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

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

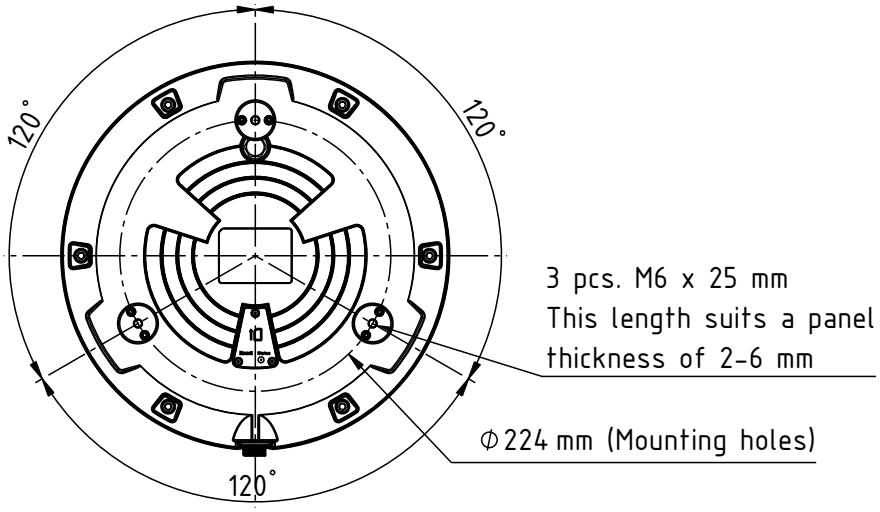
To mount the terminal, do as follows:

1. Use the already mounted plastic spacers or use similar mounting plates of 10 mm height. See the drawing below.

Important Do not mount the terminal without the spacers! If you mount the E323 directly on a roof without the spacers, this will have a significant negative impact on antenna performance.

Also, free airflow under the terminal is necessary for the ventilation hole in the bottom of the terminal not to be blocked and to prevent over-heating.

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



3. Drill the 3 holes in the roof according to the previous step.
4. Mount the terminal with the spacers/mounting plates using the 3 included M6 bolts and washers. If the mounting plates are less than 10 mm thick, use spacers to obtain a distance of 10 mm between the roof and the terminal bottom. This is to ensure that the ventilation hole in the bottom of the terminal is not blocked, and to ensure free airflow under the terminal to prevent over-heating.

   Important The bolts must never penetrate more than 10 mm into the bushings in the terminal!

5. Connect the cable from the terminal to power and LAN equipment (if used).
   Refer to *To connect cables* on page 11.

Magnetic Mount Solution (optional)

Overview

We recommend mounting the terminal with bolts through the roof instead of using magnets. However, a Magnetic Mount Solution for use in temporary installations is available from Cobham SATCOM (order number 403723A-009).

The Magnetic Mount Solution consists of 3 individual high intensity magnets with rubber coating. You can place the EXPLORER 323 directly on the roof of the vehicle using these magnets.

To install the terminal with the Magnetic Mount Solution

To mount the magnets on the EXPLORER 323, do as follows:

1. Remove the 3 external plastic spacers and mount the magnetic feet in the 3 threaded holes as described in the installation guide included with the Magnetic Mount Solution.

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

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

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

5. Connect the cable from the terminal to power and LAN equipment (if used).
   Refer to *To connect cables* on page 11.

To detach the terminal

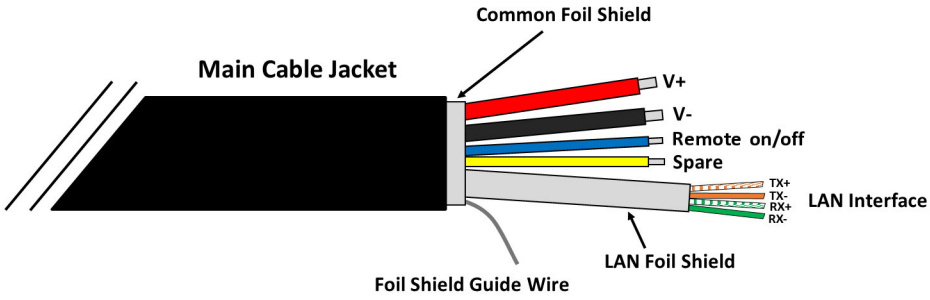
Grab the terminal near one of the magnets and lift it. When one magnet is off, the other two are easier to detach.

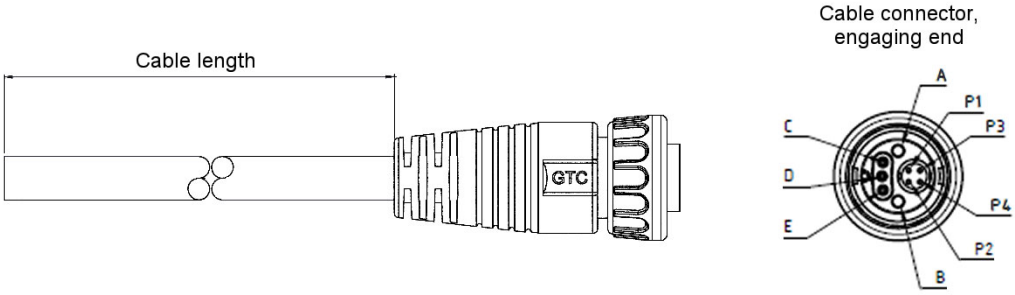
To connect cables

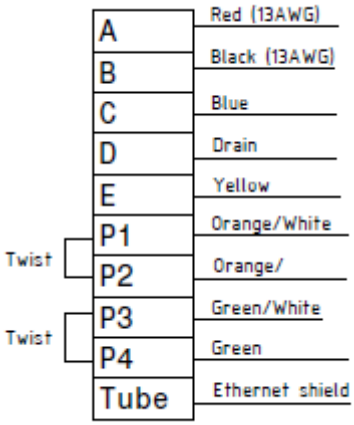
Included cable

A combined cable for connection to power supply and Ethernet equipment comes with the system. If you need a longer cable, a 15 meter cable is also available.

Important The 15 m cable **requires 24 V operation!**







Pin	Function	Wire color
A	V+	Red
B	V-	Black
C	Remote on/off	Blue
D	Foil shield guide wire	Metal
E	Spare	Yellow
P1	TX+	Orange/ White
P2	TX-	Orange
P3	RX+	Green/ White
P4	RX-	Green

1. Connect the cable to the circular connector on the EXPLORER 323.
2. Connect the other end of the cable as described in the following sections.

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

To connect power

We recommend to use the included 6 m combined cable. If you want a longer cable, you can use the 15 meter cable available from Cobham SATCOM (only for 24 V operation!).

Note If you are using the EXPLORER Mobile Gateway, all connections are made via the EXPLORER Connection Box. See *PTT connection example* on page 15.

Important When used **without** the EXPLORER Mobile Gateway, the **Remote on/off function is disabled by default** in the EXPLORER 323. This means that when you have connected the EXPLORER 323 to the battery power of the vehicle, the EXPLORER 323 is always on, and **can potentially drain the battery**!

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

Note Do not use the cigarette lighter socket in the vehicle to supply power for the EXPLORER 323. Connect directly to the 12 or 24 V supply instead.

Connect the wires from the combined cable as follows:

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

To connect Ignition

You can use the Ignition system of the vehicle to switch the EXPLORER 323 on and off.

Do as follows:

1. Connect the power wires from the included cable to positive (+, thick red wire) and negative (-, thick black wire) in the vehicle as described above.
2. Connect the blue wire from the cable (pin C in the connector) to the ignition signal of the vehicle.
   Refer to the vehicle manual for information on where and how to connect to the Ignition signal in your vehicle.
3. If you have connected via the EXPLORER Mobile Gateway, the Remote on/off function may be automatically enabled, and you can go straight to step 7.
   If you are **not** using a EXPLORER Mobile Gateway, you can use the web interface to enable the Remote on/off function as described in the next steps.

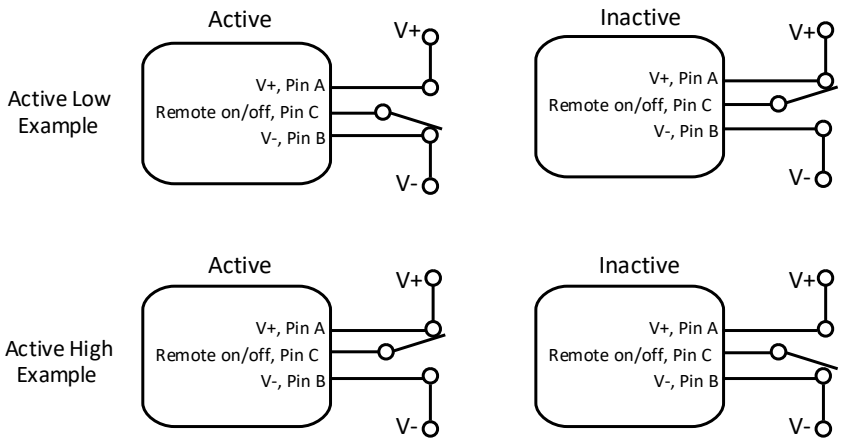
4. Connect a computer, either with the Ethernet interface as described in the next section, or via WLAN as described in *To connect your WLAN-enabled device* on page 19.
5. On the connected computer, open your browser and access the web interface by typing the local IP address in the address bar (default IP address: 192.168.0.1).
6. Select **Advanced > Power control** and enable the **Remote on/off** function as described in *Power save* on page 90.
7. Verify the Remote on/off function by starting and stopping the ignition of the vehicle and observing the EXPLORER 323 switching on and off.

The Power control pin (Remote on/off signal)

The Power control pin is connected to the blue Remote on/off wire in the EXPLORER 323 cable. See *To connect Ignition* on page 12.

Connection example for the Power control pin:

Important The Power control pin, pin C in the EXPLORER 323 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.

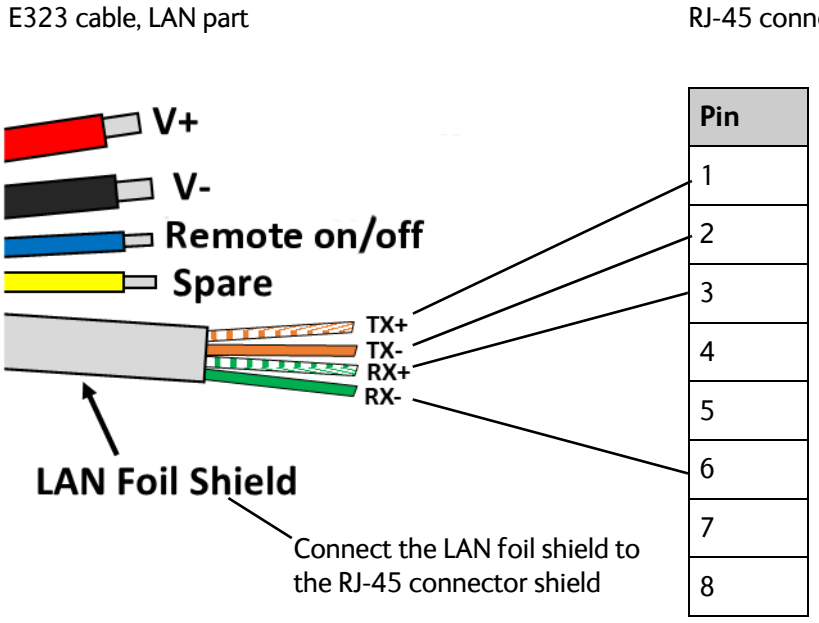


- If you have configured the input to be Active low (default):
  To deactivate: Connect the Power control pin (blue wire) to V+ (*High: 2.8 - 32 VDC*).
  To activate: Connect the Power control pin (blue wire) to GND (*Low: 0 - 0.8 VDC*).
- If you have configured the input to be Active high:
  To deactivate: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

To connect Ethernet

Depending on your configuration, you can connect the Ethernet wires from the combined cable to a switch, an EXPLORER Mobile Gateway or directly to a PC (using an RJ-45 connector). Connect the Ethernet wires as follows:

1. Connect the wires 1, 2, 3 and 4 from the EXPLORER 323 cable according to the pinout shown in the previous section *Included cable* on page 11.
   If you prefer to mount an RJ-45 connector, connect the wires as shown below.



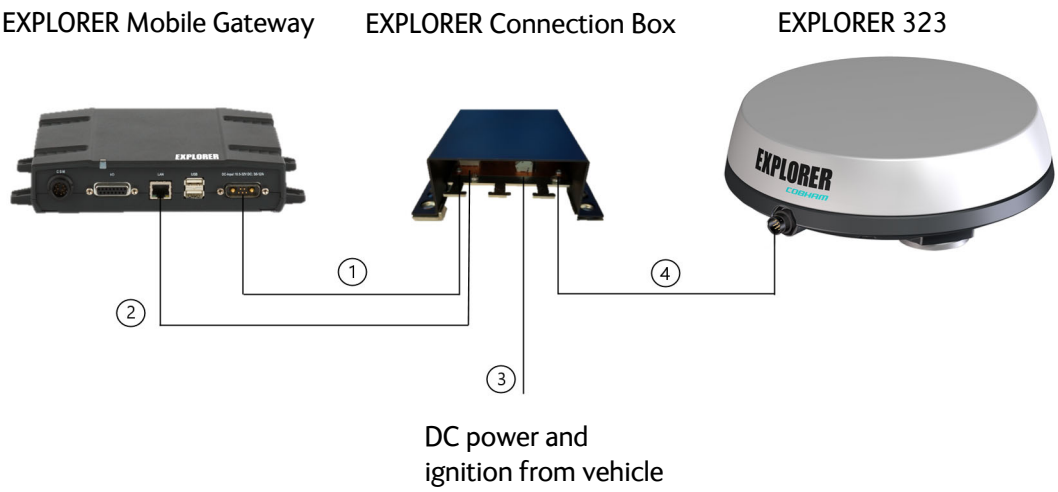
2. For further details on how to connect the LAN interface, see *To connect to the LAN interface* on page 18.

PTT connection example

You can use the EXPLORER 323 with the EXPLORER Mobile Gateway[1].

In the PTT solution, you connect the EXPLORER 323 to the EXPLORER Mobile Gateway through the EXPLORER Connection Box as shown below.

Note If you are using the EXPLORER Mobile Gateway with the EXPLORER 323, the Remote on/off function will automatically be enabled. This means that the EXPLORER 323 will normally be in power save state when the ignition is off. See *Power mode functions* on page 34.



Number	Description	Cable
1	Power	Supplied with EXPLORER Mobile Gateway
2	Ethernet	Supplied with EXPLORER Mobile Gateway
3	DC power and Ignition from vehicle	Not supplied
4	Combined power and Ethernet	Supplied with EXPLORER 323

For pinout and information on how to connect the units, see the Connections section in the installation guide included with the EXPLORER Connection Box.

1. The EXPLORER Mobile Gateway is an IP-based communications device that supports integration of satellite/LTE/3G/LAN backhaul and Land Mobile Radio.

To get started

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

- *Before you start*
- *To insert the SIM card*
- *To switch on the EXPLORER 323*
- *To connect your WLAN-enabled device*
- *To connect to the LAN interface*
- *To enter the SIM PIN for the terminal*
- *To register with the BGAN network*
- *To make phone calls over BGAN*

Before you start

Operation at high temperatures

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

Connector

There is only one connector on the terminal, placed on the side of the terminal. This connector is used for both DC power and Ethernet. A dedicated cable is included with the terminal. For details, see *To connect cables* on page 11.

SIM card

The EXPLORER 323 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 323 is operating as an M2M terminal or as a BGAN class 12 terminal.

To switch on the EXPLORER 323

To use the ignition system

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

When the ignition is switched off the terminal is in power save state, unless other conditions keep the EXPLORER 323 from going into power save state. see *Power mode functions* on page 34. For information on how to connect Ignition to the EXPLORER 323 cable, refer to *To connect Ignition* on page 12.

If you are not using the EXPLORER Mobile Gateway, you must enable the Remote on/off function in the web interface. For further information, see *Power save* on page 90.

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

To use a remote on/off switch

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

Power up completed

When the terminal is switched on and ready, the LED in the bottom of the terminal lights steady green.

If the LED is flashing green it has started up but is not yet ready to communicate on the network. You can access the terminal settings, but the terminal is not ready to make calls or running data sessions until the system is registered on the BGAN network. You may have to enter a SIM PIN before the system can register. For further information, see *To enter the SIM PIN in the web interface* on page 99.

To connect to the LAN interface

There is only one wired LAN interface in the EXPLORER 323, so you may want to connect a switch in order to connect more devices. If you want to use a wired VoIP/SIP handset you may need to connect to a PoE switch for power; the EXPLORER 323 LAN interface **does not supply PoE**.

Before you connect to the LAN interface

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

To connect a computer to the LAN interface

Note This section only describes a Standard Internet connection with default settings on the terminal. For information on other scenarios, see *To control data connections from web interface* on page 47.

To connect a computer to the LAN interface, do as follows:

1. Power up your computer.
2. Connect your LAN cable between the network connector on your computer and the LAN interface from the terminal (or a switch connected to the terminal).
   For details on the physical LAN interface, see *To connect Ethernet* on page 14.
3. When the computer and the terminal are ready and the terminal is registered on the BGAN network, you can start a data connection, e.g. from the web interface. See *To start and stop data connections* on page 24.
4. When you have started a data connection, you are ready to access the Internet over the BGAN Standard data connection.

For information on how to configure the LAN interface on the terminal, see *LAN interface setup* on page 65, *Terminal settings* on page 61 and *Advanced LAN* on page 68.

To connect your WLAN-enabled device

Prepare the WLAN interface

The WLAN interface is disabled by default, so you must first access the EXPLORER 323 using the LAN interface and then enable the WLAN interface in the web interface. Do as follows:

1. Connect a computer to the LAN interface as described in the previous section.
2. Open your browser and access the web interface as described in *To access the web interface* on page 20.
3. Click from the bottom right corner of the web interface to access the Control panel.

1. Click the W**LAN** icon at the top of the page.
2. To enable the WLAN interface, select **Enable**.
   For details on WLAN configuration, see *WLAN interface setup* on page 65.

Connect your device

1. Switch on the EXPLORER 323.
2. Place your WLAN-enabled device (computer, tablet or smartphone) close to the EXPLORER 323.
3. On your device, search for available WLAN networks.
4. Select the EXPLORER 323 WLAN access point when it appears in your list of available wireless networks.
   The default name is **EXPLORER323**.

Note You must enter a password. By default the password is the serial number[a] of your EXPLORER 323 and the encoding type is **WPA2-AES**.

a. You find the serial number on the label on the bottom side of the EXPLORER 323.

Your device is now connected to the EXPLORER 323. In the web interface, the WLAN icon shows the number of devices connected to the EXPLORER 323 via WLAN. Example: 2

For information on how to configure the WLAN interface in the EXPLORER 323, see *WLAN interface setup* on page 65.

For information on how to set up the LAN network, see *Terminal settings* on page 61 and *Advanced LAN* on page 68.

The EXPLORER Connect app

If you want to use your smartphone with the EXPLORER 323, install the **EXPLORER Connect** app, which is available for iPhone at the App Store and for Android phones at Google Play. The EXPLORER Connect app provides the following options from the main menu:

Tile	Function
Satellite Phone	Use your smartphone as a satellite phone when connected to the EXPLORER 323. **Not available with M2M subscription**
Terminal Access	Start and stop data connections and access all settings of the EXPLORER 323
Pointing	**Not applicable to the EXPLORER 323**
Dashboard	See the terminal and connection status

To access the **EXPLORER Connect** app, connect your smartphone to the WLAN access point of the EXPLORER 323 as described in *To connect your WLAN-enabled device* on page 19, and start the **EXPLORER Connect** app. To access the configuration settings select **Terminal Access**. From this point you have access to the same settings as from the web interface.

Note If you get a message saying Network Unavailable or Connection error it means you are not connected to the EXPLORER 323. Check the connection and setup of your WLAN.

