NESIE 2
User Manual
Software Version 2.10.6

CONTENTS

1. HOW TO USE THIS MANUAL

This user manual is not designed as a quick start guide. The manual layout follows that of the UI.

If a quick start guide is required the user should refer to the following section on initial setup / operation.

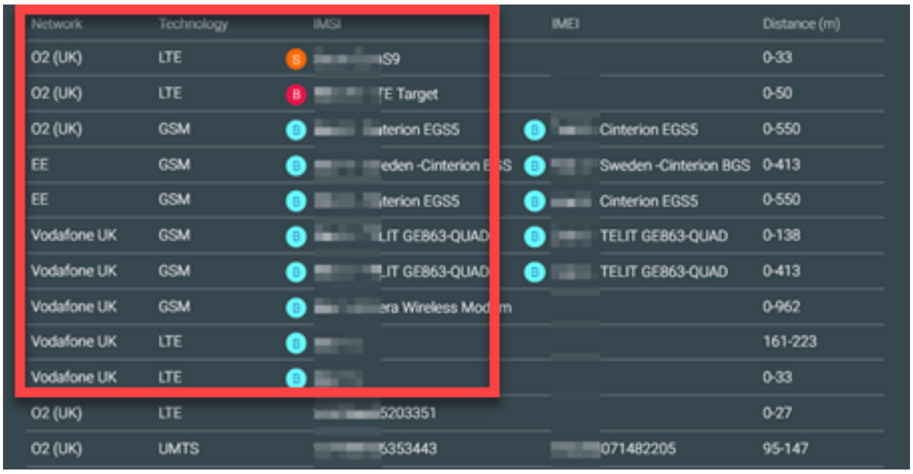
- **Log In** – section 4
- **Setting up NESIE prior to use** – section 7
- **Network Scan** – section 12
- **Conducting an ID Grab** – section 17
- **Received Data** – section 19.3

1.1 HIGHLIGHTS & BLURRED INFORMATION

In the screen shots of the User Interface different colour boxes are used to highlight sections of the screen that are of interest. These coloured boxes are not displayed on the normal use interface. They have been added for clarity when using this manual.

To hide any sensitive information that is displayed on the screenshots, some sections of the UI have been blurred. Again this is only in this manual.

An example of this highlighting and blurring can be seen below at Fig 2 below.



Network	Technology	IMSI	IMEI	Distance (m)
O2 (UK)	LTE	S S9		0-33
O2 (UK)	LTE	B 'E Target		0-50
O2 (UK)	GSM	B aterion EGS5	B Cinterion EGS5	0-550
EE	GSM	B eden -Cinterion E S	B Sweden -Cinterion BGS	0-413
EE	GSM	B terion EGS5	B Cinterion EGS5	0-550
Vodafone UK	GSM	B LIT GE863-QUAD	B TELIT GE863-QUAD	0-138
Vodafone UK	GSM	B LIT GE863-QUAD	B TELIT GE863-QUAD	0-413
Vodafone UK	GSM	B era Wireless Mod m		0-962
Vodafone UK	LTE	B		161-223
Vodafone UK	LTE	B		0-33
O2 (UK)	LTE	5203351		0-27
O2 (UK)	UMTS	6353443	071482205	95-147

Fig 1. Highlight & Blurring

2. GLOSSARY

ARFCN Absolute Radio Frequency Channel Number. A unique number given to each radio channel in GSM. The ARFCN can be used to calculate the exact frequency of the radio channel.

BTS Base transceiver Station. The radio transmitter and receiver within a cell site.

Cell ID The code transmitted by the base station that is the unique identifier for this cell.

CID Short Cell ID. The shortened version of the full UMTS cell ID.

DHCP Dynamic Host Configuration Protocol. A network management protocol in which IP addresses are dynamically assigned to network devices as opposed to each device having a fixed address.

DTG Distance to go.

FDD Frequency Division Duplexing

GPS Global Positioning System. A commonly used satellite-based radio-navigation system owned by the United States government.

GSM Global System for Mobile Communications. A standard developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols used in digital cellular networks. Often referred to as 2G.

IMEI International Mobile Equipment Identity. A unique 16-digit number used to identify a particular mobile phone. It contains a Manufacturer code, Model number, and serial number. The last digit of the IMEI is a check digit, which guards against the possibility of the equipment accepting incorrect entries.

IMSI International Mobile Subscriber Identity. A unique 16-digit number that identifies each user of a cellular network. Held on the SIM card, it contains country, network, and subscriber information. After initial registration, the actual IMSI is not used by the network which instead uses a TMSI.

LAC Location Area Code. A unique 16-digit fixed-length location area identity code, broadcast by a BTS, which identifies a group of cells for a particular area. This is also the paging area: all the cells in a LAC will page the same mobile phone with call information.

LTE Long Term Evolution. A fourth generation mobile cellular system for broadband wireless networks based on the GSM and UMTS standard. Often referred to as 4G.

MCC Mobile Country Code. A unique three-digit number transmitted by a cell site that defines the country in which it operates.

MNC Mobile Network Code. A unique two- or three-digit number, transmitted by a cell site, which defines the network operating the site.

MSISDN	The Mobile Station International Subscriber Directory Number. This is the actual phone number of the mobile. The software within the network is used to associate the IMSI/TMSI with the MSISDN. The network then uses the IMSI/TMSI to communicate with the phone. (Artemis does not use the MSISDN to identify the subscriber, instead it uses the IMSI/IMEI.)
NESIE	Network Emulation Simulation & Interrogation Equipment
PSU	Power Supply Unit.
RF	Radio Frequency.
RSSI	Relative Received Signal Strength Indicator (measured in dBm).
Rx	Receive.
SAR	Search and Rescue.
SDR	Software Defined Radio. A radio system implemented using software, rather than traditional hardware, which gives it the ability to change the frequency and modulation type.
SIM	Subscriber Identification Module. The SIM card is inserted into a cellular device to allow it to connected to a specified mobile network.
SMS	Short Message Service. A messaging system available on most cellular devices.
TA	Timing Advance. A technique used by the GSM system to ensure that the signals from multiple phones reach the cell site at the same time despite differences in distance from the site.
TAC	Type Allocation Code. The part of the IMEI that identifies the make and model of a cellular device.
TDD	Time Division Duplex
TMSI	A Temporary [International] Mobile Subscriber Identity: A temporary identifier replacement for the IMSI. Issued periodically by the network, it offers a degree of security from fraudulent use.
TRK	Track, i.e. direction of travel of the aircraft.
Tx	Transmit.
In/Out of coverage	When a mobile phone is in or out of the coverage of a cellular network. Sometimes referred to as In/Out of service.
UARFCN	UTRAN Absolute Radio Frequency Channel Number. This is a unique number given to each radio channel within the frequency bands used by the UMTS system. The UARFCN can be used to calculate the carrier frequency.
ULI	Uplink Interference. A measure of the background interference being received by the transceiver; this limits the transceiver's ability to decode low-level signals.

UI User Interface.

UMTS Universal Mobile Télécommunications Service. A third generation mobile cellular system for networks based on the GSM standard. Often referred to as 3G.

3. INTRODUCTION

The Network Emulation, Simulation, and Interrogation Equipment (NESIE) system is designed to capture the unique identifiers from GSM, UMTS and LTE cellular devices, and the SIM cards that they contain. Every GSM, UMTS & LTE device and SIM card in the world contain these unique identifiers. These identifiers can be useful when trying check for someone’s presence at a location.

There are two types of identifiers. The first type is the International Mobile Subscriber Identity (IMSI). This is contained on each SIM card and is used to identify a cellular user so they can be billed for their usage. The second type is the International Mobile Equipment Identity (IMEI). The IMEI is contained within the cellular device and identifies the make/model and serial number of the user equipment; network providers can use this to block stolen devices from access to the network.

To obtain these identities, the NESIE system emulates a network so that the device will try and register for services. This is called creating a “dummy cell”. When the device tries to register, the NESIE system allows it to proceed with the registration process. During the registration process, the NESIE requests the two identities from the device. These are then stored in a database for analysis. Finally, the NESIE system rejects the devices attempt to register, so that it returns to the real network and can make calls normally.

When the NESIE system is transmitting, it will normally capture many of these identities. Using this process at different locations, where a Target person is known to be present, it is possible to find the exact identities carried by that Target. Once the Targets identities are known, you can check for their presence at any location.

The NESIE system is designed to be easy to use and very little knowledge of cellular systems are required to use it.

3.1 WHAT IS AN IMSI GRAB

An IMSI grab is the process of transmitting a fake cellular network (or Base transceiver Station) in order to attract the cellular device off the real cellular network, onto the fake network. When the devices move over to the fake cellular network, they are persuaded to release the identities. These identities are logged. If the identities are not ‘wanted as Targets’, they are thrown back to the real network. If the identities match the Target list (and depending on the desired actions), they will be interacted with and moved to the next stage.

An IMSI grab can be brOKen down into 6 phases:

3.1.1 LISTEN

Listen to the real cellular network. The NESIE system listens to the real cellular network in order to extract the real settings used by the network to establish communications with the mobile devices.

NESIE usually listens to as many networks, technologies and cells as it can possibly hear.

3.1.2 COPY

The list of network settings are copied down into the database in NESIE.

3.1.3 CHANGE

When NESIE is instructed to transmit a fake BTS, the NESIE software automatically uses the copied network information, adjusts some of the settings to optimise our settings and prepares to transmit its own version of the cellular networks.

3.1.4 TRANSMIT

NESIE now transmits its ‘changed’ network settings as a fake base station. This can be a single cell or multiple cells over multiple technologies.

3.1.5 HANDSHAKE

When NESIE is transmitting the fake cell(s), mobile phones in the area see NESIE and move off the real network and onto the fake network. At this stage, the devices handshake with NESIE and are encouraged to release their identities (IMSI and IMEI). NESIE then automatically measures the distance to these devices and logs all this data into the database.

3.1.6 THROW AWAY

After logging the Identities and distance measurement, NESIE now releases (throws away) the devices back to the real network.

3.2 OTHER ACTIONS AFTER AN IMSI GRAB

The IMSI grab is the first part of any action. The grab is used to collect the identities of the mobile devices. If other actions such as Hunt, Hold, Deny etc have been selected; after the initial grab, NESIE will now make a decision on what to do with the cellular device. If the device is of no interest, it will be thrown back to the real cellular network. However, if the devices are of interest (a Target), the software will now carry out other actions on the device(s). These other actions are explained in detail.

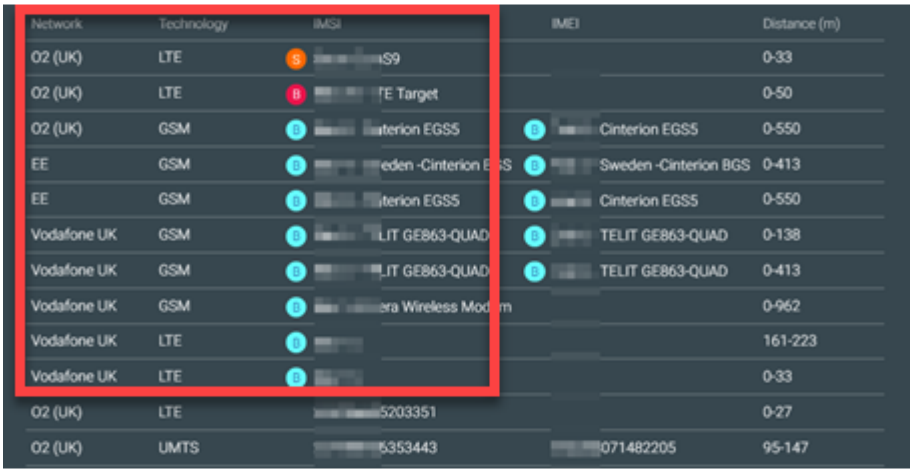
3.3 HIGHLIGHTS & BLURRED INFORMATION

In the screen shots of the User Interface (UI), different coloured boxes are used to highlight sections of the screen that are of interest. These coloured boxes are not displayed on the normal use interface. They have been added for clarity when using this manual.

To hide any sensitive information that is displayed on the screenshots, some sections of the UI have been blurred. Again this is only in this manual.

An example of this highlighting and blurring can be seen below at Fig 2 below.

When describing an icon or function on the screen, the text will be written as it is displayed on the UI.



Network	Technology	IMSI	IMEI	Distance (m)
O2 (UK)	LTE	S [redacted]S9		0-33
O2 (UK)	LTE	B [redacted]TE Target		0-50
O2 (UK)	GSM	B [redacted]terion EGS5	B [redacted] Cinterion EGS5	0-550
EE	GSM	B [redacted]eden -Cinterion E S	B [redacted] Sweden -Cinterion BGS	0-413
EE	GSM	B [redacted]terion EGS5	B [redacted] Cinterion EGS5	0-550
Vodafone UK	GSM	B [redacted]LIT GE863-QUAD	B [redacted] TELIT GE863-QUAD	0-138
Vodafone UK	GSM	B [redacted]LIT GE863-QUAD	B [redacted] TELIT GE863-QUAD	0-413
Vodafone UK	GSM	B [redacted]era Wireless Mod m		0-962
Vodafone UK	LTE	B [redacted]		161-223
Vodafone UK	LTE	B [redacted]		0-33
O2 (UK)	LTE	[redacted]5203351		0-27
O2 (UK)	UMTS	[redacted]6353443	[redacted]071482205	95-147

Fig 2. Highlight & Blurring

4. GROUP IDENTITIES

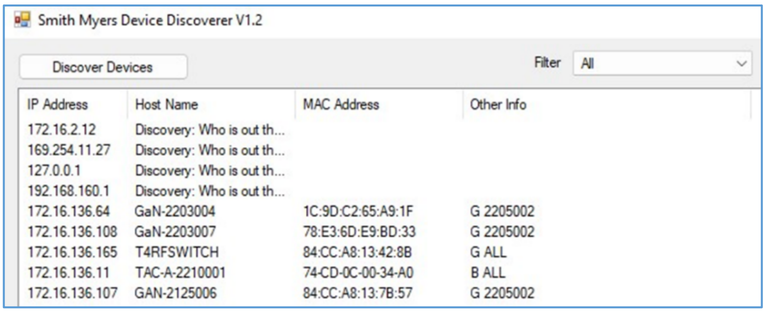
All multi transceiver NESIE systems are allocated a group identity. This identity is set on system setup. The identity is usually the serial number of the NESIE.

A group identity allows NESIE on power up, to loOK for any assets that have the same group ID, to be controlled by the Tactical control module (TCM) in the multi transceiver system (SDR's, amplifiers).

If the addresses of these assets have not got the same group ID, these assets will not be seen by the TCM. This causes a clash and the additional assets will not be visible on the STATUS page. Effectively, the assets are not being detected by the TCM and are being ignored as the group ID doesn't match.

There should be no real requirement to change the group IDs on a NESIE system, however, should the need arise, the group ID can be changed from the TCM startup page. Press the cog setting in the bottom left hand corner of the screen, but should the need arise, the following process should be followed.

Using the ethernet discoverer tool, press Discover Devices. This will populate the page with the devices connected via the ethernet port on the laptop (Fig 3).



IP Address	Host Name	MAC Address	Other Info
172.16.2.12	Discovery: Who is out th...		
169.254.11.27	Discovery: Who is out th...		
127.0.0.1	Discovery: Who is out th...		
192.168.160.1	Discovery: Who is out th...		
172.16.136.64	GaN-2203004	1C:9D:C2:65:A9:1F	G 2205002
172.16.136.108	GaN-2203007	78:E3:6D:E9:BD:33	G 2205002
172.16.136.165	T4RFSWITCH	84:CC:A8:13:42:8B	G ALL
172.16.136.11	TAC-A-2210001	74-CD-0C-00-34-A0	B ALL
172.16.136.107	GAN-2125006	84:CC:A8:13:7B:57	G 2205002

Fig 3 Ethernet discoverer

Select the asset from the list that requires the group ID changing. This will bring the item up in a separate page. In the bottom left hand corner of the page, press the cog icon (Fig 4).

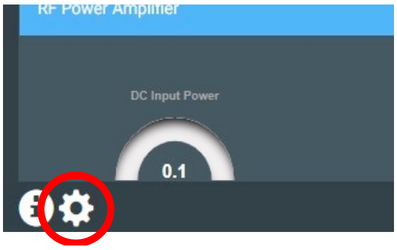
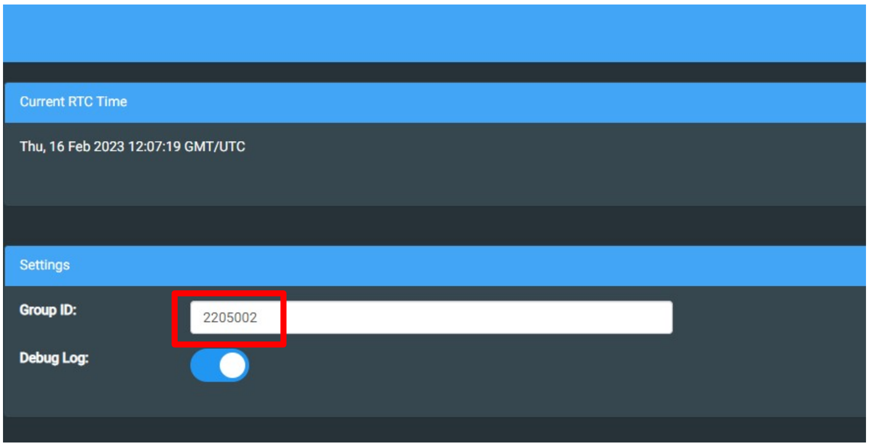


Fig 4 Cog Icon

Navigate to the group ID section of this page and chage the group ID to match the serial number of the NESIE system (minus any characters) as shown in Fig 5.



Current RTC Time

Thu, 16 Feb 2023 12:07:19 GMT/UTC

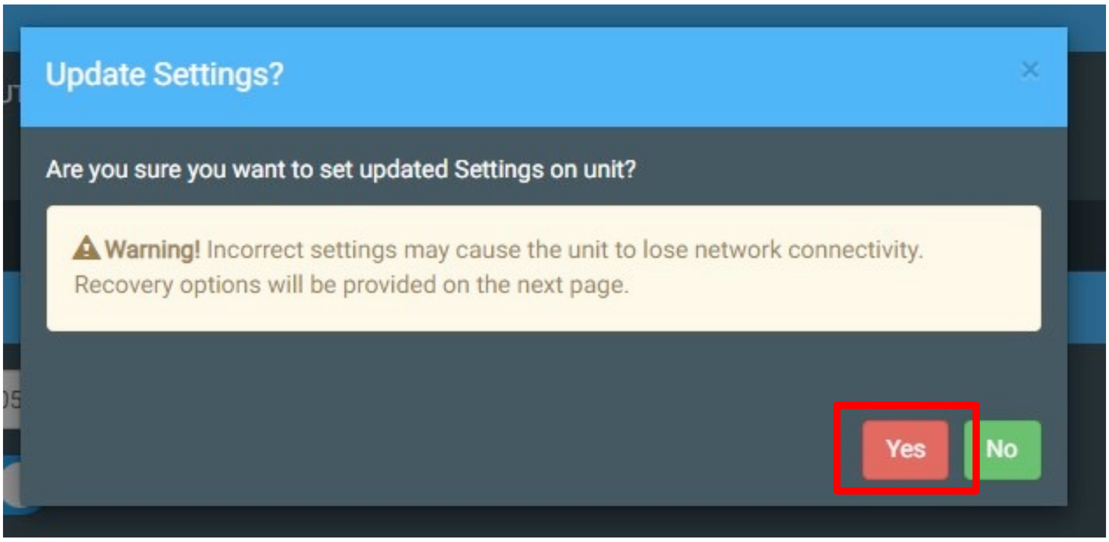
Settings

Group ID: 2205002

Debug Log:

Fig 5 Group ID Pane

Navigate to the bottom of the page where you will be asked to save the settings. A confirmation box will appear prior to closing the pop up box (Fig 6).



Update Settings?

Are you sure you want to set updated Settings on unit?

⚠ **Warning!** Incorrect settings may cause the unit to lose network connectivity. Recovery options will be provided on the next page.

Fig 6 Confirmation

5. NESIE LOG IN / LOG OUT

There are two options to log on to the NESIE system depending on whether the NESIE module is used in standalone mode or if a TCM is connected to the NESIE.

5.1 LOGIN – STAND ALONE

Power on the NESIE module and connect to the unit via an ethernet cable or Wi-Fi if appropriate.

Using a suitable web browser (Google Chrome is advised), enter the default IP address into the browser bar and click return as shown below in Fig 7 below.

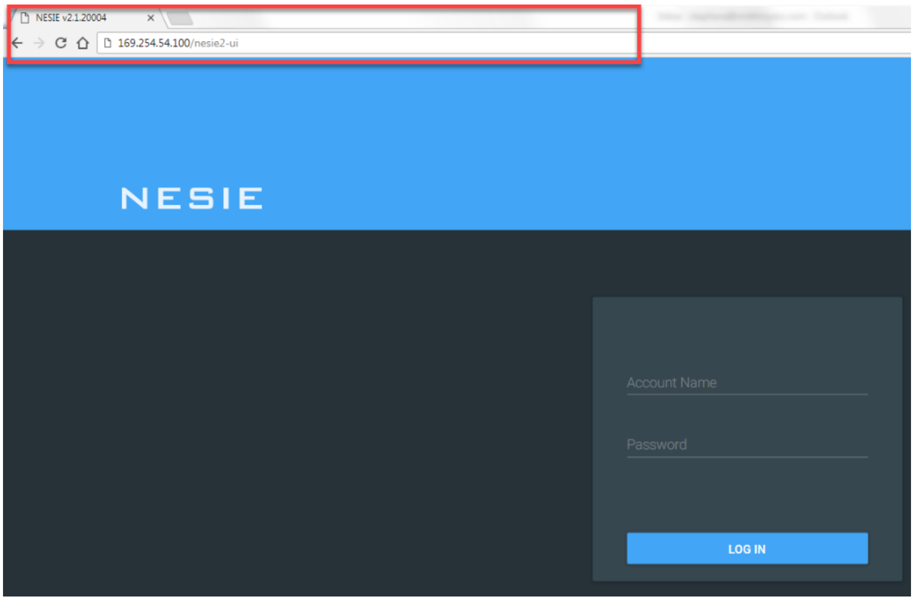


Fig 7. NESIE Log In – IP Address

The default IP addresses for the NESIE systems are listed below:

Covert NESIE – Wi-Fi:	192.168.1.254
Tactical NESIE – Wi-Fi:	192.168.1.254
Strategic NESIE:	As displayed on front panel
Tactical NESIE Controller:	As displayed on front panel
Peli NESIE Controller:	As displayed on front panel

5.2 LOGIN – CONTROL MODULE

If a control module is connected to the NESIE system, the operator will connect to this unit then log in.

To log in to the control module, the operator should read the IP address displayed in the window on the control module as shown in Fig 8 below. If the IP address is not shown, the operator should press the power button for 1 second.

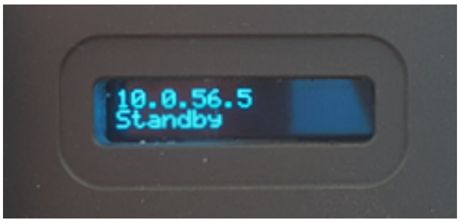
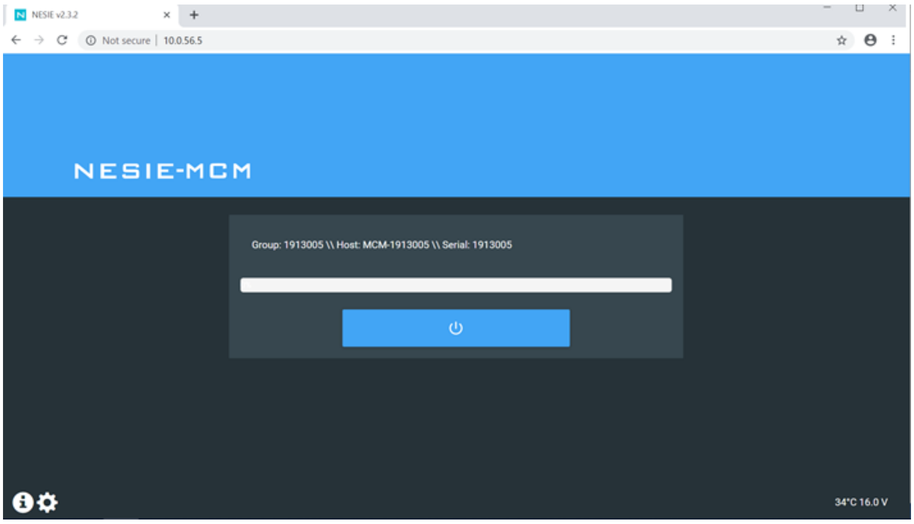


Fig 8. Control Unit – IP Address

When the operator has connected to the control module using an ethernet cable or the Wi-Fi hotspot, they should now type the displayed IP address into a web browser. The screen shown in Fig 9 will be displayed.



Group: 1913005 \\ Host: MCM-1913005 \\ Serial: 1913005

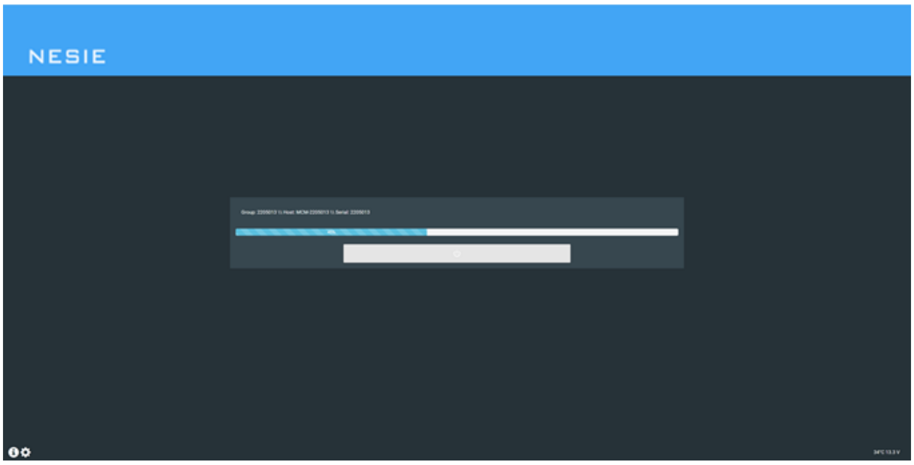
Fig 9. control module – Power On

The operator should now press the power on ⏻ button shown on the UI. The boot process will now start.

NOTE: If the user has manually powered the system on using the physical power button on the control module, then logs onto the system, the boot process will normally happen automatically.

The user will now see the blue boot process progress bar, as shown in Fig 10 below. Upon completion of the boot process ,the UI will automatically display the NESIE log on page as shown at Fig 11 below.

NOTE: If the user has been using the laptop to connect to the CNEST Cell Sites Survey Tool, ensure Wi-Fi sharing is stopped before plugging laptop back into NESIE. There can be an IP address issue, where the NESIE IP address can change and the user will not access the NESIE UI if this process is not followed.



Group: 2205013 \\ Host: MCM-2205013 \\ Serial: 2205013

Fig 10. control module – Booting

5.3 LOGIN - PASSWORD

After entering the correct IP address, the NESIE log on screen will be displayed as shown in Fig 11 below. The user is required to enter the Account Name and Password to log onto the UI then click the LOG IN button.

The default Account Name and Password are:

Account Name:	**root**
Password:	**root**

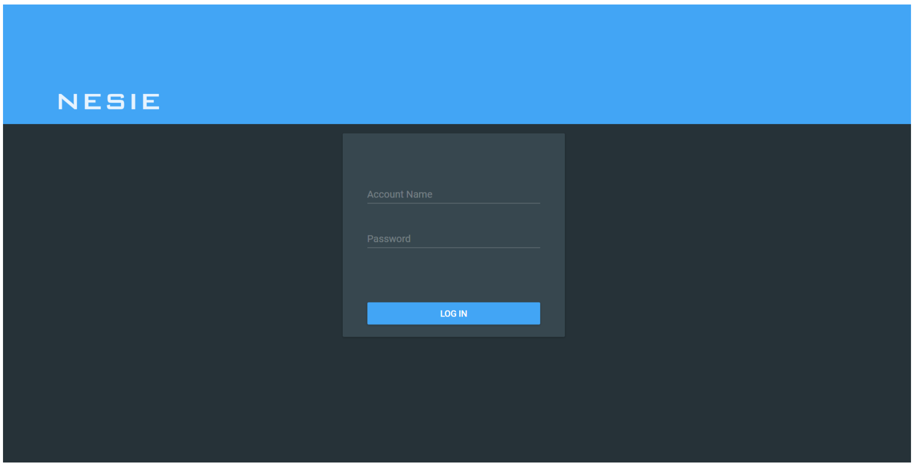


Fig 11. NESIE Log In – Account Name and Password

NOTE: It is strongly suggested that the administrator changes the default log on details upon receipt of the NESIE system.

Instructions on creating individual user profiles and changing passwords are detailed briefly at section 277.1.1 and in more detail at section 33.1.

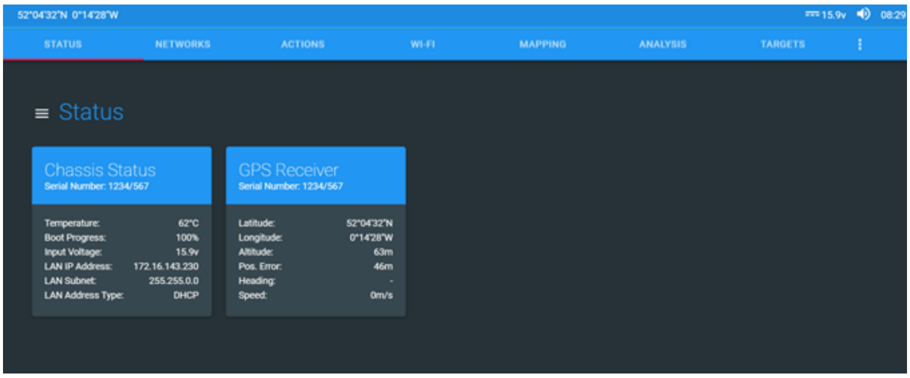
NOTE: Transmitting high power RF on some cellular bands may cause interference with the Wi-Fi Hot Spot created by NESIE. This is only temporary, and the Wi-Fi signal will be visible when the interference ceases. If required, the operator can refresh the browser after waiting for a short time.

It is strongly recommended that a backup ethernet cable is routed from the NESIE system to the location occupied by the operator. If interference is causing difficulty, the operator can simply plug in the ethernet cable, refresh the browser settings and continue working.

5.4 BOOT UP PROCESS

After powering up and logging in to the NESIE system, the user will be presented with the STATUS page which is discussed in more detail at section 10. However, the operator must be aware that it could take up to 90 seconds for the NESIE system to power up completely.

Upon entering the UI,, the operator may see the screen shown below in Fig 12. The operator will observe that the NESIE system is at the start of the boot process and only limited resources are shown on the screen.



Chassis Status
Serial Number: 1234/567

Temperature:	62°C
Boot Progress:	100%
Input Voltage:	15.9v
LAN IP Address:	172.16.143.230
LAN Subnet:	255.255.0.0
LAN Address Type:	DHCP

GPS Receiver
Serial Number: 1234/567

Latitude:	52°04'32"N
Longitude:	0°14'28"W
Altitude:	63m
Pos. Error:	46m
Heading:	-
Speed:	0m/s

Fig 12. Booting Up

As the boot up process progresses, more resources will be shown on the UI. The operator should wait for all resources eg: 3 x transceivers modules and a control module to be shown before any operations are started.

5.5 SOFTWARE REBUILD

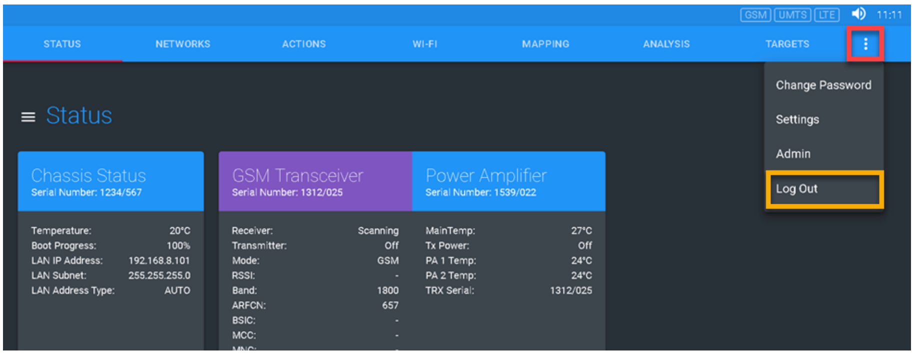
Care must be taken when using the NESIE system; as for any computer system, if the power is incorrectly withdrawn or if the external battery fails, it may cause a software crash and corrupt the internal HDD.

If there is fatal software crash, the NESIE system will automatically repair itself upon the next power on cycle.

This software rebuild process could take several minutes. The operator should be patient and allow plenty of time for the rebuild to happen. Do not be impatient and take the power out of the system, as this will damage the system further and the rebuild process will take even longer.

5.6 LOG OUT

If the operator needs to log out of the UI, they should use the additional menu button (red box) then the Log Out button (amber box) as shown below at Fig 13.



Chassis Status
Serial Number: 1234/567

Temperature: 20°C
Boot Progress: 100%
LAN IP Address: 192.168.8.101
LAN Subnet: 255.255.255.0
LAN Address Type: AUTO

GSM Transceiver
Serial Number: 1312/025

Receiver: Scanning
Transmitter: Off
Mode: GSM
RSSI: -
Band: 1800
ARFCN: 657
BSIC: -
MCC: -
MNC:

Power Amplifier
Serial Number: 1539/022

MainTemp: 27°C
Tx Power: Off
PA 1 Temp: 24°C
PA 2 Temp: 24°C
TRX Serial: 1312/025

Fig 13. Log Off

5.7 POWER OFF

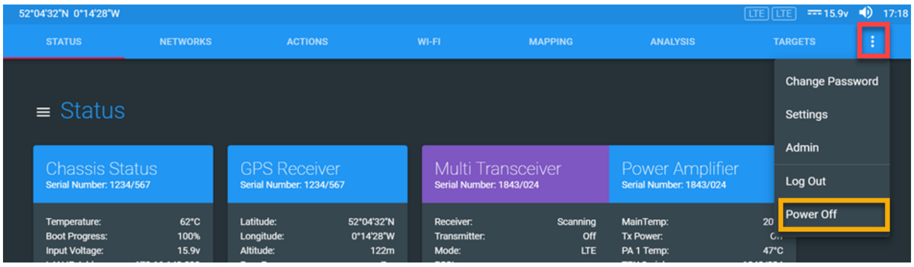
Depending on the NESIE system, there are several different ways to power off the system:

5.7.1 STANDALONE NESIE UNIT

Press and hold the power button until Power Off is seen in the screen (approx. 5 sec). The operator must allow the software to completely close the system down. This will be achieved when the screen goes blank.

5.7.2 CONTROL MODULE – STACKED NESIE MODULES

On a multi transceiver (stacked) NESIE system that has a control module, the operator can either press and hold the physical power button on the control module or use the software Power Off button (amber box) in the additional menu (red box), as shown below in Fig 14.



52°04'32"N 0°14'28"W

15.9v 17:18

Chassis Status
Serial Number: 1234/567
Temperature: 62°C
Boot Progress: 100%
Input Voltage: 15.9v

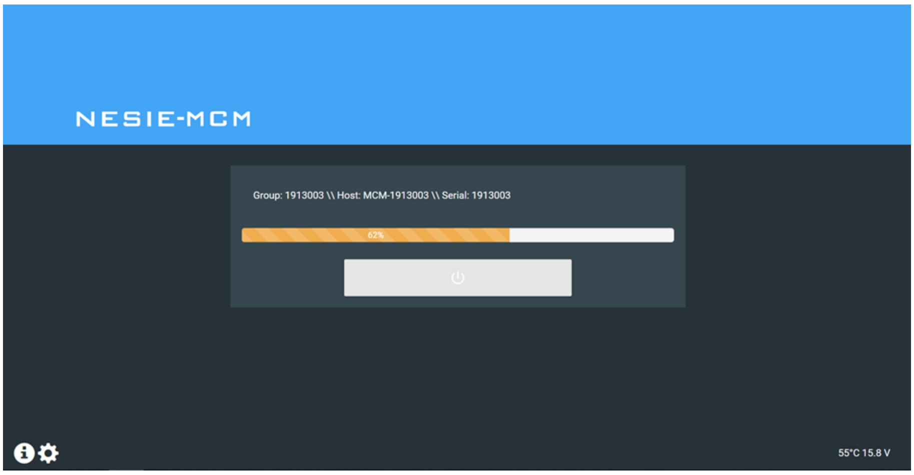
GPS Receiver
Serial Number: 1234/567
Latitude: 52°04'32"N
Longitude: 0°14'28"W
Altitude: 122m

Multi Transceiver
Serial Number: 1843/024
Receiver: Scanning
Transmitter: Off
Mode: LTE

Power Amplifier
Serial Number: 1843/024
MainTemp: 20
Tx Power:
PA 1 Temp: 47°C

Fig 14. control module – Software Power Off

After pressing the Power Off button, the user will get a confirmation message displayed, asking if they want to power off the unit. The UI will change to display the control module screen as shown below in Fig 15. The progress bar will initially show 100% in amber. The operator must allow the progress bar to decrease to 0% (a completely white bar will be visible). This may take up to 60 seconds.



Group: 1913003 \\ Host: MCM-1913003 \\ Serial: 1913003

55°C 15.8 V

Fig 15. Power Off – Progress Bar

When the progress bar shows zero, the software has completely ceased running but 12V power is still applied through the control module, therefore the power on / off screen is still available.

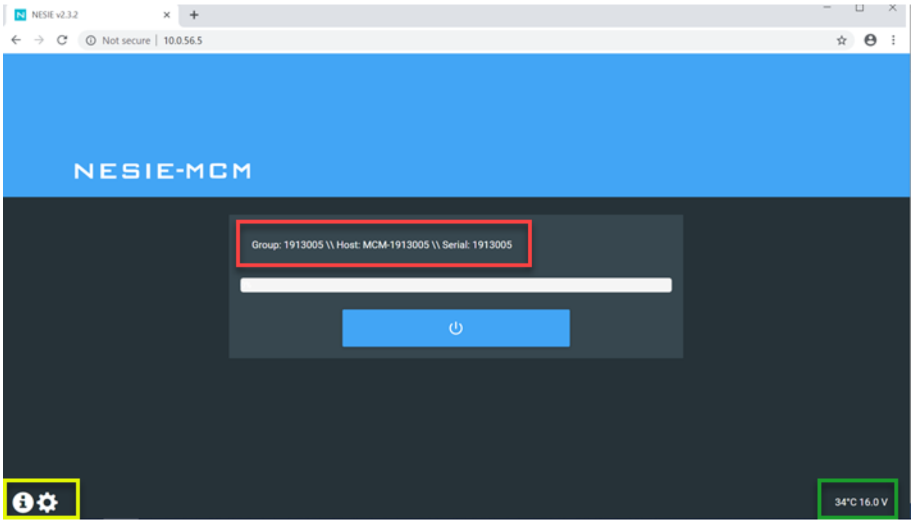
The operator can now remove the mains or battery power from the control module.

NOTE: Removing the 12v power supply from the NESIE unit before the system is fully shutdown, whether through the UI or physically using the power button, has the potential to corrupt the database and cause issues using the equipment at next log on. The operator should wait until the message in the NESIE window reads “Shutdown” or “Standby”. Only then is safe to remove the 12v power supply from the NESIE.,

6. CONTROL MODULE

Some NESIE systems can be used with a NESIE control module. This control module is used to combine and control multiple NESIE modules and forms them into one (stacked) system. When a control module is used, the operator will initially log on to the control module then into the NESIE UI.

On the control module log on page, there are several pieces of data that may be relevant to the operator as displayed below in Fig 16.



Group: 1913005 \\ Host: MCM-1913005 \\ Serial: 1913005

34°C 16.0 V

Fig 16. control module – On Screen Data

- **Red box** Group data
- **Green box** Internal temperature & voltage data
- **Yellow box** The information & settings page

6.1 GROUP DATA

The group data is used by the control module to synchronise multiple NESIE modules for internal communications. It uses the control module serial number as the foundation for these communications.

6.2 TEMPERATURE & VOLTAGE DATA

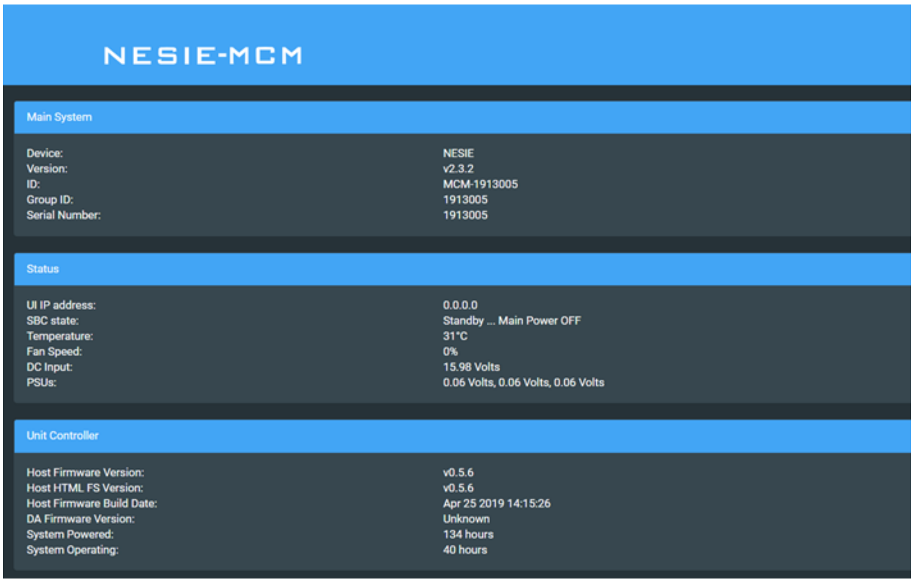
The current running temperature of the control module and the current external voltage that is applied to the control module.

6.3 INFORMATION & SETTINGS DATA

At the bottom of the control module log on page, the operator is presented with information & settings data buttons as displayed in Fig 17 below.

Fig 17. Control module – info & settings buttons

If the operator presses the information ⓘ button, the page shown below in Fig 18 will be displayed.



NESIE-MCM

Main System

Device:	NESIE
Version:	v2.3.2
ID:	MCM-1913005
Group ID:	1913005
Serial Number:	1913005

Status

UI IP address:	0.0.0.0
SBC state:	Standby ... Main Power OFF
Temperature:	31°C
Fan Speed:	0%
DC Input:	15.98 Volts
PSUs:	0.06 Volts, 0.06 Volts, 0.06 Volts

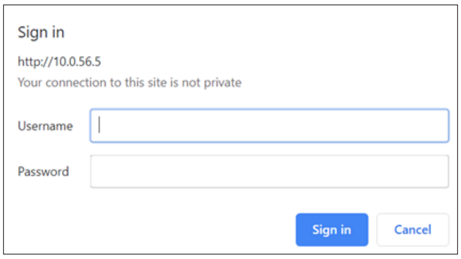
Unit Controller

Host Firmware Version:	v0.5.6
Host HTML FS Version:	v0.5.6
Host Firmware Build Date:	Apr 25 2019 14:15:26
DA Firmware Version:	Unknown
System Powered:	134 hours
System Operating:	40 hours

Fig 18. Control module – information screen

If the operator presses the ⚙ button, a pop-up box will appear as shown below in Fig 19 below.

NOTE: The user will not be given the log on details to the settings section. If required, they should contact Smith Myers.



Sign in

http://10.0.56.5

Your connection to this site is not private

Username

Password

Fig 19. Control module – settings page password

7. SETTING UP NESIE PRIOR TO USE

Note: This section does not give a full overview of the settings within NESIE. It is designed to enable the operator to set up NESIE upon initial receipt or prior to use in a new area / region.

Prior to deploying NESIE, it is important to ensure that the system has been configured for use in the desired region / country.

The NESIE receivers listen to the real cellular networks to extract the network data that will be used to create the fake base stations. If the correct frequency bands are not selected, NESIE will not perform in the desired manner and may miss the Target cellular devices.

Similarly, when NESIE transmits, the correct amplifiers and/or filters must be employed or the performance of NESIE will be reduced.

These settings may also need to be modified when moving to a different region, a border area where different cellular networks may be heard, or into a different country.

NOTE: There are additional settings that can be adjusted by the user, however, they are usually not changed from the default. Further instructions on these settings are at section 33.

7.1 SETTINGS - ADDITIONAL MENU OPTIONS ICON

To set up the NESIE prior to use, the operator should navigate to and press the additional menu options icon which is displayed below (red box) in Fig 20.

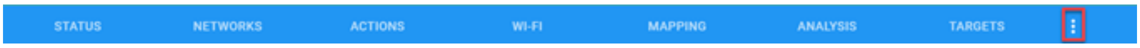


Fig 20. Settings – additional menu options icon

The operator will be presented with the additional options drop-down menu. Depending on the system, some options will not be available. The full range of options are shown in Fig 21 below.

The user will have the option to adjust the following sections:

- **Change Password**
- **Redirect**
- **Settings**
- **Admin**
- **Log Out**
- **Power Off**

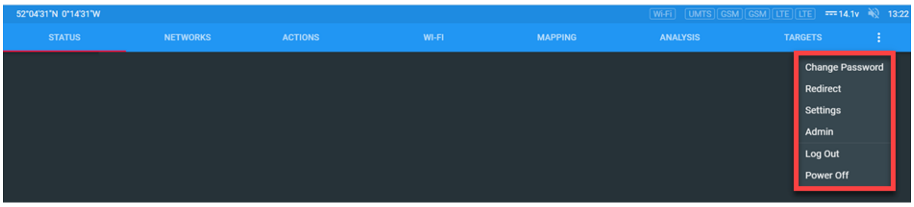


Fig 21. Menu – Options

7.1.1 CHANGE PASSWORD

A pop-up menu will be displayed as shown in Fig 22 below. The operator now has the option to change the default password.

Enter the Current Password, then enter the New Password and Repeat New Password to ensure it is correct.

To apply the change, press the CHANGE PASSWORD button.

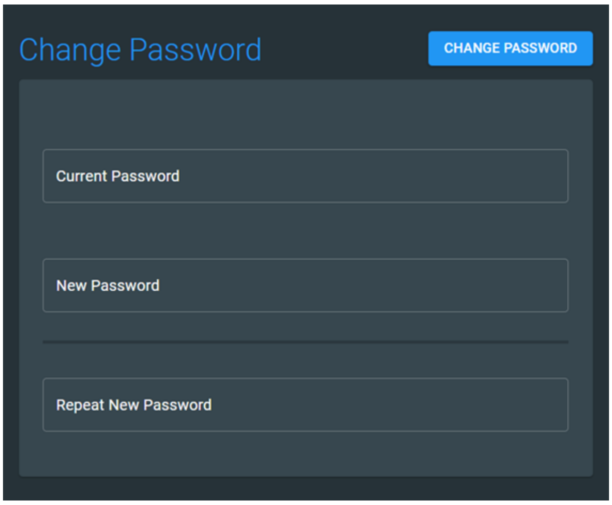
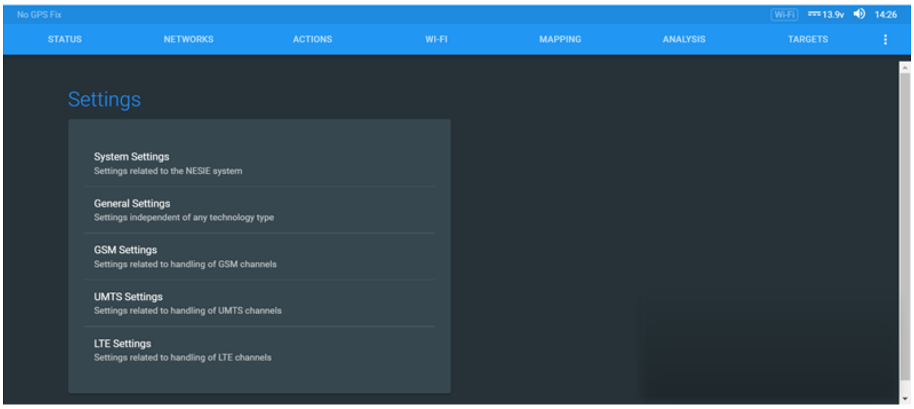


Fig 22. Change Password

7.1.2 SETTINGS

When the Settings button is pressed, the settings page will be displayed as shown in Fig 23 below.



Settings

System Settings
Settings related to the NESIE system

General Settings
Settings independent of any technology type

GSM Settings
Settings related to handling of GSM channels

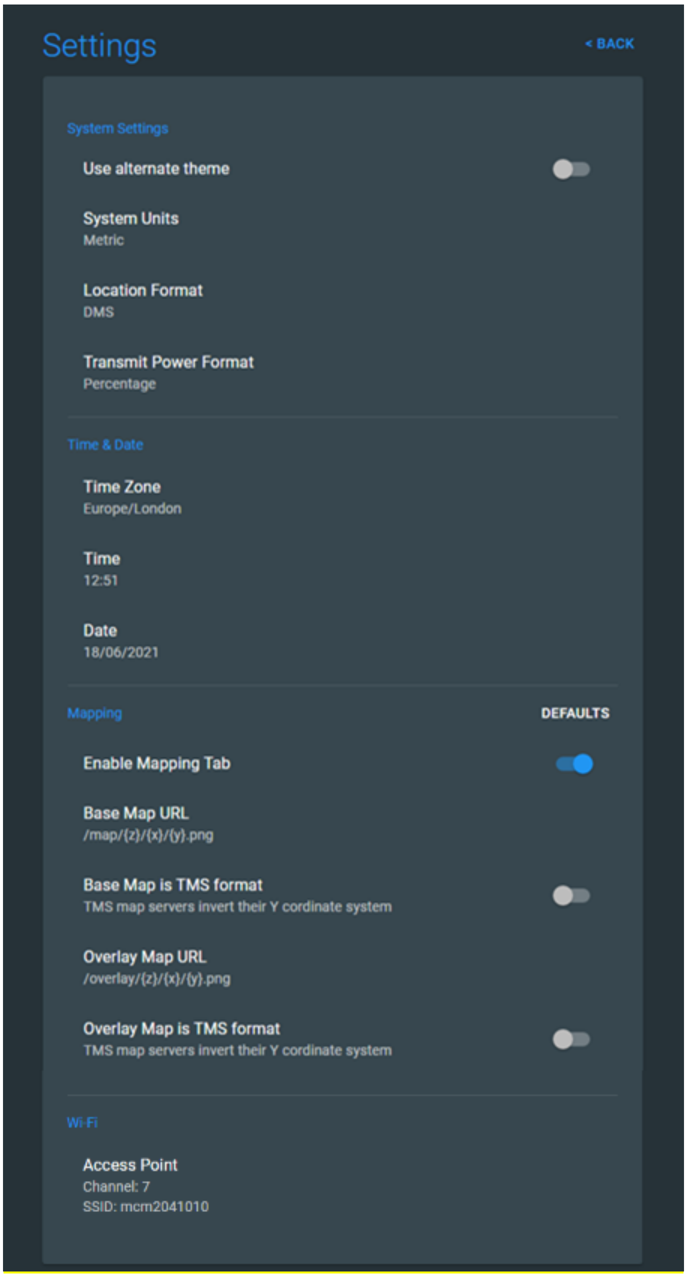
UMTS Settings
Settings related to handling of UMTS channels

LTE Settings
Settings related to handling of LTE channels

Fig 23. Settings Options - Detail

7.1.3 SYSTEM SETTINGS

When clicking on the System Settings, the operator will see the page shown below at Fig 24.



Settings

< BACK

System Settings

Use alternate theme ○

System Units
Metric

Location Format
DMS

Transmit Power Format
Percentage

Time & Date

Time Zone
Europe/London

Time
12:51

Date
18/06/2021

Mapping

DEFAULTS

Enable Mapping Tab ●

Base Map URL
/map/{z}/{x}/{y}.png

Base Map is TMS format ○
TMS map servers invert their Y cordinate system

Overlay Map URL
/overlay/{z}/{x}/{y}.png

Overlay Map is TMS format ○
TMS map servers invert their Y cordinate system

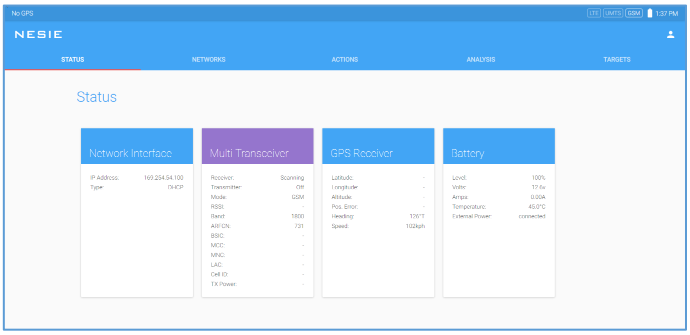
Wi-Fi

Access Point
Channel: 7
SSID: mcm2041010

Fig 24. System Settings

7.1.3.1 ALTERNATIVE THEME

By default, the NESIE UI will display the black screen backgrounds and muted colours to ensure the UI does not drawn attention to the operator at night. If required, the UI can be switched to a brighter colour scheme by sliding the button from grey to blue. An example of the alternative UI is shown below at Fig 25.



Status

Network Interface

IP Address:	169.254.54.100
Type:	DHCP

Multi Transceiver

Receiver:	Scanning
Transmitter:	Off
Mode:	GSM
RSSI:	-
Band:	1800
ARFCN:	731
BSIC:	-
MCC:	-
MNC:	-
LAC:	-
Cell ID:	-
TX Power:	-

GPS Receiver

Latitude:	-
Longitude:	-
Altitude:	-
Pos. Error:	-
Heading:	126°T
Speed:	102kph

Battery

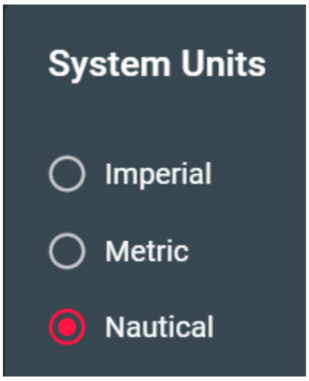
Level:	100%
Volts:	12.6v
Amps:	0.00A
Temperature:	45.0°C
External Power:	connected

Fig 25. Alternate theme

7.1.3.2 SYSTEM UNITS

The system measurement units used in the NESIE UI can be switched between Metric (Km and meters), Imperial (Miles and yards) or Nautical (Nautical Miles).

To select a System Unit, the operator must click on the adjacent radio button. The chosen option radio button will turn red, and the pop-up menu will disappear.



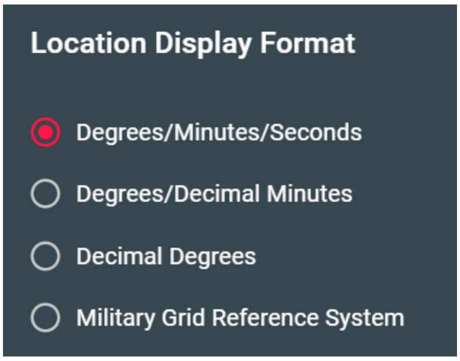
System Units

○ Imperial
○ Metric
● Nautical

Fig 26. System Units

7.1.3.3 GPS LOCATION FORMAT

The location/fix data received by the GPS antenna on the NESIE system can be displayed in four different formats. The operator can choose which format is used by clicking on Location Display Format. A pop-up menu showing the available formats will be displayed as shown at Fig 27 below. The operator can now select the required format by clicking in the adjacent radio button. The chosen option button will turn red, and the pop-up menu will disappear.



Location Display Format

● Degrees/Minutes/Seconds
○ Degrees/Decimal Minutes
○ Decimal Degrees
○ Military Grid Reference System

Fig 27. GPS Format

The Formats available are:

Degrees / Minutes / Seconds

Degrees / Decimal Minutes

Decimal Degrees

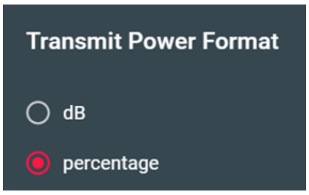
Military Grid Reference System (MGRS)

7.1.3.4 TRANSMIT POWER FORMAT

If required, the operator can apply attenuation to the transmitted NESIE signal. If attenuation is applied, the NESIE systems output power is reduced. The attenuation scale can be displayed in 2 formats.

- Percentage (%)
- Decibel (dB)

To change the Transmit Power Format, the operator must click on the Transmit Power Format line. A pop-up window will be shown where the operator can select the required value. The chosen option button will turn red, and the pop-up menu will disappear.



Transmit Power Format

○ dB

● percentage

Fig 28. Transmit Power Format

7.1.3.5 TIME ZONE

The system settings for the Time Zone of the local continent/region and city are detected from the machine the web browser is running on and cannot be altered from within the UI. The time zone of the system is always in UTC (Coordinated Universal Time), and the data is only changed to local time for display.

If the time zone settings are incorrect, they will need to be altered on the PC/tablet or mobile device that is being used to control the NESIE.

7.1.3.6 TIME

To adjust the time, click on the time displayed, a pop-up box with appear showing the current time. When clicked the hours screen shown at Fig 29 below will be displayed. Click and drag to the hour required and press OK. The minutes screen will then be shown, as at Fig 29 below. The user can now click and drag to the required minute.

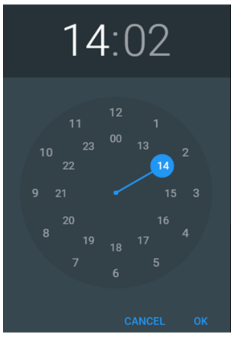


Fig 29. Hours

Click and drag to adjust the minute's pointer to the desired number and press OK.

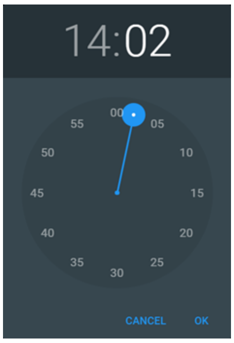


Fig 30. Minutes

7.1.3.7 DATE

To adjust the date, the operator should first click on date. A pop-up box will appear with the date on it. The operator then clicks on the date line and another pop-up box will appear. The operator can then use < left arrow or right > arrow to move to the correct month and year. Then click on the required date as shown in Fig 31 below. When the date is correct click the OK button to save the settings.

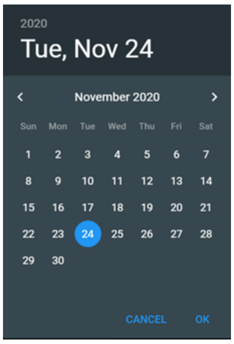
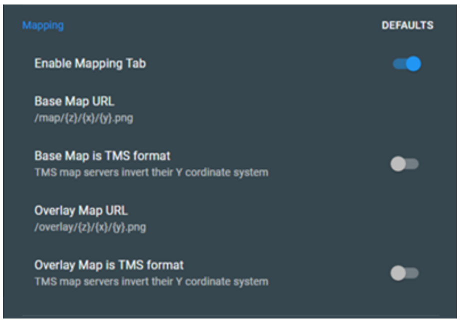


Fig 31. Date

7.1.3.8 MAPPING

The mapping sections allows the NESIE operator to select between the installed mapping, and the ability to set up and direct the NESIE software to an external mapping server or link to on line mapping such as Google Maps.



Mapping

DEFAULTS

Enable Mapping Tab

Base Map URL
/map/{z}/{x}/{y}.png

Base Map is TMS format
TMS map servers invert their Y cordinate system

Overlay Map URL
/overlay/{z}/{x}/{y}.png

Overlay Map is TMS format
TMS map servers invert their Y cordinate system

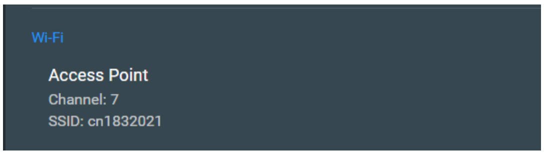
Fig 32. Mapping

By default, the system will be set up to use the installed mapping if using a Tactical NESIE system, or will be disabled if mapping is not installed.

For detailed instructions on how to set up an external map server or on line mapping, the operator should refer to section 33.3.1.8.

7.1.3.9 WI-FI - HOT SPOT SETTINGS (IF APPLICABLE)

If the NESIE system or control module is fitted with a Wi-Fi access point (Hotspot), the additional settings to adjust the Wi-Fi will be displayed as below in Fig 33.



Wi-Fi

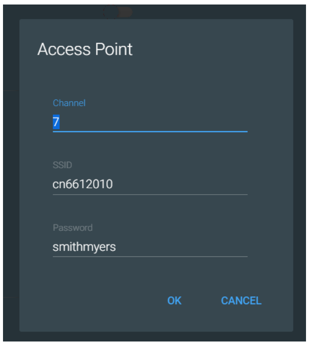
Access Point
Channel: 7
SSID: cn1832021

Fig 33. Wi-Fi

As soon as the NESIE system is turned, on a Wi-Fi access point (Hotspot) is created to enable the user to connect wirelessly to the UI. By default, the Wi-Fi settings are:

Channel:	7
SSID:	cn (or) mcm (or) pn & Serial No (of the control module)
Password:	smithmyers (no spaces, lower case)

To change the default Wi-Fi access point settings, click on the Wi-Fi button. The pop up screen shown at Fig 34 will be displayed.



Access Point

Channel
7

SSID
cn6612010

Password
smithmyers

Fig 34. Wi-Fi Settings

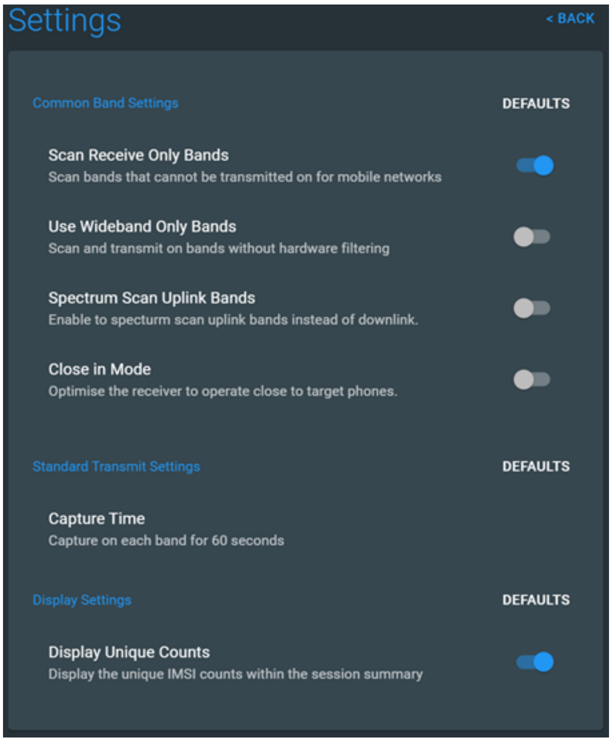
Channel: The Wi-Fi channel that the access point is transmitted on. The channels available are 1 – 14.

SSID: The name or SSID of the access point that is transmitted. Anyone in Wi-Fi detection range will be able to see the broadcast SSID.

Password: The password that is required by anyone who is logging in to the Wi-Fi access point.

7.1.4 GENERAL SETTINGS

When clicking on General Settings the operator will see the page shown at Fig 35 below.



Settings

Common Band Settings — DEFAULTS

Scan Receive Only Bands: on
Scan bands that cannot be transmitted on for mobile networks

Use Wideband Only Bands: off
Scan and transmit on bands without hardware filtering

Spectrum Scan Uplink Bands: off
Enable to specturm scan uplink bands instead of downlink.

Close in Mode: off
Optimise the receiver to operate close to target phones.

Standard Transmit Settings — DEFAULTS

Capture Time
Capture on each band for 60 seconds

Display Settings — DEFAULTS

Display Unique Counts: on
Display the unique IMSI counts within the session summary

Fig 35. General Settings

7.1.4.1 COMMON BAND SETTINGS

Scan Receive Only Bands:
Some NESIE units may only have limited transmit amplifiers or filters fitted (normally the airborne systems), however, the receivers are still capable of receiving other bands. Scan Only Receive Bands instructs the system to scan the frequency bands that the system cannot transmit on. This will list the other neighbour cells that the system is competing against. This is to extract other pertinent cell data that can be used to configure the transmission and attract devices to the system.

When the Scan Receive Only Bands is selected (Blue), additional bands may be shown in the GSM, UMTS and LTE Settings page.

Use Wideband Only Bands:
The Use Wideband Only Bands function is for use on low powered covert systems. By not using any filtration across the whole of its operating frequency spectrum, it can attract devices using international frequency bands in most countries straight out of the box.

Spectrum Scan Uplink Bands
If this setting is not enabled, when the Spectrum Scan is viewed on the NETWORKS page, only the downlink frequency bands are displayed. By selecting the Spectrum Scan Uplink Bands function, the uplink frequency bands will be displayed only,

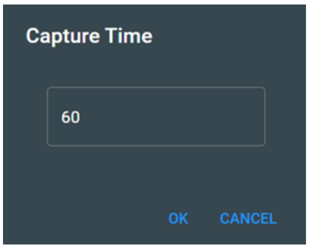
Close in Mode

This function allows NESIE to be used a basic form of direction finding tool, used to locate Targets in rooms, hotel corridors etc. The system will than likely be being used for close in work in the tactical backpack. When the system puts a device into Hold, a meter is displayed below the Target details on the ACTIONS page (see section 23.6). As the system is moved, the meter reading will change and will identify whether the operator is moving towards or away from the Target.

7.1.4.2 STANDARD TRANSMIT SETTINGS

Capture time:

Is used to adjust the time that the NESIE transmits a GSM fake base station signal to encourage the devices to register onto the system. The value is the number of seconds the NESIE will transmit for. The time set is displayed in the screen and if required, the operator can press the Defaults button to return the value to 60 seconds as shown in Fig 36.

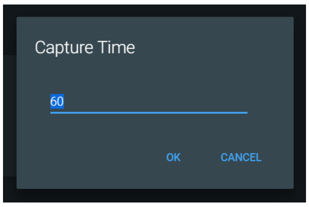


Capture Time

60

Fig 36. Standard Transmit Settings

If the operator needs to adjust the time, click on the Standard Transmit Settings button and a pop-up box will be displayed as shown below in Fig 37. The operator can adjust the time between the minimum of 30 seconds and maximum of 100,000 seconds (over 24hrs).



Capture Time

60

Fig 37. Capture Time

NOTE: When transmitting a fake base station, the standard capture time will automatically change depending on the number of transceiver (channels) in the NESIE system.

In a single channel system – the capture time will automatically adjust to match the technology that is being transmitted. GSM – the standard capture time will be 60 seconds or whatever value is set by the operator. In the UMTS & LTE bands, NESIE will automatically detect the number of channels in the real networks band and transmit for a default of 30 seconds on each of these channels.

In a multiple channel system - the standard (GSM) capture time will be overruled by the detected settings of either the UMTS or the LTE band. E.g.: If there are 3 UMTS channels detected in the band, the capture time will default to 30 seconds per channel (90secs). However, if there are 4 channels detected in the LTE band the capture time will now be overruled to 4 x 30secs (120 secs). All transceivers will now be synchronised and transmit on the highest total. Therefore, in this example, a 3-channel system will transmit for 120 seconds on GSM, UMTS and LTE.

DISPLAY SETTINGS

Display Unique Counts:
When an ID is captured, it will be displayed in the list. Regularly, an ID may be captured multiple times e.g. in GSM, UMTS and LTE – therefore it could be shown as being captured a total of 3 times. This may then give a false impression of the number of unique IDs (individual mobile devices) in the Grab.

By default, the NESIE cross checks the IDs captured in the Grab to give a true number of unique IDs. So, if the number of IDs captured is display as **100 (95).** The total number of IDs captured including multiple ID is 100, however, the number of individual mobile devices captured is 95.

To turn off the unique number and only show the total number of mobile devices, the operator should slide the button from blue to grey.

7.1.4.3 GSM SETTINGS

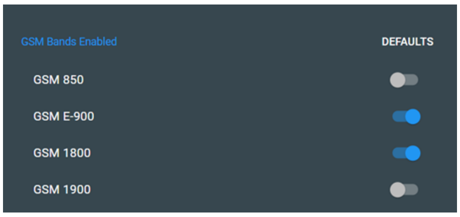
The GSM Band Settings screen allows the operator to choose which GSM bands to scan to log the local area cellular provider's data. These settings are usually applied upon initial configuration of the NESIE system and should not change unless the NESIE is moved into a different region / country or the network providers change their settings.

To successfully log the network providers BTS settings, NESIE must scan the available GSM band, tuning its receiver every 200kHz. If a signal is present, it must pause and attempt to decode the signal. In the EGSM 900 band that equates to 173 individual channels / steps.

NOTE: If more bands are selected than necessary, NESIE will scan parts of the frequency spectrum not used for GSM in this area, region or country and add unnecessary time to the scan.

GSM Band Enabled:
The operator must adjust the toggle switches to reflect the GSM frequency bands present in their operational area. Grey indicates off/ blue indicates on as shown below in Fig 38.

In Fig 31, NESIE has be configured to scan the GSM E-900 and 1800 Bands with GSM 850 & GSM 1900 turned off. The scanning of the network providers is discussed in more detail in section 12.



GSM Bands Enabled DEFAULTS

GSM 850

GSM E-900

GSM 1800

GSM 1900

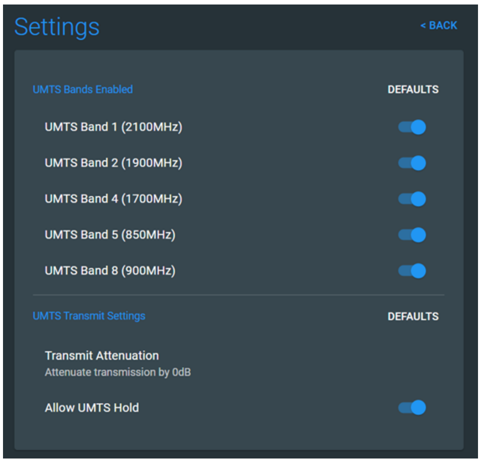
Fig 38. GSM Band Settings

7.1.4.4 UMTS SETTINGS

UMTS Bands Enabled:

This section sets NESIE to the UMTS frequency bands it should carry out a Network Scan on (listen to) to log the local area network signals. If bands that are not used in the region / country are included in the scan, NESIE will waste time listening to these bands when there is no requirement.

CAUTION – IF THE DEFAULT OPTION IS TICKED FOR EACH BAND, ALL BANDS WILL BE SELECTED. IF ALL BANDS ARE INCLUDED IN THE SCAN THE TIME REQUIRED FOR THE SCAN WILL INCREASE.



Settings < BACK

UMTS Bands Enabled DEFAULTS

UMTS Band 1 (2100MHz)

UMTS Band 2 (1900MHz)

UMTS Band 4 (1700MHz)

UMTS Band 5 (850MHz)

UMTS Band 8 (900MHz)

UMTS Transmit Settings DEFAULTS

Transmit Attenuation
Attenuate transmission by 0dB

Allow UMTS Hold

Fig 39. UMTS Bands to Scan

Allow UMTS Hold:

If the user requires the ability to Hold a cellular device on UMTS, this toggle switch should be blue. Now NESIE will have the ability to Hold on UMTS and GSM.

7.1.4.5 LTE SETTINGS

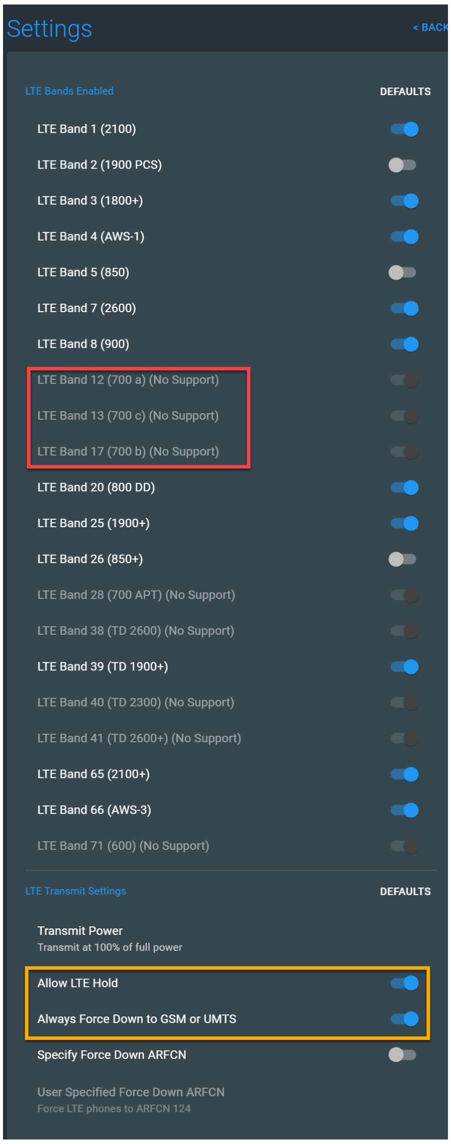
LTE Bands Enabled:

This section tells the NESIE which LTE frequency bands it should carry out a Network Scan on (listen to) to log the local area network signals. If bands that are not used in the region / country are included in the scan, NESIE will waste time listening to these bands when there is no requirement.

The operator can select the LTE bands used in the country / area. If required additional bands can be selected to monitor the RF in that band, as shown in Fig 40 below.

The bands are listed as LTE Bands, but cellular network providers may use GSM or UMTS in the band as well.

As shown in Fig 40 below, there are several LTE bands that are displayed but are greyed out. This indicates the other bands that are available upon request. NESIE is fitted with a specific number of amplifiers and filters depending on the region of the world that it is deployed in. If required some components can be swapped to allow other bands.



Settings

< BACK

LTE Bands Enabled

DEFAULTS

- LTE Band 1 (2100) ☑
- LTE Band 2 (1900 PCS) □
- LTE Band 3 (1800+) ☑
- LTE Band 4 (AWS-1) ☑
- LTE Band 5 (850) □
- LTE Band 7 (2600) ☑
- LTE Band 8 (900) ☑
- LTE Band 12 (700 a) (No Support) □
- LTE Band 13 (700 c) (No Support) □
- LTE Band 17 (700 b) (No Support) □
- LTE Band 20 (800 DD) ☑
- LTE Band 25 (1900+) ☑
- LTE Band 26 (850+) □
- LTE Band 28 (700 APT) (No Support) □
- LTE Band 38 (TD 2600) (No Support) □
- LTE Band 39 (TD 1900+) ☑
- LTE Band 40 (TD 2300) (No Support) □
- LTE Band 41 (TD 2600+) (No Support) □
- LTE Band 65 (2100+) ☑
- LTE Band 66 (AWS-3) ☑
- LTE Band 71 (600) (No Support) □

LTE Transmit Settings

DEFAULTS

Transmit Power
Transmit at 100% of full power

- Allow LTE Hold ☑
- Always Force Down to GSM or UMTS ☑
- Specify Force Down ARFCN □

User Specified Force Down ARFCN
Force LTE phones to ARFCN 124

Fig 40. LTE Bands Enabled

7.1.4.6 LTE TRANSMIT SETTINGS

Allow LTE Hold:
Can be enabled by making the toggle switch blue. This now enables NESIE to Hold a mobile device on LTE. If the other technologies are enabled, the system may have the ability to Hold devices on GSM, UMTS and LTE.

Always Force Down to GSM or UMTS:
When this toggle button is blue, NESIE will transmit a cell tower and the LTE bands to detect the device, extract the IMSI and measure the distance to the device. However, due to the security settings within LTE devices, the IMEI will not be released. So, to ensure NESIE can detect the IMEI a Redirect command is sent to the device ‘move from LTE to UMTS or GSM’. When the device moves to GSM or UMTS,℃ it will attempt to register onto NESIE on this technology. NESIE will now show the IMSI and IMEI as well as measure the distance again.

8. TEMPERATURE & VOLTAGE

8.1 TACTICAL NESIE

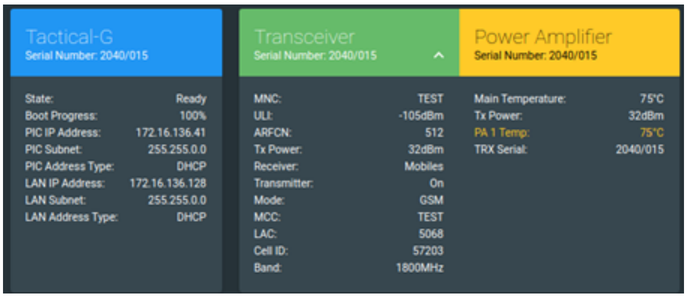
The Tactical NESIE temperature and voltage warning are shown below.

8.1.1 TEMPERARTUE WARNINGS

The Tactical units are capable of working in ambient temperatures of up to 55℃. When fitted into the backpack, they are capable of working up to an ambient temperature of 42℃.

The main temperature to monitor is that associated with the Power Amplifier.

AMBER WARNING
The UI will display an AMBER warning when the PA temperature reaches 75℃ as shown below in Fig 41 below. This is to indicate to the operator that the temperature is increasing and if possible the unit should be allowed to cool down



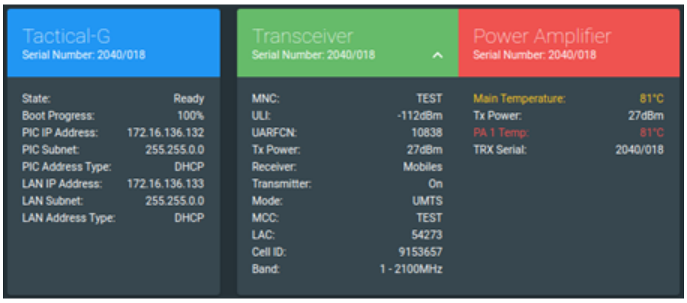
Tactical-G Serial Number: 2040/015	
State:	Ready
Boot Progress:	100%
PIC IP Address:	172.16.136.41
PIC Subnet:	255.255.0.0
PIC Address Type:	DHCP
LAN IP Address:	172.16.136.128
LAN Subnet:	255.255.0.0
LAN Address Type:	DHCP

Transceiver Serial Number: 2040/015	
MNC:	TEST
ULI:	-105dBm
ARFCN:	512
Tx Power:	32dBm
Receiver:	Mobiles
Transmitter:	On
Mode:	GSM
MCC:	TEST
LAC:	5068
Cell ID:	57203
Band:	1800MHz

Power Amplifier Serial Number: 2040/015	
Main Temperature:	75°C
Tx Power:	32dBm
PA 1 Temp:	75°C
TRX Serial:	2040/015

Fig 41. Tactical – Amber Temp Warning

RED WARNING
The UI will display a RED warning when the PA temperature reaches 80℃, as shown below at Fig 42 below. This is to show that the temperature has now reached its higher threshold and the operator is advised to stop transmission and allow the system to cool down.



Tactical-G Serial Number: 2040/018	
State:	Ready
Boot Progress:	100%
PIC IP Address:	172.16.136.132
PIC Subnet:	255.255.0.0
PIC Address Type:	DHCP
LAN IP Address:	172.16.136.133
LAN Subnet:	255.255.0.0
LAN Address Type:	DHCP

Transceiver Serial Number: 2040/018	
MNC:	TEST
ULI:	-112dBm
UARFCN:	10838
Tx Power:	27dBm
Receiver:	Mobiles
Transmitter:	On
Mode:	UMTS
MCC:	TEST
LAC:	54273
Cell ID:	9153657
Band:	1 - 2100MHz

Power Amplifier Serial Number: 2040/018	
Main Temperature:	81°C
Tx Power:	27dBm
PA 1 Temp:	81°C
TRX Serial:	2040/018

Fig 42. Tactical – Red Temp Warning

AUTOMTIC SHUTDOWN
When the power amplifier temperature reaches 85℃, the software will automatically initiate a software shutdown.

8.1.2 VOLTAGE WARNINGS

When the Tactical units are running on battery power, the system will issue amber and red warnings if the battery voltage drops below set thresholds.

AMBER WARNING
The UI will display an amber warning if the voltage drops below 9.8V. This indicates that the battery is dropping below optimum charge and the operator is advised to replace the battery as soon as possible.

If the voltage continues to drop it may affect the output and operation of the system.

RED WARNING
The UI will display a red warning when the voltage drops below 9.2V. This indicates that the system is now operating below its minimum battery threshold and will reduce its capability. The operator should replace the battery immediately or shut down the software before the battery voltage causes a system crash.

The Tactical NESIE system will continue running until the battery voltage drops to approx. 8.8V. At this point the system will cease working.

9. THE NESIE USER INTERFACE

The NESIE UI software is stored as a web browser on the NESIE systems internal memory. No specialist software is required and any laptop, tablet or device which has a suitable web browser installed can be used. Google Chrome is the preferred browser but others such as Firefox can be used.

Once the user has successfully logged in to UI the STATUS page will be displayed as shown in Fig 43 and Fig 44 below.

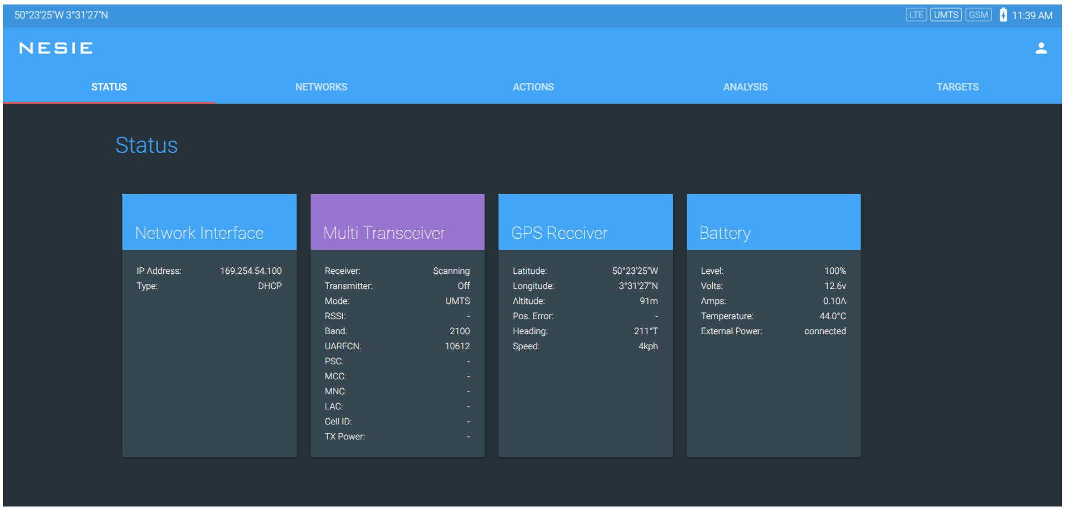
9.1 SINGLE CHANNEL SYSTEM

Single channel systems can consist of:

- Covert Ground
  - Single low power module
- Tactical Ground & Single Use Adaptor (SUA)
  - Single, standalone medium power NESIE module
- Tactical Ground & Tactical Control Module (TCM)
  - Single medium power module connected to a TCM
- Strategic Ground
  - Single, standalone high power NESIE Module
- Strategic Ground & Strategic control module (SCM)
  - Single, high power NESIE module connected to a SCM

If using a Covert Ground, Tactical Ground & SUA or a Strategic Ground module, the UI will loOK similar to that shown in Fig 43 below.

Only one transceiver will be visible. This single transceiver will normally be operating in MULTI TRANSCEIVER mode as shown below in Fig 43 below. This multi transceiver will automatically switch between GSM, UMTS and LTE.



Network Interface

IP Address: 169.254.54.100
Type: DHCP

Multi Transceiver

Receiver: Scanning
Transmitter: Off
Mode: UMTS
RSSI: -
Band: 2100
UARFCN: 10612
PSC: -
MCC: -
MNC: -
LAC: -
Cell ID: -
TX Power: -

GPS Receiver

Latitude: 50°23'25"W
Longitude: 3°31'27"N
Altitude: 91m
Pos. Error: -
Heading: 211°T
Speed: 4kph

Battery

Level: 100%
Volts: 12.6v
Amps: 0.10A
Temperature: 44.0°C
External Power: connected

Fig 43. Status Page – Single Channel System

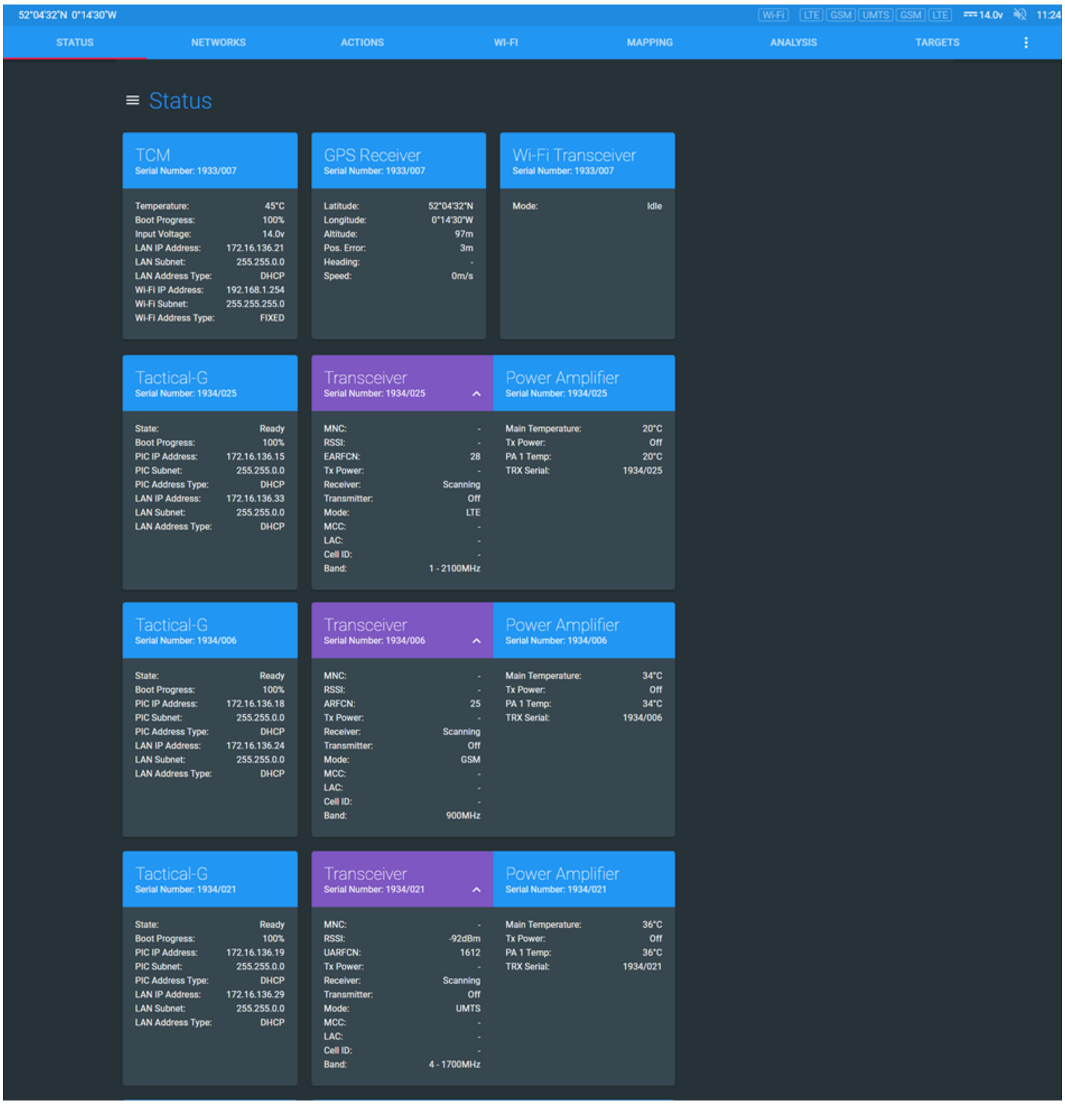
9.2 MULTI-CHANNEL SYSTEM

Multi-channel systems can consist of:

- Multiple Tactical Ground units & Tactical Control Module (TCM)
    - Multiple medium power units connected to form a stack.
- Multiple Strategic Ground & Strategic control module (SCM)
    - Multiple high-power units connected to form a stack.

If the NESIE system consists of multiple transceivers and associated amplifiers, the individual modules will be displayed as shown in Fig 44 below.

The screen below shows a Tactical 3 stack. This is a Tactical Control Module (TCM) and 3 x Tactical Ground (Tactical-G) units combined to create 1 system.



TCM
Serial Number: 1933/007

Temperature:	45°C
Boot Progress:	100%
Input Voltage:	14.0v
LAN IP Address:	172.16.136.21
LAN Subnet:	255.255.0.0
LAN Address Type:	DHCP
Wi-Fi IP Address:	192.168.1.254
Wi-Fi Subnet:	255.255.255.0
Wi-Fi Address Type:	FIXED

GPS Receiver
Serial Number: 1933/007

Latitude:	52°04'32"N
Longitude:	0°14'30"W
Altitude:	97m
Pos. Error:	3m
Heading:	-
Speed:	0m/s

Wi-Fi Transceiver
Serial Number: 1933/007

Mode:	Idle

Tactical-G
Serial Number: 1934/025

State:	Ready
Boot Progress:	100%
PIC IP Address:	172.16.136.15
PIC Subnet:	255.255.0.0
PIC Address Type:	DHCP
LAN IP Address:	172.16.136.33
LAN Subnet:	255.255.0.0
LAN Address Type:	DHCP

Transceiver
Serial Number: 1934/025

MNC:	-
RSSI:	-
EARFCN:	28
Tx Power:	-
Receiver:	Scanning
Transmitter:	Off
Mode:	LTE
MCC:	-
LAC:	-
Cell ID:	-
Band:	1 - 2100MHz

Power Amplifier
Serial Number: 1934/025

Main Temperature:	20°C
Tx Power:	Off
PA 1 Temp:	20°C
TRX Serial:	1934/025

Tactical-G
Serial Number: 1934/006

State:	Ready
Boot Progress:	100%
PIC IP Address:	172.16.136.18
PIC Subnet:	255.255.0.0
PIC Address Type:	DHCP
LAN IP Address:	172.16.136.24
LAN Subnet:	255.255.0.0
LAN Address Type:	DHCP

Transceiver
Serial Number: 1934/006

MNC:	-
RSSI:	-
ARFCN:	25
Tx Power:	-
Receiver:	Scanning
Transmitter:	Off
Mode:	GSM
MCC:	-
LAC:	-
Cell ID:	-
Band:	900MHz

Power Amplifier
Serial Number: 1934/006

Main Temperature:	34°C
Tx Power:	Off
PA 1 Temp:	34°C
TRX Serial:	1934/006

Tactical-G
Serial Number: 1934/021

State:	Ready
Boot Progress:	100%
PIC IP Address:	172.16.136.19
PIC Subnet:	255.255.0.0
PIC Address Type:	DHCP
LAN IP Address:	172.16.136.29
LAN Subnet:	255.255.0.0
LAN Address Type:	DHCP

Transceiver
Serial Number: 1934/021

MNC:	-
RSSI:	-92dBm
UARFCN:	1612
Tx Power:	-
Receiver:	Scanning
Transmitter:	Off
Mode:	UMTS
MCC:	-
LAC:	-
Cell ID:	-
Band:	4 - 1700MHz

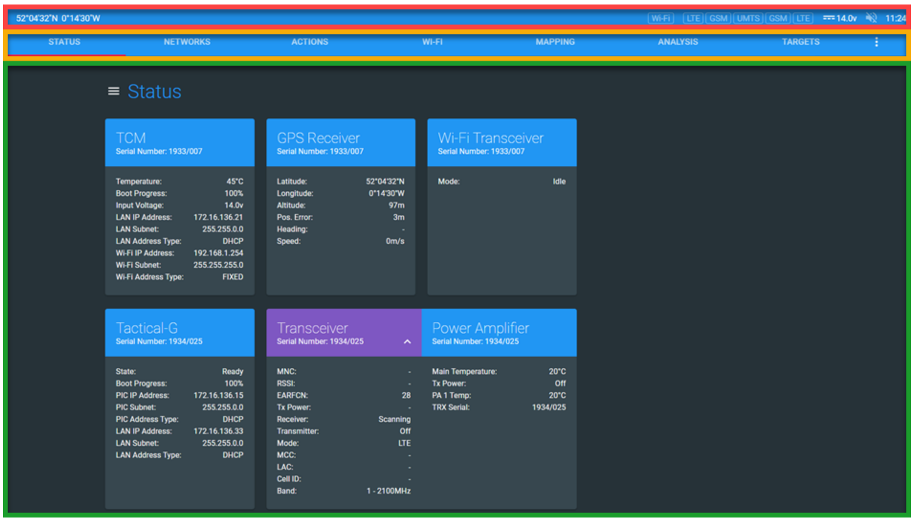
Power Amplifier
Serial Number: 1934/021

Main Temperature:	36°C
Tx Power:	Off
PA 1 Temp:	36°C
TRX Serial:	1934/021

Fig 44. STATUS Page – Multi Channel System

The NESIE UI can be brOKen down into three sections:

1.	RED	Header Bar
2.	AMBER	Menu Buttons
3.	GREEN	Selected Page



Status

TCM
Serial Number: 1933/007

Temperature: 45°C
Boot Progress: 100%
Input Voltage: 14.0v
LAN IP Address: 172.16.136.21
LAN Subnet: 255.255.0.0
LAN Address Type: DHCP
Wi-Fi IP Address: 192.168.1.254
Wi-Fi Subnet: 255.255.255.0
Wi-Fi Address Type: FIXED

GPS Receiver
Serial Number: 1933/007

Latitude: 52°04'32"N
Longitude: 0°14'30"W
Altitude: 97m
Pos. Error: 3m
Heading: -
Speed: 0m/s

Wi-Fi Transceiver
Serial Number: 1933/007

Mode: Idle

Tactical-G
Serial Number: 1934/025

State: Ready
Boot Progress: 100%
PIC IP Address: 172.16.136.15
PIC Subnet: 255.255.0.0
PIC Address Type: DHCP
LAN IP Address: 172.16.136.33
LAN Subnet: 255.255.0.0
LAN Address Type: DHCP

Transceiver
Serial Number: 1934/025

MNC: -
RSSI: -
EARFCN: 28
Tx Power: -
Receiver: Scanning
Transmitter: Off
Mode: LTE
MCC: -
LAC: -
Cell ID: -
Band: 1 - 2100MHz

Power Amplifier
Serial Number: 1934/025

Main Temperature: 20°C
Tx Power: Off
PA 1 Temp: 20°C
TRX Serial: 1934/025

Fig 45. NESIE UI – Sections

9.3 HEADER

The header bar, as shown below at Fig 46, will be displayed at the top of all NESIE pages and will float (remain) at the top of any screen that can be scrolled.

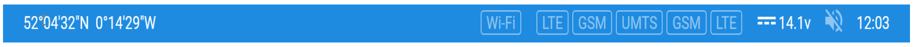


Fig 46. UI header bar

The header bar displays the following information:

9.3.1 GPS LOCATION

If a GPS location fix has been established, the position will be displayed in the format selected on the Settings page. An example of a Degrees/Minutes/Seconds fix is shown in Fig 47 below. If the GPS fix has not been established, then “No GPS Fix” will be displayed and an amber (non-critical) error will be generated by the system.

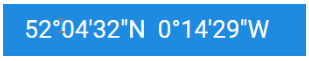


Fig 47. Header bar – GPS Fix

The operator has the option to change the GPS fix to other formats:

- **Degrees / Minutes / Seconds**
- **Degrees / Decimal Minutes**
- **Decimal Degrees**
- **Military Grid Reference System**

For instructions on how to change the GPS fix format that is displayed, see section 33.3.1.3**.**

9.3.2 ALERTS / WARNINGS

When necessary, important alerts and warnings will be displayed in the header bar. As shown in Fig 48 below, a critical (RED) notification has been displayed. When the user clicks on the red notification, more detailed information is available as well as the DISMISS button.

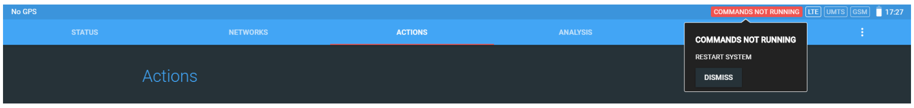


Fig 48. Header bar - alerts / warnings

9.3.3 WI-FI

If a Wi-Fi module (usually fitted in the Tactical of Strategic control module) is part of the system, the Wi-Fi module icon will be shown on the header bar. If the Wi-Fi module is idle, it will be greyed out. If the Wi-Fi module is conducting a Wi-Fi Grab, the icon will be shown in bold as shown below at Fig 49.

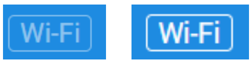


Fig 49. Wi-Fi Module Icon

9.3.4 CELLULAR MODULE & TECHNOLOGY

If a stack of NESIE modules is combined, the header bar will show how many modules are in the stack. In the example below, 3 modules have been combined to create a 3 stack. The header bar then displays the current technology that each individual module is configured for as shown below in Fig 50.

If the NESIE module is being used as a single channel, only one technology icon will be visible and it will rotate through LTE, UMTS and GSM as directed.

If the system is configured as a multiple channel system e.g: 3 Channel Peli NESIE, the system will most likely be set up to scan and transmit on all 3 technologies at the same time, therefore all 3 icons will be shown.

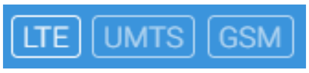


Fig 50. Header bar – technology

When the technology icons are grey, this indicates that the transceiver modules are in the listening / scanning (to the cellular networks) mode. If the icons are shown in bold, the transceiver modules are in transmitting (fake BTS) mode and will be listening to the reply from the cellular devices in the area.

9.3.5 ALARM SPEAKER / MUTE

The NESIE UI will sound an audible alert when a Target device is found or is placed into a Hold state. This alert will be heard on the speakers of the operators' device (laptop, tablet or mobile device). By default, the alert is activated. If required, the alerts can be muted by clicking on the speaker icon. The 2 possible options are displayed below at Fig 51.

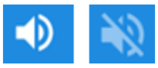
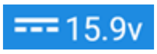


Fig 51. Header bar - speaker / mute

9.3.6 VOLTAGE / BATTERY STATUS

When the NESIE system is connected to a mains power supply unit or an external battery, the UI will display the current voltage.

When connected to a mains power supply or an external 12V battery the symbol shown below in figure Fig 52 will be displayed. This symbol shows that DC power is applied along with the current voltage supplied.



⎓ 15.9v

Fig 52. Header bar – DC power supply

If the NESIE unit has an internal battery fitted (only available in the Covert NESIE) the battery status will be displayed in the format shown at Fig 53 below.

This icon displays the battery charge status. If an external power supply is connected, the charging symbol will appear inside the battery symbol. The battery status will be:

- Fully charged
- Partially charged (showing % of charge)
- Charging

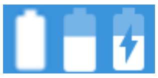


Fig 53. Header bar – battery status

9.3.7 SYSTEM TIME

The system time is displayed on the header bar of the NESIE UI. This time can be displayed as 12 hour or 24 hour format. As displayed in Fig 54 below.

This system time is used to log all events on the NESIE software. It is therefore important for the user to set the time correctly.

Fig 54. Header bar – system time

9.3.8 HEADER BAR COLOURS

The Header bar will be shown in one of three colours, depending on the current state of the system:

- Blue – Idle

When the NESIE is in idle mode, it will display the blue header bar. However, the transceivers are normally in receive mode.

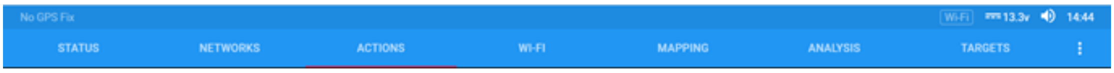


Fig 55. Header bar colour – blue

- Purple – Paused transmit for Network Scan.

  The header bar will be displayed in purple whenever the NESIE system has paused transmitting to conduct additional network scanning, as shown below in Fig 56. This pause may be at the begging of the transmit cycle to check the network scan data or after one complete transmit cycle.

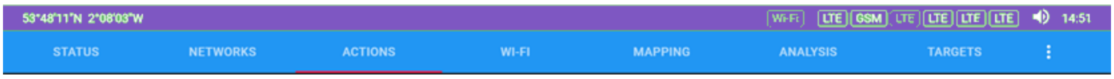


Fig 56. Header bar colour – purple

- Green – Transmitting.

Whenever the NESIE system is transmitting, the header bar will change colour to green, as shown below at Fig 57.

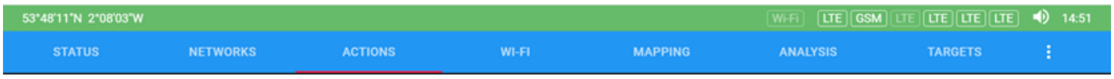


Fig 57. Header bar colour – green

9.4 MENU BUTTONS

Situated under the header bar are the NESIE menu buttons. By clicking on these buttons, the operator can navigate across the UI. The selected menu button will be highlighted by a thin red bar, as shown in Fig 58 below.

