KLC GROUP

FIPS CERTIFIED 140-2

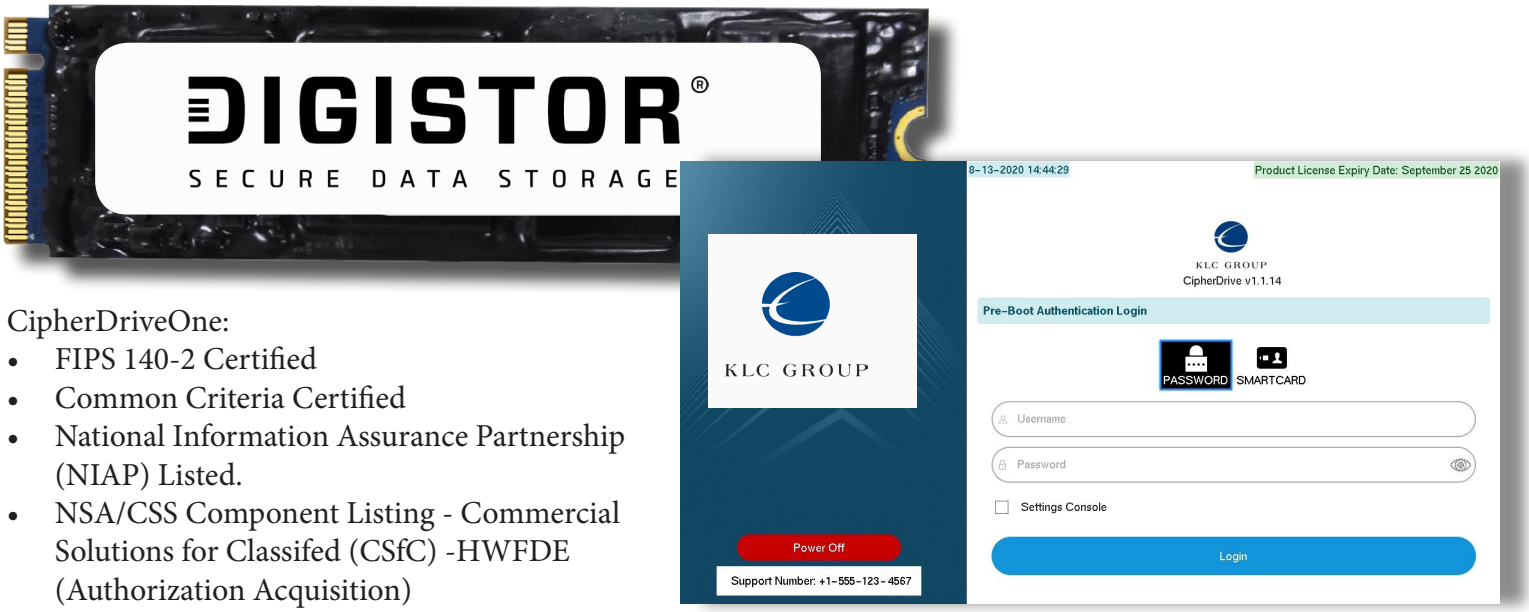
COMMON CRITERIA

NSA CSfC Listed

Partner Program

DIGISTOR® SECURE DATA STORAGE

CipherDriveOne integrated into the Digistor SED with managed multi-factor authentication is the fastest and most secure encrypted SSD Data-at-Rest solution in the world today.



CipherDriveOne:

- FIPS 140-2 Certified
- Common Criteria Certified
- National Information Assurance Partnership (NIAP) Listed.
- NSA/CSS Component Listing - Commercial Solutions for Classifed (CSfC) -HWFDE (Authorization Acquisition)

Protects remote users using laptops and workstations against unauthorized data access.

Easy Integration & OS Agnostic

Microsoft

Linux

SECUREVIEW

vmware®

CipherDriveOne and the Digistor Secure SED SSD provides unparalleled data protection for every computer with advanced pre-boot authentication combined with military grade AES 256-bit encryption. CipherDriveOne provides a managed single, two-factor and multi-factor authentication before the SSD is unlocked and any operating system or virtual machine can start up.

CipherDriveOne Features

Pre-boot Locking

CipherDriveOne protects the computer that is turned off and data is at rest or at an unclassified state. The software authenticates a user before the computer can start the operating system. This method of protection protects the entire Digistor hard drive and not just individual files that may only be password protected or encrypted.

Military Grade Encryption

CipherDriveOne utilizes military grade encryption algorithms with FIPS-140-2 and Common Criteria certification.

Strong Multi-factor Authentication

CipherDriveOne manages users to use username/passwords, 2-factor (smartcards, CAC and SIPR) and multi-factor authentication.

Multiple User Configuration

CipherDriveOne can be configured and managed to allow four user profiles to unlock the desktop or laptop.

