**COBHAM SATCOM**

# EXPLORER 540

**User & integrator's manual**

**Document number:** 98-148232-M

**Release date:** 11 December 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

- **Inmarsat** is a registered trademark of the International Maritime Satellite Organisation (IMSO) and is licensed by IMSO to Inmarsat Limited and Inmarsat Ventures plc.
- 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.

If the equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

> ⚠ **WARNING!** This equipment is not suitable for use in locations where children are likely to be present.

### Keep away from live circuits
Operating personnel must not remove equipment covers, other than the cover for the interface enclosure. Component replacement and internal adjustment must be made by qualified maintenance personnel. 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 touching them.

### Do not substitute parts or modify equipment
Because of the danger of introducing additional hazards, do not substitute parts or perform any unauthorized modification to the equipment.

### Keep away from antenna front
This device emits radio frequency energy when switched on. To avoid injury, keep a minimum safety distance of 1 m/ 3.2 ft from the antenna front when the EXPLORER 540 is on.

### Garder à l'écart de l'avant de l'antenne
Le présent appareil émet des radiofréquences lors de son utilisation.
Afin d'éviter tout risque pour la santé, une distance minimale de 1 m/ 3.2 ft est nécessaire entre l'utilisateur et l'avant de l'EXPLORER 540.

### Observe marked areas
Under extreme heat conditions do not touch areas of the EXPLORER 540 that are marked with this symbol, as it may result in injury.

### C1D2
This equipment is suitable for use in Class I, Division 2, Groups A, B, C and D OR non-hazardous locations only.

This equipment must be installed using wiring methods as required for Class I, Division 2 as per the NEC and/or CEC.

> ⚠ **WARNING!** **EXPLOSION HAZARD** – Do not connect or disconnect equipment unless power has been removed or the area is known to be non-hazardous.

**Cyber security**

For security reasons, ensure that you are using the latest version of the manual and have the latest software version installed on your device. Both can be found in the Cobham Satcom Partner Portal https://partnerportal.cobhamsatcom.com/eshop/downloads.

**Do not** connect the terminal directly to **unsecured devices**. Route all traffic through a firewall or similar.

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

# Antenna safety instructions

**Use only manufacturer supplied antennas.**
**Antenna minimum safe distance: 1 m/ 3.2 ft**

## Antenna gain

Directional, with maximum gain of 11.25 dBi (with reference to isotropic).

The Federal Communications Commission has adopted a safety standard for human exposure to RF (Radio Frequency) energy which is below the OSHA (Occupational Safety and Health Act) limits.

## Antenna mounting

The antenna supplied by the manufacturer must be located such that during radio transmission, no person or persons can come closer than the above indicated minimum safe distance to the front face of the antenna, i.e. 1 m./ 3.2 ft

L'antenne fournie par le fabricant doit être placée de telle sorte que, durant les transmissions radio, personne ni aucun groupe de personnes ne puisse s'approcher à une distance inférieur à la distance de sécurité minimal indiquée ci-dessus, c.-à-d., 1 m/ 3.2 ft.

To comply with current FCC RF Exposure limits, the antenna must be installed at or exceeding the minimum safe distance shown above, and in accordance with the requirements of the antenna manufacturer or supplier.

## Radiation warning

> ⚠️ **WARNING!** Maintain a separation distance of at least 1 m/ 3.2 ft from the front face of the antenna to a person. This safety distance is based on a radiation level of 4.1W/m$^2$ (IC).

You, as the qualified end-user of this radio device, must control the exposure conditions of bystanders to ensure the minimum separation distance (above) is maintained between the antenna and nearby persons, for satisfying RF Exposure compliance. The operation of this transmitter must satisfy the requirements of General Population/ Uncontrolled Environment. Only use the terminal when persons are at least the minimum distance from the front face of the antenna.

# About this manual

**Intended readers**

This manual is a user and integrator's manual for the EXPLORER 540. The manual is intended for anyone who is using or intends to use the EXPLORER 540, including system integrators. No specific skills are required to operate the EXPLORER 540. However, it is important that you observe all safety requirements listed in the **Safety summary** in the beginning of this manual, and operate the EXPLORER 540 according to the guidelines in this manual.

**Related documents**

The following documents are related to this manual and to the EXPLORER 540 system.

| Title and description | Document number |
|---|---|
| EXPLORER 540 Installation guide (English) | 98-148231 |
| EXPLORER 540 Installation guide (German) | 98-150246 |
| EXPLORER 540 Installation guide (French) | 98-150247 |
| EXPLORER 540 Installation guide (Spanish) | 98-150248 |
| EXPLORER 540 Installation guide (Russian) | 98-150249 |
| EXPLORER 540 Installation guide (Japanese) | 98-150250 |
| EXPLORER 540 Installation guide (Chinese) | 98-150251 |
| EXPLORER 540 Cellular Modem Installation guide | 98-174222 |

## 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 antenna front during pointing".
- To indicate what the user should select in the user interface.
  Example: "Select **Control panel** > **LAN** and click **Enable**".

*Italic* is used to emphasize the paragraph title in cross-references.

> Example: "For further information, see *Connecting Cables* on page...".

`Courier` is used to indicate low level commands, e.g. AT commands.

# Table of contents

# Introduction to EXPLORER 540

## 1.1    General description

The EXPLORER 540 is a small and light BGAN M2M terminal, with the option to operate on both Inmarsat and cellular networks. The durable casing and a dust and water resistant design makes the EXPLORER 540 the perfect choice for any kind of fixed outside installation.

Depending on your airtime subscription, the EXPLORER 540 either operates as an M2M (machine-to-machine) terminal or as a BGAN class 2 terminal.

With the optional EXPLORER 540 Cellular Modem, the EXPLORER 540 provides unique flexibility and M2M data communication cost-control, as it ensures the most cost-effective communication service can be chosen. The dual-mode operation delivers significant fail-over capabilities with the automatic switching between the BGAN network and the cellular network. For organizations transferring critical real-time data within their M2M networks, the dual mode of the EXPLORER 540 can provide unmatched service availability.

## 1.2     Features and interfaces of the EXPLORER 540

### 1.2.1     Features

- M2M or BGAN class 2, depending on airtime subscription (SIM card)
- Automatic installation function
- Standard data up to 464/448 kbps (download/upload)
- Remote management
- SMS for remote management
- Power save functions with various "wake on" methods (timer, input pin and wake-on-LAN)
- Software upgrade and file transfer over-the-air
- 2 watchdog functions
    - Connection watchdog (Link monitoring)
    - Terminal watchdog that continuously monitors the operational condition of the terminal
- Automatic Context Activation (ACA)
- With **M2M** SIM card only:
- Inmarsat M2M Access Platform
- Access to Inmarsat FTP server for firmware upgrade
- With **non-M2M** SIM card only:
- Streaming data rates of 32, 64 and 128 kbps
- Voice over IP (Standard voice 4 kbps AMBE+2 codec or Premium voice 3.1 kHz audio 64 kbps)
- IP66 protection
- Built-in web interface allowing you to manage connections and customize the terminal to your specific needs, using a computer
- Support for GPS, GLONASS and BeiDou navigation systems
- Optional cellular modem for dual mode operation
- Support for external 3rd party cellular modem/router via LAN connection
- For cellular operation: Optional PRISM technology (Private Routing & Intelligent System Management) for seamless and transparent data transfer independent of the network used (Cellular network or the BGAN backup connection)
- Dedicated connections (BGAN only)

## 1.2.2    Interfaces

There are no external connectors on the EXPLORER 540. The following interfaces are contained inside the compartment at the back of the EXPLORER 540:

- LAN interface with Power over Ethernet (PoE) input
- I/O ports for control of power save mode and for remote control/status
- Power input from:
  - PoE+ (IEEE 802.3at type 2 class 4, 25 W) or
  - separate DC power source, e.g. a battery (max. range 10.5-32 VDC)
- USB interface for connection to EXPLORER 540 Cellular Modem unit

For specifications on the interfaces, see *Interfaces specifications* on page A-2.

### Approvals/certificates

| Country | Approval / certificate |
|---|---|
| EU | CE |
| US | FCC |
| Canada | IC |
| Australia / New Zealand | RCM |
| Russia | Type approval certificate in the field of communications |
| Japan | Radio Law |
| International | GMPCS |
| International | C1D2 |
| International | Inmarsat Class 2 Type Approved and BGAN M2M Certified |

## 1.3     Your EXPLORER 540 terminal

### 1.3.1     EXPLORER 540 overview

The EXPLORER 540 is a small, compact unit comprising transceiver and antenna in one unit.

Antenna for
BGAN and
GNSS

Status LED

Cable glands for:

- LAN
- DC power
- Optional: Cable(s) for external cellular antenna(s) (when used with EXPLORER 540 Cellular Modem)

BGAN SIM card

Optional:
EXPLORER 540
Cellular Modem unit
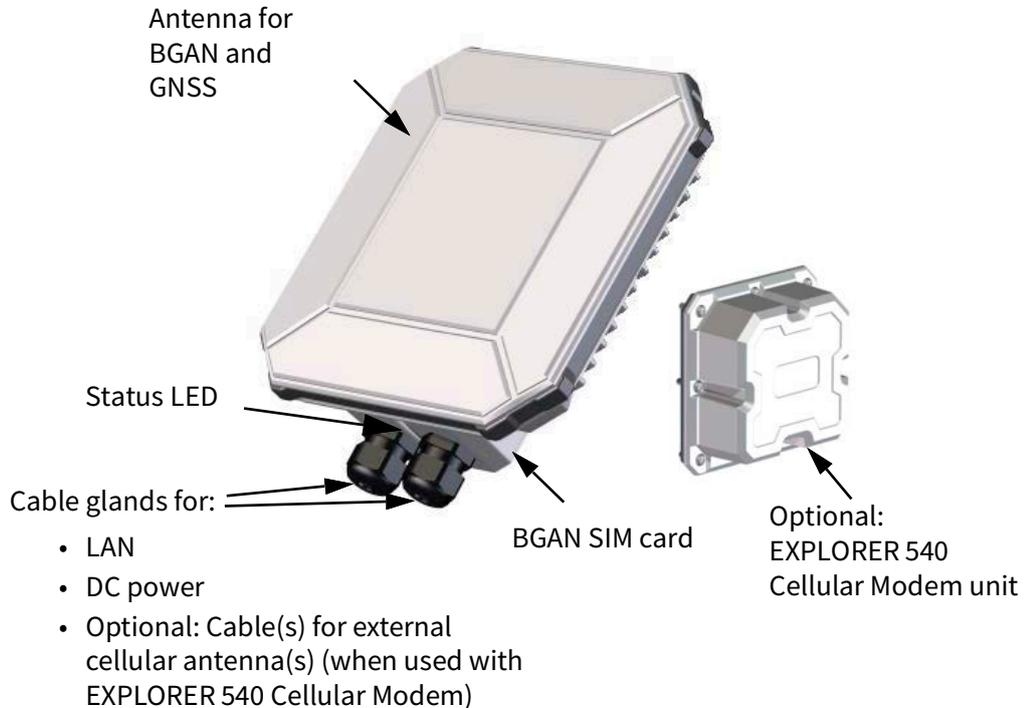
### 1.3.2     User interfaces

The **web interface** is a built-in web interface for easy configuration. The web interface is accessed from a computer connected to the EXPLORER 540, using an Internet browser. No installation of software is needed on the computer. For further information on the web interface, see *The web interface* on page 4-2.

With **AT commands** you can configure and control the EXPLORER 540 from a computer using a Telnet session, or from connected equipment, e.g. in M2M applications. For further details see *To access the terminal using AT commands* on page 3-3.

With **SMS commands** you can configure and control the EXPLORER 540 remotely. For details, see *Remote access with SMS* on page 3-4.

The distributors may have their own Graphical User Interface, which could be built on e.g. Inmarsat's M2M API (M2MAP) or similar. Contact your distributor for information.

### 1.3.3     Antenna

The light-colored front of the EXPLORER 540 holds the antenna part comprising:

- **GNSS** (Global Navigation Satellite System) antenna for GPS, GLONASS and BeiDou.
- **BGAN** antenna for the Inmarsat BGAN network.

**Cellular antenna(s)**: If you have purchased the EXPLORER 540 Cellular Modem option, the cellular modem is installed on top of the compartment on the back of the EXPLORER 540, connected internally with a USB cable and a DC cable. The antenna(s) for the cellular modem, however, are purchased separately and **installed externally**, connected with cable(s) to the modem. The EXPLORER 540 Cellular Modem with 3rd party embedded

modem and cellular antenna(s) provide connection to cellular networks. The type of cellular network used is depending on the purchased embedded module, which is to be installed in the EXPLORER 540 Cellular Modem.

If you are using an external 3rd party cellular modem/router connected to the LAN interface, see the documentation for the modem/router.

## 1.3.4    SIM card

The EXPLORER 540 requires a SIM card to go online with BGAN. Without a SIM card you can still configure the terminal, but you cannot make calls nor access the Internet.

Your SIM card determines whether your EXPLORER 540 is operating as an M2M terminal or as a BGAN class 2 terminal.

> **Note**  If you are going to use a cellular modem with your EXPLORER 540, a SIM card for cellular network must be installed in the cellular modem.

**SIM lock**: The supplier may have locked the SIM card to a specific provider. For further information, contact your supplier.

# 1.4    Services

## 1.4.1    BGAN services

The Inmarsat BGAN services are based on the BGAN I4 geostationary satellites and the Alphasat satellite. The map below shows the coverage area.
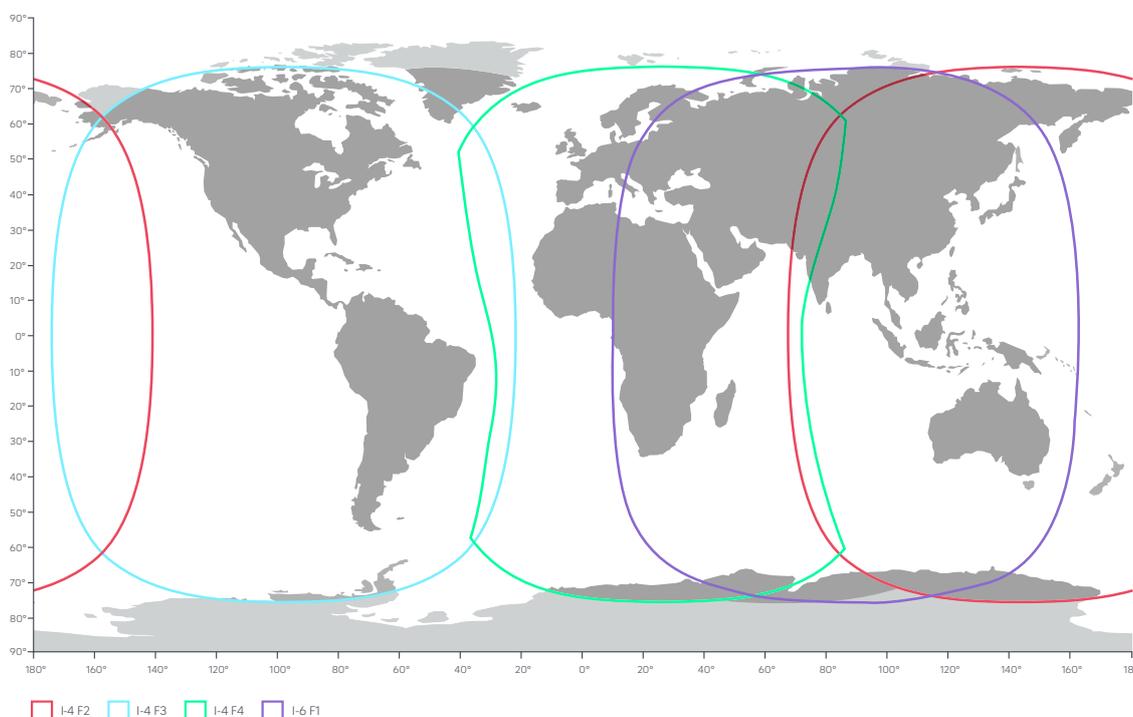


> **Note** | The services available depend on the SIM card installed in the EXPLORER 540. You can have A BGAN M2M subscription or a BGAN class 2 subscription.

### BGAN M2M services

BGAN M2M gives you a data connection to remote equipment and applications. With a BGAN M2M SIM card you have the following data capabilities:

- Standard data (background and interactive) up to 464 kbps/448 kbps.
- SMS for remote management.

**Not supported**: Streaming and voice calls.

### BGAN class 2 services

With a BGAN Class 2 SIM card you have the following data capabilities:

- Standard data (background and interactive) up to 464 kbps/448 kbps.
- Streaming data rates of 32, 64 and 128 kbps.

Via the EXPLORER 540 LAN interface, a SIP client (in a phone or M2M equipment) has the following voice capabilities:

- Standard voice 4 kbps AMBE+2 codec
- Premium voice 3.1 kHz audio 64 kbps

Additionally:

- SMS for remote management

For details about non-M2M functions, see *BGAN non-M2M functions* on page C-1.

## 1.4.2    Services with optional cellular modem

With the EXPLORER 540 Cellular Modem installed and one of the **Cellular modem preferred** settings selected, you have the following data capabilities (depending on the installed embedded modem):

**Supported:**

- **Data**: 2G (GSM), LTE-M, NB-IoT, 3G (UMTS), 4G (LTE).
  For specifications see *Optional EXPLORER 540 Cellular Modem* on page A-9.

**Not supported**:

- **Voice calls and SMS for remote management** are not supported via cellular connection, but will run on the standby BGAN connection when the EXPLORER 540 is in Cellular modem preferred or Cellular modem preferred (PRISM) mode.

- **Dedicated connections** are not supported in **Cellular modem preferred** nor **Cellular modem preferred (PRISM) mode**.

For details, see *Optional: To use a cellular network (dual mode)* on page 1-8.

# 1.5    Optional: To use a cellular network (dual mode)

The EXPLORER 540 is a BGAN terminal by default. However, if you are within coverage of a cellular network, you may want to acquire a cellular modem and use the cellular network as your primary connection. If you also install a PRISM server, you can have seamless and transparent data transfer independent of the network used (Cellular network or the BGAN backup connection).

| **Important** | If you are not using PRISM, you must enable the Connection watchdog before using the external modem. Otherwise the terminal will not be able to detect if the cellular connection is lost, and consequently will not switch over to BGAN backup. See *Connection watchdog (Link monitoring)* on page 4-34. |

You can use one of the following:

- *EXPLORER 540 cellular modem*, or
- *External cellular modem via LAN*

## 1.5.1    EXPLORER 540 cellular modem

In order to support as many applications, locations and certifications as possible, the EXPLORER 540 Cellular Modem is provided as a modular solution, with different options for the embedded modem. Acquire:

- One of the below EXPLORER Modem Bundles, **and**
- one or two EXPLORER Cellular Antenna(s), depending on the selected modem bundle.

The following options are available from Cobham SATCOM.

| Part number | Product |
|---|---|
| 403715A-00212 | EXPLORER Modem Bundle LTE Cat 4 EU |
| 403715A-00214 | EXPLORER Modem Bundle 4G LTE-M Global |
| 403715A-00215 | EXPLORER Modem Bundle 3G GLOBAL HSPA+ |
| 403715A-00220 | EXPLORER Modem Bundle LTE Cat 4 US (AT&T) |
| 403715A-00221 | EXPLORER Modem Bundle LTE Cat 4 US (Verizon) |
| 403715A-00222 | EXPLORER Modem Bundle LTE Cat 1 (US) |
| 403715A-00105 | EXPLORER Cellular Antenna |

| **Note** | To access the cellular network you need a separate **SIM card for the cellular modem**, the EXPLORER 540 SIM card can only be used for the BGAN network. |

You install the EXPLORER 540 Cellular Modem as an integrated part of the EXPLORER 540, but with the cellular antenna(s) installed externally, connected with cable(s).

> **Note** Install the cellular antenna(s) min. 2 m. away from the EXPLORER 540, not in front of the EXPLORER 540 BGAN antenna and not pointing through the EXPLORER 540.

Cellular antennas

EXPLORER 540 Cellular Modem (integrated)
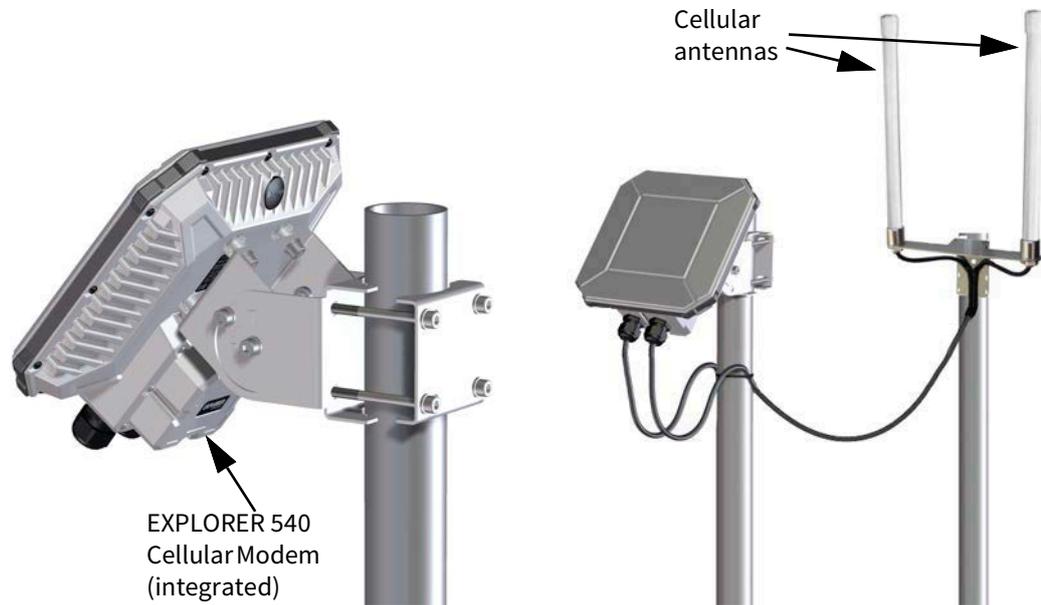
For installation of the EXPLORER 540 Cellular Modem, see the installation guide that comes with the modem.

For configuration, see *Optional: To set up cellular network for data (dual mode)* on page 4-48.

## 1.5.2 External cellular modem via LAN

Instead of the EXPLORER 540 Cellular Modem you can purchase a stand-alone 3rd party cellular modem/router with LAN interface and connect it to the EXPLORER 540 LAN interface.

For configuration, see *To set up the EXPLORER 540 for cellular operation* on page 4-48.

# 1.6　System overview

## 1.6.1　Power supply and additional equipment

There is one LAN interface and one DC power input on the EXPLORER 540.

> **Note** The EXPLORER 540 works as a Powered Device (PD). This means it may be powered by PoE, but it does **not** supply PoE.

Depending on your configuration, you may have to use a PoE switch or a PoE injector connected to the LAN interface or a battery connected to the DC input in order to provide power to the EXPLORER 540.

> **Note** If you are using a cellular modem, you cannot use PoE to power the system. Use the DC input instead.

For examples, see *M2M application examples* on page 2-11. You may also need to provide a switch to be able to accommodate more than one LAN connection, e.g. for local access to the web interface during installation or service.

## 1.6.2　M2M overview, example

In the example below, the M2M system has a built-in PoE switch, providing the power to the EXPLORER 540 together with the M2M communication through the LAN interface.
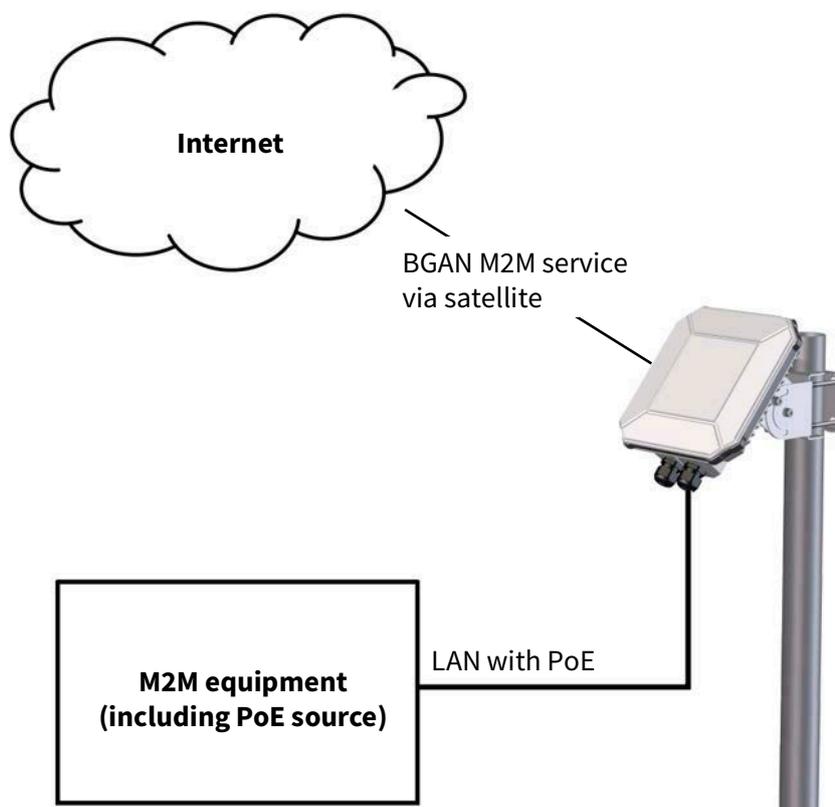
# To get started

This chapter describes:

- *To unpack the EXPLORER 540*
- *SIM card*
- *Cable connections*
- *Fixed installation of the EXPLORER 540*
- *To power the EXPLORER 540*
- *Installation process*
- *To access the web interface*
- *M2M application examples*

## 2.1    To unpack the EXPLORER 540

### 2.1.1    Initial inspection

Inspect the shipping carton immediately upon receipt for evidence of damage during transport. If the shipping carton is severely damaged or water stained, request that the carrier's agent be present when opening the carton. Save the carton packing material for future use.

| ⚠ | **WARNING!** | To avoid electric shock, do not apply power to the system if there is any sign of shipping damage to any part of the front or rear panel or the outer cover. Read the safety summary at the front of this manual before installing or operating the system. |
|---|---|---|

After unpacking the system, inspect it thoroughly for hidden damage and loose components or fittings. If the contents are incomplete, if there is mechanical damage or defect, or if the system does not work properly, notify your dealer.

### 2.1.2    What's in the delivery

The following items are included in the delivery:

- EXPLORER 540 terminal
- Pole mount kit
- 2 standard cable glands
- 2 C1D2 approved cable glands (for C1D2 operation, hazardous locations)
- 1 Blanking plug
- Torx bit for mounting/dismounting the cover for the interface enclosure
- Installation guide for EXPLORER 540

## 2.2    SIM card

### 2.2.1    SIM card for BGAN operation

The BGAN SIM card determines whether the terminal operates as an M2M terminal or a BGAN class 2 terminal.

> **Important** Do not insert or remove the SIM card while the EXPLORER 540 is powered!

You insert the SIM card before installing the EXPLORER 540. The picture below shows the location of the SIM card holder, in the interface enclosure at the back of the terminal.



For details on how to insert the SIM card, see the installation guide.

### 2.2.2    Optional: SIM card for cellular operation

If you are using the optional EXPLORER 540 Cellular Modem, it must have a SIM card for cellular network installed. For details, see the Installation guide that comes with the EXPLORER 540 Cellular modem.

## 2.3 Cable connections

There are no external connectors on the EXPLORER 540. All cable connections on the EXPLORER 540 are made during installation.

Remove the 8 screws from the small cover at the back of the terminal and take off the cover. Then connect the cables to the relevant terminals or connectors. Two standard cable glands and two C1D2 approved cable glands with gaskets are provided for the cables.

> **Note** For C1D2 operation, use C1D2 approved cable glands, e.g. the supplied cable glands with Cobham Part no 32-207214-612.
>
> Note that a LAN connector cannot pass through the C1D2 approved cable gland.
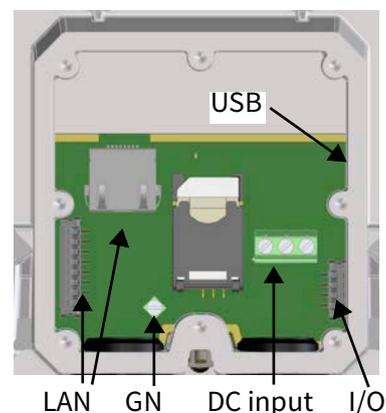
**After making all connections, remount the 8 screws for the small cover and tighten to torque 0.5 Nm/ 4.5 lbf in.**

See *Interfaces specifications* on page A-2 for specifications and pin-out for the interfaces.

See the section below for instructions specific to the DC input.

See the EXPLORER 540 Installation guide for details on how to connect cables.

> **Note** If you are going to use the optional EXPLORER 540 Cellular Modem, connect the modem to the USB connector and to DC power in the interface enclosure of the EXPLORER 540. For details see the installation guide included with the EXPLORER 540 Cellular Modem.

### 2.3.1 Instructions for power input

Use one of the following power sources (connected at installation, see the Installation guide):

- PoE+ via the LAN interface
- 12 or 24 VDC nominal, e.g. from a battery (absolute maximum rating 10.5-32 VDC)

> **Note** When you use the EXPLORER 540 with the cellular modem, a separate DC supply is required instead of PoE in order to supply sufficient power for the modem as well as the EXPLORER 540.

### Requirements for DC input

Observe the following requirements for connecting to the DC input:

- Power supply: Fuse the power source with a fuse rated 6 A when the input voltage range is 10.5 VDC to 16 VDC; and rated at 3 A when the input voltage range is >16 VDC to 32 VDC.
- Cable requirements:
  - Wire size 1.5 mm$^2$/ 15 AWG, copper
  - Torque for screw terminals: 0.5 N m/ 4.5 lbf in
  - Temperature rating: Min. 105 °C/ 221°F
  - Max. length: 12 m/ 39 ft at 12 VDC, 200 m/ 656 ft at 24 VDC
  - UV resistant cable

## Requirements for LAN (PoE) input

Observe the following requirements for connecting power to the LAN input:

- Must comply with the requirements for **PoE+ IEEE 802.3at type 2 class 4.**
- Cable requirements:
  - Temperature rating: Min. 95 °C/ 203°F
  - PoE+ mode A and/or B (both are supported, see *Connector pin-out* on page A-2)

## To connect to the DC input

> ⚠ **CAUTION!** Make sure there is no power on the cables while you connect them to the EXPLORER 540.

Use a flat blade screw driver (max. 3.5 mm/ 0.14" wide) to unscrew and fasten the screw terminals. Do as follows:

1. Lead the cable through the cable gasket at the DC input.
2. If the DC cable is shielded, insert the end of the shield into the screw terminal **3-GND** in the DC terminal block and tighten the screw to torque 0.5 N m/ 4.5 lbf in.

> ⚠ **CAUTION!** 3-GND is only for connection of shield! Do **not** connect the positive or negative wire to 3-GND!

3. Insert the **negative wire** into the terminal marked **2-DCIN-** in the DC terminal block and tighten the screw to torque 0.5 N m/ 4.5 lbf in.
4. Insert the **positive wire** into the terminal marked **1-DCIN+** in the DC terminal block and tighten the screw to torque 0.5 N m/ 4.5 lbf in.
5. Tighten the cable gland.
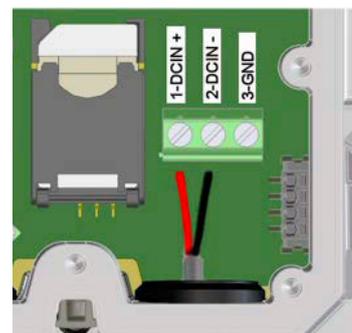
> **Important** ▶ If you are using the EXPLORER 540 Cellular Modem, the antenna cable(s) go through the same cable gland as the DC input. In that case, use cable glands of Ø3.2 mm (RG316) and add silicone glue inside the cable gland gasket to make sure that the cable gland is waterproof before tightening the cable gland. It is vital for the life of the product that the cable gland is waterproof!

## 2.4    Fixed installation of the EXPLORER 540

To install the EXPLORER 540 in a fixed installation, use the pole mount kit included in the delivery.



For details on how to install the EXPLORER 540, see the included installation guide.

**Important** ▶ | Make sure all cables are connected and the *Installation process for satellite operation* is completed before you fasten the EXPLORER 540 in your fixed installation.

## 2.5    To power the EXPLORER 540

The EXPLORER 540 has no power switch, but is automatically switched on when power is applied to the DC input or the LAN interface (PoE).

For details how to connect power, see *Instructions for power input* on page 2-3.

## 2.6     Installation process

### 2.6.1     Physical installation

See also the supplied Installation guide.

A pole mount kit is included in the delivery. To mount the
EXPLORER 540 on a pole, do as follows:

1.  Attach the base of the pole mount bracket to the
    EXPLORER 540 using the included Hex L key on the 4
    screws.
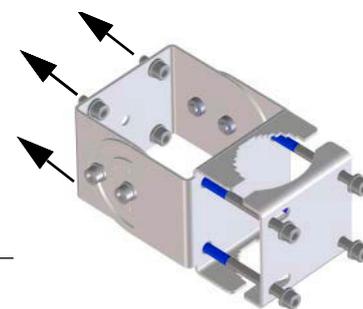
| ⚠ | **CAUTION!** | Max. length of the screws is 9 mm/ 0.35"! Longer screws can damage the EXPLORER 540. |
|---|---|---|

| ⚠ | **CAUTION!** | For continual and thorough protection of the equipment, ensure that the pole for the EXPLORER 540 is properly grounded. |
|---|---|---|

2.  Unscrew two of the long screws from the pole mount kit
    to leave one side open for the pole.
3.  Place the pole mount kit with the EXPLORER 540 around
    the pole as shown. Note that the cables and cable entry
    gaskets are always on the bottom.

    | Note | The pole mount kit is designed for 1" to 1.5" poles (outer diameter 33.7 to 48.3 mm). |
    |---|---|

4.  Remount the two remaining long screws. Do not tighten the screws completely until you
    have pointed the antenna.

### 2.6.2     BGAN or cellular network

The EXPLORER 540 is a BGAN terminal. However, if you have purchased the EXPLORER 540
Cellular modem option or a stand-alone cellular modem with LAN interface, you can use the
cellular network when it is available, with BGAN as backup. See *Optional: To use a cellular
network (dual mode)* on page 1-8.

To use the BGAN network, you must first point the antenna in the direction of the satellite
and find the best possible signal strength. For fixed installation you only have to do this once.
See the next sections for details.

## 2.6.3    Pointing

Before pointing the antenna you can use the coverage map below to find your approximate location in relation to the satellites. Pointing is part of the Installation procedure described in the next section.

The Inmarsat satellites are positioned above the equator, at the center of each "footprint".
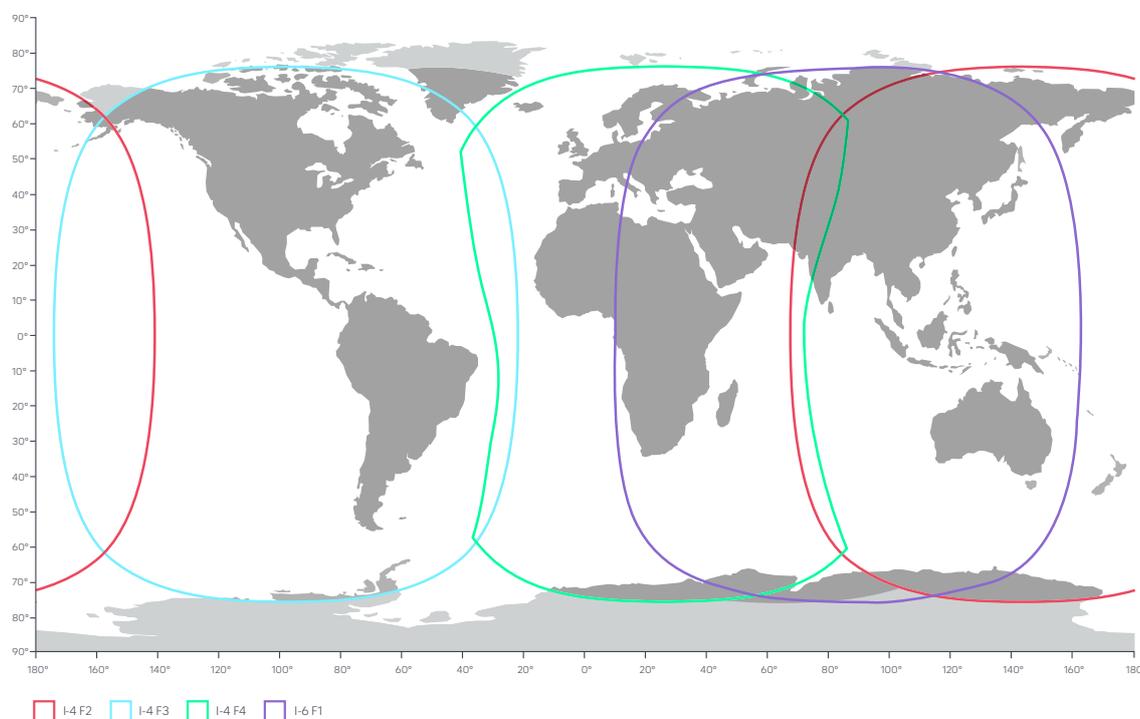


## 2.6.4    Installation process for satellite operation

> **Note** **PIN code:** Normally you are not required to enter a PIN code for the BGAN service, because the SIM PIN is either disabled or set up for automatic validation. However, if the PIN is enabled and not set up for auto validation, you have to enter the PIN before you can access the BGAN network. For details, see *To enter the SIM PIN in the web interface* on page 4-47.

> **Note** **APN:** By default, the terminal is set up to use the APN from the SIM card. However, if the SIM card requires a user defined APN, the installation process will fail, because the APN is not defined. If this is the case, use the web interface to enter the APN and restart the installation. For details, see *To change the APN for a connection package* on page 4-6 and *To restart the installation process (BGAN)* on page 4-13.

The installation process starts up automatically when you apply power to the EXPLORER 540. The process is as follows:

1.  Apply power to the EXPLORER 540 from a separate power supply or from a PoE source. The light indicator (LED) between the two cable glands shows the status during startup.[1]
    - Green flashing rapidly: Starting up
    - Yellow flashing: BGAN pointing

---

1.  If you have a computer connected to the EXPLORER 540, you can follow the process in the web interface, see *To restart the installation process (BGAN)* on page 4-13.

2. When the LED flashes yellow and you hear the pointing sound, you can start pointing the antenna.

3. Turn and tilt the EXPLORER 540 until you have obtained the highest possible signal strength (when the pointing sound is continuous you have the optimum signal, see the next section *Audio assisted pointing*).

4. Tighten the screws to fix the EXPLORER 540 in the pointed position. When the signal has been stable for about 60 seconds[1] the pointing procedure automatically ends, and the terminal attempts to register on the network and verify the satellite connection (LED flashing green).

LED

> ⚠ **CAUTION!** When the connection is established, keep the minimum safety distance of **1 m/ 3.2 ft from the antenna front face**. The antenna radiates microwave power as soon as the pointing procedure is completed.

5. When installation is completed successfully, the LED turns steady green and then, after a few minutes, the light goes off. If you have enabled Automatic Context Activation, the data connection is established automatically.

> **Note** The LED is **off** after successful installation. The LED only comes on again during reboot or if you restart installation.

> **Note** If the LED is steady yellow after pointing, it means the installation failed. See *Troubleshooting* on page 5-5.

6. The EXPLORER 540 is now ready for use. For details on how to access the EXPLORER 540 from a remote location, see *To access the terminal from a remote location* on page 3-4.

After successful installation, the EXPLORER 540 will automatically register on the BGAN network at every power-up and, if Automatic Context Activation is enabled, establish a data connection again. This is also the case following one of the "wake-on" actions after power save.

## Audio assisted pointing

By default, the EXPLORER 540 uses a pointing sound to indicate the signal level during the pointing procedure (Audio assisted pointing). The sound pattern is as follows:

- Poor signal strength:    •    •    •    •
- Good signal strength:    ••••••••••••••••••
- Optimum signal strength: ▬▬▬▬▬▬▬▬▬ (continuous sound instead of single "beeps")

You can disable the pointing sound using the web interface. For details, see *To enable or disable the pointing sound* on page 4-19.

---

1. If the terminal detects a signal but the signal is not stable, it will stop the pointing process after 8 minutes and proceed with the installation process. If no signal is detected within 10 minutes, the pointing and installation process will stop and the installation status will be shown as failed.

## To repoint the antenna

You may need to point the antenna again later, e.g. if the terminal has been moved or the signal is blocked.

To start the installation process again, you can do one of the following:

- Use the web interface (  (Control panel) and then **Installation)**. See *To restart the installation process (BGAN)* on page 4-13.
- Reset the EXPLORER 540 using the Reset button inside the interface enclosure on the back of the terminal. See *Reset button* on page 5-4.

## 2.6.5    Do you need a PIN? (BGAN)

> **Important** | If your EXPLORER 540 is used in an unmanned M2M system, you will not be able to enter a PIN code. In this case we strongly recommend enabling **Auto SIM PIN validation** in the web interface before using the system. See below.

**To avoid having to enter a PIN** at startup, you have two options:

- Enable **Auto SIM PIN validation**. See *Auto SIM PIN validation* on page 4-32.
  With this option enabled, the EXPLORER 540 automatically sends the PIN to the SIM card at every startup. Note that if you later want change the SIM card, you should first disable Auto SIM PIN validation.
- Disable the use of a SIM PIN. See *To enable or disable the use of a SIM PIN* on page 4-31.
  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 *To enter the SIM PIN* on page 4-47.

