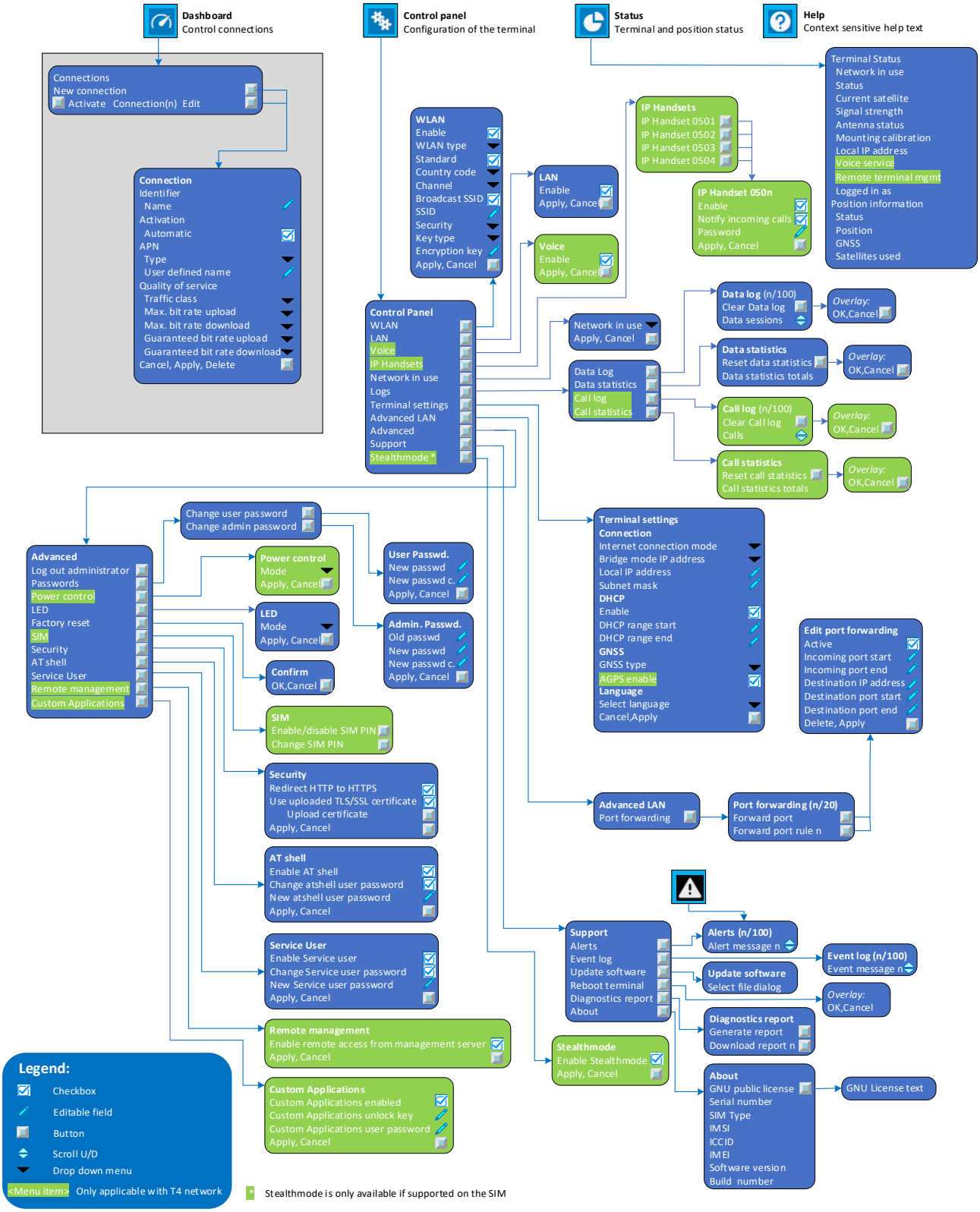
To navigate the web interface

- **To access status and settings**, tap or click the relevant icon in the icon bar or select to access the **Control panel**. The status or settings are displayed in the contents section.
- **To see your current location and to move back through the Control Panel menu**, use the breadcrumbs just below the icon bar.
- **To scroll through longer pages**, use the scroll bar or swipe.
- **To refresh the current page**, press Ctrl+F5 (PC) or Apple+R (Apple) or Cmd+R (Apple).

5.1.4 Menu tree for the web interface

The drawing below shows the menu structure of the Commander NEO web interface.

Note The green colored items are only available with T4-NGS.



5.2 To enter the SIM PIN in the web interface

Note You need a SIM to access the network. The SIM can be a physical SIM card inserted in the terminal or an eSIM which is embedded in the terminal.

5.2.1 Do you need a SIM PIN?

Note You may not have to enter a SIM PIN to access the terminal. This depends on whether or not the use of a SIM PIN is enabled on your SIM card.

The administrator can enable and disable the use of a SIM PIN. For details, see *To enable or disable the use of a SIM PIN* on page 5-27.

If a smartphone or computer is connected when you start up the terminal, you can access the web interface and enter the SIM PIN there.

5.2.2 To enter the SIM PIN

If your SIM card requires a PIN and the PIN has not yet been entered, you must enter it before you can make calls or access the external network. Until you have entered the PIN you cannot access the network, but you can still configure your terminal.

To enter the PIN, do as follows:

1. Access the web interface.
   If the terminal needs a PIN, a popup window tells you to enter PIN.
2. Type in your PIN and click **OK**.

When pointing is completed and the correct PIN is entered, you are ready to make calls or data sessions.

5.2.3 To cancel the SIM PIN

If you select **Cancel** when you are asked for a PIN, you can use the web interface as normal, but you will not be able to access the network to make calls or data sessions.

To enter the PIN later, after canceling the first time, do as follows:

1. From the icon bar at the top, click ⚠.
   The **Alerts** list opens.
2. Click **Resolve** next to **Enter PIN**.
3. Type in your PIN and click **OK**.

5.3 To control data connections from web interface

The main page of the web interface is used to start and stop data connections and to set up the data connections.

5.3.1 To start and stop data connections

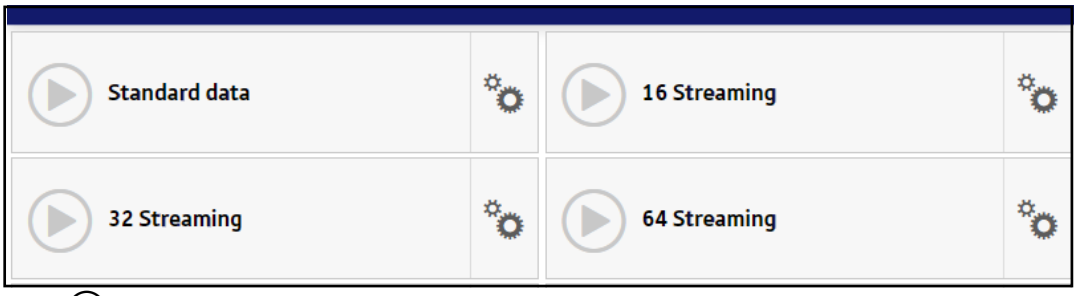
Note By default, if you want to use a data connection, you must manually start it from the web interface. However, you can set up the Commander NEO to automatically establish a data connection when you connect equipment to the LAN or WLAN interface. See *Enable Automatic Connection Activation* on page 5-9.

To start and stop data connections on your Commander NEO:

1. In the opening page, locate the connection you want to start.

   Note The icons for starting ▶ and stopping ■ connections are only active if the terminal is ready and registered on the satellite network. Otherwise you cannot start data connections.

   If a connection is automatically activated (has Automatic Activation enabled), the icons for starting and stopping are replaced by a lock symbol 🔒.



2. Click ▶ to start the connection. The connections icon at the bottom of the page shows 1 when a satellite data connection is running.

   Note With T4-NGS network, up to 8 Standard data connections or 3 Streaming connections at a time can be active.
   (only 1 connection with T2/T3)

3. Click ■ to stop the connection.

If the connection fails, the connection tile shows an exclamation mark ⓘ and an error message. The error message is also shown in the data log, see *Data log* on page 5-13.

When a connection is active, the icon changes to ■ and the tile for the active connection shows:

- IP address: The IP address that has been assigned by the service provider to this session.
- Transferred data: For Standard data, the tile shows the total amount of transmitted and received data since the connection was established.
- Connection duration: The tile shows the total time the connection has been active.
- Bit rate: For Streaming connections, the tile shows the fixed bit rate.

5.3.2 To change a connection

Available default connections

By default, the following connections are available:

Name	Type of connection
Standard data	Several users can share the data connection. This type of connection is ideal for TCP/IP traffic such as e-mail, file transfer, and Internet/intranet access. The user pays for the amount of data sent and received.
Streaming data The following default Streaming classes are available: **16, 32, 64, 128, 256, 384, 512, 768,** and **1024**[1] kbps Streaming (symmetric)	An exclusive, high-priority connection, ensuring seamless transfer of data. This type of connection is ideal for time critical applications like live video over IP. The user pays for the duration of the connection.

1. For T2/T3 network, the max Streaming rate is 384 kbps.

You can use these connections as they are, or build your own connections as described in the next section.

To customize connections

You access the connections from the Dashboard.

1. To access the Dashboard click at the bottom of the page.
2. To change a connection, click in the right side of the tile with the connection.

Note You must be logged in as administrator in order to change, delete or create connections.

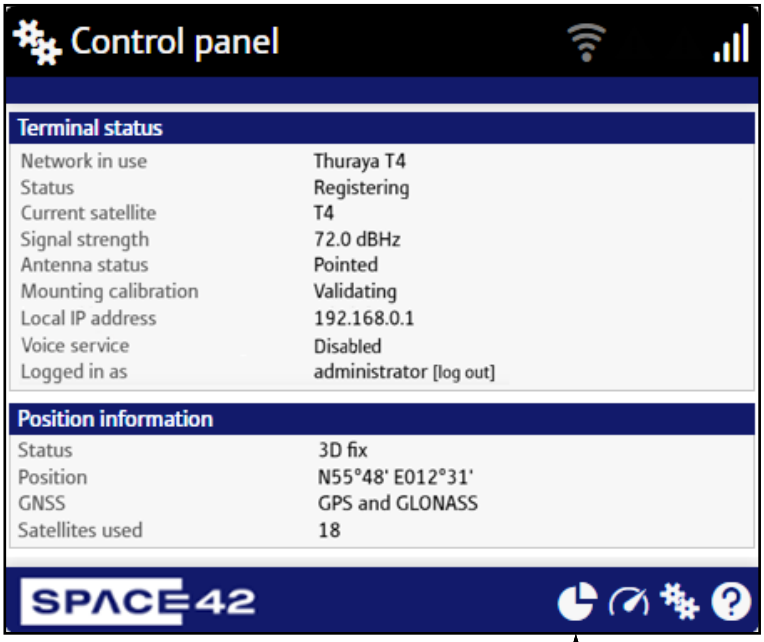
You have the following options to change a connection:

If you want to	Do the following
Change the name of the connection	Under **Identifier**, type in the new name and click **Apply**. The new name is shown on the tile on the startup page.
Enable Automatic Connection Activation	At **Activation**, select **Automatic**. • When you select **Automatic** at **Activation** and connect to the LAN or WLAN interface, the data connection is automatically established as soon as the Commander NEO is registered on the satellite network. • When you **disable** automatic activation (default), you can control the data connection manually from the startup page.
Change the APN for the connection	By default a connection is set to use the APN (Access Point Name) from the terminal (defined by Thuraya). This is suitable for most applications. If you want to use a different APN: 1. Under **APN**, select the Type of the APN. • **Default** (default and recommended setting): The APN is taken from the terminal (defined by Thuraya). • **User defined**: Type in the APN next to **User defined name**. The Airtime Provider provides the APNs. 2. Click **Apply**.
Change the Quality of Service	1. Under **Quality of service**, Select the **Traffic class** from the dropdown list. • **Standard**. A shared background connection used e.g. for TCP/IP traffic such as e-mail, file transfer, and Internet/ intranet access. • **Streaming**: An exclusive, high-priority connection, ensuring seamless transfer of data. This type of connection is ideal for e.g. live video over IP. 2. If you selected Streaming, select the Max. upload bit rate, Max. download bit rate, guaranteed upload bit rate and guaranteed download bit rate for the streaming connection. 3. Click **Apply**.
Delete a connection	Click **Delete**[1] at the bottom of the page. Note: you cannot delete the default **Standard** connection.

1. If you accidentally delete a connection, you can either create a new manually or restore factory settings. Note, however, that all changes to the configuration will be lost if you restore factory settings.

5.4 Status information

If the window is large enough, it shows a status field at the bottom of the page or in the right side of the page. If not, click at the bottom of the page to show the status page. Click again to return to the previous page.



The following status is available:

Terminal status:

- Network in use: The network currently used.
- Status: The status of the satellite network. Data means a data connection is running. The status could also be e.g. Registering or Ready.
- Current satellite: The satellite to which the Commander NEO is currently registered.
- Signal strength: The signal strength of the satellite connection.
- Antenna status: The status of the antenna, e.g. Tracking.
- Mounting calibration: The status of the calibration process that detects how the Commander NEO is oriented in relation to the vehicle. Can be Calibrating, Validating or Completed. For details, see *Mounting calibration* on page 3-10.
- Local IP address: The local IP address of the Commander NEO. E.g. used to connect to the web interface.
- Voice service[1]: The status of the voice service, e.g. Disabled, Not registered, Registered.
- Remote terminal management: The status of Remote terminal management, e.g. Disabled, Registered or Not ready.
- Logged in as: This field shows if you are logged in as administrator or user. You can click [log out] to log out.

Position information:

- Status: Shows the status of the GNSS, e.g. if there is 2D fix, 3D fix or no position fix.
- Position and GNSS: The geographic position of the Commander NEO and the position system used.
- Satellites used: Shows how many GNSS satellites are used to obtain the position.

1. Voice is only supported when connected to T4-NGS network.

Data information (only shown if a data connection is running).

- Standard data (or other connection name): Shows which type of data is running within the connection. For details on connections, see *To control data connections from web interface* on page 5-7.

Call information (only shown if a voice call is ongoing)

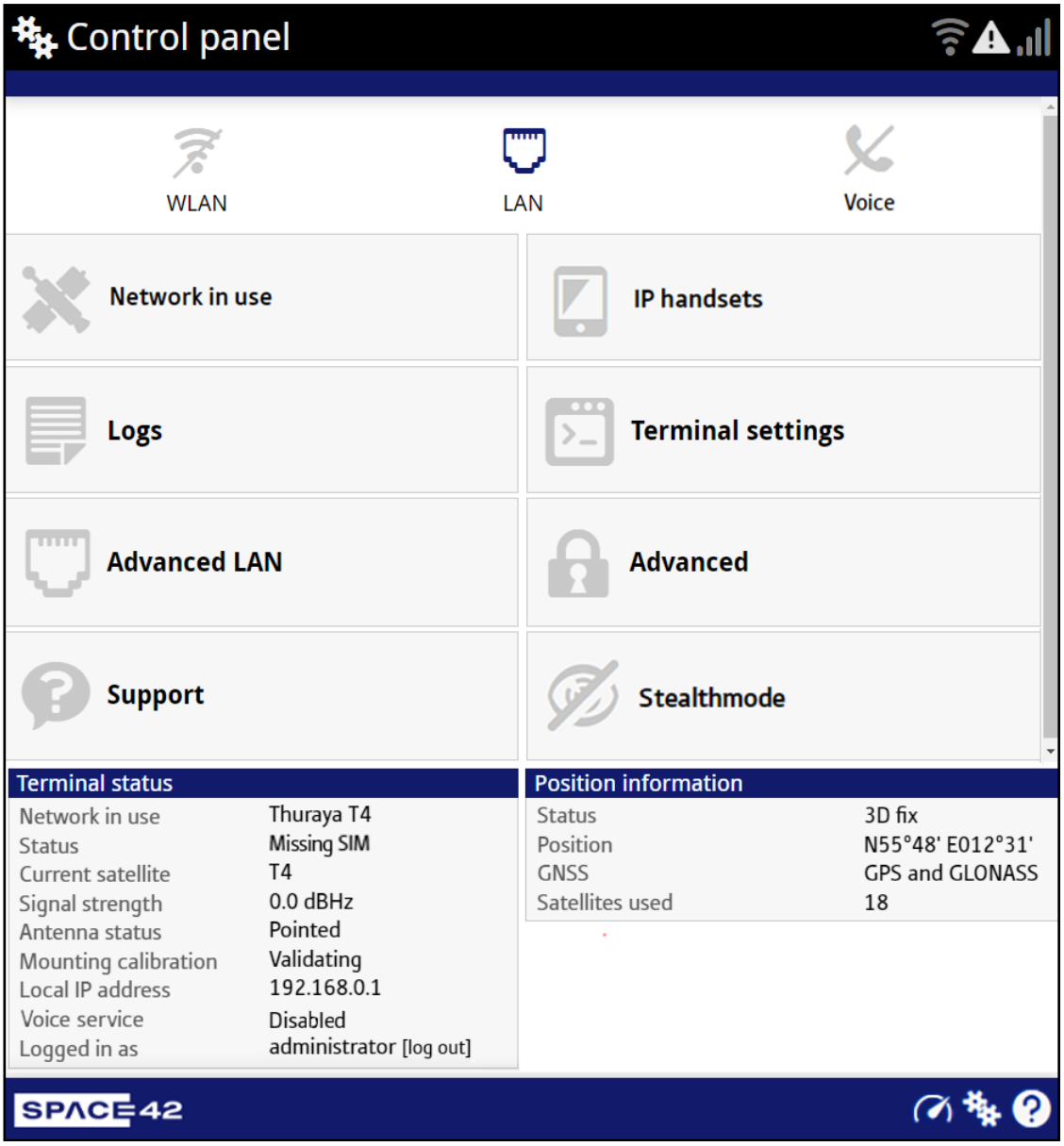
- Status: The status of the call, e.g. Connected or Ringing....
- Call duration: The duration of the call.
- Originator: The phone number from which the call was made.
- Receiver: The phone number that receives the call.

