

# BitRaser Drive Eraser

User Guide for version 3.0

[Legal Notices](#) | [About Stellar](#) | [Contact Us](#)

Copyright © Stellar Information Technology Private Limited. All rights reserved.

## Table of Contents

1. GENERAL INFORMATION .....	1
1.1. ABOUT BITRASER DRIVE ERASER .....	2
1.2. ABOUT THE GUIDE .....	4
1.3. CONTACT INFORMATION.....	6
2. GETTING STARTED.....	7
2.1. SYSTEM REQUIREMENTS.....	8
2.2. HOW TO BOOT AND RUN BITRASER DRIVE ERASER .....	9
2.3. CONNECTING TO INTERNET.....	12
2.4. CONNECTING TO BITRASER SERVER .....	16
2.5. GENERAL OVERVIEW OF USER INTERFACE .....	18
3. WORKING WITH THE SOFTWARE.....	20
3.1. ERASURE PROCESS .....	21
3.2. CONFIGURING ERASURE DETAILS.....	26
3.2.1. ERASURE DETAILS.....	27
3.2.2. ASSET TAG DETAILS.....	28
3.2.3. CUSTOM FIELDS .....	29
3.3. WORKING ON REPORT AND CERTIFICATE .....	30
3.3.1. VIEW AND CUSTOMIZE REPORT .....	32
3.3.2. SAVE REPORT .....	34
3.3.3. EXPORT REPORT.....	36
3.3.4. GENERATE AND SAVE CERTIFICATE .....	38
3.4. GENERAL SETTINGS.....	39
3.5. WORKING WITH THE LICENSE MANAGER.....	44
3.6. USING THE HEX VIEWER.....	47
4. FREQUENTLY ASKED QUESTIONS (FAQ).....	48
5. LEGAL NOTICES .....	50
6. ABOUT STELLAR.....	53

# 1. GENERAL INFORMATION

---

1.1. [About BitRaser Drive Eraser](#)

1.2. [About the Guide](#)

1.3. [Contact Information](#)

## 1.1. ABOUT BITRASER DRIVE ERASER

---

### What is BitRaser Drive Eraser?

**BitRaser Drive Eraser** is a portable and reliable application providing permanent data erasure of storage devices. This application erases data in order to prevent the recovery of sensitive data that is no more required. Many organizations and users, while formatting their hard drives, still found an open possibility of data being recovered. **BitRaser Drive Eraser** solves this problem efficiently by using powerful algorithms that fill the storage device with useless binary data. This leaves no possibility for the data to be recovered.

**BitRaser Drive Eraser** is a product of **Stellar**.

### What is disk erasing and how it works?

Disk erasing is the process of permanently deleting data from a hard disk. In its simplest form, a disk erasure method will write all zeros, but in more advanced algorithms, a combination of filling up a disk with random data (either 1s or 0s) plus multiple passes to ensure the impossibility of retrieving data from an erased disk.

### Key Features of BitRaser Drive Eraser:

- **Permanent Data Erasure:** Securely and permanently erase sensitive data from hard drives.
- **Supports Multiple Drives Types:** Supports erasure of IDE, SATA, SCSI hard drives SSD, USB drive and SD card. It also supports reading and writes ATA commands and HPA/DCO detection and removal.
- **Multiple Erasure Methods:** Equipped with 24 world-class erasure methods and up to 5 custom erasure methods can be added as per requirement.
- **Erasure Validation:** Option to verify the erasure through Random verification or Total verification method.
- **Option to Erase Multiple Drives in a Single Session:** Supports up to 32 hard drives for simultaneous erasure.
- **Support for RAID:** Raid dismantling supported for MegaRaid and Adaptec card.
- **Support to Erase Bad/Remap Sectors:** Effectively erase disks containing bad/remapped sectors.
- **Option to Locate a Disk:** While erasing multiple disks, the disk locate feature helps to locate the required disk with a glowing bulb.
- **Option to Add Fingerprint to Drive:** Supports addition of fingerprint at a drive sector after erasure, to verify that the drive has been erased using **BitRaser Drive Eraser** application.

- **Option to View Hard Drive Contents in Hexadecimal:** Provides **Hex Viewer** to view the raw and exact content of the hard drive in hexadecimal format.
- **Reporting and Certification:**
  - Generate 100% secure and tamper-proof reports/certificates.
  - Option to customize a report layout as per requirements.
  - Option to add customized fields to report as per requirements.
  - Option to add verification signatures in a certificate.
  - Automatic report delivering to **BitRaser Cloud Console**. (*Applicable only if you have BitRaser Drive Eraser's licenses on cloud.*)
  - Generates NIST compatible certificates.
  - Support for generating erasure certificates with annexure.
  - Digital identifier and report/certificate data validation feature.
  - Option to save a report in PDF, CSV and XML format.
  - Option to save a certificate in PDF format with or without annexure.
  - Option to export a report from **BitRaser Drive Eraser Lock Key** (USB) edition to import it in **BitRaser Cloud Console**.
  - Full visibility of hardware and erasure details for customized reporting.
- **Cloud Management with BitRaser Server** (*Applicable only if you have BitRaser Drive Eraser's licenses on cloud*): Cloud integration for user management, licenses, and reports. Also, the software automatically saves all reports and certificates on **BitRaser Server**.
- **Supports Encryption for Data Security** (*Applicable only if you have BitRaser Drive Eraser's licenses on cloud*): All the data transferred between the software and **BitRaser Server** is encrypted for data security.
- **Multiple Options to Boot and Run:** Option to boot using either a USB dongle or CD/DVD.
- **Multiple Options to Connect to Internet** (*Applicable only if you have BitRaser Drive Eraser's licenses on cloud*): Option to connect to the internet using either Ethernet or Wireless. It also supports connecting to the internet using a Proxy Server.
- **Option to Change Keyboard Layout:** Supports a keyboard layout of your preferred language.
- **No Expiry of License:** Pay per use – The licenses never get expired.
- **Option to Transfer Licenses** (*Applicable only if you have BitRaser Drive Eraser's licenses on cloud*): Supports transferring of licenses from **BitRaser Cloud Console** to **BitRaser Lock Key**.

## 1.2. ABOUT THE GUIDE

---

Welcome to **BitRaser Drive Eraser User Guide** for version 3.0! Choose a topic from the left to navigate through different topics that are in this guide.

This user guide contains sequential steps to assist you through various functions of **BitRaser Drive Eraser**. Each function is explained in detail, in the corresponding sections. The guide covers the following major topics:

1. [General Information](#)
2. [Getting Started](#)
3. [Working with the Software](#)
4. [Frequently Asked Questions \(FAQ\)](#)
5. [Legal Notices](#)
6. [About Stellar](#)

This guide is intended for individuals who use **BitRaser Drive Eraser** to erase storage devices to prevent recovery of sensitive data that is no more required.

This guide is helpful if you are using **BitRaser Drive Eraser** application with license information either on cloud or a USB lock key. There are minor differences in the functionality of **BitRaser Drive Eraser** if you are using cloud or a USB lock key for accessing the license information. These differences are given in detail, in the corresponding topics of this guide.

This guide has the following features for easy navigation and understanding:

There are **Cautions** and **Notes** in some topics of this guide for better understanding and ease of work. These **Cautions** and **Notes** are given in *italics style*.

Definition of acronyms used in this guide:

ITEM	EXPLANATION
Bad Sectors/Bad Blocks	Bad sectors or bad blocks are the space of the disk which can't be used due to the permanent damage or OS is unable to access it.
BIOS	BIOS stands for Basic Input/Output System. The BIOS is a computer program embedded on a chip on a computer's motherboard that recognizes and controls various devices that make up the computer.
HDD	Hard disk drive (HDD) storage is made up of magnetic tape and has mechanical parts inside. This type of drive is cheaper and available with more storage space than SSDs.
HPA/DCO	The Host Protected Area (HPA) and Device Configuration Overlay (DCO) are features for hiding sectors of a hard disk from being accessible to the end user.
ISO file	An ISO file, often called an ISO image, is a single file that's a perfect representation of an entire CD or DVD. The entire contents of a disc can be precisely duplicated in a single ISO file.

KB, MB, GB and TB	This measure is used to describe memory capacity and disk storage. A kilobyte (KB) is 1,024 bytes, and one megabyte (MB) is 1,024 kilobytes. One gigabyte (GB) is equal to 1,024 megabytes, while a terabyte (TB) is 1,024 gigabytes.
PDF	"Portable Document Format" is a file format designed to present documents consistently across multiple devices and platforms.
PNG	Portable Network Graphics (PNG) is a raster-graphics file-format for image compression.
SSD	Solid State Drive (SSD) is flash storage and has no moving parts whatsoever. As a result, they're smaller and take up less space in a PC. They are much faster to read and write when comparison to HDD.
User ID	Stands for User identification, which by default is the e-mail address of the user in this guide.
XML	"Extensible Markup Language" is a metalanguage that allows users to define their own customized markup languages, especially to display documents on the Internet.
ZIP	ZIP is an archive file format that supports data compression. A ZIP file may contain one or more files or directories that may have been compressed.

For any queries or feedback related to this guide, kindly [contact us](#).

## 1.3. CONTACT INFORMATION

---

Our **Technical Support** professionals will give solutions for all your queries related to **BitRaser Drive Eraser**.

- You can either call us or go online to our support section at <http://www.stellarinfo.com/support/>
- For price details and to place the order, click <https://www.bitraser.com/buy/> or e-mail the sales team at [sales@bitraser.com](mailto:sales@bitraser.com)
- To join our partner network, click <https://www.bitraser.com/partner/>
- To connect to our partner team, e-mail us at [partner@bitraser.com](mailto:partner@bitraser.com)
- Chat Live with an Online technician at <https://www.bitraser.com/>
- Search in our extensive Knowledgebase at <https://www.bitraser.com/kb/>
- Submit query at <https://www.bitraser.com/contact-us/>
- E-mail to Stellar Support at [support@stellarinfo.com](mailto:support@stellarinfo.com)



## 2. GETTING STARTED

---

- 2.1. [System Requirements](#)
- 2.2. [How to Boot and run BitRaser Drive Eraser](#)
- 2.3. [Connecting to Internet](#)
- 2.4. [Connecting to BitRaser Server](#)
- 2.5. [General Overview of User Interface](#)

## 2.1. SYSTEM REQUIREMENTS

---

Before you start using **BitRaser Drive Eraser**, make sure that your computer meets the following requirements.

### Minimum System Requirements:

- **Processor:** x86 or x64 Processor
- **RAM:** 1 GB Minimum (4 GB Recommended)
- **Optical Drive**, if you are using an optical disk (CD/DVD) to boot your computer.
- **USB PORT 2.0 / 3.0**, with an option in the BIOS to boot computer from USB device, if you are using a USB to boot your computer.

**Note:** For the **BitRaser Drive Eraser** with cloud licensing, you need an active internet connection.

**Note:** If you are using a **BitRaser Lock Key (USB)** for licensing, you need two USB ports - one for bootable USB device and another one for **BitRaser Lock key**.

## 2.2. HOW TO BOOT AND RUN BITRASER DRIVE ERASER

---

To boot and run **BitRaser Drive Eraser** on your computer or laptop, you will need a bootable media with **BitRaser Drive Eraser ISO file** installed on it. An ISO file combines all the **BitRaser Drive Eraser** installation files into a single uncompressed file.

- For the **BitRaser Drive Eraser**'s edition with licenses on cloud, you can receive the software in two ways: You can receive a **BitRaser Drive Eraser** bootable media (USB drive or DVD), or you can receive a link to download a **BitRaser Drive Eraser ISO file**.

If you have downloaded the **BitRaser Drive Eraser ISO file**, you can create a bootable media. To do this, copy the ISO file onto your drive and then burn the ISO onto a USB drive or DVD using any 3rd party software. Now install **BitRaser Drive Eraser** onto your computer directly from your USB or DVD drive using the steps given below.

- For the **BitRaser Drive Eraser**'s edition with licenses on a lock key (USB), you will receive a USB device called as **BitRaser Lock Key** for licenses and a bootable media (USB drive or DVD) when you purchase the software. Using the bootable media, you can boot and run **BitRaser Drive Eraser** with steps as given below.

