inmarsat
The mobile satellite company

BGAN Radio Module Terminal Development Kit User Guide

Version 1.8

Publication Date: 02-Jul-2018

While the information in this document has been prepared in good faith, no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability (howsoever arising) is or will be accepted by the Inmarsat group or any of its officers, employees or agents in relation to the adequacy, accuracy, completeness, reasonableness or fitness for purpose of the information in this document. All and any such responsibility and liability is expressly disclaimed and excluded to the maximum extent permitted by applicable law. INMARSAT is a trademark owned by the International Mobile Satellite Organisation, the Inmarsat LOGO is a trademark owned by Inmarsat (IP) Company Limited. Both trademarks are licensed to Inmarsat Global Limited. All other Inmarsat trade marks in this document are owned by Inmarsat Global Limited.

Contents

1: Version History

Version	Date	Description
1.8	02-Jul-2018	- BRM and FEM versions updated to 5.8 and 1.23, respectively. - Reference to User and Engineering WebUI upgrade from cmd window" added in section "Accessing the BRM WebUI" - Section "7: Antenna Pointing and Establishing a Data Connection for On Air Data operations" split in: "10: Using the User WebUI" and "11: Using the Engineering WebUI". - Duplicated information about antenna pointing removed from section "10.2: Antenna Pointing" - Additional note about data connections in section "10.3: Connections" - Reference to "Firmware Upgrading a BRM based Terminal Application Note" - Mention to Remote Upgrade Server IP address substituted by its hostname in section "11.1.2: Remote Firmware Upgrade" and new description about it in section "11.10: Device". - New section "11.1.2: Remote Firmware Upgrade" - Additional information about the frequency at which location and temperature Websocket notification are displayed. - Further information about "Transmit Cable Calibration Test Signal" in section "11.10: Device" - Added description about the ACL functionality "Download Outbound IP ACL log" in section "11.16: IP Access Control List" - Figures updated according the Release 5.8

2: Conventions-BRM

This document uses the following conventions.

Note: Key points are shown in this format.

Bold font indicates commands, keywords and text labels on GUI items.

Italic font indicates titles of other documents in the suite of BRM-related documentation.

`Monospace font` indicates text that you must enter.

SMALL CAPITALS indicate keys that you must press.

3: Safety Instructions / Consignes de Sécurité / Sicherheitshinweise

Safety alert messages call attention to potential safety hazards and tell you how to avoid them. These messages are identified by the signal words DANGER, WARNING, CAUTION, or NOTICE, as illustrated in the following sections. To avoid possible property damage, personal injury or in some cases possible death read and comply with all safety alert messages.

Messages d'alerte de sécurité attirent l'attention sur les dangers potentiels et de vous dire comment les éviter. Ces messages sont identifiés par un signal mots DANGER, AVERTISSEMENT, ATTENTION, ou avis, comme illustré ci-dessous. Pour éviter des dommages matériels, des blessures ou la mort dans certains cas possible de lire et de respecter tous les messages d'alerte de sécurité.

Sicherheitshinweise machen auf potenzielle Gefahren aufmerksam und geben Rat wie sie vermieden werden können. Diese Meldungen sind durch die Signalwörter GEFAHR, WARNUNG, VORSICHT oder HINWEIS gekennzeichnet, wie in den folgenden Abschnitten beschrieben. Um mögliche Sachschäden, Verletzungen oder in einigen Fällen den Tod zu vermeiden, lesen und beachten Sie alle Sicherheitswarnmeldungen.

3.1: Messages Concerning Personal Injury / Messages Concernant des Blessures Corporelles / Meldungen über Personenschäden

The signal words DANGER, WARNING, and CAUTION indicate hazards that could result in personal injury or in some cases death, as explained below. Each of these signal words indicates the severity of the potential hazard.

Le signal de DANGER mots, AVERTISSEMENT et ATTENTION indiquer les dangers qui pourraient entraîner des blessures ou, dans certains cas la mort, comme expliqué ci-dessous. Chacun de ces mots du signal indique la gravité du danger potentiel.

Die Signalwörter GEFAHR, WARNUNG und VORSICHT weisen auf Gefahren hin die zu Verletzungen oder in einigen Fällen zum Tod führen können, wie im im Folgenden beschrieben. Die Signalwörter selbst stehen für den Schweregrad der potenziellen Gefahr.

⚠ DANGER

DANGER indicates a potentially hazardous situation which, if not avoided, will result in death or serious injury.

DANGER indique une situation potentiellement dangereuse qui, si elle n'est pas évitée, entraînera la mort ou des blessures graves.

GEFAHR bezeichnet eine potenzielle Gafahrensituation, welche, falls sie nicht vermieden wird, zum Tode oder zu schweren Verletzungen führt.

⚠ WARNING

WARNING indicates a potentially hazardous situation which, if not avoided, could result in serious injury.

AVERTISSEMENT indique une situation potentiellement dangereuse qui, si elle n'est pas évitée, pourrait entraîner des blessures graves.

WARNUNG bezeichnet eine potenzielle Gefahrensituation, welche, falls sie nicht vermieden wird, zu schweren Verletzungen führen könnte.

⚠CAUTION

CAUTION indicates a potentially hazardous situation which, if not avoided, could result in minor or moderate injury.

ATTENTION indique une situation potentiellement dangereuse qui, si elle n'est pas évitée, pourrait entraîner des blessures mineures ou modérées.

VORSICHT bezeichnet eine potenzielle Gefahrensituation, welche, falls sie nicht vermieden wird, zu geringfügigen oder mittelmäßigen Verletzungen führen könnte.

3.2: Messages Concerning Property Damage / Messages Concernant des Dommages Matériels / Meldungen über Sachschäden

NOTICE

NOTICE is used for messages concerning possible property damage, product damage or malfunction, data loss, or other unwanted results—but not personal injury.

AVIS est utilisée pour les messages concernant les dommages matériels, des dommages au produit ou de dysfonctionnement, de perte de données ou d'autres résultats indésirables, mais des blessures non personnelle.

HINWEIS wird für Mitteilungen verwendet die mögliche Sachschäden, Produktbeschädigungen oder Funktionsstörungen, Datenverlust oder ungewollte Ergebnisse – nicht aber Verletzungen betreffen.

3.3: Safety Symbols / Symboles de sécurité / Sicherheitssymbole

The generic safety alert symbol calls attention to a potential personal injury hazard. It appears next to the DANGER, WARNING, and CAUTION signal words as part of the signal word label. Other symbols may appear next to DANGER, WARNING, or CAUTION to indicate a specific type of hazard (for example, fire or electric shock). If other hazard symbols are used in this document they are identified in this section.

Le symbole générique d'alerte suivant attire l'attention sur un danger potentiel de risque de blessures. Il apparaît à côté des mots DANGER, AVERTISSEMENT et ATTENTION dans le cadre de l'affichage d’alerte . D'autres symboles peuvent apparaître à côté de DANGER, AVERTISSEMENT ou ATTENTION pour indiquer un type spécifique de danger (par exemple, un incendie ou un choc électrique). Si d’autres symboles de danger sont utilisés dans ce document, ils sont décrits dans cette section.

Das allgemeine Gefahrensymbol kennzeichnet eine potentialle Verletzungsgefahr. Es erscheint neben den GEFAHR -, WARNUNG - und VORSICHT - Signalwörtern als Teil der Signalwortkennzeichnung. Weitere Symbole können neben GEFAHR, WARNUNG oder VORSICHT angegeben sein um auf die Art der Gefahr (zum Beispiel Feuer oder elektrischer Schock) hinzuweisen. Falls weitere Gefahrensymbole in diesem Dokument verwendet werden, sind sie in diesem Abschnitt aufgeführt.

3.3.1: Additional Symbols / Les Symboles Supplémentaires / Zusätzliche Symbole

Warning Potential Radio Frequency (RF) hazard. Where you see this alert symbol and WARNING heading, strictly follow the warning instructions to avoid injury to eyes or other personal injury.

Avertissement Danger possible de Fréquence Radio (RF). A la vue de ce symbole d’alerte et du terme AVERTISSEMENT, suivez rigoureusement les instructions d'avertissement afin d’éviter une blessure aux yeux ou toute autre blessure.

Warnung vor möglicher radiofrequenter (RF) Strahlungsgefahr. Wo dieses Gefahrensymbol mit dem Stichwort WARNUNG zu sehen ist, sind die Warnhinweise unbedingt zu beachten um Augenverletzungen oder andere Verletzungen zu vermeiden.

Warning Where you see this alert symbol and WARNING heading, strictly follow the warning instructions to avoid personal injury.

Avertissement A la vue de ce symbole d’alerte et du terme AVERTISSEMENT, suivez rigoureusement les instructions d'avertissement pour éviter toute blessure.

Warnung Wo dieses Gefahrensymbol mit dem Wort WARNUNG zu sehen ist, sind die Warnhinweise unbedingt zu beachten um Verletzungen zu vermeiden.

Danger Electric shock hazard: Where you see this alert symbol and DANGER heading, strictly follow the warning instructions to avoid electric shock injury or death.

Danger Risque de choc électrique: A la vue de ce symbole d’alerte et du terme DANGER, suivez rigoureusement les instructions d'avertissement pour éviter tout choc électrique ou blessure mortelle.

Stromschlag Gefahr: Wenn dises Gefahrensymbol mit dem Wort GEFAHR zu sehen ist, sind die Warnhinweise unbedingt zu beachten um Verletzungen durch Stromschlag oder Tod zu vermeiden.

3.4: Warnings for Satellite Terminal / Avertissements pour le Terminal Satellite / Warnungen für Satellitenterminal

Do not stand in front of the Antenna. This device emits radio frequency energy. To avoid injury, do not place head or other body parts in front of the satellite antenna when system is operational. Maintain a distance of 1 m or more from the front of the TDK antenna.

Ne pas se tenir en face de l’antenne. Cet appareil émet une énergie de fréquence radio. Pour éviter toute blessure, ne placez pas la tête ou toute autre partie du corps en face de l'antenne satellite lorsque le système est opérationnel. Maintenez une distance de 1 m ou plus par rapport à l’antenne du terminal satellite.

Nicht vor der Antenne stehen. Dieses Gerät gibt Strahlungsenergie im Radiofrequenzbereich ab. Um Verletzungen zu vermeiden, Kopf oder andere Körperteile von der Satellitenantenne fernhalten, wenn das System in Betrieb ist. Halten Sie einen Abstand von 1 m oder mehr von der Vorderseite der TDK Antenne ein.

⚠

General Handle the TDK with care. Avoid exposing your Satellite Terminal to extreme hot or cold temperatures outside the range +15ºC to +35ºC.

Avoid placing the TDK close to cigarettes, open flames or any source of heat. Changes or modifications to the TDK not expressly approved by Inmarsat will void the Warranty and could void your authority to operate this equipment.

To avoid impaired TDK performance, please ensure only the recommended Antenna is used and that the Antenna is not damaged or covered with foreign material like paint or labelling.

When inserting the SIM, do not bend it or damage the contacts in any way. When connecting the interface cables, do not use excessive force.

The Ethernet port is intended to connected to indoor cables less than 10m in length.

Général Manipulez votre TDK avec soin. Évitez d'exposer votre terminal satellite à des températures extrêmement chaudes ou froides en dehors de la plage +15ºC to +35ºC.

Évitez de placer le TDK à proximité de la cigarette, de flammes nues ou de toute source de chaleur.

Les changements ou modifications apportées au TDK et non expressément approuvées par Inmarsat annulent la garantie et peuvent annuler votre droit à utiliser cet équipement.

Utilisez uniquement un chiffon doux humide pour nettoyer le TDK.

Pour éviter toute dégradation des performances du TDK , veuillez vous assurer que l’antenne de l'unité n'est pas endommagée ou recouverte d’un corps étranger, comme de la peinture ou de l'étiquetage.

Lorsque vous insérez la carte SIM, ne pas la plier ni endommager les contacts en aucune manière. Ne pas forcer lors de la connexion des câbles d’interface.

Le port Ethernet est prévu pour des câbles Ethernet d’intérieur mesurant moins de 10m.

Allgemein Das TDK ist mit vorsicht zu behandeln. Vermeiden Sie das Satellitenterminal extrem hohen oder niedrigen Temperaturen auszusetzen, die außderhab des Bereichs von +15ºC bis +35ºC sind.

Vermeiden Sie, das TDK in der Nähe von Zigaretten, offenem Feuer oder jeglicher Art von Hitzequelle aufzustellen. Änderungen oder Anpassungen des TDK die nicht ausdrücklich von Inmarsat genehmigt sind, führen zum Verlust der Gewährleistung und könnten zum Verlust der Betriebsgenehmigung für das Gerät führen.

Um die Leistungsfähigkeit des TDK nicht zu beeinträchtigen, ist bitte sicherzustellen, daß nur die empfohlene Antenne verwendet wird, und daß die Antenne nicht beschädigt oder mit Fremdmaterial wie Farbe oder Beschriftungen überdeckt ist.

Beim Einsetzen der SIM, die Kontakte nicht verbiegen oder beschädigen. Keine Gewalt beim Verbinden der Schnittstellenkabel anwenden.

Der Netzwerkanschluss ist für Innenraumkabel von weniger als 10 m Länge vorgesehen.

Electrostatic Discharge (ESD) can cause immediate or latent damage to electronic circuits. It is possible to damage the TDK by delivering electrostatic discharges when touching the electronic parts of the TDK. To make sure you are not delivering high static voltages to the TDK: Handle ESD sensitive components on a properly grounded and protected ESD workbench. If such a workbench is not available, you can provide some ESD protection by wearing an antistatic wrist strap and attaching it to a metal part of the system chassis. Always hold the board by the edges and avoid touching the component contacts.

Les décharges électrostatiques (ESD) causent des dégâts dans les systèmes électroniques. Toucher les parties électroniques de la TDK peut provoquer des décharges électrostatiques. Afin d’éviter les décharges électrostatiques, les composants sensibles doivent être manipulés sur une table de travail reliée à la terre et protégée contre les décharges électrostatiques. Au cas où une table de travail ne soit pas disponible, porter un bracelet ESD relié à une partie métal de la TDK réduit les dangers d’ESD. Saisissez les cartes électroniques par les côtés et évitez de toucher les composants.

Elektrostatische Entladung (ESD) kann unmittelbare oder Folgeschäden an elektronischen Bauteilen hervorrufen. Das TDK kann durch die Übertragung elektrischer Ladungen bei der Berührung von elektronischen Bauteile beschädigt werden. Um sicherzustellen, daß keine hohen statischen Spannungen auf das TDK übertragen werden: Handhaben Sie ESD-empfindliche Komponenten auf einem korrekt geerdeten und statisch geschützten ESD Arbeitstisch. Falls ein solcher Arbeitstisch nicht verfügbar ist, kann teilweiser ESD Schutz durch Tragen eines antistatischen Armbands gewährleistet werden, das an einem Metallstück des Gehäuses befestigt ist. Halten Sie die Platine immer an den Kanten und vermeiden Sie die direkte Berührung der elektrischen Kontakte der Bauteile.

In the vicinity of blasting work and in explosive environments Never use the TDK where blasting work is in progress. Observe all restrictions and follow any regulations or rules. Areas with a potentially explosive environment are often, but not always, clearly marked.

A proximité de travaux de dynamitage et d’environnements explosifs N'utilisez jamais le TDK près de travaux de dynamitage en cours. Respectez toutes les restrictions et suivez toutes les instructions ou la règlementation. Les zones présentant une atmosphère potentiellement explosive sont généralement, mais pas toujours, clairement signalées.

In der Nähe von Sprengarbeiten und in explosiven Umgebungen Niemals das TDK dort einsetzen wo Sprengungen durchgeführt werden. Halten Sie sich an alle Beschränkungen und befolgen Sie alle Bestimmungen oder Regeln. Bereiche in potenziell explosiven Umgebungen sind meistens, aber nicht immer, klar gekennzeichnet.

Do not attempt to use the TDK in ways not explicitly described within this user guide. Only trained personnel may evaluate the TDK in ways not explicitly described in this user guide.

Il est interdit de faire fonctionner la TDK d’une manière qui n’est pas décrite dans ce guide. Seulement des personnes qualifiées peuvent évaluer la TDK avec des configuration différentes.

Es ist nicht gestattet, das TDK für Zwecke einzusetzen, die nicht ausdrücklich in dieser Bedienungsanleitung beschrieben sind. Nur ausgebildetes Personal darf das TDK für Zwecke einsetzen, die nicht ausdrücklich in dieser Bedienungsanleitung beschrieben sind.

Pacemakers The various brands and models of cardiac pacemakers available exhibit a wide range of immunity levels to radio signals. Therefore, people who wear a cardiac pacemaker and who want to use a Satellite Terminal should seek the advice of their cardiologist. If, as a pacemaker user, you are still concerned about interaction with the TDK, we suggest you follow these guidelines:

- Maintain a distance of one meter from the front and sides of the antenna and your pacemaker;
- Refer to your pacemaker product literature for information on your particular device.

If you have any reason to suspect that interference is taking place, turn off your TDK immediately.

Stimulateurs Cardiaques Les différentes marques et modèles de stimulateurs cardiaques disponibles présentent un large éventail de niveaux d'immunité aux signaux radio. Par conséquent, les personnes qui portent un stimulateur cardiaque et qui veulent utiliser un terminal satellite doivent demander l'avis de leur cardiologue. Si, en tant qu'utilisateur de stimulateur cardiaque, vous êtes toujours soucieux d’une éventuelle interaction avec le terminal satellite, nous vous suggérons de suivre ces directives:

- Maintenez un mètre de distance entre votre stimulateur cardiaque et l'avant ou les côtés de l'antenne;
- Reportez-vous à la documentation de votre stimulateur cardiaque pour toute information spécifique à celui-ci.

Si vous avez un doute que des interférences se produisent, éteignez votre terminal satellite immédiatement.

Herzschrittmacher Die unterschiedlichen Marken und Modelle verfügbarer Herzschrittmacher weisen sehr unterschiedliche Unempfindlichkeiten gegenüber radiofrequenter Strahlung auf. Daher sollten sich Personen mit Herzschrittmachern die ein Satellitenterminal benutzen wollen von einem

Kardiologen beraten lassen. Sollten Sie als Träger eines Herzschrittmachers dennoch beunruhigt sein, schlagen wir vor, daß Sie sich an diese Richtlinien halten:

> Halten Sie einen Abstand von mindestens einem Meter zwischen der Vorderseite und allen Seiten der Antenne zu Ihrem Herzschrittmacher ein;

> Beziehen Sie sich auf die Produktbeschreibungen Ihres Herzschrittmachers für Informationen zu Ihrem spezifischen Gerät.

Sollten Sie Grund zur Annahme von Beeinträchtigungen haben, stellen Sie das TDK sofort ab.

Hearing Aids Most new models of hearing aids are immune to radio frequency interference from Satellite Terminals that are more than 2 meters away. Many types of older hearing aids may be susceptible to interference, making it very difficult to use them near a Terminal. Should interference be experienced, maintain additional separation between you and the TDK.

Appareils Auditifs La plupart des nouveaux appareils auditifs sont insensibles aux interférences dues aux fréquences radio des terminaux satellites situés à plus de 2 m . De nombreux modèles plus anciens peuvent être sensibles aux interférences, ce qui les rend très difficiles à utiliser à proximité d'un terminal. En cas d'interférences détectées, veuillez maintenir une distance supplémentaire entre vous et le terminal.

Hörhilfen Die meisten neueren Hörhilfen sind gegenüber radiofrequenter Strahlung unempfindlich die von Satellitenterminals in einer Entfernung von mehr als 2 m ausgestrahlt werden. Viele ältere Hörhilfen sind jedoch durch Interferenz beeinflussbar, was ihren Einsatz in der Nähe eines Terminals erschwert. Sollte Interferenz auftreten, halten Sie einen zusätzlichen Abstand zwischen Ihnen und dem TDK ein.

Electrical Storms Installation of the TDK during electrical storms may result in severe personal injury or death.

Orages Electriques L'installation d'un terminal satellite pendant un orage électrique peut entrainer des blessures graves ou mortelles.

Gewitter Installation des TDK während eines Gewitters kann zu ernsthaften Verletzungen oder zum Tod führen.

4: Introduction

Note: The content of this document is Inmarsat proprietary and confidential, and as such external distribution is available only to Inmarsat-approved Value Added Manufacturer Partners involved in development using the BGAN Radio Module.

This document is a **User Guide** for the **Terminal Development Kit (TDK)**, which is made up of the following elements:

- **Hardware Development Kit** (**HDK**) motherboard (Revision **2**)
- **BGAN Radio Module** (**BRM**) (Revision **2**, with **Firmware** version **5.8**)
- **Front End Module** (**FEM**) (Revision **2**, with **Firmware** version **1.23**)

The TDK is a pre-certified terminal development kit allowing the BRM to be evaluated and used as a starting point to develop BRM based terminals and applications. The kit is supplied pre-configured as a Class 2 terminal suitable for "on-air" use with a Hughes 9502 antenna (not supplied) kit.

For an overview of the **Broadband Global Area Network** (**BGAN**) network, please refer to the *BGAN Radio Module Overview* document by logging in to the **Inmarsat Developer Website** and navigating to **Developer Resources > Technology Platforms > BGAN > Hardware > BGAN Radio Module (BRM) > Documentation and Resources**, under the **BRM Resources** section.

Notes:
In case of any inconsistency between this document and the latest Release Note, the latest release note supersedes this User Guide.

The images in this document may contain firmware version numbers that does not represent the latest versions of the BRM firmware available. Always consult the latest Firmware release notes available on the Inmarsat Developer Website.

4.1: Reference Documents

The documents that must be referenced in conjunction with this document are as follows:

Document Name	Description
BGAN Radio Module Terminal Development Kit Technical Specification	Details the technical specifications for the TDK, and the default configurations required.
BGAN Radio Module Application Protocol Interfaces Reference	Provides an overview of the different APIs that can be run on the BRM.
BGAN Radio Module AT Commands - Telnet Interface Control Document	Details the AT commands that can be run on a BRM.
BGAN Radio Module Technical Specification	Details the technical specifications for the BRM.
BGAN Radio Module Overview	Provides an overview of the BRM and the BGAN network.
Signal Quality Scores - BRM Implementation and Guidelines for Value Added Manufacturers	Provides the details of BRM Signal Quality Score and its usage.

4.2: Approval for On Air Use

The BRM and TDK components are pre-certified and configured for use on air as a Class 2 Terminal. The BRM and TDK components cannot be used on air in any other configuration without Inmarsat approval.

Use of non-approved components can and will impact other BGAN users and potentially BGAN-related safety services.

5: Product Description

5.1: Packing List

- BGAN Radio Module (BRM):
  - 1 x Hardware Developer Kit (HDK) motherboard (Revision 2)
  - 1 x BRM (Revision 2, with Firmware version 5.8)
  - 1 x 12V Power Supply (Part number: SDI50-12-U-P5)
  - 1 x FEM control interface cable
  - 1 x 5.5V power cable
  - 1 x 8 - 28V power cable
  - 4 x RF Coaxial leads
- Reference Front End Module:
  - 1 x Class 2 Revision 2 FEM (Revision 2, with Firmware Version 1.23)
  - 1 x GNSS Antenna

5.2: Other Items Required for On Air Operation Not Supplied with TDK

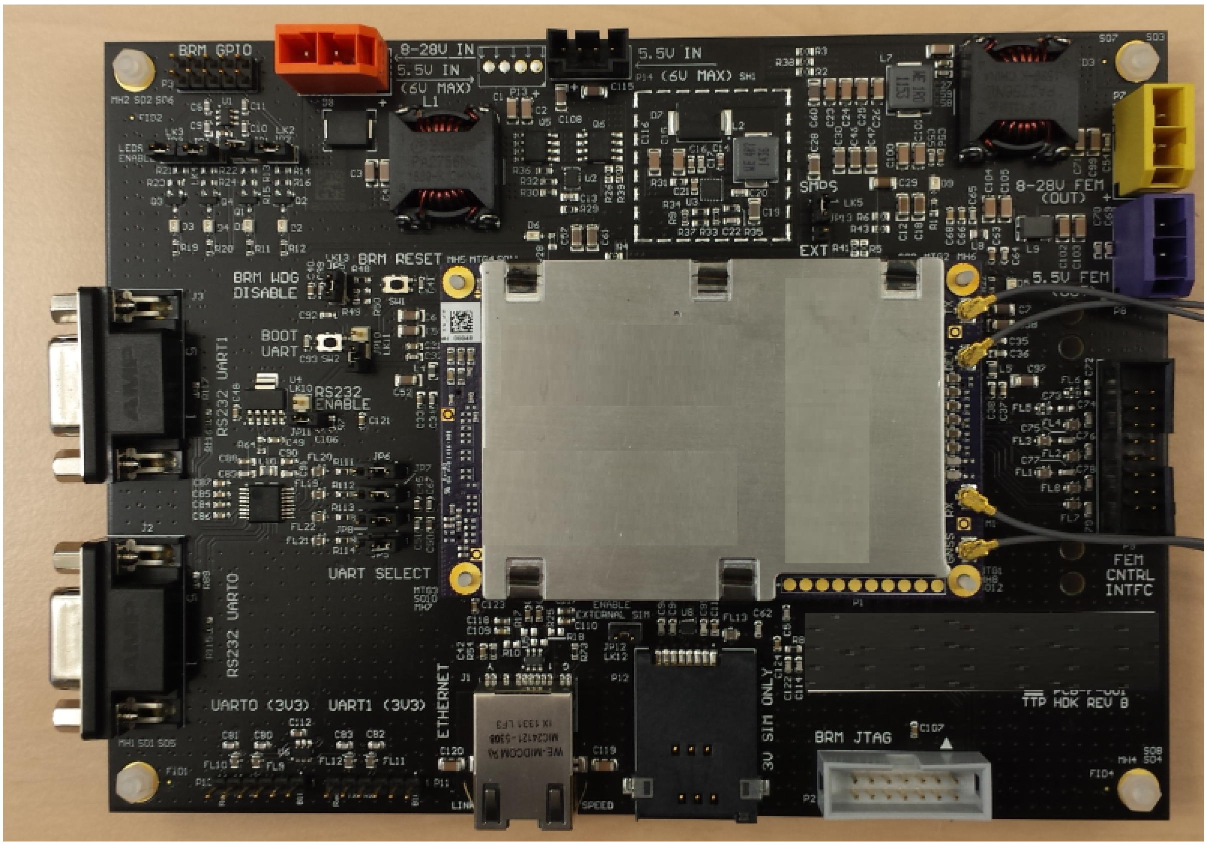
- Hughes 9502 antenna with an LMR-400 or equivalent 10m coaxial cable
- BGAN USIM

5.3: Main Features of the HDK

5.3.1: HDK Motherboard

The HDK motherboard is used for mounting and interfacing to the BRM. It incorporates all the essential items needed for a VAM to evaluate and develop terminals with the BRM. These include:

- 12V nominal input power supply with protection suitable for a wide range of applications used to supply the BRM, HDK
- Interface header to the BRMs GPIO with links to LEDs
- Ethernet transformer and RJ45 connector with activity detector
- RS232 serial ports and low voltages interfaces for the BRM’s UARTs
- FEM interface
- USIM card holder

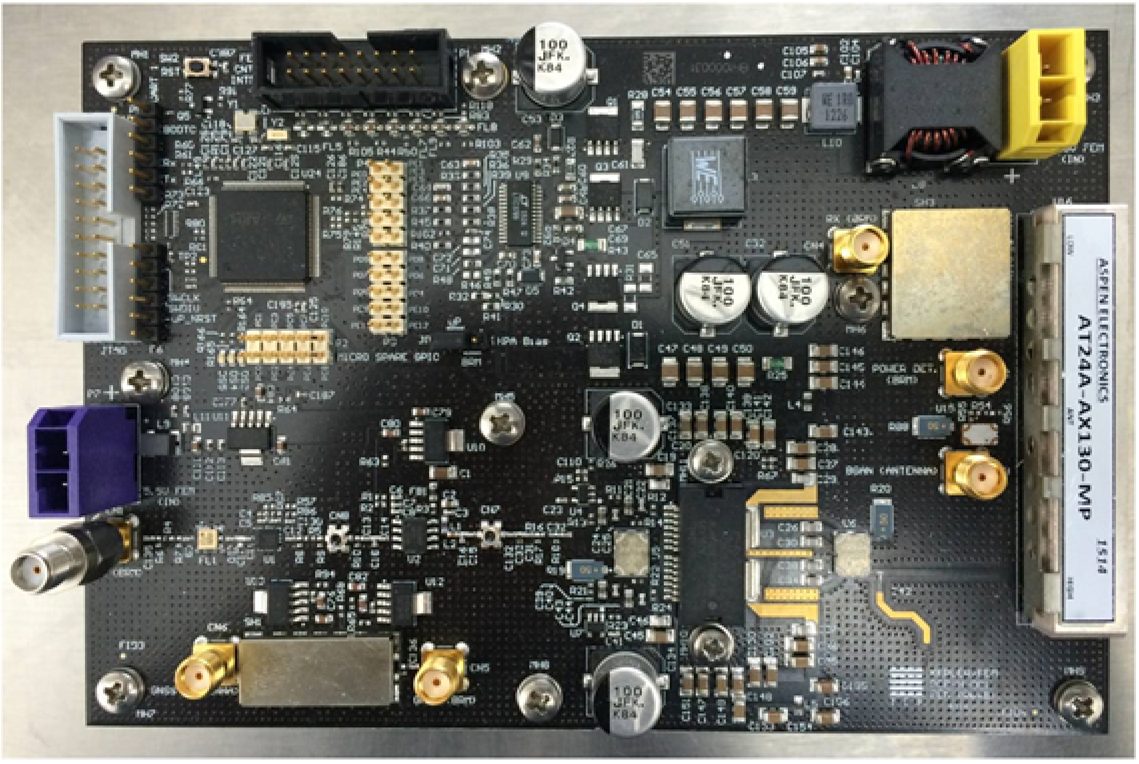


5.3.2: Reference Front End Module

The Front End Module (FEM) contains the HPA, LNA and duplexer needed to use the BRM as a terminal.

The FEM is supplied as an example reference design configured for BGAN Class 2 operation but capable of meeting the RF performance requirements for all BGAN land and maritime classes. Some further development work is typically required to adapt the reference design for use within a specific production ready terminal design.

Note: If you need to upgrade the Firmware for the FEM, please refer to **FEM Firmware Update Procedure**.



5.3.3: TDK Specifications

Specification	Details
Satellite Transmit Frequency	1626.5 to 1675 MHz
Satellite Receive Frequency	1518 to 1559 MHz
GNSS Frequency	1559 to 1610 MHz
HDK Dimensions (nominal)	Length: 175 mm Width: 125 mm Thickness: 34 mm
HDK Mass with BRM (nominal)	263g
FEM Dimensions (nominal)	Length: 155 mm Width: 104 mm Thickness: 52 mm
FEM Mass (nominal, with heat sink)	763g
Environmental	Operating Temperature: 15 to 35 °C Storage Temperature: 40 to 80 °C
Power Supply	Input: 100 - 240 V AC Output: +12 V DC, 4.2A Manufacturer: CUI.inc Part Number: SDI50-12-U-P5

6: Setting up the Terminal Development Kit

This section describes how to connect the TDK together, ready for it to be used over-the-air.

> **Notes:**
> **Do not** supply power to the TDK until **all** the steps in this section have been completed.
>
> The HDK board must be used on a clear and level surface, and do not place any items on top of the HDK board.