To access the web interface

You can use the built-in web interface for configuration and operation of the EXPLORER 323. To access the web interface, do as follows:

1. Start up the terminal.
   For details, see *To switch on the EXPLORER 323* on page 17.
2. Connect your computer or smartphone to the terminal, using LAN or WLAN as described in the previous sections.
3. Open your browser and enter the IP address of the terminal in the address bar. The default IP address of the terminal is 192.168.0.1.
4. Enter user name and password. You can log in as user or as administrator.
   - Default for **user**: User id = user, Password = <serial number of the EXPLORER 323>
   - Default for **administrator**: User id = administrator, Password = admin

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

If the terminal is waiting for a PIN, the web interface will start up on the page where you enter the pin. Otherwise it will start up on the dashboard. For more information on the web interface, see *The web interface* on page 44.

To enter the SIM PIN for the terminal

Do you need a SIM PIN?

Important If your EXPLORER 323 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 81.
  With this option enabled, the EXPLORER 323 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 80.
  When the SIM PIN is disabled, the SIM can be used by other terminals without a PIN.

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

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

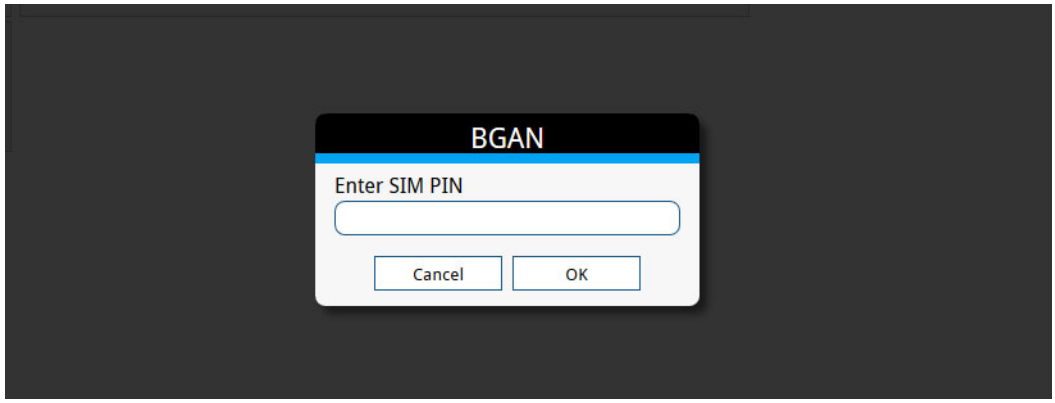
For information on how to connect your computer, see *To connect a computer to the LAN interface* on page 18 or *To connect your WLAN-enabled device* on page 19

To enter the SIM PIN using the web interface

To enter the SIM PIN

Do as follows:

1. On a computer connected to the terminal, open your browser and enter the IP address of the terminal in the address bar (default IP address: **http://192.168.0.1**).
   If your SIM card uses a PIN and the PIN has not yet been entered, the web interface will open with an **Enter SIM PIN** popup.



2. Type in the PIN and click **OK**.

When the PIN is accepted, the web interface opens the Dashboard and is ready for use. If the PIN is not accepted, see the next section *Wrong PIN*.

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

Wrong PIN

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

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

To register with the BGAN network

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

When the SIM PIN is accepted by the terminal, the EXPLORER 323 System automatically starts the registration procedure on the BGAN network.

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

The normal startup procedure is shown as follows:

1. **Searching**. The terminal has instructed the antenna to search for the BGAN signal.
2. **Registering**. The terminal is attempting to register with the Satellite Access Station (SAS).
3. **Ready**. The terminal has registered and attached to the SAS and is ready to accept a service request (a call or a data session).

Note that the registration procedure may take several minutes.

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

When the system is ready, the **Antenna status** field shows **Tracking** or **Pointed** and the **Status** field shows **Ready** (unless a call or data session is active).

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

Note The EXPLORER 323 needs information on its mounting orientation in relation to the vehicle. To obtain or verify this information it runs a calibration or validation process when moving after restart. For details, see the next section, *Mounting calibration*.

Mounting calibration

Every time you start up the EXPLORER 323 and move the vehicle, the EXPLORER 323 will try to detect how it is oriented in relation to the vehicle (Mounting calibration). This is necessary in order to obtain and maintain the best possible signal strength when the vehicle is moving.

After a restart, the EXPLORER 323 will run a calibration process, which may take a couple of minutes.

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

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

Status of the mounting calibration

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

- **Calibrating**: Shown after first installation or factory reset. The EXPLORER 323 runs a complete calibration process and goes directly to status **Completed** when done. When moving in this state the terminal is **not** able to track the satellite.
- **Validating**: Shown after restart of the EXPLORER 323. The EXPLORER 323 validates the mounting information from previous startup and goes directly to status **Completed** when done. When moving in this state the terminal will attempt to track the satellite using the previous mounting information.
- **Completed**: Shown when the calibration (or validation) process has finished. The EXPLORER 323 now has the correct information of its mounting orientation in relation to the vehicle and is able to track the satellite while moving.

To start and stop data connections

By default, you have to start a data connection manually when the terminal is ready and connected to the BGAN network. However, you can enable automatic activation of a data connection. See *Internet and LAN connection modes* on page 62.

To start and stop data connections on your EXPLORER 323, do as follows:

1. On the connected device, open your browser and type the IP address of the terminal (default IP address: **192.168.0.1**) in the address bar to access the web interface, or
   On your smartphone, start the **EXPLORER Connect** app and select **Terminal access**.
2. Locate the connection package you want to start.

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

3. Click ▶ to start the connection.

   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.

4. Click ■ to stop the connection.

For details, see *To control data connections from web interface* on page 47.

To make phone calls over BGAN

To connect a smartphone or IP handset

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

Note Make sure your phone has an integrated SIP client. Cobham SATCOM offers the **EXPLORER Connect app** with a built-in SIP client that is ready to use with the EXPLORER 323. You can also find other SIP applications on the Internet.

To connect your smartphone for making calls

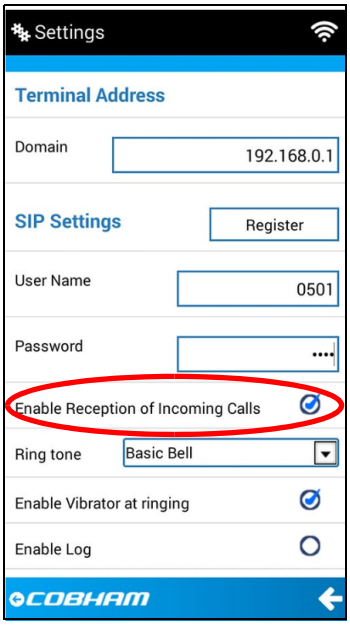
For details on **initial setup** of your smartphone and the EXPLORER 323, see:

- The documentation for your smartphone
- *First time SIP setup* on page 40
- *To manage VoIP phones or smartphones (Not M2M)* on page 66

To use your phone to make calls through the EXPLORER 323 using WLAN, do as follows:

1. Start up the EXPLORER 323 terminal.
2. Connect your smartphone to the wireless access point of the EXPLORER 323.
   See *To connect your WLAN-enabled device* on page 19.
3. Start the EXPLORER Connect app and select **Satellite Phone** (or start another SIP application).
   If it is the first time you use the EXPLORER Connect app, you must select **Register** when prompted.

Note If you are using the EXPLORER Connect app for the first time, select ⚙ in the bottom right corner and make sure that **Enable Reception of Incoming Calls** is selected in the settings page of the EXPLORER Connect app. This is to prevent your smartphone from closing the WLAN connection when not in use. This is necessary in order to be able to receive calls on your smartphone.



You should now be ready to make and receive calls over BGAN.

When the terminal is registered with the BGAN network and your phone is configured and connected to the LAN or WLAN interface, you are ready to make or receive the first call. The following sections provide a short guide to making calls. For more detailed information, see *To make or receive a phone call with EXPLORER 323* on page 41.

To connect a wired IP handset for making calls

For details on **initial setup** of your IP handset and the EXPLORER 323, see:

- The documentation for your handset
- The documentation for your PoE switch
- *First time SIP setup* on page 40
- *To manage VoIP phones or smartphones (Not M2M)* on page 66

Note The EXPLORER 323 does not supply PoE, so if your IP handset requires PoE you must connect a PoE switch or similar to supply power for the IP handset.

To connect a wired IP handset, do as follows:

1. Start up the EXPLORER 323 terminal.
2. Connect your PoE switch or similar to the LAN interface in the EXPLORER 323 cable (see *To connect Ethernet* on page 14).
3. Connect a LAN cable between the IP handset and the PoE switch.
4. Setup and register the handset as described in *First time SIP setup* on page 40 and *To manage VoIP phones or smartphones (Not M2M)* on page 66.

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

To make a call from the EXPLORER 323

To make a call from a phone connected to the terminal, dial

00 <country code> <phone number>

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

To make a call to the EXPLORER 323

Note By default, any handset connected to the terminal will ring on incoming calls.

To make a call to a phone connected to the terminal, dial

+ <Mobile number>

- **+** is the international call prefix[1] used in front of the country code for international calls.
- **Mobile number**: The mobile number of the terminal/handset you are calling. The first part of the number is always 870, which is the "country code" for the BGAN system.

1. The plus sign indicates the code required to dial out of one's country code area, such as 00 in most of Europe, 011 in the United States, and other short codes in other parts of the world.

Example: If you are calling from Denmark and the mobile number for Standard Voice is 870772420567 on your terminal, and you want to make a call to the terminal, dial **00 870 772420567**.

For the mobile number of your terminal, refer to the documents provided with your airtime subscription.

To use the EXPLORER 323

This chapter describes how to use the EXPLORER 323. It has the following sections:

- *Tools for setup and use*
- *Data connection with computer, smartphone or tablet*
- *To control data connections*
- *Power mode functions*
- *To access the terminal from a remote location*
- *To make phone calls over BGAN (not M2M version)*
- *Tracking and location reporting*

Tools for setup and use

The **web interface** is a built-in web interface for easy configuration. The web interface is accessed from a computer connected to the EXPLORER 323, using an Internet browser. No installation of software is needed on the computer. For further information on the web interface, see *Configuration with web interface* on page 43.

A **smartphone app**, **EXPLORER Connect**, is also available for iPhone and for Android phones. The app includes a **Satellite phone** function that enables you to make calls to and from your smartphone over the satellite network using the EXPLORER 323 terminal (not M2M subscriptions). It also includes the complete feature set from the built-in web interface of the terminal, allowing you to set up and use the terminal with your smartphone.

With **AT commands** you can configure and control the EXPLORER 323 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 33 and Appendix B, *Command reference*.

With **SMS commands** you can configure and control the EXPLORER 323 remotely. For details, see *Remote access with SMS* on page 37 and Appendix B, *Command reference*.

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.

Data connection with computer, smartphone or tablet

Overview

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

- LAN
- WLAN

Router function

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

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

Standard or Streaming data

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

- Using a **Standard data** connection, several users can share the data connection simultaneously. This type of connection is ideal for TCP/IP traffic such as e-mail, file transfer, and Internet and intranet access.
  The user pays for the amount of data sent and received.
- Using a **Streaming data** connection, you get an exclusive, guaranteed bit rate connection, ensuring seamless transfer of data. This type of connection is ideal for time critical applications like live video over IP.
  The user pays for the duration of the connection (per minute charge).

To control data connections

Automatic Context Activation (ACA)

In the web interface you can set up the EXPLORER 323 to automatically establish a data connection when it is registered on the satellite network. See *Automatic Context Activation (ACA)* on page 55. Automatic Context Activation also applies to the "wake-on" actions after power save (see *Power mode functions* on page 34) and by recovery after e.g. loss of power. This means when ACA is enabled, your data connection will automatically be reestablished when the terminal "wakes up" and registers on the network after power save, loss of power, or loss of the network connection.

Connection watchdog

Especially for M2M applications, it is recommended to use the Connection watchdog function to monitor your locally established IP connection, as it enables you to test the BGAN 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 try to reestablish the connection and may eventually restart the terminal.

For configuration with the web interface, see *Connection watchdog* on page 30.

For configuration with SMS command, see *WATCHDOG* on page 120.

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.

Important The Terminal watchdog can potentially drain the vehicle battery, because in certain cases it will prevent the terminal from going into power save state. If possible, we recommend using the Connection watchdog instead.

For configuration with the web interface, see *Terminal watchdog* on page 84.

For configuration with SMS command, see *ADVWATCHDOG* on page 120.

Manual activation of data connections

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

- Remote: Send an SMS to the EXPLORER 323. See *ACTIVATE* on page 120.
- Local (EXPLORER 323 LAN/WLAN 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 47, or
- Send an AT command to the terminal. See *To configure the connected equipment for PPPoE* on page 32, *To access the terminal using AT commands* on page 33 and *Context management AT commands* on page 133.

PPPoE (Point-to-Point Protocol over Ethernet)

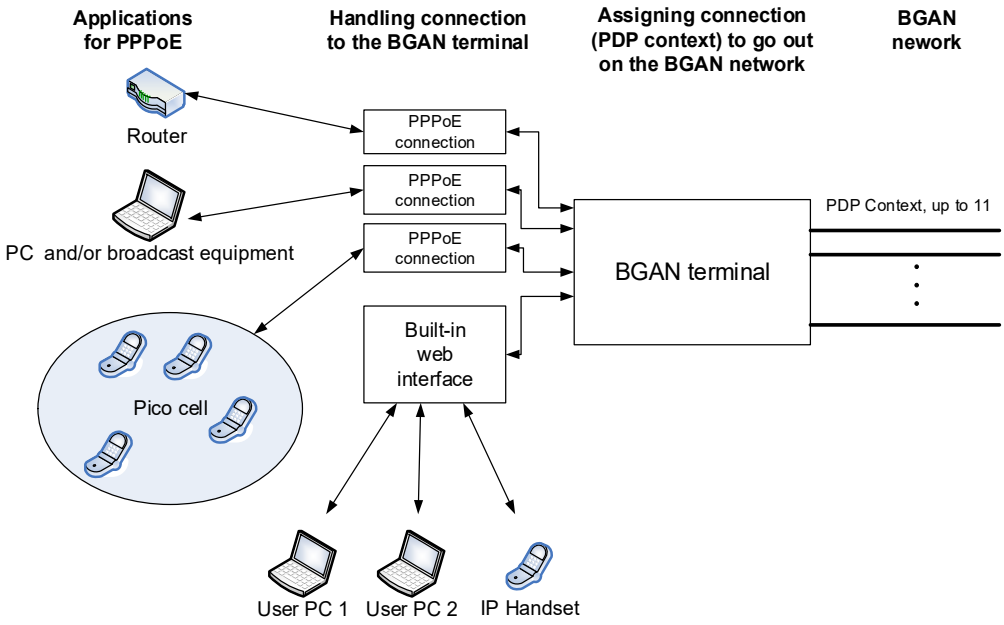
Overview

You can establish a PPPoE connection to the BGAN network using the EXPLORER 323 system. Use PPPoE if you want to control your connection independently of the web interface.

Possible applications are:

- Connect an EXPLORER Mobile Gateway, see *PTT connection example* on page 15
- Connect a router
- Connect broadcast equipment, optionally through a PC
- Establish a Picocell for the use of cell phones

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



To configure the connected equipment for PPPoE

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

- User name and password.
  The user name and password can be left blank (or insert user name: void and password: void). Then the registration on the Access Point is most commonly done in such a way that the data connection is established with a dynamic IP address from the airtime provider. To request a static IP (if subscribed to) from the Access Point you must type in the user name and password from your airtime subscription.
  Note for MAC OS: User name and password are required. Use user name void and password void. This works for some ISPs. Contact your airtime provider for further information.
- For setups that have a check box for "Enable LCP extensions", deselect this.
- APN.
  You have the option to define an APN specifically for your PPPoE connection. See *To change the APN for PPPoE* on page 69.

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, 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	Initiates a Primary Streaming 32 kbps connection
XBB:STREAM64K	Initiates a Primary Streaming 64 kbps connection[a]
XBB:<AT String>	This allows the PPPoE clients to enter a full AT context activation string. Examples: XBB:AT+CGDCONT=1,ip,"bgan.inmarsat.com" XBB:AT+CGEQREQ=1,1,64,64,64,64

a. 64 kbps is only available in elevations above 20 degrees.

To access the terminal using AT commands

1. Connect your computer to the EXPLORER 323 terminal.
   You may connect directly to the terminal or use a remote connection as described in the next sections.
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 323 (default 192.168.0.1) and port number 5454.
   - For **remote connection**, use the external IP address of the terminal (step 4 in the section *To get remote access from a trusted IP address (preconfigured)* on page 27). The port number for AT commands is normally 5454, but is defined in the Remote management page under AT commands (see *To set up remote access with IP* on page 71).
4. When the connection is established, type in your AT commands.

Power mode functions

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 323 enter power save state as well as how and when to wake up the terminal. For details, see *Power save* on page 90.

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 137.

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 35.

Always on

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

Important When the EXPLORER 323 is powered from the vehicle battery there is a risk of draining the battery if you use this method! We recommend to use the Remote on/off method instead.

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 save* on page 90) or with AT commands (see *To set up power save functions with AT commands* on page 137.

Note To use the Remote on/off function you must first connect the blue Remote on/off wire to the ignition of your vehicle (or to another remote on/off switch) as described in *To connect Ignition* on page 12.

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.

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.
- 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 save* on page 90.

For configuration with AT commands, see the section *To set up power save functions with AT commands* on page 137.

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)

To access the terminal from a remote location

Remote access with SMS

You can perform a number of actions and some configuration on the EXPLORER 323 using SMS commands.

1. Prepare the terminal for SMS commands as described in *To set up remote access with SMS* on page 88.
2. **Send an SMS** from a trusted phone number 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.

The following SMS commands are supported.

For an explanation of syntax and parameters, see *SMS remote commands* on page 120.

SMS command	Function
ACTIVATE	Activates BGAN data connections for the device(s) connected to the EXPLORER 323.
DEACTIVATE	Deactivates some or all the BGAN data connections for devices connected to the EXPLORER 323.
CLEAR	Deletes SMS messages in the EXPLORER 323.
GETINFO	Gets information from the EXPLORER 323 such as call time, data usage, GPS position and global IP address.
RESTART	Restarts the EXPLORER 323.
WATCHDOG	Gets or allows you to set the Connection watchdog parameters (Link monitoring).
ADVWATCHDOG	Gets or allows you to set the Terminal watchdog parameters.
ATCO	Allows you to send AT commands in an SMS to the EXPLORER 323 which returns the response in an SMS. **Note:** The ATCO command only supports a subset of the AT commands, see *ATCO commands* on page 98.
ADPWRST	Resets the EXPLORER 323 administrator password to **admin**.

Remote access with 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).

- Accessing an EXPLORER 323 that is preconfigured 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 get remote access from a trusted IP address (preconfigured)

Note This method requires that you initially have local access to the EXPLORER 323. If not, use the **_IREMWEB** command described in the previous section.

Initial local configuration

1. Connect a computer to the EXPLORER 323 and access the web interface locally.
2. Prepare the terminal as described in *To set up remote access with IP* on page 71.
3. Activate a data connection in one of the following ways:
   - Automatic Context Activation of a Standard data connection, see *Automatic Context Activation (ACA)* on page 39.
   - Manual activation of a data connection, see *To start and stop data connections* on page 36.
4. Note the terminal's external IP address as follows:
   In the web interface on the locally connected computer, the external IP address of the terminal is shown in the tile with the connection you started in the previous step.
   This is the IP address you must use afterwards to access the terminal from your remote computer.

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 38.

Remote access to web interface:

1. Make sure your remote computer has access to the Internet.
2. On the remote computer, open your web browser.
3. 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 323. 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 *Remote access with SMS* on page 37.
   - <incoming port> is the port you defined in *To set up remote access with IP* on page 71 (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.

Remote access with AT commands

1. Prepare the terminal for remote management as described in the previous section *Initial local configuration* on page 27.
2. Access the terminal as described in *To access the terminal using AT commands* on page 24.

For more information on AT commands, see *Command reference* on page 118.

To make phone calls over BGAN (not M2M version)

Note Phone calls are only possible if the airtime subscription is a BGAN class 12 subscription (not M2M).

To connect a VoIP phone or smartphone

Your VoIP phone or smartphone 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 323 has an integrated SIP server.

