Bittium Tough Mobile C

Secure OS Guide

Bittium

Introduction

This quick guide describes the Tough Mobile C device security enhancements. We also encourage you to read Bittium Tough Mobile Quick Start Guide that can be found in the sales box and via www.bittium.com/BittiumToughMobile

It will guide you through some of the generic device features. This guide acts as a supplement to that guide and the features described here are provided in addition to the features and functionalities described in Bittium Tough Mobile Quick Start Guide.

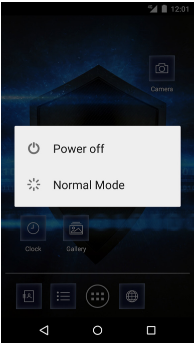
Security features

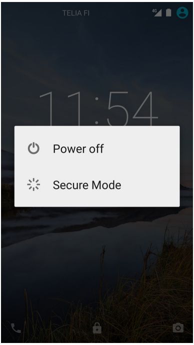
- Dualboot
  - Two separate operating systems
- Normal mode, Android 6.0.1
  Secure mode: Bittium Secure OS
- Two-phase user authentication
- SafeSave
  - High security data storage for sensitive information.
  - Application for moving sensitive files.
- System cleaning
  - Secure file erase
- Bittium Enterprise Application Library
- Application whitelist

Dualboot

The device has a Dualboot feature: it contains two operating systems: Normal Mode for daily personal use and Secure Mode for high security usage. The operating systems are completely separate to ensure security for the highly critical information stored and used in Secure Mode. Note that files cannot be used or copied between modes.

Switching between Normal Mode and Secure Mode can be done via the power key:



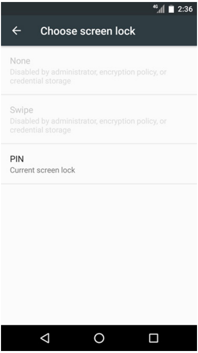


Pressing the power key lightly on top of the device opens the Power key menu with options for Power off, Normal Mode and Secure Mode, depending on the currently active mode.

Changing the PIN code

Setting a PIN code for screen unlocking is mandatory for security reasons. When using the device for the first time, the security wizard Setup screen lock (see figure below) requests you to specify a PIN code for screen unlock.

In the Unlock selection screen choose PIN. Next, enter the PIN and re-type it for confirmation. Now you are ready for the next phase.



None
Disabled by administrator, encryption policy, or credential storage

Swipe
Disabled by administrator, encryption policy, or credential storage

PIN
Current screen lock

NOTE! Both operating systems require their own PIN codes and these must be set separately.

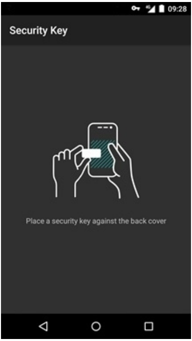
A new PIN can be entered via: Settings -> Security -> Screen lock.

Two-phase user authentication

In Secure Mode the user is authenticated with two-phase authentication. Two-phase authentication means that both PIN code and a personal security key are used to make sure that the correct person is unlocking the device. "Something you know and something you have".

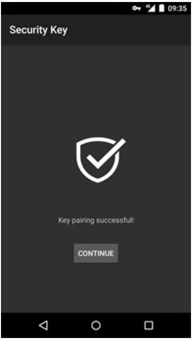
Security Key

The device comes supplied with a Security Key which is used in the Secure Mode. To authenticate with the security key follow the on-screen instructions. NOTE! To authenticate, place the Security Key against the device back cover as instructed.



Security Key

Place a security key against the back cover



Security Key

Key pairing successful!

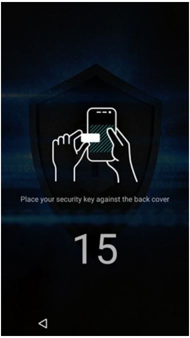
The device will indicate that pairing is successful by stating ‘Key pairing successful!’ Tapping ‘Continue’ finalizes the two-phase authentication setup.

In case the Security Key is damaged or lost please contact the system administrator for assistance.

Daily use: Locking and unlocking the device

To unlock, switch on the device screen and swipe up. Enter your PIN code. Once the correct PIN is entered, Unlock view is displayed. Place your Security Key against the back cover to unlock the device.

There is a 15-second time limit for placing the Security Key correctly when unlocking the device. The timer is shown on the device screen.



