KLC GROUP

KLC Group LLC

CipherDrive v1.2

KLC PBA

This manual covers version 1.2.2 (and later)

KLC
1-31-2021

Contents

CipherDriveOne Installation and configuration guide 2
Preparation 2
Installation 3
Configuration 9
Dashboard 13
User roles 16
Edit User with Password 17
Edit user with Smart card 18
Delete user 19
Importing (common group of) Users 20
Entering a License Key 21
Generate License Request and Import/Upgrade License 21
Erase Disk – Wipe Disk 25
Upgrade - (product upgrade) to a new version 26
Settings - Configuration 28
Dead Man's Switch Code Operation 29
Change Authentication Key 30
Change DEK 31
Export Configuration 32
Disk Information 32
Logs 33
(Temporary) Deactivation and Uninstall 35
Reactivation 37
About CipherDrive 37
Annexure 1 – Replacing a bad disk with a new disk 38
Annexure 2 – CDOkey disk information collection tool 38

CipherDriveOne Installation and configuration guide

CipherDrive is a Pre-Boot Authentication (PBA) software, which paired with a Self-Encrypting Drive (SED) forms a complete Full Disk Encryption (FDE) system.

This manual covers CipherDrive standalone installation on PC systems with Opal2 compatible SED drives. The name CipherDrive or PBA will be used interchangeably when we discuss the CipherDrive product.

The CipherDrive PBA software will be installed on the 128MB read-only "ShadowMBR" partition on the SED drive.

After completed install the system will boot to the PBA logon screen and the user will enter the user's credentials and log into the PBA which after successful authentication will unlock the SED drive and initiate boot to the HOST OS or Hypervisor environment.

Preparation

To prepare for the installation you will need a small (min 4 GB) USB connected thumb drive FAT 32bit formatted (mostly factory default). Copy the self-contained CipherDrive installer package onto the USB thumb drive and then boot from the USB drive. You will be prompted for any required input during the install. After installation the system is ready to receive the first user logon (which will be described in more detail after the step by step install description below). (Alternatively the installation software can use a CD instead of the USB drive.).

Prepare separate USB thumb drive (for installation of PBA):

- Format a USB thumb drive (1GB or larger) in 'FAT32' format.
- Download CipherDrive_1-2-x.zip and a License file (EvaluationLicense) from Web/FTP through the link provided by email or as otherwise instructed
- Extract the zip file in the root folder of the USB drive.
- Make sure you have also have extracted the /EFI folder to be off of the root folder.
- Download and Copy the Evaluation License file to the root folder

Prepare the SED Disk:
Note: Using PSID as described below is not required if the disk is used for the first time. Instead just jump to the bullet point for installing OS or Hypervisor.

- Disk type supported: SATA/NVMe Opal-2 compliant SED drives
- Make a note of the PSID code of the disk (usually written on the disk label).

- BIOS setting: SATA operation should be set to ‘AHCI’.
- BIOS setting: Secure Boot should be disabled (at this time)
  Boot the system with the above USB drive and revert (PSID) the disk by executing the command:
  CipherDriveInstaller -d /dev/nvme0 -r <PSID>or sedutil-cli –PSIDrevert <PSID> /dev/nvme0

- **Install OpenXT or Linux or Flash an 'ADI'/OSimage on the system.**

Prepare the Customization File:

If you want to customize the legal notice/disclaimer message shown to the users at logon, displaying your organization’s name at the top of the login screen and/or display a phone numbers for users to call to your organizations IT Support in case they need help, all can be customized in a custom file in below (json) format. This file can be used as parameter to the installer. Below is a sample format of the customization file:

{"Disclaimer Data":"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:\n\n……Such communications and work product are private and confidential. See the user hand bock for details.", "Organization Name":"KLC Group LLC", "Support Number":"+1-555-123-4567"};

Installation

The following section covers the actual installation steps.

Note: The example below is based on installing on a system with NVMe drive. If your drive is a SATA drive and not an NVMe drive. Please replace the “nvme0” parameter with “sda1” (or the drive letter corresponding to the SATA drive you want to install on) for the command line in the example below.

Installation of the PBA:

- Boot the system with a prepared USB drive.
- To get a list of all supported install options, you can get help by running the following command:
  CipherDriveInstaller -h

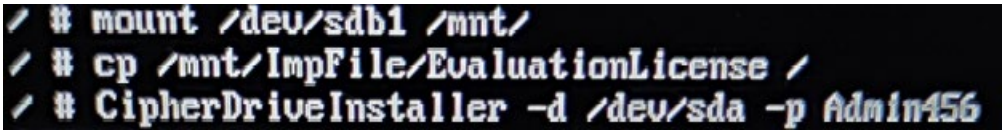
- Install the PBA by executing command with following syntax:

  For licenses with single disk drive support (standard license) use the following command:
  CipherDriveInstaller -d /dev/<disk> -p <password>

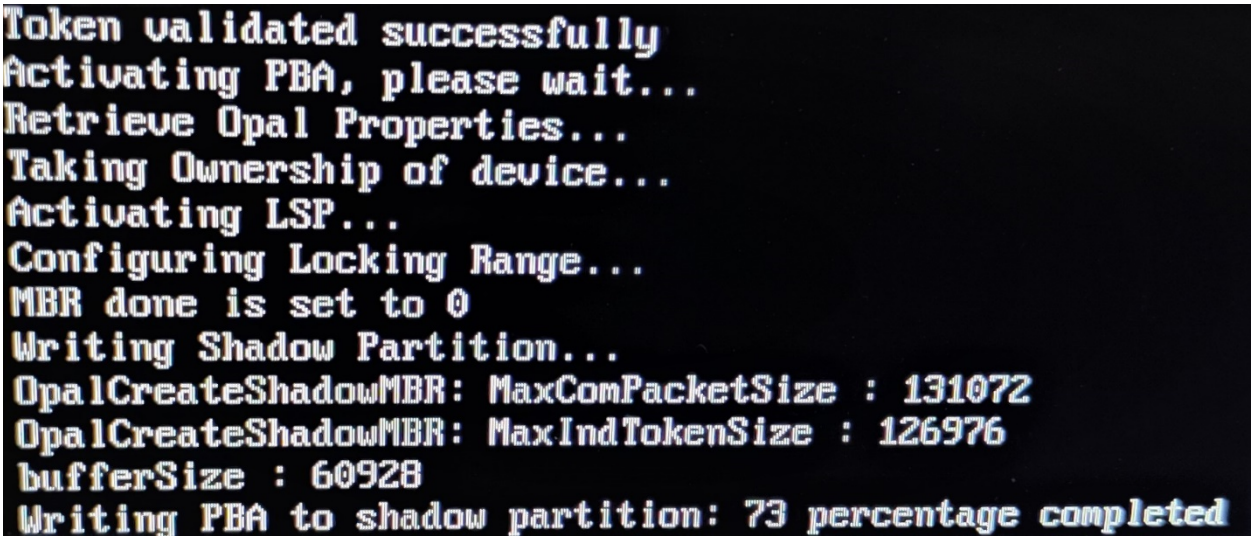
If your system has multiple disks you need multi-disk (auto SED sync) license.
Install MultiDisk license using the following command, comma separated between disks:
CipherDriveInstaller -d /dev/<disk1>,/dev/<disk2>,/dev/<disk3> -p <password>

Examples of install commands:

- **CipherDriveInstaller -d /dev/nvme0 -p Admin456**
  - Installing on single internal NVMe disk
- **CipherDriveInstaller -d /dev/nvme0,/dev/sda -p Admin456**
  - Installing two internal disks, first NVMe drive and first SATA drive
- **CipherDriveInstaller -d /dev/sda,/dev/sdb -p Admin456**
  - Install two internal SATA disks, SATA-A and SATA-B
- **CipherDriveInstaller -d /dev/nvme0,/dev/nvme1,/dev/nvme2,/dev/nvme3 -p Admin456**
  - Install on four internal NVMe disks, NVMe0-3



- This is the example of what the screen looks like during the installation



Install PBA with a given license file:

If you have been provided a specific license file either on account of purchase or custom duration, please install the PBA by executing the following command:

CipherDriveInstaller -d /dev/nvme0 -p <password> -lic <License File name>
(With extension if applicable)

Install PBA with Custom (Legal Notice) File:

If you have prepared the optional custom legal notice file (e.g. customFile on the USB root). (Make sure to enter both filename and any extension, if extension is used, e.g. .json). Then instead of issuing the above regular install command, please install the PBA by executing the following command

CipherDriveInstaller -d /dev/nvme0 -p <password> -l customFile

Install PBA with BIOS boot entry:

On some systems, BIOS needs an explicit boot entry to invoke the PBA from the MBR shadow. On such systems, please install the PBA by executing the following command **CipherDriveInstaller -d /dev/nvme0 -p <password> -b bootentry**

Install PBA with exported configuration file (CDO 1.1.16 and later):

In some cases you may want to duplicate the whole setup from one system to one or more additional systems. In such case, once you have an exported configuration file (e.g. CDExportDB file on the USB root) from Settings Console of another PBA installation, then import that configuration by executing the following command:
CipherDriveInstaller -d /dev/nvme0 -p <password> -db CDExportDB -ps <Passphrase>

If you want to replace a secondary disk that has gone bad with a new disk, you can use the following command to install the PBA to secure the new disk in-place and then bring it up seamlessly, use the following command.
CipherDriveInstaller -d /dev/nvme0 -p <password> -dbp CDExportDB -ps <Passphrase>

This command is also useful if you need to install on a server with many disks and would like to make sure the disks are swappable.

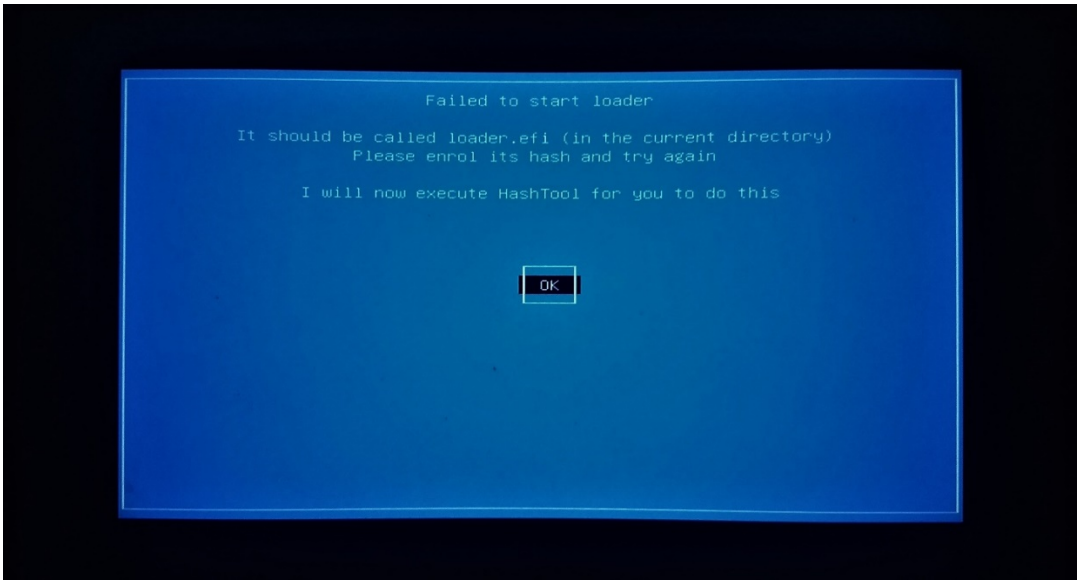
In case recovery is to be disabled, you can use the “noexport” parameter to disable the options to export configuration or backup database. This field maps to Recovery field (available to Security Officer role only) in the Settings Configuration page.
CipherDriveInstaller -d /dev/nvme0 -p <password> -n noexport

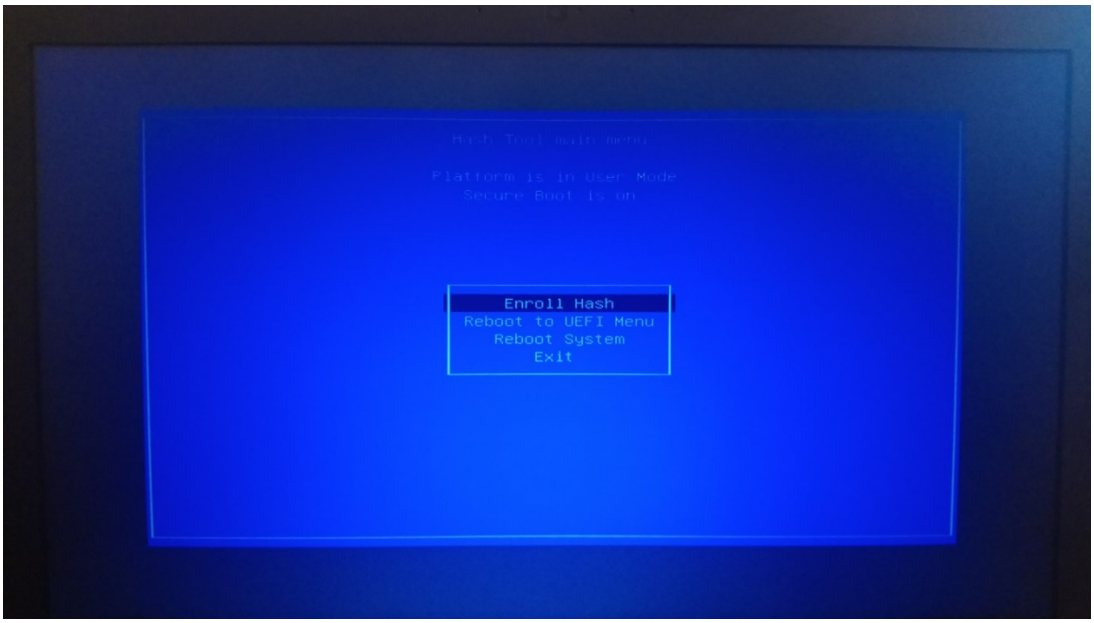
Please note that the commands above for custom file for legal notice, adding a boot option, installing on multiple drives (if your license permits multi-disk), and importing from exported database can all be combined in one install command. Use space in-between each option you want to include.
Example:
CipherDriveInstaller -d /dev/nvme0,/dev/nvme1 -p <password> -l customFile -b bootentry -db CDExportDB -ps <Passphrase>

Installation with Secure Boot on

If Secure Boot is on and on booting with CipherDrive from USB for the first time, the system will enroll the boot loader before it can boot to install PBA. Below images describe the steps:

When booting the system from the USB thumb drive, the firmware will display the screen and message below.





