



User Manual

**Rocstor DataSecure FX5 Encrypted USB Flash Drive**  
**FIPS 140-2 Level 3\* Validated**



# TABLE OF CONTENTS

**SECTION 1: DATASECURE OVERVIEW ..... 2**

SecureUSB Features .....3

PIN Requirements.....4

Procedural Conventions .....4

Cancelling a Procedure.....4

**SECTION 2: USER MODE..... 5**

Unlocking the USB in User Mode .....5

Changing the User PIN.....5

User Mode Options.....6

**SECTION 3: ADMIN MODE ..... 8**

Button Pressing Conventions .....8

Admin PINs.....8

Admin Mode Options.....11

**SECTION 4: MANAGING THE USB ..... 13**

Verifying which PINs have Been Set.....13

Deleting all Files in Admin Mode .....13

Brute Force Hacking Detection .....14

Resetting (Deleting) the SecureUSB .....15

Reformatting the SecureUSB .....15

**SECTION 5: CONTACT AND WARRANTY INFORMATION ..... 20**

Contact Information.....20

Warranty and RMA Information .....20

## SECTION 1: SECUREUSB KP OVERVIEW

Thank you for purchasing the DataSecure FX5 Model. 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 SecureData FX5 incorporates a rechargeable battery allowing you to enter a PIN into the keypad before inserting the FX5 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 Technical Support at [support@rocstor.com](mailto:support@rocstor.com).


### 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 DataSecure FX5 (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.

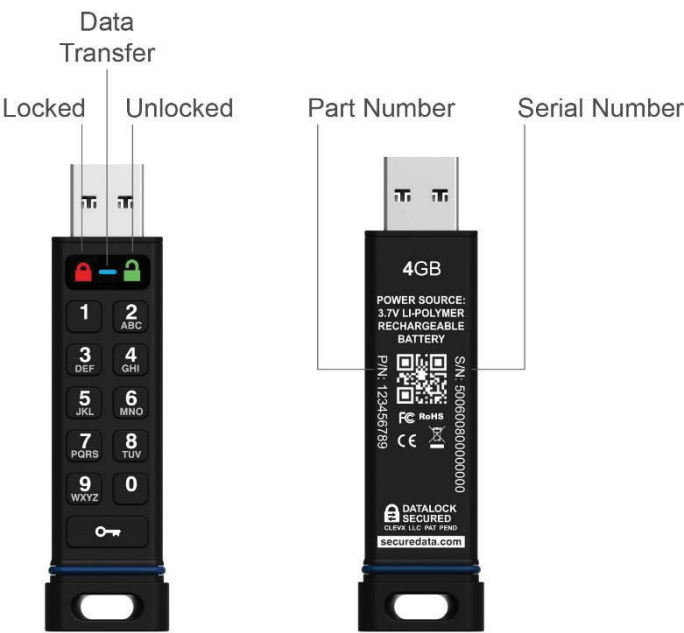
### Precautions

-  Do not expose the USB to water or moisture. USB is IP57 rated which, with the protective sleeve on, is dust protected and water resistant up to 1 meter (approx. 3 feet) for 30 minutes.
-  Resetting the USB will delete all stored data as well as all passwords.
-  Forgetting your password will render the USB inaccessible. There is no 'backdoor.'
-  Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the device.

### EMI 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.

# DataSecure FX5 Features



## LED Interpretations

LEDs on the SecureUSB are represented here by colored icons.

| LED   | Meaning   |
|---|---|
| no LEDs lit   | USB is unplugged and locked   |
| <br>(blink all together once)  | Plugged into computer; momentary LED test   |
|  = Red solid   | Locked  |
|  = Red blinking <sup>1</sup>   | Locked, ready for input (other than a Setting code). Also, specific feedback <sup>1</sup>   |
|  = 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  |
| <br>Blue & Green solid<br><br>Blue blinking & Green solid | USB is plugged into a computer and unlocked<br>NOTE: The blue LED may be on solid or blinking during any procedure after the USB is unlocked. |
| <br>Blue blinking then Red solid   | Procedure failed or the drive is locked and the battery is charging.  |

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

## 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

---

**Note:** 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.

## SECTION 2: User Mode

This section describes how to unlock and lock the USB, change the PIN, and disconnecting the USB from your computer in User Mode.



**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.



**CAUTION:** Loss of data will occur. 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 14.

### Unlocking the USB in User Mode

**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).

| STEPS   | LED | ERROR STATE |
|---|-----|-------------|
| Prior to inserting the USB into a computer, press           |     | -           |
| Enter the <b>User PIN*</b> .                                |     | -           |
| Press .   |     | -           |
| Within 30 seconds, insert the USB drive into your computer. |     | -           |

\*The factory PIN for new USBs is 11223344. We strongly recommend changing the password once it is unlocked. See *Changing the User PIN* below. 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

| STEPS  | LED | ERROR STATE  |
|--|-----|--|
| Enter the current user PIN and press  to unlock the USB. |     | -  |
| Within 30 seconds, press  .                              |     | -  |
| Enter the new <b>User PIN</b> .                          |     | -  |
| Press  .   |     | If the PIN does not meet requirements.   |
| Re-enter the new <b>PIN</b> .                            |     | -  |
| Press the <b>key button</b> twice.                       | →   | (1)  If re-entry does not match.   |
|  |     | <b>OR</b>  |
|  |     | (2)  →  (momentarily) if any error was made.<br><b>*If either occur, the new PIN was not created.*</b> |

**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 section describe options and features requiring only a User PIN. For Administration options see Admin Mode on page 11. This section includes instructions on enabling read-only and read/write options in user mode as well as enabling and disabling a timeout lock.

