SECURE DRIVE
BLUETOOTH

FIPS VALIDATED 140-2™

SECURE DRIVE
BLUETOOTH

USER MANUAL

SECURE DATA

Contents

SecureDrive-BT Overview

Thank you for purchasing the SecureDrive™-BT Model ('*Drive*' hereafter). It's an easy to use, hardware encrypted USB 3.0, password activated external Drive. 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 Drive 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 Drive 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' Drives. This makes it perfect for corporate and government deployment (not covered in this manual.)

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

REQUIREMENTS
The Drive 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.

WHAT'S INCLUDED?
• 1 Drive • 1 Quick Start Guide • 1 USB 3.0 cable

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 Drive to water or moisture.
- Resetting the Drive will delete all stored data as well as all passwords.
- Forgetting your password will render the Drive 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.

CAUTION:

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.

SecureDrive-BT Features

Device ID

12345678

Data
Locked   Transfer   Unlocked

Three easy steps

1 Plug in USB connector   2 Enter PIN on phone   3 Unlocked

FCC ID: 2AOOJCGASDTAS
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.

S/N: 123456789

DATALOCK SECURED
CLEVX, LLC
PATS. PENDING   FCC RoHS

ASSEMBLED IN U.S.A.   CE

securedata.com SecureData, Inc.

SECURE DRIVE
BLUETOOTH

Serial Number

Figure 1:   SecureDrive BT layout showing LEDs and ID numbers.

Icon Interpretations

ON THE DRIVE

LEDs on the Drive are represented here by colored icons.

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 Drive is unlocked and accessed (Drive is transferring data). NOTE: The blue LED may be on or blinking during any procedure after the Drive is unlocked.
🔓 = **Green** solid	Powered and Unlocked. Settings operation was successful.

ON THE APP

App Icon	Meaning
🔒	Drive is locked
🔓	Drive is unlocked
🔒	Drive is blank such as when not formatted
◐	The Drive is BT-connected to the app and Authenticated. If you don't see this icon, the Drive is BT-connected but not Authenticated which means that if the Drive 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 the Accompanying App

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

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 SecureDrive–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 not '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

All actions require the Drive to be connected to a computer with the USB cable. 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 Drive to the App (Pairing)

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

Adding the Drive	LED	APP
1. Connect the Drive to a computer with the USB cable.	🔓 ➖ 🔓 (one blink) Then 🔒	
2. Start the DataLock App on your device. NOTE: Ensure your device is BT enabled.	🔒	
3. Tap ⊕ if you don't see the new Drive's SN in the list.	🔒	🔒
4. Tap the Drive name that appears and follow the app instructions.	🔒	
5. Tap **Continue** and follow the app instructions.	🔒	

Unlocking the Drive

> ⚠ **CAUTION**: Possible loss of data. After ten failed attempts to unlock the Drive, the password, all data, and the formatting will be deleted. Refer to *Brute Force Hacking Detection* on page 31.

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

Unlock the Drive	LED	APP
A. *WHEN NOT CONNECTED:* 1. Connect the Drive to a computer with the USB cable.	🔒 ▬ 🔓 (one blink) Then 🔒	
2. Start the DataLock App on your device. NOTE: Ensure your device is BT enabled.	🔒	
3. Tap the Drive 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).* 1. Open the app.	🔒 or 🔒	🔒
2. Tap the Drive name.	🔒	
3. Type in the password1.	🔒	
4. Tap Unlock.	🔓	🔓

[1] The password on new Drives is 11223344.
We strongly suggest changing the password after unlocking.
Refer to Changing the Password on page 11.

> **NOTE:** If the Drive still doesn't appear in your computer's file manager, refer to *Troubleshooting* on page 39.

Disconnecting the Drive from Your Computer

Generally, you can just unplug the USB cable.

> **NOTE:** Some computer systems may require clicking the Safely Remove Hardware/Eject icon on your system prior to unplugging the cable 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.

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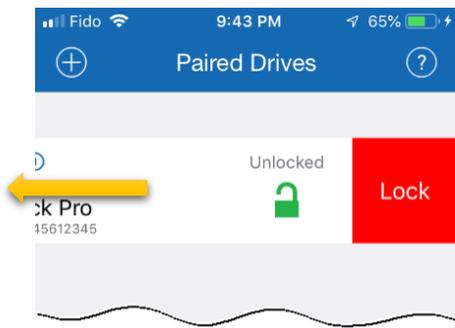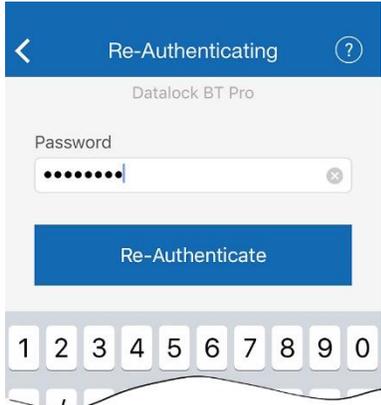
Setting Options

The following headings describe enabling options and features.

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

> NOTE: All actions require the Drive to be connected to a computer with the USB cable.
>
> NOTE: Unless otherwise noted, procedures listed below assume the Drive 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 Drive name anytime it's unlocked and authenticated.
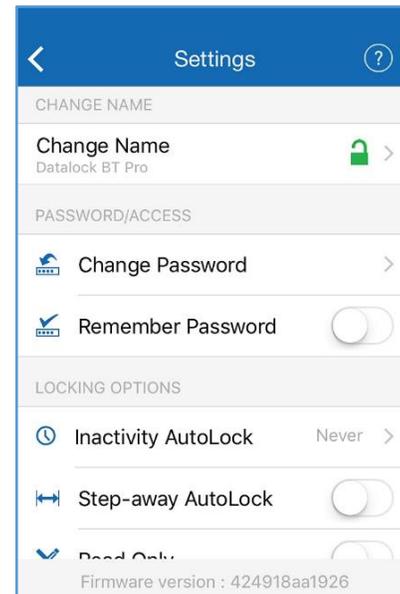
Figure 2:   The Settings Menu, partial view. ⇨

Password Options

CHANGING THE PASSWORD

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

Change the Password	LED	APP
1. With the Drive unlocked, tap the desired Drive name.	🔓	
2. Tap Change Password and enter your current password.	🔓	Refer to Figure 2: 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 Drive 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 Drive. With this setting we strongly suggest that you enable a

passcode on your iOS/Android device.
Also, if the *Step-away AutoLock* feature is on, the Drive will authenticate and unlock automatically as soon as the app is opened and within BT range.

