



KLC GROUP

Quick Start Guide: Steps to Deploy CipherDriveOne

1. Collect important pre-installation information for CipherDriveOne.

By collecting this information, it can be useful for the installation and record keeping. This information can be used by KLC technical support later to aid in any support tickets. Once you have completed installation, you may want to keep a copy or delete it permanently.

1. Computer make and model: _____

2. Computer BIOS version: _____

3. Hard drive make and model (primary): _____

(secondary): _____

4. Hard drive PSID number (Primary Drive): _____



Suggestion: Take a picture of the PSID number on the hard drive. All OPAL hard drives have a PSID number and if your drive does not, it may not be OPAL compliant and unsuitable for installation of CipherDriveOne.



The PSID number is required to permanently erase the hard drive. You can do this prior to CipherDriveOne installation but all data on the hard drive will be permanently erased! Please refer to the User's Guide on how to boot from the USB and run the commands below.

SYNTAX

`CipherDriveInstaller -d <drive location> -r <PSID number>`

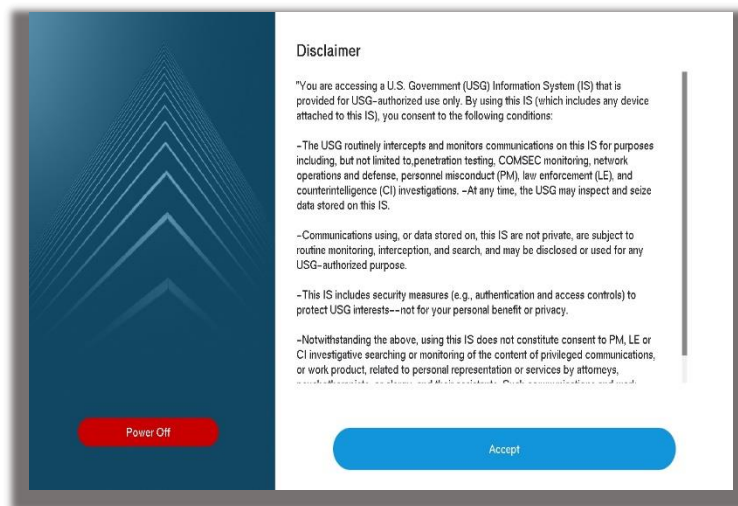
EXAMPLE

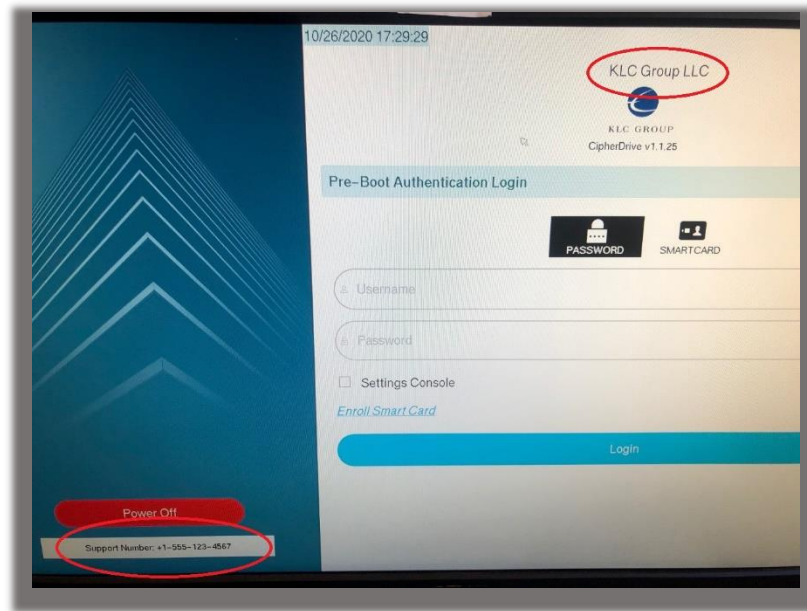
`CipherDriveInstaller -d /dev/nvme0 -r AC9847-475A-AASD-8475-87474646`

5. DEFAULT USERNAME: Administrator

6. Select an Installation Password: _____

2. Create a custom disclaimer, title, and support number for the login screens.





The title is located just above the KLC software logo. The support number appears in the bottom left-hand corner. You may leave these blank.

To create your own custom disclaimer, title, and support number page, please create a json file with your own information. The syntax must comply with json. Save the file in the .json format and you will use this file during the initial installation.

