

DataLocker™ Pro AES / Enterprise 2.0 Product Manual - February 2011

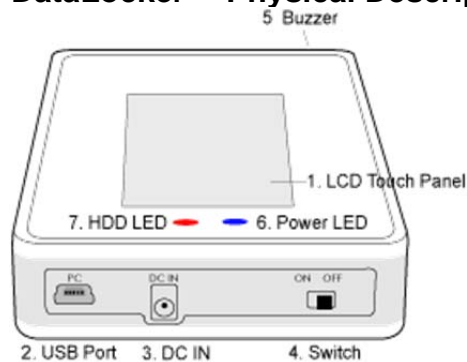
Package Contents :

- DataLocker™ unit
- Standard USB cable - Use the standard cable to connect the DataLocker™ to a properly powered USB port on the host system.
- Y cable - Use the Y split USB Cable when a single USB port does not provide enough power for the DataLocker™ unit.
- Silicone Band - Optional black band used for added durability.

Table of Contents

Section I: Setting up a New User Password
Section II: Description of the Status Screen
Section III: Disconnecting Your DataLocker™
Section IV: Deleting Contents/Redeploying Drive – Generating New Encryption Key
Section V: Changing User Options
Section VI: Special Features
Section VII: Setting the Master Administrative Password
Section VIII : Resetting Drive to Original Factory State

DataLocker™ Physical Description



1. LCD Touch panel interface
2. USB Port: Connects the DataLocker™ unit to the host system via a USB cable.
3. DC Input: Is only used with older computers that may not have a sufficiently powered USB port.
4. Power Switch: Powers the DataLocker™ on and off.
5. Buzzer: Provides audio feedback while connecting to a host system and navigating the menus.
6. Power LED: Indicates power status.
7. HDD LED: Indicates hard disk access.

Getting Started

The DataLocker™ has a minimum power requirement of 5 Volts and 500mA of current that is drawn from a USB port. Older computers and external USB hubs may not provide sufficient power to operate an external hard drive. If your computer cannot deliver adequate power, you may be required to use the “Y” split USB cable.

The DataLocker™ come preformatted with Windows NTFS file system. All major files systems are supported (Mac, Linux, FAT32). Please consult your operating system guide on reformatting instructions.

Section I: Setting up a New User Password

Step 1: Connect the included standard USB Cable to the DataLocker™. If your computer does not generate sufficient power to operate the DataLocker™, use the “Y” split USB cable, plugging both the “black” and “red” prongs into the host computer.

Step 2: Turn the power switch to the “on” position.

Step 3: Enter the **default password “000000”** and press the return key.



Step 4: The next screen will prompt you to change the default password, press the “OK” button. (Once you have changed the default password this screen will no longer appear after logging in).



Step 5: IMMEDIATELY press the “SETUP” key on the touch screen. If the “SETUP” key is not selected within 3 seconds, the DataLocker™ will automatically connect to the host computer.



Step 6: Press “CHANGE PASSWORD” on the touch screen.



Step 7: Press the “OK” button on the touch screen. Enter the **default password “000000”** and press the enter key.



Step 8: Press the “OK” button on the touch screen. Enter a new password 6 to 18 digits long and press the enter key.



Step 9: Press the “OK” button on the touch screen. Enter the same password you entered in the previous step to confirm the new password. Press the enter key.



Step 10: Press the touch screen 8 times randomly to initiate the seed key generation process. The seed key is used to make each drive unique.



Step 11: Press the back arrow key to leave the setup menu and connect the DataLocker™ to the host system.



Your DataLocker™ is now ready for use with your new password.

WARNING: YOUR PASSWORD CAN NOT BE RECOVERED OR RESET WITHOUT LOSING ALL OF THE DATA STORED ON THE DATALOCKER™! MAKE SURE YOU RECORD YOUR PASSWORD IN A SECURE LOCATION!

Section II: Description of the Status Screen

Once the DataLocker™ is connected to the host system it will display an informational status screen. This is an explanation of the information displayed to you on this screen.

1. FIPS KEY/SELF KEY ACTIVE : This denotes the source of the main AES encryption key the DataLocker™ is currently using.



The DataLocker™ comes from the factory operating in “FIPS KEY” mode. This key was generated in accordance to FIPS guidelines and inserted at the factory level. If you perform the “Regenerate Encryption Key” function, the “FIPS KEY” will be erased. The DataLocker™ will then generate a “SELF KEY” in its place. The screen will then display the words “SELF KEY ACTIVE”.



While your drive is operating with a “SELF KEY”, your data is still being encrypted with the same strength and protection as though it were operating in “FIPS KEY” mode. The key being used in the encryption process has been generated by the unit.

To regenerate the factory FIPS KEY, please contact the support team for instructions.

