

QINETIQ/EMEA/CIT/PUB1902044

BRACER™

Training Module

Version 1.6.0

QinetiQ



QINETIQ

This training material is subject to change without notification.



QINETIQ CONFIDENCE

Structure

- 1 Important Safety Information
- 2 Module 1 – BRACER™ Overview
- 3 Module 2 - Iridium Network Overview
- 4 Module 3 – BRACER™ CES
- 5 Module 4 – BRACER™ Device
- 6 Module 5 – Operating the Device
- 7 **Practical Exercise - Device**
- 8 Module 6 – Part 1 – Command Centre TG
- 9 Module 6 – Part 2 – Command Centre Devices
- 10 **Practical Exercise - Command Centre**
- 11 Module 7 – Key Management System
- 12 **Practical Exercise - Key Management**
- 13 Module 8 – Situational Awareness
- 14 **Practical Exercise – Situational Awareness**



QINETIQ IN CONFIDENCE

QINETIQ/EMEA/CIT/PUB1902044

BRACER™

Important Safety Information



QINETIQ

This training material is subject to change without notification.

BRACER Important Safety Information

- **IMPORTANT:** Please refer to the BRACER PTT User Manual (QINETIQ/18/2745) for a full list of Warnings and Cautions.
- Li-iON Battery, sealed, non replaceable.
- RF Hazard – Safe for body worn use.
- Risk of high Audio Levels for third party ancillaries.
- AC Mains charger.
- Before Air transportation check with airline on regulations for transporting Li-iON Batteries.



QINETIQ

QINETIQ IN CONFIDENCE

QINETIQ/EMEA/CIT/PUB1902044

BRACER™

Module 1

Overview



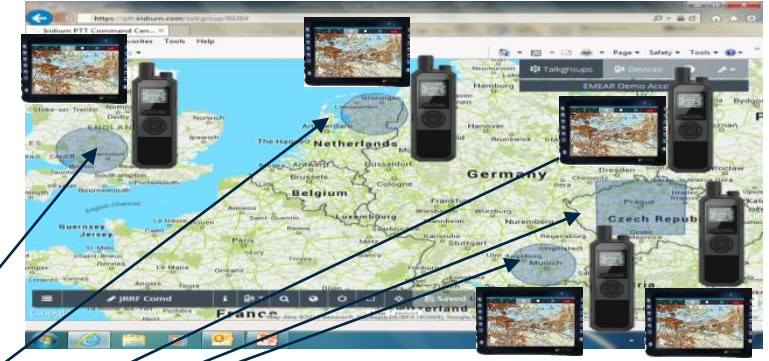
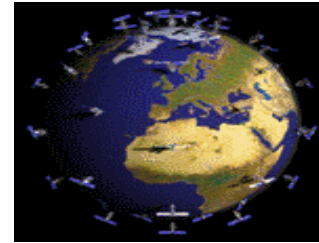
BRACER

QINETIQ

This training material is subject to change without notification.

Bracer™ – End to End secure Push To Talk (PTT) Radio

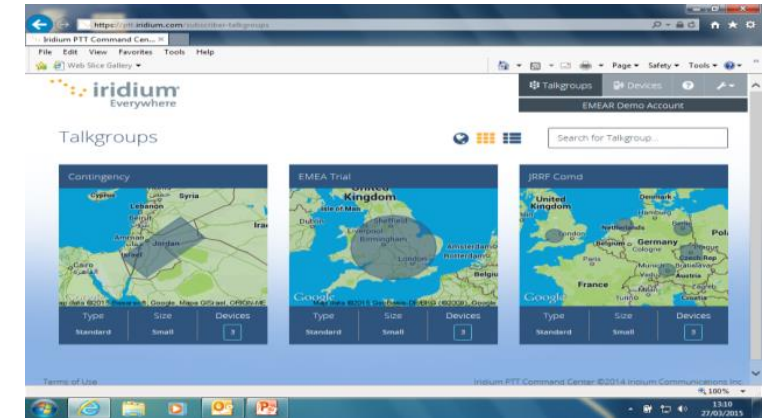
- Zero Infrastructure.
- Frequency Clearance – Cleared in most countries.
- Lightweight, Robust (IP 66 + IP 67).
- Easy to Use.
- Truly Global Coverage.
- Low Latency (0.5 Seconds).
- User Autonomy - Talkgroup Setup (15 per handset).
- Multiple Talkgroup Locations/Priority Talkgroup.
- End to End Encryption (PTT/Situational Awareness).
- Interoperability with 9575 Extreme PTT.
- Low Cost Airtime.
- Emergency Alert.
- Interoperable with many NATO U229 audio Ancillaries.
- Secure Asset Tracking (low latency).



Global Coverage



Bracer®



Command Centre

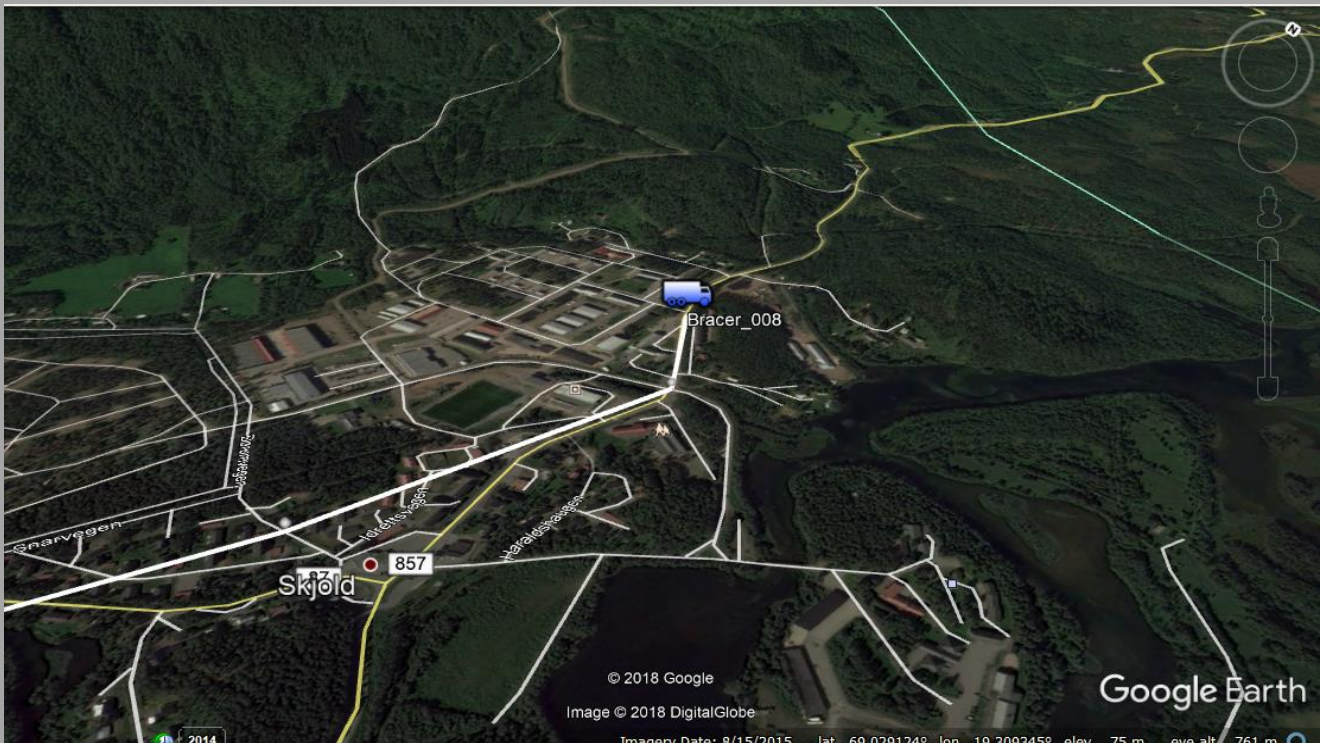
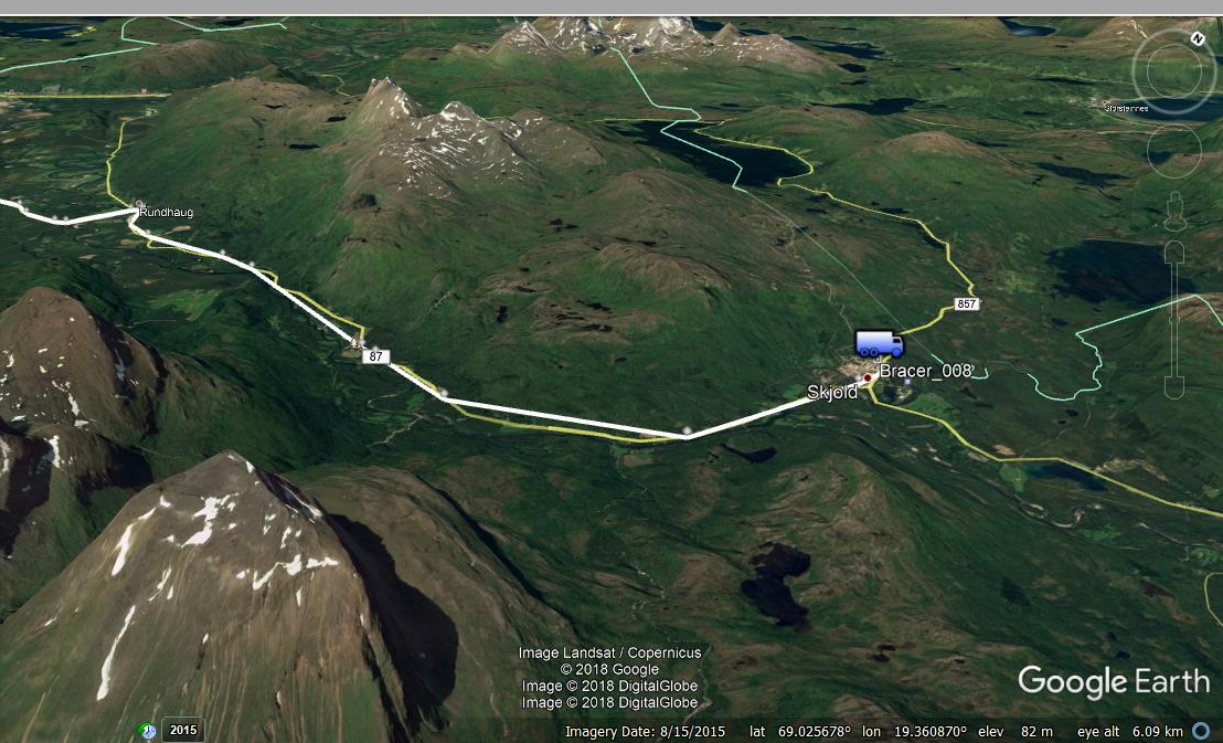
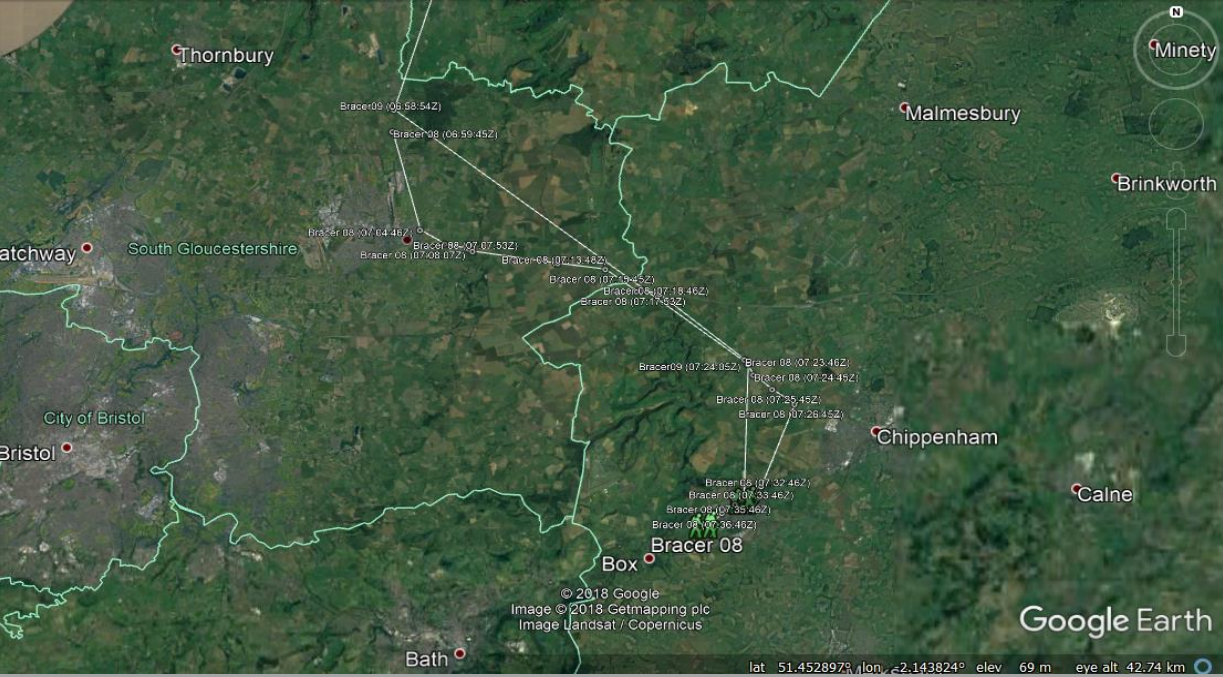


Situational Awareness and PTT Data

- Operational picture in Tactical/Operational/Strategic domains
- Low Latency – 500ms
- Adaptable to most PC/Laptop/Tablet

- Potential Airborne integration (aircrew access to SA picture)
- Commander and User profiles
 - 5 min Epoch
 - Every transmission
 - Commander Request
- Emergency Alert (Audible tone) + Bearing & Dir
- Alert Acknowledge





Bracer® | Buttons

On/Off

PTT

Function Button 1

Soft Keys

Nav Keys

SOS

Volume

Function Button 2



Bracer® | Features

Lanyard Attachment

SMA
(Remote Antenna)

2 x Power / Data
Connectors

LED

SIM Cover



QINETIQ

Bracer Satellite Push To Talk (PTT)

System Overview

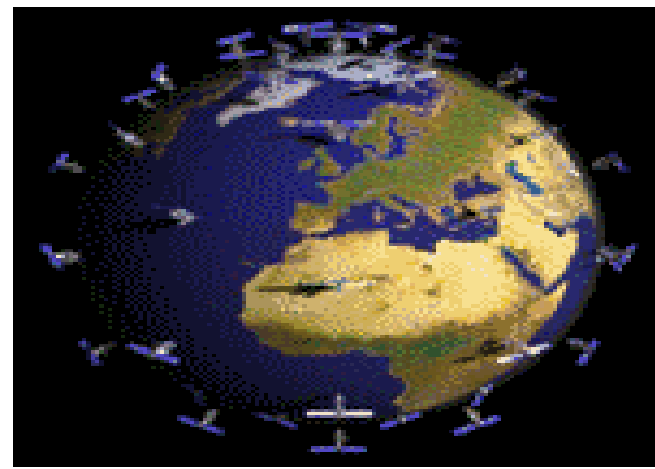


Iridium 9575 PTT

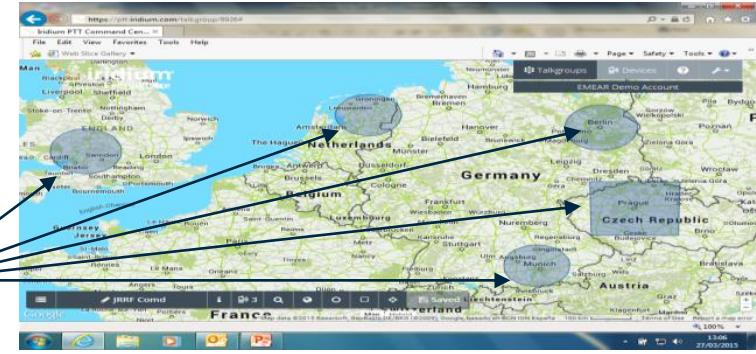
Over the Air
reconfiguration



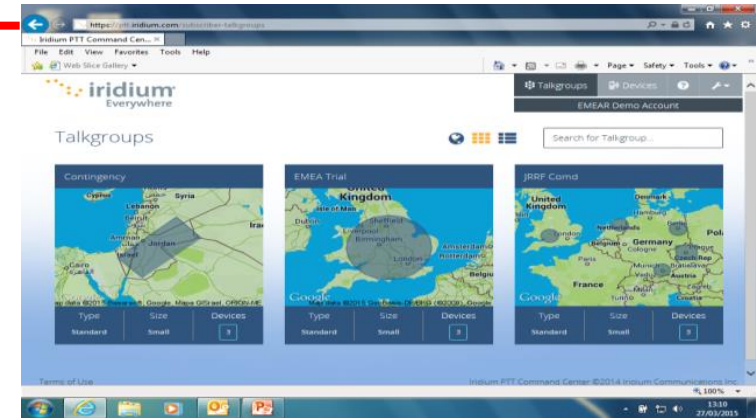
BRACER
(end to end encryption)



Iridium LEO
Satellite
Constellation



Global Coverage



Command Centre



Command Centre Interface Account 'Setting Up the Talkgroups and Devices'

The screenshot displays the Iridium PTT Command Centre web interface. The browser address bar shows the URL <https://ptt.iridium.com/subscriber-talkgroups>. The page title is "Iridium PTT Command Cen...". The interface includes a navigation menu with "Talkgroups" and "Devices" tabs, and a sub-header for "EMEAR Demo Account". The main content area is titled "Talkgroups" and features a search bar labeled "Search for Talkgroup...". Three talkgroup cards are displayed, each with a map and a table of details:

Contingency	EMEA Trial	JRRF Comd
Type	Type	Type
Standard	Standard	Standard
Size	Size	Size
Small	Small	Small
Devices	Devices	Devices
3	3	3



A/CIT/PUB1601270

Talkgroup Area at 100,000 Sq Km Single Area of Coverage

The screenshot displays a web browser window with the URL <https://ptt.iridium.com/talkgroup/10237>. The browser's address bar and menu items (File, Edit, View, Favorites, Tools, Help) are visible. The main content area shows a map of the Middle East and surrounding regions, including Turkey, Syria, Jordan, Israel, Iraq, and Saudi Arabia. A blue shaded area on the map indicates the talkgroup coverage area, which is approximately 100,000 Sq Km. The map includes labels for various cities and countries, such as Istanbul, Ankara, Damascus, and Baghdad. The browser's status bar at the bottom shows the time as 13:01 and the date as 27/03/2015.

BRACER /CIT/PUB1601270

Talkgroup Area at 100,000 Sq Km Divided into 2 x Areas

https://ptt.iridium.com/talkgroup/8926

Iridium PTT Command Cen... x

File Edit View Favorites Tools Help

Web Slice Gallery

Talkgroups

Devices

EMEAR Demo Account

ENGLAND

Netherlands

Belgium

Luxembourg

Germany

Czech Republic

Austria

France

Switzerland

Liechtenstein

BRACER

QinetiQ Proprietary
Unclassified

13:03
27/03/2015

Talkgroup Area at 100,000 Sq Km Divided into 5 x Areas

The screenshot displays a web browser window with the URL <https://ptt.iridium.com/talkgroup/8926#>. The browser's address bar and menu bar are visible at the top. The main content is a map of Europe, with five specific regions highlighted in blue, representing talkgroup areas. These areas are: a circle in the southwest of England; a circle in the northern Netherlands; a circle in the northern part of Germany; a circle in the southern part of Germany; and a rectangle in the western part of the Czech Republic. The map includes labels for various countries and cities. At the bottom of the browser window, there is a status bar with the text "BRACER /CIT/PUB1601270" and a system tray showing the time "13:06" and date "27/03/2015".

Adding Devices to Talkgroups

The screenshot shows a web browser window with the URL <https://ptt.iridium.com/subscriber-devices>. The browser's address bar and menu bar are visible. The page content includes the Iridium logo with the tagline "Everywhere". A navigation bar at the top right contains "Talkgroups" and "Devices" tabs, with "EMEAR Demo Account" displayed below. The main interface is divided into two sections: "Devices 3" and "Talkgroups". The "Devices" section has a sub-header "Drag and drop devices onto talkgroups" and a search box labeled "Search Devices...". It contains three device icons labeled "PTT 1", "PTT 2", and "PTT 3", each with a mobile phone icon. The "Talkgroups" section has tabs for "Talkgroups" and "Templates" and contains three talkgroup icons labeled "Contingency", "EMEA Trial", and "JRRF Comd", each with a network diagram icon.

Example Requirement Areas



CT Tasks



Peace-Keeping



NEO



Intervention



Counter Narcotics



Counter Piracy

Early Entry

Responsive

Global

Small Scale

Interoperability

Enduring



Military Training Safety



Operational Training



Discreet Surveillance



Indigenous Force Comms



Capacity Building

Example Requirement Areas



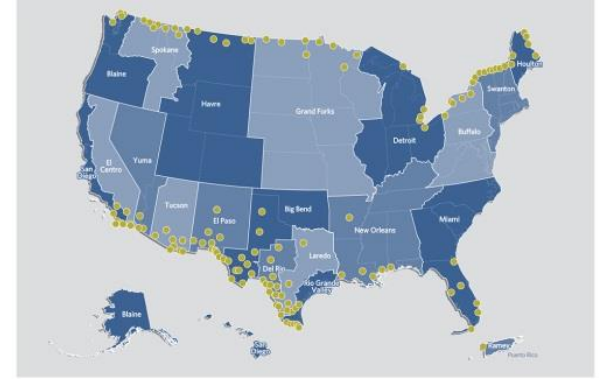
Routine Patrol



Airborne Comms



Immigration Control



Routine Patrol



Counter Narcotics



Maritime Operations



Operational Training



Mobile Platforms



Adaptive

Responsive

Flexible

Small Scale

Interoperability

Mobile

Example Requirement Areas



Disaster Response



Air Operations/Logistics



Maritime Operations



Immediate C2

Early Entry

Responsive



Crisis Coordination

Global

Small Scale



Humanitarian Aid

Interoperability

Enduring



Remote Teams



Remote Locations



Logistics Coord



Aid Coordination



Aid Support

BRACER Security Aspects

- Maximum Commercial approach – Not Crypto or Protective Marking higher than OS at rest
- FIPS 140-2 level 3 –
- User Authentication access – USB Token with Passcode.
 - Black and Red power modes.
 - Zeroise.
 - AES256 Algorithm implementation to FIPS standards.
 - Encryption Key elements.
 - Traffic Key (Time bound, symmetric Symmetric - unique per talkgroup, forward loading / refresh).
 - Key Transfer Key (Unique per handset/KVM pair, USB).
 - Key Encryption Key (Black Key Store, Generated at first logon, unique per handset).
 - Situational Awareness Key (over USB).
 - Keys in Black store when off.
 - Keys in red store when on.
 - Tamper resistance.
 - Tamper evidence.
 - Tamper reaction (zeroise).
 - GPS.

QINETIQ/EMEA/CIT/PUB1902044

BRACER™

Module 2

Iridium PTT Network



QINETIQ

This training material is subject to change without notification.

The Iridium Network

- Low Earth Orbiting (LEO).
- LEO vs Geostationary (UHF, Inmarsat, Thuraya).
- Not constrained by Azimuth (bearing, elevation).
- Low Latency and Global Coverage.
- Good in Built up Areas, mountainous regions and canyons.
- Smaller, lighter end user equipment.
- Tolerates movement up to Mach 2.0.

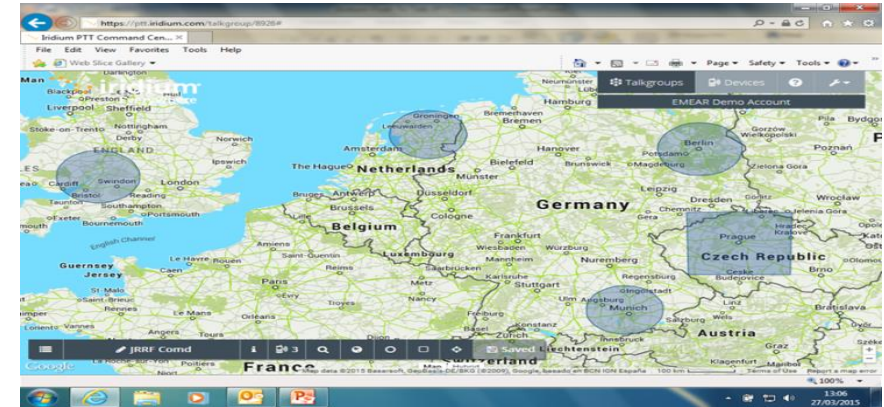


Iridium Satellite Global Coverage Map



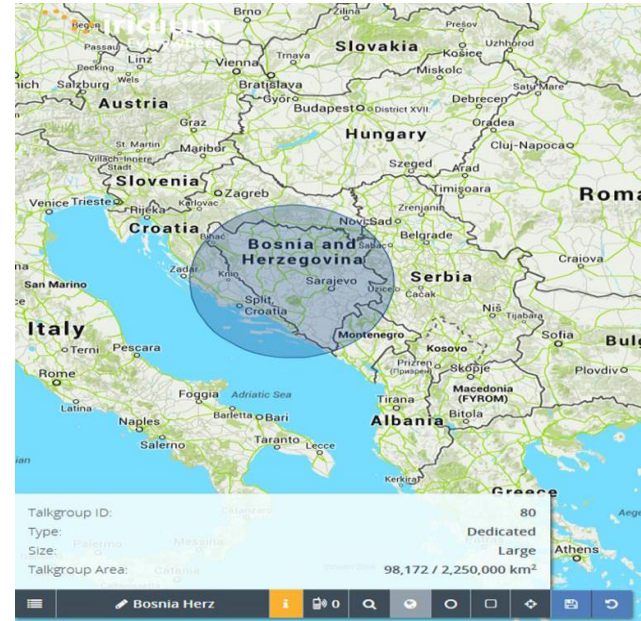
Talkgroups – PTT geographical area coverage

- Geographical area/s enabled for Bracer PTT communications.
- Area set by User Command Centre.
- Areas defined by Circles, Squares or Rectangles.
- Satellite beam covers area on the Earth.
- As satellites move North to South or South to North, beams covering the shapes shift, with leading beams rolling off and trailing beams rolling on to maintain communications.
- Satellite beam coverage is provided with many look angles to accommodate many situations including urban canyons, mountainous regions, etc.

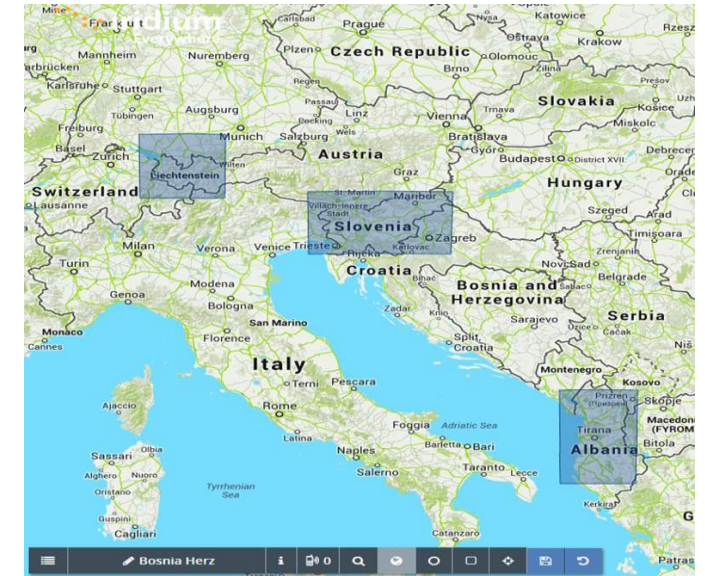


Talkgroup Sizes

- Small – 100,000 km².
- Medium – 300,000 km².
- Large – 750,000 km².
- Extra Large – 1.5M km².
- Jumbo – 2.5M km².



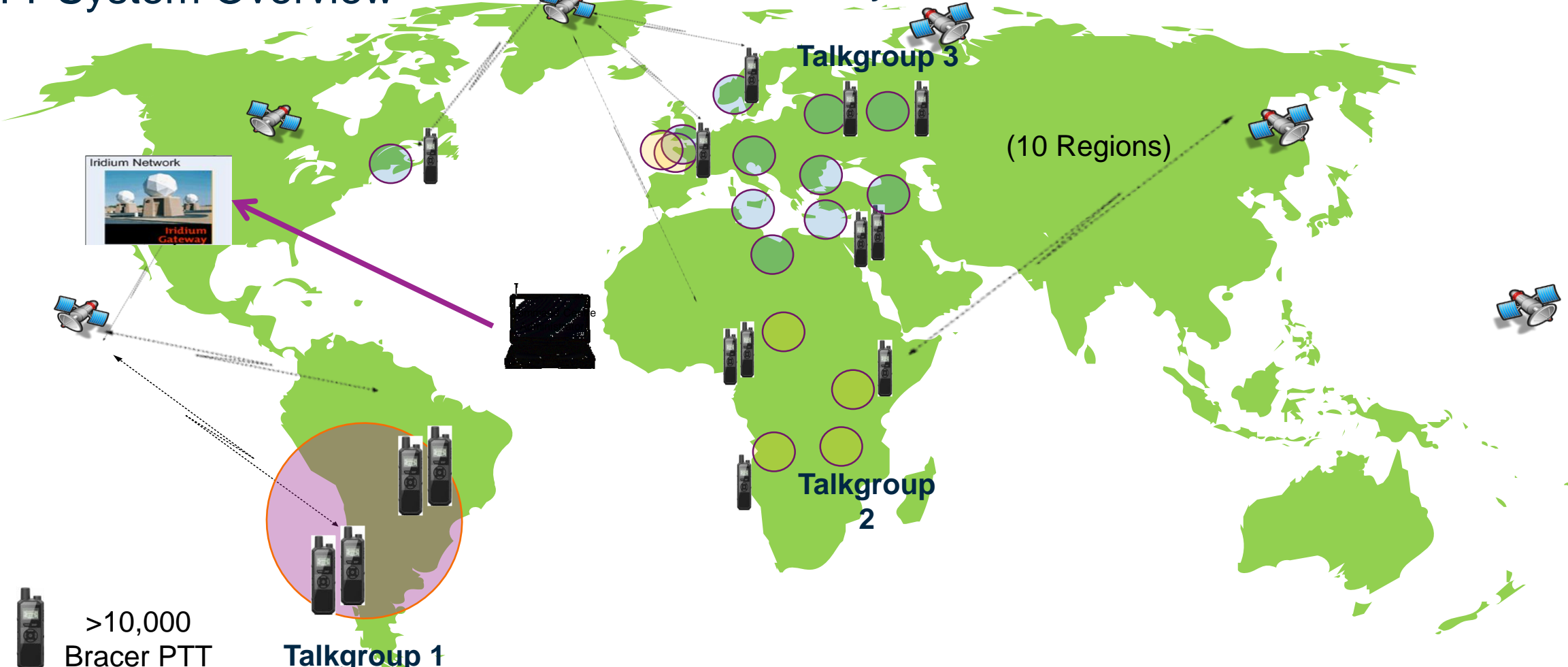
Area of England 130,395 km²



NB - Talkgroup can be a Single Region or broken into up to 10 smaller Regions.