5.5 The Control panel

The **Control panel** is used for accessing settings and functions of your Commander NEO.

To open the **Control panel**, click from the bottom right corner of the web interface.

Note Some functions (e.g. Voice) are only available when T4-NGS network is selected. Also, Stealth mode is only shown and available if supported by the SIM.



5.6 To select the satellite network

The Commander NEO supports the T2/T3 network and the newer T4-NGS network (available fall 2025).

Note Some of the features described in this manual, e.g. all voice related features, are only available with T4-NGS network.

To select the network to use from your Commander NEO:

1. From the **Control panel**, select **Network in use**.
2. Select the network you are going to use and click **Apply**. You can select **Thuraya T4** or **Thuraya T2/T3**.

   Note The terminal will reboot when you change the network.

3. Click **Apply**.

The terminal reboots and starts up with the features of the selected network enabled.

5.7 To activate Stealth mode

If Stealth mode is supported by the SIM, you can put the Commander NEO in Stealth mode. When the Commander NEO is in Stealth mode, **WLAN, LEDs and system sounds are disabled**. To activate Stealth mode:

1. From the **Control panel**, click the **Stealthmode** tile.
2. Select **Enable Stealthmode** and click **Apply**.
   When Stealth is activated, the tile image is red, and a red Stealth icon appears in the status bar at the top of the page.
3. To **exit** Stealth mode, click the **Stealthmode** tile again, remove the checkmark and click **Apply**. The text and image on the tile becomes gray and the Stealth icon disappears from the status line at the top.

5.8 To use the logs

5.8.1 To access the logs

To access the Logs, select and select **Logs** from the menu. The Logs page contains:

- **Call log**[1]: A list of all incoming, outgoing and missed calls since the log was last cleared.
- **Data log:** A list of all data sessions since the log was last cleared.
- **Call statistics**[1]**:** Totals (number of calls and duration) for calls since the log was last cleared.
- **Data statistics**: Totals (amount of data or duration) for data since the log was last cleared.

Date and time is the international UTC time, received from the satellite.

5.8.2 Call log

The Call log[1] shows:

- **Outgoing calls** shows the start time, receiving end phone number and duration.
- **Received calls** shows the start time, calling phone number and duration of each incoming call.
- **Missed calls** shows the start time and calling phone number of each incoming call that was not received.

The Call log also shows the termination cause for failed calls. For a list of possible cause codes, see *List of VoLTE cause codes* on page 6-20.
To clear the Call log, click the **Clear call log** button at the top.

5.8.3 Data log

The Data log shows:

- Data usage (bytes), date and time of each Standard data session.
- Duration and type (such as 64 kbps, 128 kbps), date and time of each Streaming data session.

If the connection terminates unexpectedly or cannot be started, the Data log also shows the termination cause of each data session. For a list of possible cause codes, see *List of Connection cause codes* on page 6-15.

To clear the Data log, click the **Clear data log** button at the top.

5.8.4 Statistics for calls and data sessions

- **Call statistics**[1] shows the number of incoming, outgoing and missed calls and the total duration (hh:mm:ss) of incoming and outgoing calls since the log was last cleared.
  To reset the statistics counter, click the **Reset call statistics** button at the top.
- **Data statistics** shows totals for each data connection type since the log was last cleared. For Standard data the totals are shown as amount of data transferred (kB) and for Streaming connections the totals are shown in duration (hh:mm:ss).
  To reset the statistics counter, click the **Reset data statistics** button at the top.

1. Voice is only supported with T4-NGS network.

5.9 To set up the interfaces

5.9.1 LAN interface setup

The Commander NEO has one LAN interface with PoE in (which can be used for powering the Commander NEO, if a separate DC supply is not used).

To enable or disable the LAN interface:

1. In the **Control panel**, click the **LAN** icon at the top of the page.
2. To enable the LAN interface, select **Enable** (default enabled).

Important If you disable LAN you may not be able to access the Commander NEO. Before disabling the LAN interface, make sure you have a working WLAN connection.

You can restore the LAN and WLAN settings with the Reset button, see *Restore the settings of the Commander NEO* on page 6-4.

Note It may take some seconds to enable the interface.

3. Click **Apply**.
   - A line through a grayed-out **LAN** icon means the interface is **disabled**.
   - A blue **LAN** icon means the interface is **enabled**.

For a description of how to set up the **local network parameters**, see *Internet and LAN connection modes* on page 5-20 and *Advanced LAN* on page 5-23.

5.9.2 WLAN interface setup

Note The network settings entered in the Terminal settings page also apply for the WLAN interface. See *Internet and LAN connection modes* on page 5-20.

To configure the WLAN interface:

1. In the **Control panel**, click the **WLAN** icon at the top of the page.
2. To enable the WLAN interface, select **Enable**. (default disabled)

Important If you disable WLAN you may not be able to access the Commander NEO. Before disabling the WLAN interface, make sure you have a working LAN connection.

You can restore the LAN and WLAN settings with the Reset button, see *Restore the settings of the Commander NEO* on page 6-4.

Note It may take some seconds to enable the interface.

3. Select the **WLAN type**, 2.4 GHz (default) or 5 GHz.
   - Select 5 GHz for faster connection, if the connected equipment supports it.
   - Select 2.4 GHz if your connected equipment does not support 5 GHz.
4. Select the WLAN standard to use (all disabled by default).
   For 2.4 GHz, select **802.11n** if your equipment supports it. Otherwise deselect it.
   For 5 GHz, select **802.11n** or **802.11ac** or nothing, depending on your equipment.

5. Next to **Country code**, select the country you are located in (default is AE).

   Note In some countries, the use of WLAN is not allowed. Before continuing, make sure WLAN is allowed and licensed in the country where you intend to use it.

   Note If the Commander NEO is sold and used in the US, the country will be fixed and **not selectable**.

6. Select the **Channel** number used for communication on the WLAN interface.
   For **automatic channel selection** between the legal channels in the selected country, select channel number **0** (default selected).
7. Select **Broadcast SSID** to show your WLAN access point to other users (default selected).
   If you **clear** the box, your WLAN access point is hidden.
8. Type in the **SSID**.
   The SSID is a max. 32 character text identifying the wireless local area network. All wireless devices on a WLAN must use the same SSID in order to communicate with each other. The default SSID is the product name followed by underscore (_) and the last 4 digits in the serial number (**Commander-NEO_**<last 4 digits of serial number>).
9. Select the **Security** standard. You may select:
   - None (no encryption is applied), or
   - WPA2-AES (selected by default)
10. Next to **Key type**, select **Hexadecimal** or **Text**.
    The encryption key must normally be a hexadecimal code. However, if you are using WPA2-AES encryption (default) you can choose to use a text string, which may be easier to memorize. **Text** is selected by default.
11. Type in the **Encryption key** for the selected Security standard (not applicable if security mode = None). The default encryption key is the **serial number** of the Commander NEO. You can find the serial number under **Control panel** > **Support** > **About** or on the label on the Commander NEO.

    Important Change the encryption key to a personal code in order to keep your WLAN connection secure and protected!

12. Click **Apply**.
    -  A line through a grayed-out **WLAN** icon means the interface is **disabled**.
    -  A blue **WLAN** icon means the interface is **enabled**.

For a description of how to set up the **local network parameters**, see *Internet and LAN connection modes* on page 5-20 and *Advanced LAN* on page 5-23.

5.10 Voice setup[1]

Your smartphone or IP handset can be set up to make and receive calls over the satellite network, using the terminal's phone number.

For details, see *To enable phone calls over satellite* on page 3-11. This section describes the voice configuration of the Commander NEO terminal in the web interface.

To enable the voice service in your Commander NEO:

1. In the **Control panel**, click the **Voice** icon at the top of the page.
2. To enable the use of the Voice service, select **Voice service enabled**.
3. Click **Apply**.
   - A line through a grayed-out **Voice** icon means the voice service is **disabled**.
   - A **blue Voice** icon means the interface is **enabled**.

Note When **Voice service** in the **Terminal Status** field changes to **Registered**, the Voice service is ready for use.

5.10.1 To manage IP handsets[1]

This section describes how to manage IP handsets and smartphones connected to the Commander NEO.

The WLAN interface supports connection of up to 8 units (max. 4 phones). Each phone must have a local number in the range 0501 to 0504 as well as a unique password. For details, see the next section.

For details on SIP settings and how to connect your phone to the LAN or WLAN interface, see *To enable phone calls over satellite (only T4-NGS)* on page 2-18.

To manage phones in your Commander NEO

Do as follows:

1. Connect your phone to the terminal via LAN or WLAN. For details, see *To enable phone calls over satellite* on page 3-11.
2. In the web interface, select (**Control panel**) › **IP handsets**.
3. Click the tile for the handset number you want to manage.

   Note The handset number is also the **user name** for the handset.

4. Select **Enable** to enable the handset.

   Note It may take some seconds to enable the handset.

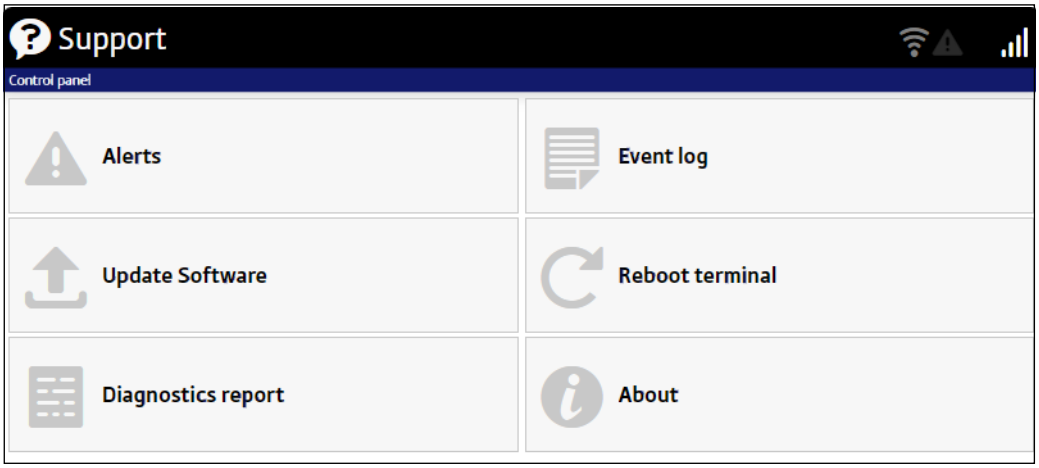
   - on the tile for your handset means the handset is disabled.
   - on the tile for your handset means the handset is enabled.
5. To change the **Password**, simply type in the new password.
6. Select whether or not the handset should **Notify incoming calls**.
7. Click **Apply**.
8. In your phone, enter the user name (local number) and the password you just entered in the Commander NEO. See the documentation for your phone for details.

The handset remains in the list after disconnecting. When the handset is connected again, it is automatically recognized and ready for use, if enabled.

1. Voice is only supported when connected to T4-NGS network.

5.11 Support features

To open the Support page, select (Control panel) > **Support.**



5.11.1 To view the Alerts

When an alert is registered, the web interface shows a warning icon in the icon bar as long as the alert is active. The **Alerts** list only shows alerts that are currently active.

1. To view the alerts, click from the icon bar at the top of the web interface, or select **Alerts** from the **Support** page.

The **Alerts** page shows a detailed list of active alerts including the time of the first occurrence, ID and severity of the alert message, and a short text describing the error. For more information on the alert messages, see *List of alert messages* on page 6-10.

5.11.2 To view the Event log

The Event log shows all events that have occurred. It includes events of informational character describing normal phases of operation for the terminal, and also activation and clearing of alerts that appear in the Alerts list.

To view the event log, select **Event log** from the **Support** page.

5.11.3 To create a diagnostics report

The diagnostic report contains relevant information for troubleshooting. When contacting your supplier for support, please enclose this file. To generate a diagnostic report:

1. From the **Support** page, click **Diagnostics report**.
2. Click **Generate report**.

Note | It may take a few minutes to generate the report.

3. Select **Download report**.
4. Choose a location for the file and save it on your connected device.

5.11.4 To update software

To update the software in the Commander NEO:

1. Download the new software or acquire the software from Thuraya and save it on your computer.
2. Open the web interface and enter the Control panel .
3. Click **Support** > **Update software**.
4. Click **Update software...**
5. Browse to the new software version and click **Open**. The software file has the extension ".tiif".
6. The terminal restarts and completes the software update.

> **Note** The update procedure takes some minutes to complete. During the software update, the Status LED is blinking blue.

You can check the software version under **Control panel** > **Support** > **About**.

See also *Over the Air software update (Only T4-NGS network)* on page 6-2 and *Recovery software update* on page 6-3.

5.11.5 To restart the terminal

If you want to restart the terminal:

1. From the **Support** page, select **Reboot terminal**.
2. Click to confirm the reboot.

The terminal restarts. Note that this is the equivalent to switching the terminal off and on again.

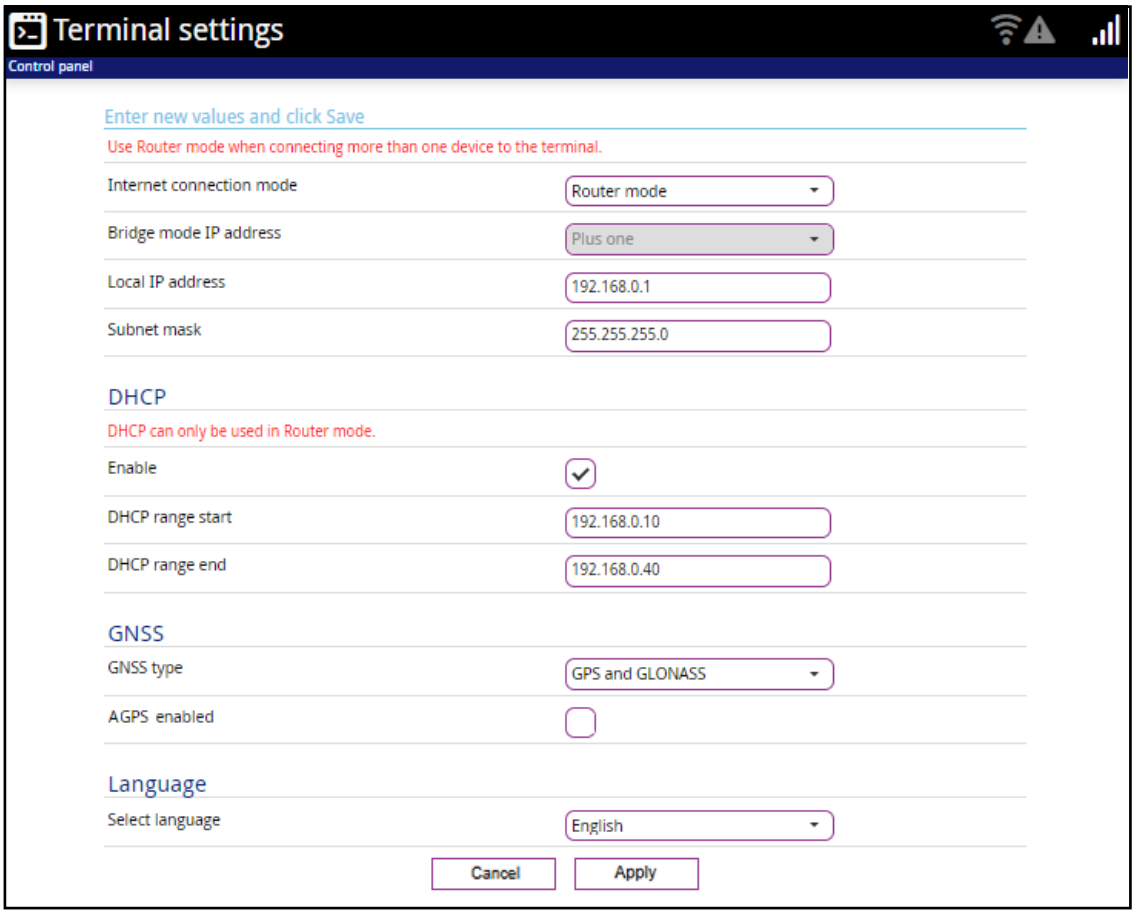
5.11.6 About

The **About** page shows the **Serial number**, **SIM type**, **IMSI number**, **ICCID**, **IMEI number** and **software version** of your Commander NEO.