**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).












| STEPS   | LED   | ERROR STATE |
|---|---|-------------|
| Unlock USB with User PIN.   |    | -           |
| Press    . |     | -           |
| Press 7, 6. (R, O for Read-Only)  |     | -           |
| Press  .   |  →  | -           |

If plugged into the computer, the LED will change to . 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.

| STEPS   | LED   | ERROR STATE |
|---|---|-------------|
| Unlock USB with User PIN.   |    | -           |
| Press    . |     | -           |
| Press <b>7, 9.</b> ( <b>R, W</b> for Read/Write)  |     | -           |
| Press  .   |  →  | -           |

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.

| STEPS   | LED   | ERROR STATE |
|---|---|-------------|
| Unlock USB with User PIN.   |    | -           |
| Press    . |     | -           |
| Press <b>8, 5.</b> ( <b>T, L</b> for Timeout Lock)  |     | -           |
| Press  .   |    | -           |
| Press the keypad to enter the number of minutes before a Timeout Lock activates. <b>Two digits are required.</b><br><b>Example:</b> Press <b>0</b> and <b>1</b> for 1 minute, up to 99 minutes.   |    | -           |
| Press  .   |  →  | -           |

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.








## SECTION 3: 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. 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 4.

### 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 describes how to create or change an Admin PIN, create or change a User's PIN in Admin mode, and how to unlock and lock 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<br>Cannot access USB until User or Admin PIN is defined   |
| SET      | NOT SET   | Can change <b>User PIN</b> when unlocked as User<br>Can set <b>Admin PIN</b> when unlocked with <b>User PIN</b><br>Can access data when unlocked as User                                     |
| NOT SET  | SET       | Can create <b>User PIN</b><br>Can unlock USB with <b>Admin PIN</b><br>Can change <b>Admin PIN</b> when unlocked as Administrator<br>Can perform Administrator commands                       |
| SET      | SET       | Can unlock USB and access data with either <b>User</b> or <b>Admin PIN</b><br>Can change <b>User PIN</b> when unlocked as User<br>Can change <b>Admin PIN</b> when unlocked as Administrator |

1.21.2020

## Creating an Admin PIN

| STEPS  | LED  | ERROR STATE  |
|--|--|--|
| Unlock with your User PIN (Refer to PIN requirements on page 4, except don't insert into your computer).   |   | -  |
| Press and hold down <b>1</b> -and then press   . |  <br>rapidly | -  |
| Enter a new Admin PIN.   |  <br>rapidly | -  |
| Press   .  |   |  -if the PIN does not meet requirements, no Admin PIN is saved. |
| Re-enter your new Admin PIN.   |   |  -if the PINs don't match, no Admin PIN is saved.               |
| Press   .  |  →           |  -briefly if unsuccessful.                                      |






**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 14.















**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.

| STEPS  | LED   | ERROR STATE  |
|--|---|--|
| Press and hold down <b>1</b> -and then press  .       |     | -  |
| Enter the Admin PIN.   |     | -  |
| Press  . Insert into your computer within 30 seconds. |  →  |  - briefly if unsuccessful. |

**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 4.

| STEPS   | LED   | ERROR STATE   |
|---|---|---|
| Unlock the USB KP with the Admin PIN. (Refer to previous procedure.)  |              | -   |
| Press   . |              | -   |
| Enter a new <b>User PIN</b> .   |              | -   |
| Press   . |              | -   |
| Re-enter the <b>User PIN</b>  |              | -   |
| Press   . |  momentarily |  if the PIN does not meet requirements.<br> if unsuccessful, such as the PINs don't match, the light will remain on for more than 30 seconds. |



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 13.

















## 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 6.

## 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.” PIN requirements on page 4.

| STEPS   | LED  | ERROR STATE  |
|---|--|--|
| Unlock the USB KP with the Admin PIN.   |   | -  |
| Press and hold down <b>1</b> and then press   . |  <br>rapidly   | -  |
| Enter a new <b>Admin PIN</b> .  |  <br>rapidly   | -  |
| Press   .                                       |   | -  |
| Re-enter the <b>Admin PIN</b>   |   | -  |
| Press   .                                       |  briefly then  |  if unsuccessful, such as the 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 such as enabling read-only and read/write mode, and setting Timeout Lock in Admin or User Mode.

**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.

### Enabling Read-Only in Admin Mode

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












| STEPS   | LED   | ERROR STATE |
|---|---|-------------|
| Unlock the USB KP with the Admin PIN.   |    | -           |
| Press    . |     | -           |
| Press <b>7, 6.</b> ( <b>R, O</b> for Read-Only).  |     | -           |
| Press  .   |  →  | -           |

The USB FX5 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.
















| STEPS   | LED   | ERROR STATE |
|---|---|-------------|
| Unlock the USB FX5 with the Admin PIN.  |    | -           |
| Press    . |     | -           |
| Press <b>7, 9.</b> ( <b>R, W</b> for Read/Write)  |     | -           |
| Press  .   |  →  | -           |

The USB FX5 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 FX5 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.

| STEPS   | LED   | ERROR STATE |
|---|---|-------------|
| Unlock the USB FX5 with the Admin PIN.  |    | -           |
| Press    . |     | -           |
| Press 8, 5. (T, L for Timeout Lock)   |     | -           |
| Press  .   |  →  | -           |
| Enter the length of idle time for Timeout. Two digits required. Example: Press 0 and 1 for 1 minute, up to 99 minutes.  |    | -           |
| Press  .   |  →  | -           |

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.