SYNTAX

```
{"Disclaimer Data":"This is where you add text for the disclaimer",  
  "Organization Name":"Add the title you wish to appear over the KLC Logo",  
  "Support Number":"Add your support number" }
```

EXAMPLE

```
{"Disclaimer Data":"You are accessing John's Kingdom and please leave your pledge at the  
door",  
  "Organization Name":"KLC Group LLC",  
  "Support Number":"+1-555-123-4567" }
```

3. Download the CipherDriveOne software and prepare a USB/External bootable drive.

Steps:

- a) Download the software from www.cipherdriveone.com. Contact: john@klc-group.com if you do not have access to the website portal.
- b) Unpack the zip file and copy the files onto a USB/external drive. **The USB must be formatted to FAT32 only.** Make sure that your USB/external drive looks like this:

Name	Date modified	Type	Size
EFI	9/9/2020 5:34 PM	File folder	
EvaluationLicense	9/9/2020 5:34 PM	File	1 KB
Hash	9/9/2020 5:34 PM	Text Document	1 KB
ReadMe - CipherDrive Beta Release_1.1.19	9/9/2020 5:34 PM	Text Document	4 KB

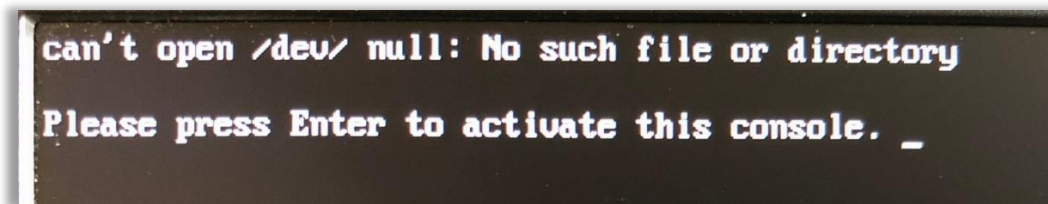
- c) Add the custom disclaimer file (in .json extension) to the USB/external hard drive location. Your boot media should look like this:

EFI	10/27/2020 4:02 PM	File folder	
EvaluationLicense	10/26/2020 7:30 AM	File	2 KB
Hash	10/26/2020 12:07 PM	Text Document	1 KB
Disclaimer	10/26/2020 9:19 AM	JSON File	1 KB
ReadMe - CipherDrive Release_1.1.25	10/26/2020 12:07 PM	Text Document	6 KB

4. Check the locations of TGC OPAL SED Hard Drive and clean the system of previous boot order.

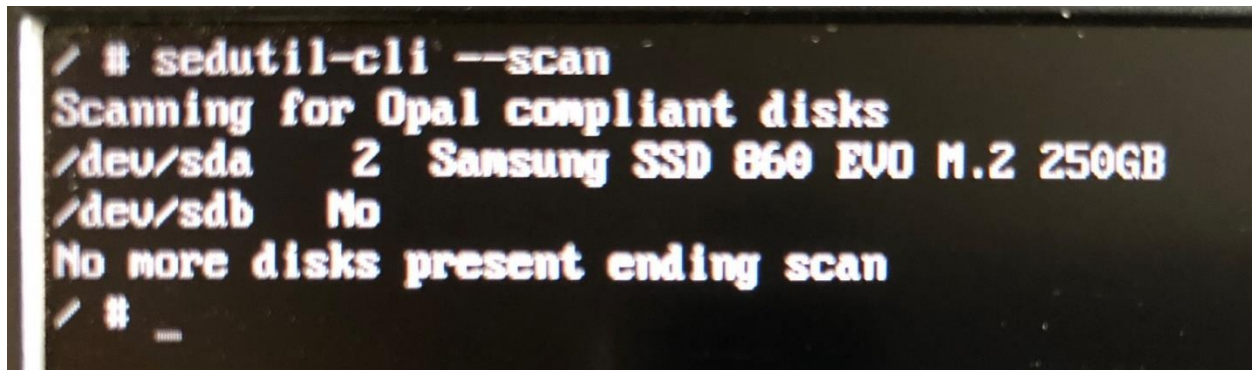
Steps:

- a) Enter the BIOS on your computer system and set the boot order to start the USB drive.
- b) Boot from the USB boot drive with the CipherDriveOne software. Press enter to bring up the root account (#).



```
can't open /dev/ null: No such file or directory
Please press Enter to activate this console. _
```

- c) Type this command: `sedutil-cli --scan` (two dashes together before scan)



```
/ # sedutil-cli --scan
Scanning for Opal compliant disks
/dev/sda      2  Samsung SSD 860 EVO M.2 250GB
/dev/sdb      No
No more disks present ending scan
/ # _
```

d) At the location of the drive (`/dev/sda`), it is followed by a number “2” or “12”. The number “2” or “12” denotes that this drive is Opal compliant. The USB drive located at `/dev/sdb` is not Opal compliant as designated by the word – “No”. **You must have an TCG OPAL compliant drive to install the software.**

Write down the locations of your hard drive: _____

Go the the next step and clean out older boot orders.