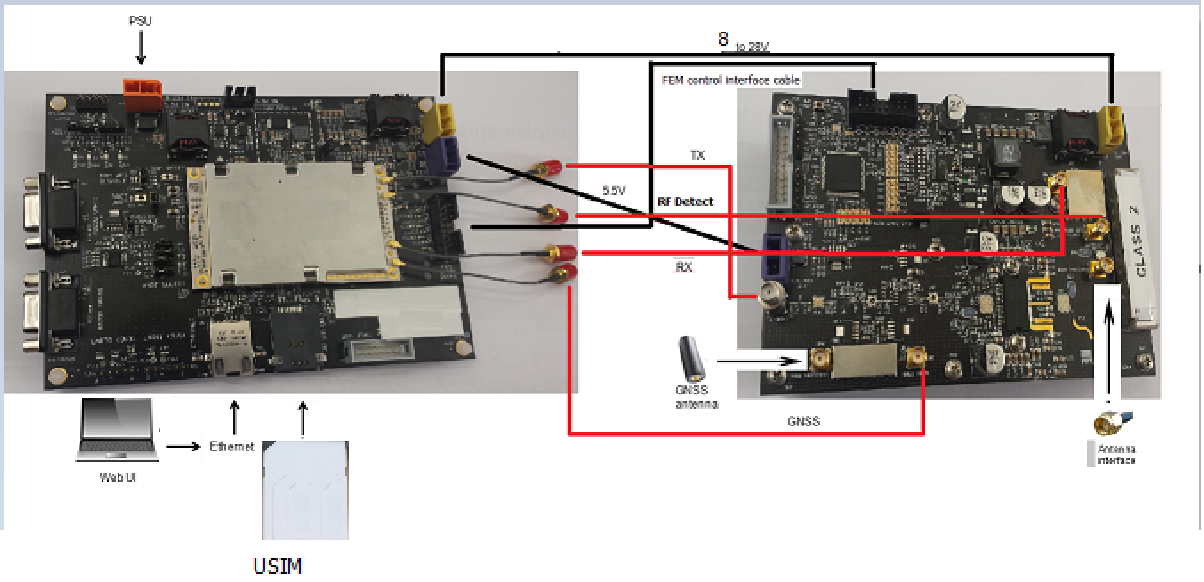


Figure 1. TDK Connection Set Up for On-Air Operation

6.1: Connecting the FEM to the HDK

NOTICE

1. Assemble the RF cables as shown in *Figure 1*.

> **Notes:**
> RF leads are part of the calibrated terminal. The labelled cables must be used as marked, i.e., the TX cable must be connected between the TX connectors on the BRM and FEM; RX cable must be connected between the RX connectors on the BRM and FEM, etc.
>
> The BRM's U.FL cables have a limited number of mating cycles.

2. Assemble the colour-coded power leads as shown in *Figure 1*.

3. Connect both ends of the FEM control interface cable as shown in *Figure 1*.

4. Connect the GNSS antenna to the FEM as shown in *Figure 1*.

Note: The GNSS antenna should be placed on a coaxial lead (not supplied) and placed in an area with good visibility of the sky in order to receive the GNSS signal. If it is not possible to locate the TDK in a suitable location then the supplied GNSS antenna may be connected to the GNSS antenna port on the FEM using a suitable RF cable (not supplied); it is recommended that this should be no more than 3m long.

6.2: Connecting the Hughes 9502 Antenna to the FEM

⚠CAUTION

Note: Please refer to the safety notices in the **Hughes 9502 Fixed Satellite Terminal User Guide**, for instructions on safe handling of the Hughes 9502 antenna during installation and over-the-air use.

1. Connect a Hughes 9502 BGAN antenna to the antenna interface on the FEM, as shown in *Figure 1*.

NOTICE

Note: The Hughes 9502 antenna must be attached to the terminal with the 10m of coaxial cable supplied with the antenna. No other antennas or cables are permitted, and no other type of antenna is permitted, as the TDK is set up to be used in a Class 2 BGAN terminal with a Hughes 9502 BGAN antenna.

6.3: Connections for the HDK

1. Connect either a cross-over or straight-through ethernet cable (not supplied) between the ethernet port on the HDK and your computer, as shown in *Figure 1*.

2. Insert the USIM into the external SIM port on the HDK, as shown in *Figure 1*.

3. Connect the 12 V Power Supply (Part Number: SDI50-12-U-P5) to the PSU port on the HDK, as shown in *Figure 1*. No other power supply should be used.

4. Refer to **Power** for how to apply power to the TDK.

Power

Note: Before you supply power to the TDK, ensure you are familiar with the safety notices for the Hughes 9502 antenna, in the **Hughes 9502 Fixed Satellite Terminal User Guide.**

1. Switch on the power supply.

The LED configuration on the HDK should look as shown in *Figure 2*, with the D5, D6 and D9 LEDs static green, and D3 and D1 blinking at different rates.

Notes:

D3 = ARM1: blinking green LED = running.

D1 = DSP1:

slow blinking green LED = RX idle (It will take about 30 seconds after power is first supplied to the TDK, before the D1 LED is in a slow-blinking green light state, because the BRM will only exit low power mode after being switched on once a GNSS/GPS fix has been established)

fast blinking green LED = RX tracking

solid green LED = BRM crash

solid off LED = BRM in low power mode (or possible BRM crash)

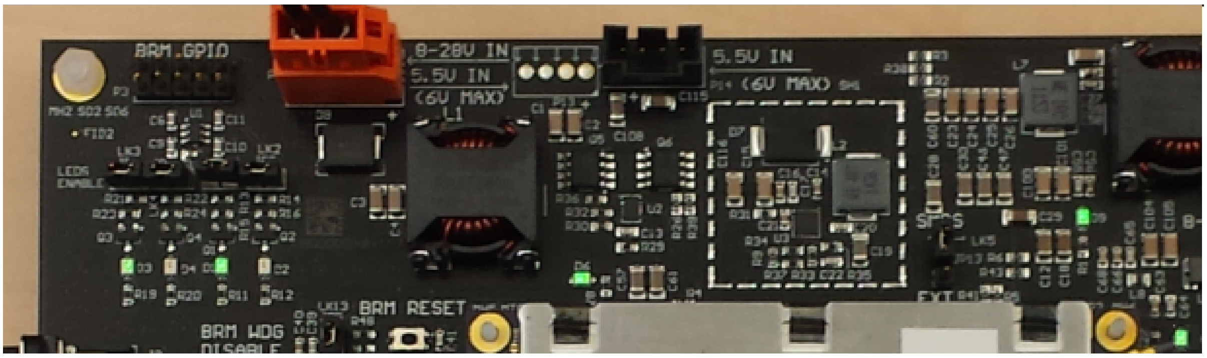


Figure 2. LED Configuration

2. Refer to **Accessing the BRM WebUI** for how to access the BRM WebUI from your computer.

Accessing the BRM WebUI

1. In a web browser (any type), enter any of the following options in the address bar:

> https://192.168.1.1/auth/

> https://brm.inmarsat.com/auth/

> brm.inmarsat.com

> 192.168.1.1

Notes:

If you are having any problems accessing the BRM WebUI, take the following steps (steps assume use of Windows 7):

a. On the laptop, navigate to **Control Panel > Network and Sharing Center > Change Adaptor Settings**.

b. Double-click on **Local Area Connection (wired ethernet connection)**.

c. Navigate to **Properties**.

d. Double-click **Internet Protocol Version 4**.

It should be set to `Obtain an IP Address automatically`, or, you can set a static IP as long as it is in the subnet `192.168.1.0/32`, i.e., anything apart from the BRM default IP address in that subnet.

If the IP address is set by static means, ensure that the Gateway and DNS (or any other public DNS server) IP address is 192.168.1.1.

If the WebUI is accessed via HTTP, the BRM would then redirect automatically to an unauthenticated HTTPS page and if there is no "unauthenticated" user defined would then redirect automatically to the "authenticated" page.

If an "authenticated" user exists, BRM would stay on the unauthenticated HTTPS page and then provide a link to the authenticated user page. Refer to **Unauthenticated User** for more details.

2. Select **Continue to this website** when you see the Certificate Error screen

3. Enter `admin` for the username.

4. Enter `m@nufacturing` for the password.

You are now in the BRM WebUI, ready to use the BRM.

Note: If you enter `https://192.168.1.1/auth` in the address bar, i.e., you accidentally omit the forward slash after 'auth', then you will still be permitted to enter the user name and password, but you will then receive a 404 error.

> For instructions on how to navigate and use the User WebUI, refer to **Using the User WebUI**

> For instructions on how to navigate and use the **Engineering** WebUI (has to be downloaded from the Inmarsat Developer Website and reverted to), refer to **Using the Engineering WebUI**

Note: Please refer to *User and Engineering WebUI Upgrade from Command Window* for how to change between the Engineering WebUI and the User WebUI.

7: Telnet Sessions

To run a Telnet session on your PC or laptop connected to the BRM, to use AT commands on the BRM, take the following steps:

Note: A telnet session cannot be established until at least 30 seconds after the BRM has been powered on or rebooted, because the BRM does not have a location fix until that point.

1. Access the BRM WebUI and navigate to the **Configuration** page.

2. If they are not already, set **telnet_enabled** to `true` and **bui_mode** to `false`.

3. Start a telnet session on your PC or laptop connected to the BRM.

Notes:
No username or password is required, and the connection address is `192.168.1.1`, port `23`.

The Telnet port is set, by default, to the standard port 23. However, the BRM can be configured to another port of choice through a configuration parameter.

Refer to *AT Commands Interface Control Document - Telnet*, for which AT commands are available.

8: Physical Layer Testing

To run Physical Layer Mandatory Test Requirements (PHY MTRs), you will use either a BGAN Physical Layer Tester (BPLT) or BGAN Multi-Channel Platform (BMCP).

Notes:
The **bui_mode** parameter must be set to `true` when running the PHY MTRs. Refer to **Enable_ BUI** for how to set this without having to do it in the **Configuration** page and then rebooting (and only if the parameter is already set to `false`), otherwise please set it in the **Configuration** page, and then reboot the BRM for the change to take effect.

8.1: Running PHY MTRs on a Standalone BRM

The BRM as supplied in the TDK operates as a class 1 UT when not connected to a FEM. To run PHY MTRs on a standalone BRM, take the following steps:

1. Close the BRM transmit power loop with a power splitter, per **BRM Closed Loop Transmit Operation with Power Splitter**.

2. Connect the splitter output to the BPLT or BMCP RX port, bypassing the BPLT or BMCP duplexer.

3. Connect the BRM RX to the BPLT or BMCP TX port, bypassing the BPLT or BMCP duplexer.

4. Are you using a BPLT or BMCP?

- **BPLT** - go to **Step 5**
- **BMCP** - go to **Step 6**

5. Set the attenuators to the following values, then proceed to **Step 6**:

Note: Refer to the user guide provided by Square Peg Communications for how to set the attenuators on the BPLT.

- TX (forward path) 40dB
- RX (return path) 50dB

6. Use the BRM level `BRM_UT.ini` and `BPLT.ini` files available on the Inmarsat Developer Website to run Class 1 MTRs.

Note: See comments in BPLT.ini on selecting the correct .ini parameters, according to whether a BPLT or BMCP is used.

8.2: Running PHY MTRs on a BRM and FEM

The FEM as supplied with the TDK is set to operate as a class 2 UT. To run PHY MTRs on a BRM with a FEM attached, take the following steps:

1. With a 30dB power attenuator in the path, connect the FEM antenna port to the BPLT or BMCP RF connector.

2. Are you using a BPLT or BMCP?

- **BPLT** - go to **Step 3**
- **BMCP** - go to **Step 4**

3. Set the attenuators to the following values, then proceed to **Step 4**:

Note: Refer to the user guide provided by Square Peg Communications for how to set the attenuators on the BPLT.

- TX (forward path) 40dB
- RX (return path) 50dB

4. Use the FEM level `FEM_UT.ini` and `BPLT.ini` files available on the Inmarsat Developer Website to run Class 2 MTRs.

Note: See comments in BPLT.ini on selecting the correct .ini parameters, according to whether a BPLT or BMCP is used.

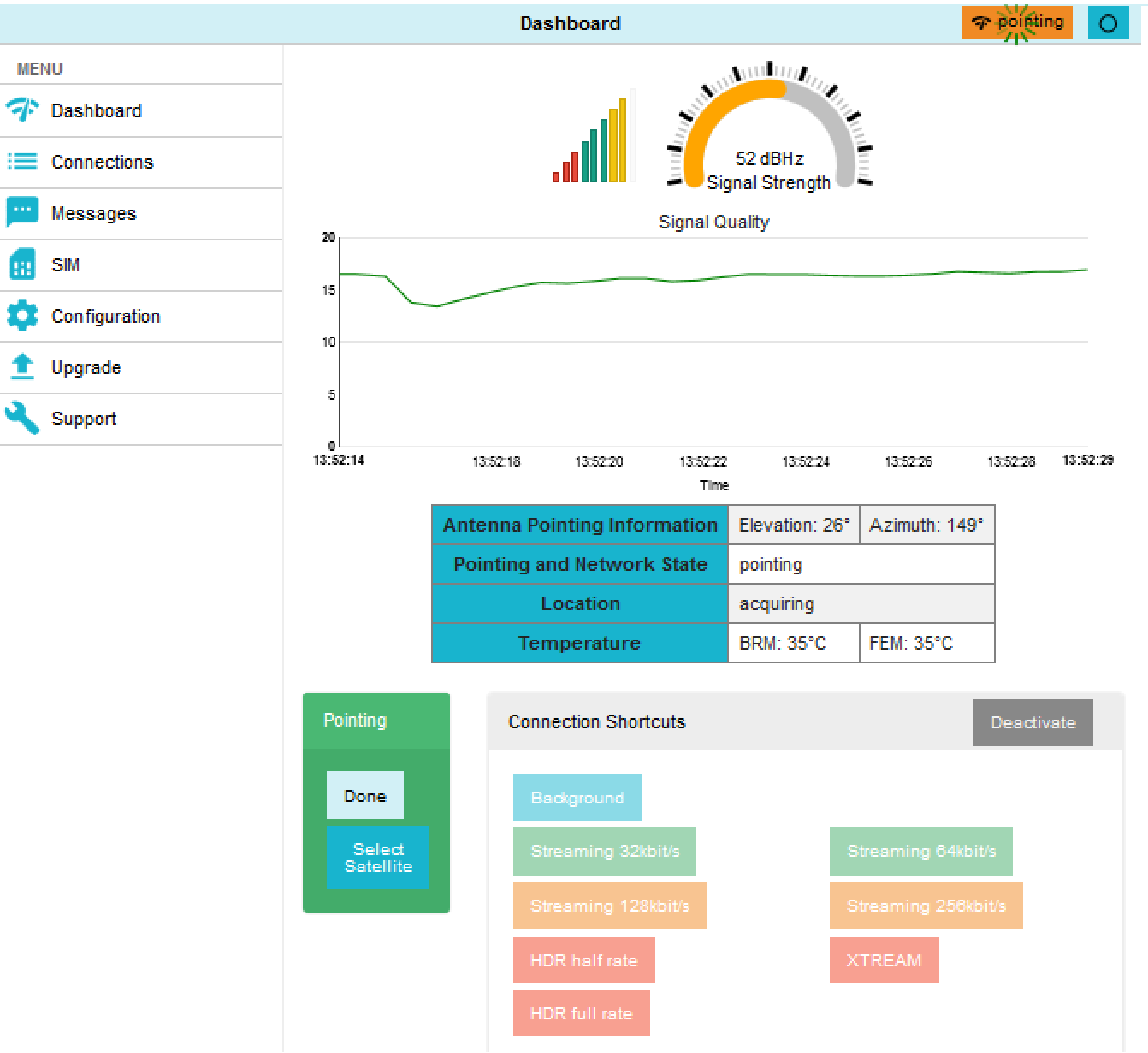
9: Using the User WebUI

The following dashboard loads up when you access the User WebUI, per *Figure 3*.

The Dashboard shows the following details and operational options:

- Current signal strength (graphical and visual representation)
- Signal Quality Indicator
- Antenna Pointing Information | Pointing and Network State | Location | BRM and FEM Temperature
- Connection and Antenna Pointing shortcuts
- Alert notifications
- Manual Activity notifications, e.g., Enter SIM PIN; bypass pointing mode
- Left-hand menu options navigation bar:
  - Dashboard
  - Connections
  - Messages
  - SIM
  - Configuration
  - Upgrade
  - Support

Note: There is not an option to log out; instead, simply closing the web browser means that the next time you try to access it, you will need to log in again.



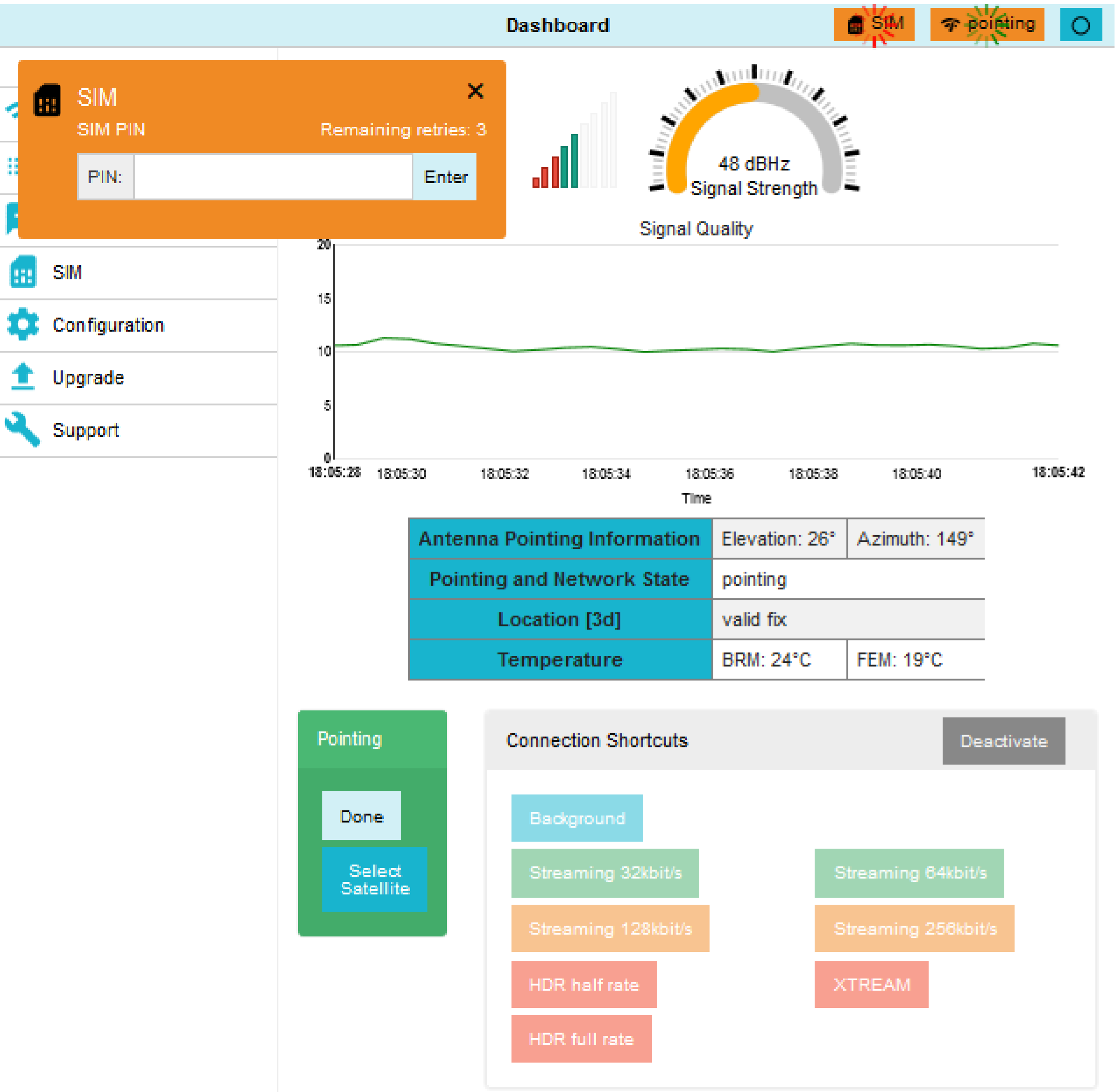
Antenna Pointing Information	Elevation: 26°	Azimuth: 149°
Pointing and Network State	pointing	
Location	acquiring	
Temperature	BRM: 35°C	FEM: 35°C

Figure 3. Default WebUI Dashboard

Note: If you wish to use APIs via Websocket connections to perform the activities described in the following sections, please refer to the **BGAN Radio Module Application Protocol Interfaces Reference** on the **Developer Website**.

9.1: Enter SIM PIN

Once you have logged in to the default WebUI and the Dashboard has loaded up, if the external Universal Subscriber Identity Module (USIM) loaded into the BRM-based User Terminal (UT) has a Personal Identification Number (PIN) associated and enabled with it, then the Dashboard will indicate that the SIM PIN must be entered before you can start to use the WebUI, per *Figure 4*.



Antenna Pointing Information	Elevation: 26°	Azimuth: 149°
Pointing and Network State	pointing	
Location [3d]	valid fix	
Temperature	BRM: 24°C	FEM: 19°C

Figure 4. Enter SIM PIN

Enter the SIM PIN in the **SIM PIN** dialog box and select **Enter**.

Once the correct PIN is entered, the SIM alert icon in the top right-hand corner of the Dashboard disappears.

Notes:
If an incorrect PIN is entered, the "Remaining retries" value will decrease by one and a message is shown saying `incorrect password`. More information can be found in the upper right-hand corner of the dashboard saying `SIM PIN entry: insufficient permissions. [Date and time] incorrect password`. In that case, re-enter the correct SIM PIN.

The number of incorrect entries is restricted and entering one more than the maximum allowable incorrect entries would block the SIM. A PIN Unblocking Key (PUK) would then be required to unblock the PIN.

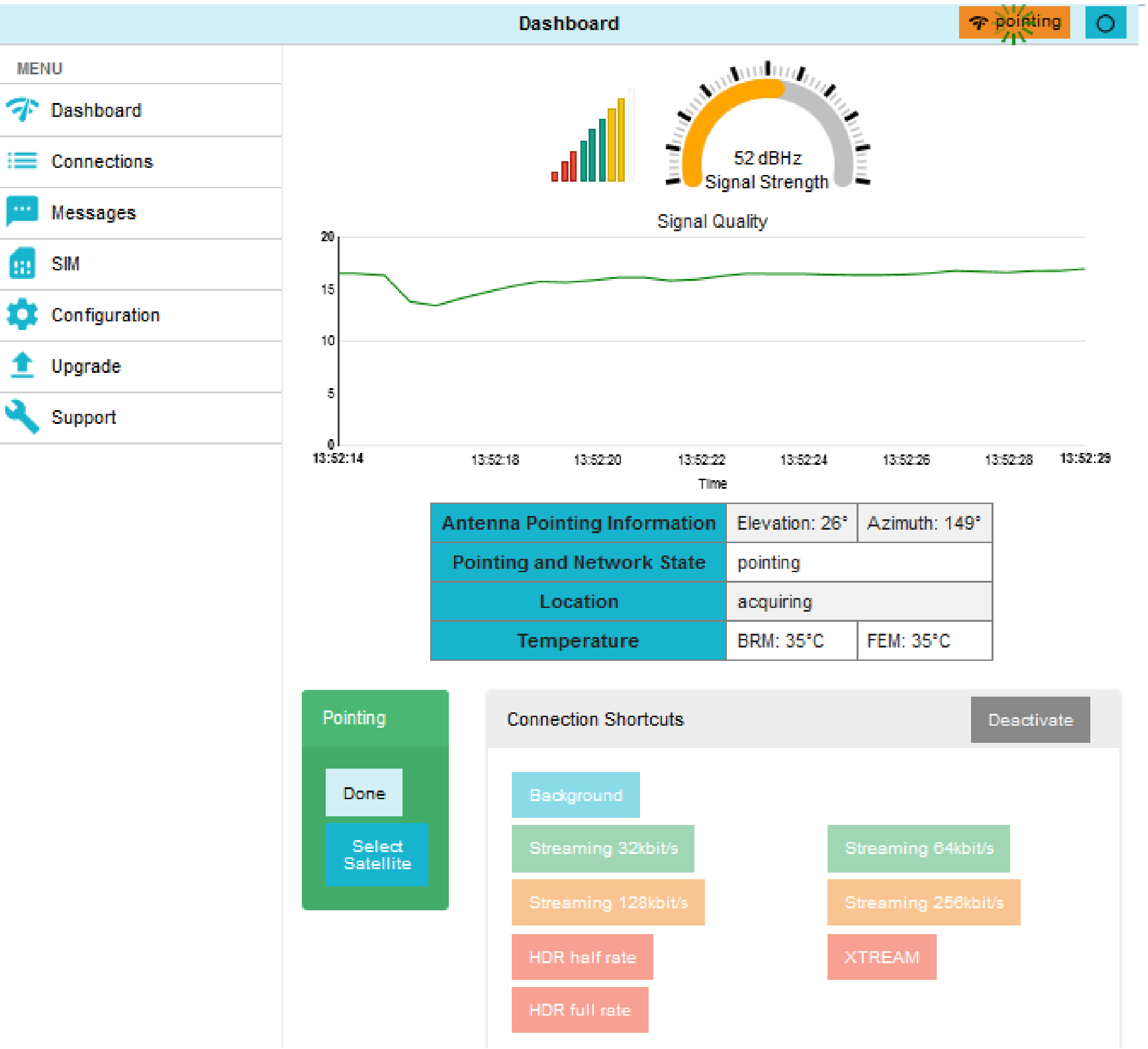
If you enter a PIN that is outside the specified number of digits, a red error notification message is generated in the top right-hand corner of the Dashboard saying `SIM PIN entry: Invalid Request. [Date and time] SIM error: PIN value must have between 4 and`

`8 digits`. If this error occurs, re-enter the correct SIM PIN, and in that case the remaining retries value does not decrease.

9.2: Antenna Pointing

Per *Figure 5*, a notification button (pointing) appears in the top right-hand corner of the Dashboard.

Note: This notification will only appear if the BRM-based Terminal has not been configured to perform an auto-pointing function. If it is configured to perform an auto-point on power up, then the Pointing box will always be greyed-out.

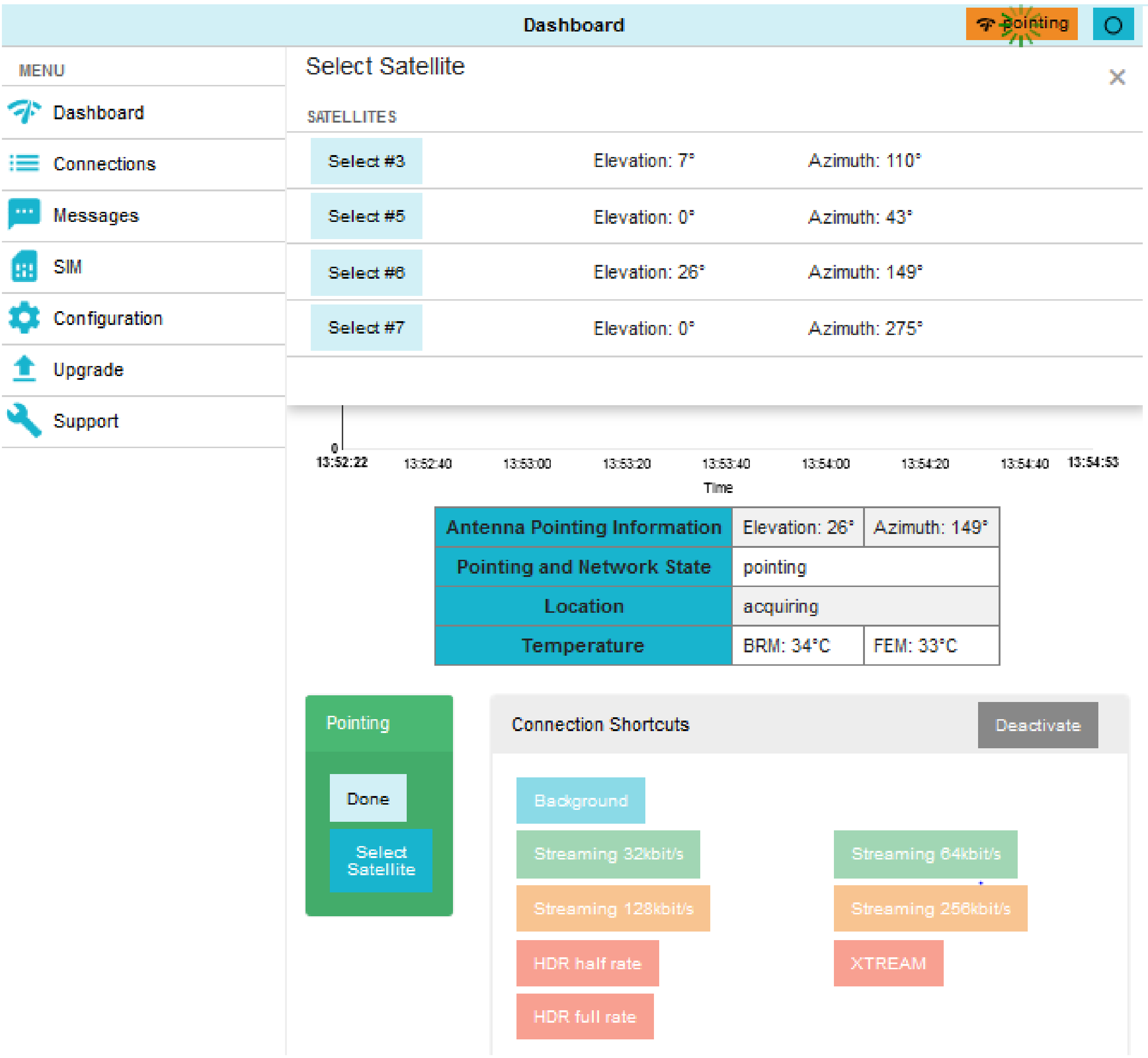


Antenna Pointing Information	Elevation: 26°	Azimuth: 149°
Pointing and Network State	pointing	
Location	acquiring	
Temperature	BRM: 35°C	FEM: 35°C

Figure 5. Manual Pointing

1. In the **Pointing** box, select *Select Satellite*.

The **Select Satellite** list appears towards the top of the Dashboard, per *Figure 6*.



