

SECURE DRIVE

KEYPAD MODEL



USER MANUAL

Contents

SecureDrive Overview 3

Safety Information 3

SecureDrive Features 4

PINs and Procedures 5

User Mode 5

User PINs 5

Unlocking the Drive in User Mode 6

Changing the User PIN 6

Options for User Mode 7

Admin Mode 8

Button Pressing Conventions 9

Admin PINs 9

Options for Admin Mode 11

Managing the Drive 13

Verifying which PINs have Been Set 13

Deleting all Files in Admin Mode 13

Brute Force Hacking Detection 14

Resetting (Deleting) the Drive 15

Creating a User PIN after a Reset (blank Drive) 15

Reformatting the SecureDrive 15

Technical Support 20

Contact Information 20

Troubleshooting 21

Warranty and RMA information 22

SecureDrive Overview

Thank you for purchasing the SecureDrive-Keypad Model ('Drive' hereafter), an easy to use hardware encrypted USB 3.0 portable external data storage drive with on-board alphanumeric 11 button keypad for OS-independent user-authentication.

The Drive uses XTS-AES 256-bit hardware encryption, which encrypts all data on it in real time. It requires no software drivers nor updates and 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 PIN (Person-Identification-Number).

The Drive can be configured with both a User and Admin PINs, making it perfect for personal use and business use such as healthcare, legal, corporate, and government.

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 systems, or any embedded systems supporting USB 2.0 port, minimum.

WHAT'S INCLUDED?

- 1 SecureDrive
- 1 Quick Start Guide
- 1 USB 3.0 cable

Safety Information

This icon  indicates important information regarding the safety of the product and your data (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 PINs and settings. The Drive will become blank and require formatting.
- Forgetting your PIN will render the Drive inaccessible. There is no 'backdoor.' (If an Admin exists, the Admin can unlock the Drive and create a new User PIN.)

SecureDrive Features

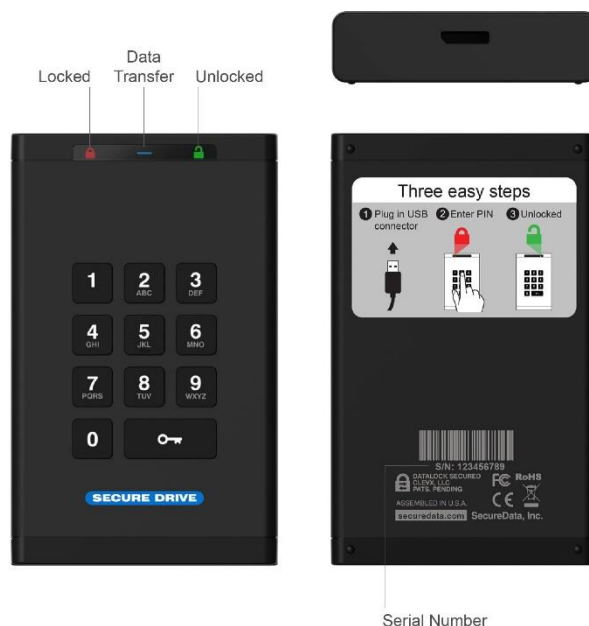











Figure 1: The Drive Layout

LED INTERPRETATIONS

LEDs on the SecureDrive are represented here by colored icons.

LED	Meaning
 (blink all together once)	Plugged into computer; LED test
 = Red solid	Locked; Momentarily preparing for next input; or failed procedure.
 = Red blinking ¹	Locked, ready for input (other than a Setting code). Also, specific feedback ¹
 = Red blinking with Green solid	(Settings Mode) Locked & ready for keypad input within 10 seconds, or idle for 30 seconds if procedure is done.
 = Green blinking	Unlocked and ready for keypad input
 = Green blinking slowly	Unlocked for use in Read-Only Mode
 = Blue solid  = Blue blinking	Drive is powered and when blinking is transferring data. NOTE: The blue LED may be on or blinking during any procedure after the Drive is unlocked.
 = Green solid	Unlocked; operation was successful.

¹-For other LED combinations see specific status requests: *Verifying Existing PIN* and *Determining the Version Number* described in this manual.

PINs and Procedures


PIN REQUIREMENTS

Your User PIN or Admin PIN must:

- be between 7-15 digits in length
- not contain only repetitive numbers, e.g. (3-3-3-3-3-3)
- not contain only consecutive numbers, e.g. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)

NOTE: Creating words (using the corresponding number key for each letter) can be more memorable than a string of numbers.

PROCEDURAL CONVENTIONS USED

All procedures below require the Drive to be connected to a computer with the USB cable. LED status shown is what you should see after performing each step. Unless otherwise noted, all procedures start with the Drive locked. []

NOTE: Each step in all procedures listed below have a 10 second window to perform the next step. In general, a blinking LED times out after 10 seconds.

User Mode

New drives are shipped with a default User PIN which is 11223344 (otherwise, your vendor will supply it). We strongly recommend changing the password once it is unlocked.