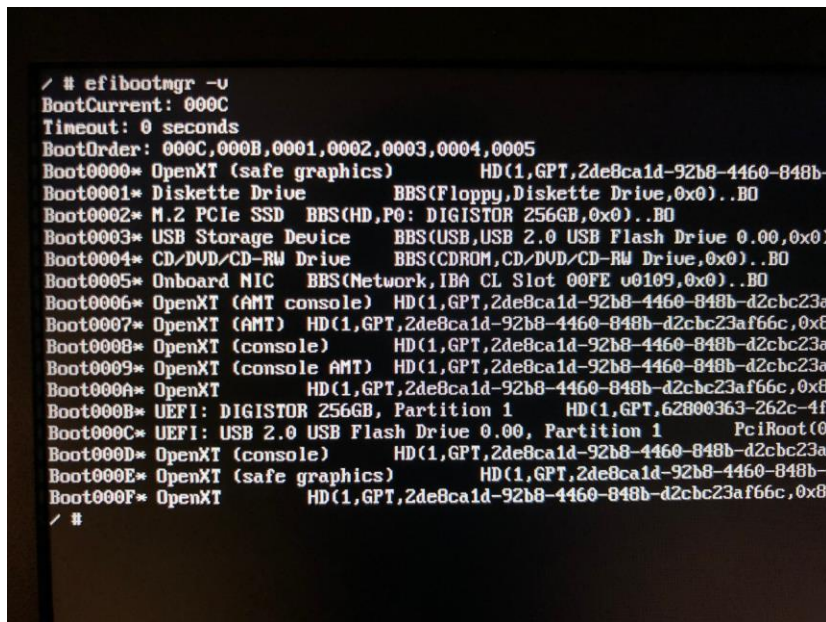
Check and clean older boot orders:

It is important to clean out older operating system boot orders. There are times when the BIOS does not erase the boot order from the efivars. Older boot orders can cause CipherDriveOne or the operating system to reboot over and over.

Check the boot order:

1. Use the unix command: `efibootmgr -v`

This will bring up a list of boot orders – example: `Boot0006* OpenXT (AMT Console)`



```

/ # efibootmgr -v
BootCurrent: 000C
Timeout: 0 seconds
BootOrder: 000C,000B,0001,0002,0003,0004,0005
Boot0000* OpenXT (safe graphics) HD(1,GPT,2de8ca1d-92b8-4460-848b-
Boot0001* Diskette Drive BBS(Floppy,Diskette Drive,0x0)..BO
Boot0002* M.2 PCIe SSD BBS(HD,P0: DIGISTOR 256GB,0x0)..BO
Boot0003* USB Storage Device BBS(USB,USB 2.0 USB Flash Drive 0.00,0x0)
Boot0004* CD/DVD/CD-RW Drive BBS(CDROM,CD/DVD/CD-RW Drive,0x0)..BO
Boot0005* Onboard NIC BBS(Network,IBA CL Slot 00FE 00109,0x0)..BO
Boot0006* OpenXT (AMT console) HD(1,GPT,2de8ca1d-92b8-4460-848b-d2cbc23a
Boot0007* OpenXT (AMT) HD(1,GPT,2de8ca1d-92b8-4460-848b-d2cbc23af66c,0x8
Boot0008* OpenXT (console) HD(1,GPT,2de8ca1d-92b8-4460-848b-d2cbc23a
Boot0009* OpenXT (console AMT) HD(1,GPT,2de8ca1d-92b8-4460-848b-d2cbc23a
Boot000A* OpenXT HD(1,GPT,2de8ca1d-92b8-4460-848b-d2cbc23af66c,0x8
Boot000B* UEFI: DIGISTOR 256GB, Partition 1 HD(1,GPT,62800363-262c-4f
Boot000C* UEFI: USB 2.0 USB Flash Drive 0.00, Partition 1 PciRoot(0
Boot000D* OpenXT (console) HD(1,GPT,2de8ca1d-92b8-4460-848b-d2cbc23a
Boot000E* OpenXT (safe graphics) HD(1,GPT,2de8ca1d-92b8-4460-848b-
Boot000F* OpenXT HD(1,GPT,2de8ca1d-92b8-4460-848b-d2cbc23af66c,0x8
/ #
```

2. Use the unix command: `efibootmgr -B -b 0006`

Remove all boot orders except the UEFI: USB flash drive. This will remove the boot order from the efivars permanently.

3. Reboot the machine into Bios and set your USB to boot first.

5. Install CipherDriveOne



For the Dell 7290 Workstation, you must disable x2aipc in SYSTEM BIOS SETTING - PROCESSOR SETTINGS to boot and install CipherDriveOne.

CipherDriveOne installs the management console on the primary hard drive and a chained pre-boot authentication to all secondary hard drives.

Steps:

- a) Use this command if you have a SATA drive (Without a custom disclaimer file):

SYNTAX

CipherDriveInstaller -d <drive location> -p <password>

EXAMPLE

CipherDriveInstaller -d /dev/sda, -p Admin456

- i. The drive location maybe “sda” or “sda1” – check using the command: `sedutil-cli –scan`
- ii. Add all drive locations to install CipherDriveOne. Each drive will be installed sequentially.
- iii. Note: There is no space after the comma separating the drive locations.

