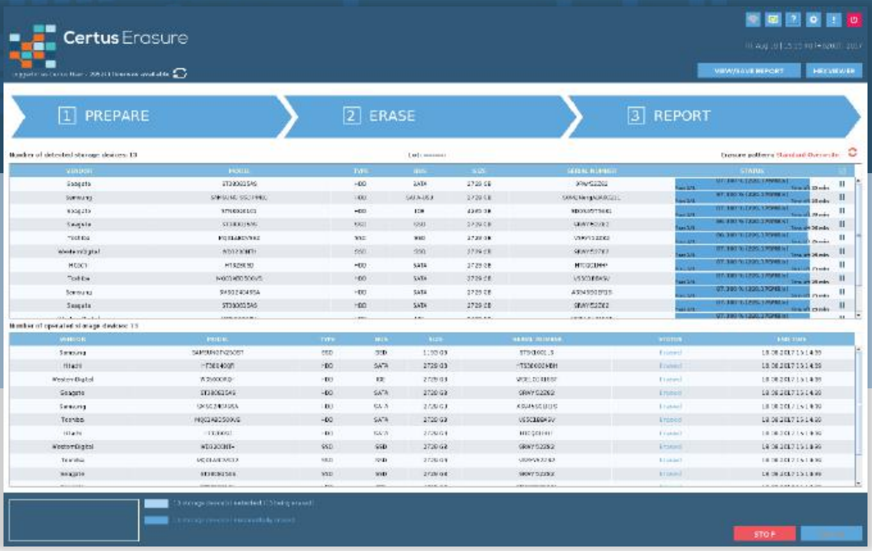
Certus Software

Certified Data Erasure Professionals



Certus Erasure

User Manual

for v3.13.0

Certus Software GmbH

HRB 29785

Karl Nolan Strasse 3
86157 Augsburg
Germany

Tel: +49 (0) 821 - 650 688 - 0
Fax: +49 (0) 821 - 650 688 - 20
Email: contact@certus.software
Website: www.certus.software

CONTENTS

CHAPTER 1. GENERAL INFORMATION

Please note that after successfully using the product on your storage devices, all the data contained will be destroyed in such way that it will be impossible to be recovered by any existing method or tool. After performing the Certus erasure procedure, your storage devices will be perfectly usable.

1.1. Certus Erasure installation prerequisites

Minimum system requirements to run Certus Erasure:

- x86 or x86-64 Pentium 4 or equivalent machine;
- 512 MB RAM memory;
- USB port;
- VGA video card (minimum screen resolution: 1024x768);
- Active Ethernet connection (optional for HASP solution).

Software requirements:

- CertusErasure-X.X.X.iso file downloaded from Certus Software Web Manager (CEWM) - an online application used to store and manage Certus erasure reports https://cloud.certus.software;
- USB Flash drive;
- Computer running Microsoft Windows, Linux or MacOS family operating systems.

For Windows operating system, the user should install Win32 Disk Imager from **https://sourceforge.net/projects/win32diskimager** and use it to write Certus Erasure ISO image. For Linux and MacOS operating systems, the user should identify the USB flash drive in a terminal, unmount it and write Certus Erasure ISO image. A detailed description of the installation steps can be found in the Quick User Guide document, which can be downloaded from CEWM.

1.2. Certus Erasure online solution

Certus Erasure Web Manager (CEWM) is a management tool designed to integrate functionalities related to the erasures procedures performed through the Certus Erasure application.
The tool serves as a centralized control point, which manages users, erasure licenses and data erasure reports generated by Certus Erasure. Its usage offers clients the online solution to:

- create, edit, delete a group/user;
- transfer group/user data;
- check group/user activity;
- assign licenses to users;
- transfer licenses between users;
- suspend or activate user accounts;
- create, edit or delete a template erasure report;
- edit, delete, export reports;
- check report properties.

For more information regarding the CEWM tool please consult Certus Erasure Web Manager User Manual. To get access to this user manual, you must login into the CEWM tool from the link: https://cloud.certus.software and the select the Downloads module.

1.3. Certus Erasure offline solution

The offline solution, recommended by the Certus team, is represented by the HASP (Hardware Against Software Piracy) key. It is a management solution which enables the use of Certus Erasure software enforcing software protection and licensing.

To use the offline solution, first, the user must insert the HASP key into a USB slot on a computer and then login into the Certus Erasure application. The application will automatically start if the HASP key is recognized and validated by the application.

For more details regarding the HASP Key refer to the HASP Key User Guide available on CEWM.

NOTE: No internet connection is required while operating with the Certus Erasure software through the HASP key.

NOTE: A HASP Key solution is available on request at the contact@certus.software email address.

NOTE: It is highly recommended for the user to periodically check, at least once a week, for the latest version of Certus Erasure. Because of the lack of internet connectivity, the software is unable to check the latest version as it does in case of the online solution, therefore the operation must be done manually. To do this, access the Downloads module from CEWM (https://cloud.certus.software) and check the available software versions. If there's a higher version than the one you're currently using, please download it and use it to create a new bootable USB Flash Drive. Please check the Quick User Guide which can be found on the same page and follow the instructions presented in it to learn how you should use the Certus Erasure ISO image properly.

1.4. Recommendations for the user

The person using this software is advised to follow the guidelines offered by Certus team in the documents stored on CEWM, Downloads module – Certus Erasure Manual, Certus Erasure Quick User Guide and Certus Erasure Web Manager Manual.

WARNING:
The user can copy, install, access and benefit from using Certus Erasure Software, during the license term, only for his own internal operations.

The user shall:

- ensure that the Software is installed on designated equipment(s) only;
- keep a complete and accurate record of the use of the Software;
- notify Certus Software GmbH as soon as it becomes aware of any unauthorized use of the Software;
- not use or access the Software if he is or becomes a direct competitor of Certus Software GmbH, except with Certus Software GmbH prior written consent or for purposes of competitive benchmarking or similar purposes;

- not be allowed to commercially exploit the Software in any way;
- not produce any derivative works based on, any part of the Software for any reason or purpose;
- not be entitled to license, sublicense, sell, resell, transfer, assign, distribute, rent, to the maximum extent such restriction is permitted by applicable law;
- comply with all applicable data protection laws and not use the Software in contravention with such laws.

CHAPTER 2. LOGIN SCREEN

When Certus Erasure has booted successfully, the login screen is shown. The following credentials are asked for: ***username***, ***password*** and ***customer code***.

The login screen also contains **Wi-Fi**, **Internet connection**, **Help**, **Settings** and **Shutdown** buttons. Please refer to **Wi-Fi button, Internet connection icon**, **Help button, Settings button, Report an issue button** and **Shutdown button** chapters for more information.

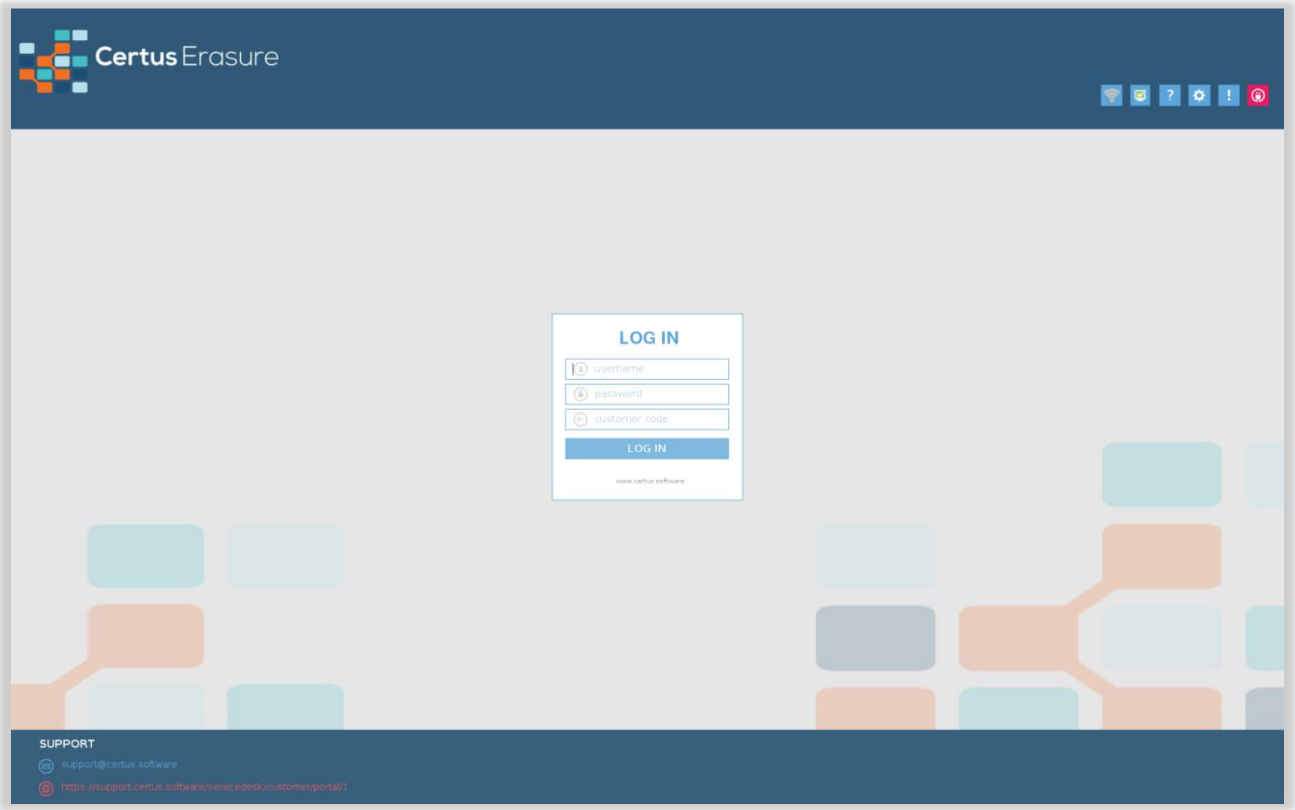
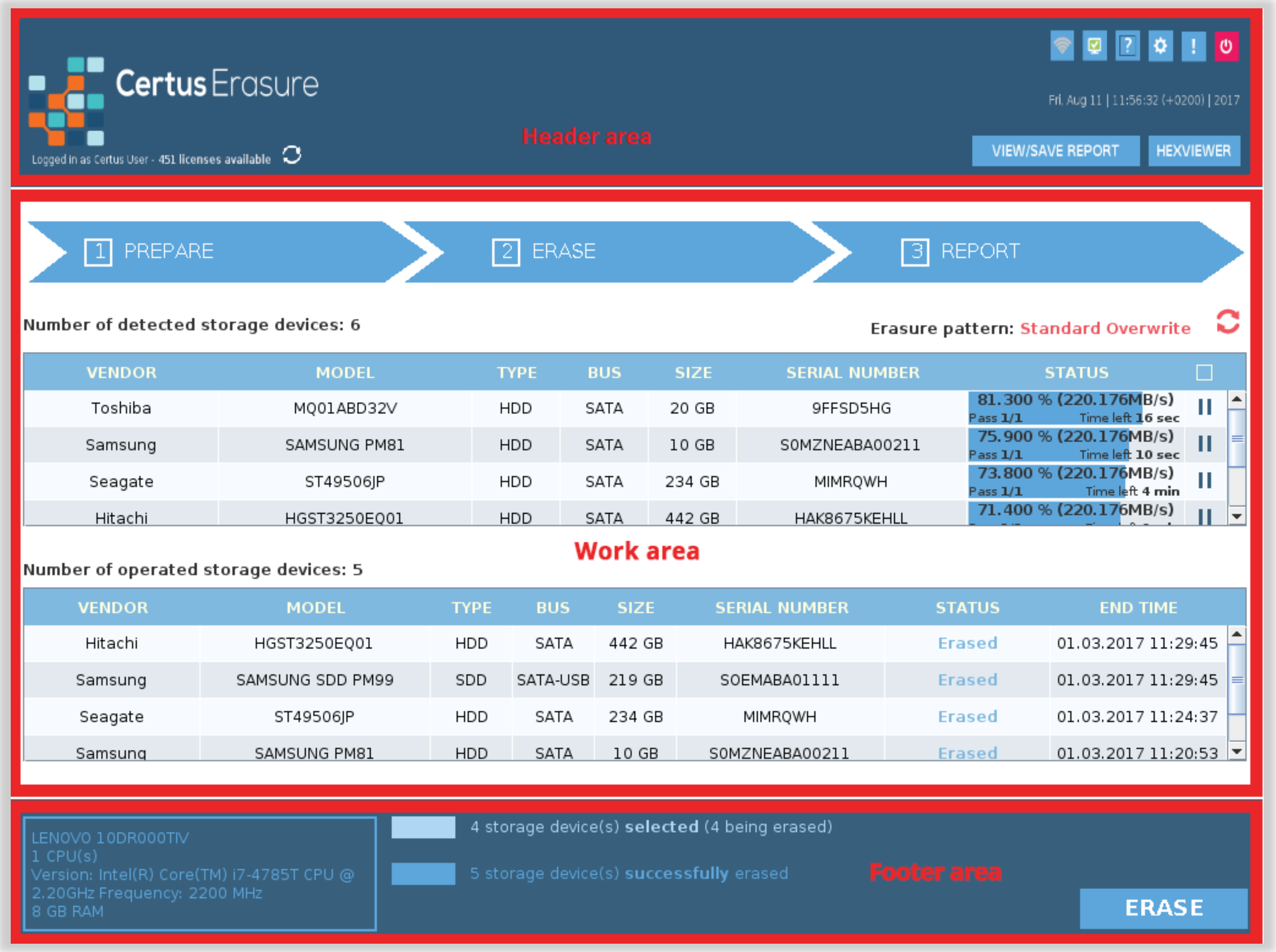


Fig. 2.1 Login screen

CHAPTER 3. CERTUS ERASURE USER INTERFACE

The Certus Erasure user interface is divided into three main areas as follows: the **header** area, the **work** area and the **footer** area.



Certus Erasure

Logged in as Certus User - 451 licenses available

Fri, Aug 11 | 11:56:32 (+0200) | 2017

Number of detected storage devices: 6

Erasure pattern: Standard Overwrite

VENDOR	MODEL	TYPE	BUS	SIZE	SERIAL NUMBER	STATUS
Toshiba	MQ01ABD32V	HDD	SATA	20 GB	9FFSD5HG	81.300 % (220.176MB/s) Pass 1/1 Time left 16 sec
Samsung	SAMSUNG PM81	HDD	SATA	10 GB	S0MZNEABA00211	75.900 % (220.176MB/s) Pass 1/1 Time left 10 sec
Seagate	ST49506JP	HDD	SATA	234 GB	MIMRQWH	73.800 % (220.176MB/s) Pass 1/1 Time left 4 min
Hitachi	HGST3250EQ01	HDD	SATA	442 GB	HAK8675KEHLL	71.400 % (220.176MB/s)

Number of operated storage devices: 5

VENDOR	MODEL	TYPE	BUS	SIZE	SERIAL NUMBER	STATUS	END TIME
Hitachi	HGST3250EQ01	HDD	SATA	442 GB	HAK8675KEHLL	Erased	01.03.2017 11:29:45
Samsung	SAMSUNG SDD PM99	SDD	SATA-USB	219 GB	S0EMABA01111	Erased	01.03.2017 11:29:45
Seagate	ST49506JP	HDD	SATA	234 GB	MIMRQWH	Erased	01.03.2017 11:24:37
Samsung	SAMSUNG PM81	HDD	SATA	10 GB	S0MZNEABA00211	Erased	01.03.2017 11:20:53

LENOVO 10DR000TIV
1 CPU(s)
Version: Intel(R) Core(TM) i7-4785T CPU @ 2.20GHz Frequency: 2200 MHz
8 GB RAM

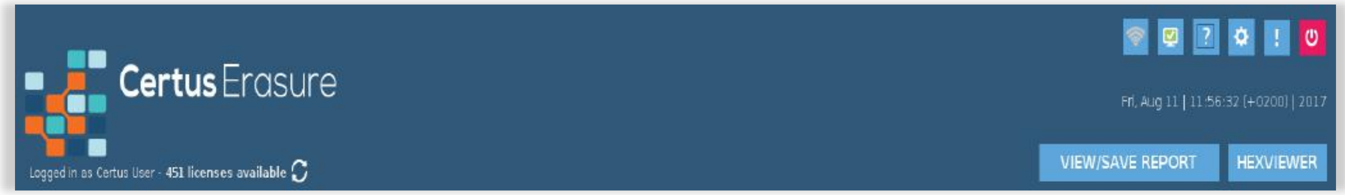
4 storage device(s) **selected** (4 being erased)

5 storage device(s) **successfully** erased

Fig. 3.1 The user interface

3.1. Header area

The header area contains information about the software in use, such as the software name and the version. The username and the available licenses are displayed on the left side of the header area, along with a button to refresh them. Wi-Fi button, Internet connection button, Help button, Settings button, Report an issue button, Shutdown button, date and time, View Report button and Hexviewer button are displayed on the right side of the header area.