User PINs

This Section:

- Unlocking the Drive in User Mode
- Changing the User PIN
- Disconnecting from Your Computer
- Locking the Drive without Disconnecting



CAUTION: Risk of loss of data. If you forget your User PIN and no Admin PIN exists, or you forget both PINs, all data will be inaccessible and reformatting will be required.

Unlocking the Drive in User Mode



CAUTION: Possible deletion of data. After ten failed attempts to unlock the Drive, the User PIN and all data on the Drive will be deleted. Refer to *Brute Force Hacking Detection* on page 14.

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

1. Connect the Drive to your computer with the USB cable.
2. Press []
3. Enter the **User PIN***. []
4. Press []

*The factory PIN for **new** drives is 11223344. For other drives, contact your vendor. We strongly recommend changing the password once it is unlocked. See *Changing the User PIN* below.

NOTE: If the Drive still doesn't appear in your computer's file manager, refer to *Troubleshooting* on page 21.

Changing the User PIN

1. Press []
2. Enter the User PIN. []
3. Press [momentarily]
4. After you see then press []
5. Enter the new User PIN []
6. Press []
7. Re-enter the new PIN. []
8. Press [] To use the new PIN unplug and plug the drive back

Note that if a mistake was made while defining a new PIN or the procedure was not completed, the Drive will retain the old PIN.

DISCONNECTING FROM YOUR COMPUTER

Generally, you can just unplug the USB cable. However, some computer systems may require you to click the Safely Remove Hardware/Eject icon within your operating system prior to unplugging the drive cable from your computer. Wait for the red LED to light momentarily indicating it is locked and ready to disconnect from the computer.

LOCKING THE DRIVE WITHOUT DISCONNECTING




USER AND ADMIN MODES: To lock the Drive without unplugging the USB cable, press and hold until the red LED lights (about 4 seconds).

Options for User Mode

The following headings describe enabling options and features requiring only a User PIN. For Administration options see *Options for Admin Mode* on page 11.

This Section:

- Enabling Read-Only in User Mode
- Enabling Read/Write in User Mode
- Setting the Timeout Lock in User Mode
- Disabling the Timeout Lock in User Mode

Procedures that end with these LEDs [ ], will eventually change to  .



















NOTE: All procedures require the Drive to be connected to a computer with the USB cable.

NOTE: Each step in all procedures listed below have a ten second window to perform the next step. In general, a blinking LED times out after ten seconds.

ENABLING READ-ONLY IN USER MODE

The User is able to write content to the Drive and then restrict access to read-only (R-O). Once R-O Mode is activated, access is limited to reading only, until Read/Write is enabled which can be accomplished by a User (or an Administrator, described in the Admin section).



















Setting to Read-Only does not unlock the drive.

1. With the Drive locked, press  []
2. Enter your User PIN. []
3. Press   []
4. Wait for   , then press    [ ]
5. Press 7,6 (R,O for Read-Only) [ ]
6. Press  [ ]

If successful, the next time the Drive is unlocked it will be in R-O Mode as indicated by the **slow blinking** green LED (as well as messages provided by your computer when you try to save or delete a file).

ENABLING READ/WRITE IN USER MODE

Read-Only (Write Restriction) can be turned off restoring Read and Write access. Note that setting the drive to R-W does not unlock the drive.

1. With the Drive locked, press  []
2. Enter your User PIN. []
3. Press   []
4. Wait for   , then press    [ ]
5. Press 7,9 (R,W for Read/Write) [ ]
6. Press  [ ]




















If successful, the next time the Drive is unlocked it will be in Read/Write Mode as indicated by a **solid** green LED.

SETTING THE TIMEOUT LOCK IN USER MODE

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 idle time (no read or write activity).

NOTE: When set in User Mode, the Timeout Lock is only active in User Mode and not Admin Mode.

The default state of the Timeout Lock feature is OFF. The Timeout Lock feature can be set to activate (lock) any time between 1 and 99 minutes.

1. With the Drive locked, press  []
2. Enter your User PIN. []
3. Press   []
4. Wait for   , then press    []
5. Press 8,5 (T,L for Timeout Lock) []
6. Press  []
7. Enter the length of unattended time for Timeout.
Two digits required. [] Examples:
 01 = 1 minute
 99 = 99 minutes
8. Press  [ ]

The Timeout Lock is now set for subsequent Drive use, until changed.

DISABLING THE TIMEOUT LOCK IN USER MODE

Follow the same steps for setting the Timeout Lock (above) and enter **00** for the time delay.

The Timeout Lock is now disabled.



Admin Mode




An Admin PIN is a useful feature, especially for corporate deployment and it can be used to usage policy. For example:

- Recovering data from a Drive and creating a new User PIN in the event that you or an employee has forgotten the User PIN.
- Retrieving data from a Drive if an employee leaves the company.
- Setting policies such as Read-Only or the Timeout Lock.