PTT System Overview

Iridium Satellite System



PTT System Overview

GPS Satellites for Position information



Static HQs

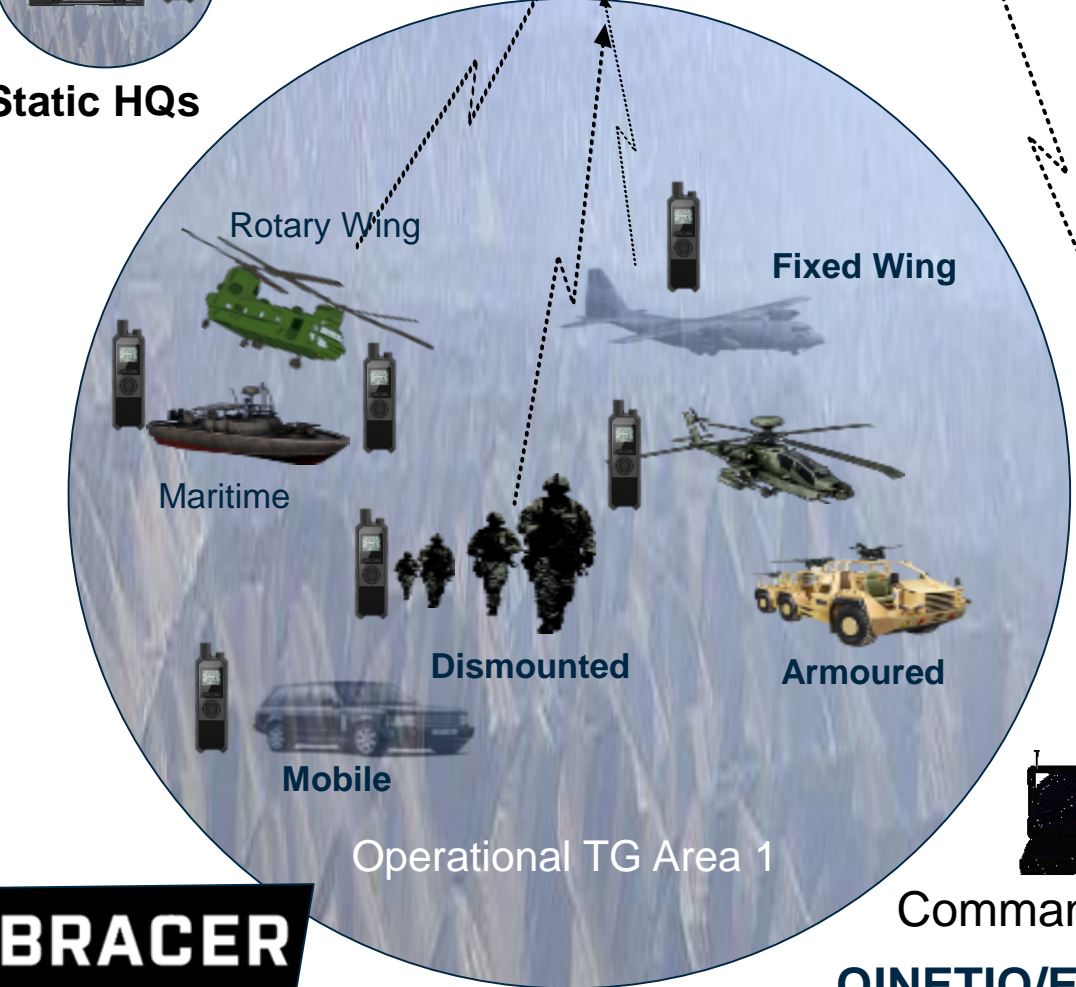
Iridium Satellites for transmission

Iridium SGS
Tempe, Arizona, USA

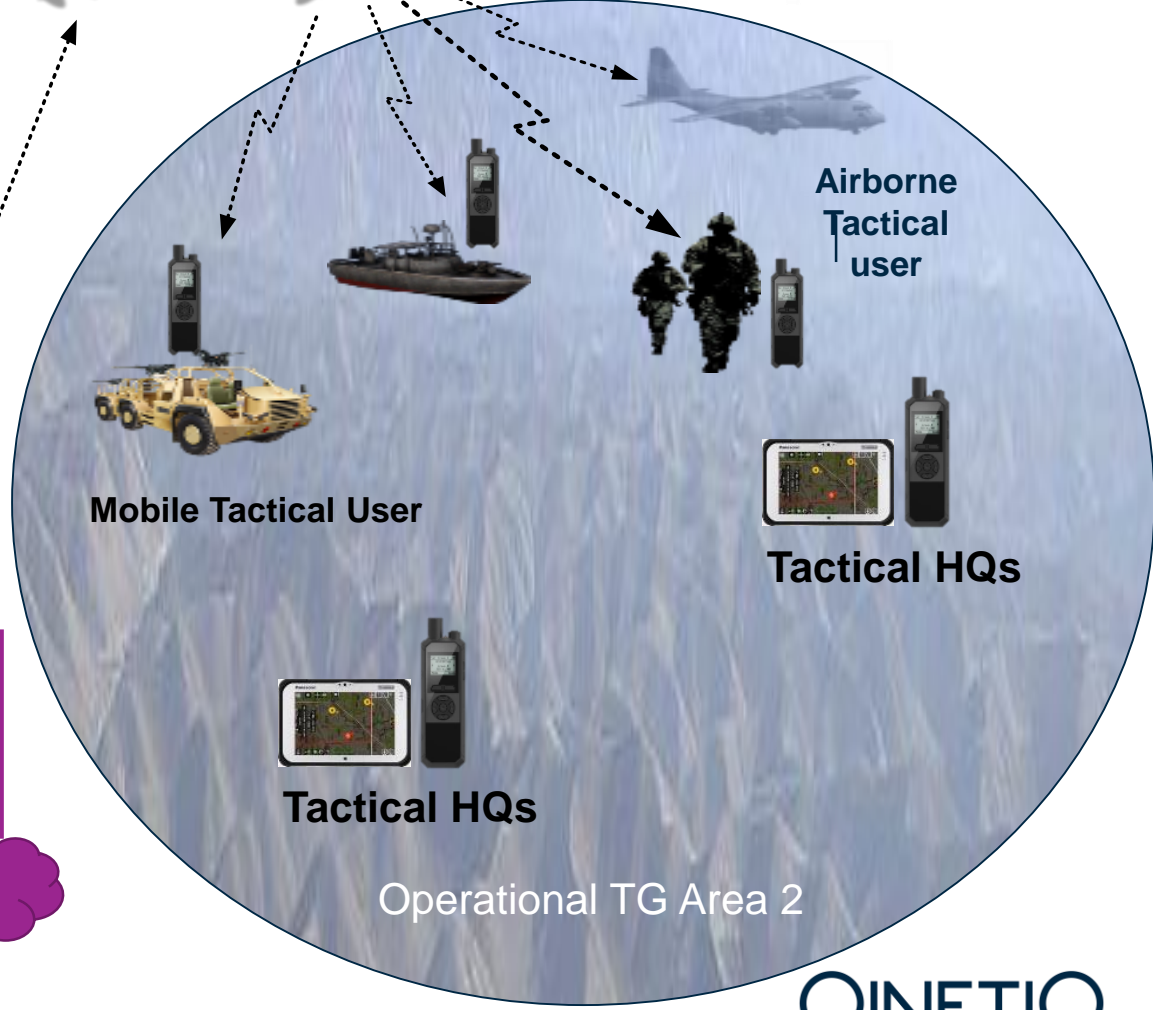


Command Centre

QINETIQ/EMEA/CIT/PUB1902044



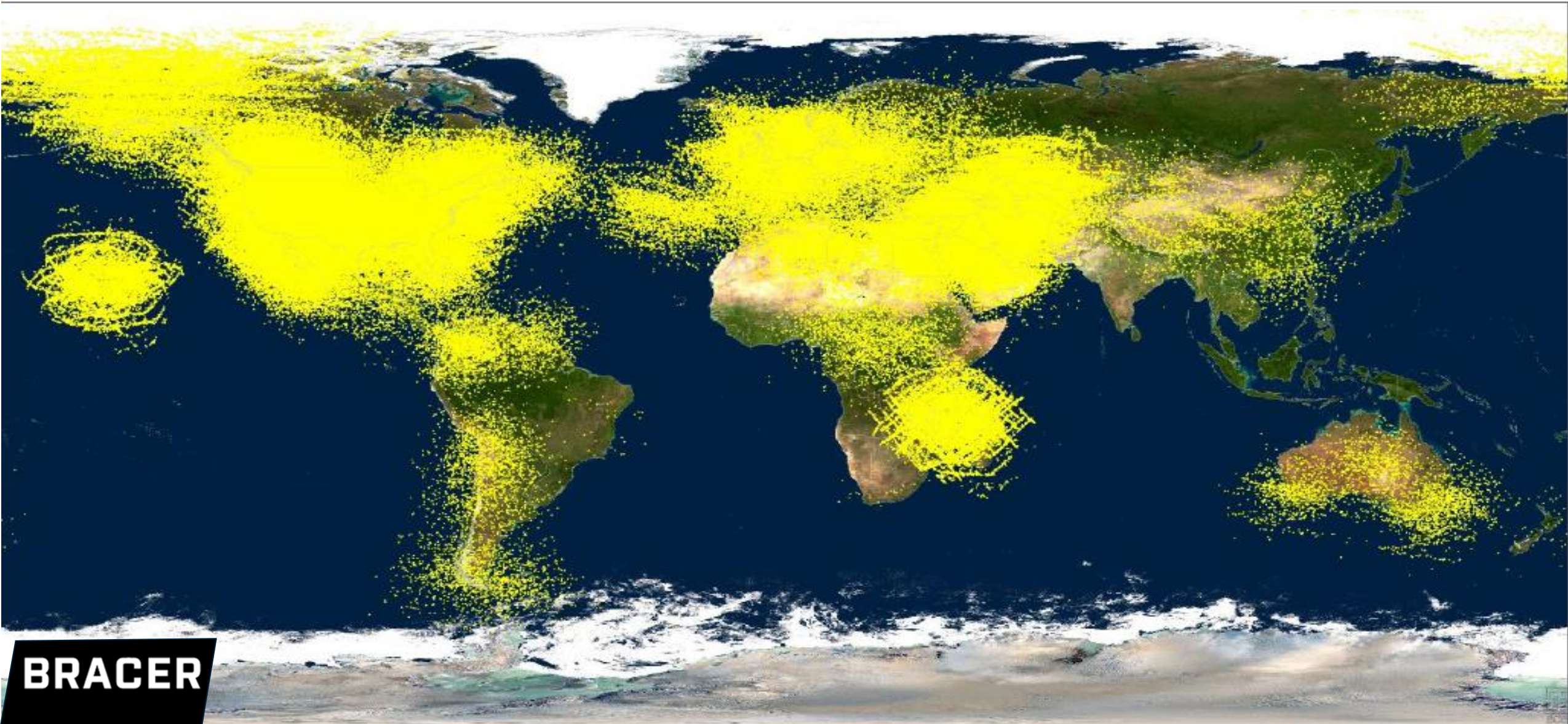
Operational TG Area 1

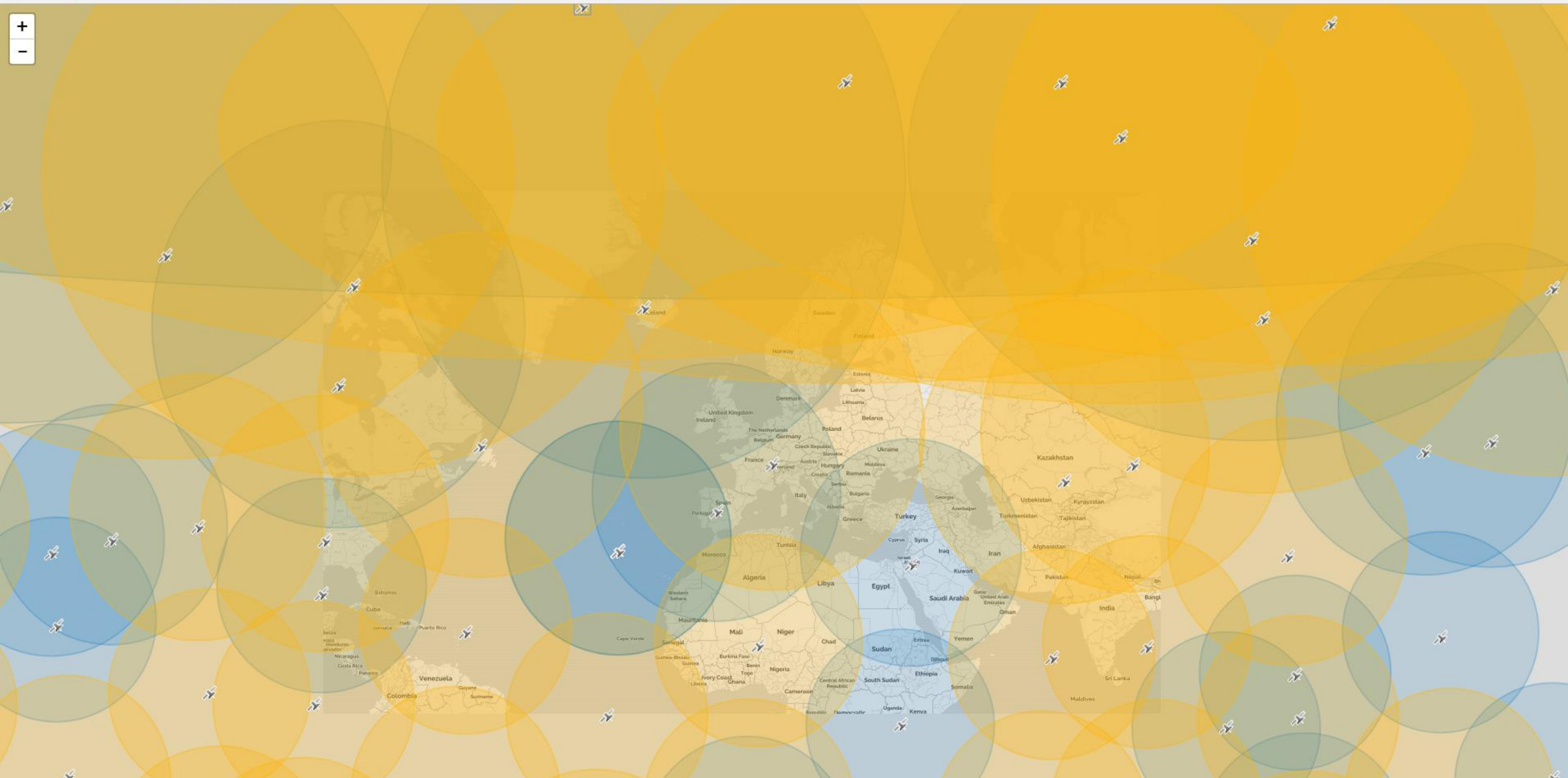


Operational TG Area 2



Iridium Usage Map May-Jun 2018





Questions?

QINETIQ/EMEA/CIT/PUB1902044

BRACER™

Module 3

BRACER CES



QINETIQ

This training material is subject to change without notification.

BRACER

QINETIQ CONFIDENTIAL

BRACER PTT Accessories

1. AC Charger.
2. International Plug Adapter kit.
3. DC Vehicle Charger.
4. DC Charging Adapter Cable.
5. Standard PTT Headset.
6. Mobile Phone Headset Adapter.
7. Military 6 Pin Audio Headset Adapter.
8. External Magnetic Mount Iridium Antenna.
9. External Antenna Adapter Cable.
10. USB Cable.
11. USB Host Cable.
12. USB Key Token.



User Guides

- User guide and Quick Start guide in lid.
- PDF copies available.



Audio Accessories

- D-Hanger Audio headset.
- Mobile Phone Headset adapter.
 - iPhone and Android phone headset compatible
 - PTT Switch in cable.
- U229 – Military Audio MBITR Adapter.
 - For adaption to most existing Military Audio Ancills
 - Requires PTT Switch device.



Current Compatible Audio Ancillaries



H-250 Handset



Speaker Mic



D-Hanger
Earpiece
(included)



Mobile Phone
Handsfree



Peltor
Comtac XPi



Silynx
Optimus &
H4-Ops



Invisio

Battery

- Integral sealed Lithium-ion rechargeable battery – 6.6AH.
- 4 hours for full charge (Quickest Charge cycle in Standby mode).
- Provides 24 hours of use (8:1:1 duty cycle).
- Delivered and transported approximately 30% charged and should be stored in a fully charged state in shipping mode.
- Charge state should be verified every 12 months and the battery recharged if less than 30%.
- **IMPORTANT:** The battery should only be charged in environments between 0°C and 45°C.
- Storage as close to between 10°C – 25°C . It is possible to store between -40°C and +60°C but will impact on cycle life and capacity delivered and discharge time will be reduced.
- If properly stored and maintained, the battery has a shelf life of 5 years.
- The battery is not user replaceable. Contact QinetiQ if the battery needs to be replaced.



Charging Accessories

- AC Charger with International Plug set.
 - 90-250 VAC.
 - 12 Volts DC.
 - UK, US, Aus, Europe adapters.
 - Connect to Power / Data Silver port via adapter.
 - 4 Hours full charge from flat.
- DC Vehicle Charger.
 - 12 Volts DC (Not 24VDC).
 - Connect to Power / Data Silver port via adapter.
 - 4 Hours full charge from flat.
- USB Charging.
 - 5 Volts DC.
 - Any USB available port (500mA max).
 - USB 1, 2 or 3.
 - 10 Hours full charge.



USB Accessories

- USB Device cable.
 - Connecting to PC for Key load etc.
 - Connecting to PC for SA Data Receive.
 - Connecting to any Available USB for charging.

- USB Host cable.
 - Connecting token for Authentication start up.
 - Loading additional Mission keys.

- USB Token.
 - Used for Authentication Start up.
 - Can be used to load additional mission keys.



External Antenna

- USB Device cable.
 - Included Mag-Mount external Antenna.
 - TNC Termination – for use with SMA adapter.
- TNC to SMA Adapter.
 - To allow connection of any Iridium antenna with either SMA or TNC.



BRACER Remote Speaker Mic



Bracer Handset, Remote Speaker Mic, Wireless
Pressel and Peltor Headset



Bracer Handset, Remote Speaker Mic,
Wireless Pressel

BRACER

QINETIQ/EMEA/CIT/PUB1902044

QINETIQ

3.5mm
jack for
earpiece

Mounting
clip /
loop



Peltor
headset
socket



Volume

Centre
PTT
Button /
Speaker

Side PTT
Button

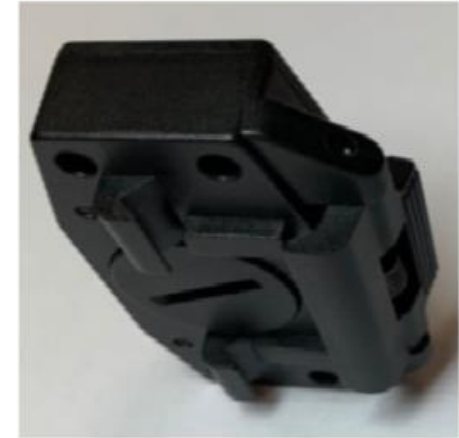
Microphone



Bracer Audio
Connector



BRACER Remote Speaker Mic



Wireless Pressel
Picatinny rail mount



Bracer Multi-Charging Case (MCC) and Multi-Charging Desktop (MCD)

- 16-Way charger
- Carry Case
- MCC comes with storage for 16 Bracer devices and ancillaries (plus a tool roll for decanting ancillaries for tasks)
- Same as MCC, but smaller case and no storage



Multi-Charging Desktop (MCD)



Multi-Charging Case (MCC)



QINETIQ/EMEA/CIT/PUB1902044

BRACER™

Module 4

BRACER PTT Device



QINETIQ

This training material is subject to change without notification.

BRACER

Maintenance

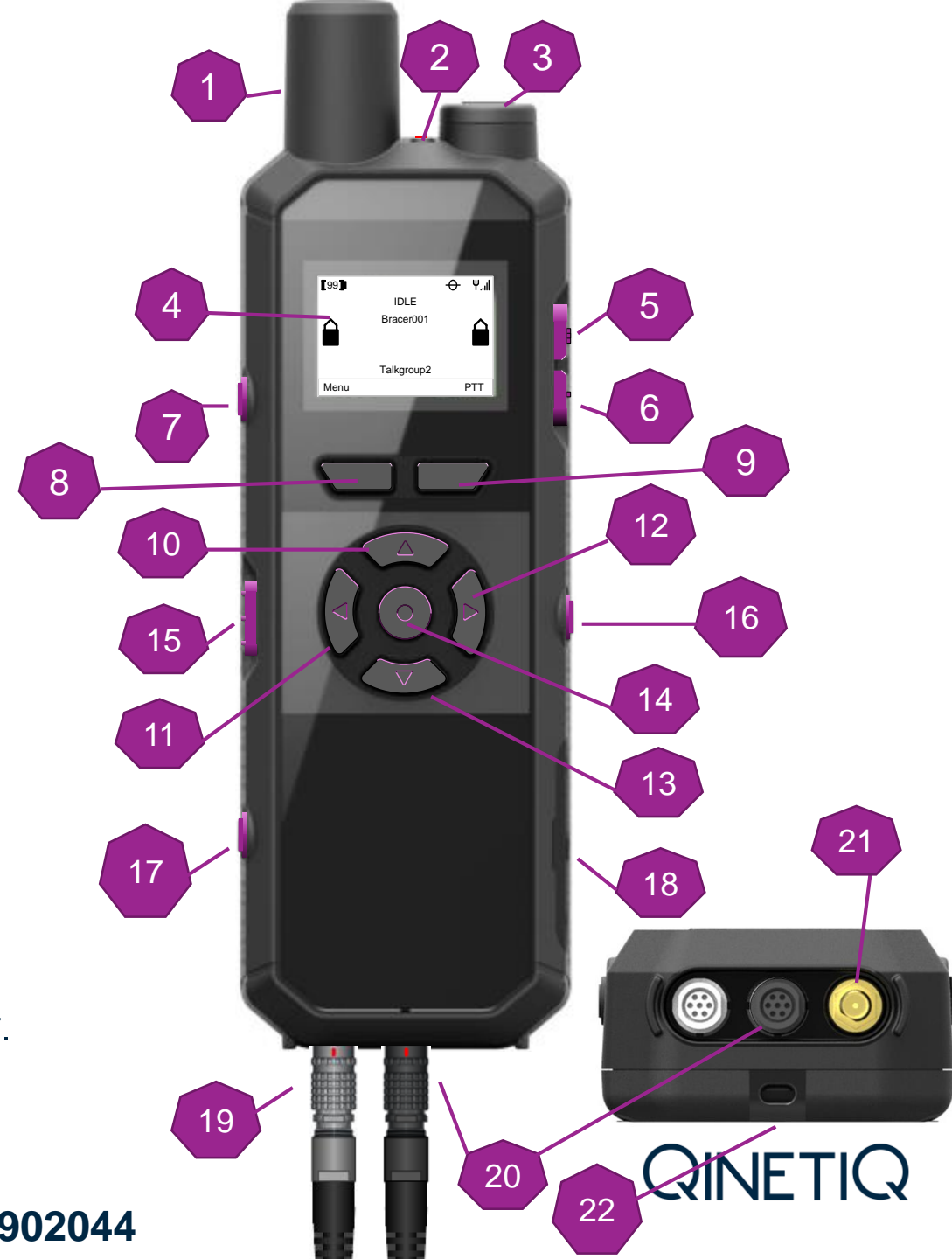
- Keep All ports clean and free from dust/dirt.
- Wash after exposure to salt water.
- **SOS cap and SIM Cover replaceable.**
- **No other User replaceable parts.**
- **Not repairable in the field – 1st to 4th Line repair.**
- **NB – Do not attempt to remove rear plate screws. Device will tamper / Zeroise.**



QINETIQ

BRACER PTT Device

- 1. Antenna.
- 2. LED Indicator.
- 3. SOS button.
- 4. LCD display.
- 5. Volume up button.
- 6. Volume down button.
- 7. Power On/Off button.
- 8. Left soft key.
- 9. Right soft key.
- 10. Up navigation key.
- 11. Left navigation key.
- 12. Right navigation key.
- 13. Down navigation key.
- 14. Centre navigation key.
- 15. PTT button.
- 16. Multi-function button 2 (Waypoint Generator).
- 17. Multi-function button 1.
- 18. SIM card slot.
- 19. Power/USB connector
- 20. Audio/PTT connector.
- 21. External antenna connector.
- 22. Lanyard tether point.



Environmental Specification

- IP66 – High Pressure Jets.
- IP67 – 1 m submersion for 30 minutes.
- Mil STD 810G & Def-Stan 00-35.
 - Drop from 1m onto hard surface.
 - Shock.
 - Vibration (Vehicle, Tracked, & Chinook fixed mount).
 - Air Transportation.
- Temperature.
 - Operating -10°C to +55°C.
 - Battery charging 0°C to +55°C.
 - Storage -40°C to +60°C.



QINETIQ/EMEA/CIT/PUB1902044

BRACER™

Module 5

Operating the Device







QINETIQ

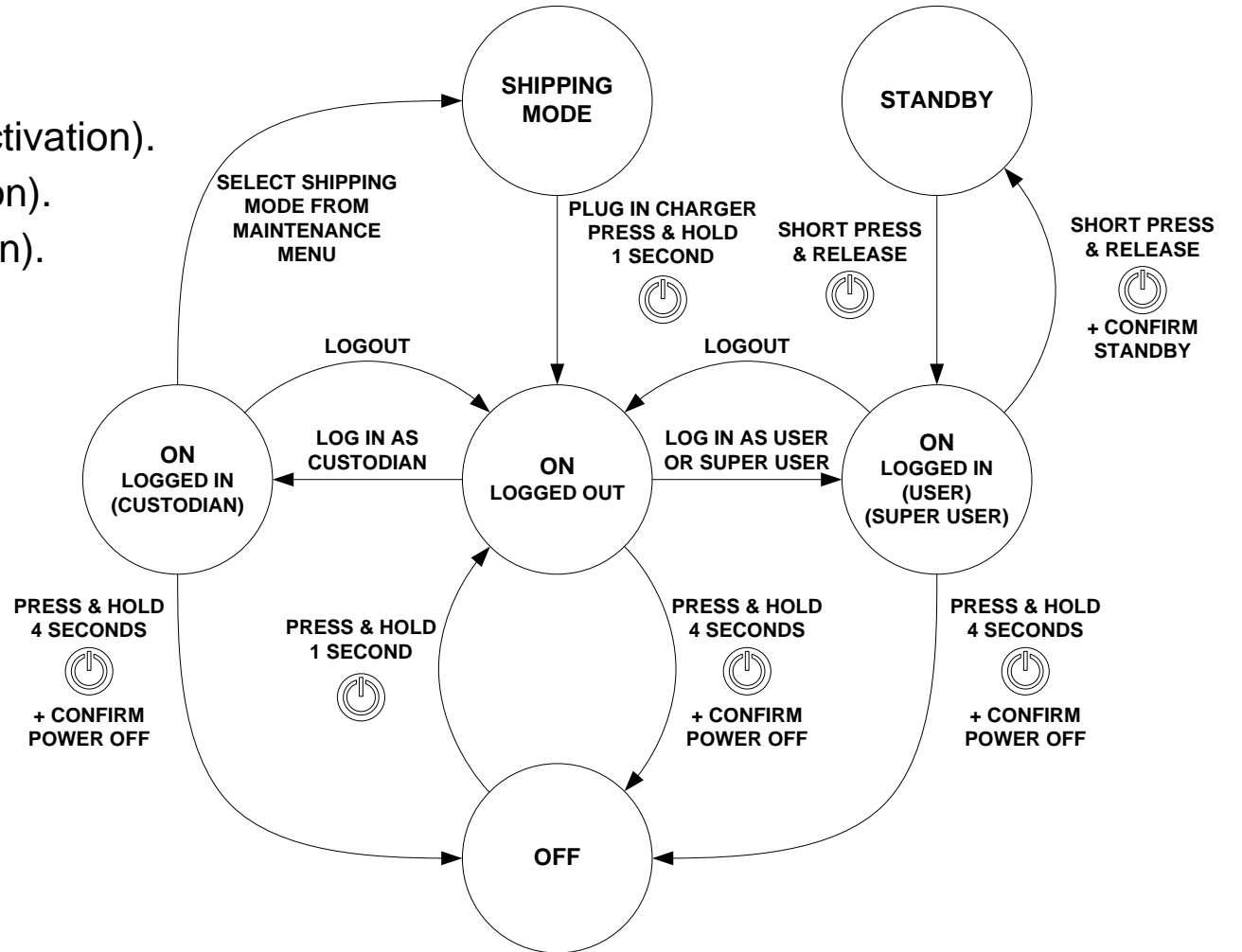
This training material is subject to change without notification.

BRACER

Bracer – Operating the Device



- 4 Power states:
 - Shipping Mode (Requires rekey from USB token on activation).
 - Off Mode (Requires rekey from USB token on activation).
 - Standby Mode (only requires reregistering on activation).
 - On.

Battery Icons	
	Fully Charged
	Partially Charged
	Plugged in – Charging
	Plugged in – Fully Charged



GPS

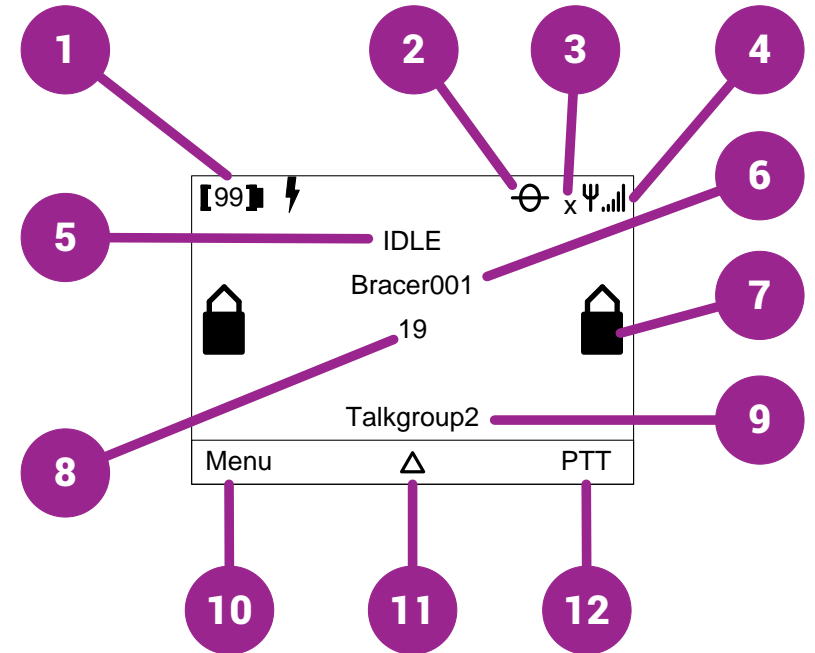
- Bracer is reliant on GPS Fix for Encryption Key AND successful Iridium Comms.
- GPS receiver is embedded in the Handset.
- HQ mode allows for GPS Fix to be stored and timing and fix achieved through internal handset clock. (used for using handset in doors with external antenna).

GPS Status Icons	
	No GPS Lock
	GPS locked
	HQ Mode (use last GPS fix)

Main Display

The following items appear in Bracer™ PTT device display, to provide information about the PTT device's activity.

1	Battery status	7	Secure/Clear status
2	GPS status	8	Talk timer
3	Antenna source	9	Talkgroup name
4	Signal strength	10	Left soft key function
5	PTT status	11	SOS status
6	Device name	12	Right soft key function

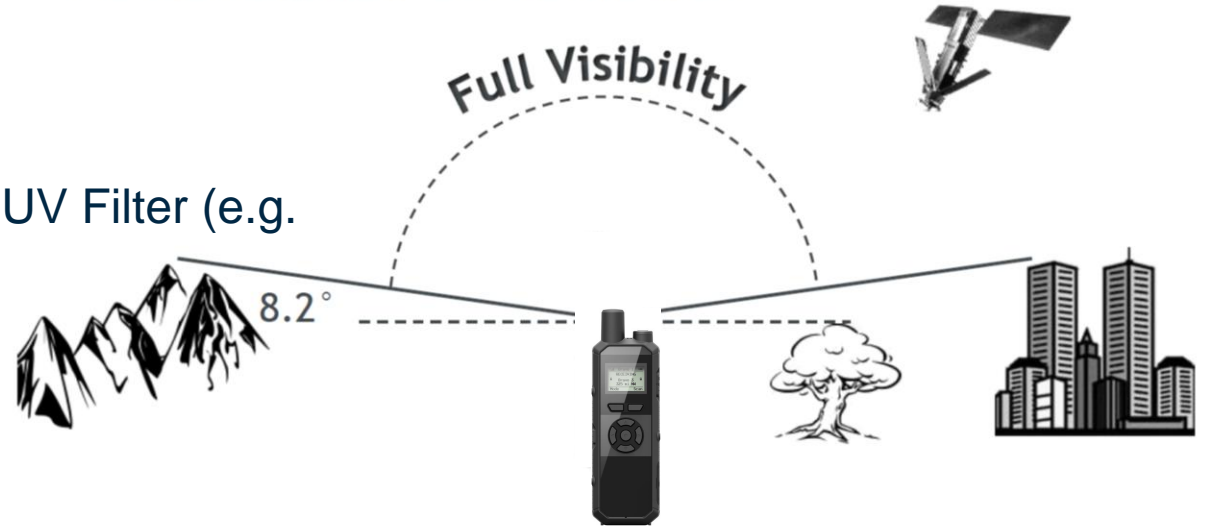


Display Features

Bracer Antenna

- Visibility of the sky is essential.
- Some windows filter Iridium frequency (Double Glazing, UV Filter (e.g. Cars, Hotels)).
- Internal Antenna settings:
 - Low Power – 2W.
 - High Power – 7W (Recommended).
- External Antenna settings (using remote antenna):
 - Low Power – 2W.
 - High Power – 7W (Recommended).
 - Ensure that external antenna is correctly connected to the Bracer port.

Maintaining Network Connection



Antenna Source Icons



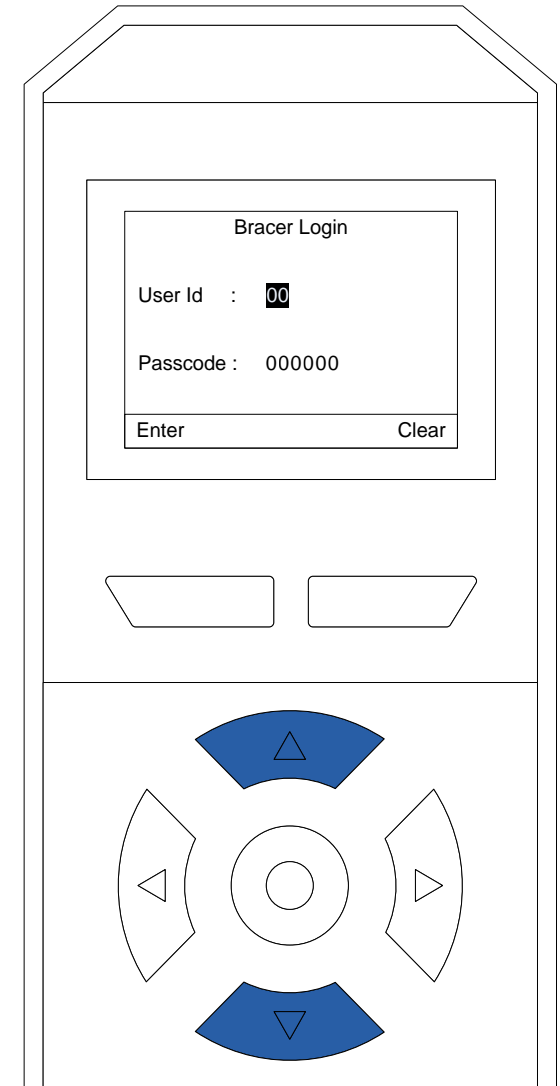
Internal Antenna



External Antenna

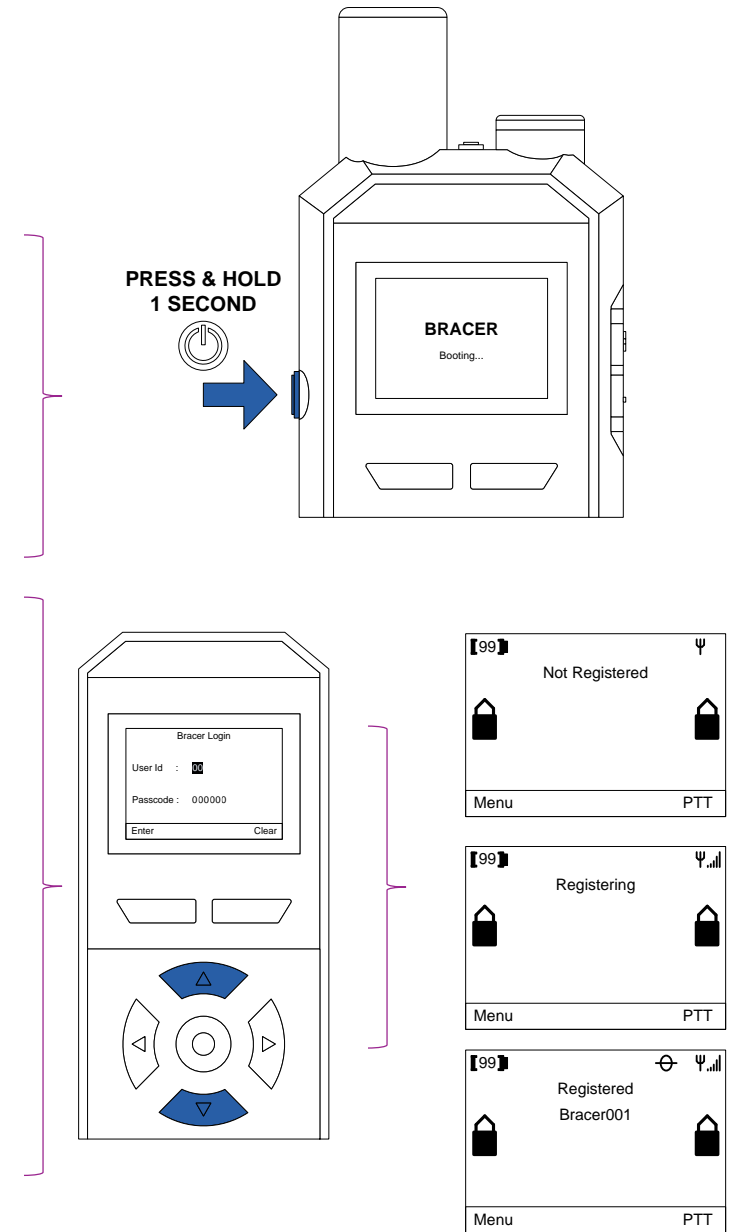
User types

- Bracer™ supports three user types: User; Super User and Custodian.
- **User:** A user has access to all of the PTT functions and the main menu and can view SOS reports.
- **Super User** access to the same Menus and PTT functions as a standard User, but also has some additional situational awareness options to request SA reports, Cancel SOS reports and has the ability to export PLI via USB.
- **Custodian:** a custodian is able to access the maintenance menu which provides the capability to allocate users to the device, to transfer mission keys to the device and to put the device into shipping mode.
- Your Bracer™ PTT device supports up to eight User IDs:
 - 00 – Custodian
 - 01 – Custodian
 - 02 – Super User
 - 03 – Super User
 - 04 – User
 - 05 – User
 - 06 – User
 - 07 – User



Turning on the device

- Connect loaded USB token to the correct Bracer Device (USB port, using Short USB lead).
- Turn on device by holding power button for 1 sec.
- Device will show User ID and passcode. Scroll using navigation keys to set User ID (00-01 Custodian, 02-03 Super User, 04-07 User). Then scroll right.
- Enter dedicated passcode for Bracer device using Navigation keys and press enter - (this must have been preprogrammed – see set up details).
- If incorrect passcode device will remain in login screen (3 attempts attempts). As a code is entered it is obscured by astricks.
- If correct passcode Device will show 'registering' on the screen. Disconnect and store USB token. A signal is required to register and receive GPS fix.
- Device will show 'registered' once registered on the network. Await the GPS fix.
- Select TG via PTT hot key.

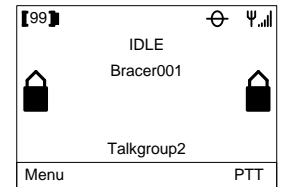
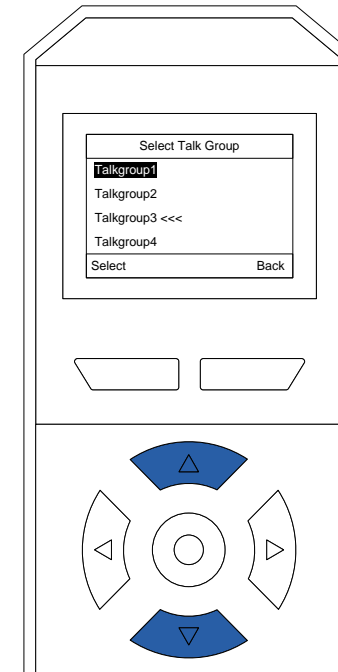
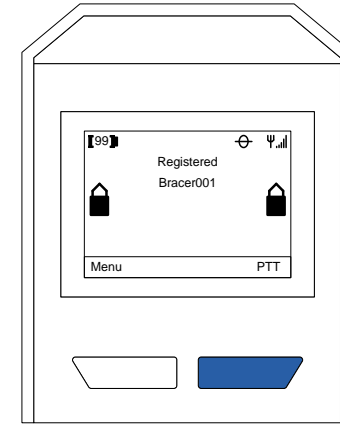


Practical Demonstration / Exercise

1. CES Walk through
2. Startup using token (Users 02 and 04)
3. Screen layout
4. Menu settings (SA, Display settings, PTT Options etc. etc.)
5. Charging
6. Power states
7. User 00 Menu items (inc Shipping mode)

Selecting a TG

- Devices are set up in TGs via the Command Centre.
- Once GPS fix has been received and Device is Registered to the network.
- Press the right soft key to select the PTT menu. A list of talkgroups for which your device is provisioned will be displayed.
- The current monitored talkgroup, if there is one, will be marked with a <<< indicator.
- Secure talkgroups for which keys are loaded on the device are indicated by '(s)' following the talkgroup name.
- If you choose to join a Clear talkgroup, you will be prompted to confirm by pressing the left soft key that you do indeed wish to participate in Clear talkgroup.
- **Note:** If you highlight the current monitored talkgroup from the list (marked with <<<) and press Select, this returns your device to a state where no talkgroup is being monitored.



