

# SECURE USB

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 9

Locking without Unplugging from the Computer 9

## **Setting Options 10**

Entering Settings Mode 11

Password Options 11

Access Options and Locking Options 20

## **Managing the SecureUSB BT 29**

Removing a SecureUSB BT 30

Brute Force Hacking Detection 30

Resetting (Deleting) the SecureUSB BT 30

Reformatting the SecureUSB BT 31

## **Technical Support 35**

Contact Information 35

Troubleshooting 36

Warranty and RMA Information 36

# 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 USB 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 Management 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 USB 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 USB (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

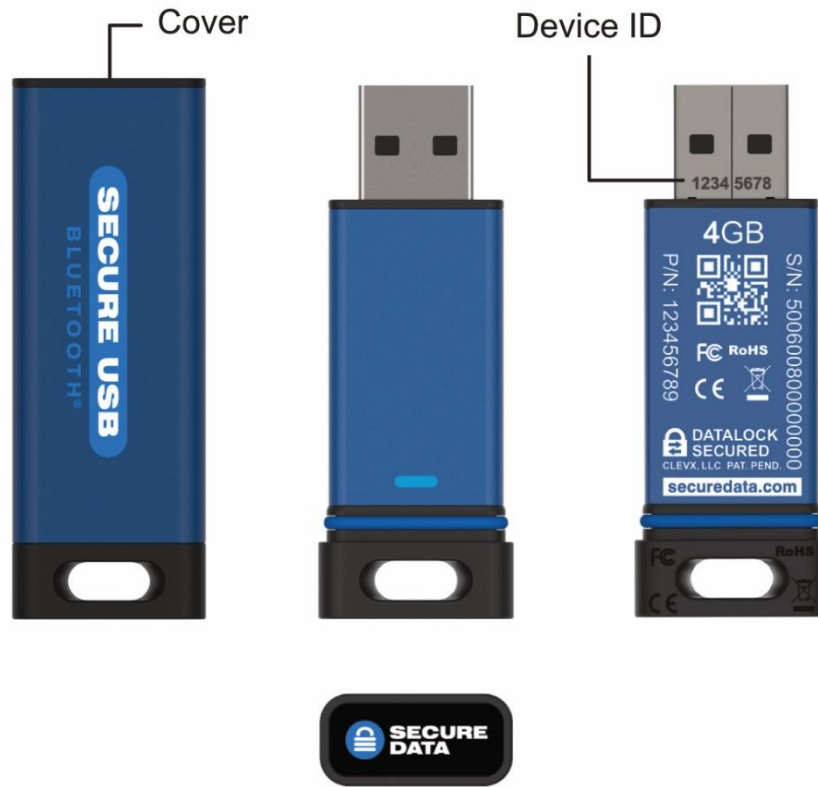







Figure 1: SecureUSB BT layout showing the LED, Device ID number, Serial Number and Part Number
















## Icon Interpretations

### ON THE SECUREUSB

LEDs on the USB are represented here by colored icons.

LED	Meaning
 (one blink)	Plugged into computer; LED test
 = <b>Red</b> solid	Powered and locked <i>but not</i> BT-connected
 = <b>Red</b> blinking	Powered and locked <i>and</i> BT-connected via the App
 <b>Blue</b> solid  <b>Blue</b> 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
	Touch ID
	Face ID
	App will remember the password
	Inactivity AutoLock
	Step-away AutoLock
	Read-Only Mode
	Enable Apple Watch®
	Reset the USB (erase all data and settings)
	Password Recovery
	Remote Wipe

## Installing the Accompanying App

The app, named **DataLock**, for your new USB 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 USB 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:

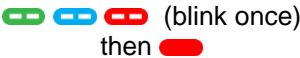





- be 7-15 characters in length, letters or numbers. Special characters okay.
- not contain only repetitive numbers or letters, e.g. (3333333) or (cccccc)
- not contain only consecutive numbers or letters, e.g. (1234567), (78901234), (7654321), (abcdefg)



## 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  if you don't see your new Drive's S/N in the list.		
4. Tap the Drive's name that appears.		

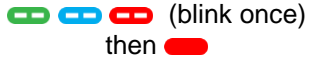






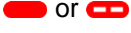





<p>5. Tap <b>Continue</b> and follow the app instructions.</p>		
--	--	---

## Unlocking the SecureUSB



**CAUTION:** Possible loss of data. After ten failed attempts to unlock the USB, the password, all data, and the formatting will be deleted. Refer to *Brute Force Hacking Detection* on page 30.

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

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



<sup>1</sup> 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 36.


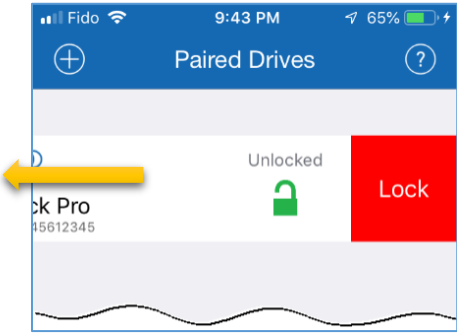


## Disconnecting the SecureUSB from Your Computer



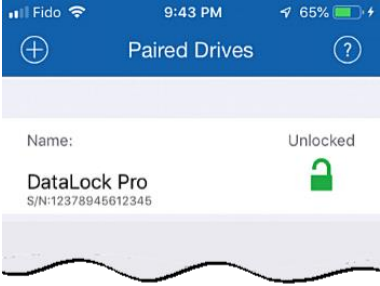

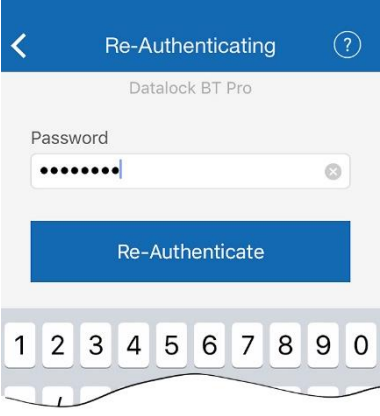


Generally, you can just unplug the USB Drive—it will lock automatically.

**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
<p><i>A. If the App is still BT-connected to the USB and unlocked:</i></p> <p>1. In the app, <b>swipe</b> the desired USB name to the <b>left</b>. If it does not swipe left, it needs to be authenticated. See B below.</p>		
<p>2. Tap <b>Lock</b>. The USB locks.</p>		

<p><b>B.</b> If the App is still BT-connected to the USB but not Authenticated (this icon  does not appear):</p> <ol style="list-style-type: none"> <li>In the app, tap the desired USB name. NOTE: If <i>Remember Password</i> is on, skip the next step.</li> </ol>		
<ol style="list-style-type: none"> <li>Type in the password and tap Re-Authenticate.</li> </ol>		
<ol style="list-style-type: none"> <li>Lock the USB—refer to the steps in part A above.</li> </ol>		

## 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.

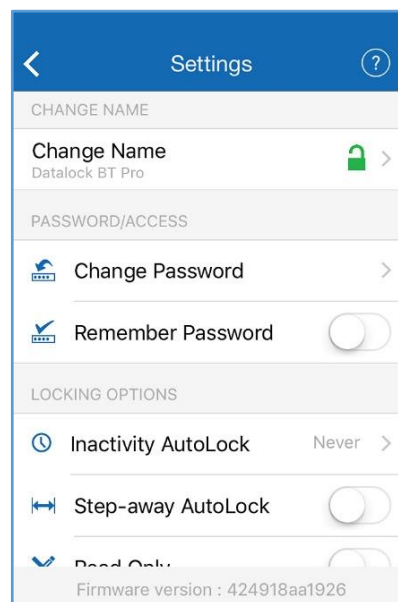


Figure 2: The Settings Menu, partial view. ⇨

## Password Options

### CHANGING THE PASSWORD

Follow these steps to change an existing USB BT password.