Select #3	Elevation: 7°	Azimuth: 110°
Select #5	Elevation: 0°	Azimuth: 43°
Select #6	Elevation: 26°	Azimuth: 149°
Select #7	Elevation: 0°	Azimuth: 275°

Antenna Pointing Information	Elevation: 26°	Azimuth: 149°
Pointing and Network State	pointing	
Location	acquiring	
Temperature	BRM: 34°C	FEM: 33°C

Figure 6. Select Satellite

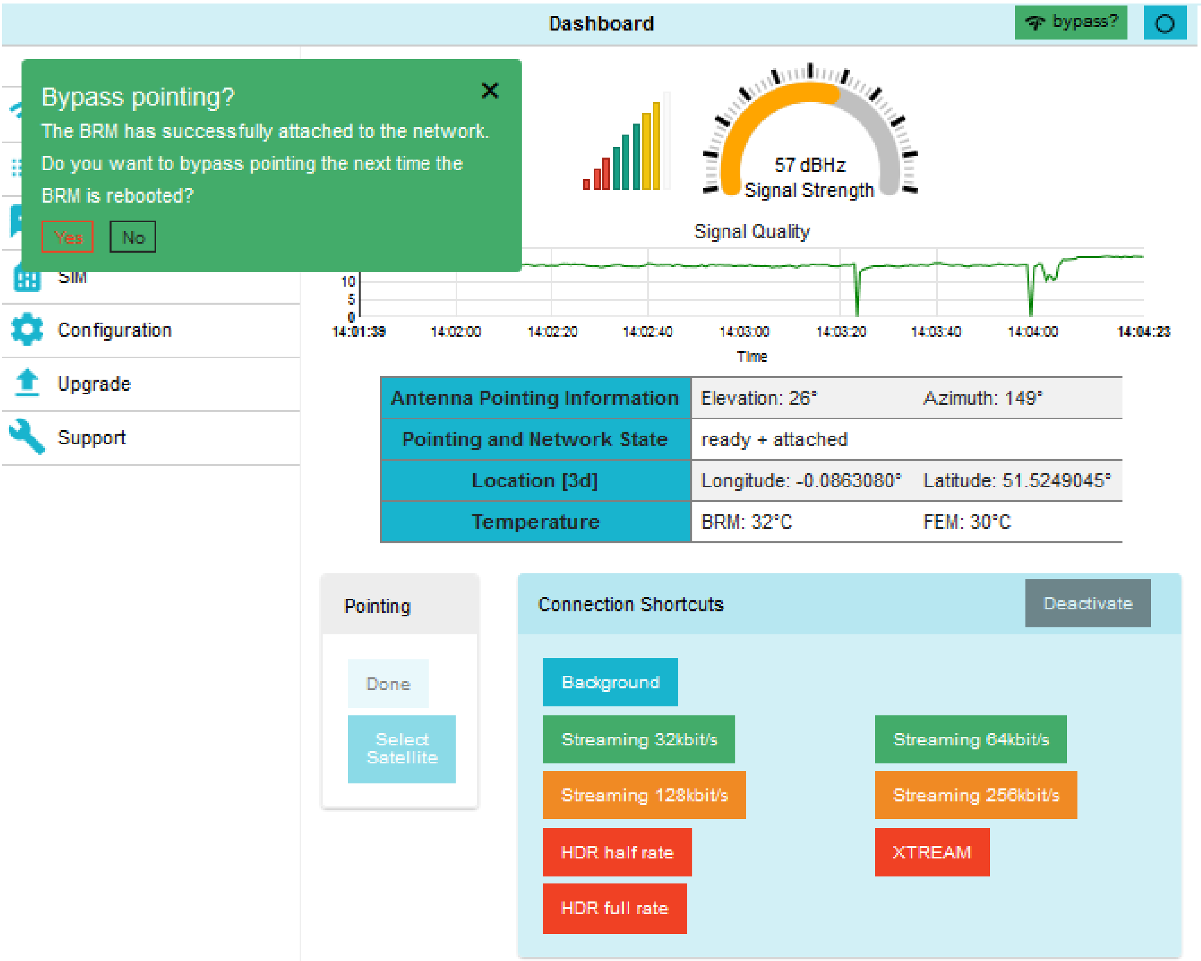
2. From the list, select the Satellite with the largest Azimuth value.

3. In the Pointing box, select **Done**.

The BRM-based Terminal will proceed to point to the selected satellite, and once pointing has been successful the value for **Pointing and Network State** will change from `pointing` to `ready + attached`, and a `Latitude` and `Longitude` value will show for **Location (3d)**.

Once **Done** is selected, the **Pointing** box is greyed-out and the pointing notification disappears from the top right-hand corner of the Dashboard, to be replaced by a green icon indicating that connectivity to the BGAN network is `active`.

A green box appears in the top left-hand corner of the Dashboard, and a green icon (`bypass?`) appears in the top right-hand corner of the Dashboard, per *Figure 7*.



Bypass pointing?

The BRM has successfully attached to the network. Do you want to bypass pointing the next time the BRM is rebooted?

Yes No

Antenna Pointing Information	Elevation: 26°	Azimuth: 149°
Pointing and Network State	ready + attached	
Location [3d]	Longitude: -0.0863080°	Latitude: 51.5249045°
Temperature	BRM: 32°C	FEM: 30°C

Figure 7. Bypass Pointing notification

- Select **Yes** if you want the BRM-based Terminal to perform an auto-point of the antenna the next time the UT is activated

- Select **No** if you want to carry out the antenna pointing manually, the next time the UT is activated

Once an option has been selected, the **Bypass Pointing?** pop-up and **bypass?** notifications disappear from the Dashboard view.

> **Note:** If an error occurs with the BRM-based UT attaching to the BGAN network, a red error notification appears in the top right-hand corner of the Dashboard, saying `Network: Failed to attach to the network.`

9.3: Establishing a Data Connection for On-Air Operations

In order to access the BGAN network, a connection profile should be activated. The User WebUI offers two different options for achieving this:

- **Connection** shortcuts on the **Dashboard**
  - Once the BRM is attached, select one of the eight available shortcuts. A green icon appears in the right corner of the WebUI, which specifies the status of the connection. as long no errors have occurred during the activation process, the status will change from `activating` to `active`

- **Connections** page
    - Refer to **Connections**

9.4: Connections

To view and administer the BRM-based UT connections to the BGAN network, select the **Connections** option from the left-hand navigation.

The **Connections** list loads up, per *9.4*.

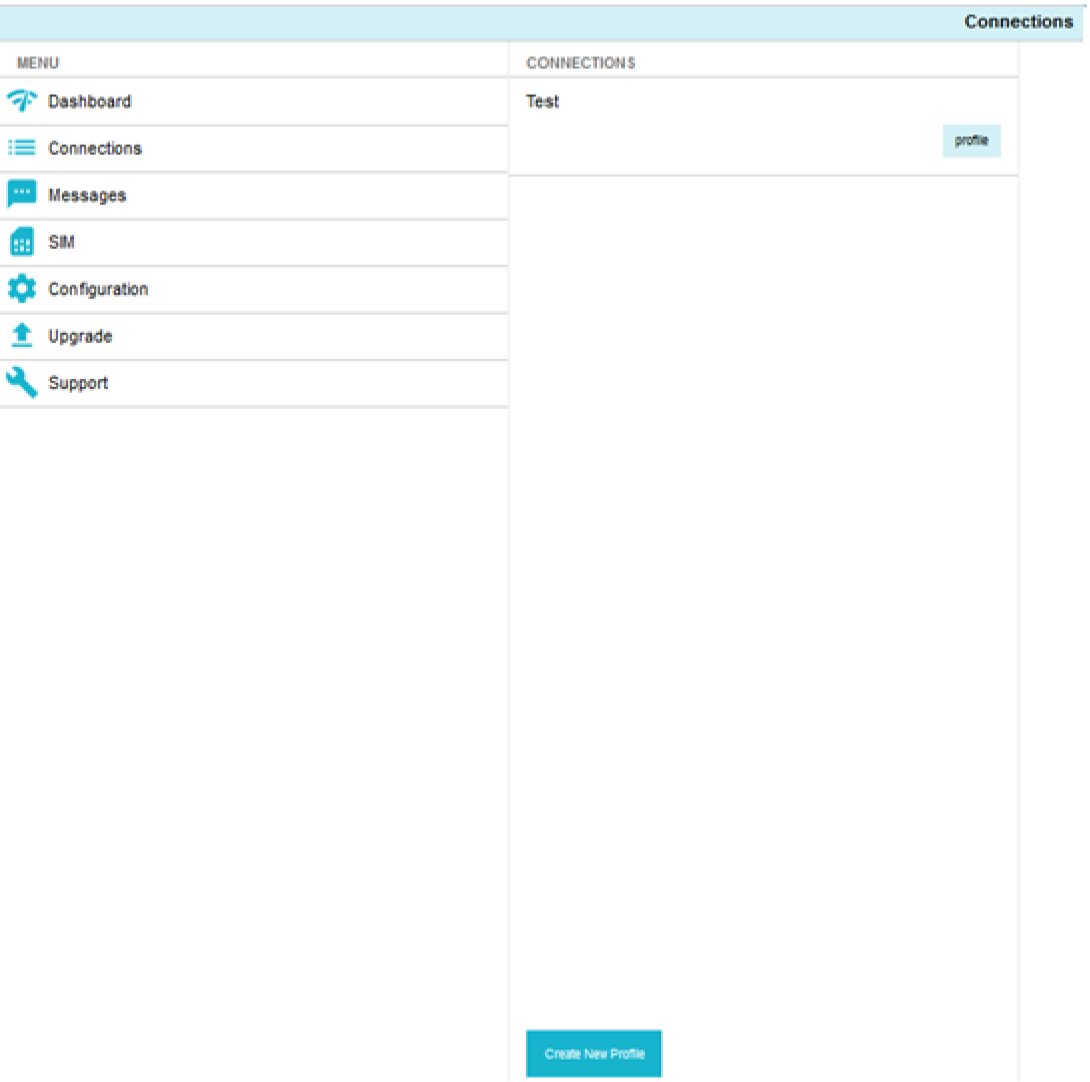
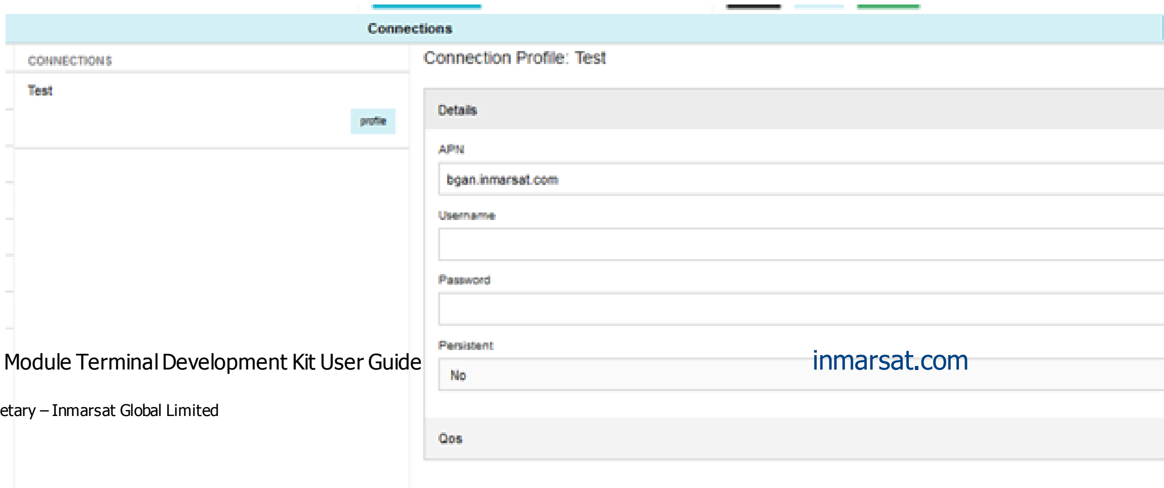


Figure 8. Connections

- To view an existing profile, select the profile icon next to the connection in question
    - The profile details load up to the right of the connections list. There are two categories: **Details** and **QoS**



Connection Profile: Test

APN: bgan.inmarsat.com

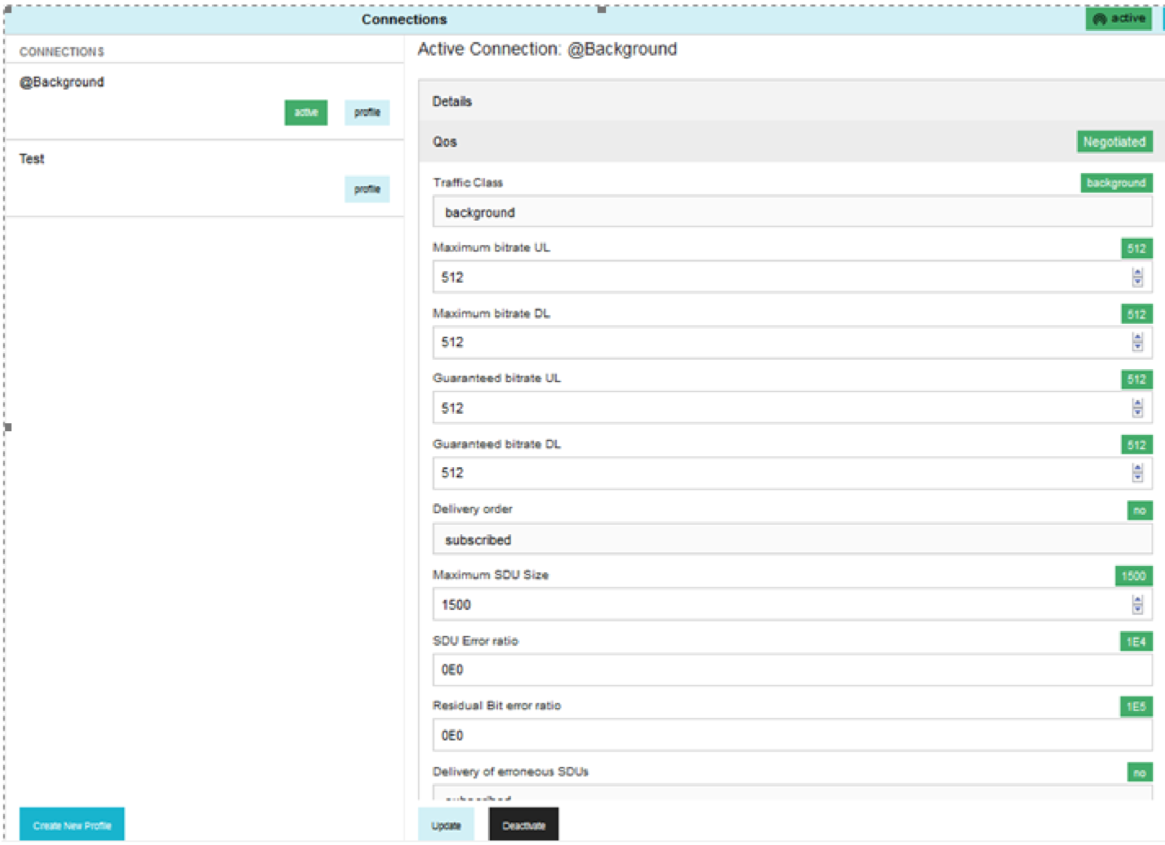
Username:

Password:

Persistent: No

- You can do any of the following with the profile in the **QoS** category:
  - **Delete**
  - Amend one or more profile configurations shown, then select **Save**
    - **Traffic class** is either `background` or `streaming` or `subscribed`
    - **Delivery order** is either `subscribed` or `Yes` or `No`
    - **Delivery of erroneous SDUs** is either `subscribed` or `No` or `Yes` or `no detect`
  - **Activate** the profile if it is not already activated

    Once activation has started, a connection profile will have an `activating` icon, and then once connection completes an `active` icon is added next to the profile button in the connections list. If you select the active icon, the negotiated QoS and connection parameters will be displayed in the right-hand part of the page, highlighted in green, as opposed to the requested parameters shown in white.



Active Connection: @Background

Traffic Class: background (background)

Maximum bitrate UL: 512 (512)

Maximum bitrate DL: 512 (512)

Guaranteed bitrate UL: 512 (512)

Guaranteed bitrate DL: 512 (512)

Delivery order: subscribed (no)

Maximum SDU Size: 1500 (1500)

SDU Error ratio: 0E0 (1E4)

Residual Bit error ratio: 0E0 (1E5)

Delivery of erroneous SDUs: subscribed (no)

  - **Deactivate** the profile if it is already active and you do not want the BRM-based UT to use it

    In that case, a connection profile will have a `deactivating` icon, and then once deactivation is complete the `deactivating` button will disappear.

- You can do any of the following with the profile in the **Details** category:
  - Specify a Username and Password for the profile
  - Specify an Access Point Name (APN) for the profile
  - Specify whether the Connection is persistent
- To amend an existing active connection, select the **active** button for the connection in question, then modify the required configurations for that connection, and select **Save**
- To create a new connection profile, select **Create New Profile**.

  A **Create New Connection Profile** dialog box loads up.
- Enter a **Connection Profile** name and select **Create**

  The new connection (default details) profile shows in the profiles list, and you can view and amend it as described in the aforementioned instructions.

Notes:
If an error occurs during a connection activation, a red button with the word "error" will appear next to the "profile" button. If you press this button, the error cause will be displayed at the top of the connection parameters. The same cause and error button can be seen in the right upper corner of the page. To delete the error, click on the "Clear Error" button from the current connection page.

If it is the first time a connection is activated from the connection shortcuts on the Dashboard, a new entry of the form `@ + connection type and rate`, e.g., `@Streaming 32kbps` appears in the connection profiles list in the **Connections** menu. Any actions detailed in the previous paragraphs applies here too.

9.5: Messages

To view, manage, or send Simple Message Service (SMS) messages using the BRM-based UT, select the **Messages** option from the left-hand navigation menu.

The **Messages** page loads up, per *9.5*.

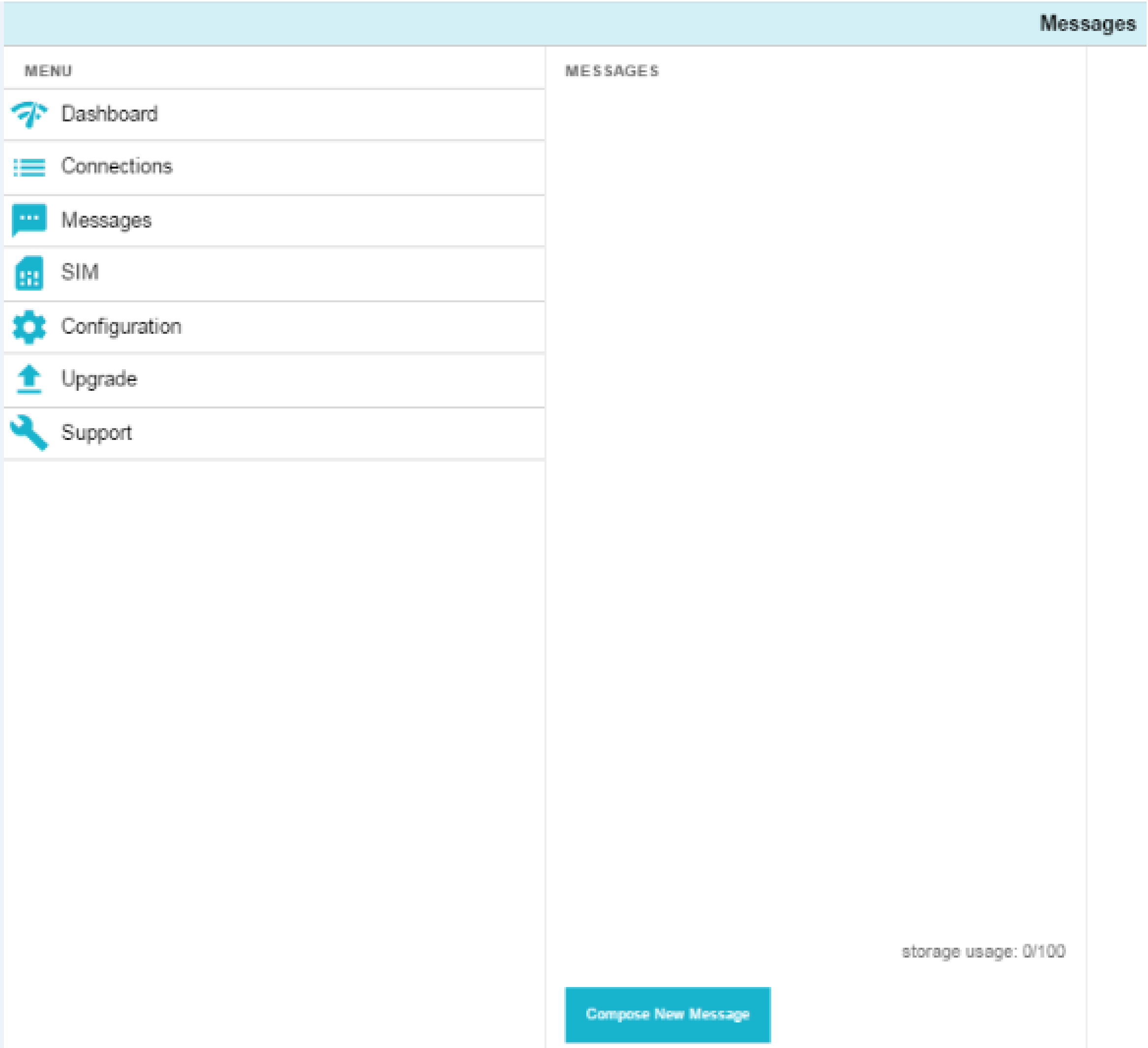
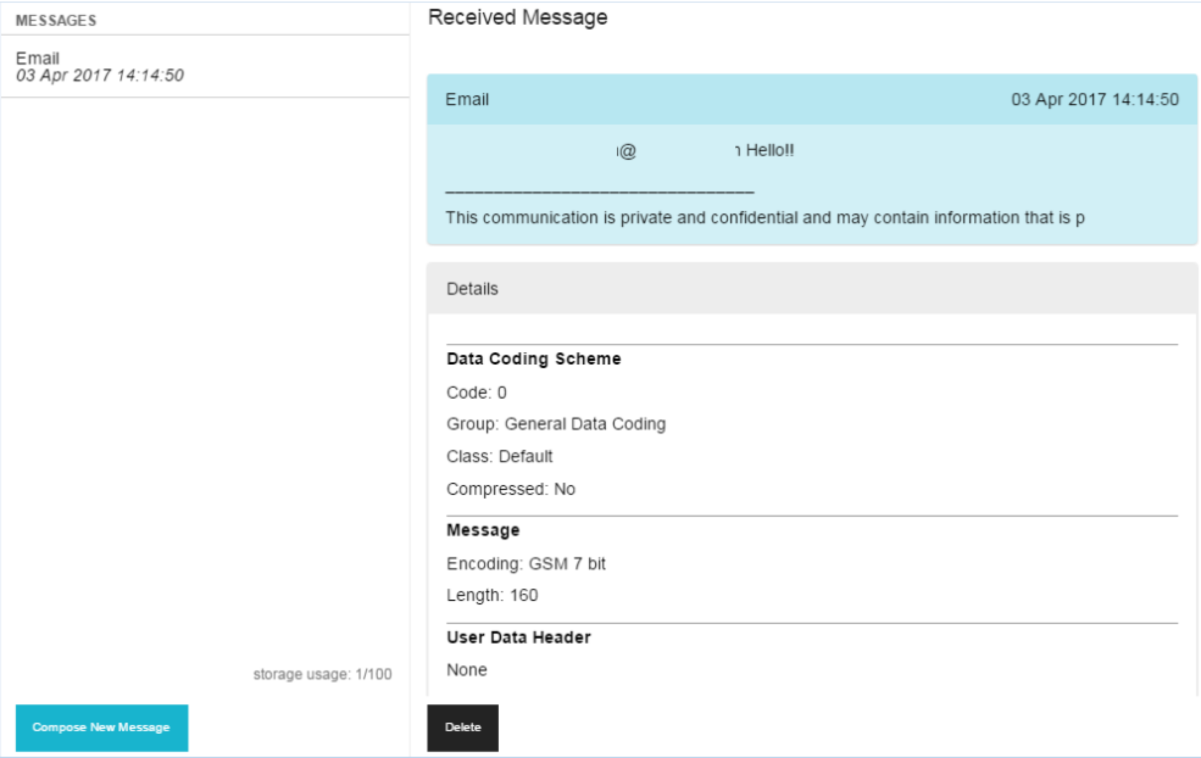


Figure 9. Messages

9.5.1: Viewing Messages

A summary of the message appears as soon as the BRM receives it. To view the message, single-click it and it will open up in the main part of the screen, per *Figure 10*.



MESSAGES

Email
03 Apr 2017 14:14:50

storage usage: 1/100

Received Message

Email 03 Apr 2017 14:14:50

@ Hello!!

____

This communication is private and confidential and may contain information that is p

Details

Data Coding Scheme

Code: 0

Group: General Data Coding

Class: Default

Compressed: No

Message

Encoding: GSM 7 bit

Length: 160

User Data Header

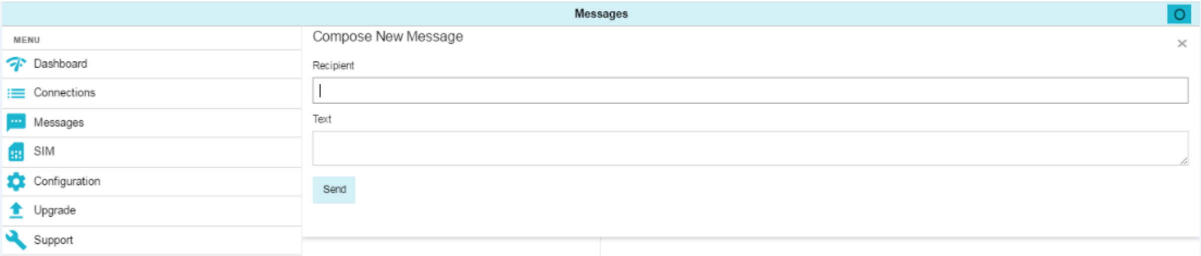
None

Figure 10. Viewing a Message

- You have the option to **Delete** the message
- You can store up to 100 SMS messages

9.5.2: Composing a New Message

To create a new SMS message and send it, take the following actions, per *Figure 11*.



Compose New Message

Recipient

Text

Figure 11. Composing a new SMS

1. Enter the phone number (must be prefixed with the country code, e.g., +44, with the leading zero removed) of the person you are sending the message to in the **Recipient** field.

2. Enter the message (maximum 160 characters) in the **Text** field.

3. Select **Send**.

9.6: SIM

To manage the PIN and/or Lock Mode for the USIM inserted in the BRM-based UT, select the **SIM** option from the left-hand navigation menu.

The **SIM** page loads up, per *9.6*.

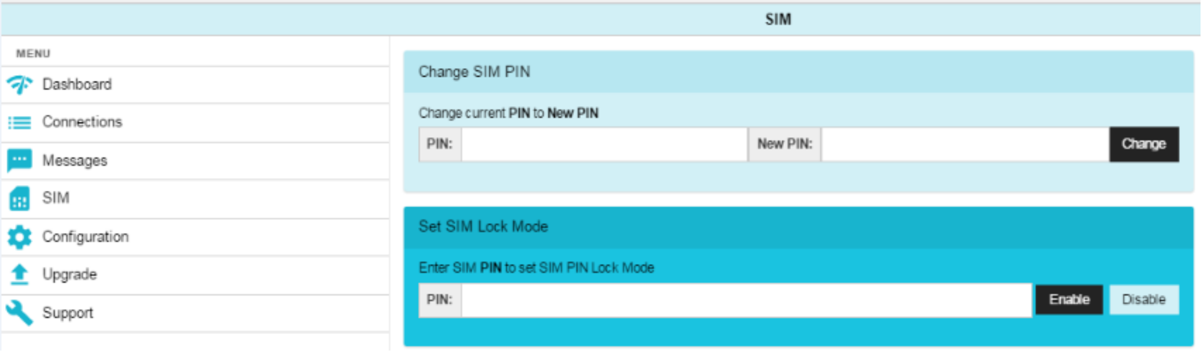


Figure 12. SIM

9.6.1: Change SIM PIN

To change the PIN of the USIM (if it has one), take the following actions:

1. Enter the current PIN in the **PIN** field.

2. Enter the new PIN in the **New PIN** field.

3. Select **Change**.

9.6.2: Set SIM Lock Mode

To enable or disable the SIM Lock Mode, enter the current SIM PIN in the **PIN** field and select **Enable** or **Disable**.

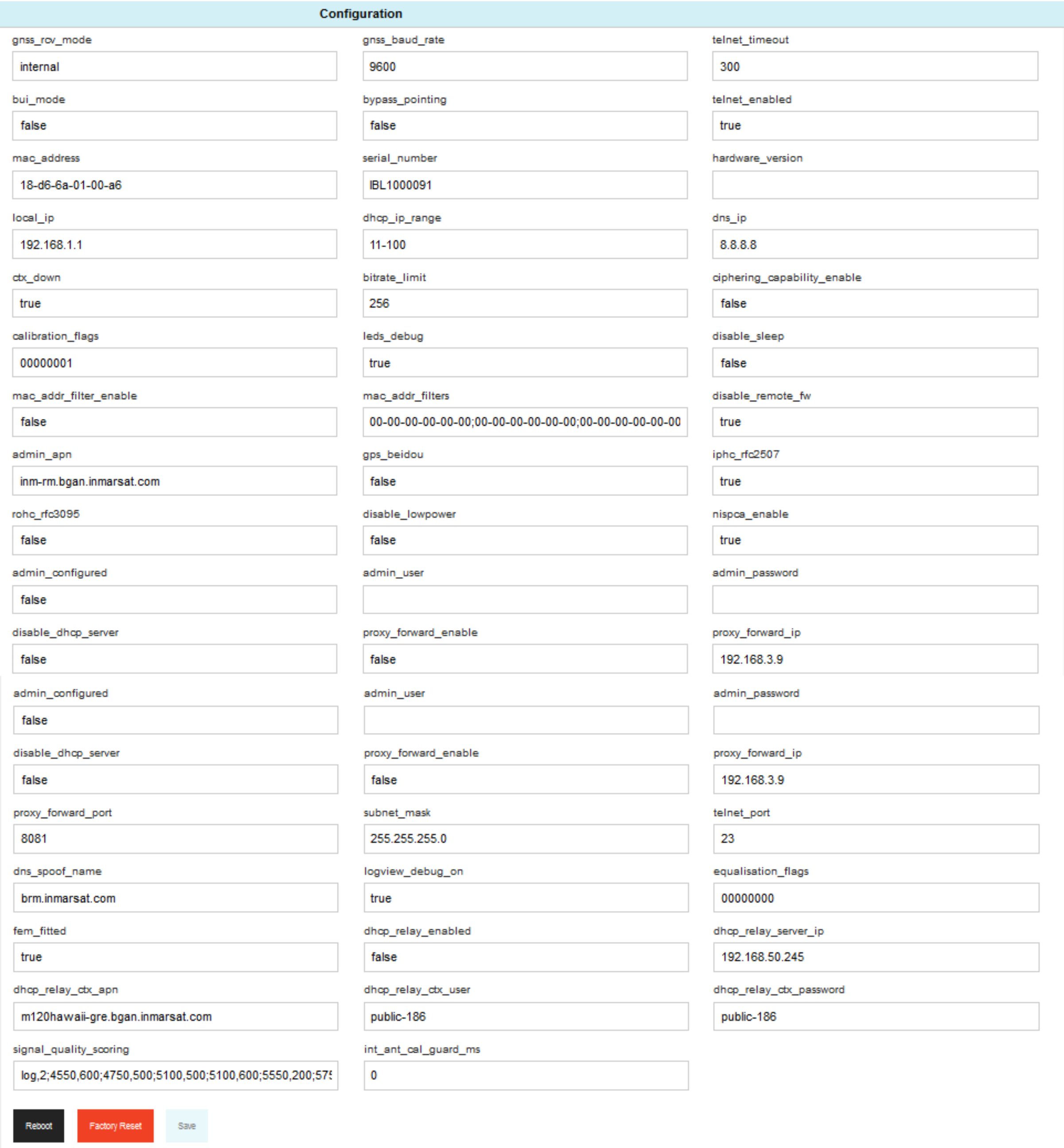
If enabled, a SIM PIN is required on every reboot/restart.

Note: If SIM Lock Mode is disabled, that implies the user won't be asked for a PIN ever again, however it still has a PIN associated with it. That PIN is the one the user has to enter whenever he wants to lock it again.

9.7: Configuration

To manage the configurations for the BRM-based UT, select the **Configurations** option from the left-hand navigation menu.

The **Configurations** page loads up, per *Figure 13*.



