TABLE OF CONTENTS

1 INTRODUCTION 2
1.1 Welcome 2
1.2 Contacts for your Service 2
1.3 What Happens if your Vehicle is Stolen 3
1.4 Periodic Health Check for your Device 4
1.5 Driver Card 4
1.6 Override code / emergency disarming 4
2 USING SPECIAL MODES 6
2.1 Transport Mode 6
2.2 Garage Mode 6
2.3 Forced unset Mode 6
3 CONNEX GUARDIAN SERVICE DETAILS 7
3.1 Private Service 7
3.2 Personal Service 9
3.3 Service with WEB option (Private/Personal) 11
GLOSSARY 16

1 INTRODUCTION

Congratulations on purchasing one of the following **Connex Guardian** services:

- Private
- Private with WEB Option
- Personal
- Personal with WEB Option

This **User Manual** describes how to use these services. Where there are differences, the specific service names will be mentioned in italics. When you have completed and signed the Stolen Vehicle Recovery Service Agreement it should be given to the Service Provider (NSP) in order to test and activate your Stolen Vehicle Recovery service as soon as it is fitted to the vehicle.
This Stolen Vehicle Recovery Service Agreement is part of the Service Manual which also contains the telephone numbers of the Service Provider (NSP) and Secure Operating Centre (SOC). You will need these numbers to interact with the service operators.
Please keep your Service Agreement with this manual.

1.1 Welcome

In addition to the Service Manual, you will receive a Welcome Letter. This contains your client number, your contract number and information on how to contact the Service Provider (NSP) and Secure Operating Centre (SOC). Please keep this information safe. When your contract is activated, you will receive a Welcome message on your mobile phone. If you have chosen the ***WEB Option*** service, your password will be sent to you in the Welcome Message.

1.2 Contacts for your Service

To access the Service Provider (NSP) or the Secure Operating Centre (SOC), simply call the Phone Number which you can find in your Service Manual. You will be guided by a step-by-step voice menu to use the following functions:

1.2.1 Secure Operating Centre (SOC)

You should contact the Secure Operating Centre (SOC) for Voluntary Theft Declarations or setting Special Modes. These are described later in this manual. The Secure Operating Centre (SOC) number can be found in the Service Manual.
If your device detects a theft, the Secure Operating Centre (SOC) intervenes; an operator will contact you and ask you for some data to open your file. You will then be asked the identity questions which you have indicated on the Connex Guardian contract form. You must answer these questions correctly.
The Secure Operating Centre (SOC) is active 24 hours a day, 365 days a year.

1.2.2 Service Provider (NSP)

Should you require any information relating to your service, contact the Service Provider (NSP). If at any time you need to change any details you have entered in the Connex Guardian Service form or if you sell your vehicle, you must immediately contact the Service Provider (NSP).

Examples of a change of contact/vehicle details are:

- you change your mobile phone number,
- you change the registration number to your vehicle,
- you change your address,
- you change/forget your identity questions/answers.

The Service Provider (NSP) can be contacted during normal office hours (see Terms and Conditions in the Service Manual).

Important:
Change your identity questions.
The identity questions/answers specified in your Stolen Vehicle Recovery Service Agreement are preliminary. The answers are known to the dealer. Therefore, we strongly recommend that you change the identity questions/answers by calling the Service Provider (NSP).

1.3 What Happens if your Vehicle is Stolen

The device installed in your vehicle can detect a number of parameters about the vehicle. When these are detected, messages (also known as alerts) are sent to the Secure Operating Centre (SOC) and/or your mobile phone.
Depending on the Connex Guardian service you have subscribed to, certain messages may start the theft tracking automatically. You can also start the theft tracking by contacting the Secure Operating Centre (SOC) and voluntarily declaring the vehicle as stolen. For details of the different services, please see Chapter 3.

1.3.1 You Detect that your Vehicle is Stolen

If you detect that your vehicle has been stolen you can start the theft tracking by a Voluntary Declaration.

You should:

1. Contact the Secure Operating Centre (SOC) immediately. The Secure Operating Centre (SOC) will commence tracking your vehicle.
2. Follow the Secure Operating Centre (SOC) instructions precisely.
3. For UK services you will need to contact the local Police to report the theft and obtain a Crime Reference Number which you will then provide to the Secure Operating Centre (SOC).

