SecureUSB® BT
USER MANUAL

Hardware Encrypted
USB Flash Drive

SECURE
DATA

TABLE OF CONTENTS

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 USB. This Bluetooth® capable model uses an application via wireless user-authentication on a smartphone—iOS and Android. (Apple iOS includes Apple 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 SecureData Lock 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 USB must be connected to a computer for use. It works on Windows, Mac, Android, Linux, or Chrome operating system, or any host such as an embedded system. The computer/host must have a USB 2.0 port, minimum.

Included: • 1 USB • 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.

Precaution

⚠ Do not expose the USB to water or moisture. USB is IP57 rated which, with the protective sleeve on, is dust protected and water resistant up to 1 meter (approx. 3 feet) for 30 minutes.

⚠ Resetting the USB will delete all stored data as well as all passwords.

⚠ Forgetting your password will render the USB 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.

Cautions

Changes or modifications not expressly approved by the party responsible could void the user's authority to operate this device.The normal function of the product may be disturbed by strong Electro Magnetic Interference. If so, simply reset the product to resume normal operation by following the instruction manual. In case the function could not resume, please use the product in other 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.

RF Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

12.26.2019

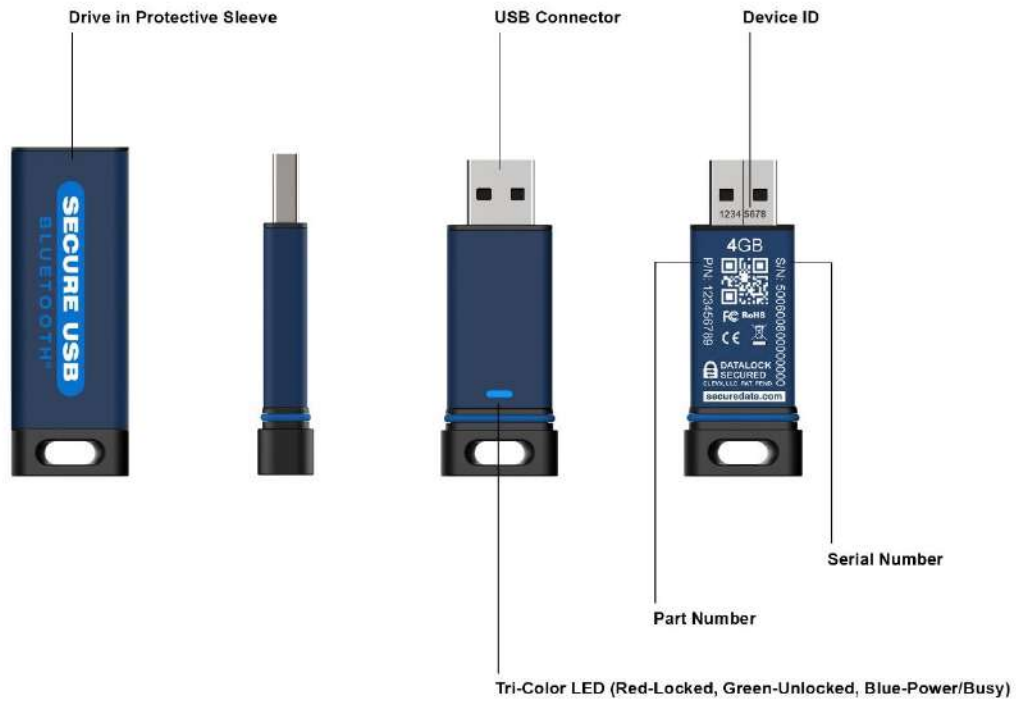# SecureUSB BT Features

Drive in Protective Sleeve

USB Connector

Device ID

4GB
P/N: 123456789
S/N: 500600800000000

Serial Number

Part Number

Tri-Color LED (Red-Locked, Green-Unlocked, Blue-Power/Busy)

Figure 1.1: SecureUSB BT layout showing LEDs, Device ID number, Serial number, and Part number

Icon Interpretations

On the USB:

LED	Meaning
(one blink)	Plugged into computer; LED test
= Red solid	Powered and locked *but not* BT-connected
= Red blinking	Powered and locked *and* BT-connected
= 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
🔒	USB is blank such as when not formatted
◑	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.
	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 SecureData Lock App

The app, named SecureData Lock User, 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 SecureData Lock User 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 are okay.
- not contain only repetitive numbers or letters, e.g. (3333333) or (ccccccc)
- not contain only consecutive numbers or letters, e.g. (1234567), (7654321), (abcdefg)

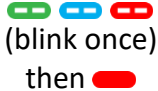# Procedural Conventions

All actions require the drive to be connected to a computer. 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 USB to the App (Pairing)

The eight-digit Device ID is required; is it printed on the USB connector.
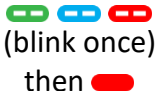
To add the USB, follow these steps:

Adding the USB	LED
1. Plug the USB into a computer.	🟢 🔵 🔴 (blink once) then 🔴
2. Start the **SecureData Lock App** on your device. **Note**: Ensure your device is BT enabled.	🔴
3. If you have no paired drives, the new drive will automatically appear. If you have existing paired drives, tap ⊕.	🔴
4. Tap the **Drive name**.	🔴
5. Enter the **Device ID**.	🔴

Unlocking the USB

⚠️ **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 19**. Until the USB is unlocked it does not display in your computer's File Manager (Explorer or Finder).

To unlock the USB, follow these steps:

Unlock the USB	LED	APP
1. Connect the USB to a computer.	🟢 🔵 🔴 (blink once) then 🔴	-
2. Start the **SecureData Lock App** on your device.	🔴	-
3. After it initializes, tap the **USB name**.	🔴	🔒
4. Type in the password and tap **Unlock**.	🔵	🔓
Unlock the USB – After waking up from sleep	**LED**	**APP**
1. Open the app.	🔴 or 🔴	🔒
2. After it initializes, tap the **USB name**.	🔴	-
3. Type in the password.	🔴	-
4. Tap Unlock.	🔵	🔓

Note: The password on new USBs is 11223344. We strongly suggest changing the password after unlocking. Refer to *Changing the Password* on **page 10**. If the USB still doesn't appear in your computer's file manager, refer to *Troubleshooting* on **page 24**.
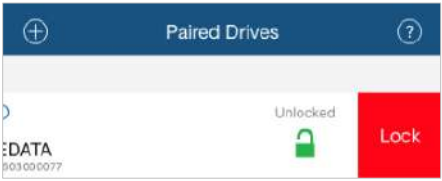
Disconnecting the USB from Your Computer

Generally, you can just unplug the USB, 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 from the computer. 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.

A: Lock without Unplugging – USB is paired with App and unlocked	LED	APP
1. In the app, swipe the desired **USB name** to the left. **Note:** If it does not swipe left, it needs to be authenticated. See B below.		
2. Tap **Lock**. The USB locks.		
B: Lock without Unplugging – App is connected to USB but not authenticated. ⦿ **Does not appear.**	LED	APP
1. In the app, tap the desired **USB name**. **Note:** If Remember Password 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: All actions require the USB to be connected to a computer. 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 different settings available like 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.

The image is an example of settings that may appear. Depending on the type of biometric settings available on the phone, these settings may vary.