Configuration

gnss_rov_mode	gnss_baud_rate	telnet_timeout
internal	9600	300
bui_mode	bypass_pointing	telnet_enabled
false	false	true
mac_address	serial_number	hardware_version
18-d6-6a-01-00-a6	IBL1000091	
local_ip	dhcp_ip_range	dns_ip
192.168.1.1	11-100	8.8.8.8
ctx_down	bitrate_limit	ciphering_capability_enable
true	256	false
calibration_flags	leds_debug	disable_sleep
00000001	true	false
mac_addr_filter_enable	mac_addr_filters	disable_remote_fw
false	00-00-00-00-00-00;00-00-00-00-00-00;00-00-00-00-00-00	true
admin_apn	gps_beidou	iphc_rfc2507
inm-rm.bgan.inmarsat.com	false	true
rohc_rfc3095	disable_lowpower	nispca_enable
false	false	true
admin_configured	admin_user	admin_password
false		
disable_dhcp_server	proxy_forward_enable	proxy_forward_ip
false	false	192.168.3.9
admin_configured	admin_user	admin_password
false		
disable_dhcp_server	proxy_forward_enable	proxy_forward_ip
false	false	192.168.3.9
proxy_forward_port	subnet_mask	telnet_port
8081	255.255.255.0	23
dns_spoof_name	logview_debug_on	equalisation_flags
brm.inmarsat.com	true	00000000
fem_fitted	dhcp_relay_enabled	dhcp_relay_server_ip
true	false	192.168.50.245
dhcp_relay_ctx_apn	dhcp_relay_ctx_user	dhcp_relay_ctx_password
m120hawaii-gre.bgan.inmarsat.com	public-186	public-186
signal_quality_scoring	int_ant_cal_guard_ms	
log,2;4550,600;4750,500;5100,500;5100,600;5550,200;575	0	

Figure 13. Configurations

You can amend as required any of the configuration values. The values presented when you first access this page are the default configuration settings.

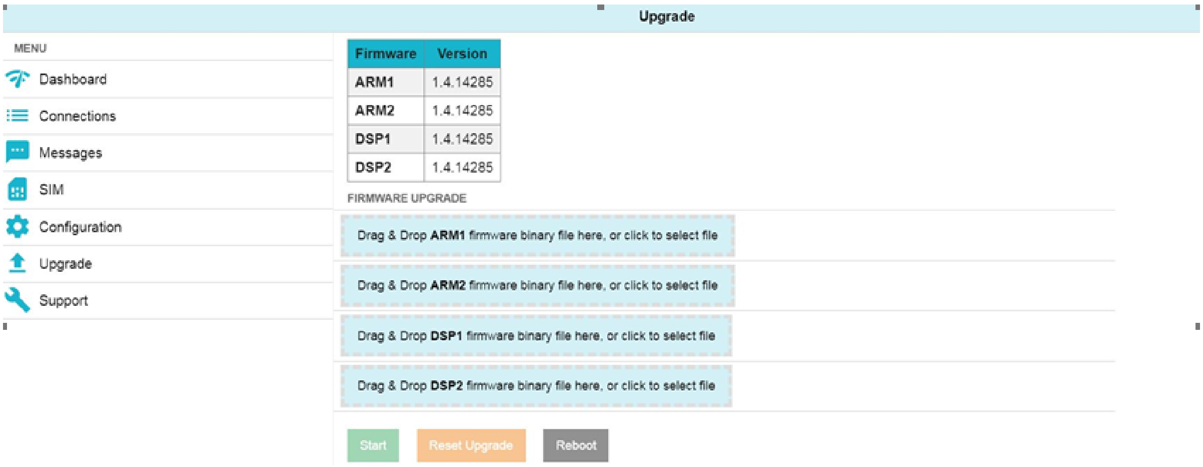
You have the following options:

- Select **Factory Reset**, which will reset all the BRM-based UT configurations to their basis factory defaults
- Amend one or more of the existing configurations, and select **Save** once the amendments are complete
- Whether Factory Reset is used or some configurations amendments have been saved, you will need to select **Reboot** to ensure the configuration change(s) are implemented

9.8: Upgrade

To upgrade the BRM firmware for the BRM-based UT, select the **Upgrade** option from the left-hand navigation menu on the Dashboard.

The **Upgrade** page loads up, per *9.8*.



Firmware	Version
ARM1	1.4.14285
ARM2	1.4.14285
DSP1	1.4.14285
DSP2	1.4.14285

FIRMWARE UPGRADE

Drag & Drop **ARM1** firmware binary file here, or click to select file

Drag & Drop **ARM2** firmware binary file here, or click to select file

Drag & Drop **DSP1** firmware binary file here, or click to select file

Drag & Drop **DSP2** firmware binary file here, or click to select file

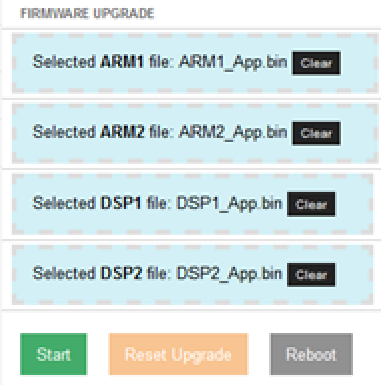
Figure 14. Upgrade

You can upgrade one or more of the cores by either dragging and dropping the relevant file from a local or network drive on your PC or laptop, or selecting each core and then browsing to the relevant file location on your PC or laptop to select the desired core.

Once each file has been selected, select **Start**.

Once each core upgrade has been completed, the **Reboot** icon will be activated. You must select this to ensure the upgrade is properly implemented.

Figure 15, *Figure 16*, *Figure 17*, and *Figure 18* show the different stages that a successful core upgrade goes through until completion.



FIRMWARE UPGRADE

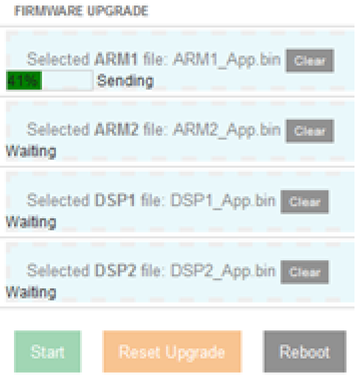
Selected **ARM1** file: ARM1_App.bin

Selected **ARM2** file: ARM2_App.bin

Selected **DSP1** file: DSP1_App.bin

Selected **DSP2** file: DSP2_App.bin

Figure 15. Cores Added


FIRMWARE UPGRADE

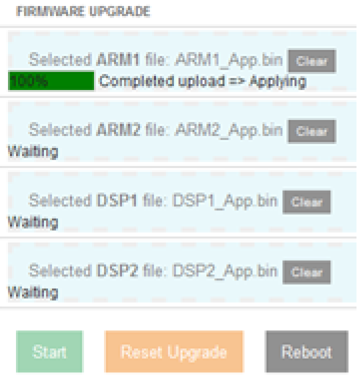
Selected **ARM1** file: ARM1_App.bin
41% Sending

Selected **ARM2** file: ARM2_App.bin
Waiting

Selected **DSP1** file: DSP1_App.bin
Waiting

Selected **DSP2** file: DSP2_App.bin
Waiting

Figure 16. Sending Core


FIRMWARE UPGRADE

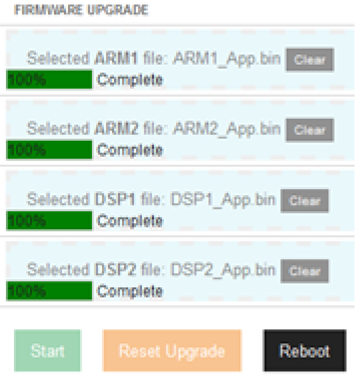
Selected **ARM1** file: ARM1_App.bin
100% Completed upload => Applying

Selected **ARM2** file: ARM2_App.bin
Waiting

Selected **DSP1** file: DSP1_App.bin
Waiting

Selected **DSP2** file: DSP2_App.bin
Waiting

Figure 17. Applying Core upgrade


FIRMWARE UPGRADE

Selected **ARM1** file: ARM1_App.bin
100% Complete

Selected **ARM2** file: ARM2_App.bin
100% Complete

Selected **DSP1** file: DSP1_App.bin
100% Complete

Selected **DSP2** file: DSP2_App.bin
100% Complete

Figure 18. All Core upgrades complete

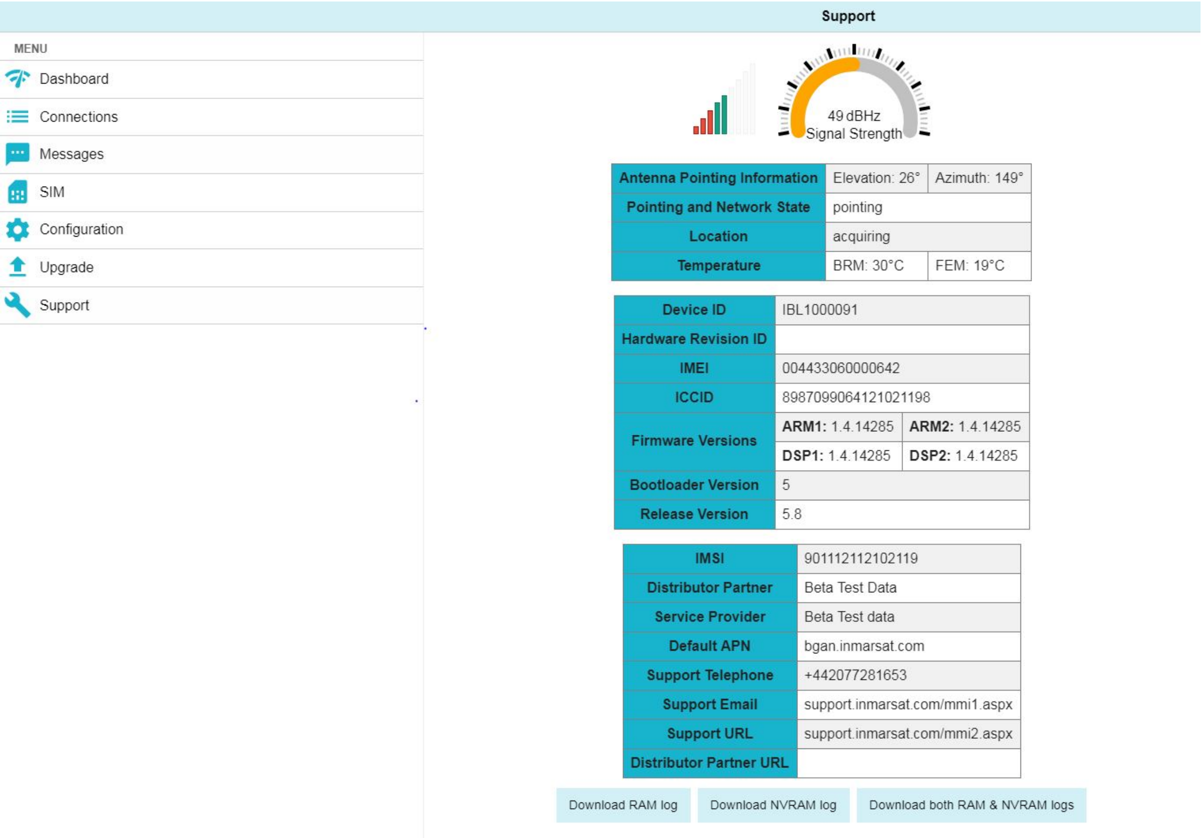
You can check that the firmware upgrade has been successful, by re-accessing the Upgrade page and checking the Firmware version for each core. The version number in each case should have changed to the expected value.

Note: If any of the core upgrades fail, you can select **Reset Upgrade**, which causes the previous firmware to be reinitialised for each core so it is possible to still use the BRM-based UT. **Reboot** would need to be selected to ensure the reversion to the previous firmware is implemented successfully.

9.9: Support

To view details of the BRM-based UT, obtain support contact details, and download relevant diagnostic logs, select the **Support** option from the left-hand navigation menu.

The **Support** page loads up, per *9.9*.



Antenna Pointing Information	Elevation: 26°	Azimuth: 149°
Pointing and Network State	pointing	
Location	acquiring	
Temperature	BRM: 30°C	FEM: 19°C

Device ID	IBL1000091	
Hardware Revision ID		
IMEI	004433060000642	
ICCID	8987099064121021198	
Firmware Versions	**ARM1:** 1.4.14285	**ARM2:** 1.4.14285
	DSP1: 1.4.14285	**DSP2:** 1.4.14285
Bootloader Version	5	
Release Version	5.8	

IMSI	901112112102119
Distributor Partner	Beta Test Data
Service Provider	Beta Test data
Default APN	bgan.inmarsat.com
Support Telephone	+442077281653
Support Email	support.inmarsat.com/mmi1.aspx
Support URL	support.inmarsat.com/mmi2.aspx
Distributor Partner URL	

Figure 19. Support

You can either download the Random Access Memory (RAM) log, the Non-Volatile RAM (NVRAM) log, or both of those logs, to a local or network location via your PC or laptop, to assist with diagnostics.

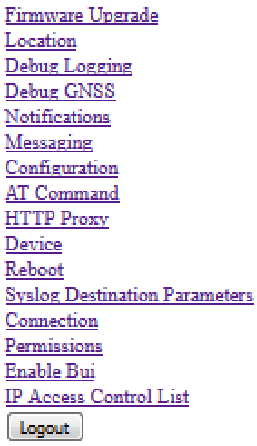
Note: The RAM log contains logs collected since the last power-up. The NVRAM logs, as the name suggests, are non-volatile and would stay in the memory until deleted or overwritten.

10: Using the Engineering WebUI

Note: The WebUI described in the following sub-sections is an **Engineering** WebUI. This WebUI is not included in the BRM Firmware and is instead available to download (*WebUIUpdater.zip*) from the **Inmarsat Developer Website** under the **TDK Resources** category at **Developer Resources > Technology Platforms > BGAN > Hardware > BGAN Radio Module (BRM) > Documentation and Resources** (You will need to sign in to be able to access this section of the website).

The BRM WebUI is a reference WebUI for VAMs to use to understand how to command and control the BRM.

The following sections detail how to use the BRM WebUI via a laptop or PC, per the list of functions shown in *Figure 20*.



- Firmware Upgrade
- Location
- Debug Logging
- Debug GNSS
- Notifications
- Messaging
- Configuration
- AT Command
- HTTP Proxy
- Device
- Reboot
- Syslog Destination Parameters
- Connection
- Permissions
- Enable Bui
- IP Access Control List

Logout

Figure 20. BRM WebUI Main Menu

Note: If you wish to use APIs via Websocket connections to perform the activities described in the following sections, please refer to the **BGAN Radio Module Application Protocol Interfaces Reference** on the **Developer Website**.

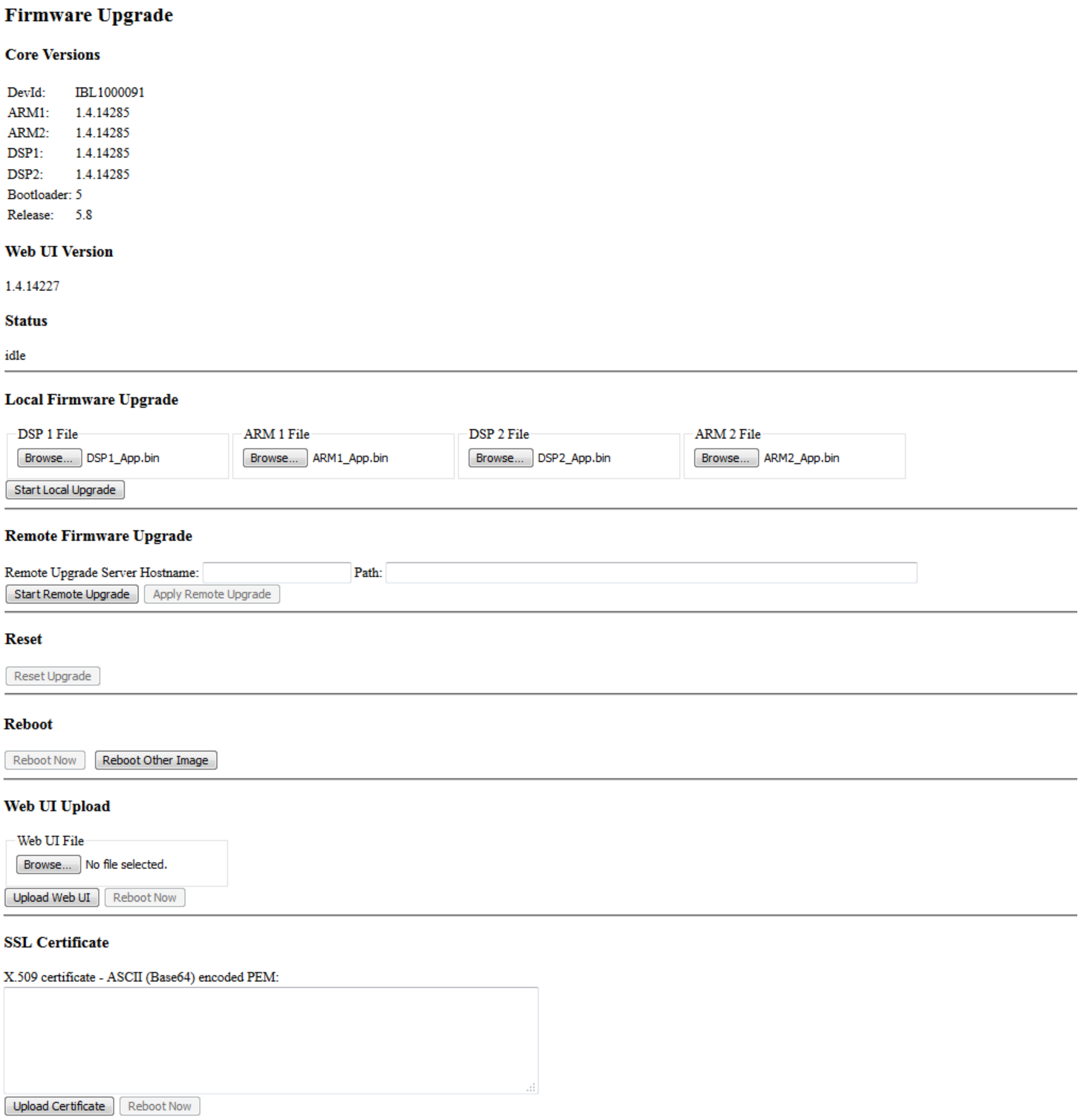
10.1: Firmware Upgrade

You can either upgrade or downgrade firmware, for one, some, or all of the four cores.

Note: The cores do not need to be upgraded in any particular order.

To access this functionality, select **Firmware Upgrade** from the main menu.

The **Firmware Upgrade** page loads up, per *Figure 21*.



Firmware Upgrade

Core Versions

DevId:	IBL1000091
ARM1:	1.4.14285
ARM2:	1.4.14285
DSP1:	1.4.14285
DSP2:	1.4.14285
Bootloader:	5
Release:	5.8

Web UI Version

1.4.14227

Status

idle

Local Firmware Upgrade

DSP 1 File: DSP1_App.bin

ARM 1 File: ARM1_App.bin

DSP 2 File: DSP2_App.bin

ARM 2 File: ARM2_App.bin

Remote Firmware Upgrade

Remote Upgrade Server Hostname: Path:

Reset

Reboot

Web UI Upload

Web UI File: No file selected.

SSL Certificate

X.509 certificate - ASCII (Base64) encoded PEM:

Figure 21. Firmware Upgrade

- **Core Versions** shows the device ID and the current versions of the firmware installed on the BRM, including Bootloader and current firmware release versions

- **WebUI Version** shows the current Engineering WebUI version installed on the BRM

- **Status** shows the current status of a firmware upgrade:
  - `idle` - status when firmware is not being upgraded
  - `local_upgrade_in_progress` - status when the **Start Upgrade** icon has been selected and the first core is being flashed
  - `local_upgrade_stage1` - status once the first core firmware upgrade has completed successfully (cores updated sequentially from left-to right as displayed on the screen)
  - `local_upgrade_stage2` - status once the second core firmware upgrade has completed successfully
  - `local_upgrade_stage3` - status once the third core firmware upgrade has completed successfully
  - `complete_awaiting_reset` - status once all four or all cores selected firmware upgrades have completed successfully. This is the prompt to select the **Reboot Now** icon

10.1.1: Local Firmware Upgrade

A Local firmware upgrade is done if you are upgrading the stored firmware from a device that is directly connected to the HDK via ethernet.

To perform a local firmware upgrade, take the following steps:

1. Log in to the **Inmarsat Developer Website** and download to a local drive on your laptop or PC connected to the TDK the latest BRM firmware from the following navigation:

- **Developer Resources > Technology Platforms > BGAN > Hardware > BGAN Radio Module (BRM) > Documentation and Resources > TDK Resources**

2. Extract the `[DSP][ARM][1][2]_App.bin` files from the downloaded .zip file.

3. Select the **Browse** button and select/open the corresponding image file for the processor cores selected to be upgraded or downgraded.

Note: You need to select the relevant `.bin` file (ARM1_App.bin; ARM2_App.bin; DSP1_App.bin; DSP2_App.bin) to run an upgrade. Do **not** select the .zip file.

4. Select the **Start Local Upgrade** icon to start the upload and upgrade or downgrade process.

Note: The first core upgrade or downgrade will take the longest to complete, because part of the process involves erasing the entire previous flash.

Select **Reset Upgrade** if you wish to abort and reset the upload and upgrade process. Do not select this option unless you wish to abort the process. This option only becomes available once the **Start Local Upgrade** icon has been selected.

5. Select **Reboot Now** to restart the BRM and boot from the stored firmware upgrade.

Note: This option only becomes available once the upgrade of a firmware file is complete.

If the upgrade or downgrade has not succeeded for some reason, you can also return the BRM to its previous firmware version, by selecting the **Reboot Other Image** button.

Note: If for any reason the upgrade is not successful and the connection to the BRM is lost then reboot the BRM three (3) times using the Reset button on the HDK, and the BRM will boot up using the previous working image.

10.1.2: Remote Firmware Upgrade

You may want to test an upgrade of BRM firmware against a remote firmware server, in which case the new firmware will be downloaded over the relevant network from the relevant file path (one per image) on a remote server, via an active Admin PDP Context on the BRM.

Note: It is possible to use a BGAN Application Tester (BAT) or BGAN-on-a-Bench (BoB) to simulate a Firmware Upgrade with upgraded firmware on it.

To perform a remote firmware upgrade, take the following steps:

1. Set the following values in the **Configuration** page and then **reboot** the BRM, to ensure that the **Admin PDP Context** is **active** and **correctly configured**, to allow you to remotely upgrade the firmware:

> **admin_apn** = `<APN provided by Inmarsat>`

> **admin_configured** = `true`

> **admin_user** = `<Provided by Inmarsat>`

> **admin_password** = `<Provided by Inmarsat>`

> **disable_remote_fw** = `false`

2. In the **Firmware Upgrade** page, enter the Hostname of the server from which the new firmware will be downloaded into the **Remote Upgrade Server Hostname** field.

3. Enter the file path on the server from which the new firmware will be downloaded into the **Path** field.

4. Select the **Start Remote Upgrade** icon. This will only download the core images that are different to the current ones on the BRM.

5. Once the new firmware has been downloaded, select the **Apply Remote Upgrade** icon.

You can use **Reset Upgrade**, **Reboot Other Image**, or **Reboot Now** as described in **Local Firmware Upgrade**.

For more information about the remote firmware upgrade, please refer to *Firmware Upgrading a BRM based Terminal Application Note*.

10.1.3: WebUI Upload

To upload an alternative WebUI, select **WebUI Upload**, choose the relevant file, and select **Upload WebUI**.

Note: You need to select the corresponding `.zip` file (`EngineeringWebUI.zip`), available on the **Inmarsat Developer Website**.

The BRM needs to be rebooted so that the new WebUI can be properly installed.

10.1.4: SSL Certificate

The Secure Sockets Layer (SSL) certificate section of the page allows you to upload an SSL certificate (in this case, a Domain Validation Certificate) upon the expiry of the pre-loaded certificate on the BRM. The validity of the certificate is set to 10 years, and when it does expire a new certificate must be installed on the BRM, without which any browser access would warn of an expired security certificate.

Note: A unique SSL certificate for making an HTTPS connection is pre-loaded on the BRM.

To upload an alternative SSL certificate, once it has been received from Inmarsat or an Inmarsat-nominated entity, take the following actions:

1. Save the SSL certificate (.PEM file) to a local drive on the laptop or PC connected to the TDK.

2. Open the .PEM file and copy the entire content.

3. Paste that content into the free-text box in the **SSL Certificate** section.

4. Select **Upload Certificate**.

5. Once the upload is complete, select **Reboot Now**.

10.2: Location

To access this functionality, select **Location** from the main menu.

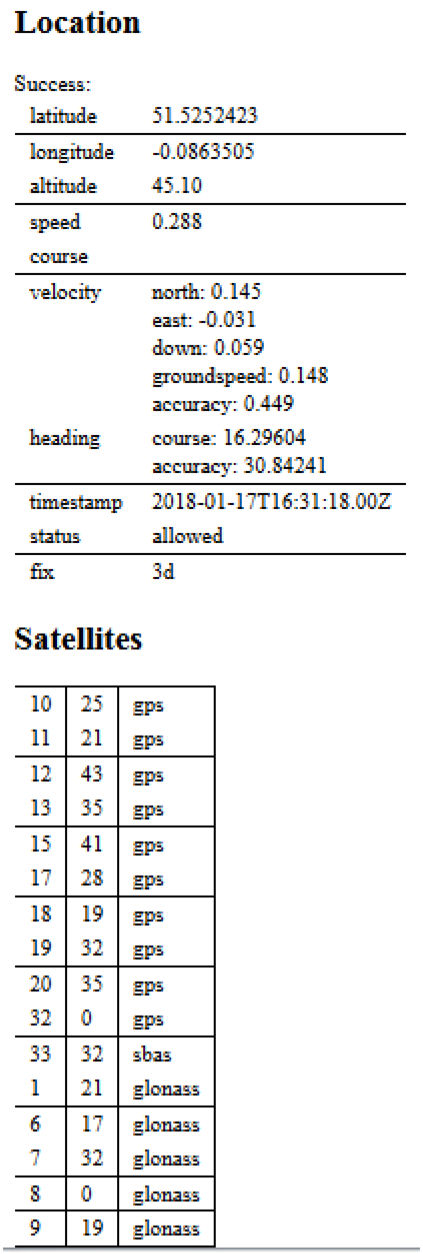
Note: This functionality will return the appropriate location value in the WebUI if an appropriate GNSS antenna is connected to the GNSS U.FL connector on the BRM, and if the GNSS antenna has good visibility to the sky.

The **Location** page loads up, per *10.2*.

This page shows the location of the BRM, as received from the GNSS satellite constellations for which the BRM is configured. It also shows speed, course data, velocity and heading.

Notes:
Per *10.2*, if the BRM is configured to receive the Beidou GPS satellite constellation, then the output will show `gps_beidou` instead of `gps` and `glonass`.

The first (looking from left to right in the output) value in each entry in the example output in *10.2* represents the satellite identifier in the relevant GNSS constellation, and the second value represents the signal quality received for that satellite.



Location

Success:

latitude	51.5252423
longitude	-0.0863505
altitude	45.10
speed	0.288
course	
velocity	north: 0.145 east: -0.031 down: 0.059 groundspeed: 0.148 accuracy: 0.449
heading	course: 16.29604 accuracy: 30.84241
timestamp	2018-01-17T16:31:18.00Z
status	allowed
fix	3d

Satellites

10	25	gps
11	21	gps
12	43	gps
13	35	gps
15	41	gps
17	28	gps
18	19	gps
19	32	gps
20	35	gps
32	0	gps
33	32	sbas
1	21	glonass
6	17	glonass
7	32	glonass
8	0	glonass
9	19	glonass

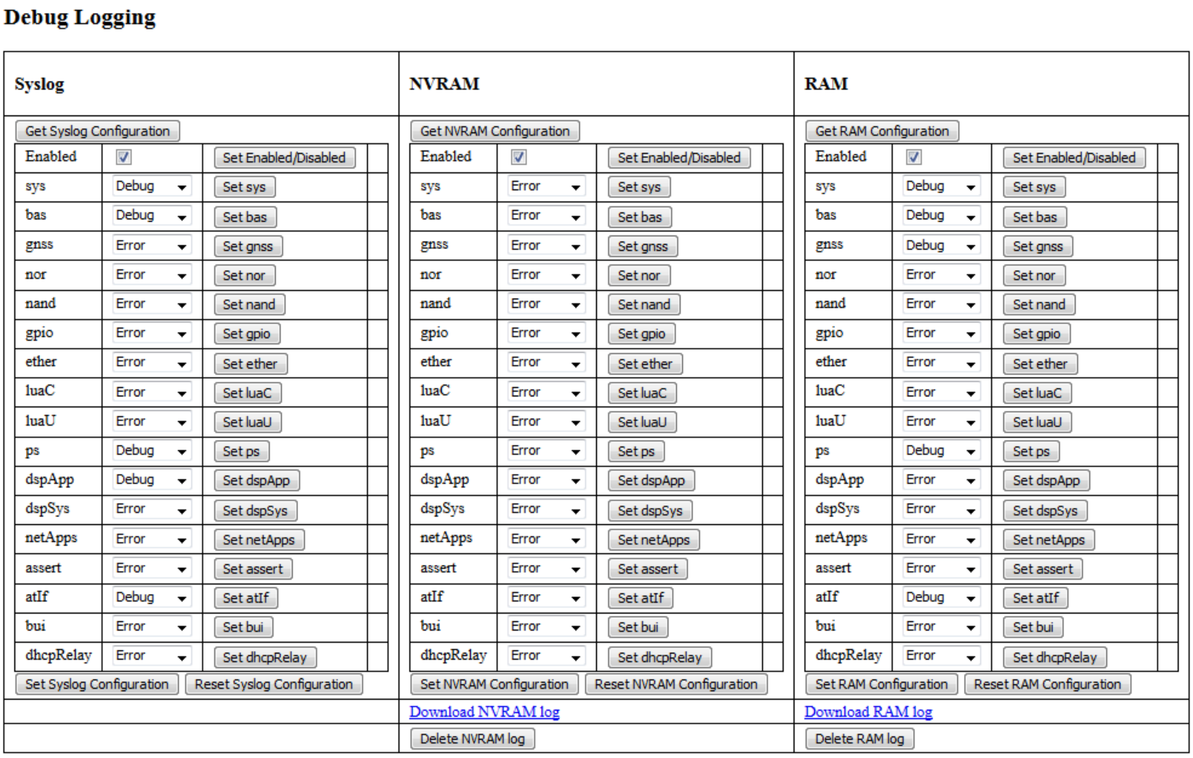
Figure 22. Location

10.3: Debug Logging

To access this functionality, select **Debug Logging** from the main menu.

The **Debug Logging** page loads up, per *Figure 23*. It shows the current logging configurations for each aspect of **Syslog**, **NVRAM** and **RAM** logging, and allows you to amend those configurations if required.

Note: Refer to the **Development and Monitoring Interfaces** section of the *BGAN Radio Module Technical Specification* for more details about Logging messages, including the different message categories.