1.3.2 The System Detects that your Vehicle is Stolen

If your device detects an event which it interprets as a possible theft, the theft tracking is started immediately and the device informs the Secure Operating Centre (SOC). They will contact you immediately to verify the theft and then proceed with recovering the vehicle, liaising with the appropriate authorities. Depending on the service to which you have subscribed, the device can alert the Secure Operating Centre (SOC) in the following cases:

- Vehicle Intrusion
- Unauthorised movement of the vehicle, i.e., your vehicle is moved without the ignition key ON.
- Attempted tampering of the device in your vehicle.
- Radio Frequency Jamming
- A hijack attempt

In these cases, an alert will automatically be triggered. The Secure Operating Centre (SOC) will then contact you to verify that the theft is genuine. Upon your confirmation, the tracking and localisation of your vehicle will start immediately.

1.3.3 What happens if your Vehicle is Stolen Abroad?

Your first point of contact is always your National Secure Operating Centre (SOC) using the phone number which appears in your *Service Manual*. The Secure Operating Centre (SOC) will then re-direct the confirmed theft to the Secure Operating Centre (SOC) in the country of theft in order to track the vehicle and liaise with the Police authorities in the local language and abiding to local laws.

1.4 Periodic Health Check for your Device

Your device is self-monitoring. It periodically performs a health check. If a potential problem is detected during the Health Check, the Service Provider (NSP) will contact you to perform additional checks. The Service Provider (NSP) may ask you to have the system checked at a dealer.
This Service is provided exclusively by the Service Provider (NSP) based on the End User's Terms and Conditions.

1.5 Driver Card

The Connex Guardian services feature a radio frequency device which is the Driver Card.
The device can also be connected to the vehicle's CAN bus. This allows the use of the vehicle's original key control to arm and disarm the system (i.e., when opening and closing the doors).

1.5.1 Arming and disarming of the system

If you have a Driver Card, the device will automatically detect the presence of the card to disarm the system. Alternatively, when the Driver Card is no longer detected, the system is armed.
If the Driver Card is not detected (for example, the battery is very low), the Override code can be used to disarm the system.

1.6 Procedure to override the engine with emergency code (override code)

When the service is activated, you will be sent a welcome message which will also include your emergency code (override code) to unlock the engine locally.
This code can be used in case of lack of driver card, lack of GSM network (attempt to jamming) or unable to contact the SOC.

In case of lack a driver card, the emergency code is also able to disarm the system for about five minutes, allowing you to start the vehicle without generating false alarms.

The following is the procedure to do:

Note: first be sure to have with you the emergency code to four digits.

1. Turn ON the ignition and leave the key in the ON position for at least 2 min.
2. Turn OFF the ignition and leave it in this position for a time equivalent to the value of the first digit of your code multiplied by 10 s
3. Turn ON the ignition and leave it in this position for a time equivalent to the value of the second digit of your code multiplied by 10 s
4. Turn OFF the ignition and leave it in this position for a time equivalent to the value of the third digit of your code multiplied by 10 s

5. Turn ON the ignition and leave it in this position for a time equivalent to the value of the fourth digit of your code multiplied by 10 s

6. Turn OFF the ignition

7. Start the engine

If the engine does not start, repeat the procedure from step 1.

Example with emergency code equivalent to "1234":

- Turn ON the ignition for 2 min.
- Turn OFF the ignition for 10 s
- Turn ON the ignition for 20 s
- Turn OFF the ignition for 30 s
- Turn ON the ignition for 40 s
- Turn OFF the ignition
- Start the engine

Note: If you enter a wrong emergency code for at least five attempts during the same day, it will be notified to you and you will have to wait at least five minutes before repeat the unlock procedure.

In case you are not aware of such attempts, immediately contact the security center.

2 USING SPECIAL MODES

To avoid your service generating false theft alerts in certain special conditions, there are 3 *Special Modes* that can be used:

- Transport Mode
- Garage Mode
- Forced Unset Mode

These modes can be used separately or in any combination. It is also possible to set the duration for each of these modes.

To set these modes, either:

1. Call the Secure Operating Centre (SOC) to request that the system be set to Transport, Garage or Forced Unset mode, or a combination. If you are not sure, just describe why you think you need a *Special Mode* and the operator will apply the appropriate settings.
2. If you have subscribed to the ***with WEB option*** service you can set these Special Modes yourself using the web application. Instruction for using the web application can be found in the web application on-line help.