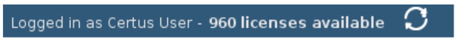
Certus Erasure

Logged in as Certus User - 451 licenses available

Fri, Aug 11 | 11:56:32 (+0200) | 2017

Fig. 3.2 Header area

3.1.1. User and licenses



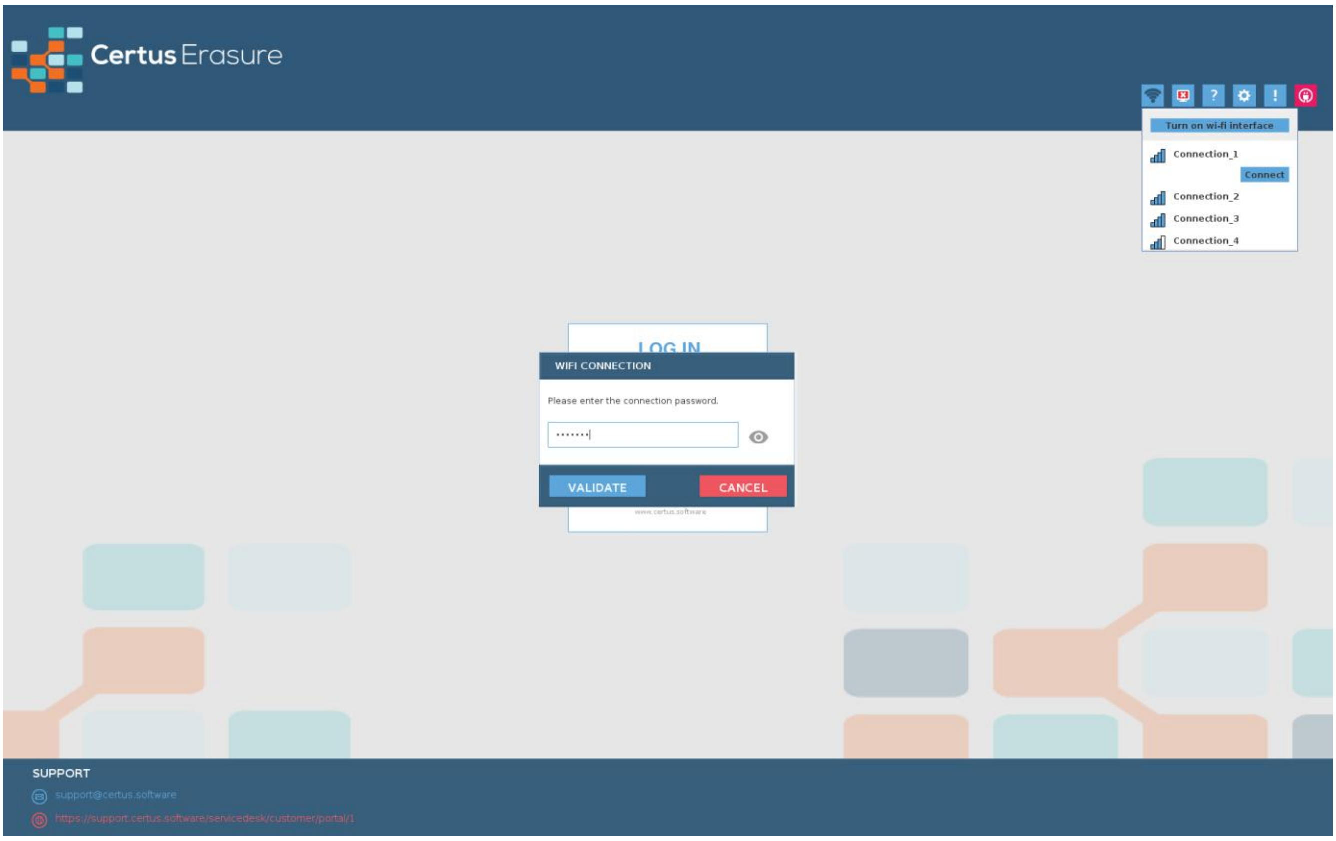
Logged in as Certus User - **960 licenses available**

This section of header area contains the username and the total number of the available licenses of the currently logged in person. The button next to it will allow you to initiate a request to CEWM for refreshing the settings and the number of available licenses.

3.1.2. Wi-Fi button

The user can connect to the internet through a Wi-Fi network by selecting the first button from the top right side of the main window from CE application. Then, after selecting the “Turn on wi-fi interface” function, a list with all the Wi-Fi available networks will appear in the Wi-fi menu. After selecting a Wi-Fi network, If the network is secured you will need to provide a password to connect to it, otherwise the system will connect automatically to the related Wi-Fi network. Once you're connected, the WI-FI network will be marked with blue.

NOTE: The machine on which Certus Erasure runs must have a Wi-Fi card.



Please enter the connection password.

•••••••

support@certus.software

https://support.certus.software/servicedesk/customer/portal/1

Fig. 3.3 Password window for wi-fi

3.1.3. Internet connection icon

Certus Erasure monitors the internet connection and offers a set of icons, which shows its status, located in the header area. The user can, at any time, hover the mouse on the displayed icon to read the status of the internet connection.

For an active internet connection and a successful connection to Certus server, the icon will be a white checkmark on green background.

In case of a detected internet connection with a problematic connection to Certus server, the icon will be a white exclamation mark on yellow background. For this situation, the user is asked to click on the icon for resetting the internet connection. If this action is successful, the icon will become green, if not, it will remain the same. For the second case, the user must check the settings of the router or call the support number displayed on Certus Software website www.certus.software.

The icon will be a white "x" on red background in case the software cannot reach the cloud server. There are three different scenarios which can cause this issue:

- The machine is not connected to a network – you should plug a network cable in the erasure machine or check for faulty cables;
- DNS resolution fails – you should check your network configuration;
- The cloud server is malfunctioning – you should contact Certus Software support immediately.

3.1.4. Help button

Click on the **Help** button to open a window in which the Certus Erasure User Manual is displayed for the current version of Certus Erasure.

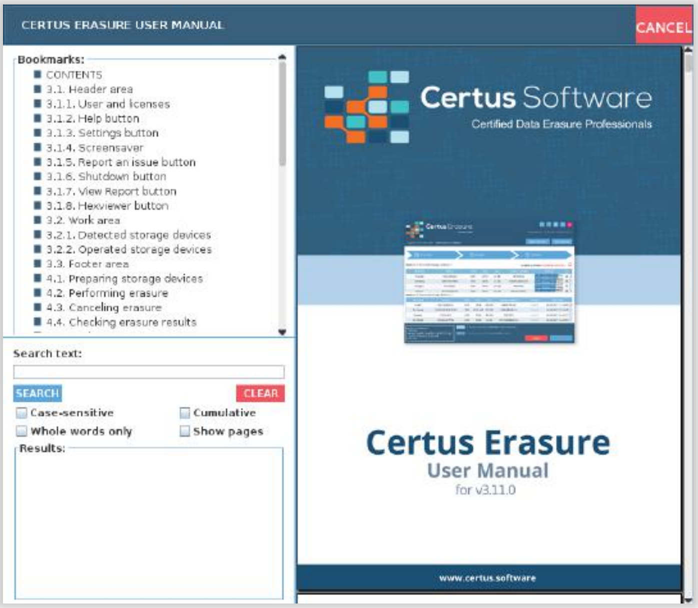


Fig. 3.4 User Manual window

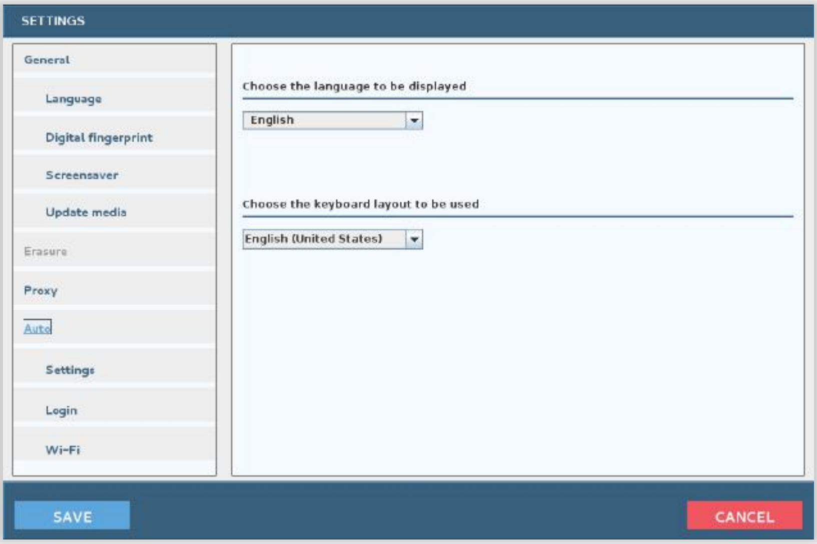
3.1.5. Settings button

The **Settings** button function is organized in 4 tabs:

- **General** with settings for language, digital fingerprint, screensaver and update ISO functionality;
- **Erasure** where the user can set the erasure pattern and the verification percentage;
- **Proxy** where the user can choose how to connect to internet: with or without proxy.
- **Auto** where the user can set several options related to automatic procedures.

Note that in the login screen the available tabs are General and Proxy. In the main interface the available tabs are General and Erasure. The Auto tab is available at all times, but it's options can only *be modified in the presence of a HASP key. Alternatively, those settings can be changed in the CEWM and at the next login in Certus Erasure, they will be imported from the CEWM.*

3.1.5.1. Language and keyboard tab



Choose the language to be displayed

English

Choose the keyboard layout to be used

English (United States)

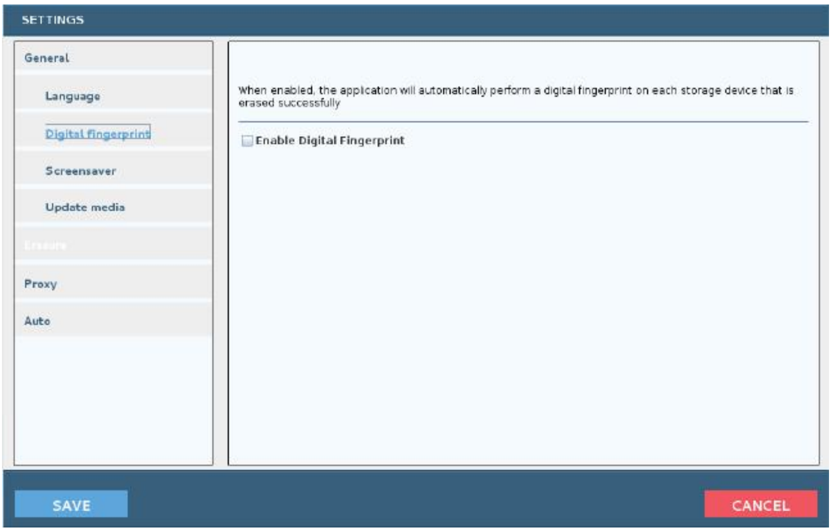
Fig. 3.5 Settings – Language tab

The user has the possibility to change the display language (which takes effect immediately) and between different keyboard layouts.

3.1.5.2. Digital Fingerprint tab

When enabled, Certus Erasure will digitally sign each storage device that is erased successfully. The digital signature consists of the following information:

- the time at which the erasure procedure took place;
- the name and the verification percent of the pattern that was used to erase the storage device;
- the version of the software that has been used;

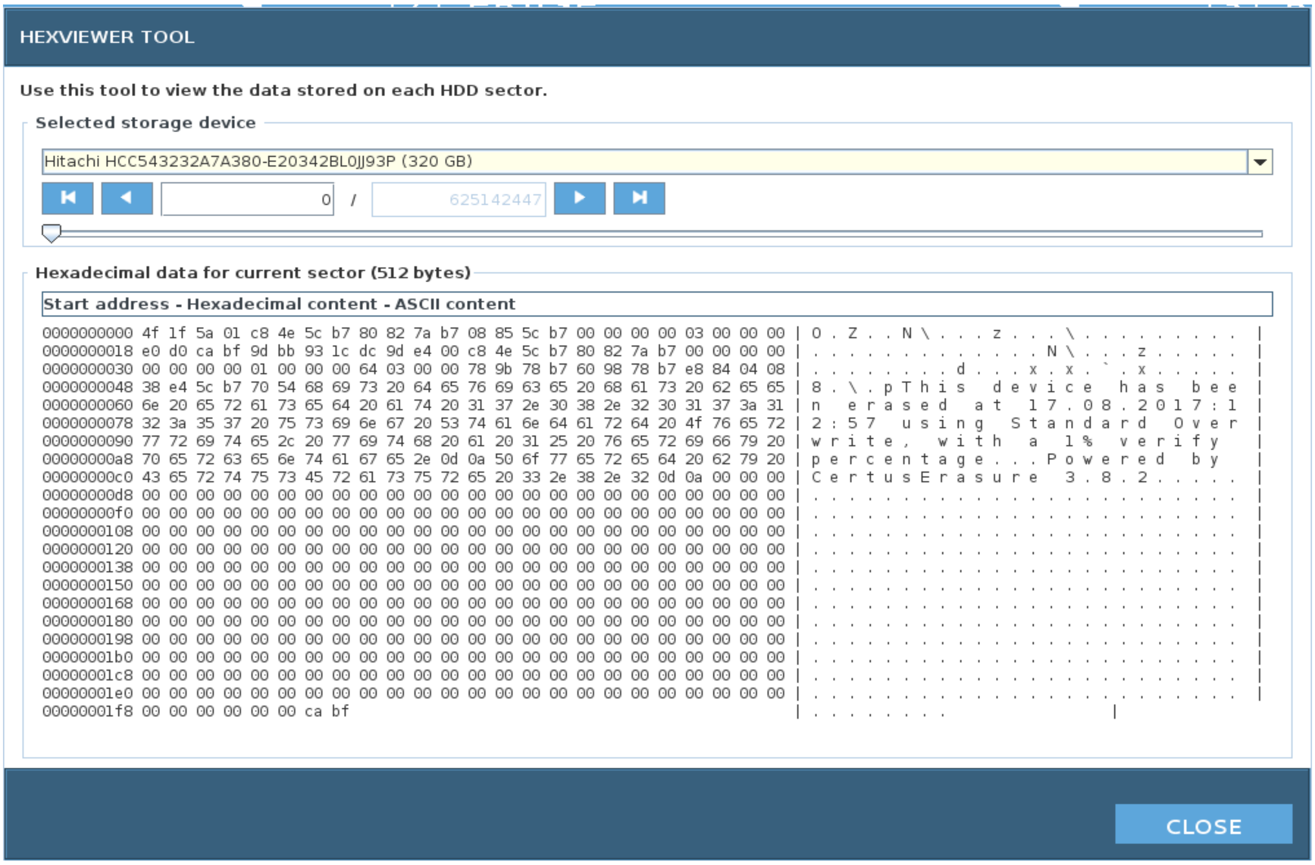


When enabled, the application will automatically perform a digital fingerprint on each storage device that is erased successfully

□ Enable Digital Fingerprint

Fig. 3.6 Settings – Digital fingerprint tab

After performing an erasure procedure, the user has the possibility to verify if the digital fingerprint took place. To do this, the user must select the Hexviewer button from the CE main window. Then in the “HEXVIEWER Tool” window, the user must select the storage device from the list and selector sector 0 to be displayed. In the ASCII table the information that has been signed on the storage device can be seen.



Use this tool to view the data stored on each HDD sector.

Selected storage device: Hitachi HCC543232A7A380-E20342BL0JJ93P (320 GB)

0 / 625142447

Hexadecimal data for current sector (512 bytes)

Start address - Hexadecimal content - ASCII content

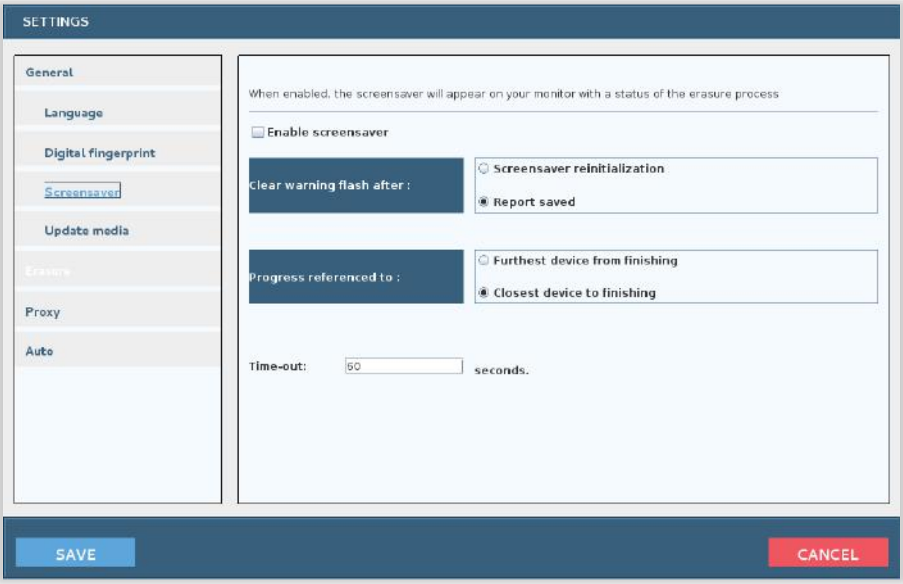
```
0000000000 4f 1f 5a 01 c8 4e 5c b7 80 82 7a b7 08 85 5c b7 00 00 00 00 03 00 00 00 | O . Z . . N \ . . . z . . . \ . . . . . . . . . |
0000000018 e0 d0 ca bf 9d bb 93 1c dc 9d e4 00 c8 4e 5c b7 80 82 7a b7 00 00 00 00 | . . . . . . . . . . . . . N \ . . . z . . . . . |
0000000030 00 00 00 00 01 00 00 00 64 03 00 00 78 9b 78 b7 60 98 78 b7 e8 84 04 08 | . . . . . . . . d . . . x . x . ` . x . . . . . |
0000000048 38 e4 5c b7 70 54 68 69 73 20 64 65 76 69 63 65 20 68 61 73 20 62 65 65 | 8 . \ . p T h i s   d e v i c e   h a s   b e e |
0000000060 6e 20 65 72 61 73 65 64 20 61 74 20 31 37 2e 30 38 2e 32 30 31 37 3a 31 | n   e r a s e d   a t   1 7 . 0 8 . 2 0 1 7 : 1 |
0000000078 32 3a 35 37 20 75 73 69 6e 67 20 53 74 61 6e 64 61 72 64 20 4f 76 65 72 | 2 : 5 7   u s i n g   S t a n d a r d   O v e r |
0000000090 77 72 69 74 65 2c 20 77 69 74 68 20 61 20 31 25 20 76 65 72 69 66 79 20 | w r i t e ,   w i t h   a   1 %   v e r i f y   |
00000000a8 70 65 72 63 65 6e 74 61 67 65 2e 0d 0a 50 6f 77 65 72 65 64 20 62 79 20 | p e r c e n t a g e . . . P o w e r e d   b y   |
00000000c0 43 65 72 74 75 73 45 72 61 73 75 72 65 20 33 2e 38 2e 32 0d 0a 00 00 00 | C e r t u s E r a s u r e   3 . 8 . 2 . . . . . |
00000000d8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | . . . . . . . . . . . . . . . . . . . . . . . . |
00000000f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | . . . . . . . . . . . . . . . . . . . . . . . . |
0000000108 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | . . . . . . . . . . . . . . . . . . . . . . . . |
0000000120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | . . . . . . . . . . . . . . . . . . . . . . . . |
0000000138 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | . . . . . . . . . . . . . . . . . . . . . . . . |
0000000150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | . . . . . . . . . . . . . . . . . . . . . . . . |
0000000168 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | . . . . . . . . . . . . . . . . . . . . . . . . |
0000000180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | . . . . . . . . . . . . . . . . . . . . . . . . |
0000000198 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | . . . . . . . . . . . . . . . . . . . . . . . . |
00000001b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | . . . . . . . . . . . . . . . . . . . . . . . . |
00000001c8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | . . . . . . . . . . . . . . . . . . . . . . . . |
00000001e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | . . . . . . . . . . . . . . . . . . . . . . . . |
00000001f8 00 00 00 00 00 00 ca bf                                                 | . . . . . . . .                 |
```

Fig. 3.7 Sector 0 of a digitally signed storage device

3.1.5.3. Screensaver tab

The user has the possibility to modify the following screensaver options:

- enable or disable screensaver by checking or unchecking the corresponding box.
- enable or disable the digital fingerprint feature.
- choose the way to clear the warning flash which notifies the errors of the erasure processes; the user has the option of clearing it after screen reinitialization or after the erasure report is saved.
- choose the information displayed regarding the progress of the erasure process – progress referenced to the longest time-consuming device (furthest device from finishing) or progress referenced to the shortest time-consuming device (closest device to finishing).
- choose the time-out - number of seconds before screensaver display; time cannot be less than 5 seconds; the default value is 60 seconds.