To connect your phone for making calls

For details on initial setup of your VoIP phone and the EXPLORER 323, see

- The documentation for your handset
- *First time SIP setup* on page 29
- *To manage VoIP phones or smartphones in your EXPLORER 323* on page 51

To connect a VoIP phone, do as follows:

1. Start up the EXPLORER 323 terminal.
2. Connect your phone via a switch to the LAN interface on the EXPLORER 323[1], OR connect your smartphone to the WLAN interface of the EXPLORER 323 and install and use the EXPLORER Connect App or a SIP client to be able to make calls over the satellite network.

   Note By default, one SIP client is enabled in the EXPLORER 323 with the user name 0501. Additional phones (SIP clients) must first be set up in the web interface and enabled before you can use them.

When the VoIP phone is powered and ready, you are able to make and receive calls over BGAN.

First time SIP setup

If it is the first time you connect your phone to the EXPLORER 323 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 323 (0501 to 0516)
- Password: Default same as user name

1. Since there is only one LAN interface and the EXPLORER 323 cannot provide power, you must connect the phone(s) via external equipment such as a PoE switch.

- Codec priority: Highest priority codec type: G.711

Note The user name and password must match the IP handset settings in the EXPLORER 323. See *To manage VoIP phones or smartphones* on page 51.

To make or receive a phone call with EXPLORER 323

Connect your smartphone or IP handset as described in *To connect a VoIP phone or smartphone* on page 29.

To make a call from the EXPLORER 323

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 323 shows an error message.

To receive a call

By default, all phones connected to the EXPLORER 323 will ring when the mobile number is called.

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

To make a call to the EXPLORER 323

To make a call to a phone connected to the EXPLORER 323, 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 number, refer to your airtime subscription.

Local numbers and special functions

Overview

There are a number of local numbers and dialing functions available in the EXPLORER 323.

The following list shows the allocated local numbers and special-purpose numbers for the EXPLORER 323.

Number	Function
0 followed by one of the numbers 501-516 and off-hook key	Local call to one smartphone or IP handset.

Apart from the numbers above, the EXPLORER 323 uses the following dialing prefixes:

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

Tracking and location reporting

The EXPLORER 323 can be used for tracking purposes. You can set up the terminal to report its position to a server at certain time intervals or after moving a given distance.

To use the tracking feature you must either set up a tracking server or get a tracking solution from your service provider. The EXPLORER 323 must be set up to match this server. For information how to set up the EXPLORER 323, see *To set up tracking and location reporting* on page 60. Once set up on both sides, the EXPLORER 323 will send position reports to the server as specified.

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*
- *Status information*
- *The Control panel*
- *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*

The web interface

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.

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 37.
4. If you have an M2M subscription, you must log in to access the web interface, see next step.
   If you have a non-M2M subscription, the web interface will now open to the Dashboard page and you will have normal User access.
5. Enter user name and password. You can log in as user or as administrator.
   - Default for user: User id = user, Password = <serial number of the EXPLORER 323>
   - Default for admin: User id = administrator, Password = admin

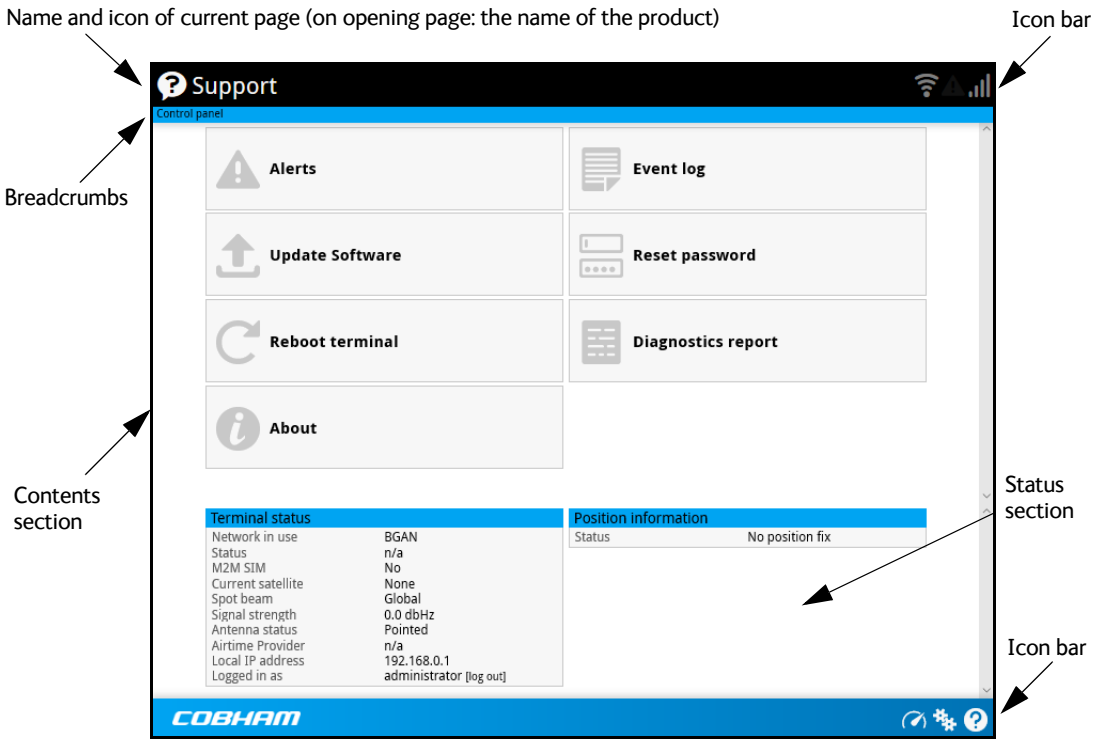
   Note If you enter a wrong password 5 times in a row, you are locked out for 15 minutes (other users can still access the login page). After 15 minutes you can try again.

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 79.

You can change the language to **French**, **German**, **Russian**, **Spanish**, **Portuguese**, **Chinese** or **Japanese**. See *To select the language* on page 64.

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.



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), position information, ongoing calls and data sessions etc. The Status section is not shown on small screens. If the screen is small (e.g. on a smartphone), you can show/hide the status by clicking at the bottom of the page.

Icons in the icon bars

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

Icon	Explanation
	Signal level of the external network (BGAN).
	WLAN interface. Bright when WLAN is enabled, grayed when it is disabled. Click to access WLAN settings.
	The WLAN icon shows the number of connected devices.
	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.
	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).

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 Streaming data is not available with an M2M subscription.

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 55.

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 ?.

To start and stop data connections on your EXPLORER 323, 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 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 60.

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.
- 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.

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. The user pays for the amount of data sent and received.
Streaming data The following Streaming classes are available: 32 or 64[a] 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. The user pays for the duration of the connection. **Note that Streaming is not available in M2M subscriptions.**

a. 64 kbps streaming is only available in elevations over 20 degrees.

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.

To set up your data connection packages

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

Connection packages

If you want to	Do as follows
Run one connection at a time from the startup page.	This is the default setup, with only one connection in each connection package. Start the connection you need from the web interface or the display.
Use different connection types for different types of traffic.	Add more connections to a connection package and apply filters to assign different connection types to different types of traffic. See *To create a package with multiple connections* on page 52. Start all the connections in the package by starting the package from the web interface or the display.

To change the contents of a connection package

You access the connection packages from the Dashboard.

- To access the Dashboard click at the bottom of the page.
- To change the contents of a connection package, click in the right side of the tile with the connection package.

If you want to	Do as follows
Change the name of 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.
Delete a connection package	Click **Delete package**[a] Note: You cannot delete **Standard data**.
Remove connections from the connection package	Click in the tile with the connection you want to remove.
Add a connection to the package	See *Multiple data connections* on page 51.

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

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.

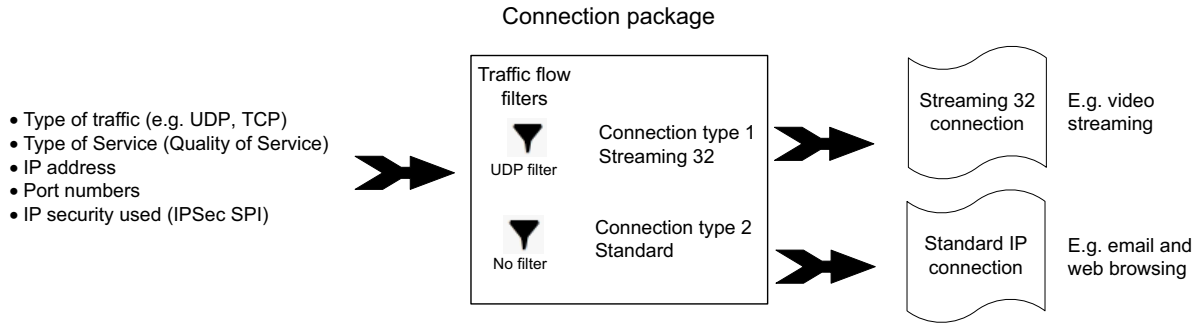
Note It is recommended to leave **IP Header compression** disabled. This means that the data packets are transmitted more reliably with less data loss.

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**.

Multiple data connections

If you want to have different types of connections running at the same time, you can build connection packages with the connections you want, using filters to determine which traffic should use which connection type.



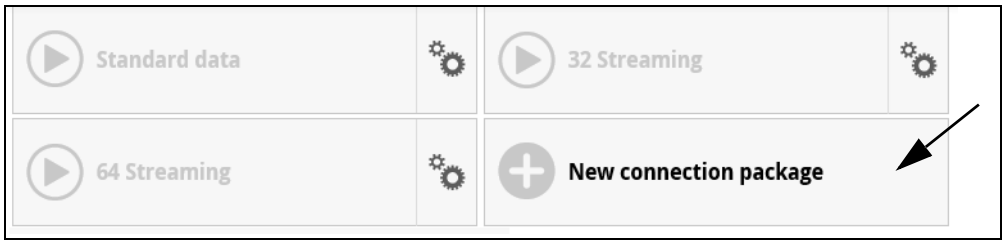
You then have to set up the following:

- Create a new package. See the next section *To create a package with multiple connections*.
- Add connections to the package.and select a predefined filter for each connection.
- Optional: Change the APN for the package. See *To change the APN for a connection package* on page 50.

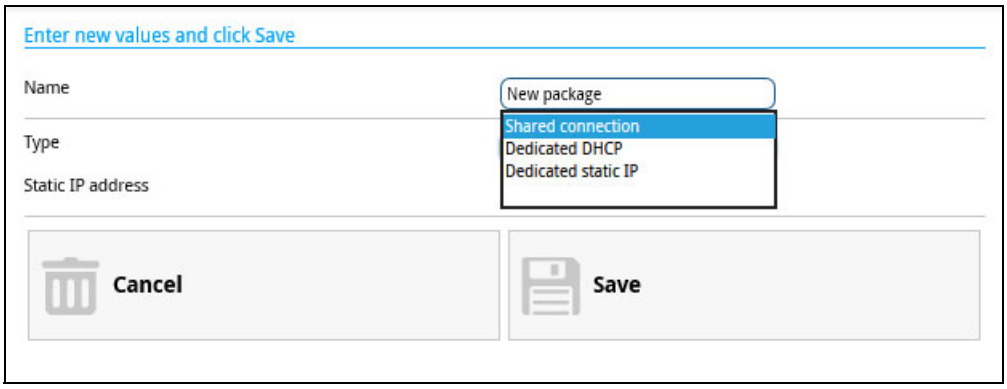
Example: You want to be able to send email while making a live video transmission with your EXPLORER 323:
You build a new package containing 2 connections:
1: A streaming connection (for your video transmission). Select the UDP filter.
2: A Standard connection (for email etc.). Select “No filter”.
When you have started this connection package, your video input to the EXPLORER 323 terminal is now automatically routed to the streaming connection. All other traffic is routed to the Standard data connection.

To create a package with multiple connections

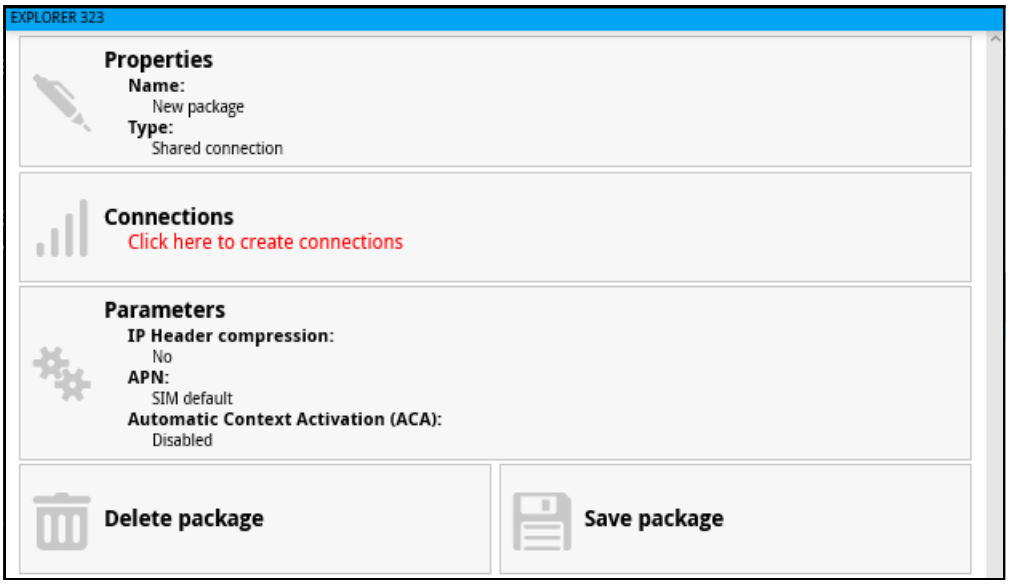
1. From the startup page, click **New connection package**.



2. Type a name for the new connection package.
3. Select the type of connection (see *To set up dedicated connections* on page 56).

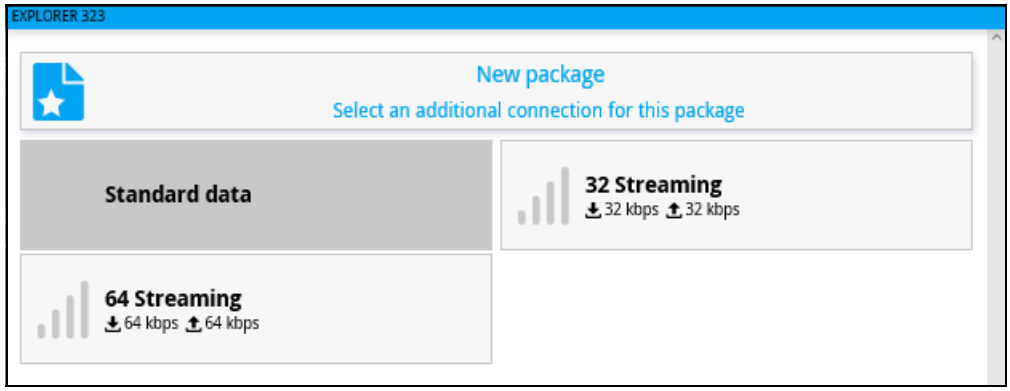


4. Click **Save**
5. Click **Click here to create connections**.

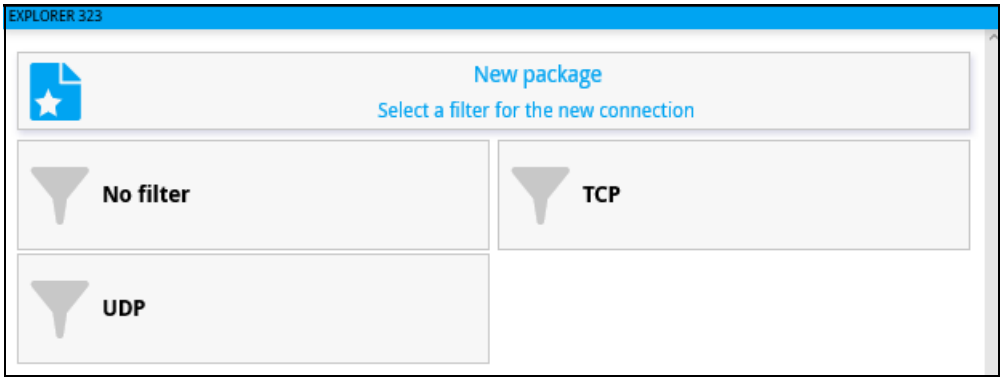


6. To add a connection to the connection package, click **Add connection** and select the type of connection you want to add.

Important The filters are applied in the order they are added. This means that if you want to have a connection with no filter, it must be the last connection you add to your connection package. If not, the next filters are ignored, because "No filter" means all data passes through without filtering.



7. Select a predefined filter for your new connection.



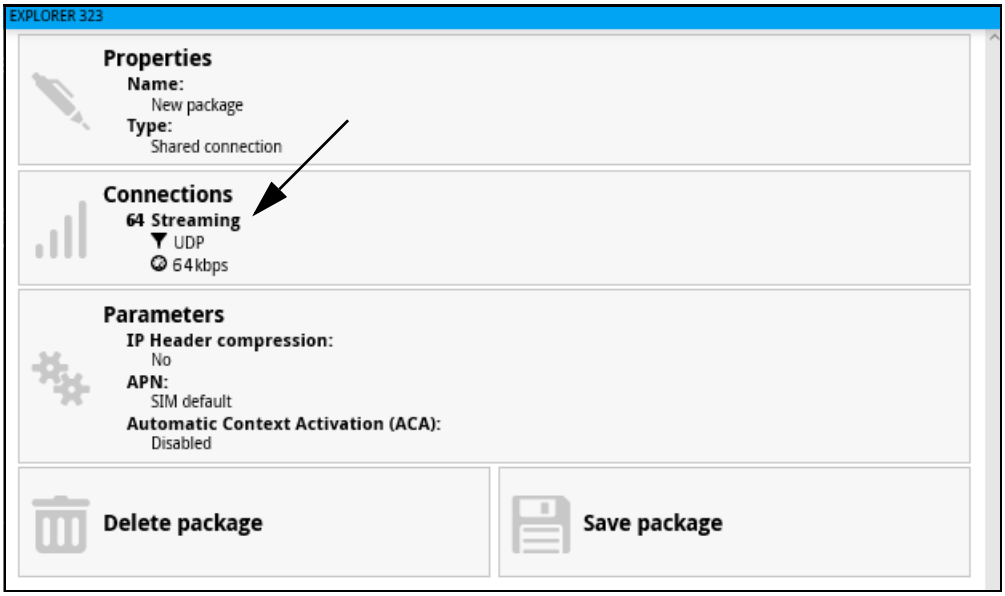
The predefined filters are:

- **UDP**: Filters traffic using UDP protocol (such as video streaming or Voice over IP).
- **TCP**: Filters Traffic using TCP protocol (such as web browsing)
- **No filter**: All data pass through. **Use only for the last connection** you add to your package.

The filters are applied in the order in which they were defined. This means that if you have a connection with no filter as the last connection, all traffic that does not match the first filters in the list will be passed through on this last connection. For this reason we recommend a Standard data connection for the "No filter" connection.

Note If you need a different filter than the ones available, you can log in as administrator and add new filters to the list. See *Traffic flow filter templates* on page 94.