> **NOTE: Depending on the NESIE system used, the MAPPING button may or may not be visible on the header bar. If the system does not have mapping available, the MAPPING button will not be visible.**

The individual pages and options will be described in detail in the remainder of this manual.

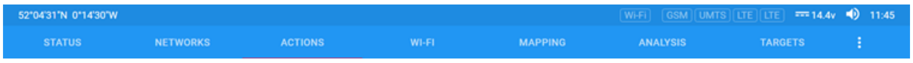


Fig 58. UI menu buttons

9.4.1 NOTIFICATIONS

At times during the operation, notifications will be displayed next to the relevant menu button bar. These notifications can be displayed in green for information or red for warnings. Multiple notifications will be represented by a number inside the notification icon. It can be seen below at Fig 59 that two green notifications are available on the ACTIONS page.

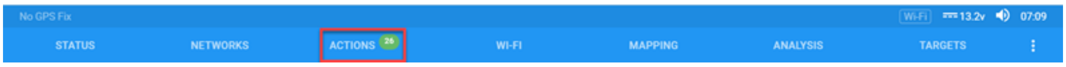
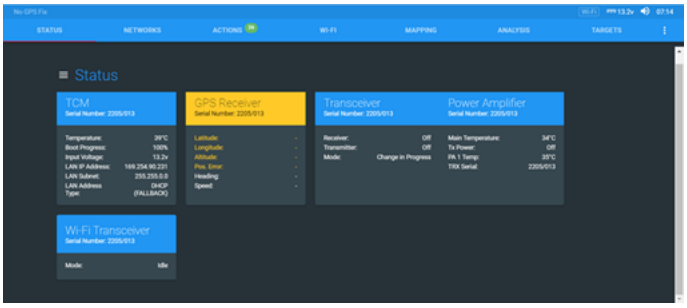


Fig 59. UI menu buttons – notifications

9.4.2 STATUS PAGE

The STATUS page is the default log on page and displays the status of any resources that are being used by the NESIE system. The STATUS page for a Covert Ground system is as shown below at Fig 60. A more detailed description of the STATUS page is available at section 10.



Status

TCM
Serial Number: 2205/013

Temperature: 39°C
Boot Progress: 100%
Input Voltage: 13.2v
LAN IP Address: 169.254.90.231
LAN Subnet: 255.255.0.0
LAN Address Type: DHCP (FALLBACK)

GPS Receiver
Serial Number: 2205/013

Latitude: -
Longitude: -
Altitude: -
Pos. Error: -
Heading: -
Speed: -

Transceiver
Serial Number: 2205/013

Receiver: Off
Transmitter: Off
Mode: Change in Progress

Power Amplifier
Serial Number: 2205/013

Main Temperature: 34°C
Tx Power: Off
PA 1 Temp: 35°C
TRX Serial: 2205/013

Wi-Fi Transceiver
Serial Number: 2205/013

Mode: Idle

Fig 60. UI menu buttons – STATUS page

9.4.3 NETWORKS PAGE

The NETWORKS page displays the over the air information that is broadcast by the mobile network operators. NESIE collects this GSM, UMTS and LTE data and stores it for future use. The NETWORKS page and a sample set of data is shown below at Fig 61. A more detailed description of the NETWORKS page is available in section 12.

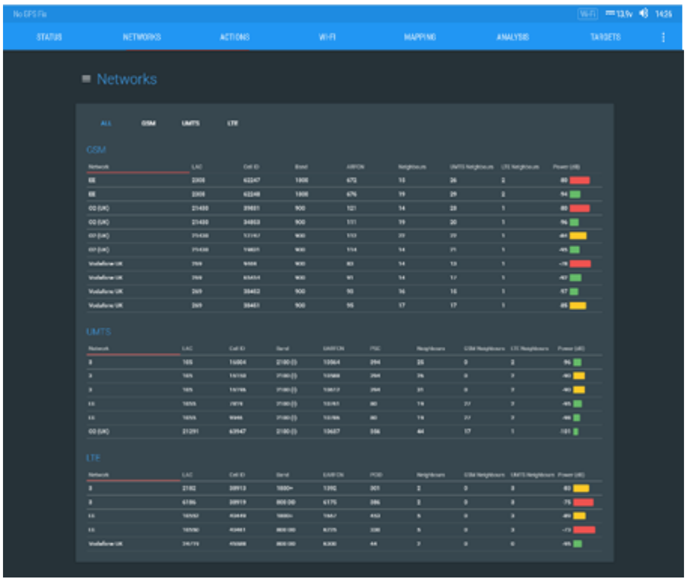


Fig 61. UI menu buttons – NETWORS page

9.4.4 ACTIONS PAGE

The ACTIONS page is the main page of the UI and the operator will become very familiar with its layout. This page enables the operator to make the NESIE carry out the operational functions of the system. A blank ACTIONS page is shown below at Fig 62. A more detailed description of the ACTIONS page is available in section 17.

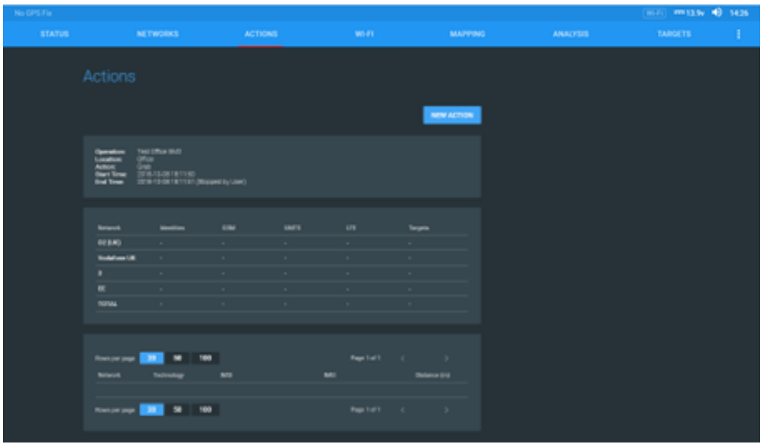


Fig 62. UI menu buttons – ACTIONS page

9.4.5 MAPPING PAGE

The MAPPING page is used to display the location of the NESIE system and any locations of Target devices that have been calculated or extracted by the NESIE software. An example of the MAPPING page is shown below at Fig 63. A more detailed description of the MAPPING page is available in section 24.

NOTE: Depending on the NESIE system being used, the MAPPING button may or may not be visible on the header bar.

The mapping is not normally available on Covert Ground systems or if a Tactical Ground system is being used in standalone mode.

If the system does not have mapping available, the MAPPING button will not be displayed.

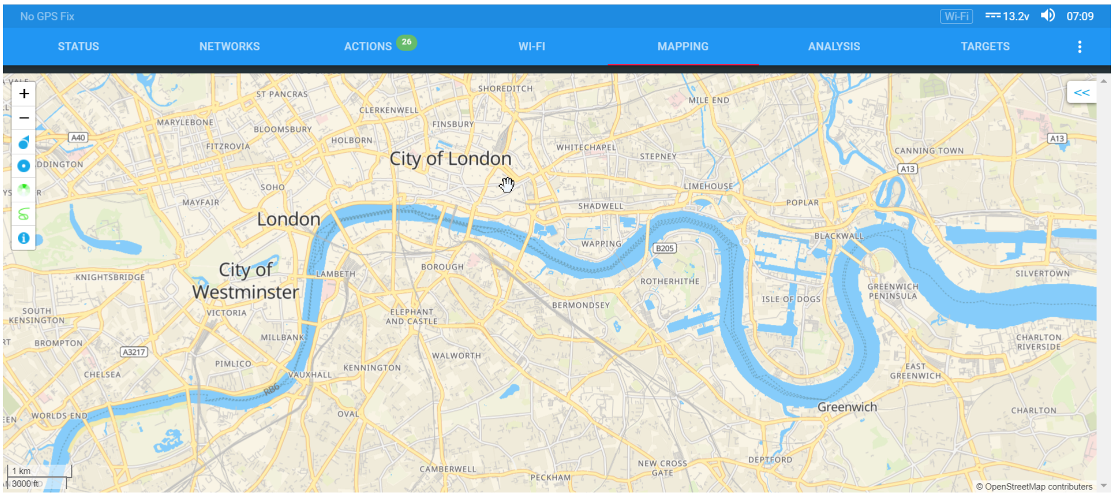
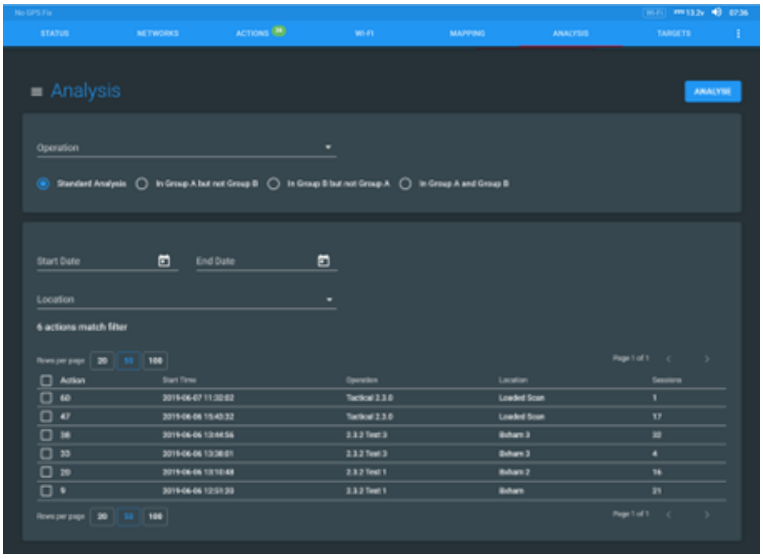


Fig 63. UI menu buttons – MAPPING page

9.4.6 ANALYSIS PAGE

The ANALYSIS page allows the operator to combine and compare different data sets to identify the Target cellular device. A sample ANALYSIS page is displayed below at Fig 64. A more detailed description of the ANALYSIS page is available in section 32.



Analysis

Operation

● Standard Analysis ○ In Group A but not Group B ○ In Group B but not Group A ○ In Group A and Group B

Start Date

End Date

Location

6 actions match filter

Rows per page 20 50 100 Page 1 of 1

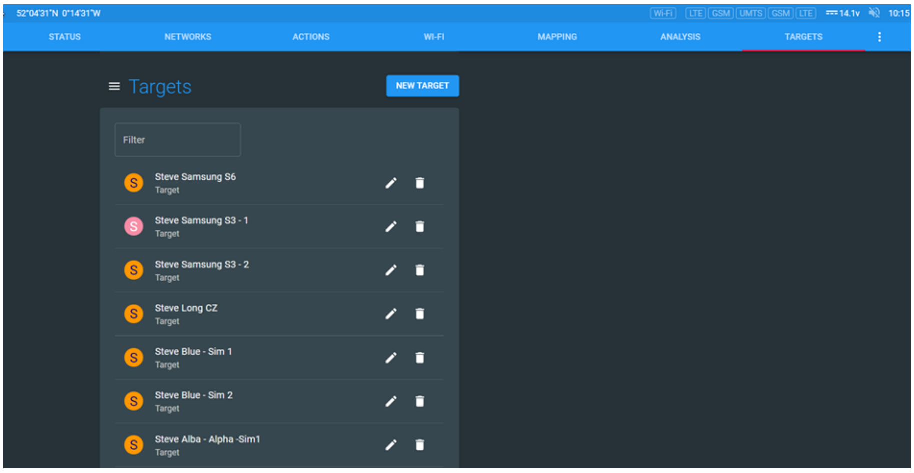
□ Action	Start Time	Operation	Location	Sessions
□ 60	2019-06-07 11:32:02	Tactical 2.3.0	Loaded Scan	1
□ 47	2019-06-06 15:43:32	Tactical 2.3.0	Loaded Scan	17
□ 38	2019-06-06 13:44:56	2.3.2 Test 3	Bxham 3	32
□ 33	2019-06-06 13:38:01	2.3.2 Test 3	Bxham 3	4
□ 20	2019-06-06 13:10:48	2.3.2 Test 1	Bxham 2	16
□ 9	2019-06-06 12:51:30	2.3.2 Test 1	Bxham	21

Rows per page 20 50 100 Page 1 of 1

Fig 64. UI menu buttons – ANALYSIS page

9.4.7 TARGETS PAGE

The TARGETRS page is used by the operator to add, edit or delete Target cellular devices from the Target list. A sample Target list is displayed below at Fig 65. A more detailed description of the TARGETS page is available in Section 13120.



Targets

Filter

- S Steve Samsung S6 – Target
- S Steve Samsung S3 - 1 – Target
- S Steve Samsung S3 - 2 – Target
- S Steve Long CZ – Target
- S Steve Blue - Sim 1 – Target
- S Steve Blue - Sim 2 – Target
- S Steve Alba - Alpha -Sim1 – Target

Fig 65. UI menu buttons – TARGETS page

9.4.8 ADDITIONAL MENU OPTIONS ICON

The additional menu options (three dots) icon, is used to manage the passwords, settings and other menu items that are not normally accessed regularly by the NESIE operator.

The icon is displayed in the red box in Fig 66 below. A more detailed description of the functions that can be viewed and altered via the additional menu icon drop-down can be found in Section 33.

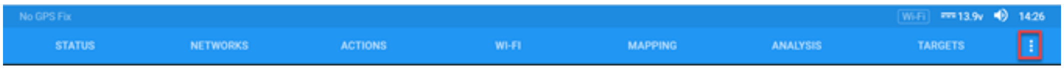


Fig 66. UI menu buttons – additional menu options Icon

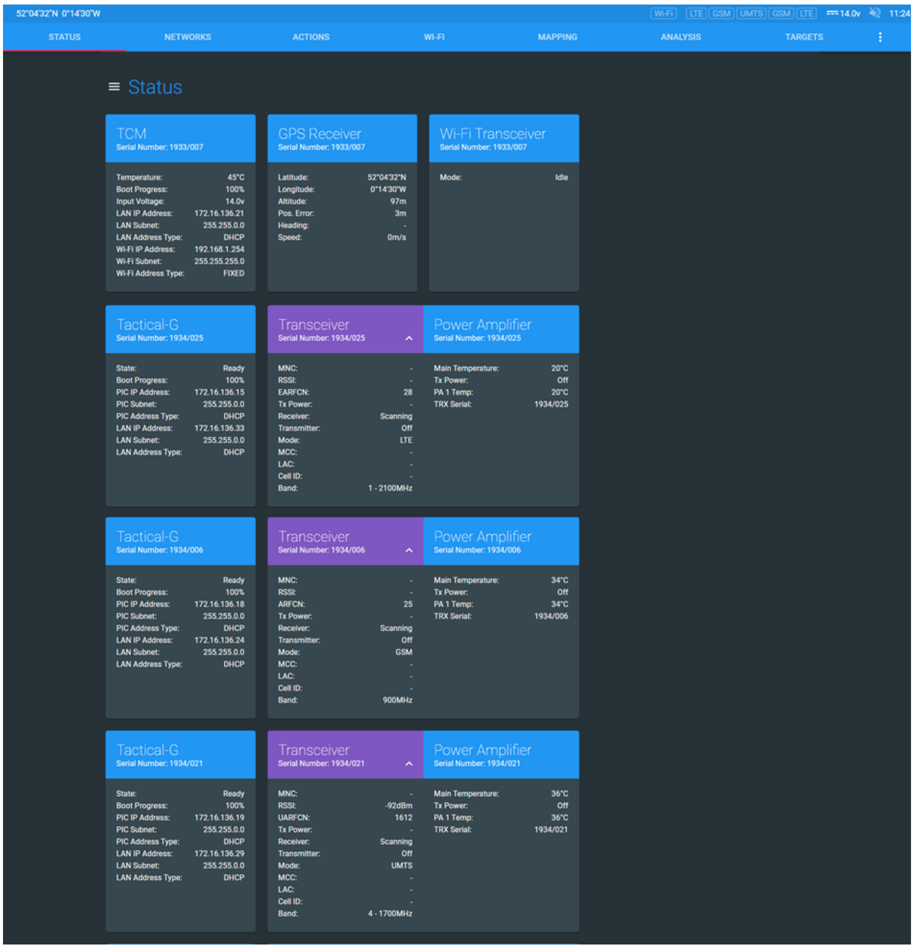
10. STATUS PAGE

The NESIE system will automatically detect if multiple resources are connected in a stack using a control module, via an ethernet cable or a switch.

The system will display each available resource and its status on the STATUS page. For example, if there are three NESIE transceivers modules with attached Power Amplifiers plus a control module (that is fitted with a Wi-Fi module and GPS module) these will all be displayed.

As an example, it can be seen in Fig 67 that this system is a 3 Stack Tactical NESIE system comprises of:

- 1 x Tactical Control Module (TCM) displaying
  - TCM status
  - GPS receiver
  - Wi-Fi transceiver
- 3 x Tactical Ground Modules displaying:
  - Tactical-G status
  - transceiver status
  - Power Amplifier status



TCM
Serial Number: 1933/007

Temperature:	45°C
Boot Progress:	100%
Input Voltage:	14.0v
LAN IP Address:	172.16.136.21
LAN Subnet:	255.255.0.0
LAN Address Type:	DHCP
Wi-Fi IP Address:	192.168.1.254
Wi-Fi Subnet:	255.255.255.0
Wi-Fi Address Type:	FIXED

GPS Receiver
Serial Number: 1933/007

Latitude:	52°04'32"N
Longitude:	0°14'30"W
Altitude:	97m
Pos. Error:	3m
Heading:	-
Speed:	0m/s

Wi-Fi Transceiver
Serial Number: 1933/007

Mode:	Idle

Tactical-G
Serial Number: 1934/025

State:	Ready
Boot Progress:	100%
PIC IP Address:	172.16.136.15
PIC Subnet:	255.255.0.0
PIC Address Type:	DHCP
LAN IP Address:	172.16.136.33
LAN Subnet:	255.255.0.0
LAN Address Type:	DHCP

Transceiver
Serial Number: 1934/025

MNC:	-
RSSI:	-
EARFCN:	28
Tx Power:	-
Receiver:	Scanning
Transmitter:	Off
Mode:	LTE
MCC:	-
LAC:	-
Cell ID:	-
Band:	1 - 2100MHz

Power Amplifier
Serial Number: 1934/025

Main Temperature:	20°C
Tx Power:	Off
PA 1 Temp:	20°C
TRX Serial:	1934/025

Tactical-G
Serial Number: 1934/006

State:	Ready
Boot Progress:	100%
PIC IP Address:	172.16.136.18
PIC Subnet:	255.255.0.0
PIC Address Type:	DHCP
LAN IP Address:	172.16.136.24
LAN Subnet:	255.255.0.0
LAN Address Type:	DHCP

Transceiver
Serial Number: 1934/006

MNC:	-
RSSI:	-
ARFCN:	25
Tx Power:	-
Receiver:	Scanning
Transmitter:	Off
Mode:	GSM
MCC:	-
LAC:	-
Cell ID:	-
Band:	900MHz

Power Amplifier
Serial Number: 1934/006

Main Temperature:	34°C
Tx Power:	Off
PA 1 Temp:	34°C
TRX Serial:	1934/006

Tactical-G
Serial Number: 1934/021

State:	Ready
Boot Progress:	100%
PIC IP Address:	172.16.136.19
PIC Subnet:	255.255.0.0
PIC Address Type:	DHCP
LAN IP Address:	172.16.136.29
LAN Subnet:	255.255.0.0
LAN Address Type:	DHCP

Transceiver
Serial Number: 1934/021

MNC:	-
RSSI:	-92dBm
UARFCN:	1612
Tx Power:	-
Receiver:	Scanning
Transmitter:	Off
Mode:	UMTS
MCC:	-
LAC:	-
Cell ID:	-
Band:	4 - 1700MHz

Power Amplifier
Serial Number: 1934/021

Main Temperature:	36°C
Tx Power:	Off
PA 1 Temp:	36°C
TRX Serial:	1934/021

Fig 67. STATUS page

10.1 RESOURCE BAR COLOURS

The resource panes header bars display different colours depending on the current mode. The colours / modes are shown below:

🟦 Blue – Resource is on but currently idle or switching software.

🟪 Purple – The transceiver is in receive mode.

🟨 Amber – the resource has a warning/non-critical alert.

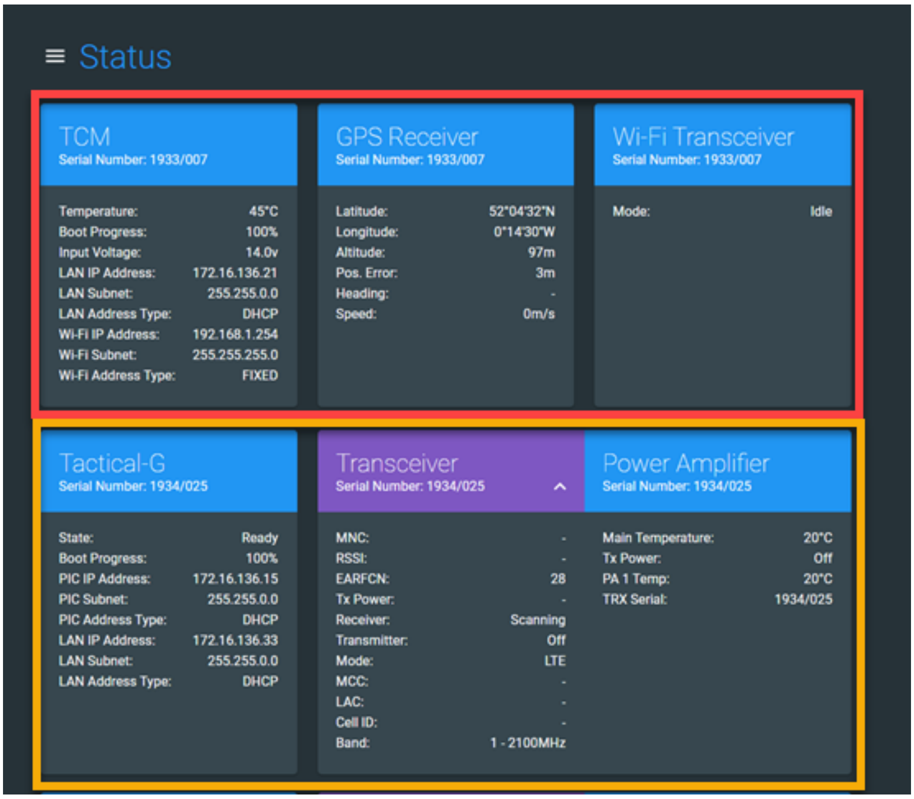
🟩 Green – the transceiver is in currently transmitting.

Note: Normally whenever a NESIE system is in idle mode, the transceiver is actually in scanning (the cellular networks) mode.

10.2 RESOURCE PANES

In Fig 68 below, each line or block of panes represents a different module in the stack. In this example, the TCM is shown in the top line (red box) and the Tactical G unit is shown in the second line (amber box).

The resources shown and the lay out of the UI will vary according to the NESIE system and associated components.



≡ Status

TCM
Serial Number: 1933/007

Temperature:	45°C
Boot Progress:	100%
Input Voltage:	14.0v
LAN IP Address:	172.16.136.21
LAN Subnet:	255.255.0.0
LAN Address Type:	DHCP
Wi-Fi IP Address:	192.168.1.254
Wi-Fi Subnet:	255.255.255.0
Wi-Fi Address Type:	FIXED

GPS Receiver
Serial Number: 1933/007

Latitude:	52°04'32"N
Longitude:	0°14'30"W
Altitude:	97m
Pos. Error:	3m
Heading:	-
Speed:	0m/s

Wi-Fi Transceiver
Serial Number: 1933/007

Mode:	Idle

Tactical-G
Serial Number: 1934/025

State:	Ready
Boot Progress:	100%
PIC IP Address:	172.16.136.15
PIC Subnet:	255.255.0.0
PIC Address Type:	DHCP
LAN IP Address:	172.16.136.33
LAN Subnet:	255.255.0.0
LAN Address Type:	DHCP

Transceiver
Serial Number: 1934/025

MNC:	-
RSSI:	-
EARFCN:	28
Tx Power:	-
Receiver:	Scanning
Transmitter:	Off
Mode:	LTE
MCC:	-
LAC:	-
Cell ID:	-
Band:	1 - 2100MHz

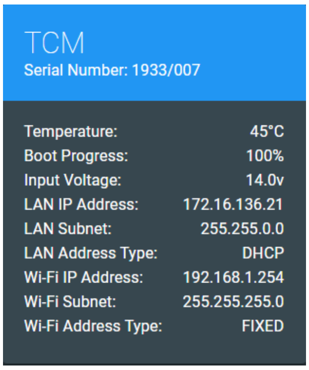
Power Amplifier
Serial Number: 1934/025

Main Temperature:	20°C
Tx Power:	Off
PA 1 Temp:	20°C
TRX Serial:	1934/025

Fig 68. Resource panes

10.2.1 CONTROL MODULE – STATUS PANE

The information shown in the control module status pane will vary slightly depending on the type of NESIE system / type of control module in the system. However, the overall settings of the system will be displayed as in Fig 69 below.



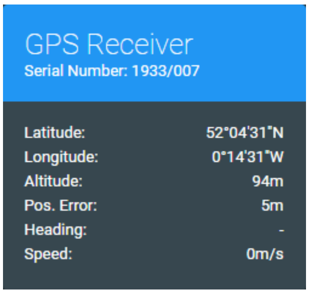
TCM
Serial Number: 1933/007

Temperature: 45°C
Boot Progress: 100%
Input Voltage: 14.0v
LAN IP Address: 172.16.136.21
LAN Subnet: 255.255.0.0
LAN Address Type: DHCP
Wi-Fi IP Address: 192.168.1.254
Wi-Fi Subnet: 255.255.255.0
Wi-Fi Address Type: FIXED

Fig 69. Control module

- **Name** TCM or SCM
- **Serial Number** Serial number of the control module in the stack
- **Temperature** Temperature of the control module
- **Boot Progress** Percentage of boot progress completed
- **Input Voltage** Voltage applied to the system
- **LAN IP address** LAN IP address of the module
- **LAN Subnet** LAN Subnet address
- **LAN Address Type** DHCP
- **Wi-Fi IP address** Default Wi-Fi IP address
- **Wi-Fi Subnet** Wi-Fi Subnet address
- **Wi-Fi Address Type** FIXED

10.2.2 CONTROL MODULE - GPS RECEIVER PANE



GPS Receiver
Serial Number: 1933/007

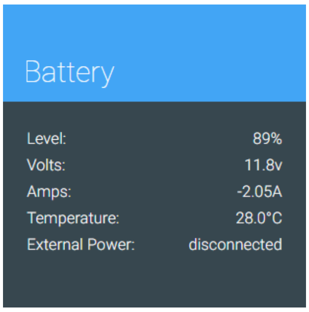
Latitude: 52°04'31"N
Longitude: 0°14'31"W
Altitude: 94m
Pos. Error: 5m
Heading: -
Speed: 0m/s

Fig 70. GPS receiver pane

- **Name:** GPS receiver
- **Serial Number:** Serial number of control module
- **Latitude:** Latitude received by the NESIE GPS
- **Longitude:** Longitude received by the NESIE GPS
- **Pos. Error:** Any error or no fix has been calculated by the GPS
- **Heading:** Shown if NESIE is moving – displayed in true degrees
- **Speed:** Shown if the NESIE system is moving

10.2.3 BATTERY PANE

Only displayed if an internal battery is fitted to the NESIE system (usually only in the Covert Ground system).



Battery

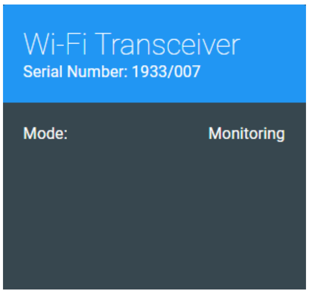
Level: 89%
Volts: 11.8v
Amps: -2.05A
Temperature: 28.0°C
External Power: disconnected

Fig 71. Battery pane

Level:	Percentage of the battery remaining
Volts:	The current battery voltage remaining
Amps:	The current draw of the equipment
Temperature:	Current battery temperatures
External Power:	Indicates if external power is connected

10.2.4 CONTROL MODULE - WI-FI TRANSCEIVER PANE

If the NESIE system is fitted with a Wi-Fi module, an additional pane for the Wi-Fi module will be displayed.



Wi-Fi Transceiver
Serial Number: 1933/007

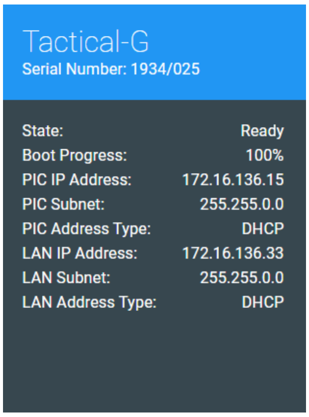
Mode: Monitoring

Fig 72. Wi-Fi transceiver pane

Name:	Wi-Fi transceiver
Serial number:	Serial number of the control module
Mode:	Current mode of Wi-Fi transceiver

Idle	When the Wi-Fi transceiver is not listening to the Wi-Fi data
Monitoring	Displayed when the Wi-Fi transceiver is switched to monitor the Wi-Fi networks

10.2.5 NESIE MODULE – STATUS PANE



Tactical-G
Serial Number: 1934/025

State:	Ready
Boot Progress:	100%
PIC IP Address:	172.16.136.15
PIC Subnet:	255.255.0.0
PIC Address Type:	DHCP
LAN IP Address:	172.16.136.33
LAN Subnet:	255.255.0.0
LAN Address Type:	DHCP

Fig 73. NESIE modules

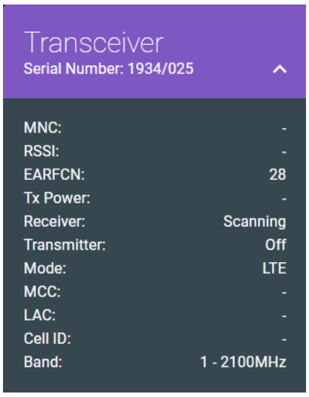
- **Name:** Name of the transceiver module
- **Serial Number:** Serial number of the transceiver module
- **State:** Current state of the module
- **Boot Process:** Percentage of boot progress completed
- **PIC IP Address:** PIC address of the module
- **PIC Subnet:** PIC subnet address
- **PIC Address Type:** PIC address type
- **LAN IP Address:** LAN IP address of the module
- **LAN Subnet:** LAN subnet address
- **LAN Address Type:** DHCP

10.2.6 NESIE MODULE – TRANSCEIVER PANE

The NESIE system you use may contain various types of transceivers that can be in different modes and states. The types and current modes/states are indicated by the colour of the header as can be seen below.

🟪 Multi Transceiver	Purple	transceiver (Multi Tech) in network scan mode
🟩 GSM Transceiver	Green	transceiver in transmit mode
🟦 UMTS Transceiver	Blue	transceiver in software swap or idle mode
🟥 Multi Transceiver	Red	system error

Note: if the NESIE system consists of only one transceiver module, this module will automatically switch between technology modes (GSM, UMTS & LTE). This single module will then normally display as a Multi (Mode) transceiver/



Transceiver
Serial Number: 1934/025

MNC:	-
RSSI:	-
EARFCN:	28
Tx Power:	-
Receiver:	Scanning
Transmitter:	Off
Mode:	LTE
MCC:	-
LAC:	-
Cell ID:	-
Band:	1 - 2100MHz

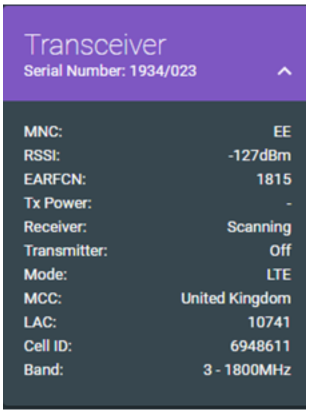
Fig 74. transceiver pane – scanning

10.2.6.1 TRANSCEIVER PANE - SCANNING

Upon initial boot up, the NESIE system automatically starts to scan the user defined cellular radio frequency environment on the downlink frequencies; to gather the cellular network provider's settings. The transceiver pane will display Scanning when it is conducting a Network Scan as shown Fig 74 above. This scanning is also shown by the header bar being purple.

As the network scan progresses, NESIE will listen to the whole of the selected bands and attempt to decode the data transmitted by the network providers. This scan will be shown by the changes to the channel number (ARFCN for GSM, UARFCN for UMTS and EARFCN for LTE) and the changes to the band. If NESIE has not detected any network data on the channel, the pane will remain blank, as shown above.

If network data is detected, the relevant data will be displayed in the transceiver pane shown below at Fig 75.



Transceiver
Serial Number: 1934/023

MNC:	EE
RSSI:	-127dBm
EARFCN:	1815
Tx Power:	-
Receiver:	Scanning
Transmitter:	Off
Mode:	LTE
MCC:	United Kingdom
LAC:	10741
Cell ID:	6948611
Band:	3 - 1800MHz

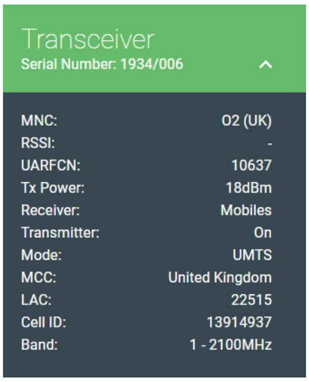
Fig 75. transceiver pane – network data

The transceivers will automatically enter the scanning state whenever the system is powered on and not transmitting a fake base station. This may be when initially powered up or after transmitting.

NESIE gathers this network data for GSM, UMTS and LTE and stores it on the NETWORKS page, for more information refer to section 12.

10.2.6.2 TRANSCEIVER PANE - MOBILES

Mobiles will be shown in the transceiver pane when NESIE is transmitting a fake base station on the downlink and receiving the return signal from the Mobiles (Cellular devices) on the uplink frequency.



Transceiver
Serial Number: 1934/006

MNC:	O2 (UK)
RSSI:	-
UARFCN:	10637
Tx Power:	18dBm
Receiver:	Mobiles
Transmitter:	On
Mode:	UMTS
MCC:	United Kingdom
LAC:	22515
Cell ID:	13914937
Band:	1 - 2100MHz

Fig 76. transceiver pane – mobiles

The transceivers automatically stop scanning the cellular network providers (Downlink) whilst transmitting its own fake base station on the Downlink. The receive section of the transceiver now switches to listening for the mobile devices that are responding to the NESIE transmissions, sending data on the uplink.

The transceiver panes contain the following information.

- **Name:** transceiver or Multi transceiver
- **Serial Number** Serial number of NESIE module

- **Receiver:** Current mode of transceiver

  Scanning: Receiving the network data (downlink)
  Mobiles: Receiving the signal from the cellular devices (uplink)

- **Transmitter:** Current state of transmitter

  Off: Not transmitting
  On: Transmitter on and producing a fake BTS

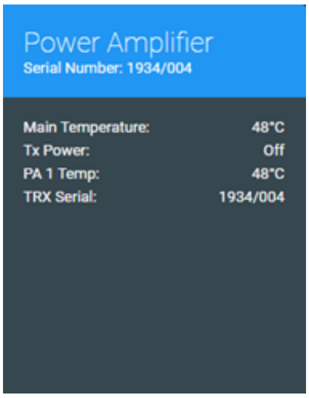
- **Mode:** Current technology mode of the transceiver
- **RSSI:** Relative Received Signal Strength (dBm)
- **Band:** Band NESIE is currently receiving or transmitting on
- **ARFCN*:** GSM channel number NESIE is transmitting on
- **UARFCN*:** UMTS channel number NESIE is transmitting on
- **EARFCN*:** LTE channel number NESIE is transmitting on
- **PSC*:** Primary Spreading Code transmitted by NESIE
- **MCC:** Mobile Country Code transmitted by NESIE
- **MNC:** Mobile Network Code transmitted by NESIE
- **LAC:** Local Area Code transmitted by NESIE
- **Cell ID:** Cell ID transmitted by NESIE
- **PCID*:** Physical Cell ID transmitted by NESIE
- **Tx Power:** Power transmitted by NESIE (dBm)

*** - The relevant field will be displayed depending on which technology is being transmitted**

10.2.7 NESIE MODULE - POWER AMPLIFIER PANE

If the NESIE system has amplifiers attached', the Power Amplifier pane will be attached to the associated transceiver. The power amplifier will only ever be in one of two states:

Off: Power Amplifier is on standby but not transmitting
This is indicated by the header bar showing blue.



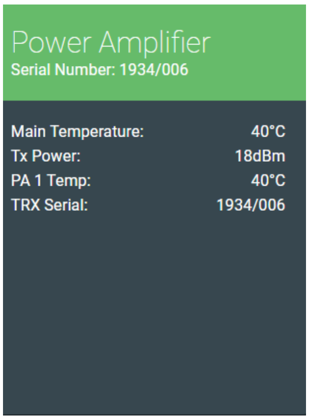
Power Amplifier
Serial Number: 1934/004

Main Temperature:	48°C
Tx Power:	Off
PA 1 Temp:	48°C
TRX Serial:	1934/004

Fig 77. Power Amplifier pane – idle

Transmitting: The power amplifier will show the current transmit power being produced by the amplifier.

The header bar will show green when transmitting.



Power Amplifier
Serial Number: 1934/006

Main Temperature:	40°C
Tx Power:	18dBm
PA 1 Temp:	40°C
TRX Serial:	1934/006

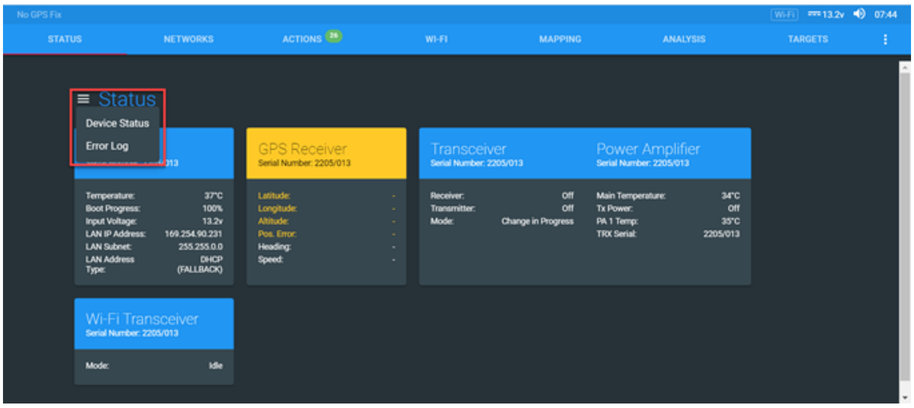
Fig 78. Power Amplifier pane - transmitting

- **Name:** Power Amplifier
- **Serial Number:** Serial number of the NESIE / PA Module
- **Main Temperature:** Current temperature of the amplifier
- **Tx Power:** Current power of signal being transmitted
- **PA 1 Temp:** Temperature of the amplifier
- **TRX Serial:** Serial number of amplifier if different to the NESIE

11. STATUS – SUB MENU

There is also the option for the user to use the Status sub menu as shown in Fig 79 below. The sub menu allows the following options:

- **Device Status**
- **Error Log**



GPS Receiver
Serial Number: 2205/013

Transceiver
Serial Number: 2205/013

Power Amplifier
Serial Number: 2205/013

Temperature: 37°C
Boot Progress: 100%
Input Voltage: 13.2v
LAN IP Address: 169.254.90.231
LAN Subnet: 255.255.0.0
LAN Address Type: DHCP (FALLBACK)

Latitude: -
Longitude: -
Altitude: -
Pos. Error: -
Heading: -
Speed: -

Receiver: Off
Transmitter: Off
Mode: Change in Progress

Main Temperature: 34°C
Tx Power: Off
PA 1 Temp: 35°C
TRX Serial: 2205/013

Wi-Fi Transceiver
Serial Number: 2205/013

Mode: Idle

Fig 79. Status – sub menu

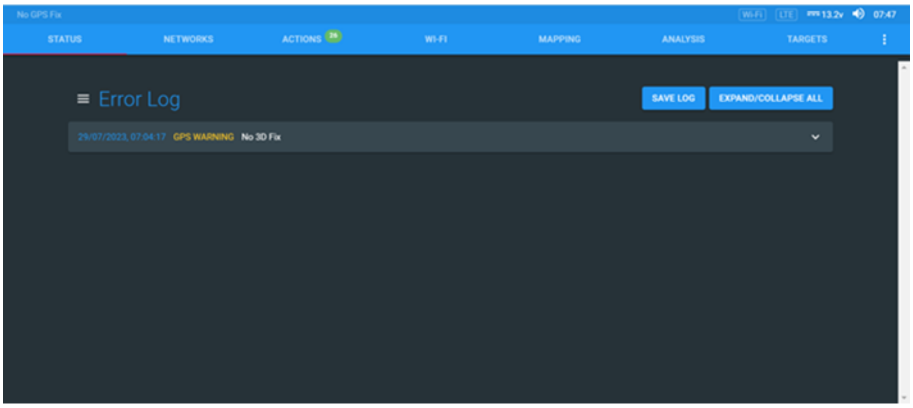
11.1 DEVICE STATUS

The device status button allows the user to navigate back to the main status display, usually after loOKing at the error log.

11.2 ERROR LOG

When the operator clicks the error log button, the UI will navigate to the error log page. Any errors that occur will be displayed in this page. Upon opening the page, the list will be displayed in compacted format. However, if required each error can be expanded by pressing the white ^ arrow as shown below at Fig 80 below.

There is also the option to expand or collapse all errors displayed by using the EXPAND/COLLAPSE ALL button.

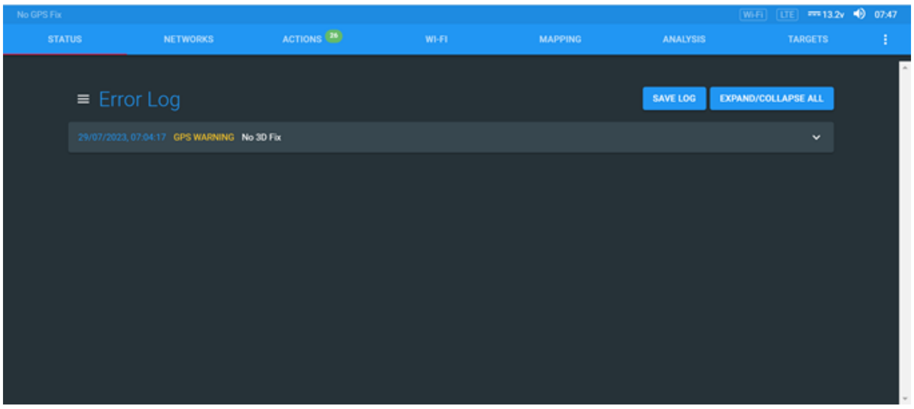


29/07/2023, 07:04:17 GPS WARNING No 3D Fix

Fig 80. Error log

11.2.1 ERROR MESSAGE

When the error message is expanded (individually or the whole log) the message will loOK similar to that shown at Fig 81 below.



29/07/2023, 07:04:17 GPS WARNING No 3D Fix

Fig 81. Error message & code

The error message consists of:

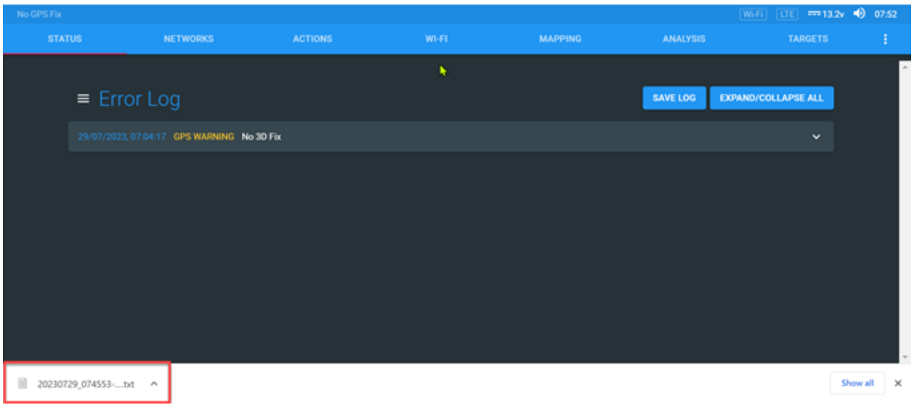
Date & Time: when error occurred
Error Message: Shown in amber / red
Remedial Action: What action should be carried out by the operator
Error Code: A unique code generated by the NESIE software

11.2.2 ERROR CODE

The unique error code generated by the NESIE software will usually allow the Smith Myers engineers to more accurately identify the fault with the system. This error code can be photographed, noted down or saved then sent to Smith Myers.

11.2.3 SAVE ERROR LOG

If required, the operator can save the error log by pressing the SAVE LOG button. A text (txt) file will be created and downloaded to the operator's tablet / laptop as shown in Fig 82 below.



29/07/2023, 07:04:17 GPS WARNING No 3D Fix

20230729_074553-....txt

Fig 82. Error log – save

If required, this error log could then be sent to Smith Myers for further fault finding.

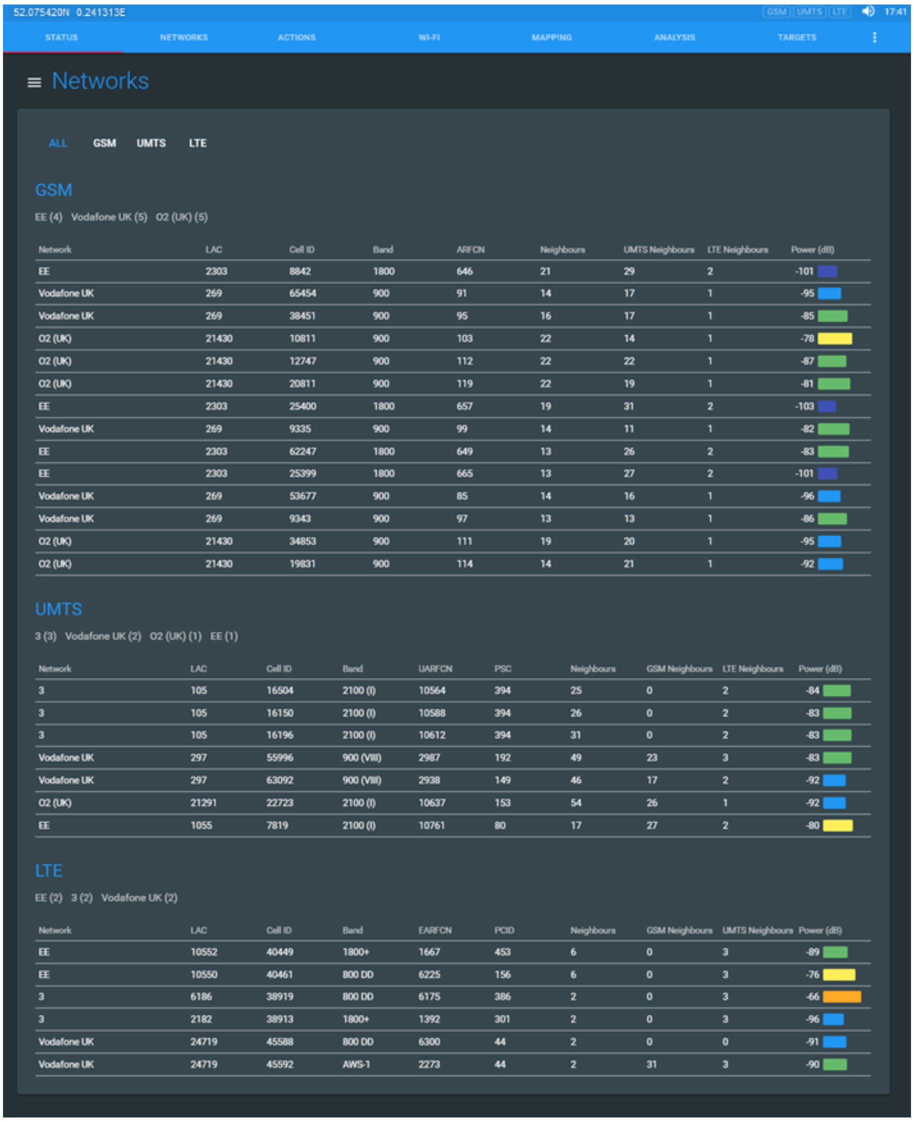
NOTE: The current error log will be deleted when the system is powered off. If the log is to be saved, it should be done prior to powering down the system.

12. NETWORKS PAGE & NETWORK SCAN

Upon power on, the NESIE system transceivers will automatically commence a network scan on all user programmed cellular bands (as detailed in Section 7.1.2 above).

The NESIE will use all available transceivers to conduct the network scan. If 3 or more transceivers are available, one will normally be allocated to each technology (GSM, UMTS and LTE). If less transceivers are available, the NESIE system will allocate transceivers to technologies, and where required switch between technologies.

As the network scan is running any decoded data will be displayed on the NETWORKS page as shown below in Fig 83.



GSM

EE (4) Vodafone UK (5) O2 (UK) (5)

Network	LAC	Cell ID	Band	ARFCN	Neighbours	UMTS Neighbours	LTE Neighbours	Power (dB)
EE	2303	8842	1800	646	21	29	2	-101 🟦
Vodafone UK	269	65454	900	91	14	17	1	-95 🟦
Vodafone UK	269	38451	900	95	16	17	1	-85 🟩
O2 (UK)	21430	10811	900	103	22	14	1	-78 🟨
O2 (UK)	21430	12747	900	112	22	22	1	-87 🟩
O2 (UK)	21430	20811	900	119	22	19	1	-81 🟩
EE	2303	25400	1800	657	19	31	2	-103 🟦
Vodafone UK	269	9335	900	99	14	11	1	-82 🟩
EE	2303	62247	1800	649	13	26	2	-83 🟩
EE	2303	25399	1800	665	13	27	2	-101 🟦
Vodafone UK	269	53677	900	85	14	16	1	-96 🟦
Vodafone UK	269	9343	900	97	13	13	1	-86 🟩
O2 (UK)	21430	34853	900	111	19	20	1	-95 🟦
O2 (UK)	21430	19831	900	114	14	21	1	-92 🟦

UMTS

3 (3) Vodafone UK (2) O2 (UK) (1) EE (1)

Network	LAC	Cell ID	Band	UARFCN	PSC	Neighbours	GSM Neighbours	LTE Neighbours	Power (dB)
3	105	16504	2100 (I)	10564	394	25	0	2	-84 🟩
3	105	16150	2100 (I)	10588	394	26	0	2	-83 🟩
3	105	16196	2100 (I)	10612	394	31	0	2	-83 🟩
Vodafone UK	297	55996	900 (VIII)	2987	192	49	23	3	-83 🟩
Vodafone UK	297	63092	900 (VIII)	2938	149	46	17	2	-92 🟦
O2 (UK)	21291	22723	2100 (I)	10637	153	54	26	1	-92 🟦
EE	1055	7819	2100 (I)	10761	80	17	27	2	-80 🟨

LTE

EE (2) 3 (2) Vodafone UK (2)

Network	LAC	Cell ID	Band	EARFCN	PCID	Neighbours	GSM Neighbours	UMTS Neighbours	Power (dB)
EE	10552	40449	1800+	1667	453	6	0	3	-89 🟩
EE	10550	40461	800 DD	6225	156	6	0	3	-76 🟨
3	6186	38919	800 DD	6175	386	2	0	3	-66 🟧
3	2182	38913	1800+	1392	301	2	0	3	-96 🟦
Vodafone UK	24719	45588	800 DD	6300	44	2	0	0	-91 🟦
Vodafone UK	24719	45592	AWS-1	2273	44	2	31	3	-90 🟩

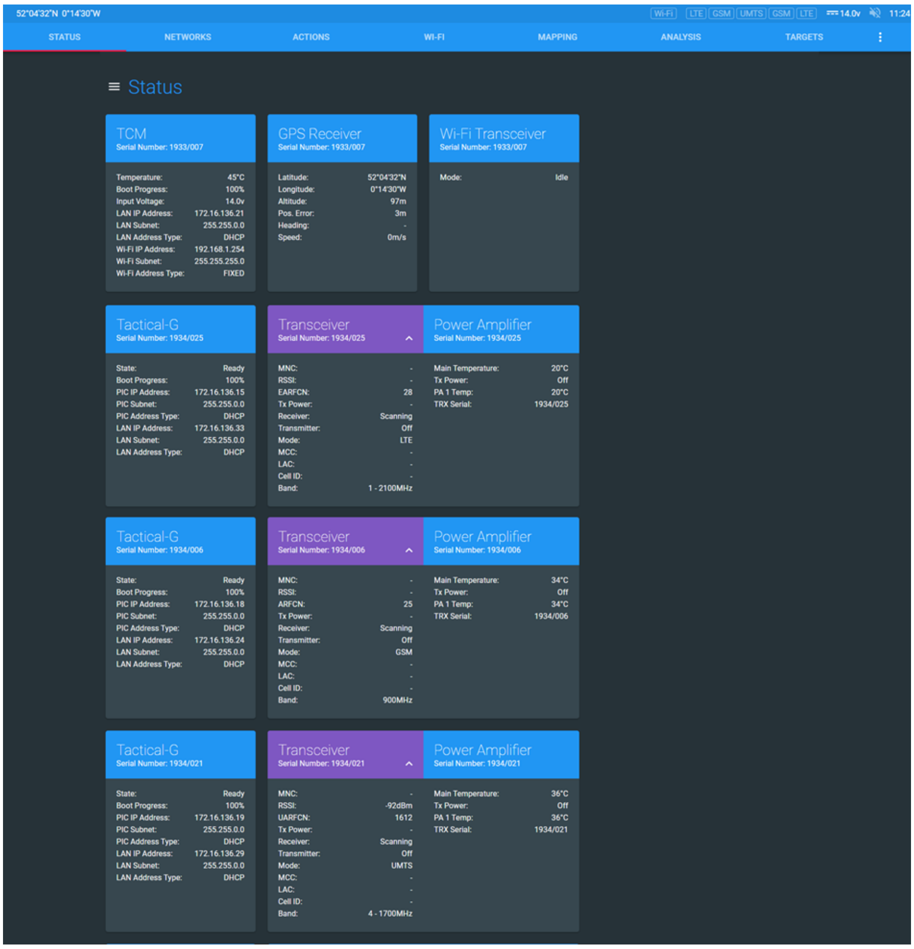
Fig 83. Network scan data

12.1 NETWORK SCAN – 3 CHANNEL NESIE

In Fig 84 below, there are 3 transceivers in the NESIE system. Therefore, NESIE will allocate one transceiver to conduct a network scan on each technology. The fact that NESIE is carrying out a network scan is indicated by the purple bar shown on each transceiver pane. Each transceiver will now independently scan the user defined frequency bands loOKing for the real over the air data transmitted by the cellular networks.

The LTE scan will be completed quickly due to the bandwidth of each LTE channel. The UMTS scan will usually take longer, and the GSM scan may take considerably longer due to the bandwidth of each GSM channel and the width of the spectrum allocated to the bands.

NOTE: In a densely populated GSM environment or in a border area where several countries GSM networks can be detected, the GSM network scan may take several minutes.



≡ Status

TCM
Serial Number: 1933/007

Temperature:	45°C
Boot Progress:	100%
Input Voltage:	14.0v
LAN IP Address:	172.16.136.21
LAN Subnet:	255.255.0.0
LAN Address Type:	DHCP
Wi-Fi IP Address:	192.168.1.254
Wi-Fi Subnet:	255.255.255.0
Wi-Fi Address Type:	FIXED

GPS Receiver
Serial Number: 1933/007

Latitude:	52°04'32"N
Longitude:	0°14'30"W
Altitude:	97m
Pos. Error:	3m
Heading:	-
Speed:	0m/s

Wi-Fi Transceiver
Serial Number: 1933/007

Mode:	Idle

Tactical-G
Serial Number: 1934/025

State:	Ready
Boot Progress:	100%
PIC IP Address:	172.16.136.15
PIC Subnet:	255.255.0.0
PIC Address Type:	DHCP
LAN IP Address:	172.16.136.33
LAN Subnet:	255.255.0.0
LAN Address Type:	DHCP

Transceiver
Serial Number: 1934/025

MNC:	-
RSSI:	-
EARFCN:	28
Tx Power:	-
Receiver:	Scanning
Transmitter:	Off
Mode:	LTE
MCC:	-
LAC:	-
Cell ID:	-
Band:	1 - 2100MHz

Power Amplifier
Serial Number: 1934/025

Main Temperature:	20°C
Tx Power:	Off
PA 1 Temp:	20°C
TRX Serial:	1934/025

Tactical-G
Serial Number: 1934/006

State:	Ready
Boot Progress:	100%
PIC IP Address:	172.16.136.18
PIC Subnet:	255.255.0.0
PIC Address Type:	DHCP
LAN IP Address:	172.16.136.24
LAN Subnet:	255.255.0.0
LAN Address Type:	DHCP

Transceiver
Serial Number: 1934/006

MNC:	-
RSSI:	-
ARFCN:	25
Tx Power:	-
Receiver:	Scanning
Transmitter:	Off
Mode:	GSM
MCC:	-
LAC:	-
Cell ID:	-
Band:	900MHz

Power Amplifier
Serial Number: 1934/006

Main Temperature:	34°C
Tx Power:	Off
PA 1 Temp:	34°C
TRX Serial:	1934/006

Tactical-G
Serial Number: 1934/021

State:	Ready
Boot Progress:	100%
PIC IP Address:	172.16.136.19
PIC Subnet:	255.255.0.0
PIC Address Type:	DHCP
LAN IP Address:	172.16.136.29
LAN Subnet:	255.255.0.0
LAN Address Type:	DHCP

Transceiver
Serial Number: 1934/021

MNC:	-
RSSI:	-92dBm
UARFCN:	1612
Tx Power:	-
Receiver:	Scanning
Transmitter:	Off
Mode:	UMTS
MCC:	-
LAC:	-
Cell ID:	-
Band:	4 - 1700MHz

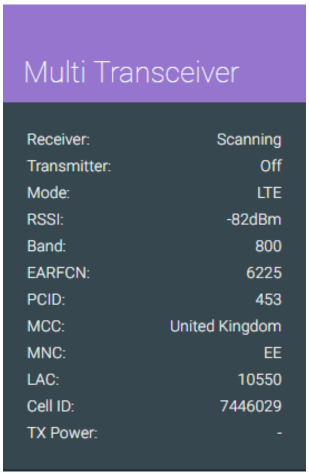
Power Amplifier
Serial Number: 1934/021

Main Temperature:	36°C
Tx Power:	Off
PA 1 Temp:	36°C
TRX Serial:	1934/021

Fig 84. 3 channel NESIE – transceivers scanning

12.2 NETWORK SCAN – SINGLE CHANNEL

If the NESIE system consists of 1 transceiver module, such as a Covert Ground system, the transceiver will be in Multi transceiver Mode as shown in Fig 85 below. The transceiver will automatically switch modes between LTE, UMTS and GSM. In the screen shot below, it can be seen that this transceiver is currently scanning on the LTE band and has decoded a channel and displaying the data from the network provider.



Multi Transceiver

Receiver:	Scanning
Transmitter:	Off
Mode:	LTE
RSSI:	-82dBm
Band:	800
EARFCN:	6225
PCID:	453
MCC:	United Kingdom
MNC:	EE
LAC:	10550
Cell ID:	7446029
TX Power:	-

Fig 85. Single channel NESIE – scanning

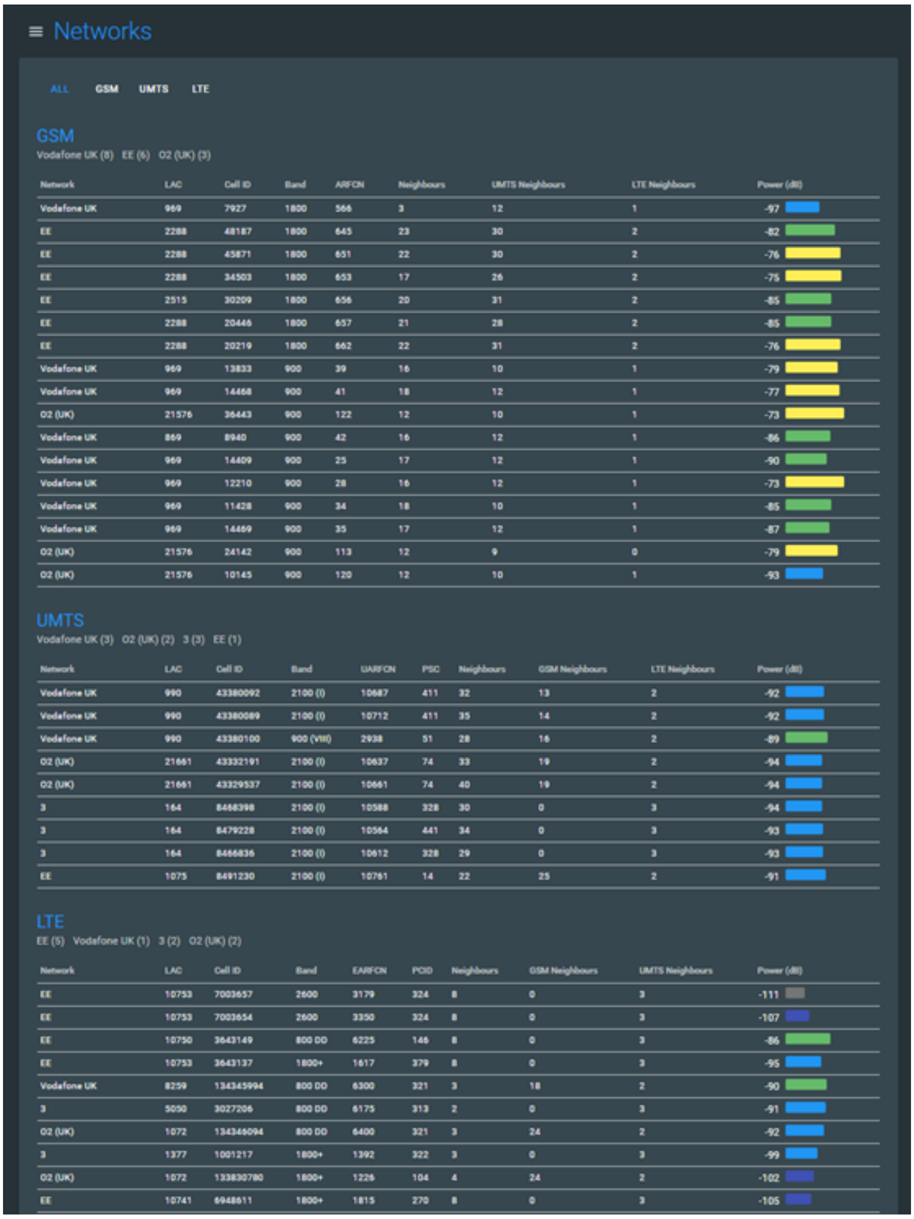
Initially, the NESIE will identify the wideband LTE signals (normally 10MHz or 20MHz but other LTE band sizes are used and can be detected by NESIE). NESIE will then identify the gaps in the cellular spectrum and identify any UMTS signals. Then the remaining spectrum is monitored for GSM signals.

Any cellular base station signals that are detected will be decoded and the serving cell along with neighbouring cell data is logged.

NESIE will spend the required time (depending on the number of bands selected to scan) covering the LTE, UMTS and GSM bands and will continually cycle through these technologies whenever it is not transmitting or has a previous network scan file loaded.

13. NETWORK SCAN – VIEW DATA

The network scan data is displayed on the NETWORKS page as shown in Fig 86 below.



≡ Networks

GSM

Vodafone UK (8) EE (6) O2 (UK) (3)

Network	LAC	Cell ID	Band	ARFCN	Neighbours	UMTS Neighbours	LTE Neighbours	Power (dB)
Vodafone UK	969	7927	1800	566	3	12	1	-97 🟦
EE	2288	48187	1800	645	23	30	2	-82 🟩
EE	2288	45871	1800	651	22	30	2	-76 🟨
EE	2288	34503	1800	653	17	26	2	-75 🟨
EE	2515	30209	1800	656	20	31	2	-85 🟩
EE	2288	20446	1800	657	21	28	2	-85 🟩
EE	2288	20219	1800	662	22	31	2	-76 🟨
Vodafone UK	969	13833	900	39	16	10	1	-79 🟨
Vodafone UK	969	14468	900	41	18	12	1	-77 🟨
O2 (UK)	21576	36443	900	122	12	10	1	-73 🟨
Vodafone UK	869	8940	900	42	16	12	1	-86 🟩
Vodafone UK	969	14409	900	25	17	12	1	-90 🟩
Vodafone UK	969	12210	900	28	16	12	1	-73 🟨
Vodafone UK	969	11428	900	34	18	10	1	-85 🟩
Vodafone UK	969	14469	900	35	17	12	1	-87 🟩
O2 (UK)	21576	24142	900	113	12	9	0	-79 🟨
O2 (UK)	21576	10145	900	120	12	10	1	-93 🟦

UMTS

Vodafone UK (3) O2 (UK) (2) 3 (3) EE (1)

Network	LAC	Cell ID	Band	UARFCN	PSC	Neighbours	GSM Neighbours	LTE Neighbours	Power (dB)
Vodafone UK	990	43380092	2100 (I)	10687	411	32	13	2	-92 🟦
Vodafone UK	990	43380089	2100 (I)	10712	411	35	14	2	-92 🟦
Vodafone UK	990	43380100	900 (VIII)	2938	51	28	16	2	-89 🟩
O2 (UK)	21661	43332191	2100 (I)	10637	74	33	19	2	-94 🟦
O2 (UK)	21661	43329537	2100 (I)	10661	74	40	19	2	-94 🟦
3	164	8468398	2100 (I)	10588	328	30	0	3	-94 🟦
3	164	8479228	2100 (I)	10564	441	34	0	3	-93 🟦
3	164	8466836	2100 (I)	10612	328	29	0	3	-93 🟦
EE	1075	8491230	2100 (I)	10761	14	22	25	2	-91 🟦

LTE

EE (5) Vodafone UK (1) 3 (2) O2 (UK) (2)

Network	LAC	Cell ID	Band	EARFCN	PCID	Neighbours	GSM Neighbours	UMTS Neighbours	Power (dB)
EE	10753	7003657	2600	3179	324	8	0	3	-111 ⬜
EE	10753	7003654	2600	3350	324	8	0	3	-107 🟪
EE	10750	3643149	800 DD	6225	146	8	0	3	-86 🟩
EE	10753	3643137	1800+	1617	379	8	0	3	-95 🟦
Vodafone UK	8259	134345994	800 DD	6300	321	3	18	2	-90 🟩
3	5050	3027206	800 DD	6175	313	2	0	3	-91 🟦
O2 (UK)	1072	134346094	800 DD	6400	321	3	24	2	-92 🟦
3	1377	1001217	1800+	1392	322	3	0	3	-99 🟦
O2 (UK)	1072	133830780	1800+	1226	104	4	24	2	-102 🟪
EE	10741	6948611	1800+	1815	270	8	0	3	-105 🟪

Fig 86. Network scan data

By default, all technologies are displayed on one page. If required, the operator can display each individual technology by using the navigation button at the top of the NETWORKS page as shown in Fig 87 below. The page selected by the operator is shown in blue text.

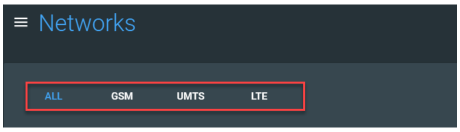
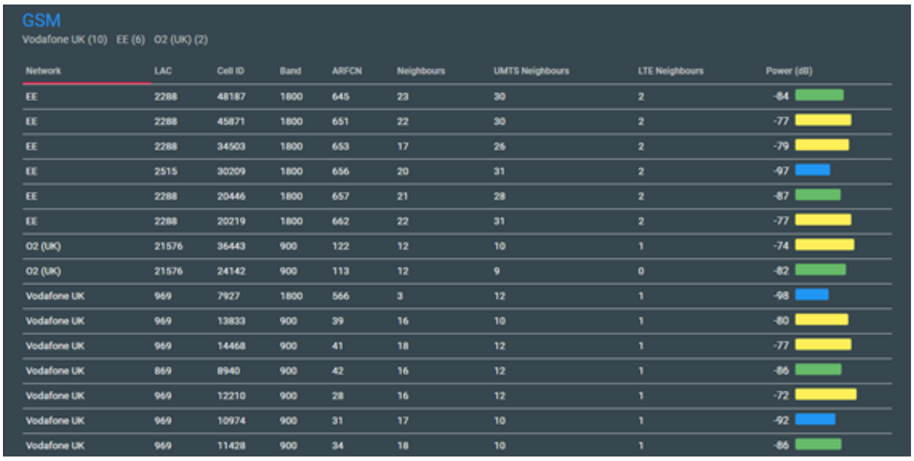


Fig 87. Network scan – tables

As the network scan progresses, the detected network data is displayed on the NETWORKS page. The earliest data is normally displayed at the top of the list. Therefore, the order of the list may seem random. However, if required the operator can order the list.

To order the list, the operator should click on one of the column headers. In the table shown below at Fig 88, the operator has ordered the data by clicking on the Network column header, this will now group the data by network operator. A red line under the Network header, indicates that the order has been changed.



GSM

Vodafone UK (10) EE (6) O2 (UK) (2)

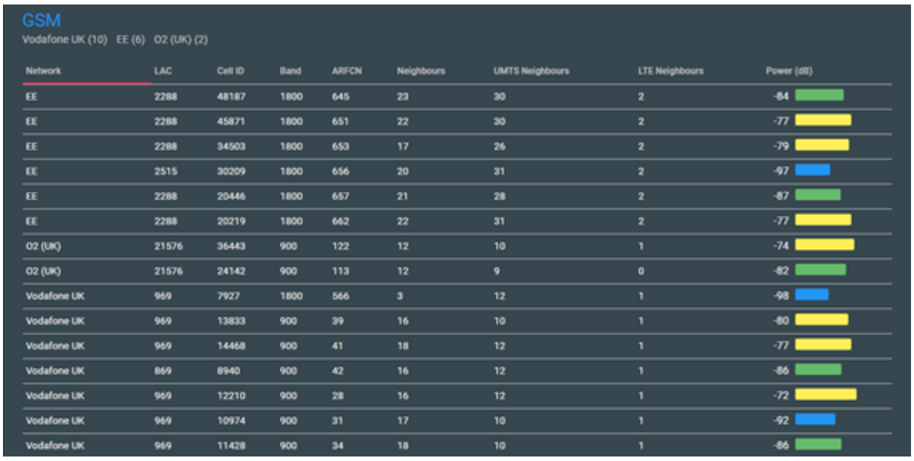
Network	LAC	Cell ID	Band	ARFCN	Neighbours	UMTS Neighbours	LTE Neighbours	Power (dB)
EE	2288	48187	1800	645	23	30	2	-84 🟩
EE	2288	45871	1800	651	22	30	2	-77 🟨
EE	2288	34503	1800	653	17	26	2	-79 🟨
EE	2515	30209	1800	656	20	31	2	-97 🟦
EE	2288	20446	1800	657	21	28	2	-87 🟩
EE	2288	20219	1800	662	22	31	2	-77 🟨
O2 (UK)	21576	36443	900	122	12	10	1	-74 🟨
O2 (UK)	21576	24142	900	113	12	9	0	-82 🟩
Vodafone UK	969	7927	1800	566	3	12	1	-98 🟦
Vodafone UK	969	13833	900	39	16	10	1	-80 🟨
Vodafone UK	969	14468	900	41	18	12	1	-77 🟨
Vodafone UK	869	8940	900	42	16	12	1	-86 🟩
Vodafone UK	969	12210	900	28	16	12	1	-72 🟨
Vodafone UK	969	10974	900	31	17	10	1	-92 🟦
Vodafone UK	969	11428	900	34	18	10	1	-86 🟩

Fig 88. Network data – ordered

If all technology tables are displayed on one screen, the operator must change the order of each list manually.

13.1 GSM SCAN DATA

The GSM scan data table is shown at Fig 89 below. This table displays the GSM channels currently detected by the NESIE system during the scan.



GSM

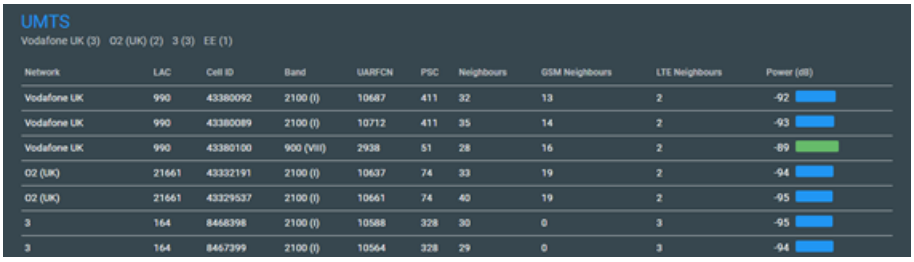
Vodafone UK (10) EE (6) O2 (UK) (2)

Network	LAC	Cell ID	Band	ARFCN	Neighbours	UMTS Neighbours	LTE Neighbours	Power (dB)
EE	2288	48187	1800	645	23	30	2	-84 🟩
EE	2288	45871	1800	651	22	30	2	-77 🟨
EE	2288	34503	1800	653	17	26	2	-79 🟨
EE	2515	30209	1800	656	20	31	2	-97 🟦
EE	2288	20446	1800	657	21	28	2	-87 🟩
EE	2288	20219	1800	662	22	31	2	-77 🟨
O2 (UK)	21576	36443	900	122	12	10	1	-74 🟨
O2 (UK)	21576	24142	900	113	12	9	0	-82 🟩
Vodafone UK	969	7927	1800	566	3	12	1	-98 🟦
Vodafone UK	969	13833	900	39	16	10	1	-80 🟨
Vodafone UK	969	14468	900	41	18	12	1	-77 🟨
Vodafone UK	869	8940	900	42	16	12	1	-86 🟩
Vodafone UK	969	12210	900	28	16	12	1	-72 🟨
Vodafone UK	969	10974	900	31	17	10	1	-92 🟦
Vodafone UK	969	11428	900	34	18	10	1	-86 🟩

Fig 89. GSM scan data

13.2 UMTS SCAN DATA

The UMTS scan data table is shown at Fig 90 below. This table displays the UMTS channels currently detected by the NESIE system during the scan.



UMTS

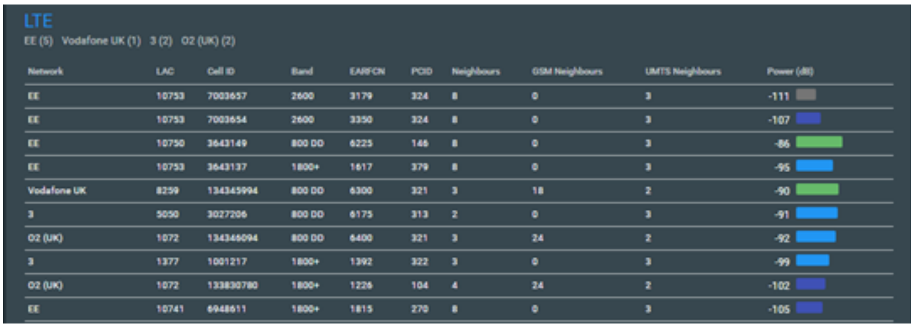
Vodafone UK (3)   O2 (UK) (2)   3 (3)   EE (1)

Network	LAC	Cell ID	Band	UARFCN	PSC	Neighbours	GSM Neighbours	LTE Neighbours	Power (dB)
Vodafone UK	990	43380092	2100 (I)	10687	411	32	13	2	-92 🟦
Vodafone UK	990	43380089	2100 (I)	10712	411	35	14	2	-93 🟦
Vodafone UK	990	43380100	900 (VIII)	2938	51	28	16	2	-89 🟩
O2 (UK)	21661	43332191	2100 (I)	10637	74	33	19	2	-94 🟦
O2 (UK)	21661	43329537	2100 (I)	10661	74	40	19	2	-95 🟦
3	164	8468398	2100 (I)	10588	328	30	0	3	-95 🟦
3	164	8467399	2100 (I)	10564	328	29	0	3	-94 🟦

Fig 90. UMTS scan data

13.3 LTE CHANNEL LIST

The LTE scan data table is shown at Fig 91 below. This table displays the LTE channels currently detected by the NESIE system during the scan.



LTE

EE (5)   Vodafone UK (1)   3 (2)   O2 (UK) (2)

Network	LAC	Cell ID	Band	EARFCN	PCID	Neighbours	GSM Neighbours	UMTS Neighbours	Power (dB)
EE	10753	7003657	2600	3179	324	8	0	3	-111 ⬜
EE	10753	7003654	2600	3350	324	8	0	3	-107 🟦
EE	10750	3643149	800 DD	6225	146	8	0	3	-86 🟩
EE	10753	3643137	1800+	1617	379	8	0	3	-95 🟦
Vodafone UK	8259	134345994	800 DD	6300	321	3	18	2	-90 🟩
3	5050	3027206	800 DD	6175	313	2	0	3	-91 🟦
O2 (UK)	1072	134346094	800 DD	6400	321	3	24	2	-92 🟦
3	1377	1001217	1800+	1392	322	3	0	3	-99 🟦
O2 (UK)	1072	133830780	1800+	1226	104	4	24	2	-102 🟦
EE	10741	6948611	1800+	1815	270	8	0	3	-105 🟦

Fig 91. LTE scan data

13.3.1 LTE FREQUENCY DIVISION DUPLEX (FDD)

FDD requires two separate wireless communications channels on separate frequencies, one for transmit and the other for received data.

LTE systems need two separate channels. A sufficient amount of guard band separates the two channels so the transmitter and receiver don’t interfere with one another.

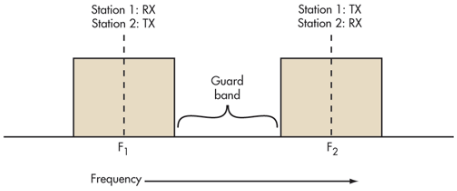


Fig 92. FDD

FDD requires two symmetrical segments of spectrum for the uplink and downlink channels.

FDD uses lots of frequency spectrum, though, generally at least twice the spectrum needed by TDD. In addition, there must be adequate spectrum separation between the transmit and receive channels. These so-called guard bands aren't useable, so they're wasteful. Given the scarcity and expense of spectrum, these are real disadvantages.

However, FDD is very widely used in cellular telephone systems, such as the widely used GSM system. In some systems the 25-MHz band from 869 to 894 MHz is used as the downlink (DL) spectrum from the cell site tower to the handset, and the 25-MHz band from 824 to 849 MHz is used as the uplink (UL) spectrum from the handset to cell site.

Another disadvantage with FDD is the difficulty of using special antenna techniques like multiple-input multiple-output (MIMO) and beamforming. These technologies are a core part of the new Long-Term Evolution (LTE) 4G cell phone strategies for increasing data rates. It is difficult to make antenna bandwidths broad enough to cover both sets of spectrum.

13.3.2 LTE TIME DIVISION DUPLEX (TDD) – SYNC PICTURES ADDED?

TDD uses a single frequency (Channel) for both transmit and receive. Then it shares that channel by assigning alternating time slots to transmit and receive operations. The information to be transmitted—whether it's voice, video, or data—is in serial binary format. Each time slot may be 1 byte long or could be a frame of multiple bytes.

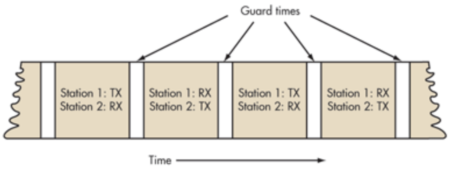


Fig 93. TDD

TDD alternates the transmission and reception of station data over time. Time slots may be variable in length. Because of the high-speed nature of the data, the communicating parties cannot tell that the transmissions are intermittent. The transmissions are concurrent rather than simultaneous.

In some TDD systems, the alternating time slots are of the same duration or have equal DL and UL times. However, the system doesn't have to be 50/50 symmetrical. The system can be asymmetrical as required. For instance, in Internet access, download times are usually much longer than upload times so more or fewer frame time slots are assigned as needed. Some TDD formats offer dynamic bandwidth allocation where time-slot numbers or durations are changed on the fly as required.

The real advantage of TDD is that it only needs a single channel of frequency spectrum. Furthermore, no spectrum-wasteful guard bands or channel separations are needed. The downside is that successful implementation of TDD needs a very precise timing and synchronization system at both the transmitter and receiver to make sure time slots don't overlap or otherwise interfere with one another.

Guard times are also needed between time slots to prevent overlap.

13.4 NETWORK SCAN – DETECTED DATA

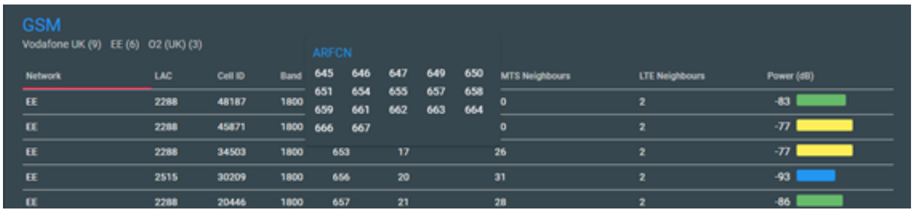
The data that is received, decoded and displayed on the NETWORKS page. It is shown in its native technology table (GSM, UMTS and LTE). The table headers and meaning are listed below.

Network:	Network operator/providers commercial name
LAC:	Location Area Code
Cell ID:	Unique network cell identifier
Band:	The frequency band of detected channel
ARFCN*:	GSM Absolute Reference Frequency Channel Number
UARFCN*:	UMTS ARFCN
EARFCH*:	LTE ARFCN
PSC*:	Primary Scrambling Code
PCID*:	Physical Cell ID
Neighbours:	Count of same tech neighbour cells
GSM Neighbours:	Count of alternative tech neighbours
UMTS Neighbours:	Count of alternative tech neighbours
LTE Neighbours:	Count of alternative tech neighbours
Power (dB):	Power received from cell site.

*** The relevant field will be displayed depending on which technology is being transmitted**

13.4.1 GSM NEIGHBOUR CELL DATA

By placing the cursor over any of the ‘Neighbour’ columns on the GSM table, additional data will be displayed showing the GSM neighbours for that serving cell, as per Fig 94. This additional data is the channel numbers used by any of the neighbouring cells.



GSM

Vodafone UK (9) EE (6) O2 (UK) (3)

Network	LAC	Cell ID	Band			MTS Neighbours	LTE Neighbours	Power (dB)
EE	2288	48187	1800			0	2	-83 🟩
EE	2288	45871	1800			0	2	-77 🟨
EE	2288	34503	1800	653	17	26	2	-77 🟨
EE	2515	30209	1800	656	20	31	2	-93 🟦
EE	2288	20446	1800	657	21	28	2	-86 🟩

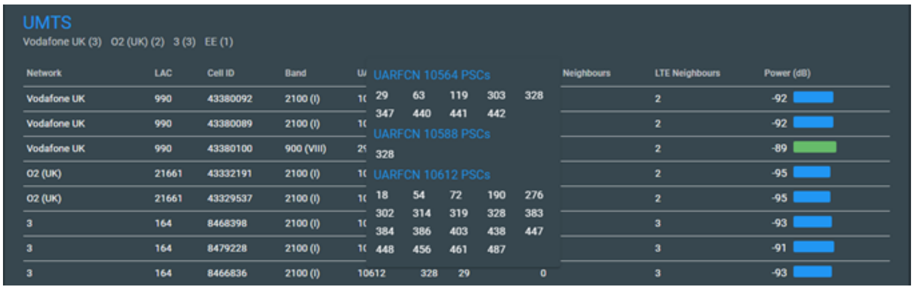
ARFCN

645	646	647	649	650
651	654	655	657	658
659	661	662	663	664
666	667			

Fig 94. GSM neighbour list

13.4.2 UMTS NEIGHBOUR CELL DATA

By placing the cursor over any of the ‘Neighbour’ columns on the UMTS table, additional data will be displayed showing the UMTS neighbours for that serving cell, as per Fig 95. UMTS neighbour list Fig 95 below. This additional data is the Primary Scrambling Codes (PSC) for each of the channels detected.



UMTS

Vodafone UK (3)   O2 (UK) (2)   3 (3)   EE (1)

Network	LAC	Cell ID	Band	U				Neighbours	LTE Neighbours	Power (dB)
Vodafone UK	990	43380092	2100 (I)	10					2	-92 🟦
Vodafone UK	990	43380089	2100 (I)	10					2	-92 🟦
Vodafone UK	990	43380100	900 (VIII)	29					2	-89 🟩
O2 (UK)	21661	43332191	2100 (I)	10					2	-95 🟦
O2 (UK)	21661	43329537	2100 (I)	10					2	-95 🟦
3	164	8468398	2100 (I)	10					3	-93 🟦
3	164	8479228	2100 (I)	10					3	-91 🟦
3	164	8466836	2100 (I)	10612	328	29	0		3	-93 🟦

UARFCN 10564 PSCs

29	63	119	303	328
347	440	441	442	

UARFCN 10588 PSCs

328

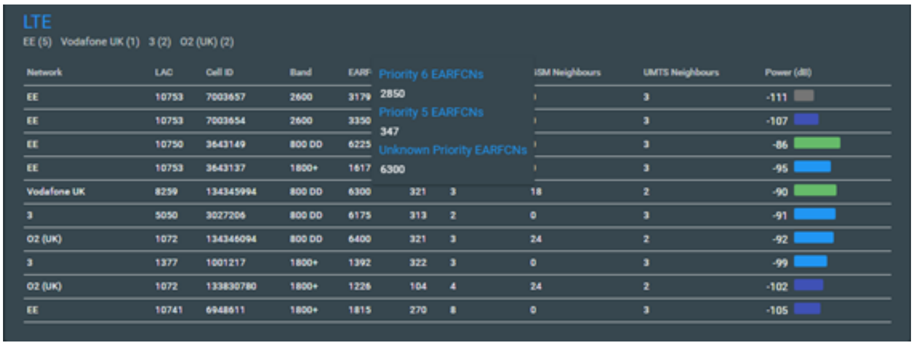
UARFCN 10612 PSCs

18	54	72	190	276
302	314	319	328	383
384	386	403	438	447
448	456	461	487	

Fig 95. UMTS neighbour list

13.4.3 LTE NEIGHBOUR CELL DATA

By placing the cursor over any of the ‘Neighbour’ columns on the LTE table, additional data will be displayed showing the LTE neighbours for that serving cell, as per Fig 96 below. This additional data is the priority allocated to each of the channels.



LTE

EE (5)   Vodafone UK (1)   3 (2)   O2 (UK) (2)

Network	LAC	Cell ID	Band	EARF			ISM Neighbours	UMTS Neighbours	Power (dB)
EE	10753	7003657	2600	3179				3	-111 ⬜
EE	10753	7003654	2600	3350				3	-107 🟦
EE	10750	3643149	800 DD	6225				3	-86 🟩
EE	10753	3643137	1800+	1617				3	-95 🟦
Vodafone UK	8259	134345994	800 DD	6300	321	3	18	2	-90 🟩
3	5050	3027206	800 DD	6175	313	2	0	3	-91 🟦
O2 (UK)	1072	134346094	800 DD	6400	321	3	24	2	-92 🟦
3	1377	1001217	1800+	1392	322	3	0	3	-99 🟦
O2 (UK)	1072	133830780	1800+	1226	104	4	24	2	-102 🟦
EE	10741	6948611	1800+	1815	270	8	0	3	-105 🟦

Priority 6 EARFCNs

2850

Priority 5 EARFCNs

347

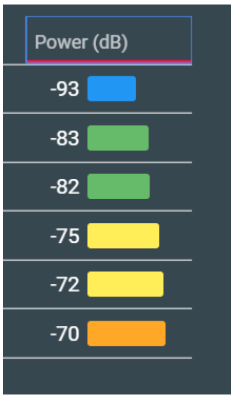
Unknown Priority EARFCNs

6300

Fig 96. LTE neighbour list

13.4.4 RECEIVED POWER

The received power (signal strength) of the individual cell, is displayed on the right of the network scan tables. The signal strength is expressed as a decibel figure e.g. -78dB, where the more negative the figure, the lower the power (e.g. -100dB is less power than -50dB) and a coloured bar as shown below in Fig 97 below.



Power (dB)
-93 🟦
-83 🟩
-82 🟩
-75 🟨
-72 🟨
-70 🟧

Fig 97. Power display

The colour and size of the bar represents the relative signal strength and can be used as an indication of the likely effect of the NESIE system against that cell / network.

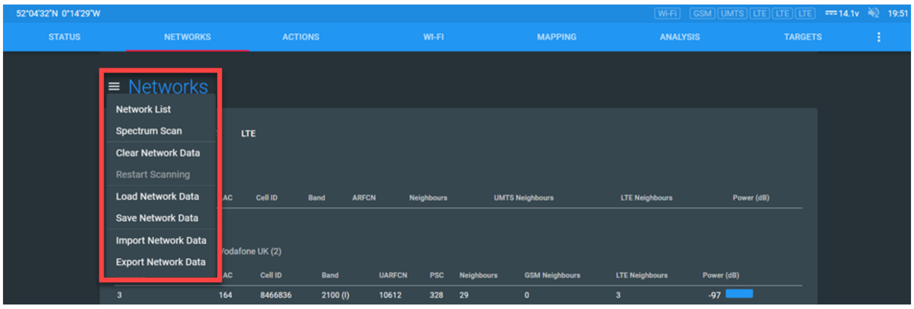
The colour of the power icon and its relative size denotes the power range that the signal was detected at. Each of the allocated colours is used to indicate a power band of 10dB. The power bands and colours are shown below:

🟥	-60dB and above
🟧	Between -60dB and -70dB
🟨	Between -70dB and -80dB
🟩	Between -80dB and -90dB
🟦	Between -90dB and -100dB
🟦	Between -100dB and -110dB
⬜	Between -110dB and -120dB

14. NETWORKS SCAN – SUB MENU

The additional menu icon within the NETWORKS page is shown below at Fig 98. When clicked, an additional dialogue box appears showing the following options:

- **Network List**
- **Spectrum Scan**
- **Clear Network Data**
- **Restart Scanning**
- **Load Network Data**
- **Save Network Data**
- **Import Network Data**
- **Export Network Data**



LTE

AC	Cell ID	Band	ARFCN	Neighbours	UMTS Neighbours	LTE Neighbours	Power (dB)

odafone UK (2)

	AC	Cell ID	Band	UARFCN	PSC	Neighbours	GSM Neighbours	LTE Neighbours	Power (dB)
3	164	8466836	2100 (I)	10612	328	29	0	3	-97

Fig 98. Network – sub menu

14.1 NETWORK LIST

Clicking the Network List button will return the user to the list of network data, as described at section 13.

14.2 SPECTRUM SCAN

The Spectrum Scan button will display a snapshot of the cellular spectrum on any bands that are set by the operator for the LTE scan.

If required, the operator may decide to add additional LTE bands to observe additional (non LTE) bands.

NOTE: If additional (non LTE) bands are added to the LTE, scan this will add additional time to the overall scan time.

Each of the individual LTE bands is scanned and a display of the spectrum is shown on the Spectrum Scan page as shown in Fig 99 below.

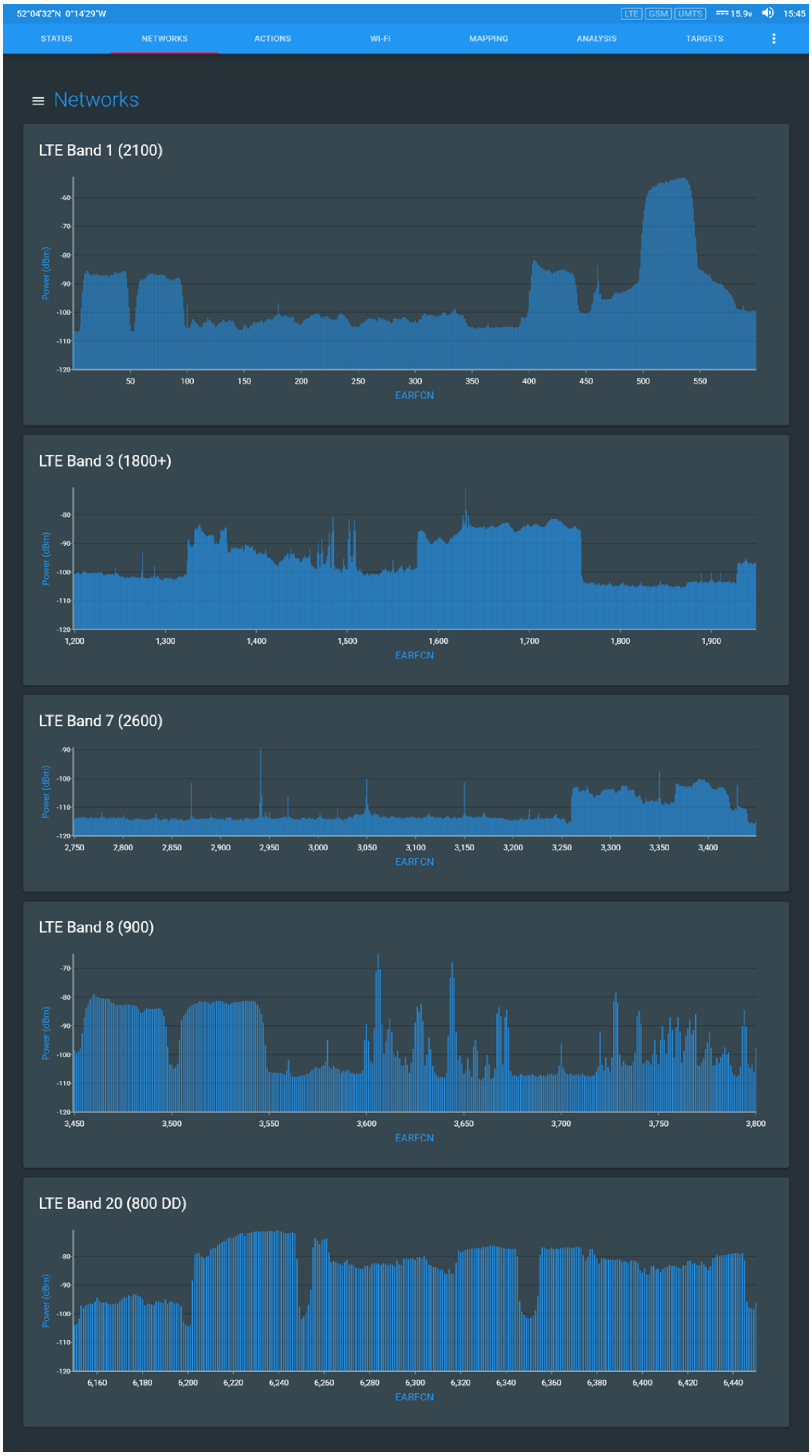


Fig 99. Spectrum scan

14.2.1 SPECTRUM SCAN – DETAILS

A. The band which has been scanned e.g.- LTE Band 3 (1800+) MHz
B. Downlink Signal Strength in Decibel
C. LTE ARFCN for the displayed band e.g. 1200–1950

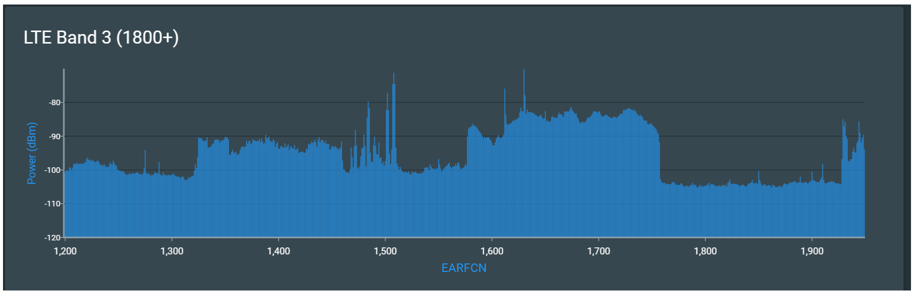


Fig 100. Spectrum scan - labels

14.2.2 SPECTRUM SCAN – VIEW OF CELLULAR SIGNALS.

As shown in Fig 101 and Fig 102 below, you can view the cellular network signals that have been detected by the NESIE system. The signals in the diagram may differ to the signals detected in another country / area.

> **NOTE: The operator must take care to read the scale at the bottom of the individual spectrum display as the scale will automatically adjust according to the band scanned.**

A. Red Box	2 x 5MHz wide UMTS signal
B. Amber Box	Multiple 200KHz wide GSM signals
C. White Box	2 x 5MHz wide UMTS signal
D. Green Box	10 MHz LTE signal

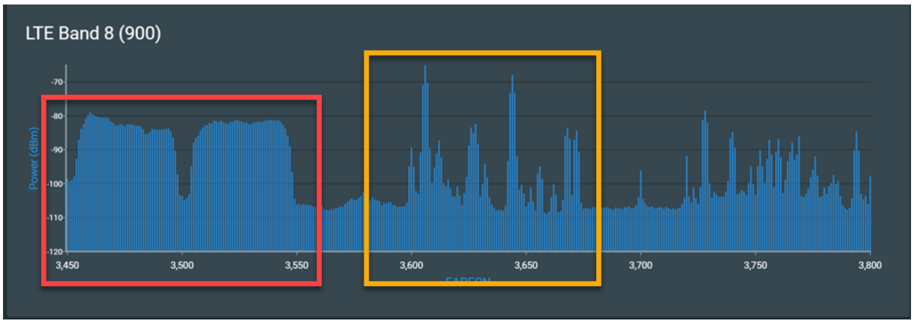


Fig 101. Spectrum scan – UMTS & GSM data

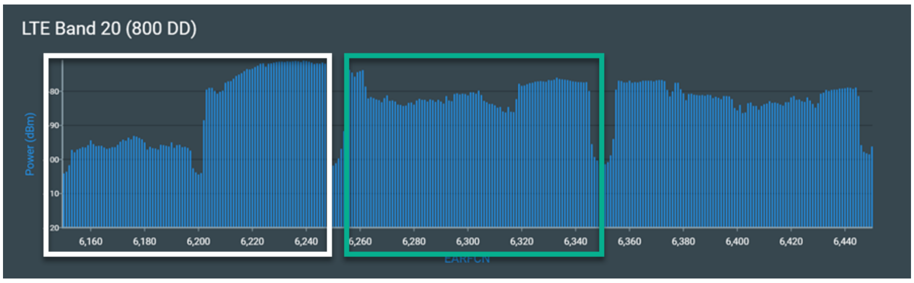


Fig 102. Spectrum scan – UMTS & LTE data

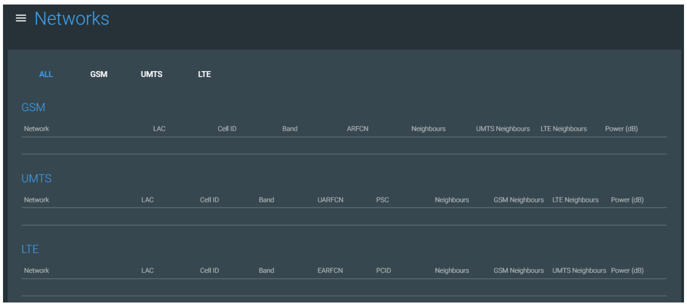
14.3 SAVE, LOAD AND CLEAR NETWORK DATA

It may become apparent that a user does not have enough time to let NESIE complete a full network scan of the cellular bands before starting an operation. This may because the user cannot loiter at a location too long without drawing attention to themselves or the Target may only be present for a very short time.

With some knowledge of the Target and his likely movements, the user may wish to conduct a network scan prior to the operation. This could be conducted one hour or even one week before the Target presents themselves at the location. This scan data can then be saved and re loaded when required. The operator has the option to Clear, Save and Load Network Data, as shown in Fig 98 above.

14.3.1 CLEAR NETWORK DATA

If required, the operator can choose to Clear (delete) the previously collected or loaded network scan data. To clear the data, the operator should use click Clear Network Data as shown in Fig 98 above. The data will be deleted, the tables will go blank as shown Fig 103 below and the NESIE system will automatically restart the network scan and repopulate the tables.