2. ADMINSTRATOR /MASTER PASSWORD INDICATOR : If a “Master” or “Administrator” password has been set, it will be indicated by the double padlock icon on the following screen.

	
No secondary master password	Master password set

3. AES-256 : This denotes the length of the AES encryption key.

4. v2.30E : This denotes the firmware version.

Section III: Disconnecting Your DataLocker™

Use your operating system's "Safely Remove Hardware" or "Eject" function before you power down or detach the DataLocker™ from the host system. This will help prevent damage to the disk.

Windows Users: Left click the "Safely Remove Hardware" icon located on the right side of the tool bar.

MAC Users: Click the eject button that corresponds with the DataLocker™ on your MAC operating system.

Use the "Disconnect" button on the connected screen of the DataLocker™, if your operating system's "Safely Remove Hardware" or "Eject" function is not working properly. This is a secondary disconnect function and should only be used if it is the **only** option.

Section IV: Deleting Contents/Redeploying Drive – Generating New Encryption Key

SPECIAL NOTE : Once a Master Password is set you must login using the Master Password to change the encryption key. Regenerating the encryption deletes all data and user password but it does not delete the Master Password.

If you require it or would like to delete all your data, you are able to regenerate your AES encryption key. This feature can also be used to redeploy the DataLocker™ to a new user. Once this function is performed, all the data is **IRREVERSIBLY DELETED**. Use this feature with extreme caution. You should also note that the drive will no longer be operating with a FIPS validated key. To reestablish a FIPS validated key, please visit www.DataLockerDrive.com for specific instructions.

Step 1: Enter the default password "000000" or your user defined password and press the enter key.

Step 2: IMMEDIATELY press the "SETUP" key on the touch screen. If the "SETUP" key is not selected within 3 seconds, the DataLocker™ will automatically connect to the host computer.



Step 3: Press "REGENERATE ENCRYPTION KEY" on the touch screen.



Step 4: Press “Continue”, if you are 100% certain you want to delete all drive data and generate a new AES encryption key.



Step 5: Press “YES” to confirm that you want to continue.

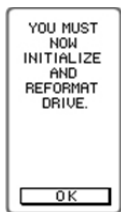


Step 6: Press the touch screen 8 times randomly to initiate the key generation process.



Your new AES encryption key has now been generated. All data previously stored on the DataLocker™ is no longer accessible, and **CANNOT** be recovered.

Step 7: You **MUST** now reinitialize and reformat the DataLocker™. This process is different depending on your computer's operating system. Please consult your operating system for instruction on reinitializing and formatting the hard drive.



Section V: Changing User Options

The DataLocker™ has three user options that can be disabled or enabled through the setup menu. All of these features are enabled with the factory presets.

ENTERING THE SETUP MENU

Step 1: Enter the default password “000000”, or your user defined password and press the enter key.



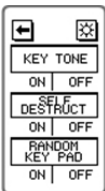
Step 2: IMMEDIATELY press the “SETUP” key on the touch screen. If the “SETUP” key is not selected within 3 seconds, the DataLocker™ will automatically connect to the host computer.



Step 3: Press the “OTHER” key on the touch screen.



Step 4: On this screen you can disable or enable the “KEY TONE”, “SELF DESTRUCT”, and “RANDOM KEY PAD” mode.



1. Self-Destruct Mode: This is a security measure that will DELETE all data stored on the DataLocker™ after nine unsuccessful password attempts. Once initiated, this function is IRREVERSIBLE. The password attempt counter will reset once the correct password is successfully entered.

Note to Enterprise Edition Users : Once a Master Password is set you must login using the Master Password to change the encryption key.

2. Key Tone: You may choose to disable the key tones.

3. Random Keypad: In order to prevent finger print reading or “shoulder hacking”, the DataLocker™ has the ability to generate rotating keypads.

4. Screen Contrast : Adjust contrast of the screen

Section VI: Special Features

USB Malware / Hack Detection

The DataLocker™ will detect any process that attempts to alter the DataLocker™'s file system or partition. This includes, malware, viruses, and any attempts to reformat or alter the drive.



WARNING: IF THIS MENU IS DISPLAYED UNEXPECTEDLY, IMMEDIATELY PRESS THE “CANCEL” KEY AND DISCONNECT THE DATALOCKER™ FROM THE COMPUTER. YOU SHOULD THEN SCAN YOUR COMPUTER FOR VIRUSES.

NOTE: THIS WARNING IS DISPLAYED DURING THE INITIALIZATION PROCESS. IF YOU ARE PERFORMING THIS OPERATION, DISREGARD THIS WARNING.

Auto Secure Feature

This feature will allow you to automatically secure your DataLocker™ after performing a lengthy disk operation (large file transfer or backup operation). Simply press the “DISCONNECT” button after starting the operation and the DataLocker™ will secure itself once the operation has completed.



