

SECURE DRIVE

BLUETOOTH



SecureUSB BT USER MANUAL

Contents

SecureUSB BT Overview 3

Safety Information 3

SecureUSB BT Features 5

Icon Interpretations 5

Installing the Accompanying App 6

Passwords and Procedures 7

Password Requirements 7

Procedural Conventions 7

Adding the SecureUSB to the App (Pairing) 7

Unlocking the SecureUSB 8

Disconnecting the SecureUSB from Your Computer 8

Locking without Unplugging from the Computer 9

Setting Options 10

Entering Settings Mode 10

Password Options 10

Access Options and Locking Options 11

Managing the SecureUSB BT 13

Removing a SecureUSB BT 14

Brute Force Hacking Detection 14

Resetting (Deleting) the SecureUSB BT 14

Reformatting the SecureUSB BT 15

Technical Support 19

Contact Information 19

Troubleshooting 20

Warranty and RMA Information 20

SecureUSB BT Overview

Thank you for purchasing the SecureUSB BT Model ('USB' hereafter). It's an easy to use, hardware encrypted, password activated USB 3.0 drive. This Bluetooth®-capable model uses an application with wireless user-authentication on a smartphone—iOS and Android. (Apple iOS includes Apple iPhone, Watch, and iPad.)

The SecureUSB uses military grade XTS-AES 256-bit hardware encryption, which encrypts all data stored on it in real-time. It works on all computer and embedded systems that support standard USB protocol.

Should your SecureUSB get lost or stolen, rest assured that all data on it is protected by military grade encryption and cannot be accessed without entering the password via the DataLock App.

NOTE: For extra security with multiple users, the Remote Manager Model allows a User and an Admin password as well as allowing the admin to remotely make settings to Users' USBs. This makes it perfect for corporate and government deployment (NOT COVERED IN THIS MANUAL).

Your SecureUSB may have Cloud Backup and built-in Antivirus features installed. For more information, please contact Support at SecureData™.

REQUIREMENTS

The SecureUSB works on Windows, Mac, Android, Linux, or Chrome operating systems, or any host such as an embedded system. The computer/host must have a USB 2.0 port, minimum.

WHAT'S INCLUDED?

- 1 SecureUSB (with PDF User Manual)
- 1 Quick Start Guide

Safety Information

This icon  indicates important information regarding the safety of the product (Cautions). Please be mindful of these messages. Contact [support](#) if you have questions.

PRECAUTIONS

- Do not expose the USB to water or moisture.
- Resetting the USB will delete all stored data as well as all passwords.
- Forgetting your password will render the USB data inaccessible. There is no 'backdoor.'
- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.

EMI CAUTIONS

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

The normal function of the product may be disturbed by strong Electro Magnetic Interference. If so, simply remove and reinsert the product to resume normal operation by following the instruction manual. In case the function could not resume, please use the product in another location.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) this device must accept any interference received, including interference that may cause undesired operation.

SecureUSB BT Features

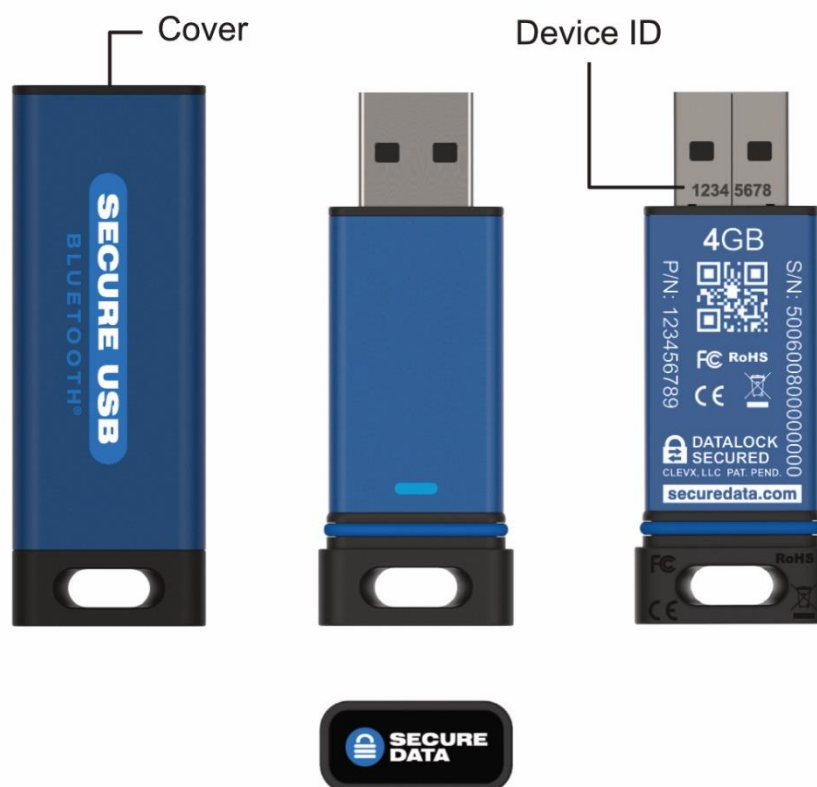


Figure 1: SecureUSB BT layout showing the LED, Device ID number, Serial Number and Part Number

Icon Interpretations

ON THE SECUREUSB

LEDs on the USB are represented here by colored icons.

