BitRaser Drive Eraser

User Guide for version 3.0

Table of Contents

1. GENERAL INFORMATION

1.1. ABOUT BITRASER DRIVE ERASER

What is BitRaser Drive Eraser?

BitRaser Drive Eraser is a portable and highly reliable application that provides permanent data erasure for storage devices. This application erases data in order to prevent the recovery of sensitive data that is no longer required. Many refurbishers, organizations, and users, while formatting their hard drives, still found the possibility of data being recovered. BitRaser Drive Eraser solves this problem efficiently by using advanced algorithms that fill the storage device with useless binary data. This leaves no possibility for the data to be recovered and ensures that sensitive data does not fall into the wrong hands when storage devices are disposed of, recycled, or sold.

The software helps meet statutory and regulatory compliance needs with tamper-proof audit trails for data security and privacy – SOX, GLB, HIPAA, ISO27001, EU-GDPR, and PCI-DSS. The application allows the user to generate an erasure report containing the result of the process. The report can be saved to a hard drive/external media or collected by the **BitRaser Cloud Console**.

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

What is disk erasing and how it works?

Disk erasing is the process of permanently deleting the 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 ensures the impossibility of retrieving the 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 the erasure of hard drives like PATA, SATA, SED, SCSI, SAS, etc. SSDs (NVMe, ATA, SAS, etc.), USB drives, and SD cards. It also supports reading and writing 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 100 hard drives for simultaneous erasure.
- **Support for RAID**: Raid dismantling is supported for MegaRaid and Adaptec card.
- **Support to Erase Bad/Remapped 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 the marking of fingerprints 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 delivery to **BitRaser Cloud Console** (Applicable only if you have **BitRaser Drive Eraser's** licenses on BitRaser 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 BitRaser cloud):** Cloud integration for user management, licenses, and reports. Also, the software automatically saves all the reports and certificates on BitRaser Server.
- **Supports Encryption for Data Security (Applicable only if you have BitRaser Drive Eraser's licenses on BitRaser 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 either using a USB dongle or CD/DVD.
- **Multiple Options to Connect to Internet (Applicable only if you have BitRaser Drive Eraser's licenses on BitRaser cloud):** Option to connect to the internet either using 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 BitRaser cloud):** Supports the transfer 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. How to
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.

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*.

Acronyms used in this guide with their definitions:

ITEM	EXPLANATION
Bad Sectors/Bad Blocks	Bad sectors/bad blocks are the areas of the disk, that can't be used due to the permanent damage or Operating System (OS) is unable to access them.
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 (PDF) 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 in 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 (XML) 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

BitRaser Support

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

- You can either call us or go online to our support section
- Chat Live with an Online Technician
- Search in our extensive Knowledgebase
- Submit query from here
- E-mail BitRaser Support at: techsupport@stellarinfo.com

2. GETTING STARTED

This section covers the following topics:

2.1. SYSTEM REQUIREMENTS

Before you start the installation of **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 the computer from USB device, if you are using a USB to boot your computer

Note: *For the **BitRaser Drive Eraser** with BitRaser 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 for **BitRaser Lock key**.*

2.2. 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 BitRaser 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 so, copy the ISO file onto your drive and then burn the ISO onto a USB drive or DVD using any third-party software.

Now install **BitRaser Drive Eraser** onto your computer directly from your USB or DVD drive, following 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** following the steps given below:

Note: *The **BitRaser Drive Eraser** application boots and runs 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 until 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:

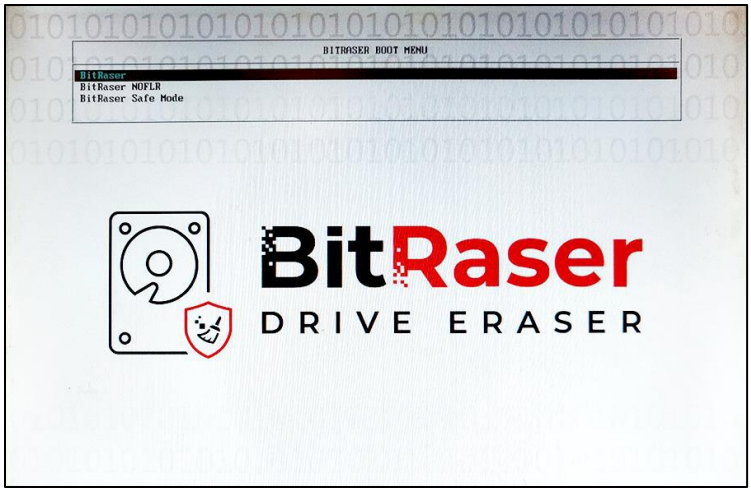
Verify that the **BitRaser Drive Eraser** bootable media is connected to your computer and follow the below steps:

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:

   a) **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.*

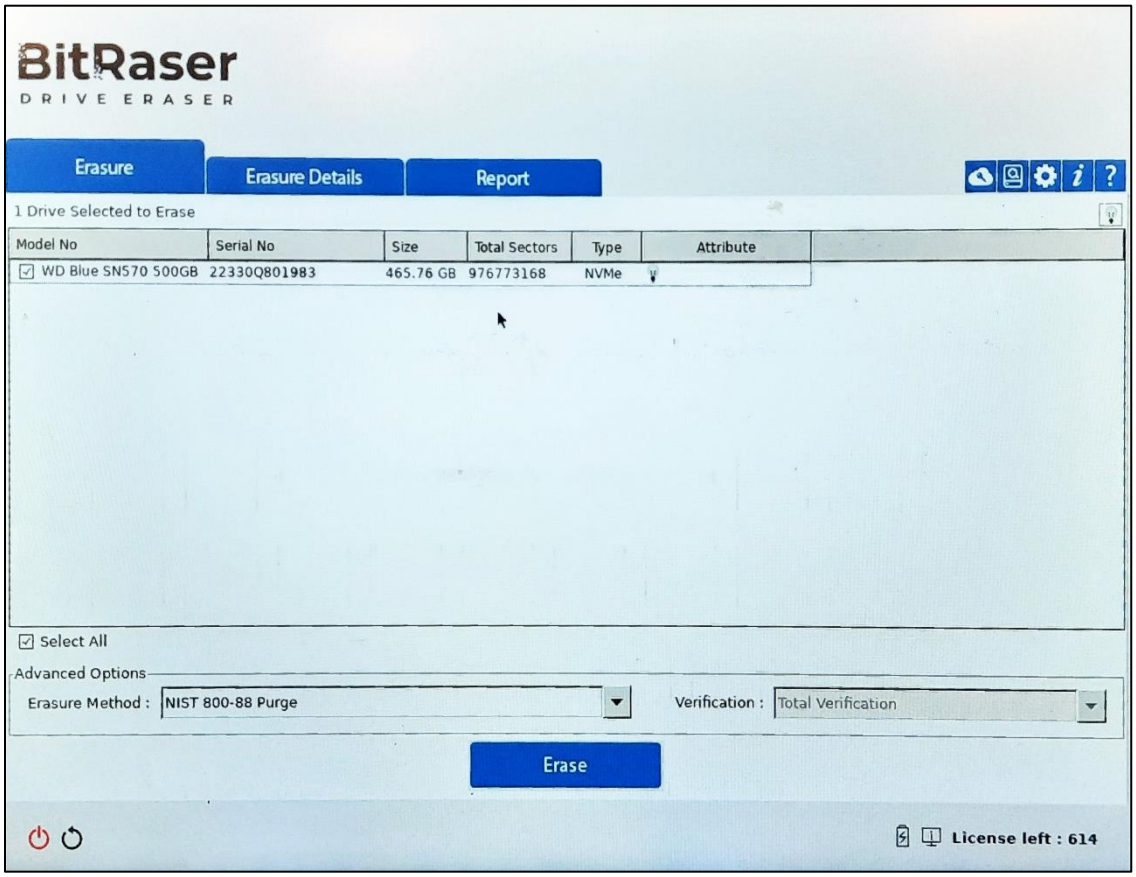
   b) **BitRaser NOFLR:** This option uses NOFLR functionality and is mostly used if the **BitRaser Drive Eraser** fails to run using the first option.

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

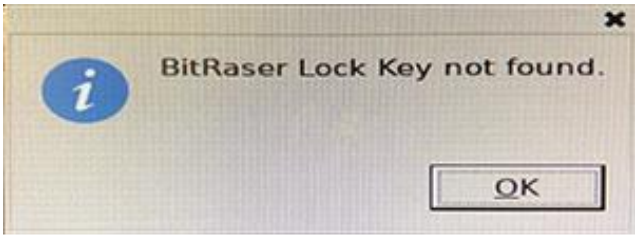
   Note: BitRaser Drive Eraser *automatically runs using the first option if there is no input from the user in 30 seconds. Use the arrow keys on your keyboard to cancel the action within 30 seconds.*

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

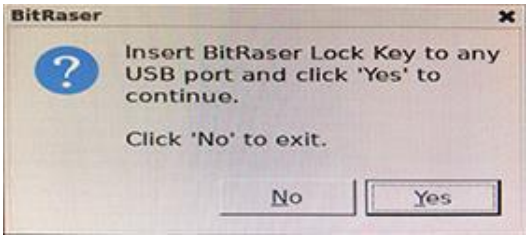
5. Once the system booting completes, it shows the **BitRaser Drive Eraser** running on the screen as shown below:



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:

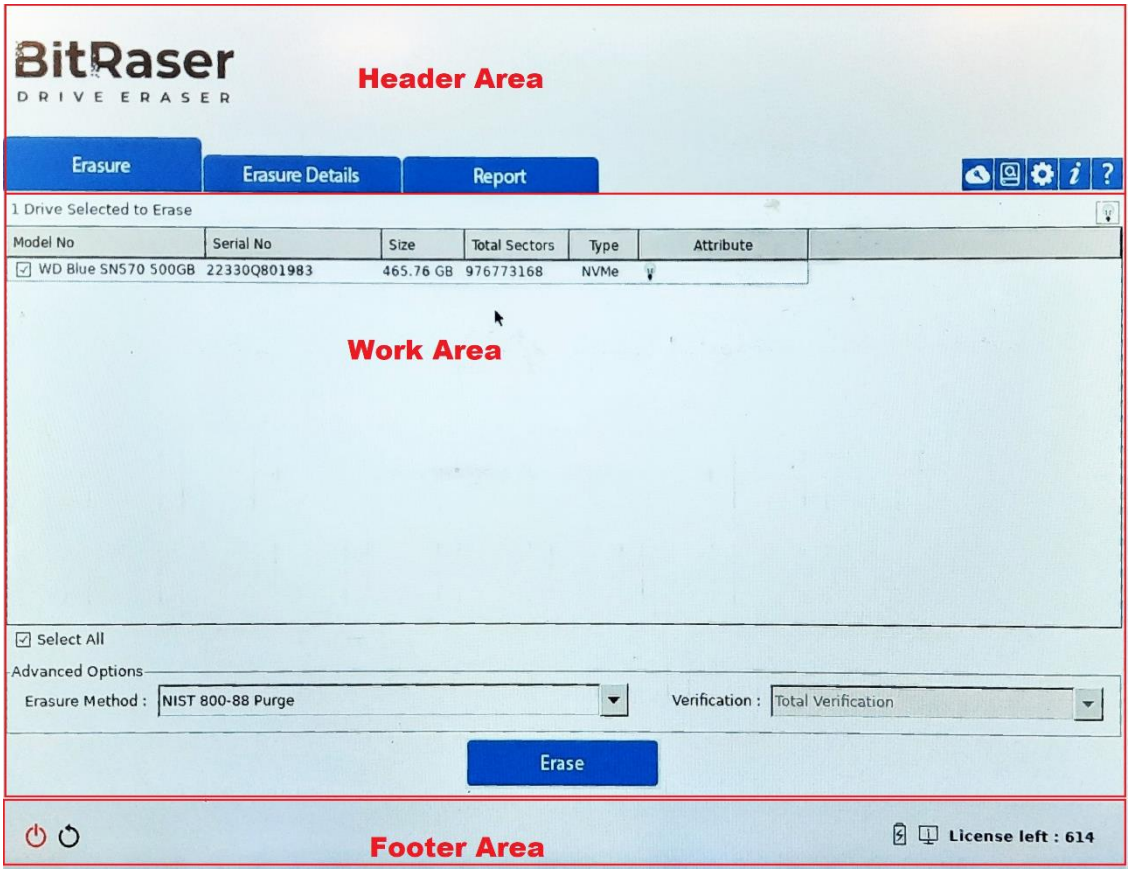


Connect the **BitRaser Lock Key** to the USB port of your computer and Click **Yes**.