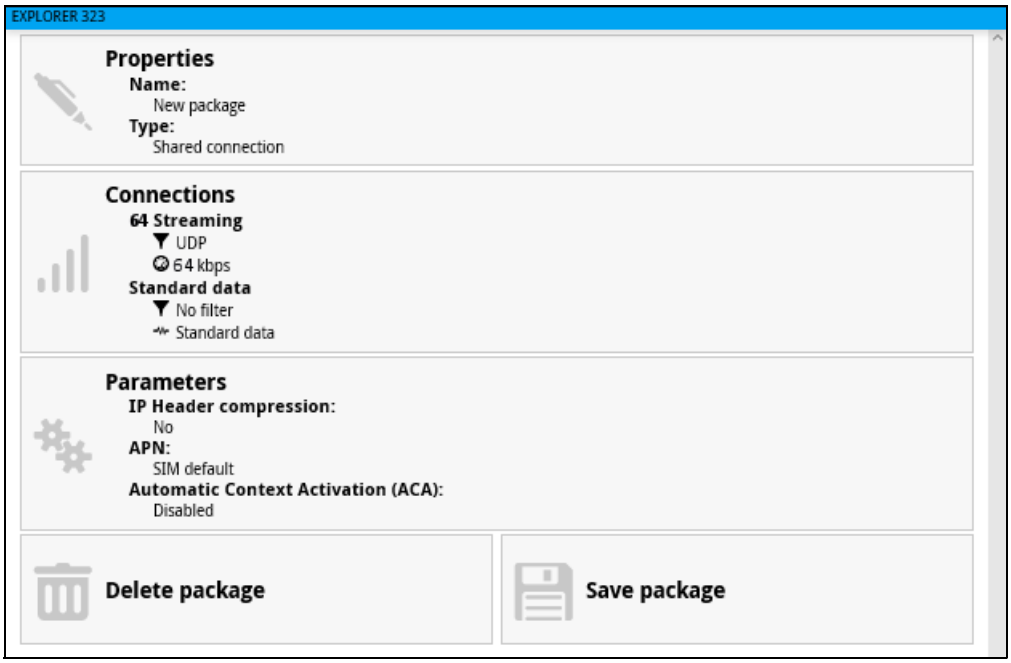
The connection package now shows your first connection.



8. Click the **Connections** tile.
9. To add a second connection, click **Add connection**.
10. Select a connection type for your second connection.

> **Note** You may not have all connection types available if you have selected a streaming type for your first connection, because your total bandwidth will be "filled up".

11. Select a filter for the connection.
    If this is the last connection in your connection package, you may select No filter, in order to let all remaining traffic use this connection
    The connection package now contains the two connection types.



12. Click **Save package**.

The new connection package is now on the startup page (Dashboard).

When you have started this connection package and traffic is detected on the LAN or WLAN interface, the filters are used to route the traffic. E.g. if you connect your video equipment with UDP traffic to the EXPLORER 323, your video transmission will use the connection that has UDP in the filter settings (64 Streaming in the example above).

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 323 and its BGAN connection are ready.

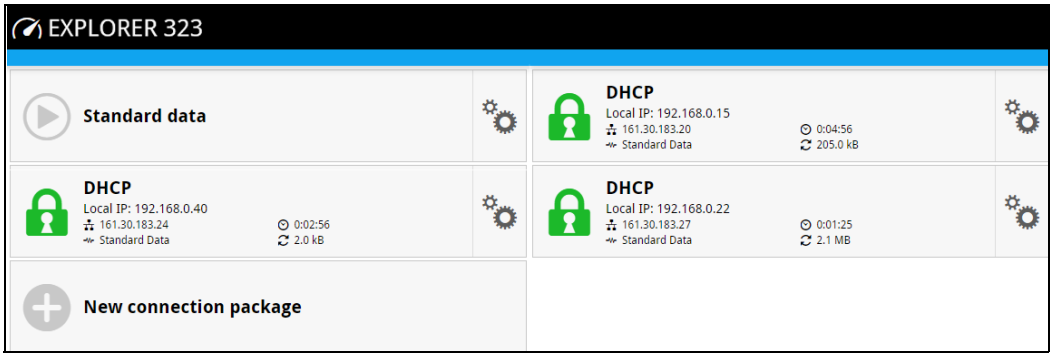
     Note You are charged for the data transferred. You may want to disable automatic updates in your LAN device to avoid unnecessary charges.

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

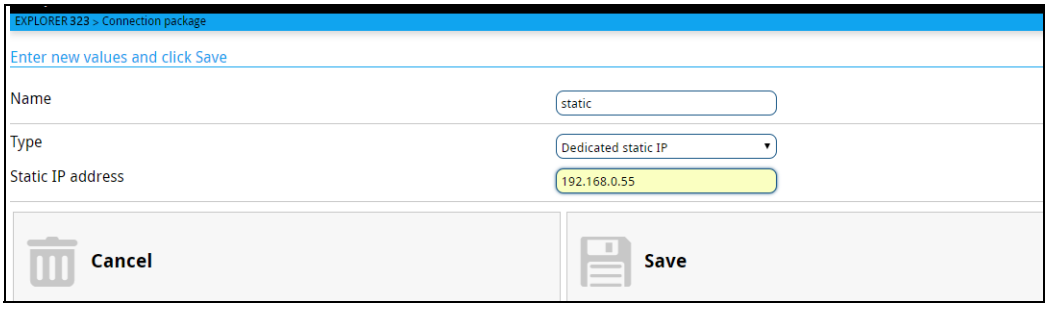
To set up dedicated connections

You can set up dedicated connections for the EXPLORER 323, e.g. for M2M equipment.

1. From the Dashboard, click **New connection package** to create a new connection package, or
   click ⚙ in the right side of the tile with the connection package that you want to change and click **Properties**.
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 323 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**.



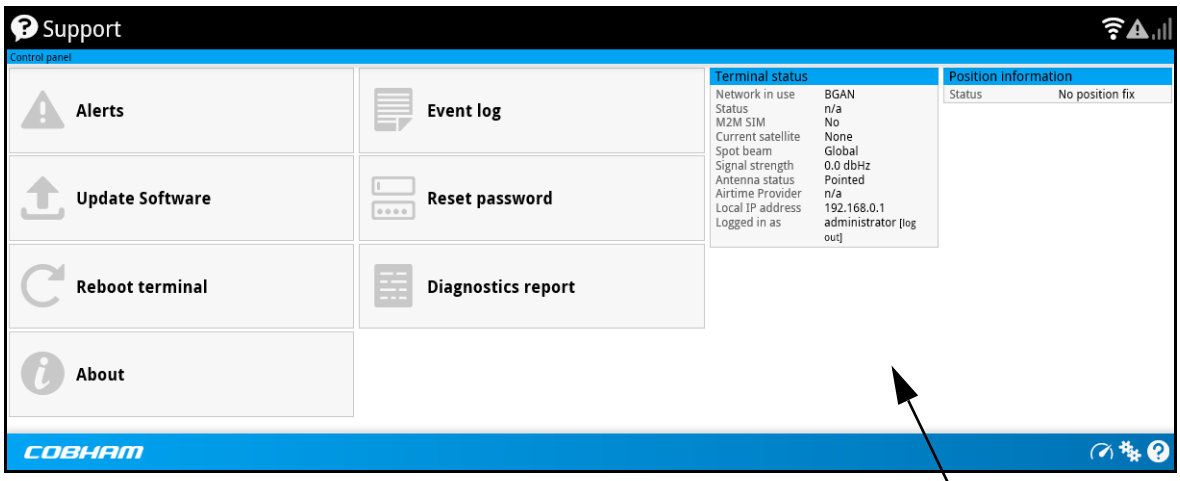
   If Automatic Context Activation (ACA) is enabled, the connection is established automatically. Only the unit with the configured static IP address can use this connection.

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

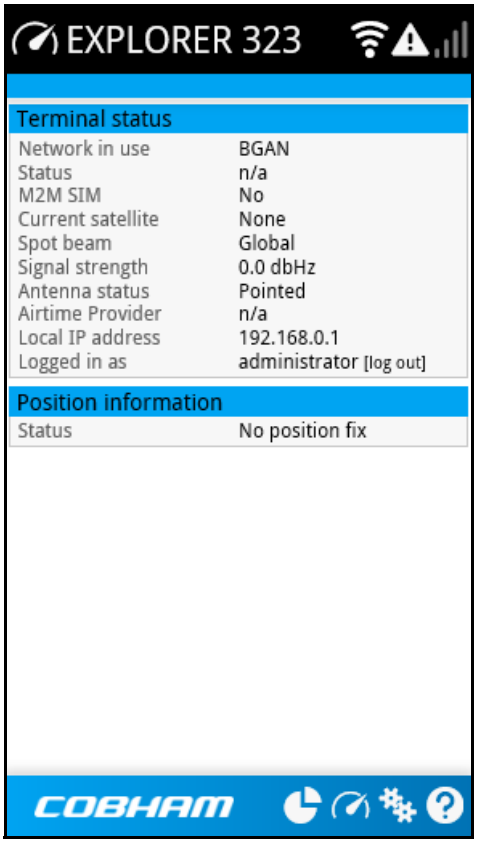
3. Click **Save**.

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



Small screen: Toggle between status and contents page

The following status is available:

Terminal status:

- 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.
- M2M SIM: Shows whether or not the BGAN SIM card is an M2M SIM (Yes or No)
- Current satellite: The satellite to which the EXPLORER 323 is currently registered.
- Spot beam: The type of spot beam currently used, e.g. Regional or Narrow.
- Signal strength: The signal strength of the BGAN connection.
- Antenna status: The status of the antenna, such as Sky scan, Tracking, Pointed etc.
- Airtime Provider: The provider of the BGAN services.
- Mounting calibration: The status of the calibration process that detects how the EXPLORER 323 is oriented in relation to the vehicle. Can be Calibrating, Validating or Completed. For details, see *Mounting calibration* on page 23.
- Local IP address: The local IP address of the EXPLORER 323. E.g. used to connect to the web interface.
- 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 323.
- 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):

- Standard data: Shows that a Standard data connection is running on the Standard data connection package.
- Streaming xxx kbit/s: Shows that a Streaming data connection is running (not possible with M2M subscription).

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

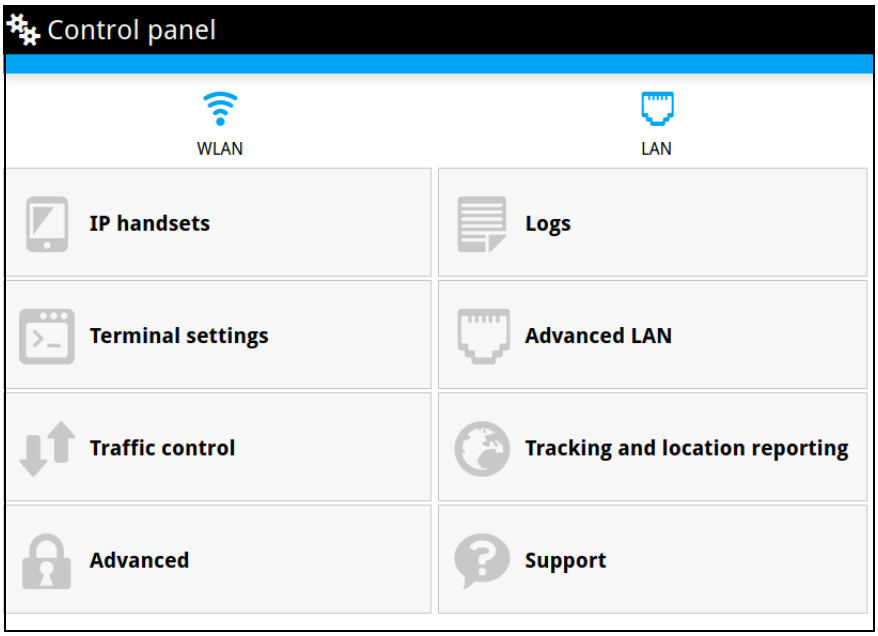
- Status: The status of the call, e.g. “Connected” or “Ringing”.
- Call type: Shows the call type (Standard voice).
- Call duration: The duration of the call.
- Originator: The phone number from which the call was made.
- Receiver: The phone number that receives the call.

The Control panel

The **Control panel** is used for accessing the settings and functions of your EXPLORER 323.

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

Note IP handsets: The M2M subscription does not support Voice over IP (VoIP).



To use the logs

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.

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.

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).

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

Total counters

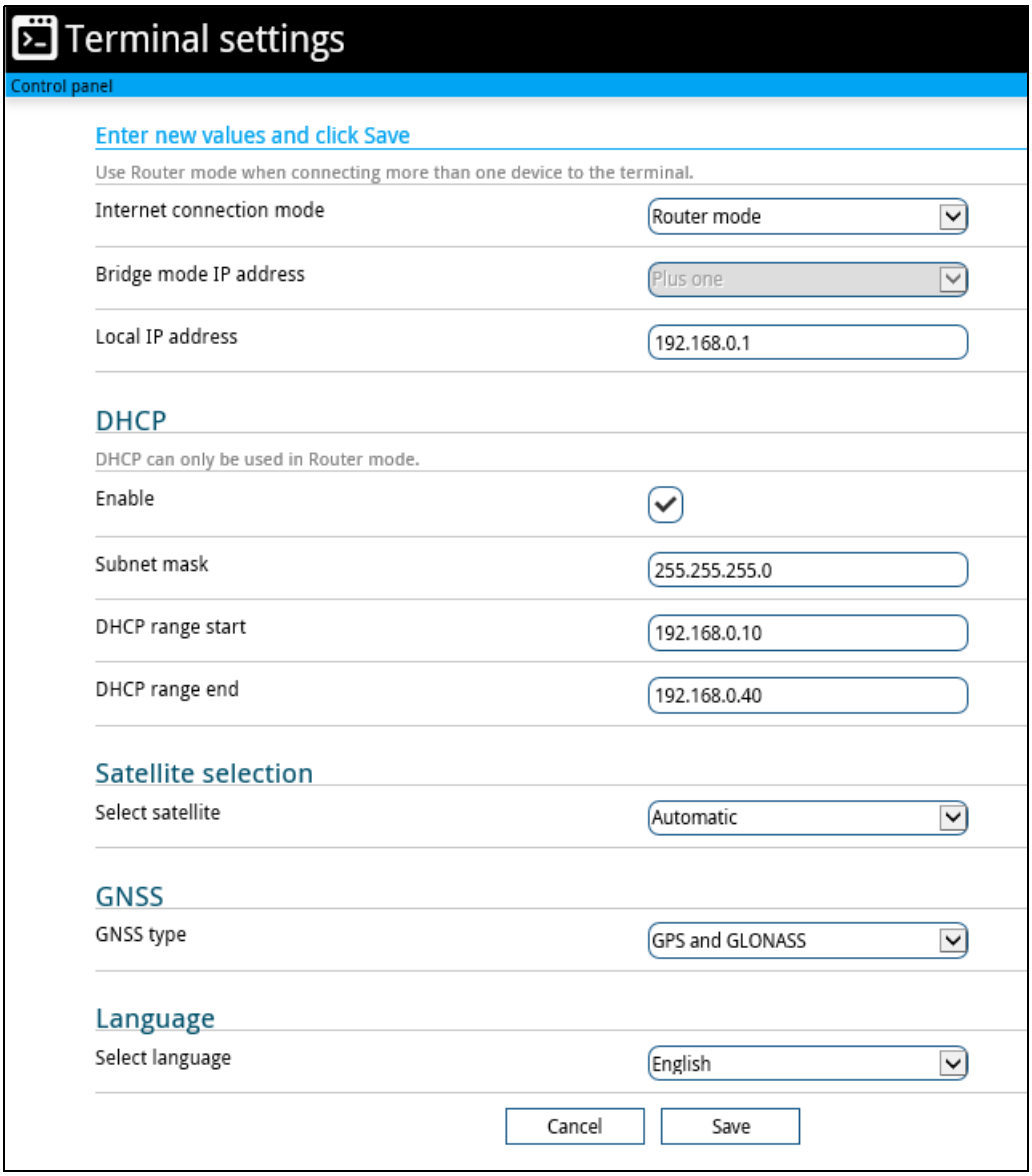
The total counters show:

- **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).

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

Terminal settings

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

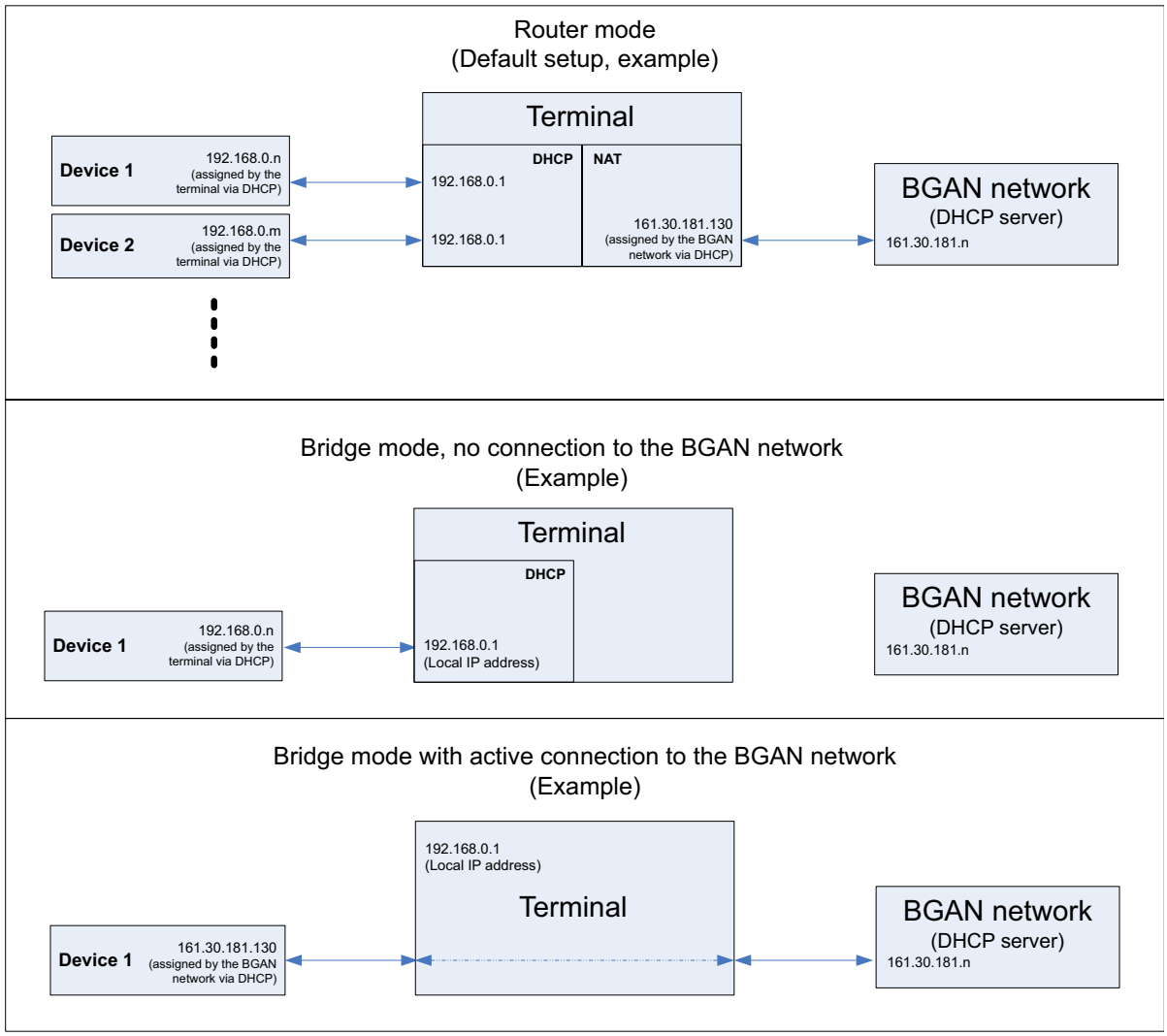


To set up the connection mode

Internet and LAN connection modes

In the web interface you can set up the Internet connection mode and the IP addressing between the EXPLORER 323 and devices connected to the EXPLORER 323. The EXPLORER 323 has a built-in DHCP server which can be used to dynamically assign IP addresses to devices connected to the EXPLORER 323.

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



To set up the connection mode of the EXPLORER 323, 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 323 should act as a router. When Router mode is selected, the EXPLORER 323 uses the built-in NAT module for making the necessary address translations.
   - Select **Bridge mode** if only one computer is connected, and the EXPLORER 323 should act as a modem, or more than one computer is connected using an external router.

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

2. If you selected **Bridge mode**, select under **Bridge mode IP address** how the terminal's IP address should be assigned.
   - **Dynamic** example: If the IP address assigned by the DHCP server to the locally connected equipment is 10.30.27.130, the terminal will get the IP address 10.40.27.130. (in most cases it will be 10 added to the second octet of the assigned IP address).
   - **Plus one** example: 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 111.

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**.

