DataLocker **DL2**

USB 2.0 external encrypted hard drive

DATALOCKER®

Table of Contents

What is the DataLocker DL2?

- FIPS 140-2 validated external hard drive - FIPS certificate #1504
  - Uses FIPS validated Enova chip, certificate #1472
- AES 256-bit always on encryption in CBC mode
- Formerly known as DataLocker Enterprise, now known as DL2
- USB 2.0 interface

What is FIPS?

- The National Institute of Standards and Technologies (NIST) approves and/or revokes Federal Information Processing Standards (FIPS) certificates – it is an expensive process, but once approved and validated the device can not undergo any further changes without recertification
- FIPS is a requirement for all encryption solutions utilized by U.S. government personnel and contractors
- It is very important to educate government customers that a FIPS validation solution is a requirement
- FIPS 140-2 refers to the device and FIPS 197 is the AES encryption algorithm

Pros and Cons of FIPS Validation

Pros

- Required by the U.S. Government
- Recognized by many as the industry standard

Cons

- Expensive solution
- Device is locked in (no firmware updates)

What Does AES-256 Mean?

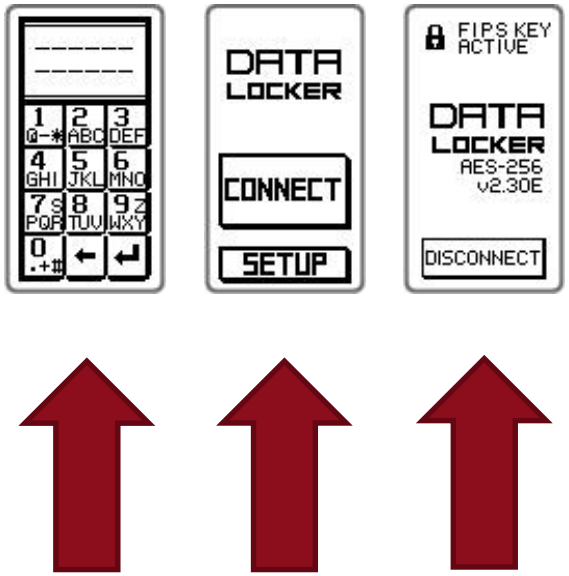
- **Advanced Encryption Standard (AES)** is the method of encryption used by the U.S. Government
- The U.S. Government held a contest where a group of highly intelligent mathematicians competed to build the worlds best encryption and AES won
- **If a device has been FIPS 140-2 validated, then it is also FIPS 197 compliant**
- 256-bit is the size of the key used to unlock the data – it looks something like the below:

01011001 01111010 01100101 00111000 00110001
01100001 01011010 01110111 01000011 01110010
01000001 01110011 01101010 01110010 01010110
00110010 00110000 01111001 01100001 00111001
01110101 00111000 00110010 01000101 01110010
00111000 00110001 01010101 01010101 01010111
01000101 00110101

DATALOCKER®

Menu Overview

- The DL2 is designed to be user friendly
- After initial setup, a user simply enters their password, connects, and the DL2 functions the same as any other external drive
- Encryption occurs behind the scenes with a dedicated hardware based crypto chip utilizing 256-bit AES encryption in CBC mode
- Security is not compromised by user friendliness because of features such as self destruct and random key pad