**Note:** The **BitRaser Drive Eraser** application boots and run using the RAM of your computer; which means **BitRaser Drive Eraser** does not occupy space on your computer's hard drive and the working of **BitRaser Drive Eraser** is not affected if you erase your hard drive using the application. Also, it means that a single session of **BitRaser Drive Eraser** is only valid till your system reboots. Upon rebooting, you must boot and run **BitRaser Drive Eraser** again using the bootable media for another session.

### Steps to Boot and run BitRaser Drive Eraser:

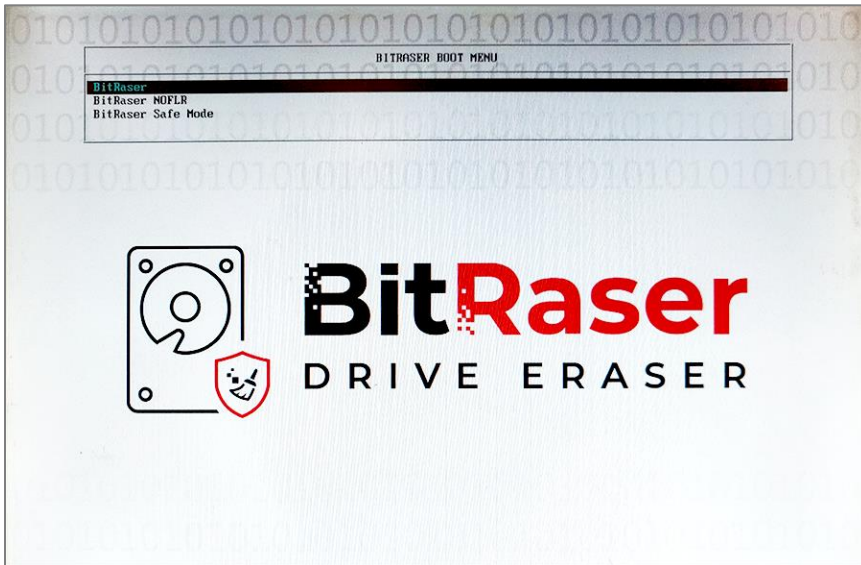
Verify the **BitRaser Drive Eraser** bootable media is connected to your computer and use the following steps:

**Note:** Also, connect the **BitRaser Lock Key** at this stage if you have licenses on **BitRaser Lock Key**.

1. Power on your computer and check the BIOS boot options to boot from the bootable media (USB drive or DVD).

**Note:** To know how to check the BIOS boot options, refer to the manufacturer's documentation that came with your computer.

2. Once the computer boots, you will see the "**BitRaser Boot Menu**" screen.



3. This screen has the following options:

3.1. **BitRaser**: This is the default option to run **BitRaser Drive Eraser**. This option runs **BitRaser Drive Eraser** automatically in the most commonly used system configuration.

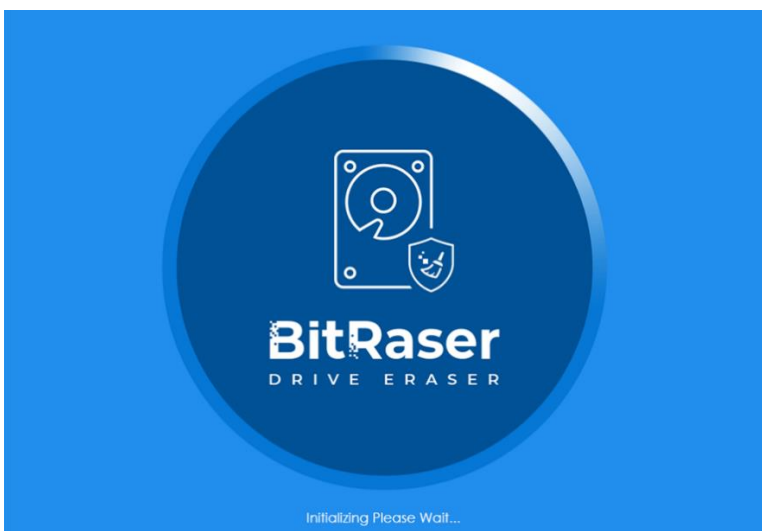
**Note:** *It is recommended that you use this option to run the **BitRaser Drive Eraser** successfully.*

3.2. **BitRaser NOFLR**: This option uses a NOFLR functionality and mostly used if the **BitRaser Drive Eraser** fails to run using the first option.

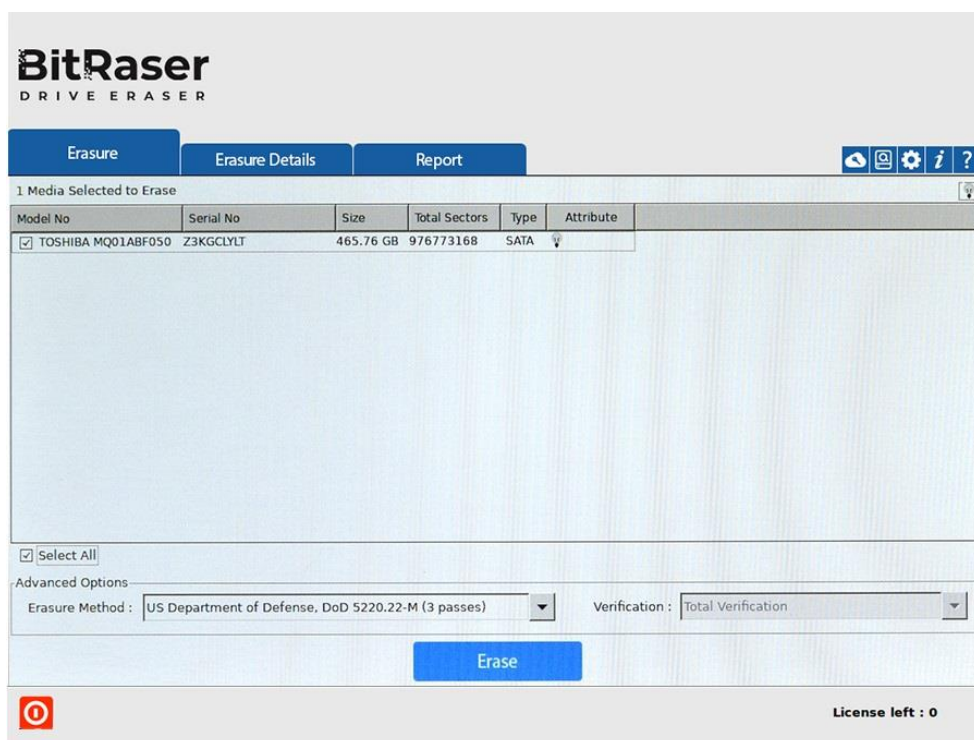
3.3. **BitRaser Safe Mode**: This option uses a safe mode functionality and boots up the **BitRaser Drive Eraser** with minimum resources that are required to run the application.

**Note:** ***BitRaser Drive Eraser** automatically runs using the first option if there is no input from the user in 30 seconds. Use the arrow keys on your keyboard to cancel the action within 30 seconds.*

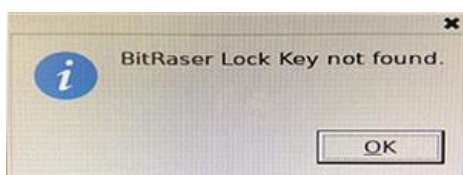
4. The **BitRaser Drive Eraser** now starts to boot and load from the bootable media. The following screen appears:



5. Once the system booting is completed, you see the **BitRaser Drive Eraser** running on your screen as shown below:



**Note:** If you have license information on **BitRaser Lock Key** and the key is not connected, you will see an error message as shown below:



Click **OK**, the following dialog box appears:




Connect the **BitRaser Lock Key** to the USB port of your computer and Click **Yes**.

## 2.3. CONNECTING TO INTERNET

*This topic is only applicable if you have BitRaser Drive Eraser's licenses on cloud.*

Once the **BitRaser Drive Eraser** application is started, you must connect to the internet to connect **BitRaser Server** and acquire license information. To connect to the internet, use the following steps:

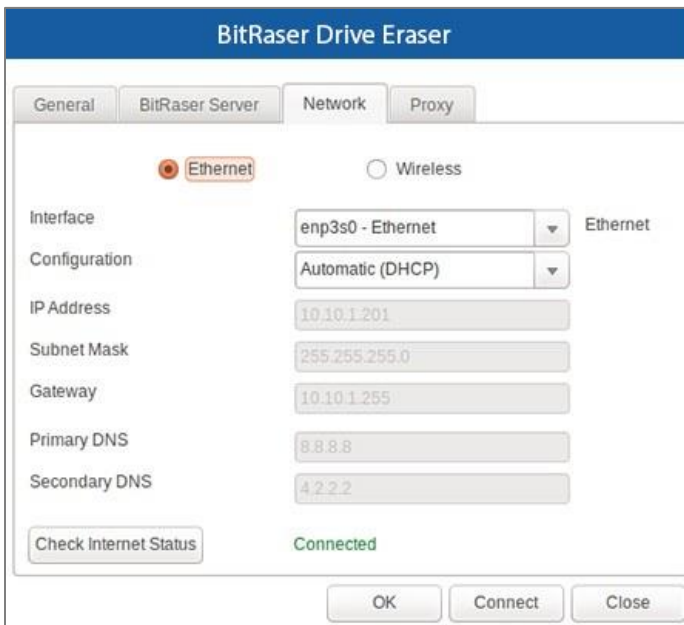
1. Click on the **Settings**  icon on the top right corner of the screen, the settings window appears. This window can be used to change various general and default settings of the software. This window has the following tabs:
  - [General settings](#)
  - [BitRaser Server settings](#)
  - [Network settings](#)
  - [Proxy settings](#)
2. Click on **Network** tab. This tab has the following options to connect to the internet:
  - [Ethernet](#)
  - [Wireless](#)

**Note:** The **Wireless** option will only be available if you have a wireless network card installed on your computer.

**Note:** If you wish to connect internet using a proxy, see [Proxy Settings](#).

- **Ethernet:**

This option has the following fields:



- **Interface:** Use this field to select the Interface Device from the drop-down options, with which you wish to connect the **BitRaser Drive Eraser** to the internet.

- **Configuration:** Use this field to select **Automatic (DHCP)** or **Manual** Internet Protocol (IP) configuration from the drop-down options.
  1. **Automatic (DHCP)** Configuration: The **Automatic (DHCP)** configuration is selected in this field by default. This configuration will fill up all the required fields automatically.
  2. **Manual** Configuration: This configuration has the following fields to fill:
    - **IP Address** - In the given field, enter the IP address as provided by your network administrator. Enter the network's Subnet Mask in the field below it.
    - **Gateway** - The network's gateway IP address.
    - **Primary DNS** - The network's primary DNS IP address.
    - **Secondary DNS** - The network's secondary DNS IP address.

- **Wireless:**

The screenshot shows the 'BitRaser Drive Eraser' application window with the 'Network' tab active. Under the 'Wireless' section, the 'Interface' is set to 'wlp4s4 - Wireless', the 'SSID Name' is 'Bitraser-M', and the 'Password' field is masked with dots. A 'Check Internet Status' button is present, and the status is shown as 'Connected'. Navigation buttons 'OK', 'Connect', and 'Close' are at the bottom.

This option has the following fields:

- **Interface:** From the Interface dropdown menu, select the interface device you wish to use.
- **SSID Name:** From the SSID Name menu, select the wireless network that you wish to connect to.
- **Password:** Enter the password of the wireless network, if the network is password protected (password is not required if you are connecting to an open network).

**Note:** You will not see any network in the **SSID Name** dropdown menu if the wireless adapter is switched off or is not configured correctly.

3. After filling in the above details, click on **Connect**. **Configured DHCP/Network/Wifi connection** message appears showing you that the settings have been configured.
4. Check the internet connectivity by clicking on "**Check Internet Status**" button.

5. If the application is successfully connected to internet, the **Network Status** shows "Connected". If the connection is unsuccessful, the **Network Status** shows "Delay in response. Check status again."

**Note:** If the **Network Status** shows "Delay in response. Check status again." -

- Check that the LAN cable is properly connected to your computer when connecting using **Ethernet**.
- Check the details you have entered are correct.


