KLC GROUP

KLC Group LLC

CipherDriveOne
Kryptr Administrator Guide

V 1.0.1

This manual covers CDO Kryptr 1.1.0 build 17 (and later)

KLC
4-18-2024

CDO Kryptr Administrator Guide

Introduction

CipherDriveOne Kryptr (CDO Kryptr) is a Pre-Boot Authentication (PBA) plus software based Full Disk Encryption (FDE) combined into one product providing Data-at-Rest DAR) protection. This means that a user must successfully authenticate (pre-boot) to the PBA module before getting access to the protected Host OS and any data partitions/disks (that always stays fully encrypted). The PBA module generate the keys needed by the FDE storage encryption driver to, transparent to the user, automatically encrypt any data written to the disk and decrypt data read from the disk (without Host OS' active involvement).

This manual covers CipherDriveOne Kryptr standalone installation on PC systems. The product supports both Windows and a number of Linux based host operating systems (OS).

Note: The name CipherDriveOne Kryptr or CDO Kryptr will be used interchangeably when discussing this CipherDrive product.

After successful product installation, the system will boot to the CDO Kryptr PBA and display the logon screen, where the user will enter user credentials and log into the CDO Kryptr PBA which, after successful authentication, will initiate chain-booting to the host OS or hypervisor environment.

Preparation

To prepare for the installation you will need a small (minimum 4 GB) USB connected thumb drive FAT32(bit) formatted (which is mostly factory default when you get the USB thumb drive). Copy the self-contained CDO Kryptr installer package onto the USB thumb drive and then boot from the USB thumb drive. You will then be prompted for any required input during the installation. After installation the system is ready to receive the first user logon (which will be described in more detail after the step-by-step installation description below).

Note: An ISO can be made available on request, in case it better fits your needs..

Prepare separate USB thumb drive (for installation of CDO Kryptr):

- Format a USB thumb drive (4GB or larger) in 'FAT32' format.
- Download cdo-kryptr-installer-release-0.0.1-buildNo-hash.zip. (A separate installer is needed if you want to install CDO Kryptr on OpenXT).

- Extract archive to root folder of USB thumb drive.

Installation of CDO Kryptr

CDO Kryptr Linux host OS installation (for Windows installation see page 8)

Step-by-Step - installing CDO Kryptr on Linux:

1. **Install Linux OS** (Ubuntu, Centos, RedHat)

   Note: When a fresh installation of Linux is made – remove all old partitions and boot to Linux at least once to verify that it is working as expected.
2. **Install (EE software encryption layer)** cdoksetup on the host OS
   Get the cdoksetup installation package from the folder with the corresponding OS version:
   - On Ubuntu (18.04, 20.04 or 22.04):
     - Install cdoksetup package on Ubuntu using: sudo dpkg -i <cdpsetup_*version*.deb>.
     - Execute the command cdoksetup with root privilege typing the full path to the file, for instance: sudo /usr/local/bin/ cdoksetup. Select 'Y' on all questions (if there are any).
   - CentOS (7.9 Linux or 8 Stream) and RedHat (8.4, 8.6, 9 and 9.1)
     - Install cdoksetup package on rpm using: sudo rpm -i <cdoksetup-*version*.rpm>).
     - Execute the command cdoksetup with root privilege typing the full path to the file, for instance: sudo /usr/local/bin/cdoksetup. Select 'Y' on all questions (if there are any).
   - OpenXT - a separate installer with integrated CDOK is needed.

3. **Install CDO Kryptr**
   Extract <cdo-krytpr-installer-*buildinfo*.zip> on a USB thumb drive. Install CDO Kryptr booting from the USB thumb drive on UEFI equipped computer with desired Linux installed on it. Here are the installation steps:

   Note: If you have SED disk with CDO installed on it – the disk should be in unlocked state to install CDO Kryptr (i.e. logon to the CDO and boot to the CDO Kryptr installation USB thumb drive without shutting down the computer).

   3.1. Install and encrypt on one disk

   a. To install CDO Kryptr boot from the CDO Kryptr installation USB thumb drive and execute:
      "**sh install-fde.sh -d /dev/sda -p Admin456**" or
      "**sh install-fde.sh -d /dev/nvme0n1 -p Admin456**"
      The default username with administrator rights is "Administrator".

b. After initial disk encryption (automatically performed during install) and CDO Kryptr activation are completed, reboot computer
c. CDO Kryptr login screen should show
d. Login with Administrator credentials

3.2. Install and encrypt on multiple disks/partitions

a. Boot from the CDO Kryptr installation USB thumb drive and check disk names (e.g. dev/sda has Linux OS, /dev/sdb is the second disk)
b. If the second disk is not formatted, you can use FormatDev.sh to format it. Type for instance:
   "sh FormatDev.sh -d /dev/sdb"
   (if you want to create a new partition with ext4 file system on /dev/sdb using the whole space of the disk) or
   "sh FormatDev.sh -d /dev/nvme1n1 –t xfs –s 20GB -l"
   (if you want to create new LVM partition on /dev/nvme1n1) or
   "sh FormatDev.sh -h" for more details

Note 1: Remember the path (after VolumePath=) printed at the end of the execution of the script to add it in the /etc/fstab file:

sh FormatDev.sh -d /dev/sdb -l
…
sudo lvmdevices --adddev **/dev/sdb1**
…
VolumePath=**/dev/mapper/pba2-storage**

Note 2: If the host OS is RedHat and the created partition is LVM, it is important to run in RedHat "**sudo lvmdevices --adddev *PV_NAME***" (*PV_NAME* is /dev/sdb1 from the example above). Boot from the CDO Kryptr installation USB thumb drive to proceed with step c.

Note 3: Skip this step if the second disk is formatted.

c. If you want to automatically encrypt an additional partition:

   <u>Method 1</u> (using a script in CDO Kryptr console):
   - Type the following command for instance:
     "sh AddVolumeToFstab.sh -d /dev/sda –p /dev/sdb1 –m /media/mydrive2"
     (where /dev/sda is the system disk with the host OS, /dev/sdb1 is partition to be encrypted and added to the /etc/fstab file, /media/mydrive2 is the mount point) or
     "sh AddVolumeToFstab.sh –d /dev/sda2 –p /dev/mapper/pba2-storage –m /media/mydrive2"
     (where /dev/sda2 is host OS root partition, /dev/mapper/pba2-storage is LVM partition to be encrypted and added to the /etc/fstab file, /media/mydrive2 is the mount point)

Method 2 (edit the /etc/fstab file in the host OS):
For non-LVM partitions on Ubuntu:

- Get the filesystem UUID of the partitions you want to use e.g.

"blkid -s UUID -o value /dev/sdb1"
Suppose that the output is "1fa85e0a-1c90-4c11-a4a8-9918d453e24b"

- Open /etc/fstab file and add the following line in it.

"UUID=1fa85e0a-1c90-4c11-a4a8-9918d453e24b /media/mydrive2 ext4 defaults 0 1"
(where /media/mydrive2 is the mount point, ext4 is the file system type)

For all other partitions:

- Open /etc/fstab file and add the following line in it.

"/dev/mapper/pba2-storage /media/mydrive2 ext4 defaults 0 1"
(where **/dev/mapper/pba2-storage** is VolumePath; /media/mydrive2 is the mount point, ext4 is the file system type)

Note: Skip this step if you have added the partitions for encryption in the /etc/fstab.

d. Execute b. and c. for every additional disk if you want to be automatically encrypted.
e. Boot to host OS to verify if everything is ok and boot again from the CDO Kryptr installation USB.
f. Use the standard command to install CDO Kryptr:
"sh install-fde.sh -d /dev/sda -p Admin456"
f. After disk encryption (automatically performed for the host OS partitions and partitions added in the fstab file during install) and CDO Kryptr activation are completed, reboot computer
g. CDO Kryptr login screen should show
h. Login with Administrator credentials

4. Login to Linux (normal operation)

If you want to boot to Linux, just type the Administrator credentials and leave the checkbox for Management Console blank. After these steps click 'Login' and the computer should chain-boot to Linux.

Note: To collect CDO Kryptr install logs make sure that the CDO Kryptr installation USB thumb drive is inserted and please follow these steps:

1) After CDO Kryptr is installed (and if USB thumb drive is attached) logs are collected automatically to the USB thumb drive and a message is given about that.
2) If for any reason the auto-collection of logs fails, you can collect the installation logs manually by entering the command: sh collect-logs.sh
3) Wait for logs to be collected to the USB thumb drive (around 1 min)
4) Unplug USB thumb drive from computer where you are performing the install and insert it into a different computer where you can analyze or send logs for further analysis.
5) All collected logs are in the klcpba2env.tar.gz archive and should be visible under the KLC folder.

This should be performed right after installation (while still on installation console) because the logs are in the memory and the installation log will be lost on restart/shutdown.

When using CDO Kryptr, collect console/login logs by pressing **F8/Fn+F8** while the CDO Kryptr installation USB thumb drive is attached.
Please note that if you collect logs again (after collecting them earlier) previous logs will be archived in the KLC folder with a unique name containing the date of collection.

CDO Kryptr for Windows Installation

Step-by-step - Installing CDO Kryptr on Windows:

1. I**nstall Windows 10/11,**
    a. Reboot and login to Windows as administrator
    b. Install EE software encryption layer for Windows (see step 2 below)

2. **CDOK_setup.exe (EE software encryption layer) -** Installation Steps:
    a. Run CDOK_setup.exe and go through the installation wizard
    b. Restart the computer
    c. Now ready for CDO Kryptr installation

    Note: Hibernation and Fast boot will be hidden/disabled temporarily from CDOK_setup.exe until some drive is encrypted by CDO Krytpr installation.

3. **Install CDO Kryptr and encrypt the disk(s) (same as on Linux)**

Extract <cdo-kryptr-installer-buildinfo.zip> onto a USB thumb drive. Install CDO Kryptr booting from the USB thumb drive on a UEFI equipped computer with Windows installed on it. Here are the installation steps:

a. Boot from the CDO Kryptr installation USB thumb drive and at the prompt execute:

“sh install-fde.sh -d /dev/sda -p Admin456” or

“sh install-fde.sh -d /dev/nvme0n1 -p Admin456”
The default username with administrator rights is “Administrator”

b. After disk encryption (automatically performed during installation) and CDO Kryptr activation are completed, reboot computer. Note that all valid partitions (created and formatted in Windows) on GPT bootable drives found on the computer will be encrypted. There should be at least one NTFS partition on a given disk to be encrypted.
c. CDO Kryptr login screen should now show
d. Login with Administrator credentials

Note: To collect CDO Kryptr installation logs make sure that the CDO Kryptr installation USB thumb drive is inserted and please follow these steps:

1) After CDO Kryptr is installed (and if USB thumb drive is plugged) logs are collected automatically to the USB thumb drive, a message is given about that.
2) If for any reason the auto collection of logs fails, you can collect installation logs manually by entering the command: sh collect-logs.sh
3) Wait for logs to be collected to USB thumb drive (around 1 min)
4) Unplug USB thumb drive from computer where you are performing the install and insert it into a different computer where you can analyze or send logs for further analysis.
5) All collected logs are in the klcpba2env.tar.gz archive and should be visible under the KLC folder.

This log collection procedure must be performed right after installation (while still on installation console) because the logs are in volatile (RAM) memory and the installation log will therefore be lost on restart/shutdown.

When using CDO Kryptr, collect console/login logs by pressing **F8/Fn+F8** while the CDO Kryptr installation USB thumb drive is attached.
Please note that if you collect logs again (after collecting them in an earlier install) previous logs will be archived in the KLC folder with a unique name containing the date of collection.

4. **Login to Windows (normal operation)**

If you want to boot to Windows, just type Administrator credentials and leave the checkbox for Management Console blank. After these steps click 'Login' and computer should chain-boot to Windows.

CDO Kryptr installation mandatory options:

-d <device name>: device (disk) on which CDO Kryptr is to be installed
-p <password>: Password of default Administrator account to be created during install

CDO Kryptr installation optional parameters

Install CDO Kryptr with a given license file:

If you have been provided a specific license file, please install CDO Kryptr and the license by executing the following command to install using the custom license file:

sh install-fde.sh -d <device name> -p <password> –lic <file name>

Install CDO Kryptr with Custom Legal Notice File:

If you have prepared the optional custom legal notice file (e.g. customFile on the USB thumb drive root, make sure to enter both filename and any extension, if extension is used, e.g. .json). Then please install CDO Kryptr by executing the following command:

sh install-fde.sh –d <device name> -p <password> -l customFile

Example content of custom/legal notice file:

{"Disclaimer Data":"Your disclaimer text.", "Organization Name":"Your company name", "Support Number":"Your company "}

If you want to insert a new paragraph use \n\n in text between paragraphs.

Install CDO Kryptr using exported configuration file

- In some cases, you may want to duplicate the whole setup from one system to one or more additional systems. In such cases, you can export the complete installation with users and settings for import into a new computer.
- Once you have the exported configuration file (e.g. CDExportDB file on the USB thumb drive root), from the Settings Console of another CDO Kryptr installation, then you can import that configuration by executing the following command:

Note: The provided password should be the password of Administrator at the time of export configuration. Passphrase in all commands below is the passphrase used in security console when CDExportDB file was exported.

sh install-fde.sh -d <device name> -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 CDO Kryptr to secure the new disk in-place and then bring it up seamlessly, use the following command:

  sh install-fde.sh 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.

Other options:

- In case recovery is to be disabled, you can use the “noexport” parameter to disable the options (disable the ability) to export configuration or backup the database. This parameter maps to the Recovery field (available to the Security Officer role only) in the Settings Configuration page.

  sh install-fde.sh -d <device name> -p <password> -n noexport

- If you want to use TPM2.0 to additionally protect the CDO Kryptr database (adding an extra layer of security), you can use the “- t allow_tpm” parameter:

  sh install-fde.sh -d <device name> -p <password> -t allow_tpm

If you want to see all possible options supported by the CDO Kryptr installer, you can type:

sh install-fde.sh -h

If auto-collection of installation logs fails you can type (to manually collect logs):

sh collect-logs.sh

1. Wait for logs to be collected to the USB thumb drive (around 1 min)

2. Unplug USB thumb drive from computer where you are performing the install and insert it into a different computer where you can analyze or send logs for further analysis.
3. All collected logs should be visible under the KLC folder.

   This procedure must be performed right after installation (while still on installation console) because the logs are in volatile (RAM) memory and the installation log will therefore be lost on restart/shutdown.

   When using the CDO Kryptr, collect console/login logs by pressing **F8/Fn+F8** while the CDO Kryptr installation USB thumb drive is attached.
   Please note that if you collect logs again (after collecting them at an earlier installation) previous logs will be archived in the KLC folder with a unique name containing the date of collection.

```
Loading CipherDriveOne Kryptr. Please wait...

Please press Enter to activate this console.
/bin/sh: can't access tty; job control turned off
/ # sh install-fde.sh -d /dev/sda -p Admin456
Installing CipherDriveOne Kryptr on /dev/sda ...
/**********************************************/
CipherDriveOne Kryptr Installer version: 1.1.0, build: 8, time UTC:Sep 21 2023 12:05:55
The Default License File 'EvaluationLicense_FDE' was found on a USB drive
Signed PBA image file is copied
License File is copied from the USB.
Device Path : /dev/sda
Resizing partition ...
Creating partition: start = 1050624  end = 19789823 size = 18739200
Creating partition: start = 19789824  end = 20838399 size = 1048576
Encrypting partition: /dev/sda2
Progress:   8.7%, ETA 07m47s,  792 MiB written, speed  17.9 MiB/s
```

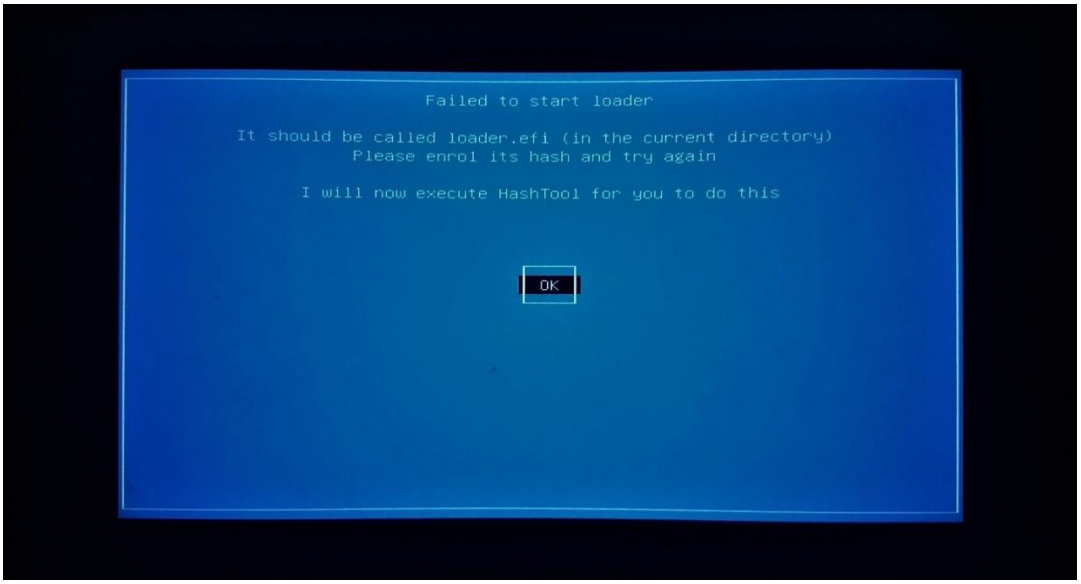
```
Loading CipherDriveOne Kryptr. Please wait...

Please press Enter to activate this console.
/bin/sh: can't access tty; job control turned off
/ # sh install-fde.sh -d /dev/sda -p Admin456
Installing CipherDriveOne Kryptr on /dev/sda ...
/**********************************************/
CipherDriveOne Kryptr Installer version: 1.1.0, build: 8, time UTC:Sep 21 2023 12:05:55
The Default License File 'EvaluationLicense_FDE' was found on a USB drive
Signed PBA image file is copied
License File is copied from the USB.
Device Path : /dev/sda
Resizing partition ...
Creating partition: start = 1050624  end = 19789823 size = 18739200
Creating partition: start = 19789824  end = 20838399 size = 1048576
Encrypting partition: /dev/sda2
Finished, time 08m34s,    8 GiB written, speed  17.8 MiB/s
Updating initramfs. It may take several minutes ...

PBA Activated Successfully.
Logs are collected to /dev/sdb1
/ #
```

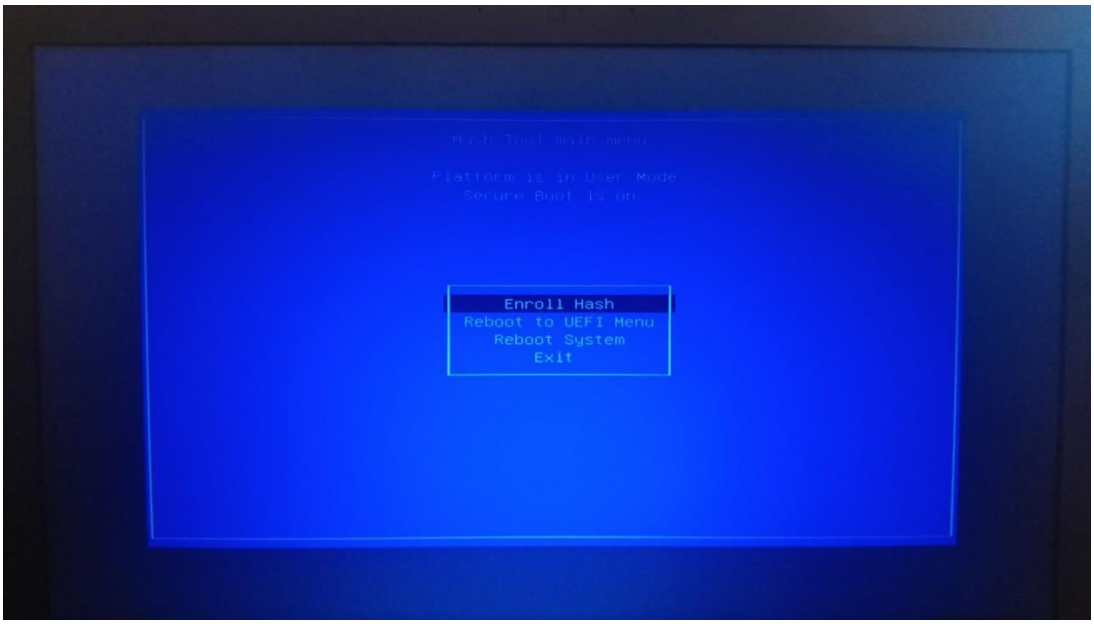
Installation with Microsoft signed bootloader

For this method, if Secure Boot is on, and on booting with CDO Kryptr from USB thumb drive for the first time, the system will enroll the boot loader before it can boot to install CDO Kryptr. The following images describe the steps:

Steps for enrolling boot loader before CDO Kryptr installation:

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





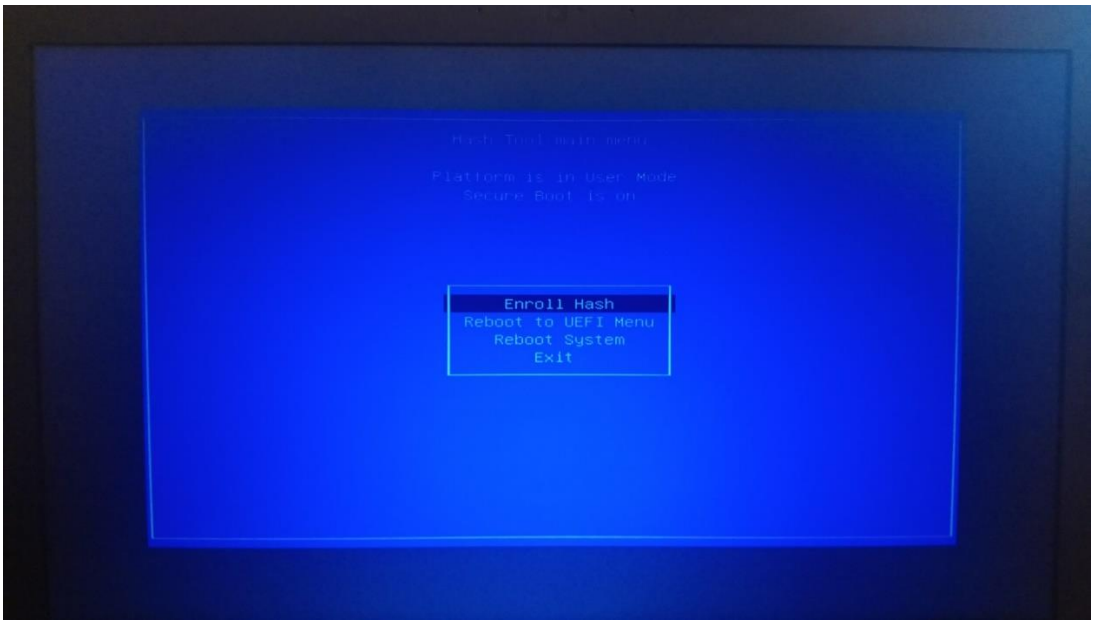
Enroll the loader by following the step in the picture below (select Yes).

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

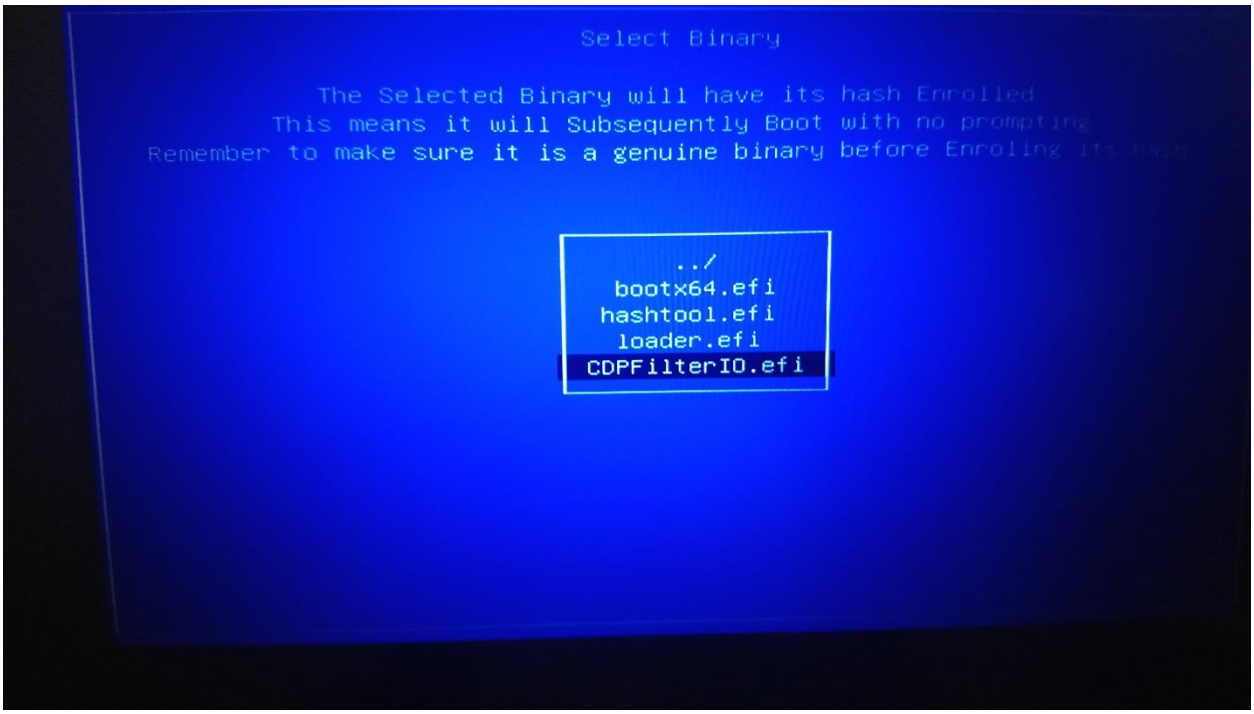
Steps for enrolling boot loader after CDO Kryptr installation:

After successful installation of CDO Kryptr, when booting from the hard-drive of the system, a similar procedure should be carried out one more time.

This time, after enrolling hash of loader.efi please select Enroll Hash (instead of Exit)…



so that CDOKFilterIO.efi can be enrolled in the same manner:



Subsequent to this, CDO Kryptr is setup to boot using Secure Boot and perform its operations securely (these setup screens will not be shown again).

Installation with custom signed binaries

The prerequisite for using this option is to manually clear the default Secure Boot keys. On most systems, the following is the procedure:

- Enter the BIOS setup screen by pressing F2 during startup.
- Go to Secure Boot -> Secure boot enable and choose ‘Disabled’.
- Go to Secure Boot -> Expert Key Management.
- Enable Expert Key Management.
- Click on 'Delete All Keys' button
- Save and Exit BIOS.

Note: Before installing in custom mode please make sure PBA_custom.img.gz file and SecurityTokenCustom file are copied to root of the USB thumb drive. Also, Secure Boot should be disabled in the BIOS right before installation in custom mode.

You can use the following command to install a custom signed bootloader:

sh install-fde.sh -d /dev/sda –p <password> -sb custom_signed

In case the BIOS secure boot keys are not cleared, this command will not be successful and will return an error. However, despite the error, if you want to go ahead and install, you can use the following command:

sh install-fde.sh -d /dev/sda -p <password> -sbf custom_signed

Note: If –sbf option is used, the installation should finish ignoring any error in Secure boot keys update (if there is any). However, secure boot could still not be successfully configured. Use this option only if BIOS secure boot keys were recently updated with CDO Kryptr keys.

After installation, shutdown the computer, enable Secure boot in BIOS and power back on.

Note:
If you want to restore default BIOS secure Boot Keys, here is the procedure:

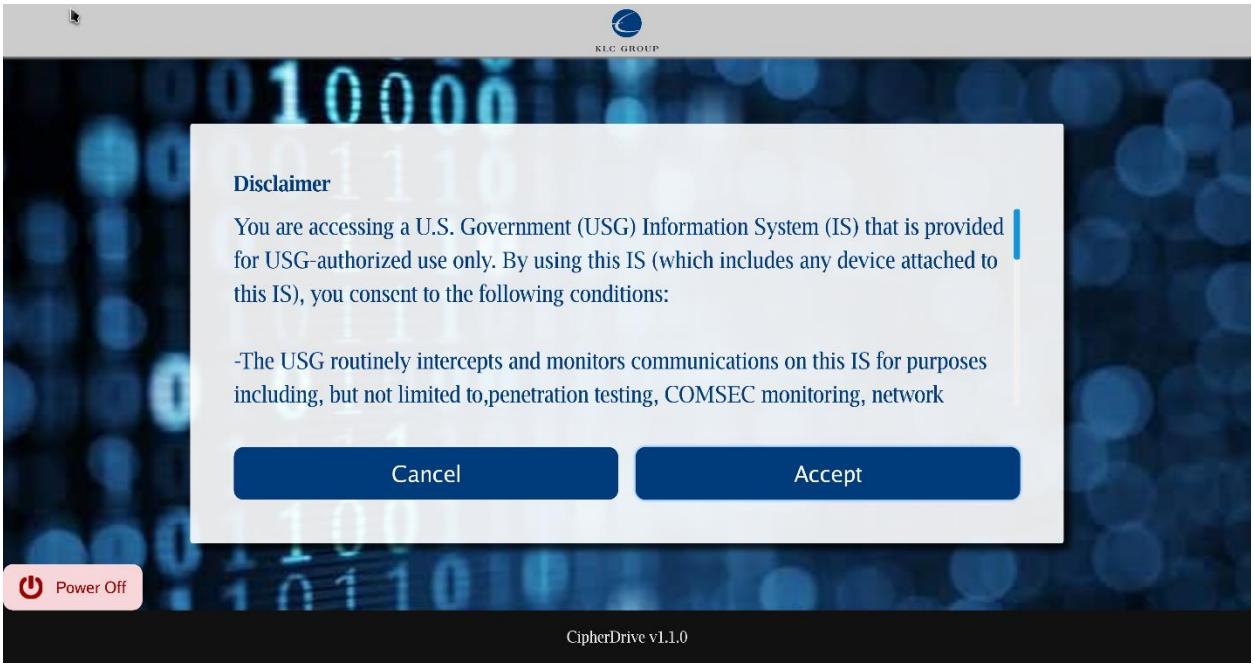
- Enter the BIOS setup screen by pressing F2 during startup.
- Once the BIOS setup screen comes up, go to Secure Boot -> Expert Key Management.
- Enable Expert Key Management.
- Click on 'Reset All Keys' button.
- Save and Exit BIOS.