Debug Logging

Syslog			NVRAM			RAM		
Get Syslog Configuration			Get NVRAM Configuration			Get RAM Configuration		
Enabled	☑	Set Enabled/Disabled	Enabled	☑	Set Enabled/Disabled	Enabled	☑	Set Enabled/Disabled
sys	Debug	Set sys	sys	Error	Set sys	sys	Debug	Set sys
bas	Debug	Set bas	bas	Error	Set bas	bas	Debug	Set bas
gnss	Error	Set gnss	gnss	Error	Set gnss	gnss	Debug	Set gnss
nor	Error	Set nor	nor	Error	Set nor	nor	Error	Set nor
nand	Error	Set nand	nand	Error	Set nand	nand	Error	Set nand
gpio	Error	Set gpio	gpio	Error	Set gpio	gpio	Error	Set gpio
ether	Error	Set ether	ether	Error	Set ether	ether	Error	Set ether
luaC	Error	Set luaC	luaC	Error	Set luaC	luaC	Error	Set luaC
luaU	Error	Set luaU	luaU	Error	Set luaU	luaU	Error	Set luaU
ps	Debug	Set ps	ps	Error	Set ps	ps	Debug	Set ps
dspApp	Debug	Set dspApp	dspApp	Error	Set dspApp	dspApp	Error	Set dspApp
dspSys	Error	Set dspSys	dspSys	Error	Set dspSys	dspSys	Error	Set dspSys
netApps	Error	Set netApps	netApps	Error	Set netApps	netApps	Error	Set netApps
assert	Error	Set assert	assert	Error	Set assert	assert	Error	Set assert
atIf	Debug	Set atIf	atIf	Error	Set atIf	atIf	Debug	Set atIf
bui	Error	Set bui	bui	Error	Set bui	bui	Error	Set bui
dhcpRelay	Error	Set dhcpRelay	dhcpRelay	Error	Set dhcpRelay	dhcpRelay	Error	Set dhcpRelay
Set Syslog Configuration	Reset Syslog Configuration		Set NVRAM Configuration	Reset NVRAM Configuration		Set RAM Configuration	Reset RAM Configuration	
			Download NVRAM log			Download RAM log		
			Delete NVRAM log			Delete RAM log		

Figure 23. Debug Logging

- Select the **Get Syslog Configuration** icon to see the current syslog logging configuration values, if the configuration is not already shown by default

- Select the **Get NVRAM Configuration** icon to see the current NVRAM (Non-Volatile RAM) logging configuration values, if the configuration is not already shown by default

- Select the **Get RAM Configuration** icon to see the current RAM Random Access Memory) logging configuration values, if the configuration is not already shown by default

- Select the **Set Enabled/Disabled** icon to enable or disable the ability to amend logging configuration values

- Select the relevant **Set** icon to confirm an amendment you have made to a particular setting

- Select the **Set Syslog Configuration** icon to confirm modification of any syslog logging configuration values

- Select the **Set NVRAM Configuration** icon to confirm modification of any NVRAM logging configuration values

- Select the **Set RAM Configuration** icon to confirm modification of any RAM logging configuration values

- Select the **Reset Syslog Configuration**, **Reset NVRAM Configuration** or **Reset RAM Configuration** to change to default configuration of each of the debugging blocks

- Select the relevant **Download** link to view the requested log on your local machine

- Select the relevant **Delete** icon to delete a log you have previously downloaded

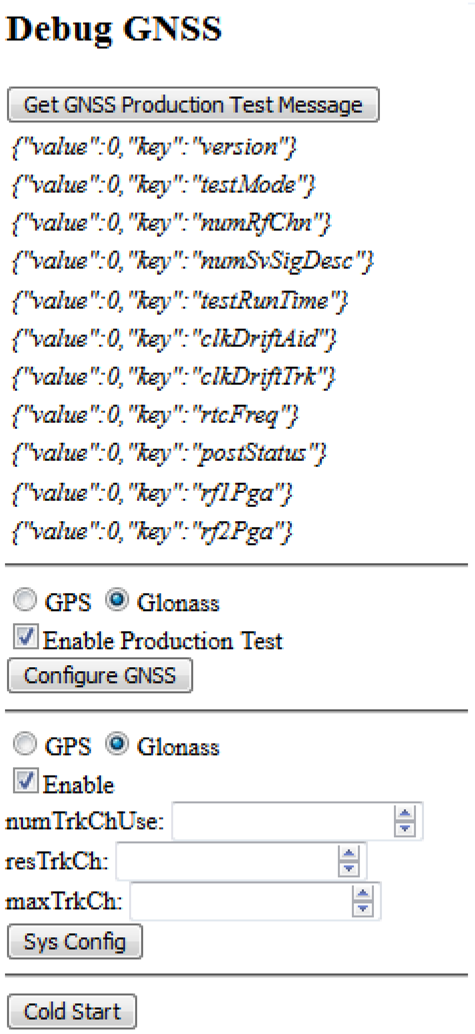
10.4: Debug GNSS

This functionality is intended for production test of the GNSS receiver with a specific single satellite test signal for use by VAMs.

Note: This functionality only debugs the internal GNSS chipset on the BRM.

To access this functionality, select **Debug GNSS** from the main menu.

The **Debug GNSS** page loads up, per *Figure 24*. It allows you to test, configure, and perform a restart of the GNSS functionality on the BRM.



Debug GNSS

```
{"value":0,"key":"version"}
{"value":0,"key":"testMode"}
{"value":0,"key":"numRfChn"}
{"value":0,"key":"numSvSigDesc"}
{"value":0,"key":"testRunTime"}
{"value":0,"key":"clkDriftAid"}
{"value":0,"key":"clkDriftTrk"}
{"value":0,"key":"rtcFreq"}
{"value":0,"key":"postStatus"}
{"value":0,"key":"rf1Pga"}
{"value":0,"key":"rf2Pga"}
```

○ GPS ● Glonass

☑ Enable Production Test

○ GPS ● Glonass

☑ Enable

numTrkChUse:

resTrkCh:

maxTrkCh:

Figure 24. Debug GNSS

- Select **Get GNSS Production Test Message** if you want to see the outcome of a GNSS Test Message
- Select either the **GPS** or **Glonass** radio button, according to which constellation of GPS satellites you want to test the GNSS receiver with
- Check the **Enable Production Test** check box if you want to enable the BRM to perform a production test of the GNSS receiver
- Select either the **GPS** or **Glonass** radio button, according to which constellation of GPS satellites you want to configure the GNSS receiver with

- Check the **Enable** check box if you want to enable the GNSS receiver
- Enter suitable values for the following fields, to configure the GNSS receiver accordingly:
  - `numTrkChUse` - the numerical value entered indicates the number of Tracked Channels you want the GNSS receiver to use
  - `resTrkCh` - the numerical value entered indicates the minimum number of Tracked Channels per GNSS you want the GNSS receiver to use
  - `maxTrkCh` - the numerical value entered indicates the maximum number of Tracked Channels per GNSS you want the GNSS receiver to use
- Select **Sys Config** to implement the configurations you have set for the Tracked Channels
- Select **Cold Start** if you want to see how the GNSS Receiver operates if it has no knowledge of the previous GPS location of the BRM, and has to re-learn the GPS location

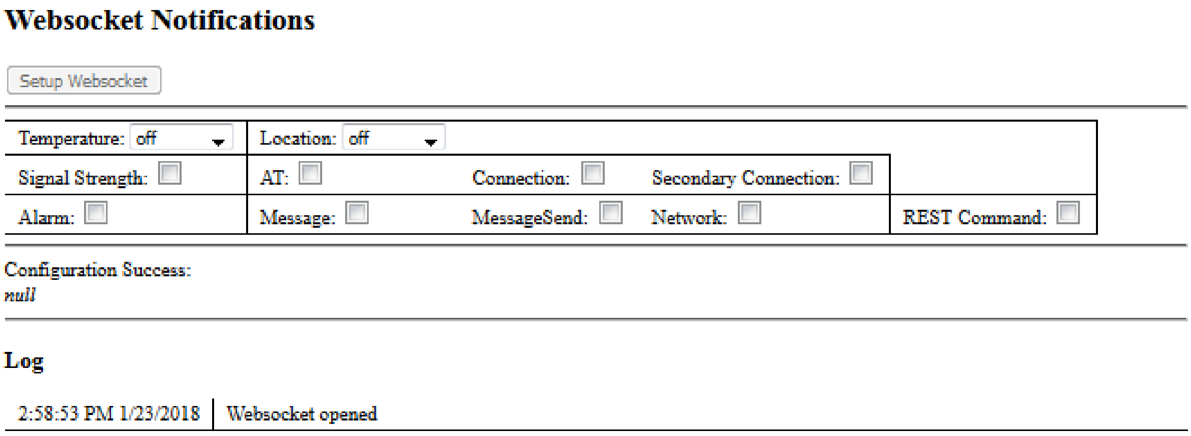
> **Note:** The GNSS Receiver will typically remember the GPS location from when it was last operational; however, this knowledge may not be present if the BRM has not been operational for an extended period of time, or if the BRM has not previously been able to establish its GPS location.

10.5: Notifications

To access this functionality, select **Notifications** from the main menu.

Refer to the **Websockets** section of the *BGAN Radio Module Technical Specification* for details.

The **Websocket Notifications** page loads up, per **10.5**.



Websocket Notifications

Temperature: off	Location: off			
Signal Strength: □	AT: □	Connection: □	Secondary Connection: □	
Alarm: □	Message: □	MessageSend: □	Network: □	REST Command: □

Configuration Success:
null

Log

2:58:53 PM 1/23/2018 | Websocket opened

Figure 25. Notifications

You can configure the BRM to report websocket notifications for any of the following parameters by selecting `fast`, `slow`, or `medium`, from the relevant drop-down menu. These are set to `off` by default:

> **Note:** Fast, slow, and medium relate to the frequency with which each notification is listed in the output. Fast = one notification per second; Medium = one notification every 10 seconds; Slow = one notification every 30 seconds.

- **Temperature** (of the BRM and the FEM)
- **Location**

You can also configure the BRM to report **Signal Strength**, **AT**, **Message** / **Messagesends**, **Connection**/**Secondary Connection**/**Network**-related Websocket notifications, or any **Alarm** that may be generated for the UT via Websocket, by checking the relevant check box. These boxes are unchecked by default.

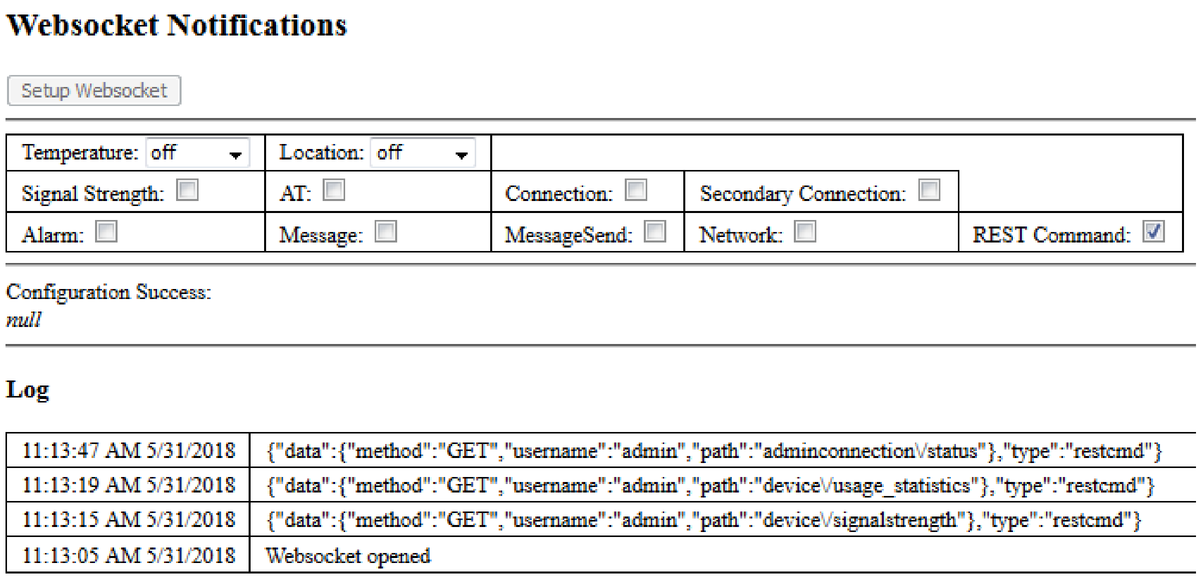
10.5.1: REST Command Notifications

Local and Remote RESTful commands can be captured in the Notifications page.

As an example, in *10.5* the same REST Commands have been locally generated (through WebUI) and remotely issued with an identical result at the end, per *Table 1*.

Locally Generated REST Commands	Remotely Generated REST Commands
Device / Get Admin Connection Enabled	GET https://[remote server]/auth/v1/adminconnection/status
Device / Get Usage Statistics	GET https://[remote server]/auth/v1/device/usage_statistics
Device / Get Signal Strength	GET https://[remote server]/auth/v1/device/signalstrength

Table 1. Locally and Remotely generated REST commands



Websocket Notifications

Temperature: off	Location: off			
Signal Strength: □	AT: □	Connection: □	Secondary Connection: □	
Alarm: □	Message: □	MessageSend: □	Network: □	REST Command: ☑

Configuration Success:
null

Log

```
11:13:47 AM 5/31/2018  {"data":{"method":"GET","username":"admin","path":"adminconnection\/status"},"type":"restcmd"}
11:13:19 AM 5/31/2018  {"data":{"method":"GET","username":"admin","path":"device\/usage_statistics"},"type":"restcmd"}
11:13:15 AM 5/31/2018  {"data":{"method":"GET","username":"admin","path":"device\/signalstrength"},"type":"restcmd"}
11:13:05 AM 5/31/2018  Websocket opened
```

Figure 26. REST Command Websocket Notifications

10.6: Messaging

To access this functionality, select **Messaging** from the main menu.

The **Messaging** page loads up, per *10.6*.

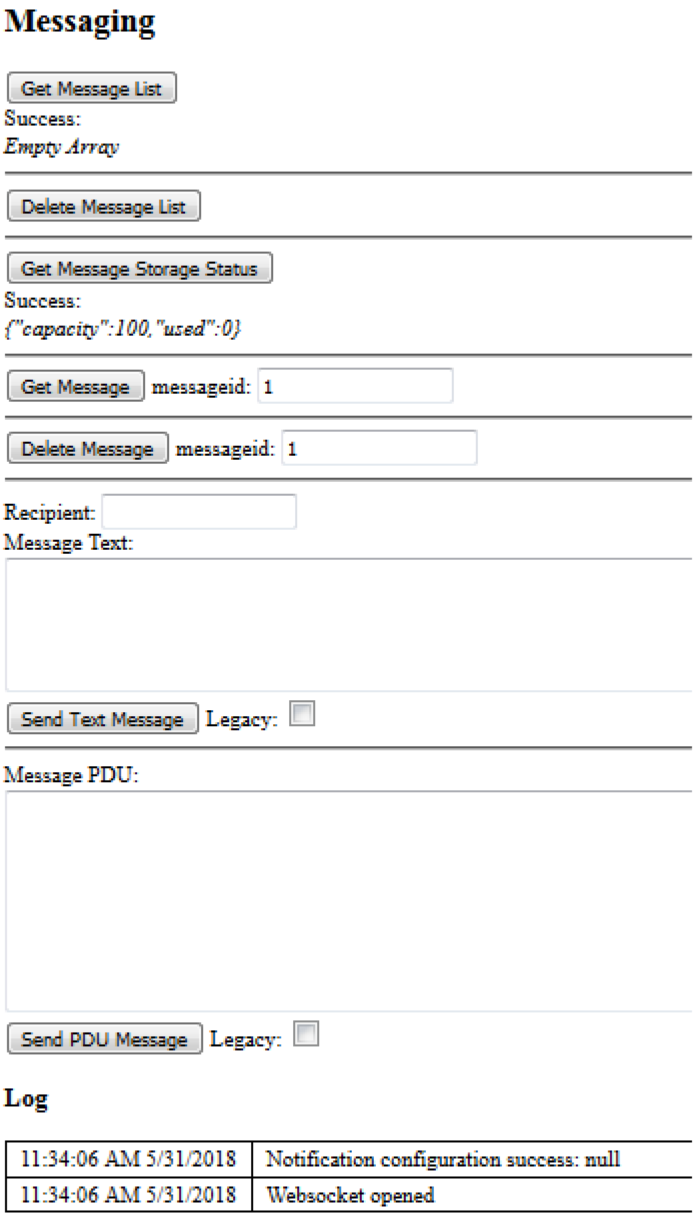
This part of the WebUI allows a user to view or delete all or specific SMS messages, or to compose and send an SMS message using the BRM, or to check the message storage status.

Notes:

The BRM stores SMS messages on the external USIM. The number of messages that can be stored is dependent on the available memory on the USIM.

If a user has permissions to view SMS messages, then that user is able to view all sent and received SMS messages on the BRM, regardless of which user has sent or received the SMS.

If SIM PIN entry is required, the user has to enter it in the Device page before accessing the SMS list, otherwise an error will be displayed in the **Message List** and **Message Storage Status** saying `Error 43: {“errors”: {“message”:”\r\n+CMS ERROR: SM BL not ready\r\n”,”code”:403}}`.



Messaging

Success:
Empty Array

Success:
{"capacity":100,"used":0}

messageid: 1

messageid: 1

Recipient:
Message Text:

Legacy: □

Message PDU:

Legacy: □

Log

11:34:06 AM 5/31/2018	Notification configuration success: null
11:34:06 AM 5/31/2018	Websocket opened

Figure 27. Messaging

Message sending options are either Text mode or PDU mode:

Text Mode	PDU Mode
When entering the telephone number in the **Recipient** field, start it with +. **Note:** If + is omitted in the **Recipient** field, the message will be sent from the BRM, but will not be delivered to the other end.	The telephone number and the type is encoded in the pdu message itself. Although some encoders constructs the PDU without considering the + in the recipient number, please ensure that a + is not used with the recipient number. **Note:** If PDU is constructed with +, `AT+CMGS` command immediately returns `ERROR`.
When composing a message using the **Text** mode, please remember that the size limit for a message is 140 bytes (equivalent to 160 characters with the GSM 7-bit encoding used for Text mode).	If more than 140 bytes need to be sent, they can be sent as concatenated PDU strings in PDU mode. Each PDU string is sent separately which are received at the remote device where the SMS application would combine to form on human-readable message.

Note: The WebUI does not have the intelligence to split a large message to PDU strings nor combine received PDU strings into a human-readable single message.

10.6.1: Synchronous and Asynchronous SMS Sending Process

10.6.1.1: Synchronous

Synchronous mode ensures that the message is successfully sent. In order to enable this mode, the **Legacy** box has to be checked (unchecked by default).

If the message is sent out successfully, the following response will be given after selecting **Send Text Message** or **Send PDU Message**:

```
Success: null
```

Or, if there is an error in sending:

```
Error
```

In this case, the REST command issued, as shown in the **Notifications** page, is:

```
{“data”:
{”path”:”message”,”username”:”admin”,”method”:”POST”},”type”:”restcm
d”}
```

10.6.1.2: Asynchronous

Asynchronous mode returns a response immediately with a `request_id` thus immediately freeing up the REST channel. In order to enable this mode, the **Legacy** box must be unchecked (default setting).

Whenever the message is sent to the network, a response that includes the unique REST API request ID will be returned:

```
Success: {“status”:”sending”,”request_id”:1537803266}
```

In this case, the REST commands issued, as shown in the **Notifications** page, is:

```
{“data”:
{”path”:”messagesend\/text”,”username”:”admin”,”method”:”POST”},”type”
:”restcmd”}
```

```
{“data”:{”status”:”sending”,”request_
id”:1537803266},”type”:”messagesend”}
```

And as soon as the response from the network is received:

```
{“data”:{”status”:”success”,”request_
id”:1537803266},”type”:”messagesend”}
```

10.6.2: SMS Encoding and Sending/Receiving

SMS messages are sent/received via the following mechanism:

1. Character encoding at the Terminal Equipment (TE):

   Encode the characters at the sending TE/machine/processor using any of the 5 encoding options supported by the BRM.

   UCS_2, GSM_8-bit and Hex encoded characters can only be sent in PDU mode. GSM_7-bit characters can be sent either in PDU or Text mode.

   The message is then sent from the TE to the BRM.

2. Transporting the message across the Inmarsat Air Interface:

   Once the BRM receives the appropriately encoded message it transports it to the Inmarsat network with GSM_7bit encoding.

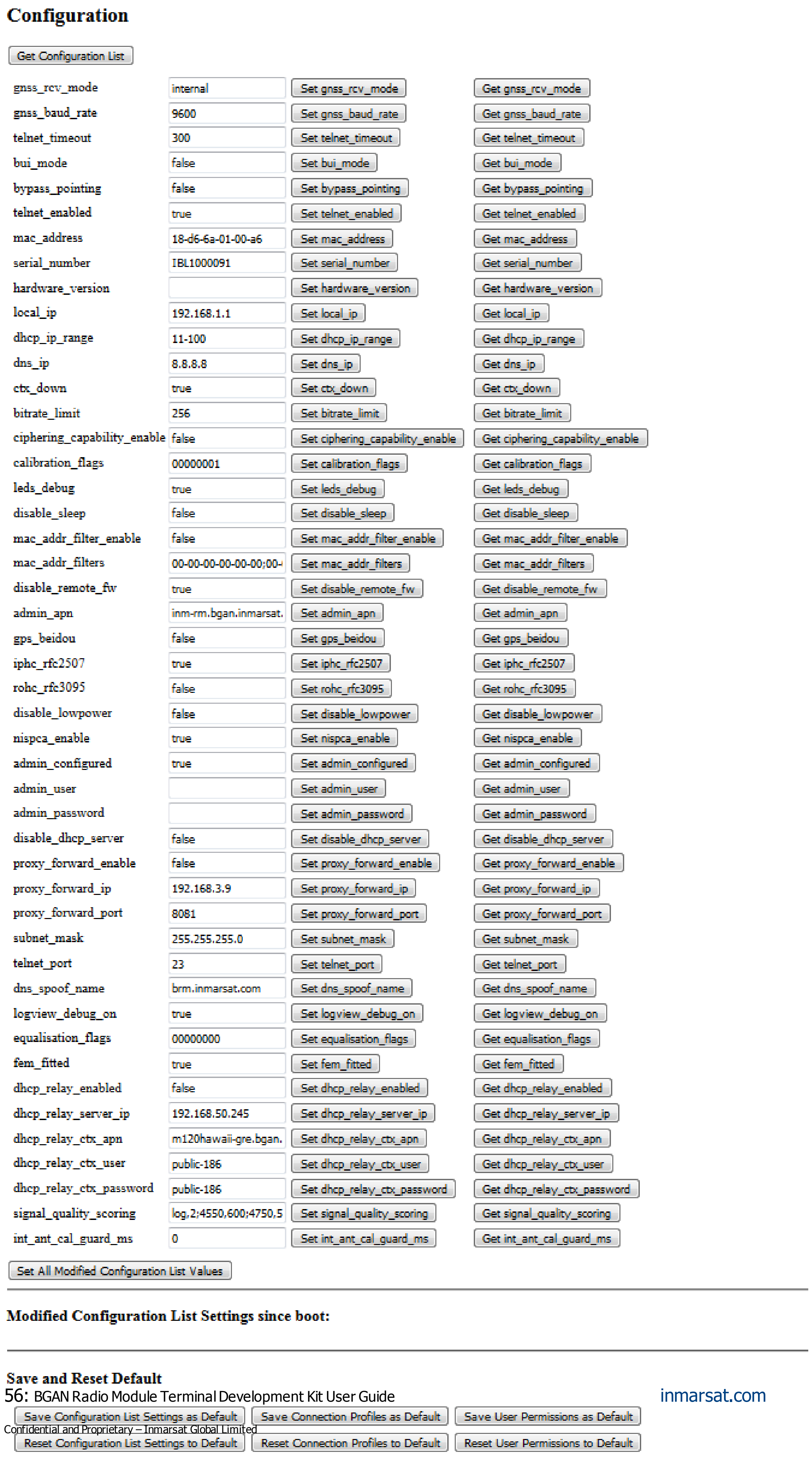
When receiving an SMS message, the opposite process takes place.

10.7: Configuration

To access this functionality, select **Configuration** from the main menu.

The **Configuration** page loads up, per *Figure 28*.

Please refer to the **BRM Configuration Keys** section of the *BGAN Radio Module Technical Specification* document for details of what each configuration key is, and the default values for each.



Configuration

Get Configuration List

gnss_rcv_mode	internal	Set gnss_rcv_mode	Get gnss_rcv_mode
gnss_baud_rate	9600	Set gnss_baud_rate	Get gnss_baud_rate
telnet_timeout	300	Set telnet_timeout	Get telnet_timeout
bui_mode	false	Set bui_mode	Get bui_mode
bypass_pointing	false	Set bypass_pointing	Get bypass_pointing
telnet_enabled	true	Set telnet_enabled	Get telnet_enabled
mac_address	18-d6-6a-01-00-a6	Set mac_address	Get mac_address
serial_number	IBL1000091	Set serial_number	Get serial_number
hardware_version		Set hardware_version	Get hardware_version
local_ip	192.168.1.1	Set local_ip	Get local_ip
dhcp_ip_range	11-100	Set dhcp_ip_range	Get dhcp_ip_range
dns_ip	8.8.8.8	Set dns_ip	Get dns_ip
ctx_down	true	Set ctx_down	Get ctx_down
bitrate_limit	256	Set bitrate_limit	Get bitrate_limit
ciphering_capability_enable	false	Set ciphering_capability_enable	Get ciphering_capability_enable
calibration_flags	00000001	Set calibration_flags	Get calibration_flags
leds_debug	true	Set leds_debug	Get leds_debug
disable_sleep	false	Set disable_sleep	Get disable_sleep
mac_addr_filter_enable	false	Set mac_addr_filter_enable	Get mac_addr_filter_enable
mac_addr_filters	00-00-00-00-00-00;00-	Set mac_addr_filters	Get mac_addr_filters
disable_remote_fw	true	Set disable_remote_fw	Get disable_remote_fw
admin_apn	inm-rm.bgan.inmarsat.	Set admin_apn	Get admin_apn
gps_beidou	false	Set gps_beidou	Get gps_beidou
iphc_rfc2507	true	Set iphc_rfc2507	Get iphc_rfc2507
rohc_rfc3095	false	Set rohc_rfc3095	Get rohc_rfc3095
disable_lowpower	false	Set disable_lowpower	Get disable_lowpower
nispca_enable	true	Set nispca_enable	Get nispca_enable
admin_configured	true	Set admin_configured	Get admin_configured
admin_user		Set admin_user	Get admin_user
admin_password		Set admin_password	Get admin_password
disable_dhcp_server	false	Set disable_dhcp_server	Get disable_dhcp_server
proxy_forward_enable	false	Set proxy_forward_enable	Get proxy_forward_enable
proxy_forward_ip	192.168.3.9	Set proxy_forward_ip	Get proxy_forward_ip
proxy_forward_port	8081	Set proxy_forward_port	Get proxy_forward_port
subnet_mask	255.255.255.0	Set subnet_mask	Get subnet_mask
telnet_port	23	Set telnet_port	Get telnet_port
dns_spoof_name	brm.inmarsat.com	Set dns_spoof_name	Get dns_spoof_name
logview_debug_on	true	Set logview_debug_on	Get logview_debug_on
equalisation_flags	00000000	Set equalisation_flags	Get equalisation_flags
fem_fitted	true	Set fem_fitted	Get fem_fitted
dhcp_relay_enabled	false	Set dhcp_relay_enabled	Get dhcp_relay_enabled
dhcp_relay_server_ip	192.168.50.245	Set dhcp_relay_server_ip	Get dhcp_relay_server_ip
dhcp_relay_ctx_apn	m120hawaii-gre.bgan.	Set dhcp_relay_ctx_apn	Get dhcp_relay_ctx_apn
dhcp_relay_ctx_user	public-186	Set dhcp_relay_ctx_user	Get dhcp_relay_ctx_user
dhcp_relay_ctx_password	public-186	Set dhcp_relay_ctx_password	Get dhcp_relay_ctx_password
signal_quality_scoring	log.2;4550.600;4750.5	Set signal_quality_scoring	Get signal_quality_scoring
int_ant_cal_guard_ms	0	Set int_ant_cal_guard_ms	Get int_ant_cal_guard_ms

Set All Modified Configuration List Values

Modified Configuration List Settings since boot:

Save and Reset Default

Save Configuration List Settings as Default
Save Connection Profiles as Default
Save User Permissions as Default
Reset Configuration List Settings to Default
Reset Connection Profiles to Default
Reset User Permissions to Default

Figure 28. Configuration

- Select the **Get Configuration List** icon to view the current BRM configurations
- Select the **Get** icon for any specific BRM configuration for which you wish to view the current value
- Amend values for any BRM configurations you wish to amend, and select the **Set** icon for each BRM configuration you have amended to update it accordingly
- Select the **Set All Modified Configurations** icon if you have changed all BRM configurations
- Select the **Save Configuration List Settings as Default** icon if you wish to set the current configuration as default
- Select the **Reset Configuration List Settings to Default** icon if you have changed the configuration and want to revert it back to the default one
- Select the **Save Connection Profiles as Default** icon if you wish to save the current connection profiles as default
- Select the **Reset Connection Profiles to Default** icon if, after modifying them, you want to go back to the default connection profiles setup
- Select the **Save User Permissions as Default** icon if you wish to set the current users permissions as default
- Select the **Reset User Permissions to Default** icon if you have changed any user permission and want to revert it back to the default value

Note: The BRM must be rebooted for any configuration amendments to take effect.

10.7.1: Bypassing Antenna Pointing Mode

To configure the BRM to bypass antenna pointing mode, please take the following steps in the **Configuration** page:

1. Locate **bypass_pointing**, and type in `true` in the text box.

2. Select the **Set bypass_pointing** button.

3. Refer to **Reboot** for how to reboot the BRM, so that the configuration change can take effect.

4. If you need to set the configuration back to its original setting, repeat **Steps 1 through 3** but enter `false` for **Step 2** instead of true.

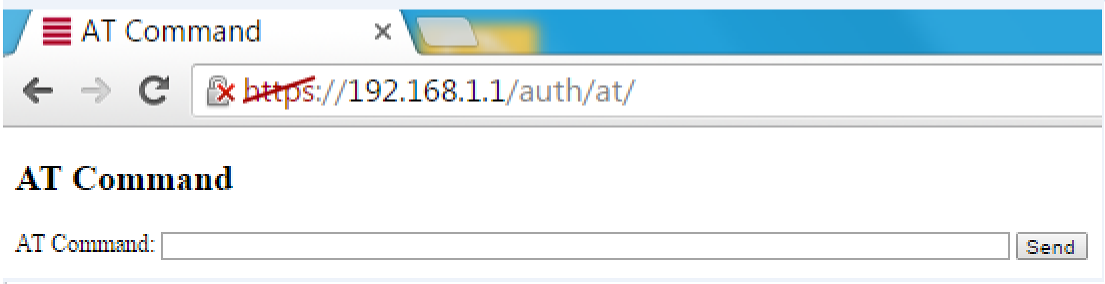
10.8: AT Command

To access this functionality, select **AT Command** from the main menu.

The **AT Command** page loads up, per *Figure 29*.

Refer to the *BGAN Radio Module AT Commands Interface Control Document* for details of what AT commands are available and the functions they serve, so that you can type in the relevant command in the AT Command free-text field and select **Send**.

Note: Concatenated AT Commands are only supported if run using a Telnet session.