The below sub-sections describe how to utilize these settings. If you have any questions, contact Technical Support.
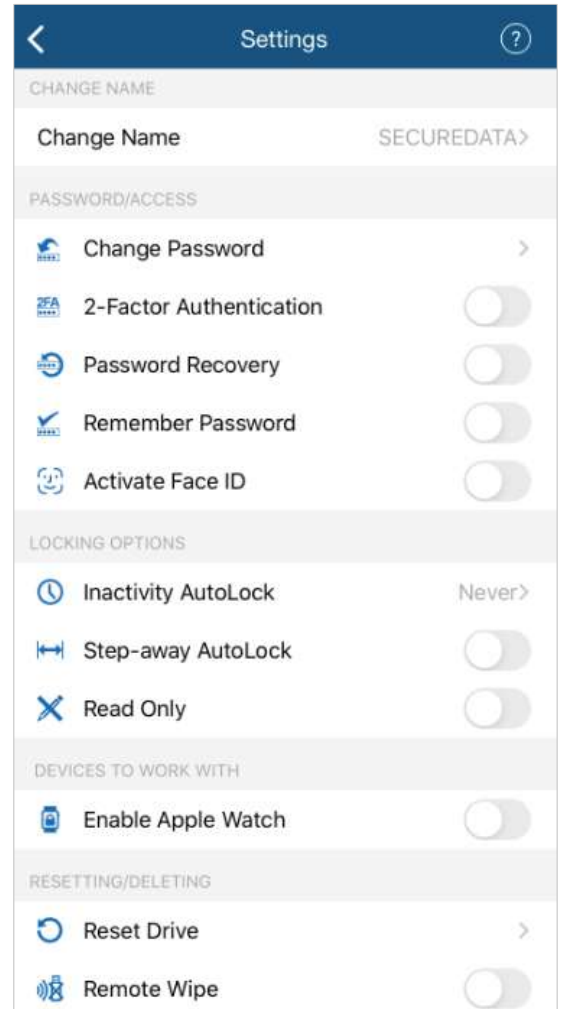
Password Options

Changing the Password

With your USB connected to a computer, follow these steps to change an existing password.

Change the Password	LED	APP
1. With the USB unlocked, tap the desired **USB name**.	▬	-
2. Tap **Change Password**.	▬	Refer to Settings image above.
3. Enter your old password, then 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. The application will not require a password to unlock your USB. With this setting we strongly suggest that you enable a passcode on your iOS/Android device.

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).	▬	☑ Remember Password 🟢
3. Tap **Yes** to confirm.	▬	🔓

Enabling the Password Recovery Feature

The Password Recovery feature will send a recovery code to your registered mobile number as a text message. There are two places where you can enable the Password Recovery:

- After creating password (refer to *Changing the Password* on **page 10**)
- From the Settings menu
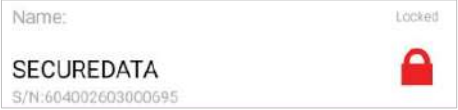
Enabling Password Recovery	APP
1. Make sure the USB is unlocked and authorized (logged-in) via the SecureData Lock app.	Name: ◐ Unlocked SECUREDATA S/N:604002603000077
2. Tap the **USB name** to access Settings.	-
3. Tap the **Password Recovery** button (green is ON).	↺ Password Recovery 🟢
4. Read the **Password Recovery** message and tap **Continue**.	-
5. Enter your mobile phone number.	Please enter your mobile number: 🇺🇸 United States +1 Continue
6. Tap **Continue**.	-
7. Confirm your mobile phone number.	-
8. Wait for a text message and enter the confirmation code received. (This is an example only.) Click **Continue**.	Enter Confirmation Code Please enter the 6 digit code below: 5 5 8 7 3 6 Continue

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.

Part A: Recovering Forgotten Password	APP
1. Tap the **USB name**.	Name: Locked / SECUREDATA / S/N:604002603000695
2. Tap **Forgot Password**.	Forgot Your Password? / Reset Drive
3. Tap **Yes** on the **Forgot Your Password** dialog.	-
4. Wait for the text message and then enter received confirmation code. (Example code used in image.)	**Enter Confirmation Code** / Please enter the 6 digit code below: / 5 5 8 7 3 6 / Continue
5. If entered correctly, you will see a Change Password dialog. Just create a new password. Once complete, your USB should be unlocked.	Old Password / •••••••• / New Password / Case-Sensitive / Confirm Password / Case-Sensitive / Change Password

Part B: If you previously did not enable Password Recovery and forgot your password, resetting the USB is the only way to make it usable again. Although your data will be erased from the USB, this ensures that it is not breached or compromised. You will need the serial number that is printed on the USB or listed on the Drives page of the app under the Drive name to allow resetting the Drive.

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

1. Tap the **USB name**.

   Name: Locked
   SECUREDATA
   S/N:604002603000695

2. Tap **Reset Drive**.

   Forgot Your Password?

   Reset Drive

3. Read the warning and tap **Reset Drive**.

   Resetting drive will delete all data and settings from the drive.

