BitRaser Admin Console

User Guide for version 1.0.0.0

TABLE OF CONTENTS

1. GENERAL INFORMATION 1
   1.1. ABOUT BITRASER ADMIN CONSOLE 1
   1.2. ABOUT THE GUIDE 3
   1.3. CONTACT INFORMATION 3
2. GETTING STARTED 4
   2.1. SYSTEM REQUIREMENTS 4
   2.2. CREATE BOOTABLE MEDIA 4
   2.3. BOOT AND RUN BITRASER ADMIN CONSOLE 9
   2.4. BITRASER SERVER CONFIGURATION TO ADD LICENSE 13
   2.5. GETTING FAMILIAR WITH USER INTERFACE 23
   2.6. GENERAL SETTINGS 25
3. HOW TO 28
   3.1. PERFORM DRIVE ERASURE OPERATIONS 28
      3.1.1. BEGIN ERASURE PROCESS FROM SERVER SYSTEM 29
      3.1.2. BEGIN ERASURE PROCESS FROM CLIENT SYSTEM 36
   3.2. CONFIGURE DETAILS 60
      3.2.1. ENTER ERASURE DETAILS 60
      3.2.2. ENTER CUSTOM FIELDS 62
   3.3. WORK ON REPORT AND CERTIFICATE 64
      3.3.1. VIEW AND CUSTOMIZE REPORT 66
      3.3.2. SAVE REPORT 68
      3.3.3. EXPORT REPORT 70
      3.3.4. GENERATE AND SAVE CERTIFICATE 71
      3.3.5. SEARCH REPORT 72
4. FREQUENTLY ASKED QUESTIONS 76
5. LEGAL NOTICE 79
6. ABOUT STELLAR 89

1. GENERAL INFORMATION

1.1. About BitRaser Admin Console

1.2. About the Guide

1.3. Contact Information

1.1. ABOUT BITRASER ADMIN CONSOLE

BitRaser Admin Console is a portable and highly reliable application that provides permanent data erasure for storage devices. This application erases data to prevent the recovery of sensitive data that is no longer required. Many refurbishers, organizations, and users, while formatting their drives, still find the possibility of data being recovered. **BitRaser Admin Console** 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 results of the process. The report can be saved to a drive/external media or collected by the **BitRaser Admin Console**.

Key Features of BitRaser Admin Console:

- **Erase Multiple Machines:** Erase multiple machines through **BitRaser Admin Console**.
- **Permanent Data Erasure:** Securely and permanently erase sensitive data from drives.
- **Supports Multiple Drive Types:** Supports the erasure of 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 26 world-class erasure methods, including NIST 800- 88 and IEEE 2883-2022 erasure standards.
- **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 drives for simultaneous erasure.
- **Support for RAID:** RAID dismantling is supported for MegaRAID and Adaptec cards.
- **Support to Erase Remapped Sectors**: Effectively erase drives containing remapped sectors.
- **Option to Locate a Drive:** While erasing multiple drives, the drive locate feature helps to locate the required drive 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 the **BitRaser Admin Console** application.
- **Option to View Drive Contents in Hexadecimal:** Provides a Hex Viewer on client side to view the drive's raw, exact content in hexadecimal format.
- **Reporting and Certification:**
    - Generate 100% secure and tamper-proof reports/certificates.
    - Option to customize the layout elements such as the top-right logo, header, and watermark based on specific requirements.
    - Option to add custom fields to the report as per requirements.
    - Option to add Technician/Validator signatures in reports/certificates.
    - Automatic report delivery to **BitRaser Admin Console**.
    - 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.
- **Multiple Options to Boot and Run**: Option to boot either using a USB flash drive (NAND-supported TLC/MLC) or Commercial SSDs.
- **Option to Change Keyboard Layout:** Supports a keyboard layout of your preferred language on the client side only.
- **No Expiry of License:** Pay per use – The licenses never expire.
- **Option to Transfer License:** Supports the transfer of the license from **BitRaser Hardware Lock Key** to **BitRaser Admin Console.**

1.2. ABOUT THE GUIDE

Welcome to the **BitRaser Admin Console** User Guide for version 1.0. Choose a topic from the **Table of Contents** to navigate through different topics that are in this guide.

This user guide contains sequential steps to assist you through various functions of **BitRaser Admin Console**. 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 (FAQs)
5. Legal Notice
6. About Stellar

This guide is intended for individuals who use **BitRaser Admin Console** to erase the storage of the devices to prevent recovery of sensitive data that is no longer required.

This guide is helpful if you are using **BitRaser Admin Console** application with license information on a USB lock key.

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

1.3. CONTACT INFORMATION

BitRaser Support

Our **Technical support** professionals will provide solutions for all your queries related to **BitRaser Admin Console.**

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

2. GETTING STARTED

2.1. System Requirements

2.2. Create Bootable Media

2.3. Boot and Run BitRaser Admin Console

2.4. BitRaser Server Configuration To Add License

2.5. Getting Familiar with User Interface

2.6. General Settings

2.1. SYSTEM REQUIREMENTS

Before installing **BitRaser Admin Console**, make sure your computer meets the following requirements.

Minimum Requirements:

- **Processor:** Intel i5 (10th Gen).
- **RAM:** 16 GB.
- **USB Type:** Commercial SSDs / NAND Flash TLC / MLC Minimum.
- **Network:** 100 Mbps / Gigabit LAN.
- **Display Resolution:** 1920 x 1080 / 1920 x 1200.

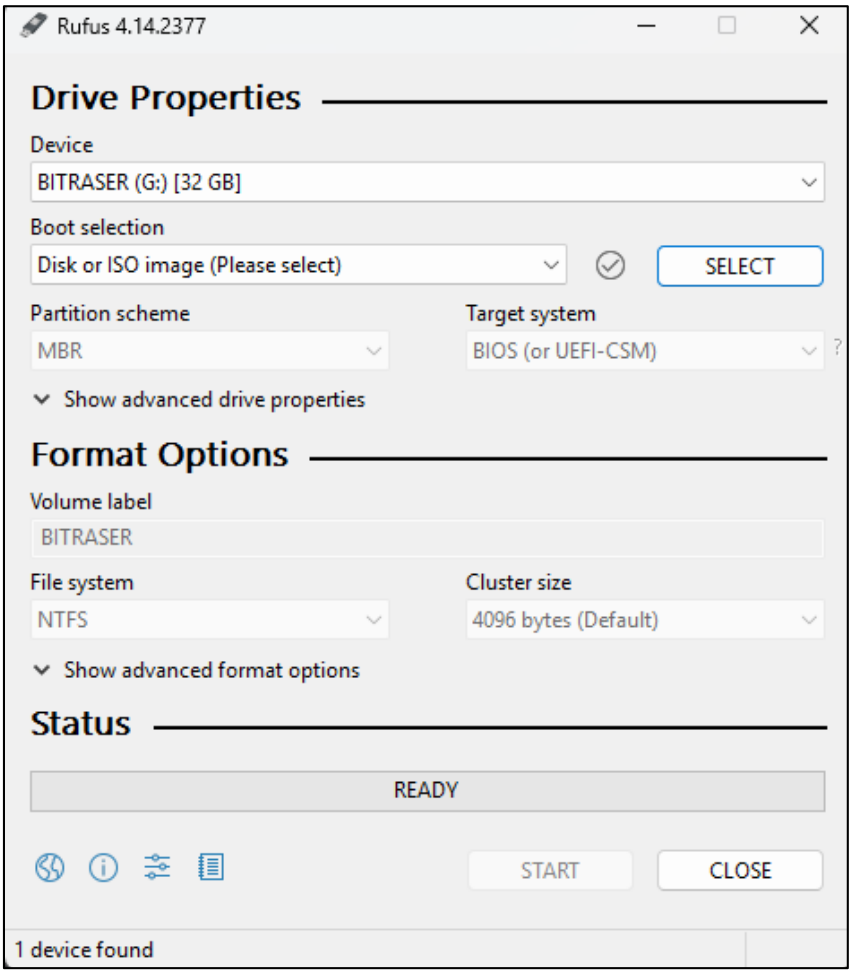
2.2. CREATE BOOTABLE MEDIA

To install and run **BitRaser Admin Console** smoothly, you have to install some supporting software given below:

To create bootable media, follow the steps below:

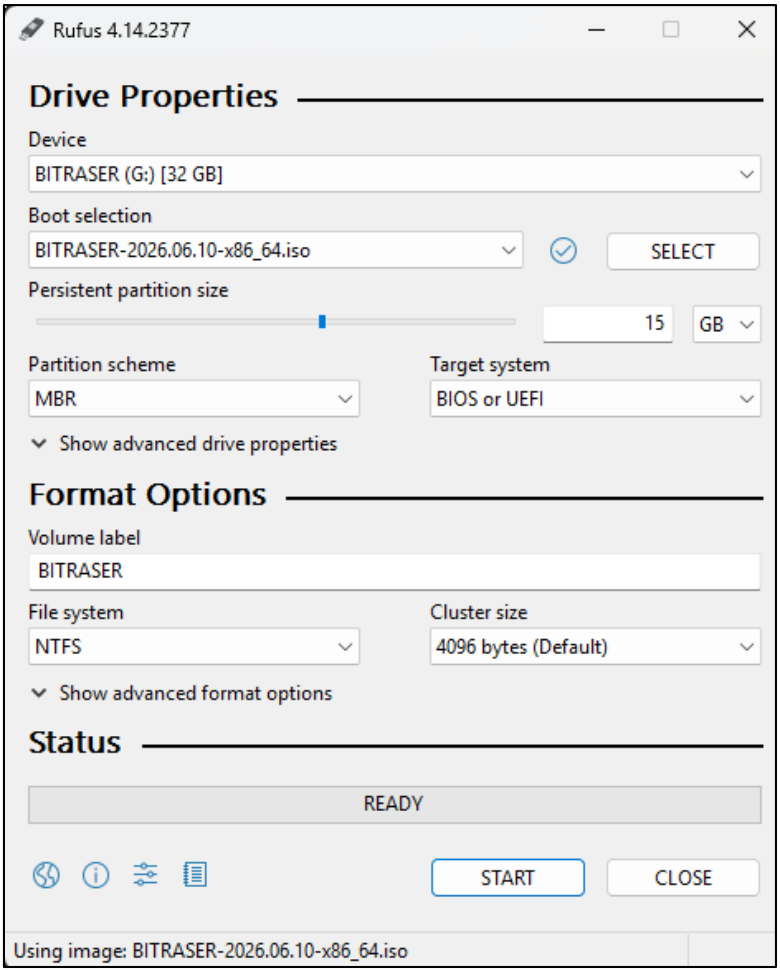
1. Download & install the latest version of Rufus if not present on your system.
2. Insert the NAND-supported USB flash drive or commercial SSD into the system.

3. Open Rufus; a screen appears shown below.



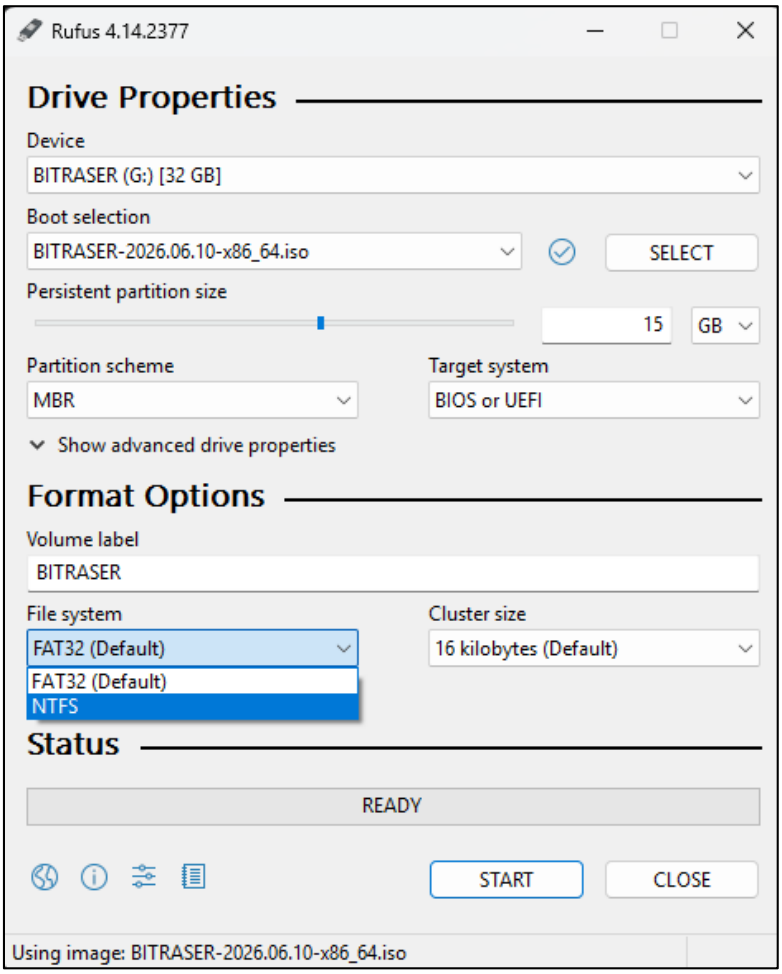
4. Click SELECT and select the BitRaser ISO provided with the software.

5. Select the partition size for the BitRaser ISO and the database by adjusting the **Persistent partition size**.

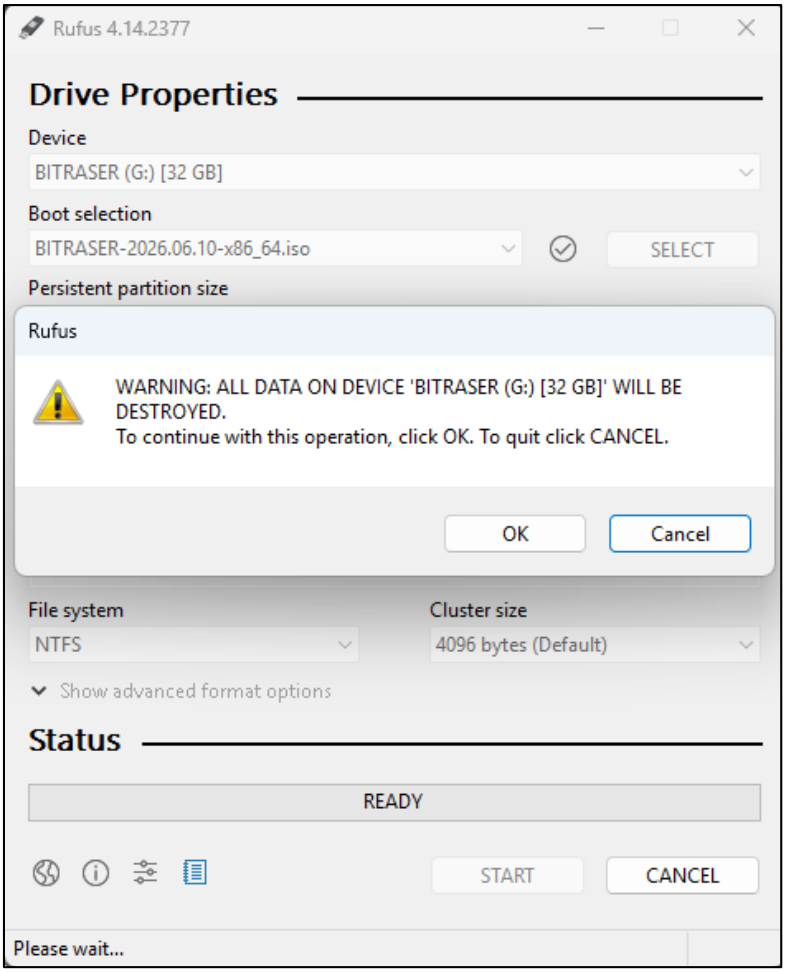


Note: *The minimum size for the database partition should be 15GB or 20GB in 32GB USB.*

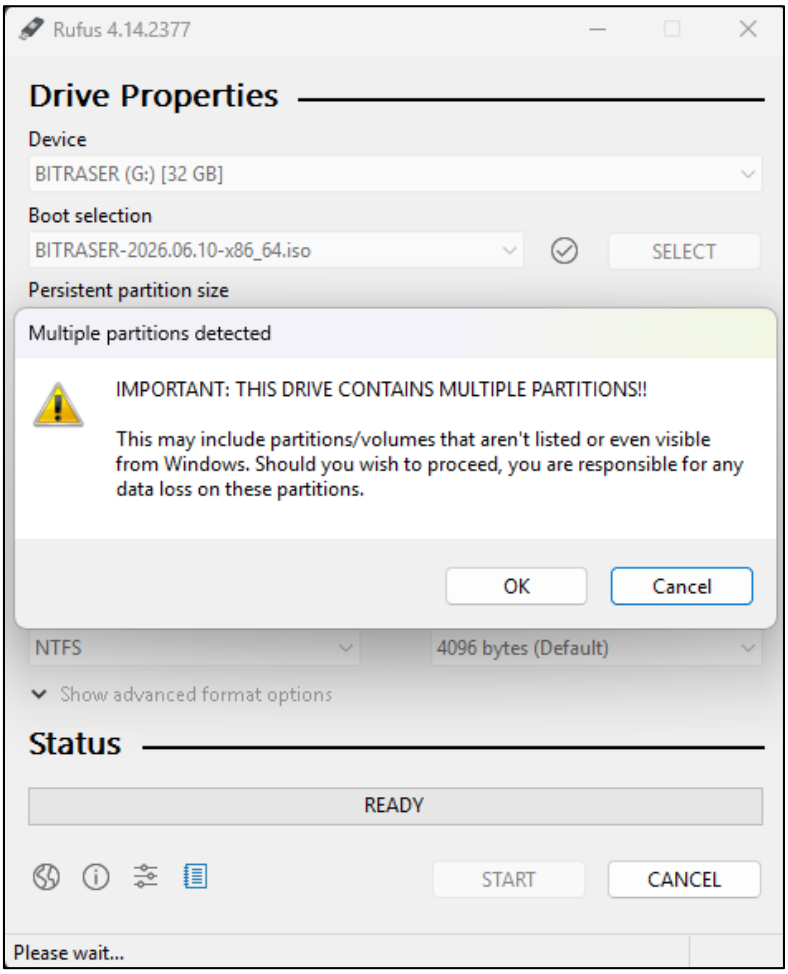
6. Change the File system from the **Format Options** to NTFS.



7. Click **Start**, a Rufus dialog box appears with a “WARNING: ALL DATA ON DEVICE ‘BITRASER (G;) [32 GB]’ WILL BE DESTROYED”.



8. Click **OK**. The **Multiple partitions detected** dialog box appears.



9. Click **OK** to start the process.

Notes:

- *The process can take 20 minutes or more to complete.*
- *Do not disconnect the storage device during the process.*

2.3. BOOT AND RUN BITRASER ADMIN CONSOLE

To Boot and run **BitRaser Admin Console** on your computer or laptop, you need to connect the bootable media to your device.

You can now run the **BitRaser Admin Console** on your computer directly from bootable media (NAND-supported USB flash drive or commercial SSD), following the steps below:

For the **BitRaser Admin Console** edition with licenses on a lock key (USB), you will receive a USB device called the BitRaser Lock Key for licenses when you purchase the software. Using the bootable media, you can boot and run **BitRaser Admin Console** following the steps given below:

Note: *The* ***BitRaser Admin Console*** *application boots and runs using the RAM of your computer, which means* ***BitRaser Admin Console*** *does not occupy space on your computer's drive. Also, it means that a single session of* ***BitRaser Admin Console*** *is only valid until your system reboots. Upon rebooting, you must boot and run* ***BitRaser Admin Console*** *again using the bootable media for another session.*

Steps to Boot and Run BitRaser Admin Console:

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

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

   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. This menu consists of the following options:

a) **BitRaser**: This is the default option to run **BitRaser Admin Console**. This option runs **BitRaser Admin Console** automatically in the most commonly used system configuration.

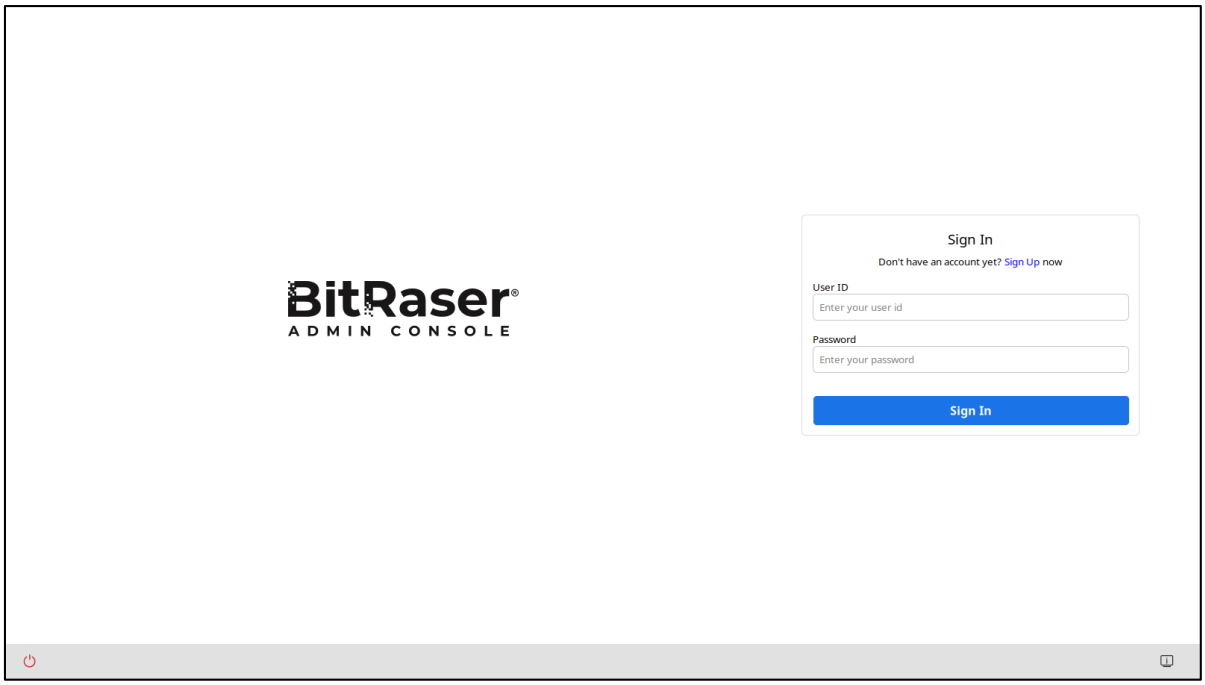
b) **BitRaser noflr:** This option uses NOFLR functionality and is mostly used if the **BitRaser Admin Console** fails to run using the first option.