## SECTION 4: Managing the USB

The following headings discuss important, though less common, actions for managing your USB. All procedures are performed before inserting the USB FX5 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 exists. [
-  Both PINs exist. [ 




















### Deleting all Files in Admin Mode

An Administrator can delete all data stored on the USB FX5 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 15](#).



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

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

| STEPS   | LED   | ERROR STATE  |
|---|---|--|
| Unlock the USB FX5 with the Admin PIN.  |    | -  |
| Press    . |     | -  |
| Press 3, 2. (D, A for Delete All.)  |     | -  |
| Press  .   |  ↔ <br>alternating  | -  |
| Enter the Admin PIN again.  |  ↔ <br>alternating  | -  |
| Press  .   |  <br>briefly<br> rapidly | If unsuccessful:<br> briefly<br> rapidly |

All data and User settings have now been deleted from the USB FX5. The next time you insert the USB FX5 into your computer, your system will generally prompt you to reformat it. Refer to [Reformatting the SecureUSB on page 15](#).

# 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 15.**

## 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.

| 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.<br>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 FX5 including the PINs, you can perform the following Reset function. It also removes the encryption, requiring the USB to be reformatted—to format the USB refer to the heading Reformatting the SecureUSB below.

| STEPS                                | LED              | ERROR STATE |
|--------------------------------------|------------------|-------------|
| Press and hold down 7-and then press | ↔<br>alternating | -           |
| Press 999.                           | ↔<br>alternating | -           |
| Press and hold down 7-and then press | &<br>momentarily | -           |

The USB is now blank and locked.

## 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 FX5 when formatted, whether or not the Brute Force Hacking Detection was triggered or not.

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

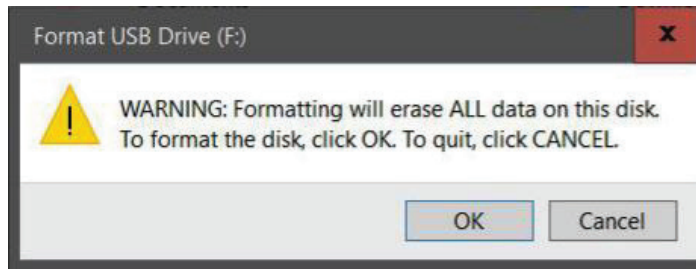
### For a Windows OS



Admin permission on the PC is required for this procedure.

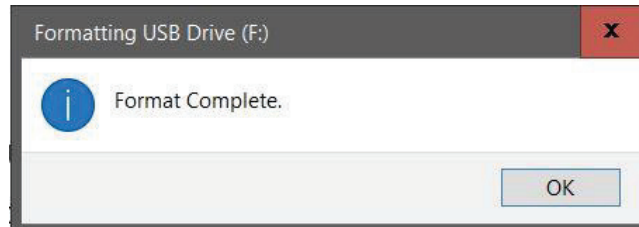
1. Unlock the USB with the default User PIN (or the Admin PIN if all files were deleted with the Admin PIN). Refer to *PIN Requirements* on page 4 or to *Unlocking the USB in Admin Mode* on page 9.
2. Insert the USB into your computer.
3. In the popup message click **Format Disk**.
4. Select **FAT32** 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.







