

Bittium Tough Mobile

Quick start guide

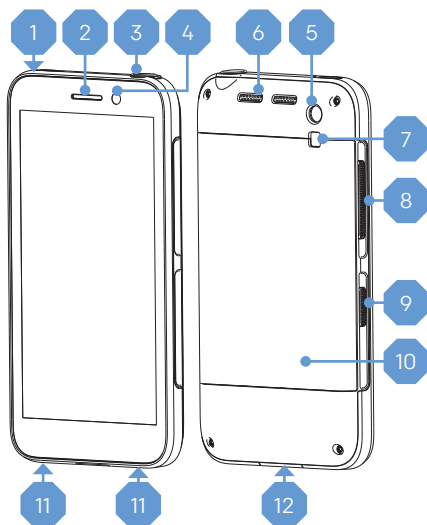


Bittium

Device at-a-glance

- 1 Power key / status indicator LED / emergency key
- 2 Earpiece and microphone
- 3 Headset and protective cover
- 4 Front Camera
- 5 Back Camera
- 6 Loudspeakers
- 7 Flash LED
- 8 Volume Key
- 9 Programmable Key
- 10 Battery Cover
- 11 Battery charging connectors
- 12 USB 3.0 port and protective cover

The ambient light sensor and proximity sensor are located next to the camera on the front of the Tough Mobile. The micro USB 3.0 port is located on the bottom of the Tough Mobile.



Please read this user manual carefully before using the device. The Tough Mobile is water and dust resistant (IP67). In order to maintain the water and dust resistance the battery cover, the USB connector cover and the headset cover must be properly closed and undamaged.

Intentional underwater immersion of the Tough Mobile should be avoided. The Tough Mobile is not designed for purposeful underwater or shower usage. Purposeful use of the phone in these environments will result in a void of the warranty. For more info on Bittium Tough Mobile Ingress Protection see <http://www.bittium.com/BittiumToughMobile#support>

Box contents

The Tough Mobile sales package contains the following items:

- Battery
- Charger, with US, UK and EU adapters
- Micro USB 3.0 cable
- 3.5mm Headset
- Quick Start Guide

The box contents and the appearance of the accessories may vary.

Operating system and applications

The Bittium Tough Mobile runs the Android operating system. This Quick User Guide contains only highlights and Bittium Tough Mobile specific features and functionalities. For a full Android User Guide please refer to: **<http://www.bittium.com/Bittium-ToughMobile#support>**

The Tough Mobile may have 3rd party applications pre-installed. For more information, see **<http://www.bittium.com/BittiumToughMobile#support>**.

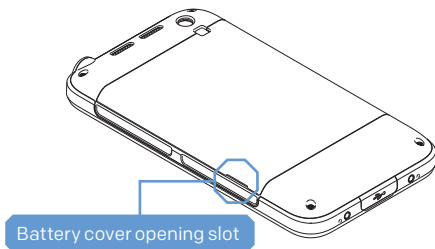


Verify that the Tough Mobile is turned OFF before removing the battery and inserting SIM card(s).

Getting started

To start using the Tough Mobile first remove the battery cover and insert the SIM card(s).

To open the Tough Mobile battery cover insert a thin plastic wedge to the slot between the battery cover and the body at the lower left and pry the cover open. The back cover of the Tough Mobile should “pop-up” with a moderate level of force.

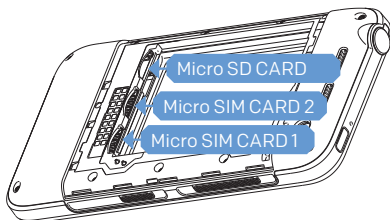


The Battery Cover of the Tough Mobile is intentionally tight to meet IP67 requirements.

Use only micro SIM cards in the Tough Mobile.