To access the About page, select **Support** > **About**.

5.12 Terminal settings

To configure the terminal settings, select (Control panel) > **Terminal settings**.

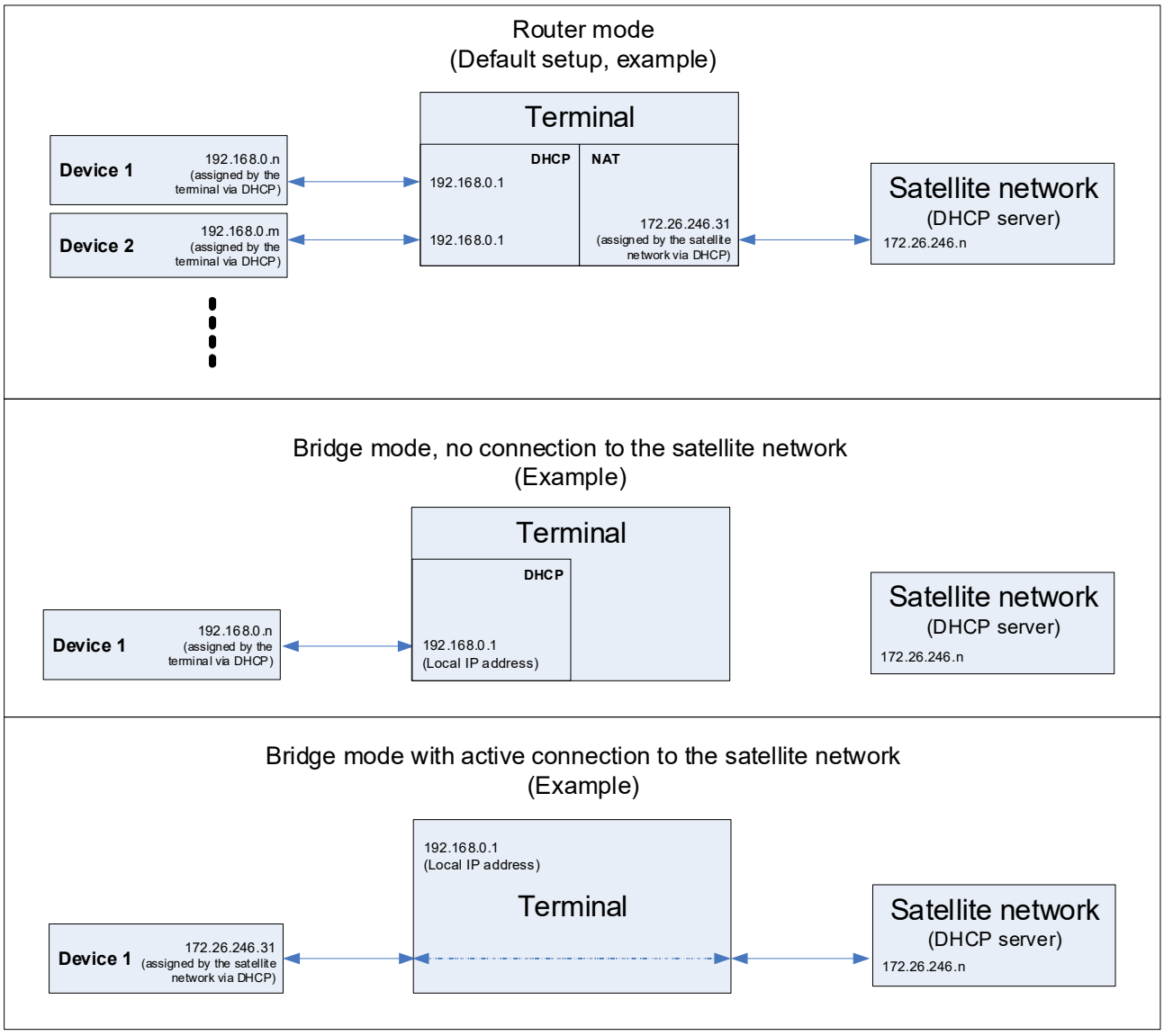


5.12.1 To set up the connection mode

Internet and LAN connection modes

In the web interface you can set up the Internet connection mode and the IP addressing between the Commander NEO and devices connected to the Commander NEO. The Commander NEO has a built-in DHCP server which can be used to dynamically assign IP addresses to devices connected to the Commander NEO.

The drawing below shows examples of the IP addressing in router mode (default setup) and Bridge mode.



To set up the Internet connection mode of the Commander NEO:

1. In the **Terminal settings** page, at **Internet connection mode**, select **Bridge mode** or **Router mode**. Router mode is the default setting and is recommended for most purposes.
   - Select **Router mode** if one or more computers are connected and the Commander NEO should act as a router. When Router mode is selected, the Commander NEO uses the built-in NAT module for making the necessary address translations.
   - Select **Bridge mode** if only one computer is connected, and the Commander NEO should act as a modem, or if more than one computer is connected using an external router.

   Note Do **not** connect more than one computer in Bridge mode, unless you have an external router.

2. If you selected **Bridge mode**, select under **Bridge mode IP address** how the terminal's IP address should be assigned.
   - **Dynamic** example: If the IP address assigned by the DHCP server to the locally connected equipment is 10.30.27.130, the terminal will get the IP address 10.40.27.130. (in most cases it will be 10 added to the second octet of the assigned IP address).
   - **Plus one** example (default): If the IP address assigned by the DHCP server to the locally connected equipment is 172.26.246.30, the terminal will get the IP address 172.26.246.31 (the assigned IP address plus one).
3. Under **Local IP address**, type in a new IP address if you want to change the Local IP address of the terminal. This is the address used to access the web interface. The default IP address is **192.168.0.1**.

   Important When you change the local IP address and click Apply you will no longer have access to the web interface! You must type in the new IP address in your browser to regain access.

4. If you want to change the **Subnet mask** for the local network of the terminal, type in the new network mask. The default network mask is **255.255.255.0**.
5. Under **DHCP,** select **Enable** (default and recommended for most purposes).[1]
   - If you select **Enable**, the terminal assigns dynamic IP addresses to devices connected to the terminal.
   - If you **disable DHCP** you need to set up a static IP address in the connected device.
6. Under **DHCP range start** and **DHCP range end**, type in the range of IP addresses that should be assigned to locally connected equipment.
7. Click **Apply**.

1. Note that if the Commander NEO is used with the Mobile Gateway M NEO, the DHCP server in the Commander NEO must be disabled and the local IP address of the Commander NEO must be the default IP address (192.168.0.1). See also the Mobile Gateway M NEO manual.

5.12.2 To select the type of navigation system (GNSS)

To select which navigation system(s) to use with your Commander NEO:

1. In the **Terminal settings** page, locate the **GNSS** section (Global Navigation Satellite System).
2. Select a navigation system, or combination of navigation systems, from the list.
   There are various combinations of GPS, GLONASS, Galileo and BeiDou. Default is **GPS and GLONASS**.
3. If you want to use Assisted GPS, select **AGPS enabled**.
4. Click **Apply**.

Note It may take some minutes for the Commander NEO to change the navigation system.

5.12.3 To select the language

The default language of the web interface is **English**. You can change the language to **Arabic, Chinese, French, Japanese, Portuguese, Russian** or **Spanish**.

To change the language:

1. In the **Terminal settings** page, locate the **Language** section.
2. Select a language from the list and click **Apply**.

5.13 Advanced LAN

5.13.1 Port forwarding

Note Make the port forwarding configuration before starting the data session.

Port forwarding enables you to set up a server connected to the terminal while the terminal is in Router mode. Without port forwarding it would not be possible to contact the server from the Internet. We recommend using a static public IP address for the terminal in order to provide easy access to the terminal. To use the static IP address, it must be included in your subscription and you must set the APN source to Default. For details, see *Change the APN for the connection* on page 5-9.

The following example shows how to allow Internet access to a mail server (smtp) connected to the terminal.

The mail server in this example has the IP address 192.167.0.100.

1. From the **Control panel** , select **Advanced LAN** > **Port forwarding**.
2. Select **Forward port** to add a new port forwarding.
3. Select **Active** to activate the port forwarding (default not active).
4. Type in the **Incoming port start** and the **Incoming port end**.
   This is the range of port numbers on the Commander NEO for which incoming traffic to the Commander NEO will be forwarded.
5. Type in the **Destination IP address**, which in this example is the IP address of the mail server: 192.167.0.100.
   This is the IP address to which the incoming traffic is forwarded.
6. Type in the **Destination port start** and the **Destination port end**.
   This is the range of port numbers, in this example on the mail server, to which the incoming traffic will be forwarded.
7. Click **Apply**.

When you have activated a data connection, you can now access the mail server from the Internet, using the external IP address of the terminal. You can see the external IP address in the tile with the data connection you have started. For information on how to activate your data connection, see *To start and stop data connections* on page 5-7.

5.14 Advanced settings

5.14.1 Passwords

The Commander NEO web interface is password protected at two levels: A user password and an administrator password. You will always be prompted for a password when you access the web interface. Default settings are[1]:

- **user**:
  User name: **user**
  Password: <empty>
- **administrator**:
  User name: **administrator**
  Password: <**serial number of the Commander NEO**>

You can change the passwords if you are logged in as administrator, see the next sections.

For details on the access rights on the different user levels, see *Access levels for the web interface* on page 5-2.

To log in as user

When you log in as user you cannot change the configuration, but you can see all settings, except the Advanced settings. You can also start and stop data connections.

You are prompted for user id and password when accessing the web interface.

1. At **User id**, type **user**.
2. At **Password**, type the user password (by default, the user password is empty).
3. Click **OK**.

To log in as administrator

To change the configuration or to access the Advanced settings you must enter an administrator password. To log in as administrator:

If you have not yet logged in, you are prompted for a password when accessing the web interface. When prompted:

1. At **User id**, type **administrator**.
2. At **Password**, type the administrator password (default: the serial number of the Commander NEO).
3. Click **OK**.

If you are already logged in as user:

1. From the Control panel , select **Advanced**.
   You are now prompted to log in as administrator.
2. Enter the administrator password.
3. Click **Login**.

Note After logging in with the default administrator password, you are forced to change the password, for security reasons.

1. If you have forgotten the password you can restore the terminal to factory default settings. Before doing so, be aware that all settings will be restored and you will lose any configuration you may have entered.

To log out as administrator

To log out, click **Log out administrator** in the **Advanced** page or click [log out] next to administrator in the **Terminal status** field.

To change the administrator password

To change the administrator password:

1. Log in as administrator.
2. Under **Advanced**, select **Passwords** > **Change administrator password**.
3. Type in the **Old password**.
4. Type in the **New password** and retype it on the next line.
   Rules for new password:
   - Minimum length: 4 characters
   - Maximum length: 50 characters
   - Valid characters: **0-9A-Za-z** and **`!$~@#%^&*()_=+[{}\|;:'.<>/?]-**
5. Click **Apply**.
   At the next login the new password is required.

To change the user password

To change the user password:

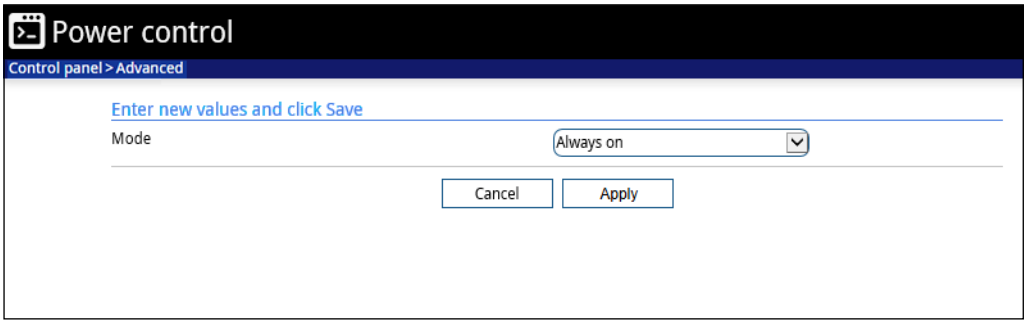
1. Log in as administrator.
2. Under **Advanced**, select **Passwords** > **Change user password**.
3. Type in the **User id (**default: **user)**.
4. Type in the **New password** and retype it on the next line.
   Rules for new password:
   - Minimum length: 0 characters
   - Maximum length: 50 characters
   - Valid characters: **0-9A-Za-z** and **`!$~@#%^&*()_=+[{}\|;:'.<>/?]-**
5. Click **Apply**.
   At the next login the new password is required.

5.14.2 Power control

You can use the Remote on/off function to save power in the Commander NEO.

To set up Remote on/off:

1. Under **Advanced**, select **Power control**.



2. Select the mode you want to use.
   - **Always on**. This is the default setting. The terminal will never go into power save state but will always be on when connected to power.
   - **Remote on/off**. The terminal will go into power save state when the Power control pin (Remote on/off signal) is inactive. For details see *Power mode functions* on page 4-8.

Important Be aware that once you have enabled the Remote on/off function, the Commander NEO will be in **power save state** until you have connected the blue Remote on/off wire **and** it is active! See *The Remote on/off signal (Power control pin)* on page 1-5.

If you selected Remote on/off:

3. At **Delayed shut down**, select the wanted shut-down delay after the power control pin is deactivated.
4. At **Power control pin** (Remote on/off), select the polarity of the power control signal (Active high/Active low).

Important If you are connecting the power control pin to ignition, you must select Active high, because the ignition signal in the vehicle is active high.

5. Click **Apply**.

5.14.3 To configure the LED mode

The LED is configurable in the web interface and can have 3 modes:

- **On for 5 minutes.** The LED stays on for 5 minutes after the terminal has started up and is ready (LED is constant green). After the 5 minutes the LED turns off, but will be turned on again if a warning or error occurs (yellow or red light). See *Status signaling* on page 6-8.
- **Always on:** The LED is always on when the terminal is powered.
- **Always off:** The LED is always off.

To change the LED mode, do as follows:

1. Under **Advanced**, select **LED**.
2. Select the mode and click **Apply**.

5.14.4 To restore factory settings

To restore the factory settings of the Commander NEO:

1. Under **Advanced**, select **Factory reset**.

   Important | All configuration will be lost and the Commander NEO will return to the default configuration.

2. Click **OK**.
   The terminal will now restart and start up with the factory settings.

5.14.5 SIM for satellite network

To select the SIM mode

There are two options for the SIM:

- A physical SIM card: Nano SIM card (4FF) from your Commander NEO supplier.
- An electronic SIM card: eSIM preinstalled in the terminal.

1. Under **Advanced**, select **SIM.**
2. Click **SIM Configuration**.
3. At **SIM Mode,** select the type of SIM you are going to use.
   - **uSIM**: A physical SIM card, inserted in the Commander NEO terminal.
   - **eSIM**: An electronic SIM preinstalled in the Commander NEO terminal.
   - **Automatic**: The Commander NEO terminal automatically detects whether you are using an uSIM or an eSIM.
4. Click **Apply**.

To enable or disable the use of a SIM PIN

To enable or disable the use of a PIN to access the satellite network, do as follows:

1. Under **Advanced**, select **SIM**.
2. Select **Enable/disable SIM PIN**.
3. Under **Enable/disable PIN** select or clear the box next to **Require PIN on startup**.
   - If you **clear** the box, you can access and use the terminal without entering a PIN.
   - If you **select** the box, you must enter a PIN on startup to be able to access the network.
4. If you selected **Require PIN on startup**, type in the PIN next to **Enter current PIN**.
5. Click **Apply**.
   The new PIN settings will take effect at next power on.

To change the SIM PIN

To change the PIN used to access the satellite network, do as follows:

1. Under **Advanced**, select **SIM**.
2. Select **Change SIM PIN**.
3. Under **Change PIN** type in the **Current PIN**.
4. Type in the **New PIN** and retype it on the next line.
5. Click **Apply**. The new PIN settings will take effect at next power on.

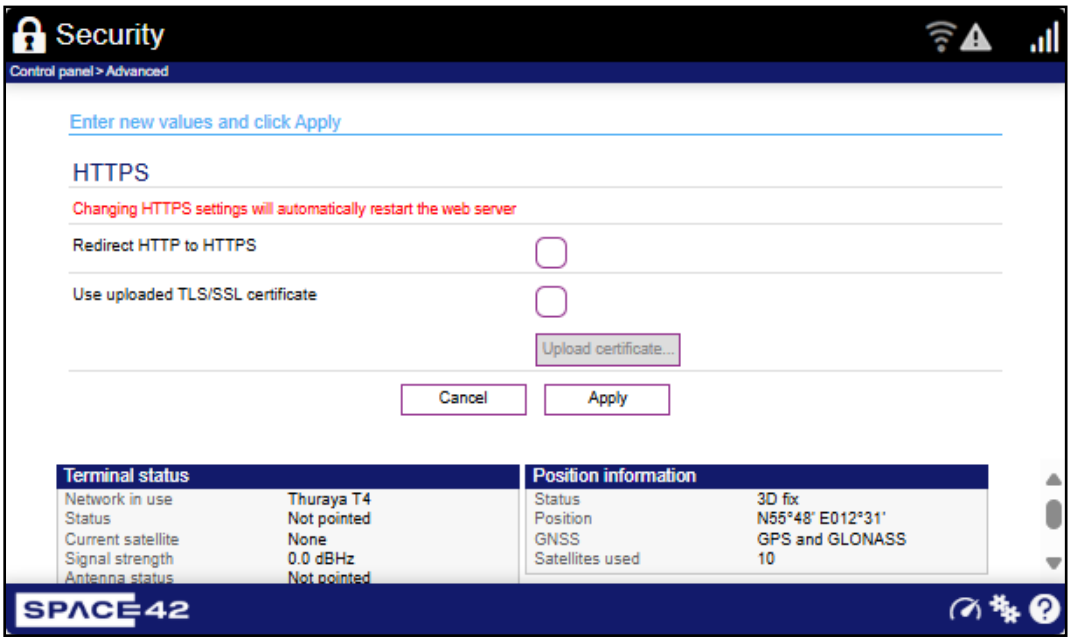
5.14.6 Security

HTTPS settings

The Commander NEO internal web server supports HTTPS, which includes encryption of the exchanged web traffic when accessing the Commander NEO web interface.