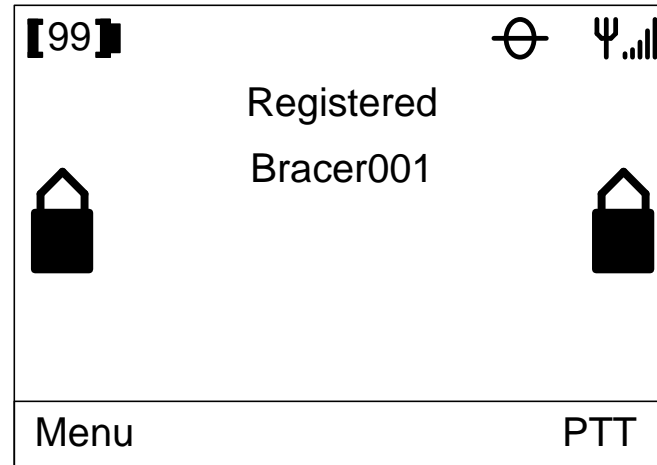
Talkgroup States

When your device is monitoring a talkgroup, the screen will display one of the following four states: IDLE; LISTENING; TALKING or OPEN.

- **Idle** - Device displays IDLE when the monitored talkgroup is not active or satellite coverage is not available.
- **Listening** - Device displays LISTENING when receiving a call. Name of calling station, and distance and direction is shown on screen. Location Unknown is displayed if the system cannot determine the location of the calling ID (i.e. location sharing is switched off).
- **Talking** - The device displays TALKING when you are transmitting (Other participants in the talkgroup will see LISTENING).
- **Floor Pending** – Device can see network but cannot access the floor (e.g. other user transmitting).
- **Open** - When the talkgroup is active, but no one is talking, the screen displays OPEN. This indicates that the floor is available and that participants may request the floor by pressing and holding the PTT button.
- Your device will return to the IDLE state when there has been no activity on the monitored talkgroup for more than 90 seconds.

Secure and In-Secure Talkgroups

- If a selected Talkgroup has a valid mission key, the device will be in a “Secure” mode indicated by two padlocks on the display.



- If a Talkgroup is selected which has no valid mission key, the device switches to Insecure mode and the padlocks are replaced by two exclamation marks.
- Audio Tones for talkgroup entry and exit etc. are different for Secure and In-Secure mode to provide audible indication to user of the security mode of operation.

IRIDIUM® EXTREME PTT 9575



**Bracer is fully
Compatible with the
Iridium® Extreme PTT
handset**

**(BRACER in unencrypted
Talkgroup)**

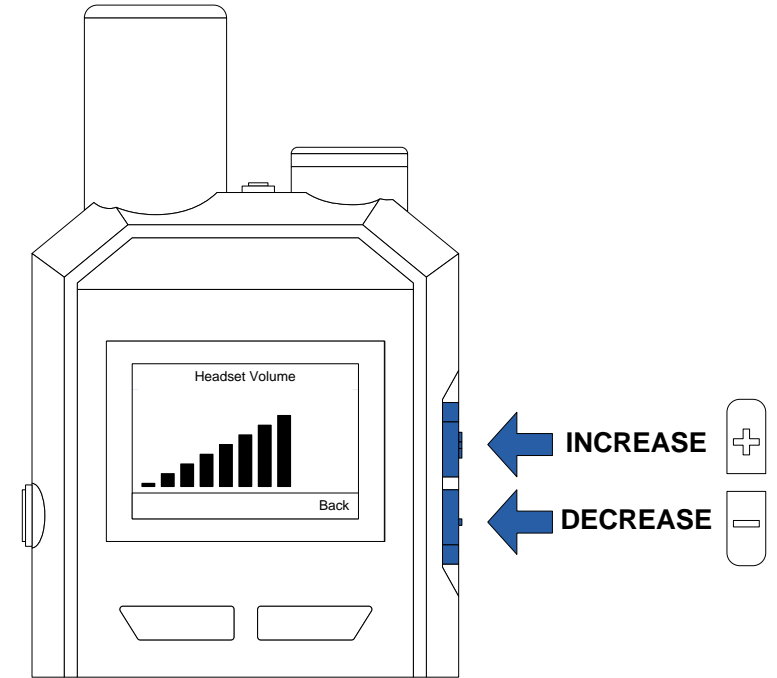
BRACER

QINETIQ/EMEA/CIT/PUB1902044

QINETIQ

Volume Adjustment

- **Adjusting the Headset Volume** - Press the volume up/down buttons on the side of your Bracer™ PTT device. The display will show the current volume level.
- **Warning:** Exposure to loud noise from any source for extended periods of time may affect your hearing. The louder the volume sound level, the less exposure is required to affect your hearing.
- **Firmware Requirement.** Bracer is set up to support a number of audio ancillaries. Adjustments will be required to support new ancillaries to ensure correct volume balancing and specific connector pin out.



Transmitting

- Ensure you have good coverage and view of the sky.
- Press and hold PTT button and wait.
- Tones.
 - 3 x ascending tones - Floor granted.
 - 2 x descending tones – Reject tone, access denied (no network or other user has the floor) - **Wait 2 seconds retry.**
 - 2 x 2 repeated ascending tones – Floor pending – **Wait for 3 x ascending tones then retry.**
 - 2 x descending tones – floor released post transmission.
- User sends message. “Talking” shown on device screen.
- Timeout 40 Seconds – countdown time on screen.
- Release PTT button, releasing the floor – 2 x ascending tones.

BRACER and 9575 Call tones

Secure

Insecure

9575 Extreme

Note: No beep the pressing PTT

call success from idle
then close



call success from open
then close



call rejected



Network Unavailable
(No Signal Strength or Out Of
coverage area)



Floor pending

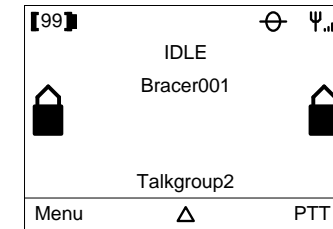
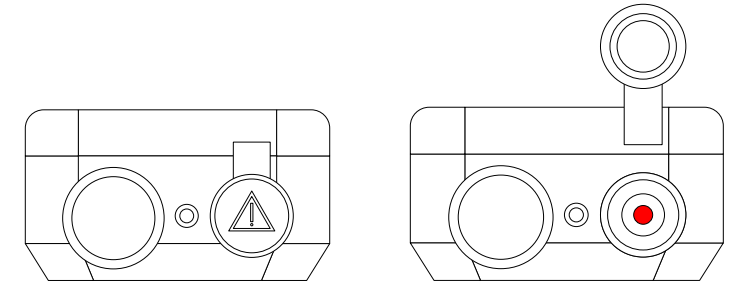


LED Light Indicator

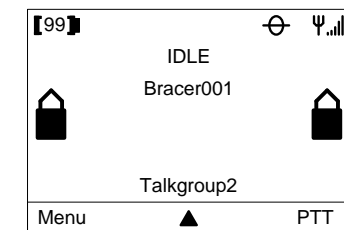
LED Appearance	Indicates
Red – flashing on-off-on	Handset not registered with Iridium Handset not active with Iridium Handset not assigned any talkgroups User Logged in but no talkgroup selected
Red – short flash every 5 seconds	Cryptographic function has failed
Amber – Flashing on-off-on	Clear mode – receiving traffic
Amber – Short flash every 5 seconds	Clear Mode – Talkgroup OPEN or IDLE
Green – Flashing on-off-on	Secure Mode – receiving traffic
Green – Short flash every 5 seconds	Secure Mode – talkgroup OPEN or IDLE
Green – Short flash every 10 seconds	Standby mode
Blue – Flashing on-off-on	SOS activated (this handset)
Blue - Short flash every second	SOS activated (other handset)
Blue – Short flash every 5 seconds	SOS Acknowledged by other user
Magenta – On	Zeroised or Tamper detected
Magenta – Short flash every 2 seconds	Handset Booting
Magenta – Short flash every 5 seconds	Login Mode
White – Short flash every 5 seconds	Maintenance mode

Activating SOS

- Flip open the protective SOS button cover on the top of the handset and press the red button to send an SOS. The SOS function is only available when the handset is participating in a secure talkgroup.
- This will send a message containing your location and a request for assistance to your current talkgroup. The LED indicator on the handset will turn blue and flash on and off. A flashing empty triangle will be displayed on the bottom line of the display.
- The other participants in the talkgroup will hear an SOS tone and the LED indicator on their handsets will flash blue once per second.
- Details of SOS reports received on a handset can be obtained from the Situational Awareness sub menu.
- When the SOS is acknowledged by another participant in the talkgroup, the bottom line of the display will show a flashing filled triangle.
- Clear down SOS by holding red button for >10 Secs.
- **NB – SOS messages have priority over standard PLI and Voice.**



SOS Active



SOS
Acknowledged

Situational Awareness and SOS

- Select Situational Awareness from Sub-Menu. **NB** - A standard user will only be able to see SOS reports and SA Report Distance.
- A Commander or Super User will be able to see; SA Reports, Request SOS Reports, Request SA Reports, Enable PLI Output, Enable SA Storage and SA Report Distance.
- Selecting SOS reports allows you to view details of received SOS reports.
- The right soft key (Clear) can be pressed to clear the report and return to the main display. However, the SOS display will reappear when the next report is received.
- There is an option for the user to set a specific distance where a PLI message will be triggered by the handset. This is the distance from the last PLI report. It can be set at 500, 1000 or 2000 **NB** – Faster moving platforms should use 1000m or 2000m reporting.

Situational Awareness	
SOS Reports	
Select	Back

Situational Awareness	
Request SA Reports	
Enable SA Storage	
View SOS Reports	
View SA reports	
Select	Back

Request SA Reports	
SA Report requested	
Disabled	
5 minutes	
10 minutes	
Select	Back

SOS Reports	
Bracer001	
Bracer002	
Details	Back

SOS – Active	
Bracer001	
120m E	
7m 53s	
9m 58s	
Options	Clear

SA Report Distance	
Disabled <<<	
500m	
1000m	
2000m	
Select	Back

Viewing SA Report

- Situational Awareness Reports from Bracer devices can be received by Super User (Commander) handsets.
- PLI can be disabled or enabled at different epochs i.e. 5, 10, mins.
- PLI will be sent from a handset on transmission and epoch.
- Selecting Request SA Reports allows a Super User to request other handsets in the talkgroup to send SA reports immediately, or at defined intervals.
- Request now option expedites reports from users.
- Enable PLI Storage (Super User only) Options.
- **NB – Consideration when setting up HQ device (enabling PLI and location sharing!).**

SA Reports	
Bracer001	
Bracer002	
Details	Back

SA Details	
Name: Bracer001	
Latest Location:	
Time: 11:12:48	
Refresh	Back

Several Pages of Information

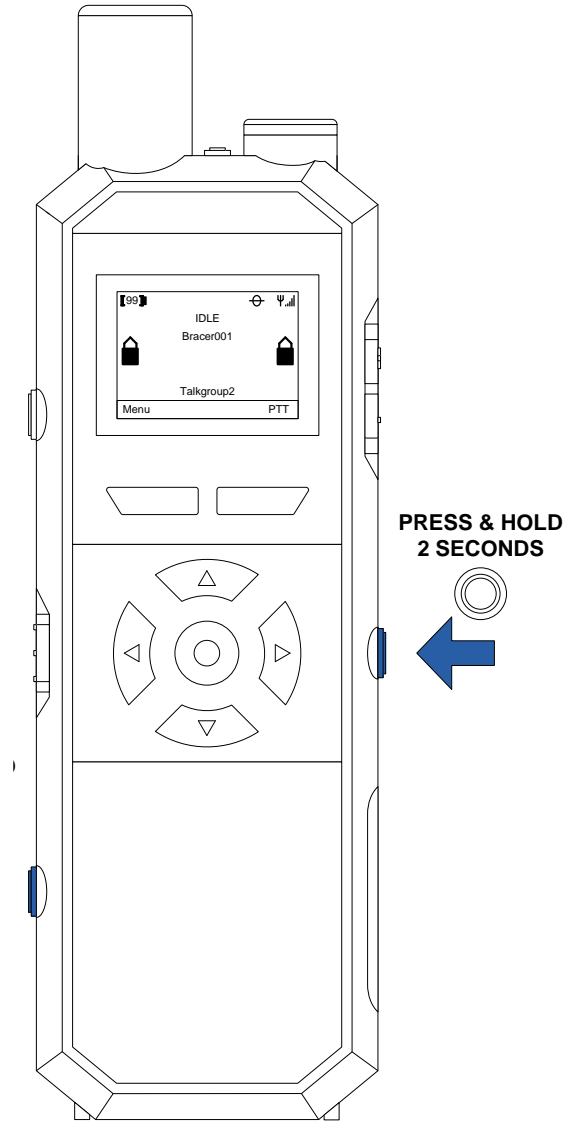
Request SA Reports	
Request Now	
Disabled <<<	
5 minutes	
10 minutes	
Select	Back

(5,10,30,1hr, 2hr options)

Request SA Reports	
SA Report requested	
Disabled	
5 minutes	
10 minutes	
Select	Back

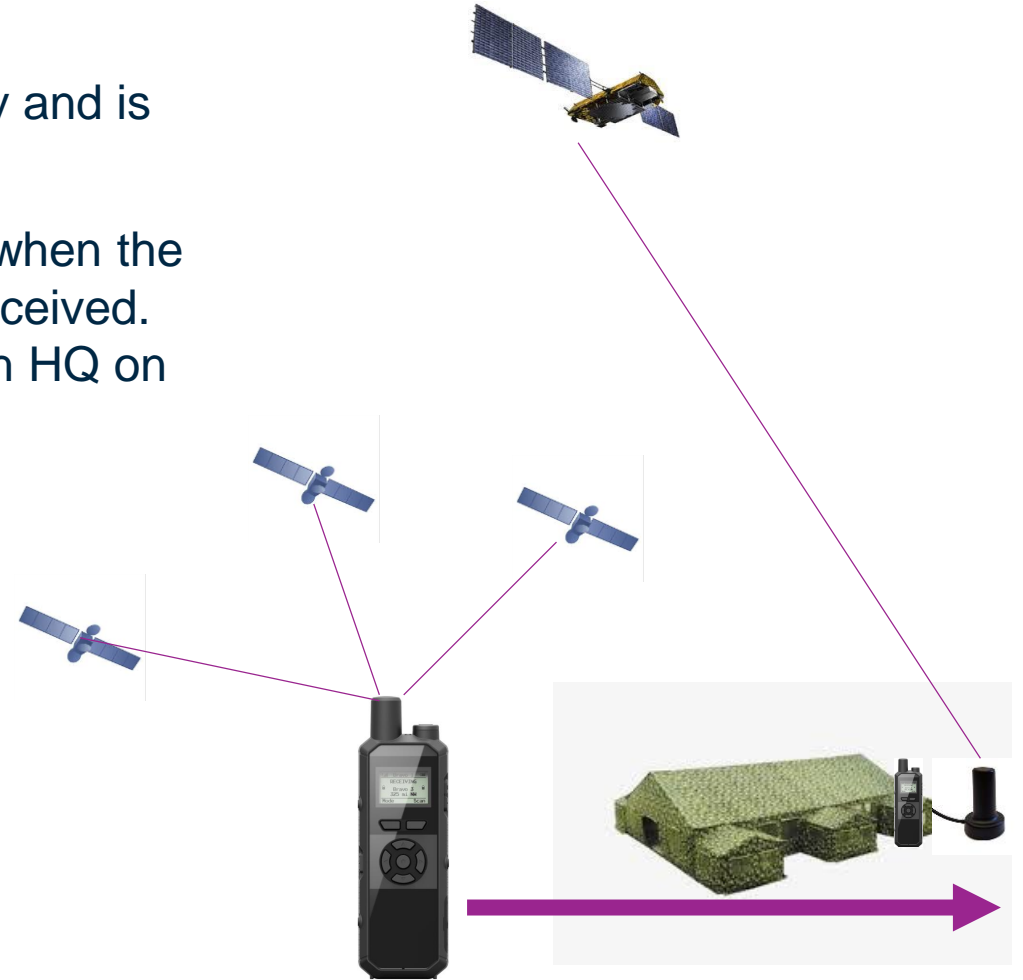
Send Position Feature

- Users can send their position report by pressing and holding the 'Function 2' button for 2 seconds.
- This allows for a position report to be generated from the handset and broadcast to the Talkgroup without making a voice call.
- Once a position report has been generated it will transmit immediately or store and transmit once the handset is in coverage.
- A message will appear in the screen to confirm that the message has been generated.



HQ Mode

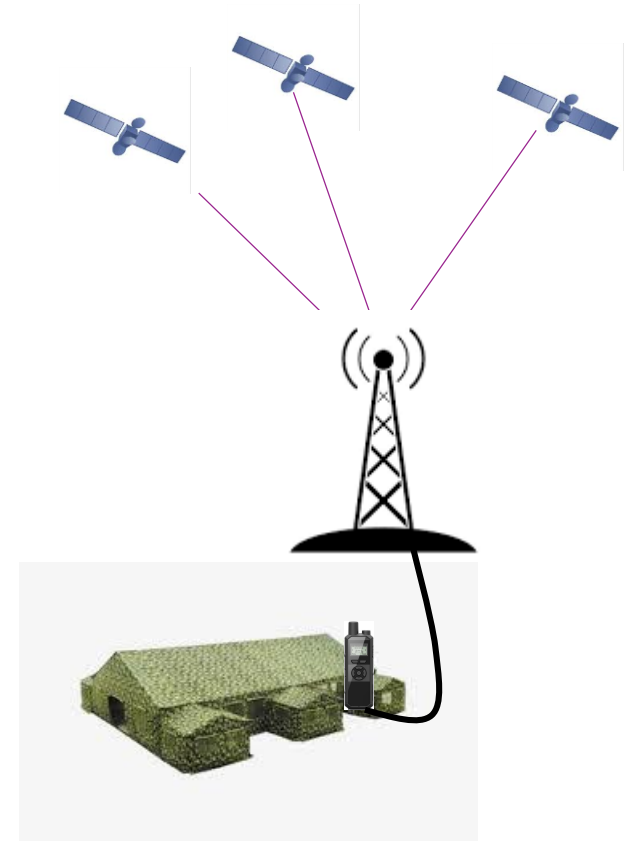
- Used when using Bracer in a location where it cannot see the sky and is using an external antenna (fixed locations i.e. buildings).
- HQ mode allows the handset to continue to use the last GPS fix when the handset is taken into a location where a GPS signal cannot be received. When HQ mode is enabled, the GPS lock symbol is replaced with HQ on the display.
- GPS required for key timing.
- Go outside and get GPS Fix. Once complete;
 - Switch to HQ mode (PTT Options menu),
 - Enable HQ mode once GPS fix has been received,
 - Enable external antenna port for power setting desired,
 - Fix external antenna.
- In HQ mode the device will continue to listen for GPS
- Bracer timing has a slippage of approx 500ms per month. It is highly recommended that a device in HQ mode, in a position that cannot receive GPS is placed outside once a month for 10 mins to refresh GPS timing.



HQ Mode

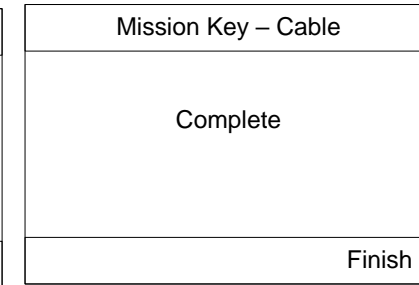
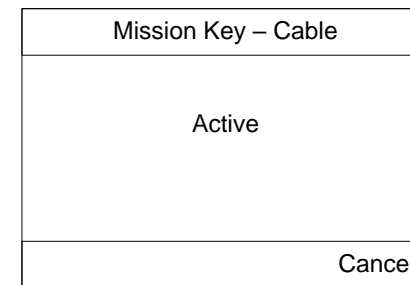
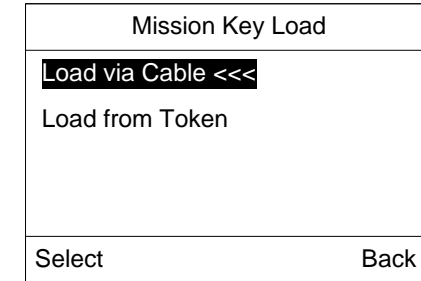
Importance of the static HQ Antenna

- The HQ antenna set up is the most important site.
- Mobile uses can adjust location quickly. Static HQ sites cannot.
- Antenna should be placed to give 180° view of the sky. Where possible antennas should be sited at the highest point. This enables more seamless communications on satellite handover (less obstructions, better communications).
- As the system is only 7W at peak, low loss coax (e.g. LMR 400) for any lengthy lays should be used and this should not exceed 25m (it will work beyond this length but is subject to inefficiencies).
- Where possible the most efficient Iridium antenna should be selected for static HQ sites.
- Beyond 25m – RF over fibre options should be considered (remoting up to 2km).



Mission Key Loading

- Allows a user or super user to load mission keys. Mission keys are required for secure communications on a talkgroup and for secure transmission of Position Location Information to support the Situational Awareness function. Keys can be loaded over a USB cable or from a USB token.
- **Load via Cable** - Your device will display the Mission Key – Cable menu, and will indicate that it is active.
- Connect the supplied USB data cable to your Bracer™ handset and connect the other end to a PC running the Bracer™ Key Management software. The software will authenticate the handset, and allow a custodian to select and transfer mission keys.
- **Load via USB Token** - Connect the supplied USB host cable to the handset, and then connect a USB token which has been pre-loaded with the required mission keys using the Bracer™ Key Management software. This provides a convenient way to transfer a common set of keys to several handsets.



Disable/Enable Mission Key

- When a key is generated for a TG, Bracer will default to use an end to end encryption key when operating in the TG.
- It is possible to disable the end to end encryption by selecting 'disable Mission Key' from the PTT Options menu.
- When disabled the Bracer radio will work as a standard Iridium PTT device (at reduced security and will not have Situational Awareness functionality). The radio tones differ from that in secure mode.
- This function could be used for interoperability with Iridium 9575 handsets in the same TG. Although it is advised that Iridium 9575 and Bracer (in fully secure mode) should operate on separate talkgroups as the differing types of handsets cannot hear each other when Bracer is working in fully secure mode.



Deleting Mission Keys

- When loading Mission Keys onto Bracer it will not overwrite previous keys which can lead to degraded communications. **Before loading new keys into Bracer it is essential that the previous TG keys are deleted.** This is achieved by:
- In the main menu – Select Delete Mission Keys. The keys can be deleted TG by TG or delete all TG Mission Keys. TGs will be shown by the Iridium ID or if the device is registered will show by the description given in the Iridium Command Centre. A confirmation message will appear in screen. Continue if you wish to erase.
- Keys will need to be reloaded from the Bracer Key Management software.
- If the function 1 and function 2 button are pressed and held, simultaneously for more than 2 seconds it will give an option in the main screen to delete mission keys. This is a quick way to access the delete mission key menu.

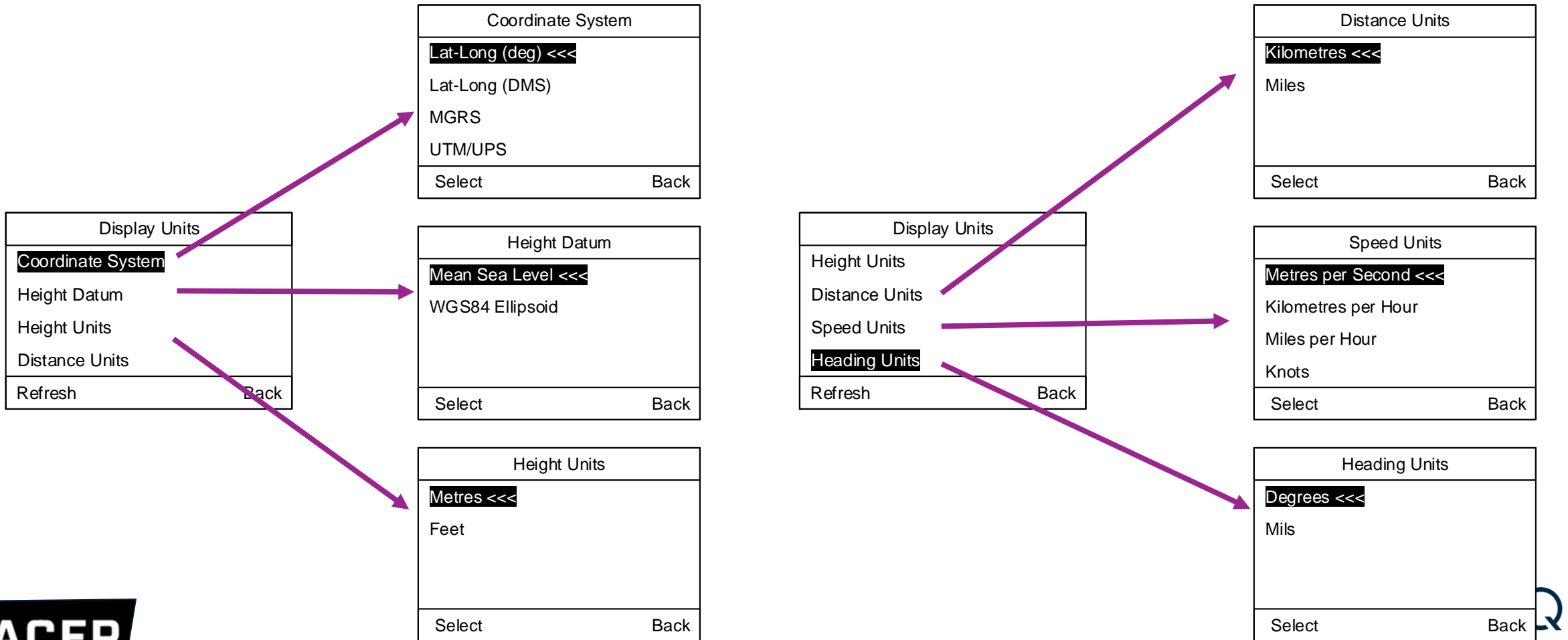
Mission Key Delete	
Delete All	
12345	
67890	
13579	
Select	Back

Mission Key Delete	
Delete All	
Talkgroup1	
Talkgroup2	
Talkgroup3	
Select	Back

Mission Key Delete	
Erase keys for ALL Talkgroups from this device?	
Continue	Cancel

Display Units

- In PTT Options Menu the user can change the display units to meet specific needs. Options are as follows:



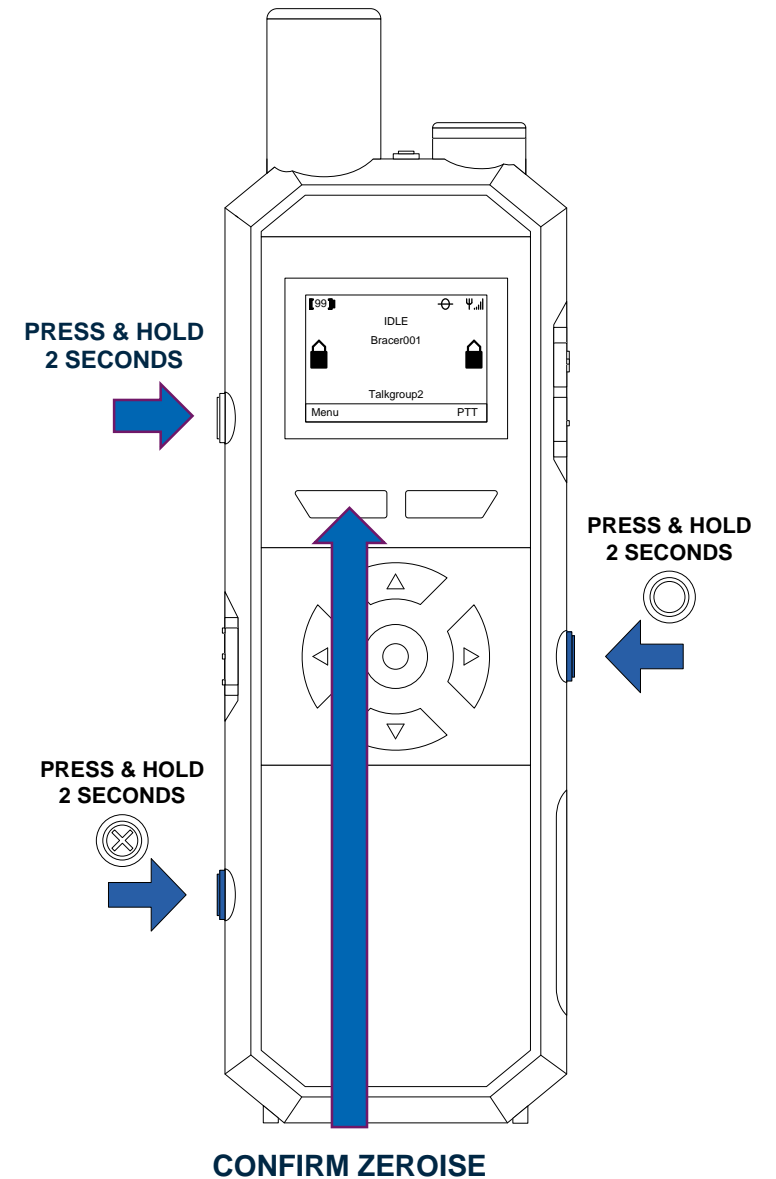
Enabling and Disabling Login Token

- The user can enable or disable the use of the physical USB token as part of the login process to the handset.
- To adjust this setting the user must be in a Custodian Account (00) and select Login Mode on the menu. From here they can select 'Token and PIN or PIN Only. If PIN only is selected only the Login code will be required at boot up until the setting is changed.
- Assessment of whether they physical token is required will be driven by the user and the threat environment they are operating in.
- The physical token is an additional layer of security which is above the FIPS 140-2 Level 3 requirement and therefore does not impact on the actual security or encryption of the system, only the login process.

Login Mode	
Token and PIN <<<	
PIN Only	
Select	Back

Purge/Zeroising the device

- **Action** - All users and encryption keys can be removed from the device by simultaneously pressing and holding multi-function button 1, multi-function button 2 and power off button for two seconds. A confirmation message will be shown in the screen. Select confirm to zeroise
- **NB** - When a zeroised device is powered on, only user ID 00 will be available. A custodian must log-in and configure the device before it can be used again.
- **Crypto Error** - If an error is detected in the crypto module when in secure mode, a message is displayed to notify the user. The LED will flash red once every 5 seconds. The device will then zeroise and shut down. Handset recovery will require reconfiguration by a custodian.



QINETIQ/EMEA/CIT/PUB1902044

BRACER™

Module 5

Bracer Speaker Mic and
Wireless Pressel



QINETIQ

This training material is subject to change without notification.

Bracer Speaker Mic

The Sonic Communications Tactical Remote Speaker Microphone Kit allows the user to remotely operate a connected two-way radio from a body-mounted interface.

- The unit is designed as an interface which houses dual Push-to-transmit (PTT) buttons and connectivity for a tactical headset. There is also a provision to connect an additional remote earpiece.
- The Wireless In-Line PTT (with rail mount) gives the operator easy access to the Push-To-Transmit (PTT) button which is designed to be worn on the chest area, easy for operators to use in fast-paced combat situations.



Bracer Speaker Mic

- Audio Toggle (button below PTT button) - Allows the user to switch the loudspeaker On/Off. Press and hold the Audio Toggle for 3 seconds.
- Headset Socket - This can be used to attach a headset/helmet to the device. When connected, receive audio will be diverted to this path from the loudspeaker. Audio Toggle will still function in this mode.
- Earphone Jack - This can be used to attach earphones to the device. When connected, receive audio will be diverted to this path from the loudspeaker. Audio Toggle will not function in this mode.
- Push-To-Transmit (PTT) - Press and hold the PTT to transmit. Release the button to end the transmission. The LED will illuminate RED during transmissions.
- Vol +/- The buttons can be used to adjust the receive volume.



BRACER Remote Speaker Mic



BRACER

QINETIQ

QINETIQ

Bracer Speaker Mic – Pairing the Wireless Pressel

Setting up the Wireless Pressel

- Connect a headset to the RSM, and this to the radio. The radio should be powered OFF.
- Press and hold the Wireless PTT button. The LED will illuminate RED.
- Switch on the radio. After a few moments the LED will rapidly flash. Release the PTT to pair the devices. The LED will flash 3 times to confirm the pairing.
- The LED will pulse during operation to indicate the wireless connection. The LED will become a solid red if the Wireless Keyfob becomes out of range or if it is not paired with an ancillary.

Wireless Keyfob Battery Replacement

- The Wireless Keyfob is fitted with a CR2032 battery. This can be replaced as follows;
 - Unscrew the battery cover.
 - Carefully release the battery from its housing.
 - Slide a replacement battery into the contacts ensuring the correct polarities are observed.
 - Fit the Wireless Keyfob back together.

Mic Bias and Audio Ancillary Voltage Settings

- Standard Bracer ancillaries inclusive of the speaker Mic and the iPhone headset will be automatically detected by Bracer handsets and will set the volume accordingly.
- Mic Bias and Voltage (5v (default) or 12v) are in the PTT Options Menu.
- These are utilised when using ancillaries that require additional power from the handset or require the mic to be powered.
- **NB** – When using the U229 Bracer connection lead, MIC Bias should be switched on.
- If quiet audio from a Bracer transmission is received, check volume on receiving handset and also ensure that Mic Bias is switched on, on the transmitting handset.



Hints and Tips

- **Signal Strength is critical** – Where possible have visibility of the device screen to see signal strength. Over 3 bars is required for successful communications. Note that some windows have UV filtering that impacts on Iridium Signal.
- Turn handset direction to establish if better signal strength can be achieved.
- Iridium network conducts handover of satellites. If access denied wait a few seconds and try again.
- If constant hiss is received in headset. Switch to standby mode, turn on again and re-register device.
- Always carry USB token so that device can be switched off (not standby) and reinitiated.
- Maintain a good charge on device. It will pull power from any USB source as well as Mains and 12V DC. Full discharge may result in all keys lost.
- In vehicles and other platforms note that the device needs to be able to receive GPS.
- **NB** - Do not site Iridium Antennas near Inmarsat Antennas.



Practical Demonstration / Exercise

1. Plug in ancillaries.
2. Power On.
3. Load Keys from Token.
4. GPS/Register/Select TG/Signal Strength.
5. Transmit (Talk timer, Iridium idiosyncrasy's , Tones) – emphasis on Voice Procedure.
6. Receive a call.
7. Ancillaries.
8. SA demo (enable PLI, allow locations sharing, PLI request, report).
9. SOS demo (initiate, report, acknowledge, cancel).
10. In-secure to Extreme demo (change to Insecure TG, leave insecure TG)
11. Power off to Standby – Reboot.
12. Power off.

QINETIQ/EMEA/CIT/PUB1902044

BRACER™

Module 6 – Part 1

PTT Command Centre

Talkgroups



QINETIQ

This training material is subject to change without notification.

PTT Command Centre Capabilities

- The PTT Command Centre is where Talkgroups and Devices are managed by the End Users (Subscriber Organisation).
- The Service Provider (SP) creates Devices and Talkgroups via a secure web service. PTT hardware is delivered.
- Devices and Talkgroups appear in the SO's PTT Command Centre within SECONDS!
- SO Administrator may now manage the Devices and Talkgroups:
 - Define Talkgroup names.
 - Allocate a Priority Talkgroup.
 - Define geographic location for each Talkgroup.
 - Define Device names.
 - Place Devices in Talkgroups (15 max./device).
 - Devices receive Command Centre updates Over-The-Air (OTA).