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

Note: ***BitRaser Admin Console*** *automatically runs using the first option if there is no input from the user within 5 seconds. Use the arrow keys on your keyboard to cancel the action within 5 seconds.*

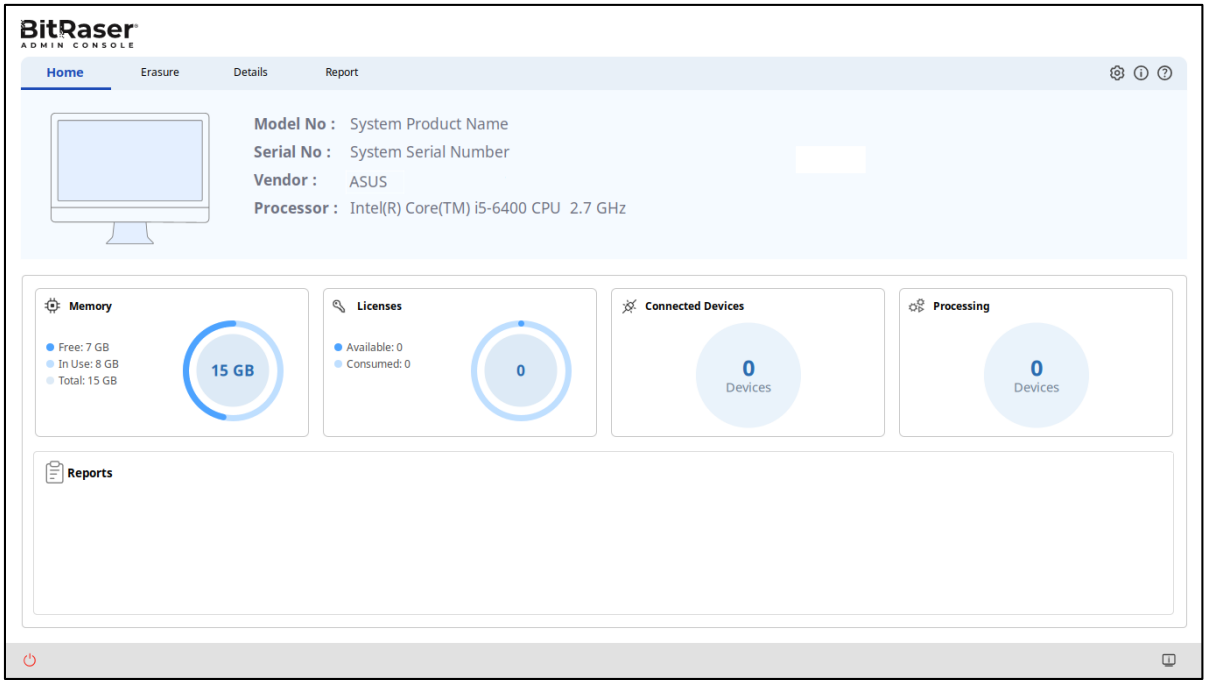
3. The **BitRaser Admin Console** now starts to boot and load from the bootable media. The following screen appears:

4. Once the system boot completes, it shows the **BitRaser Admin Console** running on the screen.



Note: *To know how to* ***Sign In,*** *click here.*

5. After Signing In, the main interface appears.



Warning: *Do not eject the bootable media directly once the device completes the boot process. To remove the bootable media, make sure to properly shut down the device, then remove the bootable media.*

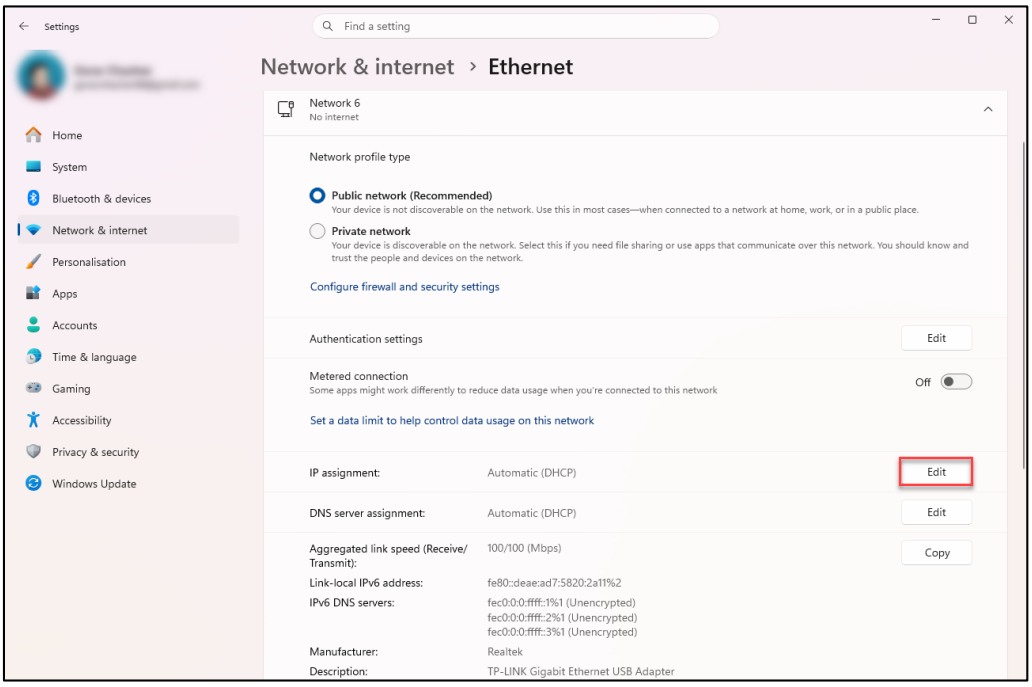
2.4. BITRASER SERVER CONFIGURATION TO ADD LICENSE

To install **BitRaser Hardware Lock Manager**, you have to set the IP range of your system that contains the operating system.

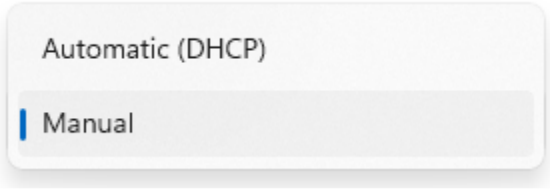
To set the IP range of your system, follow the steps below:

1. Open settings of your Computer or laptop.
2. Click **Network & Internet** settings and select **Ethernet**.

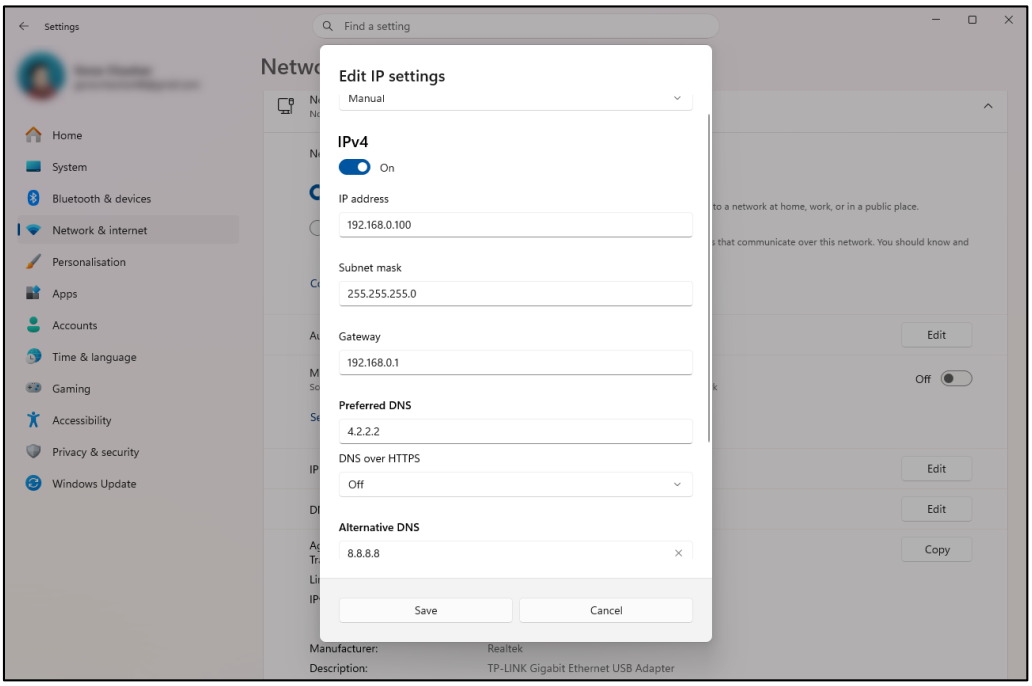
3. Click **Edit** button next to IP assignment.



4. Change IP assignment from Automatic to Manual.

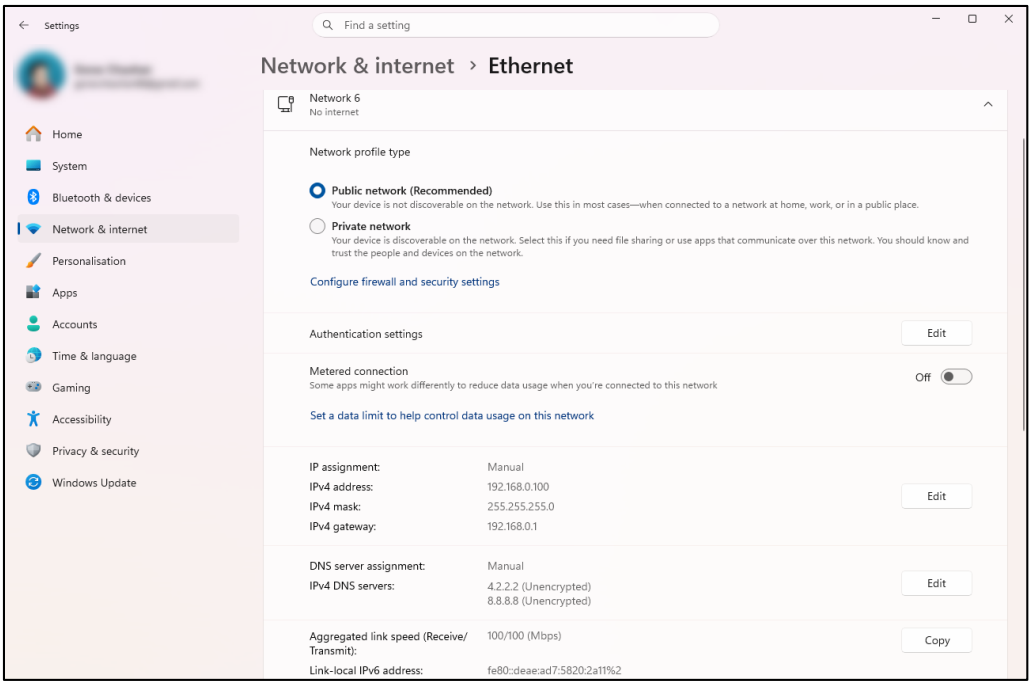


5. **Edit IP settings** screen appears. Add **IPv4** settings.



6. Set the IP range by entering the **IP address**, **Subnet mask**, and **Gateway**.
7. Click **Save**.

8. The details you entered will be displayed on the screen.



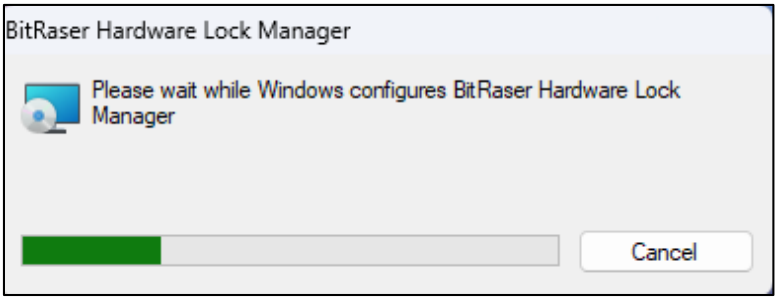
BitRaser Hardware Lock Manager

To install **BitRaser Hardware Lock Manager** after configuring the IP settings. Click here.

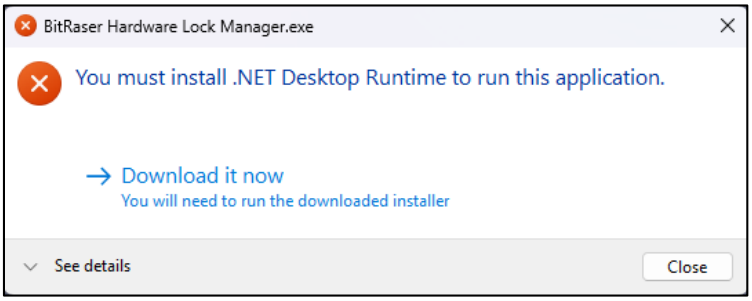
After you click on the link, **BitRaser Hardware Lock Manager** starts downloading in your default browser.

Steps to install BitRaser Hardware Lock Manager:

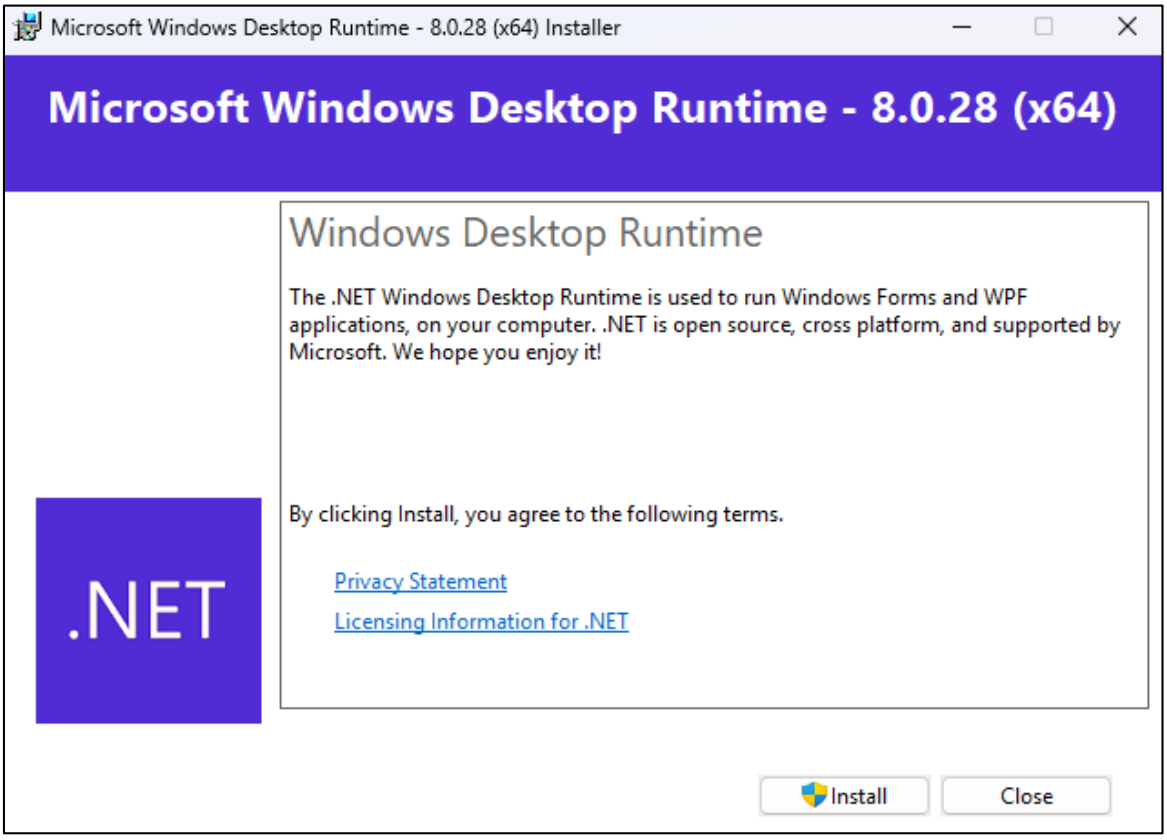
1. Once the download completes. Double-click on the downloaded file.



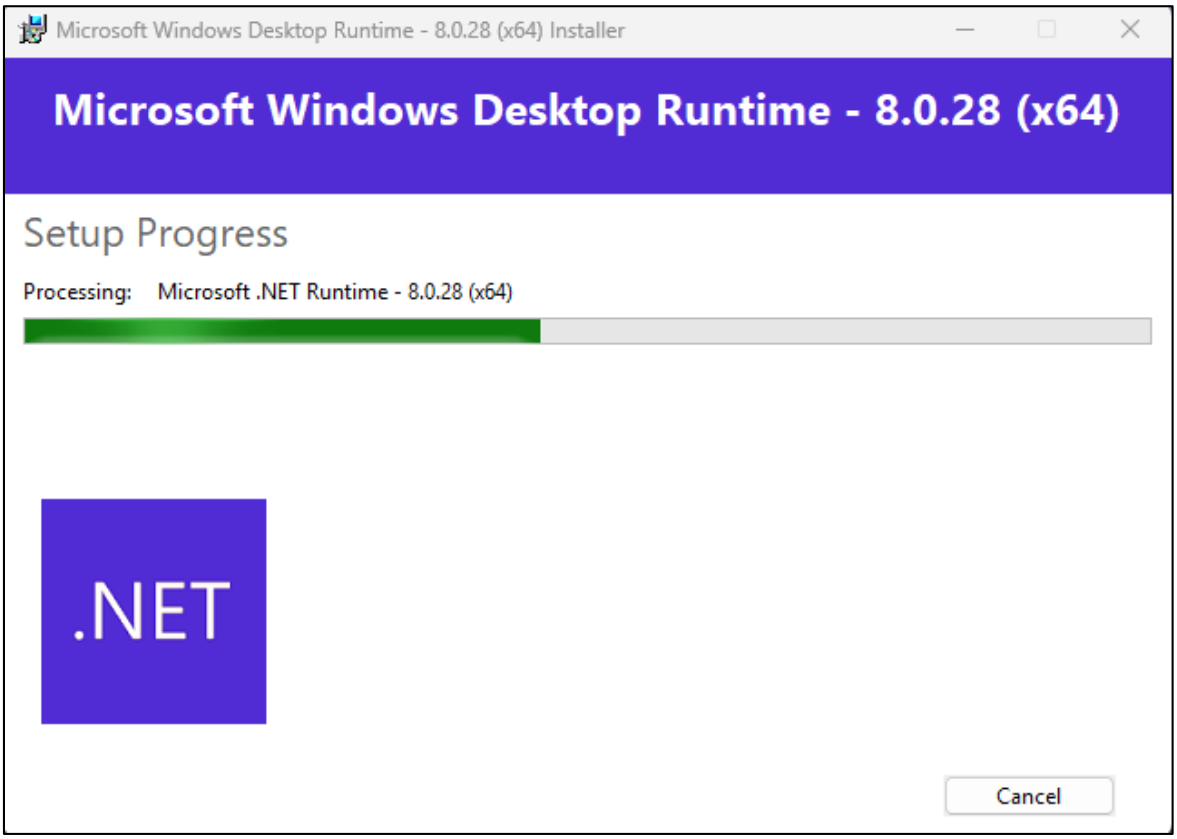
2. The **BitRaser Hardware Lock Manager.exe** dialog box appears with a download link.



3. Click **Download it now**. The .NET Desktop Runtime exe starts to download.
4. Double-click the downloaded **WindowsDesktop-runtime** exe file.
5. Microsoft Windows desktop Runtime – 8.0.28(x64) Installer screen appears. Click **Install**.



6. Installation starts.



Note: *Do not click* ***Cancel****. Otherwise, the process stops working.*

7. Once the process is completed, a screen appears with a message "**Installation was successful**". Click **Close**.

Transfer license from BitRaser Hardware Lock Manager:

To transfer license from BitRaser Lock Key to the **BitRaser Admin Console** server, you have to create an account.

Click here to create account on **BitRaser Admin Console** server.