GSM

Network	LAC	Cell ID	Band	ARFCN	Neighbours	UMTS Neighbours	LTE Neighbours	Power (dB)

UMTS

Network	LAC	Cell ID	Band	UARFCN	PSC	Neighbours	GSM Neighbours	LTE Neighbours	Power (dB)

LTE

Network	LAC	Cell ID	Band	EARFCN	PCID	Neighbours	GSM Neighbours	UMTS Neighbours	Power (dB)

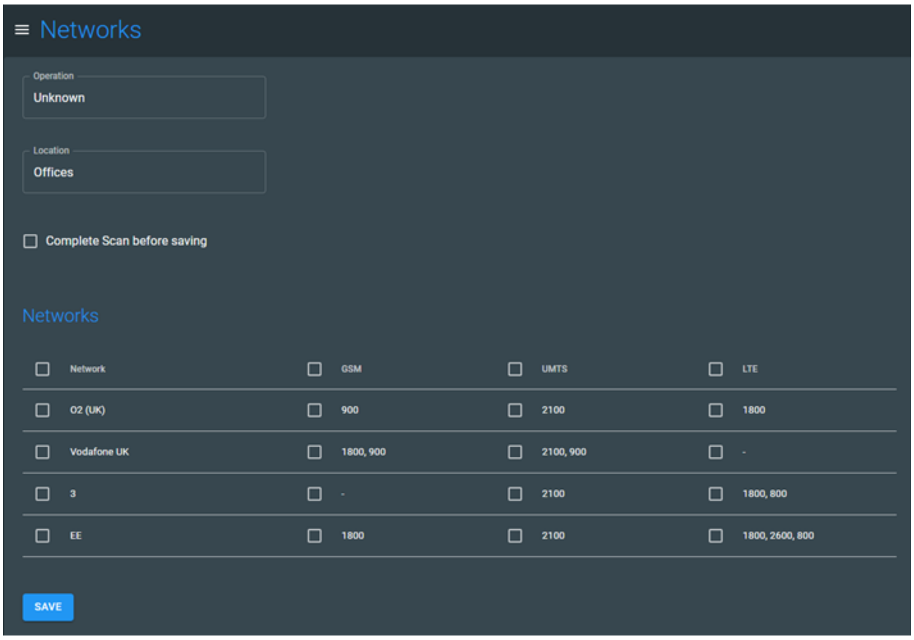
Fig 103. Clear network data

14.3.2 SAVE NETWORK DATA

To store (save) a set of network scan data, the user must can click Store Network Data as show at Fig 98 above.

The operator will be presented with the page shown at Fig 104 below. After choosing Store Network Data, the operator will be prompted to enter an Operation name and Location, then select the networks and technologies that he wishes to store for later use.   There is also the optional tick box ‘Complete Scan Before Saving’. This forces NESIE to scan all the selected bands before saving the data.

When the required settings are chosen the operator must press the SAVE button.



Operation: Unknown

Location: Offices

□ Complete Scan before saving

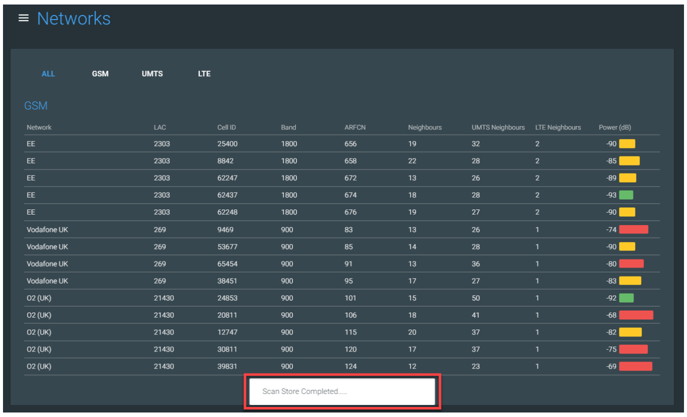
Networks

□ Network	□ GSM	□ UMTS	□ LTE
□ O2 (UK)	□ 900	□ 2100	□ 1800
□ Vodafone UK	□ 1800, 900	□ 2100, 900	□ -
□ 3	□ -	□ 2100	□ 1800, 800
□ EE	□ 1800	□ 2100	□ 1800, 2600, 800

Fig 104. Save network data

NESIE will now use the available transceivers to scan the cellular networks again. If the NESIE system has a GPS fix and has recently conducted a scan, the network scan will be performed relatively quickly. If there is no GPS fix available, the NESIE may not know its current location and conduct a full network scan across all bands and technologies. This network scan could take several minutes depending on the number of available receivers, bands and technologies.

A pop-up box will be displayed showing Scan Store Completed when the network scan process has been completed and saved to the database, as shown in Fig 105 below.



GSM

Network	LAC	Cell ID	Band	ARFCN	Neighbours	UMTS Neighbours	LTE Neighbours	Power (dB)
EE	2303	25400	1800	656	19	32	2	-90 🟨
EE	2303	8842	1800	658	22	28	2	-85 🟨
EE	2303	62247	1800	672	13	26	2	-89 🟨
EE	2303	62437	1800	674	18	28	2	-93 🟩
EE	2303	62248	1800	676	19	27	2	-90 🟨
Vodafone UK	269	9469	900	83	13	26	1	-74 🟥
Vodafone UK	269	53677	900	85	14	28	1	-90 🟨
Vodafone UK	269	65454	900	91	13	36	1	-80 🟥
Vodafone UK	269	38451	900	95	17	27	1	-83 🟨
O2 (UK)	21430	24853	900	101	15	50	1	-92 🟩
O2 (UK)	21430	20811	900	106	18	41	1	-68 🟥
O2 (UK)	21430	12747	900	115	20	37	1	-82 🟨
O2 (UK)	21430	30811	900	120	17	37	1	-75 🟥
O2 (UK)	21430	39831	900	124	12	23	1	-69 🟥

Scan Store Completed.....

Fig 105. Scan save warning

CAUTION: IF THE NESIE OPERATOR ATTEMPTS TO STORE THE SCAN DATA DURING AN OPERATION (GRAB, HUNT, HOLD ETC) THE OPERATION WILL BE STOPPED SO THE NESIE CAN USE THE RECEIVER.

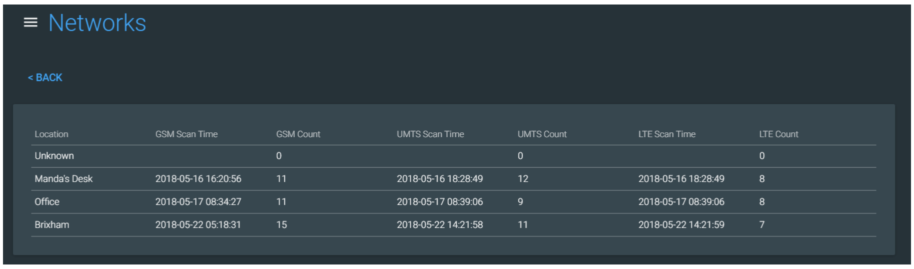
NOTE: It should also be noted that whenever an Action (Grab, Hunt, Hold, Deny, etc) is carried out, NESIE will automatically store the current network scan data to the database. This data will be filed using the current Operation and Location as entered by the operator and the GPS fix as detected by the NESIE system.

These files can also be viewed and loaded as per the section below.

14.3.3 LOAD SCAN DATA

To load a previous set of stored network scan data, the operator must press the Load Scan Data button. The operator will now be presented with a page displaying a list of previously stored data.

The operator can choose the scan data by placing the cursor over the desired row and clicking, as shown in Fig 106 below.



Location	GSM Scan Time	GSM Count	UMTS Scan Time	UMTS Count	LTE Scan Time	LTE Count
Unknown		0		0		0
Manda's Desk	2018-05-16 16:20:56	11	2018-05-16 18:28:49	12	2018-05-16 18:28:49	8
Office	2018-05-17 08:34:27	11	2018-05-17 08:39:06	9	2018-05-17 08:39:06	8
Brixham	2018-05-22 05:18:31	15	2018-05-22 14:21:58	11	2018-05-22 14:21:59	7

Fig 106. Load scan data

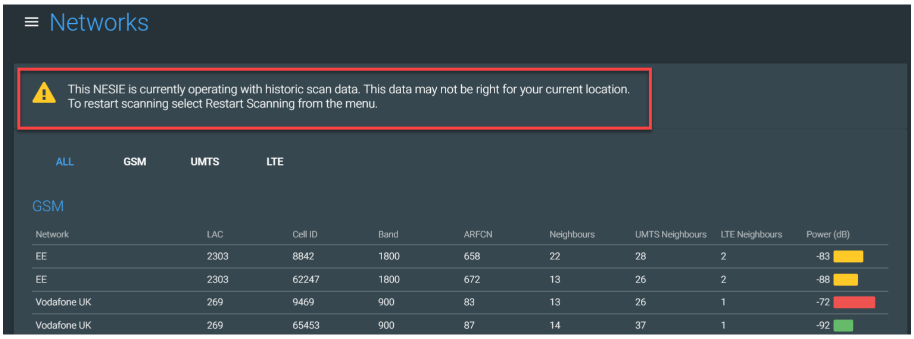
The data displayed in the saved network data table is:

Location: The location as entered by the operator
GSM Scan Time: The time logged when the GSM scan was saved
GSM Count: The number of GSM channels detected / logged
UMTS Scan Time: The time logged when the UMTS scan data was saved
UMTS Count: The number of UMTS channels detected / logged
LTE Scan Time: The time logged when the LTE scan data was saved
LTE Count: The number of LTE channels detected / logged

If required, the table can be reordered by clicking any of the table headers.

CAUTION: WHEN A SET OF STORED NETWORK SCAN DATA IS LOADED, THE TRANSCEIVER WILL STOP THE AUTOMATIC SCANNING / UPDATING OF THE NETWORK DATA.

A DIALOGUE BOX WILL BE DISPLAYED WARNING THE OPERATOR THAT IF THE USUAL NETWORK SCAN IS REQUIRED IT MUST BE MANUALLY RESTARTED AS SHOWN IN FIG 107. A WARNING SYMBOL WILL ALSO BE DISPLAYED ON THE HEADER BAR OF THE UI AS SHOWN BELOW.



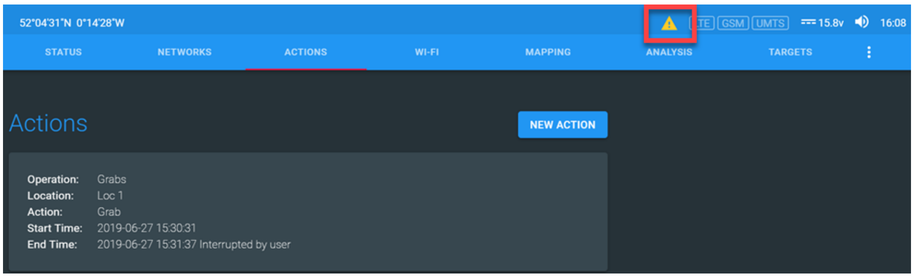
Networks

⚠ This NESIE is currently operating with historic scan data. This data may not be right for your current location. To restart scanning select Restart Scanning from the menu.

GSM

Network	LAC	Cell ID	Band	ARFCN	Neighbours	UMTS Neighbours	LTE Neighbours	Power (dB)
EE	2303	8842	1800	658	22	28	2	-83
EE	2303	62247	1800	672	13	26	2	-88
Vodafone UK	269	9469	900	83	13	26	1	-72
Vodafone UK	269	65453	900	87	14	37	1	-92

Fig 107. Restart scanning - warning dialogue box



Actions

Operation: Grabs
Location: Loc 1
Action: Grab
Start Time: 2019-06-27 15:30:31
End Time: 2019-06-27 15:31:37 Interrupted by user

Fig 108. Loaded scan – warning in header bar

Whenever a set of stored network scan data is loaded into the NESIE system, the receivers will be turned off and the system will no longer scan the cellular bands for the network data. The operator must manually restart the scanning process if required.

Under normal circumstances, the Restart Scanning button is greyed out. However, whenever the system has been forced to stop scanning the button will become active.

The Networks sub menu will now change to allow the operator to Restart Scanning, as shown at Fig 109 below.

14.3.4 RESTART SCANNING

To restart the scanning of the cellular bands to gather the network data, the operator should open the Networks sub menu as per Fig 109 below and click Restart Scanning. The transceivers will start scanning for the network data and will overwrite the data that was previously loaded.

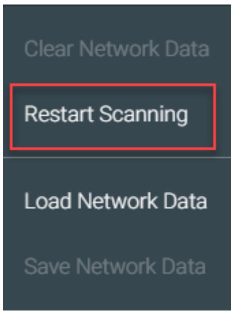


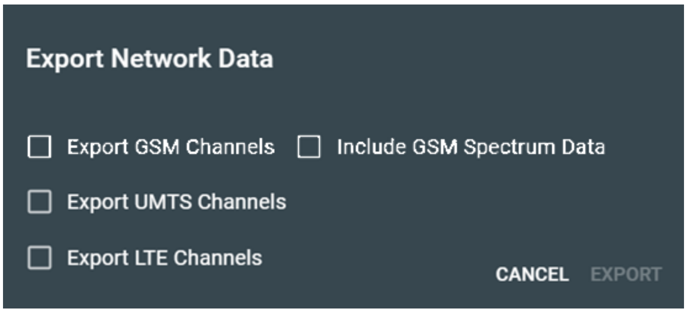
Fig 109. Restart Scanning

14.3.5 IMPORT / EXPORT NETWORK DATA

If required, the operator can export the saved network scan data off one NESIE unit and import it on to another unit.

To export the network scan data the operator will click the Export Network Data button, a pop-up box as shown below at Fig 110 will appear.

The operator must now tick the desired boxes and press the EXPORT button.



Export Network Data

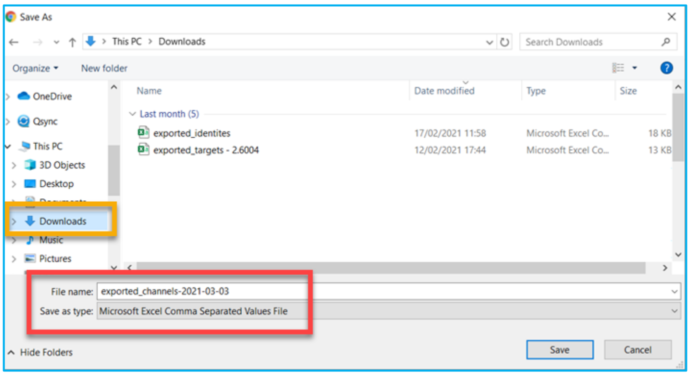
□ Export GSM Channels □ Include GSM Spectrum Data

□ Export UMTS Channels

□ Export LTE Channels

Fig 110. Export Network Data

The exported network data will be saved in the downloads folder of the attached laptop. The file will be given a default file name of ‘exported channels-(date)’. The file is saved as a .CSV file, as shown below at Fig 111.



Name	Date modified	Type	Size
Last month (5)			
exported_identites	17/02/2021 11:58	Microsoft Excel Co...	18 KB
exported_targets - 2.6004	12/02/2021 17:44	Microsoft Excel Co...	13 KB

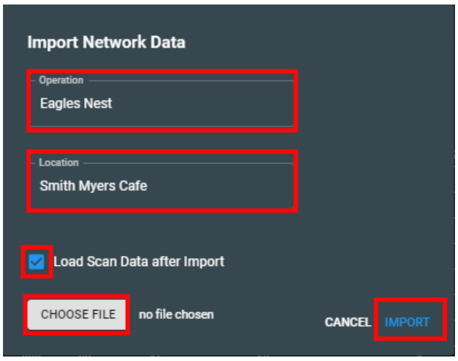
File name: exported_channels-2021-03-03

Save as type: Microsoft Excel Comma Separated Values File

Fig 111. Exported network data – Save As

To import a previously exported network data file, the operator should click the Import Network Data button from the NETWORKS page drop down menu as displayed below at Fig 112.

Enter the Operation and Location that is associated with the imported file, on this occasion they are Operation Eagles Nest and location Smith Myers Cafe.
If the file is to be loaded and used as the current network scan, tick the Load Scan Data after Import box. Click the CHOOSE FILE button and this will open a Windows dialogue box, navigate to the location of your previously saved network data files and select the appropriate file. Finally, press the IMPORT button. This process can be cancelled by clicking the CANCEL button at any stage.



Import Network Data

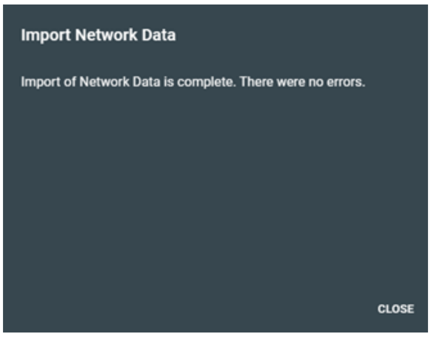
Operation: Eagles Nest

Location: Smith Myers Cafe

☑ Load Scan Data after Import

Fig 112. Import Network Data drop down

When the scan data has been imported, a pop-up window will be displayed.
If there are any errors, they will be reported accordingly as displayed below in Fig 113.



Import Network Data

Import of Network Data is complete. There were no errors.

Fig 113. Import Network Data - error

15. TIME TAKEN FOR THE NETWORK SCAN

The NESIE transceivers automatically start / restart the scan whenever they are not in transmit mode.

The time taken for the scan is predicated by the number of bands the user has configured NESIE to monitor and the number of active base station channels that are received and require decoding. The denser the cellular environment, the longer the scan could take.

NESIE must scan each user defined cellular band, stepping though the band, tuning to any possible cellular signals, decoding the data and store it before stepping onto the next possible channel.

> **NOTE: If the operator initiates a Grab or any other operation and NESIE has not had enough time to gather enough network data, NESIE will pause the start of the operation until it has enough data. If this happens, the operator has the option to use Fast Start on the ACTIONS page.**

15.1 SINGLE CHANNEL SYSTEM

If the NESIE system consists of only one transceiver, the software will automatically configure itself as a Multi transceiver and will scan the cellular bands in turn.

Normally the NESIE system will start up in LTE mode, conduct the network scan on the pre-selected bands then change to UMTS then GSM.

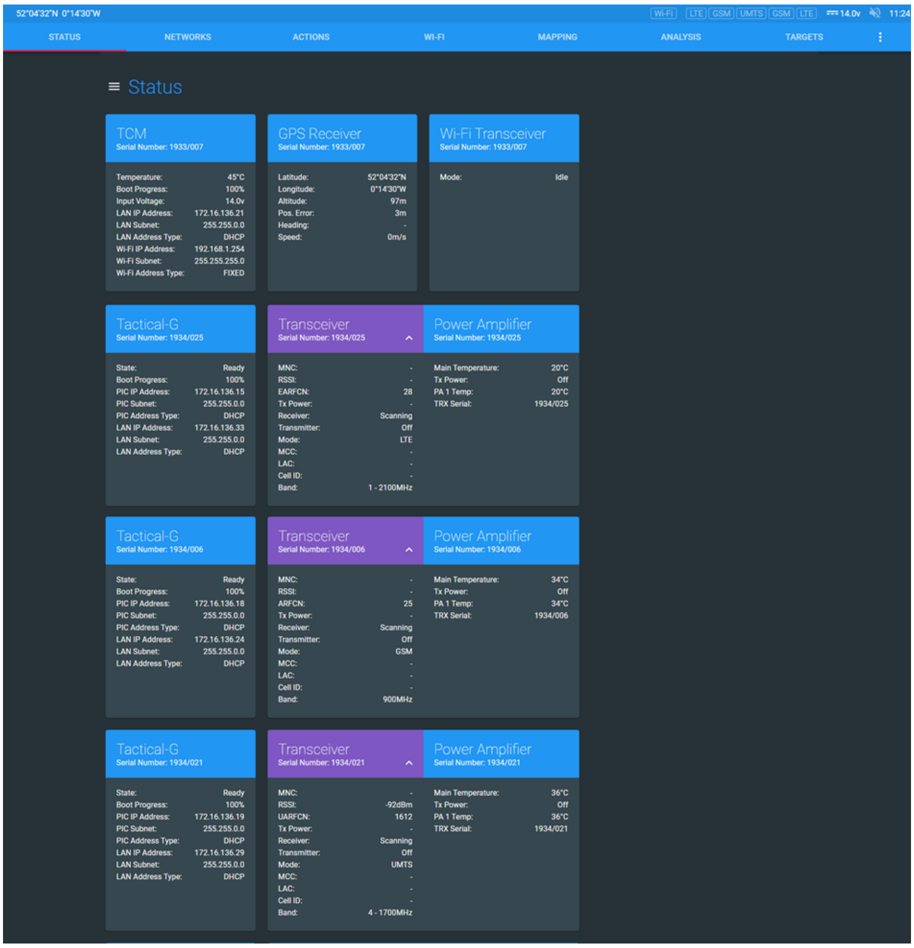
These mode changes can be monitored in the UI either in the header bar or on the STATUS page.

15.2 MULTI-CHANNEL SYSTEM

If the NESIE system consists of multiple transceivers (eg: a stack of 3), the software will automatically detect the transceivers and allocate 1 transceiver to LTE, one to UMTS and 1 to GSM. These 3 transceivers then continually monitor the user defined cellular bands for the network data.

15.3 NETWORK SCAN – RESOURCE COLOURS

Whenever NESIE is idle, the system will be conducting a network scan. The UI will display blue in the header bar, but the transceivers will be purple on the STATUS page as shown below in Fig 114 below.



Status

TCM
Serial Number: 1933/007

Temperature: 45°C
Boot Progress: 100%
Input Voltage: 14.0v
LAN IP Address: 172.16.136.21
LAN Subnet: 255.255.0.0
LAN Address Type: DHCP
Wi-Fi IP Address: 192.168.1.254
Wi-Fi Subnet: 255.255.255.0
Wi-Fi Address Type: FIXED

GPS Receiver
Serial Number: 1933/007

Latitude: 52°04'32"N
Longitude: 0°14'30"W
Altitude: 97m
Pos. Error: 3m
Heading: -
Speed: 0m/s

Wi-Fi Transceiver
Serial Number: 1933/007

Mode: Idle

Tactical-G
Serial Number: 1934/025

State: Ready
Boot Progress: 100%
PIC IP Address: 172.16.136.15
PIC Subnet: 255.255.0.0
PIC Address Type: DHCP
LAN IP Address: 172.16.136.33
LAN Subnet: 255.255.0.0
LAN Address Type: DHCP

Transceiver
Serial Number: 1934/025

MNC: -
RSSI: -
EARFCN: 28
Tx Power: -
Receiver: Scanning
Transmitter: Off
Mode: LTE
MCC: -
LAC: -
Cell ID: -
Band: 1 - 2100MHz

Power Amplifier
Serial Number: 1934/025

Main Temperature: 20°C
Tx Power: Off
PA 1 Temp: 20°C
TRX Serial: 1934/025

Tactical-G
Serial Number: 1934/006

State: Ready
Boot Progress: 100%
PIC IP Address: 172.16.136.18
PIC Subnet: 255.255.0.0
PIC Address Type: DHCP
LAN IP Address: 172.16.136.24
LAN Subnet: 255.255.0.0
LAN Address Type: DHCP

Transceiver
Serial Number: 1934/006

MNC: -
RSSI: -
ARFCN: 25
Tx Power: -
Receiver: Scanning
Transmitter: Off
Mode: GSM
MCC: -
LAC: -
Cell ID: -
Band: 900MHz

Power Amplifier
Serial Number: 1934/006

Main Temperature: 34°C
Tx Power: Off
PA 1 Temp: 34°C
TRX Serial: 1934/006

Tactical-G
Serial Number: 1934/021

State: Ready
Boot Progress: 100%
PIC IP Address: 172.16.136.19
PIC Subnet: 255.255.0.0
PIC Address Type: DHCP
LAN IP Address: 172.16.136.29
LAN Subnet: 255.255.0.0
LAN Address Type: DHCP

Transceiver
Serial Number: 1934/021

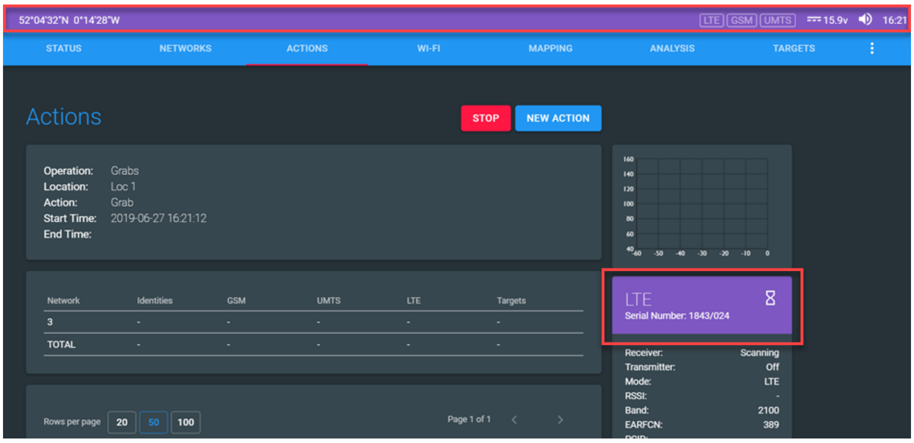
MNC: -
RSSI: -92dBm
UARFCN: 1612
Tx Power: -
Receiver: Scanning
Transmitter: Off
Mode: UMTS
MCC: -
LAC: -
Cell ID: -
Band: 4 - 1700MHz

Power Amplifier
Serial Number: 1934/021

Main Temperature: 36°C
Tx Power: Off
PA 1 Temp: 36°C
TRX Serial: 1934/021

Fig 114. Idle – network scan

If the operator attempts to start a Grab or any other action before NESIE has detected and decoded enough network data, the UI will display a purple header bar as shown below in Fig 115. This purple bar indicated that NESIE is still conducting a network scan or is re-checking the data and has paused the transmission until it has detected enough network data.



Actions

Operation: Grabs
Location: Loc 1
Action: Grab
Start Time: 2019-06-27 16:21:12
End Time:

Network	Identities	GSM	UMTS	LTE	Targets
3	-	-	-	-	-
TOTAL	-	-	-	-	-

Rows per page 20 50 100 Page 1 of 1

LTE
Serial Number: 1843/024

Receiver: Scanning
Transmitter: Off
Mode: LTE
RSSI: -
Band: 2100
EARFCN: 389

Fig 115. Rescan – purple

If NESIE is re-checking the stored data, the bar will only be purple for several seconds. However, if NESIE has not had long enough to detect & decode sufficient data, the bar may remain purple for several minutes.

If required, the operator has the option to force the NESIE to initiate a Fast Start.

This forces the NESIE to stop the automatic network scan, use the data it has already collected, even if it is not complete, and start transmitting. Details on the Fast Start function are at Section 17.6.

NOTE: Allowing more time for network scan - NESIE will start an operation (if commanded to) with the lowest amount of data it needs. If the system is scanning for longer it will continue to collect additional network data. The longer NESIE can scan, the better the networks scan data will be. This will increase the likelihood of a successful operation.

15.4 MINIMUM SCAN DATA REQUIRED

NESIE needs to do a network scan of all the bands that have been defined by the user. This scan is designed to collect enough data to allow NESIE to transmit a fake base station that can attract as many mobile devices as possible.

The primary data that is required is the serving cell and neighbour list from at least 2 cells in each network. This list is logged and NESIE then calculates the best ‘neighbour’ channel to transmit on.

There is no predefined minimum network scan time. However, if the system has only 1 receiver it will take longer to scan the network than if the system was made up of 3 transceivers.

Note: It is anticipated that a 3 channel NESIE system should need less than 3 mins to conduct a network scan.

It may take longer to conduct a comprehensive network scan if using a single channel NESIE system.

15.5 ADDITIONAL NETWORK SCAN TIME

If NESIE is given longer in network scanning mode, it will continue to scan the network environment. This will allow more data to be collected and possibly additional cells / channels and neighbour lists detected. This may allow NESIE to refine its settings to increase its detect capability.

16. AUTOMATICALLY RE-SCAN OR CHECK

Prior to transmitting, NESIE will always check that it has sufficient network data, and that the data is still correct, to configure itself to the optimum settings.

16.1 AUTOMATIC RE CHECK

After pressing the START button, NESIE will conduct a re check of the previous network scan data. The header bar will turn purple for several seconds as NESIE checks the data and then turn green when it starts transmitting. The automatic re check usually only takes several seconds.

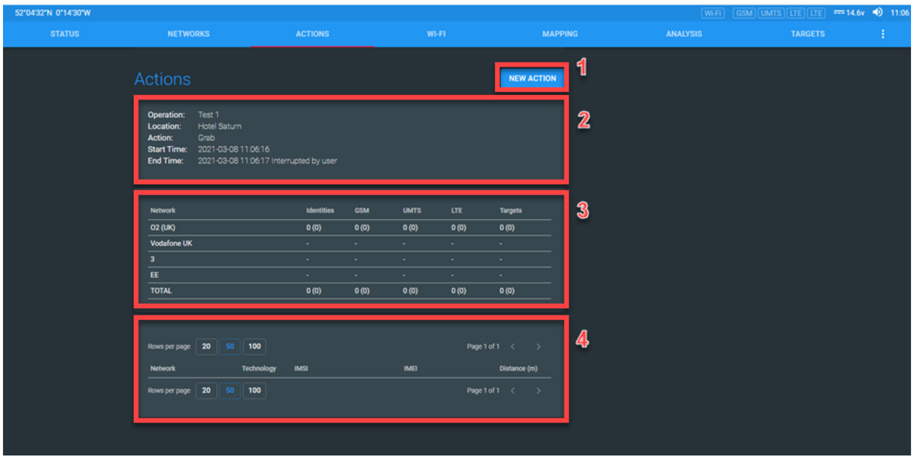
16.2 AUTOMATIC RE SCAN

NESIE will automatically start a full re-scan of the network scan on several occasions:

- If the user types in a new location
- If the GPS detects that the NESIE has moved more than 50m
- If no GPS fix is detected and the operator commences an operation

17. ACTIONS PAGE

An Action is the process of using the received or loaded network scan data then adjusting the network scan data before transmitting the altered data as a fake base transceiver station. The ACTIONS page is shown at Fig 116 below.



Operation: Test 1
Location: Hotel Saturn
Action: Grab
Start Time: 2021-03-08 11:06:16
End Time: 2021-03-08 11:06:17 Interrupted by user

Network	Identities	GSM	UMTS	LTE	Targets
O2 (UK)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
Vodafone UK	-	-	-	-	-
3	-	-	-	-	-
EE	-	-	-	-	-
TOTAL	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)

Rows per page 20 50 100 Page 1 of 1

Network	Technology	IMSI	IMEI	Distance (m)

Rows per page 20 50 100 Page 1 of 1

Fig 116. ACTIONS page

The ACTIONS page is made up of 4 panes

1. NEW ACTION button – discussed at Section 17.1 below.
2. Actions summary pane
3. Identity summary pane
4. Identity list pane

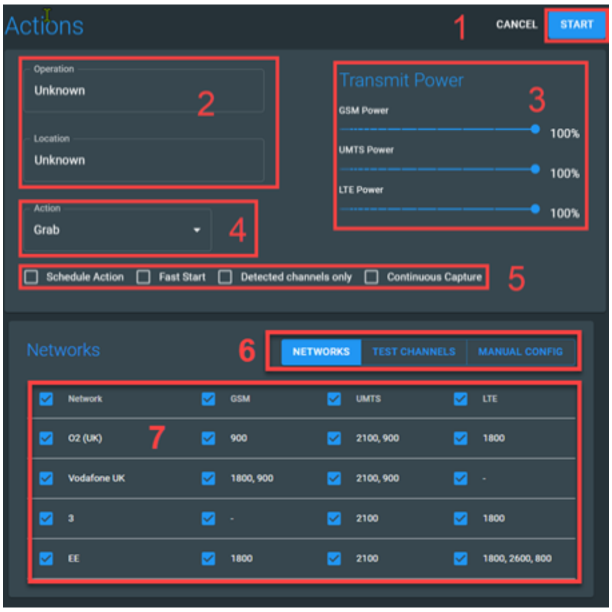
NOTE: Previous Action data - If the NESIE system has previously been used to carry out an Action, the previous Action data may still be displayed on the screen.

To start a NEW ACTION, the Operator must press the NEW ACTION button. The process of starting a new Action is detailed at Section 17.1 below.

NOTE: The remainder of the ACTIONS page will be discussed during the individual Actions.

17.1 NEW ACTIONS

When the operator presses the NEW ACTION button on the ACTIONS page as shown in Fig 116 above, the Actions set up page will be displayed, as shown below in Fig 117 below.



Operation: Unknown

Location: Unknown

GSM Power 100%

UMTS Power 100%

LTE Power 100%

Action: Grab

□ Schedule Action □ Fast Start □ Detected channels only □ Continuous Capture

☑ Network	☑ GSM	☑ UMTS	☑ LTE
☑ O2 (UK)	☑ 900	☑ 2100, 900	☑ 1800
☑ Vodafone UK	☑ 1800, 900	☑ 2100, 900	☑ -
☑ 3	☑ -	☑ 2100	☑ 1800
☑ EE	☑ 1800	☑ 2100	☑ 1800, 2600, 800

Fig 117. NEW ACTION page

The NEW ACTION page is made up from 7 panes:

1. CANCEL/START button
2. Operation & Location pane
3. Transmit Power pane
4. Action pane
5. Fast Start / Detected Channels pane
6. NETWORKS/TEST CHANNEL/MANUAL CONFIG pane
7. Networks pane

17.2 START / CANCEL BUTTON

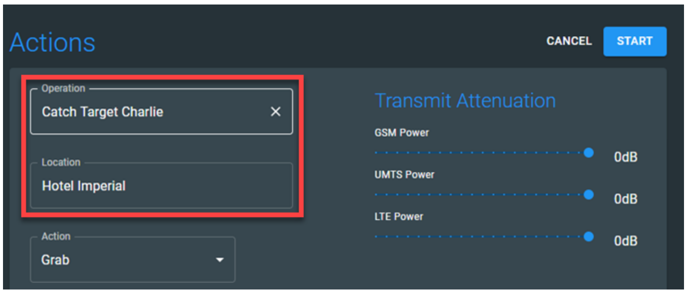
The NEW ACTION button will be replaced by the CANCEL START button. When the other panes have been completed, the operator will press the START button. The START button will start the NESIE transmitting.

17.3 CREATING AN OPERATION AND LOCATION

Before a user can carry out any Action (transmitting a fake BTS to collect or interact with cellular devices) the NESIE software will ask the operator for the name of the Operation and Location as shown below at Fig 118 below.

These Operation & Locations names are used to store and identify the files of data that will be used to identify the Targets details. If the files are not labelled correctly, it will make it harder to select the correct files.

Note: If the operator moves to a different area and forgets to rename the Location, the last captured data is stored by time/date stamp in the ANALYSIS page. The previous Location information is not overwritten.



Actions

CANCEL START

Operation: Catch Target Charlie

Location: Hotel Imperial

Action: Grab

Transmit Attenuation

GSM Power 0dB

UMTS Power 0dB

LTE Power 0dB

Fig 118. Operation & Location

Operation: The name of the current “job” the user is working on. This job may consist of several days or weeks’ worth of data at a variety of different locations. This operation may be a small, localised job to catch one drug dealer e.g. “Drug Dealer Stakeout” or a larger operation to catch a large gang of criminals over the whole region. In the example shown the Operation is called ‘Catch Target Charlie’.

Location: The name of the location is used as a reference so all users can easily identify where the Action was carried out later. There may be multiple Actions carried out at each location, all in the same operation. In the example shown the Location is called ‘Hotel Imperial’.

A user may want to retrieve multiple data files and compare them to see if the same mobile device has been seen at all locations.

A new location should be created each time a user performs an action or network scan at a new location.

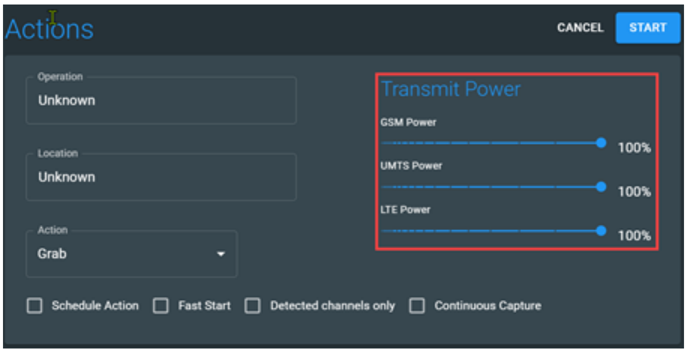
The location name can be for a broad area such as a town, if you will be moving and scanning, or very specific e.g. “The Nag’s Head Pub, Peckham”, if the scans will only be performed at that exact location,

The NESIE unit will continue the network scan until the START button is pressed and the system starts to transmit.

NOTE: An automatic re-scan is done if the location name is changed

17.4 TRANSMIT POWER

In certain operational situations, there may be a requirement for the NESIE operator to reduce the amount of power transmitted through the system transceivers. The Transmit Power pane permits the operator to apply amounts of **attenuation** to each individual transceiver. To alter the amount of attenuation applied to a transceiver, the operator must click on the blue slider button and drag it left to apply the appropriate amount of attenuation. Transmit attenuation control can be displayed in two ways, either as a percentage as seen below in Fig 119 or as a dB level.



Actions

CANCEL START

Operation: Unknown

Location: Unknown

Action: Grab

Transmit Power

GSM Power 100%

UMTS Power 100%

LTE Power 100%

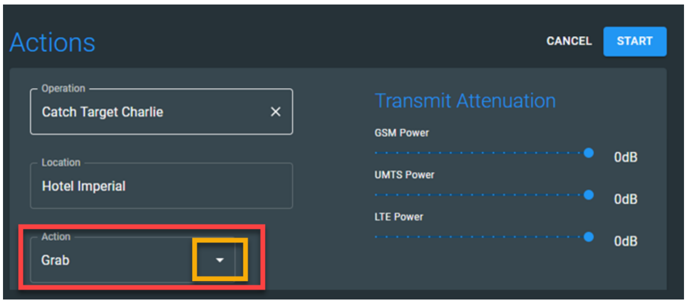
□ Schedule Action □ Fast Start □ Detected channels only □ Continuous Capture

Fig 119. Transmit Power

The operator can change the transmit Attenuation type (dB or %) in the Settings Section, as detailed at section 33.3.1.4.

17.5 ACTION TYPE PANE

The Action selelction pane allows the operator to choose from the available Action types. By default, Grab is selected. If the operator needs to select any of the other options, the drop-down arrow should be pressed as shown in the yellow box in Fig 120 below.



Actions

CANCEL START

Operation: Catch Target Charlie

Location: Hotel Imperial

Action: Grab

Transmit Attenuation

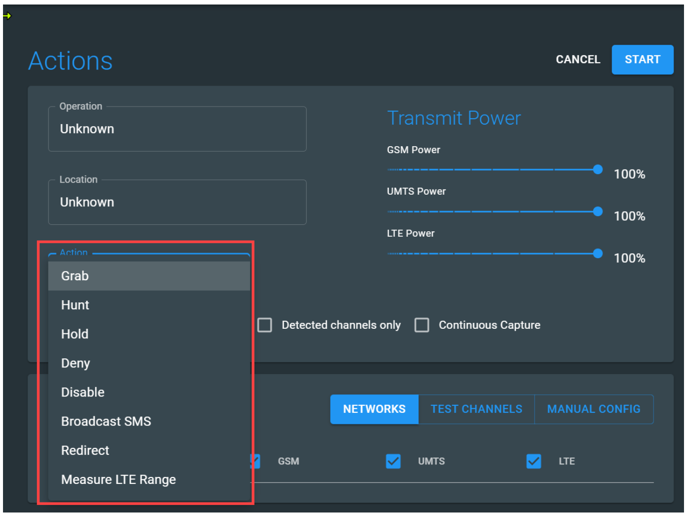
GSM Power 0dB

UMTS Power 0dB

LTE Power 0dB

Fig 120. Action type – drop-down

When the drop-down menu button is pressed, the Action selection menu is displayed as shown Fig 121 below. The currently selected Action is highlighted in grey.



Operation: Unknown

Location: Unknown

GSM Power: 100%

UMTS Power: 100%

LTE Power: 100%

□ Detected channels only □ Continuous Capture

☑ GSM ☑ UMTS ☑ LTE

Fig 121. Action selection menu

NOTE: A summary of each action type is below. Detailed instructions for each action type are found at:

Grab	**Section** Error! Reference source not found.
Hunt	**Section** Error! Reference source not found.
Hold	**Section 23**
Deny	**Section** Error! Reference source not found.
Disable	**Section** Error! Reference source not found.
Broadcast SMS	**Section** Error! Reference source not found.
Redirect	**Section** Error! Reference source not found.
Measure LTE Range	**Section 30**

17.5.1 GRAB

Grab is the process of transmitting fake base transceiver stations to gather the IMEIs and IMSIs from all the cellular devices in the area before rejecting them back to the real network. There is a way of using the grab process for ‘manual’ geolocation of a Target device.

17.5.2 HUNT

Hunt is the process of transmitting fake base transceiver stations to gather the IMEIs and IMSIs from all the cellular devices in the area loOKing for one or multiple Target identities, before rejecting them back to the real network. An audible and visual alarm will be used to alert the operator to the presence of a Target.

17.5.3 HOLD

Hold is the process of transmitting fake base transceiver stations to gather the IMEIs and IMSIs from all the cellular devices in the area loOKing for the first Target identified. This Target cellular device is moved onto a designated traffic channel and put into a Hold (Silent Call) state. When in this Hold state, the Target phone can be geolocated accurately using several methods.

17.5.4 DENY

Deny is the process of transmitting fake base transceiver stations to gather the IMEIs and IMSIs from all the cellular devices in the area loOKing for one or multiple Target identities. When the required identities are seen, they will be registered onto the NESIE base transceiver station and denied access to the real network. Any identities not required will be rejected back to the real network. This Deny state can be as long as required, even if the mobile device moves out of range of NESIE.

17.5.5 DISABLE

Disable is the process of transmitting fake base transceiver stations to gather the IMEIs and IMSIs from all the cellular devices in the area loOKing for one or multiple Target identities. When the required identities are seen, they will be sent a Disable code. This Disable code will temporarily Disable the mobile device and Deny it access to the real network. Any identities not required will be rejected back to the real network and not affected.

17.5.6 BROADCAST SMS

Broadcast SMS is the process of transmitting fake base transceiver stations to gather the IMEIs and IMSIs from all the cellular devices in the area loOKing for one or multiple Target identities. When the required identities are seen, they will be registered onto the NESIE base transceiver station and denied access to the real network. Upon registration on the NESIE network, an SMS will be broadcast (sent) to the Target cellular device(s). Any identities not required will be rejected back to the real network and not affected.

17.5.7 REDIRECT

Redirect is the process of transmitting fake base transceiver stations to gather the IMEIs and IMSIs from all the cellular devices on UMTS and LTE, then sending the Target devices a network command. This network command Redirects the Target devices off LTE and/or UMTS and down to GSM.

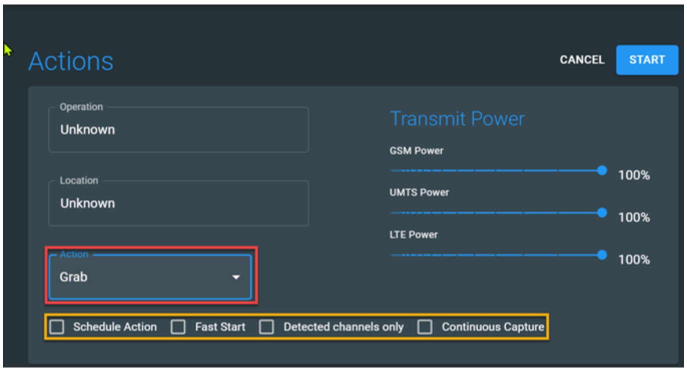
17.5.8 MEASURE LTE RANGE

Measure LTE Range is used in conjunction with the Cell Sites function on the CNEST survey tool. This Action can be used pre mission to conduct a rehearsal in a potential grab area. The CNEST can be taken into the area where the suspected Target will be. The SIM card numbers of SIMs in the CNEST module are saved as Targets in the NESIE UI. When NESIE is transmitting, it should capture the CNEST, if the NESIE is in range of the CNEST.

17.6 FAST START PANE

Depending on the type of action selected, the tick boxes displayed in this pane will change accordingly.

For Grab, the available options are displayed in Fig 122 below.



Operation: Unknown

Location: Unknown

Action: Grab

GSM Power 100%

UMTS Power 100%

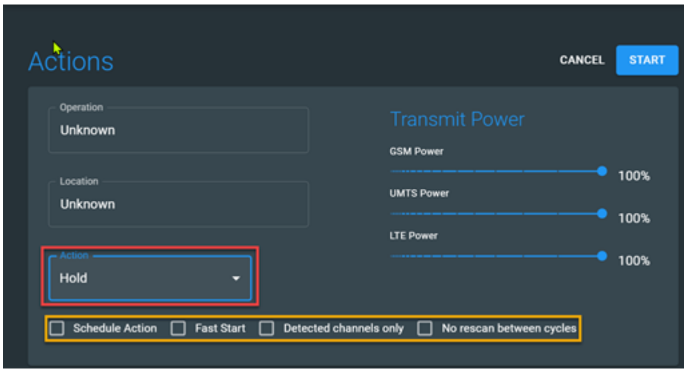
LTE Power 100%

□ Schedule Action □ Fast Start □ Detected channels only □ Continuous Capture

Fig 122. Tick boxes – Grab

- **Schedule Action**
- **Fast Start**
- **Detected channels only**
- **Continuous Capture**

For Hunt, Hold, Disable and Redirect, the available options are displayed in Fig 123 below.



Operation: Unknown

Location: Unknown

Action: Hold

GSM Power 100%

UMTS Power 100%

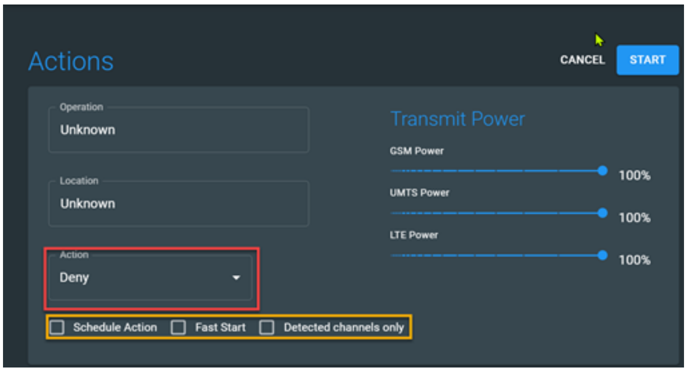
LTE Power 100%

□ Schedule Action □ Fast Start □ Detected channels only □ No rescan between cycles

Fig 123. Tick boxes - Hold

- **Schedule Action**
- **Fast Start**
- **Detected channels only**
- **No rescan between cycles**

For Deny and Broadcast SMS, the available options are displayed in Fig 124 below.



Actions

Operation: Unknown

Location: Unknown

Action: Deny

Transmit Power

GSM Power 100%

UMTS Power 100%

LTE Power 100%

□ Schedule Action □ Fast Start □ Detected channels only

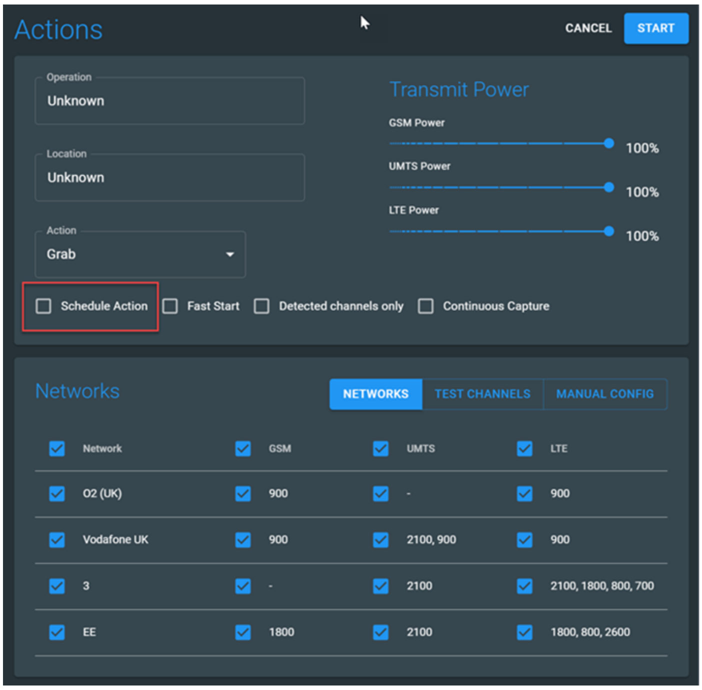
Fig 124. Tick boxes – Deny

- **Schedule Action**
- **Fast Start**
- **Detected channels only**

17.6.1 SCHEDULE ACTION

Schedule Action is available in all action types. There are no limits to the amount of Actions that can be scheduled.

Schedule Action allows the operator to set the system up to carry out an Action without the operator being present. The system must have power permanently applied to allow this to happen. The system is NOT able to switch itself on to carry out a scheduled Action. If using a multi channel system, all networks, technologies and bands can be selected, as required.



Actions

Operation: Unknown

Location: Unknown

Action: Grab

Transmit Power

GSM Power 100%

UMTS Power 100%

LTE Power 100%

□ Schedule Action □ Fast Start □ Detected channels only □ Continuous Capture

Networks

☑ Network	☑ GSM	☑ UMTS	☑ LTE
☑ O2 (UK)	☑ 900	☑ -	☑ 900
☑ Vodafone UK	☑ 900	☑ 2100, 900	☑ 900
☑ 3	☑ -	☑ 2100	☑ 2100, 1800, 800, 700
☑ EE	☑ 1800	☑ 2100	☑ 1800, 800, 2600

Fig 125 Schedule Action - selected

17.6.1.1 SET UP

Once the Schedule Action box has been ticked, this brings up and additional pane on the ACTIONS page (Fig 126).

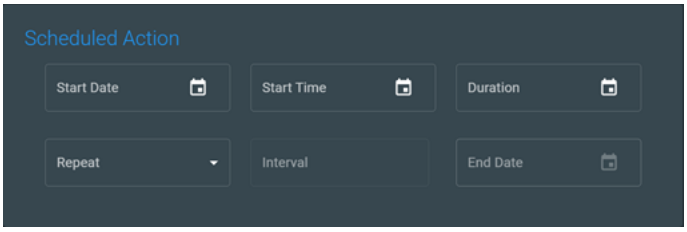


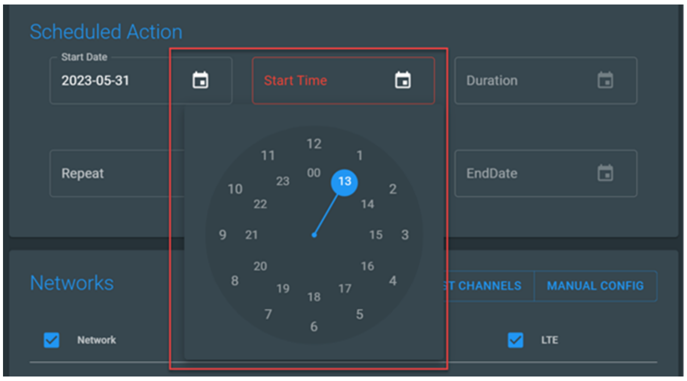
Fig 126 Schedule Action - options

This Schedule Action pane consists of the following options that can be adjusted to set up the Scheduled Action:

- Start Date
- Start Time
- Duration
- Repeat
- Interval
- End Date

Start Date – click on the calendar icon and select a date from the calendar that appears. Any time from the present onwards can be selected. It should be noted that if a date in the past is entered, the system will still allow the schedule to be saved. Alternatively, a date can be manually entered by clicking in the Start Date box.

Start Time – click on the calendar icon and a clock face appears, displaying hours. Click, hold and drag the blue circle to the required start hour. If the time to be set is on the outer clock face, click, hold drag the blue circle to the outer ring. When the blue circle is released, this will automatically set the hour. Once the hour is set, the minute clock face appears automatically. Again, click, hold and drag the blue circle to the required scheduled minute. Once the minute has been set, click anywhere outside of the clock face to set the Start Time.



Start Date: 2023-05-31

Fig 127 Scheduled Action - set start hour

Duration – how long does the NESIE need to carry out this Action for? By selecting the calendar icon in the Duration box, a clock face appears. The Duration is programmed exactly as if programming a Start Time.

The calendar icon in the Duration box will be highlighted for all Actions, except Grab. A Duration is required to be set if Continuous Capture has been selected.

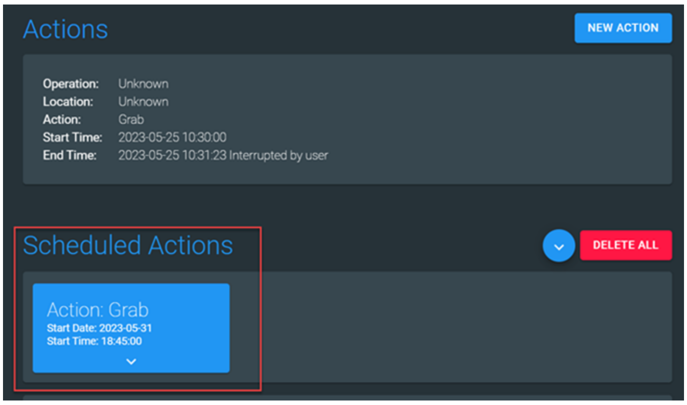
Repeat – how often do you want the scheduled action to be repeated? The options are:

- Never
- Minute
- Hourly
- Daily
- Weekly

Interval – all schedules require and interval. This box is closely tied to the Repeat duration selected. The interval is the duration of time between the Repeat actions.

End Date – when do you want the scheduled Action to end? Programmed exactly as per the Start Date.

Once the Scheduled Action has been programmed, the operator should press the ADD button at the top of the page. The Scheduled Action will appear in a separate pane on the ACTIONS page (Fig 128).



Actions

Operation: Unknown
Location: Unknown
Action: Grab
Start Time: 2023-05-25 10:30:00
End Time: 2023-05-25 10:31:23 Interrupted by user

Scheduled Actions

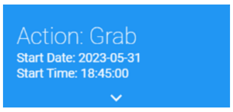
Action: Grab
Start Date: 2023-05-31
Start Time: 18:45:00

Fig 128 Scheduled Action – programmed

17.6.1.2 COLOUR OF SCHEDULED ACTIONS

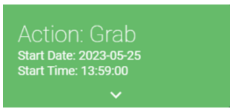
As is common across all NESIE interfaces, the colours of the programmed Scheduled Action give a quick loOK reference to the operator regarding the current state of the Scheduled Action.

There are three colours:



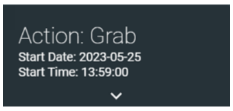
Action: Grab
Start Date: 2023-05-31
Start Time: 18:45:00

Scheduled Action still to take place



Action: Grab
Start Date: 2023-05-25
Start Time: 13:59:00

Scheduled Action in progress

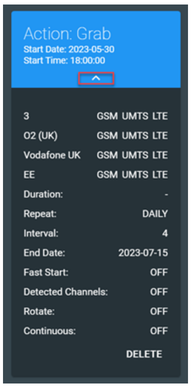


Action: Grab
Start Date: 2023-05-25
Start Time: 13:59:00

Scheduled Action expired

17.6.1.3 EXPANDING SCHEDULED ACTION PANE

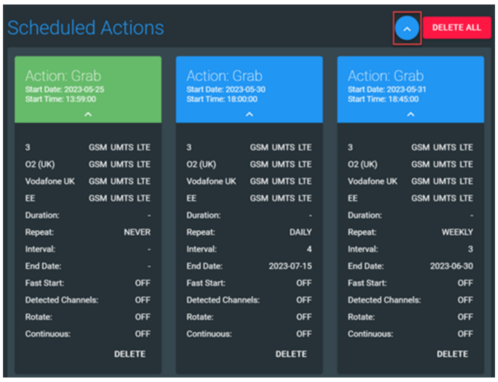
Once the Scheduled Action have been programmed and appear on the ACTIONS page, the pane can be expanded to view the Scheduled Action in more detail. This can be done on individual panes (Fig 129) or on the collective Scheduled Actions pane (Fig 130).



Action: Grab
Start Date: 2023-05-30
Start Time: 18:00:00

3	GSM UMTS LTE
O2 (UK)	GSM UMTS LTE
Vodafone UK	GSM UMTS LTE
EE	GSM UMTS LTE
Duration:	-
Repeat:	DAILY
Interval:	4
End Date:	2023-07-15
Fast Start:	OFF
Detected Channels:	OFF
Rotate:	OFF
Continuous:	OFF

Fig 129 Individual pane expansion



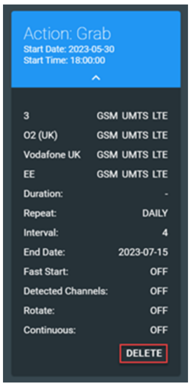
Scheduled Actions

Action: Grab Start Date: 2023-05-25 Start Time: 13:59:00		Action: Grab Start Date: 2023-05-30 Start Time: 18:00:00		Action: Grab Start Date: 2023-05-31 Start Time: 18:45:00	
3	GSM UMTS LTE	3	GSM UMTS LTE	3	GSM UMTS LTE
O2 (UK)	GSM UMTS LTE	O2 (UK)	GSM UMTS LTE	O2 (UK)	GSM UMTS LTE
Vodafone UK	GSM UMTS LTE	Vodafone UK	GSM UMTS LTE	Vodafone UK	GSM UMTS LTE
EE	GSM UMTS LTE	EE	GSM UMTS LTE	EE	GSM UMTS LTE
Duration:	-	Duration:	-	Duration:	-
Repeat:	NEVER	Repeat:	DAILY	Repeat:	WEEKLY
Interval:	-	Interval:	4	Interval:	3
End Date:	-	End Date:	2023-07-15	End Date:	2023-06-30
Fast Start:	OFF	Fast Start:	OFF	Fast Start:	OFF
Detected Channels:	OFF	Detected Channels:	OFF	Detected Channels:	OFF
Rotate:	OFF	Rotate:	OFF	Rotate:	OFF
Continuous:	OFF	Continuous:	OFF	Continuous:	OFF

Fig 130 Collective pane expansion

17.6.1.4 DELETING SCHEDULED ACTIONS

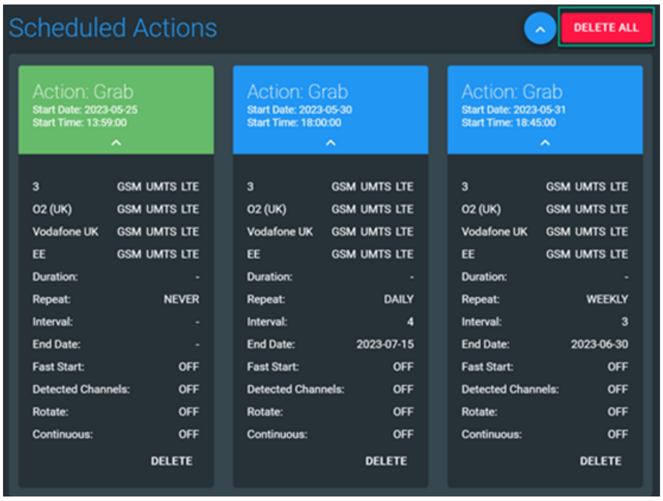
Deleting the Scheduled Actions and removing them from the ACTIONS page can be done both individually (Fig 131) and collectively (Fig 132).



Action: Grab
Start Date: 2023-05-30
Start Time: 18:00:00

3	GSM UMTS LTE
O2 (UK)	GSM UMTS LTE
Vodafone UK	GSM UMTS LTE
EE	GSM UMTS LTE
Duration:	-
Repeat:	DAILY
Interval:	4
End Date:	2023-07-15
Fast Start:	OFF
Detected Channels:	OFF
Rotate:	OFF
Continuous:	OFF

Fig 131 Delete Scheduled Action – individually



Scheduled Actions

	Action: Grab Start Date: 2023-05-25 Start Time: 13:59:00	Action: Grab Start Date: 2023-05-30 Start Time: 18:00:00	Action: Grab Start Date: 2023-05-31 Start Time: 18:45:00
3	GSM UMTS LTE	GSM UMTS LTE	GSM UMTS LTE
O2 (UK)	GSM UMTS LTE	GSM UMTS LTE	GSM UMTS LTE
Vodafone UK	GSM UMTS LTE	GSM UMTS LTE	GSM UMTS LTE
EE	GSM UMTS LTE	GSM UMTS LTE	GSM UMTS LTE
Duration:	-	-	-
Repeat:	NEVER	DAILY	WEEKLY
Interval:	-	4	3
End Date:	-	2023-07-15	2023-06-30
Fast Start:	OFF	OFF	OFF
Detected Channels:	OFF	OFF	OFF
Rotate:	OFF	OFF	OFF
Continuous:	OFF	OFF	OFF
	DELETE	DELETE	DELETE

Fig 132 Delete Scheduled Action - collectively

17.6.2 FAST START

The Fast Start option is available in all action types.

During normal operation (Fast Start Un-Ticked), the NESIE system will automatically re check the current network scan data that has been collected prior to transmitting. If a GPS fix has been achieved, the NESIE system will know if the unit is still at the same location and start within several seconds. However, if no GPS fix has been achieved, the NESIE system cannot be sure that the unit has not been moved and will automatically rescan the network data. Depending on the density of the cellular networks, this may take a up to 2 – 3 minutes or more if the NESIE is made up of a single transceiver unit.

If the operator is certain that the system has been in position for a sufficient time, and they are happy that the NESIE has completed a network scan or if there is an urgent operational need to transmit immediately, they can override this automatic check facility and command the NESIE to start immediately by ticking the Fast Start box.

To initiate the Fast Start, the operator should click in the white box and ensure the box turns blue and a tick is displayed ☑ Fast Start. Then press the START button. The NESIE system will now bypass the network scan and recheck and will normally start transmitting within 10 seconds.

17.6.3 DETECTED CHANNELS ONLY

The Detected Channels Only option is available in all five action types.

During normal operations, the NESIE system will carry out a network scan on all technologies and bands that have been pre-set by the operator. During this network scan, the NESIE extracts and stores the received serving cell and neighbour cell data as it is transmitted by the cellular network providers. This network data may include additional channels and bands that may not be in the detect range of the NESIE system or not currently in use by any mobile devices / devices in this area.

The NESIE operator therefore has the option to ignore any channels that the NESIE has not detected itself and only transmit on the channels that have been received / detected during the network scan. This may be from the current or loaded scan data.

Examples:

- The LTE neighbour lists indicate that there are channels in 1800,2600 and 800. However, the NESIE can only see 1800 and 800.

  If Detected Channels Only is selected, NESIE will only Tx on 1800 and 800, saving time.

- The UMTS neighbour lists indicate that there are channels in 2100 and 900. However, the NESIE can only see 2100.

  If Detected Channels Only is selected, NESIE will only Tx on 2100

- If a network provider does not operate on GSM channels, only UMTS & LTE.

  If Detected Channels Only is selected, the NESIE (even if the operator has selected GSM for capture) will not transmit on GSM.

NOTE: The example above for No GSM, holds true for the other techs. If there are no channels for the tech, NESIE will not transmit on that technology if Detected Channels Only is selected.

To enable the Detected Channels Only facility, the operator should click in the box, ensure the box turns blue and a tick is displayed ☑ Detected channels only. Then press the START button.

17.6.4 CONTINUOUS CAPTURE

If the operator wishes to conduct a continuous capture, this box should be ticked. The NESIE will now conduct a capture across all the networks and technologies selected (one cycle). Under normal operation, the NESIE will pause the transmit phase after the completion of each cycle and conduct another network scan phase.

Then, upon completion of the network scan the system will automatically restart the transmit phase. This transmit and network scan process will continue constantly until the STOP button is pressed.

The transmit phase is shown by the green header bar and the network scan phase is shown by the purple header bar.

17.6.5 NO RESCAN BETWEEN CYCLES

The No Rescan Between Cycles option will only be displayed when the operator chooses either the Continuous Capture, Grab, Hunt, Hold Actions, where an operator requires the option to search for a Target over a long period.

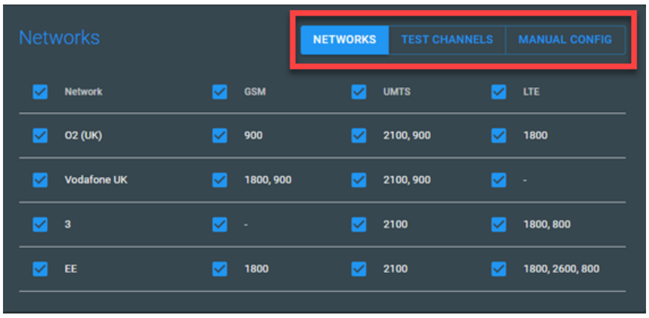
In normal operation (box not ticked), NESIE will complete one transmit cycle of the chosen network operators and technologies, stop transmitting, then carry out another network scan. This network scan may take several minutes, or longer if the user is in a moving vehicle.

When the No rescan between cycles option is selected ☑ No rescan between cycles the operator is commanding NESIE not to carry out a network scan at the end of every transmit cycle. The operator must be aware that the data used to create the fake BTSs may be less effective at grabbing the Target mobile device.

When ticked, the system will now complete a cycle of the chosen network providers and technologies and immediately start the cycle again. There will be no pause in the transmit cycle to carry out a network scan.

17.7 NETWORKS / TEST CHANNELS / MANUAL CONFIG

By default, the NETWORKS button is activated. This allows the operator to choose the networks and technologies from the table as shown in Fig 133 below.



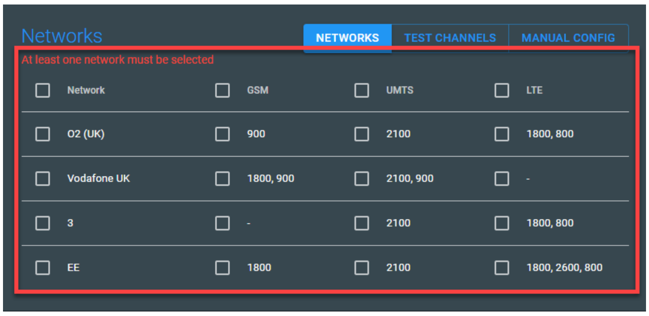
☑ Network	☑ GSM	☑ UMTS	☑ LTE
☑ O2 (UK)	☑ 900	☑ 2100, 900	☑ 1800
☑ Vodafone UK	☑ 1800, 900	☑ 2100, 900	☑ -
☑ 3	☑ -	☑ 2100	☑ 1800, 800
☑ EE	☑ 1800	☑ 2100	☑ 1800, 2600, 800

Fig 133. NETWORKS/TEST CHANNELS/ MANUAL CONFIG buttons

If required, the operator can choose TEST CHANNELS or MANUAL CONFIG and press the relevant button. Test channels are discussed in detail at section 18.2. Manual Configuration is discussed in detail at section 18.3.

17.7.1 NETWORKS

The lower selection of the ACTIONS page is the Networks pane as displayed at Fig 134 below. This pane allows the operator to choose which networks and technologies NESIE will mimic and create a fake base transceiver station on.

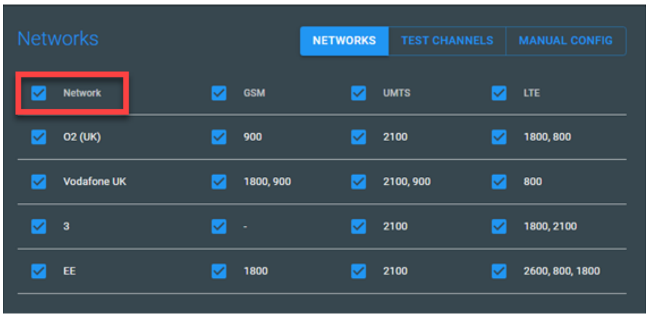


At least one network must be selected

□ Network	□ GSM	□ UMTS	□ LTE
□ O2 (UK)	□ 900	□ 2100	□ 1800, 800
□ Vodafone UK	□ 1800, 900	□ 2100, 900	□ -
□ 3	□ -	□ 2100	□ 1800, 800
□ EE	□ 1800	□ 2100	□ 1800, 2600, 800

Fig 134. Networks pane

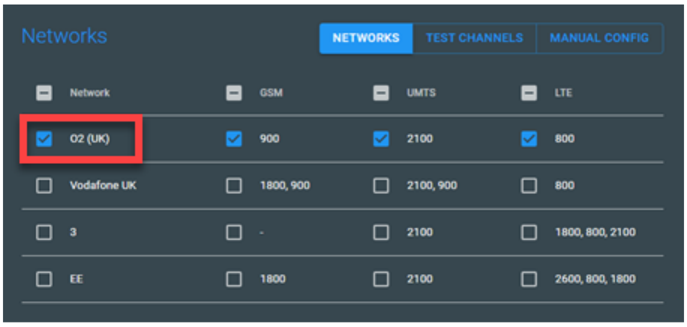
If the all networks tick box is selected, all network operators and all technologies will be automatically selected as shown in Fig 135 below.



☑ Network	☑ GSM	☑ UMTS	☑ LTE
☑ O2 (UK)	☑ 900	☑ 2100	☑ 1800, 800
☑ Vodafone UK	☑ 1800, 900	☑ 2100, 900	☑ 800
☑ 3	☑ -	☑ 2100	☑ 1800, 2100
☑ EE	☑ 1800	☑ 2100	☑ 2600, 800, 1800

Fig 135. All networks & technologies

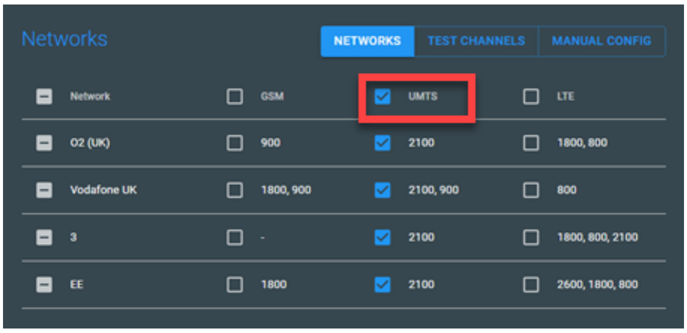
If all the available technologies are required on only one network operator, the user must tick the box next to that network operator. The other boxes in that row will be automatically selected as shown in Fig 136 below.



⊟ Network	⊟ GSM	⊟ UMTS	⊟ LTE
☑ O2 (UK)	☑ 900	☑ 2100	☑ 800
□ Vodafone UK	□ 1800, 900	□ 2100, 900	□ 800
□ 3	□ -	□ 2100	□ 1800, 800, 2100
□ EE	□ 1800	□ 2100	□ 2600, 800, 1800

Fig 136. All technologies on O2 (UK)

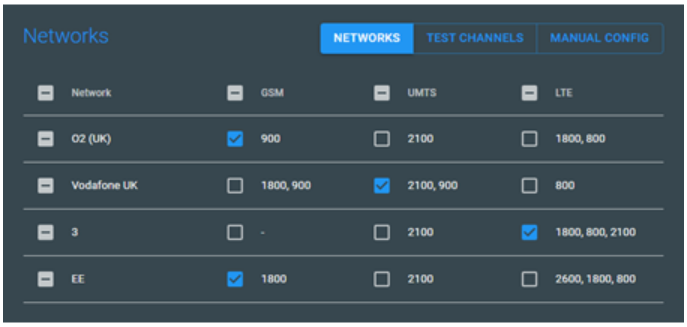
If the operator wants to select UMTS on all network operators, the top UMTS box can be ticked and all the other UMTS boxes in that column will automatically be selected, as shown below in Fig 137.



⊟ Network	☐ GSM	☑ UMTS	☐ LTE
⊟ O2 (UK)	☐ 900	☑ 2100	☐ 1800, 800
⊟ Vodafone UK	☐ 1800, 900	☑ 2100, 900	☐ 800
⊟ 3	☐ -	☑ 2100	☐ 1800, 800, 2100
⊟ EE	☐ 1800	☑ 2100	☐ 2600, 1800, 800

Fig 137. UMTS on all providers

If required, the operator can manually tick any network providers and technologies as shown below in Fig 138.



⊟ Network	⊟ GSM	⊟ UMTS	⊟ LTE
⊟ O2 (UK)	☑ 900	☐ 2100	☐ 1800, 800
⊟ Vodafone UK	☐ 1800, 900	☑ 2100, 900	☐ 800
⊟ 3	☐ -	☐ 2100	☑ 1800, 800, 2100
⊟ EE	☑ 1800	☐ 2100	☐ 2600, 1800, 800

Fig 138. Manual selection

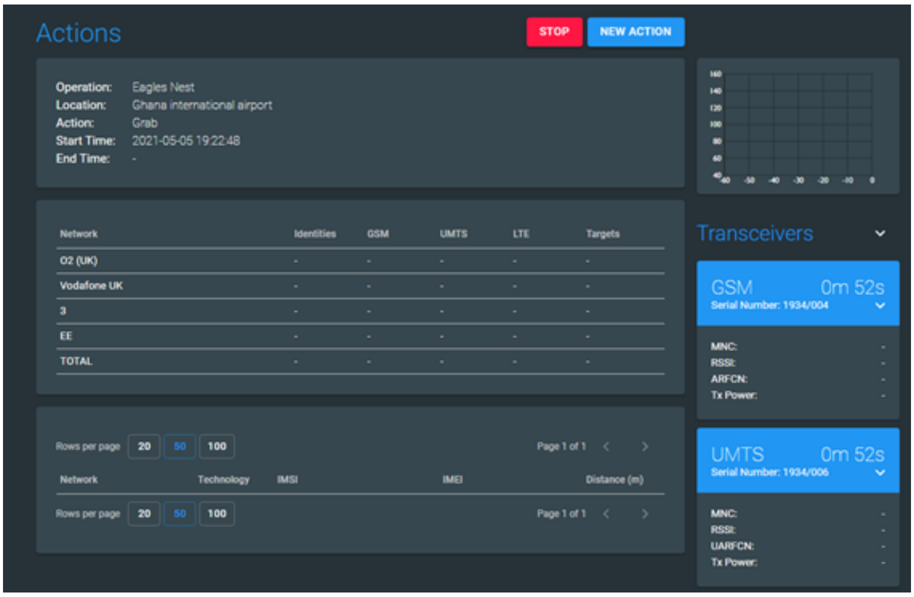
17.7.2 ADDITIONAL PANES

Depending on the Action type selected, other panes below the network / technology selection pane will be displayed. These additional panes will be discussed in detail during the relevant Action instructions.

17.7.3 START BUTTON

Pressing the START button will stop NESIE conducting a network scan and the software will use the data gathered to automatically set up the fake base transceiver stations. The NESIE will now move to the transmit phase, to attract the cellular devices in the area over to the fake base transceiver stations. The receive side of the NESIE system now swaps from listening to the downlink frequency (the network providers) and starts listening to the uplink frequencies to detect the cellular device to extract the IMEI and IMSIs.

When the operator presses the START button, the ACTIONS page will clear down any previously displayed information and present the new Action data as shown below at Fig 139.



Operation: Eagles Nest
Location: Ghana international airport
Action: Grab
Start Time: 2021-05-05 19:22:48
End Time: -

Network	Identities	GSM	UMTS	LTE	Targets
O2 (UK)	-	-	-	-	-
Vodafone UK	-	-	-	-	-
3	-	-	-	-	-
EE	-	-	-	-	-
TOTAL	-	-	-	-	-

Network	Technology	IMSI	IMEI	Distance (m)

GSM 0m 52s
Serial Number: 1934/004
MNC: -
RSSI: -
ARFCN: -
Tx Power: -

UMTS 0m 52s
Serial Number: 1934/006
MNC: -
RSSI: -
UARFCN: -
Tx Power: -

Fig 139. ACTIONS page

17.7.4 TEST CHANNELS (TEST NETWORKS)

The TEST CHANNELS feature allows the operator to manually create a test network and specify which channels the test network is transmitted on.

A test network can be used for:

- Creating a fake cell tower in an area where no cellular coverage exists. Under normal operations, NESIE carries out a network scan to detect the real network settings before using the real data as a basis for creating fake towers. However, if no cellular coverage exists, NESIE has nothing to copy before changing this data into a fake cell tower.

- Creating a test network which can be used in conjunction with cellular device that are fitted with Test SIM cards. This allows over the air testing without impacting on the real networks.

A Test Network will always create a network with the following settings:

Mobile Country Code	001	
Mobile Network Code	01	(usually displayed as TEST)

Therefore, only devices out of real cellular coverage and or those with test SIMs, loOKing for a MCC of 001 and MNC of 01 will see the test network.

17.7.5 TEST NETWORK – OUT OF COVERAGE

If the operator is required to create a cell tower in an area where no real cellular network data is available, they can manually enter the desired channel numbers and start transmitting.

When the START button is pressed, the NESIE will create and transmit a fake cell tower using the following settings:

Mobile Country Code	001
Mobile Network Code	01
Local Area Code	Randomly generated by NESIE
Cell ID	Randomly generated by NESIE
ARFCN	As selected by the user
UARFCN	As selected by the user
EARFCN	As selected by the user
PSC	Randomly generated by NESIE
PCID	Randomly generated by NESIE

Because the NESIE is in an area of no cellular coverage, all the cellular devices will be Out of Service and searching for any network. They will see the NESIE system and attempt to register on to it. They will then be requested to send their IMEI & IMSI and NESIE will measure the distance to the device.

This Out of Service process can also be used to conduct other operational modes such as Hold, Deny, Disable etc.

18. TEST CHANNELS – TESTING

If required, the NESIE system can be configured manually to work in test mode.

18.1 TEST SIM CARDS

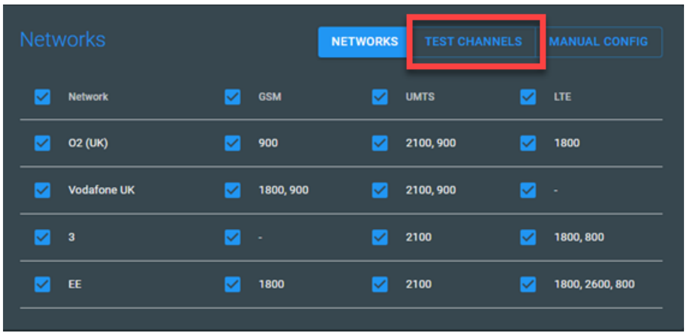
When NESIE transmits in TEST CHANNELS mode, it creates a cell tower with an MCC and MNC that match the test SIM cards, therefore any cellular devices with a test SIM card fitted will connect to the NESIE system and all other devices should ignore NESIE.

NOTE: It is normal for devices using standard SIM cards, as issued by the cellular network providers, which are not in cellular coverage, will still attempt to register with NESIE.

18.2 TEST CHANNELS - SET UP

To create a TEST CHANNEL, the NESIE operator should start a Grab operation as per the previous section.

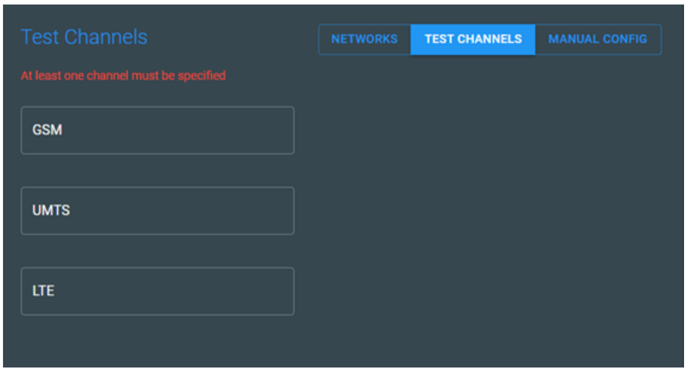
- **Navigate to the ACTIONS page**
- **Pressed the NEW ACTION button**
- **Choose the Grab, Hunt, Deny etc Action from the drop-down menu**



☑ Network	☑ GSM	☑ UMTS	☑ LTE
☑ O2 (UK)	☑ 900	☑ 2100, 900	☑ 1800
☑ Vodafone UK	☑ 1800, 900	☑ 2100, 900	☑ -
☑ 3	☑ -	☑ 2100	☑ 1800, 800
☑ EE	☑ 1800	☑ 2100	☑ 1800, 2600, 800

Fig 140. TEST CHANNELS

The operator should now press the TEST CHANNELS button, shown in the red box in Fig 140 above. The screen shown below at will now be shown.



Test Channels

At least one channel must be specified

Fig 141. TEST CHANNELS – settings

The operator can now enter the desired channel number for GSM, UMTS and LTE.

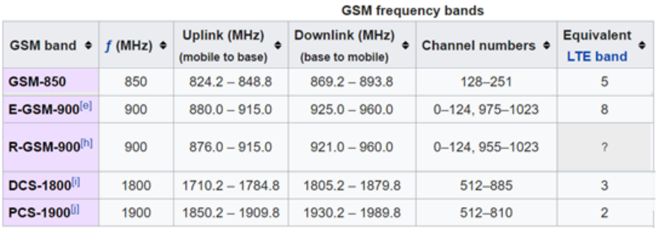
If only the channel number for one technology (e.g. GSM) is entered, only that technology will be transmitted.

If the channel number for 2 or more technologies is entered (e.g. UMTS and LTE), NESIE will now either rotate through both channels (if using a single channel system) or transmit multiple channels depending on the resources available.

18.2.1 TEST NETWORK – GSM

To create a GSM test network, the operator must choose which GSM ARFCN (Absolute Radio Frequency Channel Number) to transmit on.

NESIE will detect which ARFCN has been chosen and if possible, change the frequency accordingly. However, caution must be used for the 1800/1900 bands due to the ARFCN channel number clash as shown below in Fig 142 below.

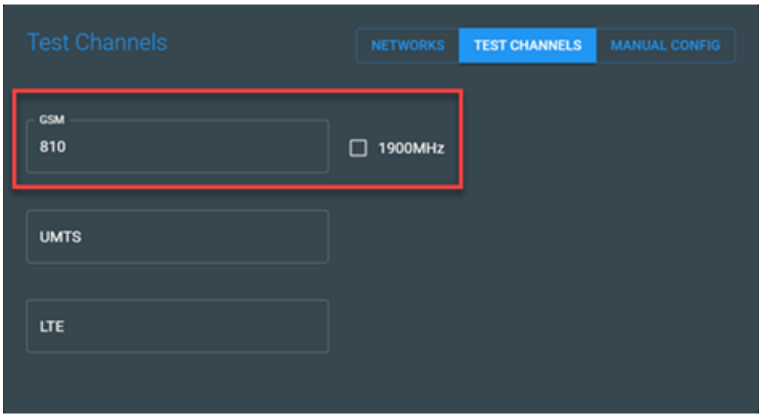


GSM frequency bands

GSM band	*f* (MHz)	Uplink (MHz) (mobile to base)	Downlink (MHz) (base to mobile)	Channel numbers	Equivalent LTE band
GSM-850	850	824.2 – 848.8	869.2 – 893.8	128–251	5
E-GSM-900[e]	900	880.0 – 915.0	925.0 – 960.0	0–124, 975–1023	8
R-GSM-900[h]	900	876.0 – 915.0	921.0 – 960.0	0–124, 955–1023	?
DCS-1800[i]	1800	1710.2 – 1784.8	1805.2 – 1879.8	512–885	3
PCS-1900[j]	1900	1850.2 – 1909.8	1930.2 – 1989.8	512–810	2

Fig 142. GSM channels

To overcome this problem, if a channel number is inserted between 512-810, a tick box will appear next to the GSM channel box. This will give the operator the option to select whether NESIE transmits on 1800MHz (unticked) or 1900MHz (ticked). (Fig 143)



GSM 810

☐ 1900MHz

UMTS

LTE

Fig 143. 1900MHz tick box

When the operator presses the START button, NESIE will create and transmit a fake cell tower using the following settings:

Mobile Country Code	001
Mobile Network Code	01
Local Area Code	Randomly chosen
Cell ID	Randomly chosen
ARFCN	As selected by user

18.2.2 TEST NETWORK - UMTS

To create a UMTS test network, the operator must choose which UARFCN (UMTS Absolute Radio Frequency Channel Number) to transmit on. NESIE will detect which UARFCN has been chosen and change the frequency accordingly. The list of possible UARFCNs is shown below in Fig 144.

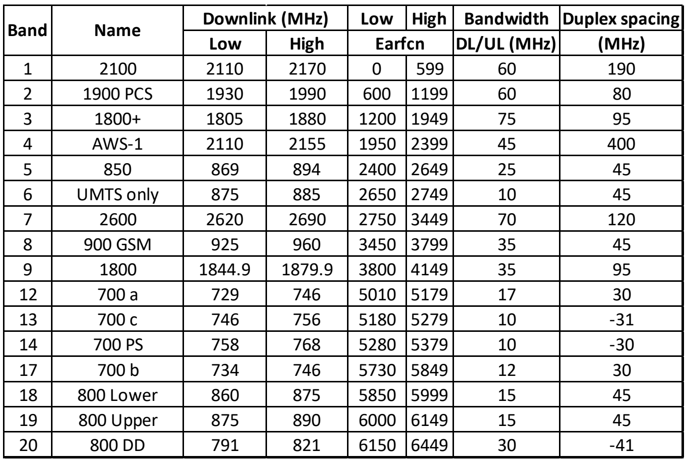
Band	Name	Downlink (MHz)		UARFCN		Bandwidth	Equivalent
		Low	High			(MHz)	GSM band
1	2100	2112.4	2167.6	10562	10838	60	
2	1900 PCS	1932.4	1987.6	9662	9938	60	PCS 1900
3	1800 DCS	1807.4	1877.6	1162	1513	75	DCS 1800
5	850	871.4	891.6	4357	4458	25	GSM 850
8	900 GSM	927.4	957.6	2937	3088	35	E-GSM 900
20	800 DD	793.4	818.6	4512	4638	30	

Fig 144. UMTS channels

NESIE will automatically create a Primary Scrambling Code (PSC). The downlink PSC's are used for cell separation. One PSC is allocated for each cell. The PSC (0 to 511) is used to select which base station is to be accessed and should be different to any BTS in the area on the selected UARFCN.

18.2.3 TEST NETWORK – LTE

To create an LTE test network, the operator must choose which EARFCN (LTE Absolute Radio Frequency Channel Number) to transmit on. NESIE will detect which EARFCN has been chosen and change the frequency accordingly. The list of possible EARFCNs is shown below in Fig 145.



Band	Name	Downlink (MHz)		Low	High	Bandwidth	Duplex spacing
		Low	High	Earfcn		DL/UL (MHz)	(MHz)
1	2100	2110	2170	0	599	60	190
2	1900 PCS	1930	1990	600	1199	60	80
3	1800+	1805	1880	1200	1949	75	95
4	AWS-1	2110	2155	1950	2399	45	400
5	850	869	894	2400	2649	25	45
6	UMTS only	875	885	2650	2749	10	45
7	2600	2620	2690	2750	3449	70	120
8	900 GSM	925	960	3450	3799	35	45
9	1800	1844.9	1879.9	3800	4149	35	95
12	700 a	729	746	5010	5179	17	30
13	700 c	746	756	5180	5279	10	-31
14	700 PS	758	768	5280	5379	10	-30
17	700 b	734	746	5730	5849	12	30
18	800 Lower	860	875	5850	5999	15	45
19	800 Upper	875	890	6000	6149	15	45
20	800 DD	791	821	6150	6449	30	-41

Fig 145. LTE channels

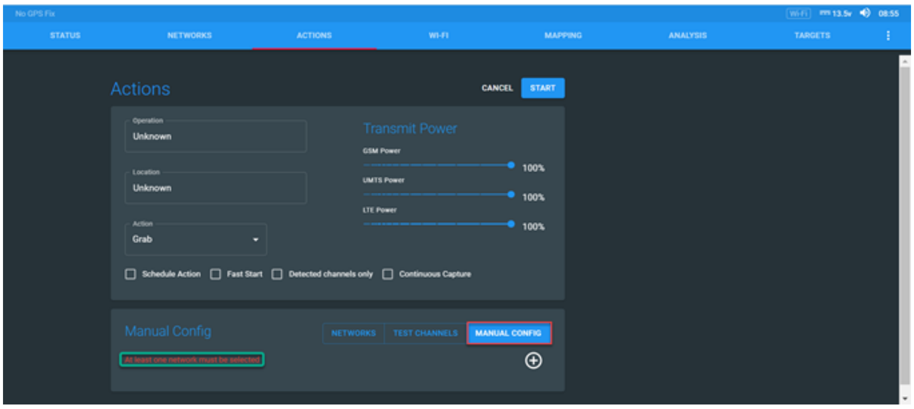
18.3 MANUAL CONFIGURATION

Manual configuration allows the NESIE operator to manually create base stations transmitting any MCC, MNC, LAC, Cell ID and on any Channel.

To set up a manual configuration, the operator should click the MANUAL CONFIG button as shown in the red box in Fig 146 below.

The MANUAL CONFIG pane will appear, as shown below in Fig 146.

The screen will display a warning stating that At least one network must be selected, as shown in the green box. To add a configuration the operator must press the ⊕ button as shown in the amber box.



Actions

Operation: Unknown

Location: Unknown

Action: Grab

Transmit Power

GSM Power 100%

UMTS Power 100%

LTE Power 100%

□ Schedule Action □ Fast Start □ Detected channels only □ Continuous Capture

Manual Config

At least one network must be selected

Fig 146. MANUAL CONFIG

18.3.1 MANUAL CONFIG – SECTIONS

The operator will then be presented with the MANUAL CONFIG pane which consists of 3 areas as seen below in Fig 147.

The first section, in the red box, will be populated with information as the operator completes the fields in the yellow box. The operator should now select the appropriate technology from the drop-down menu, then, as a minimum complete the fields for the channel number (ARFCN for GSM, UARFCN for UMTS and EARFCN for LTE), the MCC (Mobile Country Code) and the MNC (Mobile Network Code) for each individual configuration created.

Once the operator has selected an MCC from the drop-down list, the MNC drop-down list will be populated with all the known network providers MNCs for that country (at time of software release). The operator must now select the relevant MNC. If the operator has further data that they need to apply to the configuration, this can be found in the ADVANCED section which can be accessed by clicking on ADVANCED inside the green box.

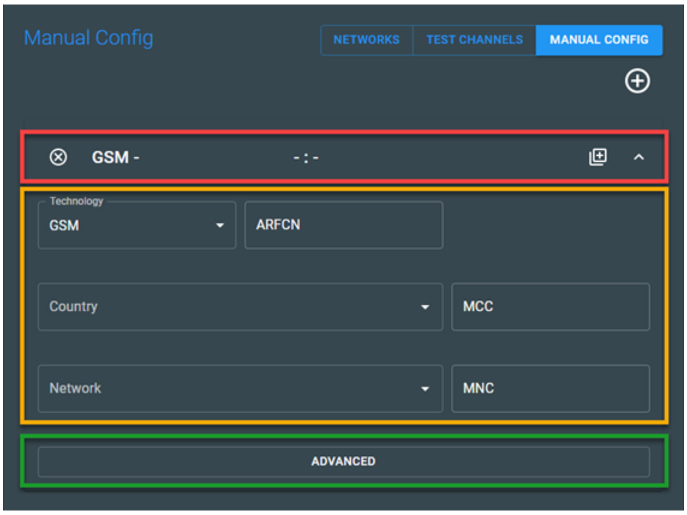


Fig 147. MANUAL CONFIG – sections

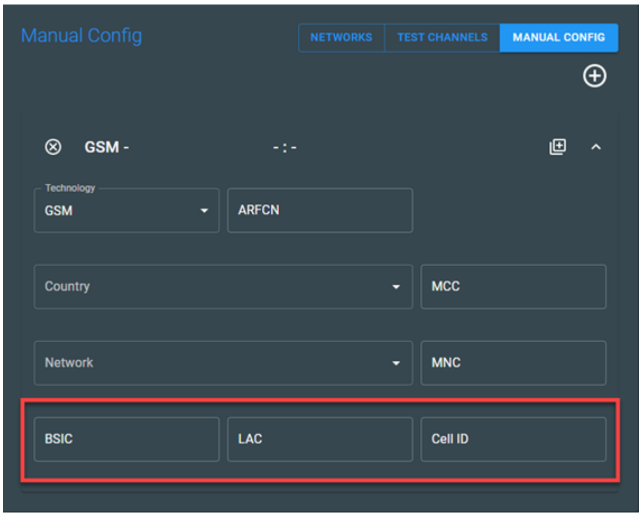
18.3.2 MANUAL CONFIG – ADVANCED

When the operator clicks on ADVANCED, a further set of three fields will open as seen in Fig 148 below. These provide the operator the ability to add further information to their manual configuration.

The left hand field of the ADVANCED selections, changes depending on what technology the configuration is for:

- GSM will show BSIC (Base Station Identity Code) field.
- UMTS will show PSC (Primary Scrambling Code) field.
- LTE will show PCID (Physical Cell ID) field.

The other two fields are for the LAC (Local Area Code) and Cell ID that will be transmitted when the START button is pressed.


Manual Config

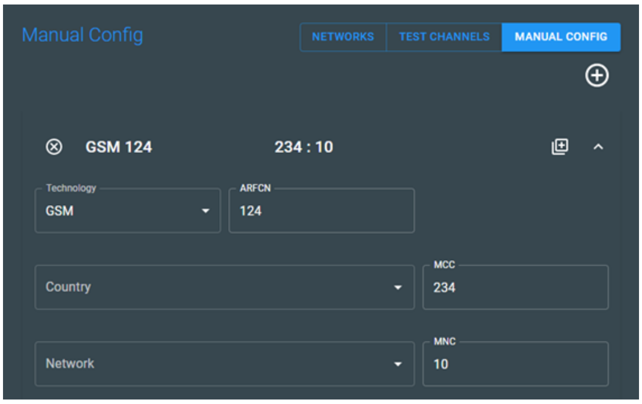
GSM - -:-

Technology: GSM
ARFCN
Country
MCC
Network
MNC
BSIC
LAC
Cell ID

Fig 148. MANUAL CONFIG – advanced

18.3.3 MANUAL CONFIG - EXAMPLES

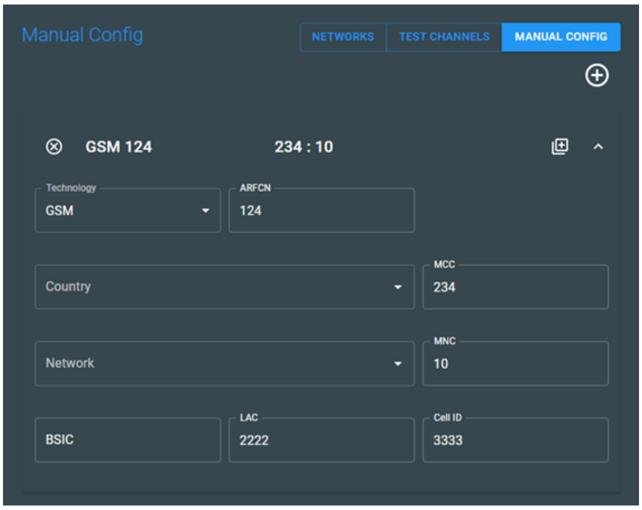
An example of a basic manual configuration entry to input MCC and MNC can be seen below at Fig 149 and an advanced manual configuration entry to enable the operator to input BSIC/LAC and Cell ID can be seen below at Fig 150.


Manual Config

GSM 124 234 : 10

Technology: GSM
ARFCN: 124
Country
MCC: 234
Network
MNC: 10

Fig 149. MANUAL CONFIG – MCC & MNC



GSM 124 234 : 10

Technology: GSM

ARFCN: 124

Country

MCC: 234

Network

MNC: 10

BSIC

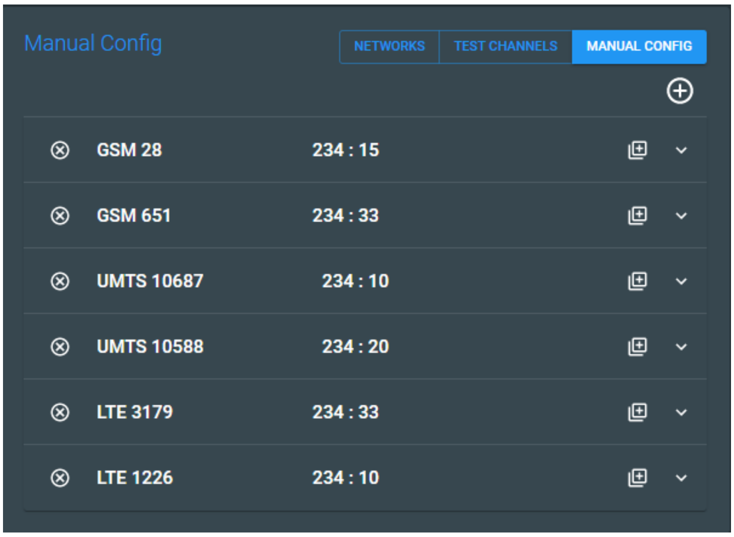
LAC: 2222

Cell ID: 3333

Fig 150. MANUAL CONFIG - BSIC/LAC and Cell ID

18.3.4 MANUAL CONFIG – MULTIPLE TECHNOLOGIES AND NETWORKS

An example of manual configuration using all technologies and various mobile networks and frequency channels is shown below at Fig 151.



GSM 28 234 : 15

GSM 651 234 : 33

UMTS 10687 234 : 10

UMTS 10588 234 : 20

LTE 3179 234 : 33

LTE 1226 234 : 10

Fig 151. MANUAL CONFIG – multiple entries

CAUTION: MANUAL CONFIGURATION SHOULD ONLY BE UNDERTAKEN BY EXPERIENCED OPERATORS. THIS OPTION IS INTENDED TO PROVIDE A VERY PRECISE WAY OF TUNING THE SYSTEM FOR SPECIFIC ENVIRONMENTS OR OPERATIONAL SITUATIONS. IT IS SUGGESTED THAT LESS EXPERIENCED OPEATORS USE THE NETWOKRS SELECTION PROCES, WHICH ALLOWS NESIE TO AUTOMATICALLY CONFIGURE THE SYSTEM

19. GRAB

A Grab is the process of transmitting fake base transceiver stations to capture and log the IMSI and IMEI; whilst measuring the distance from the NESIE system to all the cellular devices that can be detected. Once the IDs have been logged and the distance measured, the cellular devices are rejected back to the real network.

NESIE can log between 1200-1500 identities per channel in one minute. Therefore, if a 3 channel NESIE system is used in a very dense cellular environment it, could capture up to 4500 identities in 1 minute.

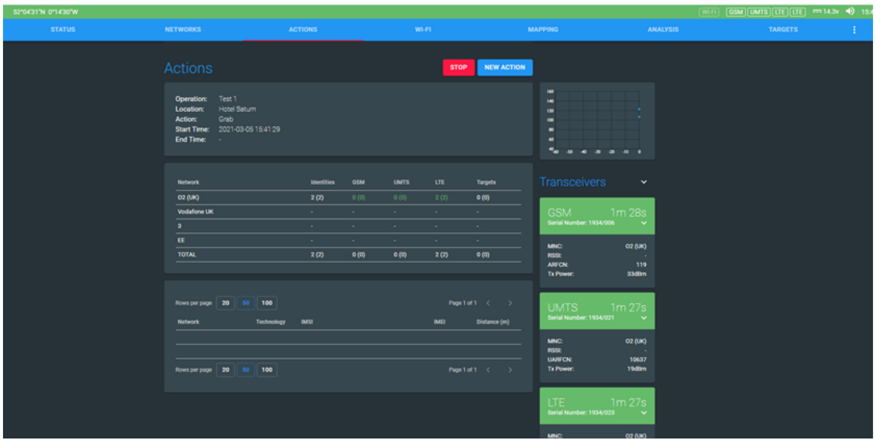
Wherever possible, this capture should be conducted whilst the NESIE system is static.

By default, the Grab will complete 1 transmit cycle of the user defined network providers & technologies then stop transmitting (unless Continuous Capture is selected). The transmit phase is highlighted by displaying a green bar on the UI header bar and on any required resource panes. When the transmitters are turned off, the system automatically returns to the network scan phase.

To start a Grab action, the user should follow the NEW ACTION procedure detailed in Section 17.1 above.

- Navigate to the ACTIONS page
- Press the NEW ACTION button
- Enter the Operation name and Location
- Choose the Grab from the drop-down menu
- Adjust the Transmit Power if required
- Choose Fast Start if required
- Choose Detected Channels only if required
- Choose Continuous Capture if required
- Select the required networks providers and technologies
- Press the START button

When the START button is pressed, the current view of the Actions page will be refreshed and show the live results of the Grab. This will be referred to as the Action summary page as shown below at Fig 152. All the data from the screen has been removed apart from the Grab headings.



Actions

Operation: Test 1
Location: Hotel Saturn
Action: Grab
Start Time: 2021-03-05 15:41:29
End Time: -

Network	Identities	GSM	UMTS	LTE	Targets
O2 (UK)	2 (2)	0 (0)	0 (0)	2 (2)	0 (0)
Vodafone UK	-	-	-	-	-
3	-	-	-	-	-
EE	-	-	-	-	-
TOTAL	2 (2)	0 (0)	0 (0)	2 (2)	0 (0)

Network	Technology	IMSI	IMEI	Distance (m)

Transceivers

GSM 1m 28s
Serial Number: 1934/006
MNC: O2 (UK)
RSSI: -
ARFCN: 119
Tx Power: 33dBm

UMTS 1m 27s
Serial Number: 1934/021
MNC: O2 (UK)
RSSI: -
UARFCN: 10637
Tx Power: 19dBm

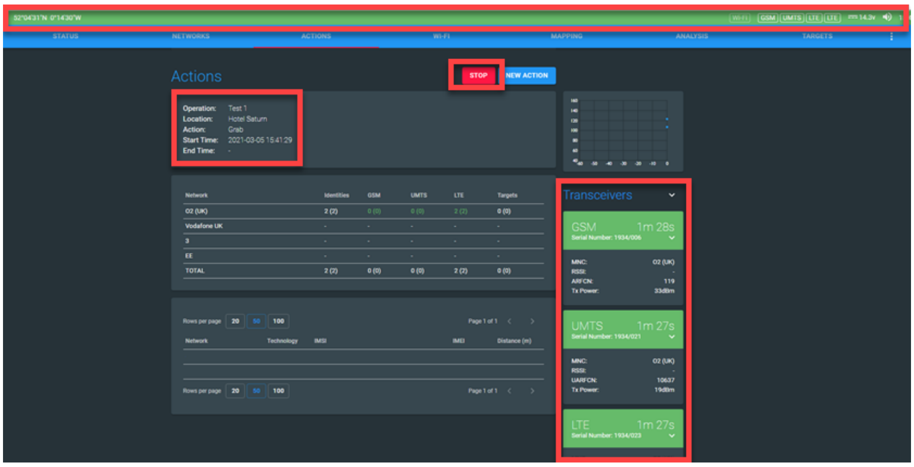
LTE 1m 27s
Serial Number: 1934/023
MNC: O2 (UK)

Fig 152. Refreshed Action summary

19.1 ACTION SUMMARY PAGE

The Actions summary page will initially refresh and show the current Action details and most of the other details will be blank, as shown below at Fig 153.