To select the preferred BGAN satellite

By default the terminal is set up to automatically find the most appropriate satellite to connect to (Automatic mode). However, if you are located in an area with more than one BGAN satellite available, you can select the satellite you prefer to use when the terminal registers on the BGAN network. Do as follows:

1. In the **Terminal settings** page, locate the **Satellite selection** section.
2. Select the satellite you want to connect to, or select Automatic to let the terminal find the most appropriate satellite.
3. Click **Save**.

To select the type of navigation system (GNSS)

To select which navigation system to use with your EXPLORER 323, do as follows:

1. In the **Terminal settings** page, locate the GNSS section (Global Navigation Satellite System).
2. Select **GPS**, **GPS and GLONASS** or **GPS and BeiDou**.
3. Click **Save**. Note that it may take some minutes for the EXPLORER 323 to change the navigation system.

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**.

To set up the interfaces

LAN interface setup

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

   Important If you disable LAN you may not be able to access the EXPLORER 323. Before disabling the LAN interface, make sure you have a working WLAN connection.

   You can restore the LAN settings with the Reset button, see *Reset button* on page 103.

   Note It may take some seconds to enable the interface.

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

For a description of how to set up the **local network parameters**, see *To set up the connection mode* on page 62 and *Advanced LAN* on page 68.

WLAN interface setup

Note The Internet settings entered in the Terminal settings page also apply for the WLAN interface. See *Internet and LAN connection modes* on page 62.

To configure the WLAN interface, do as follows:

1. In the **Control panel**, click the W**LAN** icon at the top of the page.
2. To enable the WLAN interface, select **Enable**.

   Important If you disable WLAN you may not be able to access the EXPLORER 323. Before disabling the WLAN interface, make sure you have a working LAN connection.

   Note It may take some seconds to enable the interface.

3. Next to **Region**, select the region you are located in.

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

4. Select the **Channel** number used for communication on the WLAN interface.
5. Select **Broadcast SSID** to show your WLAN access point to other users.
   If you **clear** the box, your WLAN access point is hidden.
6. Type in the **SSID**.

The SSID is a max. 32 character text identifying the wireless local area network. All wireless devices on a WLAN must use the same SSID in order to communicate with each other. The default SSID is **EXPLORER323**.

7. Select the **Security** standard. You may select one of the following encryption standards:
   - None (no encryption is applied)
   - WEP-40/64
   - WEP-104/128
   - WPA-TKIP
   - WPA2-AES (selected by default)
8. Next to **Key type**, select **Hexadecimal** or **Text**.
   The encryption key must normally be a hexadecimal code. However, if you are using WPA-TKIP or WPA2-AES encryption (default) you can choose to use a text string, which may be easier to memorize.
9. Type in the **Encryption key** for the selected Security standard (not applicable if security mode = None). The default encryption key is the **serial number** of the EXPLORER 323. You can find the serial number under **Control panel > Support > About** or on the label on the EXPLORER 323.
10. Click **Save**.
    - A line through a grayed-out **WLAN** icon means the interface is **disabled**.
    - A blue **WLAN** icon means the interface is **enabled**.

Note You can restore the WLAN settings by clicking the button **Load default values** at the bottom of the WLAN page in the web interface.

For a description of how to set up the **local network parameters**, see *Internet and LAN connection modes* on page 62 and *Advanced LAN* on page 68.

To manage VoIP phones or smartphones (Not M2M)

Overview

This section describes how to manage VoIP phones or smartphones connected to the EXPLORER 323.

Note Connection of VoIP phones or smartphones is not possible with M2M subscription.

The terminal supports connection of up to 16 phones through the LAN interface (up to 10 phones on the WLAN 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 or WLAN interface, see *To connect a VoIP phone or smartphone* on page 40.

To manage VoIP phones or smartphones in your EXPLORER 323

Do as follows:

1. Connect your smartphone to the WLAN interface or your VoIP phone via a switch to the LAN interface. For details, see *To connect a VoIP phone or smartphone* on page 40.
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. Click **Save**.
7. In the smartphone or IP handset, enter the local number and the password you just entered in the EXPLORER 323. 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.

Advanced LAN

Port forwarding

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

Port forwarding enables you to set up a server connected to the terminal while the terminal is in Router mode. Without port forwarding it would not be possible to contact the server from the Internet. We recommend using a static public IP address for the terminal in order to provide easy access to the terminal. To use the static IP address, it must be included in your subscription and you must set the APN source to SIM default. For details, see *To change the APN for a connection package* on page 50.

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 323 for which incoming traffic to the EXPLORER 323 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 24.

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 56.

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.

To change the APN for PPPoE

For general information on PPPoE and setup of connected equipment, see *PPPoE (Point-to-Point Protocol over Ethernet)* on page 31.

Before you can establish a PPPoE connection with the EXPLORER 323 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**.

To manage connected devices (Traffic control)

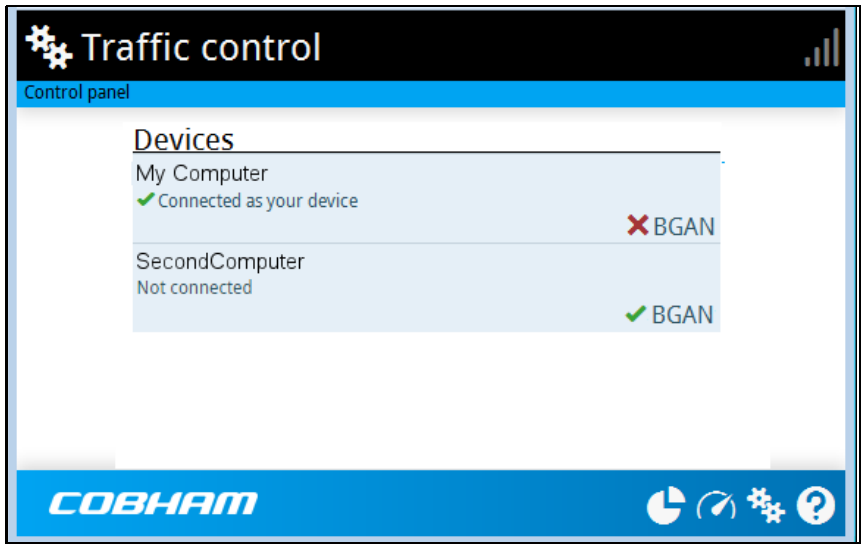
By default, traffic control is disabled, which means that all traffic is allowed.

With the Traffic control function you can get an overview of devices connected locally to your EXPLORER 323 and control which devices you want to connect. You can also select whether or not they should be allowed to use the BGAN network. Note that the available settings depend on whether or not you are logged in as administrator.

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 network. See the next section.

To block BGAN 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**, if you want to deny access to the BGAN 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**.

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** if you want to deny access to BGAN 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 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**, if you want to deny access to the BGAN 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:

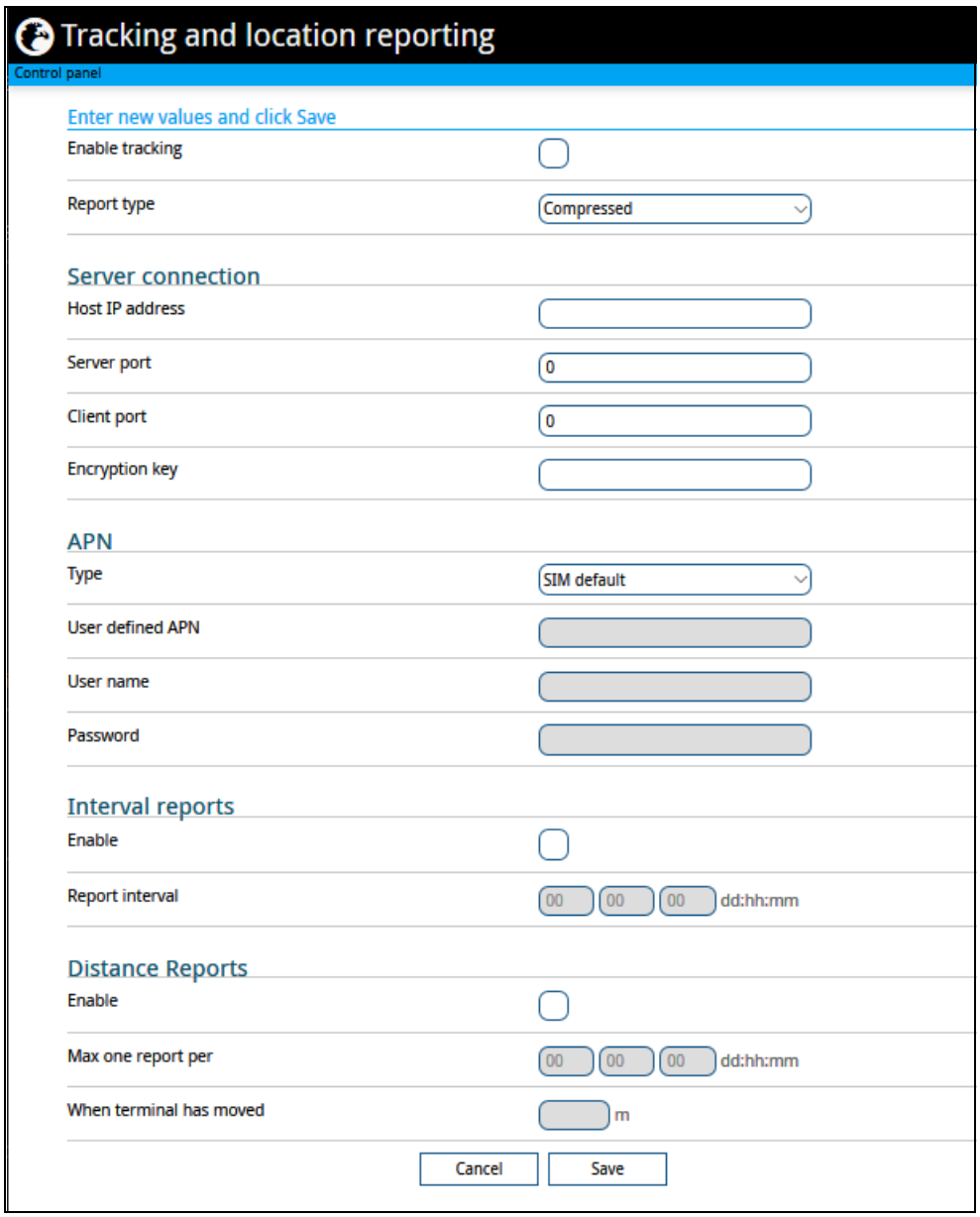
1. In the **Devices** page, click the **Add device** button.
2. Type in the **Name** and the **MAC address** for the device.
3. Select **Block BGAN traffic**, if you want to deny access to BGAN network for the selected device.
   If you want to allow access, clear the box. The device will then be able 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.

To set up tracking and location reporting

You can set up the EXPLORER 323 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 323, select **Enable tracking**.
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 323 will report to.
- **Server port**: Port number on the server. Default number is 7474.
- **Client port**: Port number on the EXPLORER 323. 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. If required, type in the user name and password for the APN.
7. Under **Interval reports**, select **Enable** and type in the **Report interval** in days (dd), hours (hh) and minutes (mm).

   Example: If you type in "01", "12" and "00" the EXPLORER 323 will send a report for every 1½ day.

   Note | If the EXPLORER 323 is in power save state, no report is sent!

8. Under **Distance reports**, select **Enable** and type in the following:
   - **Max one report per**. Enter the minimum time that should pass between two reports (days (dd), hours (hh) and minutes (mm)).
   - **When terminal has moved**. Enter the distance the vehicle should be moved before the EXPLORER 323 sends a report.

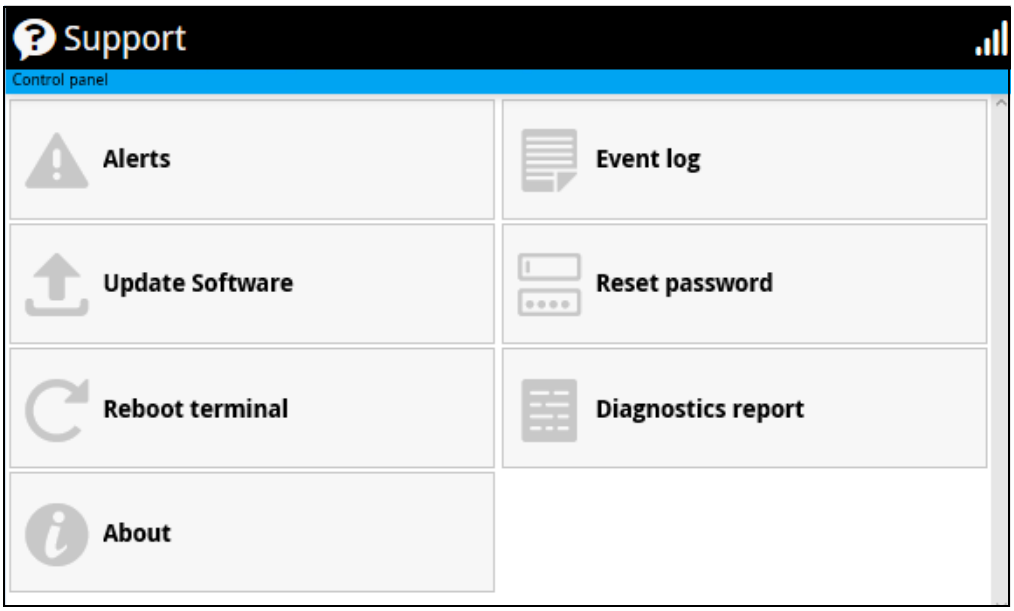
   Example: The distance is set to 10000 m and the time is set to 15 minutes. The EXPLORER system has moved 10000 m since last report, but only 10 minutes have passed. A report will not be sent until 15 minutes have passed.
9. Click **Save**.

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 89.

Support features

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



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 106.

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.

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.

To update software

To update the software in the EXPLORER 323 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 has not yet been completed, the Status LED flashes blue during the software update.

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

To reset the administrator password

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

> **Note** If you have physical access to the EXPLORER 323, you can also use the Reset button. For details, see *Reset button* on page 103.

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**.

1. You can download the software from the "Cobham SYNC Partner Portal" at www.cobham.com/satcom, select **Cobham SYNC Partner Portal** > **Downloads**. Locate the EXPLORER 323 software.

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.

About

The **About** page shows the **Serial number**, **software version**, **IMSI** and **IMEI** of your EXPLORER 323 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**.

Advanced settings

Passwords

The EXPLORER 323 web interface is password protected at two levels: A user password and an administrator password. You will always be prompted for a password when you access the web interface. Default settings are:

- **User**: User name: **user**, Password: <serial number of the EXPLORER 323>
- **Administrator**: User name: **administrator**, Password: **admin**

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

Important Change the administrator password immediately after first login!

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**.
   If you are not logged in as administrator 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 76. The old user name and password will apply until you have finished the reset procedure.
3. Click **OK**.

To change the user password

To change the user password, do as follows:

1. Log in as administrator.
2. Under **Advanced**, select **Passwords**.
3. Select **Change user password**.
4. Type in the **User id** (default: **user**).
5. Type in the **New password** and retype it on the next line.
6. Click **Save**.
   At the next 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 5 to 15 characters long and cannot contain spaces.

   Avoid special characters. Accepted characters: A through Z (uppercase characters), a through z (lowercase characters) and 0 through 9 (numeric characters).

6. Click **Save**.
   At the next 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.

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. Under **Allow AT commands on:**, select **LAN/WLAN interface** if you want to allow the use of AT commands.
4. Under **Allow user accounts:**, select **Service user account** if you want to enable the use of a service user account.
5. Click **Save**.

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

To restore factory settings

To restore the factory settings of the EXPLORER 323, do as follows:

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

   Important | All configuration will be lost and the EXPLORER 323 will return to the default configuration.

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

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 323 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 323 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 323. The next time the EXPLORER 323 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 80.

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.

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 323 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 323.
3. Click **Download configuration...**
   The configuration is downloaded from the EXPLORER 323 to the downloads section of your computer.

To load a configuration from a file

To load a configuration from a file into your EXPLORER 323, 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 323. When the configuration is loaded successfully, the EXPLORER 323 restarts with the new configuration.

Connection watchdog (Link monitoring)

Especially for M2M applications, it is recommended to use the Connection watchdog to monitor your locally established IP connection, as it enables you to test the satellite connectivity and to keep your PDP context alive.

Function

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 it fails again the terminal will eventually restart.

Note Ping commands are sent on all active data connections. The data connection must be activated before the Connection watchdog can start. See *To start and stop data connections* on page 47.

To set up the Connection watchdog

Do as follows:

1. Under **Advanced**, select **Connection watchdog**.
2. Select **Enable Connection watchdog**.
3. At **Ping interval (minutes)** select the interval in minutes between the ping commands.
   - Minimum interval is 5 minutes.
   - Depending on the Ping mode (step 5), this interval is the time from **last ping** or from **last transmission**.
4. Select the **Number of retries**.
   - The number of retries applies to each of the listed IP addresses (step 6).
   - The time between the retries is 40 seconds.
   - 40 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. 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.
6. Type in 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.
7. Click **Save**.

If no response is received from any of the IP addresses, the terminal will first try to reconnect and go through the entire procedure once again. If it fails on all IP addresses again, the terminal will eventually restart.

Terminal watchdog

Important The Terminal watchdog can potentially drain the vehicle battery, because in certain cases it will prevent the terminal from going into power save state. If possible, we recommend using the Connection watchdog instead.

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)
- 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 323 operates with UTC time, local time is not available.

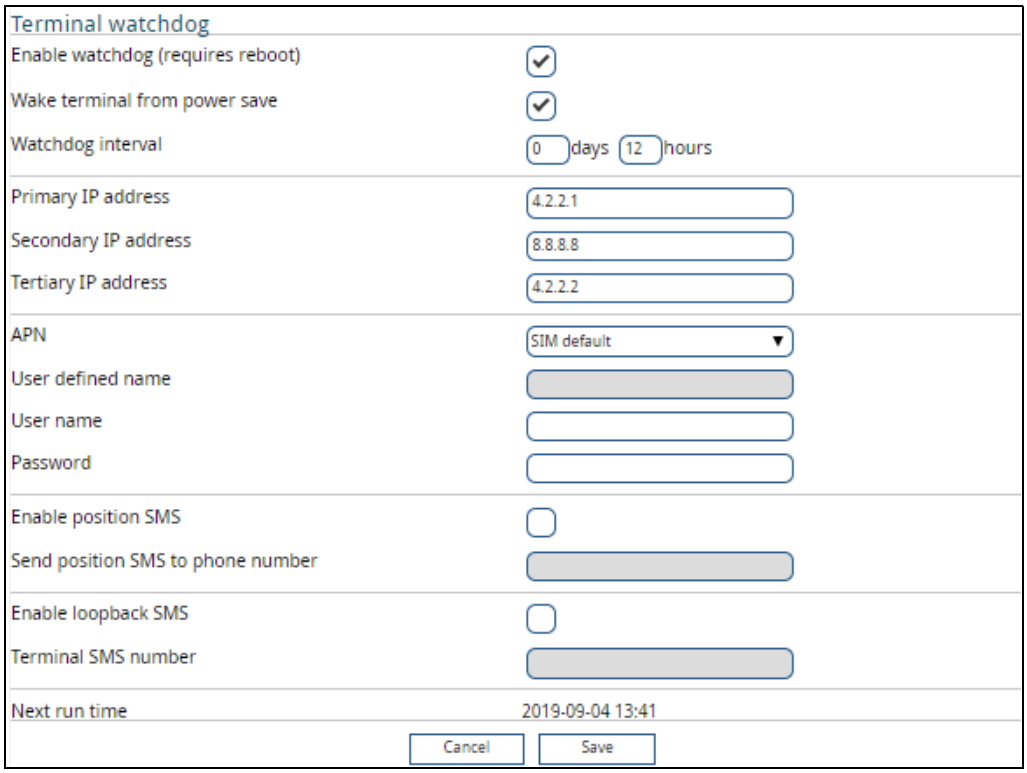
- CS-attach (the status of circuit-switched connection)

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**.



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).

Data limits

You can set a limit for the use of the BGAN data services with the EXPLORER 323 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.

Call charges

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.