The Admin PIN can be used to override all User-Mode settings.

Button Pressing Conventions

Many Admin procedures start with pressing and holding a number button down (**1** or **7**, for example) and while holding it, pressing  button: abbreviated in the steps below as: *Press and hold down 7-and then press-.*

In some cases, you must hold down the number while pressing and releasing  button twice: abbreviated as: *Press and hold down 1-and then press- .*

NOTE: All procedures under this heading start with the Drive connected to a computer but still locked, unless otherwise noted.

NOTE: Each step in all procedures listed below have a 10 second window to perform the next step. In general, a blinking LED times out after 10 seconds.

The PIN requirements are the same as User-Mode. Refer to *PIN Requirements* on page 5.

Admin PINs





















CAUTION: Risk of loss of data. If you forget your User PIN and no Admin PIN exists, or you forget both PINs, all data will be inaccessible and reformatting will be required.

This Section:

- Creating an Admin PIN (no User PIN)
- Creating an Admin PIN (User PIN exists)
- Unlocking the Drive in Admin Mode
- Adding or Changing a User PIN in Admin Mode
- Locking the Drive in Admin Mode
- Changing the Admin PIN

CREATING AN ADMIN PIN (NO USER PIN)























The Drive must be locked and have no User PIN.

1. Press  []
2. Press and hold down **1**-and then press-  [ ]
3. Enter a new Admin PIN. [ ]
4. Press  . []
5. Re-enter your new Admin PIN. []
6. Press  . [ momentarily, then  ]
If unsuccessful [ briefly]

NOTE: If a mistake was made or the procedure not completed, no Admin PIN will be created.

CREATING AN ADMIN PIN (USER PIN EXISTS)

The Drive must be locked.










1. Press  []
2. Enter the User PIN []
3. Press   []
4. Wait for   , then press and hold down **1**-and then press-  [ ]
5. Enter a new Admin PIN. [ ]
6. Press  . []
7. Re-enter your new Admin PIN. []
8. Press  . [ ]

NOTE: If a mistake was made or procedure not completed, no Admin PIN will be created.

UNLOCKING THE DRIVE IN ADMIN MODE

















CAUTION: Possible deletion of all data, settings, and both PINs. After ten failed attempts to unlock the Drive, it will reset to the blank factory setting. Refer to *Brute Force Hacking Detection* on page 14.










1. Press and hold down **1**-and then press- [ ]
2. Enter the Admin PIN. [ ]
3. Press  [ momentarily, then ]
If unsuccessful [ briefly]

NOTE: If your computer goes into sleep mode while the Drive is unlocked, the Drive may lock after some time depending on your power management settings regarding the USB port.

ADDING OR CHANGING A USER PIN IN ADMIN MODE

For PIN requirements refer to page 5.

1. With the Drive locked, press and hold down **1**-and then press-  [ ]
2. Enter your **Admin PIN**. [ ]
3. Press   []
4. Wait for   , then press   []

5. Enter a new **User PIN**. []
6. Press   []
7. Re-enter the **User PIN** []
8. Press   [ momentarily, eventually ]



If successful, the User PIN is now added or changed.

LOCKING THE DRIVE IN ADMIN MODE


























Locking the Drive without unplugging the USB cable is the same for both modes. Refer to page 6.

CHANGING THE ADMIN PIN

The Admin PIN cannot be changed from the User mode.

Remember that *Press and hold down 1-and then press- * means ‘hold down #1 button and press the Key button twice.’

For PIN requirements see page 5.

1. With the locked, press and hold down **1**-and then press- [ ]
2. Enter the Admin PIN. [ ]
3. Press   []
4. Wait for   , then press and hold down **1**-and then press-  [ ]
5. Enter a new Admin PIN. [ ]
6. Press   []
7. Re-enter the Admin PIN []
8. Press   [ slowly &  , eventually ]

NOTE: If a mistake is made while defining a new Admin PIN or the procedure is not completed, the Drive retains the old Admin PIN (as well as the old User PIN if one exists).

Options for Admin Mode

The following headings describe enabling options and features requiring only a User PIN.






















This Section:

- Enabling Read-Only in Admin Mode
- Enabling Read/Write in Admin Mode
- Setting the Timeout Lock in User Mode
- Setting the Timeout Lock in Admin Mode

ENABLING READ-ONLY IN ADMIN MODE

NOTE: When Admin restricts access to Read-Only, the User cannot change this setting.

Setting to Read-Only does not unlock the drive.





















1. Press and hold down **1**-and then press- [ 
2. Enter the Admin PIN. [ 
3. Press   [
4. Wait for  , then press    [ 
5. Press 7,6 (R,O for Read-Only) [ 
6. Press  [ slowly &  momentarily, then 

If successful, the next time the Drive is unlocked it will be in R-O Mode as indicated by the **slow** blinking green LED (as well as messages provided by your computer when you try to save or delete a file).