2.3. GENERAL OVERVIEW OF USER INTERFACE

The User Interface is divided into three main areas:

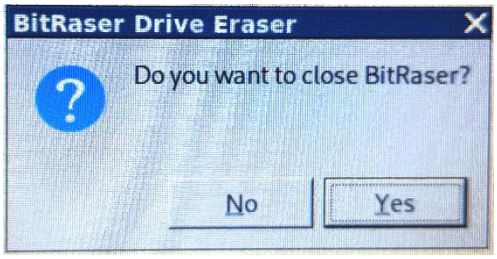
- Header Area
- Work Area
- Footer Area



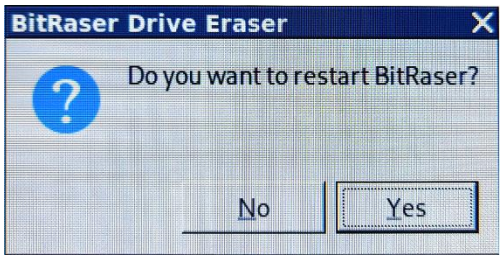
- **Header Area:** The header area contains following tabs and buttons:
  - **Erasure Tab** – This tab contains a list of the connected drives in a list view and is used to perform erasure process.
  - **Erasure Details Tab** – This tab is used to enter various details to be included in reports. To know more, see the Configure 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 BitRaser 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:
  - **Shutdown Button** : Click this button to shut down **BitRaser Drive Eraser**. The screen appears as shown, click **Yes** to close and **No** to cancel the action:



  - **Restart Button** : Click this button to restart **BitRaser Drive Eraser**. The screen appears as shown, click **Yes** to confirm or else click **No**.



  - **Battery Information** : Hover on this icon to know the device's battery percentage.
  - **System Information** : Hover on this icon to learn about the device's RAM and Processor info.
  - **License left:** This shows the number of licenses left to perform erasure process.

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

2.4. CONNECTING TO INTERNET

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

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

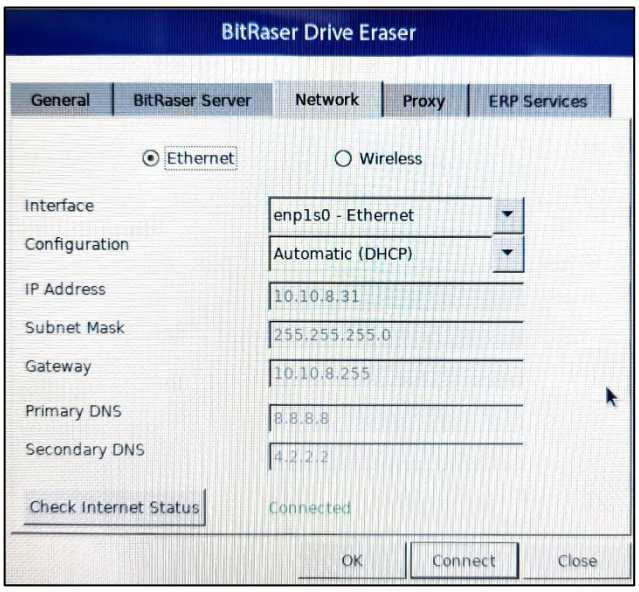
1. Click on the **Settings** icon in the top right corner of the screen. The settings window appears that can be used to change various general and default settings of the software. This window has the following tabs:

   - General Settings
   - BitRaser Server Settings
   - Network Settings
   - Proxy Settings
   - ERP Services

2. Click on **Network** tab. This tab has the following options to connect to the internet:
   - Ethernet
   - Wireless

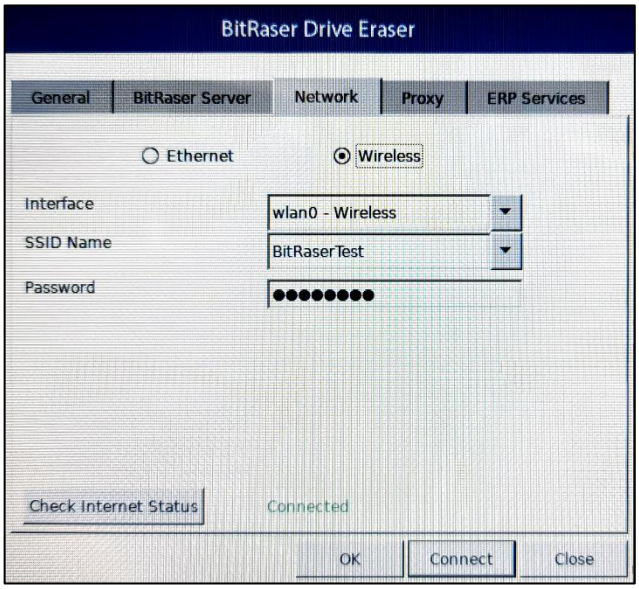
Note: *The* ***Wireless*** *option will only be available if you have a wireless network card installed on your computer.*

- **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.
    i. **Automatic (DHCP) Configuration:** The **Automatic (DHCP)** configuration is selected in this field by default. This configuration will fill up all the required fields automatically.
    ii. **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:**



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

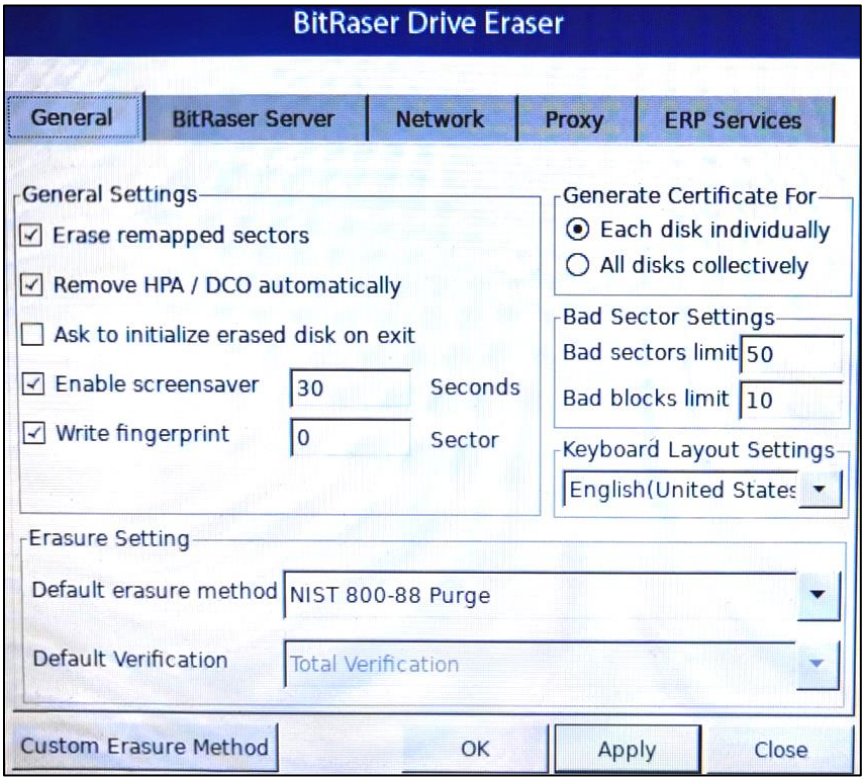
6. Click **OK** or **Close** button to exit the settings window.

Note: *If you wish to connect internet using a proxy, see Proxy Settings.*

2.5. GENERAL SETTINGS

To begin with **BitRaser Drive Eraser** application, it is necessary to understand and configure various settings. Click the **Settings** icon on the top right corner of the screen. This window allows to change various general and default settings of the software. All these are the configurations that are mandatory either for setting up the application or for an ease of using the application. The Settings window has the following tabs:

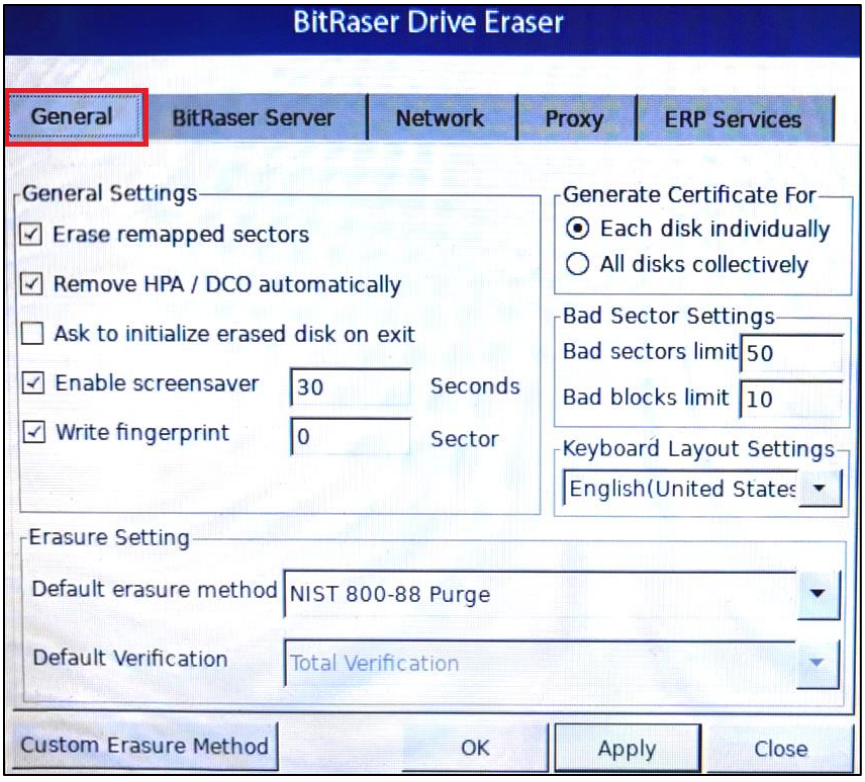
1. General Settings
2. BitRaser Server Settings (Applicable only if you have licenses on BitRaser cloud)
3. Network Settings (Applicable only if you have licenses on BitRaser cloud)
4. Proxy Settings (Applicable only if you have licenses on BitRaser cloud)
5. ERP Services (Applicable only if you have licenses on BitRaser cloud)



The **General Settings** tab allows you to configure some very basic details that are needed during the drive erasure process, Certificate settings, Bad Sector settings, and Keyboard Layout Settings. The default settings can be set for Erasure method and Data Erasure verification.

Further, the Custom Erasure Method button allows you to add customization for erasing the data.

Each tab is described in details below:



General Settings:

- **Erase remapped sectors** – Check-mark this field to erase the remapped sectors of the hard drives if any.

Note: *This feature 'Erase remapped sectors' is only applicable for Linux version*

- **Remove HPA/DCO automatically** – Check-mark this field to remove Host Protected Area (HPA)/Device Configuration Overlay (DCO) area of memory on a hard drive which means this part of the hard drive will also be considered for data erasure.

Note: *This feature 'Remove HPA/DCO' is not applicable for Mac version*

- **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 completes.
- **Enable screensaver** – This field enables a screensaver that shows you the process status such as erasure completed, failed or in-progress. Set the duration between 10 to 240 seconds after which the screensaver should start appearing.

Note: *This feature 'Enable screensaver' is not applicable for Windows version*

- **Write fingerprint** – This field enables you to mark a fingerprint at drive's sector after the completion of erasure process. This fingerprint acts as a unique identifier to verify at a later

stage that the drive has been erased using **BitRaser Drive Eraser** application. Specify the sector number for the drive in the text field provided, where you wish to mark 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.
- **All disks collectively** – Checking this field will generate a single certificate for all the disks collectively.

Bad Sector Settings:

- **Bad Sector Limit** – Specify the Bad Sector limit after which the wiping process would stop.
- **Bad Block Limit** – Specify the Bad Block limit after which the wiping process would stop.