2.1 Transport Mode

This mode inhibits the alerts that would be generated by unexpected movement of the vehicle, such as the Unauthorised Movement alerts.

Transport Mode needs to be set if the vehicle is to be transported:
- by train
- by ferry
- by vehicle transporter
- by tow truck
- or is likely to move for any other reason with the ignition OFF

2.2 Garage Mode

This mode inhibits the alerts that would be **generated by unexpected tampering** with the vehicle, such as the **sabotage alerts**.

Garage Mode needs to be set if:

- the vehicle is to be serviced
- the battery is to be disconnected
- dealer maintenance on the device is to be performed

2.3 Forced Unset Mode (for systems with Driver Card)

This mode inhibits alerts that would be generated by the **vehicle moving without the presence of the Driver Card**.

Forced Unset mode needs to be set if:

- you have forgotten your Driver Card and you wish to use the vehicle without it
- the Driver Cards are not working
- any situation where you need to use the vehicle but the device cannot be disarmed in the normal manner

3 CONNEX GUARDIAN SERVICE DETAILS

There are the following services in the Guardian service family:

- Private
- Private with WEB option
- Personal
- Personal with WEB option

The details of these services are described below.

3.1 Private service

The ***Private*** service comes to arm/disarm the system with the original vehicle remote control (CAN bus), this provides an extra level of protection as the system can be armed and disarmed using the vehicle original remote control.

This service will generate an alert in the following cases.

Unauthorised Movement

This alert is triggered when vehicle motion is detected with the ignition switched OFF.

There are 2 ways in which your ***Private*** service protects your vehicle from illegal movement:

1. When you switch OFF the vehicle ignition, the device uses its GPS to set the vehicle position and define an “autozone” of 400 metres (100 metres UK) around the vehicle. If the vehicle moves outside of this “autozone” without the ignition being switched on, an alert is sent to the Secure Operating Centre (SOC). They will contact you immediately.
2. With the ignition switched OFF, if the device detects 4 consecutive speed measurements greater than 8 kph (5 mph) an alert is sent to the Secure Operating Centre (SOC). They will contact you immediately.

Tamper

If the device sensors detect an attempt to sabotage the device, an alert is sent to the Secure Operating Centre (SOC). They will contact you immediately.The sabotage can be either to the GPS antenna or to the device itself. These alerts can be sent in error if the car is taken to a garage for maintenance and the *Garage Mode* is not set (see section 2.2).

Jamming

The device can detect jamming of the GSM frequencies.
As soon as the device can use the GSM network, an alert is sent to the Secure Operating Centre (SOC). They will contact you immediately.

3.1.1 Options to the Private Service

In addition to the standard protection the following options can be added to the ***Private*** service and will generate a theft alert:

External Alarm Connection

If there is an external alarm connected to your device, when this alarm is triggered (i.e., the alarm siren sounds). an alert is also sent to the Secure Operating Centre (SOC). They will contact you immediately.

Panic Button Connection

If a Panic Button is connected to your device, when this is pressed, an alert is sent to the Secure Operating Centre (SOC). They will contact you immediately.

Perimetric Alarm Connection

The device can detect an intrusion if the vehicle doors are opened while the system is armed. This will send an alert to the Secure Operating Centre (SOC). To avoid this alert being sent when you open the doors to use the vehicle, this feature can be enabled/ disabled using the original vehicle key to disarm the system.

***Note*: These features require a specific installation of the device. If you wish to add them after the device has been installed, you may be required to return to the Installer.**

3.1.2 What Messages You Will Receive

In addition to the protection offered by the ***Private*** service, the device monitors various other parameters and will send messages to you to help you manage your service. These messages are described in the table at the end of this manual.

3.2 Personal service

The ***Personal*** service comes with a Driver Card.
When the device detects the Driver Card, the device is disarmed. This does not mean that the vehicle is not protected, only that certain events will not send an alert to the Secure Operating Centre (SOC).
When the Driver Card is no longer detected, the device becomes armed. In this mode, there are different events that will trigger an alert to the Secure Operating Centre (SOC).
If you have the option to arm/disarm the system with the original vehicle remote control (CAN bus), this provides an extra level of protection as the system can be armed using the original vehicle remote control only and disarmed using the vehicle original remote control and carrying the Driver Card.