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




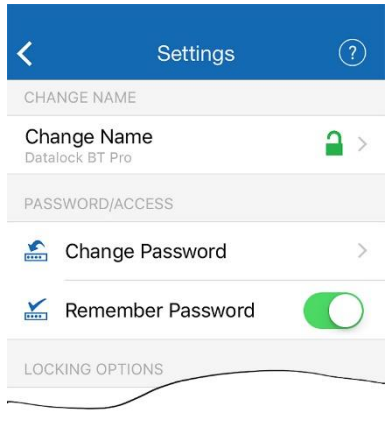


**NOTE:** If a mistake was made while defining a new password or the procedure was not completed, the USB will retain the old password.

### 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 USB. 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.

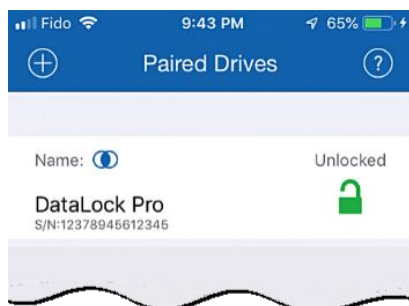
Remember Password	LED	App
1. With the USB unlocked and authenticated (logged in), tap the desired USB name.		
2. Tap the <b>Remember Password</b> button to the ON position (green).		
3. Tap <b>Yes</b> to confirm.		

## ENABLING THE PASSWORD RECOVERY FEATURE

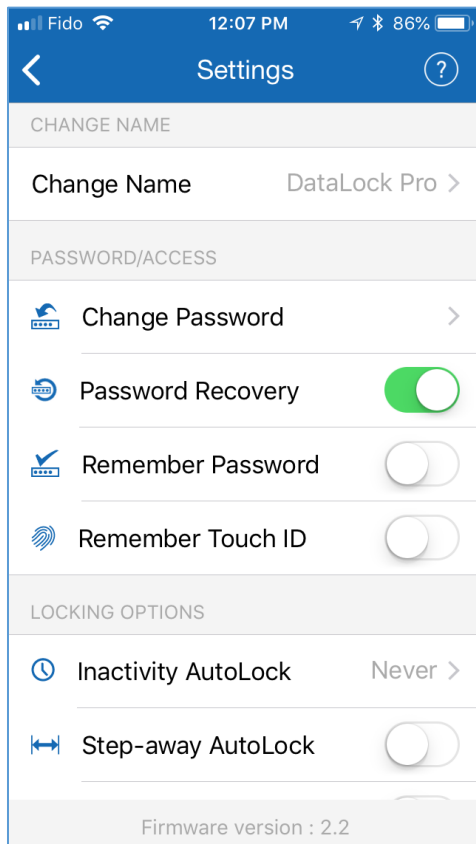
The Password Recovery feature can send a recovery code to your registered mobile number as a text message.

There are two places where Password Recovery can be enabled:

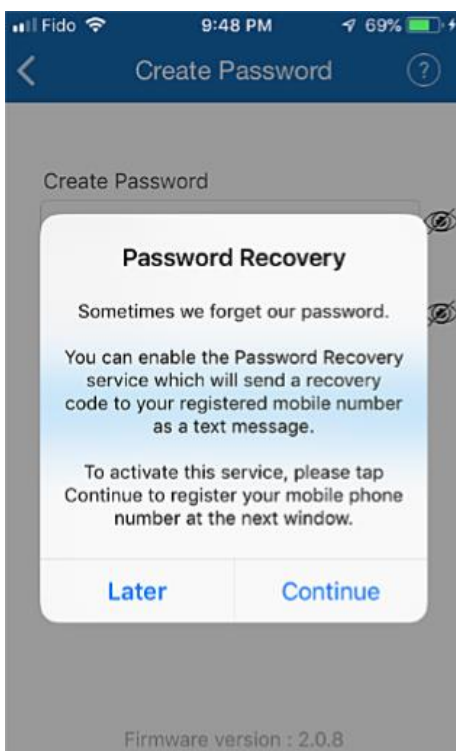
- After creating password (refer to [Changing the Password](#) on page 11)
  - From the Settings menu
1. Make sure the Drive is unlocked and authorized (logged-in) via the DataLock app.
  2. Tap the Drive name to access Settings.



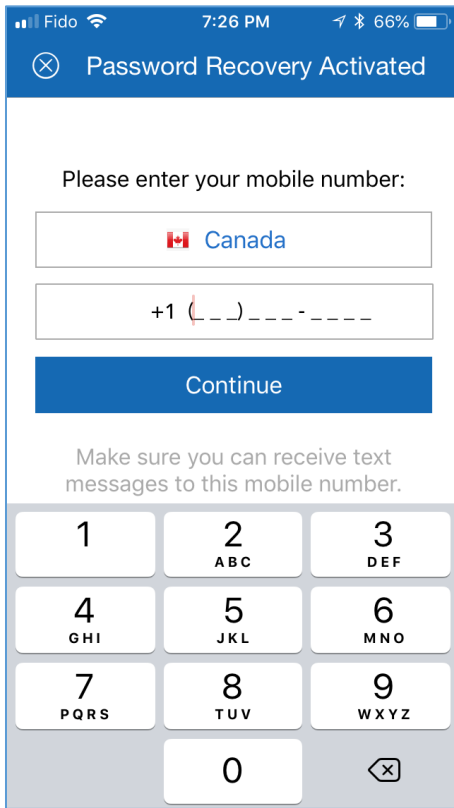
3. Tap the Password Recovery button (green is ON).



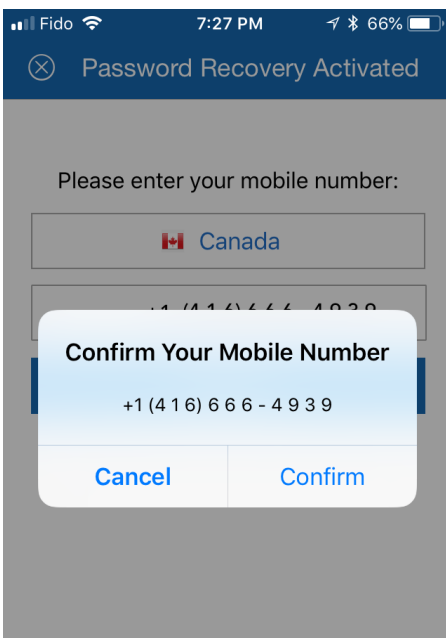
4. Read the Password Recovery message and tap Continue.