When enabled, the screensaver will appear on your monitor with a status of the erasure process

□ Enable screensaver

Clear warning flash after :
○ Screensaver reinitialization
● Report saved

Progress referenced to :
○ Furthest device from finishing
● Closest device to finishing

Time-out: 60 seconds.

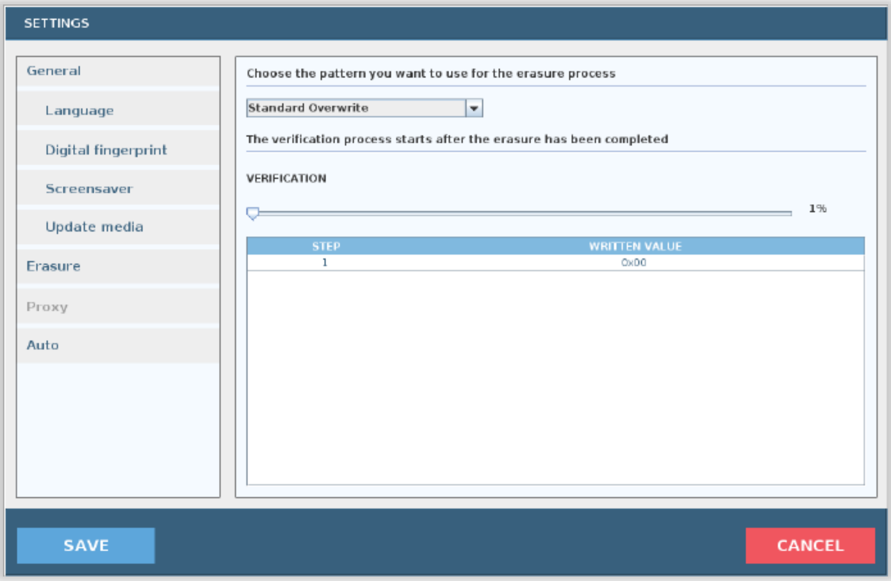
Fig. 3.8 Settings – Screensaver tab

3.1.5.4. Erasure tab

The erasure tab contains the main settings which are used when wiping devices: **erasure pattern** and **verification**.

Certus Erasure currently provides 14 *erasure patterns* which are detailed in the **ERASURE PATTERNS** chapter. The *verification* setting lets the user set a percentage of the overwritten data to be verified, in order to be sure that the erasure process successfully took place; the verification value can be set from 1% to 100%, the default being 1%.

NOTE: Please pay attention when configuring the erasure settings, and set the appropriate values according to the chosen standard and your internal security requirements, before starting the erasure process.



Choose the pattern you want to use for the erasure process

Standard Overwrite

The verification process starts after the erasure has been completed

VERIFICATION

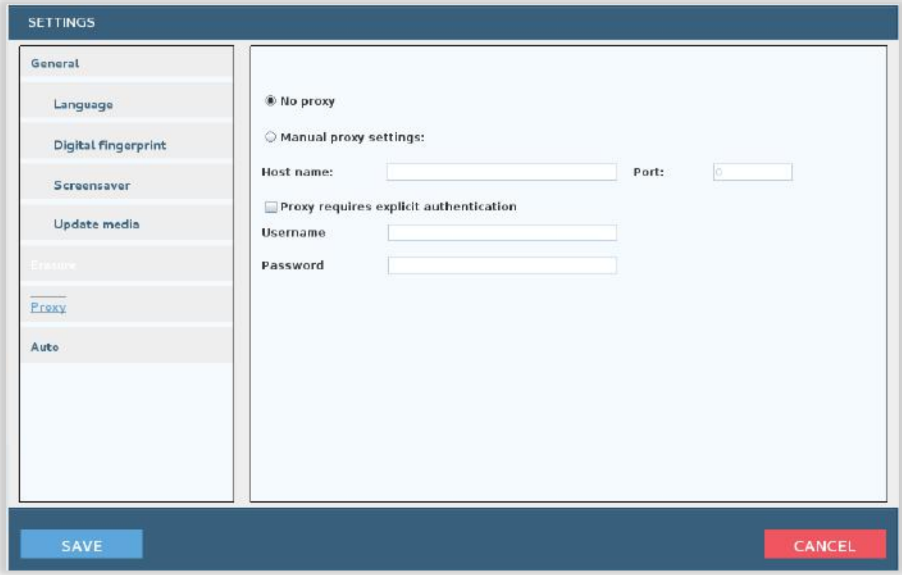
1%

STEP	WRITTEN VALUE
1	0x00

Fig. 3.9 Settings - Erasure tab

3.1.5.5. Proxy tab

A proxy can be configured for connecting to the internet through it in the proxy tab. Note that if the connection to the proxy server requires authentication, they must be completed in the respective fields.



● No proxy

○ Manual proxy settings:

Host name: Port: 0

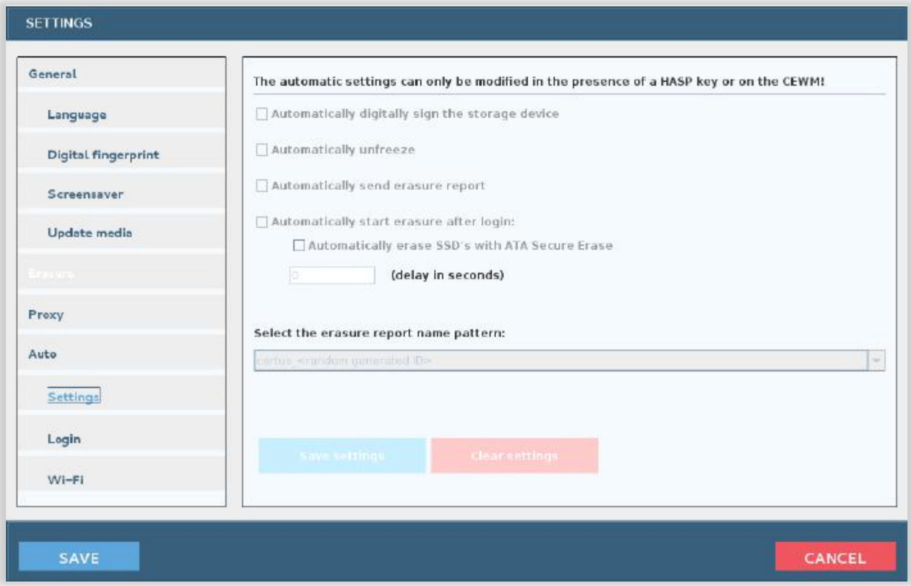
□ Proxy requires explicit authentication

Username

Password

Fig. 3.10 Settings - Proxy tab

3.1.5.6. Automatic procedures tab



The automatic settings can only be modified in the presence of a HASP key or on the CEWM!

□ Automatically digitally sign the storage device

□ Automatically unfreeze

□ Automatically send erasure report

□ Automatically start erasure after login:

□ Automatically erase SSD's with ATA Secure Erase

0 (delay in seconds)

Select the erasure report name pattern:

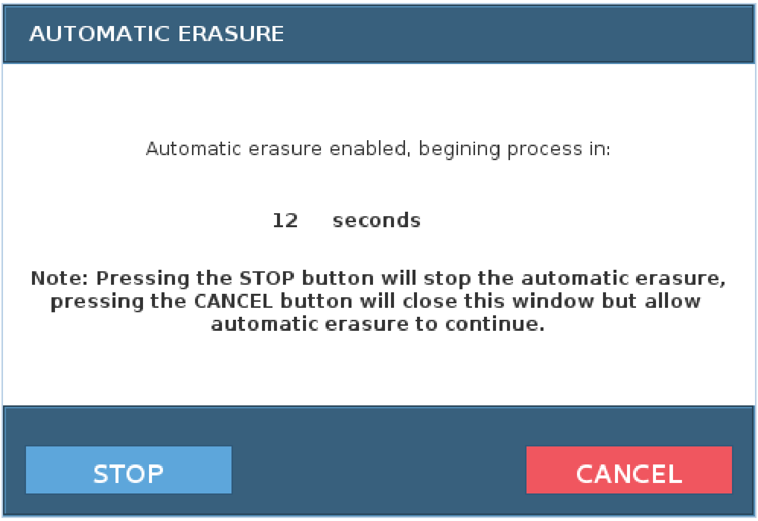
certus_<random generated ID>

Fig. 3.11 Settings - Auto settings tab

The **Auto Settings** tab provides the user with the following options:

- Automatically digitally sign the storage device
  - When enabled, the application will automatically perform a digital fingerprint on each storage device whose erasure has finished with success;

- Automatically unfreeze
    - When enabled, the application will automatically perform an unfreeze operation when detecting a storage device which is **FROZEN**;
- Automatically send erasure report
    - When enabled, the application will automatically upload the erasure report after each erasure that finishes;
- Automatically start erasure after logging in
    - When enabled, the application will automatically select all the storage devices in the table and start an erasure on each of them;
    - If the user whishes this automatic erasure procedure to be delayed with a certain period, he can set up an optional delay in seconds. The application will display a window with a countdown timer related to that delay, and allow the user to either stop the automatic erasure or allow it to continue.



AUTOMATIC ERASURE

Automatic erasure enabled, begining process in:

12 seconds

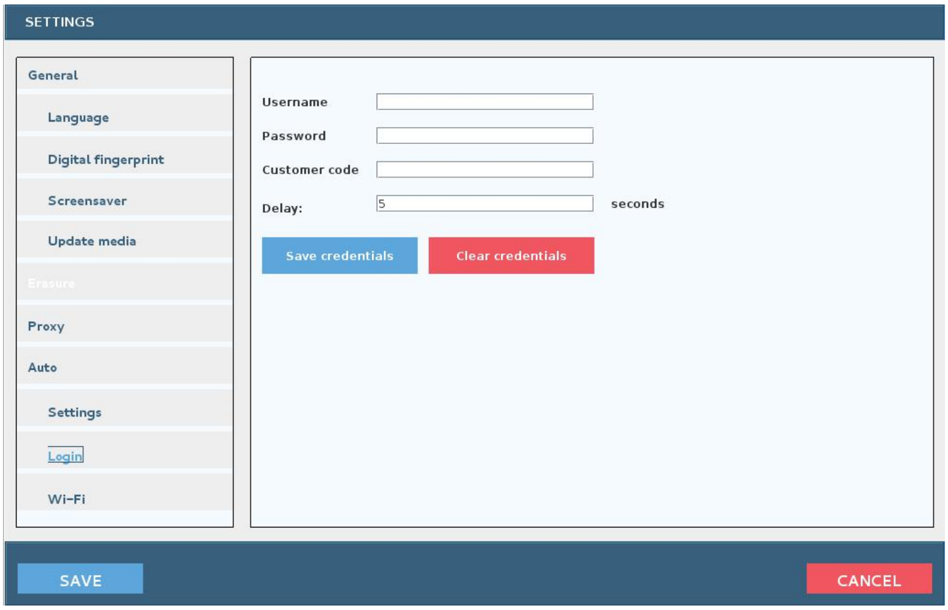
Note: Pressing the STOP button will stop the automatic erasure, pressing the CANCEL button will close this window but allow automatic erasure to continue.

Fig. 3.12 Automatic erasure window

- Automatically erase SSD with ATA Secure Erase
    - When enabled with the automatic erasure, the application will automatically perform the ATA Secure Erase on all the storage devices that are SSD's;
- Customize the report name
    - When enabled, the document ID of the erasure will be set with the following format:
        - Serial number of the motherboard on which the application is running
        - Underscore character (_)
        - Serial number of the first storage device in the table
    - In case there are no storage devices detected, the last part will be comprised of a default value "no_storage_device".

Note: The options above can be modified either on CEWM, if the operator has been provided with the ability to edit his automatic settings (if not, they can be set by the administrator), either on Certus Erasure if the operator has used a HASP key to log in.

The **Auto Login** tab provides the user with the possibility to save the credentials on the media, so that the next time the application boots up, it will automatically try to log in with those credentials. When choosing to save the credentials, Certus will verify if the credentials are valid and only if they pass the validation they are saved on the media. The user also has the possibility to clear the credentials from the media.



Username

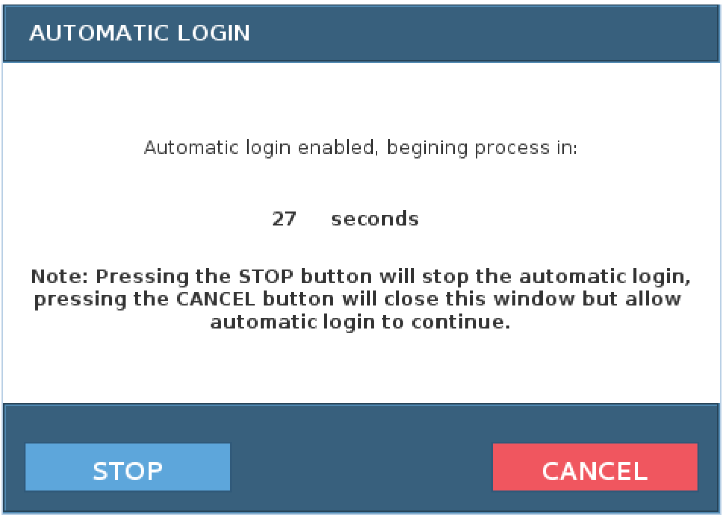
Password

Customer code

Delay: 5 seconds

Fig. 3.13 Settings - Auto login tab

If the application detects saved credentials on the media, it will display a window in which the user has the possibility to stop the automatic login procedure.



Automatic login enabled, begining process in:

27 seconds

Note: Pressing the STOP button will stop the automatic login, pressing the CANCEL button will close this window but allow automatic login to continue.

Fig. 3.14 Automatic login window

Note: After clearing the media, a reboot is required for the change to take place.

The **Auto Wi-Fi** tab provides the user with the possibility to save the information used to connect to a wireless network, so that the next time the application boots up, it will automatically try to connect to that wireless network. When choosing to save the credentials, Certus will verify if the wireless network is present and attempt to connect to it. If the connection succeeds, then Certus will save the data on the media, if the connection fails, it will not save the data and inform the user that the network is unreachable.

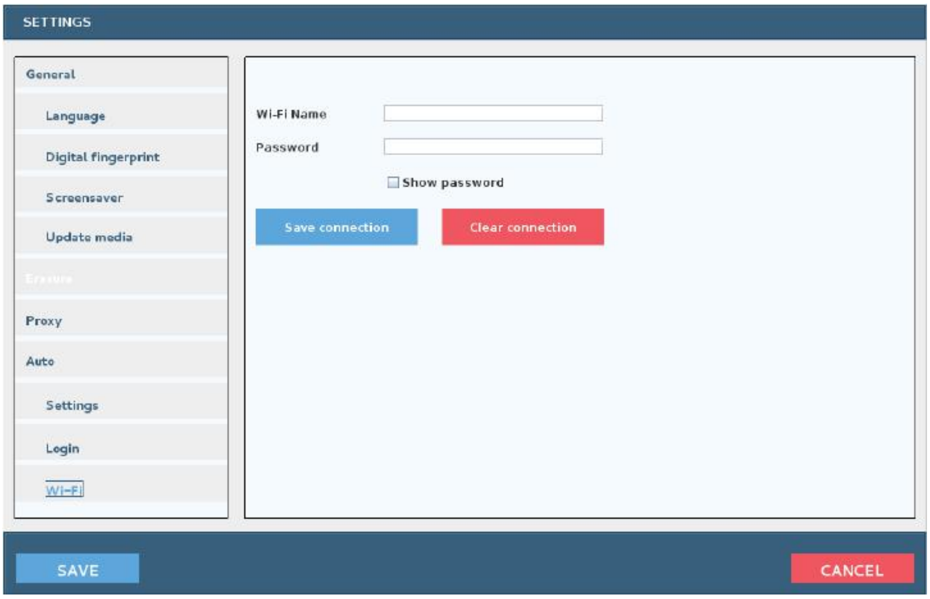


Fig. 3.15 Settings – Auto Wi-Fi tab

Note: After clearing the media, a reboot is required for the change to take place.

3.1.6. Screensaver

The Certus screensaver shows the progress of all erasure processes on the computer.
It displays:

- the erasure progress bar;
- a percentage of the average progress of the erasure processes;
- the average time left to complete the erasure(s).

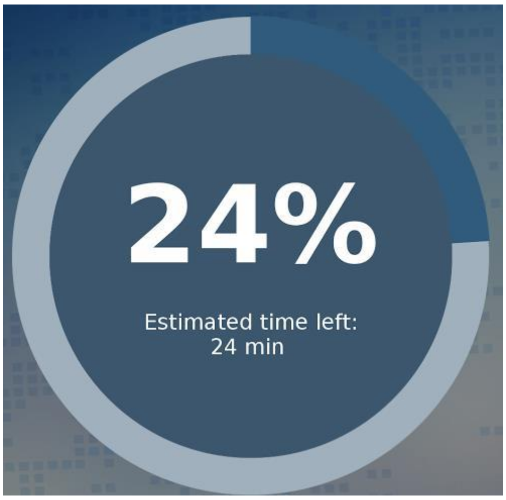


Fig. 3.16 Screensaver – progress bar

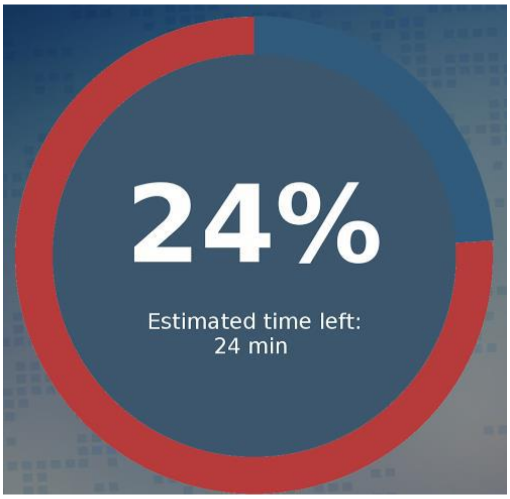
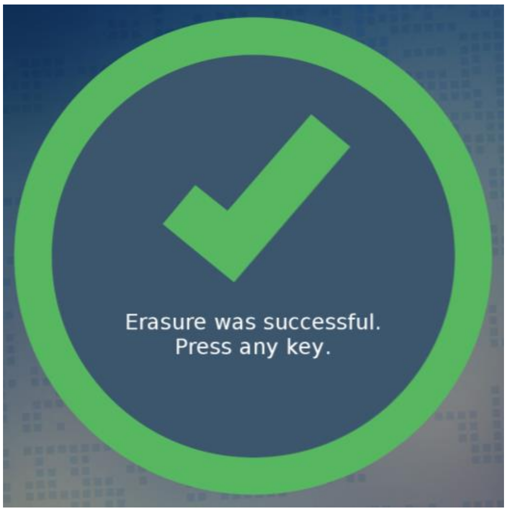


Fig. 3.17 Screensaver – progress bar with warning

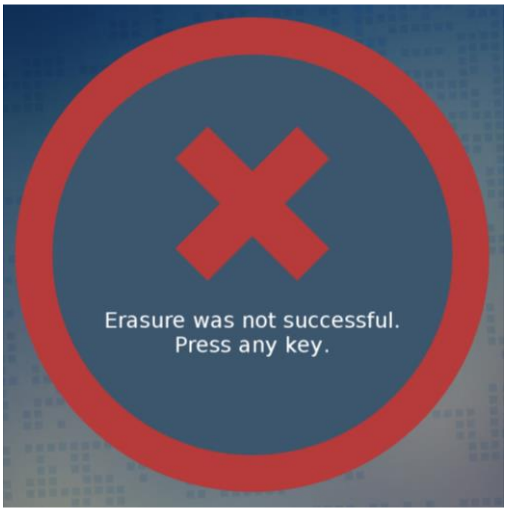
If any errors occur during the erasure process, the screensaver will provide a notification of this by shifting the color of the progress bar between grey (default color) and red.