AT Command

~~https~~://192.168.1.1/auth/at/

AT Command

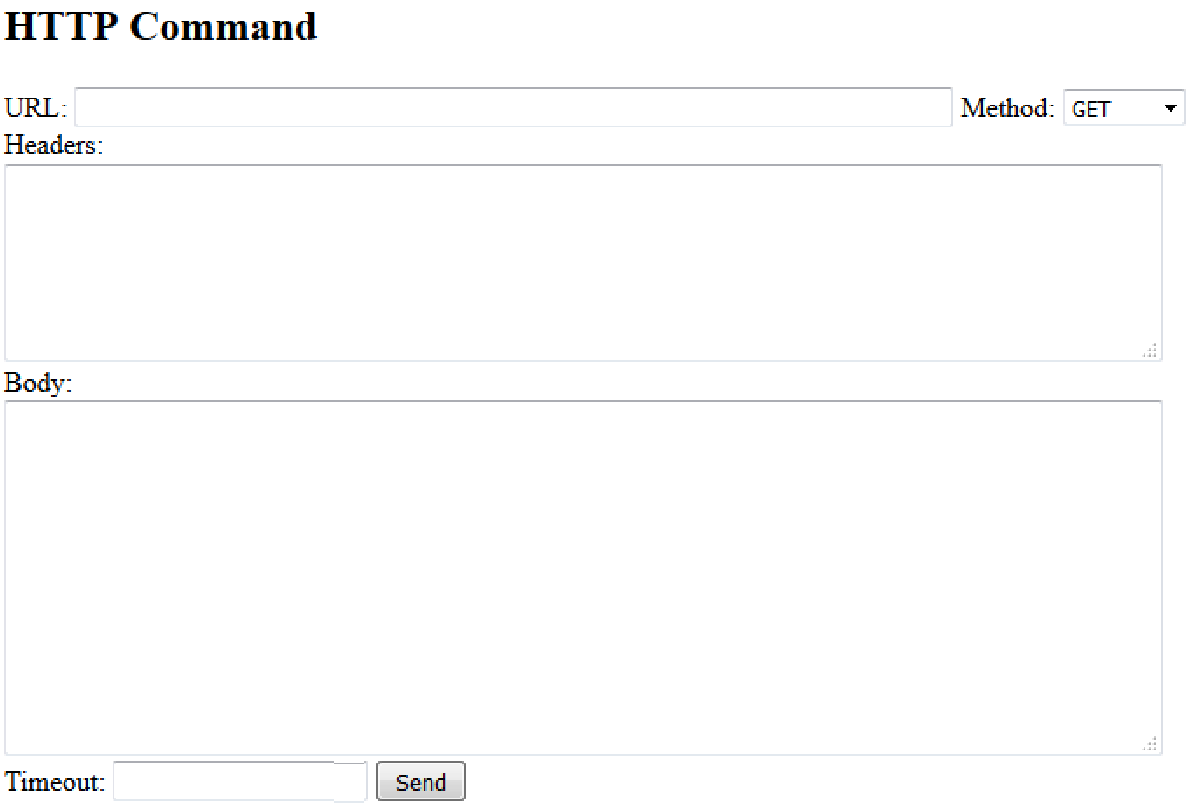
AT Command:

Figure 29. AT Command

10.9: HTTP Proxy

To access this functionality, select **HTTP Proxy** from the main menu.

The **HTTP Proxy** page loads up, per *Figure 30*.



HTTP Command

URL:

Method: GET

Headers:

Body:

Timeout:

Figure 30. HTTP Proxy

This functionality allows a VAM to send custom commands to a host processor, by issuing generic HTTP command requests using the HTTP proxy on the BRM.

The HTTP proxy provides the functionality required to issue HTTP requests to a VAMs host processor via the BRM's RESTful API and this is available using the REST /httpcommand POST method. Access to this method is authenticated using the BRM's user permissions system.

The parameters available can accommodate use cases and variations in VAM host server implementation, such as:

- A command comprising an HTTP request URL and method with no parameters, e.g., `http://192.168.1.10/command POST` (assumes host processor is at 192.168.1.10)
- A simple string command comprising a HTTP request URL and method with the string command encoded as plain text or JSON in the message Body
- Complex commands comprising:
  - An HTTPS secure socket connection request
  - URL parameters
  - Encoding and content Headers
  - Support for independent VAM host authentication (using authentication headers)
  - Message Body parameters

It is recommended that the BRM TCP proxy is disabled, so that you can instead use the /httpcommand mechanism to implement your own commands to control the host processor. This method is straightforward to use and does not involve the host processor acting as a proxy for the BRM RESTful APIs, because doing that would mean that all the BRM REST API calls would need to be passed through the host processor in addition to it processing and responding to its own commands.

Set the values for the following three parameters in the Configuration page in the WebUI as required, to ensure TCP Proxy is enabled or disabled:

- `proxy_forward_enable`
  - If set to `false`, the TCP proxy is disabled, and the BRM's RESTful API is bound to port 443 on the admin PDP interface as normal
  - If set to `true`, the TCP proxy is enabled, and the TCP proxy is bound to port 443 on the admin PDP interface. The BRM's RESTful API binding is changed to port 8443 on the admin PDP interface, but will be still available on the Ethernet port 443 which will be used by the VAM host processor
  - If set to `true`, all commands (BRM RESTful API and VAM-specific commands), would be forwarded to the VAM host processor. In both cases, the BRM's RESTful API is bound to port 443 on the Ethernet interface as normal, and the Inmarsat remote management platform connects to port 443 on the BRM's admin PDP interface

    - When the VAM host processor receives a request from the Inmarsat Remote Management Platform via the TCP proxy that is targeted at the BRM in question, the VAM host processor:
        - Connects to the BRM on port 443 on the Ethernet interface
        - Forwards the request with the HTTP authentication credentials (username and password) supplied within the original request from the Inmarsat Remote Management Platform
        - Receives the response from the BRM and sends it back using the original connection to the Inmarsat remote management platform via the TCP proxy
    - When the VAM host processor receives a request from the Inmarsat Remote Management Platform via the TCP proxy that is targeted for the VAM host processor, the VAM host processor:
        - Connects to the BRM on port 443 on the Ethernet interface
        - Checks the validity of the HTTP authentication credentials (username and password) supplied within the request from the Remote Management Platform

          Note:
          This could be achieved with the BRM's RESTful `/v1/config GET` method which responds with `401 Unauthorized` if the credentials do not match the BRM's user permissions records.
        - May check the requesting user's permission records using the BRM's RESTful `/config/permission/{userid} GET` method (using a stored VAM user authentication credential with permission to access the permission records). This will allow the VAM host processor to use the BRM's user permissions API to help control authorisation of its own command API
        - Sends its own response back using the original connection to the Inmarsat Remote Management platform via the TCP proxy

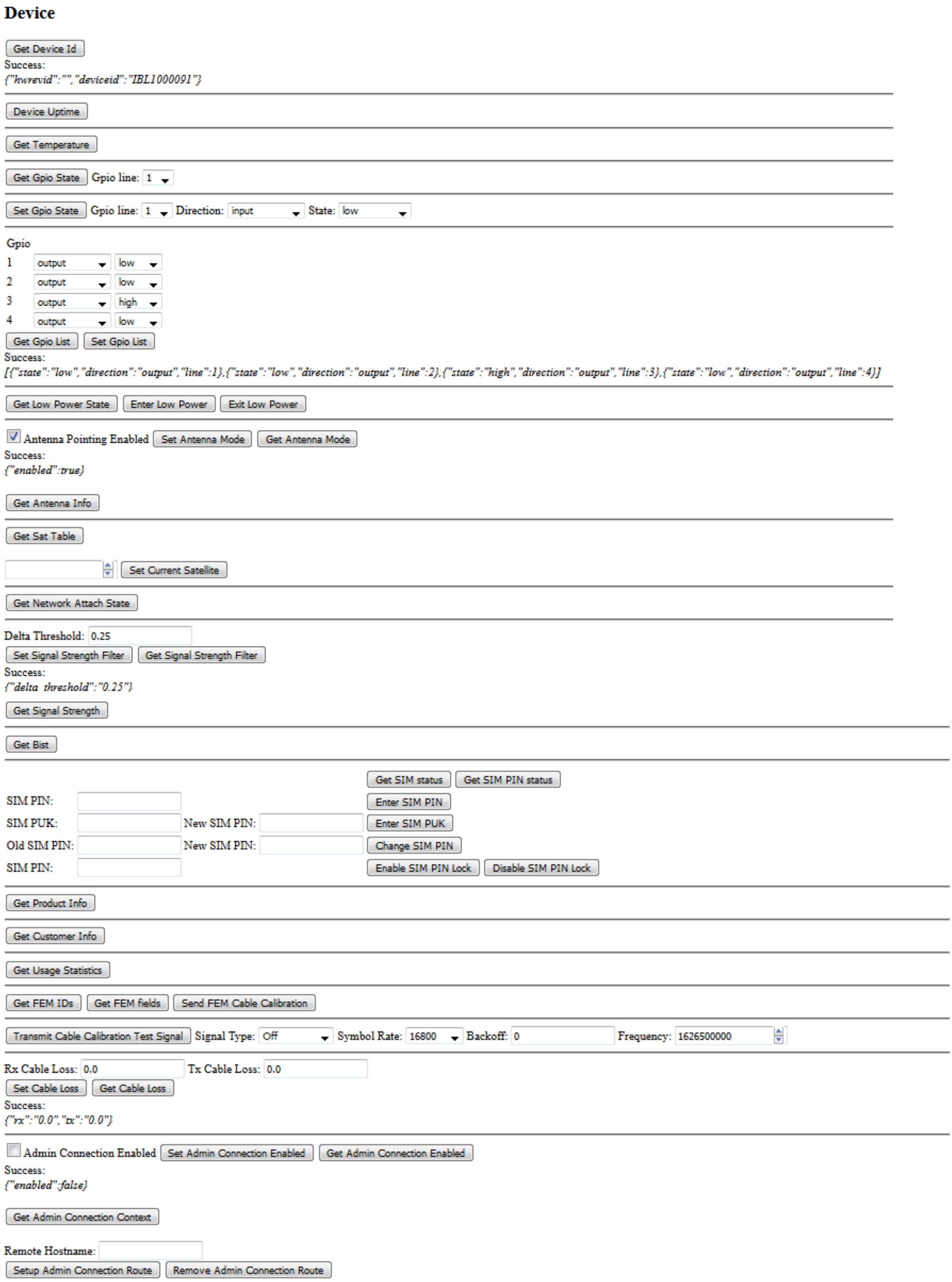
- `proxy_forward_ip` and `proxy_forward_port`
    - This is the IPv4 address and port (of the VAM host processor) on the Ethernet LAN to which the TCP proxy will forward TCP connections and data from port 443 on the admin PDP interface

10.10: Device

To access this functionality, select **Device** from the main menu.

The **Device** page loads up, per *10.10*.

This section allows you to view the status of certain aspects of the operation of the BRM, as well as control some of those aspects of operation.



Success:
{"hwrevid":"","deviceid":"IBL1000091"}

Gpio line: 1

Gpio line: 1 Direction: input State: low

Gpio

1	output	low
2	output	low
3	output	high
4	output	low

Success:
[{"state":"low","direction":"output","line":1},{"state":"low","direction":"output","line":2},{"state":"high","direction":"output","line":3},{"state":"low","direction":"output","line":4}]

☑ Antenna Pointing Enabled

Success:
{"enabled":true}

Delta Threshold: 0.25

Success:
{"delta threshold":"0.25"}

SIM PIN:

SIM PUK: New SIM PIN:

Old SIM PIN: New SIM PIN:

SIM PIN:

Signal Type: Off Symbol Rate: 16800 Backoff: 0 Frequency: 1626500000

Rx Cable Loss: 0.0 Tx Cable Loss: 0.0

Success:
{"rx":"0.0","tx":"0.0"}

☐ Admin Connection Enabled

Success:
{"enabled":false}

Remote Hostname:

Figure 31. Device

- Select the relevant **Get** icon to view the following for the BRM:
  - **Device Id**
  - **Temperature**

  - **GPIO State**
  - **GPIO List**

- Select the relevant values from the drop-down menus and select the relevant **Set** icon for the GPIO State and/or List, to amend values for **GPIO State** or **GPIO List**
- Select the **Device Uptime** icon if you wish to see for how long the BRM has been continuously operational
- Select one of the **Low Power** icons, according to whether you wish to view the low power status or enable or come out from low power mode
- Refer to **Antenna Pointing** for how the **Antenna Pointing** and **Get Sat Table** sections are used
- Select **Get Signal Strength Filter**, to see which value is set for the signal threshold at which notifications should be generated
  - If you want to set or amend the threshold value, enter the value into the **Delta Threshold** field and select **Set Signal Strength Filter**, e.g., if you enter `1`, then signal strength notifications will be generated if the signal fluctuates by 1 dB or more from the previous value
- Select **Get Signal Strength** to see what the current signal strength is for the UT
- Select **Get Bist** if you want the BRM to run a self-test (Built-In Self-Test (BIST))
- Select **Get SIM status** if you want to know the current status of the SIM card inserted in the external SIM card holder on the BRM. If the response is `Success: {"status": "SIM PIN"}`, a PIN entry will be required. **Get SIM PIN Status** will return the remaining PIN retries
  - You can also:
    - Enter the SIM PIN
    - Enter the PIN Unlock Code (PUK)
    - Change the SIM PIN
    - Enable or Disable the SIM Lock Mode
- Select **Get Product Info** to view the International Mobile Equipment Identifier (IMEI) and Integrated Circuit Card Identifier (ICCID) of the SIM
- Select **Get Customer Info** if you want to view the details of the provisioned SIM card
- Select **Get Usage Statistics** if you want to have an estimation of IP data passing through all background class contexts, including the Admin Context, on the BRM
- Select **Get FEM IDs** if you want to know the software ("swrevid") or hardware ("hwrevid") FEM identifiers

- Select **Get FEM Fields** if you want to see what configurations have been implemented on the FEM

- Select **Send FEM Cable Calibration** to obtain the antenna cable calibration values from a steered antenna back to the FEM

- Select **Transmit Cable Calibration Test Signal** to configure the BRM to set up a transmit carrier CW or modulated in order to perform the antenna cable calibration. The following parameters will determine which type of signals are generated:

  - Signal Type: `OFF | QPSK | PI/4 QPSK | QAM16 | QAM32 | QAM64 | CW`

  - Symbol Rate (ignored if CW is used): `16800, 33600, 67200, 84000, 151200, 168000`

  - Backoff: in the range `0.00` to `10.00dB`

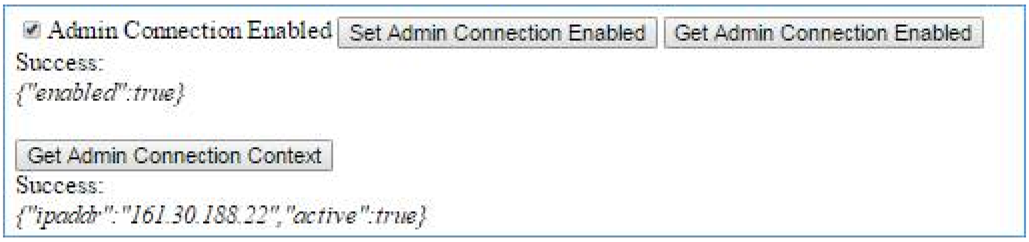
  - Frequency: in the range `1616500000` to `1660500000` and `1668000000` to `1675000000`

- Select **Get Cable Loss** to know which are the RX and TX cable losses setup or **Set Cable Loss** to modify them

  Note: FEM Cable Loss setup functionality is not fully implemented yet. These two values, "RX Cable Loss" and "TX Cable Loss" are intended to be employed in S-band systems. It might be applied for L-band systems as well, in the future.

- Refer to **BRM Remote Firmware Update Server Addressing Scheme** for how the **Set** and **Delete Admin Connection Route** functions are used

If an Admin Connection has been set up, then the Admin Connection buttons/check boxes/outputs will show per *Figure 32*.


Set Admin Connection Enabled
Get Admin Connection Enabled
Get Admin Connection Context

☑ Admin Connection Enabled

Success:

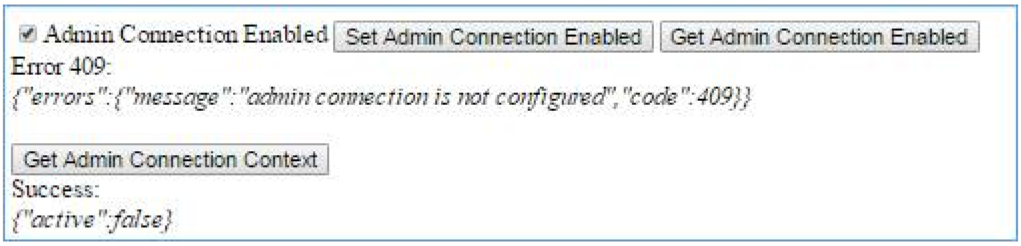
{"enabled":true}

Success:

{"ipaddr":"161.30.188.22","active":true}

Figure 32. Admin Connection Enabled

If an Admin Connection has not been set up, then the Admin Connection buttons/check box/outputs will show per *Figure 33*.


Set Admin Connection Enabled
Get Admin Connection Enabled
Get Admin Connection Context

☑ Admin Connection Enabled

Error 409:

{"errors":{"message":"admin connection is not configured","code":409}}

Success:

{"active":false}

Figure 33. Admin Connection Disabled

Note: To disable the Admin Connection from the Device page, you just need to un-check the **Admin Connection Enabled** check box.

10.10.1: Antenna Pointing Mode

Note: These instructions assume that the antenna being used requires manual pointing. If you require instructions for a steerable antenna, please refer to **BRM Support for Steered Antennas**.

By default, once the BRM is on, the BRM enters Antenna Pointing mode; it will be pointing to the satellite the user chooses until they decides the signal strength is good enough to have a reliable connection over the network.

If you open the **Notifications** page and select the `Signal Strength` option, you will find a good way to check the quality of the signal strength. `Signal Quality` and `Signal Strength` are displayed, followed by the corresponding bearer type.

Return to the **Device** page and note the following indications:

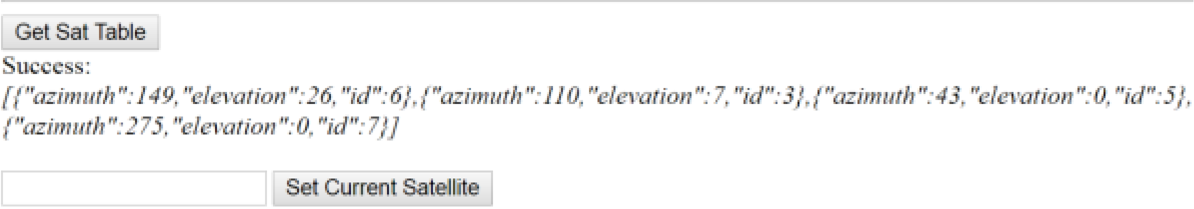
1. Verify the antenna pointing is enabled (should be enabled by default) by selecting Get_Antenna_ Mode.

- If **enabled** the response is `Success: {"enabled" :true}`
- If **not enabled** the response is `Success: {"enabled" :false}`

2. Is antenna pointing disabled?

- If **Yes**, enable it by checking the **Antenna Pointing Enabled** check box and selecting **Set Antenna Mode**
- If **No**, proceed to **Step 6**

3. Select the **Get Sat Table** button which displays a list of satellite IDs with their current azimuth and elevation, per *Figure 34*.



```
Success:
[{"azimuth":149,"elevation":26,"id":6},{"azimuth":110,"elevation":7,"id":3},{"azimuth":43,"elevation":0,"id":5},
{"azimuth":275,"elevation":0,"id":7}]
```

Figure 34. Get Sat Table

4. Note the ID of the Satellite with the highest elevation value, and enter that ID into the **Set Current Satellite** field and select the **Set Current Satellite** button.

5. Manually point the antenna until a sustained optimal signal strength and quality is achieved (Signal strength of 45dBHz or greater is usually sufficient for a data connection to be successfully established). As signal strength improves, so does signal quality. Please refer to *Signal Quality Scores - BRM Implementation and Guidelines for Value Added Manufacturers* for more details.

Note: Monitor the `signalstrength` value on the **Websocket Notifications** page until the optimal signal strength value and signal quality is consistently achieved, per *Figure 34*.

6. Fix the antenna position in place at the optimal signal strength.

7. On the **Device** page, un-check **Antenna Pointing Enabled** and select the **Set Antenna Mode** button to disable antenna-pointing mode.

Note: The signal strength should move to between 50 to 57 dBHz, indicating that the BRM has moved to a Regional Beam.

8. Set the fluctuation levels at which the signal strength will be displayed, as explained in **Device**.

9. In the other browser window, in the **Notifications** page, check `AT`.

10. Wait for 30 seconds, then navigate to the **AT Command** page, enter `AT+CGATT?`, and select **Send**.

- A response of `+CGATT=1` indicates that the BRM is attached to the Inmarsat network
- A response `+CGATT=0` indicates that the terminal is not attached. In that case, repeat Steps 1 through 13, ensuring that:
  - A USIM is inserted (and the PIN set, in case a SIM PIN entry is required)
  - A location fix is available
  - Signal strength is within 45 to 52 dBHz in Global Beam
  - **bui_mode** is set to `false` in the **Configuration** page

The BRM waits for up to 30 seconds after it is switched on for a GNSS/GPS fix to be established before exiting low power mode.

If the antenna is already pointed and fixed for the best signal strength, the user may want to bypass the antenna pointing steps mentioned above by making a configuration change. If the configuration change is not done, the user will have to follow **Steps 1** through **13** every time they power up the TDK in order to establish a data connection. Refer to **Bypassing Antenna Pointing Mode** for details of how to amend the default configuration to bypass antenna pointing mode.

Please, refer to **Establishing a Data Connection for On-Air Operations** for how to open a connection over the network and send data across it.

10.10.2: BRM Remote Firmware Update Server Addressing Scheme

The **Remote Hostname** section provides a method for setting up a route to a remote host via the admin PDP context to establish a network path for the terminal's host processor to access firmware upgrade images.

In order to use this functionality, ensure the admin connection is enabled and an IP address allocated. In order to set up the route from the host processor to the server where the firmware upgrade images are stored, specify the server hostname in the free-text box and select **Setup Admin Connection Route**.

The BRM performs a type A DSN query for the hostname and returns the resolved IP address to the processor. A response of the following type will be displayed:

```
{"local_ipaddr":"192.168.1.10","remote_ipaddr":"212.219.56.184"}
```

where `local_ipaddr` is the address of the host processor, and `remote_ipaddr` is the resolved address for the hostname specified.

At that point, a static route will have been created by the BRM between the Ethernet Interface and the admin connection, and any packet received on the BRM's Ethernet interface with source and destination matching the local and remote IP address will be sent out of the admin interface with the source address replaced with the admin interface IP address.

Select **Remove Admin Connection Route** to remove this route once the download has been completed.

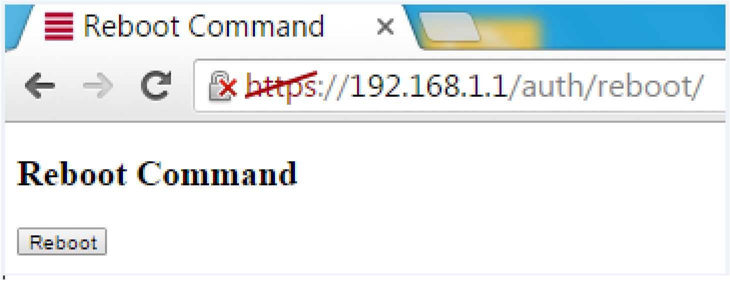
For more information about the remote firmware upgrade, please refer to *Firmware Upgrading a BRM-based Terminal Application Note*.

10.11: Reboot

To access this functionality, select **Reboot** from the main menu.

The **Reboot Command** page loads up, per *10.11*.

Select the **Reboot** icon to reboot the BRM.



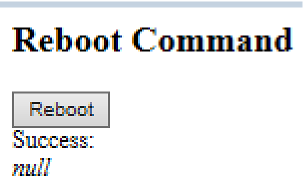
Reboot Command

~~https~~://192.168.1.1/auth/reboot/

Reboot Command

Figure 35. Reboot

A successful reboot of the BRM is indicated per *Figure 36*.



Reboot Command

Success:
null

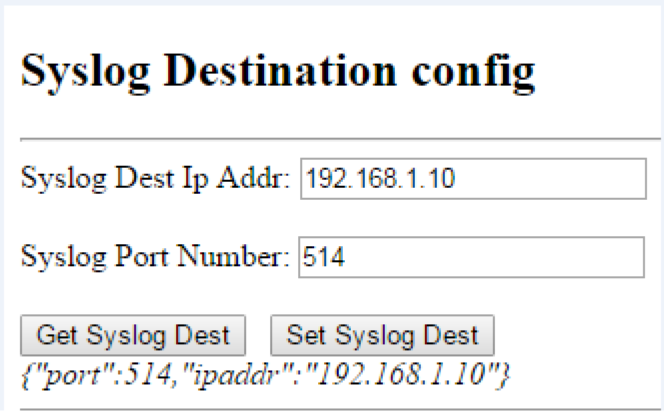
Figure 36. Successful Reboot

10.12: Syslog Destination Config

To access this functionality, select **Syslog Destination Parameters** from the main menu.

This functionality allows you to configure a remote location where syslog files collected on the BRM must be sent, for analysis and storage.

The **Syslog Destination Config** page loads up, per *Figure 37*.



Syslog Destination config

Syslog Dest Ip Addr: 192.168.1.10

Syslog Port Number: 514

```
{"port":514,"ipaddr":"192.168.1.10"}
```

Figure 37. Syslog Destination Configuration

To use this function, take the following steps:

1. Select **Get Syslog Dest** to see if a destination already exists.

2. If you need to set or change the destination, enter the relevant syslog destination IP address and port number.

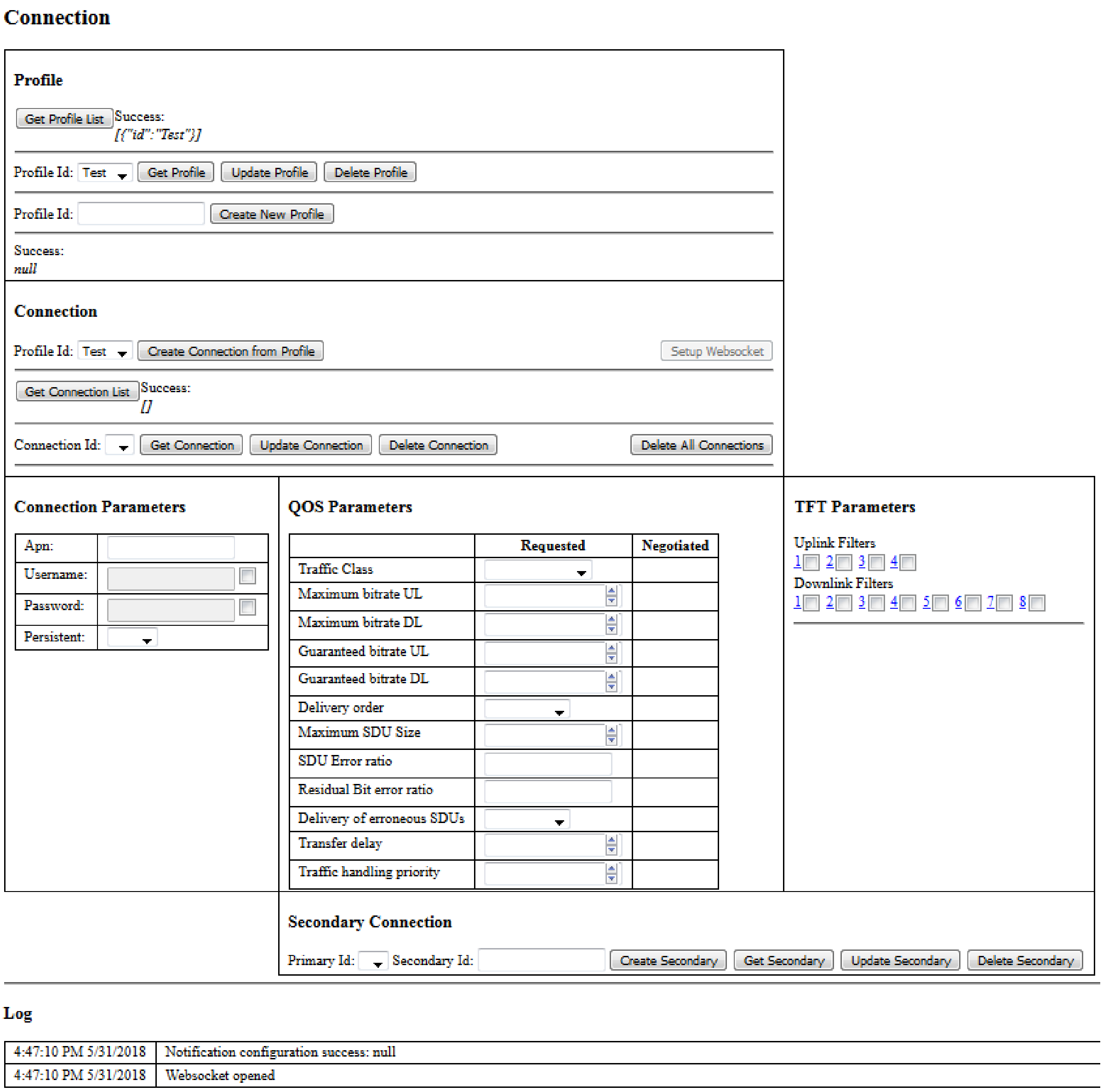
3. Select the **Set Syslog Dest** button.

4. Navigate to the **Debug Logging** page and configure syslog filters accordingly.

10.13: Connection

To access this functionality, select **Connection** from the main menu.

The **Connection** page loads up, per *10.13*.



Connection

Profile

Success:
[{"id":"Test"}]

Profile Id: Test

Profile Id:

Success:
null

Connection

Profile Id: Test

Success:
[]

Connection Id:

Connection Parameters

Apn:	
Username:	□
Password:	□
Persistent:	

QOS Parameters

	Requested	Negotiated
Traffic Class		
Maximum bitrate UL		
Maximum bitrate DL		
Guaranteed bitrate UL		
Guaranteed bitrate DL		
Delivery order		
Maximum SDU Size		
SDU Error ratio		
Residual Bit error ratio		
Delivery of erroneous SDUs		
Transfer delay		
Traffic handling priority		

TFT Parameters

Uplink Filters
1□ 2□ 3□ 4□
Downlink Filters
1□ 2□ 3□ 4□ 5□ 6□ 7□ 8□

Secondary Connection

Primary Id: Secondary Id:

Log

4:47:10 PM 5/31/2018	Notification configuration success: null
4:47:10 PM 5/31/2018	Websocket opened

Figure 38. Connection

Refer to **Establishing a Data Connection for On-Air Data Operations** for an example of how the **Profile** and **Connection** sections are used.

10.13.1: Creating a New Connection Profile

To create a new connection profile, take the following steps:

1. Enter a new name into the **Profile Id** field.

2. Select the **Create New Profile** button. A default connection profile will be created at this point.

> **Note:** A connection profile can be copied by: 1. Get an existing connection profile by selecting in the scroll-down **Profile Id** menu the connection you want to copy and select **Get Profile**. 2. Write the new name of the connection in the **Profile Id** free-text box and select **Create New Profile**. The parameters and QoS of that new profile will be the same ones as the original profile you used to copy from.

3. Ensure the entries in the **Connection Parameters** and **QoS Parameters** sections are the same as the ones you want. If that is not the case, make the changes first and then select **Update Profile** and ensure the connection profile you want to update is selected from the scroll-down menu.

4. If you want to go over the air, follow the steps in **Antenna Pointing** and **Establishing a Data Connection for On-Air Operations** to establish a data connection using the connection profile you have just created.

