Aegis Fortress

FIPS 140-2 VALIDATED ENCRYPTED USB 3.0 DRIVE

- FIPS VALIDATED 140-2 LEVEL 2 PORTABLE USB 3.0 DRIVE
- AES-XTS 256-BIT HARDWARE ENCRYPTION
- SOFTWARE-FREE SETUP & OPERATION
- ONBOARD KEYPAD AUTHENTICATION SHARES NO CRITICAL SECURITY PARAMETERS WITH HOST
- AEGIS CONFIGURATOR COMPATIBLE
- ADMIN FORCED ENROLLMENT
- USER FORCED ENROLLMENT
- INDEPENDENT ADMIN / USER PINS
- DATA RECOVERY PINS
- NO ADMIN RIGHTS NEEDED
- IP66 CERTIFIED: DUST & WATER RESISTANT
- INTEGRATED SUPER SPEED USB 3.0 CABLE
- ADMINISTRATOR MODE
- COMPATIBLE WITH ANY USB PORT AND OPERATING SYSTEM WINDOWS®, MAC®, LINUX, ETC.
- BUS-POWERED
- DRIVE RESET FEATURE
- UNATTENDED AUTO LOCK & SELF DESTRUCT PIN
- BRUTE FORCE PROTECTION
- TAA COMPLIANT / GSA DISCOUNTS
- 3-YEAR WARRANTY

FIPS 140-2 Level 2 Validated

USB 3.0

Protects Data From Theft AND the Elements.

Tested and validated to meet NIST FIPS 140-2 Level 2 requirements with an easy-to-use keypad that is IP66 certified as impervious to dust and grit, the Aegis Fortress brings software-free setup and operation, with onboard PIN authentication.

Military-Grade 100% Hardware Encryption: Featuring AES-XTS 256-bit hardware encryption, the Aegis Fortress seamlessly encrypts all data on the drive in real-time, keeping your data safe even if the hard drive is removed from its enclosure.

Software-Free Design: The Aegis Fortress is ready to use right out of the box–no software, no drivers, no updates. It can even be utilized where no keyboard is present. Completely cross-platform compatible, the Fortress excels virtually anywhere–PCs, MACs, Linux, or any OS with a powered USB port and a storage file system.

Configurable: Create custom profiles and mass configure multiple Configurator-compatible Aegis devices at once with Apricorn's new Configurator / Powered Hub bundle.

Embedded Keypad: All PIN entries and controls are performed on the keypad of the Aegis Fortress. No critical security parameters are ever shared with the host computer.

FIPS 140-2 Level 2 Validated: The Aegis Fortress FIPS 140-2 validation is the cryptography standard required by the US federal government for protection of sensitive data. It covers 11 areas of its cryptographic security system, including physical security, cryptographic key management and design integrity. Tested and validated by the National Institute of Standards and Technology (NIST) for use by the Federal governments of the USA, Canada and others, the Aegis Fortress Drive is based on Apricorn's FIPS 140-2 Level 2 validated encryption module as indicated by certificate #2835. The Fortress' security policy is located on the NIST site at http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2835.pdf. The epoxy coated boundary includes all encryption functions and all Critical Security Parameters (CSPs) such as PIN storage, encryption key generation and storage, random number and seed generators, and all firmware storage. The FIPS module is a complete encryption system, and all CSPs never leave the boundary and are never shared with a host system. By design, the HDD/SSD that stores the encrypted data is excluded from this boundary to both maximize affordability and product line flexibility in capacity and form factor offerings.

Lock-Override Mode: Designated for specific cases in which the drive needs to remain unlocked, e.g., during reboot, passing the drive through a virtual machine, or other similar situations that would normally prompt the Fortress to automatically lock. When enabled, Lock-Override Mode allows the drive to remain unlocked through USB port re-enumeration and will not re-lock until USB power is interrupted.

Two Read-Only Modes: Perfect for accessing data on the drive in a public setting to protect against USB viruses. Particularly important in forensics, Read-Only Mode is ideal for applications that require data to be preserved in its original, unaltered state and can't be overwritten or modified. The Fortress has two read-only modes. One is set by the admin within the admin mode and can't be modified or disabled by anyone other than the admin. The second read-only mode can be set and disabled by anyone with a recognized PIN.