The screensaver provides a good overview of the result, whether all erasure processes are successful (green icon) or at least one erasure process is failed/canceled (red icon).



Erasure was successful.
Press any key.

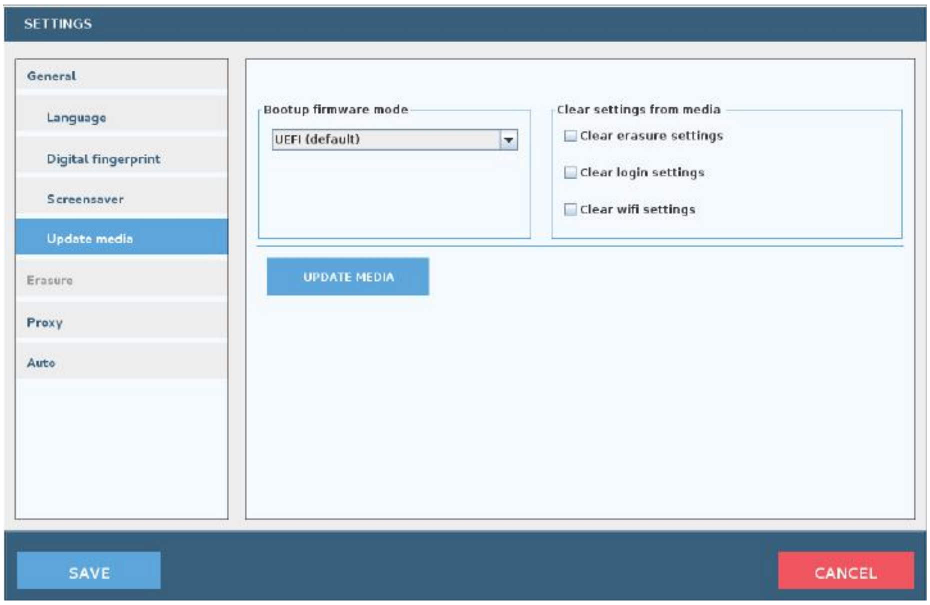
Fig. 3.18 Screensaver – Successful erasure



Erasure was not successful.
Press any key.

Fig. 3.19 Screensaver – Failed erasure

3.1.7. Update ISO



Bootup firmware mode: UEFI (default)

Clear settings from media
□ Clear erasure settings
□ Clear login settings
□ Clear wifi settings

Fig. 3.17 Settings – Update Media

The application will verify if it is currently running the latest available version when the user logs in, and in case it detects a newer version on the CEWS (Certus Erasure Web Server), it will notify the user by displaying a pop-up in which he is prompted to update his version.

To update the Certus Erasure software, the user should press the F3 key (or click on the Settings icon), and there go the Update Media section where he should choose the type of ISO to download (whether

UEFI or **BIOS**). It is recommended to use the same type as he previously used for installing Certus Erasure on the USB.

UEFI and BIOS represent two firmware interfaces for computers which are used at the startup of the computer to initialize the hardware components and start the operating system stored on a storage device. The difference between them resides in the way they boot up the system. The user is advised to first try to use the BIOS ISO image. In case this fails, he should try the UEFI ISO image.

Note that the user also has the possibility to remove any type of stored automatic settings on the media if he wants to. To remove them, the user must check any of the three boxes before pressing the **UPDATE MEDIA** button.

After that, the user must make sure that the USB stick used to start Certus Erasure is still plugged into the computer, and he should press the **UPDATE MEDIA** button. If no error occurs during the process of updating the software, the user will be notified, after the process is finished, that the update is successful and he should reboot the computer. The errors that can occur during the process are the following:

1. **Target media is up to date!**

This means that the user is already running the latest available version of Certus Erasure.

2. **No target media connected!**

This means that there is no USB stick with Certus Erasure installed on it currently plugged into the computer. Please insert your USB stick with Certus Erasure installed on it.

3. **Not enough RAM!**

This means that the computer where Certus Erasure is running has an insufficient amount of RAM available for the process to begin. The user is advised to use Certus Erasure on a computer with more amount of RAM available.

4. **Integrity check failed!**

This means that the file that has been downloaded is corrupted and cannot be written to the disk. The user is advised to reboot Certus Erasure and try again.

5. **Target unmount failed!**

This means that the USB stick plugged into the computer has failed to unmount itself. The user is advised to use another USB port to plug the stick.

6. **Too many target devices!**

This means that there is more than one USB stick with Certus Erasure on it that are plugged into the computer. The user is advised to remove all other USB devices and keep only one USB with Certus Erasure installed on it.

7. **Download failed!**

This means that an error has occurred during the download of the ISO image. The user should check his internet connection, reboot the computer and try again.

8. **Write to target failed!**

This means that an error has occurred during the writing of the ISO image to the USB stick. The user is advised to use another USB slot for the USB device with Certus on it.

9. **Target media unplugged during writing!**

This means that the USB stick has been unplugged while the ISO image was still being written to it. The user should not remove the USB device until the application notifies him that the update has taken place.

3.1.8. Report an issue button

! If issues are found, they can be reported by pressing **Report an issue** button. Inside Report an issue window, the user can write a description of the problem encountered while using Certus Erasure.

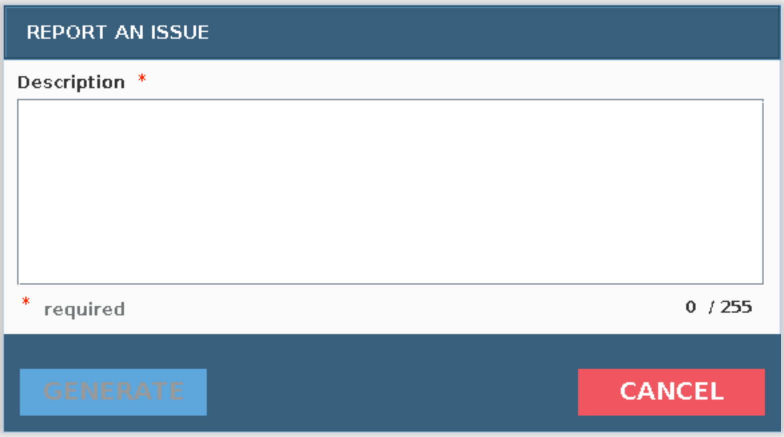
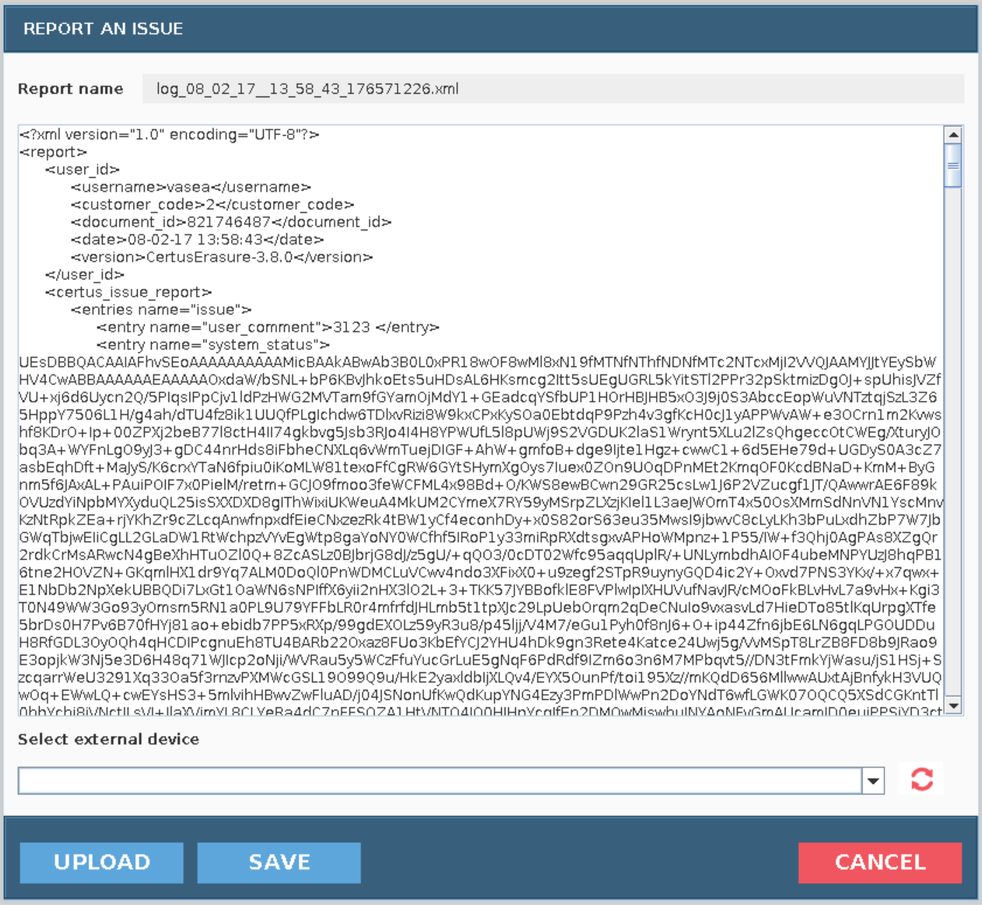


Fig. 3.20 Report an issue – Description

Pressing the **Generate** button leads to an XML report which can be saved to a removable device or can be uploaded to server.



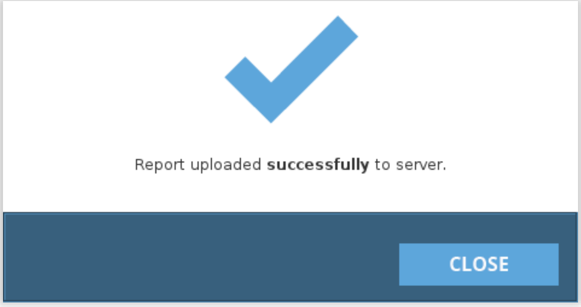
Report name log_08_02_17__13_58_43_176571226.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<report>
    <user_id>
        <username>vasea</username>
        <customer_code>2</customer_code>
        <document_id>821746487</document_id>
        <date>08-02-17 13:58:43</date>
        <version>CertusErasure-3.8.0</version>
    </user_id>
    <certus_issue_report>
        <entries name="issue">
            <entry name="user_comment">3123 </entry>
            <entry name="system_status">
UEsDBBQACAAIAFhvSEoAAAAAAAAAAAMicBAAkABwAb3B0L0xPR18wOF8wMl8xN19fMTNfNThfNDNfMTc2NTcxMjI2VVQJAAMYJJtYEySbW
HV4CwABBAAAAAAEAAAAAOxdaW/bSNL+bP6KBvJhkoEts5uHDsAL6HKsmcg2Itt5sUEgUGRL5kYitSTl2PPr32pSktmizDgOJ+spUhisJVZf
VU+xj6d6Uycn2Q/5PIqsIPpCjv1ldPzHWG2MVTam9fGYamOjMdY1+GEadcqYSfbUP1HOrHBJHB5xO3J9j0S3AbccEopWuVNTztqjSzL3Z6
5HppY7506L1H/g4ah/dTU4fz8ik1UUQfPLgIchdw6TDlxvRizi8W9kxCPxKySOa0EbtdqP9Pzh4v3gfKcH0cJ1yAPPWvAW+e3OCrn1m2Kvws
hf8KDrO+Ip+00ZPXj2beB77l8ctH4Il74gkbvg5Jsb3RJo4I4H8YPWUfL5l8pUWj9S2VGDUK2laS1Wrynt5XLu2lZsQhgeccOtCWEg/XturyJO
bq3A+WYFnLgO9yJ3+gDC44nrHds8iFbheCNXLq6vWmTuejDIGF+AhW+gmfoB+dge9Ijte1Hgz+cwwC1+6d5EHe79d+UGDyS0A3cZ7
asbEqhDft+MaJyS/K6crxYTaN6fpiu0iKoMLW81texoFfCgRW6GYtSHymXgOys7Iuex0ZOn9UOqDPnMEt2KmqOF0KcdBNaD+KmM+ByG
nm5f6JAxAL+PAuiPOIF7x0PielM/retm+GCJO9fmoo3feWCFML4x98Bd+O/KWS8ewBCwn29GR25csLw1J6P2VZucgf1JT/QAwwrAE6F89k
OVUzdYiNpbMYXyduQL25isSXXDXD8gIThWixiUKWeuA4MkUM2CYmeX7RY59yMSrpZLXzjKlel1L3aeJWOmT4x50OsXMmSdNnVN1YscMnv
KzNtRpkZEa+rjYKhZr9cZLcqAnwfnpxdfEieCNxzezRk4tBW1yCf4econhDy+x0S82orS63eu35MwsI9jbwvC8cLyLKh3bPuLxdhZbP7W7Jb
GWqTbjwEliCgLL2GLaDW1RtWchpzVYvEgWtp8gaYoNY0WCfhf5IRoP1y33miRpRXdtsgxvAPHoWMpnz+1P55/IW+f3Qhj0AgPAs8XZgQr
2rdkCrMsARwcN4gBeXhHTuOZl0Q+8ZcASLz0BJbrjG8dJ/z5gU/+qQO3/0cDT02Wfc95aqqUplR/+UNLymbdhAIOF4ubeMNPYUzJ8hqPB1
6tne2HOVZN+GKqmlHX1dr9Yq7ALM0DoQl0PnWDMCLuVCwv4ndo3XFixX0+u9zegf2STpR9uynyGQD4ic2Y+Oxvd7PNS3YKx/+x7qwx+
E1NbDb2NpXekUBBQDi7LxGt1OaWN6sNPIffX6yii2nHX3lO2L+3+TKK57JYBBofklE8FVPlwIpIXHUVufNavJR/cMOoFkBLvHvL7a9vHx+Kgi3
T0N49WW3Go93yOmsm5RN1a0PL9U79YFFbLR0r4mfrfdJHLmb5t1tpXJc29LpUebOrqm2qDeCNuIo9vxasvLd7HieDTo85tlKqUrpgXTfe
5brDs0H7Pv6B70fHYj81ao+ebidb7PP5xRXp/99gdEXOLz59yR3u8/p45ljj/V4M7/eGu1Pyh0f8nJ6+O+ip44Zfn6jbE6LN6gqLPGOUDDu
H8RfGDL3OyOQh4qHCDIPcgnuEh8TU4BARb22Oxaz8FUo3KbEfYCJ2YHU4hDk9gn3Rete4Katce24Uwj5g/VvMSpT8LrZB8FD8b9JRao9
E3opjkW3Nj5e3D6H48q71WJIcp2oNji/WVRau5y5WCzFfuYucGrLuE5gNqF6PdRdf9IZm6o3n6M7MPbqvt5//DN3tFmkYjWasu/jS1HSj+S
zcqarrWeU3291Xq33Oa5f3rnzvPXMWcGSL19O99Q9u/HkE2yaxldbIjXLQv4/EYX5OunPf/toi195Xz//mKQdD656MllwwAUxtAjBnfykH3VUQ
wOq+EWwLQ+cwEYsHS3+5mlvihHBwvZwFluAD/j04JSNonUfKwQdKupYNG4Ezy3PmPDlWwPn2DoYNdT6wfLGWK07OQCQ5XSdCGKntTl
0bbYchi8iVNctILsVl+IlaXVimYL8CLYeBa4dC7nFESOZA1HtVNTO4IO0HIHnYcqIfEn2DMOwMiswbuINYAoNFvGmAUcamID0euiPPSiYD3ct
```

Select external device

Fig. 3.21 Report an issue – XML report

If the upload to server or the saving to removable device is successful, one of the following windows will appear:


Report uploaded **successfully** to server.

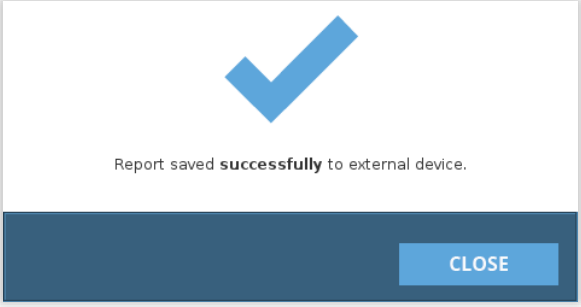
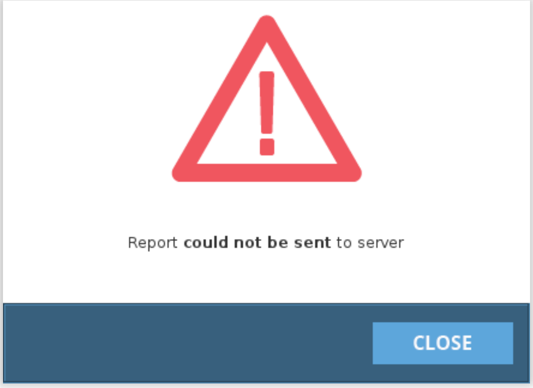

Report saved **successfully** to external device.

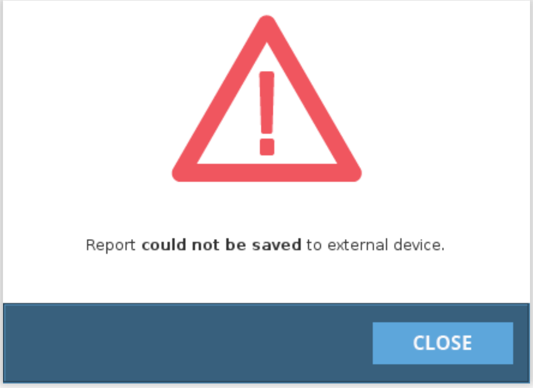
Fig. 3.22 Report saved successfully to server

Fig. 3.23 Report saved successfully to external device

If the upload to server or the saving to removable device is unsuccessful, one of the following windows will appear:



Report **could not be sent** to server



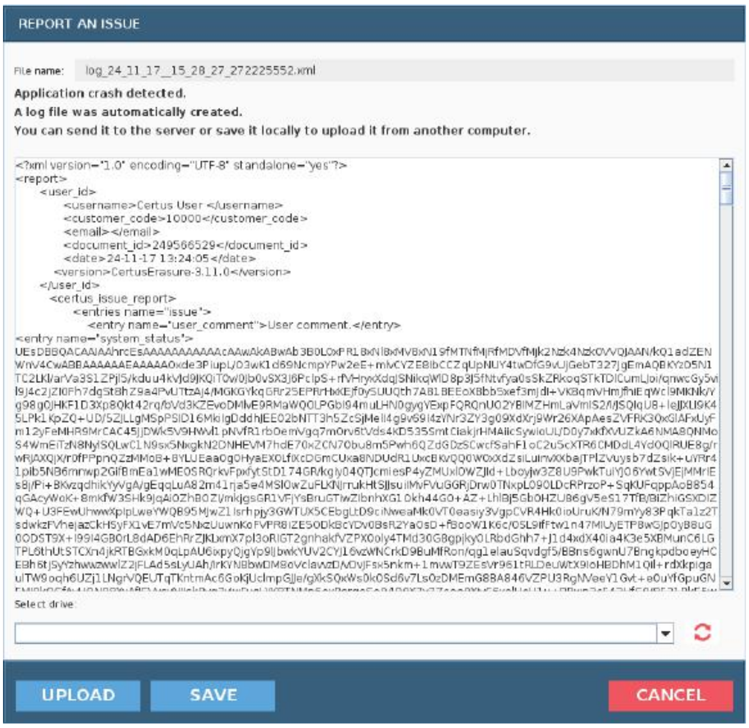
Report **could not be saved** to external device.

Fig. 3.24 Report saved unsuccessfully to server

Fig. 3.25 Report saved unsuccessfully to external device

3.1.9. Automatic issue report

Should the application encounter a critical error and crash or shut down, a log file will be automatically created with the error details and the application will be restarted. After restarting, it will first present to the user the option to upload to the CEWM or save the log and upload it on another computer so that the Certus team can analyze it and come back with a resolution as to why the error occurred.



File name: log_24_11_17__15_28_27_272225552.xml

Application crash detected.

A log file was automatically created.

You can send it to the server or save it locally to upload it from another computer.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<report>
    <user_id>
        <username>Certus User </username>
        <customer_code>10000</customer_code>
        <email></email>
        <document_id>249566529</document_id>
        <date>24-11-17 13:24:05</date>
      <version>CertusErasure-3.11.0</version>
    </user_id>
      <certus_issue_report>
          <entries name="issue">
            <entry name="user_comment">User comment.</entry>
<entry name="system_status">
```