7. The procedure will finish formatting the USB FX5 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.

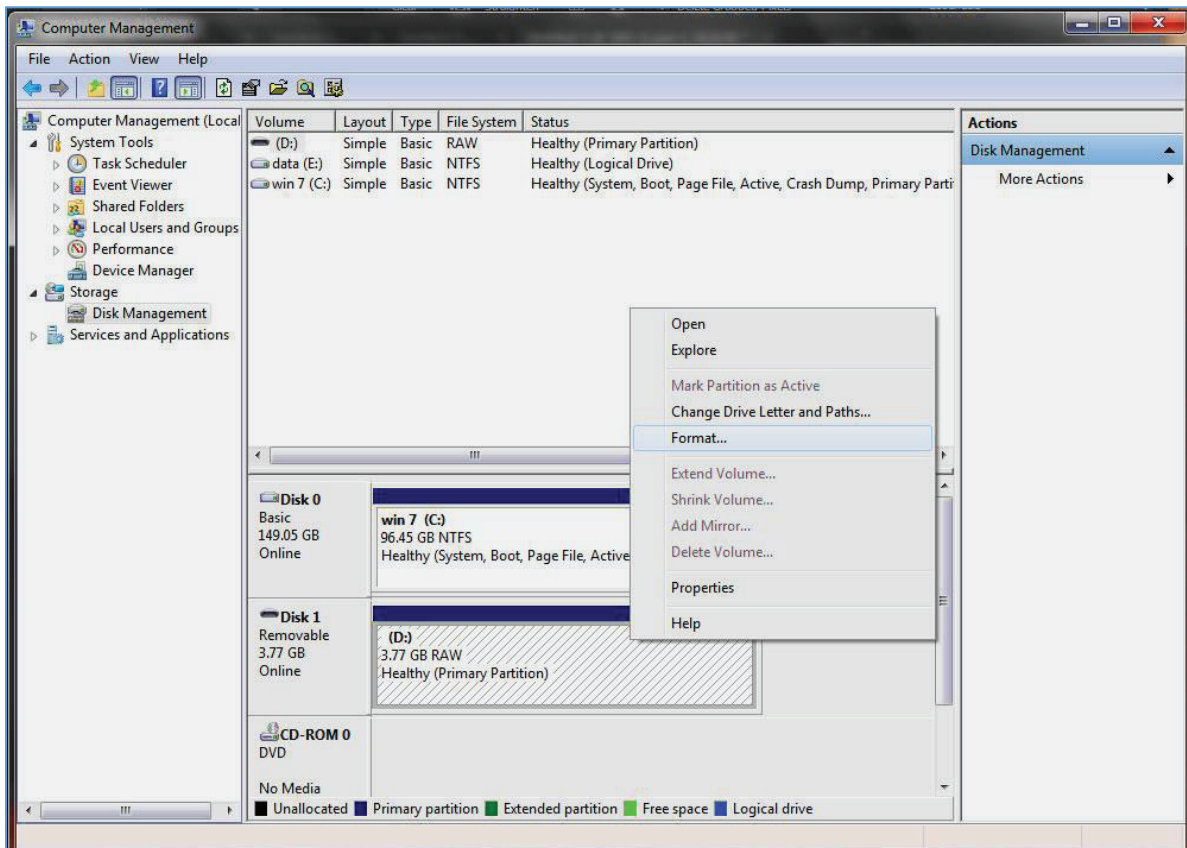


Figure 1: Initializing the Secure USB FX5 (shown here as Disk 1). Until initialized it displays as RAW. (The hash marks indicate an unallocated drive.)

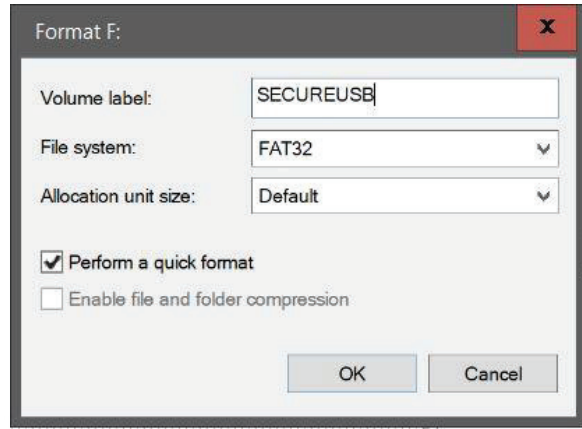
3. In the blank (hashed) area of the unallocated section, right click the **Removable** drive and click **Format**

---

**Note:** If the Format command is unavailable (dimmed), the drive may be Write-protected. Remove the drive and then refer to either *Enabling Read-Only in User Mode* on page 6 or *Enabling Read/Write in Admin Mode* on page 11.



---

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.

---

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

---

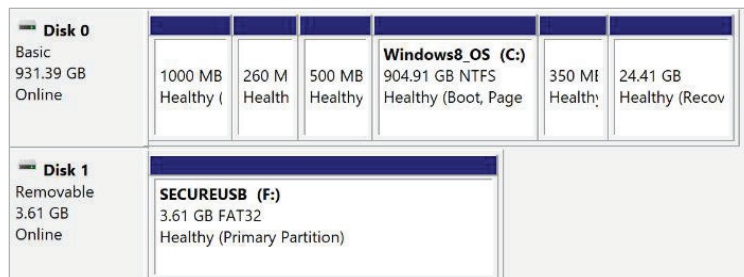


Figure 2: The SecureUSB is displayed here as “Disk 1.”  
It is Online and allocated (Healthy) and ready for use.

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

---

**Note:** When finished the New Volume 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 PIN Requirements on page 4, or to Unlocking the USB in Admin Mode on page 9.**
2. **Insert the FX5 into your Mac within thirty seconds (green LED still lit).**
3. **Click Initialize in the popup message (shown below). The Disk Utility Dialog displays.**