LED	Meaning
   (one blink)	Plugged into computer; LED test
 = Red solid	Powered and locked <i>but not</i> BT-connected
 = Red blinking	Powered and locked <i>and</i> BT-connected via the App
 Blue solid  Blue blinking	The USB is unlocked and accessed (USB is transferring data). NOTE: The blue LED may be on or blinking during any procedure after the USB is unlocked.

ON THE APP

App Icon	Meaning
	USB is locked
	USB is unlocked (password has been entered) although it may still need formatting for use if it has been reset.
	USB is blank (such as when not formatted) and the password is not set yet
	The USB is BT-connected to the app and Authenticated. If you don't see this icon, the USB is BT-connected but not Authenticated which means that if the USB is unlocked you can access your files but cannot access the Settings Menu or swipe right to lock. To Authenticate, enter the password.
	Change the password
	App will remember the password
	Inactivity AutoLock
	Step-away AutoLock
	Read-Only Mode
	Reset the USB (erase all data and settings)

Installing the Accompanying App

The app, named DataLock®, for your new SecureUSB must be installed on an iOS or Android device to control all the USB's functions. Only one app is required to control multiple USBs.

Download the app for an iOS device from the Apple App Store or for an Android device from Google Play. It can be installed just like any other app, clicking Download then Install.



Download the DataLock App and then install it.

Passwords and Procedures

The SecureUSB BT Model is shipped with password 11223344. We strongly suggest changing the password for security.



CAUTION: Risk of loss of data. If you forget your password all data will be inaccessible and reformatting will be required. There is no 'backdoor.'

Password Requirements

Your password must:

- be 7-15 characters in length, letters or numbers. Special characters okay.
- not contain only repetitive numbers or letters, e.g. (3333333) or (ccccccc)
- not contain only consecutive numbers or letters, e.g. (1234567), (78901234), (7654321), (abcdefg)

Procedural Conventions

The procedures in this manual show LED status that you should see after performing each step. Next to it is what the app displays at some point during the procedure.

Adding the SecureUSB to the App (Pairing)

The eight-digit Device ID is required; it is printed on the USB connector.

Adding the USB	LED	APP
1. Plug the USB into a computer.	   (blink once) then 	
2. Start the DataLock App on your device. NOTE: Ensure your device is BT enabled.		
3. Tap  .		
4. Tap the USB drive name that appears.		
5. Tap Continue if you know the Device ID, otherwise tap Unplug Drive and a. unplug the USB b. write down the ID that's on the connector c. re-insert the USB  d. tap the USB name e. enter the password and tap Unlock  6. restart this main procedure from 1.		 1. Please unplug and write down Device ID from your SecureData Flash drive, located on the USB connector.  2. Plug your SecureData Flash drive into your computer. Unplug Drive Continue

Unlocking the SecureUSB



CAUTION: Possible loss of data. After ten failed attempts to unlock the SecureUSB, the password, all data, and the formatting will be deleted. Refer to *Brute Force Hacking Detection* on page 14.

NOTE: Until the USB is unlocked it does not display in your computer's File Manager (Explorer or Finder).

Unlock the USB	LED	APP
A. WHEN STARTING USE: 1. Plug the USB into a computer if it's not already.	   (blink once) then 	
2. Start the DataLock App on your device. NOTE: Ensure your device BT is on.		
3. After it initializes, tap the USB name.		
4. Type in the password ¹ and tap Unlock .		
B. AFTER WAKING FROM SLEEP, i.e., 'not authenticated' which is caused when some OS's sleep, or the app is closed. <i>This icon  means Authenticated.</i>		
1. Open the app.		
2. After it initializes, tap the USB name.		
3. Type in the password.		
4. Tap Unlock.		

¹ When new the password is 11223344

NOTE: If the USB still doesn't appear in your computer's file manager, refer to *Troubleshooting* on page 20.

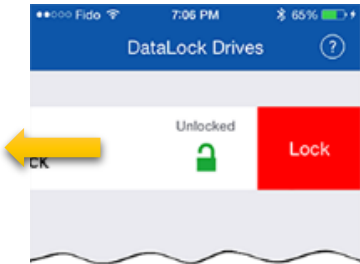
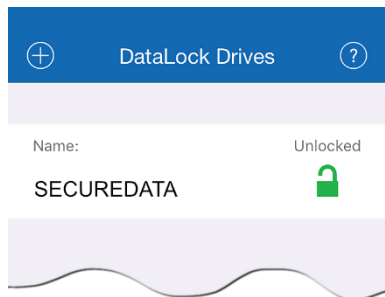
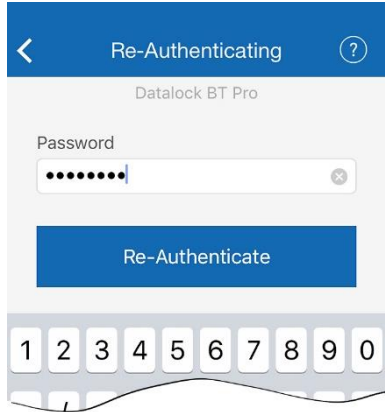
Disconnecting the SecureUSB from Your Computer

Generally, you can just unplug the USB drive—it will lock automatically.