UEsDBBQACAAIAAhrcEsAAAAAAAAAAAAcAAwAkABwAb3B0LOxPR1BxNlBxMVBxN19fMTNfMjRfMDVfMjk2Nzk4NzkOVVQJAAN/kQ1adZEN
WnV4CwABBAAAAAAEAAAAAOxde3PiupL/O3wK1d69NcmpYPw2eE+mMCYZE8IbCCZqUpNUY4twDfG9vUjGebT327jgEmAQBKYzD5N1
TC2LKl/arVa3S1ZPjl5/kduu4kVJd9JKQiT0w0Jb0vSX3J6PclpS+rfVHryxXdqJSNikqWID8p3J5fNtvfya0sSkZRkoqSTkTDICumLJoi/qnwcGy5vi
l9J4c2jZI0Fh7dqSt8hZ9a4PvUTtzAj4/MGKGYkqGRr25EPRrHxKEjf0ySUUQth7AB1BEEoXBbb5xef3mJdI+VK8qmVHmJfhIEqWcl9MKNk/Y
g98g0JHKF1D3Xp8Qkt42rq/bVd3KZEvoDMlvE9RMaWQ0LPGbI94muLHN0gygYExpFQRQnU02YBIMZHmLaVmlS2/l/JSQlqU8+leJJXLI9K4
5LPk1KpZQ+UD/5ZJLLgMSpPSID16MkIgDddhJEE02bNTT3h5ZcSjMeII4g9v69I4zYNr3ZY3g09XdXrj9Wr26XApAesZVFRK3QxGIAFxUyF
m12yFeMHR9MrCAC45jJDWk5V9HWvl1pNVfR1rb0emVgq7m0rv6tVds4KD535SmtCiakjrHMAiicSywioUL/D0y7xKfXVUZkA6NMA8QNMo
S4WmEiTzN8NyISQLwC1N9sx5NxgkN2DNHEVM7hdE70xZCN70bu8m5Pwh6QZdGDzSCwcfSahF1oC2u5cXTR6CMDdL4YdOQIRUE8g/r
wRJAXQjX/r0fPPpnQZzMMoB+BYLUEaaOg0HyaEX0LfXcDGmCUxa8NDUdR1UxcBKvQQ0WOxXdZsiLuinvXXbajTPlZVuysb7dZsik+uYRr4
1pib5NB6mnwp2GifBmEa1wME0SRQrkvFpxfytStD174GR/kgIy04QTJcmiesP4yZMUxl0WZJId+Lboyjw3Z8U9PwkTuIYJ06YwtSVjEjMMrIE
s8j/Pi+BKvzqdhikYyVgA/gEqqLuA82m41ria5e4MSl0wZuFLKNjrrukHtSJJsuiIMvFVuGGRjDrw0TNxpL090LDcRPrzoP+SqKUFqppAoB854
qGAcyWoK+8mKfW3SHk9JqAi0ZhB0ZI/mkjgsGR1VFjYsBruGTIwZIbnhXG10kh44G0+AZ+LhlBj5Gb0HZUB6gV5eS17TfB/BiZhiGSXDIZ
WQ+U3FEwUhwwXpIpLweYWQB95MJwZ1IsrhpjY3GWTUX5CEbgLtD9ciNweaMk0VT0easiy3VgpCVR4Hk0ioUruK/N79mYy83PqkTa1z2T
sdwkzFVhejazCkHSyFX1vE7mVc5NxzUuwnKoFVPR8IZE50DkBcYDv0BsRZYa0sD+fBooW1K6c/05L9ifFtw1n47MlUyETPBwGJp0yB8uG
0ODST9X+I99I4GB0rL8dAD6EhRrZJKLxmX7pl3oRIGT2gnhakfVZPX0oly4TMd30GBgpjky0LRbdGhh7+J1d4xdX40ia4K3e5XBMunC6LG
TPL6thUtSTCXn4jkRTBGxkM0qLpAU6xpyQjgYp9lJbwkYUV2CYJ16vzWNCrkD9BuMfRon/qg1elauSqvdgf5/BBns6gwnU7BngkpdboeyHC
EBh6tJSyYzhwwzwwlZ2jFLAd5sLyUAh/IrKYNBbwDM8oVclawzD/VDvJFsx5nkm+1mwT9ZEsVr961tRLDeUWtX9loHBDhM1QlI+rdXkpiga
uITW9oqh6UZj1LNgrVQEUTqTKntmAc6GoKjUclmpGJJe/gXkSQxWs0k0Sd6v7Ls0zDMEmG8BA846VZPU3RgNVeeY1Gvt+e0uYfGpuGN

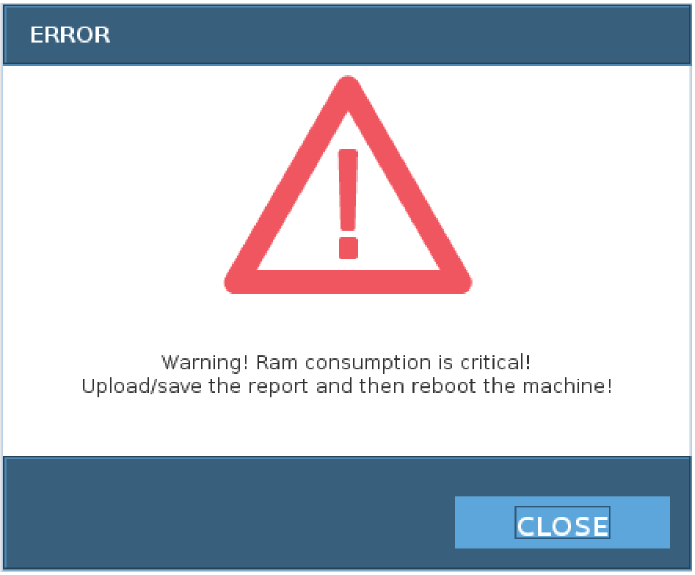
Select drive:

Fig. 3.26 Automatic issue window

Note: This issue window will appear before the login window.

3.1.10. RAM monitoring

The application constantly monitors the available RAM and should it ever encounter a situation where the amount of available RAM is insufficient, it will notify the user to save or upload the report and reboot the machine.



ERROR

Warning! Ram consumption is critical!
Upload/save the report and then reboot the machine!

Fig. 3.27 RAM notification window

3.1.11. Shutdown button

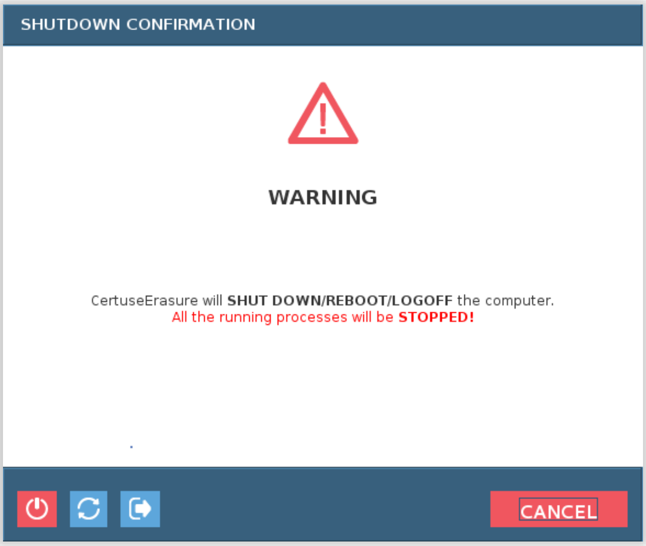
To shut down the machine click the **Shutdown** button. The user can confirm the shutting down of the machine by pressing **Shutdown** button or cancel the action by pressing **Cancel** button.

The **Reboot** button allows restarting the machine on which Certus Erasure software is running

To access this function, the user should press the Shutdown button, from the header Area and then click on the **Reboot** button from the new opened window.

The **Log off** button allows the user to log off the current account and go back to the **Login** window.

To access this function, the user should press the Shutdown button, from the header Area and then click on the **Log off** button from the new opened window.



SHUTDOWN CONFIRMATION

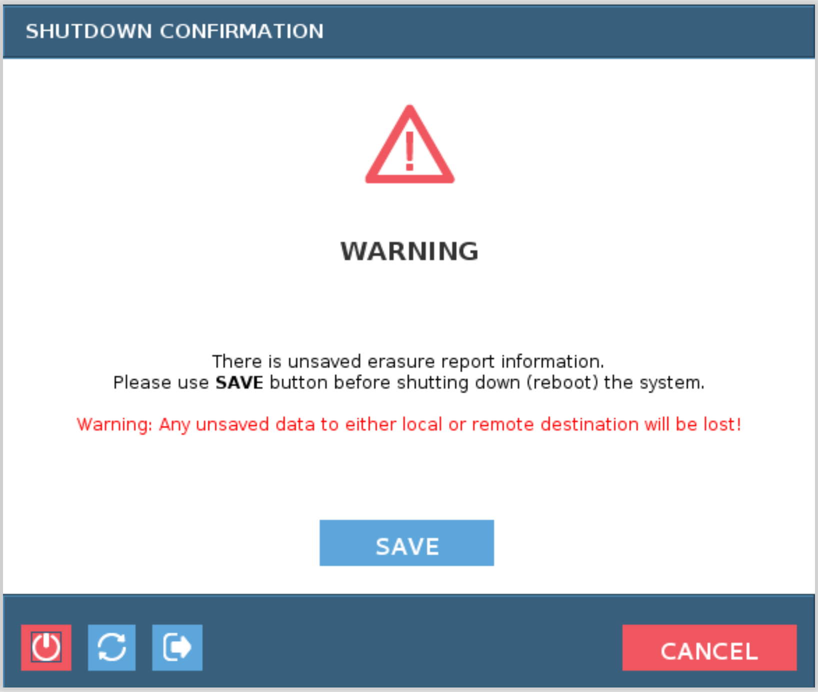
WARNING

CertuseErasure will **SHUT DOWN/REBOOT/LOGOFF** the computer.
All the running processes will be **STOPPED!**

Fig. 3.28 Shutdown dialog

If one or more erasures took place and no report has been saved, a different pop-up window appears.

- If the user clicks the **Shutdown** or the **Reboot** button, the action will be confirmed, but no report will be saved;
- If the user clicks **Save** button, he will be redirected to **Save report** dialog;
- If the user clicks **Cancel** button, the action will be canceled.



SHUTDOWN CONFIRMATION

WARNING

There is unsaved erasure report information.
Please use **SAVE** button before shutting down (reboot) the system.

Warning: Any unsaved data to either local or remote destination will be lost!

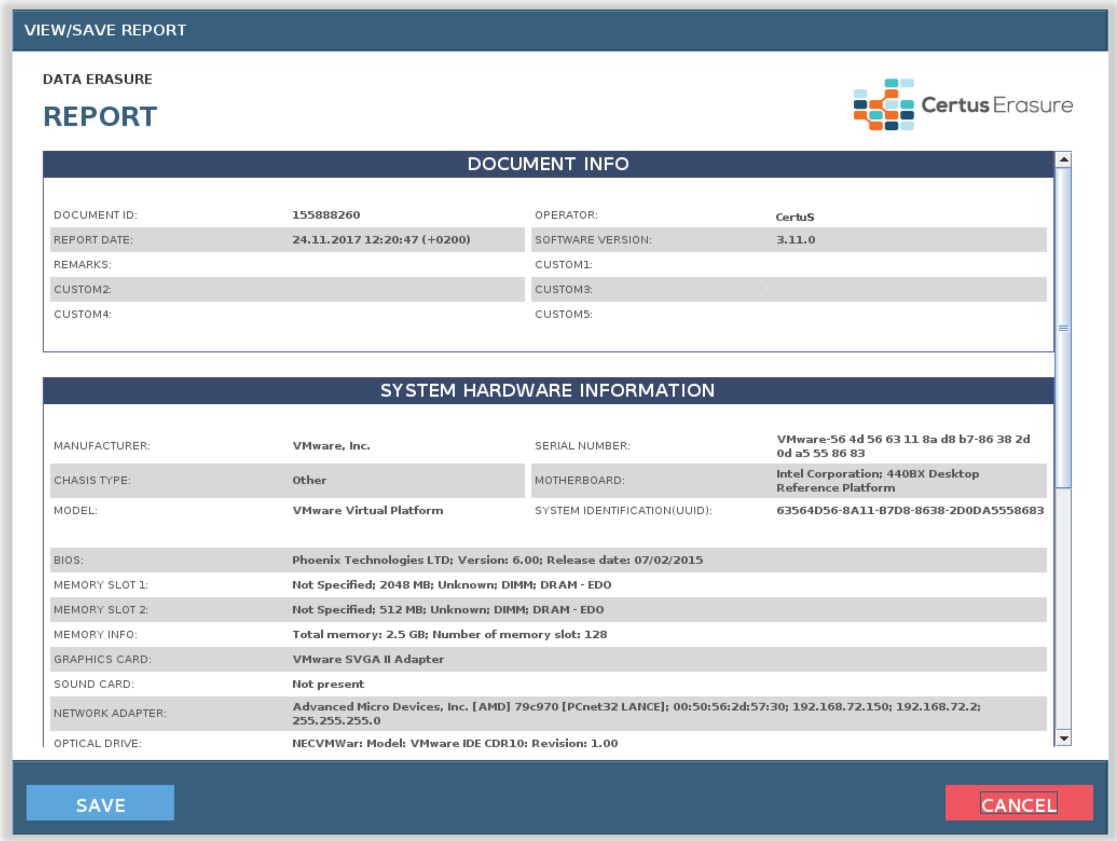
Fig. 3.29 Shutdown confirmation dialog

3.1.12. View Report button

VIEW/SAVE REPORT

Pressing this button opens the Data Erasure Report. The report contains detailed information regarding:

- the document - document ID, report date, software version, operator and custom fields;
- the system hardware - information about the erasure machine;
- the erasure - information about erased device(s) and erasure process results.



DATA ERASURE

REPORT

DOCUMENT INFO

DOCUMENT ID:	155888260	OPERATOR:	CertuS
REPORT DATE:	24.11.2017 12:20:47 (+0200)	SOFTWARE VERSION:	3.11.0
REMARKS:		CUSTOM1:	
CUSTOM2:		CUSTOM3:	
CUSTOM4:		CUSTOM5:	

SYSTEM HARDWARE INFORMATION

MANUFACTURER:	VMware, Inc.	SERIAL NUMBER:	VMware-56 4d 56 63 11 8a d8 b7-86 38 2d 0d a5 55 86 83
CHASIS TYPE:	Other	MOTHERBOARD:	Intel Corporation; 440BX Desktop Reference Platform
MODEL:	VMware Virtual Platform	SYSTEM IDENTIFICATION(UUID):	63564D56-8A11-B7D8-8638-2D0DA5558683

BIOS:	Phoenix Technologies LTD; Version: 6.00; Release date: 07/02/2015
MEMORY SLOT 1:	Not Specified; 2048 MB; Unknown; DIMM; DRAM - EDO
MEMORY SLOT 2:	Not Specified; 512 MB; Unknown; DIMM; DRAM - EDO
MEMORY INFO:	Total memory: 2.5 GB; Number of memory slot: 128
GRAPHICS CARD:	VMware SVGA II Adapter
SOUND CARD:	Not present
NETWORK ADAPTER:	Advanced Micro Devices, Inc. [AMD] 79c970 [PCnet32 LANCE]; 00:50:56:2d:57:30; 192.168.72.150; 192.168.72.2; 255.255.255.0
OPTICAL DRIVE:	NECVMWar: Model: VMware IDE CDR10: Revision: 1.00

Fig. 3.30 View report window

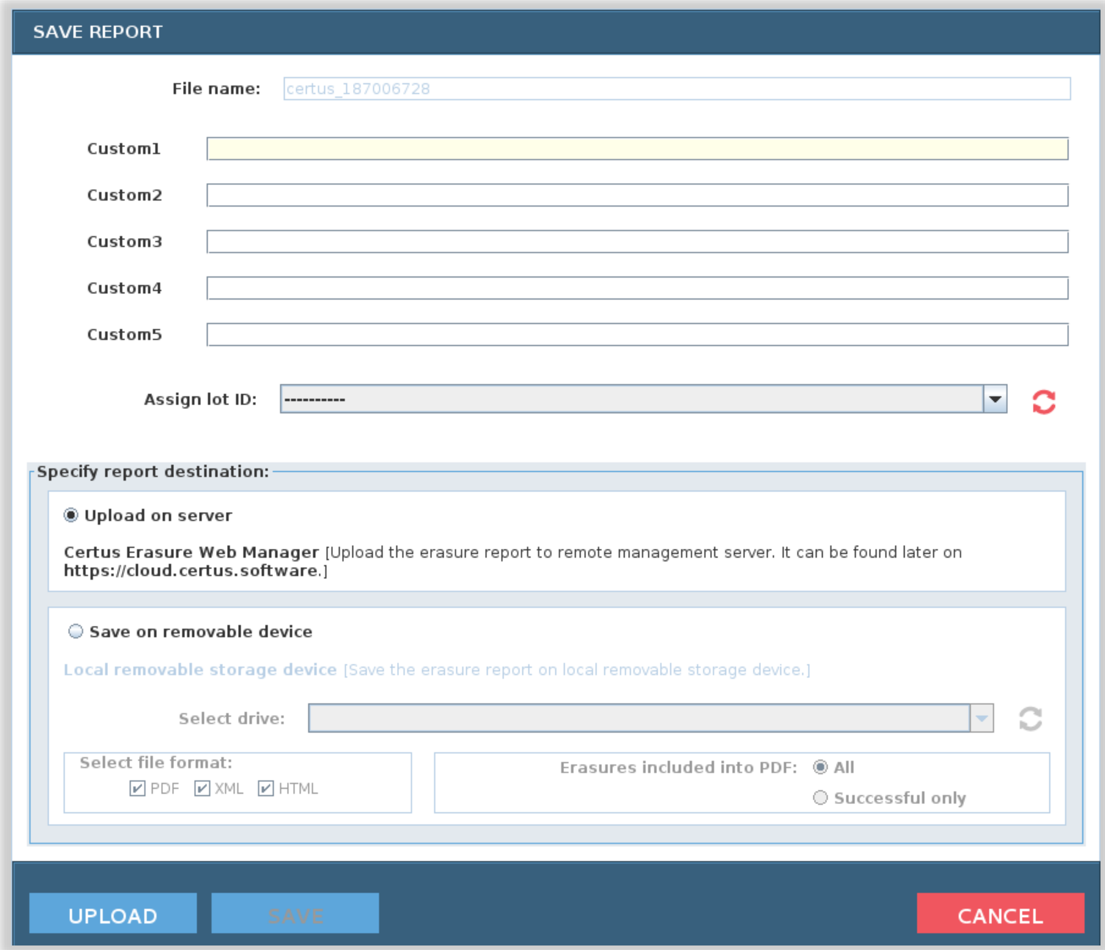
To download the report, select the “SAVE” button, otherwise select “CANCEL”.