Place your security key against the back cover

15

If unlocking fails or the timer runs out, the device remains locked. A PIN code is required again before using the Security Key to unlock the device.

NOTE! Always when switching from Normal Mode to Secure Mode authenticate yourself at least once to re-enable secure data services, like updating the e-mail. Secure connection will be established after a successful logon.

NOTE! When the screen is locked SafeSave is also locked and encrypted. Successful two-phase user authentication gives access also to the SafeSave data.

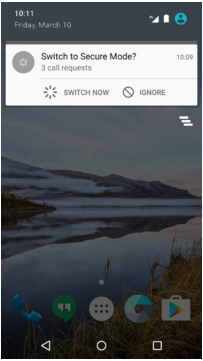
Security Key authentication timer

The device may have an authentication timer enabled by the device administrator. If this timer is enabled, the device does not require the use of the Security Key every time to unlock the device. If the timer value is set for example to 30 minutes, it is enough to enter only your PIN code for authentication during the 30 minute period to get access to the device. After 30 minutes, both the PIN code and Security Key authentication is again required to unlock the device.

NOTE! SafeSave cannot be used when the timer is enabled. For security reasons access to the full content of SafeSave requires two-phase user authentication.

Secure Mode activity user notifications

Normal Mode can notify the user about Secure Mode activity that requires user attention. This can be, for example, a secure communication request which cannot be responded to from Normal Mode. The notification prompts the user to switch into the Secure Mode. It is also possible that the system administrator has disabled some or all of the notifications depending on the security policy used.



10:11
Friday, March 10

Switch to Secure Mode? 10:09
3 call requests

Storing confidential information

In Secure Mode the device has a SafeSave (high security data storage) feature. It is recommended to use SafeSave to store sensitive information. Any old data and files that have not been modified within 30 days are automatically deleted from the SafeSave folder. A notification will be displayed three days before the data removal so that you can back up the data before it is deleted. SafeSave has limited capacity, so it should be used strictly for confidential data. SafeSave is closed after a short timeframe every time the screen is locked. After SafeSave has been closed it can be accessed only by using the two-phase user authentication. SafeSave is not available as a storage folder in Normal Mode on a computer when connected.

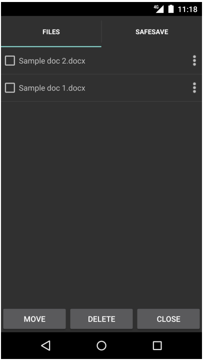
SafeSave application

The SafeSave application can be used to display all common document files stored in Download and SafeSave folders. The application allows the user to move files to the SafeSave folder and to remove files from the Download and SafeSave folders.

NOTE!: Files stored under third party applications, such as e-mail, are not listed by the SafeSave application.
NOTE!: SafeSave capacity is 150MB.

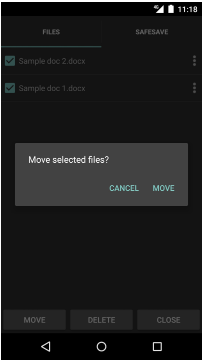
If a file, for example an e-mail, contains sensitive information it is suggested to first save the file to the Download folder and then use the SafeSave application for the easy move operation.

When the SafeSave application is started, it lists document files from the file system in the Files tab.



Files can be selected for a MOVE or DELETE operation.

NOTE! Neither MOVE or DELETE operations can be undone using the SafeSave application. The move operation moves the files to the SafeSave folder.

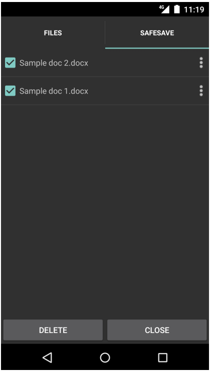


☑ Sample doc 2.docx

☑ Sample doc 1.docx

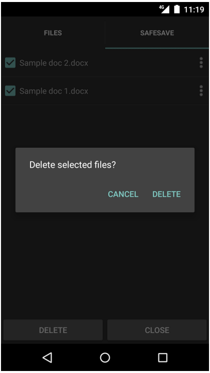
Move selected files?

The SafeSave tab provides easy functionality for deleting files from the SafeSave folder.



☑ Sample doc 2.docx

☑ Sample doc 1.docx



☑ Sample doc 2.docx

☑ Sample doc 1.docx

Delete selected files?

Double-tapping or pressing and holding on a list item in the SafeSave or Files tab will open the file using the application that is capable of opening the file.