10.13.2: Establishing a Data Connection for On-Air Data Operations

1. Select **Connection** from the **Engineering WebUI** main menu.

   The **Connection** page loads up. The **Profile Id** field in the **Profile** section should be populated with `Test`.

2. Select the **Get Profile** button.

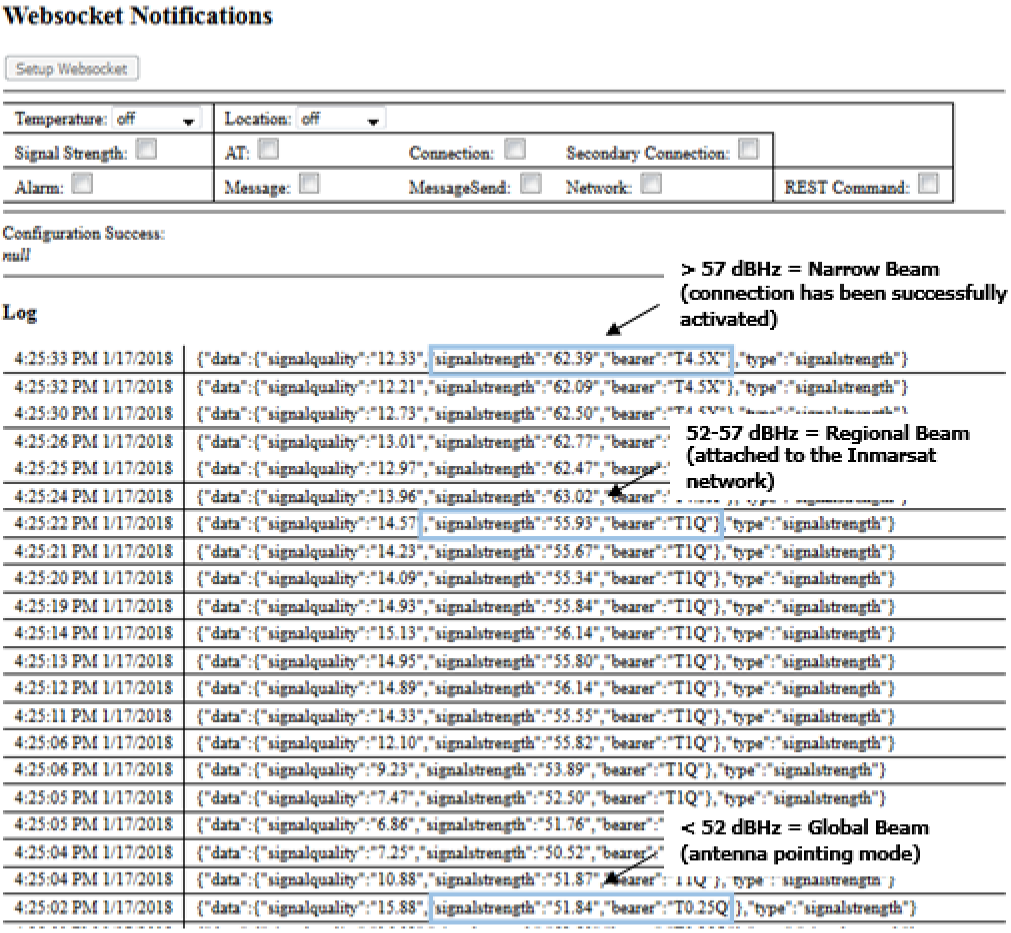
   The **Connection Parameters** and **QOS Parameters** sections of the **Connection** page are auto-populated with the pre-defined `Test` connection profile parameters.

   > **Note:** If you did not get a positive response to **Step 13** in **Establishing a Data Connection for On-Air Data Operations**, then before you carry out **Step 3**, wait for a few seconds until the BRM has established a connection with the satellite.

3. Under the **Connection** section of the **Connection** page, select the **Create Connection from Profile** button.

4. Select the **Get Connection List** button to see what the connection status is.

   The connection is fully established once the status shows per *Figure 39*.



Websocket Notifications

Temperature: off ▾ | Location: off ▾
Signal Strength: ☐ | AT: ☐ | Connection: ☐ | Secondary Connection: ☐
Alarm: ☐ | Message: ☐ | MessageSend: ☐ | Network: ☐ | REST Command: ☐

Configuration Success:
null

Log

```
4:25:33 PM 1/17/2018 | {"data":{"signalquality":"12.33","signalstrength":"62.39","bearer":"T4.5X"},"type":"signalstrength"}
4:25:32 PM 1/17/2018 | {"data":{"signalquality":"12.21","signalstrength":"62.09","bearer":"T4.5X"},"type":"signalstrength"}
4:25:30 PM 1/17/2018 | {"data":{"signalquality":"12.73","signalstrength":"62.50","bearer":
4:25:26 PM 1/17/2018 | {"data":{"signalquality":"13.01","signalstrength":"62.77","bearer":
4:25:25 PM 1/17/2018 | {"data":{"signalquality":"12.97","signalstrength":"62.47","bearer":
4:25:24 PM 1/17/2018 | {"data":{"signalquality":"13.96","signalstrength":"63.02","bearer":
4:25:22 PM 1/17/2018 | {"data":{"signalquality":"14.57","signalstrength":"55.93","bearer":"T1Q"},"type":"signalstrength"}
4:25:21 PM 1/17/2018 | {"data":{"signalquality":"14.23","signalstrength":"55.67","bearer":"T1Q"},"type":"signalstrength"}
4:25:20 PM 1/17/2018 | {"data":{"signalquality":"14.09","signalstrength":"55.34","bearer":"T1Q"},"type":"signalstrength"}
4:25:19 PM 1/17/2018 | {"data":{"signalquality":"14.93","signalstrength":"55.84","bearer":"T1Q"},"type":"signalstrength"}
4:25:14 PM 1/17/2018 | {"data":{"signalquality":"15.13","signalstrength":"56.14","bearer":"T1Q"},"type":"signalstrength"}
4:25:13 PM 1/17/2018 | {"data":{"signalquality":"14.95","signalstrength":"55.80","bearer":"T1Q"},"type":"signalstrength"}
4:25:12 PM 1/17/2018 | {"data":{"signalquality":"14.89","signalstrength":"56.14","bearer":"T1Q"},"type":"signalstrength"}
4:25:11 PM 1/17/2018 | {"data":{"signalquality":"14.33","signalstrength":"55.55","bearer":"T1Q"},"type":"signalstrength"}
4:25:06 PM 1/17/2018 | {"data":{"signalquality":"12.10","signalstrength":"55.82","bearer":"T1Q"},"type":"signalstrength"}
4:25:06 PM 1/17/2018 | {"data":{"signalquality":"9.23","signalstrength":"53.89","bearer":"T1Q"},"type":"signalstrength"}
4:25:05 PM 1/17/2018 | {"data":{"signalquality":"7.47","signalstrength":"52.50","bearer":"T1Q"},"type":"signalstrength"}
4:25:05 PM 1/17/2018 | {"data":{"signalquality":"6.86","signalstrength":"51.76","bearer":"
4:25:04 PM 1/17/2018 | {"data":{"signalquality":"7.25","signalstrength":"50.52","bearer":"
4:25:04 PM 1/17/2018 | {"data":{"signalquality":"10.88","signalstrength":"51.87","bearer":
4:25:02 PM 1/17/2018 | {"data":{"signalquality":"15.88","signalstrength":"51.84","bearer":"T0.25Q"},"type":"signalstrength"}
```

> 57 dBHz = Narrow Beam (connection has been successfully activated)

52-57 dBHz = Regional Beam (attached to the Inmarsat network)

< 52 dBHz = Global Beam (antenna pointing mode)

Figure 39. Successful Data Connection

Once the connection is activated, the negotiated QoS parameters will be displayed in the “QoS Parameters" table. In case they are different from the requested ones, the table will be updated with the negotiated values.

To find out how to modify the on-air connection parameters, refer to **Creating a New Connection Profile**.

5. On the **Notifications** page the signal quality should now move to being between 56 to 67 dBHz, indicating the transition to Narrow spot beam for data transmission, per *Figure 39*.

6. On the **Connection** page, select the **Get Connection List** button to see what the connection status is.

7. If the connection is not active, then select **Delete Connection**.

8. Repeat **Steps3** through **6**.

Once the connection is active the computer connected to the BRM can be used for transferring data through the public internet, e.g., web browsing; pings; FTP data transfer, etc.

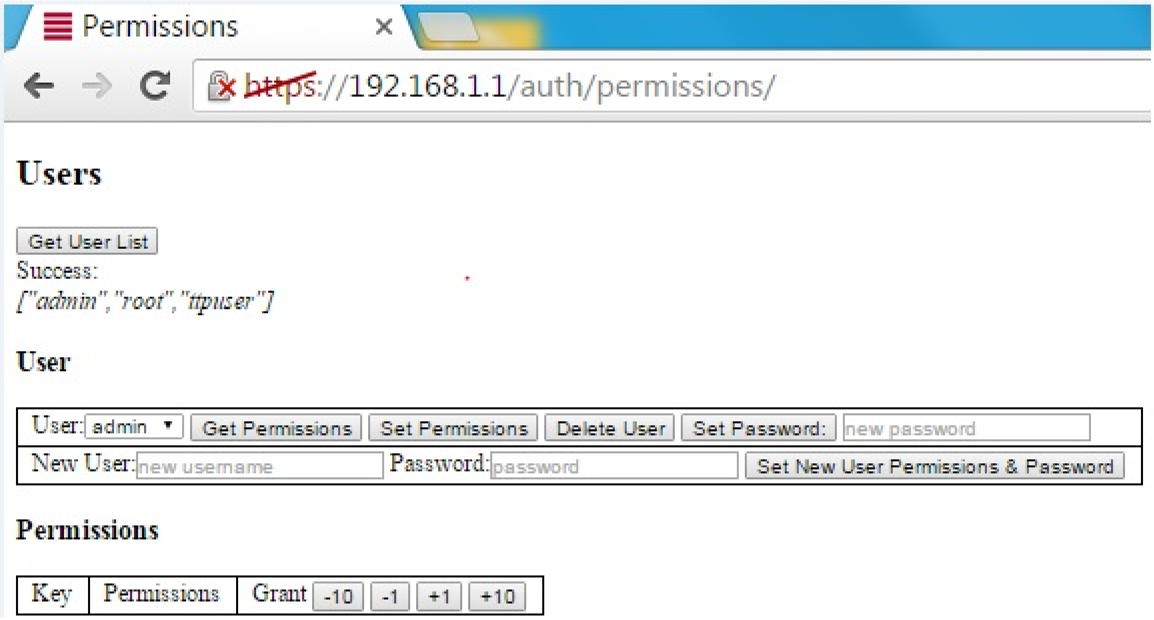
When using the WebUI or Telnet to make connections, the data connection is always NAT'ed inside the BRM because in-bound NAT is not supported, and as such supported applications which need to open a connection with your computer would fail. This means that while using FTP, only passive mode will work.

If you are using the User WebUI, please follow the instructions in **Connections** to establish a successful data connection.

10.14: Users

To access this functionality, select **Permissions** from the main menu.

The **Users** page loads up, per *10.14*.



Users

Success:
["admin","root","ttpuser"]

User

Permissions

Figure 40. Users

This section allows you to:

- View a list of user accounts authorised to access the BRM
- View or set permissions for a user account
- Create or Delete a user account
- Reset a password for an existing user account
- Set or amend Permissions and Grant levels for a user in regard to specific operations on the BRM

Notes:
Refer to the following sections of the *BGAN Radio Module Technical Specification* for more details on user permissions:

User Permissions

Permissions Table

Permissions Value for RESTful Commands and Websocket Notifications

Permissions Value for Configuration Keys

Permissions Grant Level

10.14.1: Get User List

Select the **Get User List** icon if you wish to view a list of user accounts that are authorised to access one or more functionalities, to greater or lesser extents, on the BRM.

Per *10.14*, the output is an indication of whether the request has been successful, and if so a list of authorised users is displayed.

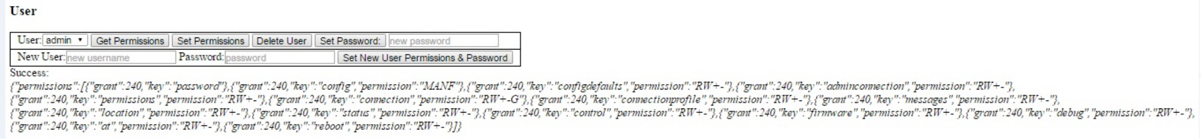
10.14.2: User

The **User** field is a drop-down menu showing a list of all user accounts authorised to access the BRM in question.

To administer one of the user accounts, select one from the drop-down list.

10.14.2.1: Get Permissions

To view the permissions already set for a user account, select the **Get Permissions** icon. The output shows per the example in *Figure 41*.



```
Success:
{"permissions":[{"grant":240,"key":"password"},{"grant":240,"key":"config","permission":"MANF"},{"grant":240,"key":"configdefaults","permission":"RW+-"},{"grant":240,"key":"adminconnection","permission":"RW+-"},
{"grant":240,"key":"permissions","permission":"RW+-"},{"grant":240,"key":"connection","permission":"RW+-G"},{"grant":240,"key":"connectionprofile","permission":"RW+-"},{"grant":240,"key":"messages","permission":"RW+-"},
{"grant":240,"key":"location","permission":"RW+-"},{"grant":240,"key":"status","permission":"RW+-"},{"grant":240,"key":"control","permission":"RW+-"},{"grant":240,"key":"firmware","permission":"RW+-"},{"grant":240,"key":"debug","permission":"RW+-"},
{"grant":240,"key":"at","permission":"RW+-"},{"grant":240,"key":"reboot","permission":"RW+-"}]}
```

Figure 41. Permissions

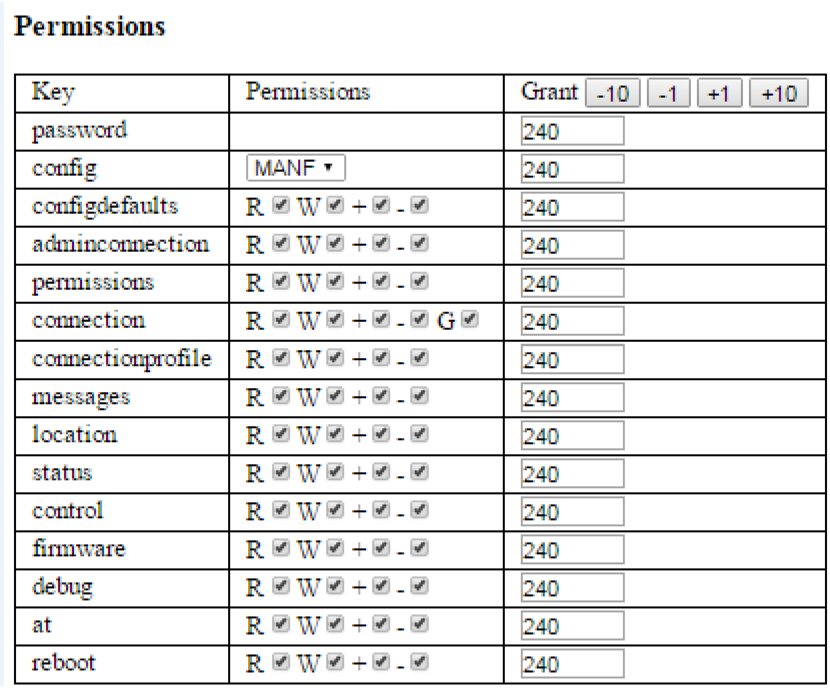
The output can be interpreted as follows:

- `"grant":<nnn>` - relates to the level of permission granted for the user account for a particular BRM function, with `240` being the highest level of permission granting the highest level of access to functionality
- `R` - Read-only permission
- `W` - Write permission
- `+` - allows the user to increase the Grant level for a user account for BRM functionalities
- `–` - allows the user to decrease the Grant level for a user account for BRM functionalities
- `G` - allows the user to deactivate a connection made by all other users. This is a special permission only used for the connection resource
- `"key"` - refers to the specific BRM functionality, .e.g., Location

10.14.2.2: Set Permissions

To set permissions for a new user account, or amend permissions for an existing one, amend the Permissions grid accordingly, an example of which is shown in *Figure 42*, then once ready select the **Set Permissions** icon.

Note: You will only be able to set or amend the Grant level for a BRM function for a user account to a level which is lower than the current grant level to which your own user account is set for that particular BRM function. You will also only be able to amend permissions if you have been granted `Write` access to the **permissions** functionality on the BRM, and only be able to amend the Grant level up or down if you have been granted `+` and `–` access to that function.



Permissions

Key	Permissions	Grant -10 -1 +1 +10
password		240
config	MANF ▾	240
configdefaults	R ☑ W ☑ + ☑ - ☑	240
adminconnection	R ☑ W ☑ + ☑ - ☑	240
permissions	R ☑ W ☑ + ☑ - ☑	240
connection	R ☑ W ☑ + ☑ - ☑ G ☑	240
connectionprofile	R ☑ W ☑ + ☑ - ☑	240
messages	R ☑ W ☑ + ☑ - ☑	240
location	R ☑ W ☑ + ☑ - ☑	240
status	R ☑ W ☑ + ☑ - ☑	240
control	R ☑ W ☑ + ☑ - ☑	240
firmware	R ☑ W ☑ + ☑ - ☑	240
debug	R ☑ W ☑ + ☑ - ☑	240
at	R ☑ W ☑ + ☑ - ☑	240
reboot	R ☑ W ☑ + ☑ - ☑	240

Figure 42. Set Permissions

10.14.3: Delete User

To delete a user account from access to the BRM in question, select the relevant user from the **User** field drop-down menu, and select the **Delete User** icon.

10.14.4: Set Password

To set a new password for a user account:

1. Select the relevant user from the **User** field drop-down menu.

2. Type the new password into the free-text field located to the right-hand side of the **Set Password:** icon.

3. Select the **Set Password:** icon.

10.14.5: New User

To create a new User Account for access to the BRM in question:

1. Type in a unique user name into the **New User** field.

2. Type a unique password into the **Password** field.

3. Follow the instructions in **Set Permissions**, except that you must select the **Set New User Permissions and Password** icon to complete the creation of the new user account.

10.14.6: Unauthenticated User

To create an unauthenticated (guest) User Account for access to the BRM in question:

Note: Ensure you are logged into the WebUI as an **authenticated** user.

1. Select **Get Permissions** for the `admin` user.

2. Set the required permissions for a guest user, for example:

- Select NONE in the **config** drop-down menu (any level of config access, i.e., MANF; RSVD; BASE; NONE, could be provided to an unauthenticated user. Use with caution)

- Un-check all permissions except R (Recommend that if write permissions are provided to an unauthenticated user, use with caution)

- Reduce **Grant** level to be less than that set for the admin user, e.g., <240

- Enter unauthenticated as the **New User**

  Note: The username must be unauthenticated.

- Enter a valid password

  Note: The password will not be required for the unauthenticated user access.

3. Select **Set New Permissions and Password** to create a guest user

4. Log out of the WebUI, then access it again using **https://192.168.1.1** in the browser address bar.

Note: When switching from a guest user to authenticated user, close and re-open the web browser.

10.15: Enable_BUI

Selecting this link allows you to enable BUI mode without having to reboot the BRM, in cases where **bui_mode** is set to false.

Per *Figure 43*, select **Enable BUI** to enable BUI mode.

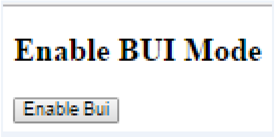

Enable BUI Mode

Figure 43. Enable_BUI

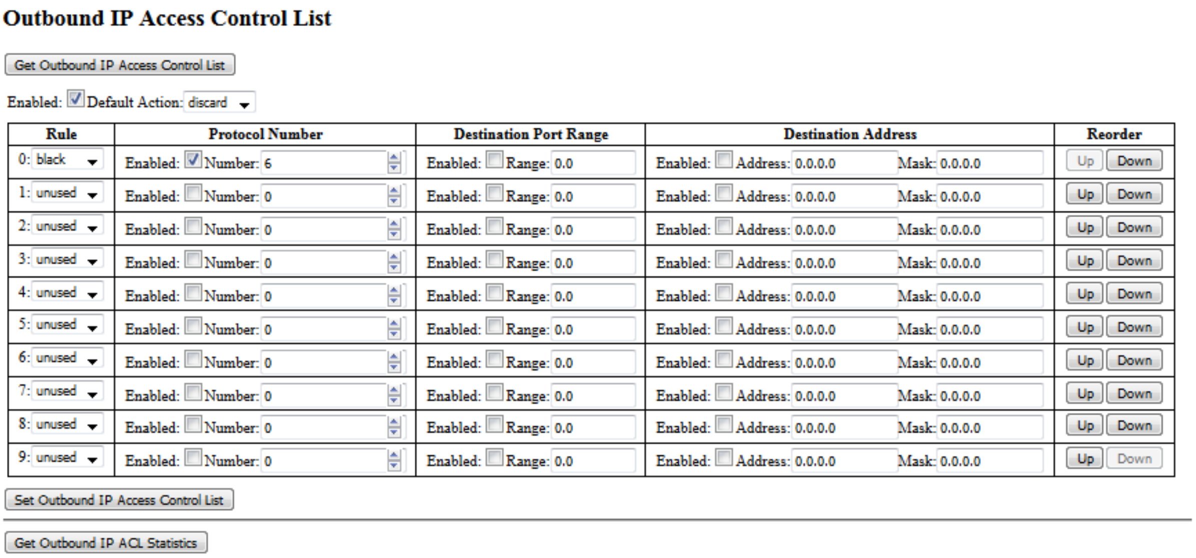
A subsequent reboot of the BRM would reset **bui_mode** back to false.

10.16: IP Access Control List

To access this functionality, select **IP Access Control List** from the main menu.

The **IP Access Control List** page loads up, per *Figure 44*.

This page contains all the resources to run the BRM firewall functionality. It is based in up to 10 different rules which may depend on protocol number, destination port range and/or destination address.



Outbound IP Access Control List

Get Outbound IP Access Control List

Enabled: ☑ Default Action: discard

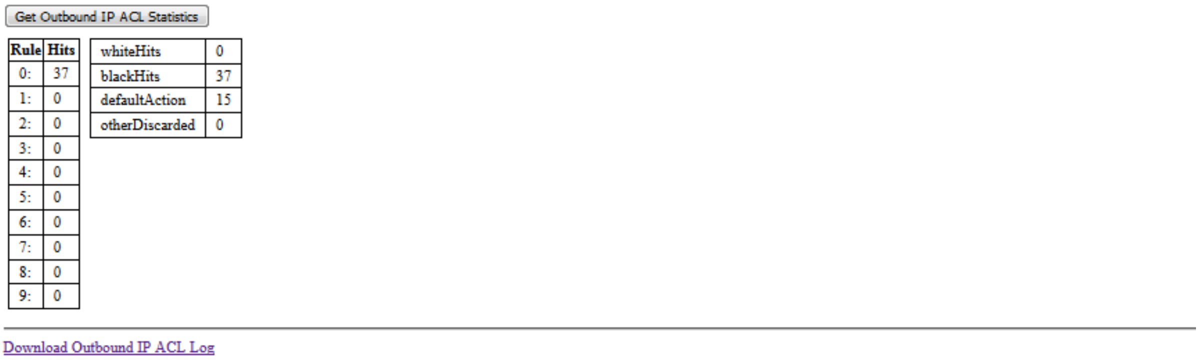
Rule	Protocol Number	Destination Port Range	Destination Address		Reorder
0: black	Enabled: ☑ Number: 6	Enabled: □ Range: 0.0	Enabled: □ Address: 0.0.0.0	Mask: 0.0.0.0	Up Down
1: unused	Enabled: □ Number: 0	Enabled: □ Range: 0.0	Enabled: □ Address: 0.0.0.0	Mask: 0.0.0.0	Up Down
2: unused	Enabled: □ Number: 0	Enabled: □ Range: 0.0	Enabled: □ Address: 0.0.0.0	Mask: 0.0.0.0	Up Down
3: unused	Enabled: □ Number: 0	Enabled: □ Range: 0.0	Enabled: □ Address: 0.0.0.0	Mask: 0.0.0.0	Up Down
4: unused	Enabled: □ Number: 0	Enabled: □ Range: 0.0	Enabled: □ Address: 0.0.0.0	Mask: 0.0.0.0	Up Down
5: unused	Enabled: □ Number: 0	Enabled: □ Range: 0.0	Enabled: □ Address: 0.0.0.0	Mask: 0.0.0.0	Up Down
6: unused	Enabled: □ Number: 0	Enabled: □ Range: 0.0	Enabled: □ Address: 0.0.0.0	Mask: 0.0.0.0	Up Down
7: unused	Enabled: □ Number: 0	Enabled: □ Range: 0.0	Enabled: □ Address: 0.0.0.0	Mask: 0.0.0.0	Up Down
8: unused	Enabled: □ Number: 0	Enabled: □ Range: 0.0	Enabled: □ Address: 0.0.0.0	Mask: 0.0.0.0	Up Down
9: unused	Enabled: □ Number: 0	Enabled: □ Range: 0.0	Enabled: □ Address: 0.0.0.0	Mask: 0.0.0.0	Up Down

Set Outbound IP Access Control List

Get Outbound IP ACL Statistics

Figure 44. IP Access Control List

- Select **Get Outbound IP Access Control List** to view the current ACLs setup
- Select **Set Outbound IP Access Control List** to apply any changes to the ACLs
- Select **Get Outbound IP ACL Statistics** to get an overview of the firewall activity, per *Figure 45*.



Get Outbound IP ACL Statistics

Rule	Hits
0:	37
1:	0
2:	0
3:	0
4:	0
5:	0
6:	0
7:	0
8:	0
9:	0

whiteHits	0
blackHits	37
defaultAction	15
otherDiscarded	0

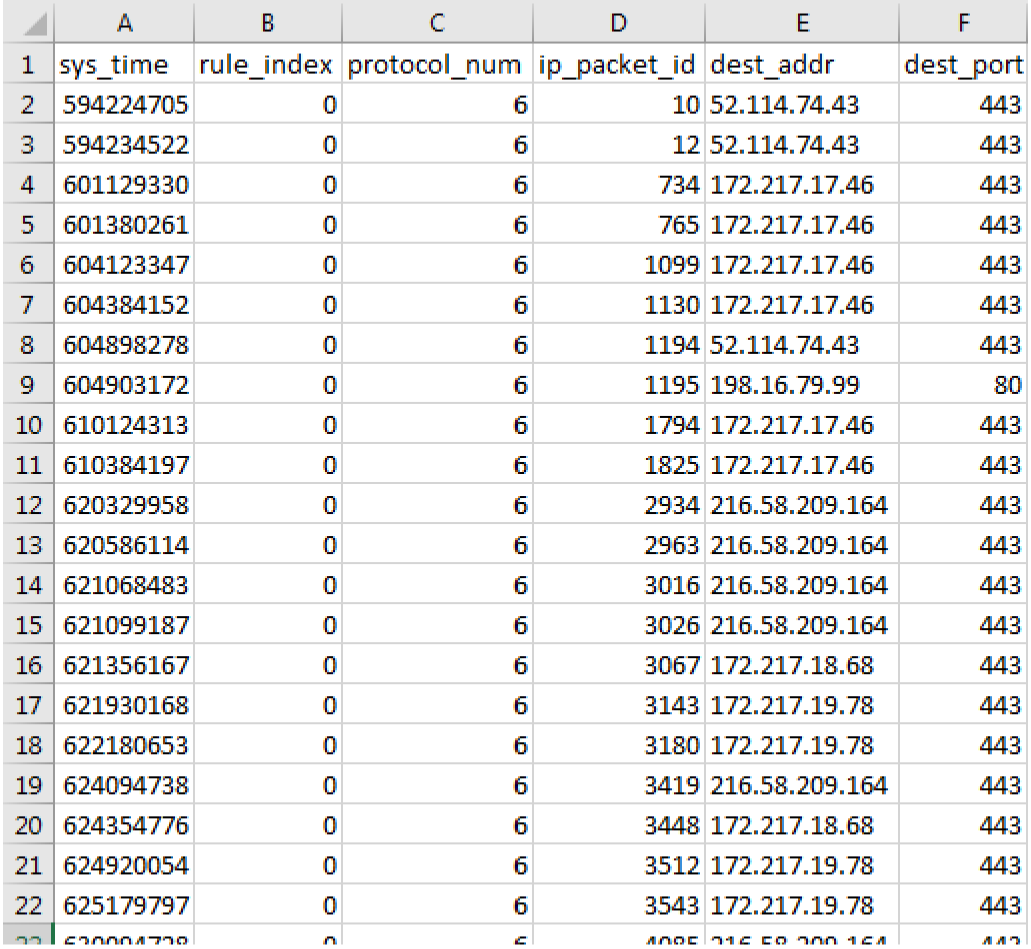
Download Outbound IP ACL Log

Figure 45. Get Outbound IP ACL Statistics

By default, the **Outbound IP Access Control List** functionality is disabled. Check the `Enabled` check box at the beginning of the page to apply the firewall to the outgoing packets.

> **Note:** The `defaultAction` only applies when there is a combination of blacklist and whitelist rules.

All packets affected by the firewall will be captured in a log accessible by the user. Select **Download Outbound IP ACL Log** to get that log. It will be downloaded as a .csv file, per *Figure 46*.



	A	B	C	D	E	F
1	sys_time	rule_index	protocol_num	ip_packet_id	dest_addr	dest_port
2	594224705	0	6	10	52.114.74.43	443
3	594234522	0	6	12	52.114.74.43	443
4	601129330	0	6	734	172.217.17.46	443
5	601380261	0	6	765	172.217.17.46	443
6	604123347	0	6	1099	172.217.17.46	443
7	604384152	0	6	1130	172.217.17.46	443
8	604898278	0	6	1194	52.114.74.43	443
9	604903172	0	6	1195	198.16.79.99	80
10	610124313	0	6	1794	172.217.17.46	443
11	610384197	0	6	1825	172.217.17.46	443
12	620329958	0	6	2934	216.58.209.164	443
13	620586114	0	6	2963	216.58.209.164	443
14	621068483	0	6	3016	216.58.209.164	443
15	621099187	0	6	3026	216.58.209.164	443
16	621356167	0	6	3067	172.217.18.68	443
17	621930168	0	6	3143	172.217.19.78	443
18	622180653	0	6	3180	172.217.19.78	443
19	624094738	0	6	3419	216.58.209.164	443
20	624354776	0	6	3448	172.217.18.68	443
21	624920054	0	6	3512	172.217.19.78	443
22	625179797	0	6	3543	172.217.19.78	443
23	630004728	0	6	4085	216.58.209.164	443

Figure 46. Example Outbound IP ACL Log

All the information is displayed in chronological order. The corresponding index rule, protocol number, IP packet ID, destination address and destination port are specified.

Notes:
Any change in the Access Control List is applied straight away after selecting **Set Outbound IP Access Control List**. A reboot is not required.

For more information about Firewall functionality and Access Control Lists, please refer to *BRM Outbound Packet Filtering – Access Control List.*

10.17: Logout

To log out from the BRM WebUI, select the **Logout** button from the main menu.

You are logged out of the BRM WebUI.

11: Regulatory Information

11.1: European Regulatory Information

As defined in Article 2 "Scope" of directive 2014/53/EU, this Terminal Development Kit is a custom built evaluation kit, configured as ordered, intended for use by professionals, to be used solely at research and development facilities for the purposes of evaluation of the BGAN Radio Module (BRM) and therefore is excluded from the directive.