Enroll the loader by following the step in the picture below (select Yes).

On successful enrollment, the screen below will be displayed. Exit and proceed further:

After successful installation of CipherDrive, when booting from the hard-drive of the system, a similar procedure should be carried out one more time. Subsequent to this, CipherDrive is setup to boot using Secure Boot and perform its operations securely (the setup screens will not be seen again).

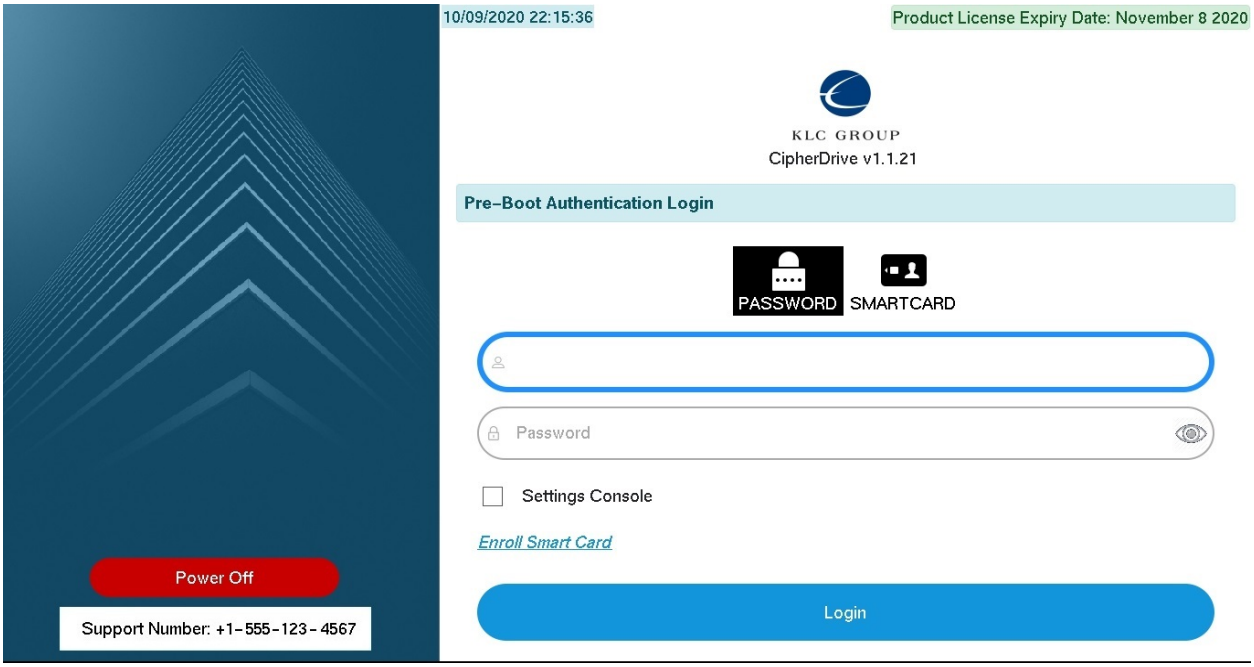
Configuration

After successfully installing and activating the PBA, the installer will power off the system.

Manually power on the system and the system will boot into the PBA, first displaying a splash-screen (see below) then followed by displaying the PBA logon screen. You are now ready for configuring the system.

The only active account directly after install is the default Administrator account, with the password that was setup at activation (if you check the activation parameters in the screenshot above, you will see the default Admin456 was used)

Logon Screen (Password)



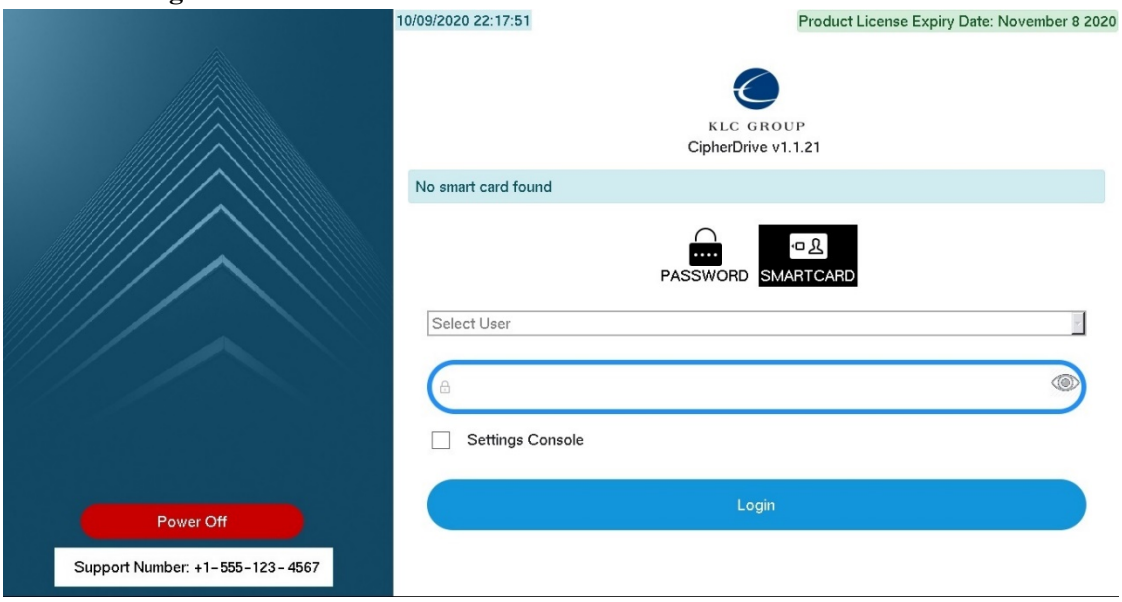
Enter the username and password and press enter or “Login” button to logon (boot) to the host OS. If allowed (policy), users can select to check-mark “Remember me” which will remember the latest used username between logons.

In case we want to logon as user Administrator (for the default administrator) in order to enter the settings pages. Enter username “Administrator” and the admin password (as set during installation), checkmark the “Settings Console” option to get to the settings pages and press “Login” or just press enter.

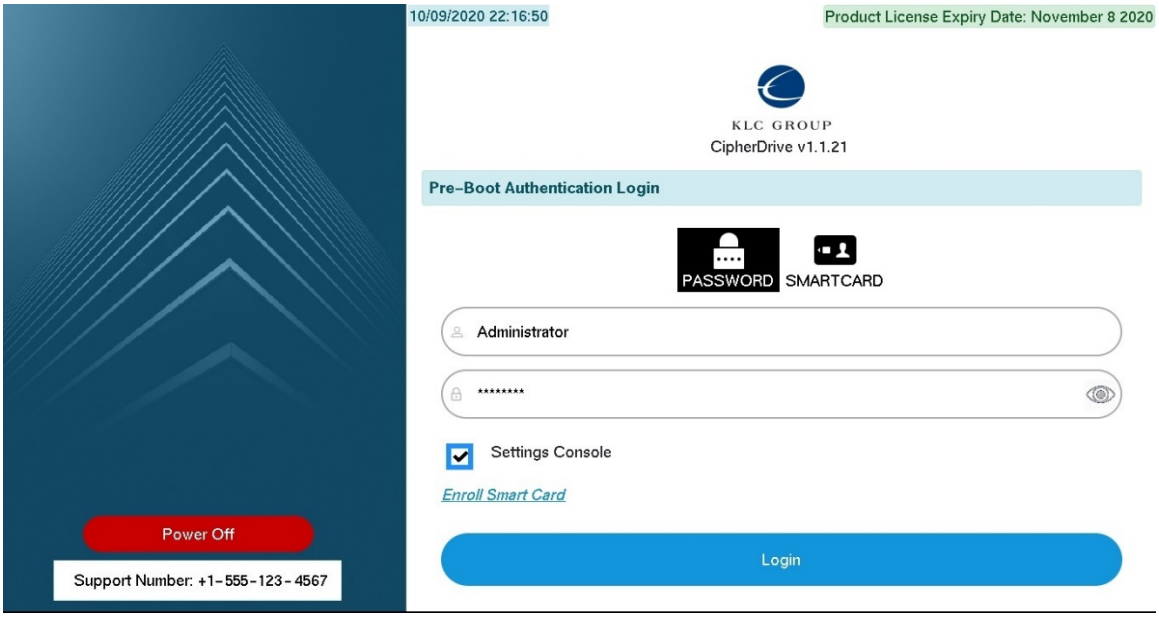
In the case of Single factor authentication, if the user wants to enroll Smartcard for the first time, enter the username / password credentials and click on the Enroll Smart Card link. Enter the

smart card credentials and click Login. The system will authenticate the username/password and save the Smart Card credentials for authentication from next Login.

Smartcard logon screen

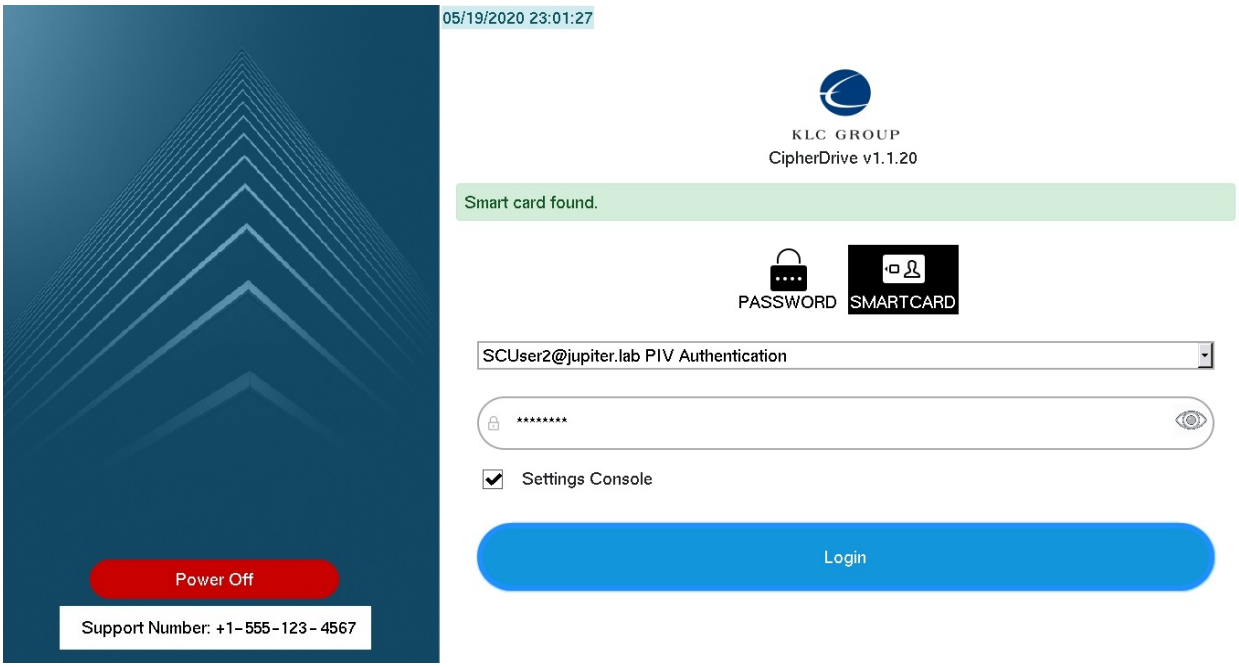


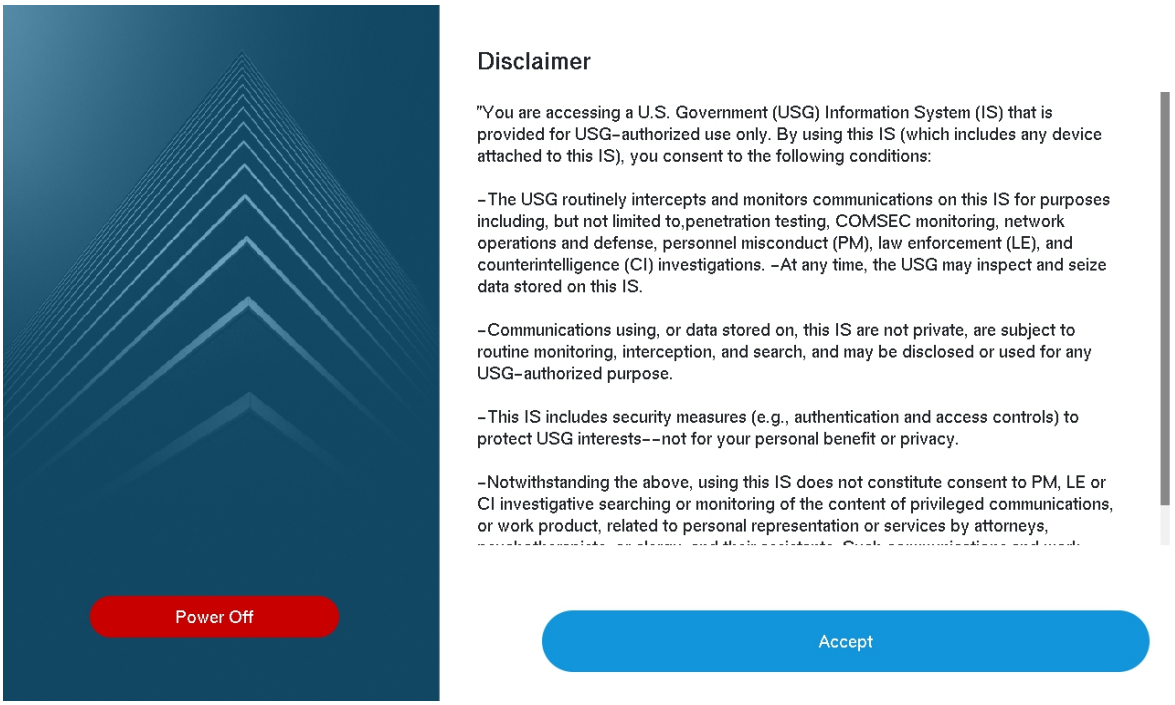
When logging in with Smart card, select the user name from dropdown (showing names from the installed certificates on the smartcard), enter the PIN for the card and press “Login” button (or just press the “Enter” key).
For settings pages, checkmark the “Settings Console” option before pressing “Login”.