> **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.

## 2.7    To access the web interface

You can use the built-in web interface for configuration and operation of the EXPLORER 540. To access the web interface, do as follows:

1. Start up the terminal.
2. Connect your computer to the LAN interface of the terminal. If the terminal is already installed in your system, you must connect via a router or switch, because there is only one LAN interface on the EXPLORER 540.
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. Log in as user or administrator. Default user names and passwords are:
   - **user**: User name = **user**, password = <**serial number of the EXPLORER 540**>
   - **administrator**: User name = **administrator**, password = **admin**

   Note | If you logged in as administrator with the default password, you are immediately prompted to type in a new administrator password.  Type in the new administrator password twice and click **OK**.

If the terminal is not yet installed, it will automatically start the installation procedure and the web interface will show the progress. Otherwise the web interface will show the dashboard.

For more information on the web interface, see *The web interface* on page 4-2.

## 2.8    M2M application examples

When an M2M SIM card is installed, the EXPLORER 540 uses the BGAN M2M service (see *BGAN M2M services* on page 1-6).

If a PoE switch is not included in the connected M2M equipment, you must provide power either through the LAN interface with a PoE injector or a PoE switch connected, or from a battery connected to the DC input. The following sections show examples.

### 2.8.1    Separate battery supply

Another example is the scenario below, where power is supplied from a separate battery connected to the DC input of the EXPLORER 540. This solution may be used e.g. if you want to limit the power consumption, or if a PoE source is not available. For specifications and pinout for the DC input on the EXPLORER 540, see *DC power input (X4)* on page A-4.

For installation instructions, see the supplied EXPLORER 540 Installation guide. Note that you must use a fused or current-limiting DC power supply (battery).
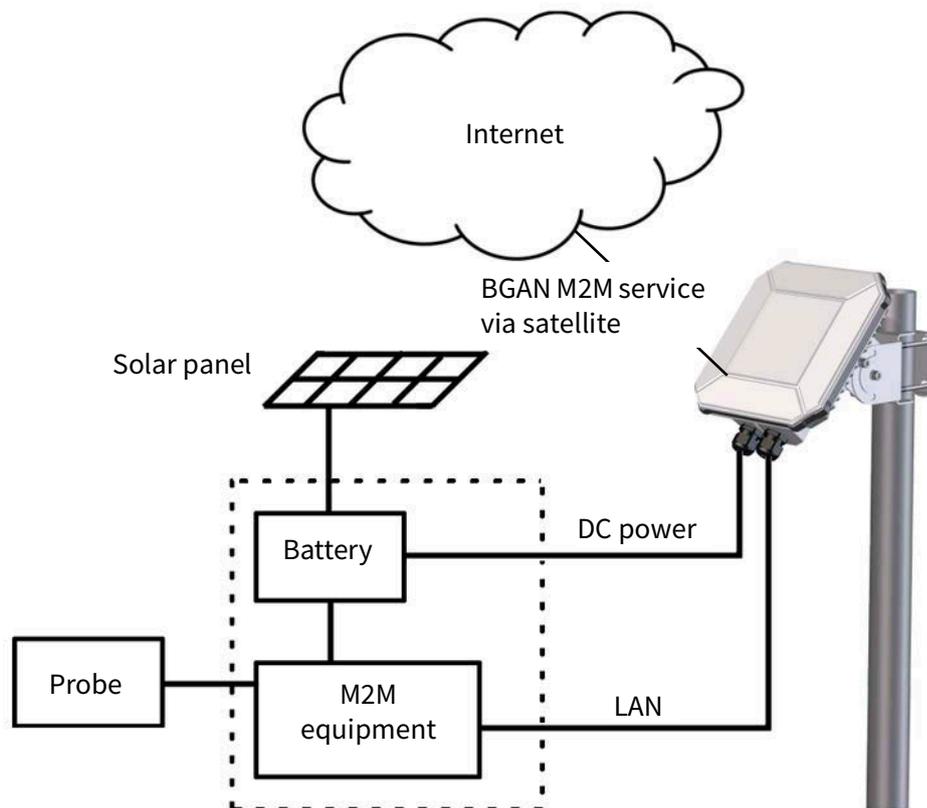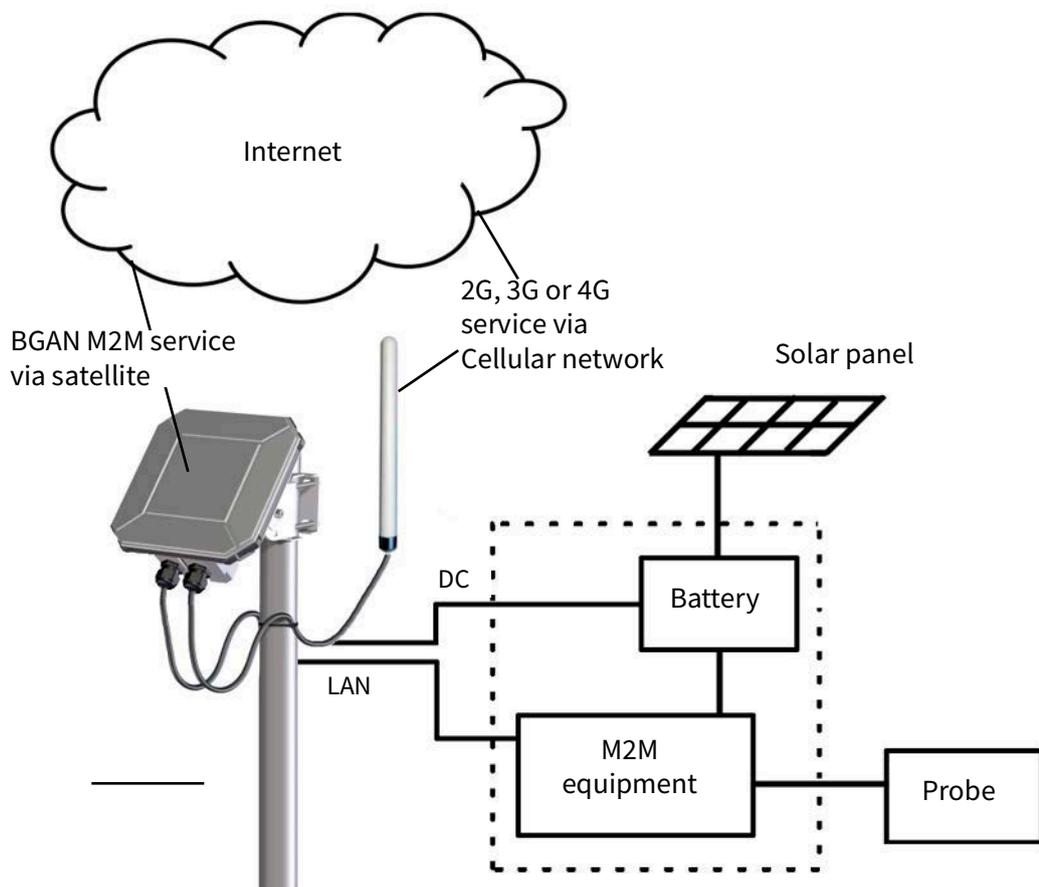
## 2.8.2     Dual mode

### Dual mode with EXPLORER 540 Cellular Modem

In the scenario below, an EXPLORER 540 Cellular Modem is used to provide connection to a cellular network while the BGAN connection is used for backup. Power is supplied from a separate battery connected to the DC input of the EXPLORER 540, in order to provide enough power for both the EXPLORER 540 and the cellular modem.

- For specifications and pinout for the DC input on the EXPLORER 540, see *DC power input (X4)* on page A-4.
- For installation instructions for the EXPLORER 540 terminal, see the supplied EXPLORER 540 Installation guide. Note that you must use a fused or current-limiting DC power supply (battery).
- For installation instructions for the EXPLORER 540 Cellular Modem, see the guide included with the EXPLORER 540 Cellular Modem.

> **Note**  In addition to the EXPLORER 540 Cellular Modem, which is purchased as a bundle with an embedded modem, you must purchase cellular antenna(s) matching the embedded modem.

- For dual mode configuration of the EXPLORER 540 terminal, see *Optional: To set up cellular network for data (dual mode)* on page 4-48.

## Dual mode with external cellular modem/router

As an alternative to the EXPLORER 540 Cellular Modem you can use an external 3rd party cellular modem/router connected to the LAN interface.

In the scenario below, an external cellular modem/router is used to provide connection to a cellular network while the BGAN connection is used for backup. Power is supplied from a separate battery connected to the DC input of the EXPLORER 540 and to the external cellular modem/router.

- For specifications and pinout for the DC input on the EXPLORER 540, see *DC power input (X4)* on page A-4.
- For specifications and pinout for the LAN input on the EXPLORER 540, see *LAN interface (X1 or X2)* on page A-2.
- For installation instructions for the EXPLORER 540 terminal, see the supplied EXPLORER 540 Installation guide. Note that you must use a fused or current-limiting DC power supply (battery).
- For installation instructions for the external modem/router, see the documentation for the modem/router.
- For dual mode configuration of the EXPLORER 540 terminal, see *Optional: To set up cellular network for data (dual mode)* on page 4-48.
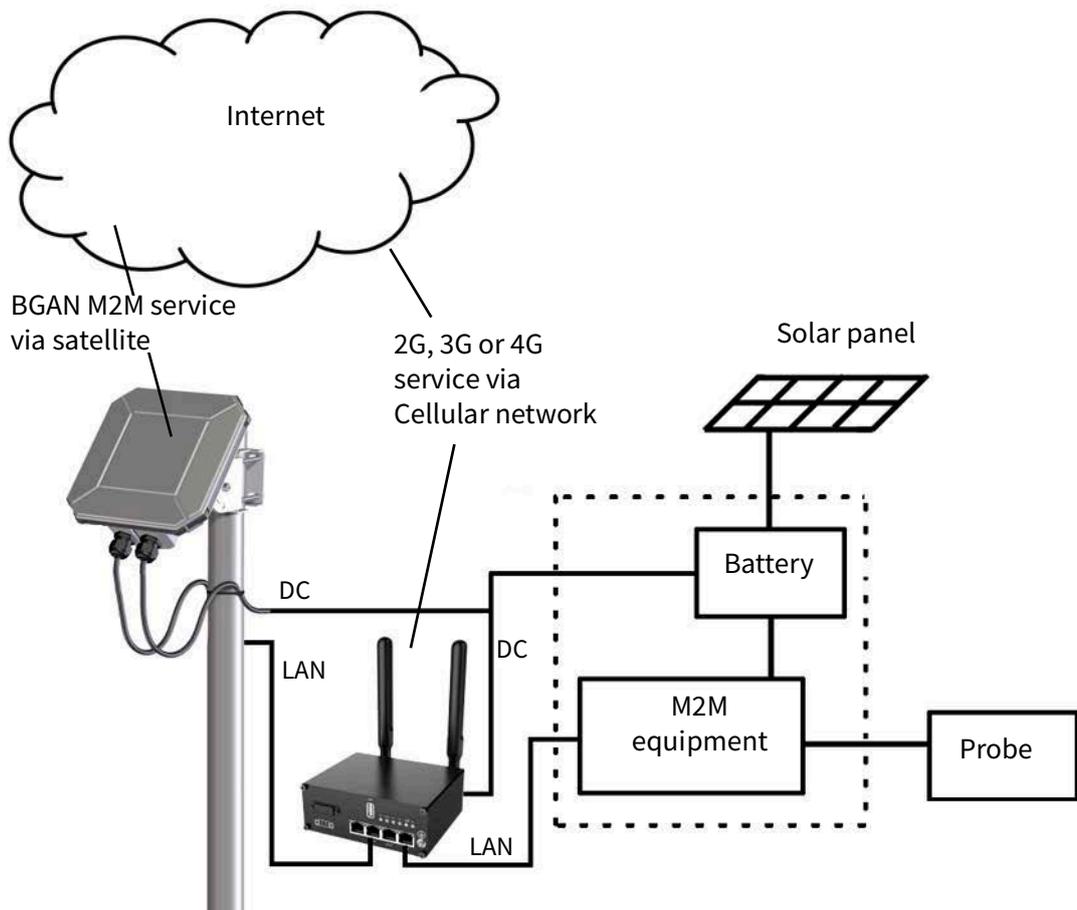
## 2.8.3    PoE injector

The picture below shows an example of an M2M application using a PoE injector to provide the power to the EXPLORER 540 through the LAN interface. Note that the PoE injector must comply with the requirements for **PoE+ IEEE 802.3at type 2 class 4**. The PoE injector is connected to a power supply and "adds" power to the LAN connection for the EXPLORER 540. For specifications and pinout for the LAN interface on the EXPLORER 540, see *LAN interface (X1 or X2)* on page A-2.
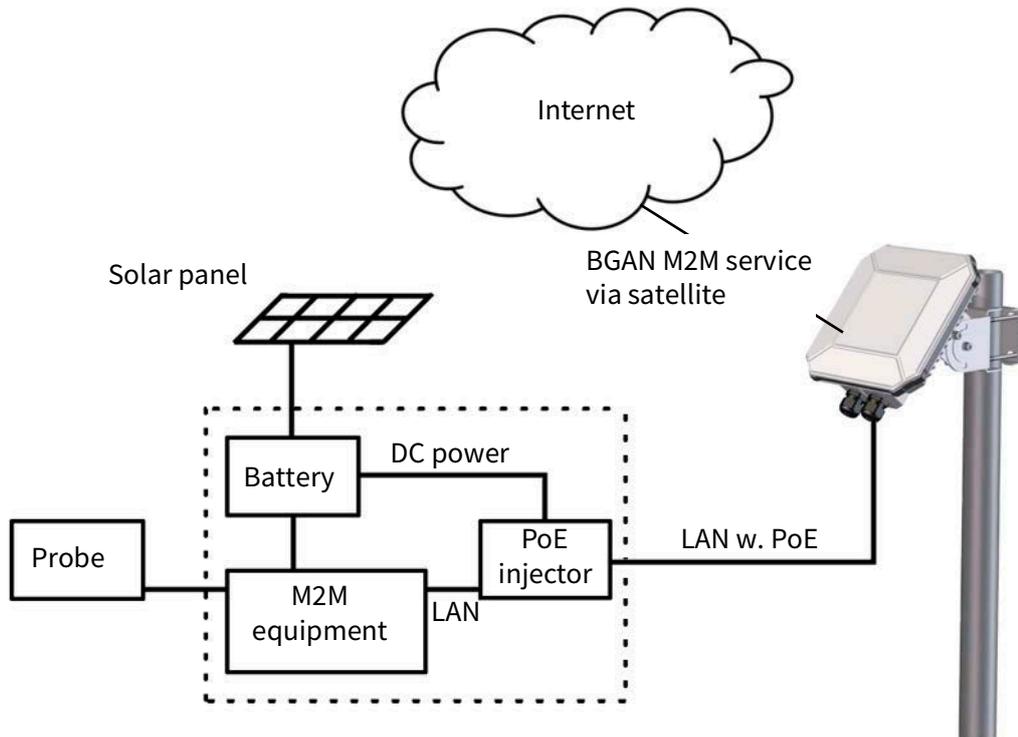
## 2.8.4    I/O pins

The EXPLORER 540 has 3 I/O pins: two assigned pins and 1 general purpose pin.

- 1-GPI: Power control pin (input)
  Controls whether the terminal should go into power save mode or stay on. Configurable in web interface (active high/low)
  See *Power control* on page 3-19 and *Remote on/off mode* on page 4-43.
- 2-GPO: Terminal ready (output)
  Signals when the terminal is powered on and logged onto the BGAN network. Configurable in web interface (active high/low).
  See *Terminal ready signaling with 2-GPO* on page 3-28.
- 3-GPIO: General purpose input/output
  Configurable in web interface. Using an AT command, you can activate this pin (when configured as output) or get the status of this pin (when configured as input).
  See *Control or status with 3-GPIO* on page 3-29.

For details, see also:

- **Configuration with web interface**: *GPIO pins* on page 4-44.
- **Pinout and specifications:** *I/O connector (X5)* on page A-5.
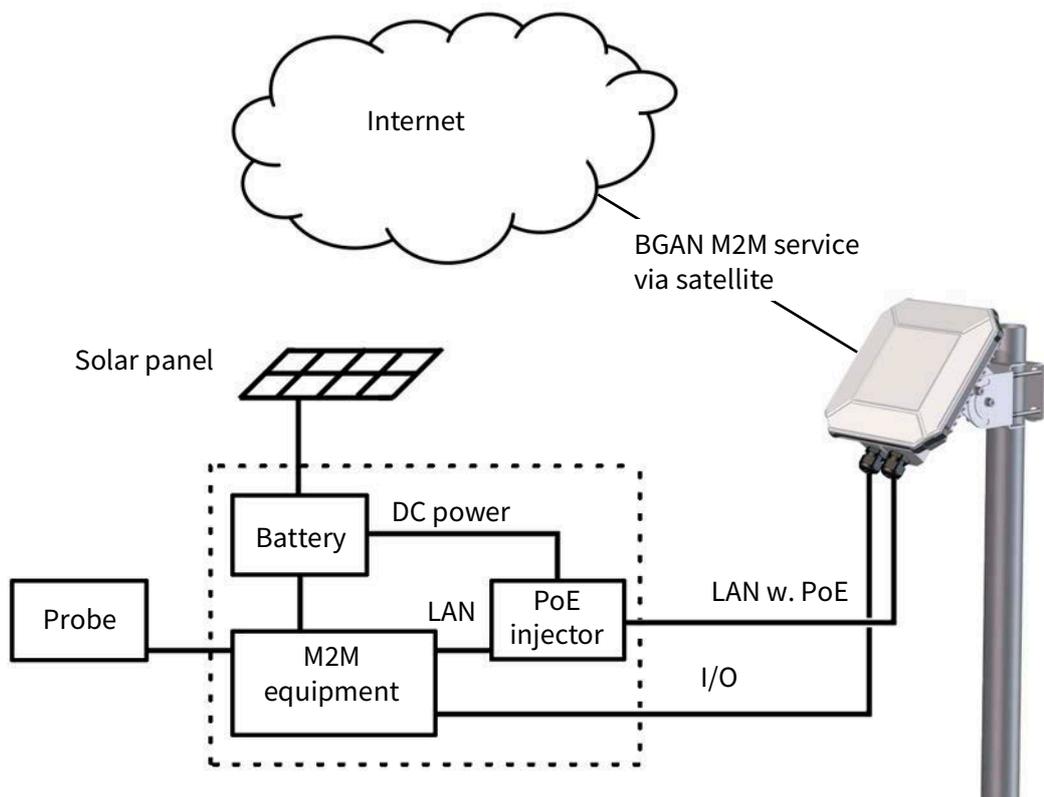
# Operation

This chapter describes operation and basic setup, primarily for M2M use.

For information on **configuration** with the web interface, see *Configuration with web interface* on page 4-1.

This chapter describes:

- *Local or remote control*
- *To access the terminal using AT commands*
- *To access the terminal from a remote location*
- *Security setup*
- *To control data connections (PDP contexts)*
- *Power control*
- *Remote software upgrade*
- *File transfer*
- *Status of the EXPLORER 540*

For information on functions that are **not** available with an M2M subscription but only with a standard BGAN subscription, see *BGAN non-M2M functions* on page C-1.

For information on setting up **dual mode (cellular and BGAN)**, see:

- Using web interface: *Optional: To set up cellular network for data (dual mode)* on page 4-48
- Using AT commands: *AT commands for dual mode with cellular modem* on page B-19.

# 3.1    Local or remote control

The EXPLORER 540 can be controlled both locally using the LAN interface and from a remote location over the BGAN network or optionally the cellular network. For M2M operation, remote control is essential, since the EXPLORER 540 is most likely installed in a remote location where local human access is rare and maybe difficult.

Note that different levels of access control apply to different means of access. See *Security setup* on page 3-12.

You have the following options:

**Local control:**

- web interface: Connect a computer to the LAN interface and use a browser to access the built-in web interface. See *Configuration with web interface* on page 4-1.

- AT-commands: Connect equipment capable of issuing AT commands to the EXPLORER 540 (e.g. in an M2M application) or connect a computer to the LAN interface and use a terminal program to send commands to the EXPLORER 540. See *To access the terminal using AT commands* on page 3-3.

**Remote control**:

- SMS commands: You can use SMS commands e.g. to start and stop your data connection and send and receive AT commands to and from the terminal. See *Remote access with SMS* on page 3-4.

   > **Note** | The SMS commands will always use the BGAN connection, even if the terminal is in Cellular modem preferred mode.
   >
   > If the terminal is in Cellular modem preferred mode you cannot start and stop data connections.

- AT commands: When a data connection is established you can control the EXPLORER 540 with AT commands over the BGAN satellite network or optionally the cellular network. See *To access the terminal from a remote location* on page 3-4 and *To access the terminal using AT commands* on page 3-3.

   > **Note** | In Cellular modem preferred mode you cannot use the context management AT commands.

- web interface: When a data connection is established you can control the EXPLORER 540 over the BGAN satellite network or optionally over a cellular network by accessing the built-in web interface. See *Remote access to the web interface* on page 3-10.

- The distributors may have their own Graphical User Interface, which could be built on e.g. Inmarsat's M2M API or similar. Contact your distributor for information.

## 3.2    To access the terminal using AT commands

> **Important**  Before putting the EXPLORER 540 into operation, remember to set up the security features in order to avoid unintended use. See *Security setup* on page 3-12.

The EXPLORER 540 supports a number of M2M specific AT commands as well as a set of general AT commands. For a list of the most common commands, see *AT commands* on page B-9.

AT commands can also be encapsulated in an SMS sent to (and from) the terminal's phone number. See *Remote access with SMS* on page 3-4.

1. Connect your computer (or other equipment) to the EXPLORER 540 terminal.
   You may connect locally to the terminal or use a remote connection.
2. On the connected computer, start a Telnet session.
3. Select TCP/IP and type in the IP address and port number.
   - For **local connection**, use the local IP address of the EXPLORER 540 (default 192.168.0.1) and port number 5454.
   - For **remote connection**, use the external IP address[1] of the terminal. The port number for AT commands is normally 5454 but can be changed in the web interface **Remote management** page under **AT commands** (see *Remote management* on page 4-38).
4. When the connection is established, type in your AT commands. Note that you have to enter the administrator password using the AT_ICLCK command. See *Security setup* on page 3-12.

---

1. The external IP address is found in one of the following ways:
   1. If you are using SMS activation, you will receive an SMS with the IP address.
    See *ACTIVATE: Activate a data connection with an SMS (BGAN only)* on page 3-5
   2. Otherwise, you can use the GETINFO (ALL) command to obtain the external IP address, if you already have a session running.
   This is the IP address you must use to access the terminal.
   Note: If Static IP is included in your airtime subscription, we recommend using this static public IP address for the terminal in order to provide easy access to the terminal. To use the static IP address, you must set the APN source to SIM default. For details, see *To change the APN for a connection package* on page 4-6.
   If you are using a cellular connection, the best way to access the global IP address of the terminal is to use PRISM. See *To set up the connection mode* on page 4-16 and *To set up PRISM* on page 4-55

# 3.3    To access the terminal from a remote location

## 3.3.1    Remote access with SMS

**Important** ▶ By default, anyone can access the EXPLORER 540 with an SMS, if they have the phone number of the terminal and the remote SMS password. Before installing the EXPLORER 540 you should set up the security measures for the terminal. See *Security setup* on page 3-12 and *To set up remote access with SMS* on page 4-40.

You can perform a number of actions and some configuration on the EXPLORER 540 using SMS commands.

**Note** ▶ If you are using a cellular connection as your primary network connection, the SMS commands will be sent over the BGAN backup connection.

**Send an SMS** to the mobile number of the terminal. The text in the SMS must start with the SMS command and follow the syntax for the SMS commands. Note that the remote SMS password (default: **remote**) must be included with every command.

**For an explanation of syntax and parameters,** see *SMS remote commands* on page B-4. Note that the remote SMS function is password protected.

The following SMS commands are supported.

| SMS command | Function |
|---|---|
| ACTIVATE[1] | Activates BGAN data connections for the device(s) connected to the EXPLORER 540. |
| DEACTIVATE[a] | Deactivates some or all the BGAN data connections for devices connected to the EXPLORER 540. |
| CLEAR | Deletes SMS messages in the EXPLORER 540. |
| GETINFO | Gets current information from the EXPLORER 540 such as call time, data usage, GPS position and global IP address. |
| RESTART | Restarts the EXPLORER 540. |
| WATCHDOG | Gets or sets the current Connection watchdog parameters (Link monitoring). |
| ADVWATCHDOG | Gets or sets the current Terminal watchdog parameters. |
| ATCO | Allows you to send M2M related AT commands to the EXPLORER 540 which returns the response in an SMS. |
| ADPWRST | Resets the EXPLORER 540 admin password to **admin.** |
| WANMODE | Gets or sets the WAN connection mode (BGAN only, Cellular modem preferred, Cellular modem preferred (PRISM), External modem preferred or External modem preferred (PRISM)) |

1. These commands cannot be used in Cellular modem preferred mode, Cellular modem preferred (PRISM) mode, External modem preferred mode nor External modem preferred (PRISM) mode.

The next sections show examples of each SMS command.

| Note | The following examples use the default remote SMS password, which is **remote**. the password may be different in your EXPLORER 540. |

## ACTIVATE: Activate a data connection with an SMS (BGAN only)

The text in the activation SMS must have the following format for activating a connection:

```
ACTIVATE 1 {DHCP|STATIC|<name>|<IP addr>|ANY} {NA|<apn>}
{NA|<apn_user>} {NA|<apn_pwd>} <rsms_pwd>
```

**Example:** To activate one or more connections for remote management for connected equipment with IP address(es) assigned by DHCP, using default settings (NA) for APN, APN user name and APN password, send an SMS to the terminal with the text:
**ACTIVATE 1 DHCP NA NA NA remote**

**Response:**
You receive a response with the IP address you must use to access the terminal from a remote location.

**Example:** A confirmation SMS after sending an activation SMS may look like this:
```
IP: 161.30.181.31 (192.168.128.104)
SMS-Free: 88/100
WARNING: Ensure SMS-free > 5. Cleanup old msgs for
orderly remote-SMS-control
```

The first IP address is the global IP address assigned to the PDP context by the network, and the second IP address (in parenthesis) is the IP address (or host name, if the device was identified by host name) of the device connected on the local LAN, for which the PDP context was created.

## DEACTIVATE: Deactivate a data connection (BGAN only)

The text in the deactivation SMS must have the following format for deactivating a connection:

```
DEACTIVATE 1 {DHCP|STATIC|AWO|<name>|<IP addr>|ANY} <rsms_pwd>
```

**Example:** To deactivate connections for all DHCP IP addresses, send an SMS to the terminal with the text: **DEACTIVATE 1 DHCP remote**

**Response:**
You receive a response showing the IP address(es) for which the connection was deactivated.

**Example:** A confirmation SMS after sending a deactivation SMS may look like this:
```
LOCAL IP 192.168.128.104 DEACTIVATED
SMS-Free: 77/100
WARNING: Ensure SMS-free > 5. Cleanup old msgs for
orderly remote-SMS-control
```

## CLEAR: Delete SMS messages in the EXPLORER 540

The text in the CLEAR SMS must have the following format:

```
CLEAR <category> SMS <rsms_pwd>
```

**Example:** To delete all SMS messages from the EXPLORER 540, send an SMS to the terminal with the text: **CLEAR 4 SMS remote**

**Response:**
No response is sent for this command.

## GETINFO: Get information from the EXPLORER 540

The text in the GETINFO SMS must have the following format:

```
GETINFO <info_mode> {GPS|ALL|USAGE} <rsms_pwd>
```

**Example:** To request all information with titles, send an SMS with the text:
**GETINFO 1 ALL remote**

**Response**: The response depends on the requested format (GPS/ALL/USAGE) and info mode. For the command in the example, the response would have the titles shown below.

```
Example: IMSI: 901112112456789
         IMEI: 35393803001003
         LAT: 32.89495
         LON:-117.20205
         SW: 1.0
         C/N0: 66
         Beam: 84
         Uptime: 59483
         GIP: 161.30.23.43
```

The Uptime is in seconds, and GIP is the global IP address of the first active PDP context (BGAN or cellular, depending on the network in use).

> **Note** You may not be able to access a private cellular IP address. If you use PRISM instead, it will give you the same IP address regardless of the network used (BGAN or cellular).

## RESTART: Restart the EXPLORER 540

The text in the RESTART SMS must have the following format:

```
RESTART 1 BGAN <rsms_pwd>
```

**Example:** To restart the EXPLORER 540, send an SMS with the text:
**RESTART 1 BGAN remote**

**Response:**
No response is sent for this command.

## WATCHDOG: Get or set watchdog parameters

**Request:** The text in the WATCHDOG SMS must have the following format:
WATCHDOG 1 <rsms_pwd>

**Modify:** The text in the WATCHDOG SMS must have the following format:
**WATCHDOG 2 {<ping1>|NA} {<ping2>|NA} {<ping3>|NA} <ping_always> {<ping_interval>|NA} <wdog_enable> <rsms_pwd>**

**Example**: WATCHDOG 2 100.100.100.130 100.100.100.110 NA 0 20 1 remote

In this example, the Connection watchdog is set up as follows:

**2**: Set watchdog parameters.
**100.100.100.130**: Primary IP address.
**100.100.100.110**: Secondary IP address.
**NA**: Tertiary IP address is left unchanged.
**0**: Send ping only if no IP data traffic.
**20**: Ping interval (number of minutes between pings).
**1**: Enable watchdog.
**remote**: Remote SMS password.

**Response:**
You do not get an OK response. You can use the **WATCHDOG 1** command to get the status of the WATCHDOG feature.

See also *Connection watchdog (Link monitoring)* on page 3-15 and *SMS remote command summary* on page B-4.

> **Note** If a data connection was running, the Connection watchdog will restart the connection and then start sending ping commands.

## ADVWATCHDOG: Get or set Terminal watchdog parameters

**Request:** The text in the ADVWATCHDOG SMS must have the following format:
ADVWATCHDOG 1 <rsms_pwd>

**Response:**
IMEI: <IMEI>
Terminal watchdog enabled = <YES/NO>
Wake up = <YES/NO>
Interval = <days, hours>
IP = <ping1/NA> <ping2/NA> <ping3/NA>
APN type = "SIM default", "Network assigned" or "User defined"
APN name = <APN>   (only present if APN type is "User defined")
APN username = <apn_user>
APN password = <apn_passwd>
Next run: <yyyy-mm-dd hh:mm/NA>   (NA if AWD is not enabled) **Note: UTC time!**
Position SMS response = <YES/NO>
Position SMS number = <sms_number>

**Modify:** The text in the ADVWATCHDOG SMS must have the following format:
**ADVWATCHDOG 2 {<enabled>|NA} {<wake_up>|NA} {<interval>|NA} {<ping1>|NA} {<ping2>|NA} {<ping3>|NA} {<apn_type>|NA} {<apn>|NA|CLR} {<apn_user>|NA|CLR} {<apn_pwd>|NA|CLR} {<pos_response>|NA} {<sms_number>|NA} <rsms_pwd>**

**Example:**   ADVWATCHDOG 2 1 1 24 100.100.100.130 100.100.100.110 200.247.237.254 0 NA CLR CLR NA NA remote

In this example, the Terminal watchdog is set up as follows:

**2**: Set Terminal watchdog parameters.

**1**: Enable Terminal watchdog.

**1**: Wake up the terminal from power save.

**24**: Run the Terminal watchdog once a day (24 hours).

**100.100.100.130**: Primary IP address.

**100.100.100.110**: Secondary IP address.

**200.247.237.254**: Tertiary IP address.

**0**: Set the APN type to SIM default (0 = SIM default, 1 = Network assigned, 2 = User defined).

**NA**: When the APN type is SIM default, the APN name is ignored.

**CLR**: The user name is cleared. When the default APN is used, any previous user name and password should be cleared, unless a new manual user name is entered (NA would maintain any previous setting).

**CLR**: The password is cleared. When the default APN is used, any previous user name and password should be cleared, unless a new manual password is entered (NA would maintain any previous setting).

**NA**: Position SMS response is not applicable (see note below).

**NA**: Number for position SMS response is not applicable (see note below).

> **Note** | Position SMS response is for future use, and should be set to NA.

**Response:**

You do not get an OK response. You can use the **ADVWATCHDOG 1** command to get the settings of the ADVWATCHDOG feature.

See also *Terminal watchdog* on page 3-15 and *SMS remote command summary* on page B-4.

## ADPWRST: Reset the administrator password

To reset the administrator password you need the IMEI number of your terminal. If you can access the web interface, you can find the IMEI number under **Support > About,** see *About* on page 4-28.

The text in the ADPWRST SMS must have the following format:

```
ADPWRST 1 <imei> <rsms_pwd>
```

**Example:** To reset the administrator password of a terminal with the IMEI number 363833-09-012345, send an SMS with the text:
**ADPWRST 1 36383309012345 remote**

**Response:**

You receive a response with the result of the action.

**Example:** A response for a successful ADPWRST command, could be:
```
ADMIN RESET SUCCESS
SMS-Free: 88/100
WARNING: Ensure SMS-free > 5. Cleanup old msgs for
orderly Remote SMS Control
```

## WANMODE: Get or set the WAN connection mode

For information on the different WAN modes, see *Select WAN network (Mode)* on page 4-16 and *<wanmode>* on page B-7.

| Note | If you are going to use one of the cellular modes (WANMODE 4, 6, 7 or 8), you must first set up all dual mode parameters in the web interface or with AT commands. See |

- *To set up the connection mode* on page 4-16
- *Optional: To set up cellular network for data (dual mode)* on page 4-48
- *PRISM/WAN switching* on page 4-54
- *AT commands for dual mode with cellular modem* on page B-19

The text in the WANMODE SMS must have the following format:

```
WANMODE <cmd_op> {<wanmode>} <rsms_pwd>
```

**Example:** To set the connection mode to **Cellular modem preferred**, send an SMS with the text:
**WANMODE 2 4 remote**

In this example, the WAN connection mode is set up as follows:

**2**: Set WANMODE parameters.
**4**: Select Cellular modem preferred.

**Response:**
You receive a response with the result of the action.

**Example:** The response to the command in the example above would be:
WANMODE=4

## ATCO: Send AT commands to the EXPLORER 540

The text in the ATCO SMS must have the following format:

```
ATCO <resp_mode> <rsms_pwd> <at_cmd>
```

**Example:** To command the EXPLORER 540 to download new software from the default FTP server via the default APN and upgrade to the new version immediately, send an SMS with the text:
**ATCO 2 remote _IGETFW=1**

**Response:**
You receive a response with the result of the action. In this example we have chosen to see only the final response (`<resp_mode>` = 2) and we have chosen immediate upgrade (`<mode>` =1), so the final (and only) response will be related to the upgrade of the EXPLORER 540.

**Example:** For a successful completion of the command in the above example, the response would then be: _IUPDFW: 0, Complete

See also *ATCO response codes* on page B-12.

**List of supported ATCO commands:**

The following AT commands are supported using the ATCO command in an SMS. For syntax and parameters, see *ATCO commands* on page B-10.

- **_IGETFW** Get new firmware (and optionally install it).
  See *Remote software upgrade* on page 3-24.

- **_IUPDFW** Update the terminal with new firmware.
  See *Remote software upgrade* on page 3-24.
- **_ISENDFILE** Send a file from the terminal to an FTP server.
  See *File transfer* on page 3-25.
- **_IGETFILE** Retrieve a file from an FTP server to the terminal.
  See *File transfer* on page 3-25.
- **_IUPDCFG** Update to a new configuration file.
  See *File transfer* on page 3-25.
- **_IREMWEB** Open a connection for remote access to the terminal's Web interface.
  See *Remote access to the web interface* on page 3-10.
- **_ICPWD** Change the terminal's admin password.
  See *Security setup* on page 3-12.
- **_IATCROBST** Configure 3GGP LTE robustness feature.

## 3.3.2 Remote access with AT commands

Access the terminal as described in *To access the terminal using AT commands* on page 3-3. You must use the global IP address of the EXPLORER 540.

## 3.3.3 Remote access to the web interface

> **Note** When using remote access, the web interface may take a long time to load the pages, because the Internet connection may be slow.

There are two methods of getting remote access to the web interface:

- Using the AT command _IREMWEB, e.g. sent in an SMS (ATCO command).
- Using an EXPLORER 540 that is pre-configured with trusted IP addresses.

The following sections describe these two methods.

> **Note** Only one PDP context at a time can be used for remote web interface access.

### To use AT commands to get remote access to the web interface

You can send the AT commands encapsulated in an SMS (ATCO commands). For details, see *Remote access with SMS* on page 3-4.

> **Note** If remote SMS command access has been disabled, you can enable it either using the web interface or using AT commands. See *To set up remote access with SMS* on page 4-40 and *To set up the security with AT commands* on page 3-13 (step 4).

Relevant commands:

**_IREMWEB**

See *ATCO commands* on page B-10 for syntax and parameters.

1. To use an SMS to allow access to the web interface for specific IP addresses, send the following command:
   ATCO <resp_mode> <rsms_pwd> _IREMWEB=1,<ip address>[,<ip address>]

   **Example:**  ATCO 2 remote _IREMWEB=1,214.123.189.119

   In this example the command specifies no immediate response, only when the global IP address is sent along (2). The remote SMS password is **remote** and the IP address

214.123.189.119 can get remote access to the web interface (if two IP addresses are listed, it is interpreted as a range of IP addresses).

2. The EXPLORER 540 should now return an SMS response with the external IP address of the terminal.

   **Example:** _IREMWEB:81, GlobalIP:161.30.181.31

   **81** is the response code for a remote web connection that was set up successfully. It is followed by the global IP address, which is the IP address to enter in your browser to access the web interface from the remote device with the IP address you specified in the command.

3. On the remote computer, open your web browser.

4. In the address bar of your browser, enter the global IP address of the EXPLORER 540 (received in the response above).

You should now be connected to the built-in web interface of the terminal.

> **Note** | Access to the EXPLORER 540 web interface is restricted with a password. See *Security setup* on page 3-12 and *Passwords* on page 4-29.

## To get remote access to the web interface from a trusted IP address (preconfigured)

> **Note** | This method requires that you initially have local access to the EXPLORER 540. If not, use the **_IREMWEB** command described in the previous section.

1. Connect a computer to the EXPLORER 540 and access the web interface locally.

2. Prepare the terminal as described in *Remote management* on page 4-38.

3. Make sure your remote computer has access to the Internet.

4. On the remote computer, open your web browser.

5. In the address bar of your browser, enter the IP address of the terminal followed by a colon and the port number
   **http://<ip address>:<incoming port>**.
   - <ip address> is the external IP address of the EXPLORER 540. The external IP address can only be obtained when a data connection (PDP context) is established. If a data connection is started. you can get the external IP address with the GETINFO SMS command, see *GETINFO: Get information from the EXPLORER 540* on page 3-6.
   - <incoming port> is the port you defined in *Remote management* on page 4-38 (Incoming port for web application, default port 80).

   **Example:** If the IP address of the terminal is 161.30.180.12 and the incoming port number defined in the Remote management page in the web interface is 80, enter **http://161.30.180.12:80**.

You should now be connected to the built-in web interface of the terminal.

> **Note** | Access to the EXPLORER 540 web interface is restricted with a password. See *Security setup* on page 3-12 and *Passwords* on page 4-29.

# 3.4    Security setup

| Important | By default any phone number can access the EXPLORER 540 with an SMS! To protect against unauthorized access, change the remote SMS password and make a list of trusted phone numbers. See *To set up remote access with SMS* on page 4-40 and *To set up the security with AT commands* below. |

## 3.4.1    Overview of security measures

Since the EXPLORER 540 is most likely placed in remote areas without direct supervision, it is important to protect it against unauthorized access.

The EXPLORER 540 has the following security measures:

- User and administrator passwords for the web interface.
- Deny access to AT commands on LAN.
- Admin password for AT shell and SMS control.
- White list for SMS control (list of trusted phone numbers).
- MAC filtering.
- SIM personalization.
  Optional SIM lock (lock to provider) and optional PIN lock (lock to EXPLORER 540 terminal).
- Disable Reset button.
  One of the functions of the Reset button is to reset to factory default, which also resets the administrator password. This function can be disabled using the web interface.
- Redirect to HTTPS.
- Enable/disable support for Thrane IP Handset.

You can set up these security measures in the web interface or with AT commands. see the next sections for details.

## 3.4.2    To set up the security with AT commands

For details on how to send AT commands to the EXPLORER 540, see *To access the terminal using AT commands* on page 3-3.

For details on syntax and parameters for the AT commands, see *AT commands* on page B-9.

Do as follows:

1.  Disable administration lock:
    AT_ICLCK=AD,0,<password>

    **Example:**    AT_ICLCK=AD,0,admin

    When you get an OK reply you have administrator access to the AT shell.

2.  Set new administrator password:
    AT_ICPWD=AD,<old password>,<new password>

    > **Note** | The password must be 5 to 15 characters long and cannot contain spaces. Avoid special characters. Accepted characters are: A through Z (uppercase characters), a through z (lowercase characters) and 0 through 9 (numeric characters).

    **Example:**    AT_ICPWD=AD,admin,myadmpwd

    When you get an OK reply the administrator password is set to the new password (myadmpwd in the example).

3.  Set new password for remote SMS:
    AT_ICPWD=RS,<old password>,<new password>

    > **Note** | The password must be 5 to 15 characters long and cannot contain spaces. Avoid special characters. Accepted characters are: A through Z (uppercase characters), a through z (lowercase characters) and 0 through 9 (numeric characters).

