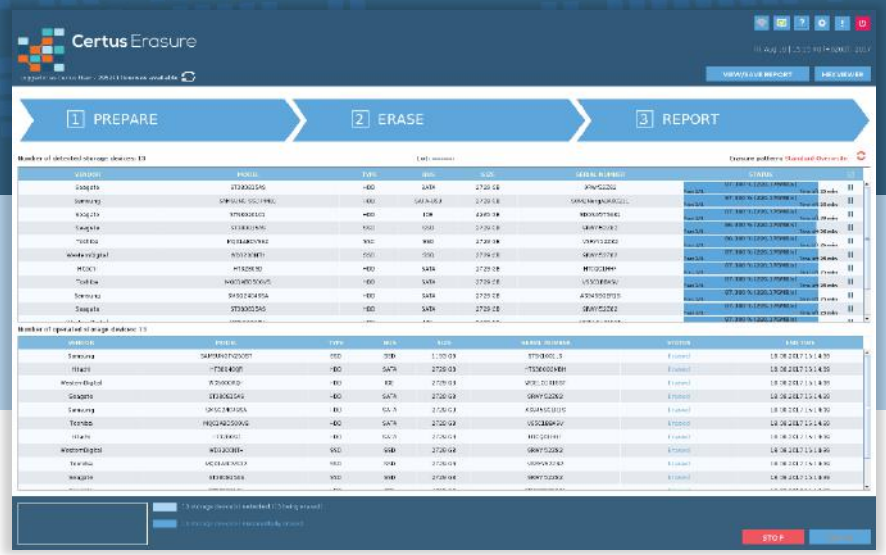
Certus Software

Certified Data Erasure Professionals



Certus Erasure

Quick User Guide

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. INTRODUCTION

This document is a quick guide about how to create the bootable media containing Certus Erasure product, from the downloaded ISO file and how to use it in order to fulfil its designed functionality – completely erase the data contained on the storage devices attached to a computer.

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).

CHAPTER 2. CREATING USB BOOTABLE DRIVE (WINDOWS)

Prerequisites:

1. Computer running Microsoft Windows family operating system;
2. **CertusErasure-X.Y.Z.iso** file and its SHA-256 hash which can both be found on Certus Erasure Web Manager, under “Downloads” section;
3. USB flash drive;
4. Windows application “Win32 Disk Imager”.

2.1. Check the ISO file integrity

After downloading the Certus Erasure ISO file and before attempting to write it on the USB flash drive, make sure that it is not damaged and has not been tampered with. There are many options that can be used in order to achieve this, using online services or various tools; listed below are just a few examples in no specific order, use any method you think is suitable for your case: HTML5 File Hash Online Calculator, OnlineMD5, QuickHash GUI, HashTab.

Here is how the verification should work:

Step 1) Select the downloaded Certus Erasure ISO file;

Step 2) Choose the SHA-256 hashing algorithm;

Step 3) Calculate the hash;

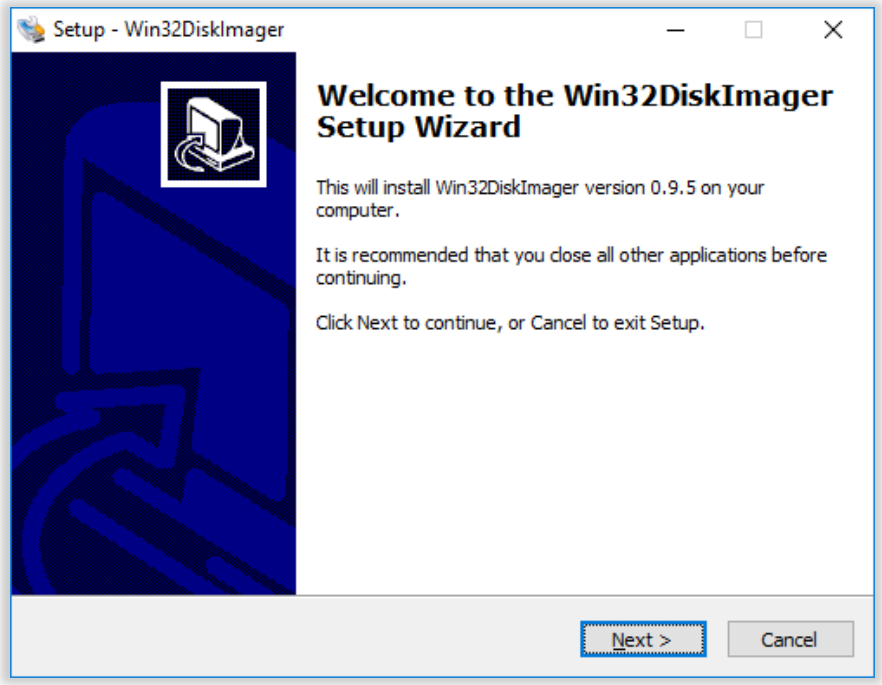
Step 4) Verify that the generated hash matches the file’s hash.

If the values do not match, the downloaded ISO file is NOT valid. In this case do not proceed with the next steps and instead, download the file again and recheck. If the problem persists, please notify us (see **CONTACT** section).