By default, the system uses a self-signed certificate, but it also allows you to upload your own certificate signed by a trusted Certificate Authority.

1. From the **Advanced** page select **Security**.

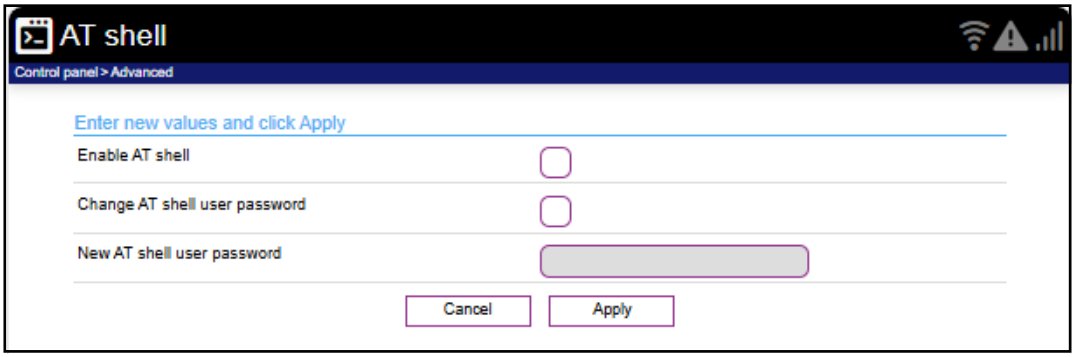


2. Select **Redirect HTTP to HTTPS** if you want the Commander NEO to automatically redirect your HTTP traffic to HTTPS (default not selected).
3. Select **Use uploaded TLS/SSL** certificate and click **Upload certificate** if you want to upload your own generated SSL certificate for the system to use (default not selected). Please note that the uploaded certificate file (.pem file format) must include the RSA private key used to generate the certificate:
   -----BEGIN CERTIFICATE-----
   ...
   ... <your certificate here> ...
   ...
   -----END CERTIFICATE-----
   -----BEGIN RSA PRIVATE KEY-----
   ...
   ... <your key here> ...
   ...
   -----END RSA PRIVATE KEY-----
4. Click **Apply**.

5.14.7 To set up AT shell

If you want to use AT commands with the terminal: To enable initial login on the AT shell, you must enable AT shell and define the password to use.

1. From the **Advanced** page select **AT shell**.



2. Select **Enable AT shell** if you want to use AT commands with the terminal.
3. To define the password for the AT shell, select **Change atshell user password** and type in the new password under **New atshell user password**.
   Rules for new password:
   - Minimum length: 4 characters
   - Maximum length: 50 characters
   - Valid characters: **0-9A-Za-z** and **`!$~@#%^&*()_=+[{}\|;:'.<>/?]-**
4. Click **Apply**.

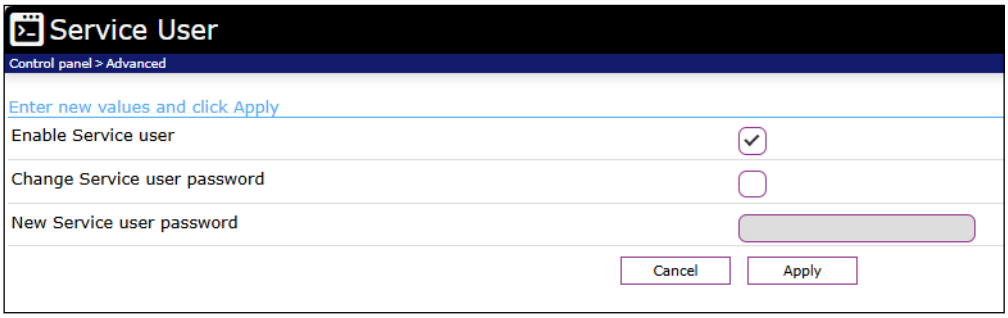
5.14.8 To set up a Service user account

The terminal includes a service user account that provides a series of advanced service-related commands and features for advanced users only.

When logged in via SSH using "service" as username, type "help" at the prompt to get a list of supported commands.

To set up the Service user account:

1. From the **Advanced** page select **Service User**.



2. Select **Enable Service user**, if you want to enable the Service user account for the terminal.
3. To define the password for the Service user, select **Change Service user password** and type in the new password under **New Service user password**.
   Rules for new password:
   - Minimum length: 4 characters
   - Maximum length: 50 characters
   - Valid characters: **0-9A-Za-z** and **`!$~@#%^&*()_=+[{}\|;:'.<>/?]-**
4. Click **Apply**.

5.14.9 To enable/disable remote management (only with T4-NGS)

With **Remote Terminal Manager (RTM)**, a remote operator can configure and manage several NEO terminals registered with the RTM service platform. To enable access to your Commander NEO terminal from the RTM:

1. From the **Advanced** page select **Remote management**.
2. Select **Enable remote access from management server**.
3. Click **Apply**.

The terminal now sets up a data connection reserved for remote management.This data connection is visible in the status section in the web interface (Data information field). Your Commander NEO terminal is now ready to be accessed, configured and managed from the RTM service platform. Note that the data connection for RTM can only be deactivated again by disabling **Remote access from management server** in the setting above.

5.14.10 To enable the use of custom applications in the terminal (only T4-NGS)

Contact your provider if you want to use 3rd party software with the terminal. To enable the use of your software in the terminal:

1. From the **Advanced** page select **Custom Applications**.
2. Select **Custom Applications enabled**.
3. Enter the **Custom Applications unlock key** received from your provider.
4. Enter the **Custom Applications user password**.
5. Click **Apply**.

Maintenance and troubleshooting

This chapter describes maintenance and troubleshooting. It has the following sections:

- *Support*
- *Software update*
- *Restore the settings of the Commander NEO*
- *Maintenance*
- *Troubleshooting*
- *Log files*

6.1 Support

6.1.1 To repack for shipment

Should you need to send the product for repair, please read the below information before packing the product.

The shipping carton has been carefully designed to protect the Commander NEO and its accessories during shipment. This carton and its associated packing material should be used when repacking for shipment. Attach a tag indicating the type of service required, return address, part number and full serial number. Mark the carton FRAGILE to ensure careful handling.

Note Correct shipment is the customer's own responsibility.

If the original shipping carton is not available, the following general instructions should be used for repacking with commercially available material.

1. Wrap the defective unit in heavy paper or plastic. Attach a tag indicating the type of service required, return address, part number and full serial number.
2. Use a strong shipping container, e.g. a double walled carton.
3. Protect the front- and rear panel with cardboard and insert a layer of shock-absorbing material between all surfaces of the equipment and the sides of the container.
4. Seal the shipping container securely.
5. Mark the shipping container FRAGILE to ensure careful handling.

Failure to do so may invalidate the warranty.

6.2 Software update

6.2.1 To update software with the web interface

1. Download the new software or acquire the software from Thuraya and save it to your computer.
2. Connect your computer to the Commander NEO.
3. Open the web interface in your browser and enter the Control panel.
4. Click **Support** › **Update software**.
5. Click **Update software...**
6. Browse to the new software version and click **Open**. The file has the extension ".tiif".
7. The Commander NEO now restarts and completes the software update.

You can check the software version under **Control panel** › **Support** › **About**.

Note The update procedure takes a couple of minutes.

6.2.2 Over the Air software update (Only T4-NGS network)

If you are registered on the T4-NGS network, you can update the Commander NEO software Over the Air via https.

Note If possible, connect external power to the terminal before starting the software update.

Over the Air software update is **only possible from an authorized Space42 server**.
There are two methods, depending on your configuration:

- RTM (Remote Terminal Management): The RTM operator can update the software in your Commander NEO from the Service Platform **Remote Terminal Manager**.

  Note Remote access must first be enabled in the Commander NEO web interface under **Control panel** › **Advanced** › **Remote management**.

- REST API
  Use the command sw/update/initiate and enter the url for the new software. For details, see the REST API documentation for the Commander NEO (doc. number *98-182365*) attached to this PDF file.

6.2.3 Recovery software update

If the Commander NEO becomes inoperative, a recovery software update may bring it back into an operational state.

Important The recovery software update will restore your Commander NEO configuration to factory default!

To make a recovery software update:

1. Acquire the new software and save it to your computer.
2. While powering on the Commander NEO, push and hold the **Reset** button until the **Status** LED is blinking rapidly blue, which means the Commander NEO is in **safe mode**. See *Restore the settings of the Commander NEO* on page 6-4.
3. Connect your computer with the new software to the Commander NEO.

   Note WLAN is not accessible when the Commander NEO is in safe mode.

4. On the connected computer, use **http** to access the web interface (https is **not supported** in safe mode). The web interface will open in a limited version that only supports updating software.
5. In the **Safe Mode** page, click **Choose file** and browse to the new software version on your computer and click **Open**. The file has the extension ".tiif".
6. Click **Upload** and wait for the upload to complete. **Do not** reload the web page during the file upload.
7. After successful upload, the new software is automatically installed.
8. The Commander NEO restarts and completes the software update.

   Note The update procedure can take up to 15 minutes.

9. Wait for the status LED to become steady green to indicate the software update process is completed.

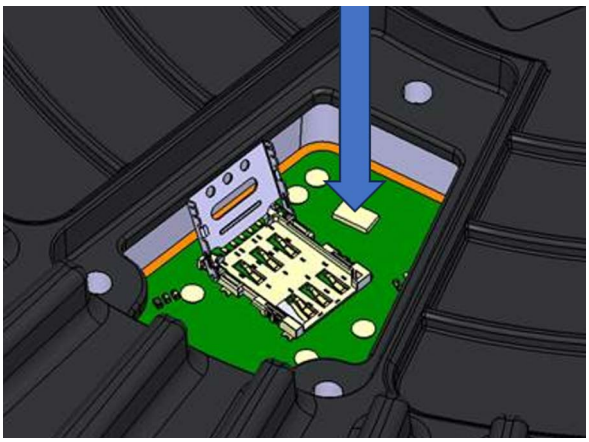
6.3 Restore the settings of the Commander NEO

The Commander NEO has a Reset button that has three functions: To restore all settings to factory settings, to restore WLAN settings and Local IP address only, and to put the Commander NEO into safe mode for recovery software update.

Action	Function
Push and hold the Reset button for 2-10 seconds	**LAN settings**: The terminal IP address and IP netmask are temporarily set to the default value (default IP address: 192.168.0.1). **WLAN settings** are restored to default. Default WLAN settings: • WLAN is **Disabled** • Broadcast SSID: **Commander-NEO_<last 4 digits of serial number>** • Encryption standard: **WPA2-AES** • Encryption key: **serial number** of the Commander NEO • Region: **AE**
Push and hold the Reset button for > 10 seconds	The Commander NEO restores factory settings and restarts the system. All changes to the configuration are lost.
Push and hold the Reset button while you switch on the Commander NEO.	The Commander NEO enters safe mode. The Status LED is blinking rapidly blue. In safe mode the Commander NEO is ready for a recovery software upload through the LAN interface (see *Recovery software update* on page 6-3).

The Reset button is located inside the SIM compartment in the bottom of the terminal.

Reset button



1. Loosen the three screws holding the cover for the SIM compartment.
2. Remove the cover.
3. Push the Reset button.
   The function depends on the length of time you hold the button, see the table above.
4. Close the cover and tighten the three screws carefully.
   This is important in order to maintain the IP grade of the Commander NEO.

6.4 Maintenance

6.4.1 Cleaning the Commander NEO

Clean the exterior of the Commander NEO with a damp cloth.

CAUTION! Do not spray water directly on the Commander NEO with high pressure! The Commander NEO can be washed gently, but it is not designed to be exposed to high pressure water-jets. The Commander NEO protection is IP68.

6.4.2 Disposal of the Commander NEO

Old electrical and electronic equipment marked with this symbol can contain substances hazardous to human beings and the environment. Never dispose these items together with unsorted municipal waste (household waste).

In order to protect the environment and ensure the correct recycling of old equipment as well as the re-utilization of individual components, use either public collection or private collection by the local supplier of old electrical and electronic equipment marked with this symbol.

Contact the local supplier for information about what type of return system to use.

Important This procedure is only for disposal of your terminal after dismantling it.

6.5 Troubleshooting

6.5.1 Troubleshooting guide

Problem	Possible cause	Remedy
The Commander NEO is not operational.	Software error	Restart the terminal. If the problem persists, you can restore factory settings as described in *Restore the settings of the Commander NEO* on page 6-4. **Note**: This will restore the configuration of your terminal to factory default!
The web interface Terminal status shows **Missing SIM**.	The SIM card is not present.	Switch off the Commander NEO and insert the SIM card in the SIM slot according to the instructions in this manual.
	The SIM card is not inserted properly.	Switch off the Commander NEO and remove the SIM card and re-insert it according to the instructions in this manual.
	The SIM card is invalid	Switch off the Commander NEO and replace the SIM card with a valid SIM card.
The web interface Terminal status shows **Scanning, Registering** or **Channel search** for more than a few minutes.	The Commander NEO cannot register on the satellite network.	Check your subscription with the Airtime Provider. Check that the signal strength is sufficient to register on the network (min. 45 dBHz) Check that your SIM card is valid for communication on the satellite network. Switch off the Commander NEO and remove and reinsert the SIM card.
No signal or weak signal from the satellite.	The view to the satellite is blocked.	Make sure the Commander NEO has a clear view to the satellite.
The Commander NEO cannot obtain its position using GNSS. The web interface Terminal status shows **Acquiring position**.	There is no GNSS signal, or the signal is weak. If the Commander NEO has not been used recently within the same location, it can take up to 10 minutes to obtain the position.	Check the position status in the web interface. To help the Commander NEO obtain position fix, it should be placed with a clear view to as much of the sky as possible.

Problem	Possible cause	Remedy
Connection to the Internet cannot be established.	The signal strength is too low.	Check the signal strength in the web interface. As a rule of thumb, you should have a signal strength of 45 dBHz or more to be able to make a call or data session.
The web interface cannot be accessed.	The browser is configured to use a proxy server.	For **Chrome**: select **Settings** › **System** › **Open you computer's proxy settings** and select **Off** at **Use a proxy server**.
	You have entered a wrong IP address.	Check the IP address and re-enter it. The default IP address is **192.168.0.1**
	The terminal has switched to DHCP client mode because a DHCP server is connected to the LAN/WLAN interface. This means the local IP address of the terminal has changed.	If connecting a DHCP server was a mistake, disconnect the unit or reconfigure it to be DHCP client. If the terminal is meant to act as a DHCP client, contact the administrator of the system.
A LAN connection cannot be established.	The cable is not properly connected.	Connect the cable.
	The cable type or connector type is not correct.	The LAN cable must be minimum Cat. 5E or 6A with an RJ45 connector. For more details, see the section *To connect cables* in this manual.
	The LAN interface is disabled.	Use the WLAN interface to access the web interface and enable the LAN interface by selecting **Control panel** › **LAN** › **Enable**. If both LAN and WLAN are disabled, restore factory settings as described in *Restore the settings of the Commander NEO* on page 6-4.

Problem	Possible cause	Remedy
A WLAN connection cannot be established.	The WLAN interface is disabled in the Commander NEO	Use the LAN interface to access the web interface and enable WLAN by selecting **Control panel** › **WLAN** › **Enable**. If both LAN and WLAN are disabled, restore factory settings as described in *Restore the settings of the Commander NEO* on page 6-4.
	Your computer or smartphone is placed too far away from the Commander NEO.	Bring the computer closer to the Commander NEO. Note that the listed max. distance is only valid under ideal conditions.

6.5.2 Status signaling

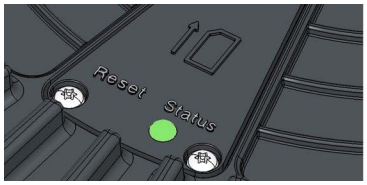
Means of signaling

The Commander NEO system provides two methods for signaling the status of the system.

- **Light indicator** on the bottom side of the Commander NEO.
- **Messages** shown in the web interface.