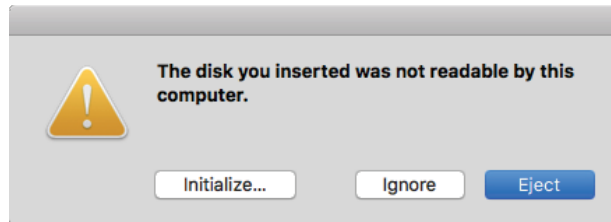
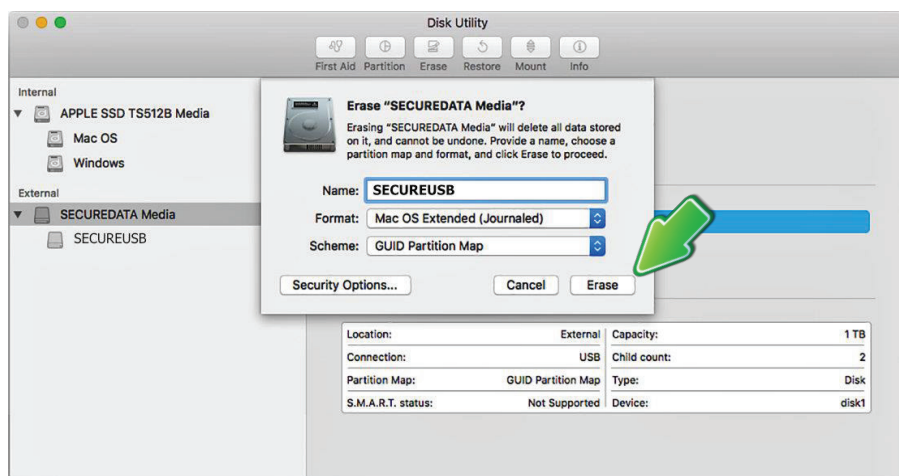
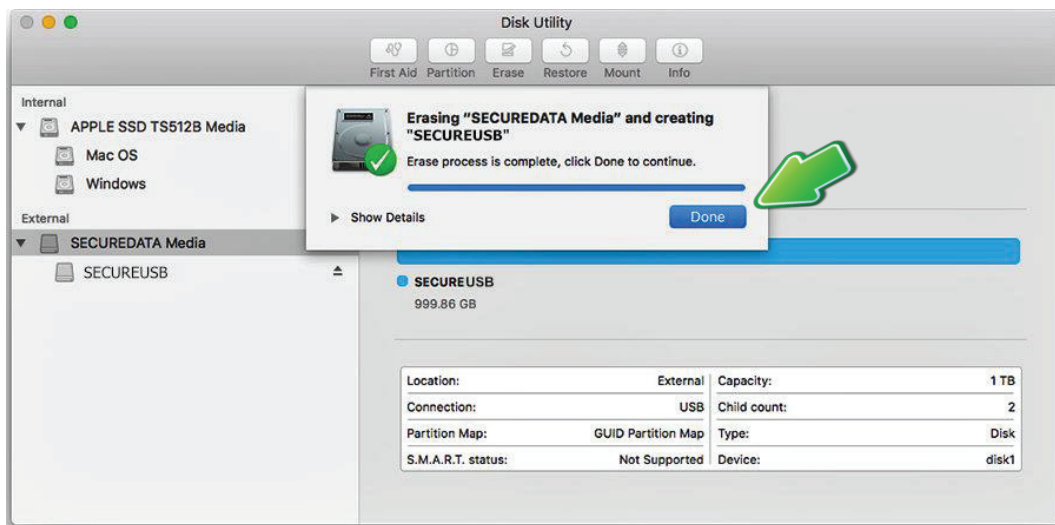
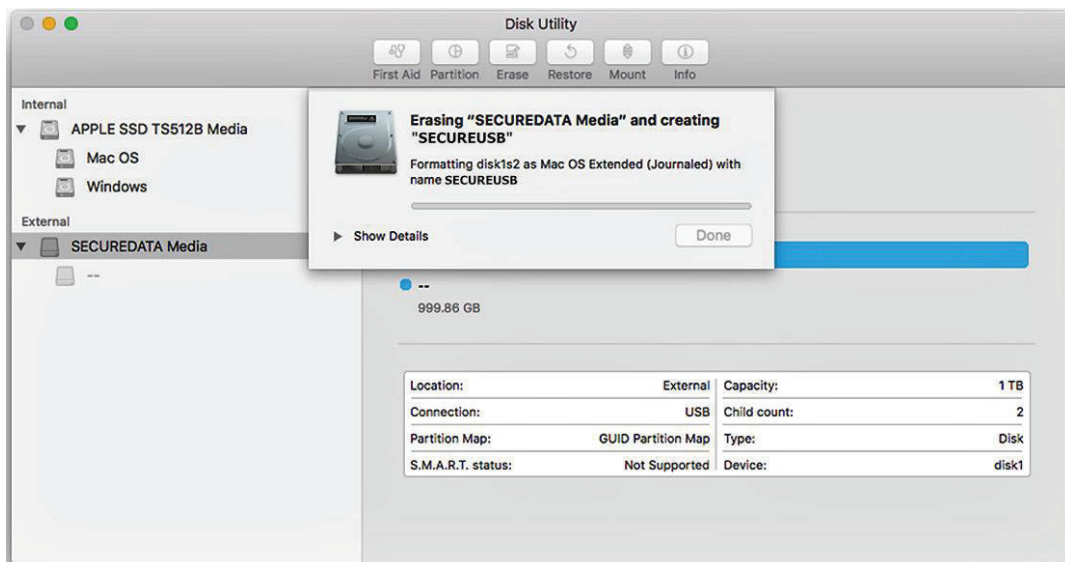


Figure 3: The Disk Utility Dialog. Make sure the correct drive is highlighted (There is only one External drive listed in this image).

4. **Ensure that your SecureData FX5 is highlighted in the list of External drives and click Erase. The system begins erasing the external USB.**





**Figure 4:** 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.**

---

**Note:** SecureUSB is now displayed under External in the left column.

---

**6. Close the Disk Utility.**

# SECTION 5: CONTACT AND WARRANTY INFORMATION

## LIMITED WARRANTY

This Limited Warranty is provided by Rocstorage, Inc. (hereinafter: Rocstor) for all lines of products.

### General Terms

EXCEPT AS EXPRESSLY SET FORTH IN THIS LIMITED WARRANTY, ROCSTOR MAKES NO OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ROCSTOR EXPRESSLY DISCLAIMS ALL WARRANTIES AND CONDITIONS NOT STATED IN THIS LIMITED WARRANTY. ANY IMPLIED WARRANTIES THAT MAY BE IMPOSED BY LAW ARE LIMITED IN DURATION TO THE LIMITED WARRANTY PERIOD. SOME STATES OR COUNTRIES DO NOT ALLOW A LIMITATION ON HOW LONG AN IMPLIED WARRANTY LASTS OR THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES FOR CONSUMER PRODUCTS. IN SUCH STATES OR COUNTRIES, SOME EXCLUSIONS OR LIMITATIONS OF THIS LIMITED WARRANTY MAY NOT APPLY TO YOU.

This Limited Warranty applies to the Rocstor branded hardware products sold by or leased from Rocstorage, Inc., its worldwide subsidiaries, affiliates, authorized resellers, or country distributors (collectively referred to in this Limited Warranty as "Rocstor") with this Limited Warranty. This Limited Warranty is applicable in all countries and may be enforced in any country where Rocstor or its authorized service providers offer warranty service subject to the terms and conditions set forth in this Limited Warranty. However, warranty service availability and response times may vary from country to country and may also be subject to registration requirements in the country of purchase.

