SECURE USB

KEYPAD

SecureUSB KP
USER MANUAL

SECURE DATA

Contents

SecureUSB Overview

Thank you for purchasing the SecureUSB KP Model ('USB' and 'USB KP' hereafter). It's an easy to use, hardware encrypted, password activated USB 3.0 Flash drive, with an onboard alphanumeric, 11 button keypad for OS-independent user-authentication.

The USB uses XTS-AES 256-bit hardware encryption which encrypts all data on it in real time. It requires neither software drivers nor updates and works on all computers 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 PIN (Personal Identification Number).

The SecureUSB KP incorporates a rechargeable battery allowing you to enter a PIN into the keypad before inserting the USB KP into a computer USB port. The USB 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 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 access (except for during keypad 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 SecureUSB KP (with PDF User Manual)
- 1 Quick Start Guide

Safety Information

This icon ⚠ indicates important information regarding the safety of the product and your data (Caution messages). Please be mindful of these messages. Contact support if you have questions.

PRECAUTIONS

- Do not expose the USB to water or moisture.
- Resetting the USB will delete all stored data as well as all PINs and settings.
- Forgetting your PIN 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 NOTICE

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

SecureUSB Features

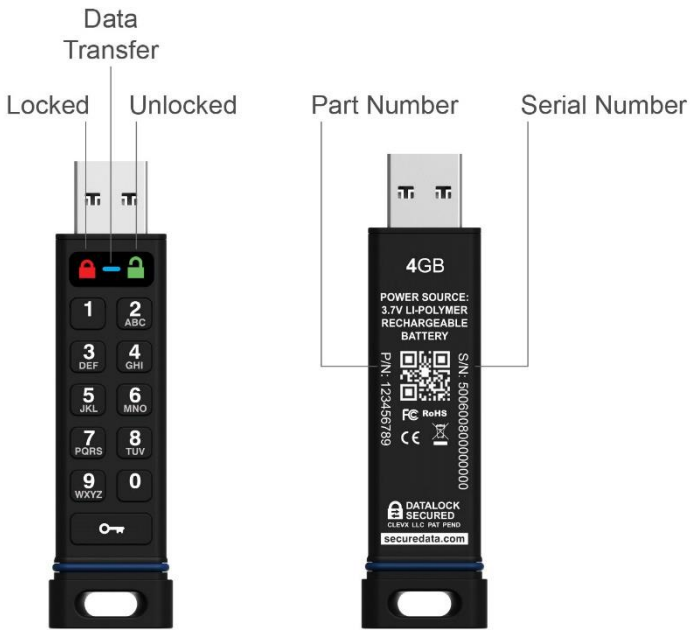


Figure 1: The USB KP Layout.

LED Interpretations

LEDs on the SecureUSB are represented here by colored icons.

LED	Meaning
no LEDs lit	USB is unplugged and locked
(blink all together once)	Plugged into computer; momentary LED test
= **Red** solid	Locked
= **Red** blinking[1]	Locked, ready for input (other than a Setting code). Also, specific feedback[1]
= **Green** blinking	Unlocked and ready for keypad input
= **Green** blinking **slowly**	Unlocked for use in Read-Only Mode
= **Green** solid	Temporarily unlocked (30 seconds) and not inserted into a computer
Blue & **Green** solid **Blue** blinking & **Green** solid	USB is plugged into a computer and unlocked NOTE: The blue LED may be on solid or blinking during any procedure after the USB is unlocked.
Blue blinking slowly	USB is plugged in to computer and locked
Blue blinking then **Red** solid	Procedure failed.

[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. (3-3-3-3-3-3-3)
- 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

- **All procedures must be performed prior to inserting the USB KP into a computer**.
- The LED status shown in these procedures is what you should see after performing each step.
- Unless otherwise noted, all procedures start with the USB locked.
- In this manual, 🔑🔑 means press the key button twice; 🔑🔑🔑 means press it three times.

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

After unlocking the USB, it will lock again if not inserted into a computer within 30 seconds.

Cancelling a Procedure

To cancel most procedures prior to finishing, press and hold 🔑 for six seconds. The exception are procedures for setting options (🔑🔑🔑) which you can just let time out between steps.

User Mode

New USBs 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 USB in User Mode
- Locking the USB KP
- Changing the User PIN
- Disconnecting from Your Computer

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 USB in User Mode

CAUTION: Possible deletion of data. After ten failed attempts to unlock the USB, the User PIN and all data on the USB will be deleted. Refer to *Brute Force Hacking Detection* on page 15.