- b) Use this command if you have an NVMe drive (Without a custom disclaimer file):

SYNTAX

CipherDriveInstaller -d <drive location> -p <password>

EXAMPLE

CipherDriveInstaller -d /dev/nvme0 -p Admin567

- i. The drive locations could be “nvme0” or “nvme1” - check using the command: `sedutil-cli –scan`.
- ii. Add all drive locations to install CipherDriveOne. Each drive will be installed sequentially.

```
/ # CipherDriveInstaller -d /dev/sda,/dev/sdb -p Admin456
```

Installation with a custom disclaimer file:

- a) Use this command if you have a SATA drive (With a custom disclaimer file):

SYNTAX

CipherDriveInstaller -d <drive location> -p <password> -l customdisclaimer.json

EXAMPLE

CipherDriveInstaller -d /dev/sda -p Admin456 -l mydisclaimer.json

- i. The drive location maybe “sda” or “sda1” – check using the command: `sedutil-cli –scan`
- ii. Add all drive locations to install CipherDriveOne. Each drive will be installed sequentially.
- iii. Note: There is no space after the comma separating the drive locations.

- b) Use this command if you have an NVMe drive (With a custom disclaimer file):

SYNTAX

CipherDriveInstaller -d <drive location> -p <password> -l customdisclaimer.json

EXAMPLE

CipherDriveInstaller -d /dev/nvme0 -p Admin567 -l mydisclaimer.json



Remember to write down your password in a safe place. You will need it to login to the administrative console. There is no password recovery feature in CipherDriveOne.



For RAID deployments, AHCI must be enabled and RAID will only support SATA hard drives.

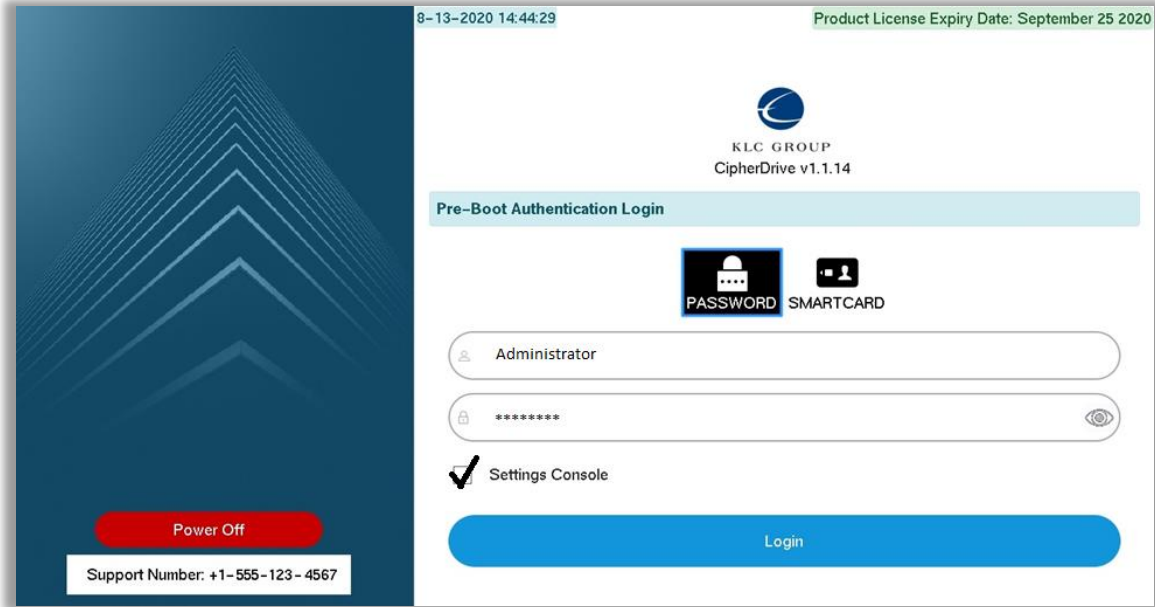
c) The software will start the installation for each drive sequentially. After the software is finished, the computer will shut down. Restart the computer and wait for CipherDriveOne warning disclaimer to appear.

```
Token validated successfully
Activating PBA, please wait...
Retrieve Opal Properties...
Taking Ownership of device...
Activating LSP...
Configuring Locking Range...
MBR done is set to 0
Writing Shadow Partition...
OpalCreateShadowMBR: MaxComPacketSize : 131072
OpalCreateShadowMBR: MaxIndTokenSize : 126976
bufferSize : 60928
Writing PBA to shadow partition: 73 percentage completed
```