> **NOTE: Prior to starting a Grab, NESIE will carry out a recheck of the network scan data. If required, it will pause the transmit phase in order to collect more network data – this is shown by the purple bar on the header or in the transceiver resource panes. If required, the NESIE operator could stop the Grab and restart it after clicking the Fast Start button.**



Operation: Test 1
Location: Hotel Saturn
Action: Grab
Start Time: 2021-03-05 15:41:29
End Time: -

Network	Identities	GSM	UMTS	LTE	Targets
O2 (UK)	2 (2)	0 (0)	0 (0)	2 (2)	0 (0)
Vodafone UK	-	-	-	-	-
3	-	-	-	-	-
EE	-	-	-	-	-
TOTAL	2 (2)	0 (0)	0 (0)	2 (2)	0 (0)

Network	Technology	IMSI	IMEI	Distance (m)

GSM 1m 28s
Serial Number: 1934/006
MNC: O2 (UK)
RSSI: -
ARFCN: 119
Tx Power: 33dBm

UMTS 1m 27s
Serial Number: 1934/021
MNC: O2 (UK)
RSSI: -
UARFCN: 10637
Tx Power: 19dBm

LTE 1m 27s
Serial Number: 1934/023

Fig 153. Refreshed Action summary page

As seen in Fig 153 above, the following will be displayed on the refreshed page:

- Top bar will turn green to indicate that the system is transmitting
- A STOP button will be displayed next to the NEW ACTION button
- The Action summary pane will be updated with the new Action details
- The transceiver pane(s) will appear. This will display the settings of the BTS or multiple BTSs's that are being transmitted, along with the time left to run in this configuration
- Identity summary pane will refresh, showing blank fields
- The identity results pane will refresh and reset to blank fields

19.1.1 ACTION SUMMARY PANE

The Action summary pane display is shown below at Fig 154. The pane displays the following data:

Operation: Name of current operation

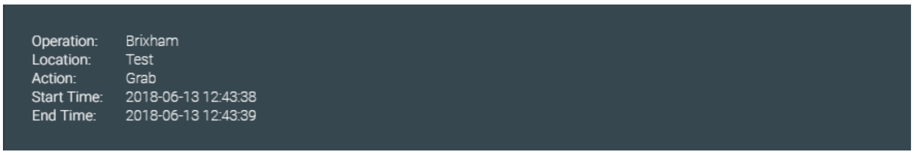
Location: Name of location as entered by the operator

Action: Action type

Start Time: Time the Action was started

End Time: Will display one of three things:

Running, if still conducting an Action
The **Time** the action was completed
Interrupted by User – If user presses the STOP button



Operation: Brixham
Location: Test
Action: Grab
Start Time: 2018-06-13 12:43:38
End Time: 2018-06-13 12:43:39

Fig 154. Action summary pane

19.1.2 IDENTITY SUMMARY PANE

The identity summary pane, as shown at Fig 155 below, displays the total number of identities and unique identities that have been captured on each network provider and technology. If any of the identities are listed on the NESIE as a Target, they will be counted and displayed in the Targets column.

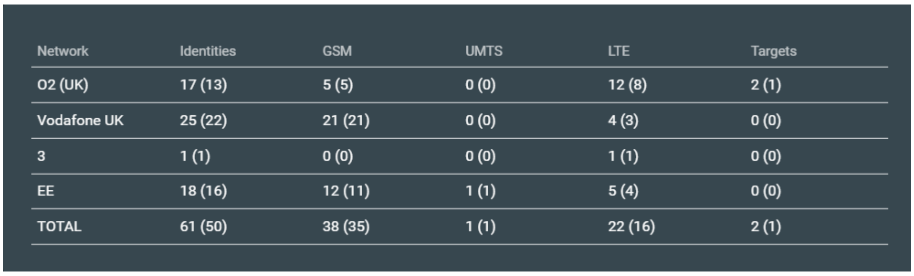
In the table below, it can be seen that on the O2 network, a total of 17 identities and (13) unique identities have been gathered.

- Totals:
  5 on GSM, 0 on UMTS, 12 on LTE.

- Unique Identities:
  (5) on GSM, however, only (8) of the 12 identities found on LTE were unique. This may mean that some of the devices were captured more than once during the Grab.

- Targets:
  In the 02 Grab, a total of 2 identities were captured, but both identities belonged to 1 unique Target.

The bottom line of the table displays the total number of identities and breaks down the total for each technology and Targets.



Network	Identities	GSM	UMTS	LTE	Targets
O2 (UK)	17 (13)	5 (5)	0 (0)	12 (8)	2 (1)
Vodafone UK	25 (22)	21 (21)	0 (0)	4 (3)	0 (0)
3	1 (1)	0 (0)	0 (0)	1 (1)	0 (0)
EE	18 (16)	12 (11)	1 (1)	5 (4)	0 (0)
TOTAL	61 (50)	38 (35)	1 (1)	22 (16)	2 (1)

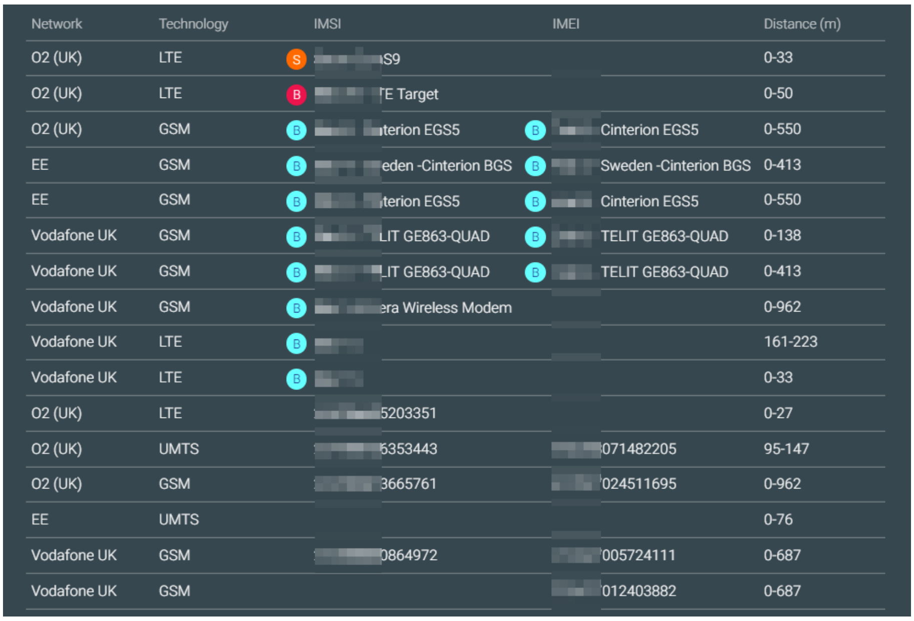
Fig 155. Identity summary pane

NOTE: The unique identities are displayed by default. If the user wishes to turn this facility off, they should refer to section 33.3.2.3.

19.1.3 IDENTITY LIST PANE

The identity results pane is the main page that will be used by the operator. As identities are gathered, they will be displayed in this pane. The identity results pane is displayed at Fig 156 below.

NOTE: The table below has some information blurred to ensure no sensitive data is shown.



Network	Technology	IMSI	IMEI	Distance (m)
O2 (UK)	LTE	S [redacted]S9	[redacted]	0-33
O2 (UK)	LTE	B [redacted]TE Target		0-50
O2 (UK)	GSM	B [redacted]terion EGS5	B [redacted] Cinterion EGS5	0-550
EE	GSM	B [redacted]eden -Cinterion BGS	B [redacted] Sweden -Cinterion BGS	0-413
EE	GSM	B [redacted]terion EGS5	B [redacted] Cinterion EGS5	0-550
Vodafone UK	GSM	B [redacted]LIT GE863-QUAD	B [redacted] TELIT GE863-QUAD	0-138
Vodafone UK	GSM	B [redacted]LIT GE863-QUAD	B [redacted] TELIT GE863-QUAD	0-413
Vodafone UK	GSM	B [redacted]era Wireless Modem		0-962
Vodafone UK	LTE	B [redacted]		161-223
Vodafone UK	LTE	B [redacted]		0-33
O2 (UK)	LTE	[redacted]5203351		0-27
O2 (UK)	UMTS	[redacted]6353443	[redacted]071482205	95-147
O2 (UK)	GSM	[redacted]3665761	[redacted]024511695	0-962
EE	UMTS			0-76
Vodafone UK	GSM	[redacted]0864972	[redacted]005724111	0-687
Vodafone UK	GSM		[redacted]012403882	0-687

Fig 156. Identity list pane

The data displayed in the pane is:

Network: Network that the identity was detected on

Technology: The technology being transmitted when the ID was detected

IMSI: The IMSI reported by the cellular device

IMEI: The IMEI reported by the cellular device

Distance: The distance measured between NESIE and the cellular device

The operator can choose the number of lines to display per page by selecting from 10, 20 or 50. By default the number of rows is set to 50. As shown below in Fig 157.

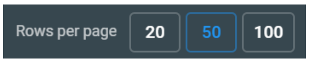


Fig 157. Rows per page

If more than one page of identities is detected, the number of pages will be updated. If the operator wants to scroll through the available pages the < or > button can be used, as shown below in Fig 158.

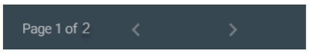


Fig 158. Page navigation

If any Targets are detected, the Target identities are indicated by a coloured circle showing the first letter of the Target name, as shown below in Fig 159. Any Targets found will appear at the top of the identity list whereas all other identities will scroll down on the master list.

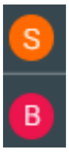


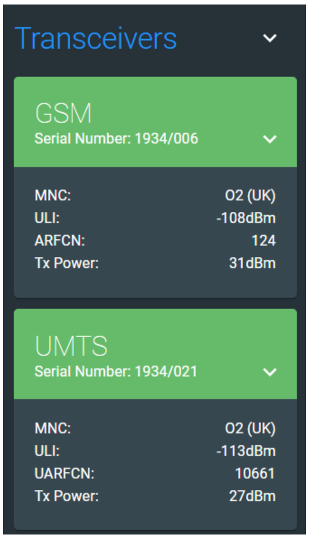
Fig 159. Target icon

19.1.4 **TRANSCEIVER PANE**

When the START button is pressed, NESIE switches from the network scan phase (monitoring the network providers settings on the downlink frequencies) to the transmit phase, transmitting the fake BTS data on the downlink frequencies and monitoring the uplink frequencies for any cellular devices in the area.

19.1.4.1 TRANSCEIVER PANE – COMPACT VIEW

As shown in Fig 160 below, by default the transceiver pane(s) are shown in the compact view. In this view only the basic information is displayed:



Transceivers

GSM
Serial Number: 1934/006

MNC: O2 (UK)
ULI: -108dBm
ARFCN: 124
Tx Power: 31dBm

UMTS
Serial Number: 1934/021

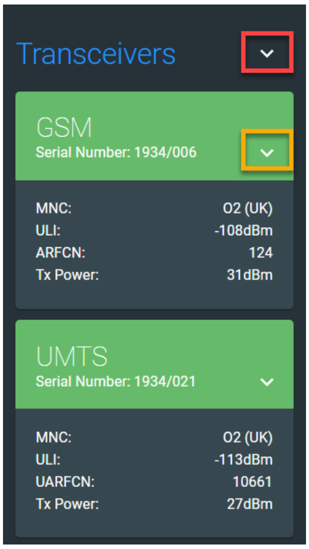
MNC: O2 (UK)
ULI: -113dBm
UARFCN: 10661
Tx Power: 27dBm

Fig 160. transceiver panes – compact view

MNC	Mobile Network Code being transmitted
ULI	Uplink Interference
ARFCN	Channel Number NESIE is transmitting on
Tx Power	Output Power

NOTE – ULI readings should be monitored in GSM bands. If the ULI readings are high (>-95dBm) then the operator should check the distance between the transmit and receive antennas. Ideally, there should be 2m separation between antennas. If the ULI readings are strong, this will decrease the detection range of NESIE.

It is possible to expand the transceiver panes. Each individual transceiver can be expanded individually by clicking on the ⌄ arrow. All transceiver panes can be expanded by clicking the arrow next to the transceiver title. Transceivers ⌄.



Transceivers

GSM
Serial Number: 1934/006

MNC: O2 (UK)
ULI: -108dBm
ARFCN: 124
Tx Power: 31dBm

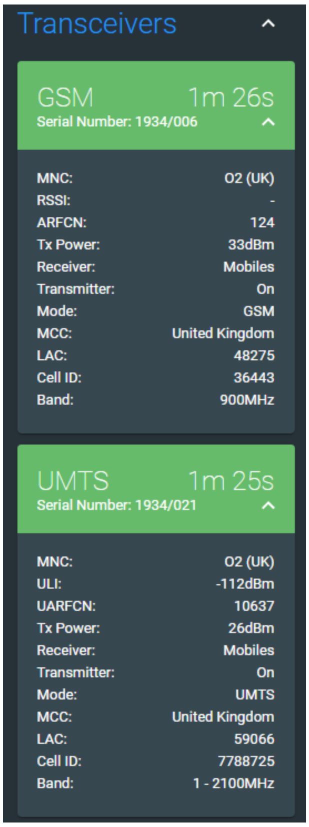
UMTS
Serial Number: 1934/021

MNC: O2 (UK)
ULI: -113dBm
UARFCN: 10661
Tx Power: 27dBm

Fig 161. transceiver panes – expand arrow

19.1.4.2 TRANSCEIVER PANE – EXPANDED VIEW

During the transmit phase, the transceiver panes will display the data that is being transmitted by the NESIE system. They can be expanded to show all the available information, as shown below in Fig 162.



Transceivers

GSM 1m 26s
Serial Number: 1934/006

MNC:	O2 (UK)
RSSI:	-
ARFCN:	124
Tx Power:	33dBm
Receiver:	Mobiles
Transmitter:	On
Mode:	GSM
MCC:	United Kingdom
LAC:	48275
Cell ID:	36443
Band:	900MHz

UMTS 1m 25s
Serial Number: 1934/021

MNC:	O2 (UK)
ULI:	-112dBm
UARFCN:	10637
Tx Power:	26dBm
Receiver:	Mobiles
Transmitter:	On
Mode:	UMTS
MCC:	United Kingdom
LAC:	59066
Cell ID:	7788725
Band:	1 - 2100MHz

Fig 162. transceiver pane – transmit

- HEADER Technology & Remaining time in this configuration
  Serial Number of the module
- **MNC:** Mobile Network Code NESIE is transmitting
- **RSSI:** Received Signal Strength Indication
- **ULI:** Uplink Interference
- **ARFCN*:** GSM channel number NESIE is transmitting on
- **UARFCN*:** UMTS channel number NESIE is transmitting on
- **EARFCN*:** LTE channel number NESIE is transmitting on
- **Tx Power**: Transmit power output by NESIE
- **Receiver**: Mobiles – Listening to the cellular devices on uplink
- **Transmitter:** On / Off
- **Mode:** Current Technology
- **MCC:** Mobile Country Code NESIE is transmitting
- **LAC:** Local Area Code that NESIE is transmitting
- **Cell ID:** Cell ID that NESIE is transmitting
- **Band:** Frequency band NESIE is transmitting in
- **PSC*:** UMTS Primary Scrambling Code NESIE is transmitting
- **PCID*:** LTE Physical Cell ID NESIE is transmitting

* - The relevant field will be displayed depending on which technology is being transmitted.

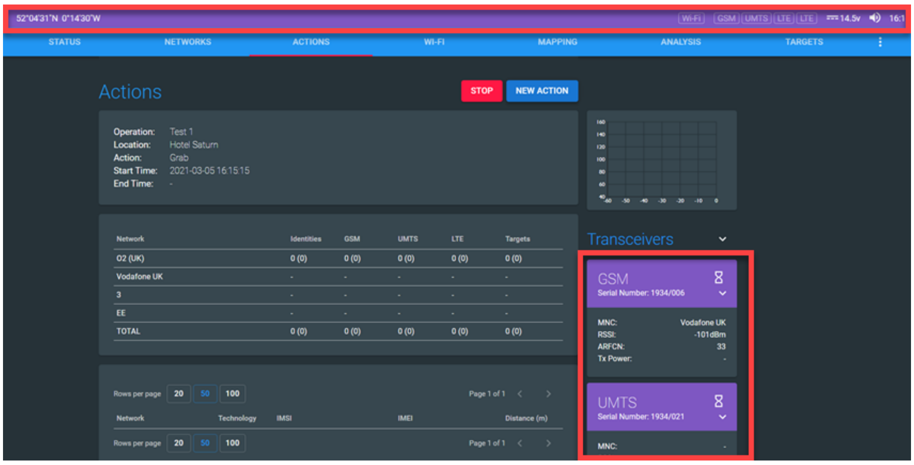
19.2 START

After the user has pressed the START button, NESIE will enter the transmit phase. If NESIE has a GPS Fix and has logged enough network scan data, the Grab will commence within a few seconds and the Action summary page will be displayed.

19.2.1 PAUSE BEFORE START - VALIDATING SCAN DATA

If the NESIE does not have enough network scan data, or if it needs to re-validate the data, NESIE will not commence transmitting until the revalidation is complete. This validation is a quick (usually only several seconds) check on the scan data already in the NESIE memory. This check will be shown by a purple header bar on the UI.

The Action summary page will be refreshed as normal; however, the green header bar will not be displayed until the network scan is completed. There will also be an hourglass timer displayed in the transceiver pane, as shown in Fig 163 below.



Operation: Test 1
Location: Hotel Saturn
Action: Grab
Start Time: 2021-03-05 16:15:15
End Time: -

Network	Identities	GSM	UMTS	LTE	Targets
O2 (UK)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
Vodafone UK	-	-	-	-	-
3	-	-	-	-	-
EE	-	-	-	-	-
TOTAL	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)

Network	Technology	IMSI	IMEI	Distance (m)

GSM
Serial Number: 1934/006
MNC: Vodafone UK
RSSI: -101dBm
ARFCN: 33
Tx Power: -

UMTS
Serial Number: 1934/021
MNC: -

Fig 163. Action summary – not transmitting

19.2.2 TRANSMIT – CYCLE THROUGH NETWORKS / TECHNOLOGIES

If the user has chosen multiple network providers and technologies, the system will automatically move from provider 1 to provider 2, then to provider 3 etc.

19.2.2.1 SINGLE CHANNEL NESIE

The single channel NESIE system will automatically cycle through the pre-set network providers and technologies, but will minimise the number of software changes to save time for the Action. It takes approx. 10 seconds to swap the system software from 1 technology to another.

Therefore, if the GSM transmit time is set to 60s and the NESIE has automatically detected 3 channels for each of the UMTS and LTE bands and there are 3 network providers, and each provider has 3 technologies the time taken for a Grab would be:

Provider 1	LTE	Transmit time = 90s, Software swap = 10s
Provider 1	GSM	Transmit time = 60s, Software swap = 10s
Provider 1	UMTS	Transmit time = 90s, Software swap = 0s
Provider 2	UMTS	Transmit time = 90s, Software swap = 10s
Provider 2	GSM	Transmit time = 60s, Software swap = 10s
Provider 2	LTE	Transmit time = 90s, Software swap = 0s
Provider 3	LTE	Transmit time = 90s, Software swap = 10s
Provider 3	GSM	Transmit time = 60s, Software swap = 10s
Provider 3	UMTS	Transmit time = 90s, STOP transmitting

Total Time **Transmit time = 12mins + Software swaps = 1min**

19.2.2.2 MULTIPLE CHANNEL NESIE – 3 STACK

A 3 channel (3 Stack) system will allocate 1 technology per transceiver (TRX) and transmit on one network provider at a time. Therefore, if NESIE has detected 3 channels on each of the UMTS & LTE bands for each of the 3 network providers, the system will carry out the process below:

TRX 1	Provider 1 – GSM		
TRX 2	Provider 1 – UMTS	}	90 Secs
TRX 3	Provider 1 – LTE		
Software Swap			10 Secs
TRX 1	Provider 2 – GSM		
TRX 2	Provider 2 – UMTS	}	90 Secs
TRX 3	Provider 2 – LTE		
Software Swap			10 Secs
TRX 1	Provider 3 – GSM		
TRX 2	Provider 3 – UMTS	}	90 Secs
TRX 3	Provider 3 – LTE		

Total Time **Transmit time = 4mins 30sec + software swap = 20s**

During the transmit phase, the header bar will turn green and at the end of the Grab transmit cycle, the NESIE will turn off the transmitters and automatically re commence the network scan. The top bar will turn blue, but the transceivers will be show purple in the STATUS page.

19.2.3 IDENTITY SUMMARY PANE – LIVE UPDATE

As the NESIE system conducts the Grab, the number of IDs (IMSI, IMEI or both) collected will be updated in real time. If any of the captured identities are listed in the database as Targets, the number in the Targets column will also increase.

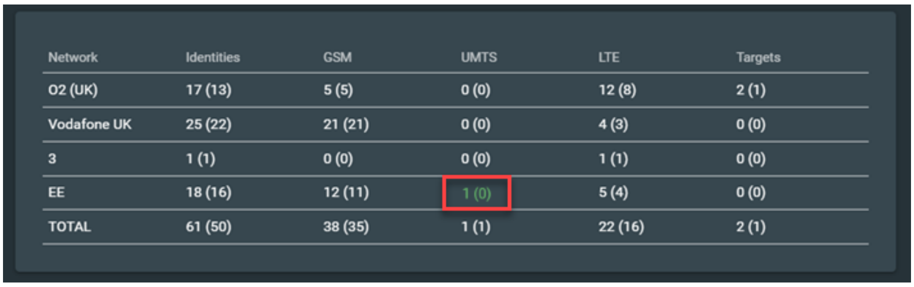
19.2.3.1 SINGLE CHANNEL NESIE

A single channel NESIE module rotating through each operator / technology is shown below in Fig 164.

The operator can also identify which network and technology the NESIE system is transmitting on from the ID summary page. As shown below in Fig 164, NESIE is transmitting on EE – UMTS, this is identified by the number of IDs displayed as a green number.

If the NESIE does not obtain any identities on a particular network provider / technology, a '0' will be displayed in the appropriate row / column.

If the NESIE has yet to transmit on a particular network / technology, a '-' will be displayed.



Network	Identities	GSM	UMTS	LTE	Targets
O2 (UK)	17 (13)	5 (5)	0 (0)	12 (8)	2 (1)
Vodafone UK	25 (22)	21 (21)	0 (0)	4 (3)	0 (0)
3	1 (1)	0 (0)	0 (0)	1 (1)	0 (0)
EE	18 (16)	12 (11)	1 (0)	5 (4)	0 (0)
TOTAL	61 (50)	38 (35)	1 (1)	22 (16)	2 (1)

Fig 164. Single channel identity summary – live

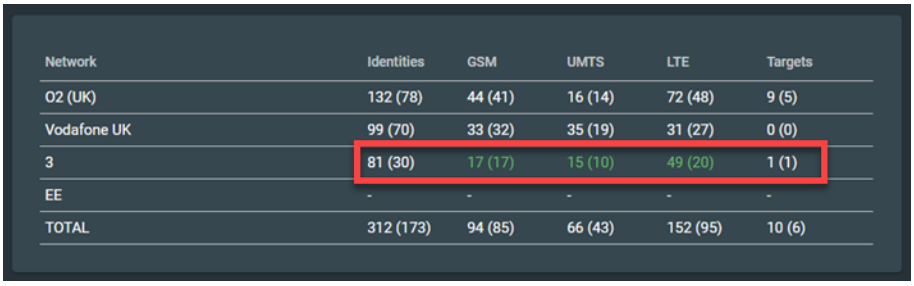
In the pane above the NESIE system is:

- Transmitting as the EE UMTS – identified by the green number
- Has found a total of 61 Identities with (50) unique identities

- On O2 (UK) the system has detected:
  - Total of 17 GSM identities, (13) of them unique
  - 5 GSM identities, (5) of them unique
  - 0 UMTS identities
  - 12 LTE identities, (8) of them unique
  - And has found 2 Targets, (1) unique identity

19.2.3.2 MULTI-CHANNEL NESIE

A multi-channel NESIE (3 Stack), transmitting on GSM, UMTS and LTE simultaneously is shown at Fig 165 below.

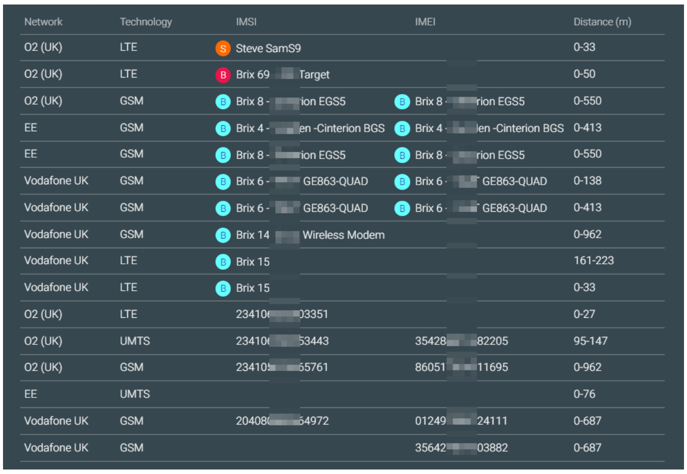


Network	Identities	GSM	UMTS	LTE	Targets
O2 (UK)	132 (78)	44 (41)	16 (14)	72 (48)	9 (5)
Vodafone UK	99 (70)	33 (32)	35 (19)	31 (27)	0 (0)
3	81 (30)	17 (17)	15 (10)	49 (20)	1 (1)
EE	-	-	-	-	-
TOTAL	312 (173)	94 (85)	66 (43)	152 (95)	10 (6)

Fig 165. Single channel identity summary – live

19.3 IDENTITY LIST

As the NESIE software rotates through the user defined network providers and technologies, the identity list will be displayed. As the Action commences, the pane will be refreshed and all previous identities will disappear from the screen.



Network	Technology	IMSI	IMEI	Distance (m)
O2 (UK)	LTE	S Steve SamS9		0-33
O2 (UK)	LTE	B Brix 69 [redacted] Target		0-50
O2 (UK)	GSM	B Brix 8 - [redacted] ion EGS5	B Brix 8 - [redacted] rion EGS5	0-550
EE	GSM	B Brix 4 - [redacted] en -Cinterion BGS	B Brix 4 - [redacted] len -Cinterion BGS	0-413
EE	GSM	B Brix 8 - [redacted] ion EGS5	B Brix 8 - [redacted] rion EGS5	0-550
Vodafone UK	GSM	B Brix 6 - [redacted] GE863-QUAD	B Brix 6 - [redacted] GE863-QUAD	0-138
Vodafone UK	GSM	B Brix 6 - [redacted] GE863-QUAD	B Brix 6 - [redacted] GE863-QUAD	0-413
Vodafone UK	GSM	B Brix 14 [redacted] Wireless Modem		0-962
Vodafone UK	LTE	B Brix 15		161-223
Vodafone UK	LTE	B Brix 15		0-33
O2 (UK)	LTE	23410[redacted]03351		0-27
O2 (UK)	UMTS	23410[redacted]53443	35428[redacted]82205	95-147
O2 (UK)	GSM	23410[redacted]65761	86051[redacted]11695	0-962
EE	UMTS			0-76
Vodafone UK	GSM	20408[redacted]54972	01249[redacted]24111	0-687
Vodafone UK	GSM		35642[redacted]03882	0-687

Fig 166. Identity list

The pane updates in real time with entries added to the top of the list. The pane displays the following data:

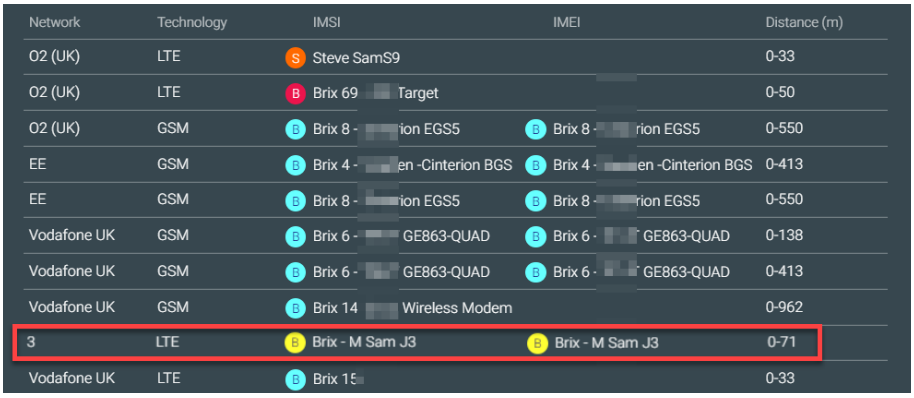
- **Network**
- **Technology**
- **IMSI**
- **IMEI**
- **Distance (M)**

If the captured identity has previously been annotated as a Target, a coloured tag will be shown next to the identity (in the colour that was added to the Target name). All Targets that are identified will be 'held' at the top of the table. This allows the operator to interrogate the information further if required without the Target identity scrolling down the table.

19.3.1 IDENTITY LIST DETAILS - IMSI

If required, the operator can investigate any captured identity further by clicking on the IMSI, IMEI shown on the identity list table. This will then take the user to a summary of information held within the database for that individual identity.

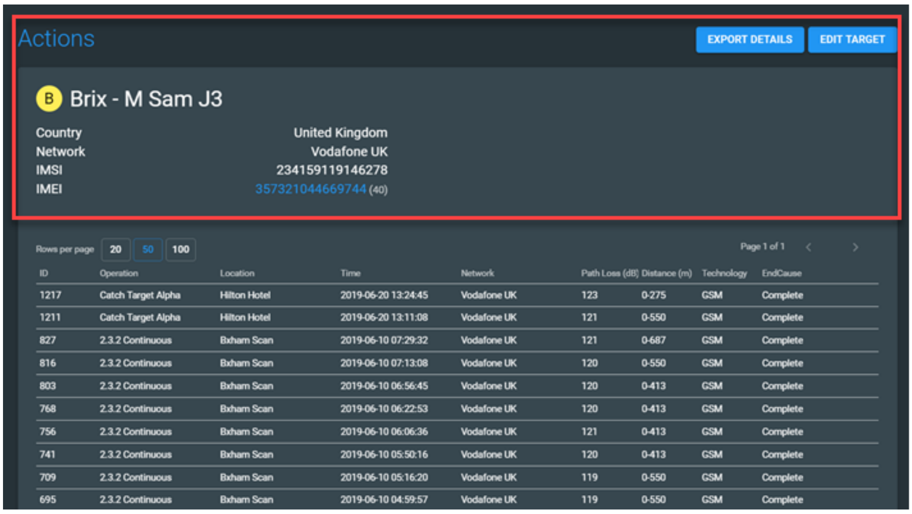
As shown in Fig 167 below, a Target B Brix - M Sam J3 has been captured. Both the IMEI and IMSI have been listed for the Target.



Network	Technology	IMSI	IMEI	Distance (m)
O2 (UK)	LTE	S Steve SamS9		0-33
O2 (UK)	LTE	B Brix 69 [redacted] Target		0-50
O2 (UK)	GSM	B Brix 8 - [redacted] ion EGS5	B Brix 8 - [redacted] rion EGS5	0-550
EE	GSM	B Brix 4 - [redacted] en -Cinterion BGS	B Brix 4 - [redacted] en -Cinterion BGS	0-413
EE	GSM	B Brix 8 - [redacted] ion EGS5	B Brix 8 - [redacted] rion EGS5	0-550
Vodafone UK	GSM	B Brix 6 - [redacted] GE863-QUAD	B Brix 6 - [redacted] GE863-QUAD	0-138
Vodafone UK	GSM	B Brix 6 - [redacted] GE863-QUAD	B Brix 6 - [redacted] GE863-QUAD	0-413
Vodafone UK	GSM	B Brix 14 [redacted] Wireless Modem		0-962
3	LTE	B Brix - M Sam J3	B Brix - M Sam J3	0-71
Vodafone UK	LTE	B Brix 15[redacted]		0-33

Fig 167. Target lists – details

If the user now clicks on the IMSI column of the Target row, he will be presented with the details of the Target IMSI as shown in Fig 168 below.



B Brix - M Sam J3

Country	United Kingdom
Network	Vodafone UK
IMSI	234159119146278
IMEI	357321044669744 (40)

ID	Operation	Location	Time	Network	Path Loss (dB)	Distance (m)	Technology	EndCause
1217	Catch Target Alpha	Hilton Hotel	2019-06-20 13:24:45	Vodafone UK	123	0-275	GSM	Complete
1211	Catch Target Alpha	Hilton Hotel	2019-06-20 13:11:08	Vodafone UK	121	0-550	GSM	Complete
827	2.3.2 Continuous	Bxham Scan	2019-06-10 07:29:32	Vodafone UK	121	0-687	GSM	Complete
816	2.3.2 Continuous	Bxham Scan	2019-06-10 07:13:08	Vodafone UK	120	0-550	GSM	Complete
803	2.3.2 Continuous	Bxham Scan	2019-06-10 06:56:45	Vodafone UK	120	0-413	GSM	Complete
768	2.3.2 Continuous	Bxham Scan	2019-06-10 06:22:53	Vodafone UK	120	0-413	GSM	Complete
756	2.3.2 Continuous	Bxham Scan	2019-06-10 06:06:36	Vodafone UK	121	0-413	GSM	Complete
741	2.3.2 Continuous	Bxham Scan	2019-06-10 05:50:16	Vodafone UK	120	0-413	GSM	Complete
709	2.3.2 Continuous	Bxham Scan	2019-06-10 05:16:20	Vodafone UK	119	0-550	GSM	Complete
695	2.3.2 Continuous	Bxham Scan	2019-06-10 04:59:57	Vodafone UK	119	0-550	GSM	Complete

Fig 168. Identity details - IMSI

The identity details page shows the following information in the header:

- Name of Target & Colour Icon
- Country — Home country - extracted from the MCC in the IMSI
- Network — Home network - extracted from the MNC in the IMSI
- IMSI — The IMSI of the ID chosen
- IMEI (in Blue) — The IMEI associated with this IMSI is displayed
- (No in Brackets) — The total number of times IMEI captured in the database
- EXPORT DETAILS — Download the data shown on the screen as .CSV
- EDIT TARGET — Edit the details for the Target

NOTE: In this screen, the IMEI is shown in blue. This indicates that the operator can click this number. The screen will then display the database entries for this IMEI.

The table at the lower portion of the identity details page shows the following information:

ID	A serial/line number allocated to each capture in the database
Operation	The name of the operation the ID was captured in
Location	The name of the location that the ID was captured in
Time	DTG of the capture
Network	The network NESIE was transmitting when captured
Path Loss	Strength of the signal from the mobile device when detected
Distance	The calculated distance from the NESE to the mobile device
Technology	The technology that the ID was captured on

19.3.1.1 EXPORT DETAILS

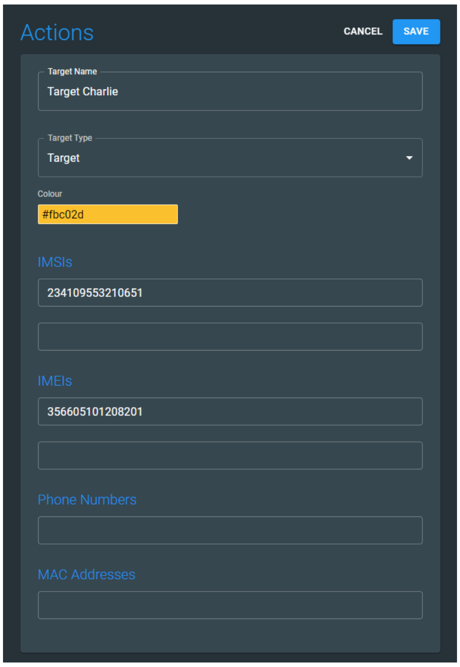
If required, the operator has the option to export the details shown on this screen.

The EXPORT DETAILS button, can be found at the top of the identity details page, as shown in Fig 168 above. Exporting the details will download all the data displayed on the screen to the operator's laptop as a CSV file. This file can then be interrogated using a suitable programme (Microsoft XL) or imported to external analysis software.

The data is usually saved in the downloads folder on the laptop/PC and is saved in the .CSV format.

19.3.1.2 EDIT TARGET

If required, the operator can edit the current details that are saved for this Target. Pressing the EDIT TARGET button. The Target page will open as shown below in Fig 169.



Target Name: Target Charlie

Target Type: Target

Colour: #fbc02d

IMSIs: 234109553210651

IMEIs: 356605101208201

Phone Numbers

MAC Addresses

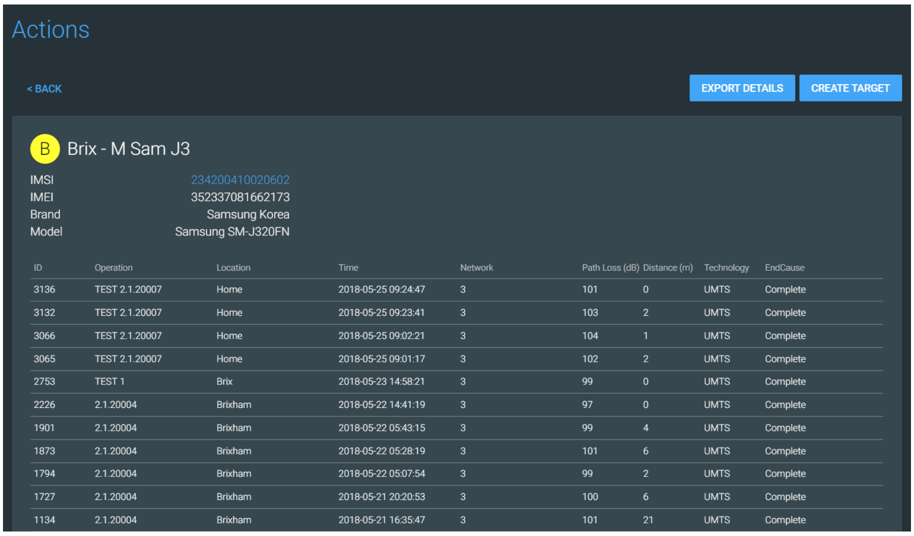
Fig 169. Edit Target

A detailed description of the Edit Target pane is at section 20.5.

19.3.2 IDENTITY LIST DETAILS - IMEI

If the operator chooses to interrogate a chosen identity by IMEI, they can select the IMEI using the process previously described in Section 19.3.1 above.

When the IMEI is selected from the table, the page displayed at Fig 170 below is shown. This page is like the one discussed above, however the details of the IMEI will be displayed:



B Brix - M Sam J3

IMSI	234200410020602
IMEI	352337081662173
Brand	Samsung Korea
Model	Samsung SM-J320FN

ID	Operation	Location	Time	Network	Path Loss (dB)	Distance (m)	Technology	EndCause
3136	TEST 2.1.20007	Home	2018-05-25 09:24:47	3	101	0	UMTS	Complete
3132	TEST 2.1.20007	Home	2018-05-25 09:23:41	3	103	2	UMTS	Complete
3066	TEST 2.1.20007	Home	2018-05-25 09:02:21	3	104	1	UMTS	Complete
3065	TEST 2.1.20007	Home	2018-05-25 09:01:17	3	102	2	UMTS	Complete
2753	TEST 1	Brix	2018-05-23 14:58:21	3	99	0	UMTS	Complete
2226	2.1.20004	Brixham	2018-05-22 14:41:19	3	97	0	UMTS	Complete
1901	2.1.20004	Brixham	2018-05-22 05:43:15	3	99	4	UMTS	Complete
1873	2.1.20004	Brixham	2018-05-22 05:28:19	3	101	6	UMTS	Complete
1794	2.1.20004	Brixham	2018-05-22 05:07:54	3	99	2	UMTS	Complete
1727	2.1.20004	Brixham	2018-05-21 20:20:53	3	100	6	UMTS	Complete
1134	2.1.20004	Brixham	2018-05-21 16:35:47	3	101	21	UMTS	Complete

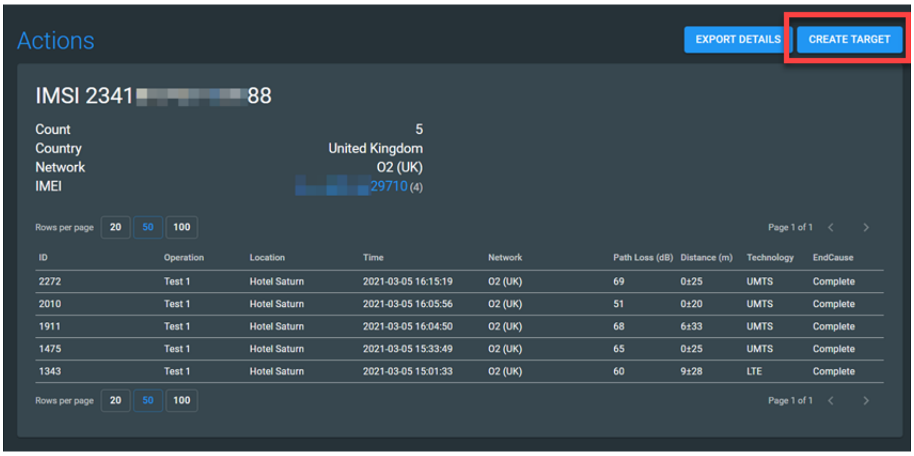
Fig 170. Identity details – IMEI

• Name of Target & Colour Icon	
• IMSI (In Blue)	The IMSI of the ID chosen
• IMEI	The IMEI associated with this IMSI is displayed
• Brand	Brand of device – extracted from the IMEI
• Model	Model of device – extracted from the IMEI
• EXPORT DETAILS	Download the data shown on the screen as .CSV
• EDIT TARGET	Edit the details for the Target

The identity details table shows the same information as that shown in IMSI table shown in Fig 168 above.

19.4 CREATE TARGET

As soon as an IMEI and / or an IMSI has been identified as a Target, the operator can add them into the Target List. The CREATE TARGET button appears every time the identity details are interrogated as shown in Fig 171 below.



IMSI 2341[redacted]88

Count	5
Country	United Kingdom
Network	O2 (UK)
IMEI	[redacted]29710 (4)

Rows per page 20 50 100 Page 1 of 1

ID	Operation	Location	Time	Network	Path Loss (dB)	Distance (m)	Technology	EndCause
2272	Test 1	Hotel Saturn	2021-03-05 16:15:19	O2 (UK)	69	0±25	UMTS	Complete
2010	Test 1	Hotel Saturn	2021-03-05 16:05:56	O2 (UK)	51	0±20	UMTS	Complete
1911	Test 1	Hotel Saturn	2021-03-05 16:04:50	O2 (UK)	68	6±33	UMTS	Complete
1475	Test 1	Hotel Saturn	2021-03-05 15:33:49	O2 (UK)	65	0±25	UMTS	Complete
1343	Test 1	Hotel Saturn	2021-03-05 15:01:33	O2 (UK)	60	9±28	LTE	Complete

Rows per page 20 50 100 Page 1 of 1

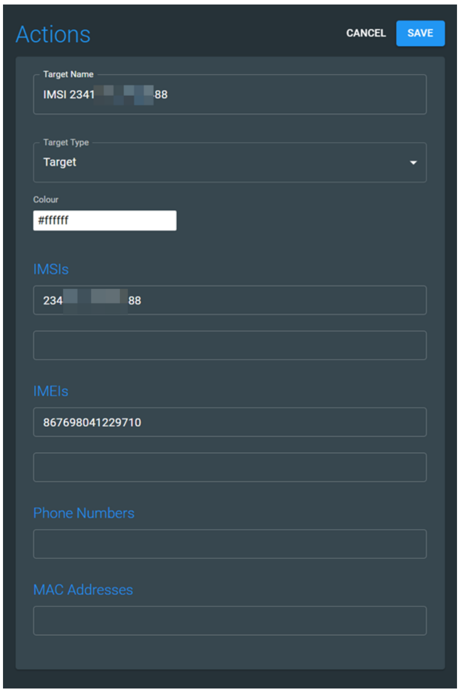
Fig 171. CREATE TARGET

19.5 EDIT TARGET PAGE

When the operator presses the CREATE TARGET button, the Edit Target page is shown as per Fig 172 below. As this page opens, the Chosen ID (in this case the IMSI) has been automatically added to the Target Name field, by default, the IMSI ************ will be shown. If the IMEI had been selected, the default Target name IMEI************ would be used.

The operator now has the option to edit the Target Name, Target type, and Target Colour Icon.

NOTE: Whilst adding an IMSI to the Target list and an IMEI has been found, both will be added to the Target unless the operator wishes to delete the details.



Target Name: IMSI 2341[redacted]88

Target Type: Target

Colour: #ffffff

IMSIs: 234[redacted]88

IMEIs: 867698041229710

Phone Numbers

MAC Addresses

Fig 172. Edit Target

When the details are correctly entered, the operator should press the SAVE button.

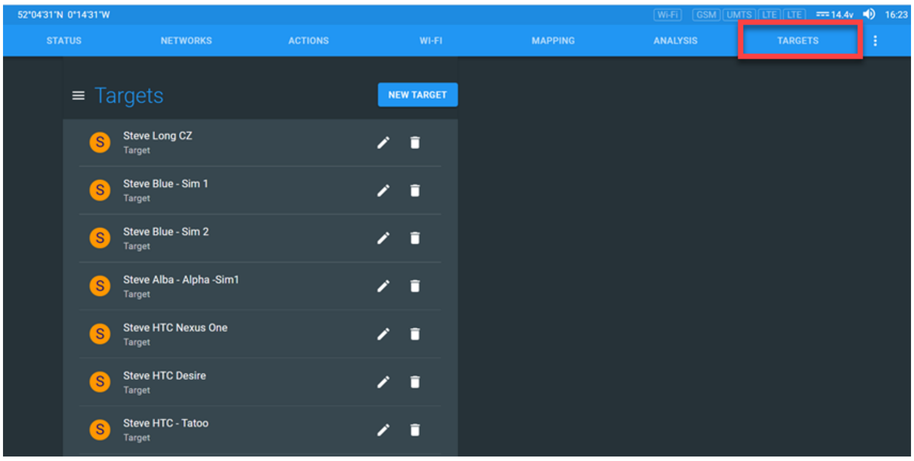
The newly created Target has now been added to the Target List and will be shown as a Target every time that the IMSI and/or IMEI are found. This will also apply to the last ID Grab.

To display the newly created Target in the last ID Grab, the user must navigate back to the summary page. This can either be done by using the back button on the UI, the web browser back button, or by pressing the ACTIONS button on the menu bar.

The UI will should automatically refresh, however on occasion, it may need to be refreshed manually. By refreshing the page, the NESIE system will apply the new Target details to the data in the last Grab list and the new Target will be shown in the UI.

20. TARGETS

The operator has the option to view, edit or manually add details to the Target List at any time. The page can be opened by using the TARGETS button as shown at Fig 173 below. When pressed, the list of Targets that have been created or imported to the NESIE system will be displayed.



S Steve Long CZ
Target

S Steve Blue - Sim 1
Target

S Steve Blue - Sim 2
Target

S Steve Alba - Alpha -Sim1
Target

S Steve HTC Nexus One
Target

S Steve HTC Desire
Target

S Steve HTC - Tatoo
Target

Fig 173. Target list

The Targets list consists of the following data:

① Target Icon	A coloured circle as chosen by the user. The digit displayed in the circle is the first letter of Target name
Target Name	The name given to the Target by the user
Type	Type of list the Identity has been added to
✎	Edit Target
🗑	Delete the Target

20.1 TARGET TYPES

There are four types of Target lists that are used in the NESIE system:

- Target
- Whitelist
- Disabled
- SAR Target

20.1.1 TARGET

A list of identities that have been linked to a Target. The Target is given a name and a coloured icon that will be displayed in the UI whenever these identities are detected by NESIE.

These identities may have been collected with the NESIE system or passed from other intelligence sources.

There is no limit to the number of Targets in the list or the number of individual identities in each of the IMEI, IMSI, mobile device number or MAC fields.

20.1.2 WHITELIST

The whitelist is a list of identities that will not be displayed when captured by NESIE. This list is usually made up with IMEIs and IMSIs of the NESIE operators, supporting forces and other likely unit personnel.

NESIE will capture the whitelist identities during its normal operation, however, when the identities are checked against the Target and Whitelist, they will be identified as part of the Whitelist and not displayed on the current views of the UI.

The whitelist identities are still entered into the database and can be viewed / downloaded if required.

20.1.3 DISABLED TARGETS

Disabled Targets are identities that have been temporarily taken out of the Target list. This allows an operation to be conducted and ensures ‘non required’ Targets are not shown on the UI.

20.1.4 SEARCH AND RESCUE (SAR) TARGET

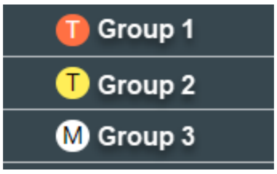
This allows the operator to save a Target in the NESIE software, then switch the software from NESIE to the SAR software. The Targets saved in this list will now be visible in the SAR Software. All others (Target, White or Disabled) will not be visible.

NOTE: If a Target is entered into the NESIE software as a Target, then the software is swapped into SAR mode and then the operator attempts to put the same identity into the SAR software, a conflict will arise and the identity will be rejected.

In this instance, the SAR Target should be used.

20.2 TARGET COLOUR – GROUPS

When adding a Target to the Target list, the operator can choose which colour icon is allocated to each Target. Using this feature, the operator can create Target groups. For example, Criminal Group 1 can be allocated an Orange Icon, Criminal Group 2 the Yellow icon and Criminal Group 3 the White Icon.



T Group 1

T Group 2

M Group 3

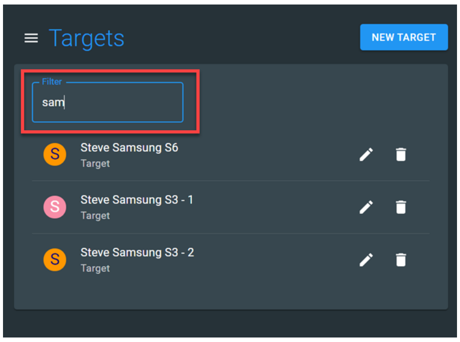
Fig 174. Colour icons / groups

20.3 ADD NEW TARGET

To add a new Target to the Target list, the operator should press the NEW TARGET button. A blank Target details page will be displayed. To add the details, the operator should follow the instructions at the Section below.

20.4 FILTER TARGETS

If required, the operator can filter the Target list to present a shortened list. As shown below in Fig 175, when the operator types into the Filter section, the Target list will dynamically update to show all those Targets containing the typed letters.



Filter: sam

S Steve Samsung S6
Target

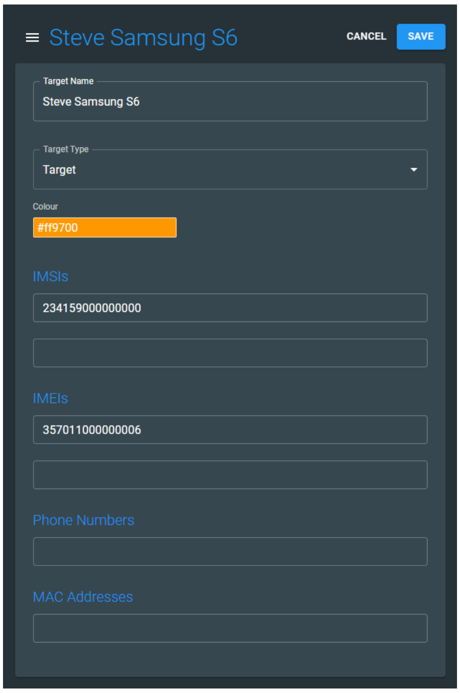
S Steve Samsung S3 - 1
Target

S Steve Samsung S3 - 2
Target

Fig 175. Targets – Filter

20.5 EDIT TARGET

To edit the details of the Target, the operator should click on EDIT icon ✎ next to the desired Target name. The individual Target entry page will be displayed as shown Fig 176 below.



Target Name: Steve Samsung S6

Target Type: Target

Colour: #ff9700

IMSIs: 234159000000000

IMEIs: 357011000000006

Phone Numbers

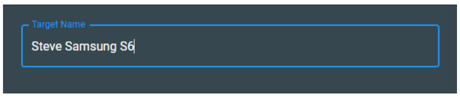
MAC Addresses

Fig 176. Edit Target

The Target list consists of the following fields:

• Target Name	Name to be displayed
• Target Type	Target list, Whitelist or Disabled
• Colour	Colour of identifier icon
• IMSIs	IMSI currently or previously used by Target
• IMEIs	IMEI currently or previously used by Target
• Device Numbers	Device numbers linked to Target
• MAC Address	MAC Address associated with Target

If the operator clicks onto a field, it will be shown as active by a blue box as per Fig 177 below.



Target Name: Steve Samsung S6

Fig 177. Edit Field

20.5.1 TARGET NAME

Type the Target name into this field to a maximum of 30 characters.

20.5.2 TARGET TYPE

Using the drop-down menu, the operator has the option to add the identity to the Target List, Whitelist, Disable the ID from all lists or add to the SAR Target list, as shown in Fig 178 below.

- Target	Adds the Identity to the Target List
- Whitelist	Adds the identity to the Whitelist
- Disabled	Disables the ID from all lists
- SAR Target	Add Target to SAR list and make available in the ARTEMIS software

The current list shown by the grey bar as shown in Fig 178 below.

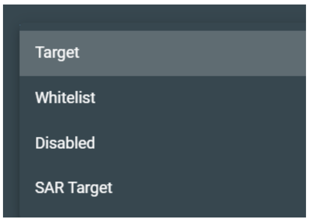
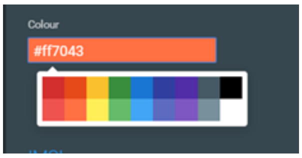


Fig 178. Target type

20.5.3 TARGET COLOUR

The colour of the identifier shown in the Target list can be selected. By default, the colour is set to White. If the operator wishes to adjust the colour, they should click on the colour bar. his action will display the colour picker as shown in Fig 179 below.



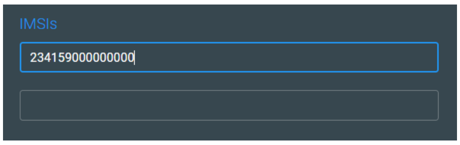
Colour
#ff7043

Fig 179. Target colour

By clicking on the desired colour, the coloured bar will change, and the picker will close. The digits displayed in the colour picker are the hexadecimal reference for that colour.

20.5.4 IMSI

Previously saved IMSIs will be displayed, and an additional blank box will be displayed below. This blank box allows another IMSI to be entered. If the operator enters a second IMSI, another box will automatically appear below, allowing an unlimited number of IDs to be entered. The operator has the option to manually enter or cut / paste additional identities to the Target. The IMSI field **must** contain 15 digits. There is no limit to the number of IMSIs that can be associated with a Target. The IMSI field is shown in Fig 180 below.



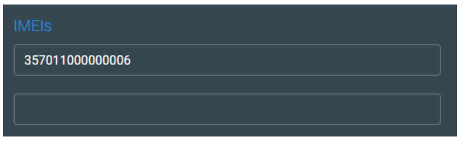
IMSIs

234159000000000

Fig 180. Add IMSI

20.5.5 IMEI

If previous IMEIs exist for this Target, they will be listed. An additional blank box is displayed below and this allows the operator to manually type in the new IMEI as shown in Fig 181 below. If the operator enters a second IMEI a third box will automatically appear below, allowing an unlimited number of IDs to be entered.



IMEIs

357011000000006

Fig 181. Add IMEI

20.5.6 PHONE NUMBERS

If required, phone numbers associated with the Target can be manually entered into this field as shown below at Fig 182.

If during Hold, Deny, of Broadcast SMS operations, that number is transmitted by a cellular device that can be detected by NESIE, it will be flagged as belonging to this Target.

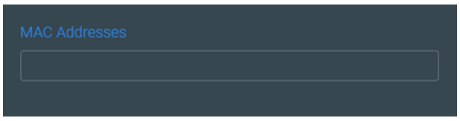
Phone Numbers

Fig 182. Add device numbers

NOTE: The NESIE system cannot extract phone numbers from a Target device as these are not sent over the air.

20.5.7 MAC ADDRESSES

When using the Wi-Fi sniffer module that is fitted to some NESIE systems to collect MAC address data, the NESIE system can ‘alarm’ when a MAC address of interest is captured. Like an IMEI and IMSI, a MAC Address can be entered into the Target list and used to identify a Target.



MAC Addresses

Fig 183. Device Numbers & MAC Addresses

20.5.8 SAVE / CANCEL

To save the edited data the operator should press the SAVE button.

If an error has been made or if the operator wishes to cancel the changes, they can press the CANCEL button.

20.6 TARGETS – SUB MENU

By pressing the ≡ sub menu button on the Targets page, the operator will be presented with a drop-down menu. This drop-down menu will allow the operator to Export, Import or Clear the Target list. The drop-down menu is shown below at Fig 184.

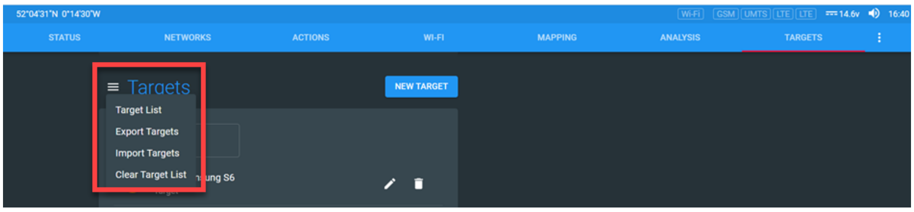


Fig 184. Targets – sub menu

20.6.1 EXPORT TARGETS

If required, an operator can export the current Target List. This could then be transferred to another NESIE system, added to another intelligence database, or opened in Microsoft XL, edited and re imported.

To export the Target List, click the Export Targets button. A Comma Separated Value (CSV) file will be created and downloaded to the laptop / tablet that is being used to control the NESIE, as shown in Fig 185 below.

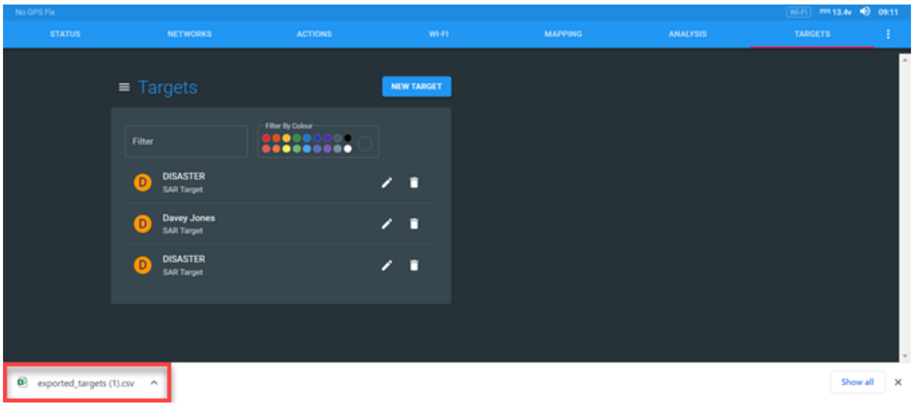
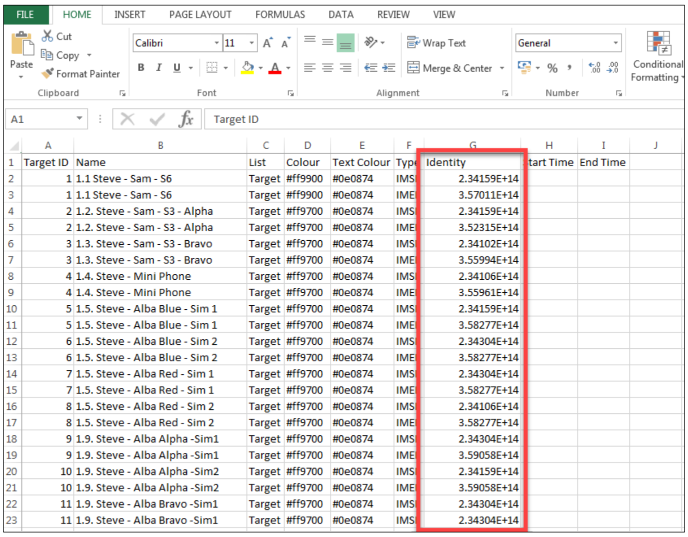


Fig 185. Target list – downloaded

Every exported Target list will be given a default name of **exported_Targets.csv**. If other exported Target lists already exist, a one up number **(1)** will be added. The user should change this file name if required.

20.6.2 OPENING EXPORTED TARGETS IN EXCEL

To open the exported Target List, the operator can click on the downloaded file. By default, the Target list will be opened in Microsoft XL (or similar depending on what is installed on the computer). However, because the exported file is created as a Comma Separated Value (.CSV) file it will be opened without being formatted correctly. As show in Fig 186 below, you can see the Identity column (IMEI or IMSI) is displayed incorrectly.

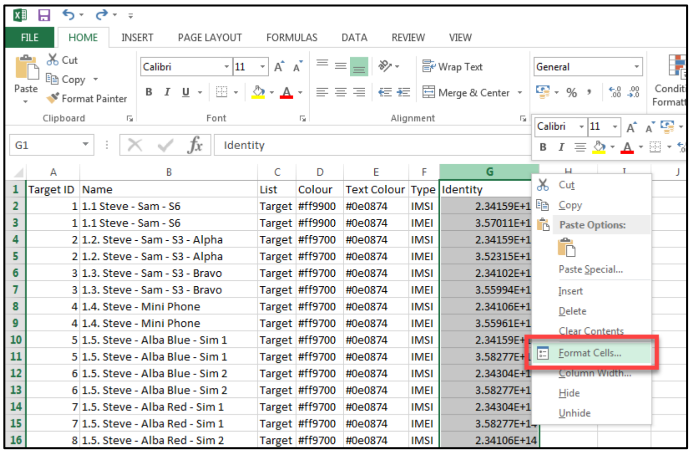


	A	B	C	D	E	F	G	H	I	J
1	Target ID	Name	List	Colour	Text Colour	Typ	Identity	tart Time	End Time	
2	1	1.1 Steve - Sam - S6	Target	#ff9900	#0e0874	IMS	2.34159E+14			
3	1	1.1 Steve - Sam - S6	Target	#ff9900	#0e0874	IME	3.57011E+14			
4	2	1.2. Steve - Sam - S3 - Alpha	Target	#ff9700	#0e0874	IMS	2.34159E+14			
5	2	1.2. Steve - Sam - S3 - Alpha	Target	#ff9700	#0e0874	IME	3.52315E+14			
6	3	1.3. Steve - Sam - S3 - Bravo	Target	#ff9700	#0e0874	IMS	2.34102E+14			
7	3	1.3. Steve - Sam - S3 - Bravo	Target	#ff9700	#0e0874	IME	3.55994E+14			
8	4	1.4. Steve - Mini Phone	Target	#ff9700	#0e0874	IMS	2.34106E+14			
9	4	1.4. Steve - Mini Phone	Target	#ff9700	#0e0874	IME	3.55961E+14			
10	5	1.5. Steve - Alba Blue - Sim 1	Target	#ff9700	#0e0874	IMS	2.34159E+14			
11	5	1.5. Steve - Alba Blue - Sim 1	Target	#ff9700	#0e0874	IME	3.58277E+14			
12	6	1.5. Steve - Alba Blue - Sim 2	Target	#ff9700	#0e0874	IMS	2.34304E+14			
13	6	1.5. Steve - Alba Blue - Sim 2	Target	#ff9700	#0e0874	IME	3.58277E+14			
14	7	1.5. Steve - Alba Red - Sim 1	Target	#ff9700	#0e0874	IMS	2.34304E+14			
15	7	1.5. Steve - Alba Red - Sim 1	Target	#ff9700	#0e0874	IME	3.58277E+14			
16	8	1.5. Steve - Alba Red - Sim 2	Target	#ff9700	#0e0874	IMS	2.34106E+14			
17	8	1.5. Steve - Alba Red - Sim 2	Target	#ff9700	#0e0874	IME	3.58277E+14			
18	9	1.9. Steve - Alba Alpha -Sim1	Target	#ff9700	#0e0874	IMS	2.34304E+14			
19	9	1.9. Steve - Alba Alpha -Sim1	Target	#ff9700	#0e0874	IME	3.59058E+14			
20	10	1.9. Steve - Alba Alpha -Sim2	Target	#ff9700	#0e0874	IMS	2.34159E+14			
21	10	1.9. Steve - Alba Alpha -Sim2	Target	#ff9700	#0e0874	IME	3.59058E+14			
22	11	1.9. Steve - Alba Bravo -Sim1	Target	#ff9700	#0e0874	IMS	2.34304E+14			
23	11	1.9. Steve - Alba Bravo -Sim1	Target	#ff9700	#0e0874	IMS	2.34304E+14			

Fig 186. Target list – automatically opens

The user can now save this file in its raw .CSV format or change the formatting and save the file as in .XL format.

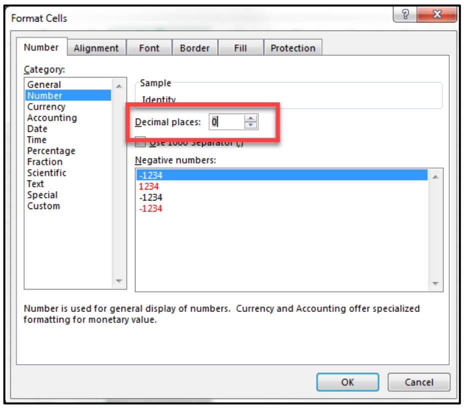
To change the format of the identity column, the user should select the required column, as shown in Fig 187 below. Then right click and select Format Cells.



	A	B	C	D	E	F	G
1	Target ID	Name	List	Colour	Text Colour	Type	Identity
2	1	1.1 Steve - Sam - S6	Target	#ff9900	#0e0874	IMSI	2.34159E+1
3	1	1.1 Steve - Sam - S6	Target	#ff9900	#0e0874	IMEI	3.57011E+1
4	2	1.2. Steve - Sam - S3 - Alpha	Target	#ff9700	#0e0874	IMSI	2.34159E+1
5	2	1.2. Steve - Sam - S3 - Alpha	Target	#ff9700	#0e0874	IMEI	3.52315E+1
6	3	1.3. Steve - Sam - S3 - Bravo	Target	#ff9700	#0e0874	IMSI	2.34102E+1
7	3	1.3. Steve - Sam - S3 - Bravo	Target	#ff9700	#0e0874	IMEI	3.55994E+1
8	4	1.4. Steve - Mini Phone	Target	#ff9700	#0e0874	IMSI	2.34106E+1
9	4	1.4. Steve - Mini Phone	Target	#ff9700	#0e0874	IMEI	3.55961E+1
10	5	1.5. Steve - Alba Blue - Sim 1	Target	#ff9700	#0e0874	IMSI	2.34159E+
11	5	1.5. Steve - Alba Blue - Sim 1	Target	#ff9700	#0e0874	IMEI	3.58277E+
12	6	1.5. Steve - Alba Blue - Sim 2	Target	#ff9700	#0e0874	IMSI	2.34304E+1
13	6	1.5. Steve - Alba Blue - Sim 2	Target	#ff9700	#0e0874	IMEI	3.58277E+1
14	7	1.5. Steve - Alba Red - Sim 1	Target	#ff9700	#0e0874	IMSI	2.34304E+1
15	7	1.5. Steve - Alba Red - Sim 1	Target	#ff9700	#0e0874	IMEI	3.58277E+14
16	8	1.5. Steve - Alba Red - Sim 2	Target	#ff9700	#0e0874	IMSI	2.34106E+14

Fig 187. Target list – Format Cells

The Format Cells dialog box will now be shown as at Fig 188 below. The operator should now ensure the Number category and change the Decimal places to 0 and click OK**.**



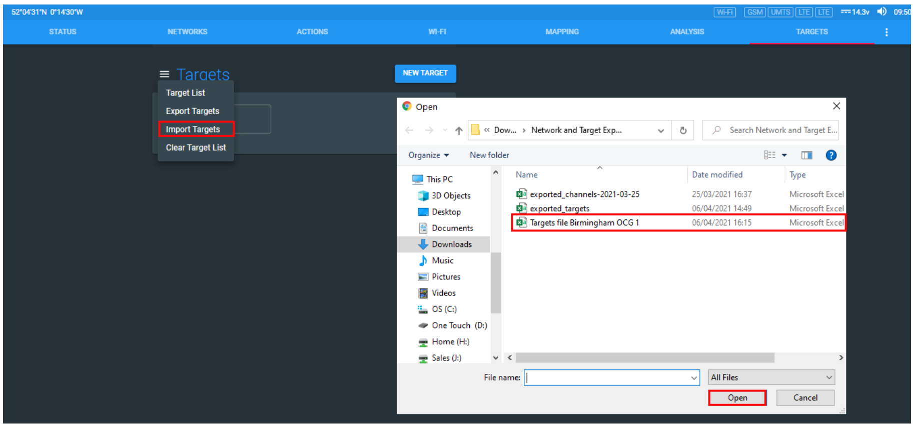
Decimal places: 0

Number is used for general display of numbers. Currency and Accounting offer specialized formatting for monetary value.

Fig 188. Target list - column settings

20.6.3 IMPORT TARGET LIST

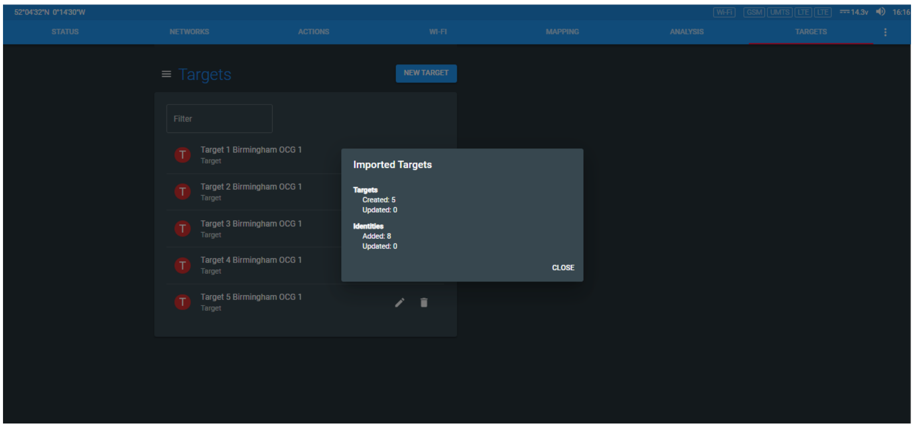
To import a pre saved Target list, the operator must press the Import Targets button from the drop-down. A windows dialogue box will pop up and the operator must navigate to the folder where the Target list file is stored. Once the required .CSV file is located, the operator must select it and click on Open in the bottom corner of the windows dialogue box as shown below in Fig 189.



Name	Date modified	Type
exported_channels-2021-03-25	25/03/2021 16:37	Microsoft Excel
exported_targets	06/04/2021 14:49	Microsoft Excel
Targets file Birmingham OCG 1	06/04/2021 16:15	Microsoft Excel

Fig 189. Import Target list

When the Target list has been imported, the dialogue box will disappear. Then the Target list will be shown along with a pop up Import Targets summary box as seen below in Fig 190. If there have been any errors encountered in the import, they will be shown in this summary box.



Target 1 Birmingham OCG 1
Target

Target 2 Birmingham OCG 1
Target

Target 3 Birmingham OCG 1
Target

Target 4 Birmingham OCG 1
Target

Target 5 Birmingham OCG 1
Target

Imported Targets

Targets
Created: 5
Updated: 0

Identities
Added: 8
Updated: 0

CLOSE

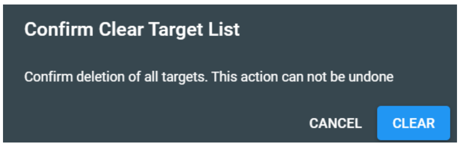
Fig 190. Imported Target list

NOTE: The file to be imported must be in .CSV format. If the file imported is in another format, or contains errors, the file will not be recognised and will not be loaded. Importing a Target list will overwrite any other Target list on the NESIE system.

20.6.4 CLEAR TARGET LISTS

If required, the operator can clear all entries on the Targets page, this includes the Whitelist, Disabled and SAR Targets list.

To clear the Targets list, the operator should click on the Clear Targets button. A dialogue box will appear asking the user to confirm deletion. Now click the CLEAs button to continue, as shown below in Fig 191 below.



Confirm Clear Target List

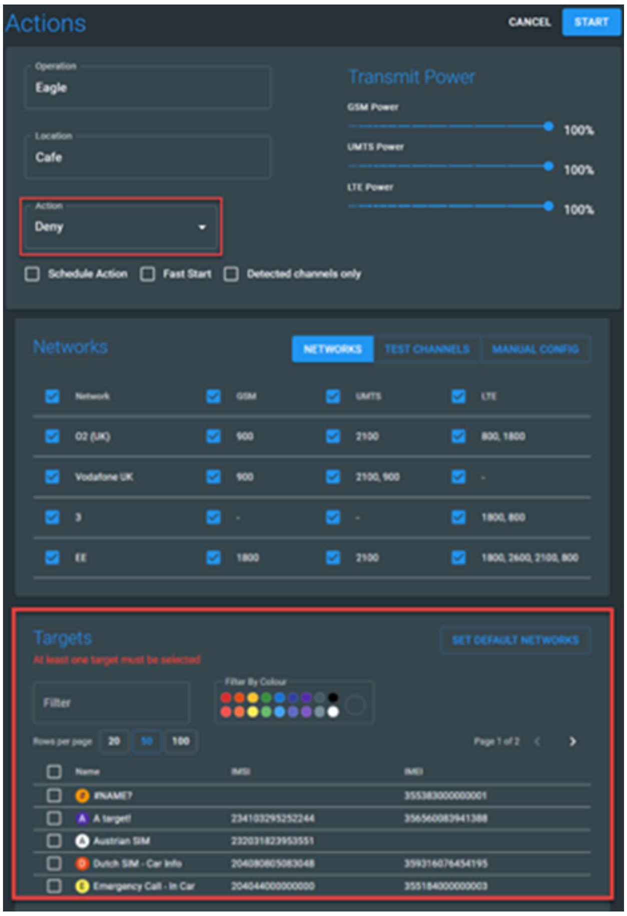
Confirm deletion of all targets. This action can not be undone

CANCEL CLEAR

Fig 191. Clear Target list – confirmation

21. TARGET SELECTION PANE

In some Actions, the operator may need to select a Target device to be interacted with. When the operator selects Hunt, Hold, Deny, Disable, Broadcast SMS or Redirect, an additional Targets pane will be displayed, as shown at the bottom of Fig 192 below.



Operation: Eagle

Location: Cafe

Action: Deny

GSM Power 100%

UMTS Power 100%

LTE Power 100%

☐ Schedule Action ☐ Fast Start ☐ Detected channels only

☑ Network	☑ GSM	☑ UMTS	☑ LTE
☑ O2 (UK)	☑ 900	☑ 2100	☑ 800, 1800
☑ Vodafone UK	☑ 900	☑ 2100, 900	☑ -
☑ 3	☑ -	☑ -	☑ 1800, 800
☑ EE	☑ 1800	☑ 2100	☑ 1800, 2600, 2100, 800

At least one target must be selected

Filter

☐	Name	IMSI	IMEI
☐	#NAME?		355383000000001
☐	A target!	234103295252244	356560083941388
☐	Austrian SIM	232031823953551	
☐	Dutch SIM - Car Info	204080805083048	359316076454195
☐	Emergency Call - In Car	204044000000000	355184000000003

Fig 192. Target selection pane

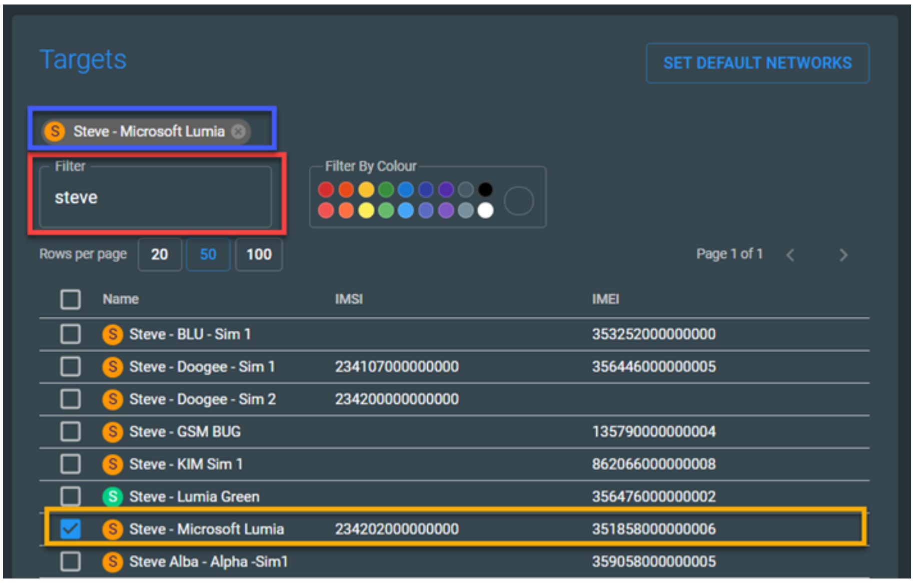
The Target selection pane consists of the following sections

- Filter
- Filter by colours
- Set Default Networks button
- All Targets tick box
- Target list

21.1 FILTER

If the operator types in any part of the Target name / identification into the Filter box, the Target list will dynamically change. As shown in Fig 193 below, the operator has typed STEVE in the filter box (Red). The list below dynamically changes to show all the Target names with STEVE in them. The operator has ticked one Target (yellow box). The selected Target is now added to the Targets (blue box).

If the operator has made a mistake, they can click the X next to the Target name (blue box) to remove it from the Targets list.



Filter: steve

□	Name	IMSI	IMEI
□	S Steve - BLU - Sim 1		353252000000000
□	S Steve - Doogee - Sim 1	234107000000000	356446000000005
□	S Steve - Doogee - Sim 2	234200000000000	
□	S Steve - GSM BUG		135790000000004
□	S Steve - KIM Sim 1		862066000000008
□	S Steve - Lumia Green		356476000000002
☑	S Steve - Microsoft Lumia	234202000000000	351858000000006
□	S Steve Alba - Alpha -Sim1		359058000000005

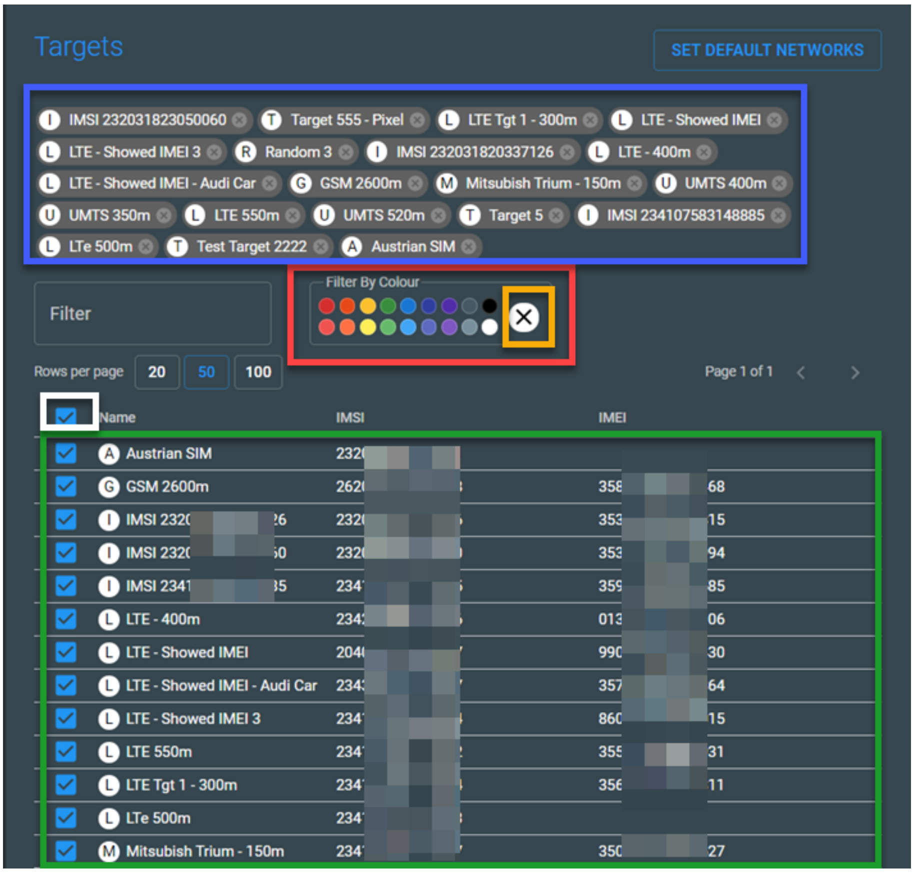
Fig 193. Target Selection – Filter

21.2 FILTER BY COLOUR

In the scenario seen below in Fig 194, the NESIE operator has selected the Targets by the colour picker (shown in the red box). The operator has selected the white colour circle (shown in the amber box). If required, the X can be pressed to delete this colour and another selected.

All Targets that have been tagged with a white icon are now displayed in the Target list (green box). The operator has then used the select all tick box (white box). The selected Targets are then displayed as selected Targets (blue box)

If required, multiple colours can be selected one at a time. The operator should choose the colour then select the Targets to be added to the list. Then select the second colour and add the Targets to the list.



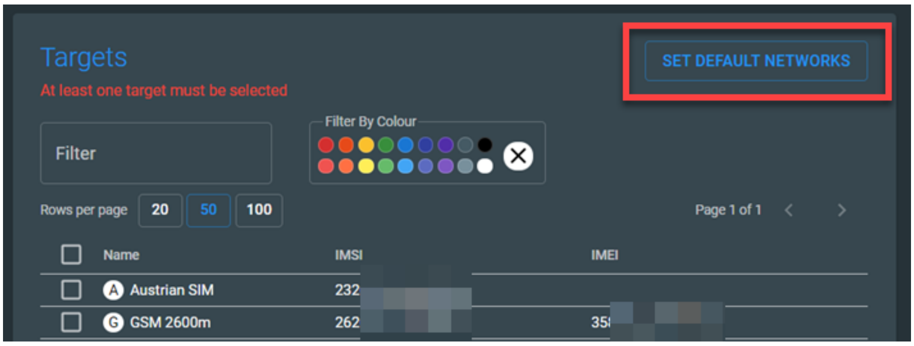
Targets

☑	Name	IMSI	IMEI
☑	Austrian SIM	232[redacted]	
☑	GSM 2600m	262[redacted]	358[redacted]68
☑	IMSI 232[redacted]26	232[redacted]	353[redacted]15
☑	IMSI 232[redacted]50	232[redacted]	353[redacted]94
☑	IMSI 2341[redacted]35	234[redacted]	359[redacted]85
☑	LTE - 400m	234[redacted]	013[redacted]06
☑	LTE - Showed IMEI	204[redacted]	990[redacted]30
☑	LTE - Showed IMEI - Audi Car	234[redacted]	357[redacted]64
☑	LTE - Showed IMEI 3	234[redacted]	860[redacted]15
☑	LTE 550m	234[redacted]	355[redacted]31
☑	LTE Tgt 1 - 300m	234[redacted]	356[redacted]11
☑	LTe 500m	234[redacted]	
☑	Mitsubish Trium - 150m	234[redacted]	350[redacted]27

Fig 194. Target selection – filter by colour

21.3 SET DEFAULT NETWORKS

When selecting a Target, the operator may need to choose which network(s) to carry out the actions (Grab, Hunt etc). Instead of the operator needing to remember network details or opening the Target list to check, he can press the Set Default Networks button as highlighted in the red box in Fig 195 below.



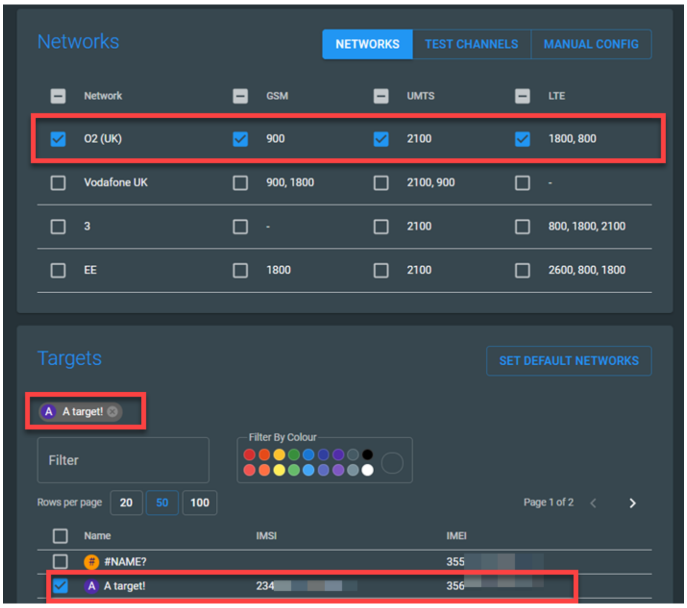
Targets

At least one target must be selected

☐	Name	IMSI	IMEI
☐	Austrian SIM	232[redacted]	
☐	GSM 2600m	262[redacted]	35[redacted]

Fig 195. Target selection – SET DEFAULT NETWORKS

When pressing the SET DEFAULT NETWORKS button, the NESIE software will examine the database to see what networks(s) the Target has been detected on and which network the SIM card is registered to. If the Target device has only ever been detected on one network provider for example O2(UK), the software will automatically select the O2(UK) network. All the other networks / technologies have been un-ticked as shown below in Fig 196.



☐ Network	☐ GSM	☐ UMTS	☐ LTE
☑ O2 (UK)	☑ 900	☑ 2100	☑ 1800, 800
☐ Vodafone UK	☐ 900, 1800	☐ 2100, 900	☐ -
☐ 3	☐ -	☐ 2100	☐ 800, 1800, 2100
☐ EE	☐ 1800	☐ 2100	☐ 2600, 800, 1800

☐ Name	IMSI	IMEI
☐ # #NAME?		355[redacted]
☑ A A target!	234[redacted]	356[redacted]

Fig 196 SET DEFAULT NETWORKS – network selected

If the selected Target uses several SIM cards from different networks, or has a roaming network SIM card, the software will choose multiple networks.

> **NOTE: Where multiple Targets across multiple networks are selected, the software will automatically select the required networks, this may result in ALL networks being selected.**

21.4 TARGET TYPE

In the Deny, Disable, Broadcast SMS and Redirect actions, an additional Target type pane will be displayed, as shown below in Fig 197. This pane now allows the operator to choose which type of Target to select:

21.4.1 ALL TARGETS

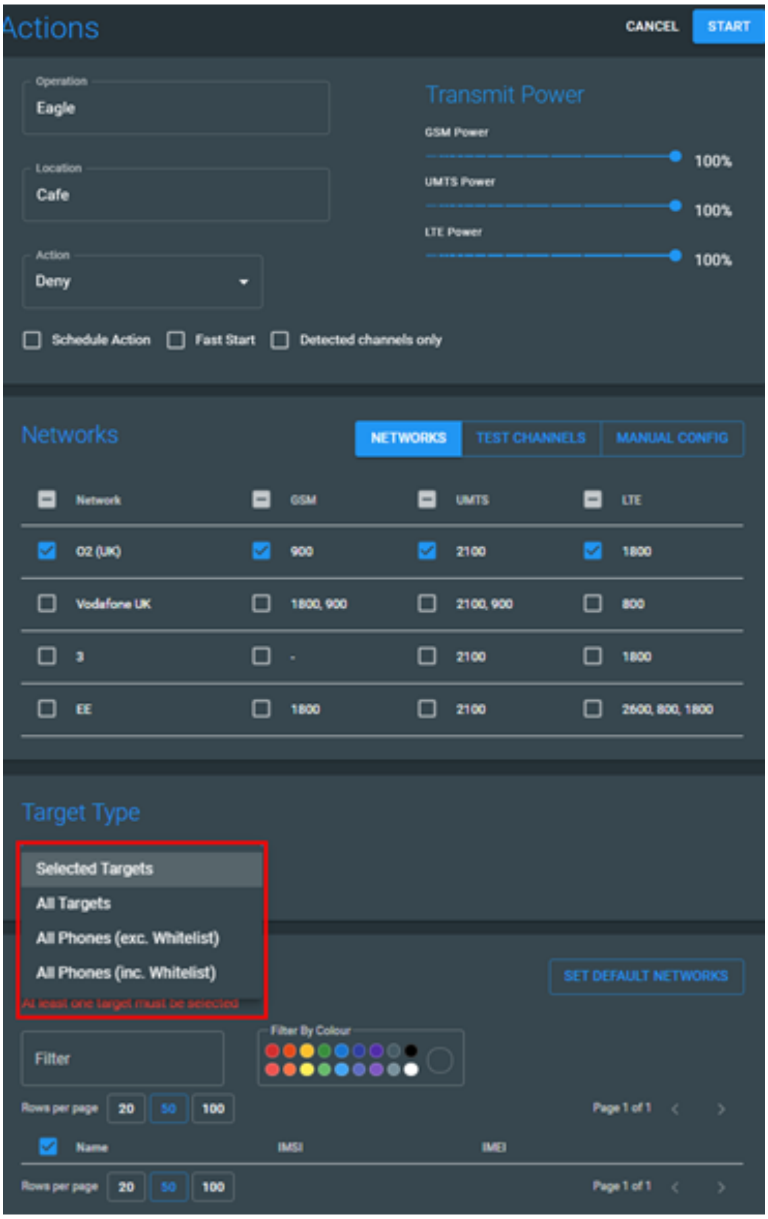
All Targets will automatically add all Targets to the selected Targets list. This is the same as manually pressing the All button or ticking each Target in the list.

21.4.2 ALL PHONES - EXCLUDING WHITELIST

This section allows the NESIE software to Target **ALL PHONES** even if they are not in the Target list. For example, you may want to Deny or Disable every device in range of the NESIE system. In this option, any devices that are already entered in the Whitelist will be detected and automatically released back to the real network.

21.4.3 ALL PHONES – INCLUDING WHITELIST

This option allows the NESIE software to Target **ALL PHONES,** even if they are not in the Target list. For example, you may want to Deny or Disable every device in range of the NESIE system. However, in this option it will automatically include any devices that are in the whitelist.



Actions

Operation: Eagle

Location: Cafe

Action: Deny

Transmit Power

GSM Power 100%

UMTS Power 100%

LTE Power 100%

□ Schedule Action □ Fast Start □ Detected channels only

Networks

☐ Network	☐ GSM	☐ UMTS	☐ LTE
☑ O2 (UK)	☑ 900	☑ 2100	☑ 1800
□ Vodafone UK	□ 1800, 900	□ 2100, 900	□ 800
□ 3	□ -	□ 2100	□ 1800
□ EE	□ 1800	□ 2100	□ 2600, 800, 1800

Target Type

- Selected Targets
- All Targets
- All Phones (exc. Whitelist)
- All Phones (inc. Whitelist)

At least one target must be selected

Fig 197. Target type pane

22. HUNT

The Hunt (for Target) mode should be used when the operator wants to check for the presence of a Target mobile device in an area. The NESIE system allows you to search all networks / technologies or restrict the search to known networks to speed up the Hunt process.

The Hunt is like a Grab, but the system is specifically searching for an individual identity or identities (IMSI/IMEI) as chosen for the operation.

NESIE will capture all cellular devices in the area and compare all the identities collected to those in the Target list chosen for this operation. When the **FIRST** listed Target is found, the NESIE will stop transmitting and stop the Hunt. An alarm will be sounded and the details of the **FIRST** Target identity detected will be shown.

Because this is a Hunt operation, the system will automatically continue switching through the chosen networks / technologies indefinitely.

By default, the NESIE system will complete one rotation through the networks / technologies (as selected by the operator) then turn off the transmitters to complete another network scan. This is to ensure the network scan data is still relevant and the NESIE has the best possible information. When the NESIE system is conducting a network scan during the Hunt action, a purple bar will be displayed.

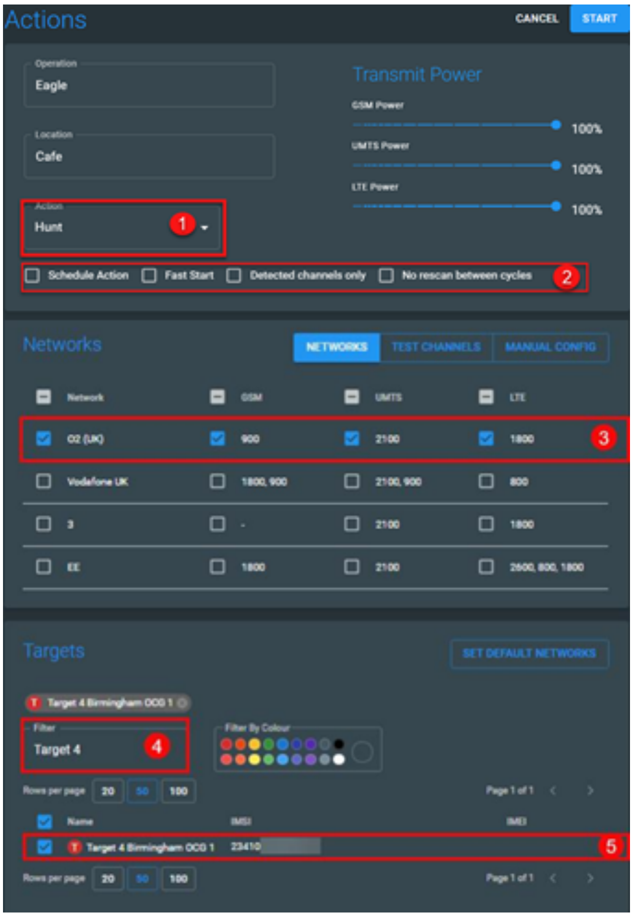
If required, the operator can force the NESIE system to ignore this network scan and restart transmitting immediately.

As previous discussed in the Target Selection Pane section, when the operator selects the Hunt action, an additional Targets selection pane will be displayed. The Targets selection pane allows the operator to add individual or multiple Target identities to the list of those to be flagged when found.

22.1 HUNT – SET UP

As shown in Fig 198. Hunt – set up below, the operator has followed the process:

- Navigated to the ACTIONS page
- Pressed the NEW ACTION button
- Chosen the Hunt Action from the Action drop-down menu – 1
- Adjust the Transmit Power if necessary
- Selected Fast Start / No Rescan between cycles etc - 2
- Selected technologies and networks - 3
- Filtered the Target list by ‘Target 4’ - 4
- Selected the desired Targets from the filtered Target list - 5



Actions

Operation: Eagle

Location: Cafe

Action: Hunt

□ Schedule Action □ Fast Start □ Detected channels only □ No rescan between cycles

Transmit Power

GSM Power: 100%

UMTS Power: 100%

LTE Power: 100%

Networks

Network	GSM	UMTS	LTE
☑ O2 (UK)	☑ 900	☑ 2100	☑ 1800
□ Vodafone UK	□ 1800, 900	□ 2100, 900	□ 800
□ 3	□ -	□ 2100	□ 1800
□ EE	□ 1800	□ 2100	□ 2600, 800, 1800

Targets

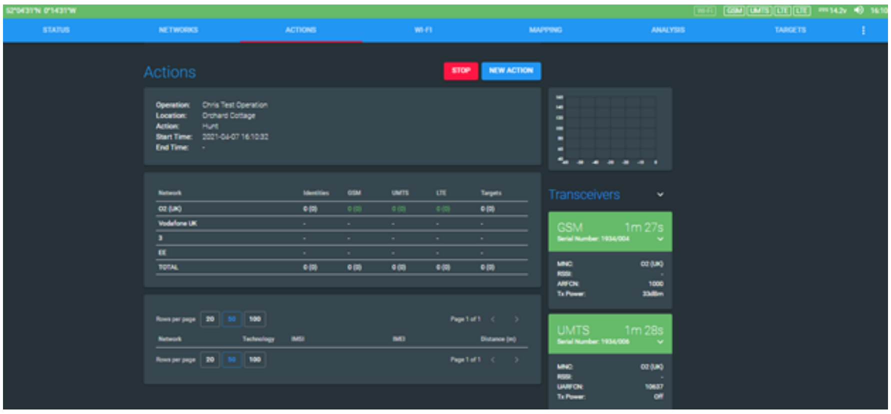
Filter: Target 4

Name	IMSI	IMEI
☑ Target 4 Birmingham OCG 1	23410[redacted]	

Fig 198. Hunt – set up

The operator should now click START button.

As previously discussed, when the operator presses the START button, the refreshed Actions summary screen will be shown, as displayed in Fig 199 below.



Actions

Operation: Chris Test Operation

Location: Orchard Cottage

Action: Hunt

Start Time: 2021-04-07 16:10:32

End Time: -

Network	Identities	GSM	UMTS	LTE	Targets
O2 (UK)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
Vodafone UK	-	-	-	-	-
3	-	-	-	-	-
EE	-	-	-	-	-
TOTAL	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)

Network	Technology	IMSI	IMEI	Distance (m)

Transceivers

GSM 1m 27s
Serial Number: 1934/004
MNC: O2 (UK)
RSSI: -
ARFCN: 1000
Tx Power: 33dBm

UMTS 1m 28s
Serial Number: 1934/006
MNC: O2 (UK)
RSSI: -
UARFCN: 10637
Tx Power: Off

Fig 199. Hunt – refreshed

The NESIE will now conduct a Hunt operation loOKing for the listed identities.

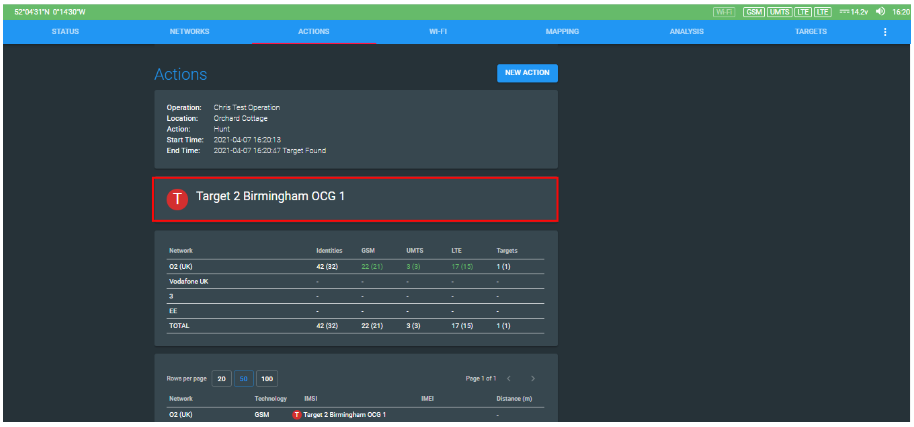
If No Rescan between cycles was selected, NESIE will complete 1 cycle through the chosen networks and technologies then start at the beginning again. This cycle will continue until the operator presses the STOP button.

If the operator did not tick the No Rescan Between Cycles option, the NESIE will complete one cycle, then carry out another Network Scan and when ready, start the Hunt process again. This cycle of Hunt and Network Scan will continue until the operator presses the STOP button.

22.2 HUNT – TARGET FOUND

The NESIE will now conduct a Hunt, transmitting the required signals to attract the cellular devices onto the NESIE BTS and extract the IMEIs and IMSIs. As soon as NESIE collects the first Target identity (as selected previously), an audible alarm will sound and a notification box will be displayed on the UI, as shown at Fig 200 below.

> **NOTE: When the first Target has been identified, NESIE will stop transmitting and resume the network scan phase. This will be identified by the green header bar reverting to blue.**



Operation: Chris Test Operation
Location: Orchard Cottage
Action: Hunt
Start Time: 2021-04-07 16:20:13
End Time: 2021-04-07 16:20:47 Target Found

T Target 2 Birmingham OCG 1

Network	Identities	GSM	UMTS	LTE	Targets
O2 (UK)	42 (32)	22 (21)	3 (3)	17 (15)	1 (1)
Vodafone UK	-	-	-	-	-
3	-	-	-	-	-
EE	-	-	-	-	-
TOTAL	42 (32)	22 (21)	3 (3)	17 (15)	1 (1)

Rows per page 20 50 100   Page 1 of 1

Network	Technology	IMSI	IMEI	Distance (m)
O2 (UK)	GSM	T Target 2 Birmingham OCG 1		-

Fig 200. Hunt - target found

22.3 AUDIBLE ALARM

If the operator is using a handheld device to control the NESIE system, it may not be desirable for the alarm to be sounded from this device. The operator can mute this alarm by clicking on the speaker icon on the header bar as shown in Fig 201 below.