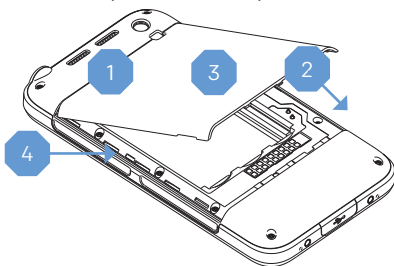
Insert your primary micro SIM card into the SIM card slot 1. If you have a secondary micro SIM card, insert it into the SIM card slot 2. Insert your micro SD card into the SD card slot. After the SIM and SD cards are inserted, insert the battery. Close the battery cover and push the power key to power the Tough Mobile.

To remove the micro SIM card use a pointed tool to pull out the SIM card.



To maintain the water and dust resistance, the battery cover must be properly closed.

- 1 Align the upper edge of the battery cover notches in place.
- 2 Snap lower edge notches in place.
- 3 Squeeze the battery cover in place.
- 4 Verify that all notches are closed on all sides by squeezing around the battery cover perimeter with your thumbs.

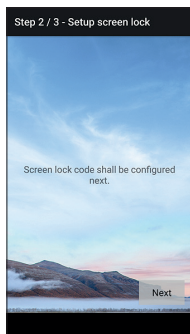


Prior to using the Tough Mobile the battery should be fully charged using the charger and the USB cable provided inside of the sales package.

Once the Tough Mobile has powered up, follow the on-screen instructions to set up the device using the Security Wizard.

Security wizard

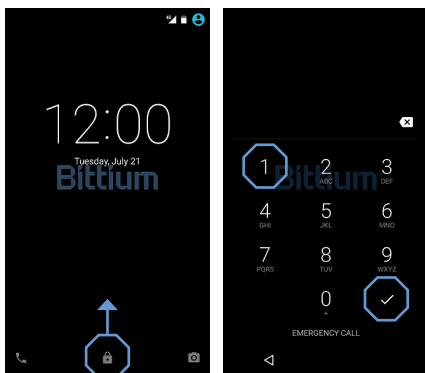
The Tough Mobile is equipped with a Security Wizard that is launched during the initial power up of the device. The Security Wizard is used to set up a number of different device settings. Follow the on-screen instructions by first setting a screen lock code.



The number of set-up steps may vary depending on the security features of the device.

Lock screen

Turning off the display locks the Tough Mobile. The Tough Mobile also locks after a period of inactivity. Turn the display off by pressing the power key once. The display can be turned on by pressing the power key or programmable key.



To open the screen lock and to access the home screen, follow the steps outlined below:

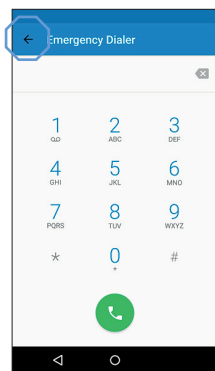
1. Swipe the lock upwards.
2. Enter screen lock code.
3. Press the "check" mark ✓.

Emergency dialer

The Emergency Dialer can be entered directly from the lock screen by pressing the text “EMERGENCY CALL”.

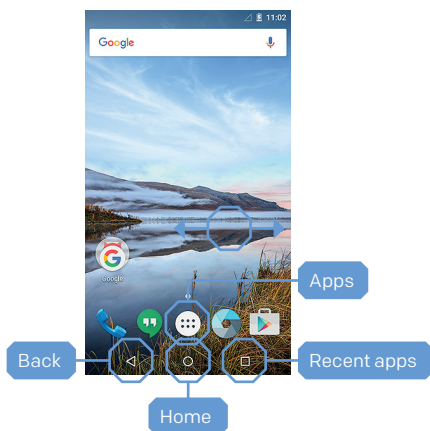
To place an emergency call, dial the emergency number and press the green icon.

To return back to the lock screen, push the arrow near the top left corner.



