KLC GROUP

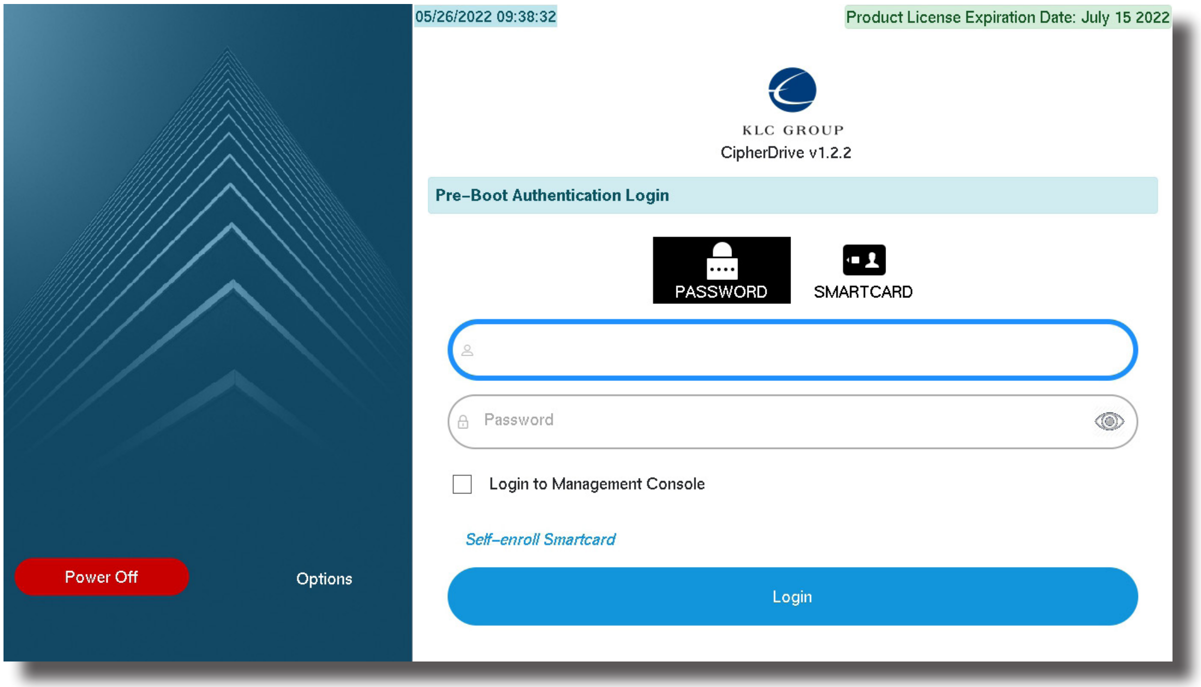
CipherDriveOne

FIPS VALIDATED 140-2

COMMON CRITERIA

NSA CSfC
Listed
HWFDE

DATA-at-REST (DaR)
SSD/HDD Protection



05/26/2022 09:38:32

Product License Expiration Date: July 15 2022

KLC GROUP
CipherDrive v1.2.2

Pre–Boot Authentication Login

□ Login to Management Console

Self–enroll Smartcard

Load, Lock, and Authenticate Any TCG OPAL SSD/HDD

OS Agnostic

Microsoft

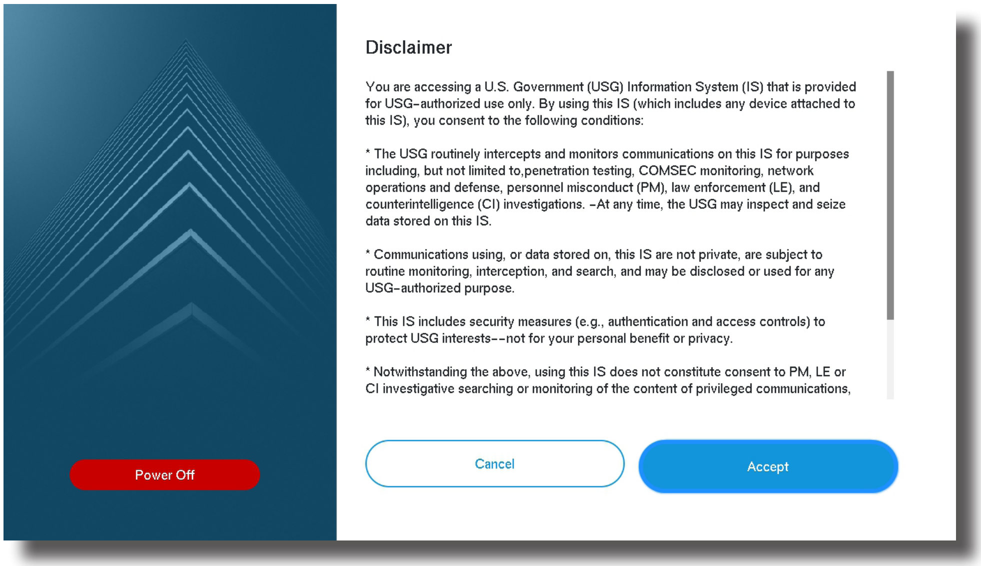
Linux

SECUREVIEW

OpenXT™

CipherDriveOne provides unparalleled Data-at-Rest (DaR) protection for every computer using pre-boot authentication and military grade AES 256-bit encryption. CipherDriveOne installs in the protected shadow partition of the SSD/HDD, where the pre-boot authentication must be acheieved before the SSD/HDD will unlock and the Operating System or Hypervisor machine can start.

CipherDriveOne Technology Features - Easy to Use



Disclaimer

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG–authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