ENABLING READ/WRITE IN ADMIN MODE

Admin can override a User-set Read-Only state by enabling Read/Write using the Admin PIN.

Setting to Read-Write does not unlock the drive.
























1. Press and hold down **1**-and then press- [ 
2. Enter the Admin PIN. [ 
3. Press   [
4. Wait for  , then press    [ 
5. Press 7,9 (R,W for Read/Write) [ 
6. Press  [ slowly & 

If successful, the next time the Drive is unlocked it will be in R/W Mode as indicated by the **solid** green LED.

SETTING THE TIMEOUT LOCK IN ADMIN MODE

To protect against unauthorized access when the Drive is connected to a computer and unattended, it can be set to automatically lock after a preset amount of time.

In its default state, the Timeout Lock feature is turned off. It can be set to activate (lock the Drive) any time between 1 and 99 minutes. Admin Timeout Lock settings will override User settings.

1. Press and hold down **1**-and then press- [ 
2. Enter the Admin PIN. [ 
3. Press   [
4. Wait for  , then press    [ 
5. Press 8,5 (T,L for Timeout Lock) [ 
6. Press  [
7. Enter the length of unattended time for Timeout.
Two digits required. [] Examples:
01 = 1 minute
99 = 99 minutes
8. Press  [ slowly & 

If successful, the Timeout Lock is now set.

DISABLING THE TIMEOUT LOCK IN ADMIN MODE


Follow the same steps for setting the Timeout Lock (above) and enter **00** for the time delay. The Timeout Lock will be disabled.






Managing the Drive

The following headings discuss important, though less common, actions for managing your Drive. Except where noted, all procedures assume your Drive is connected to a computer and locked (red LED).

Verifying which PINs have Been Set

To determine which PINs have been set up:

Press  ; The LEDs display for 10 seconds:

- No PIN exists []
- Only User PIN exists. [ rapidly]
- Only Admin PIN exists. [ rapidly]
- Both PINs exist. [ ]

Deleting all Files in Admin Mode























An Admin operator can delete all data stored on the Drive including User settings and PIN. All Admin settings (and only the Admin settings) will remain on the Drive. The Drive will need to be reformatted. For reformatting, refer to *Reformatting the SecureDrive* on page 15.

NOTE: All procedures require the Drive to be connected to a computer with the USB cable.

NOTE: Each step in all procedures listed below have a 10 second window to perform the next step. In general, a blinking LED times out after 10 seconds.



CAUTION: The 'Delete All' procedure deletes all data, User settings, and formatting. The Drive must be reformatted.

1. With the Drive locked, press and hold down **1**-and then press- [ ]
2. Enter the Admin PIN. [ ]
3. Press   []
4. Wait for   , then press    [ ]
5. Press **3,2** (D,A for Delete All) [ ]
6. Press  [  alternate]
7. Enter the Admin PIN again [  alternate]

8. Press  [ slowly &  momentarily]
If unsuccessful [ briefly]

All data and User settings have now been deleted from the Drive.

Brute Force Hacking Detection

USER

Status: Both Admin and User PINs have been created.

If a User enters an incorrect User PIN ten consecutive times, regardless of the time intervals in between attempts, the Drive's brute force detection will trigger and **the User PIN will be deleted**. All data remains on the Drive and can be accessed by the Admin entering the correct Admin PIN.

Status: Only User PIN have been created.

If a User enters an incorrect User PIN ten consecutive times regardless of the time intervals in between attempts, the Drive's brute force detection triggers and the **User PIN and encryption key will be deleted and all data will become inaccessible and lost forever**. The Drive will need to be formatted before it can be reused. Refer to *Reformatting the SecureDrive* on page 15.

ADMIN

Status: Admin PIN, or Admin and User PINs have been created.

If an Admin enters an incorrect Admin PIN ten consecutive times, regardless of the time intervals in between attempts, the Drive's brute force detection triggers and **both the User and Admin PINs and the encryption key will be deleted and all data will become inaccessible and lost forever**. The Drive will need to be formatted before it can be reused. Refer to *Reformatting the SecureDrive* on the next page.

This table illustrates the different PIN states and what happens when Hacking Detection triggers.







Hacking Detection		
PIN attempted to use to unlock	PINs setup on the Drive at the time	After 10 consecutive incorrect PIN entries, the brute force mechanism triggers and does this:
User PIN	Admin & User PINs	The User PIN will be deleted. All data will remain on the Drive and can only be accessed by the Admin entering the correct Admin PIN.
User PIN	User PIN Only	The encryption key will be deleted, and all data will be inaccessible and lost forever including the PINs.
Admin PIN	Admin & User PINS	
Admin PIN	Admin PIN Only	

Resetting (Deleting) the Drive



CAUTION: Resetting the Drive will delete all data stored on it including both PINs. After Resetting, the Drive must be formatted (initialized). (See heading *Reformatting the Drive* after this procedure.)