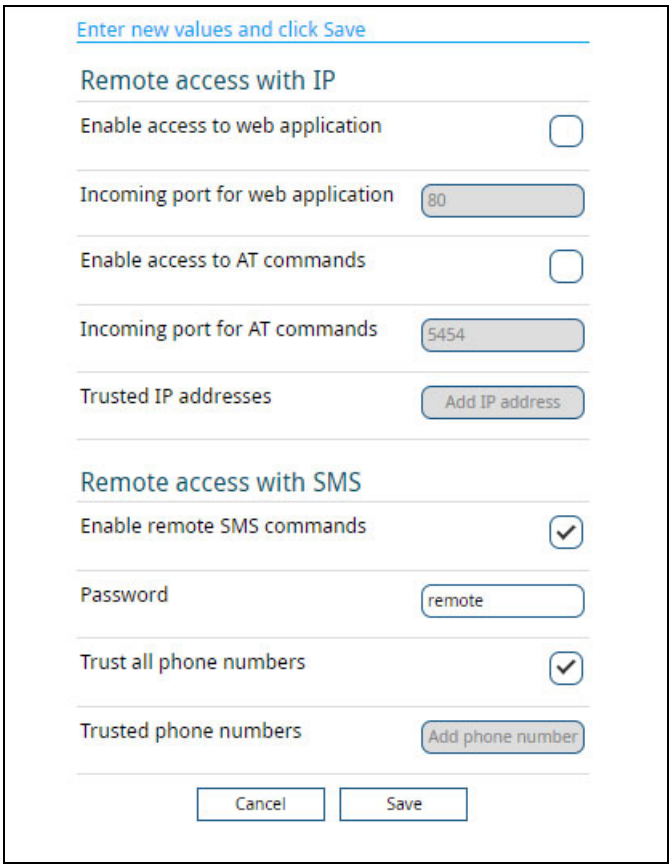
If you know the tariff for your subscribed BGAN services, you can enter these tariffs in the web interface and automatically calculate the estimated charges for your calls and data sessions. To enter the call tariffs, do as follows:

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 60.

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 136.

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.

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 37.

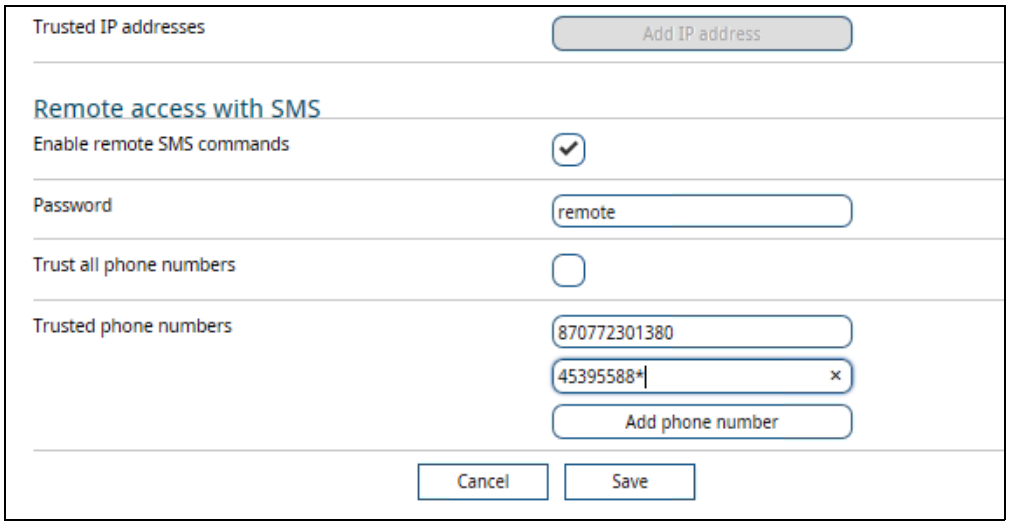
If Static IP is included in your airtime subscription, we recommend using this static public IP address for the terminal in order to provide easy access to the terminal. To use the static IP address, it must be included in your airtime subscription and you must set the APN source to SIM default. For details, see *To change the APN for a connection package* on page 50.

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**.
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**.
3. Select **Trust all phone numbers** or, at **Trusted phone numbers**, 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 37.

Remote control of tracking

When you are using the tracking function of the EXPLORER 323, you can set up the terminal so that the tracking server can access the EXPLORER 323 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**.

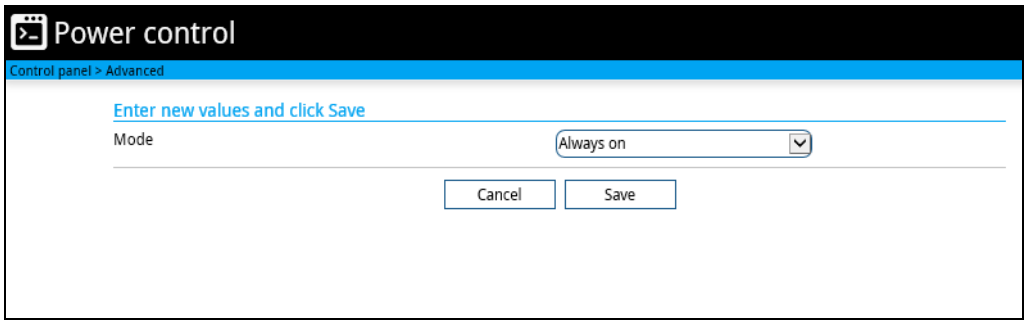
The EXPLORER terminal will now accept commands from the specified tracking server, for example to change reporting intervals or start/stop reporting.

Power save

There are a number of options to save power in the EXPLORER 323. For a general description of the power save options, see *Power mode functions* on page 34.

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

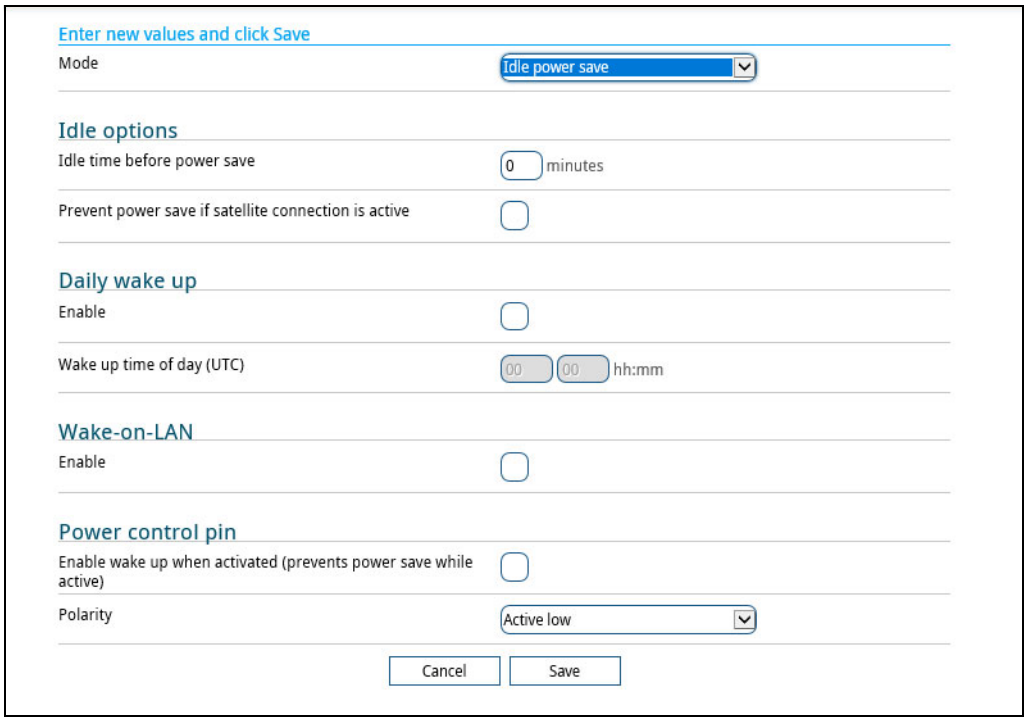
1. Under **Advanced**, select **Power control**.



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 92.
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.

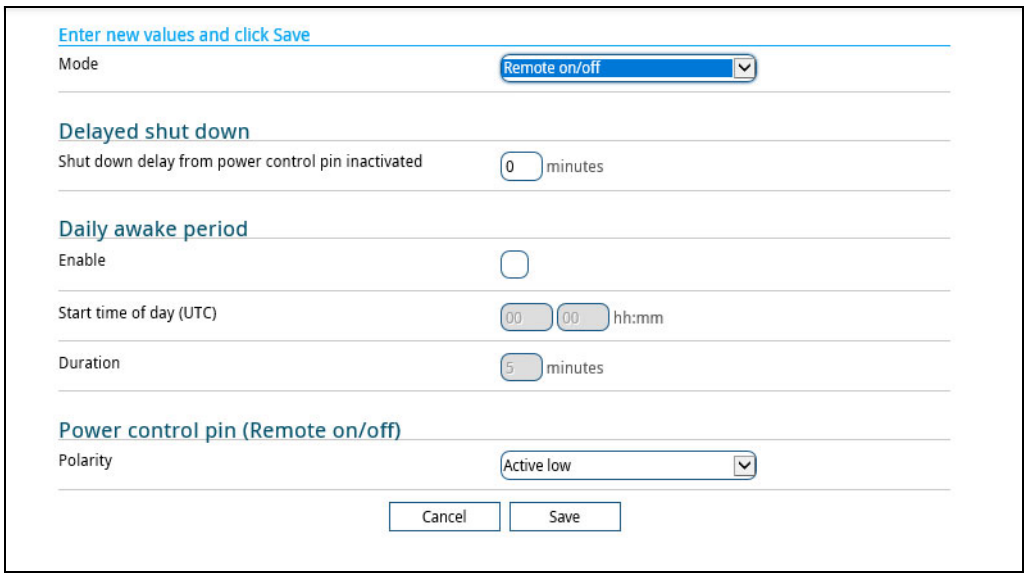
   Note With this option selected the terminal will be active when the Power control pin is active.

   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 323 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 mode functions* on page 34.



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**.

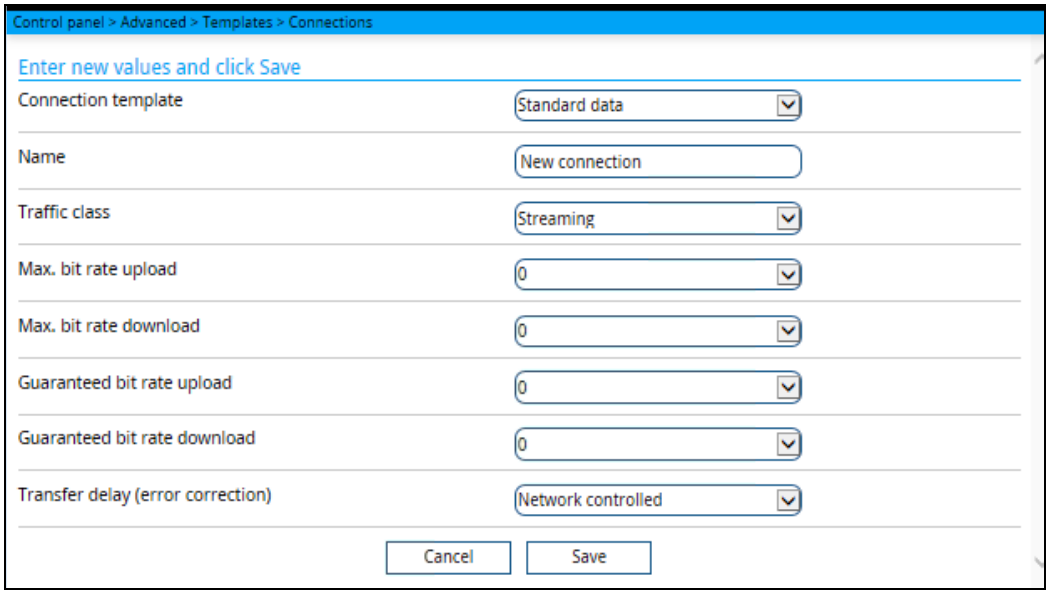
To configure data connection types and filters

If the default connection types and filters do not meet your requirements, you can build new templates for the connection types and/or traffic flow filters to match your needs.

Connection templates

To access the connection templates, do as follows:

1. Under **Advanced**, select **Templates**.
2. Select **Connections**.
3. To delete a connection type, click ? in the right side of the connection type.
4. To add a new connection type, click **Add template** and proceed with the next steps.



5. Select an existing **Connection template** as a basis for your new template.
6. Type in a suitable **Name** for the connection type.
7. Select the **Traffic class**.
   - **Standard** is a shared, best-effort connection, used e.g. for email or Internet browsing.
   - **Streaming** is an exclusive, high-priority connection with a guaranteed bit rate.
8. Select the following bit rates:
   - **Max. bit rate upload** is the maximum upload bit rate allowed for this connection type.
   - **Max. bit rate download** is the maximum download bit rate allowed for this connection type.
   - **Guaranteed bit rate upload**: For Streaming services this is the guaranteed upload bit rate needed for this connection type.
   - **Guaranteed bit rate download**: For Streaming services this is the guaranteed download bit rate needed for this connection type.

9. In the **Transfer delay (error correction)** field, select **Enabled**, **Disabled** or **Network controlled**.
   - Enabled: Error correction is applied
   - Disabled: Error correction is disabled (recommended for time critical applications)
   - Network controlled: Error correction determined by network
10. Click **Save**.

The new template will now be available for selection when you build your connection packages.

Traffic flow filter templates

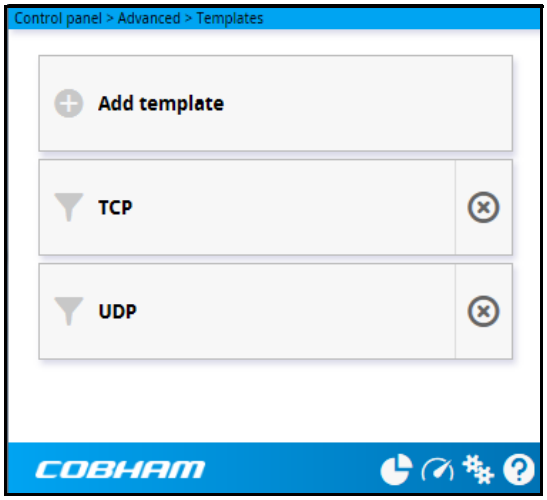
The traffic flow filters are used to filter the data traffic, so you can use different connection types for different types of traffic. There are two predefined filters, UDP and TCP.

- **UDP** is used for traffic using UDP protocol (such as video streaming or Voice over IP)
- **TCP** is used for traffic using TCP protocol (such as web browsing).

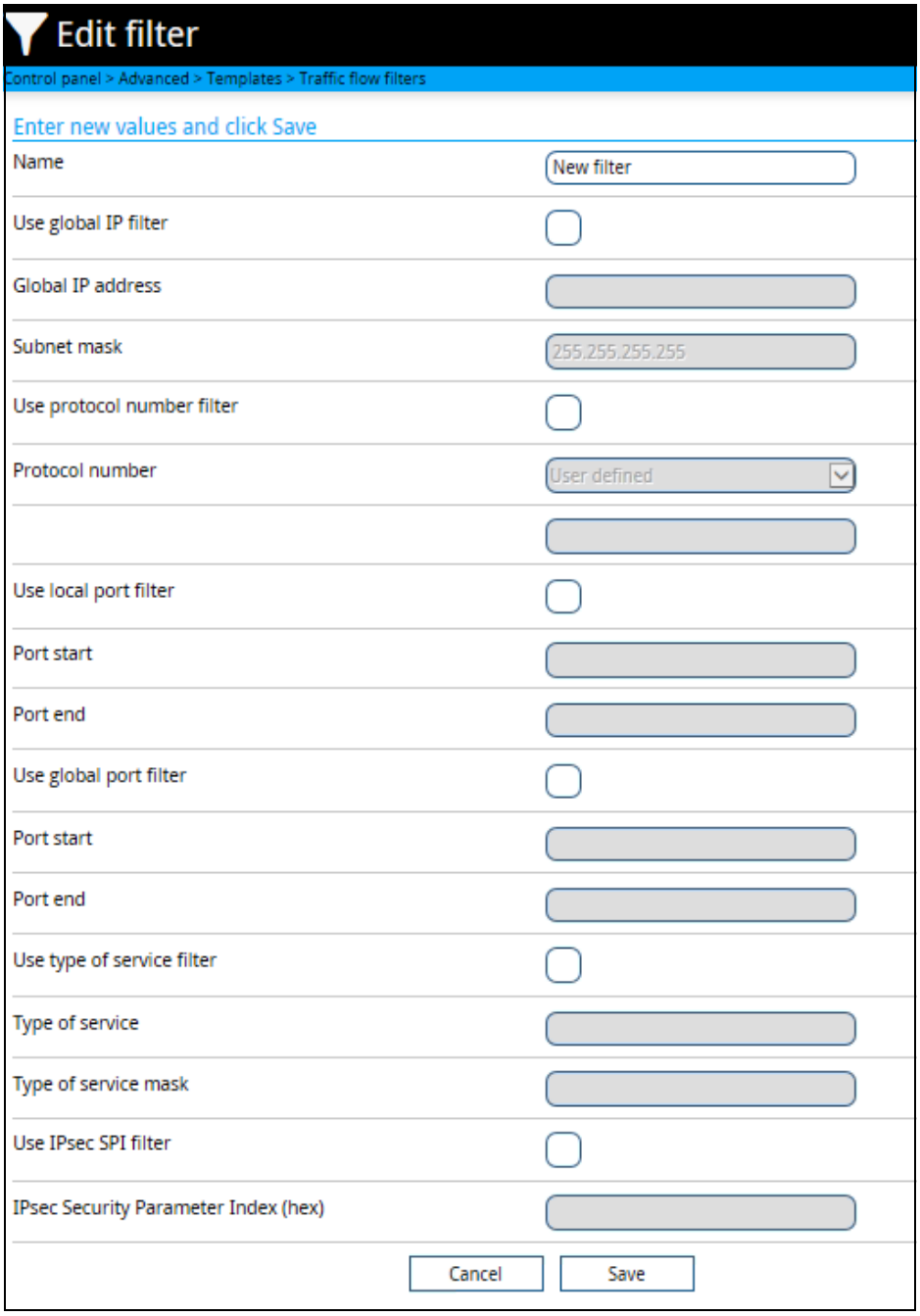
You can also select **No filter**. This option is only suitable for the last connection you add to a connection package, because the filters are applied in the order they are added to the connection package. See *Multiple data connections* on page 51.

If the predefined filters do not meet your requirements, you can create additional filter templates. Do as follows:

1. Under **Advanced**, select **Templates**.
2. Select **Traffic flow filters**.



3. To delete a traffic flow filter, click ? in the right side of the filter tile.
4. To add a new traffic flow filter, click **Add template** and proceed with the next steps.



5. Type in a suitable name for the filter.

6. Select the item(s) you want to use for filtering and enter the details for the item(s). You can select one or more of the following items:
   - Use global IP filter.
     Traffic to and from the IP address or network (subnet mask) entered here is automatically routed to the connection type associated with this traffic flow filter.
   - Use protocol number filter.
     This is the type of protocol that is used for the data traffic. E.g. if this is set to 17 (UDP), the filter will automatically route UDP data traffic to the connection type associated with this traffic flow filter.

- Use local port filter.
  This is a range of local port numbers on the terminal. The filter will route traffic to and from any of these port numbers to the connection type associated with this traffic flow filter.
- Use global port filter.
  This is a range of global port numbers on the terminal. The filter will route traffic to and from any of these port numbers to the connection type associated with this traffic flow filter.
- Use type of service filter.
  Type of Service (TOS) is used to define the Quality of Service. Set this value to a number between 0 and 255.The filter will route traffic with this Quality of Service to the connection type associated with this traffic flow filter.
- Use IPsec SPI filter.
  IP security. The filter will route traffic using the Security Parameter Index (SPI) stated here (in hexadecimal numbers) to the connection type associated with this traffic flow filter.

7. Click **Save**.

The new filter will now be available for selection when you add new connections to a connection package.