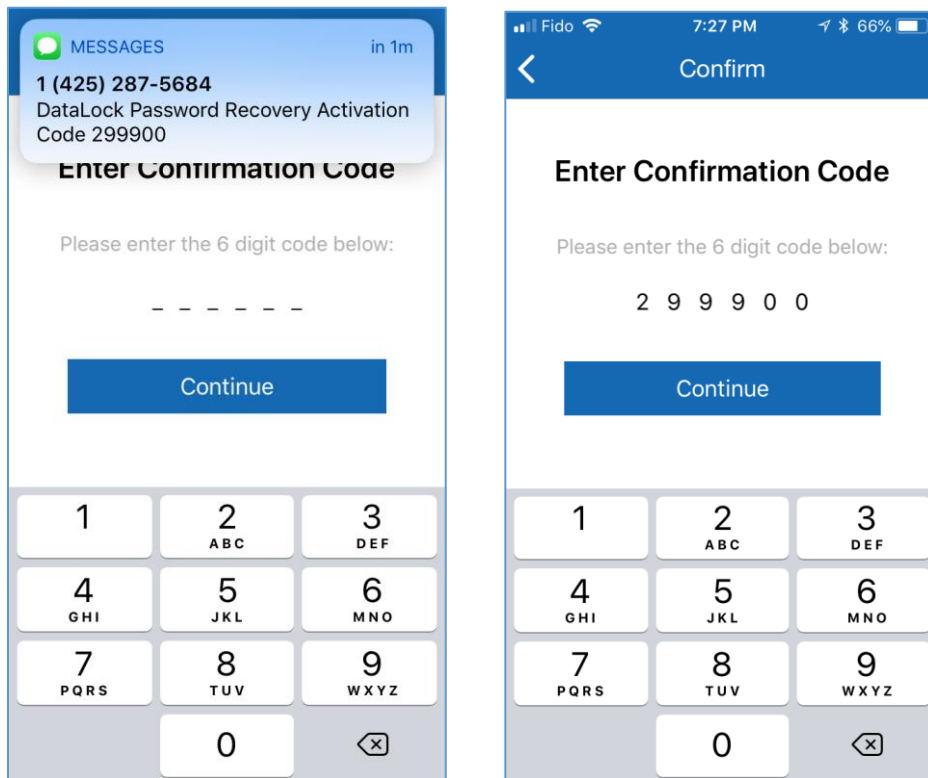
5. Enter your mobile phone number.



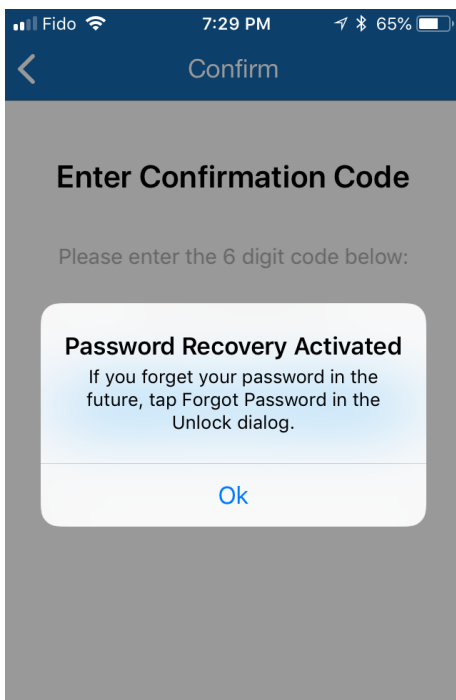
- 6. Tap Continue.
- 7. Confirm your mobile phone number.



- Wait for a text message and enter the confirmation code received. (This is an example only.)



You should get a confirmation that Password Recovery is Activated.



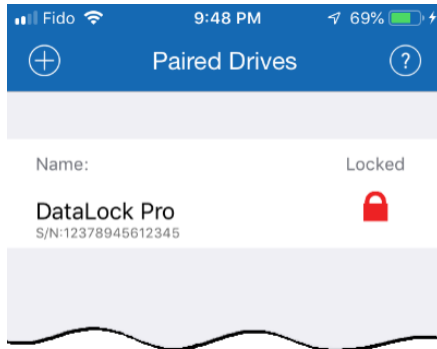
To recover your password, see the next heading.

## RECOVERING A FORGOTTEN PASSWORD

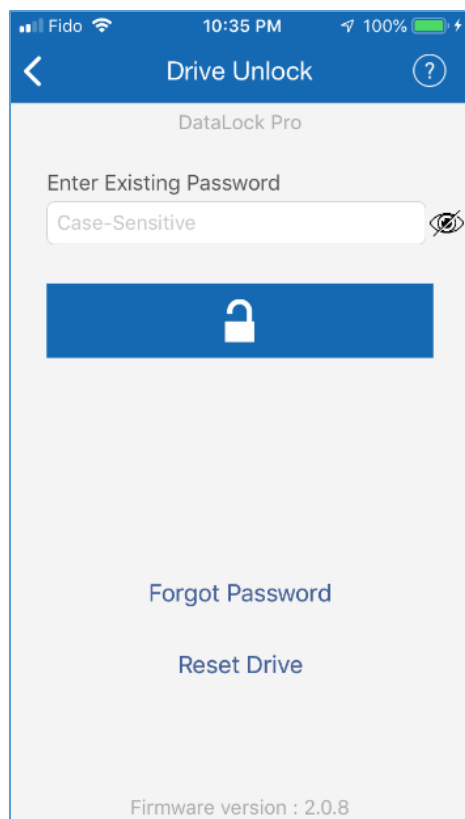
**Part A:** If you have previously enabled the Password Recovery feature, follow these steps, otherwise skip down to part B.

NOTE: To receive password recovery code by text message you must be able to receive text messages to the phone number from where Password Recovery was enabled.