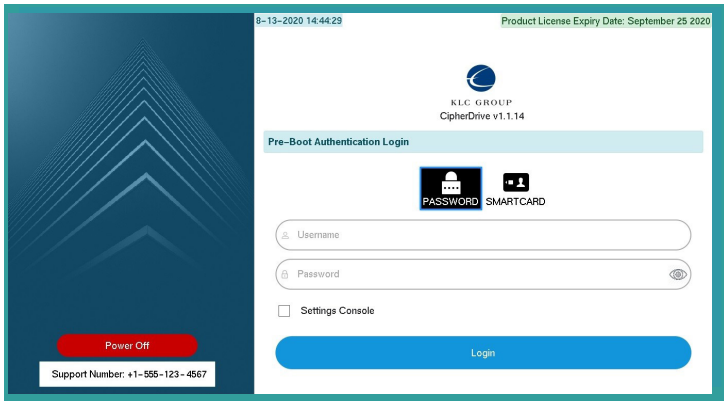
Audit and Logging

CipherDriveOne allows administrators to review audit logs and authentication reports. These reports can be used in investigations, meets privacy compliance laws, and government mandates.

Self Destruct / Cryptographic Erase

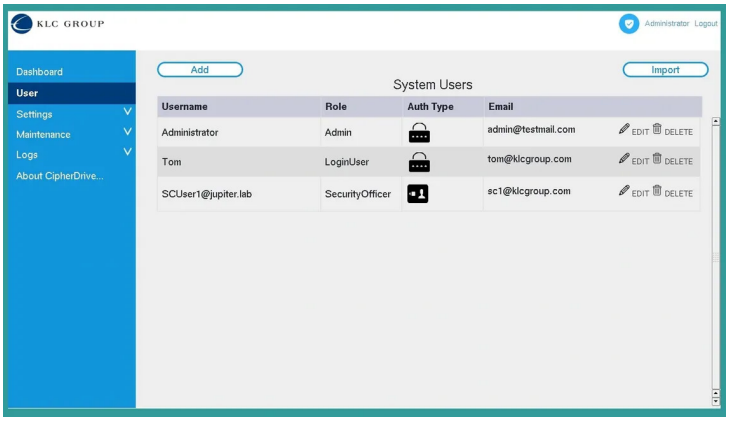
CipherDriveOne supports a "dead-man's switch" for all users using NSA level Cryptographic Erase (CE) of the encryption keys providing a self destruct of the hard drive. The Security Officer or Administrator can also issue a command to cryptographically erase all the data on the drive using CipherDriveOne's Secure Erase feature.

Easy to Use Security



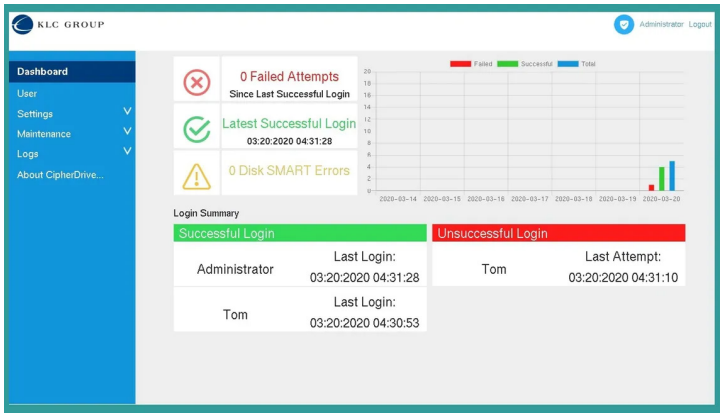
Pre-boot Lock

CipherDriveOne is a pre-boot authentication software. Once the computer user turns on the machine, CipherDriveOne prompts the user for authentication (single, two-factor and multi-factor).



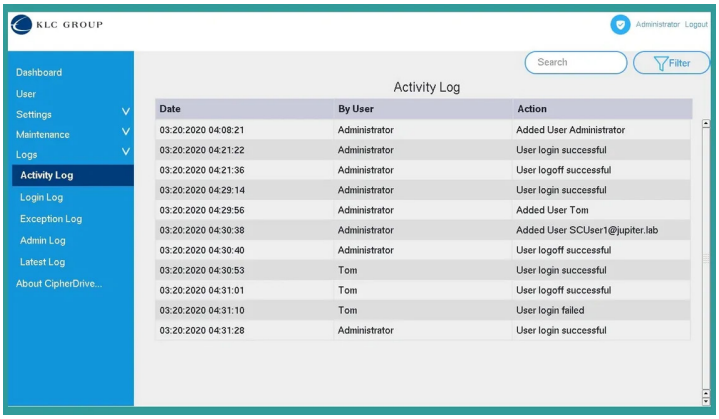
Multiple User Support

CipherDriveOne can be configured and managed to allow multiple users selected from four user profiles (Login User, Administrator, Security Officer and Helpdesk) to unlock and manage the desktop or laptop



Dashboard

The CipherDriveOne dashboard gives a quick and detailed over-view of the security profile of the computer.