For information this Terminal Development Kit has been assessed to be compliant with the following standards and/or other normative documents:

- For article 3.1(a), Health and Safety:
  - IEC 60950-1:2005 (Second Edition) + Am 1:2009 + Am 2:2013
  - EN 60950-1:2006 + A11:2009 + A1:2010 + A12:2011 + A2:2013
  - EN 62311:2008
- For article 3.1(b), Electromagnetic Compatibility:
  - EN 301 489-20 V1.2.1:2002
  - EN 301 489-1 V2.1.0
  - EN 60945:2002 + AC1:2008 (Clauses 9 and 10 only)

The Terminal Development Kit has been assessed for compliance with EN 301 444 V2.1.0 (2016-02). In its present form the Terminal Development Kit does not comply with requirement clause 4.2.2, "unwanted emissions outside the band" with the emissions at the second harmonic of the transmitter, radiating from the unenclosed, unshielded TDK exceeding the mask.

The technical documentation relevant to the above equipment will be held at: **Inmarsat Global Limited, of 99 City Road, London, EC1Y 1AX, United Kingdom**.

System integrators designing BRM based terminal equipment will need to take necessary steps within their design to reduce second harmonic emissions, for example by using a shielded enclosure.

11.2: FCC Regulatory Information

As defined in section FCC Part 47 section 2.803 "Marketing of radio frequency devices prior to equipment authorization" the Terminal Development Kit is not FCC approved.

FCC NOTICE: This kit is designed to allow:

1. Product developers to evaluate electronic components, circuitry, or software associated with the kit to determine whether to incorporate such items in a finished product and

2. Software developers to write software applications for use with the end product. This kit is not a finished product and when assembled may not be resold or otherwise marketed unless all required FCC equipment authorizations are first obtained. Operation is subject to the condition that this product not cause harmful interference to licensed radio stations and that this product accept harmful interference. Unless the assembled kit is designed to operate under part 15, part 18 or part 95 of this chapter, the operator of the kit must operate under the authority of an FCC license holder or must secure an experimental authorization under part 5 of this chapter.

For information this Terminal Development Kit has been assessed to be compliant with the following standards and/or other normative documents:

- FCC Rules CFR 47, 1st October 2015,
  - Part 15.107 and 15.109 Class B
- FCC CFR 47 Part 25*
  - 25.202(d) – Frequency Stability
  - 25.202(f) – Spurious Emissions at Antenna Terminal
  - 25.204 – RF Output Power
  - 25.216 (h,I,j) - Field Strength of Spurious Emissions for protection of aeronautical radio navigation-satellite service

The Terminal Development Kit has been assessed for compliance with FCC CFR 47 Part 25 – Field Strength of Spurious Radiation. In its present form the Terminal Development Kit does not comply with the requirement with the emissions at the second harmonic of the transmitter, radiating from the unenclosed, unshielded TDK exceeding the mask.

System integrators designing BRM based terminal equipment will need to take necessary steps within their design to reduce second harmonic emissions, for example by using a shielded enclosure.

11.3: Industry Canada Regulatory Information

As defined in Section 2 of RSP-100 this Terminal Development Kit is imported for demonstration or trial purposes only and therefore does not require certification. However, the TDK may require a developmental radio licence. Further information may be obtained from Innovation, Science and Economic Development Canada's (ISED) regional office nearest to the demonstration or trial site.

For information this Terminal Development Kit has been assessed to be compliant with the following standards and/or other normative documents:

- ISED/IC RSS-170 Issue 3 July 2015*
  - 5.4.4 – Carrier-off state emissions
  - Occupied Bandwidth

- 5.2 – Frequency Stability
- 5.4.3.1 – Transmitter unwanted emissions
- 5.3.2 – RF output power
- 5.4.3.2.1 - Field Strength of Spurious Emissions for protection of aeronautical radio navigation-satellite service

The Terminal Development Kit has been assessed for compliance with ISED/IC RSS-170 Issue 3 July 2015 section 5.4.3.1 – Transmitter unwanted emissions. In its present form the Terminal Development Kit does not comply with the requirement with the emissions at the second harmonic of the transmitter, radiating from the unenclosed, unshielded TDK exceeding the mask.

System integrators designing BRM based terminal equipment will need to take necessary steps within their design to reduce second harmonic emissions, for example by using a shielded enclosure.

Radiation Exposure Statement

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This antenna used for this transmitter must be installed to provide a separation distance of at least 1 metre from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

L'exposition aux Radiations

Cet appareil est conforme aux limites d'exposition aux rayonnements définies pour un environnement non contrôlé. Cette antenne utilisée pour ce transmetteur doit être installé pour fournir une distance de séparation d'au moins 100cm de toutes les personnes et ne doit pas être co-localisées ou opérant en conjonction avec une autre antenne ou émetteur.

11.4: Safety - North America

The Terminal Development Kit has been assessed for compliance with and is certified to the following standards:

- UL 60950-1/CSA C22.2 No. 60950-1, Second Edition: Safety of Information Technology Equipment, Rev. October 14,2014
- MET Listing Number: E114361
- MET Report Number: 92893
- Original Certification: January 18, 2017

Appendix A: BRM Support for Steered Antennas

A.1: Steered Antenna Control

In conjunction with the BRM's RESTful and web-socket interface the BRM can support a wide range of automatic steered antenna types.

The process for the antenna to seek the satellite is initiated by the BRM whenever the BRM enters (or re-enters) pointing mode. The BRM provides to the FEM/antenna via the I2C interface aids to aid antenna alignment including:

- Current satellite azimuth and elevation
- Current receive frequency
- Current received signal strength (C/No) and bearer type
- GNSS derived heading
- GNSS derived speed

Methods the FEM/antenna may use for determining how well aligned the antenna is to the satellite include:

- Dead reckoning
- Using a receiver incorporated in the FEM/antenna tuned to the current BRM receive frequency to measure signal strength
- Using the BRM's receiver to provide received signal strength and bearer type

The FEM/antenna is responsible for deciding if the antenna has successfully 'seeked' the satellite and can start to track the satellite maintaining antenna alignment as the antenna moves. The decision to move from seeking to tracking is typically through receiving a predefined signal strength threshold and/or detection of a peak in received signal strength.

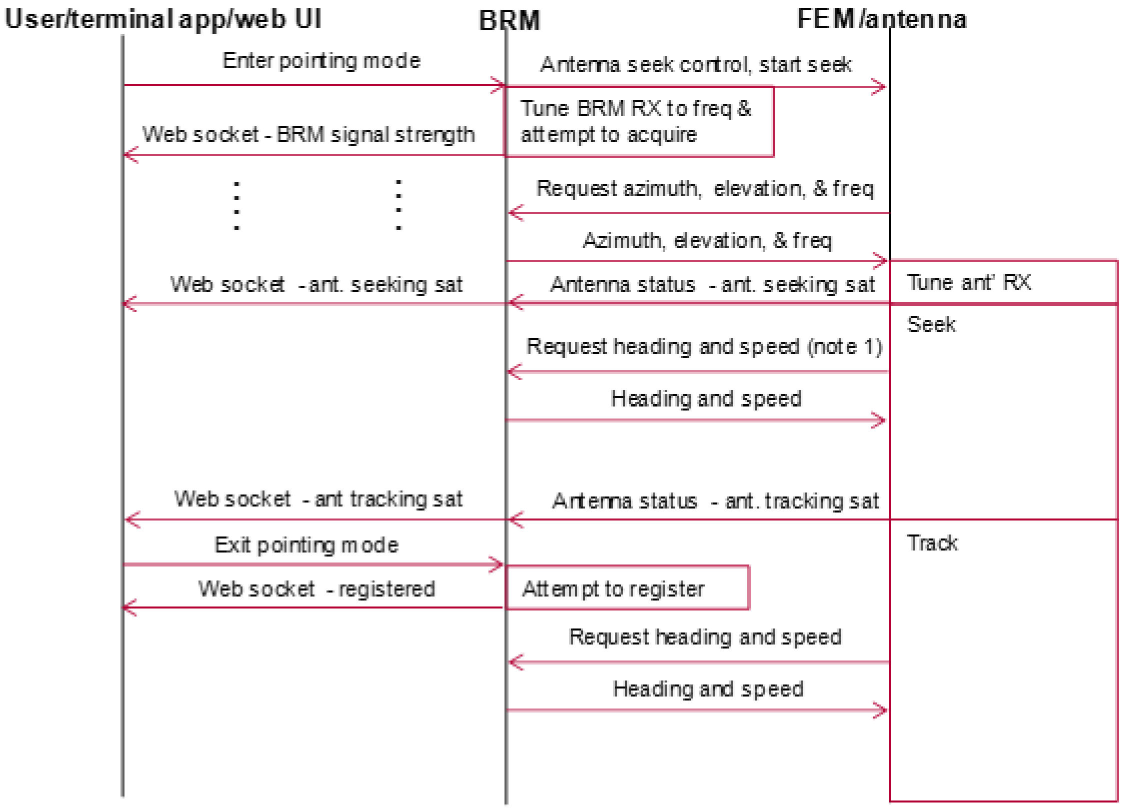
The FEM/antenna is responsible for providing antenna status messages to the BRM which are then passed onto the user of the antenna status via a web-socket.

The user, or possibly automation built into the terminal application or web UI, knowing both the BRM received signal strength and antenna status is responsible for making the decision on when the terminal exits pointing mode and starts the registration process.

A.1.1: Example With Receiver Incorporated into the Antenna

A message sequence chart for a steered antenna using a custom receiver built into the antenna to determine received signal strength is shown in *Figure 47*.

Note: Heading and speed may be continually requested at intervals of up to once per second.



User/terminal app/web UI
BRM
FEM/antenna
Enter pointing mode
Antenna seek control, start seek
Tune BRM RX to freq & attempt to acquire
Web socket - BRM signal strength
Request azimuth, elevation, & freq
Azimuth, elevation, & freq
Web socket - ant. seeking sat
Antenna status - ant. seeking sat
Tune ant' RX
Seek
Request heading and speed (note 1)
Heading and speed
Web socket - ant tracking sat
Antenna status - ant. tracking sat
Track
Exit pointing mode
Web socket - registered
Attempt to register
Request heading and speed
Heading and speed

Figure 47. Message Sequence Chart for Antenna with Custom Receiver

A.1.2: Example With Antenna Using the BRM Receiver

A message sequence chart for a steered antenna using the BRM's receiver to determine received signal strength is shown in *Figure 48*.

Notes:
Heading and speed may be continually requested at intervals of up to once per second.

Signal strength may be continually requested at intervals of up to once per 80ms.

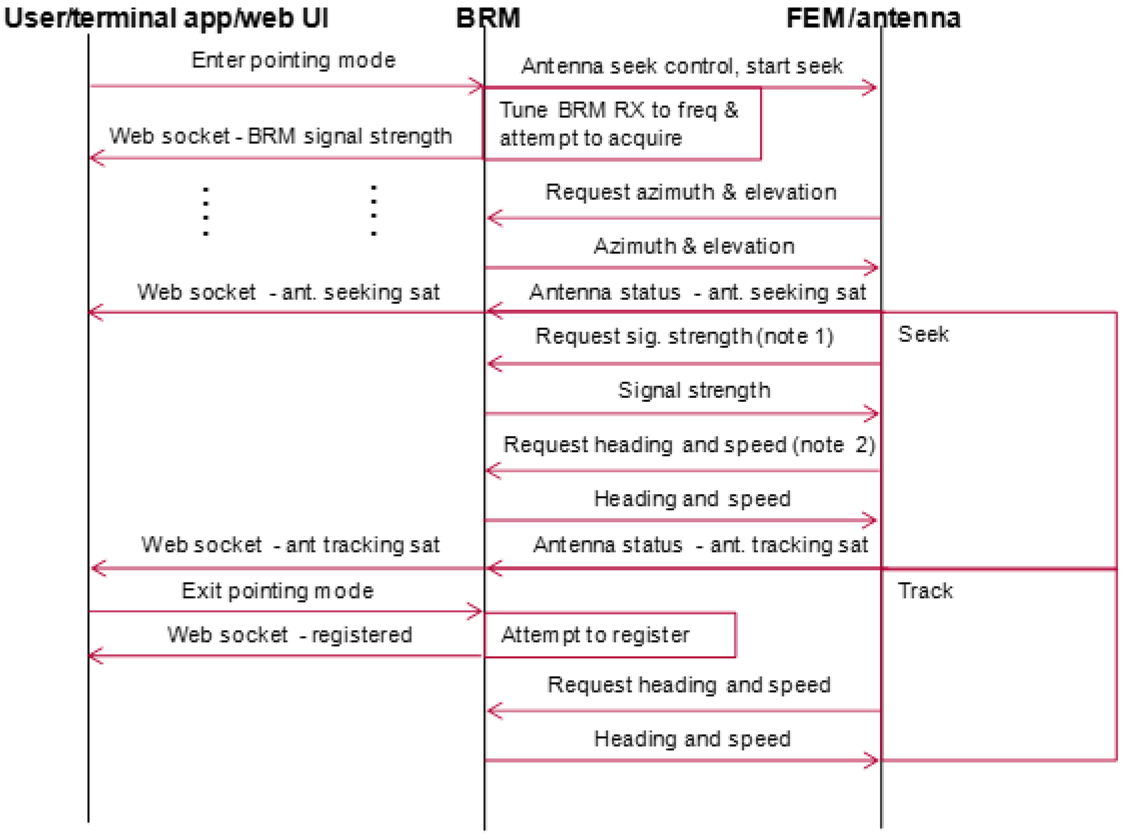

User/terminal app/web UI
BRM
FEM/antenna
Enter pointing mode
Antenna seek control, start seek
Tune BRM RX to freq & attempt to acquire
Web socket - BRM signal strength
Request azimuth & elevation
Azimuth & elevation
Web socket - ant. seeking sat
Antenna status - ant. seeking sat
Request sig. strength (note 1)
Seek
Signal strength
Request heading and speed (note 2)
Heading and speed
Web socket - ant tracking sat
Antenna status - ant. tracking sat
Exit pointing mode
Track
Web socket - registered
Attempt to register
Request heading and speed
Heading and speed

Figure 48. Message Sequence Chart for Antenna Using BRM

Appendix B: BRM Closed Loop Transmit Operation with Power Splitter

When the BRM without a FEM attached is used with the BAT/BNE or BPLT, to close the transmit power loop a proportion of the TX output should be fed to the RF detect using the circuit shown in *Figure 49*. Short coaxial cables should be used to connect the parts together.

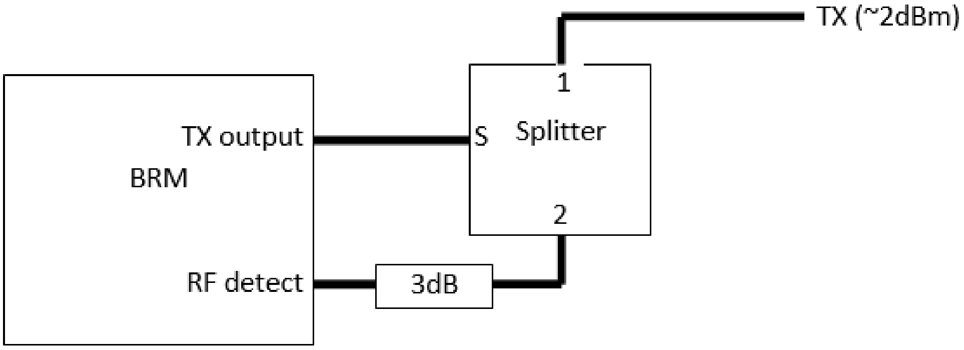


Figure 49. BRM Closed Loop Transmit Operation with Power Splitter

11.5: Recommended Parts

Part	Manufacturer	Part Number
3dB pad	Mini-circuits	VAT-3+
Splitter	Mini-circuits	ZFRSC-183-S+

Table 2. Recommended Parts

Appendix C: FEM Firmware Update Procedure

Note: To upgrade the FEM module firmware, the FEM must have resistor R78 fitted.

The FEM firmware can be upgraded using the STM32 built in bootloader on UART0

Hardware requirements: USB to serial FTDI cable, TTL-232R-3V3

https://shop.clickandbuild.com/cnb/shop/ftdichip?productID=53&op=catalogue-product_info-null&prodCategoryID=296

Software requirements: ST Flash Loader demonstrator

http://www.st.com/content/st_com/en/products/development-tools/software-development-tools/stm32-software-development-tools/stm32-programmers/flasher-stm32.html

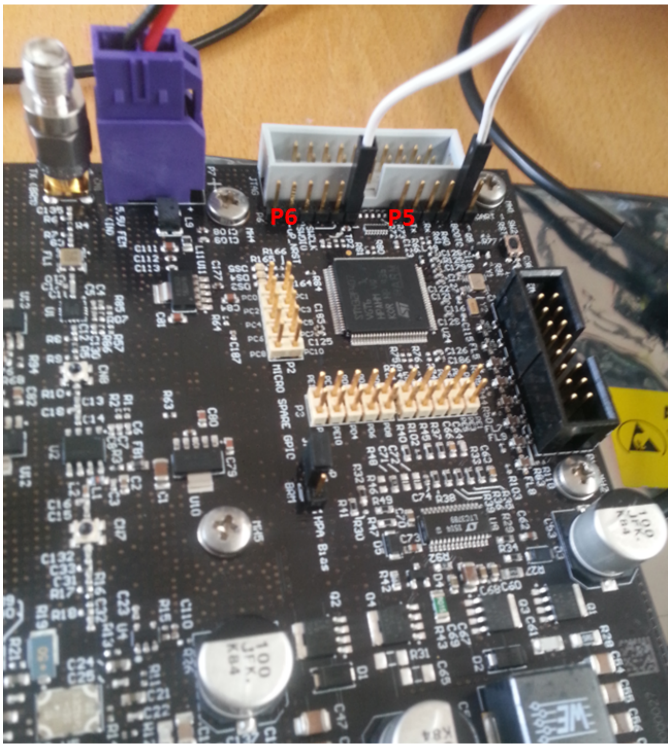
FEM firmware binary file: FemApp.bin (available)

C.1: Procedure

Note: The first steps of the procedure are slightly different depending on the type of the FEM (black –preproduction units - / green – production units) that needs to be updated. From the fifth step onwards, the process applies to both FEMs.

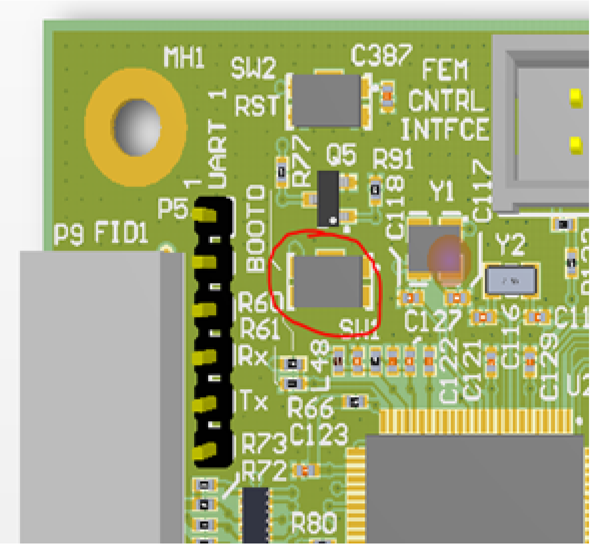
C.1.1: Black FEM

1. Make sure FEM module is powered off
2. Connect Pin 1 of P6 to pin 2 on P5
3. Power on FEM
4. Remove P5 to P6 link



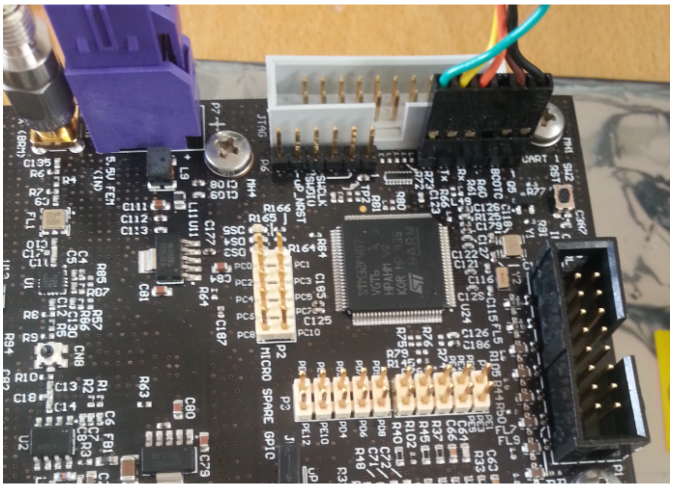
C.1.2: Green FEM

1. Make sure FEM module is powered off
2. Hold the button SW1
3. While holding the button, power on FEM
4. Release the button.

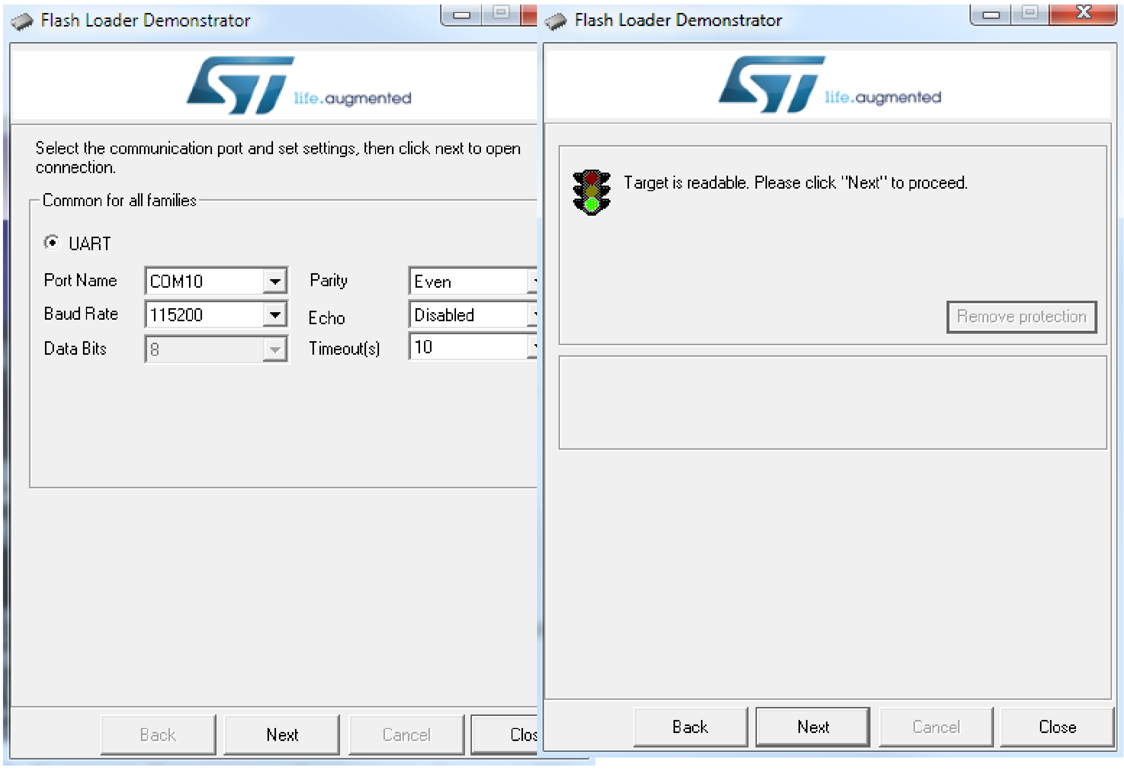


C.1.3: All FEMs

5. Connect FTDI cable.



6. Run ST’s Flash Loader Demonstrator software selecting the correct COM port



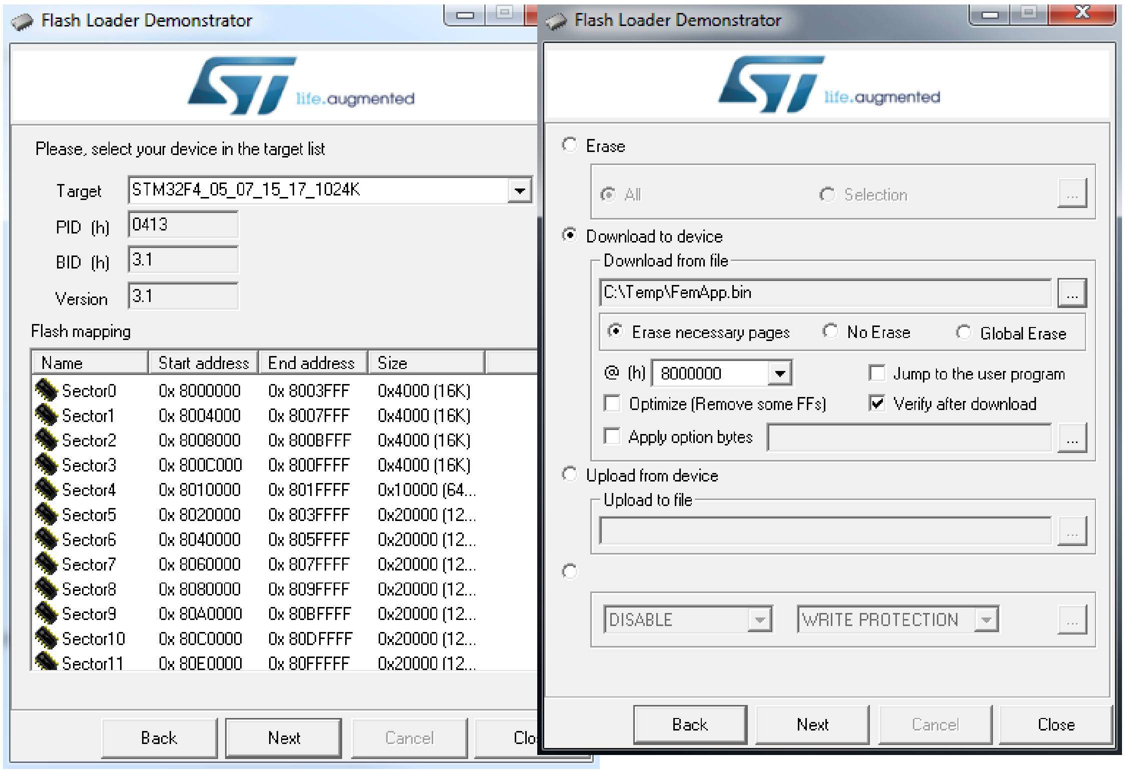
Select the communication port and set settings, then click next to open connection.

Common for all families

● UART

Port Name	COM10	Parity	Even
Baud Rate	115200	Echo	Disabled
Data Bits	8	Timeout(s)	10

Target is readable. Please click "Next" to proceed.



Please, select your device in the target list

Target: STM32F4_05_07_15_17_1024K

PID (h): 0413

BID (h): 3.1

Version: 3.1

Flash mapping

Name	Start address	End address	Size
Sector0	0x 8000000	0x 8003FFF	0x4000 (16K)
Sector1	0x 8004000	0x 8007FFF	0x4000 (16K)
Sector2	0x 8008000	0x 800BFFF	0x4000 (16K)
Sector3	0x 800C000	0x 800FFFF	0x4000 (16K)
Sector4	0x 8010000	0x 801FFFF	0x10000 (64...
Sector5	0x 8020000	0x 803FFFF	0x20000 (12...
Sector6	0x 8040000	0x 805FFFF	0x20000 (12...
Sector7	0x 8060000	0x 807FFFF	0x20000 (12...
Sector8	0x 8080000	0x 809FFFF	0x20000 (12...
Sector9	0x 80A0000	0x 80BFFFF	0x20000 (12...
Sector10	0x 80C0000	0x 80DFFFF	0x20000 (12...
Sector11	0x 80E0000	0x 80FFFFF	0x20000 (12...

○ Erase

○ All ○ Selection

● Download to device

Download from file: C:\Temp\FemApp.bin

● Erase necessary pages ○ No Erase ○ Global Erase

@ (h) 8000000 □ Jump to the user program

□ Optimize (Remove some FFs) ☑ Verify after download

□ Apply option bytes

○ Upload from device

Upload to file

○

DISABLE WRITE PROTECTION

7. Reboot FEM

C.2: BGAN Sub-Class Check

After upgrade, to check the BGAN sub-class:

1. With the FEM powered off, attach a serial cable to P5 as for the upgrade procedure

2. Open a serial connection using Putty (or similar) at 115200 baud for the serial cable attached to the FEM

3. Power on the BRM

4. Once booted the FEM will report its version. The FEM software version should now be reported as 1.18L (r11694) on the serial terminal.

5. Query the BGAN sub-class via the serial terminal by typing the following (without quotes) and pressing return: "BS ?"

6. If not 0, set the BGAN sub-class to 0 by typing: "BS 0". Power cycle the BRM for the change to take effect

C.3: BGAN GID3 Value Check

Check the GID3 field by typing `G3 ?`.

If the GID3 value reported is not `0`, then set it to `0` by typing `G3 0`.

Appendix D: Troubleshooting

Issue	Investigation	Workaround
BRM appears unresponsive when first booted up, and unable to issue any commands for uSIM; connection; messaging; AT-related activities, go on air, or connect to a BAT or BNE.	Is this unresponsiveness lasting more than 30 seconds?	If **No**, then the reason for the initial unresponsiveness is that the BRM remains in Low Power mode until it obtains a valid GPS location fix, which can take up to 30 seconds. This fix is obtained either from the internal GNSS or external NMEA interface. If after 30 seconds no valid GPS fix is obtained, the BRM will use the last known fix instead (`0N`, `0E` is the default if no previous fix is available). If **Yes**, then ensure the SIM card is inserted and is valid for the class of BGAN Terminal being used, and that the supplied FEM has been set to operate as a Class 2.
BRM freezes up during on air data transfer or when connected to a BAT or BNE.	N/A	Reboot the BRM.
Amending one or more of the following configurations has no effect on the operation of the BRM: > am_buffer_size > um_buffer_size	N/A	These configuration settings are currently unsupported by the BRM.
Some BRM WebUI pages occasionally lock up.	N/A	Reboot the BRM.
On air connection problems.	Is the location provided to the BRM accurate?	If **No**, then ensure the location is correct. If the Terminal is mobile, place it in a static location first so it can obtain a valid GPS fix before it becoming mobile again. If **Yes** and the Terminal is either static, or is mobile but has obtained a valid GPS fix in a static format, then please contact your point of contact at Inmarsat.

Issue	Investigation	Workaround
initial on-air connection establishment is intermittent	N/A	Reboot the BRM. If a Reboot fails to resolve, then please contact your point of contact at Inmarsat.

12: Glossary

Term	Abbreviation	Definition
Application Programming Interface	API	Specifies how software components in computer programmes should interface with each other. APIs can either come in the form of a library that includes specifications for routines, data structures, object classes, and variables, or, for SOAP and REST services, an API comes as just a specification of remote calls exposed to the API consumers. For GX, APIs have been written to specify the interactions between the Inmarsat Gateway platform and the various back-end systems responsible for billing; order fulfilment; customer relationship management; network management.
ATtention	AT	
Broadband Global Area Network	BGAN	Inmarsat's BGAN service provides simultaneous voice and broadband data communications globally from small and lightweight satcom terminals. The service is provided by Inmarsat's global constellation of I-4 satellites.
BGAN Radio Module	BRM	
Global Navigation Satellite System	GNSS	
General Purpose Input Output	GPIO	
Non-Volatile	NVRAM	

Random Access Memory		
Random Access Memory	RAM	A type of computer memory that can be accessed randomly; that is, any byte of memory can be accessed without touching the preceding bytes.
Terminal Development Kit	TDK	
User Interface	UI	