    **Example:**    AT_ICPWD=RS,remote,mysmspwd

    When you get an OK reply the password for remote SMS access is set to the new password (mysmspwd in the example).

4.  Disable/enable remote SMS commands:
    Disable: AT_ISMSRMT=0
    Enable: AT_ISMSRMT=1

    > **Important** | If you disable remote SMS commands there is no way to access the terminal remotely, unless you have an open data connection (PDP context)! Instead we recommend to define a set of trusted phone numbers, see *To set up remote access with SMS* on page 4-40.

5.  Specify a white list of trusted MAC addresses:

    > **Note** | Until MAC address filtering is enabled, all MAC addresses are allowed and the white list has no effect.

    AT_IMACLOCAD=1,0,<MAC address>[,<MAC address> (etc.)]

    **Example:**    AT_IMACLOCAD=1,0,00:B5:E0:76:FD:C2,00:B5:A0:84:F9:E2

    When you get an OK reply, the specified MAC addresses are added to the white list.

    > **Important** | Remember to add the MAC address of your own device. Enabling the MAC address locking without adding your own device MAC address will block for any local access to the Terminal!

6. Turn on MAC address filtering:
   AT_IMACLOC=1,0
   When you get an OK reply, MAC address filtering is enabled for Ethernet, and only the MAC addresses specified in the white list can get access (previous step).

7. Enable administration lock:
   AT_ICLCK=AD,1,<password>

   **Example:**   AT_ICLCK=AD,1,myadmpwd

   When you get an OK reply, the system is protected with the administrator password.

## 3.4.3   To set up the security with the web interface

If you want to set up the security with the web interface, see the following sections:

- User and administrator passwords for web interface: *Passwords* on page 4-29.
- Admin password for AT shell (same as for web interface): *Passwords* on page 4-29.
- Password for remote SMS access: *To set up remote access with SMS* on page 4-40.
- Trusted phone numbers for SMS control: *To set up remote access with SMS* on page 4-40.
- MAC filtering: *To manage connected devices (Traffic control)* on page 4-22.
- SIM personalization: *Auto SIM PIN validation* on page 4-32 and *SIM lock* on page 4-32.
- Disable Reset button: *Reset button* on page 4-45.
- Access to AT commands on LAN: *Security* on page 4-45.
- Redirect to HTTPS: *Security* on page 4-45.
- Support for Thrane IP Handset: *To enable the use of Thrane IP Handset* on page C-8.

# 3.5 To control data connections (PDP contexts)

## 3.5.1 Automatic Context Activation (ACA)

In the web interface you can set up the EXPLORER 540 to automatically establish a data connection when it is registered on the satellite network. See *Automatic Context Activation (ACA)* on page 4-7. Automatic Context Activation also applies to the "wake-on" actions after power save mode (see *Power control* on page 3-19) and by recovery after e.g. loss of power.

If the terminal is in Cellular modem preferred mode or Cellular modem preferred (PRISM) mode, ACA is mandatory on both the cellular and the BGAN connection, i.e. a data connection is automatically established on both networks.

## 3.5.2 Connection watchdog (Link monitoring)

If you are not using the Terminal watchdog function, or if you need to monitor your individual data connections, it is strongly recommended to use the Connection watchdog function to monitor your IP connection, as it enables you to test the BGAN (or cellular) connectivity and to keep your PDP context alive.

With this feature activated, the terminal will send out ping commands to up to three servers of your choice. When a data session is started, the terminal will start sending ping commands to the Primary IP address the number of times specified. If no response is received, it will send the same number of ping commands to the Secondary and then Tertiary IP address, if available. If no response is received from any of the IP addresses, the terminal will eventually restart.

For setup with the web interface, see *Connection watchdog (Link monitoring)* on page 4-34.

For setup with SMS command, see *WATCHDOG: Get or set watchdog parameters* on page 3-7.

> **Note** The Connection watchdog does not work with PRISM.

## 3.5.3 Terminal watchdog

The Terminal watchdog monitors the terminal to ensure that it remains operational. It continuously monitors valid system time (UTC) and CS attach (the BGAN circuit-switched connection) status. Additionally, at regular intervals set by the user, the Terminal watchdog can wake up the terminal from power save, start a data connection and verify a positive response to a ping request, and send a position SMS or a loopback SMS to verify SMS connection.

> **Note** Unlike the Connection watchdog, the Terminal watchdog does **not** check your individual BGAN (or cellular) data connections - it only sends ping requests on the data connection set up by the Terminal watchdog itself.

For configuration with the web interface, see *Terminal watchdog* on page 4-36.

For configuration with SMS command, see *ADVWATCHDOG: Get or set Terminal watchdog parameters* on page 3-7 and *SMS remote commands* on page B-4.

## 3.5.4    Manual activation of data connections

You can manually activate a data connection in the following ways:

- Remote: Send an SMS to the EXPLORER 540. See *ACTIVATE: Activate a data connection with an SMS (BGAN only)* on page 3-5.
- Local (EXPLORER 540 LAN interface):
  - 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 4-5, or
  - Send an AT command to the terminal. See *To configure the connected equipment for PPPoE* on page 3-17 (the example), *To access the terminal using AT commands* on page 3-3 and *Context management AT commands* on page B-17.

**Cellular connection**: If you are using the optional cellular connection with the EXPLORER 540 Modem, the data connection is started automatically when the cellular connection is established. For details, see *Optional: To set up cellular network for data (dual mode)* on page 4-48.

## 3.5.5    PPPoE (Point-to-Point Protocol over Ethernet), BGAN only

### Overview

By using PPPoE, users can virtually "dial" from one machine to another over an Ethernet network, establish a point to point connection between them and then transport data packets over the connection. You can establish a PPPoE connection to the BGAN network using the EXPLORER 540 system.

| Note | You can **not** use PPPoE to control a cellular connection. |

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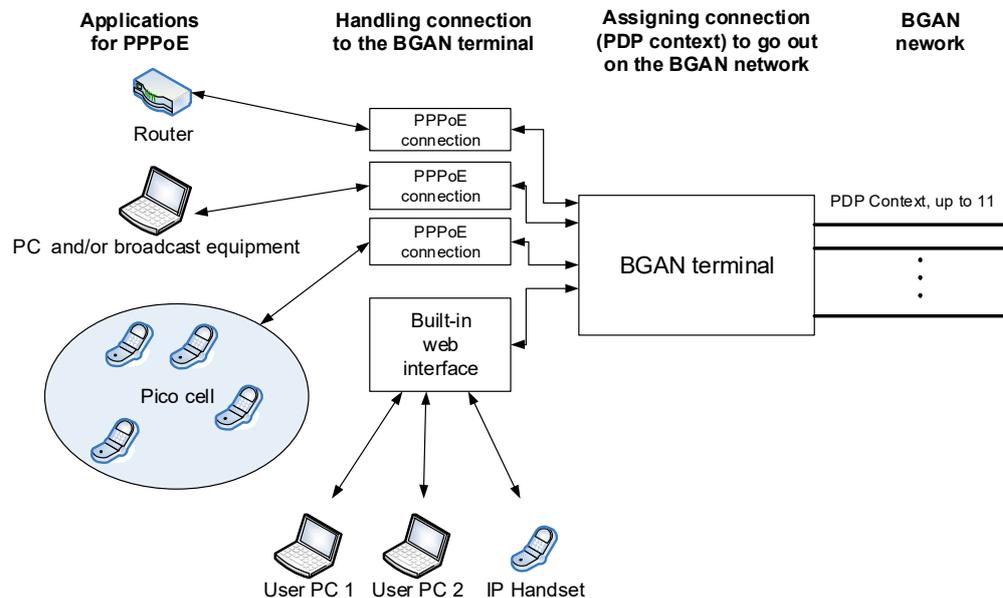


### To configure the connected equipment for PPPoE

On the equipment connected to the EXPLORER 540 you must enter a few settings for your PPPoE connection. For example you need to set up which service to use (e.g. 64 kbps Streaming) and a user name and password. How to configure your equipment depends on the type of equipment. Refer to the user documentation of the equipment.

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.

Note for MAC OS: User name and password are required. For some service providers you can use user name void and password void. Contact your airtime provider for further information.

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.

On the EXPLORER 540 you must set up the APN to use before you can establish a PPPoE connection. See *To change the APN for PPPoE (BGAN only)* on page 4-21.

## To send commands with PPPoE

You can use the command **XBB:<AT String>** to send AT commands over PPPoE.

**Example:**  To start a Standard data connection with the Context identifier "1", type
**XBB:AT+CGDCONT=1,ip,bgan.inmarsat.com;+CGEQREQ=1,3**

Note that there are two commands involved, +CGDCONT and +CGEQREQ.

+CGDCONT defines the context ID (1), the connection type (IP) and the APN (bgan.inmarsat.com).

+CGEQREQ starts a data connection for the defined context ID (1) using traffic class Standard data (3).

Note that because the traffic class is 3 (Standard data), the remaining parameters (max. and guaranteed bit rates etc.) are omitted. See also *Context management AT commands* on page B-17.

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

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 (not available in M2M subscription), 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:STREAM32K[1] | Initiates a Primary Streaming 32 kbps connection |
| XBB:STREAM64K[a] | Initiates a Primary Streaming 64 kbps connection |
| XBB:STREAM128K[a] | Initiates a Primary Streaming 128 kbps connection |
| XBB:<AT String> | This allows the PPPoE clients to enter a full AT context activation string.<br>Examples:<br>XBB:AT+CGDCONT=1,ip,"bgan.inmarsat.com"<br>XBB:AT+CGEQREQ=1,1,64,64,64,64 |

1. Streaming is not available for M2M subscription

# 3.6    Power control

You can configure the Power mode options with the web interface and with AT commands.

With **the web interface** you can set up what should make the EXPLORER 540 enter power save state as well as how and when to wake up the terminal. For details, see *Power control* on page 4-41.

With **AT commands** you can set up: **Idle power save** and **Remote on/off**. See *To set up power save functions with AT commands* on page 3-22.

You can choose between three 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*.
- **Idle power save**. The terminal will go into power save state after a (configured) period with no activity. For details, see *Idle power save* on page 3-21.

## 3.6.1    Always on

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

## 3.6.2    Remote on/off

When Remote on/off is selected in the web interface or with AT commands, you can control the power save function using the Power control pin (Remote on/off signal).

Wake-up methods in Remote on/off mode:

- Power control pin (Remote on/off signal) is active. See the next section for details.
- Daily awake period

You can configure the function in the web interface (see *Power control* on page 4-41) or with AT commands (see *Remote on/off* on page 3-22).

> **Note** To use the Remote on/off function you must first connect the Power control pin to a remote on/off switch as described in *Connection example for the Power control pin* on page 3-20.

### 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.
- The terminal watchdog is executing.

- Optional daily awake period ongoing.
  This is an optional configurable period of time that the terminal should stay awake every day.
- 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.

## Connection example for the Power control pin

**Important** | The Power control pin, 1-GPI in the EXPLORER 540 I/O connector, is internally pulled down. This means that 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, or if **Idle power save** mode is selected with the wake-up function **Power control pin** enabled.
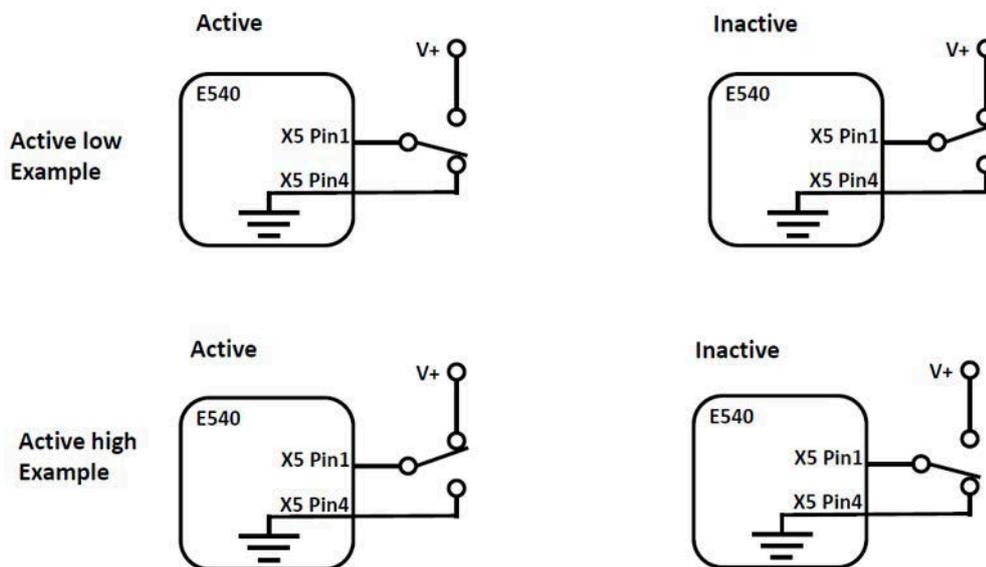


- If you have configured the input to be Active low (default):
  To deactivate: Connect the Power control pin to V+ (*High: 2.8 - 32 VDC*).
  To activate: Connect the Power control pin to GND (*Low: 0 - 0.8 VDC*).
- If you have configured the input to be Active high:
  To deactivate: Connect the Power control pin to GND (*Low: 0 - 0.8 VDC*).
  To activate: Connect the Power control pin to V+ (*High: 2.8 - 32 VDC*).

For specifications of the I/O connector, see *I/O connector (X5)* on page A-5.

## 3.6.3    Idle power save

When **Idle power save** is selected in the web interface and the Idle time has run out, the terminal deregisters and gracefully closes down the terminal to save power.

> **Note** The terminal is considered active (**not idle**) if one or more of the following conditions are present:
> - The web interface is open.
> - A cellular connection is started
> - Data or SMS traffic.
> - Software update ongoing.
> - Incoming/outgoing calls.
> - Terminal watchdog executing.
> - The terminal is started by connecting power and the 3 minute grace period is still ongoing.
> - One of the configured wake-up methods are active (see below).

To use the Idle power save mode you must configure one or more "wake-up" methods and a few general settings:

Wake-up methods:

- Daily wake up: Set a time of day where the terminal will wake up
- Wake-on-LAN: Set up the terminal to wake up when it receives a "magic packet" on the LAN interface.
- Power control pin: Set up the terminal to wake up when the Power control pin is active. See the following section *Power control pin function when Idle power save is selected*. (Note that with AT commands you cannot configure this wake-up method for Idle power save).

General power save settings:

- Idle time - Set the number of minutes without any activity before the terminal enters power save state.
- Set whether or not the power save function should be prevented when a satellite connection (PDP context) is open (only configurable with web interface).

You can configure the wake up methods and the general power save settings in the web interface under **Advanced** > **Power control.** See *Power control* on page 4-41.

For configuration with AT commands, see the section *To set up power save functions with AT commands* on page 3-22.

### Power control pin function when Idle power save is selected

When you have selected Idle power save you can choose to enable the Power control pin in the web interface.

**Disabled:** If the Power control pin is disabled, the state of the pin is ignored.

**Enabled**: If the Power control pin is enabled, the function is as follows:

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 enabled Power control pin in Idle power save 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 go into power save state when the Idle time has expired and none of the configured wake-up methods are active. See also the note in the previous page.

## 3.6.4    To set up power save functions with AT commands

For details on how to use AT commands see *To access the terminal using AT commands* on page 3-3.

You can set up the following power save functions with AT commands:

- Remote on/off
- Idle time with Daily wake-up and/or Wake-on-LAN

### Remote on/off

With the AT command AT_ITREMONOFF you can set up

- Enable or disable the Remote on/off function
- Shut down delay after the Power control pin is deactivated
- Daily awake period (time of day and duration)
- Polarity of the Power control pin (active high or low)

**Important** | Before configuring the remote on/off function, connect the Power control pin as described in *Connection example for the Power control pin* on page 3-20.

Set up the Remote on/off function as follows:

1. Type in the AT command:
   AT_ITREMONOFF=<active mode>,<power down delay>,<awake time of day>,<awake duration>,<polarity>

   **Example:**    AT_ITREMONOFF=1,3,60,10,HIGH

   In the example above, Remote on/off is activated (1) with 3 minutes shut down delay (3), awake time of day 60 minutes after midnight (60), 10 minutes duration of awake time (10) and Power control pin active high (HIGH).

**Note** | If you set Awake time of day to **0**, the daily awake period is disabled.

**Note** | Changing <active mode> from **1** to **0** will change the power mode from Remote on/off to Always on.
Changing <active mode> from **0** to **1** will change the power mode to Remote on/off.

### Idle power save

When you use the AT_IPWSAVSCHD command you set the power save mode to Idle power save, provided you define an idle time (more that zero) and you define at least one valid wake-up method.

**Important** | If the terminal was already in Idle power save mode before the command and the Idle time is set to "0" with the AT command below, or you have not defined a wake-up method, the Power save function is disabled and the terminal will be **always on**.

If the terminal was **not** in Idle power save mode and the time is set to "0", the parameter is stored, but the power save mode is **not** changed to Idle power save mode.

**To set the idle time before power save**

If you are using power save mode **Idle power save** and none of the conditions that prevent power save state are present (mentioned in the section *Idle power save* on page 4-8), the system will go into power save state after a defined idle time. You can configure this Idle time with the AT command _IPWSAVSCHD as follows:

1. Set the idle time before power save:
   AT_IPWSAVSCHD=<psmode>,<psvalue>

   **Example:**   AT_IPWSAVSCHD=IDLE_TRG,15

   In this example, the power save mode is Idle power save, the trigger is idle time (IDLE_TRIG), and the idle time before the terminal enters power save state is 15 minutes.

   | Important | Remember to configure one or more wake up functions - otherwise the EXPLORER 540 will not be able to enter power save state. |

**To configure wake up on daily basis**

1. Set the time of day that the terminal must wake up from power save:
   AT_IPWSAVSCHD=<psmode>,<psvalue>

   **Example:**   AT_IPWSAVSCHD=TOD_TRG,24:00

   In the example above, the wake-up method Time Of Day (TOD) is selected, and the time of day to wake up from power save is 24:00 UTC time.

   | Note | If the wake-up time of day is set to "0" with this AT command, the "Wake up time of day" function is disabled! You must configure another wake-up method. |

**To configure Wake-On-LAN**

1. Set the Wake-On-LAN function to On or Off:
   AT_IPWSAVSCHD=<psmode>,<psvalue>

   **Example:**   AT_IPWSAVSCHD=WOL_STATUS,1

In the example above, the wake-up method Wake-On-LAN is selected. This means the terminal will wake up from power save when a "Magic packet" is received on the LAN interface.

# 3.7 Remote software upgrade

## 3.7.1 User initiated software upgrade

You can initiate a remote software upgrade with an AT command, either from the command interface or encapsulated in an SMS (ATCO command).

**_IGETFW** tells the terminal to get software from an FTP server and either upgrade the terminal software or download the software file to the terminal for later upgrade.

> **Note** | FTP server: With M2M subscription you can use Inmarsat's M2M FUP server (default FTP server for software upgrade). This is not available for Non-M2M subscriptions.

**_IUPDFW** tells the terminal to upgrade its software to the downloaded file.

For syntax and parameters, see *ATCO commands* on page B-10.

## 3.7.2 To upgrade the software

If you have an M2M subscription, the EXPLORER 540 software should be available from the Inmarsat FTP server. If not, download the new software[1] or acquire the software from Cobham SATCOM and place it on your FTP server.

1. To access the EXPLORER 540, use one of the following:
   - a computer connected to the Internet, *Remote access with AT commands* on page 3-10.
   - equipment capable of sending and receiving SMS messages, see *Remote access with SMS* on page 3-4.

   Note that you need a password for both access methods. For AT commands, use the AT_ICLCK command with the admin password, for SMS, use the remote SMS password.

2. Use the command **_IGETFW** to initiate the software download (and maybe upgrade) from the specified FTP server. If you are using default APN and default FTP server these can be left out.

   **Example:**  AT_IGETFW=1

   In this example, the terminal will get the software from the default FTP server via the default APN and download and then upgrade the software in the terminal.

   > **Note** | The Inmarsat FTP server for firmware upgrade is only available with M2M subscription. If you have a non-M2M subscription you must specify a third party FTP server for the software upgrade.

3. The terminal prepares for software update, connects to the specified FTP server and downloads the software image.
   If you have selected **Deferred update** (_IGETFW=0), you have to use the command **_IUPDFW** followed by the file name when you want the terminal to upgrade the software.

4. If you have selected **Immediate update** (_IGETFW=1), the terminal updates the system, reboots, installs the update and verifies the online connection.

5. When the software upgrade is successfully completed you get an AT or SMS command response with the message **Complete**.

   **Example:** `_IUPDFW: 0, Complete`

For information on software update with the web interface, see *To update software* on page 4-27.

---

1. You can download the software from the Cobham Satcom Partner Portal at https://partnerportal.cobhamsatcom.com/.

# 3.8    File transfer

Using AT commands, you can transfer a configuration file or a log file between the EXPLORER 540 (local directory in EXPLORER 540 is "/") and an FTP server over the satellite network.

**_IGETFILE** tells the terminal to get a file from an FTP server (e.g. a configuration file).

**_ISENDFILE** tells the terminal to send a file to an FTP server (e.g. a log file).

**_IUPDCFG** tells the terminal to update the EXPLORER 540 configuration with the contents of the previously downloaded configuration file.

For Syntax and parameters, see *ATCO commands* on page B-10.

## 3.8.1    Configuration file

If you need to reuse a configuration in other terminals of the same type, you can save your current configuration to a file, which can then be loaded into the other terminal(s).

| Note | Be aware that if the terminals have different software versions, some of the settings may be different than expected. If possible, use the same software version in the terminals. |
|------|------|

### Save configuration

To command the EXPLORER 540 to save its configuration to a file and transfer it to an FTP server, do as follows:

1.  To access the EXPLORER 540, use one of the following:
    - a computer connected to the Internet, see *Remote access with AT commands* on page 3-10, or
    - equipment connected to a cellular network, see *Remote access with SMS* on page 3-4.

    Note that you need a password for both access methods. For AT commands, use the AT_ICLCK command with the admin password, for SMS, use the remote SMS password.

2.  Send the command **_ISENDFILE** to the EXPLORER 540 to make it send the configuration file to the specified destination on your FTP server.

    **Example: AT_ISENDFILE="/**
    **        ","config.txt","ftpdirectory","ftp.myftpserver.com","**
    **        ftp-username","ftp-password"**

    In this example. the terminal will look for a file named **config.txt** in the local directory (**/**) in the terminal, and send the file to the directory **ftpdirectory** on the FTP server named **ftp.myftpserver.com**. The user name **ftp-username** and password **ftp-password** give access to the FTP server. The default APN is used (APN info is left out).

3.  You get a response command that the file was transferred successfully.

    **Example:** _ISENDFILE: 0, Complete

## Load configuration

To command the EXPLORER 540 to update its configuration, do as follows:

1. Place the configuration file on your FTP server.
2. To access the EXPLORER 540, use one of the following:
   - a computer connected to the Internet, see *Remote access with AT commands* on page 3-10, or
   - equipment connected to a cellular network, see *Remote access with SMS* on page 3-4.

   Note that you need a password for both access methods. For AT commands, use the AT_ICLCK command with the admin password, for SMS, use the remote SMS password.
3. Send the command **_IGETFILE** to the EXPLORER 540 to download the configuration file from the specified FTP server.
   Leave out APN information if you are using default APN.

   **Example:** `AT_IGETFILE="ftpdirectory","config.txt","/",`
   `"ftp.myftpserver.com","ftp-username","ftp-password"`

   In this example. the terminal will look for a file named **config.txt** in the directory **ftpdirectory** on the FTP server named **ftp.myftpserver.com** and download the file to the directory named **/** in the terminal. The user name **ftp-username** and password **ftp-password** give access to the FTP server. The default APN is used (APN info is left out).
4. You get a response command that the configuration file was successfully downloaded from the ftp server to the terminal.

   **Example:** `_IGETFILE: 0, Complete`
5. Use the command **AT_IUPDCFG** to upgrade the EXPLORER 540 configuration using the file downloaded in step 3

   **Example:** `AT_IUPDCFG=config.txt`

   This command will take the downloaded configuration file named **config.txt** and use it to update the configuration of the EXPLORER 540.

   > **Note** The terminal will reboot when the configuration is updated.

6. You get a response command that the configuration was successfully upgraded.

   **Example:** `_IUPDCFG: 0, Complete`

To save or load a configuration using the web interface, see *To save or load a configuration* on page 4-33.

## 3.8.2    Log file(s)

Using AT commands, you can command the EXPLORER 540 to send the following log files to an FTP server:

- Diagnostics report: **diagreport.tar.gz**. A report containing useful information for troubleshooting (includes the logs below as well as other information).
- Event log: **event.csv**. A log of events that are signaled to the user.
- System log: **syslog.log**. A log of internal events in the EXPLORER 540.
- AT command log: **at_log.txt**. A log of all AT commands sent and received by the EXPLORER 540 and SMS commands with responses.

To command the EXPLORER 540 to send a log file to an FTP server, do as follows:

1. To access the EXPLORER 540, use one of the following:
   - a computer connected to the Internet, see *Remote access with AT commands* on page 3-10, or
   - equipment connected to a cellular network, see *Remote access with SMS* on page 3-4.

   Note that you need a password for both access methods. For AT commands, use the AT_ICLCK command with the admin password, for SMS, use the remote SMS password.

2. Send the command **_ISENDFILE** to the EXPLORER 540 to make it send a log file to the specified destination on your FTP server.