Remember Password	LED	App
1. With the Drive unlocked and authenticated (logged in), tap the desired Drive name.	🔓	🔓
2. Tap the **Remember Password** button to the ON position (green).	🔓	
3. Tap **Yes** to confirm.	🔓	🔓
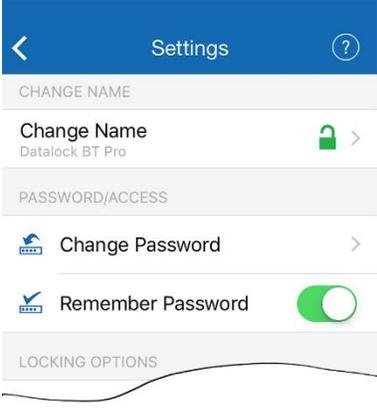
ENABLING THE PASSWORD RECOVERY FEATURE

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 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.
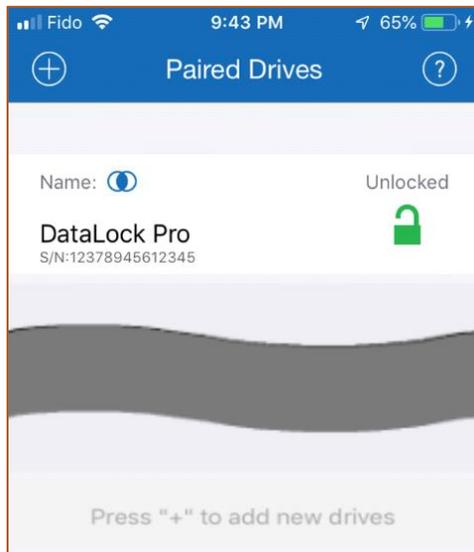
3. Tap the Password Recovery button (green is ON).
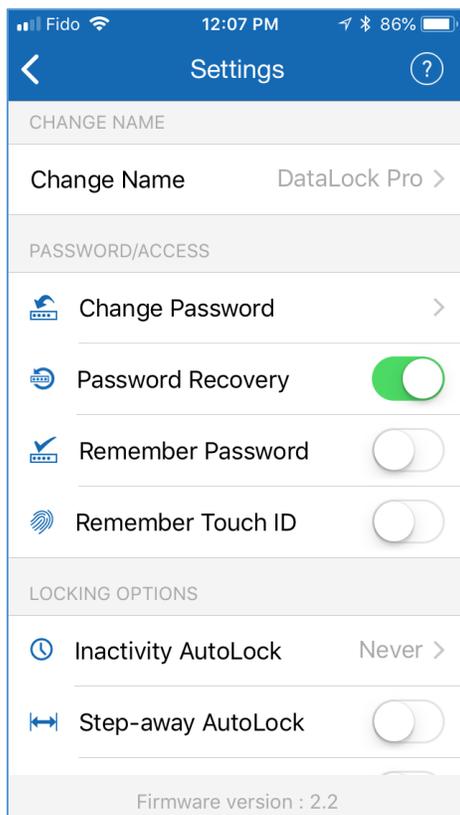
4. Read the Password Recovery message and tap Continue.

5. Enter your mobile phone number.
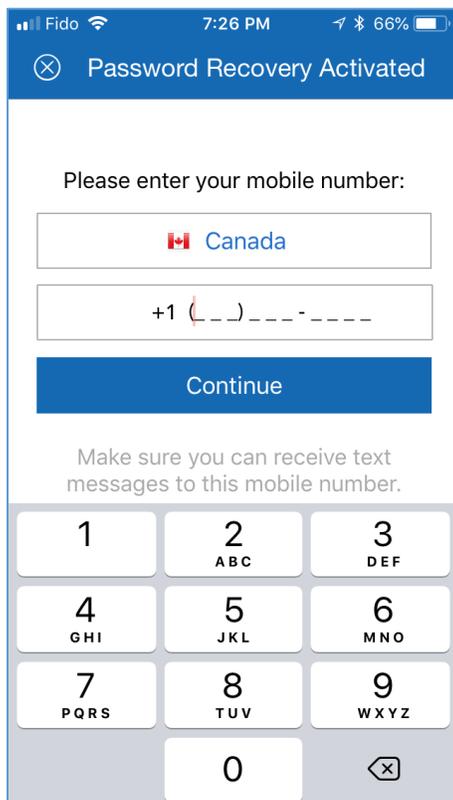
6. Tap Continue.
7. Confirm your mobile phone number.
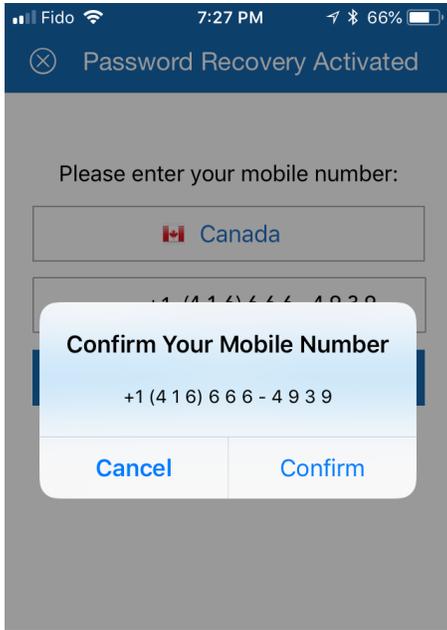
8. Wait for a text message and enter the confirmation code received. (This is an example only.)
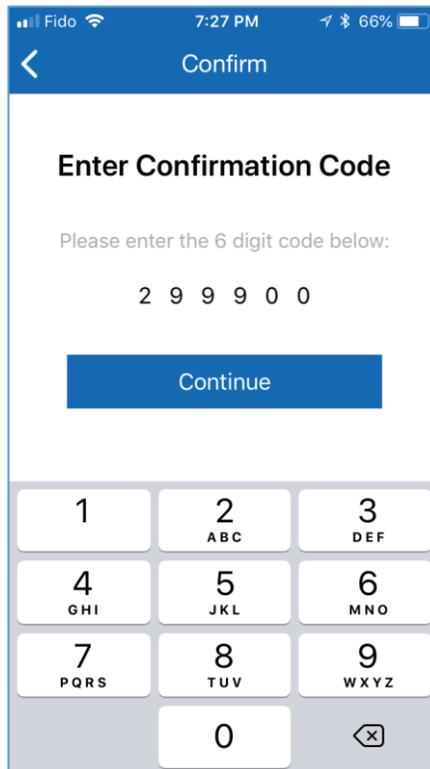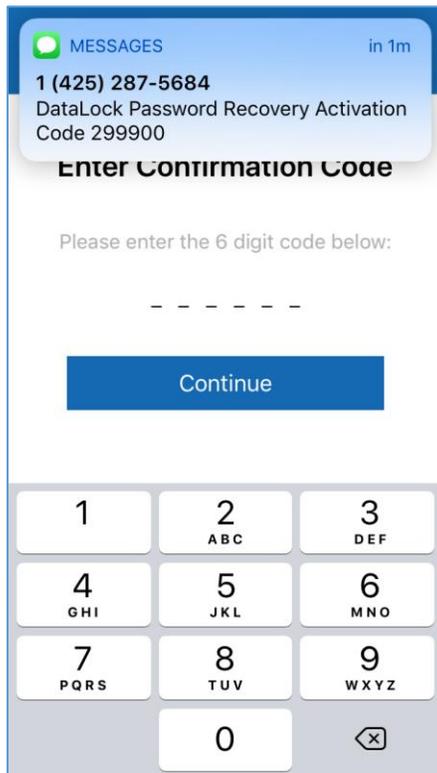
You should get a confirmation that Password Recovery is Activated.
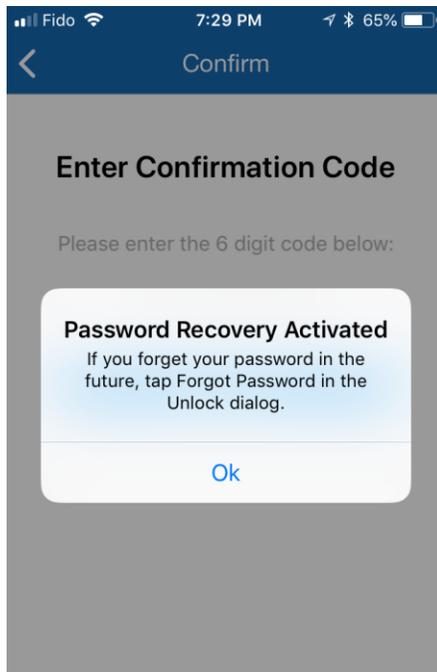
To recovery your password, see the next heading.

