Product Datasheet: CipherDriveOne™ and CipherDrive2+

CipherDriveOne™

CipherDrive2+

Ortman Consulting is an authorized SDVOSB reseller of KLC Group's CipherDriveOne™ and CipherDrive2+ Full-Disk Encryption software. These products are the first Authorization Acquisition (AA) host encryption software solutions that meet NSA Data-at-Rest (DAR) and NIAP collaborative Protection Profiles (cPPs) for full disk encryption.

CipherDriveOne™ and CipherDrive2+ provide unparalleled protection to computers and servers using pre-boot disk locking. This software locks the entire hard drive – not just individual data files. NSA-grade encryption keys must be unlocked by an authorized account before the operating system, virtual machine, or any files stored on the protected disk can be read or executed. CipherDriveOne™ and CipherDrive2+ protect high-value, mobile, and deployed computing systems against unauthorized access, data theft, and privacy breaches.

Purchase through GSA Advantage:

www.ortmanconsulting.com/orders

Email: orders@ortmanconsulting.com

Phone: 202 905 2648

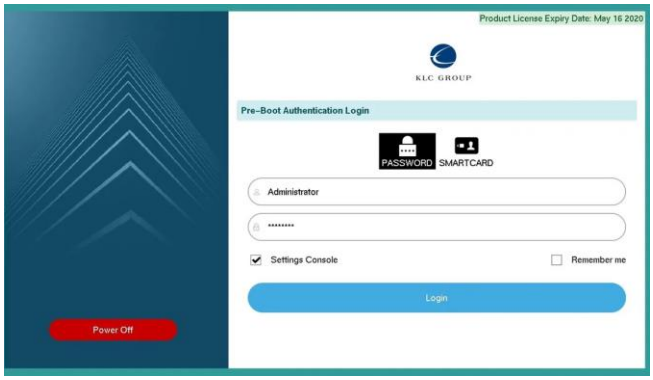
Web: www.ortmanconsulting.com

SECURITY SPECIFICATIONS

- Encryption - AES-256, FIPS PUB 197 specification
- NIAP and Common Criteria FED Certification
- Authentication Acquisition (AA) software
- Compliant under collaborative Protection Profiles (cPP)
- Pre-Boot Authentication (PBA) supports booting and chain loading Open XT / SecureView.
- PBA Admin and Management capabilities
- 2-Factor / Multi-factor Authentication support
- Support for CAC/PIV/CIV and SIPRNET cards and tokens
- Cryptographic Erase (CE)
- User Management module
- TPM 2.0 support
- Key Management – No recovery feature
- Boot package for initial setup and implementation of solution

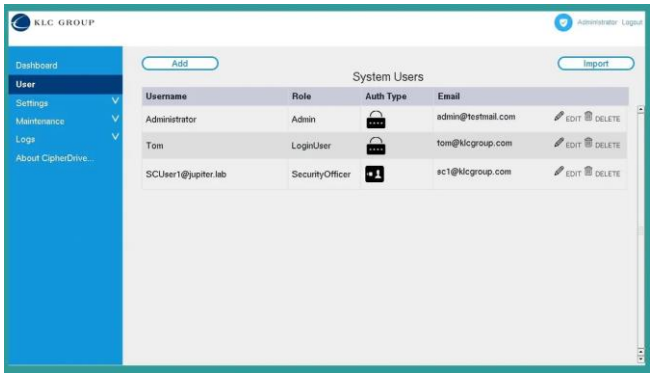
KEY FEATURES

Pre-boot Locking and Strong Authentication: CipherDriveOne and CipherDrive2+ provide pre-boot authentication. Once a computing system powers on, CipherDriveOne prompts the user for authentication (password or smartcard token).



Military Grade Encryption: CipherDriveOne and CipherDrive2+ utilize military grade encryption algorithms with FIPS-140-2 and Common Criteria certification.