NOTE: If the USB is inserted into a computer when locked, its contents does not appear in your computer's File Manager (Explorer or Finder).

1. Prior to inserting the USB into a computer, press [ ]
2. Enter the **User PIN***. [ ]
3. Press [ ]
4. Within 30 seconds, insert the USB drive into your computer. [ ]

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

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

Changing the User PIN

1. Unlock the USB (see procedure above except don't insert into your computer).[ ]
2. Within 30 seconds, press [ ]
3. Enter the new User PIN. [ ]
4. Press [ ] ;
   Or [ ] if PIN does not meet requirements.
5. Re-enter the new PIN. [ ]

6. Press 🔑🔑 [🔒 then 🔓] ;
   Or [🔓] if re-entry doesn't match;
   Or [▬ then 🔒 momentarily] if any error was made, the new PIN was not created.
   NOTE: If the PIN was re-entered incorrectly, the USB will not accept the new PIN but will remain unlocked with the original PIN (returning to the initial state after step 1).

If successful and the USB is inserted into your computer within 30 seconds, it will be unlocked.

Locking the USB KP

Unplugging the USB KP from your computer will automatically lock it.

Disconnecting from Your Computer

Generally, you can just unplug the USB as long as the blue LED is not blinking and it will lock automatically. However, some computer systems may require you to click the Safely Remove Hardware/Eject icon within your operating system prior to unplugging it from your computer. Wait for the indication from your operating system. [▬]

User Mode Options

The following headings describe options and features requiring only a User PIN. For Administration options see *Admin Mode* on page 12.

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

NOTE: Each step in all procedures have a ten second window to start the step after it. 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 USB 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).

1. Unlock the USB with your User PIN. [🔓]. (Refer to page 6, except don't insert into your computer.)
2. Press 🔑🔑🔑 [▬ 🔓]
3. Press **7**,**6** (R,O for Read-Only) [▬ 🔓]
4. Press 🔑 [🔒 briefly, then 🔓] (changes to 🔓 if subsequently inserted into your computer)

The USB drive is unlocked in Read-Only Mode and for thirty seconds is ready to be inserted into your computer. If not inserted, it will still be in Read-Only Mode the next time it is unlocked.

NOTE: When plugged into your computer in R-O Mode, the green LED blinks very slowly to distinguish it from the regular R/W Mode. Also, if you try to save or delete a file your computer will display a message.

Enabling Read/Write in User Mode

Read-Only (Write Restriction) can be turned off restoring Read/Write access.

1. Unlock the USB with your User PIN. []
2. Press  []
3. Press **7**,**9** (R,W for Read/Write). []
4. Press  [ briefly, then ]

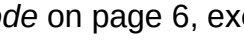
The USB KP is unlocked in Read/Write Mode and for thirty seconds is ready to be inserted into your computer. If not inserted it will still be in Read/Write Mode the next time it is unlocked.

Setting the Timeout Lock in User Mode

To protect against unauthorized access when the USB drive is connected to a host computer and unattended, the USB drive can be set to automatically lock after a pre-set amount of idle time (no access or write activity).

NOTE: When set in User Mode, the Timeout Lock is only active in User Mode and not Admin Mode (unlocked with an Admin PIN).

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. Unlock the USB with your User PIN. [] (Refer to *Unlocking the USB in User Mode* on page 6, except don't insert into your computer.)
2. Press  []
3. Press **8**,**5** (T,L for Timeout Lock). []
4. Press  []
5. Enter the length of unattended time for Timeout.
   Two digits required. []
   Examples:
   01 = 1 minute
   99 = 99 minutes
6. Press  [ briefly, then ]

The Timeout Lock is now set and for thirty seconds is ready to be inserted into your computer. If not inserted it will retain your Timeout Lock settings 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

When unlocked with and Admin PIN the USB KP is in *Admin Mode*. Admin Mode is especially useful for corporate deployment and it can be used to ensure policy. For example:

- Recovering data from a USB drive and creating a new User PIN in the event that you or an employee has forgotten the User PIN.
- Retrieving data from a USB drive if an employee leaves the company.
- Setting policies such as 'Read-Only' or 'Time Out Lock'
- The Admin PIN can be used to override all User 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 USB unplugged from a computer.**

NOTE: Each step in all procedures listed below has a 10 second window to start the step after it. 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
- Creating or Changing a User PIN in Admin Mode
- Changing the Admin PIN
- Unlocking the USB in Admin Mode
- Locking the USB in Admin Mode

The following table displays actions that are possible when different combinations of PINs are set:

User PIN	Admin PIN	Possible Actions
NOT SET	NOT SET	• Can set either **User** or **Admin PIN** • Cannot access USB until **User** or **Admin PIN** is defined
SET	NOT SET	• Can change **User PIN** when unlocked as User • Can set **Admin PIN** when unlocked with **User PIN** • Can access data when unlocked as User
NOT SET	SET	• Can create **User PIN** • Can unlock USB with **Admin PIN** • Can change **Admin PIN** when unlocked as Administrator • Can perform Administrator commands
SET	SET	• Can unlock USB and access data with either **User** or **Admin PIN** • Can change **User PIN** when unlocked as User • Can change **Admin PIN** when unlocked as Administrator

CREATING AN ADMIN PIN

1. Unlock with your User PIN (Refer to *Unlocking the USB in User Mode* on page 6, except don't insert into your computer). [ ]
2. Press and hold down **1**-and then press [rapidly]
3. Enter a new Admin PIN. [rapidly]
4. Press . [ ];
   Or if the PINs don't match [ ] and no Admin PIN is saved.
5. Re-enter your new Admin PIN. [ ];
   Or if the PINs don't match [ ] and no Admin PIN is saved.
6. Press . [momentarily, then]
   If unsuccessful [briefly]

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

UNLOCKING THE USB IN ADMIN MODE

CAUTION: Possible deletion of all data, settings, and both PINs. After ten failed attempts to unlock the USB, it will reset to the blank factory setting. Refer to *Brute Force Hacking Detection* on page 15.

NOTE: Unlocking the USB drive with the Admin PIN will delete the User PIN. For security reasons, we highly recommend that a new User PIN be created immediately after unplugging the USB drive. Refer to the next heading on this page.

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

Insert into your computer within 30 seconds.

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

CREATING OR CHANGING A USER PIN IN ADMIN MODE

For PIN requirements refer to page 5.

1. Unlock the USB KP with the Admin PIN. [ ] (Refer to the previous procedure.)
2. Press [ ]
3. Enter a new **User PIN**. [ ]
4. Press [ ]
5. Re-enter the **User PIN** [ ]
6. Press [briefly];
   Or if the PIN does not meet the requirements [ ]
   If unsuccessful, such as the PINs don't match [briefly]

If successful, the User PIN is now added or changed (and the USB is still locked). To verify which PINs currently exist, see *Verifying which PINs have Been Set* on page 14.

LOCKING THE USB IN ADMIN MODE

The procedure for locking the USB KP is the same for both modes, User and Admin. Refer to *Locking the USB KP* on page 7.

CHANGING THE ADMIN PIN

NOTE: Unlocking the USB KP with the Admin PIN will delete the User PIN. For security reasons, we highly recommend that a new User PIN be created immediately after this procedure.

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. Unlock the USB KP with your Admin PIN. [🔓]
2. Press and hold down **1**-and then press 🔑🔑 [🔒 ➖ rapidly]
3. Enter a new Admin PIN. [🔒 ➖ rapidly]
4. Press 🔑🔑 [🔓]
5. Re-enter the Admin PIN. [🔓]
6. Press 🔑🔑 [🔒 briefly, then 🔓];
   Or, if unsuccessful, such as PINs don’t match, [🔓]

NOTE: If a mistake is made while defining a new Admin PIN or the procedure is not completed, the USB retains the old Admin PIN.

Admin Mode Options

The following headings describe enabling options and features requiring an Admin PIN.

NOTE: Unlocking the USB KP with the Admin PIN will delete the User PIN (regardless of the procedure being performed). For security reasons, we highly recommend that a new User PIN be created immediately after unplugging the USB KP.

This Section:

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

1. Unlock the USB KP with the Admin PIN. [🔓]
2. Press 🔑🔑🔑 [➖ 🔓]
3. Press **7**,**6** (R,O for Read-Only) [➖ 🔓]

4. Press 🔑 [🔒 briefly, then 🔓]

The USB KP is now unlocked in Read-Only Mode and for thirty seconds is ready to be inserted into your computer. If not inserted it will still be in Read-Only Mode the next time it is unlocked.

NOTE: When plugged into your computer in R-O Mode, the green LED blinks very slowly to distinguish it from the regular R/W Mode. Also, if you try to save or delete a file your computer will display a message.

ENABLING READ/WRITE IN ADMIN MODE

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

1. Unlock the USB KP with the Admin PIN. [🔓]
2. Press 🔑🔑🔑 [▬ 🔓]
3. Press **7**,**9** (R,W for Read/Write) [▬ 🔓]
4. Press 🔑 [🔒 briefly, then 🔓]

The USB KP is unlocked in Read/Write Mode and for thirty seconds is ready to be inserted into your computer. If not inserted it will still be in Read/Write Mode the next time it is unlocked.