After selecting the “SAVE” button, a popup window appears (“SAVE Report”) which gives the opportunity to the user to do the following:

- assigning a lot ID for the report (for more details regarding the lots refer to the CEWM User manual)
    - the refresh button next to the list of lots will synchronize the list of lots from CE with the one from CEWM;
- uploading the report to the Certus Erasure Web Manager (CEWM) application
- fill any of the custom fields (note that the name of the custom fields is by default “Custom 1…” but if the operator changes the name of these fields on CEWM, those changes will be reflected in the application and instead of “Custom 1…” it will display the name set on that field on CEWM);
- downloading the erasure report to an external removable device in XML, PDF or HTML format
- selecting the status of the erasures included in the report:

- **“Successful only” -** will include in the report only the erasures that have been finished successfully;

- **“All “**will include in the report every erasure, including the ones that were not finished successfully;



SAVE REPORT

File name: certus_187006728

Custom1

Custom2

Custom3

Custom4

Custom5

Assign lot ID: ----------

Specify report destination:

● Upload on server

Certus Erasure Web Manager [Upload the erasure report to remote management server. It can be found later on **https://cloud.certus.software.**]

○ Save on removable device

Local removable storage device [Save the erasure report on local removable storage device.]

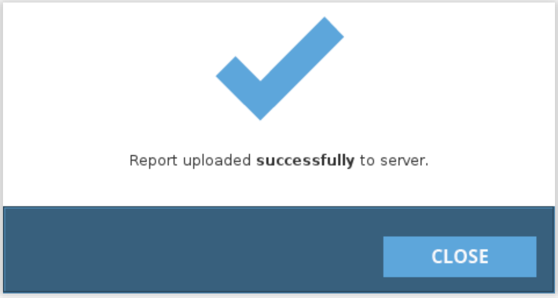
Select drive:

Select file format: ☑ PDF ☑ XML ☑ HTML

Erasures included into PDF: ● All ○ Successful only

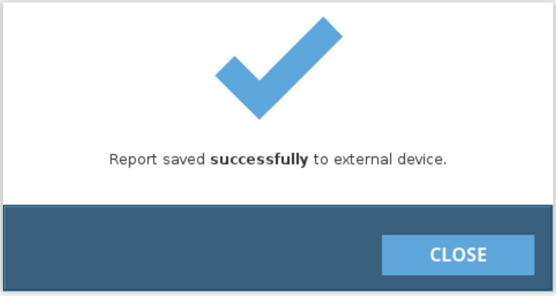
Fig. 3.31 Save Report window

If the upload to server/saving to removable device is successful, one of the following windows will appear:



Report uploaded **successfully** to server.

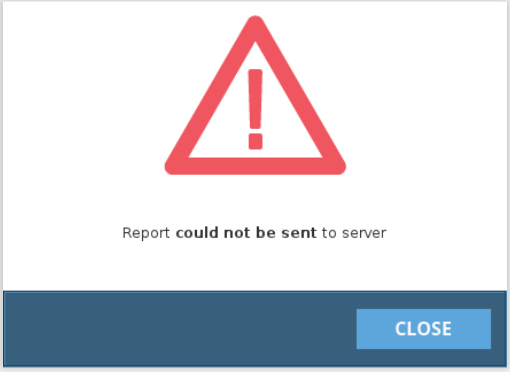
Fig. 3.32 Report saved successfully to server



Report saved **successfully** to external device.

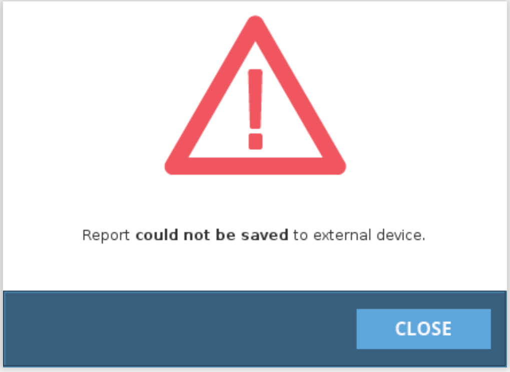
Fig. 3.33 Report saved successfully to external device

If the upload to server/saving to removable device is unsuccessful, one of the following windows will appear:



Report **could not be sent** to server

Fig. 3.34 Report saved unsuccessfully to server

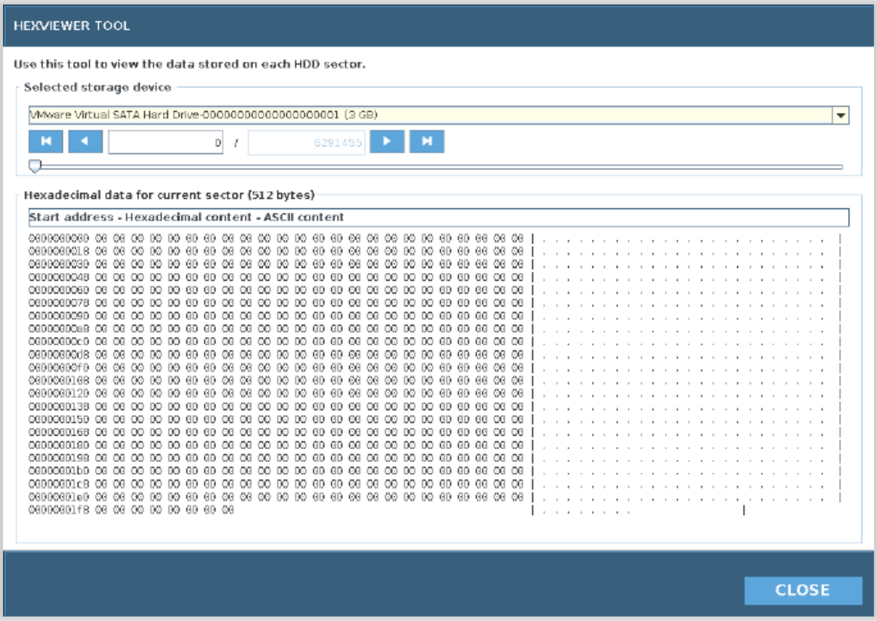


Report **could not be saved** to external device.

Fig. 3.35 Report saved unsuccessfully to external device

3.1.13. Hexviewer button

HEXVIEWER This button shows the visual content of a storage device in hexadecimal format. Hexviewer allows the user to see the hex-format pattern of the erasure result.



HEXVIEWER TOOL

Use this tool to view the data stored on each HDD sector.

Selected storage device

VMware Virtual SATA Hard Drive-00000000000000000001 (3 GB)

0 / 6291455

Hexadecimal data for current sector (512 bytes)

Start address - Hexadecimal content - ASCII content

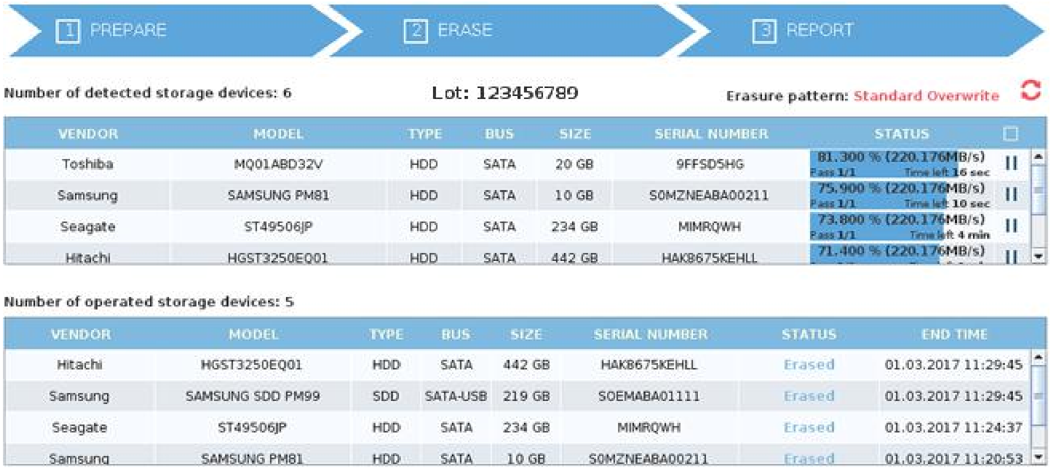
```
0000000000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................ |
0000000018 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................ |
0000000030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................ |
0000000048 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................ |
0000000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................ |
0000000078 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................ |
0000000090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................ |
00000000a8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................ |
00000000c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................ |
00000000d8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................ |
00000000f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................ |
0000000108 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................ |
0000000120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................ |
0000000138 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................ |
0000000150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................ |
0000000168 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................ |
0000000180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................ |
0000000198 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................ |
00000001b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................ |
00000001c8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................ |
00000001e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ........................ |
00000001f8 00 00 00 00 00 00 00 00                                                 | ........
```

Fig. 3.36 Hex viewer

3.2. Work area

Work area contains:

- the graphic description of the 3-step process - Prepare, Erase, Report;
- the table of information regarding the detected storage devices;
- the current lot and pattern that have been selected;
- the table of information regarding the operated storage devices.



Number of detected storage devices: 6 Lot: 123456789 Erasure pattern: Standard Overwrite

VENDOR	MODEL	TYPE	BUS	SIZE	SERIAL NUMBER	STATUS	□
Toshiba	MQ01ABD32V	HDD	SATA	20 GB	9FFSD5HG	81.300 % (220.176MB/s) Pass 1/1 Time left 16 sec	⏸
Samsung	SAMSUNG PM81	HDD	SATA	10 GB	S0MZNEABA00211	75.900 % (220.176MB/s) Pass 1/1 Time left 10 sec	⏸
Seagate	ST49506JP	HDD	SATA	234 GB	MIMRQWH	73.800 % (220.176MB/s) Pass 1/1 Time left 4 min	⏸
Hitachi	HGST3250EQ01	HDD	SATA	442 GB	HAK8675KEHLL	71.400 % (220.176MB/s)	⏸

Number of operated storage devices: 5

VENDOR	MODEL	TYPE	BUS	SIZE	SERIAL NUMBER	STATUS	END TIME
Hitachi	HGST3250EQ01	HDD	SATA	442 GB	HAK8675KEHLL	Erased	01.03.2017 11:29:45
Samsung	SAMSUNG SDD PM99	SDD	SATA-USB	219 GB	SOEMABA01111	Erased	01.03.2017 11:29:45
Seagate	ST49506JP	HDD	SATA	234 GB	MIMRQWH	Erased	01.03.2017 11:24:37
Samsung	SAMSUNG PM81	HDD	SATA	10 GB	S0MZNEABA00211	Erased	01.03.2017 11:20:53

Fig. 3.37 Work area

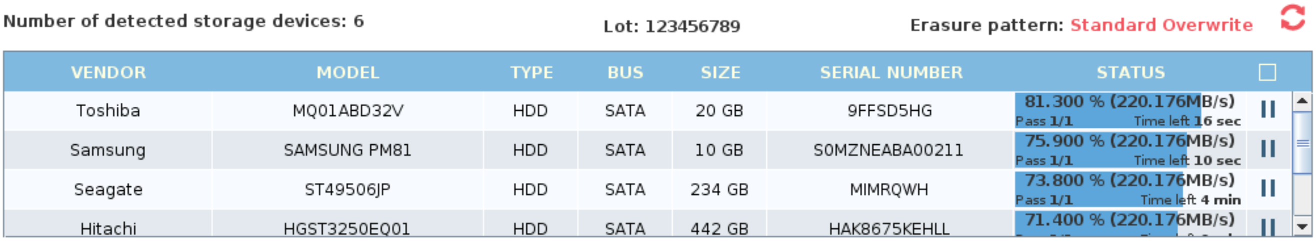
3.2.1. Detected storage devices

The total number of the detected storage devices, the currently used lot and erasure pattern and the refresh button are present on top of the table.

The user can select in CEWM a default lot to be assigned to it's account so that it is automatically selected by the application after logging in. If there is no default lot selected, then the lot label will not be visible after logging into the application. The user can assign a lot from the "Save Report" window. See View Report button section. After a lot is selected, it will be displayed above the detected storage devices. The user can also click on the lot and it will automatically open the "Save Report" window so another one can be selected.

The table contains information about the storage devices detected by the erasure machine: vendor, model, type, bus, size, serial number and status. The status column presents erasure information: percentage, speed, pass and time left.

For multiple erasures, the user can select all drives using the checkbox located at the top right corner of the table.

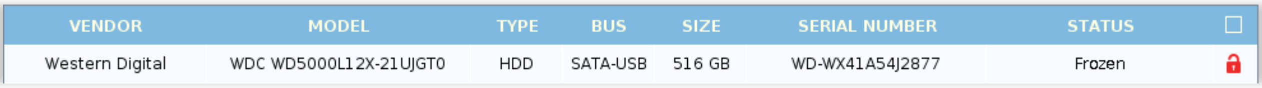


Number of detected storage devices: 6 Lot: 123456789 Erasure pattern: Standard Overwrite

VENDOR	MODEL	TYPE	BUS	SIZE	SERIAL NUMBER	STATUS	□
Toshiba	MQ01ABD32V	HDD	SATA	20 GB	9FFSD5HG	81.300 % (220.176MB/s) Pass 1/1 Time left 16 sec	⏸
Samsung	SAMSUNG PM81	HDD	SATA	10 GB	S0MZNEABA00211	75.900 % (220.176MB/s) Pass 1/1 Time left 10 sec	⏸
Seagate	ST49506JP	HDD	SATA	234 GB	MIMRQWH	73.800 % (220.176MB/s) Pass 1/1 Time left 4 min	⏸
Hitachi	HGST3250EQ01	HDD	SATA	442 GB	HAK8675KEHLL	71.400 % (220.176MB/s)	⏸

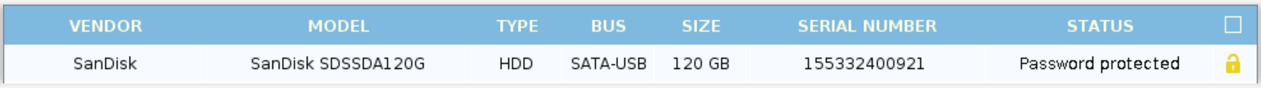
Fig. 3.38 Detected storage devices

The erasure process cannot be performed on password protected devices or freeze locked drives. Certus Erasure shows these statuses by displaying the "locked" icon in red color for frozen drives and in yellow color for password protected devices.



VENDOR	MODEL	TYPE	BUS	SIZE	SERIAL NUMBER	STATUS	□
Western Digital	WDC WD5000L12X-21UJGT0	HDD	SATA-USB	516 GB	WD-WX41A54J2877	Frozen	🔒

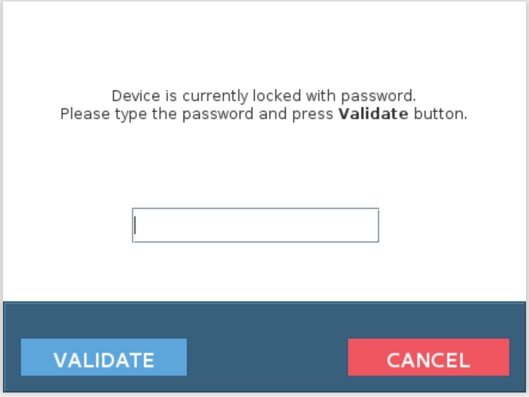
Fig. 3.39 Freeze locked storage device



VENDOR	MODEL	TYPE	BUS	SIZE	SERIAL NUMBER	STATUS	□
SanDisk	SanDisk SDSSDA120G	HDD	SATA-USB	120 GB	155332400921	Password protected	🔒

Fig. 3.40 Password protected storage device

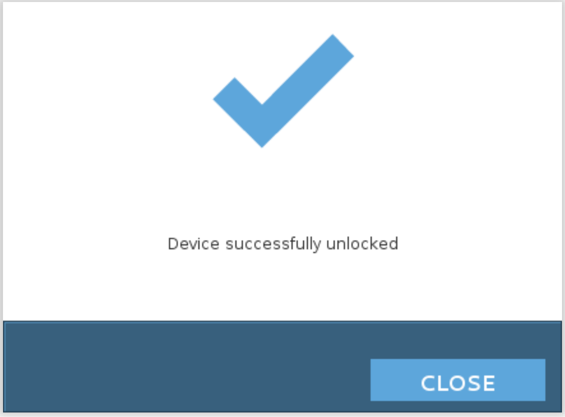
The user is invited to remove the password protection by clicking on the yellow icon. The window that appears allows typing the password and validating it. If the user is not aware of a password being set on the drive, it is recommended to check the documentation of the storage device in question or contact the drive manufacturer/provider.