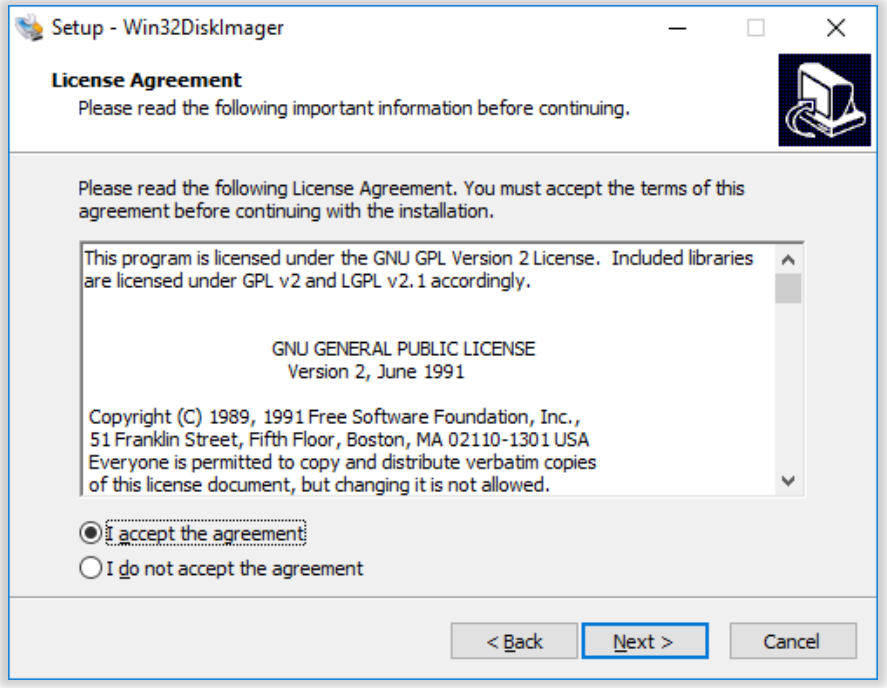
2.2. Installing Win32 Disk Imager

This tool is used to write the raw disk image (e.g. CertusErasure-3.8.0.iso) to the USB Flash drive. Below are the steps needed to be completed in order to install it:

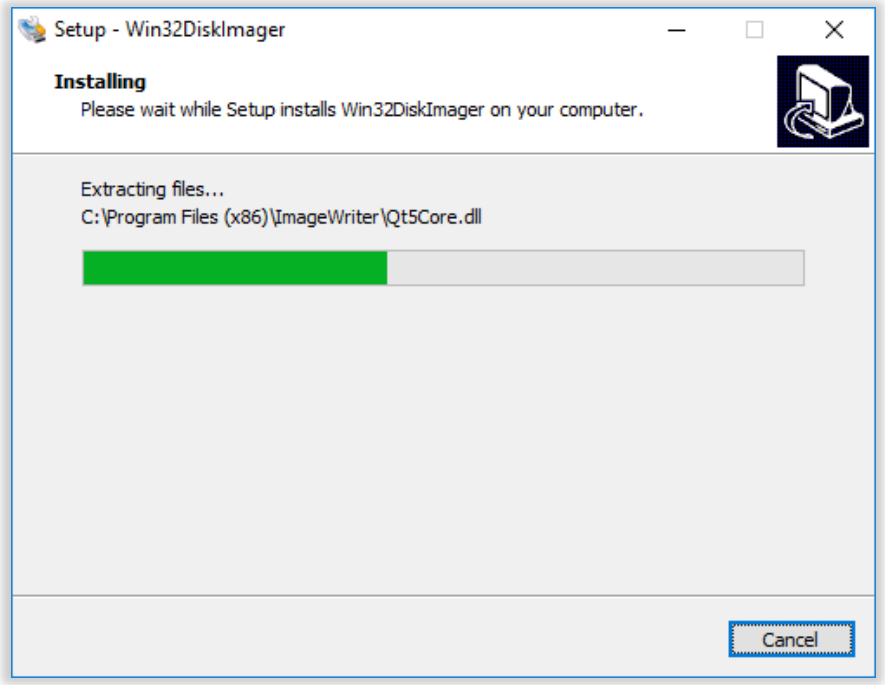
- Download the installer from https://sourceforge.net/projects/win32diskimager/;
- Start the installation process by double clicking on the downloaded file (e.g. Win32DiskImager-0.9.5-install.exe);



- Accept the EULA;

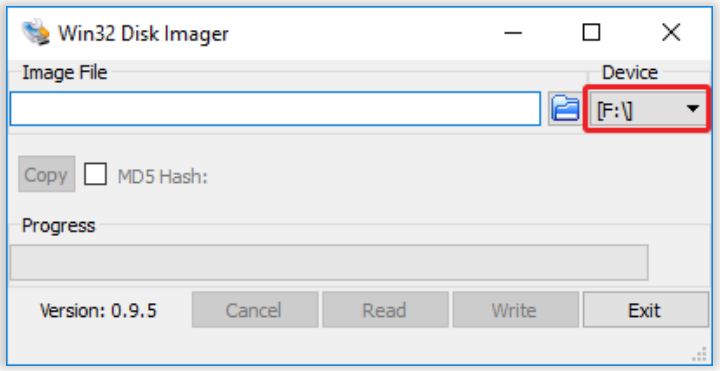


- Follow the installation wizard in order to complete the process.