1. Tap the Drive name.

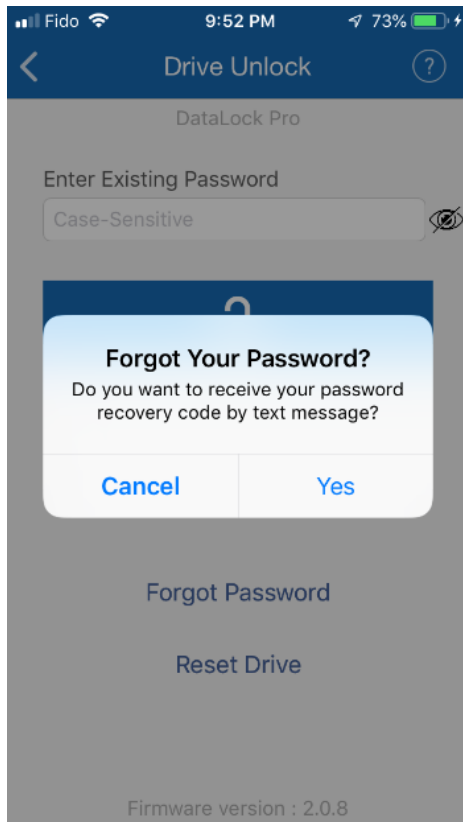


2. Tap Forgot Password.

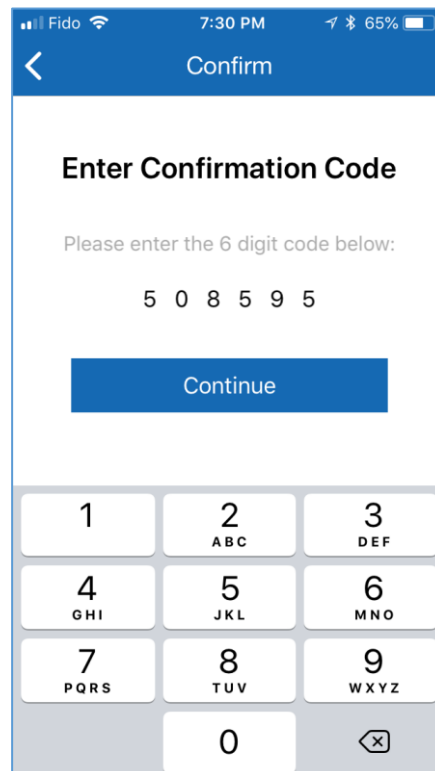
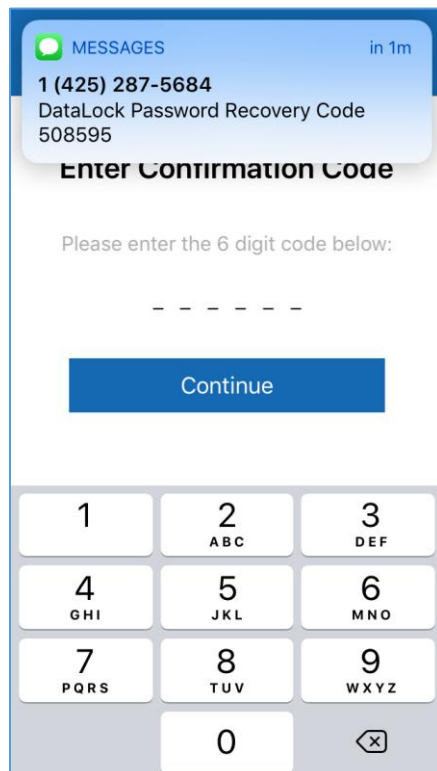




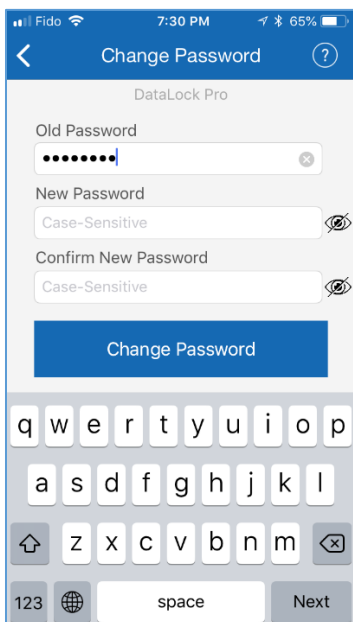
3. Tap Yes on the Forgot Your Password dialog.



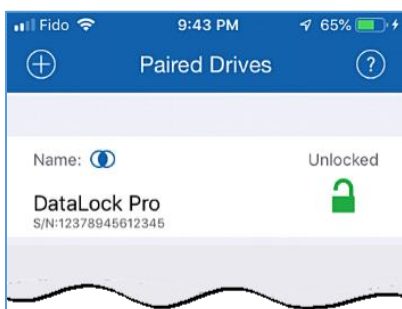
4. Wait for the text message and then enter received confirmation code.



- If entered correctly, you should see a Change Password dialog. Just create a new password.



Now your Drive should be unlocked.



#### RECOVERING A FORGOTTEN PASSWORD

**Part B:** If you previously did not enable Password Recovery and forgot your password, resetting the Drive is the only way to make it usable again. Although your data will be erased from the Drive, this ensures that it is not breached or compromised. The DataLock BT Device ID is printed on the Drive to allow resetting the Drive.

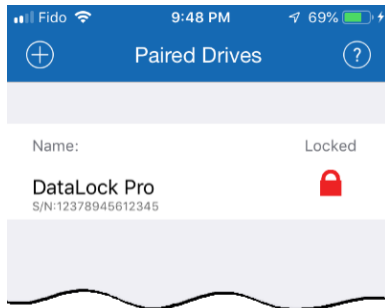


**CAUTION:** Data will be deleted. After performing a Drive RESET, it reverts to the default state: unformatted AND ALL USER DATA AND SETTINGS WILL BE DELETED. Also, all settings (such as drive name, password, step-away, inactivity timer) will be set to default values.

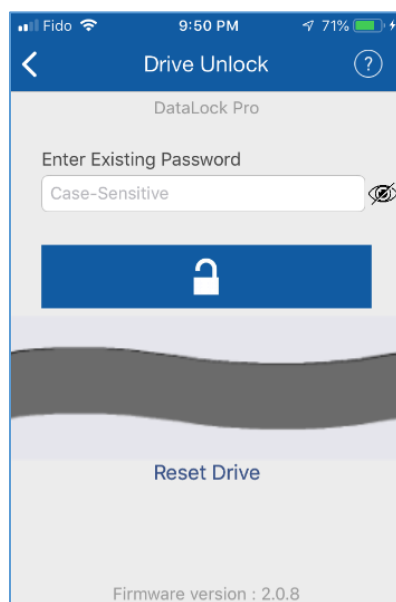
You will need the Serial Number of the USB.

Make sure the Drive is authorized (logged-in) via the app.

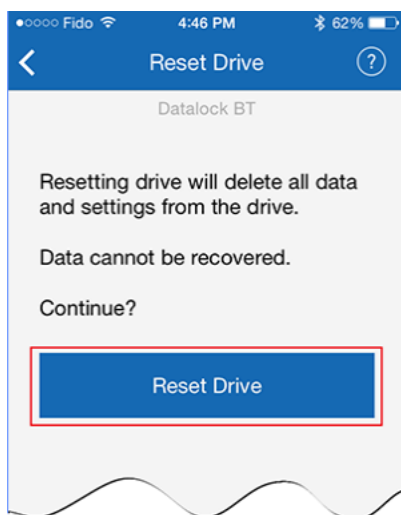
1. Tap the Drive name.