6. Click **OK** or **Close** button to exit the settings window.



## PROXY SETTINGS:

*This topic is only applicable if you have BitRaser Drive Eraser's licenses on cloud.*

**BitRaser Drive Eraser** gives an option to connect to a Proxy server if required. To connect to a Proxy, do the following steps-

1. Click on the **Settings**  icon on the top right corner of the screen, the settings window appears. This window can be used to change various general and default settings of the software. This window has the following tabs:

- [General settings](#)
- [BitRaser Server settings](#)
- [Network settings](#)
- [Proxy settings](#)

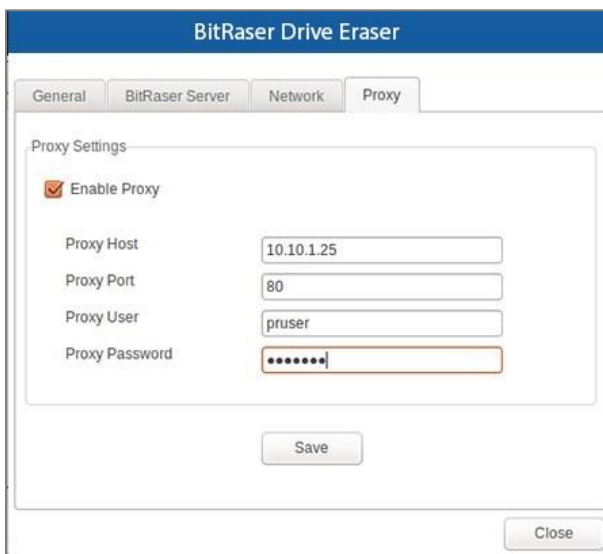
2. Click on **Proxy** tab.

3. Check the **Enable Proxy** check-box.

**Note:** If you are connected to the internet, selecting **Enable Proxy** will disconnect the internet.

4. The following fields need to be filled:

FIELD NAME	DESCRIPTION
Proxy Host	Enter the address of the proxy server.
Proxy Port	Enter the port number that the proxy server uses.
Proxy User	Enter the proxy user name.
Proxy Password	Enter the authentication password of the proxy user.




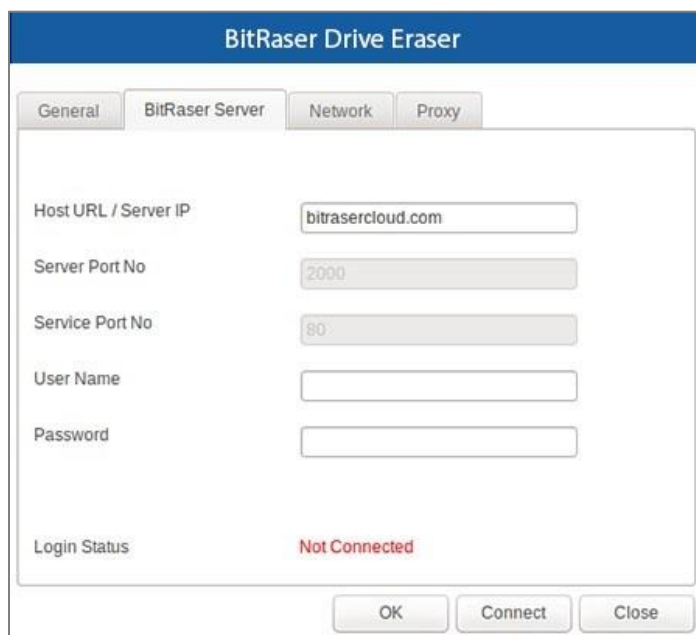
5. Click on **Save** to use the entered proxy settings.
6. Use the **Network Tab** to connect to the internet with the saved proxy details.

## 2.4. CONNECTING TO BITRASER SERVER

*This topic is only applicable if you have BitRaser Drive Eraser's licenses on cloud.*

In order to acquire the **BitRaser Drive Eraser** licenses for performing the erasure process, you need to connect **BitRaser Drive Eraser** application to the **BitRaser Server**. Once the **BitRaser Drive Eraser** is [connected to internet](#), use the following steps to connect to **BitRaser Server**:

1. Click on the **Settings**  icon on the top right corner of the screen, the settings window appears. This window has the following tabs:
  - [General settings](#)
  - [BitRaser Server settings](#)
  - [Network settings](#)
  - [Proxy settings](#)
2. Click on **BitRaser Server** tab. This tab has the following fields to fill:



The screenshot shows the 'BitRaser Drive Eraser' settings window with the 'BitRaser Server' tab selected. The window contains the following fields and controls:

- Host URL / Server IP:** A text field containing 'bitrasercloud.com'.
- Server Port No:** A text field containing '2000'.
- Service Port No:** A text field containing '80'.
- User Name:** An empty text field.
- Password:** An empty text field.
- Login Status:** A label showing 'Not Connected' in red text.
- Buttons:** 'OK', 'Connect', and 'Close' buttons at the bottom.

FIELD NAME	DESCRIPTION
Host URL / Server IP	Host URL or Server IP address where the BitRaser Cloud Console is located.
User Name	User Name which is used to login to the BitRaser Cloud Console.
Password	Password which is used to login to the BitRaser Cloud Console.

**Note:** The fields **Server Port No** and **Service Port No** are disabled and cannot be modified.

3. After filling the above details. Click on **Connect**.
4. If the application is successfully logged into **BitRaser Server**, the **Login Status** shows "Connected". If the login is unsuccessful, the **Login Status** shows "Not Connected".

The screenshot shows the 'BitRaser Drive Eraser' application window with the 'BitRaser Server' tab selected. The window contains the following fields and controls:

- Host URL / Server IP:** A text box containing 'bitrasercloud.com'.
- Server Port No:** A text box containing '2000'.
- Service Port No:** A text box containing '80'.
- User Name:** A text box containing 'disk@merge.com'.
- Password:** A password field represented by ten black dots.
- Login Status:** A label showing 'Connected' in green text.
- Buttons:** 'OK', 'Connect', and 'Close' buttons are located at the bottom right of the window.

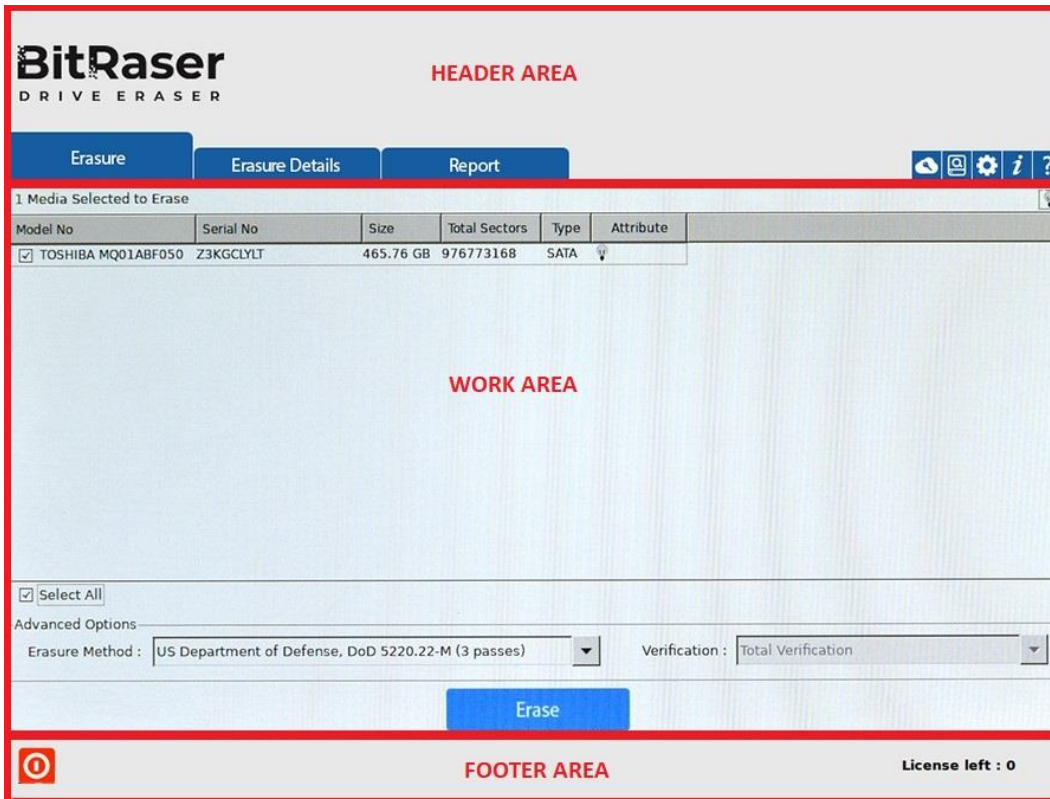
**Note:** If the **Login Status** shows **Not Connected**, check the details you have entered are correct and try again.






5. Click **OK** or **Close** button to exit the settings window.





## 2.5. GENERAL OVERVIEW OF USER INTERFACE

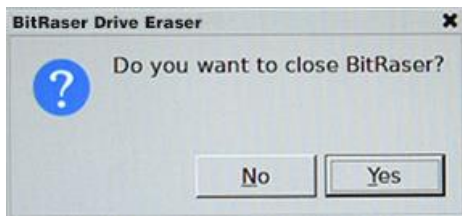
The User Interface is divided into three main areas:

- Header area
- Work area
- Footer area



- **Header Area:** The header area contains following tabs and buttons:
  - **Erase Tab** : This tab contains a list of the connected drives in a list view and is used to perform erasure process.
  - **Erasure Details Tab** : This tab is used to enter various details to be included in reports. To know more, see the [Configuring Erasure Details](#) Section.
  - **Report Tab** : This tab provides **BitRaser Drive Eraser** report and various options for [Working on Reports](#).
  - **License Manager Button**  (*Available only if you have BitRaser Drive Eraser's licenses on cloud*): Click this button to get the license information from **BitRaser Cloud** or to transfer licenses from **BitRaser Cloud** to **BitRaser Lock Key**.
  - **Hex Viewer Button** : Click this button to view the data on the attached hard drives in 'raw' hexadecimal code.

- **Settings Button**  : Click this button to update various settings available for **BitRaser Drive Eraser**.
- **About Button**  : Click this button to see information about **BitRaser Drive Eraser** and system information. The about page also has buttons for **Support** and **License** information.
- **Help Button**  : Click this button to open this help guide from the application.
- **Work Area:** The work area contains all the specific information and functionality of the selected tab or button.
- **Footer Area:** The footer area contains the following button and information:
  - **Power Button**  : Click this button to shut down **BitRaser Drive Eraser**. The following screen appears, click **Yes** to close and **No** to cancel the action:



- **License Information:** This shows the number of licenses left to perform erasure process.

**Note:** If you have the licenses on cloud and the application is not connected to **BitRaser Server**, the number of licenses will be shown as zero.