Light indicator

The LED is located in the cover for the SIM compartment in the bottom of the terminal.



The functions of the LED are:

Light pattern		Meaning
●	Green blinking rapidly	Starting up.
●	Yellow blinking	Antenna searching for satellite signal
●	Green blinking	Antenna tracking on satellite signal.
●	Green constant	Ready.
●	Yellow blinking rapidly	Closing down.
●	Yellow constant	Warning (user recoverable). See web interface for details.
●	Red constant	Error. See the web interface.
●	Blue blinking	Uploading software to the terminal.
●	Blue blinking rapidly	Safe mode.
○	Off	Power off or Power save state, or LED is configured to be **Always off** or **On for 5 minutes** (and the 5 minutes have passed).

The LED is configurable in the web interface and can have 3 modes:

- **On for 5 minutes**. The LED stays on for 5 minutes after the terminal has started up and is ready (LED is constant green). After the 5 minutes the LED turns off, but will be turned on again if a warning or error occurs (yellow or red light)
- **Always on**: The LED is always on when the terminal is powered.
- **Always off**: The LED is always off.

Alert messages and status messages

In the web interface of the Commander NEO you can see status messages and alerts that are currently active.

When a warning or error alert is active, the web interface shows a warning symbol ⚠. Select it to see a list of currently active alerts.

6.5.3 List of alert messages

The following list explains some of the alert messages that may show in the web interface of the Commander NEO.

Alert ID and Severity	Displayed text	Explanation	Remedy
8056 Warning	SIM rejected[1]	You have entered too many wrong PINs and PUKs, or The type of USIM card inserted in the terminal is not correct for your terminal, or PIN code validation is enabled on your SIM card.	Contact your airtime provider. Make sure you have the correct type of USIM card for your type of terminal. Contact your provider.
8057 Warning	SIM missing	No SIM is inserted in the terminal, or the SIM is not properly inserted	Insert the SIM card as shown in *To insert the SIM card* on page 2-2.
10150 Warning	Enter PIN[2]	A SIM PIN is required but has not been provided.	Enter the PIN as shown in *To enter the SIM PIN in the web interface* on page 5-6.
10151 Warning	Enter PUK[2]	A PUK code is required because the PIN has been blocked (too many failed attempts).	Enter the PUK in the web interface popup window.
10152 Error	SIM card blocked[2]	The SIM card is blocked, probably because of too many failed attempts.	Contact your provider.
10191 Warning	No position fix	The terminal was not able to get a position fix from the positioning system (GPS, GLONASS, Galileo or BeiDou).	It may take some time to obtain position fix. Make sure the terminal has a clear view to the sky. You can see position status in the status section in the web interface. If the problem persists, contact your provider.
10206 Warning	Closing terminal due to high temperature	The terminal has reached a critically high temperature, and will close down by itself.	Move the terminal to a cooler location.
10207 Warning	Terminal temperature too low	Low ambient temperature is causing the performance of the terminal to be degraded or halted.	Move the terminal to a warmer location. For information on ambient temperature limits, see the Specifications appendix.

Alert ID and Severity	Displayed text	Explanation	Remedy
10209 Warning	`Terminal temperature high`	The temperature in the terminal is high. If it continues to go up, it may affect the performance of the terminal negatively.	If possible, move the terminal to a cooler location.
10300 Warning	`Updating software...`	Software update has begun.	Wait for the software update to complete.
10302 Warning	`Preparing for software update`	Initial preparations for software upload are started.	Wait until preparations are over, either the terminal is rebooted or an error is shown.
10303 Warning	`Error opening software file`	The file requested to use for the update procedure cannot be opened or found.	Make sure the update file is correct and the file exists.
10305 Warning	`Software downgrade prevented. Use a newer software version.`	Not possible to perform a software downgrade, use a newer version.	Use a newer version of software for the update, or contact your provider.
10306 Warning	`File does not support this product`	The file used for software update does not support this terminal type.	Use the correct tiif file for your terminal.
10307 Warning	`File is corrupt. Download the file again.`	The file used for software update appears to be corrupt and the content cannot be validated.	Download the file again.
10308 Warning	`Software update failed. Try running the update again.`	Software upload failed to initialize, can be a sporadic issue.	Try running the update again. If the problem persists, contact your provider.
10309 Warning	`Software update failed. Update to the latest software version.`	The software has been rolled back to the version in use before starting this software upload. The new image was not validated correctly.	Try running the update again. If the problem persists, contact your provider.
1030A Error	`Software failed. Update to the latest software version from Safe Mode.`	Not all subunits have been properly verified with the new image.	Attempt software update procedure again. If not successful, update from Safe Mode as described in the section Recovery software update.
1030C Warning	`Software update is already started`	Another software update cycle is currently running.	Wait until the current software upload has finished.

Alert ID and Severity	Displayed text	Explanation	Remedy
1030D Warning	`Software version is already installed`	The software image you are trying to install is already active on the terminal.	Update with a different software image, or skip the update.
1030E Warning	`Software update forced roll-back`	Software update failed and the terminal forced a roll-back to the previous version.	Check that you have the correct file for software update and try again. If the problem persists, contact your provider.
18001 Warning	`Failed to read IMEI`	IMEI number is missing.	Contact you provider.
18002 Warning	`Illegal ME`	The satellite terminal used is not accepted by the network.	Contact your provider.
18003 Warning	`IMEI not accepted`	The satellite terminal used is not accepted by the network.	Contact your provider.
1812E Warning	`PLMN not allowed`	The terminal is not allowed to operate in the requested network.	Contact your provider.
1812F Warning	`Roaming not allowed`	It is not allowed to use the terminal on another operator's network.	Contact your provider.
18130 Warning	`IMSI unknown in HLR`	The SIM of the terminal (IMSI number) is unknown in Home Location Register	Contact your provider.
18131 Warning	`IMSI unknown in VLR`	The SIM of the terminal (IMSI number) is unknown in Visitor Location Register	Contact your provider.
18134 Warning	`Network detached mobile`	The terminal was detached by the network	Repoint the terminal. If not successful, switch the terminal off and then on again (power cycle). If the problem persists, contact your provider.
18135 Warning	`Data service not allowed`	The requested data service is not allowed.	If possible, use another data service. If the problem persists, contact your provider.
18136 Warning	`Service not allowed`	The requested service is not allowed.	If possible, use another service. If the problem persists, contact your provider.

Alert ID and Severity	Displayed text	Explanation	Remedy
18137 Warning	`Identity cannot be derived`	The identity of the terminal cannot be derived by the network.	Switch the terminal off and then on again (power cycle). If the problem persists, contact your provider.
18138 Warning	`Location area not allowed`	The terminal is not allowed to operate in this location area.	Switch the terminal off and then on again (power cycle). If the problem persists, contact your provider.
18139 Warning	`Temporary satellite registration failure`	The terminal is temporarily unable to register with the satellite network.	Wait for the terminal to retry. If not successful, repoint the terminal. If the problem persists, contact your provider.
1813A Warning	`General satellite registration failure`	The terminal is unable to register with the satellite network.	Contact your provider
1813B Warning	`Satellite registration retries exhausted`	The terminal has attempted to register too many times without success.	Repoint the terminal. If not successful, reboot the terminal. If the problem persists, contact your provider.
18191 Warning	`Satellite signal lost`	The system no longer receives a signal from the satellite.	Wait for the terminal to recover the signal. If not successful, repoint the terminal (Make sure the antenna has a clear view to the satellite). If the problem persists, contact your provider.
18194 Warning	`Old position`	The latest geographical position registered in the terminal is old and cannot be used to register on the satellite network.	Switch the terminal off and then on again (power cycle). Make sure the terminal has a clear view to the sky. You can see position status in the status section in the web interface. If the problem persists, contact your provider.
25800 Error	`Hardware fault detected`	A hardware fault related to the satellite connection is detected.	Contact your provider for repair.
2BC00 Error	`Hardware fault detected`	A general hardware fault is detected.	Contact your provider for repair.
2BE00 Error	`Missing calibration data`	Invalid calibration values found (satellite connection).	Contact your provider for repair.

Alert ID and Severity	Displayed text	Explanation	Remedy
2C100 Error	Temperature sensor hardware fault detected	There is a hardware fault with a temperature sensor.	Switch off the terminal and contact your provider for repair.
2C600 Error	Missing calibration data	Invalid calibration values found (satellite connection).	Contact your provider for repair.
2C700 Error	Hardware fault detected	A hardware fault related to the satellite connection is detected.	Contact your provider for repair.
2C800 Error	Hardware fault detected	A hardware fault related to the satellite connection is detected.	Contact your provider for repair.
2C900 Error	Hardware fault detected	A hardware fault related to the satellite connection is detected.	Contact your provider for repair.
2CA00 Error	Temperature sensor hardware fault detected	There is a hardware fault with a temperature sensor.	Switch off the terminal and contact your provider for repair.
2CB00 Error	Missing calibration data	Invalid calibration values found (related to satellite connection).	Switch the terminal of and then on again (power cycle). If the problem persists, contact your provider for repair.
2CD00 Error	Temperature sensor hardware fault detected	There is a hardware fault with a temperature sensor.	Switch off the terminal and contact your provider for repair.
2CE00 Error	Missing calibration data	Invalid calibration values found (related to satellite connection).	Switch the terminal of and then on again (power cycle). If the problem persists, contact your provider for repair.
38402 Error	Hardware fault detected	A general hardware fault is detected.	Contact your provider for repair.
38403 Error	Hardware fault detected	A general hardware fault is detected.	Contact your provider for repair.
38404 Error	WLAN hardware fault detected	A hardware fault with the WLAN module is detected.	Contact your provider for repair. **Note**: You can stiill use the terminal without WLAN.
38409 Error	Hardware fault detected	A general hardware fault is detected.	Contact your provider for repair.
3840A Error	Hardware fault detected	A general hardware fault is detected.	Contact your provider for repair.

Alert ID and Severity	Displayed text	Explanation	Remedy
38411 Error	`GNSS hardware fault detected`	There is a hardware fault with the GNSS module.	Contact your provider for repair.
38412 Error	`IMU hardware fault detected`	A hardware fault related to satellite tracking is detected	Contact your provider for repair.

1. This event only applies when connected to T2/T3 network.
2. This event only applies when connected to T4 network

6.5.4 List of Connection cause codes

The following list shows cause codes related to the external connection. These can appear on a connection tile in the web interface or in the logs, e.g., if there is a delay or an error occurs.

Connection cause code	Cause
0x01	Data or time limit exceeded
0x02	Automatic activation failed. Reconnecting...
0x03	Connection failed
0x04	Connection failed
0x05	Network failure
0x06	Connecting...
0x07	LAN disconnected
0x08	Connection failed
0x09	Connection closed. Temperature too high.
0x0a	Connection closed. Connection watchdog (Link monitoring) failure.
0x0b	Connection closed. Modify failed
0x0c	Terminal deregistered
0x2710	Unknown clearing
0x2711	Normal clearing
0x2712	Modem removed
0x2713	Stalled
0x2714	Timeout
0x2715	APN invalid
0x2716	Communication error
0x2717	Call cleared, reconnecting
0x2718	Connection hung up

Connection cause code	Cause
0x2719	Unspecified error
0x271a	Attach error
0x271b	Dial-up error
0x10000008	Operator Determined Barring
0x10000019	LLC or SNDCP failure
0x1000001a	Insufficient resources
0x1000001b	Missing or unknown APN
0x1000001c	Unknown PDP/PDN type
0x1000001d	User authentication failed
0x1000001e	Activation rejected by gateway
0x1000001f	Activation rejected, unspecified
0x10000020	Service option not supported
0x10000021	Requested service option not subscribed
0x10000022	Service option temporarily out of order
0x10000023	NSAPI/PTI already used
0x10000024	Normal deactivation
0x10000025	QoS not accepted
0x10000026	Activation rejected, Network failure
0x10000027	Reactivation requested
0x10000028	Feature not supported
0x10000029	Semantic error in the TFT operation
0x1000002a	Syntactical error in the TFT operation
0x1000002b	Unknown PDP context
0x1000002c	Semantic errors in packet filter(s)
0x1000002d	Syntactical errors in packet filter(s)
0x1000002e	PDP context without TFT already activated
0x1000002f	PTI mismatch
0x10000031	Last PDN disconnection not allowed
0x10000032	PDN type IPv4 only allowed
0x10000033	PDN type IPv6 only allowed
0x10000034	Single address bearers only allowed

Connection cause code	Cause
0x10000035	ESM information not received
0x10000036	PDN connection does not exist
0x10000037	Multiple PDN connections for a given APN not allowed
0x10000038	Collission with network initiated request
0x10000039	PDN type IPv4v6 only allowed
0x1000003a	PDN type non IP only allowed
0x1000003b	Unsupported QCI value
0x1000003c	Bearer handling not supported
0x10000041	Maximum number of EPS bearers reached
0x10000042	Requested APN not supported
0x10000051	Invalid PTI value
0x1000005f	Semantically incorrect message
0x10000060	Invalid mandatory information
0x10000061	Message type non-existent or not implemented
0x10000062	Message type not compatible with protocol state
0x10000063	Information element non-existent or not implemented
0x10000064	Conditional IE error
0x10000065	Message not compatible with protocol state
0x1000006f	Protocol error, unspecified
0x10000070	Incompatible APN restriction value
0x10000071	Multiple accesses to a PDN connection not allowed
0x10024002	Network failure IMSI unknown (HLR)
0x10024003	Network failure, Mobile Station illegal
0x10024006	Network failure, Mobile Equipment illegal
0x10024007	Attach reject, GPRS not allowed
0x10024008	Attach reject, services not allowed
0x10024009	Network failure, Mobile station id unknown
0x1002400a	Network failure, implicitly detached
0x1002400b	Network failure, PLMN not allowed
0x1002400c	Network failure, Location area not allowed
0x1002400d	Network failure, roaming not allowed at location

Connection cause code	Cause
0x1002400e	Network failure, no GPRS service allowed
0x1002400f	Network failure, no service at location
0x10024010	Network failure, service temporarily unreachable
0x10024100	Reject, unspecified
0x10024101	Reject, reattach required
0x10024102	Connection timeout
0x10024103	Reject, authentication failure
0x10024104	Reject, network invalid
0x10024105	Attach Reject, not allowed
0x10024106	Reject, normal detach
0x10024107	Attach reject, no IMSI
0x10024108	Attach reject, Service request denied
0x10024109	Attach reject, searching for PLMN
0x10034011	Network failure, PLMN failure
0x10034014	Authentication reject, MAC failure
0x10034015	Authentication reject, sync failure
0x10034016	Network failure, congestion
0x10034017	Authentication reject, GSM unacceptable
0x1003405f	Network error, detached
0x10034060	Network error, invalid mandatory info
0x10034061	Network error, message invalid
0x10034062	Network error, protocol state error
0x10034064	Network error, invalid conditional info
0x10034065	Network error, not compatible with protocol state
0x1003406f	Network error, unspecified protocol error
0x10040001	Reject, detaching
0x10040002	Timeout
0x10040003	PS attach rejected
0x10040004	Activation error, invalid
0x10040005	Re-activation timeout
0x10040008	Attach reject, timeout

Connection cause code	Cause
0x10040101	Normal deactivation (from Core Network)
0x10040102	Normal deactivation (power down or reboot)
0x10040103	Normal deactivation (PDP context removed)
0x10040107	Normal deactivation (AT command)
0x1004010b	Normal deactivation
0x1004010c	No response for PDN connectivity request
0x1004010d	No response for bearer modification request
0x1004010e	Preemption
0x1004010f	Missing on service resume
0x10051001	Attach reject, detaching
0x10051002	Attach reject, powerdown
0x10051003	Attach reject, domain blocked
0x10051004	Reject, missing PIN
0x10051005	Reject, no selected PLMN
0x10051006	Reject, PLMN forbidden
0x10051007	Reject, PLMN/GPRS not allowed
0x10086300	Establish Reject, normal
0x10086301	Establish Reject, Radio Network failure
0x10086302	Establish Reject, congestion
0x10086303	Establish Reject, unsupported IAI version
0x10086304	Establish Reject, unsupported UE class
0x10086305	Establish Reject, USIM required
0x10086306	Establish Reject, physical channel failure
0x10086307	Establish Reject, access Class not allowed
0x10086308	Establish Reject, unspecified
0x10086309	Conn. release, normal
0x1008630a	Conn. release, Radio Network security failure
0x1008630b	Conn. release, physical channel failure
0x1008630c	Conn. release, PLMN Search
0x1008630d	Conn. release, security command failure
0x10086314	Deregister, register with no complete

Connection cause code	Cause
0x10086315	Deregister, service area BARRED
0x10086316	Deregister, position required
0x10086317	Deregister, Core Network reset
0x10086318	Deregister, inactivity
0x10086319	Deregister, position response not received
0x1008631a	Deregister, position age expired
0x1008631b	Deregister, decryption error
0x1008631c	Deregister, user specified position not permitted
0x1008631d	Deregister, Radio Network initiated Deregistration
0x1008631e	Deregister, unknown cause
0x1008631f	Deregister, tracked SAT below minimum
0x10086320	Deregister, Lease Group not available
0x10086321	Deregister, Lease Mode handover failed
0x10086322	Deregister, Radio Failure
0x10086323	Deregister, Unsupported UE subclass
0x10086324	Deregister, Elevation too low
0x10086325	Deregister, Protocol Failure
0x10086326	Deregister, Invalid UE capabilities

6.5.5 List of VoLTE cause codes

The following list shows cause codes that can appear in the **call log**, e.g., to explain the cause of a failed call.