   **Example:** ```_ISENDFILE="/","syslog.log","ftpdirectory",```
   ```"ftp.myftpserver.com","ftp-username","ftp-password"```

   In this example. the terminal will look for a file named **syslog.log** in the local directory **/** in the terminal, and send the file to the directory **ftpdirectory** on the FTP server named **ftp.myftpserver.com**. The user name **ftp-username** and password **ftp-password** give access to the FTP server. The APN is left out to indicate that the default APN is used.

3. You get a response command that the file was transferred successfully.

   **Example:** ```_ISENDFILE: 0, Complete```

Using the web interface you can see the Event log and create a diagnostics report. See *Log files* on page 5-15.

# 3.9    Status of the EXPLORER 540

There are basically three ways of getting status from the EXPLORER 540:

- Access the built-in web interface. The Status page shows information such as terminal status, network status, position status and ongoing communication. See *Status information* on page 4-10.
- Send the SMS command **GETINFO** to the EXPLORER 540. This commands retrieves information from the EXPLORER 540 such as call time, data usage, GPS position and global IP address. For details, see *ATCO commands* on page B-10.
- I/O pins
    - 2-GPO (Terminal ready output).
    - 3-GPIO, see next section.

Additionally, until installation is completed you can use the LED to follow the status. See *LED* on page 5-8.

## 3.9.1    Terminal ready signaling with 2-GPO

2-GPO signals when the terminal is registered on the BGAN network and is ready to communicate with connected equipment. Used in combination with a relay, you can use this signal to switch on connected equipment when the terminal is ready.

For configuration (Active High or Low), see *GPIO pins* on page 4-44.

For specifications, see *I/O connector (X5)* on page A-5.

Connection example for 2-GPO with an SPDT relay (V+ = up to 32 VDC):
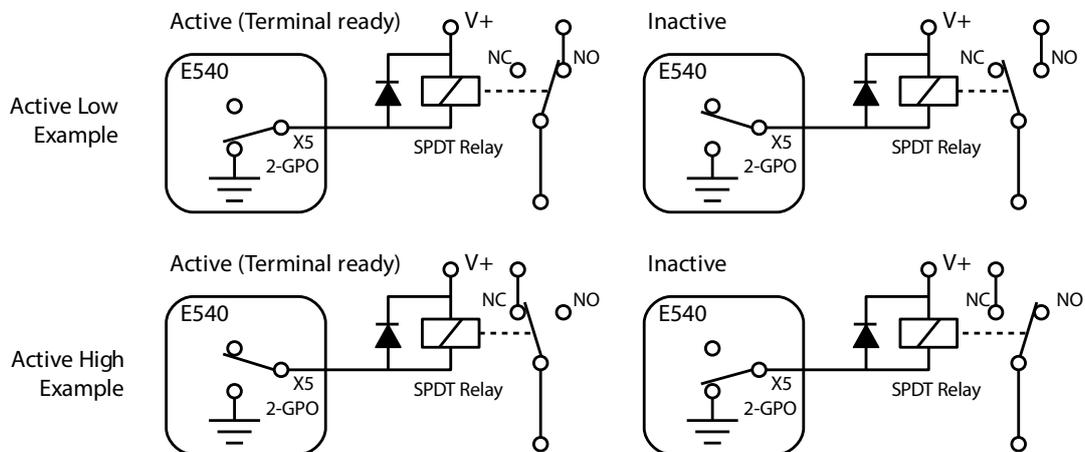


Note  | Place a flyback diode close to the terminals of the relay coil as shown.

## 3.9.2    Control or status with 3-GPIO

### To configure and connect 3-GPIO

3-GPIO is configurable in the web interface to be input or output, and active low or active high.

- For configuration with web interface, see *GPIO pins* on page 4-44.
- For specifications, see *I/O connector (X5)* on page A-5.

### Connection examples for 3-GPIO:

**Configured as output** (V+ = up to 32 VDC):

> **Note** Place a flyback diode close to the terminals of the relay coil as shown below.
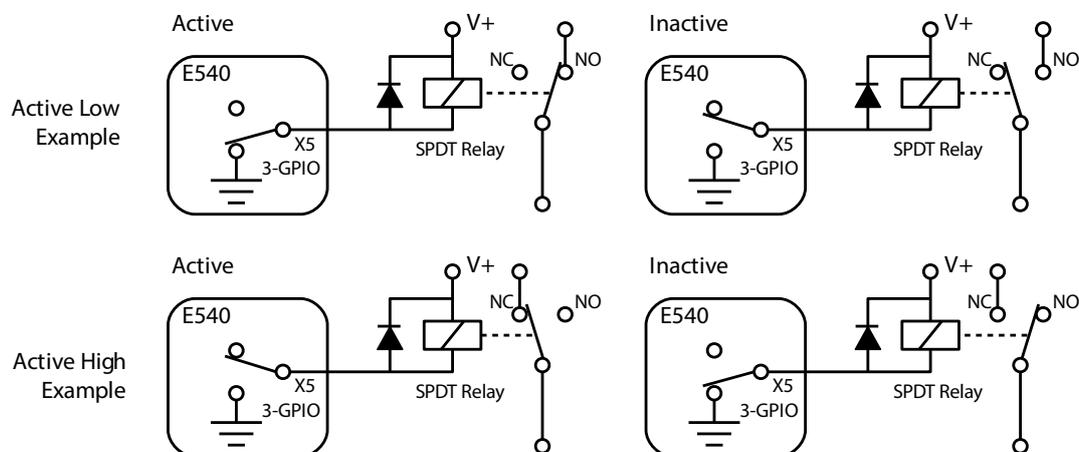


**Configured as input** (*Low: 0 - 0.8 VDC*, *High: 2.8 - 32 VDC*):

> **Note** Place a pull-up resistor (10 kOhm, 125 mW) as shown below.
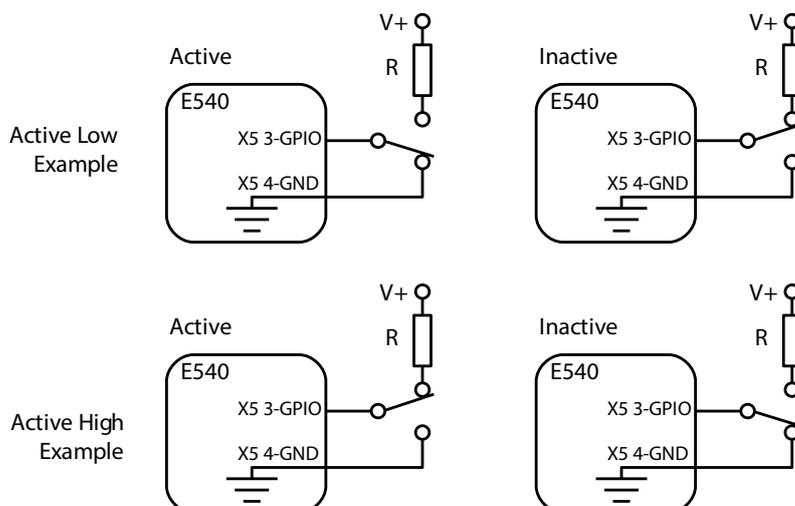


You can use the AT command _ITGPIO to activate or deactivate the pin (if configured as output) or read the status of the pin (if configured as input), see the next sections.

## To read the status of 3-GPIO pin (input) with AT commands

Do as follows:

1. Configure GPIO pin 3 in the web interface to be input.
2. Send the command **_ITGPIO?** to the terminal.
3. You get a response saying whether the pin is active or inactive (1 is active, 0 is inactive). Note that the setting in the web interface determines whether the pin is active high or low.

   **Example:**   **_ITGPIO: 1**
                **OK**

## To activate or deactivate 3-GPIO pin (output) with AT commands

Do as follows:

1. Configure GPIO pin 3 in the web interface to be output.
2. Send the command **_ITGPIO=1** (activate) or **_ITGPIO=0** (deactivate) to the terminal.
3. You get an **OK** response when the pin is successfully activated or deactivated.

# Configuration with web interface

This chapter describes how to use the **web interface** to operate, set up and configure your system. It has the following sections:

- *The web interface*
- *To control data connections from web interface*
- *To set up your data connection packages (BGAN M2M)*
- *Status information*
- *The Control panel*
- *To restart the installation process (BGAN)*
- *To use the logs*
- *Terminal settings*
- *Advanced LAN*
- *To manage connected devices (Traffic control)*
- *To set up tracking and location reporting*
- *Support features*
- *Advanced settings*
- *To enter the SIM PIN in the web interface*
- *Optional: To set up cellular network for data (dual mode)*

# 4.1 The web interface

## 4.1.1 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 Internet browser as described below.

## 4.1.2 To access and navigate the web interface

### To access the web interface

To access the web interface, do as follows:

1. Start up the terminal.
2. Connect your computer to the terminal.
   You can connect locally to the LAN interface or use a remote connection.
3. Open your browser and enter the IP address of the terminal in the address bar.
   For local connection, the default IP address of the terminal is **192.168.0.1**.
   For remote connection, see *Remote access with the web interface* on page 4-10.
4. Enter the user ID and password for the terminal. You can log in as user or administrator. Note that for **first time use** you must log in as administrator with **user id: administrator** and **password: admin**.

   **Important** ▶ If you logged in with the default administrator password you are immediately prompted to change the password. The new password must be a secure password with min. 8 characters consisting of lowercase and uppercase, numbers and special characters.

   Login as normal **user** is only possible if set up first by the administrator. See *To change the user password* on page 4-29.

   **Note** ▶ If you enter a wrong password 5 times in a row, you are locked out for 15 minutes (other users can still access the login page). After 15 minutes you can try again.

   **Note** ▶ Some parts of the web interface may not be accessible if the user permissions are limited. For information on how to set up user permissions, see *To set up user permissions* on page 4-30.

If the installation process is ongoing, the web interface will show a popup window with the progress of the installation process.

You can change the language to **French, German, Russian, Spanish, Portuguese**, **Chinese** or **Japanese**. See *To select the language* on page 4-19.

# Overview of the web interface

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

Name and icon of current page (on opening page: the name of the product)        Icon bar



Breadcrumbs

Contents section

Status section
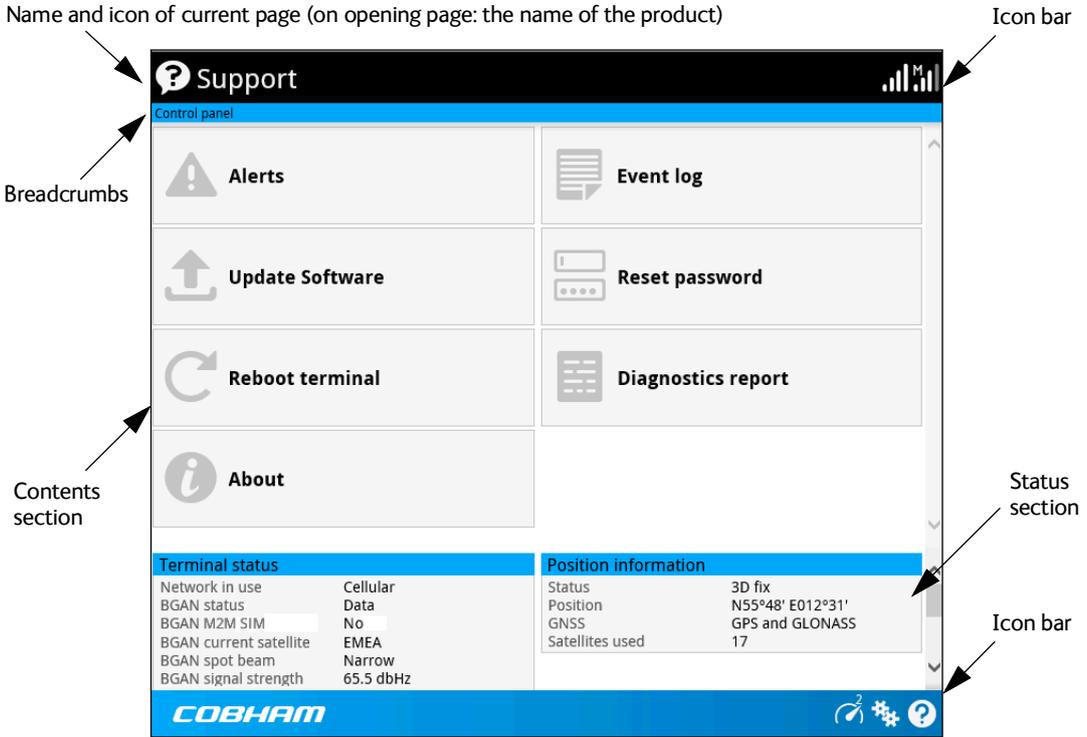
Icon bar

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*.
- **Breadcrumbs** right below the icon bar show the current location in the menu system and gives access to the higher levels in the menu.
- **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 section** shows the status of the terminal and the network connection (BGAN and Cellular if used), 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 |
|---|---|
| .ıll | Signal level of the external network (BGAN). |
| ᴹ.ıll | Signal level of the external network (Cellular). |
| ❷ | Help. Click to get context-sensitive help for the current page. |
| ⚙ | Control panel. Click to access the settings. |
| ⌽ | Dashboard page where you can start and stop data connections. Click to go to the Dashboard page. |
| ⌽¹ | The "1" at the icon shows that a BGAN data connection package 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. |
| ⚠ | 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. |

## 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).

## 4.2　To control data connections from web interface

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

> **Note** With a non-M2M subscription you have more options for the data connection. See Appendix C, *BGAN non-M2M functions*.

### 4.2.1　To start and stop data connections

By default, you must activate your data connection before you can access the Internet. However, you can enable Automatic Context Activation, see *Automatic Context Activation (ACA)* on page 4-7.

> **Note** The icons for starting ▶ and stopping ■ connections are only active if the terminal is ready and registered on the BGAN network. Otherwise the text is grayed out and you cannot start data connections.
>
> If a connection is automatically activated (has ACA enabled), the icons for starting and stopping are replaced by a lock symbol 🔒.
>
> If you have a cellular modem installed and the EXPLORER 540 is in one of the **Cellular modem preferred** modes, you cannot start and stop data connections. For details, see *Limitations in Cellular modem preferred mode and External modem preferred mode* on page 4-58 and *To set up the connection mode* on page 4-16.

To start and stop data connections on your EXPLORER 540, do as follows:

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



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

3. Click ■ to stop the connection.

If data is temporarily suspended, e.g. due to a blockage, the icon on the active connection turns yellow in stead of green, and the **Status** field shows **Data suspended**.

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 4-14.

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

- IP address: The external IP address that has been assigned by the service provider to this session. If the connection was started by remote SMS, the local IP address is also shown.
- Transferred data: For Standard data, the tile shows the total amount of transmitted and received data since the connection was established.

## 4.3    To set up your data connection packages (BGAN M2M)

> **Note** This section only describes the Standard data connection available with M2M subscriptions. For information on BGAN class 2 subscription, see *To set up data connections* on page C-3.

> **Note** You must be logged in as administrator to change the settings for a data package.

### 4.3.1    To change the name of a connection package

To change the name of a connection package, go to the Dashboard and click ⚙ in the right side of the tile with the connection package.
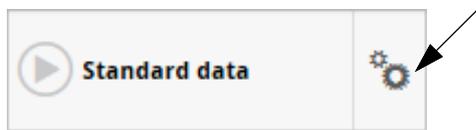


Click **Properties**, type in the new name and click **Save**. The new name is shown on the tile on the startup page.

### 4.3.2    To change the APN for a connection package

By default a connection package is set to use no IP Header compression and to use the APN (Access Point Name) from the SIM card. This is suitable for most applications.

> **Note** It is recommended to leave **IP Header compression** disabled. This means that the data packets are transmitted more reliably with less data loss.

If you want to use a different APN, do as follows:

1. Click ⚙ in the right side of the tile with the connection package that you want to change.
2. Select **Parameters**.
3. Next to **APN**, select the source of the APN.
   * **SIM default** (default and recommended setting): The APN is taken from the SIM card.
   * **Network assigned**: The APN is assigned from the network.
   * **User defined**: APNs are provided from the Airtime Provider. Type in the APN next to **User defined name**.
4. If your APN uses a password, type in the **User name** and **Password** provided from the Airtime Provider.
5. Click **Save**.

## 4.3.3    Automatic Context Activation (ACA)

To enable Automatic Context Activation of your Standard data connection, do as follows:

1. From the Dashboard, click ⚙ in the right side of the tile with the connection package that you want to change.
2. Select **Parameters**.
3. Select **Automatic Context Activation (ACA) of Standard data**.
   - When you **select** ACA, the data connection is automatically established after restart as soon as the EXPLORER 540 and its BGAN connection are ready.
     This setting is mandatory when the terminal is in one of the **Cellular modem preferred** modes.

   > **Note** You are charged for the data transferred. You may want to disable automatic updates in your LAN device to avoid unnecessary charges.

   - When you **disable** ACA, you can control the data connection manually from the startup page ⟳ or with the SMS command ACTIVATE.

## 4.3.4    To create a new connection package

> **Note** You must be logged in as administrator to be able to create connection packages.

Do as follows:

1. Click **New connection package**.
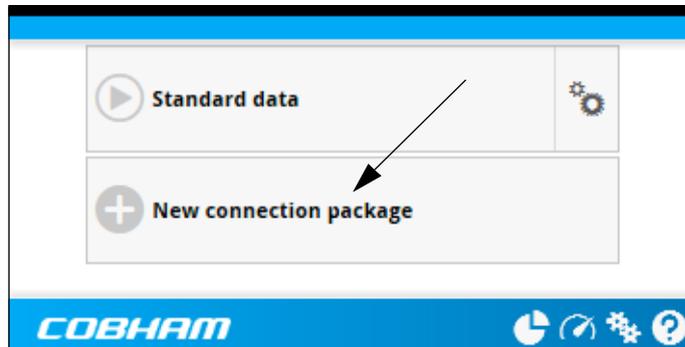


2. Type a **Name** for the new package.
3. If you want to create dedicated connections, select the **Type**. For details on dedicated connections, see *To set up dedicated connections* on page 4-9.
4. Click **Save**
5. Click **Click here to create connections**.
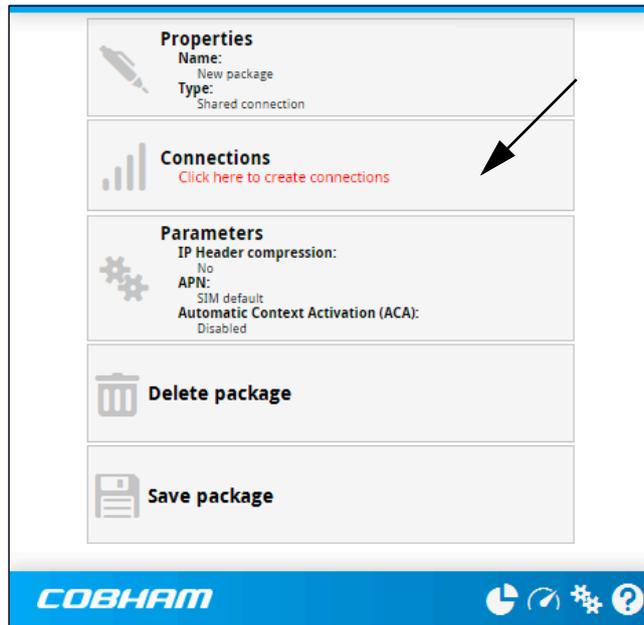
6. Select the connection type you want for your new connection package. For M2M subscription, you can only select **Standard**.

7. Click **Save package**.

The new package should now appear as a new tile on the startup page. For details on **Parameters**, see *To change the APN for a connection package* and *Automatic Context Activation (ACA)* on page 4-7.

## 4.3.5    To set up dedicated connections

You can set up dedicated connections for the EXPLORER 540, e.g. for M2M equipment.

> **Note** The terminal must be in BGAN mode in order to use dedicated connections. Under
> **Terminal settings** > **Connection** > **Mode** select **BGAN only**.

1. From the Dashboard, click **New connection package** to create a new connection package.
2. Under **Type**, select the connection type you want.
   - **Shared connection**. This is the default setting, a shared background data connection. ACA is disabled and there are no dedicated connections.
   - **Dedicated DHCP**. This is a dedicated connection using DHCP. With this type, any DHCP-enabled unit you connect to the EXPLORER 540 will get a new dedicated connection used only for that unit. When you disconnect the unit, the connection is removed after a few minutes. Each new connection gets its own tile on the Dashboard as long as it is running. In the example below, three units are connected using Dedicated DHCP. ACA is enabled for all Dedicated DHCP connections and cannot be disabled, unless you delete the connection package.
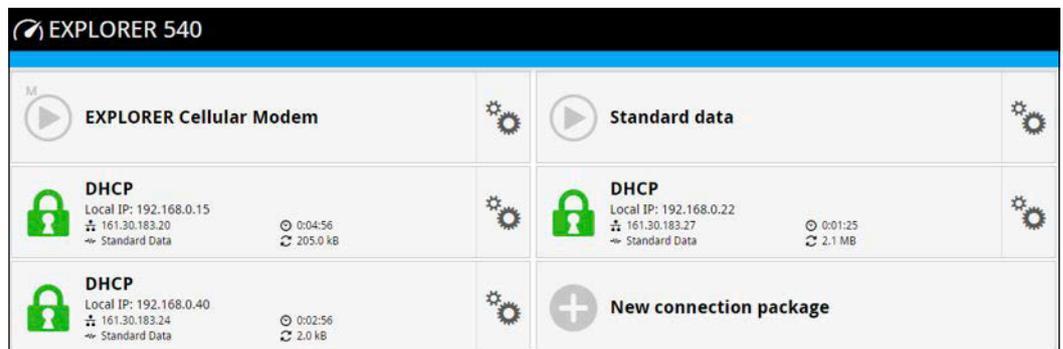


   - **Dedicated static IP**. This is a dedicated connection using a static IP address. Set up the connected unit to use a static IP address and type in this IP address under **Static IP address**.



   If Automatic Context Activation (ACA) is enabled, the connection is established automatically. Only the unit with the configured static IP address can use this connection.

> **Note** You can only start and stop a dedicated static IP connection by enabling and disabling ACA under **Parameters** or using SMS commands.

3. Click **Save**.

# 4.4    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.
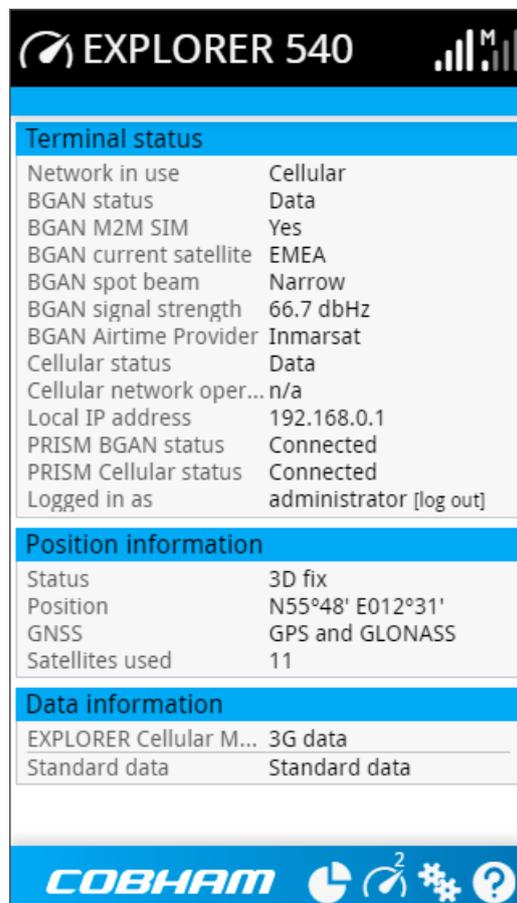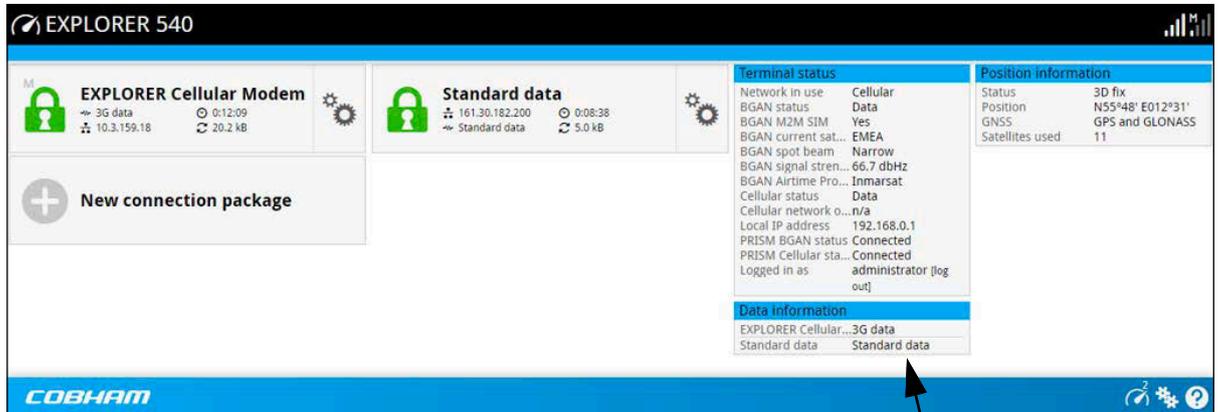


Status field

Toggle between status and contents page

The following status is available:

**Terminal status:**

> **Note** If the terminal is running as BGAN only, the cellular status fields are not shown. Likewise, the PRISM status fields are only shown if PRISM is used.

- Network in use: The network currently used (BGAN or Cellular).
- (BGAN) status: The current status of the BGAN network. In the example in the previous page, Data means a data connection is running. The status could also be e.g. Registering or Ready.
- BGAN M2M SIM: Shows whether or not the BGAN SIM card is an M2M SIM (Yes or No)
- (BGAN) current satellite: The satellite to which the EXPLORER 540 is currently registered.
- (BGAN) spot beam: The type of spot beam currently used, e.g. Regional or Narrow.
- (BGAN) signal strength: The signal strength of the BGAN connection.
- (BGAN) Airtime Provider: The provider of the BGAN services.
- Cellular status: The current status of the cellular network. In the example, a data connection is running.
- Cellular network operator: The operator (or provider) of the Cellular network.
- Local IP address: The local IP address of the EXPLORER 540. E.g. used to connect to the web interface.
- PRISM BGAN status: The status of the BGAN connection to the PRISM server (Connecting or Connected)
- PRISM Cellular status: The status of the Cellular connection to the PRISM server (Connecting or Connected)
- Logged in as: You can log in as User or Administrator. this field shows how you are logged in.

**Position information:**

- Status: Shows the status of the GNSS connection, e.g. if there is 2D fix, 3D fix or no fix.
- Position: The geographic position of the EXPLORER 540.
- GNSS: Shows which GNSS systems are currently used to obtain the position.
- Satellites used: Shows how many GNSS satellites are used to obtain the position.

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

- EXPLORER Cellular Modem: Shows which type of data is running on the cellular connection.
- Standard data: Shows that a Standard data connection is running on the Standard data connection package. This is the only option when the terminal is running in one of the Cellular modem preferred modes.
- Data suspended: Data is temporarily suspended, e.g. due to a blockage.

**Call information** (only shown if a voice call is ongoing, not possible with M2M subscription):

- Status: The status of the call, e.g. Connected or Ringing.
- Call type: Shows whether the call type is Standard voice or Premium voice (3.1 kHz Audio).
- 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.

## 4.5   The Control panel

The **Control panel** is used for accessing the settings and functions of your EXPLORER 540.
To open the **Control panel**, click ✱ from the bottom right corner of the web interface.

## 4.6    To restart the installation process (BGAN)

If you need to restart the installation process, e.g. because the EXPLORER 540 has been moved to another location, click the **Installation tile** in the Control panel. This will reboot the terminal and restart the installation process. For details about the installation process, see *Installation process* on page 2-6.

To start the installation process from the web interface, do as follows:

1. Select ✤ (Control panel) and then **Installation**.
2. Select **OK** to reboot the terminal and start the installation process. Note that you must log into the web interface with user name and password after reboot.
   The BGAN signal strength is shown on the screen during the pointing process.
3. Turn and tilt the antenna slowly until you have obtained the highest possible signal strength. You can use the pointing sound as well as the signal strength shown on screen. For details, see *Installation process for satellite operation* on page 2-7.
4. When the EXPLORER 540 has detected a stable BGAN signal it automatically exits the pointing process and starts to connect to the BGAN network.
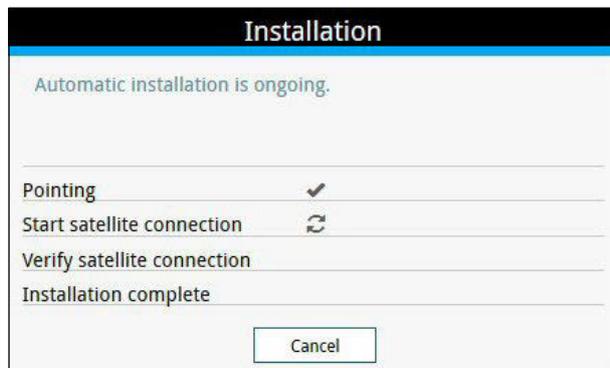


   - If you do nothing, the EXPLORER 540 automatically connects to the BGAN network (if possible) and then completes the installation process.
   - If you want to cancel installation and start over at next power-up, click **Cancel**. You can still configure the EXPLORER 540, and the LED will be active.

   If there are problems with the installation, the web interface will show a warning icon next to the failing step in the installation window. The LED on the EXPLORER 540 will be yellow (warning). See *Troubleshooting guide* on page 5-5.
5. Tighten the screws to fix the EXPLORER 540 in the pointed position.
6. When the installation process has ended, click **Close** to close the **Installation** window.
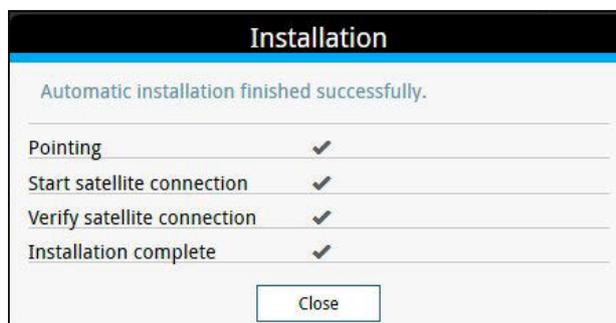
# 4.7 To use the logs

## 4.7.1 To access the logs

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

- **Call log:** 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.
- **Total counters:** Totals for each type of service since the log was last cleared.

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

## 4.7.2 Call log (Non-M2M only)

The Call log shows:

- **Outgoing calls** shows the start time, receiving end phone number, duration, type, termination cause and, if Call charges have been entered, estimated charge of each outgoing call.
- **Received calls** shows the start time, calling phone number, duration, type and termination cause of each incoming call.
- **Missed calls** shows the start time, calling phone number, type and termination cause of each incoming call that was not received.

To clear the Call log, click the **Clear call log** button at the top.

## 4.7.3 Data log

The Data log shows:

- **Standard data** shows data usage, date and time, termination cause and estimated charge of each Standard data session (if Call charges have been entered).
- **For Non-M2M only: Streaming data** shows the duration and type (such as 64 kbps), date and time, termination cause and estimated charge of each Streaming data session (if Call charges have been entered).
- **Cellular modem data** (only present if the optional cellular modem is used) shows data usage, date and time and termination cause of each cellular data connection.

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

## 4.7.4 Total counters

The total counters show:

- **For Non-M2M only: Call session totals** shows the total duration (hh:mm:ss) for each call type since the log was last cleared. It also shows the estimated call charge for each call type (if Call charges have been entered).
- **Data session totals** 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). It also shows the estimated charge for each data type (if Call charges have been entered).
- **Cellular session totals (**only present if an EXPLORER 540 Cellular Modem is used) shows totals for each cellular data connection since the log was last cleared.

To reset the Total counters, click the **Reset total counters** button at the top.

## 4.8    Terminal settings

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

## 4.8.1    To set up the connection mode

### Select WAN network (Mode)

**Cellular network:**

The EXPLORER 540 can use a **cellular network** as an alternative to the BGAN network, if you have installed an EXPLORER 540 Cellular Modem or an external cellular modem.

**For details how to set up the EXPLORER 540 for cellular network**, see *Optional: To set up cellular network for data (dual mode)* on page 4-48.

**BGAN network only:**

1.  If you are **not** going to use a cellular network, leave the **Mode** setting at **BGAN only**.
2.  Under **Timeout parameters**, if you selected Mode **BGAN only**, the following settings are available:

    | Important | Only change these parameters if you know what you're doing! Setting a lower value than the default value may result in undesirable states, such as a fast reboot looping situation where the user interface is inaccessible because of insufficient time to start up. |
    |---|---|

    *   **BGAN connection timeout (seconds)**: The amount of time allowed for the terminal to establish a BGAN connection. If unsuccessful, the terminal will reboot.
    *   **BGAN start reconnection delay (seconds):** The amount of time the terminal waits before trying to re-establish BGAN connection after Connection Watchdog failure.

# Internet and LAN connection modes

In the web interface you can set up the Internet connection mode and the IP addressing between the EXPLORER 540 and devices connected to the EXPLORER 540. The EXPLORER 540 has a built-in DHCP server which can be used to dynamically assign IP addresses to devices connected to the EXPLORER 540.

The drawing below shows examples of the IP addressing in router mode (default setup) and bridge mode.
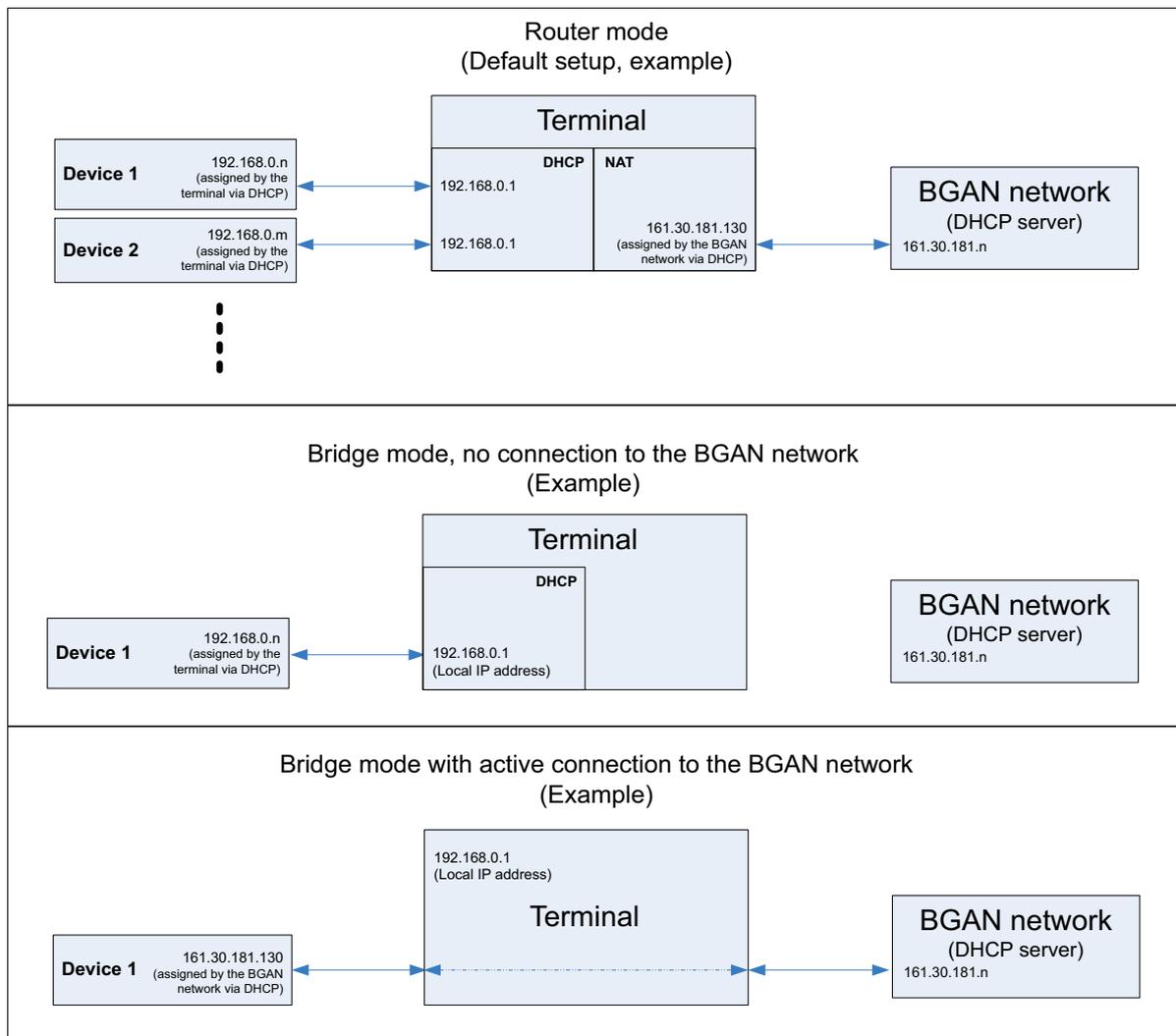
To set up the Internet connection mode of the EXPLORER 540, do as follows:

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 EXPLORER 540 should act as a router. When Router mode is selected, the EXPLORER 540 uses the built-in NAT module for making the necessary address translations.
   - Select **Bridge mode** if only one computer is connected, and the EXPLORER 540 should act as a modem, or more than one computer is connected using an external router.

   **Important** | Bridge mode is only supported in **BGAN only** mode. If you are using a cellular modem, you must select Router mode at Internet connection mode.

   **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: If the IP address assigned by the DHCP server to the locally connected equipment is 161.30.181.130, the terminal will get the IP address 161.30.181.131 (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** | Do **not** use any of the reserved IP addresses listed in *List of reserved IP subnets* on page 6-13.

4. Under **DHCP,** select **Enable** (recommended for most purposes).
   - 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.

5. 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**.

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 **Save**.

## 4.8.2    To enable or disable the pointing sound

The EXPLORER 540 can make a sound to guide you through the pointing procedure (default enabled). To enable or disable the pointing sound, do as follows:

1.  In the **Terminal settings** page, locate the **Audio indication** section.
2.  Select **Audio assisted pointing** if you want to use a pointing sound to assist your pointing process.
3.  At **Audio assisted pointing volume (0 - 100)** type the volume level you want for the pointing sound.
4.  Click **Save**.

## 4.8.3    To select the type of navigation system (GNSS)

To select which navigation system to use with your EXPLORER 540, do as follows:

1.  In the **Terminal settings** page, locate the **GNSS** section (Global Navigation Satellite System).
2.  Select **GPS**, **GLONASS**, **GPS and GLONASS** or **BeiDou**.
3.  Click **Save**. Note that it may take some minutes for the EXPLORER 540 to change the navigation system.

## 4.8.4    To select the language

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

To change the language, do as follows:

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

# 4.9 Advanced LAN

## 4.9.1 Port forwarding

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

> **Note** Normal port forwarding configuration is ignored in Cellular modem preferred (PRISM) mode and External modem preferred (PRISM) mode because all connected units are directly accessible by PRISM port forwarding.

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 SIM default. For details, see *To change the APN for a connection package* on page 4-6.

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 192.168.0.100.

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.
4. Type in the **Incoming port start** and the **Incoming port end**.
   This is the range of port numbers on the EXPLORER 540 for which incoming traffic to the EXPLORER 540 will be forwarded.
5. Type in the **Destination IP address**, which in this example is the IP address of the mail server: 192.168.0.100.
   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 at the server, to which the incoming traffic will be forwarded. If only a single port is used, type the same port for **Destination port start** and **Destination port end**.
7. Click **Save**.

When you have activated a data connection, you can now access the server from the Internet, using the external IP address of the terminal. If you are using the web interface, 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 3-12.

To add more ports for port forwarding, select **+ Forward port** again and repeat the procedure above.

As an alternative to Port forwarding, you may use a dedicated connection, see *To set up dedicated connections* on page 4-9.

## 4.9.2    Static routing

When you have an external gateway connected to your terminal, the terminal is not automatically able to "see" the network on the other side of the gateway. However, you can set up your terminal to communicate with a device on the other side of a gateway, by using Static routing. To set up a new device for static routing, do as follows:

1. From the **Control panel** ⚙, select **Advanced LAN > Static routing.**
2. Click **Add route**.
3. Enter the values for your device.
   - Destination: The IP address you want to route to.
   - Subnet mask: The subnet mask you want to route to.
   - Gateway: The gateway, e.g. the address of a wireless access point or router to which the destination device is connected.
4. Click **Save**.
   The values for the new entry are now in the list. This means that the terminal can communicate with the destination IP address on the other side of the gateway.

## 4.9.3    To change the APN for PPPoE (BGAN only)

For general information on PPPoE and setup of connected equipment, see *PPPoE (Point-to-Point Protocol over Ethernet), BGAN only* on page 3-17.

Before you can establish a PPPoE connection with the EXPLORER 540 you must set up the APN to use. Do as follows:

1. From the **Control panel** ⚙, select **Advanced LAN > PPPoE APN.**
2. Select the **APN** to use for PPPoE. You have the following options:
   - **SIM default**. The APN is taken from the SIM card. This is the recommended option, unless you have special requirements.
   - **Network assigned**. The APN is assigned from the network.
   - **User defined**. Type in the APN at **User defined name**. APNs are provided from the Airtime Provider.
     If you are using a user ID and password for your user-defined APN, you must enter the same user ID and password in your PPPoE setup.
3. Click **Save**.

# 4.10 To manage connected devices (Traffic control)

By default, traffic control is disabled, which means that all traffic is allowed.

With the Traffic control function you can get an overview of devices connected locally to your EXPLORER 540 and control which devices you want to connect. You can also select whether or not they should be allowed to use the BGAN or cellular network. Note that the available settings depend on whether or not you are logged in as administrator.

**Note** | The cellular modem setting is only displayed if an EXPLORER 540 Cellular Modem is installed in the EXPLORER 540. It is **not** shown with an external cellular modem connected.

## 4.10.1 Traffic control (Non-administrator user)

To set up traffic control, do as follows:

1. In the **Control panel** ⚙, click **Traffic control**.
   A list of connected and added devices appears.
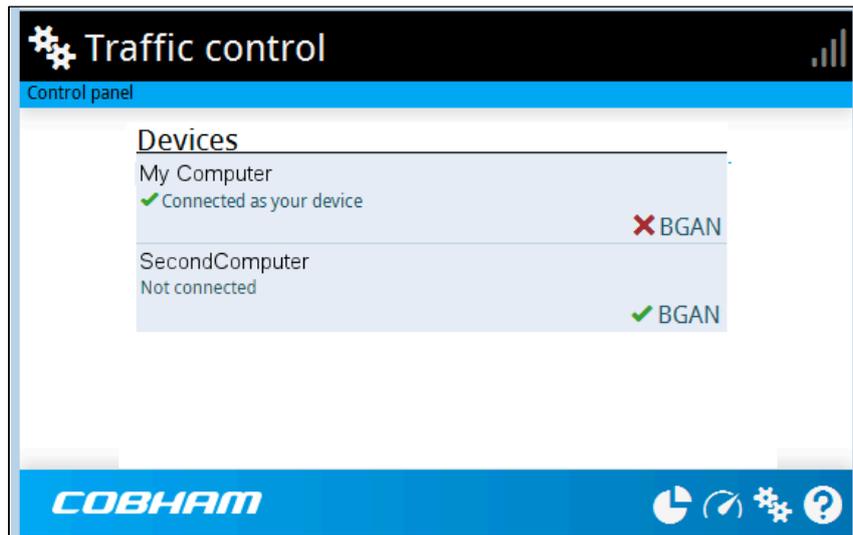


2. Click your connected device to see MAC address and IP address and to change the name or block/allow the use of BGAN or Cellular network. See the next section.

### To block BGAN or cellular traffic or edit the name for your device

**Note** | You can only change these settings if traffic control is enabled. If the administrator has disabled traffic control, all traffic is allowed.

1. In the **Traffic control** page, click your connected device.
   The page shows the name, MAC address, IP address and traffic rule for the device.
2. Select **Block BGAN traffic** or **Block cellular modem traffic** (if available), if you want to deny access to the BGAN or cellular network for your device.

   **Note** | If it is already blocked by the administrator, this setting is not editable.

3. At **Name**, type in the name you want for your device.
4. Click **Save**.

## 4.10.2    Traffic control (administrator)

When you are logged in as administrator, the Traffic control setup offers more options. To set up traffic control as administrator, do as follows:

1. Log in as administrator.
2. In the **Control panel** ✵, click **Traffic control**.
   A list of connected and added devices appears.
3. Click the **Enable** button to enable Traffic control.
   By default Traffic control is disabled, which means all devices are allowed access.

   > **Note** | When you enable traffic control, BGAN is blocked by default for all new devices. To change the default settings, see the next section.



### To change the default settings for all devices

> **Important** | All devices in the list are updated with the default settings when you click Save.

1. Click the button **Default settings**.
2. Select **Block BGAN traffic** or **Block Cellular modem traffic** (if available) if you want to deny access to BGAN or cellular network for all devices. With this option selected, only the administrator will be able to allow access for selected or all devices.
3. Click **Save**.
   All devices in the list will now have the new default settings.

## To block or allow BGAN or cellular traffic or edit the name for a device

1. In the **Traffic control** page, click the device you want to set up.
   The page shows the name, MAC address, IP address and traffic rule for the device.
2. Select **Block BGAN traffic** or **Block Cellular traffic**, if you want to deny access to the BGAN or cellular network for the selected device.
   If you want to allow access, clear the box. The selected device will then be able to access the network, even if it is blocked in the default settings (see previous section).
3. At **Name**, type in the name you want for your device.
4. Click **Save**.

**Reset to default:** You can reset the settings for the device to the default settings.

- If the device is connected and you click the button **Reset to default**, the traffic rules will be reset to the default values set in the previous section, but the name remains the same.
- If the device is not connected and you click the button **Reset to default**, the device is removed from the list.

## To Add a device

When you connect a device, it is automatically added to the list using the default settings. If you want to add a device for later use, do as follows:

1. In the **Devices** page, click the **Add device** button.
2. Type in the **Name** and the **MAC address** for the device.
3. Select **Block BGAN traffic** or **Block Cellular modem traffic**, if you want to deny access to BGAN or cellular network for the selected device.
   If you want to allow access, clear the box. The device will then be able to access the network, even if it is blocked in the default settings (see previous section).
4. Click **Save**.

When the device with this MAC address is connected, it will appear with the entered name in the list, and access will be allowed or denied depending on the setting in this page.

## 4.11 To set up tracking and location reporting

You can set up the EXPLORER 540 to report to a server at certain time intervals. To set up tracking, do as follows:

1. From the Control panel ⚙, select **Tracking and location reporting**.
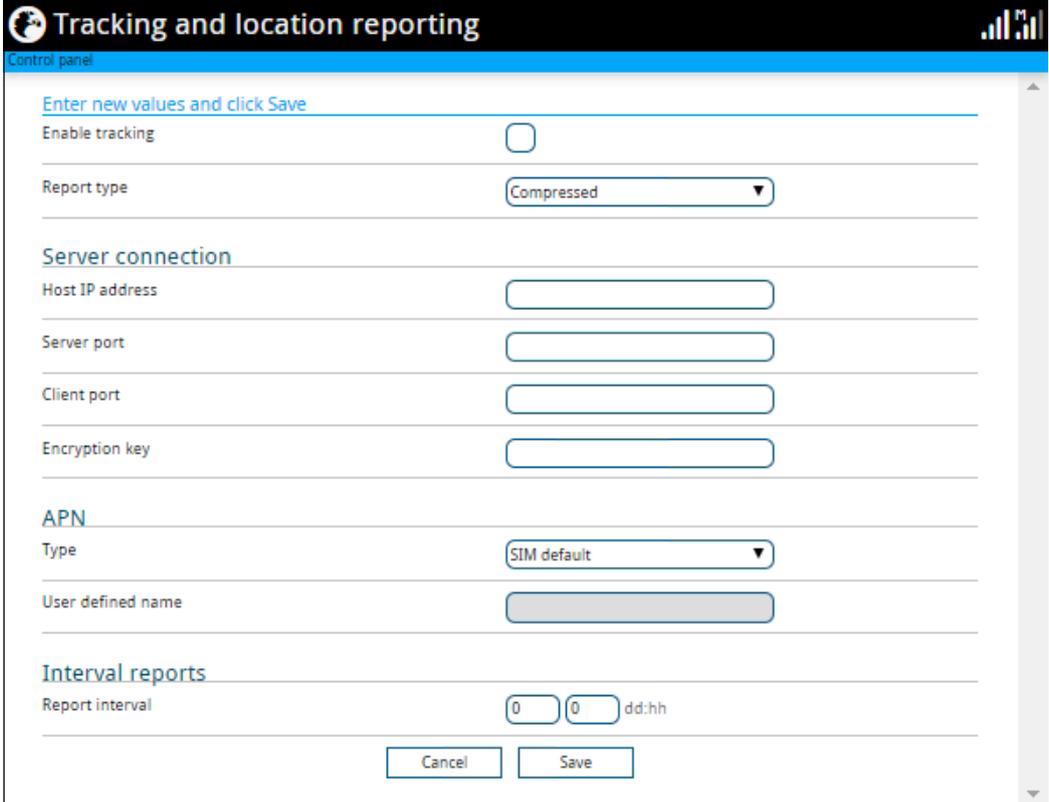


2. To enable tracking of the EXPLORER 540, select **Enable tracking**.

   | Note | Tracking runs on its own BGAN connection, and is independent of the connection mode (Cellular or BGAN).

3. Select the **Report type**.
   - **Compressed**. Only latitude and longitude are reported.
   - **Extended**. Apart from latitude and longitude, heading and altitude are also included.
   - **ECEF**. The same information as Extended, but position and speed data are 3D (ECEF coordinates).

4. Under **Server connection**, type in the following details:
   - **Host**: The IP address of the server that the EXPLORER 540 will report to.
   - **Server port**: Port number on the server. Default number is 7474.
   - **Client port**: Port number on the EXPLORER 540. Default number is 7475.
   - **Encryption key**: A 128 bit key which must match on both the client and server side. Supplied from the server manager.

5. Under **APN**, select the source of the APN.
   - **SIM default** (recommended): The APN is taken from the SIM card.
   - **Network assigned**: The APN is assigned from the network.
   - **User defined**: APNs are provided from the Airtime Provider. Type in the APN next to **User defined APN**.

6. Under **Interval reports**, type in the **Report interval** in days (dd) and hours (hh).

**Example:** If you type in "01" and "12", the EXPLORER 540 will send a report for every 1½ day.

> **Note** If the EXPLORER 540 is in power save state, no report is sent!

7. Click **Save**.

You can see the status of the tracking link in the status area of the web interface. If the status area is not shown, click ◕ to see it.

> **Note** You can set up whether or not you want to allow the tracking server to control these settings. See *Remote control of tracking* on page 4-41.

## 4.12 Support features

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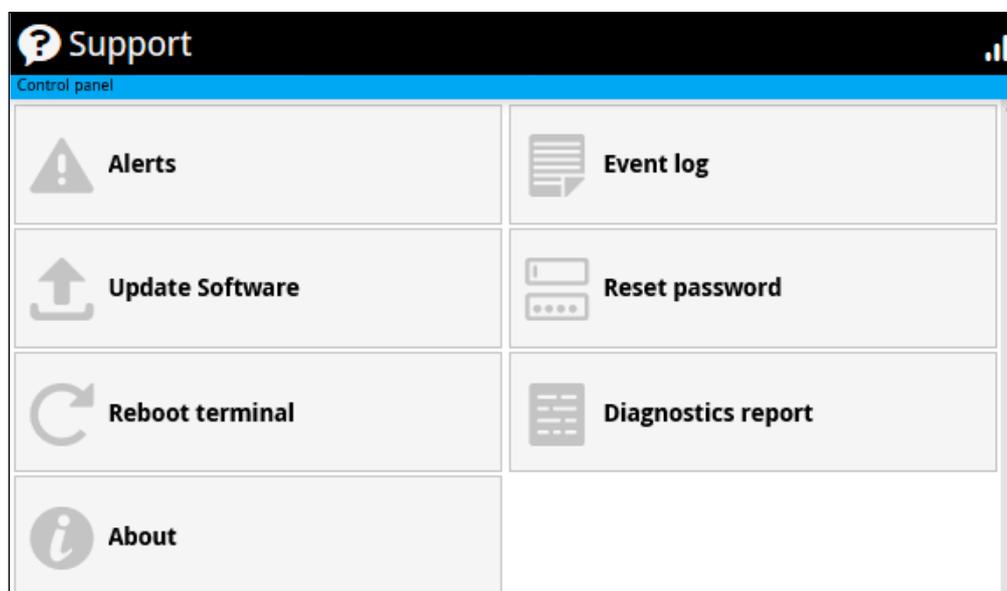


### 4.12.1 To view the Alerts

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 list of active events. For more information on the event messages, refer to *List of messages* on page 5-9.

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

## 4.12.3  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, do as follows:

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.

## 4.12.4  To update software

To update the software in the EXPLORER 540 using the web interface, do as follows:

1. Download the new software[1] or acquire the software from Cobham SATCOM 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. If the installation process is not yet completed, the LED flashes blue during the software update.

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

---

1. You can download the software from the Cobham Satcom Partner Portal at https://partnerportal.cobhamsatcom.com/.

### 4.12.5 To reset the administrator password

If you have forgotten the administrator password, do as follows:

> **Note** | If you have physical access to the EXPLORER 540, you can also use the Reset button. For details, see *Reset button* on page 5-4.

1. Contact your supplier for a reset code.
   Report the serial number and IMEI number of the terminal.
   You can find the serial number and the IMEI number under **Control panel > Support > About**.
2. After receiving the reset code from your supplier, select **Reset password** from the **Support** page.
3. Type in the reset code obtained from your supplier and click **Reset**.
4. The password is reset to **admin**.

### 4.12.6 To restart the terminal

If you want to restart the terminal, do as follows:

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. It is **not** the same as pushing the Reset button, the installation process will not restart.

### 4.12.7 About

The **About** page shows the **Serial number**, **software version, IMSI** and **IMEI** of your EXPLORER 540 as well as legal information. It also shows your **Help desk** information, if it has been entered under **Advanced** > **Help desk**.