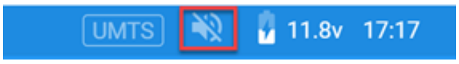


Fig 201. Alarm mute

23. HOLD – ADD BUGFINDER

The Hold action is initially a Grab, with the aim of detecting device identities, but searching for the Target mobile device(s). The IMSIs and IMEIs of non-Target cellular devices are logged and rejected back to the real network. When the Target or first of the pre-set Target list is found, it is moved off the real cellular network into a Hold.

To move the Target device from the real network, the device is sent a protocol message saying that the network (NESIE) wants to establish a phone call to the device. After this initial message, NESIE now sends a protocol message and moves the Target device from the normal (BCCH) channel and onto a specified traffic channel and establishes a 'silent call'.

The Targeted mobile device is now conducting a silent voice call to the NESIE system. The user is not aware of this silent call. When the call was established, the phone did not ring, vibrate, or display anything on the screen. During a silent call, no voice will be transmitted back to the NESIE System as the microphone cannot be activated.

Whilst the Target device is in a Hold, it is taken off the real network and is conducting a silent phone call to the NESIE system. Therefore, if any real calls or text messages are sent across the real network, they will not be sent to the Target device. When the Target device returns to the real network, the device will be told that they have missed calls and/or text messages will be sent.

This Hold Action could also be described as turning the Target device into a beacon – transmitting a signal. Whilst the Target device is transmitting as a beacon, additional Direction-Finding equipment can be utilised to geo-locate the mobile device. In some circumstances (2G), the operator also has the option to increase or decrease the transmit power of the mobile device. This can be used to aid the direction-finding operation.

CAUTION: ALTHOUGH THE USER IS NOT AWARE OF THE SILENT CALL BEING INITIATED BY THE HOLD OPERATION, THE NESIE OPERATOR MUST BE AWARE THAT BY MAKING THE MOBILE DEVICE PERMANENTLY TRANSMIT AT HIGH POWER, IT MAY DRAIN THE DEVICE BATTERY QUICKLY. THERE IS ALSO THE POSSIBILITY THAT THE BATTERY OF THE MOBILE DEVICE COULD GET WARM AS IT IS BEING USED AT FULL POWER.

NOTE: If the Target attempts to make a call during the Hold operation, they will see a 'network busy' message or similar. The voice call will not be possible as the device is already in a (silent) call to the NESIE system.

If the user attempts to sends an SMS whilst in Hold, the message will not be sent, and the user will get a warning to state message 'failed to send' or similar if supported by the mobile device.

23.1 HOLD - SINGLE CHANNEL SYSTEMS

It is possible to conduct Hold Actions/operations on a single channel NESIE system however, there will be limitations. A single channel NESIE system can only transmit on one technology at a time e.g. GSM then UMTS then LTE. Therefore, if the NESIE is commanded to Hold a Target device, it will search for the device on the technologies as programmed by the operator. If the NESIE detects the device on LTE it will attempt to Hold the device on LTE.

A single channel NESIE system cannot detect a device on LTE then Redirect the device down to another technology e.g. GSM. NESIE would have to Redirect the device then change the software from LTE to GSM, then transmit a GSM BTS to capture the Target device. Ideally, NESIE would have a minimum of 2 channels. This would provide the opportunity to detect the device on channel No1, then send a Redirect code. The second channel would be set up on a different technology ready to catch the device after it has been Redirected.

23.2 HOLD - MULTI CHANNEL SYSTEMS

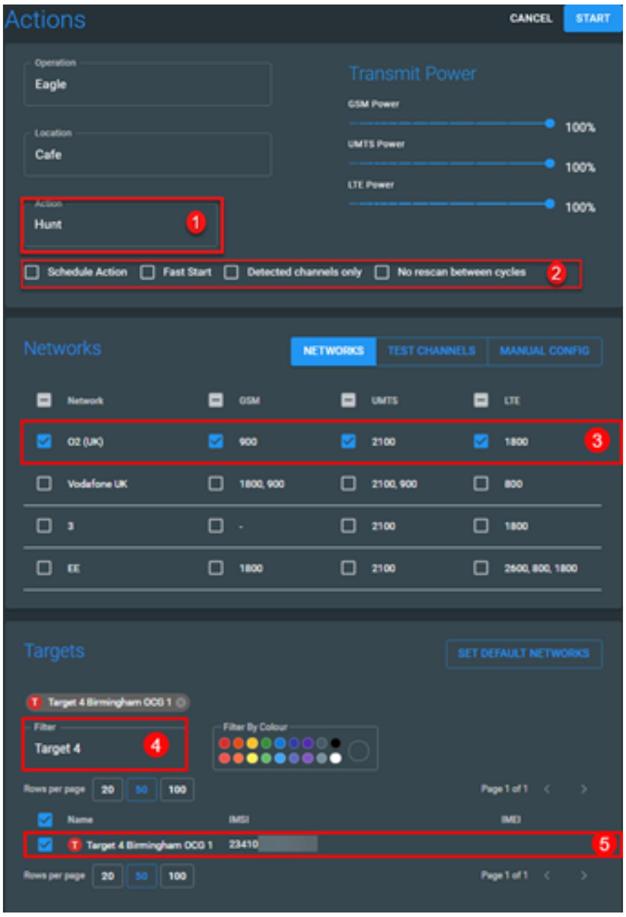
Ideally, the NESIE system would consist of at least 2 channels, as described above. If the system is made up from three or more channels, it is possible to conduct a Hold operation on all three technologies simultaneously (if the system has been configured to Hold using one channel per technology).

If there are more than 3 channels in the system, it is possible to Hold 1 Target device per channel. However, it must be remembered that the exact lay out of the transceiver's modules will depend on the technologies programmed e.g. (1 on GSM, 1 on UMTS and 3 modules on LTE)

23.3 HOLD – SET UP

The Hold process is initiated on the Actions page and is very similar to the previous Grab and Hunt processes. As shown in Fig 202 below the operator has followed the process below:

- ACTIONS page
- NEW ACTIONS button has been pressed
- Entered the Operation / Location Name
- Chosen the Hold action from the drop-down menu – 1
- Adjusted the Transmit Power if necessary
- Selected Fast Start, No Rescan etc buttons as required – 2
- Selected the networks and technologies required - 3
- Filtered the Target list by 'Target 4' – 4
- Ticked the required Target from the list – 5



Actions

CANCEL START

Operation: Eagle

Location: Cafe

Action: Hunt

Transmit Power

GSM Power 100%

UMTS Power 100%

LTE Power 100%

□ Schedule Action □ Fast Start □ Detected channels only □ No rescan between cycles

Networks

NETWORKS TEST CHANNELS MANUAL CONFIG

Network	GSM	UMTS	LTE
☑ O2 (UK)	☑ 900	☑ 2100	☑ 1800
□ Vodafone UK	□ 1800, 900	□ 2100, 900	□ 800
□ 3	□ -	□ 2100	□ 1800
□ EE	□ 1800	□ 2100	□ 2600, 800, 1800

Targets

SET DEFAULT NETWORKS

T Target 4 Birmingham OCG 1

Filter: Target 4

Filter By Colour

Rows per page 20 50 100 Page 1 of 1

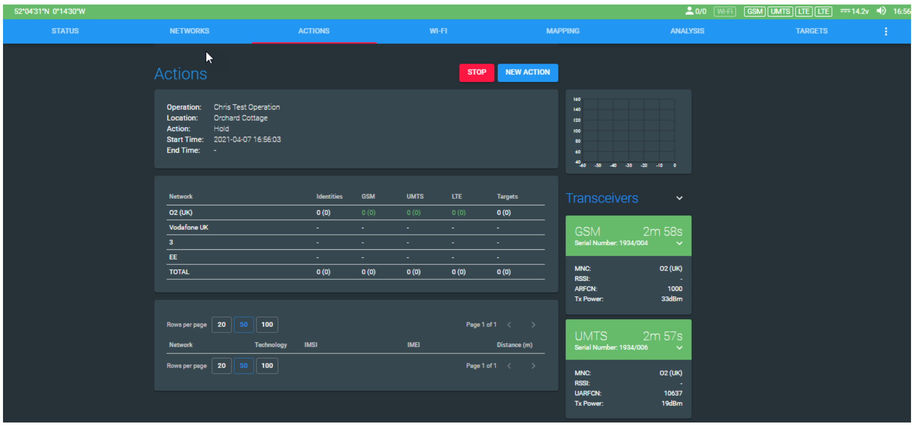
Name	IMSI	IMEI
☑ T Target 4 Birmingham OCG 1	23410[redacted]	

Rows per page 20 50 100 Page 1 of 1

Fig 202. Hold Action – set up

The operator should now click the START button.

As previously discussed, when the operator presses the START button, the refreshed Actions summary screen will be shown as shown in Fig 203 below.



52°04'31"N 0°14'30"W 0/0 Wi-Fi GSM UMTS LTE LTE 14.2v 16:56

STATUS NETWORKS ACTIONS WI-FI MAPPING ANALYSIS TARGETS

Actions

STOP NEW ACTION

Operation: Chris Test Operation
Location: Orchard Cottage
Action: Hold
Start Time: 2021-04-07 16:56:03
End Time: -

Network	Identities	GSM	UMTS	LTE	Targets
O2 (UK)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
Vodafone UK	-	-	-	-	-
3	-	-	-	-	-
EE	-	-	-	-	-
TOTAL	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)

Rows per page 20 50 100 Page 1 of 1

Network	Technology	IMSI	IMEI	Distance (m)

Rows per page 20 50 100 Page 1 of 1

Transceivers

GSM 2m 58s
Serial Number: 1934/004

MNC: O2 (UK)
RSSI: -
ARFCN: 1000
Tx Power: 33dBm

UMTS 2m 57s
Serial Number: 1934/006

MNC: O2 (UK)
RSSI: -
UARFCN: 10637
Tx Power: 19dBm

Fig 203. Hold – refreshed

NESIE will now conduct a Hold operation loOKing for the listed identities.

If No Rescan between cycles has been checked, NESIE will complete 1 cycle through the chosen networks and technologies and then begin the same cycle again. This cycle will continue until the operator presses the Stop button.

If the operator has not checked the No Rescan between cycles option, the NESIE will complete one cycle then carry out a Network Scan, and, when ready start the Hold process again. This cycle of Hold and Network Scan will continue until the operator presses the STOP button.

23.4 HOLD – TARGET FOUND – COMPASS

Whenever a Target device is found and successfully in Hold (on GSM, UMTS or LTE), the MAPPING page will display a compass instead of the Target selection filters. As shown in Fig 204. Hold – Compass Fig 204. This compass is used to indicate the direction of the Target when a fix has been calculated. This has been discussed in detail at section

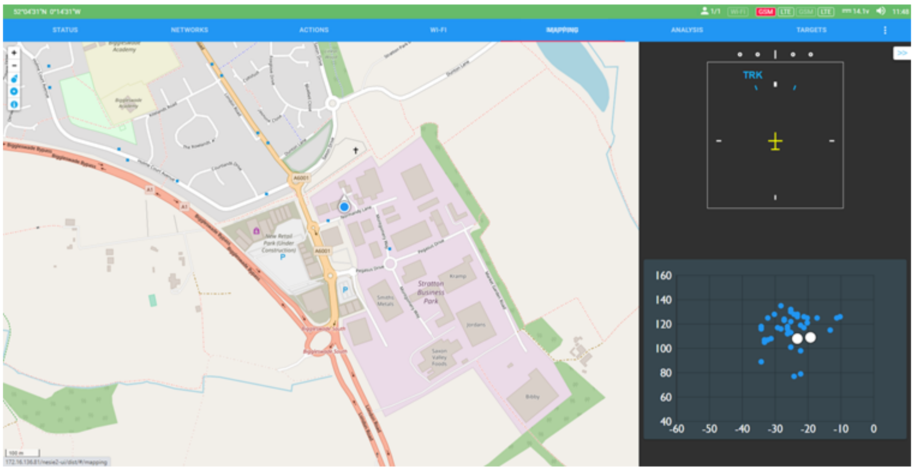


Fig 204. Hold – Compass map key

23.5 HOLD – TARGET FOUND ON GSM

When a Target is found, NESIE will automatically move the device to a traffic channel and establish the Hold. During this process NESIE will send two alert types:

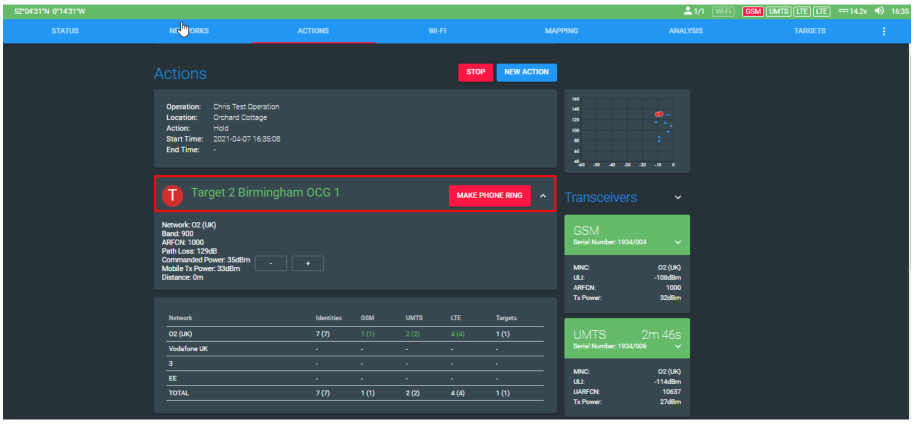
Audible Alert. When a Target device is detected, an audible alert will be heard by the operator (unless the mute button has been activated)

A second 'heart beat' alert will then periodically sound to let the operator know that the Hold is continuing. If the Hold is lost a third alert will be heard.

Visual Alert. The visual alerts will consist of two notification boxes that appear in the UI, as shown below in Fig 205.

- Header Bar: The transceiver (GSM) icon on the header bar will turn red to notify the operator that a Hold has been initiated using the UMTS transceiver.

- Hold Notification: When a Target has been placed into GSM Hold, a notification box will appear stating the Target name and the details of the Hold technology, band and channel number.



Actions

Operation: Chris Test Operation
Location: Orchard Cottage
Action: Hold
Start Time: 2021-04-07 16:35:08
End Time: -

T Target 2 Birmingham OCG 1

Network: O2 (UK)
Band: 900
ARFCN: 1000
Path Loss: 129dB
Commanded Power: 35dBm
Mobile Tx Power: 33dBm
Distance: 0m

Network	Identities	GSM	UMTS	LTE	Targets
O2 (UK)	7 (7)	1 (1)	2 (2)	4 (4)	1 (1)
Vodafone UK	-	-	-	-	-
3	-	-	-	-	-
EE	-	-	-	-	-
TOTAL	7 (7)	1 (1)	2 (2)	4 (4)	1 (1)

GSM
Serial Number: 1934/004

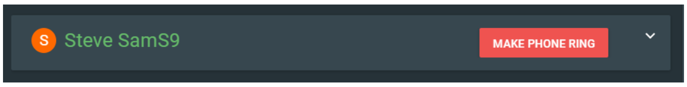
MNC:	O2 (UK)
ULI:	-108dBm
ARFCN:	1000
Tx Power:	32dBm

UMTS 2m 46s
Serial Number: 1934/006

MNC:	O2 (UK)
ULI:	-114dBm
UARFCN:	10637
Tx Power:	27dBm

Fig 205. Hold - Action summary

The first notification will show the Target icon and name as shown below at Fig 206. Whilst in GSM Hold, there is also the option to make the Target device ring. This option is discussed further in the Make phone Ring Button section below.



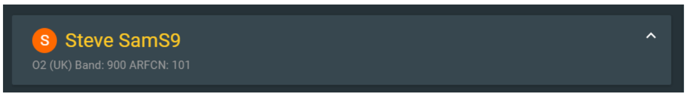
S Steve SamS9

Fig 206. Hold notification

The colour of the Target name may change depending on the status of the Hold being carried out on the Target device

Green Target is in Hold, as per Fig 206 above.

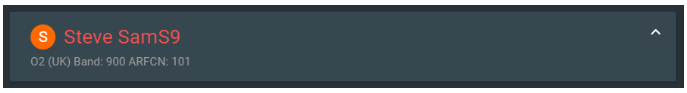
Amber Target device has dropped from the Hold. The NESIE software is automatically trying to regain the Hold on the same channel as shown in Fig 207 below.



S Steve SamS9
O2 (UK) Band: 900 ARFCN: 101

Fig 207. Hold lost – auto regain - Hold

Red Target device is no longer in Hold. Attempts to recapture the device on the same channel have failed. The Hold process has started again, as shown in Fig 208 below.



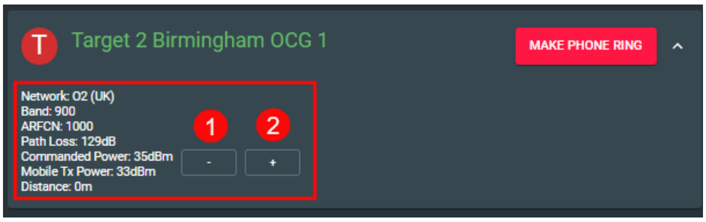
S Steve SamS9
O2 (UK) Band: 900 ARFCN: 101

Fig 208. Hold lost – Hold restarted

As shown in the red box in Fig 205 above, when the Target device is in Hold, the Target icon and name will be displayed with the MAKE PHONE RING button.

When NESIE has the device in Hold, the Action summary page will display the Hold information. If the operator presses the ⌄ button, the dialogue box will expand to show additional information as shown below at Fig 209 below.

Once a mobile device is in a GSM Hold, the operator can increase/decrease the transmitted power of the DF beacon channel by using the **-** and **+** buttons at position 1 and 2 if it is required to maintain a good signal for DF. The information inside the red box can be passed to the Direction Finding team and can be programmed into the DF equipment to geolocate the Target mobile device. More information about this process can be found in the section 23.5.2 below.


T Target 2 Birmingham OCG 1

Network: O2 (UK)
Band: 900
ARFCN: 1000
Path Loss: 129dB
Commanded Power: 35dBm
Mobile Tx Power: 33dBm
Distance: 0m

Fig 209. Hold – channel info

The information inside the red box that the DF team require is:

Band Freq band that the mobile device is using – GSM 900.

Channel No Depending on the Hold settings set up by the operator, the NESIE system will automatically select the quietest traffic channel and move the Target mobile device to it – in this case **ARFCN 1000** within the **GSM 900** band. This will differ depending on what technology the mobile device is being held on – UARFCN for UMTS and EARFCN for LTE.

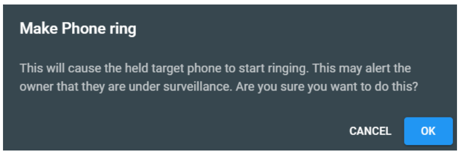
Path Loss This is the difference in the power level transmitted by the mobile device in the Hold and the level that the NESIE system receives it. The lower the Path Loss the closer the phone is and less objects are obstructing the line of sight**.**

Commanded Power The power level that has been requested by NESIE

Mobile Tx Power The power level acknowledged by the mobile device

23.5.1 MAKE PHONE RING BUTTON

Whilst in GSM Hold, the NESIE operator has the option to make the Target mobile device ring. After pressing the MAKE PHONE RING button, a warning message will be displayed, as shown at Fig 210 below. After the OK button has been pressed, a protocol message will be sent to the Target mobile device that will force it to ring. The Target device will receive a call from an ‘Unknown Number’.


Make Phone ring

This will cause the held target phone to start ringing. This may alert the owner that they are under surveillance. Are you sure you want to do this?

Fig 210. Make Phone Ring – warning

NOTE: The Hold command is sent from NESIE to the Target device. It is the decision of the device (and the software installed on it) if it obeys the commands sent. Some mobile devices may refuse to move to GSM or UMTS for the Hold process to start or they may drop off the Hold process. It has been seen that some devices can refuse to be put into Hold and some have a more random response. An example of this is the mobile device will drop the Hold and be reacquired every 30 seconds.

As explained above, this process of Hold / dropped can be seen in the UI.

23.5.2 HOLD – MOBILE POWER CONTROL

During normal device activity, when a cellular device is connected to the real network it will regularly change the transmit power. This change in transmit power is controlled by the network. The network calculates the distance of the cellular device and adjusts the amount of power that would be required to allow the device to communicate with the tower. As the cellular device moves further away from the tower, the device is commanded by the tower to increase its transmission power. NESIE can replicate this power control process, sending commands to the device to increase or decrease its power.

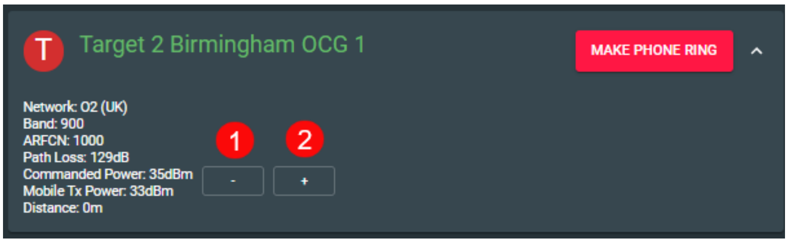
Upon establishing the Hold, the distance to the device is calculated and logged. NESIE automatically sends a command to control (increase / decrease) the power to a suitable level to maintain the Hold. This ideal power level will let the device use as little power as required so that will not drain the device battery too quickly but high enough to maintain the Hold.

23.5.2.1 USING POWER CONTROL FOR DF

The NESIE operator can manually control the output power of the Target mobile device. It may be required to increase the output power to make it easier for the direction finding team to locate the Target at the initial stages. Then, as the direction finding team gets closer to the Target, the output power of the mobile device would normally be reduced.

Auto power control is disabled when the user manually increases / decreases the mobile device transmit power. If a new Hold operation is started manually or automatically (if the Target drops from Hold), the auto power control will recommence.

The operator can manually increase or decrease the desired output power of the cellular device by using the + and – buttons shown at position 1 and 2 in Fig 211 below.



Target 2 Birmingham OCG 1

Network: O2 (UK)
Band: 900
ARFCN: 1000
Path Loss: 129dB
Commanded Power: 35dBm
Mobile Tx Power: 33dBm
Distance: 0m

Fig 211. Manual power control

CAUTION: THE OPERATOR MUST BE AWARE THAT THERE IS A POSSIBILITY THAT PERSISTENT USE OF THE HOLD ACTION AND USING THE POWER CONTROL FOR DF TO INCREASE THE TRANSMITTED SIGNAL OF THE TARGET MOBILE DEVICE COULD EVENTUALLY DRAIN ITS BATTERY. THIS IS A VERY IMPORTANT OPERATIONAL CONSIDERATION, SPECIFICALLY IF THE OPERATION IS INTENDED TO LOCATE A VULNERABLE/SUICIDAL PERSON.

NOTE: In complete contrast to the above caution, in specific operational environments, the operator may wish to increase the Target mobile device transmit power to run down the battery on the Target device so that it cannot be used.

23.5.3 HOLD – DISTANCE MEASUREMENTS

Whilst in Hold, the NESIE BTS continually calculates and displays the distance to the Target device.

GSM. If the Target device is controlled via the GSM protocol, the distance is measured via the Timing Advance (TA) measurement. This measurement has a maximum achievable accuracy of 550m.

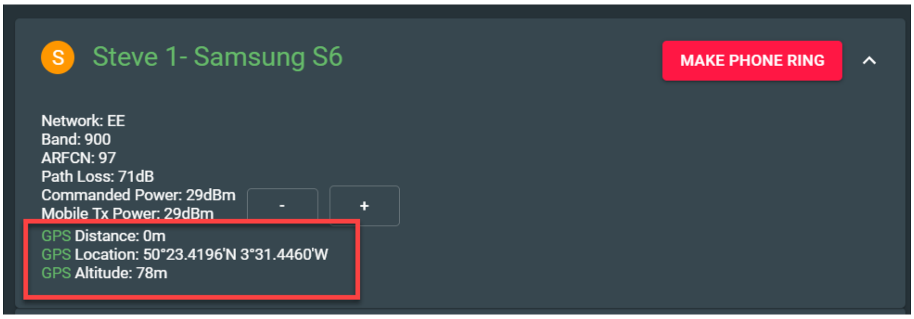
UMTS. If the Target device is controlled via the UMTS protocol, the distance is measured via the Chip Rate measurement. This measurement has a maximum achievable accuracy of 20m.

LTE. If the Target device is controlled via the LTE protocol, the distance is measured via the Chip Rate measurement. This measurement has a maximum achievable accuracy of 20m.

NOTE: A detailed explanation of the distance measurement process is covered in section 25.2 below.

23.5.4 HOLD – GPS RETRIEVED

As soon as a mobile device has been moved to the Hold on GSM and the Hold is successful, the NESIE system continually attempts to retrieve a GPS location from the mobile device. If the cellular device is compliant (and the command works upon its first attempt), it will take approximately 10-15 to retrieve the GPS results. If successful, the Target GPS Latitude and Longitude will be displayed as shown in Fig 212 below.



S Steve 1- Samsung S6

Network: EE
Band: 900
ARFCN: 97
Path Loss: 71dB
Commanded Power: 29dBm
Mobile Tx Power: 29dBm
GPS Distance: 0m
GPS Location: 50°23.4196'N 3°31.4460'W
GPS Altitude: 78m

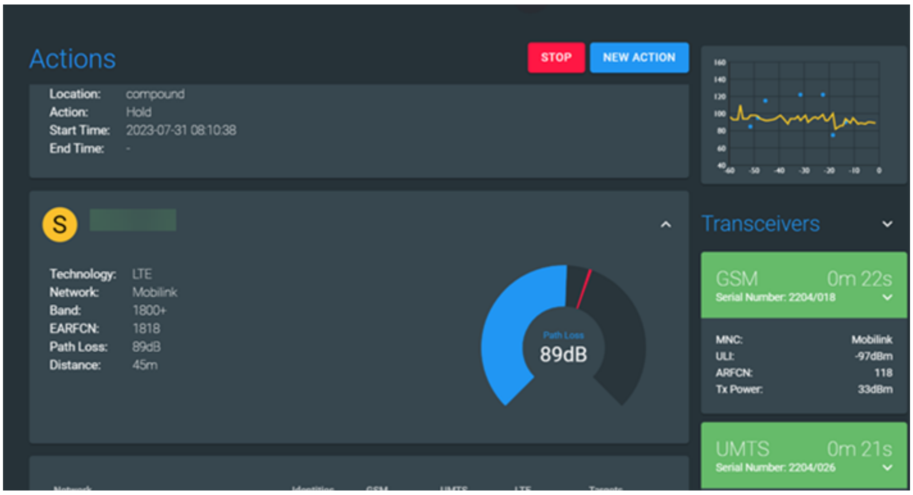
Fig 212. Timing Advance & GPS

During the 2G Hold process, the NESIE system continually attempts to extract the GPS from the Target device. However, if the device is unable to achieve a GPS fix, it cannot be displayed e.g. when the device is inside a building.

If the Target device is subsequently moved to a location where a GPS fix could be achieved, the results will then appear on the UI.

23.6 HOLD – CLOSE IN MODE

When a device is placed in a Hold, a meter will be displayed in the Target pane on the ACTIONS page. This information will allow the user to use NESIE in the tactical backpack as a basic form of location device. The red marker inside the meter displays the path loss to the Target device when it was first placed in a Hold. The operator can now move the NESIE. If the operator moves closer to the Target device, the meter will move to the right (stronger signal). If the operator is moving away from the Target device, then the meter will move to the left. This meter will appear when any device is placed in a Hold (Fig 213).



Actions

Location: compound
Action: Hold
Start Time: 2023-07-31 08:10:38
End Time: -

S [redacted]

Technology: LTE
Network: Mobilink
Band: 1800+
EARFCN: 1818
Path Loss: 89dB
Distance: 45m

Transceivers

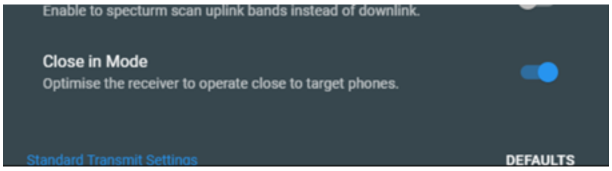
GSM 0m 22s
Serial Number: 2204/018

MNC: Mobilink
UL: -97dBm
ARFCN: 118
Tx Power: 33dBm

UMTS 0m 21s
Serial Number: 2204/026

Fig 213 Path Loss meter

This meter can also be used inside buildings to find hidden bugs placed in a meeting room, hotel bedroom or other enclosed spaces. To allows this to happen, the sensitivity of the receiver has to be increased. In the Settings page, the operator must navigate to Close in Mode and toggle on the slider (Fig 214).



Enable to specturm scan uplink bands instead of downlink.

Close in Mode
Optimise the receiver to operate close to target phones.

Fig 214 Close in Mode

When Close in Mode has been enabled, the following icon will be displayed on the header bar at the top of the screen. Close in mode is disabled when the system is shut down (Fig 215).

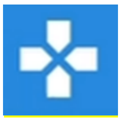


Fig 215 Close in Mode Icon

23.7 HOLD – TARGET FOUND ON UMTS

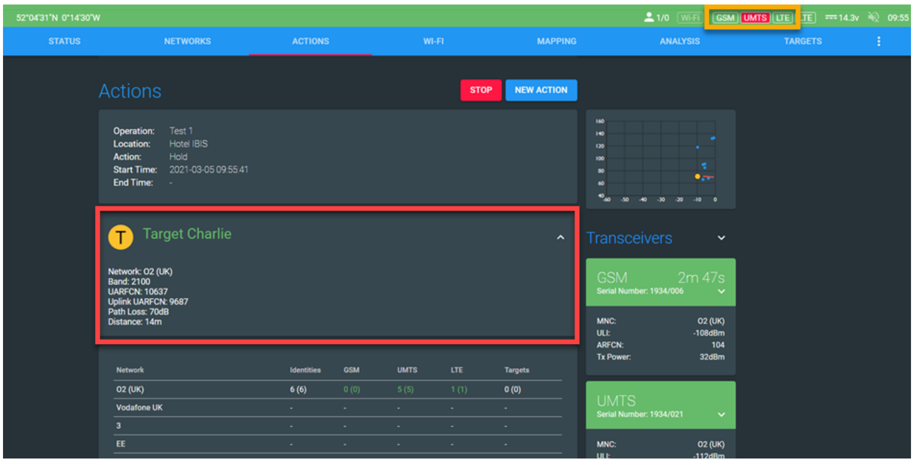
When a Target is found on UMTS, NESIE will automatically move the device to a UMTS traffic channel and establish the Hold. During this process NESIE will send two alerts types:

Audible alert. When a Target is detected, an audible alert will sound through the laptop / tablet that is used to control the NESIE system. A second ‘heart beat’ alert will then periodically sound to let the operator know that the Hold is continuing. If the Hold is lost, a third alert will be heard.

Visual Alert. The visual alerts will consist of two notification boxes that appear in the UI, as shown below in Fig 216.

- Header Bar: The transceiver (UMTS) icon on the header bar will turn red to notify the operator that a Hold has been initiated using the UMTS transceiver.

- Hold notification: When a Target has been placed into UMTS Hold, a notification box will appear stating the Target name and the details of the Hold technology, band and channel number.



Actions

Operation: Test 1
Location: Hotel IBIS
Action: Hold
Start Time: 2021-03-05 09:55:41
End Time: -

T Target Charlie

Network: O2 (UK)
Band: 2100
UARFCN: 10637
Uplink UARFCN: 9687
Path Loss: 70dB
Distance: 14m

Network	Identities	GSM	UMTS	LTE	Targets
O2 (UK)	6 (6)	0 (0)	5 (5)	1 (1)	0 (0)
Vodafone UK	-	-	-	-	-
3	-	-	-	-	-
EE	-	-	-	-	-

Transceivers

GSM 2m 47s
Serial Number: 1934/006

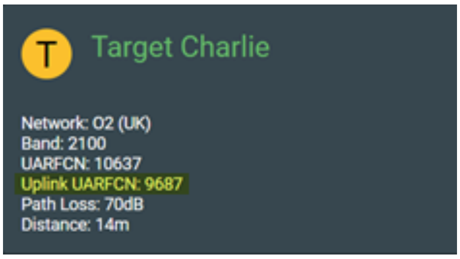
MNC: O2 (UK)
ULI: -108dBm
ARFCN: 104
Tx Power: 32dBm

UMTS
Serial Number: 1934/021

MNC: O2 (UK)
ULI: -112dBm

Fig 216. UMTS Hold - Action Summary

If the device is held on UMTS, the Hold details are listed in the pane. The important part of this section is the Uplink Channel Number or UARFCN as shown in yellow in Fig 217. This is the channel that the Target device is transmitting on and would normally be used by the direction finding team to geolocate the Target.



T Target Charlie

Network: O2 (UK)
Band: 2100
UARFCN: 10637
Uplink UARFCN: 9687
Path Loss: 70dB
Distance: 14m

Fig 217. UMTS Hold – uplink UARFCN

NOTE: Due to the additional security measure on the UMTS protocol, there are less options available during the Hold process. NESIE is not able to change the power of the device or make the device ring.

23.8 HOLD – TARGET FOUND ON LTE

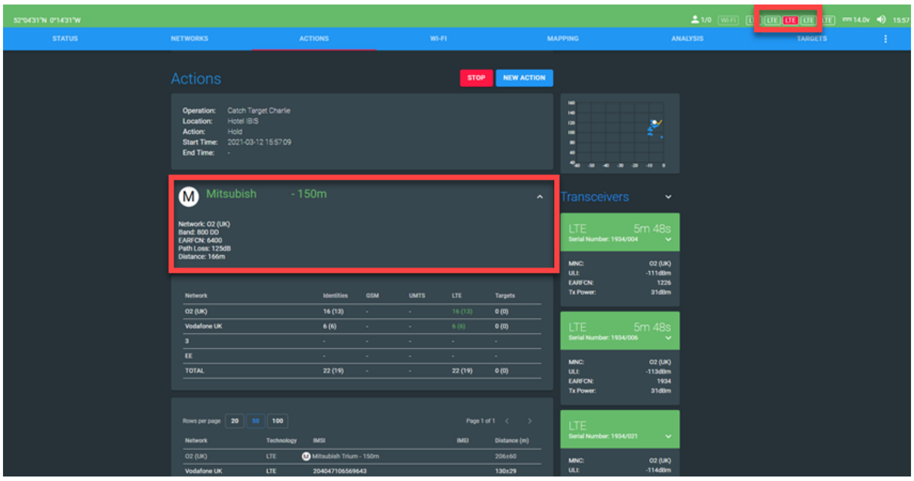
When a Target is found on LTE, NESIE will automatically move the device to an LTE traffic channel and establish the Hold. During this process NESIE will send two alerts:

Audible alert. When a Target is detected, an audible alert will sound through the laptop / tablet that is used to control the NESIE system. A second 'heart beat' alert will then periodically sound to let the operator know that the Hold is continuing. If the Hold is lost, a third alert will be heard.

Visual Alert. The visual alerts will consist of two notification boxes that appear in the UI, as shown below in Fig 218.

- Header Bar: The transceiver (LTE) icon on the header bar will turn red to notify the operator that a Hold has been initiated using that LTE transceiver.

- Hold notification: When a Target has been placed into LTE Hold, a notification box will appear stating the Target name and the details of the Hold technology, band and Channel Number.



Actions

Operation: Catch Target Charlie
Location: Hotel IBIS
Action: Hold
Start Time: 2021-03-12 15:57:09
End Time: -

M Mitsubish - 150m

Network: O2 (UK)
Band: 800 DD
EARFCN: 6400
Path Loss: 125dB
Distance: 166m

Network	Identities	GSM	UMTS	LTE	Targets
O2 (UK)	16 (13)	-	-	16 (13)	0 (0)
Vodafone UK	6 (6)	-	-	6 (6)	0 (0)
3	-	-	-	-	-
EE	-	-	-	-	-
TOTAL	22 (19)	-	-	22 (19)	0 (0)

Rows per page 20 50 100 Page 1 of 1

Network	Technology	IMSI	IMEI	Distance (m)
O2 (UK)	LTE	M Mitsubish Trium - 150m		206±60
Vodafone UK	LTE	204047106569643		130±29

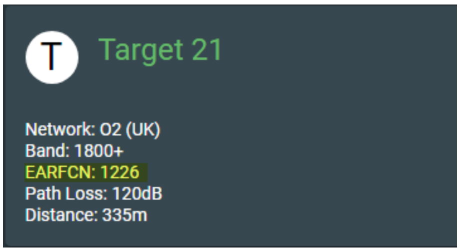
LTE 5m 48s
Serial Number: 1934/004
MNC: O2 (UK)
ULI: -111dBm
EARFCN: 1226
Tx Power: 31dBm

LTE 5m 48s
Serial Number: 1934/006
MNC: O2 (UK)
ULI: -113dBm
EARFCN: 1934
Tx Power: 31dBm

LTE
Serial Number: 1934/021
MNC: O2 (UK)
ULI: -114dBm

Fig 218. LTE Hold - Action summary

If the device is held on LTE, the Hold details are listed in the pane. The important part of this section is the uplink Channel Number or EARFCN Fig 219. This is the channel that the Target device is transmitting on and would normally be used by the direction finding team to geolocate the Target.



T Target 21

Network: O2 (UK)
Band: 1800+
EARFCN: 1226
Path Loss: 120dB
Distance: 335m

Fig 219. LTE Hold – Uplink EARFCN

NOTE: Due to the additional security measure on the LTE protocol, there is less options available during the Hold process. NESIE is not able to change the power of the device or make the device ring.

24. MAPPING

This section covers the manipulation of the mapping and its features. Normally the mapping is used to geo-locate Targets. The geo-locate process is described in detail in section 25. The mapping section and geolocation sections should be read in conjunction.

NESIE has been pre-loaded with operational mapping to cover the whole world. This whole world map is Open Street Map. As the map is zoomed in or out, the mapping automatically adjusts to the relevant scale.

NOTE. Several zoom levels of the map will display automatically, however, the larger zooms levels may initially take several seconds to appear when opening to a new location for the first time. Once these layers have been retrieved from the memory they are formatted correctly and put in the cache for future use. It is suggested that when you start operations in a new area, navigate around the expected area of operations and zoom in/out to reduce the amount of time it takes to render the map tiles.

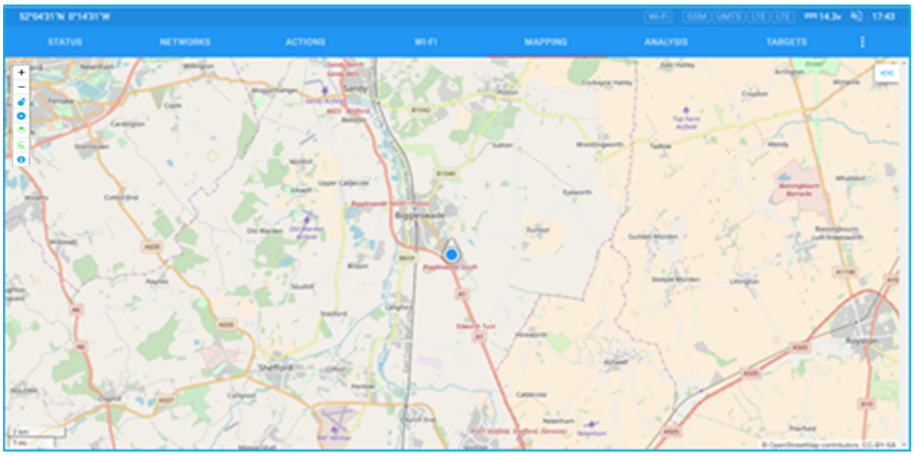


Fig 220. Mapping Page

The mapping will always remain orientated towards North, the icon representing the NESIE System will rotate in accordance with the direction of flight.

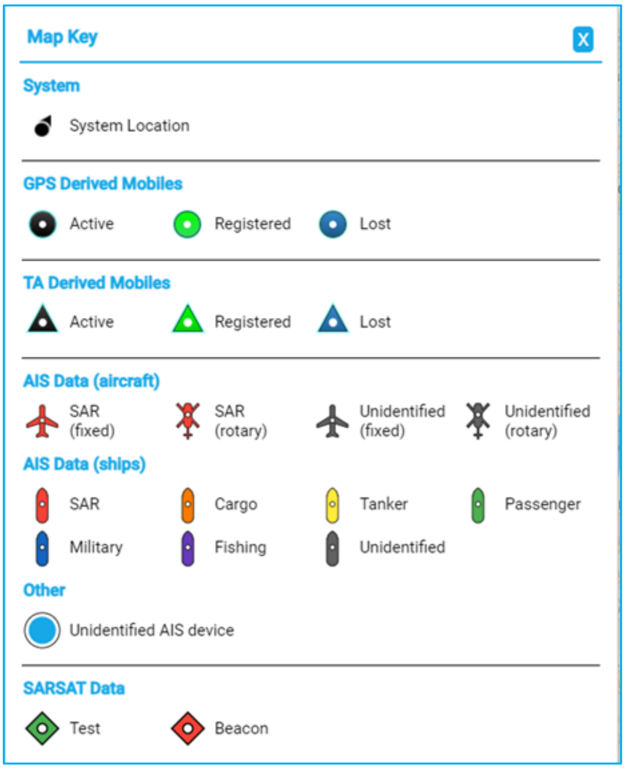
24.1 MAP MANIPULATION

The map can be manipulated by using the buttons in the top left of the map view. These are:

+	Zoom in
−	Zoom out
●	Centre on NESIE location
◉	Centre on current device in Hold
◎	Display range ring error and heatmap
∽	Display route travelled (Target Hold locations)
ⓘ	Display map key

24.2 MAP KEY

Clicking the map key button ⓘ, will display the map key pane as seen below in Fig 221. Unless the NESIE system has an AIS transmitter or a COSPAS/SARSAT receiver installed, the majority of these icons will not be seen on a ground based system.



Map Key X

System

● System Location

GPS Derived Mobiles

● Active ● Registered ● Lost

TA Derived Mobiles

▲ Active ▲ Registered ▲ Lost

AIS Data (aircraft)

✈ SAR (fixed) ✈ SAR (rotary) ✈ Unidentified (fixed) ✈ Unidentified (rotary)

AIS Data (ships)

▯ SAR ▯ Cargo ▯ Tanker ▯ Passenger

▯ Military ▯ Fishing ▯ Unidentified

Other

● Unidentified AIS device

SARSAT Data

◆ Test ◆ Beacon

Fig 221. Map key

The colour of the geo-location icon will change depending on the status:

Active Target is in Locate Mobile mode or on an active voice call.

Registered Target has been registered but is not currently being located.

It is possible for a large group of Target mobile devices to be registered to the system. Only one device can be located at a time and the operator can switch which registered Target is located.

Lost The last calculated location before the signal was lost by the system.

24.3 MAP AND POP-OUT PANEL

By clicking the pop-out panel icon << on the top-right of the screen, the operator can display an additional pane. Depending on the current operation, the pane will be displayed in one of two options:

- Filter — Filter the operation / Target and display the distance measurements (range rings)
- Compass — Only displayed if device is successfully held. The compass will indicate the direction to the fix.

The map with filter panel is shown in Fig 222. This pop-out panel can be hidden by clicking the >> button again.

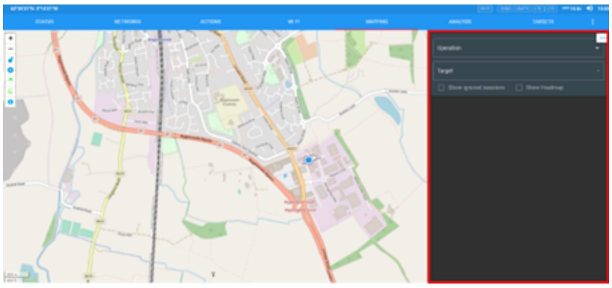
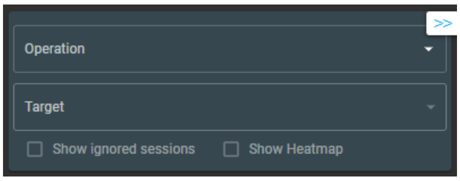


Fig 222. Mapping pop-out panel

24.4 POP-OUT PANEL – FILTER

The Filter pane will be displayed whenever the operator is conducting Grab, Hunt, Deny and Broadcast SMS operations. The pane allows the operator to manually control the current or historical range rings that are displayed on the screen.

The pop-out panel shown below in Fig 223. Map pop-out panel allows the NESIE operator to select which Operation and Target is displayed on the map and any associated distance measurement range rings. The operator also has the option to Show ignored sessions and Show Heatmap by checking the relevant tick box.



Operation

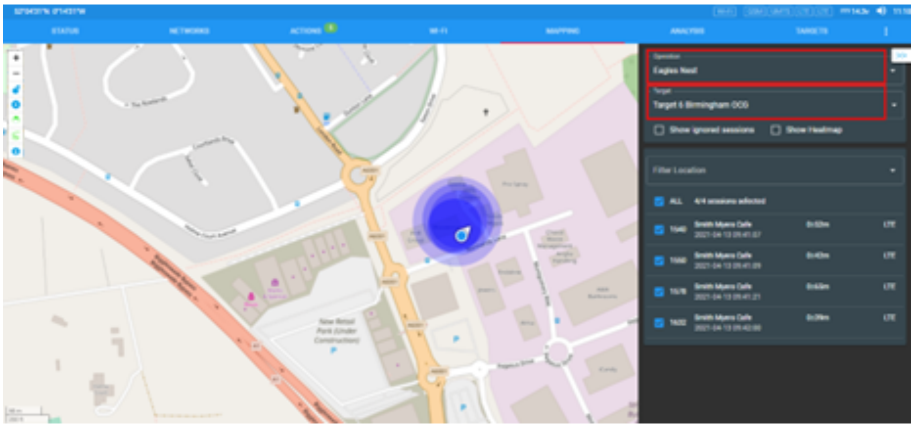
Target

□ Show ignored sessions □ Show Heatmap

Fig 223. Map pop-out panel

NOTE: Within the NESIE system, the list of sessions (an Action/Interaction with a mobile device) does not include any GSM sessions that have a large error in relation to the range (ranges more than 100m and an error of +/-500m.) The 'Show Ignored Sessions' option displays these sessions in the list, although they are not selectable for display on the map.

Fig 224 below shows the filter options that will become available for a selected operation and Target. In this example, the Operation Eagles Nest and Target 6 Birmingham OCG have been selected. When an Operation and Target are selected, all sessions are selected by default (except ignored sessions) and their appropriate distance measurement rings are displayed on the map. If the operator only wants to view certain sessions, they can click the adjacent check box(s).



Operation: Eagles Nest

Target: Target 6 Birmingham OCG

□ Show ignored sessions □ Show Heatmap

Filter Location

☑ ALL 4/4 sessions selected

☑ [illegible] Smith Myers Cafe 2021-04-13 09:41:07 [illegible] LTE

☑ [illegible] Smith Myers Cafe 2021-04-13 09:41:09 [illegible] LTE

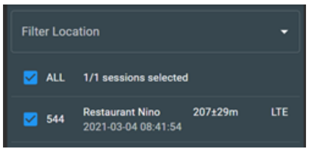
☑ [illegible] Smith Myers Cafe 2021-04-13 09:41:21 [illegible] LTE

☑ [illegible] Smith Myers Cafe 2021-04-13 09:42:00 [illegible] LTE

Fig 224. Map pop-out – Target selected

Fig 225 below shows the details for a session for a particular Operation and Target, the operator has the option to select all sessions or pick individual sessions to display on the map by clicking in the relevant tick box, this is covered in more detail in the explanation for Fig 226. The options and information displayed in the sessions selection pane are as follows:

- Tick Box – For all sessions or individual/multiple session selection
- Session Numbers
- Location Name & date
- Distance & +/- error
- Technology the device was Grabbed on



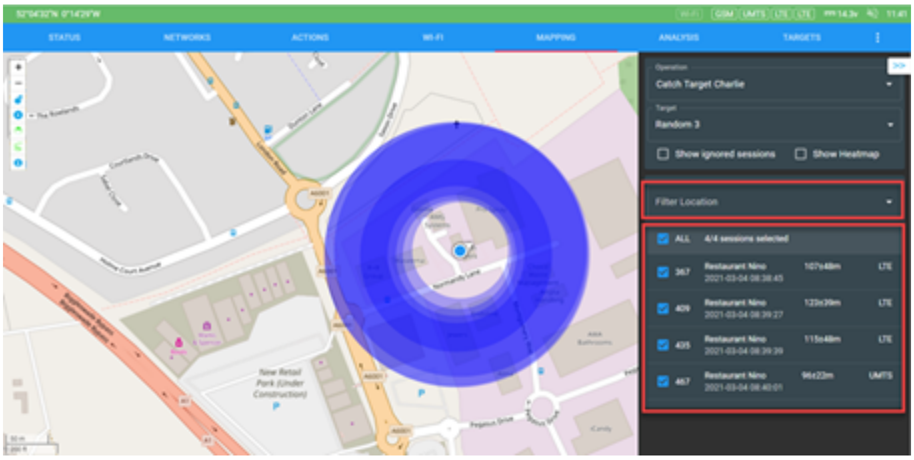
Filter Location

☑ ALL	1/1 sessions selected			
☑ 544	Restaurant Nino 2021-03-04 08:41:54	207±29m	LTE	

Fig 225. Map pop-out – session selection details

In Fig 226 below, the selected Target (Random 3) has 4 range rings that are displayed on the map. All 4 of these rings are automatically selected when an Operation and Target are selected from the drop down menus. If required, the operator can untick some or all these boxes to investigate individual range rings and how they affect the overall picture of where the Target device is estimated to be.

It may be that the range rings cover several different physical locations e.g. 2 were calculated at the restaurant and 2 were calculated at the hotel. In this instance the operator can filter the range rings displayed by using the Filter Location drop-down menu.



Operation: Catch Target Charlie

Target: Random 3

☐ Show ignored sessions ☐ Show Heatmap

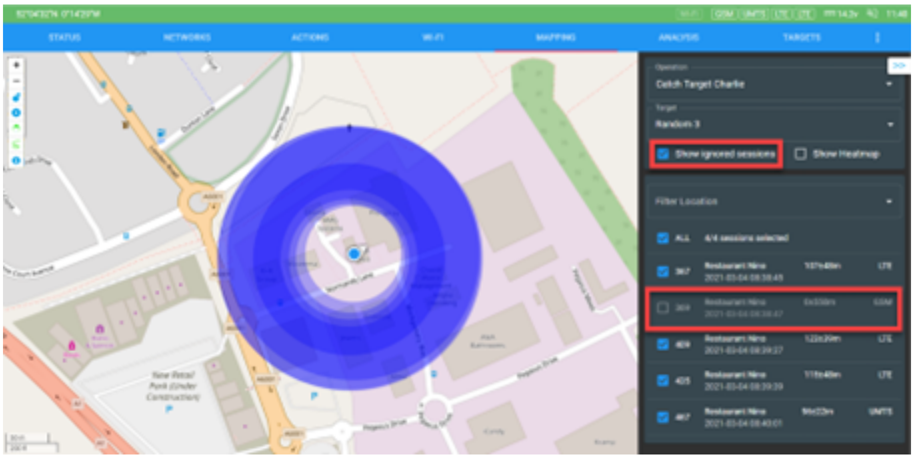
Filter Location

☑ ALL	4/4 sessions selected		
☑ 367	Restaurant Nino 2021-03-04 08:38:45	107±48m	LTE
☑ 409	Restaurant Nino 2021-03-04 08:39:27	123±39m	LTE
☑ 435	Restaurant Nino 2021-03-04 08:39:39	115±48m	LTE
☑ 467	Restaurant Nino 2021-03-04 08:40:01	96±22m	UMTS

Fig 226. Map pop-out – multiple range rings

Due to the inherent error of the GSM Timing Advance protocol (always has an error of +550m and -550m), the GSM range rings will not be displayed on the map unless the distance is over 2Km. So, the operator may believe that a distance measurement is available, but it is not displayed on the screen, as shown in Fig 227 below.

By clicking the Show Ignored Sessions, any range rings that were ignored / hidden will now be shown, but they will be greyed out and cannot be added to the screen.



Operation
Catch Target Charlie

Target
Random 3

☑ Show ignored sessions ☐ Show Heatmap

Filter Location

☑ ALL 4/4 sessions selected

☑ 367 Restaurant Nino 2021-03-04 08:38:45 107±48m LTE

☐ 369 Restaurant Nino 2021-03-04 08:38:47 0±550m GSM

☑ 409 Restaurant Nino 2021-03-04 08:39:27 122±20m LTE

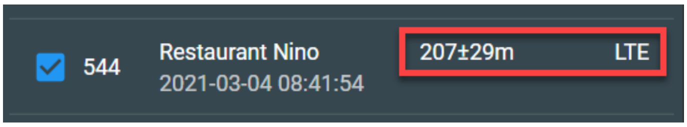
☑ 405 Restaurant Nino 2021-03-04 08:39:39 118±48m LTE

☑ 467 Restaurant Nino 2021-03-04 08:40:01 94±22m UMTS

Fig 227. Map pop-out – Show Ignored Sessions

The range ring is calculated using the GSM, UMTS or LTE protocol. As previously mentioned, the GSM protocol has an inherent error of +/- 500m. Both the UMTS and LTE protocols are a lot more accurate.

When a range ring is displayed, the details of that data are displayed in the list of results. The range ring comprises the calculated distance to the device and resultant error. In the example shown at Fig 228, the calculated distance is shown as 207m with an error of +29m and –29m from that calculated distance. Therefore, a range ring is displayed that covers the area.

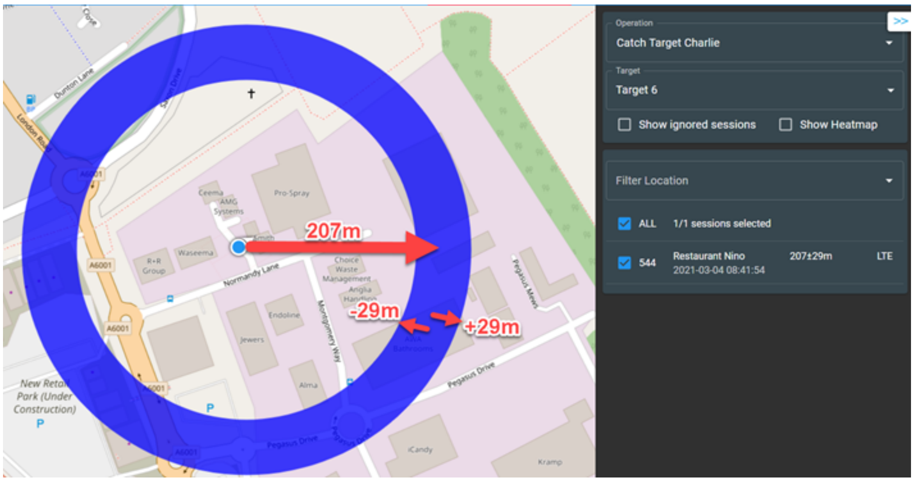


☑ 544 Restaurant Nino 2021-03-04 08:41:54 207±29m LTE

Fig 228. Distance & Error

Therefore, NESIE displays a range ring that is centred at 207m and covers an area of -29m and +29m. The resultant range ring is 59m across as shown below in Fig 229.

The range ring is shown as a ring because the NESIE system usually uses omni directional antennas, therefore the NESIE software does not know which direction or area the Target device could be in.



Operation
Catch Target Charlie

Target
Target 6

☐ Show ignored sessions ☐ Show Heatmap

Filter Location

☑ ALL	1/1 sessions selected			
☑ 544	Restaurant Nino 2021-03-04 08:41:54	207±29m	LTE	

Fig 229. Range ring depicting error

24.5 POP-OUT PANEL – COMPASS

Whenever an operator initiates a Hold, the pop-out display will automatically show the compass pane in place of the filter pane, as shown below in Fig 230.

The compass pop-out pane is actually made up of 2 sections:

- Compass
- Graph

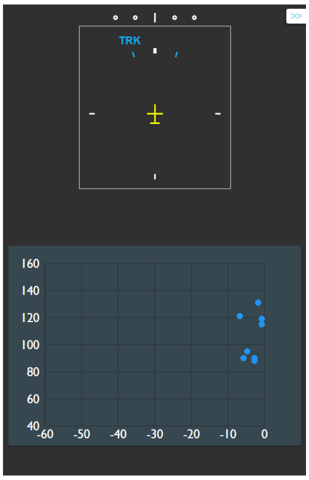


Fig 230. Hold – compass & graph pane

NOTE: If the NESIE system is stationary, the compass will not know which direction it is facing, therefore the bearing will not be displayed on the compass.

NOTE: THE USE OF THE COMPASS WHILST OPERATING ON THE GROUND MAY ONLY HAVE LIMITED FUNCTIONALITY DUE TO THE STATIC NATURE OF THE OPERATIONS.

24.5.1 COMPASS

Initially the compass will appear blank, as shown in Fig 230 above. If the NESIE systems GPS has not detected movement, it will not know which way it is facing and will therefore not display the bearing (number ring) on the outer. Once the system knows its location and which direction it is pointing, the number ring will appear, as shown in Fig 231 below.

In the image below it can be seen that the NESIE system is pointing at a bearing of 170T (170 Degrees True)

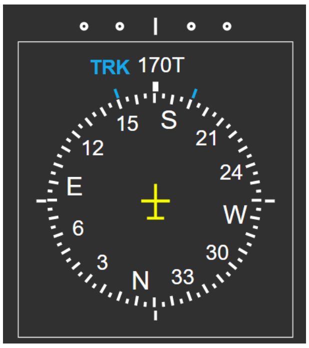


Fig 231. Compass – with bearings

Only after a GPS fix has been extracted from the Target device, or a Timing Advance fix has been calculated, will the direction arrow appear. As shown in Fig 232 below.

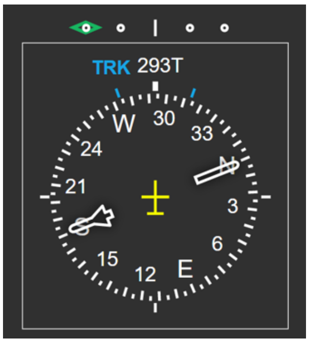


Fig 232. Compass – direction to target

In the image above, the NESIE system is now pointing at a bearing of 293T (293 degrees True and the direction arrow is pointing at a bearing of 180 degrees (shown as South (S) on the display). The direction arrow will change accordingly as the NESIE system refines the geolocation fix or if the NESIE system moves.

24.5.2 RAPH

The lower section of the pane displays the activity graph. The graph is used to display the phones being grabbed against time and signal strength. As shown below in Fig 233.

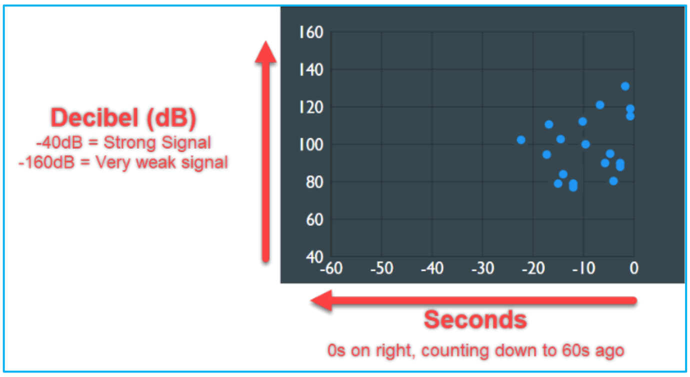


Fig 233. Hold – graph pane axis

- X Axis Signal strength in Decibel (dB)
  -40 to – 160 dB

- Y Axis Elapsed time in seconds
  0 being the current time
  Then moving to the left in -10 seconds intervals

● Small blue dot A cellular device detected by NESIE

● Large Coloured dot A Target device – colour will be same as that selected when making it a Target

25. GEO-LOCATE A TARGET

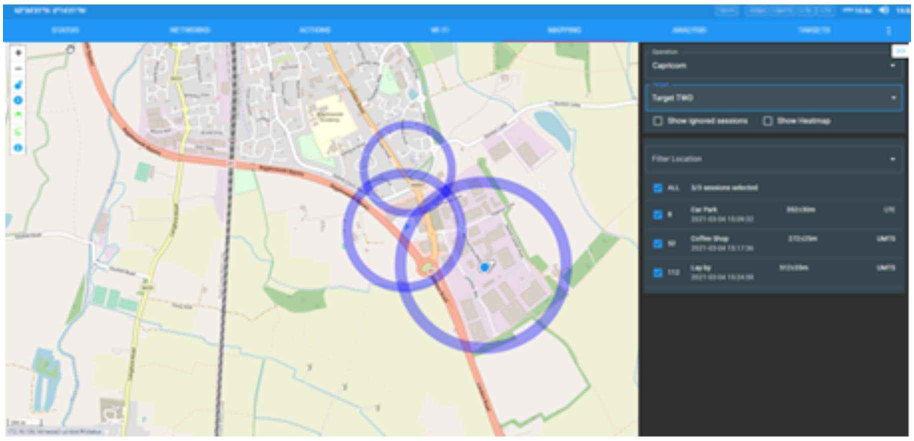
There are four ways to locate a Target mobile device using the NESIE system:

- Multiple Grabs & combing multiple range rings (Range Rings)
- Hold & Geo-Locate on the Move (Running Fix)
- Hold & extract the GPS
- Hold & traditional Hand Held Direction Finding (HHDF)

25.1 GEO-LOCATE A TARGET - PROCESS

It is suggested that the following process is used whenever possible to locate a Target. This process allows the NESIE to be utilised as much as possible to ensure the minimum amount of manpower is required on the ground. Additional manpower and equipment should be called into the area after NESIE has narrowed down the search area to the smallest area possible.

1. Conduct a minimum of three Grabs, at three different locations to obtain distance measurements (Range Rings) to the Target device. Then combine these distance measurements on the Mapping window to obtain a Heat Map showing the estimated location of the Target device as shown in Fig 234 below.



Operation: Capricorn

Target: Target TWO

□ Show ignored sessions □ Show Heatmap

Filter Location

☑ ALL 3/3 sessions selected

☑ 8 Car Park 2021-03-04 15:09:32 392±30m LTE

☑ 92 Coffee Shop 2021-03-04 15:17:36 272±29m UMTS

☑ 112 Lay-by 2021-03-04 15:24:38 512±35m UMTS

Fig 234. Target mapping - Heat Map

2. Advise the Direction-Finding team of the estimated area of the Target. However, before putting more team members onto the ground, start a Hold operation on the Target device. During the Hold operation, NESIE will automatically attempt to activate the devices GPS and ask for the results to be sent to NESIE. If the mobile device returns a GPS fix, it will be displayed on the Target mapping as a circle as shown in Fig 235.

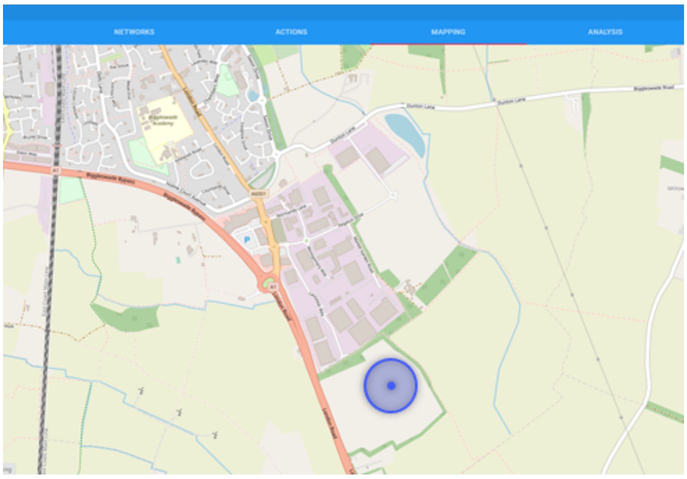


Fig 235. GPS fix obtained

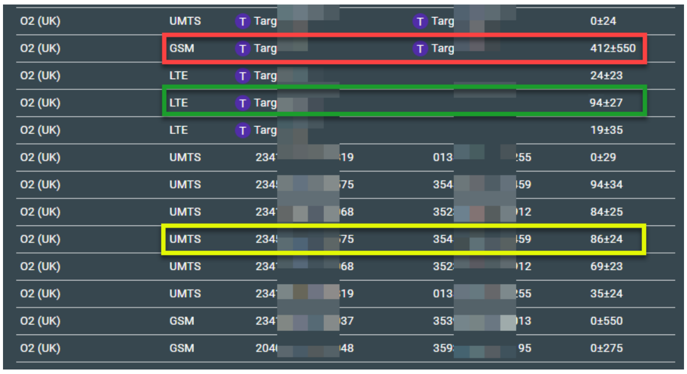
3. Whilst attempting to obtain a GPS fix from the Target device, the Target mobile device will be place into a Hold. The operator should now communicate the required channel, frequency and technology that the Target device is transmitting on to the direction finding team.

4. The direction finding team use the data sent from the NESIE team to program the direction finding equipment and commence the direction finding process to locate the Target device. They may need to request that the device is made to transmit more power if possible (2G only).

25.2 GEO-LOCATE A TARGET – MULTIPLE GRABS & DISTANCE MEASUREMENTS

When carrying out any of the Actions (Grab, Hunt, Hold, Deny, Broadcast SMS and Disable), the NESIE system initially carries out a Grab to extract the cellular devices IMEI / IMSI before carrying out the second part of the operation.

During the Grab, NESIE uses the native (2G, 3G or 4G) protocol to measure the distance from its own location to the mobile device. This distance is shown in the UI alongside the IMSI / IMEI and logged in the database as shown in Fig 236 below.



O2 (UK)	UMTS	T Targ[redacted]	T Targ[redacted]	0±24
O2 (UK)	GSM	T Targ[redacted]	T Targ[redacted]	412±550
O2 (UK)	LTE	T Targ[redacted]		24±23
O2 (UK)	LTE	T Targ[redacted]		94±27
O2 (UK)	LTE	T Targ[redacted]		19±35
O2 (UK)	UMTS	234[redacted]19	013[redacted]55	0±29
O2 (UK)	UMTS	234[redacted]75	354[redacted]59	94±34
O2 (UK)	UMTS	234[redacted]68	352[redacted]12	84±25
O2 (UK)	UMTS	234[redacted]75	354[redacted]59	86±24
O2 (UK)	UMTS	234[redacted]68	352[redacted]12	69±23
O2 (UK)	UMTS	234[redacted]19	013[redacted]55	35±24
O2 (UK)	GSM	234[redacted]37	353[redacted]13	0±550
O2 (UK)	GSM	204[redacted]48	359[redacted]95	0±275

Fig 236. Distance measurements

25.2.1 DISTANCE MEASUREMENT - GSM

The standard GSM signalling protocol used in the cellular network needs to know where a mobile device is within approximately 550m. This 550m distance is calculated using the Timing Advance process. NESIE uses this same protocol to measure the distance to a device, but due to these 550m limits, there is always a +/- 550m error added on to the distance calculated E.g. **2550-3000m (+/- 550m)**. Therefore, a range ring between 2000m – 3550m would be shown on the map.

As shown in Fig 236 above, in the red box, a device has been found on a GSM band and has been measured at 412m +550m error / -550m error

NOTE: Due to the +/-550m inaccuracy, NESIE will not show a distance measurement on the MAPPING screen for any distance to Target under 2Km as the resultant error will be too great.

25.2.2 DISTANCE MEASUREMENT - UMTS

The standard UMTS signalling protocol used in the cellular network needs to know where a mobile device is within a range of approximately 80m. NESIE uses this protocol to measure the distance to all devices on the UMTS bands. NESIE also uses another technique where it may be able to calculate the distance down to an accuracy of +/- 20m.

As shown above at Fig 236, a device in the yellow box has been found on UMTS and the distance has been measured at 86m +/- 24m of error from the NESIE system.

25.2.3 DISTANCE MEASUREMENT - LTE

The standard LTE signalling protocol used in the cellular networks need to know where a mobile device is to within a range of 80m. NESIE uses this protocol to measure the distance to all devices on the LTE bands. NESIE also uses another technique where it may be possible to calculate the distance down to an accuracy of +/-20m.

As shown in Fig 236 above, a device, in the green box has been detected on an LTE band and been measured at 94m +/-27m of error from the NESIE system.

25.3 GEO-LOCATE A TARGET – HEAT MAP PROCESS

Heat mapping is the process of conducting multiple Grabs, measuring the distances and displaying the combined, multiple range rings to show the location of the Target device.

Prerequisites:

- The identity must be listed as a Target or made into a Target after the event.
- The Target device must be static whilst conducting the multiple Grabs. If the Target is moving, the results will be compromised.
- NESIE must be able to find the Target device during a Grab.

Example:
During planning, the NESIE team have identified the approximate area of the Target or have been given his current Cell ID. They now plan to conduct a minimum of 3 Grabs at the locations shown on the map at Fig 237 below.

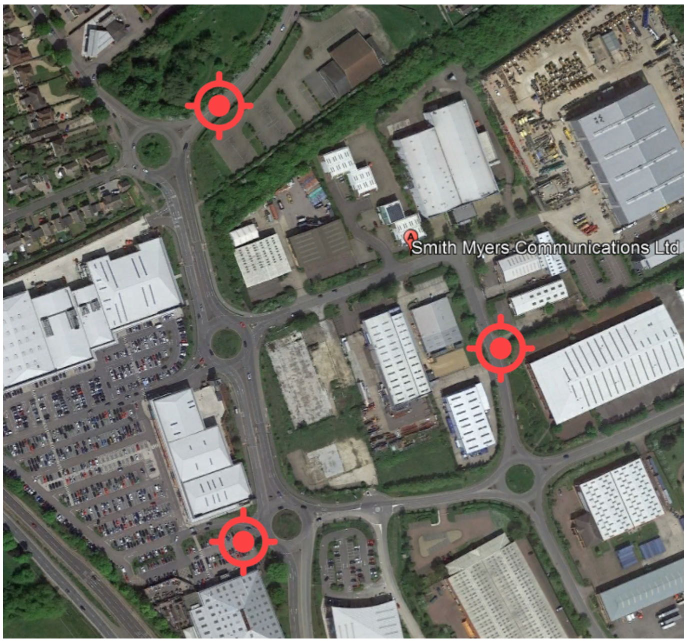
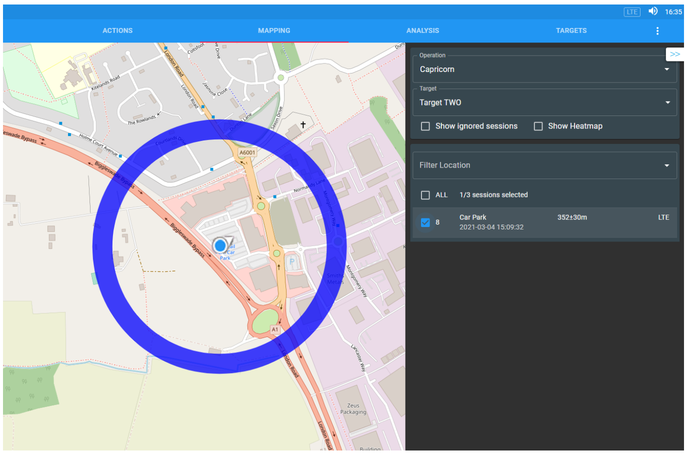


Fig 237. Pre planning map

Location 1
At location 1, conduct a Grab on the Targets network (if known). Monitor the ID List and when the Targets details are displayed, you can confirm you are within detect range of the Target. Ensure a distance measurement is displayed in the UI, and, if required, the Grab can be stopped. However, if required, the operator may wish to complete the Grab so other IDs in the area are logged.

If a full network and technology Grab was started, note the network and technology that the Target was found on.

When the Target is displayed in the UI, the operator can switch to the MAPPING page and display the range ring. Select the correct Operation name then select the Target name. The first range ring will be displayed on the map page, as shown in Fig 238 below.



Operation: Capricorn

Target: Target TWO

☐ Show ignored sessions ☐ Show Heatmap

Filter Location

☐ ALL 1/3 sessions selected

☑	8	Car Park 2021-03-04 15:09:32	352±30m	LTE

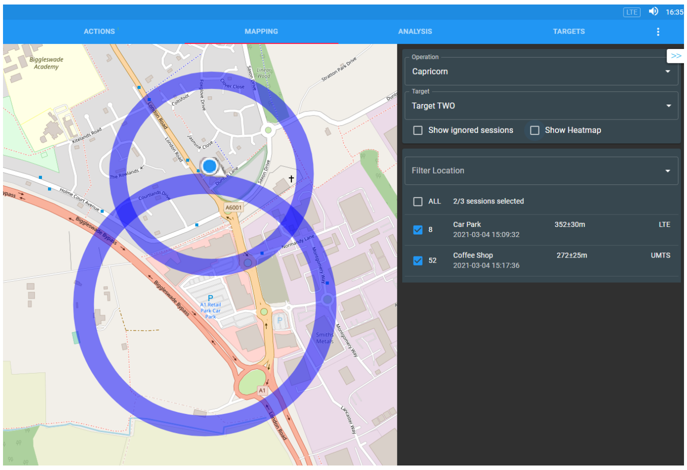
Fig 238. Location one – range ring

NOTE: If the Target has been captured on GSM and the range is under 2Km, the range ring will be ignored and not displayed on the map.

Location 2

Move the NESIE system to location 2 and conduct a second Grab using the same Operation name but ensure the location name is changed to reflect the second location. When the Target device is seen in the ID list, ensure a distance is displayed. Again, if required, the Grab can be stopped or allowed to continue to its natural conclusion.

The operator can now switch to the mapping page and ensure the correct Operation and Target name are selected. The range rings from location 1 (Car Park) and location 2 (Coffee Shop) will now be displayed.



Operation: Capricorn

Target: Target TWO

☐ Show ignored sessions ☐ Show Heatmap

Filter Location

☐ ALL 2/3 sessions selected

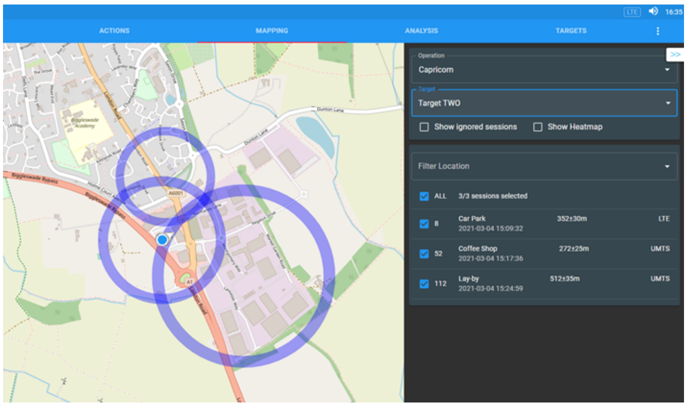
☑	8	Car Park 2021-03-04 15:09:32	352±30m	LTE
☑	52	Coffee Shop 2021-03-04 15:17:36	272±25m	UMTS

Fig 239. Location two – two range rings

Location 3

Move NESIE to location 3 and conduct a third Grab as above.

The operator can now switch to the MAPPING page and ensure the correct Operation and Target name are selected. The range rings from location 1 (Car Park), location 2 (Coffee Shop) and location 3 (lay by) will be displayed.



Operation: Capricorn

Target: Target TWO

☐ Show ignored sessions ☐ Show Heatmap

Filter Location

☑	ALL	3/3 sessions selected		
☑	8	Car Park 2021-03-04 15:09:32	352±30m	LTE
☑	52	Coffee Shop 2021-03-04 15:17:36	272±25m	UMTS
☑	112	Lay-by 2021-03-04 15:24:59	512±35m	UMTS

Fig 240. Location three – three range rings

As shown in the pictures above, the operator must:

- Choose the Operation name from the drop-down arrow.
- Choose the Target name from the drop-down arrow.
- Select the required grabs from the list.
- The range rings will be displayed.

The distance measurements obtained during the ID capture will be shown as rings on the screen. Where the three range rings intersect will be the most likely location of the Target device.

If only two range rings are shown, there could be two possible locations for the Target,; where the two range rings intersect, shown in red circles in Fig 241 below.

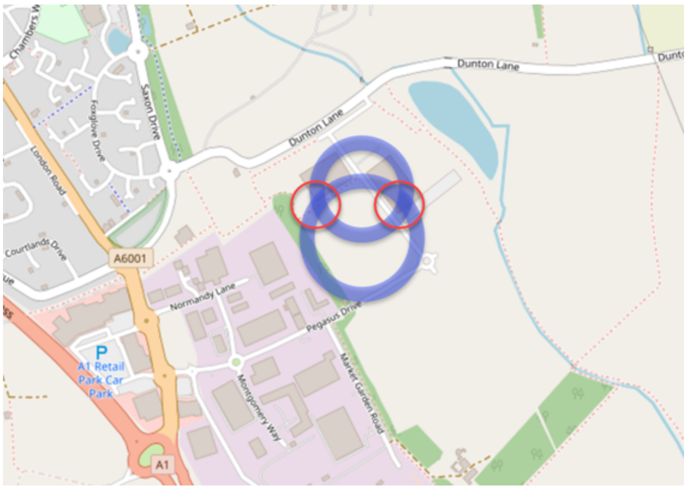
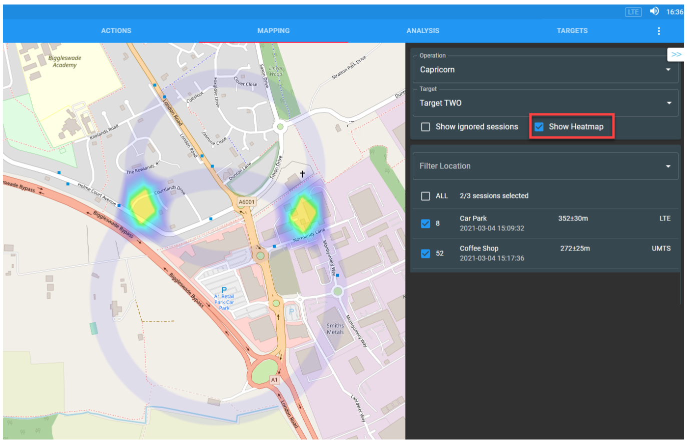


Fig 241. Two range rings

If after obtaining two range rings, the NESIE operator can tick the Show Heatmap button. The range rings will disappear and the software will now highlight where the most likely location(s) for the Target device, as shown in Fig 242 below.



Operation: Capricorn

Target: Target TWO

□ Show ignored sessions ☑ Show Heatmap

Filter Location

□ ALL 2/3 sessions selected

☑	8	Car Park 2021-03-04 15:09:32	352±30m	LTE
☑	52	Coffee Shop 2021-03-04 15:17:36	272±25m	UMTS

Fig 242. Two range rings - Heatmap

If possible, the NESIE operator should attempt to obtain a third range ring. This should then give a clear indication of the location for the Target device. As shown in the red circle in Fig 243 below.

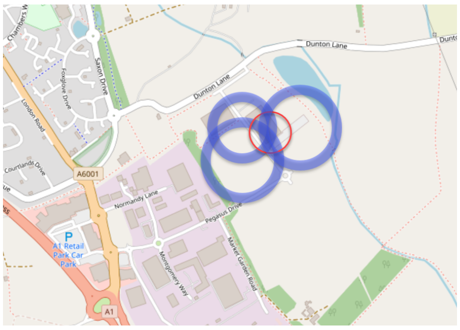
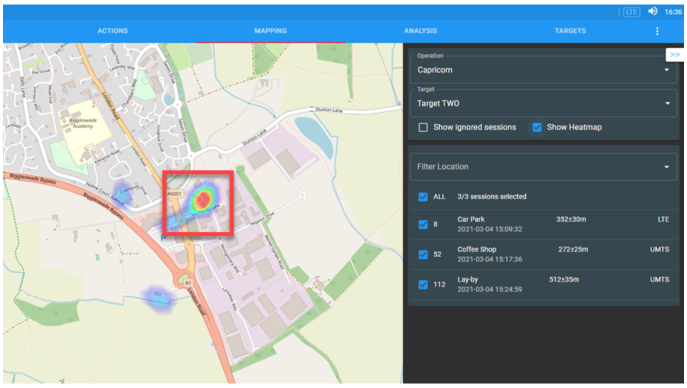


Fig 243. Three range Rings

If after obtaining three range rings, the NESIE operator can tick the Show Heatmap button. The range rings will disappear, and the software will now highlight where the most likely location(s) for the Target device, as shown in Fig 244 below.



Operation: Capricorn

Target: Target TWO

□ Show ignored sessions ☑ Show Heatmap

Filter Location

☑ ALL 3/3 sessions selected

☑	8	Car Park 2021-03-04 15:09:32	352±30m	LTE
☑	52	Coffee Shop 2021-03-04 15:17:36	272±25m	UMTS
☑	112	Lay-by 2021-03-04 15:24:59	512±35m	UMTS

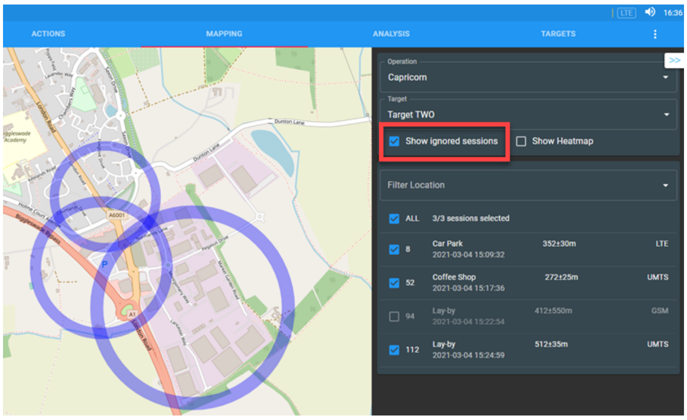
Fig 244. Three range rings – Heatmap

Even when three range rings are available, the area covered may still be too large to identify the location of the Target device. In this case, the NESIE operator has the option to move and Grab in more locations.

25.3.1 RANGE RINGS IN GSM – UNDER 2KM

When conducting a Grab on GSM, no range rings will be displayed if the calculated range is below 2Km. This is due to the possible error of +/- 550m. When combining two or three range rings, the resultant error could be over 1Km. This area is deemed as too large and of no practical use to the surveillance team.

When the operator switches to the MAPPING page, the range rings available on UMTS, LTE and GSM over 2 Km will be shown in the table. Any GSM range rings under 2Km are not shown in the list and not used to calculate the location. However, the data is still available. If required, the operator can tick the Show Ignored Sessions box. Any ignored sessions will now be displayed in the table but will be greyed out to show they have been ignored, as shown at Fig 245 below.



Operation: Capricorn

Target: Target TWO

☑ Show ignored sessions ☐ Show Heatmap

Filter Location

☑ ALL 3/3 sessions selected

☑ 8 Car Park 2021-03-04 15:09:32 352±30m LTE

☑ 52 Coffee Shop 2021-03-04 15:17:36 272±25m UMTS

☐ 94 Lay-by 2021-03-04 15:22:54 412±550m GSM

☑ 112 Lay-by 2021-03-04 15:24:59 512±35m UMTS

Fig 245. Show Ignored Sessions

NOTE: NESIE must have a GPS lock to calculate the distance to a Target.

25.4 HOLD & GEO-LOCATE ON THE MOVE

The second method to geo-locate a Target is to put the Target device into a Hold operation. This Hold is a silent call to the device. The device is tricked into transmitting on a specified voice channel. When first establishing this silent call (Hold), the NESIE system calculates the distance to the Target device, using the protocol measurement process.

If the NESIE operator wishes, they can now drive (move) the NESIE system whilst maintaining a Hold to the Target device.

NOTE: There is a risk that by moving the NESIE system, the Hold link to the Target may be lost, especially if the NESIE system is moved behind a building or other obstacle.

25.4.1 GEO-LOCATE ON THE MOVE – MAP

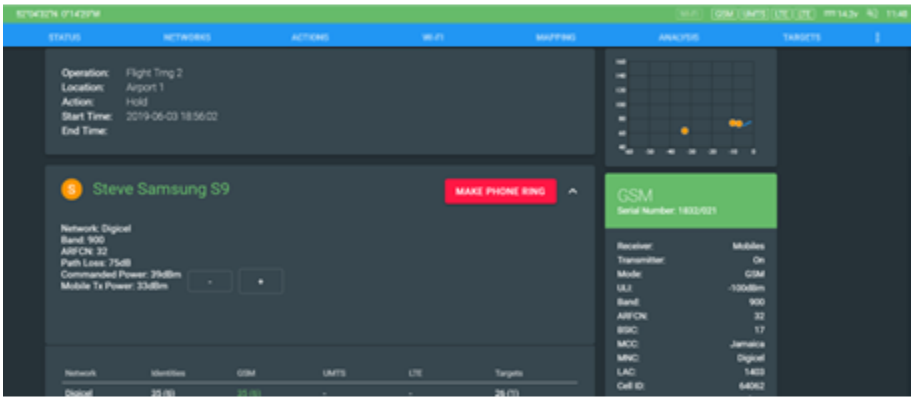
As previously discussed at section 24.5, the operator may wish to use the map and compass display to assist with geolocation on the move.

25.4.2 GEOLOCATE ON THE MOVE – GSM

The preferred method of Holding a Target device is using the GSM protocol. This enables the NESIE to interact with the Target device more than when holding in UMTS and LTE. However, the GSM distance measurement only has an accuracy of +/-550m.

To increase this accuracy, the operator can move the NESIE system whilst continuing to Hold the Target device. As the NESIE system is moved, the software recognises the movement and will automatically conduct multiple distance measurements. The further the NESIE is moved, the more distance measurements are calculated and the more accurate the fix can be. It is normal that the GSM Hold on the move is typically able to calculate the position of a Target to within 150m of accuracy.

To geolocate on the move, the operator should first ensure that Target device is in Hold as shown below in Fig 246 below.



Operation: Flight Trng 2
Location: Airport 1
Action: Hold
Start Time: 2019-06-03 18:56:02
End Time:

Steve Samsung S9

Network: Digicel
Band: 900
ARFCN: 32
Path Loss: 75dB
Commanded Power: 39dBm
Mobile Tx Power: 33dBm

Network	Identities	GSM	UMTS	LTE	Targets
Digicel	25 (6)	25 (6)	-	-	26 (1)

GSM
Serial Number: 1832/021

Receiver:	Mobiles
Transmitter:	On
Mode:	GSM
ULI:	-100dBm
Band:	900
ARFCN:	32
BSIC:	17
MCC:	Jamaica
MNC:	Digicel
LAC:	1403
Cell ID:	64062

Fig 246. Target in Hold – GSM

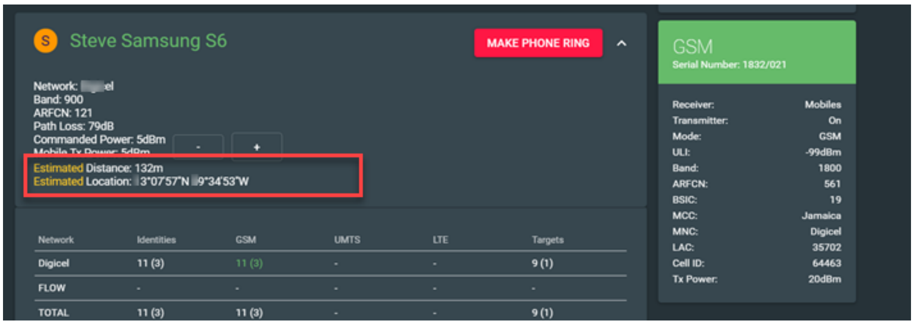
NOTE: The operator now needs to make a tactical decision as to whether it is feasible to move location and start the geolocation process. If the NESIE system moves, the Target device could drop from Hold and may not be found again.

To start the geolocation process, the NESIE system must be moved approx. 200m from its current location. As the NESIE system detects that the system has moved (using its GPS), multiple distance measurements will be taken.

The further NESIE moves, the more measurements will be calculated and the more accurate the geolocation process will be.

NOTE: The NESIE system should be moved in an arc or L shape to aid the calculations and firm up the position fix.

As the NESIE system continues to geo-locate the Target, the position of the device will be shown on the UI as shown in Fig 247 below.



S Steve Samsung S6

Network: [redacted]el
Band: 900
ARFCN: 121
Path Loss: 79dB
Commanded Power: 5dBm
Mobile Tx Power: 5dBm

Estimated Distance: 132m
Estimated Location: [redacted]3°07'57"N [redacted]9°34'53"W

Network	Identities	GSM	UMTS	LTE	Targets
Digicel	11 (3)	11 (3)	-	-	9 (1)
FLOW	-	-	-	-	-
TOTAL	11 (3)	11 (3)	-	-	9 (1)

GSM
Serial Number: 1832/021

Receiver:	Mobiles
Transmitter:	On
Mode:	GSM
ULI:	-99dBm
Band:	1800
ARFCN:	561
BSIC:	19
MCC:	Jamaica
MNC:	Digicel
LAC:	35702
Cell ID:	64463
Tx Power:	20dBm

Fig 247. Estimated fix

The colour of the Estimated label will change to indicate the quality of the fix.

Red	Poor fix	Error over 250m
Amber	Average fix	Error between 100m and 250m
Green	Good fix	Error under 100m

When the operator opens the MAPPING page, the map will show the location of the NESIE system (blue circle) and the calculated (estimated) location of the Target, as shown below in Fig 248.

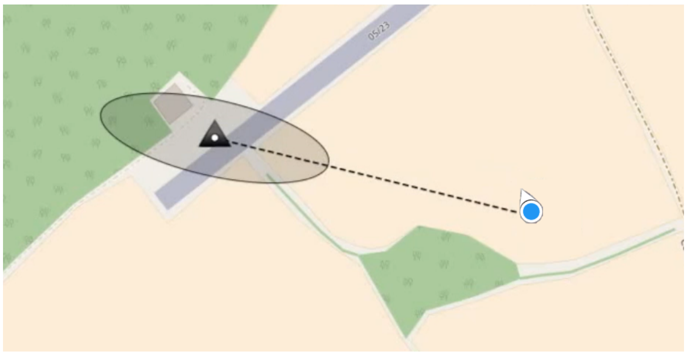


Fig 248. Geolocate Target

Initially, the estimated location may switch left and right but as the NESIE system moves in an arc, or L shape, the location will settle as the fix firms up.

Now that the Target device is in Hold, when the NESIE system is moved in the vehicle, a trail tracing the route the vehicle has followed will be displayed on the map. When the NESIE is holding the Target device, the colour of the trace will be dark blue. If at any point along that route NESIE drops the Hold on the Target device, the trace will turn light blue. The purpose of this function is to allow an operator to return to a known location along a route where they know that the Target device was in a Hold. This may allow them to re-establish a Hold on a Target device that has been dropped along the route (Fig 249).

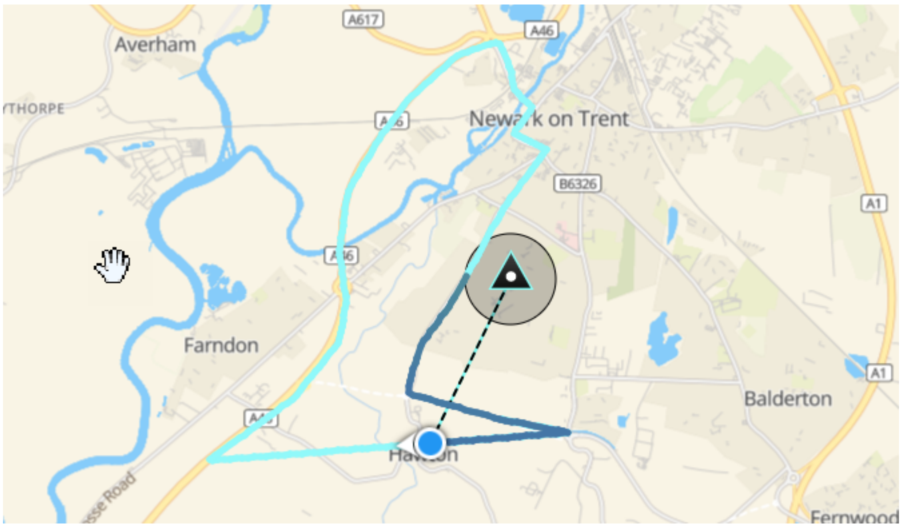


Fig 249 Route trace

The operator also has the option to turn on a heatmap function in the map key. The display will show the error ellipse around the Target area when the geolocation process has begun, and it will also show the degree of error as an area of red. The larger the red area, the larger the error and vice versa (Fig 250).

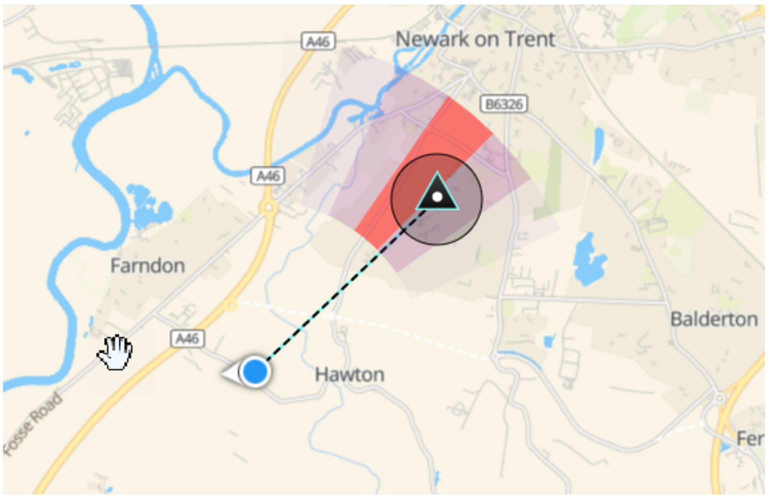


Fig 250 Geolocation Heatmap

25.4.3 ERROR ELLIPSE

Initially, the error ellipse calculated by the NESIE system may be represented by a large, elongated oval. This indicates that a large error has been calculated. This ellipse will shrink and become circular as the error decreases.

25.4.4 GEO-LOCATE ON THE MOVE - UMTS

The process of geolocatingg a Target on UMTS is the same as discussed for GSM above. However, the accuracy of the fix is usually improved.

As mentioned previously, for distance measurement of a UMTS signal, the accuracy of the range rings is +/- 20m. Therefore, as the operator moves the NESIE system, a fix will be achieved but the location that is calculated will be more accurate.

CAUTION: DUE TO THE WAY A UMTS SIGNAL IS TRANSMITTED OVER THE AIR (A 5MHZ WIDE SIGNAL WHICH IS GENERALLY WEAKER THAN GSM) THERE IS SIGNIFICANTLY MORE RISK OF LOSING THE TARGET DEVICE AS THE NESIE SYSTEM IS MOVED.

25.4.5 GEOLOCATE ON THE MOVE - LTE

The process ofmgeolocating a Target on LTE is the same as discussed for GSM above. However, the accuracy of the fix is usually improved.

As mentioned previously, for distance measurement of an LTE signal, the accuracy of the range rings is +/- 20m. Therefore, as the operator moves the NESIE system, multiple measurements will be taken and a fix will be achieved but, the location that is calculated will be more accurate.

CAUTION: DUE TO THE WAY AN LTE SIGNAL IS TRANSMITTED OVER THE AIR (A WIDEBAND SIGNAL WHICH IS GENERALLY WEAKER THAN GSM) THERE IS SIGNIFICANTLY MORE RISK OF LOSING THE TARGET DEVICE AS THE NESIE SYSTEM IS MOVED.

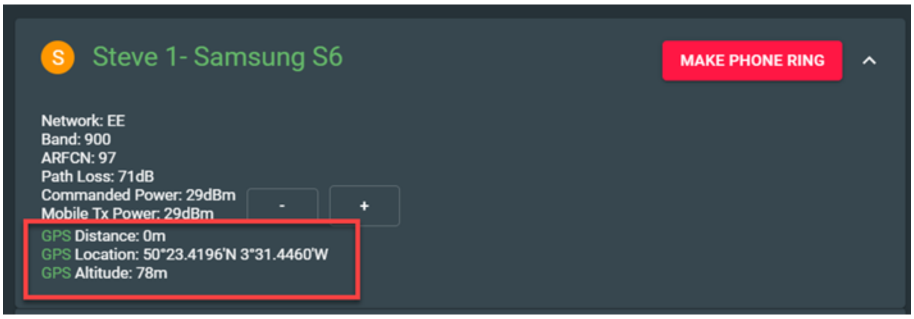
25.5 HOLD & EXTRACT GPS

The third method of locating a Target mobile device is to attempt to extract the GPS results from the mobile device itself. Most modern mobile devices are fitted with a GPS chip. This chip can be exploited, and the mobile device can be requested to send its GPS location to the NESIE system.

Whenever a Hold operation is carried out and a mobile device is successfully held, NESIE will automatically attempt to extract the GPS from the ‘registered’ mobile device. It takes approximately 15 seconds for this process to be completed, and, if successful, the Latitude and Longitude for the Target mobile device will be displayed on the UI, as shown at Fig 251 below.

NOTE: Not all devices will comply with a GPS request command sent by the NESIE system to return their GPS position. It depends on the make, model, software installed and sometimes the GPS chip fitted in the cellular device.

The NESIE operator should also note that most modern devices will not return a GPS fix due to the newer security features in the software.



Steve 1- Samsung S6

Network: EE
Band: 900
ARFCN: 97
Path Loss: 71dB
Commanded Power: 29dBm
Mobile Tx Power: 29dBm
GPS Distance: 0m
GPS Location: 50°23.4196'N 3°31.4460'W
GPS Altitude: 78m

Fig 251. GPS returned by mobile device

NOTE: To enable NESIE to control a mobile device and extract the GPS data, the mobile device must be held using GSM. This allows NESIE to circumnavigate the security controls in the protocol.

25.5.1 HOLD & EXTRACT GPS – PROCESS

The NESIE operator should conduct a GSM Hold operation as previously discussed.

When the Target device is successfully in a GSM Hold, the NESIE software automatically attempts to extract the GPS approximately every 10-15 seconds.

This GPS extraction will be attempted continually, even if the device does not respond. Therefore, if the Target device is inside a building and does not return a GPS fix, if it is subsequently moves outside, it may return its GPS at this point.

The NESIE operator will be notified of a successful GPS extraction by the coordinates appearing in the UI as shown above in Fig 251 above.

If a GPS result is obtained from the device, the NESIE operator can now view the location of the Target device on the mapping page, as shown in Fig 252 below.

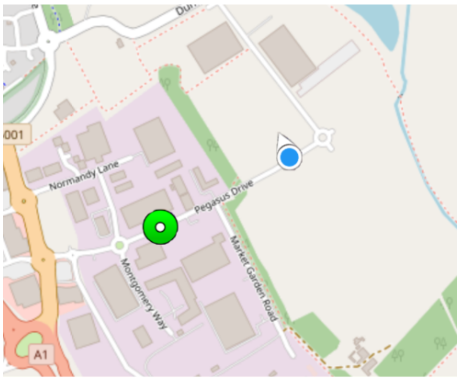


Fig 252. GPS displayed on map

NOTE: If the Target device is moved whilst it is returning its GPS location as shown above, and the Hold is maintained, the fix icon will move on the map to represent its current location.

25.6 HOLD & TRADITIONAL DIRECTION FINDING

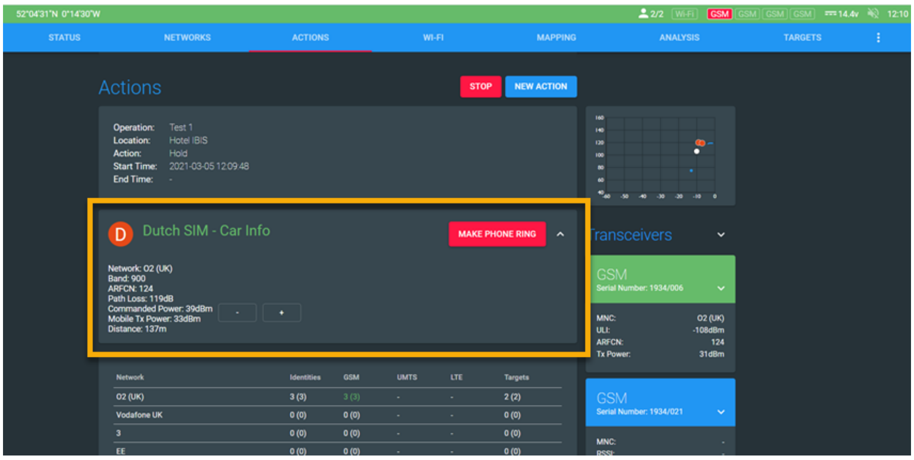
The fourth method of locating a Target is by forcing the Target mobile device into a Hold (permanent transmit / silent call), then, whilst the Target device is transmitting, a second team with the direction finding (DF) equipment tune into the frequency the Target mobile device is transmitting on. Then, using the DF equipment, they proceed to locate the Target mobile device.