When Multi-Factor Authentication is enabled, the user has to use both Password and Smart Card methods. In this case, the logon Password screen automatically shows “Next” button. After entering the username and password, when user clicks on this button, screen will automatically switch to Smart Card and the button switches to “Login”. The user can select the Smart Card user and enter the pin and click “Login” button to logon using both the factors. In case the Smart Card is used for the first time, it will be auto-enrolled after validating the password. From next login onwards, that user will be mandatorily validated for both Password and Smart Card (with credentials used during auto-enrolment).

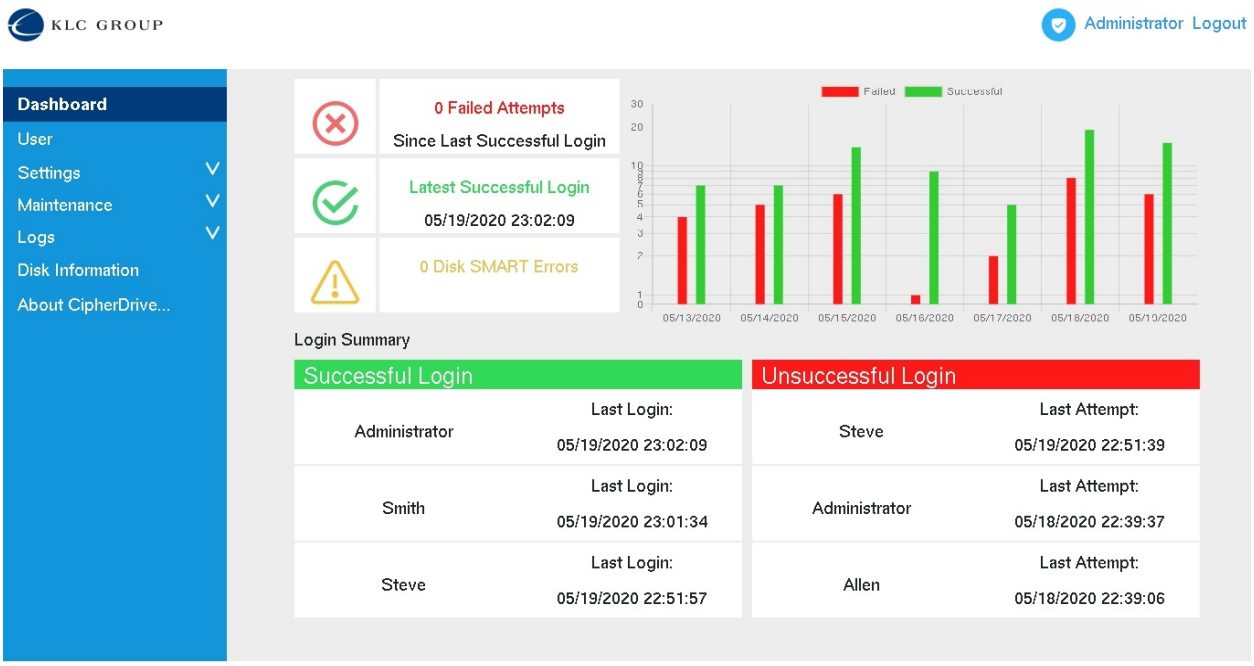
“Administrator” is a special user and will be allowed to logon with a single factor (Password) by simply clicking the “Logon” button even if Multi Factor Authentication is enabled.





If “Settings Console” was selected at the logon screen, then after Sign-In (and showing Disclaimer/Legal notice), the PBA will show the settings pages Dashboard screen by default.

Dashboard



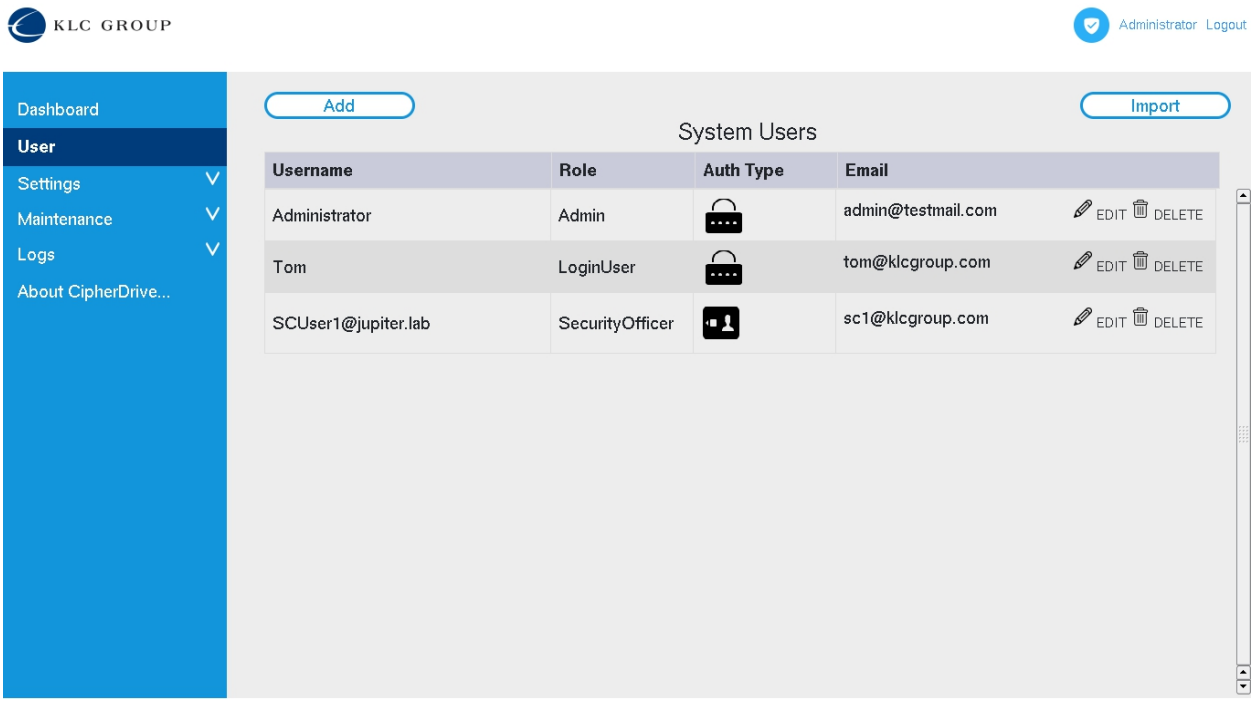
The Dashboard gives the Administrator/User a quick overview of the system's security posture.

The dashboard screen shows the following events summary:

- Number of Failed (logon) Attempts since last Successful login
- Latest (previously) Successful Login time and date (i.e. the logon before current logon)
- Smart Error count (disk errors reported by the SED disk - if any)
- Graph displays the last 7 days of records of failed, successful, and total login attempts
- Login Summary consist of latest successful and unsuccessful login attempts of distinct users.
- Admin and Security officer can view the successful and failed attempts of all Users

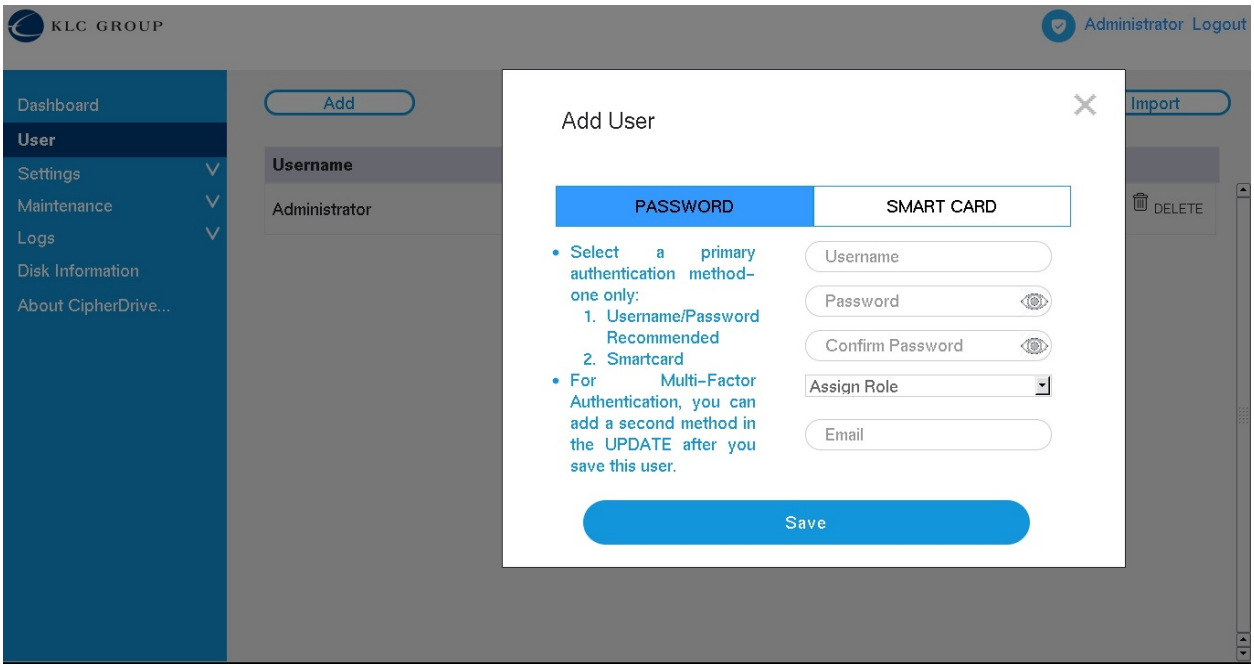
Add User with Password:

To add a user with password credential. Select “User” on the left navigation bar and then press “Add”.



A popup windows will be shown. Make sure the tab “PASSWORD” is highlighted.

1. Enter a unique Username of the user to be added
   Max 40 char, Upper, Lowercase, Numbers and Special characters allowed)
2. Enter the initial password for the user
   Max 128 characters Upper, Lowercase, Numbers and Special characters allowed)
3. Re-enter the password to confirm.
   (The user will need to change the password at the user’s first logon)
4. Enter the user role
   See “Roles” section below
5. Enter email address.
   Currently used as user identifier
6. Press “Save”
7. This will popup a dialog to enter Logged in User Password.
   The logged in user password for reauthentication (verifying action) purpose
8. The user account is now ready for logon



Add user with Smart card:

Please note that users can be given the rights to register their smart card on first use (register SC at first logon with password for Multi Factor Authentication). However, system administrators can also register the SC in case the administrator has access to the card at the time of registration.

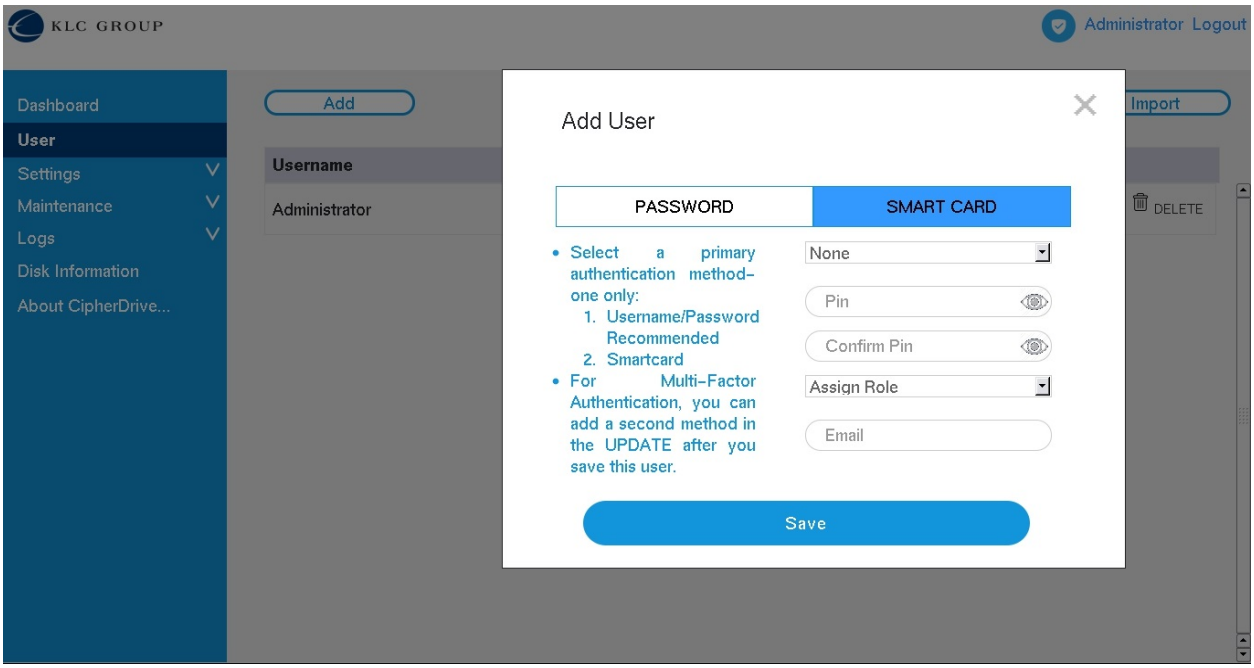
Please also note that SmartCard only Administrators will have limited administration functionality as CipherDrive currently treats Password as primary mechanism for configuration and administration tasks. A single factor SmartCard user is configurable only for Logon and viewing options such as Logs. In addition, it should also be noted that the proposed combinations for Common Criteria certification are 1) Password only and 2) Dual factor (Password and SmartCard).

To configure SC for user resgistration, set “Enable Multi-Factor Authentication” on the Configuration page.

To enter the SC either as a user or admin, make sure you have access to the card and the PIN for the card. Then select “User” on the left navigation bar and then press “Add”. A popup windows will be shown. Make sure the tab “SMARTCARD” is highlighted. Insert the Smart Card to be added into the reader.