NOTE: Some computer systems may require clicking the *Safely Remove Hardware/Eject* icon on your system prior to unplugging the USB. Wait for the red LED to come on indicating it is locked and ready to disconnect from the computer.

Locking without Unplugging from the Computer

The two methods shown below (A & B) allow for the two states the app could be in: Authenticated (logged in) or not.

Lock without Unplugging	LED	APP
A. If the App is still BT-connected to the USB and unlocked: 1. In the app, swipe the desired USB name to the left. If it does not swipe left, it needs to be authenticated. See B below.		
5. Tap Lock . The USB locks.		
B. If the App is still BT-connected to the USB but not Authenticated (this icon  does not appear): 1. In the app, tap the desired USB name. NOTE: If <i>Remember Password</i> is on, skip the next step.		
2. Type in the password and tap Re-Authenticate .		
3. Lock the USB—refer to the steps in part A above.		

Setting Options

The following headings describe enabling options and features.

For Remote Management options and corporate administrators, see our website for the Remote Management SecureUSB BT Model.

NOTE: Unless otherwise noted, procedures listed below assume the USB has already been unlocked  and authenticated .

Entering Settings Mode

The Settings Mode allows functions such as enabling and disabling the *Read-Only* feature and an automatic *Step-away AutoLock*. Access the Settings Mode by tapping the desired USB name anytime it's unlocked and authenticated.

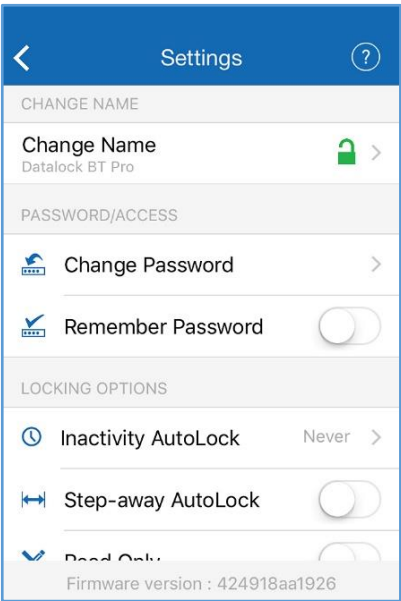


Figure 2: The Settings Menu, partial view. ➞

Password Options

CHANGING THE PASSWORD

Follow these steps to change an existing SecureUSB BT password.

Change the Password	LED	APP
1. With the USB unlocked, tap the desired USB name .		
2. Tap Change Password and enter your current password.		Refer to Figure 2: above.
3. Enter your current password, then the new password and retype it into the Confirm field.		
4. Tap Change Password.		

NOTE: If a mistake was made while defining a new password or the procedure was not completed, the USB will retain the old password.

SETTING TO REMEMBER PASSWORD

To skip entering your password every time, you can have the password field auto-fill.



CAUTION: Security risk. When Remember Password is set, the application will not require a password to unlock the SecureUSB. With this setting we strongly suggest that you use a passcode on your iOS/Android device. If the Step-away AutoLock feature is also on, the USB will authenticate and unlock automatically as soon as the app is opened and within BT range.

Remember Password	LED	App
1. With the USB unlocked and authenticated (logged in), tap the desired USB name.		
2. Tap the Remember Password button to the ON position (green).		
3. Tap Yes to confirm.		

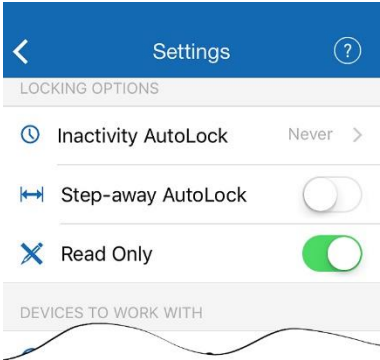
Access Options and Locking Options

Below are the three features for locking or restricting usage (and resetting them).

ENABLING READ-ONLY

Once Read-Only is set, access prevents writing or changing data and saving or deleting files until Read/Write is enabled.

Enable Read-Only	LED	App
1. With the USB unlocked and authenticated, tap the desired USB name .		

2. Tap the Read Only button to the ON position (green).		
3. Tap Lock to the confirmation message.		

The USB locks and will be in R-O Mode when unlocked.

ENABLING READ/WRITE

Read-Only can be turned off restoring read and write access.

