CipherDriveOne

FIPS VALIDATED 140-2

NIAP®

COMMON CRITERIA

NATIONAL SECURITY AGENCY · UNITED STATES OF AMERICA

CSfC Listed

KLC GROUP
CipherDrive v1.2.3

Pre–Boot Authentication Login

PASSWORD   SMARTCARD

Password

☐ Login to Management Console   *Forgot Password?*
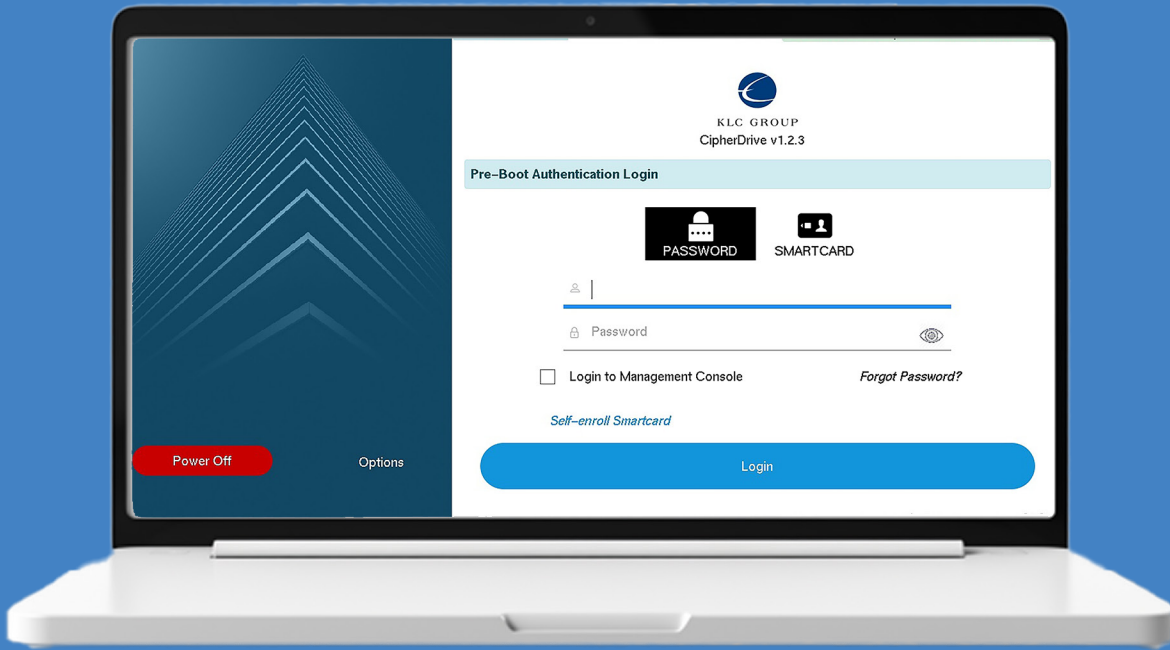
Self–enroll Smartcard

Power Off   Options   Login

Unified Encryption for Data-at-Rest

Experience unparalleled data protection with our cutting-edge solutions – CipherDriveOne is an integral component of our unified encryption suite. Safeguard your sensitive information with ease, efficiency, and confidence. CipherDriveOne is a pre-boot Authorization Acquistion (AA) host software solution that manages a hardware Encryption Engine (EE). This unified encryption solution 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's hardware full disk encryption (HWFDE) standards.
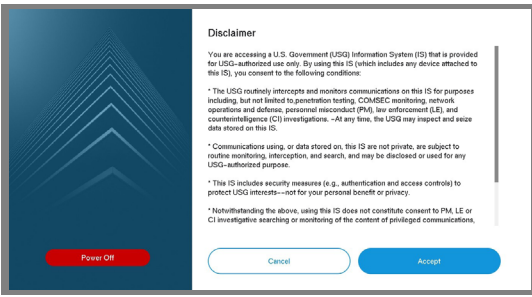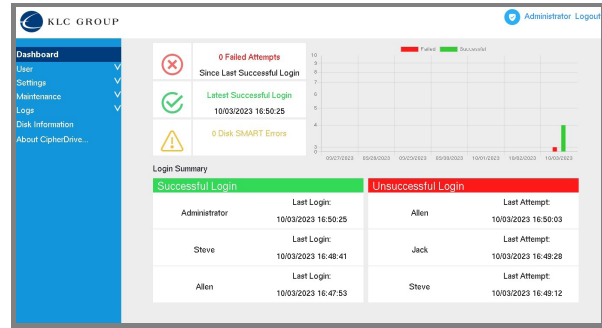
Tablets