* The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to,penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. –At any time, the USG may inspect and seize data stored on this IS.

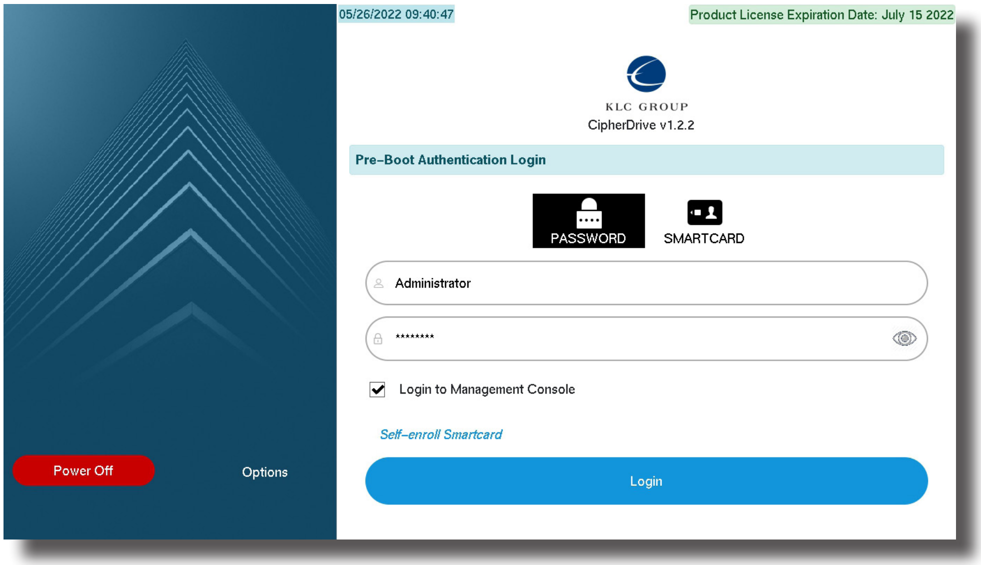
* Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG–authorized purpose.

* This IS includes security measures (e.g., authentication and access controls) to protect USG interests––not for your personal benefit or privacy.

* Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications,

Disclaimer

- CipherDriveOne provides for a pre/post login disclaimer.
- The disclaimer can be customized by the customer.



05/26/2022 09:40:47

Product License Expiration Date: July 15 2022

KLC GROUP
CipherDrive v1.2.2

Pre–Boot Authentication Login

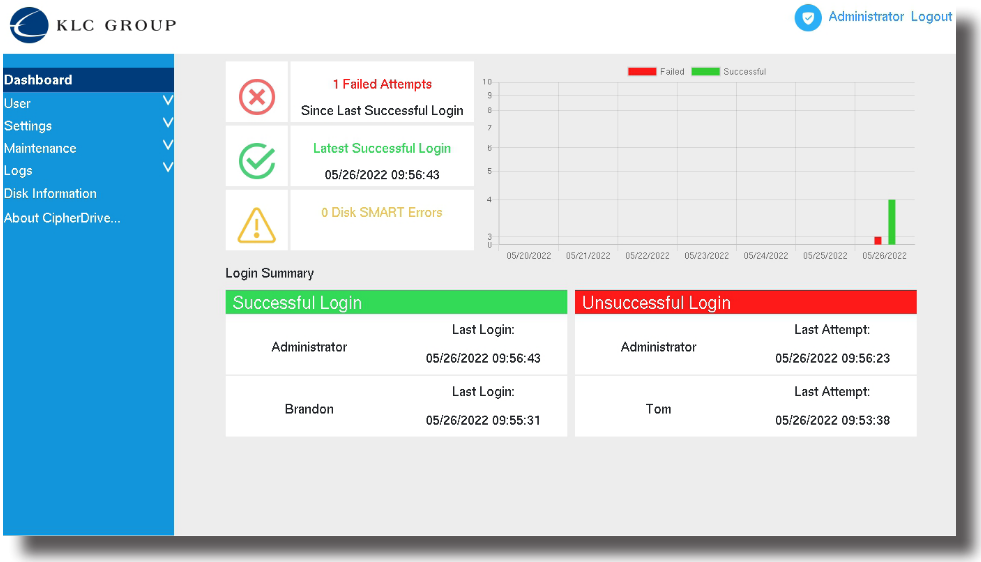
Administrator

****

☑ Login to Management Console

Login Page

- Username/password (SA)
- Smart cards using CAC, SPIRNET, PIV/CIV and YubiKeys (2FA)
- Multifactor Authentication (MFA) combined (SA) plus (2FA)