Rocstor warrants that the Rocstor hardware product and all the internal components of the product that you have purchased or leased from Rocstor are free from defects in materials or workmanship under normal use during the Limited Warranty Period. The Limited Warranty Period starts on the date of purchase or lease from Rocstor. Your dated sales or delivery receipt, showing the date of purchase or lease of the product, is your proof of the purchase or lease date. You may be required to provide proof of purchase or lease as a condition of receiving warranty service. You are entitled to warranty service according to the terms and conditions of this document if a repair to your Rocstor branded hardware is required within the Limited Warranty Period. This Limited Warranty extends only to the original purchaser or lessee of this Rocstor branded product and is not transferable to anyone who obtains ownership of the Rocstor branded product from the original purchaser or lessee.

Rocstor products are manufactured using new materials or new and used materials equivalent to new in performance and reliability. Spare parts may be new or equivalent to new. Spare parts are warranted to be free from defects in material or workmanship for thirty (30) days or for the remainder of the Limited Warranty Period of the Rocstor hardware product in which they are installed, whichever is longer.

### Rocstor's Obligation under the Limited Warranty

During the Limited Warranty Period, Rocstor will repair or replace the defective component parts or the hardware product. All component parts or hardware products removed under this Limited Warranty become the property of Rocstor. The replacement part or product takes on either the Limited Warranty status of the removed part or product or the thirty (30) day limited warranty of the spare part. In the unlikely event that your Rocstor product has a recurring failure, Rocstor, at its discretion, may elect to provide you with a replacement unit of Rocstor's choosing that is at least equivalent to your Rocstor branded product in hardware performance. Rocstor reserves the right to elect, at its sole discretion, to give you a refund of your purchase price or lease payments (less interest) instead of a replacement. This is your exclusive remedy for defective products.

**The original Limited Warranty is not extended when the product, or a part of the product, is repaired or replaced during the Limited Warranty period. Rocstor shall not be responsible or liable for backing up any data that is on a drive being returned for service**

**YOU SHOULD MAKE PERIODIC BACKUP COPIES OF THE DATA STORED ON YOUR HARD DRIVE OR OTHER STORAGE DEVICES AS A PRECAUTION AGAINST POSSIBLE FAILURES, ALTERATION, OR LOSS OF THE DATA. BEFORE RETURNING ANY UNIT FOR SERVICE, BE SURE TO BACK UP DATA AND REMOVE ANY CONFIDENTIAL, PROPRIETARY, OR PERSONAL INFORMATION. ROCSTOR IS NOT RESPONSIBLE FOR DAMAGE TO OR LOSS OF ANY PROGRAMS, DATA, OR REMOVABLE STORAGE MEDIA. ROCSTOR IS NOT RESPONSIBLE FOR THE RESTORATION OR REINSTALLATION OF ANY PROGRAMS OR DATA OTHER THAN SOFTWARE INSTALLED BY ROCSTOR WHEN THE PRODUCT WAS MANUFACTURED.**

Rocstor does not warrant that the operation of this product will be uninterrupted or error-free. Rocstor is not responsible for damage that occurs as a result of your failure to follow the instructions that came with the Rocstor branded product.

This Limited Warranty does not apply to expendable parts. This Limited Warranty does not extend to any product from which the serial number has been removed or that has been damaged or rendered defective (a) as a result of accident, misuse, abuse, or other external causes; (b) by operation outside the usage parameters stated in the user documentation that shipped with the product and/or posted on the Rocstor website; (c) by the use of parts not manufactured or sold by Rocstor; (d) as a result of normal wear; or (e) by modification or service by anyone other than (i) Rocstor, (ii) a Rocstor authorized service provider, or (iii) your own installation of end-user replaceable Rocstor or Rocstor approved parts if available for your product in the servicing country.

These terms and conditions constitute the complete and exclusive limited warranty agreement between Rocstor and you regarding the Rocstor branded product you have purchased or leased. These terms and conditions supersede any prior agreements or representations including representations made in Rocstor sales literature or advice given to you by Rocstor or an agent or employee of Rocstor-that may have been made in connection with your purchase or lease of the Rocstor branded product. No change to the conditions of this Limited Warranty is valid unless it is made in writing and signed by an authorized representative of Rocstor.

1.21.2020

## Buyer's Obligation under the Warranty

The person requesting coverage under this warranty shall prove that he or she is the original purchaser and declares that the product has not been sold, leased, bartered or otherwise changed possession. **The purchaser shall frequently backup the Rocpro hard drive and backup the data immediately prior to returning the drive for warranty service.**

The buyer must notify Rocstor and show proof of notification, through any reasonable means of communication. See full street address email address and toll free phone numbers below or updated contact information are available on Rocstor.com website. The notification shall identify any defect, malfunction, or nonconformity promptly upon discovery. Rocstor will acknowledge receipt of the communication and issue a Return Merchandise Authorization (RMA) code. The buyer is obligated to securely and safely package(s) the product, preferably in the original packing materials, WITH THE RMA number, and deliver it together with a copy of the original purchase receipt and a description of the problem to the Rocstor home office. Buyer is responsible for the product until it is received by Rocstor. It is recommended that the product be insured during transportation by the sender. You must prepay any shipping charges, taxes, or duties associated with transportation of the product. In addition, you are responsible for insuring any product shipped or returned for service. You assume risk of loss during shipping.