2. Tap Reset Drive.

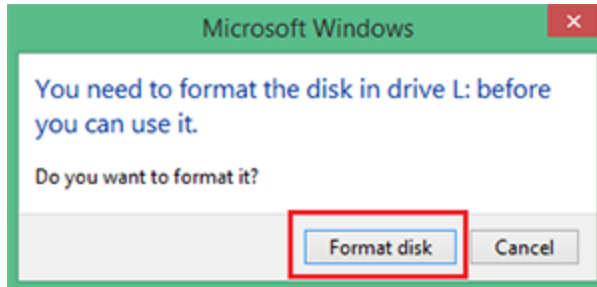


3. Read the warning and tap Reset Drive.

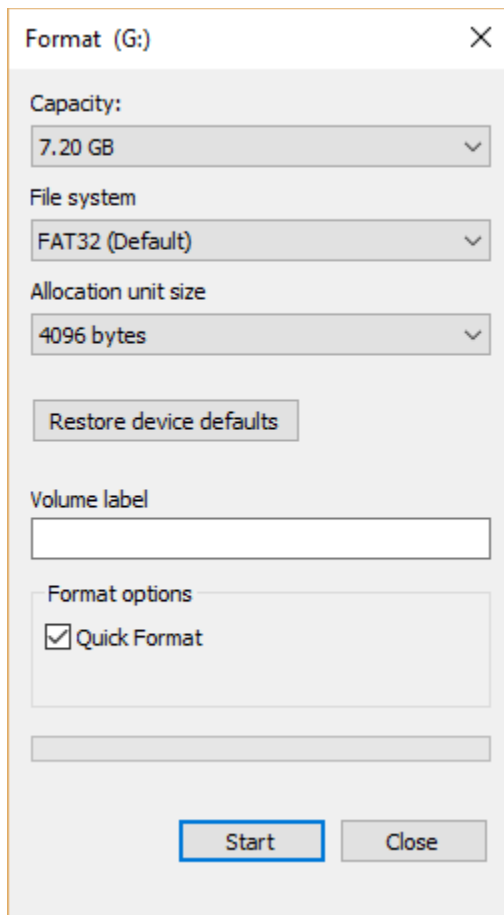


The Drive reverts back to the default state. The default state is blank (has no password) and locked. Please see [Changing the Password](#) to initialize your Drive.

If, or when, the reset (unformatted) Drive is unlocked, this message appears:



## FORMAT SETTINGS




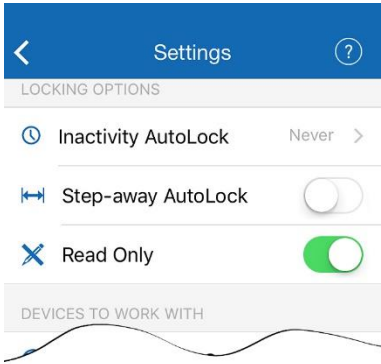




## Access Options and Locking Options

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 <b>USB name</b> .		
2. Tap the <b>Read Only</b> button to the ON position (green).		
3. Tap <b>Lock</b> 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 <b>USB name</b> .		
2. Tap the <b>Read Only</b> button to the OFF position (not green).		
3. Tap <b>Lock</b> 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 USB 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 <b>USB name</b> .		
2. Tap Inactivity Lock.		
3. Tap the desired inactivity <b>interval</b> 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




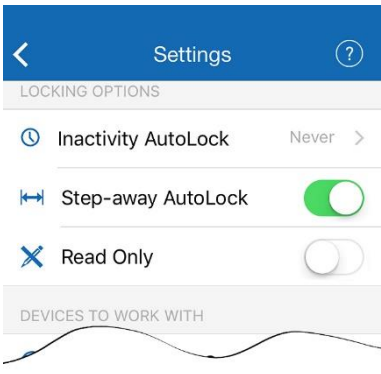


Disable the Inactivity Lock	LED	App
1. With the USB unlocked and authenticated, tap the desired USB name.		
2. Tap Inactivity Lock.		
3. Tap Never.		A checkmark displays adjacent to your selection. ✓

The Inactivity Lock is now disabled.

## SETTING THE STEP-AWAY AUTOLOCK ON AND OFF

The Step-away AutoLock will lock the USB (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 <b>USB name</b> .		
2. Tap the <b>Step-away AutoLock</b> button to the ON position (green).		
3. Tap <b>Yes</b> to confirm.		

The Step-away AutoLock is now on.

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

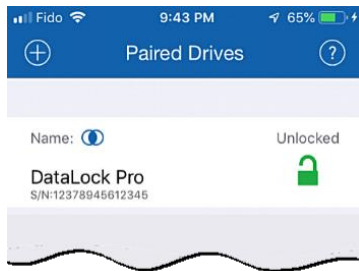
## SET TO REMEMBER TOUCH ID (FACE ID) FOR SOME IPHONES

Requirement: iPhone 5S or newer.

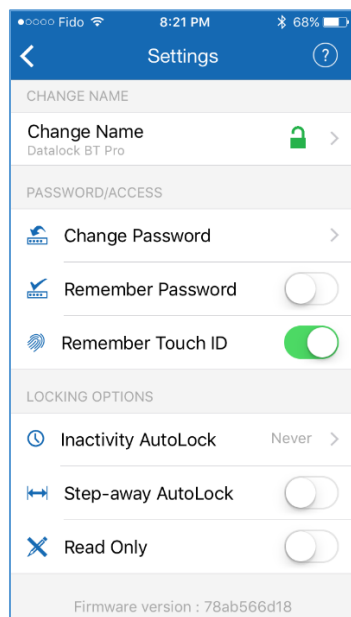
To use the fingerprint feature of your iPhone to unlock the Drive, enable the Remember Touch ID setting.

1. Make sure the Drive is unlocked and authorized (logged-in) via the app.

2. Tap the Drive name to access Settings.



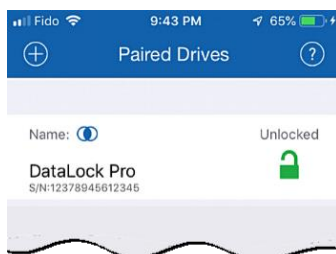
3. Tap the Remember Touch ID button (green is ON).



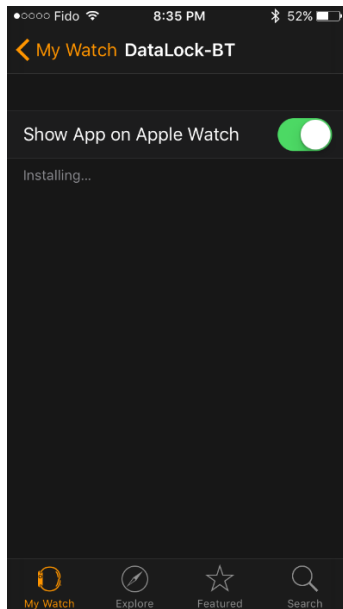
## UNLOCK THE DRIVE WITH AN APPLE WATCH

You can unlock your Drive with an Apple Watch® if used with iPhone 5S, 6, 6 Plus, 6S, or 6S Plus.

1. Make sure the Drive is unlocked and authorized (logged-in) via the app.
2. Tap the Drive name to access Settings.

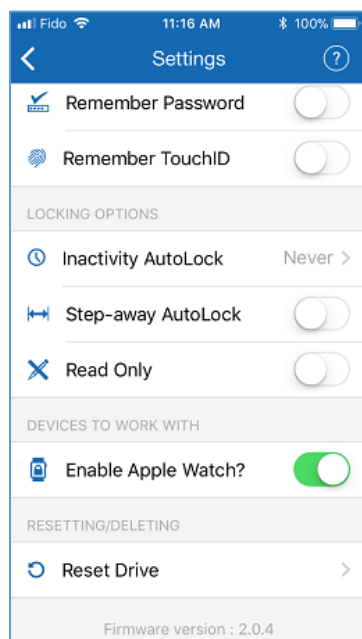


3. Make sure DataLock app is installed on your Apple Watch.



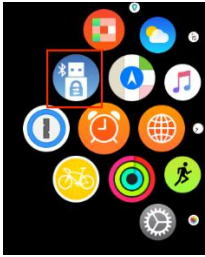
4. Turn ON Enable Apple Watch.