Note:

- *The Lock Key provided with the software should be connected to the USB port of the operating system machine.*

- *To follow the further steps, BitRaser Admin Console server and the operating system machine should be connected through the LAN.*

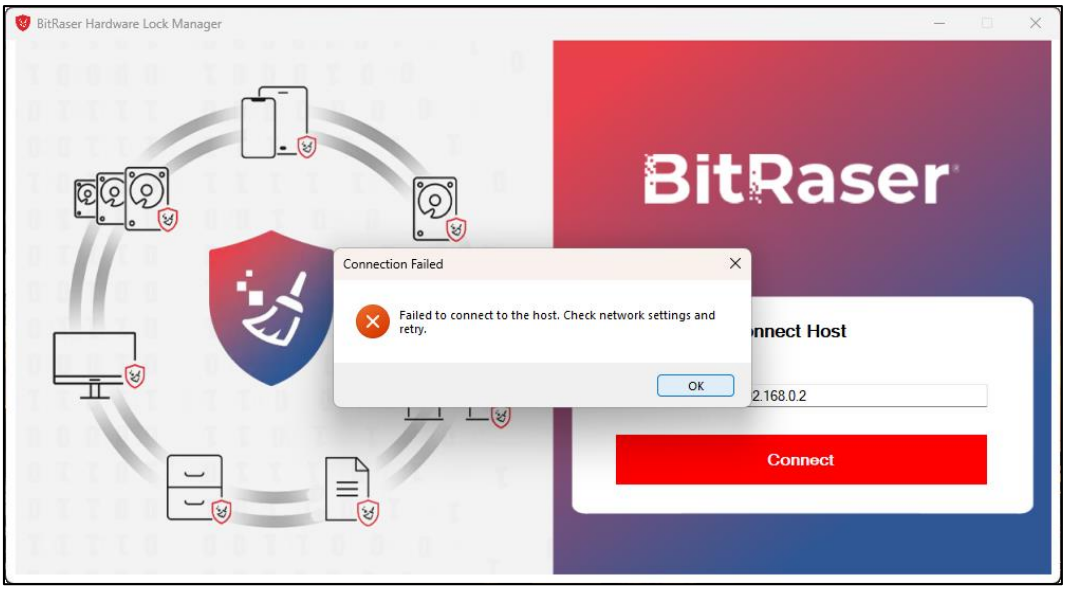
Steps to follow to transfer license:

1. Run BitRaser Hardware Lock Manager. **BitRaser Hardware Lock Manager** screen appears.

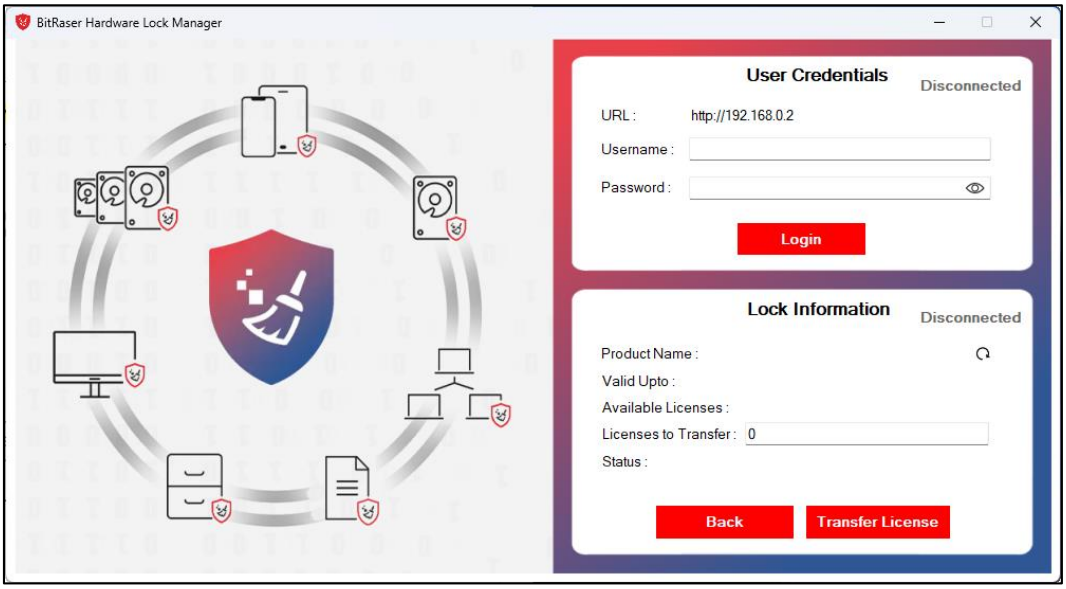
2. Enter the **Host URL**. Click **Connect**.

Notes:

- *The format for the host URL will be http://192.168.0.2.*
- *If the Host system is not working, check your LAN cables or reconnect them properly.*

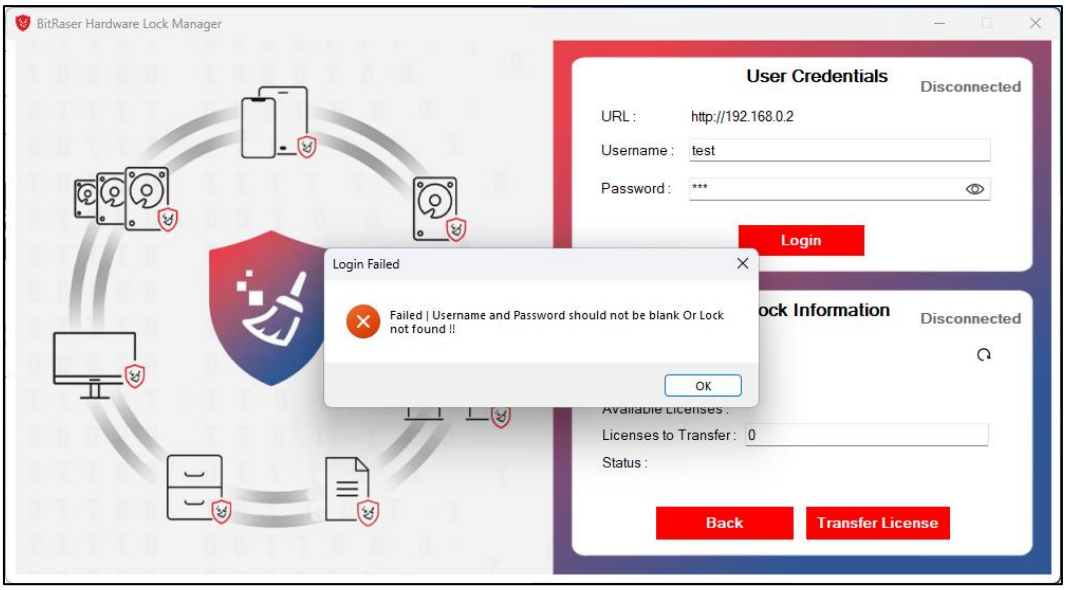


3. Enter the **Username** and **Password** you created while creating the account on **BitRaser Admin Console**. Click **Login.**



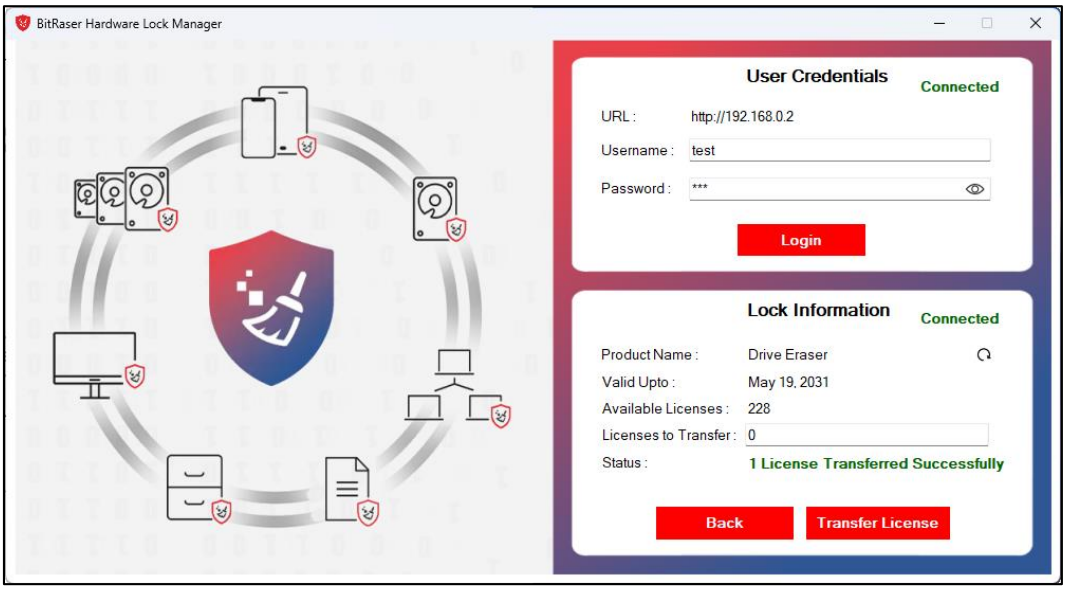
Note:

- *If you do not have the account, click Create Account.*
- *The **Login Failed** dialog box appears if the Lock key is not inserted properly into the USB port.*



4. The Host system is connected. Enter the number of licenses you wish to transfer in **Licenses to Transfer** text box.

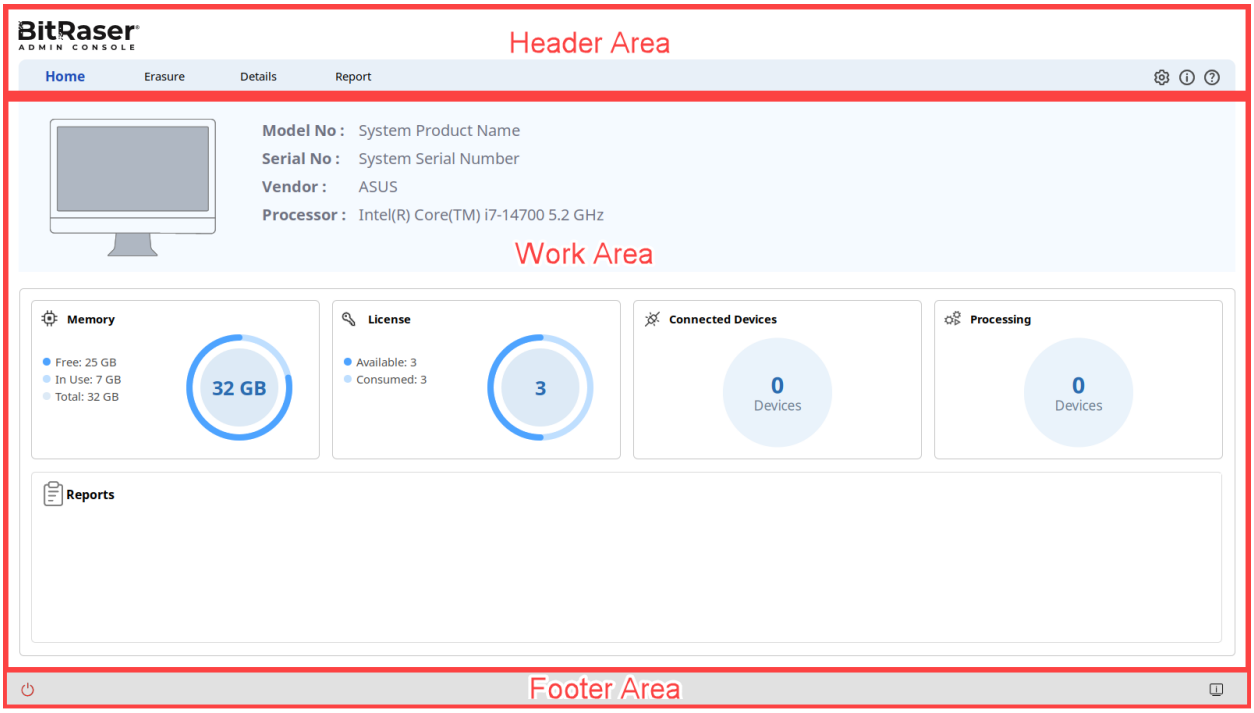
5. Click **Transfer License** button. It will show the status with the number of licenses transferred successfully.



2.5. GETTING FAMILIAR WITH USER INTERFACE

The User Interface is divided into three main areas:

- Header Area
- Work Area
- Footer Area

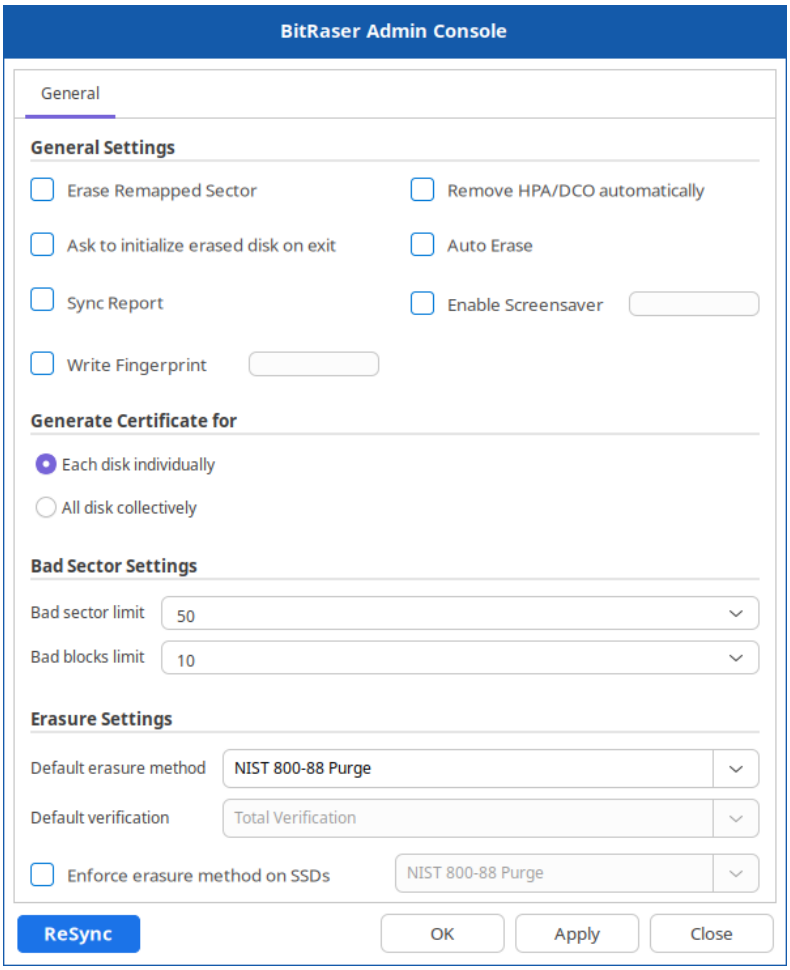


- **Header Area:** The header area contains the following tabs and buttons:
  - **Home tab:** This tab contains the details about the present status of Memory, Licenses, Connected Devices, and Processing.
  - **Erasure Tab** – This tab contains a list of the connected drives in a list view and is used to perform erasure process.
  - **Details Tab** – Click this tab to add **Custom Fields** and **Erasure Details**.
  - **Reports Tab** – This tab provides **BitRaser Admin Console** report and various options for **working on Reports**.
  - **Settings Button:** Click this button to update the various settings available for **BitRaser Admin Console**.
  - **About Button:** Click this button to see information about **BitRaser Admin Console** 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 the details about the present status of Memory, Licenses, Connected Devices, and Processing.
    - The Upper section of the work area consists of details about the server system, such as Model No. Serial No., Vendor, and Processor.
    - **Memory:** This card displays the free, in-use, and total memory of the system.
    - **License:** This card displays the Available and Consumed license information.
    - **Connected Devices:** This card displays the number of connected devices with the server.
    - **Processing:** This card displays the number of devices in process.
    - **Reports:** This section displays recent erasure reports.
- **Footer Area:** The Footer area contains the following buttons and information:
    - **Shutdown Button:** Click this button to shut down **BitRaser Admin Console**.
    - **Battery Information:** Hover over this icon to know the device's battery percentage.
    - **Processor Information:** Hover over this icon to learn about the device's RAM and Processor information.

2.6. GENERAL SETTINGS

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



The **General Settings** allow you to configure some very basic details that are needed during the erasure process, such as **General Settings, Generate Certificate for, Bad Sector Settings,** and **Erasure Settings**. The default settings can be set for the Erasure method and Data Erasure verification. Each section are/is described in detail below:

General Settings:

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

- **Remove HPA/DCO automatically** – Check this field to remove Host Protected Area (HPA)/Device Configuration Overlay (DCO) area of memory on a drive, which means this part of the drive will also be considered for data erasure.
- **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.
- **AutoErase** – After the client machine completes the boot process, it automatically connects to the server. The erasing process starts automatically after the connection is established.
- **Sync report**– On checking this field, the report will be updated at each percentage of the erasure process.
- **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 and 240 seconds after which the screensaver should start appearing.
- **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 Admin Console** 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 a certificate for a single drive or all the drives 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.

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.

- **Enforce erasure method on SSDs** – Check this field if you have SSD in your device, as certain erasure methods may not be compatible with SSDs.
    1. **Erasure Method** – Select the erasure method between NIST 800-88 Purge, IEEE 2883-2022 Purge, and BitRaser Secure & SSD Erasure.
    2. **Verification** - Total Verification method is set by default and cannot be changed.

    Note: *If the bootable media is accidentally ejected while the server is running, perform the following steps to prevent data corruption:*

    1. *Reinsert the bootable media into the server machine.*
    2. *Click the* ***ReSync*** *button to synchronize the bootable media.*

3. HOW TO

3.1. PERFORM DRIVE ERASURE OPERATIONS

3.2. CONFIGURE DETAILS

3.3. WORK ON REPORTS AND CERTIFICATES

3.1. PERFORM DRIVE ERASURE OPERATIONS

The **BitRaser Admin Console** lets you permanently erase data from multiple devices simultaneously. You have to follow the following procedure to erase data:

3.1.1. BEGIN ERASURE PROCESS FROM SERVER SYSTEM

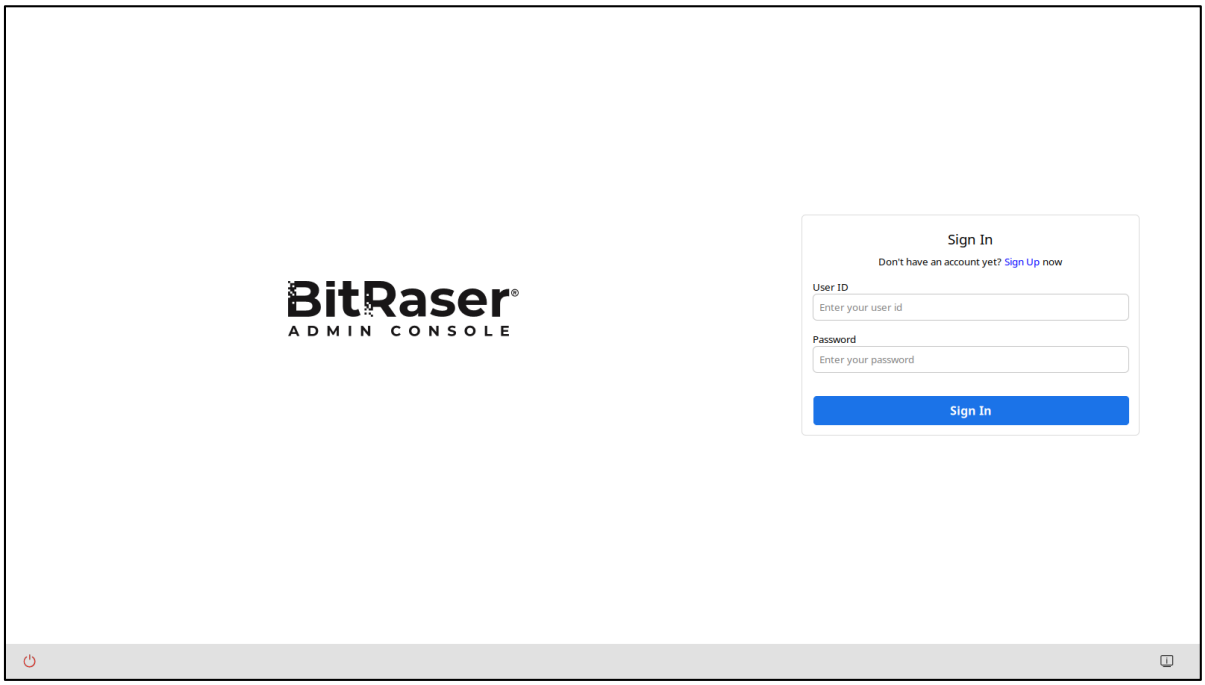
3.1.2. BEGIN ERASURE PROCESS FROM CLIENT SYSTEM

3.1.1. BEGIN ERASURE PROCESS FROM SERVER SYSTEM

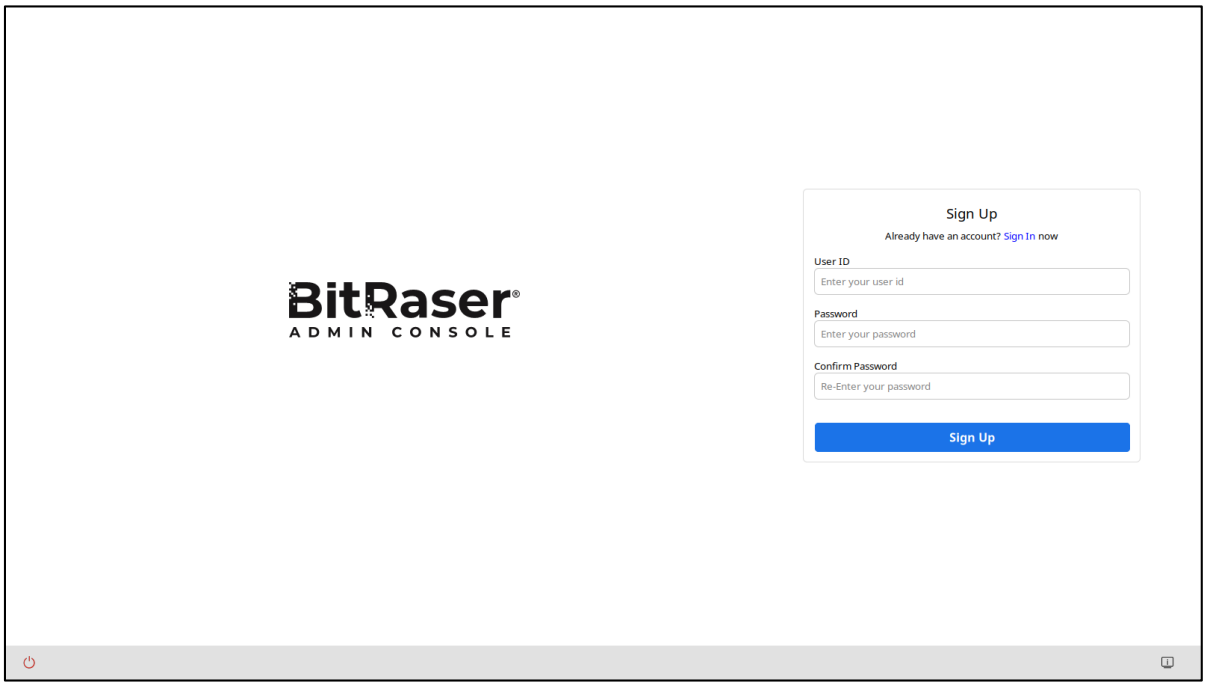
To erase data from the devices using **BitRaser Admin Console** through server system, follow the process below.