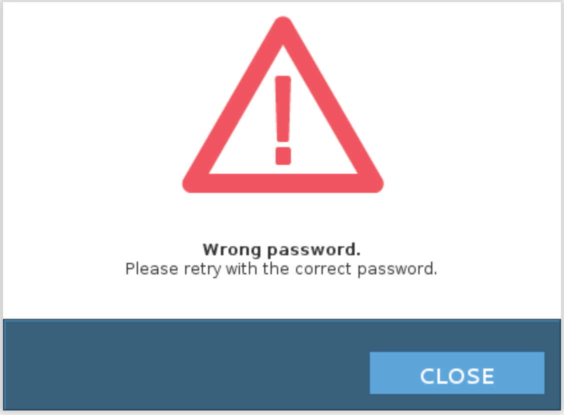
Device is currently locked with password.
Please type the password and press **Validate** button.

Fig. 3.41 Password removal

Certus provides the overview of the removal result, whether it is successful or unsuccessful (wrong password or failed password removal).



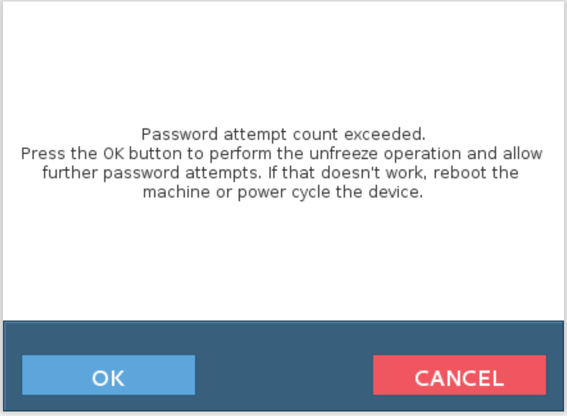
Device successfully unlocked



Wrong password.
Please retry with the correct password.

Fig. 3.42 Successful password removal

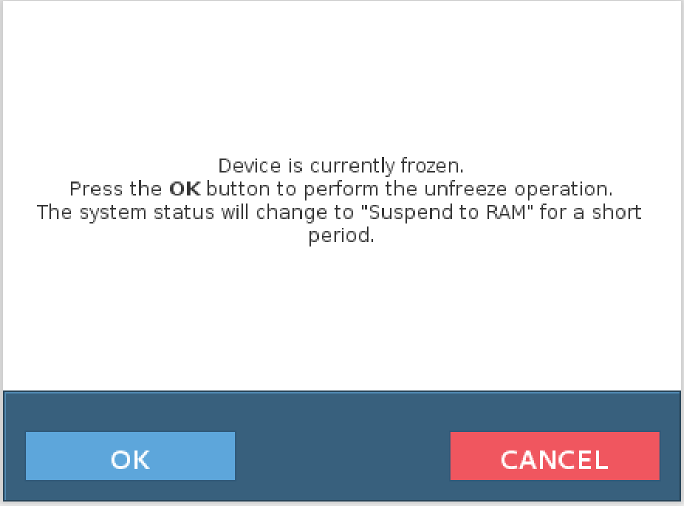
Fig. 3.43 Wrong password



Password attempt count exceeded.
Press the OK button to perform the unfreeze operation and allow further password attempts. If that doesn't work, reboot the machine or power cycle the device.

Fig. 3.44 Failed password removal

Certus detects if at least one of the drives about to be erased is freeze locked. When a drive is freeze locked, Certus notifies the user by displaying a red lock icon. Pressing this icon and clicking the ok button from the new opened window, will prompt Certus to perform an unfreeze operation which will power cycle the machine (the machine is put to sleep, the screen blanks out for a couple of seconds and then the machine is woken up). As the machine is power cycled, Certus attempts to remove the freeze locks on all locked drives at once. If this process is successful, the red icon will be removed for all the locked drives.



Device is currently frozen.
Press the **OK** button to perform the unfreeze operation.
The system status will change to "Suspend to RAM" for a short period.

Fig. 3.45 Device is frozen

Caution! On some hardware configurations, the screen might not turn back on due to the fact the machine is not waking up properly/at all. This can be caused by the machine’s underlying hardware, such as the motherboard, its BIOS or graphical device(s). The erasure process is either interrupted or continues in the background, however the user will not be able to save any report in the latter case.

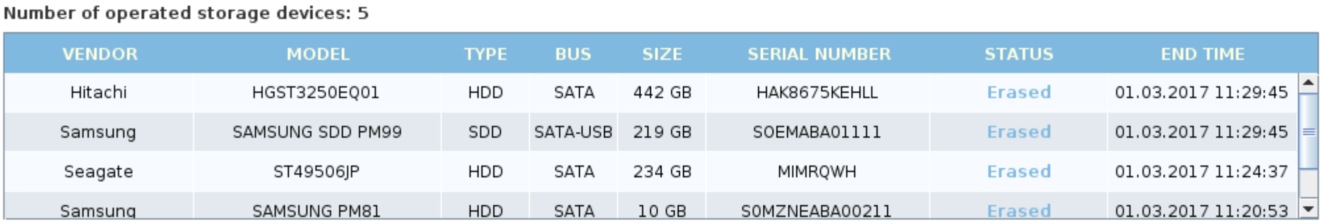
3.2.2. Operated storage devices

The total number of operated devices is placed on top of the table.

The table provides data about the operated storage devices: vendor, model, type, bus, size, serial number, status, end time of the operation.

Status messages can be:

- **Erased** – the storage device was successfully erased;
- **Erasure finished with warning** – the storage device was successfully erased but warnings occurred:
  - *Remapped sectors were not erased*.
    Note: For further guidelines on remapped sectors, please check **Remapped sectors** chapter.
- **Interrupted by user** – the erasure process was stopped by the user (*Note that if the erasure process was started, all the data on the storage device is compromised);*
- **Interrupted by program** – the erasure engine encountered a critical error when initializing or during erasure process;
- **Disconnected** – the storage device was disconnected during the erasure process;
- **Not erased** – the storage device has hidden areas (HPA/DCO) that are not accessible or the storage device contains failed sectors.



Number of operated storage devices: 5

VENDOR	MODEL	TYPE	BUS	SIZE	SERIAL NUMBER	STATUS	END TIME
Hitachi	HGST3250EQ01	HDD	SATA	442 GB	HAK8675KEHLL	Erased	01.03.2017 11:29:45
Samsung	SAMSUNG SDD PM99	SDD	SATA-USB	219 GB	S0EMABA01111	Erased	01.03.2017 11:29:45
Seagate	ST49506JP	HDD	SATA	234 GB	MIMRQWH	Erased	01.03.2017 11:24:37
Samsung	SAMSUNG PM81	HDD	SATA	10 GB	S0MZNEABA00211	Erased	01.03.2017 11:20:53

Fig. 3.46 Operated storage devices

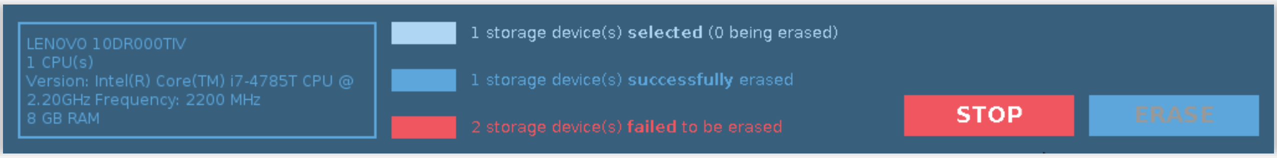
3.3. Footer area

The lower left corner of the section contains system information: station name, number of CPUs, CPU, CPU frequency, RAM.

The status of the erasure process, presented next to system information box, shows if the device(s) is/are:

- in progress of being erased;
- successfully erased;
- failed to be erased.

The lower right corner of the section contains Erase button which allows the erasure process to start. If one or several erasures are in progress, the Stop button appears. It allows the user to stop the erasure process.



LENOVO 10DR000TIV
1 CPU(s)
Version: Intel(R) Core(TM) i7-4785T CPU @ 2.20GHz Frequency: 2200 MHz
8 GB RAM

1 storage device(s) **selected** (0 being erased)

1 storage device(s) **successfully** erased

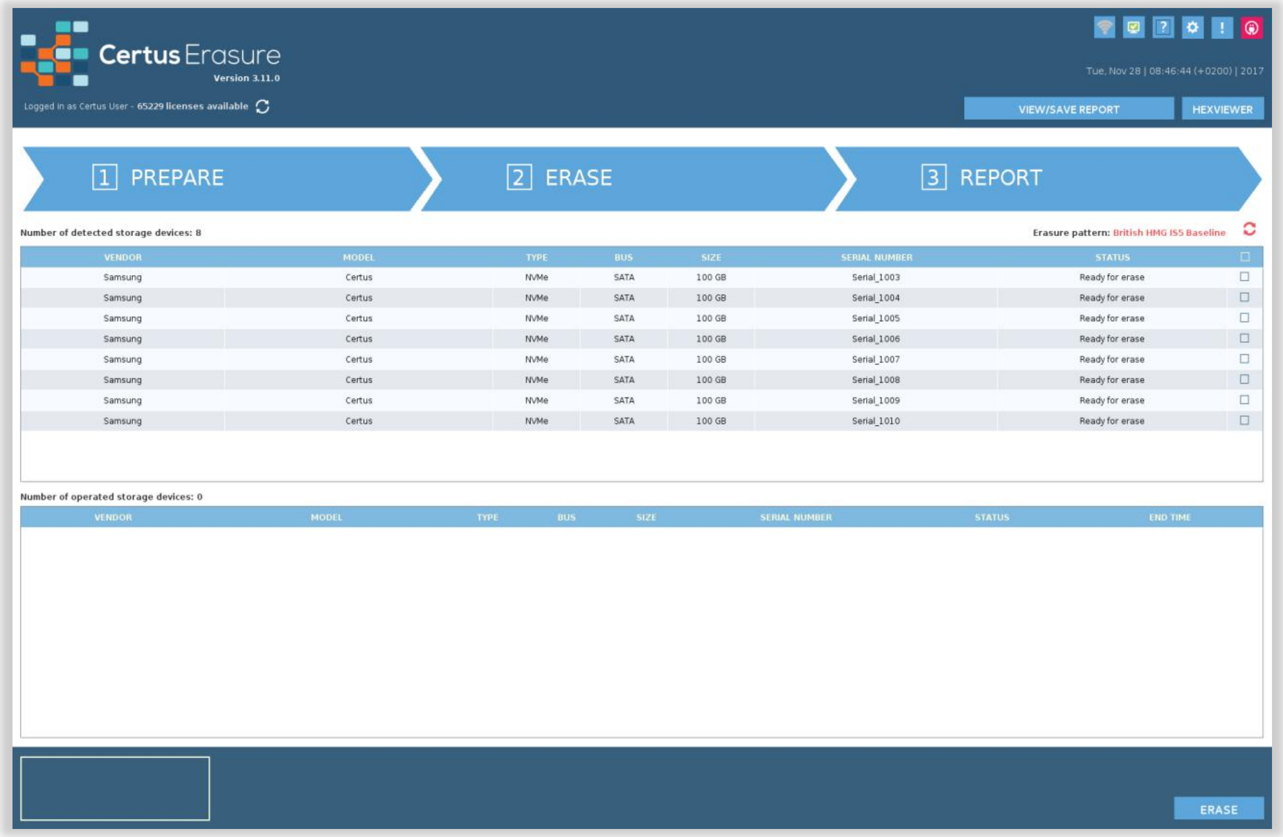
2 storage device(s) **failed** to be erased

Fig. 3.47 Footer area

CHAPTER 4. USING CERTUS ERASURE SOFTWARE PRODUCT

4.1. Preparing storage devices

After a successful authentication, Certus main window is displayed. Certus Software will automatically display the storage device(s) connected to the erasing machine.



Logged in as Certus User - 65229 licenses available

Tue, Nov 28 | 08:46:44 (+0200) | 2017

Number of detected storage devices: 8

Erasure pattern: British HMG IS5 Baseline

VENDOR	MODEL	TYPE	BUS	SIZE	SERIAL NUMBER	STATUS	□
Samsung	Certus	NVMe	SATA	100 GB	Serial_1003	Ready for erase	□
Samsung	Certus	NVMe	SATA	100 GB	Serial_1004	Ready for erase	□
Samsung	Certus	NVMe	SATA	100 GB	Serial_1005	Ready for erase	□
Samsung	Certus	NVMe	SATA	100 GB	Serial_1006	Ready for erase	□
Samsung	Certus	NVMe	SATA	100 GB	Serial_1007	Ready for erase	□
Samsung	Certus	NVMe	SATA	100 GB	Serial_1008	Ready for erase	□
Samsung	Certus	NVMe	SATA	100 GB	Serial_1009	Ready for erase	□
Samsung	Certus	NVMe	SATA	100 GB	Serial_1010	Ready for erase	□

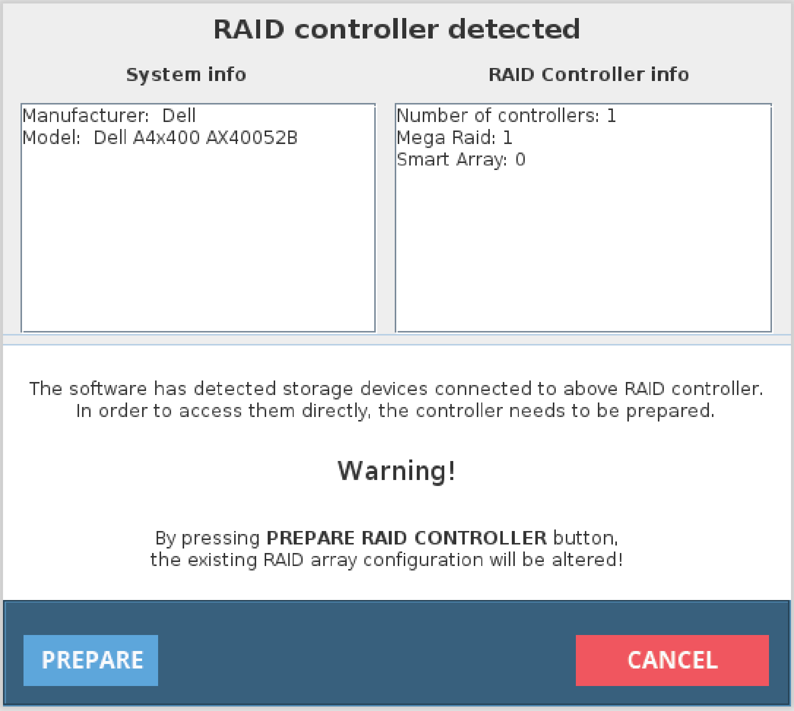
Number of operated storage devices: 0

VENDOR	MODEL	TYPE	BUS	SIZE	SERIAL NUMBER	STATUS	END TIME

Fig. 4.1 Main window with detected storage devices

*Please note that that the status of the storage device(s) connected to the erasing machine is **Ready for erase** in case no erasure operation has been performed on them, and **Operated** when at least one erasure operation has been performed on them.*

If a RAID controller is detected, a window appears with system info and RAID controller info. To dismantle the RAID array, click the **Prepare** button. To cancel the action, click the **Cancel** button.



RAID controller detected

System info

Manufacturer: Dell
Model: Dell A4x400 AX40052B

RAID Controller info

Number of controllers: 1
Mega Raid: 1
Smart Array: 0

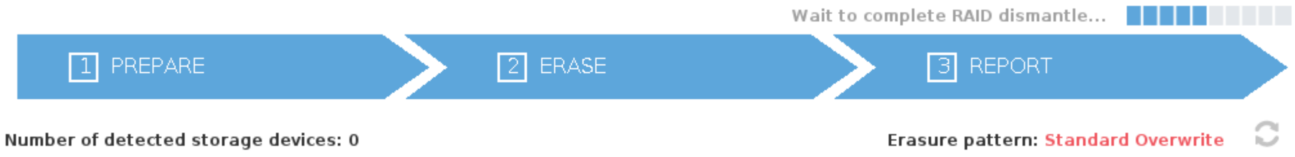
The software has detected storage devices connected to above RAID controller. In order to access them directly, the controller needs to be prepared.

Warning!

By pressing **PREPARE RAID CONTROLLER** button, the existing RAID array configuration will be altered!

Fig. 4.2 RAID controller detected

After clicking **Prepare** button, a loading message appears. During the dismantle process the refresh icon is disabled (the user can't refresh the device list until the dismantle process is completed).



Wait to complete RAID dismantle...

Number of detected storage devices: 0

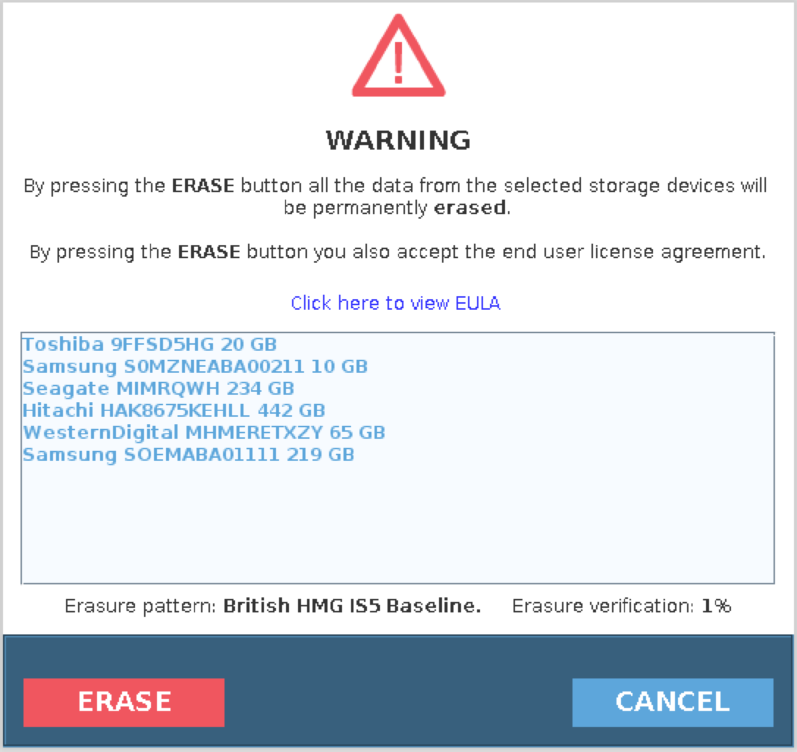
Erasure pattern: Standard Overwrite

Fig. 4.3 Loading message

4.2. Performing erasure

The user can start the erasure process by selecting one or more storage devices from the detected storage devices table and by pressing the **Erase** button located in the footer area. A confirmation dialog with a list of the selected storage devices, erasure pattern and erasure verification percentage appear. To start the erasure process, click the **Erase** button. To cancel the action, click the **Cancel** button.

Please note that pressing the Erase button will automatically reduce the amount of the available licenses with the number of the selected storage devices.



WARNING

By pressing the **ERASE** button all the data from the selected storage devices will be permanently **erased**.

By pressing the **ERASE** button you also accept the end user license agreement.