The ***Personal*** service automatically protects your vehicle against a number of events:

Unauthorised Movement

This alert is triggered when vehicle movement is detected with the ignition switched OFF.

There are 2 ways in which your ***Personal*** service protects your vehicle from unauthorised movement:

1. When you switch OFF the vehicle ignition, the device uses its GPS to set the vehicle position and define an “autozone” of 400 metres (100 metres UK) around the vehicle. If the vehicle moves outside of this “autozone” without the ignition being switched on, an alert is sent to the Secure Operating Centre (SOC). They will contact you immediately.
2. With the ignition switched OFF, if the device detects 4 consecutive speed measurements greater than 8 kph (5 mph) an alert is sent to the Secure Operating Centre (SOC). They will contact you immediately.

Tamper

If the device sensors detect an attempt to sabotage the device, an alert is sent to the Secure Operating Centre (SOC). They will contact you immediately.The sabotage can be either to the GPS antenna or to the device itself. These alerts can be sent in error if the car is taken to a garage for maintenance and the *Garage Mode* is not set (see section 2.2).
The device sabotage is detected when the device is armed.

Jamming

The device can detect jamming of the GSM frequencies.
As soon as the device can use the GSM network, an alert is sent to the Secure Operating Centre (SOC). They will contact you immediately.

3.2.1 Options to the Personal Service

In addition to the standard protection the following options can be added to the ***Personal*** service and will generate a Theft alert

External Alarm Connection

If there is an external alarm connected to your device, when this

alarm is triggered (i.e., the alarm siren sounds).

Panic Button Connection

If a Panic Button is connected to your device, when this is pressed, an alert is sent to the Secure Operating Centre (SOC). They will contact you immediately.

Perimetric Alarm Connection

The device can detect an intrusion if the vehicle doors are opened while the system is armed.

***Note*: These features require a specific installation of the device. If you wish to add any of them after the device has been installed, you may be required to return to the Installer.**

3.2.2 What Messages You Will Receive

In addition to the protection offered by the ***Personal*** service, the device monitors various other parameters and will send messages to you to help you manage your service. These messages are described in the table at the end of this manual.

3.3 Service with WEB option (*Private/Personal*)

The ***service with Web option*** functions in exactly the same way with respect to the vehicle protection, Driver Cards, etc. In addition, it provides a Web application for you to manage your service.

Your Client ID is your Client Number which is in the Welcome Letter.

Your password will be sent to you in the Welcome Message.

To login:

- go to the Cobra Connex site: https://myweb.cobratelematics.com
- enter your Client ID (Client Number) and password in the window below.

To learn how to use the web application, click on the ***Help*** tab to bring up the on-line help.

The web application allows you to:

1. Perform service management tasks:
   - Locate your vehicle
   - Define the GeoFence alert (Zone in/out definition)
   - Define vehicle speed alert
   - Arm/Disarm the system remotely (only with *Personal Web*)
   - Manage Special modes
2. Perform administration tasks
   - Change your personal codes
   - Configure the way in which you receive alerts
3. Manage multiple vehicles of a Multiple Vehicle contract.
   - Selecting a vehicle
   - Managing Account Managers

The on-line help provides full details of these features including detailed descriptions of each window and how to navigate through the application.

3.3.1 What Messages You Will Receive

In addition to the protection offered by the ***service with web option***, the device monitors various other parameters and will send messages to you to help you manage your service. These messages are described in the table below:

Message type	Reason for Message	Your Actions
Welcome Message	This message is sent when your service is activated. It contains the “Override code” to disarm the system in case of emergency. It contains also the password to access your WEB application.	None.
Codes Transmission	Your personal codes can be resent or regenerated and resent by the Service Provider (NSP) or by the Secure Operating Centre (SOC).	Keep these codes safe.
Theft Alert	This message is sent if the device has sent a theft alert to the Secure Operating Centre (SOC).	If possible, check the state of the vehicle. If the Secure Operating Centre (SOC) does not contact you immediately, you should contact them.
Vehicle Ignition On Alert	This message is sent to you when the vehicle ignition is switched on while the system is armed.	In case it is not a false alert (you forgot to disarm the system) contact the Secure Operating Centre (SOC).
Zone entry Alert	This message is sent to you when the vehicle enters the zone you have set through the WEB application.	
Zone exit Alert	This message is sent to you when the vehicle exits the zone you have set through the WEB application.	
Automatic deletion of Zone failed	This message is sent to you if the configured time period for the GeoFence has passed but the Connex system has been unable to delete the zone in the device.	Access your WEB application and delete the zone.
Garage Mode active for more than xx days	This message is received when the device has been set to Garage Mode for more than the expected number of days.	Contact the Secure Operating Centre (SOC). If the Garage mode is still required, it can be reset.