Note: This process can be conducted in GSM, UMTS and LTE. GSM is preferred, as the NESIE system has more control over the Target device.

25.6.1 HOLD & TRADITIONAL DF – GSM

Where possible, a Hold should be completed using the GSM protocol as this allows increased interaction with the Target device.

After initiating a Hold operation against the Target device. When the Target device is successfully in a Hold, an additional pane will be displayed on the UI to show the device is being held, as shown in Fig 254 below.



Operation: Test 1
Location: Hotel IBIS
Action: Hold
Start Time: 2021-03-05 12:09:48
End Time: -

Network: O2 (UK)
Band: 900
ARFCN: 124
Path Loss: 119dB
Commanded Power: 39dBm
Mobile Tx Power: 33dBm
Distance: 137m

Network	Identities	GSM	UMTS	LTE	Targets
O2 (UK)	3 (3)	3 (3)	-	-	2 (2)
Vodafone UK	0 (0)	0 (0)	-	-	0 (0)
3	0 (0)	0 (0)	-	-	0 (0)
EE	0 (0)	0 (0)	-	-	0 (0)

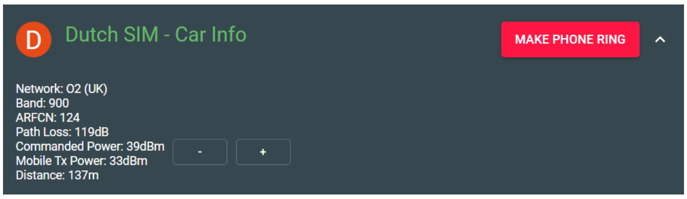
Serial Number: 1934/006
MNC: O2 (UK)
ULI: -108dBm
ARFCN: 124
Tx Power: 31dBm

Serial Number: 1934/021
MNC: -
RSSI: -

Fig 253. Hold – GSM

The Hold pane displays the details of the device and the network, frequency band, channel number and current power as shown below in Fig 254 below.

The NESIE operator would normally coordinate with the DF team to inform them that the Target device is successfully held and what settings are required for the DF equipment, so it can be tuned to the correct band and channel number and locate the device.



Network: O2 (UK)
Band: 900
ARFCN: 124
Path Loss: 119dB
Commanded Power: 39dBm
Mobile Tx Power: 33dBm
Distance: 137m

Fig 254. Hold – DF info

25.6.1.1 INFORM THE DF TEAM

As shown in Fig 254 above, the Target device is being held on:

Technology:	GSM
Band:	900MHz
ARFCN:	124

This information must be passed to the DF team, who would then set up the equipment to mirror these settings.

25.6.1.2 INCREASE / DECREASE THE DEVICE TRANSMIT POWER

In some circumstances, the DF team may not be able to hear the transmitted signal from the Target device. Therefore, the NESIE operator may need to change the power of the signal that is being transmitted by the Target device (2G only).

Commanded Power: Command sent by NESIE – 'transmit at xx power'
Mobile Tx Power: Reply from device 'I am transmitting at xx power'

To increase the transmit power of the Target device, the operator should press the + button. NESIE will then send a command to the device, to increase its output power.

E.g.: **Commanded Power: 33db**

When the Target device accepts this command, it will adjust the transmit power and send a reply to NESIE showing its new transmit power.

E.g. **Mobile Tx Power: 33dB**

> **NOTE: The Target device may be sent a command to increase its transmit power to 37dB, however, the device may not actually be able to transmit that much power. In this case, the device will report the maximum power it can achieve e.g. 35db.**

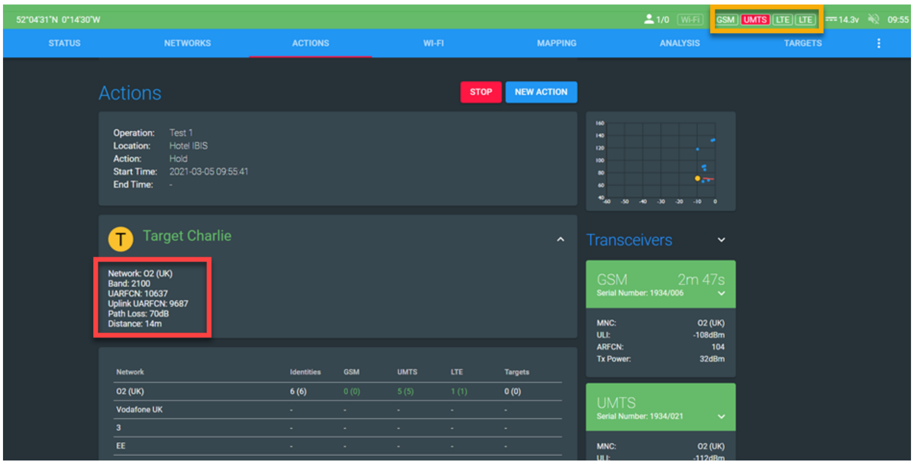
If required, the operator can also reduce the power of the Target device by pressing the - button.

25.7 HOLD & TRADITIONAL DF – UMTS

As per the GSM section above, a Hold can be carried out on UMTS. However, due to the increased security in the protocol, there are less options available to the operator. There is no longer an option to control the output power of the device or make the device ring.

As shown below in Fig 255 the UMTS Hold is being carried on:

Band:	2100Hz
Uplink UARFCN:	9687



Operation: Test 1
Location: Hotel IBIS
Action: Hold
Start Time: 2021-03-05 09:55:41
End Time: -

Network: O2 (UK)
Band: 2100
UARFCN: 10637
Uplink UARFCN: 9687
Path Loss: 70dB
Distance: 14m

Network	Identities	GSM	UMTS	LTE	Targets
O2 (UK)	6 (6)	0 (0)	5 (5)	1 (1)	0 (0)
Vodafone UK	-	-	-	-	-
3	-	-	-	-	-
EE	-	-	-	-	-

GSM Serial Number: 1934/006
MNC: O2 (UK)
ULI: -108dBm
ARFCN: 104
Tx Power: 32dBm

UMTS Serial Number: 1934/021
MNC: O2 (UK)
ULI: -112dBm

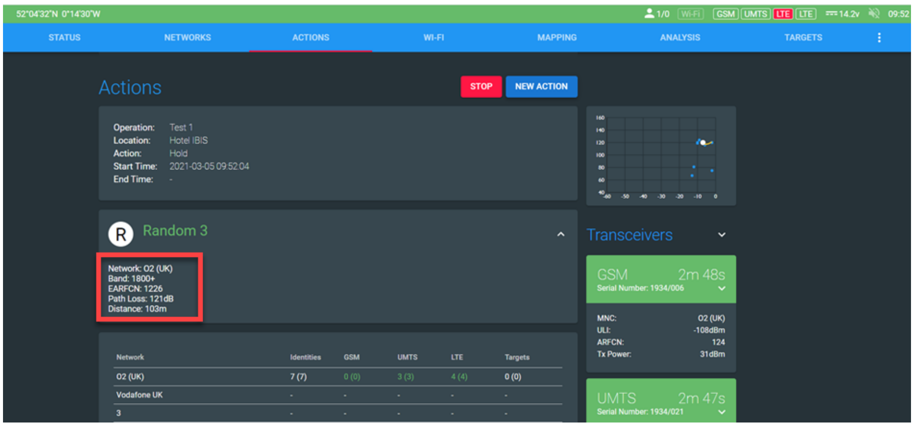
Fig 255. UMTS Hold

25.8 HOLD & TRADITIONAL DF – LTE

As per the GSM section above, a Hold can be carried out on LTE. However, due to the increased security in the protocol, there are less options available to the operator. There is no longer an option to control the output power of the device or make the device ring.

As shown below in Fig 256, the UMTS Hold is being carried on:

Band:	1800+
EARFCN:	1226



Operation: Test 1
Location: Hotel IBIS
Action: Hold
Start Time: 2021-03-05 09:52:04
End Time: -

Network: O2 (UK)
Band: 1800+
EARFCN: 1226
Path Loss: 121dB
Distance: 103m

Network	Identities	GSM	UMTS	LTE	Targets
O2 (UK)	7 (7)	0 (0)	3 (3)	4 (4)	0 (0)
Vodafone UK	-	-	-	-	-
3	-	-	-	-	-

GSM Serial Number: 1934/006
MNC: O2 (UK)
ULI: -108dBm
ARFCN: 124
Tx Power: 31dBm

UMTS Serial Number: 1934/021

Fig 256. LTE Hold

25.9 HOLD – SINGLE CHANNEL SYSTEM

If the NESIE system is made up from only one transceiver module, only that module can carry out the grabbing and holding. Normally, only one device can be held per module.

Therefore, if the Target is detected on LTE, NESIE will automatically attempt to Hold the device on LTE.

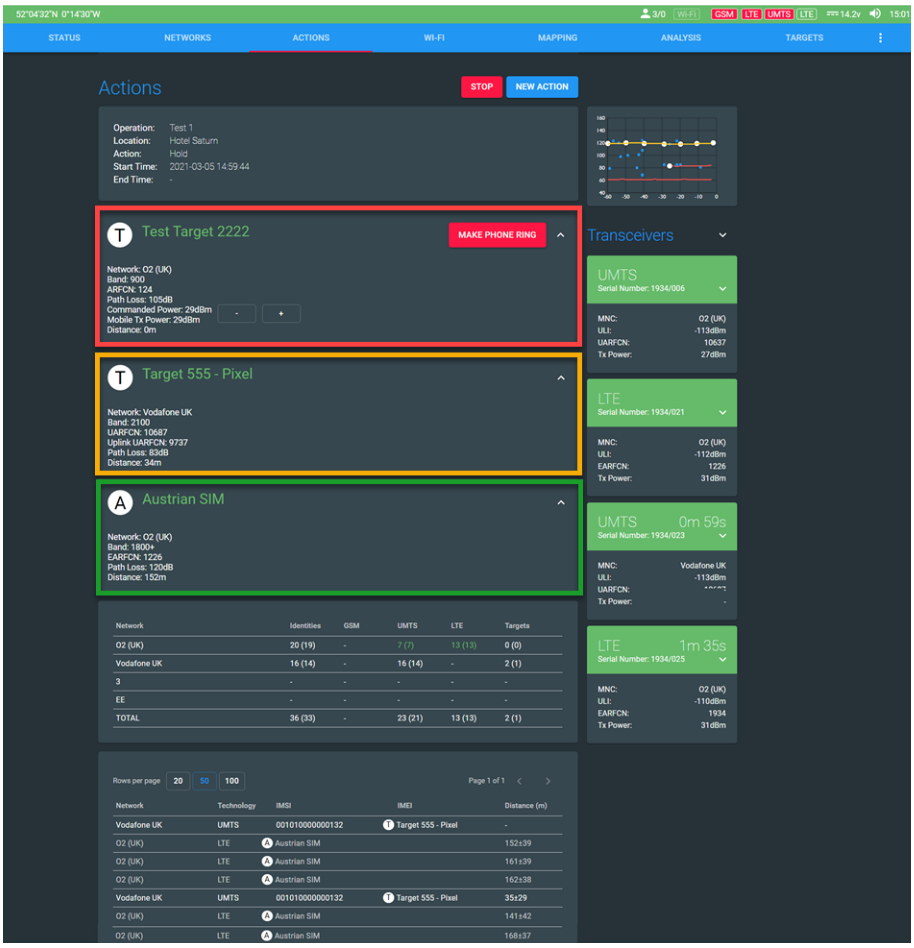
It is not possible to detect a device on LTE and send a command to move to a Hold on a different technology (in this example GSM). As the single NESIE module would now have to swap technologies and start transmitting as a GSM tower to catch the Target device on GSM.

In this scenario, you would ideally have at least 2 x NESIE modules, one to detect and command the device to move. The second module to be waiting on the desired technology, waiting to catch the device when it receives the command and changes technology.

25.9.1 HOLD – MULTI CHANNEL SYSTEM

If the NESIE system is formed of multiple transceivers, it is possible to Hold multiple Targets simultaneously. However, only 1 Target can be held per NESIE module.

The 4 channel NESIE system shown in Fig 257 below, is Holding 3 devices, one device on GSM, the second device on UMTS and the third device on LTE.



Operation: Test 1
Location: Hotel Saturn
Action: Hold
Start Time: 2021-03-05 14:59:44
End Time: -

Test Target 2222

Network: O2 (UK)
Band: 900
ARFCN: 124
Path Loss: 105dB
Commanded Power: 29dBm
Mobile Tx Power: 29dBm
Distance: 0m

Target 555 - Pixel

Network: Vodafone UK
Band: 2100
UARFCN: 10687
Uplink UARFCN: 9737
Path Loss: 83dB
Distance: 34m

Austrian SIM

Network: O2 (UK)
Band: 1800+
EARFCN: 1226
Path Loss: 120dB
Distance: 152m

Network	Identities	GSM	UMTS	LTE	Targets
O2 (UK)	20 (19)	-	7 (7)	13 (13)	0 (0)
Vodafone UK	16 (14)	-	16 (14)	-	2 (1)
3	-	-	-	-	-
EE	-	-	-	-	-
TOTAL	36 (33)	-	23 (21)	13 (13)	2 (1)

Network	Technology	IMSI	IMEI	Distance (m)
Vodafone UK	UMTS	001010000000132	T Target 555 - Pixel	-
O2 (UK)	LTE	A Austrian SIM		152±39
O2 (UK)	LTE	A Austrian SIM		161±39
O2 (UK)	LTE	A Austrian SIM		162±38
Vodafone UK	UMTS	001010000000132	T Target 555 - Pixel	35±29
O2 (UK)	LTE	A Austrian SIM		141±42
O2 (UK)	LTE	A Austrian SIM		168±37

UMTS
Serial Number: 1934/006

MNC:	O2 (UK)
ULI:	-113dBm
UARFCN:	10637
Tx Power:	27dBm

LTE
Serial Number: 1934/021

MNC:	O2 (UK)
ULI:	-112dBm
EARFCN:	1226
Tx Power:	31dBm

UMTS 0m 59s
Serial Number: 1934/023

MNC:	Vodafone UK
ULI:	-113dBm
UARFCN:	[illegible]
Tx Power:	-

LTE 1m 35s
Serial Number: 1934/025

MNC:	O2 (UK)
ULI:	-110dBm
EARFCN:	1934
Tx Power:	31dBm

Fig 257. Hold - 3 devices

26. DENY

The Deny action is a denial of service mode which is designed to deny cellular network service to a Target, multiple Targets or if required, all mobile devices in the vicinity of the NESIE system.

As for all actions on the NESIE system, the Deny is initially a Grab which collects the identities of all cellular devices in the detect range of NESIE. Once the identity of a device has been logged and the distance calculated, any non-Target devices will be rejected back to their real network. Target mobile devices will be allowed to register onto the NESIE system and commanded not to move away from the NESIE BTS.

Once registered onto NESIE, the Target device should remain registered unless it moves out of detect range or NESIE stops transmitting. At this point, the device will start to search for and re-register with the real network.

Whilst a device is registered onto the NESIE system, it will not be able to receive calls or SMS messages from the real network. If the Target device makes a phone call or sends an SMS, it will be sent to the NESIE system.

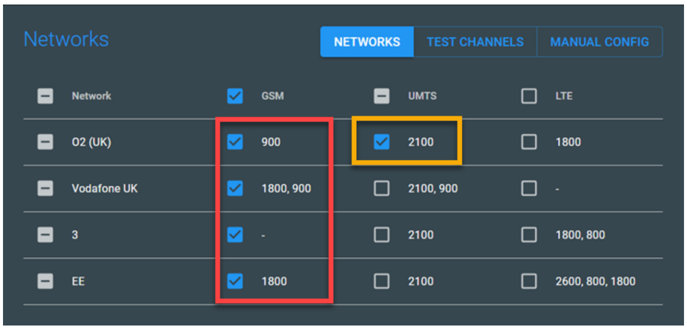
> **Limitation – Number of transceivers**
>
> **Deny uses the GSM protocol to communicate to the Target devices. Target mobile devices can be found on any technology, but the Targeted mobile devices must be moved from LTE and UMTS to the GSM transceiver to receive the protocol messages.**
>
> **Therefore, at least 2 transceivers are required. One transceiver on LTE or UMTS to find the Target and send it down to the second transceiver. The second transceiver transmitting on GSM is ready to ‘catch’ the Target device if it is sent down from LTE or UMTS.**
>
> **One transceiver cannot find the Target device on LTE, send the command to move the device to GSM, switch between network technologies e.g. LTE to GSM in time to catch the Target device.**
>
> **Even when a command is sent to a Target device sending it down from LTE to GSM, the software in the Target device may decide to move to UMTS instead. Therefore, a third transceiver is usually needed to ensure that GSM, UMTS and LTE is covered.**

26.1 LIMITATION – NUMBER OF TRANSCEIVERS/NETWORKS

The number of transceivers in the system will determine how many networks can be denied at any one time.

• 1 transceiver = 1 Network	Covering GSM
• 2 transceivers = 1 Network	Covering GSM & UMTS or LTE
• 3 transceivers = 1 Network	Covering GSM, UMTS and LTE
• 6 transceivers = 2 Networks	
• 9 transceivers = 3 Networks	

In the example below at Fig 258, using a 5 transceiver system, four transceivers have been allocated to GSM on each of the four networks providers. The fifth transceiver has been allocated to UMTS on one (the O2 UK) network.



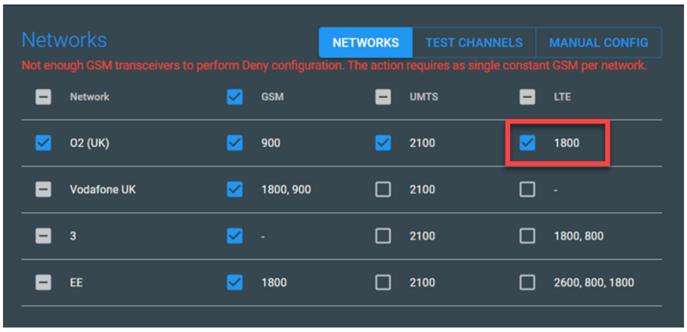
Networks

⊟ Network	☑ GSM	⊟ UMTS	□ LTE
⊟ O2 (UK)	☑ 900	☑ 2100	□ 1800
⊟ Vodafone UK	☑ 1800, 900	□ 2100, 900	□ -
⊟ 3	☑ -	□ 2100	□ 1800, 800
⊟ EE	☑ 1800	□ 2100	□ 2600, 800, 1800

Fig 258. Deny – 5 transceivers

In the example below at Fig 259, using a 5 transceiver system, four transceivers have been allocated to GSM on each of the four networks providers. The fifth transceiver has been allocated to UMTS on one network, and the operator has attempted to allocate a sixth to LTE.

A red warning has been displayed to indicate that not enough transceivers are available for this task. The system only has five transceivers and the operator attempted to use six.



Networks

Not enough GSM transceivers to perform Deny configuration. The action requires as single constant GSM per network.

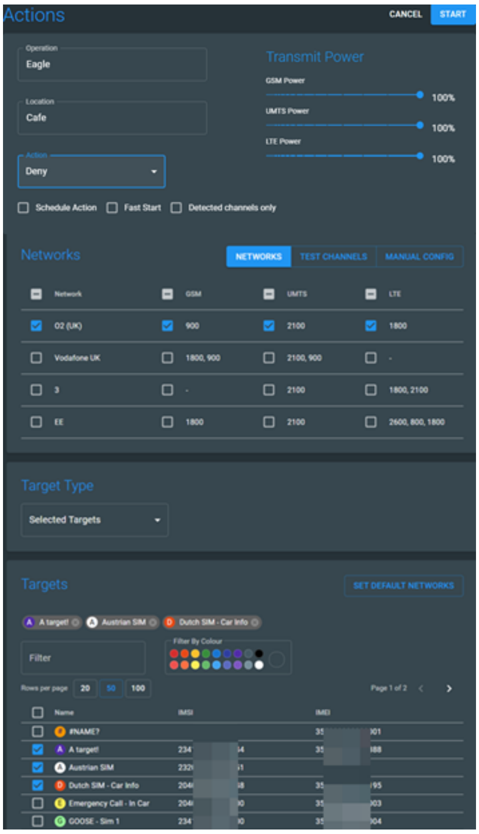
⊟ Network	☑ GSM	⊟ UMTS	⊟ LTE
☑ O2 (UK)	☑ 900	☑ 2100	☑ 1800
⊟ Vodafone UK	☑ 1800, 900	□ 2100	□ -
⊟ 3	☑ -	□ 2100	□ 1800, 800
⊟ EE	☑ 1800	□ 2100	□ 2600, 800, 1800

Fig 259. Deny – not enough transceivers

26.2 DENY – SET UP

As shown in Fig 260 below, the user has started a Deny operation by following the actions bellow:

- ACTIONS page
- NEW ACTIONS button has been pressed
- Entered the Operation / Location Name
- Chosen the Deny action from the drop-down menu
- Adjusted the Transmit Power if required
- Selected Fast Start, No Rescan etc buttons as required
- Selected the networks and technologies required
- Selected the Target Type
- Selected the Targets



Actions

Operation: Eagle

Location: Cafe

Action: Deny

Transmit Power

GSM Power 100%

UMTS Power 100%

LTE Power 100%

□ Schedule Action □ Fast Start □ Detected channels only

Networks

⊟ Network	⊟ GSM	⊟ UMTS	⊟ LTE
☑ O2 (UK)	☑ 900	☑ 2100	☑ 1800
□ Vodafone UK	□ 1800, 900	□ 2100, 900	□ -
□ 3	□ -	□ 2100	□ 1800, 2100
□ EE	□ 1800	□ 2100	□ 2600, 800, 1800

Target Type

Selected Targets

Targets

Filter

Filter By Colour

Rows per page 20 50 100

Page 1 of 2

□ Name	IMSI	IMEI
□ #NAME?		35[redacted]001
☑ A target!	234[redacted]4	35[redacted]188
☑ Austrian SIM	232[redacted]1	
☑ Dutch SIM - Car Info	204[redacted]8	35[redacted]95
□ Emergency Call - In Car	204[redacted]0	35[redacted]003
□ GOOSE - Sim 1	234[redacted]0	35[redacted]004

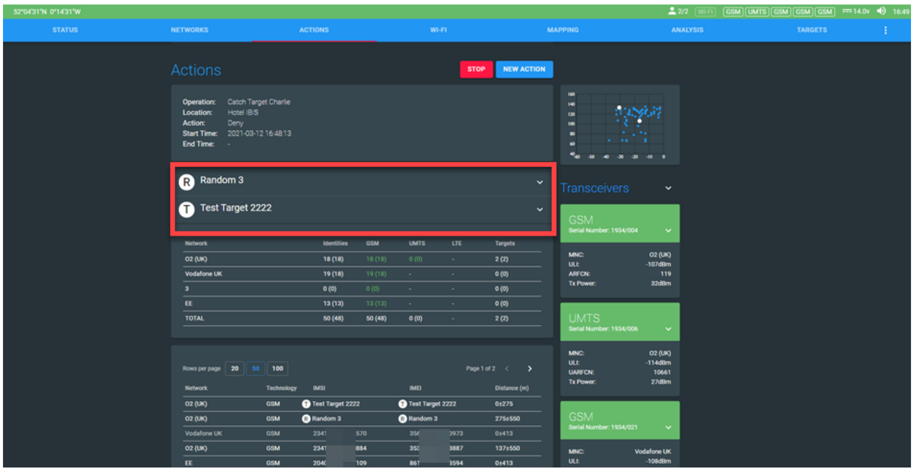
Fig 260. Deny – select Targets

26.3 DENY – ACTION SUMMARY

As the Deny action commences, the Action summary page will appear as shown in Fig 261 below.

The Action summary page for a Deny action will display an additional pane as shown in the red box. This additional pane will show the identity of any devices that have successfully be denied service.

Whilst the cellular devices are registered onto NESIE, they will not be connected to the real network. Therefore, any device that makes a device call or sends an SMS will in fact send the call or SMS to the NESIE system.



Operation: Catch Target Charlie
Location: Hotel IBIS
Action: Deny
Start Time: 2021-03-12 16:48:13
End Time: -

R Random 3

T Test Target 2222

Network	Identities	GSM	UMTS	LTE	Targets
O2 (UK)	18 (18)	18 (18)	0 (0)	-	2 (2)
Vodafone UK	19 (18)	19 (18)	-	-	0 (0)
3	0 (0)	0 (0)	-	-	0 (0)
EE	13 (13)	13 (13)	-	-	0 (0)
TOTAL	50 (48)	50 (48)	0 (0)	-	2 (2)

Network	Technology	IMSI	IMEI	Distance (m)
O2 (UK)	GSM	T Test Target 2222	T Test Target 2222	0±275
O2 (UK)	GSM	R Random 3	R Random 3	275±550
Vodafone UK	GSM	2341[redacted]570	356[redacted]0973	0±413
O2 (UK)	GSM	2341[redacted]884	353[redacted]3887	137±550
EE	GSM	2040[redacted]109	861[redacted]3594	0±413

GSM
Serial Number: 1934/004
MNC: O2 (UK)
ULI: -107dBm
ARFCN: 119
Tx Power: 32dBm

UMTS
Serial Number: 1934/006
MNC: O2 (UK)
ULI: -114dBm
UARFCN: 10661
Tx Power: 27dBm

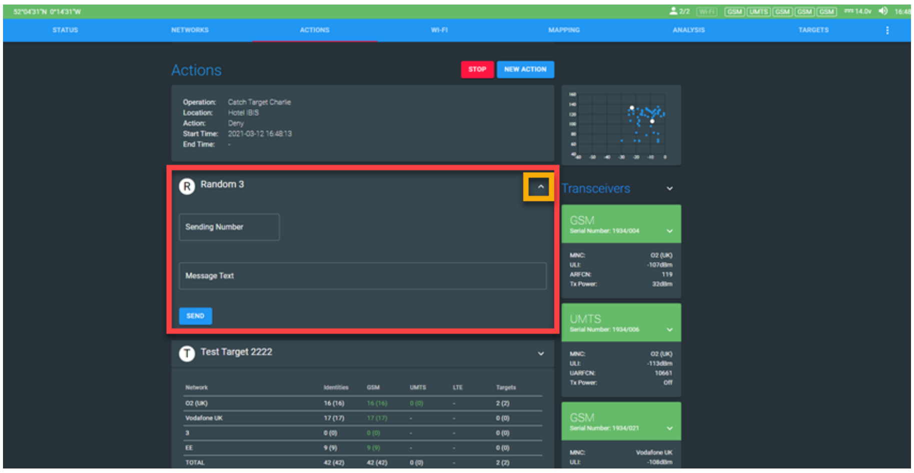
GSM
Serial Number: 1934/021
MNC: Vodafone UK
ULI: -108dBm

Fig 261. Deny - Actions summary

26.4 DENY – CALLS & SMS

As shown below at Fig 262, the NESIE operator can expand or reduce the details / activity shown of any individual identity that is currently denied. To expand or reduce the details, the operator can use the white up / down arrow shown in the orange box.

By default, when the operator expands an individual identity, they will be shown the Send SMS option as displayed below in the red box.



Operation: Catch Target Charlie
Location: Hotel IBIS
Action: Deny
Start Time: 2021-03-12 16:48:13
End Time: -

R Random 3

Sending Number

Message Text

T Test Target 2222

Network	Identities	GSM	UMTS	LTE	Targets
O2 (UK)	16 (16)	16 (16)	0 (0)	-	2 (2)
Vodafone UK	17 (17)	17 (17)	-	-	0 (0)
3	0 (0)	0 (0)	-	-	0 (0)
EE	9 (9)	9 (9)	-	-	0 (0)
TOTAL	42 (42)	42 (42)	0 (0)	-	2 (2)

GSM
Serial Number: 1934/004
MNC: O2 (UK)
ULI: -107dBm
ARFCN: 119
Tx Power: 32dBm

UMTS
Serial Number: 1934/006
MNC: O2 (UK)
ULI: -113dBm
UARFCN: 10661
Tx Power: Off

GSM
Serial Number: 1934/021
MNC: Vodafone UK
ULI: -108dBm

Fig 262. Deny – calls & SMS

26.4.1 DENY - SMS

If required, the NESIE operator can now send an SMS to the Target device.

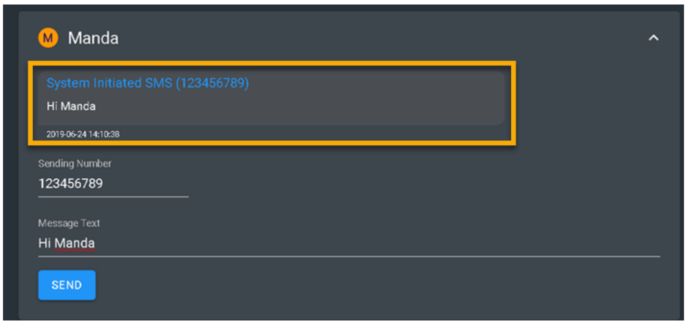
- Sending Number:	Any number can be typed into this field.
- Message Text:	Free text box allows the operator to enter any text.

When ready, the operator should press the SEND button.

In the example shown below at Fig 263, the operator has entered:

Sending number:	123456789
Message Text:	Hi Manda

When the message has been sent, it will be displayed as a System Initiated SMS (and the number sent from) and will have a date stamp below the SMS as shown below in Fig 263.



M Manda

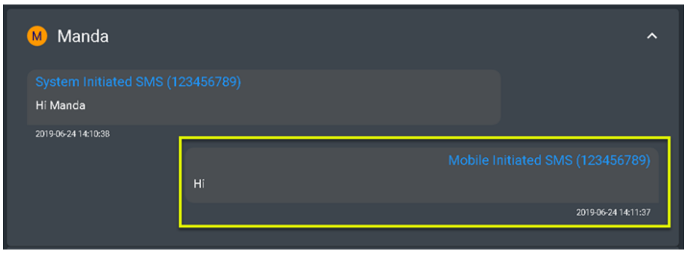
System Initiated SMS (123456789)
Hi Manda
2019-06-24 14:10:38

Sending Number
123456789

Message Text
Hi Manda

Fig 263. System Initiated SMS

If the Target device replies, then an SMS annotated as Mobile Initiated SMS (and number sent from) will be displayed, as well as a date stamp when the SMS was received at NESIE, as shown in Fig 264 below.



M Manda

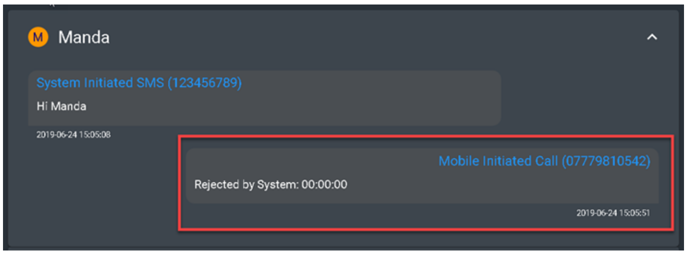
System Initiated SMS (123456789)
Hi Manda
2019-06-24 14:10:38

Mobile Initiated SMS (123456789)
Hi
2019-06-24 14:11:37

Fig 264. Mobile Initiated SMS

26.4.2 DENY - CALLS

If the Target device initiates a phone call, the call will be sent to the NESIE system. NESIE will display Mobile Initiated Call (Number dialled). However, the call will be automatically rejected upon receipt; and the message Rejected by System will be displayed on the NESIE screen as shown in Fig 265 below. Therefore, the Target device dialling out will not be able to establish a call.



M Manda

System Initiated SMS (123456789)
Hi Manda
2019-06-24 15:05:08

Mobile Initiated Call (07779810542)
Rejected by System: 00:00:00
2019-06-24 15:05:51

Fig 265. Mobile Initiated Call

NOTE: The NESIE system cannot intercept the call content.

27. DISABLE

The Disable action is another denial of service type operation that allows the NESIE operator to send a protocol message to the Target device(s) which will Disable them in order to Deny them access to the real cellular network.

This method of disabling the mobile device involves a protocol message being sent to the Target device(s) which effectively stuns the SIM card in the device and knocks it off the network. The user will be able to see that the cellular device no longer has network coverage, and the device will normally display a No Network Available (or similar) message on the equipment screen.

NOTE: The Disable command is only a temporary action. If the device is power cycled, it will attempt to re-establish connectivity with the real network.

Depending on the make / model of the device, it may need to power off, then on again or enable airplane mode.

These actions will force the device to search for a network again, however, if the mobile device is still in the vicinity of the transmitting NESIE, the mobile device will be identified again and the Deny command will be sent again. If NESIE is not in the area, or has stopped transmitting the Disable operation, the devices will be allowed back onto the real network.

CAUTION: UNLIKE OTHER OPERATIONS, THE TARGET WILL BE AWARE THAT THEY ARE NOT CONNECTED TO THE REAL CELLULAR NETWORK. THEIR DEVICE WILL BE DISABLED AND NOT ALLOWED TO CONNECT, THEREFORE A ‘NETWORK UNAVAILABLE’ TYPE MESSAGE WILL BE DISPLAYED ON THE MOBILE DEVICE.

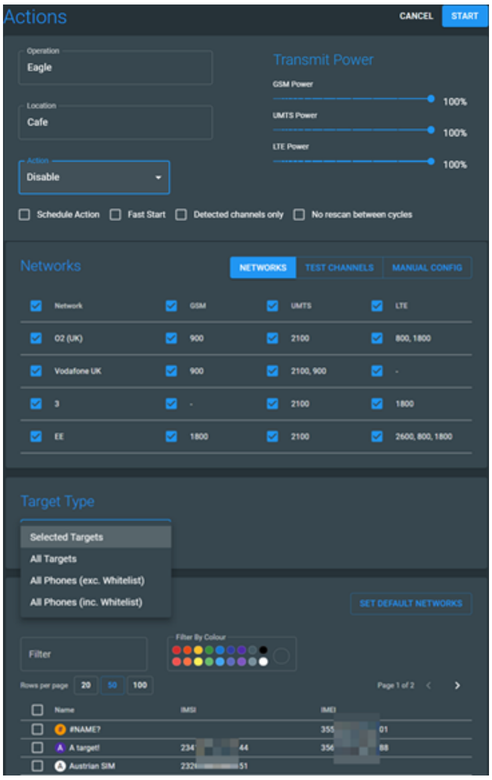
NESIE can send the Disable message using GSM and UMTS and LTE protocols.

Because NESIE detects the device, then sends the Disable command (effectively ending any connection with the device), there is no requirement to remain on one network. Therefore, if required the operator can choose multiple networks and rotate through them continually.

27.1 DISABLE SET UP

As per Fig 266 below, the user has started a Disable operation by following the actions bellow:

- ACTIONS page
- NEW ACTIONS button has been pressed
- Entered the Operation / Location Name
- Chosen the Disable action from the drop-down menu
- Adjusted the Transmit Power if required
- Selected Fast Start, No Rescan etc buttons as required
- Selected the networks and technologies required
- Selected the Target Type / Targets as required



Operation: Eagle

Location: Cafe

Action: Disable

Transmit Power

GSM Power 100%

UMTS Power 100%

LTE Power 100%

□ Schedule Action □ Fast Start □ Detected channels only □ No rescan between cycles

☑ Network	☑ GSM	☑ UMTS	☑ LTE
☑ O2 (UK)	☑ 900	☑ 2100	☑ 800, 1800
☑ Vodafone UK	☑ 900	☑ 2100, 900	☑ -
☑ 3	☑ -	☑ 2100	☑ 1800
☑ EE	☑ 1800	☑ 2100	☑ 2600, 800, 1800

□ Name	IMSI	IMEI
□ #NAME?		355[redacted]01
□ A target!	234[redacted]44	356[redacted]88
□ Austrian SIM	232[redacted]51	

Fig 266. Disable set up

27.2 DISABLE – ACTION SUMMARY

As the Disable action commences, the Action summary page will appear in the UI. There is no additional indication that a device has been Disabled apart from appearing in the identity list or Target list depending on the Target type selected.

The NESIE will carry on rotating through the chosen networks / technology until the STOP button is pressed or the system is powered off.

28. BROADCAST SMS

Broadcast SMS is another denial of service type action which allows the NESIE operator to automatically send an SMS to the selected Target devices as soon as they register with the NESIE system. The operator then has the option to reject the device(s), keep them registered on to NESIE or send a series of text messages.

The Targets will not be aware that they are connected to the NESIE system instead of the real cellular network as the mobile device will display the correct information for their network.

CAUTION: IF THE NESIE OPERATOR SENDS AN SMS FROM THE SYSTEM TO TARGET DEVICES THERE WILL BE A RECORD OF THE SMS ON THE DEVICE BUT NOT ON ANY NETWORK CALL RECORDS. ALSO, IF THE NESIE OPERATOR USES A REAL MOBILE DEVICE NUMBER (FOR INSTANCE TO SIMULATE AN SMS SENT FROM A COLLEAGUE) TO SEND AN SMS FROM THE NESIE; TO ANOTHER TARGET DEVICE NUMBER, THERE WILL NOT BE ANY RECORD OF THE SENT SMS ON THE COPIED/EMULATED MOBILE DEVICE.

28.1 LIMITATION – NUMBER OF TRANSCEIVERS

Broadcast SMS uses the GSM protocol to communicate to the Target devices. Target mobile devices can be found on any technology, but the Targeted mobile devices must be moved from LTE and UMTS to the GSM transceiver to receive the protocol messages.

Therefore, at least 2 transceivers are required. One transceiver on LTE or UMTS to find the Target and send it down to the second transceiver. The second transceiver transmitting on GSM is ready to ‘catch’ the Target device if it is sent down from LTE or UMTS.

One transceiver cannot find the Target device on LTE, send the command to move the device to GSM, switch between network technologies e.g. LTE to GSM in time to catch the Target device.

Even when a command is sent to a Target device sending it down from LTE to GSM, the software in the Target device may decide to move to UMTS instead. Therefore, a third transceiver is usually needed to ensure that GSM, UMTS and LTE is covered.

28.2 LIMITATION – NUMBER OF TRANSCEIVERS/NETWORKS

The number of transceivers in the system will determine how many networks can be set up for Broadcast SMS at any one time.

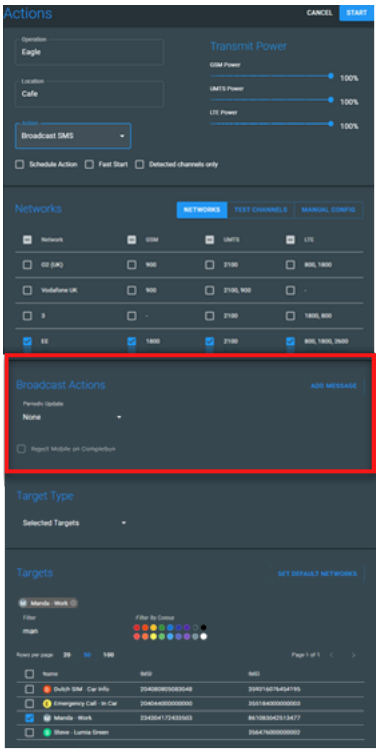
As this action is a denial of service type operation, the NESIE system is set up to continuously transmit. Therefore, the software will only allow you to set up the Broadcast SMS operation depending on the number of transceivers:

- 1 transceiver = 1 Network Covering GSM
- 2 transceivers = 1 Network Covering GSM & UMTS or LTE
- 3 transceivers = 1 Network Covering GSM, UMTS and LTE
- 6 transceivers = 2 Networks
- 9 transceivers = 3 Networks

28.3 BROADCAST SMS – SET UP PROCESS

As shown in Fig 267 below, the NESIE operator has set up the Broadcast SMS as follows:

- ACTIONS page
- NEW ACTIONS button has been pressed
- Entered the Operation / Location Name
- Choose the Broadcast SMS action from the drop-down menu
- Adjusted the Transmit Power if required
- Selected Fast Start, No Rescan etc buttons as required
- Selected the networks and technologies required
- Selected the Target Type / Targets



Operation: Eagle

Location: Cafe

Action: Broadcast SMS

Transmit Power

GSM Power 100%

UMTS Power 100%

LTE Power 100%

□ Schedule Action □ Fast Start □ Detected channels only

☐ Network	☐ GSM	☐ UMTS	☐ LTE
□ O2 (UK)	□ 900	□ 2100	□ 800, 1800
□ Vodafone UK	□ 900	□ 2100, 900	□ -
□ 3	□ -	□ 2100	□ 1800, 800
☑ EE	☑ 1800	☑ 2100	☑ 800, 1800, 2600

Periodic Update: None

□ Reject Mobile on Completion

Selected Targets

Filter: man

Filter By Colour

Rows per page: 20 50 100 Page 1 of 1

□ Name	IMSI	IMEI
□ Dutch SIM - Car Info	204080805083048	359216076454195
□ Emergency Call - In Car	204044000000000	355184000000003
☑ Manda - Work	234304172433503	861083042513477
□ Steve - Lumia Green		356476000000002

Fig 267. Broadcast SMS – set up

When the Broadcast SMS action is selected, an additional box is displayed as shown in the red box in Fig 267 above. This Broadcast SMS Actions pane has the following options:

- ADD MESSAGE
- Periodic Update
- Reject Mobile on Completion

28.3.1 ADD MESSAGE

When the ADD MESSAGE button is clicked, the pane will expand to show the Sending Number and Message Text field, as shown below at Fig 268. It should also be noted that the ADD MESSAGE button will then become greyed out, unless the periodic update is selected.

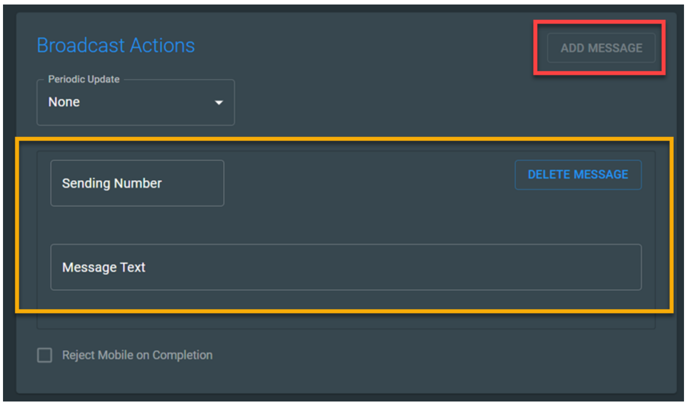


Fig 268. Broadcast SMS – ADD MESSAGE

- **Sending Number**. The operator can enter any number into this field. This is the number that will appear on the Target device when the SMS has been received.

NOTE: The SMS device number field can only contain numbers and the '+' symbol. To a maximum of 20 characters. There should be no spaces in the number.

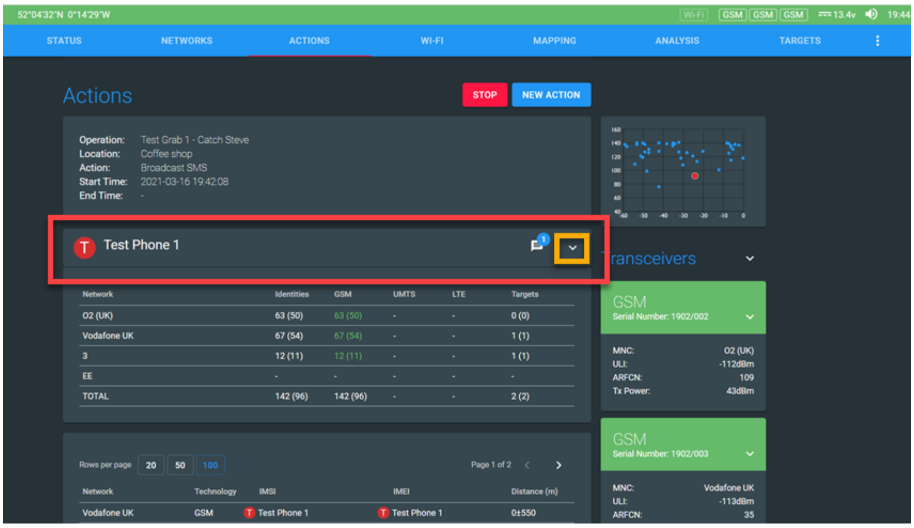
- **Message Text.** A free flow text box where the SMS can be entered.

NOTE: As per a standard SMS, a maximum of 160 characters can be entered in this field.

If a text message is entered and the operation is started, a single SMS will be sent to all Target devices. After the SMS has been sent, the Target devices will be retained on NESIE until the operation is stopped.

28.3.2 BROADCAST SMS – RESULTS

When a Target device registers on to the NESIE system on GSM, the software will automatically send the SMS to the device. The UI will then display an additional pane to indicate the SMS has been sent. As shown in Fig 269 below.



Actions

STOP NEW ACTION

Operation: Test Grab 1 - Catch Steve
Location: Coffee shop
Action: Broadcast SMS
Start Time: 2021-03-16 19:42:08
End Time: -

T Test Phone 1

Network	Identities	GSM	UMTS	LTE	Targets
O2 (UK)	63 (50)	63 (50)	-	-	0 (0)
Vodafone UK	67 (54)	67 (54)	-	-	1 (1)
3	12 (11)	12 (11)	-	-	1 (1)
EE	-	-	-	-	-
TOTAL	142 (96)	142 (96)	-	-	2 (2)

Rows per page 20 50 100 Page 1 of 2

Network	Technology	IMSI	IMEI	Distance (m)
Vodafone UK	GSM	T Test Phone 1	T Test Phone 1	0±550

Transceivers

GSM
Serial Number: 1902/002

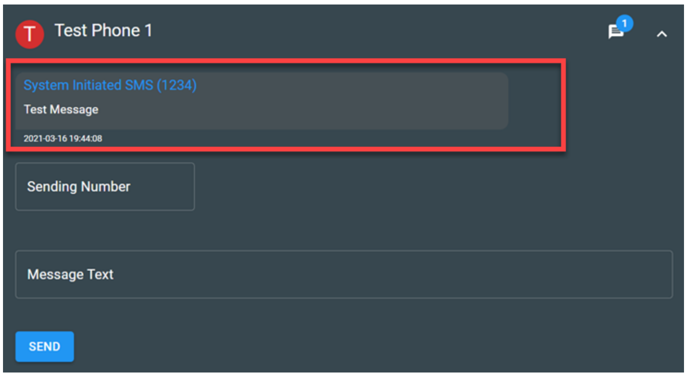
MNC: O2 (UK)
ULI: -112dBm
ARFCN: 109
Tx Power: 43dBm

GSM
Serial Number: 1902/003

MNC: Vodafone UK
ULI: -113dBm
ARFCN: 35

Fig 269. Broadcast SMS – SMS sent notification

This notification pane displays the name / label of the Target device and a message icon to indicate that one message has been sent (from NESIE). The operator can expand the pane by clicking on the down arrow (amber box). This expanded view shows the details of the sent SMS, as shown in Fig 270 below.



T Test Phone 1

System Initiated SMS (1234)
Test Message
2021-03-16 19:44:08

Sending Number

Message Text

SEND

Fig 270. Broadcast SMS – expanded view

The red box shows the details of the Broadcast SMS:

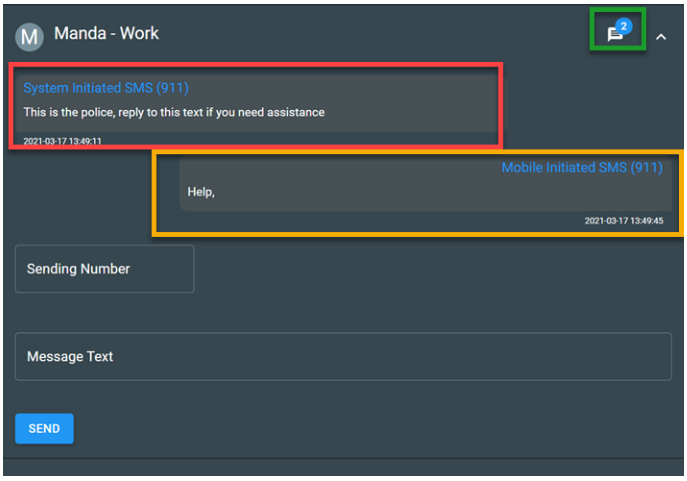
System Initiated SMS	Indicates that the SMS was sent from NESIE
(1234)	The number entered by the operator
Message Text	The SMS text entered by the operator
Date / Time	The date / time the SMS was sent from NESIE

By default, NESIE will maintain the device(s) in denial of service mode after the SMS has been transmitted.

NOTE: In this default mode, any phones that have been sent an SMS are now registered onto NESIE, they will remain registered until they move out of range or the action is stopped.

28.3.3 REPLY FROM TARGET DEVICE

If the Target device sends a reply to the Broadcast SMS, it will be displayed in the notification pane as shown in Fig 271 below.



Manda - Work

System Initiated SMS (911)
This is the police, reply to this text if you need assistance
2021-03-17 13:49:11

Mobile Initiated SMS (911)
Help,
2021-03-17 13:49:45

Fig 271. Broadcast SMS – reply

The message icon (green box), will now show the number 2 to indicate that an SMS has been received. The Broadcast SMS is shown in the red box. The reply from the Target device is shown in the yellow box. The information shown for the reply is:

• **Mobile Initiated SMS**	An SMS sent from the Target device
• **(911)**	The number the SMS was sent to
• Help	SMS text
• Date / Time	Date & time SMS sent to NESIE

The SMS pane still displays the sending number / message text fields, so if required, the operator can continue to send manually entered SMS to the Target device

By default, the Target device will be maintained in the denial of service mode until the operator stops transmitting or the device moves out of the coverage of the NESIE system. However, there will be no way to indicate that the device is still in the denial of service mode.

28.3.4 PERIODIC UPDATE

If required, the NESIE operator can send an SMS to the Target mobile devices and then maintain the denial of service mode, whilst requesting that the Target devices re-register at periodic intervals, to show that the device is still in the area and able to register onto the NESIE System.

Set up the Broadcast SMS as previously discussed. Now the NESIE operator should select the Periodic Update time from the drop-down menu as shown in Fig 272 below.

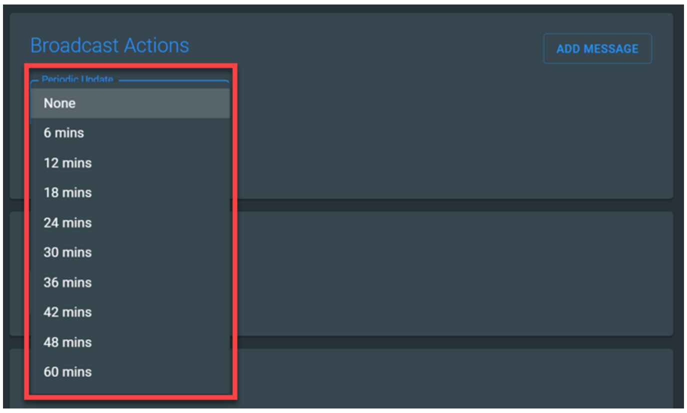
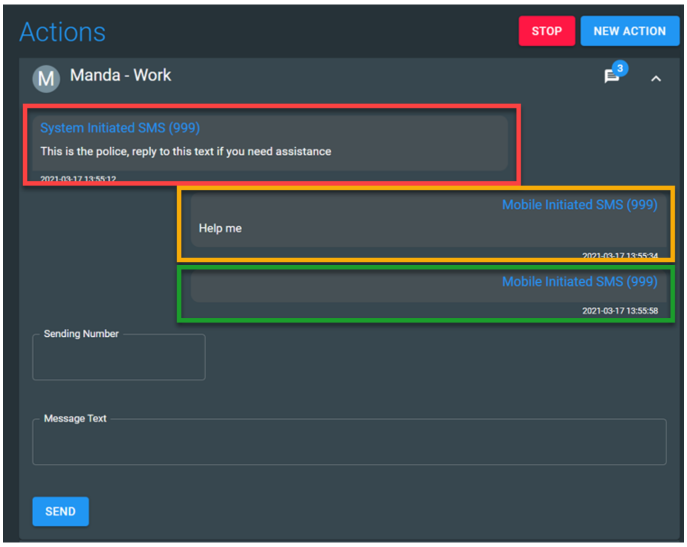


Fig 272. Broadcast SMS - Periodic Update

After choosing the Periodic Update time, the operator should complete the set up as previously discussed and start the operation.

NOTE: The time chosen from the drop-down menu is an approximate time from when the mobile device last registered with the NESIE system. The mobile device is sent a protocol message requesting that it re-registers. The mobile device maintains the time record. If at any time the mobile device sends an SMS or makes a call, this will be counted as a registration event (and shown on the NESIE registration screen). The re-registration timer will reset, and the mobile device should re-register with the NESIE system after a further 6 minutes (or other periodic time chosen by the operator).

In the example below, a Periodic Update time of 6 minutes was chosen. The initial Broadcast SMS was sent (Red Box) and the Target device has replied (Yellow Box). A periodic update was sent from the Target device (Green box). However, the time between the SMS and the periodic update will not always be accurate.



System Initiated SMS (999)
This is the police, reply to this text if you need assistance
2021-03-17 13:55:12

Mobile Initiated SMS (999)
Help me
2021-03-17 13:55:34

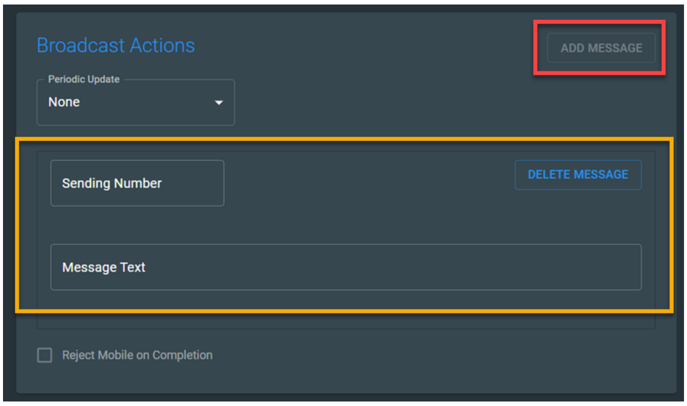
Mobile Initiated SMS (999)
2021-03-17 13:55:58

Fig 273. Broadcast SMS - Periodic Update from device

28.3.5 REJECT MOBILE ON COMPLETION

If required, the mobile devices can be rejected (sent back to the real cellular networks) after receiving the SMS. This rejection requires a protocol message to be sent to the Target mobile device.

To reject the device, the operator should tick the Reject Mobile on Completion box, as shown in Fig 274 below.



Periodic Update: None

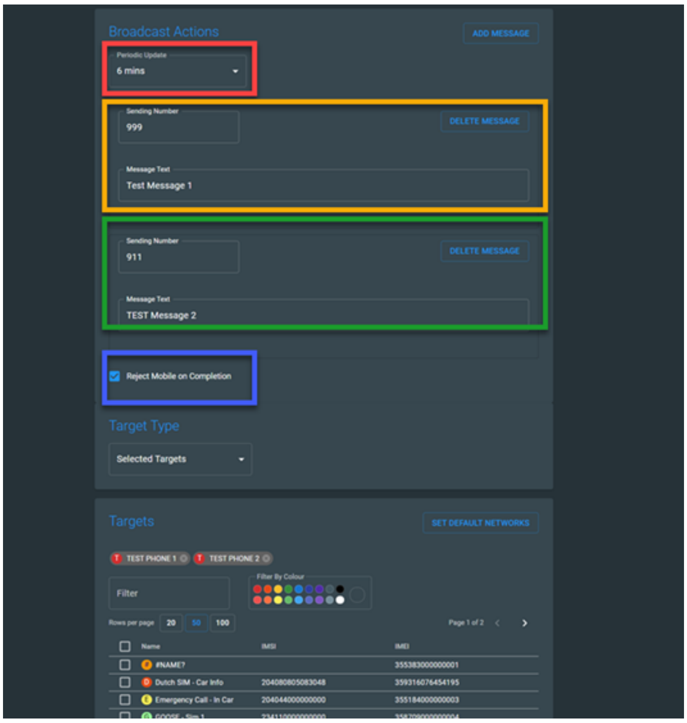
□ Reject Mobile on Completion

Fig 274. Reject Mobile on Completion

28.3.6 SEND SMS – MULTIPLE SMS'S

If required, the NESIE system can be set up to send multiple SMS at periodic intervals. This could be used to represent a conversation, broadcast warnings' to encourage the Target to dial a device number or send an SMS to another mobile device.

As for the previous examples, set up the Broadcasts SMS Action. However, after selecting a Periodic Update from the drop-down menu E.g.: 6 mins, the operator should add the 2nd SMS etc (or multiples) as shown in Fig 275 below.



Broadcast Actions

ADD MESSAGE

Periodic Update: 6 mins

Sending Number: 999

DELETE MESSAGE

Message Text: Test Message 1

Sending Number: 911

DELETE MESSAGE

Message Text: TEST Message 2

☑ Reject Mobile on Completion

Target Type

Selected Targets

Targets

SET DEFAULT NETWORKS

TEST PHONE 1 · TEST PHONE 2

Filter

Filter By Colour

Rows per page 20 50 100

Page 1 of 2

□	Name	IMSI	IMEI
□	#NAME?		355383000000001
□	Dutch SIM - Car Info	204080805083048	359316076454195
□	Emergency Call - In Car	204044000000000	355184000000003
□	GOOSE - Sim 1		

Fig 275. Broadcast SMS – send multiple SMS

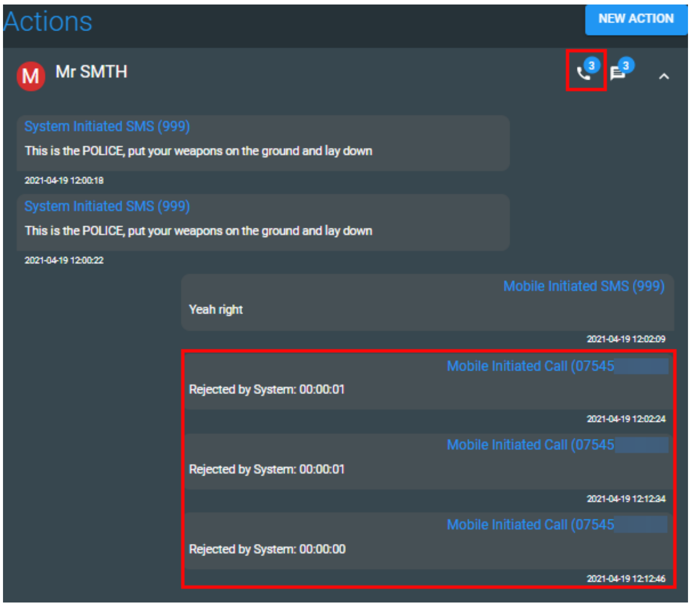
NOTE: if a periodic time is allocated, it will apply to all future SMS. Therefore every SMS will be sent after the chosen Periodic Update.

In the example shown in Fig 275, the operator has selected a Periodic Update of 6 mins (red box) and entered SMS 1 (Amber Box) and SMS 2 (Green Box) and selected Reject Mobile on Completion (Blue Box). Therefore, the first SMS will be sent as soon as the Target device registers onto NESIE. After approximately 6 minutes, the 2nd SMS will be sent. Then, after the 2nd SMS has been sent, the device will be rejected back to the real network.

If the Reject Mobile after Completion was not ticked, the 1st and 2nd SMS would be sent as previously stated. Then the device would periodically update (re-register) approximately every 6 minutes, until the operation is stopped.

28.3.7 BROADCAST SMS – CALL LIST

Whilst conducting a Broadcast SMS operation, all mobile devices registered onto the NESIE will be under a denial of service mode. If the mobile device attempts to make a call, it will be directed to the NESIE system. The call details will be logged / displayed on the UI, but the call will be automatically rejected, as shown below in Fig 276.



System Initiated SMS (999)
This is the POLICE, put your weapons on the ground and lay down
2021-04-19 12:00:18

System Initiated SMS (999)
This is the POLICE, put your weapons on the ground and lay down
2021-04-19 12:00:22

Mobile Initiated SMS (999)
Yeah right
2021-04-19 12:02:09

Mobile Initiated Call (07545[redacted]
Rejected by System: 00:00:01
2021-04-19 12:02:24

Mobile Initiated Call (07545[redacted]
Rejected by System: 00:00:01
2021-04-19 12:12:34

Mobile Initiated Call (07545[redacted]
Rejected by System: 00:00:00
2021-04-19 12:12:46

Fig 276. Broadcast SMS - call LIst

In the example above, two SMS were Broadcast to the Target phone (**System Initiated SMS(999)**). The Target replied via SMS (**Mobile Initiated SMS (999)**). Then the Target attempted to make three voice calls. The details of the calls are shown in the red box.

- **Mobile Initiated Call (Number Dialled by Target)**
- Rejected by System
- Date/Time stamp

As previously stated, NESIE cannot receive these voice calls and they will be automatically rejected by the system. However, the number dialled will be displayed on the UI.

The Target phone will attempt to establish the call. The call will be sent to NESIE not the real network. NESIE will reject the call and the call will drop.

29. REDIRECT

Redirect is the process of transmitting fake base transceiver stations to gather the IMEIs and IMSI from all the cellular devices on UMTS and LTE and then sending a network command to the devices, so they are redirected to GSM.

Normally this operation would be done in conjunction with another piece of GSM intercept equipment (Not supplied by Smith Myers).

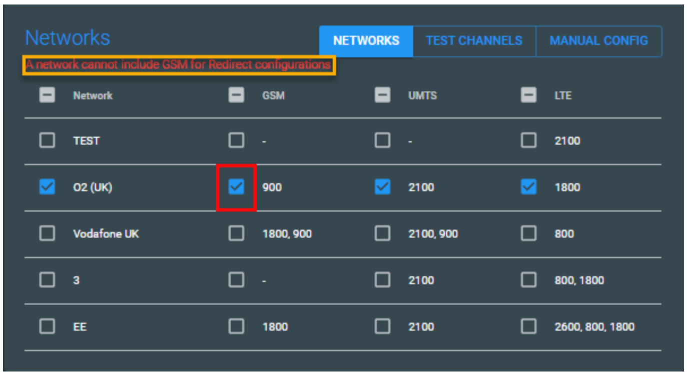
There are 2 methods of launching a Redirect action:

29.1 REDIRECT – ACTIONS PAGE

This redirect options gives the operator the ability to select the desired networks and technologies to redirect from. Then choose the devices to Target eg: All phones (including / excluding whitelist), all Target devices or specified Targets to be redirected. The redirect will then send the Targets down to GSM and will not specify which GSM channel to move to.

From the Action selection drop-down menu, the operator selects the Redirect action. The operator must then select the networks and technologies to Redirect from. This operation is intended to redirect down from UMTS and/or LTE to GSM.

NOTE: If the operator selects GSM by mistake, a warning message stating “A network cannot include GSM for Redirect configurations” will appear as seen below in Fig 277.



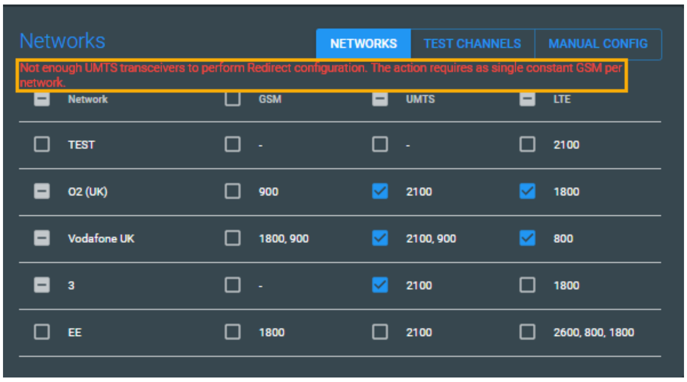
Networks

A network cannot include GSM for Redirect configurations

⊟ Network	⊟ GSM	⊟ UMTS	⊟ LTE
□ TEST	□ -	□ -	□ 2100
☑ O2 (UK)	☑ 900	☑ 2100	☑ 1800
□ Vodafone UK	□ 1800, 900	□ 2100, 900	□ 800
□ 3	□ -	□ 2100	□ 800, 1800
□ EE	□ 1800	□ 2100	□ 2600, 800, 1800

Fig 277. Redirect GSM selected warning

The number of UMTS/LTE networks that are redirected depends on the number of transceivers that are available in the system. If the operator selects more network/technology options than are available, a warning message will appear stating “Not enough UMTS/LTE transceivers to perform redirect configuration. The action requires a single constant GSM per network” as seen below in Fig 278.



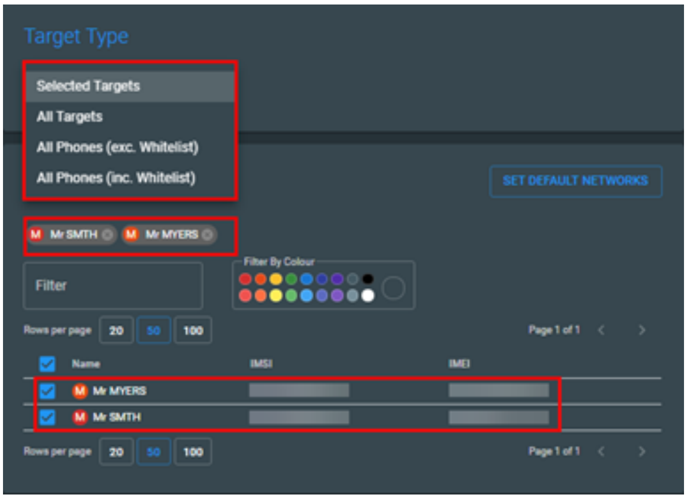
Not enough UMTS transceivers to perform Redirect configuration. The action requires as single constant GSM per network.

	Network		GSM		UMTS		LTE
□	TEST	□	-	□	-	□	2100
⊟	O2 (UK)	□	900	☑	2100	☑	1800
⊟	Vodafone UK	□	1800, 900	☑	2100, 900	☑	800
⊟	3	□	-	☑	2100	□	1800
□	EE	□	1800	□	2100	□	2600, 800, 1800

Fig 278. Redirect UMTS/LTE warning

NOTE: During Redirect operations, it is anticipated that the system will be operating on the UMTS and/or LTE bands selected permanently in order to capture and redirect all phones. Therefore, the NESIE software will not rotate across different networks.

The operator must then choose the Target type and select the Target identities if required, as seen in Fig 279.



☑	Name	IMSI	IMEI
☑	M Mr MYERS	[redacted]	[redacted]
☑	M Mr SMTH	[redacted]	[redacted]

Fig 279. Redirect Target Type/Target

Once the operator has selected all the information to carry out the Redirect Action, they should press the START button.

When the START button is pressed, the UI will change to show the refreshed Action summary page. As previously shown, the list of IDs captured will be shown along with the automatically measured distances.

NOTE: There is no indication that the devices have been sent a Redirect code or have moved down to GSM.

29.2 REDIRECT – ADDITIONAL MENU

The Redirect Action option from the additional menu shown in Fig 280 and Fig 281 below, lets the operator select the Redirect Action, choose a single network and specifies a specific GSM channel to Redirect the mobile devices down to.

This option will try to automatically Redirect all devices on LTE and UMTS on the selected network. The NESIE system will then send the mobile devices to a specified Target ARFCN (GSM channel).

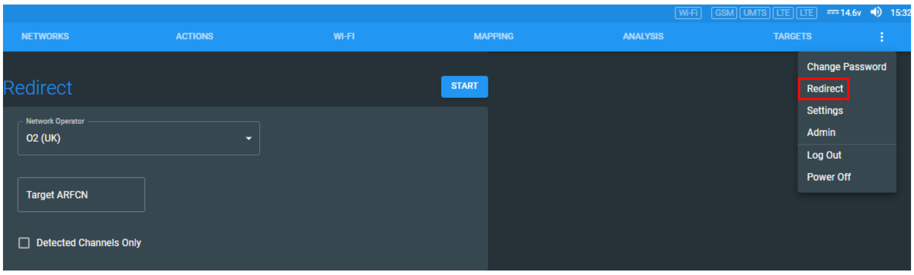


Fig 280. Redirect additional menu

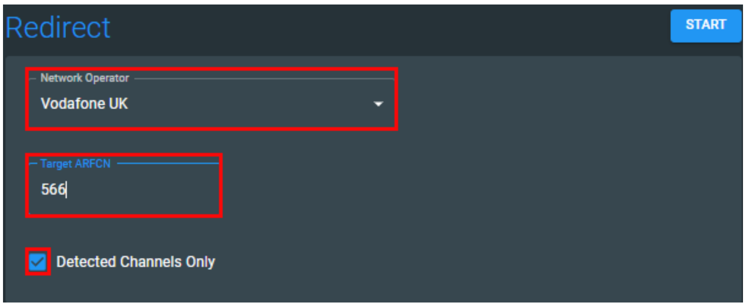


Fig 281. Redirect – sub menu

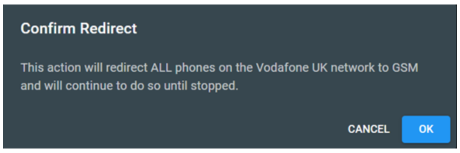
As shown in Fig 281 above, the NESIE operator has selected the Redirect option form the additional menu. The page displayed gives the operator the following options:

- **Network Operator**: A drop-down list will be populated with the networks detected during the network scan. The operator can choose one of these networks.

- **Target ARFCN**: The operator must enter the GSM channel number that all the devices will be sent down to.

- **Detected Channels Only**: If this box is ticked, NESIE will only redirect the devices down to a GSM channel that has been detected by the NESIE System.

After the operator has set up the Redirect operation, the START button should be pressed. A pop-up box will be displayed to confirm the Action, as shown below in Fig 282 below. This notification box will ensure the operator is aware that they are about to start a Redirect Action on all devices on the chosen network.



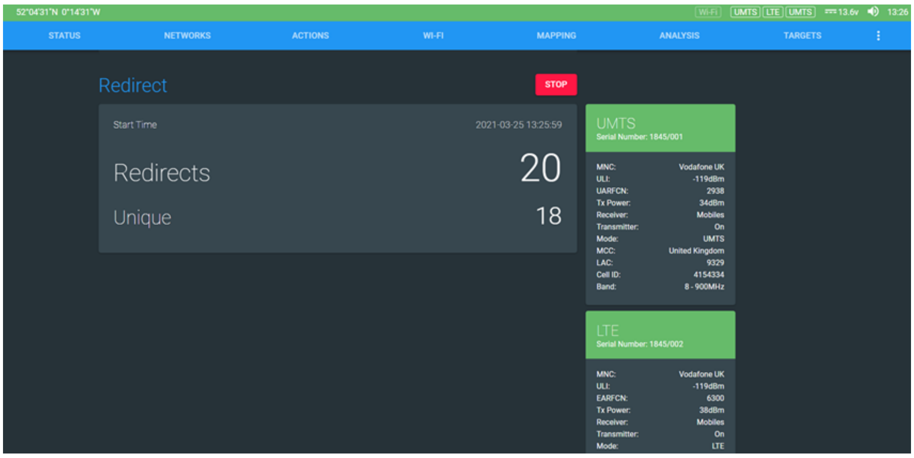
Confirm Redirect

This action will redirect ALL phones on the Vodafone UK network to GSM and will continue to do so until stopped.

Fig 282. Confirm Redirect

After the operator has pressed OK, the screen will change to show the Actions summary, as shown below at Fig 283. The screen will display the following information:

- **Start Time** The date / time the operation was started
- **Redirects** Number of devices that a Redirect has been sent to
- **Unique** Number of unique devices a Redirect has been sent to



Redirect

Start Time 2021-03-25 13:25:59

Redirects 20

Unique 18

UMTS
Serial Number: 1845/001

MNC: Vodafone UK
ULI: -119dBm
UARFCN: 2938
Tx Power: 34dBm
Receiver: Mobiles
Transmitter: On
Mode: UMTS
MCC: United Kingdom
LAC: 9329
Cell ID: 4154334
Band: 8 - 900MHz

LTE
Serial Number: 1845/002

MNC: Vodafone UK
ULI: -119dBm
EARFCN: 6300
Tx Power: 38dBm
Receiver: Mobiles
Transmitter: On
Mode: LTE

Fig 283. Redirect – summary

NOTE: The Redirect operation will run continually until the operator presses the STOP button.

It is suggested that Redirect would usually only be carried out on a Multi-Channel system, due to the requirement to identify and Redirect devices on both LTE and UMTS before they are Redirected down to GSM

30. MEASURE LTE RANGE

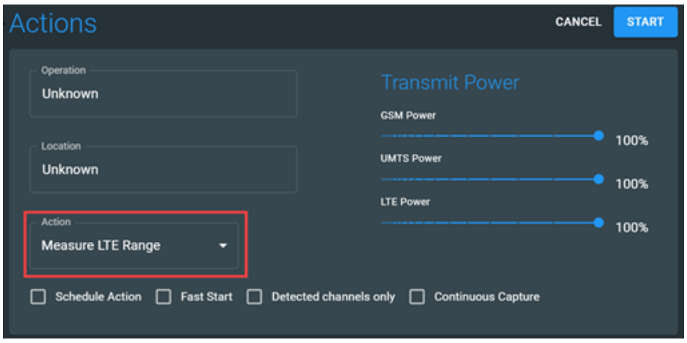
This action is used in conjunction with the CNEST Cellsites software. This function will allow the team to conduct reconnaissance on possible grab locations and assist with the placement of the NESIE system to greatly increase the likelihood of capturing the Target IMSI/IMEI.

The information displayed on the CNEST will give a true reflection of the signal strength being received from the transmitting NESIE. This will give the team a confidence factor on whether the grab will be successful. If the signal strength received from the NESIE is weak, the system may need to be moved closer, or another location for the grab to be successful.

30.1 MEASURE LTE RANGE - SETUP

As per below, the user has started a Measure LTE Range operation by following the actions bellow:

- ACTIONS page
- NEW ACTIONS button has been pressed
- Entered the Operation / Location Name
- Chosen the Measure LTE Range action from the drop-down menu
- Adjusted the Transmit Power if required
- Selected Fast Start, No Rescan etc buttons as required



Operation: Unknown

Location: Unknown

Action: Measure LTE Range

GSM Power 100%

UMTS Power 100%

LTE Power 100%

□ Schedule Action □ Fast Start □ Detected channels only □ Continuous Capture

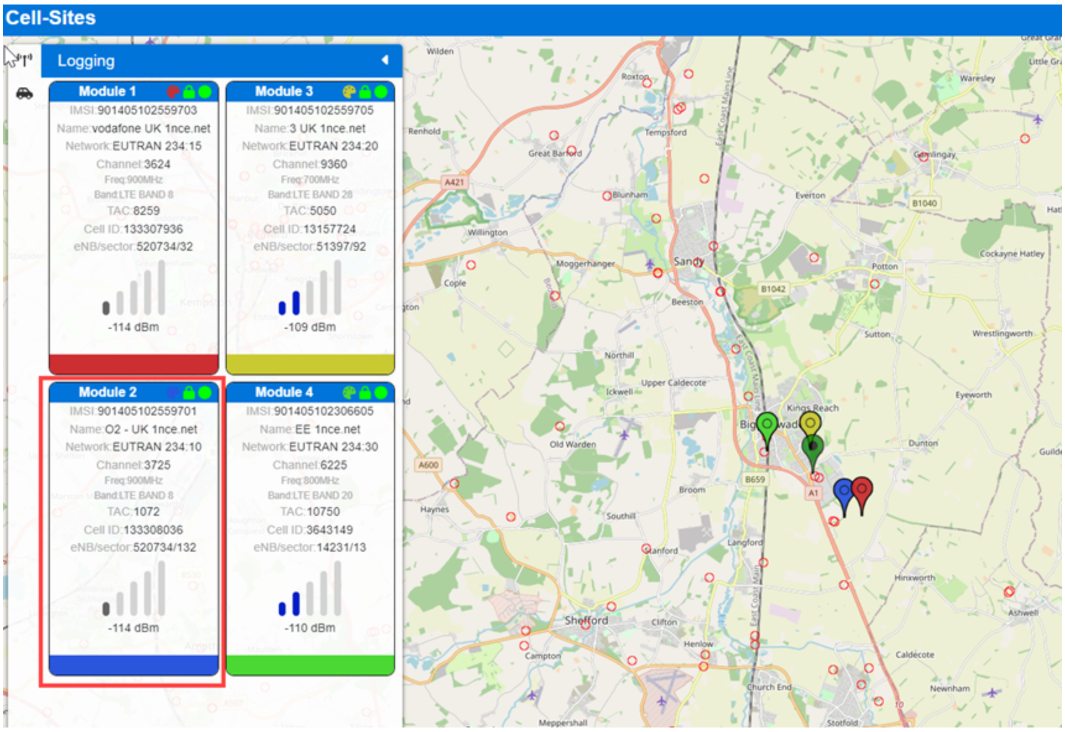
Fig 284. Measure LTE Range Action

As the Action name suggests, this operation can only be used against LTE technology on all networks. If on the ACTIONS page, GSM or UMTS is selected for the Action, an error message will be displayed.

The IMSI number(s) of the SIM cards in the CNEST modules should be noted, or alternatively, use the IMSI numbers to create Targets for the CNEST modules. The operator should now press the START button.

30.2 CNEST DISPLAY

On the CNEST, prior to NESIE transmitting, the CNEST (module two for demonstration purposes), will display all the relevant information pertaining to that particular network from the current serving cell, including signal strength. The IMSI number required to set up a Target logged prior to the Action taking place can be seen (Fig 285). The coloured pins on the map represent the estimated position of the serving cells for all networks. The blue pin represents module two.



Cell-Sites

Logging

Module 1
IMSI:901405102559703
Name:vodafone UK 1nce.net
Network:EUTRAN 234:15
Channel:3624
Freq:900MHz
Band:LTE BAND 8
TAC:8259
Cell ID:133307936
eNB/sector:520734/32
-114 dBm

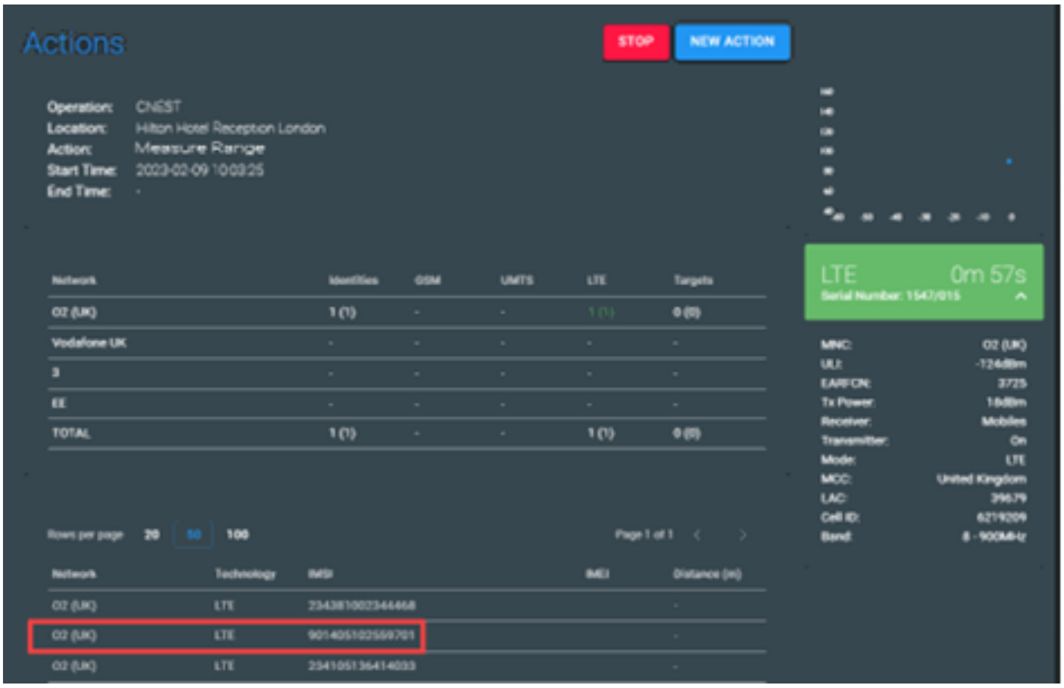
Module 3
IMSI:901405102559705
Name:3 UK 1nce.net
Network:EUTRAN 234:20
Channel:9360
Freq:700MHz
Band:LTE BAND 28
TAC:5050
Cell ID:13157724
eNB/sector:51397/92
-109 dBm

Module 2
IMSI:901405102559701
Name:O2 - UK 1nce.net
Network:EUTRAN 234:10
Channel:3725
Freq:900MHz
Band:LTE BAND 8
TAC:1072
Cell ID:133308036
eNB/sector:520734/132
-114 dBm

Module 4
IMSI:901405102306605
Name:EE 1nce.net
Network:EUTRAN 234:30
Channel:6225
Freq:800MHz
Band:LTE BAND 20
TAC:10750
Cell ID:3643149
eNB/sector:14231/13
-110 dBm

Fig 285. CNEST display - prior to transmitting

The NESIE will grab all IMSI as per a normal Grab. If the CNEST modules have been entered as a Target, when the IMSI is found, the NESIE will display the Target name in the capture list. This way, both the NESIE and CNEST operators have confidence that the CNEST modules have been captured and an effective IMSI Grab in that location is highly likely. If the IMSI is not entered as a Target, watch the capture list for the CNEST module IMSI being detected (Fig 286).



Actions

Operation:	CNEST
Location:	Hilton Hotel Reception London
Action:	Measure Range
Start Time:	2023-02-09 10:03:25
End Time:	-

Network	Identities	GSM	UMTS	LTE	Targets
O2 (UK)	1 (1)	-	-	1 (1)	0 (0)
Vodafone UK	-	-	-	-	-
3	-	-	-	-	-
EE	-	-	-	-	-
TOTAL	1 (1)	-	-	1 (1)	0 (0)

Rows per page 20 50 100 Page 1 of 1

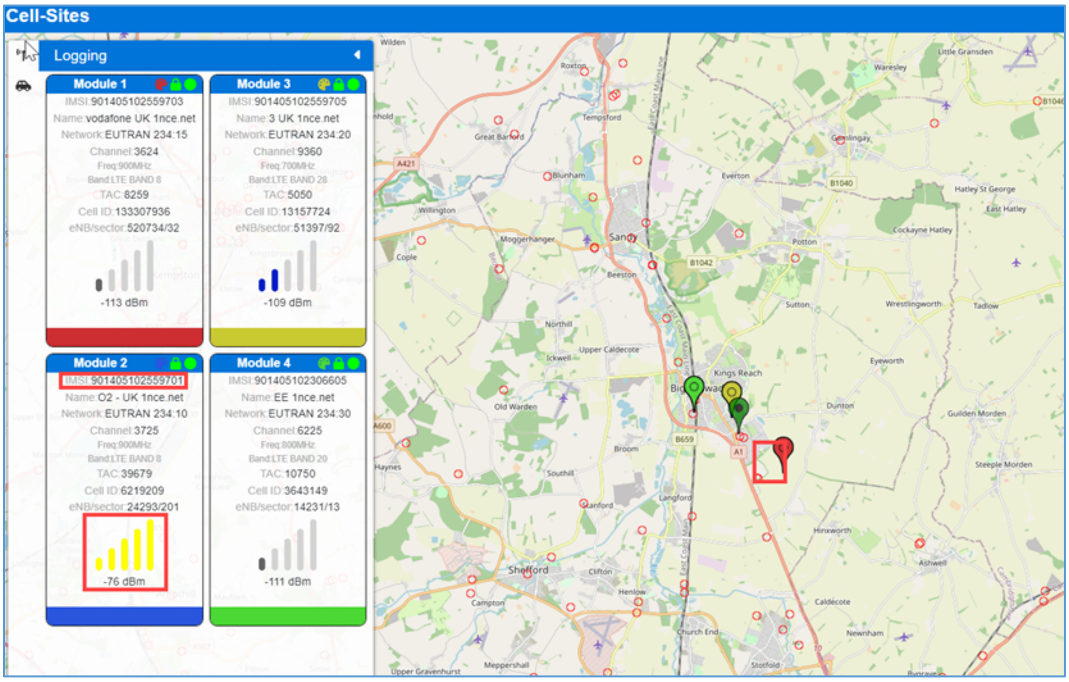
Network	Technology	IMSI	IMEI	Distance (m)
O2 (UK)	LTE	234381002344468		-
O2 (UK)	LTE	901405102559701		-
O2 (UK)	LTE	234105136414033		-

LTE 0m 57s
Serial Number: 1547/015

MNC:	O2 (UK)
ULI:	-124dBm
EARFCN:	3725
Tx Power:	18dBm
Receiver:	Mobiles
Transmitter:	On
Mode:	LTE
MCC:	United Kingdom
LAC:	39679
Cell ID:	6219209
Band:	8 - 900MHz

Fig 286. CNEST module IMSI detected

When the NESIE is transmitting, module two on the CNEST is now displaying the signal strength received from the active NESIE. This will give an idea of how successful an IMSI grab in this location against a Target is likely to be. Point to note, the blue pin, representing the current serving cell has disappeared from the map. This is due to the fact that the module is trying to retrieve a tower position using the broadcast data received from the NESIE. As the NESIE is not a real tower, CNEST cannot resolve that loOK up and removes the pin from the map. If required, carry out the same actions for all networks to measure the NESIE signal strength. Once NESIE stops transmitting, the CNEST module two display will return to its original state (Fig 285).



Cell-Sites

Logging

Module 1

IMSI:901405102559703
Name:vodafone UK 1nce.net
Network:EUTRAN 234:15
Channel:3624
Freq:900MHz
Band:LTE BAND 8
TAC:8259
Cell ID:133307936
eNB/sector:520734/32

-113 dBm

Module 3

IMSI:901405102559705
Name:3 UK 1nce.net
Network:EUTRAN 234:20
Channel:9360
Freq:700MHz
Band:LTE BAND 28
TAC:5050
Cell ID:13157724
eNB/sector:51397/92

-109 dBm

Module 2

IMSI:901405102559701
Name:O2 - UK 1nce.net
Network:EUTRAN 234:10
Channel:3725
Freq:900MHz
Band:LTE BAND 8
TAC:39679
Cell ID:6219209
eNB/sector:24293/201

-76 dBm

Module 4

IMSI:901405102306605
Name:EE 1nce.net
Network:EUTRAN 234:30
Channel:6225
Freq:800MHz
Band:LTE BAND 20
TAC:10750
Cell ID:3643149
eNB/sector:14231/13

-111 dBm

Fig 287. CNEST display - NESIE transmitting

31. WI-FI MODULE

The Wi-Fi module fitted in NESIE control modules is a 2.4GHz & 5GHz Wi-Fi transceiver. This unit is capable of 2 modes:

Passive	Listening to Wi-Fi or Wi-Fi sniffing
Active	Transmitting a Wi-Fi Access Point (WAP) or Hotspot

31.1 PASSIVE - WI-FI SNIFFER

By listening to the Wi-Fi signals in the area, NESIE can detect and log the Wi-Fi settings that are transmitted by Wi-Fi enabled devices. The Wi-Fi sniffer can detect and capture:

- Wi-Fi Access Point (Hotspots)
- Wi-Fi names (SSID)
- Device MAC address details
- Device Hotspot SSIDs and MAC address details
- Probed request for SSIDs

31.2 ACTIVE - WI-FI TRANSCEIVER

Although the Wi-Fi transceiver is capable of transmitting Wi-Fi data, NESIE does not currently use the transmit portion of the transceiver.

31.3 WI-FI DEVICES / SETTINGS EXPLAINED

A brief explanation of the Wi-Fi data that will be seen in the NESIE UI is below:

31.3.1 WIRELESS ACCESS POINT (WAP)

More commonly known as Access Point (AP), this is a piece of computer hardware that allows a Wi-Fi device to connect to a wired network. The AP is connected to a router (via a wired network) as a standalone device, or it could be contained in the router itself. The Wi-Fi hotspot is usually the physical location where Wi-Fi access is available.

31.3.2 SSID

Is a Wi-Fi network name. It is a case sensitive, unique identifier that can contain up to 32 alphanumeric characters. The SSID acts as a gateway (that can be open or encrypted and protected with a password) when a mobile device tries to connect to the Wi-Fi Access Point or Hotspot.

31.3.3 MAC address

A Media Access Control (MAC) address is assigned to a Network Interface Card (NIC) of a computer (Laptop/Tablet/Smart Device). It is a unique 6 byte (48-bit) address that is (usually) permanently burned into a network interface card or other physical-layer networking device and that uniquely identifies the device on an ethernet or Wi-Fi based network. The MAC address is constructed as shown below in Fig 288.

The first 3 bytes (6 characters) 1 are the Organisationally Unique Identifier (OUI) or which is a unique code issued to the manufacturer by the Institute of Electrical and Electronics Engineers (IEEE). The remaining 3 bytes (6 characters) 2 are a unique serial number assigned by the manufacturer that represent an identification number for the specific device.

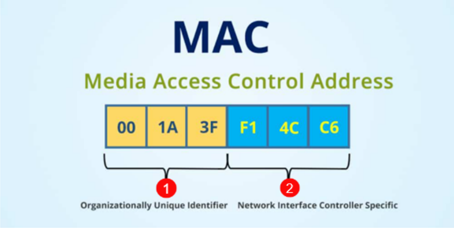

MAC
Media Access Control Address
00
1A
3F
F1
4C
C6
1
2
Organizationally Unique Identifier
Network Interface Controller Specific

Fig 288. MAC Address composition

31.3.4 PROBED SSID

Some Wi-Fi devices continually transmit a signal (probe request) loOKing for previously used Wi-Fi APs. If this data can be collected, the NESIE operator may be able to investigate the history of a particular Wi-Fi device.

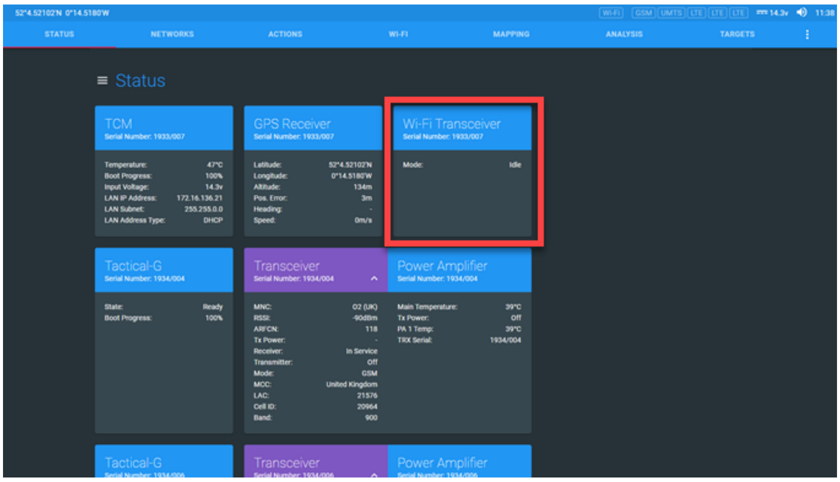
When a device connects to a Wi-Fi network for the first time, users usually save the log on information and some devices save it automatically. This saved data can then be used again when the device is within range of the same Wi-Fi hotspot and automatically connect without prompting the user.

This database of saved Wi-Fi data could contain the name of the Wi-Fi hotspots the device has connected to e.g.: Hilton Hotel Paris, Heathrow Airport Wi-Fi, Home Broadband Wi-Fi, Police HQ Wi-Fi.

NOTE: the average range of a Wi-Fi device is approx. 30-40m, therefore, the average detect range for a Wi-Fi sniffer is approx. 30-40m. But as per all radio signals, this can depend on transmitted signal strength, antenna used, environment, obstacles and other factors.

31.4 WI-FI TRANSCEIVER

If a Wi-Fi transceiver module is fitted to a NESIE system, it will automatically be detected and will be visible in the STATUS page, as a Wi-Fi transceiver resource pane on the UI, as shown in Fig 289 below.



TCM
Serial Number: 1933/007
Temperature: 47°C
Boot Progress: 100%
Input Voltage: 14.3v
LAN IP Address: 172.16.136.21
LAN Subnet: 255.255.0.0
LAN Address Type: DHCP

GPS Receiver
Serial Number: 1933/007
Latitude: 52°4.52102'N
Longitude: 0°14.5180'W
Altitude: 134m
Pos. Error: 3m
Heading: -
Speed: 0m/s

Wi-Fi Transceiver
Serial Number: 1933/007
Mode: Idle

Tactical-G
Serial Number: 1934/004
State: Ready
Boot Progress: 100%

Transceiver
Serial Number: 1934/004
MNC: O2 (UK)
RSSI: -90dBm
ARFCN: 118
Tx Power: -
Receiver: In Service
Transmitter: Off
Mode: GSM
MCC: United Kingdom
LAC: 21576
Cell ID: 20964
Band: 900

Power Amplifier
Serial Number: 1934/004
Main Temperature: 39°C
Tx Power: Off
PA 1 Temp: 39°C
TRX Serial: 1934/004

Tactical-G
Serial Number: 1934/006

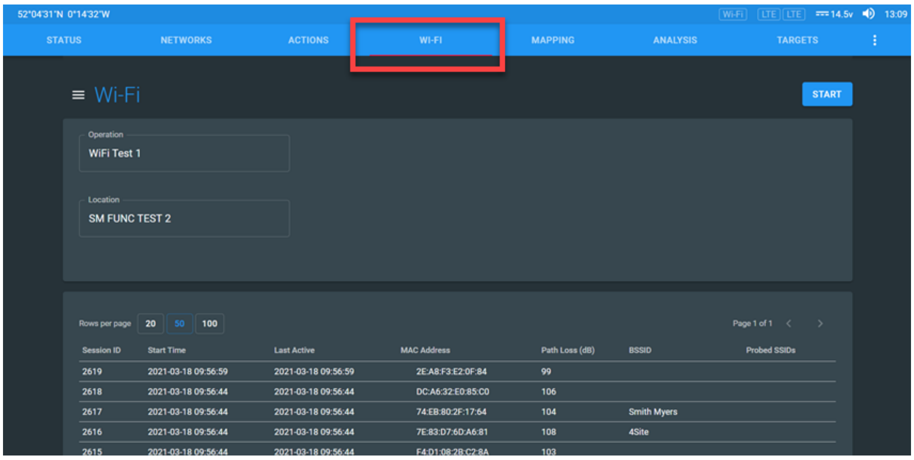
Transceiver
Serial Number: 1934/006

Power Amplifier
Serial Number: 1934/006

Fig 289. Wi-Fi module – STATUS page

Upon initial power up, the Wi-Fi Module will be shown with a blue header bar. This indicates the module is available but is currently idle (not sniffing the Wi-Fi environment).

Upon pressing the Wi-Fi button on the header bar , the operator will be shown the Wi-Fi page as shown below at Fig 290.



Operation: WiFi Test 1

Location: SM FUNC TEST 2

Session ID	Start Time	Last Active	MAC Address	Path Loss (dB)	BSSID	Probed SSIDs
2619	2021-03-18 09:56:59	2021-03-18 09:56:59	2E:A8:F3:E2:0F:84	99		
2618	2021-03-18 09:56:44	2021-03-18 09:56:44	DC:A6:32:E0:85:C0	106		
2617	2021-03-18 09:56:44	2021-03-18 09:56:44	74:EB:80:2F:17:64	104	Smith Myers	
2616	2021-03-18 09:56:44	2021-03-18 09:56:44	7E:83:D7:6D:A6:81	108	4Site	
2615	2021-03-18 09:56:44	2021-03-18 09:56:44	F4:D1:08:2B:C2:8A	103		

Fig 290. Wi-Fi page

NOTE: If previous Wi-Fi data has been collected, it may be shown on this screen. If this is the first time the Wi-Fi device has been used, the screen will be blank.

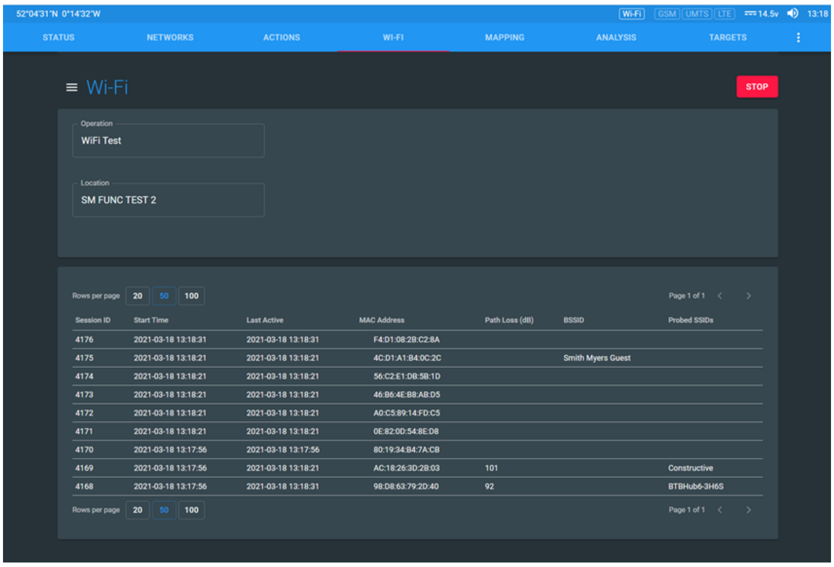
If previous results are shown, the screen will be refreshed when a new sniff is started.

31.4.1 START A WI-FI SNIFF

The operator should enter the Operation name and Location of the Wi-Fi sniff then Press the START Button.

When a Wi-Fi sniff has been started, the START button will change to a STOP button and the detected Wi-Fi results will be displayed. The Wi-Fi module is now in receive/monitor mode, as shown in Fig 291 below.

NOTE: The Wi-Fi module will automatically alternate between monitoring the 2.4GHz & 5GHz Wi-Fi Bands.



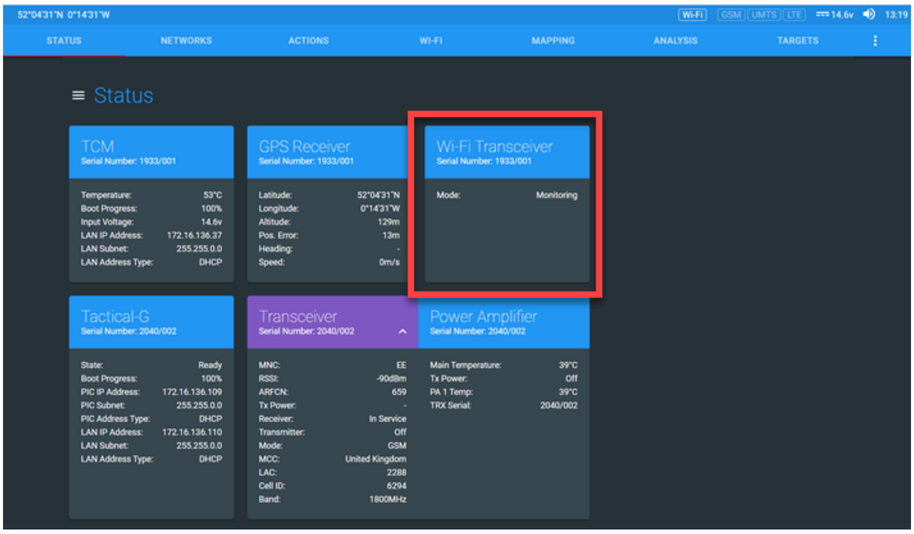
Operation: WiFi Test

Location: SM FUNC TEST 2

Session ID	Start Time	Last Active	MAC Address	Path Loss (dB)	BSSID	Probed SSIDs
4176	2021-03-18 13:18:31	2021-03-18 13:18:31	F4:D1:08:2B:C2:8A			
4175	2021-03-18 13:18:21	2021-03-18 13:18:21	4C:D1:A1:B4:0C:2C		Smith Myers Guest	
4174	2021-03-18 13:18:21	2021-03-18 13:18:21	56:C2:E1:DB:5B:1D			
4173	2021-03-18 13:18:21	2021-03-18 13:18:21	46:B6:4E:B8:AB:D5			
4172	2021-03-18 13:18:21	2021-03-18 13:18:21	A0:C5:89:14:FD:C5			
4171	2021-03-18 13:18:21	2021-03-18 13:18:21	0E:82:0D:54:8E:D8			
4170	2021-03-18 13:17:56	2021-03-18 13:17:56	80:19:34:B4:7A:CB			
4169	2021-03-18 13:17:56	2021-03-18 13:18:21	AC:18:26:3D:2B:03	101		Constructive
4168	2021-03-18 13:17:56	2021-03-18 13:18:31	98:D8:63:79:2D:40	92		BTBHub6-3H6S

Fig 291. Wi-Fi sniffer – running

If required, the operator can also check on the status of the Wi-Fi module on the STATUS page. If the operator loOKs at the STATUS page, the Wi-Fi module will now show that it is in monitoring mode as shown below in Fig 292.