## 3. WORKING WITH THE SOFTWARE

---

- 3.1. [Erasure Process](#)
- 3.2. [Configuring Erasure Details](#)
- 3.3. [Working on Report and Certificate](#)
  - 3.3.1. [View and Customize Report](#)
  - 3.3.2. [Save Report](#)
  - 3.3.3. [Export Report](#)
  - 3.3.4. [Generate and Save Certificate](#)
- 3.4. [General Settings](#)

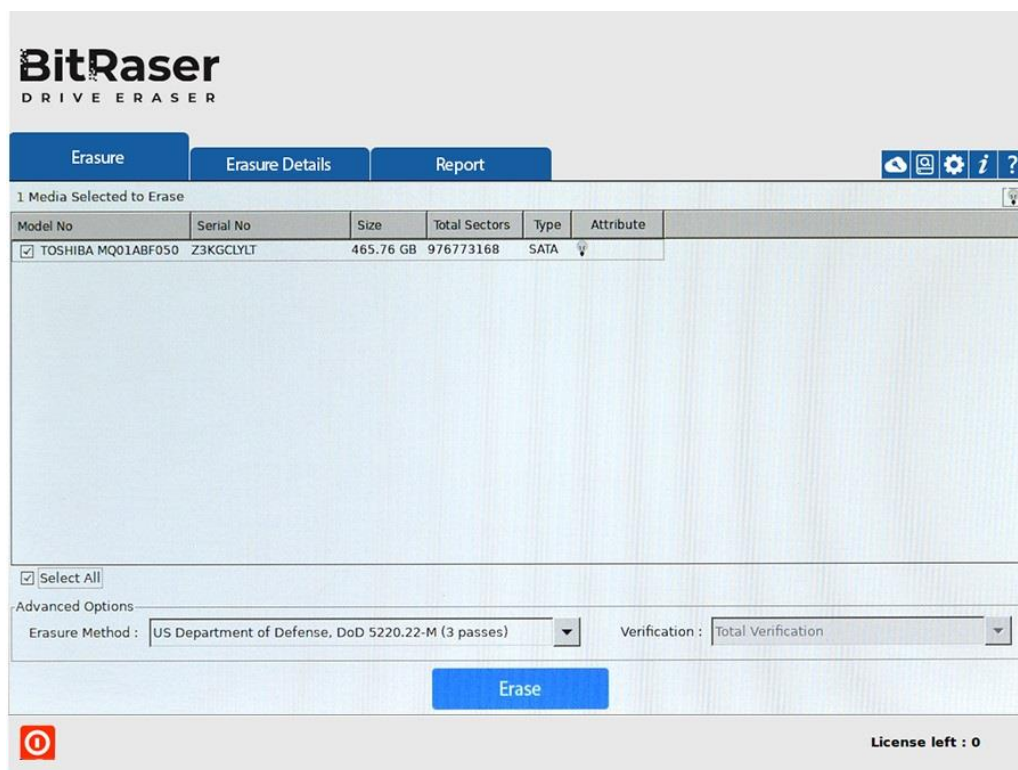
## 3.1. ERASURE PROCESS

You can securely erase data from your hard drive by using erasure feature of **BitRaser Drive Eraser**. You can choose an erasure method from a list of 24 data erasure methods. Selection of erasure method is available under **Advanced Options** section. Also, three verification options are available to you to verify that the data has been erased permanently and is no longer recoverable.




**Note:** You can erase up to 32 hard drives simultaneously using **BitRaser Drive Eraser**.

To erase data using BitRaser Drive Eraser:

1. Run **BitRaser Drive Eraser** application. You will see the screen as displayed below.



2. All storage devices along with their information like model number, serial number, size, total sectors, type, and attribute are displayed in the form of a list.

3. If you have multiple disks, **BitRaser Drive Eraser** provides an option to locate the disk from the application. Click on  in the Attribute column of the disk that you want to locate. Alternatively, click on  in top right corner of the screen to locate all the disks listed in the application. This illuminates the LED light  (commonly known as activity indicator) on the disks to locate them easily.

4. All the storage devices are selected by default for erasure. Uncheck against the storage devices that you do not want to erase.

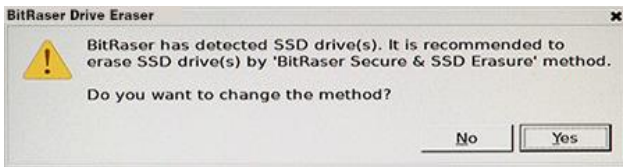
5. From **Advanced Option** section, select any one of the following erasure methods:

ERASURE METHODS	DESCRIPTION
Zeroes	This algorithm erases data by overwriting it with zeros in a single pass. This is the fastest algorithm available to a user.
Pseudo-random	This algorithm erases data by overwriting an entire hard drive with randomly generated numbers in a single pass.
Pseudo-random & Zeroes (2 passes)	This algorithm erases data by overwriting the hard drive in two passes. In first pass, it overwrites data with randomly generated numbers and in second pass it overwrites the previously generated data with zeros.
Random Random Zero (6 passes)	This algorithm erases data by overwriting a storage media with random characters in multiple passes.
US Department of Defense, DoD 5220.22-M (3 passes)	This algorithm erases data by overwriting the hard drive in three passes. In first pass, it overwrites data with zeros, then in second pass, it overwrites the data with ones and finally in the third pass overwrites the data with randomly generated bytes. This is a U.S. Department of Defense algorithm.
US Department of Defense, DoD 5220.22-M (ECE) (7 passes)	This algorithm erases data by overwriting the hard drive in seven passes. The first, fourth and fifth pass is overwriting with a random byte, its 8 right-bit shift complement and 16 right-bit shift complement; second and sixth passes are overwriting with zeros, and third and seventh pass with random data. This is a U.S. Department of Defense algorithm.
US Department of Defense, DoD 5200.28-STD (7 passes)	This algorithm erases data by overwriting the hard drive in seven passes. In first two passes, it overwrites data with certain bytes and their complements, then in next two passes it overwrites data with random characters. In fifth and sixth passes, it overwrites data with a character and its complements and finally, it overwrites data with random characters. This is a U.S. Department of Defense algorithm.
Russian Standard - GOST-R-50739-95(2 passes)	This algorithm erases data by overwriting the hard disk with zeros followed by a single pass of random characters.
B.Schneier's algorithm (7 passes)	This algorithm erases data in seven passes. In the first two passes, it overwrites the hard disk with ones and then zeros and in next five passes, it overwrites data with random characters.
German Standard, VSITR (7 passes)	This algorithm erases data by overwriting data with three alternating patterns of zeros and ones and then a last pass which overwrites with random characters.
Peter Gutmann, (35 passes)	This algorithm erases data by overwriting it 35 times, making recovery of the erased data by any tool impossible. This algorithm takes more time than other wiping algorithms.
US Army AR 380-19 (3 passes)	This algorithm erases data by overwriting the media in three passes. In the first pass, it overwrites data with random bytes, then in second and third pass, it overwrites data with certain bytes and their complements. This is a U.S. Army algorithm.



North Atlantic Treaty Organization-NATO Standard (7 passes)	This algorithm erases data by overwriting the media in seven passes. From pass one to six, it overwrites the data with a number and its complement alternatively. Then, in the final pass, it overwrites data with random characters.
US Air Force, AFSSI 5020 (3 passes)	This algorithm erases the data by overwriting the media in three passes. First, it overwrites with zeros, then with ones and finally with random characters.
Pfitzner algorithm (33 passes)	The Pfitzner algorithm is used in file shredding and data destruction programs to overwrite existing information on a hard drive or other storage devices. All the passes in Pfitzner method consist entirely of random overwriting of data in the storage device.
Canadian RCMP TSSIT OPS-II (4 passes)	This algorithm is four pass overwriting algorithm with alternating patterns of zeros and ones and the last pass - with a random byte.
British HMG IS5 Baseline Standard	One Pass-Random Pattern.
British HMG IS5 Enhanced Standard (3 passes)	This algorithm is a three pass overwriting algorithm: first pass with zeros, second pass with ones and the last pass with random data.
NAVSO P-5239-26 (3 passes)	This algorithm is a three pass overwriting algorithm: Pass 1: Writes a specified character (e.g. one) Pass 2: Writes the complement of the specified character (e.g. zero) Pass 3: Writes a random character and verifies the write.
NCSC-TG-025 (3 passes)	This algorithm is a three pass overwriting algorithm: Pass 1: Writes a zero and verifies the write Pass 2: Writes a one and verifies the write Pass 3: Writes a random character and verifies the write
BitRaser Secure & SSD Erasure	SSDs differ from HDDs as in SSD data is stored electronically on transistor arrays, thus this algorithm for SSD ensures complete data erasure.
Firmware Based Disk Array Erasure	This algorithm uses internal commands (located in the device firmware). The erasure commands can differ depending on the drive interface (ATA, SCSI, SAS, SATA).
NIST 800- 88 Clear	This algorithm overwrites media by using organizationally approved and validated overwriting technologies/methods/tools.
NIST 800-88 Purge	Apply the ATA Secure Erase command. The sanitize command is preferred to Secure Erase when the sanitize command is supported by the device.
Custom Methods	This algorithm is added by the user. Users can create up to 5 <a href="#">custom erasure methods</a> .

**Note:** For the erasure of SSDs, it is recommended to use the "**BitRaser Secure & SSD Erasure**" erasure method. If any other method is selected while initiating an erasure process of an SSD, **BitRaser Drive Eraser** prompts the user to change the erasure method as follows:

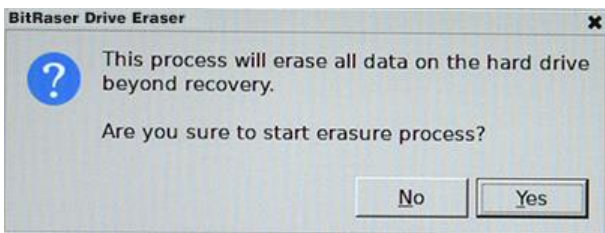


6. Next from **Advanced Option** section, select any one of the verification methods:

VERIFICATION METHODS	DESCRIPTION
No Verification	No verification is done after the media is erased.
Random Verification	Random verification of the storage device is done after the wiping operation, that is, randomly selected sectors of the storage device are verified after wiping operation.
Total Verification	Total verification verifies all the sectors of the storage device after the wiping operation is completed.

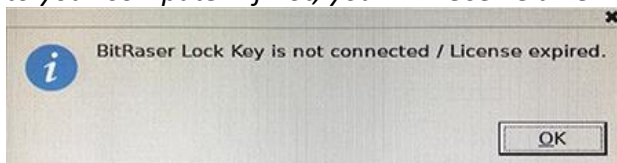
**Note:** Depending on the type of **Erasure Method** that you have selected, verification method may or may not be available.

7. Click **Erase** to initiate the erasure process, the following screen appears:



**Note:**

- For licenses on cloud, to initiate the erasure process the application must be connected to internet and **BitRaser Server**. If not, **BitRaser Drive Eraser** will open the settings dialog box when you click on **Erasure** button. Refer to [Connecting to Internet](#) and [Connecting to BitRaser Server](#) to know these settings.
- For licenses on BitRaser Lock Key, to initiate the erasure process **BitRaser Lock Key** must be connected to your computer. If not, you will receive an error message as follows:



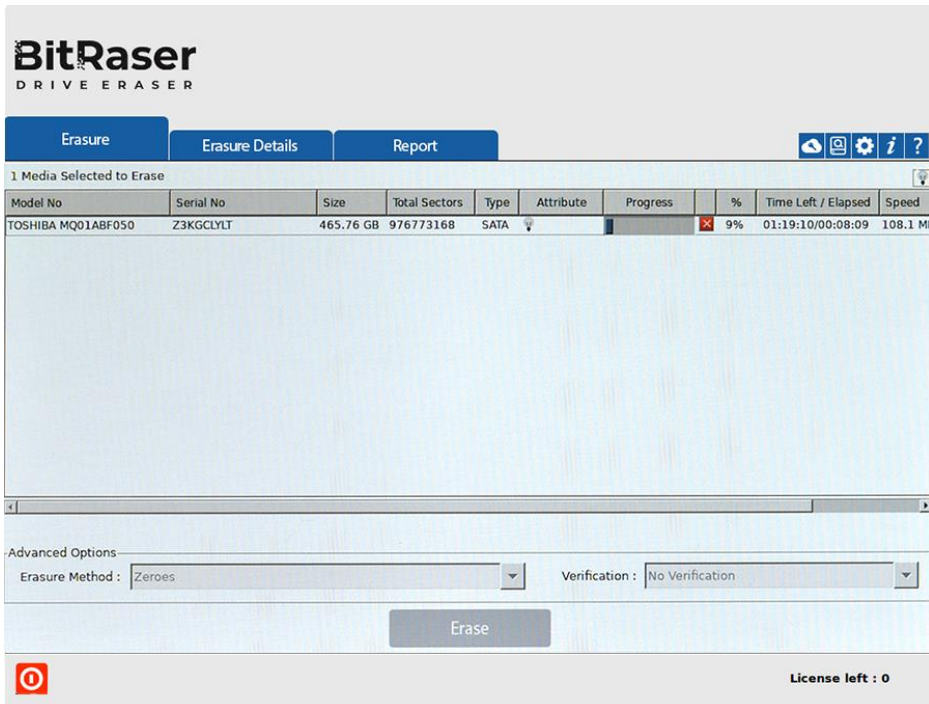
In that case, make sure the **BitRaser Lock Key** is connected and initiate the erasure process again.