Home screen

Once the Tough Mobile is successfully booted up and the screen is unlocked, it will display the home screen. Press the APPS symbol in the middle section of the bottom of the screen to open the application grid. Press the square RECENT APPS symbol to open the list of recent applications. The circular HOME symbol is used to return to the home screen. The triangular BACK symbol is pressed to return to the prior screen. A swipe motion to the right or left is used to navigate around the home screen.



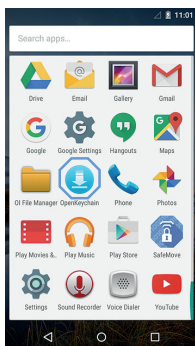
Encrypted email

The Tough Mobile supports email encryption using OpenPGP.

PGP related key management, encryption, decryption and key signing are performed using the OpenKeyChain application.

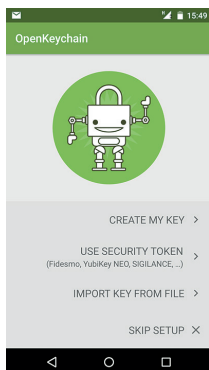
To set up the email encryption, the security keys must be created or imported for the cipher.

NOTE: The Tough Mobile with the Google Mobile Services does not have the OpenKeyChain application pre-installed. To install, touch the OpenKeyChain icon in the application grid and follow the instructions.



To create or import keys, open the OpenKeyChain application and follow the step-by-step instructions.

More information about OpenKeyChain can be found at <http://www.openkeychain.org/>

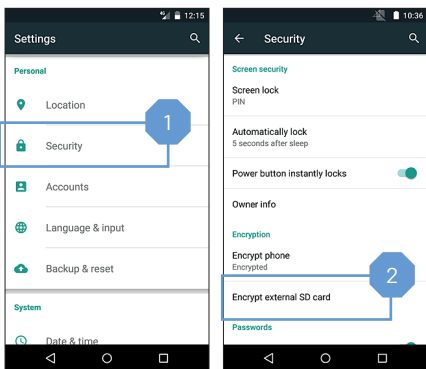


Device encryption

The Bittium Tough Mobile supports file system encryption for both the device internal flash memory and micro SD card. The internal flash memory is encrypted by default.

To enable micro SD card encryption select “Security” from the device Settings menu and Encrypt SD card from the Security settings menu. Follow the instructions provided on the Tough Mobile screen.

The Bittium Tough Mobile battery must be sufficiently charged or connected to a charger in order to proceed with the encryption set-up.

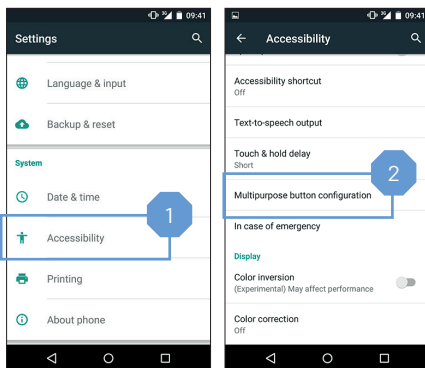


Programmable key

The Programmable Key can be configured via the Settings menu for the following features:

1. Operate the Push-to-Talk (PTT) functionality.
2. Enter sleep or Wake up the device from sleep.
3. Select active SIM card (SIM card 1 or SIM card 2).
4. Launch camera application.
5. Launch a defined application.

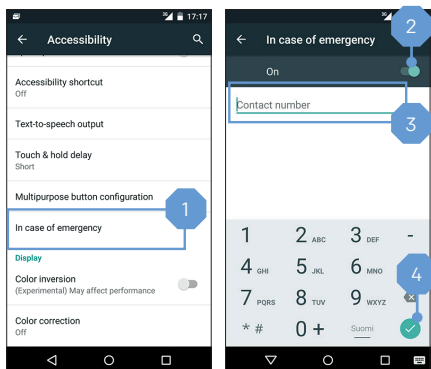
To enable Programmable Key configuration select "Accessibility" from the device Settings menu and "Multipurpose button configuration".