In the event that both the Admin and User PINs have been forgotten, or you want to delete all data stored on the Drive including the PINs, you can perform the following reset function. It also removes the encryption, requiring the Drive to be reformatted to generate new encryption—to format the Drive refer to the heading *Reformatting the SecureDrive* below.










1. With Drive locked, press and hold down **7**-and then press-**0** [  alternately]*
2. Press **999** [  alternately]
3. Press and hold down **7**-and then press-**0** [ ]

The Drive is now blank and locked.

*If only red LED lights, the Drive may already be blank.

Creating a User PIN after a Reset (blank Drive)

Follow this procedure when the Drive is blank: such as after it has been reset or Hacking Detection has triggered.

1. Connect the Drive to your computer with the USB cable.
2. Press **0** []
3. Wait four seconds, press **0 0** []
4. Enter your desired **User PIN**. []
5. Press **0 0** []
6. Re-enter the new **User PIN**. []
7. Press **0 0** [ fades off, then ]
If unsuccessful [ fades off, then ]

Note that the Drive still requires formatting.

Reformatting the SecureDrive

In the event that hacking detection has been triggered or the Drive has been reset, all data on the Drive will be lost forever. The Drive must then be reformatted.

To initialize your SecureDrive, do the following:

FOR A WINDOWS OS

Admin permissions on the PC is required for this procedure.

1. Connect the Drive to your computer with the USB cable.

2. Unlock the drive with either User or Admin PIN. (To create a User PIN if you have not already done so, see *Creating a User PIN after a Reset (blank Drive)* on page 15.)
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 the Initialize Disk dialog doesn't popup, R-click the 'Unknown' (or 'Not Initialized'), usually Disk 1, and click Initialize disk.

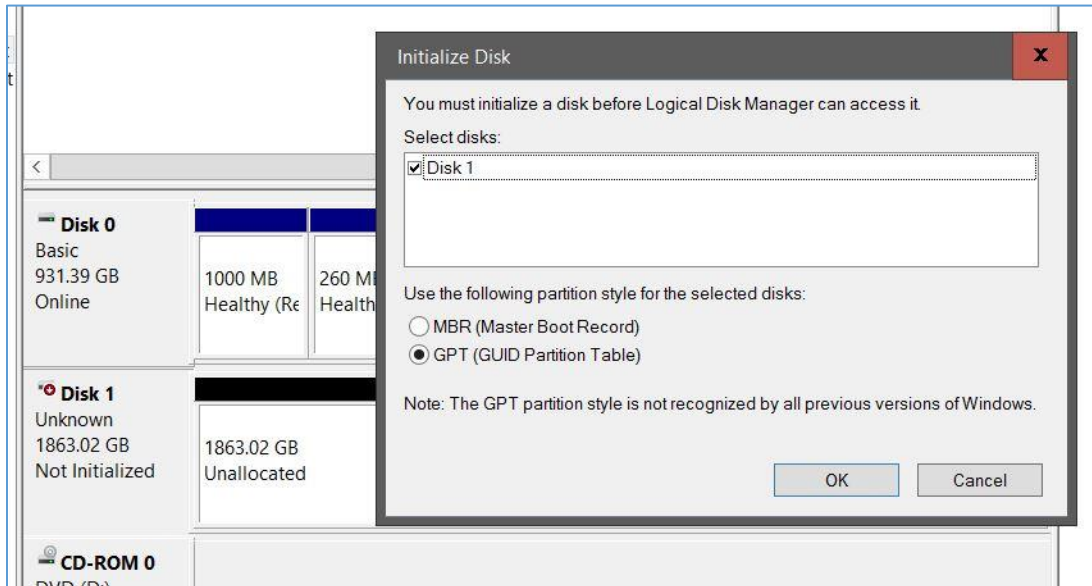


Figure 2: Initializing the Secure Drive disk (shown here as Disk 1).