VoLTE cause code	Cause
0x00	Disconnect, not specified
0x01	Unassigned number
0x02	No route to network
0x03	No route to destination
0x06	Channel unacceptable
0x07	Call awarded
0x08	Operator barring
0x10	Hangup
0x11	Busy

VoLTE cause code	Cause
0x12	No response
0x13	No answer
0x15	Call rejected
0x16	Number changed
0x19	Pre-emption
0x1A	Core Network failure
0x1B	Core Network failure
0x1C	Invalid number
0x1F	Normal, unspecified
0x22	Call Rejected, no channel/circuit
0x29	Temporary failure
0x2C	Phone channel not available
0x42	Channel type not implemented
0x66	Network timeout, no answer
0x6F	Unspecified protocol error
0x00034002	Network failure IMSI unknown (HLR)
0x00034003	Network failure, Mobile Station illegal
0x00034004	Network failure IMSI unknown (VLR)
0x00034006	Network failure, Mobile Equipment illegal
0x0003400b	Network failure, PLMN not allowed
0x0003400c	Network failure, Location area not allowed
0x0003400d	Network failure, roaming not allowed at location
0x0003400f	Network failure, no service at location
0x00034011	Network failure, PLMN failure
0x00034014	Authentication reject, MAC failure
0x00034015	Authentication reject, sync failure
0x00034016	Network failure, congestion
0x00034017	Authentication reject, GSM unacceptable
0x00034020	Service option rejected, not supported
0x00034022	Service option rejected, temporarily out of order
0x00034026	Network failure, call cannot be identified
0x00034030	Network failure, retry upon entry to new cell
0x0003405f	Network error, detached

VoLTE cause code	Cause
0x00034060	Network error, invalid mandatory info
0x00034061	Network error, message invalid
0x00034062	Network error, protocol state error
0x00034064	Network error, invalid conditional info
0x00034065	Network error, not compatible with protocol state
0x0003406f	Network error, unspecified protocol error
0x00034100	Reject, normal
0x00034101	Reject, unspecified
0x00034102	Connection timeout
0x00034103	Reject, no IMSI
0x00034104	Reject, limited Service
0x00034105	Reject, access class not allowed
0x00034106	Reject, connection not idle
0x00034107	Reject, no cell or Radio Network
0x00034108	Reject, authentication failure active conn.
0x00034109	Reject, authentication failure
0x00040102	Power down or reboot
0x00051001	Attach reject, detaching
0x00051002	Attach reject, powerdown
0x00051003	Attach reject, domain blocked
0x00051004	Reject, missing pin
0x00051005	Reject, no selected PLMN
0x00051006	Reject, PLMN forbidden
0x00051007	Reject, PLMN/GPRS not allowed
0x00086400	Establish Reject, normal
0x00086401	Establish Reject, Radio Network failure
0x00086402	Establish Reject, congestion
0x00086403	Establish Reject, unsupported IAI version
0x00086404	Establish Reject, unsupported UE class
0x00086405	Establish Reject, USIM required
0x00086406	Establish Reject, physical channel failure
0x00086407	Establish Reject, access Class not allowed
0x00086408	Establish Reject, unspecified

VoLTE cause code	Cause
0x00086409	Conn. release, normal
0x0008640a	Conn. release, Radio Network security failure
0x0008640b	Conn. release, physical channel failure
0x0008640c	Conn. release, PLMN Search
0x0008640d	Conn. release, security command failure
0x0008641e	Deregister, unknown cause
0x00086414	Deregister, register with no complete
0x00086415	Deregister, service area BARRED
0x00086416	Deregister, position required
0x00086417	Deregister, Core Network reset
0x00086418	Deregister, inactivity
0x00086419	Deregister, position response not received
0x0008641a	Deregister, position age expired
0x0008641b	Deregister, decryption error
0x0008641c	Deregister, user specified position not permitted
0x0008641d	Deregister, Radio Network initiated Deregistration
0x0008641f	Deregister, tracked SAT below minimum
0x00086420	Deregister, Lease Group not available
0x00086421	Deregister, Lease Mode handover failed
0x00086422	Deregister, Radio Failure
0x00086423	Deregister, Unsupported UE subclass
0x00086424	Deregister, Elevation too low
0x00086425	Deregister, Protocol Failure
0x00086426	Deregister, Invalid UE capabilities
0x00134166	Call Rejected, no channel
0x00134366	Call Rejected, no response from network
0x00134a66	Call disconnect, no response from network
0x00134d66	Call Release, no response from network

6.6 Log files

6.6.1 To create a diagnostics report

The diagnostic report contains relevant information for troubleshooting. When contacting your supplier for support, please enclose this file. To generate a diagnostic report, access the web interface and select (Control panel) › **Support** › **Diagnostics report**. See *To create a diagnostics report* on page 5-17).

Note | It may take a few minutes to generate the report.

If you are using the PRISM Lite service, you can also generate a diagnostics report from the PRISM PTT+ Portal.

6.6.2 Call log[1] and Data log

The log holds detailed information on each call or data session to and from the Commander NEO, including date and time, phone numbers, duration, amount of data transferred etc.

Date and time is UTC time, received from the satellite.

To see the log in the web interface, select (Control panel) › **Logs**. See *To use the logs* on page 5-13.

6.6.3 Event log

The Event log shows events that occurred in the past and are no longer active. It includes events of informational character describing normal phases of operation for the terminal, and also alerts that have appeared in the Alerts list.

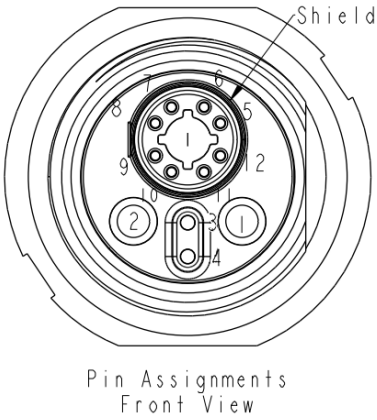
To view the event log in the web interface, select **Event log** from the **Support** page.

1. Calls are only supported when connected to T4-NGS network.

Specifications

A.1 Commander NEO terminal

A.1.1 General specifications

Characteristics	Specification
Type	Vehicular one-box satellite terminal with integrated beam steering antenna (no moving parts).
Services Voice Data Standard IP Streaming IP	 4 kbps AMBE+2 Up to 1 Mbps 16, 32, 64, 128, 256, 384, 512, 768 or 1024 kbps, symmetric or asymmetric up/down
Interfaces Wired  Pin Assignments Front View Wireless	 One combined connector with: • DC power input, 12-24 VDC nominal (MIL-STD 1275 28 Vnom) max. range 10.8 to 33.6 VDC (pin 1 and 2) • Remote on/off signal (pin 3) • Ethernet PoE (input) interface, T568B,10/100/1000 Mbps, PoE Type 4/ Class 8 (pin 5 to 12) See *WLAN access point* on page A-2.
Frequencies Transmit Receive	 1626.5 - 1660.5 MHz 1518.0 MHz - 1559.0 MHz
G/T	≥-18.5 dB/K, for elevations between 20° and 90° ≥-19 dB/K, for elevations between 5° and 20°
EIRP	Max. 15 dBW

Characteristics	Specification
Dimensions	Diameter: 320 mm Height: 117 mm incl. 30 mm plastic spacers (93.5 mm without spacers)
Weight	4800 g / 10.6 lbs including spacers
Mounting	With 3 bolts through the vehicle roof, or Optional: Magnetic Mount Solution, order number 403723B-009 (3 magnetic feet)[1]
Altitude during operation	Maximum 2000 m
Supply Voltage	**DC input**: 12 VDC to 24 VDC (MIL-STD 1275 28 Vnom). Max range for Commander NEO: 10.8 VDC to 33.6 VDC **PoE In:** A PoE supplying device used with the Commander NEO must comply with minimum Type 4 Class 8 (IEEE802.3bt), capable of supplying 52-57 VDC, 90 W.
Supported MIL standards	MIL-STD-810 MIL-STD-463 MIL-STD-901 MIL-STD-1275

1. Note that the magnetic mounts **do not provide 30 mm distance** between the terminal bottom and the mounting surface. This means there may not be sufficient airflow to keep the terminal operational in case of very high ambient temperatures.

A.1.2 WLAN access point

Characteristics	Specification
Standard	IEEE 802.11
Antenna	Built-in
Frequencies Country selection dependent	2.412 - 2.472 MHz (EU) 2.412 - 2.462 MHz (US) 5.180 - 5.240 MHz 5.260 - 5.320 MHz 5.500 - 5.700 MHz 5.600 - 5.650 MHz (special DFS requirements) 5.735 - 5.825 MHz
Bandwidth	Max. 20 MHz, 40 MHz, 80 MHz
Modes	IEEE 802.11b/g/a/n/ac HT20/HT40/HT80
DFS frequencies	Operation as slave device supported

A.1.3 Environmental specifications

Characteristics	Specification
Water and dust	IP68 with SIM cover and recommended connector housing mounted correctly.
Ambient temperature Operating Storage	 -25°C to +55°C at min. 1 m/s windload -40°C to +85°C
Relative humidity	MIL-STD-810H, Test method 507.6.
Solar radiation	1120 W/m^2, MIL-STD-810G Test method 505.6.
EMI/EMC	MIL-STD-461G.

A.2 Outline dimensions

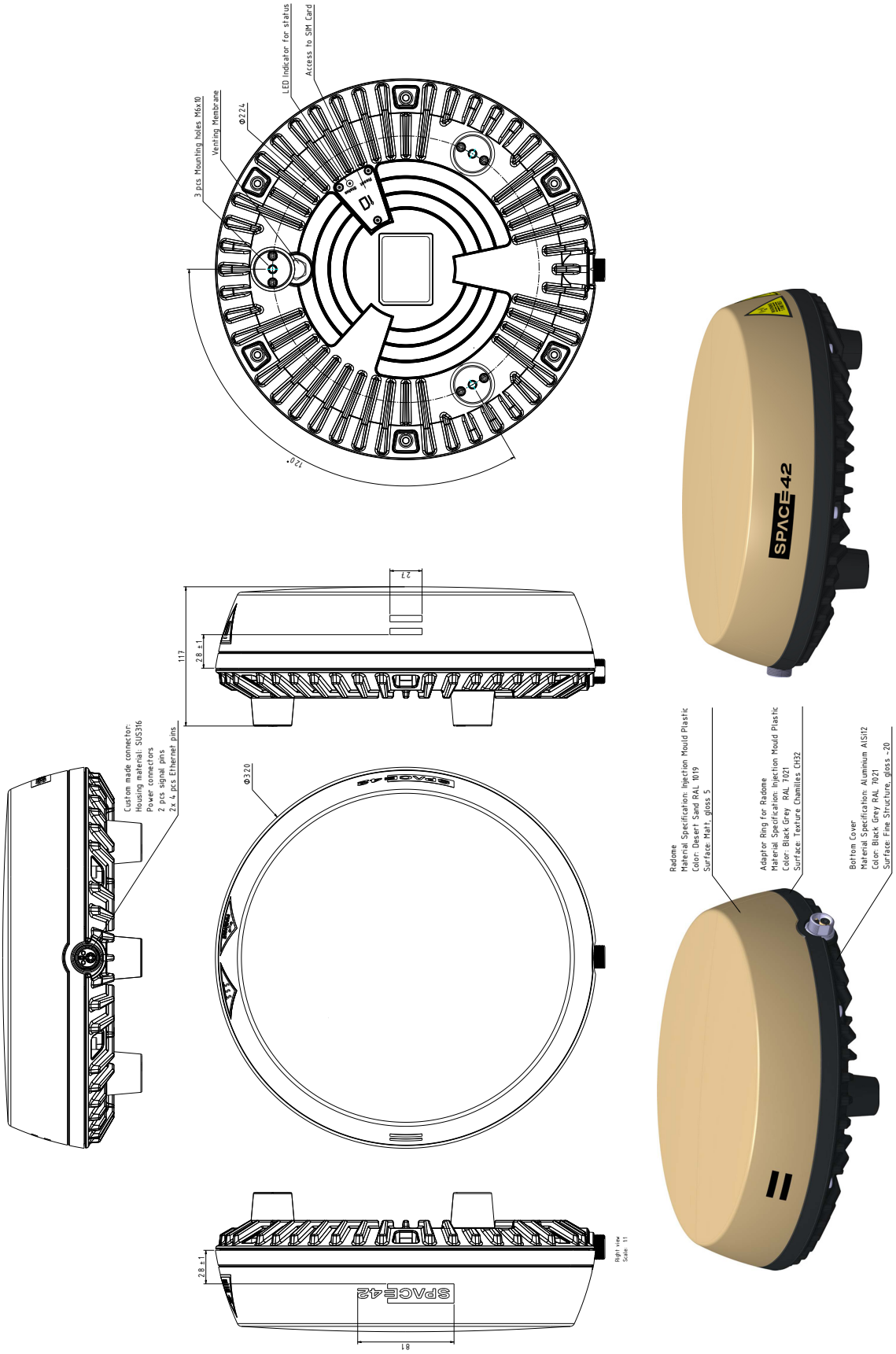


Figure A-1: Commander NEO outline dimensions drawing

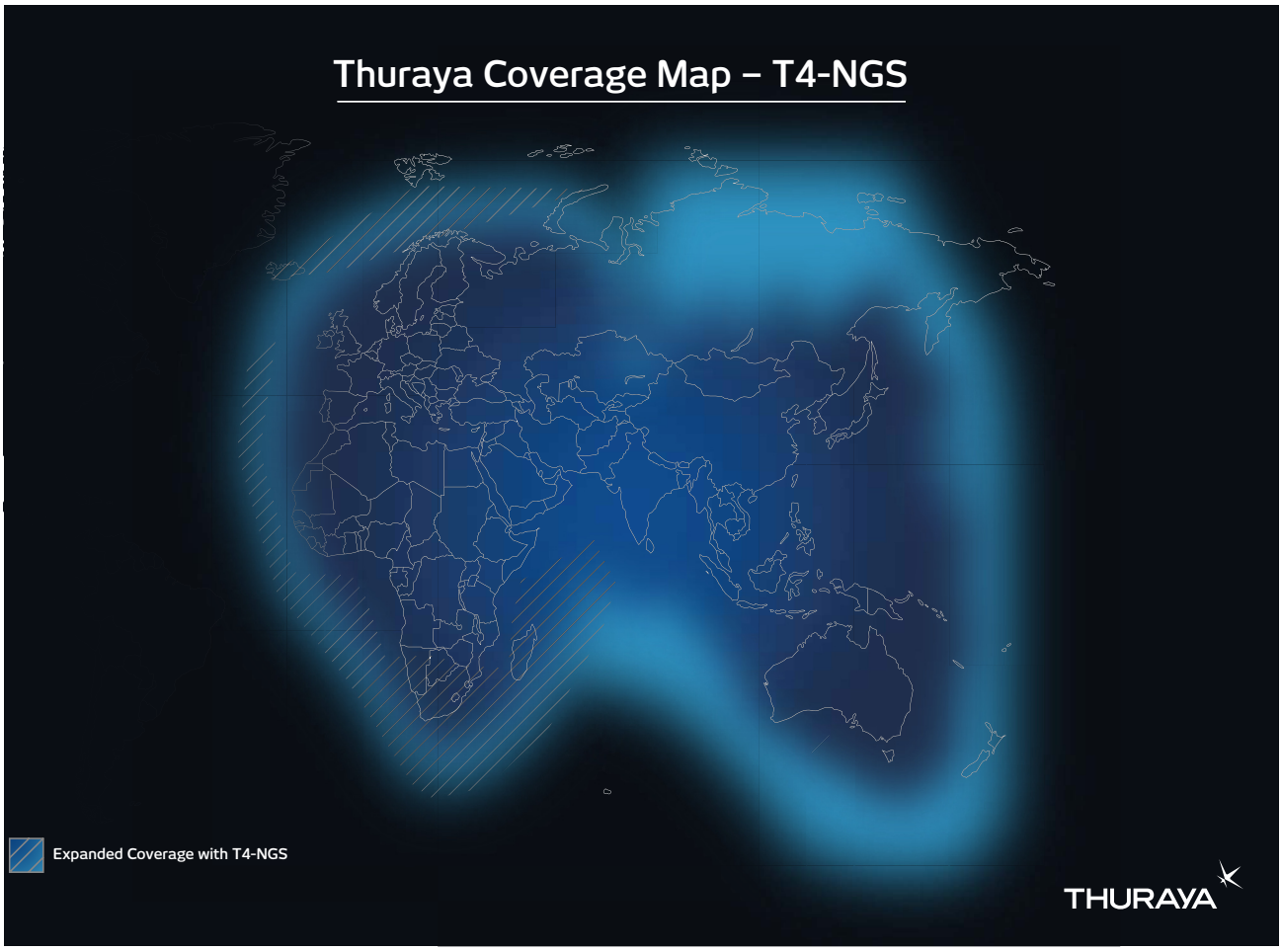
A.3 Satellite coverage

The satellite services are based on geostationary satellites situated above the equator. Each satellite covers a certain area (footprint). The coverage map below shows the footprints of the T2, T3 and T4-NGS satellites.