CREATE ACCOUNT

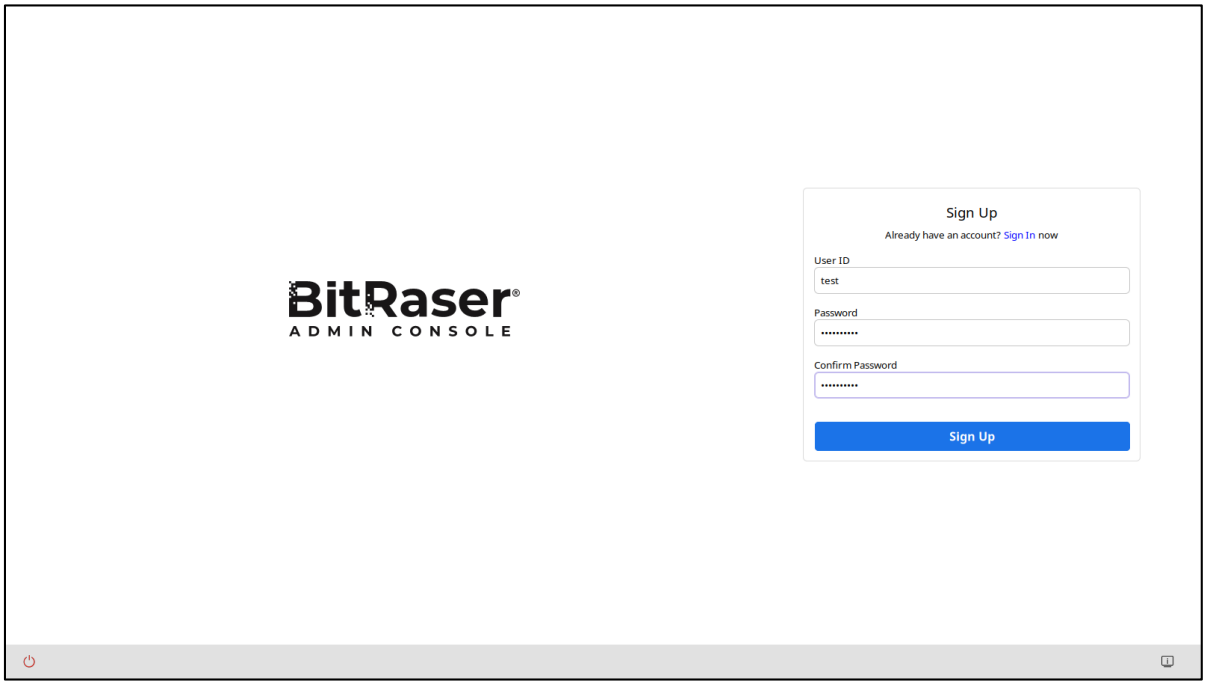
1. After the boot process completes, the **Sign In** screen appears.



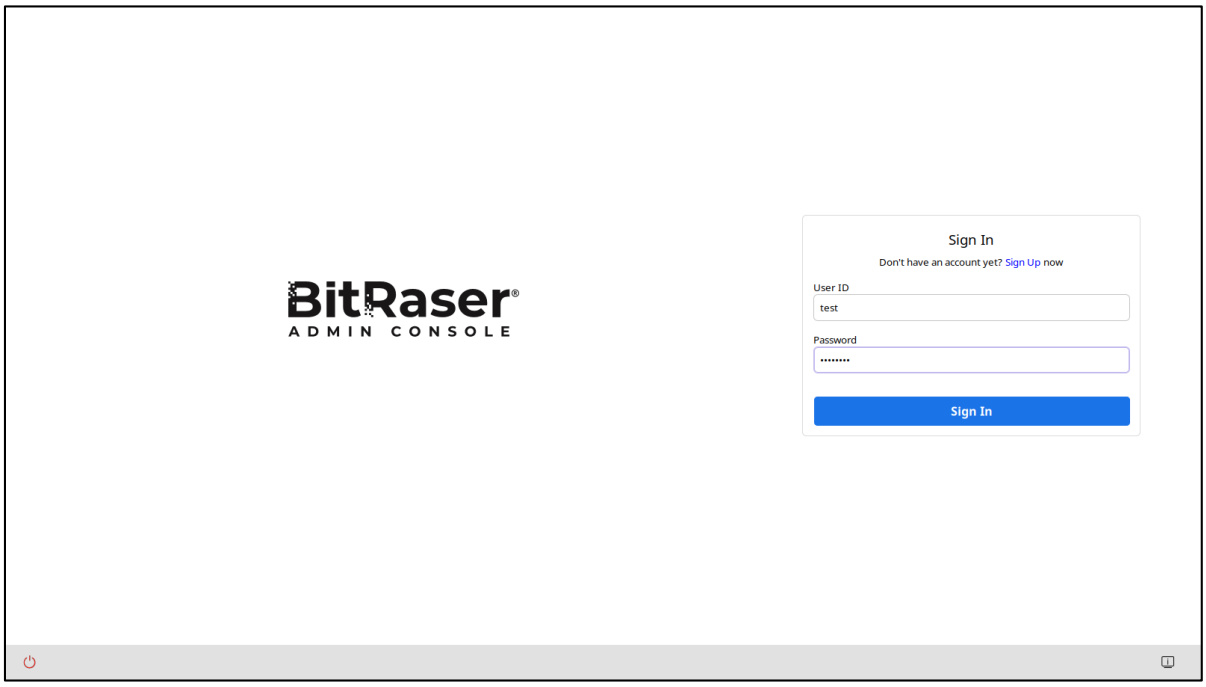
2. Click the **Sign Up** button to create an account first.



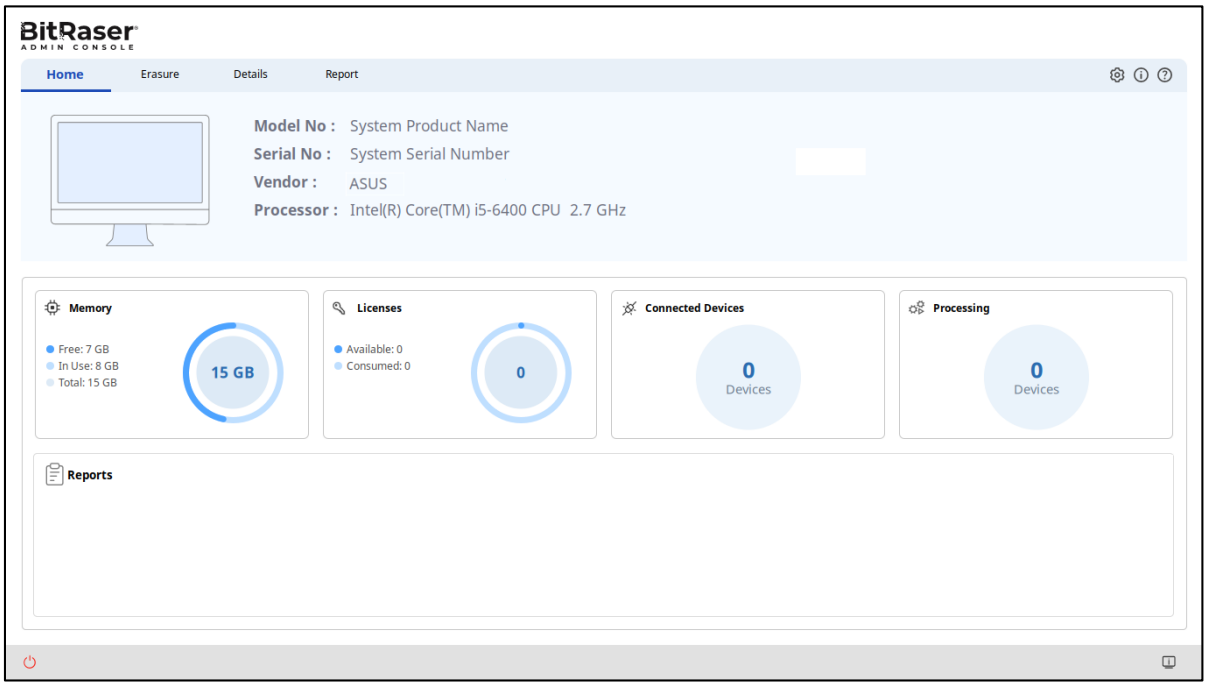
3. Fill in the details on the **Sign Up** screen for **User ID**, **Password**, and **Confirm Password**. Click **Sign Up**.



4. **Sign In** screen appears. Enter the **User ID** and **Password**. Click **Sign In**.

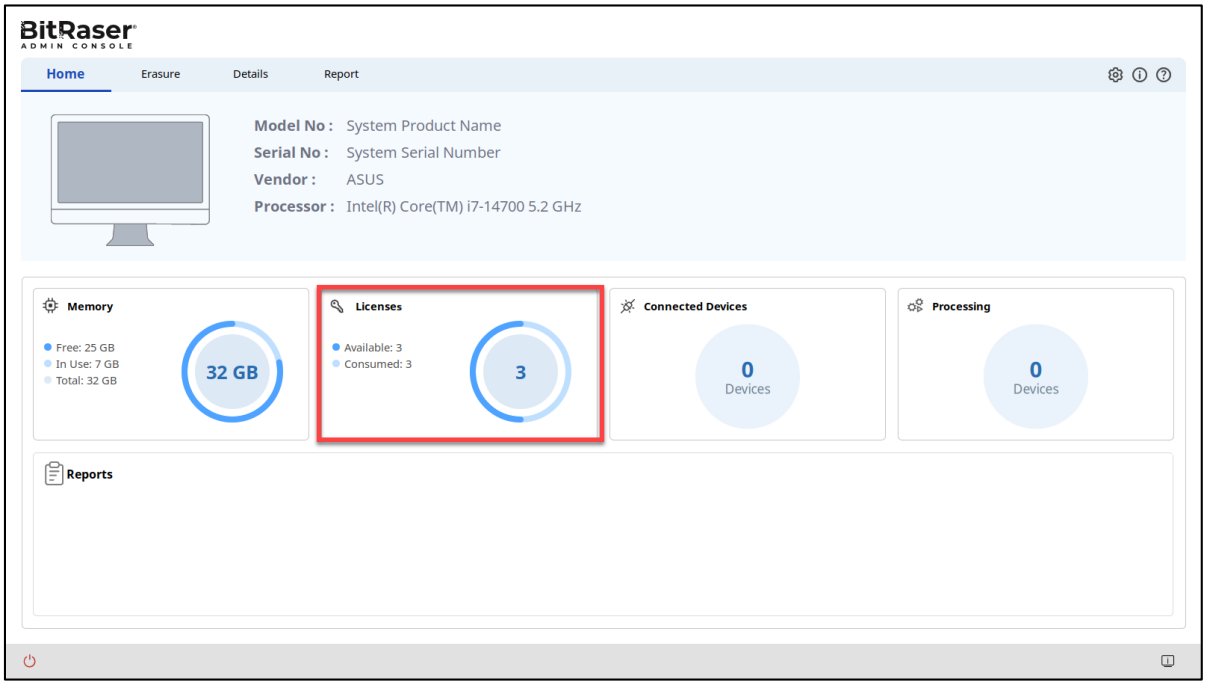


5. **BitRaser Admin Console** main screen appears.



Note: *Before starting the erasing process, add licenses to* ***BitRaser Admin Console.*** *To know how to add licenses, click here.*

6. After adding licenses to the **BitRaser Admin Console**, the total license count on the main screen will change from 0 to the number of licenses added.



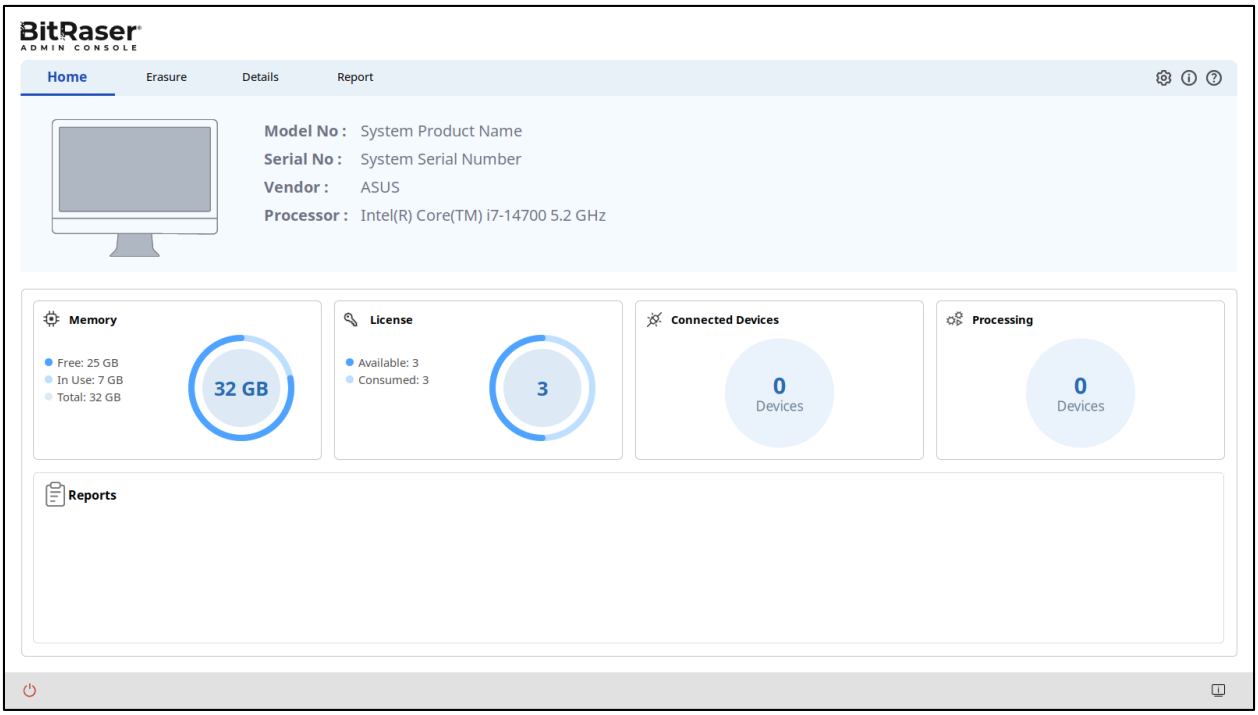
ERASING PROCESS

BitRaser Admin Console application allows you to securely erase data from the client machine drives by using various erasure methods available. There are **26** data erasure methods available to erase the data. Selection of erasure method is available under **Erasure Options** section. Also, there are verification options available to verify that the data has been erased permanently and is no longer recoverable.

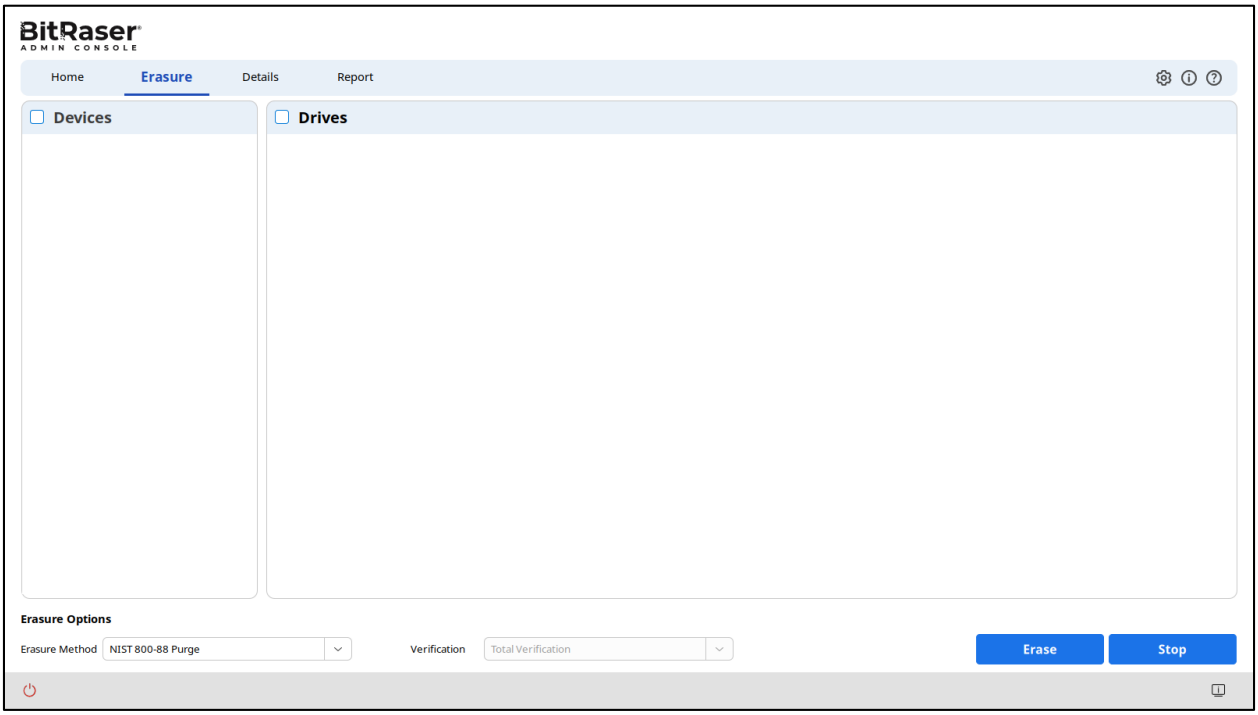
Note: *You can erase up to 100 drives simultaneously using* ***BitRaser Admin Console.***

Steps to erase data using BitRaser Admin Console:

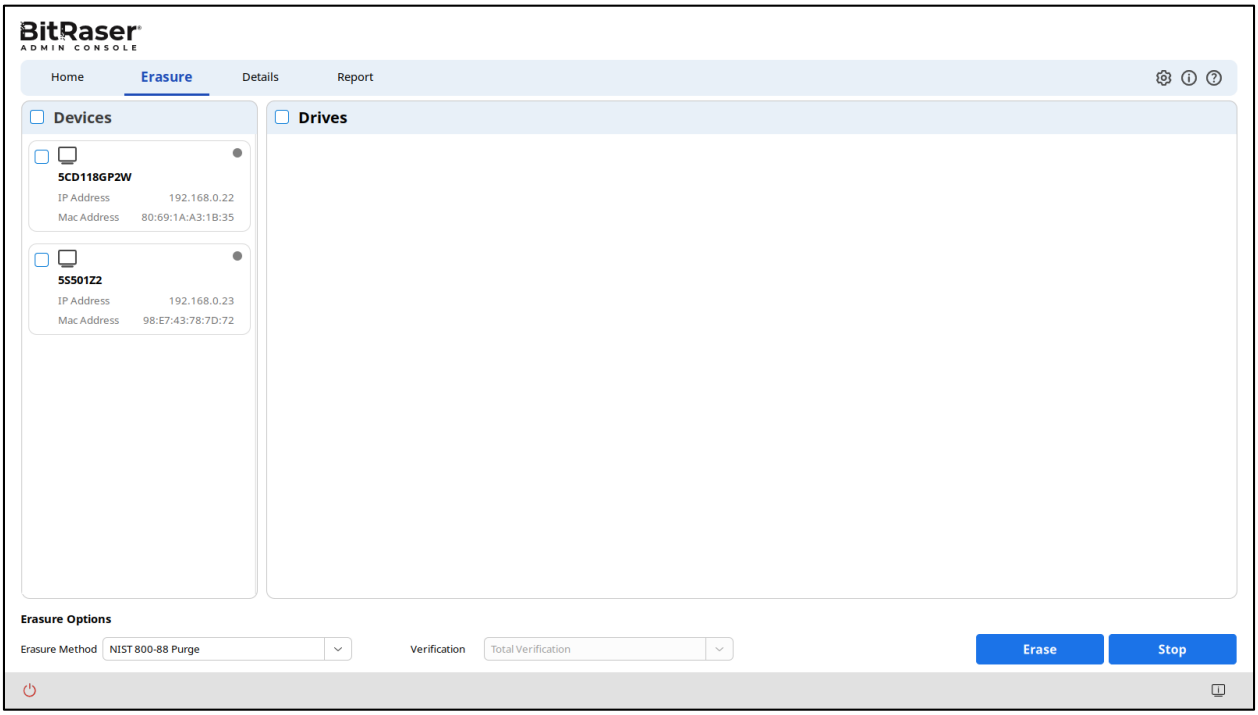
1. Run **BitRaser Admin Console** application. The screen appears, as shown below:



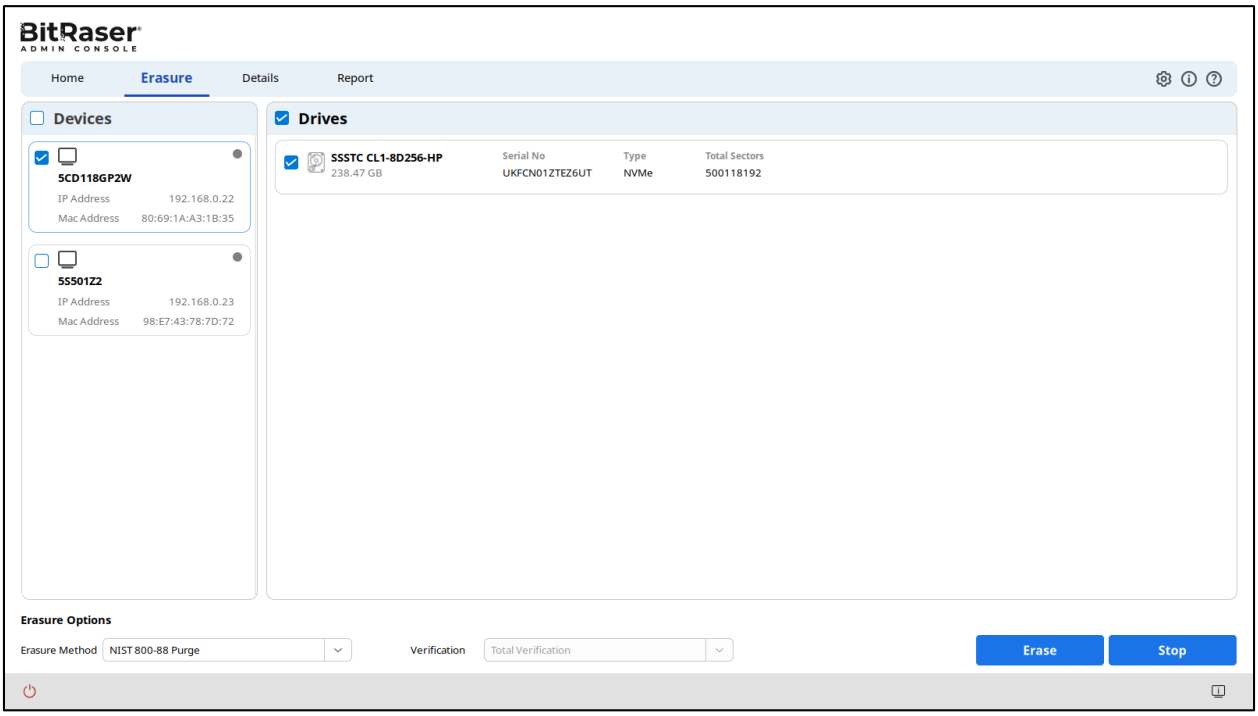
2. Click **Erasure** tab. The screen will appear.