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

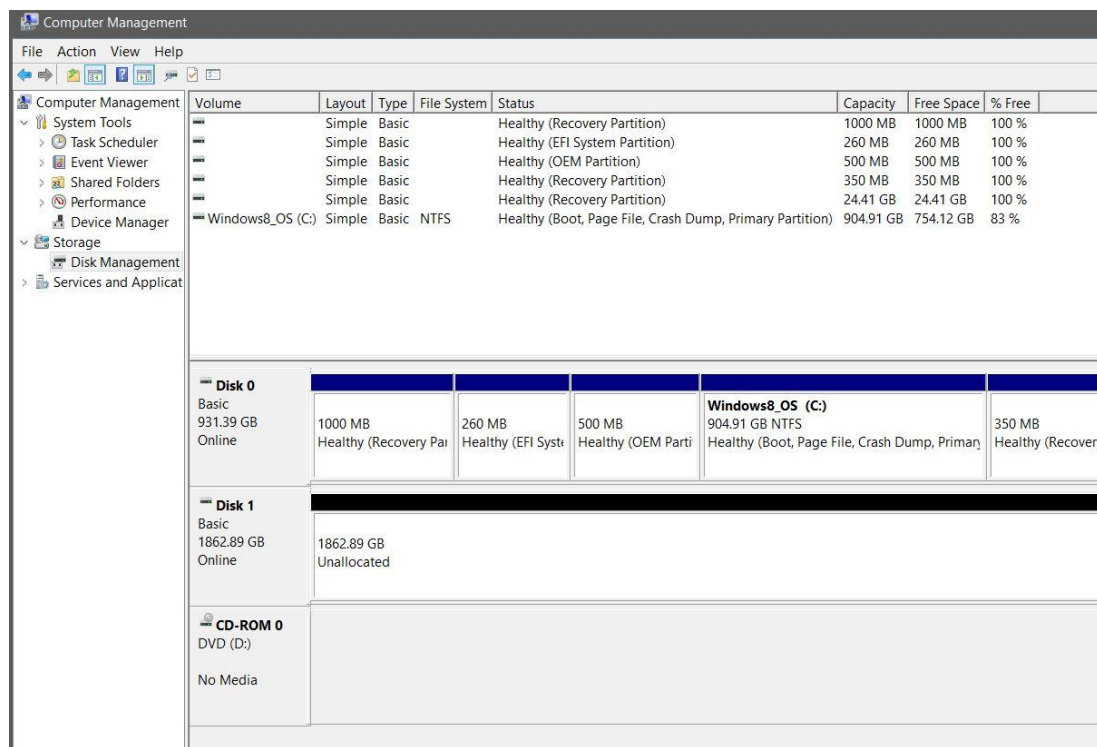


Figure 3: The SecureDrive is displayed here as “Disk 1.” It is Online but not yet allocated. (Windows 10 shown here.)

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 SecureDrive is formatting the blue LED blinks.
12. Click Finish to end and close the Wizard.

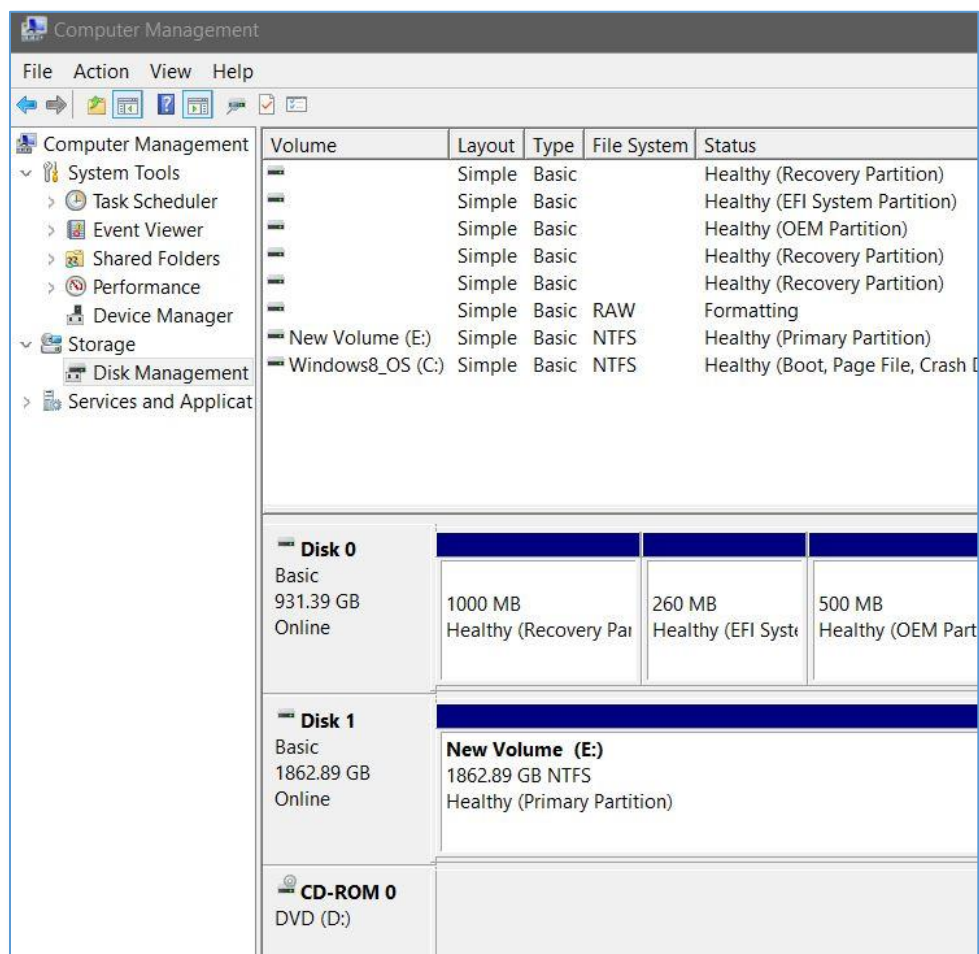


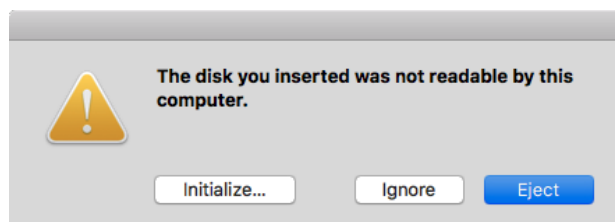
Figure 4: The SecureDrive is displayed here as “Disk 1.” It is Online and allocated (Healthy) and ready for use.