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

# 4.13  Advanced settings

## 4.13.1  Passwords

The EXPLORER 540 web interface is password protected at two levels: A user password and an administrator password. You are always prompted for a password when you access the web interface. Default settings are:

- administrator level: User id: **administrator**, Password: **admin**
- user level: **No user level access**. Must first be defined by the administrator; until then you can only access the terminal web interface as administrator.

You can change the passwords when you are logged in as admnistrator.

| **Important** | If you have logged in with the default administrator password you are immediately prompted to change the password. |

### First time use

The first time you access the EXPLORER 540 web interface (and after reset to factory defaults) you must log in as administrator with **user id: administrator** and **password: admin**.

### To log in as administrator

Access to the Advanced settings requires an administrator password. If you are already logged in as user and you want to access the **Advanced** settings, do as follows:

1. From the Control panel ✵, select **Advanced**.
   You are now prompted to log in.

2. Enter the administrator password.
   If you have forgotten the administrator password, you can reset the password. For details, see *To reset the administrator password* on page 4-28. The old user ID and password will apply until you have finished the reset procedure.

3. Click **OK**.

### To change the user password

If you want to enable non-administrator users to use the terminal web interface without getting access to administrator settings, you must first set up a user password.

If no user password is set up, you can only access the web interface using the administrator password.

To change the user password, do as follows:

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.

   | **Note** | The password must be min. 8 characters long and consist of lowercase and uppercase letters, numbers and special characters. |

5. Click **Save**.
   At the next user login the new password is required.

## To change the administrator password

To change the administrator password, do as follows:

1. Log in as administrator.
2. Under **Advanced**, select **Passwords**.
3. Select **Change administrator password**.
4. Type in the **Old password**.
5. Type in the **New password** and retype it on the next line.

   | Note | The password must be min. 8 characters long and consist of lowercase and uppercase letters, numbers and special characters.

6. Click **Save**.
   At the next administrator login the new password is required.

## To log out as administrator

If you close the web interface, you are logged out automatically after 30 seconds. To log out manually, click **Log out administrator** in the **Advanced** page or click **[log out]** next to **administrator** in the **Terminal status** field.

## 4.13.2   To set up user permissions

You can allow or deny users access to certain functions and make these pages read-only. This is useful if you want to protect the system against unintended changes. Study this screen thoroughly and decide to which areas of the system you want to give non-administrator users access. To set up the user permissions, do as follows:

1. Under **Advanced**, select **User permissions**.
2. Under **Allow users to**, select the settings you want to **allow** users to access.
3. Click **Save**.

**Only the settings with a check mark** can be changed by the non-administrator user, other settings can only be viewed.

## 4.13.3   To restore factory settings

To restore the factory settings of the EXPLORER 540, do as follows:

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

> **Important** | All configuration will be lost and the EXPLORER 540 will return to the default configuration.

2.   Click **OK**.
The terminal will now restart and start up with the factory settings. The installation process is also restarted.

## 4.13.4   SIM PIN for BGAN

### To enable or disable the use of a SIM PIN

To enable or disable the use of a PIN to access the BGAN 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 before you can make calls or data sessions
4.   If you selected Require PIN on startup, type in the PIN next to **Enter current PIN**.
5.   Click **Save**.
The new PIN settings will take effect at next power on.

### To change the SIM PIN

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

1.   Under **Advanced**, select **SIM**.
2.   Select **Change SIM PIN**.

> **Note** | The SIM PIN must be enabled before you can change it.

3.   Under **Change PIN** type in the **Current PIN**.
4.   Type in the **New PIN** and retype it on the next line.
5.   Click **Save**. The new PIN settings will take effect at next power on.

## Auto SIM PIN validation

The Auto SIM PIN validation feature allows the EXPLORER 540 to automatically send the PIN to the SIM at power up. This enables the SIM to be PIN locked (to prevent unauthorized re-use of the SIM elsewhere), while still allowing the EXPLORER 540 to connect to the BGAN network without using a PIN.

When this feature is enabled, the PIN you enter when setting the Auto SIM PIN validation feature is encrypted and stored locally in the EXPLORER 540. The next time the EXPLORER 540 restarts, the terminal decrypts the PIN and automatically sends it to the SIM without user intervention.

**Note** | The SIM PIN must be enabled before you can use this feature. See *To enable or disable the use of a SIM PIN* on page 4-31.

To set up the Auto SIM PIN validation feature, do as follows:

1. Under **Advanced**, select **SIM**.
2. Select **Auto SIM PIN validation**.
3. Select **Automatically validate SIM PIN on startup**.
4. Type in the PIN.
5. Click **Save**.

**Note** | If the SIM PIN is changed either using the web interface or AT commands, the Auto SIM PIN validation feature is disabled and must be reenabled manually.

**Note** | If the SIM card is replaced without disabling the Auto SIM PIN validation feature, and the first verification of the SIM PIN fails, the Auto SIM PIN validation feature will disable itself to avoid locking the SIM card.

## SIM lock

The SIM lock feature can be used by suppliers to lock your SIM card to a specific provider or distribution partner. For further information, contact your supplier.

## 4.13.5    SIM PIN for cellular network

See *Optional: To set up cellular network for data (dual mode)* on page 4-48.

## 4.13.6    To save or load a configuration

If you need to reuse a configuration in other terminals of the same type, you can save your current configuration to a file, which can then be loaded into the other terminal(s).

| Note | Be aware that if the terminals have different software versions, some of the settings may be different than expected. If possible, use the same software version in the terminals. |

### To save a configuration to a file

To save the current configuration of your EXPLORER 540 to a file on your computer, do as follows:

1.  In the **Advanced** page, click **Load/save configuration**.
2.  Click **Save configuration**.
    The configuration file is saved in the EXPLORER 540.
3.  Click **Download configuration…**
    The configuration is downloaded from the EXPLORER 540 to the downloads section of your computer.

### To load a configuration from a file

To load a configuration from a file into your EXPLORER 540, do as follows:

1.  In the **Advanced** page, click **Load/save configuration**.
2.  Click **Load configuration**.
3.  Browse to the configuration file and click **Open**.

The configuration is now loaded into your EXPLORER 540. When the configuration is loaded successfully, the EXPLORER 540 restarts with the new configuration.

## 4.13.7 Connection watchdog (Link monitoring)

If you are not using the Terminal watchdog function (see *Terminal watchdog* on page 4-36) nor PRISM, it is strongly recommended to use the Connection watchdog to monitor your IP connection, as it enables you to test the satellite (or cellular) connectivity and to keep your PDP context alive.

> **Note** | The Connection watchdog does not work with PRISM.

The function is slightly different if you are using the cellular network with the optional EXPLORER 540 Cellular Modem installed. The function is described below for BGAN only and then for cellular connection.

> **Note** | We recommend enabling ACA (Automatic Context Activation) if it is important to always have an active connection. See *Automatic Context Activation (ACA)* on page 4-7.

### Function with BGAN only

With the connection watchdog activated, the terminal will send out ping commands to up to three servers of your choice. When a data session is started, the terminal will start sending ping commands to the Primary IP address the number of times specified. If no response is received, it will send the same number of ping commands to the Secondary and then the Tertiary IP address, if available. If no response is received from any of the IP addresses, the terminal will first try to reconnect (if ACA is enabled). If it fails again the terminal will eventually restart.

> **Note** | Ping commands are sent on all active data connections. For the Connection watchdog to work, the data connection must be (re)started after enabling the Connection Watchdog. If ACA is enabled, the data connection is restarted automatically. See *To start and stop data connections* on page 4-5.

### Function with optional Cellular network

When using the cellular network with the connection watchdog activated, the terminal will send out ping commands to up to three servers of your choice. When a data session is started, the terminal will start sending ping commands to the Primary IP address the number of times specified. If no response is received, it will send the same number of ping commands to the Secondary and then the Tertiary IP address, if available. If no response is received from any of the IP addresses, the terminal will switch to the BGAN connection and repeat the pinging over the BGAN network. If it still fails, the terminal will eventually restart.

## To set up the Connection watchdog

Do as follows:

1.  Under **Advanced**, select **Connection watchdog**.
2.  Select **Enable Connection watchdog**.
3.  At **Ping interval (seconds)** write the interval in **seconds** between the ping commands on the BGAN connection.
    *   Minimum interval is 4 seconds, default is 300 seconds (5 minutes).
    *   Depending on the Ping mode (step 9), this interval is the time from **last ping** or from **last transmission**.
4.  Write the **Number of retries** on the BGAN connection.
    *   The number of retries applies to each of the listed IP addresses (step 10). This is the number of times that the terminal will retry after a ping has failed.
    *   The time between the retries on the BGAN connection is set to 20 seconds.
    *   20 seconds after the stated number of retries on an IP address, the next IP address on the list is pinged with the same number of retries.
5.  At **Ping interval after failure (seconds)**, write the number of seconds between pings after a ping failure on the BGAN connection. The interval can be from 3 to 255 seconds, default is 20 seconds.
6.  At **Ping interval - cellular (seconds)** write the interval in seconds between the ping commands on the cellular connection.
    *   Minimum interval is 3 seconds.
7.  At **Number of retries - cellular** write the number of retries on the cellular connection.
    *   The number of retries applies to each of the listed IP addresses (step 10). This is the number of times that the terminal will retry after a ping has failed.
    *   The time between the retries is set in the next step (Ping interval after failure - cellular)
    *   After the stated number of retries on an IP address (plus the interval defined in step 8), the next IP address on the list is pinged with the same number of retries.
8.  At **Ping interval after failure - cellular (seconds)**, write the number of seconds between pings after a ping failure on the cellular connection. The interval can be from 3 to 255 seconds, default is 20 seconds.
9.  Select the **Ping mode.**
    *   **Ping always**: Always send ping, regardless of data traffic.
    *   **Ping when no traffic**: Send ping only if no data traffic is ongoing.[1]
10. Write the Primary and optionally the Secondary and Tertiary IP address. This is the IP address of the server(s) to which the terminal will send ping commands.

    > **Note** Use a server that is reliable and that responds to ICMP Echo Requests.

11. Click **Save**.

    > **Note** When the Connection watchdog settings are saved the terminal ends any active connections. If ACA is enabled the BGAN connection restarts automatically.

---

1.  This setting only applies to BGAN - the cellular connection will always ping, regardless of data traffic.

## 4.13.8    Terminal watchdog

The Terminal watchdog continuously monitors the operational status of the terminal and allows you to perform the following actions at regular intervals (set by the user):

- Wake up the terminal from power save state
- Start a data connection (PDP context)
- Check your IP connection (ping - similar to Connection watchdog, but only on the data connection started by the Terminal watchdog)
- Send a position SMS or a loopback SMS to verify SMS connection

The terminal continuously monitors:

- The time (monitors that UTC time is received from GPS at startup)

> **Note** | The EXPLORER 540 operates with UTC time, local time is not available.

- CS-attach (the status of circuit-switched connection)

If any of the actions fail, the terminal restarts.

### Set up Terminal watchdog

To set up the Terminal watchdog, do as follows:

1. Under **Advanced**, select **Terminal watchdog**.

Terminal watchdog

| | |
|---|---|
| Enable watchdog (requires reboot) | ☑ |
| Wake terminal from power save | ☑ |
| Watchdog interval | [0] days [12] hours |
| Primary IP address | 4.2.2.1 |
| Secondary IP address | 8.8.8.8 |
| Tertiary IP address | 4.2.2.2 |
| APN | SIM default ▼ |
| User defined name | |
| User name | |
| Password | |
| Enable position SMS | ☐ |
| Send position SMS to phone number | |
| Enable loopback SMS | ☐ |
| Terminal SMS number | |
| Next run time | 2019-09-04 13:41 |

Cancel    Save

2. Select **Enable watchdog**.
3. Select **Wake terminal from power save** if you want the terminal to wake up from power save state each time the watchdog interval has passed.
   If this option is not selected, the Terminal watchdog will only run when the terminal is awake.
4. Select the **Watchdog interval**.
   The interval can be from one hour up to 21 days.
5. Type in the **Primary** and optionally the **Secondary** and **Tertiary IP address.**
   This is the IP address(es) of the server(s) to which the terminal will send ping commands.

The terminal will start sending ping commands to the Primary IP address. If there is no response after 10 attempts, the terminal will send up to 10 ping commands to the Secondary and then the Tertiary IP address, if available. If no response is received from any of the IP addresses, the terminal will eventually restart.

> **Note** If no IP addresses are entered pinging is skipped, but the other actions still apply.

6. Enter the **APN** (and user name and password if required) to use for the data connection.

7. Select **Enable position SMS** and enter the phone number, if you want the terminal to send SMSes with the position of the terminal to a phone number. The SMSes will be sent with the Watchdog interval from step 4.

8. Select **Enable loopback SMS** and enter the phone number of the terminal, if you want the terminal to send SMSes to itself in order to check the SMS function. The SMSes will be sent with the Watchdog interval from step 4.

9. Click **Save**.

> **Note** When the Watchdog is enabled, you must reboot the terminal before the Watchdog settings are activated.

**Next run time:** This field at the bottom of the page shows what time the Terminal watchdog will run next (UTC time).

## 4.13.9 Data limits (BGAN only)

You can set a limit for the use of the BGAN data services with the EXPLORER 540 system. If you have entered the call charges in the menu **Call charges**, the system automatically calculates and displays the estimated maximum charges for your data sessions.

> **Note** Thrane & Thrane A/S does not take responsibility for the correctness of the estimated charges. This calculation is only a rough estimate of the charge, based on the tariff entered by the user. Also, the airtime provider may have different methods of calculating the charge.

Once the entered limit is reached, the connection is automatically stopped. This is recorded in the data log. To continue using the data service you must start a new connection by clicking on the desired connection on the startup page.

> **Note** If you have enabled automatic context activation of the Standard data connection and you set a data limit for the Standard data connection, automatic context activation is **disabled**.

To set data limits, do as follows:

1. Under **Advanced**, select **Data limits**.

2. Select the type of connection you want to limit.

3. Type in the amount of data or time allowed and select the appropriate units.

> **Note** The limit is **per PDP context**. This means that if you have e.g. two Standard data connections running, and one of them reaches the limit for Standard data, only that connection closes down, but others can still continue to run until they also reach the limit.

4. Select **Enable**.

5. Click **Save** to save the settings.

## 4.13.10  Call charges (BGAN only)

> **Note**  Thrane & Thrane A/S does not take responsibility for the correctness of the estimated charges. This calculation is only a rough estimate of the charge, based on the tariff entered by the user. Also, the Airtime Provider may have different methods of measuring the airtime used.

If you know the tariff for your subscribed BGAN services, you can enter these tariffs in the web interface and automatically calculate the estimated charges for your calls and data sessions. To enter the call tariffs, do as follows:

1. Under **Advanced**, select **Call Charges**.
2. Select the currency from the **Displayed currency** drop-down list.
3. Enter the tariff for each of the services.
4. Click **Save**. The entered tariffs are used for estimating the charges for calls and data sessions. For further information, see *Call log (Non-M2M only)* on page 4-14.

## 4.13.11  Remote management

You can set up the terminal so that it can be controlled from a remote location.

To set up the terminal for remote management, select **Advanced** > **Remote management** from the **Control panel**.

## To set up remote access with IP

> **Note** The settings for Remote access with IP are **not** relevant if you are using the **_IREMWEB** command. See *To use AT commands to get remote access to the web interface* on page 3-10.

1. From the **Remote management** page, select **Enable access to web application** and/or **Enable access to AT commands**.
2. Type in the **Incoming port** numbers to use for the web server and for AT commands. The default port numbers are:
   - web server: 80
   - AT commands: 5454

   > **Note** If you type another port number, the port number must be available at your service provider.

3. Under **Trusted IP addresses**, click **Add IP address** and type in the IP address of the device you want to give access to the terminal.
4. To add more IP addresses, click **Add IP address** again.
5. Select **Enable ping response** if you want to enable the terminal to respond to ping commands.

   > **Note** To be able to access the terminal you must have an active data connection.

After preparing the terminal and activating the connection you can access the terminal from one of the trusted IP addresses, using the incoming port defined in the Incoming port field.

- For information on how to prepare the terminal for remote activation of a data connection, see the next section *To set up remote access with SMS*.
- For information on how to access the terminal, see *To access the terminal from a remote location* on page 3-4.

If Static IP is included in your airtime subscription, we recommend using this 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 airtime subscription and you must set the APN source to SIM default. For details, see *To change the APN for a connection package* on page 4-6.

## To set up remote access with SMS

> **Note** The terminal must be registered to the satellite services to receive and accept an SMS.

1. From the **Remote management** page, select whether you want to **Enable remote SMS commands**.

   > **Note** If you are using a cellular connection as your primary network connection, the SMS commands will be sent over the BGAN backup connection. Note that some SMS commands will not work, see *Remote access with SMS* on page 3-4.

2. Enter the password for remote SMS. It can be 5 to 15 characters long. The characters 0-9, a-z and A-Z are allowed. **The password is mandatory**. This password must be entered every time you send an SMS command. Default password is **remote**.

   > **Important** Change the password in order to keep the terminal protected.

3. Clear the box **Trust all phone numbers** and enter at least one trusted mobile number from which the terminal accepts an SMS. Use the wild card * to accept a range of trusted numbers.

| Entered mobile number with wild card | Mobile numbers accepted |
|---|---|
| +453955880* | +4539558800 to +4539558809 |
| +45395588* | +4539558800 to +4539558899 |



4. To add more phone numbers, click **Add phone number** again.
5. Click **Save**.

For information on how to send SMS commands, see *Remote access with SMS* on page 3-4.

## 4.13.12  Remote control of tracking

When you are using the tracking function of the EXPLORER 540, you can set up the terminal so that the tracking server can access the EXPLORER 540 e.g. to start or stop tracking or to change reporting intervals.

To allow the tracking server to control the tracking settings, do as follows:

1. Under **Advanced**, select **Tracking settings.**
2. Select **Allow remote control of tracking**.
3. Click **Save**.

The EXPLORER terminal will now accept commands from the specified tracking server, for example to change reporting intervals or start/stop reporting.

## 4.13.13  Power control

There are a number of options to save power in the EXPLORER 540. For a general description of the power save options, see *Power control* on page 3-19.

To set up the power save options, do as follows:

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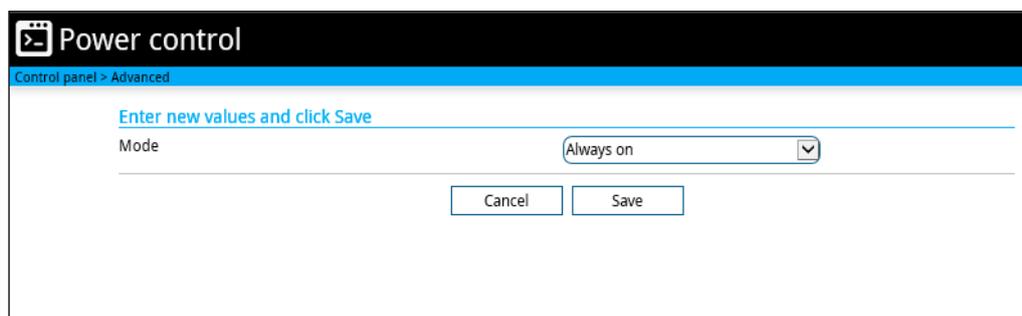


2. Select the mode you want to use.
   - **Always on**. This is the default setting. The terminal will never go into power save state but will always be on when connected to power.
   - **Idle power save**. The terminal will go into power save state after a (configured) period with no activity. For details, see the next section *Idle power save mode*.
   - **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 *Remote on/off mode* on page 4-43.
3. Click **Save**.

## Idle power save mode

1. In the **Power control** page, select **Idle power save** from the drop-down list.



> **Important** When you select Idle power save mode you must enable minimum one wake-up method (Daily wake up, Wake-on-LAN and/or Power control pin).

2. Select how many minutes with no activity before the terminal should enter power save state (Idle time before power save).

3. Select **Prevent power save if satellite connection is active** if you do not want the terminal to enter power save state while a data connection (PDP context) is opened on the satellite connection.

   > **Note** With this option selected, the terminal will not enter power save state if there is a PDP context open, even if it is not currently used to send or receive data.

4. Under **Daily wake up**, select **Enable** and enter the **Wake up time of day** if you want the terminal to "wake up" from power save state at a specific time every day.

   > **Note** Local time must be converted to UTC time!

5. Under **Wake-on-LAN**, select **Enable** if you want the terminal to wake up from power save when the LAN port receives a magic packet from locally connected equipment.

6. Under **Power control pin**, select **Enable wake up when activated** if you want to use the power control signal (e.g. connected to the ignition of your vehicle) to wake up the terminal from power save state.

   > **Note** With this option selected the terminal will be active when the Power control pin is active.

   Set the polarity (Active high/Active low) for the power control pin.

7. Click **Save**.

## Remote on/off mode

1.  In the **Power control** page, select **Remote on/off** from the drop-down list.

    | Important | Be aware that once you have enabled the Remote on/off function, the EXPLORER 540 will be in power save state until you have connected the Remote on/off wire **and** it is active, or one of the other conditions that can prevent power save is present! See *Power control* on page 3-19. |
    |---|---|

    

2.  At **Delayed shut down**, select the wanted shut-down delay after the power control pin is deactivated.

3.  At **Daily awake period**, select **Enable** and enter the start time and duration of the awake period, if you want the terminal to have a fixed awake period every day.

    | Note | Local time must be converted to UTC time! |
    |---|---|

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 **Save**.

## 4.13.14  GPIO pins

The EXPLORER 540 has 3 I/O pins, two assigned pins and 1 general purpose pin.

- Power control (input). Note that this input is configured under *Power control* on page 4-41.
- Terminal ready (output)
- Control/Status (input/output)

Do as follows to configure 2-GPO (Terminal ready) and 3-GPIO (General purpose):

1. Under **Advanced**, select **GPIO pins.**



2. Select whether the **2-GPO (Terminal ready)** output should be active high or low. This output signals when the EXPLORER 540 is registered on the BGAN network and is ready to communicate with connected equipment. For details, see *Terminal ready signaling with 2-GPO* on page 3-28.

   > **Note**  "Terminal ready" only signals that the terminal is awake, registered on the BGAN network and ready to communicate with connected equipment. It does **not** show whether or not a data connection is established. See *Power control* on page 3-19 and *Automatic Context Activation (ACA)* on page 3-15.

3. If you want to use 3-GPIO (General purpose), select the direction and polarity.
   The 3-GPIO pin does not have a predefined function, but can be used for remote control/status of connected equipment using AT command **_ITGPIO**. See *Control or status with 3-GPIO* on page 3-29.

4. Click **Save**.

## 4.13.15  Help desk

Under Help desk you can enter the contact information you want for your EXPLORER 540. The Help desk contact information is empty by default. You must provide the contact information, e.g. the phone number for your Airtime Provider. Do as follows:

1. In the **Advanced** page, select **Help desk**.

2. Type in the contact information you want.

3. select **Save**.

The Help desk information is now available from ⚙ (Control panel) > **Support > About**.

## 4.13.16  Reset button

You can change the function of the Reset button. See *Reset button* on page 5-4. Do as follows:

1. From the **Advanced** page, select **Reset Button**.
2. Select the behavior you want for the Reset button.
   - **Enabled**: Short push: The EXPLORER 540 restarts (power cycle) and begins the installation process again, Long push: Reset to factory default.
   - **Long press disabled**: The Reset button will not be able to reset to factory default, but the short push function (power cycle) will still work.
   - **Disabled**: The Reset button can only be used for safe mode (see *Recovery software update* on page 5-3).
3. Click **Save**.

## 4.13.17  Security

### To enable the use of a Cobham Satcom IP Handset

> **Note** | This setting applies to the EXPLORER IP+ Handset as well as to the Thrane IP Handset.

The Thrane IP Handset is not relevant in M2M systems.

> **Important** | This setting is disabled by default, and **should be left disabled**, if you do not intend to use the Thrane IP Handset.

For details, see *To enable the use of Thrane IP Handset* on page C-8 and the user manual for the EXPLORER IP+ Handset or the Thrane IP Handset.

### To allow the use of AT commands on LAN interface

1. Under **Advanced** > **Security**, locate the field **AT commands**.
2. Select **Allow on LAN interface** if you want to allow the use of AT commands.
3. If you want users to be able to use AT commands on the LAN interface without entering a password, remove the check mark at **Require password**.
   By default, users must enter administrator password (with the _ICLCK command) before they can send AT commands on the LAN interface.
4. Click **Save**.

### HTTPS settings

The EXPLORER 540 internal web server supports HTTPS, which includes encryption of the exchanged web traffic when accessing the EXPLORER 540 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.

Do as follows:

1. Under **Advanced** > **Security**, locate the field **HTTPS**.
2. Select **Redirect HTTP to HTTPS** if you want the EXPLORER 540 to automatically redirect your HTTP traffic to HTTPS.

3.  Select **Use uploaded TLS/SSL** certificate and click **Upload certificate** if you want to upload and make the system use you own generated SSL certificate. 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 **Save**.

## 4.14   To enter the SIM PIN in the web interface

| Note | Whether you are using the BGAN network or a cellular network, you need a SIM card to access the network. The BGAN SIM card is inserted in the terminal and if you are using the EXPLORER 540 Cellular Modem the SIM card is inserted in the modem. |
| --- | --- |
| | The method for entering the PIN is the same for both types of network. |

### 4.14.1   Do you need a SIM PIN?

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 and whether or not the Auto SIM PIN validation is used. The administrator can enable and disable the use of a SIM PIN and set up Auto SIM PIN validation. For details, see

- *To enable or disable the use of a SIM PIN* on page 4-31
- *Auto SIM PIN validation* on page 4-32

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

| Important | If your EXPLORER 540 is used in an unmanned M2M system, you will normally not be able to enter a PIN code. In this case we strongly recommend enabling **Auto SIM PIN validation** in the web interface before using the system. See *Auto SIM PIN validation* on page 4-32. |
| --- | --- |

### 4.14.2   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 Internet. 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 access the Internet.

### 4.14.3   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 for BGAN** or **Enter PIN for cellular modem**.
3. Type in your PIN and click **OK**.

## 4.15 Optional: To set up cellular network for data (dual mode)

The EXPLORER 540 is a BGAN terminal by default. However, if you are within coverage of a cellular network, you may want to acquire an EXPLORER 540 Cellular Modem or an external modem with LAN interface as an alternative to the BGAN network. Note that you need a separate SIM card for the cellular modem to access the cellular network, the EXPLORER 540 SIM card can only be used for the BGAN network.

For general information of the EXPLORER 540 function with the cellular network, see *Optional: To use a cellular network (dual mode)* on page 1-8.

### 4.15.1 To set up the EXPLORER 540 for cellular operation

To enable the EXPLORER 540 to use the cellular network, do as follows:

1. Acquire one of the following:
   • an EXPLORER 540 Cellular Modem from Cobham SATCOM and matching antenna(s), or
   • an external modem with LAN interface.
2. Install the EXPLORER 540 Cellular Modem as described in the installation guide supplied with the modem, or
   If you are using an external modem, connect the modem to the LAN interface of the EXPLORER 540 and set up the modem according to the modem documentation.
3. Connect your computer to the EXPLORER 540.
4. Access the web interface and set up the EXPLORER 540 as described in the next sections.

> **Note** For optimal operation in dual mode, set up the WAN switching settings and the connection watchdog, and optionally PRISM. This will ensure the best possible switchover between the cellular connection and the BGAN backup connection.

   • WAN switching and PRISM[1]: *PRISM/WAN switching* on page 4-54.
   • Connection watchdog: *Connection watchdog (Link monitoring)* on page 4-34.

---

1. PRISM requires installation and configuration of a server and configuration of the EXPLORER 540, see *EXPLORER 540 operation in Cellular modem preferred (PRISM) mode and External modem preferred (PRISM) mode* on page 4-60.

## To select the cellular network

1. Select ⚙ (Control panel) > **Terminal settings** and locate **Connection**.



2. At **Mode**, select from the drop-down list which mode you want for the EXPLORER 540. You have the following options:
   - **BGAN only** (default): The EXPLORER 540 uses BGAN.
   - **Cellular modem preferred**: The EXPLORER 540 uses the EXPLORER 540 Cellular Modem with the cellular network when it is available, with BGAN as backup. BGAN can still be used e.g. for remote access with SMS. If an EXPLORER 540 Cellular Modem is not connected, or if the cellular network does not work, the BGAN connection is used. For details, see *EXPLORER 540 operation in Cellular modem preferred or External modem preferred mode* on page 4-58.
   - **Cellular modem preferred (PRISM):** Similar to Cellular modem preferred mode, the EXPLORER 540 uses the EXPLORER 540 Cellular Modem with cellular network when it is available, with BGAN as backup. But with PRISM, all traffic is routed through a Multi-Path tunnel to/from a server, providing a continuous connection through a single IP address, independent of the network technology (cellular or BGAN).
     For general information, see *EXPLORER 540 operation in Cellular modem preferred (PRISM) mode and External modem preferred (PRISM) mode* on page 4-60.
     For setup of PRISM see *To set up PRISM* on page 4-55.
   - **External modem preferred:** Same function as Cellular modem preferred, but instead of the EXPLORER 540 Cellular Modem, an external modem is connected via the LAN interface of the EXPLORER 540.

   **Important** ▶ Before selecting this option, set up the Connection watchdog to monitor the connection (see *Connection watchdog (Link monitoring)* on page 4-34). Otherwise the terminal will **not be able to detect if the cellular connection is lost**, and consequently will not switch over to BGAN backup.

   - **External modem preferred (PRISM):** Same function as Cellular modem preferred (PRISM), but instead of the EXPLORER 540 Cellular Modem, an external modem is

connected via the LAN interface of the EXPLORER 540. PRISM will monitor the connection.

If you are using an external modem connected to the LAN interface, See also *To set up an external cellular modem* on page 4-53.

3.  Under **Timeout parameters**, if you selected one of the cellular modes, the following settings are available:

> **Important** ▶ | Only change these parameters if you know what you're doing! Setting a lower value than the default value may result in undesirable states, such as a fast reboot looping situation where the user interface is inaccessible because of insufficient time to start up.

- **BGAN connection timeout (seconds)**: The amount of time allowed for the terminal to establish a BGAN connection. If unsuccessful, the terminal will reboot.
- **BGAN start reconnection delay (seconds):** The amount of time the terminal waits before trying to re-establish BGAN connection after losing connection to the PRISM server or after Connection Watchdog failure.The purpose of the delay is to give some time for the BGAN satellite fix to complete if the terminal lost sight.
- **BGAN reconnection timeout (seconds)**: The amount of time allowed for the terminal to re-establish BGAN connection after 'BGAN start reconnection delay'.
- **Cellular connection timeout (seconds)**: The amount of time allowed for the terminal to establish a cellular connection. If unsuccessful, the terminal will try to set up a BGAN connection if it is not already up.
- **Override cellular minimum reboot timer**: Allows you to modify 'Cellular minimum reboot timer' field.
- **Cellular minimum reboot timer (seconds)**: By default, the terminal attempts to connect to the cellular network (via AT commands) around 6 times per hour from shorter intervals to longer ones. All this happens during one cellular modem power cycle.
  This gradual increase of the interval between connection attempts is done to avoid excessive connection requests that may temporarily restrict the SIM card from connecting to the cellular provider. At the moment, only AT&T is known to penalize excessive connection requests.
  To make the cellular modem power cycle for every connection timeout, set this field lower than 'Cellular connection timeout'.

> **Note** ▶ | In some situations, a power cycle of the cellular modem  may be needed to re-establish connection. By default, it takes 1 hour from the last cellular modem boot/reboot event to power cycle the modem.

4.  Click **Save**.

5.  When the modem is set up and connected, the opening page of the web interface shows a new tile with the cellular connection. The "M" on the tile for the cellular modem indicates that it is a cellular modem and not a BGAN connection.
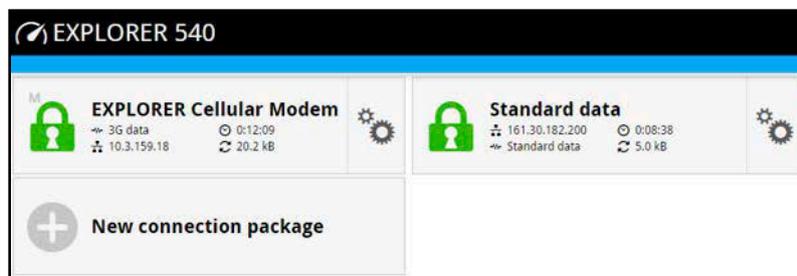
> **Note** | If the **BGAN link mode** in the PRISM/WAN switching page is **Always connected**, the Standard data connection on the BGAN network will still be running in the background and cannot be stopped. See *PRISM/WAN switching* on page 4-54.

6. If required, select ⚙ on the tile to set or change the name or the APN of your cellular connection. For details, see the next section.