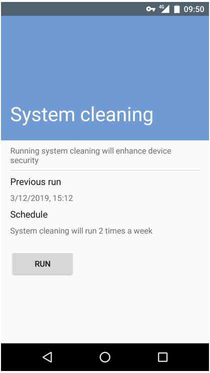
Using an SD card

SD memory card can be used both in the Secure Mode or the Normal Mode. In addition to the normal formatting operation before use, the SD card is also encrypted if it is taken into use in the Secure Mode. If the SD card is not in use in the selected mode a notification will be displayed after the device has started.

NOTE: if you try to access an encrypted SD memory card in Normal Mode the encypted contents of the card is reported by the system as 'corrupt data'. However - DO NOT format the content of the SD memory card in Normal Mode. If you format it, you will loose the data stored to the SD memory card in Secure Mode.

System cleaning

The System cleaning function erases temporary and obsolete files to improve device performance and to maintain device security. The function is set to run automatically and it can also be started manually via Settings -> Security -> Advanced -> System cleaning.



09:50

System cleaning

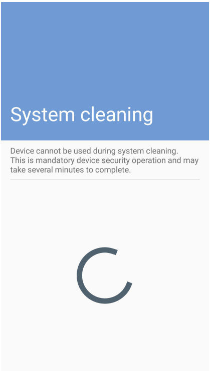
Running system cleaning will enhance device security

Previous run

3/12/2019, 15:12

Schedule

System cleaning will run 2 times a week



System cleaning

Device cannot be used during system cleaning. This is mandatory device security operation and may take several minutes to complete.

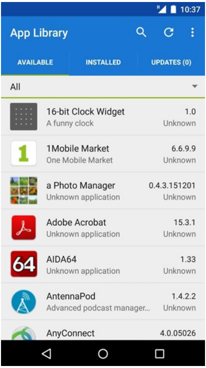
System cleaning runs both in the Secure and Normal modes. The cleaning is performed even if the device is powered only briefly at a time.

Enterprise Application Library

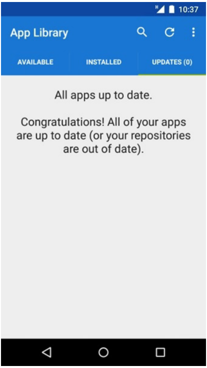
The Enterprise Application Library is available in the main view as an application named App Library.

It contains approved applications which can be downloaded and installed to the device from a network server. However, some application installations may be blocked although they appear in the library.

You can also view all installed applications and receive application updates.



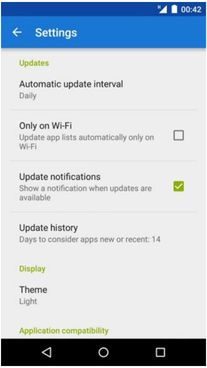
16-bit Clock Widget A funny clock	1.0 Unknown
1Mobile Market One Mobile Market	6.6.9.9 Unknown
a Photo Manager Unknown application	0.4.3.151201 Unknown
Adobe Acrobat Unknown application	15.3.1 Unknown
AIDA64 Unknown application	1.33 Unknown
AntennaPod Advanced podcast manager...	1.4.2.2 Unknown
AnyConnect	4.0.05026



All apps up to date.

Congratulations! All of your apps are up to date (or your repositories are out of date).

You can change application settings such as Updates, Application compatibility or Display Theme by opening Settings in the menu in the upper right corner. You can also rename the local repository via Settings, but you cannot change the network repository itself.



Updates

Automatic update interval
Daily

Only on Wi-Fi □
Update app lists automatically only on Wi-Fi

Update notifications ☑
Show a notification when updates are available

Update history
Days to consider apps new or recent: 14

Display

Theme
Light

Application compatibility

System updates

In Bittium Tough Mobile C, receiving and installing system software updates is possible only in Secure Mode. The handset's battery level must be more than 50% for a successful update to commence.

The availability of an update can be checked at any time by going to Settings -> About phone –> Software Updates –> Check now.

Published by:
Bittium Wireless Ltd.
Ritaharjuntie 1
90590 Oulu
Finland
Phone: +358 40 344 2000
www.bittium.com

For the latest Secure OS Guide, visit:
https://www.bittium.com/secure-communications-connectivity/bittium-tough-mobile-c

Legal Notice

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 damage in connection with the furnishing, performance, or use of this material.

www.bittium.com