Logging

CipherDriveOne offers 5 detailed logging types, Administrators can review the security profile of the computer and mitigate unauthorized access.

KLC GROUP

FIPS CERTIFIED 140-2

COMMON CRITERIA

NSA CSfC Listed

Partner Program

DIGISTOR® SECURE DATA STORAGE

Protecting Your Data

In accordance with Common Criteria collaborative Protection Profiles (cPP), CipherDriveOne can be installed and will manage key exchange with the Digistor Secure SED (cPP Encryption Engine). CipherDriveOne and the Digistor solution is available to be integrated into a CSfC one or two-independent layer security solution today.

Secure Your Data-at-Rest

CipherDriveOne is a Authorization Acquistion (AA) host software solution that manages the Digistor Secure SED Encryption Engine (EE). This flexibility allows government customers the ability to provide storage of classified, secret, and top-secret data in accordance with the Commercial Solutions for Classified (CSfC) program conforming to a number of different solution designs in Section 6 of the NSA's DAR Capability Package 5.0 - Nov 2020.

Remote Computers - Secure your mobile workforce using CiphperDriveOne's pre-boot locking software. CipherDriveOne protects the entire contents of the hard drive when the computer is turned on or off. CipherDriveOne is easy to use and requires minimal configuration.

Loss and Theft - Organized criminals can remove hard drives from any system to retrieve the data using a number of hacker tools. CipherDriveOne protects your intellectual property from accidental loss or the stealing of confidential data by thieves.

CipherDriveOne Features

- FIPS 140-2 Certified - AES-256 Encryption
- Common Criteria Certification and NIAP listed
- NSA CSfC Component Listed - HWFDE Authentication Acquisition (AA) software
- collaborative Protection Profiles (cPP) HWFDE AA
- Pre-Boot Authentication (PBA) supports booting and chain loading VMs / SecureView.
- PBA Admin and Management capabilities
- Single, 2-Factor / Multi-factor Authentication
- Support for CAC/PIV/CIV and SIPRNET cards and PIV certificates
- Cryptographic Erase (CE)
- User Management - four profiles roles
- TPM 2.0 support
- Key Management – Custom AK and DEK
- Custom signed binaries for SecureBoot
- Operating system agnostic - supports Windows, Linux and Virtual Machines

Privacy Compliance

Comply with data protection mandates

Meet and exceeds local, federal, and international privacy compliance rules and policies.

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

CipherDriveOne™+ Digistor Secure SED

Technical Specifications

M.2 SSD Secure SED are Self-Encrypting Drives securing all critical data using strong AES 256-bit Encryption. TCG Opal 2.0 specificaton with AES 256-bit encryption means the encryption/decryption is performed on device, independent from the host, reducing CPU load.

Models Available:

DIGISTOR 512GB M.2 SATA III Solid State Drive, TAA Compliant, FIPS 140-2 L2
DIGISTOR 1TB M.2 SATA III Solid State Drive, TAA Compliant, FIPS 140-2 L2
DIGISTOR 2TB M.2 SATA III Solid State Drive, TAA Compliant, FIPS 140-2 L2
DIGISTOR 512GB M.2 2280 PCIe (3x4) NVMe Solid State Drive, TAA Compliant, FIPS 14-2 L2
DIGISTOR 1TB M.2 2280 PCIe (3x4) NVMe Solid State Drive, TAA Compliant, FIPS 14-2 L2
DIGISTOR 2TB M.2 2280 PCIe (3x4) NVMe Solid State Drive, TAA Compliant, FIPS 14-2 L2

Form Factor	M.2 2280	MTBF	More than 2,000,000 hours
SATA Interface	SATA III SATA Revision 3.2	Advanced Flash Management	Static & Dynamic Wear Leveling Bad Block Management TRIM SMART
Flash Interface	Flash type: BiCS3 TLC	Encryption	TCG Opal 2.0 hardware level AES 256-bit encryption
Performance	Read: up to 550MB/s Write: up to 530MB/s	Temperature Range	Operation: 0°C ~ 70°C Storage: -40°C ~ 85°C
Power Consumption	Active mode: ≤ 3,735mW Idle mode : ≤ 525mW	RoHS compliant	YES

CipherDriveOne Software Technical Specificatons

Security Service	CNSA Suite Standards / Specification	Protection Level
Confidentiality (Encryption)	AES-256 / FIPS PUB.197	Up to Top Secret*
Authentication (Digital Signature)	Elliptic Curve Digital Signature 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*

* Requires two independent layers of encryption as defined by the NSA DAR 5.0

CDSG /Digistor
1000 SE Tech Center Dr
Suite 160
Vancouver, WA 98683
+1 (408) 796-5140
sales@digistor.com

KLC Group LLC
1900 Camden Ave.
San Jose, CA 95124
1-408-614-1414
sales@klc-group.com