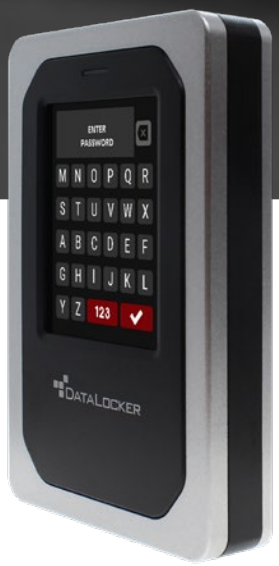
DATALOCKER

DL4 FE ENCRYPTED DRIVE

FIPS 140-3 Level 3 Validated Encrypted Drive With Powerful Remote Management



SECURE TO THE CORE

The DL4 FE is a FIPS 140-3 Level 3 validated device built around a powerful AES 256-bit cryptographic hardware architecture that then adds layer after layer of security with automated policies that intelligently change its security posture based on its location, how it's being used, and the type of data being stored on it. The DL4 FE is a TAA-compliant device that meets the strictest security requirements while offering large capacity (up to 15.3TB) and an easy-to-use touchscreen for setup and use. A powerful addition to the DataLocker line of securely managed solutions, the DL4 FE continues our proud tradition of providing Simply Secure™ solutions, plus it's backed by a 3-year limited warranty.

Powerful Encryption Right Out Of The Box

Everything you need to encrypt data is built into the FIPS 140-3 Level 3 and Common Criteria validated DL4 FE. No drivers. No setup. Just iron-clad, hardware-based AES 256-bit encryption in an easy-to-use interface is further guarded by an army of automated security policies.

Never Risk Losing Your Data

Remote management policies with SafeConsole® lets admins remotely lock, erase or render devices unusable with remote device detonate, destroying all data in cases of attempted theft. SilentKill™ further gives users a special code to destroy the device's encrypted data in case of emergencies.

Ensure User Adoption With Easy-to-Use Touchscreen

A color touchscreen gives end-users quick access to secure data and allows them to customize their device. On-screen instructions make setup fast and easy. Randomized keypad layout with letters, numbers and special characters prevents surface analysis of fingerprints or prevents threat actors from guessing a repeated input pattern.

Remotely Manage & Audit Your Entire Fleet

All DL4 FE drives are remotely manageable with SafeConsole, giving admins the ability to remotely lock or wipe drives, reset passwords, view last-used locations, and see what data has been added, removed, or changed on the drive. Set device or group-specific policies for all the drives in your fleet.

Get a Custom Demo

datalocker.com | sales@datalocker.com

THE DL4 FE

FIPS 140-3 Level 3 Validation
FIPS 140-3 Level 3 validated with a Common Criteria EAL5+ certified controller inside. Provides always-on hardware-based encryption. Dedicated AES 256-bit XTS mode crypto engine meets rigorous cryptographic standards and is more secure than software-based alternatives. Expoxy coated internals and enclosure for increased physical security.

SilentKill™
Allow users under duress to destroy the device or the stored data without leaving traces by entering a special code (admin configurable).

Fully Manageable Device
Use DataLocker SafeConsole to manage individual and groups of devices using automated policies.

Admin Policies & User Data Recovery
Admins can set rigorous password policies (non-sequential, non-repeating special characters, minimum characters). Should users forget a password, admins can unlock the DL4 FE using the admin password. Admins can also recover the user's data by logging in with the admin password. The user will be forced to reset their password upon their next use.

Brute Force Password Protection
When in use, admins can configure how many failed password attempts are needed before the device destroys its payload.

Nothing to Install
All encryption, administration, and authentication performed on the DL4 FE unit. This means devices in standalone mode don't require a software agent; they work right out of the box.

THE DL4 FE MANAGED FEATURES

Remote Device Detonation
Lets admins functionally destroy the device and its data remotely to protect against data or encryption key theft (Admin configurable. Requires SafeConsole).

On Board Anti-malware
Automatically scans files and quarantines/ destroys bad apps/files based on policy settings (optional upgrade. Requires SafeConsole).

Data Geofencing
SafeConsole uses geofencing, trusted networks, and ZoneBuilder to ensure a device changes its security posture based on its location (Admin configurable. Requires SafeConsole).

Comprehensive Audit Capabilities
Have a complete record of file activity (including name changes on the device), password attempts, device locations and machines, device health, and policies in force (Admin configurable. Requires SafeConsole).

TECHNICAL SPECIFICATIONS

CAPACITIES
SSD: 1TB, 2TB, 4TB, 7.6TB, 15.3TB

HDD: 1TB, 2TB

DIMENSIONS
L: 12.3 cm (4.8 in)
W: 7.7 cm (3 in)
H: 2.1 cm (.82 in)

WEIGHT
.65 lbs / 294 grams and up

PHYSICAL SECURITY
Kensington Security Slot™

Epoxy coated internals and robust enclosure

CRYPTOGRAPHIC PROCESS
FIPS 140-3 Level 3 validated, Certificate #5091

AES 256-bit XTS hardware encryption onboard

Integrates a Common Criteria EAL 5+ certified secure microprocessor

INTERFACE
USB-C on the device, compatible with USB 3.2, USB 2.0 (7.6TB drives and under)

15.3TB requires USB Type-C (15W+) - to use on hosts with USB A, a powered USB-A hub with USB-C ports is required.

(USB-C to USB-A and USB-C to USB-C cables included)

TRANSFER SPEEDS

Type	Read	Write
SSD	USB-C 3.2 -258 MB/s	USB-C 3.2 -244 MB/s
	USB 3.0 -260 MB/s	USB 3.0 -248 MB/s
	USB 2.0 -39 MB/s	USB 2.0 -32 MB/s
HDD	USB-C 3.2 -149 MB/s	USB-C 3.2 -147 MB/s
	USB 3.0 -149 MB/s	USB 3.0 -152 MB/s
	USB 2.0 -39 MB/s	USB 2.0 -31 MB/s

STANDARDS AND CERTIFICATION
FIPS 140-3 Level 3 Validated
TAA Compliance
IP64 Certified
RoHS Compliant
FCC, CE, UKCA, KC, WEEE

DEVICE LANGUAGES
English, French, German, Spanish

MANAGEMENT COMPATIBILITY
Microsoft Windows

OS COMPATIBILITY
Microsoft Windows, macOS®, Linux® or any machine that supports a USB mass storage device.

PART NUMBERS
DL4-1TB-FE
DL4-2TB-FE
DL4-SSD-1TB-FE
DL4-SSD-2TB-FE
DL4-SSD-4TB-FE
DL4-SSD-7.6TB-FE
DL4-SSD-15.3TB-FE

WARRANTY
3-year limited warranty

TRUSTED BY

DATALOCKER®
SIMPLY SECURE

Get a Custom Demo

datalocker.com | sales@datalocker.com