NOTE: Your Drive's password must contain numbers only to unlock with Apple Watch. If your current password contains letters then you will be redirected to the Change Password dialog.

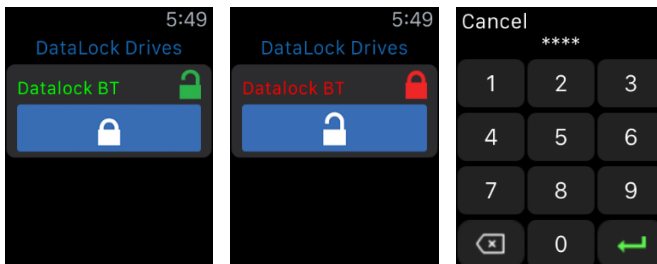


5. Start DataLock app on your Apple Watch.





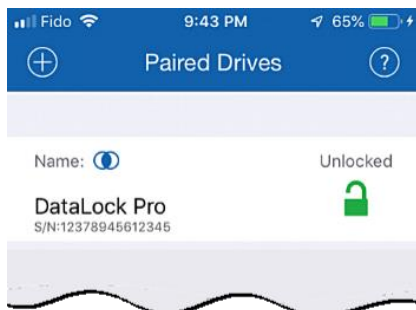
You should be able to lock and unlock your Drive from your Apple Watch.



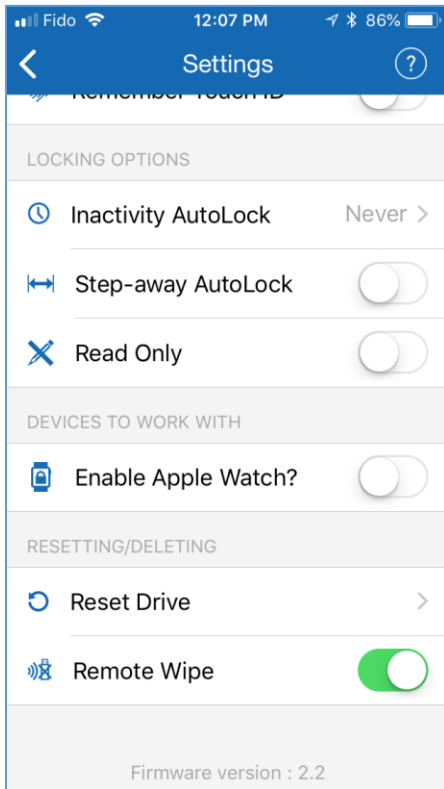
## ENABLING REMOTE WIPE

To enhance protection for your Drive in case it becomes lost, you can enable the Remote Wipe feature that will allow you to Remote Wipe (Reset) your lost Drive.

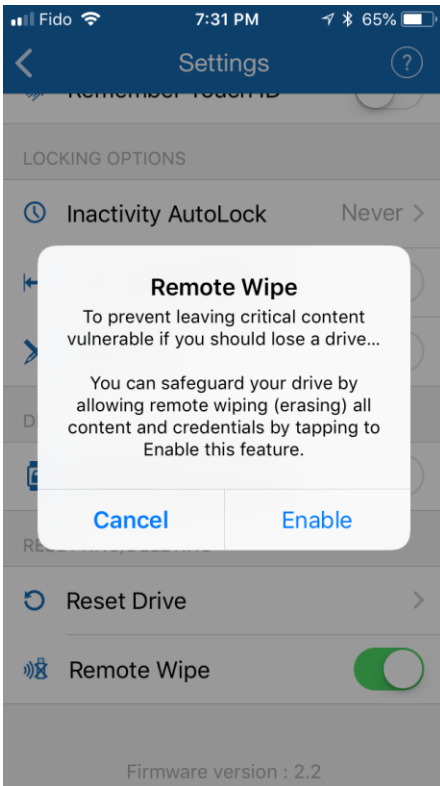
1. Make sure the Drive is unlocked and authorized (logged-in) via the app.
2. Tap the Drive name to access Settings.



3. Tap the Remote Wipe button (green is ON).

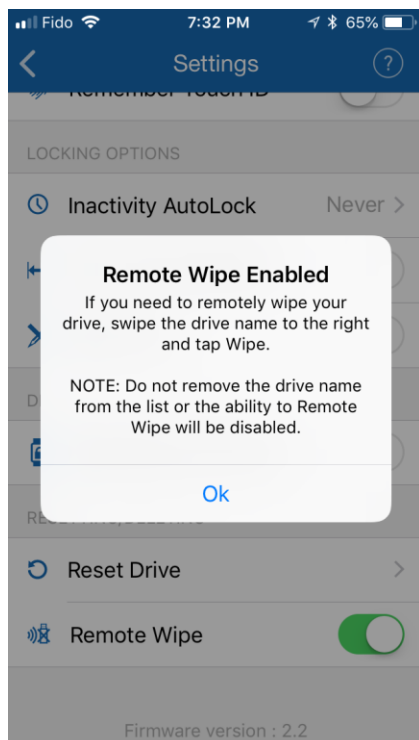


4. Tap Enable on the Remote Wipe dialog.



You should see a confirmation that Remote Wipe is enabled.

NOTE: The Remote Wipe feature is only enabled, it is not turned on. To turn it on, see the next heading.



## ACTIVATING REMOTE WIPE IF YOU LOST YOUR USB

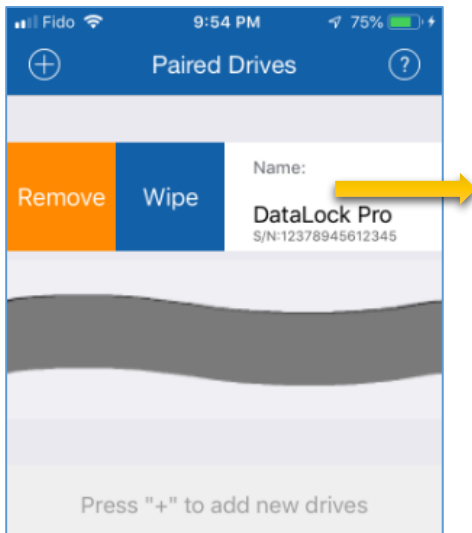
The Remote Wipe option must have been enabled prior to losing the Drive. (Ref. [Enabling Remote Wipe](#) above.) If it has not been enabled, rest assured that your data on the Drive cannot be accessed by whomever finds it.

Follow this Remote Wipe activation procedure:

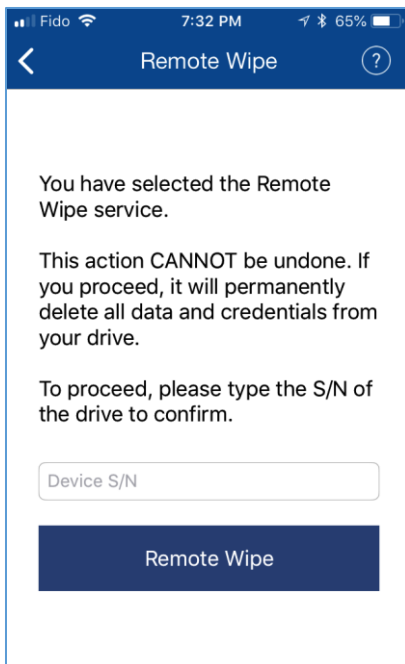


**CAUTION:** Possible inadvertent loss of data. Once activated, there is no way to disable it. The next time the Drive is discovered by the DataLock app, it will be immediately wiped (reset) even if it is you who finds and attempts to use it. Please be sure you are ready to commit.