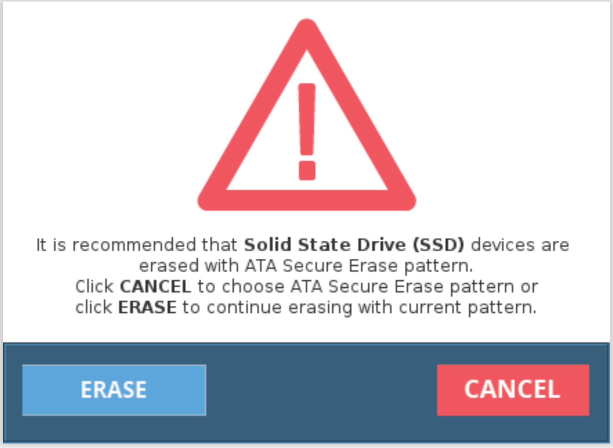
Click here to view EULA

Toshiba 9FFSD5HG 20 GB
Samsung S0MZNEABA00211 10 GB
Seagate MIMRQWH 234 GB
Hitachi HAK8675KEHLL 442 GB
WesternDigital MHMERETXZY 65 GB
Samsung SOEMABA01111 219 GB

Erasure pattern: **British HMG IS5 Baseline.** Erasure verification: **1%**

Fig. 4.4 Erasure confirmation window

If a SSD is detected and the erasure pattern is not ATA Secure Erase, another window appears. To confirm the erasure with current pattern, click **Erase**. To cancel the action, click **Cancel.**



It is recommended that **Solid State Drive (SSD)** devices are erased with ATA Secure Erase pattern.
Click **CANCEL** to choose ATA Secure Erase pattern or click **ERASE** to continue erasing with current pattern.

Fig. 4.5 SSD Erasure confirmation window

4.3. Pause and resume erasure

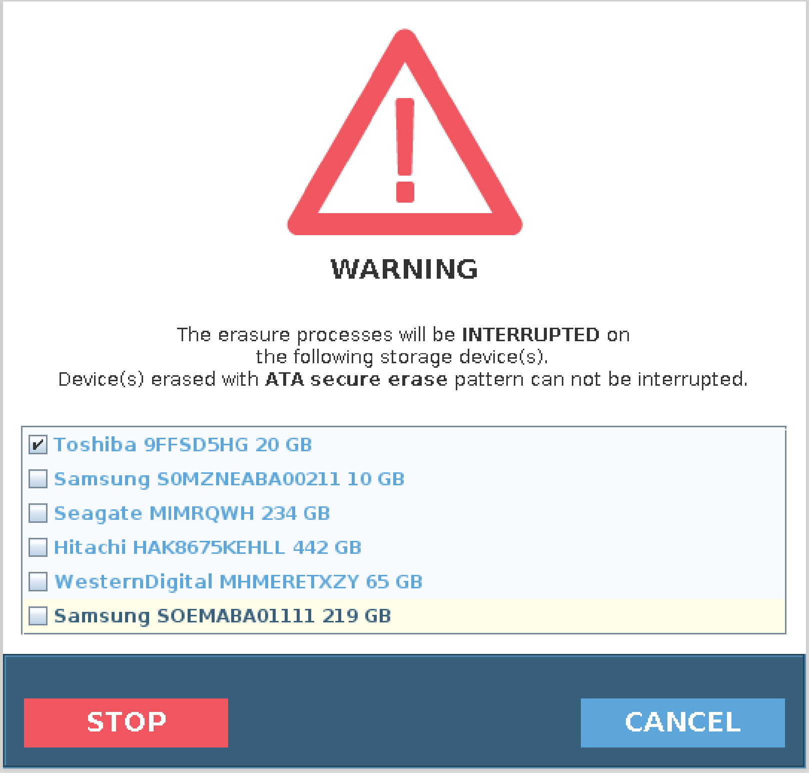
⏸ The user has the possibility to pause any erasure process, which is currently running, by clicking on the corresponding icon.

▶ The user has the possibility to resume any paused erasure, allowing the continuation of the erasure process, by clicking on the corresponding icon.

Please note that a paused erasure can only be continued in the current session of Certus Erasure. If the user reboots the machine or if it is by any means power cycled, the erasure cannot be continued.

4.4. Canceling erasure

During the erasure of one or more storage devices, the user can cancel the process at any time by clicking the **Stop** button. A confirmation dialog with a list of storage devices with ongoing erasures appears. To stop the erasure process, select the desired device(s), then click the **Stop** button. To cancel the action, click the **Cancel** button.



WARNING

The erasure processes will be **INTERRUPTED** on
the following storage device(s).
Device(s) erased with **ATA secure erase** pattern can not be interrupted.

☑ Toshiba 9FFSD5HG 20 GB
□ Samsung S0MZNEABA00211 10 GB
□ Seagate MIMRQWH 234 GB
□ Hitachi HAK8675KEHLL 442 GB
□ WesternDigital MHMERETXZY 65 GB
□ Samsung SOEMABA01111 219 GB

Fig. 4.6 Cancel erasure confirmation dialog

4.5. Checking erasure results

HEXVIEWER

In order to examine the results, at the end of an erasure, click on the **Hexviewer** button.

4.6. Saving erasure reports

VIEW REPORT

After a successful or failed erasure, from the header area, click on the **View report** button and then on the **Save** button, detailed in chapter **3.1.13**.

All Certus erasure reports are digitally signed by the application to assure their authenticity. The user can check their digital signature. After saving the erasure reports and opening them with Adobe Reader (for Windows operating systems), the following message should be displayed: “You are currently viewing a signed version”.

The upload of the reports on Certus Erasure Web Manager is based on the automatic verification and validation of the digital signature.

CHAPTER 5. DATA ERASURE REPORT

The erasure report is an important component, as part of the erasure and hardware identification processes carried out by Certus Erasure. The document serves as a certified evidence that the application conducted erasure and/or hardware related operations on the host machine.

The Certus Erasure Data Erasure report is divided in three main sections, which are described in the following chapters; these sections are:

- Document Information;
- System Hardware Information;
- Storage Device Information.

The first time a report is generated is when the user logs into the application. After the user boots the software and authenticates, Certus Erasure starts an identification process to detect the system configuration before any erasure operation is started. The program generates a hardware audit report, which contains only document and hardware information; this report is then updated after certain operations take place: an erasure process is finished (successful or not) or identification of hardware. For each erasure process finished, an additional Storage Device Information section is added to the report.

5.1. Document Information

The *Document Info* is the first section of the report and contains document related information like the identification number, the date of the report, the operator which performed the operations and the software version.

Important to note here is the ***report date*** field which is constantly updated after each erasure process is finished or after hardware changes are detected by the software (like plugging new devices).

The *Document Info* section is generated when a working session begins (after user login).

5.2. System Hardware Information

The *System Hardware Info* is the second section of the report and represents the hardware audit part of the document. This section contains the main hardware components of the system, identified by Certus Erasure: manufacturer, chassis type, model, serial number, motherboard, UUID, BIOS, processor, memory, graphics card, sound card, network adapter, optical drive, storage controller, storage device, peripheral ports and battery.

The *System Hardware Info* section is generated at the beginning of and during of a working session if hardware changes are detected.

5.3. Storage Device Information

The *Storage Device Info* section is the last part of the report. For each erasure process started, a Storage Device Info section is added to the report; if no erasure process took place, the report contains only document and hardware info.

Each storage device block is divided in two main areas as follows:

- Device Information – it presents the main characteristics of the operated device (e.g.: vendor, type, size, sectors etc.);
- Erasure Information – contains all the details of the erasure process (e.g.: erasure pattern and verification, start time and end time, duration, sectors related info, erasure status etc.).

5.3.1. Hidden areas in a drive

The **Host Protected Area (HPA)** is a feature set implemented by some ATA conforming devices allowing for the possibility of reducing the number of addressable sectors, thus creating an area on the device hidden from view using regular access. The operations that can be conducted on this area are specific to the HPA feature set.

The **Device Configuration Overlay (DCO)** is a feature set implemented by some ATA conforming devices allowing for the possibility of changing several configuration items from different feature sets implemented by the device. Among these configuration items is the number of addressable sectors, thus allowing for the creation of another form of hidden area on the device. The operations that can be conducted on this area are specific to the DCO feature set.

If the device has a hidden area (HPA or DCO) before the erasure, the appropriate field (HPA or DCO) in the *Device Information* section will contain information following the pattern: *'X/Y Enabled'*, where *X* and *Y* are the lower and higher ends of the hidden area. For example, if a device has 1000 addressable sectors, a HPA of 100 sectors and a DCO of another 100 sectors, the fields in *Device Information* would appear as: *'Sectors: 1000'*, *'HPA: 1000/1100 Enabled'*, *'DCO: 1100/1200 Enabled'*.

If there are hidden areas enabled on the device, it's total capacity is the greatest number of sectors between the fields *'Sectors'* and the *Y* values of the fields *'HPA'* and *'DCO'* from the *Device Information* section.

In the *Erasure Information* section, there is a field '*Sectors*' holding information about the number of total sectors that have been erased. If, in the example above, the software successfully deletes the hidden areas, then the field '*Sectors*' in the section *Erasure Information* will hold the value 1200 which is the maximum capacity of the device.

5.3.2. Remapped sectors

The number of reallocated sectors is a parameter of S.M.A.R.T. which in turn is a feature set implemented by some ATA conforming devices. Devices implementing this feature set and supporting the reallocated sectors parameter mark the sectors where it encounters a read/write/verification error as *'reallocated'* and transfers the data to a special reserved area (spare area). Thus, the data then resides on a fresh sector, while the one which encountered an error is hidden from view.

Although the remapped sector remains hidden, it may still contain user data. The standard ATA interface does not allow access on a reallocated sector, thus, when erasing a device with remapped sectors, Certus Erasure will produce a report with a status *'Erasure finished with warning (Remapped sectors: X)'* where *X* is the value of the remapped sectors after the erasure. **It is important to note that those remapped sectors were not erased by Certus.**

Recommendation: A positive value of this parameter could indicate imminent drive failure. Do not repurpose a drive with a positive value of this parameter without refurbishment.

CHAPTER 6. ERASURE PATTERNS

The following are the erasure standards (patterns) supported by Certus Erasure Software:

Pattern	Description
Standard overwrite	Single pass over each sector writing 0x00.
British HMG IS5 Baseline	Pass over each sector once writing random value.
British HMG IS5 Enhanced	Pass over each sector 3 times writing 0x00, 0xFF and a random value.
Bruce Schneier	Pass over each sector 7 times, writing 0xFF, 0x00 and then five times random values.
Canadian OPS-II	Pass over each sector 7 times, writing 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF and a random value.
Gutmann Algorithm	Pass over each sector 35 times, writing random values the first four times, then respectively write 0x555555, 0xAAAAAA, 0x924924, 0x492492, 0x249249, 0x000000, 0x111111, 0x222222, 0x333333, 0x444444, 0x555555, 0x666666, 0x777777, 0x888888, 0x999999, 0xAAAAAA, 0xBBBBBB, 0xCCCCCC, 0xDDDDDD, 0xEEEEEE, 0xFFFFFF, 0x924924, 0x492492, 0x249249, 0x6DB6DB, 0xB6DB6D, 0xDB6DB6 and another four times random values.
German VSITR	Pass over each sector 7 times writing 0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF and 0xAA.
NAVSO P-5329-26	Pass over each sector 3 times writing 0x00, 0xFF and a random value.
NCSC-TG-025	Pass over each sector 3 times writing 0x00, 0xFF and a random value.
NSA 130-2	Pass over each sector 2 times writing a random value.
Russian GOST R 50739-95	Pass over each sector 2 times writing 0x00 and a random value.
US Air Force 5020	Pass over each sector 3 times writing 0xFF, 0x00 and a random value.
US DoD 5220.22-M	Pass over each sector 3 times writing 0x00, 0xFF and a random value.
ATA Secure Erase	Standard overwrite*

* **Warning!** To be used **only** with Solid State Drives (SSD). Firmware based erasure. Once the erasure process is started with this pattern, it cannot be stopped.

CHAPTER 7. KEYBOARD SHORTCUTS

7.1. Generic controls

7.1.1. Tab key Tab ↹

The Tab key moves the focus inside a window, element to element, from left to right, top to bottom (except from the two tables from the main window and the table with the erasure pattern description from the settings window, where shifting is done with two arrows - up and down). By combining the Shift-key with Tab-key (Shift + Tab), the direction is reversed (goes backwards: from right to left, bottom to top). If the focused component is a button, a checkbox or a radio button, the focus is highlighted with a rectangle. If the focused component is a text area, the focus is highlighted with a low opacity yellow color. If the focused component is a table, the focused row is highlighted with a border.

7.1.2. Arrow keys ← ↑ ↓ →

Whenever the focus is:

- On an area that contains a horizontal and/or vertical scroll-bar (Report View, Help window, EULA window, Settings window, table with operated devices, table with erasure history, etc.):
  - The arrow keys can be used to go up/down/left/right inside that area.
- On a drop-down list (list of erasure patterns, list of languages, list of drives from Hex Viewer, list of drives from Stop window, etc.):
  - The arrow keys can be used to scroll those lists.
- On a slider's handle (verification percentage slider, current sector slider):
  - The arrow keys can be used to move the handle.
- On a wi-fi list of connections, it will move between the available connections.

7.1.3. Home key Home

In the Settings window and the Hexviewer window, the Home key moves the handle to the home position. In an expanded drop-down list, it selects the first item.

7.1.4. End key End

In the Settings window and the Hexviewer window, the End key moves the handle to the end position. In an expanded drop-down list, it selects the last item.

7.1.5. Space bar Space

Whenever the focus is:

- On top of a checkbox or on top of a radio button:
  - The Space bar selects/deselects it.
- On a row of a table with connected drives:
  - The Space bar selects/deselects it.
- On top of a button:
  - The Space bar pushes it.

7.1.6. Enter key Enter ↲

- In the Login window:
  - The enter key pushes the login button.
- Whenever the focus is on an element of an expanded drop-down list:
  - The Enter key selects that element.
- Whenever the focus is on a wi-fi connection from the wi-fi list:
  - The Enter key expands/contracts that connection.

7.1.7. Ctrl + Enter key CTRL + Enter ↲

Whenever the focus is on a wi-fi connection from the wi-fi list, this key combination will attempt to connect to the focused wi-fi connection.

7.1.8. Esc key Esc

Whenever the focus is:

- On top of an expanded drop-down list:
  - Escape key collapses it.
- Inside an open window (pop-up, dialog):
  - Escape key closes it without saving any change (equivalent to Cancel/Close).

7.2. Specific controls

7.2.1. F1 key F1

Pushes the Help button (opens the Help window).

7.2.2. F2 key F2

Pushes the View Report button (opens the View Report window).

7.2.3. F3 key F3

Pushes the Settings button (opens the Settings window).

7.2.4. F4 key F4

Pushes the Hexviewer button (opens the Hexviewer window).

7.2.5. F5 key F5

Pushes the Report an issue button (opens the Report an issue window).

7.2.6. F10 key F10

Pushes the Shutdown button (opens the Shutdown confirmation window).

7.2.7. Shift + F10 key SHIFT + F10

Pushes the Shutdown button in the Shut Down confirmation window (shuts down the system).

7.2.8. Ctrl + A key CTRL + A

This key combination selects/deselects all drives for erasure.

7.2.9. Ctrl + R key CTRL+R

This key combination pushes the Refresh button (in the main window refreshes the list of connected drives, in the Save Report window refreshes the connected removable devices).

7.2.10. Ctrl + Shift + R key CTRL+SHIFT+R

This key combination pushes the Refresh lot list button. (in the report save window downloads from CEWM the lot list and replaces the local list with it).

7.2.11. Ctrl + E key CTRL+E

This key combination pushes the Erase button (opens the Erase confirmation window).

7.2.12. Ctrl + Shift + E key CTRL+SHIFT+E

This key combination pushes the Erase button in the Erase confirmation window (starts the erasure).

7.2.13. Ctrl + O key CTRL+O

This key combination pushes the Stop button (opens the Stop confirmation window).

7.2.14. Ctrl + Shift + O key CTRL+SHIFT+O

This key combination pushes the Stop button in the Stop confirmation window (stopping selected devices).

7.2.15. Ctrl + S key CTRL+S

This key combination pushes the Save button (in the View Report window opens the Save Report window, in the Save Report or Report an issue windows saves report to the external device, in the Settings window saves the changes).

7.2.16. Ctrl + U key CTRL+U

This key combination pushes the Upload button in the Save Report window (uploads the report on the server).

7.2.17. Ctrl + P key CTRL+P

This key combination pushes the Prepare RAID Controller button (starting the dismantle process).

7.2.18. Ctrl + V key CTRL+V

This key combination pushes the Validate button (sends device password to the ATA Secure Erase process).

7.2.19. Ctrl + F key CTRL+F

This key combination pushes the OK button in the Unfreeze dialog.

7.2.20. Ctrl + G key CTRL+G

This key combination pushes the Generate button in the Report an issue window.

CHAPTER 8. CONTACT

If you have any questions or if you need our help don’t hesitate to submit a technical support ticket using the following link:

https://support.certus.software/servicedesk/customer/portal/1

For more information about the latest data erasure products and for contact details, visit Certus website using the following link:

https://www.certus.software

We are always looking for ways to improve our products and services. If you have any suggestions, please provide us with your feedback!

CHAPTER 9. DOCUMENT REVISIONS

Date	Revision History	Revision Class	Comments
21/10/2016	1.0	Major	- Initial version.
09/02/2017	1.1	Minor	- Updated images; - Updated page layout; - Added information about “Report an issue”; - Added information about new “Settings” window.
02/03/2017	1.2	Minor	- Replaced buttons from “Contact” chapter with links.
15/03/2017	1.3	Minor	- Added information about “Screensaver”; - Added information about “Hasp key”.
05/04/2017	1.4	Minor	- Added “General information” chapter; - Updated information.
07/04/2017	1.5	Minor	- Added information about “Handle password protected devices” and “Unfreeze DCO and Security Features”.
25/04/2017	2.0	Major	- Added information about “Pause and resume erasure”, “Digital signature of reports”, “Internet connection icon”, “Update ISO”; - Updated information.
12/05/2017	2.1	Minor	- Improved the grammar and meaning of certain parts of the text.
12/08/2017	2.2	Minor	- Added information about “Wi-Fi button”, “Digital fingerprint”; - Updated pictures and information.
21/09/2017	2.3	Minor	- Added information about “Automatic procedures”; - Updated pictures and information.
23/11/2017	2.4	Minor	-Updated information about “Automatic procedures”; -Added information about “RAM monitoring”,” Automatic issue report”; -Updated pictures and information.
15/01/2018	2.5	Minor	-Updated content.
31/01/2018	2.6	Minor	-Updated information about “Update Media”; -Updated information about “Report”; -Updated pictures and information.
20/03/2018	2.7	Minor	-Updated information about lots.
23/04/2018	2.8	Minor	- Updated information about erasure status; - Added information about the erasure report, hidden areas and remapped sectors.
19/06/2018	2.9	Minor	- Updated content;