Menu Overview

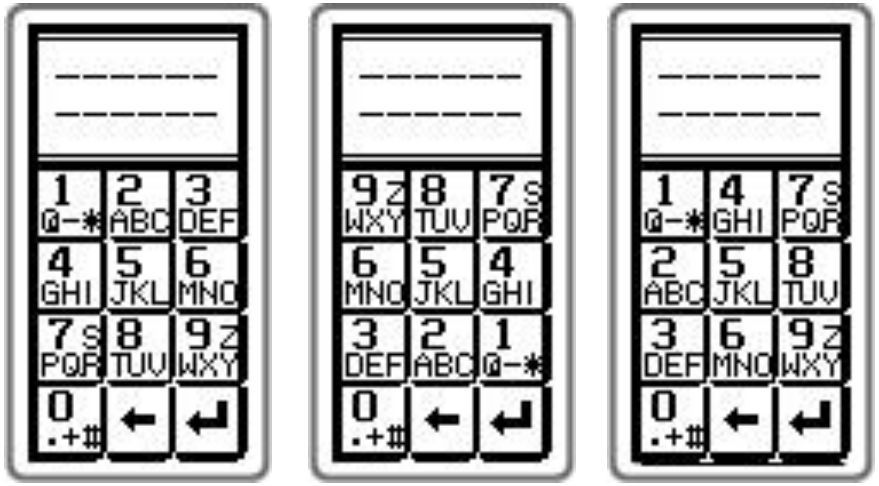
Self Destruct

- The self destruct feature is designed to defend against brute force password hacks
- If enabled, data destruction is activated after 9 unsuccessful password attempts – which wipes the encryption key and prevents data from being recovered
- This is useful if a malicious party is trying to gain unauthorized entry to the data
- Once initiated, this function is IRREVERSIBLE
- Powering off the unit does NOT reset the unsuccessful password attempt counter
- The password attempt counter will only reset once the correct password is successfully entered

Menu Overview

Random Key Pad
The random key pad feature is designed to defend against surface pattern analyzing or “shoulder hacking”

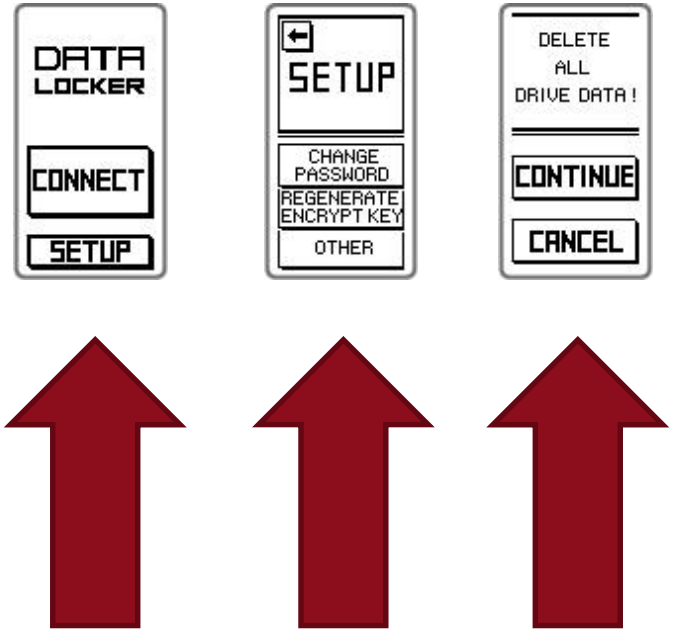
If enabled, the key pad will rotate randomly each time the DL2 is powered on