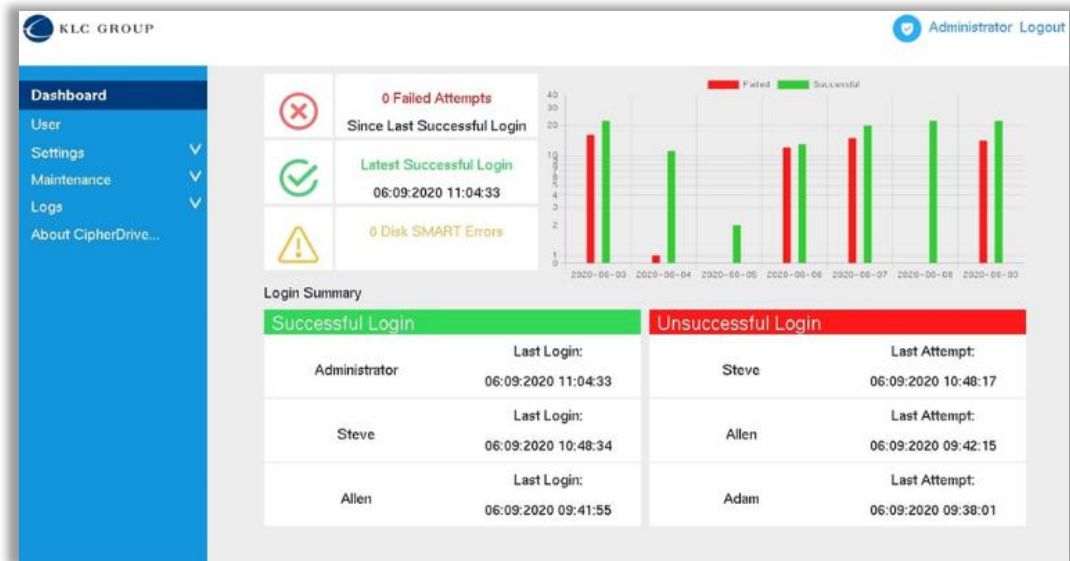
6. Login to the CipherDriveOne, pre-boot authentication software.

Steps:

- a) You will see a legal disclaimer splash screen. Click “Accept” and a login page will appear.
- b) Use the Username: **Administrator (default)** and the **password** you set at installation to login. **Check the Settings Console to enter the Administrative Dashboard.**
- c) Once you authenticate to the primary hard drive, CipherDriveOne will authenticate and unlock all other secondary hard drives.



c) The CipherDriveOne Dashboard will appear:



7. Configure the security settings for all users.

Many of these settings can match your internal security practices like password length, login attempts and password strength.

Steps:

- a) Click Settings, then Configuration
- b) Set your security settings for your environment



Note: The Dead Man's Switch is a 4-digit alpha-numeric code. Once enabled, you can trigger it by adding to the end any password. If your password is **Admin4567** and your Dead Man's Switch is **kl55**, you would type **Admin4567kl55**.



Warning! Once you trigger the Dead Man's Code, it permanently disables the pre-boot authentication. On the next boot, the login page will come up, but no account will be able to login. It gives the appearance that the pre-boot is still operational, but the keys are permanently deleted, and the hard drive is locked forever.

KLC GROUP Administrator Logout

Settings - Configuration

Failed Logins Before Lockout: (1-20)

Maximum Log File Size: kb

Maximum Log Retention Duration: Months

Password Complexity: 1+ Uppercase 1+ Numeric
 1+ Lowercase 1+ Sp. Character

Password History: (1-10)

Show Remember Me: Yes No

Show Legal Notice Before Login: Yes No

Enable 2-Factor Authentication: Yes No

Dead Man's Switch Code: Enable Show

Save

8. Adding users or importing a list of users that can administer or login to the computer system.



Please remember, these accounts are to authenticate to the pre-boot authentication software and not the operating system.