SETTING THE TIMEOUT LOCK IN ADMIN MODE

To protect against unauthorized access when the USB KP is connected to a computer and idle, 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 USB) any time between 1 and 99 minutes. Admin Timeout Lock settings will override User settings.

1. Unlock the USB KP with the Admin PIN. [🔓] (Refer to *Unlocking the USB in Admin Mode* on page 11.)
2. Press 🔑🔑🔑 [▬ 🔓]
3. Press **8**,**5** (T,L for Timeout Lock). [▬ 🔓]
4. Press 🔑 [🔓]
5. Enter the length of idle time for Timeout.
   Two digits required. [🔓]
   Examples:
   01 = 1 minute
   99 = 99 minutes
6. Press 🔑 [🔒 briefly, then 🔓]

The Timeout Lock is now set and for thirty seconds is ready to be inserted into your computer. If not inserted it will retain your Timeout Lock settings until changed.

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 USB

The following headings discuss important, though less common, actions for managing your USB. All procedures are performed before inserting the USB KP into a computer.

Verifying which PINs have Been Set

To determine which PINs have been set:

Press 🔑 ; These LEDs display for 10 seconds:

- No PIN exists [🔴]
- Only User PIN exists. [🔴]
- Only Admin PIN exits. [🔵]
- Both PINs exist. [🔴 🔵]

Deleting all Files in Admin Mode

An Administrator can delete all data stored on the USB KP including User settings and PIN. All Admin settings (and only the Admin settings) will remain on the USB. For further use, the USB will need to be reformatted. For reformatting, refer to *Reformatting the SecureUSB* on page 16.

NOTE: All procedures must be performed before inserting into a computer.

NOTE: Each step in all procedures below has a 10 second window to start the step after it. In general, a resulting status (indicated by the LEDs) times out after 10 seconds.

⚠ **CAUTION**: The 'Delete All' procedure deletes all data, User settings, and formatting. The USB must be reformatted for further use.

1. Unlock the USB KP with the Admin PIN. [🟢]
2. Press 🔑🔑🔑 [🔵 🟢]
3. Press **3**,**2** (D,A for Delete All). [🔵 🟢]
4. Press 🔑 [🔴 🟢 alternately]
5. Enter the Admin PIN again. [🔴 🟢 alternately]
6. Press 🔑 [🔴 & 🟢 momentarily]
   If unsuccessful [🟢]

All data and User settings have now been deleted from the USB KP. The next time you insert the USB KP into your computer, your system will generally prompt you to reformat it. Refer to *Reformatting the SecureUSB* on page 16.

Brute Force Hacking Detection

Entering a User PIN

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 USB's brute force detection will trigger and **the User PIN will be deleted**. All data remains on the USB and can be accessed by the Admin after entering the correct Admin PIN.

Status: Only User PIN has been created.

If a User enters an incorrect User PIN ten consecutive times regardless of the time intervals in between attempts, the USB'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 USB will need to be formatted before it can be reused. Refer to *Reformatting the SecureUSB* on page 16.

Entering an Admin PIN

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 USB'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 USB will need to be formatted before it can be reused. Refer to *Reformatting the SecureUSB* 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 USB 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 USB 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 SecureUSB

CAUTION: Resetting the USB will delete all data stored on it including both PINs. After Resetting, the USB must be formatted (initialized).

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

1. Press and hold down **7**-and then press [alternately*]
2. Press **999**. [alternately]
3. Press and hold down **7**-and then press [momentarily]

The USB is now blank and locked.
*If only the red LED lights, the USB may already be blank.

Reformatting the SecureUSB

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

CAUTION: Loss of data. All data and settings will be deleted from the USB KP when formatted, whether or not the Brute Force Hacking Detection was triggered or not.

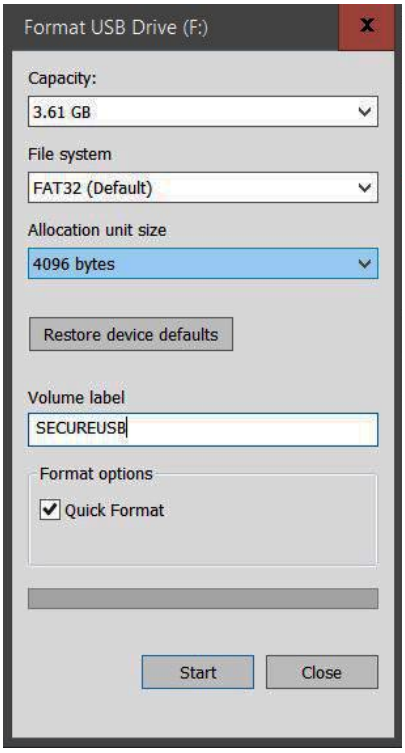
To initialize (reformat) your SecureUSB, do the following:

For a Windows OS

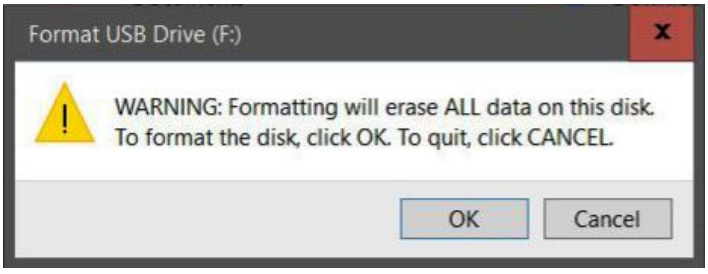
Admin permission on the PC is required for this procedure.

1. Unlock the USB with the default User PIN (or the Admin PIN if all files were deleted with the Admin PIN).
   Refer to *Unlocking the USB in User Mode* on page 6,
   or to *Unlocking the USB in Admin Mode* on page 11.
2. Insert the USB into your computer.
3. In the popup message click Format Disk.

4. Select FAT32 or NTFS depending on your needs.
5. Enter a Volume Label (optional) and click Start.



6. At the popup warning message, click OK to continue with formatting the drive. **This procedure will erase ALL data on the USB KP**.



7. The procedure will finish formatting the USB KP and confirm that formatting has been completed. While formatting, the blue LED blinks.

8. Click OK.

In the Event that the Formatting Wizard Doesn't Display

1. In File Explorer, right click This PC and then click Manage in the drop-down menu.
2. Click Disk Management. You may need to wait while the screen populates.

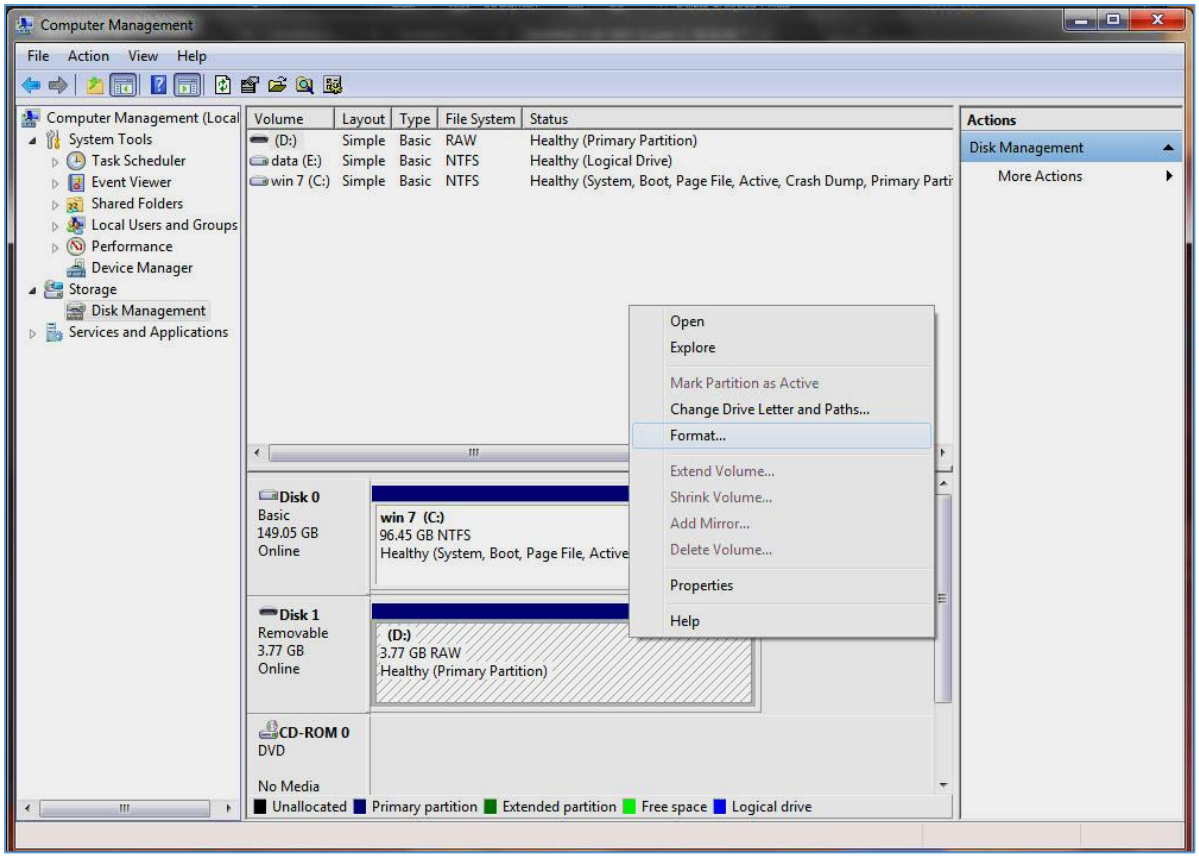
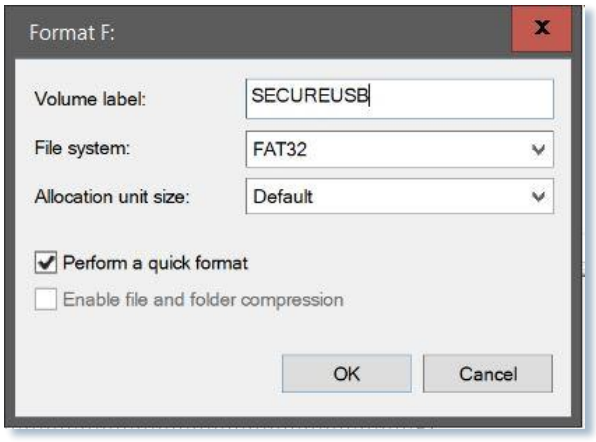