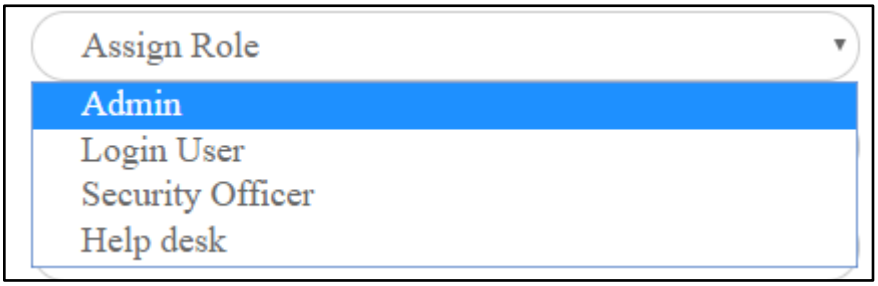
1. Select Username the user to be added from the username in SC certs from the drop down menu.
   Must select from available usernames on SC.
2. Enter the PIN
   Max 20 char
3. Re-enter the PIN.
   Max 20 char

4. Enter the user role
   See “Roles” section below (must be same role as for password setting)
5. Enter email address.
   Currently used as user identifier
6. Press “Save”
7. This will popup a dialog for entering Current User Password.
   The logged in user password for reauthentication (verifying action) purpose
8. The user account is now ready for first logon



User roles

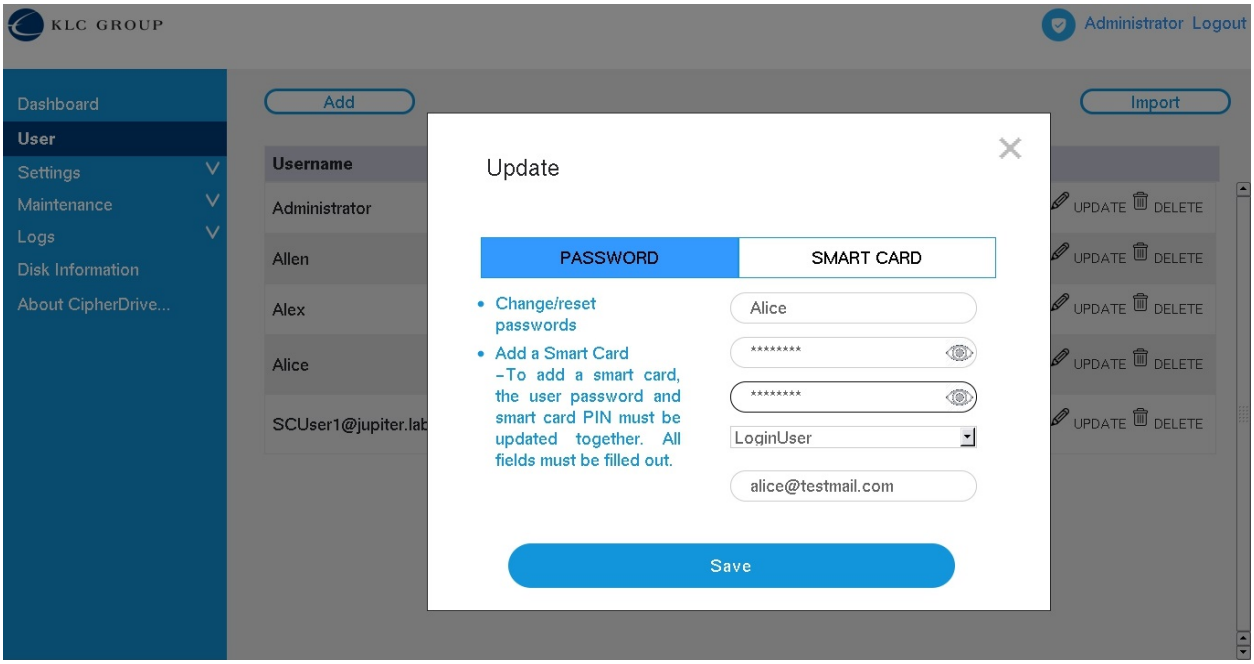
Following roles are supported:



Admin: Administration of users and features, except for deleting logs, Wipe disk and changing DEK.
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.

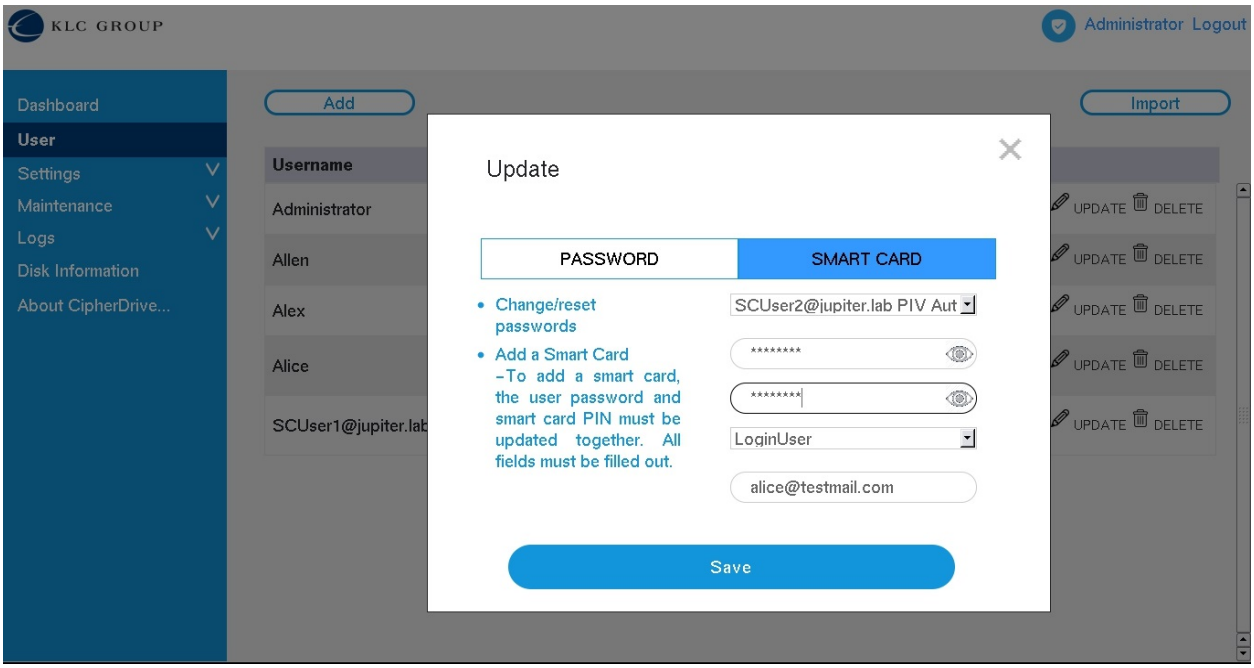
Edit User with Password



On the dashboard panel under the User tab click Users this will then bring up the current list of users. To edit a user the administrator goes into the Settings Console selects the user they want to edit. You will see an edit icon to the right side of the screen. Click on the Edit icon for the User you want to Edit and it will bring up Edit User screen. For a Password user type, you can change all the fields except the Username. Only, Admin and Security Officer role users can change the user role in the Edit User screen. After updating the fields, click on the Save button.

1. Enter the password for the user
   Max 128 characters Upper, Lowercase, Numbers and Special characters allowed)
2. Re-enter the password to confirm.
   Reenter the same password
3. Enter the user role
   a. See “Roles” section above. Only Admin and Secutity Officer roles can modify this field
4. Enter email address.
   a. Currently used as user identifier
5. Press “Save”
6. This will popup a dialog for entering Current User Password.
   a. The logged in user password for reauthentication (verifying action) purpose
7. Now changes are commited to the database

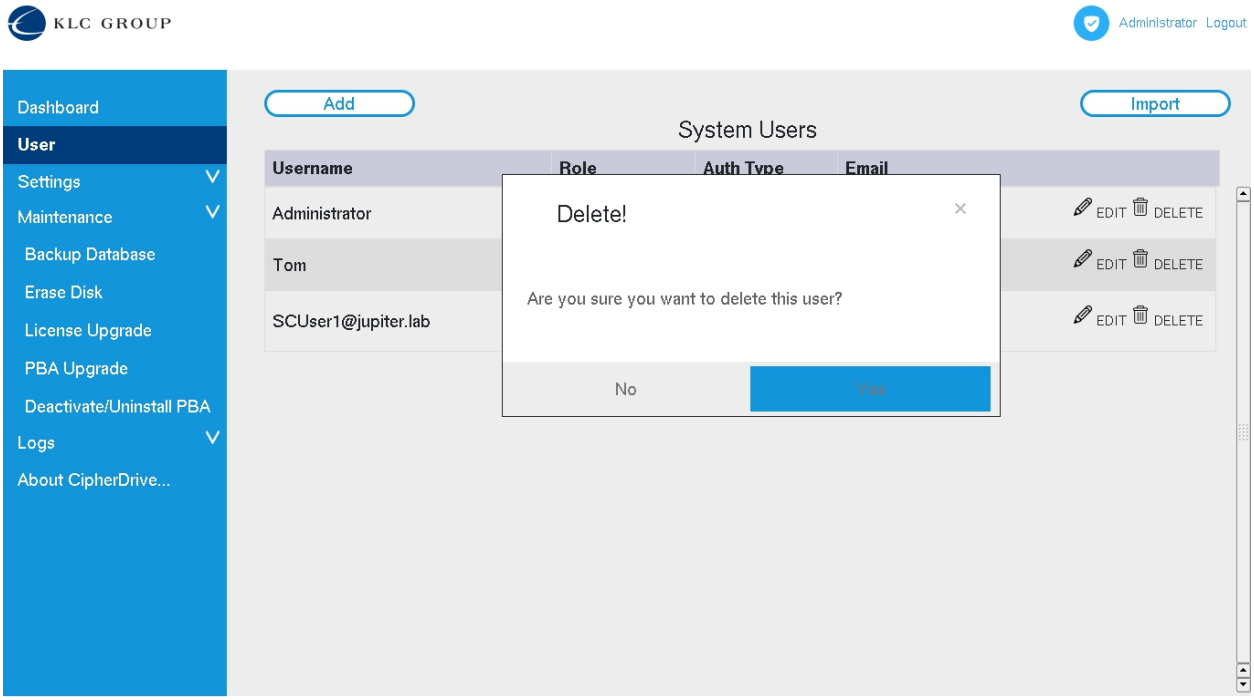
Edit user with Smart card



Click on the Smart card tab on the Edit user screen to edit the Smart card related fields. Only Password users can edit Smart card users. All the fields including Smartcard username are modifiable. After updating the fields, click on the Save button to commit the changes.

1. Select Username the user to be added from the username in SC certs from the drop down menu.
   Must select from available usernames on SC.
2. Enter the PIN
   Max 20 char
3. Re-enter the PIN.
   Max 20 char
4. Enter the user role
   See “Roles” section below (must be same role as for password setting). Administrator and Security Officers only can modify this field.
5. Enter email address.
   Currently used as user identifier
6. Press “Save”
7. This will popup a dialog for entering Current User Password.Type in the logged in user password for reauthentication (verifying action) purpose
8. The changes are now committed.

Delete user



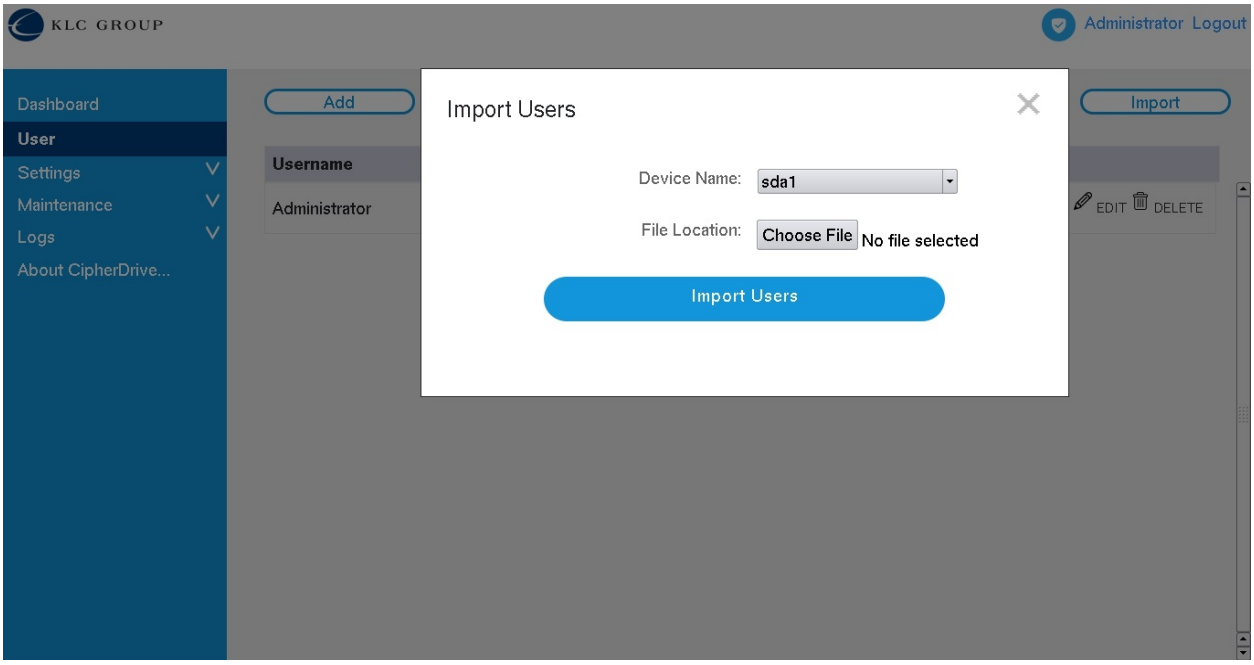
On the dashboard panel under the User tab click Users this will then bring up the current list of users. To delete a user the administrator goes into the Settings Console selects the user they want to delete. You will see a delete icon to the right side of the screen. Then click on the icon and it will bring up a panel asking you if you want to delete the user. Chose the answer.