   Data cannot be recovered.

   Continue?

   Reset Drive

4. Enter the drive's serial number and tap **OK**. All data is now removed from the USB.

   or

   If available on your device, click **Scan A Barcode** to scan the USB's code and tap **OK**.

   Please Enter S/N (Drive's Serial Numbe

   -OR-

   Scan A Barcode

The USB reverts back to the default state. The default state is blank (has no password) and locked.

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

Microsoft Windows

You need to format the disk in drive L: before you can use it.

Do you want to format it?

Format disk   Cancel

Format Settings
The following are formatting settings:

Format (G:)

Capacity:
7.20 GB

File system
FAT32 (Default)

Allocation unit size
4096 bytes

Restore device defaults

Volume label

Format options
☑ Quick Format
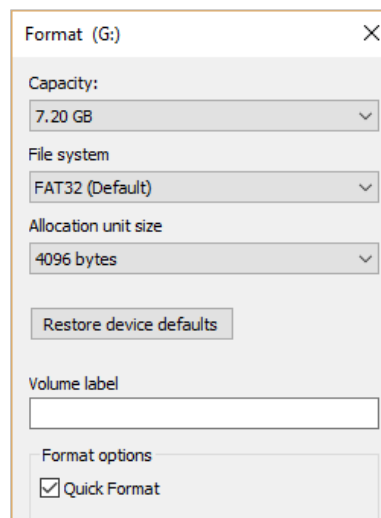
Access Options and Locking Options

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).		✕ Read Only ⬤
3. Tap **Lock Now** to the message about relocking. The USB 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).		✕ Read Only ⬤
3. Tap **Lock Now** to confirm disabling Read-Only. The USB 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 **USB name**.		🔓
2. Tap **Inactivity Lock**.		-
3. Tap the desired inactivity **interval** after which time the USB will automatically lock.		A checkmark displays. ✓

Note: 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**. The Inactivity Lock is now disabled.		A checkmark displays. ✓

Setting the Step-away AutoLock On and Off

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

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).		Step-away AutoLock 🟢
3. Tap **Yes** to confirm. The Step-away AutoLock is now on.		-

Note: To disable the Step-away AutoLock, tap the Step-away AutoLock button OFF (not green).
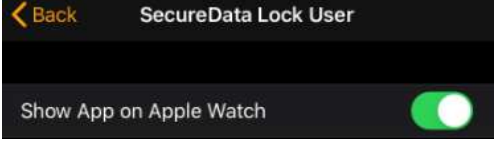
Set to Activate Biometric (Touch ID, Face ID, Facial Recognition)

Requirement: Android/iOS. Depending on the available biometric settings on the device, options for settings may vary. The following is an example. To use the Face ID feature of your iPhone to unlock the USB, enable the setting:

Remember Touch ID	APP
1. Make sure the USB is unlocked and authorized (logged-in) via the app.	Name: SECUREDATA S/N:604002603000077 — Unlocked
2. Tap the **USB name** to access **Settings**.	-
3. Tap the **Activate Face ID** button (green is ON).	Activate Face ID ●

Unlock the USB with an Apple Watch

You can unlock your USB with an Apple Watch® if used with iPhone 5S or newer.
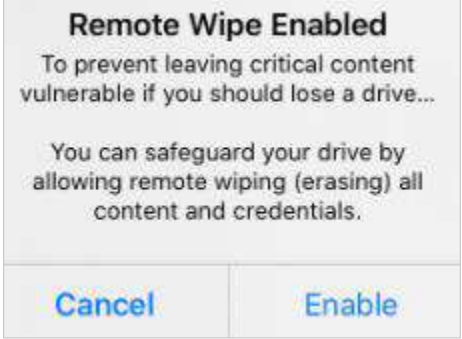
Unlock USB with Apple Watch	APP
1. Make sure the USB is unlocked and authorized (logged-in) via the app.	Name: SECUREDATA S/N:604002603000077 — Unlocked
2. Tap the **USB name** to access **Settings**.	-
3. Make sure SecureData Lock app is installed on your Apple Watch.	Back SecureData Lock User — Show App on Apple Watch ●
4. Turn ON **Enable Apple Watch**.	Enable Apple Watch ●
5. Start SecureData Lock app on your Apple Watch. **Note:** Your USB'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.	