TCM
Serial Number: 1933/001

Temperature:	53°C
Boot Progress:	100%
Input Voltage:	14.6v
LAN IP Address:	172.16.136.37
LAN Subnet:	255.255.0.0
LAN Address Type:	DHCP

GPS Receiver
Serial Number: 1933/001

Latitude:	52°04'31"N
Longitude:	0°14'31"W
Altitude:	129m
Pos. Error:	13m
Heading:	-
Speed:	0m/s

Wi-Fi Transceiver
Serial Number: 1933/001

Mode:	Monitoring

Tactical-G
Serial Number: 2040/002

State:	Ready
Boot Progress:	100%
PIC IP Address:	172.16.136.109
PIC Subnet:	255.255.0.0
PIC Address Type:	DHCP
LAN IP Address:	172.16.136.110
LAN Subnet:	255.255.0.0
LAN Address Type:	DHCP

Transceiver
Serial Number: 2040/002

MNC:	EE
RSSI:	-90dBm
ARFCN:	659
Tx Power:	-
Receiver:	In Service
Transmitter:	Off
Mode:	GSM
MCC:	United Kingdom
LAC:	2288
Cell ID:	6294
Band:	1800MHz

Power Amplifier
Serial Number: 2040/002

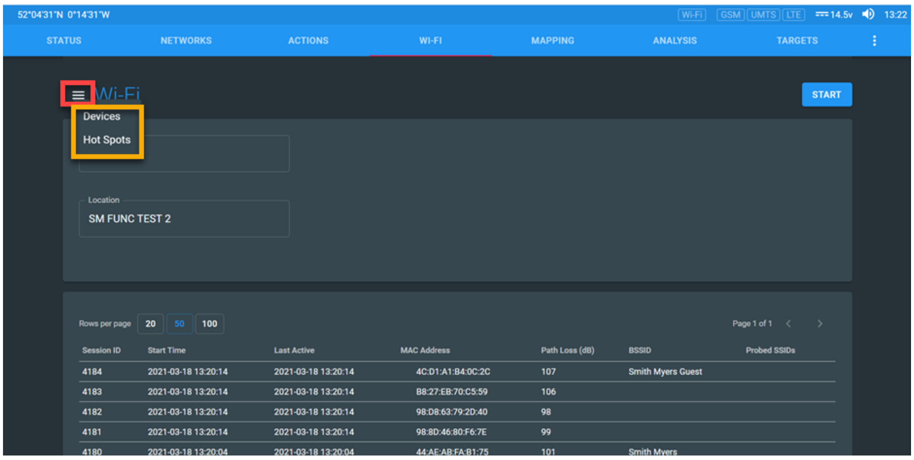
Main Temperature:	39°C
Tx Power:	Off
PA 1 Temp:	39°C
TRX Serial:	2040/002

Fig 292. Wi-Fi module – monitor status

The results of the Wi-Fi sniff are displayed on 2 different pages:

• Devices	Devices, laptops and other devices transmitting Wi-Fi
• Hotspots	Access Points transmitting Wi-Fi data

By default, the Devices page is displayed. To change between these pages, the operator should press the sub menu button (red box) and choose from the drop-down menu (amber box), shown below in Fig 293.



Location
SM FUNC TEST 2

Session ID	Start Time	Last Active	MAC Address	Path Loss (dB)	BSSID	Probed SSIDs
4184	2021-03-18 13:20:14	2021-03-18 13:20:14	4C:D1:A1:B4:0C:2C	107	Smith Myers Guest	
4183	2021-03-18 13:20:14	2021-03-18 13:20:14	B8:27:EB:70:C5:59	106		
4182	2021-03-18 13:20:14	2021-03-18 13:20:14	98:D8:63:79:2D:40	98		
4181	2021-03-18 13:20:14	2021-03-18 13:20:14	98:8D:46:80:F6:7E	99		
4180	2021-03-18 13:20:04	2021-03-18 13:20:04	44:AE:AB:FA:B1:75	101	Smith Myers	

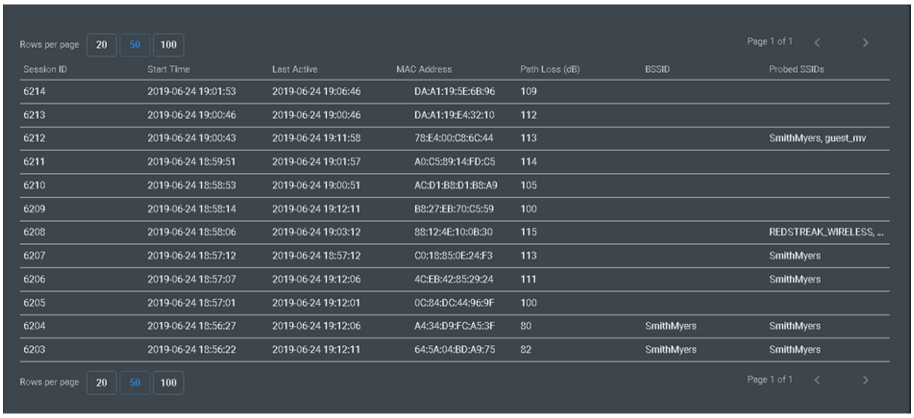
Fig 293. Wi-Fi – drop-down

31.4.2 WI-FI RESULTS – DEVICES PAGE

By default, the Devices page is displayed.

As shown at Fig 294 below, the data displayed on the Devices page is:

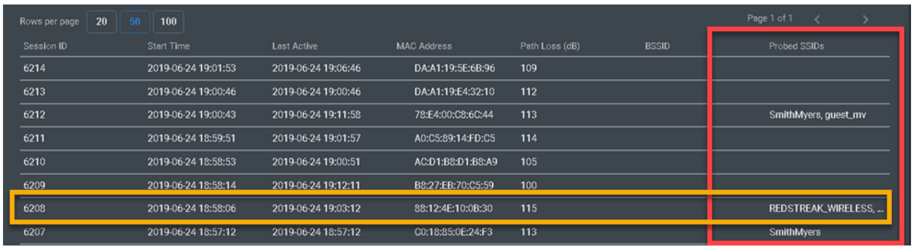
- **Session ID** One up serial number for the database entry
- **Start Time** Date/time stamp of when the data was collected
- **Last Active** The last time the data was collected
- **MAC Address** MAC address of the device detected
- **Path Loss** The signal received at NESIE
- **BSSID** The transmittted name of the Access Point
- **Probed SSIDs** The data transmitted by a mobile device / device loOKing to connect to previous hotspots (History)



Session ID	Start Time	Last Active	MAC Address	Path Loss (dB)	BSSID	Probed SSIDs
6214	2019-06-24 19:01:53	2019-06-24 19:06:46	DA:A1:19:5E:6B:96	109		
6213	2019-06-24 19:00:46	2019-06-24 19:00:46	DA:A1:19:E4:32:10	112		
6212	2019-06-24 19:00:43	2019-06-24 19:11:58	78:E4:00:C8:6C:44	113		SmithMyers, guest_mv
6211	2019-06-24 18:59:51	2019-06-24 19:01:57	A0:C5:89:14:FD:C5	114		
6210	2019-06-24 18:58:53	2019-06-24 19:00:51	AC:D1:B8:D1:B8:A9	105		
6209	2019-06-24 18:58:14	2019-06-24 19:12:11	B8:27:EB:70:C5:59	100		
6208	2019-06-24 18:58:06	2019-06-24 19:03:12	88:12:4E:10:0B:30	115		REDSTREAK_WIRELESS, ...
6207	2019-06-24 18:57:12	2019-06-24 18:57:12	C0:18:85:0E:24:F3	113		SmithMyers
6206	2019-06-24 18:57:07	2019-06-24 19:12:06	4C:EB:42:85:29:24	111		SmithMyers
6205	2019-06-24 18:57:01	2019-06-24 19:12:01	0C:84:DC:44:96:9F	100		
6204	2019-06-24 18:56:27	2019-06-24 19:12:06	A4:34:D9:FC:A5:3F	80	SmithMyers	SmithMyers
6203	2019-06-24 18:56:22	2019-06-24 19:12:11	64:5A:04:BD:A9:75	82	SmithMyers	SmithMyers

Fig 294. Wi-Fi – Devices

In the example shown at Fig 295 below, some Probed SSID data has been detected (Red Box). Two devices are transmitting probes in order to search for and connect to a previously used Wi-Fi AP. These probes are loOKing for a previously used Wi-Fi AP (Smith Myers). These probes are listed in the UI.



Session ID	Start Time	Last Active	MAC Address	Path Loss (dB)	BSSID	Probed SSIDs
6214	2019-06-24 19:01:53	2019-06-24 19:06:46	DA:A1:19:5E:6B:96	109		
6213	2019-06-24 19:00:46	2019-06-24 19:00:46	DA:A1:19:E4:32:10	112		
6212	2019-06-24 19:00:43	2019-06-24 19:11:58	78:E4:00:C8:6C:44	113		SmithMyers, guest_mv
6211	2019-06-24 18:59:51	2019-06-24 19:01:57	A0:C5:89:14:FD:C5	114		
6210	2019-06-24 18:58:53	2019-06-24 19:00:51	AC:D1:B8:D1:B8:A9	105		
6209	2019-06-24 18:58:14	2019-06-24 19:12:11	B8:27:EB:70:C5:59	100		
6208	2019-06-24 18:58:06	2019-06-24 19:03:12	88:12:4E:10:0B:30	115		REDSTREAK_WIRELESS, ...
6207	2019-06-24 18:57:12	2019-06-24 18:57:12	C0:18:85:0E:24:F3	113		SmithMyers

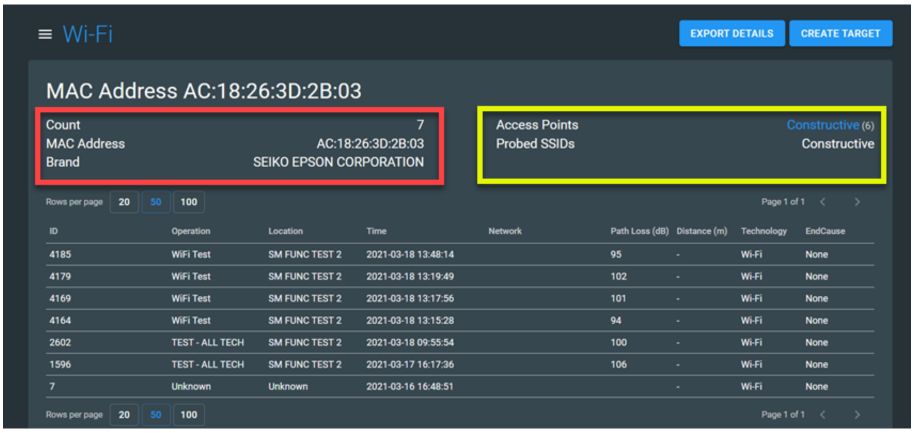
Fig 295. Probed SSID

In the example highlighted in the amber box, one device is transmitting to multiple access points. This is shown in the Probed SSIDs column as:

‘REDSTREAK_WIRELESS, **...**’

The ‘**...**’ indicates that multiple probe requests have been detected and there is not enough room in the column to display the data. If the operator hovers over the column, the other data will be displayed.

At any time, the operator can investigate what other data is held on a MAC address that has issued these probe requests by clicking on the MAC address as shown below in Fig 296.



MAC Address AC:18:26:3D:2B:03

Count	7
MAC Address	AC:18:26:3D:2B:03
Brand	SEIKO EPSON CORPORATION

Access Points	Constructive (6)
Probed SSIDs	Constructive

ID	Operation	Location	Time	Network	Path Loss (dB)	Distance (m)	Technology	EndCause
4185	WiFi Test	SM FUNC TEST 2	2021-03-18 13:48:14		95	-	Wi-Fi	None
4179	WiFi Test	SM FUNC TEST 2	2021-03-18 13:19:49		102	-	Wi-Fi	None
4169	WiFi Test	SM FUNC TEST 2	2021-03-18 13:17:56		101	-	Wi-Fi	None
4164	WiFi Test	SM FUNC TEST 2	2021-03-18 13:15:28		94	-	Wi-Fi	None
2602	TEST - ALL TECH	SM FUNC TEST 2	2021-03-18 09:55:54		100	-	Wi-Fi	None
1596	TEST - ALL TECH	SM FUNC TEST 2	2021-03-17 16:17:36		106	-	Wi-Fi	None
7	Unknown	Unknown	2021-03-16 16:48:51			-	Wi-Fi	None

Fig 296. MAC addres – details

In the example shown above, the red box contains the following information:

- **Count** Number of times this MAC has been detected
- **MAC Address** The MAC address for the device
- **Brand** Make / Model for the MAC device

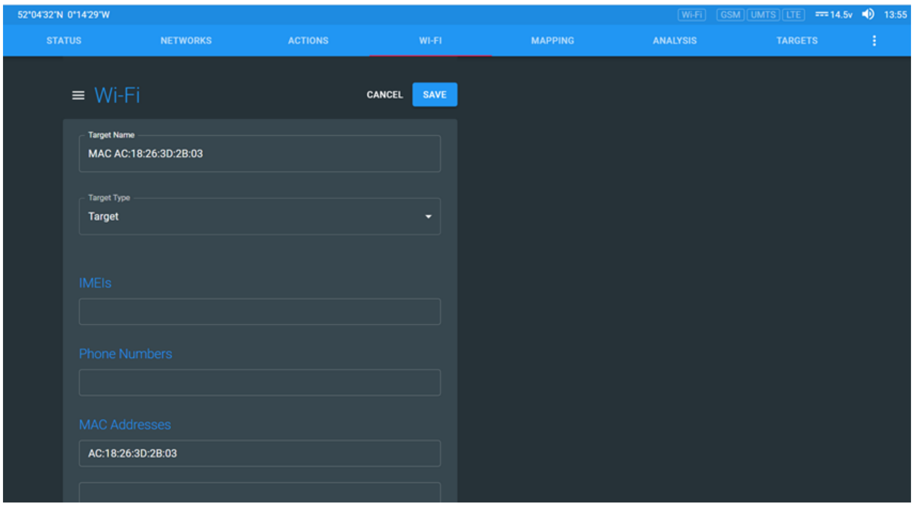
The yellow box shows the following information:

- **Access Points** APs that have been associated with this device
- **Probed SSIDs** Any probes that have been detected

The operator can now turn this device into a Target by pressing the CREATE TARGET button. When the CREATE TARGET button is pressed, the Target page is displayed as shown below in Fig 297.

This page is the same as the cellular Target page, however, the MAC address will be used as the default Target name.

If required, the operator could add the MAC address to a previously created cellular Target.



Wi-Fi

Target Name: MAC AC:18:26:3D:2B:03

Target Type: Target

IMEIs

Phone Numbers

MAC Addresses: AC:18:26:3D:2B:03

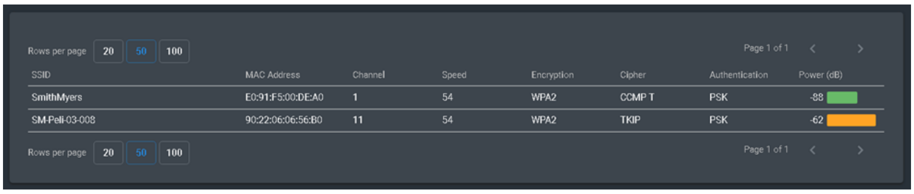
Fig 297. Wi-Fi Target

31.4.3 WI-FI RESULTS – HOTSPOTS

The NESIE operator can also view the list of Hotspots that have been detected during a Wi-Fi sniff by navigating to Wi-Fi / Hotspots as shown at Fig 293 above.

The data in the Wi-Fi channel list table is as follows:

• **SSID**	The name of the device as detected
• **MAC Address**	MAC address for the device detected
• **Channel**	The Wi-Fi channel being used by the device
• **Speed**	Data speed
• **Encrypt**	The type of encryption used by the AP device
• **Cipher**	The security protocols used by the AP device
• **Authentication**	Authentication protocols used by the AP device
• **Power**	The signal strength of the received signal

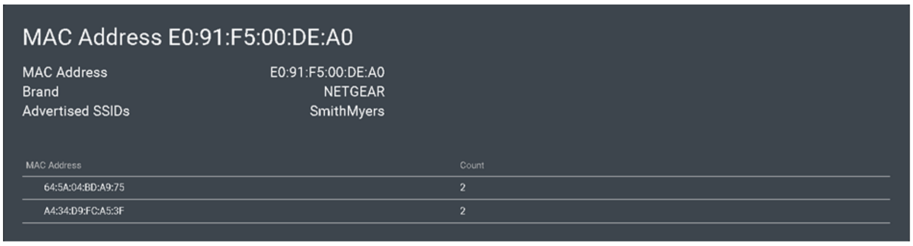


SSID	MAC Address	Channel	Speed	Encryption	Cipher	Authentication	Power (dB)
SmithMyers	E0:91:F5:00:DE:A0	1	54	WPA2	CCMP T	PSK	-88 🟩
SM-Peli-03-008	90:22:06:06:56:B0	11	54	WPA2	TKIP	PSK	-62 🟧

Fig 298. Channel list

The NESIE operator can also investigate the devices that are currently connected to any listed Access Point. The operator should click the MAC address for the required SSID.

In the example below at Fig 299, 2 Wi-Fi devices were logged as being connected to the Smith Myers Access Point. The MAC address for each of these devices is displayed.



MAC Address E0:91:F5:00:DE:A0

MAC Address	E0:91:F5:00:DE:A0
Brand	NETGEAR
Advertised SSIDs	SmithMyers

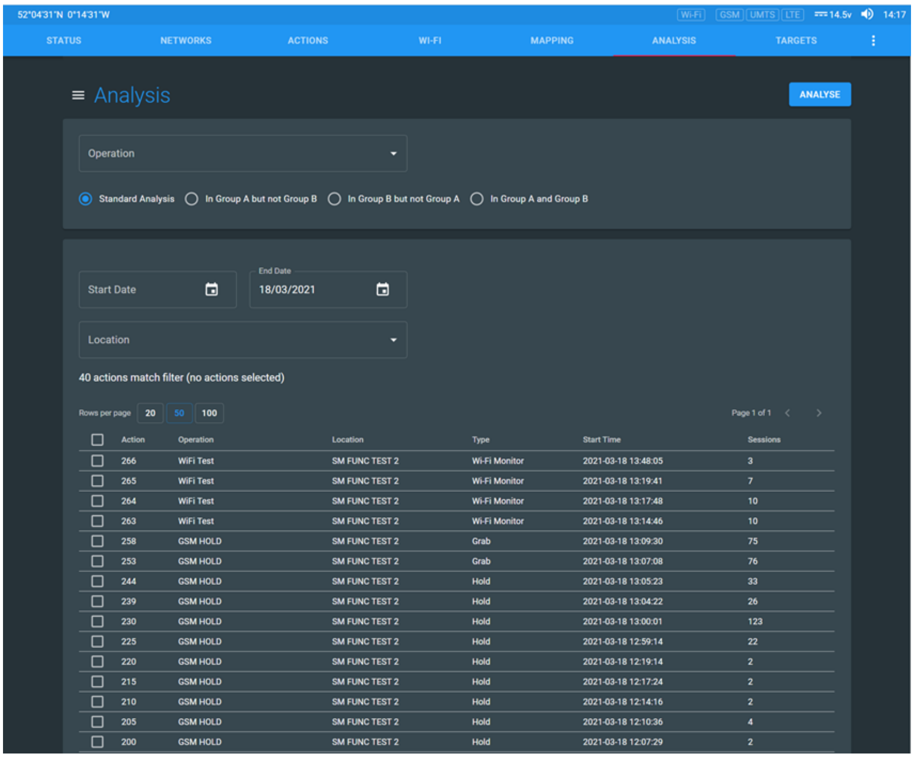
MAC Address	Count
64:5A:04:BD:A9:75	2
A4:34:D9:FC:A5:3F	2

Fig 299. Wi-Fi devices connected to AP

The Wi-Fi module will continue to run independently of the NESIE cellular activity. To stop the Wi-Fi monitoring, the operator must use the STOP button. The Wi-Fi module will return to idle mode when the operation is stopped.

32. ANALYSIS

The NESIE operator has the option to carry out first line analysis of the data collected by using the ANALYSIS page on the UI as shown in Fig 300 below.



● Standard Analysis ○ In Group A but not Group B ○ In Group B but not Group A ○ In Group A and Group B

End Date: 18/03/2021

40 actions match filter (no actions selected)

□	Action	Operation	Location	Type	Start Time	Sessions
□	266	WiFi Test	SM FUNC TEST 2	Wi-Fi Monitor	2021-03-18 13:48:05	3
□	265	WiFi Test	SM FUNC TEST 2	Wi-Fi Monitor	2021-03-18 13:19:41	7
□	264	WiFi Test	SM FUNC TEST 2	Wi-Fi Monitor	2021-03-18 13:17:48	10
□	263	WiFi Test	SM FUNC TEST 2	Wi-Fi Monitor	2021-03-18 13:14:46	10
□	258	GSM HOLD	SM FUNC TEST 2	Grab	2021-03-18 13:09:30	75
□	253	GSM HOLD	SM FUNC TEST 2	Grab	2021-03-18 13:07:08	76
□	244	GSM HOLD	SM FUNC TEST 2	Hold	2021-03-18 13:05:23	33
□	239	GSM HOLD	SM FUNC TEST 2	Hold	2021-03-18 13:04:22	26
□	230	GSM HOLD	SM FUNC TEST 2	Hold	2021-03-18 13:00:01	123
□	225	GSM HOLD	SM FUNC TEST 2	Hold	2021-03-18 12:59:14	22
□	220	GSM HOLD	SM FUNC TEST 2	Hold	2021-03-18 12:19:14	2
□	215	GSM HOLD	SM FUNC TEST 2	Hold	2021-03-18 12:17:24	2
□	210	GSM HOLD	SM FUNC TEST 2	Hold	2021-03-18 12:14:16	2
□	205	GSM HOLD	SM FUNC TEST 2	Hold	2021-03-18 12:10:36	4
□	200	GSM HOLD	SM FUNC TEST 2	Hold	2021-03-18 12:07:29	2

Fig 300. ANALYSIS page

32.1 ANALYSIS – SUB MENU

By default, the ANALYSIS Actions page is displayed. The ANALYSIS page also has a sub menu as shown below in Fig 301, giving the following options:

- **Analyse Actions**
- **Search**

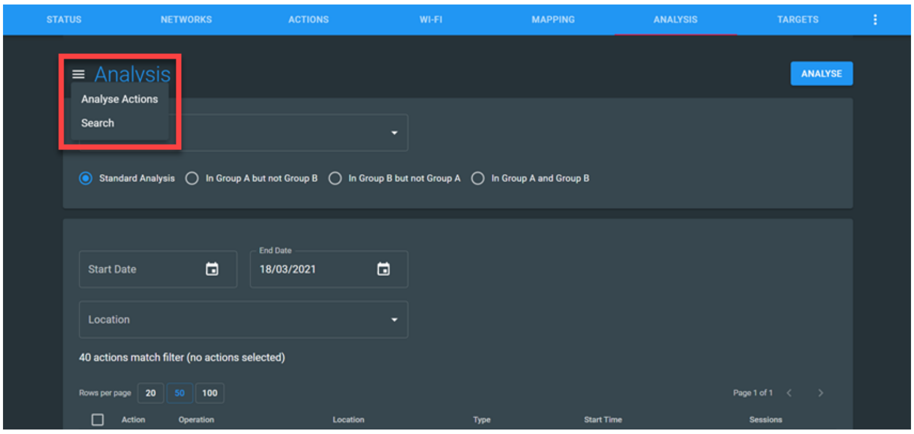
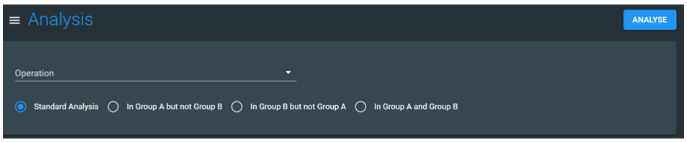


Fig 301. ANALYSIS page – sub menu

32.2 ANALYSE ACTIONS

The ANALYSIS page header as shown below in Fig 302, allows the operator to choose several different options:



● Standard Analysis ○ In Group A but not Group B ○ In Group B but not Group A ○ In Group A and Group B

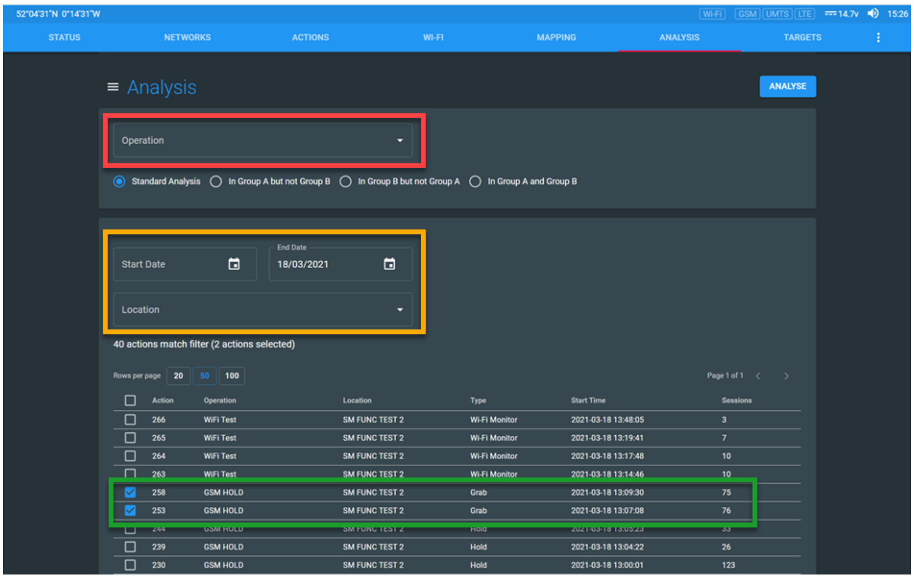
Fig 302. ANALYSIS page - options

- **Standard Analysis**
- **Advanced Analysis**
  - **In Group A but not Group B**
  - **In Group B but not Group A**
  - **In Group A and Group B**

32.2.1 STANDARD ANALYSIS

By default, when the operator navigates to the ANALYSIS page, the Standard Analysis option will be displayed as shown in Fig 300 above. This page will display a list of every Action (Grab, Hunt, Hold etc) that is contained on the system memory. This list is ordered by start time, with the newest data at the top of the list.

The operator can now filter the files displayed by Operation (Red Box), Start Date, End Date and Location (Yellow Box) as shown below in Fig 303. The operator can now select the required files by ticking the box as shown in the green box.



● Standard Analysis ○ In Group A but not Group B ○ In Group B but not Group A ○ In Group A and Group B

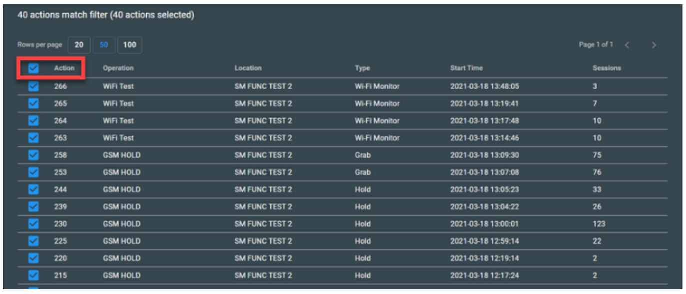
End Date: 18/03/2021

40 actions match filter (2 actions selected)

□	Action	Operation	Location	Type	Start Time	Sessions
□	266	WiFi Test	SM FUNC TEST 2	Wi-Fi Monitor	2021-03-18 13:48:05	3
□	265	WiFi Test	SM FUNC TEST 2	Wi-Fi Monitor	2021-03-18 13:19:41	7
□	264	WiFi Test	SM FUNC TEST 2	Wi-Fi Monitor	2021-03-18 13:17:48	10
□	263	WiFi Test	SM FUNC TEST 2	Wi-Fi Monitor	2021-03-18 13:14:46	10
☑	258	GSM HOLD	SM FUNC TEST 2	Grab	2021-03-18 13:09:30	75
☑	253	GSM HOLD	SM FUNC TEST 2	Grab	2021-03-18 13:07:08	76
□	244	GSM HOLD	SM FUNC TEST 2	Hold	2021-03-18 13:05:23	33
□	239	GSM HOLD	SM FUNC TEST 2	Hold	2021-03-18 13:04:22	26
□	230	GSM HOLD	SM FUNC TEST 2	Hold	2021-03-18 13:00:01	123

Fig 303. ANALYSIS page – select files

If all files from an Operation and its locations are required, the operator can check the All Action button. All the files will be checked, as shown in Fig 304 below.



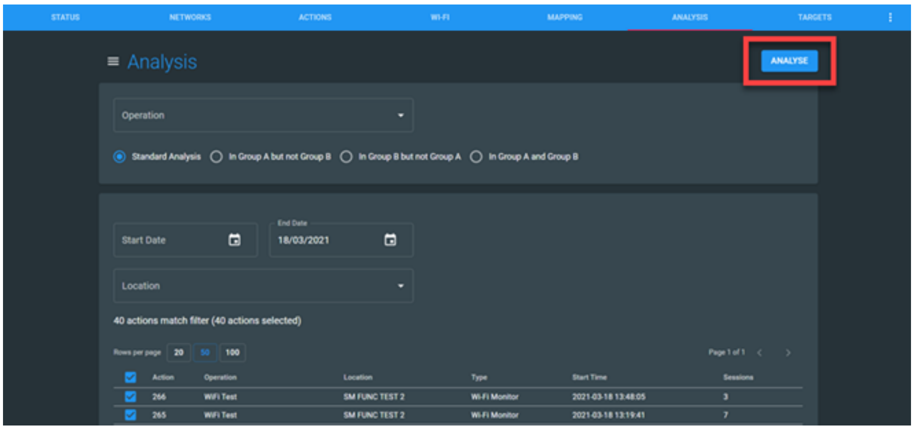
40 actions match filter (40 actions selected)

Rows per page 20 50 100 Page 1 of 1

☑	Action	Operation	Location	Type	Start Time	Sessions
☑	266	WiFi Test	SM FUNC TEST 2	Wi-Fi Monitor	2021-03-18 13:48:05	3
☑	265	WiFi Test	SM FUNC TEST 2	Wi-Fi Monitor	2021-03-18 13:19:41	7
☑	264	WiFi Test	SM FUNC TEST 2	Wi-Fi Monitor	2021-03-18 13:17:48	10
☑	263	WiFi Test	SM FUNC TEST 2	Wi-Fi Monitor	2021-03-18 13:14:46	10
☑	258	GSM HOLD	SM FUNC TEST 2	Grab	2021-03-18 13:09:30	75
☑	253	GSM HOLD	SM FUNC TEST 2	Grab	2021-03-18 13:07:08	76
☑	244	GSM HOLD	SM FUNC TEST 2	Hold	2021-03-18 13:05:23	33
☑	239	GSM HOLD	SM FUNC TEST 2	Hold	2021-03-18 13:04:22	26
☑	230	GSM HOLD	SM FUNC TEST 2	Hold	2021-03-18 13:00:01	123
☑	225	GSM HOLD	SM FUNC TEST 2	Hold	2021-03-18 12:59:14	22
☑	220	GSM HOLD	SM FUNC TEST 2	Hold	2021-03-18 12:19:14	2
☑	215	GSM HOLD	SM FUNC TEST 2	Hold	2021-03-18 12:17:24	2

Fig 304. ANALYSIS page – select all

When the operator has selected the appropriate files, the ANALYSE button should be pressed as shown below in Fig 305.



Analysis

Operation

● Standard Analysis ○ In Group A but not Group B ○ In Group B but not Group A ○ In Group A and Group B

Start Date

End Date 18/03/2021

Location

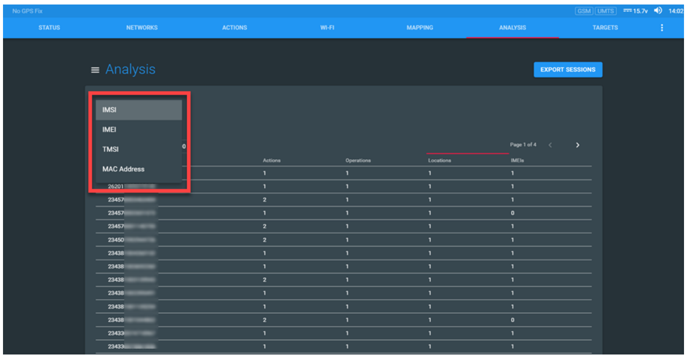
40 actions match filter (40 actions selected)

Rows per page 20 50 100 Page 1 of 1

☑	Action	Operation	Location	Type	Start Time	Sessions
☑	266	WiFi Test	SM FUNC TEST 2	Wi-Fi Monitor	2021-03-18 13:48:05	3
☑	265	WiFi Test	SM FUNC TEST 2	Wi-Fi Monitor	2021-03-18 13:19:41	7

Fig 305. ANALYSE button

The operator will be presented with a table of identities captured from all the selected actions as shown in Fig 306 below.



Analysis

Page 1 of 4

	Actions	Operations	Locations	IMEIs
	1	1	1	1
26201[redacted]	1	1	1	1
23457[redacted]	2	1	1	1
23457[redacted]	1	1	1	0
23457[redacted]	2	1	1	1
23450[redacted]	2	1	1	1
23438[redacted]	1	1	1	1
23438[redacted]	1	1	1	1
23438[redacted]	2	1	1	1
23438[redacted]	1	1	1	1
23438[redacted]	1	1	1	1
23438[redacted]	2	1	1	0
23433[redacted]	1	1	1	1
23433[redacted]	1	1	1	1

Fig 306. Analyse identity captures

By default, the identities in this table are listed by IMSI, however, if required, the operator has the option to change the type of data displayed in the table by choosing from the Identity Type drop-down menu shown in the red box in Fig 306 above. These options are IMEI, IMSI, TMSI or MAC Address.

The combined files to be analysed will be presented in a table with the following columns:

Identity Identity – IMEI, IMSI TMSI or MAC Address

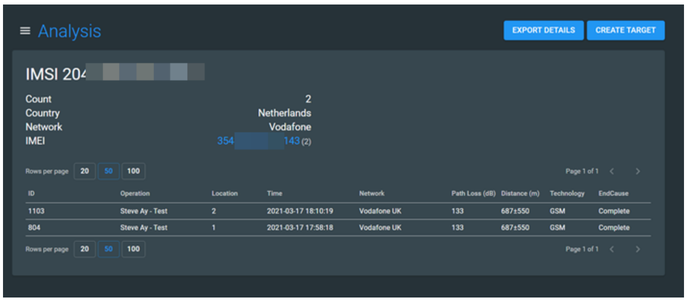
Actions Number of Actions (Grabs etc) that the identity was seen in

Operations How many operations the ID was found in
(usually only one if selected by Operation previously)

Locations How many locations the ID was seen at

IMEIs How many associated IMEIs with this identity

By clicking on any identity, the operator can investigate if any further information is in the database for that identity. As shown at Fig 307 below, the operator has clicked on the identity and has found additional data is already in the database.



IMSI 204[redacted]

Count 2
Country Netherlands
Network Vodafone
IMEI 354[redacted]143 (2)

ID	Operation	Location	Time	Network	Path Loss (dB)	Distance (m)	Technology	EndCause
1103	Steve Ay - Test	2	2021-03-17 18:10:19	Vodafone UK	133	687±550	GSM	Complete
804	Steve Ay - Test	1	2021-03-17 17:58:18	Vodafone UK	133	687±550	GSM	Complete

Fig 307. Further identity details

The identity details page displays the following data:

Header information:

- **IMSI** ID of the Target
- **IMEI** ID of the Target
- **Count** Number of time ID has been detected in database
- **Country** Country of origin of the SIM card
- **Target Name** Name of Target as saved by the operator
- **Device Brand** Brand of device as extracted from the IMEI
- **Device Model** Model of device as extracted from the IMEI
- **Total Session** Number of times the Identity has be captures

Table Data:

- **ID** A one up serial for the database entry
- **Operation** Name of the operation where data was collected
- **Location** Location entered by operator
- **Time** Date time stamp as logged by NESIE
- **Network** Network the Target was on when logged
- **Path Loss** Path loss between NESIE and Target device
- **Distance** The distance to the Target as calculated by NESIE

- **Technology** Tech transmitted by NESIE when ID was captured
- **End Cause** Reason the connection to the phone was ended

32.2.2 ADVANCED ANALYSIS

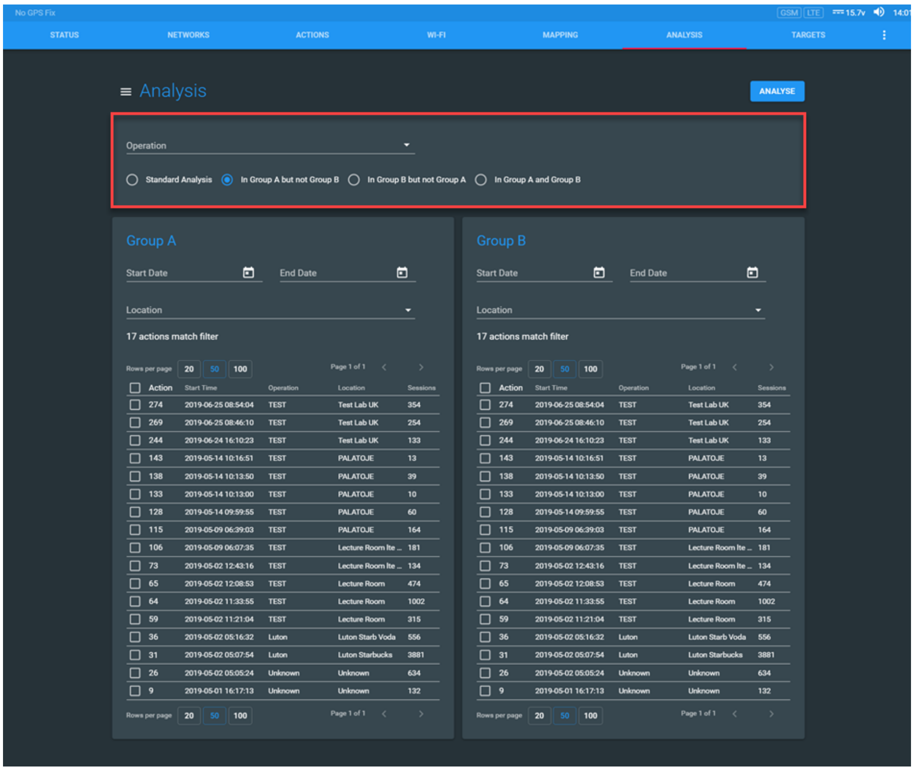
In the Advanced Analysis section, the operator has the option to compare different sets of complied files on the UI. E.g.: a series of 5 Grabs have been carried out whilst a Target has been in a coffee shop. After the first 5 Grabs, another person enters the coffee shop and is in a meeting with the primary Target. The NESIE operator carried out another 5 Grabs to identify the secondary Targets device ID.

In this case the first 5 Grabs are compiled in GROUP A, the second series of 5 Grabs are compiled into GROUP B. These two groups could then be compared loOKing for the identity that has appeared. The operator has the option to compare these groups in the following way:

- In Group A but not Group B
- In Group B but not Group A
- In Group A and Group B

The operator can choose which comparison type they wish to use by clicking the relevant button in the user analysis header bar as shown below in Fig 308 below.

As shown below, when the operator chooses one of the advanced options, the UI will change to reflect the selection. In this example, the UI shows the list of files that can be complied into GROUP A and the second pane shows the files that can be selected and compiled into GROUP B.



○ Standard Analysis ● In Group A but not Group B ○ In Group B but not Group A ○ In Group A and Group B

17 actions match filter

Rows per page 20 50 100 Page 1 of 1

□	Action	Start Time	Operation	Location	Sessions
□	274	2019-06-25 08:54:04	TEST	Test Lab UK	354
□	269	2019-06-25 08:46:10	TEST	Test Lab UK	254
□	244	2019-06-24 16:10:23	TEST	Test Lab UK	133
□	143	2019-05-14 10:16:51	TEST	PALATOJE	13
□	138	2019-05-14 10:13:50	TEST	PALATOJE	39
□	133	2019-05-14 10:13:00	TEST	PALATOJE	10
□	128	2019-05-14 09:59:55	TEST	PALATOJE	60
□	115	2019-05-09 06:39:03	TEST	PALATOJE	164
□	106	2019-05-09 06:07:35	TEST	Lecture Room lte ...	181
□	73	2019-05-02 12:43:16	TEST	Lecture Room lte ...	134
□	65	2019-05-02 12:08:53	TEST	Lecture Room	474
□	64	2019-05-02 11:33:55	TEST	Lecture Room	1002
□	59	2019-05-02 11:21:04	TEST	Lecture Room	315
□	36	2019-05-02 05:16:32	Luton	Luton Starb Voda	556
□	31	2019-05-02 05:07:54	Luton	Luton Starbucks	3881
□	26	2019-05-02 05:05:24	Unknown	Unknown	634
□	9	2019-05-01 16:17:13	Unknown	Unknown	132

Rows per page 20 50 100 Page 1 of 1

17 actions match filter

Rows per page 20 50 100 Page 1 of 1

□	Action	Start Time	Operation	Location	Sessions
□	274	2019-06-25 08:54:04	TEST	Test Lab UK	354
□	269	2019-06-25 08:46:10	TEST	Test Lab UK	254
□	244	2019-06-24 16:10:23	TEST	Test Lab UK	133
□	143	2019-05-14 10:16:51	TEST	PALATOJE	13
□	138	2019-05-14 10:13:50	TEST	PALATOJE	39
□	133	2019-05-14 10:13:00	TEST	PALATOJE	10
□	128	2019-05-14 09:59:55	TEST	PALATOJE	60
□	115	2019-05-09 06:39:03	TEST	PALATOJE	164
□	106	2019-05-09 06:07:35	TEST	Lecture Room lte ...	181
□	73	2019-05-02 12:43:16	TEST	Lecture Room lte ...	134
□	65	2019-05-02 12:08:53	TEST	Lecture Room	474
□	64	2019-05-02 11:33:55	TEST	Lecture Room	1002
□	59	2019-05-02 11:21:04	TEST	Lecture Room	315
□	36	2019-05-02 05:16:32	Luton	Luton Starb Voda	556
□	31	2019-05-02 05:07:54	Luton	Luton Starbucks	3881
□	26	2019-05-02 05:05:24	Unknown	Unknown	634
□	9	2019-05-01 16:17:13	Unknown	Unknown	132

Rows per page 20 50 100 Page 1 of 1

Fig 308. Analysis – advanced options

As per the instructions in the standard analysis section, when the user has selected the files required, he will then press the ANALYSE button.

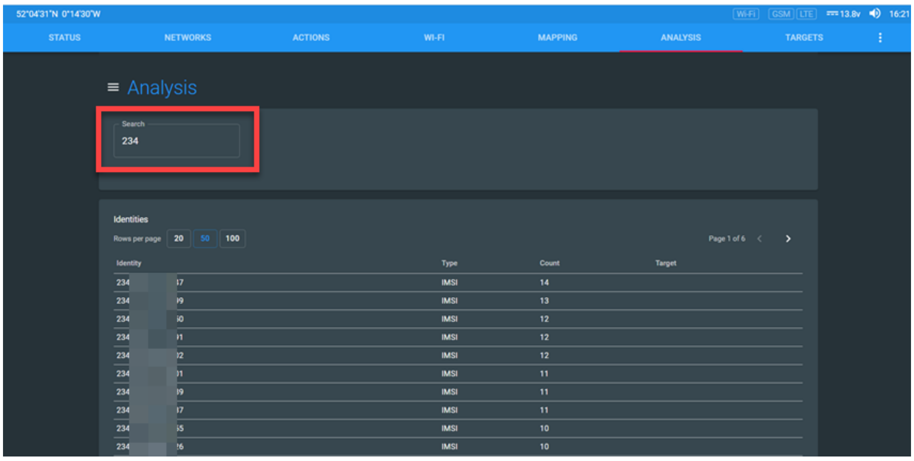
The UI will now present the resultant information for further analysis.

32.3 IDENTITY SEARCH

The operator can use the Search facility to carry out a search of the whole database for any identity. This search is a 'wild card' search and may contain any part of the identity (IMEI, IMSI, TIMSI, MAC or Mobile Device Number), as shown in Fig 309 below. The search can be accessed via ANALYSIS / Sub Menu / Identity Search**.**

Enter at least 3 or more characters into the Filter field. As the values are entered the list will dynamically adjust to show the matching identities. This search can be from any part of the identity (front, middle or end) and the more digits entered, the shorter the list of possible matches.

In the example below, the digits 234 have been entered into the search field. The list below now shows any entry from the database that contains a string of digits to match 234. The results are listed by the number of times that they have been found in the database.



Search: 234

Identity	Type	Count	Target
234[redacted]7	IMSI	14	
234[redacted]9	IMSI	13	
234[redacted]0	IMSI	12	
234[redacted]1	IMSI	12	
234[redacted]2	IMSI	12	
234[redacted]1	IMSI	11	
234[redacted]9	IMSI	11	
234[redacted]7	IMSI	11	
234[redacted]5	IMSI	10	
234[redacted]6	IMSI	10	

Fig 309. Identity search

As per previous sections the operator has the option to click on the identity or Target name to investigate the data saved in the NESIE database.

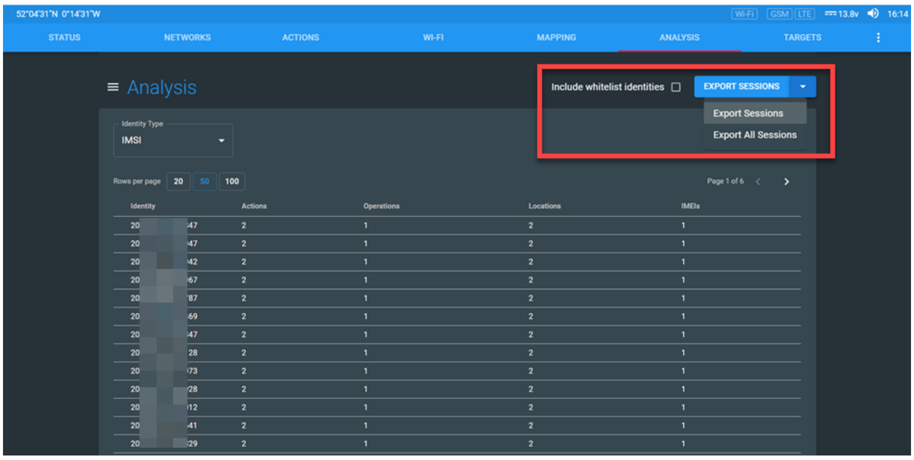
32.4 EXPORTING THE DATA

Whilst analysing the gathered data, it is possible to export the captured identities and information associated to it, as a Comma Separated Value (CSV) file, that can then be imported into a spread sheet or database application for more detailed analysis.

NOTE: Further details of how to import / export a CSV file in Microsoft XL are detailed at section 38.

32.4.1 EXPORT SESSIONS

As shown in Fig 310, the operator has the option to export the session data that is currently being analysed. In the example shown below the NESIE operator has selected two individual files and combined them into one file. If required, this combined file can now be exported for further analysis.   However, the operator has options to include / exclude data by choosing the options in the red box.



Identity	Actions	Operations	Locations	IMEIs
20[redacted]47	2	1	2	1
20[redacted]47	2	1	2	1
20[redacted]42	2	1	2	1
20[redacted]67	2	1	2	1
20[redacted]87	2	1	2	1
20[redacted]69	2	1	2	1
20[redacted]47	2	1	2	1
20[redacted]28	2	1	2	1
20[redacted]73	2	1	2	1
20[redacted]28	2	1	2	1
20[redacted]12	2	1	2	1
20[redacted]41	2	1	2	1
20[redacted]29	2	1	2	1

Fig 310. Export identity captures

32.4.1.1 EXPORT SESSIONS OPTIONS

- **Include whitelist identities**
  By default, the tick box is blank and any whitelist identities will be excluded from the export. If the whitelist IDs are to be included, the operator should click this box prior to exporting the data.

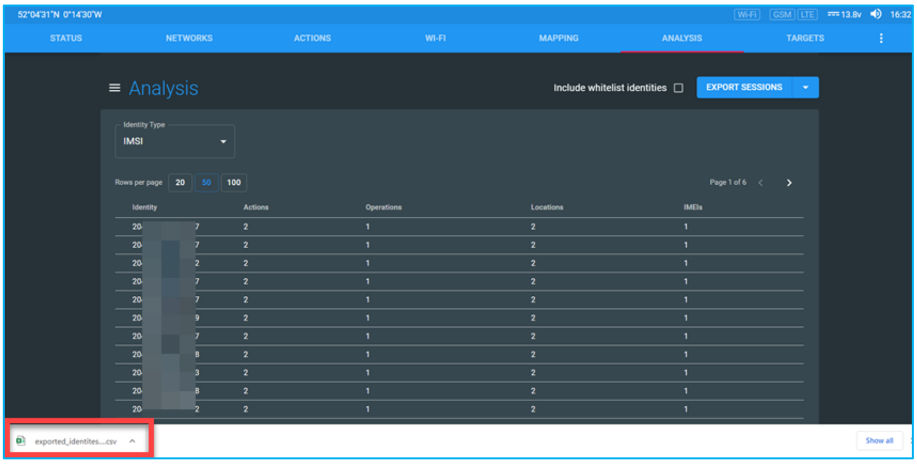
- **Export Sessions**
  The EXPORT SESSIONS option will export the compiled data for this selected ID (IMEI / IMSI / TMSI) only.

  When the operator presses the EXPORT SESSIONS button, a .CSV file will be downloaded to the laptop. The file that is created will contain all the ID data (only that selected) in this current analysis, but will exclude any invalid identities or any identities in the Whitelist (unless ticked)

- **Export All Sessions**
  The Export All Sessions option will export the compiled data and include all IDs (IMEI / IMSI / TMSI) if they are held in the database.

  When the operator presses the EXPORT ALL SESSIONS button, a .CSV file will be downloaded to the laptop. The file that is created will contain all the IMEI, IMSI, TMSI and MAC data in this current analysis, but will exclude any invalid identities or any identities in the Whitelist (unless ticked)

The export file will be downloaded from the NESIE system onto the tablet/laptop using the normal browser download method. In the example shown below at Fig 311, Google Chrome has been used and a link to the downloaded file is shown at the bottom of the browser window.



Identity Type: IMSI

Identity	Actions	Operations	Locations	IMEIs
20[redacted]7	2	1	2	1
20[redacted]7	2	1	2	1
20[redacted]2	2	1	2	1
20[redacted]7	2	1	2	1
20[redacted]7	2	1	2	1
20[redacted]9	2	1	2	1
20[redacted]7	2	1	2	1
20[redacted]8	2	1	2	1
20[redacted]3	2	1	2	1
20[redacted]8	2	1	2	1
20[redacted]2	2	1	2	1

Fig 311. Analysis – exported CSV file

This downloaded file is in the .CSV format and if the operator clicks onto the file, it will open directly in Microsoft XL. However, as previously mentioned, .CSV files will not normally be display correctly in Microsoft XL. The file usually has to be formatted to ensure the data is displayed correctly. For more instructions refer to section 38.

33. ADDITIONAL MENU ICON - SETTINGS

NOTE: Some of these settings have been previously discussed in section 7 'Setting up NESIE prior to use'.

These sections have been repeated here and any additional information / settings are discussed.

By default, the NESIE system will have been set up for testing in the United Kingdom. Where possible, the system will be set up for in country operations prior to delivery. However, the user should ensure that the NESIE is optimized for operations in their region.

To change the NESIE settings, the user should click on the Menu icon that as shown below in Fig 312.

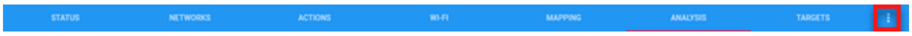


Fig 312. Menu – options icon

The additional menu will appear, and the user will have the option to adjust the following sections:

- **Change Password**
- **Redirect**
- **Settings**
- **Admin**
- **Log Out**
- **Power Off**

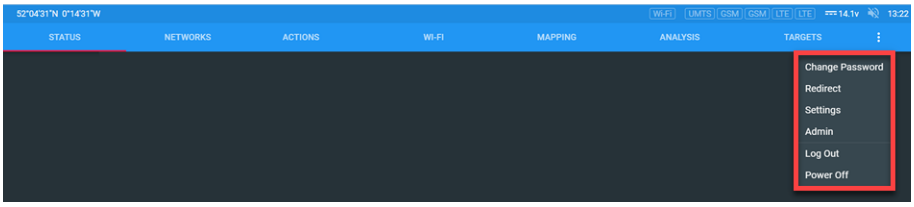
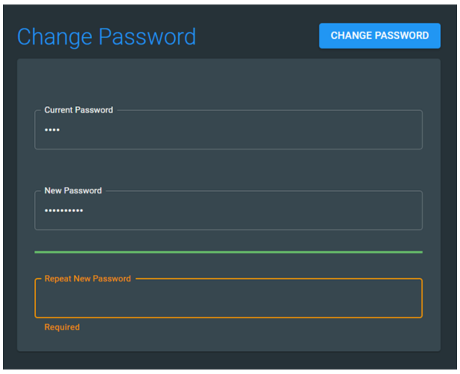


Fig 313. Menu – options menu

33.1 CHANGE PASSWORD

When Change Password is pressed, a pop-up menu will be displayed as shown in Fig 314 below.

To change the password, the Current Password should be entered in the top field. Then enter the New Password in the second field; The New Password must then be repeated in the third field. Then press the CHANGE PASSWORD button.



Current Password
····

New Password
··········

Repeat New Password

Required

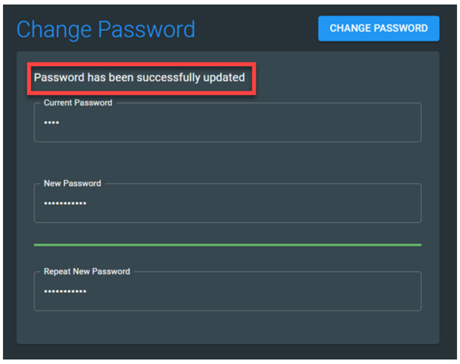
Fig 314. Change Password

NOTE: The default NESIE password is: root

The coloured bar under the New Password will show:

- **Red** If the password contains 3 or less characters
- **Amber** If the password contains 3 – 10 numbers
- **Amber** If the password contains 3 – 7 letters
- **Green** If the password contains more than 10 numbers
- **Green** If the password contains 8 or more letters or a combination of letters / numbers.

If the current password is correct and the new passwords match, the password will be successfully updated and the UI will display Password has been successfully updated, as shown in Fig 315.



Password has been successfully updated

Current Password
····

New Password
···········

Repeat New Password
···········

Fig 315. Password changed successfully

NOTE: There is no requirement for a minimum number or type of characters to be used in the password. However, it is recommended that the password should be:

- **At least 8 characters**
- **Contain at least one capital letter**
- **Contain at least one number**
- **Contain at least one special character**

It is also recommended that the password is changed at the following times:

- **After arrival in country**
- **After the system has been away for update / repair**
- **After training – if a Smith Myers representative was present**
- **After personnel leave the unit**
- **Periodically e.g. every 6 months.**

33.2 REDIRECT

A Redirect is an Action that has 2 different options to start it running. The option shown in the Settings menu is the 2nd option.

A Redirect is the process of transmitting fake base transceiver stations to gather the IMEIs and IMSI from all the cellular devices on UMTS and LTE and then sending a network command to the devices, so they are redirected down to GSM.

Normally this operation would be done in conjunction with another piece of GSM intercept equipment (Not supplied by Smith Myers).

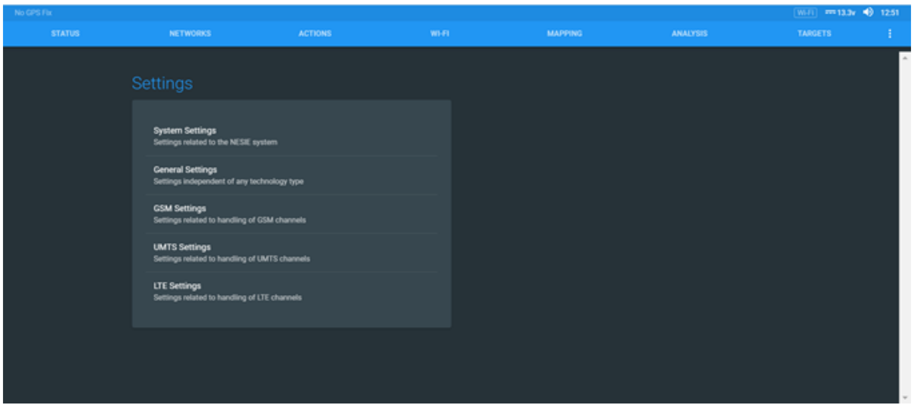
NOTE: Because this is an Action and they have all be individually detailed previously, the operator should refer to section 29.2 for detailed instructions.

33.3 SETTINGS

When the Settings button is pressed, the Settings page will be displayed, as shown in Fig 316 below.

The Settings page has the following options:

- **System Settings**
- **General Settings**
- **GSM Settings**
- **UMTS Settings**
- **LTE Settings**



Settings

System Settings
Settings related to the NESIE system

General Settings
Settings independent of any technology type

GSM Settings
Settings related to handling of GSM channels

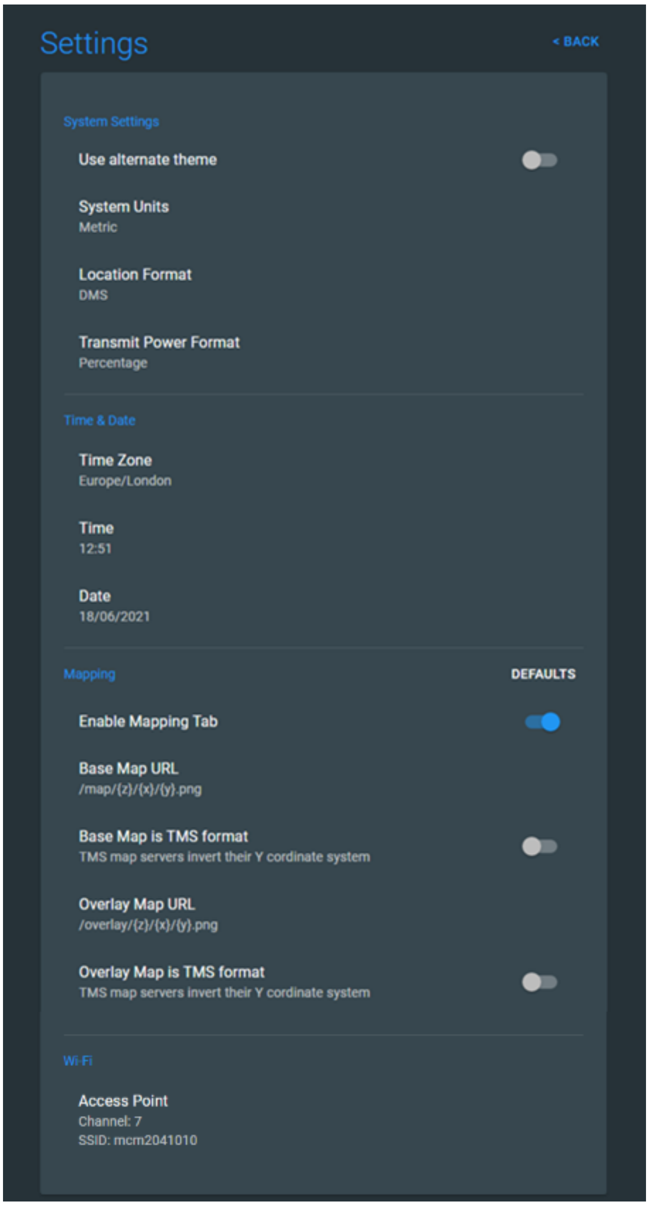
UMTS Settings
Settings related to handling of UMTS channels

LTE Settings
Settings related to handling of LTE channels

Fig 316. Settings options – detail

33.3.1 SYSTEM SETTINGS

When clicking on the System Settings, the operator will see the page shown below at Fig 317.



Settings

< BACK

System Settings

Use alternate theme ○

System Units
Metric

Location Format
DMS

Transmit Power Format
Percentage

Time & Date

Time Zone
Europe/London

Time
12:51

Date
18/06/2021

Mapping

DEFAULTS

Enable Mapping Tab ●

Base Map URL
/map/{z}/{x}/{y}.png

Base Map is TMS format ○
TMS map servers invert their Y cordinate system

Overlay Map URL
/overlay/{z}/{x}/{y}.png

Overlay Map is TMS format ○
TMS map servers invert their Y cordinate system

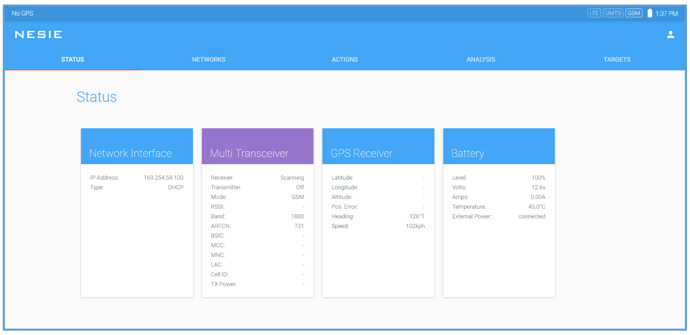
Wi-Fi

Access Point
Channel: 7
SSID: mcm2041010

Fig 317. System Settings

33.3.1.1 ALTERNATIVE THEME

By default, the NESIE UI will display the black background and muted colours to ensure the UI does not drawn attention to the operator at night. The UI can be swapped into brighter colours by sliding the button from grey to blue. Alternative theme is shown below at Fig 318.



No GPS   LTE UMTS GSM 1:37 PM

NESIE

Status

Network Interface

IP Address:	169.254.54.100
Type:	DHCP

Multi Transceiver

Receiver:	Scanning
Transmitter:	Off
Mode:	GSM
RSSI:	-
Band:	1800
ARFCN:	731
BSIC:	-
MCC:	-
MNC:	-
LAC:	-
Cell ID:	-
TX Power:	-

GPS Receiver

Latitude:	-
Longitude:	-
Altitude:	-
Pos. Error:	-
Heading:	126°T
Speed:	102kph

Battery

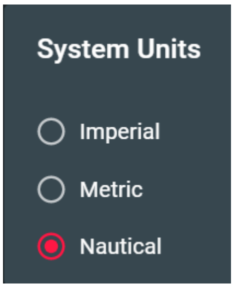
Level:	100%
Volts:	12.6v
Amps:	0.00A
Temperature:	45.0°C
External Power:	connected

Fig 318. Alternate Theme

33.3.1.2 SYSTEM UNITS

The distances shown on the NESIE UI can be changed between Metric (Km and meters), Imperial (Miles and yards) or Nautical (Nautical Miles). By default, the distance is set to Metric.

The currently selected option is shown by the red marker. To change the units the operator should click on System Units button. The dialogue box is displayed at Fig 319. The operator now clicks on the desired format. The red marker will be displayed next to the chosen setting and the window will close.



System Units

○ Imperial

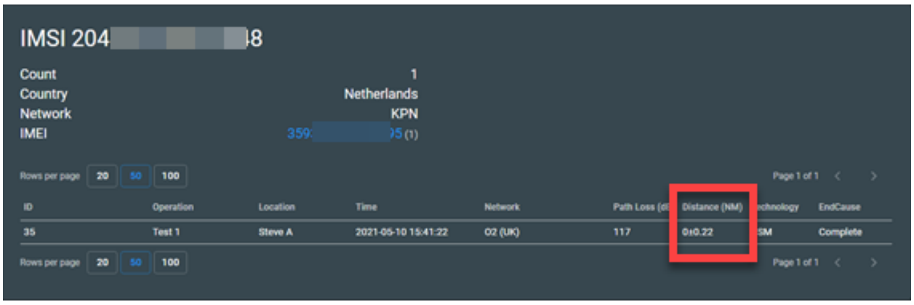
○ Metric

● Nautical

Fig 319. System Units

Any measurements / distances displayed on the UI will now be shown in the selected format. The system unit format options available are:

- **Imperial** Distances displayed in Feet
- **Metric** Distances displayed in Meters
- **Nautical** Distances displayed in Nautical Miles



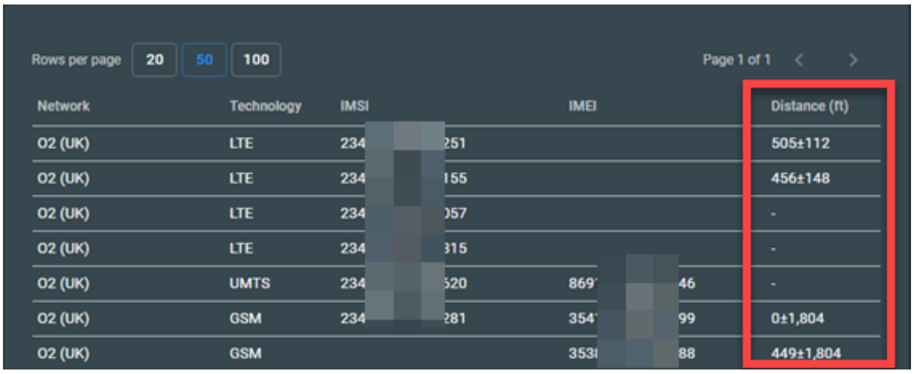
IMSI 204[redacted]8

Count	1
Country	Netherlands
Network	KPN
IMEI	359[redacted]95 (1)

ID	Operation	Location	Time	Network	Path Loss (dl	Distance (NM)	echnology	EndCause
35	Test 1	Steve A	2021-05-10 15:41:22	O2 (UK)	117	0±0.22	SM	Complete

Fig 320. Distance – Nautical Miles

When the measurement units are changed, the data displayed on different screens in the UI will be change. At Fig 320 above, the detailed database entry for a device now displays the distance in Nautical Miles. Then at Fig 321 below, the distance measurements in the main Grab identity list are now displayed in Imperial (feet).



Rows per page 20 50 100 Page 1 of 1

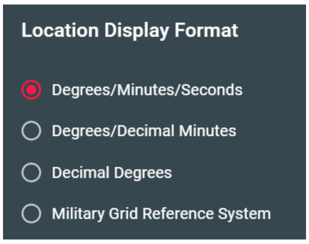
Network	Technology	IMSI	IMEI	Distance (ft)
O2 (UK)	LTE	234[redacted]251		505±112
O2 (UK)	LTE	234[redacted]155		456±148
O2 (UK)	LTE	234[redacted]057		-
O2 (UK)	LTE	234[redacted]315		-
O2 (UK)	UMTS	234[redacted]520	869[redacted]46	-
O2 (UK)	GSM	234[redacted]281	354[redacted]99	0±1,804
O2 (UK)	GSM		353[redacted]88	449±1,804

Fig 321. Distance - Imperial

33.3.1.3 GPS LOCATION FORMAT

The GPS fitted / connected to the NESIE system can display the results in four different formats. The operator can choose which Format by clicking on the Location Format button.

A pop-up menu showing the available formats will be displayed as shown at Fig 322 below. The operator can choose the desired format by clicking on the radio button. The current selected option will be shown by the red marker. To change the format, click on the desired format; the icon will turn red, and the screen will disappear.



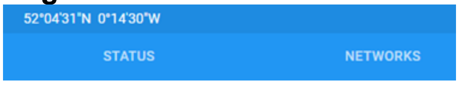
Location Display Format

● Degrees/Minutes/Seconds
○ Degrees/Decimal Minutes
○ Decimal Degrees
○ Military Grid Reference System

Fig 322. GPS format

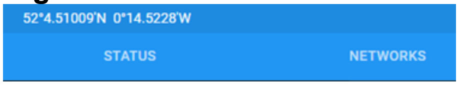
When the Location Format is changed, the UI will change accordingly. The different formats are displayed below:

- **Degrees / Minutes / Seconds**



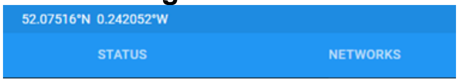
52°04'31"N 0°14'30"W

- **Digress / Decimal Minutes**



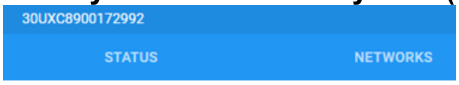
52°4.51009'N 0°14.5228'W

- **Decimal Degrees**



52.07516°N 0.242052°W

- **Military Grid Reference System (MGRS)**



30UXC8900172992

After selecting the desired format, the GPS fix on the header bar will change to correspond to the chosen format. Any GPS data saved to the NESIE database will now be saved in the new format.

NOTE: Any data saved prior to the format change will still be in the old format.

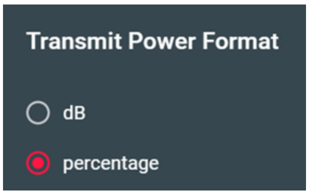
33.3.1.4 TRANSMIT POWER FORMAT

As discussed at section 17.4, the operator can add attenuation to the transmitted NESIE signal. By adding attenuation, the output power is reduced.

By default, the attenuation scale is set to display in percent, however, the attenuation scale can be displayed in 2 formats:

- **Percentage (%)**
- **Decibel (dB)**

To change the scale, the operator should click on the Transmit Power Format button. A pop-up window, as shown at Fig 323 will be displayed. The current format will be shown by a red marker. The operator can switch formats by clicking the new format icon. The red marker will swap to the new format and the dialogue box will disappear.



Transmit Power Format

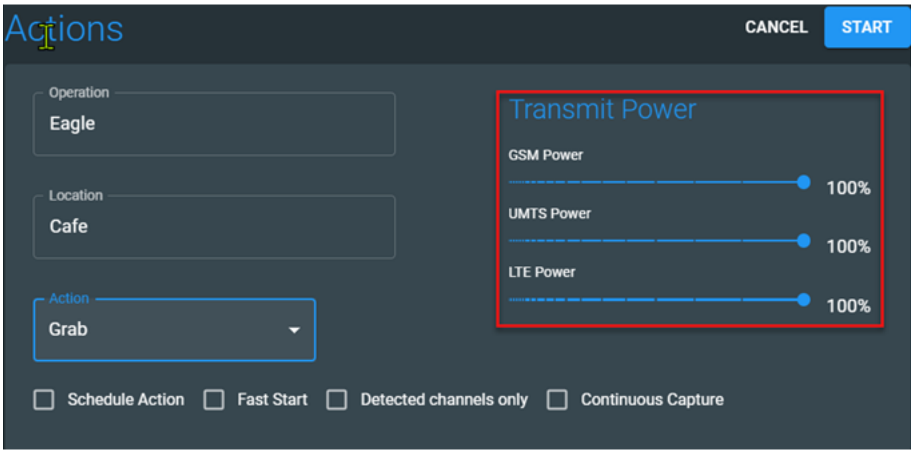
○ dB

● percentage

Fig 323. Transmit Power Format

As shown below in Fig 324, the (default) transmit attenuation is displayed at percentage (%). The blue slider is by default at 100%, which equals maximum power output. Each graticule represents approximately 1dB of attenuation. Therefore 3 graticules = a 50% reduction in transmit power or 3 dB of attenuation.

Fig 325 shows the transmit attenuation is displayed in Decibel (dB). Each graticule represents 1 dB of attenuation. 3dB of attenuation = a reduction in power by half (50%).



Actions

CANCEL START

Operation: Eagle

Location: Cafe

Action: Grab

Transmit Power

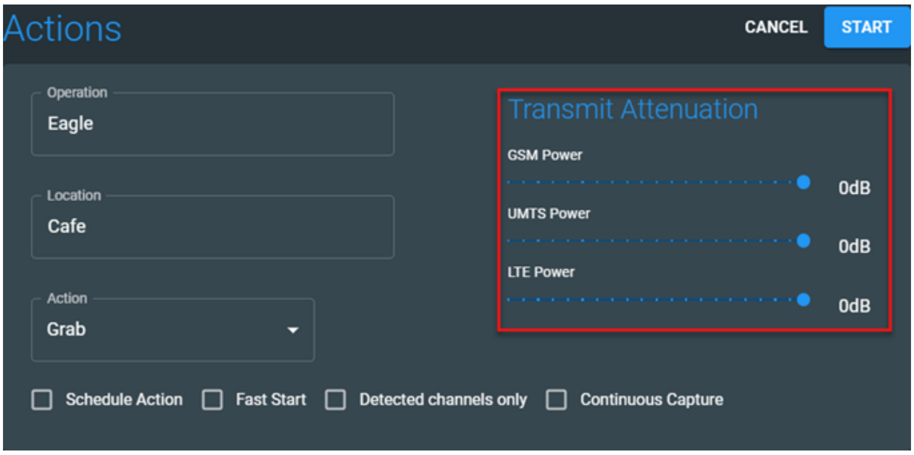
GSM Power 100%

UMTS Power 100%

LTE Power 100%

□ Schedule Action □ Fast Start □ Detected channels only □ Continuous Capture

Fig 324. Transmit attenuation - percentage



Actions

CANCEL START

Operation: Eagle

Location: Cafe

Action: Grab

Transmit Attenuation

GSM Power 0dB

UMTS Power 0dB

LTE Power 0dB

□ Schedule Action □ Fast Start □ Detected channels only □ Continuous Capture

Fig 325. Transmit attenuation – dB scale

33.3.1.5 TIME ZONE

The Time Zone settings are detected from the laptop / tablet that the NESIE software is running on and cannot be altered from within the UI. The time zone of the system is always in UTC (Coordinated Universal Time), and the data is only changed to local time for displaying in the UI.

If the time zone settings are incorrect, they will need to be altered on the PC/Tablet that is being used to control the NESIE.

33.3.1.6 TIME

To adjust the time, click on the current time; a pop-up box with be displayed showing the time in 12hr and 24hr formats, as shown at Fig 326 below. Click and drag to the hour required (in either 12 or 24hr format) and press OK. The Minutes screen will then appear, as at Fig 327 below. The user can now click and drag to the required minute.

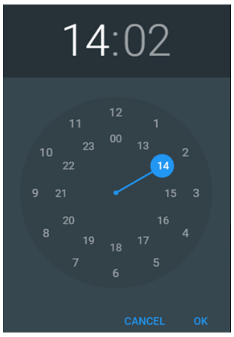


Fig 326. Hours

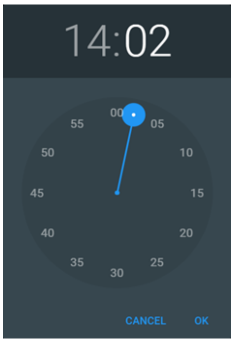


Fig 327. Minutes

33.3.1.7 DATE

To adjust the date, the operator should click on the < left arrow or > right arrow to move the correct Month and Year. Then click on the required date as shown in Fig 328 below. When the date is correct, click the OK button to save the settings.

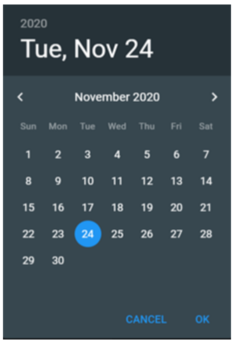
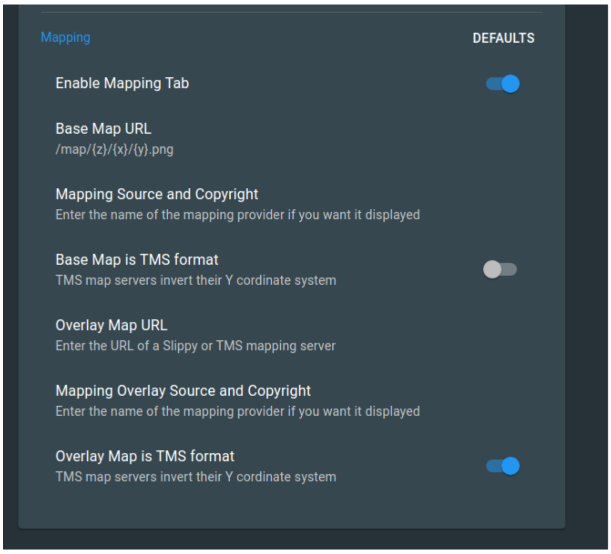


Fig 328. Date

33.3.1.8 MAPPING

The mapping section shown below at Fig 329, allows the NESIE operator to select between the installed mapping, set up access to an external mapping server, or on line mapping such as Google Maps.

By default, the system will be set up to use the installed mapping on Tactical NESIE systems and will usually be disabled if mapping is not installed, such as in a Covert NESIE system.



Mapping

Enable Mapping Tab ●

Base Map URL
/map/{z}/{x}/{y}.png

Mapping Source and Copyright
Enter the name of the mapping provider if you want it displayed

Base Map is TMS format ○
TMS map servers invert their Y cordinate system

Overlay Map URL
Enter the URL of a Slippy or TMS mapping server

Mapping Overlay Source and Copyright
Enter the name of the mapping provider if you want it displayed

Overlay Map is TMS format ●
TMS map servers invert their Y cordinate system

Fig 329. Mapping

- Enable Mapping Tab

  By default, the MAPPING page button will be shown on the header bar of the UI if the system you are using has the default mapping installed. If the mapping is not available or not installed in your system, the button will be greyed out and the MAPPING button on the top bar of the UI will not be shown.

  If the user is setting up the system to use an external map server or on line mapping, the Enable Mapping slider should be moved to the blue position. This will force the MAPPING button onto the UI.

- Base Map URL

  Sets the tile server source for main (background) map layer. The value can be any valid URL containing the place holders {x},{y} and {z}.

NOTE: The default URL is /map/{z}/{x}/{y}.png.

This default map URL is the stored mapping originated from OpenStreetMap. If at any time the DEFAULT button is pressed, the original settings will be applied.

The URL can also be set to nothing to disable mapping tile requests for the base layer.

The URL must point to a valid "Slippy Map" or TMS tile server.

- Mapping Source and Copyright

  Gives the user the option to input the mapping source and copyright information to be displayed on the system mapping.

- Base Map is TMS format

  In some cases, the map may appear inverted, and the tiles will appear in the wrong order in the horizontal axis. This is because some TMS map servers use an inverted Y Axis. If the maps appear jumbled, this tick box should be turned blue. This will automatically invert the Y axis and the map tiles should appear in correct order.

  The default map is not in TMS format so this tick box should remain grey if using the default map.

- **Overlay Map URL**

  This allows the user to apply an overlay on top of the base map. These tiles are drawn over the top of the base map. Often used to display additional information like labels and road names on satellite images.

  These overlays can also be used to display the users country specific mapping.

  By default, value will be empty so no overlays are applied.

- **Overlay Map is TMS format**

  As previously discussed, if the Base Map is TMS Format, but this time inverts the Y axis of the overlay tiles.

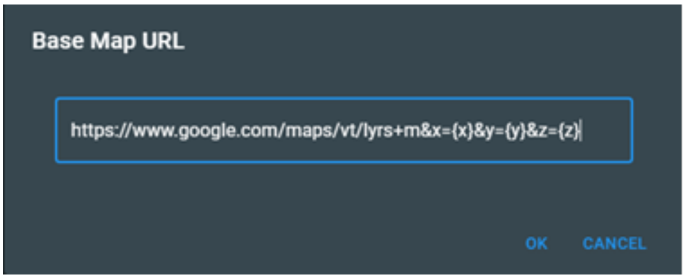
33.3.1.9 EXTERNAL MAP SERVERS & ONLINE MAPPING

If the customer wishes to use their own map server, they should turn Enable Mapping Tab switch blue (if not already). Then change the Base Map URL to the location of the attached map server.

If online mapping is to be shown in the MAPPING page, the user should ensure the laptop / PC displaying the NESIE UI has a good data connection (ethernet, Wi-Fi or cellular data)

NOTE: Remember that when NESIE is transmitting, it may temporarily knock out your remote Wi-Fi or cellular connection and the maps may not display.

Then change the Base Map URL to ensure the NESIE UI is directed to the correct map server: by clicking on the current URL. A pop-up dialogue box will appear as shown in Fig 330 below.

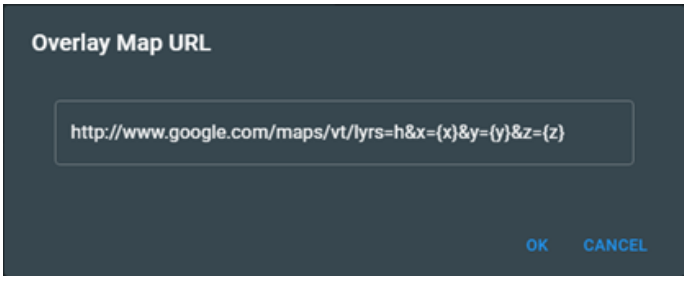


Base Map URL

https://www.google.com/maps/vt/lyrs+m&x={x}&y={y}&z={z}

Fig 330. Change Base Map URL

To apply an overlay, the operator should click on the Map Overlay URL and change the current URL to the desired URL as shown in Fig 331 below.



Overlay Map URL

http://www.google.com/maps/vt/lyrs=h&x={x}&y={y}&z={z}

Fig 331. Map Overlay URL

In this example, the user has an external internet connection and has changed the Base Map URL to Google Map Satellite images and has applied an overlay on the map to show roads, street names and other labels. As shown below Fig 332 below.

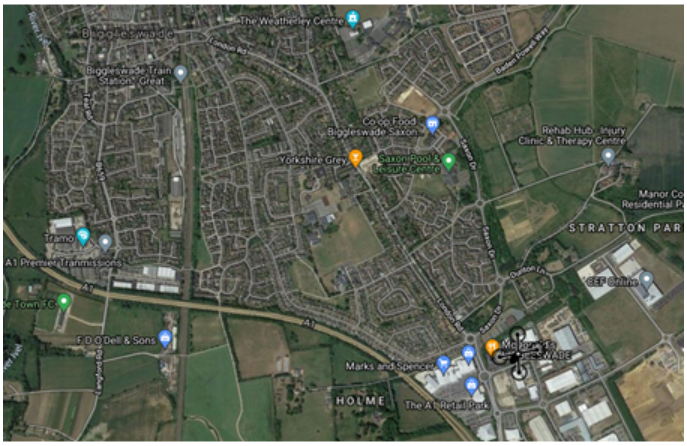


Fig 332. Google Maps displayed

Example On Line Map URLs (none are in TMS format)

- Open Street Map (same as the installed mapping for Tactical Ground)

  https://tile.openstreetmap.org/{z}/{x}/{y}.png

- Google maps:

  http://www.google.com/maps/vt/lyrs=m&x={x}&y={y}&z={z}

- Google Maps Satellite images:

  http://www.google.com/maps/vt/lyrs=s&x={x}&y={y}&z={z}

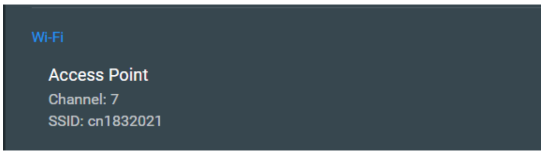
An example of the Overlay can be found at Google's hybrid layer (**not** TMS format)

- Google Maps Hybrid overlay:

  http://www.google.com/maps/vt/lyrs=h&x={x}&y={y}&z={z}

33.3.1.10 WI-FI – HOT SPOT SETTINGS (IF APPLICABLE)

If the NESIE system or control module is fitted with a Wi-Fi module, the additional settings, to allow for adjusting the Wi-Fi settings will be available, as shown at Fig 333 below.



Wi-Fi

Access Point

Channel: 7

SSID: cn1832021

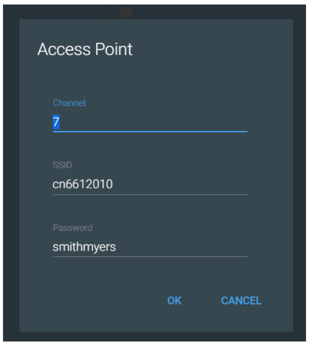
Fig 333. Wi-Fi

NOTE: If a Wi-Fi module (Covert Ground) or Wi-Fi dongle (Tactical Ground) is fitted and the NESIE system is powered up; a Wi-Fi Access point (Hotspot) is created/transmitted to allow the user to connect to the UI.

By default, the Wi-Fi settings are:

- **Channel**: 7
- **SSID**: cn & Serial No (Covert NESIE& Srl No of control module)
  tn & Serial No (Tactical NESIE& Srl No of control module)
  sn & Serial No (Strategic NESIE & Srl No of control module)
- **Password**: smithmyers

To change the default Wi-Fi Access point settings, click on the Wi-Fi button, the pop-up screen shown at Fig 334 will be displayed.



Access Point

Channel
7

SSID
cn6612010

Password
smithmyers

Fig 334. Wi-Fi settings

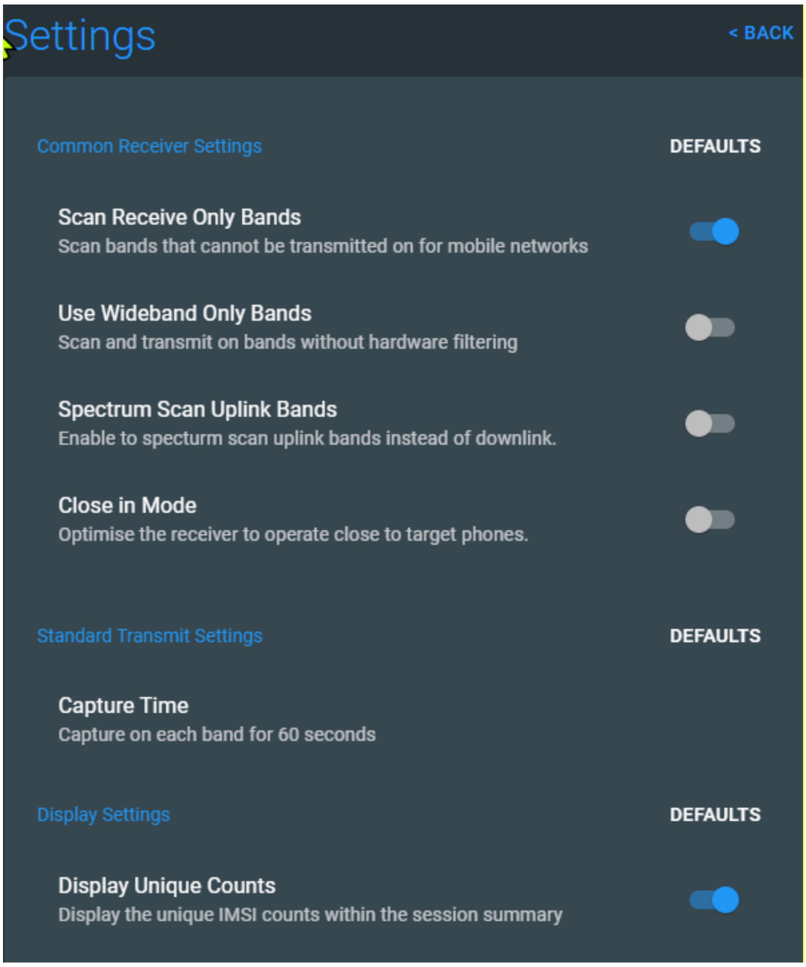
- **Channel**: The Wi-Fi channel that the access points is transmitted on. The channels available are 1 – 14.
- **SSID**: The name of the access point that is transmitted.
- **Password**: The password that is required by anyone who is logging in to the Wi-Fi access point.

CAUTION: ANYONE IN WI-FI DETECTION RANGE WILL BE ABLE TO SEE THE BROADCAST SSID.

IT IS STRONGLY ADVISED THAT THE BROADCAST SSID / NAME IS CHANGED REGULARLY EG: PRIOR TO EVERY OPERATION OR EVERY TIME YOU RETURN TO THE SAME LOCATION

ITS IS ALSO STRONGLY ADVISED THAT THE WIFI SSID IS CHANGED TO REFLECT SOMETHING NON DESCRIPT EG: A WIFI HOTSPOT IN THE AREA OR A COMMONLY USED HOME BROADBAND DEVICE OR PRINTER

33.3.2 GENERAL SETTINGS



Settings

< BACK

Common Receiver Settings — DEFAULTS

Scan Receive Only Bands — Scan bands that cannot be transmitted on for mobile networks — ●

Use Wideband Only Bands — Scan and transmit on bands without hardware filtering — ○

Spectrum Scan Uplink Bands — Enable to specturm scan uplink bands instead of downlink. — ○

Close in Mode — Optimise the receiver to operate close to target phones. — ○

Standard Transmit Settings — DEFAULTS

Capture Time — Capture on each band for 60 seconds

Display Settings — DEFAULTS

Display Unique Counts — Display the unique IMSI counts within the session summary — ●

Fig 335. General Settings

33.3.2.1 COMMON RECEIVE SETTINGS

Scan Receive Only Bands:

Some NESIE units may only have limited transmit amplifiers or filters fitted (normally the airborne systems), however, the receivers are still capable of receiving other bands. Scan Only Receive Bands instructs the system to scan the frequency bands that the system cannot transmit on. This will list the other neighbour cells that the system is competing against. This is to extract other pertinent cell data that can be used to configure the transmission and attract devices to the system.

Use Wideband Only Bands:

The Use Wideband Only Bands function is for use on low powered covert systems. By not using any filtration across the whole of its operating frequency spectrum it can attract devices using international frequency bands in most countries straight out of the box.

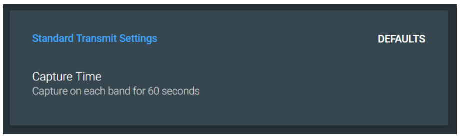
Spectrum Scan Uplink Bands

Enabling this function allows the operator to view the spectrum scan of the uplink frequencies as opposed to the usual spectrum scan, which monitors the downlink frequencies. This should help the operator to establish the cause of any high uplink interference (ULI) readings on the NESIE UI.

33.3.2.2 STANDARD TRANSMIT SETTINGS

Capture Time:
Is used to adjust the time that the NESIE transmits a fake base station signal on each network / technology to encourage the devices to register onto the system. The value is the number of seconds the NESIE will transmit for.

The time set is displayed in the screen and, if required, the operator can press the DEFAULTS button to return the value to 60 seconds as shown in Fig 336.

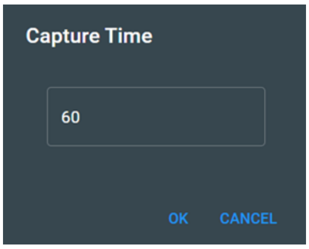

Standard Transmit Settings

Capture Time
Capture on each band for 60 seconds

Fig 336. Standard Transmit Settings

If the operator needs to adjust the time, click on the Capture Time button and a pop-up box will be displayed, as shown below in Fig 337.

The operator can now type in the required capture time (in seconds) and click OK. The default time is set at 60 seconds, but the minimum allowed is 30 seconds and maximum of 100,000 seconds (over 24hrs).


Capture Time

60

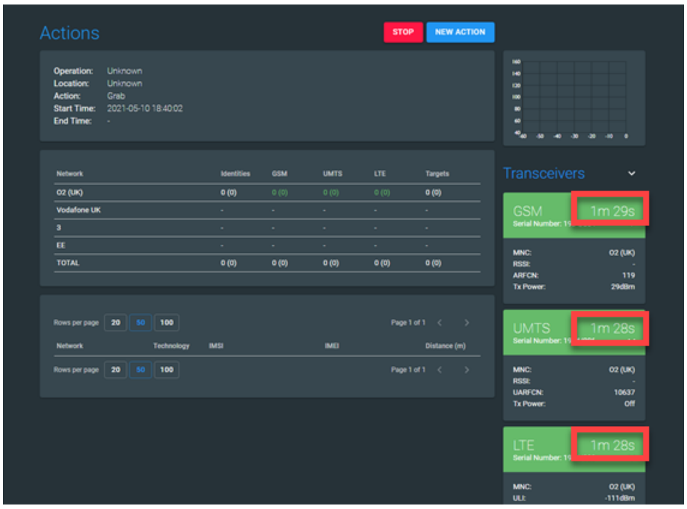
Fig 337. Transmit Time

NOTE: When transmitting a fake base station, the standard capture time will automatically change depending on the number of transceiver (channels) in the NESIE system.

In a <u>Single Channel</u> system: The capture time will automatically adjust to match the technology that is being transmitted. GSM – the standard capture time will be 60 seconds or whatever value is set by the operator. In the UMTS & LTE bands NESIE will automatically detect the number of channels in the real networks bands and transmit for a default of 30 seconds on each of these channels.

In a <u>Multiple Channel</u> system: The Standard (GSM) Capture Time will be overruled by the detected settings of either the UMTS or LTE band. E.g.: If there are 3 UMTS channels detected in the band the Capture Time will default to 30 seconds per channel (90secs). However, if there are 4 channels detected in the LTE band the capture time will now be overruled to 4 x 30secs (120 secs). All transceivers will now be synchronised and transmit on the highest total. Therefore in this example a 3 channel system will transmit for 120 seconds on GSM, UMTS and LTE.

As shown in the example below at Fig 338, the transmit time has been set at 60 seconds, however, for this network the NESIE software has detected 3 channels on either UMTS or LTE; therefore the transmit time has automatically been adjusted to 90 seconds. All transceivers in the stack are synchronised to start and stop at the same time.



Operation: Unknown
Location: Unknown
Action: Grab
Start Time: 2021-05-10 18:40:02
End Time: -

Network	Identities	GSM	UMTS	LTE	Targets
O2 (UK)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
Vodafone UK	-	-	-	-	-
3	-	-	-	-	-
EE	-	-	-	-	-
TOTAL	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)

Rows per page 20 50 100 Page 1 of 1

Network	Technology	IMSI	IMEI	Distance (m)

Rows per page 20 50 100 Page 1 of 1

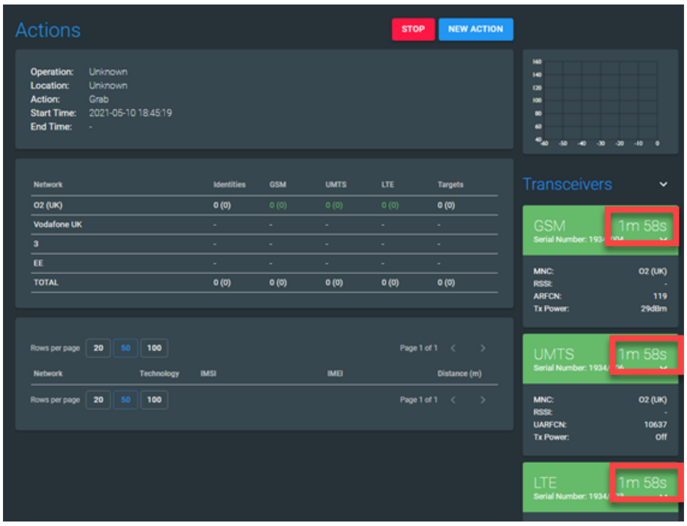
GSM 1m 29s
Serial Number: 19
MNC: O2 (UK)
RSSI: -
ARFCN: 119
Tx Power: 29dBm

UMTS 1m 28s
Serial Number: 19
MNC: O2 (UK)
RSSI: -
UARFCN: 10637
Tx Power: Off

LTE 1m 28s
Serial Number: 19
MNC: O2 (UK)
ULI: -111dBm

Fig 338. Synchronised transmit tme – 60s

As shown in the example below at Fig 339, the transmit time has been set at 120 seconds. Again, for this network the NESIE software has detected 3 channels on either UMTS or LTE. However, because the 3 x 30seconds required for UMTS or LTE is less than the default transmit time, the software has overruled this and allocated 120 seconds to all transceivers. All transceivers in the stack are synchronised to start and stop at the same time but the allocated time will be shared between the bands eg: if only 2 GSM bands are found, the software will allocate 60 seconds to each band.



Operation: Unknown
Location: Unknown
Action: Grab
Start Time: 2021-05-10 18:45:19
End Time: -

Network	Identities	GSM	UMTS	LTE	Targets
O2 (UK)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
Vodafone UK	-	-	-	-	-
3	-	-	-	-	-
EE	-	-	-	-	-
TOTAL	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)

Rows per page 20 50 100 Page 1 of 1

Network	Technology	IMSI	IMEI	Distance (m)

Rows per page 20 50 100 Page 1 of 1

GSM 1m 58s
Serial Number: 193
MNC: O2 (UK)
RSSI: -
ARFCN: 119
Tx Power: 29dBm

UMTS 1m 58s
Serial Number: 1934/
MNC: O2 (UK)
RSSI: -
UARFCN: 10637
Tx Power: Off

LTE 1m 58s
Serial Number: 1934/

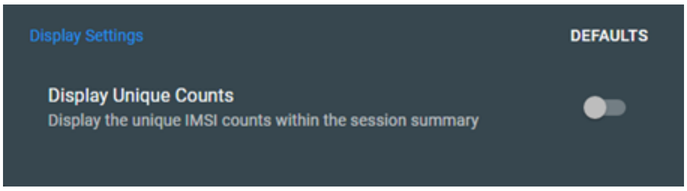
Fig 339. Synchronised transmit time – 120s

33.3.2.3 DISPLAY SETTINGS

Unique IDs:
When an ID is captured, it will be displayed in the list. Regularly an ID may be captured multiple times e.g.: in GSM, UMTS and LTE – therefore, it could be shown as being captured a total of 3 times. This may then give a false impression of the number of unique IDs in the Grab.

By default, the NESIE cross checks the IDs captured in the Grab to give a true number of unique IDs. So, if the number of IDs captured is displayed as **100 (95).** The total number of IDs captured including multiple ID is 100, however, the number of individual devices captured is 95.

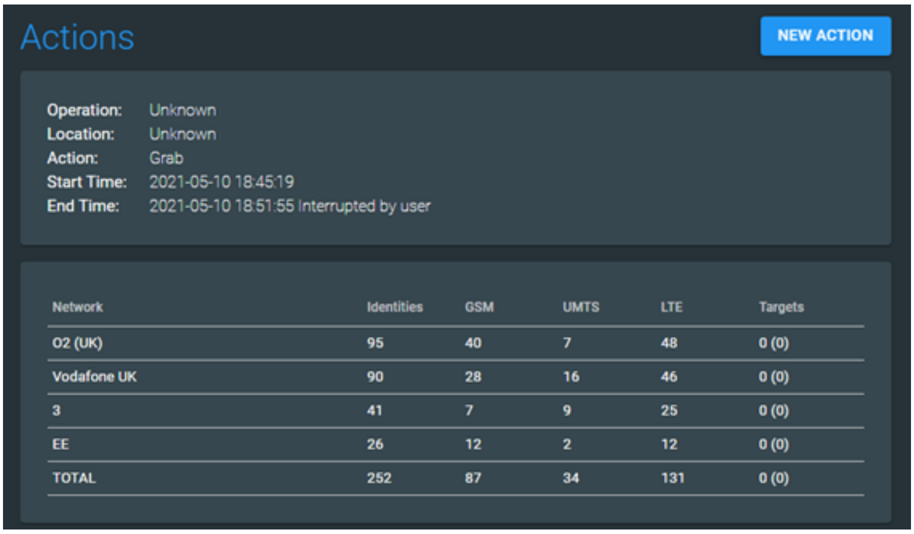
To turn off the unique number and only show the total, the operator should slide the button from blue to grey, as shown below at Fig 340.



Display Unique Counts
Display the unique IMSI counts within the session summary

Fig 340. Unique count – disabled

If the Display Unique Count is deactivated, the (Unique) number will no longer be displayed in the Action summary page, as shown below at Fig 341.



Operation: Unknown
Location: Unknown
Action: Grab
Start Time: 2021-05-10 18:45:19
End Time: 2021-05-10 18:51:55 Interrupted by user

Network	Identities	GSM	UMTS	LTE	Targets
O2 (UK)	95	40	7	48	0 (0)
Vodafone UK	90	28	16	46	0 (0)
3	41	7	9	25	0 (0)
EE	26	12	2	12	0 (0)
TOTAL	252	87	34	131	0 (0)

Fig 341 – Action summary – unique count disabled

33.3.3 GSM SETTINGS

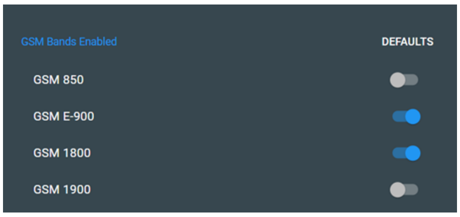
The GSM Settings screen allows the operator to choose which GSM bands to scan to detect and log the local area cellular provider's data. This screen is usually set upon initial configuration and should not change unless the NESIE is moved into a different region / country, or the network providers change their settings.

To successfully log the network providers BTS settings, NESIE must scan the available GSM band and tune its receiver every 200kHz. If a signal is present, it must pause and attempt to decode the signal. In the EGSM 900 band that equates to 173 individual channels / steps.

NOTE: If more bands are selected than necessary, NESIE will scan parts of the frequency spectrum not used for GSM and add unnecessary time to the scan.

33.3.3.1 GSM BANDS ENABLED

The user should adjust the toggle switches to reflect the GSM frequency bands present in their operational area. Grey indicates off / blue indicates on, as shown below at Fig 342. The scanning of the network providers is discussed in more detail at Section 12.