- Thuraya 2 is located at 44 degrees East longitude.
- Thuraya 3 is located at 98.5 degrees East longitude.
- Thuraya 4-NGS, located at 44 degrees East longitude, is launched in fall 2025.

For updated information on coverage, see Thuraya's home page at Thuraya.com.

Note If the Commander NEO is sold and used in the US, satellite functionality is not available.



Command reference

This appendix lists the function, syntax and parameters for commands used with the Commander NEO. You can send commands to the Commander NEO via AT shell. See *To access the terminal using AT commands* on page 4-5.

Note The use of AT shell must be enabled in the terminal. You can do this in the web interface, see *To set up AT shell* on page 5-29.

This appendix has the following sections:

- *Overview of AT commands*
- *AT commands*
  - *Syntax conventions*
  - *Identification related AT commands*
  - *Context management AT commands*
- *Configuration examples*

B.1 Overview of AT commands

Function	Command
Request manufacturer identification of the satellite terminal. (Use any one of the two commands).	+GMI +CGMI
Request model identification of the satellite terminal. (Use any one of the two commands).	+GMM +CGMM
Request Revision Identification of the satellite terminal. (Use any one of the two commands).	+GMR +CGMR
Request Product Serial Number Identification (IMEI) of the satellite terminal.	+CGSN
Request International Mobile Subscriber Identity (IMSI) of the satellite terminal.	+CIMI
Define PDP Context	+CGDCONT
PDP context read dynamic parameters	+CGCONTRDP[1]
Define Secondary PDP Context	+CGDSCONT[1]
PDP context read dynamic parameters	+CGSCONTRDP[1]
Traffic flow template read dynamic parameters	+CGTFTRDP[1]
Request the state of PS (attached or detached)	+CGATT?
PDP context activate or deactivate	+CGACT
Delete non-active PDP contexts	+CGDEL[1]
Show PDP address	+CGPADDR
Define EPS quality of service	+CGEQOS[1]
EPS quality of service read dynamic parameters	+CGEQOSRDP[1]
3G Quality of Service Profile (requested)	+CGEQREQ[2]

1. This command is only supported in T4-NGS network.
2. This command is only supported in T2 and T3 network.

B.2 AT commands

The following most used AT commands are explained in this manual. Other AT commands not mentioned here may still be supported.

- *Identification related AT commands*
- *Context management AT commands*

B.2.1 Syntax conventions

Syntax definitions use the following conventions:

- ‹parm› indicates that a parameter (without ‹ and ›) can be filled in by the user.
- {‹opt1› | ‹opt2› | ... } indicates that one of various options must be chosen by the user.
- [‹options›] indicates that ‹options› may or may not be included in the command.
- Keywords and parameters are separated by commas.
  Note: If parameters in the middle are left out, the commas must still be there as placeholders, e.g. **<parm1>,,,<parm4>** - In this case parm 2 and parm 3 are left out, but ‹parm4› is used. If the last parameters are left out, the commas are not needed, e.g. **<parm1>,<parm2>**
- String type parameters must be enclosed in quotes (“”)

B.2.2 Identification related AT commands

The identification related AT commands are “read” commands. They are written without parameters.

Possible responses for the identification related AT commands

The following tables summarize the possible responses to some of the most used AT commands for identification.

Command	Possible responses
+CGMI	‹manufacturer› ERROR
+CGMM	‹model› ERROR
+CGMR	‹revision› ERROR
+CGSN	‹sn› ERROR
+CIMI	‹IMSI› ERROR
+GMI	‹manufacturer›
+GMM	‹model›
+GMR	‹revision›

Response parameters for identification related AT commands

The table below summarizes the available parameters for the AT commands for identification.

Parameter	Meaning
<IMSI>	The IMSI number of the satellite terminal
<manufacturer>	The name of the manufacturer of the satellite terminal
<model>	The model of the satellite terminal
<revision>	The revision of the satellite terminal
<sn>	The IMEI number of the satellite terminal

B.2.3 Context management AT commands

The table below summarizes some of the most used AT commands for context management. Parameters are explained in *Parameters for context management AT commands* on page B-6. For details, refer to the 3GPP standard TS 27.007.

Command	Parameters
+CGACT	[<state>[,<cid>[,<cid>[,...]]]]
+CGATT?	No parameters (this is a “read” command)
+CGCONTRDP[1]	[=<cid>]
+CGDCONT	<cid>[,<PDP_type>[,<APN>[,<PDP_addr>[,<d_comp>[,<h_comp>[,<pd1>[,[,<pdN>]]]]]]]]
+CGDEL[1]	[=<cid>]
+CGDSCONT[1]	<cid>,<p_cid>[,<d_comp>[,<h_comp>]]
+CGEQOS[1]	<cid>[,<QCI>[,<DL_GBR>,<UL_GBR>[,<DL_MBR>,<UL_MBR>]]]
+CGEQOSRDP[1]	[=<cid>]
+CGEQREQ[2]	<cid>[,<Traffic class>[,<UL_MBR>[,<DL_MBR>[,<UL_GBR>[,<DL_GBR>[,<Delivery order>[,<Maximum SDU size>[,<SDU error ratio>[,<Residual bit error ratio>[,<Delivery of erroneous SDUs>[,<Transfer delay>[,<Traffic handling priority>]]]]]]]]]]]
+CGPADDR	[=<cid>[,<cid>[,...]]]
+CGSCONTRDP[1]	[=<cid>]
+CGTFTRDP[1]	[=<cid>]

1. This command is only supported when connected to T4-NGS network.
2. This command is not supported in T4-NGS network, only in T2 and T3 network.

Possible responses for context management AT commands

The possible responses for the context management AT commands are listed in the following table:

Command	Possible response(s)
+CGACT	OK ERROR
+CGATT?	+CGATT: <state>
+CGCONTRDP[1]	+CGCONTRDP:<cid>,<bearer_id>,<apn> [<CR><LF>+CGCONTRDP:<cid>,<bearer_id>,<apn>[...]]
+CGDCONT	OK ERROR
+CGDEL[1]	OK ERROR [+CGDEL: <cid>[,<cid>[,...]]
+CGDSCONT[1]	OK ERROR
+CGEQOS[1]	OK ERROR
+CGEQOSRDP[1]	[+CGEQOSRDP: <cid>,<QCI>, [<DL_GBR>,<UL_GBR>], [<DL_MBR>,<UL_MBR>], [<DL_AMBR>,<UL_AMBR>]] [<CR><LF>+CGEQOSRDP: <cid>, <QCI>, [<DL_GBR>,<UL_GBR>], [<DL_MBR>,<UL_MBR>], [<DL_AMBR>,<UL_AMBR>]][...]]
+CGEQREQ	OK ERROR
+CGPADDR	+CGPADDR: <cid>,<PDP_addr> [<CR><LF>+CGPADDR: <cid>,<PDP_addr> [...]]

Command	Possible response(s)
+CGSCONTRDP[1]	+CGSCONTRDP:<cid>, <p_cid>, <bearer_id> [<CR><LF>+CGSCONTRDP:<cid>,<p_cid>,<bearer_id>[...]] OK ERROR
+CGTFTRDP[1]	[+CGTFTRDP: <cid>,<packet filter identifier>, <evaluation precedence index>,<remote address and subnet mask>, <protocol number (ipv4) / next header (ipv6)>,<local port range>, <remote port range>,<ipsec security parameter index (spi)>, <type of service (tos) (ipv4) and mask / traffic class (ipv6) and mask>, <flow label (ipv6)>,<NW packet filter Identifier>,<QRI>] [<CR><LF>+CGTFTRDP: <cid>,<packet filter identifier>, <evaluation precedence index>,<remote address and subnet mask>, <protocol number (ipv4) / next header (ipv6)>,<local port range>, <remote port range>,<ipsec security parameter index (spi)>, <type of service (tos) (ipv4) and mask / traffic class (ipv6) and mask>, <flow label (ipv6)>,<NW packet filter Identifier>, <QRI>][...]]

1. This command is only supported when connected to T4-NGS network.

Parameters for context management AT commands

The table below states the main parameters for the AT commands for context management. For details, refer to the 3GPP standard TS 27.007 and ITU-T V.250.

Parameter	Values	Meaning
<APN>	<APN>	Access Point Name. A string parameter which is a logical name that is used to select the GGSN or the external packet data network. If the value is null or omitted, then the subscription value will be requested.
<cid>	<cid> (1-11)	The Context Identifier for the PDP context. A numeric parameter identifying the specific PDP context - maximum 11 PDP contexts may be defined.
<d_comp>	0	A numeric parameter that controls PDP data compression: Off (default if value is omitted)
<Delivery of erroneous SDUs>	0 1 2 3	Indicates whether SDUs detected as erroneous shall be delivered or not. No Yes No detect Subscribed value
<Delivery order>	0 1 2	Indicates whether the UMTS bearer shall provide in-sequence SDU delivery or not. No Yes Subscribed value
<DL_AMBR>	<DL_AMBR>	The APN aggregate maximum bit rate downlink (see 3GPP TS 24.301 [83]). The value is in kbit/s.

Parameter	Values	Meaning
<DL_GBR>	<DLGBR>	The guaranteed bit rate down link. The value is in kbit/s. This parameter is omitted for a non-GBR QCI.
<DL_MBR>	<DL_MBR>	The maximum bit rate down link. The value is in kbit/s. This parameter is omitted for a non-GBR QCI.
<evaluation precedence index>	<evaluation precedence index> (0-255)	The evaluation precedence index defines the order in which the traffic flow filters are applied to packets. 0 is first, then 1, 2 etc. Numeric parameter, value range from 0 to 255.
<flow label (ipv6)>	from 00000 to FFFFF	A label to identify a packet as being part of a specific flow. Numeric value in hexadecimal format. Valid for IPv6 only.
<h_comp>	0 1	A numeric parameter that controls PDP header compression Off (default if value is omitted) On NOTE: At present only one data compression algorithm (V.42bis) is provided in SNDCP. If and when other algorithms become available, a command will be provided to select one or more of these.
<ipsec security parameter index (spi)>	from 00000000 to FFFFFFFF	A numeric value in hexadecimal format from 00000000 to FFFFFFFF, used to secure IP communication.
<local port range>	0-65535.0-65535	Local port range in the form **From**.**To** (0-65535).(0-65535)
<Maximum SDU size>	Integer type; (1,2,3,...)	Indicates the maximum allowed SDU size in octets. If the parameter is set to '0' the subscribed value will be requested.
<NW packet filter Identifier>	1-16	Integer type. In EPS the value is assigned by the network when established
<p_cid>	<p_cid> (1-11)	Primary PDP Context Identifier. The primary context to which the secondary context is related. A numeric parameter which specifies a particular PDP context definition which has been specified by use of the +CGDCONT command. The parameter is local to the TE-MT interface. The list of permitted values is returned by the test form of the command.
<packet filter identifier>	<packet filter identifier> (1-8)	The packet filter identifier. Numeric parameter, value range from 1 to 8.
<pd1>, <pdN>	<pd1> <pd2> .... <pdN>	Zero to N string parameters whose meanings are specific to the <PDP_type> For PDP type OSP:IHOSS the following parameters are defined: <pd1> = <host> The fully formed domain name extended hostname of the Internet host. <pd2> = <port > The TCP or UDP port on the Internet host. <pd3> = <protocol> The protocol to be used over IP on the Internet - "TCP" or "UDP.

Parameter	Values	Meaning
<PDP_addr>	<PDP_address>	A string parameter that identifies the MT in the address space applicable to the PDP context. If the value is null or omitted, then a value may be provided by the TE during the PDP startup procedure or, failing that, a dynamic address will be requested. The allocated address may be read using the +CGPADDR command.
<PDP_type>	IP IPV6 PPP	Internet Protocol (IETF STD 5) Internet Protocol, version 6 (IETF RFC 2460) Point to Point Protocol (IETF STD 51)
<protocol number (ipv4) / next header (ipv6)>	0-255	The Protocol Number / Next Header attribute of a valid packet filter shall contain either an IPv4 Protocol Number or an IPv6 Next Header value. Numeric parameter, value range from 0 to 255
<QCI>	0-255	Integer type; specifies a class of EPS QoS (see TS 23.203 and TS 24.301). 0 QCI is selected by network [1 – 4]value range for guaranteed bit rate Traffic Flows 75 value for guaranteed bit rate Traffic Flows [82 – 85]value range for guaranteed bit rate Traffic Flows [5 – 9]value range for non-guaranteed bit rate Traffic Flows 79 value for non-guaranteed bit rate Traffic Flows [128 – 254]value range for Operator-specific QCIs The QCI values 65, 66, 67, 69 and 70 are not allowed to be requested by the UE. If the TE requests a QCI parameter 65, 66, 67, 69 or 70, the MT responds with result code +CME ERROR: 181 (unsupported QCI value).
<QRI>	(Integer type)	Identifies the QoS rule, see 3GPP TS 23.501 and 3GPP TS 24.501
<remote port range>	0-65535.0-65535	Remote port range in the form **From.To** (0-65535).(0-65535)
<Residual bit error ratio>	(String type)	Indicates the target value for the undetected bit error ratio in the delivered SDUs. If no error detection is requested, Residual bit error ratio indicates the bit error ratio in the delivered SDUs. The value is specified as "mEe". As an example a target residual bit error ratio of $5x10^{-3}$ would be specified as "5E3" (AT+CGEQREQ=...,"5E3",...). "0E0" means subscribed value.
<SDU error ratio>	(String type)	Indicates the target value for the fraction of SDUs lost or detected as erroneous. SDU error ratio is defined only for conforming traffic. The value is specified as 'mEe'. As an example a target SDU error ratio of $5x10^{-3}$ would be specified as "5E3" (AT+CGEQREQ=...,"5E3",...). "0E0" means subscribed value.
<state>	0 1	Deactivate or Detached Activate or Attached
<Traffic class>	1 3	Streaming Standard data (Background).
<Traffic handling priority>	Integer type; (1,2,3,...)	Specifies the relative importance for handling of all SDUs belonging to the UMTS bearer compared to the SDUs of other bearers. If the parameter is set to '0' the subscribed value will be requested

Parameter	Values	Meaning
<Transfer delay>	0 500 4000	0 ms, error correction is determined by the network 500 ms, error correction is disabled 4000 ms, error correction is applied
<type of service (tos) (ipv4) and mask / traffic class (ipv6) and mask>	(0-255).(0-255)	String type. The string is given as dot-separated numeric (0-255) parameters on the form "t.m", where “t” is the type of service or traffic class, and “m” is the mask.
<UL_AMBR>	<UL_AMBR>	The APN aggregate maximum bit rate uplink (see 3GPP TS 24.301). The value is in kbit/s.
<UL_GBR>	<UL_GBR>	The guaranteed bit rate up link. The value is in kbit/s. This parameter is omitted for a non-GBR QCI.
<UL_MBR>	<UL_MBR>	The maximum bit rate up link. The value is in kbit/s. This parameter is omitted for a non-GBR QCI.

B.3 Configuration examples

For general syntax, see *Syntax conventions* on page B-3.
For parameters, see *Parameters for context management AT commands* on page B-6.

B.3.1 To create a primary PDP context

Relevant command: **at+cgdcont**

1. To create a primary PDP context, send the command:
   `at+cgdcont=[<cid>[,<PDP_type>[,<APN>[,<PDP_addr>[,<d_comp>[,<h_comp>[,<pd1>[,[,<pdN>]]]]]]]]]`

   Example: at+cgdcont=1,"IP","AccessPointName"

   In this example the command specifies:
   - **1:** The CID of this primary PDP context.
   - **IP**: The PDP type of this PDP context. **IP** means **Internet Protocol (IETF STD 5)**.
   - **AccessPointName:** The APN (Access Point Name) for the data connection.

   If the command was successful, the terminal returns with the response: `OK`
2. To get the parameters set up for primary PDP context, send the command:
   at+cgdcont?
   The response for the example above will be:
   `+CGDCONT: 1, "IP", "AccessPointName", 0.0.0.0, 0, 0, "", ""`
   `OK`

B.3.2 To create two secondary PDP contexts attached to the primary PDP context with ID=1 (only for T4-NGS network)

Relevant command: **at+cgdscont**

1. To create a secondary PDP context attached to the primary PDP context, send the command:
   `at+cgdscont=[<cid>,<p_cid>]`

   Example: at+cgdscont=2,1
   at+cgdscont=4,1

   In this example, two secondary contexts are created. The first command specifies:
   - **2:** The CID of this secondary PDP context.
   - **1:** This secondary PDP context is attached to primary PDP context with CID **1**.

   The second command specifies:
   - **4**: The CID of this secondary PDP context.
   - **1:** This secondary PDP context is attached to the primary PDP context with CID **1**.