Figure 2: Initializing the Secure USB KP (shown here as Disk 1). Until initialized it displays as RAW. (The hash marks indicate an unallocated drive.)

3. In the blank (hashed) area of the unallocated section, right click the Removable drive and click Format.

NOTE: If the Format command is unavailable (dimmed), the drive may be Write-protected. Remove the drive and then refer to either *Enabling Read/Write in User Mode* on page 8 or *Enabling Read/Write in Admin Mode* on page 13.

4. In the Format window, enter a Volume label (optional) and then select FAT32 or NTFS.



5. Click OK. This will erase ALL data on the drive (as stated on the popup message).
6. Click OK to the popup warning message.

The USB LEDs display  when complete (not blinking). The computer will generally return to the Computer Management window.

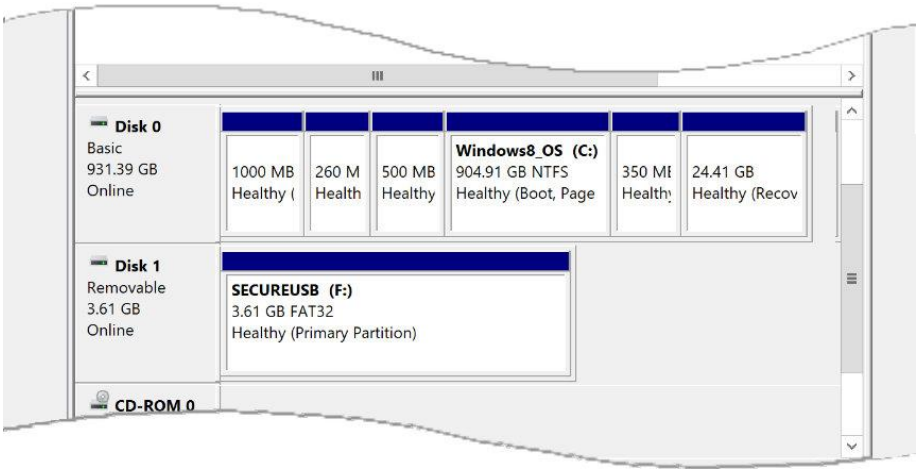


Figure 3: The SecureUSB is displayed here as “Disk 1.” It is Online and allocated (Healthy) and ready for use.

7. Close the Computer Management dialog if it’s still open.

When finished the New Volume (usually E) reads Healthy and another File Explorer window opens to display the USB contents.

For Mac OS

1. Unlock the USB with the default User PIN (or the Admin PIN if all files were deleted with the Admin PIN).
   Refer to *Unlocking the USB in User Mode* on page 6,
   or to *Unlocking the USB in Admin Mode* on page 11.
2. Insert the USB KP into your Mac within thirty seconds (green LED still lit).