Use your operating system's “Safely Remove Hardware” or “Eject” function, before you power down or detach the DataLocker™ from the host system. This will help prevent damage to the disk.



Self-Tests

The DataLocker™ runs a series self-diagnostic check during start up. The DataLocker™ will then give you a series of beeps to inform you of the problem. Each pattern of beeps denotes a different problem.

1. If there is a problem with the hard drive its self, the DataLocker™ will beep once every second until it is turned off.
2. If there is a problem with the AES engine, the DataLocker™ will beep twice every second until it is turned off.
3. If there is a problem with the firmware, the DataLocker™ will beep three times every second until it is turned off.

Section VII: Setting the Master Administrative Password

Once a Master Administrative password is set, the user password will no longer be able to access the administrative functions such as, “Regenerate Encryption Key”, or disable the “Self Destruct Mode”. Only the administrator will have access to these functions. This feature is not utilized in the factory preset. If the Master Password Utility has not run on the DataLocker™, only the user password is utilized.

Step 1. Connect the DataLocker™ to a MS Windows based PC and download the “Master Password Utility” from the support section.

Step 2. Once downloaded, extract all files to a new directory.

Step 3. Run the utility within the newly created directory.

Step 4. If this is the first time a Master Password has been set for the DataLocker™, leave the field labeled “Enter Current Master Password” empty.

Step 5. Enter a new Master Password, 6 to 18 digits long, in the field labeled “Enter New Master Password”.

Step 6. Confirm the new Master Password in the field labeled “Re-enter New Master Password”.

Step 7. Left click the “Set Master Password” button.

Your new Master Password is now set.

Section VIII : Resetting Drive to Original Factory State

The DataLocker can be completely reset to the original factory state by either initiating the “Self Destruct” mode by incorrectly entering a password in 10 times or by running the Windows “DL Reset Tool” program available on our website. Both processes will delete all data, user password and master password.

FCC DECLARATION OF CONFORMANCE

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

DATA LOCKER WARRANTY, DISCLAIMER OF WARRANTY

LIMITED DEVICE WARRANTY. Data Locker warrants our Product to be free of any defects in materials or workmanship that would prevent the Data Locker product from performing to the published hardware specifications for one (1) year from the date of purchase.

If any Data Locker Device Product fails to so conform, or proves to have any such defects during said one (1) year period, Data Locker, at its option, will provide a new or refurbished Data Locker Product at no charge to you. The foregoing warranty (i) applies only to the original user with proof of purchase, and (ii) will not apply to Data Locker Products that have been damaged as a result of negligent handling, modification, disassembly or misuse.

Data Locker's products are not warranted to operate without failure.

Data Locker products should only be incorporated in systems designed with appropriate redundancy, fault tolerance or back-up features. Accordingly, Data Locker does not recommend the use of Data Locker products in life support systems or other applications where failure could cause injury or loss of life. Therefore if you decide to use Data Locker products in life support applications you assume all risk of such use and indemnify Data Locker, Data Locker employees, Data Locker investors against all potential damages and liabilities.

LIMITATION OF OUR WARRANTY. EXCEPT AS EXPLICITLY SET FORTH ABOVE, THE DATA LOCKER PRODUCT IS PROVIDED "AS-IS" AND DATA LOCKER MAKES AND YOU RECEIVE NO WARRANTY (EXPRESS, IMPLIED OR STATUTORY) WITH RESPECT TO THE DATA LOCKER PRODUCT. DATA LOCKER EXPRESSLY DISCLAIMS ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. YOU UNDERSTAND AND ACKNOWLEDGE THAT, EXCEPT AS EXPLICITLY SET FORTH ABOVE, DATA LOCKER DOES NOT WARRANT THAT THE DATA LOCKER PRODUCT WILL MEET YOUR REQUIREMENTS, OR THAT OPERATION OF THE DATA LOCKER PRODUCT WILL BE UNINTERRUPTED OR ERROR FREE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY DATA LOCKER, ITS EMPLOYEES, DISTRIBUTORS, DEALERS OR AGENTS SHALL CREATE ANY WARRANTY OF ANY KIND. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. IN THAT EVENT, ANY IMPLIED WARRANTIES ARE LIMITED IN DURATION TO ONE (1) YEAR FROM THE DATE OF PURCHASE OF THE DATA LOCKER PRODUCT. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. LIMITATION ON INTERNATIONAL USE. DATA LOCKER DOES NOT MAKE ANY REPRESENTATION THAT ANY CONTENT OR USE OF THE DATA LOCKER PRODUCT IS APPROPRIATE OR AVAILABLE FOR USE IN LOCATIONS OUTSIDE OF THE UNITED STATES OR WHERE IT IS ILLEGAL OR PROHIBITED BY LAW.