Keyboard Layout Settings:

Select the 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

Erasure Settings:

This option allows you to edit the default erasure settings:

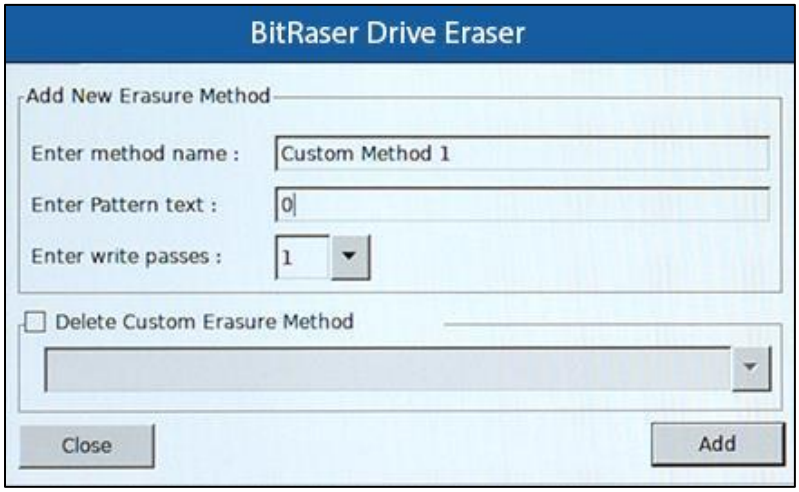
- **Default erasure method** – Select the default erasure method from the drop-down.
- **Default Verification** – Select the default verification method from the drop-down.

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.



3. In '**Enter method name**' field, type the name you want to give to your erasure method.

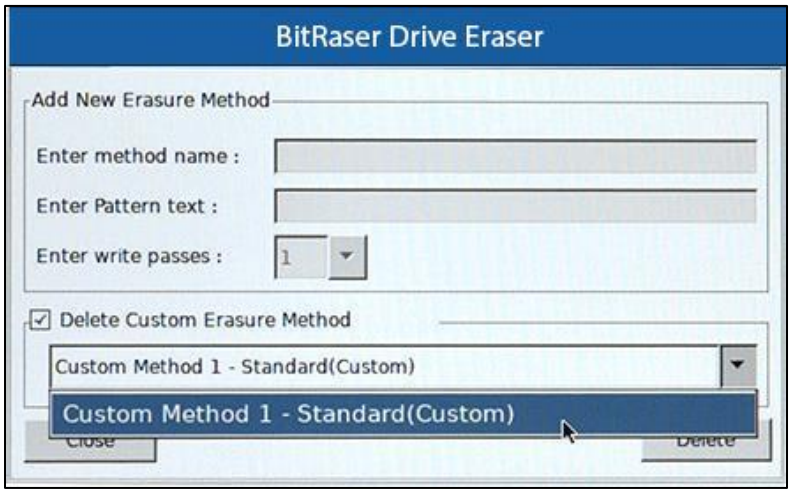
4. In '**Enter Pattern text**' field, type the pattern or data you want to overwrite on the disk during the wiping process.

5. In '**Enter write passes**' field, select the number of passes from one to nine, in which you want your erasure to be completed.

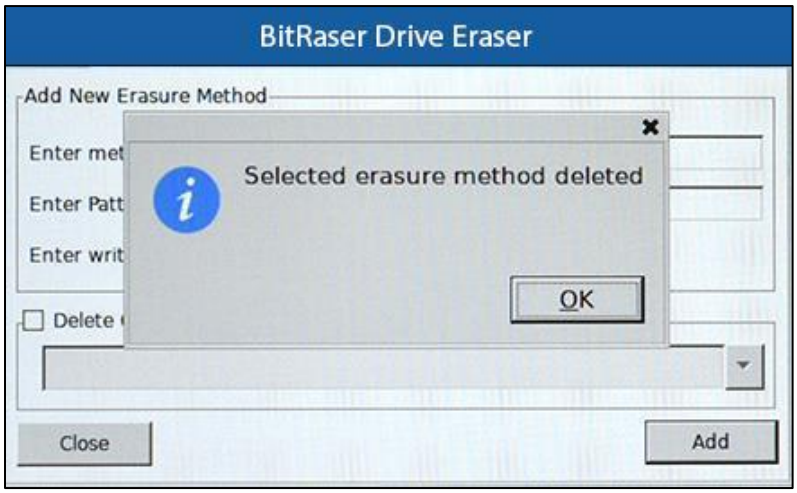
6. Click on **Add.**

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.



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.*

2.6. CONNECTING TO BITRASER SERVER

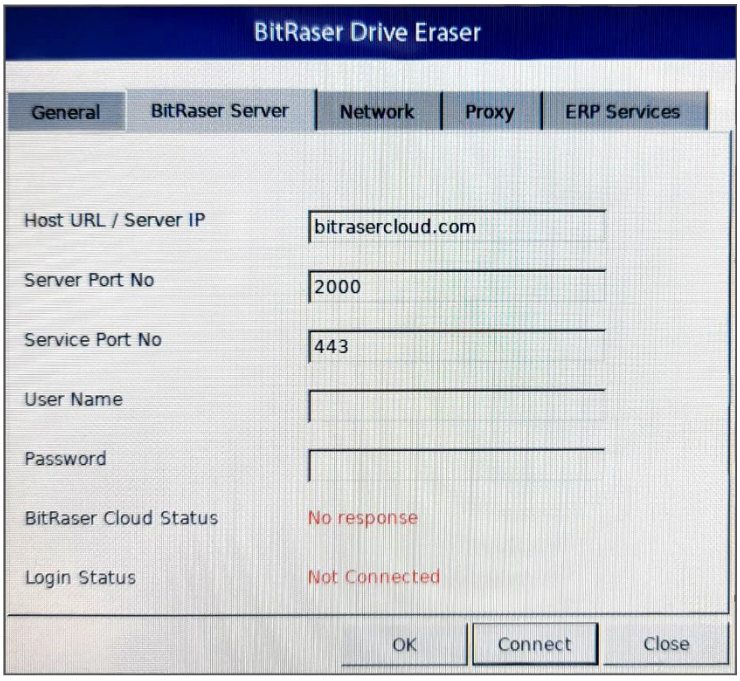
This topic is applicable only if you have BitRaser Drive Eraser's licenses on BitRaser cloud

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, follow the below steps to connect to the **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
   - ERP Services

2. Click on **BitRaser Server** tab. This tab has the following fields to fill:



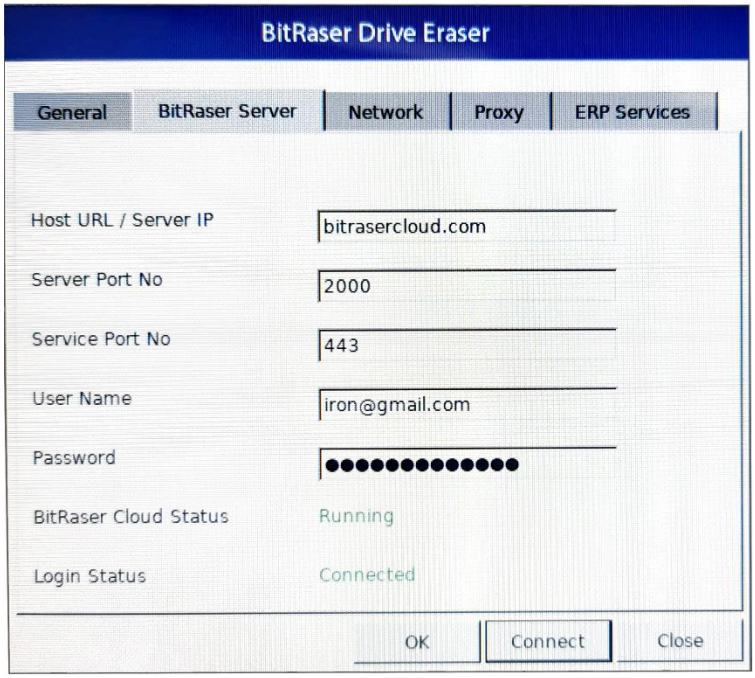
***Note**: **BitRaser Cloud Status** shows "No Response" when **BitRaser Cloud Server** is not accessible from your network otherwise it shows Running.*

Sr. No.	Field Name	Description
1.	Host URL/ Server IP	Host URL or Server IP address where the BitRaser Cloud Console is located
2.	User Name	User Name which is used to login to the BitRaser Cloud Console
3.	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**.



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

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

2.7. PROXY SETTINGS

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

BitRaser Drive Eraser gives an option to connect to a Proxy server if required. To connect to a Proxy, follow the below 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.

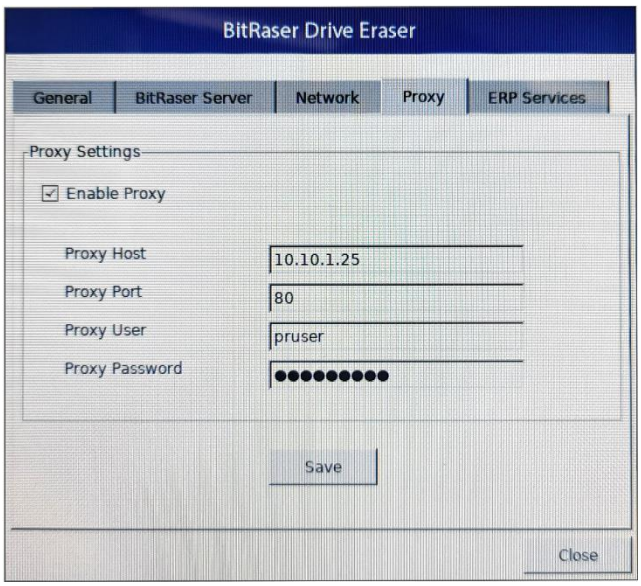
2. Click on **Proxy** tab.

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

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

The following fields need to be filled:

Sr. No.	Field Name	Description
1.	Proxy Host	Enter the address of proxy server
2.	Proxy Port	Enter the port number that the proxy server uses
3.	Proxy User	Enter the proxy user name
4.	Proxy Password	Enter the authentication password of the proxy user



4. Click on **Save** to use the entered proxy settings.

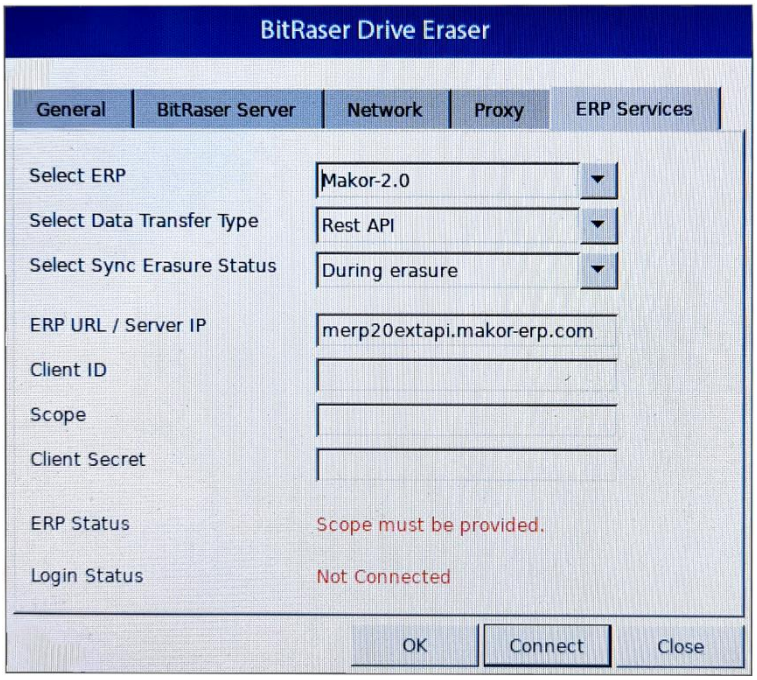
5. Use the **Network Tab** to connect to the internet with the saved proxy details.