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.
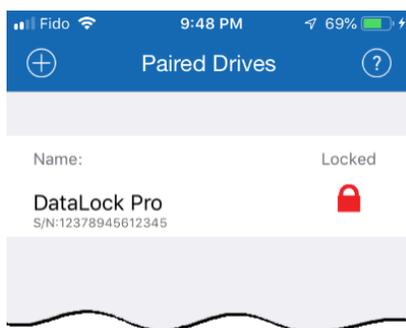
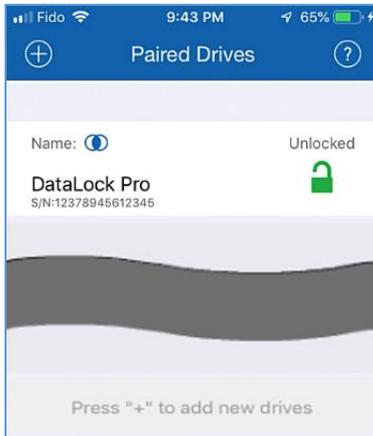2. Tap Forgot Password.
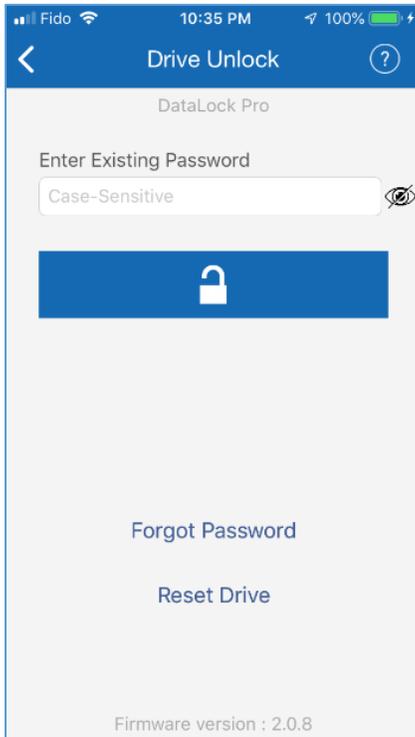
3. Tap Yes on the Forgot Your Password dialog.
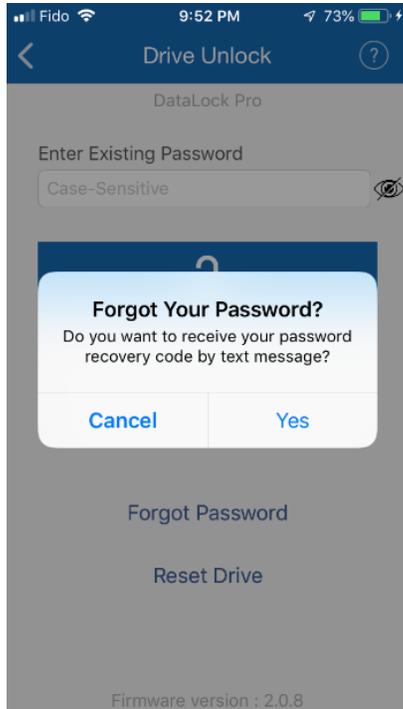
4. Wait for the text message and then enter received confirmation code.
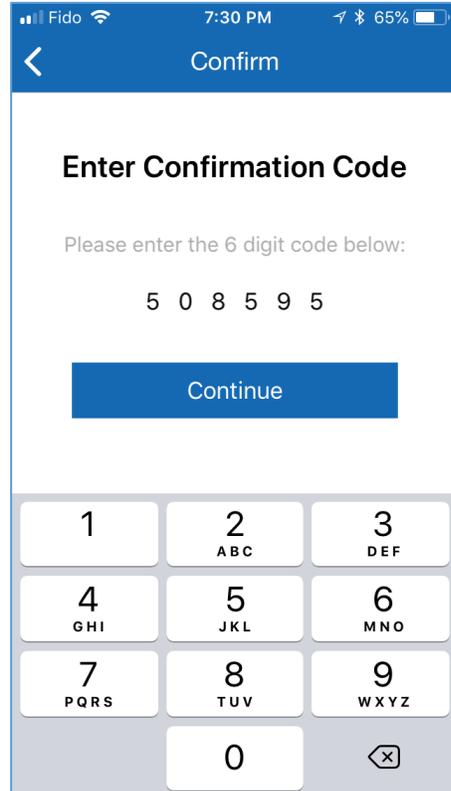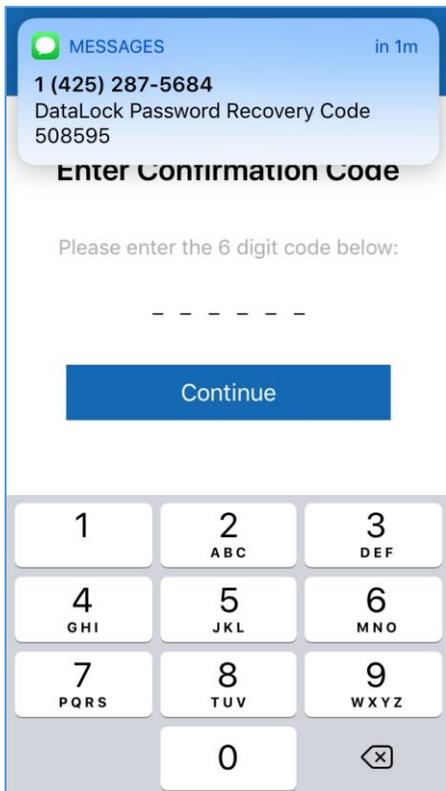
5. If entered correctly, you will see a Change Password dialog. Just create a new password.
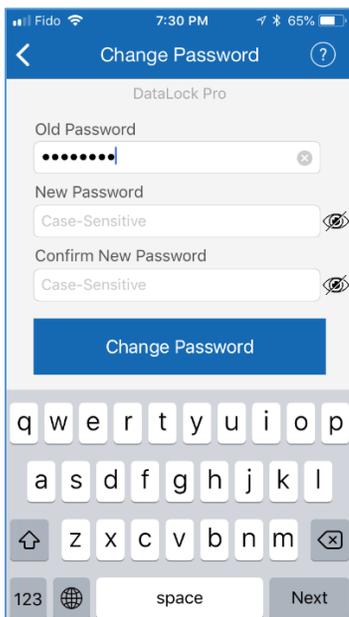
Now your Drive should be unlocked.