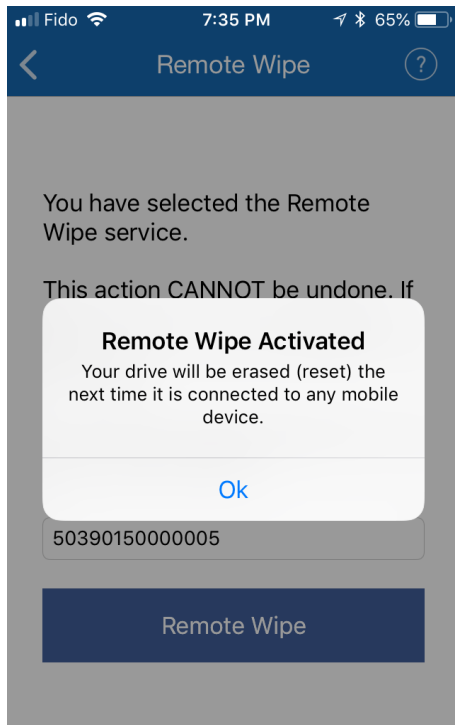
1. In the app, copy the Drive's Serial Number which is displayed below the Drive's name.
2. Swipe the Drive's name to the right and tap Wipe.



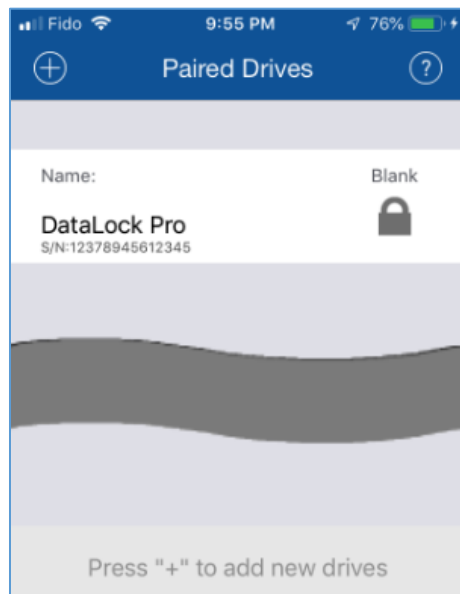
3. As a validation, you must enter your Drive's Serial Number and tap Remote Wipe.



4. You should see a confirmation that Remote Wipe is Activated. Tap OK.




The next time the Drive is discovered by any mobile device with the DataLock app installed, it will be immediately wiped (reset).



## Managing the SecureUSB BT





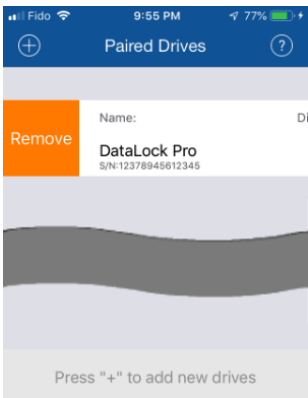




The following headings discuss important, though less common, actions for managing your USB.

## 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 USB 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 <b>swipe right</b> . (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 31. The data is not recoverable.




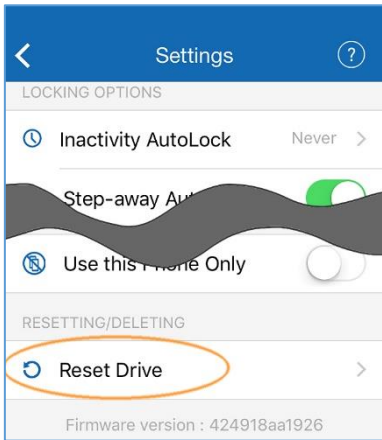







## Resetting (Deleting) the SecureUSB BT



**CAUTION:** Resetting the USB 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 31.

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 31.

The Device ID is required.








Reset the USB	LED	App
1. With the USB unlocked and authenticated (logged in), tap the desired <b>USB name</b> .		
2. Tap Reset Drive.		
3. Tap <b>Reset Drive</b> to continue.		
4. Tap <b>Continue</b> and, <ol style="list-style-type: none"> <li>unplug the USB</li> <li>write down the ID that's on the connector</li> <li>re-insert the USB </li> </ol>		
5. Tap <b>Reset</b> 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 USB, do the following:

Create a Password	LED	App
1. <b>Insert</b> the USB Drive if it is not already.		
2. Tap the desired <b>USB name</b> .		
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

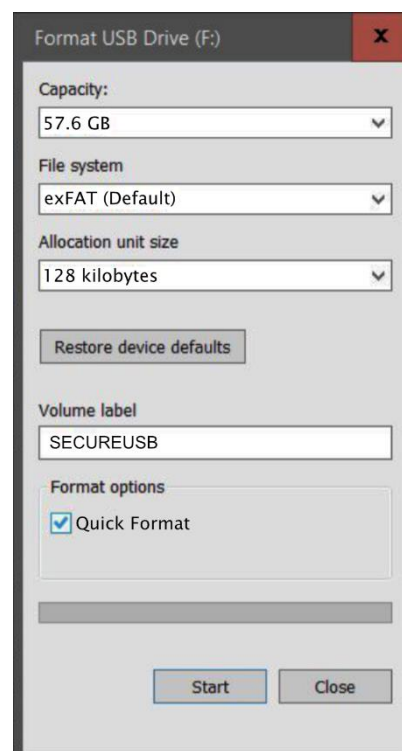
1. At the system popup message (shown below) click Format Disk.



2. If the settings are okay, click Start. Generally the default values are good. Use FAT32 or exFAT for the file system. See Figure 3: .
3. Click OK to the warning about erasure.
4. Click OK to complete.
5. 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