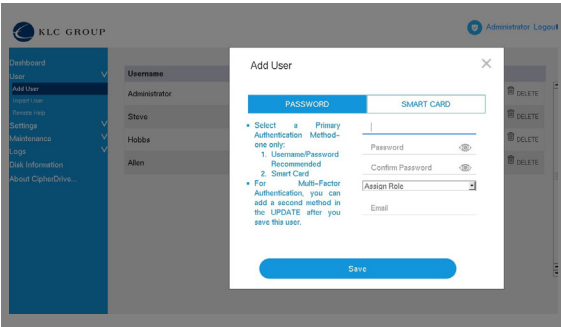### Workstations

Laptops
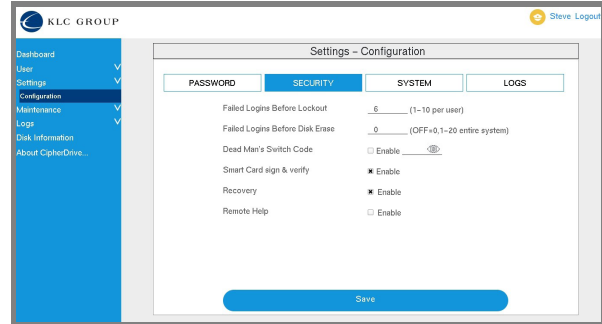
CipherDriveOne Features

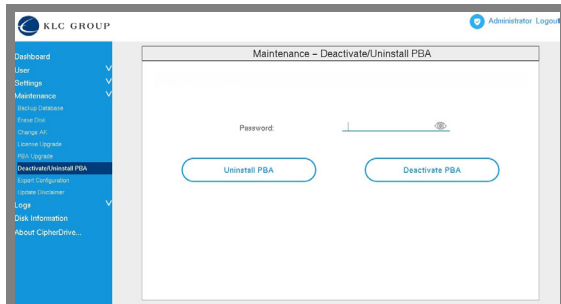A custom disclaimer can be displayed before or after user authentication.

CipherDriveOne features a easy to use management console for setup and administration.

Four different user roles can be set up with 3 forms of authentication: user/pass, smart card, and 2FA.
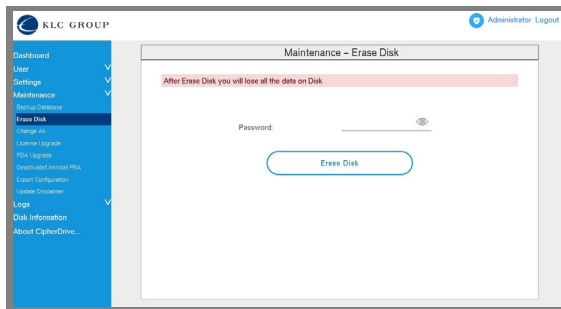

User and system settings are highly configurable from one easy to use location.
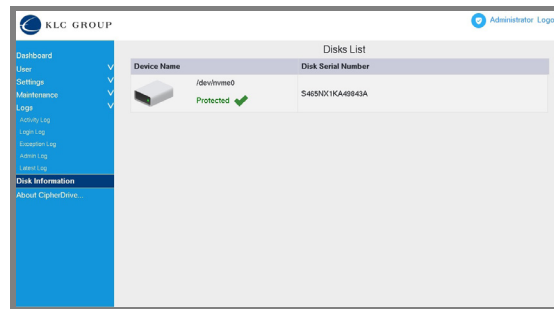

Easy upgrading and exporting of configurations for scalable deployment makes CipherDriveOne the choice of many US and NATO customers.
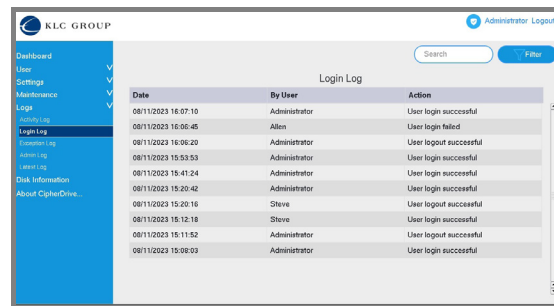
Detailed logging and event data is available to Administrators and Security Officers.

Administrative and rules-based crypto erase can implemented to remove data instantly and permanantely.


Visual confirmation of the harddrive(s) in the system and the one(s) that are protected by CipherDriveOne.