Enable Read/Write	LED	App
1. With the USB unlocked and authenticated (logged in), tap the desired USB name .		
2. Tap the Read Only button to the OFF position (not green).		
3. Tap Lock to confirm disabling Read-Only.		

The USB locks and will be in Read/Write mode when unlocked.

SETTING THE INACTIVITY LOCK

To protect against unauthorized access when the SecureUSB is connected to a host computer and unattended, the USB can be set to automatically lock after a pre-set amount of time.

The default state of the Inactivity Lock is OFF. This feature can be set to activate (lock) at predefined times between 1 and 60 minutes.

Enable Inactivity Lock	LED	App
1. With the USB unlocked and authenticated, tap the desired USB name .		
2. Tap Inactivity Lock.		
3. Tap the desired inactivity interval after which time the USB will automatically lock.		A checkmark displays adjacent to your selection. ✓

The Inactivity Lock is now set for subsequent USB use, until changed. When it locks, the red USB LED lights.

DISABLING THE INACTIVITY LOCK

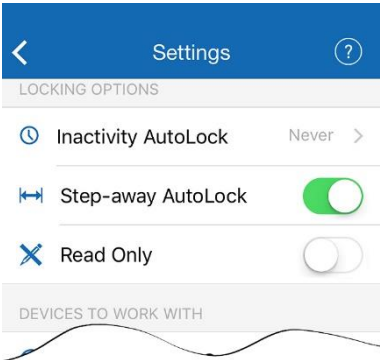
Disable the Inactivity Lock	LED	App
1. With the USB unlocked and authenticated, tap the desired USB name.		
2. Tap Inactivity Lock.		
3. Tap Never.		A checkmark displays adjacent to your selection. ✓

The Inactivity Lock is now disabled.

SETTING THE STEP-AWAY AUTOLOCK ON AND OFF

The Step-away AutoLock will lock the SecureUSB (the drive disappears from the File Explorer/Finder) when the iOS/Android device is moved about 3m away from the USB for longer than 5 seconds.

NOTE: If Remember Password option is also on, when the device is returned to the vicinity, the USB will unlock automatically.

Set the Step-away AutoLock	LED	App
1. With the USB unlocked and authenticated, tap the desired USB name .		
2. Tap the Step-away AutoLock button to the ON position (green).		
3. Tap Yes to confirm.		

The Step-away AutoLock is now on.

To disable the Step-away AutoLock, tap the Step-away AutoLock button OFF (not green).

Managing the SecureUSB BT

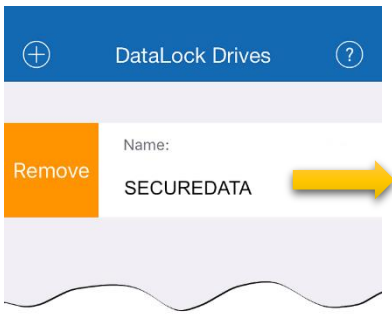
The following headings discuss important, though less common, actions for managing your USB.

Removing a SecureUSB BT

If you don't want to use a previously paired USB with your smartphone app, you can remove this USB from the app. You can add it back again by tapping the plus sign  at the *Home* window. To add a USB, see *Adding the SecureUSB to the App (Pairing)* on page 7.



CAUTION: Risk of unprotected data. Removing the SecureUSB name from your device when it's unlocked will leave the USB unlocked. Anyone will be able to access your data without a password until it is unplugged from the computer which will lock it.

Remove USB	LED	App
1. With the USB locked or unlocked, touch the desired USB name and swipe right . (If unlocked, see the caution message above.)	 or 	 or 
2. Tap Remove.		
3. Tap Remove to confirm.	 or 	 or 

Brute Force Hacking Detection

If an incorrect password is entered ten consecutive times, the USB brute force hacking detection triggers and **the password, all data, and format will be deleted**. To re-use the USB see *Reformatting the SecureUSB* on page 15. The data is not recoverable.

Resetting (Deleting) the SecureUSB BT

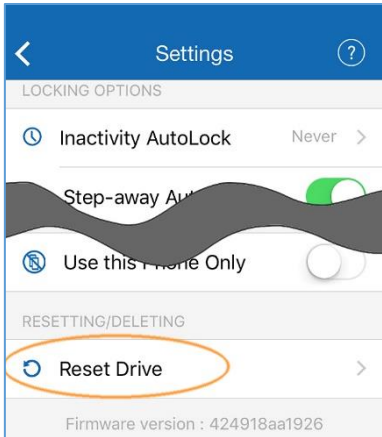


CAUTION: Resetting the SecureUSB will delete all data stored on it including the password and formatting. After resetting it, the USB must be formatted again to use it. See *Reformatting the SecureUSB* on page 15.

If you want to delete all data stored on the USB (including the password), you can perform the following Reset function. It also removes the encryption, requiring the USB to

be reformatted to generate new encryption. To reformat the USB after resetting it, see the heading *Reformatting the SecureUSB* on page 15.