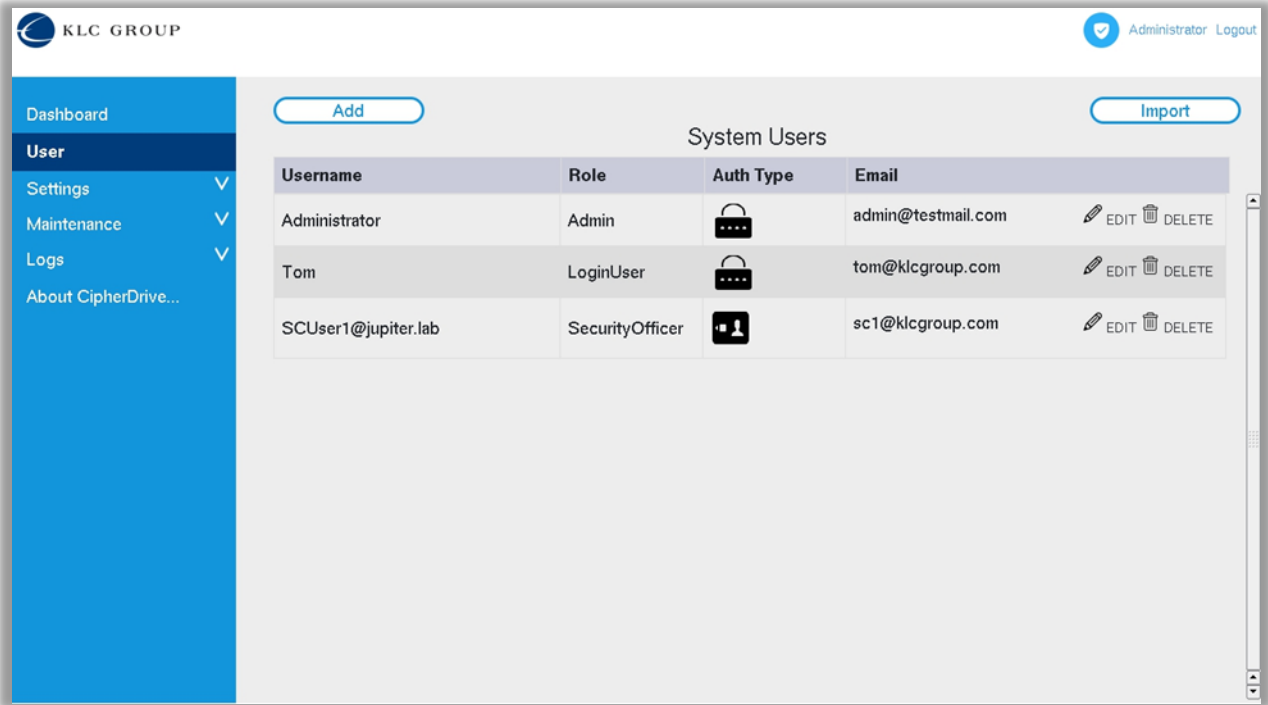


There are several user roles you may assign to a user. They are:

- **Admin:** Administration of users and features, Wipe disk and changing DEK. The Administrator cannot delete the logs.
- **Security Officer:** This role allows the user to Wipe disk (Cryptographic Erase), change DEK, and delete logs; and administration of users and features.
- **Login User:** This role allows login to the system and console access for the user.
- **Help Desk:** This role allows edit passwords for other Login and Helpdesk users only. Help Desk role can also view the logs of other users.

Steps: [Adding manually or importing a custom list.](#)

- a) **Adding users manually. Click “User” from the console and click “Add”**
 - i. **Fill out all the fields and click Save.**



b) Create a custom import user file.

i. The file must be saved as a .json file.

ii. 4 account “roles” are available, and their syntax are: a) Admin, b) SecurityOfficer, c) LoginUser, d) Helpdesk

SYNTAX

```
"{'Data':[{ 'UserName': 'realname', 'Role': 'roles', 'Email': 'abc@yourdomain.com' }, { 'UserName': 'realname', 'Role': 'roles', 'Email': 'abc@yourdomain.com' }, { 'UserName': 'realname', 'Role': 'roles', 'Email': 'abc@yourdomain.com' }, { 'UserName': 'realname', 'Role': 'roles', 'Email': 'abc@yourdomain.com' } ]}"
```

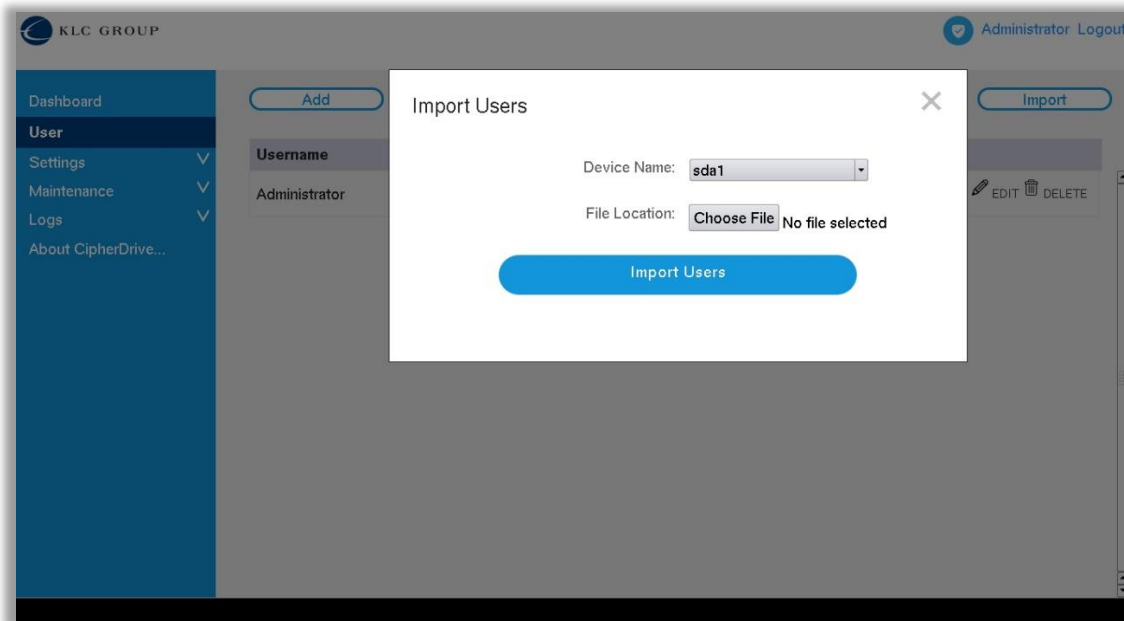
EXAMPLE

```
"{'Data':[{ 'UserName': 'Lucy', 'Role': 'Admin', 'Email': 'lucy@klc-group.com' }, { 'UserName': 'Adam', 'Role': 'LoginUser', 'Email': 'adam@ klc-group.com' }, { 'UserName': 'hobbs', 'Role': 'SecurityOfficer',
```

'Email': 'hobbs@ klc-group.com' ' } , { 'UserName': 'steve', 'Role': 'Helpdesk', 'Email': 'steve@ klc-group.com' } } }"

c) Importing from a JSON file.