Technical Specifications

CipherDriveOne meets the NSA's Commercial National Security Algorithm Suite (CNSA) suite for DAR

Security Suite	CNSA Suite Standards	Specifications
CONFIDENTIALITY (ENCRYPTION)	AES-256	FIPS PUB 197
AUTHENTICATION (DIGITAL SIGNATURE)	RSA 3072 (MINIMUM)	FIPS PUB 186-4
INTEGRITY (HASHING)	SHA-384	FIPS PUB 180-4
CAN PROTECT	UP TO TOP SECRET	----

Authentication Acquistion (AA) - Single, 2FA & MFA
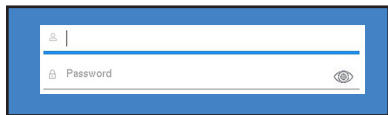
Username / Password

Smart Card
CAC using PIV

Yubikey
PIV

USB
Hashed Secret
(Stealth Version Only)

Encryption Engine (EE) - Advantech 2040 & 2020 Series SSDs (Sold Separately)

- AES-256 Encryption
- TCG OPAL 2.0
- Operating Temp: 0 - 70 Celsius
- Shock: 1500G, Peak /.05 ms
- Vibration: 20G, Peak / 80-2000 Hz
- Gold plated pins
- Layer 2 tamper proof coating
- 3-year warranty
- Optional "keep your drive" for classified environments
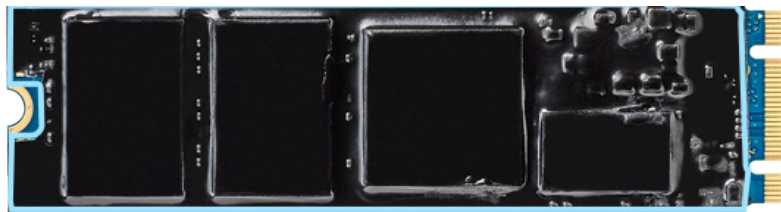
Available in NVMe & SATA

NIAP "In Evaluation" December 2023

Operation System Agnostic - CipherDriveOne Installs On Shadow Partition

Windows 10/11   RHEL   SECUREVIEW   Forcepoint   ARCHON SECURE ACCESS ANYWHERE   TRIITUS
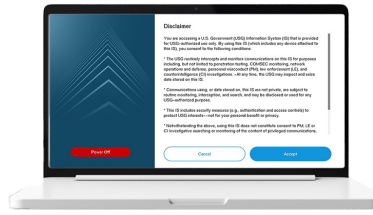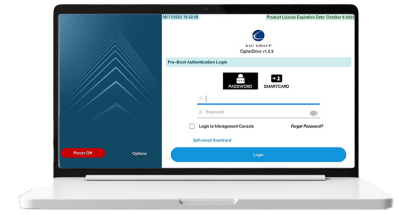
CipherDriveOne - Easy to Use

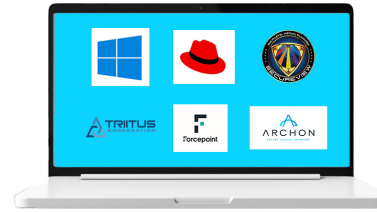Step 1: At power off, CipherDrive-One locks the harddrive(s)

Step 2: At pre-boot, a custom discliamer can be displayed.

Step 3: CipherDriveOne asks for authentication.

Step 4: A successful authentication will unlock the harddrive(s) and the system will soft reboot or chainboot to the operating system.

Step 5: The operating system or thin client loads. If the system is turned off or the harddrive(s) removed, they are locked and data protected using AES-256 bit encryption

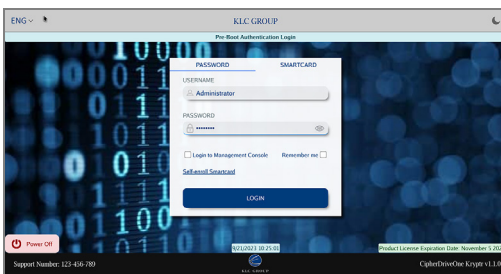# CipherDriveOne Unified Encryption Products
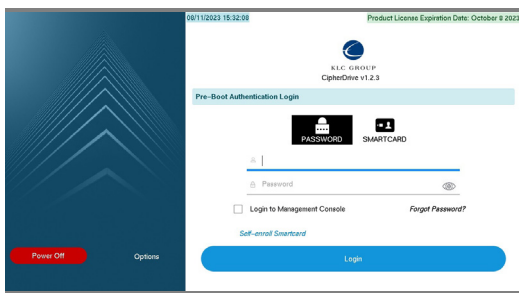
CipherDriveOne
(Single Disk HWFDE)

CipherDriveOne Plus
(Multi-Disk HWFDE)

CipherDriveOne Stealth
(Remote / UAV HWFDE)

CipherDriveOne Kryptr
(Single and Multi-disk SWFDE)

CipherDriveOne™ is Common Criteria certified and on the NSA's CSfC listing for meeting the Data-at-Rest Capability Package.

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