When the connection is established, an "M" on the signal bar in the top right corner indicates that it is a cellular (<u>M</u>odem) connection, and the tile shows details about the connection.

The data connection is automatically established when set up correctly, so you cannot start and stop connections from the tiles as you can when the terminal is in BGAN mode.

> **Note** | You may have to enter a PIN before you can use the cellular network, see *To enter the SIM PIN in the web interface* on page 4-47.

You can now access the Internet through the cellular network from a device connected to the EXPLORER 540.

> **Note** | You cannot make calls on the cellular network through the EXPLORER 540. Only data connection is possible.

## 4.15.2   To set up the EXPLORER 540 Cellular Modem

> **Note** | This section is only for the **EXPLORER 540 Cellular Modem**. If you have an **external modem connected to LAN**, you must set up the APN, SIM PIN and other settings in the modem. See *To set up an external cellular modem* on page 4-53.

> **Note** | You may not have to change any of the EXPLORER 540 Cellular Modem settings below. The default settings will apply to most setups.

### To set or change the APN for your cellular connection

If the APN for your cellular connection is not set up automatically, you must set it up before you can connect to the cellular network. Do as follows:

1. Select ⚙ on the tile with the cellular connection.
2. Type in the new name for your connection.
3. Type in the name of the APN you are going to use for your cellular connection.
4. If required, type in user name and password for your APN.
5. Click **Save**.

### To disable the use of a SIM PIN

To disable the use of a PIN to access the cellular network, do as follows:

1. Under **Advanced**, select **EXPLORER Cellular Modem**.
2. Select **Enable/disable SIM PIN**.
3. Under **Enable/Disable PIN** 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. **Recommended for M2M operation!**
   - If you select the box, you must enter a PIN before you can use the cellular network.
4. If you selected Require PIN on startup, type in the PIN next to **Enter current PIN**.
5. Click **Save**. The new PIN settings will take effect at next power on.

## To change the SIM PIN

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

1. Under **Advanced**, select **EXPLORER Cellular Modem**.
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 **Save**. The new PIN settings will take effect at next power on.

## To set up the cellular network settings

1. Under **Advanced**, select **EXPLORER Cellular Modem**.
2. Select **Advanced modem settings**.



3. Select the Network operator mode.
   - **SIM default**: The cellular modem uses the operator from the SIM card.
   - **Locked to operator:** Type in the **MCC** and **MNC** for the operator you want to use. The cellular modem will only use this operator.
4. If you want to manually enter a CID for the connection, select **Manual CID**.

   | **Important** | Do not change the CID unless you are absolutely sure what you are doing! |
   
5. If you selected Manual CID, type in the **Connection ID (CID)** for the cellular connection.

   | **Note** | If you need to change the CID, talk to your airtime provider. The EXPLORER 540 terminal must restart for the setting to take effect. |

6. **At Network type**, select the preferred cellular network type (**2G (GSM)**, **LTE-M**, **NB-IoT**, **3G (UMTS)**, **4G (LTE)**), or select **Automatic** to let the terminal find the network suitable for your installation. Note that the selected network must be supported by the embedded 3rd party modem and the service provider.
   For details, see *Optional EXPLORER 540 Cellular Modem* on page A-9.

7. If the installed modem is a **TC1NAG** or **TC4NAG**, select which operator you are using (**AT&T** or **Verizon**).
   For other types of modem, the operator is fixed and cannot be changed.

   | **Important** | If you change the operator setting you must restart the EXPLORER 540 terminal for the setting to take effect. |

8. Click **Save**.

## 4.15.3  To set up an external cellular modem

If you are using an external cellular modem, set up the EXPLORER 540 as follows:

1. Set up the external modem according to the modem documentation.
2. In the EXPLORER 540 web interface, select ✥ (Control panel) > **Terminal settings** and locate **Connection**.
3. Select connection mode **External modem preferred** or **External modem preferred (PRISM)**.

   | Important | If you are using an external modem **without** PRISM, set up the Connection watchdog to monitor the connection. Otherwise the terminal will **not be able to detect if the cellular connection is lost**, and consequently will not switch over to BGAN backup. See *Connection watchdog (Link monitoring)* on page 4-34. |
   |---|---|

4. Select ✥ (Control panel) > **Advanced** > **External cellular modem**.
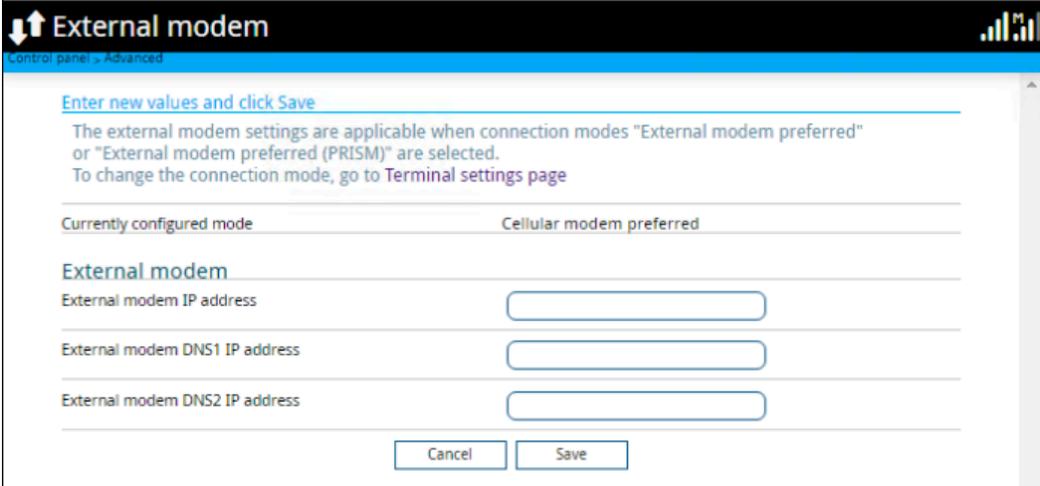


5. Type in the **External modem IP address**.
6. Type in the IP addresses of the primary and secondary DNS.
   - **External modem DNS1 IP address**: IP address of the primary DNS.
   - **External modem DNS2 IP address**: IP address of the secondary DNS.

   If you only have one DNS IP address, enter the same IP address for DNS1 and DNS2.
7. Click **Save**.

   | Note | If you already have an external modem running on a different IP address, you have to reboot the terminal to reset the IP routing. |
   |---|---|

8. Set up the WAN switching parameters, see the next section *PRISM/WAN switching* on page 4-54.
9. If the connection mode is **External modem preferred (PRISM)**, set up the PRISM parameters as described in *PRISM/WAN switching* on page 4-54.

# 4.16   PRISM/WAN switching

If you are using a cellular network with the EXPLORER 540, you must set up the switching between the two types of network (WAN switching).

Furthermore, if you are using PRISM to control and monitor the connection, you must set up the PRISM settings in the EXPLORER 540.

Access the PRISM/WAN switching settings at **Control Panel** > **PRISM/WAN switching**.

## 4.16.1   To set up PRISM

If you are going to use PRISM you must first install the PRISM server software from Cobham SATCOM, set up the server and then set up the EXPLORER 540.

- For general information on PRISM, see *EXPLORER 540 operation in Cellular modem preferred (PRISM) mode and External modem preferred (PRISM) mode* on page 4-60.
- For details on setup with cellular modem, see *To set up the EXPLORER 540 for cellular operation* on page 4-48 and *To set up an external cellular modem* on page 4-53.

To configure the EXPLORER 540 for PRISM, do as follows:

1. Configure the cellular modem settings as described in the previous pages. Remember to set the connection mode to a PRISM mode in the Terminal settings page.

2. Select �֍ (Control panel) and then **PRISM/WAN switching**.
   You can see the **Currently configured mode** at the top of the page.
   The **Terminal ID** is used to identify the EXPLORER 540 on the PRISM server.

3. In the **PRISM server settings** section, type the following for the primary and (optionally) the secondary server[1]:
   - **Shared authentication key**. This key must be identical to the key entered in the PRISM server. Note that the (optional) secondary server must have a different key than the primary server.
   - **IP address of the PRISM server**.
   - **Server port number** (default 6666).

4. **Client negotiation duration (seconds)**:  This parameter is the amount of time allowed for the terminal to establish a connection to the PRISM server.

   > **Note**  Leave this setting as is. Only change if you really need to, and you know what you are doing.

5. In the **PRISM terminal settings** section, type a **Connection test IP address** (optional). This is an optional test server address used to check the data connection if the PRISM server is not responding.

   > **Important**  This address must be different from the PRISM server address(es) and be able to respond to ping commands, e.g. the Google DNS server 8.8.8.8.

   The test IP address is used in the following way:
   If **BGAN link mode** is set to **Always connected**:
   - If the **PRISM server connection fails** on both the cellular and BGAN link (or if the BGAN link cannot be connected), a maximum of 5 pings are sent to the test IP address on the physical links.
   - If **no ping responses** are received on the test IP address neither on the cellular nor the BGAN link, the terminal will reboot immediately.

   > **Important**  Make sure you have a valid test IP address - if not, the terminal will keep rebooting every time the test ping fails after a failed PRISM server connection!

   - If **a ping response is received** the network(s) are probably OK but the PRISM server may be down. In this case the terminal will switch to the secondary PRISM server, if a secondary server is configured. If there is no secondary server, the terminal will

---

1. Specifying a secondary PRISM server is optional. The secondary server will be used if a connect sequence to the primary PRISM server fails (after both primary/cellular link and secondary/BGAN link have been connected or link connect has failed). If a test ping IP server has been specified, a switch to the secondary server also requires a successful ping response from the test server.

continue to try to connect to the primary PRISM server. If PRISM continues to fail, the terminal will reboot after a reboot delay, defined in the next step 6.

If **BGAN link mode** is set to **Connected when needed**:

- If the **PRISM server connect fails** on the cellular connection, a maximum of 5 pings are sent to the test IP address on both the cellular link and the BGAN link.

- If **no ping responses** are received from the test IP address on any of the physical links, the terminal will reboot immediately.

- If **a ping response is received** on the test IP address, the terminal will switch to the secondary PRISM server, if a secondary server is configured. If the connection to the secondary PRISM server also fails, the terminal will try to connect to the secondary PRISM server through the backup BGAN connection. If the connection continues to fail, the terminal will reboot after a reboot delay, defined in the next step 6.

6. Type in a **Reboot delay**.
   This delay is used if test ping was successful and both links have been connected (or cellular has been connected but BGAN connect has failed) but no connection to the PRISM server(s) has been possible. A typical value is 24*3600=86400 seconds (1 day).

7. Set the **Connect delay**.
   If you want to limit airtime cost during PRISM server downtime, you can specify a delay from a failed connect attempt until further connect attempts are made. A typical value is 1800 seconds (30 minutes).

   > **Important** Specify a Connect delay that is shorter than the Reboot delay. Otherwise, the terminal will reboot before making further connect attempts.

   > **Note** In some cases (when the cellular modem has been unable to establish a connection), modem reboot will be delayed to avoid making excessive connect attempts on the cellular connection – some carriers do not allow excessive connect attempts.

8. For both **BGAN** and **cellular** network, type in the ping settings.
   - **Ping interval (seconds)**: Type the interval between ping commands sent to the remote PRISM server. The ping commands are only sent if no data is received since last ping.[1]
   - **Ping interval after first failure (seconds)**: This ping interval is used to determine whether the failure was a single packet loss or if the link is down. Low values (1) on cellular secure fast failover but may increase BGAN usage. Higher values ensure that failover only happens for longer outages.
   - **Max. number of failed pings**: Type the number of failed ping commands before the link is considered to be down.

   > **Note** The ping interval for PRISM overrules any ping interval entered for the Connection watchdog. The Terminal watchdog, however, will continue to use the entered Watchdog interval independently of the interval entered for PRISM.

9. Click **Save**.

---

1. If your airtime connection uses a private IP address and your ping interval is set to more than 27 seconds, you may experience timeouts in the network, which will break the PRISM IP tunnel. To avoid this, contact your service provider to get a public IP address for the BGAN connection, which will allow the BGAN ping interval to be longer. If this is not possible, you must set the ping interval to less than 27 seconds.

## 4.16.2   To set up WAN switching

If you are using a cellular network with the EXPLORER 540, set up the parameters for switching between the cellular and BGAN network. Do as follows;

1. In the PRISM/WAN switching page, locate the section **WAN switching** at the bottom of the page.

2. Select the **BGAN link mode**.
   - **Always connected**: The BGAN data connection will always be running in the background while the cellular connection is used.
   - **Connected when needed**.: The BGAN data connection will only be established when the cellular connection fails.

3. If you selected **Connected when needed**, set the Connect wait time and the Disconnect wait time.
   - **Connect wait time (seconds)**: The time between a failed cellular connection and startup of the backup BGAN connection. **0** means the BGAN connection will be started immediately after cellular failure.
   - **Disconnect wait time (seconds)**: The time from when the cellular connection is up again until the backup BGAN connection is closed.

4. If you are **not** using PRISM, set up the following:
   - **Link switch during data traffic**:
     - Select **Yes** (recommended) if you want to switch back to cellular as soon as the cellular connection is ready again. This may result in disruption of the data traffic, but will limit the use of BGAN airtime.
     - Select **No** if you want a current BGAN backup connection to complete any ongoing data traffic before switching back to the cellular connection[1]. This will limit a possible disruption of data traffic, but will also increase cost, because BGAN airtime is normally more expensive than cellular airtime.
   - **Probe ping interval (seconds)**: If the Connection watchdog reports link failure on the primary/cellular link and the backup BGAN link is then used, a probe ping will start to detect whether the cellular link is OK again. A low value (3) ensures fast recovery but a larger value (20) ensures stability over a longer period of time.
   - **Number of OK ping replies**: This is the number of OK probe ping responses needed before the cellular link is declared OK again after the Connection watchdog has reported a link failure.

5. Click **Save**.

---

1. Note that regardless of this setting and the data traffic, the terminal will switch back to the cellular connection no later than 30 minutes after the cellular link is up again.

## 4.16.3 EXPLORER 540 operation in Cellular modem preferred or External modem preferred mode

### Normal operation

When **Cellular modem preferred** or **External modem preferred** is selected under **Terminal settings**, the EXPLORER 540 will persistently attempt to establish a data connection for the cellular modem and, if BGAN link mode is set to Always connected, also on the BGAN air interface.

If data connections are successfully established, the cellular data connection will be used as the primary connection (indicated on the Web interface under **Terminal status**, **Network in use**). The BGAN data connection will be ready as backup if BGAN link mode is set to Always connected. If BGAN link mode is set to Connected when needed, the data connection will be established if the cellular connection fails.

| Important | In External modem preferred mode, you must enable the Connection watchdog for the EXPLORER 540 to be able to detect a failed cellular connection! |
|---|---|

The EXPLORER 540 will now route all data traffic via the cellular connection. It will monitor the status of the cellular connection and the backup BGAN connection. If the Connection watchdog is enabled (mandatory if an external cellular modem is used), this function will also be used to monitor and verify connectivity of the Cellular connection.

### Limitations in Cellular modem preferred mode and External modem preferred mode

- Streaming is not allowed as a BGAN backup connection.
- Remote Activate/Deactivate of BGAN connections is not supported.
- AT command control of the Cellular connection is not supported.
- PPPoE control of the Cellular connection is not supported.
- Use of Data limits is not supported for the Cellular connection.

| Note | If the Cellular connection is to be used for remote access to the EXPLORER 540 (or attached equipment) the Cellular USIM should have a "Static/Global IP address" that can be accessed from the WAN side. If not, once the EXPLORER 540 is connected to the cellular network, you can get the global IP address with the SMS command GETINFO, see *GETINFO: Get information from the EXPLORER 540* on page 3-6. |
|---|---|
| | Alternatively, you may set up a PRISM server and use PRISM technology. See *EXPLORER 540 operation in Cellular modem preferred (PRISM) mode and External modem preferred (PRISM) mode* on page 4-60. |

## If the cellular connection fails in Cellular modem preferred mode or External modem preferred mode

**Important** ▶ | In **External modem preferred** mode, if you are **not** using the Connection watchdog nor PRISM, the terminal will **not be able to detect if the cellular connection fails**, and consequently will not switch over to BGAN backup.

**Note** ▶ | After terminal start-up or initial activation of Cellular modem preferred mode, the EXPLORER 540 will allow the Cellular connection a period of 3 min. to become operational before it is considered failing and the EXPLORER 540 switches to the BGAN connection.

If the EXPLORER 540 detects that the cellular connection is failing, it will switch the traffic to the BGAN connection, which now becomes the **Network in use**.

After a switch to the BGAN backup connection the EXPLORER 540 will try to recover the Cellular data connection. If the Cellular data connection is successfully re-established, the EXPLORER 540 will start to monitor and validate the Cellular connection. The EXPLORER 540 will now prepare a switch back to the Cellular connection but will monitor the traffic volume in order to avoid switching while traffic volume is high. The EXPLORER 540 will monitor the traffic volume at regular intervals in order to switch back to the Cellular connection. If the traffic volume remains high the EXPLORER 540 will eventually switch back to the Cellular connection after 30 min.

If recovery of the Cellular data connection continues to fail, the EXPLORER 540 will continue to use the BGAN connection as Network in use (while still trying to reestablish the cellular connection) until the EXPLORER 540 is restarted or the BGAN connection fails.

If the BGAN connection fails while it is Network in use or if the backup BGAN connection is down or fails when the EXPLORER 540 attempts to switch to the backup BGAN connection, the EXPLORER 540 will reboot in order to attempt to recover both the Cellular and BGAN connections.

If the BGAN connection fails while it is operating as standby connection, the EXPLORER 540 will try to re-establish the BGAN connection without rebooting the terminal.

## 4.16.4 EXPLORER 540 operation in Cellular modem preferred (PRISM) mode and External modem preferred (PRISM) mode

When the cellular modem is installed, the terminal offers simultaneous cellular and BGAN IP-network connectivity, where each link receives an IP-address from the corresponding Network Operator.

With the PRISM option, you can route all traffic to and from the EXPLORER 540 through a multi-path tunnel between the terminal and a server, using cellular or BGAN connectivity. Devices connected to the EXPLORER 540 will be immediately reachable from server applications, regardless of the network technology (cellular or BGAN), using the same IP address. Depending on server routing, devices attached to the EXPLORER 540 will likewise have direct access to services on the server and beyond.
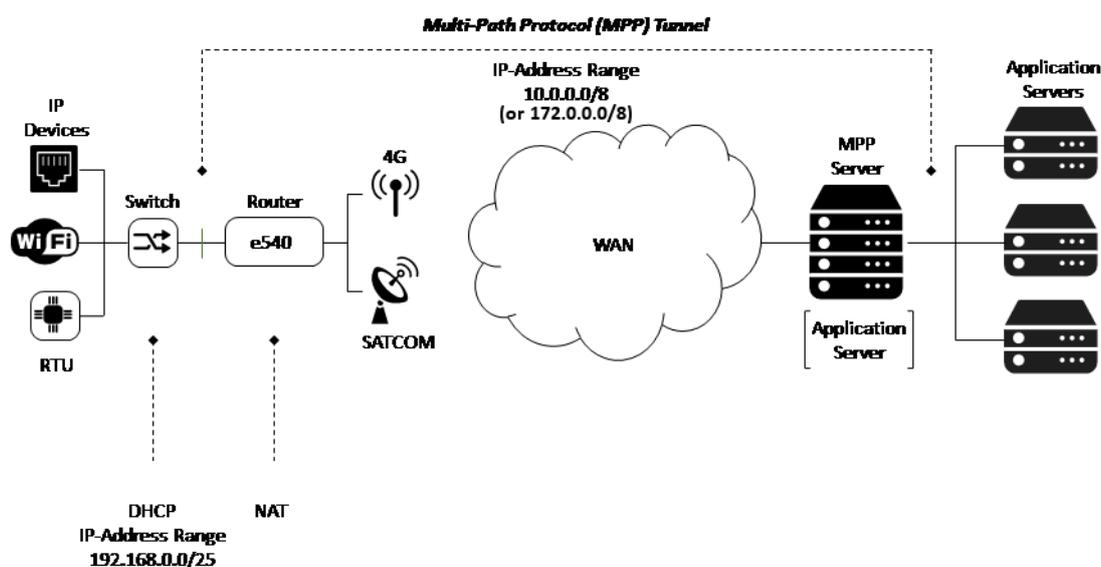


To set up PRISM you must install the PRISM server software from Cobham SATCOM, configure the PRISM server and set up your EXPLORER 540 to communicate with this server.

For details how to set up the EXPLORER 540 for PRISM, see *To set up the connection mode* on page 4-16 and *To set up PRISM* on page 4-55.

### Limitations in the PRISM connection modes

If your airtime network connection uses a private IP address and your ping interval is set to more than 27 seconds, you may experience timeouts in the network, which will break the PRISM IP tunnel.

To avoid this, contact your service provider to get a public IP address for the BGAN connection, which will allow the BGAN ping interval to be longer. If this is not possible, you must set the ping interval to less than 27 seconds.

### If the cellular connection fails in Cellular modem preferred (PRISM) mode or External modem preferred (PRISM) mode

In the PRISM modes, link selection is handled by the PRISM client in the EXPLORER 540 - it will always use the primary link (cellular) if it is available. If the primary link goes down or if ping fails, it will switch to the secondary link (BGAN). As link switch-over does not interrupt the data stream, it will switch back to the primary link as soon as it is available again (Link failure or link monitoring failure will require a new authentication phase).

If you have configured a test IP address, it will be used to check the physical connections when the PRISM server ping fails. This is done to establish whether it is the PRISM server or the physical connection that fails. For details, see *To set up PRISM* on page 4-55.

# Maintenance and troubleshooting

## 5.1 Support

### 5.1.1 Contact information

Should your Cobham Satcom product fail, contact your dealer or installer, or the nearest Cobham Satcom partner. You will find the partner details on www.cobhamsatcom.com/where-to-buy. You can also access the partner portal at partnerportal.cobhamsatcom.com, which may help you solve the problem. Your dealer, installer or Cobham Satcom partner will assist you whether the need is user training, technical support, arranging on-site repair or sending the product for repair. Your dealer, installer or Cobham Satcom partner will also take care of any warranty issue.

### 5.1.2 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 EXPLORER 540 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.

## 5.2    Software update

### 5.2.1    Remote software update

See *Remote software upgrade* on page 3-24.

### 5.2.2    To update software locally with the web interface

To update the software in the EXPLORER 540, do as follows:

1. Download the new software[1] or acquire the software from Cobham SATCOM and save it to your computer.
2. Connect your computer to the EXPLORER 540.

   > **Note**  Connect to the LAN interface of the EXPLORER 540. Depending on your system configuration, you may have to connect through a router or a switch.

3. Open the web interface in your browser.
   For details on how to access the web interface, see *To access and navigate the web interface* on page 4-2.
4. Click � (Control panel) at the bottom of the page.
5. Click **Support > Update software**.
6. Click **Update software...**
7. Browse to the new software version and click **Open**. The file has the extension ".tiif".
8. The EXPLORER 540 now restarts and completes the software update.

   > **Note**  The update procedure takes a couple of minutes.

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

---

1. You can download the software from the Partner Portal at www.cobham-satcom.com, select **Partner Portal** and search for EXPLORER 540 software.

## 5.2.3 Recovery software update

If the EXPLORER 540 becomes inoperative, a recovery software update may bring it back into an operational state.

**Important** | The recovery software update will reset your EXPLORER 540 configuration to factory default!

**Note** | You will need:

1. A USB memory stick.
2. A converter cable between the Micro USB connector in the EXPLORER 540 and your USB memory stick (Micro USB to Standard USB).

### To prepare the USB memory stick

Do as follows:

1. Download the EXPLORER 540 software to your computer.
2. Insert the USB memory stick into your computer and copy the EXPLORER 540 software image file to the USB drive.
3. Rename the file name to "tt3715a.tiif".
4. Remove the USB memory stick from the computer.

### To make a recovery software update

Do as follows:

1. Prepare the USB stick as described in the previous section.
2. Insert the Micro USB end of the converter cable into the EXPLORER 540 Micro USB connector in the cable compartment on the back of the EXPLORER 540.
3. Push and hold the **Reset** button while powering on the EXPLORER 540. Hold until the LED is flashing rapidly blue.
4. Insert the USB memory stick with the new software into the standard USB end of the converter cable.
   The EXPLORER 540 reads the software image from the USB memory stick and starts the software update process (LED flashing slowly blue).
5. Wait for the status LED to become green to indicate the software update process is completed.
6. Remove the USB memory stick.
7. Switch the EXPLORER 540 off and on again.

# 5.3 Reset button

The EXPLORER 540 has a Reset button that has three functions: To restore all settings to factory settings, to restart the EXPLORER 540, or to put the EXPLORER 540 into safe mode for recovery software upload.

| Note | You can disable or limit the function of the Reset button using the web interface. See *Reset button* on page 4-45. **NOTE** that you can still use the Reset button for safe mode, even if it is disabled. |

The Reset button is located inside the interface enclosure at the back of the terminal and can only be accessed when the cover is removed.
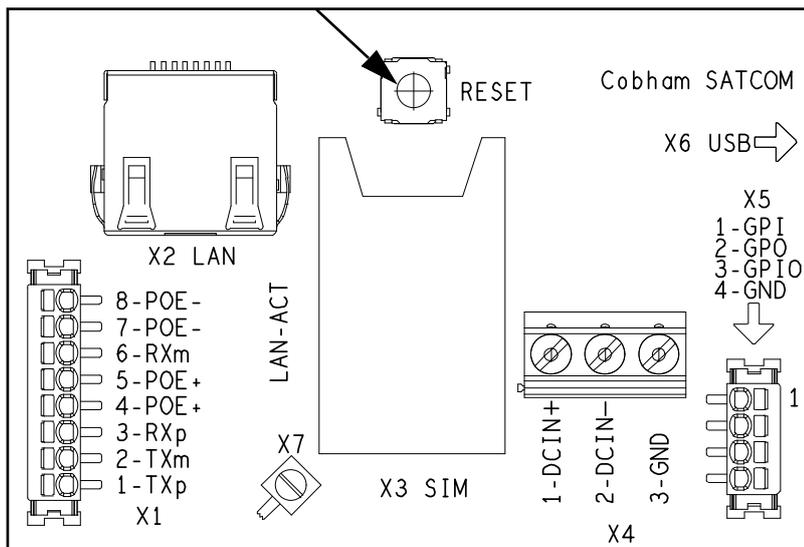


Do as follows:

1. Use the included Torx bit to unscrew the screws holding the cover for the interface enclosure.
2. Locate the Reset button.
3. Use a pointed device to push the Reset button.

| Action | Function |
|---|---|
| Push and hold the Reset button for 2 seconds | The EXPLORER 540 restarts (power cycle) and begins the installation process again. |
| Push and hold the Reset button for > 10 seconds | The EXPLORER 540 restores factory settings and restarts the system. All changes to the configuration are lost and the administrator password is reset to **admin**. |
| Push and hold the Reset button during power-up of the EXPLORER 540 | The EXPLORER 540 enters safe mode. The LED is flashing rapidly blue.<br><br>In safe mode the EXPLORER 540is ready for recovery software upload (see *Recovery software update* on page 5-3). |

4. Close the cover and tighten the screws carefully to torque **0.5 Nm/ 4.5 lbf in**. This is important in order to maintain the IP grade of the EXPLORER 540.

## 5.4    Maintenance

### 5.4.1    Cleaning the EXPLORER 540

Clean the exterior of the EXPLORER 540 with a damp cloth.

### 5.4.2    Disposal of the EXPLORER 540

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 distributor of old electrical and electronic equipment marked with this symbol.

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

## 5.5    Troubleshooting

### 5.5.1    Troubleshooting guide

| Problem | Possible cause | Remedy |
|---|---|---|
| Installation process: The pointing process fails. | The view to the satellite is blocked. | Make sure the EXPLORER 540 has a clear view to the satellite. Reboot the terminal to run installation again. |
|  | The antenna is pointed in the wrong direction. | Check that the antenna is pointed according to the position data. Adjust the position to the highest possible signal strength. |
| Installation process: "Start satellite connection" fails. | Missing SIM. SIM error. Missing PIN. | Insert SIM. Replace SIM card. Enter or cancel PIN, see *To enter the SIM PIN in the web interface* on page 4-47. |
|  | Poor satellite signal. | Check that the antenna is pointed according to the position data, and that nothing is blocking the line of sight. Adjust the position to the highest possible signal strength. |

| Problem | Possible cause | Remedy |
|---------|----------------|--------|
| Installation process: "Verify satellite connection" fails. | Wrong APN. | Enter correct APN or select **SIM default** (if allowed by SIM card). See *To change the APN for a connection package* on page 4-6. |
| | APN is set to SIM default, but the SIM requires a user defined APN | Enter the user defined APN in the web interface. See link above. |
| | Wrong watchdog IP addresses. | Enter correct watchdog IP addresses, or disable watchdog to skip ping verification. See *Connection watchdog (Link monitoring)* on page 4-34. |
| | Network issues. | Try again later. To skip ping verification, disable watchdog. |
| The EXPLORER 540 is not operational. | Software error. | Restart the terminal. If the problem persists, you can restore to factory defaults as described in *Reset button* on page 5-4. Note: This will reset the configuration of your terminal to factory default! |
| The web interface shows **Insert SIM**. | The SIM card is not present. | Remove power and Insert the SIM card in the SIM slot according to the instructions in the installation guide. |
| | The SIM card is not inserted properly. | Remove power and then remove the SIM card and re-insert it according to the instructions in the installation guide. |
| The web interface shows **No position fix**. | The EXPLORER 540 is unable to register on the network, because the GNSS position is unknown. | Make sure the view to the GNSS satellites is not blocked. To obtain position fix, the EXPLORER 540 should be placed flat on an even surface pointing straight upwards, with a clear view to as much of the sky as possible. When the EXPLORER 540 has obtained position fix, you can point the antenna towards the BGAN satellite. You can see position status in the Dashboard of the web interface (status section). |
| The web interface shows **Not registered**. | The EXPLORER 540 cannot register on the BGAN network. | Check that your SIM card is valid for communication on the BGAN network. Check your subscription with the Airtime Provider. |

| Problem | Possible cause | Remedy |
|---------|----------------|--------|
| The web interface shows **External control**. | The EXPLORER 540 is currently controlled by an external application, e.g. LaunchPad or an AT command interface. | If you want to use the built-in web interface, stop the external application and restart the EXPLORER 540. Then open your browser and access the web interface. |
| The EXPLORER 540 cannot obtain its position using GNSS. | There is no GNSS signal, or the signal is weak.<br><br>If the EXPLORER 540 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.<br><br>To help the EXPLORER 540 obtain position fix, it should be placed flat on an even surface pointing straight upwards, with a clear view to as much of the sky as possible.<br><br>When the EXPLORER 540 has obtained position fix, you can point the antenna towards the BGAN satellite. |
| No signal or weak signal from the BGAN satellite. | The view to the satellite is blocked. | Make sure the EXPLORER 540 has a clear view to the satellite. Be aware that window glass may reduce the signal level. |
| | The antenna is pointed in the wrong direction. | Check that the antenna is pointed according to the position data.<br><br>Adjust the position to the highest possible signal strength. |
| Connection to the Internet cannot be established. | The signal strength is too low. | Check that the antenna is pointed according to the position data.<br><br>Adjust the position to the highest signal strength you can obtain.<br><br>As a rule of thumb, you should have a 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 Microsoft Internet Explorer, select **Tools > Internet Options > Connections > LAN Settings** and uncheck **Use a proxy server for your LAN**. |
| | You have entered a wrong IP address. | Check the IP address and re-enter it. The default IP address is **192.168.0.1**. |
| A LAN connection cannot be established. | The cable is not properly connected. | Connect the cable. |
| | The cable type is not correct. | Use Ethernet Min. Cat 5 Solid copper wire, STP. Max. length: 100 m/ 328 ft |

## 5.5.2    Status signaling

### Means of signaling

The EXPLORER 540 system provides two methods for signaling the status of the system.

- **LED** between the cable glands.
- **Messages** shown in the web interface.

### LED

The EXPLORER 540 has one LED showing status before and during installation. The Status LED is located between the two cable glands.
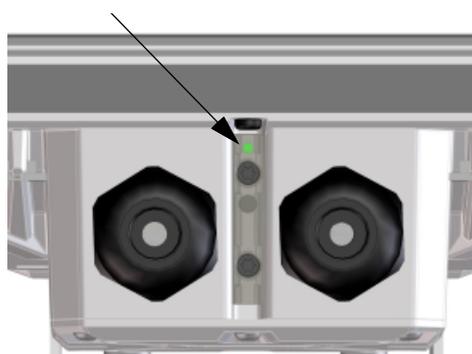


| Note | The LED is only in use until installation is completed, and is **automatically disabled** 10 minutes after the connection is established. After this, the LED is only active during reboot of the EXPLORER 540 or if you restart the installation process. |

### LED light pattern **before and during** installation

| Light pattern | | Meaning |
|---|---|---|
| 🟢 | Green flashing rapidly | Starting up. |
| 🟡 | Yellow flashing | BGAN pointing. |
| 🟢 | Green flashing | Verify network connectivity. |
| 🟢 | Green constant | Ready. |
| 🟡 | Yellow flashing rapidly | Closing down. |
| 🟡 | Yellow constant | Warning (user recoverable). See web interface for the warning text. |
| 🔴 | Red constant | Error. See the web interface. |
| 🔵 | Blue flashing | Uploading software to the terminal, or Safe mode (see *Reset button* on page 5-4). |
| ⚪ | Off | Power off. |

## LED light pattern **after** installation

| Light pattern | | Meaning |
|---|---|---|
| 🟢 | Green flashing rapidly | Starting up. |
| 🟡 | Yellow flashing rapidly | Closing down. |
| ⚪ | Off | Power off **or** normal function after installation is completed. |

## Event messages and status messages

In the web interface of the EXPLORER 540 you can see status messages and alerts that are currently active.

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

## 5.5.3    List of messages

The following list explains some of the messages that may show in the web interface of the EXPLORER 540.

| Event ID (Hex) | Displayed text | Explanation | Remedy |
|---|---|---|---|
| 1010 | `Temperature too low (critical)` | 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. |
| 1020 | `Too low temperature warning` | 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. |
| 1110 | `Temperature too high (critical)` | **Terminal**: Critically high temperature is causing the terminal to shut down.<br>**Antenna**: Critically high temperature is causing the antenna to stop transmission. | If possible, move the failing unit to a cooler location. For information on ambient temperature, see the Specifications appendix.<br>Contact your distributor if the problem persists. |
| 1120 | `Too high temperature warning` | High ambient temperature is causing the performance of the system to be degraded or halted. The bit rate is reduced. | Move the terminal to a cooler location. For information on ambient temperature limits, see the Specifications appendix. |
| 1400 | `Satellite signal lost` | The system no longer receives a signal from the satellite. | Make sure the antenna has a clear view to the satellite. |

| Event ID (Hex) | Displayed text | Explanation | Remedy |
|---|---|---|---|
| 1600 | `SIM blocked` | The SIM card is not accepted by the network, e.g. because you have entered too many wrong PINs and PUKs. Only emergency calls are allowed. | Enter the PIN and wait for network approval. If the problem persists, contact your airtime Provider. |
| 1700 | `Registration for voice failed` | The system has not yet been allowed to register for voice services (Circuit Switched). | If the problem persists, contact your airtime provider. |
| 1800 | `Registration for data failed` | The system has not yet been allowed to register for data services (Packet Switched). | If the problem persists, contact your airtime provider. |
| 2900 | `Network failed authentication` | The system does not accept the network as a valid BGAN network. | Restart the system. If the problem persists, contact your distributor. |
| 3900 | `Air link error` | Error condition in DSP which modulates and demodulates BGAN signal. | Reboot the terminal. Contact your distributor if the problem persists. |
| 8049 | `Data rate reduction due to high temperature` | The bit rate of the data channel is reduced because the temperature is too high. | Move the terminal to a cooler location. |
| 8056 | `SIM rejected` | The type of USIM card inserted in the terminal is not correct for your terminal. | Make sure you have the correct type of USIM card. For example, an USIM card for a land mobile system will not work for a maritime system and vice versa. |
| 80A6 | `SIM heater - temperature too low - SIM disabled` | The SIM is disabled because the temperature is too low and the heater has not been able to bring the temperature up. | Wait for the SIM heater to bring the temperature back up. |
| 80AA | `A low LTE blocker level is detected - this might affect terminal performance` | A cellular network signal has been detected. It may impact the performance of the terminal | If possible, move the terminal to another location with lower LTE blocker level. |
| 80AB | `A high LTE blocker level is detected - this will affect terminal performance` | High cellular network interference detected, high risk of impairing terminal performance | If possible, move the terminal to another location with lower LTE blocker level. |

| Event ID (Hex) | Displayed text | Explanation | Remedy |
|---|---|---|---|
| 80AD | `The terminal has re-registered due to a high LTE blocker level` | The terminal has re-registered to the network in attempt to regain functionality after an interfering cellular network signal. | The event is cleared after 5 minutes, but the terminal has limited the frequencies used. To restore original behavior, reboot the terminal. |
| 9220 | `Antenna temperature above critical limit` | Antenna temperature too high, might affect performance. | If possible, move the antenna to a cooler location. |