KLC GROUP

Administrator Logout

1 Failed Attempts
Since Last Successful Login

Latest Successful Login
05/26/2022 09:56:43

0 Disk SMART Errors

Login Summary

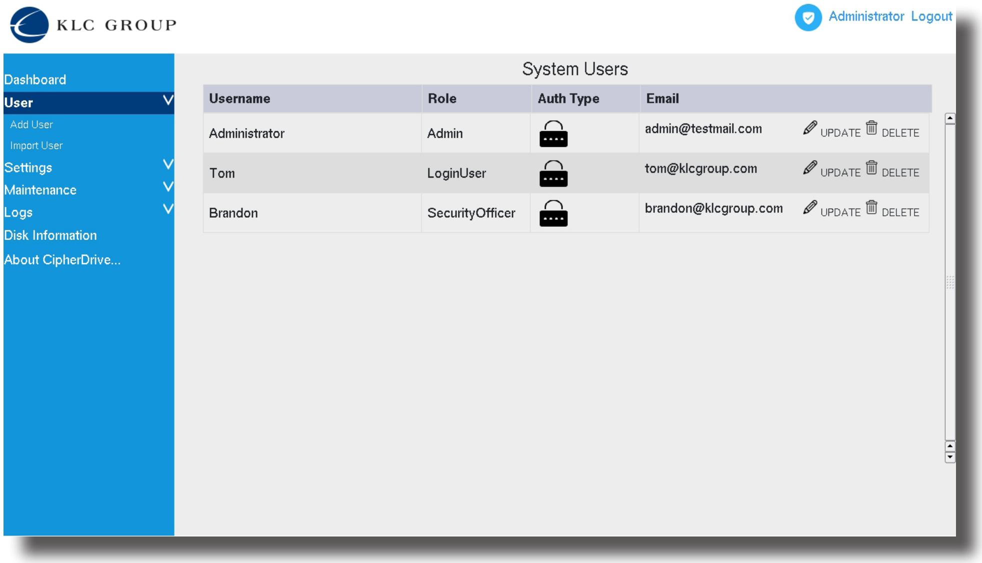
Successful Login		Unsuccessful Login	
Administrator	Last Login: 05/26/2022 09:56:43	Administrator	Last Attempt: 05/26/2022 09:56:23
Brandon	Last Login: 05/26/2022 09:55:31	Tom	Last Attempt: 05/26/2022 09:53:38

Dashboard

- Quick view of system
- Successful logins
- Failed login attempts
- Disk status

www.cipherdriveone.com

CipherDriveOne Technology Features - Easy to Use

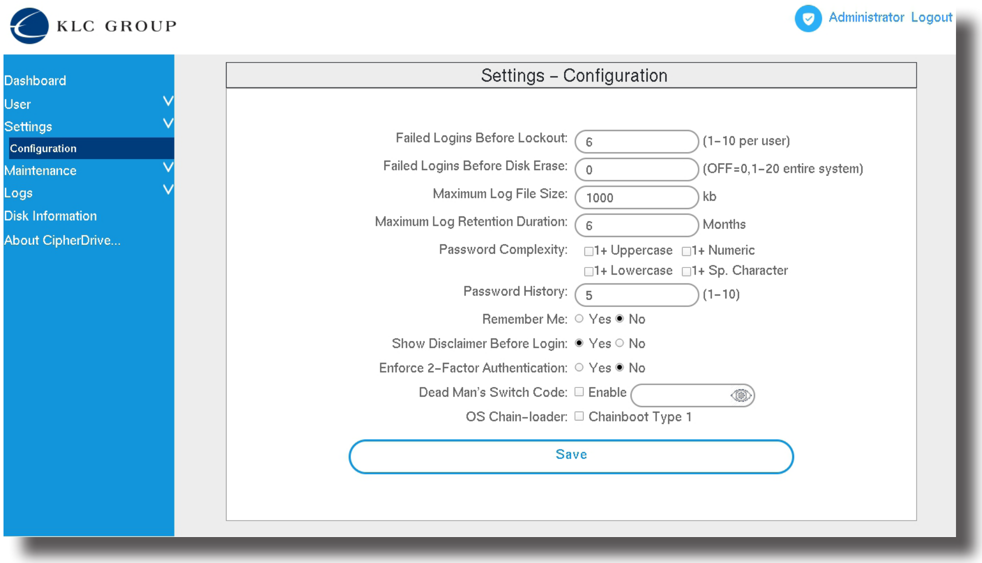


System Users

Username	Role	Auth Type	Email
Administrator	Admin		admin@testmail.com
Tom	LoginUser		tom@klcgroup.com
Brandon	SecurityOfficer		brandon@klcgroup.com