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.
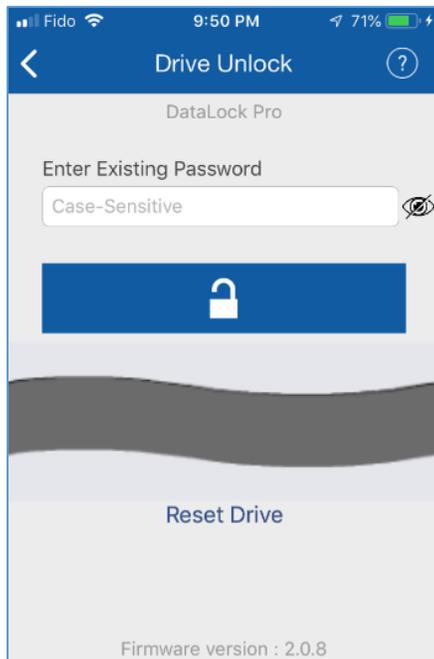
You will need the Serial Number of the Drive.

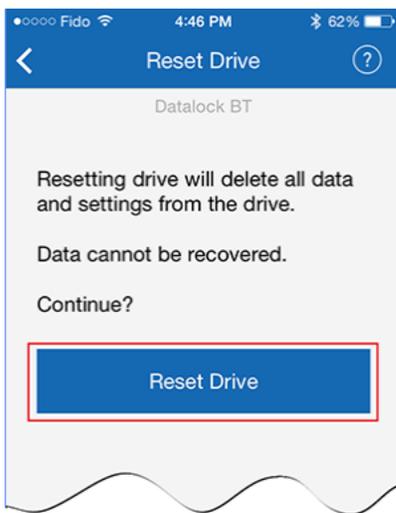Make sure the Drive is authorized (logged-in) via the app.
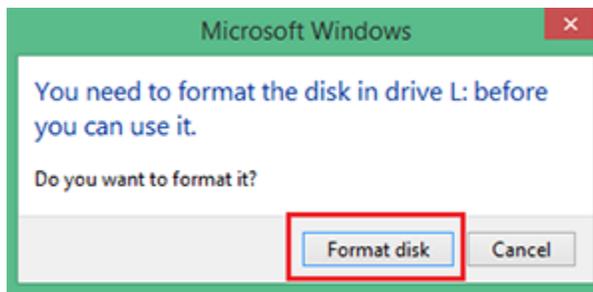
1. Tap the Drive name.
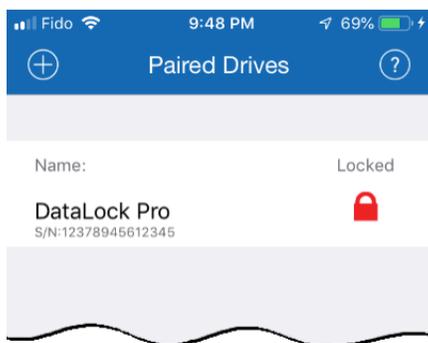
2. Tap Reset Drive.

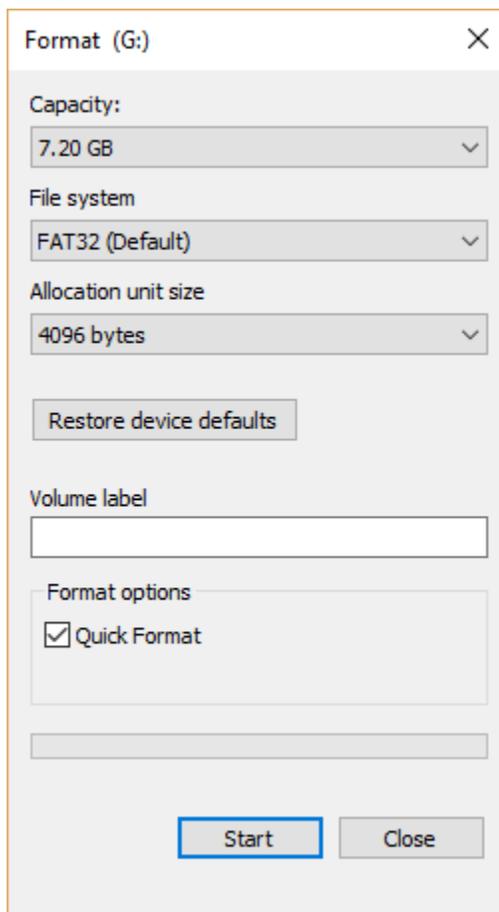3. Read the warning and tap Reset Drive.

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 undoing 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 Drive unlocked and authenticated, tap the desired Drive name.	🔓	🔓
2. Tap the **Read Only** button to the ON position (green).	🔓	
3. Tap **Lock Now** to the message about relocking.	🔒	🔒

The Drive 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 Drive unlocked and authenticated (logged in), tap the desired Drive name.	🔓	🔓
2. Tap the **Read Only** button to the OFF position (not green).	🔓	
3. Tap **Lock Now** to confirm disabling Read-Only.	🔒	🔒

The Drive will be in Read/Write mode when unlocked.

SETTING THE INACTIVITY LOCK

To protect against unauthorized access when the Drive is connected to a host computer and unattended, the Drive 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 Drive unlocked and authenticated, tap the desired Drive name.	🔓	🔓
2. Tap Inactivity Lock.	🔓	
3. Tap the desired inactivity **interval** after which time the Drive will automatically lock.	🔓	A checkmark displays. ✓

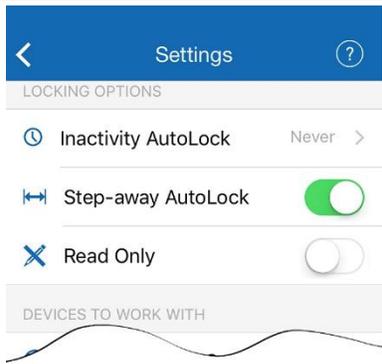The Inactivity Lock is now set for subsequent Drive use, until changed. When it locks, the red Drive LED lights.

DISABLING THE INACTIVITY LOCK

Disable the Inactivity Lock	LED	App
1. With the Drive unlocked and authenticated, tap the desired Drive name.	🔓	🔓
2. Tap Inactivity Lock.	🔓	
3. Tap **Never**.	🔓	A checkmark displays. ✓

The Inactivity Lock is now disabled.

SETTING THE STEP-AWAY AUTOLOCK ON AND OFF

The Step-away AutoLock will lock the Drive (disappear from the File Explorer/Finder) when the iOS/Android device is moved about 3m away from the Drive for longer than 5 seconds. When returned to the Drive vicinity, the Drive unlocks automatically when Remember Password option is ON (see *Setting to Remember Password* on page 11).

Set the Step-away AutoLock	LED	App
1. With the Drive unlocked and authenticated, tap the desired Drive 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).

SET TO REMEMBER TOUCH ID (FACE ID) FOR SOME IPHONES
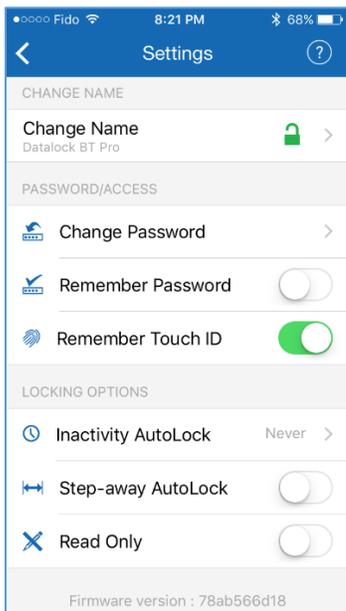Requirement: iPhone 5S and newer.

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.