The Device ID is required.

Reset the USB	LED	App
1. With the USB unlocked and authenticated (logged in), tap the desired USB name .		
2. Tap Reset Drive.		
3. Tap Reset Drive to continue.		
4. Tap Continue if you know the Device ID, otherwise tap Unplug Drive and f. unplug the USB g. write down the ID that's on the connector h. re-insert the USB  i. tap the USB name j. enter the password and tap Unlock  k. restart this main procedure from 1.		
5. Tap Reset to the confirmation message.		
6. Follow the onscreen instructions for entering the Device ID.		

All data is now removed from the USB.

Reformatting the SecureUSB BT

In the event that hacking detection has been triggered or the USB has been reset (all data on the USB has been deleted) the USB must be reformatted for future use.

To reformat your SecureUSB, do the following:

Create a Password	LED	App
1. Insert the USB drive if it is not already.		
2. Tap the desired USB name .		
3. Type in a new password.		
4. Type password again to confirm.		
5. Tap Create Password.		

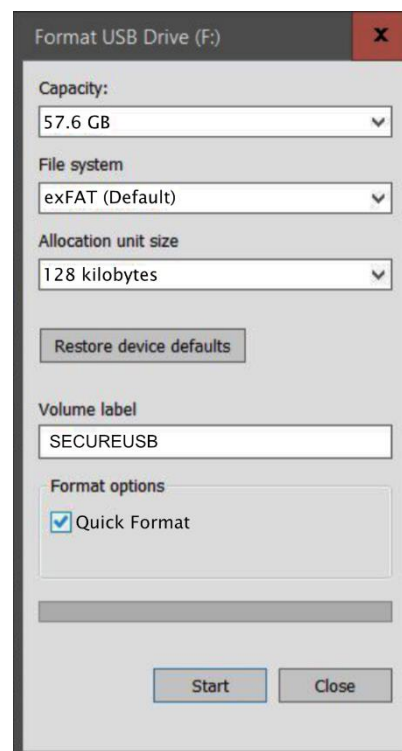
A system popup will appear regarding the 'disk' inserted. **To continue**, follow the steps below for your type of computer.

FOR WINDOWS OS

- At the system popup message (shown below) click Format Disk.



- If the settings are okay, click Start.
Generally the default values are good. Use FAT32 or exFAT for the file system. See Figure 3: (like SecureUSB).
- Click OK to the warning about erasure.
- Click OK to complete.
- Click Close to exit the dialog.

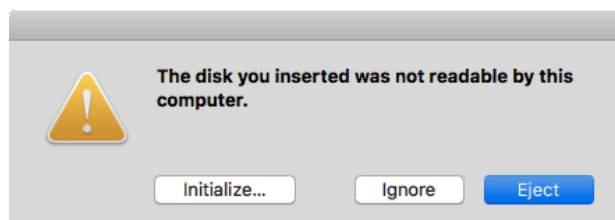


When finished the blue USB LED lights.

Figure 3: The Format USB Drive dialog in Windows OS. ⇨

FOR MAC OS

- At the system popup message (shown below) click Initialize. The Disk Utility dialog displays.