**Caution:** **BitRaser Drive Eraser** erases the selected storage device beyond recovery. Back up the data which you want to preserve from your storage device before starting the erasure process.

8. Click **Yes** to start the erasure process or **No** to cancel the action.




**Note:** At this stage, **BitRaser Drive Eraser** accesses the license information and licenses are consumed depending upon the number of disks you have selected for erasure.

9. A progress bar as shown below appears, showing the progress of the erasure along with percentage of completion, time left/elapsed, speed and bad sectors found on disk during the process:



10. If you wish to cancel the erasure process, click on stop button  next to the progress bar.

**Note:** If you have **BitRaser Drive Eraser**'s licenses on cloud, the erasure report is automatically sent to **BitRaser Server** when the erasure process is completed or canceled:

- If the report is successfully sent to **BitRaser Server**, you will see  icon on the bottom right corner of the report under **Report Tab**.
- If **BitRaser Drive Eraser** is not connected to internet and the report is not sent to **BitRaser Server**, you will see  icon on the top right corner of **Report Tab** and  on the bottom right corner of the report. In that case, check your LAN cable connection and re-establish internet connection. Once the internet is connected, **BitRaser Drive Eraser** will automatically send the report to **BitRaser Server**.

**Note:** If you have **BitRaser Drive Eraser**'s licenses on lock key, you need to save the reports manually on a connected drive after the erasure process is completed or canceled.

## 3.2. CONFIGURING ERASURE DETAILS

---

The **Erasure Details** tab of **BitRaser Drive Eraser** allows you to configure the generic information related to the customer that you serve and the hard drive that you erase. The information entered in this section will be added to the **Erasure Reports** and can be modified later if required. The **Erasure Details** tab has the following three sub-sections:

1. **Erasure Details** allows you to enter information like customer details, media details, technician performing erasure and person validating erasure.
2. **Asset Details** shows the information of the erasure process carried out on the different hard disks like asset tag, model number, serial number, and size. You can either enter different asset tags for individual erased hard disks or enter a specific asset tag for all the erased hard disks.
3. **Custom Fields** allows you to enter up to 20 sets of customized fields that are added to the **Erasure Reports**.

## 3.2.1. ERASURE DETAILS

To enter the Erasure Details, use the following steps:

1. Run **BitRaser Drive Eraser**. Select the **Erasure Details** tab.
2. Select the radio button **Enter Erasure Details**.
3. In the **Erasure Details** screen, you can edit the following fields:

The screenshot shows the 'Enter Erasure Details' screen of the BitRaser Drive Eraser application. It features three radio buttons at the top: 'Enter Erasure Details' (selected), 'Enter Asset Details', and 'Enter Custom Fields'. Below these are four sections for data entry:

- Customer Details:** Fields for 'Customer Name' (John) and 'Customer Address' (norway).
- Media Details:** Fields for 'Media Source' (MS-0011) and 'Media Destination' (MD-0022).
- Technician Performing Erasure:** Fields for 'Technician Name' (David) and 'Organization' (SW).
- Person Validating Erasure:** Fields for 'Validator Name' (Smith) and 'Organization' (NZ).

At the bottom of the form are two buttons: 'Reset' and 'Save'.

- **Customer Details:** Enter the details associated with the customer like Customer Name and Customer Address.
  - **Media Details:** Enter the details associated with the media/machine like Media Source and Media Destination.
  - **Technician Performing Erasure:** Enter the details of the technician who has to perform the erasure process. It contains fields Technician Name and Organization.
  - **Person Validating Erasure:** Enter the details of the person who is validating the erasure process. It contains fields Validator Name and Organization.
4. Click **Reset** to reset the fields, if required, or click **Save** to save the information you have entered.

## 3.2.2. ASSET TAG DETAILS

To enter the Asset Tag Details, use the following steps:

1. Run **BitRaser Drive Eraser**. Select the **Erasure Details** tab.
2. Select the radio button **Enter Asset Details**.
3. Enter the Machine Asset tag in the provided field.

The screenshot shows the 'Enter Asset Details' dialog box in BitRaser Drive Eraser. At the top, there are three radio buttons: 'Enter Erasure Details', 'Enter Asset Details' (which is selected), and 'Enter Custom Fields'. Below the radio buttons, there is a text field labeled 'Enter Machine Asset Tag' containing the text 'MAC00199 Tag'. To the right of this field is a checkbox labeled 'Fill the same asset tag for all disks'. Below this is a section titled 'Enter Disk Asset Tag :'. It contains a table with four columns: 'Asset Tag', 'Model No', 'Serial No', and 'Size'. The table has one row of data: 'Hard drive 1 Toshiba', 'TOSHIBA MQ01ABF050', 'XSE3SMECS', and '465.76 GB'. Below the table is a large empty text area. At the bottom of the dialog box are two buttons: 'Reset' and 'Save'.

Asset Tag	Model No	Serial No	Size
Hard drive 1 Toshiba	TOSHIBA MQ01ABF050	XSE3SMECS	465.76 GB

4. Select the checkbox '**Fill the same asset tag for all disks**' if you want to provide the same asset tag to all the erased disks.
5. You can see the information such as Asset Tag, Model No, Serial No, and Size.
6. To enter a different asset tag to a disk, click on its particular field.
7. Click **Reset** to reset the fields, if required, or click **Save** to save the information you have entered.

## 3.2.3. CUSTOM FIELDS

To enter the Custom Fields, use the following steps:

1. Run **BitRaser Drive Eraser**. Select the **Erasure Details** tab.
2. Select the radio button **Enter Custom Fields**.
3. You can create up to 20 sets of custom fields. The following two fields are available for each set:
  - Enter Custom Field Name: Enter the name of the custom field.
  - Enter Custom Field Value: Enter the value of the custom field.

Custom Fields Set 1		Custom Fields Set 2	
Enter Custom Field Name	Enter Custom Field Value	Enter Custom Field Name	Enter Custom Field Value
1. First Name	Jacob	11.	
2. Last Name	D'souza	12.	
3. User ID	jacob@bitraser.com	13.	
4. Enter Password	*****	14.	
5. Confirm Password	*****	15.	
6. Mobile Phone	123456789	16.	
7. Address	55, Mark Lane	17.	
8. Country	California	18.	
9.		19.	
10.		20.	

Reset Save

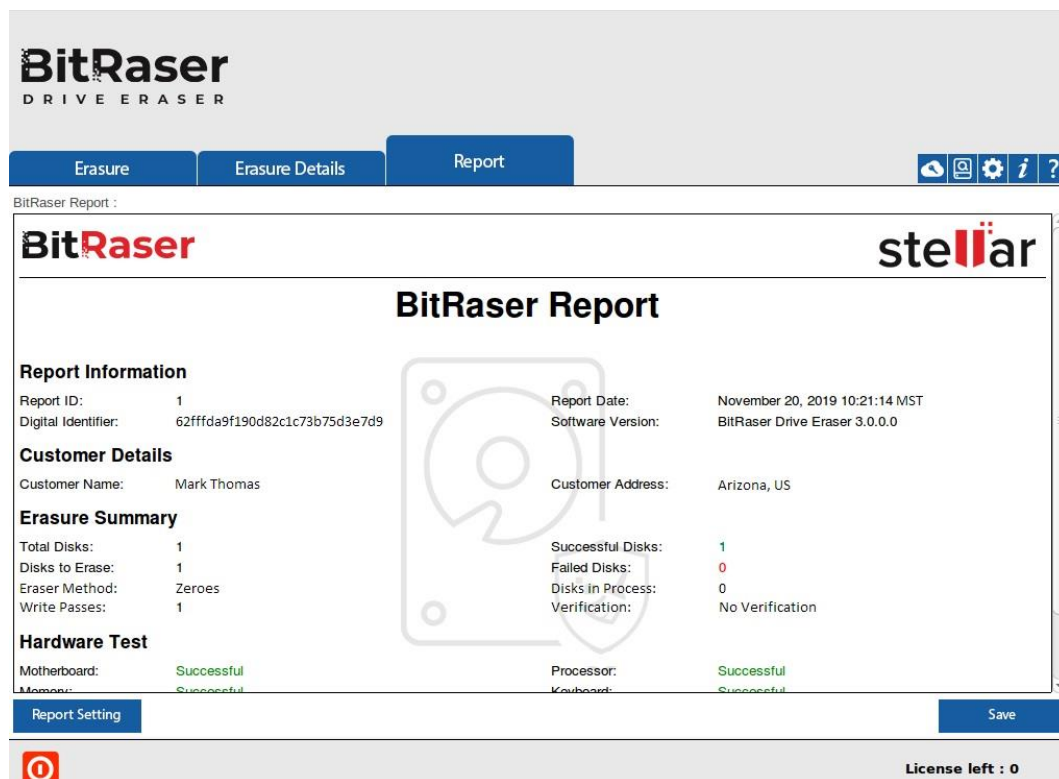
4. Click **Reset** to reset the fields, if required, or click **Save** to save the information you have entered.



## 3.3. WORKING ON REPORT AND CERTIFICATE

### BitRaser Drive Eraser Report:

**BitRaser Drive Eraser** provides you with a detailed report which contains Report Information, Customer Details, Erasure Summary, Hardware Test, Hardware Information, Custom Fields, and Erasure Results. The details are given as follows:



The screenshot shows the BitRaser Drive Eraser Report interface. The report is titled "BitRaser Report" and is generated by stellar. It includes sections for Report Information, Customer Details, Erasure Summary, and Hardware Test.

Report Information	
Report ID:	1
Digital Identifier:	62ffda9f190d82c1c73b75d3e7d9
Report Date:	November 20, 2019 10:21:14 MST
Software Version:	BitRaser Drive Eraser 3.0.0.0

Customer Details	
Customer Name:	Mark Thomas
Customer Address:	Arizona, US

Erasure Summary	
Total Disks:	1
Disks to Erase:	1
Eraser Method:	Zeroes
Write Passes:	1
Successful Disks:	1
Failed Disks:	0
Disks in Process:	0
Verification:	No Verification

Hardware Test	
Motherboard:	Successful
Memory:	Successful
Processor:	Successful
Keyboard:	Successful

Report Setting Save

License left : 0

- **Report Information** contains details such as Report ID, Report Date, Digital Identifier and Software Version.
- **Customer Details** contains details such as Customer Name and Address.
- **Erasure Summary** contains number of disks, disks to erase, disks to process, number of successful or failed erasure of disks.
- **Hardware Test** contains details of tests performed on various hardware devices of the system such as motherboard, memory, processor, and so on.
- **Hardware Information** lists out the hardware details of the computer such as manufacturer details, detailed system information, Disk information, Processor details, Network Adapter details, BIOS, Battery and so on.
- **Custom Fields** contains the customized information that you have defined using [Custom Fields](#) option of **BitRaser Drive Eraser**.
- **Erasure Results** contains disk wise details of the erasure performed such as erasure method, number of sectors processed, asset tag, start and end time of process along with duration and status.

For information about viewing and customizing a report, see [View and Customize Report](#).

For information about saving a report in PDF, CSV or XML format, see [Save Report](#).



For information about sending a report to **BitRaser Server** or exporting a report to media in RPT format, see [Export Report](#) (Applicable only if you have licenses on cloud).

## BitRaser Drive Eraser Certificate:

**BitRaser Drive Eraser** also provides you with a certificate of the erasure process performed. This certificate contains all the erasure details along with the signature and details of technician and validator performing the erasure process.

For information about generating and saving the certificate, see [Generate and Save Certificate](#).