2.8. ERP SERVICES

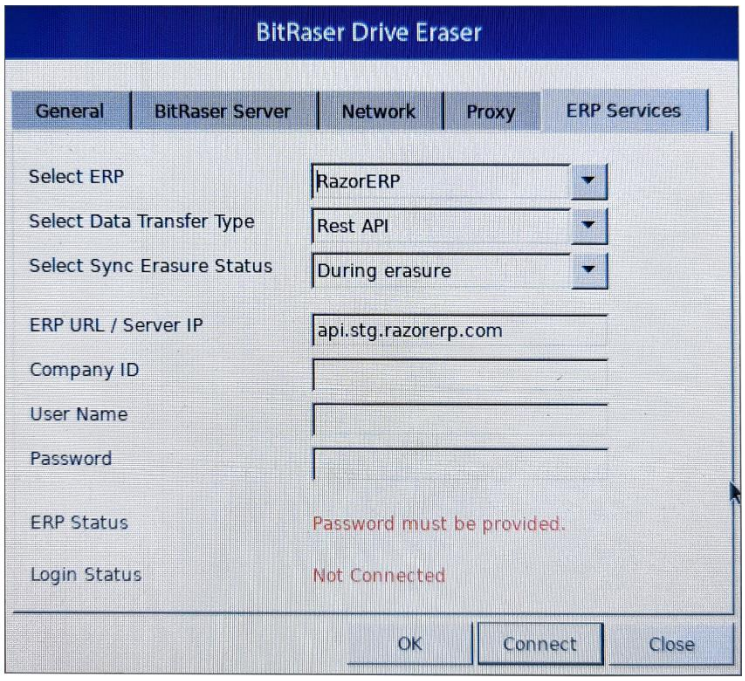
Note: This feature 'ERP Services' is only applicable for Linux version

BitRaser Drive Eraser supports integration with **Makor-2.0** and **RazorERP**. Fill in the required details in order to connect and import the reports to your preferred server.

Makor-2.0



RazorERP


BitRaser Drive Eraser
General
BitRaser Server
Network
Proxy
ERP Services
Select ERP
RazorERP
Select Data Transfer Type
Rest API
Select Sync Erasure Status
During erasure
ERP URL / Server IP
api.stg.razorerp.com
Company ID
User Name
Password
ERP Status
Password must be provided.
Login Status
Not Connected
OK
Connect
Close

3. HOW TO

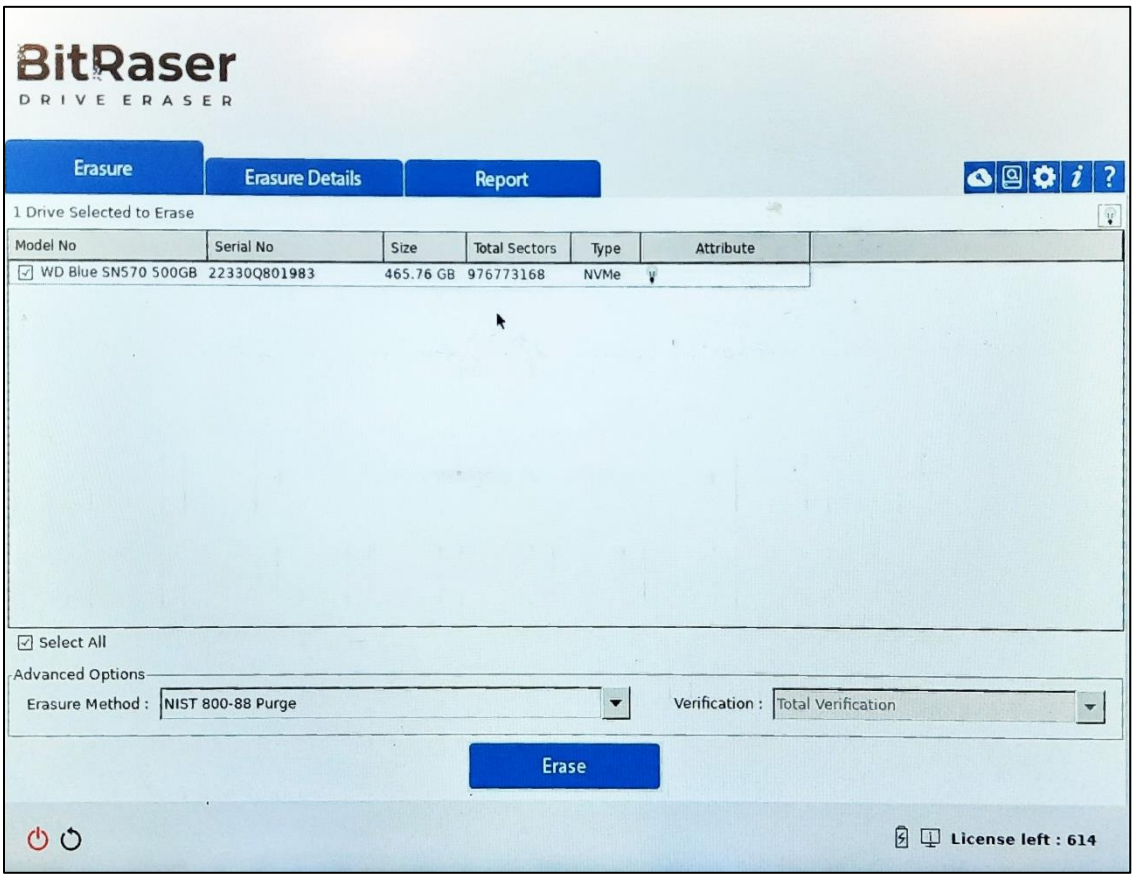
3.1. BEGIN ERASURE PROCESS

BitRaser Drive Eraser application allows you to securely erase data from hard drive by using various erasure methods available. There are 24 data erasure methods available to erase the data. Selection of erasure method is available under **Advanced Options** section. Also, there are verification options available to verify that the data has been erased permanently and is no longer recoverable.

Note: *You can erase up to* ***100 hard drives*** *simultaneously using* ***BitRaser Drive Eraser****.*

To erase data using BitRaser Drive Eraser:

1. Run **BitRaser Drive Eraser** application. The screen would be as shown below:



2. All the storage devices along with its 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 as mentioned in the table.

Sr. No.	Erasure Methods	Description
1.	Zeroes	This algorithm erases data by overwriting it with zeros in a single pass. This is the fastest algorithm available to a user.
2.	Pseudo-random	This algorithm erases data by overwriting an entire hard drive with randomly generated numbers in a single pass.
3.	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.
4.	Random Random Zero (6 passes)	This algorithm erases data by overwriting a storage media with random characters in multiple passes.
5.	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.
6.	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.
7.	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.

8.	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.
9.	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.
10.	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.
11.	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.
12.	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.
13.	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.
14.	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.
15.	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.
16.	Canadian CSEC ITSG-06	This algorithm uses a combination of zeros and random characters, plus ones.
17.	British HMG IS5 Baseline Standard	One Pass-Random Pattern.
18.	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.
19.	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.

20.	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
21.	BitRaser Secure & SSD Erasure	SSDs differ from HDDs as in SDD data is stored electronically on transistor arrays, thus this algorithm for SSD ensures complete data erasure.
22.	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).
23.	NIST 800- 88 Clear	This algorithm overwrites media by using organizationally approved and validated overwriting technologies/methods/tools
24.	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.
25.	NSA 130-1	Defined by the National Security Agency, this method uses a 3-pass overwrite: writes a random character, writes another random character and writes a known value. This process is completed by verifying the write.
26.	Custom Methods	This algorithm is added by the user. Users can create up to 5 custom erasure methods.

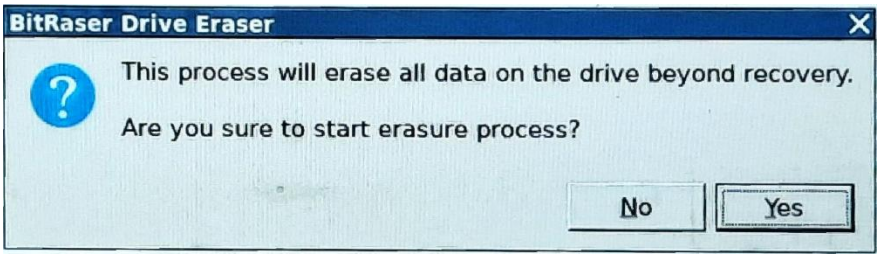
6. From **Advanced Option** section, select any one of the verification methods:

Sr. No.	Verification Methods	Description
1.	No Verification	Select this option if verification is not needed for the erasure process.
2.	Random Verification	In Random Verification method, the sectors of the storage devices are selected randomly to verify the erasure operation performed.
3.	Total Verification	In Total Verification method, all the sectors of the storage devices are verified after the erasure operation is performed.

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

Note: *If the drive selected by you is a SED, refer to Erasure Process for SED Drive before proceeding.*

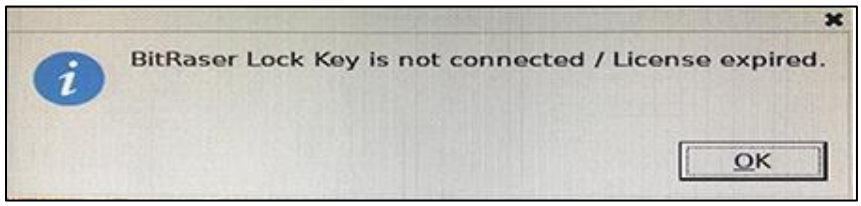
7. Click **Erase** to initiate the erasure process. The following screen appears:



Note:

- *For licenses on BitRaser 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 Erase 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:*



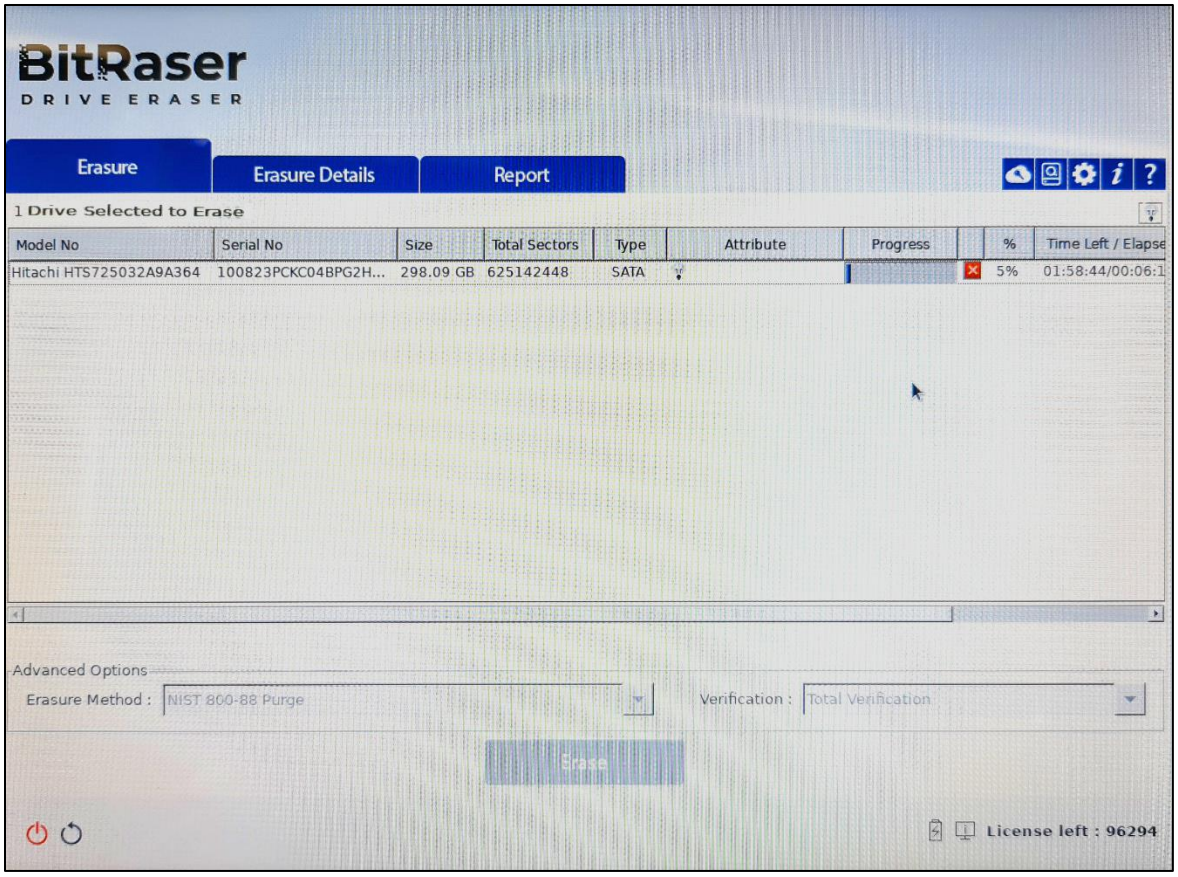
*In that case, make sure the **BitRaser Lock Key** is connected and initiate the erasure process again.*

***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, shows the progress of the erasure along with the 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 BitRaser cloud, the erasure report is automatically sent to* ***BitRaser Server*** *when the erasure process is completed or cancelled:*