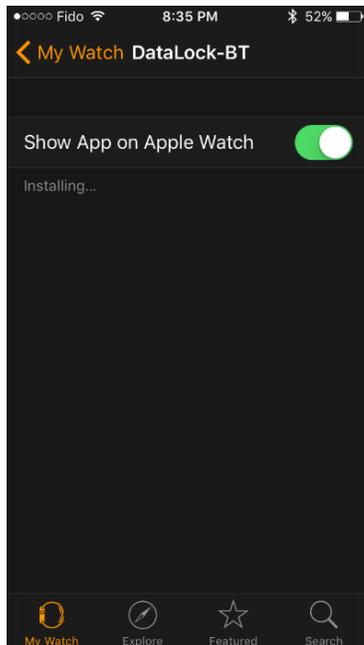3. Tap the Remember Touch ID button (green is ON).

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.
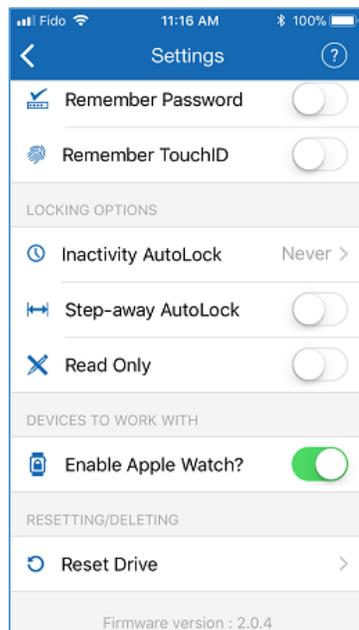2. Tap the Drive name to access Settings.

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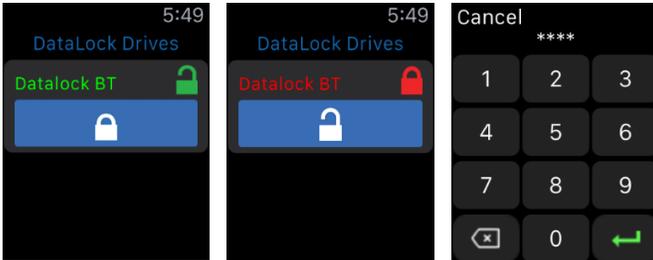

4. Turn ON Enable Apple Watch.

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.
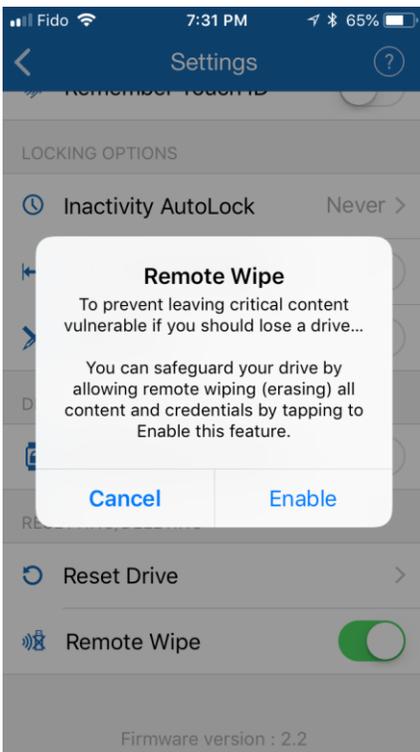
1. Make sure the Drive is unlocked and authorized (logged-in) via the app.
2. Tap the Drive name to access Settings.
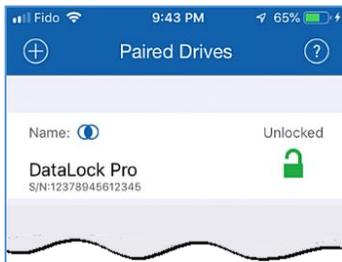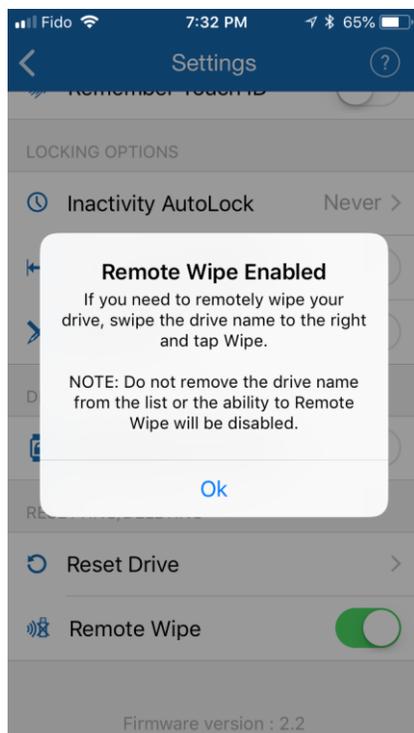
3. Tap the Remote Wipe button (green is ON).
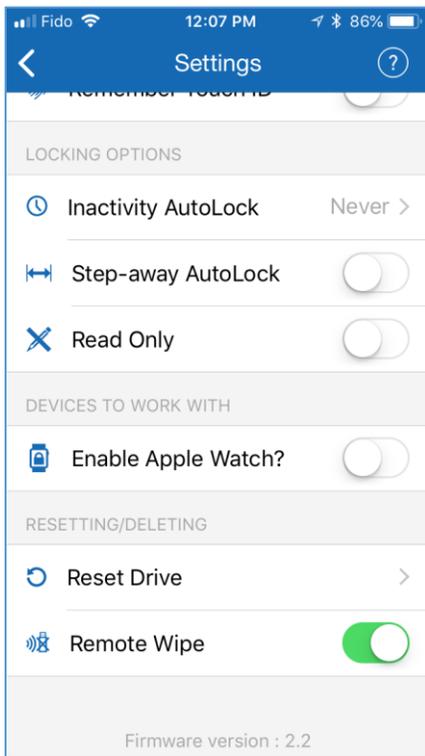
4. Tap Enable on the Remote Wipe dialog.

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 DRIVE

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.

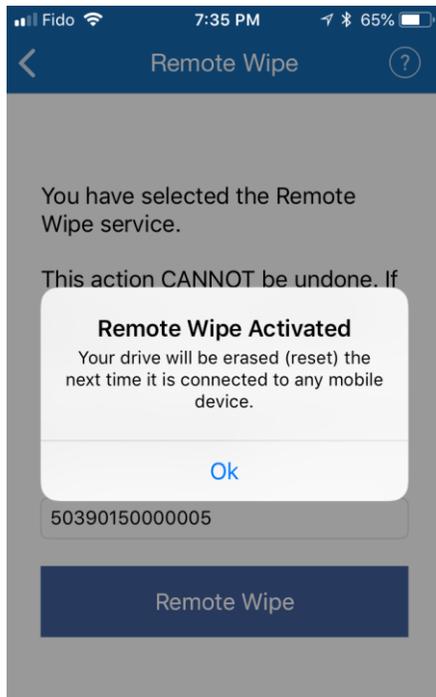1. In the app, copy the Drive's Serial Number which is displayed below the Drive's name.