After uninstallation of CDO Kryptr and if Secure Boot remains enabled we need to reset the BIOS keys to boot into the host OS

Configuration

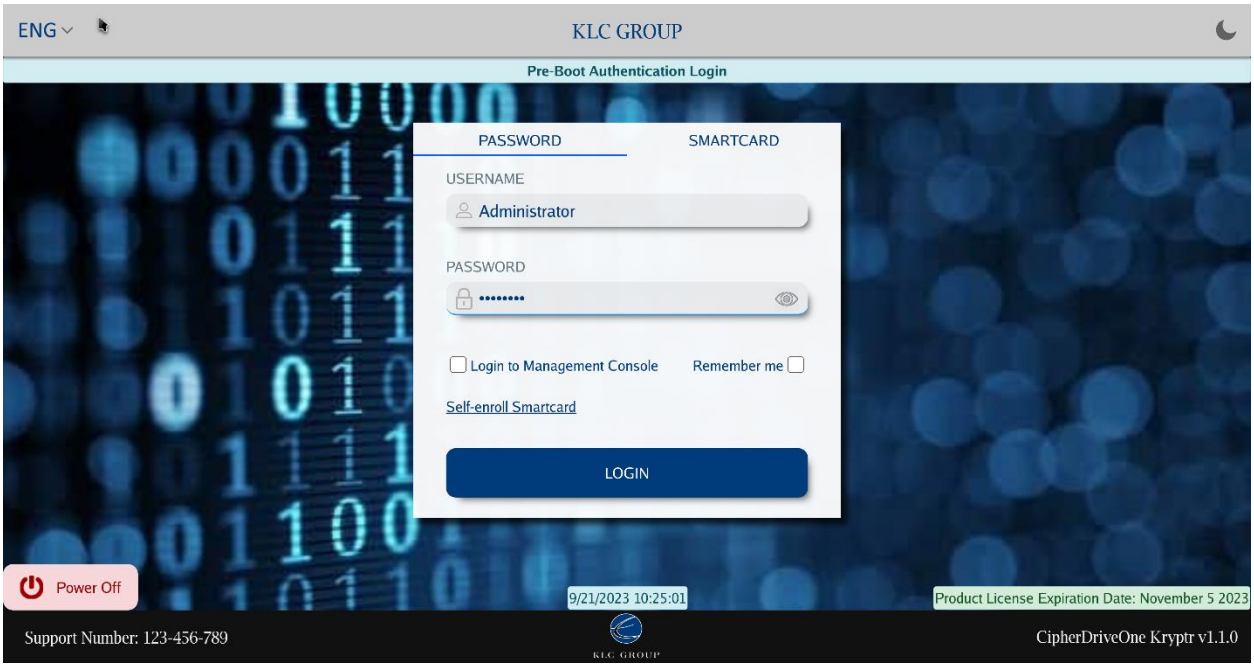
After the computer is turned on again, the system will boot into CDO Kryptr, first displaying a splash-screen (Disclaimer):

Disclaimer



The disclaimer screen contains conditions of usage of CDO Kryptr. If you don't agree to them, click 'cancel' or "power off". If you accept them, click 'Accept" and CDO Kryptr Login screen will appear. You are now ready to configure the system.

CDO Kryptr Password Login

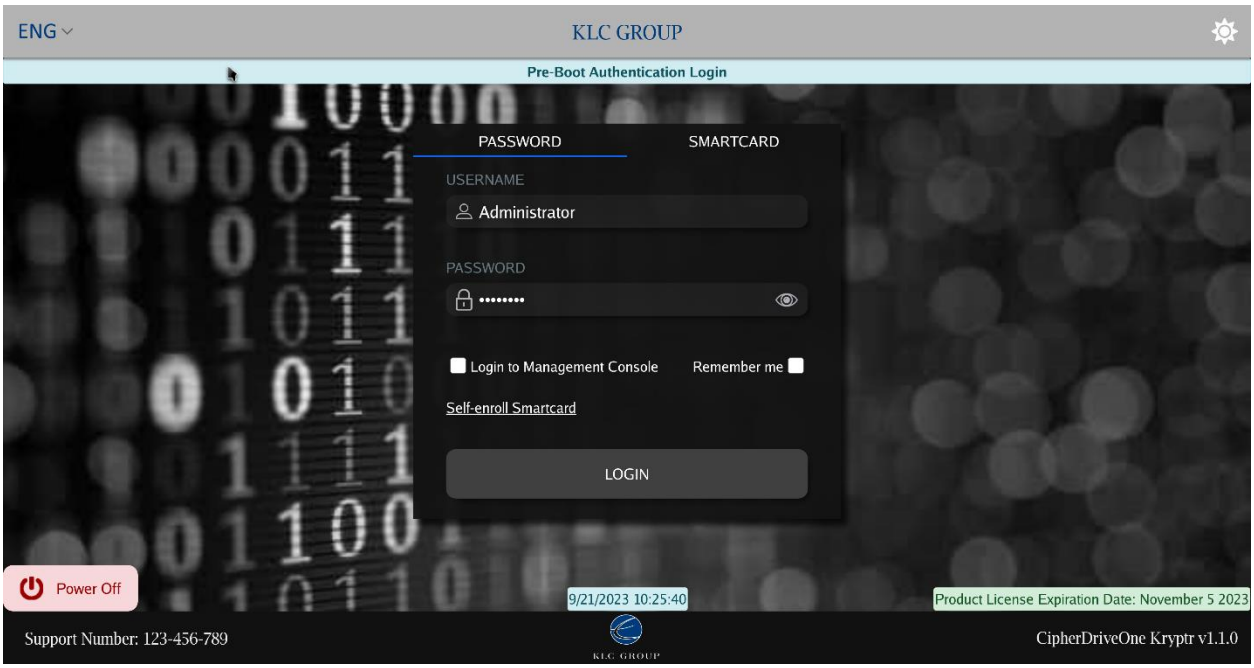


The only active account directly after installation is the default Administrator account, with the password that was setup during activation/installation.

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

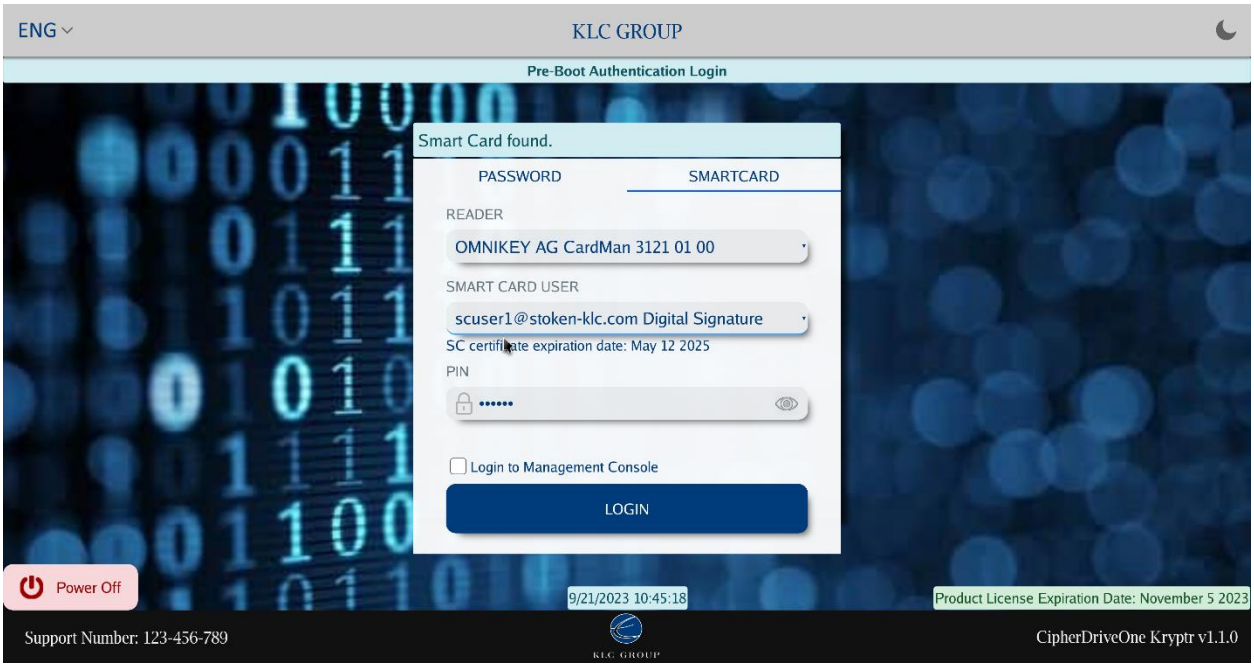
In case we want to logon as the user, Administrator (for the default administrator), in order to enter Management Console: please enter username "Administrator" and the admin password (as set during installation), checkmark the "Login to Management Console" option and press "Login" or just press enter.

Note: Clicking the 'Moon' icon in the upper right corner enables the dark theme for the CDO Kryptr login screen:



Clicking the ‘Sun’ icon restores the previous theme.

CDO Kryptr Smartcard login

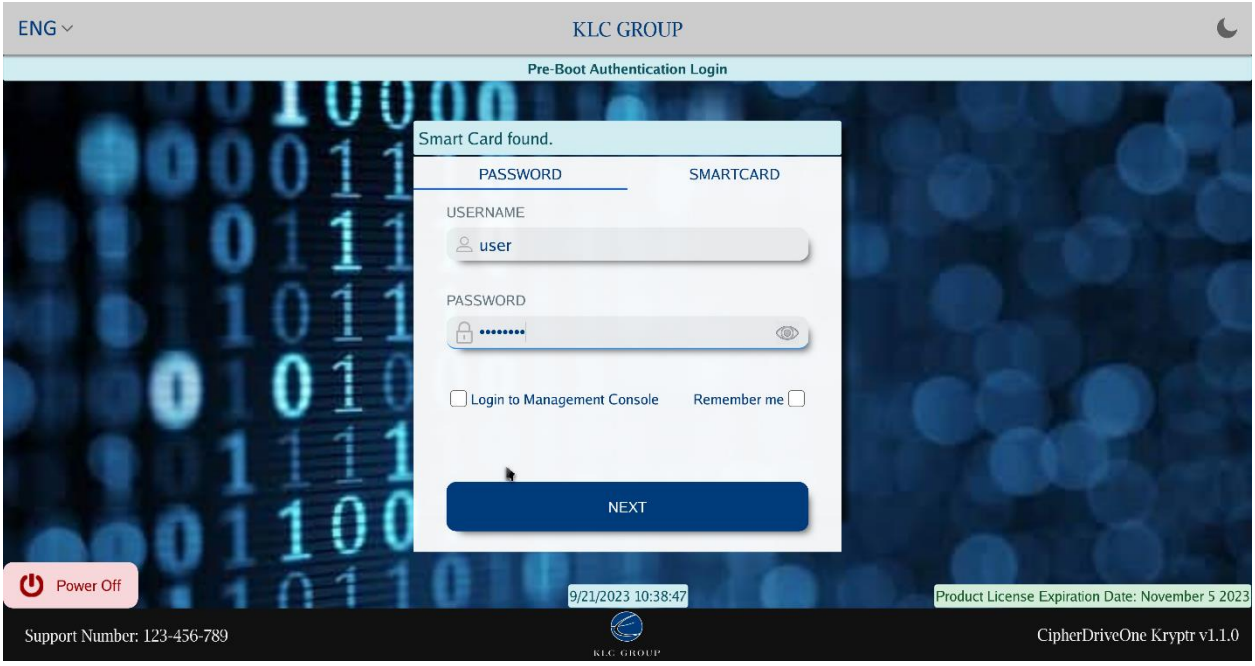


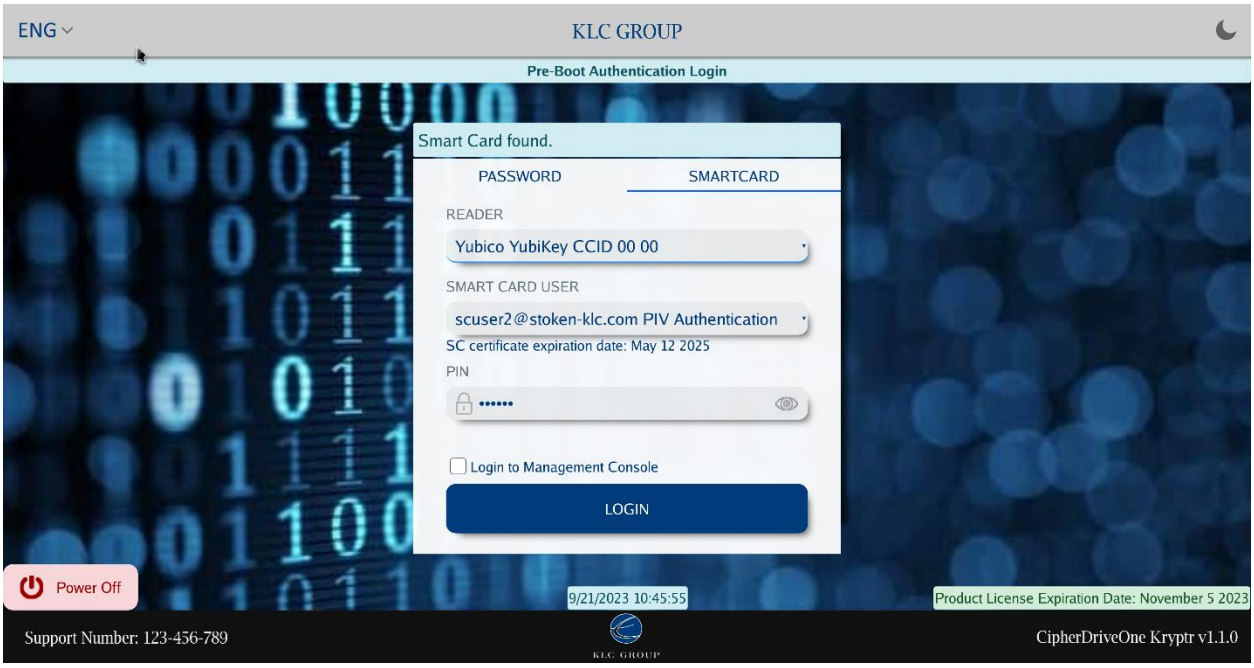
Note: Smartcard only is not part of the Common Criteria Evaluated Configuration

When logging in with smart card, please select SC reader and the user name from the dropdown (showing names from the installed certificates on the smart card), enter the PIN for the card and click “Login” button (or just press the “Enter” key). This will log into the Protected OS.

For Management Console access, please checkmark the “Login to Management Console” option before pressing “Login”.

Multifactor Authentication (MFA)

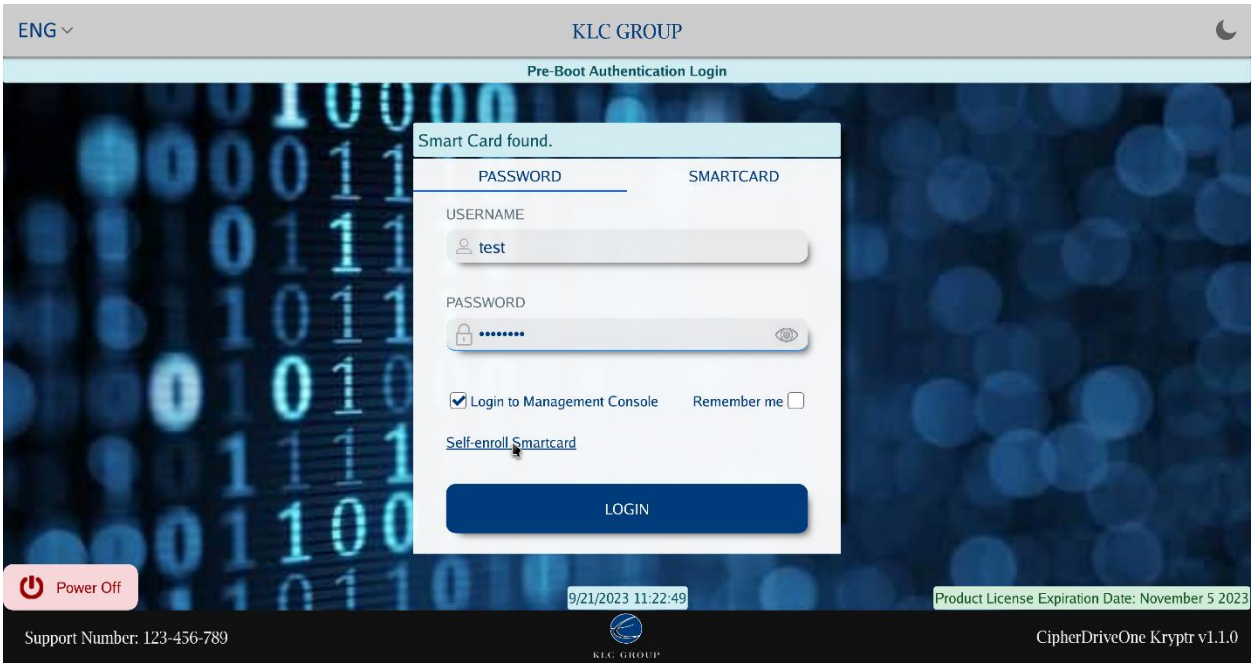


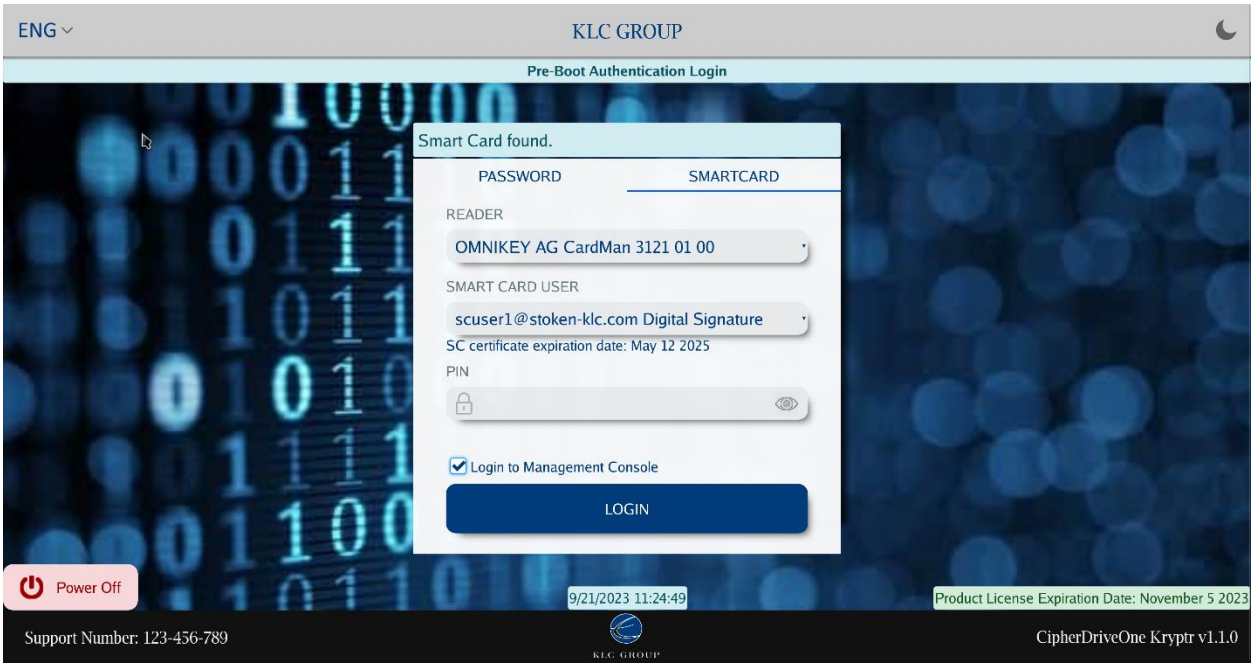


When Multi-Factor Authentication is enabled, both Password and smart card methods are required for login. In this case, the logon Password screen automatically shows the “Next” button. After entering the username and password, when the user clicks on the “Next’ button, the screen will automatically switch to the SMART CARD tab and the

button text changes to “Login”. The user can select the smart card reader and user and then enter the PIN. Click the “Login” button to log into the Protected OS. If you want to log into the Management Console, checkmark ‘Login to Management Console’ option as well before clicking the ‘Login’ button.

Enroll Smart Card

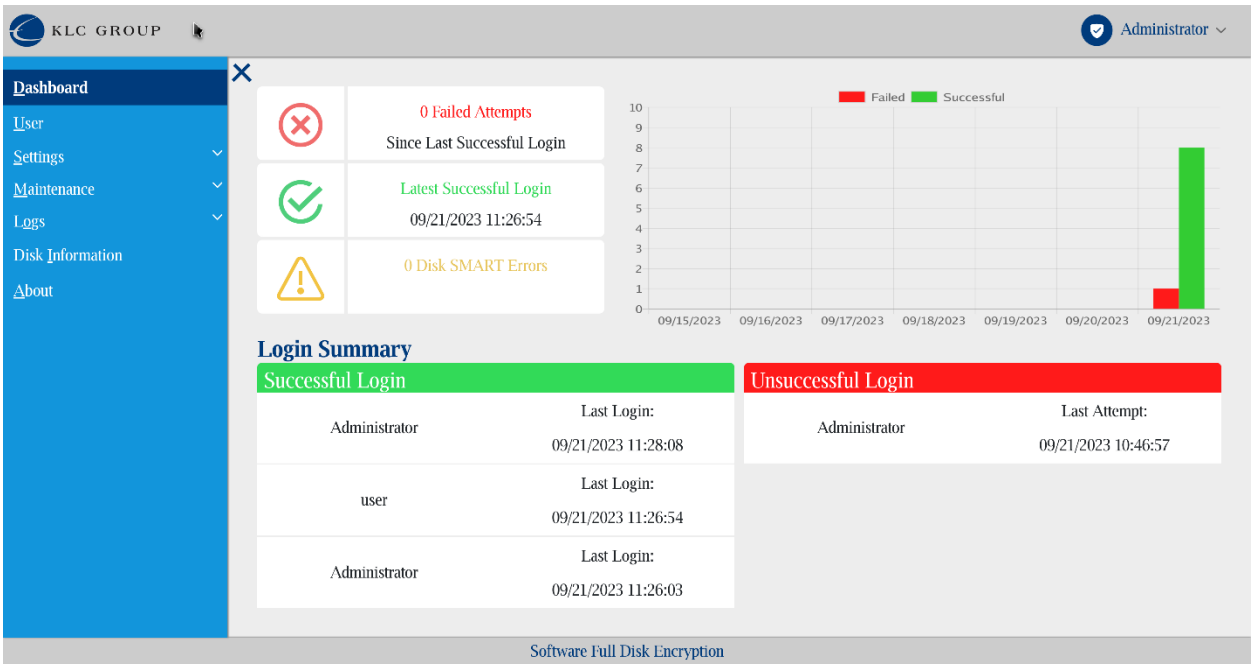




If a PW-only (password-only) user is successfully created, this user can be enrolled with SC (smart card) login method while on CDO Kryptr login screen:

1. Create a PW-only user.
2. Logout.
3. On the CDO Kryptr PW login screen, enter valid credentials (UN and PW).
4. Checkmark Login to Management Console and click ‘Self-Enroll Smart Card’.
5. We are then taken to the SC login screen: here add valid SC info (SC reader, SC cert and SC PIN). (note: This combination of cert and PIN should not be used in another already created user.)
6. Click ‘Login’.
7. On the Management Console (Users table) check that now PW-only user has an enrolled SC method as well and can be authenticated into MFA mode.

Dashboard



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

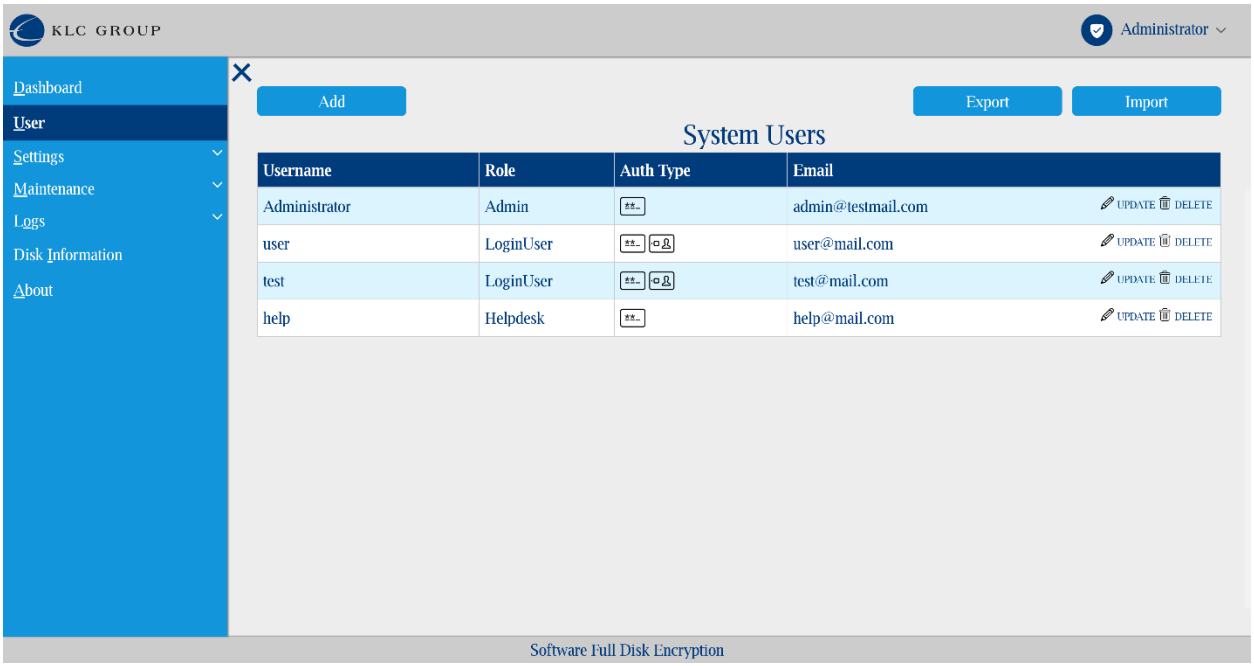
The dashboard screen shows the following events summary:

- 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 disk - if any)
- Graph displays the last 7 days of records of failed and successful login attempts

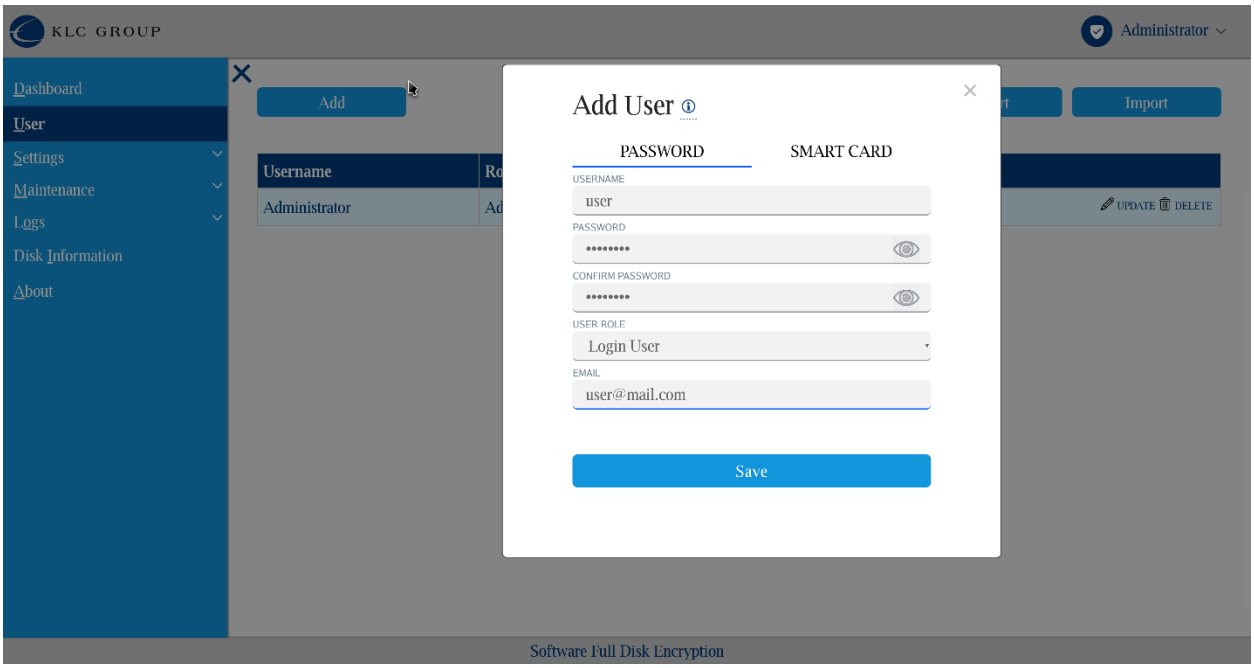
- Login Summary consists of latest successful and unsuccessful login attempts of distinct users
- Admin and Security officer can view the successful and failed attempts of all Users

Users

To add a new user select “User” on the left navigation bar and then press “Add”.