### 3.3.1. VIEW AND CUSTOMIZE REPORT

To view and customize BitRaser Drive Eraser report:

1. Run **BitRaser Drive Eraser** and select **Report** tab, the current report appears as shown below:

The screenshot shows the BitRaser Drive Eraser application interface. At the top, there's a header with the BitRaser logo and 'DRIVE ERASER' text. Below the header, there are three tabs: 'Erasure', 'Erasure Details', and 'Report'. The 'Report' tab is selected. The main content area displays the 'BitRaser Report' with the following sections:

- Report Information**
  - Report ID: 1
  - Digital Identifier: 62ffda9f190d82c1c73b75d3e7d9
  - Report Date: November 20, 2019 10:21:14 MST
  - Software Version: BitRaser Drive Eraser 3.0.0.0
- Customer Details**
  - Customer Name: Mark Thomas
  - Customer Address: Arizona, US
- Erasure Summary**
  - Total Disks: 1
  - Disks to Erase: 1
  - Eraser Method: Zeroes
  - Write Passes: 1
  - Successful Disks: 1
  - Failed Disks: 0
  - Disks In Process: 0
  - Verification: No Verification
- Hardware Test**
  - Motherboard: Successful
  - Processor: Successful
  - Memory: Successful
  - Keyboard: Successful

At the bottom of the report window, there are buttons for 'Report Setting' and 'Save'. A license status bar at the very bottom indicates 'License left : 0'.

2. In case you want to customize the report, select **Report Settings** button located at the bottom left of the screen.

The screenshot shows the 'BitRaser Drive Eraser' application window with the 'Settings' dialog box open. The dialog box has two main sections:

- Settings**
  - Enter Report Header Text: BitRaser Report
- Image Settings**
  - ☒ Select top right logo (170 x 48 PNG) with a file path: /home/BitRaserConfig/Images/right-logo.png and a 'Browse...' button.
  - ☒ Select watermark (250 x 300 PNG) with a file path: /home/BitRaserConfig/Images/BitRaser.png and a 'Browse...' button.
  - ☒ Select erasure person signature (170 x 48 PNG) with a file path: /home/BitRaserConfig/Images/erasurer-sign.png and a 'Browse...' button.
  - ☒ Select validation person signature (170 x 48 PNG) with a file path: /home/BitRaserConfig/Images/validator-sign.png and a 'Browse...' button.

At the bottom of the dialog box, there are buttons for 'Reset', 'OK', and 'Close'.

3. In **Report Settings** dialog box, you can edit the following fields:

FIELD NAME	DESCRIPTION
Enter report header text	Enter header text that appears on the header of the report (must be maximum of 30 characters)
Select top right Logo	Select the check-box and click <b>Browse</b> to select the top-right logo of the report (image size and format - 170 x 48 PNG)
Select watermark	Select the check-box and click <b>Browse</b> to select the watermark (image size and format - 250 x 300 PNG)
Select erasure person signature	Select the check-box and click <b>Browse</b> to select the erasure person signature (image size and format - 170 x 48 PNG)
Select validation person signature	Select the check-box and click <b>Browse</b> to select the validation person signature (image size and format - 170 x 48 PNG)

**Note:** You can reset report settings fields using the **Reset** button located at the bottom left of the **Report Settings** dialog box.

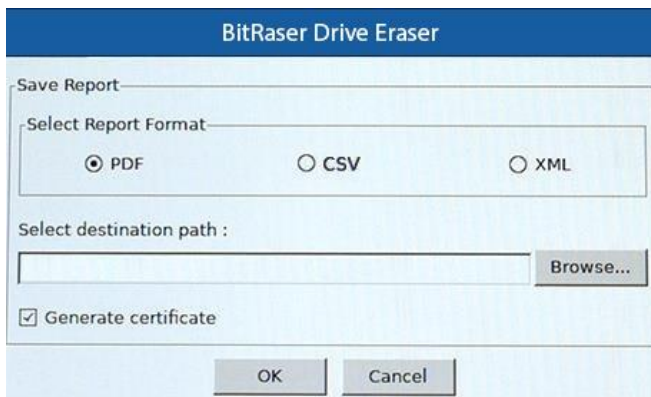
**Note:** Top right logo, watermark, erasure person signature and validation person signature image size needs to be the same as specified in **Report Settings**. Top left logo and footer image and text are set by default. **BitRaser Drive Eraser** will accept images with specified size and format only. In case of size mismatch, BitRaser Drive Eraser will continue to use the previously selected images.

4. After making the required changes to **Report Settings**, click **OK** to save.

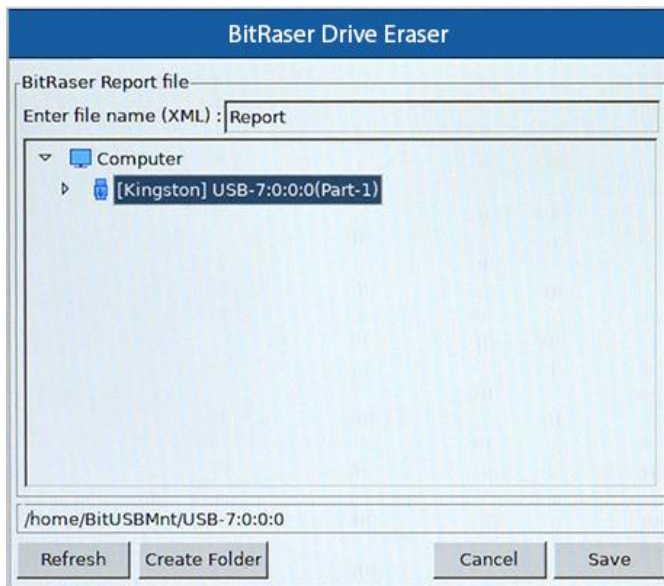
## 3.3.2. SAVE REPORT

To save a BitRaser Drive Eraser report:

1. Run **BitRaser Drive Eraser**. Select **Report** tab.
2. Click on **Save** button located at the bottom right of the screen, following dialog box appears:



3. From the dialog box, select the format in which you want to save the report, that is, either **PDF**, **CSV** or **XML** format.
4. Click **Browse**. The following screen appears:



5. Enter the file name for the file in the field provided and select the destination folder where you want the file to be saved.

**Note:** Use **Refresh** button to refresh the list of media connected to the computer and **Create Folder** to create a new folder at the destination you selected.

6. Click **Save** to continue.

7. If you also wish to generate and save the certificate in the same path, select the check-box **Generate certificate**.

8. Click **OK** and the report will be saved.

**Note:** If you have **BitRaser Drive Eraser**'s licenses on cloud, the report is sent to **BitRaser Server** once the erasure process is completed. Make sure your internet connection is active.

### 3.3.3. EXPORT REPORT

---

To export a BitRaser Drive Eraser report:

1. Run **BitRaser Drive Eraser**. Select **Report** tab.
2. Click on **Export** button located at the bottom right of the screen.
3. Select the destination to export the report, the following options are available:
  - **Send to server** (*Applicable only if you have licenses on cloud*): This option allows you to send the report to **BitRaser Server**. To do this, select **Send to server** button and click **Send**.

**Note:** Reports can be sent to **BitRaser Server** only after completion of erasure process.

**Note:** Once the erasure process is completed, the erasure report is automatically sent to **BitRaser Server**.



icon on the bottom right corner of the report under **Report Tab** indicates that the report has been successfully sent to **BitRaser Server**.

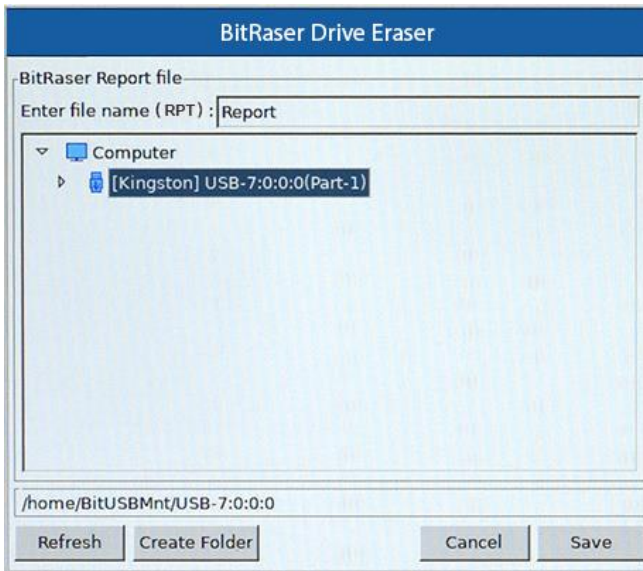
- **“Export to media” or “Export to media (Cloud)”**: This option allows to export the report to media device in RPT format. To do this:

1. Select **Export to media** button, **Select path to export report** option appears.

**Note:** For the **BitRaser Drive Eraser's** edition with licenses on a **lock key (USB)**, if you want to transfer the report to **BitRaser Cloud Console**, select **Export to media (Cloud)** option.



2. Click **Browse**.



3. Enter the file name for the RPT file in the field provided and select the destination folder where you want the file to be saved.

**Note:** Use **Refresh** button to refresh the list of media connected to the computer and **Create Folder** to create a new folder at the destination you selected.

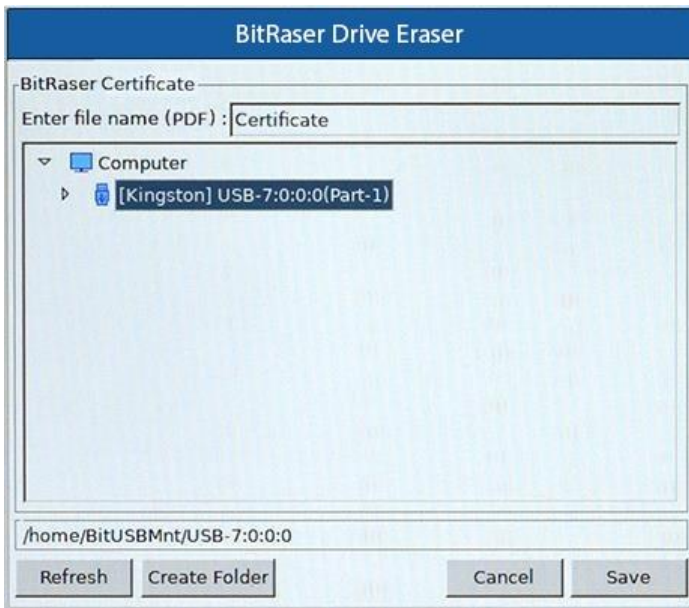
4. Click **Save** to continue.
5. On the **Select destination** dialog box, click **Export** to save the report at the selected destination.

### 3.3.4. GENERATE AND SAVE CERTIFICATE

---

This option allows to generate and save the erasure certificate to a media device in PDF format. To do this:

1. Run **BitRaser Drive Eraser**. Select **Report** tab.
2. Click on **Generate Certificate** button located at the bottom right of the screen, following dialog box appears:



3. Enter the file name for the PDF file in the field provided and select the destination folder where you want the certificate to be saved.

**Note:** Use **Refresh** button to refresh the list of media connected to the computer and **Create Folder** to create a new folder at the destination you selected.

4. Click **Save** to continue.


**Note:** It is advisable to verify the saved certificate before closing the application.

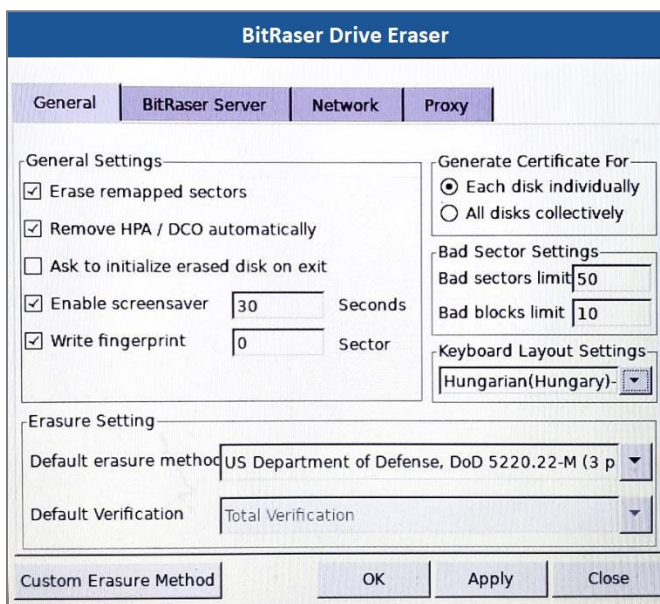


## 3.4. GENERAL SETTINGS

The **General** settings allow to update various application general settings, change bad sector limit, keyboard layout, select default erasure method and verification etc. It also allows you to create custom erasure methods.