2. Swipe the Drive's name to the right and tap Wipe.
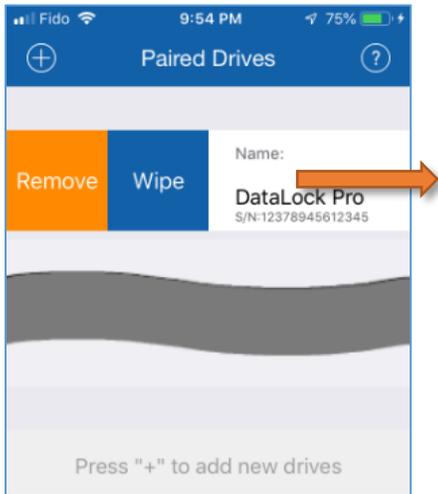
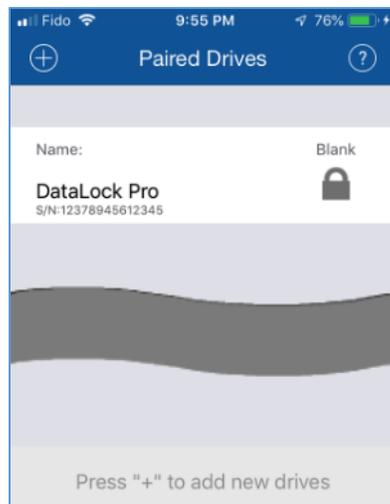3. As a validation, you must enter your Drive's Serial Number and tap Remote Wipe.
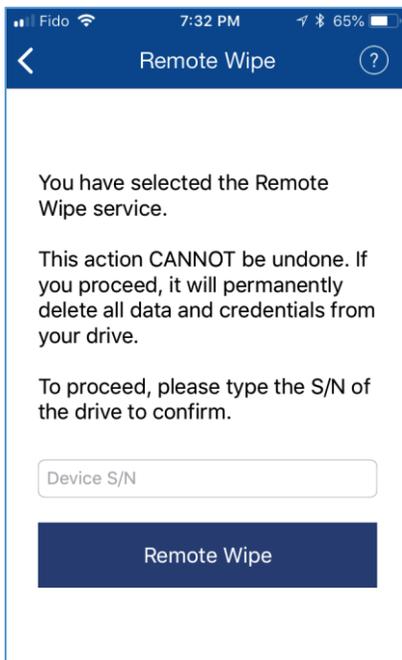
4. You should see a confirmation that Remote Wipe is Activated. Tap OK.

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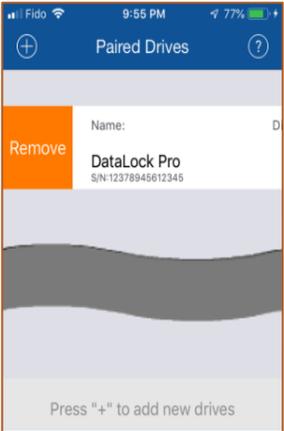

Managing the Drive

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

Removing a Drive

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

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

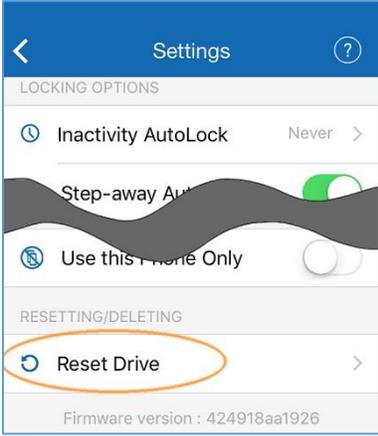| Remove a Drive	LED	App
1. With the Drive locked or unlocked, touch the desired Drive name and swipe right. (If unlocked, see the caution message above.)	🔒 or 🔓	🔒 or 🔓
2. Tap Remove.		
3. Tap Remove to confirm.	🔒 or 🔓	🔒 or 🔓

Brute Force Hacking Detection

Entering an incorrect password ten consecutive times, the Drive brute force hacking detection triggers and **the password, all data, and format will be deleted**. To re-use the Drive see *Creating a Password after a Reset (Blank Drive)* on page 32. The data is not recoverable.

Resetting (Deleting) the Drive

> ⚠️ **CAUTION**: Resetting the Drive will delete all data stored on it including password and formatting. After resetting it, the Drive must be formatted. See *Creating a Password after a Reset (Blank Drive)* on page 32.

If your password has been forgotten, or you want to delete all data stored on the Drive including the password, you can perform the following Reset function. It also removes the encryption, requiring the Drive to be reformatted to generate new encryption. To reformat the Drive after resetting it, see the heading *Reformatting the Drive* on page 33.

Reset the Drive	LED	App
1. With the Drive unlocked and authenticated (logged in), tap the desired Drive name.	🔓	🔓
2. Tap Reset Drive.	🔓	
3. Tap Reset Drive.	🔓	
4. Tap **Reset** to confirm.	🔓	
5. Type in the **Device ID** (find it next to the USB port) and tap **OK**.	🔒	🔒

All data is now removed from the Drive.

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. Connect the Drive to a computer with the USB cable.	🔒 ➖ 🔓 (one blink) then 🔒	
2. Start the app.	🔒	

3. If the Drive name doesn't appear, tap ⊕ (upper left) and then tap the Drive name.	🔒	NOTE: If the Drive is not blank you'll see 🔒. Refer to page 31.
4. Tap the Drive name.	🔒	
5. Type in password and confirm it.	🔒	**Create User Password** ⊙ Create Password Case-Sensitive Confirm Password Case-Sensitive **Create Password**
6. Tap Create Password.	🔓	🔓
To continue, your Drive now requires formatting. See *Reformatting the Drive* below.		

⚠️ **CAUTION**: If a mistake was made while defining a new password or the procedure was not completed, the red LED will come on. The Drive is unusable without a password.

Reformatting the Drive

In the event that hacking detection has been triggered or the Drive has been reset, all data on the Drive has been deleted. The Drive must then be initialized and reformatted.

To initialize your Drive, do the following:

FOR A WINDOWS OS
Admin permissions for the PC is required for this procedure.

1. Connect the Drive to your computer with the USB cable.
2. Create User Password if you have not already done so (see *Creating a Password after a Reset* (Blank Drive) on page 32).
3. Open Explorer.
4. Right-click This PC > Left-click Manage.
5. In the Computer Management dialog's left column, click Storage > Disk Management and wait for it to populate.
6. If Initialize Disk dialog doesn't popup, R-click the 'Unknown' disk, usually Disk 1, and click Initialize disk.
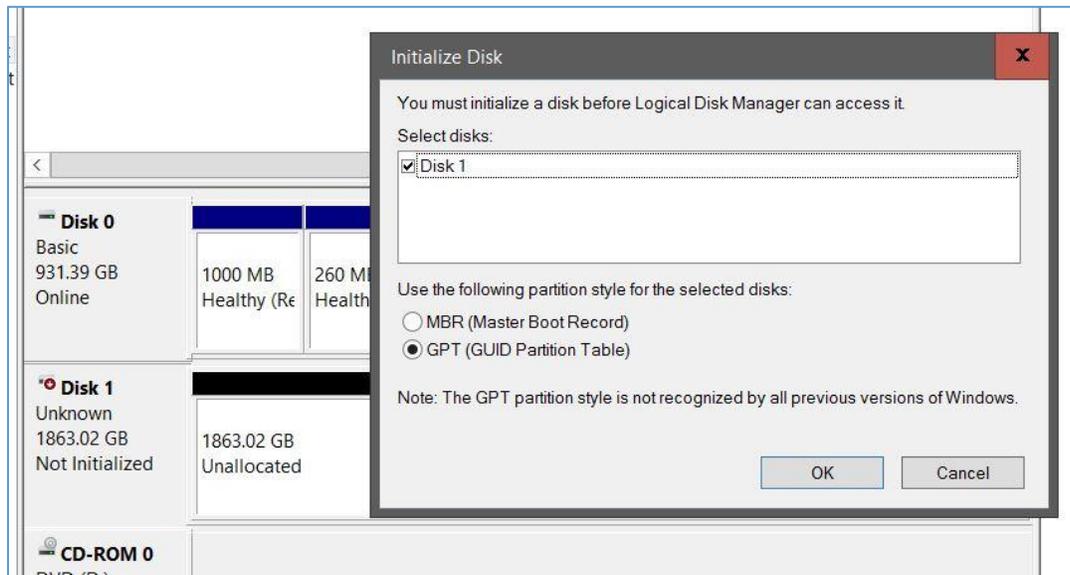
Figure 3: Initializing the SecureDrive disk (shown here as Disk 1).