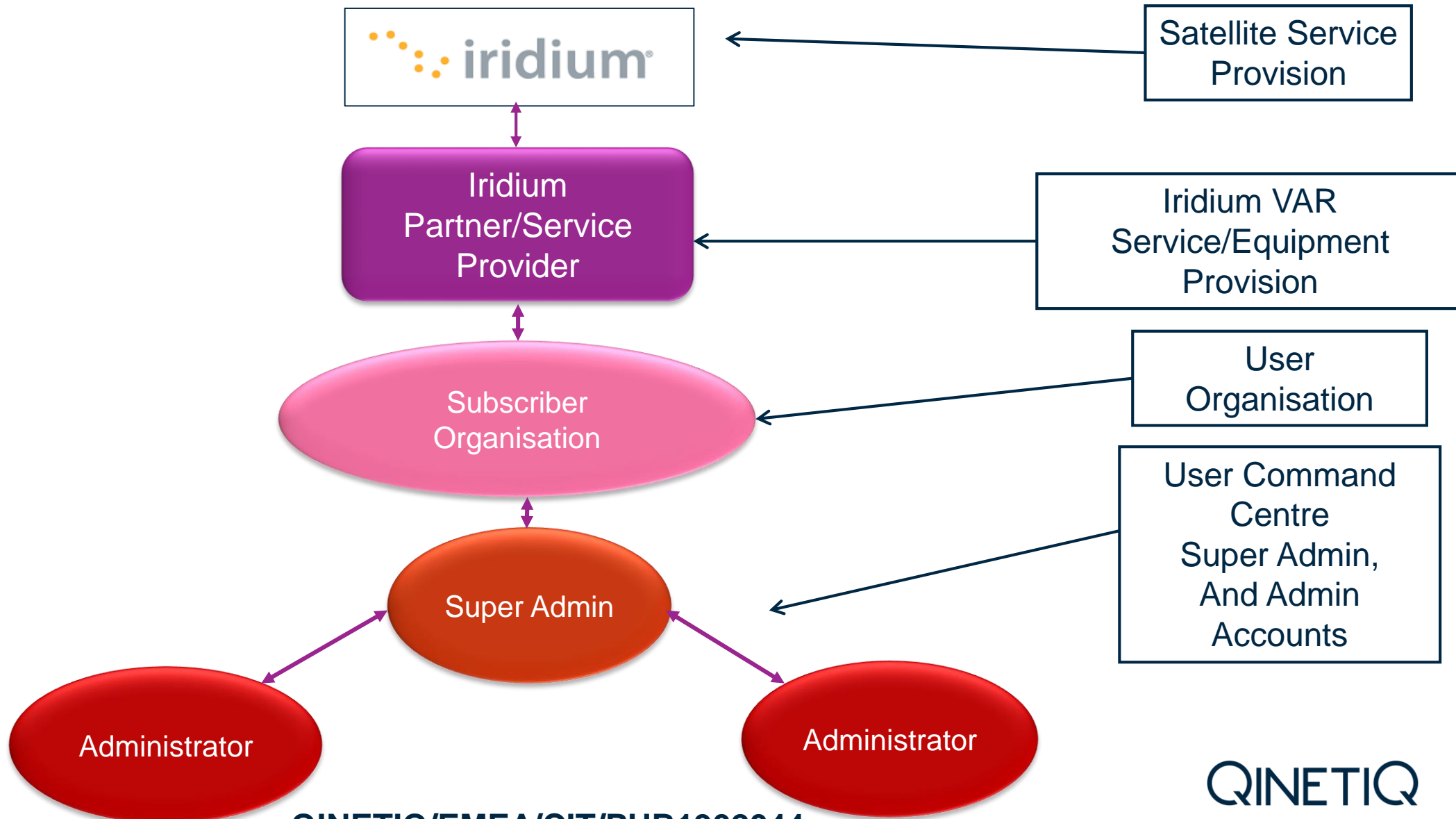


The screenshot shows the login interface for the Iridium PTT Command Center. At the top, the Iridium logo is displayed with the tagline 'Everywhere'. Below the logo, the text 'Iridium PTT Command Center' is centered. The login form consists of two input fields: 'Username' with the value 'julian.henry@panda.com' and 'Password' with masked characters. A 'Forgot your password?' link is located below the password field, and a 'Login' button is positioned to the right of the password field.

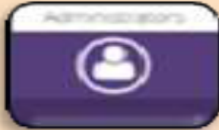
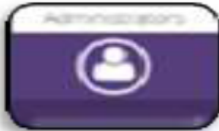



Training Objective

- To enable trainees to operate the PTT Command Centre.
- Key learning Points;
 - Understand Administration Levels.
 - Understand Hierarchy in Command Centre.
 - Registration and Login
 - Command Centre Navigation and Search Facilities.
 - Setting up Talkgroups.
 - Devices.
 - Templates.
 - Tools.

Level of Hierarchy within the Command Centre



Administration Levels, Talkgroups and Devices

Term	Definition	Icon
SuperAdmin	Top level admin that manages Command Center Admins and can perform all configuration tasks.	
Admin	Standard level admin that performs all configuration tasks but may not add new Admins to the Command Center.	
Subscriber Organization (SO)	The lowest level of the hierarchy and the entity where talkgroups and devices reside for PTT service. This is typically the level at which the end-user customer manages aspects of their PTT service.	
Talkgroups (TG)	Talkgroups are collection of devices authorized to communicate with each other within the defined geographic regions managed within the Command Center. Talkgroups are ordered by maximum geographic area permitted for allocation to the talkgroup's coverage.	
Devices	The handsets and other PTT devices ordered under a specific Subscriber Organization.	

End User



Command Centre – Subscriber Organisations

Everywhere

Subscriber Organizations

QinetiQ Blue
Billing ID: 000285

Talkgroups	Devices	Administrators
4	17	2

Patron Red
Billing ID: 000286

Talkgroups	Devices	Administrators
0	0	0

Patron Teal
Billing ID: 000287

Talkgroups	Devices	Administrators
0	0	0

Patron Green
Billing ID: 000298

Talkgroups	Devices	Administrators
0	0	0

Patron Cyan
Billing ID: 000299

Talkgroups	Devices	Administrators
0	0	3

Patron Grey
Billing ID: 000300

Talkgroups	Devices	Administrators
0	0	0

Command Centre Front Page - Global Tile View



Talkgroups Devices ?

QinetiQ Blue

Talkgroups



Blue 1

Google Map data ©2018

Type	Size	Devices	Share
Standard Voice+Data	Small	17	Add

Blue 2

Google Map data ©2018

Type	Size	Devices	Share
Standard Voice+Data	Small	15	Add

FRA-Secure1

Google Map data ©2018

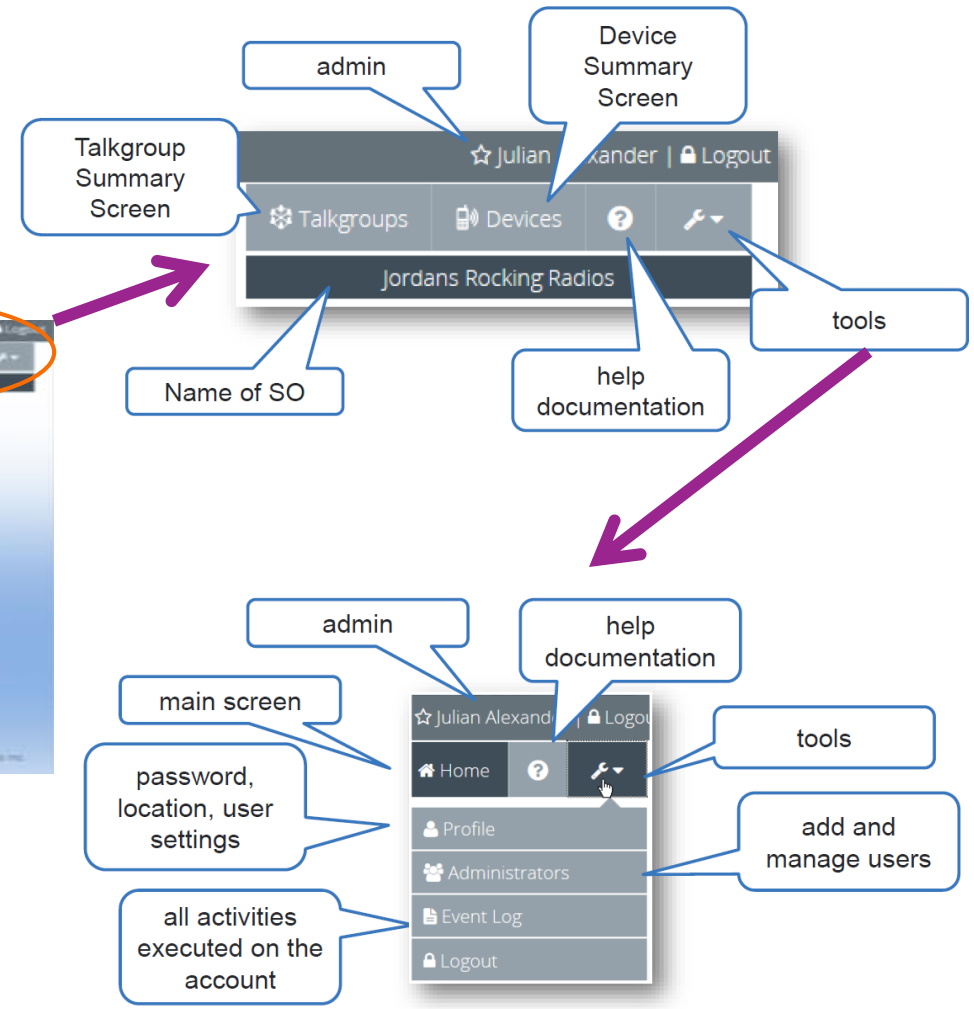
Type	Size	Devices	Share
Standard Voice+Data	Small	15	Add

FRA-Secure2

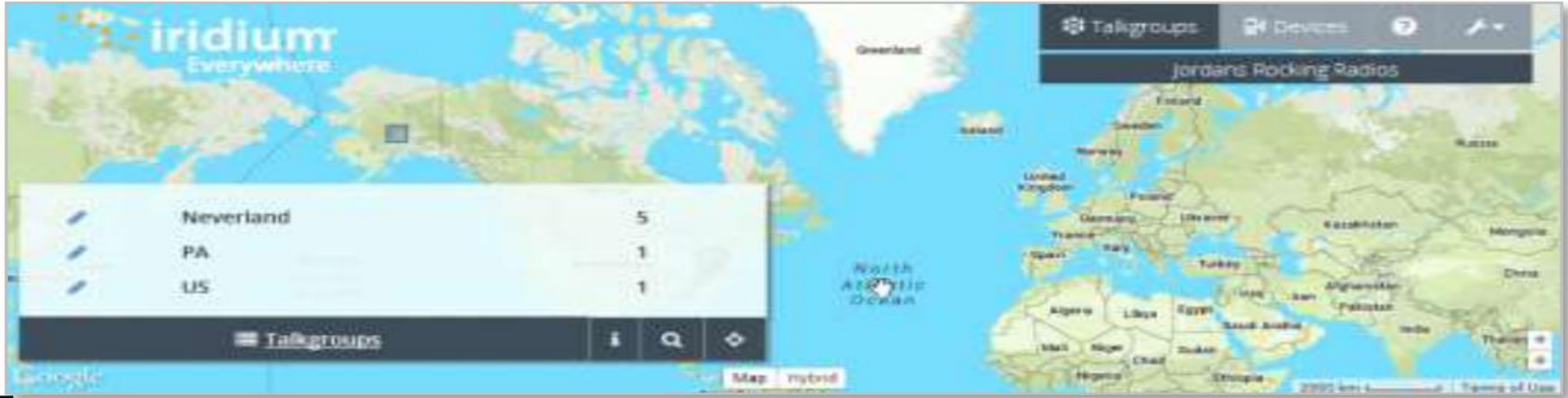
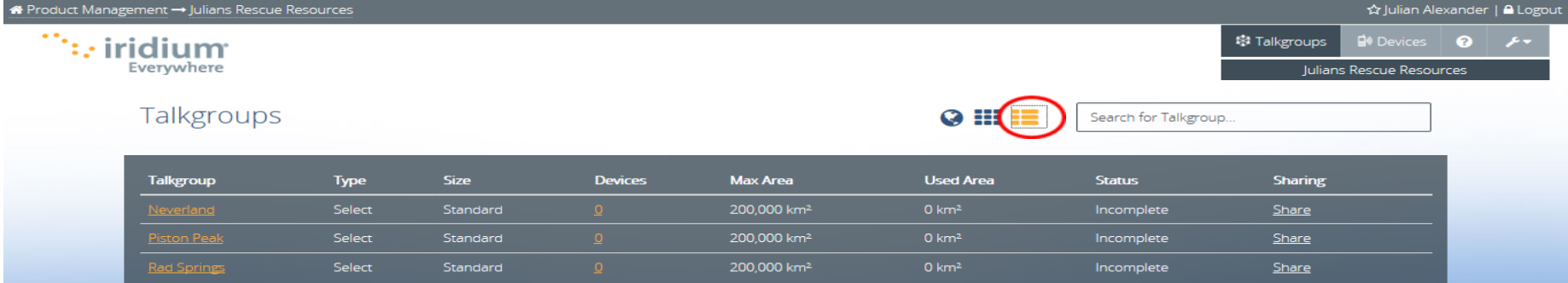
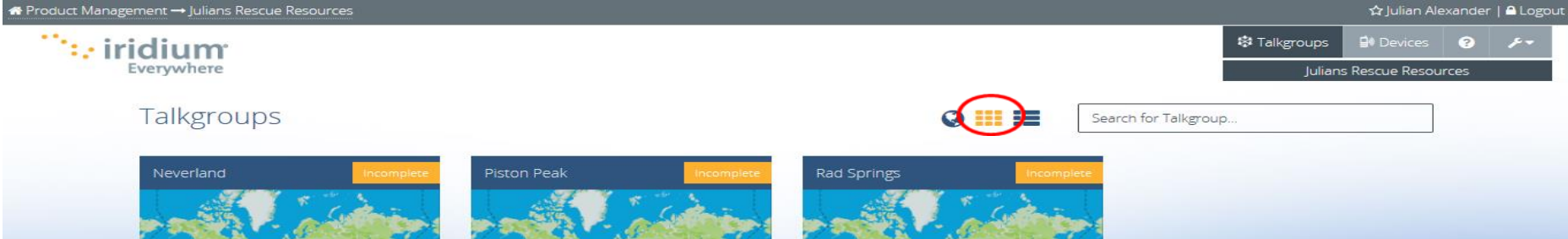
Google Map data ©2018

Type	Size	Devices	Share
Standard Voice+Data	Medium	17	Add

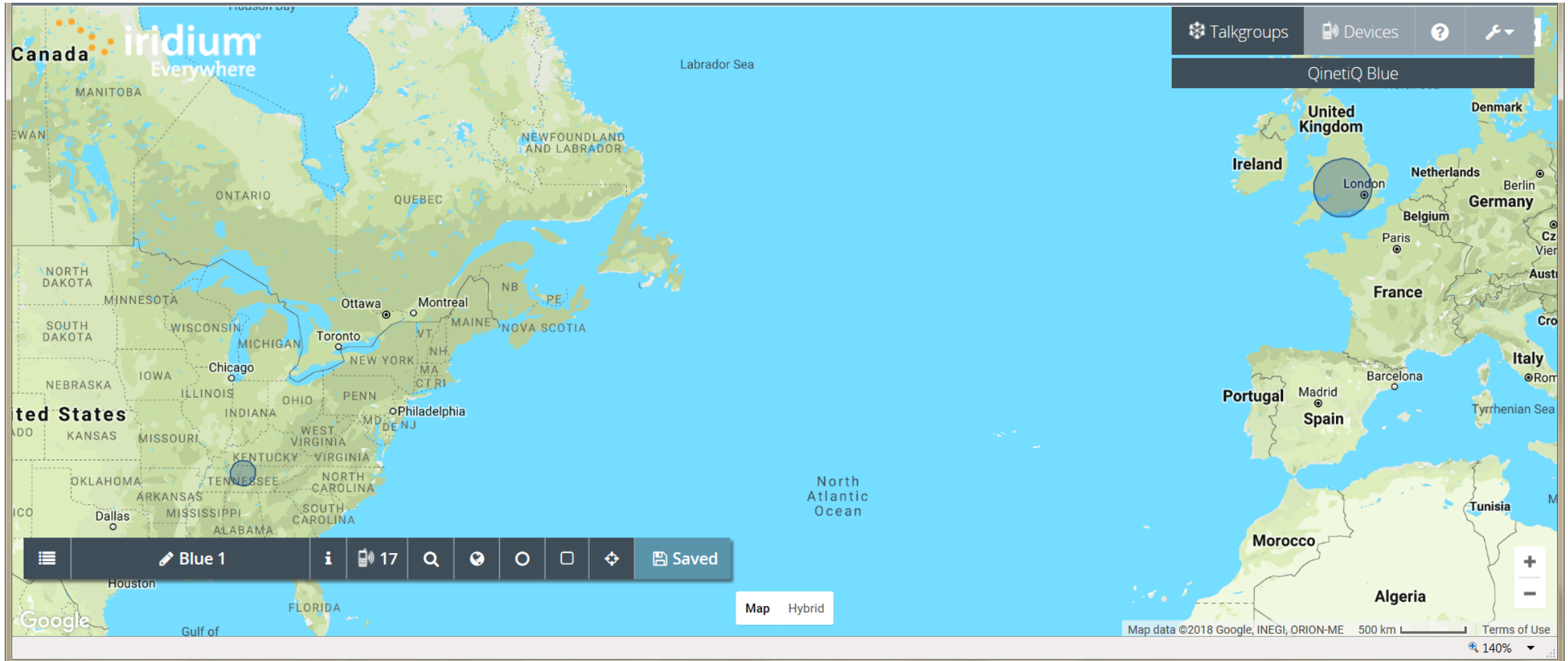
Talkgroup Summary Page – Navigation Bar



Command Centre Navigation

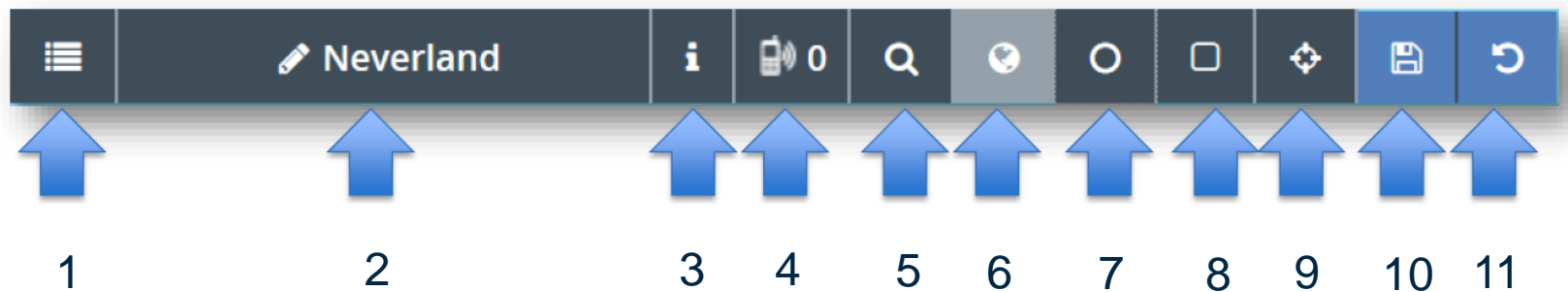


Talkgroup Setup Functional Page



End User Management – Talkgroup Action Bar

- 1 • List View
- 2 • Name
- 3 • Information
- 4 • Devices
- 5 • Search
- 6 • Copy Geography
- 7 • Circle Region
- 8 • Rectangle Region
- 9 • Autofit to Region
- 10 • Save
- 11 • Undo



Setting Up New Coverage Area

iridium
Everywhere

France

Talkgroups

Devices

QinetiQ Blue

Portugal

Area: 95,262 km²
Width: 150 km
Length: 635 km

Region Name:
Portugal

Talkgroup Area:
95,262 / 100,000 km²

Blue 1

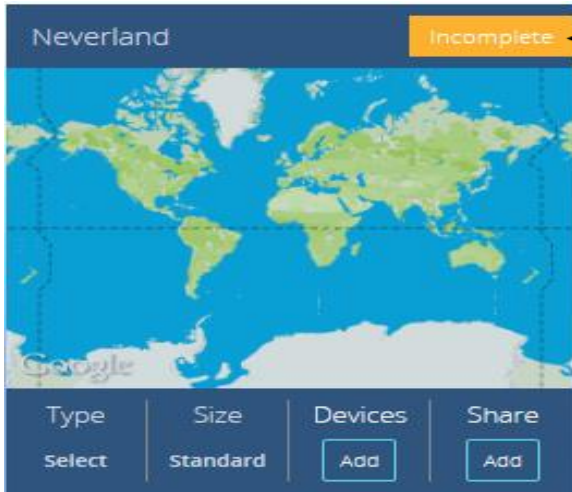
17

Map Hybrid

Google

Map data ©2018 GeoBasis-DE/BKG (©2009), Google, Inst. Geogr. Nacional, ORION-ME 200 km Terms of Use

Talkgroups



Talkgroups define geographic areas where communications is enabled. PTT devices are added to Talkgroups, permitting communications.

States – Talkgroups may have different states. Not fully configured are labelled.

Incomplete

An *incomplete* talkgroup has no regions defined. It may or may not have devices.

Shared

A *shared* talkgroup is one that you have shared with another Subscriber Organization so they may communicate with your members.

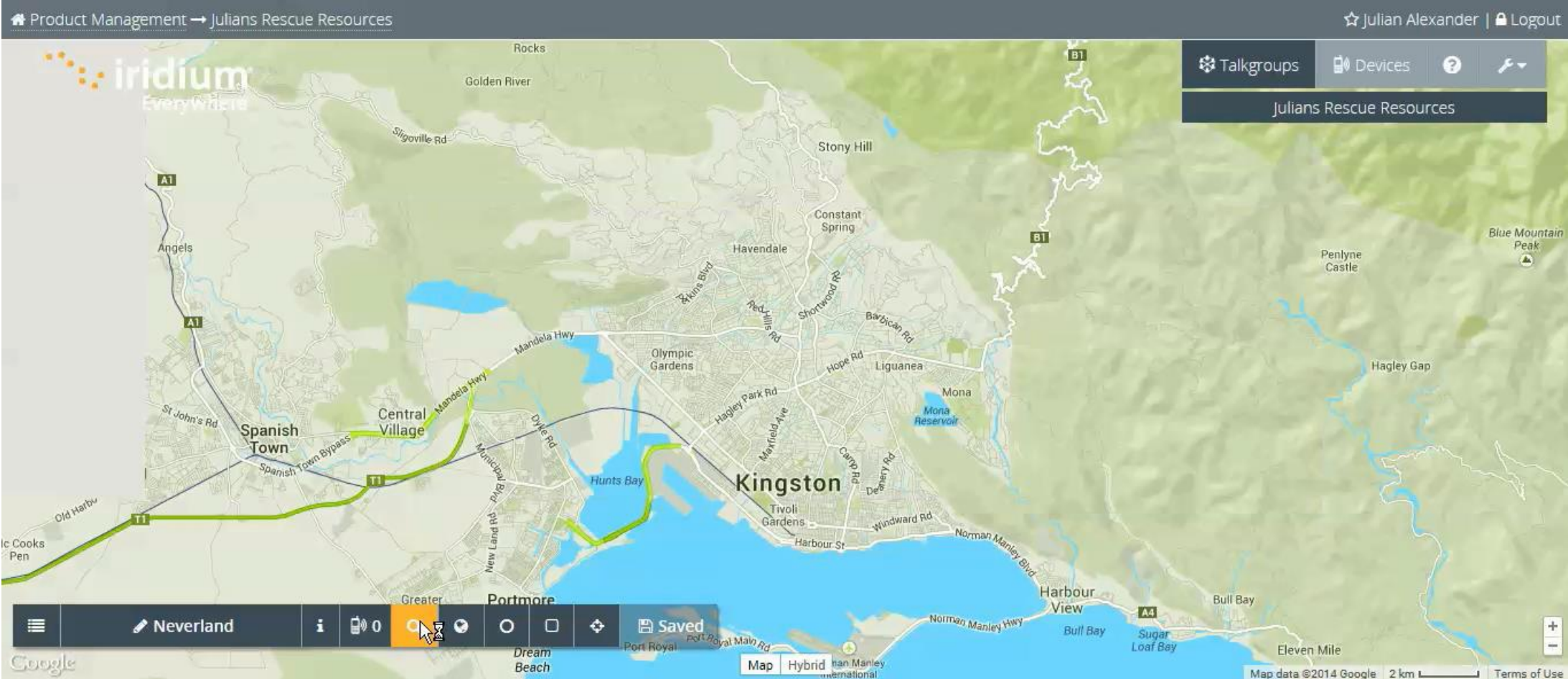
Shared with you

A *shared with you* talkgroup is owned and shared by another Subscriber Organization so you may communicate with their members.

Downsized

A *downsized* talkgroup occurs when the talkgroup size is decreased in the billing system (e.g., medium to small) and the defined regions exceed the new size limitation. It will remain inactive until the regions are adjusted to fit the new talkgroup size limits.

Search for a Specific Location



Setting Up A Talkgroup (continued)

AUTOFIT TO REGION



Zooms out (or in) to show all the regions defined in a talkgroup on one screen.

SAVE



Saves changes made to the Talkgroup.

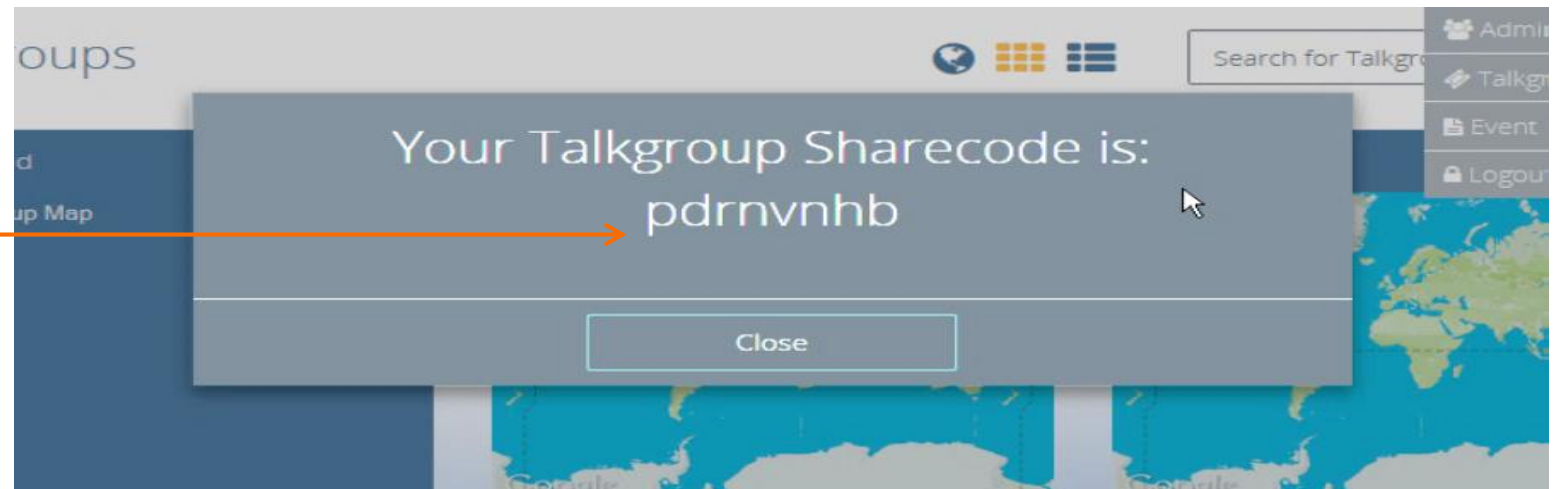
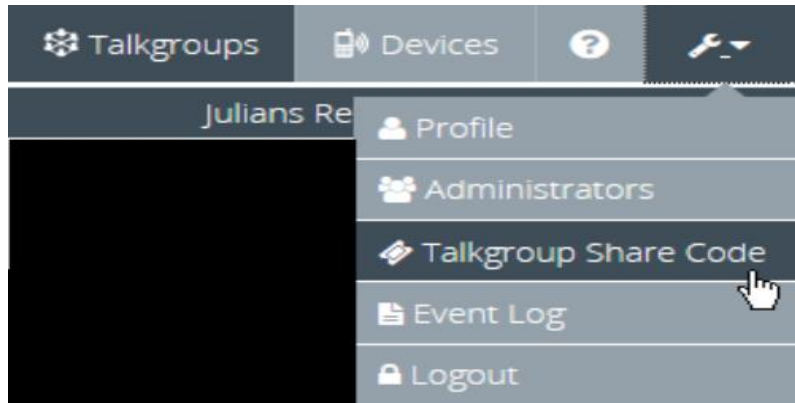
UNDO



Reverses all changes made to the Talkgroup since the last time it was saved.

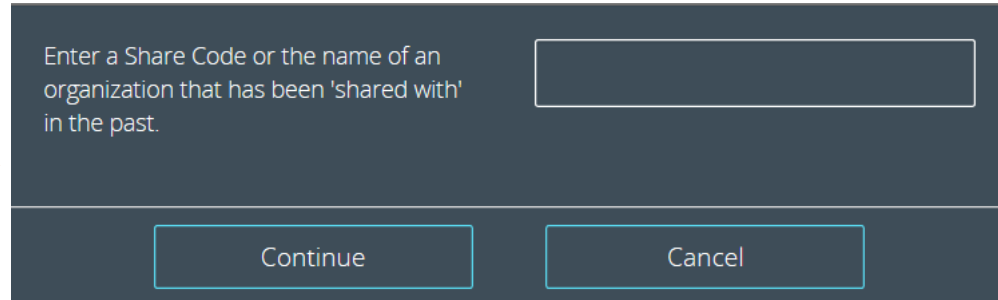
Talkgroup Sharing - Share Code

- Allows a SO to share a Talkgroup with another SO.
- Share Codes will be issued to the SOs wishing to share. **Only provided by the Iridium Administrator!**
- When code is available the sharing SO can then send the code to the SO it wishes to share with.



Sharing a Talkgroup

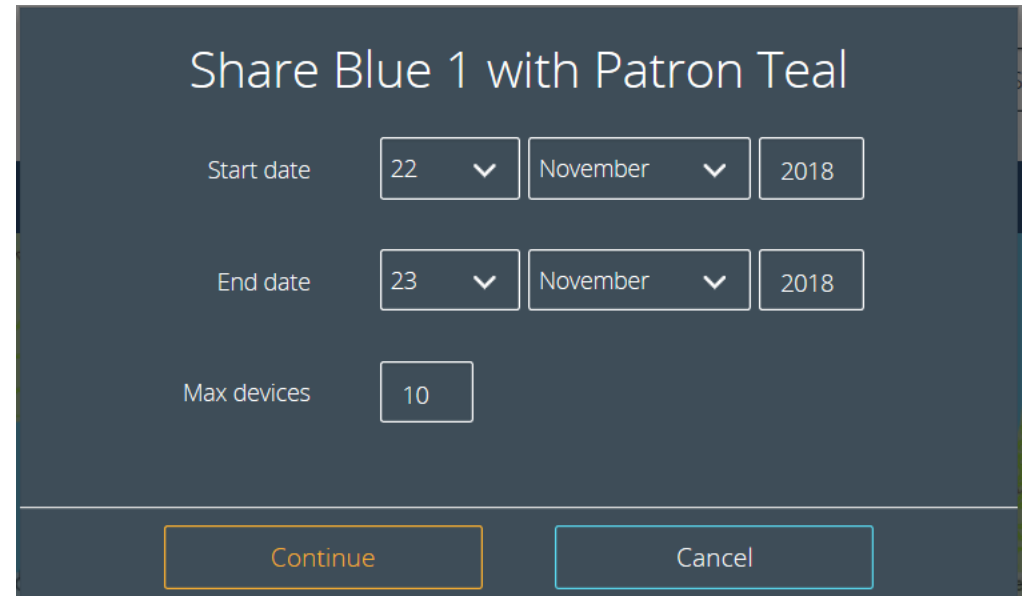
A box appears in which the share code must be entered or the shared before the name of the SO.



Enter a Share Code or the name of an organization that has been 'shared with' in the past.

Continue Cancel

The sharing SO must enter the start and end period of the share and the maximum number of Devices that can be included.



Share Blue 1 with Patron Teal

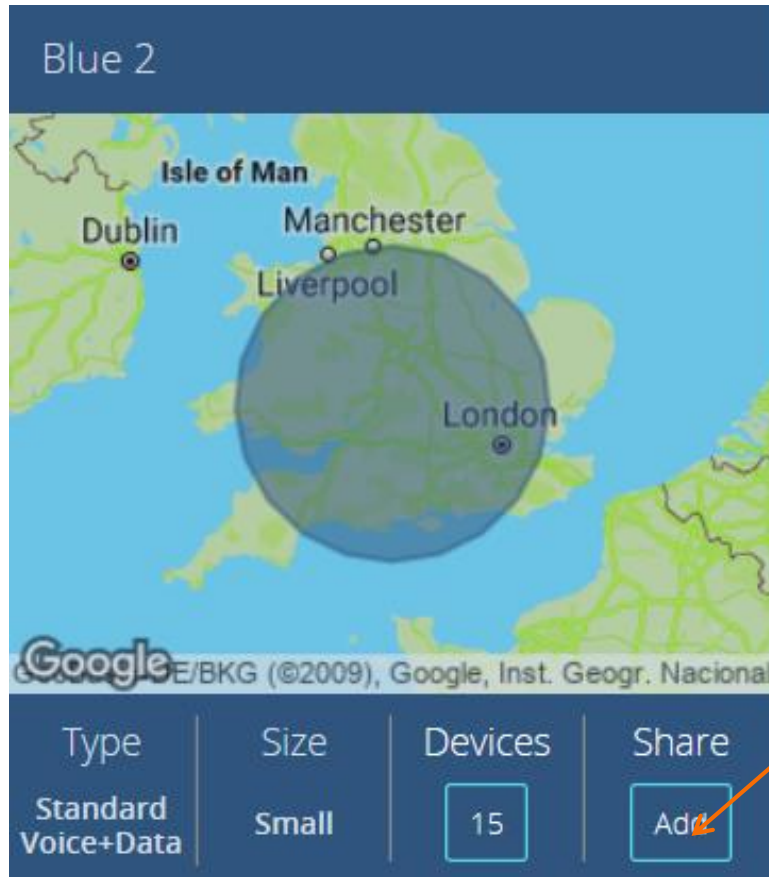
Start date 22 November 2018

End date 23 November 2018

Max devices 10

Continue Cancel

Sharing a Talkgroup



From the Talkgroup Summary Page, locate the Talkgroup to be shared. Click on the Add button.

Sharing a Talkgroup

This is how a Shared Talkgroup appears on the Talkgroup Summary Page. Clicking on the Devices ADD button allows Devices to be added.

View from the Talkgroup Owner Organisation

Type	Size	Devices	Share
Standard Voice+Data	Small	17	View

Type	Size	Devices	Share
Standard Voice+Data	Small	15	Add

View from the Sharer

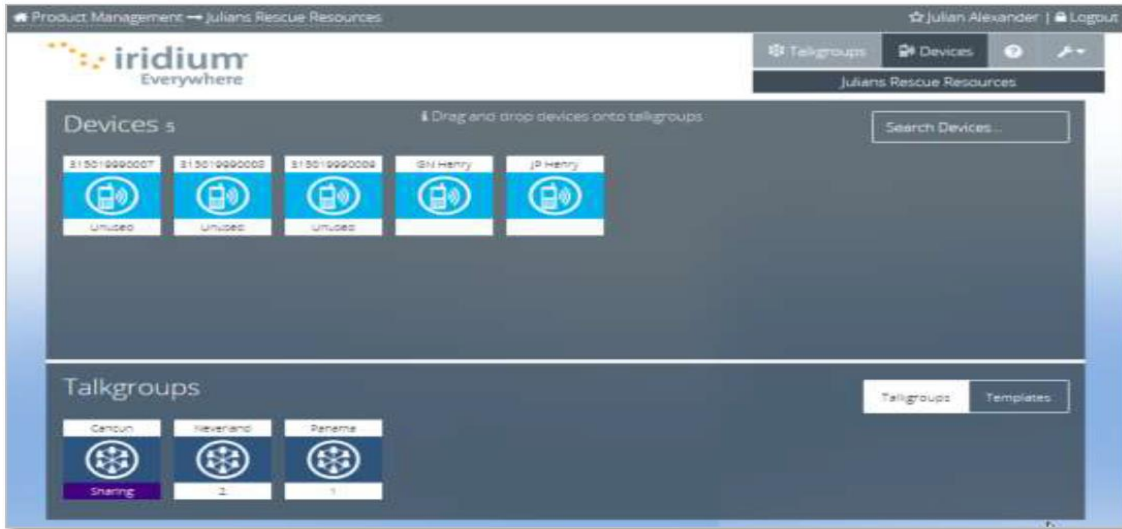
Blue 1
Talkgroup Owner: QinetiQ Blue

Share Start: 22 Nov 2018
Share End: 23 Nov 2018
Max devices: 10
Share State: Active

Devices	Share
Add	Delete

Sharing a Talkgroup

Drilling down on the Shared Talkgroup will provide details of the SO sharing and the Devices used.