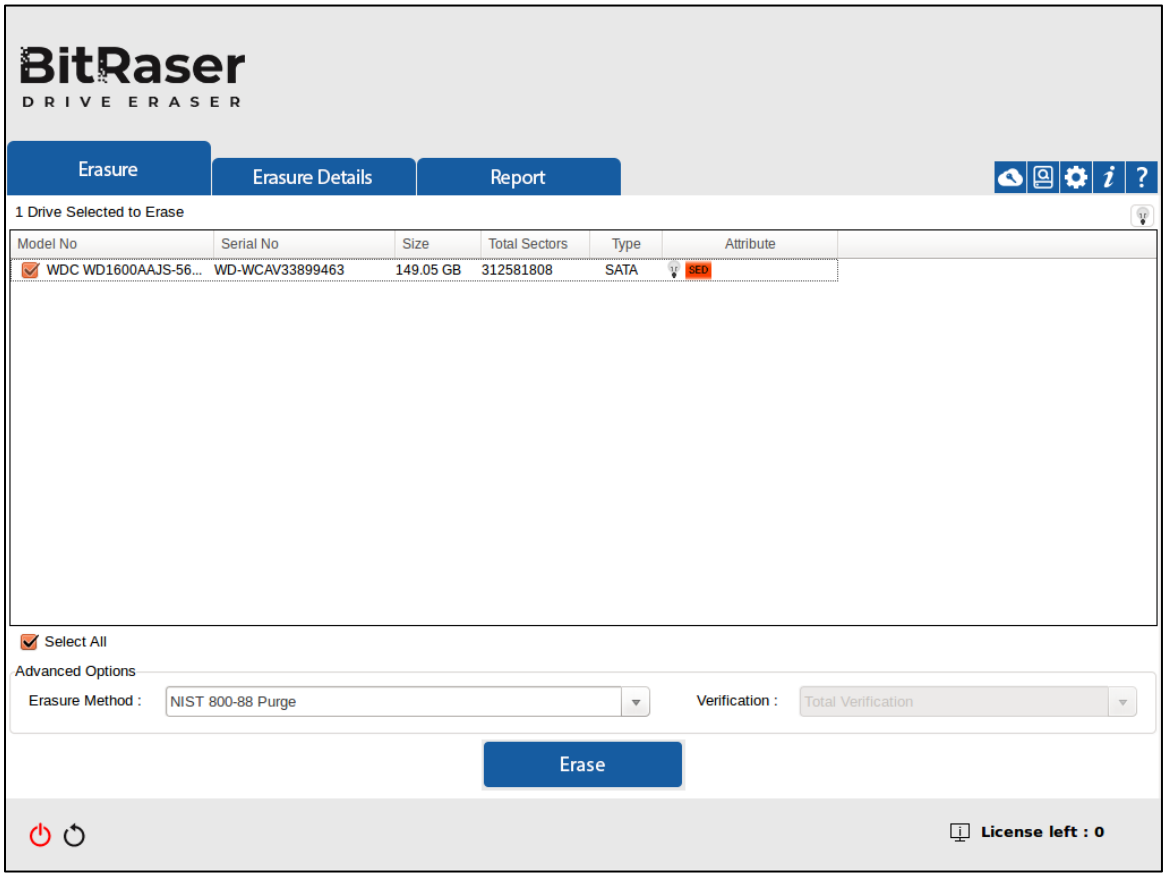
- *If the report is successfully sent to* ***BitRaser Server****, you will see* *icon on the bottom right corner of the report under* ***Report Tab****.*
- *If BitRaser Drive Eraser is not connected to internet and the report is not sent to* ***BitRaser Server****, you will see* *icon on the top right 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 re-connected, then we can manually send Report to* ***BitRaser Server****. For more information, refer Export Report section.*

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.*

This topic is only applicable for Linux version as SED drive support is provided only in Linux and not in Windows or Mac

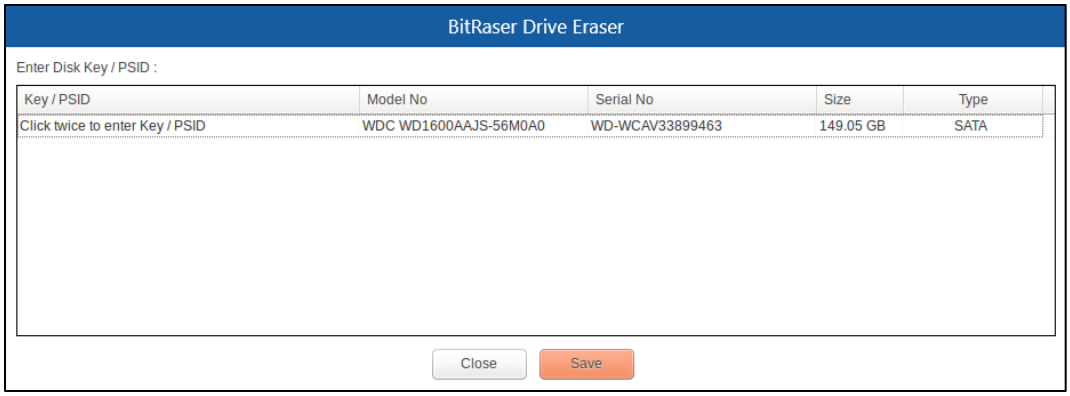
Erasure Process for the SED

1. If your selected drive is a SED (Self-Encrypting Drive), you will be required to enter its password to provide access for erasure. Once you have chosen the erasure and verification method, simply press **Erase** button for opening the password window.

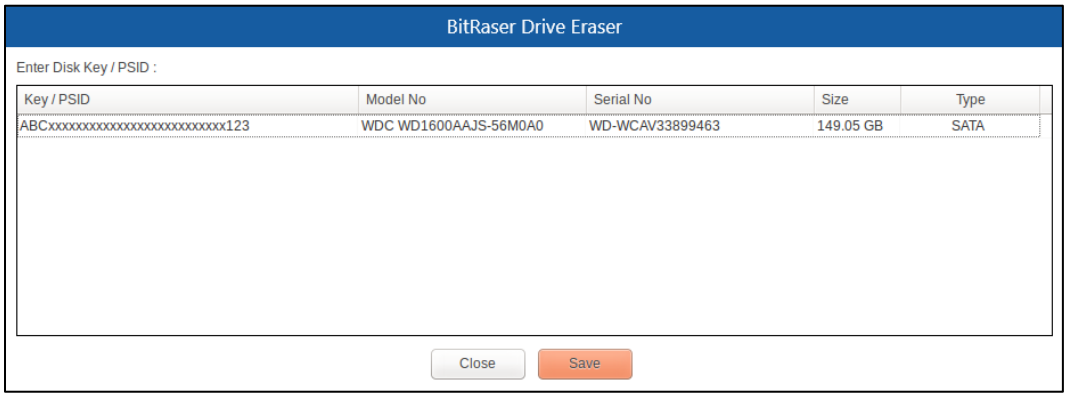


Note: *The* SED *button is provided under the Attribute tab of the SEDs for their easy identification.*

2. **BitRaser Drive Eraser** window appears. Double tap on "**Click twice to enter Key / PSID**" to enable the text field.



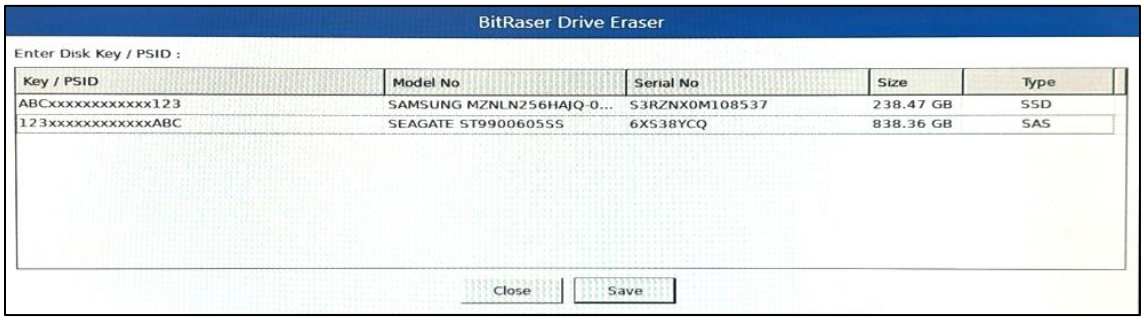
3. Enter the password or key in the text field.



Note: *You can also click on* SED *button located under the Attribute tab to access the above shown screen for entering the password of a particular SED.*

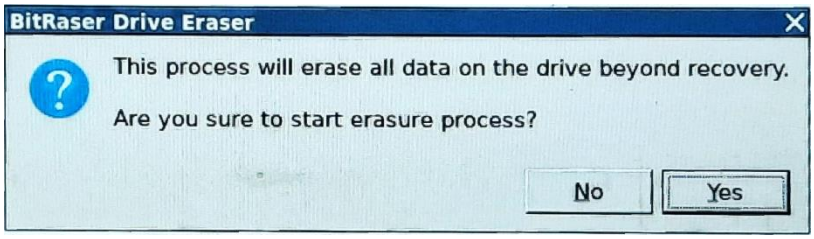
4. Click on **Save** button to proceed further.

Note: *If there are multiple SEDs, you can easily enter the password for each one by tapping on the* SED *button given individually for each SED. Alternatively, as mentioned in the previous steps, you can click on the* ***Erase*** *button, and all your SEDs will be listed. You can then enter and save the password for each SED on the same screen, as shown below.*

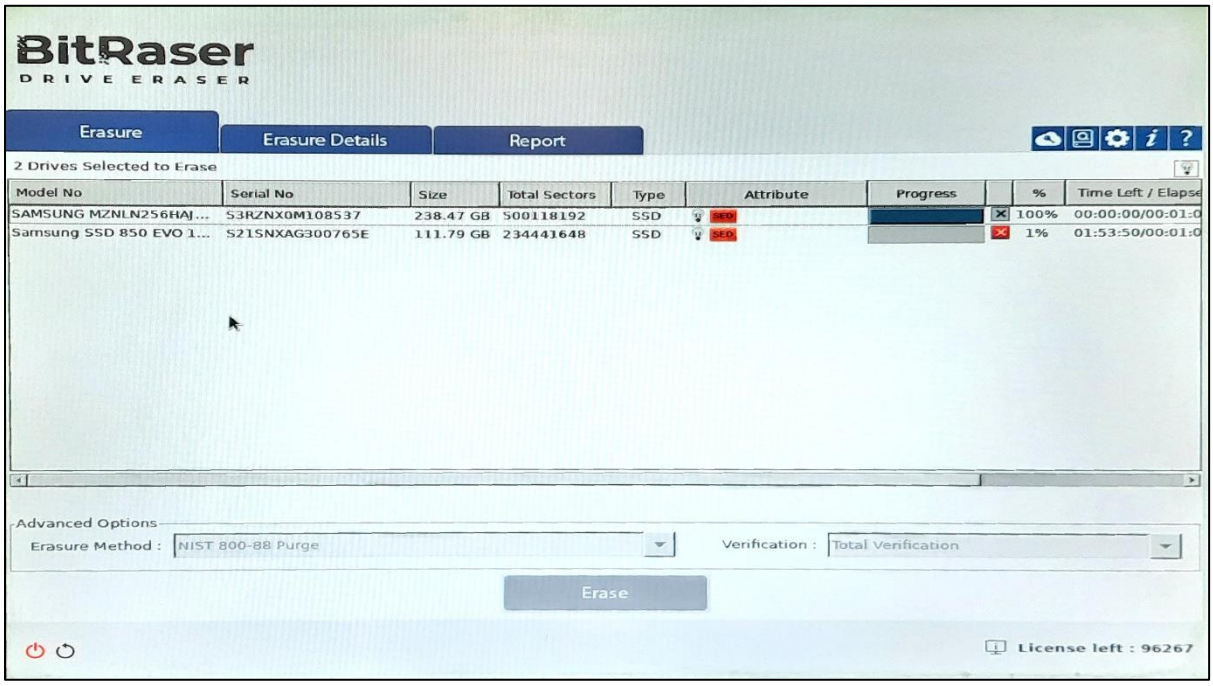


Note: *It will lead to a failed erasure attempt if you save the wrong password of a SED and you will be required to reboot your device for another attempt.*

5. Once you click on the **Save** button, the following screen appears:



6. Click **Yes** to start the erasure process or **No** to cancel the action.
7. A progress bar as shown below appears, shows the progress of the erasure along with the percentage of completion, time left/elapsed, speed and bad sectors found on disk during the process:



8. Rest of the erasure process remains same for both SED and other drives. Therefore, follow up the process from here.

3.2. CONFIGURE ERASURE DETAILS

Configure the general information about the customer, asset details, and adding custom fields as per the requirements. The information entered in this section will be added to the **Erasure Reports** and can be modified later if required. The **Erasure Details** configuration is divided into three sub-sections:

1. **Enter Erasure Details**: Erasure Details allows you to enter information like customer details, media details, details of technician performing the erasure, and the person validating erasure.