Importing (common group of) Users

"Import users" is a rapid way of adding a set of (same) users to a number of not network connected (air-gapped) systems without having to manually add them one by one on each system.

To import users, see example below:
Under the dashboard panel in the Settings console, click Import Users button to add a list of users to PBA all at once.

1. In the import user screen, In the device name field select Device Name (from the dropdown) to find the USB thumb drive or external hard drive containing the file.
2. Select the users list/database file name from "File Location"
3. Click on the "Import Users" button.



The file format for import is a JSON formatted text file. A sample import file content is as shown below. Please create a file with the edited json content and copy it to the USB for selecting the file and thus importing the users.

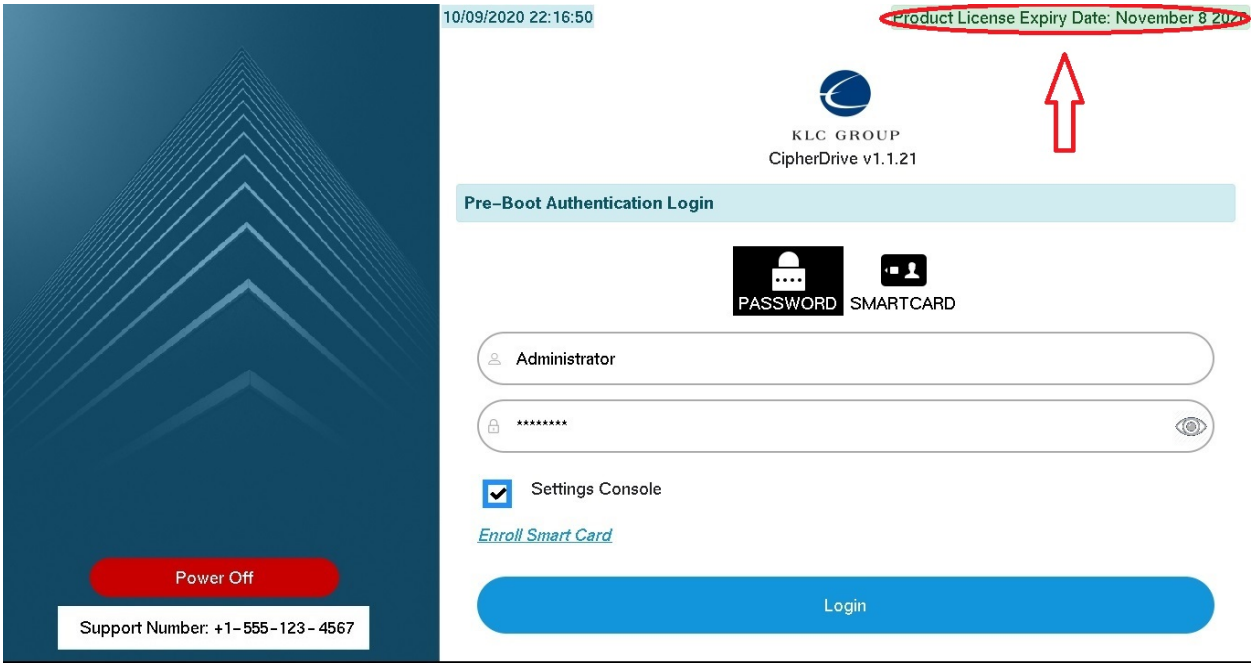
"{'Data':[{ 'UserName': 'Bob', 'Role': 'Admin', 'Email': 'bob@test.com' }, { 'UserName': 'Alice', 'Role': 'LoginUser', 'Email': 'alice@test.com' }, { 'UserName': 'Hobbs', 'Role': 'SecurityOfficer', 'Email': 'hobbs@test.com' }, { 'UserName': 'Steve', 'Role': 'Helpdesk', 'Email': 'steve@test.com' }]}"

Another way of adding users is to fully configure a system with a set of users with their valid credentials and then export an encrypted copy that can be imported in another computer. See Export Configuration section.

Entering a License Key

CipherDrive comes with a 45 days trial license without entering any license key. During this time the product is fully featured in order to allow customers to “try-before-buy”.

After the trial period a license key needs to be entered in order to continue using the product. The procedure for licensing is described below. **Product license:**



On the Login screen, Product license information is displayed. On license expiry, it will show the Product license expired and on logon, the system will continue to protect the data but all admin functions including changing of passwords will be disabled until a valid license key is entered. When a license is expired logon is delayed with 2 minutes at each logon (displaying information regarding the expired license) to make the user aware of the expired license and the need to update.

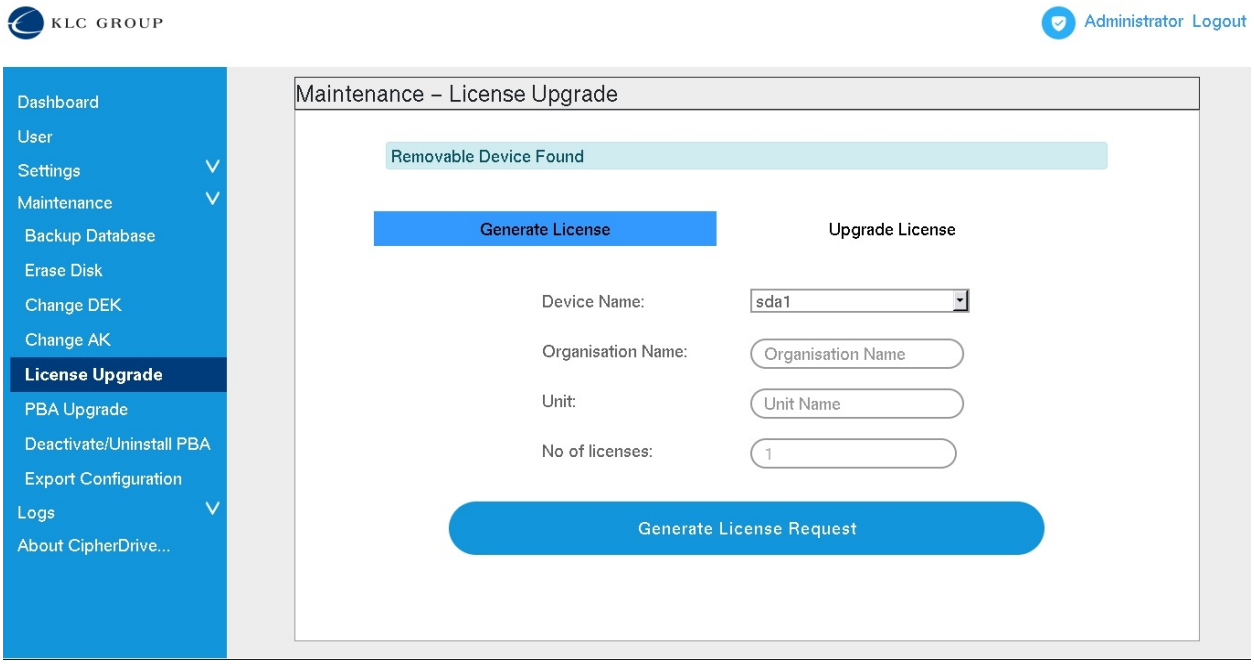
Generate License Request and Import/Upgrade License

Licensing consist of two operations. First the user will “generate a license request” that is unique to the computer where CipherDrive will be used. This license string can be exported to a network folder for automatic processing (by a licensing agent on the network) or manually giving the file to an administrator who will process the file and send back a file with an “activation key”.

The user will import the key under “Import/Upgrade license” to CipherDrive in order to remove the 45 days trial period and make the product fully featured.

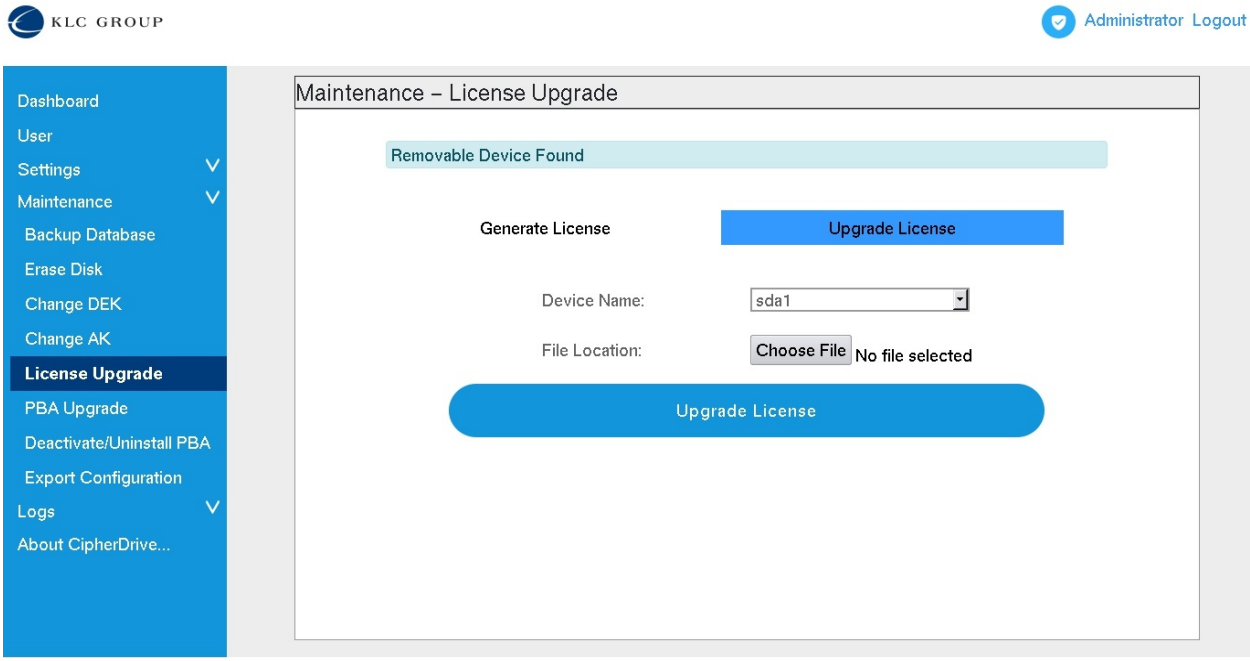
On the PBA License Upgrade panel, you will be given a choice to either Generate the License (request) String in a file or Upgrade the (import new) License.

Generating the License (request) String/File.



* For device name field - Choose what device/drive where you will store files for now
* Organization name field – Enter your Organization's name
* Unit field - Enter Organizational Unit or Department (if applicable)
* No of licenses field - Enter the number of licenses (Currently, defaulted to 1 only)
* Click on Generate License Request button to generate a License String file on the USB drive to send to support.

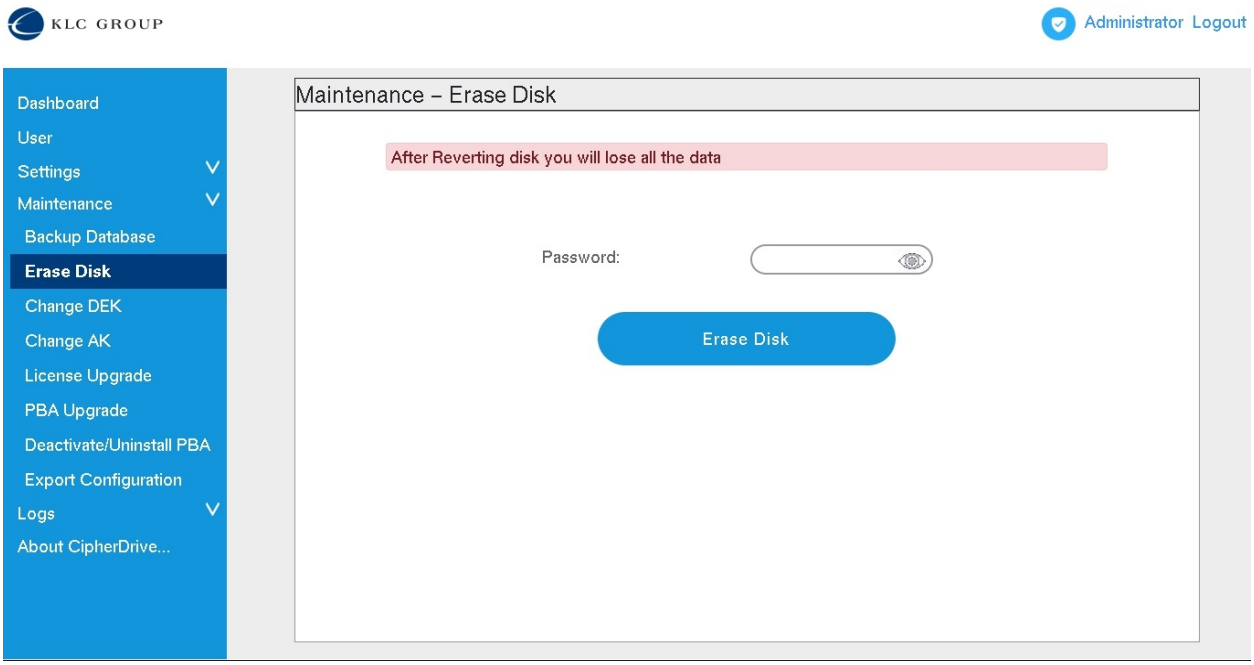
Upgrade or Importing a License file



* For device name field, choose what device the files can be found.
* Select the license file received from the Administrator
* Click on Upgrade License button,
* This will pop up a dialog to enter the logged in user password for reauthentication (verifying action) purpose
* License will now be updated but for the changes to take effect, please logout and then log back in again.

Please note that a license file field also determines the key size used for encryption/decryption of data. (Default is 256bit key size if no special request is made)

Erase Disk – Wipe Disk



In this section the Erase Disk/Wipe Disk or PBA revert erases everything on the disk and resets it to the manufactured state. In order to erase the disk you will need to enter the password (of the currently logged in Security Officer) into the Password field. Then click on the “Erase Disk” button. Note that this is an irreversible operation. The disk will have to be set up again after it is erased.