Add a Password User



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

1. Enter a unique Username of the user to be added.

   Max 40 characters (Upper and Lowercase Latin letters along with their accent, diaeresis, etc. versions (with Unicodes 00C0-017F), Numbers and Special characters). The following special characters are allowed:

   "_", ".", "'", "@", "(", ")", "\", "/", "-"

2. Enter the initial password for the user.

   From 8 to 128 characters (Upper and Lowercase Latin letters, Numbers and Special characters allowed. The following special characters are allowed:

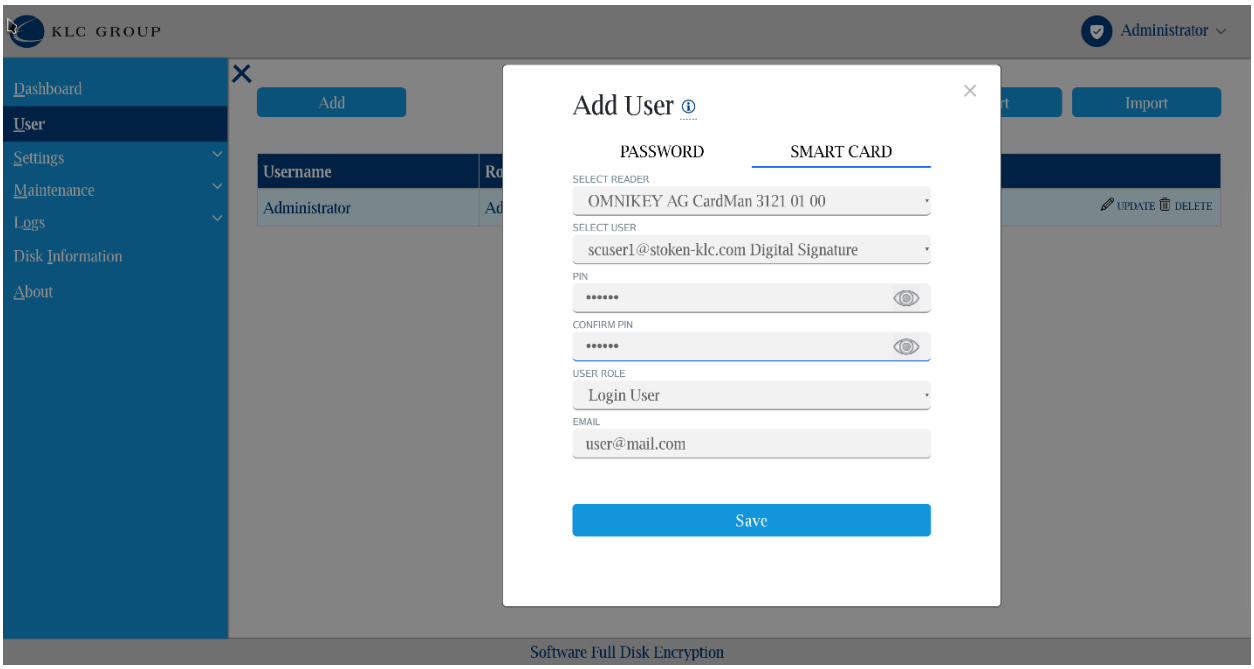
   "!", "'", "#", "$", "%", "&", "'", "(", ")", "*", "+", ",", "-", ".", "/", ":", ";", "<", "=", ">", "?", "@", "[", "\", "]", "^", "_", "`", "{", "|", "}", "~"

3. Re-enter the password to confirm.
4. Enter the user role.

See “Roles” section below.

5. Enter email address.
   Currently used as user identifier
6. Press “Save” .
7. Observe user is added to list of system users.

Add a Smart Card User



Please also note that smart card-only administrators will have limited administration functionality as CDO Kryptr currently treats Password as the primary mechanism for configuration and administration tasks. A single factor smart card 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 smart card).

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 “SMART CARD” is underlined/highlighted. Insert the smart card to be added into the reader.

1. Select SC reader (if there are more than one) on SC reader drop down menu
2. Select Username the user to be added from the username in SC certs from the drop down menu.

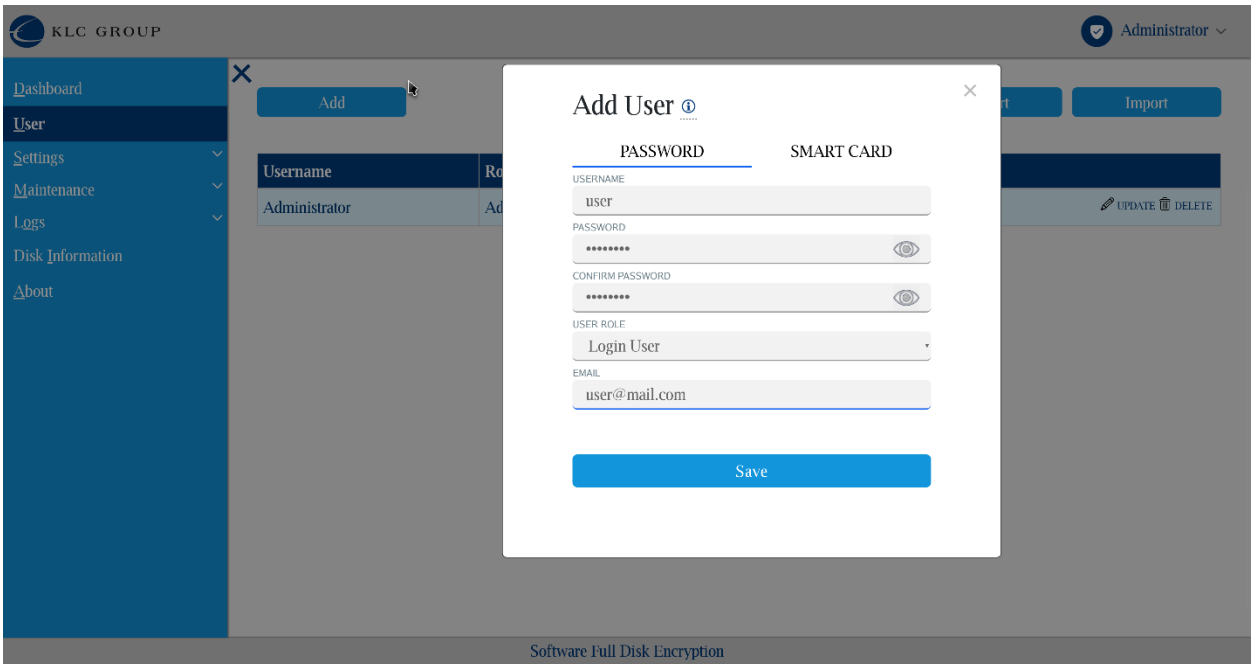
Must be selected from available usernames on SC.

3. Enter the PIN.
4. Re-enter the PIN.
5. Enter the user role.
   See “Roles” section below (must be same role as for password setting).
6. Enter email address.
   Currently used as user identifier.
7. Press “Save”.
8. Observe user is added to system users list.

Add a MFA (Multifactor Authentication) User

A MFA user is a user configured to use both enrollment methods (password and smart card). This provides more secure login into Host OS and to CDO Kryptr management console. Please find info how to create such user below:

1st step: add/configure Password method to MFA user



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

1. Enter a unique Username of the user to be added.

Max 40 characters (Upper and Lowercase Latin letters along with their accent, diaeresis, etc. versions (with Unicodes 00C0-017F), Numbers and Special characters). The following special characters are allowed:

"_", ".", "'", "@", "(", ")", "\", "/", "-"

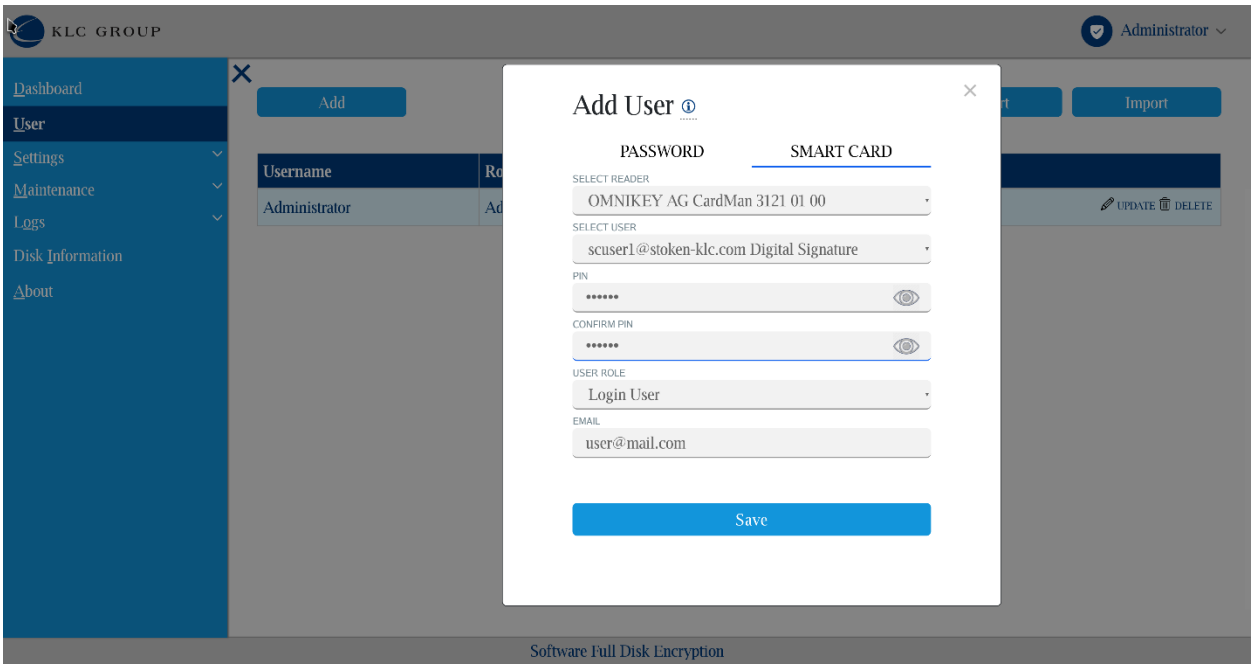
2. Enter the initial password for the user.

From 8 to 128 characters (Upper and Lowercase Latin letters, Numbers and Special characters allowed. The following special characters are allowed:

"!", "'", "#", "$", "%", "&", "'", "(", ")", "*", "+", ",", "-", ".", "/", ":", ";", "<", "=", ">", "?", "@", "[", "\", "]", "^", "_", "`", "{", "|", "}", "~"

3. Re-enter the password to confirm.
4. Enter the user role.
   See “Roles” section below.
5. Enter email address.
   Currently used as user identifier
6. Click SC tab (do not click ‘Save’ yet) to proceed to 2nd step below

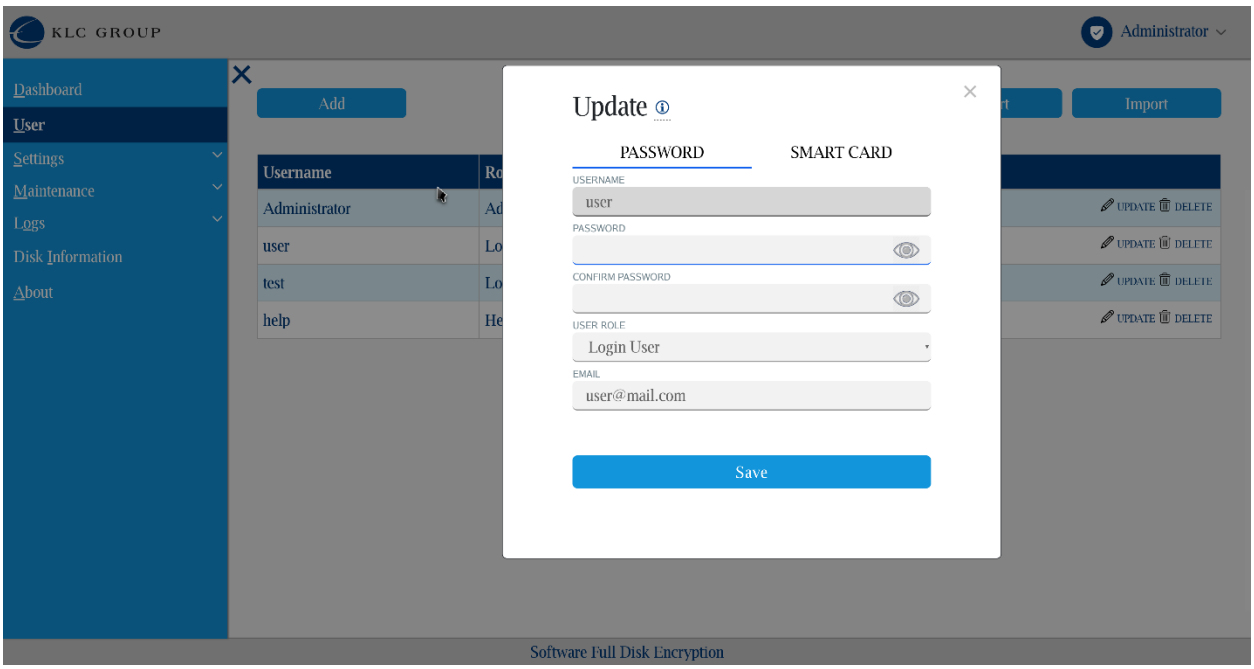
2nd step: add/configure SC method to MFA user



Click on SC tab after entering all info on PW tab as shown above. Make sure the tab “SMARTCARD” is underlined/highlighted. Insert the smart card to be added into the reader.

1. Select SC reader (if there are more than one) on SC reader drop down menu
2. Select Username the user to be added from the username in SC certs from the drop down menu.
   Must be selected from available usernames on SC.
3. Enter the PIN.
4. Re-enter the PIN.
5. Enter the user role.
   See “Roles” section below (must be same role as for password setting).
6. Enter email address.
   Currently used as user identifier.
7. Press “Save”.
8. Observe user is added to system users list.

Update Password User



After clicking Users tab you will see list of system users. To the right of a username of a user there is a ‘Update’ option. Click on it to bring up an Update user screen. Make sure

Password is underlined. 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 Update User screen. After updating the fields, click on the Save button.

1. Enter the password for the user.

   From 8 to 128 characters (Upper, Lowercase, Numbers and Special characters allowed. The following special characters are allowed:

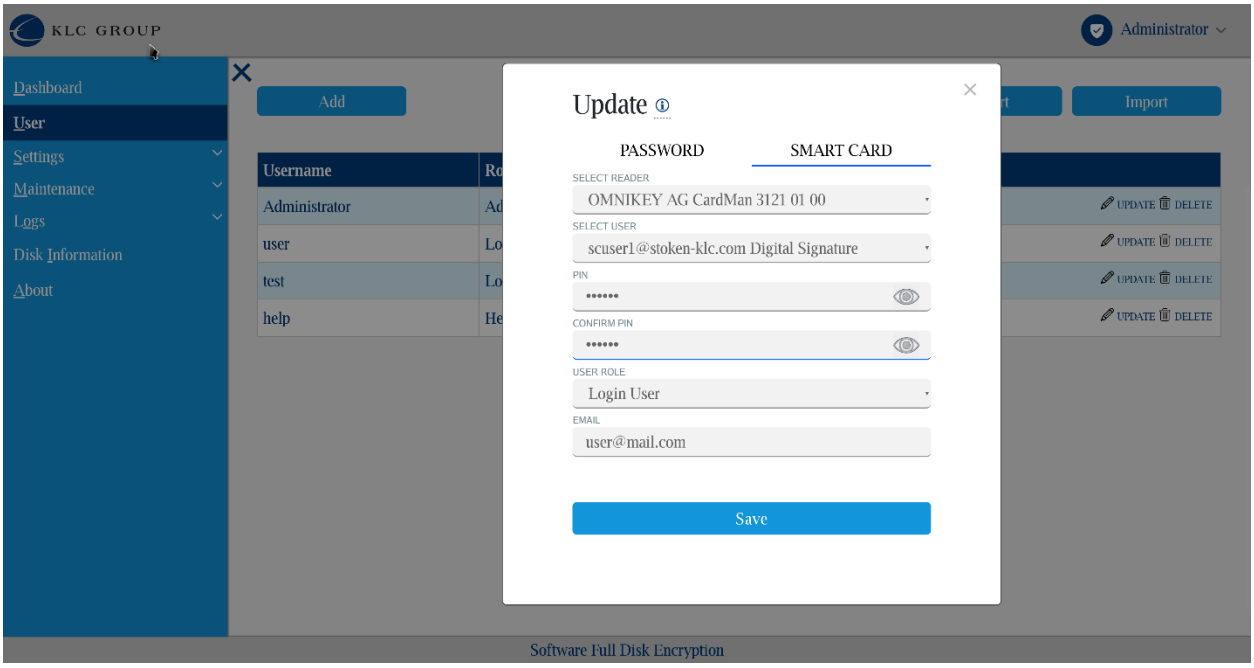
   "!", """, "#", "$", "%", "&", "'", "(", ")", "*", "+", ",", "-", ".", "/", ":", ";", "<", "=", ">", "?", "@", "[", "\", "]", "^", "_", "`", "{", "|", "}", "~"

2. Re-enter the password to confirm.
   Reenter the same password.
3. Enter the user role.
   See “Roles” section below. Only Admin and Secutity Officer roles can modify this field.
4. Enter email address.

Currently used as user identifier.

5. Press “Save”.
6. User is updated.

Update Smart Card User



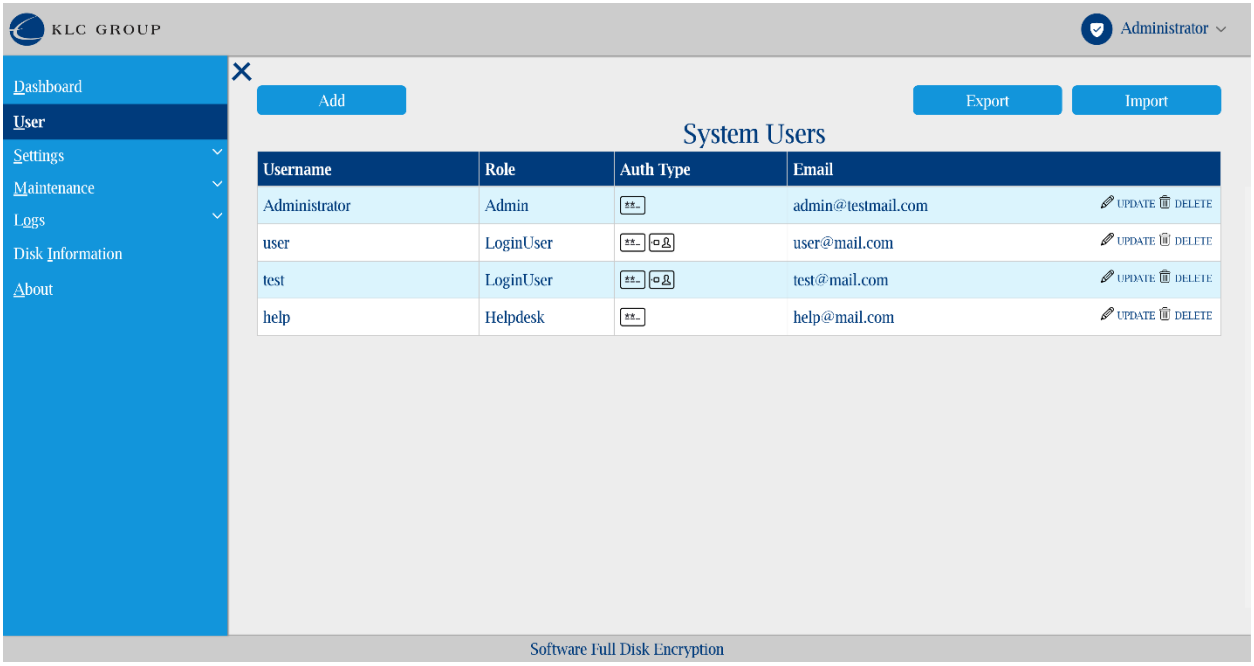
Click on the SMART CARD tab on the Update user screen to edit the smart card related fields. All the fields including smart card user are modifiable. After updating the fields, click on the Save button to commit the changes.

1. Select SC reader (if there are more than one) on SC reader drop down menu
2. Select Username the user account to be modified/updated from the username in SC certs from the drop down menu.
   Must be selected from available usernames on SC.
3. Enter the PIN.
4. Re-enter the PIN.
5. Enter the user role.
   See “Roles” section below (Administrator and Security Officers only can modify this field.
6. Enter email address.
   Currently used as user identifier
7. Press “Save”.
8. User is updated.

Update MFA User (Remove Authentication Method)

An MFA (Multi-Factor Authentication) user is required to use both login methods (password and smart card). (Please see Enable 2-factor authentication on settings configuration page).

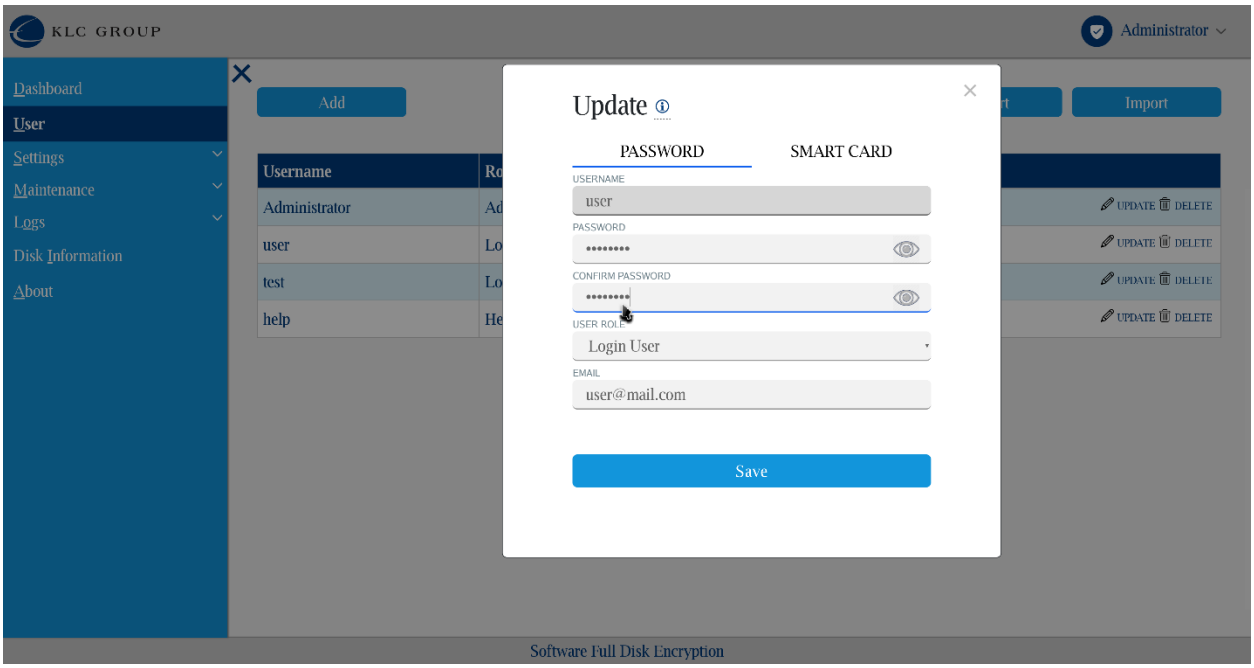
For example, in the image below you can see we have added MFA users named ‘user and ’test’ (in auth type column there are 2 icons for these users).

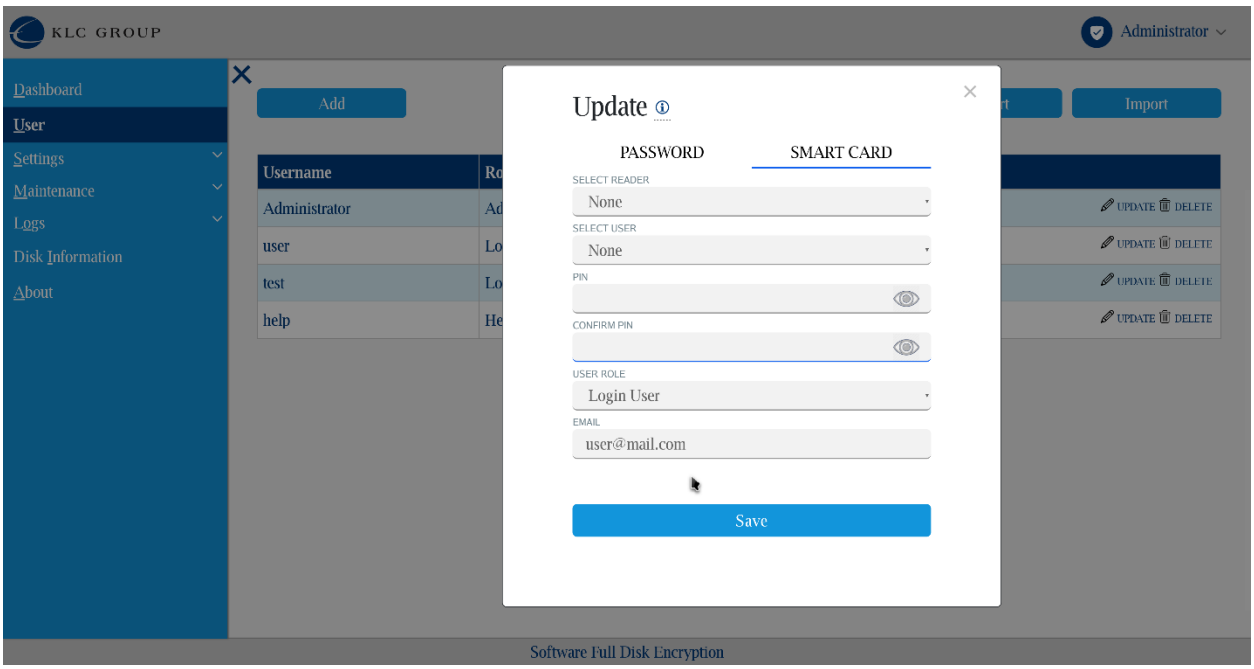


Now, suppose we need/want to remove an authentication method…

Remove Smart Card Method

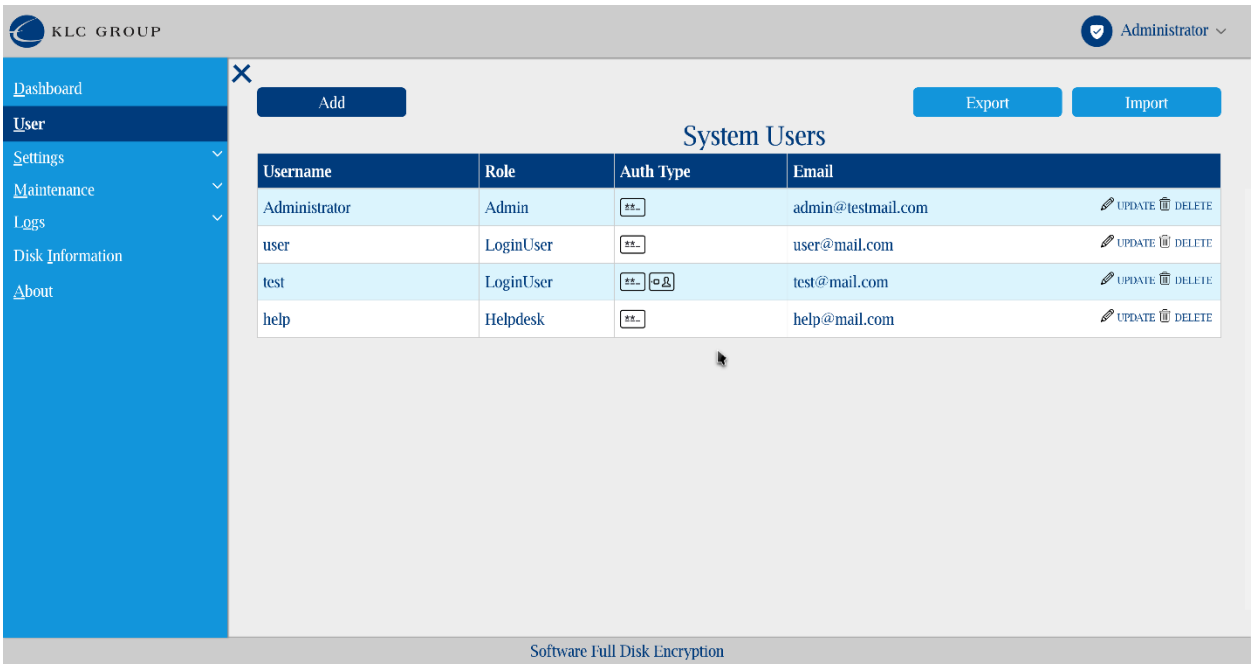
Your update user screens should look similar to this (click ‘Update’ next to ‘user’ user):





In short, we need to remove all information on the SMART CARD tab. It is important to set Select SC reader to None and leave PIN (and confirm PIN) to blank (no PIN)). After this go to the PASSWORD tab, fill in all information and select ‘Save’.