- i. Click the "Import" button and search for the location of the correct JSON file.

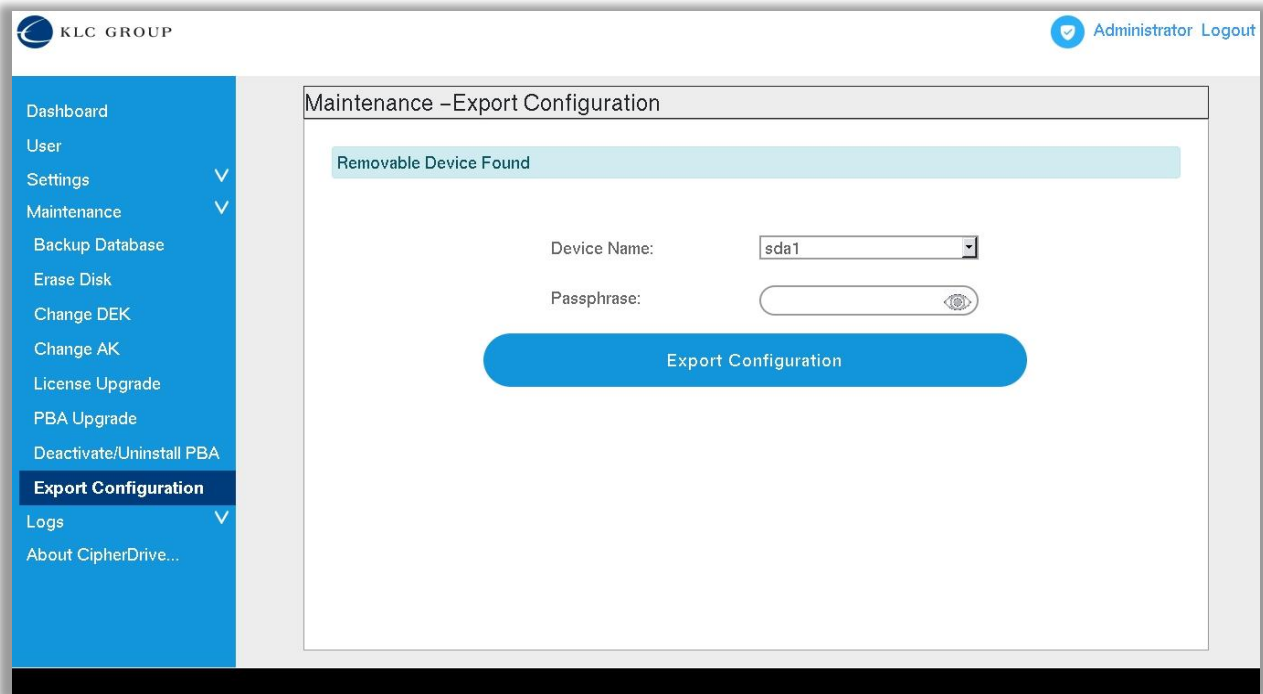


9. Exporting all the users and security configurations for other CipherDriveOne installations.

- a) Once you have the CipherDriveOne system just the way you want it, you can export the entire configuration for use in new installations of CipherDriveOne.
 - a. You can deploy other servers with the same security configurations and users.
- b) Make sure you have a USB drive inserted before you authenticate.
- c) Login to the administrative console and navigate to Maintenance > Export Configuration.
- d) Make sure the Device Name locates the USB drive, enter a 8 digit passphrase and click on the "Export Configuration" button.
- e) Remove the drive and look for CDExportDB file.



Write down the 8-digit passphrase somewhere safe. You will need it to import the configuration during the installation of new systems.



10. Installing new CipherDriveOne installations using an “Export Configuration” file.

- a) For every new installation, place the CDEExportDB file in the root directory of the USB boot drive with the CipherDriveOne software. You cannot change the name of the CDEExportDB file. It should look like this:

Name	Date modified	Type	Size
EFI	9/8/2020 5:47 PM	File folder	
CDEExportDB	9/10/2020 9:21 AM	File	45 KB
EvaluationLicense	9/8/2020 5:46 PM	File	1 KB
Hash	9/8/2020 5:46 PM	Text Document	1 KB
ReadMe - CipherDrive Beta Release_1.1.1...	9/8/2020 5:46 PM	Text Document	3 KB

- b) Use the following commands to install CipherDriveOne and import an “Exported Configuration” from the “gold master” system.