## Limitation of Damages (Liability)

IF YOUR ROCSTOR BRANDED HARDWARE PRODUCT FAILS TO WORK AS WARRANTED ABOVE, THE ORIGINAL PURCHASER'S SOLE AND EXCLUSIVE REMEDY SHALL BE REPAIR OR REPLACEMENT. ROCSTOR'S MAXIMUM LIABILITY UNDER THIS LIMITED WARRANTY IS EXPRESSLY LIMITED TO THE LESSER OF THE PRICE YOU HAVE PAID FOR THE PRODUCT OR THE COST OF REPAIR OR REPLACEMENT OF ANY ROCSTOR HARDWARE COMPONENTS THAT MALFUNCTION IN CONDITIONS OF NORMAL USE. ROCSTOR IS NOT LIABLE FOR ANY DAMAGE TO ANY OTHER PRODUCT CONNECTED TO A ROCSTOR PRODUCT.

## Limitation on Consequential Damages

ROCSTOR IS NOT LIABLE FOR ANY DAMAGES CAUSED BY THE PRODUCT OR THE FAILURE OF THE PRODUCT TO PERFORM, INCLUDING ANY LOST PROFITS OR SAVINGS OR SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES. ROCSTOR IS NOT LIABLE FOR ANY CLAIM MADE BY A THIRD PARTY OR MADE BY YOU FOR A THIRD PARTY. THIS LIMITATION OF LIABILITY ALSO APPLIES WHETHER DAMAGES ARE SOUGHT OR A CLAIM IS MADE UNDER THIS LIMITED WARRANTY OR AS A TORT CLAIM (INCLUDING NEGLIGENCE AND STRICT PRODUCT LIABILITY), A CONTRACT CLAIM OR ANY OTHER CLAIM. THIS LIMITATION OF LIABILITY CANNOT BE WAIVED OR AMENDED BY ANY PERSON. THIS LIMITATION OF LIABILITY WILL BE EFFECTIVE EVEN IF YOU HAVE ADVISED ROCSTOR OR AN AUTHORIZED REPRESENTATIVE OF ROCSTOR OF THE POSSIBILITY OF ANY SUCH DAMAGES.

THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY ALSO HAVE OTHER RIGHTS THAT MAY VARY FROM STATE TO STATE OR FROM COUNTRY TO COUNTRY. YOU ARE ADVISED TO CONSULT APPLICABLE STATE OR COUNTRY LAWS FOR A FULL DETERMINATION OF YOUR RIGHTS.

## Disclaimer

We accept no liability for any loss of data, damages and the inability of Rocstor products to work with any third party equipment. Nor can Rocstor accept any liability or responsibility for software or third party hardware products.

## Limited Warranty Period

The limited warranty period for the **DataSecure** is four (4) Year Parts and Labor. This Limited Warranty extends only to the original purchaser or lessee of this Rocstor branded product and is not transferable to anyone who obtains ownership of the Rocstor branded product from the original purchaser or lessee

## Types of Limited Warranty Service

Your Rocstor Limited Warranty consists of repair or replacement of defective parts, including hard drives identified by Rocstor Support Organization as "pre-failure".

## Carry-in Limited Warranty Service Available Monday - Friday

Under the terms of carry-in service, you may be required to deliver your Rocstor product to the Rocstor Service Center or an authorized service location for warranty repair. You must prepay any shipping charges, taxes or duties associated with transportation of the product. In addition, you are responsible for insuring any product shipped or returned for service. You assume risk of loss during shipping.

**YOU SHOULD MAKE PERIODIC BACKUP COPIES OF THE DATA STORED ON YOUR HARD DRIVE OR OTHER STORAGE DEVICES AS A PRECAUTION AGAINST POSSIBLE FAILURES, ALTERATION OR LOSS OF THE DATA. BEFORE RETURNING ANY UNIT FOR SERVICE, BE SURE TO BACK UP DATA AND REMOVE ANY CONFIDENTIAL, PROPRIETARY OR PERSONAL INFORMATION. ROCSTORAGE IS NOT RESPONSIBLE FOR DAMAGE TO OR LOSS OF ANY PROGRAMS, DATA OR REMOVABLE STORAGE MEDIA. ROCSTORAGE IS NOT RESPONSIBLE FOR THE RESTORATION OR REINSTALLATION OF ANY PROGRAMS OR DATA OTHER THAN SOFTWARE INSTALLED BY ROCSTORAGE WHEN THE PRODUCT WAS MANUFACTURED.**

**Rocstorage shall not be responsible or liable for backing up any data that is on a drive being returned for service. Expect that all data on the drive will be destroyed and not retrievable when returned for warranty service.**



## Rocstor Replaceable Parts Program

Where available, the Rocstor Replaceable Parts program ships approved replacement parts directly to you to fulfill your warranty. This will save considerable repair time. After you call the Rocstor Technical Support Center at **888.877.8777** a replaceable part can be sent directly to you. Once the part arrives, call the Rocstor Technical Support Center. A technician will assist you over the phone to ensure that the installation is quick and easy.

## Service Upgrades

Rocstor offers extra coverage for your product. For information on service upgrades, visit [www.rocstor.com](http://www.rocstor.com). Service upgrades purchased in one country are not transferable to another country.

## Capacity Disclaimer

Actual accessible hard drive capacity will indicate up to 10% lower than stated under different Operating Systems and formatting.

The storage volume is measured in total bytes before formatting. References to round numbers of gigabytes or terabytes are an approximation only. For example, a disk drive labeled as having 500GB (Gigabytes) has space for approximately 500,000,000 bytes before formatting. After formatting, the drive capacity is reduced by about 5% to 10% depending on the operating system and formatting used or "1GB = 1,000,000,000 bytes."