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 and Green LED lights.

FOR MAC OS

1. Connect to a Mac computer’s USB port.
2. Unlock the drive with either User or Admin PIN. (To create a User PIN if you have not already done so, see *Creating a User PIN after a Reset (blank Drive)* on page 15.)
3. Click Initialize in the popup message (shown below). The Disk Utility Dialog displays.



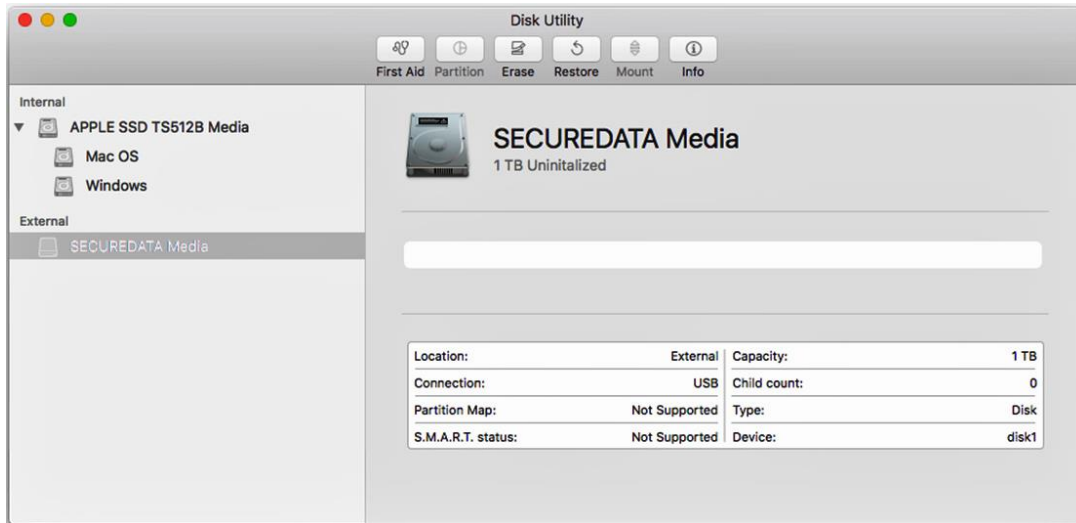
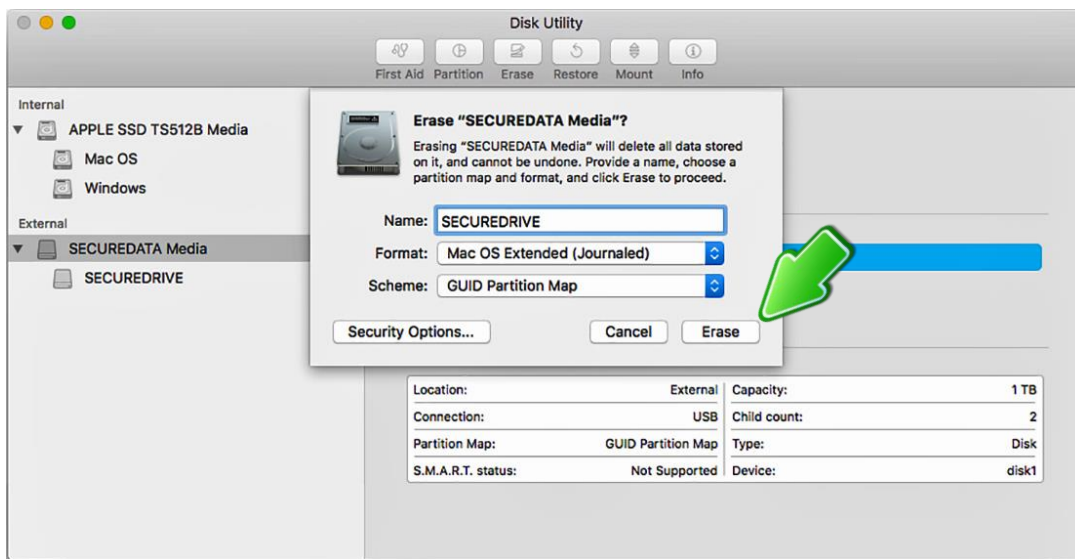


Figure 5: The Disk Utility Dialog.