Example: You want a connection package, which allows you to use uninterrupted Voice over IP while having a Standard data connection for web browsing etc. Do as follows:

1. Create a filter template with
   - Protocol=UDP (Use protocol number filter)
   - Type of Service = 0xb8 and Type of Service mask = 255 (Use type of service filter)

   The UDP protocol is suitable for UDP voice streaming and the TOS value 0xb8 is used by some linksys Voice over IP adapters.
2. Create a connection package as described in *Multiple data connections* on page 51.
3. Add an additional connection, e.g. Streaming 32 with the new filter you created in step 1.
4. Add a Standard connection with No filter.

Help desk

Under Help desk you can enter the contact information you want for your EXPLORER 323. 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**.

Reset button

You can change the function of the Reset button. See *Reset button* on page 103. 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 323 restarts (power cycle) and resets LAN and WLAN settings, 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 and reset LAN and WLAN settings) will still work.
   - **Disabled**: The Reset button will not have any function.
3. Click **Save**.

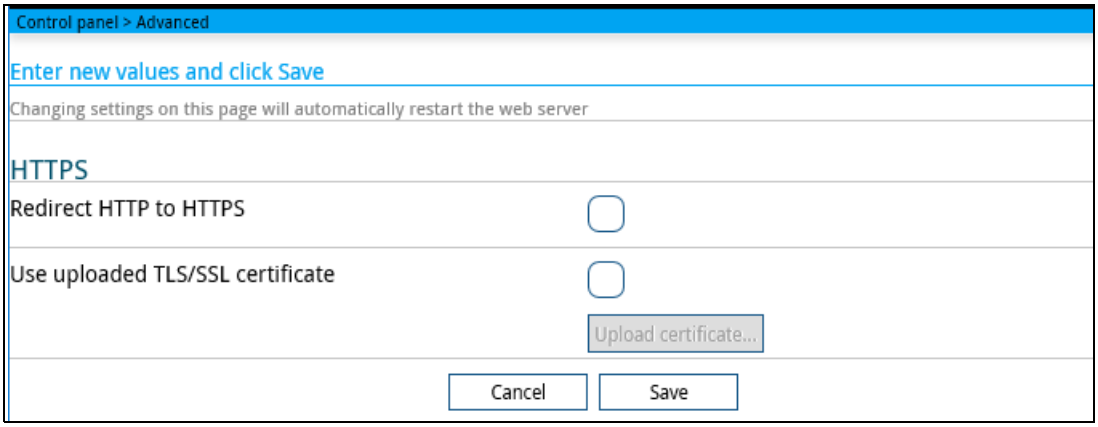
Security

The EXPLORER 323 internal web server supports HTTPS, which includes encryption of the exchanged web traffic when accessing the EXPLORER 323 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. From the **Advanced** page select **Security**.



2. Select **Redirect HTTP to HTTPS** if you want the EXPLORER 323 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**.

To enter the SIM PIN in the web interface

Do you need a SIM PIN?

Note

You may not have to enter a SIM PIN to access the terminal. This depends on whether or not the use of a SIM PIN is enabled on your SIM card 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 80
- *Auto SIM PIN validation* on page 81

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 323 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 81.

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 the terminal is pointed or trackingand the correct PIN is entered, you are ready to make calls or access the Internet.

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 cancelling 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**.
3. Type in your PIN and click **OK**.

Maintenance and troubleshooting

Support

Contact information

Should your Cobham SATCOM product fail, please contact your dealer or installer, or the nearest Cobham SATCOM partner. You will find the partner details on www.cobham.com/satcom, **Technical Service Partner List**. You can also access the **Cobham SYNC Partner Portal** at https://sync.cobham.com/satcom, 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.

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 323 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. 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.

Software update

Remote software update

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 126.

To upgrade the software

If you have an M2M subscription, the EXPLORER 323 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 323, use one of the following:
   - a computer connected to the Internet, see *To access the terminal using AT commands* on page 33, or
   - equipment capable of sending and receiving SMS messages, see *Remote access with SMS* on page 37.

   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.

1. You can download the software from the "Cobham SYNC Partner Portal" at www.cobham.com/satcom, select **Cobham SYNC Partner Portal** > **Downloads**. Locate the EXPLORER 323 software.

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 the next section.

To update software locally with the web interface

To update the software in the EXPLORER 323, 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 323.

   Note Connect to the LAN interface of the EXPLORER 323. Depending on your system configuration, you may have to connect through 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 44.
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 323 now restarts and completes the software update.

   Note The update procedure takes a couple of minutes.

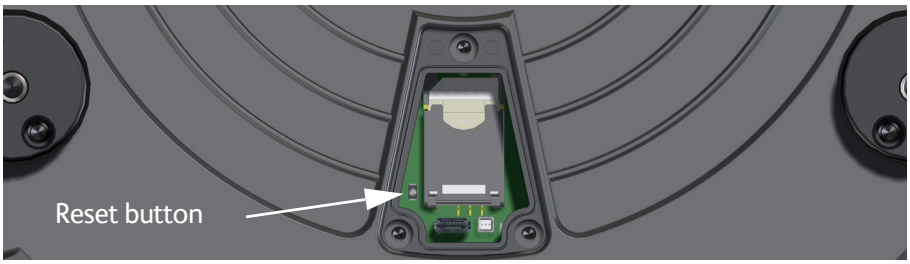
You can check the software version under **Control panel** > **Support** > **About**.

1. You can download the software from the "Cobham SYNC Partner Portal" at www.cobham.com/satcom, select **Cobham SYNC Partner Portal** > **Downloads**. Locate the EXPLORER 323 software.

Reset button

How to access the reset button

The Reset button is located inside the SIM compartment in the bottom of the EXPLORER 323.



Do as follows:

1. Loosen the three screws holding the cover for the SIM compartment.
2. Remove the cover.
3. Use a pointed device to push the Reset button. The function depends on the length of time you press and hold the button, see below.
4. Close the cover and tighten the three screws carefully.
   This is important in order to maintain the IP grade of the EXPLORER 323.

Functions of the reset button

The EXPLORER 323 has a Reset button that has three functions: 1) To restore all settings to factory settings, 2) to restore LAN and WLAN settings only and 3) to put the EXPLORER 323 into safe mode for recovery software upload.

Note You can set up in the web interface which functions should apply to the Reset button. See *Reset button* on page 97.

Action	Function
Push and hold the Reset button for 2 seconds	**LAN settings**: The terminal IP address and IP netmask are temporarily set to the default value (default IP address: 192.168.0.1). **WLAN settings** are restored to default. Default WLAN settings: • WLAN is **Disabled** • Broadcast SSID: **EXPLORER323** • Encryption standard: **WPA2-AES** • Encryption key: **serial number** of the EXPLORER 323 • Region: **Other**, i.e. the most restrictive setting

Action	Function
Push and hold the Reset button for > 10 seconds	The EXPLORER 323 restores factory settings and restarts the system. All changes to the configuration are lost.
While the EXPLORER 323 is booting, push and hold the Reset button	The EXPLORER 323 enters safe mode.

Maintenance

Cleaning the EXPLORER 323

Clean the exterior of the EXPLORER 323 with a damp cloth.

CAUTION! Do not spray water directly on the EXPLORER 323 with high pressure! The EXPLORER 323 can be washed gently, but it is not designed to be exposed to high pressure water-jets. The EXPLORER 323 is IP66.

Disposal of the EXPLORER 323

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.

Troubleshooting

Status signaling

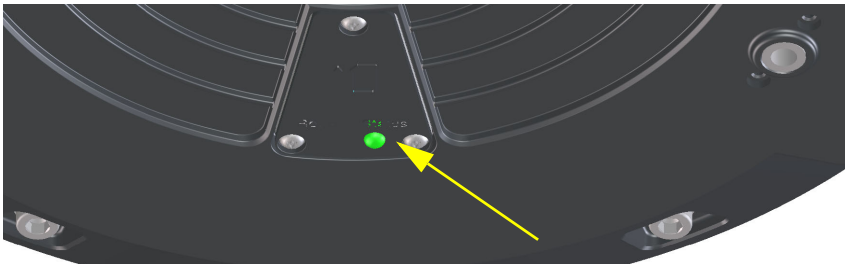
Means of signaling

The EXPLORER 323 system provides various methods for signaling the status of the system.

- **LED** in the bottom of the EXPLORER 323 is used to signal:
  - Power on/off
  - Status
  - Software update
  - Warnings
  - Errors
- **Event messages** with warnings or errors are shown in the web interface.

LED signaling

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



The functions of the LED are:

Light pattern		Meaning
●	Green flashing rapidly	Starting up.
●	Yellow flashing	Antenna searching for BGAN satellite signal
●	Green flashing	Antenna tracking on BGAN satellite signal.
●	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.
●	Blue flashing rapidly	Safe mode.
○	Off	Power off or Power save state.

Event messages and status messages

In the web interface of the EXPLORER 323 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.

List of messages

The following list explains some of the messages that may show in the web interface of the EXPLORER 323.

Displayed text	Explanation	Remedy
A destructive LTE blocker level is detected - Rx is temporarily switched off	A cellular network signal is interfering severely with the satellite signal. The LTE blocker resilience function of the terminal has switched off reception of the satellite signal (RX).	If possible, move the terminal to another location with lower LTE blocker level. You can disable the LTE blocker resilience with an AT command, see *_ILTEBLCK* on page 130.
Antenna sky-scan malfunction	There is an error with the sky-scan function of the antenna.	Contact your supplier
Automatic activation failed. Reconnecting...	The terminal failed to automatically activate a Standard data connection at start-up, even though it was configured to do so.	Wait for the terminal to reconnect.
Closing all connections due to high temperature	High temperature is causing the terminal to close all current connections.	Wait for the terminal to cool down. If possible, move to a cooler place.
Closing terminal due to high temperature	Critically high temperature is causing the terminal to power off.	Wait for the terminal to cool down. If possible, move to a cooler place.
Connection closed. Connection watchdog (Link monitoring) failure.	The terminal has closed the connection because Link monitoring failed.	TBD
Connection closed. Temperature too high.	The connection is closed because the temperature is too high.	Wait for the terminal to cool down. If possible, move to a cooler place.
Connection failed	The terminal failed to establish a connection.	Restart the connection e.g. from the Dashboard in the web interface. See *Manual activation of data connections* on page 30.

Displayed text	Explanation	Remedy
Connection lost	The data connection was lost.	Restart the connection e.g. from the Dashboard in the web interface. See *Manual activation of data connections* on page 30.
Data or time limit exceeded	The data connection is closed because a data limit defined in the web interface is exceeded. The data limit may be set to avoid unintentional use of bandwidth, e.g. if you forget to close a connection after use.	Restart the connection e.g. from the Dashboard in the web interface. See *Manual activation of data connections* on page 30. You can change the data limits in the web interface under Advanced > Data limits.
Data rate reduction due to high temperature	The data rate is reduced because the temperature is too high.	Wait for the terminal to cool down. If possible, move to a cooler place.
Error in SIM reader	The SIM reader is not able to read the SIM card.	Contact your supplier.
Error opening software file	A wrong file name may have been entered with the AT command _IUPDFW.	Use the command **_IUPDFW?** to show the correct file name before updating.
Network failure	There is a problem with the network, e.g. congestion.	Try again later. If the problem persists, contact your airtime provider.
Network failure. Reconnecting...	There is a problem, with the network, e.g. congestion. The terminal tries to reconnect because it is set up for Automatic Context Activation.	Wait for the terminal to reconnect. If the problem persists, contact your airtime provider.
No connection to terminal...	The (LAN or WLAN) connection to the terminal is lost. The terminal may be in the process of rebooting.	Try connecting again. Check that you have the correct IP address for the terminal. See *To connect to the LAN interface* on page 18 and *To connect your WLAN-enabled device* on page 19.
No position fix	The terminal was not able to get a position fix from the positioning system (GPS, GLONASS or BeiDou)	Make sure the terminal has free line of sight. If the problem persists, contact your supplier.

Displayed text	Explanation	Remedy
Online software update failed	Remote software update failed.	Try again later. If the problem persists, contact your distributor.
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.
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: no network resources, wrong APN, or 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.
Preparing for software update	The terminal is preparing to update the software.	Wait for the software update to complete.
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.
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.
Satellite signal lost	The system no longer receives a signal from the satellite.	Make sure the antenna has a clear view to the satellite.
SIM blocked	The SIM card is blocked because You have entered too many wrong SIM PINs and PUKs.	Contact your airtime provider for a new SIM card.
SIM heater - temperature too low - SIM disabled	The temperature was too low for the SIM heater to be able to warm up the SIM card.	Move the terminal to a warmer location.
Software update failed	The terminal was unable to upload new software to the antenna.	Reboot the terminal. Contact your supplier if the problem persists.
Software update forced roll-back	Something went wrong with the software update, so it was rolled back to the previous version	Check that you have the correct software version and try again.
Software update is already started	You tried to start a software update when someone else had already started one.	Wait until the software update is completed.

Displayed text	Explanation	Remedy
Software update still fails after several retries	The terminal was unable to upload new software to the antenna.	Contact your supplier.
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.
Software update transfer timeout	The system timed out before the software file was transferred to the terminal.	Try again later.
Software version is already installed	You are trying to update the software to a version that is already installed.	Check your existing software version, e.g. in the web interface under **Control panel** > **Support** > **About**.
Standard data speed limited due to high temperature	The bit rate of the data channel is reduced because the temperature is too high.	Wait for the terminal to cool down. If possible, move to a cooler place.
Temperature sensor error	The temperature sensor does not work properly.	Contact your supplier.
Temperature too high (critical)	Critically high temperature is causing the terminal to shut down.	Wait for the terminal to cool down. If possible, move to a cooler place.
Temperature too low (critical)	Critically low ambient temperature is causing the performance of the terminal to be degraded or halted.	Move the terminal to a warmer place.
Terminal temperature high	High ambient temperature may cause the performance of the system to be degraded or halted.	Wait for the terminal to cool down. If possible, move to a cooler place.
Terminal temperature too low	Low ambient temperature may cause the performance of the terminal to be degraded or halted.	Move the terminal to a warmer place.
The selected satellite is not visible at current position	The terminal cannot find the satellite selected in the user interface. You may have selected the wrong satellite for your geographic location.	See *To select the preferred BGAN satellite* on page 64.

Displayed text	Explanation	Remedy
The terminal has re-registered due to a high LTE blocker level	A cellular network signal is interfering with the satellite signal and caused the terminal to reregister.	If possible, move the terminal to another location with lower LTE blocker level. You can disable the LTE blocker resilience with an AT command, see *_ILTEBLCK* on page 130.
Too high temperature warning	High ambient temperature is causing the performance of the system to be degraded or halted. The bit rate is reduced.	Wait for the terminal to cool down. If possible, move to a cooler place.
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 place.
Unknown connection problem	There is an unknown problem with the connection.	Restart the connection e.g. from the Dashboard in the web interface. See *Manual activation of data connections* on page 30. If the problem persists, contact your airtime provider.

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

Specifications

EXPLORER 323 terminal

General specifications

Characteristics	Specification
Type	BGAN Class 12, land-vehicular one-box terminal with switched-beam antenna (no moving parts)
Services	
Voice	4 kbps AMBE+2
Data	
Standard IP	Up to 284/225 kbps (270/158 kbps for elevations < 20 degrees)
Streaming IP	32 or 64 kbps[a]
SMS	Up to 160 characters
Interfaces	
Wired	One combined connector with: • DC power input • Ethernet interface, 10/100 Mbps • Remote on/off
Wireless	2.4 GHz WLAN interface, standard: 802.11 b/g
Frequencies	
Inmarsat I-4	
Transmit	1626.5 - 1660.5 MHz
Receive	1525.0 - 1559.0 MHz
Inmarsat Alphasat	Extended L-Band[b]:
Transmit	1626.5-1660.5 MHz and 1668.0-1675.0 MHz
Receive	1518.0 - 1559.0 MHz
G/T	≥-18.5 dB/K, for elevations between 20° and 90° ≥-19 dB/K, for elevations between 5° and 20°
EIRP	10 dBW ±3dB

a. 64 kbps Streaming is only available in elevations higher that 20 degrees.
b. The extended frequency range (Extended L-Band) is only available within Alphasat coverage. For coverage area, see *Satellite coverage* on page 117.

Characteristics	Specification
Dimensions	Diameter: 320 mm Height: 97 mm including plastic spacers (87 mm without spacers)
Weight	3900 g / 8.6 lbs including spacers
Mounting	With 3 bolts through the vehicle roof, or Optional: Magnetic Mount Solution, order number 403723A-009 (3 magnetic feet)
Supply Voltage	12 VDC to 24 VDC (-10% to + 30% measured at the terminal)

Power consumption

Power consumption at 12 V operation

State of the terminal at 12 V	Typical power consumption
Power save state (configured for Remote on/off))	0.18 W
Idle (no active PDP context, LAN active)	3.9 W
Idle (no active PDP context, WLAN active)	4.1 W
Active PDP context - primarily received traffic (LAN active)	9.5 W
Active PDP context - primarily received traffic (WLAN active)	10.3 W
Active PDP context - primarily transmitted traffic (LAN active)	24.8 W
Active PDP context - primarily transmitted traffic (WLAN active)	25.7 W
Active PDP context - bidirectional traffic (LAN active)	26.9 W
Active PDP context - bidirectional traffic (WLAN active)	25.7 W

Power consumption at 24 V operation

State of the terminal at 24 V	Typical power consumption
Power save state (configured for Remote on/off))	0.29 W
Idle (no active PDP context, LAN active)	3.8 W
Idle (no active PDP context, WLAN active)	4.0 W
Active PDP context - primarily received traffic (LAN active)	9.1 W
Active PDP context - primarily received traffic (WLAN active)	10.1 W
Active PDP context - primarily transmitted traffic (LAN active)	23.5 W
Active PDP context - primarily transmitted traffic (WLAN active)	24.3 W
Active PDP context - bidirectional traffic (LAN active)	25.4 W
Active PDP context - bidirectional traffic (WLAN active)	24.4 W

Environmental specifications

Characteristics	Specification
Water and dust	IP66 (with cable inserted)
Ambient temperature Operating Survival Storage	 -25˚C to +55˚C at min. 1 m/s windload -40˚C to +80˚C -40˚C to +85˚C
Relative humidity	up to 95% non-condensing at 40˚C
Ice, survival	Up to 25 mm of ice (non-operational)
Wind	Relative wind speeds up to 200 km/h
Vibration, operational	Random vibration of 1.05 G RMS in each of three mutually perpendicular axes. The spectrum of the vibration is as follows: • 5 to 20 Hz: 0.02 G^2/Hz • 20 to 150 Hz: -3dB/octave
Vibration, survival	Random vibration of 1.7 G RMS for a period of two hours in each of three mutually perpendicular axes (six hours total). The spectrum of the vibration is as follows: • 5 to 20 Hz: 0.05 G^2/Hz • 20 to 150 Hz: -3dB/octave
Vehicle motion	Turning rate: 40˚/s Turning acceleration: 50˚/s^2 Induced acceleration: 0.5 G Velocity: Maximum vehicle velocity 110 km/h with the Magnetic Mount Solution, 200 km/h for bolt mounting.
Shock, survival	Half sine wave shock with a peak of 20 G and a period of 11 ms.