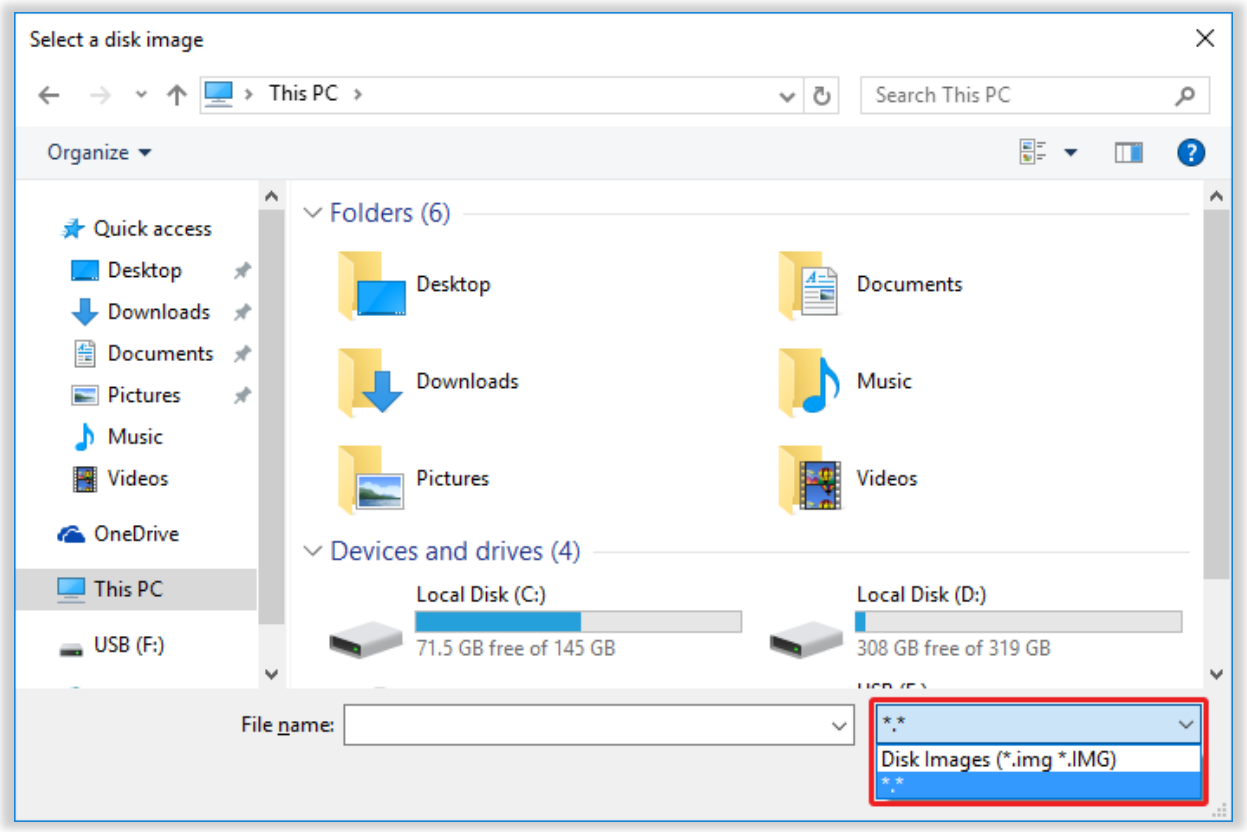


2.3. Using Win32 Disk Imager

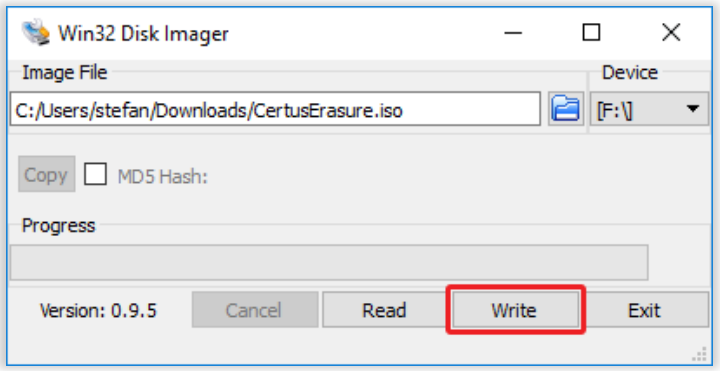
- Insert target USB flash drive;
- Launch Win32 Disk Imager and select the target drive from the device dropdown list;



- Press the file icon (from Image File section) and select the type of the file as *.* from the right dropdown list;



- Browse for the Certus Erasure ISO image file using **Select a disk image** window, select it and press **Open** button;
- Press **Write** button and confirm the start of the writing process. It will transfer the selected image to the selected USB storage device. The end of this process will provide a bootable Certus Erasure USB flash drive, ready to be used.



CHAPTER 3. CREATING USB BOOTABLE DRIVE (LINUX)

Prerequisites:

1. Computer running Linux family operating system;
2. **CertusErasure-X.Y.Z.iso** file and its SHA-256 hash which can both be found on Certus Erasure Web Manager, under “Downloads” section;
3. USB flash drive.

3.1. Check the ISO file integrity

After downloading the Certus Erasure ISO file and before attempting to write it on the USB flash drive, make sure that it is not damaged and has not been tampered with. There are many options that can be used in order to achieve this, using online services or various tools; listed below are just a few examples in no specific order, use any method you think is suitable for your case: HTML5 File Hash Online Calculator, OnlineMD5, QuickHash GUI, HashTab.

Here is how the verification should work:

Step 1) Select the downloaded Certus Erasure ISO file;

Step 2) Choose the SHA-256 hashing algorithm;

Step 3) Calculate the hash;

Step 4) Verify that the generated hash matches the file’s hash.

If the values do not match, the downloaded ISO file is NOT valid. In this case do not proceed with the next steps and instead, download the file again and recheck. If the problem persists, please notify us (see **CONTACT** section).

3.2. Identify USB flash drive

To identify your USB flash drive, in a terminal you can type:

```
[matei@debian:~/Documents]$ sudo fdisk -l
Disk /dev/sdd: 7.2 GiB, 7707033600 bytes, 15052800 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x49ea6a72

Device     Boot Start    End Sectors  Size Id Type
/dev/sdd1  *        0 417791  417792  204M  0 Empty
```

3.3. Unmount USB flash drive

To unmount your USB flash drive, in a terminal type:

```
[matei@debian:~/Documents]$ sudo umount /dev/sdd1
```

3.4. Write Certus Erasure ISO image on USB flash drive

To write the ISO image to your flash drive, in a terminal type:

CHAPTER 4. CREATING USB BOOTABLE DRIVE (MACOS)

Prerequisites:

1. Computer running macOS family operating system;
2. **CertusErasure-X.Y.Z.iso** file and its SHA-256 hash which can both be found on Certus Erasure Web Manager, under “Downloads” section;
3. USB Flash drive.

4.1. Check the ISO file integrity

After downloading the Certus Erasure ISO file and before attempting to write it on the USB flash drive, make sure that it is not damaged and has not been tampered with. There are many options that can be used in order to achieve this, using online services or various tools; listed below are just a few examples in no specific order, use any method you think is suitable for your case: HTML5 File Hash Online Calculator, OnlineMD5, QuickHash GUI, HashTab.

Here is how the verification should work:

Step 1) Select the downloaded Certus Erasure ISO file;

Step 2) Choose the SHA-256 hashing algorithm;

Step 3) Calculate the hash;

Step 4) Verify that the generated hash matches the file’s hash.

If the values do not match, the downloaded ISO file is NOT valid. In this case do not proceed with the next steps and instead, download the file again and recheck. If the problem persists, please notify us (see **CONTACT** section).