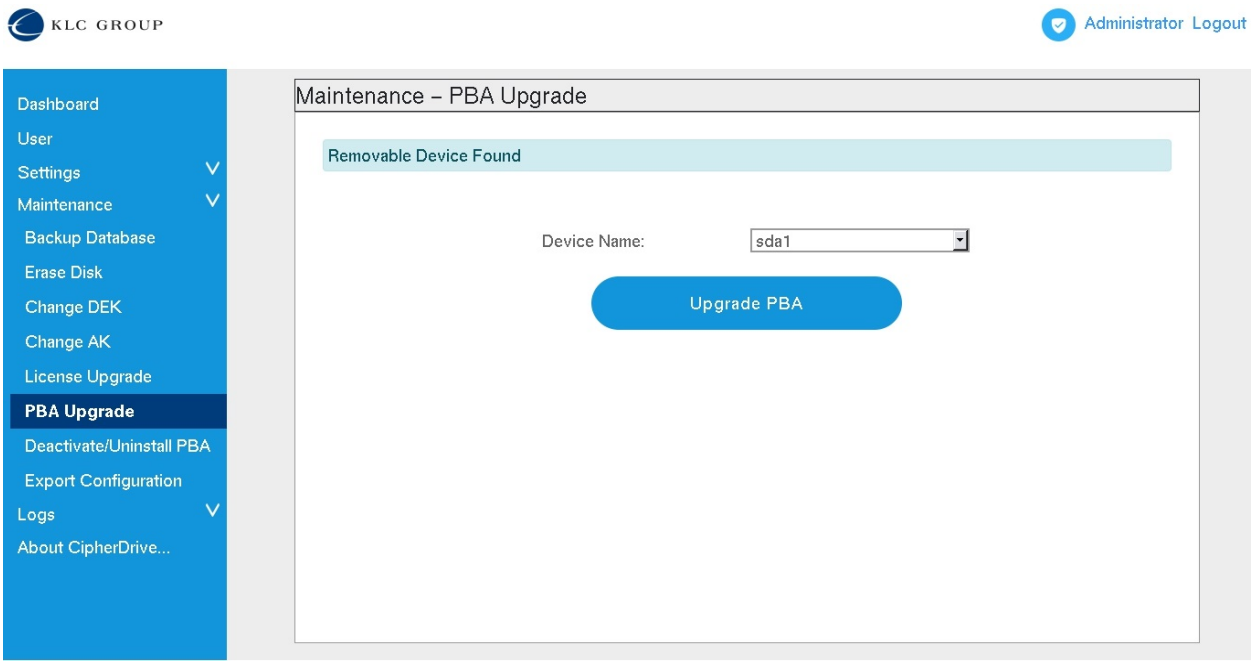
Upgrade - (product upgrade) to a new version

There are two methods to upgrade CipherDrive:

1. Settings Console UI - select the upgrade option
2. CipherDriveUpgrade command line utility

In short, for both methods (each described in detail below), copy PBA.img and SecurityToken (and if applicable customFile) to USB root and use one of the two methods to upgrade PBA. To update the disclaimer, CipherDrive will pick up the customFile automatically from the USB during the product upgrade process and modify the disclaimer contents in the database.

PBA Upgrade:



To Upgrade the PBA (product upgrade):

* Copy the PBA image file and Security Token file to the root location of the Removable USB drive.
* Device name field is where the device/drive is selected containing the PBA image.
* Upgrade PBA button - Click to upgrade the PBA.
* This will pop up a dialog to enter the administrator's password (needed to approve the upgrade).
* After a successful upgrade the system will power- off.

Short step-by-step instructions for product upgrade from UI - -> PBA Upgrade menu selection

- PBA image file and Security Token file should be copied to the root location of Removable USB drive

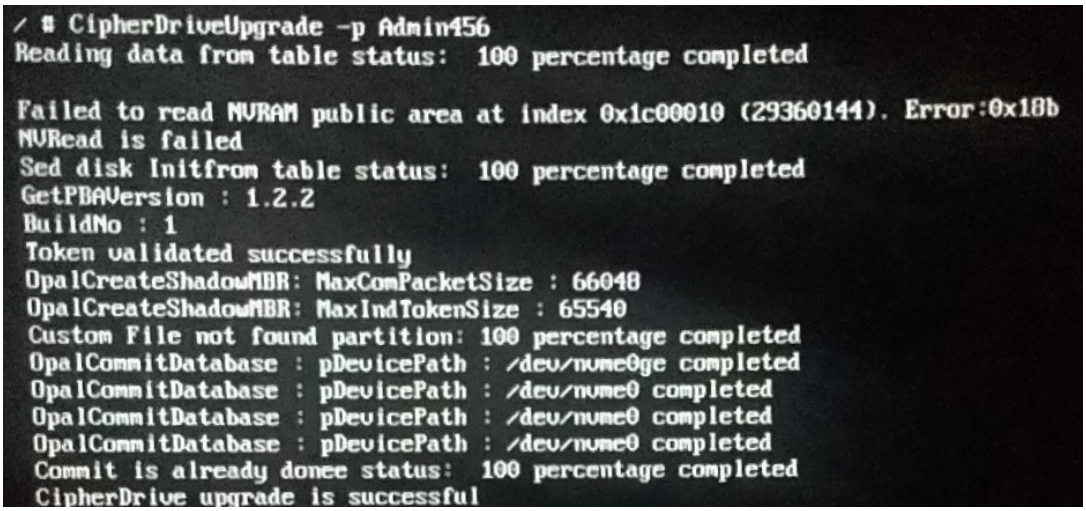
- If there are any changes in customization information (Disclaimer/Legal Notice, changes to your Organization name or your IT Support number), then the changed customFile should be copied to the root location
- For PBA Upgrade, please select device name (with PBA image)
- Click on the PBA Upgrade.
- In the popup, enter password of the logged in user having Admin (Role) rights.
- After the upgrade is successful, the system will power-off.

Instructions for upgrade using Command line utility:

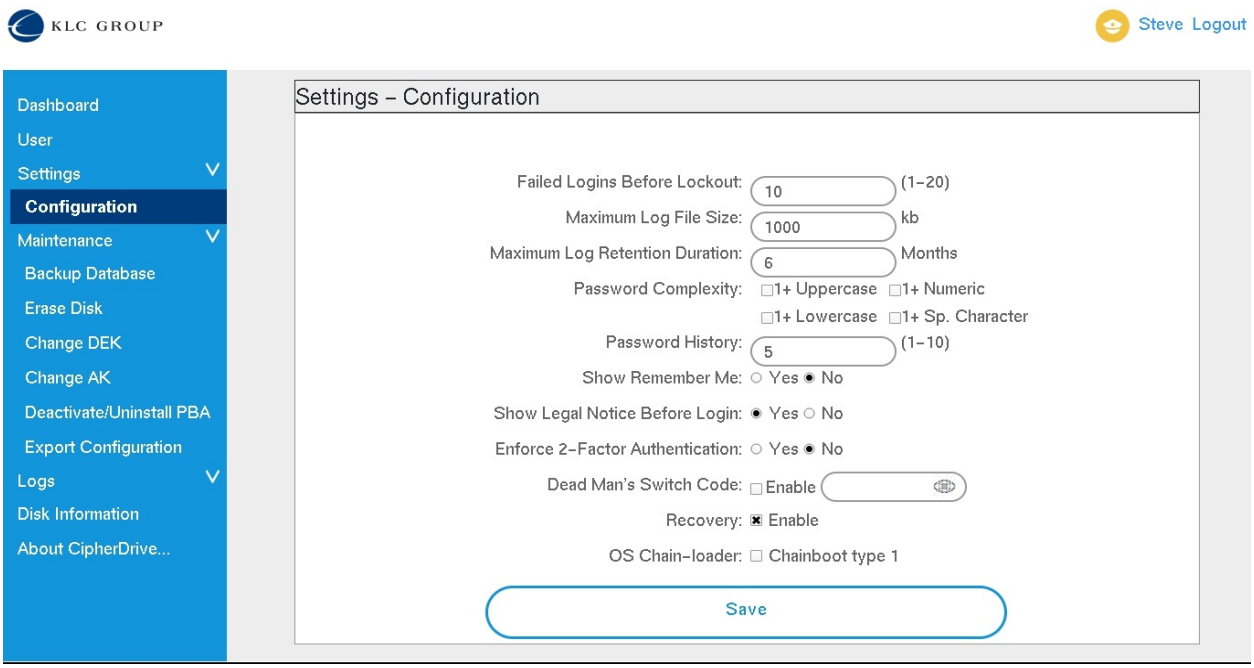
- Copy the upgrade files PBA.img and SecurityToken to the USB root having the CipherDrive installer files
- If there are any changes in customization information (Disclaimer/Legal Notice, changes to your Organization name or your IT Support number), then the changed customFile should be copied to the root location
- Boot to the USB drive
- On the command line execute the following command to upgrade the PBA:

  CipherDriveUpgrade -p <password>

  A sample screen output of the execution is as shown below:



Settings - Configuration



There are a number of configurable fields on the Settings - Configuration page:

For this section we will be describing the different fields on the panel titled Settings - Configurations.

Number of Consecutive failed login attempts:
When this number of consecutive failed login attempts is reached, further login will be disabled until a reboot of the system.

Maximum log file is the size of the log file after which older records will be automatically deleted. Maximum log retention duration is the amount of time the oldest logs will be kept. The logs will be retained based on whichever condition occurs earlier.

Password Complexity Fields: These fields define the enforced password complexity of users. There are four checkboxes that set the parameters for the password that is to be assigned. If you want passwords to contain at least one Uppercase character, then enable/checkmark the “Min One Uppercase” box. If a lowercase character is required then checkmark the checkbox at “Min one Lowercase”. If a number/digit should be required then checkmark the “Min one Numeric” box. To enable a special character then checkmark the “Min one special character” box.

Password History: Set the number of previously used (unique) passwords that should be remembered by the system before a user can use the same PW again.

Show Legal Notice before Login:

When this setting is Yes, the Disclaimer screen will be displayed prior to login screen. When the setting is No, the disclaimer screen will be shown after the Login screen.

Enforce 2-Factor Authentication:
On the configuration page this feature is enabling Two Factor Authentication (2FA) aka Multi Factor Authentication (MFA).

When this field is check-marked you have enabled "enforcing multifactor user authentication" which in short requires users to use both Smartcard and Password to logon.

If the field is disabled, then single factor login is allowed by using either Password or Smart Card (if SC is registered for the user).

Dead Man's Switch:
The DeadManSwitch is aimed to be used in an emergency situation for example in a situation where user is threatened while sitting at keyboard and pressured to logon e.g. under gun threat. Using the DeadManSwitch will erase all crypto keys and make it impossible to unlock the disk. Data will be lost permanently.

DeadManSwitch Code:
When DeadManSwitch switch is enabled, Security Officer or Administrator can set up the dead-man-switch code (PW) that can be used to authorize performing disabling access to protected OS

Recovery:
This switch is available to Security Officer role only. When this switch is enabled, Admin and Security Officer roles will be able to use the features Export Configuration and Database Backup. Otherwise, these features are not available. This field maps directly to the "-n noexport" installer option.

OS Chain-loader:
On certain systems, disks will lose power during the chain-booting process after login resulting in PBA being loaded repeatedly. On such systems, if this option is enabled, chain-loading will be used for handover from PBA to the protected OS. When this option is enabled, the PBA will display the kernels available for chain-loading. Select the kernel and click OK.

Dead Man's Switch Code Operation

The Dead-Man-Switch code is used when a threatened user wants to destroy the disk Authentication Keys making the disk content impossible to recover.

To carry out this operation, at the logon screen, enter the login user's username and password. In the password field, after entering the user's password, don't press enter/logon, instead continue by entering the Dead-Man-Switch Code directly following the user's password characters.
Now click the Logon button. The PBA will destroy all the AKs and thereby make it impossible to access the protected OS.

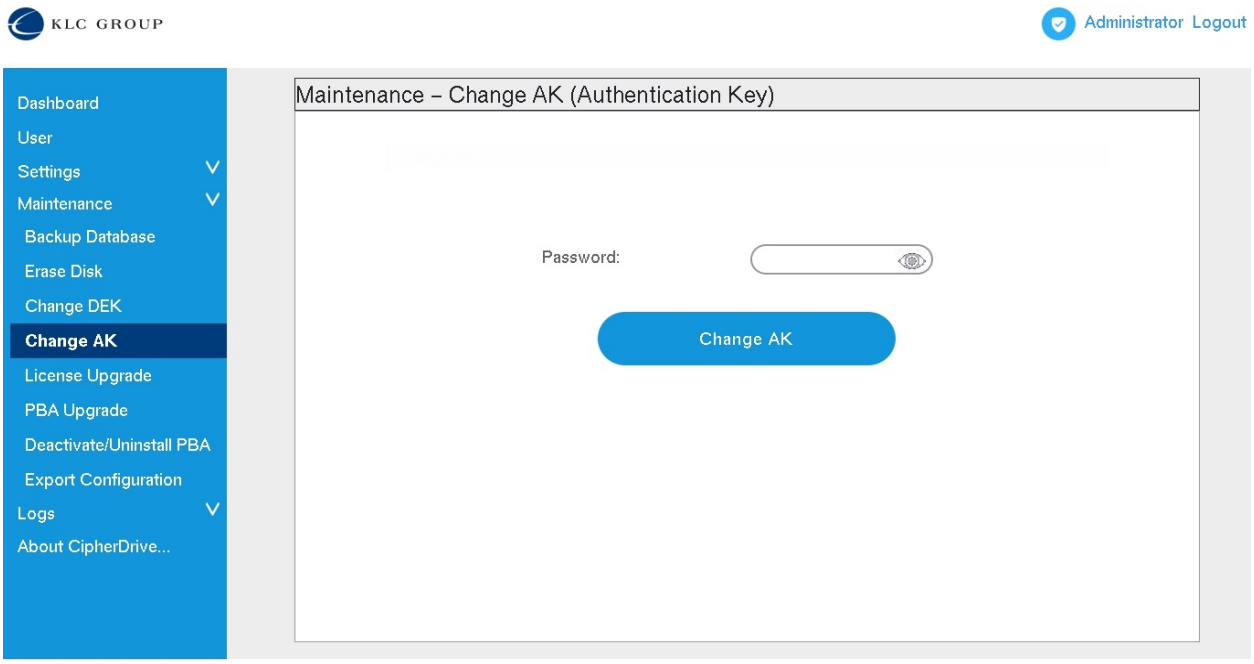
Note. To **repurpose**/reset the disk after Dead-Man-Switch has been used, there is a special utility in the installer which together with entering the so called PSID code (the factory reset code printed on the label of the physical disk) which will cryptographically erase the disk and revert the disk back to factory settings so it can be reused. The data will remain permanently lost because PSD changes the key in HW used to encrypt/decrypt sectors on the disk so there is no way to "recover" data from this operation but the disk itself can be used again.