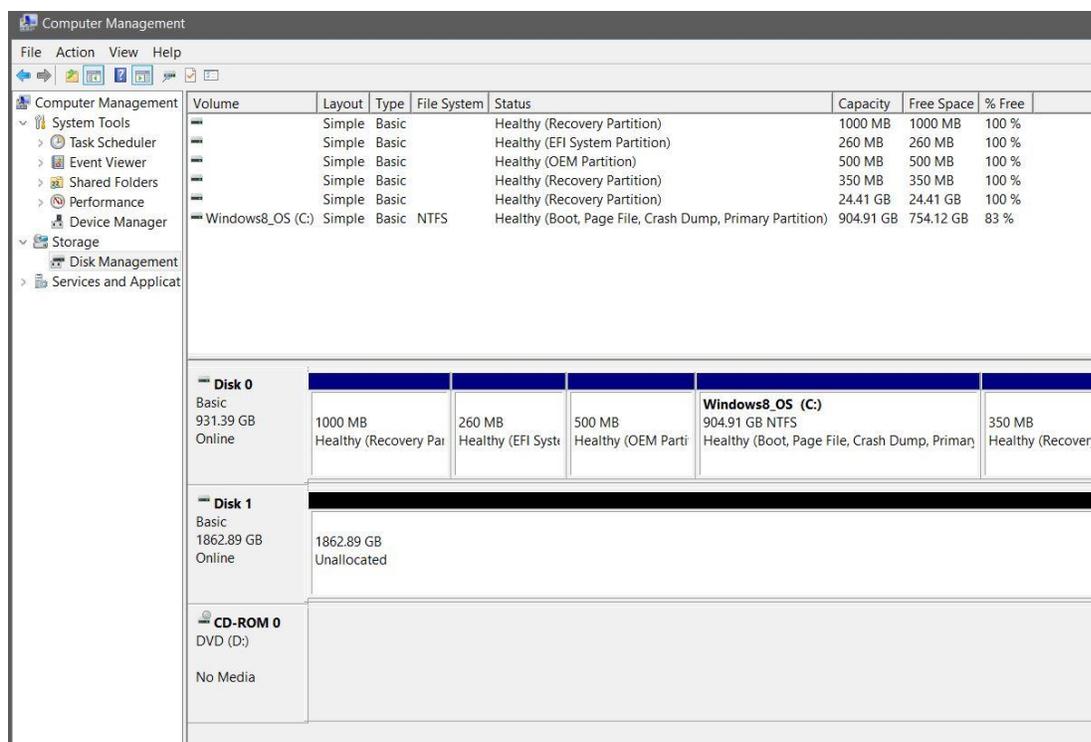7. Make sure GPT is selected and then click OK.

Figure 4: The SecureDrive is shown here as Disk 1. It is Online but not yet allocated. (Windows 10 shown here.)

8. After Unknown changes to Online, right-click near Unallocated > New Simple Volume.
9. Follow the Wizard prompts. Select a Drive letter (it generally defaults to the next available letter) and then follow the prompts in the Wizard.
10. At the Format Removable Disk dialog, select a Volume Label, and select NTFS.

11. Continue to follow the prompts.
    While the Drive is formatting the blue LED blinks.
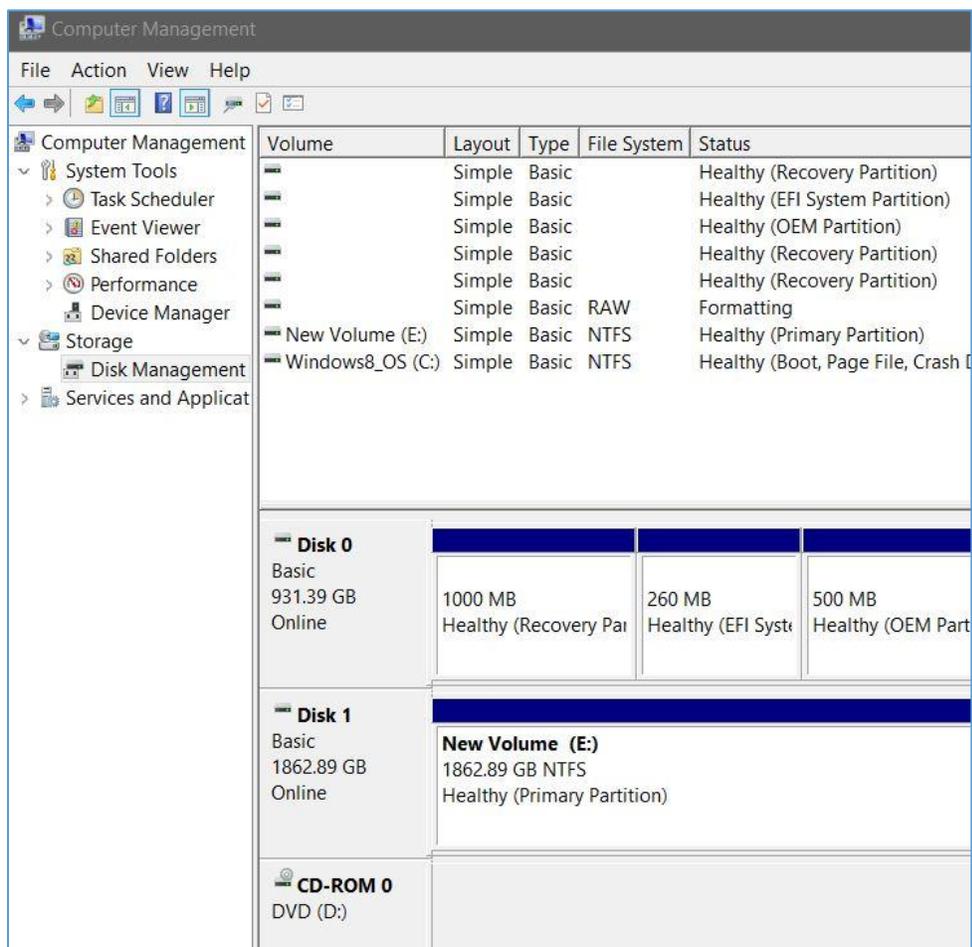12. Click Finish to end and close the Wizard.

Figure 5:   The SecureDrive is displayed here as "Disk 1." It is Online and allocated
              (Healthy) and ready for use.