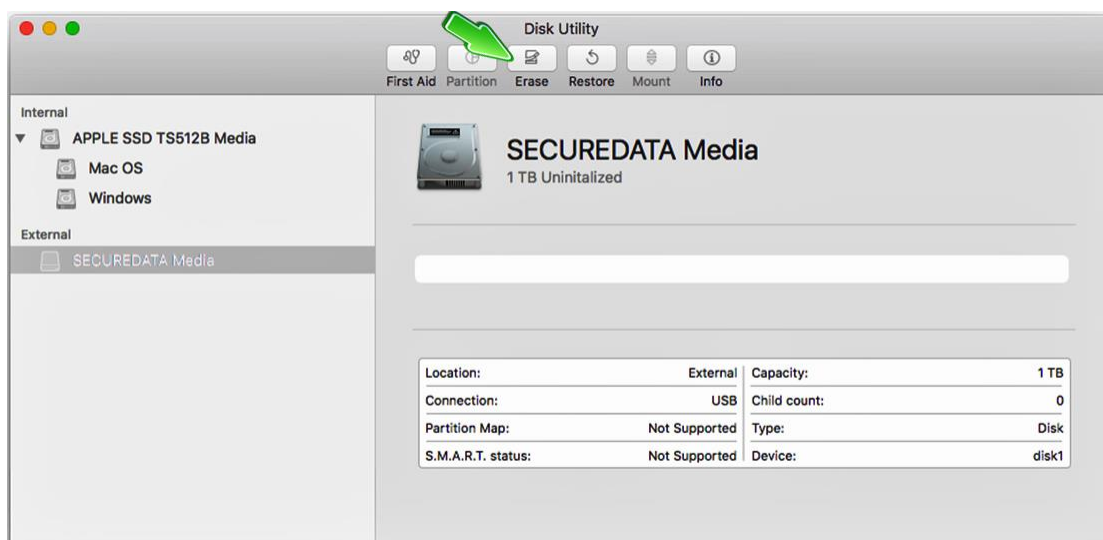
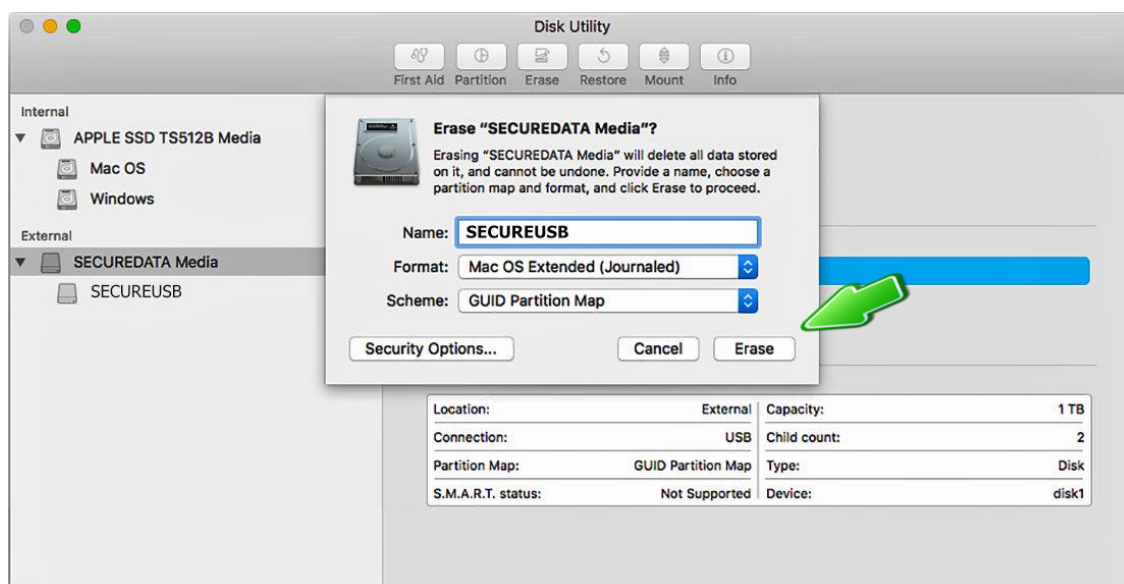


Figure 4: The Disk Utility Dialog.

2. Ensure your USB drive is selected in the list at the left, and then click Erase to open the dialog box.
3. Ensure your USB displays in the Name field and click Erase. The system begins erasing the USB (and renaming it SECUREUSB).