## Options and Software

The Limited Warranty terms and conditions for Rocstor options are as indicated in the Limited Warranty applicable to Rocstor options. ROCSTOR DOES NOT WARRANTY SOFTWARE PRODUCTS, INCLUDING ANY SOFTWARE PRODUCTS OR THE OPERATING SYSTEM PREINSTALLED BY ROCSTOR. Rocstor's only obligations with respect to software distributed by Rocstor under the Rocstor brand name are set forth in the applicable end-user license or program license agreement. Non-Rocstor hardware and software products are provided "AS IS" and without any Warranty. However, non-Rocstor manufacturers, suppliers or publishers may provide their own warranties directly to you.

The data stored in Rocstor and Rocsecure storage product lines are not guaranteed by Rocstor (or the hard disk manufacturer.) We are not responsible for any loss of data. Always back up data regularly

## TECHNICAL SUPPORT

### Software Technical Support

Software technical support is defined as assistance with questions and issues about the software that was either preinstalled by Rocstor on the Rocstor branded product or that was included with the Rocstor branded product at the time of your purchase or lease of the product. Technical support for software is available for the first ninety (90) days from date of product purchase or lease. Your dated sales or delivery receipt, showing the date of purchase or lease of the product, is your proof of the purchase or lease date. You may be required to provide proof of purchase or lease as a condition of receiving software technical support. After the first ninety (90) days, technical support for software that was either preinstalled by Rocstor on the Rocstor branded product or included with the Rocstor branded product at the time of your purchase or lease of the product is available for a fee.

**WARNING: The individual user should take care to determine prior to use whether this device is suitable, adequate or safe for the use intended. Since individual applications are subject to great variation, the manufacturer "Rocstor" makes no representation or warranty as to the suitability or fitness of these devices for any specific application.**

### Technical Support

The Rocpro T34Bay RAID is backed by free telephone technical support for two (2) years from the date of purchase. Please register your product with Rocstor. To register, fill in the Limited Warranty Registration form in the Support tab at [www.rocstor.com](http://www.rocstor.com).

Free telephone technical support is available weekdays from 9 AM until 6 PM Pacific Standard Time. Customers in the United States and Canada can call toll-free: **(888) 877-8777**; all others must call **(818) 449-2000**.

When calling for support, please have the product's serial number (printed on the label on the bottom of the drive) and system hardware information available.

## TRADEMARKS ACKNOWLEDGEMENTS

© 2018, Rocstorage, Inc; acknowledges the following trademarks for company names or products mentioned within the Rocstor site, portal pages and Articles/text/manuals: Rocstor, Rocsecure and Rocpower are registered trademarks of Rocstorage, Inc. Rocpro, Rocport, Rocbit, Rocsafe ... are the trademarks of Rocstorage, Inc. "store your future", "secure your future" and "power your future" are the slogan marks of Rocstorage, Inc. Apple, the Apple logo, Mac, Power Macintosh, FireWire, and Mac Pro, Leopard ... are trademarks of Apple Computer, Inc. in the United States and other countries. Microsoft, MS-DOS, Windows CE, Windows NT, Windows 98, Soft Windows, Vista ... are registered trademarks of Microsoft Corporation in the United States and other countries.

Intel, Itanium, Pentium, Celeron, and Xeon MMX ... are registered U.S. trademarks of Intel; Thunderbolt and the Thunderbolt logo are trademarks of Intel Corporation in the United States and other countries. HyperDuo is the Register Trademark of Marvell Technology Group LTD. This product is (may also be) integrated with SATA hard drives from the following manufactures: Seagate, Samsung, Western Digital, Hitachi, Toshiba, Fujitsu ... All other names are trademarks of their respective companies.

Rocstor wishes to acknowledge the use of tables, charts, graphs and texts from the Wikipedia website. © 2000 - 2019

## CONTACT INFORMATION

### Technical Support / RMA

Hours: 9:00 am - 5:00 pm PST  
Mon - Fri (excluding holidays)

Tell: +1 (818) 727-7000 (Domestic and Internationals)  
Fax: +1 (818) 875-0002  
Email: support@Rocstor.com

### Corporate, Government and Academic Customers

Our Corporate Sales Team's goal is to help our U.S.A. and Canadian customers find a storage solution that best serves their needs. We will help you determine your best purchasing options. For more information please contact the appropriate department below or call us at +1 (818) 727-7000.

|  |  |
|--|--|
| General sales information:                           | <a href="mailto:sales@Rocstor.com">sales@Rocstor.com</a>                       |
| Corporate sales information:                         | <a href="mailto:corporate_sales@Rocstor.com">corporate_sales@Rocstor.com</a>   |
| Educational sales information:                       | <a href="mailto:academic_sales@Rocstor.com">academic_sales@Rocstor.com</a>     |
| Federal, State & Local government sales information: | <a href="mailto:government_sales@Rocstor.com">government_sales@Rocstor.com</a> |

### Resellers/Business Development/OEM Partners

All Channel National and International Resellers, VARs, Consultants ...  
contact Rocstor Channel Sales: call: +1 (818) 727-7000  
Email: reseller\_info@Rocstor.com

### COPYRIGHTS

©2025Rocstor, Inc. All rights reserved. Rocstor is registered trademark of Rocstor, Inc. SecureDrive and SecureUSB products are developed and manufactured by SecureData and are based on DataLock technology licensed from ClevX, LLC. U.S. Patent. [www.clevx.com/patents](http://www.clevx.com/patents)

SecureDrive™ and SecureData™ are trademarks of SecureData, Inc.

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.

\*FIPS 140-2 Level 3 Validated Certificate (cert. #3297) under Securedata, Inc. SecureDrive KP Model.

Assembled and integrated in U.S.A. using domestic and / or foreign components.