Auto Lock feature and Self Destruct PIN: With the Aegis Fortress, you can set the unattended drive to lock after a pre-determined amount of time. Additionally, you can pre-program your own unique Self Destruct PIN which, once implemented, instantly destroys all PINs and data on the drive and creates a new encryption key.

Brute Force Protection: After a predetermined number (programmable; up to 20) of incorrect PIN entry attempts, the Aegis Fortress will conclude that it is under *Brute Force Attack* and will respond by performing a crypto-erase – deleting the encryption key which will render all of the drive's data useless.

Wear Resistant Key Pad - Water & Dust Resistant: Designed with protection in mind, the Aegis Fortress's keypad is impervious to dust, grit, and water, and it's wear-resistant which defends against tipping off a potential hacker to the most frequently used keys on the drive.

Integrated USB 3.0 Cable: Never forget your cables again. Connect the drive at the flick of a fingertip.

APRICORN

Aegis Fortress

FIPS 140-2 VALIDATED ENCRYPTED USB 3.0 DRIVE

FIPS 140-2 Level 2 Validated

Security	Benefits
Onboard Wear-Resistant Keypad for Authentication	Unlock the drive with your own unique 7 to 16 digit PIN and the addition of the "Shift" key, the Aegis Fortress can double the number of possible PIN combinations, further preventing brute force access to the drive's data
Real-time 256-bit AES-XTS Hardware Encryption	100% of your data is hardware-encrypted on-the-fly with military-grade, full-disk AES XTS encryption
Software-Free / Cross-Platform Compatible	Requires no software to set up or operate – completely cross-platform compatible; works with Windows, Mac, Linux and embedded systems
Administrator Mode	Allows enrollment of one Administrator for setting parameters for PIN management, Read-Only, Auto-Lock, Self-Destruct, Lock-Override, and Brute Force
Forced-Enrollment / User Forced Enrollment	With no default factory preset PINs, the Admin is required to create a unique PIN at setup prior to use; forced enrollment feature can also be extended to first User PIN before use
Programmable Minimum PIN length	For added PIN length and enhanced security, minimum PIN length requirement can be increased from 7 characters up to 16 maximum

Features	Benefits
USB 3.0 interface	Super Speed USB 3.0 connection - up to 10x faster than USB 2.0
Water & Dust Resistant	The Aegis Fortress keypad and case is impervious to dust, grit and water
Aegis Configurator Compatible	Multiple Fortress or other Aegis Configurator compatible devices can be configured at the same time in a matter of seconds with pre-set device profiles.
Advanced Options / Modes	2 Read-Only Modes, Lock-Override Mode, Self-Destruct PIN
LED Flicker Button Confirm	Indicates positive button entry with visual LED confirmation
Recovery PINs	4 one-time use PINs to recover Data in cases of forgotten User / Admin PINs
Unattended Auto Lock	Automatically locks after a pre-determined amount of time or when USB hub power is interrupted
Programmable Brute Force Protection	Program the number of incorrect PIN entries allowed; defends against grand-scale automated and physical attempts to guess the PIN
Drive Reset Feature	Infinite number of resets; performs a crypto-erase with new encryption key regeneration
Compatible on any system	Works with Windows®, Mac® and Linux
Hard Drive Capacities	HDD: 500GB, 1TB, 2TB*; SSD: 512GB, 1TB, 2TB, 4TB, 8TB
Box Contents	Aegis Padlock Fortress, Quick Start Guide, USB Y-cable and travel pouch

Specifications	
Interface	Super Speed USB 3.0 (Backwards compatible with USB 2.0)
Power Supply	100% bus powered
Buffer Size	8MB
RPM	Available with either a Standard 5400 RPM hard drive or SSD
Average seek time	12 ms
Shock - non operating	1000G 1ms (non operating)	300G 2ms (operating)
Dimensions & weight	19mm X 84.5mm X 120mm (0.75" X 3.3" X 4.7") weight: 6.7 oz.
Warranty	3 year limited
Approvals	RoHS FC CE FIPS 140-2 Level 3 (CERT #2835), IP-66
System Requirements	OS independent: Windows, Mac® OS, Linux, Android, Symbian
Ordering Information	**Apricorn Part Number: A25-3PL256-xxxxF** (xxx=drive size in GBs)

*One gigabyte (GB) = one billion bytes; accessible capacity will be less and actual capacity depends on the operating environment and formatting.

APRICORN