Message type	Reason for Message	Your Actions
Transport Mode active for more than xx days	This message is received when the device has been set to Transport Mode for more than the expected number of days.	Contact the Secure Operating Centre (SOC). If the Transport mode is still required, it can be reset.
Device disarmed for more than xx days	This message is received when the device has been set to Forced Unset Mode for more than the foreseen number of days.	Contact the Secure Operating Centre (SOC). If the Forced Unset mode is still required, it can be reset.
Driver Card Battery Low	The device has detected that the battery voltage of the Driver Card is low.	Contact your Service Provider (NSP).
Vehicle Speed Alert	The device has detected that your vehicle has exceeded the speed limit you have set in your web application.	
Vehicle Battery Low	The device has detected that the voltage of the vehicle battery is low (11.1 volts for a normal 12 volts battery).	Check your vehicle battery. Charge if required.
Wrong Override Code	The device has detected those have been digit 5 wrong Override Codes in a day.	If you don't know of those attempts, contact immediately the Secure Operating Centre (SOC).

Declaration of Conformity

The Manufacturer hereby declares, at its sole responsibility, that the following products:

Description: **GPS Control unit for vehicles + Driver Card**

Models: **4C2221ACB (CONTROL UNIT) and 2791B0 (DRIVER CARD)**

are in conformity with the essential requirements of European Directive 1999/5/EC.

The products have been tested against the following Standards and Specifications:

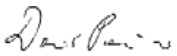
EMC :	**EN 301489-1 v.1.9.2, EN 301489-3 v.1.4.1, EN 301489-7 v.1.3.1, EN 301489-19 v.1.2.1**
Safety:	**EN 60950-1:2006 + A1:2010 + A11:2009 + A12:2011, EN 50385:2002, EN 62479:2010**
Radio Spectrum:	**EN 301511 v.9.0.2 , EN 300440-2 v.1.4.1**

The products are marked with the following CE marking and Notified Body number according to European Directive 1999/5/EC.

CE 0681

March 13, 2013

Dario Parisi
Products Homologation Engineer



Device:	The device fitted to your vehicle which communicates with the Cobra servers for vehicle tracking in case of theft.
Connex Guardian:	The name of the Connex service family.
Driver Card:	A radio frequency card which communicate with the device. When the device detects the presence of the Driver Card, the system is UNSET and the vehicle can be used.
GPS:	Global Positioning System. A network of satellites used to detect the geographic location of the vehicle.
GSM:	Global System for Mobile communications. A standard used for mobile telecommunications systems worldwide.
CAN bus:	Controller area network. The infrastructure used by the different electronic units of the vehicle to communicate each other.
Identity Question:	These questions are used to identify you when you contact the Service Provider (NSP) or Secure Operating Centre (SOC). You agree identity questions with the dealer when you purchase the service. However, for security, you can change these once the service is activated.
Jamming:	A technique used by thieves to block the radio frequencies used by GSM.
Login:	The process of entering your user name and password to enter the web option of the Personal service with WEB option.
Override Code:	The code you enter on the Remote Control to override the system arming and to manage the Garage and Transport modes.
Service Provider (NSP):	The entity which manages your service. You can contact them using the number indicated in your *Service Manual*.
Secure Operating Centre (SOC):	The entity that will track your vehicle and communicate with the local police if your vehicle is stolen. You can contact them using the number indicated in your *Service Manual*.
Theft Tracking:	If your vehicle is stolen, the fitted device will send location information to the Secure Operating Centre (SOC) in such a way that its position can be relayed to the local police.
Web Application:	The Connex Guardian application that allows you to manage certain parameters of your service.
Welcome Letter:	A printed letter you receive when signing the contract. It contains your contract number and client number.
Welcome Message:	A message you receive on your mobile telephone when the service is activated.