NB – Devices need to be allocated to a shared Talkgroup by the SO sharing the Talkgroup.

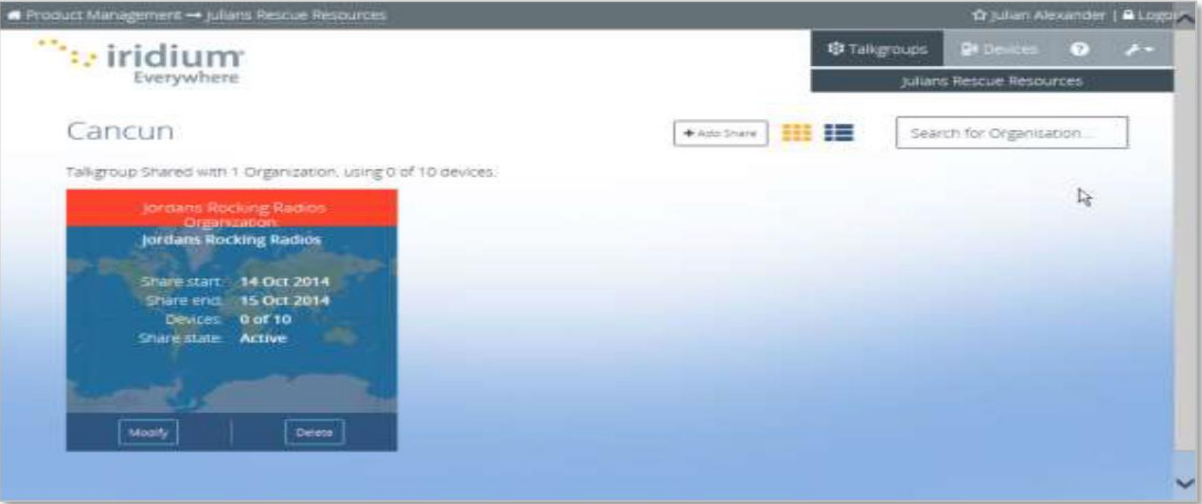


Sharing a Talkgroup

Talkgroup shown as Shared in Summary Page.



Talkgroup owner can update details of the share or delete as necessary.



Setup Administrator



Talkgroups

Talkgroups Devices ?

Qin

- Profile
- Administrators
- Talkgroup Share Code
- Event Log
- Logout

Search for Talkgroup...

Blue 1

Google Map data ©2018

Type	Size	Devices	Share
Standard Voice+Data	Small	17	Add

Blue 2

Google Map data ©2018

Type	Size	Devices	Share
Standard Voice+Data	Small	15	Add

FRA-Secure1

Google Map data ©2018

Type	Size	Devices	Share
Standard Voice+Data	Small	15	Add

FRA-Secure2

Google Map data ©2018

Type	Size	Devices	Share
Standard Voice+Data	Medium	17	Add

Add a New Administrator

The screenshot shows the 'Product Management Administrators' interface. At the top, there is a navigation bar with 'Product Management' on the left and 'Julian Alexander | Logout' on the right. Below this is the 'iridium Everywhere' logo. The main content area has a purple header with a user icon and the text 'Product Management Administrators'. A red arrow points to a button labeled 'Add New Administrator'. Below the button is a search bar with a dropdown menu set to '25', a search input field, and a 'Go' button. To the right of the search bar are 'Previous' and 'Next' buttons. Below the search bar is a light blue bar indicating 'Showing 1 to 3 of 3 Entries'. A table lists the administrators with columns for Username, Last Name, First Name, and Status.

Username	Last Name	First Name	Status
G.Henry@apl.com	Henry	Gregory	Pending
lmcantor@apl.com	Cantor	LM	Registered
jca.alexander@iridium.com	Alexander	Julian	SuperAdmin

Adding a New Administrator



Talkgroups Devices ?

QinetiQ Blue

QinetiQ Blue Administrators

Add New Administrator

First Name	Last Name
<input type="text"/>	<input type="text"/>
Email Address - used as Username/Login	Account Type
<input type="text"/>	Admin

Add New Administrator Cancel

25 Search Go

« Previous Next »

Showing 1 to 2 of 2 Entries

Username	Last Name	First Name	Status	Access Level
----------	-----------	------------	--------	--------------

New Administrator Registration



Dear Geoff:

You have been sent this email because your Service Administrator has created an Iridium PTT user account for you. To complete the registration process and create your password, please click on the following link: <https://ptt.iridium.com/register/q40cca65e-7969-4f7b-9b93-141bd8c8f10ar>. This link will expire in 7 days.

Follow the rules below to create your password.

- Password must contain a minimum of 8 characters
- Password must contain an uppercase letter
- Password must contain a lowercase letter
- Password must contain a number
- Password must contain a symbol

If you have any questions, please contact your Iridium PTT Service Administrator.

Registration

Registration

Welcome to the Iridium PTT Command Center.
Please provide a password and accept the Terms of Use to complete your registration.

Username:

Your Password:

Confirm Your Password:

Show Password

IRIDIUM – PUSH TO TALK COMMAND CENTER TERMS AND CONDITIONS OF USE

These Push to Talk Command Center Terms and Conditions of Use (these "**Push to Talk Command Center Terms**") are an agreement between Iridium Satellite LLC and you (as defined below). These Push to Talk Command Center Terms govern your use of the Push to Talk Command Center (as defined below). These Push to Talk Command Center Terms are not intended to alter any terms or conditions of any other agreement between Iridium Satellite LLC or any affiliated company of the foregoing (collectively, the "**Iridium**," "**us**" and "**we**") and any Service Partner (as defined below) (e.g., Service Provider, Value Added Reseller, Value Added Developer or Value Added Manufacturer, Non-Disclosure agreements; each a "**Service Partner Agreement**"). To the extent that there is any conflict between these Push to Talk Command Center Terms and any provision of a Service Partner Agreement to which you are a party, if any, the provision in the Service Partner Agreement will prevail.

BY CLICKING ON THE "ACCEPT" BUTTON OR EXECUTING A WRITTEN ACKNOWLEDGMENT REFERENCING THESE PUSH TO TALK COMMAND CENTER TERMS, YOU ACKNOWLEDGE THAT YOU HAVE READ THESE PUSH TO TALK COMMAND CENTER TERMS, UNDERSTAND THEM, AND, IN CONSIDERATION OF THE ACCESS TO THE PUSH TO TALK COMMAND CENTER PROVIDED HEREIN AND OTHER GOOD AND VALUABLE CONSIDERATION PROVIDED HEREUNDER, AGREE TO THE TERMS CONTAINED IN THESE PUSH TO TALK COMMAND CENTER TERMS. IF YOU DO NOT AGREE TO THESE PUSH TO TALK COMMAND CENTER TERMS, YOU MUST IMMEDIATELY DISCONTINUE YOUR ACCESS TO AND USE OF THE PUSH TO TALK COMMAND CENTER. YOU REPRESENT AND WARRANT THAT YOU HAVE THE AUTHORITY TO ACT AS AN AGENT FOR CUSTOMER.

PLEASE NOTE THAT THESE PUSH TO TALK COMMAND CENTER TERMS DISCLAIM ALL WARRANTIES AND LIMIT LIABILITY ON BEHALF OF IRIDIUM. WE ASK THAT YOU READ THE RELATED TERMS CAREFULLY.

I agree to the Terms of Use

Registration



Registration Complete

Congratulations, you have successfully completed the registration process for the Iridium PTT Command Center.

Please login



Iridium PTT Command Center

Username
gnorris@qinetiq.com

Password

[Forgot your password?](#)

Confirmation Email



Dear Geoff:

You have successfully completed your Iridium PTT user account registration. [Click here](#) to log into the system.

If you have any questions, please contact your Iridium PTT Service Administrator.



Suspending or Deleting an Administrator

BrookesBlue

Address:
QinetiQ, WR143PS, UK

Telephone:
+44(0)1684895733

Account Type:
SuperAdmin

Save

Account Actions

Suspend Reset Password Delete

QINETIQ/EMEA/CIT/PUB1902044

BRACER™

Module 6 – Part 2

PTT Command Centre

Devices



QINETIQ

This training material is subject to change without notification.

BRACER

Talkgroup Action Bar: Devices

- **NB – Devices can only be added to an account by a Service Provider**

Clicking on the Devices button will display the Device Summary page.

This shows the number of Devices available.

Devices can be added, edited or removed.



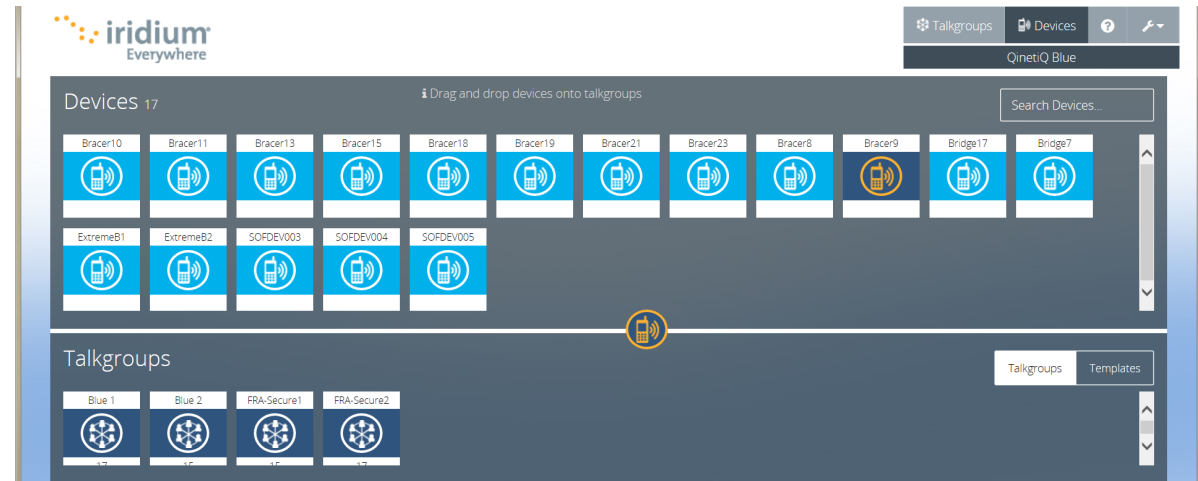
Talkgroup Action Bar: Devices

Provides a view of available Devices and Talkgroups.

Devices are assigned to a Talkgroup by “dragging and dropping” on the Talkgroup.

Device details can be viewed/edited by clicking on the Device name.

Clicking on a Talkgroup tile shows the Devices allocated to it.



Devices

PTT Devices are provisioned by the Service Provider and assigned to the Subscriber Organisation. Devices are automatically added to the Command Centre and can then be configured by the SO Administrator.

Moving Devices

Click on Device and drag and drop on to Talkgroup.

For multiple Devices hold down Shift Key select drag and drop into Talkgroup.



Devices

PTT Devices are provisioned by the Service Provider and assigned to the Subscriber Organisation. Devices are automatically added to the Command Centre and can then be configured by the SO Administrator.

Moving Devices

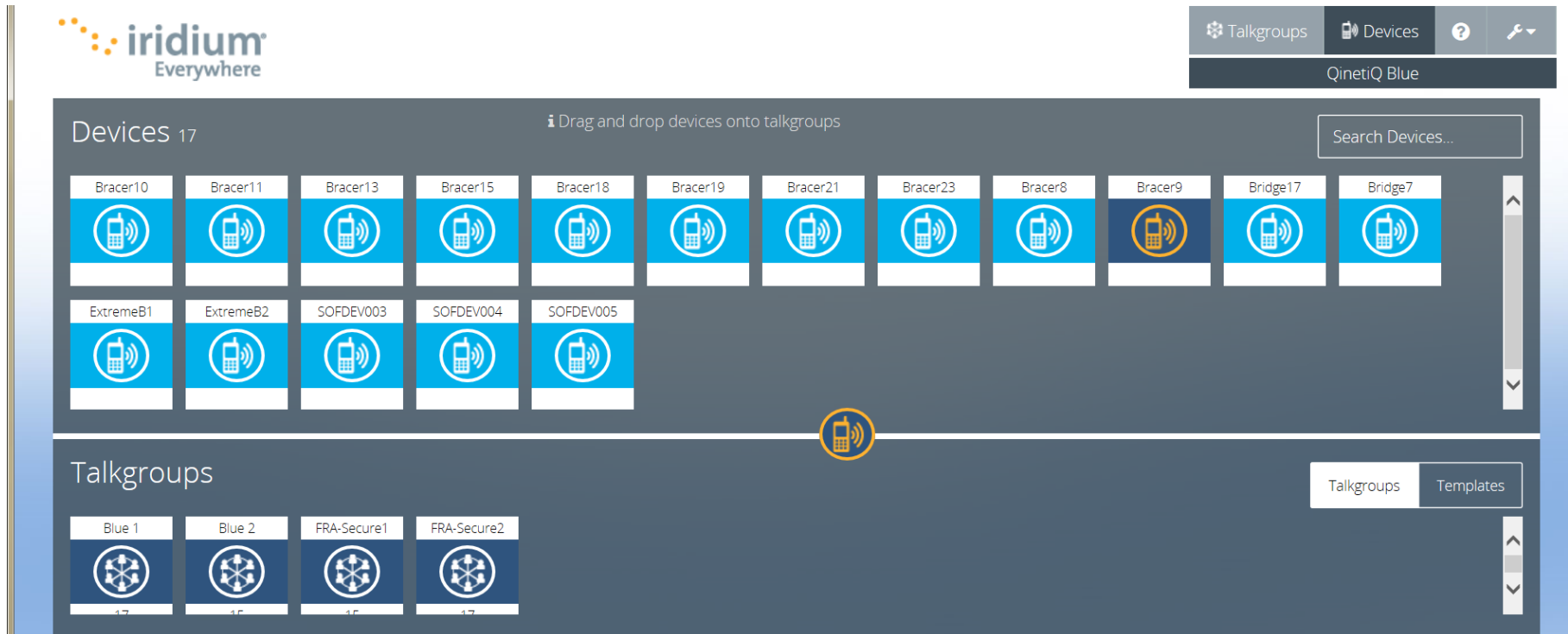
Click on Device and drag and drop on to Talkgroup.

For multiple Devices hold down Shift Key select drag and drop into Talkgroup.



Removing Devices from a Talkgroup

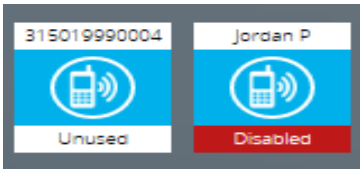
Click on the Talkgroup tile to display the Devices allocated, select Device, click and drag up to Devices area and release mouse button. For multiple Devices hold shift key and click drag and drop. Devices will be removed from the Talkgroup.



Device Detail Page

Name that will appear in Talkgroup. If not named last 12 of IMEI will be displayed e.g. 300987654321123.

Allocate a Priority Talkgroup



Provide relevant comments/detail

Create a template for multiple Devices

Note: Disabling a Device may take up to 4 hours if the Device does not re-register with the network i.e. press the PTT button.

Device Details Page

All Device Details, Device Talkgroups and Talkgroups configured are sent to the Device Over-the-Air (OTA).

These details are applied when the Device registers on the Iridium network.

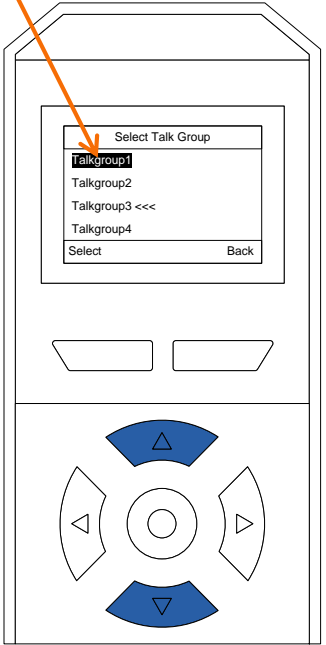


Device Talkgroups Section

Up to 15 Talkgroups can be allocated to a Device.

Drag and drop Talkgroups into slot.

The order determines how the Talkgroups appear on the Device e.g.



Templates

Templates can be created in 2 ways from an existing configuration by saving in the Device Details page.

Save As Device Template

Or by creating a new one by clicking the Device Summary Page.

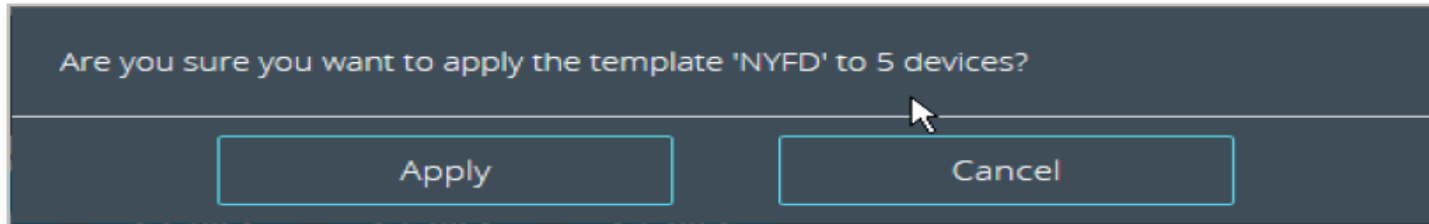
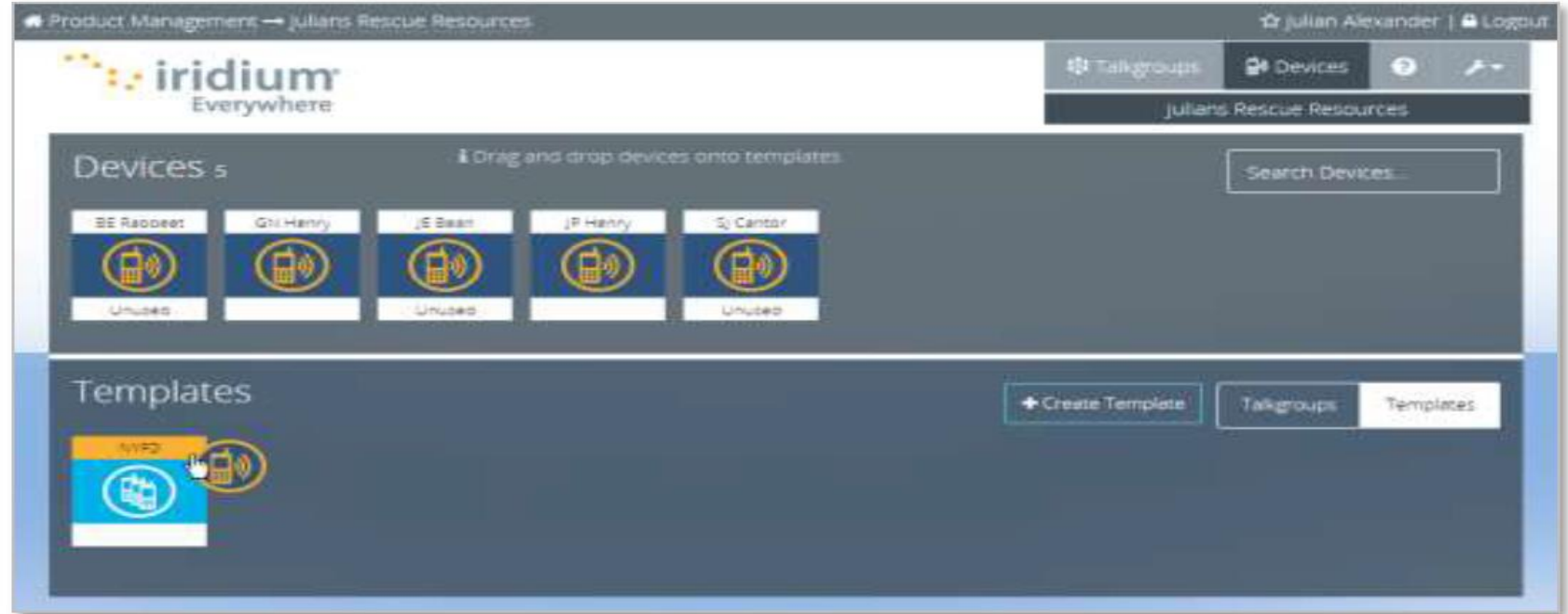
+Create Template



Using Templates to Configure Multiple Devices

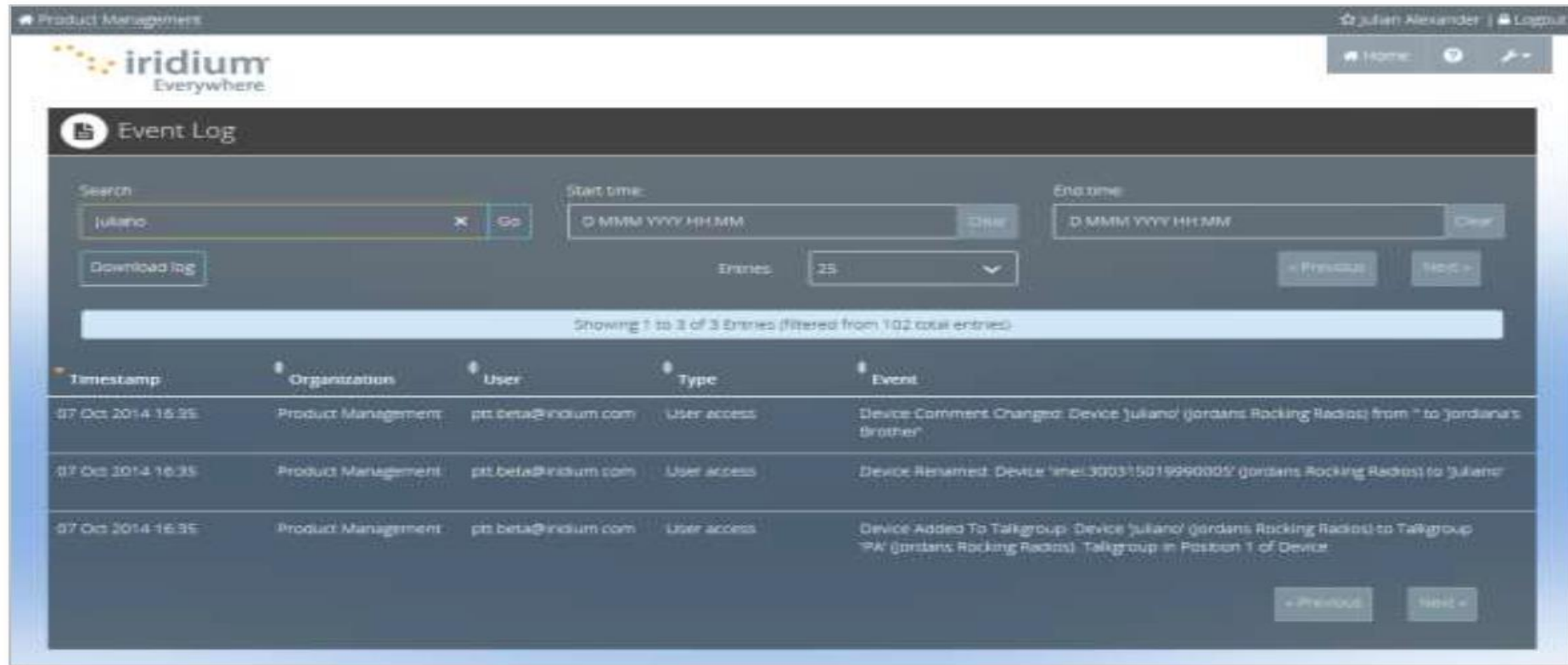
Open Device Summary Page:

- Open Template summary.
- Select Devices from top of page.
- Drag and drop onto desired template.



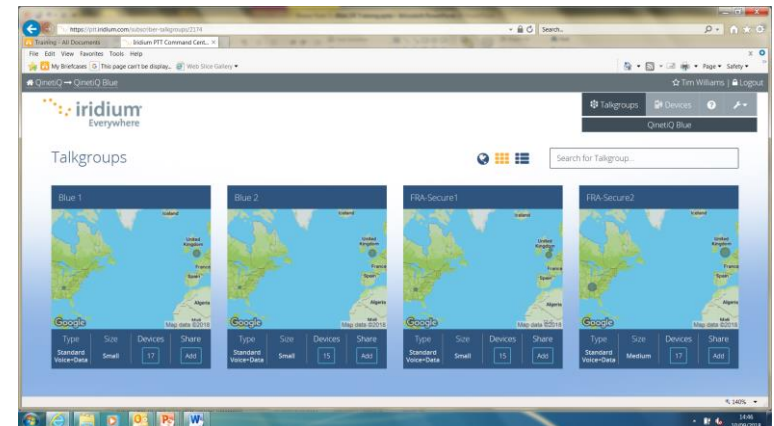
Tools – Event Log

Captures all administrative activity for a rolling 90 days.



Command Centre - Practical Demonstration / Exercise

1. Log on to account (<https://ptt.iridium.com/>).
2. Allocate Devices to a TG (Label Devices).
3. Set up a template device.
4. Set up a Priority TG.
5. Show List mode for TGs.
6. Set up TG coverage (Circle ,Square, Label, Subdivide, Save).
7. Edit and Move TG.
8. Search for a location.
9. Copy Geography – Set up TG.
10. Introduction to Sharing a TG.
11. Autofit Region.
12. Set up an administrator account.



SUMMARY

- The PTT Command Centre provides the Subscriber Organisation with the capability to autonomously manage and configure all Talkgroups and Devices that are owned by them.
- Talkgroups can be provided in Small, Medium, Large, Extra Large and Jumbo area sizes.
- Talkgroups can be broken down in up to 10 Regions.
- Talkgroups and Regions can be distributed anywhere in the world.
- Talkgroups can be Shared with other Subscriber Organisations.
- More than 10,000 PTT Devices can be allocated to a single Talkgroup.
- PTT Device details can be configured, units named, added/removed from Talkgroups and easily enabled/disabled.
- PTT Device configurations are updated OTA when the Device registers with Iridium.
- Talkgroup and Device changes can be implemented within seconds. PTT Devices are updated when they register/re-register with the network.

QINETIQ/EMEA/CIT/PUB1902044

BRACER™

Module 7

Bracer Key Management System








QINETIQ

This training material is subject to change without notification.

BRACER

QINETIQ CONFIDENTIAL

Programming Bracer™ - Overview

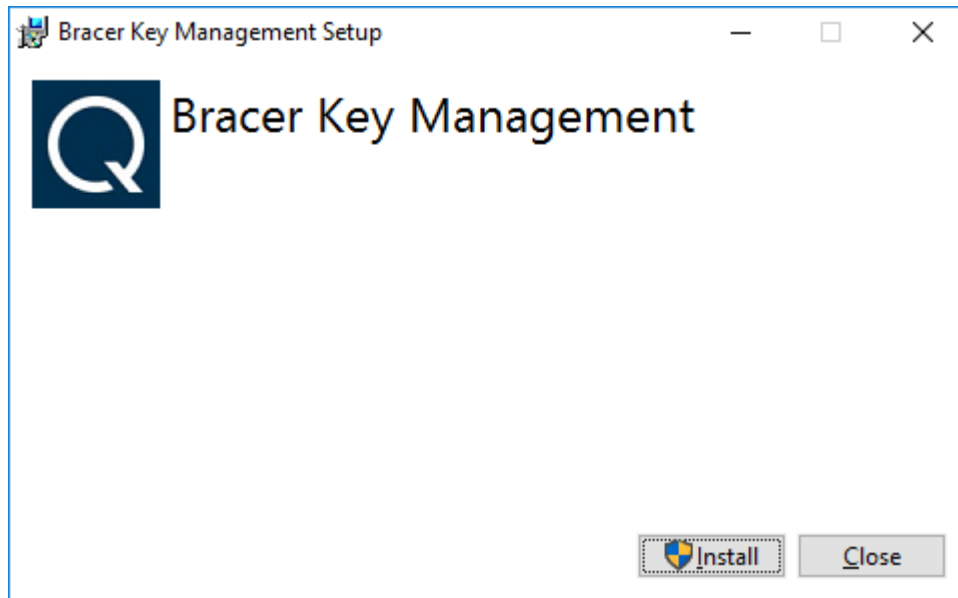
Firmware Load	Authentication	Transfer Key Load	Mission Key Load	Register on Network
				
<p>Device Firmware is checked to establish whether on latest version using the Bracer Firmware loader application as part of the Bracer Secure Tool Kit.</p> <p>Firmware upload only required when firmware is not latest version or device has no firmware</p>	<p>USB Token Authentication and passcodes are set up in Bracer using a USB token and passcode generation from the Bracer Handset for Administrator, Super User (Commander) and User profiles.</p>	<p>Transfer key is generated using the Privacy Management Sub System (BKM) Application. Bracer must be set up in Administrator profile during this process.</p>	<p>Bracer device is changed to Super User (Commander) or User profile and prepared to receive Mission keys. Mission Keys are generated for specified Talkgroups, plus the situational awareness keys and transferred to the Bracer handset. Turn off Handset Transfer and Mission Key load complete</p>	<p>Turn on Handset with USB token attached, log in to Super User (Commander) or User profile. Remove token. Register handset on network, obtain a GPS fix, check that specific Talkgroups have allocated keys within the device (denoted with (S), make a test call to other Bracer devices in the network.</p>

Installing Bracer™ Key Management (BKM) Software

Installing BKM Software

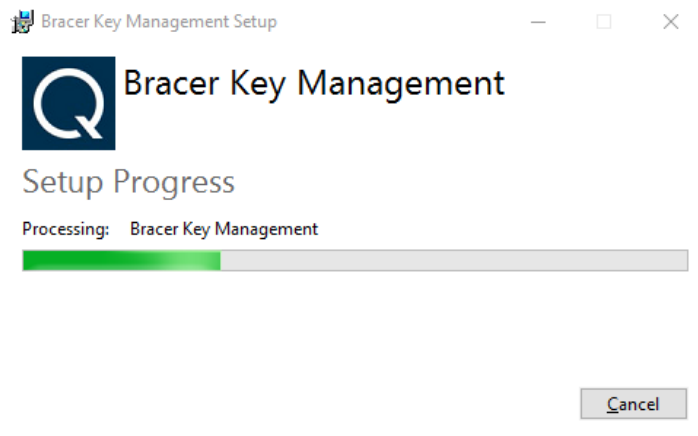


Upload Key Management File and execute.

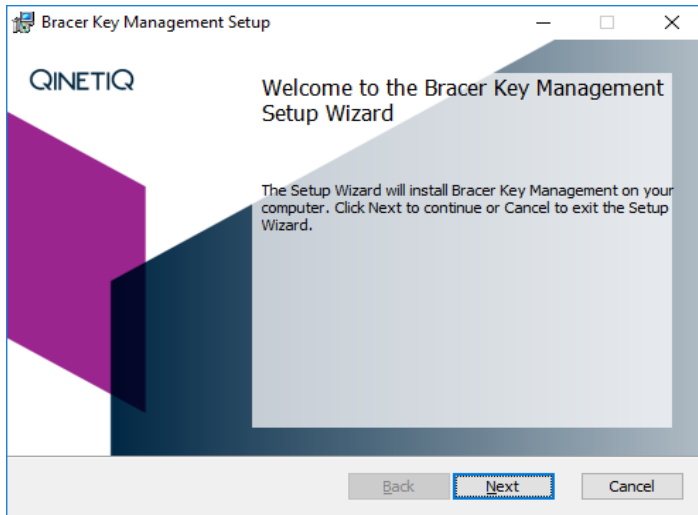


Press Install.

Installing BKM Software

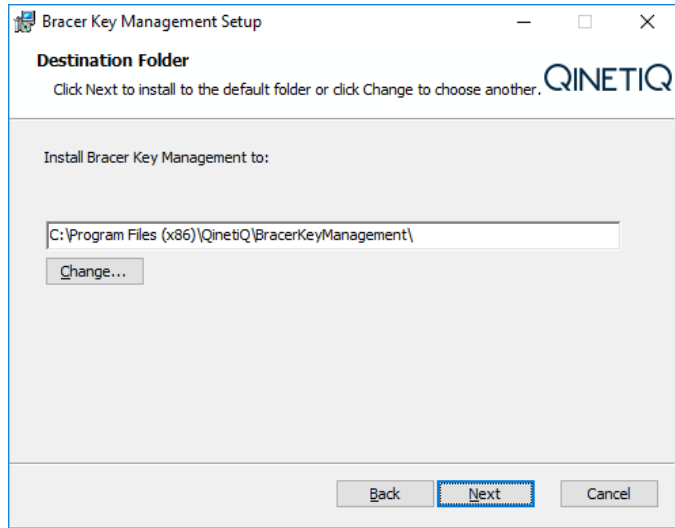


Bracer Key Management Software Loads.

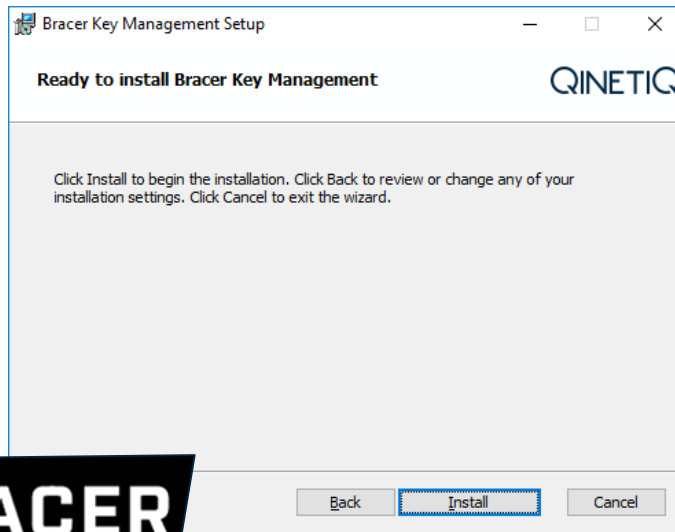


Wizard Window – Click Next.

Installing BKM Software

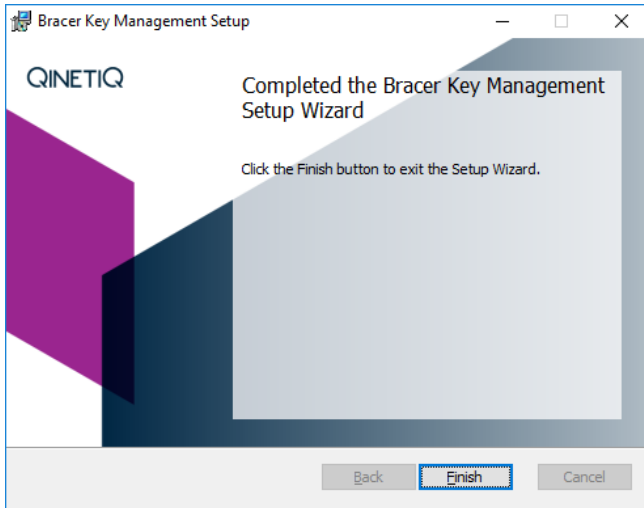


Accept or Change Destination for Programme.

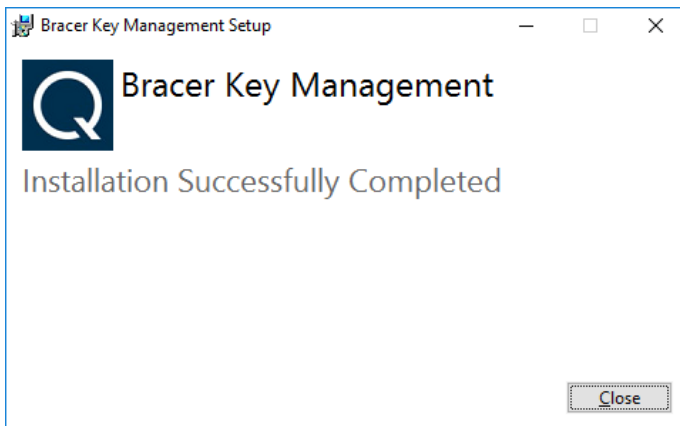


Click Install.