3. Click Initialize in the popup message (shown below). The Disk Utility Dialog displays.

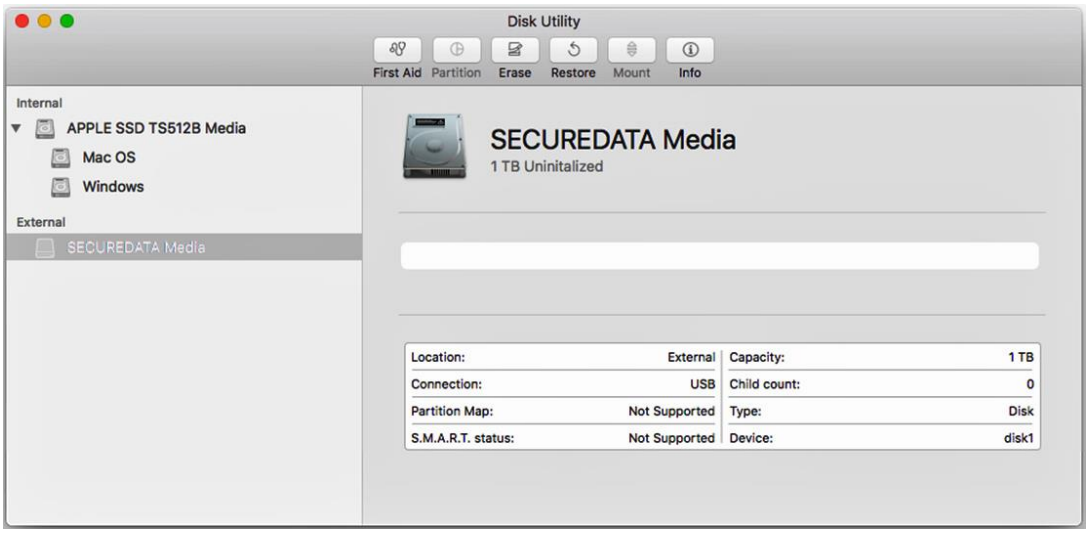
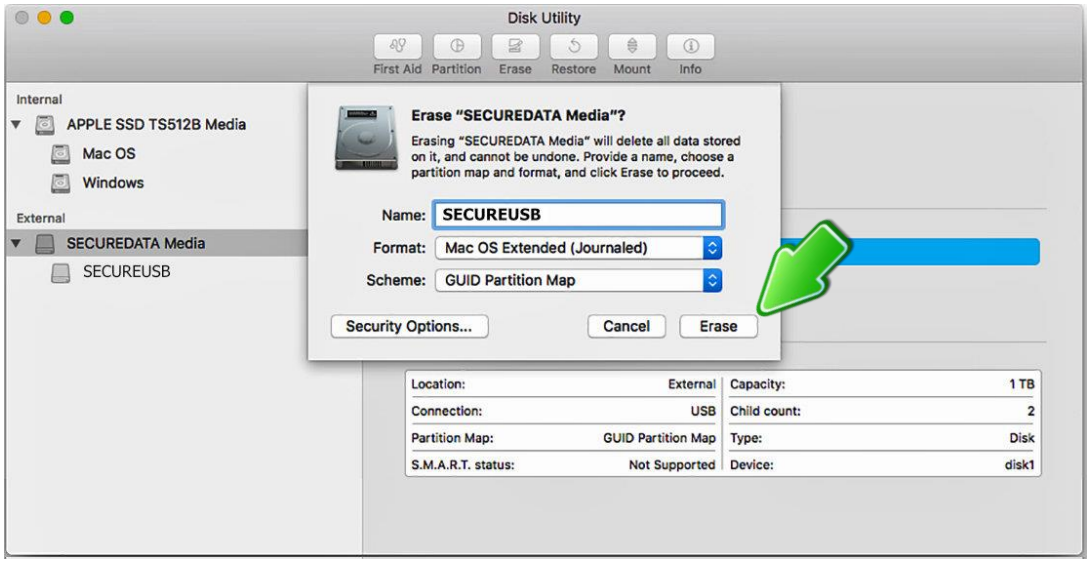
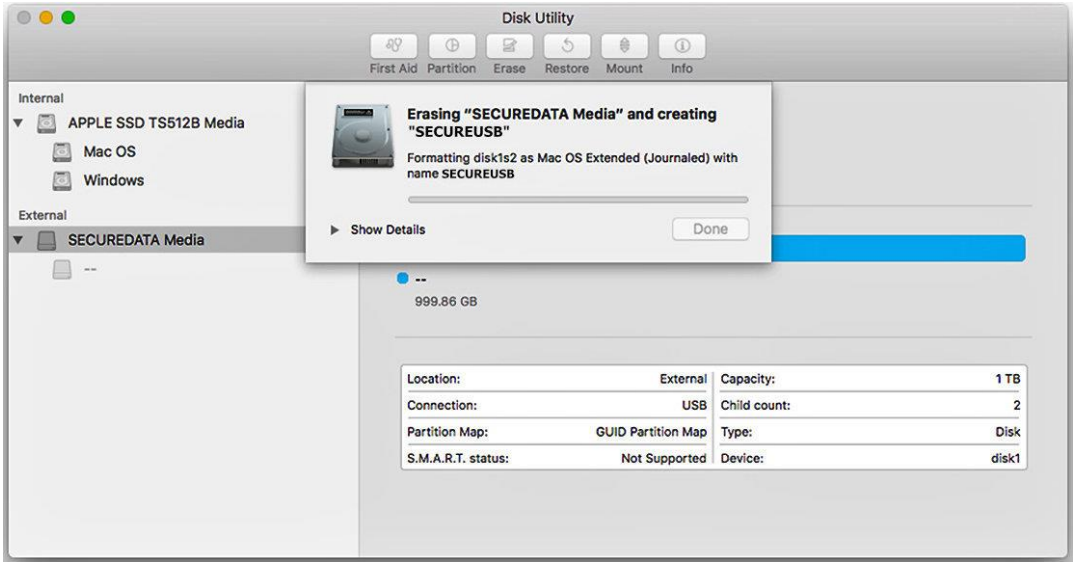