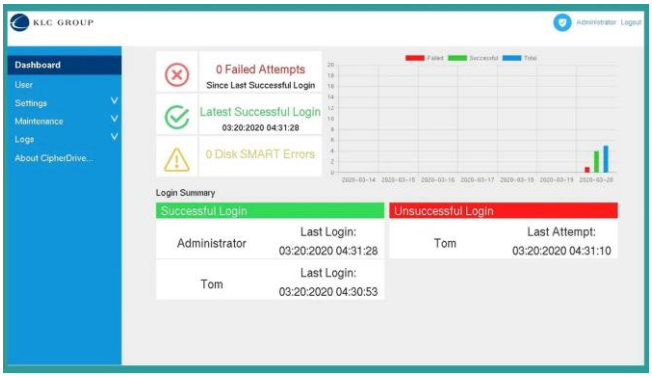
Multiple User Configuration: CipherDriveOne and CipherDrive2+ can be configured to allow multiple users to unlock drive or drives on a computing device.



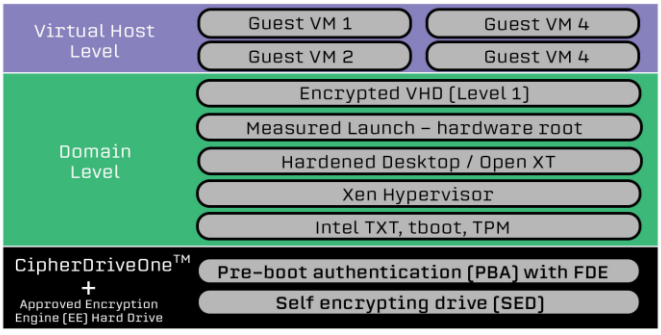
Auditing and Logging: CipherDriveOne and CipherDrive2+ allow administrators to review audit

logs and authentication reports. These reports can be used to meet privacy compliance laws.

Self-Destruct/Crypto Erase: CipherDriveOne and CipherDrive2+ support "self-destruct" of the encryption keys using a configurable "dead-man's switch" feature. The Security Officer or Administrator can issue a Crypto Erase command to cryptographically erase all the data on the drive.



Secure Virtualized Systems: CipherDriveOne and CipherDrive2+ integrate with the latest hardware and software virtualization technologies. Encryption protection at the volume/partition level makes management and configuration simple. Chain boot services living outside CipherDrive's Pre-Boot Authentication boundary makes it easier to integrate into OpenXT, SecureView, and other VM systems.



Special Features of CipherDrive2+: CipherDrive2+ allows managing and unlocking multiple physical drives on the same computing device from one single local interface. This feature is especially useful for higher-end computers and servers in mobile and deployed environments where DAR must be implemented across multiple hard drives.

SYSTEM REQUIREMENTS

Disk types supported: SATA/NVMe OPAL-2 compliant Self Encrypting Drives (SED) drives – Ortman Consulting offers compatible Digistor drives bundled with CipherDriveOne software through our GSA Advantage purchase portal

Operating Systems supported: Windows, Linux, OpenXT

ACHIEVE COMPLIANCE WITH GLOBAL PRIVACY STANDARDS

- Health Insurance Portability and
- Accountability Act (HIPAA)
- California Consumer Privacy Act (CCPA)
- Sarbanes-Oxley Act (SOX)
- General Data Protection Regulation (GDPR)
- The Payment Card Industry Data Security Standard (PCI-DSS)

Security Service	CNSA Suite Standards	Protection Level
Confidentiality (Encryption)	AES-256 / FIPS PUB.197	Up to Top Secret
Authentication (Digital Signature)	Elliptic Curve Digital Secure Algorithm (ECDSA) over the curve P-384 with SHA-384 / FIPS PUB 186.4 RSA 3072 (Minimum) / FIPS PUB 186.4	Up to Top Secret
Integrity (Hashing)	SHA-384 / FIPS PUB 180-4	Up to Top Secret

KLC GROUP

CSfC Component Listed

All product names, trademarks and registered trademarks are property of their respective owners.