Installing BKM Software



Once Programme has loaded – Click Finish.

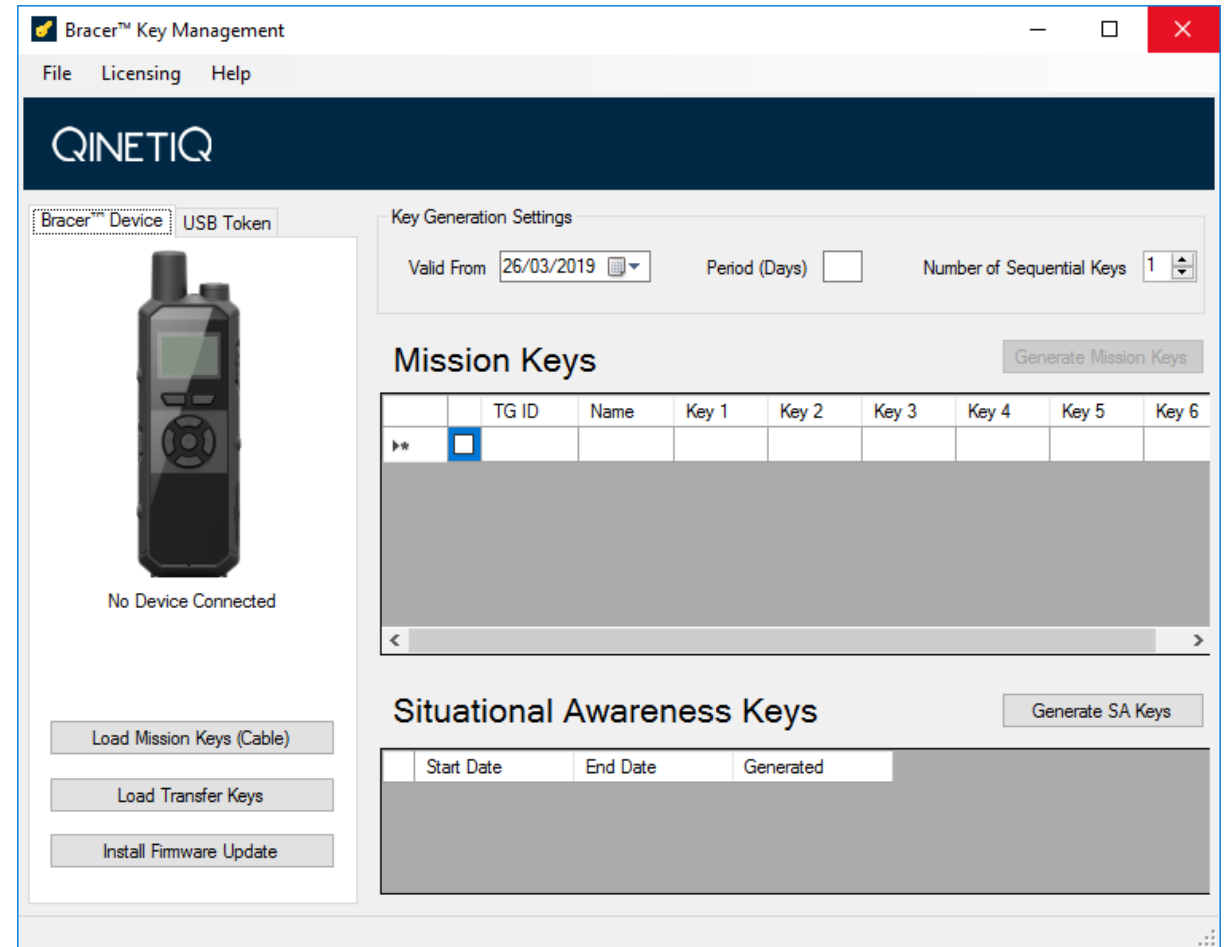


Click Close.

Using the Bracer Key Management Software

BRACER Key Management

- **Launch Key Management application**
 - Double click the Bracer Key Management application on the desktop.
- **Purpose:**
 - Installing Licences.
 - Install Firmware.
 - Commission Device (Load Transfer Key).
 - Generate Mission Keys.
 - Generate SA keys.
 - Load Mission Keys (USB Cable).
 - Load Mission Keys to USB Token.
 - Export keys to file.
 - Import keys from file.



Loading Licences

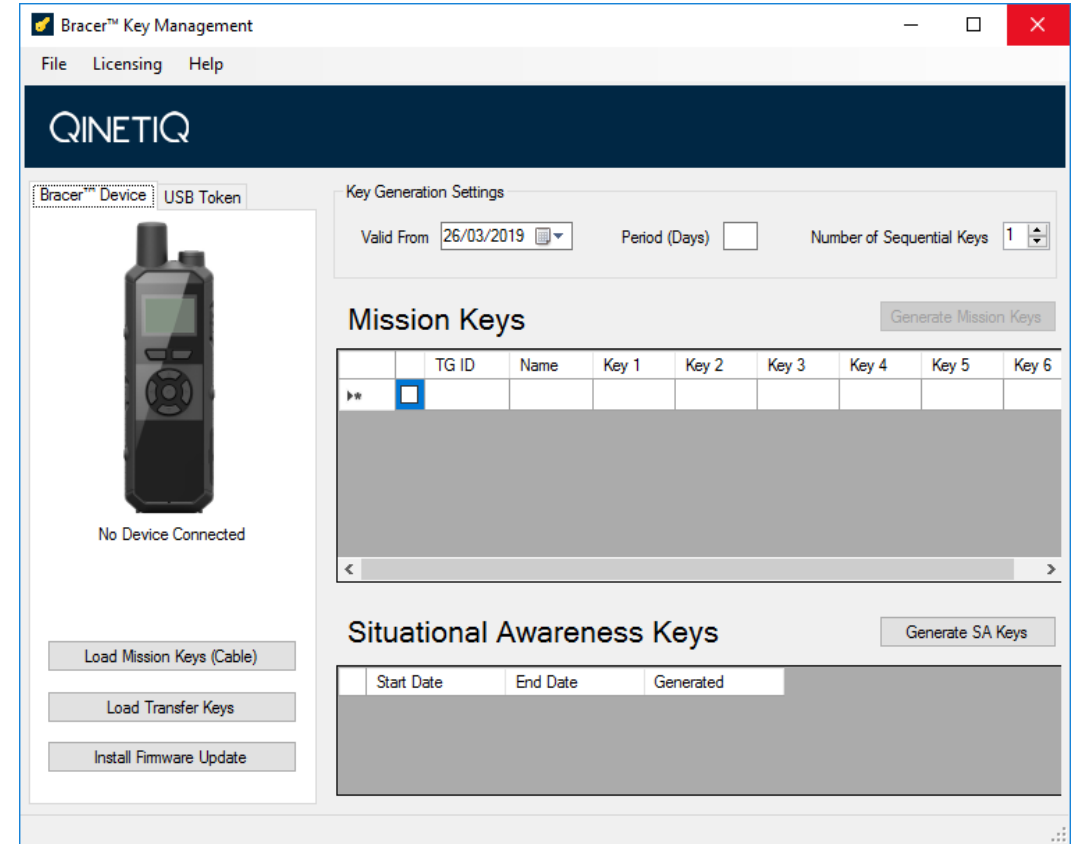
Bracer Licences

Licence Requirement - Each Bracer device requires an individual licence, this is time bound. This enables the following:

- Firmware update installation.
- key generation (transfer and mission key) and installation.
- working in an end to end encrypted mode.
- Enables access to the Situational Awareness Tools.

Getting a licence

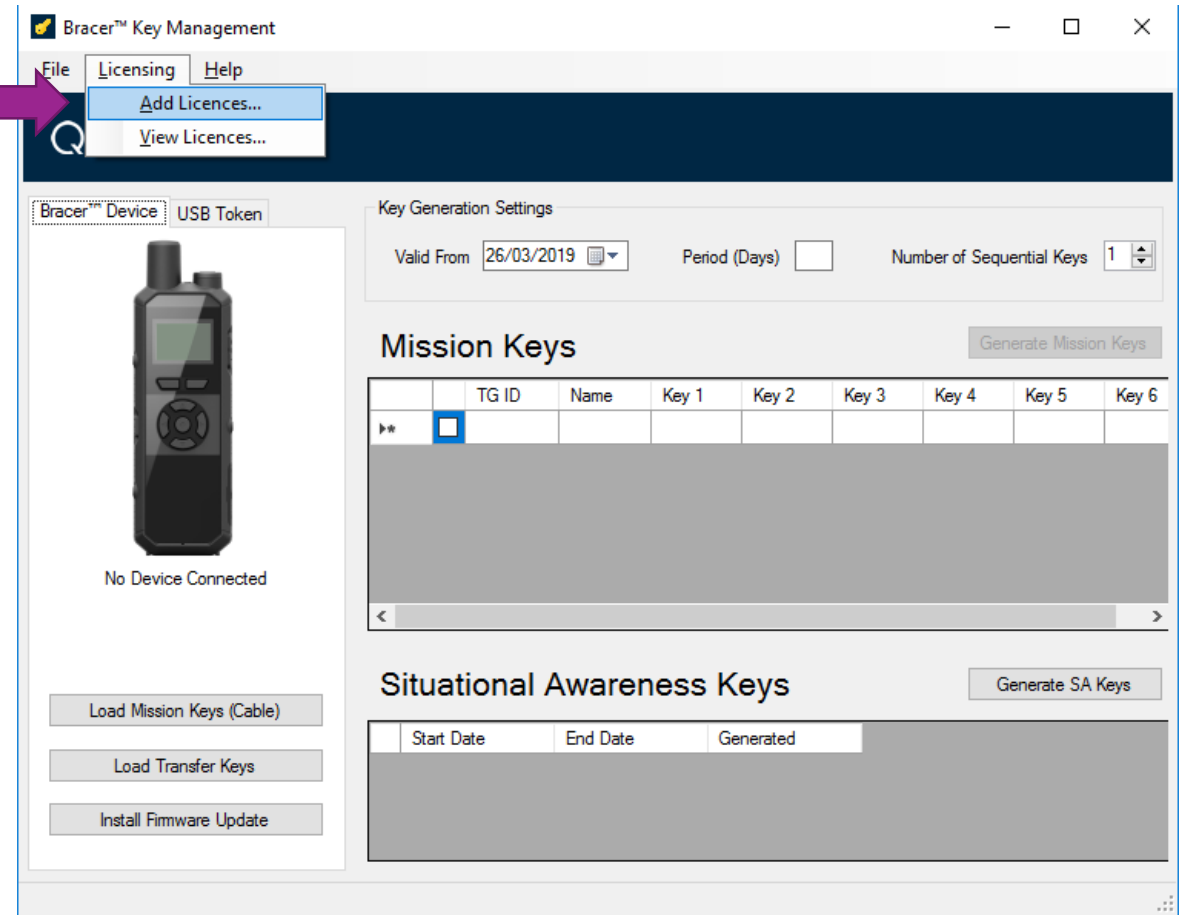
- Licence Files will be purchased through your supplier. The life of the licence will vary according to the support duration procured.



Bracer Licences

Loading the Licence

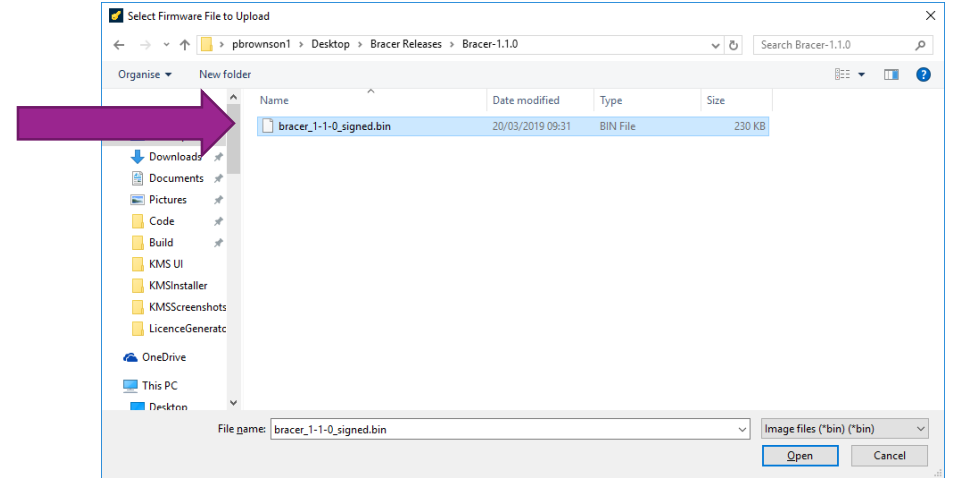
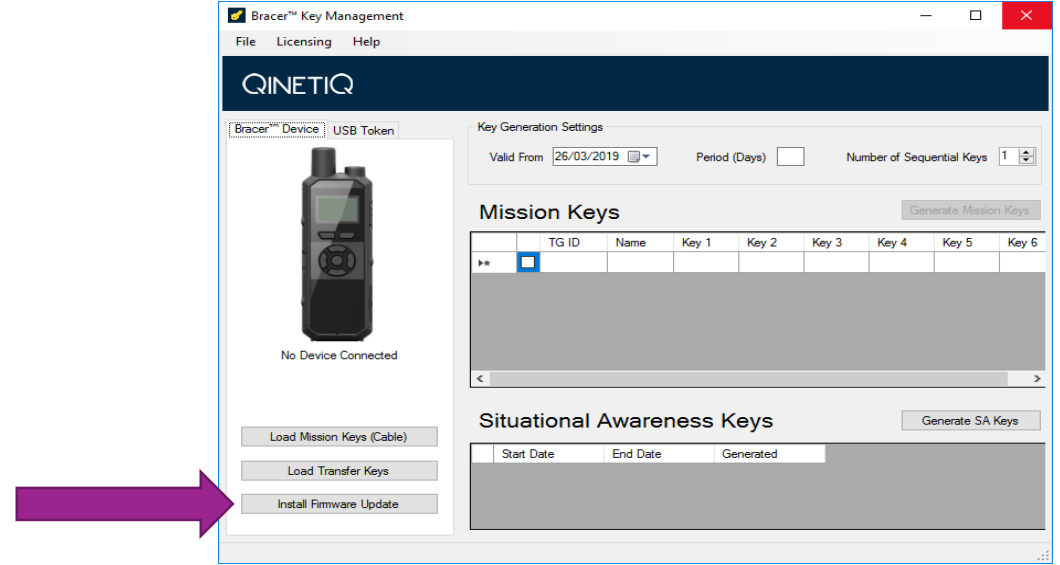
- Save the licence files to a disk (CD, USB, Hard Drive).
- Open Bracer Key Management Tool.
- Click on Add Licence (in Licencing Tab).
- Go to File with current licences.
- Select all relevant Bracer licences and press return.
- In the same Tab you can view existing licences. This shows licence serial numbers and when they are valid from and to.



Loading Firmware

Loading Firmware

- Switch Off Bracer Device.
- Connect Bracer audio ancillary.
- Press and hold PTT button on audio ancillary then press power on button. LED will flash blue.
- Connect device to PC/Laptop running Bracer Key Management tool.
- Open Bracer Key Management software.
- Click on Install Firmware update.
- Select latest firmware (.bin) from file. Double click.
- Bracer Key Management tool will load firmware.
- Device will boot up into Telephony mode.
- Switch off Bracer device.



BRACER Key Management System

- **Commission Device from New or Zeroise**

- Connect USB Token via USB Host cable.
- Switch on the handset by pressing and holding Power On/Off until device starts.
- Log in as user 00 with default passcode 123456.
- The device will assign and display a new passcode. **Record the new passcode.**
- Press 'Continue'. You will be logged out.
- Log in as user 00 using the passcode recorded above.
- From the 'Maintenance Menu', select 'User Management'.
- Select User 02 to enable user 02. This will generate and display a new passcode. **Record the passcode.**
- Select User 04 to enable user 04. This will generate and display a new passcode. **Record the passcode.**
- Click 'Continue'.
- Click 'Back' to return to the maintenance menu.
- Load Transfer Keys (section 5)..
- Load Mission Keys (section 6 or section 7 and section 8).

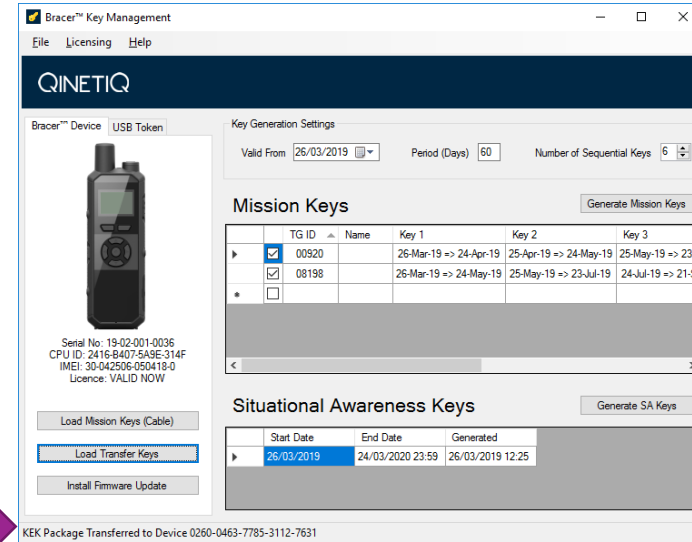
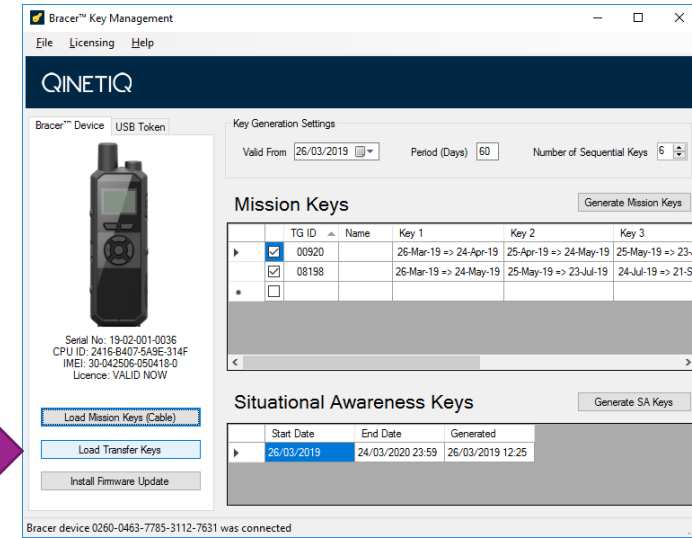
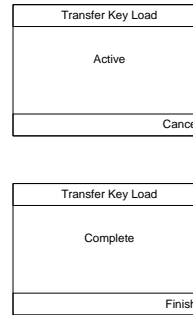
Maintenance Menu	
User Management	
Transfer Key Load	
Display Settings	
SA Options	
Select	Back

Maintenance Menu	
Device Information	
Shipping Mode	
Self Test	
Logout	
Select	Back

BRACER Key Management System

• Handset Initialise

- On zeroise or first use, the handset will have no keys loaded.
- The device must first be “paired” with the software by generation of a “Transfer Key” used to protect the import and export of keys.
- From Handset ‘Maintenance Menu’, select ‘Transfer Key Load’ – device will show Active.
- Connect Handset to laptop via USB cable.
- Bracer Key Management will ‘chime’ and show the device ID and IMEI and valid licence.
- Click Load Transfer keys.
- KEK Package Transferred To Device (*****)
- Handset will display ‘Complete’. Click Finish (right soft key).
- Disconnect handset from Key Management tool, will ‘chime’ on removal.
- Log out of Handset.



Talkgroup ID

The image shows two screenshots from the Iridium Everywhere mobile application. The left screenshot displays a map of North America with a pop-up window for a specific talkgroup. The right screenshot shows a map of Europe with a callout box.

Left Screenshot (North America):

- Map shows Iridium coverage over North America with the text "iridium Everywhere".
- Pop-up window details:
 - Talkgroup ID: 3795
 - Type: Standard : Voice+Data
 - Size: Small
 - Talkgroup Area: 100,000 / 100,000 km²
- Bottom navigation bar includes: Blue 1, info icon, 17 devices, search, location, and Saved.

Right Screenshot (Europe):

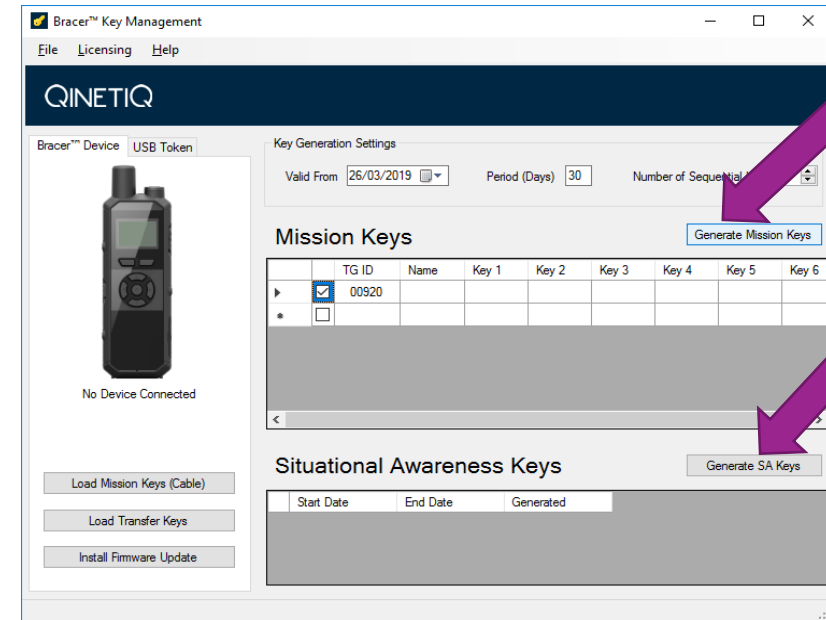
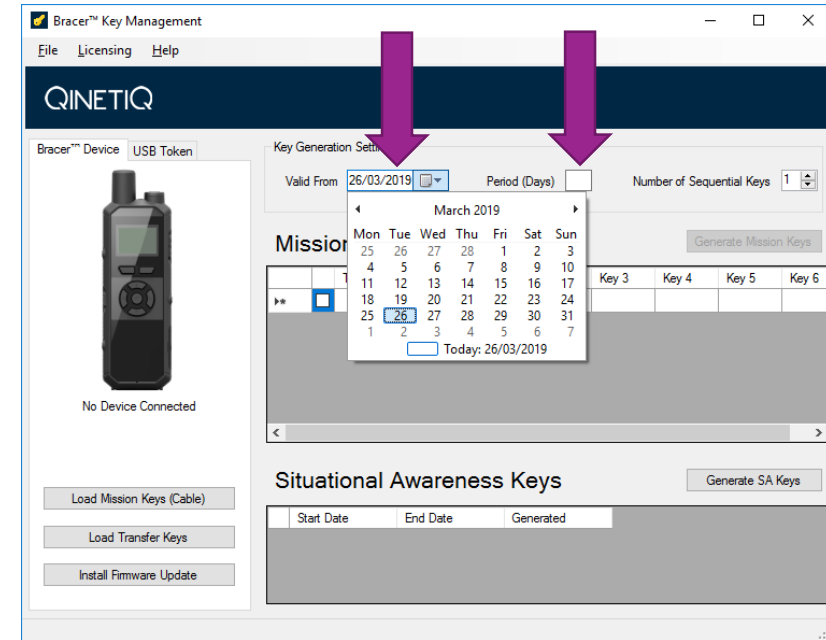
- Map shows Europe with a callout box pointing to London.
- Callout box text: "Talkgroup ID Essential for BKM to generate Key".
- Top navigation bar includes: Talkgroups, Devices, and a search icon.
- Map title: "QinetiQ Blue".

BRACER Key Management System

Generate Mission Keys

For each mission key:

- Enter Name (optional).
 - In the field at the top of the screen, set 'Valid From', 'Period', and 'Number of Sequential Keys'. The period is the length of time each key is valid for in days. The number of sequential keys is the amount of future keys to be generated (max 6).
 - Enter Talkgroup ID of the Talkgroups to be used as secure Talkgroups
 - Entry must be at least 5 characters long. Add a 0 at the beginning of TG IDs with 4 digits or less.
 - Tick the checkboxes beside the keys you wish to generate. Note: At least one mission key must be checked before the 'Generate Mission Keys' button is enabled.
 - Click 'Generate Mission Keys'.
- Generate SA Keys
 - Change Period of Days and Number of Sequential Keys as Required
 - Click 'Generate SA keys'.



BRACER Key Management

- **Export Mission Keys to file**

- Tick the checkboxes beside the keys you wish to export.
- Click the ‘Export ...’ button.
- In the Export Mission Keys dialog, select a folder and enter a filename.
- Click the ‘Save’ button.
- Enter a Password (8 or more characters) at the ‘Key File Password’ prompt.
- **NB – Ensure password is recorded as this will be required to import the keys back into the Key Management System.**



Bracer™ Key Management

File Licensing Help

Import Mission Keys...

Export Mission Keys...

Exit

Bracer™ Device USB Token

No Device Connected

Load Mission Keys (Cable)

Load Transfer Keys

Install Firmware Update

Key Generation Settings

Valid From 26/03/2019 Period (Days) 60 Number of Sequential Keys 6

Generate Mission Keys

	TG ID	Name	Key 1	Key 2	Key 3
▶	<input checked="" type="checkbox"/>	00920	26-Mar-19 => 24-Apr-19	25-Apr-19 => 24-May-19	25-May-19 => 23-Jun-19
	<input checked="" type="checkbox"/>	08198	26-Mar-19 => 24-May-19	25-May-19 => 23-Jul-19	24-Jul-19 => 21-Sep-19
*	<input type="checkbox"/>				

Generate SA Keys

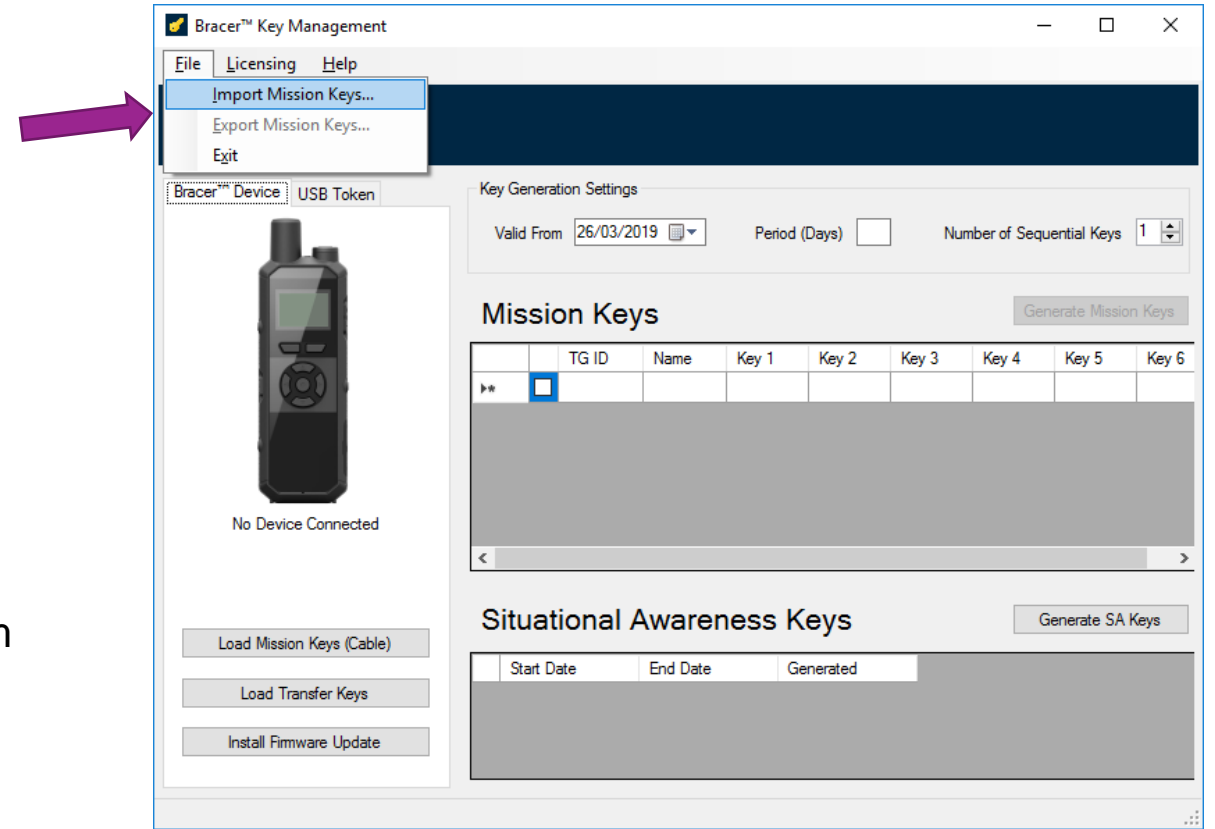
	Start Date	End Date	Generated
▶	26/03/2019	24/03/2020 23:59	26/03/2019 12:25

6 Mission Keys Generated

BRACER Key Management System

- **Import Mission Keys to file**

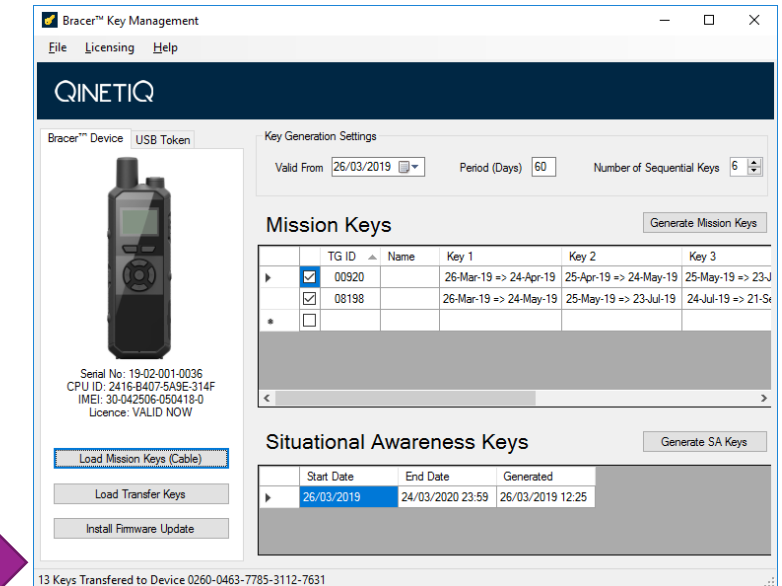
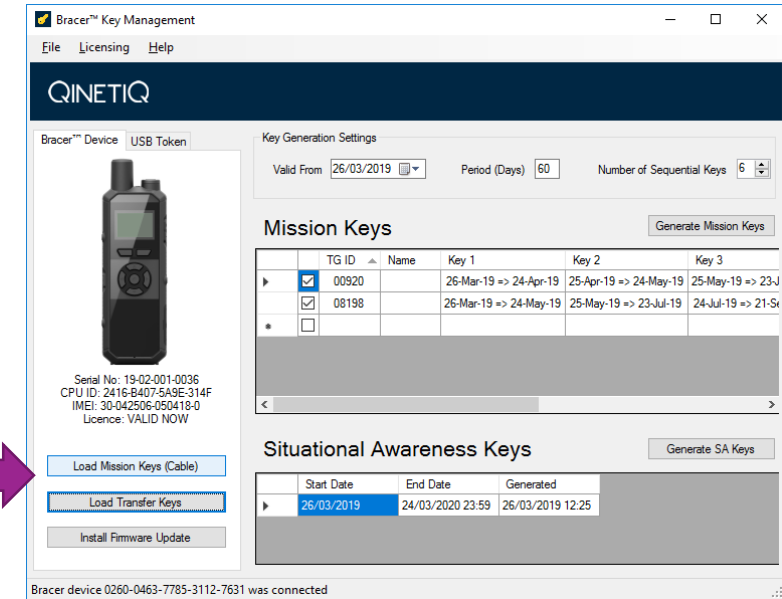
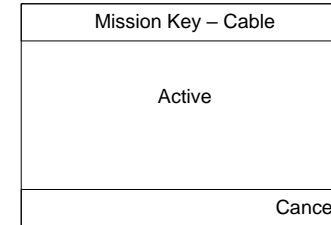
- Click on File.
- Click the ‘Import ...’ button.
- In the ‘Import Mission Keys’ dialog, select the folder and ‘.key’ file that you wish to import.
- Click ‘Open’.
- Enter Password for the file at the ‘Key File Password’ prompt.
- Ensure keys are displayed for required Talkgroup IDs (from Iridium Command Centre).



BRACER Key Management System

• Load Mission Keys (USB Cable)

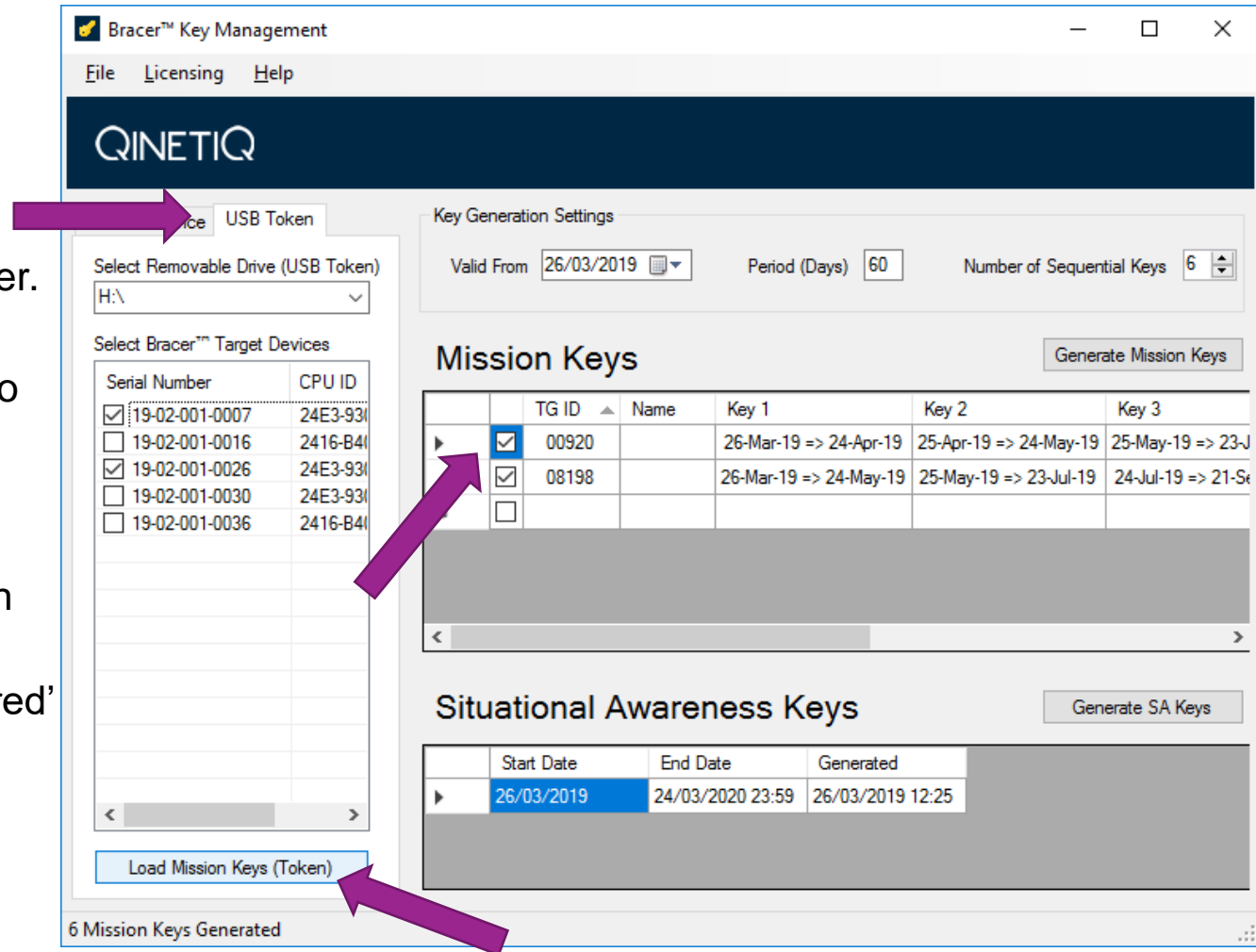
- Ensure TG keys are deleted on handset before reloading using the 'delete mission key' option – This can be done by TG if required
- From 'Main Menu', select 'Mission Key Load'. Then select 'Load via Cable'.
- Handset display will show 'Active'.
- Connect Handset to Key Management laptop via USB cable.
- Laptop will 'chime' on connection and show the device ID, IMEI and Licence.
- Tick the checkboxes beside the keys you wish to transfer.
- Click 'Load Mission Keys (Cable)'.
- The bottom line of Key Management Tool shows 'N keys transferred' – check that N is the number of keys you expected to transfer.
- Handset will show 'Complete N of N keys'.
- On Handset, click 'Finish' (right soft key).
- Disconnect handset from Laptop. Laptop will 'chime' on removal.
- Repeat as required for more handsets.