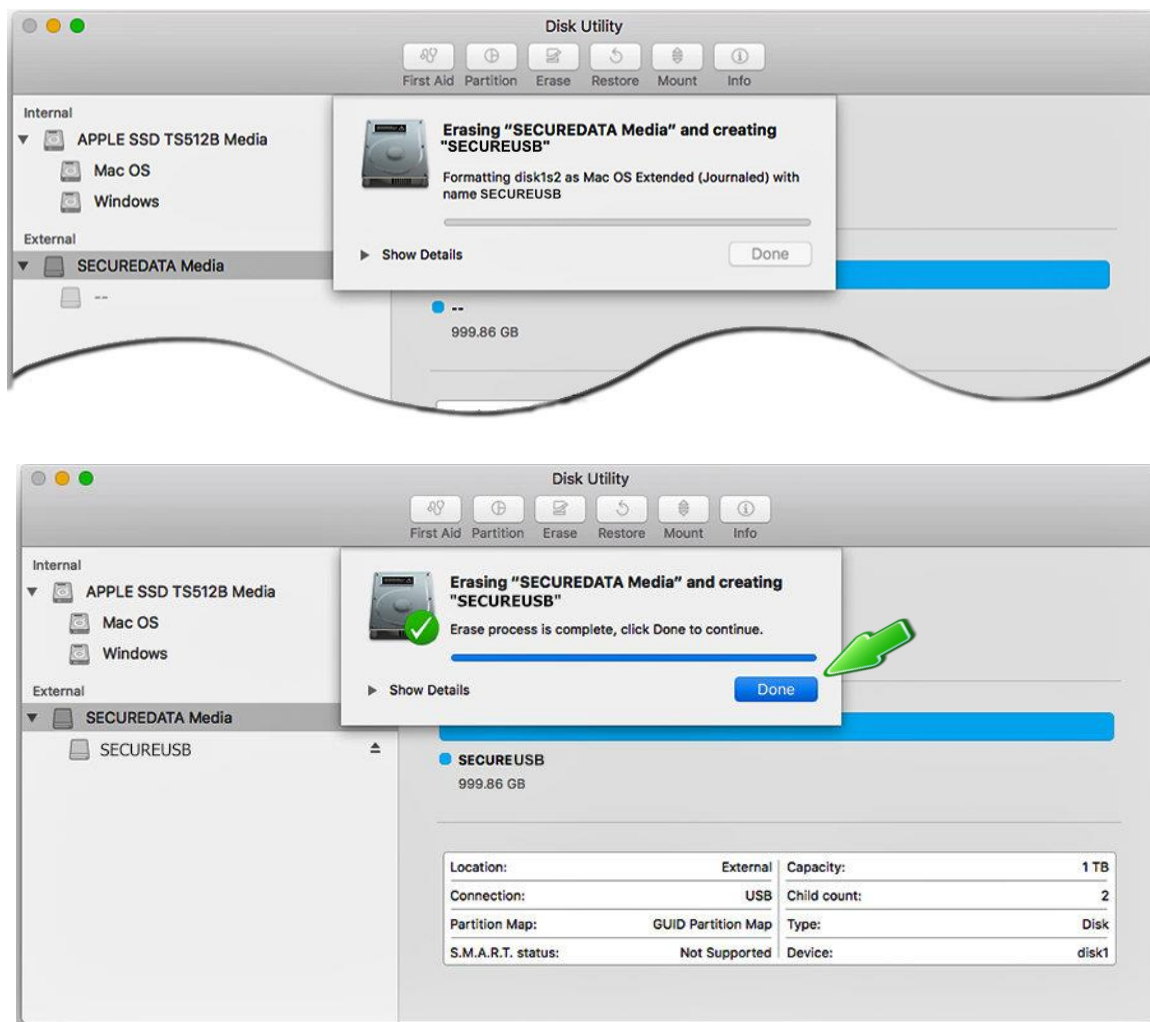


Figure 5: *SECUREUSB* displays under the list of External Drives when done (as well as on the desktop).

4. Click Done in the message dialog when available.
SECUREUSB is now displayed under External in the left column.
5. Close the Disk Utility.

Technical Support

This section covers contact information and information that SecureData, Inc. may require to quickly assist you. Our website is also a great resource.

www.securedrive.com

Contact Information

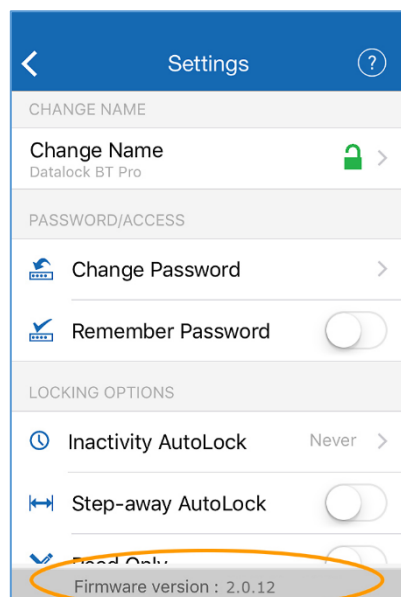
Technical Support email: help@securedrive.com

Phone	Mailing Address
USA: 1-800-875-3230 International: +1-323-944-0822	SecureData, Inc. 3255 Cahuenga Blvd. West #301 Los Angeles, CA 90068-1178

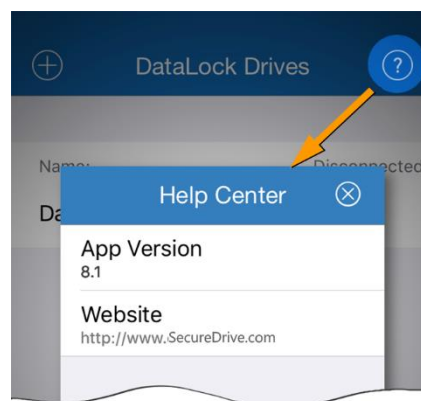
NOTE: Prior to contacting SecureData Inc., please have the following information ready.

- The USB Firmware Version Number (refer to the heading below)
- The Software Version Number (refer to the next below)
- Serial Number (S/N) on the side of the SecureUSB.

FINDING THE VERSION NUMBERS



The SecureUSB *firmware version number* is at the bottom of the Settings window. To display the Settings window, unlock the USB and tap the USB name.



The *App (software) version number* is displayed in a dialog by tapping [?] for Help.

Troubleshooting

- After unlocking the USB, your computer shows that the USB drive is connected (icon displays) but you cannot access the USB data (it doesn't display in Explorer (Windows) or Finder (Mac).
 - The USB is not initialized and needs to be formatted—no data exists. It may have been reset. (A system message should display.) To format, see *Reformatting the SecureUSB* on page 15.
- I can't swipe right to lock the USB in the DataLock App even though the USB name and unlock-icon display.
 - The USB is not authenticated (🔒 does not display). Simply tap the USB name, enter the password and tap Re-Authenticate.
- Tapping the USB name in the app doesn't do anything.
 - If you've used a different USB prior to the current one, that old one may still display in the app. With the USB plugged in, and with Bluetooth on your iOS/Android device turned on, tap the plus sign ⊕ to add your current SecureUSB.
 - If your app says Initializing Encryption and never finishes initializing, the USB may have been initialized with an app on a different device. Remove the USB from the app by sliding the name to the right and tapping Remove, and Remove to confirm. Then add the USB again. Refer to *Adding the SecureUSB to the App (Pairing)* on page 7.