4. Click Erase. The system begins erasing the external Drive.



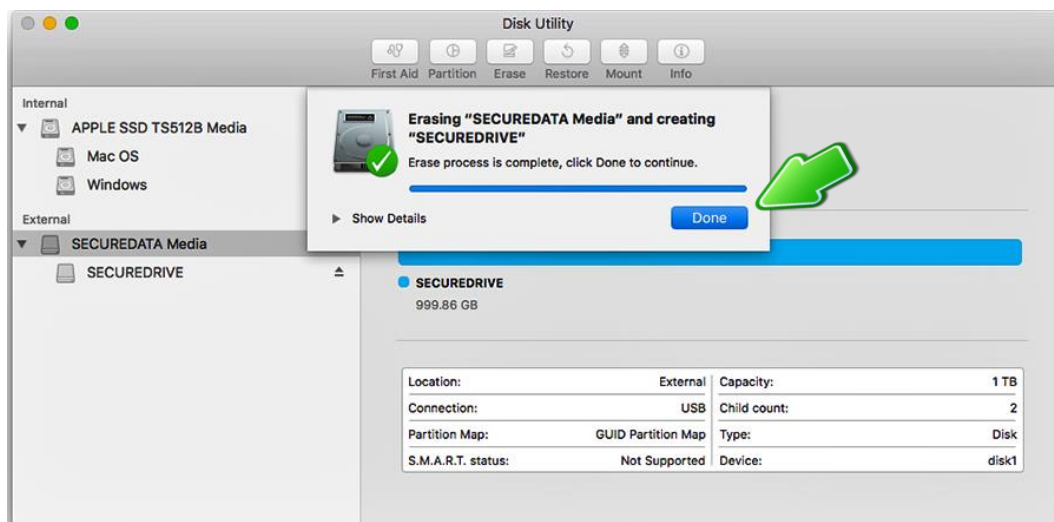
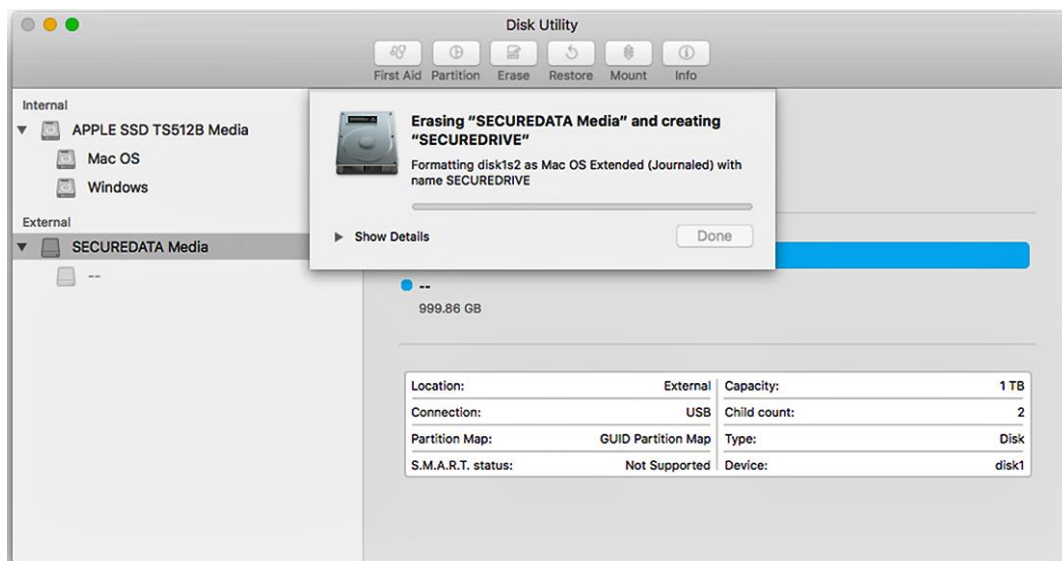


Figure 6: *SecureDrive* displays under the list of External Drives when done (as well as on the desktop).

5. Click Done in the message dialog when available.
SecureDrive 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.

- Version Number (refer to *Determining the Version Number* below)
- Serial Number (S/N) on the back of the device

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 needs to be formatted—no data exists. It may have been reset. To format the Drive Refer to *Reformatting the SecureDrive* on page 15.

■ If you think your keypad is faulty, contact Technical Support, page 20.

DETERMINING THE VERSION NUMBER

In User Mode:

1. With the Drive locked, press  
2. Enter your **User PIN**. 
3. Press   
4. Wait for  , then press     
5. Press **8,6** (**V,N** for Version Number)  
6. Press  [All LEDs blink once together]






Then the **Red** will blink the number of times that represent the major version number (left of the decimal point), and the **Green** will blink the number of times that represent the update version (right side of the decimal point).

When the sequence has ended All LEDs blink once together, then  .

EXAMPLE: if the version number is 1.7, the red LED will blink once and the green LED will blink seven times.



In Admin Mode:

1. Press and hold down **1**-and then press-  
2. Enter the Admin PIN.  
3. Then follow steps 3 and on for *User Mode* above.

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, 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.

SecureDrive™ 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.

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

FC CE RoHS