| 10117 | `PIN for cellular modem required` | The SIM card for your cellular connection requires a PIN code | You can enter the SIM PIN for the cellular modem from the web interface. |
| 10118 | `PUK for cellular modem required` | The SIM card for your cellular connection requires a PUK code, because too many wrong PINs were entered. | Enter the PUK for the cellular SIM card in the web interface. |
| 1011B | `Cellular modem SIM card error` | There is an error with the SIM card in the cellular modem | Check that you have inserted the correct SIM card, and that it is inserted properly. |
| 1011C | `Cellular modem error` | There is an error with the cellular modem. The text in the web interface will normally show more details on the type of error, e.g. unknown APN. | Check that the APN for the cellular connection is set up correctly. You can set up the APN in the web interface: In the Dashboard click in the right side of the tile with the Cellular Modem. |
| 1011D | `Cellular modem not supported` | The connected cellular modem is not supported by the terminal. | Connect a cellular modem that is supported. |
| 10206 | `Closing terminal due to high temperature` | Terminal has reached a critically high temperature, and will reboot by itself. | Move the terminal to a cooler location. |
| 10300 | `Updating software...` | Software update has begun. | Wait for the software update to complete. |
| 10302 | `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 | `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. Use the command **_IUPDFW?** to show the correct file name before updating. |

| Event ID (Hex) | Displayed text | Explanation | Remedy |
|---|---|---|---|
| 10305 | `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 distributor. |
| 10306 | `File does not support this product` | The file used for software update does not support this product. | Use the correct tiif file |
| 10307 | `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 | `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 distributor. |
| 10309 | `Software update failed. Update to the latest software version.` | The software has been rolled back to the previous version prior to starting the software upload. The new image was not validated correctly. | Try running the update again, if the problem persists, contact your distributor. |
| 1030A | `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, alternatively from Safe Mode if the problem persists. |
| 1030C | `Software update is already started` | Another software update cycle is currently running. | Wait until the current software upload has finished. |
| 1030D | `Software version is already installed` | The software image you are trying to install is already active on the terminal. | Update with a different image as it is prohibited (and nonsensical) to start a sw update process with the same image. |
| 1030E | `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 distributor. |
| 10310 | `Online software update failed.` | Remote software update failed. | Try again later. If the problem persists, contact your distributor. |

| Event ID (Hex) | Displayed text | Explanation | Remedy |
|---|---|---|---|
| 10313 | `Online software update failed. Could not establish PDP context.` | Remote software update failed because the data connection could not be established. The reason may be:<br>• no network resources,<br>• wrong APN, or<br>• no line of sight to the satellite. | Check the status of the terminal, e.g. in the web interface. Make sure there is line of sight to the satellite and that the APN is correct. |
| 10314 | `Online software update failed. Could not connect to URL.` | Remote software update failed because the terminal could not connect to the URL. | Check that you have specified the correct URL in your AT command, or enter the correct IP address instead. |
| 10315 | `Online verification ongoing` | The terminal is verifying the data connection for the software update. | Wait for the verification to finish. Either the online software update starts or an error message is shown. |
| 10316 | `Software update transfer error` | An error occurred while trying to transfer the file for software update to the terminal. | Try again later. If the problem persists, contact your distributor. |
| 10317 | `Software update transfer timeout` | The system timed out before the software file was transferred to the terminal. | Try again later. |
| 10340 | `The terminal is not installed` | The terminal has failed in the installation process, or the installation process was canceled. | If you want to restart the installation process, restart the terminal or access the web interface and select Control panel > Installation. |
| 10701 | `PRISM server rejected authentication on cellular connection` | Shared authentication key mismatch between terminal and PRISM server on the cellular connection. | Make sure the same shared authentication key is used on terminal and PRISM server. |
| 10703 | `PRISM server rejected authentication on BGAN connection` | Shared authentication key mismatch between terminal and PRISM server on the BGAN connection. | Make sure the same shared authentication key is used on terminal and PRISM server. |

| Event ID (Hex) | Displayed text | Explanation | Remedy |
|---|---|---|---|
| 10704 | `EV_MPP_TEST_PING_ FAILURE` | Terminal test ping has failed after PRISM server connect failure. | Automatic reboot may correct the problem, otherwise contact your service provider. Also check that the test ping server is available and that the test IP address is correct in the web interface of the terminal. |
| 10706 | `EV_MPP_PAUSED` | PRISM connection has failed - paused before retrying connection. | Check the state of the PRISM server. It may be down or misconfigured. Check that the IP address of the PRISM server is correct. |
| 11001 | `Calibration error` | Invalid calibration values found. | Contact your distributor. |

## 5.6 Log files

With AT commands you can command the EXPLORER 540 to send a diagnostics report or the Event log, System log or AT command log to a specified FTP server. See *Log file(s)* on page 3-27.

### 5.6.1 To create a diagnostics report

The diagnostic report contains relevant information for troubleshooting. When contacting your distributor for support, please enclose this file. To generate the report, do as follows:

1. Access the web interface.
2. Select ✤ (Control panel) at the bottom of the page.
3. Select **Support**.
4. From the **Support** page, select **Diagnostics report**.
5. Select **Generate report**.

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

6. Select **Download report**.
7. Choose a location for the file and save it.

### 5.6.2 Call log and data log

The log holds detailed information on each call or data session to and from the EXPLORER 540, 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 4-14.

### 5.6.3 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.

## 5.7 To reset the administrator password

If you have forgotten the administrator password, do as follows:

1. Contact your supplier for a reset code.
   Report the serial number and IMEI number of the terminal.
   You can find the serial number on the label on the EXPLORER 540 or under ✤ (Control panel) > **Support > About** where you also find the IMEI number.
2. After receiving the reset code from your supplier, select **Reset password** from the **Support** page.
3. Type in the reset code obtained from your supplier and select **Reset**.
4. The password is reset to **admin**.

## 5.8    Help desk

Under Help desk you can enter the contact information you want for your EXPLORER 540. The Help desk contact information is empty by default. You must provide the contact information, e.g. the phone number for your Airtime Provider under **Advanced > Help desk**. For details on how to enter the information, see *Help desk* on page 4-44.

The Help desk information is then available from the About page ( (Control panel) > **Support > About**)

## 5.9    List of reserved IP subnets

Some IP subnets are reserved for internal use in the terminal. If any of these addresses are assigned to external equipment connected to the terminal, the terminal and connected equipment will not be able to communicate.

The following local IP subnets are reserved for internal use in the terminal:

**192.168.1.x** and

**192.168.2.x**

-where x can be any number from 0 to 255. The netmask for these subnets is 255.255.255.0.

Furthermore the following local IP addresses are reserved:

**192.168.61.1**

**192.168.61.2**

**192.168.61.3**

**192.168.61.4**

**192.168.61.5**

**192.168.61.6**

**192.168.61.7**

**192.168.61.8**

**192.168.61.9**

**192.168.61.10**

**192.168.61.11**

**192.168.50.1**

**192.168.51.1**

**192.168.52.1**

**192.168.53.1**

**192.168.54.1**

**192.168.55.1**

**192.168.56.1**

**192.168.57.1**

**192.168.58.1**

**192.168.59.1**

**192.168.60.1**

# Technical specifications

## A.1    General specifications

| Item | Specification |
|---|---|
| Type | EXPLORER 540, BGAN M2M terminal/ BGAN Class 2 terminal |
| Max. IP data rate, Rx/Tx[1]<br>Streaming data[2] | 464 kbps/448 kbps (simultaneously)<br>32, 64, and 128 kbps |
| Voice[b] | Standard voice 4 kbps<br>Premium voice 3.1 kHz audio, 64 kbps |
| Physical dimensions | 202 x 202 x 51.8 mm/ 8.0" x 8.0" x 2.0" |
| Weight | 1.6 kg / 3.5 lbs (excl. cellular modem) |
| Operating temperature | -40 to +55°C/ -40 to +131°F |
| Storage temperature | -40 to +75°C/ -40 to +167°F |
| Water & Dust | IP66 |
| Environment condition | Outdoor mounting and use in harsh environment |
| Max. altitude for Hazardous locations | 2000 m/ 6561 ft |
| Relative humidity | 95% humidity non-condensing at 40°C/ 104°F |
| Pollution degree | Pollution degree 2 |
| Supported web browsers (Others may be supported, these have been tested.) | Apple Safari<br>Microsoft Edge<br>Google Chrome<br>Mozilla Firefox |
| Approvals | CE, FCC, IC, RCM, GMPCS, C1D2, Russia (Type approval certificate in the field of communication), Japan (Radio law), Inmarsat Class 2 Type Approval and BGAN M2M Certified. |

1. Performance depends on a wide range of factors and actual usage.
2. Not available for M2M subscription.

# A.2    Interfaces specifications

## A.2.1    LAN interface (X1 or X2)

### Connector pin-out

> **Important** There are two LAN connectors, but **only one at a time can be used!**

**X1**: Terminal block and **X7** (GND)

**X2**: RJ-45 connector

8 - POE -
7 - POE -
6 - RXm
5 - POE +
4 - POE +
3 - RXp
2 - TXm
1 - TXp
X1

**or**

12345678
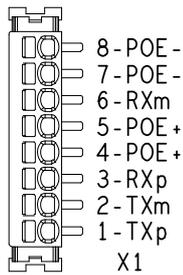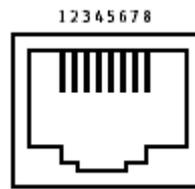
Female (receptacle)

**and**

X7

| Pin | Function[a] |
|-----|-------------|
| 1 | TXp (PoE+) |
| 2 | TXm (PoE+) |
| 3 | RXp (PoE-) |
| 4 | PoE+ |
| 5 | PoE+ |
| 6 | RXm (PoE-) |
| 7 | PoE- |
| 8 | PoE- |

a. The LAN interface accepts mode A (power and data together) and mode B (power and data separately).

> **Note** If you connect to the terminal block X1 you must connect the shield of the cable to the screw terminal X7 (GND).

To insert the wires in X1 use a screwdriver (max. 2mm/ 0.08" wide) to push each terminal open.

## Specifications

| Item | Specification |
|---|---|
| Number of connectors | 2: X1 **or** X2 - only one at a time available!<br>The two connectors are on the same electrical interface. |
| Connector types | RJ-45 female **or** spring loaded terminals |
| Standard | ISO/IEC 8877:1992 and PoE+ IEEE 802.3at type 2 class 4 (PD[1]) |
| Max. data rate | 10/100 Mbps |
| Max. cable length | 100 m / 328 ft with Cat5 UTP |
| Typical power consumption (when running BGAN only) (excluding PoE injector)[2] | Power save mode (wake on GPIO or timer): 2.4 W<br>Power save mode (wake on LAN): 2.3 W<br>Idle: 3.5 W<br>Transmitting: 21 W |

1. The EXPLORER 540 is a **Powered Device (PD)**, this means it may be powered by PoE from external Power Sourcing Equipment (PSE), but it **cannot supply PoE**.
2. If you are using the optional EXPLORER 540 Cellular Modem, do not use PoE to power the EXPLORER 540. Use the DC power input instead.

## A.2.2    DC power input (X4)

### Connector pin-out
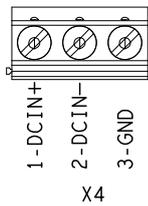
| Pin | Function |
|-----|----------|
| 1 | DCIN+ |
| 2 | DCIN- |
| 3 | GND |

Screw terminal

1 - DCIN+
2 - DCIN−
3 - GND
X4

> ⚠ **CAUTION!**    Do **not** connect the positive or negative wire to 3-GND!
> 3-GND is only for connection of the cable shield to ground.

To unscrew and fasten the screws in X4 use a screwdriver (max. 3.5 mm/ 0.14" wide). If the DC cable is shielded, connect the shield to 3-GND.

### Specifications

| Item | Specification |
|------|---------------|
| DC input range (min-max)<br>DC input, nominal | 10.5 to 32 VDC<br>12 or 24 VDC |
| Transient overvoltage | Overvoltage category II |
| Typical power consumption @12 VDC supply | Power save mode (wake on GPIO or timer): 0.1 W<br>Power save mode (wake on LAN): 0.9 W<br>Idle: 2.3 W (BGAN only mode)/ 2.9 W (Cellular preferred mode)<br>Transmitting: 19 W (BGAN only mode)/ 20 W (Cellular preferred mode), up to 23 W if using 2G cellular. |
| Connector type | Screw terminals |

## A.2.3    I/O connector (X5)

### Connector pin-out and specifications
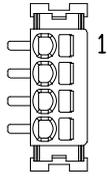
| Pin | Function | Specifications |
|---|---|---|
| 1-GPI | Power control input | Active high or low configurable in web interface. |
| | Voltage | Min 0 VDC, Max 32 VDC<br>Levels:<br>• Low: 0 - 0.8 VDC<br>• High: 2.8 - 32 VDC |
| 2-GPO | Terminal ready output | Active high or low configurable in web interface. |
| | Max current<br>Voltage | 400 mA, Open collector<br>0 to 32 VDC |
| 3-GPIO | General purpose input/output (GPIO) | Input or output configurable in web interface.<br>Active high or low configurable in web interface. |
| | **Input** voltage | Min 0 VDC, Max 32 VDC<br>Levels:<br>• Low: 0 - 0.8 VDC<br>• High: 2.8 - 32 VDC |
| | **Output** max current<br>**Output** Voltage | 400 mA, Open collector<br>0 to 32 VDC |
| 4-GND | GND | N/A |

To insert the wires in X5 use a screwdriver (max. 2mm/ 0.08" wide) to push each terminal open.
For configuration of the I/O pins, see *Power control* on page 4-41.

## A.2.4    USB (Host) interface (X6)

The USB interface is used for connecting the optional EXPLORER 540 Cellular Modem for cellular operation.

**Connector pin-out**

USB Micro
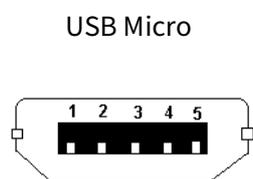
| Pin | Function |
|-----|----------|
| 1 | +5V |
| 2 | Dm |
| 3 | Dp |
| 4 | ID |
| 5 | GND |

**Specifications**

| Item | Specification |
|------|---------------|
| Version | USB v2.0 Host |
| Connector type | Type Micro B |

# A.3    Built-in BGAN antenna

| Item | Specification |
|------|---------------|
| Type | Directional patch array, manually adjustable |
| Polarization | RHCP, Right-hand circular polarization for both Tx and Rx |
| Frequencies<br><br>Inmarsat I-4<br>    Transmit<br>    Receive<br><br>Inmarsat Alphasat (EMEA)<br>    Transmit<br>    Receive<br><br>GNSS | <br><br><br>1626,5 MHz - 1660,5 MHz<br>1525 MHz - 1559 MHz<br><br>Extended L-band (XL)[1]:<br>1626,5 MHz - 1660,5 MHz and 1668 MHz - 1675 MHz<br>1518 MHz - 1559 MHz<br><br>GPS, GLONASS, BeiDou |
| EIRP | Nominal: 15.1 dBW ±1dB, Class 2 |
| Gain | 11.25 dBi |

1. Only available within Alphasat coverage (EMEA). See *BGAN services* on page 1-6.

# A.4    Outline drawing

2 x M20x1.5 threads for cable glands

202

65

202

Dimensions are in millimeter

50

M6, 4 places
Max. screw length 9 mm

50

Screw Torx 10 with security pin, 8 places

Compartment for SIM
card and connections

Pole size 1" to 1.5"
(33.7 to 48.3 mm)
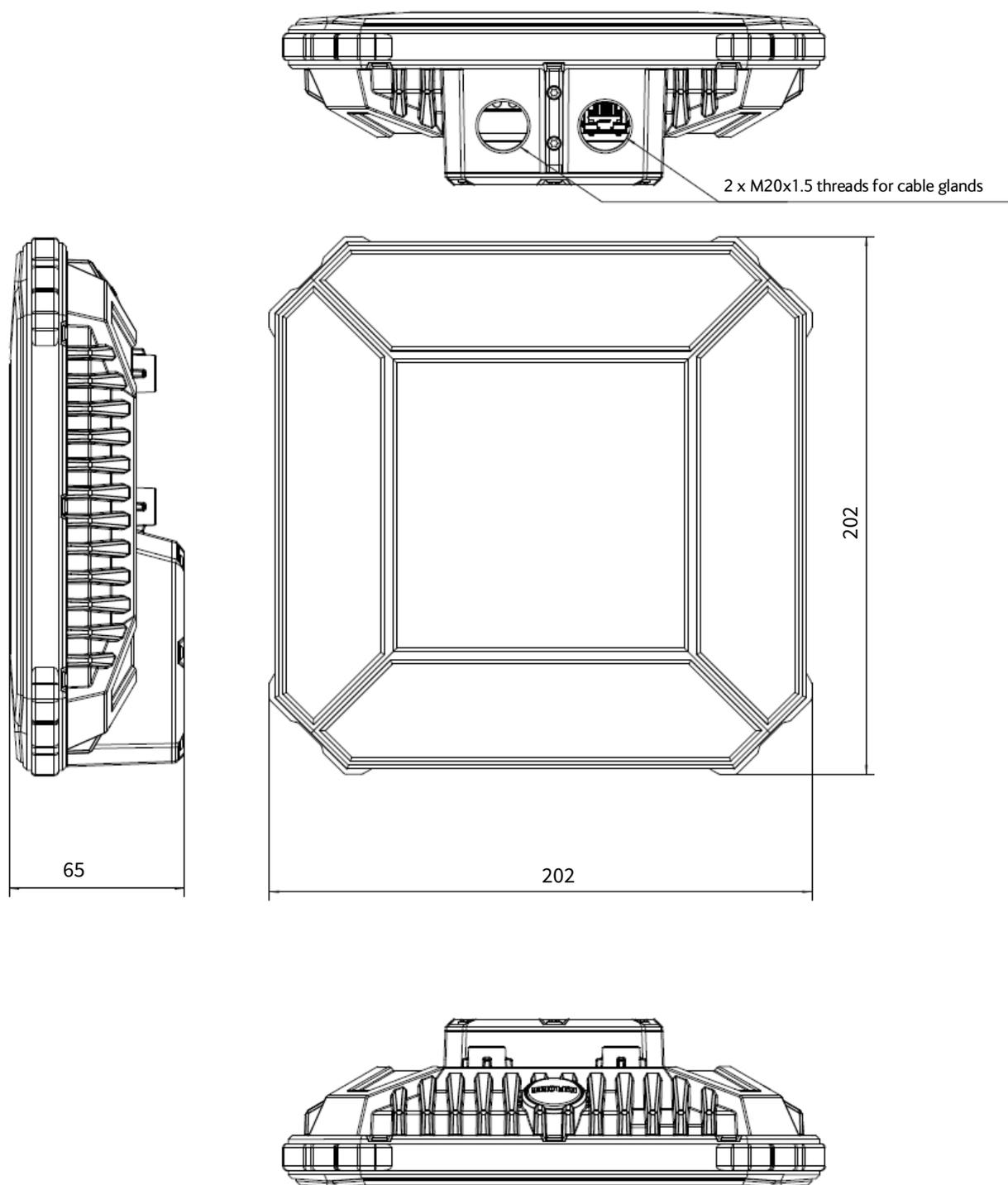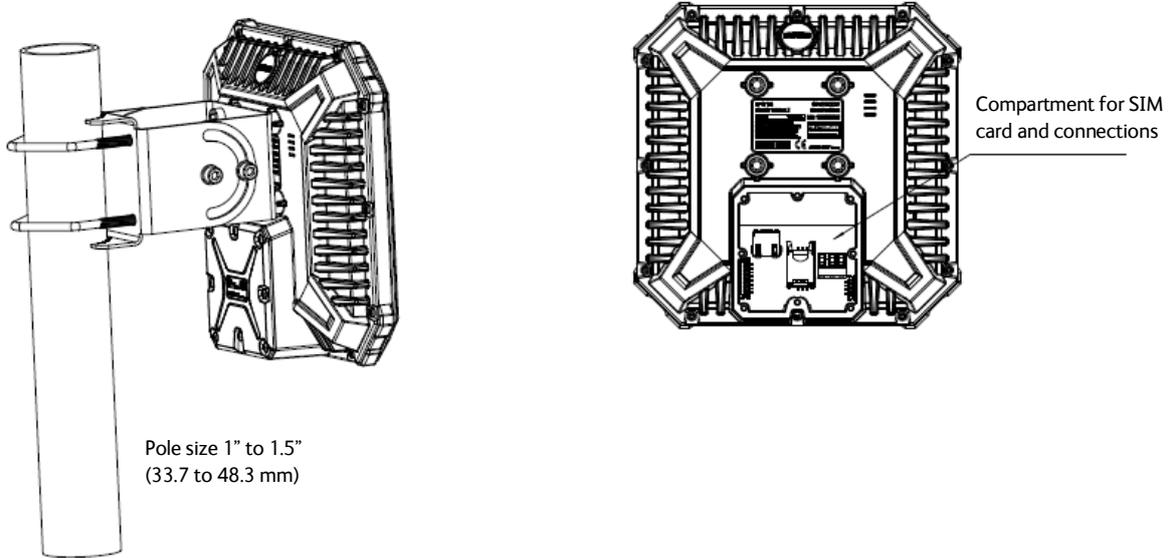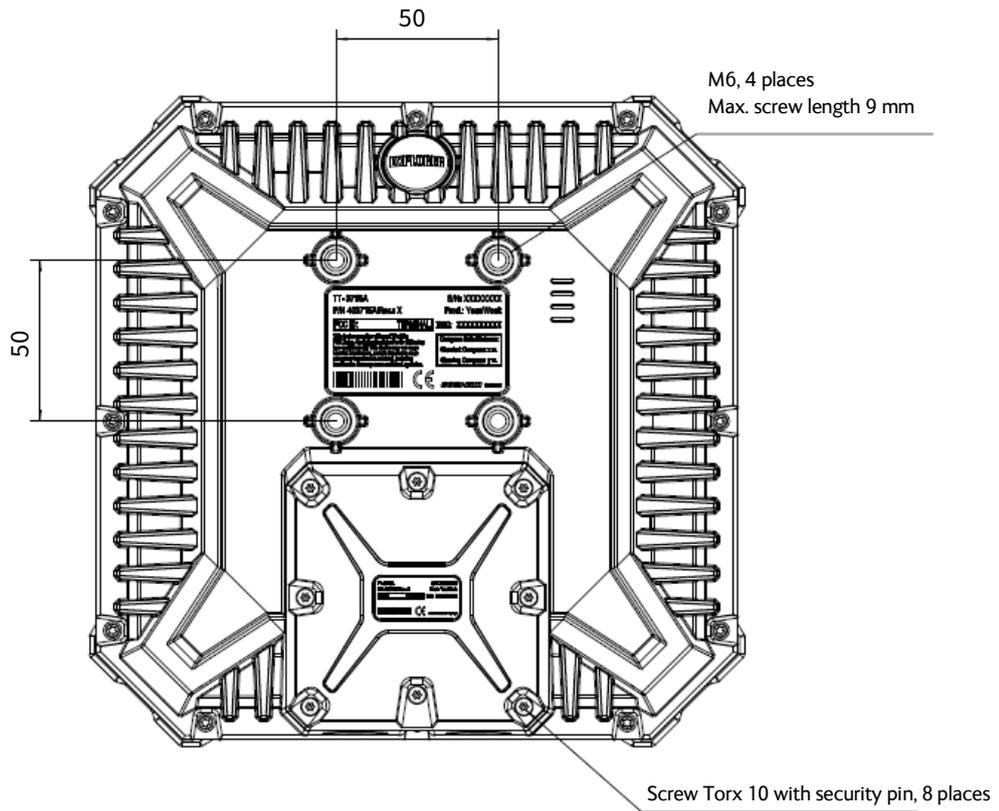
Dimensions are in mm

# A.5    Optional EXPLORER 540 Cellular Modem

## A.5.1    Specifications

### EXPLORER 540 Cellular Modem

**COBHAM**

Turns your BGAN into a dual mode M2M terminal

| Cellular Modules | NimbeLink NL-SW-HSPA | NimbeLink NL-SW-LTE-QBG9 | NimbeLink NL-SW-LTE-TC4EU |
|---|---|---|---|
| Region | Global | Global | Europe |
| Compatible Carriers | AT&T, T-Mobile, WW 3G Networks | AT&T, Orange, Telstra, Telus, Verizon, Vodafone | Orange, Vodafone |
| Cellular Technology | 3G | LTE | LTE |
| LTE Category | - | LTE-M, NB-IoT | LTE CAT 4 |
| LTE Frequency Bands | - | **LTE-FDD**: B1[2100], B2[1900], B3 [1800], B4[1700], B5[850], B8 [900], B12[700], B13[700], B18 [850], B19[850], B20[800], B26 [850], B28[700]<br>**LTE-TDD**: B39 [1900] (LTE-M only) | FDD B1[2100], B3[1800], B7 [2600], B8[900], B20[800] |
| 3G Technology | UMTS, HSPA+ | - | - |
| 3G Frequency Bands | B1[2100], B2[1900], B4[1700], B5 [850], B8[900] | - | B1 [2100], B8 [900] |
| 2G Technology | GSM, EDGE, GPRS | GSM, EDGE, GPRS | GSM, EDGE |
| 2G Frequency Bands | GSM850/900, DCS1800, PCS1900 | GSM850, EGSM900, DCS1800, PCS1900 | GSM900, DCS1800 |
| Data Rates | **Download**: HSPA+: 21.0 Mbps \|EDGE: 296 Kbps \| GPRS: 107 Kbps<br>**Upload**: HSPA+ 5.76 Mbps \| EDGE: 236.8 Kbps \| GPRS: 85.6 Kbp | **Download**: LTE-M: 375 Kbps \| NBIoT: 32 Kbps \| GPRS: 107 Kbps \| EDGE: 296 Kbps<br>**Upload**: LTE-M: 375 Kbps \| NBIoT: 70 Kbps \| GPRS: 85.6 Kbps \| EDGE: 236.8 Kbps | **Download**: LTE: 150 Mbps \| HSPA+: 42.0 Mbps \| EDGE: 296 Kbps<br>**Upload**: LTE: 50 Mbps \| HSPA+: 5.76 Mbps \| EDGE: 236.8 Kbps |
| Regulatory | GCF, PTCRB, CE/RED, FCC, IC, Anatel | PTCRB, CE/RED, FCC, IC | CE/RED |
| Carrier Approvals | AT&T, Rogers, Telus | AT&T, Rogers (In-Progress), Telus, Verizon | - |

| Cellular Modem Housing | | | | | | |
|---|---|---|---|---|---|---|
| **Specifications**<br>- Operating Temperature<br>- IP rating (in housing)<br>- Size (L / W / D)<br>- Weight in housing | -40°C to +85°C<br>IP66<br>85 / 85 / 40 mm<br>380 gram | | | | | |
| **Power Consumption** | 12V | 24V | 12V | 24V | 12V | 24V |
| - Sleep | < 2 mW | 15 mW | < 2 mW | 15 mW | < 2 mW | 15 mW |
| - Idle (Average) | 490 mW | 590 mW | 580 mW | 695 mW | 600 mW | 720 mW |
| - Transmitting (Peak - 2G) | - | - | 3.85 W | 4.05 W | - | 1.05 W |
| - Transmitting (Peak - LTE) | 930 mW | 990 mW | 1.00 W (est.) | 1.00 W (est.) | 1.00 W | 1.05 W |
| **Cellular Antenna Connector** | 2 x SMA Connectors. One primary and one for diversity (Number of antennas depends on operator requirements). EXPLORER Cellular Antenna is optional | | | | | |

| External Cellular Antenna | |
|---|---|
| **EXPLORER Cellular Antenna**<br>- Type<br>- Frequencies<br>- Gain | External, Omni-Directional<br>698 - 960 MHz, 1427 - 1518 MHz, 1710 - 2170 MHz, 2300 - 2690 MHz<br>0 dBd, 2.15 dBi (698-960 MHz), 3 dBd, 5.15 dBi (1427-1518/1710-2170 MHz), 7 dBd, 9.15 dBi (2300-2690/3300-3800 MHz) |

| Productnumbers | | | |
|---|---|---|---|
| - EXPLORER Modem bundle<br>  (Includes housing and module) | 403715A-00215 | 403715A-00214 | 403715A-00212 |
| - EXPLORER Cellular Antenna | 403715A-00105 | | |
| **BGAN Firmware** | EXPLORER 540 version 1.05 or later | | |

Cellular SIM Card

NimbeLink module

External EXPLORER Cellular Antenna

SMA Connectors for External Antenna

Cellular Modem Housing

For further information please contact:

Cobham SATCOM Land
Lundtoftegaardsvej 93 D
DK-2800  Kgs. Lyngby, Denmark
Tel:   +45 3955 8800
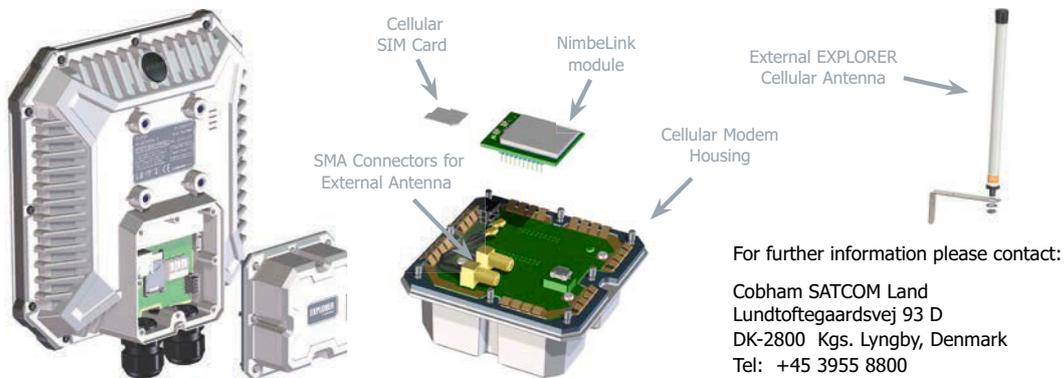
71-174696-A01 10.20 LMBU

**www.cobham.com/satcom**

## A.5.2    Outline drawing, EXPLORER 540 Cellular Modem



33.1

81.1

83.6

42.6
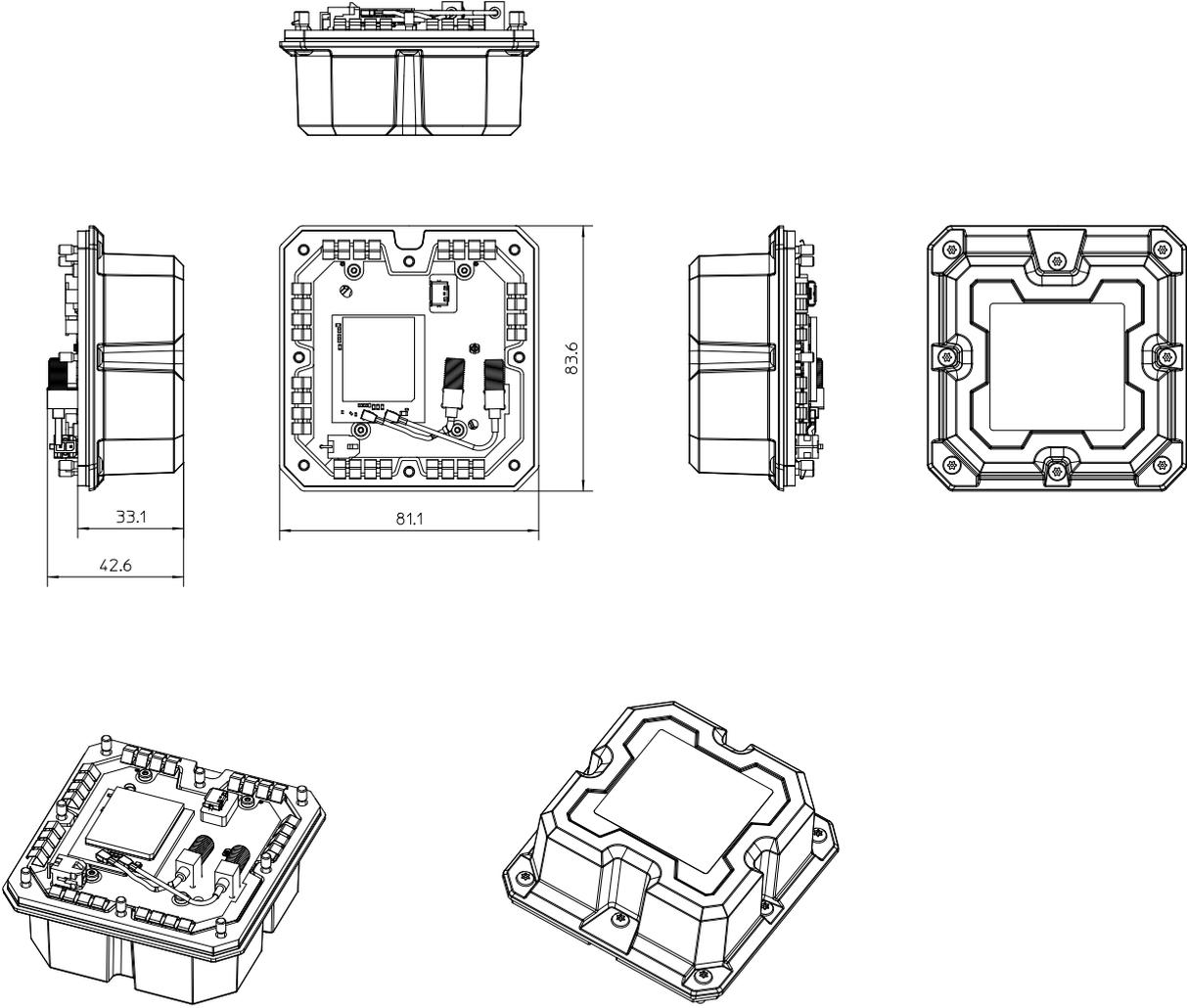
Dimensions are in millimeter

## A.5.3    Outline drawing, EXPLORER 540 with integrated cellular modem

2 x M20x1.5 Threads for cable glands

202

202

65

89.9

Dimensions are in millimeter

50

M6, 4 places
Max screw length 9 mm

50

Screw Torx 10 with security pin
8 places

Compartment for SIM
card and connections

Pole size 1" to 1.5"
(33.7 to 48.3 mm)
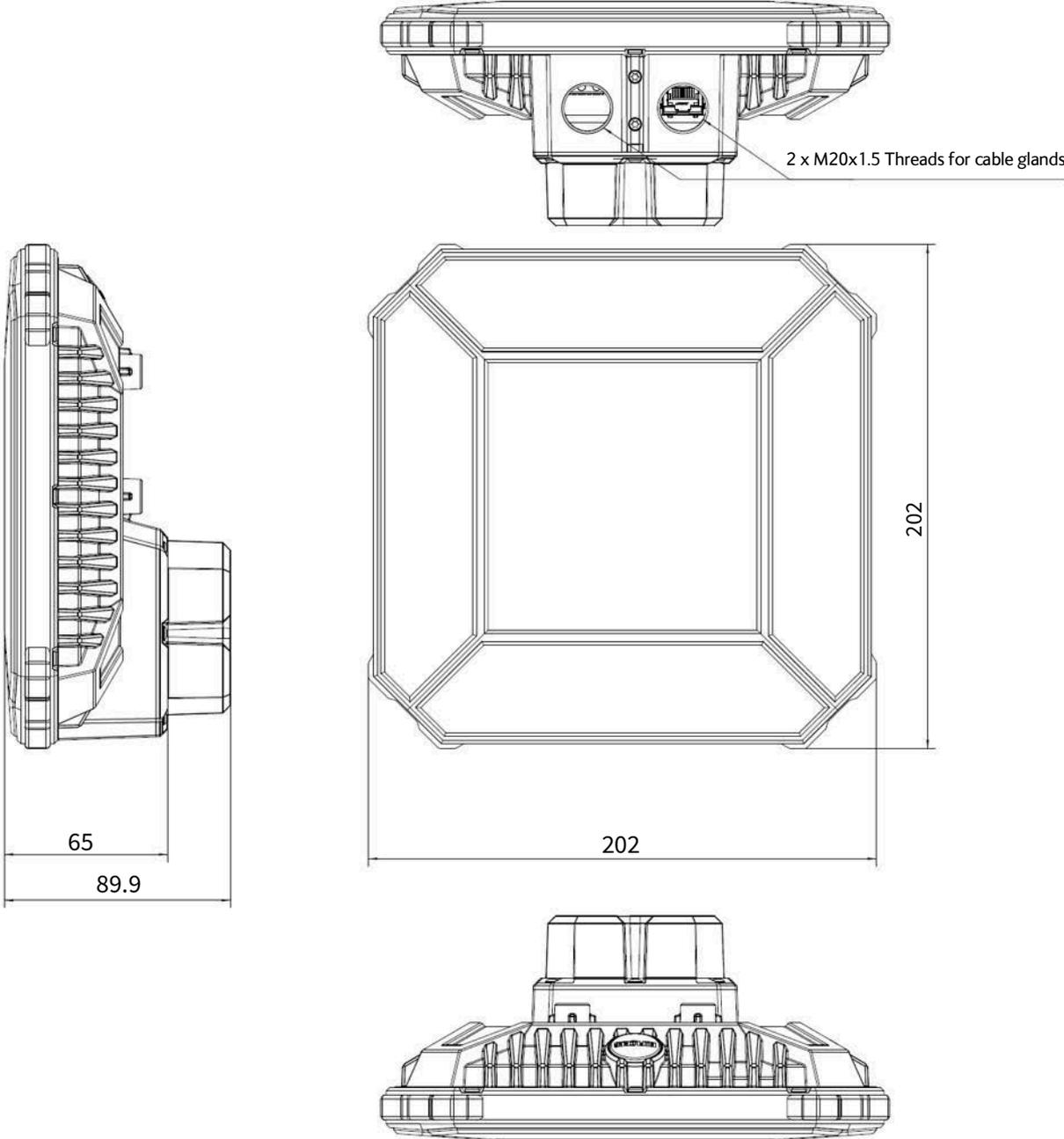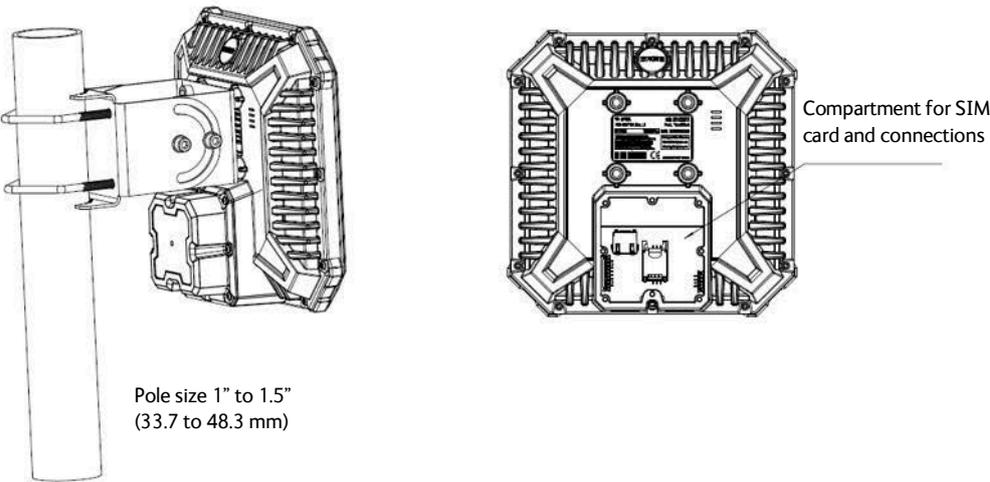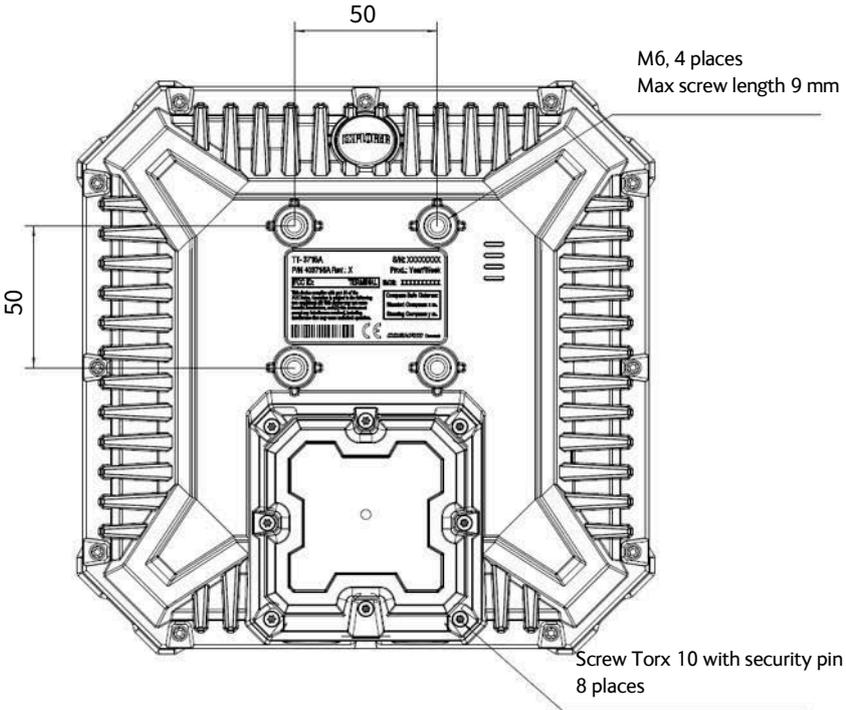
Dimensions are in millimeter

# Command reference

This appendix lists the function, syntax and parameters for commands used with the EXPLORER 540. You can send commands to the EXPLORER 540 either with an SMS or via AT shell. SMS is very useful for remote operation, because you only need the terminal's mobile number to access the terminal. This appendix has the following sections:

- *Overview of M2M AT and SMS commands*
- *SMS remote commands*
- *AT commands*

COBHAM SATCOM

# B.1   Overview of M2M AT and SMS commands

| Function | Command | Interface | | |
|---|---|---|---|---|
| | | **AT shell** | **ATCO SMS** | **SMS** |
| Lock and unlock AT shell | _ICLCK | X | | |
| Control MAC address locking | _IMACLOC | X | | |
| Configuration of MAC address list | _IMACLOCAD | X | | |
| Control remote SMS commands | _ISMSRMT | X | | |
| Reset passwords | _ICPWD | X | X | |
| Control remote access to web interface | _IREMWEB | X | X | |
| Download and update SW | _IGETFW | X | X | |
| Install new SW | _IUPDFW | X | X | |
| Send file from terminal to FTP server | _ISENDFILE | X | X | |
| Get file from FTP server to terminal | _IGETFILE | X | X | |
| Update configuration file | _IUPDCFG | X | X | |
| Power Save configuration | _IPWSAVSCHD | X | | |
| Remote on/off configuration | _ITREMONOFF | X | | |
| Link Monitoring configuration | _ITLINKMON | X | | |
| Enable Antenna RF noise filter | _IATCROBST | X | X | |
| Activate/deactivate the 3-GPIO pin or get the status of the pin (general purpose I/O) | _ITGPIO | X | X | |
| Get input voltage of the EXPLORER 540 | _ITDCIV | X | X | |
| Get list of attached equipment with IP addresses and MAC addresses | _ITARP | X | | |
| Administrator password control | ADPWRST | | | X |
| Activate PDP context | ACTIVATE | | | X |
| Deactivate PDP context | DEACTIVATE | | | X |
| Delete SMS messages | CLEAR | | | X |
| Get terminal information | GETINFO | | | X |
| Restart the terminal | RESTART | | | X |
| Configuration of Connection watchdog function | WATCHDOG | | | X |

| Function | Command | Interface | | |
|---|---|---|---|---|
| | | **AT shell** | **ATCO SMS** | **SMS** |
| Configuration of Terminal watchdog function | ADVWATCHDOG | | | X |
| Configuration of WAN mode | WANMODE | | | X |

# B.2    SMS remote commands

This section describes syntax and parameters for the SMS commands. For examples of use, see *Remote access with SMS* on page 3-4.

## 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> | … | NA } indicates that one of various options must be chosen by the user. Use **NA** when no value is defined.
- Keywords and parameters are separated by the space (ASCII 32) character.
- The command name and all keywords must be in upper case; most user-provided parameters are case sensitive but may be either case.
- **TE** means Terminal Equipment - the equipment connected locally to the EXPLORER 540.

## B.2.2    SMS remote command summary

### Commands

The table below summarizes the available SMS remote commands. The password comes just after the last parameter (except for the ATCO command, see below). For examples, see *Remote access with SMS* on page 3-4.

| Command | Parameters | Password |
|---|---|---|
| ACTIVATE | <qos> <PC/TE type> <apn> <user> <pwd> | <rsms_pwd> |
| ADPWRST | 1 <imei> | <rsms_pwd> |
| ADVWATCHDOG | <get/set> <wdog_enable> <wakeup> <interval> <ping1> <ping2> <ping3> <apn_type> <apn> <user> <pwd> <pos_response> <sms_number> | <rsms_pwd> |
| CLEAR | <category> SMS | <rsms_pwd> |
| DEACTIVATE | <qos> <PC/TE type> | <rsms_pwd> |
| GETINFO | <info_mode> <dataset> | <rsms_pwd> |
| RESTART | <reset_type> BGAN | <rsms_pwd> |
| WATCHDOG | <wdog_op> <ping1> <ping2> <ping3> <ping_always> <ping_interval> <wdog_enable> | <rsms_pwd> |
| WANMODE | <cmd_op> {<wanmode>} | <rsms_pwd> |
| **SMS command for sending AT commands** | | |
| ATCO | <resp_mode> <rsms_pwd> <at_cmd> | |

## Parameters

The table below summarizes the available parameters for the SMS remote commands.

| Parameter | Values | Meaning |
|---|---|---|
| <apn_type> | SIM default | Read the APN from the SIM card. |
| | Network assigned | Use the APN assigned by the network. |
| | User defined | Specify another APN to use. |
| | NA | Placeholder when no value is specified. The existing setting applies. |
| <apn> | <APN> | APN name, e.g. **bgan.inmarsat.com.** |
| | NA | Placeholder when no APN is specified. Note that any previously entered APN is maintained. |
| | CLR | No APN is used. |
| <at_cmd> | <at_cmd> | AT command, without prefix AT. For supported AT commands, see *ATCO commands* on page B-10. |
| <category> | 1 | Delete only Read SMS messages. |
| | 2 | Delete Read and Sent. |
| | 3 | Delete All except Unread. |
| | 4 | Delete All SMS messages. |
| <cmd_op> | 1 | Get WANMODE setting. |
| | 2 | Set WANMODE configuration. |
| <dataset> | GPS | GPS position. |
| | USAGE | Cumulative call time and data usage. |
| | ALL | GPS position plus call time and data usage. |
| <get_set> | 1 | Get parameters. |
| | 2 | Set parameters. |
| <imei> | <14 digits> | IMEI of the EXPLORER 540, without dashes or check digit. |
| <info_mode> | 1 | For GPS query: position data only. For other queries: use verbose mode (with titles). |
| | 2 | For GPS query: position data plus SMS usage. For other queries: use terse mode (no titles). |
| <interval> | <integer> | The number of hours between the Terminal watchdog sessions (1-504). |
| | NA | Placeholder when no value is specified. The existing setting applies. |
| <PC/TE type> | DHCP | All TEs known via DHCP. |
| | STATIC | All TEs known via Terminal settings. |
| | AWO | Always On, deactivate all PDP contexts including those established with ACA. |
| | <name> | Name of specific TE, as known by DHCP server. |
| | <IP addr> | IP Address of specific TE (or Global IP for DEACTIVATE). |
| | ANY | Any/all TEs attached (DEACTIVATE: all except PDP context established with ACA). |

| Parameter | Values | Meaning |
|---|---|---|
| <ping_always> | 0 | Send ping only if no traffic. |
| | 1 | Always send ping, regardless of data traffic. |
| | NA | Placeholder when no value is specified. Note that the existing setting applies. |
| <ping_interval> | <integer> | Interval between pings (minutes). |
| | NA | Placeholder when no value is specified. Note that the existing setting applies. |
| <ping[1/2/3]> | <IP addr> | Three ping destination IP addresses. **Note**: You must fill in all three places. **0.0.0.0** means any previously entered IP address in this position is deleted. |
| | NA | Placeholder when no IP address is specified. Note that any previously entered IP address is maintained. |
| <pos_response> | 0 | Send an sms response[1]. |
| | 1 | Do not send an sms response[a]. |
| | NA | Placeholder when no value is specified. |
| <pwd> | <APN password> | Password associated with APN username. |
| | NA | Placeholder when no APN password is specified. Note that any previously entered password is maintained. |
| | CLR | Password is not used. |
| <qos> | 1 | Standard/background data (currently the only qos available for M2M). |
| <reset_type> | 1 | Normal delay restart. |
| <resp_mode> | 0 | None – send no responses to AT commands. |
| | 1 | Immediate - immediate responses, but not unsolicited. |
| | 2 | Final – suppress immediate if OK, plus unsolicited. |
| | 3 | All – send both immediate and unsolicited responses. |
| <rsms_pwd> | <rsms_pwd> | Remote SMS password. The password must be 5 to 15 characters long and cannot contain spaces. |
| | | Accepted characters are: A through Z (uppercase characters), a through z (lowercase characters) and 0 through 9 (numeric characters). |
| <sms_number> | <sms_number> | The phone number to be used for sms response. |
| | NA | Placeholder when no value is specified. |
| <user> | <APN user name> | User name associated with APN. |
| | NA | Placeholder when no APN user name is specified. Note that any previously entered user name is maintained. |
| | CLR | User name is not used. |
| <wakeup> | 0 | Do not wake up the terminal. |
| | 1 | Wake up the terminal at the specified intervals. |
| | NA | Placeholder when no value is specified. The existing setting applies. Used if you want to change one of the other parameters without changing the wake-up setting. |

1. Position SMS response is only for future use, and should be set to NA

| Parameter | Values | Meaning |
|---|---|---|
| <wanmode> | 0 | Not valid for EXPLORER 540 |
| | 1 | Not valid for EXPLORER 540 |
| | 2 | BGAN only. |
| | 3 | Not valid for EXPLORER 540. |
| | 4 | Cellular modem preferred |
| | 5 | Not valid for EXPLORER 540. |
| | 6 | Cellular modem preferred (PRISM) |
| | 7 | External modem preferred |
| | 8 | External modem preferred (PRISM) |
| <wdog_enable> | 0 | Disabled. |
| | 1 | Enabled. |
| | NA | Placeholder when no value is specified. The existing setting applies. Used if you want to change one of the other parameters without changing the enabled/ disabled setting. |
| <wdog_op> | 1 | Get watchdog configuration. |
| | 2 | Set watchdog parameters. |

## B.2.3    SMS reject responses

| Reject Response SMS | Possible Cause |
|---|---|
| ACT/DEACT PARM PROBLEM | The <IP addr> provided for an ACTIVATE or DEACTIVATE command is incorrect (for ACTIVATE, it must be in same subnet as the EXPLORER 540 IP and not be the EXPLORER 540 IP; for DEACTIVATE, it must exist as a local or global IP address in the existing PDP table). |
| ATCO ERROR | Unable to send AT command to ATC handler. |
| COMMAND NOT SUPPORTED | Attempt to use an SMS command not supported by the EXPLORER 540. |
| ERROR: TERMINAL BUSY | An ACTIVATE or DEACTIVATE command is in progress. |
| INVALID RESTART REQUEST | Attempt to perform restart before EXPLORER 540 has been running for at least 15 minutes. |
| INVALID WANMODE REQUEST | The requested WAN mode is not supported by the EXPLORER 540, or invalid parameters are used. |
| INVALID WATCHDOG PING ADDRESS | Entered Ping address is out of range (0.0.0.0 – 255.255.255.254). |
| INVALID WATCHDOG PING FREQUENCY | Requested Ping Frequency is less than the minimum (5 minutes). |
| INVALID WATCHDOG REQUEST | "Ping required" or "wdog enabled" fields incorrect in remote SMS message, or watchdog request other than "get" attempted. |
| WRONG CONNECTION TYPE(NO DHCP TE) | No DHCP TEs connected to the Remote Unit. |
| WRONG CONNECTION TYPE(NO STATIC TE) | No Static TEs added in Terminal settings. |
| WRONG CONNECTION TYPE(NO TEs) | No TEs are connected to the Remote Unit. |
| WRONG PASSWORD | Authentication Failure. |
| WRONG QOS | Invalid QoS Requested (only a QoS of 1 is valid). |

# B.3   AT commands

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

> **Note** AT commands related to data connections are only applicable to the BGAN connection, not to the optional cellular connection.

- *M2M related AT commands*
- *AT commands for message (SMS) configuration*
- *Context management AT commands*
- *AT commands for dual mode with cellular modem*

> **Note** AT commands must first be enabled in the web interface of the terminal. See *To allow the use of AT commands on LAN interface* on page 4-45.

## B.3.1   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>`**
- The command name and all keywords must be in upper case; most user-provided parameters are case sensitive but may be either case.
- **TE** means Terminal Equipment - the equipment connected locally to the EXPLORER 540.

## B.3.2 M2M related AT commands

The following tables summarize some of the most used AT commands for M2M operation. Parameters are explained in *Parameters for ATCO commands* on page B-11 and *Parameters for other M2M related AT commands* on page B-14.

### ATCO commands

The table below summarizes the ATCO commands, i.e. AT commands that can be used in the SMS command **ATCO**.

> **Note** SMS commands always use the BGAN network, regardless of the selected connection mode (Cellular or BGAN).

| Command | Parameters |
|---------|-----------|
| _IATCROBST[1] | <enable> |
| _ICPWD | <type>,<old passwd>,<new passwd> |
| _IGETFILE | <ftp dir>,<filename>,<local dir>,<ftp server>,<ftp uname>,<ftp passwd>[,<apn>[,<apn uname>[,<apn passwd>]]] |
| _IGETFW | <mode>[,<ftp server>[,<ftp uname>[,<ftp passwd>[,<apn>[,<apn uname>[,<apn passwd>]]]]]] |
| _IREMWEB | <enable>,<ip_addr_lo>[,<ip_addr_hi>][,<apn>[,<apn uname>,<apn passwd>]] |
| _ISENDFILE | <local dir>,<filename>,<ftp dir>,<ftp server>,<ftp uname>,<ftp passwd>[,<apn>[,<apn uname>[,<apn passwd>]]] |
| _IUPDCFG | <filename> |
| _IUPDFW | <filename> |

1. Robustness for 3GPP LTE signals, not ATC

## Parameters for ATCO commands

| Parameter | Values | Meaning |
|---|---|---|
| <apn passwd> | <apn passwd> | Password for the APN. |
| <apn uname> | <apn uname> | User name for the APN. |
| <apn> | <apn> | APN name. |
| <enable> | 0<br>1 | Disable.<br>Enable. |
| <filename> | <filename> | The name of the file to use, including extension. |
| <ftp dir> | <ftp dir> | The name of the directory on the ftp server to use for getting or saving a file. |
| <ftp passwd> | <ftp passwd> | Password for the ftp server. |
| <ftp server> | <ftp server> | Host name or IP address of the ftp server. |
| <ftp uname> | <ftp uname> | User name for the ftp server. |
| <ip_addr_hi> | <ip_addr_hi> | The upper IP address of a range of allowed IP addresses. This parameter is optional; if omitted, only the specified single IP address <ip_addr_lo> may access the EXPLORER 540. |
| <ip_addr_lo> | <ip_addr_lo> | IP address of the HTTP client that should be allowed remote access to the EXPLORER 540, or<br>the lowest address in a range of IP addresses, if a range of addresses is allowed. |
| <local dir> | <local dir> | The name of the local directory in the EXPLORER 540 to use for getting or saving a file. |
| <mode> | 0<br>1 | Deferred activation.<br>Immediate activation. |
| <new passwd> | <new passwd> | The new password to be used after this command. The password must be 5 to 15 characters long and cannot contain spaces.<br>Avoid special characters. Accepted characters: A through Z (uppercase characters), a through z (lowercase characters) and 0 through 9 (numeric characters). |
| <old passwd> | <old passwd> | The old password that is already in the system. |
| <type> | AD<br>RS | The type of password is administrator password.<br>The type of password is remote SMS password. |

## ATCO response codes

The following response codes apply to the AT commands supported by SMS.

| Code | Text | Explanation |
|---|---|---|
| **General codes** | | |
| 0 | Complete | Operation completed successfully. |
| 1 | Unexpected software error | Software error. |
| 2 | Local file open error | _IGETFILE: could not open local file after download.<br>_ISENDFILE: could not open local file.<br>_IUPDCFG: Loading configuration failed. Incompatible file format. |
| 3 | Directory not found | Could not find specified directory on local file system. |
| 4 | File not found | Could not find specified file name on local file system. |
| 5 | Error renaming file | Could not restore after failed upgrade. |
| **Context Management codes** | | |
| 13 | Context activation error | Context activation failed. Could be problem with PS attach, SIM subscription, APN, network or connectivity. |
| **FTP Management codes** | | |
| 20 | FTP hookup fail | Connection to FTP server failed. Problem could be server unreachable or specified IP address or server name invalid, or connectivity failure. |
| 21 | FTP login fail | FTP user name or password incorrect. |
| 23 | FTP 'cwd' fail | Could not change to working directory on FTP server. |
| 24 | FTP data connection fail | Could not establish an FTP data connection with the server. |
| 26 | FTP xfer command fail | Could not initiate data transfer on an established connection. May be caused if filename not found. |
| 29 | FTP socket fail | Error while reading or writing FTP data socket. |
| 31 | FTP xfer timed out | FTP client timed out waiting for socket ready (read or write), e.g. due to loss of connectivity during transfer. |
| **_IGETFW command codes** | | |
| 40 | File in use, cannot download | The file to be downloaded is the same as the image currently in use. |
| 41 | Starting immediate upgrade… | Normal success. File downloaded successfully, now starting immediate update. |
| **_IUPDFW command codes** | | |
| 50 | New firmware file not found | Could not find specified filename. |

| Code | Text | Explanation |
|------|------|-------------|
| 51 | New firmware file corrupt | New firmware file corrupt. |
| 52 | New firmware file failure | The new firmware failed to run or failed to acquire the network and the unit fell back to the old release. |
| 54 | Upgrade status file error | Previous update has not finished yet. |
| **_IREMWEB command codes** | | |
| 81 | Global IP: <ip_addr> | Remote connection to web interface is set up successfully. Indicates global IP address assigned to the EXPLORER 540's own PDP context, to which an HTTP connection may be made. |

## Other M2M related AT commands

| Command | Parameters |
|---------|-----------|
| _ICLCK | <type>,<enable>,<passwd> |
| _IMACLOC | <enable>,<interface>[,<interface>] |
| _IMACLOCAD | <action>,<interface>,<MAC Address>[,<MAC Address>][1] |
| _IPWSAVSCHD | <psmode>,<psvalue> |
| _ISMSRMT | <enable> |
| _ITARP | <ip>,<mac> |
| _ITGPIO | <active> |
| _ITDCIV | No parameters[2] |
| _ITLINKMON | [<enabled>[,<intv>[,<retr>[,<mode>[,<ip1>[,<ip2>[,<ip3>,[,<intv_cell>[,<retr_cell>[,<intv_fail_cell>]]]]]]]]]] |
| _ITREMONOFF | <active mode>,<power down delay>,<awake time of day>,<awake duration>,<polarity> |

1. Up to 10 MAC addresses may be specified.
2. Type **_ITDCIV?** to get the input voltage (in mV) of the EXPLORER 540

**See parameters in the next page**.

## Parameters for other M2M related AT commands

The table below summarizes the available parameters for the AT commands for M2M operation.

| Parameter | Values | Meaning |
|---|---|---|
| <action> | 0<br>1 | Delete.<br>Add. |
| <active> | 0<br>1 | Inactive. The GPIO pin is in its inactive state.<br>Active. The GPIO pin is in its active state. |
| <active mode> | 0<br>1 | Inactive. Remote on/off is not used. Terminal is set to Always on.<br>Active: Remote on/off is enabled |
| <awake duration> | 3 - 1440 (minutes) | This is the duration of the daily awake period. |
| <awake time of day> | 0 - 1440 (minutes) | This is the number of minutes after midnight that the terminal should wake up every day. If you enter 0 the daily awake period is disabled. |
| <enable> | 0<br>1 | Disable.<br>Enable. |
| <enabled> | 0<br>1 | Disabled.<br>Enabled. |
| <interface> | 0 | 0 means Ethernet interface. This is the only option. |
| <intv> | 4 to 2678400 seconds (31 days) | Interval in seconds between pings over BGAN connection.<br>Default 300 seconds. |