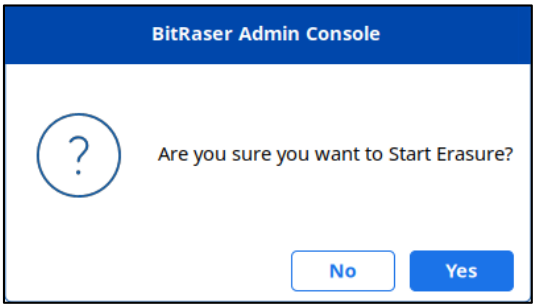
3. To list the client systems in the **Devices** pane, boot the client machines. Click here to know the steps.
4. Once the boot process completes, the devices will be listed in the **Devices** section.



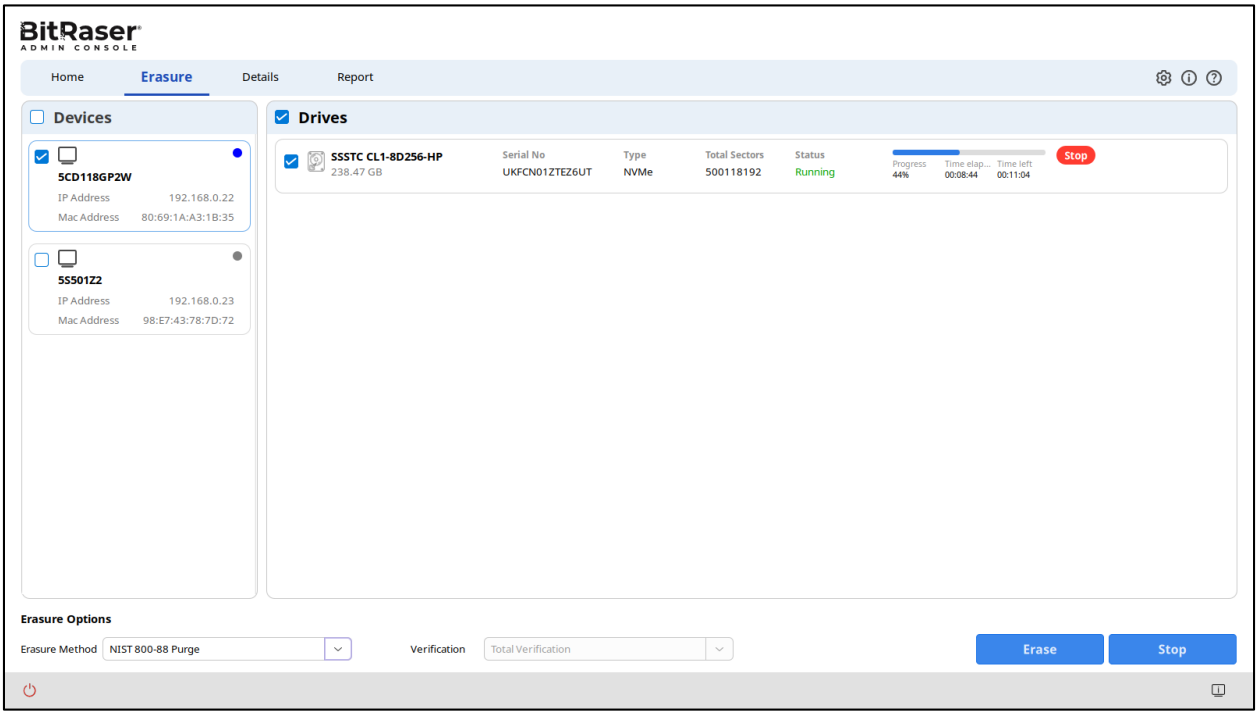
5. Select the devices/drives and click the **Erase** button to start the erasure process.



6. A dialog box appears with a message "**Are you sure want to Start Erasure?".** Click **Yes.**



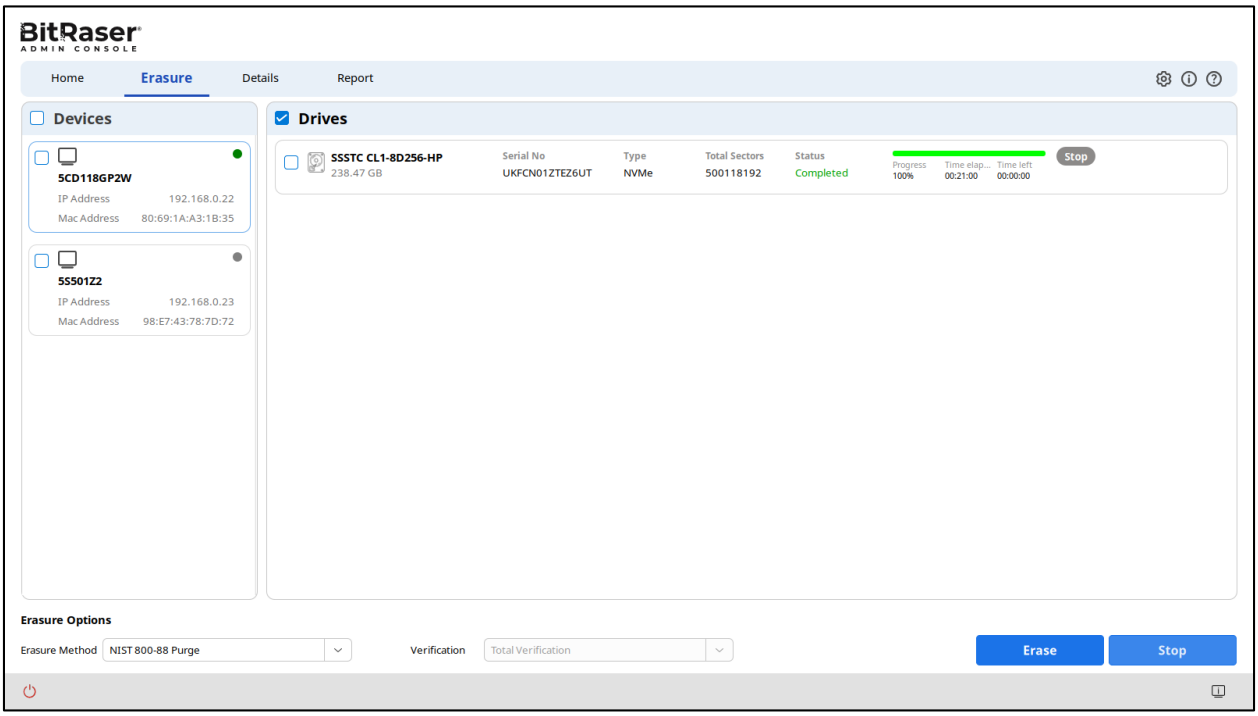
7. The erasure process starts.



Notes:

- ***To stop a single drive:*** *Click the* ***Stop*** *button next to the specific drive.*
- ***To stop all drives at the same time:*** *Select the checkbox next to* ***Devices/Drives,*** *then click the* ***Stop*** *button in the bottom right corner.*

8. The erasure process is completed.



Note: *You should save the report manually to an external drive on the server side at any state weather the process is running, stopped, or cancelled.*

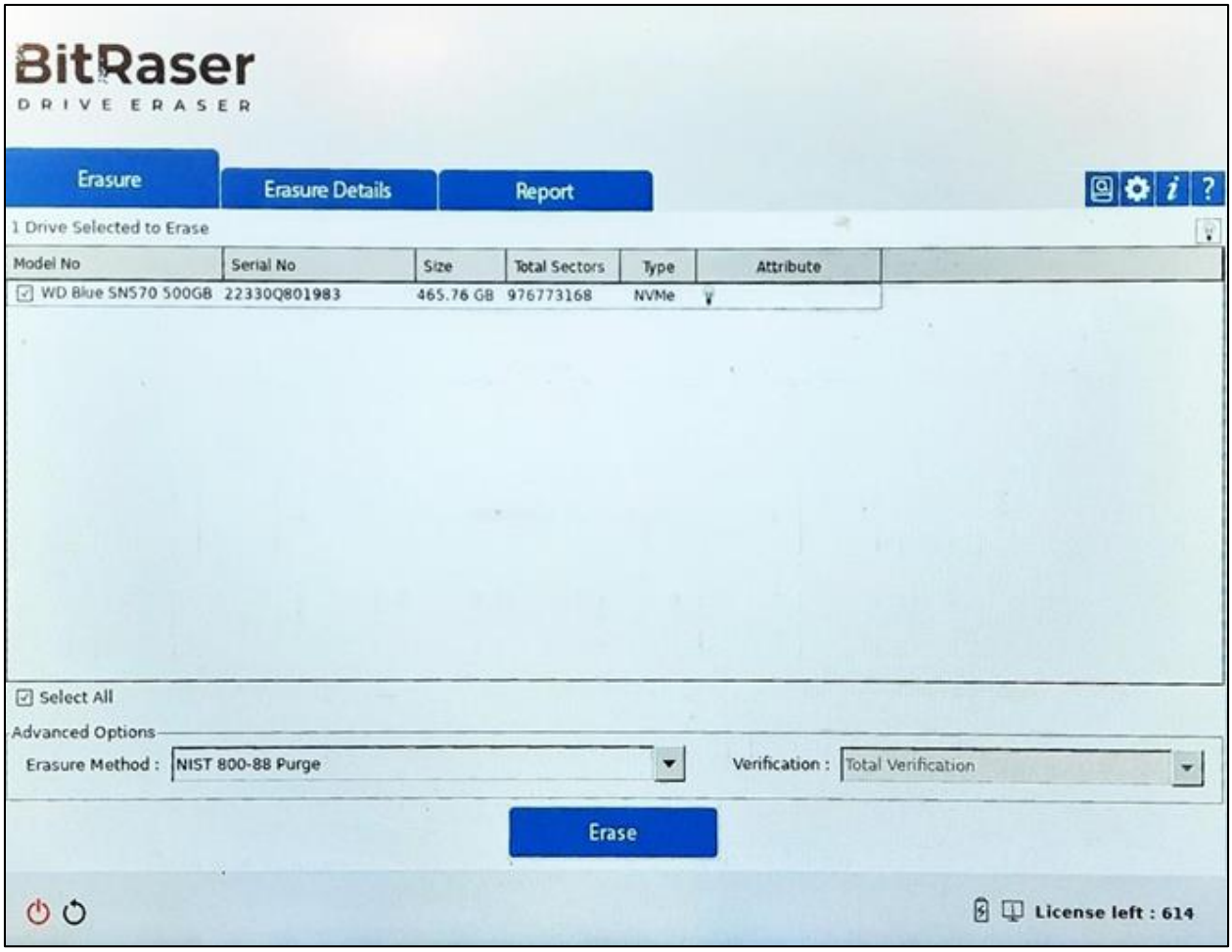
3.1.2. BEGIN ERASURE PROCESS FROM CLIENT SYSTEM

BitRaser Admin Console application allows you to securely erase data from client machine drives by using various erasure methods available. There are **26** data erasure methods available to erase the data. Selection of erasure method is available under **Erasure Options** section. Also, there are verification options available to verify that the data has been erased permanently and is no longer recoverable.

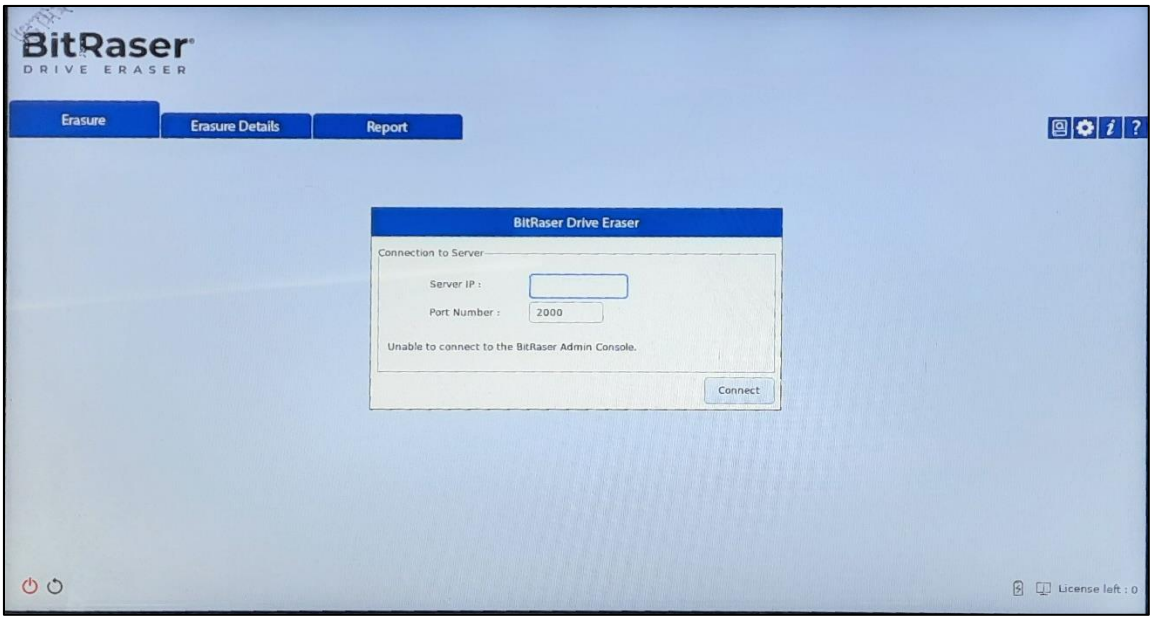
Note: *You can erase up to 100 drives simultaneously using* ***BitRaser Admin Console.***

To erase data using BitRaser Drive Eraser:

1. Switch on the client machine and enter its BIOS by pressing the required key; refer to your system manufacturer's user guide. In the BIOS, select the network booting option.
2. To know the further Booting steps, click here.
3. Run **BitRaser Drive Eraser** application. The screen appears as shown below:



Note: *If the server is not connected, a* ***BitRaser Drive Eraser*** *dialog box appears; enter the details manually (Server IP Address: 192.168.0.2, and port number). Click* ***Connect*** *button.*



4. All the 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.
5. If you have multiple drives, **BitRaser Drive Eraser** provides an option to locate the drive from the application. Click on in the Attribute column of the drive that you want to locate. Alternatively, click icon in top right corner of the screen to locate all the drives listed in the application. This illuminates the LED light (commonly known as activity indicator) on the drives to locate them easily.
6. All the storage devices are selected by default for erasure. Uncheck the storage devices that you do not want to erase.
7. From **Advanced Options** section, select any one of the following erasure methods as mentioned in the table.

Sr. No.	Erasure Methods	Description
1.	NIST 800-88 Purge	NIST 800-88 Purge is one among the media sanitization standards revealed by the National Institute of Standards and Technology. Purge involves physical or logical techniques that make Data recovery impossible, even though the advanced laboratory techniques. It involves overwrite, Block Erase, and Cryptographic Erase through dedicated, standardized device-sanitize commands that apply media-specific techniques to bypass the abstraction inherent in typical read and write commands.
2.	NIST 800- 88 Clear	This method overwrites data on user-addressable storage and the logical addressable location of a file with no sensitive data, using standard read-and-write commands.
3.	IEEE 2883-2022 Purge	IEEE 2883-2022 Purge is another media sanitization method outlined by the IEEE 2883:2022. Purge uses physical and/or logical techniques that render data recovery infeasible, even with state-of-the-art laboratory techniques. It includes commands like overwriting all addressable & non-addressable locations, Block Erase, and Cryptographic Erase.
4.	IEEE 2883-2022 Clear	This method uses logical techniques that work on every addressable storage location. The main goal is to protect the data from simple and non-invasive recovery methods.
5.	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.
6.	British HMG IS5 Baseline Standard	One Pass-Random Pattern.
7.	British HMG IS5 Enhanced Standard (3 passes)	This algorithm is a three pass overwriting algorithm: first pass with fixed value, second pass with its complement and the last pass with random data.

Sr. No.	Erasure Methods	Description
8.	B.Schneier's algorithm (7 passes)	This algorithm erases data in seven passes. In the first two passes, it overwrites the drive with fixed value and then its complement and in next five passes, it overwrites data with random characters.
9.	Canadian CSEC ITSG-06	This algorithm uses a combination of fixed value and its complement and random characters.
10.	German Standard, VSITR (7 passes)	This algorithm erases data by overwriting data with three alternating patterns of fixed value and its complement and then a last pass which overwrites with random characters.
11.	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.
12.	NAVSO P-5239-26 (3 passes)	This algorithm is a three pass overwriting algorithm: Pass 1: Writes a fixed value (e.g. one) Pass 2: Writes the complement of the fixed value (e.g. zero) Pass 3: Writes a random character and verifies the write.
13.	NCSC-TG-025 (3 passes)	This algorithm is a three pass overwriting algorithm: Pass 1: Writes a fixed value and verifies the write Pass 2: Writes a complement of fixed value and verifies the write Pass 3: Writes a random character and verifies the write
14.	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.

Sr. No.	Erasure Methods	Description
15.	Pseudo-random	This algorithm erases data by overwriting an entire hard drive with randomly generated numbers in a single pass.
16.	Pseudo-random & Zeroes (2 passes)	This algorithm erases data by overwriting the 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 zeroes.
17.	Pfitzner algorithm (33 passes)	The Pfitzner algorithm is used in file shredding and data destruction programs to overwrite existing information on a drive or other storage devices. All the passes in Pfitzner method consist entirely of random overwriting of data in the storage device.
18.	Peter Gutmann, (35 passes)	This algorithm erases data by overwriting it 35 times, making recovery of the erased data impossible with any tool. This algorithm takes more time than other wiping algorithms.
19.	Random Random Zero (6 passes)	This algorithm erases data by overwriting a storage media with random characters in multiple passes.
20.	Russian Standard - GOST-R-50739-95(2 passes)	This algorithm erases data by overwriting the drive with fixed values followed by a single pass of random characters.
21.	US Department of Defense, DoD 5220.22-M (3 passes)	This algorithm erases data by overwriting the drive in three passes. In first pass, it overwrites data with fixed value, then in second pass, it overwrites the data with its complement and finally in the third pass overwrites the data with randomly generated bytes. This is a U.S. Department of Defense algorithm.

Sr. No.	Erasure Methods	Description
22.	US Department of Defense, DoD 5220.22-M (ECE) (7 passes)	This algorithm erases data by overwriting the 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 fixed values, and third and seventh pass with random data. This is a U.S. Department of Defense algorithm.
23.	US Department of Defense, DoD 5200.28-STD (7 passes)	This algorithm erases data by overwriting the 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.
24.	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.
25.	US Air Force, AFSSI 5020 (3 passes)	This algorithm erases the data by overwriting the media in three passes. First, it overwrites with fixed value, then with its complement and finally with random characters.
26.	Zeroes	This algorithm erases data by overwriting it with fixed values in a single pass. This is the fastest algorithm available to a user.