2. **Enter Asset Details**: Asset Details Tab shows the information like adding Machine Asset Tag Name, shows the information about Asset Tag, Model No, Serial No, and Size of the connected storage device(s).

3. **Enter Custom Fields**: Custom Fields allows you to enter up to 20 sets of customized fields that can be added to the Erasure Reports.

3.2.1. ENTER ERASURE DETAILS

Configure the general information about the customer, media handling details, technician detail who will be performing the erasure, and the details like validation of the erasure process performed.

The information entered in this section will be added to the **Erasure Reports** and can be modified later if required.

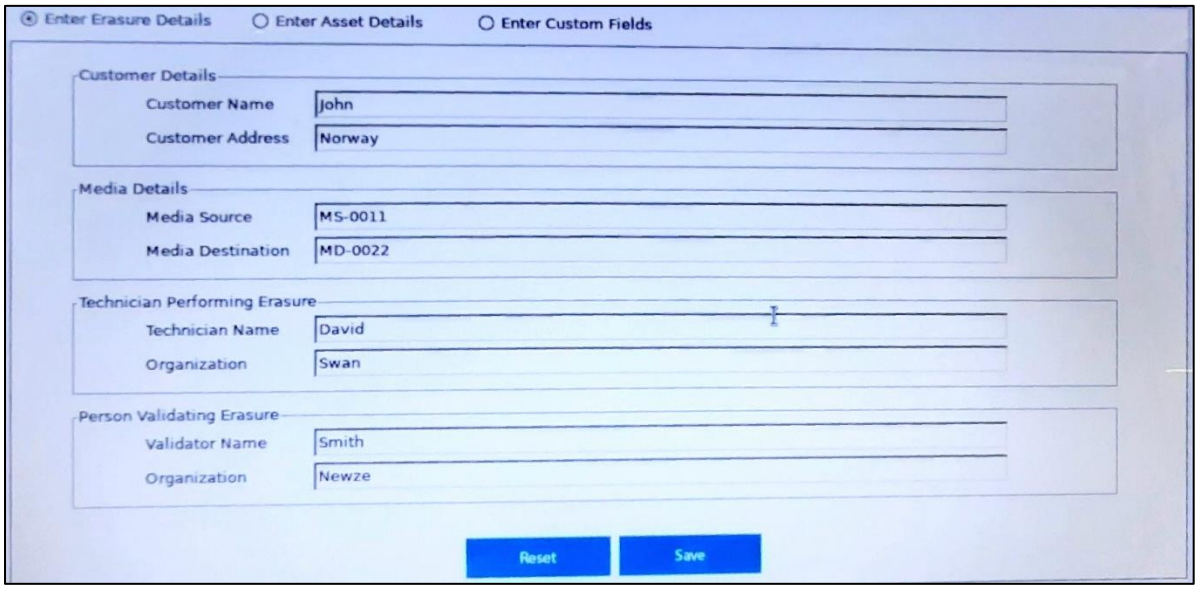
To enter the Erasure Details, follow the below steps:

1. Run **BitRaser Drive Eraser**. Select the **Erasure Details** tab.

2. Select the radio button, **Enter Erasure Details**.

3. Specify the required details:

   - **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 would 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** button to save the information.

3.2.2. ENTER ASSET TAG DETAILS

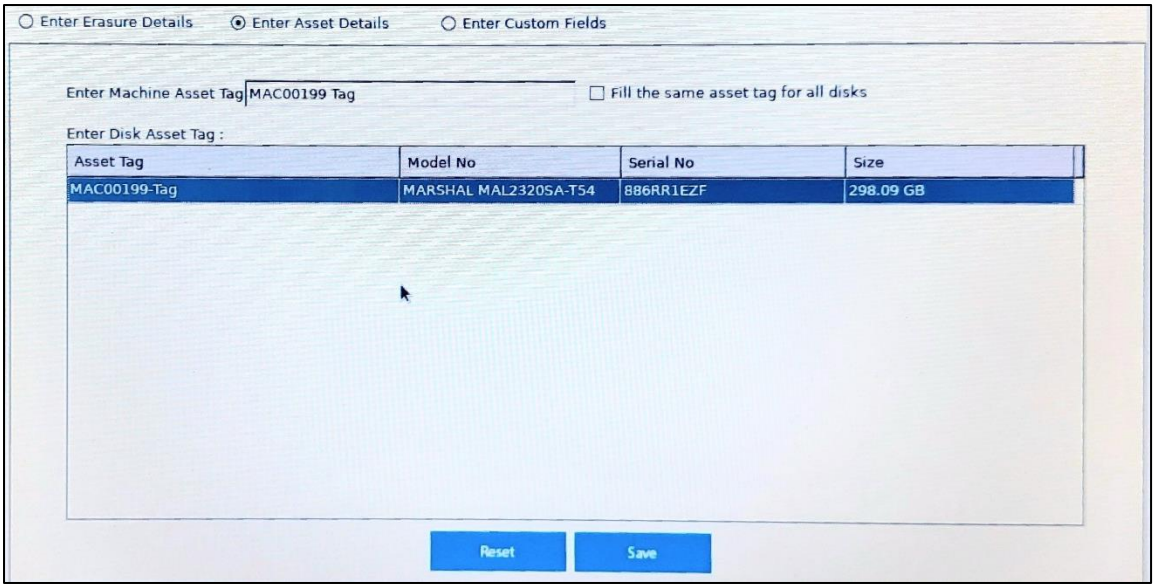
As mentioned earlier, the Asset Details Tab shows the information like adding Machine Asset Tag Name, shows the information about Asset Tag, Model No, Serial No, and Size of the connected storage device(s).

To add the Asset Tag Details, follow the below 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.



4. Select the checkbox **Fill the same asset tag for all disks** if you wish to apply the same asset tag to all the storage disks.

5. The Asset Details Tag shows 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.

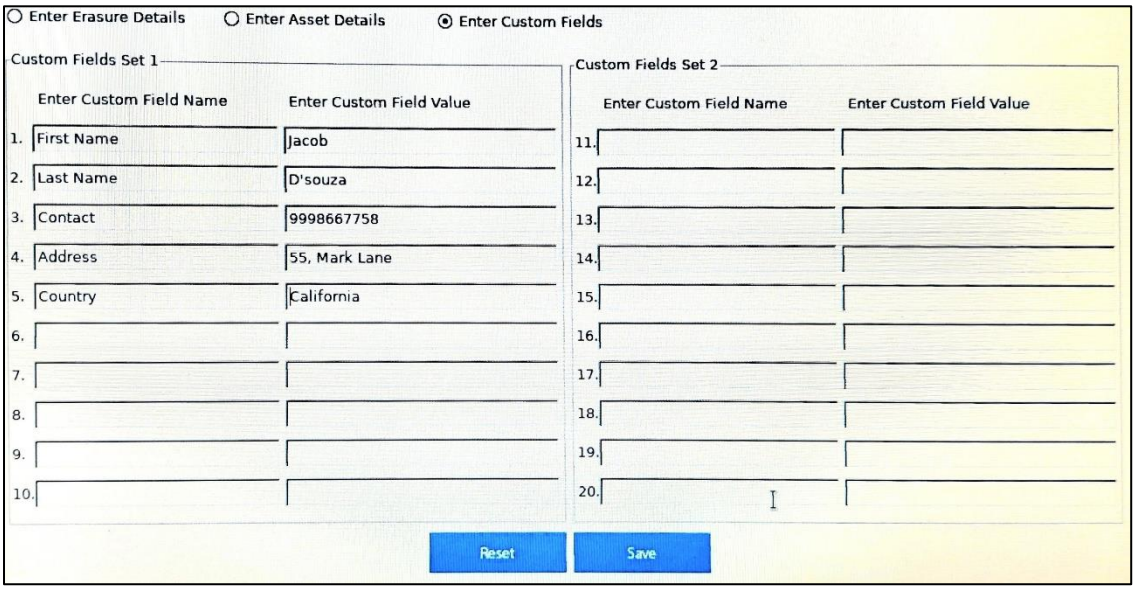
3.2.3. ENTER CUSTOM FIELDS

Add up to 20 sets of customized fields that can be used in creating the Erasure Reports.

To add Custom Fields, follow the below steps:

1. Run **BitRaser Drive Eraser**. Select the **Erasure Details** tab.

2. Select the radio button **Enter Custom Fields**.

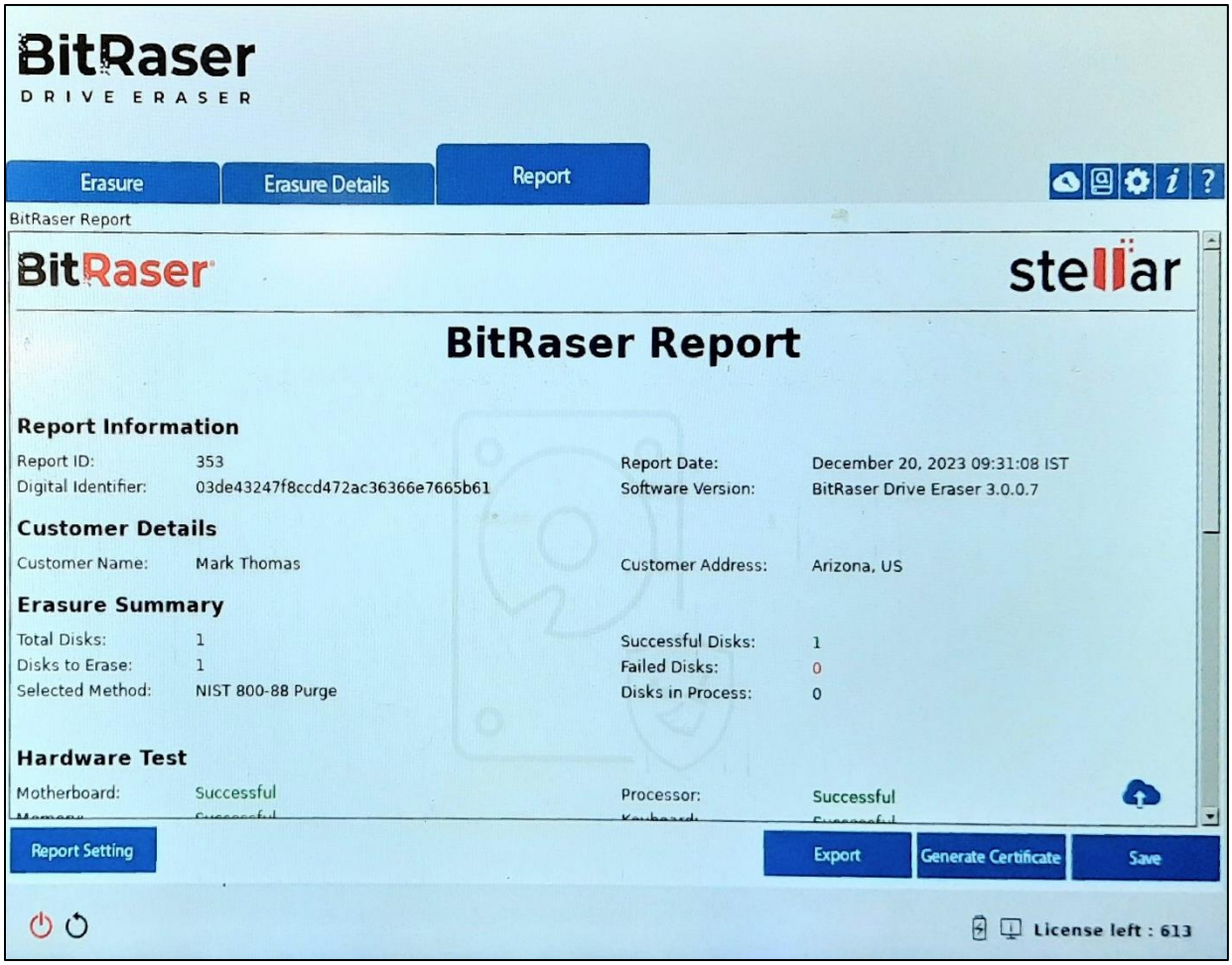


3. Specify the **Custom Field Name(s)** and **Custom Field Value(s)** respectively.

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

3.3. WORK ON REPORT AND CERTIFICATE

BitRaser Drive Eraser provides you detailed Information and contains data fields like Report Information, Customer Details, Erasure Summary, Hardware Test, Hardware Information, Custom Fields, and Erasure Results.