To change **BitRaser Drive Eraser** General settings:

1. Click on the **Settings**  icon on the top right corner of the screen, the settings window appears. This window has the following tabs:
  - [General settings](#)
  - [BitRaser Server settings \(Applicable only if you have licenses on cloud\)](#)
  - [Network settings \(Applicable only if you have licenses on cloud\)](#)
  - [Proxy settings \(Applicable only if you have licenses on cloud\)](#)
2. Click on **General** tab, if not selected by default.



3. In the **General** tab menu, you can edit the following fields:

- **General Settings:**

This option allows you to change various general and default settings associated with **BitRaser Drive Eraser** software. The following fields can be edited from this section:

- **Erase Remapped Sectors:** Checking this field erases the remapped sectors of the hard drives if any.
- **Remove HPA/DCO automatically:** Checking this field removes HPA/DCO area of memory on a hard drive.

- **Ask to initialize erased disk on exit:** Checking this field prompts a dialog box, which asks whether to initialize the erased disk before quitting the application once the erasure process is complete.
- **Enable screensaver:** This field enables a screensaver showing you the process status such as erasure completed, failed or in-progress. You can set the period between 10 to 240 seconds, after which you want the screensaver to appear while the application is running.
- **Write fingerprint:** This field enables you to write a fingerprint at a drive sector after erasure. This fingerprint acts as a unique identifier, to verify at a later stage that the drive has been erased using **BitRaser Drive Eraser** application. You can define the sector number on the drive, in the text box provided, where you want to add the fingerprint.

- **Generate Certificate For:**

This option allows you to generate certificate for a single disk or all the disks collectively. It contains the following two fields:

- **Each disk individually:** Checking this field will generate a separate certificate for each disk individually.
- **All disks collectively:** Checking this field will generate a single certificate for all the disks collectively.

- **Bad Sector Settings**

This option allows you to change the limit of bad sectors and blocks after which your wiping process would automatically stop.

- **Bad Sectors Limit:** Enter the number of bad sectors on which you want to stop the wiping process.
- **Bad Blocks Limit:** Enter the number of bad blocks on which you want to stop the wiping process.

- **Keyboard Layout Settings**

This option allows you to change your keyboard's language without changing the language that **BitRaser Drive Eraser** is using on the screen. Changing the **Keyboard Layout** settings helps you access accent marks and other specialized characters, or for typing on a keyboard with a different language layout.

The following **Keyboard Layouts** are available with **BitRaser Drive Eraser**:

- Belgian (Belgium) - be

- Danish (Denmark) - dk
- Dutch (Netherlands) - nl
- English (United Kingdom) - gb
- English (United States) - us
- Finnish (Finland) - fi
- French (France) - fr
- French (Canada) - ca
- French (Switzerland) - ch\_fr
- German (Germany) - de
- German (Switzerland) - ch
- Hungarian (Hungary) - hu
- Italian (Italy) - it
- Norwegian (Norway) - no
- Polish (Poland) - pl
- Portuguese (Portugal) - pt
- Portuguese (Brazil) - br
- Spanish (Spain) - es
- Spanish Latam (Latin American) - latam
- Slovak (Slovakia) - sk
- Swedish (Sweden) - se

- **Erase Settings**

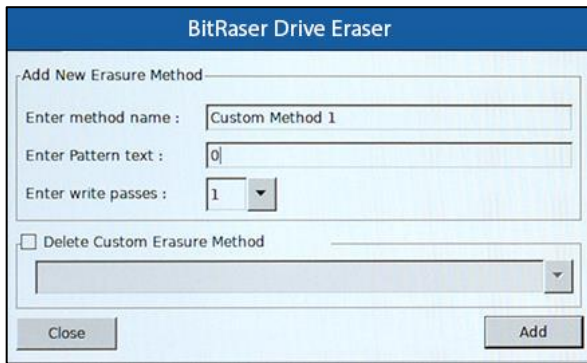
This option allows you to edit the default erasure settings:

- **Default erasure method:** Select an erasure method from the drop-down list. The selected method will act as a default erasure method.
- **Default Verification:** Select a verification method from the drop-down list, which will act as a default verification method to verify.

## Custom Erasure Method:

This option allows you to create your own erasure method. To create your own erasure method, use the following steps:

1. Click on the **Custom Erasure Method** in the general settings menu.
2. A dialog box is displayed as shown below.

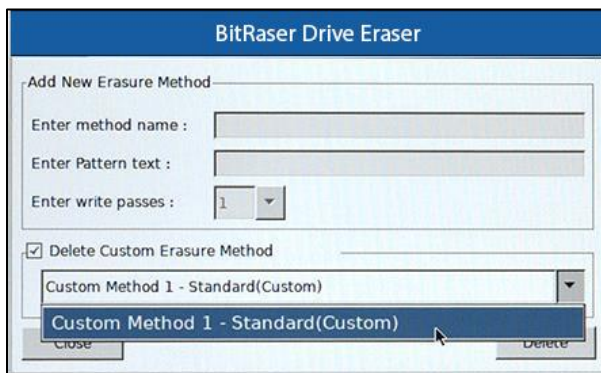


The screenshot shows the 'BitRaser Drive Eraser' dialog box with the 'Add New Erasure Method' section active. It contains three input fields: 'Enter method name' with the text 'Custom Method 1', 'Enter Pattern text' with the text '0', and 'Enter write passes' with a dropdown menu set to '1'. Below these fields is a checkbox labeled 'Delete Custom Erasure Method' which is currently unchecked. Under the checkbox is a dropdown menu. At the bottom of the dialog are 'Close' and 'Add' buttons.

3. In 'Enter method name' field, type the name you want to give to your erasure method.
4. In 'Enter Pattern text' field, type the pattern or data you want to overwrite on the disk during the wiping process.
5. In 'Enter write passes' field, select the number of passes from one to nine, in which you want your erasure to be completed.
6. Click on **Add**.

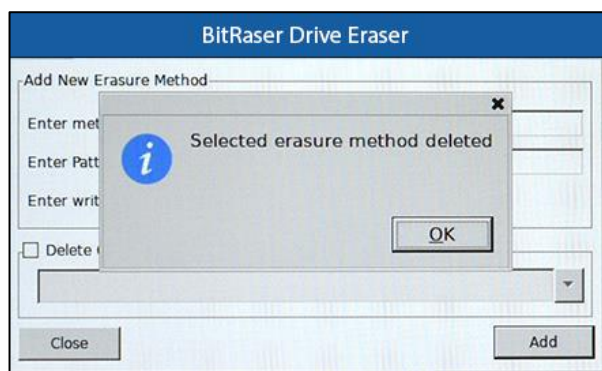
You can also delete the custom erasure method, which you added. To do this:

1. Select the check-box **Delete Custom Erasure Method** and select the custom erasure method that you want to delete from the drop down menu.



This screenshot shows the same 'BitRaser Drive Eraser' dialog box, but now the 'Delete Custom Erasure Method' checkbox is checked. The dropdown menu below it is open, showing a list with the entry 'Custom Method 1 - Standard(Custom)' selected. The 'Close' and 'Delete' buttons are visible at the bottom.

2. Click **Delete** to remove the selected custom erasure method.



**Note:** You can only add up to 5 custom erasure methods. The created custom erasure method is displayed in the list of **Erasure Method** in **Advanced Options** in **Erasure** tab.


## 3.5. WORKING WITH THE LICENSE MANAGER

*This topic is only applicable if you have BitRaser Drive Eraser's licenses on cloud.*

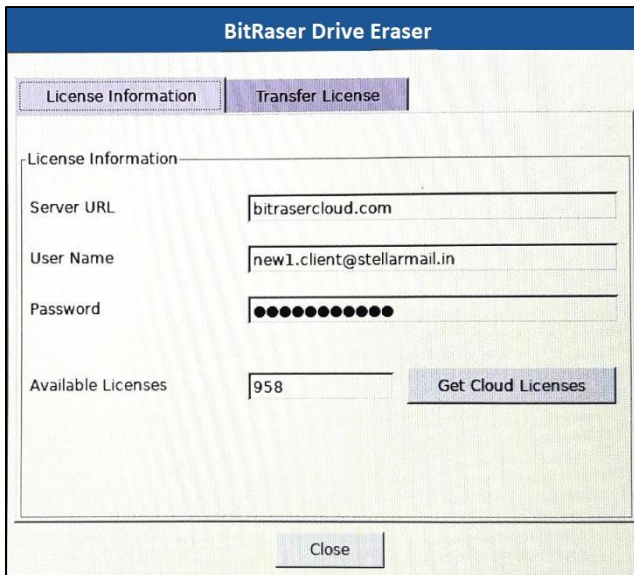
The **License Manager** is a tool that allows to view the license information on **BitRaser Cloud** and to transfer licenses from **BitRaser Cloud** to **BitRaser Lock Key**.

**Note:** Make sure your internet connection is active to fetch the license information from **BitRaser Cloud**.

To view the license information using the License Manager:

1. Click on the **License Manager**  icon on the top right corner of the screen, the license manager window appears. This window has the following tabs:

- License Information
- Transfer License



2. By default, the **License Information** tab is selected. If you have already logged into **BitRaser Server**, the license information is fetched automatically and displayed in the **Available Licenses** field. If you have not logged into **BitRaser Server** before, do the following steps:
  - a) Enter the **Server URL** and your **BitRaser Cloud** credentials – **User Name** and **Password**.
  - b) Click **Get Cloud Licenses**. The license information is fetched from **BitRaser Cloud** and displayed in the **Available Licenses** field.
3. Click **Close** to go back to the home screen.

## To transfer licenses from BitRaser Cloud to BitRaser Lock Key using License Manager:

**Note:** Before using the transfer license tool, make sure you have logged into **BitRaser Cloud** and fetched **Available Licenses** using the steps given above.

1. Click on the **License Manager** icon on the top right corner of the screen, the license manager window appears. This window has the following tabs:
  - License Information
  - Transfer License

The screenshot shows the 'BitRaser Drive Eraser' window with the 'License Information' tab selected. It contains fields for 'Server URL' (bitrasercloud.com), 'User Name' (new1.client@stellarmail.in), and 'Password' (masked with dots). Below these is a field for 'Available Licenses' showing '958' and a 'Get Cloud Licenses' button. A 'Close' button is at the bottom.

2. Click on the **Transfer License** tab.

The screenshot shows the 'BitRaser Drive Eraser' window with the 'Transfer License' tab selected. It features a 'Get Lock Information' button and a table with lock status and counts. Below is a section to 'Enter licenses to transfer from BitRaser cloud to BitRaser lock' with a 'License count' field set to '1' and a 'Transfer Licenses to Lock' button. At the bottom is a 'License Count Status' section with four fields: 'Current cloud count' (958), 'Count transferred' (0), 'Previous lock count' (0), and 'Current lock count' (0). A 'Close' button is at the bottom.

Get Lock Information	Lock status:	Active	Count used:	29
	Customer name:	Test	Count left:	88

3. Connect the **BitRaser Lock Key** to the USB port of your computer and click **Get Lock Information**. The lock information is displayed.

4. Enter the **License Count** under **Enter licenses to transfer from BitRaser cloud to BitRaser lock** section.  
***Note:** The **License Count** to transfer cannot be more than the **Available Licenses** in **BitRaser Cloud**.*
5. Click **Transfer licenses to lock**. This deducts the licenses from **BitRaser Cloud** and adds the licenses to **BitRaser Lock Key**.
6. Check the transfer information under the **License Count Status** section.
7. Click **Close** to go back to the home screen.