Change Authentication Key

Change Authentication Key is aimed to be used when the Administrator or Security Officer suspects the AK keys to be compromised. Change Authentication Key allows the Security Officer to refresh all the AK keys of all SED users (while still keeping the protected OS and all protected data intact).

Change Authentication Key (AK) Code Operation

Use this option when the Security Officer or an Admin (role) wants to periodically change the AKs of the SED users (i.e. SID, ADMIN1, USER1 and USER2 keys)...

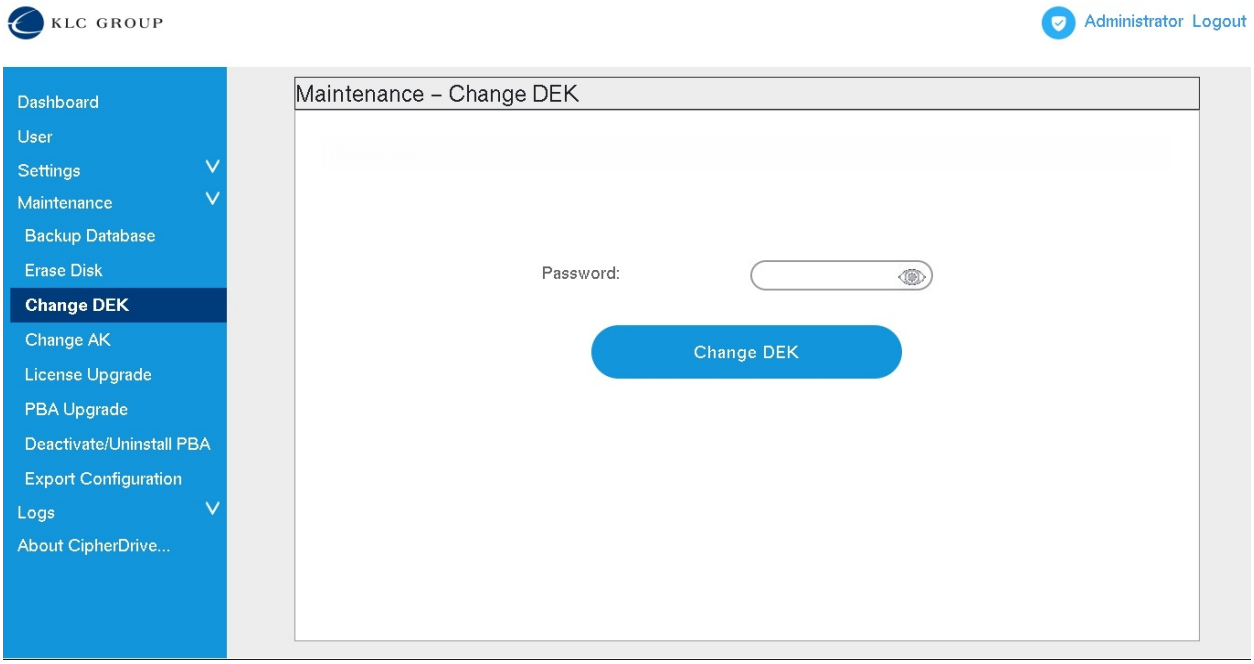


To carry out this operation, the Admin (role) or the Security Officer will select "Change AK (Authentication Key)" option from the Maintenance menu. He/she must enter PW and click "Change AK" button. A popup window is shown informing that "This operation will change the AKs used to access the SED Disk. It is nondestructive operation and the content of all the protected partitions will remain intact. Continue? Y/N" If Yes is selected, the PW is validated and

all the AKs are automatically changed and a confirmation message is shown to the user and the same message is entered into the log.

Change DEK

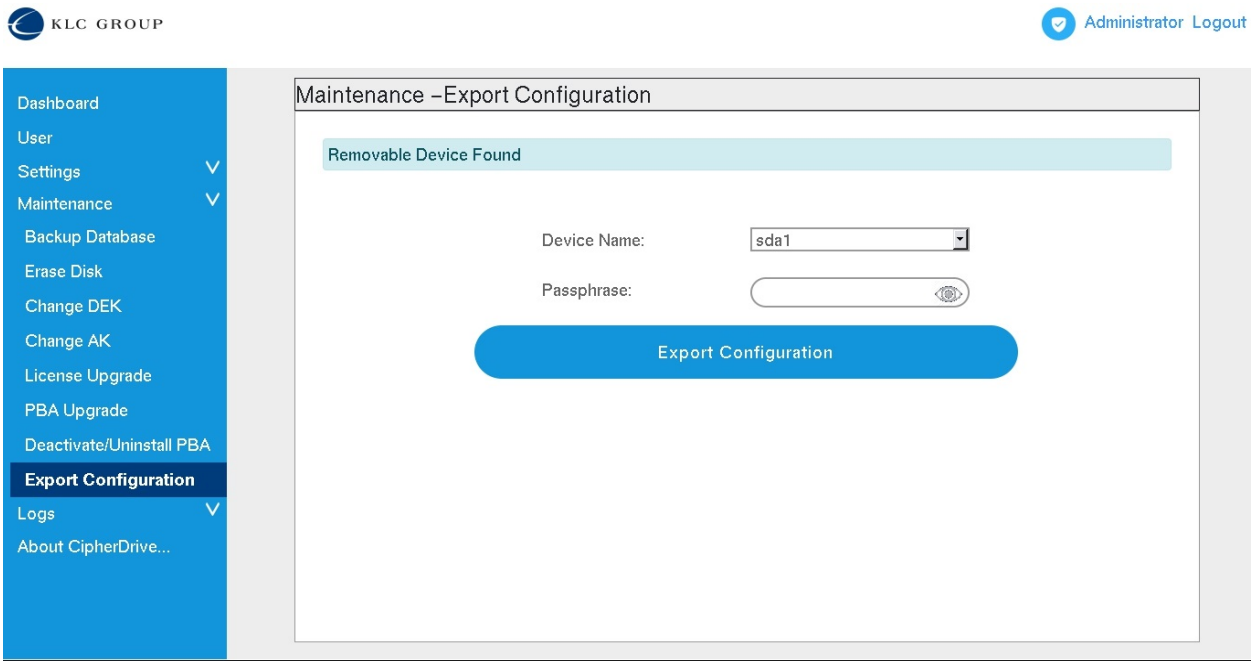
When the Security Officer wants to change the DEK of the SED this option can be used. The DEK is the actual key used to encrypt the data on the disk of the protected OS. This operation is also called “SED Gen Key” as it generates and will use a totally new key to read and write sectors on the disk independent of if there already is content on the disk or not. This command is also called Crypto-Erase as it is destructive to any current content already on the disk which will be completely (cryptographically) wiped.



To carry out this operation, the Security Officer or Admin (role) will select “Change DEK” option from the Maintenance menu. He/she must enter PW and click “Change DEK” button. A popup window is shown warning that “This operation will cryptographically and irreversibly erase/wipe the content of the SED Disk (all the protected partitions). Continue? Y/N” If selecting Yes, the PW is validated and all the content of the protected OS partitions will be erased/cryptographically wiped. A confirmation message is shown to the user and the same message is entered into the log.

Export Configuration

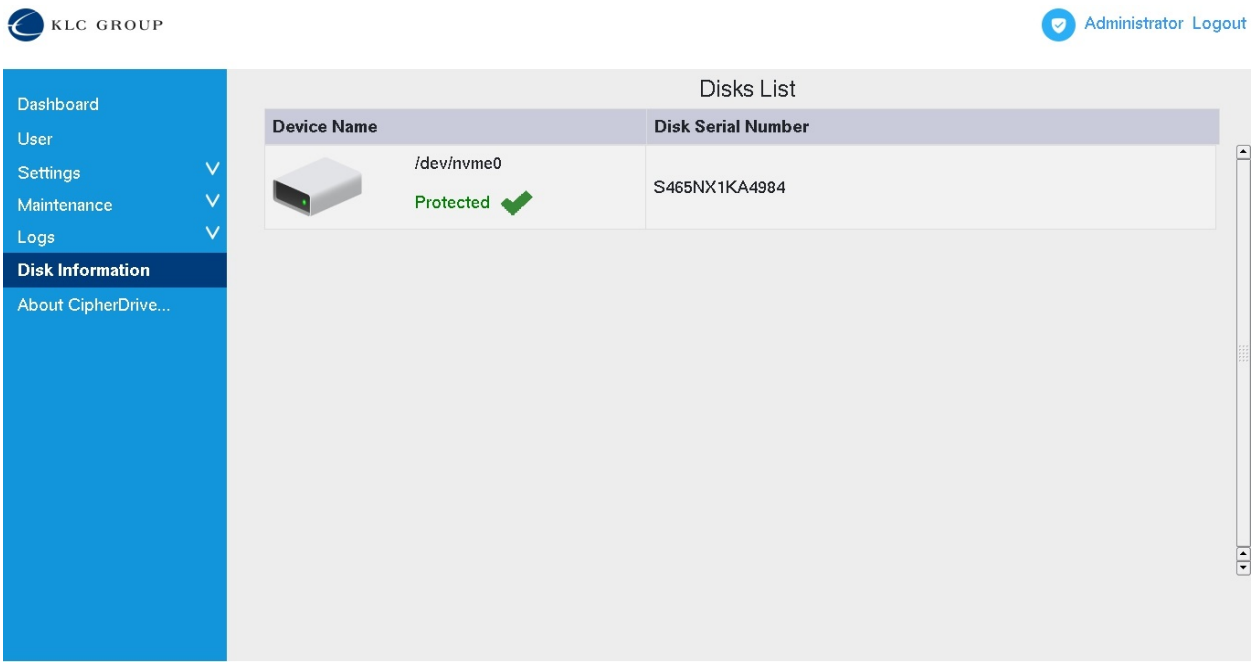
This feature is useful for deploying large number of devices with the same configuration on all of them. The configuration includes both users and settings. To carry out this operation, the Admin (role) or the Security Officer will select “Export Configuration” option from the Maintenance menu.



* For device name field, choose on what device/drive the files should be stored.
* Enter the passphrase that will be used to encrypt the output file /mnt/CDExportDB on the USB
* Click on Export Configuration button
* This will pop up a dialog to enter the logged in user password for reauthentication (verifying action) purpose
* The file will be created at the selected location and then it will display a message indicating the status of the operation.

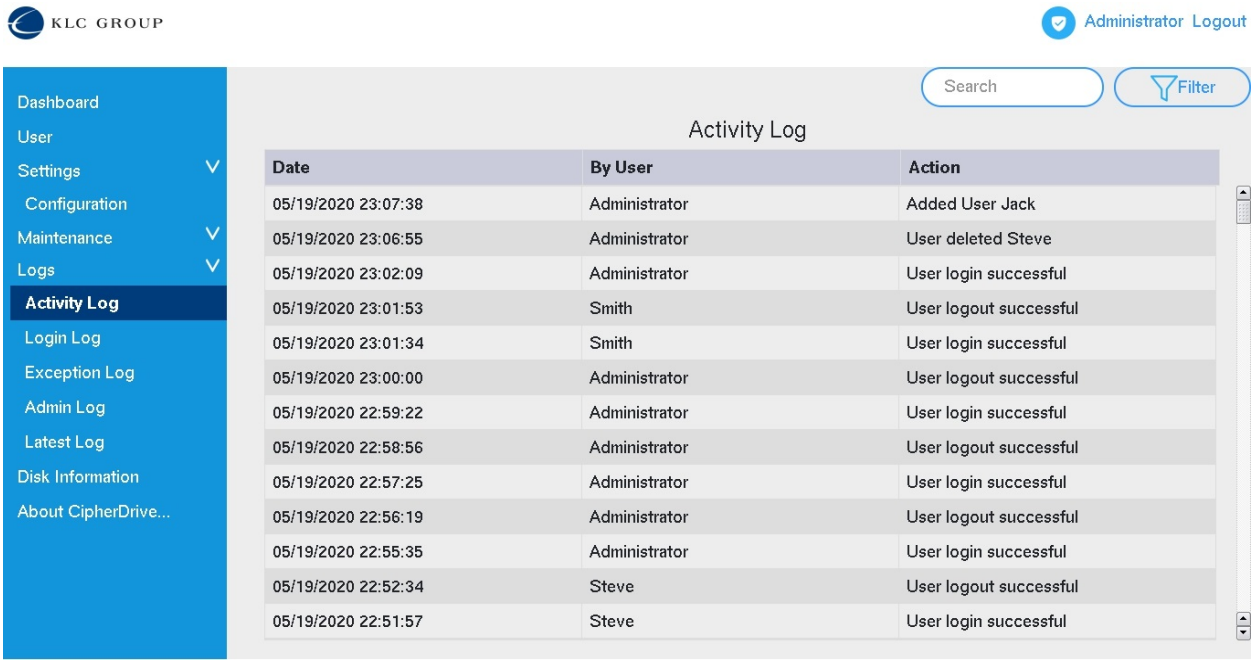
Disk Information

In Disk Information, a list of disks with device names, serial number and protection status is displayed. When multiple disks are installed in a system, the view will show all the installed disks with their protection status.



Logs

There are a number of logs collected by the system. To easily filter out what you are looking for, a number of default logs can be selected from. From the menu you can select to view the following logs: “Admin Log”, ”Login Log”, “Exception Log”, “Activity Logs” and “Latest Log”.



Logs can be divided up into 5 categories.

Admin log:
The Administrator log include all administrator actions carried out by the administrator on the account. Which includes:
Following are the examples of events under this log:

1. Added User
2. Edited User
3. User deleted

Login Log:
The Login log includes the successful and unsuccessful login and logout events of the system. Successful login means that the system was successfully unlocked by the user. Login failed means that the user was unable to unlock the system (and may have to retry). Logoff is usually not logged unless the user/administrator entered into the PBA admin application. A successful logoff shows that the user exited the admin application (and continued to boot the host system).