In case of emergency

When the “In Case of Emergency” function is turned on, you can call the pre-defined emergency Contact number by pressing the power key for a long time (>3 seconds).

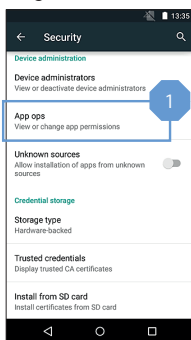
- 1 Select In Case of Emergency in the Accessibility menu.
- 2 Turn on the function.
- 3 Add the contact number you want to call in case of emergency.
- 4 Press the check mark.



Application permission firewall

The Tough Mobile allows the user to restrict access permissions of applications to phone data. This allows the user to control the data which applications may access.

Change the application permissions via the Security Settings menu.



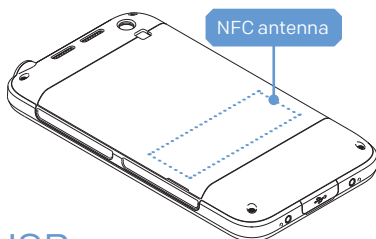
Tamper detection

The Tough Mobile is equipped with hardware tamper detection. An intrusion, other than opening the battery cover, will result in a notification from the Security Wizard. The Security Wizard will notify the user that the device integrity has possibly been compromised. Upon detection of a tampering event, the user data, including encryption keys, will be erased.

Tamper Detection is also triggered when the Tough Mobile battery has drained and the phone has lost all power. Once the Tough Mobile has been re-charged and powered on again, the Security Wizard will ask the user whether the phone should be shut down or the Tamper Detection warning should be ignored.

NFC

The NFC antenna is located in the battery cover. For security reasons, to avoid information leakage during NFC operation, NFC has been designed so that it only operates when another NFC device is placed very close to the Tough Mobile NFC antenna.



USB

The Bittium Tough Mobile has micro-USB3.0 connector and it is backward compatible with micro-USB2.0. You can use the standards-compliant micro-USB2.0 devices with the Tough Mobile. Connect the micro-USB2.0 connector to the wider slot of the micro-USB3.0 connector.

Important health and safety precautions information

Please use the Tough Mobile with the following safety precautions:

DANGER Only use the batteries, antennas, and chargers approved by The Bittium Wireless Ltd. The use of non-Bittium approved batteries, antennas, and chargers may be dangerous.

DANGER Allow only authorized personnel to service the phone and its accessories. Unauthorized service will invalidate the warranty.

CAUTION The material used in the display is glass. The display can break if your handset is dropped or if it receives significant impact. Please do not use the device if the screen is broken or cracked as this may cause an injury.

CAUTION Any modification to this product is prohibited and will void warranty. The opening of the unit and use of the components for purposes not otherwise authorized by this document, including any use in airplanes or any other Aviation application, is prohibited and will void the warranty.

CAUTION Permanent hearing loss may occur if earphones or headphones are used at high volume for prolonged periods of time.

CAUTION Do not allow children to play with the Tough Mobile since it contains small parts that could become detached and create a choking hazard.

NOTE When using your device for prolonged periods of time, such as when you're talking on the phone, charging the battery or browsing the web, the device may become warm. In most cases, this condition is normal and therefore should not be interpreted as a problem with the device.

NOTE When driving, check and obey the laws and regulations on the use of mobile phones in the area where you drive. If you are going to use your phone while driving, always pay full attention to driving and use a Handsfree Solution, if available. The law in many countries requires the use of a vehicle Handsfree Solution while driving.

NOTE Always create a backup of data you want to keep (such as contacts and calendar notes) before sending your device for service.

Important customer information

The Tough Mobile is a wireless device, containing a radio transmitter and receiver which emit radio frequency energy during its use. Most modern electronic equipment is shielded from RF signals. However, certain electronic equipment may not be shielded against the radio signals from a wireless phone.