BRACER Key Management System

- **Load Mission Keys onto Token**

- Put a USB stick into Key Management Laptop.
- Tick the checkboxes beside the keys you wish to transfer.
- Click on the USB Token Tab.
- Select the handsets that you will want to transfer keys to using the USB stick (this action downloads the licences associated with each handset).
- Click 'Load Mission Keys Token'.
- In the 'Write Tokens to File' field, click the browse button and select the USB drive.
- The bottom line of BKM display shows 'N keys transferred'
 - check that N is the number of keys you expected to transfer.



BRACER Key Management System

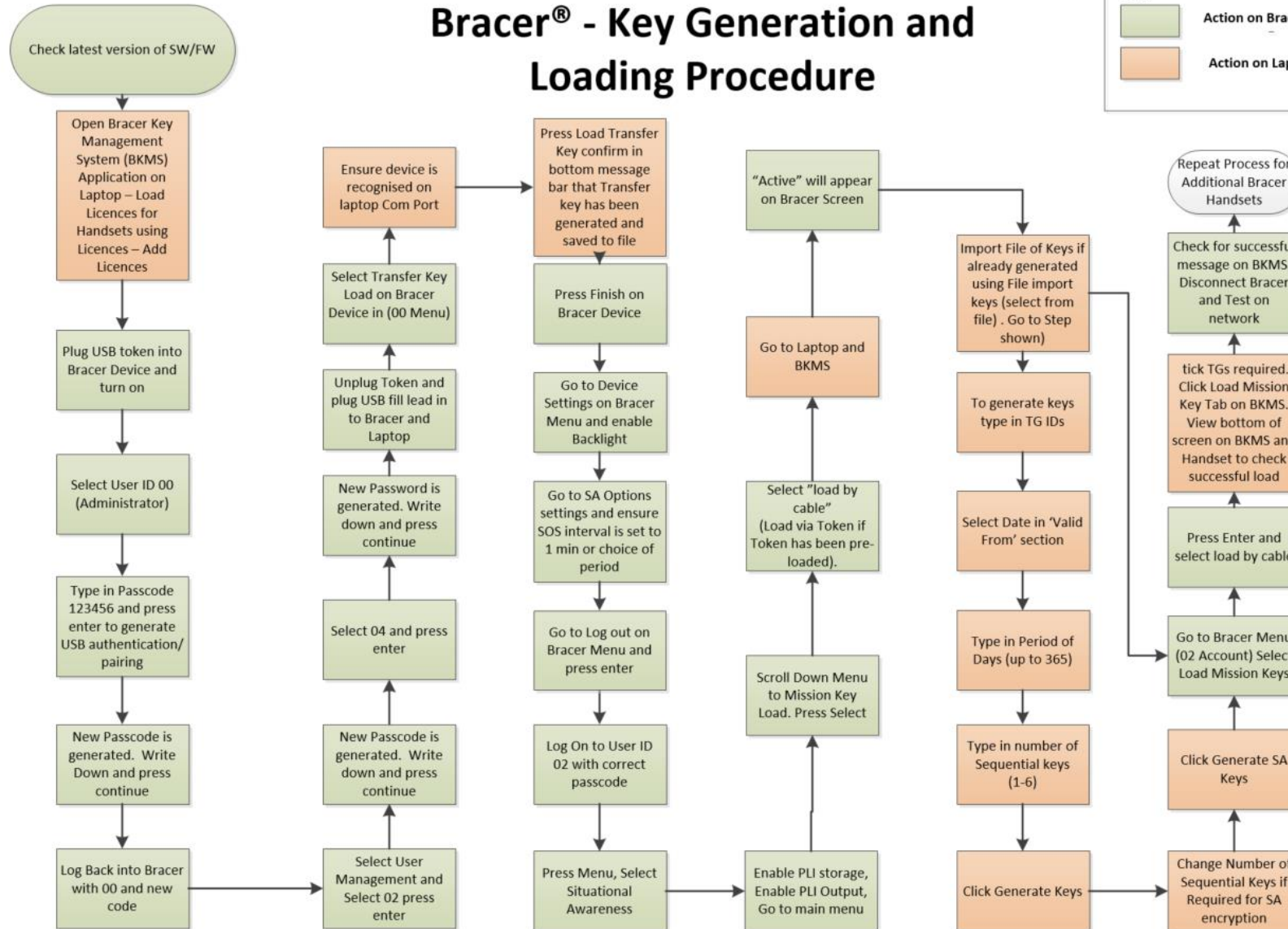
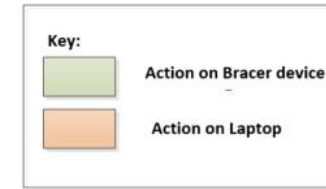
- **Load Mission Keys to device from Token**

- From 'Main Menu', select 'Mission Key Load' then select 'Load from Token'.
- Handset display will show 'Active'.
- Connect Token to handset via USB host cable.
- Screen will display that 'N' amount of keys have been transferred.
- Handset will display 'Complete'. Press 'Cancel' (or 'Finish') (right soft key).
- Disconnect token from Handset.

Mission Key – Token
Active
Cancel

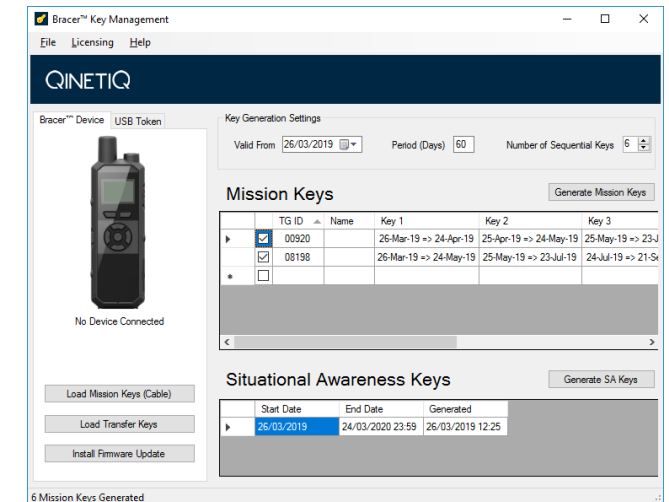
Mission Key – Token
Complete
Finish

Bracer® - Key Generation and Loading Procedure



Practical Demonstration + Training of KVMS system

1. Bringing a handset from zeroised state to fully operational and keys loaded.
2. Demonstrate Transfer key Generation.
3. Demonstrate Mission key and SA key generation, save and restore.
4. Demonstrate Mission key loading via device and token.



QINETIQ/EMEA/CIT/PUB1902044

BRACER™

Module 8

Situational Awareness



QINETIQ

This training material is subject to change without notification.

BRACER

QinetiQ Situational Awareness - Overview

There are 2 software packages that make up the QinetiQ Situational Awareness Tool:

QinetiQ Situational Awareness (QSA) Software Application (*this document*).

- This application receives, decrypts and stores PLI messages received in real time from a connected Bracer handset. It is also used to raise the alarm when Emergency alert messages are received.

QinetiQ BURT Software Application

- This application is used to inject the Bracer PLI messages into mapping packages such as a Graphical Information System (GIS) in order to display the locations of Bracer Assets on a map. The application receives the decrypted PLI messages from the QSA software and allows the user to inject them into a variety of mapping packages. It allows call signs and map symbols to be managed and also allows for multiple mapping package formats to be injected simultaneously.
- As a default, the QinetiQ BURT application will output for presentation of PLI on Google Earth. Additional translations are available, for other mapping and GIS tools, if required – please contact QinetiQ's Bracer Support Desk if you do wish to use other tools.

QinetiQ Map Injector (QMI)

QMI is a software that does the same function as BURT Lite but is a non-export controlled variant. QMI currently ingests CoT or KML. QSA has different versions to work with BURT Lite and QMI

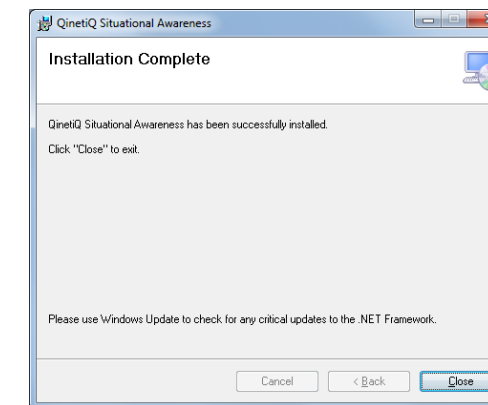
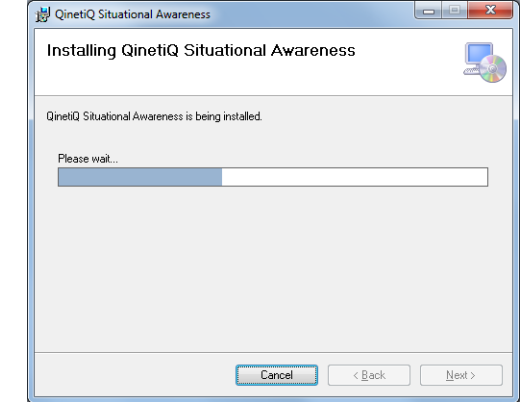
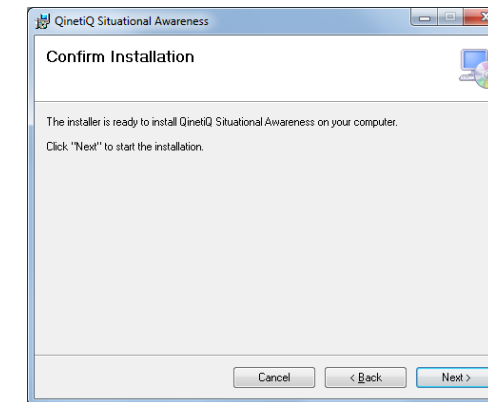
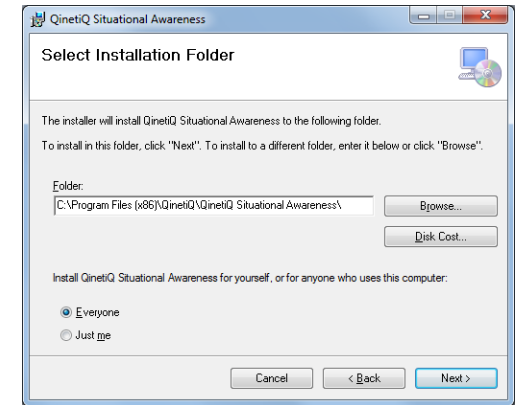
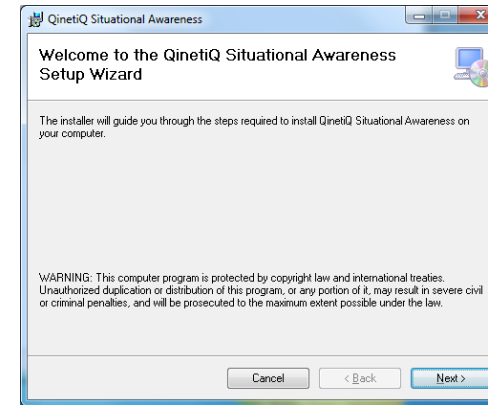
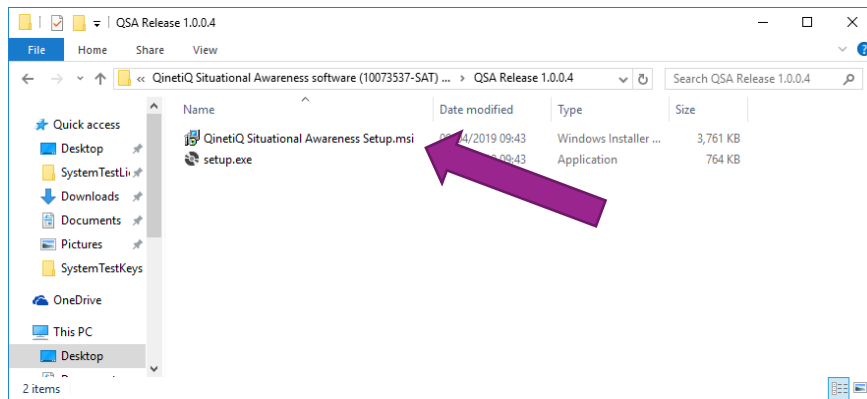
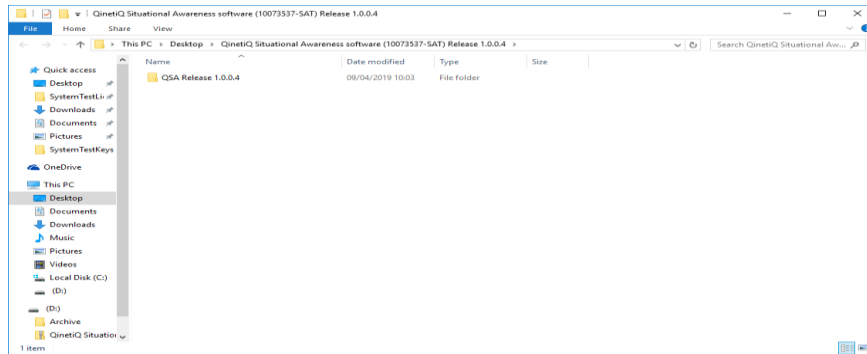
Laptop / PC Specification

The following is the minimum specification of a Laptop or PC to run the Situational Awareness Tools

Operating System	Windows 10
Processor	1GHz (minimum required to run Windows 10 and .NET)
RAM	1GB (minimum required to run Windows 10)
Available Hard Drive/SSD Storage	1.5GB (installed applications only), plus log files
Display Resolution	800 x 600

Installing QinetiQ Situational Awareness

Select QSA exe file and install software following guide on the Wizzard.

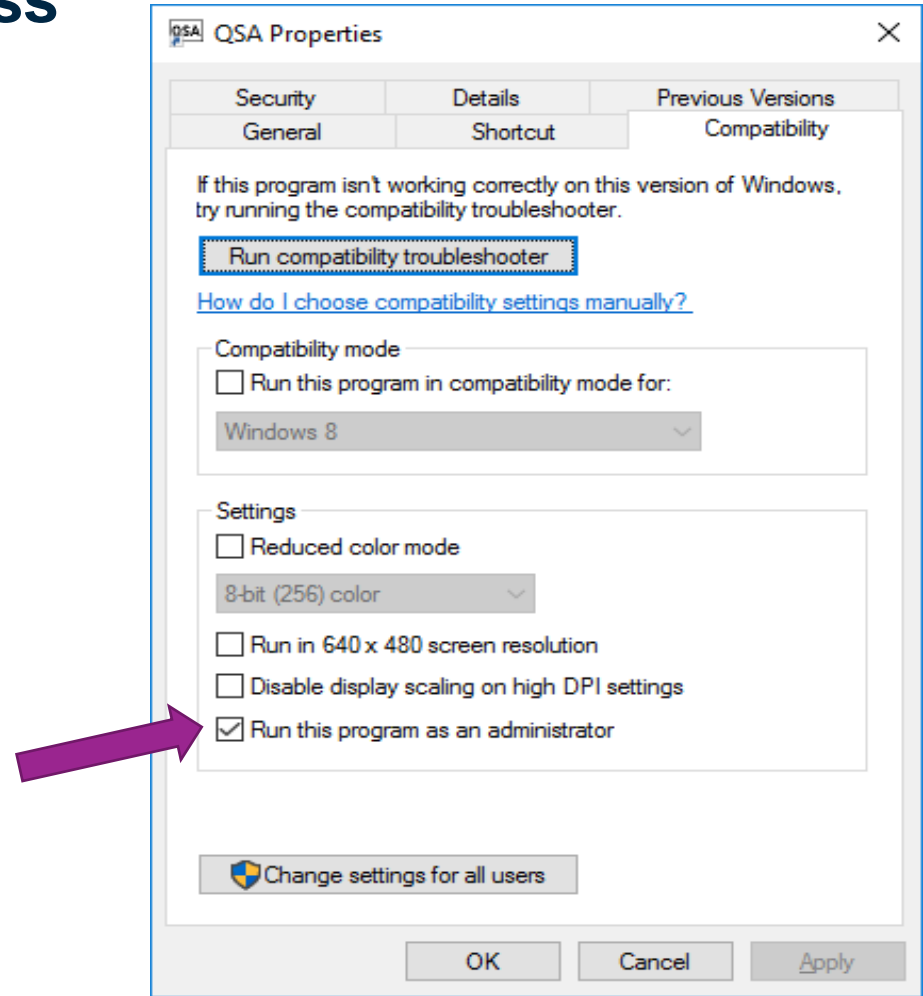


Initial Boot Up - QinetiQ Situational Awareness



QSA Icon will appear on Desktop.

NB – It is recommended that the properties are set to ‘Run this program as an administrator’, by right-clicking the desktop icon and selecting ‘Properties’, and checking the appropriate box under ‘Settings’ in the ‘Compatibility’ panel.

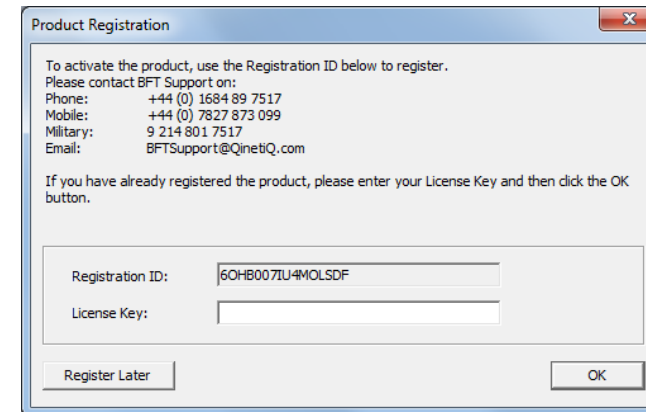
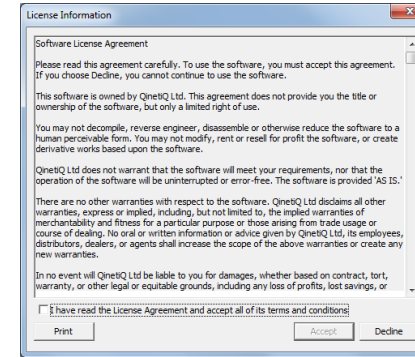
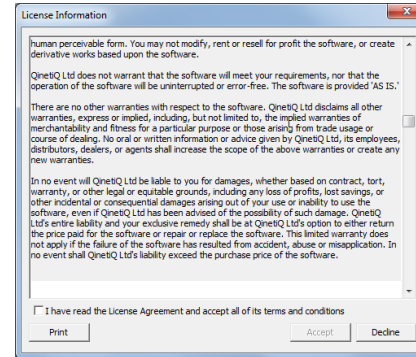


Initial Boot Up - QinetiQ Situational Awareness



Click on Desktop Icon

- Continue install process. Once ready to accept the Licence Agreement, tick the box and then press accept.
- **Registration Key** – the install will request a product registration key. Call or email the contact details stated in the dialogue box and state the Registration ID number. A key will be issued. Type in and click OK.
- **NB** – This licence is specific to the laptop/PC that it has been loaded onto. If the software is to be loaded onto other laptops/PCs another licence key will need to be requested.

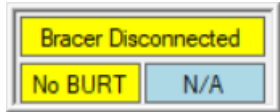


Be aware that all letters are capitalised and the number zero “0” looks similar but is different to a capitalised “O”. Also capitalised “i” is “I”, capitalised “l” is “L” and number one is “1”.

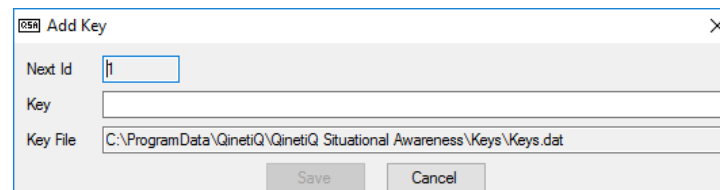
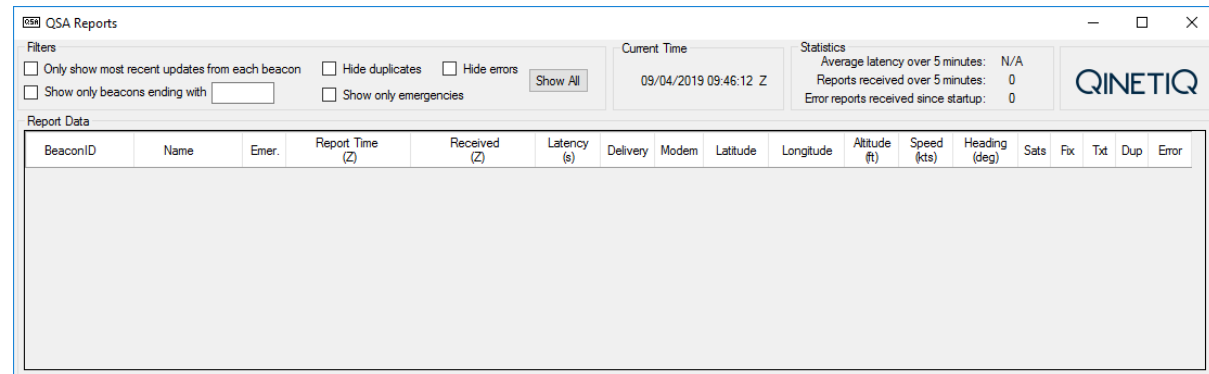
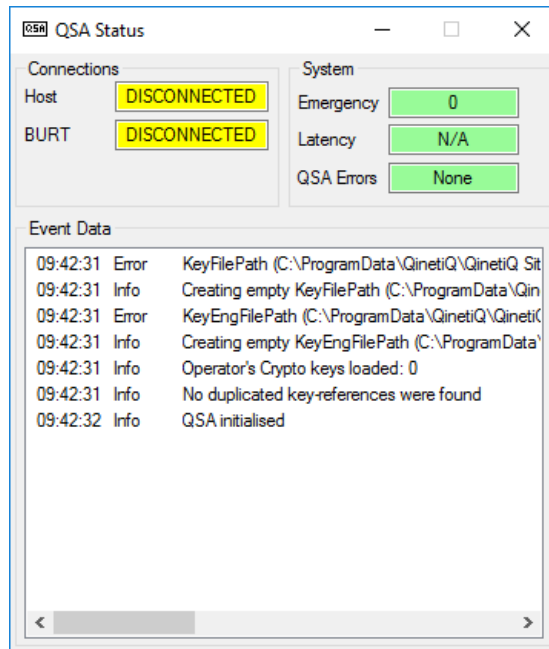
Opening QinetiQ Situational Awareness



Click on Desktop Icon.



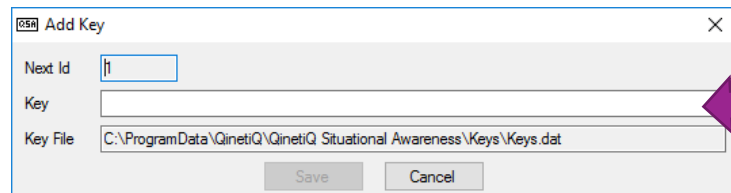
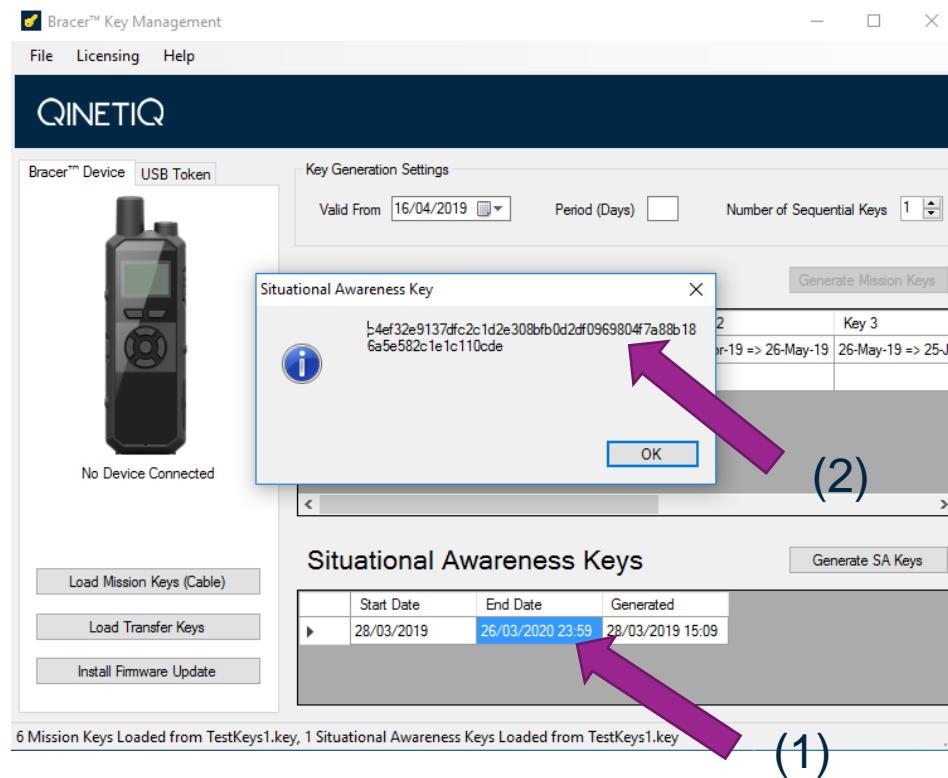
The software will now launch and the QSA 'Always on top' window will appear. Right click this to open up the Status window (Show Status), Reports window (Show Reports) and Bracer SA Key entry window (Add Key).



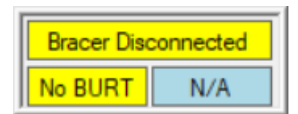
Adding the Situational Awareness Key

Open Bracer Key Management tool and ensure it has the mission key and SA key loaded. Click on Situational Awareness end date (1) and the key will appear in a dialogue screen. Highlight and copy key (Ctl+C) (2).

Switch to QSA Add Key (Right click on QSA activity ICON (3) and paste the key into the key space. Then click Save (4). Once complete **Close QSA and re-open**. QSA is now ready to use.



(3)



Installing BURT Lite

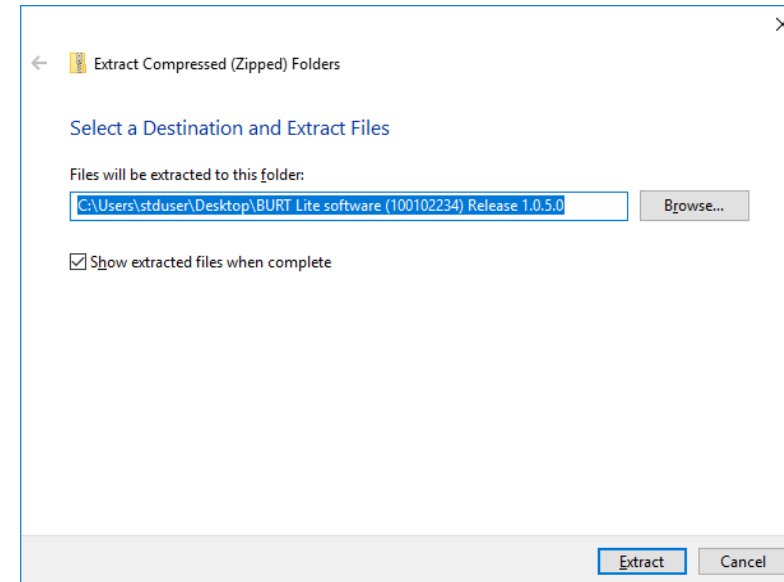
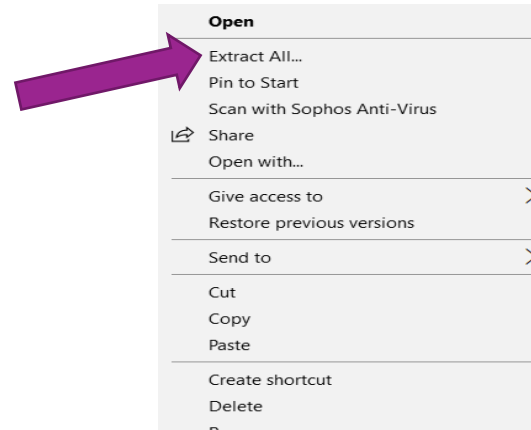
Installing Blue Force Tracking Universal Real-Time Translator (BURT) Lite

Installing the Software

When the 'BURT Lite software (100102234) Release x.x.x.x.zip' file is in place on the target PC, right click on the file to initially extract the installer applications to a local folder on the PC.

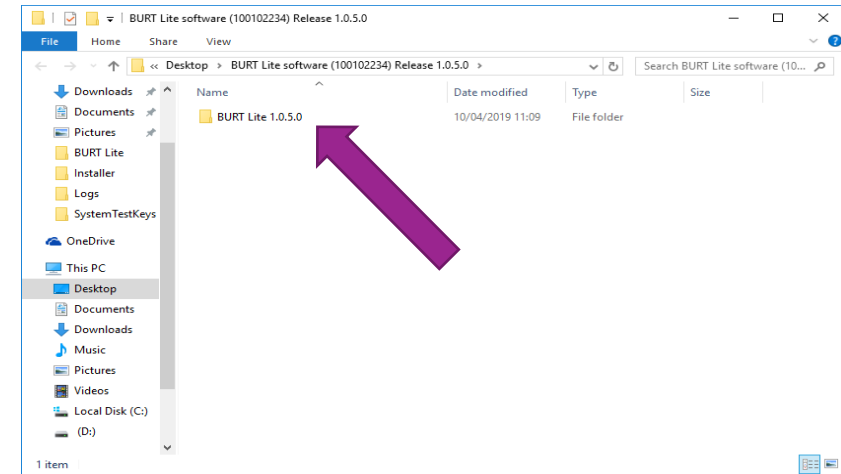
You will see the popup menu below – please click the 'Extract All' button to continue.

A popup window will prompt for a location to extract to. Enter the desired folder location and click 'Extract':



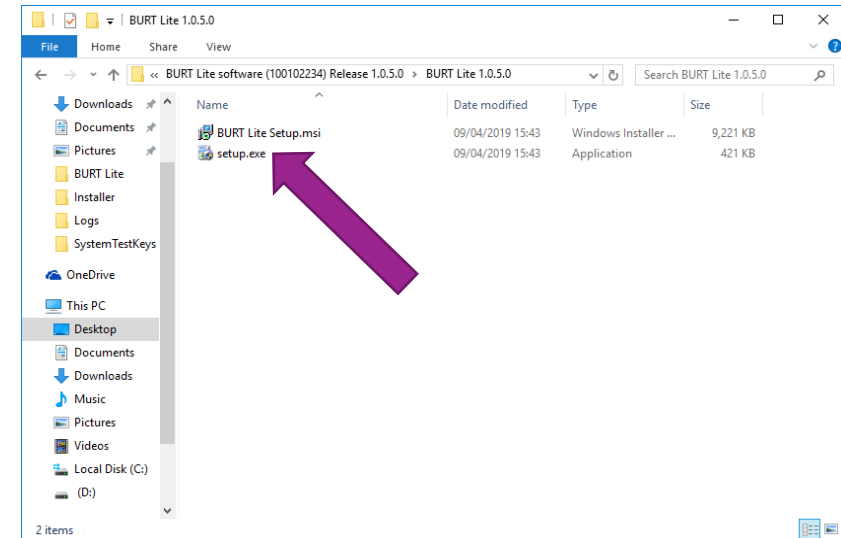
Installing Blue Force Tracking Universal Real-Time Translator (BURT) Lite

A folder will then open with the extracted contents shown. There should be a folder 'BURT Lite x.x.x.x'. The x's represents the version number.



Installing BURT

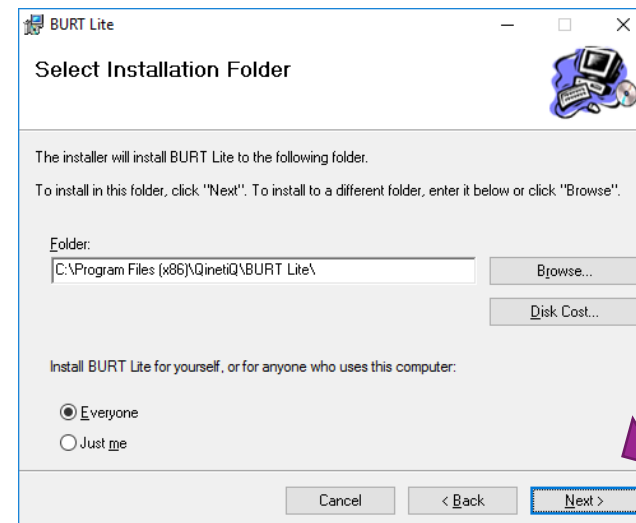
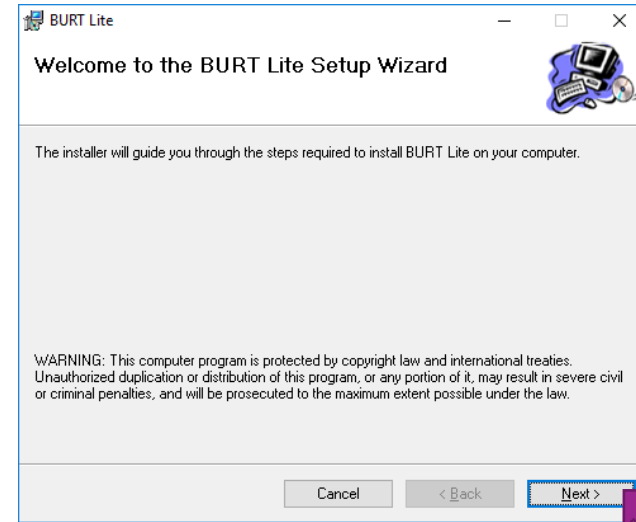
Open the BURT Lite folder and double click the 'setup.exe' file.



Installing Blue Force Tracking Universal Real-Time Translator (BURT) Lite

You will then see the popup window below. Click 'Next' to continue:

You will then see the popup window below. Unless you have a reason not to, please accept the recommended installation folder by clicking on the 'Next' button:



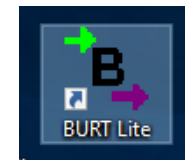
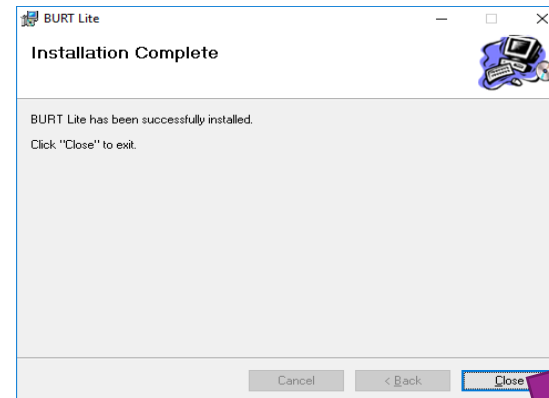
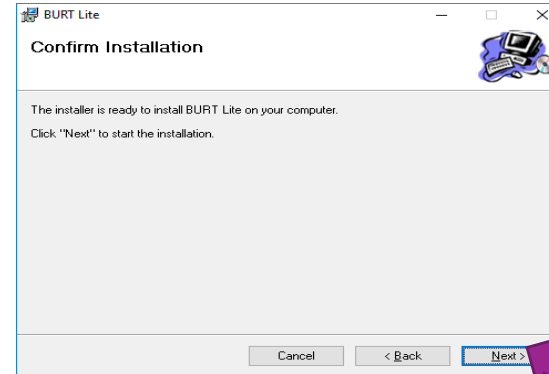
Installing Blue Force Tracking Universal Real-Time Translator (BURT) Lite

You are now ready to begin the installation process itself (see below). Please click on the 'Next' button, to proceed with installation.