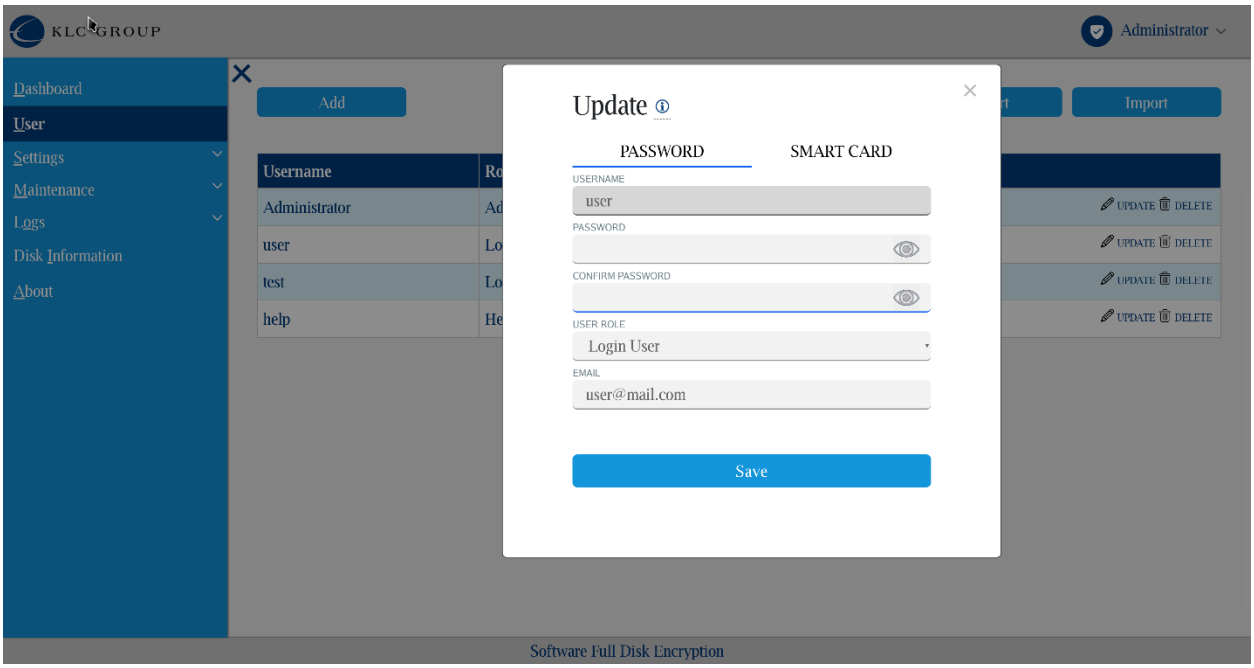
The following figure shows the result after following the process (no smart card icon on Authentication Type of user ‘user’):

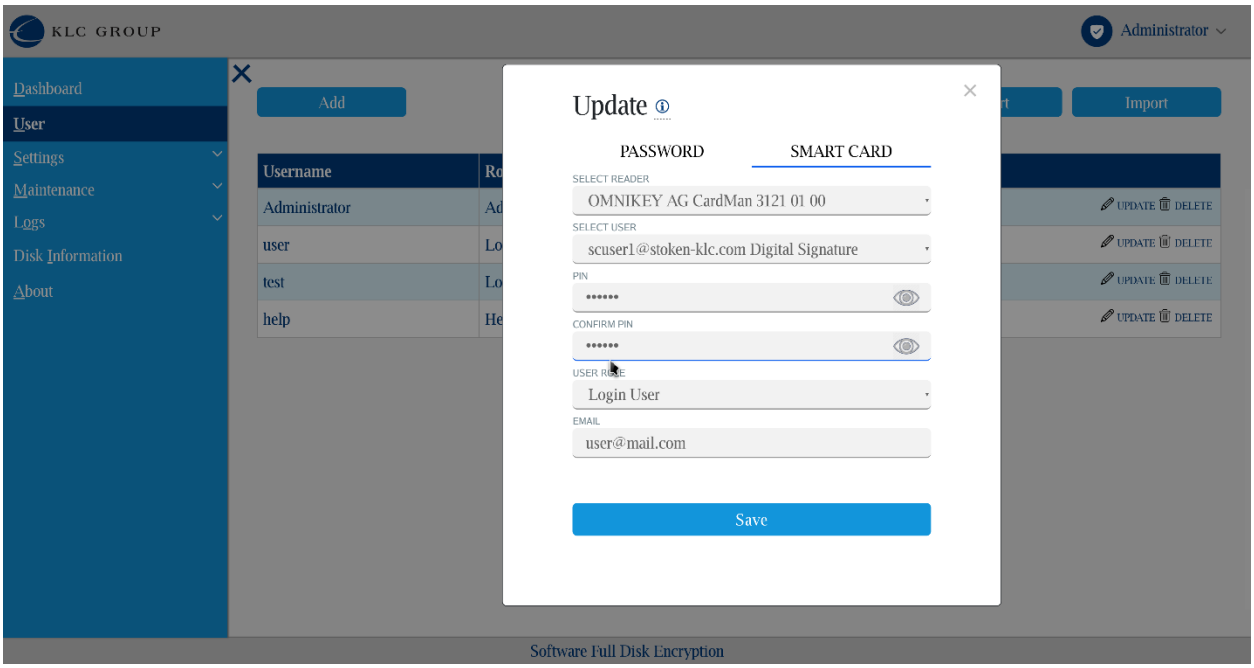


Remove Password Method

Note: Smart card-only is not part of the Common Criteria Evaluated Configuration

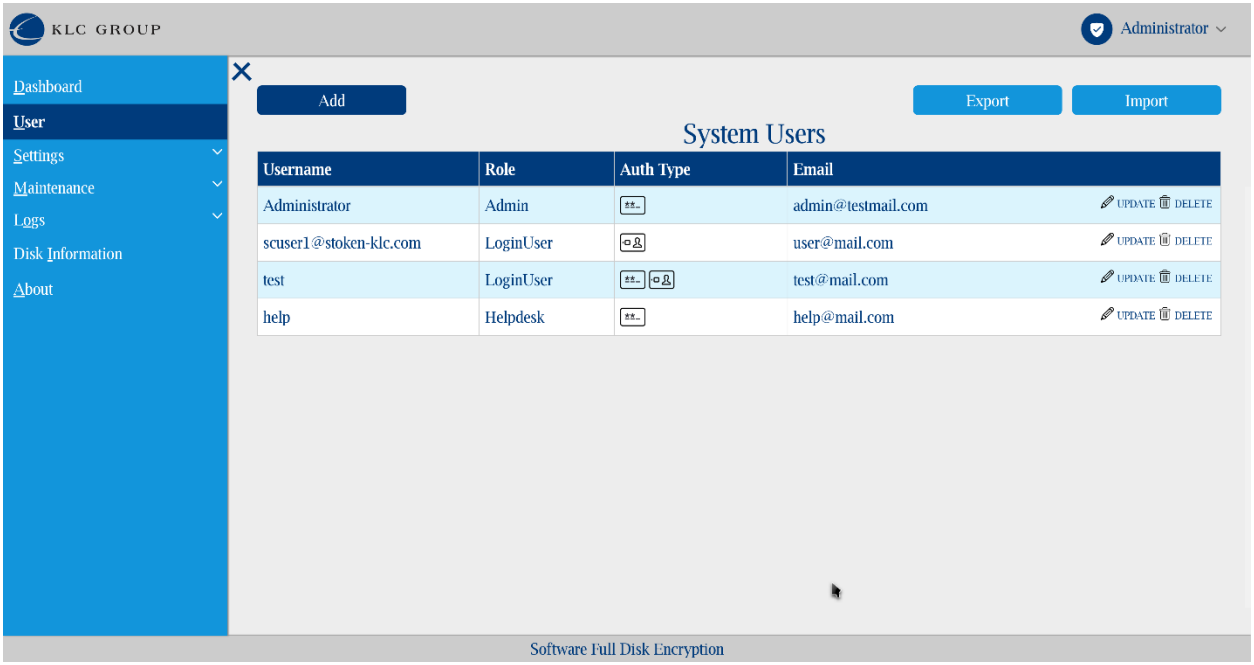
Your update user screens should be similar to this (click “Update’ next to ‘user’ user):





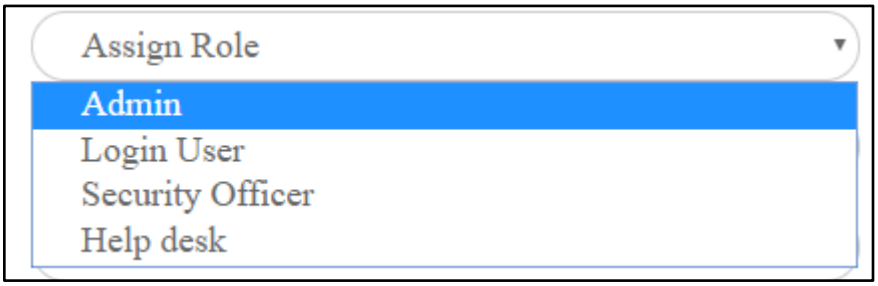
In this case, all information on the SMART CARD tab should be filled, and password/confirm password fields should be left blank on the PASSWORD tab. Click ‘Save’ on the SMART CARD tab to save the settings.

Here is the result:



Please note that 'user' is now named after smart cards certificate used (scuser1@stoken-klc.com) because PW method is removed. There is no PW icon on Authentication Type.

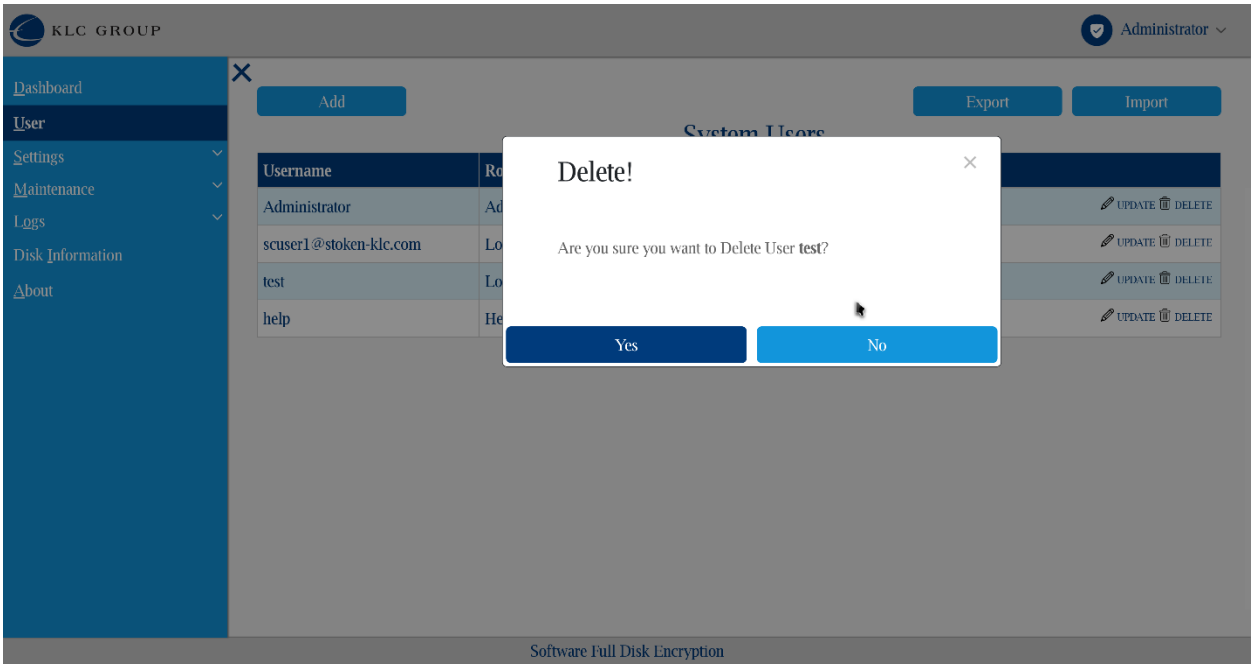
User Roles



Admin: Enables administration of users and features, except for deleting logs and control to Recovery options.
Security Officer: This role allows the user to delete logs, to update/delete users (but not add/import them). It also allows control to Recovery options (to enable/disable backup database and export configuration and users). Based on setting (controlled by Administrator role), the Security Officer can be allowed or denied rights to login into host OS.

Login User: This role allows login to the system and console access for the user.
Help Desk: This role allows editing passwords for other login and help desk users only. The Help desk user role also participates in user-forgot-password recovery assistance and to allow for updating a smart card for a user. Help desk users do not have rights to login into host OS.

Delete User



Clicking the User tab displays the list of system users. To the right of a username of a user there is a ‘Delete’ option. Click on it to bring up the Delete user popup window . Select ‘Yes’ (to delete) or ‘No’ (to just exit without deletion).

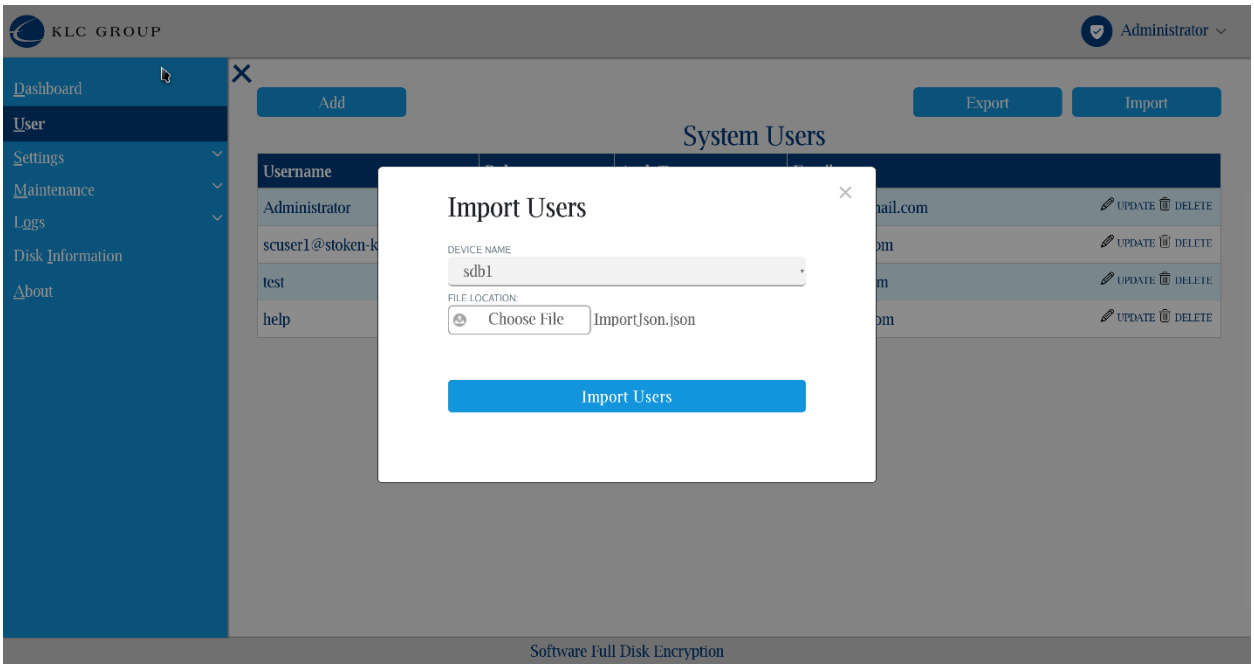
Import Users

“Import users” is a rapid way of adding a group of users to a number of not network connected systems without having to manually add them one by one on each system (using a user import file).

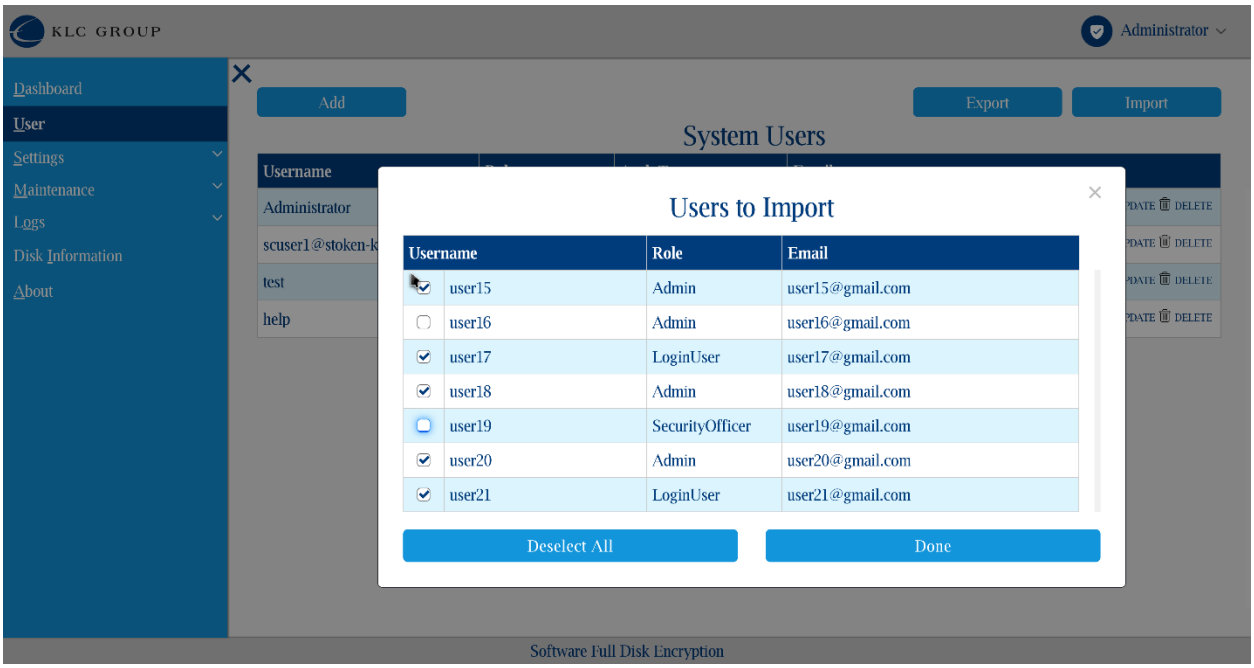
To import users, see example below:

With User tab selected click Import Users button to add a list of users to CDO Kryptr all at once.

1. In the Import Users 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/ Choose file'
3. Click on the “Import Users” button.

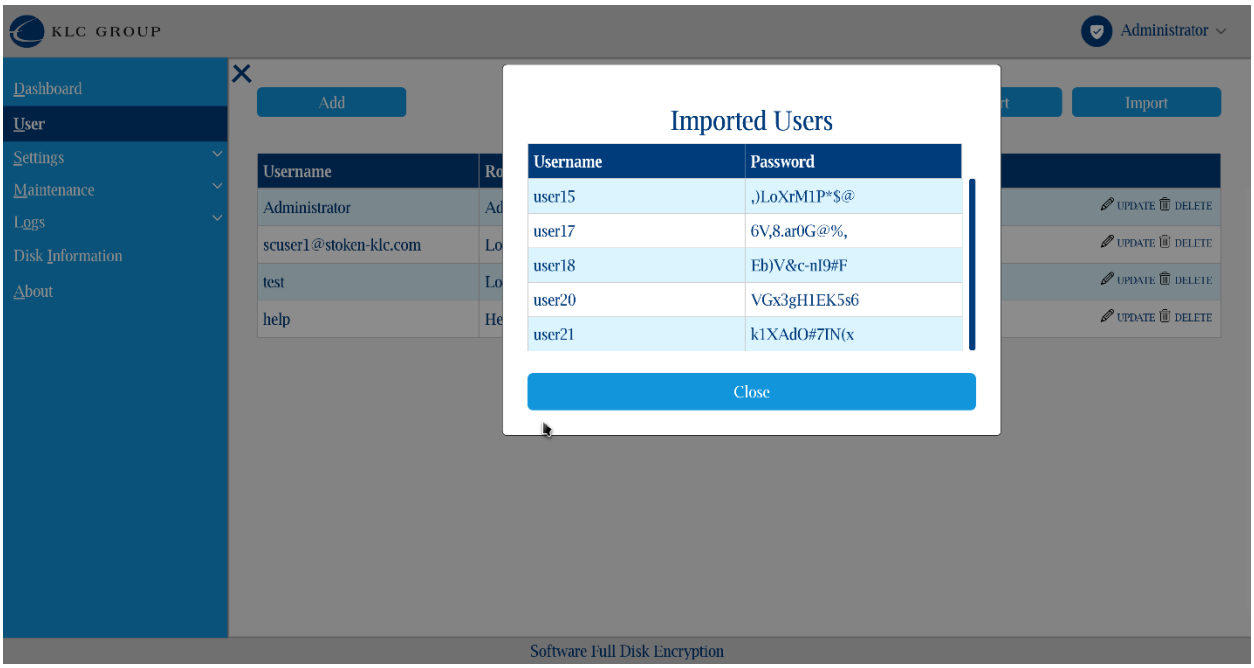


You can select which users contained in the import file to be added:



An import file is to be a JSON formatted text file. The contents of a sample import file is shown below. The sample JSON import file may be edited and copied to a USB thumb drive for selection from the Import Users dialog and thus importing specified users.

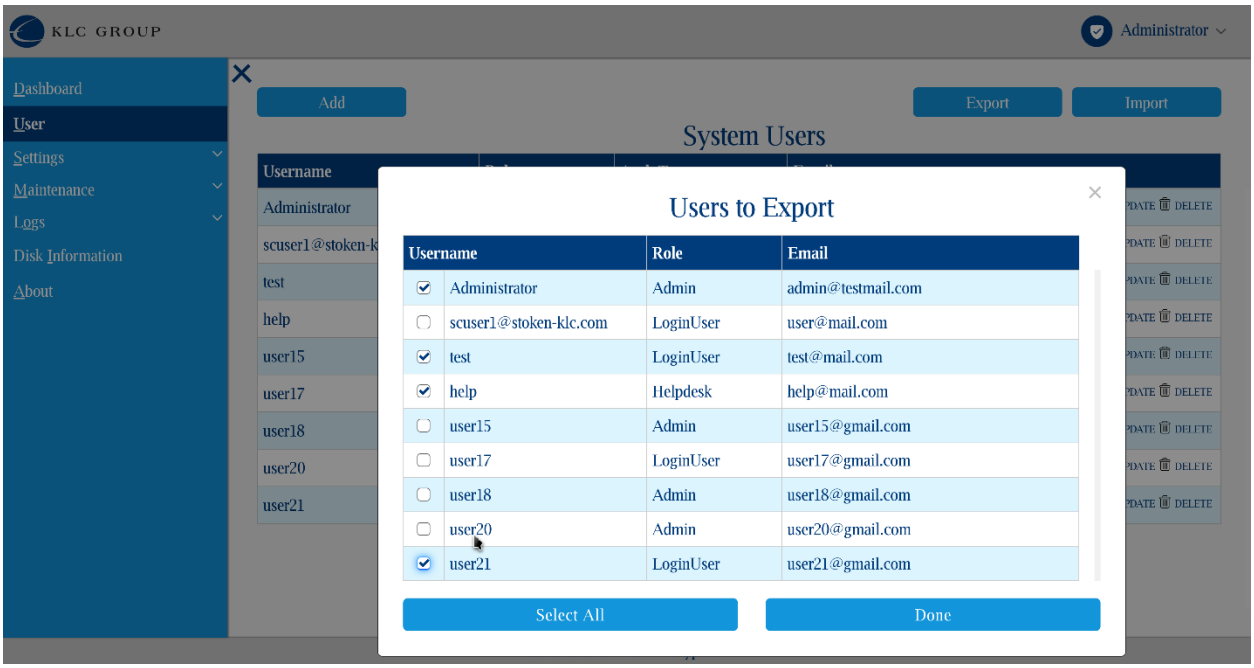
"{'Data':[{ 'UserName': 'Bob', 'Role': 'Admin', 'Email': 'bob@test.com' }, { 'UserName': 'Alice', 'Role': 'LoginUser', 'Email': 'alice@test.com' }, { 'UserName': 'Hobbs', 'Role': 'SecurityOfficer', 'Email': 'hobbs@test.com' }, { 'UserName': 'Steve', 'Role': 'Helpdesk', 'Email': 'steve@test.com' }]}"

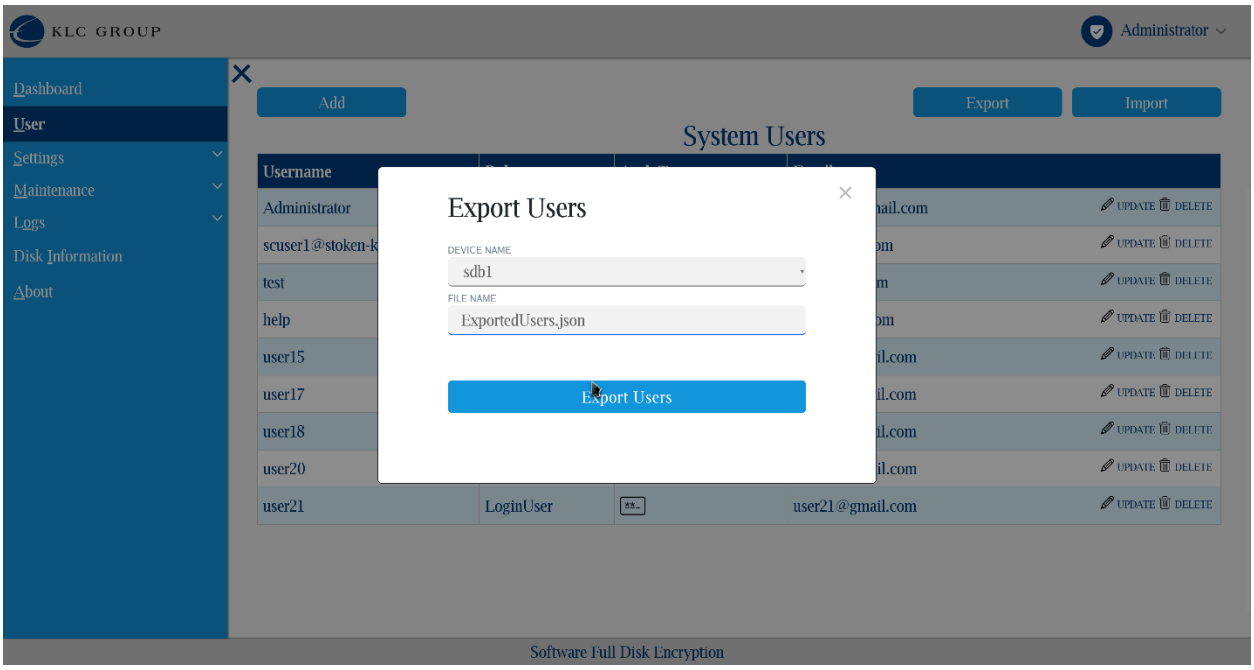


Another way of adding users is to fully configure a ‘template’ system with a set of users with their valid credentials and then exporting an encrypted copy of the database that can then be imported in other computers. See Export Configuration section.

Export Users

If you wish, you can export users – which means they will be output and stored in a JSON formatted file like the one used for importing users. In that way users can be imported on the same or other system. You can select which users to include in export file. The user passwords will naturally not be exported to the .json file. Instead, there will be a default PW that can be set during export and users will be required to change the PW at first logon.

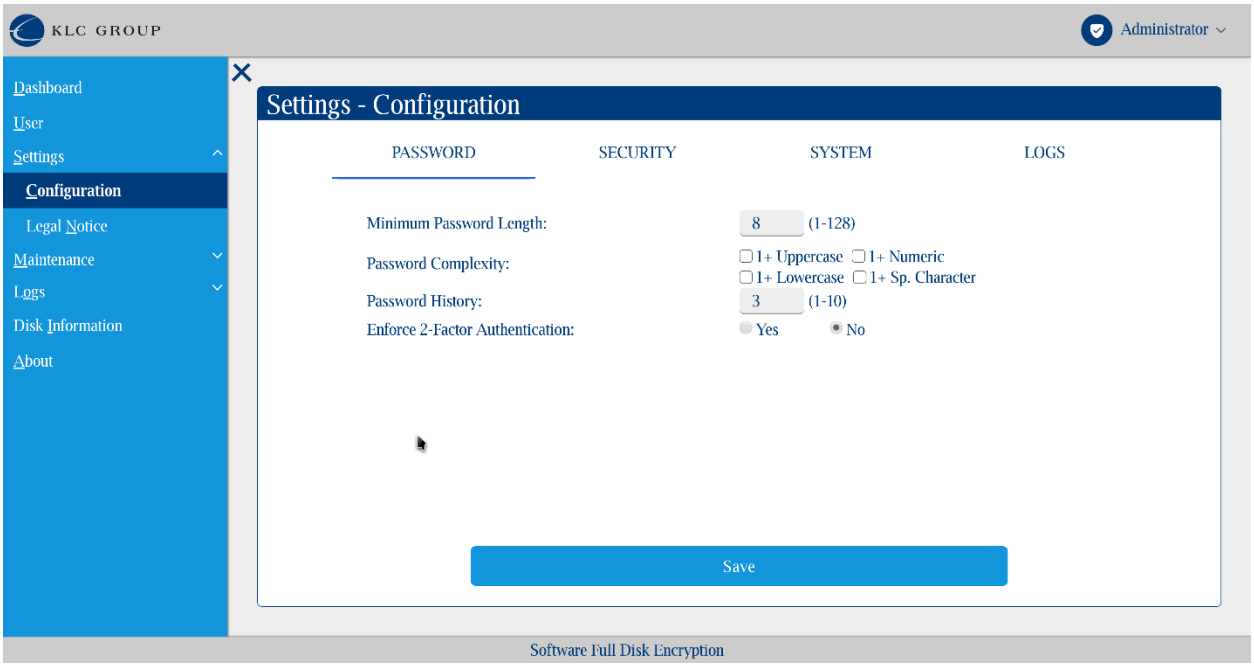

KLC GROUP
Administrator
Dashboard
User
Settings
Maintenance
Logs
Disk Information
About
Add
Export
Import
System Users
Username
Administrator
scuser1@stoken-k
test
help
user15
user17
user18
user20
user21
Users to Export
Username
Role
Email
Administrator
Admin
admin@testmail.com
scuser1@stoken-klc.com
LoginUser
user@mail.com
test
LoginUser
test@mail.com
help
Helpdesk
help@mail.com
user15
Admin
user15@gmail.com
user17
LoginUser
user17@gmail.com
user18
Admin
user18@gmail.com
user20
Admin
user20@gmail.com
user21
LoginUser
user21@gmail.com
Select All
Done


KLC GROUP
Administrator
Dashboard
User
Settings
Maintenance
Logs
Disk Information
About
Add
Export
Import
System Users
Username
Administrator
scuser1@stoken-k
test
help
user15
user17
user18
user20
user21
LoginUser
user21@gmail.com
Export Users
DEVICE NAME
sdb1
FILE NAME
ExportedUsers.json
Export Users
Software Full Disk Encryption

Settings Configuration for Administrator and Security Officer Users

There are number of settings configurable using the Settings-Configuration dialog. In this section we will be describing them.

Password tab:



Minimum Password Length:
This field defines minimum password length and affects creating new users as well as updating password of an existing user.

Password Complexity Fields:
These fields define the enforced user password complexity. 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 as part of a password, then checkmark the “Min one Numeric” box. To enable a special character then checkmark the “Min one special character” box. You can enable more than one checkbox to suit your PW complexity configuration needs.

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.

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

When this button is set to 'Yes' you have enabled "enforcing multifactor user authentication" which in short requires users to use both smart card (and its PIN) and their password to log on.

If this button is set to 'No', single factor login is allowed by using either password or smart card (if SC is registered for the user).