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

Enabling Remote Wipe

To enhance protection for your USB in case it becomes lost, you can enable the Remote Wipe feature that will allow you to Remote Wipe (Reset) your lost USB.
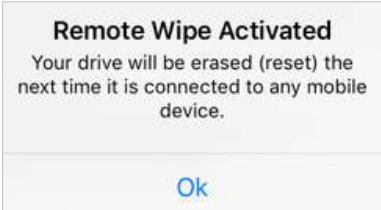
Enabling Remote Wipe	APP
1. Make sure the USB is unlocked and authorized (logged-in) via the app.	Name: ◑ Unlocked SECUREDATA S/N:604002603000077
2. Tap the **USB name** to access **Settings**.	-
3. Tap the **Remote Wipe** button (green is ON).	))̲ Remote Wipe
4. Tap **Enable** on the **Remote Wipe** dialog. You should see a confirmation that Remote Wipe is enabled.	**Remote Wipe Enabled** To prevent leaving critical content vulnerable if you should lose a drive... You can safeguard your drive by allowing remote wiping (erasing) all content and credentials. Cancel　　Enable

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 USB. (Ref. *Enabling Remote Wipe* on **page 17**.) If it has not been enabled, rest assured that your data on the USB cannot be accessed by whomever finds it. Follow this Remote Wipe activation procedure:

⚠️ **CAUTION:** Loss of data will occur. Once activated, there is no way to disable it. The next time the USB is discovered by the SecureData Lock 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.

Activating Remote Wipe	APP
1. In the app, copy the USB's Serial Number which is displayed below the USB's name.	Name: Disconnected **SECUREDATA** S/N:604002603000695
2. Swipe the **USB's name** to the right and tap Wipe.	Remove Wipe Name: **SECUREDATA** S/N:604002603000077
3. As a validation, you must enter your USB's Serial Number and tap **Remote Wipe**.	You have selected the Remote Wipe service. This action CANNOT be undone. If you proceed, it will permanently delete all data and credentials from your drive. To proceed, please type the S/N of the drive to confirm. Device S/N **Remote Wipe**
4. You should see a confirmation that Remote Wipe is Activated. Tap **OK**.	**Remote Wipe Activated** Your drive will be erased (reset) the next time it is connected to any mobile device. Ok

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

Managing the USB

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

Removing a USB

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 always add it back again by clicking ⊕ at the Home window. To add a USB, see *Adding a USB to the App* on **page 7**.

⚠️ **CAUTION:** Risk of unprotected data. Removing the USB 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 a 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**. **Note:** The 'Wipe' option will only be available if it is enabled.	-	Remove Wipe Name: SECUREDATA S/N:604002603000077
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**. The data is not recoverable.

12.26.2019

Resetting (Deleting) the USB

⚠️ **CAUTION:** Resetting the USB will delete all data stored on it including password and formatting. After resetting it, the USB must be formatted.

If your password has been forgotten, or 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 USB* on **page 21**.

Reset the USB	LED	APP
1. With the USB unlocked and authenticated (logged in), tap the desired USB name.	🔵	🔓
2. Tap **Reset Drive**.	🔵	🔄 Reset Drive ›
3. Tap the **Reset Drive** button.	🔵	-
4. Enter the drive's serial number and tap **OK**. All data is now removed from the USB.	🔴	🔒

Creating a Password after a Reset (Blank Drive)

Perform this procedure after the Drive has been reset. This password procedure is required to format the Drive and must be performed after the app has been installed on your phone (or other device) to use the Drive.

Create a Password	LED	APP
1. **Insert** the USB 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**. To continue, your Drive now requires formatting. See *Reformatting the Drive* below.	🔵	🔓

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

Reformatting the USB

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 then be initialized and reformatted for future use.

To reformat your USB, do the following:

For a Windows OS

1. At the system popup message, click **Format Disk**.
2. If the settings are okay, click **Start**.
3. Generally the default values are good. Use FAT32 or exFAT for the file system.
4. Click **OK** to the warning about erasure.
5. Click **OK** to complete.
6. Click **Close** to exit the dialog. When finished the blue USB LED lights.