   If the commands are successful, the terminal returns with the response: `OK`
2. To get the parameters set up for secondary PDP contexts, send the command:
   at+cgdscont?
   The response for the example above could be:
   +CGDSCONT: 2, 1
   +CGDSCONT: 4, 1
   OK

B.3.3 To query dynamic parameters of a selected traffic flow template (only for T4-NGS network)

Relevant command: **at+cgtftrdp**

1. To query the dynamic parameters of a selected traffic flow template, send the command:
   `at+cgtftrdp=<cid>`

   Example: at+cgtftrdp=1

   The response could be:
   `+CGTFTRDP: 1, 3, 0, 255.255.255.255.255.255.255.255,,,,,,,3,1`
   `OK`
   In this example the response shows:
   - **1:** The CID of the PDP context that the traffic flow template applies to.
   - **3:** The packet filter identifier.
   - **0:** The evaluation precedence index. **0** is the first traffic flow filter to be applied.
   - **255.255.255.255.255.255.255.255:** The source address and subnet mask.
   - **3**: The network packet filter identifier
   - **1**: The QRI (QoS rule, see 3GPP TS 23.501 and 3GPP TS 24.501)

B.3.4 To query dynamic parameters of all traffic flow templates (only for T4-NGS network)

Relevant command: **at+cgtftrdp**

1. To query the dynamic parameters of all defined traffic flow templates, send the command:
   `at+cgtftrdp`

   Example: at+cgtftrdp

   A response could be:
   `+CGTFTRDP: 1, 3, 0, 255.255.255.255.255.255.255.255, , , , , , , 3, 1`
   `+CGTFTRDP: 2, 4, 0, 255.255.255.255.255.255.255.255, , , , , , , 3, 1`
   `+CGTFTRDP: 4, 4, 0, 255.255.255.255.255.255.255.255, , , , , , , 3, 1`
   `OK`
   See the previous section for the meaning of the parameters.

B.3.5 To set the Quality of Service (QoS) of the PDP context (only for T4-NGS network)

Relevant command: **at+cgeqos**

1. To set the Quality of Service for your PDP context, send the command:
   `at+cgeqos=[<cid>[,<QCI>[,<DL_GBR>,<UL_GBR>[,<DL_MBR>,<UL_MBR>]]]]`

   Example: at+cgeqos=1,0

   In this example the parameters specify:
   - **1**: The CID of the PDP context.
   - **0 :** The QCI (class of EPS QoS). **0** means the QoS is selected by the network.

If the command was successful, the terminal returns with the response:
`OK`

Example: at+cgeqos=2,4,500,500

In this example the parameters specify:

- **2**: The CID of the PDP context.
- **4**: The QCI (class of EPS QoS). 1 to 4: value range for guaranteed bit rate Traffic Flows.
- **500**: The guaranteed download bit rate in kbit/s.
- **500**: The guaranteed upload bit rate in kbit/s.

If the command was successful, the terminal returns with the response:
`OK`

B.3.6 To set the requirements to Quality of Service of the PDP context

Relevant command: **at+cgeqreq**

1. To set the Quality of Service for your PDP context, send the command:
   `at+cgeqreq=<cid>[,<Traffic class>[,<UL_MBR>[,<DL_MBR>[,<UL_GBR>[,<DL_GBR>[,<Delivery order>[,<Maximum SDU size>[,<SDU error ratio>[,<Residual bit error ratio>[,<Delivery of erroneous SDUs>[,<Transfer delay>[,<Traffic handling priority>]]]]]]]]]]]]`

   Example: at+cgeqreq=1,3

   In this example the parameters specify:
   - **1**: The CID of the PDP context.
   - **3**: The Traffic class. **3** means the Traffic class is Background data (Standard data).

   If the command was successful, the terminal returns with the response: `OK`

   Example: at+cgeqreq=1,1,256,256,256,256

   In this example the parameters specify:
   - **1**: The CID of the PDP context.
   - **1**: The Traffic class. **1** means the Traffic class is Streaming.
   - **256**: The maximum upload bit rate in kbit/s.
   - **256**: The maximum download bit rate in kbit/s.
   - **256**: The guaranteed upload bit rate in kbit/s.
   - **256**: The guaranteed download bit rate in kbit/s.

   If the command was successful, the terminal returns with the response: `OK`

B.3.7 To query dynamic parameters of all QoS (only for T4-NGS network)

Relevant command: **at+cgeqosrdp**

1. To query the dynamic parameters of all QoS, send the command:
   at+cgeqosrdp

   Example: at+cgeqosrdp

   A response for the QoSes defined in the previous section could be:
   +CGEQOSRDP: 1, 0, 0, 0, 0, 0, 128, 512
   +CGEQOSRDP: 2, 4, 500, 500, 0, 0, 128, 512
   OK
   In the first response, the parameters specify:
   - **1**: The CID for this PDP context.
   - **0**: The QCI (class of EPS QoS). **0** means the QoS is selected by the network.
   - **0**: Guaranteed bit rate for download - 0 means no guaranteed bit rate is defined.
   - **0**: Guaranteed bit rate for upload - 0 means no guaranteed bit rate is defined.
   - **0**: Maximum bit rate for download - 0 means no maximum bit rate is defined.
   - **0**: Maximum bit rate for upload - 0 means no maximum bit rate is defined.
   - **128**: Aggregated bit rate for download in kbit/s.
   - **512**: Aggregated bit rate for upload in kbit/s.

   In the second response, the parameters specify:
   - **2**: The CID for this PDP context.
   - **4**: The QCI (class of EPS QoS). 1 to 4: value range for guaranteed bit rate Traffic Flows.
   - **500**: Guaranteed bit rate for download in kbit/s.
   - **500**: Guaranteed bit rate for upload in kbit/s.
   - **0**: Maximum bit rate for download - 0 means no maximum bit rate is defined.
   - **0**: Maximum bit rate for upload - 0 means no maximum bit rate is defined.
   - **128**: Aggregated bit rate for download in kbit/s.
   - **512**: Aggregated bit rate for upload in kbit/s.

B.3.8 To activate a PDP context

Relevant command: **at+cgact**

1. To activate a PDP context, send the command:
   at+cgact=[<state>[,<cid>[,<cid>[,...]]]]

   Example: at+cgact=1,1

   In this example, the parameters specify:
   - **1**: Set the state of the PDP context to **Activated**.
   - **1**: The CID of the PDP context that is going to be activated.

   If the command was successful, the terminal returns with the response:
   OK

B.3.9 To query the state of all PDP contexts

Relevant command: **at+cgact?**

1. To query the state (activated or deactivated) of all PDP contexts, send the command:
   at+cgact?
   The response could be:
   ```
   +CGACT: 1, 1
   +CGACT: 2, 0
   +CGACT: 4, 0
   OK
   ```
   In these responses, the **first parameter** specifies the **CID** of the PDP context and the **second parameter** specifies whether it is **activated (1)** or **deactivated (0)**.

B.3.10 To query the IP address of an activated PDP context

Relevant command: **at+cgpaddr**

1. To query the IP address of an activated PDP context, send the command:
   at+cgpaddr=<cid>

   Example: at+cgpaddr=1

   The response could be:
   ```
   +CGPADDR: 1, 10.186.2.198
   OK
   ```
   The **first parameter** is the **CID** of the PDP context, the **second** is the **IP address** of the terminal in the address space applicable to the PDP context.

B.3.11 To query the state of the Packet Domain service (Attached or Detached)

Relevant command: **at+cgatt?**

1. To read the state of the Packet Domain service, send the command:
   `at+cgatt?`

   Example: `at+cgatt?`

   Response: `+cgatt: 1`
   In this example, the parameter **1** means the terminal is attached to the Packet Domain service.

List of default settings

This appendix lists the default configuration settings that apply after a Reset to factory default.

Item	Default settings
LAN	
Enable/Disable LAN	LAN is enabled
Advanced LAN	
Port forwarding	
Active	Not active
Incoming port start	<empty>
Incoming port end	<empty>
Destination IP Addr	<empty>
Dest. port start	<empty>
Dest. port end	<empty>
WLAN	
Enable/ Disable	WLAN is disabled
WLAN type	2.4 GHz (Default)
WLAN standard	For 2.4 GHz, 802.11n (Disabled); For 5Ghz - 802.11n (Disabled), 802.11ac (Disabled)
Country code	AE
Channel number	0
Broadcast SSID	Selected
SSID	Commander-NEO_<last 4 digits of serial number>
Security standard	WPA2-AES
Key type (HEX or text)	Text
Encryption key	<serial number of the Commander NEO>
Voice	
Enable/ Disable	Voice is disabled

Item	Default settings
IP handsets	
Handset enable/disable	Handset 0501 enabled, all other handsets disabled
Password	Same as user name/local number, i.e., 0501, 0502, 0503, or 0504
Notify incoming calls	Selected
Network in use	
Satellite network, Network in use	Thuraya T4
Stealth mode	
Enable Stealth mode	Disabled (not selected)
Logs	All logs cleared
Terminal settings	
Internet connection mode	Router mode
Bridge mode IP address	(Plus one) - not applicable, Router mode is default
Local IP address	192.168.0.1
Subnet mask	255.255.255.0
DHCP	
Enable	Enabled
DHCP range start	192.168.0.10
DHCP range end	192.168.0.40
GNSS	
GNSS type	GPS and GLONASS
AGPS enabled	Not selected
Language	English
Advanced	
Passwords	
Normal user	
User id	user
Password	‹empty›
Administrator	
User id	administrator
Password	‹serial number of the terminal›

Item	Default settings
Power control	
Mode	Always on (no power save function)
Remote on/off, Delayed shut down	(0 minutes) - not applicable, Always on is default
Remote on/off, Power control pin	(Active low) - not applicable, Always on is default
LED	
Mode	On for 5 minutes
SIM Configuration, SIM Mode	uSIM
Enable/disable SIM PIN	Require PIN on startup **NOT selected**
Security	
HTTPS settings	
Redirect HTTP to HTTPS	Not selected
Use uploaded TLS/SSL certificate	Not selected
AT shell	
Enable AT shell	Not selected (Disabled)
Change AT shell user password	Not selected
New AT shell user password	<empty>
Service user	
Enable Service user	Not selected (Disabled)
Change Service user user password	Not selected
New Service user user password	<empty>
Remote Terminal Manager	
Enable remote access from management server	Disabled (not selected)
Custom applications	
Custom applications enabled	Disabled (not selected)
Custom applications unlock key	<empty>
Custom applications user password	<empty>

Item	Default settings
Connections (dashboard)	
Connections on Dashboard	Standard data Streaming 16 kbps Streaming 32 kbps Streaming 64 kbps Streaming 128 kbps Streaming 256 kbps Streaming 384 kbps Streaming 512 kbps Streaming 768 kbps Streaming 1024 kbps
Identifier	<empty>
Activation	
Automatic	Not selected (data connections must be started manually)
APN	
Type	Default (The APN is taken from the terminal, defined by Space42).
User defined name	<empty>
Quality of service	
Traffic class	Standard (shared background connection)
Max. bit rate upload	<empty> (only applicable for Streaming)
Max. bit rate download	<empty> (only applicable for Streaming)
Guaranteed bit rate upload	<empty> (only applicable for Streaming)
Guaranteed bit rate download	<empty> (only applicable for Streaming)

Conformity

Certificates of approval will be available in partnerportal.cobhamsatcom.com or from your supplier.

D.1 EU (CE)

The Commander NEO is CE certified as stated in the “EU Declaration of Conformity”.

The WLAN interface is CE certified through the manufacturer of the WLAN card.

Use of WLAN:

The WLAN interface requires that the user enters the current country of operation. See *WLAN interface setup* on page 5-14.

D.2 MIL approvals

The Commander NEO is approved to the following MIL standards:

- MIL-STD-810
- MIL-STD-463
- MIL-STD-901
- MIL-STD-1275

D.3 RCM, Australia

The Commander NEO is RCM certified as stated in the “Certificate/Declaration of Conformance RCM”.

D.4 Safety CB certificate

The Commander NEO is certified as stated in the CB Test Certificate.

D.5 FCC

FCC e-label:

Model: 8033A

Thuraya Commander NEO Terminal

FCC ID: ROJ-8033A

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

NOTICE:

This device complies with Part 15C and part 15E of the FCC Rules.

Operation is subject to the following two conditions:

(1) this device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

NOTICE:

Changes or modifications made to this equipment not expressly approved by Cobham Satcom may void the FCC authorization to operate this equipment.

Glossary

A

ACA	Automatic Connection Activation
APN	Access Point Name. The Access Point Name is used by the terminal operator to establish the connection to the required destination network.

C

cid	Context Identifier

D

DNS	Domain Name System. A system translating server names (URLs) to server addresses.

E

EPS	Evolved Packet System. Also called Universal Mobile Telecommunications Service (UMTS) is a third-generation (3G) broadband, packet-based transmission of text, digitized voice, video, and multimedia at data rates up to 2 megabits per second (Mbps) which offers a consistent set of services to mobile computer and phone users, no matter where they are located in the world. It allows computers and phones to be constantly attached to the Internet wherever they travel (roam) with access through a combination of terrestrial wireless and satellite transmissions.

G

GBR	Guaranteed bit rate (streaming rate)
GGSN	Gateway GPRS Support Node. The GGSN converts the incoming data traffic coming from the mobile users through the Service gateway GPRS support node (SGSN) and forwards it to the relevant network, and vice versa. The GGSN and the SGSN together form the GPRS support nodes (GSN)

H

HLR	Home Location Register. The HLR contains information regarding users who are registered as subscribers in the area, whereas the VLR contains information regarding users who are registered as subscribers somewhere else but are roaming in the area.
HTTP	HyperText Transfer Protocol. HTTP is the underlying protocol used by the World Wide Web. This protocol defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.
HTTPS	Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network, and is widely used on the Internet.

I

ICCID	Integrated Circuit Card Identification (SIM card number)
IMEI	International Mobile Equipment Identity. A unique number identifying your terminal.
IMSI	International Mobile Subscriber Identity. A number used to identify the user of a cellular network. It is a unique identification associated with all cellular networks.

IP	Internet Protocol
ipsec	Internet Protocol Security. A protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a session.

L

LAN	Local Aera Network
LED	Light Emitting Diode
LTE	Long-term evolution (LTE) is a standard for wireless broadband communication for mobile devices and data terminals, based on the GSM/EDGE and UMTS/HSPA standards.

M

MBR	Maximum bit rate
ME	Mobile Equipment. In this case, your satellite terminal
MT	Mobile Terminal

N

NAT	Network Address Translation. An Internet standard that enables a local-area network to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. A NAT module makes all necessary address translations.

O

OSP:IHOSS	Octet Stream Protocol for Internet Hosted Octet Stream Service

P

PDP	Packet Data Protocol. A network protocol used by external packet data networks that communicate with a GPRS network.
PIN	Personal Identification Number. A code number used to provide access to a system that has restricted access.
PLMN	Public Land Mobile Network. A term used to describe all mobile wireless networks that use earth-based stations rather than satellites.
PPPoE	Point-to-Point Protocol over Ethernet
PTT	Push To Talk
PUK	PIN Unblocking Key. An eight-digit code used to unblock a SIM card after three incorrect PINs have been entered. The PUK code is supplied with the SIM card.

Q

QCI	Quality of service Class (see 3GPP TS 23.203 and 3GPP TS 24.301)
QoS	Quality of Service

R

REST	Representational State Transfer. REST API is an application programming interface (API) that allows for interaction with RESTful web services.

S

SDU	Service Data Unit
SIM	Subscriber Identity Module. The SIM provides secure storing of the key identifying a mobile service subscriber but also subscription information, preferences and storage of text messages.
SIP	Session Initiation Protocol. An application-layer control (signaling) protocol used e.g. for Internet telephony.
SNDCP	Sub Network Dependent Convergence Protocol, is part of layer 3 of a GPRS protocol specification. SNDCP interfaces to the Internet Protocol at the top, and to the GPRS-specific Logical Link Control (LLC) protocol at the bottom.
SSL	Secure Sockets Layer. The standard technology for keeping an Internet connection secure and safeguarding any sensitive data that is being sent between two systems.

T

TCP	Transmission Control Protocol. One of the core protocols of the Internet protocol suite. TCP provides reliable, in-order delivery of a stream of bytes, making it suitable for applications like file transfer and e-mail.
TE	Terminal Equipment
TLS	Transport Layer Security. An updated, more secure, version of SSL.

U

UDP	User Datagram Protocol. Part of the TCP/IP suite of protocols used for data transferring. UDP doesn't acknowledge that the packets being sent have been received. For this reason, the UDP protocol is typically used for streaming media. While you might see skips in video or hear some fuzz in audio clips, UDP transmission prevents the playback from stopping completely.
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
UTC	Coordinated Universal Time. The International Atomic Time (TAI) with leap seconds added at irregular intervals to compensate for the Earth's slowing rotation. Leap seconds are used to allow UTC to closely track UT1, which is mean solar time at the Royal Observatory, Greenwich.

V

VHF	Very High Frequency. 30-300 MHz, a "straight-line" signal used for short-distance terrestrial communication and navigation.
VLR	Visitor Location Register. See HLR
VoIP	Voice over IP (Internet Protocol)
VPN	Virtual Private Network

W

WLAN	Wireless Local Area Network

Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W