These data fields are explained below:

- **Report Information**: Report Information contains details such as Report ID, Report Date, Digital Identifier and Software Version.
- **Customer Details**: Customer Details contains details such as Customer Name and Address.
- **Erasure Summary**: Erasure Summary contains number of disks, disks to erase, disks to process, number of successful or failed erasure of disks.
- **Hardware Test**: Hardware Test contains details of tests performed on various hardware devices of the system such as motherboard, memory, processor, and so on.

- **Hardware Information**: 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**: Custom Fields contain the customized information that you have defined using Custom Fields option of **BitRaser Drive Eraser**.
- **Erasure Results**: 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 BitRaser cloud).

BitRaser Drive Eraser Certificate:

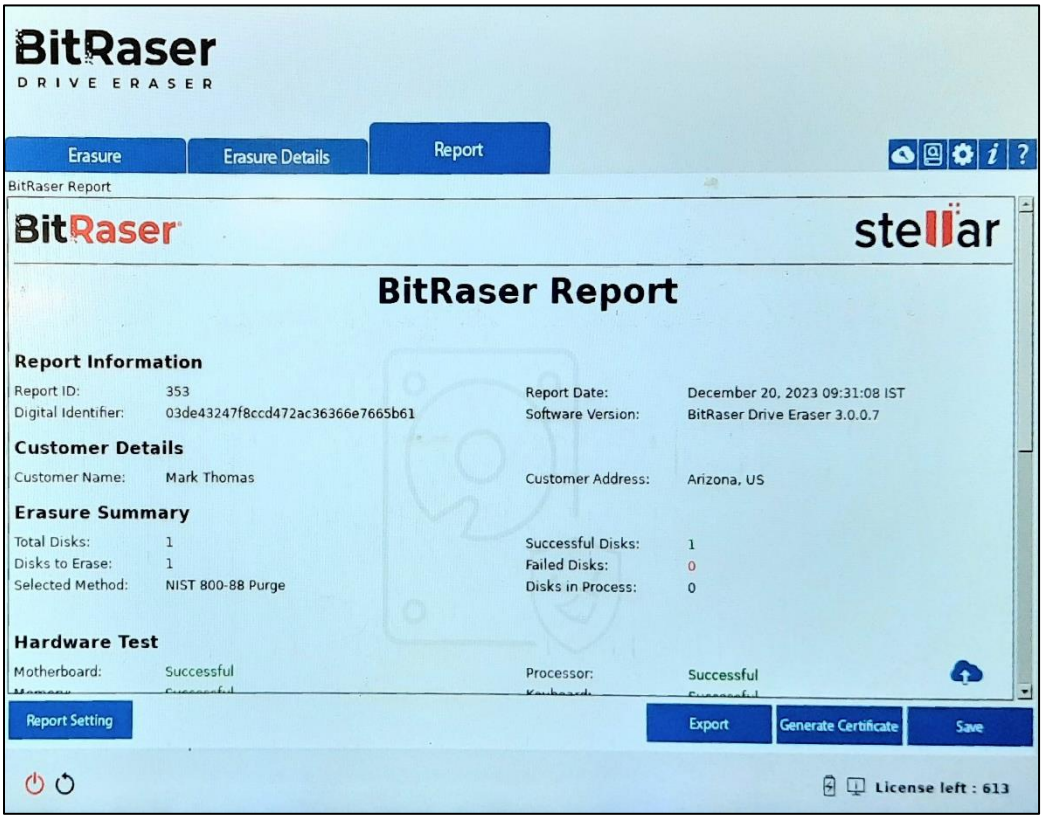
BitRaser Drive Eraser also provides you with a certificate of the erasure process performed. This certificate contains all the erasure details along with the signature and details of technician and validator performing the erasure process.

For information about generating and saving the certificate, see Generate and Save Certificate.

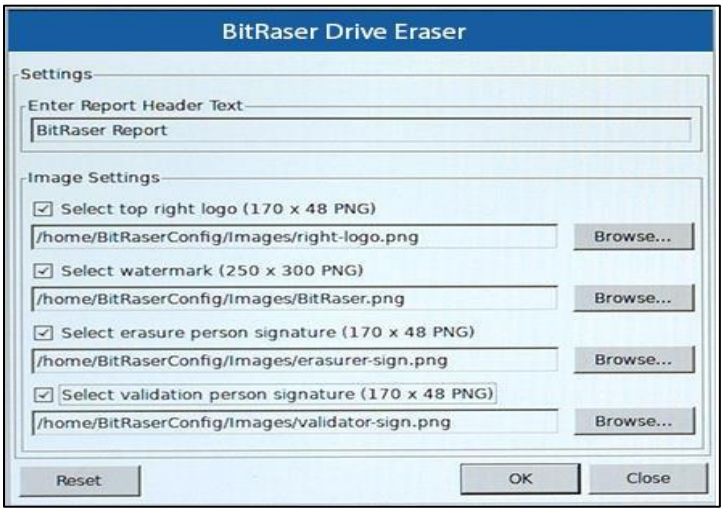
3.3.1. VIEW AND CUSTOMIZE REPORT

To View and Customize BitRaser Driver Eraser report:

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



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



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

Sr. No.	Field Name	Description
1.	Enter report header text	Enter header text that appears on the header of the report (must be maximum of 30 characters)
2.	Select top right Logo	Select the check-box and click Browse to select the top-right logo of the report (image size and format - 170 x 48 PNG)
3.	Select watermark	Select the check-box and click Browse to select the watermark (image size and format - 250 x 300 PNG)
4.	Select erasure person signature	Select the check-box and click Browse to select the erasure person signature (image size and format - 170 x 48 PNG)
5.	Select validation person signature	Select the check-box and click Browse 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.*

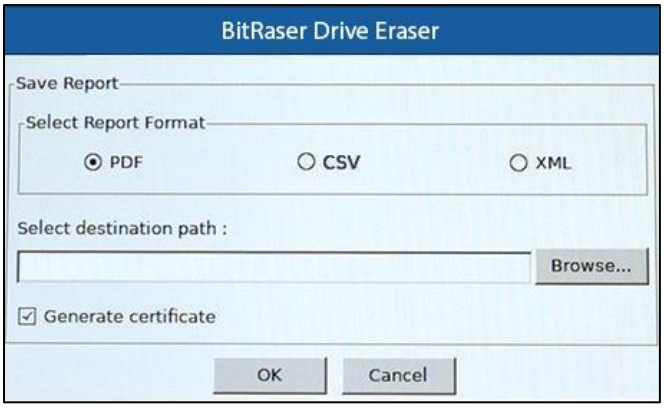
4. After making the required changes to **Report Settings**, click **OK** to save.

3.3.2. SAVE REPORT

To Save a BitRaser Driver Eraser report:

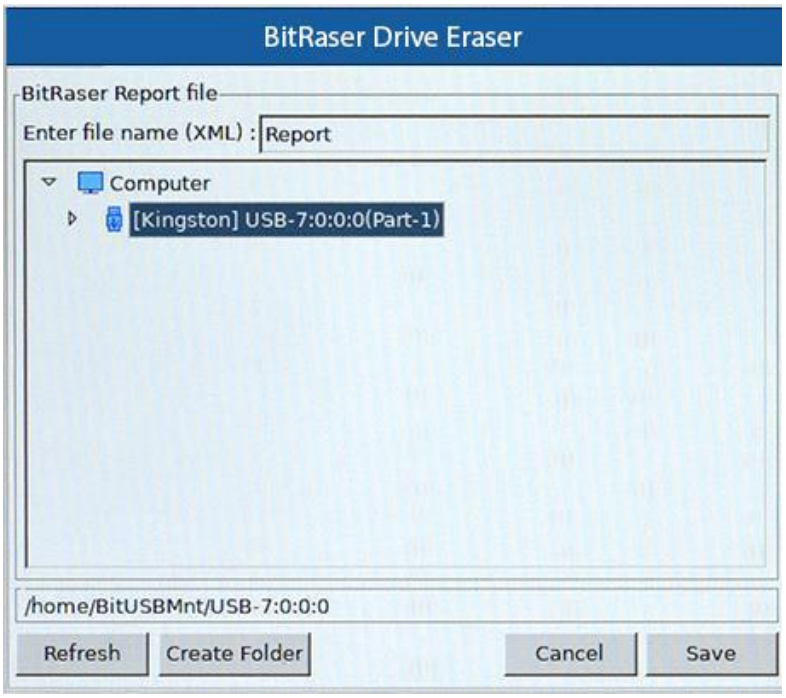
1. Run **BitRaser Drive Eraser**. Select **Report** tab.

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 below 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 BitRaser 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 cloud server (Applicable only if you have licenses on BitRaser cloud)** – This option allows you to send the report to **BitRaser Server**. To send reports, select **Send to cloud server** button and click **Send**.

     Note: *Once you initiate the erasing process, you can export your report to* ***BitRaser Server*** *anytime during the erasure process.*

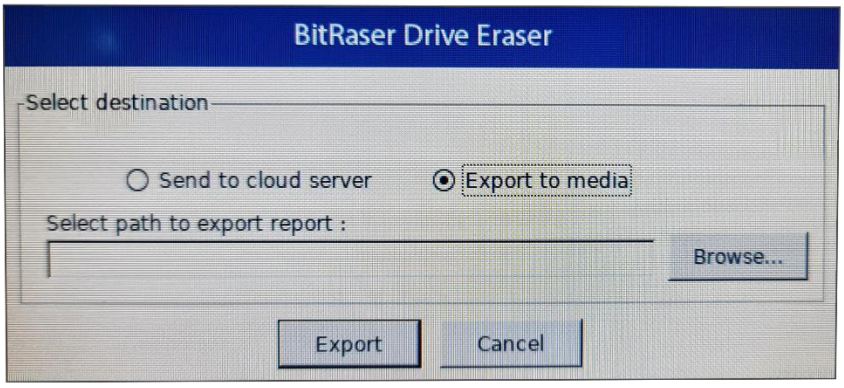
     Note: *Once the erasure process is completed, the erasure report is automatically sent to* ***BitRaser Server****.*

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

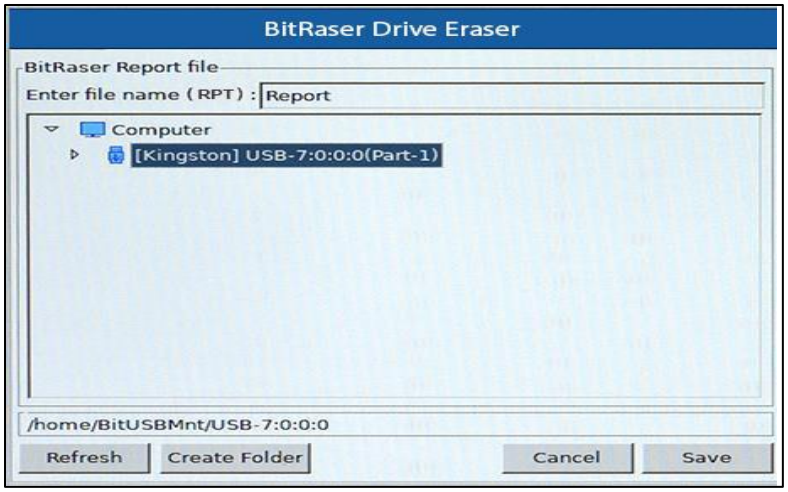
   - **Export to media** – This option allows to export the report to media device in RPT format. Follow the steps as shown below:

     1. Select **Export to media** button.

        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*** *option.*

     2. Click **Browse** button to '**Select path to export report'**.



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*** *button to create a new folder at the destination you selected.*

4. Click **Save** to continue.

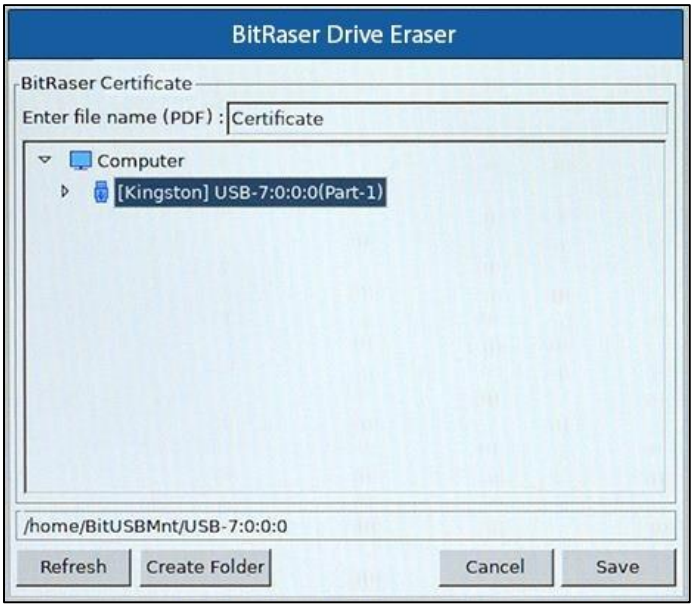
5. On the **Select destination** dialog box, click **Export** to save the report at the selected destination.