Figure 4: The Disk Utility Dialog. Make sure the correct drive is highlighted (There is only one External drive listed in this image).

4. Ensure that your SecureData USB KP is highlighted in the list of External drives and click Erase. The system begins erasing the external USB.





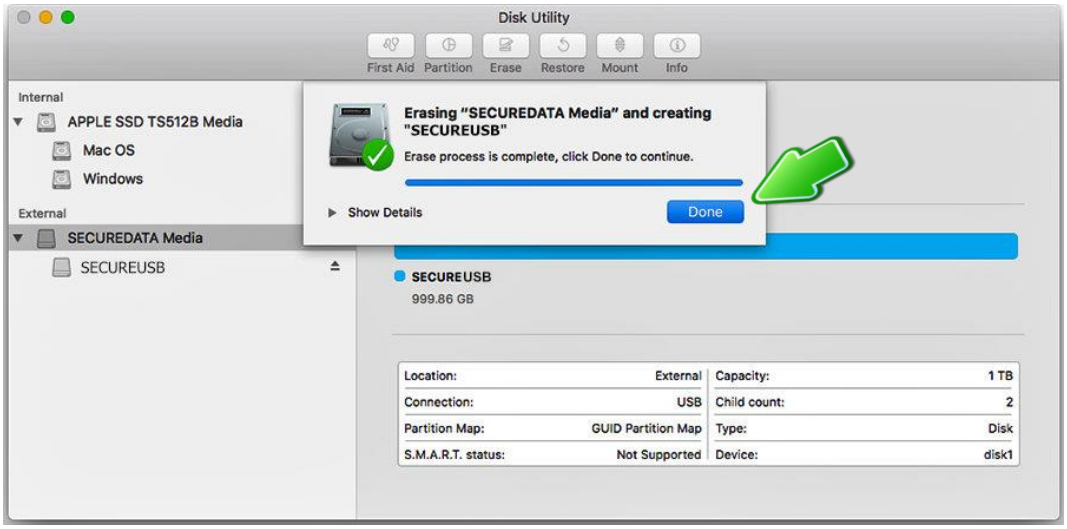


Figure 5: *SecureUSB* displays under the list of External drives when done (as well as on the desktop).

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

DETERMINING THE VERSION NUMBER

In User Mode:

1. Unlock the USB with your User PIN. [ ] (Refer to *Unlocking the USB in User Mode* on page 6.)
2. Press [ ]
3. Press **8,6** (V,N for Version Number). [ ]
4. Press [All LEDs briefly 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,

In Admin Mode:

1. Unlock the USB with your Admin PIN. [ ] (Refer to *Unlocking the USB in Admin Mode* on page 11.)
2. Press [ ]
3. Then follow the *User Mode* procedure above from step 3 on.

FAQs

Q What's the difference between *Deleting All Files* and *Resetting the SecureUSB*?

A *Deleting All Files* can only be done by an Admin and requires and Admin PIN. After deletion, the Admin PIN remains intact.
Resetting the drive can be performed by the User or Admin as neither PIN is required. Both PINs will be deleted and the default (factory) User PIN will be re-instated.

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.

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

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