4.2. Identify USB flash drive

To identify your USB flash drive, in a terminal you can type:

```
certus-MacBook-Pro:~ Admin$ diskutil list
/dev/disk0
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:      GUID_partition_scheme                        *64.0 GB    disk0
   1:                        EFI EFI                     209.7 MB   disk0s1
   2:                  Apple_HFS MacBook Pro             63.2 GB    disk0s2
   3:                 Apple_Boot Recovery HD             650.0 MB   disk0s3
/dev/disk1
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:      GUID_partition_scheme                        *29.2 MB    disk1
   1:                  Apple_HFS UNetbootin              29.1 MB    disk1s1
/dev/disk2
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:                        USB                         *31.1 GB    disk2
```

4.3. Unmount USB flash drive

To unmount your USB flash drive, in a terminal type:

```
certus-MacBook-Pro:~ Admin$ diskutil unmount /dev/disk2
Volume USB on disk2 unmounted
```

4.4. Write Certus Erasure ISO image on USB flash drive

To write the ISO image to your flash drive, in a terminal type:

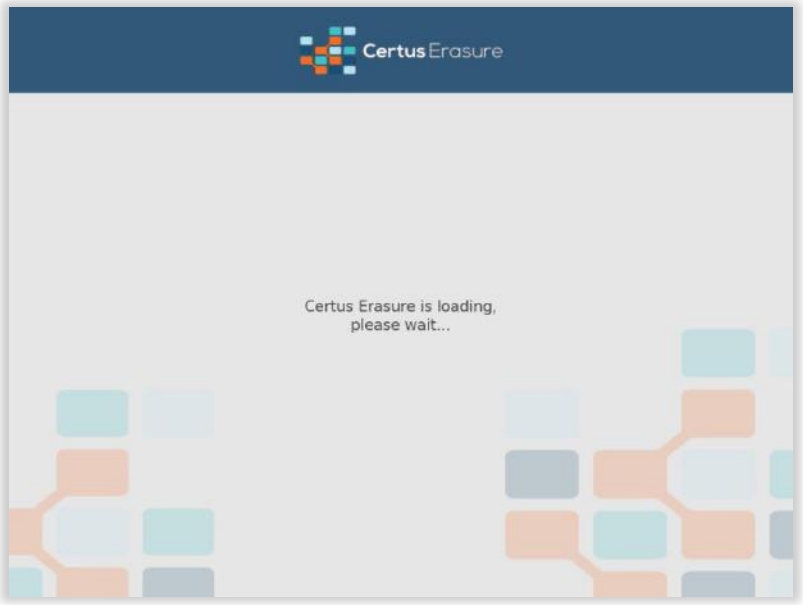
```
certus-MacBook-Pro:~ Admin$ sudo dd if=Desktop/CertusErasure-3.5.1-UEFI.iso of=/dev/disk2 bs=4m
49+1 records in
49+1 records out
207618048 bytes transferred in 30.695569 secs (6763779 bytes/sec)
```

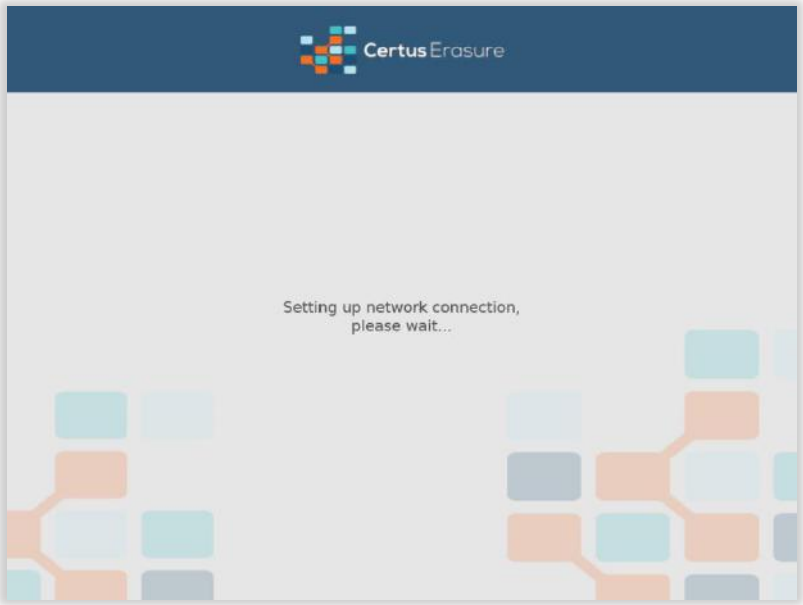
CHAPTER 5. USING CERTUS ERASURE PRODUCT

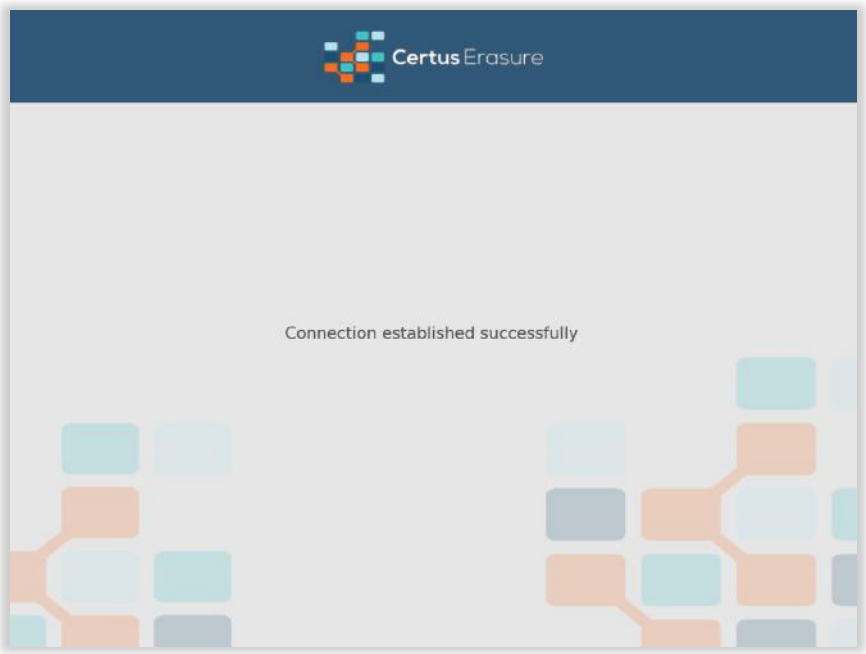
In order to use Certus Erasure on x86 systems, the host machine needs to be booted from the Certus Erasure USB storage device. In this regard, the following steps need to be followed:

5.1. Preparation

- Make sure the host system's boot order (from BIOS) has the USB as the first booting option;
- Plug in Certus Erasure USB drive;
- Power on the host system;
- The software will be loaded into the RAM memory. During the process, the following info will be displayed on the screen:





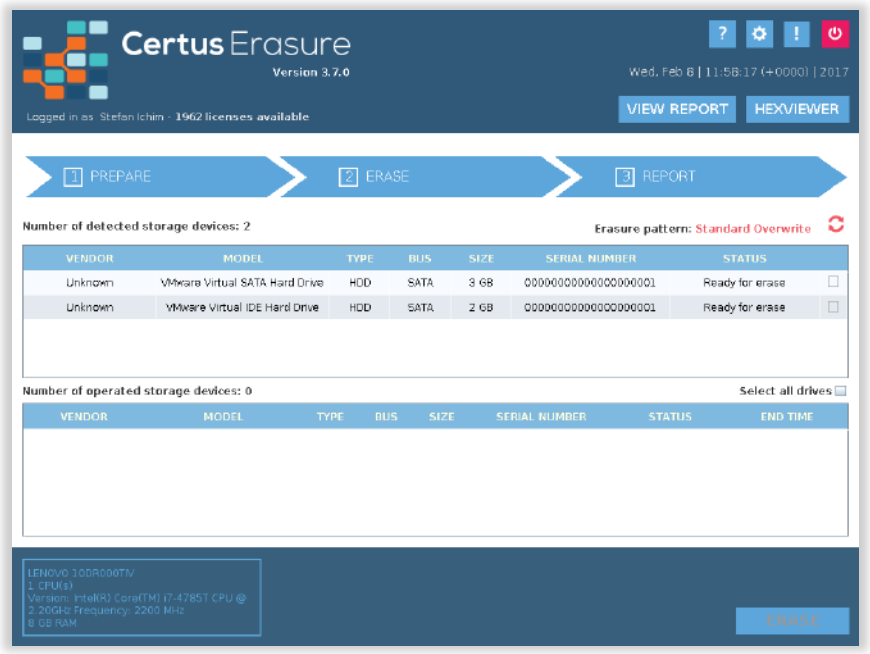


5.2. Authentication

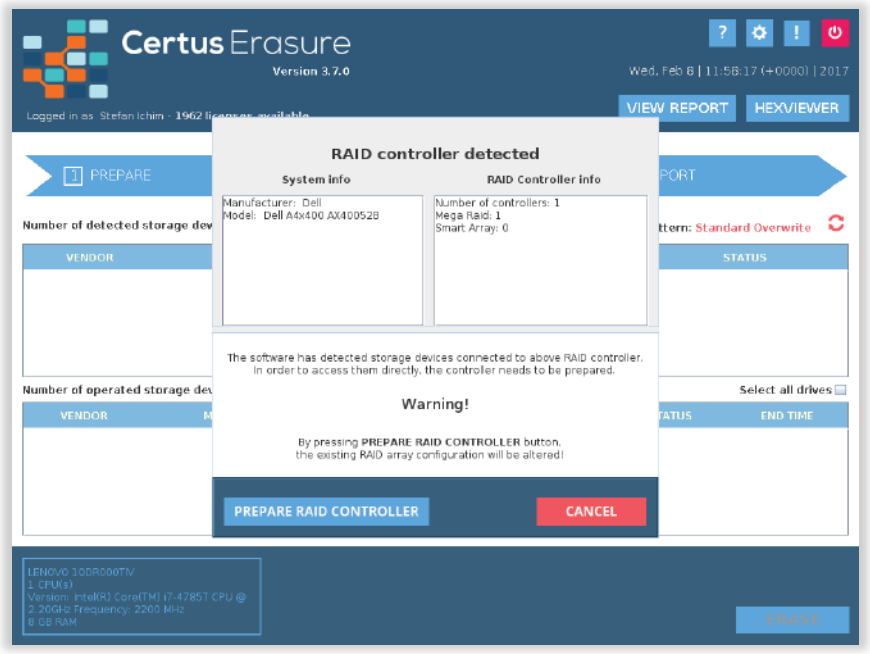
In order to continue, please insert your ***username***, ***password*** and ***customer code***.

5.3. Performing erasure

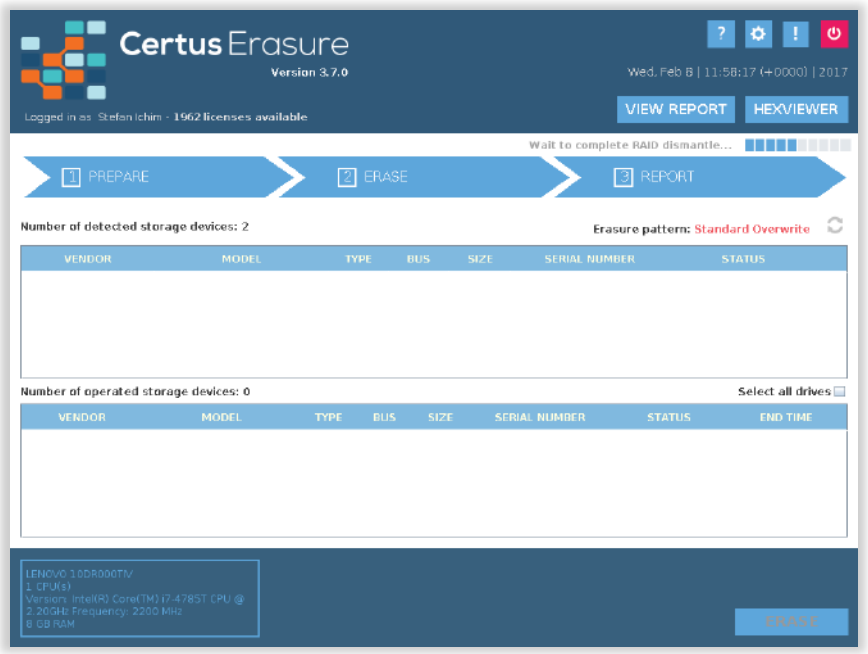
If the inserted credentials are correct, the main view of the Certus Erasure will be displayed.