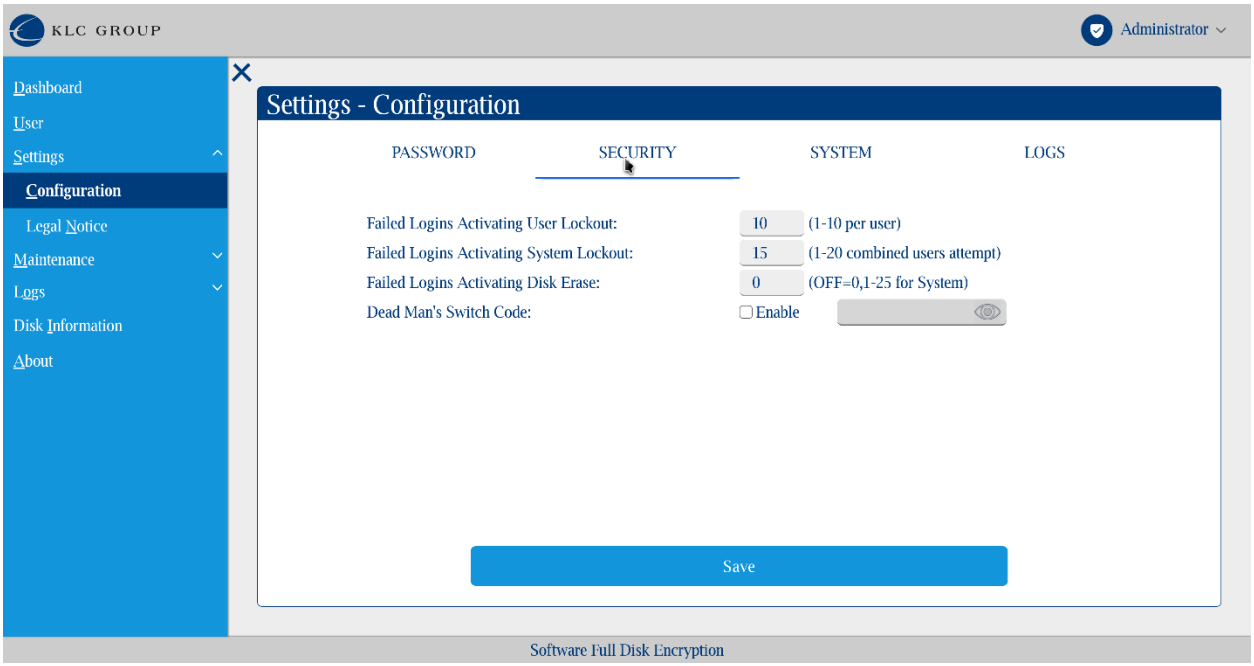
Note: Smart card only is not part of the Common Criteria Evaluated Configuration

Enforce 2FA for the built-in Administrator: When this check is enabled Administrator will need to enroll a SC certificate when logging into console/Host OS

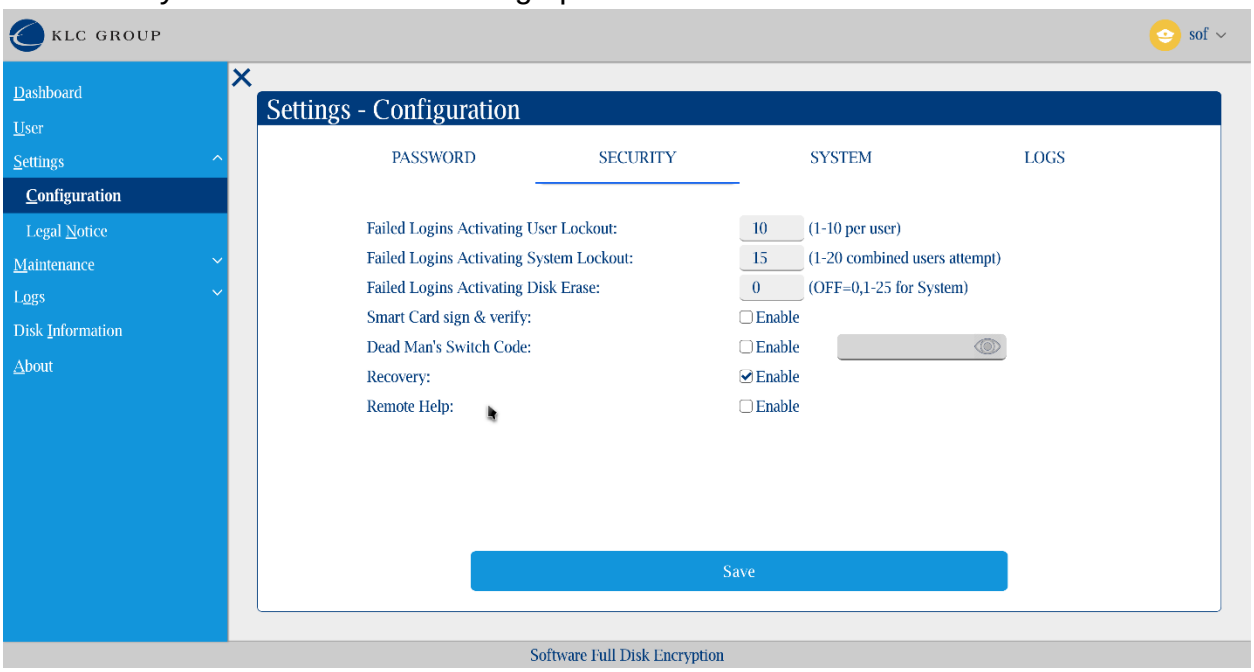
Note: This checkbox is editable only if Enforce 2-Factot Authentication is set to 'Yes'

Security tab:

For Administrator role the following options are available:



For Security Offices role the following options are available:



Failed Logins Activating User Lockout (1-10 per user):

When this number of consecutive failed logins is reached by a user, this user is locked out and cannot log into CDO Kryptr (even with correct credentials) until a reboot of the system occurs. Other users can log into CDO Kryptr with correct credentials. A system reboot resets failed logins activating user lockout counter for the locked user.

Failed Logins Activating System Lockout (1-20 per system):
When this number of consecutive failed login attempts is reached, further login will be disabled until a reboot of the system occurs. This is a system wide setting counting and accumulating consecutive failed attempts even if the failed attempts occur for different user accounts (user names). Rebooting resets the counter.

Failed Logins Activating Disk Erase (OFF=0,1-25 for system):

When enabled 1 through 25 (default is 0 = disabled) and the configured number of consecutive failed login attempts is reached (failing attempts made by all users combined), the CipherDriveOne Kryptr will “self-destruct” by destroying all cryptographic keys, effectively rendering the disks as erased. **Please note** that there is no recovery possible after Disk Erase is acted upon. If this feature is used/enabled we recommend setting the counter/number to 10 (or higher) to avoid an unintentional disk erase. A value of 0 indicates disabled status for this counter.

As mentioned above, the disk erase setting is disabled by default. If enabled, this feature is system wide (counting failed attempts for any and all users). A successful logon (for any user name) resets the counter.

Dead Man’s Switch:
The Dead Man’s Switch is intended to be used in an emergency situation. For example, in a dire situation where a user is being compelled unwillingly, perhaps under physical threat, to logon while sitting at the keyboard. Using the Dead Man’s Switch erases all cryptographic keys thus making it impossible to unlock the disk. Data will be lost permanently.

Dead Man Switch Code:
When the Dead Man's Switch is enabled, the Security Officer or Administrator can set up the dead-man-switch code (PW) that can be used to authorize the disabling of access to the protected OS.

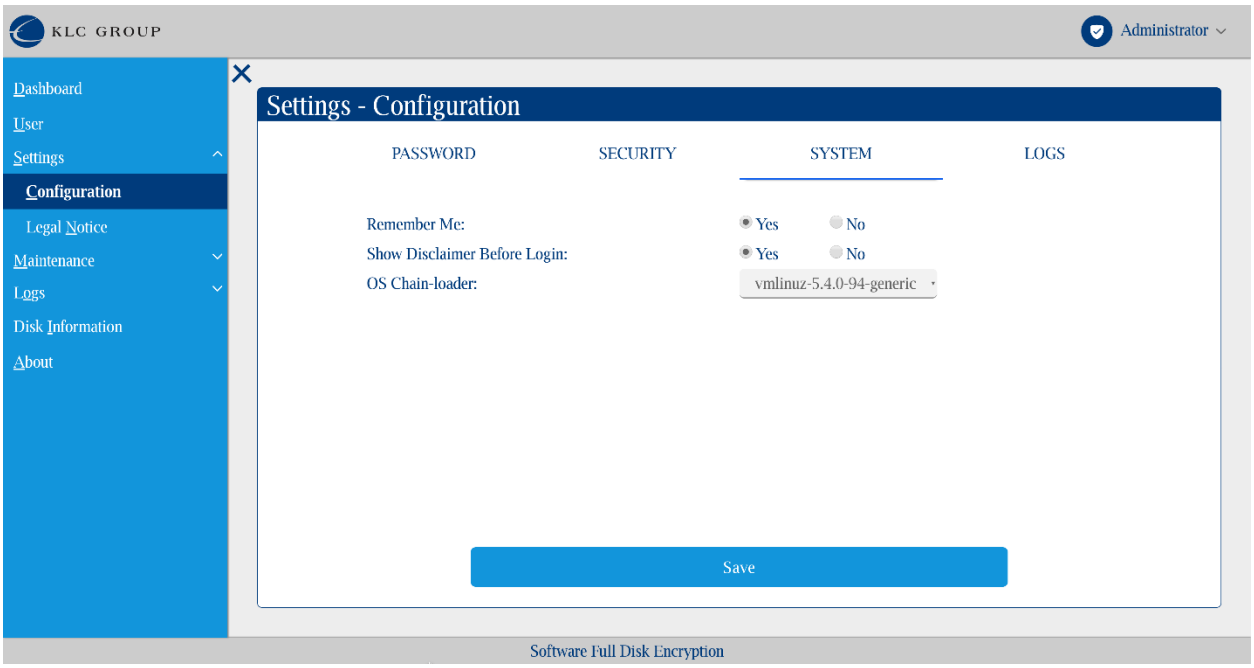
Dead Man's Switch Operation:
To carry out this operation, at the logon screen, enter the login user's username and password. In the password field, after entering the user's password, don't press enter/logon, instead continue by entering the Dead Man's Switch code directly following the user's password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

Smart Card Sign&Verify (visible to Security officer users only):
This feature is provided as an alternative smart card authentication method. There are certificates where Encrypt/Decrypt is not allowed. For example, the certificates with key usage "Certificate sign" and/or "CRL Sign". To use such certificates the "Security Officer" should enable "Smart Card Sign&Verify" option in configuration page. When this is enabled the certificate key is used for Sign&Verify sensitive data. Otherwise the certificate key is used for Encrypt&Decrypt sensitive data.

Recovery (visible to Security officer users only):
This switch (checkbox) is available to the Security Officer role only (i.e. controlled by the Security Officer). 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.

Remote Help (visible to Security Officer users only):
This setting is available to Security officer users only. When the box is checked Remote Help is enabled. Remote Help sections are added in Admin/Help desk (Helper) user management consoles so that they can participate in PW recovery process of other users. Also, the 'Forgot Password?' link is enabled on CDO Kryptr login screen so users that forgot their PW can initiate the recovery process.

System tab:



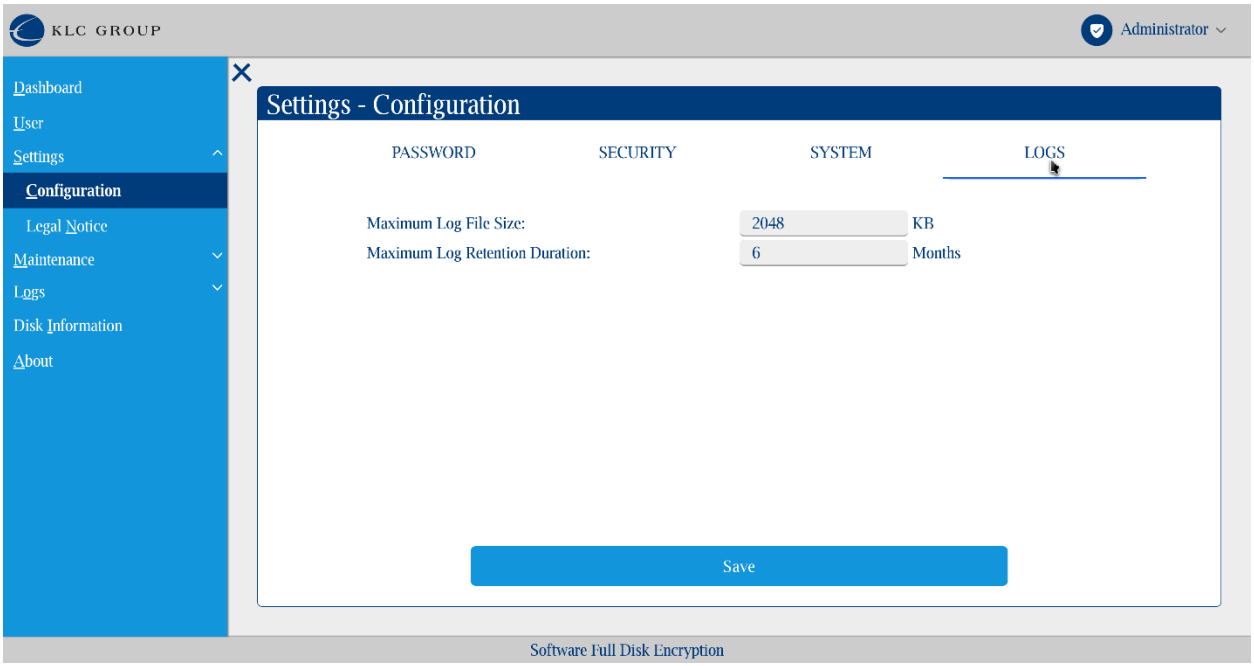
Show Remember Me:
If this setting is set to “Yes’ then the Remember Me option will be shown on the CDO Kryptr login screen. If a user logs into CDO Kryptr with this checkbox (“Remember Me’) marked as ‘Yes’ then on the next login their username/SC cert will be auto-filled and they need only provide password for login.

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

OS Chain-loader (visible on Linux host OS only):
This option is required to be enabled and configured for CDO Kryptr to boot the protected OS after user authentication for encrypted systems. Chain-loading is used to handover control from CDO Kryptr to the protected OS.

Here, the user can select which kernel to use for chain-loading from the available kernels in list.

Logs tab:



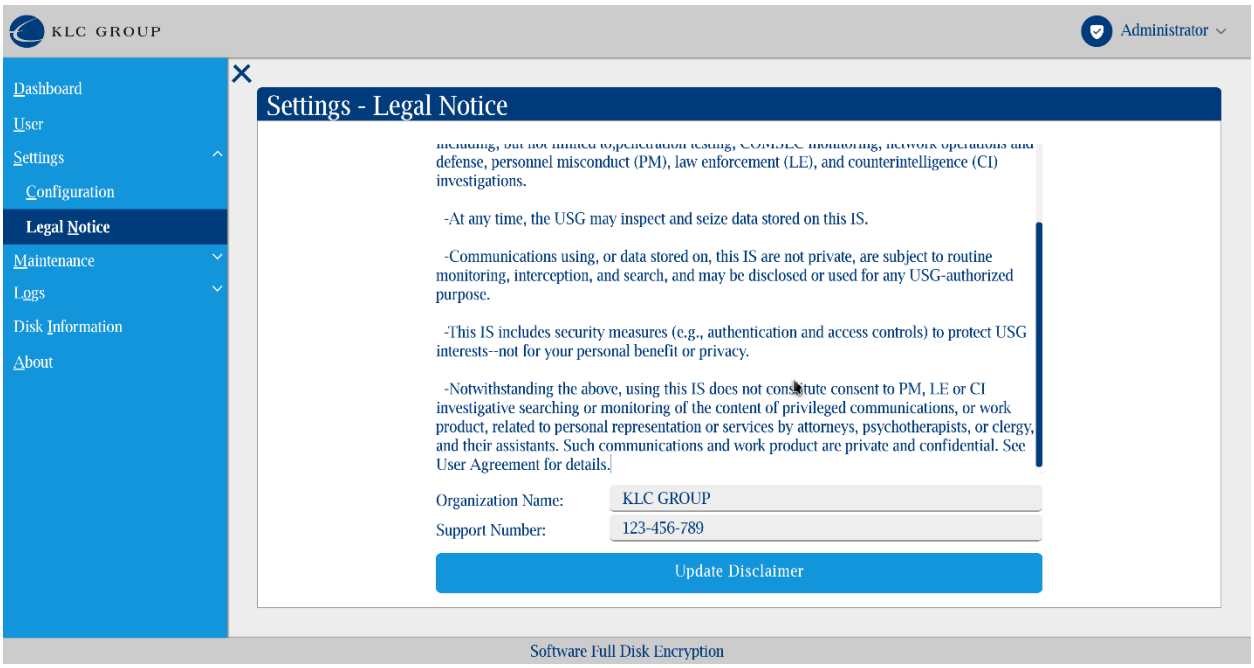
Maximum Log File Size specifies the maximum size the log file may grow after which older records will be automatically deleted.

Maximum Log Retention Duration specifies the maximum age log files will be kept before deletion.

The log data will be retained based on whichever condition occurs earlier.

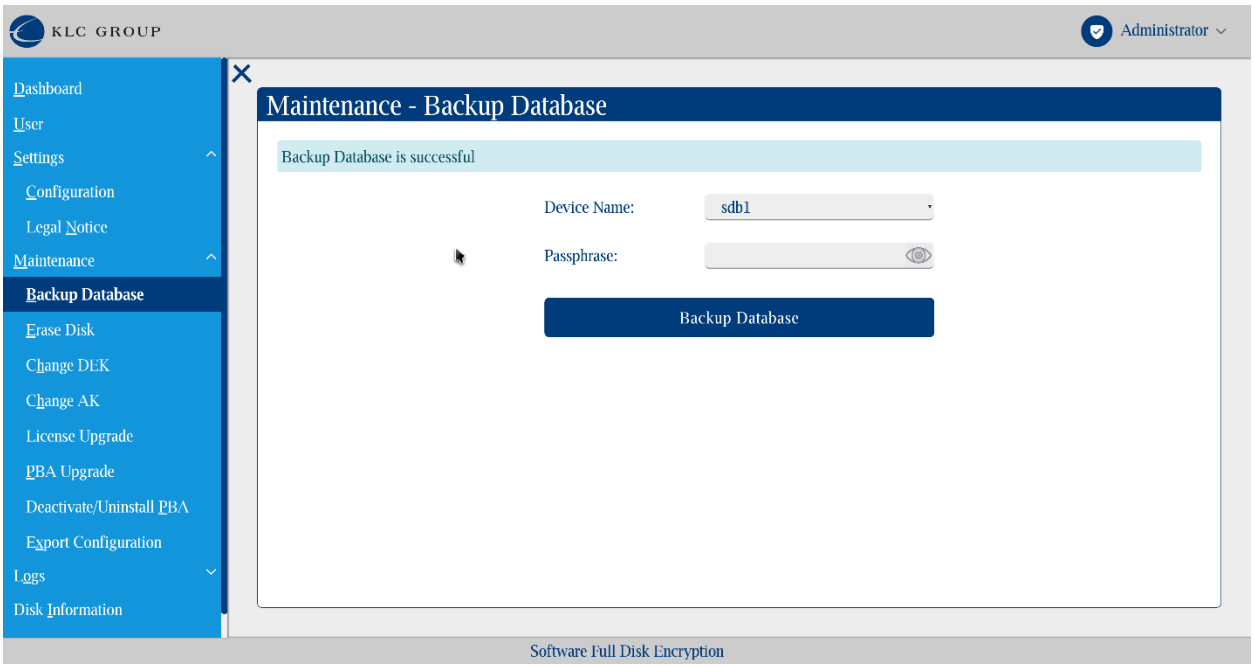
Legal Notice

On this screen a user can change values for the legal notice, organization name, and support number. Clicking ‘Update’ applies to specified settings.



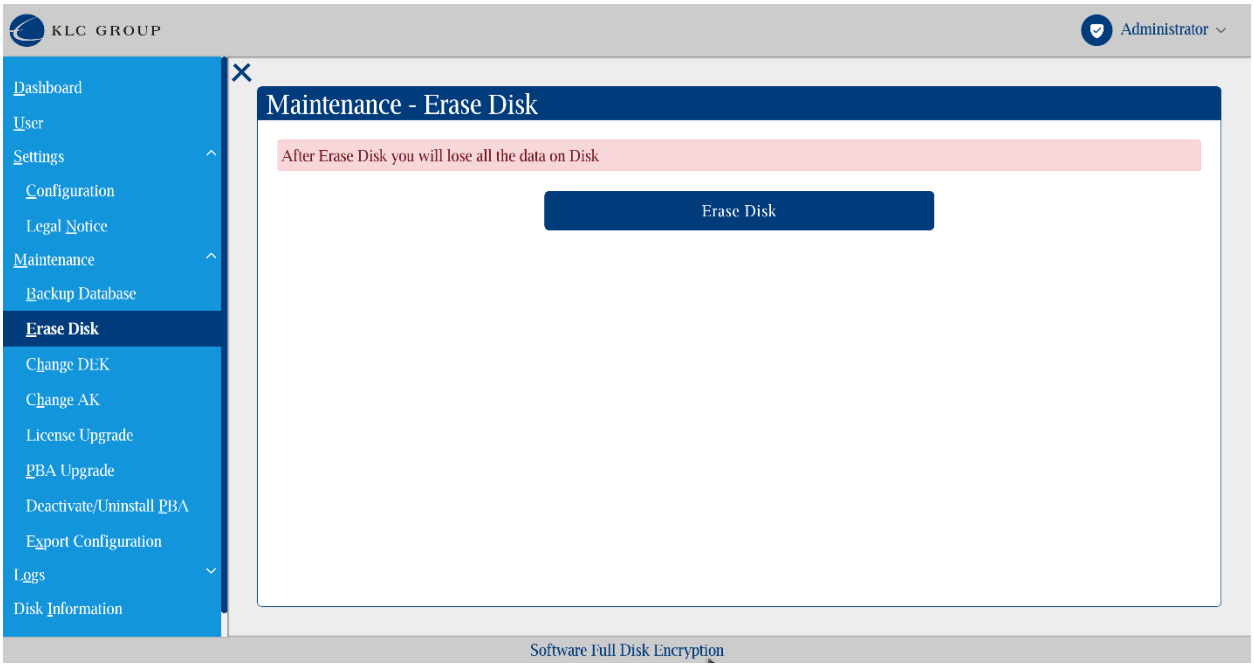
Maintenance

Backup Database



The Backup Database option allows a user to save a backup of the user database to a USB/external drive. The backup file is encrypted with a passphrase entered in the screen above and saved to a location specified in ‘Device name’. The backup file is named “PBADBbackup”.

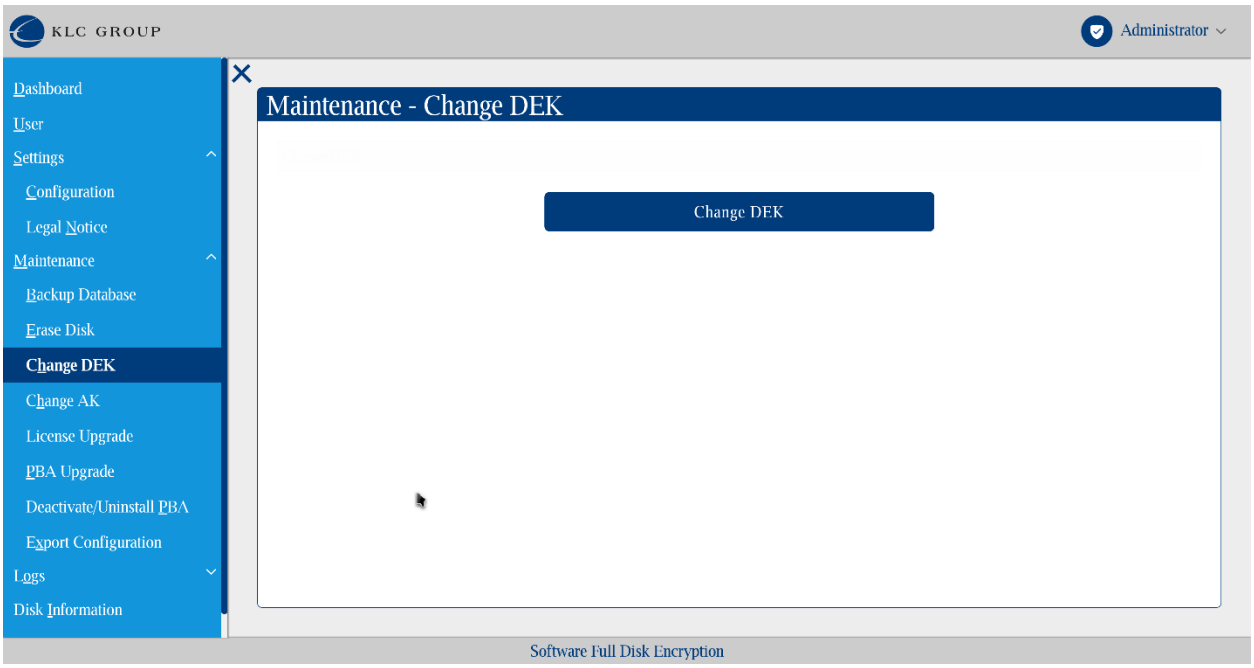
Erase Disk



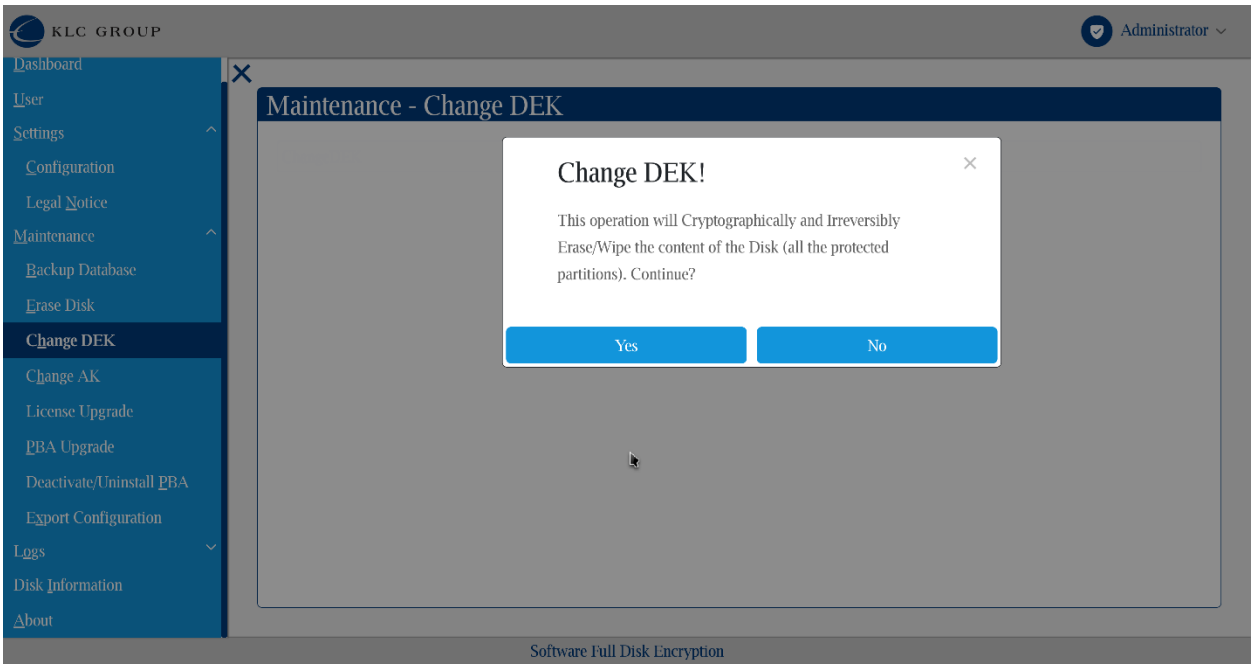
The Erase Disk feature cryptographically erases all protected contents/data on the disk. After clicking ‘Erase Disk’ a confirmation dialog appears asking the user if they really want to erase the disk followed by a dialog to confirm your Administrator/Security officer role user credentials.

Note: This is an irreversible operation which cryptographically erases all protected data on the disk. The disk will have to be set up again after it is erased.

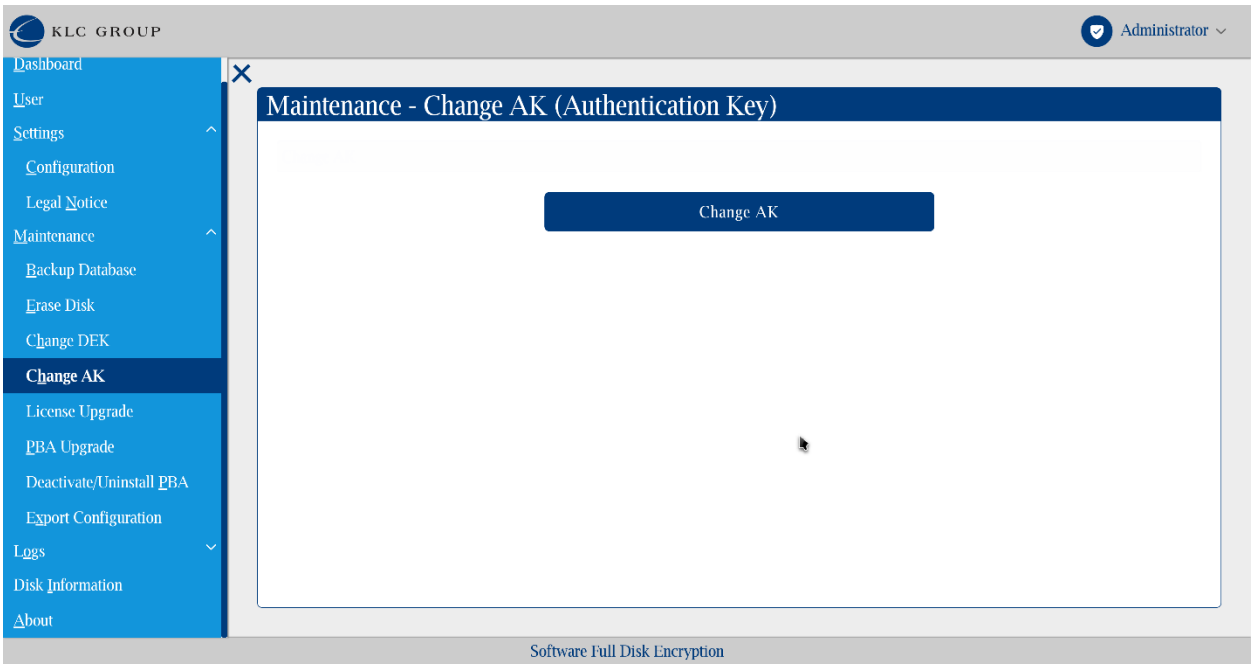
Change DEK (Disk Encryption Key)



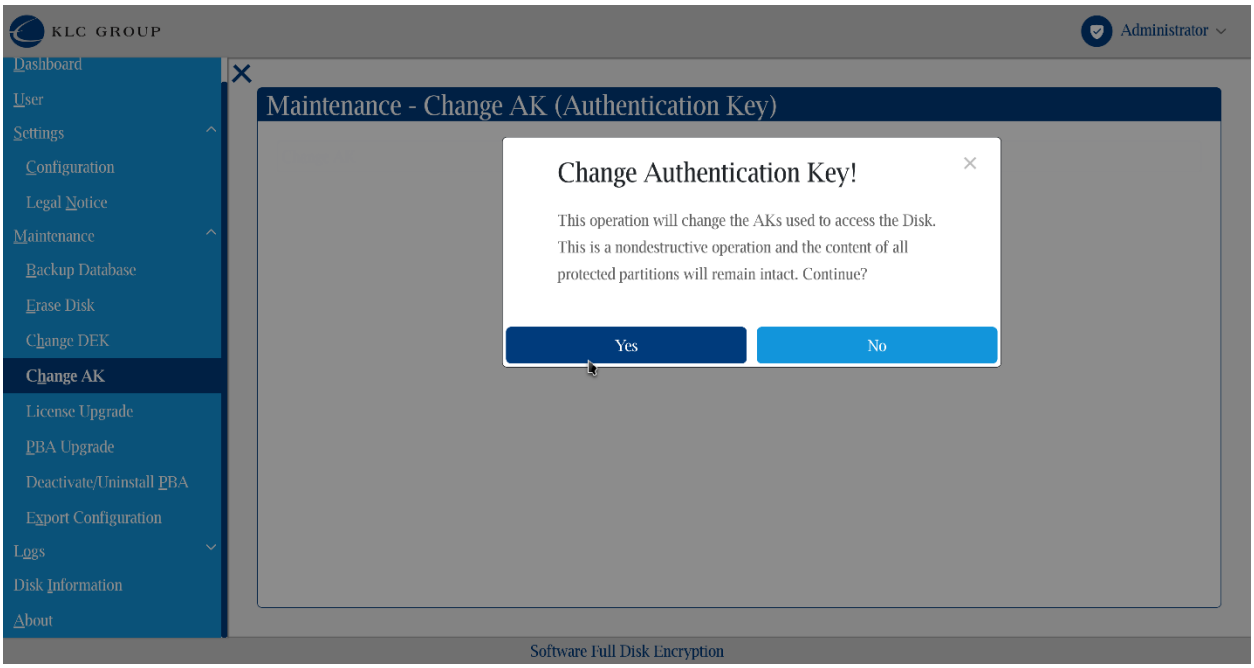
When the Security officer wants to change the DEK, the ‘Change DEK’ option is used. The DEK is the actual key used to encrypt the data on the disk of the protected OS. When this option is used, a new DEK is generated and the disk will be re-encrypted with the new DEK. This operation will take time to complete as the disk is first decrypted and then fully re-encrypted with the new DEK.