Outline dimensions

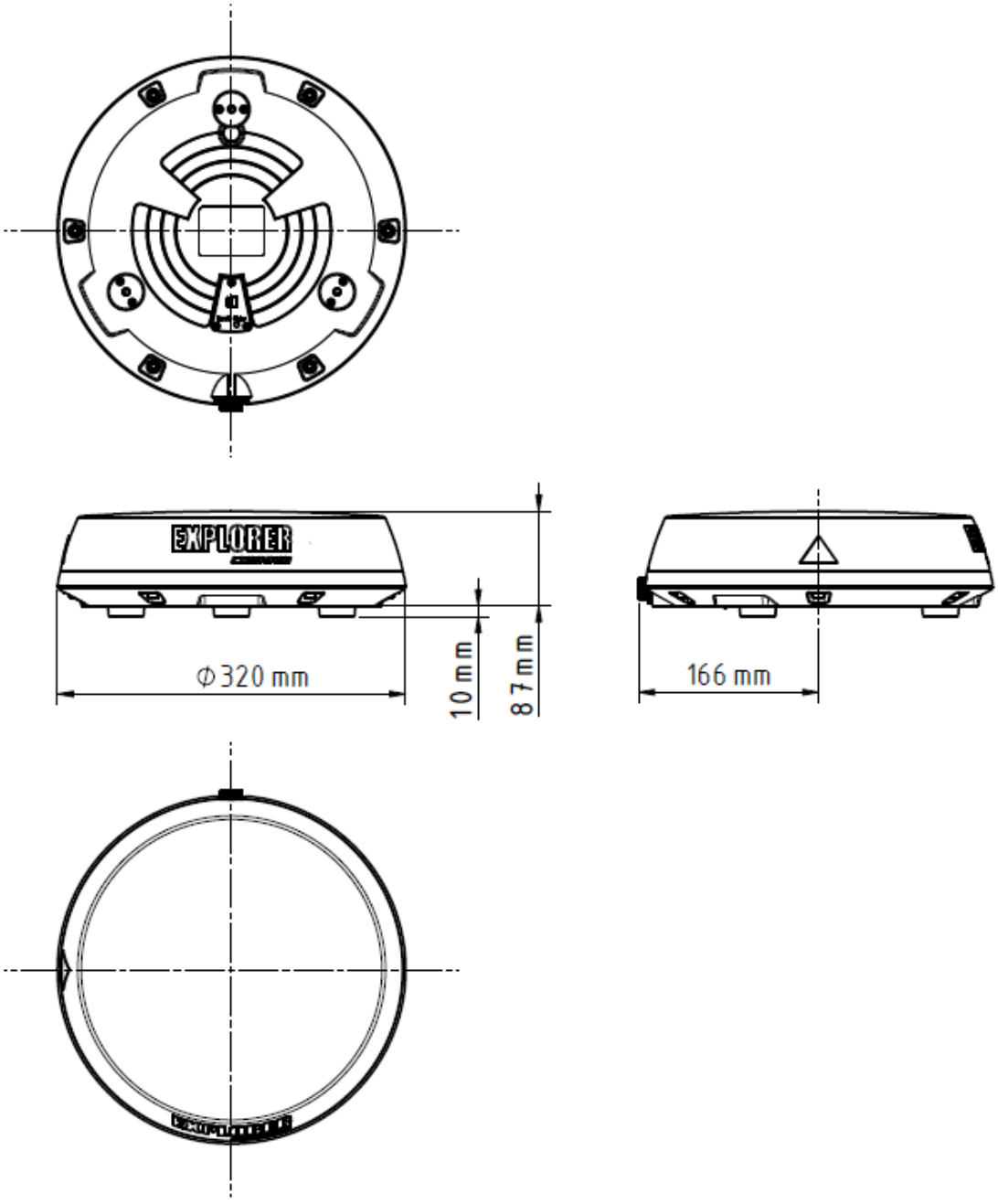
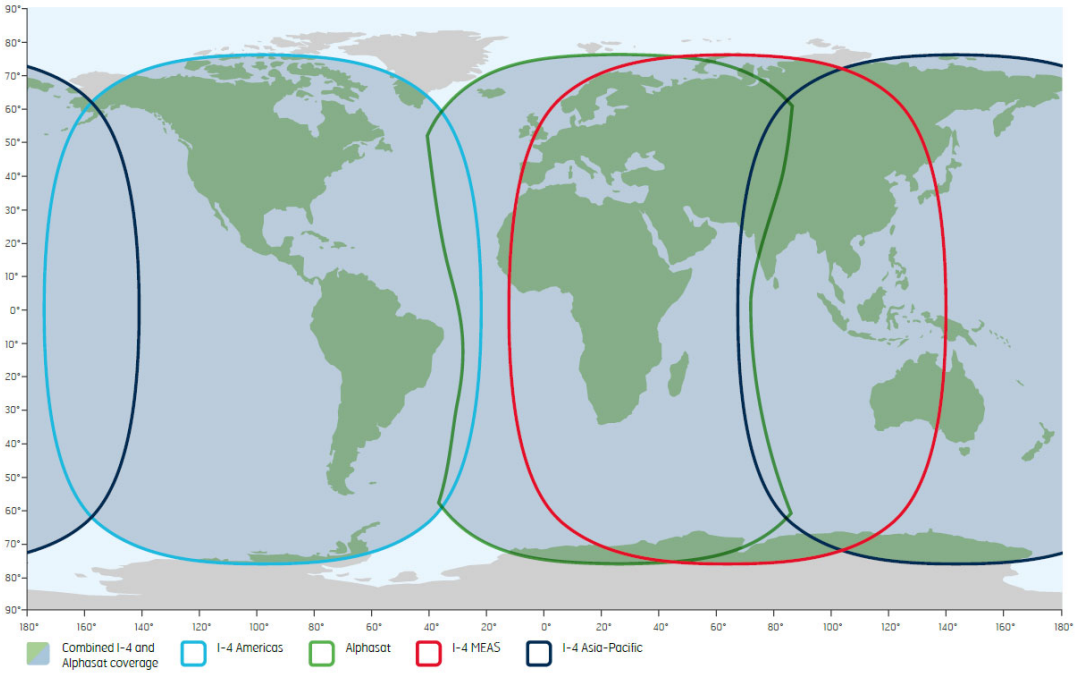


Figure 1-1: EXPLORER 323 outline dimensions drawing

Satellite coverage

The Inmarsat BGAN services are based on geostationary satellites situated above the equator. Each satellite covers a certain area (footprint). The coverage map below shows the footprints of the BGAN system. For updated information on coverage, see Inmarsat's home page at inmarsat.com.

Note In low elevations (below 20˚), performance is limited. This means that 64 kbps is not available and max. data rates for Standard data are lower, that is 270 kbps down/ 158 kbps up instead of 284 kbps down/ 225 kbps up.



Command reference

This appendix lists the function, syntax and parameters for commands used with the EXPLORER 323. You can send commands to the EXPLORER 323 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*
- *Configuration examples*

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		
Disable LTE blocker resilience	_ILTEBLCK	X		
Get input voltage of the EXPLORER 323	_ITDCIV	X	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
Configuration of Terminal Watchdog function	ADVWATCHDOG			X

SMS remote commands

This section describes syntax and parameters for the SMS commands. For examples of use, see *Remote access with SMS* on page 37

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 323.

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).

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>
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 126.
<category>	1	Delete only Read SMS messages.
	2	Delete Read and Sent.
	3	Delete All except Unread.
	4	Delete All SMS messages.
<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 323, 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 1 NA	Send ping only if no traffic. Always send ping, regardless of data traffic. Placeholder when no value is specified. Note that the existing setting applies.
<ping_interval>	<integer> NA	Interval between pings (minutes). Placeholder when no value is specified. Note that the existing setting applies.
<ping[1/2/3]>	<IP addr> NA	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. Placeholder when no IP address is specified. Note that any previously entered IP address is maintained.
<pos_response>	0 1 NA	Send an sms response[a]. Do not send an sms response[a]. Placeholder when no value is specified.
<pwd>	<APN password> NA CLR	Password associated with APN username. Placeholder when no APN password is specified. Note that any previously entered password is maintained. 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 1 2 3	None – send no responses to AT commands. Immediate - immediate responses, but not unsolicited. Final – suppress immediate if OK, plus unsolicited. 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> NA	The phone number to be used for sms response Placeholder when no value is specified.
<user>	<APN user name> NA CLR	User name associated with APN. Placeholder when no APN user name is specified. Note that any previously entered user name is maintained. User name is not used.

a. Position SMS response is only for future use, and should be set to NA

Parameter	Values	Meaning
<wakeup>	0 1 NA	
<wdog_enable>	0 1 NA	Disabled. Enabled. 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 2	Get watchdog configuration. Set watchdog parameters.

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 323 IP and not be the EXPLORER 323 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 323.
ERROR: TERMINAL BUSY	An ACTIVATE or DEACTIVATE command is in progress.
INVALID RESTART REQUEST	Attempt to perform restart before EXPLORER 323 has been running for at least 15 minutes.
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).

AT commands

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

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 323.

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 126 and *Parameters for other M2M related AT commands* on page 130.

ATCO commands

The table below summarizes the ATCO commands, i.e. AT commands that can be used in the SMS command **ATCO**.

Command	Parameters
_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>

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 1	Disable. 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 323.

Parameter	Values	Meaning
<ip_addr_lo>	<ip_addr_lo>	IP address of the HTTP client that should be allowed remote access to the EXPLORER 323, or, 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 323 to use for getting or saving a file.
<mode>	0 1	Deferred activation. 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. 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 RS	The type of password is administrator password. 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. _ISENDFILE: could not open local file. _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.

Code	Text	Explanation
_IUPDFW command codes		
50	New firmware file not found	Could not find specified filename.
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 323's own PDP context, to which an HTTP connection may be made.

Other AT commands

Command	Parameters
_ICLCK	<type>,<enable>,<passwd>
_IMACLOC	<enable>,<interface>[,<interface>]
_IMACLOCAD	<action>,<interface>,<MAC Address>[,<MAC Address>][a]
_IPWSAVSCHD	<psmode>,<psvalue>
_ITREMONOFF	<active mode>,<power down delay>,<awake time of day>,<awake duration>,<polarity>
_ISMSRMT	<enable>
_ITDCIV	No parameters[b]
_ILTEBLCK	<enable>

a. Up to 10 MAC addresses may be specified.
b. Type **_ITDCIV?** to get the input voltage (in mV) of the EXPLORER 323

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 1	Delete. Add.
<active>	0 1	Inactive. The GPIO pin is in its inactive state. Active. The GPIO pin is in its active state.
<active mode>	0 1	Inactive. Remote on/off is not used. Terminal is set to Always on. 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 1	Disable. Enable.
<interface>	0	0 means Ethernet interface. This is the only option.
<MAC Address>	<MAC Address>	MAC address(es) for MAC locking. Up to 10 MAC addresses are permitted.
<passwd>	<passwd>	The existing administrator password.
<polarity>	HIGH LOW	The Power control pin will be active high. 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 TOD_TRG WOL_STATUS	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. 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 323 wakes up from power save state. 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> <HH:MM> 0 or 1	Used with IDLE_TRG (above). Number of minutes (e.g. 15). Used with TOD_TRG (above). Time of day in UTC time (e.g. 23:30). Used with WOL_STATUS (above). 0 is Off and 1 is On

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.

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.

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)
<destination port range>	<destination port range>	Destination port range in the form **From.To** To indicate only one port number, type in the same port number under From and To. **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> 0	The guaranteed bit rate down link (32, 64, 128). If the parameter is set to '0' the subscribed value will be requested.
<Guaranteed bitrate UL>	<Guaranteed bitrate UL> 0	The guaranteed bit rate up link (32, 64, 128). If the parameter is set to '0' the subscribed value will be requested.
<h_comp>	0 1	Header compression off (default if value is omitted) Header compression on (manufacturer preferred compression)
<Max bitrate DL>	<Max bitrate DL> 0	The maximum bit rate down link (32, 64, 128). If the parameter is set to '0' the subscribed value will be requested.
<Max bitrate UL>	<Max bitrate UL> 0	The maximum bit rate up link (32, 64, 128). 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.

Parameter	Values	Meaning
<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**. See <destination port range> for example.
<state>	0 1	Deactivate. Activate.
<Traffic Class>	1 3	Streaming (not available for M2M subscription). Standard data (Background).
<Transfer delay>	0 500 4000	0 ms, error correction is determined by the network 500 ms, error correction is disabled 4000 ms, error correction is applied

Configuration examples

Remote 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 *To set up remote access with IP* on page 87.

Note If remote SMS command access has been disabled, you can enable it either using the web interface (*To set up remote access with SMS* on page 88) or using the AT command _ISMSRMT (*M2M related AT commands* on page 126). Note that you must have configured **at least one trusted phone number** that can send and receive SMS to and from the terminal.

Relevant command:

_IREMWEB

See *ATCO commands* on page 126 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, 87.123.189.119

   In this example the command specifies:
   - **2**: no immediate response, only when the global IP address is sent along.
   - **remote**: The remote SMS password
   - **1**: Enable remote access to web interface
   - **87.123.189.119**: The IP address that 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 323 should now return an SMS response with the external IP address of the terminal.

   Example:_IREMWEB: 81, Global IP: 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 323 (received in the response above).

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

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 33.

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

- Remote on/off
- Idle time and Daily wake-up

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 *To connect Ignition* on page 12.

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 35), 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 323 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.

Conformity

CE

The EXPLORER 323 terminal is CE certified as stated in the simplified EU Declaration of Conformity enclosed at the end of this appendix.
The complete EU Declaration of Conformity can be found on the Cobham SATCOM web site as described in the simplified EU Declaration of Conformity.

FCC

FCC id for EXPLORER 323 terminal: ROJ-3723A

Contains FCC id: Z64-WL18SBMOD

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.

IC

IC id for EXPLORER 323 terminal: 6200B-3723A

Contains IC id: 451I-WL18SBMOD

This device contains license-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's license-exempt RSS(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.

This Class [B] digital apparatus complies with Canadian ICES-003.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique 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.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada.

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:

Directive 2014/53/EU concerning Radio Equipment (RED)

Equipment included in this declaration

Model	Description	Part no.
TT-3723A	EXPLORER 323 Terminal	403723A-THR-001

The full text of the EU declaration of conformity is available at the following internet address:

http://sync.cobham.com/satcom/support/downloads

Document no.: 99-171948-A

A

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

C

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

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.

F

FUP	Firmware Upgrade Process.

G

GLONASS	GLObal'naya NAvigatsionnaya Sputnikovaya Sistema. Global Navigation Satellite System in English.
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

ICMP	Internet Control Message Protocol. An Internet protocol mostly used for diagnostics.
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	Internet Protocol.
IPsec	Internet Protocol Security. A protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.

L

LTE	LTE stands for Long-term Evolution, and is the path followed to achieve 4G speeds in wireless broadband networks. LTE applies more generally to the idea of improving wireless broadband speeds to meet increasing demand.

M

M2M	Machine-to-Machine
MAC	Media Access Control address. A hardware address that uniquely identifies each node of a network.

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.

P

PIN	Personal Identification Number. A code number used to provide access to a system that has restricted access.
PUK	PIN Unblocking Key. An eight-digit code used to unblock a SIM card after three incorrect PINs have been entered. The PUK code is supplied with the SIM card.

S

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.
SPI	Security Parameter Index. An identification tag added to the header while using IPsec for tunneling the IP traffic.
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, preventing criminals from reading and modifying any information transferred, including potential

personal details.

T

TLS — Transport Layer Security. An updated, more secure, version of SSL.

U

UTC — Coordinated Universal Time. The International Atomic Time (TAI) with leap seconds added at irregular intervals to compensate for the Earth's slowing rotation. Leap seconds are used to allow UTC to closely track UT1, which is mean solar time at the Royal Observatory, Greenwich.

V

VoIP — Voice Over IP. The routing of voice conversations over the Internet or through an IP-based network.

W

WLAN — Wireless Local Area Network

A

access
limit in web interface, 79
remote, 37
using AT commands, 33
accessories, 3
admin password
change, 78, 79
log in, 78
log out, 79
advanced settings, 78
alerts
view in web interface, 75
antenna
clearance to base plane, 7
drainage, 7
installation, 6
installation location, 6
interference, 6
magnetic mount, 10
obstructions, 6
radiation, 6
APN
set up for BGAN, 50
set up for PPPoE, 69
app for smartphone connection, 20
AT commands
access with IP, 33
list of, 118
remote access with IP, 39
automatic activation of data connection, 55
Automatic Context Activation, 55
automatic shut down
connection, 86

B

backup configuration, 81
BGAN
connecting to, 22
bridge mode, 63

C

cable and pinout, 11
calibration
mounting direction, 23
call charges
estimating in web interface, 86
call log, 60
calls
make, 41
missed, received, outgoing, 60
total usage, 60
CE compliance, 139
charges for calls
estimating, 86
clearance
antenna to base plane, 7
command reference, 118
computer, connecting to LAN, 18
computer, connecting to WLAN, 19
condensation in antenna, 7
configuration
copy, 81
IP handsets and smartphones, 66
LAN, 65
save or load, 81
WLAN, 65
conformity, 139
connect power, 12
connected devices
manage, 70
connecting to the BGAN network, 22
connection
automatic shut down, 86
connection packages
multiple connections, 51
connections
dedicated, 56
multiple, 51
contact information, 100
contents in delivery, 4
Control panel, 59

D

data
limits, set, 86
log, 60
Standard, definition, 29
start or stop connection, 30
Streaming definition, 29
total usage, 60

data connections
automatic activation, 55
dedicated, 56
start and stop in web interface, 47
dedicated connections, 56
default IP address, 44
delivery
contents, 4
items included, 4
devices
manage, 70
diagnostics report
create, 75
disposal, 104
drainage of antenna, 7

E

Event log, 75
EXPLORER Connect app
overview, 20

F

factory settings
restore, 80
FCC compliance, 139
features, 2
forward port, 68

G

GNSS
select system, 64

H

HTTP, redirect to HTTPS, 97
humidity in antenna, 7

I

IC compliance, 139
ignition function, 17
IMEI, 77
IMSI, 77
installation
antenna, 6
interference, 6
Internet connection, 18, 19
set mode, 63
IP address
for web interface, 44
local, setting up, 63
IP addresses, reserved, 111
IP handset
manage in the terminal, 66
SIP settings, 40
user name and password, 66
items included in delivery, 4

L

LAN
automatic activation of data, 55
configure, 65
connect an IP handset, 26
connecting a computer, 18
language
change in web interface, 64
LEDs on front panel, 105
limit
allowed kB, 86
allowed time, 86
data, 86
limiting user access, 79
load configuration, 81
location of terminal, 6
log
of calls, 60
of data connections, 60
of events, 75
log in as administrator, 78
log out as administrator, 79

M

MAC address
connected devices, 70
magnetic mount for antenna, 10
maintenance, 104
manage connected devices, 70
maximum for data, 86
microwave radiation, ii
mount antenna with bolts, 8
mount antenna with magnets, 10
mounting calibration, 23
multiple data connections, 51

N

navigation in web interface, 46
navigation system
select, 64

O

obstructions
distance and size, 6

options, 3

P

part numbers, 3
password
  change, 78, 79
  log in, 78
  log out, 79
  smartphone or IP handset, 66
permissions
  setting for users, 79
phone
  SIP settings, 40
phone call, 41
PIN
  changing for BGAN, 80
  enabling or disabling for BGAN, 80
  enter in web interface, 99
  entering, 21
  entering in web interface, 21
place the antenna, 6
port forwarding, 68
positioning system
  select, 64
power connection, 12
power save functions
  Idle time, 138
PUK code, 22

R

radiation, ii
radiation hazard, 6
radiation level, 6
registering on the BGAN network, 22
remote management
  access using AT commands, 39
  access using web interface, 37
  activation with SMS, 37
  preparation, 38
  set up in web interface, 87
remote on/off, 17
repack for shipment, 100
report
  diagnostics, 75
reserved IP addresses, 111
Reset button
  change function, 97
  location and function, 103
restore factory settings, 80
return units, 100
rights for users
  in web interface, 79
router mode, 63

S

safety summary, ii
save configuration, 81
serial number, 77
settings
  in web interface, 59
  limit access, 79
  restore, 80
SIM card, insert, 5
SIP settings, 40
smartphone
  manage in the terminal, 66
  SIP settings, 40
  user name and password, 66
SMS
  activate data connection, 37
SMS commands, 120
  list of, 118
  parameters summary, 121, 134
  summary, 120
software
  update with web interface, 76, 102
  version, 77
specifications, 112
Standard data
  definition, 29
start data connection, 30
status
  view in web interface, 57
Streaming data
  definition, 29

T

terminal watchdog
  with web interface, 84
total usage, 60
tracking the terminal, 42
  setup in web interface, 73
Traffic control, 70
troubleshooting, 105
typography used in this manual, v

U

unpack, 4
update software, 76, 102

usage
calls and data, 60
user name
smartphone or IP handset, 66
user permissions
setting up in web interface, 79

V

vehicle
compliance, 6
VoIP phones
setup, 66

W

warning messages, 75
warranty, 100
web interface
accessing, 44
change language, 64
definition, 44
navigating, 46
WLAN
configure, 65
connecting a computer, 19

Cobham Public