3.3.4. GENERATE AND SAVE CERTIFICATE

This option allows to generate and save the erasure certificate to a media device in PDF format. Follow the steps as below:

1. Run **BitRaser Drive Eraser**. Select **Report** tab.

2. Click on **Generate Certificate** button located at the bottom right of the screen, follow the dialog box as shown below:



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. WORK WITH THE LICENSE MANAGER

The topic 'Working with the License Manager' is NOT APPLICABLE for BitRaser Drive Eraser Windows and Mac version

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

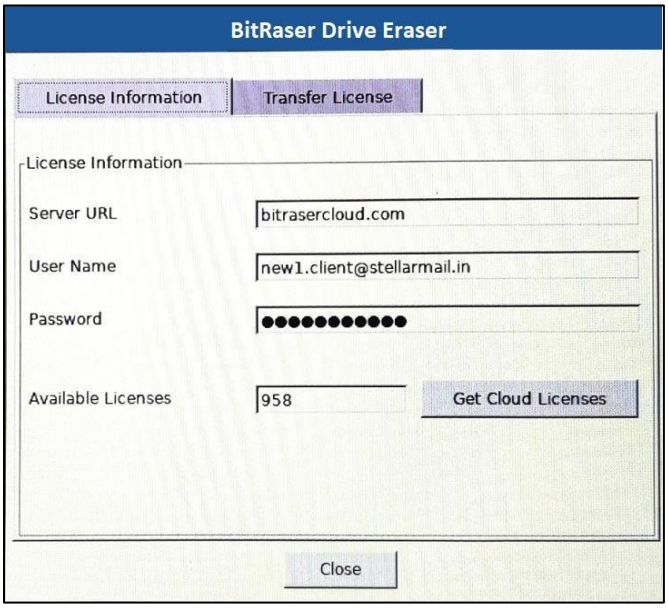
The **License Manager** is a tool that allows to view the license information on **BitRaser Cloud** and to transfer licenses from **BitRaser Cloud** to **BitRaser Lock Key**.

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. If you are already logged into BitRaser Server, the license information is fetched automatically and displayed in the **Available Licenses** field. If you are not logged into BitRaser Server, follow the below steps:
    a. **Server URL** – Specify the Server URL and your BitRaser Cloud credentials, i.e., User Name and Password.
    b. **Available Licenses** – Click on Get BitRaser Cloud Licenses button to fetch available licenses details from the BitRaser Cloud.

3. Click **Close** to go back to the home screen.

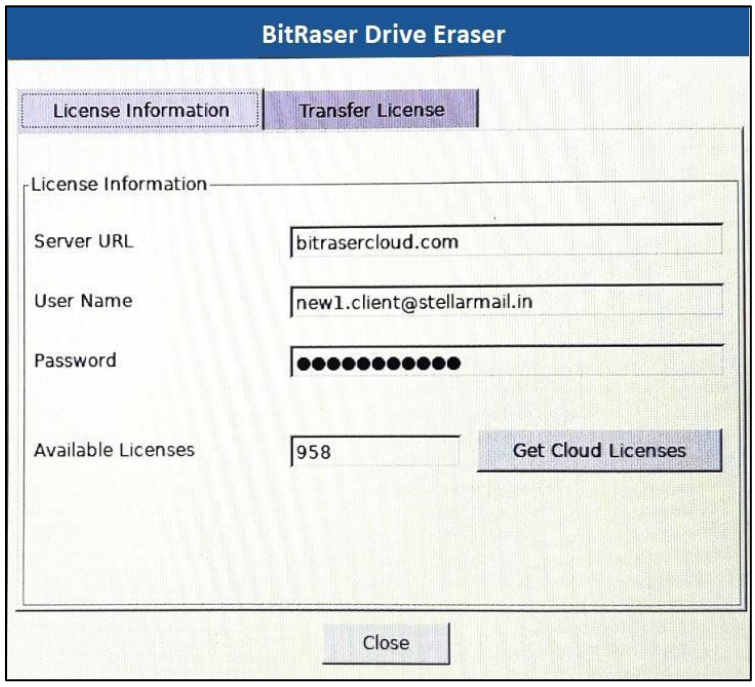
Transfer Licenses from BitRaser Cloud to BitRaser Lock Key

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

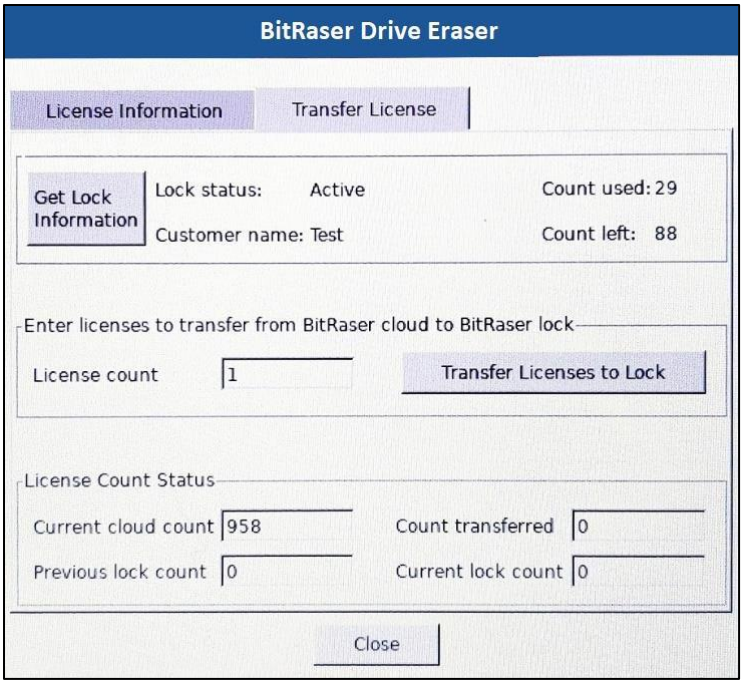
Note: *Before using the transfer license tool, make sure you are logged into* ***BitRaser Cloud*** *and fetched* ***Available Licenses*** *using the steps given above.*

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



2. Click on the **Transfer License** tab. Following window appears:



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

4. Specify the number of licenses to be transferred from **BitRaser cloud** to **BitRaser lock**.

   Note: *The **License Count** 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.

3.5. USE THE HEX VIEWER

The topic 'Using the Hex Viewer' is NOT APPLICABLE for BitRaser Drive Eraser Windows and Mac version

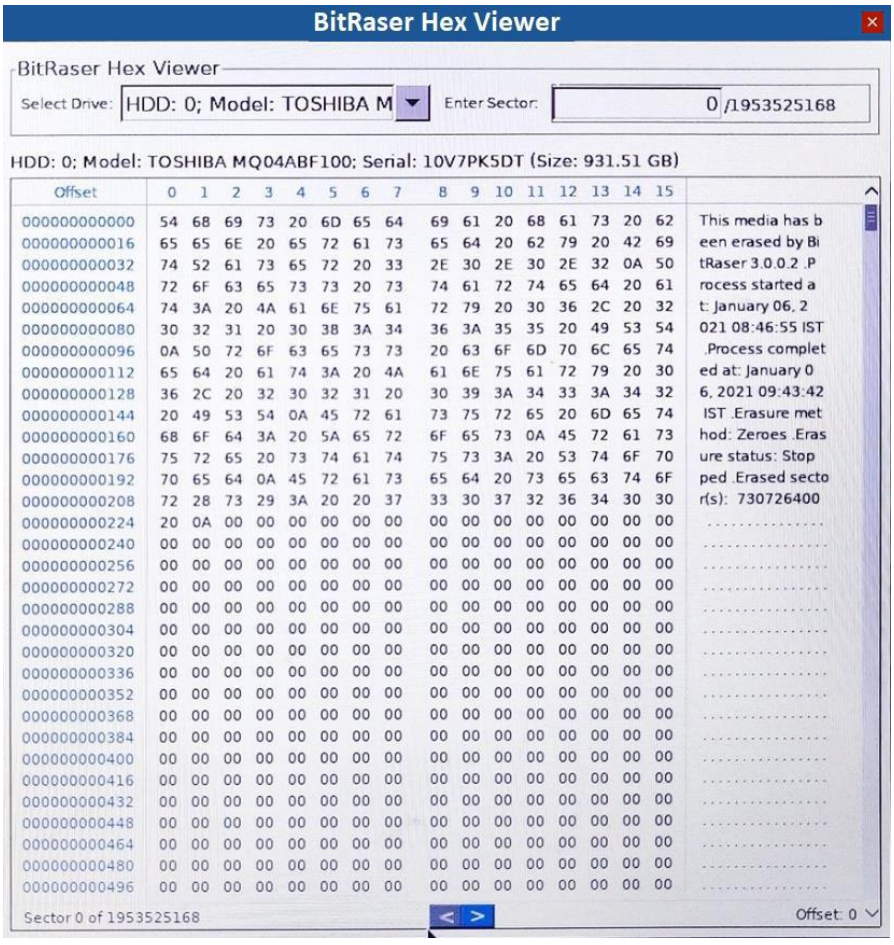
The **Hex Viewer** of **BitRaser Drive Eraser** allows you to view the raw and exact content of the hard drive in **hexadecimal** format. Thus, helping you to confirm the erasure of your hard drive by viewing its contents after completing the erasure process.

The **Hex Viewer** of **BitRaser Drive Eraser** can be used to view the content of a hard drive before and after the erasure process.

Note: *The viewer will not be 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 Hew Viewer** window appears as shown below:



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 the 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 the data from a storage media device like a hard disk, USB drive and SD card. In its simplest form, a data-wiping algorithm overwrites the storage device 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 the data 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 100 hard drives for simultaneous erasure
   - Supports erasure of hard drives like PATA, SATA, SCSI, SAS, etc. SSDs (NVMe, ATA, SAS, etc.), USB drives, and SD cards
   - 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 BitRaser 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 BitRaser cloud with **BitRaser Server**. Both options are available for the users at the time of purchase. The major differences are listed as follows:

Sr. No.	Licenses on BitRaser Cloud	Licenses on BitRaser Lock Key
1.	Stores license information on BitRaser Server	Stores license information on a USB device
2.	Needs connection to internet and BitRaser Server while running the application	Needs the USB device to be connected physically and internet connection is not required
3.	Automatically delivers reports and certificates to BitRaser Cloud Console	Reports and certificates need to be saved on a USB device

4.	Cloud integration for user management	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 100 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 Use 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.

12. **Does BitRaser Drive Eraser support data erasure from a SED?**
    Yes, **BitRaser Drive Eraser** supports data erasure from a SED. You can also erase data from multiple SEDs at once using the software. Refer to Erasure Process for the SED for detailed information.

13. **What will happen if I proceed the erasure process with an incorrect password of a SED?**
    If you save and erase with an incorrect password of a SED, the software will not be able to get access to the drive; hence, it will lead to a failed erasure attempt.

14. **Can I start the erasure procedure for a SED again if an erasure attempt fails due to entering an incorrect password?**
    Yes, however, you will be required to reboot your device for another erasure attempt. Refer to Erasure Process for the SED for more information.

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.

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

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.

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