SYNTAX

```
CipherDriveInstaller -d <drive location>,<drive location a1>,<drive locationa2> -p <password> -dbp CExportDB -ps <Passphrase>
```

EXAMPLE

```
CipherDriveInstaller -d /dev/nvme0,/dev/nvme1,/dev/nvme2 -p Admin456 -dbp CExportDB -ps safe1234
```

11. Installing an Operating System (OS) or Virtual Machine (VM)

1. Installing an OS or VM prior to the installation of CipherDriveOne.

Steps:

- a) Use the standard boot or .ISO media to install on the hard drive's main writable partition.



If you are installing Windows 10 PRO, you must disable the BitLocker encryption software.

- b) Install CipherDriveOne as prescribed in this document or the CipherDriveOne User's Guide after you have installed your OS/Virtual Machine.

2. You have a version of CipherDriveOne that is pre-installed on the hard drive.

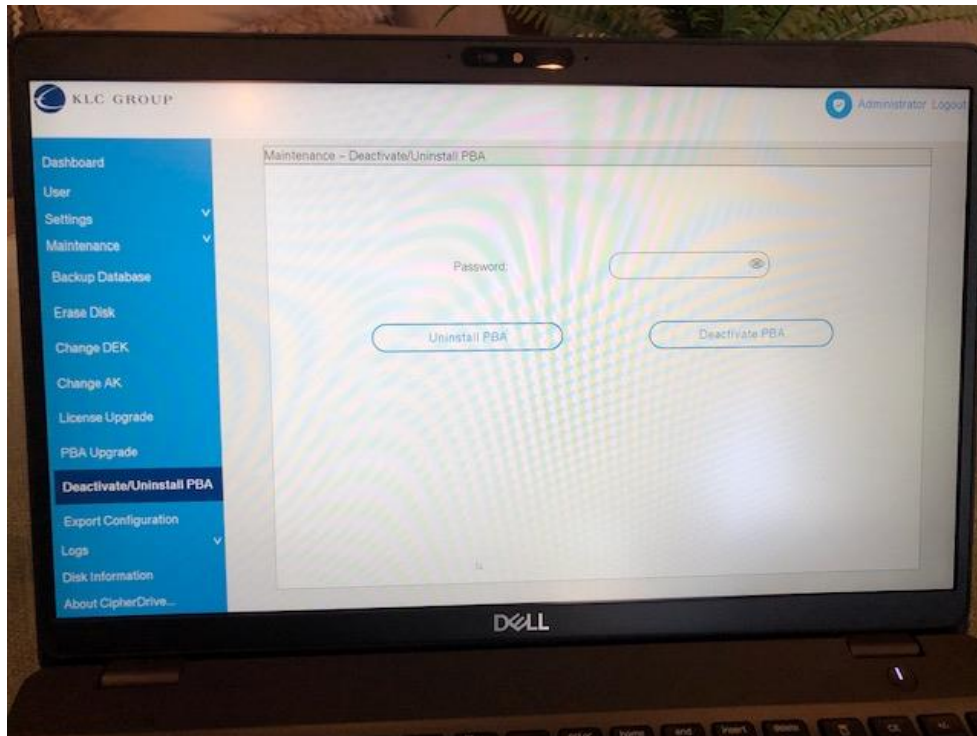


Until the hard drive is unlocked by CipherDriveOne, the writeable sector of the drives will be invisible to the computer. Do not insert OS/VM boot media until you have authenticated to CipherDriveOne.

Options 2: Deactivate and Activate

Steps:

a) Enter the Settings Console and navigate down to “Deactivate / Uninstall PBA”



b) Enter your administrative password and check the “Deactivate PBA” button. This will temporarily deactivate CipherDriveOne but all your settings and users will be kept in the secure database.

c) The system will shut down. You can now reboot.

d) Enter the Bios to make sure your boot media will launch first and exit. Your boot media should launch and installation to the writeable hard drive sectors now available.

e) Once the OS/VM or other data is loaded on the primary and secondary hard drives, you can reactivate CipherDriveOne with the following command only:

SYNTAX **CipherDriveInstaller -d <drive location>,<drive location a1>,<drive location a2> -p <password>**

EXAMPLE

**CipherDriveInstaller -d /dev/sda,/dev/sda1,/dev/sda2 -p
Admin456**

Note: there is no space after the comma separating drive locations.

Options 2: Authenticate and Reboot

Steps:

a) After installation of the hard drive into the computer with CipherDriveOne pre-installed, turn on your computer and let CipherDriveOne boot up.

b) Only after the CipherDriveOne software is loaded and the legal disclaimer is visible, insert your USB or boot media into the computer. NOTE: Legacy BIOS will not be available.

c) Login to the CipherDriveOne with your username and password.

d) The computer will restart the computer without powering off. Enter the Bios to make sure your boot media will launch first and exit. Your boot media should launch and installation to the writeable hard drive sectors now available.

NOTE: For older software that requires multiple power-off reboots, use the Deactivate / Activate method of installing software.

Last Updated: February 2021