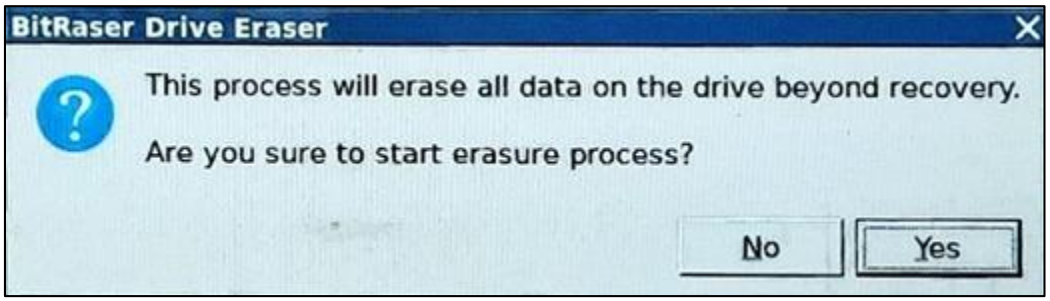
8. From **Advanced Options** section, select any one of the verification methods:

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 an SED, refer to the Erasure Process for SED Drive before proceeding.*

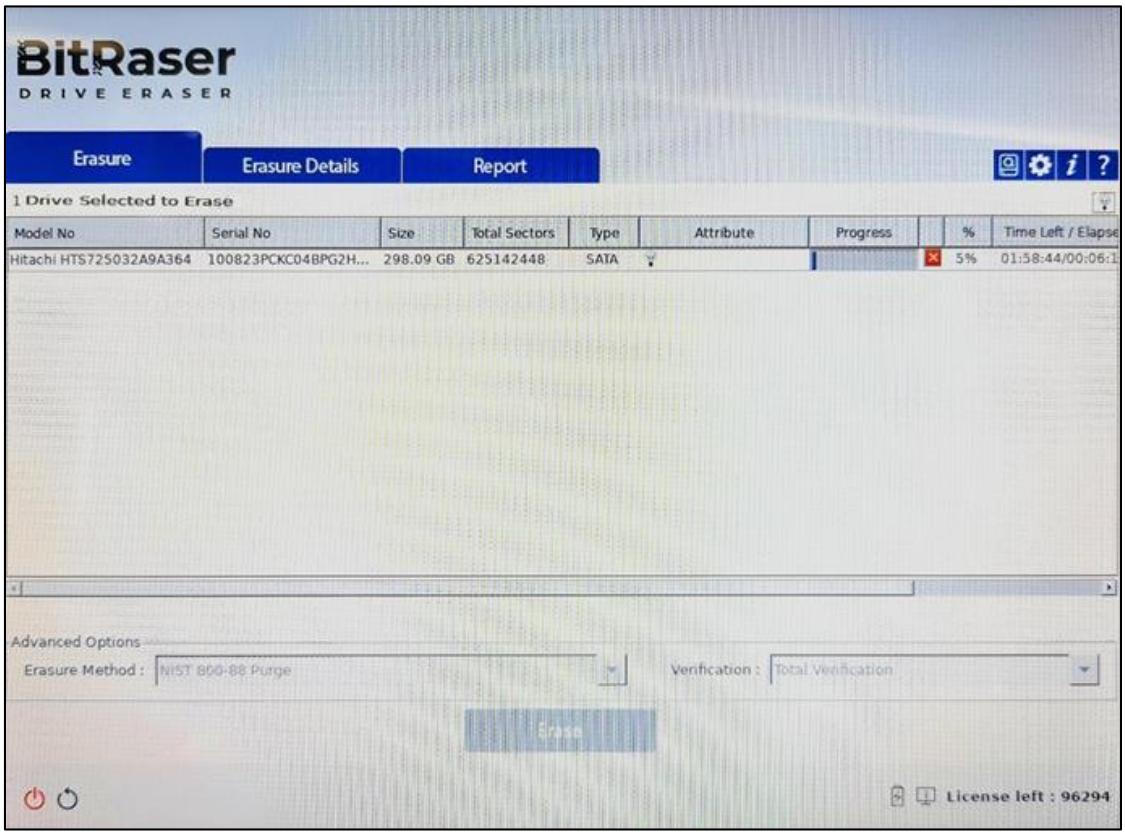
9. Click **Erase** to initiate the erasure process. The following screen appears:



10. 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 drives you have selected for erasure.*

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

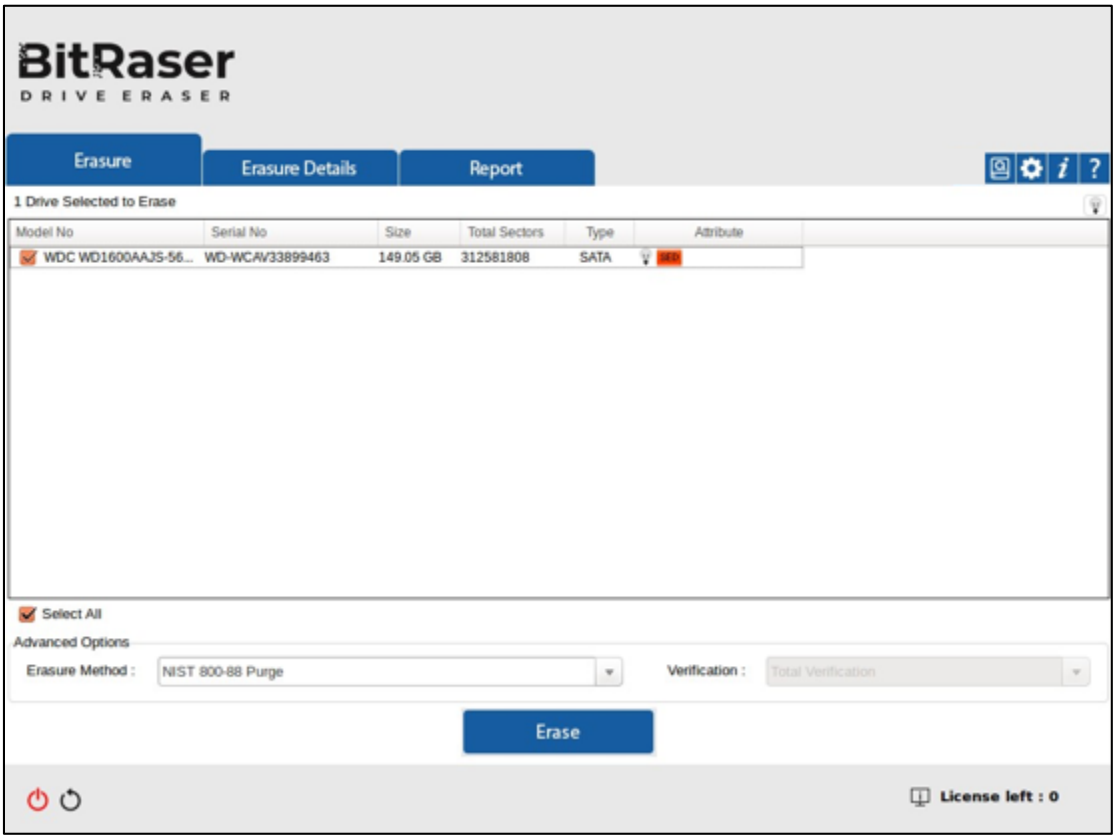


12. If you wish to cancel the erasure process, click on stop button next to the progress bar

Note: *You can save the report manually to an external drive at any stage, whether the process is running, stopped, or cancelled.*

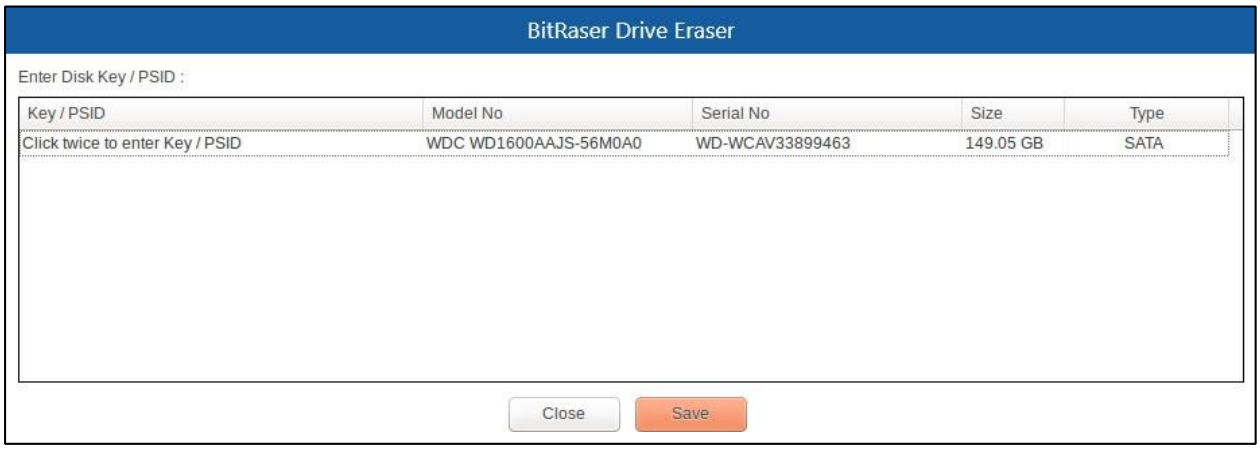
Erasure Process for the SED Drive

1. If your selected drive is an 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 to open the password window.

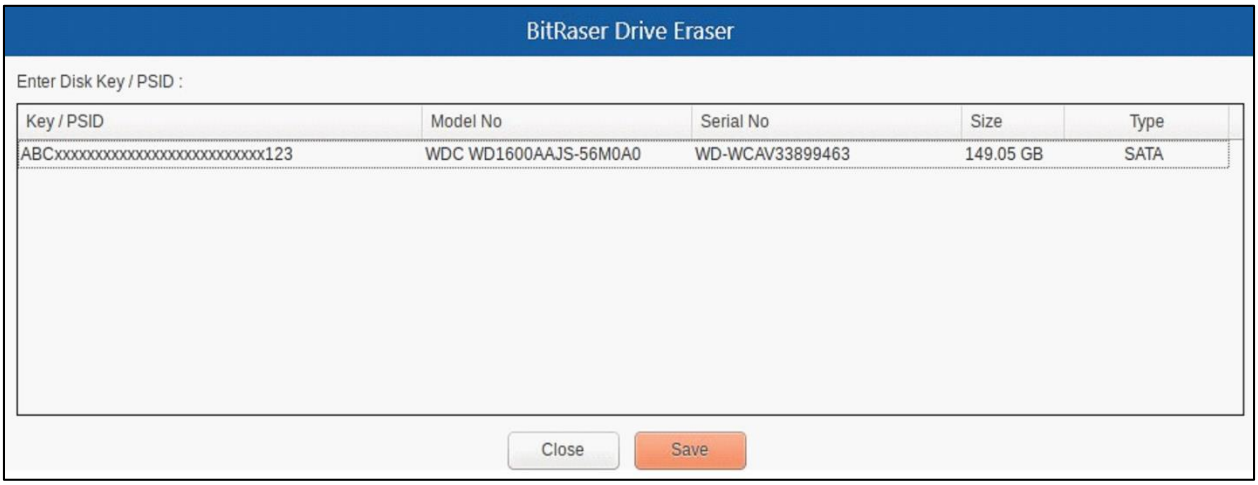


Note: *The* SED *Button is provided under the Attribute tab of the SEDs for their easy identification.*

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



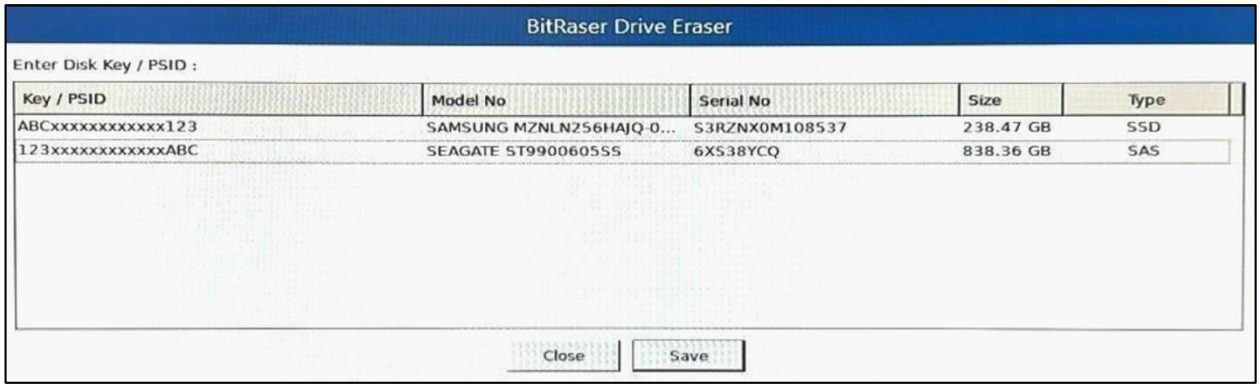
3. Enter the password or key in the text field.



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

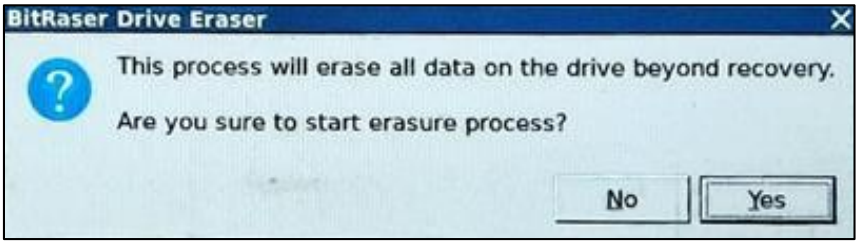
4. Click on **Save** button to proceed further.

   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.*



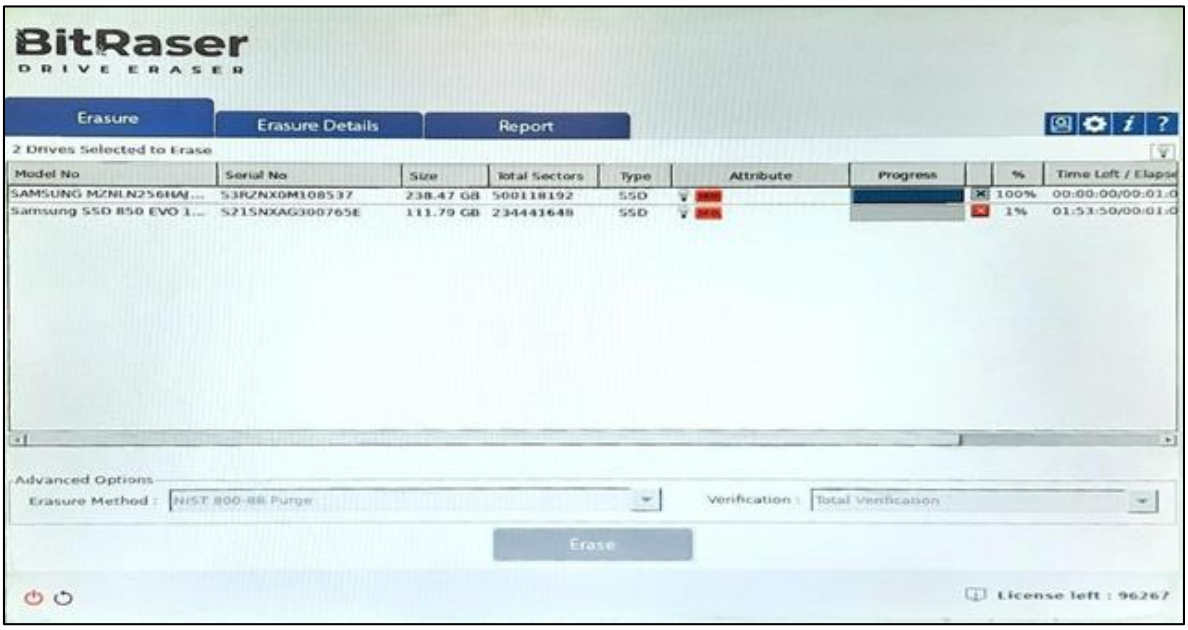
   Note: *It will lead to a failed erasure attempt if you save the wrong password for an SED, and you will be required to reboot your device for another attempt.*

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 drive during the process:



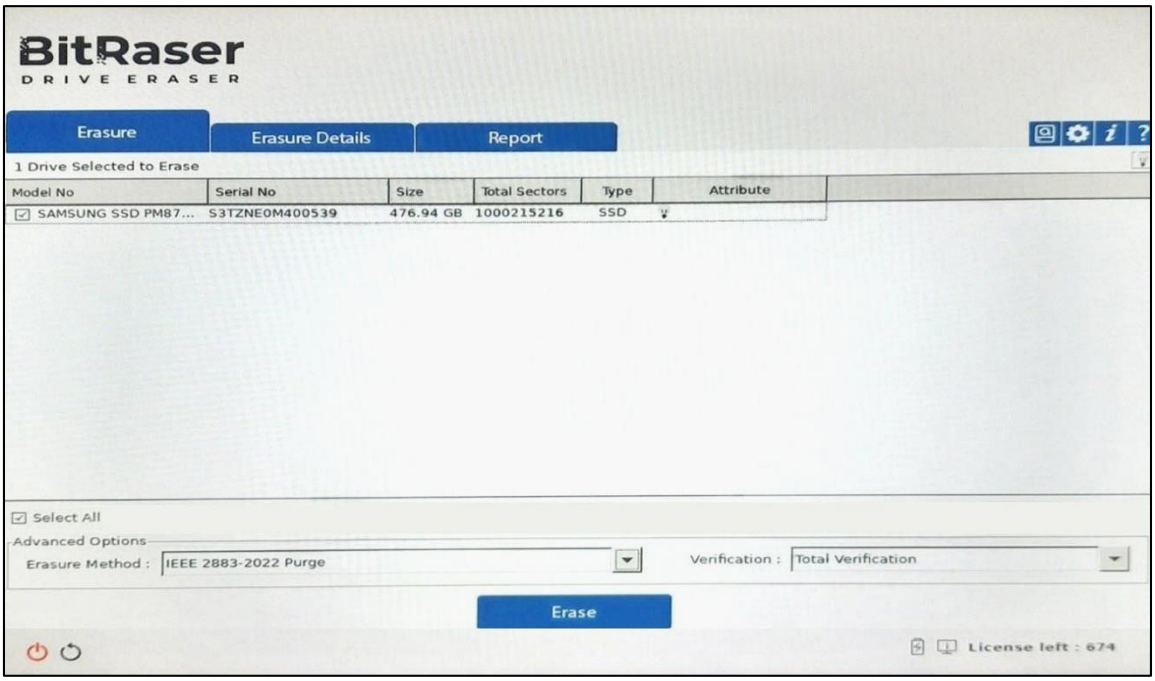
8. Rest of the erasure process remains the same for both SED and other drives. Therefore, follow up the process from here.

Erasure Process for TPM-Enabled Systems

Before proceeding with the **IEEE 2883-2022 Purge** or **IEEE 2883-2022 Clear** erasing method, you need to enable the TPM (Trusted Platform Module) chip in your system's BIOS settings and then clear the TPM. Once the TPM is cleared, you can easily erase the drive using these methods. The process for enabling TPM can vary depending on the manufacturer of your system. Therefore, you need to follow the required instructions to enable the TPM in your system.

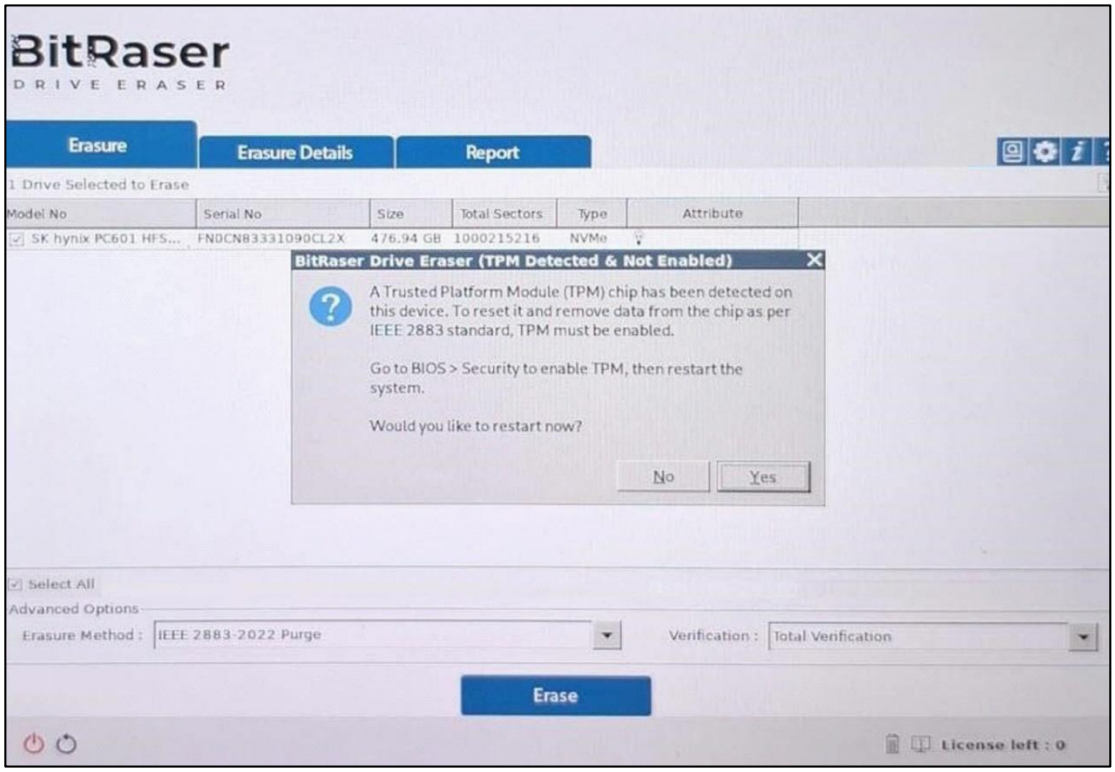
To enable the TPM, follow the steps:

1. Run **BitRaser Driver Eraser** application. The screen appears as shown below:



2. All the storage devices, along with their information such as model number, serial number, size, total sectors, type, and attributes, are displayed in the form of a list.
3. Select either **IEEE 2883-2022 Purge** or **IEEE 2883-2022 Clear** from the **Erasure Method** drop-down menu in the **Advanced Options** section under the **Erasure** tab, then click the **Erase** button.