| <intv_cell> | 4 to 2678400 seconds (31 days) | Interval in seconds between pings over Cellular connection.<br>Default 300 seconds.<br>Note that this setting is only applicable for EXPLORER 540 with Prism capability. On any other terminal the argument is ignored. |
| <ip> | <IP address > | The IP address(es) of connected equipment. |
| <ip1> | <IP address > | Primary IP address to ping, in dot-decimal notation.<br> To delete the entry, input 0.0.0.0 |
| <ip2> | <IP address > | Secondary IP address to ping, in dot-decimal notation.<br> To delete the entry, input 0.0.0.0 |
| <ip3> | <IP address > | Tertiary IP address to ping, in dot-decimal notation.<br> To delete the entry, input 0.0.0.0 |
| <mac> | <MAC address> | The MAC address(es) of connected equipment. |
| <MAC Address> | <MAC Address> | MAC address(es) for MAC locking. Up to 10 MAC addresses are permitted. |
| <mode> | 0<br>1 | Only ping when no other traffic is observed.<br>Always ping (default). |
| <passwd> | <passwd> | The existing administrator password. |

| Parameter | Values | Meaning |
|---|---|---|
| <polarity> | HIGH | The Power control pin will be active high. |
| | LOW | The Power control pin will be active low. |
| <power down delay> | 0 - 1440 (minutes) | This is the time from when the Power control pin is deactivated until the terminal enters power save state. |
| <psmode> | IDLE_TRG | The power save mode is Idle power save and the trigger to set up is "idle trigger", that is the time with no activity before entering power save state. |
| | TOD_TRG | The power save mode is Idle power save and the trigger to set up is "time of day", that is a specific time of day (UTC time) where the EXPLORER 540 wakes up from power save state. |
| | WOL_STATUS | The power save mode is Idle power save and the trigger to set up is Wake-on-LAN. A "magic packet" received on the LAN interface wakes up the terminal from power save state. |
| <psvalue> | <idle-minutes> | Used with IDLE_TRG (above). Number of minutes (e.g. 15). |
| | <HH:MM> | Used with TOD_TRG (above). Time of day in UTC time (e.g. 23:30). |
| | 0 or 1 | Used with WOL_STATUS (above). 0 is Off and 1 is On |
| <retr> | 1 to 255 | Number of ping retries needed before determining the BGAN link is down. Default 3. |
| <retr_cell> | 1 to 255 | Number of ping retries needed before determining the Cellular link is down. Default 3. Note that this setting is only applicable for EXPLORER 540 with Prism capability. On any other terminal the argument is ignored. |
| <intv_fail_cell> | 3 to 255 | Ping interval after first failure on Cellular connection. Default 20. Note that this setting is only applicable forEXPLORER 540 with Prism capability. On any other terminal the argument is ignored. |

## B.3.3    AT commands for message (SMS) configuration

The following AT commands are used for configuration of SMS.

Note ▷ For details on parameters for the message configuration commands, see the 3GPP standard ETSI TS 127 005 V4.2.1.

| Command | Parameters | Function |
|---------|-----------|----------|
| +CMGD | <index> | Delete Message. |
| +CMGF | <mode> | Message Format. |
| +CMGL | <stat> | List Messages. |
| +CMGR | <index> | Read Messages. |
| +CMGS | <da/mr>[,<toda/scts>] | Send Message. |
| +CNMI | [<mode>[,<mt>[,<bm>[,<ds>]]]] | New Message Indications to TE. |
| +CPMS | <mem1>[,<mem2>[,<mem3>]] | Preferred Message Storage. |
| +CSCA | <sca>[,<tosca>] | Service Center Address. |
| +CSMP | [<fo>[,<vp>[,<pid>[,<dcs>]]]] | Set Text Mode Parameters. |
| +CSMS | <service> | Select Message Service. |

# B.3.4 Context management AT commands

The table below summarizes some of the most used AT commands for context management. Parameters are explained in the table in the next section. For details, refer to the 3GPP standard TS 27.007.

| Note | The context management AT commands can only be used over a BGAN connection and will not work on a cellular connection. |
|------|---|

| Command | Parameters |
|---------|------------|
| +CGACT | [<state>[,<cid>[,<cid>[,...]]] |
| +CGDCONT | [<cid>[,IP[,<APN>[,<PDP_addr>[,<d_comp>[,<h_comp>[,<apn uname>,<apn_passwd>]]]]]]] |
| +CGDSCONT | [<cid>,<p_cid>[,<d_comp>[,<h_comp>]]] |
| +CGEQMIN | [<cid>[,<Traffic class>[,<Maximum bitrate UL>[,<Maximum bitrate DL>[,<Guaranteed bitrate UL>[,<Guaranteed bitrate DL>[,<Delivery order>[,<Maximum SDU size>[,<SDU error ratio>[,<Residual bit error ratio>[,<Delivery of erroneous SDUs>[,<Transfer delay>[,<Traffic handling priority>]]]]]]]]]]]]] |
| +CGEQREQ | [<cid>[,<Traffic class>[,<Maximum bitrate UL>[,<Maximum bitrate DL>[,<Guaranteed bitrate UL>[,<Guaranteed bitrate DL>[,<Delivery order>[,<Maximum SDU size>[,<SDU error ratio>[,<Residual bit error ratio>[,<Delivery of erroneous SDUs>[,<Transfer delay>[,<Traffic handling priority>]]]]]]]]]]]]] |
| +CGPADDR | [<cid>[,<cid>[,...]]] |
| +CGTFT | [<cid>[,<packet filter identifier>,<evaluation precedence index>[,<source address and subnet mask>[,<protocol number (ipv4) / next header (ipv6)>[,<destination port range>[,<source port range>[,<ipsec security parameter index (spi)>[,<type of service (tos) (ipv4) and mask / traffic class (ipv6) and mask>[,<flow label (ipv6)>]]]]]]]]] |

## Parameters for context management AT commands

The table below summarizes the main parameters for the AT commands for context management. For details, refer to the 3GPP standard TS 27.007.

| Parameter | Values | Meaning |
|-----------|--------|---------|
| <apn passwd> | <apn passwd> | Password for the APN. |
| <apn uname> | <apn uname> | User name for the APN. |
| <apn> | <apn> | APN name. |
| <cid> | <cid> | The Context Identifier (1 – 11) for the PDP context. If no cid is entered, the command applies to all defined PDP contexts. |
| <d_comp> | 0 | Data compression off (default if value is omitted). |

| Parameter | Values | Meaning |
|---|---|---|
| <destination port range> | <destination port range> | Destination port range in the form **From.To**.<br><br>To indicate only one port, type in the same port number under From and To.<br><br>**Example:** 65333.65338 indicates port numbers from 65333 to 65338, both included. |
| <evaluation precedence index> | <evaluation precedence index> | The evaluation precedence index defines the order in which the traffic flow filters are applied to packets. 0 is first, then 1, 2 etc. |
| <Guaranteed bitrate DL> | <Guaranteed bitrate DL><br><br>0 | The guaranteed bit rate down link (32, 64, 128).<br><br>If the parameter is set to '0' the subscribed value will be requested. |
| <Guaranteed bitrate UL> | <Guaranteed bitrate UL><br><br>0 | The guaranteed bit rate up link (32, 64, 128).<br><br>If the parameter is set to '0' the subscribed value will be requested. |
| <h_comp> | 0<br>1 | Header compression off (default if value is omitted).<br>Header compression on (manufacturer preferred compression). |
| <Max bitrate DL> | <Max bitrate DL><br>0 | The maximum bit rate down link (32, 64, 128).<br>If the parameter is set to '0' the subscribed value will be requested. |
| <Max bitrate UL> | <Max bitrate UL><br>0 | The maximum bit rate up link (32, 64, 128).<br>If the parameter is set to '0' the subscribed value will be requested. |
| <p_cid> | <p_cid> | The primary context to which the secondary context is related. |
| <packet filter identifier> | <packet filter identifier> | The packet filter identifier (1 – 8). |
| <PDP_addr> | <PDP_addr> | Omit this parameter - note that the comma must still be there if other parameters come after this one. |
| <protocol number> | <protocol number> | This number is uniquely assigned for the protocol being used. TCP is set to 6, and UDP is set to 17. The protocol number determines which protocol is used by the traffic flow filter (0-255). |
| <source address and subnet mask> | <source address and subnet mask> | This is an IPv4 IP address and subnet mask (0.0.0.0.0.0.0.0 to 255.255.255.255.255.255.255.255). The first four numbers are the IP address and the last four numbers are the subnet mask. |
| <source port range> | <source port range> | Source port range in the form **From.To.**<br>See <*destination port range*> for example. |
| <state> | 0<br>1 | Deactivate.<br>Activate. |
| <Traffic Class> | 1<br>3 | Streaming (not available for M2M subscription).<br>Standard data (Background). |
| <Transfer delay> | 0<br>500<br>4000 | 0 ms, error correction is determined by the network.<br>500 ms, error correction is disabled.<br>4000 ms, error correction is applied. |

## B.3.5    AT commands for dual mode with cellular modem

| Command | Parameters | Function |
|---|---|---|
| _ITEXTMODEM | [<ip>[,<dns1>[,<dns2>]]] | Get or set values related to the external modem.<br><br>Note: If you set up a new IP address and you already have an external modem running on a different IP address, you have to reboot the terminal to reset the IP routing. |
| _ITLINKSTATUS | <active>,<bgan>,<cell>,<ext> | Show link status for available connection type |
| _ITMACFG | <manual>,<mcc>,<mnc>,<2g>,<3g>,<4g>,<access tech> | Configure cellular modem access technology and operator selection |
| _ITMFWUPD | <filename-url> | Update firmware for QBG96 modem over the air from <filename-url>. Note that the terminal reboots after updating. |
| _ITMSIG | <signal strength> | Show signal strength of the cellular signal. |
| _ITPRISMCONF | [<conn_delay>[,<boot_delay>[,<test_ip>]]] | Get or set values related to the PRISM server general configuration. |
| _ITPRISMPING | <mode>[,<intv>[,<intv_fail>[,<max_fail>]]] | Get or set values related to the Cellular/BGAN monitoring. |
| _ITPRISMSRV | <n>[,<key>[,<ip>[,<port>]]] | Get or set values related to the PRISM server(s). |
| _ITWANSWITCH | [<switch_mode>[,<intvl>[,<num_ok>[,<link_mode>[,<disc_wait_time>[,<connect_wait_time>]]]]]] | Get or set values related to WAN switching |

## Parameters for AT commands for dual mode with cellular modem

| Parameter | Values | Meaning |
|---|---|---|
| <2g> | 0 = 2G Not allowed<br>1 = 2G Allowed | Only to be used with the "old" EXPLORER 540 LTE Modem (P/N 403715A-101/102).<br>Skip this parameter if you are using the new EXPLORER 540 Cellular Modem (P/N 403715A-00212/00214/00215) |
| <3g> | 0 = 3G Not allowed<br>1 = 3G Allowed | Only to be used with the "old" EXPLORER 540 LTE Modem (P/N 403715A-101/102).<br>Skip this parameter if you are using the new EXPLORER 540 Cellular Modem (P/N 403715A-00212/00214/00215) |
| <4g> | 0 = 4G Not allowed<br>1 = 4G Allowed | Only to be used with the "old" EXPLORER 540 LTE Modem (P/N 403715A-101/102).<br>Skip this parameter if you are using the new EXPLORER 540 Cellular Modem (P/N 403715A-00212/00214/00215) |
| <access tech> | AUTO<br>GSM   (Telit EU, Telit GLOBAL, Quectel)<br>UMTS  (Telit GLOBAL)<br>LTE     (Telit EU)<br>LTE-M  (Quectel)<br>NB-IOT (Quectel) | Select the technology to use. Note that the selected technology must be supported by the installed cellular modem.<br>If you select Auto, the EXPLORER 540 will select a technology based on the abilities of the installed modem. |
| <active> | 0: None / Unknown<br>1: BGAN<br>2: Cellular Modem<br>3: External Modem | Identifies which of the available connections are active. |
| <bgan> | 0: Unknown / Down<br>1: Up | Link status of the BGAN connection. |
| <boot_delay> | 0 (immediately) to 604800 seconds (7 days). | Boot delay period, time from loss of PRISM connection to a forced reboot. |
| <cell> | 0: Unknown / Down<br>1: Link up | Link status of the Cellular Modem connection. |
| <conn_delay> | 0 (immediately) to 86400 seconds (24 hours) | Connection delay period, time before initiating a new connect when connection to the PRISM server has failed. This value is only used if:<br>- Test ip is specified and the ping is successful<br>- No test IP is specified |
| <connect_wait_time> | 0 to 3600 seconds.<br>Value 0 indicates that the secondary link is connected immediately.<br>Default is 300 seconds. | Only applicable for link_mode = 0 (connected when needed).<br>Wait time for connecting the backup link after the primary link has been discovered to be down. |

| Parameter | Values | Meaning |
|---|---|---|
| <disc_wait_time> | 0 to 3600 seconds.<br><br>Value 0 indicates that the secondary link is disconnected immediately.<br><br>Default is 300 seconds. | Only applicable for link_mode = 0.<br><br>Wait time for disconnecting the backup link after the primary link has been discovered to be up. |
| <dns1> | DNS 1 IP address.<br><br>To delete the entry, enter address 0.0.0.0 | DNS address 1 (primary server) of the externally connected modem in dot-decimal notation. |
| <dns2> | DNS 2 IP address.<br><br>To delete the entry, enter address 0.0.0.0 | DNS address 2 (secondary server) of the externally connected modem in dot-decimal notation. |
| <ext> | 0: Unknown / Down<br>1: Link up | Link status of the External Modem connection. |
| <filename-url> | <filename-url> | Only applicable to QBG96 modem.<br><br>Type the URL from where the new firmware can be downloaded. |
| <intv> | For BGAN (<mode> = 0):<br>4 to 2678400 seconds (31 days).<br><br>For LTE (<mode> = 1): 3 to 2678400 seconds (31 days). | Ping interval in seconds. |
| <intv_fail> | 3 to 255 seconds | Ping interval after first failure. |
| <intvl> | 2 to 255 seconds.<br><br>Default 120 seconds. | Interval for pinging via primary connection to determine if it is up. |
| <ip> | <IP address>. | IP address of the externally connected modem in dot-decimal notation, or<br><br>IP address of the PRISM server.<br><br>To delete the entry, input 0.0.0.0. |
| <key> | <shared authentication key> | Shared authentication key used for identifying the terminal with the PRISM server. |
| <link_mode> | 0: Always connected (default)<br>1: Connected when needed | Determines whether or not the BGAN backup link is always up, or to be connected only when the primary link is considered down. |
| <manual> | 0 = Automatic operator<br>1 = Manual operator | Select 0 to use the operator from the SIM card<br><br>Select 1 to type in an operator manually (see <mcc> and <mnc>). |
| <max_fail> | 1 to 255 | Maximum number of failed ping attempts before declaring the link down. |
| <mcc> | 0-999 (if manual operator) | The Mobile Country Code |
| <mnc> | 0-999 (if manual operator) | The Mobile Network Code |
| <mode> | 0<br>1 | BGAN<br>LTE (Cellular) |

| Parameter | Values | Meaning |
|---|---|---|
| <n> | 1<br>2 | Server number 1 (Primary)<br>Server number 2 (secondary) |
| <num_ok> | 1 to 255<br>Default 10 ping replies | Number of successful ping replies needed in order to consider the primary link healthy. |
| <port> | <port number> | The port used to connect to the PRISM server.<br>The backup server (<n> = 2) has port number 6666 by default. |
| <signal strength> | 0   = -113 dBm or less<br>1   = -111 dBm<br>2...30 = -109 to -53 dBm<br>31   = -51 dBm or greater<br>99   = not known or not detectable | Shows the signal strength of the cellular connection. |
| <switch_mode> | 0: Switch immediately<br>1: Only switch when link is inactive (default) | Determines if a switch to the primary connection is allowed while there is traffic on the backup link. (cutoff point is at 5kb within 2 minutes).<br>The switch is delayed no more than 30 minutes. |
| <test_ip> | <IP address for PRISM test> | PRISM test IP address. Used to test whether BGAN or LTE has IP connectivity.<br>Starts after LTE/BGAN is up simultaneously with server connect attempts.<br>Uses 3 pings with 10 seconds between them.<br>Default value is no ip address.<br>To clear a previously defined entry, use value 0.0.0.0 |

# BGAN non-M2M functions

This appendix includes the features and functions in the EXPLORER 540 that are **not** available with an M2M subscription, but only with a BGAN Class 2 subscription.
These functions are:

- Streaming
- VoIP

## C.1 To control data connections from web interface (BGAN)

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

Note ▶ | If you are using the EXPLORER 540 Cellular Modem you cannot start and stop data connections.

The difference from the M2M version is, that Streaming connections are supported and can be configured.

### C.1.1 To start and stop data connections

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

To start and stop data connections on your EXPLORER 540, do as follows:

1. In the opening page, locate the connection package you want to start.
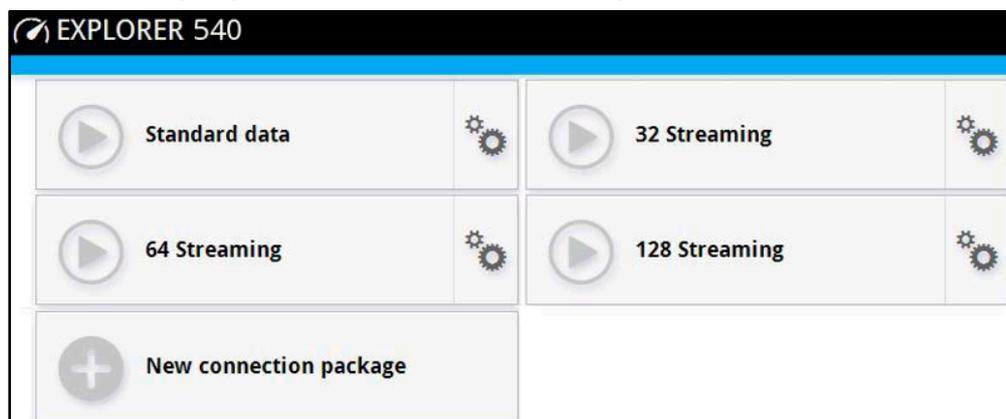
2. Click ▶ to start the connection. If more connections are included in the connection package, this will start all included connections. The connections icon at the bottom of the page shows ⚡¹ when a BGAN data connection package is running.

> **Note** | Once a Streaming connection is started, the connection will run until you stop it. You will be charged for the time you are connected.

3. Click ■ to stop the connection.

If data is temporarily suspended, e.g. due to a blockage, the icon on the active connection turns yellow in stead of green, and the **Status** field shows **Data suspended**.

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 4-14.

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: For Streaming data, the tile shows the total time the connection has been active.
- Bit rate: For Streaming connections, the tile shows the fixed bit rate.

## C.1.2 Default data connection types

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.<br><br>The user pays for the amount of data sent and received. |
| **Streaming data**<br><br>The following Streaming classes are available:<br><br>32, 64, or 128 Streaming | 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.<br><br>The user pays for the duration of the connection.<br><br>**Note that Streaming is not available in M2M subscriptions.** |

You can use these connections as they are or build your own connection packages. For set up of the connection packages, see the next section.

## C.2    To set up data connections

### C.2.1    To create a new connection package

Do as follows:

1. Click **New connection package**.
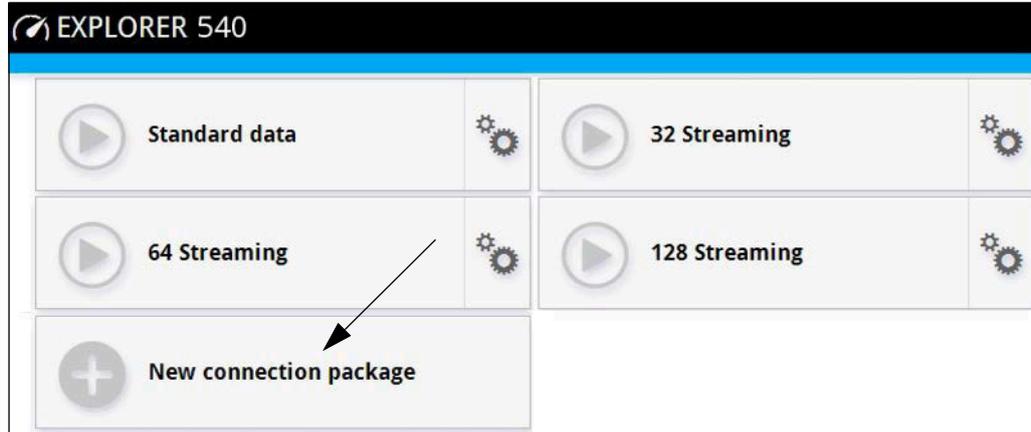


2. Type a **Name** for the new package.
3. If you want to create dedicated connections, select the **Type**. For details on dedicated connections, see *To set up dedicated connections* on page 4-9.
4.  Click **Save**
5. Click **Click here to create connections**.
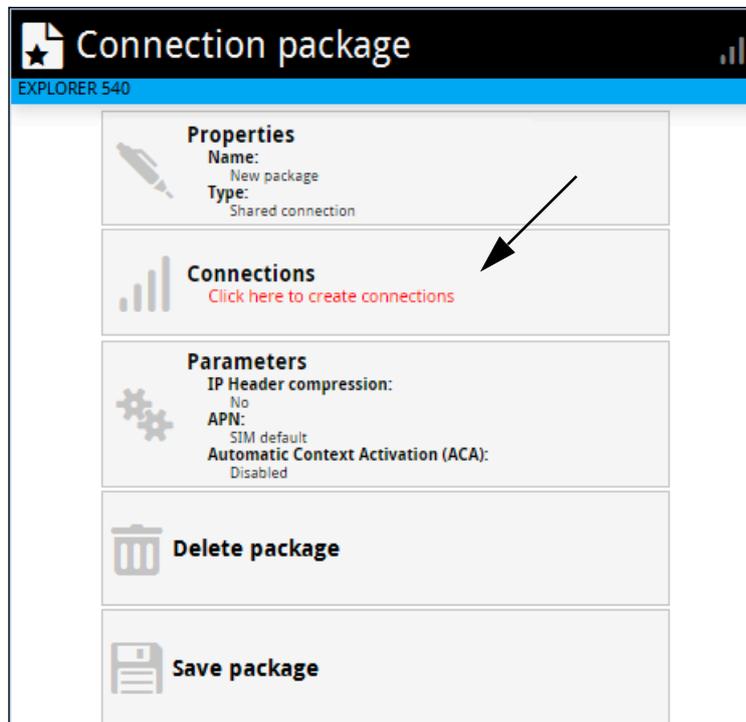


6. Select the connection type you want for your new connection package.
   You can select Standard, Streaming 32 kbps, Streaming 64 kbps or Streaming 128 kbps.
7. Click **Save package**.

The new package should now appear as a new tile on the startup page.

For details on **Parameters** (APN, Automatic Context Activation (ACA) and IP Header compression) see *To change the APN for a connection package* on page 4-6 and *Automatic Context Activation (ACA)* on page 4-7.

# C.3    To make phone calls over BGAN (not M2M version)

> **Note** Phone calls are only possible if the airtime subscription is a BGAN class 2 subscription, **not M2M**.

## C.3.1    To connect a VoIP phone

Your VoIP phone can be set up to make and receive calls over the BGAN network, using the terminal's phone number.

> **Note** Make sure your VoIP phone has an integrated SIP client. The EXPLORER 540 has an integrated SIP server.

### To connect your phone for making calls

> **Note** If you are using a Thrane IP Handset and have enabled support for it, no initial configuration is necessary.

For details on initial setup of your VoIP phone and the EXPLORER 540, see

- The documentation for your handset
- *First time SIP setup* on page C-5
- *To manage VoIP phones* on page C-7

**To connect a VoIP phone, do as follows:**

1. Start up the EXPLORER 540 terminal.

2. Connect your phone via a router/switch to the LAN interface on the EXPLORER 540[1].

When the VoIP phone is powered and ready, you are able to make and receive calls over BGAN.

---

1. Since there is only the one LAN interface and the EXPLORER 540 cannot provide power, you must connect the phone(s) via external equipment such as a router (wired or wireless) or a switch.

## First time SIP setup

If it is the first time you connect your phone to the EXPLORER 540 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. You may be asked to enter some of the following details:

- SIP server address and port: Default address: 192.168.0.1, Port: 5060
- User name: Local number in EXPLORER 540 (0501 to 0516)
- Password: Default same as user name
- Codec priority: Highest priority codec type: G.711

> **Note** The user name and password must match the IP handset settings in the EXPLORER 540. See *To manage VoIP phones* on page C-7.

## C.3.2    Call types

### Definition

The phone connection can be a **Standard voice** connection or a **3.1 kHz audio** connection.

- For **outgoing calls**, the call type is **Standard voice** by default.
  You can change the call type for your call to 3.1 kHz audio by dialing **2\*** before the number.

  **Example:**    2\*004539558800

- For incoming calls, you can set up in the web interface (IP handset page) which call types you want to receive on your IP handset. Only the call types selected for an IP handset are received. By default all, call types are accepted.

When receiving calls, the mobile number determines which call type is used. In your airtime subscription you have one number for 3.1 kHz audio and one number for Standard voice. Remember that the call is only received on your phone if the call type used is selected for that phone (called IP handset in the web interface).

For information on how to set up the call types in the web interface, see *To manage VoIP phones* on page C-7.

## C.3.3    To make or receive a phone call with EXPLORER 540

Connect your IP handset as described in *To connect a VoIP phone* on page C-4.

### To make a call from the EXPLORER 540

To make a call, dial **00 <country code> <phone number>** followed by off-hook key.

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

If there was an error establishing the connection, the web interface of the EXPLORER 540 shows an error message.

### To receive a call

By default, all phones connected to the EXPLORER 540 will ring when one of the mobile numbers is called. Note however, that this depends on the call type settings. See *Call types* on page C-5.

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 EXPLORER 540

To make a call to a phone connected to the EXPLORER 540, 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**. The first part of the mobile number is always 870, which is the "country code" for the BGAN system. For information on the mobile numbers, refer to your airtime subscription.

> **Note** | There are two mobile numbers, one for **3.1 kHz audio** and one for **Standard voice**.

## C.3.4 Local numbers and special functions

### Overview

There are a number of local numbers and dialing functions available in the EXPLORER 540.

The following list shows the allocated local numbers and special-purpose numbers for the EXPLORER 540.

| Number | Function |
|---|---|
| 0 followed by one of the numbers 501-516 and off-hook key | Local call to one IP handset. |
| 0900 followed by off-hook key | Local call broadcast to all connected phones. |

Apart from the numbers above, the EXPLORER 540 uses the following dialing prefixes:

- **1\*** before the phone number will force the connection to use **Standard voice**.
- **2\*** before the phone number will force the connection to use **3.1 kHz audio**.
- **#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.

# C.4 To manage VoIP phones

## C.4.1 Overview

This section describes how to manage VoIP phones connected to the EXPLORER 540.

The terminal supports connection of up to 16 phones through the LAN interface. Each phone must have a local number in the range 0501 to 0516 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 interface, see *To connect a VoIP phone* on page C-4.

## C.4.2 To manage VoIP phones in your EXPLORER 540

Do as follows:

1. Connect your VoIP phone via a router/switch to the LAN interface. For details, see *To connect a VoIP phone* on page C-4.
2. In the web interface, select ✿ (Control panel) **> IP handsets**.
3. Click the tile for the handset number you want to manage.
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 number.
6. Set the call type for incoming calls.
   You can select **Standard voice** or **3.1 kHz audio** or both.
   - If you select both, the handset will react (ring) on incoming calls.
   - If you select e.g. Standard voice, the handset will only react on calls made to the Standard voice phone number.
7. Select the **Preferred outgoing call type**.
   The selected type will be used by default, if possible, for any outgoing call from this handset.
8. Click **Save**.
9. In the  IP handset, enter the local number and the password you just entered in the EXPLORER 540. See the documentation for your handset for details.

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

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

## C.4.3    To enable the use of Thrane IP Handset

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



2. Locate the field Thrane IP Handset support.
3. If you want the terminal to support BGAN profile and menu in Thrane IP Handsets, select Support BGAN profile and menu in Thrane IP Handsets.
This means that, in addition to making calls with the Thrane IP Handset over the BGAN network, you can use the handset display and keypad to:
   • Enter PIN/PUK for the terminal.
   • View pending alarms.
   • View event log.
   • View current satellite status and signal strength.
   • Start/stop connection packages.

   For details, see *To manage VoIP phones in your EXPLORER 540* on page C-7 and the user manual for the Thrane IP Handset.

4. Click **Save**.

# Conformity

## D.1 CE

The EXPLORER 540 is CE certified as stated in the EU Declaration of Conformity enclosed in electronic copy at the end of this appendix.

## D.2 IC

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:
(1) this device may not cause interference, and
(2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :
(1) l'appareil ne doit pas produire de brouillage, et
(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

This Class [B] digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada.

## D.3 FCC

**Note**: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

NOTICE:
This device complies with Part 15 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.

## D.4    Japanese Radio Law and Japanese Telecommunications Business Law Compliance.

This device is granted pursuant to the Japanese Radio Law (電波法)
and the Japanese Telecommunications Business Law (電気通信事業法).

This device should not be modified (otherwise the granted designation number will become invalid).

# EU Declaration of Conformity

Hereby **Thrane & Thrane A/S trading as Cobham Satcom** declares that the following equipment complies with the specifications of:

**RED directive 2014/53/EU** concerning Radio Equipment

**Equipment included in this declaration**

| Model | Description | Part no. |
|-------|-------------|----------|
| TT-3715A | EXPLORER 540 Terminal C1D2 | 403715A-555 |
| TT-3715A | EXPLORER 540 Terminal C1D2 | 403715A-556 |

The full text of the EU declaration of conformity is available at the following internet address:

https://partnerportal.cobhamsatcom.com/eshop/downloads

Document no.: 99-157451-E

Thrane & Thrane A/S trading as Cobham Satcom. Registered no.: DK - 65 72 46 18. Registered address: Lundtoftegaardsvej 93 D, 2800 Kgs. Lyngby, Denmark.

**www.cobham-satcom.com**

# Glossary

## A

| | |
|---|---|
| ACA | Automatic Context Activation. |
| AMBE | Advanced Multi-Band Excitation. A speech coding standard. |
| APN | Access Point Name. The Access Point Name is used by the terminal operator to establish the connection to the required destination network. |
| AT commands | A command set used for controlling modems. |

## B

| | |
|---|---|
| BeiDou | Chinese satellite navigation system. |
| BGAN | Broadband Global Area Network. A satellite network based on geostationary satellites, delivering broadband data and telephony to virtually any part of the earth, with full UMTS. |

## C

| | |
|---|---|
| C1D2 | Class 1 Division 2 (C1D2) is a certification issued to a specific product that allows it to be used in potentially hazardous environments. |
| CE | Conformité Européenne. This term signifies that a CE certified product conforms to European health, environmental, and safety regulations. In short, it makes the product legal to be sold in the European Union. |
| CS | Circuit Switched. Circuit-switched networks require dedicated point-to-point connections during calls. |

## D

| | |
|---|---|
| DHCP | Dynamic Host Configuration Protocol. A protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. |
| Dual mode | A mode where the EXPLORER 540 is used with 2 WAN networks - cellular network as primary connection and BGAN satellite network as backup. |

## E

| | |
|---|---|
| ECEF | The Earth-Centered Earth-Fixed or conventional terrestrial coordinate system rotates with the Earth and has its origin at the center of the Earth. The X axis passes through the equator at the prime meridian. The Z axis passes through the north pole but it does not exactly coincide with the instantaneous Earth rotational axis. The Y axis can be determined by the right-hand rule to be passing through the equator at 90 degrees longitude. |
| EIRP | Effective Isotropically-Radiated Power. The amount of power that would have to be emitted by an isotropic antenna (that evenly distributes power in all directions) to produce the peak power density observed in the direction of maximum antenna gain. |

## F

| | |
|---|---|
| FCC | Federal Communications Commission. An independent agency of the United States government, created by Congressional statute to regulate interstate communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia and U.S. |

territories. The FCC works towards six goals in the areas of broadband, competition, the spectrum, the media, public safety and homeland security.

FTP      File Transfer Protocol. A standard network protocol used to transfer computer files between a client and server on a computer network.

FUP      Firmware Upgrade Process.

## G

GLONASS      GLObal'naya NAvigatsionnaya Sputnikovaya Sistema. Global Navigation Satellite System in English.

GMPCS      Global Mobile Personal Communications Services.

GNSS      Global Navigation Satellite System. A satellite navigation system with global coverage. Examples are GPS, GLONASS or BeiDou.

GPS      Global Positioning System. A system of satellites, computers, and receivers that is able to determine the latitude and longitude of a receiver on Earth by calculating the time difference for signals from different satellites to reach the receiver.

## H

HTTP      HyperText Transfer Protocol. HTTP is the underlying protocol used by the World Wide Web and 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

I/O      Input/Output.

IC      Industry Canada (French: Industrie Canada) is the department of the Government of Canada with a mandate of fostering a growing, competitive, knowledge-based Canadian economy.

ICMP      Internet Control Message Protocol. An Internet protocol mostly used for diagnostics.

IEEE      Institute of Electrical and Electronics Engineers. IEEE is a nonprofit organization and the world's leading professional association for the advancement of technology.

IMEI      International Mobile Equipment Identity. A unique number identifying your terminal.

IMSI      International Mobile Subscriber Identity. A unique number used to identify a mobile subscriber on a wireless network.

IMSO      International Maritime Satellite Organisation. An intergovernmental body established to ensure that Inmarsat continues to meet its public service obligations, including obligations relating to the GMDSS.

IP      Ingress Protection. An international classification system for the sealing effectiveness of enclosures of electrical equipment against the intrusion into the equipment of foreign bodies (i.e. tools, dust, fingers) and moisture. This classification system uses the letters "IP" followed by two numbers classifying the equipment with regards to foreign bodies and moisture respectively.

| | |
|---|---|
| IP | Internet Protocol. |

## K

| | |
|---|---|
| kbps | kilobits per second. |

## L

| | |
|---|---|
| LAN | Local Area Network. A computer network covering a small physical area, like a home, office, school or airport. The defining characteristics of LANs, in contrast to wide-area networks (WANs), include their usually higher data-transfer rates, smaller geographic area, and lack of a need for leased telecommunication lines. |
| LED | Light Emitting Diode. |
| LTE-M | LTE-Machine type communication. A type of low power wide area network (LPWAN) radio technology standard developed by 3GPP to enable a wide range of cellular devices and services (specifically, for machine-to-machine and Internet of Things applications). The advantage of LTE-M over NB-IoT is its comparatively higher data rate, mobility, and voice over the network, but it requires more bandwidth and is more costly. |

## M

| | |
|---|---|
| M2M | Machine-to-Machine. Direct communication between unmanned devices using any communications channel, including wired and wireless. |
| MAC | Media Access Control address. A hardware address that uniquely identifies each node of a network. |
| MCC | Mobile Country Code. An MCC consists of 3 decimal digits and is used in combination with an MNC (a combination known as an "MCC/MNC tuple") to uniquely identify a mobile network operator (carrier) using the GSM (including GSM-R), UMTS, LTE, and 5G public land mobile networks. |
| MNC | Mobile Network Code |

## 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. |
| NB-IoT | NarrowBand Internet of Things. A Low Power Wide Area Network (LPWAN) radio technology standard developed by 3GPP. NB-IoT focuses specifically on indoor coverage, low cost, long battery life, and high connection density. |
| NC | Normally-closed (NC) contacts disconnect the circuit when the relay is activated, the circuit is connected when the relay is inactive. |
| NO | Normally-open (NO) contacts connect the circuit when the relay is activated, the circuit is disconnected when the relay is inactive. |

## O

| | |
|---|---|
| OS | Operating System. |
| OSHA | Occupational Safety and Health Act. The primary federal law which governs occupational health and safety in the private sector and federal government in the United States. Its main goal is to ensure that employers provide employees with an environment free from recognized hazards, such as exposure to toxic chemicals, excessive noise levels, |

mechanical dangers, heat or cold stress, or unsanitary conditions.

## P

PDP        Packet Data Protocol. A network protocol used by external packet data networks that communicate with a GPRS network (such as the BGAN network).

PIN         Personal Identification Number. A code number used to provide access to a system that has restricted access.

ping        Packet Internet or Inter-Network Groper. A basic Internet program that allows a user to test and verify if a particular destination IP address exists and can accept requests in computer network administration.

PoE        Power over Ethernet. A standard for combining power supply with transmission of data over the Ethernet. The source unit "injects" power into the Ethernet cable and the power is "picked up" at the connected device.

PPPoE     Point-to-Point Protocol over Ethernet. A network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. By using PPPoE, users can virtually "dial" from one machine to another over an Ethernet network, establish a point to point connection between them and then securely transport data packets over the connection.

PRISM     Private Routing & Intelligent System Management. A technology used for dual mode with cellular and BGAN network to obtain seamless and transparent data transfer independent of the network used (Cellular or BGAN backup connection).

## R

RCM       Regulatory Compliance Mark. The RCM is a symbol signifying that a supplier has taken the necessary steps to have the product comply with the electrical safety and/or electromagnetic compatibility (EMC) legislative requirements of Australia and New Zealand.

RF          Radio Frequency. Electromagnetic wave frequencies between about 3 kHz and about 300 GHz including the frequencies used for communications signals (radio, television, cell-phone and satellite transmissions) or radar signals.

RHCP      Right-Hand Circular Polarization.

## S

SIM        Subscriber Identity Module. The SIM provides secure storing of the key identifying a mobile phone service subscriber but also subscription information, preferences and storage of text messages.

SIP         Session Initiation Protocol. An application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. Used e.g. for Internet telephony.

SMS       Short Message Service.

SPDT      Single Pole Double Throw. A type of relay or switch where a common terminal connects to either of two others. Including two for the coil, such a relay has five terminals in total.

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.

STP        Shielded Twisted Pair.

## T

TCP/IP        The basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet).

TE            Terminal Equipment - the equipment connected locally to the EXPLORER 540.

TLS           Transport Layer Security. An updated, more secure, version of SSL.

## U

USB           Universal Serial Bus. A specification to establish communication between devices and a host controller (usually personal computers). USB is intended to replace many varieties of serial and parallel ports. USB can connect computer peripherals such as mice, keyboards, digital cameras, printers, personal media players, flash drives, and external hard drives.

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.

UTP           Unshielded Twisted Pair.

UV            UltraViolet.

## V

VoIP          Voice Over IP. The routing of voice conversations over the Internet or through an IP-based network.

## W

WAN           Wide Area Network. A telecommunications network or computer network that extends over a large geographical distance. In this manual, WAN is the external network via BGAN or cellular connection.

# Index