Multi-role Users

- Administrator, Security Admins, Login users, Help Desk
- Import users using .json format
- Remote smart card enrollment

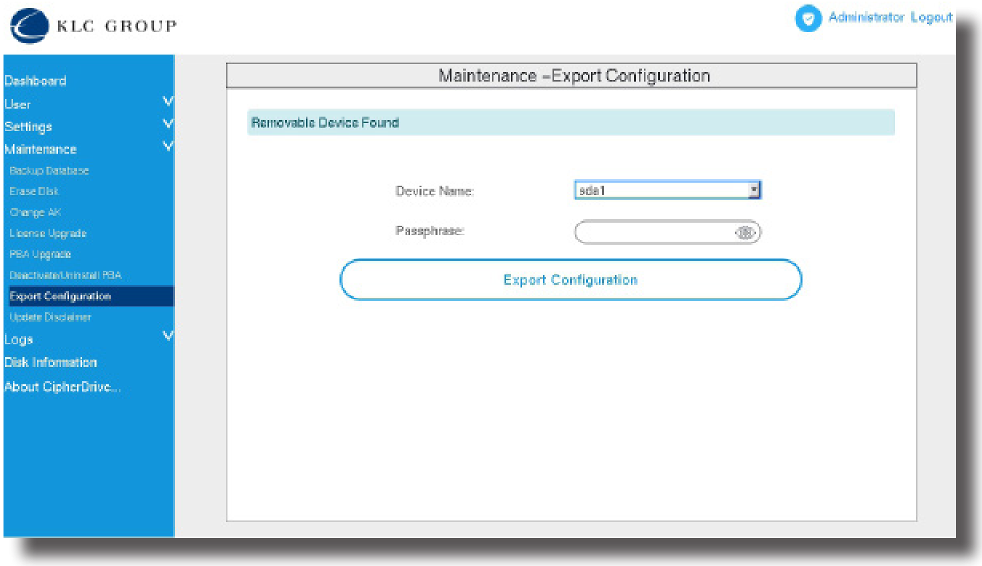


Settings – Configuration

Failed Logins Before Lockout: 6 (1–10 per user)
Failed Logins Before Disk Erase: 0 (OFF=0,1–20 entire system)
Maximum Log File Size: 1000 kb
Maximum Log Retention Duration: 6 Months
Password Complexity: □1+ Uppercase □1+ Numeric □1+ Lowercase □1+ Sp. Character
Password History: 5 (1–10)
Remember Me: ○ Yes ● No
Show Disclaimer Before Login: ● Yes ○ No
Enforce 2-Factor Authentication: ○ Yes ● No
Dead Man's Switch Code: □ Enable
OS Chain-loader: □ Chainboot Type 1

Settings

- Failed Login timeout and Secure Erase
- Password Rules
- Disclaimer Configuration
- Enforce Two-Factor Authentication (2FA)
- Dead Man's Switch
- OS chain loading



Maintenance –Export Configuration

Removable Device Found

Device Name: sda1

Passphrase:

Maintenance

- Secure Erase
- Change AK/DEK Keys
- Upgrade Software
- Deactivate/Uninstall
- Export Configuration
- Custom Disclaimer

www.cipherdriveone.com

CipherDriveOne is an Authorization Acquistion (AA) host software solution that manages any TCG OPAL SSD/HDD. This flexibility allows government customers the ability to provide secure 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.

Available software configurations:

CipherDriveOne (Single-disk)
CipherDrive2+ (Multi-disk)
CipherDriveStealth (UAV/Remote Package)

CipherDriveOne Software Technical Specificatons

- Support for CAC/PIV/CIV and SIPRNET cards and tokens
- 2-Factor / Multi-factor authentication support
- User Management - 4 user roles
- TPM 2.0 support
- Key Management – AK and DEK
- Custom signed bootloader for SecureBoot
- Custom signed bootloader for Forcepoint TTC-R
- Custom signed bootloader for IDtec Archon ZV
- Encryption - AES-256, FIPS PUB 197 specification
- NIAP and Common Criteria Certification
- Authentication Acquisition (AA) software
- Certified under collaborative Protection Profiles (cPP)
- Pre-Boot Authentication (PBA) supports booting and chain loading Open XT / SecureView
- Cryptographic Erase (CE)
- Log Reports

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*

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

* Requires two independent layers of encryption.