Change AK (Authentication key)



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



CDO Kryptr License

CDO Kryptr comes with a 45 day trial license that defers the need for entering a valid license key. During this time the product is fully featured in order to allow customers to “try-before-buy”.

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

After license expiry, the system will continue to protect the data but all admin functions including adding new users and changing of passwords will be disabled until a valid license key is entered. When a license is expired, user logon is delayed with 15 minutes at each logon to protected OS (displaying information regarding the expired license) to make the user aware of the expired license and the need to update.

Note: When the license has expired and a user chooses to log into a protected OS they have ability to log into the Management Console or select ‘Power Off’ during these 15 minutes with which login to the protected OS is delayed.

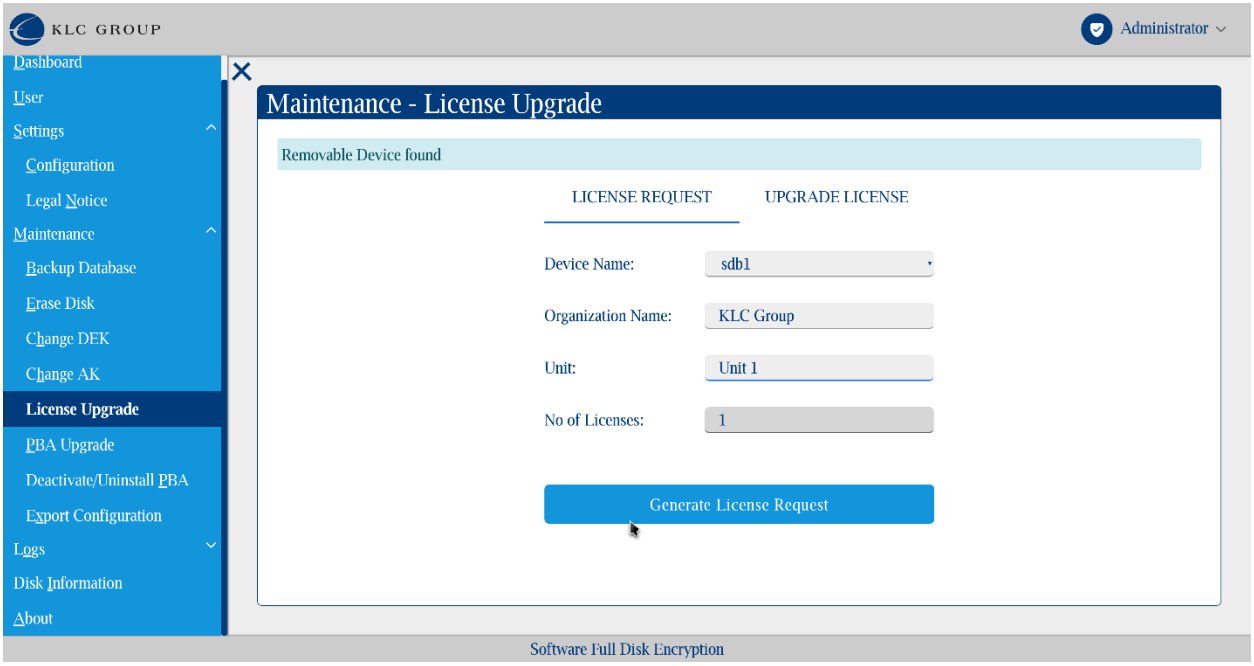
Generate License Request and Import/Upgrade License

Licensing is most frequently performed as part of installation but if the system is installed with a trial license, then the system can later be updated with a purchased license.

Licensing consists of two operations.

First, the user will “generate a license request” that is unique to the computer where CDO Kryptr is installed. This license string can be exported to a network folder for automatic processing (by a licensing agent on the network) or manually by providing the license request file to an administrator who will process the file and send back a file with an “activation key (file)” or a custom License file. To remove the 45 days trial period restriction and make the product fully featured, the user will need to import a key file using the “License Upgrade” console dialog.

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

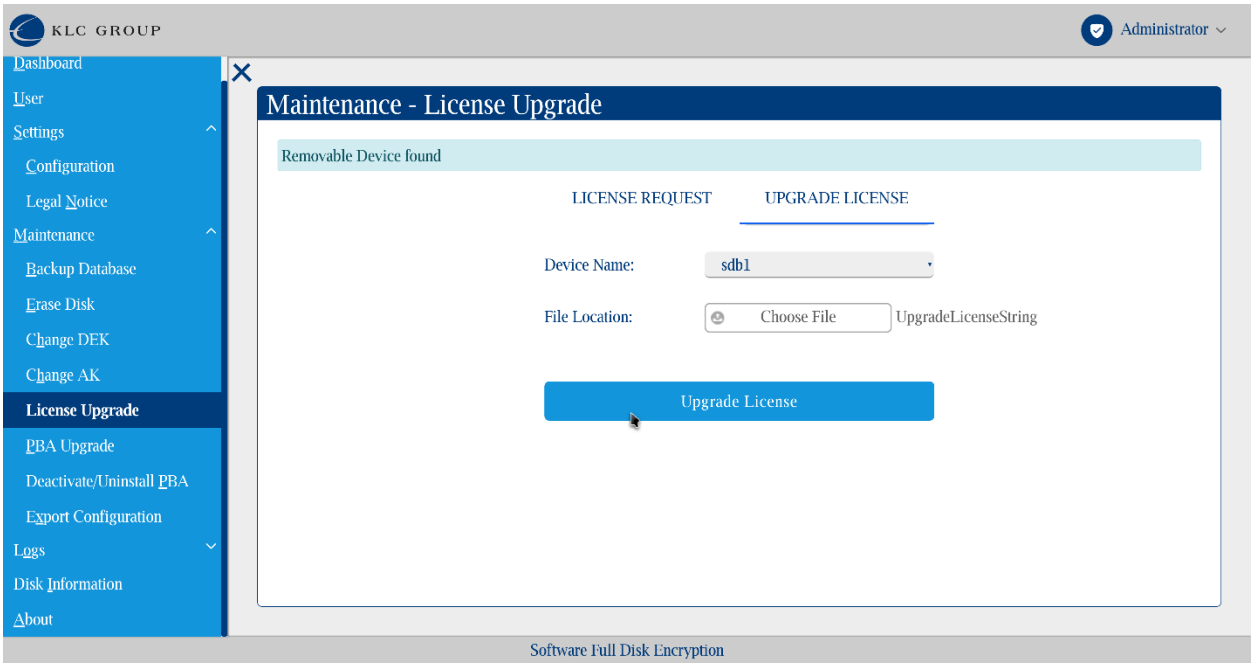


Generate a License Request File

For the **Device Name** field, choose the device/drive where you will store the license request file.
In the **Organization Name** field, enter your organization's name.
In the **Unit** field, enter the organizational unit or department (if applicable).
In **the No of Licenses** field, enter the number of licenses (Currently, only 1 by default).

Click on the **Generate License Request** button to generate a license request string file at the selected location (e.g. USB thumb drive) and send this file to your administrator, or if you are the administrator, send the file to CDO Kryptr support for use in generating the license.

Upgrade License



- In **the Device Name** field, choose a device name where the upgrade license file can be found.
- Select the license file received from the Administrator.
- Click on **Upgrade License** button**.**

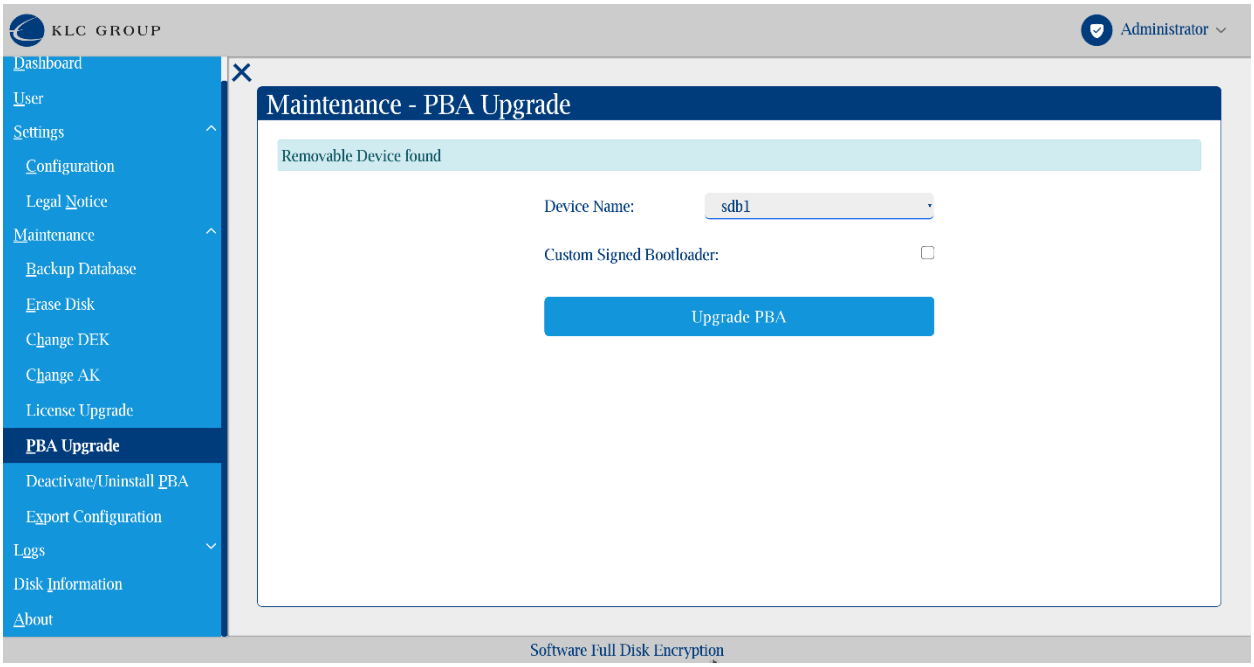
Please note that the license file data also determines the key size used for encryption/decryption of data. (Default is AES 256bit key size if no special request is made).

CDO Kryptr Upgrade

There are two methods to upgrade CDO Kryptr:

1. Management Console GUI - select the upgrade option
2. Via command line interface (CLI)

CDO Kryptr Upgrade via GUI



- CDO Kryptr image file should be copied to the root location of a removable USB thumb drive (PBA.img.gz) together with SecurityToken file.
- For CDO Kryptr upgrade, please select the USB thumb drive (with PBA image).
- Click on Upgrade PBA.
- After the upgrade is successful, the system will power-off.

- Note: For Custom Signed Upgrade from UI:
  Download and copy the PBA_custom.img.gz and SecurityTokenCustom file to the root folder of the USB thumb drive.

Check ‘Custom Signed Bootloader’.
Click on Upgrade PBA.

CDO Kryptr Upgrade via CLI

- Install CDO Kryptr build which you want to be upgraded afterwards
- Copy the upgrade files PBA.img.gz and SecurityToken to the USB thumb drive root having the CDO Kryptr installer files
- Boot to the USB thumb drive
- On the command line execute the following command to upgrade the PBA:

  sh install-fde.sh -d /dev/sda -p <password> or
  sh install-fde.sh -d /dev/nvme0n1 -p <password>

Here, the password is for the default Administrator user

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

```
Loading CipherDriveOne Kryptr. Please wait...

Please press Enter to activate this console.
/bin/sh: can't access tty; job control turned off
/ # sh install-fde.sh -d /dev/sda -p Admin456
Installing CipherDriveOne Kryptr on /dev/sda ...
/*****************************************/
CipherDriveOne Kryptr Installer version: 1.1.0, build: 8, time UTC:Sep 21 2023 12:05:55
The Default License File 'EvaluationLicense_FDE' was found on a USB drive
Signed PBA image file is copied
License File is copied from the USB.
Old PBA partitions are found and the program will perform upgrade/activation.
Are you sure you want to continue (y/n)? y
Device Path : /dev/sda
Found 'CipherDriveOne Kryptr' in boot menu: 0007
Drive is already encrypted

PBA Activated Successfully.
Logs are collected to /dev/sdb1
/ # _
```

Note: If you want to upgrade with a custom signed Bootloader image, please make sure you have copied PBA_custom.img.gz and SecurityTokenCustom file to the root folder of the USB thumb drive.

Then boot to the USB thumb drive and use command:

sh install-fde.sh -d /dev/sda -p <password> -sb custom_signed or
sh install-fde.sh -d /dev/nvme0n1 -p <password> -sb custom_signed

If the above commands fails for not being able to update Secure Boot keys in the BIOS and still if you want to upgrade the PBA, the following command can be used:

sh install-fde.sh –d /dev/sda -p <password> -sbf custom_signed or
sh install-fde.sh -d /dev/nvme0n1 -p <password> -sb custom_signed

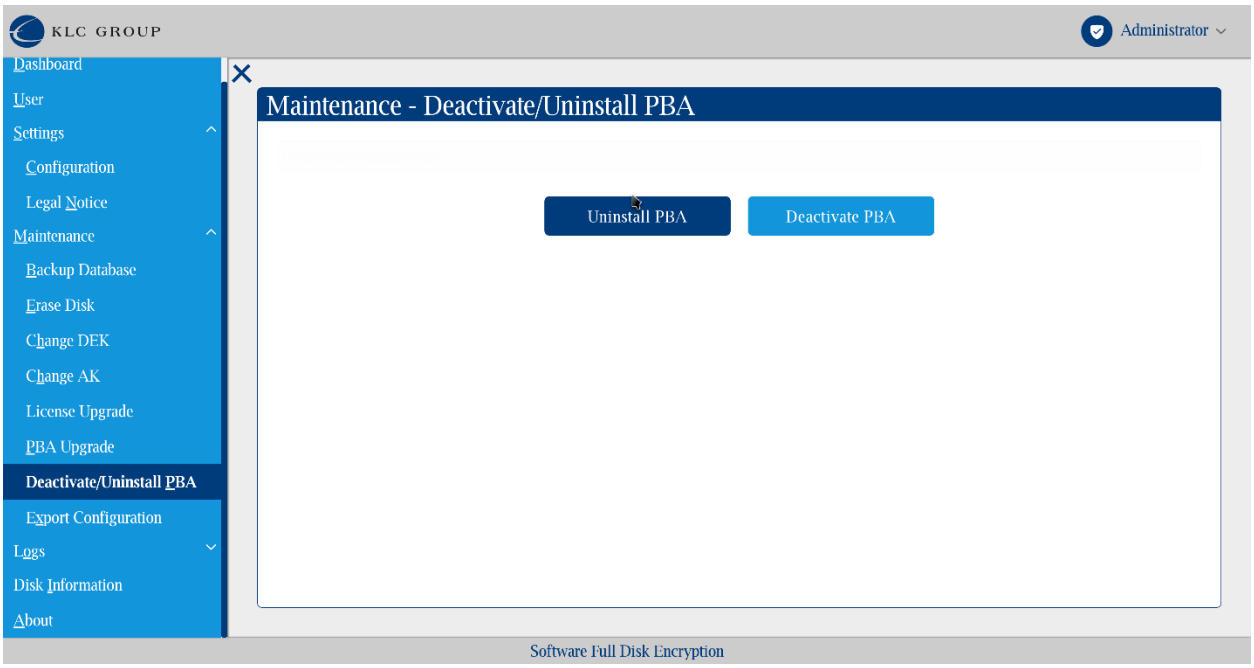
Deactivate/Uninstall CDO Kryptr

Deactivation: CDO Kryptr 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 CDO Kryptr can be re-activated again (settings and user database is kept intact).

Uninstall: In case there is a need to fully uninstall CDO Kryptr an administrator can use Uninstall to fully uninstall the product so all CDO Kryptr related files (binaries, settings and database) will be removed.

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 CDO Kryptr will be enabled again at next boot. See the “Reactivate” section below.

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



When clicking the ‘Uninstall PBA’ button, the CDO Kryptr will proceed with a confirmation dialog. Asking if you want to uninstall CDO Kryptr. followed by an authentication dialog to confirm your user credentials. After the uninstall process is started there is a progress bar informing the user about the ongoing uninstallation activity. Please note that the uninstall completely removes the database and a new empty database is created during a re-install. During uninstall there is a disk decryption process.

When the ‘Deactivate PBA’ button is clicked, the system will ask for confirmation, asking if you want to deactivate CDO Kryptr, followed by a dialog to confirm your user credentials and then proceed with the deactivation. After the deactivation process is started there is a progress bar informing user about the ongoing deactivation activity. During deactivation there is a disk decryption process.

Note: If you are logged on user other than the default Administrator account during deactivation of CDO Kryptr make sure you know the default administrator account’s password before proceeding as it is used during reactivation.

Note that for deactivation (temporarily disabling the product in order to work on the host) 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, the

installation program on the USB thumb drive is used. The installer program will check that the default administrator login credentials are valid for the database on the disk to accept reactivation.

Reactivation

In the case that the CDO Kryptr was deactivated (see Temporary Deactivation) e.g. in order to perform maintenance/debug on the host OS or any other situation requiring the temporary disabling of CDO Kryptr login then the follow procedure will reactivate CDO Kryptr 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.

CDO Kryptr can be reactivated (with the content of the CDO Kryptr database on the disk intact), by running the CDO Kryptr Installer again:

1. **Boot the system with prepared USB thumb drive containing the CDO Kryptr Installer.**
2. **Reactivate the CDO Kryptr by executing the following command:**

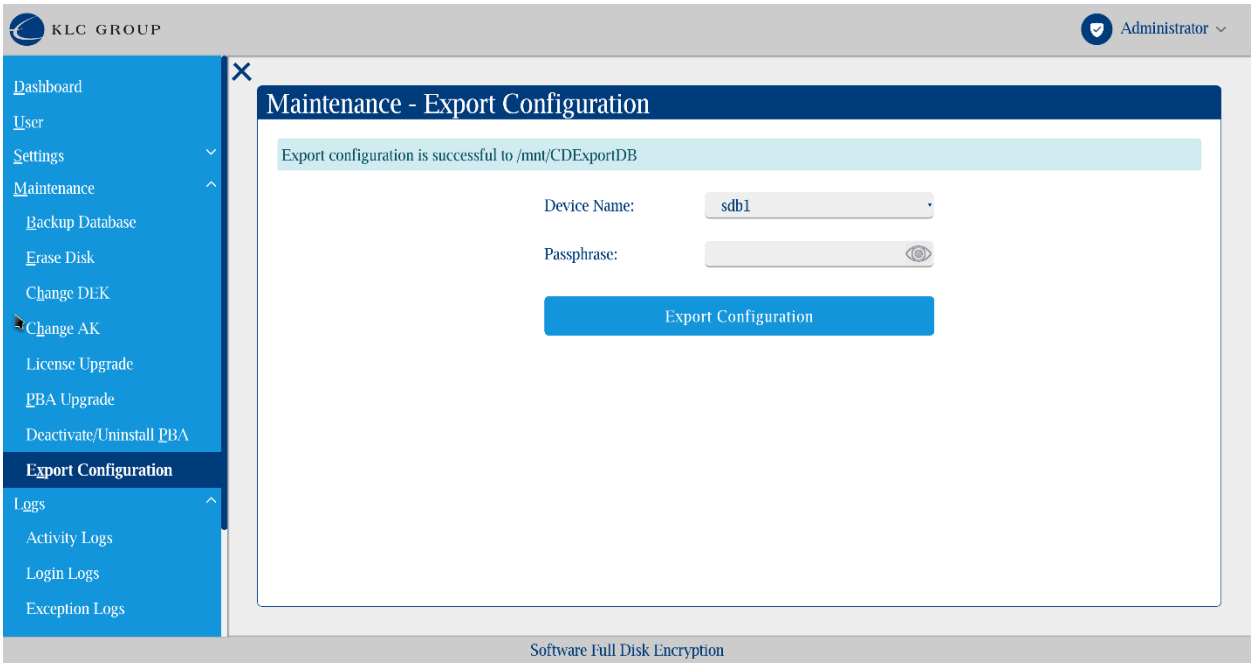
   sh install-fde.sh -d /dev/sda -p <password> or
   sh install-fde.sh -d /dev/nvme0n1 -p <password>

   Here, the password is for the default administrator user.

   Note: It is very important to remember the default administrator password. If this password is forgotten, reactivation is not possible.

```
Loading CipherDriveOne Kryptr. Please wait...

Please press Enter to activate this console.
/bin/sh: can't access tty; job control turned off
/ # sh install-fde.sh -d /dev/sda -p Admin456
Installing CipherDriveOne Kryptr on /dev/sda ...
/**********************************************/
CipherDriveOne Kryptr Installer version: 1.1.0, build: 8, time UTC:Sep 21 2023 12:05:55
The Default License File 'EvaluationLicense_FDE' was found on a USB drive
Signed PBA image file is copied
License File is copied from the USB.
Old PBA partitions are found and the program will perform upgrade/activation.
Are you sure you want to continue (y/n)? y
Device Path : /dev/sda
Found 'CipherDriveOne Kryptr' in boot menu: 0007
Drive is already encrypted

PBA Activated Successfully.
Logs are collected to /dev/sdb1
/ # _
```

Export Configuration



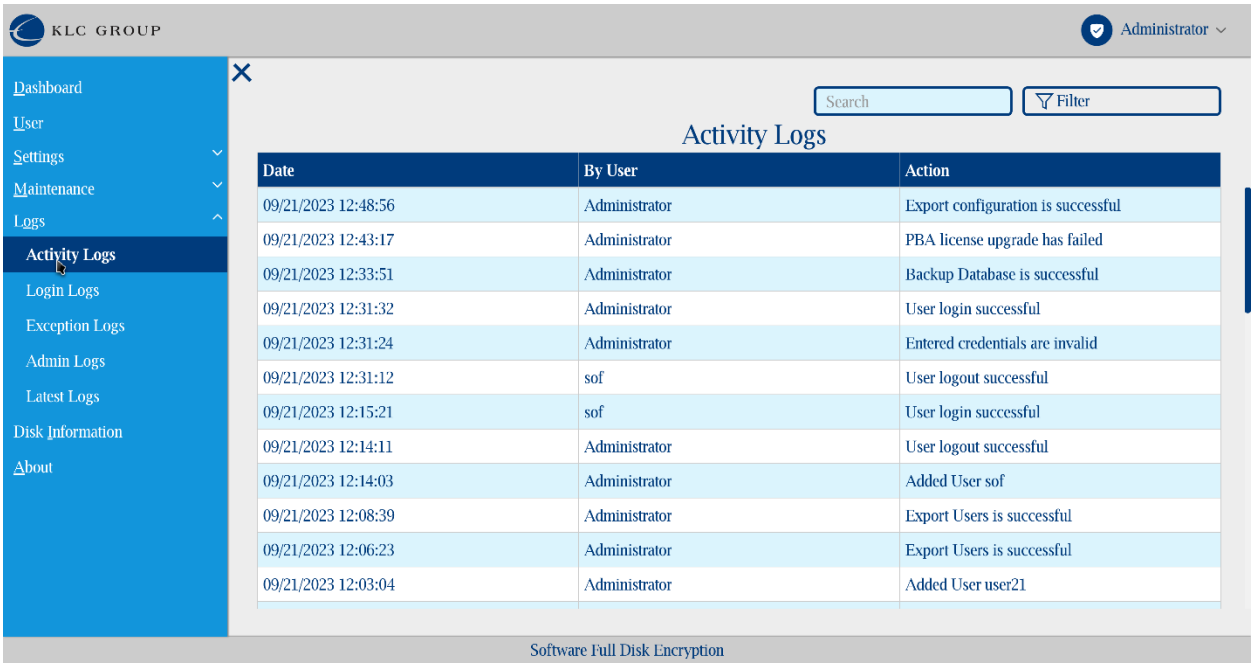
This feature is useful for deploying large number of devices with the same configuration on all of them. The configuration includes both users and settings. To carry out this operation, the Admin (role) or the Security Officer will select the “Export Configuration” option from the Maintenance menu.

- For the **Device Name** field, choose on what device/drive the files should be stored.
- For the **Passphrase** field, enter the passphrase that will be used to encrypt the output file /mnt/CDExportDB on the USB thumb drive.
- Click the Export Configuration button.
- The file will be created at the selected location and then it will display a message indicating the status of the operation.

Please remember the current password of administrator user at the time of the configuration export. You will need to provide it to the CDO Kryptr installer as you install CDO Kryptr with the import of this file. This should be entered as the –p parameter to the installer command. For more information, please see the 'Install CDO Kryptr with exported configuration file' section (under 'CDO Kryptr install optional parameters')

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 includes all 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
4. Failed to add user
5. Failed to edit user
6. Import users successful
7. PBA Deactivation successful
8. PBA Reactivation successful
9. Export PBA configuration successful
10. Export PBA configuration failed
11. Export users successful
12. Backup database successful
13. Backup database failed
14. PBA Upgrade successful
15. Change AK successful

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).

Following are the examples of events under this log:

1. User login successful
2. Entered credentials are invalid
3. User logoff successful (i.e. logging off from the CDO Kryptr administration application)

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

Following are the examples of events under this log:

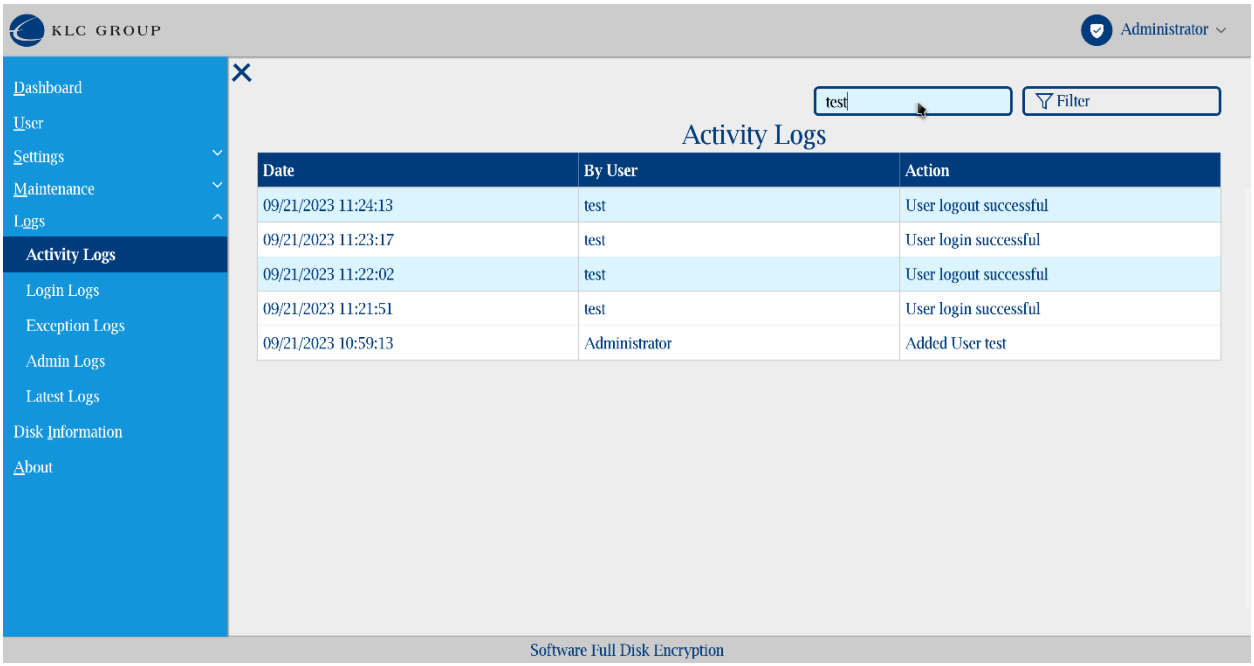
1. Entered credentials are invalid (User login failed)
2. Failed to edit User
3. Failed to add User
4. Failed to delete User
5. User logoff failed
6. Incorrect JSON data for import Users
7. PBA Upgrade has failed
8. Export PBA configuration failed
9. Backup database failed

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

1. User login Successful
2. Entered credentials are invalid (User login failed)
3. User logout successful
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
12. Import users successful
13. PBA Deactivation successful
14. PBA Reactivation successful
15. Export PBA configuration successful
16. Export PBA configuration failed
17. Export users successful
18. Backup database successful
19. Backup database failed
20. PBA Upgrade successful
21. Change AK successful

Latest log:
The latest logs lists the logs for the current day

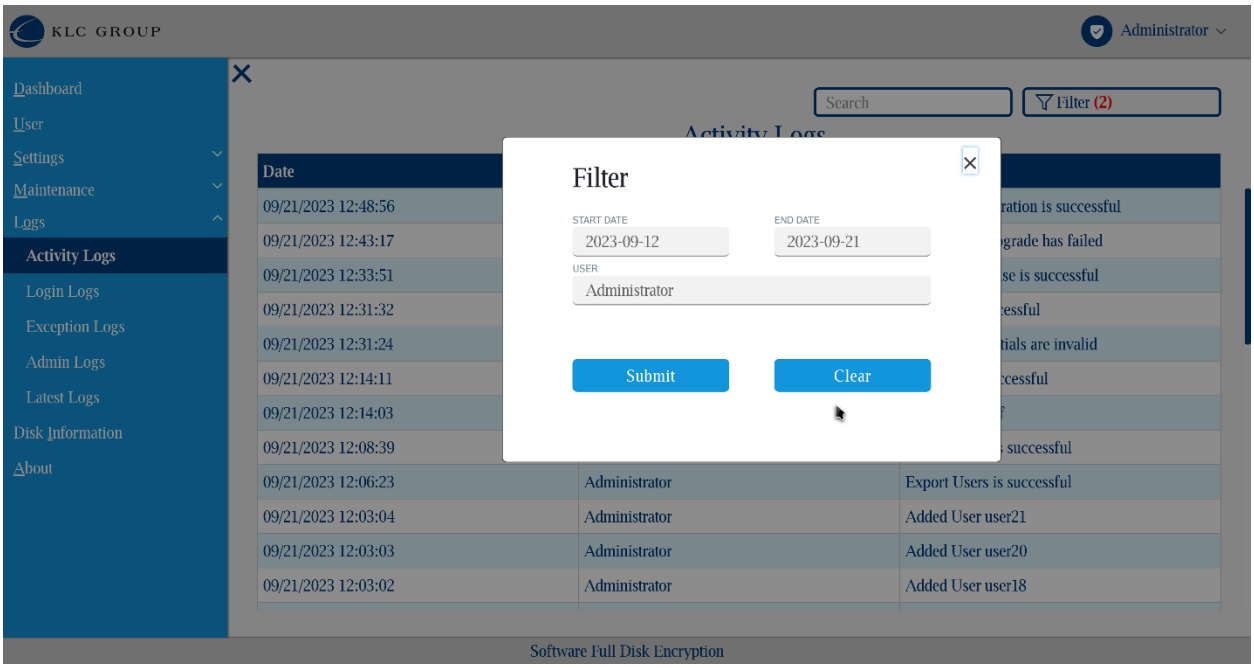
Search option



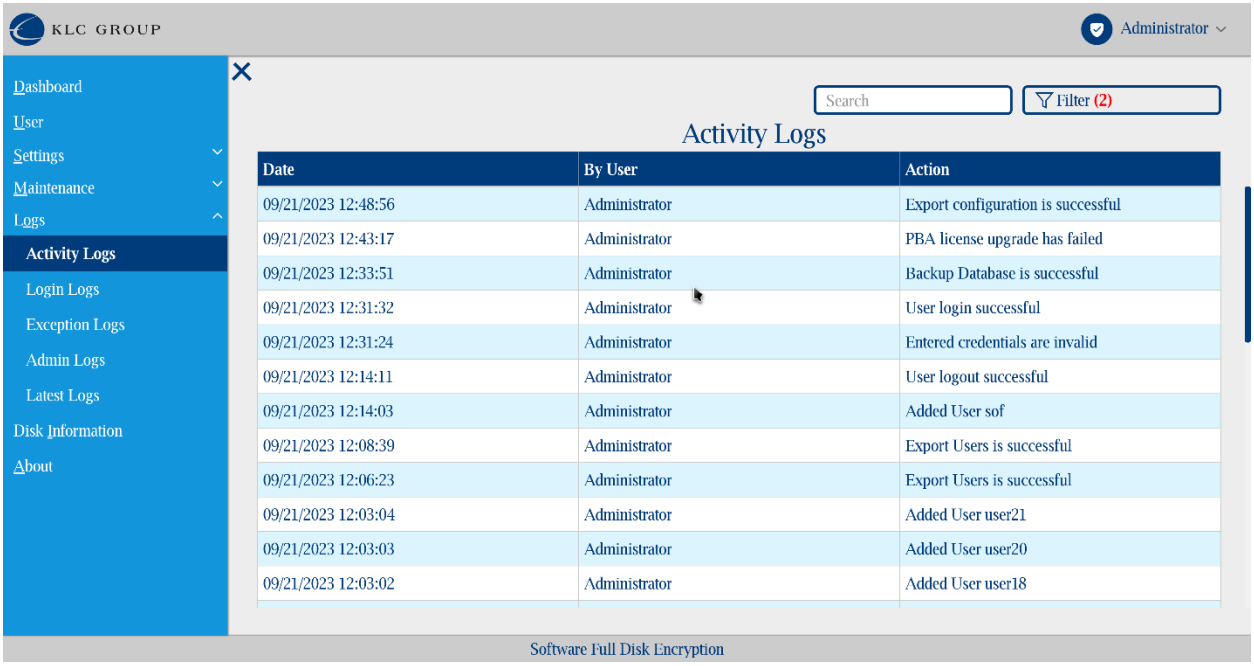
You can find selected info in logs faster and easier using the search option. In the search field enter a desired username, for example, and the search will return log entries for that user that are included in the current log you have viewed. In our case, the user ‘secure’ is entered into search field and log containing that username is displayed.