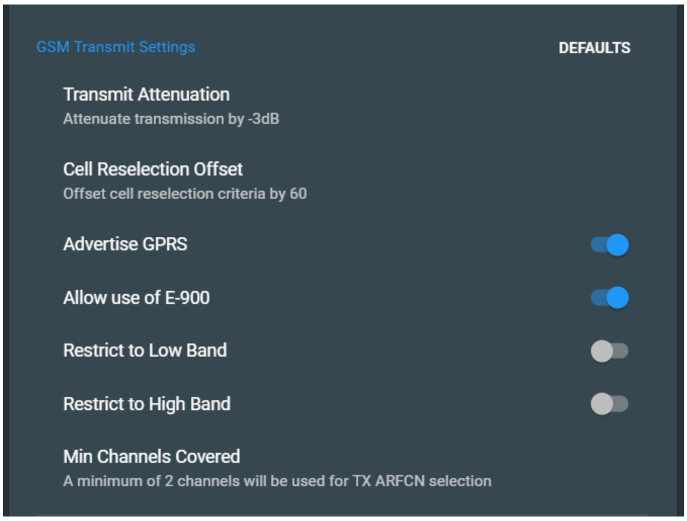
GSM 850 ○
GSM E-900 ●
GSM 1800 ●
GSM 1900 ○

Fig 342. GSM bands enabled

33.3.3.2 GSM TRANSMIT SETTINGS

In this section, the user can adjust the GSM settings used by NESIE. These settings should only be used by an advanced user to attempt to increase the default capabilities of NESIE. Fig 343 shows the GSM settings options.

CAUTION: ALTERING THESE VALUES CAN SERIOUSLY AFFECT THE WAY THE NESIE OPERATES AND REDUCE THE NUMBER OF IDENTITIES CAPTURED. DO NOT CHANGE THE DEFAULT VALUES UNLESS YOU UNDERSTAND THE POSSIBLE EFFECTS.



GSM Transmit Settings

Transmit Attenuation
Attenuate transmission by -3dB

Cell Reselection Offset
Offset cell reselection criteria by 60

Advertise GPRS ●

Allow use of E-900 ●

Restrict to Low Band ○

Restrict to High Band ○

Min Channels Covered
A minimum of 2 channels will be used for TX ARFCN selection

Fig 343. GSM transmit settings

Transmit Attenuation:
Similar to using the transmit attenuation sliders as discussed at section 17.4, this setting allows the operator to alter the power output by the NESIE during GSM transmission.

NOTE: Adjusting the attenuation setting on this page will replicate the adjustment on the ACTIONS page power sliders. And vice versa, if the sliders are adjusted, the resultant figure will be displayed on this page.

The larger the value (0 is max.) the larger the “dummy cell” produced by the NESIE. The range of the value is -60 to 0 dB. The default setting is 0 (no attenuation).

NOTE: Adding 3dB of attenuation will reduce the output by 50% e.g. 20W with 3 dB attenuation will reduce the power to 10W. See Fig 344 for more approximate values.

Attenuation (dB)	Output Power (W)
0	100
-3	50
-6	25
-9	12.5
-12	6.25
-15	3.125

Fig 344. Approximate attenuation values

Cell Reselection Offset:
Alters the Cell Reselection Offset transmitted by the NESIE while trying to register devices. The higher the Cell Reselection Offset, the more likely a device is to leave the real network and register on the NESIE (It effectively increases the size of the "dummy cell" without the need for a power increase). The range of this value is 0 to 126. The default value is 60.

Allow use of E-900:
Deselect this option to cater for Target devices that do not support E-900 (unusual these days). Default is to allow E-900 use.

E-900 is the Extended Frequency to the 900MHz cellular band. Historically some mobile devices could not cater for this band.

Restrict to Low Band:
Restricts GSM Transmit to 850/900 GSM bands. For use with a low band only or one band external PA. Default is not ticked.

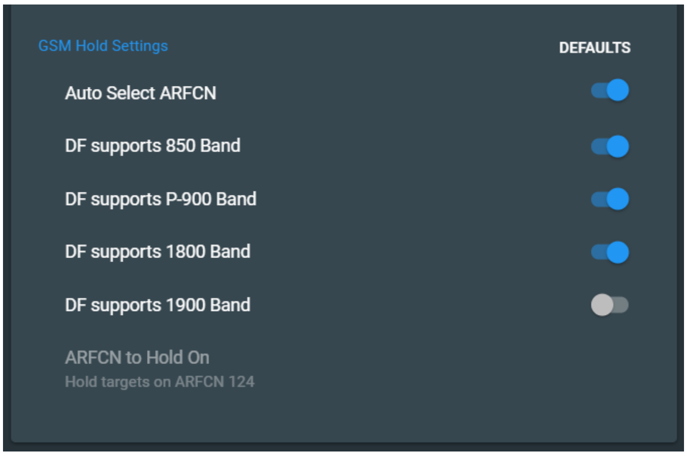
Restrict to High Band:
Restricts GSM Transmit to 1800/1900 bands. For use with a high band only or one band external PA. Default is not ticked.

Min Channels Covered
Modifies the frequency selection so that it tries to "cover" more real cells. A value of 2 (default) will cause the system to select a neighbour frequency common to the top 2 cells in the scan. The higher the number the more cells the system tries to include. Min is 2 and the max is 10.

33.3.3.3 GSM HOLD SETTINGS (DIRECTION FINDING)

The Hold settings shown if Fig 345 can be used to adjust the default settings of the NESIE during the Hold process. The Hold function moves a Target mobile device onto a dedicated channel and into a 'permanent transmit' state. Whilst the Target mobile device is transmitting, a second team can use traditional direction finding (DF) equipment to locate the mobile device.

CAUTION: ALTERING THESE VALUES CAN SERIOUSLY AFFECT THE WAY THE NESIE OPERATES AND REDUCE THE POSSIBILITY OF HOLDING OR LOCATING A TARGET MOBILE DEVICE. DO NOT CHANGE THE VALUES UNLESS YOU UNDERSTAND THE POSSIBLE EFFECTS



GSM Hold Settings

DEFAULTS

Auto Select ARFCN ●

DF supports 850 Band ●

DF supports P-900 Band ●

DF supports 1800 Band ●

DF supports 1900 Band ○

ARFCN to Hold On

Hold targets on ARFCN 124

Fig 345. GSM Hold settings

Auto select ARFCN:
If this box is checked, the Hold operation will automatically select the channel that the device is held on. If the box is not checked, the channel in the ARFCN to Hold On setting will be used. Default value is checked.

DF supports 850 Band:
If this box is checked, the Hold channel can be auto selected from the 850 Band.

DF supports P-900 Band:
If this box is checked, the Hold channel can be auto selected from the 900 Band.

DF supports 1800 Band:
If this box is checked, the Hold channel can be auto selected from the 1800 Band.

DF supports 1900 Band:
If this box is checked, the Hold channel can be auto selected from the 1900 Band

NOTE: Some older phones only support one band. So, by default the NESIE will select a channel in the band that the device was registered on. Forcing the NESIE to Hold the device on a channel outside the original band using these settings can cause the Hold to fail.

Most devices can support up to 4 GSM bands, but the users chosen DF system may only support some of the bands. This gives the user the option to force a mobile device onto specific bands to increase the DF success rate.

ARFCN to Hold on:
The channel to use if the Auto select ARFCN setting is not checked. The range of this value depends on the GSM bands available to the NESIE. The NESIE will prevent you from entering an invalid channel. Default value is blank.

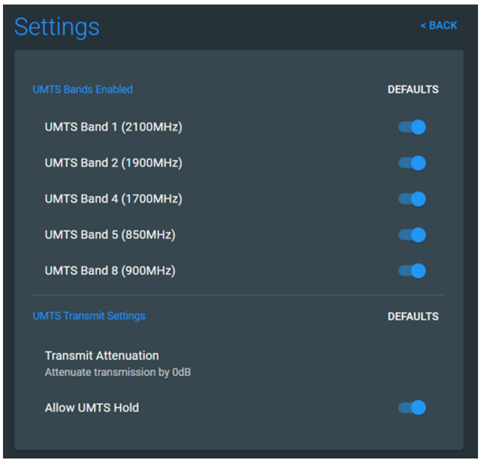
33.3.4 UMTS SETTINGS

This screen allows the operator to configure the UMTS transceiver settings.

33.3.4.1 UMTS BANDS ENABLED

This section sets NESIE to the UMTS frequency bands it should carry out a Network Scan on (listen to); to log the local area network signals. If bands that are not used in the region / country are included in the scan, NESIE will waste time listening to these bands when there is no requirement.

CAUTION – IF THE DEFAULT BUTTON IS PRESED, ALL BANDS WILL BE SELECTED. IF ALL BANDS ARE INCLUDED IN THE SCAN THE TIME REQUIRED FOR THE SCAN WILL INCREASE.


Settings
< BACK

UMTS Bands Enabled — DEFAULTS

- UMTS Band 1 (2100MHz) ●
- UMTS Band 2 (1900MHz) ●
- UMTS Band 4 (1700MHz) ●
- UMTS Band 5 (850MHz) ●
- UMTS Band 8 (900MHz) ●

UMTS Transmit Settings — DEFAULTS

Transmit Attenuation
Attenuate transmission by 0dB

Allow UMTS Hold ●

Fig 346. UMTS settings

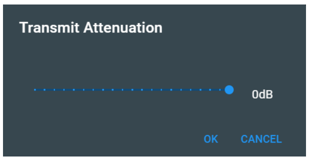
33.3.4.2 UMTS TRANSMIT SETTINGS

Transmit Attenuation:
Similar to using the transmit attenuation sliders as discussed at section 17.4, this setting allows the operator to alter the power output by the NESIE during UMTS transmissions.

NOTE: Adjusting the attenuation setting on this page will replicate the adjustment on the ACTIONS page power sliders. And vice versa, if the sliders are adjusted, the resultant figure will be displayed on this page.

The larger the value (0 is max.), the larger the “dummy cell” produced by the NESIE. The range of the value is -60 to 0 dB. The default setting is 0 (no attenuation).

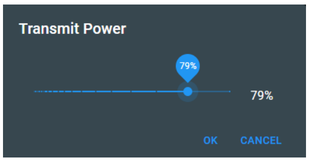
If required, the operator can reduce the amount to power transmitted by the UMTS transceiver by adding UMTS Transmit Attenuation. The operator should click on the Transmit Attenuation button as shown at Fig 346 above. A pop-up box will be displayed as shown at Fig 347 below, dependant of the settings.


Transmit Attenuation

0dB

Fig 347. UMTS Transmit Attenuation - dB

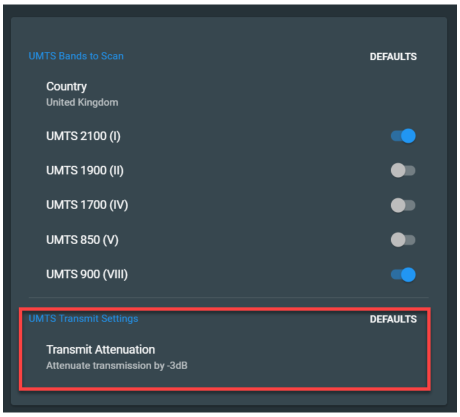
Percentage:
The operator can add transmit attenuation using the slider shown below in Fig 348. The bar is divided into sections, each section break represents approximately 1dB of attenuation. Therefore the 3rd step = 50% or 3dB of attenuation.


Transmit Power

79%

Fig 348. UMTS Transmit Attenuation -percentage

The amount of attenuation added (decibel or percent) will be displayed on the UMTS Transmit Settings pane as shown in Fig 349 below.


UMTS Bands to Scan

Country
United Kingdom

UMTS 2100 (I)

UMTS 1900 (II)

UMTS 1700 (IV)

UMTS 850 (V)

UMTS 900 (VIII)

UMTS Transmit Settings

Transmit Attenuation
Attenuate transmission by -3dB

Fig 349. UMTS Transmit – attenuation added

NOTE: If the NESIE module has a maximum output power of 40 Watts peak per channel, adding 50% or 3dB of attenuation will reduce the output by 50% = 20W, see Fig 344 for more approximate values.

33.3.4.3 ALLOW UMTS HOLD

If the user wants the ability to Hold cellular device on UMTS, this toggle switch should be blue. Now NESIE will have the ability to Hold on UMTS and GSM.

33.3.5 LTE SETTINGS

This page allows the NESIE operator to configure the LTE transceiver settings.

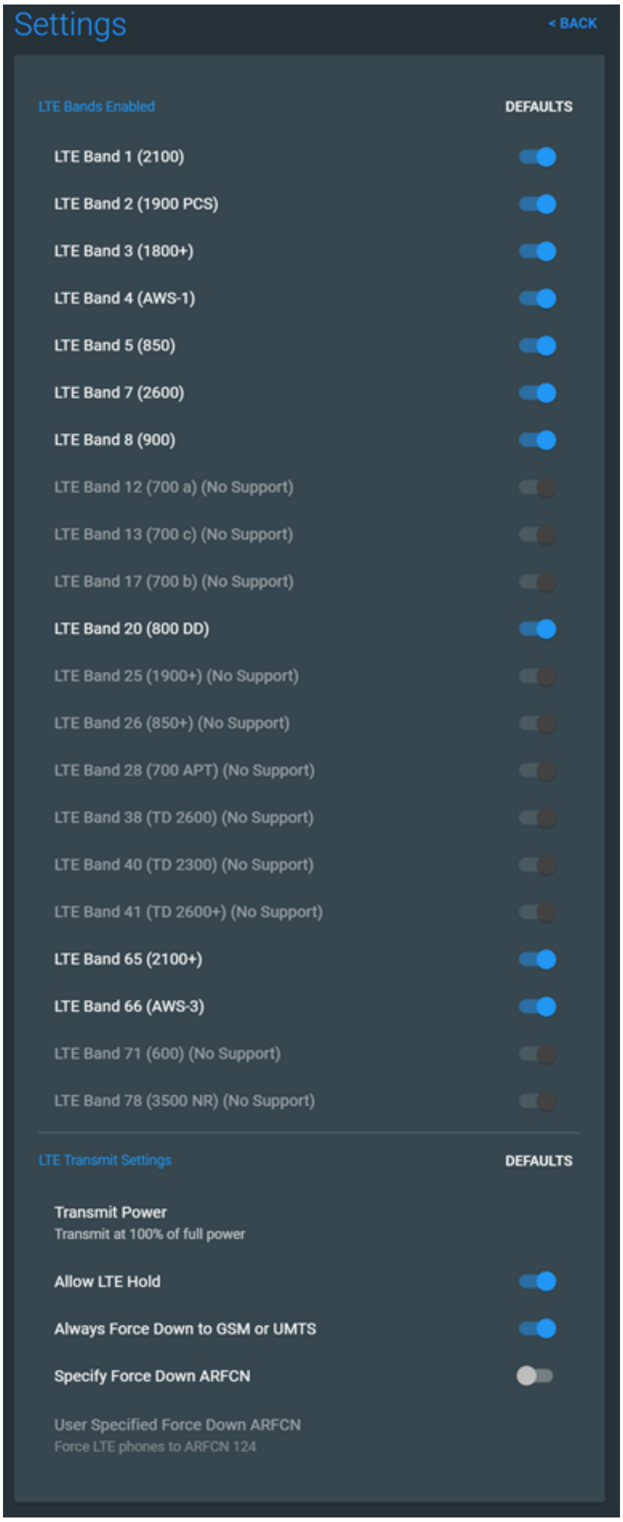
33.3.5.1 LTE BANDS ENABLED

This section tells NESIE which LTE frequency bands it should carry out a network scan on (listen to) to log the local area network signals. If bands that are not used in the region / country are included in the scan, NESIE will waste time listening to these bands when there is no requirement.

The operator can select the LTE bands used in the country / area. If required, additional bands can be selected to monitor the RF in that band, as shown in Fig 350 below.

The bands are listed under LTE, but cellular network providers may use GSM or UMTS in the band as well.

As shown below, there are several LTE bands that are displayed but are greyed out. This indicates the other bands that are available upon request. NESIE is fitted with a specific number of amplifiers and filters depending on the region of the world that it is deployed in. If required some components can be swapped to allow other bands.



Settings

< BACK

LTE Bands Enabled

DEFAULTS

LTE Band 1 (2100)

LTE Band 2 (1900 PCS)

LTE Band 3 (1800+)

LTE Band 4 (AWS-1)

LTE Band 5 (850)

LTE Band 7 (2600)

LTE Band 8 (900)

LTE Band 12 (700 a) (No Support)

LTE Band 13 (700 c) (No Support)

LTE Band 17 (700 b) (No Support)

LTE Band 20 (800 DD)

LTE Band 25 (1900+) (No Support)

LTE Band 26 (850+) (No Support)

LTE Band 28 (700 APT) (No Support)

LTE Band 38 (TD 2600) (No Support)

LTE Band 40 (TD 2300) (No Support)

LTE Band 41 (TD 2600+) (No Support)

LTE Band 65 (2100+)

LTE Band 66 (AWS-3)

LTE Band 71 (600) (No Support)

LTE Band 78 (3500 NR) (No Support)

LTE Transmit Settings

DEFAULTS

Transmit Power
Transmit at 100% of full power

Allow LTE Hold

Always Force Down to GSM or UMTS

Specify Force Down ARFCN

User Specified Force Down ARFCN
Force LTE phones to ARFCN 124

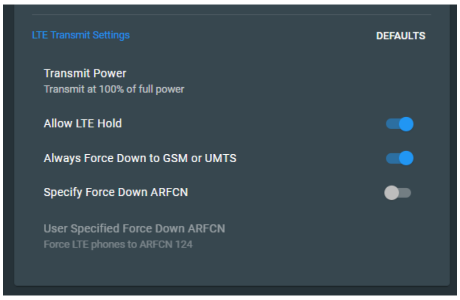
Fig 350. LTE settings

As shown in Fig 350 above, there are several LTE bands that are displayed but are greyed out and showing (No Support). This indicates the bands that are available on NESIE but have not been enabled in this unit. This may be because a hardware change is required. In this example, LTE Bands 12, 13,17, & 25, 26, 38, 40, 41 & 71 are available but have not been fitted into this NESIE unit.

33.3.6 LTE TRANSMIT SETTINGS

As shown in Fig 351, the lower section of the LTE Settings page is the LTE Transmit Settings pane and consists of the following options:

- **Transmit Power**
- **Allow LTE Hold**
- **Always Force Down to GSM or UMTS**
- **Specify Force Down ARFCN**
- **User Specified Force Down ARFCN**



LTE Transmit Settings DEFAULTS

Transmit Power
Transmit at 100% of full power

Allow LTE Hold ☑

Always Force Down to GSM or UMTS ☑

Specify Force Down ARFCN ☐

User Specified Force Down ARFCN
Force LTE phones to ARFCN 124

Fig 351. LTE Transmit Settings

33.3.6.1 TRANSMIT POWER

The amount to power transmitted by the LTE transceiver can be reduced by adding LTE transmit attenuation as shown below. Depending on the settings previously selected, the display will be either in percent (%) or decibel (dB)

The larger the value (0db or 100% is max.), the larger the “dummy cell” produced by the NESIE. The range of the value is -19dB or 1% to 0dB or 100%. The default setting is 0dB or 100% (no attenuation).

NOTE: If a NESIE module had a maximum output power of 40 Watts peak per channel, adding 3dB or 50% attenuation will reduce the output by 50% = 20W, see Fig 344 for more approximate values.

All NOTE: Adjusting the attenuation setting on this page will replicate the adjustment on the ACTIONS page power sliders. And vice versa, if the sliders are adjusted the resultant figure will be displayed on this page.

33.3.6.2 ALLOW LTE HOLD

When activated, this enables NESIE to Hold a mobile device on LTE. If the other technologies are enabled, the system may have the ability to Hold devices on GSM, UMTS and LTE.

NOTE: By default the allow LTE Hold will be activated.

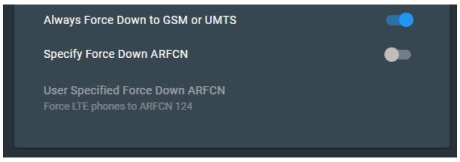
33.3.6.3 ALWAYS FORCE DOWN TO GSM

As shown in Fig 352 below, by default, the selector is set to blue (on), NESIE will automatically send a MOVE TO GSM or UMTS command to all devices found on LTE. If the device obeys this command, the device will move down to a GSM or UMTS channel and attempt to re-establish a connection to the network. In this mode, NESIE does not specify which ARFCN (channel number) to move to, so the device will select the best channel.

33.3.6.4 SPECIFY FORCE DOWN ARFCN

If the operator turns this function on, NESIE will transmit a MOVE TO GSM command and specify which channel the device should use whilst in the GSM band as shown in Fig 352 below.

By moving the selector to the on position, the User Specified Force Down ARFCN box is activated. The user can click on the button and enter the required channel as shown in Fig 353. Click OK to save the specified channel number.

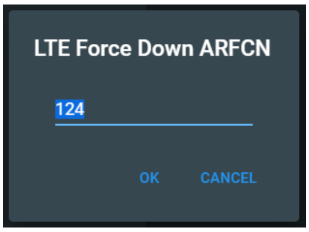


Always Force Down to GSM or UMTS

Specify Force Down ARFCN

User Specified Force Down ARFCN
Force LTE phones to ARFCN 124

Fig 352. Specify Force Down ARFCN



LTE Force Down ARFCN

124

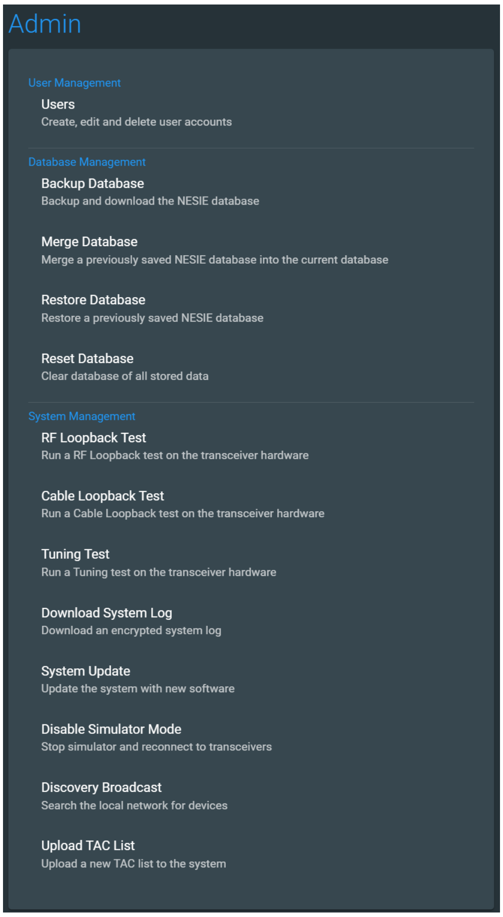
Fig 353. LTE Force Down ARFCN

34. ADMIN

When clicking on the Admin section, the user will be presented with the options displayed at Fig 354 below.

The options are:

- **Users Management**
- **Database Management**
- **System Management**



Admin

User Management

Users
Create, edit and delete user accounts

Database Management

Backup Database
Backup and download the NESIE database

Merge Database
Merge a previously saved NESIE database into the current database

Restore Database
Restore a previously saved NESIE database

Reset Database
Clear database of all stored data

System Management

RF Loopback Test
Run a RF Loopback test on the transceiver hardware

Cable Loopback Test
Run a Cable Loopback test on the transceiver hardware

Tuning Test
Run a Tuning test on the transceiver hardware

Download System Log
Download an encrypted system log

System Update
Update the system with new software

Disable Simulator Mode
Stop simulator and reconnect to transceivers

Discovery Broadcast
Search the local network for devices

Upload TAC List
Upload a new TAC list to the system

Fig 354. Admin settings options

34.1 USER MANAGEMENT – USERS

When clicking on the Users button, the operator will be presented with the screen displayed below at Fig 355. This screen will display a list of any users already created and stored in the database and allows additional users to be added to the system.

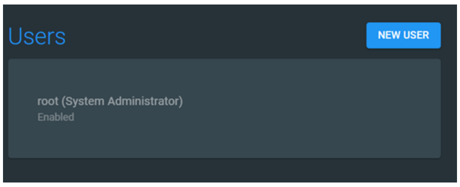
NOTE: By default, only the System Administrator has been set up. And only one Administrator account can be created.

Administrators have the permission to:

- **Create additional users**
- **Delete users**
- **Change passwords**
- **Disable accounts**

34.1.1 CREATE NEW USERS

An administrator can create additional users by pressing the NEW USER button as shown in Fig 355 below.



Users

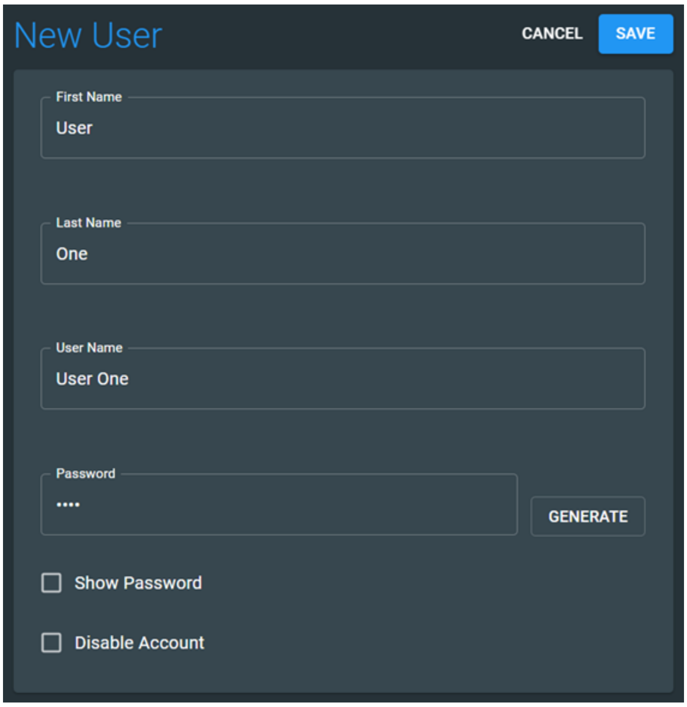
root (System Administrator)
Enabled

Fig 355. Users

The administrator will now be presented with the New User screen as shown below at Fig 356. Enter a First Name, Last Name and User Name and type in a password.

> **NOTE: If the Username has been previously used, the box will be shown in red.**

If required, the Show Password box can be checked to ensure the password is spelt correctly. Then press SAVE.



New User

First Name: User

Last Name: One

User Name: User One

Password: ••••

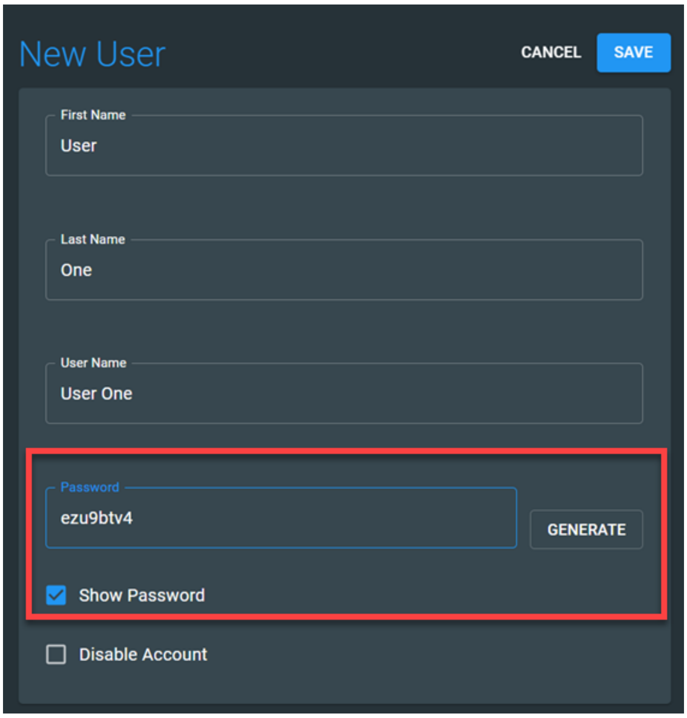
□ Show Password

□ Disable Account

Fig 356. Users - New User

The administrator also has the option to generate a password.

To generate a password, the operator should press the GENERATE button. The generated password will automatically be shown so the administrator can make a note of it, as shown below Fig 357 below.



New User

First Name: User

Last Name: One

User Name: User One

Password: ezu9btv4

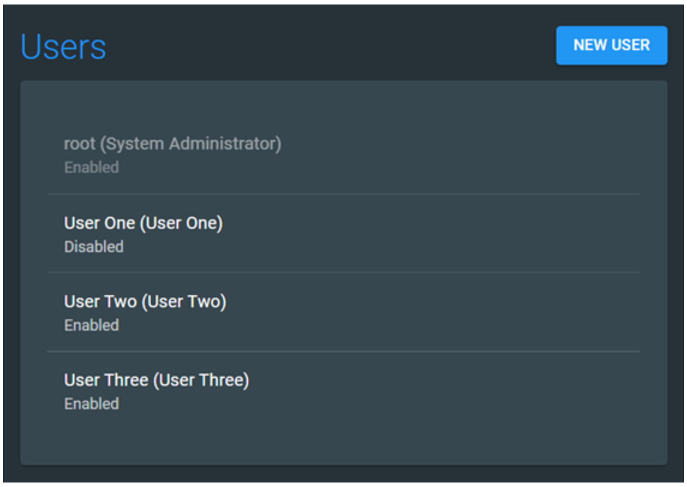
☑ Show Password

□ Disable Account

Fig 357. Users - New User – generate

NOTE: The generated password will consist of 8 characters. Which is a mix of lower case letters and numbers.

After creating the users, they will be displayed in the user list. The current state (Disabled / Enabled) will also be shown, see Fig 358 below.



Users

root (System Administrator)
Enabled

User One (User One)
Disabled

User Two (User Two)
Enabled

User Three (User Three)
Enabled

Fig 358. List of Users

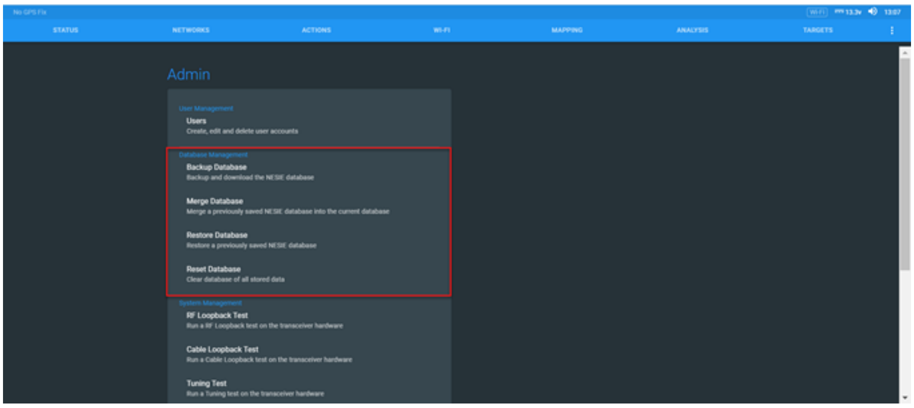
34.1.2 USER LOG ON

After a user has been created, they will now be able to log on to the NESIE system using their username and password. All Actions / button presses will now be logged against that user account.

34.2 DATABASE MANAGEMENT

The database management section allows the user to carry out the following functions shown below at Fig 359.

- Backup Database
- Merge Database
- Restore Database
- Reset Database



Admin

User Management

Users
Create, edit and delete user accounts

Database Management

Backup Database
Backup and download the NESIE database

Merge Database
Merge a previously saved NESIE database into the current database

Restore Database
Restore a previously saved NESIE database

Reset Database
Clear database of all stored data

System Management

RF Loopback Test
Run a RF Loopback test on the transceiver hardware

Cable Loopback Test
Run a Cable Loopback test on the transceiver hardware

Tuning Test
Run a Tuning test on the transceiver hardware

Fig 359. Admin – Database Management

34.2.1.1 BACKUP DATABASE

If required, the user can back up the system database. It is recommended that this backup should be carried our periodically and the sensitive data removed from the NESIE system.

To complete a backup, the user should click the Backup Database button. The dialog box shown below at Fig 360 will be displayed.

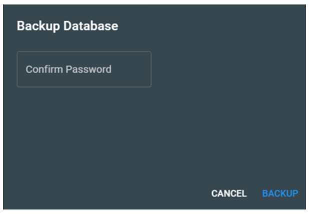
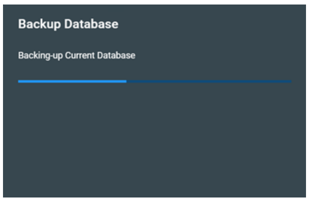


Fig 360. Backup Database – password

The user should enter the current password and click the BACKUP button.

The backup process will start, and the dialog box will show a blue progress bar along with different messages e.g. Stopping Services, Backing Up Current Database, Waiting Services to Start as shown below at Fig 361.

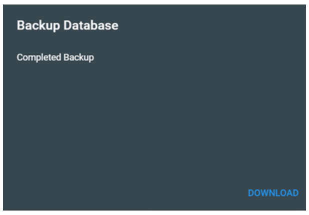


Backup Database

Backing-up Current Database

Fig 361. Backup Database – progress

When the backup is complete, the dialog box will show Completed Backup as shown below at Fig 362. The user should now click the blue DOWNLOAD button.

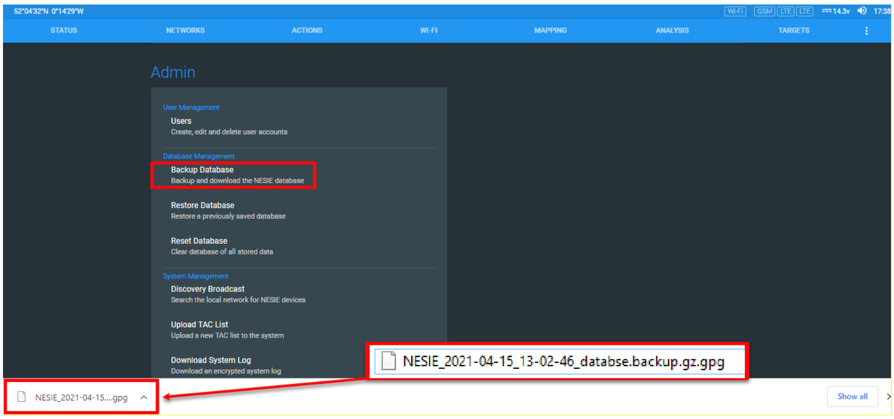


Backup Database

Completed Backup

Fig 362. Backup Database – complete

The UI will now revert to that shown below in Fig 363 . The backup file will be downloaded via the web browser. In the example shown below, the file has downloaded via Google Chrome and the file is shown at the bottom of the UI and expanded to show the full file information within the inserted windows screen capture.



User Management

Users
Create, edit and delete user accounts

Database Management

Backup Database
Backup and download the NESIE database

Restore Database
Restore a previously saved database

Reset Database
Clear database of all stored data

System Management

Discovery Broadcast
Search the local network for NESIE devices

Upload TAC List
Upload a new TAC list to the system

Download System Log
Download an encrypted system log

NESIE_2021-04-15_13-02-46_databse.backup.gz.gpg

NESIE_2021-04-15....gpg

Fig 363. Backup Database – file downloaded

The backup file is created and saved as a **.gz.gpg** file as shown below at Fig 364.

A GZ file is an archive file compressed by the standard GNU zip (gzip) compression algorithm. It contains a compressed collection of one or more files and is commonly used on Unix operating systems for file compression.

This file is automatically encrypted which adds the extra **.gpg** extension. The GPG file is a security key used to decrypt an encrypted file generated by GNU Privacy Guard (GnuPG), a file encryption program. This secure format is based on the OpenPGP standard defined by RFC2440, the same standard Pretty Good Privacy (. PGP) files use.

NOTE: Unlike PGP software, GnuPG is a free program.

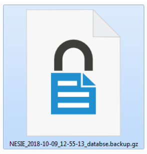


Fig 364. Backup Database – file type

34.2.1.2 MERGE DATABASE

Merge database allows the user to select a database backup to be combined with the data already present in the NESIE database (Fig 365).

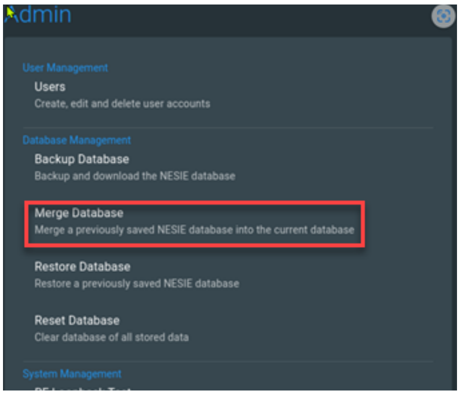
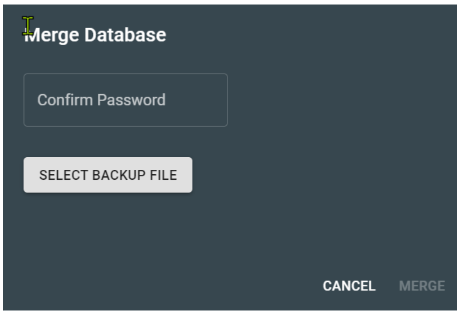

Admin
User Management
Users
Create, edit and delete user accounts
Database Management
Backup Database
Backup and download the NESIE database
Merge Database
Merge a previously saved NESIE database into the current database
Restore Database
Restore a previously saved NESIE database
Reset Database
Clear database of all stored data
System Management

Fig 365 Merge Database

The merge will add all captured data (Scans, Grabs, Identities, positions etc.) and all entered data (Users, Operations, Locations, Targets) in the database backup to the current database. Settings and tables of static information (MCC, MNC, TACs) will not be merged.

To merge the file, the user should first place the backup file onto a suitable location on the pc / laptop that is going to be used to connect to the NESIE System.

The user should enter the administrator password (default = root). Then use the SELECT BACKUP FILE button as shown in Fig 366.

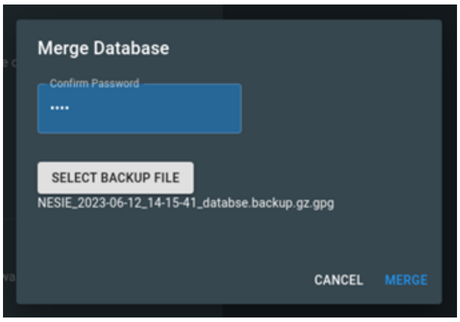


Merge Database

Confirm Password

Fig 366 Merge Database – select file

The operator should then navigate to the database backup file that they wish to merge with the current database and select it.



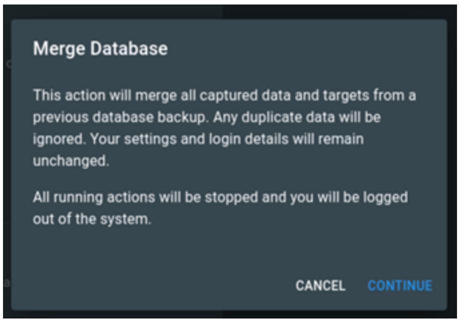
Merge Database

Confirm Password: ····

NESIE_2023-06-12_14-15-41_databse.backup.gz.gpg

Fig 367 MERGE button - active

When the file has been located, the MERGE button will turn blue (Fig 367) and allow the operator to start the restore process. A dialogue box detailing the process of the restore process will be displayed as per Fig 368.



Merge Database

This action will merge all captured data and targets from a previous database backup. Any duplicate data will be ignored. Your settings and login details will remain unchanged.

All running actions will be stopped and you will be logged out of the system.

Fig 368 Merge database - status

34.2.1.3 RESTORE DATABASE

The user can restore a previously saved backup database into the NESIE system.

To restore the file, the user should first place the backup file onto a suitable location on the pc / laptop that is going to be used to connect to the NESIE System.

The user should enter the administrator password (default = root). Then use the SELECT BACKUP FILE button as shown in Fig 369 below.

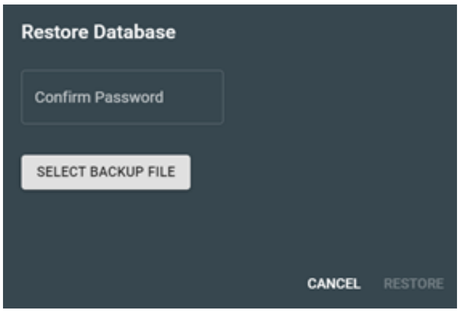
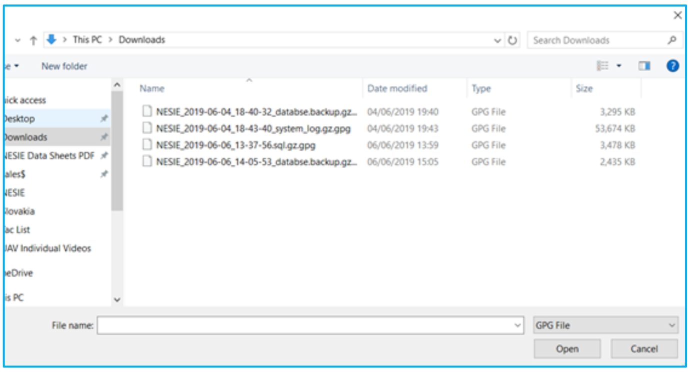


Fig 369. Restore database

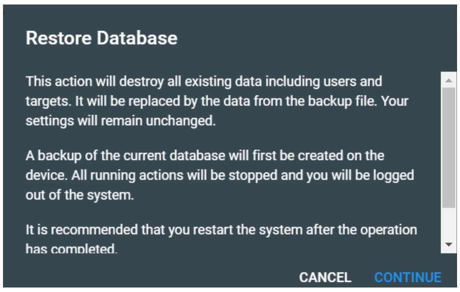
Results of the merger can be viewed in the ANALYSIS page.
When pressing the Select Backup File button, a Windows open file pop-up screen will be shown. This will allow the operator to navigate to the desired file. Select the backup file to be restored and click open, as per Fig 370.



Name	Date modified	Type	Size
NESIE_2019-06-04_18-40-32_databse.backup.gz...	04/06/2019 19:40	GPG File	3,295 KB
NESIE_2019-06-04_18-43-40_system_log.gz.gpg	04/06/2019 19:43	GPG File	53,674 KB
NESIE_2019-06-06_13-37-56.sql.gz.gpg	06/06/2019 13:59	GPG File	3,478 KB
NESIE_2019-06-06_14-05-53_databse.backup.gz...	06/06/2019 15:05	GPG File	2,435 KB

Fig 370. Select backup file

When the file has been located, the RESTORE button will turn blue and allow the operator to start the restore process. A dialogue box detailing the process of the restore process will be displayed as per Fig 371 below.



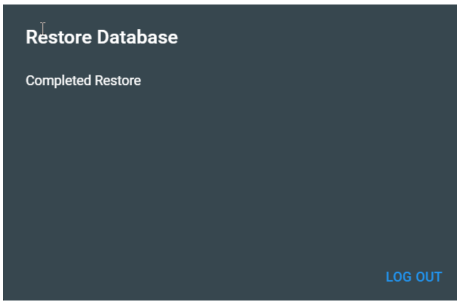
This action will destroy all existing data including users and targets. It will be replaced by the data from the backup file. Your settings will remain unchanged.

A backup of the current database will first be created on the device. All running actions will be stopped and you will be logged out of the system.

It is recommended that you restart the system after the operation has completed.

Fig 371. Restore – progress

When the restore process is completed, a dialogue box showing Complete Restore will be displayed as per Fig 372 below. The operator should now press the LOG OUT button and log back into NESIE again.



Restore Database

Completed Restore

Fig 372. Restore complete

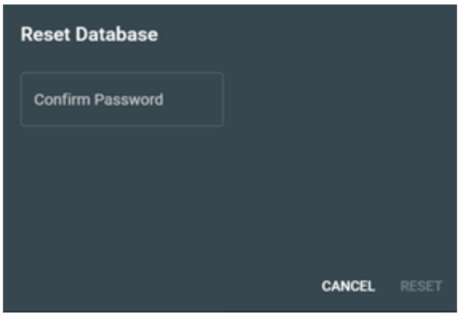
34.2.1.4 RESET DATABASE

Reset database is the process of factory resetting the entire system database. However, the software version will remain at its current version. This allows the operator to clean the system after operations, prior to storage, or returning it for update or repair.

The reset will delete all stored Users, Usernames, Passwords, IMSI, IMEI, SMS data, Geolocation data, Network Scan data, TAC list and Target data. The only log on details remaining is for the default Administrator.

As part of the reset database function, the NESIE software will automatically carry out a database backup as described in section 34.2.1.1 above.

After pressing the Reset Database button, a dialogue box requesting the password will be displayed, as shown at Fig 373 below. After entering the password, the RESET button will become available.

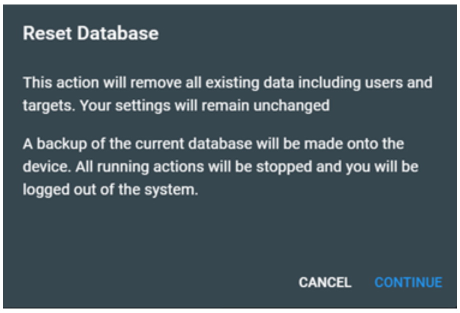


Reset Database

Confirm Password

Fig 373. Reset database

After pressing the RESET button, a dialogue box warning that the database is about to be reset / deleted will be shown. The operator should press the OK button if they wish to continue, as shown at Fig 374.


Reset Database

This action will remove all existing data including users and targets. Your settings will remain unchanged

A backup of the current database will be made onto the device. All running actions will be stopped and you will be logged out of the system.

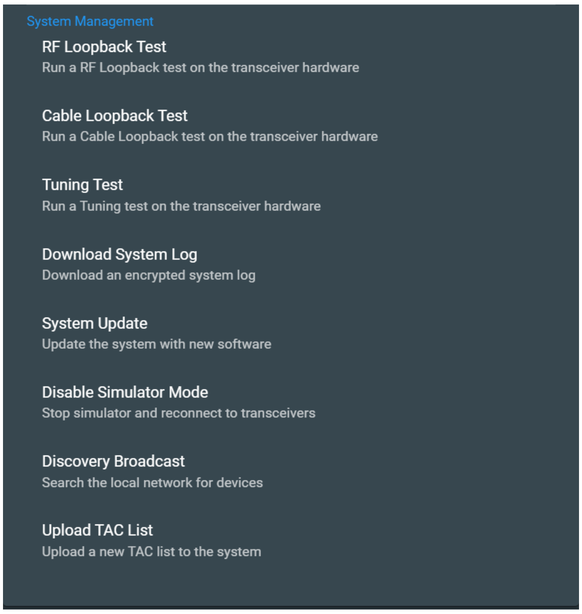
Fig 374. Reset – warning

After pressing the CONTINUE button, the system will perform a database backup then reset the database. When complete, the user will be logged out of the UI. Then log back in using the default Administrator settings.

34.3 SYSTEM MANAGEMENT

In the System Management section, the operator has eight options, as shown if Fig 375 below.

- **RF Loopback Test**
- **Cable Loopback Test**
- **Tuning Test**
- **Download System Log**
- **System Update**
- **Enable/Disable Simulator Mode**
- **Discovery Broadcast**
- **Upload TAC List**


System Management

RF Loopback Test
Run a RF Loopback test on the transceiver hardware

Cable Loopback Test
Run a Cable Loopback test on the transceiver hardware

Tuning Test
Run a Tuning test on the transceiver hardware

Download System Log
Download an encrypted system log

System Update
Update the system with new software

Disable Simulator Mode
Stop simulator and reconnect to transceivers

Discovery Broadcast
Search the local network for devices

Upload TAC List
Upload a new TAC list to the system

Fig 375. System Management

34.3.1 RF LOOPBACK TEST (AIRCRAFT ONLY)

As a part of the RF loopback test, the system conducts a re-calibration of the system frequency source (OCXO) against a local GSM base station. This portion of the RF loopback test will only be carried out if the system tuning appears to be out of specification and calibrated. The frequency source should remain stable for many years. As a result of the test, a pop-up message will be displayed.

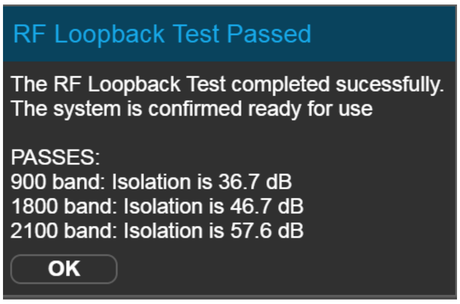
34.3.1.1 RF LOOPBACK TEST MESSAGES

There are five types of messages that can be displayed:

RF Loopback Test Passed
RF Loopback Test Failed
RF Loopback Test Passed – With Warning
RF Loopback Stopped
RF Loopback Incomplete.

These messages are given in detail below.

RF Loopback Test Passed



RF Loopback Test Passed

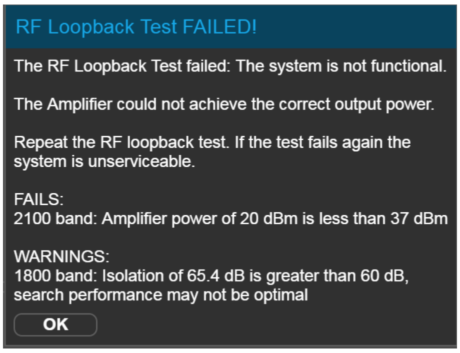
The RF Loopback Test completed sucessfully.
The system is confirmed ready for use

PASSES:
900 band: Isolation is 36.7 dB
1800 band: Isolation is 46.7 dB
2100 band: Isolation is 57.6 dB

Fig 376. RF Loopback Test Passed

As shown in the example (Fig 376), the RF loopback test has completed and passed. No errors are reported and no further action is required.

RF Loopback Test Failed



RF Loopback Test FAILED!

The RF Loopback Test failed: The system is not functional.

The Amplifier could not achieve the correct output power.

Repeat the RF loopback test. If the test fails again the system is unserviceable.

FAILS:
2100 band: Amplifier power of 20 dBm is less than 37 dBm

WARNINGS:
1800 band: Isolation of 65.4 dB is greater than 60 dB, search performance may not be optimal

Fig 377. RF Loopback Test Failed

As shown in the example (Fig 377), the RF loopback test has completed and failed. An explanation of what has caused the failure will be shown.

34.3.2 CABLE LOOPBACK TEST (AIRCRAFT ONLY)

This is effectively the same as an RF loopback test but is performed using a cable with 40dB of attenuation in it. The cable is supplied as standard with every TA/TU system. The users must disconnect the system from the antennas and connect the loopback cable between the TX and RX antenna ports. Running the test will test every band enabled by default on the system.

The reason to run this test is to verify all the bands on the system are working, and any faults are with the system not with the installation.
Results are presented in the same format as the RF loopback test.
No tuning test is run during this test, as the antennas are disconnected and no BTS would be found for the tuning test. The test run time is 10 to 15 minutes depending on the number of bands supported and the platform it is run on.

34.3.3 TUNING TEST (AIRCRAFT ONLY)

This test should be run with the antennas connected. The test searches for a GSM BTS. Once found, it compares the system frequency source to that of the GSM BTS. If the frequency is within the limits the test is passed. If the system frequency is outside the limits it is re-tuned to match the GSM BTS. This test is expected to pass as long as a GMS BTS is found. A warning is issued if no BTS is found.

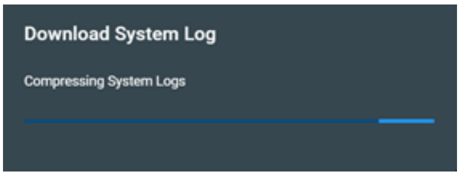
The test should be performed a minimum of once a month to maintain correct system tuning. The system should be stationary when the test is performed. Test run time is 1 to 2 minutes.

34.3.4 DOWNLOAD SYSTEM LOG

The System Log is a log of events and actions that happen in the NESIE software. This system log can be used by Smith Myers to detect and analyse the NESIE system after errors have occurred. This System log does not log any IMEI's / IMSI's, location data, Target names or other sensitive information.

When a system log is created it is saved in an encrypted .gz format. Smith Myers are the only people who Hold the password to open these files.

When the Download System Log button is pressed, a pane will show the current process, as shown at Fig 378 below.

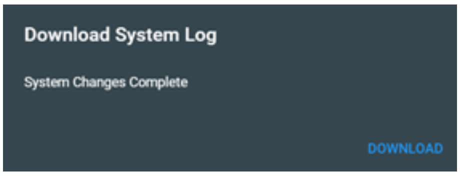


Download System Log

Compressing System Logs

Fig 378. Download System Log

When the download is complete, a dialogue box will appear allowing the user to download the log file, as shown in Fig 379 below.



Download System Log

System Changes Complete

Fig 379. Download System Log - complete

As per the section detailing the download of the database, the system log will be compiled and downloaded to the laptop download folder.

This file can now be taken off the laptop and sent to Smith Myers.

34.3.5 SYSTEM UPDATE – DOWNLOAD SOFTWARE

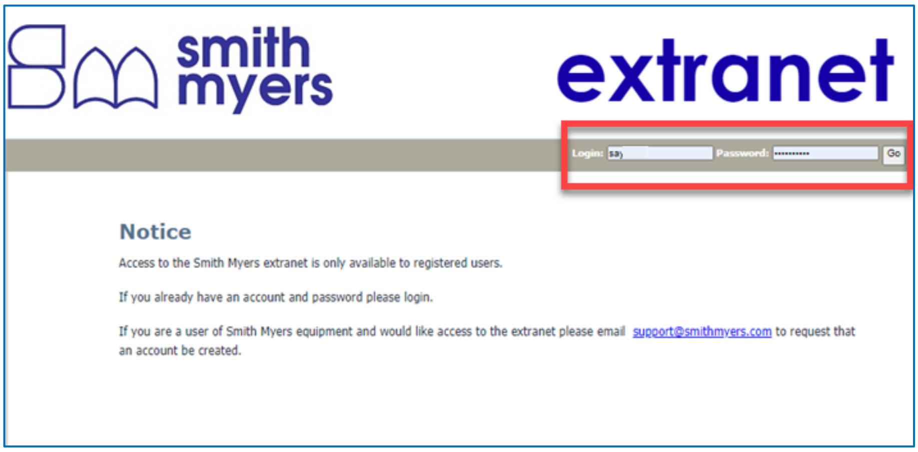
Periodically, Smith Myers will issue software updates for the NESIE system. These updates may address bugs that have been found in the software or enhancements to the capability or UI.

The user will be notified about these updates via an email from Smithmyers.com.

If the user has not previously logged at least 2 email addresses with Smith Myers, they should inform one of the staff as soon as possible.

Upon receipt of the update notification, the user will need to use the logon details (username & password) that they have been provided and log on to smithmyers.com

The user should now log on to http://extranet.smithmyers.com/index.php
And enter their unique log on details, as shown Fig 380 below.



Login: say Password: •••••••••• Go

Notice

Access to the Smith Myers extranet is only available to registered users.

If you already have an account and password please login.

If you are a user of Smith Myers equipment and would like access to the extranet please email support@smithmyers.com to request that an account be created.

Fig 380. SmithMyers.com log on

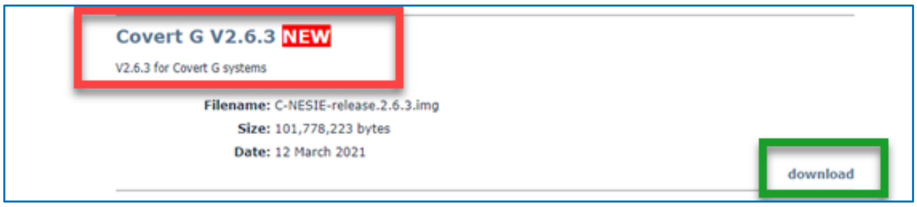
Identify the new software version and ensure it is the correct software for your system.

- Covert G Covert Ground or Covert NESIE systems
- Tactical G Tactical Ground or Tactical NESIE – individual modules
  Only to be used if the Tactical module is in standalone mode

- MCM Tactical Control Modules
  If a Tactical Module is connected to a TCM, this version of the software should be used.

NOTE: If the MCM software is used, it will initially update the software in the TCM then automatically distribute the update to any Tactical units that have been connected.

The title of the update will state the NESIE system type and the software version number. This software should now be downloaded to the laptop, as shown in Fig 381 below.



Covert G V2.6.3 NEW

V2.6.3 for Covert G systems

Filename: C-NESIE-release.2.6.3.img

Size: 101,778,223 bytes

Date: 12 March 2021

download

Fig 381. Software update – download

When the software update has been downloaded it should be uploaded onto the NESIE system.

34.3.6 SYSTEM UPDATE

The update file will normally have been downloaded from the Smith Myers website. The file should be stored / be on the tablet / laptop being used for the update.

Ideally the NESIE system should be connected via ethernet to ensure there are no errors during the upload.

The current version of the software is displayed on the tab at the top of the browser, see Fig 382.

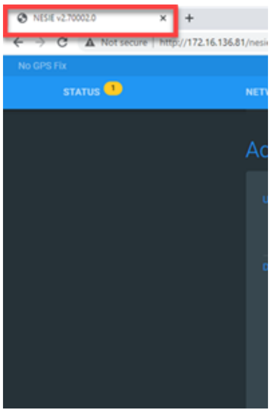
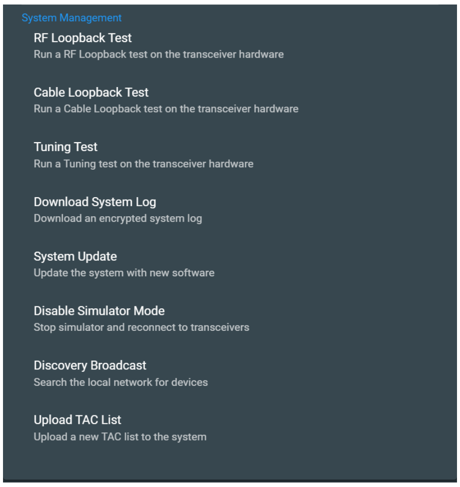


Fig 382. Software version

To carry out a software update, the operator should navigate to Settings / System Update pane as shown at Fig 383 below and press the System Update button.



System Management

RF Loopback Test
Run a RF Loopback test on the transceiver hardware

Cable Loopback Test
Run a Cable Loopback test on the transceiver hardware

Tuning Test
Run a Tuning test on the transceiver hardware

Download System Log
Download an encrypted system log

System Update
Update the system with new software

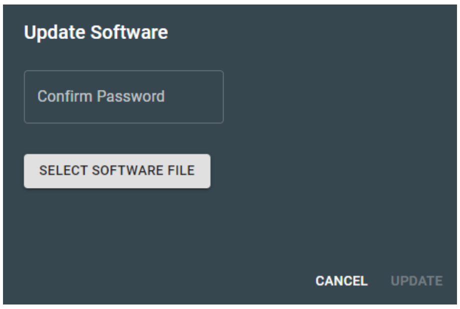
Disable Simulator Mode
Stop simulator and reconnect to transceivers

Discovery Broadcast
Search the local network for devices

Upload TAC List
Upload a new TAC list to the system

Fig 383. System Update

The Update Software dialogue box will appear. The password must be entered, and the operator should then navigate to the updated file after clicking the Select Software File button, then press the UPDATE button, as shown below Fig 384.

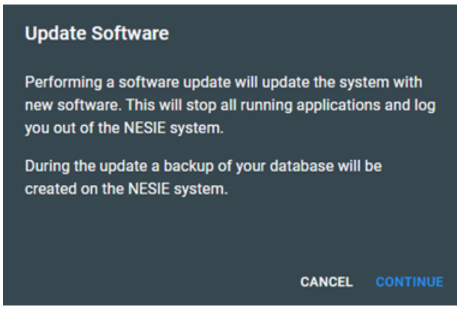


Update Software

Confirm Password

Fig 384. Software update

The warning box shown at Fig 385 will be displayed. Click the CONTINUE button.



Update Software

Performing a software update will update the system with new software. This will stop all running applications and log you out of the NESIE system.

During the update a backup of your database will be created on the NESIE system.

Fig 385. Software update – warning

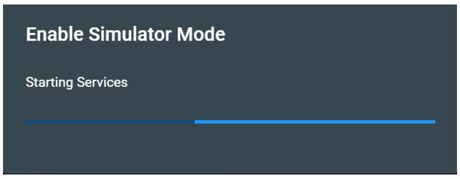
The NESIE system will now carry out the software update and notify the user of the current progress. If required, any prompts will also be displayed.

When the software update is complete, the dialogue box will show Update Complete. The user must now click the Log Out button and log back on to the NESIE system.

> **NOTE –** when updating the software, it is necessary to update the system with progressive software versions e.g. a system being updated to software version 2.10.6 that is currently running version 2.10.3, must have versions 2.10.4 and 2.10.5 installed prior to installing 2.10.6.

34.3.7 DISABLE/ENABLE SIMULATOR MODE

If the Tactical Control Module has the ability to run the NESIE simulator, this function allows the simulator software to be activated. When the function is selected, a number of system messages are displayed (Fig 386).

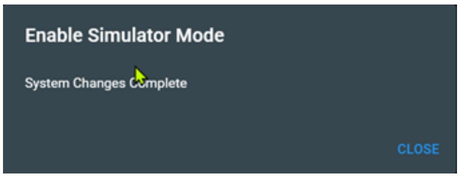


Enable Simulator Mode

Starting Services

Fig 386 Enable/Disable Simulator Mode - system messages

Once the software has been initiated successfully, the following message will be displayed (Fig 387).



Enable Simulator Mode

System Changes Complete

Fig 387 Simulator mode successfully inititiated

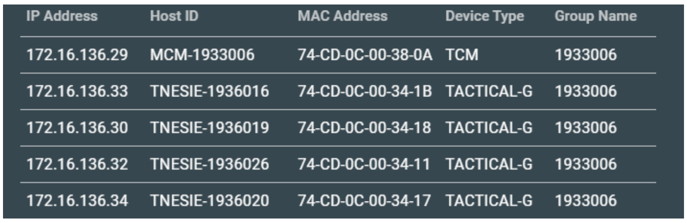
34.3.8 DISCOVERY BROADCAST

The discovery broadcast is a way of detecting the settings of other NESIE units connected in a stack or via a network. This is primarily used as an engineer feature.

When the Discovery Broadcast button is pressed, the NESIE software will discover what other units are connected to the system and display the results, as shown at Fig 388.

The Table consists of the following information:

• **IP Address**	Of the individual units
• **Host ID**	Name and serial number of the unit
• **MAC Address**	MAC address of individual units
• **Device Type**	Type of unit
• **Group Name**	The group name of the units



IP Address	Host ID	MAC Address	Device Type	Group Name
172.16.136.29	MCM-1933006	74-CD-0C-00-38-0A	TCM	1933006
172.16.136.33	TNESIE-1936016	74-CD-0C-00-34-1B	TACTICAL-G	1933006
172.16.136.30	TNESIE-1936019	74-CD-0C-00-34-18	TACTICAL-G	1933006
172.16.136.32	TNESIE-1936026	74-CD-0C-00-34-11	TACTICAL-G	1933006
172.16.136.34	TNESIE-1936020	74-CD-0C-00-34-17	TACTICAL-G	1933006

Fig 388. Discovery - results

34.3.9 TAC LIST – FORMAT BEFORE UPLOADING

The Type Allocation Code (TAC) list, uses the recovered IMEI to identify the make and model of the mobile device. The NESIE system is pre-loaded with a TAC list, but it will be become out of date very quickly. It is believed that most users groups will have access to a more up to date list from a trusted source.

The user now has the option to load a locally sourced TAC list, the pre-loaded TAC list supplied with the NESIE system will be overwritten.

The NESIE system will accept a TAC list that is in a CSV format with the following parameters:

The field separation delimiters must be either of the following:

, (Comma)

| (Post)

; (Semicolon)

The delimiters cannot be in the data fields and no escapes are supported (an escape is a special character put prior to the delimiter character to prevent it being interpreted as a delimiter).

When importing the file, the NESIE software searches the first line of the file to find the columns to import, the searches are not case sensitive.

Three columns are required, and the first column found to match each search is used. Any other data is not loaded into the NESIE system. The columns can be in any order on the top row of the spread sheet.

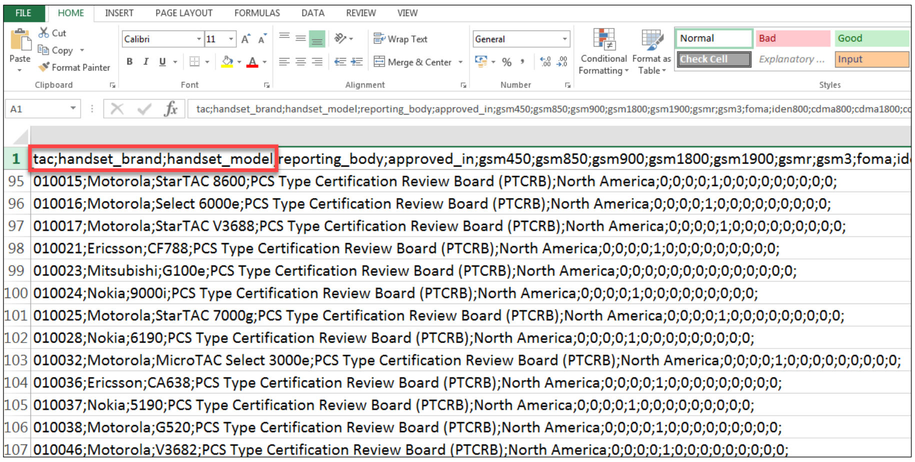
TAC:
The first column to match “ID TAC” or “TAC” as the title.

Brand:
The first column to contain “Manufacturer” or “Brand” at the end of the title, e.g. “Device brand” or “Device brand”.

Model:
The first column to contain “Name” or “Model” at the end of the title, e.g. “Marketing Name” or “Device Model”.

Shown in below in Fig 389. is an example of a TAC list in CSV Format opened in Microsoft Excel.

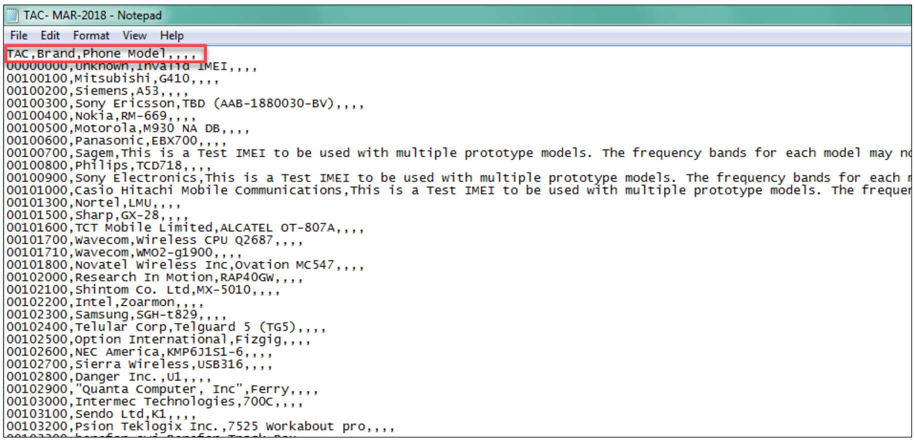
In Fig 390 below is an example TAC list in CSV format opened in Notepad. Shown in the red box are the required headers separated by semicolons. When the TAC list is imported, the software will look for the required headers then extract the data in the associated column.



```
tac;handset_brand;handset_model;reporting_body;approved_in;gsm450;gsm850;gsm900;gsm1800;gsm1900;gsmr;gsm3;foma;iden800;cdma800;cdma1800;cc
```

```
1   tac;handset_brand;handset_model;reporting_body;approved_in;gsm450;gsm850;gsm900;gsm1800;gsm1900;gsmr;gsm3;foma;id
95  010015;Motorola;StarTAC 8600;PCS Type Certification Review Board (PTCRB);North America;0;0;0;0;1;0;0;0;0;0;0;0;0;
96  010016;Motorola;Select 6000e;PCS Type Certification Review Board (PTCRB);North America;0;0;0;0;1;0;0;0;0;0;0;0;0;
97  010017;Motorola;StarTAC V3688;PCS Type Certification Review Board (PTCRB);North America;0;0;0;0;1;0;0;0;0;0;0;0;0;
98  010021;Ericsson;CF788;PCS Type Certification Review Board (PTCRB);North America;0;0;0;0;1;0;0;0;0;0;0;0;0;
99  010023;Mitsubishi;G100e;PCS Type Certification Review Board (PTCRB);North America;0;0;0;0;0;0;0;0;0;0;0;0;0;
100 010024;Nokia;9000i;PCS Type Certification Review Board (PTCRB);North America;0;0;0;0;1;0;0;0;0;0;0;0;0;
101 010025;Motorola;StarTAC 7000g;PCS Type Certification Review Board (PTCRB);North America;0;0;0;0;1;0;0;0;0;0;0;0;0;
102 010028;Nokia;6190;PCS Type Certification Review Board (PTCRB);North America;0;0;0;0;1;0;0;0;0;0;0;0;0;
103 010032;Motorola;MicroTAC Select 3000e;PCS Type Certification Review Board (PTCRB);North America;0;0;0;0;1;0;0;0;0;0;0;0;0;
104 010036;Ericsson;CA638;PCS Type Certification Review Board (PTCRB);North America;0;0;0;0;1;0;0;0;0;0;0;0;0;
105 010037;Nokia;5190;PCS Type Certification Review Board (PTCRB);North America;0;0;0;0;1;0;0;0;0;0;0;0;0;
106 010038;Motorola;G520;PCS Type Certification Review Board (PTCRB);North America;0;0;0;0;1;0;0;0;0;0;0;0;0;
107 010046;Motorola;V3682;PCS Type Certification Review Board (PTCRB);North America;0;0;0;0;1;0;0;0;0;0;0;0;0;
```

Fig 389. TAC List – Example CSV in Excel



```
TAC,Brand,Phone Model,,,,
00000000,Unknown,Invalid IMEI,,,,
00100100,Mitsubishi,G410,,,,
00100200,Siemens,A53,,,,
00100300,Sony Ericsson,TBD (AAB-1880030-BV),,,,
00100400,Nokia,RM-669,,,,
00100500,Motorola,M930 NA DB,,,,
00100600,Panasonic,EBX700,,,,
00100700,Sagem,This is a Test IMEI to be used with multiple prototype models. The frequency bands for each model may no
00100800,Philips,TCD718,,,,
00100900,Sony Electronics,This is a Test IMEI to be used with multiple prototype models. The frequency bands for each m
00101000,Casio Hitachi Mobile Communications,This is a Test IMEI to be used with multiple prototype models. The frequen
00101300,Nortel,LMU,,,,
00101500,Sharp,GX-28,,,,
00101600,TCT Mobile Limited,ALCATEL OT-807A,,,,
00101700,Wavecom,Wireless CPU Q2687,,,,
00101710,Wavecom,WMO2-g1900,,,,
00101800,Novatel Wireless Inc,Ovation MC547,,,,
00102000,Research In Motion,RAP40GW,,,,
00102100,Shintom Co. Ltd,MX-5010,,,,
00102200,Intel,Zoarmon,,,,
00102300,Samsung,SGH-t829,,,,
00102400,Telular Corp,Telguard 5 (TG5),,,,
00102500,Option International,Fizgig,,,,
00102600,NEC America,KMP6J1S1-6,,,,
00102700,Sierra Wireless,USB316,,,,
00102800,Danger Inc.,U1,,,,
00102900,"Quanta Computer, Inc",Ferry,,,,
00103000,Intermec Technologies,700C,,,,
00103100,Sendo Ltd,K1,,,,
00103200,Psion Teklogix Inc.,7525 Workabout pro,,,,
```

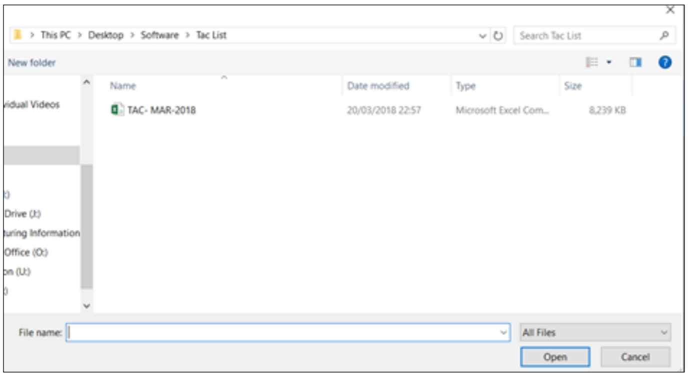
Fig 390. TAC list - example CSV in Notepad

Errors are reported on failures, warning on lines that fail to import (e.g. Lack the required columns, contain no data etc.)

34.3.9.1 UPLOAD A TAC LIST

Prior to uploading a suitably formatted TAC list, the operator must save or have access to the CSV file on the laptop used on the NESIE system. Where possible, it is advisable to connect to the NESIE system using an ethernet cable as a Wi-Fi connection may be interrupted.

When the operator presses the Upload TAC list button, a pop-up window will be displayed so the operator can select where the CSV file has been saved, as shown in Fig 391 below. The operator will select the desired file and click open.



Name	Date modified	Type	Size
TAC- MAR-2018	20/03/2018 22:57	Microsoft Excel Com...	8,239 KB

Fig 391. Upload TAC list – file location

When Open is clicked, the NESIE software will automatically upload the new data and display a processing pop-up window.

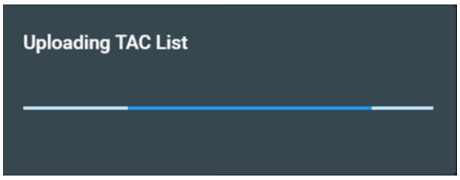
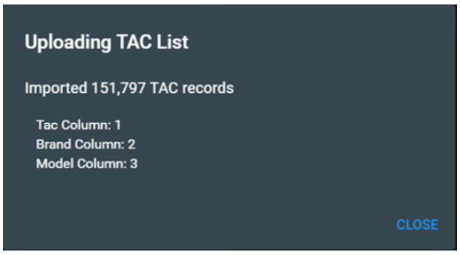

Uploading TAC List

Fig 392. Upload TAC list

When the upload is complete, a dialogue box will display the number of fields uploaded and if any errors occurred.


Uploading TAC List

Imported 151,797 TAC records

Tac Column: 1
Brand Column: 2
Model Column: 3

Fig 393. Upload TAC - complete

35. LTE FDD & LTE TDD

35.1 WHAT IS LTE?

LTE is the abbreviation of Long Term Evolution. It is a 4G standard used worldwide for transferring data over cellular networks. The terms 4G and LTE are often used synonymously; however, they do not mean the same thing. There are different 4G standards, and LTE is one of the most common. It provides 10 x the speeds of 3G networks. LTE offers higher peak data transfer rates, reduced latency and scalable bandwidth capacity, so that users access services easily in near real time and experience limited lagging.

NOTE: LTE may also refer to LTE Advanced, a newer version of LTE that supports peak download speeds of 1 Gbps and upload speeds of 500 Mbps (10x the speeds of standard LTE).

LTE uses OFDM (orthogonal frequency division multiplexing) and, in later releases, MIMO (multiple input, multiple output) antenna technology like that used in the IEEE 802.11n wireless local area network (WLAN) standard. The higher signal-to-noise ratio (SNR) at the receiver enabled by MIMO, along with OFDM, provides improved wireless network coverage and throughput, especially in dense urban areas.

35.2 LTE FDD & LTE TDD EXPLAINED

Within 4G LTE, the frequencies are split into two spectrum usage techniques:

- Frequency Division Duplexing (FDD) this technique requires paired frequency bands, one for uplink and one for the downlink.

- Time Division Duplexing (TDD) TDD uses a single band for the uplink and downlink on the same frequency but these are time-separated instead.

35.2.1 FDD ADVANTAGES/DISADVANTAGES

- **Advantages**

  - It is a proven technology for symmetric voice traffic
  - It can achieve higher rates for similar distances than TDD
  - It requires fewer base stations compared to TDD
  - Because of less base station equipment/maintenance it can be cheaper than TDD

- **Disadvantages**

  - It is not spectrally efficient, uses twice the frequencies of TDD
  - It cannot be deployed where spectrum is unpaired.
  - Though it saves costs through less base station equipment associated hardware costs are higher than TDD

35.2.2 TDD ADVANTAGES/DISADVANTAGES

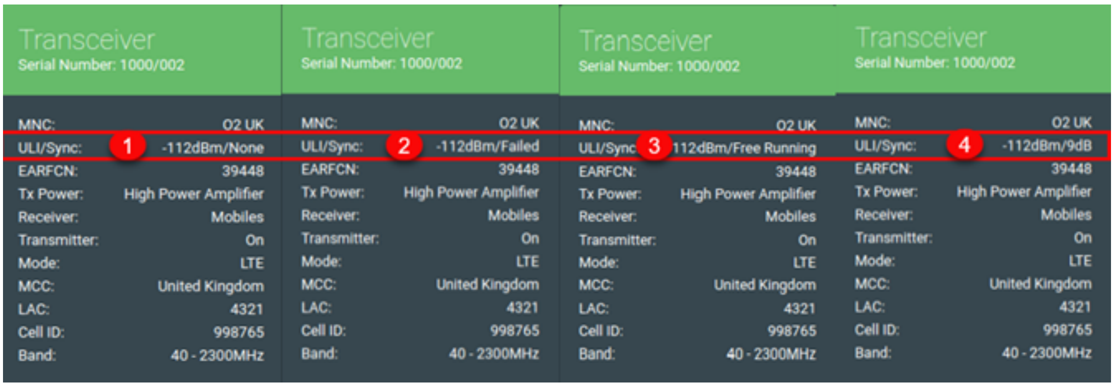
- **Advantages**
  - It does not use paired spectrum like FDD, it is more spectrally efficient
  - TDD time slots can be dynamically altered to accommodate traffic flow
- **Disadvantages**
  - It requires stringent phase/time synchronization to avoid interference between uplink and downlink transmissions
  - As transmissions are not continuous, lower data rates are achieved compared to FDD at similar distances from Base Stations
  - It supports lesser distances compared to FDD, needs more Base Stations to cover a similar area hence it is more expensive

35.3 LTE TDD - NESIE CAPABILITIES

When the NESIE system is capturing TDD in an area served by a TDD cell, it must synchronise to the serving BTS to ensure we are transmitting and receiving at the same time as the real network.

The sync status is displayed in the TRX status box during the Grab. The states are important as a failed sync or no sync make the probability of capturing phones low if there is TDD coverage in the area on the same frequency.
While transmitting a TDD cell, the NESIE UI will display one of 4 states for the sync as seen in Fig 394 below.

- 1 None – The sync was never attempted, as the Grab was started from a manual config or from a neighbour cell
- 2 Failed – The attempt to sync failed, and the Grab is proceeding as if no sync was attempted
- 3 Free Running – A sync was initially achieved but has now been lost, the system will continue to maintain sync for a minute or two in this state
- 4 9dB – A sync is currently achieved and the SNR of the BTS signal is at least 9dBs (the dB value will alter depending on the synch SNR)



Transceiver
Serial Number: 1000/002
MNC: O2 UK
ULI/Sync: -112dBm/None
EARFCN: 39448
Tx Power: High Power Amplifier
Receiver: Mobiles
Transmitter: On
Mode: LTE
MCC: United Kingdom
LAC: 4321
Cell ID: 998765
Band: 40 - 2300MHz

Transceiver
Serial Number: 1000/002
MNC: O2 UK
ULI/Sync: -112dBm/Failed
EARFCN: 39448
Tx Power: High Power Amplifier
Receiver: Mobiles
Transmitter: On
Mode: LTE
MCC: United Kingdom
LAC: 4321
Cell ID: 998765
Band: 40 - 2300MHz

Transceiver
Serial Number: 1000/002
MNC: O2 UK
ULI/Sync 112dBm/Free Running
EARFCN: 39448
Tx Power: High Power Amplifier
Receiver: Mobiles
Transmitter: On
Mode: LTE
MCC: United Kingdom
LAC: 4321
Cell ID: 998765
Band: 40 - 2300MHz

Transceiver
Serial Number: 1000/002
MNC: O2 UK
ULI/Sync: -112dBm/9dB
EARFCN: 39448
Tx Power: High Power Amplifier
Receiver: Mobiles
Transmitter: On
Mode: LTE
MCC: United Kingdom
LAC: 4321
Cell ID: 998765
Band: 40 - 2300MHz

Fig 394. LTE TDD Synch Status

36. MEMORY CARDS / DATA STORAGE

36.1 REMOVAL OF SOLID STATE DATA STORAGE

The NESIE equipment utilizes a range of electronic solid state data storage (SD/SSD/CF cards) to house its Operating System (OS) and all collected/input mission/operational data.

In some cases, these cards are accessible and can be removed from the hardware if the system OS needs updating or has become corrupt. Also, some operators may have security procedures to observe that demand the removal of the memory card to secure storage when the NESIE is not being used.

36.2 RETURNING NESIE – RECOMMENDED PROCEDURE

In certain circumstances, the NESIE system might need to be returned to Smith Myers for a repair or an upgrade. If your NESIE system has an accessible memory card, Smith Myers recommend that the following procedures are carried out prior to returning equipment.

1. Backup and download the NESIE database and the Target list to the downloads folder or operational folder on your PC/Laptop.
2. Reset the NESIE database to erase all operational data.
3. If the NESIE system has an accessible memory card, remove and format/destroy it so there is no risk of it being reinserted when the system is returned to them – A new card will be installed at Smith Myers.
4. When the NESIE is returned to the user, the database can be restored from the Admin menu.

36.3 MEMORY CARDS – OPERATIONAL CONSIDERATIONS

In certain operational scenarios, Covert NESIE can be deployed within a bag or backpack and be controlled remotely by the operator via Wi-Fi. It may be possible (but highly unlikely), that the memory card could be accidentally pushed and ejected from its slot whilst in the bag whilst the equipment was being used. To avoid this very improbable event, it is suggested that the operator places a piece of tape over the card slot to prevent this from happening.

37. UMTS LONG CELL ID OR SHORT CELL ID

The NESIE UI displays the Long Cell ID in the UMTS mode. Some users may wish to convert the Long Cell ID into the Short Cell ID.

The Long Cell ID is made up from the following information

Long CID = 65536 Multiplied by the RNC plus the CID

RNC = Radio Network Controller

CID = Short Cell ID

If you have the Long Cell ID, you can calculate the RNC and short Cell ID in the following way:

RNC = Long CID divided by 65536

CID = Long CID mod 65536

Example for long cell ID 66808694:

RNC = 66808694 / 65536 = 1019

CID = 66808694 mod 65536 = 27510

To turn the Windows laptop calculator into the correct mode carry out the following: Open the calculator and Select VIEW / Scientific as shown in Fig 395 below.

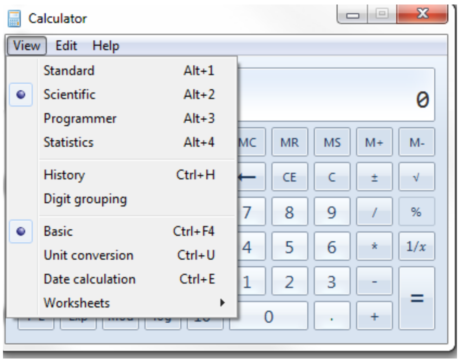
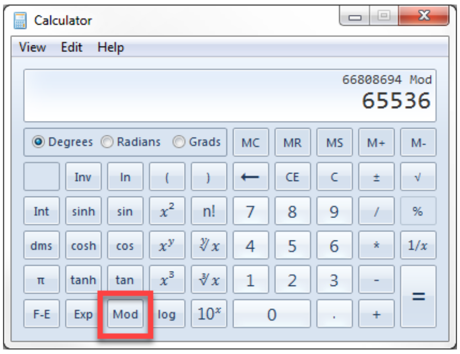


Fig 395. Scientific Calculator

To convert the Long Cell ID 66808694 to the short Cell ID, Type in 66806694 Mod (Button) 65536 **=** as shown in Fig 396 below.



```
66808694 Mod
65536
```

Calculator
View Edit Help
○ Degrees ○ Radians ○ Grads
MC MR MS M+ M-
Inv ln ( ) ← CE C ± √
Int sinh sin x^2 n! 7 8 9 / %
dms cosh cos x^y $\sqrt[y]{x}$ 4 5 6 * 1/x
π tanh tan x^3 $\sqrt[3]{x}$ 1 2 3 -
F-E Exp Mod log 10^x 0 . + =

Fig 396. Long Cell ID - Short Cell ID

38. IMPORTING & EXPORTING CSV FILES

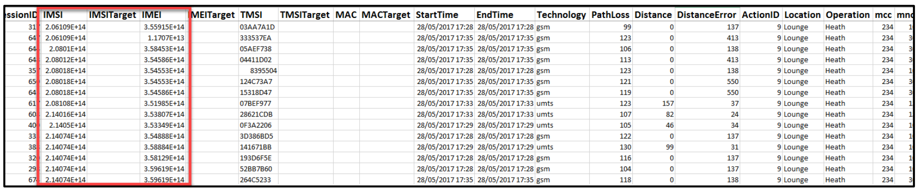
All Identities and Target List files downloaded from the NESIE system are generated in Comma Separated Value (CSV) format. Database backup files are generated in encrypted format. The file format allows the files to be imported into a wide variety of database analysis software such as i2 Analysts' Notebook or other data visualisation software. The files that can be downloaded from NESIE include:

- **Target Lists**
- **Collected ID captures from the NESIE database**
- **Database back ups**

38.1 OPENING CSV FILES IN MICROSOFT EXCEL

NOTE: In newer versions of Microsoft Excel the layout of the tools and button locations may have changed discretely but are simple to find.

CSV files can also be opened in Microsoft Excel for viewing. However, if the CSV file is double clicked, it will automatically open in XL but some of the columns (IMSI and IMEI) will be displayed incorrectly. See Fig 397 below.



ssionID	IMSI	IMSITarget	IMEI	MEITarget	TMSI	TMSITarget	MAC	MACTarget	StartTime	EndTime	Technology	PathLoss	Distance	DistanceError	ActionID	Location	Operation	mcc	mn
31	2.06109E+14		3.55915E+14		03AA7A1D				28/05/2017 17:28	28/05/2017 17:28	gsm	99	0	137	9	Lounge	Heath	234	1
64	2.06109E+14		1.1707E+13		333537EA				28/05/2017 17:35	28/05/2017 17:35	gsm	123	0	413	9	Lounge	Heath	234	3
64	2.0801E+14		3.58453E+14		05AEF738				28/05/2017 17:35	28/05/2017 17:35	gsm	106	0	138	9	Lounge	Heath	234	3
64	2.08012E+14		3.54586E+14		04411D02				28/05/2017 17:35	28/05/2017 17:35	gsm	113	0	413	9	Lounge	Heath	234	3
35	2.08018E+14		3.54553E+14		8395504				28/05/2017 17:28	28/05/2017 17:28	gsm	123	0	138	9	Lounge	Heath	234	1
65	2.08018E+14		3.54553E+14		124C73A7				28/05/2017 17:35	28/05/2017 17:35	gsm	121	0	550	9	Lounge	Heath	234	3
64	2.08018E+14		3.54586E+14		15318D47				28/05/2017 17:35	28/05/2017 17:35	gsm	119	0	550	9	Lounge	Heath	234	3
61	2.08108E+14		3.51985E+14		07BEF977				28/05/2017 17:33	28/05/2017 17:33	umts	123	157	37	9	Lounge	Heath	234	1
60	2.14016E+14		3.53807E+14		28621CDB				28/05/2017 17:33	28/05/2017 17:33	umts	107	82	24	9	Lounge	Heath	234	1
40	2.1405E+14		3.53349E+14		0F3A2206				28/05/2017 17:29	28/05/2017 17:29	umts	105	46	34	9	Lounge	Heath	234	1
33	2.14074E+14		3.54888E+14		3D386BD5				28/05/2017 17:28	28/05/2017 17:28	gsm	122	0	137	9	Lounge	Heath	234	1
38	2.14074E+14		3.58884E+14		141671BB				28/05/2017 17:29	28/05/2017 17:29	umts	130	99	31	9	Lounge	Heath	234	1
32	2.14074E+14		3.58129E+14		193D6F5E				28/05/2017 17:28	28/05/2017 17:28	gsm	116	0	137	9	Lounge	Heath	234	1
29	2.14074E+14		3.59619E+14		52BB7B60				28/05/2017 17:28	28/05/2017 17:28	gsm	104	0	137	9	Lounge	Heath	234	1
67	2.14074E+14		3.59619E+14		264C5233				28/05/2017 17:35	28/05/2017 17:35	gsm	118	0	138	9	Lounge	Heath	234	3

Fig 397. CSV directly into XL

To open a NESIE CSV file and ensure the data is displayed correctly, follow the instructions below:

1. Open Microsoft Excel from the PC, laptop or tablet menu (do not click on the CSV file directly).

2. Or open a new XL document from the File tab in XL.

3. A blank spreadsheet will be displayed.

4. Choose the Data tab and Click From Text as shown in Fig 398.

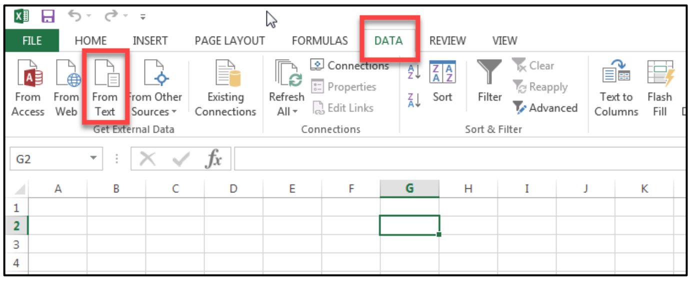
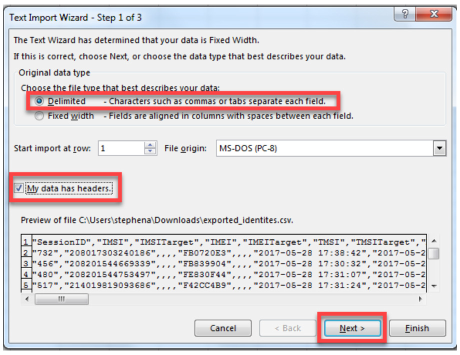


Fig 398. Open CSV in XL - From Text

5. Choose the downloaded file to open. The Text Import Wizard – Step 1 will now be displayed as shown in Fig 399.

   a. Choose Delimited (commas separate the value fields)
   b. Tick My data has headers
   c. Click Next



Text Import Wizard - Step 1 of 3

The Text Wizard has determined that your data is Fixed Width.

If this is correct, choose Next, or choose the data type that best describes your data.

Original data type

Choose the file type that best describes your data:

● Delimited - Characters such as commas or tabs separate each field.
○ Fixed width - Fields are aligned in columns with spaces between each field.

Start import at row: 1 File origin: MS-DOS (PC-8)

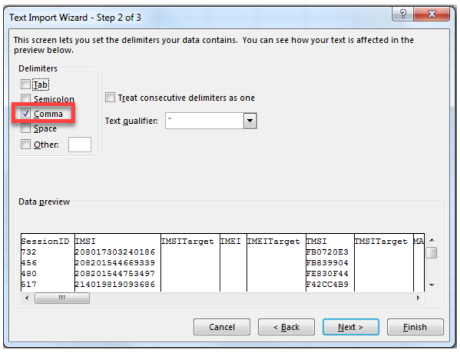
☑ My data has headers.

Preview of file C:\Users\stephena\Downloads\exported_identites.csv.

```
1 "SessionID","IMSI","IMSITarget","IMEI","IMEITarget","TMSI","TMSITarget","
2 "732","208017303240186",,,,"FB0720E3",,,,"2017-05-28 17:38:42","2017-05-2
3 "456","208201544669339",,,,"FB839904",,,,"2017-05-28 17:30:32","2017-05-2
4 "480","208201544753497",,,,"FE830F44",,,,"2017-05-28 17:31:07","2017-05-2
5 "517","214019819093686",,,,"F42CC4B9",,,,"2017-05-28 17:31:24","2017-05-2
```

Fig 399. Text import wizard – Step 1

6. In Text Import Wizard – Step 2, tick the Coma option, ensure to un-tick any others that are displayed, see Fig 400. Then press Next.



Text Import Wizard - Step 2 of 3

This screen lets you set the delimiters your data contains. You can see how your text is affected in the preview below.

Delimiters

☐ Tab
☐ Semicolon
☑ Comma
☐ Space
☐ Other:

☐ Treat consecutive delimiters as one

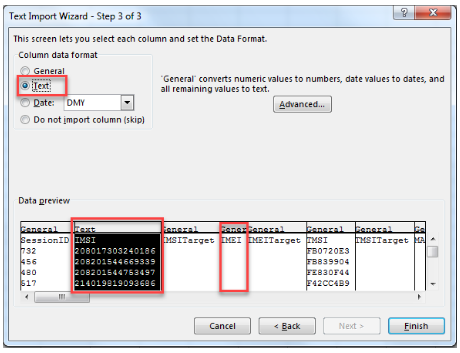
Text qualifier: "

Data preview

SessionID	IMSI	IMSITarget	IMEI	IMEITarget	TMSI	TMSITarget	MA
732	208017303240186				FB0720E3		
456	208201544669339				FB839904		
480	208201544753497				FE830F44		
517	214019819093686				F42CC4B9		

Fig 400. Text import wizard - Step 2

7. The Text Import Wizard – Step 3 pop-up box will be displayed. Then in the Data Preview pane, choose any fields that are usually displayed incorrectly (IMSI, IMEI). When selected they will be shown in black. Ensure the Colum Data Format is changed from General to Text by using the Text radial button, as shown in Fig 401. Then press Finish.



Text Import Wizard - Step 3 of 3

This screen lets you select each column and set the Data Format.

Column data format

○ General

● Text

○ Date: DMY

○ Do not import column (skip)

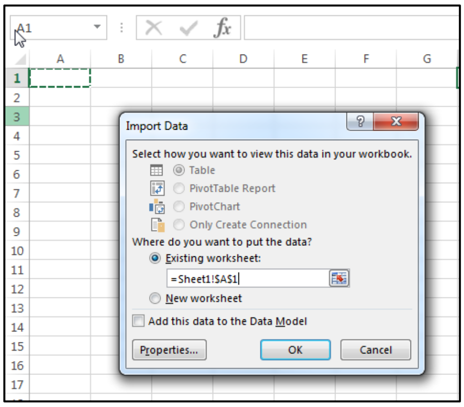
'General' converts numeric values to numbers, date values to dates, and all remaining values to text.

Data preview

General	Text	General	Gener	General	General	General	Ge
SessionID	IMSI	IMSITarget	IMEI	IMEITarget	TMSI	TMSITarget	MA
732	208017303240186				FB0720E3		
456	208201544669339				FB839904		
480	208201544753497				FE830F44		
517	214019819093686				F42CC4B9		

Fig 401. Text Import Wizard - Step 3

Ensure the XL selector is placed in square 1A then click on the Import Data pop-up box as shown in Fig 402.



Import Data

Select how you want to view this data in your workbook.

● Table

○ PivotTable Report

○ PivotChart

○ Only Create Connection

Where do you want to put the data?

● Existing worksheet:

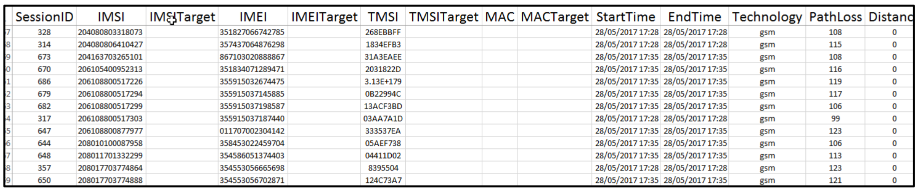
=Sheet1!A1

○ New worksheet

□ Add this data to the Data Model

Fig 402. Import Data Pop-up

8. The CSV data will now be imported into Microsoft Excel displaying the information correctly as can be seen in Fig 403

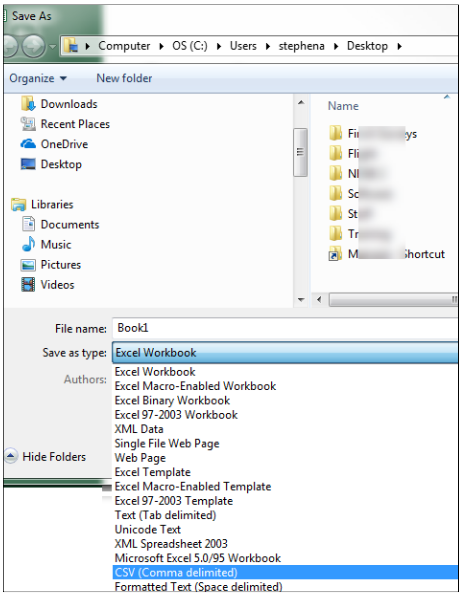


SessionID	IMSI	IMSITarget	IMEI	IMEITarget	TMSI	TMSITarget	MAC	MACTarget	StartTime	EndTime	Technology	PathLoss	Distanc
328	204080803318073		351827066742785		268EBBFF				28/05/2017 17:28	28/05/2017 17:28	gsm	108	0
314	204080806410427		357437064876298		1834EFB3				28/05/2017 17:28	28/05/2017 17:28	gsm	115	0
673	204163703265101		867103020888867		31A3EAEE				28/05/2017 17:35	28/05/2017 17:35	gsm	108	0
670	206105400952313		351834071289471		2031822D				28/05/2017 17:35	28/05/2017 17:35	gsm	116	0
686	206108800517226		355915032674475		3.13E+179				28/05/2017 17:35	28/05/2017 17:35	gsm	119	0
679	206108800517294		355915037145885		0B22994C				28/05/2017 17:35	28/05/2017 17:35	gsm	117	0
682	206108800517299		355915037198587		13ACF3BD				28/05/2017 17:35	28/05/2017 17:35	gsm	106	0
317	206108800517303		355915037187440		03AA7A1D				28/05/2017 17:28	28/05/2017 17:28	gsm	99	0
647	206108800877977		011707002304142		333537EA				28/05/2017 17:35	28/05/2017 17:35	gsm	123	0
644	208010100087958		358453022459704		05AEF738				28/05/2017 17:35	28/05/2017 17:35	gsm	106	0
648	208011701332299		354586051374403		04411D02				28/05/2017 17:35	28/05/2017 17:35	gsm	113	0
357	208017703774864		354553056665698		8395504				28/05/2017 17:28	28/05/2017 17:28	gsm	123	0
650	208017703774888		354553056702871		124C73A7				28/05/2017 17:35	28/05/2017 17:35	gsm	121	0

Fig 403. CSV data Correctly Imported Into XL

9. The operator now has the option to save the files. The operator must save the document in .XL format the maintain the correct configuration.

10. If the operator wants to re import a file back into a NESIE system or another data management software package, the file should be saved in the original format – .**CSV** as shown in Fig 404 below.



File name: Book1

Save as type: Excel Workbook

Fig 404. Save as .CSV

39. SMS CHARACTERS SUPPORTED

White space:
LF (Line feed), CR (Carriage return), Space

Punctuation:
!"#$%&'()*-./:;<=>?@_¡£¤¥§¿

Numbers:
0123456789

Letters:
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyzÄÅÆÇÉÑÖØÜß
àäåæèéìñòöøùü

40. LIST OF FIGURES

41. COPYRIGHT & WARRANTY

Copyright
This manual is protected by copyright law. No part of this manual may be reproduced, transmitted, stored in a retrieval system, or translated into any language (natural or computer), in any form or by any means without prior written permission of Smith Myers Communications Ltd.

Information in this manual is subject to change without notice and does not represent a commitment on the part of Smith Myers Communications Ltd.
CSM7901/CMS7902, the Smith Myers name and logo are registered trademarks of Smith Myers Communications Ltd in the UK and Smith Myers Inc. in the USA.

Patent Protection
Smith Myers products are protected by patent. Any infringement of these patent rights will result in prosecution.

One Year Warranty
Smith Myers Communications (hereby referred to as SMC) certify to the purchaser that the SMC hardware and software media will be free from defects in materials and workmanship, and that the software will execute its programming instructions when properly installed. SMC does not certify that the software will be uninterrupted or error free.

SMC reserves the right to repair or replace products if it receives notice of such defects during the warranty period. To obtain service, the purchaser must return the hardware to SMC. The postage, shipping, insurance and risk of loss when returning a product to SMC shall remain with the purchaser. SMC will pay for postage, shipping and insurance when returning the repaired product to the purchaser. Repaired products carry the same amount of outstanding warranty as from the original or 90 days, whichever is greater. Any claim under this warranty must include a dated proof of purchase or invoice. If SMC is unable, within a reasonable amount of time, to repair or replace any product; then the purchaser shall be entitled to a refund of the purchase.
This warranty is only valid upon proper use of the product by the purchaser, and does not cover;
Expendable component parts; or damage due to accident, unusual physical, electrical or electromechanical stress, neglect, misuse, failure of electrical power, air-conditioning, humidity control, transportation, operation with media or materials not approved by SMC, or tampering with or altering the product.
SMC makes no other express warranty whether written or oral.

Software Limitations
Any software this manual describes is protected by copyright law. Modifications, unauthorised copying, reverse engineering, decompiling, disassembling, and creative derivative works based upon the software are prohibited.

The remedies printed above are purchasers' sole and exclusive remedies. In no event shall SMC be liable for any direct, indirect, special or consequential damages (including lost profits) whether based on contract, tort or any legal theory.

The disclaimers and limitations shall not affect the statutory rights of consumer transactions in Australia, New Zealand, and the United Kingdom.