When the installation process has completed, you will see the popup window below. Please click on the 'Close' button to close the Setup Wizard.

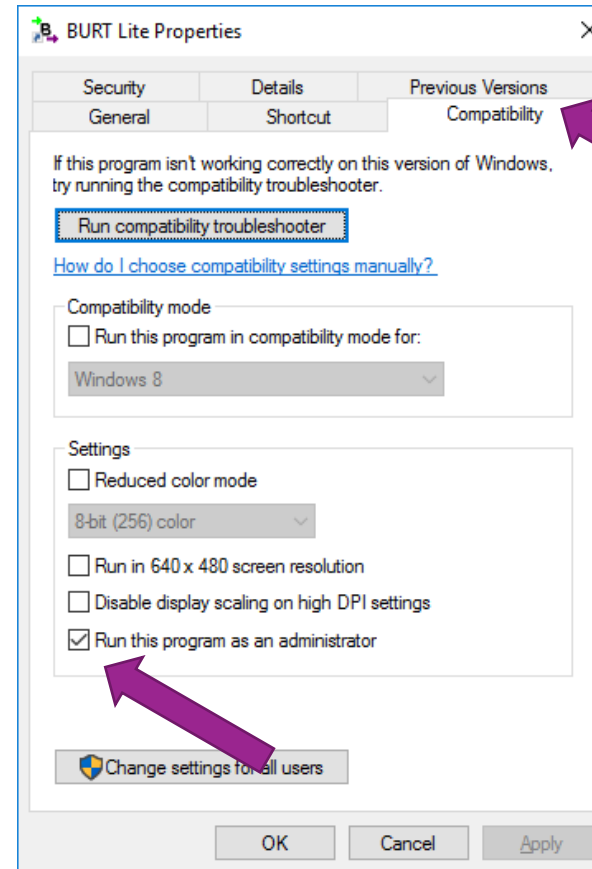
Close the window.

A BURT icon will have been placed on the desktop.



Installing Blue Force Tracking Universal Real-Time Translator (BURT) Lite

It is recommended that the properties are set to 'Run this program as an administrator', by right-clicking the desktop icon and selecting 'Properties', and checking the appropriate box under 'Settings' in the 'Compatibility' panel.

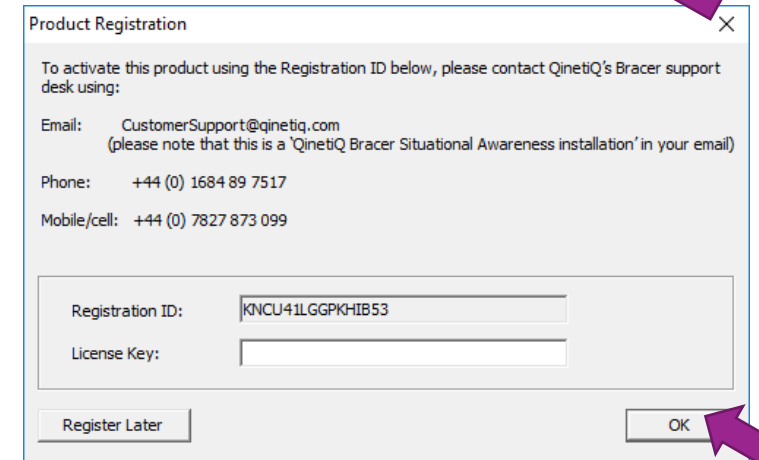
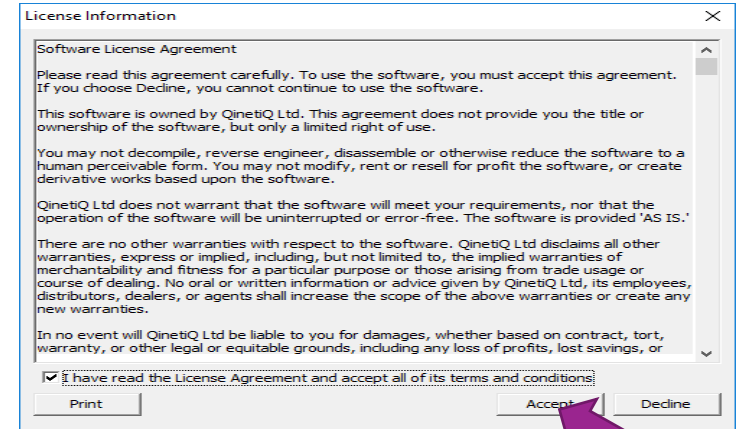


Installing Blue Force Tracking Universal Real-Time Translator (BURT) Lite

- Double click the icon to run BURT for the first time or run from the start menu – ‘BURT Lite’.
- On first time run, a Software licence agreement box will appear. If you agree, tick the ‘I have read the License Agreement and accept all of its terms and conditions’ box and then ‘Accept’ to continue.

Next a Software Activation window will appear:

- Please contact QinetiQ’s Bracer support desk by email and supply the Registration ID presented in the box. Be aware that all letters are capitalised and the number zero “0” looks similar but is different to a capitalised “O”. Also a capitalised “i” is “l”, capitalised “l” is “L” and number one is “1”.
- QinetiQ will email a License Key by return. Enter this into the License key box exactly as presented and click ‘OK’.

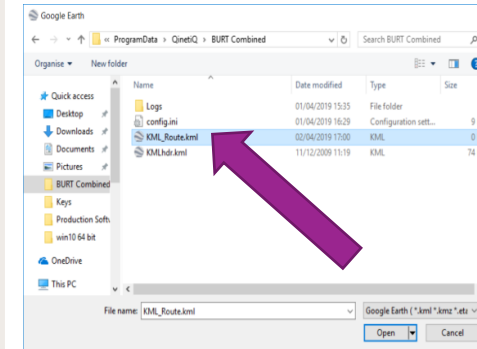
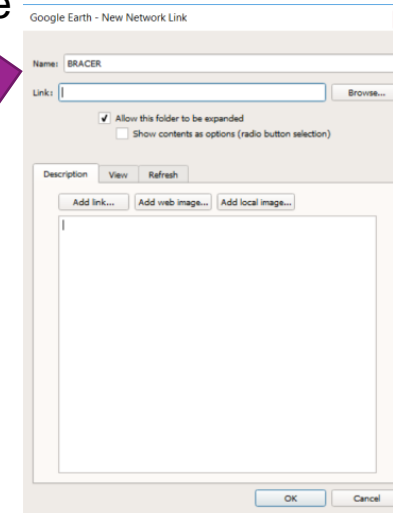
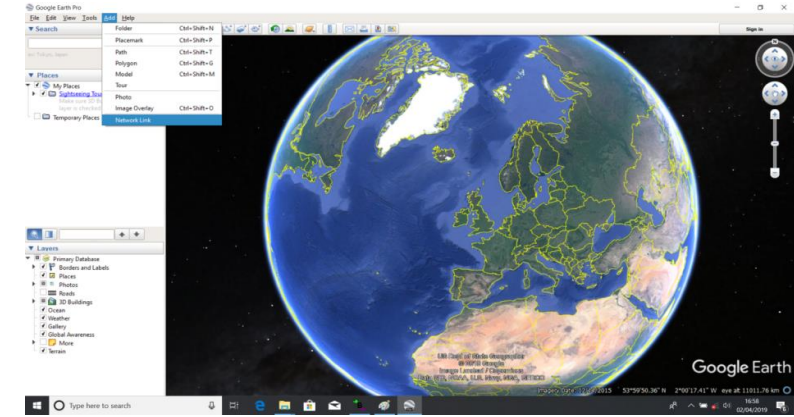


Note: If you have already installed QSA, this step may not be necessary.

Installing Google Earth Pro

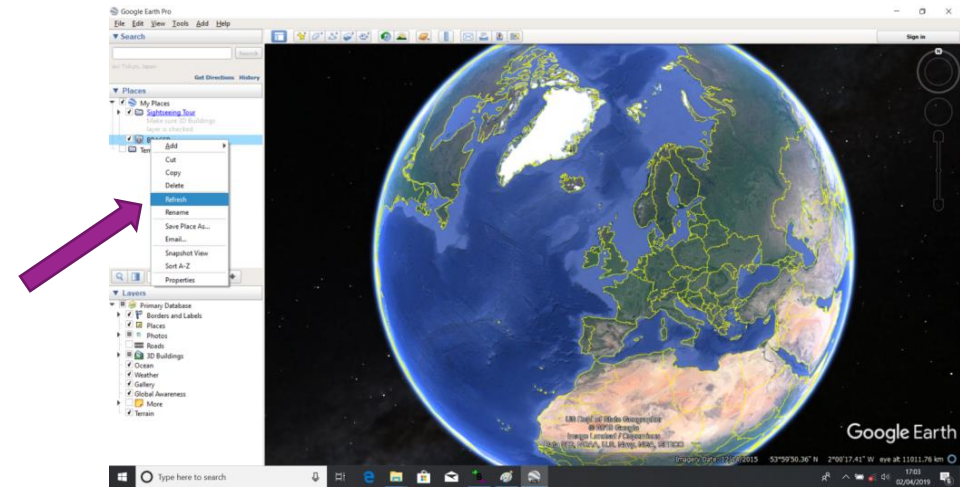
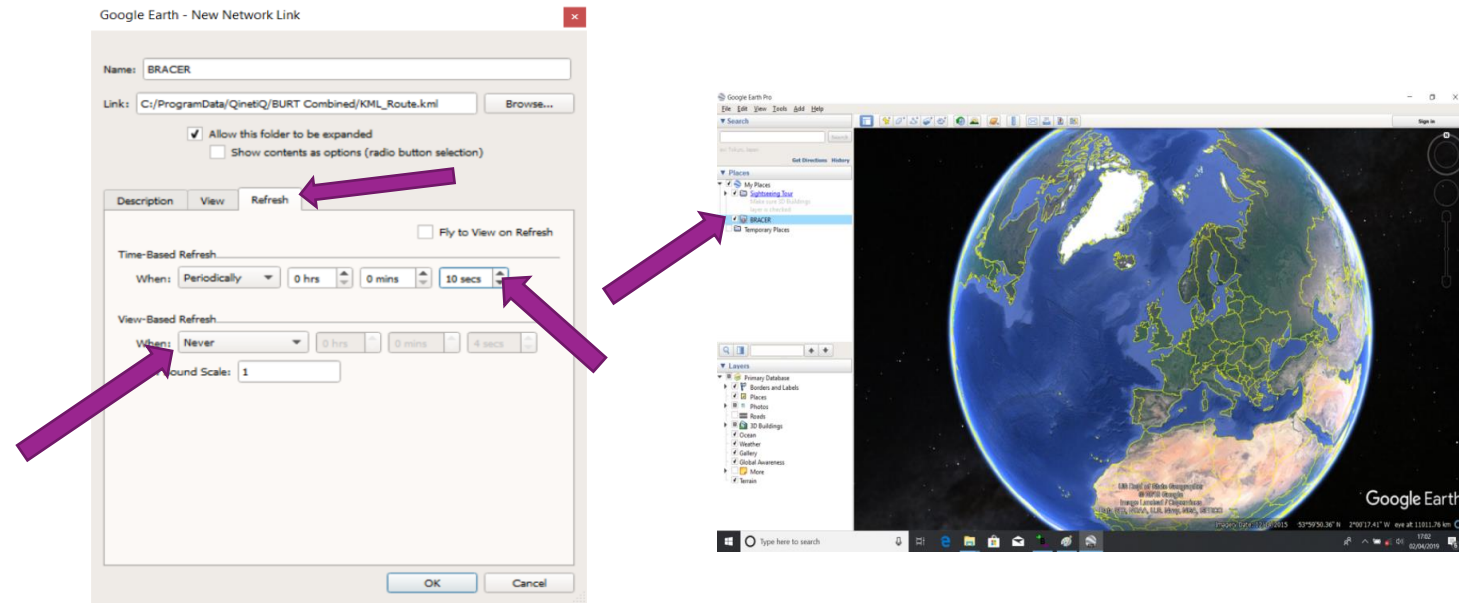
Downloading Google Earth Pro

- Download and install the latest version of Google Earth Pro from the Internet.
- To display BRACER PLI in Google Earth, set up as follows:
 - Open Google Earth Pro.
 - Click on “Add” and then Network Link:
 - Type in name as “BRACER”
 - Click “Browse” for Link location. Browse to “C:/ProgramData/QinetiQ/BURT Lite” and select file “KML_Route.kml”, and click “open”.
- **Note:** IF QSA and BURT have not been run previously and successfully received a BRACER PLI messages since first installation, the KML_Route.kml file will not be present. Run QSA and BURT, connect a BRACER handset and generate BRACER PLI on the talkgroup and the KML_Route.kml file will be instantly generated and updated thereafter.



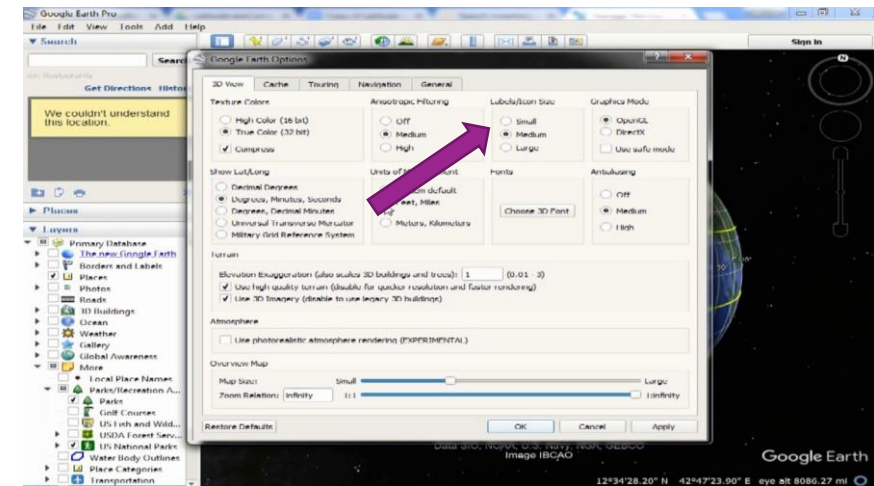
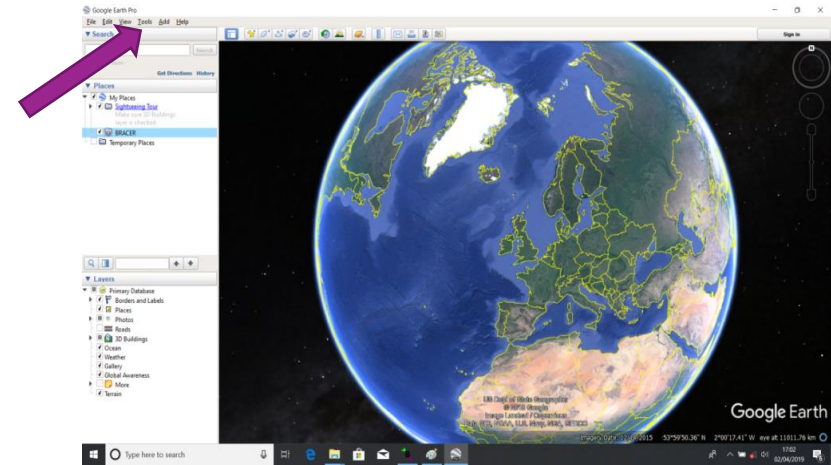
Downloading Google Earth Pro

- Select the “Refresh” tab. Set “Time-Based Refresh” to “Periodically” and 0 hrs, 0 mins, 5 secs.
- Leave “view based refresh” as “Never”
- The BRACER SA link should appear in “My places” in the left hand pane.
- Click “File” and “Save My Places” to save the link.
- **NB** - If the link gets frozen, symbolised by a red dot on the bracer folder symbol in “my places” instead of a green dot, right click on the BRACER link, and select “Refresh”.



Setting up ICON sizes in Google Earth

- Select tools tab.
- Select Options.
- Select 3D View tab.
- Select required size (Small, Medium, Large).

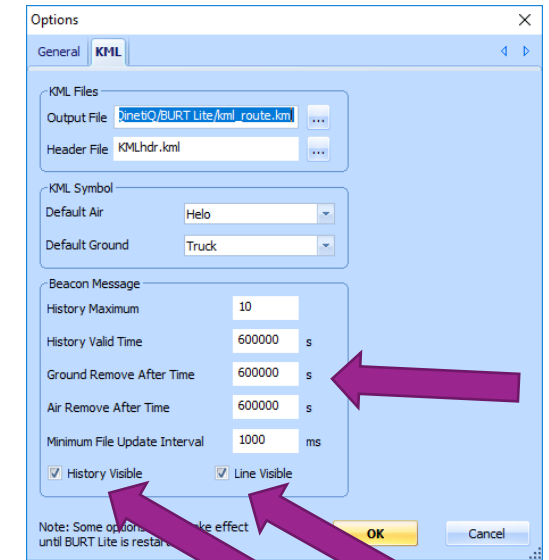
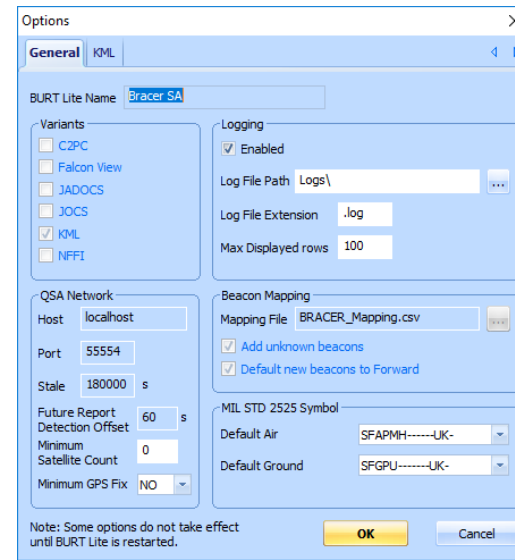
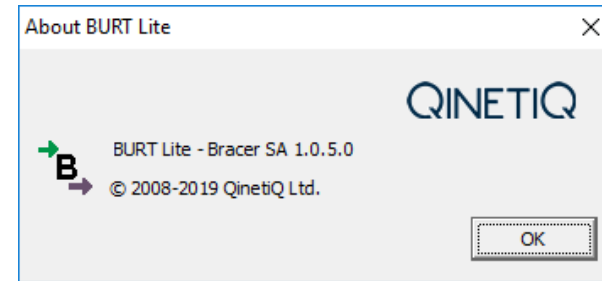


Opening and Setting up QSA and BURT Lite

Setting Up BURT Lite

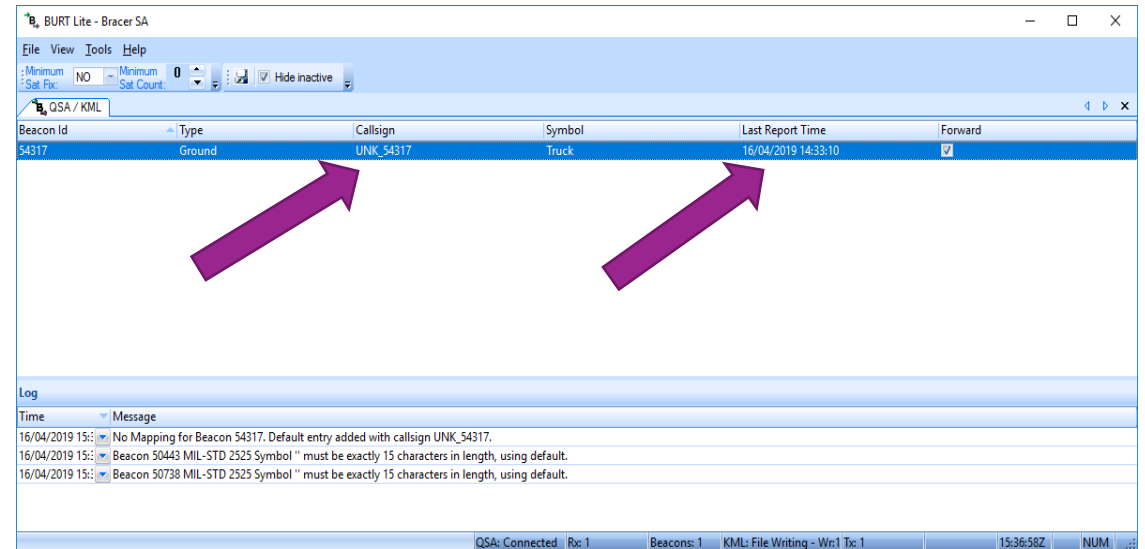
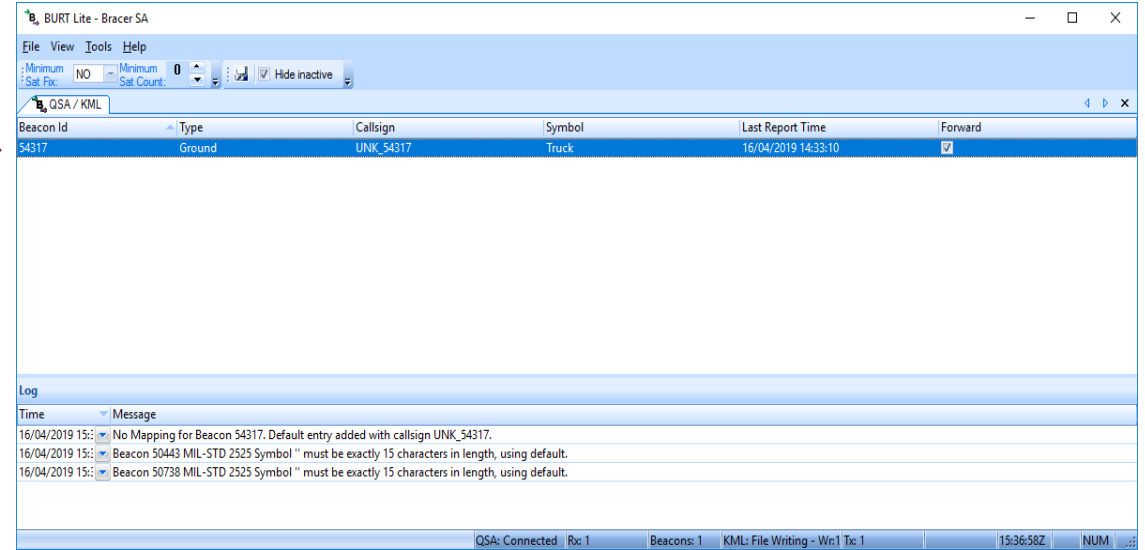
Maximise BURT Lite:

- Click on Help and select About BURT Lite. This allows you to check the version you are running.
- Click on Tools, then Options.
- Click on KML.
- Ensure that Beacon message History valid time is set to required setting. Recommendation is 600,000 seconds (Maximum setting).
- Ensure that history and line tick boxes are ticked.



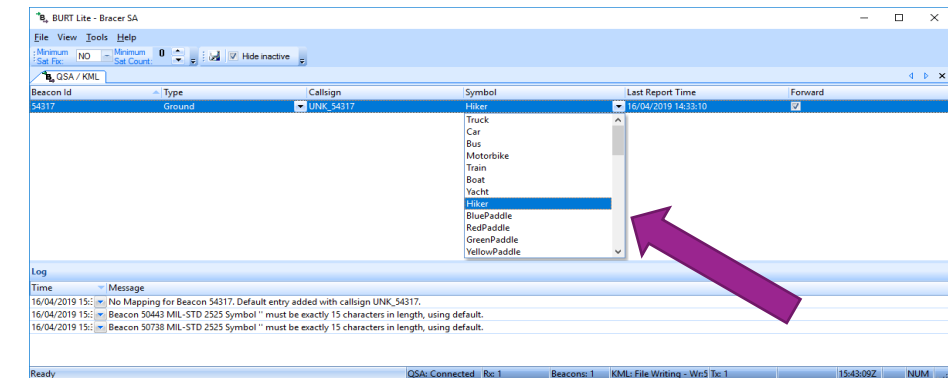
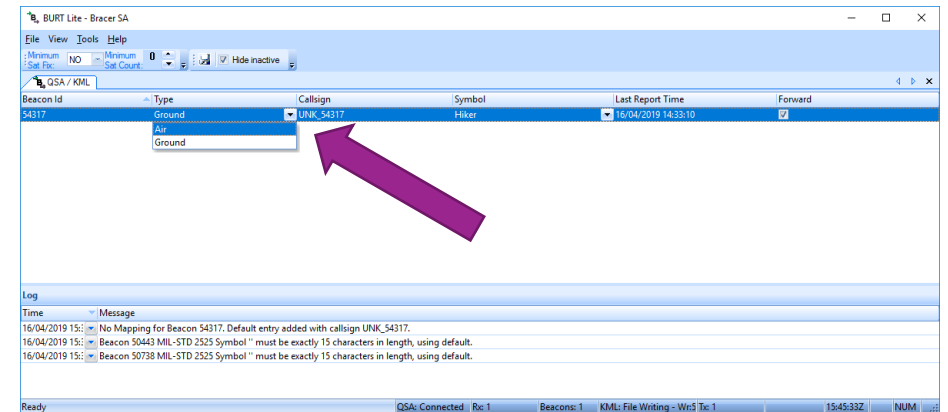
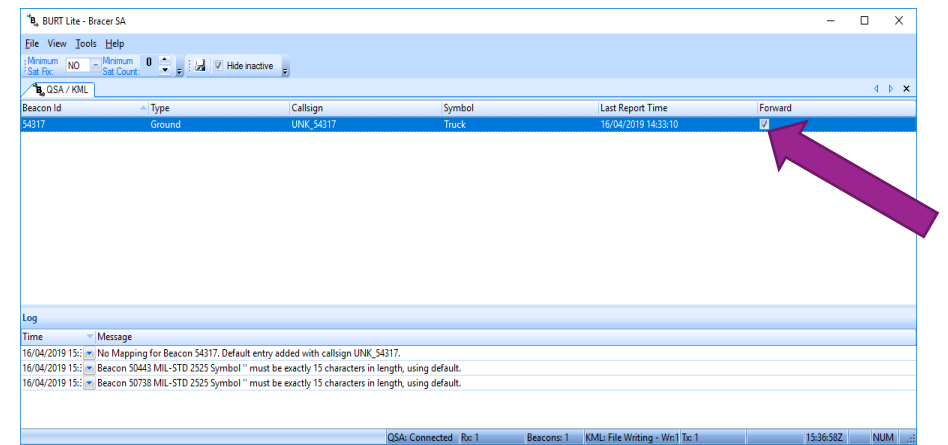
Setting up BURT Lite

- When a PLI message is received it will be decrypted by QSA and forwarded to BURT Lite. This will appear in the application.
- If Beacon callsign shows UKN (this mean unknown). Click on the callsign so that it highlights the text and rename to desired name.
- Last report time will show the last time a message was received from that beacon.



Opening BURT Lite

- Double click the icon to run BURT (if not already running).
- Ensure that Forward tick box is ticked.
- To change ICON images select type (Ground or Air)
- This corresponds to a different menus in the Symbol column. Select desired ICON.

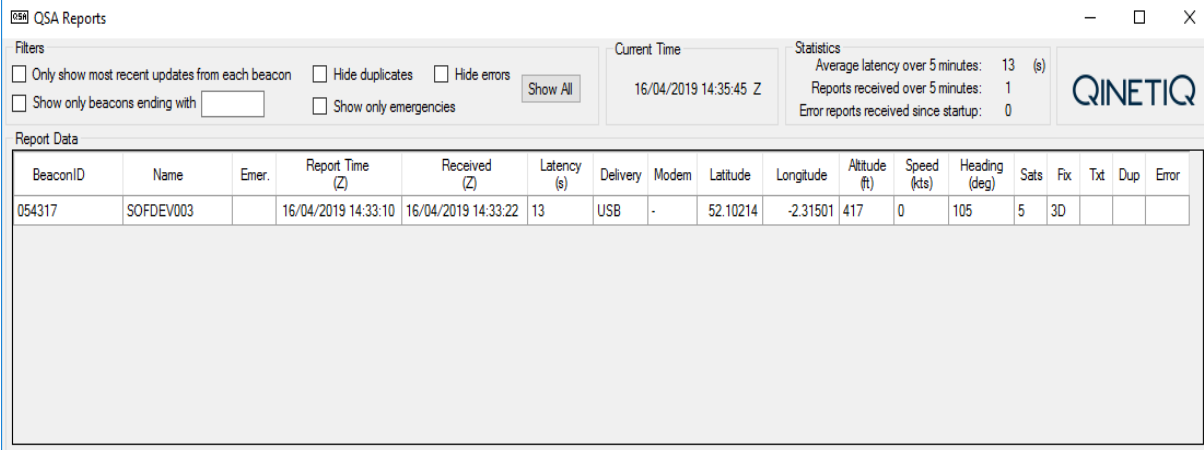


Opening QSA

Double click the icon to run QSA (if not already running)

When beacon messages are received the table will be populated with:

- Beacon ID (last 6 of IMEI less the last zero)
- Name of the Bracer device as labelled in Command Center.
- Report Time (the GMT time the message was sent).
- Received Time (the time the message was received – time taken from the computer clock – therefore ensure computer clock is set to GMT).
- The latency of report (this will also take into consideration any difference between computer clock and GPS).





The screenshot shows the 'QSA Reports' application window. It features a 'Filters' section with checkboxes for 'Only show most recent updates from each beacon', 'Hide duplicates', 'Hide errors', 'Show only beacons ending with', and 'Show only emergencies'. A 'Current Time' field displays '16/04/2019 14:35:45 Z'. A 'Statistics' section shows 'Average latency over 5 minutes: 13 (s)', 'Reports received over 5 minutes: 1', and 'Error reports received since startup: 0'. The 'Report Data' table is as follows:

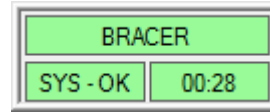
BeaconID	Name	Emer.	Report Time (Z)	Received (Z)	Latency (s)	Delivery	Modem	Latitude	Longitude	Altitude (ft)	Speed (kts)	Heading (deg)	Sats	Fix	Txt	Dup	Error
054317	SOFDEV003		16/04/2019 14:33:10	16/04/2019 14:33:22	13	USB	-	52.10214	-2.31501	417	0	105	5	3D			

Running the Bracer SA Tools

Open the applications in the following sequence:

- Open Google Earth (Connect to internet as required to cache mapping).
- Open BURT Lite  (Accept changes to device if requested).
- Open QSA  (Accept changes to device if requested).
- Connect Bracer Handset using USB programming lead.
- Ensure Handset is set up in Super User (02/03 account).
- Go to Situational Awareness Menu on Bracer Handset.
- Ensure that SA Storage and SA Output are both enabled (It will read disable in screen if it is enabled).
- Go to top menu and select 'Mission Key Load'.
- Select load via cable and then cancel – you should hear USB connect tones.
- The handset is now ready to receive SA reports and export to the applications.

Using the QSA Tool Suite



The most effective operating tools once set up are the QSA table and the GIS (e.g. Google Earth Pro) applications.



QSA Reports

Filters: Only show most recent updates from each beacon Hide duplicates Hide errors Show only beacons ending with [] Show only emergencies

Current Time: 16/04/2019 14:35:45 Z

Statistics: Average latency over 5 minutes: 13 (s), Reports received over 5 minutes: 1, Error reports received since startup: 0

Report Data

BeaconID	Name	Emer.	Report Time (Z)	Received (Z)	Latency (s)	Delivery	Modem	Latitude	Longitude	Altitude (ft)	Speed (kts)	Heading (deg)	Sats	Fx	Tx	Dup	Error
054317	SOFDEV003		16/04/2019 14:33:10	16/04/2019 14:33:22	13	USB	-	52.10214	-2.31501	417	0	105	5	3D			

BURT Lite - Bracer SA

File View Tools Help

Minimum Sat Fix: NO Minimum Sat Count: 0 Hide inactive

QSA / KML

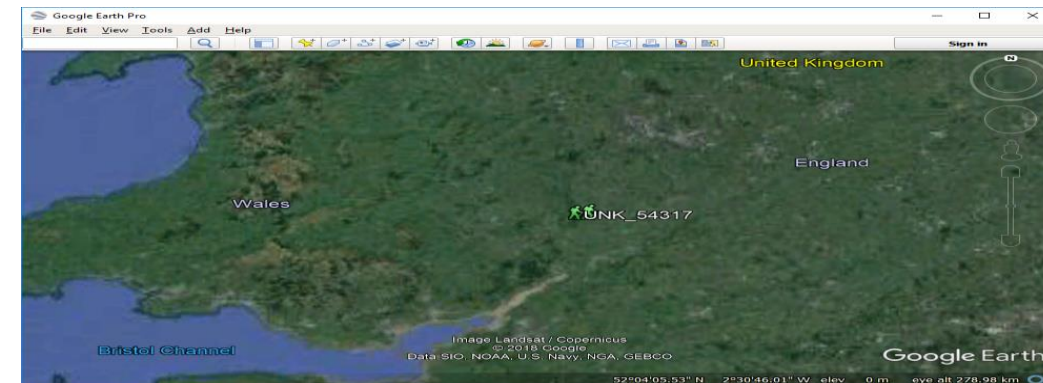
Beacon Id	Type	Callsign	Symbol	Last Report Time	Forward
54317	Ground	UNK_54317	Truck	16/04/2019 14:33:10	<input checked="" type="checkbox"/>

Log

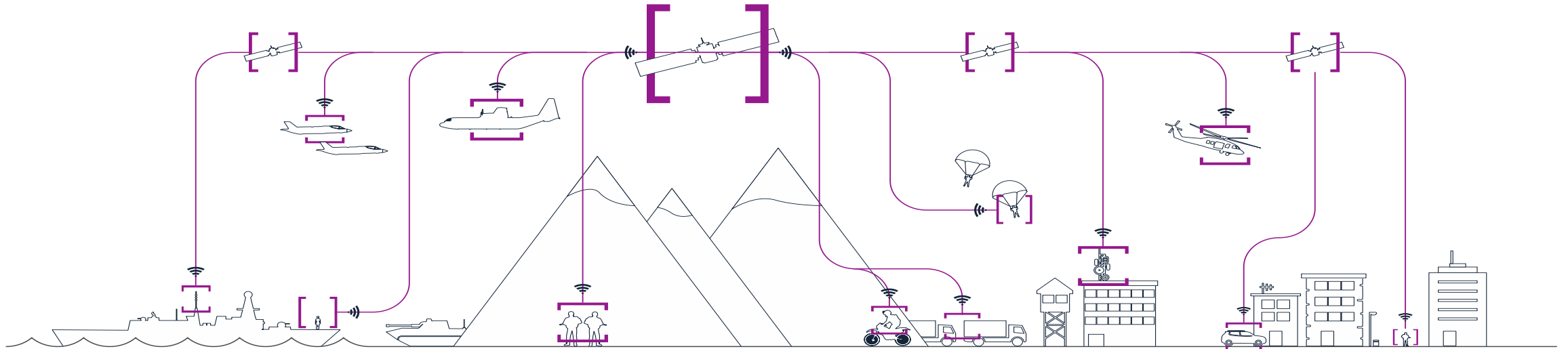
Time Message

- 16/04/2019 15: No Mapping for Beacon 54317. Default entry added with callsign UNK_54317.
- 16/04/2019 15: Beacon 50443 MIL-STD 2525 Symbol "" must be exactly 15 characters in length, using default.
- 16/04/2019 15: Beacon 50738 MIL-STD 2525 Symbol "" must be exactly 15 characters in length, using default.

QSA: Connected, Rx: 1 Beacons: 1 KML: File Writing - Wn1 Tx: 1 15:36:58Z NUM



More information:



Managing Bracer Tips

- Transfer Key can only be generated and loaded onto a handset by a laptop
- A management laptop should deploy with handsets – Rebuild in the deployed location
- Mission Keys can only be generated for the duration of the licence period.
- Best practice is to centrally control the generation of keys.
- Mission Keys are specific to a TG.
- Create an image of the Token for each handset.
- Copy the Hexidecimal code for the SA key into a text file – Transfer into QSA store.
- SA Tools should be set to ‘run as an administrator’.
- Management laptop requires all licences for handsets being programmed
- Ensure that you only transfer the keys required into a handset – **Do not overwrite – delete first!**
- Close down BKM before using SA tools.
- Ensure that the laptop is running on ZULU time (ensure daylight saving is disabled)
- Centrally control
- Interoperability – Decide on which organisation is going to generate the key for Interoperability.
- Building new laptops will require a licence code from QinetiQ – This can be produced very quickly
- If using Google Earth – Periodically check the Link indicator is green. If red then refresh.
- Good Antennas
- Mission Key Load if you change any of the settings.