For Mac OS

1. Connect to a Mac computer's USB port.
2. Click **Initialize** in the popup message (shown below). The Disk Utility Dialog displays.

Figure 1:   The Disk Utility Dialog.

3. Click **Erase** to open the dialog box.
4. Ensure your USB displays in the Name field and click Erase. The system begins erasing the external USB and renaming it SECUREUSB.
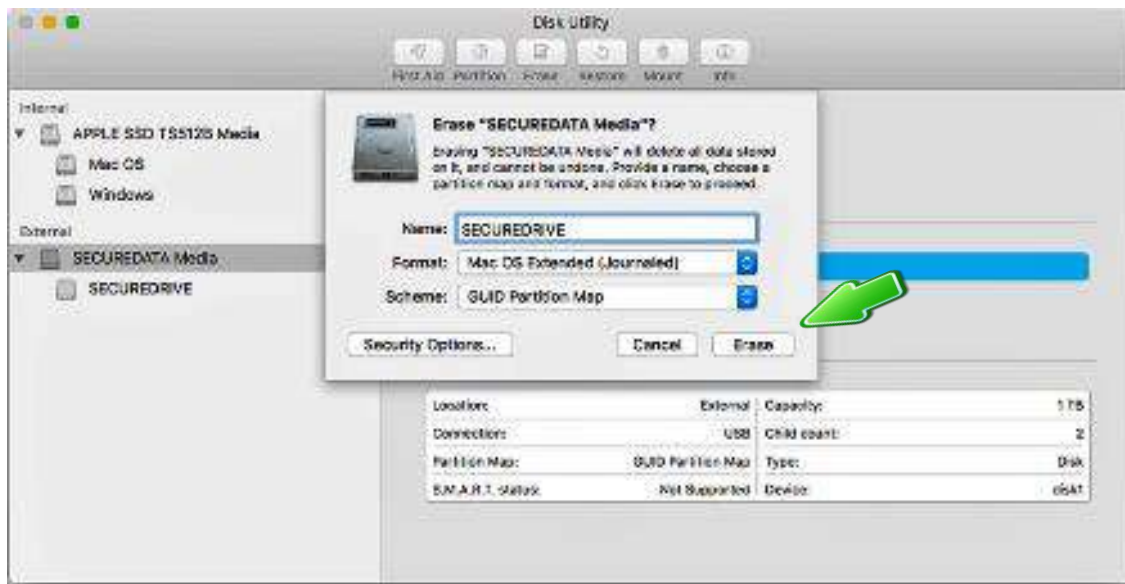
Figure 2: *SecureUSB* **displays under the list of External USB when done
(as well as on the desktop).**

5. Click **Done** in the message dialog when available. The USB is now displayed under External in the left column.
6. Close the **Disk Utility**.

CONTACT AND WARRANTY INFORMATION

Contact Information

SecureData, Inc.
625 Fair Oaks Ave Suite 325,
South Pasadena, CA 91030

www.securedrive.com
US: 1-800-875-3230
International: 1-424-363-8535

Technical Support email: support@securedrive.com

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

- The Software Version Number (refer to the next heading)
- Serial Number (S/N) on the back of the device

Finding the Version Number

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

Troubleshooting

Issue	Solution
After unlocking the USB, your computer shows that the external USB 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. To format, see *Reformatting the USB* on **page 21**.
I can't swipe right to lock the USB in the SecureData Lock 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. You'll need the USB Device ID number.

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, NEGLECT, 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.

SecureUSB and SecureUSB products are developed and manufactured by SecureData and are based on SecureData Lock technology licensed from ClevX, LLC. U.S. Patent. www.clevx.com/patents

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

Registered Trademark	Owner
Android	Google, Inc.
Bluetooth	Bluetooth SIG, Inc.
DataLock, ClevX	ClevX, LLC
Mac, iOS	Apple, Inc.
SecureUSB, SecureData	SecureData, Inc.
Windows	Microsoft

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.

12.26.2019