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

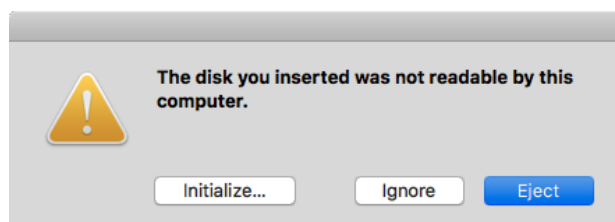
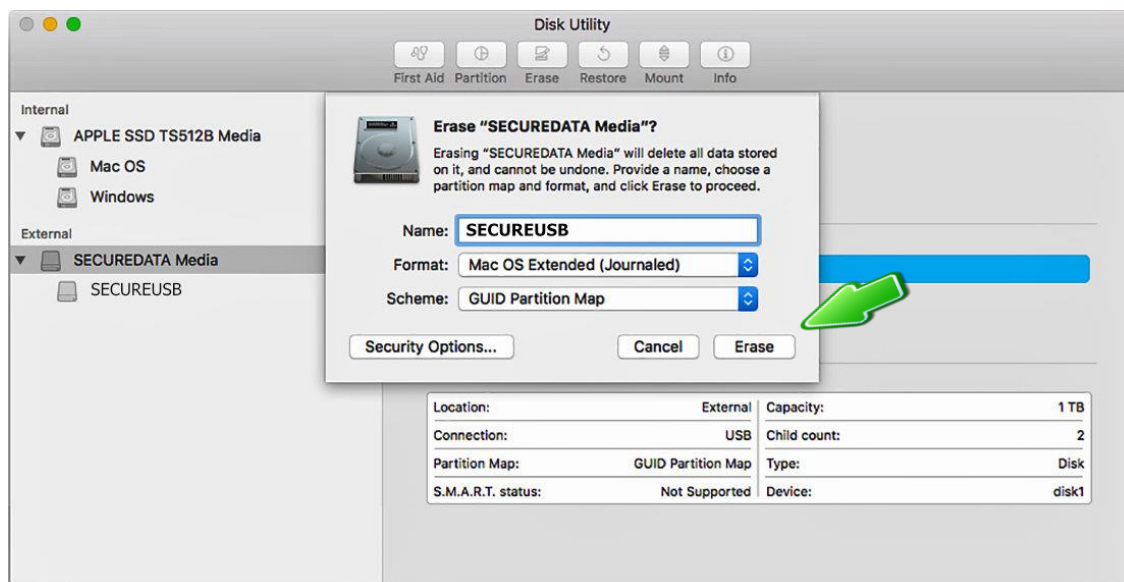






Figure 4: The Disk Utility Dialog.

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).



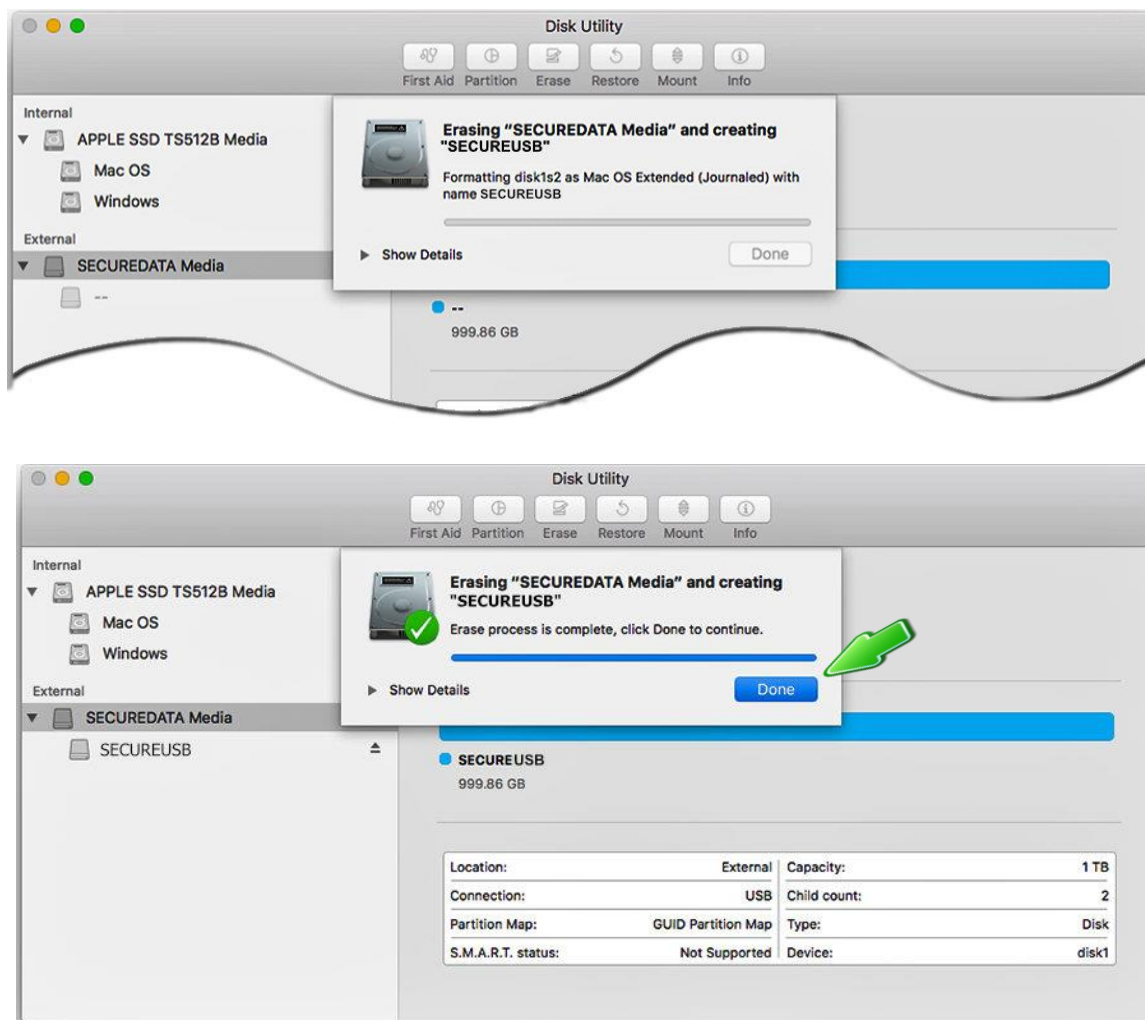


Figure 5: *SECUREUSB* displays under the list of External Drives when done (as well as on the desktop).

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](http://www.securedrive.com)

## Contact Information

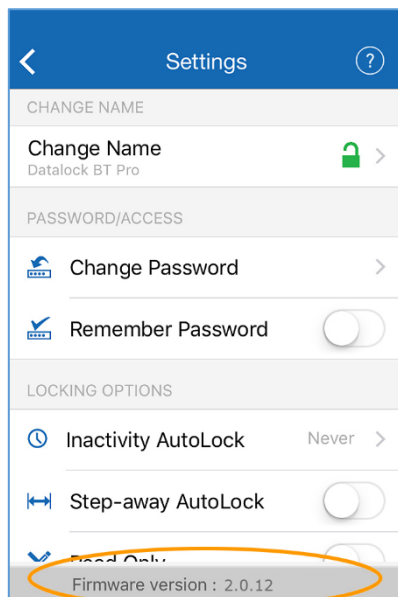
Technical Support email: [help@securedrive.com](mailto:help@securedrive.com)

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

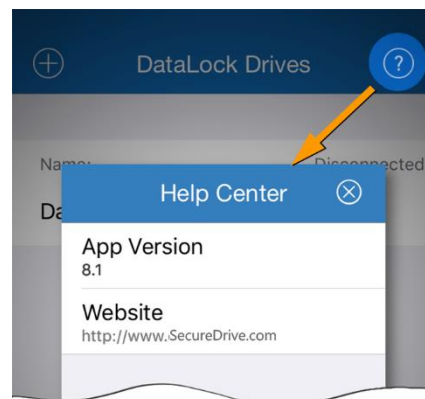
NOTE: Prior to contacting SecureData Inc., please have the following information ready.

- 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 USB.

## 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 31.
- 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 USB.
  - 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.
- I tried to reprovision my Drive, but it doesn't seem to be working.
  - You may not have the latest version of the app, or a late enough version of the iOS.

## 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 © 2019 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.