4. The application automatically detects the TPM chip on your machine and displays the **BitRaser Drive Eraser (TPM Detected & Not Enabled)** dialog box on the screen.

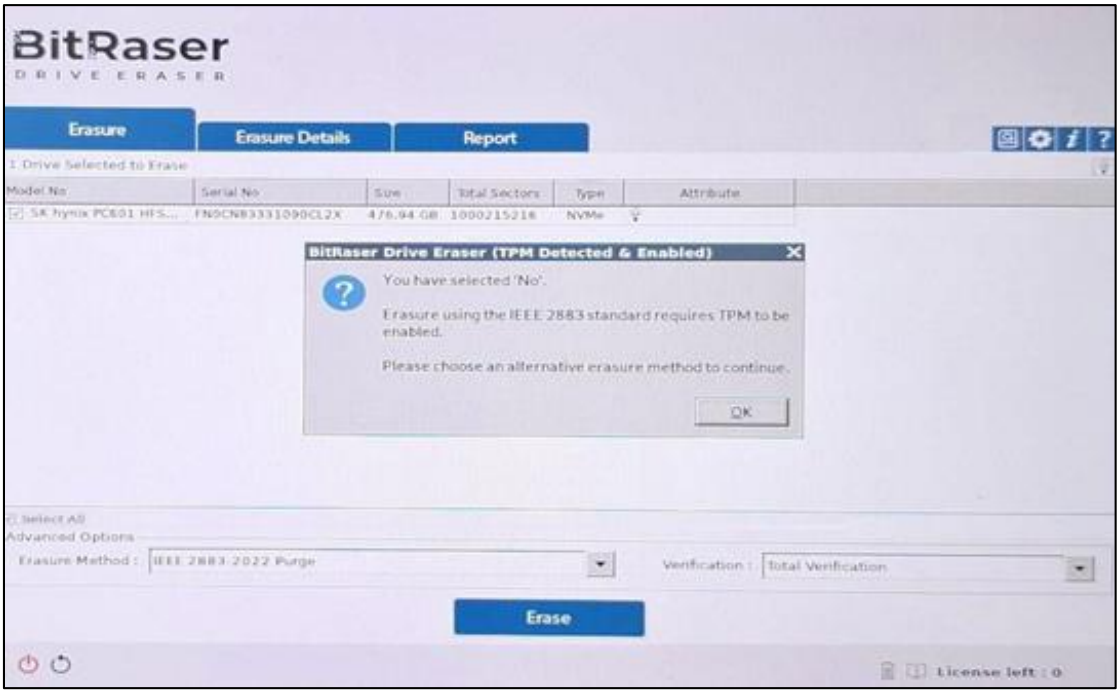


***Definition**: **TPM (Trusted Platform Module)** is a hardware security feature in BIOS that stores cryptographic keys and sensitive data securely. It helps with drive encryption, secure authentication, and system integrity checks.*

Note:

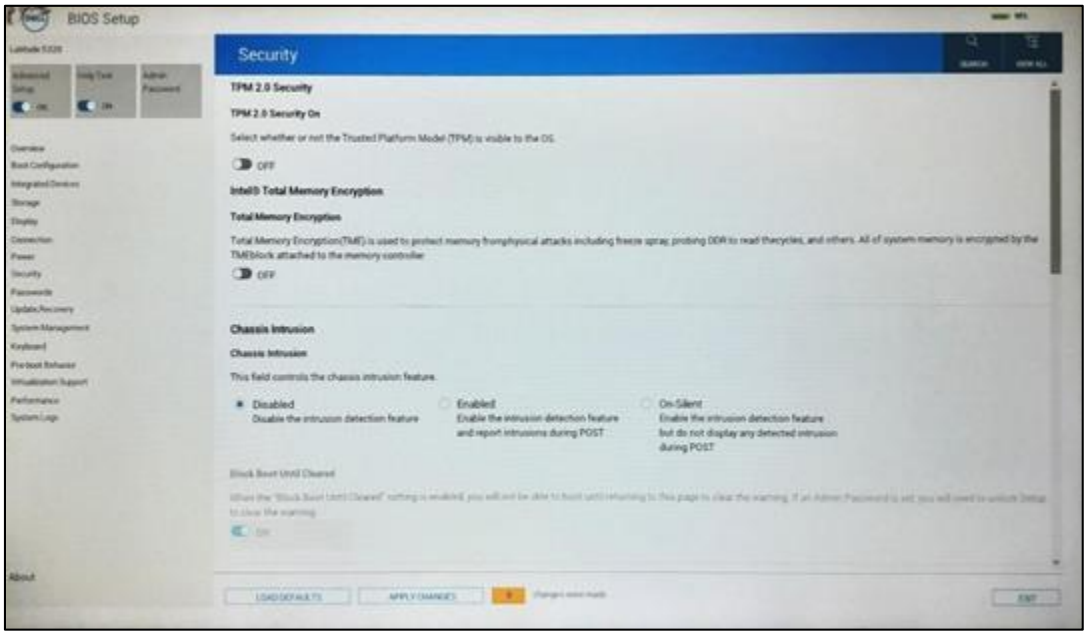
- *If the TPM chip is not activated on your machine, you need to activate it to erase data from the TPM chip.*
- *If your machine does not have a TPM chip, you can directly proceed with the erasing process.*
- *If TPM is already activated, you will not see the **BitRaser Drive Eraser (TPM Detected & Not Enabled)** dialog box.*

5. In the **BitRaser Drive Eraser (TPM Detected & Enabled)** dialog box, click **Yes** to restart your machine and activate the TPM chip.
   Note: *If you select No, you need to choose an alternative erasure method to proceed with the process.*

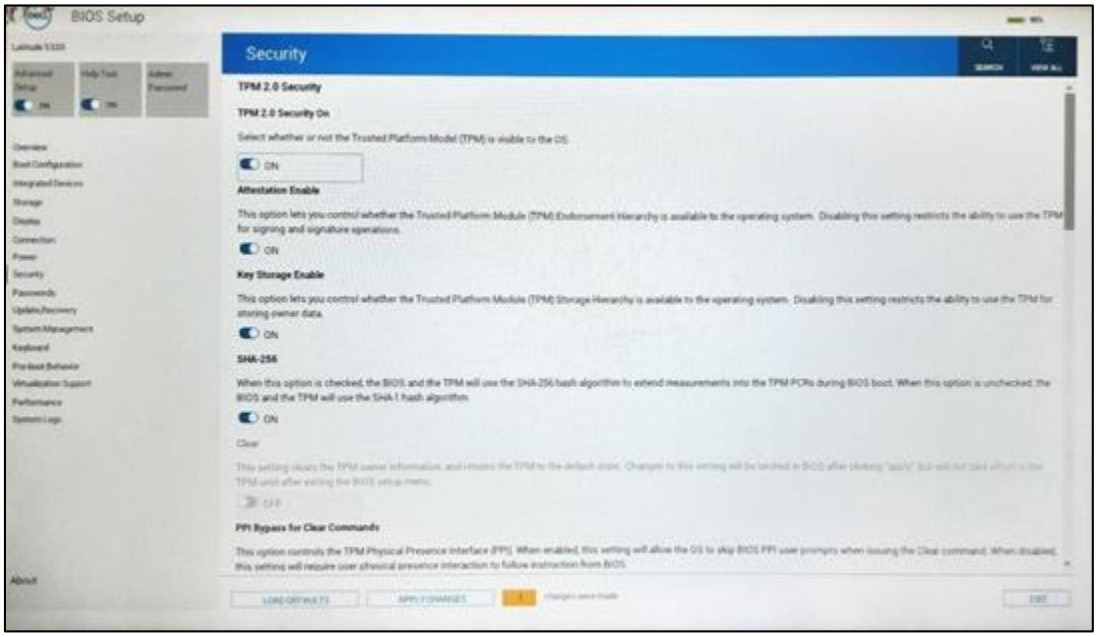


To activate the TPM chip in the Dell machine, follow these steps:

i. Navigate to the **TPM** section under the **Security** menu of the BIOS as shown below.

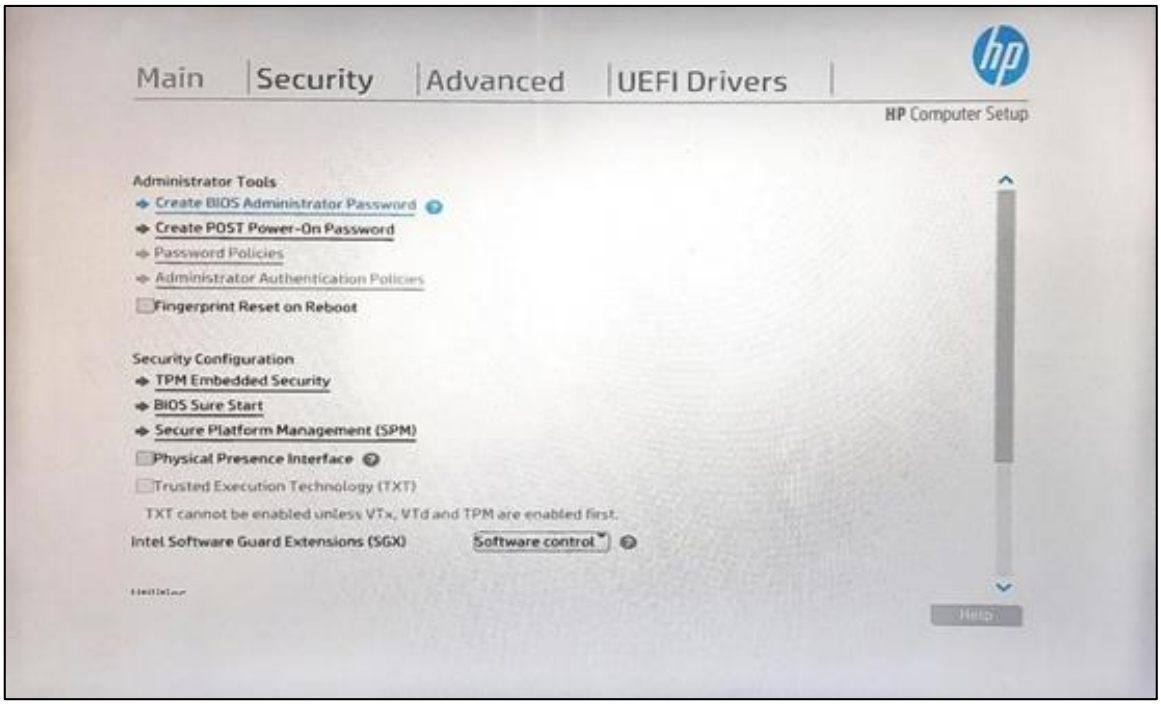


ii. In the **Security** menu of the BIOS, enable the **TPM 2.0 Security On** button, then click the **APPLY CHANGES** button.

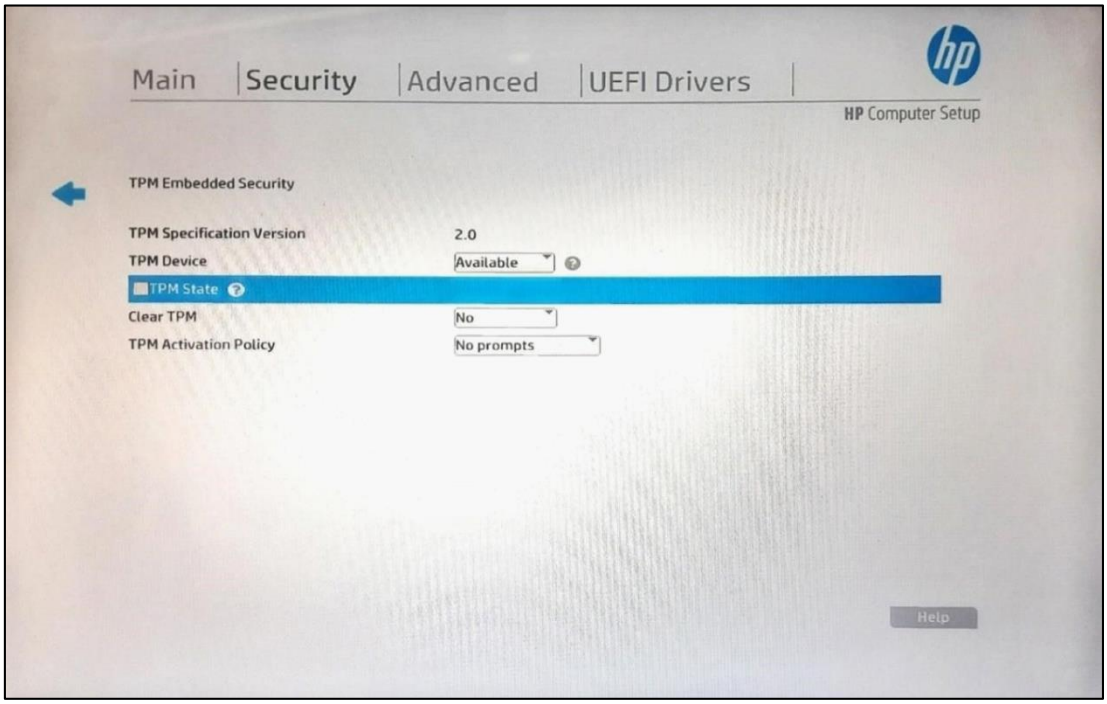


To activate the TPM chip in the HP machine, follow these steps:

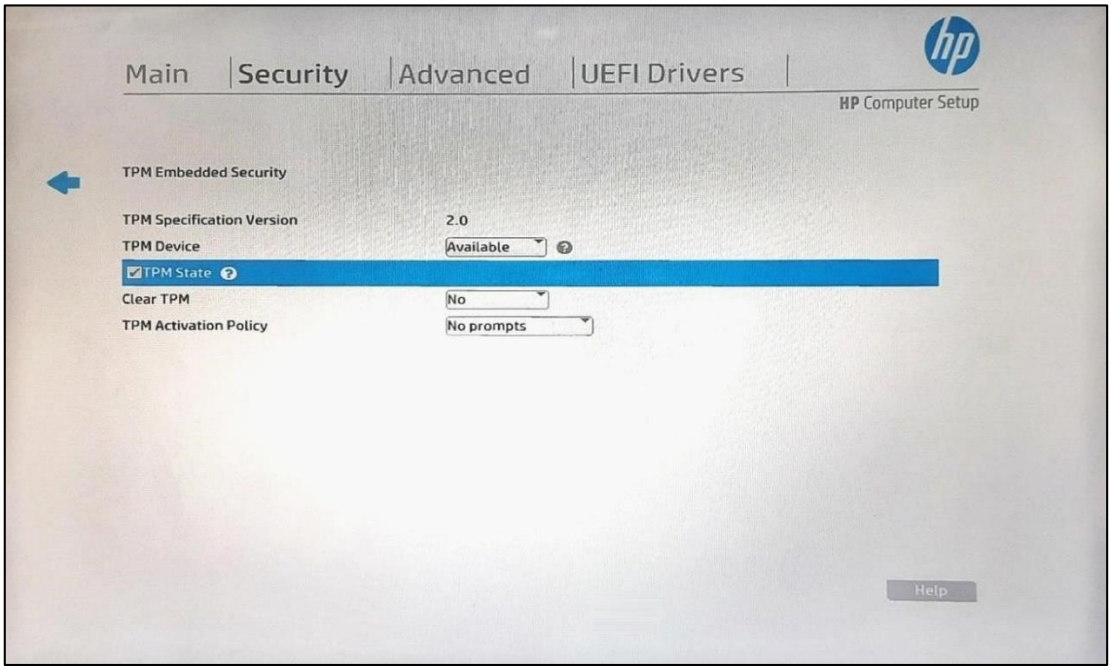
i. Navigate to the **TPM Embedded Security** section under the **Security Configuration** tab in the **Security** menu of your BIOS settings.



ii. In the **TPM Embedded Security** section, select **Available** from the **TPM Device** drop-down.



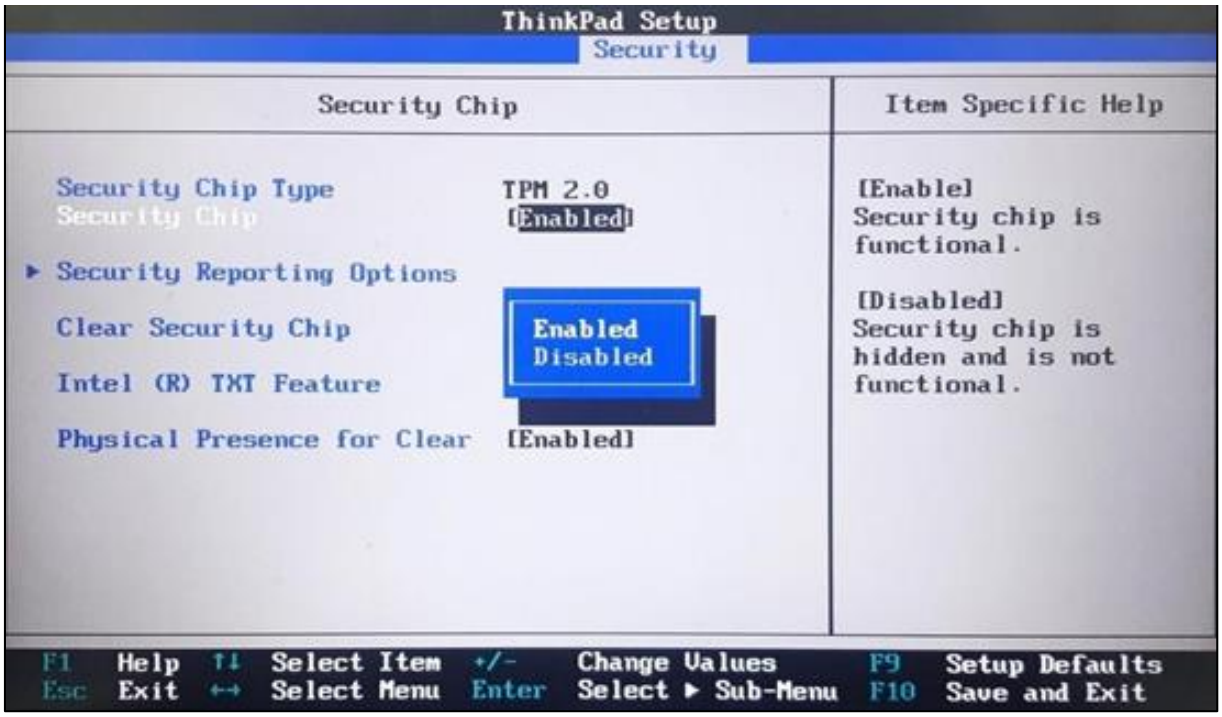
iii. The **TPM State** checkbox will be automatically selected when you choose **Available** from the **TPM Device** dropdown menu.



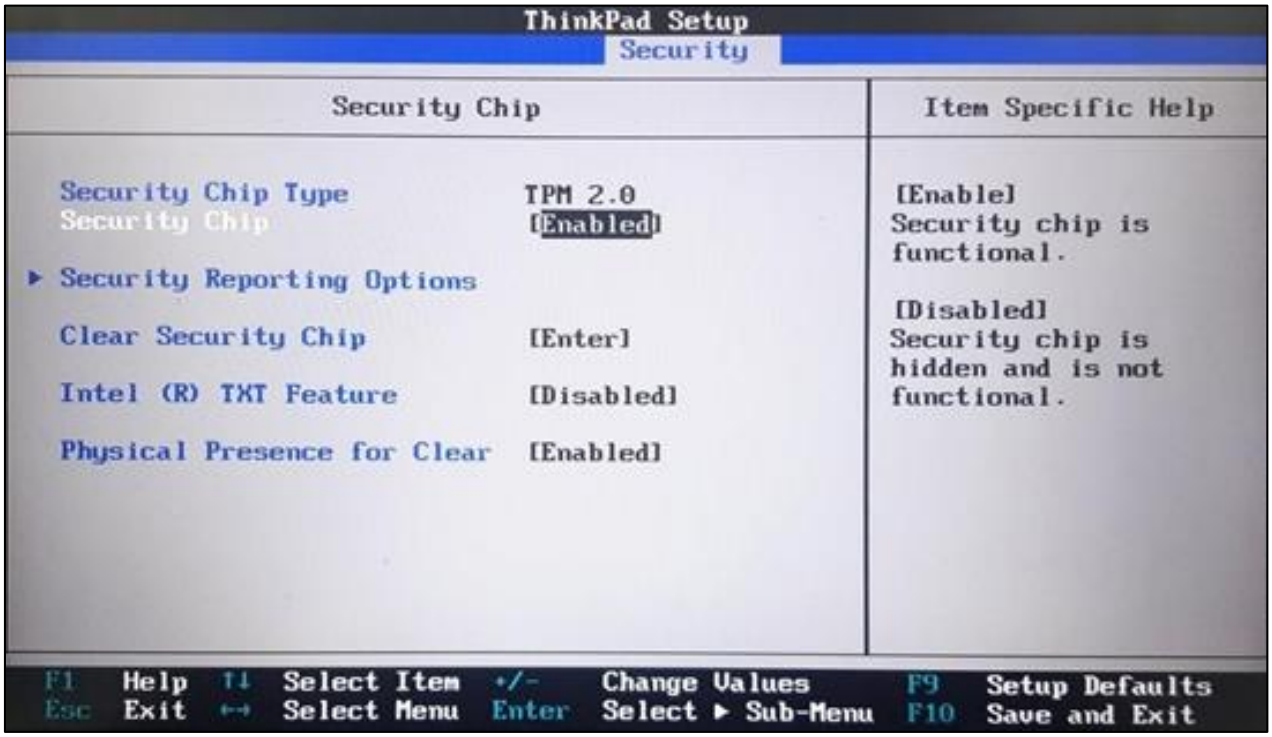
To activate the TPM chip in the Lenovo machine, follow these steps:

i. Navigate to the **Security Chip** section in the **Security** menu in your machine's BIOS settings.

ii. In the **Security Chip** section, enable the TPM security chip.