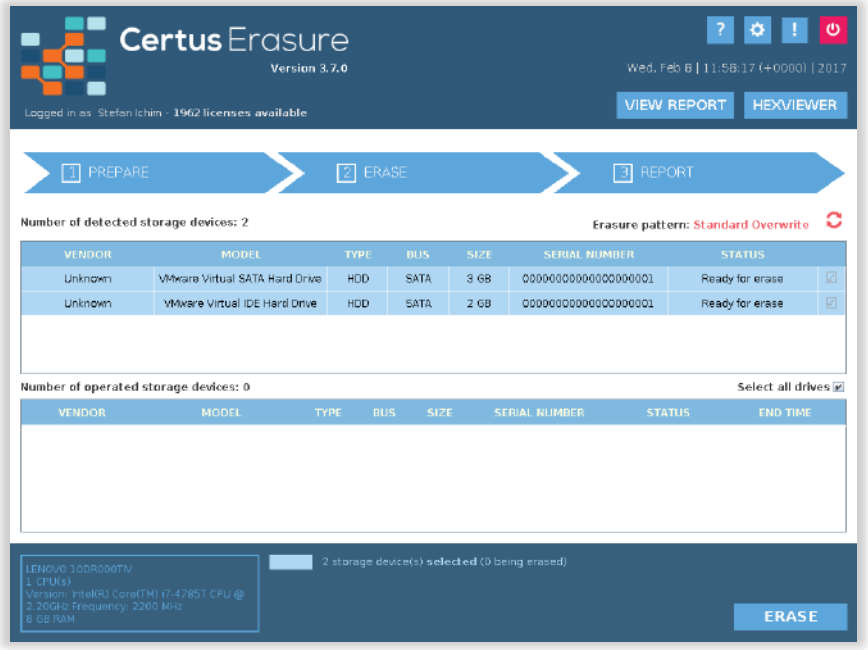
If any RAID controller is detected, a pop-up window will be displayed. In order to erase the HDDs connected to the controller, Certus Erasure product needs to prepare it for such operation. Press the **PREPARE RAID CONTROLLER** button in order to trigger the process of making the RAID HDDs ready for erasure.



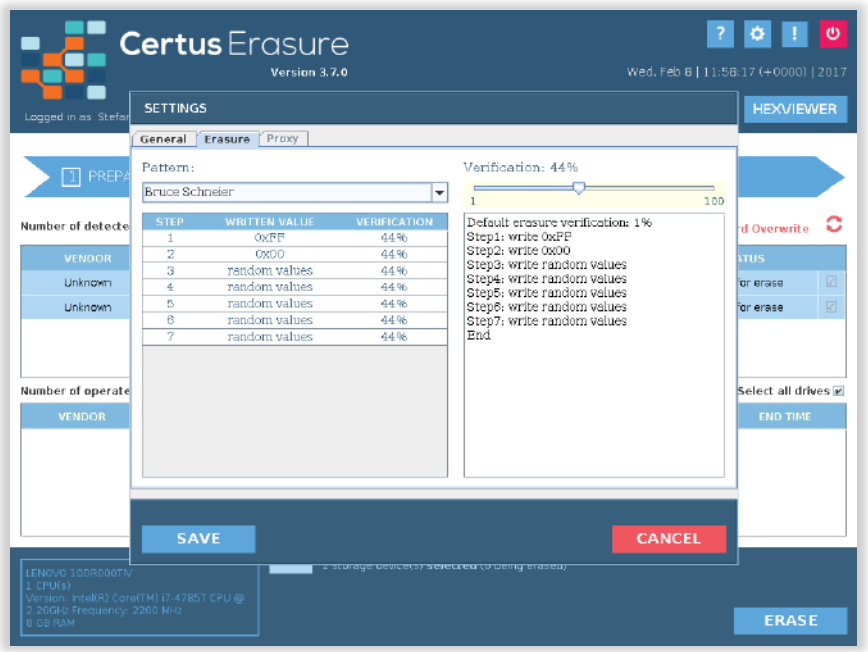
During the RAID preparation process, the following info will be displayed on the screen:



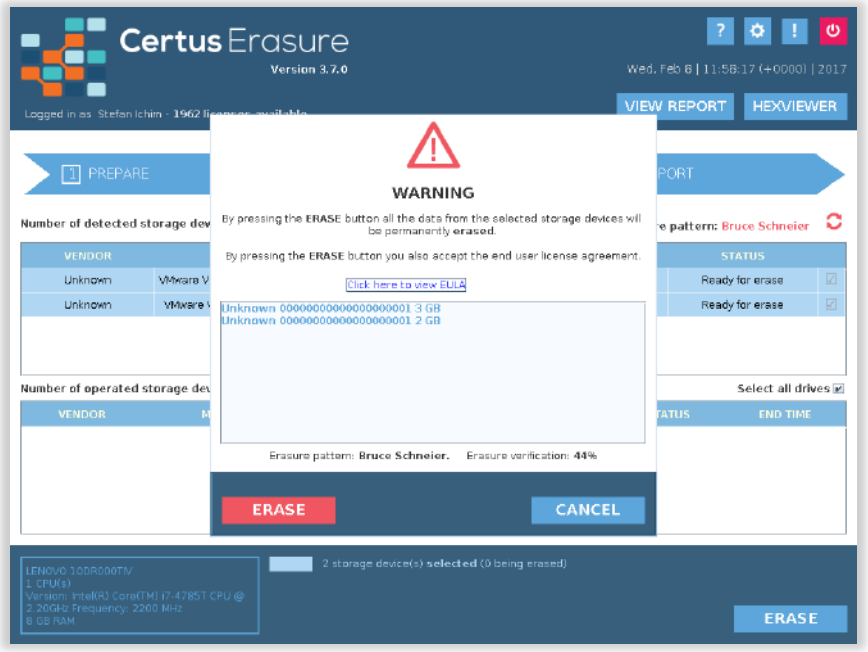
At the end of the process, the info about the connected HDDs will be displayed. Next step is to select the drives required for erasures by checking the checkbox on the right of the table:



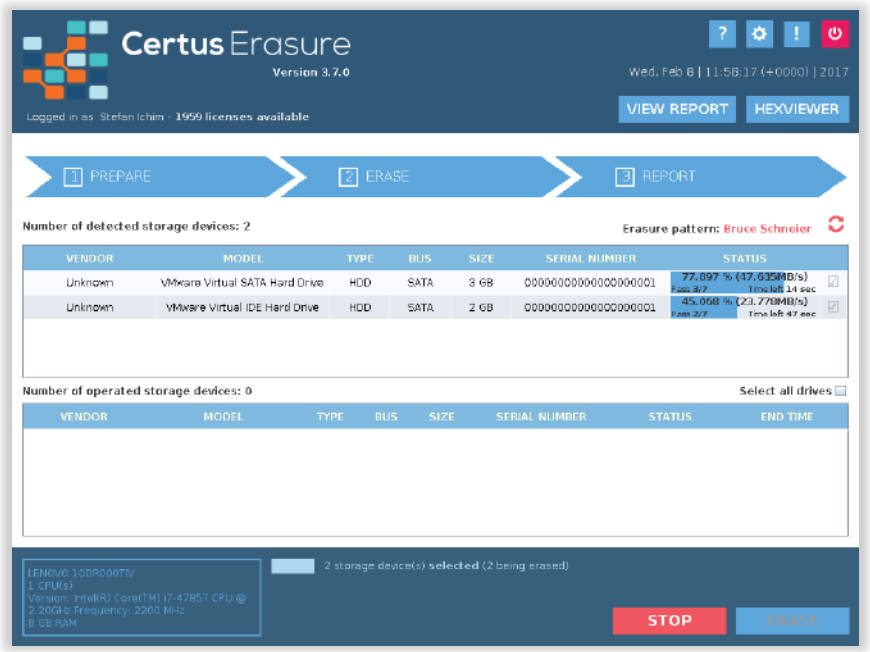
Then press the **SETTINGS** button, select from the pop-up window **Erasure** tab; after that select the erasure pattern and the verification percentage. Save the options by pressing **SAVE** button.



A pop-up confirmation window will be displayed when pressing **ERASE** button.

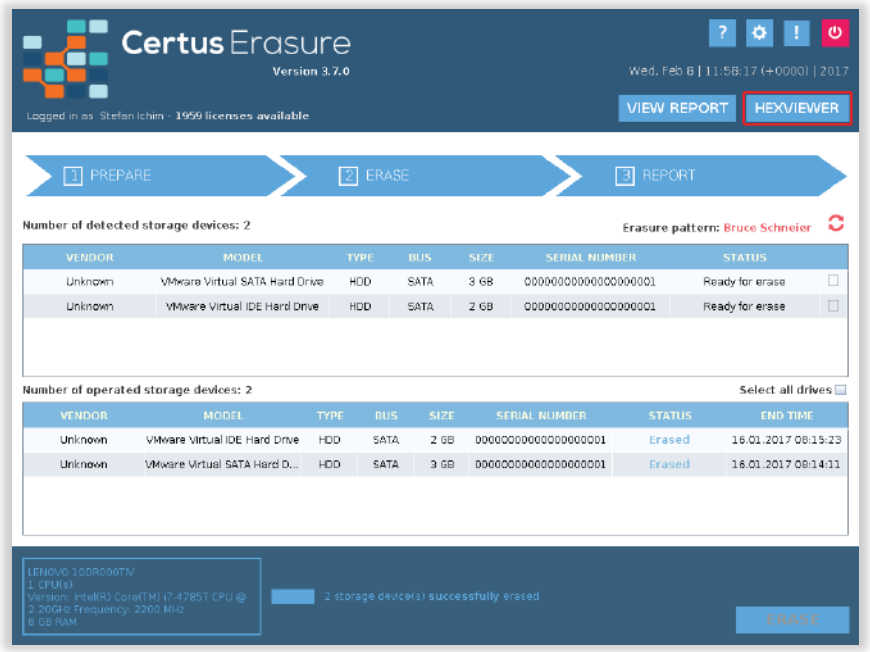


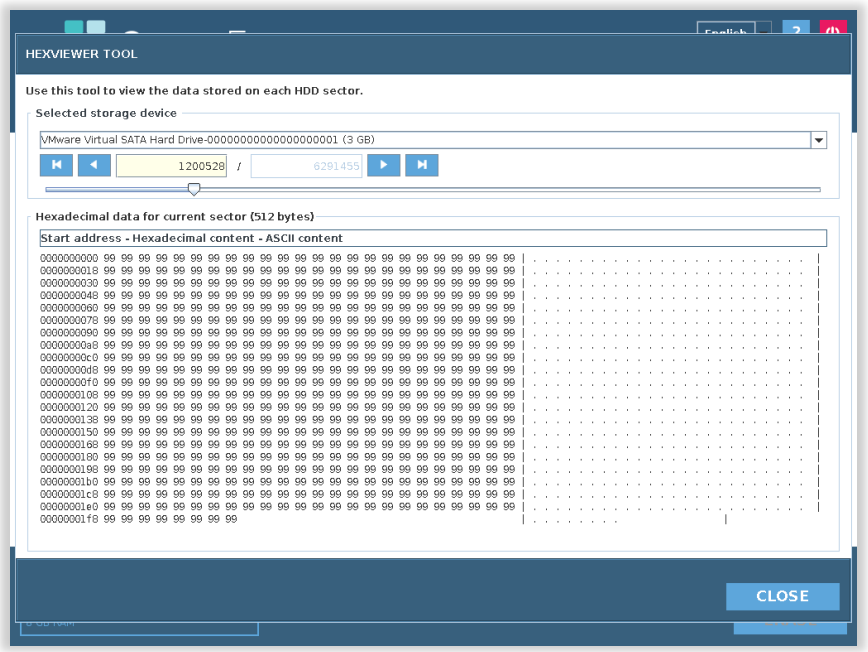
After confirming by pressing on the **ERASE** button, the erasure process will start on the selected devices:



5.4. Checking erasure results

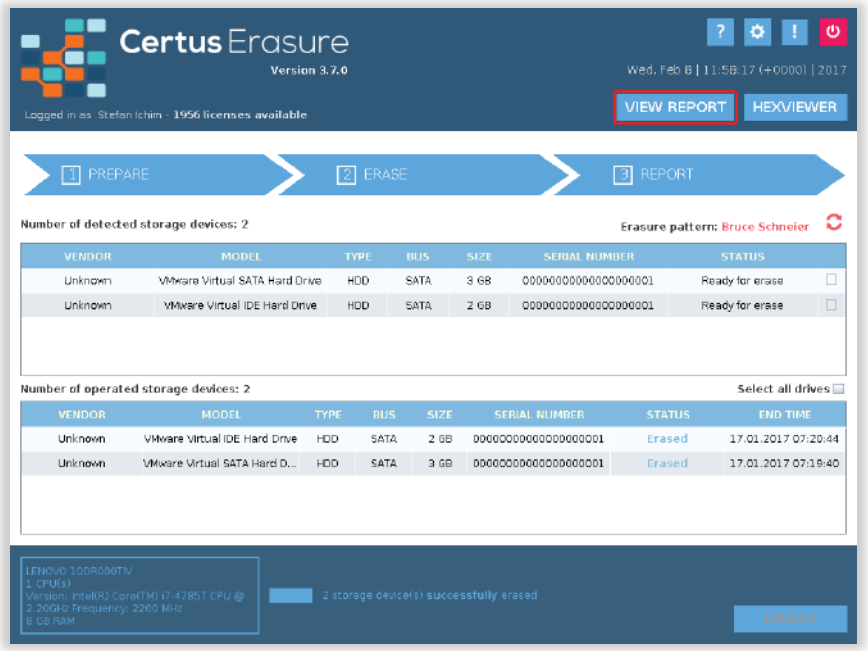
At the end of the erasure process, the results can be examined by pressing the **HEXVIEWER** button:



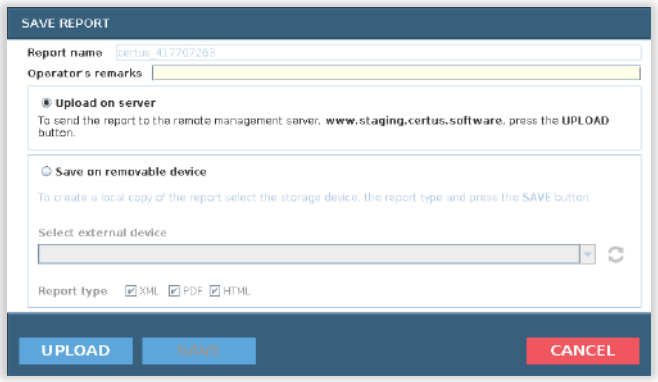


5.5. Saving erasure reports

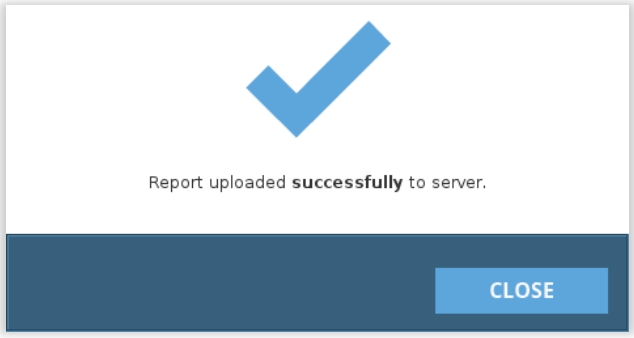
For saving the erasure report, press the **VIEW REPORT** button. A pop-up window will be displayed:

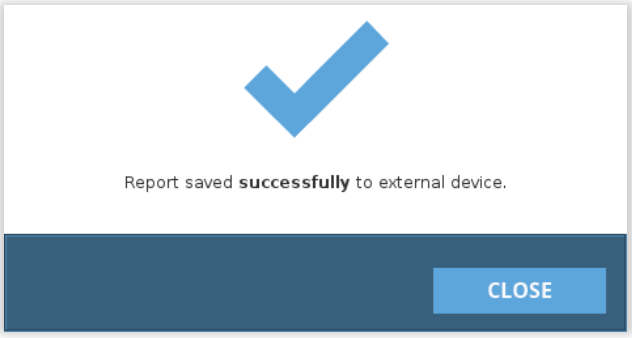


If you click **SAVE** button, a window will appear and you can upload the report on server or save the report on a removable device. If you choose to save on removable device, you can save the report in XML, PDF and HTML formats. Any user remarks can be added on "Operator's remarks" field. The completed field will be saved into the report.

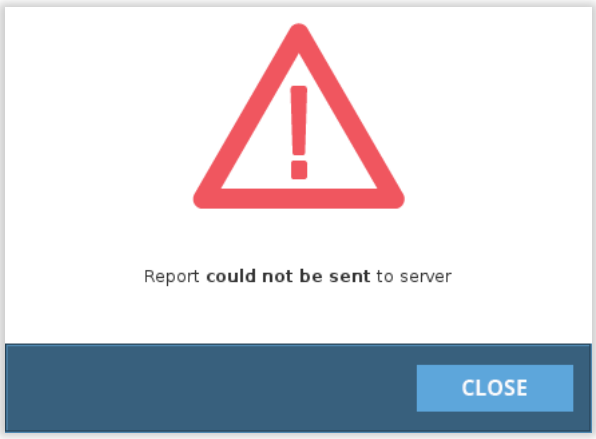


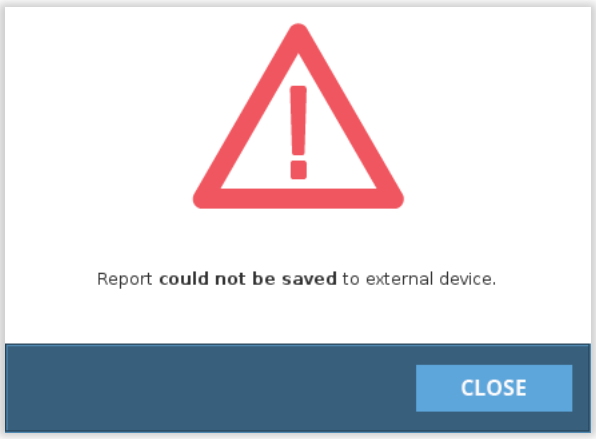
A confirmation window will be displayed after a successful upload to Web Manager server, or after the report has been successfully saved to selected local removable device:





In case of unsuccessful operations, the following windows will be displayed:





CHAPTER 6. 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 the 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 7. DOCUMENT REVISIONS

Date	Revision History	Revision Class	Comments
28/03/2016	1.0	Major	- Initial version.
12/01/2017	2.0	Major	- Updated images to comply with the new GUI; - Updated page layout.
17/01/2017	2.1	Minor	- Updated formatting of the document.
18/01/2017	2.2	Minor	- Added Linux and macOS information about creating a bootable USB flash drive with Certus Erasure.
19/01/2017	2.3	Minor	- Added minimum system requirements.
09/02/2017	2.4	Minor	- Updated images.
19/03/2018	2.5	Minor	- Updated content.