13. Close the Computer Management dialog if it's still open.

When finished the New Volume (usually E) reads Healthy and a second Explorer window
opens to display the Drive contents. The SATA blue 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.
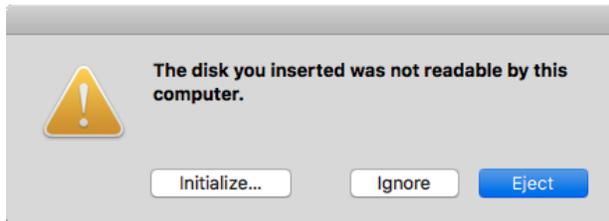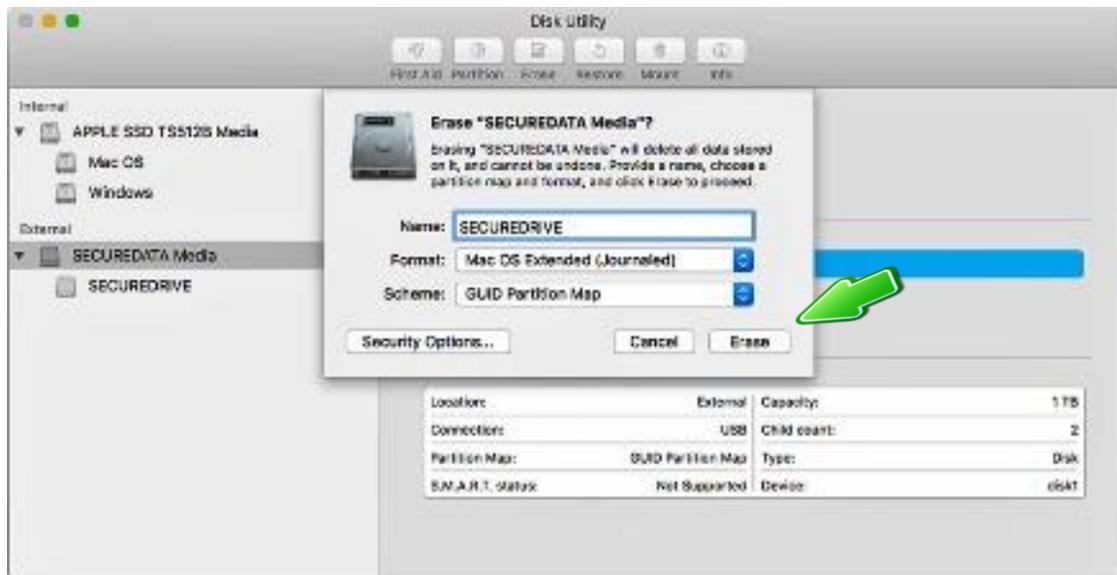

Figure 6:   The Disk Utility Dialog.

3. Click Erase to open the dialog box.
4. Ensure your Drive displays in the Name field and click Erase. The system begins erasing the external Drive and renaming it SECUREDRIVE.
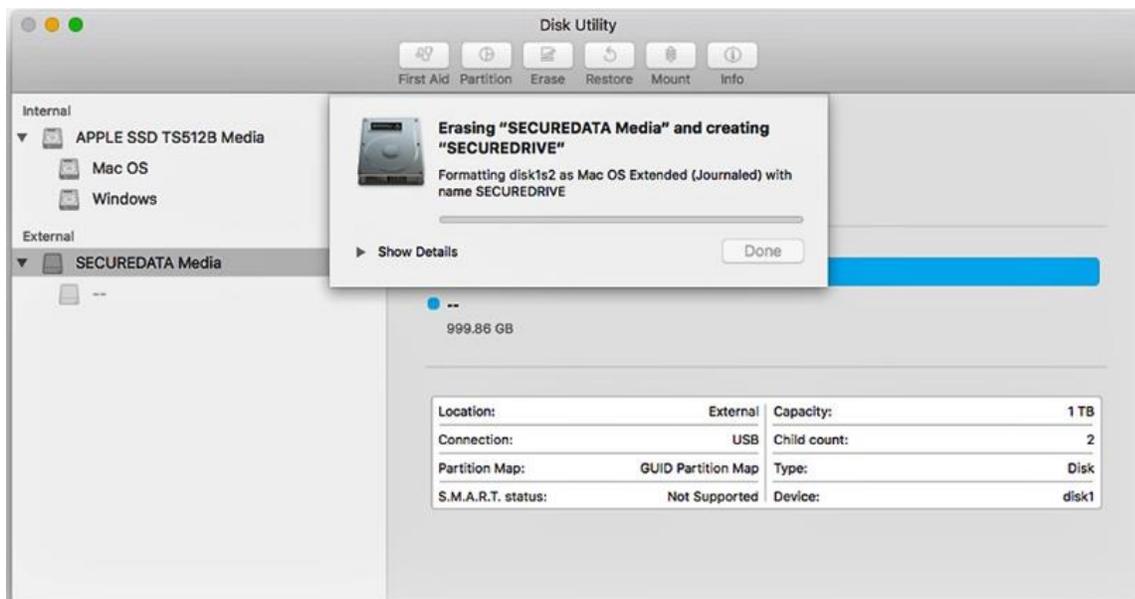
Figure 7: *SecureDrive* displays under the list of External Drive when done (as well as on the desktop).

5. Click Done in the message dialog when available.
   The Drive is now displayed under External in the left column.
6. 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 Drive Firmware Version Number (refer to the next heading)
• The Software Version Number (refer to the next heading)
• Serial Number (S/N) on the back of the device

FINDING THE VERSION NUMBERS
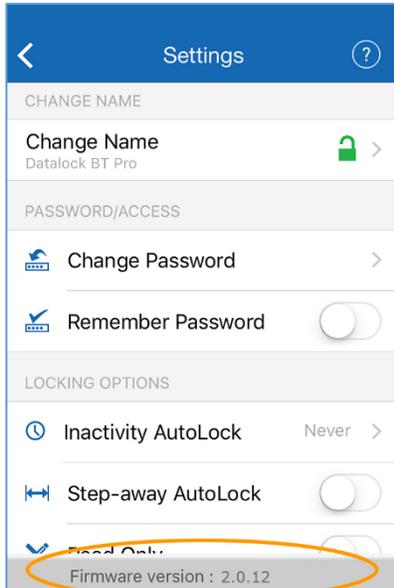
The Drive *firmware version number* is at the bottom of the Settings window. Unlock the Drive and tap the Drive name to display the Settings window.

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

Troubleshooting

■ After unlocking the Drive, your computer shows that the external drive is connected (icon displays) but you cannot access the Drive data (it doesn't display in Explorer (Windows) or Finder (Mac).

> ➢ The Drive is not initialized and needs to be formatted—no data exists. It may have been reset. To format, see *Reformatting the Drive* on page 33.

■ I can't swipe right to lock the Drive in the DataLock App even though the Drive name and unlock-icon display.

> ➢ The Drive is not authenticated (⏻ does not display). Simply tap the Drive name, enter the password and tap Re-Authenticate.

■ Tapping the Drive name in the app doesn't do anything.

> ➢ If you've used a different Drive prior to the current one, that old one may still display in the app. With the Drive plugged in, and with Bluetooth on your iOS/Android device turned on, tap the plus sign ⊕ to add your current Drive. You'll need the Drive Device ID number.

■ 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.

■ If you think your keypad is faulty, contact *Technical Support*, page 38.

Warranty and RMA Information

(Returned Merchandise Authorization)

TWO YEAR LIMITED WARRANTY

As explained below, SecureData, Inc. offers a two-year limited warranty on the SecureDrive™ 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.

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