Filter option

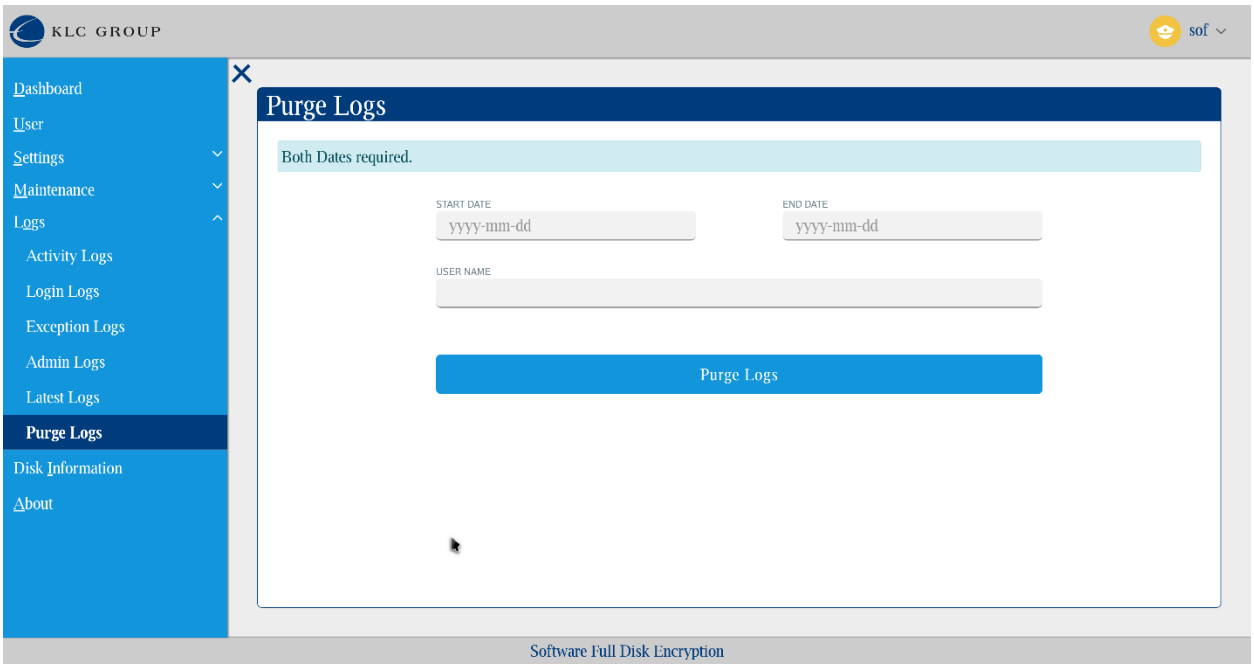
Filtering allows for narrowing down any search results in the logs by date range and/or username. Fill in one or more of the fields and press submit and the system will bring back the subset of logs of the log you have viewed. To do so click ‘Filter’ and in the popup dialog enter your criteria and click ‘Submit’



Filter settings you set will be remembered. Click on “Filter’ in the right corner above to edit them. To delete the current filter click ‘Clear’



Purge Logs Option



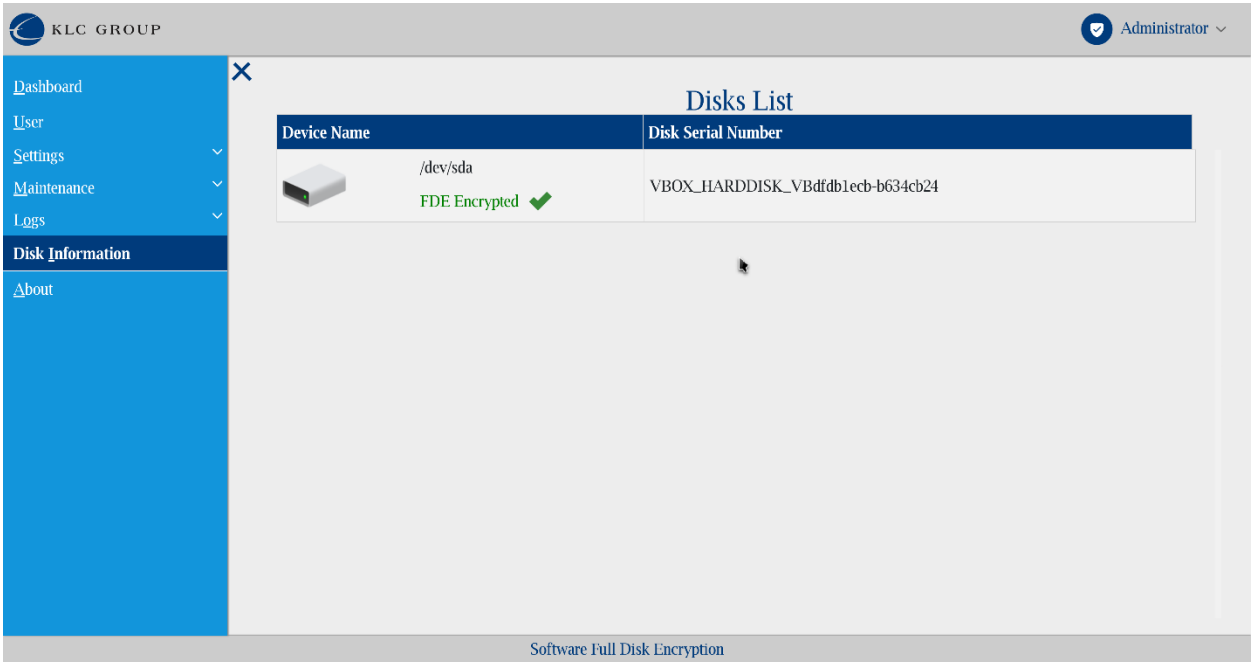
Security Officer (role) users have the exclusive right to delete (purge) logs. Enter start and end dates together with a username and click “Purge Logs”. This will remove log entries for that time period for all users or a specific user in the given time period from all logs. After purge, there will be a log entry stating that the log was purged and what filter data was used. The actual purge log info log entries (added after a purge) cannot be removed (for security reasons).

Disk Information

Disk Info on Linux

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

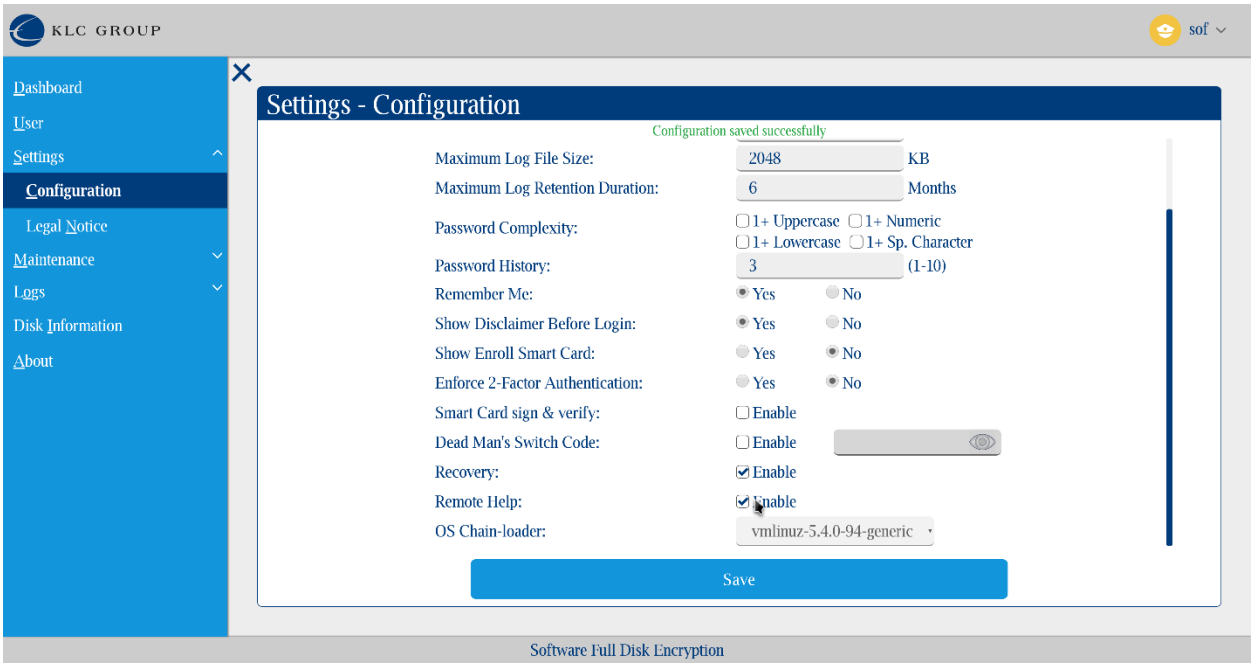
Disk info on Windows:



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.

Remote Help

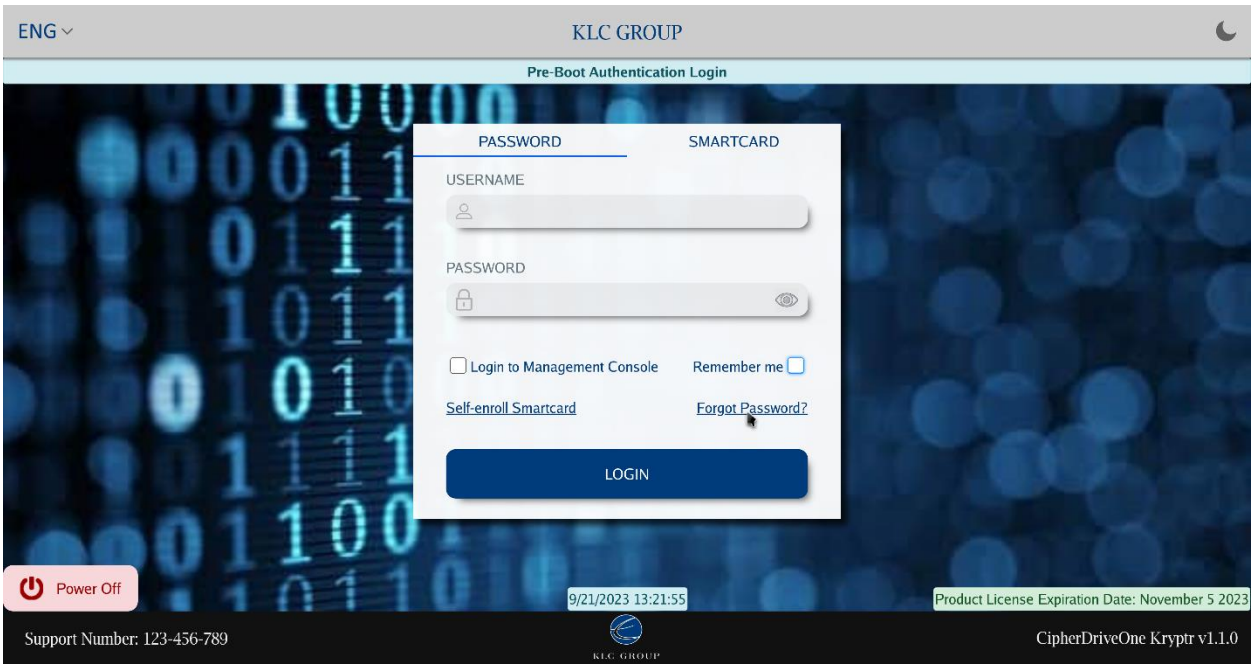
The remote help functionality can be used after a security officer user enables the Remote Help field in the console from the Settings – Configuration screen (both on user and on helper side):



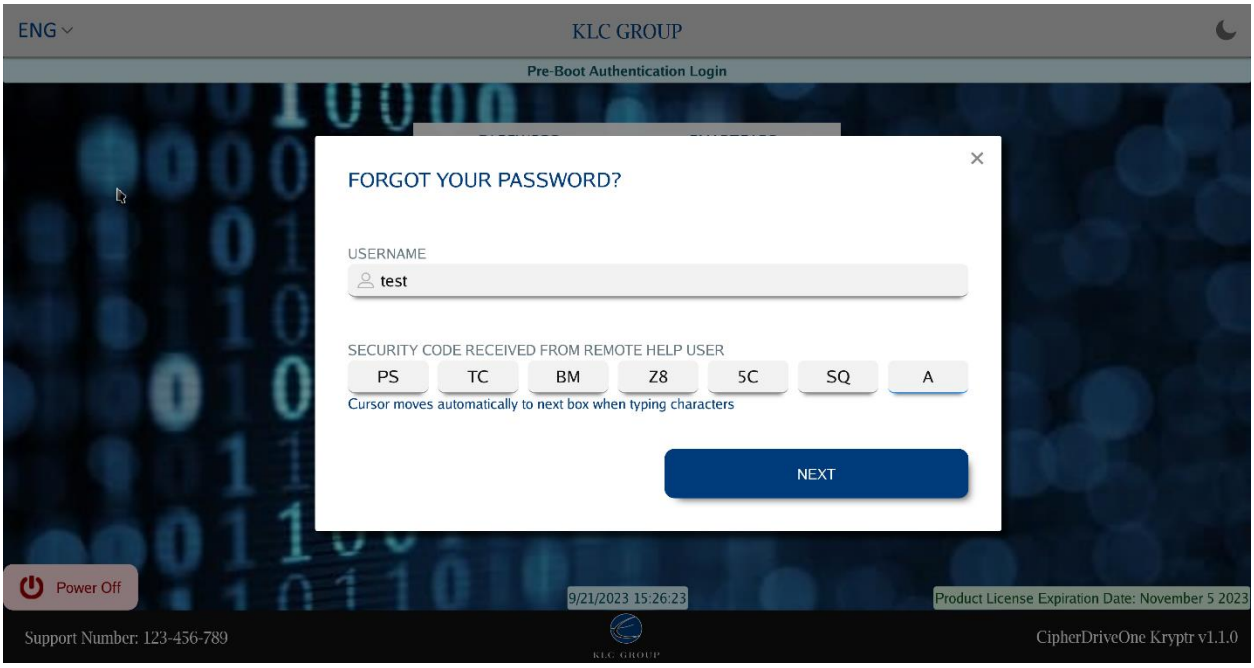
The process is as follows:

USER SIDE

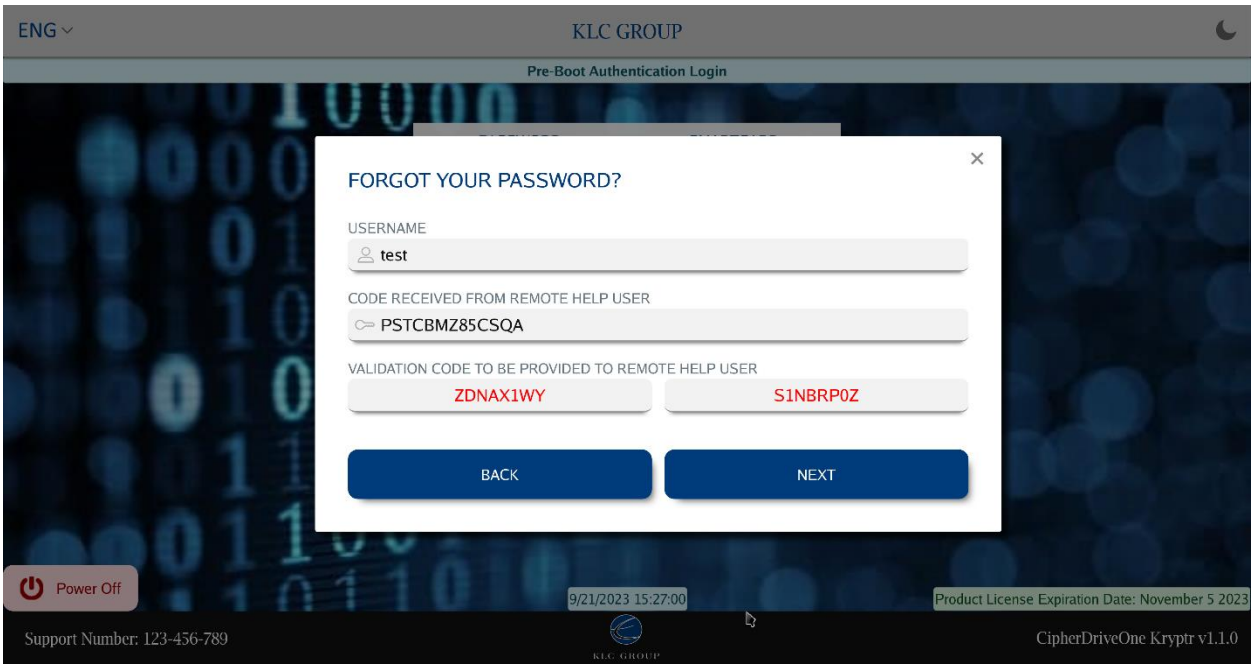
1. The user that has forgotten their password should press **Forgot password?** on the Login screen:



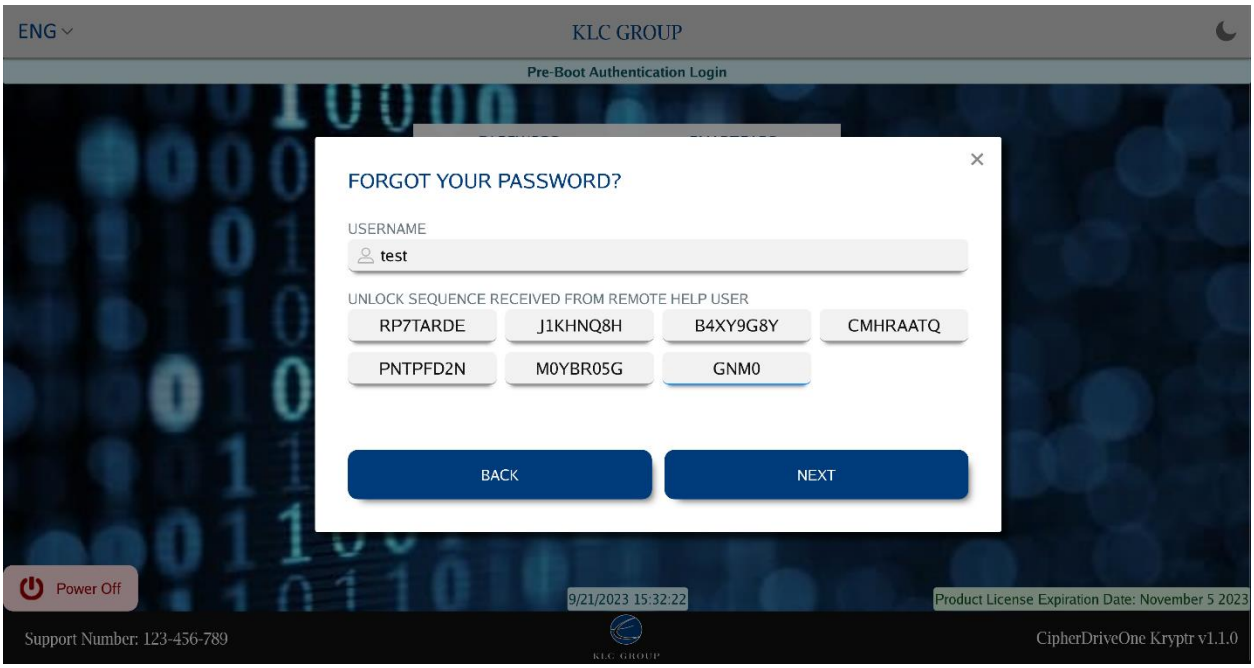
2. On the popup dialog the user should fill their user name in **USERNAME** and **SECURITY CODE** fields received from the helper:



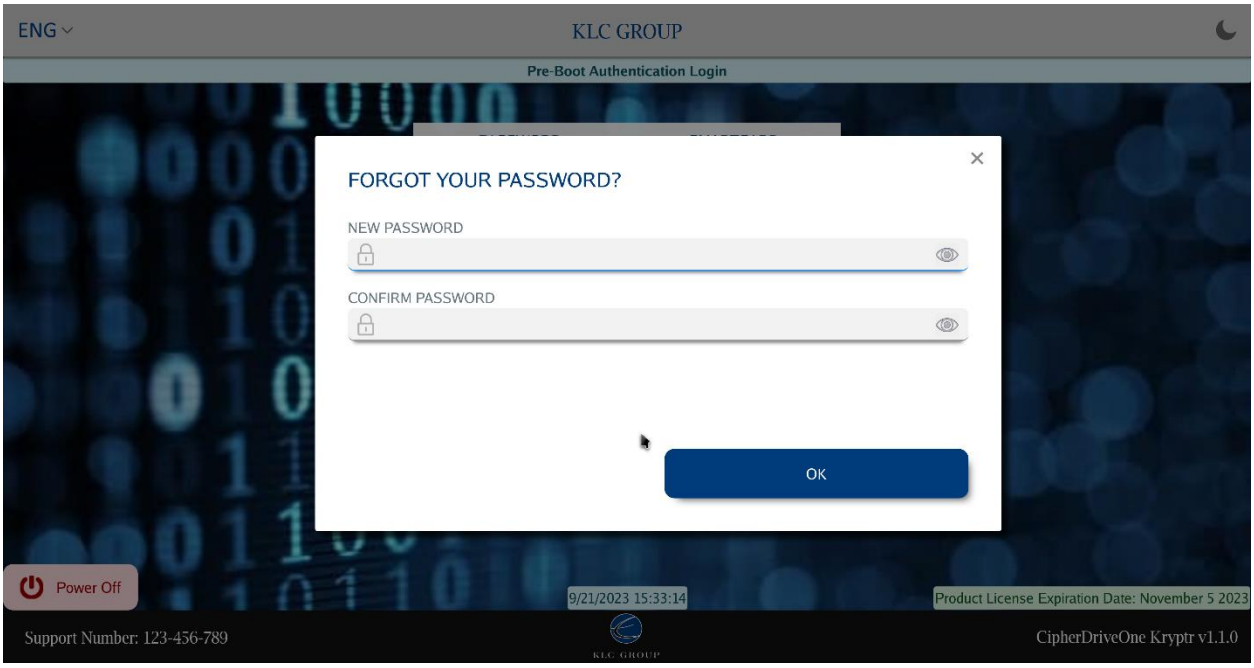
3. After **USERNAME** and **SECURITY CODE** fields are provided and the **NEXT** button is pressed new fields populated with **VALIDATION CODE** will appear. This code should be provided to the helper.



4. After the **NEXT** button is pressed a new screen will appear where the **UNLOCK SEQUENCE** provided by the remote helper should be entered:



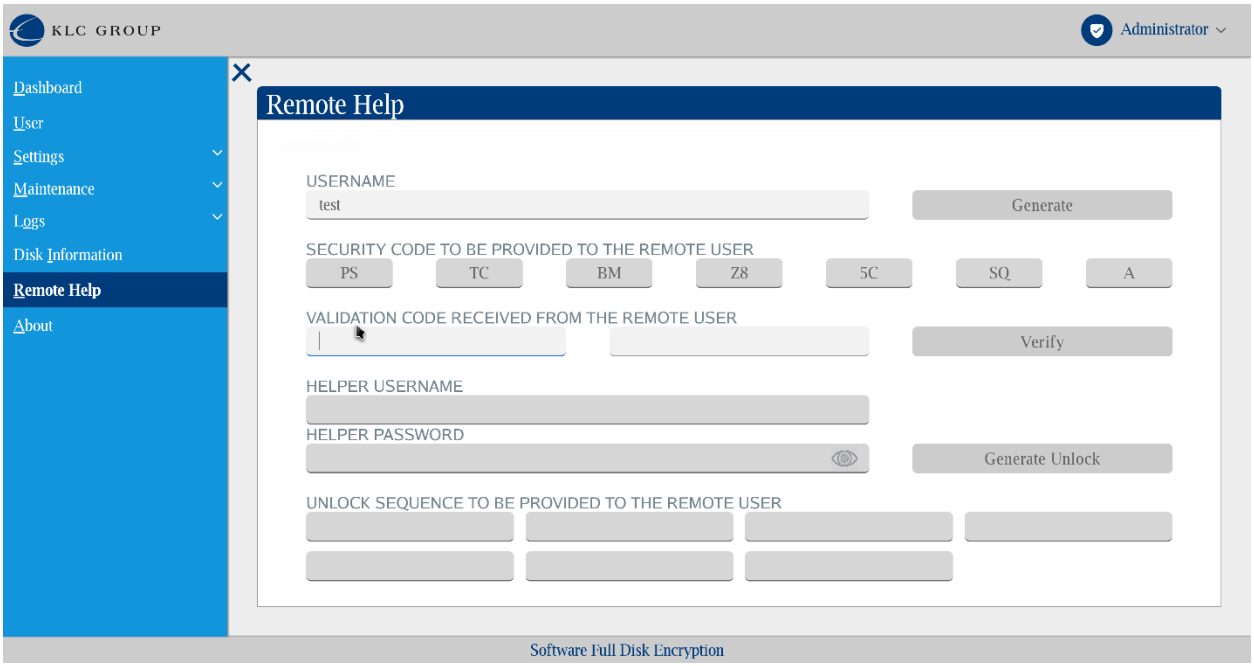
5. After pressing the **NEXT** button the user will be prompted to fill their new password:



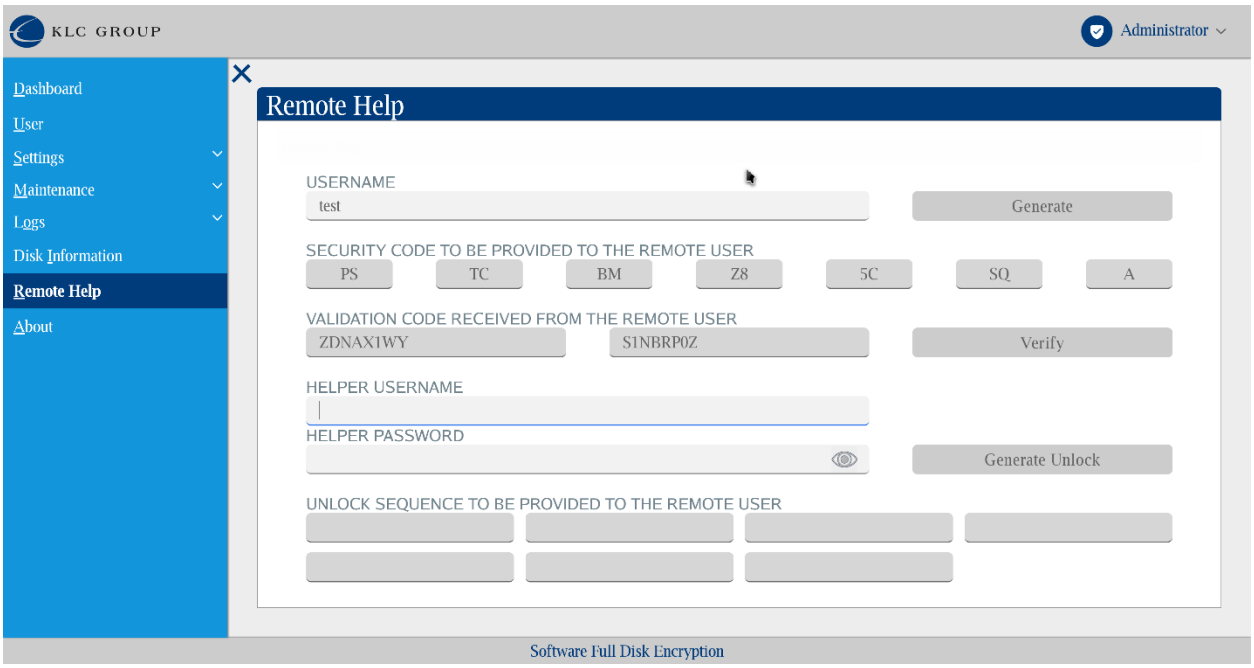
Note: Only if everything is OK, the user password will be changed.