Do not use the Tough Mobile near medical equipment without permission. A minimum of six (6) inches should be maintained between the Tough Mobile and an implantable medical device, such as a pacemaker or implantable cardiac defibrillator in order to avoid potential interference with the medical device. Persons having implanted medical devices should follow instructions from the manufacturer of the medical device for safe use within proximity of wireless devices. Wireless phones may also interfere with some hearing aids. In the event of such interference, consult the service provider or call customer service line to discuss alternatives.

Radio signals may interfere with improperly installed or inadequately shielded electronic systems in motor vehicles. Check with the vehicle manufacturer or its representative regarding your vehicle. Aftermarket electronics which have been added to the vehicle should also be checked.

Any modification of the Tough Mobile is prohibited. Only authorized personnel should service the Tough Mobile and its accessories.

Only use software updates provided by Bittium. Accessories for the Tough Mobile should be either purchased from or approved by Bittium.

Only use the battery specified by and provided by Bittium in the Tough Mobile. Do not short-circuit the battery. Do not use the battery with a charging system which has not been approved by Bittium.

Turn the Tough Mobile OFF in any facility where posted notices so require.

To avoid interfering with blasting operations turn the Tough Mobile OFF when in a blasting area or in areas posted: "Turn off two-way radio". Obey all signs and instructions.

Turn the Tough Mobile OFF when in areas with a potentially explosive atmosphere and obey all signs and instructions. Sparks in such areas could cause an explosion or fire resulting in bodily injury or even death. Areas with a potentially explosive atmosphere are often, but not always, marked clearly. Potential areas may include fueling areas (such as gas stations); below deck on boats; fuel or chemical transfer or storage facilities; vehicles using liquefied petroleum gas (such as propane or butane); areas where the air contains chemicals or particles (such as grain, dust, or metal powders); and any other area where you would normally be advised to turn off your vehicle engine.

An emergency call can be made only within a service area. For an emergency call, make sure that you are within a service area and that the device is turned on.

The device does not necessarily meet all specifications in extreme temperatures. Battery capacity (use time) is limited in low temperatures, and the device performance may be limited in high temperatures.

The device is equipped with intelligent battery charging control that limits battery charging in extremely hot and cold temperatures to ensure battery safety and extended operating life.

Limited warranty

For a period of 1 year from the date of purchase, Bittium Wireless Ltd. ("Bittium") warrants this Product, including all accessories provided in the sales box, against defects in materials or workmanship. If this Product is determined to be defective within the 1 year warranty period, Bittium will repair the Product or replace it with a new or refurbished Product, at its option, at no charge to the customer, except as set forth below.

This warranty does not cover cosmetic damage or damage due to misuse, abuse, negligence, accident, or modification of any part of the Product. This warranty does not cover damage due to improper operation or maintenance, connection to improper voltage supply, or attempted repair by anyone other than a facility authorized by Bittium to service this Product. For more info on Bittium Tough Mobile Ingress Protection see **www.bittium.com/BittiumToughMobile#support**

To obtain warranty service, you must receive a Return Authorization from Bittium and ship the Product, at your expense, to Bittium's authorized service facility. You must ship the Product in either its original packaging or packaging affording an equal degree of protection. This warranty does not cover customer instruction, set up, or set up adjustments or network coverage problems.

Please contact support@bittium.com for warranty support.

Published by:

Bittium Wireless Ltd.
Tutkijantie 8
90590 Oulu
Finland
Phone: +358 40 344 2000
Fax: +358 8 343 032
www.bittium.com

Legal Notice

Copyright 2016 Bittium. All rights reserved. The information contained herein is subject to change without notice. Bittium retains ownership of and all other rights to the material expressed in this document. Any reproduction of the content of this document without prior written permission from Bittium is prohibited.

Notice

Bittium reserves the right to change its products and the information in this document without notice due to continuous improvement and development. Bittium makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Bittium shall not be liable for errors contained herein or for damages in connection with the furnishing, performance, or use of this material.