Warranty and RMA Information

(Returned Merchandise Authorization)

TWO YEAR LIMITED WARRANTY

As explained below, SecureData, Inc. offers a two-year limited warranty on the SecureUSB™ against defects in materials and workmanship under normal use. The limited warranty period is effective from the date of purchase either directly from SecureData, Inc. or an authorized reseller.

DISCLAIMER AND TERMS OF WARRANTY

THIS LIMITED WARRANTY BECOMES EFFECTIVE ON THE DATE OF PURCHASE AND MUST BE VERIFIED WITH YOUR SALES RECEIPT OR INVOICE CLEARLY DISPLAYING THE DATE AND SOURCE OF PRODUCT PURCHASE. SECUREDATA, INC. WILL, AT NO ADDITIONAL CHARGE (EXCEPT FOR ANY DELIVERY CHARGES, WHICH REMAIN THE CUSTOMER'S RESPONSIBILITY), REPAIR OR REPLACE DEFECTIVE PARTS WITH NEW PARTS OR SERVICEABLE USED PARTS THAT ARE EQUIVALENT TO NEW IN PERFORMANCE. SECUREDATA, INC. SHALL HAVE SOLE AND COMPLETE DISCRETION ON WHETHER TO USE NEW PARTS OR SERVICEABLE USED PARTS. ALL EXCHANGED PARTS AND PRODUCTS REPLACED UNDER THIS WARRANTY WILL BECOME THE PROPERTY OF SECUREDATA, INC.

THIS WARRANTY DOES NOT EXTEND TO ANY PRODUCT NOT PURCHASED DIRECTLY FROM SECUREDATA, INC. OR AN AUTHORIZED RESELLER OR TO ANY PRODUCT THAT HAS BEEN DAMAGED OR RENDERED DEFECTIVE: 1. AS A RESULT OF ACCIDENT, MISUSE, NEGLIGENCE, ABUSE OR FAILURE AND/OR INABILITY TO FOLLOW THE WRITTEN INSTRUCTIONS PROVIDED IN THIS INSTRUCTION GUIDE; 2. BY THE USE OF PARTS NOT MANUFACTURED OR SOLD BY SECUREDATA, INC.; 3. BY MODIFICATION OF THE PRODUCT; OR 4. AS A RESULT OF SERVICE, ALTERATION OR REPAIR BY ANYONE OTHER THAN SECUREDATA, INC. IN THE

EVENT OF ANY OF THESE SITUATIONS, THIS WARRANTY SHALL BE VOID. THIS WARRANTY DOES NOT COVER NORMAL WEAR AND TEAR.

EXCEPT AS EXPRESSLY PROVIDED ABOVE, NO OTHER WARRANTY, EITHER EXPRESSED OR IMPLIED, INCLUDING ANY WARRANTY OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, HAS BEEN OR WILL BE MADE BY OR ON BEHALF OF SECUREDATA, INC. OR BY OPERATION OF LAW WITH RESPECT TO THE PRODUCT OR ITS INSTALLATION, USE, OPERATION, REPLACEMENT OR REPAIR.

LIMITATION OF LIABILITY

SECUREDATA, INC. SHALL NOT BE LIABLE BY VIRTUE OF ANY WARRANTY, PROMISE OR OTHERWISE, FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR PUNITIVE OR MULTIPLE DAMAGES, INCLUDING WITHOUT LIMITATION ANY DAMAGES RESULTING FROM ANY LOSS OF DATA RESULTING FROM THE USE OR OPERATION OF THE PRODUCT, LOSS OF USE, LOSS OF BUSINESS, LOSS OF REVENUE, OR LOSS OF PROFITS, WHETHER OR NOT SECUREDATA, INC. WAS APPRISED OF THE POSSIBILITY OF SUCH DAMAGES. SECUREDATA, INC.'S LIABILITY SHALL BE LIMITED TO THE ACTUAL COST OF THE PRODUCT OR \$1,000.00, WHICHEVER IS GREATER. THE FOREGOING LIMITATION OF LIABILITY SHALL APPLY REGARDLESS OF THE CAUSE OF ACTION UNDER WHICH SUCH DAMAGES ARE SOUGHT.

Copyright © 2018 SecureData, Inc.. All rights reserved.

SecureUSB™ and SecureData™ are trademarks of SecureData, Inc.

Windows® is a registered trademark of Microsoft Corporation.

DataLock® is a registered trademark of ClevX, LLC.

All other trademarks and copyrights referred to are the property of their respective owners.

Distribution of the work or derivative work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

DOCUMENTATION IS PROVIDED AS IS AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

SecureUSB is developed and manufactured by SecureData, Inc. and is based on technology licensed from ClevX, LLC.