HELPER SIDE

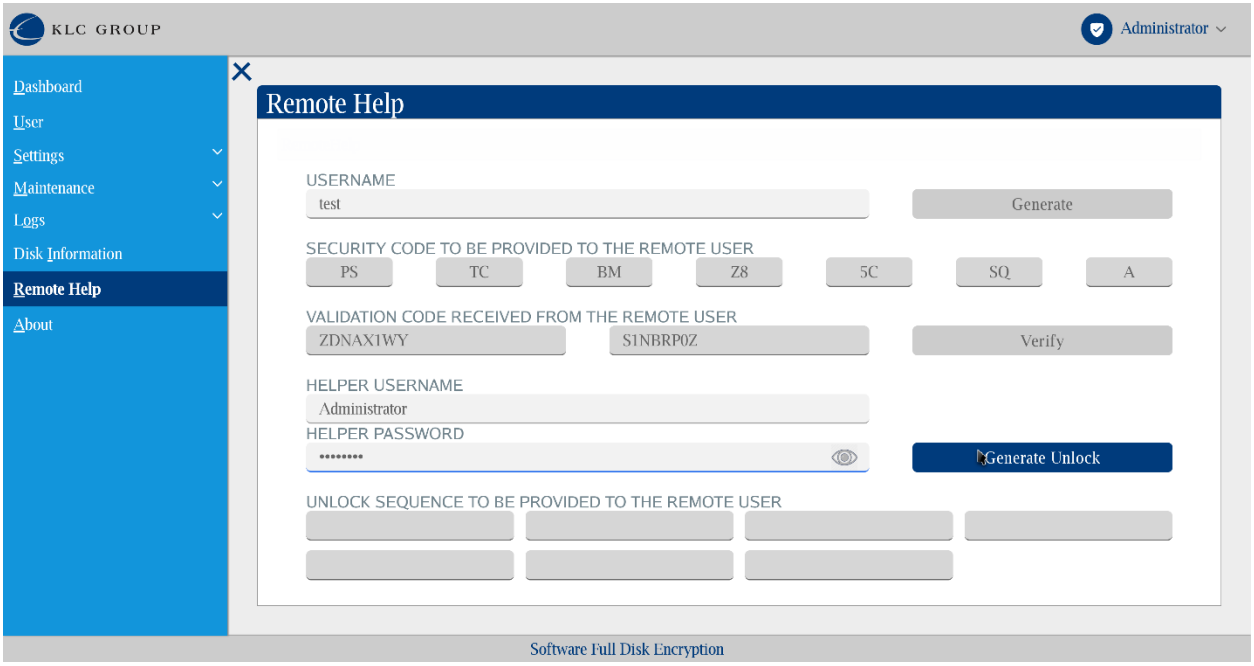
1. The admin/help-desk user should login to the CDO Kryptr console and go to the Remote Help screen. In the **USERNAME** field, enter the user name provided by the user that has forgotten their password. After the **Generate** button is pressed a **SECURITY CODE** will be displayed. This code should be provided to the user:



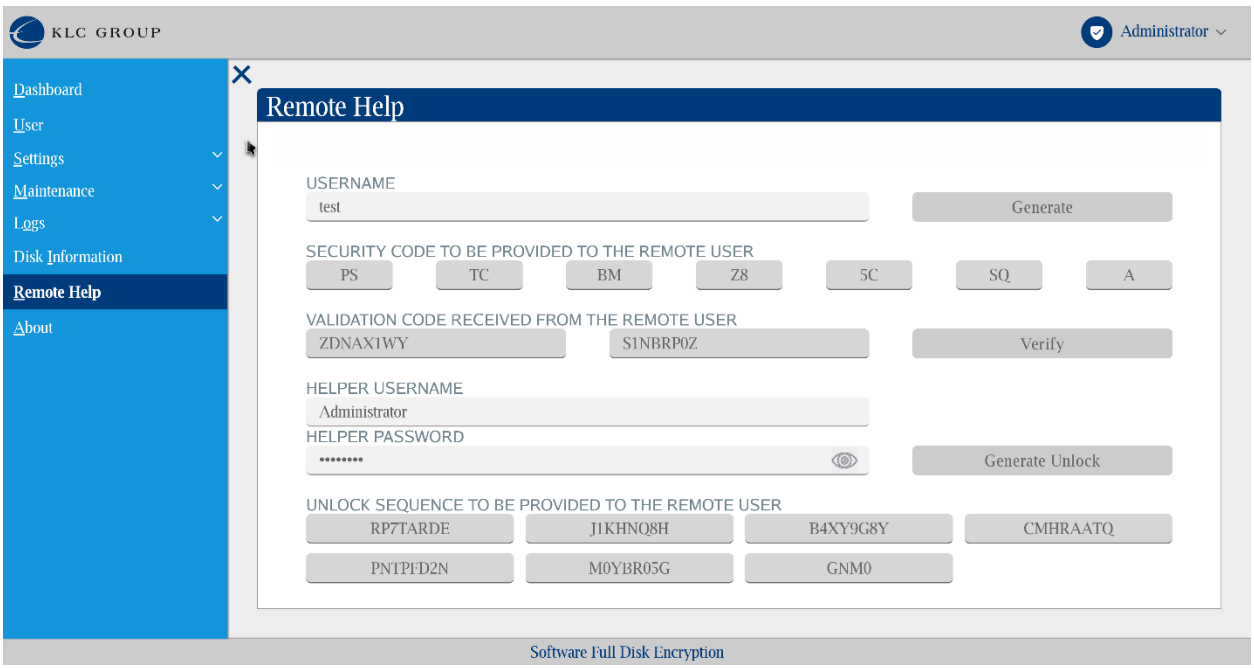
2. The user will provide back a **VALIDATION CODE** that should be entered and verified by pressing the **Verify** button:



3. If everything is OK, enter the user name and password of an admin/help-desk user from the computer on the user side and press the **Generate Unlock** button.

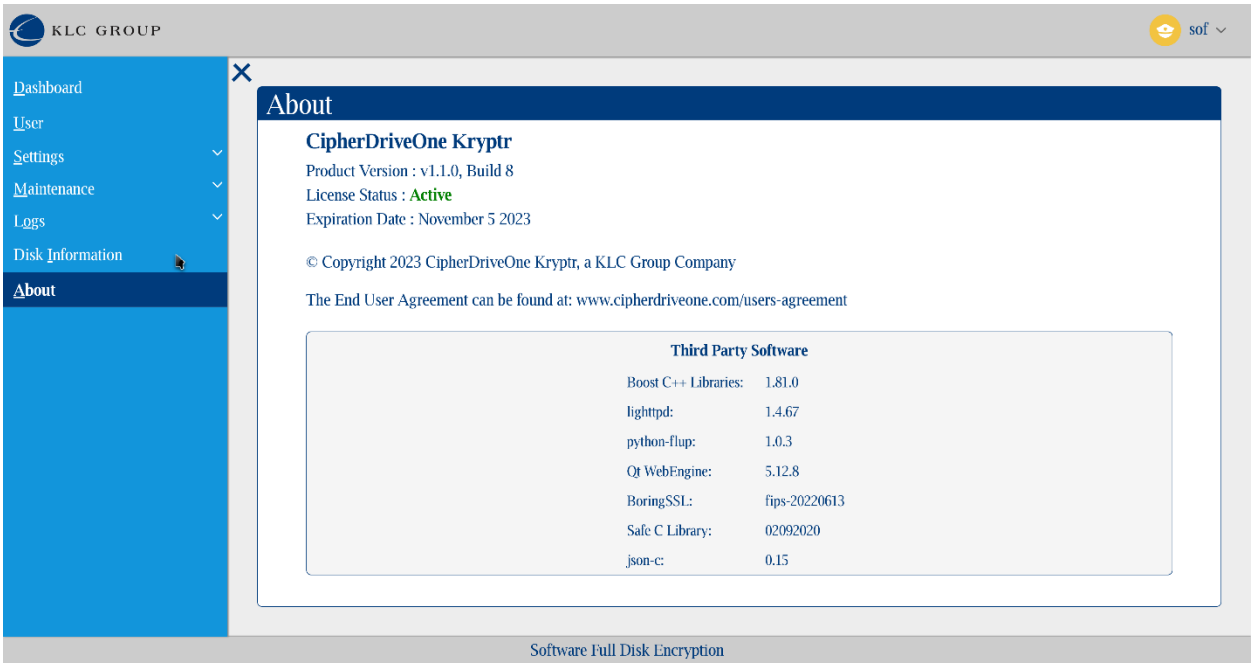


4. The **UNLOCK SEQUENCE** will be displayed. This sequence should be provided back to the user:



Once the user entered the sequence, the user will be able to choose a new password.

About CDO Kryptr



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

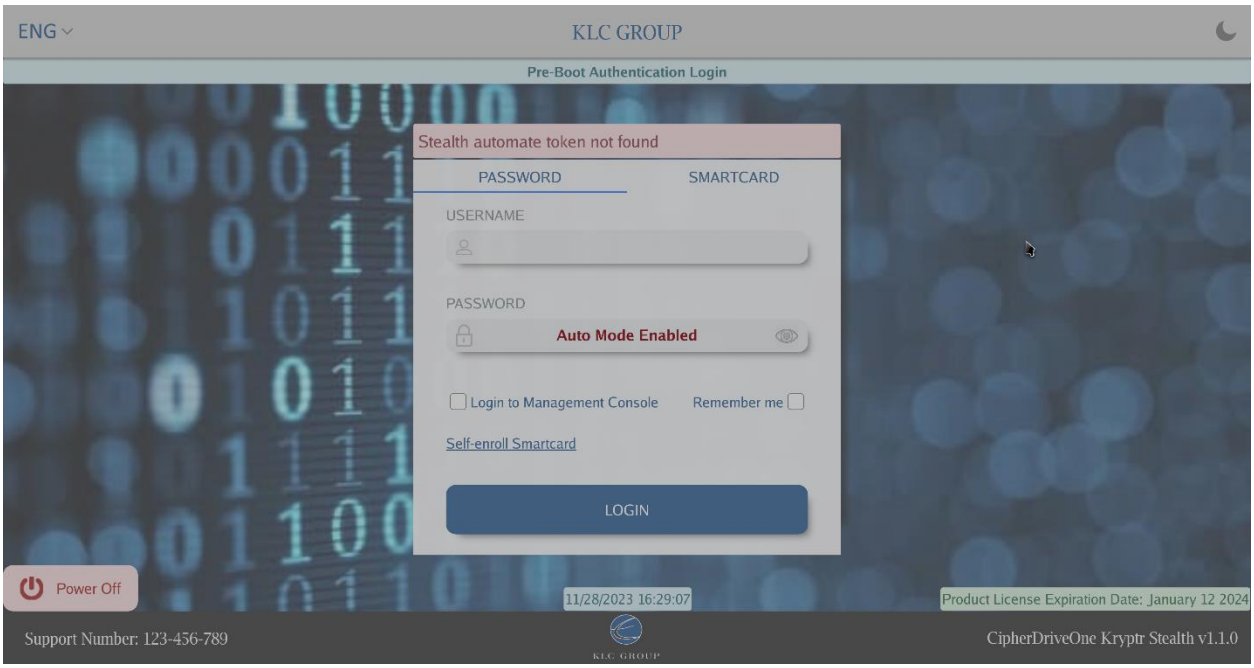
Stealth Feature

Stealth feature is enabled by a **special license** and enables a CDOK user to silently and automatically login into the protected Operating system using a secured token file located on a USB thumb drive.

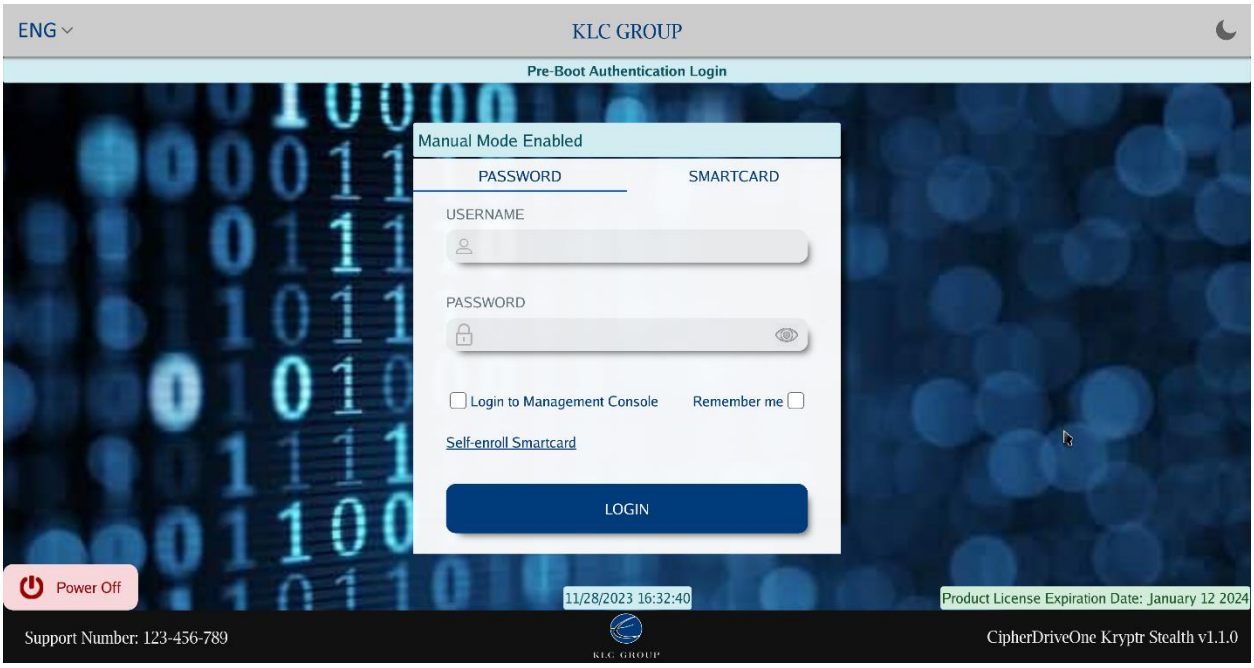
With the thumb drive inserted - containing the token file – the user does not need to enter a username and password. Instead, the encrypted token file is used for automatic authentication.

For example, this can be used in a situation where there is no standard user interface at boot (e.g. a drone) but there is a USB connector. A user with the pre-provisioned token file can insert the USB thumb drive and CDOK will recognise the insertion of the drive, pull the encrypted credentials from the token file, and then automatically unlock the drive and boot the host OS.

Login screen



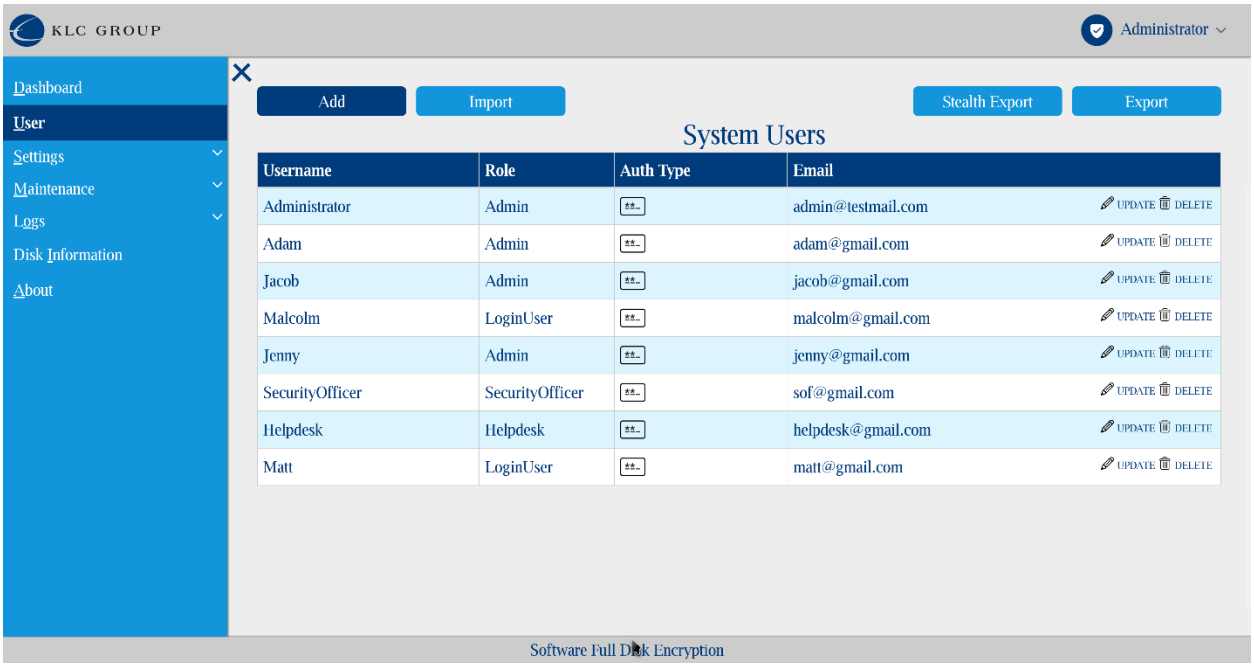
When PBA boots, it displays “Auto Mode Enabled” Label on top of Screen indicating that PBA is looking for the AutomateFdeTokenEnc file on the thumb drive. Users can press the Escape (Esc) button to switch to Manual mode



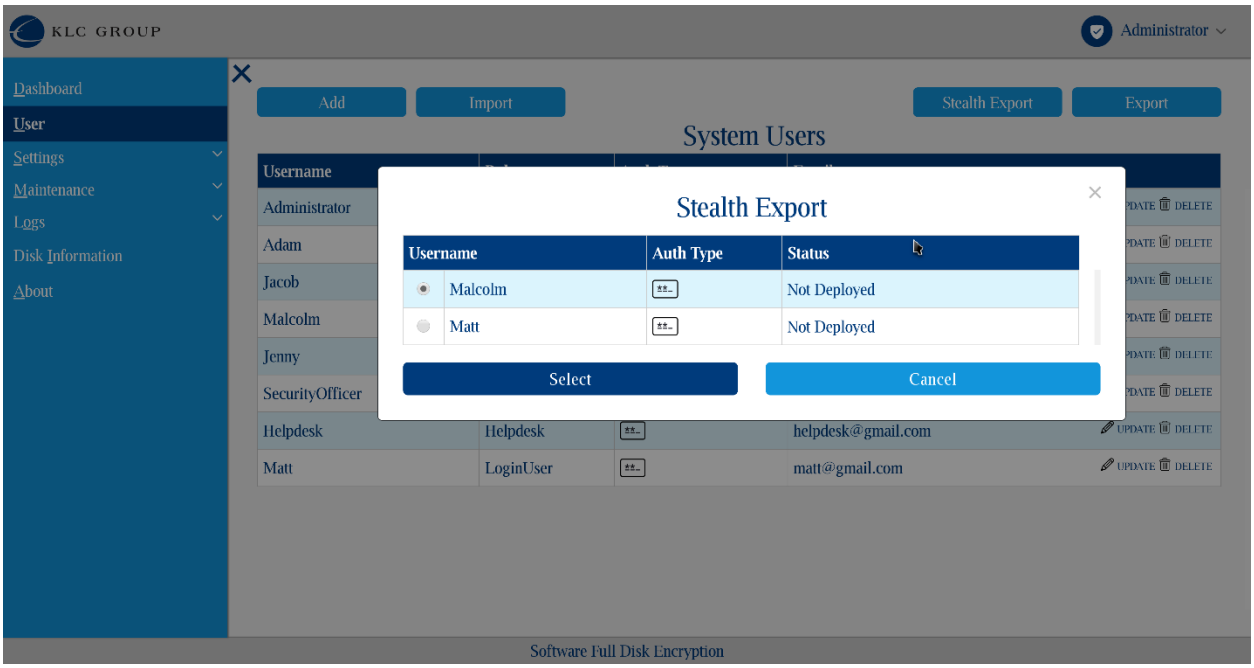
By entering Manual Mode, Administrator users can login into the management console in order to deploy Stealth users to USB and generate an “AutomateFdeTokenEnc” file on the thumb drive.

User List

In Users-> System users there is a Stealth Export button that should be clicked to start Stealth user deployment process



Stealth Export users

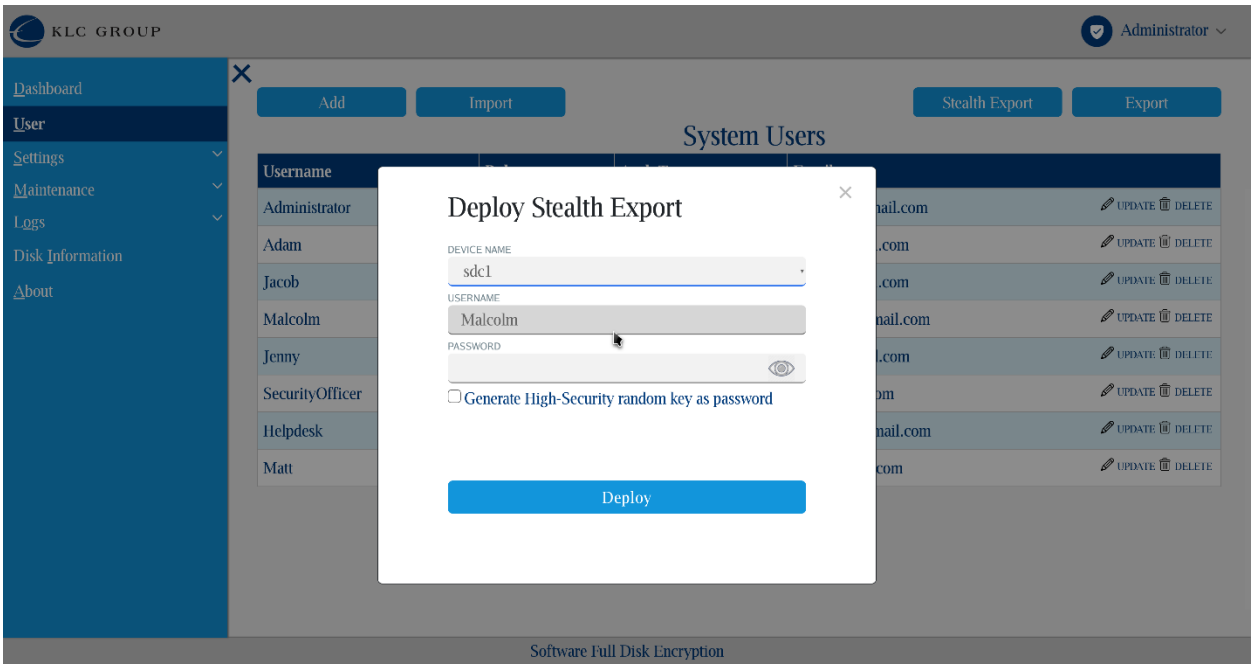


When Stealth Export is clicked, it will show only Login Users and their deployment status. Choose a user you wish to deploy and click ‘Select’

Deploy Stealth users

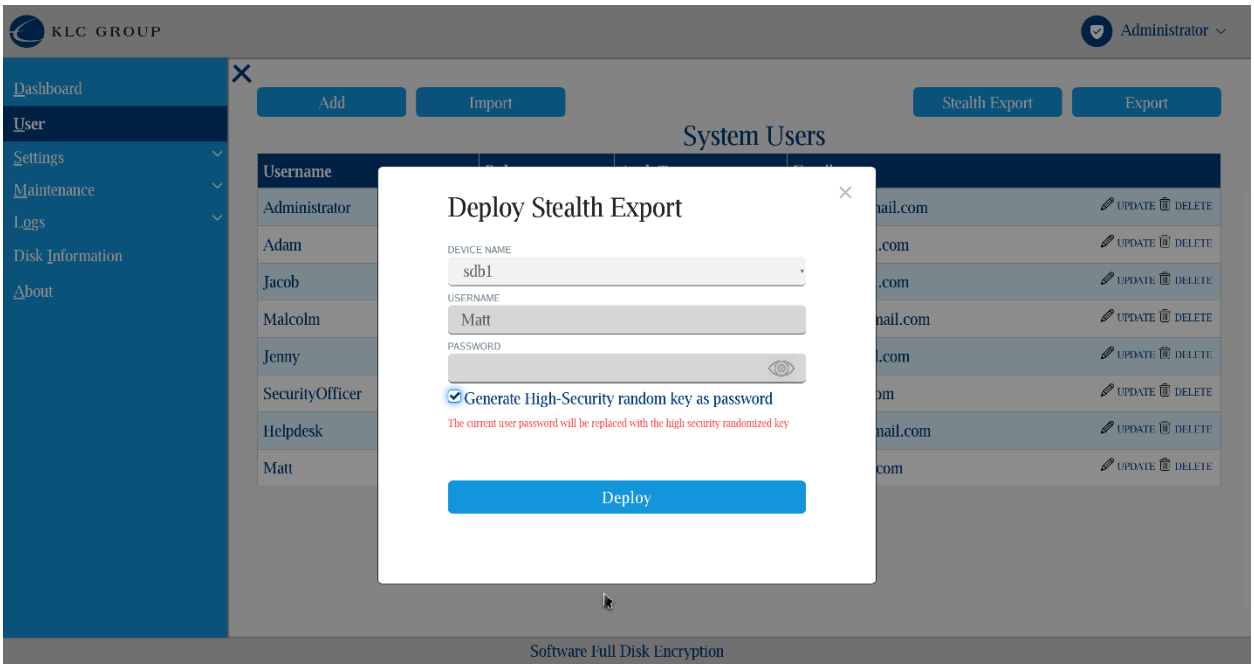
There are 2 main options to deploy a user: with manual password or with random password:

User Stealth Deployment with manual password



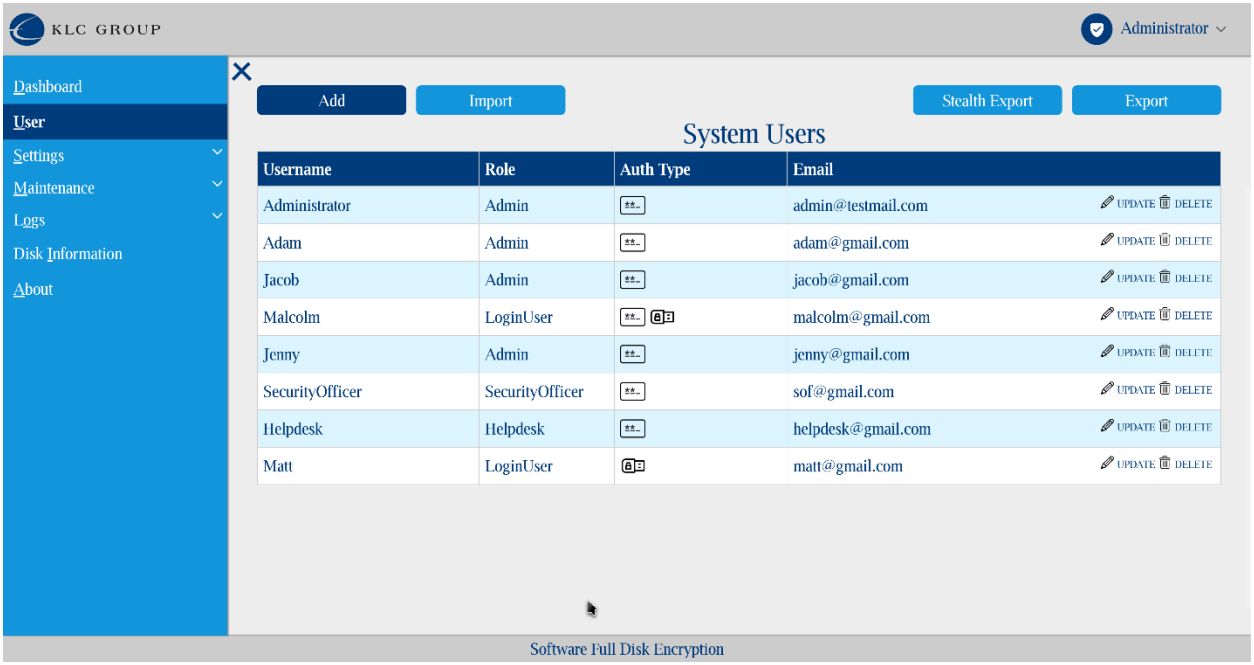
With the USB thumb drive attached to the system, enter the current user password in the Popup. When clicking Deploy button, it will authenticate the user and create and encrypt the AutomateFdeTokenEnc file on the thumb drive for deployment.

User Stealth Deployment with random password



With the USB thumb drive attached to the system, check ‘Generate High-Security random key as password. CDOK will give you a warning that current user password will be replaced by a high security randomized key. When clicking Deploy button, it will authenticate the user and create and encrypt the AutomateFdeTokenEnc file on the thumb drive for deployment.

If deployment is successful, a USB icon will be showed in System users list under Authentication type of deployed user



Verify that the file AutomateFdeTokenEnc is created on the thumb drive

Stealth user login

Power-off machine, insert USB drive, power-on and wait for CDOK login screen to appear in Auto mode. Wait for deployed user to be authenticated automatically and for protected OS to boot.