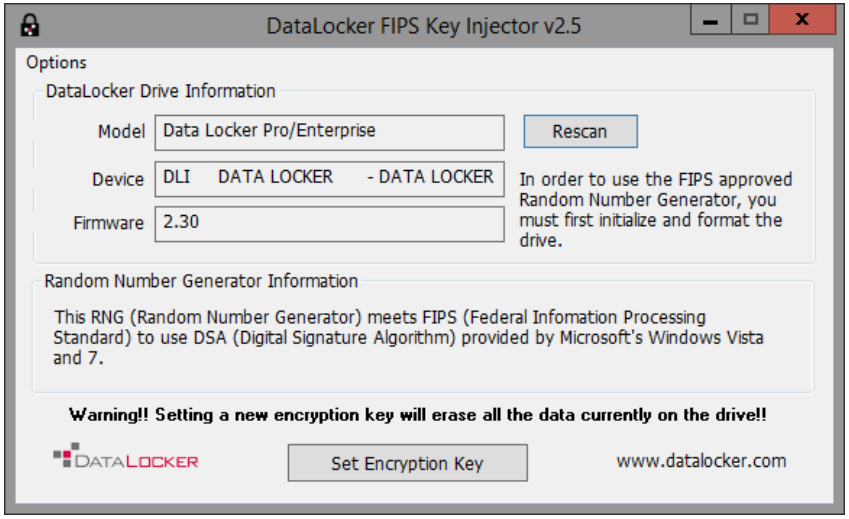


Menu and Firmware Overview

Regenerate Encryption Key

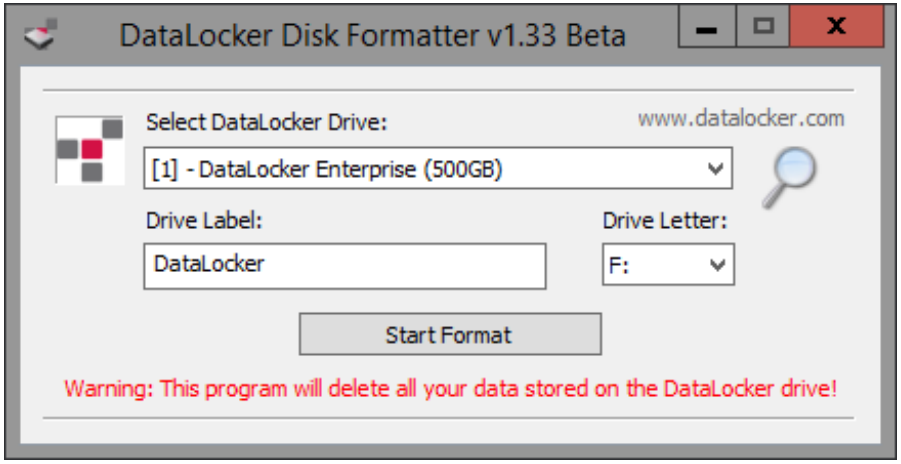
- If the user wants to wipe all data from the drive, use the regenerate encrypt key feature
- This function is IRREVERSIBLE
- After regenerating the encryption key the FIPS key must be injected to run in FIPS mode (required for government users)





Menu and Firmware Overview

The drive must then be formatted, on Windows this means using our formatter tool, tap “continue” on the DL2 screen to format the drive



Menu and Firmware Overview

Setup Screen

Allows changing password, changing encryption key, and “other”

Other

- Lets you see the LCD brightness or darkness,
- Turn self destruct off
- Randomized keypad and key tone toggle

Brightness

Makes it easier or harder to read the text

Menu Overview

DL2 Admin Password Utility v2.0 (Windows only)

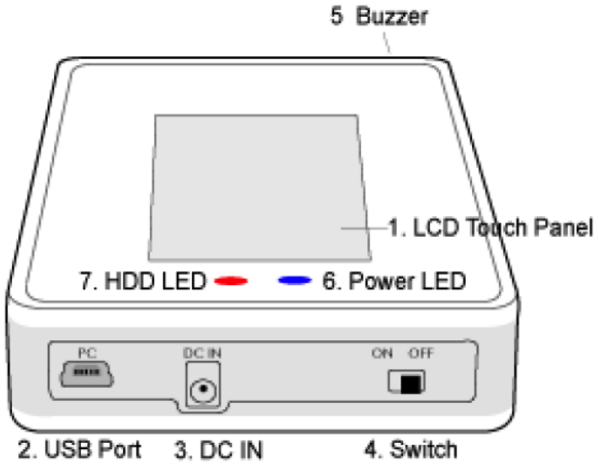
- Set an administrator password to ensure access in the event that the user forgets his/her password
- Administrator / Master Password Indicator: If a “Master” or “Administrator” password has been set, it will be indicated by the double padlock icon on the main screen
- DL2 supports two roles: one admin and one user
- Download from datalocker.com/support

Hardware Overview

- Textured aluminum and plastic enclosure
- Printed circuit board with LCD touch screen
- Hard disk drive
- Removable silicone band

Hardware Overview

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



Part Numbers

DataLocker DL2

- DL500E2
- DL1000E2
- DL2000E2

For additional resources and support visit

datalocker.com

DataLocker®