Following are the examples of events under this log:

1. User login successful
2. User login failed
3. User logoff successful (i.e. logging off from the PBA administration application)
4. User logoff failed

Exception log:
The Exception Log includes all the failed actions.

Following are the examples of events under this log:

1. User login failed
2. Failed to edit User
3. Failed to add User
4. Failed to delete User
5. User logoff failed
6. Incorrect JSON data for import Users

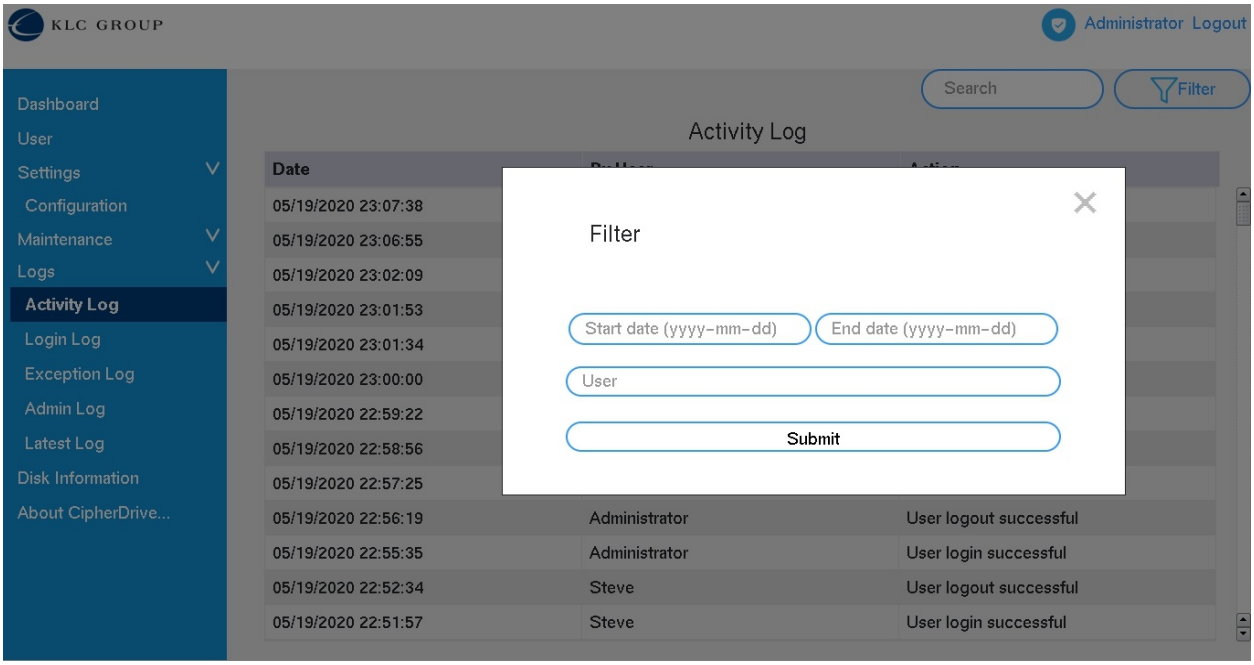
Activity log:
The Activity logs include all of the above-mentioned logs.

1. User login Successful
2. User login failed
3. User Logoff
4. Added User
5. Edited User
6. User deleted
7. Failed to edit User

8. Failed to add User
9. Failed to delete User
10. User logoff failed
11. Incorrect JSON data for import Users

Latest log:
Finally, as the “Latest logs” lists the logs for the current day (applicable to be viewed for the user role)…

Log Filter:
With Filter option, logs can be sorted/filtered by date and/or username



Log Filter
Filtering allows to narrow down any search in the logs by date range and/or username. Fill in one or more of the fields and press submit and the system will bring back the subset of logs.

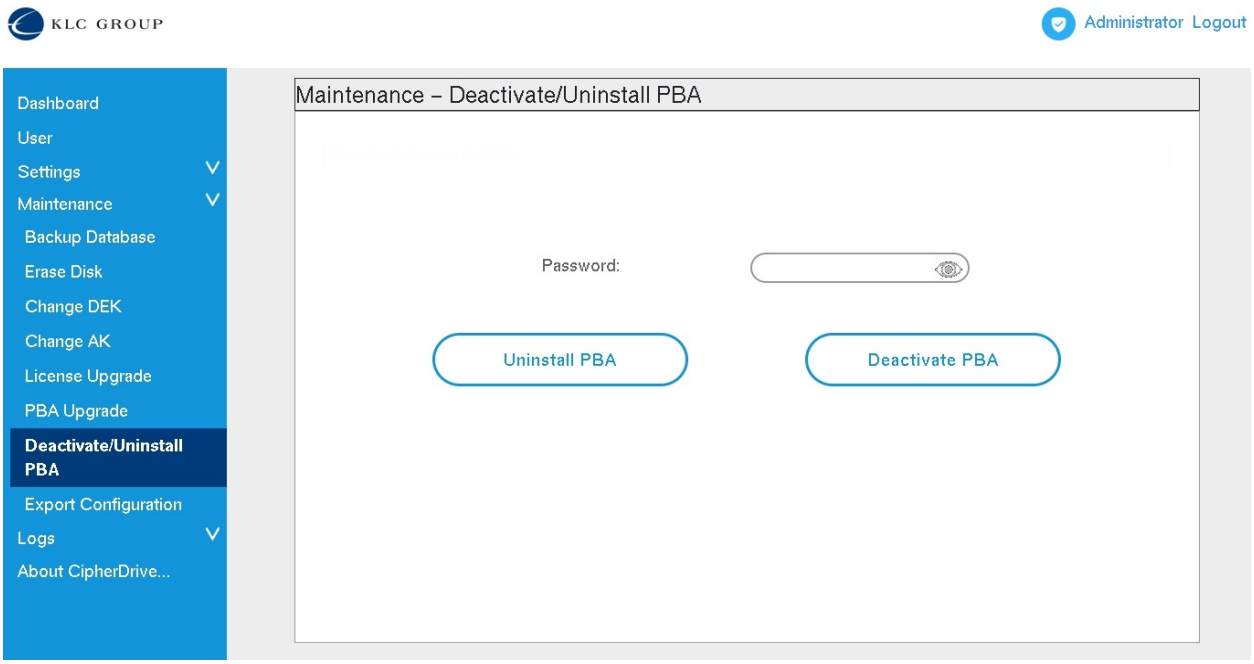
(Temporary) Deactivation and Uninstall

(Temporary) Deactivation: CipherDrive user logon can be temporary disabled by an authorized administrator to allow maintenance on the Host OS such as complex software updates on host that may require many reboots or require uninterrupted booting/reading from an USB/CD etc. Once the work on the host OS is completed CipherDrive can be re-activated again (settings and user database is kept intact).

Uninstall: In case there ever is a need to fully uninstall CipherDrive an Administrator can use Uninstall to fully uninstall the product (no settings/files will remain).

To temporarily deactivate (while keeping the database with users and settings intact) use the Deactivate option. If deactivate was used, once the work is done you can use the reactivate command and PBA will be enabled again at next boot. See “Reactivate” section below.

Use the Uninstall option to fully remove CipherDrive (all settings and users are removed).



When clicking the Uninstall PBA button, the PBA will ask for confirmation from the administrator (administrator option) and will then re-authenticate the user with the administrator’s password before proceeding with the uninstallation. Please note that the Uninstall completely removes the database and a new empty database is created during a re-install.

For Deactivation, a password needs to be provided as it is used for reauthentication of the user (verification of the action). When Deactivate PBA button is clicked, the system will ask for confirmation and then proceed with the deactivation.

Note that for Deactivation (temporary disable the product in order to work on the host) then the database (as mentioned above) will remain on the system and a following Reactivation will ask if the current database should be used. For Reactivation then the Install program (on the USB/CD) is used. The installer program will check that the administrator login credentials are valid for the database on the disk to accept re-activation.

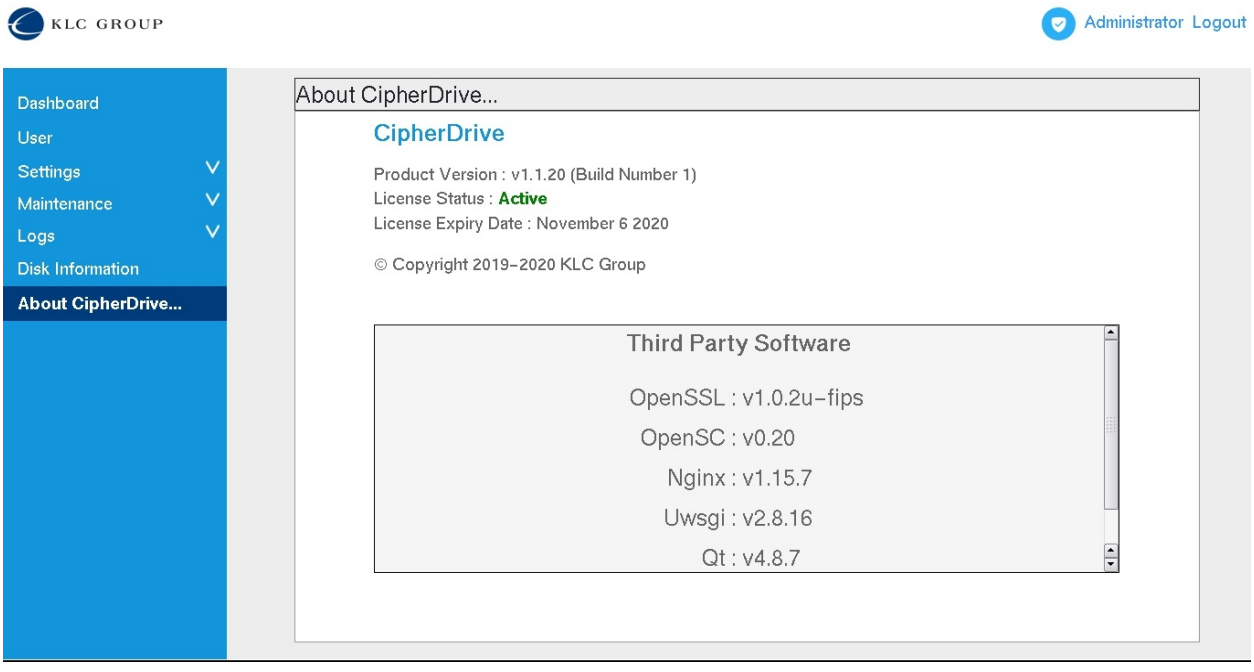
Reactivation

In the case that the PBA was deactivated (see Temporary Deactivation) e.g. in order to perform maintenance/debug on the host OS or any other situation when you temporary need to disable the PBA login. In order to re-enable the PBA login, the follow procedure will reactivate the PBA so that it will require pre-boot authentication again. When (temporary) Deactivation is enabled it keeps the user database intact so after reactivation all previous users and functionality is fully restored.

CipherDrive PBA can to be reactivated (with the content of the PBA database on the disk intact), by following the below procedure Prepare USB drive with CipherDriveInstaller and…

1. Boot the system with prepared USB drive containing the CipherDriveInstaller.
2. Mount the USB (e.g. mount /dev/sda1 /mnt or mount /dev/sdb)
3. Reactivate the PBA by executing the following command:
   CipherDriveInstaller -d /dev/nvme0 -p Password. Here, the password is for the default Administrator user (the default Administrator account) used when deactivating the PBA should be used. It is very important to remember the current/used password of Administrator user account at the time when deactivation was carried out. If this password is forgotten, reactivation is not possible.

About CipherDrive…



This screen displays the product version and the build number. It also acknowledges the “Third Party Software” used in the product.

Annexure 1 – Replacing a bad disk with a new disk

IN a multidisk system, if a disk on the system has gone bad and it needs to be replaced with a new disk, follow these steps:

1) Insert the replacement disk into the system in the manufactured state (unlocked)
2) Insert USB disk with CipherDrive installer
3) In the PBA, Export Configuration from the Settings Console using “Export Configuration” option of the Maintenance menu. After providing all the inputs, it will create a file CDExportDB in the USB root
4) Now boot CipherDriveInstaller from the inserted USB drive with CDExportDB file in the USB root and the license file for the new drive
5) Install the PBA to the new disk using the following command.

   CipherDriveInstaller -d /dev/<newdisk> -p <password> -dbp CDExportDB -ps <Passphrase>

   Where <newdisk> represents the replacement disk drive (e.g sdb, nvme1, etc)
   <password> is the Administrator’s password
   <passphrase> is the passphrase used while Exporting Configuration

After successful execution of the command, it will power-off. Boot the system and in the PBA, click on Disk Information menu item under Maintenance. The page should now display the replacement disk as protected.

Annexure 2 – CDOkey disk information collection tool

CDOKey disk info collection tool for licensing – first introduced in CDO version - 1.1.25
The CDOKey tool is collecting information from the disk already installer at customer site and where customer will collect this info from a number of computers and then send the resulting file CDO_Key.txt (from the inserted USB key) to KLC. KLC will send back activation codes that the installer will automatically find from the searching through the license activation file.

1. Start the command – cdokey

2. The tool prompts the user with the below:
   a. "This utility is used to capture the hard drive information to generate a license key for CipherDriveOne. The information will be captured to CDO_Key.txt on your USB key. A backup copy is saved in the ROOT folder."

3. The CDOKey program then intelligently grabs all the nvme and sata hard drives serial numbers, WWN and MSID and saves them in a file in the root of the USB folder.
    a. The backup file name captures the last date of appending, CDO_key_mmddyy.txt
    b. Each new serial number, WWN and MSID is automatically appended to the file.

4. The user is prompted: "CipherDrive key capture completed. Would you like to finish? (Y/N)"
    a. This is for the user who wants to continue and install CipherDriveOne.
    b. (Restart not needed, saves time for the user)

5. If user answer is:
    a. “Y”, then the computer will power off. “Please wait until the computer is completely off before removing the USB device.”
        i. Signal power off command to the user
    b. “N”, prompt the user, "Please continue to use the installer but wait until the computer is completely off before removing the USB device.”
        i. Return to prompt