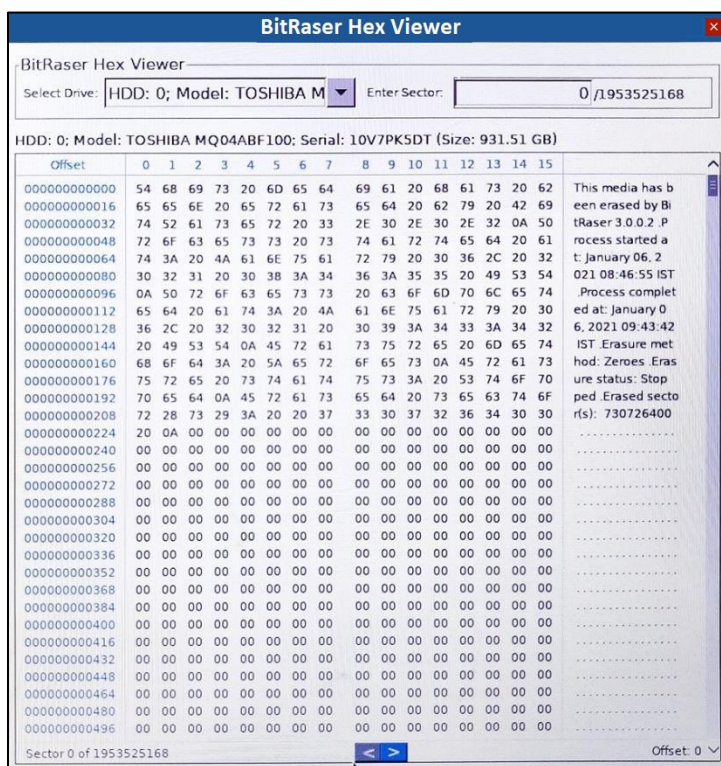
## 3.6. USING THE HEX VIEWER




The **Hex Viewer** of **BitRaser Drive Eraser** allows you to view the raw and exact content of the hard drive in **hexadecimal** format. Thus, helping you to confirm the erasure of your hard drive by viewing its contents after completing the erasure process.

The **Hex Viewer** of **BitRaser Drive Eraser** can be used to view the content of a hard drive before and after the erasure process. However, the viewer is not available while erasure is in progress.

To use the **Hex Viewer**:

1. Click on the **Hex Viewer**  icon on the top right corner of the screen. **BitRaser Hex Viewer** window appears.



2. Select the hard drive from the **Select Drive** drop-down list.
3. The raw content of the hard drive is fetched and displayed in a tabular format. Use the  (Previous) and  (Next) buttons located at the bottom or use your mouse scroll wheel to browse different pages.
4. If you want to view the content of a particular sector, type the sector number in **Enter Sector** field and press **Enter**.
5. Click  to close the window.

## 4. FREQUENTLY ASKED QUESTIONS (FAQ)

---

### 1. What is Data Erasure?

Data erasure is the process of permanently erasing data from a storage media device like a hard disk, USB drive and SD card. In its simplest form, a data-wiping algorithm overwrites with zeros, but more advanced algorithms use a combination of filling up a disk with random information plus multiple passes to ensure impossibility of retrieval from an erased disk.

### 2. What is BitRaser Drive Eraser and what are its main features?

**BitRaser Drive Eraser** is a portable application for permanent data erasure from a storage device. Using it, you can erase all data and prevent recovery of erased data.

Some of its main features are:

- Option to boot from either a USB dongle or CD/DVD.
- Supports up to 32 hard drives for simultaneous erasure.
- Supports erasure of IDE, SATA, SCSI hard drives SSD, SD Card and USB drive.
- Software allows you to customize reports and erasure certificates with an option to save reports in **PDF, CSV** and **XML** format.
- Equipped with 24 world-class wiping algorithms with three options of erasure verification (No verification, Random verification and Total verification).

### 3. What is the difference between having licenses on BitRaser Lock Key and having licenses on cloud?

**BitRaser Drive Eraser** needs access to license data for the erasure process. This license information is stored either on a USB device called as **BitRaser Lock Key** or on cloud with **BitRaser Server**. Both options are available for the users at the time of purchase. The major differences are listed as follows:

Licenses on Cloud	Licenses on BitRaser Lock Key
1. Stores license information on <b>BitRaser Server</b> .	1. Stores license information on a USB device.
2. Needs connection to internet and <b>BitRaser Server</b> while running the application.	2. Needs the USB device to be connected physically and internet connection is not required.
3. Automatically delivers reports and certificates to <b>BitRaser Cloud Console</b> .	3. Reports and certificates need to be saved on a USB device.
4. Cloud integration for user management.	4. User management option is not available.

### 4. Can I transfer the licenses from BitRaser Cloud Console to BitRaser Lock Key?

Yes, you can transfer the licenses from **BitRaser Cloud Console** to **BitRaser Lock Key**. To know how to transfer the licenses, see [Working with the License Manager](#).

### 5. I want to erase multiple drives at a time, is it possible to do so using BitRaser Drive Eraser?

Yes, of course, you can erase multiple drives at the same time. **BitRaser Drive Eraser** supports erasure of a maximum of 32 hard drives simultaneously.

#### **6. Can BitRaser Drive Eraser erase SSD drives?**

Yes, **BitRaser Drive Eraser** supports SSD drives erasure.

#### **7. What is a fingerprint in BitRaser Drive Eraser?**

The fingerprint acts as a unique identifier, to verify at a later stage that the drive has been erased using **BitRaser Drive Eraser** application. In [General Settings](#), you can define the sector number on the drive, where you want to add the fingerprint.

#### **8. What is a Hex Viewer and how is it helpful in BitRaser File Eraser?**

The **Hex Viewer** of **BitRaser Drive Eraser** allows you to view the raw and exact content of the hard drive in **hexadecimal** format. Thus, helping you to confirm the erasure of your hard drive by viewing its contents after completing the erasure process. For more information about **Hex Viewer**, see [Using the Hex Viewer](#) section.

#### **9. In how many formats, can I save my erasure report?**

**BitRaser Drive Eraser** allows you to save the erasure report in three formats. You can save your erasure report in PDF, CSV or XML format.

#### **10. Does BitRaser Drive Eraser support other languages?**

**BitRaser Drive Eraser** is currently available in **English** language only. However, the keyboard layout can be changed to your preferred language from the [General Settings](#).

#### **11. Is it possible to customize the erasure report?**

Yes, you can customize the erasure reports of **BitRaser Drive Eraser** as per your requirement. To add details such as customer information, erasure and validator person details, etc., and to add custom fields, refer to [Configure Erasure Details](#). To modify report settings such as logos, watermark and erasure and validator person signature, refer to [Report Settings](#).

## 5. LEGAL NOTICES

---

### Copyright

**BitRaser Drive Eraser** software, accompanied user manual and documentation are copyright of Stellar Information Technology Private Limited with all rights reserved. Under the copyright laws, this user manual cannot be reproduced in any form without the prior written permission of Stellar Information Technology Private Limited. No Patent Liability is assumed, however, with respect to the use of the information contained herein.

**Copyright © Stellar Information Technology Private Limited. All rights reserved.**

### Disclaimer

The Information contained in this manual, including but not limited to any product specifications, is subject to change without notice.

**STELLAR INFORMATION TECHNOLOGY PRIVATE LIMITED PROVIDES NO WARRANTY WITH REGARD TO THIS MANUAL OR ANY OTHER INFORMATION CONTAINED HEREIN AND HEREBY EXPRESSLY DISCLAIMS ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE WITH REGARD TO ANY OF THE FOREGOING STELLAR INFORMATION TECHNOLOGY PRIVATE LIMITED ASSUMES NO LIABILITY FOR ANY DAMAGES INCURRED DIRECTLY OR INDIRECTLY FROM ANY TECHNICAL OR TYPOGRAPHICAL ERRORS OR OMISSIONS CONTAINED HEREIN OR FOR DISCREPANCIES BETWEEN THE PRODUCT AND THE MANUAL. IN NO EVENT SHALL STELLAR INFORMATION TECHNOLOGY PRIVATE LIMITED, BE LIABLE FOR ANY INCIDENTAL, CONSEQUENTIAL SPECIAL, OR EXEMPLARY DAMAGES, WHETHER BASED ON TORT, CONTRACT OR OTHERWISE, ARISING OUT OF OR IN CONNECTION WITH THIS MANUAL OR ANY OTHER INFORMATION CONTAINED HEREIN OR THE USE THEREOF.**

### Trademarks

**BitRaser Drive Eraser®** is a registered trademark of Stellar Information Technology Private Limited.

All Trademarks Acknowledged.

All other brands and product names are trademarks or registered trademarks of their respective companies.

### License Agreement - BitRaser Drive Eraser

#### BitRaser Drive Eraser

Copyright © Stellar Information Technology Private Limited. INDIA

[www.stellarinfo.com](http://www.stellarinfo.com)

All rights reserved.

All product names mentioned herein are the trademarks of their respective owners.

This license applies to the standard-licensed version of **BitRaser Drive Eraser**.

## Your Agreement to this License

You should carefully read the following terms and conditions before using, installing or distributing this software, unless you have a different license agreement signed by Stellar Information Technology Private Limited.

If you do not agree to all of the terms and conditions of this License then do not copy, install, distribute or use any copy of **BitRaser Drive Eraser** with which this License is included, you may return the complete package unused without requesting an activation key within 30 days after purchase for a full refund of your payment.

The terms and conditions of this License describe the permitted use and users of each Licensed Copy of **BitRaser Drive Eraser**. For purposes of this License, if you have a valid single-user license, you have the right to use a single Licensed Copy of **BitRaser Drive Eraser**. If you or your organization has a valid multi-user license, then you or your organization has the right to use up to a number of Licensed Copies of **BitRaser Drive Eraser** equal to the number of copies indicated in the documents issued by Stellar when granting the license.

## Scope of License

Each Licensed Copy of **BitRaser Drive Eraser** may either be used by a single person or used non-simultaneously by multiple people who use the software personally installed on a single workstation. This is not a concurrent use license.

All rights of any kind in **BitRaser Drive Eraser**, which are not expressly granted in this license, are entirely and exclusively reserved to and by Stellar Information Technology Private Limited. You shall not rent, lease, modify, translate, reverse engineer, decompile, disassemble or create derivative works based on **BitRaser Drive Eraser** nor permit anyone else to do so. You shall not make access to **BitRaser Drive Eraser** available to others in connection with a service bureau, application service provider or similar business nor permit anyone else to do so.

## Warranty Disclaimers and Liability Limitations

**BitRaser Drive Eraser** and all accompanying software, files, data and materials are distributed and provided AS IS and with no warranties of any kind, whether expressed or implied. You acknowledge that good data processing procedure dictates that any program including **BitRaser Drive Eraser** must be thoroughly tested with non-critical data before there is any reliance on it and you hereby assume the entire risk of all use of the copies of **BitRaser Drive Eraser** covered by this License. This disclaimer of warranty constitutes an essential part of this License. In addition, in no event does Stellar authorize you or anyone else to use **BitRaser Drive Eraser** in applications or systems where its failure to perform can reasonably be expected to result in a significant physical injury or in loss of life. Any such use is entirely at your own risk and you would not hold Stellar responsible for any and all claims or losses relating to such unauthorized use.

In no event shall Stellar Information Technology Private Limited or its suppliers be liable for any special, incidental, indirect, or consequential damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use the software product or the provision of or failure to provide support services, even if Stellar Information Technology Private Limited has been advised of the possibility of such damages. In

any case, Stellar Information Technology Private Limited's entire liability under any provision shall be limited to the amount actually paid by you for the software product.

## **General**

This License is the complete statement of the agreement between the parties on the subject matter and merges and supersedes all other or prior understandings, purchase orders, agreements and arrangements. This License shall be governed by the laws of the State of Delhi, India. Exclusive jurisdiction and venue for all matters relating to this License shall be in courts and fora located in the State of Delhi, India and you consent to such jurisdiction and venue. There are no third party beneficiaries of any promises, obligations or representations made by Stellar herein. Any waiver by Stellar of any violation of this License by you shall not constitute nor contribute to a waiver by Stellar of any other or future violation of the same provision or any other provision of this License.

**Copyright © Stellar Information Technology Private Limited. All rights reserved.**

## 6. ABOUT STELLAR

---

**Stellar** is the world's foremost Data Care Corporation, with expertise in Data Recovery, Data Erasure, Mailbox Conversion, and File Repair software and services. Stellar has been in existence from past 25+ years and is a customer-centric, critically acclaimed, global data recovery, data migration & erasure solutions provider with cost-effective solutions available for large corporate, SMEs & Home Users.

**Stellar** is an ISO 9001 and ISO 27001 certified organization and has a strong presence across USA, Europe & Asia.

*For more information about us, please visit [www.stellarinfo.com](http://www.stellarinfo.com).*