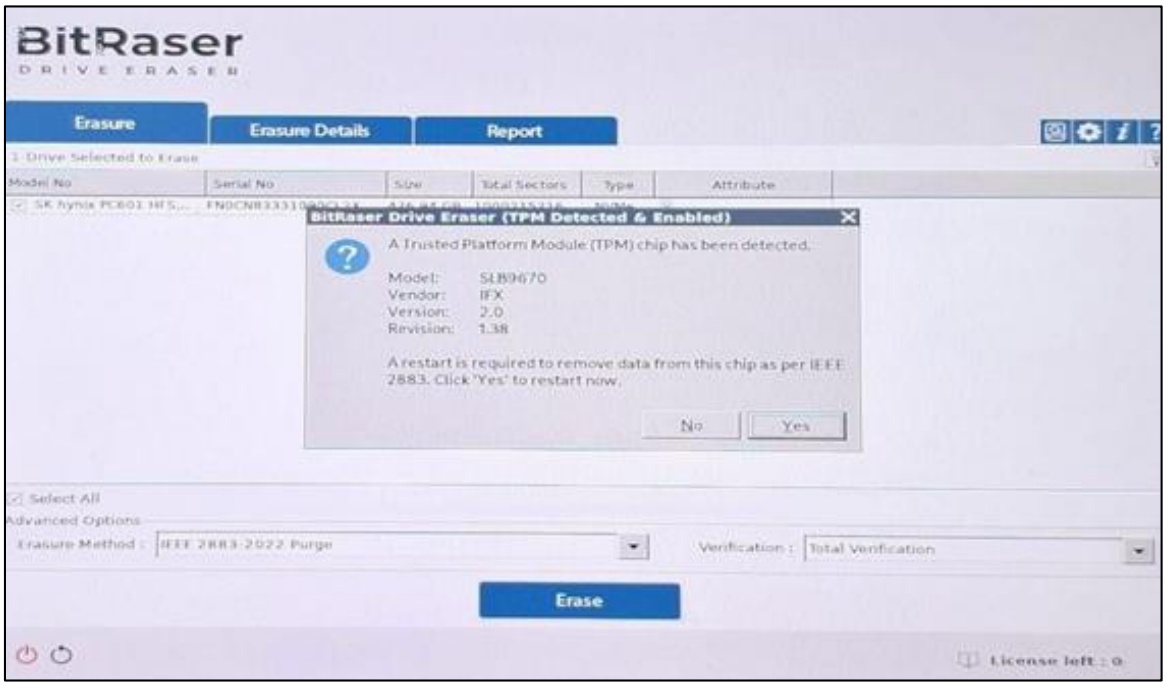


iii.The TPM chip will be enabled. Press **F10** to save the settings.

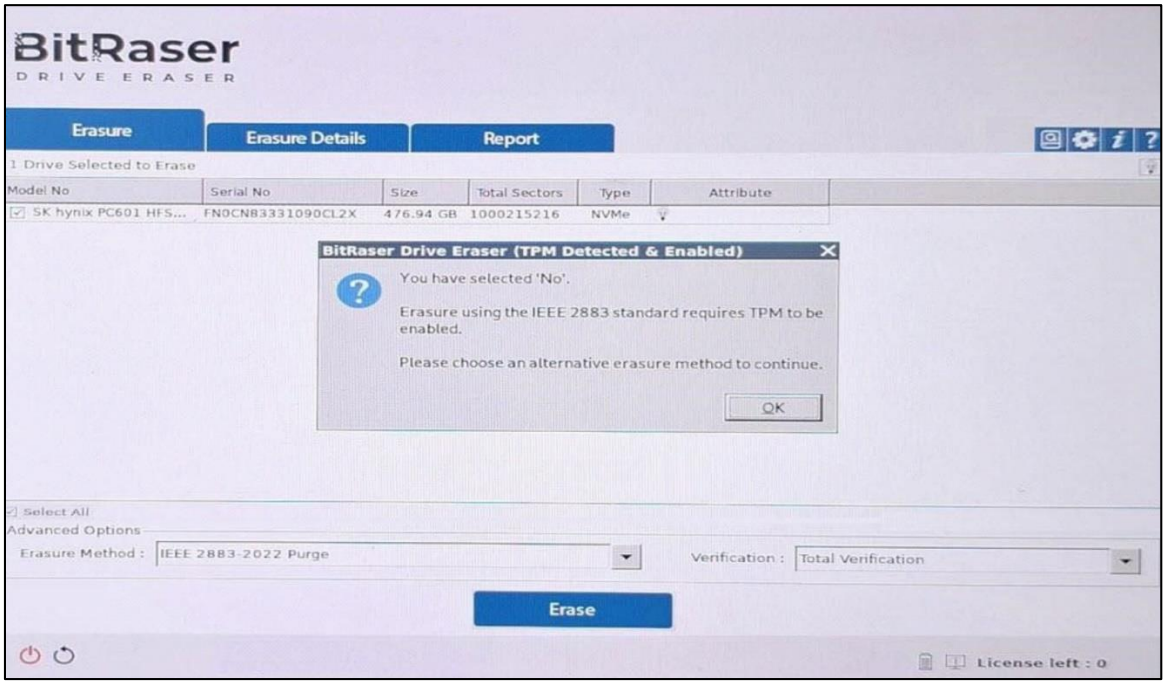


6. Once the TPM chip is activated, restart the machine and boot from the BitRaser bootable USB drive.

7. In the BitRaser Drive Eraser application, click the **Erase** button. The **BitRaser Drive Eraser (TPM Detected & Enabled)** dialog box appears with details of the detected TPM chip. Click **Yes** to continue.



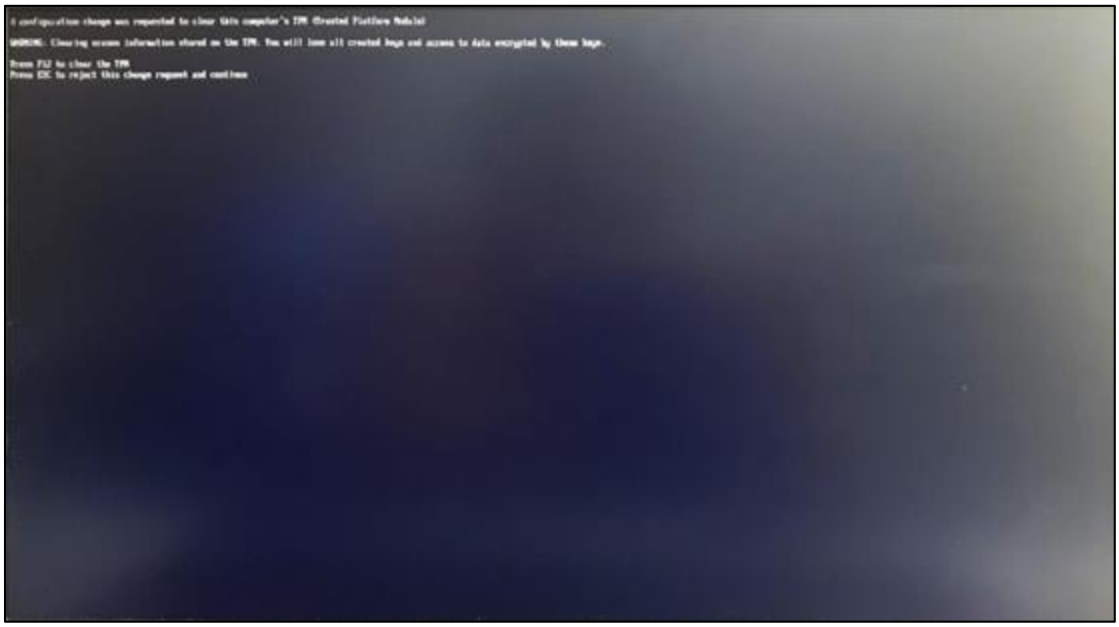
Note: *If you select* ***No,*** *you need to choose an alternative erasure method to proceed with the process.*



8. A screen will appear displaying the message "**A configuration change was requested to clear this computer's TPM (Trusted Platform Module)**".

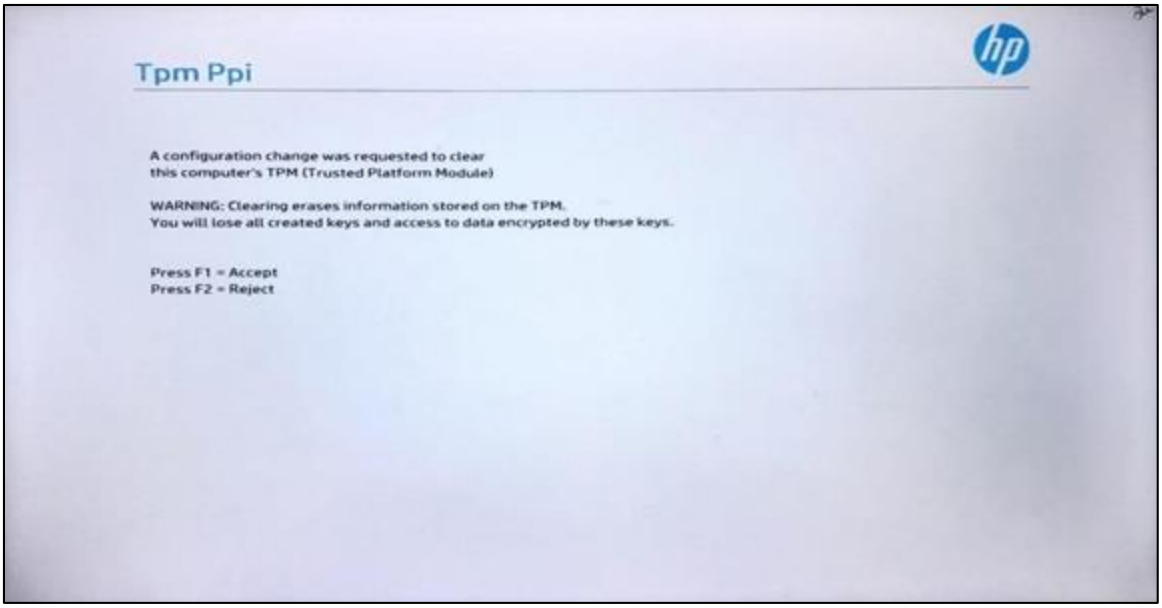
For Dell machine

Press **F12** to clear the TPM and press **ESC** to reject the change request and continue. The Machine will restart again.



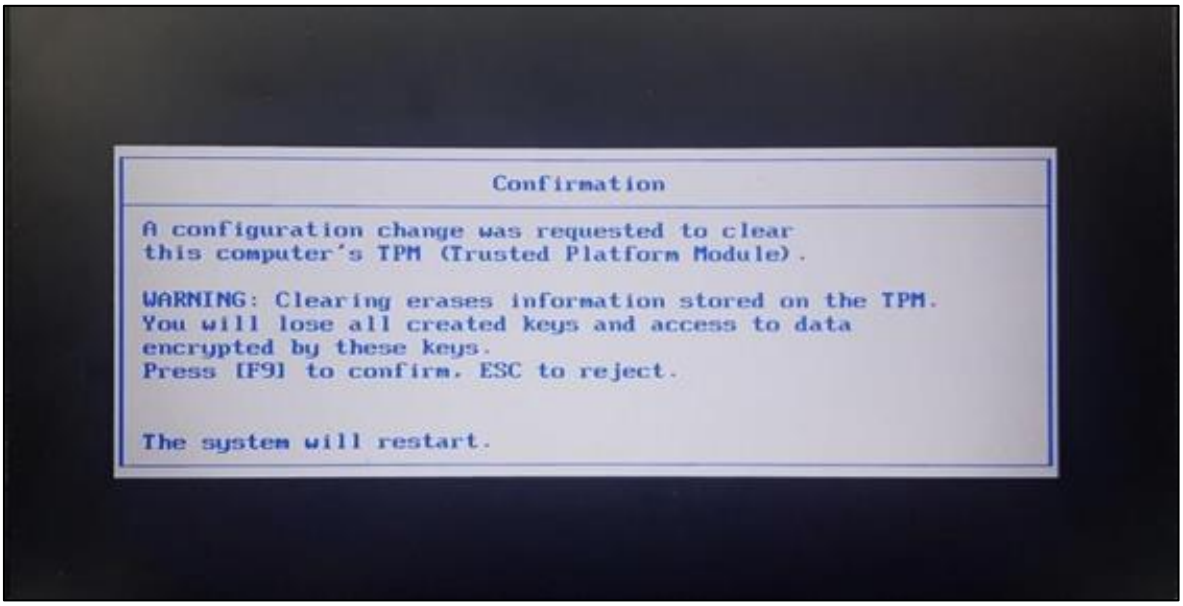
For HP machine

Press **F1** to **Accept** clearing the TPM and Press **F2** to **Reject.** The Machine will restart again.

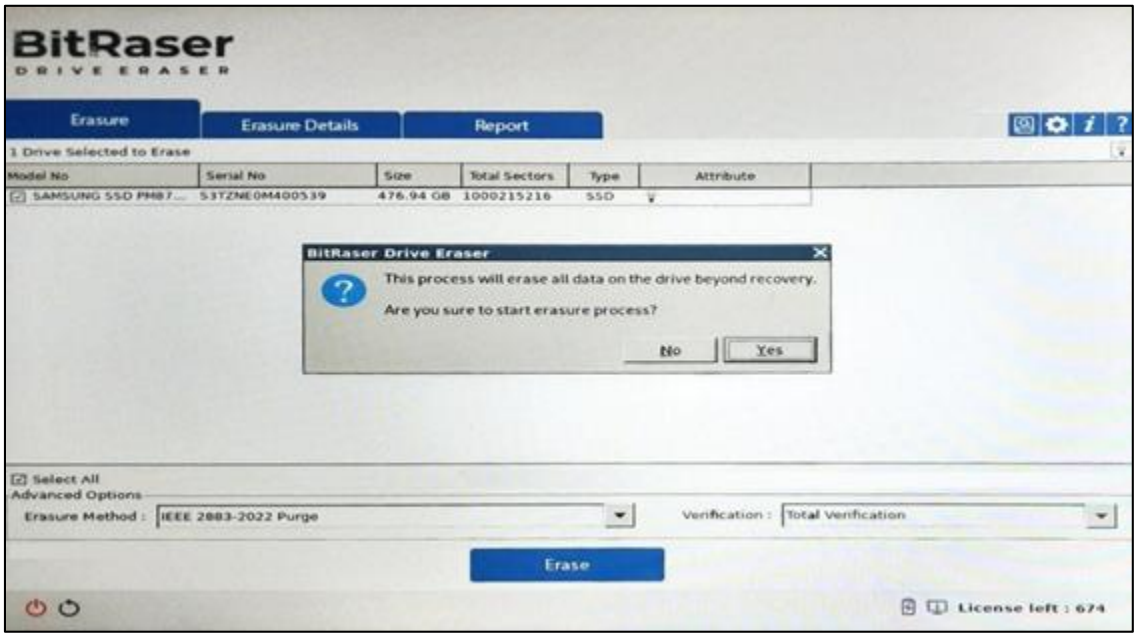


For Lenovo machine

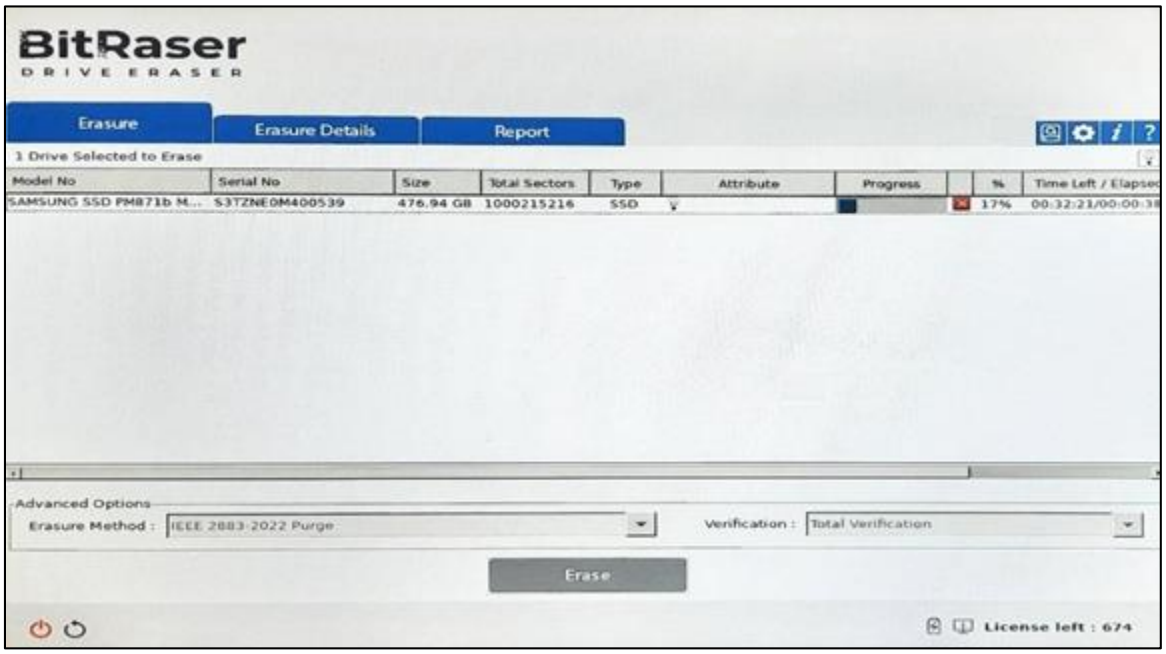
Press **F9** to **confirm** clearing the TPM, and Press **ESC** to **reject.** The Machine will restart again.



9. Connect the **BitRaser Drive Eraser** application to the network and **BitRaser** server before starting the erasure process.
10. In the **BitRaser Drive Eraser** application, click the **'Erase'** button. A **BitRaser Drive Eraser** confirmation dialog box will appear, requesting your permission to proceed. Click **'Yes'** to continue with the erasure process.

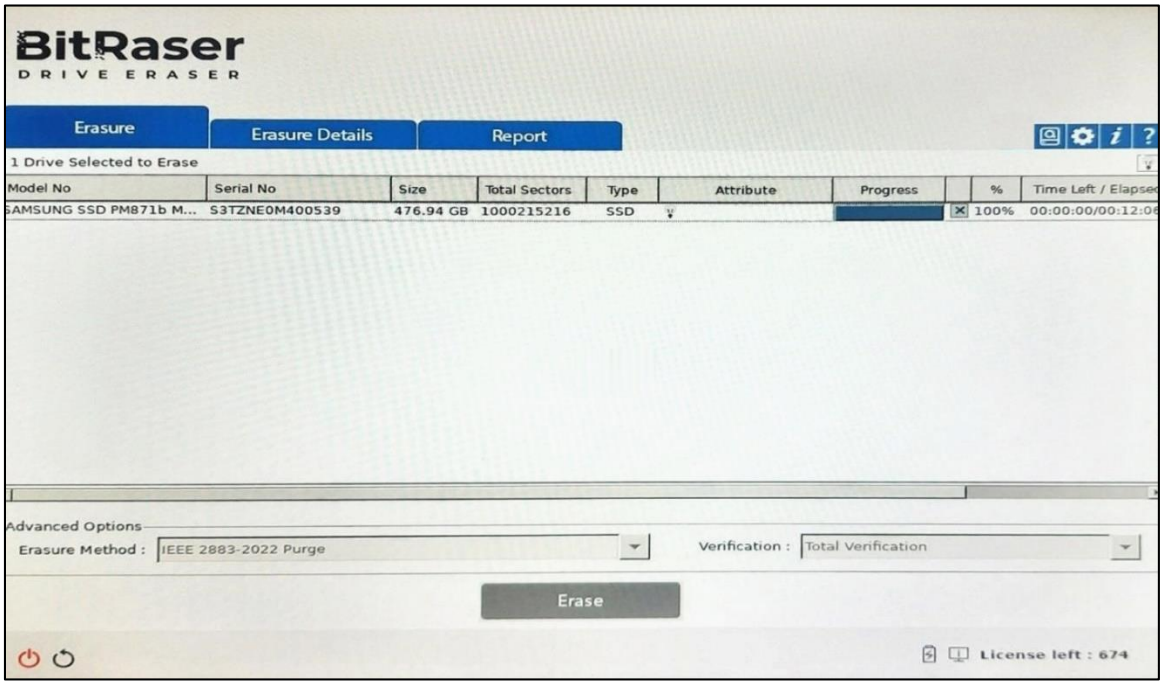


11. A progress bar, as shown below, appears and shows the progress of the erasure along with the percentage of completion, time left/elapsed, Serial number, and total sectors found on the drive during the process:



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

12. Once the process reaches **100%**, the progress bar will indicate that the erasure is complete.



3.2. CONFIGURE DETAILS

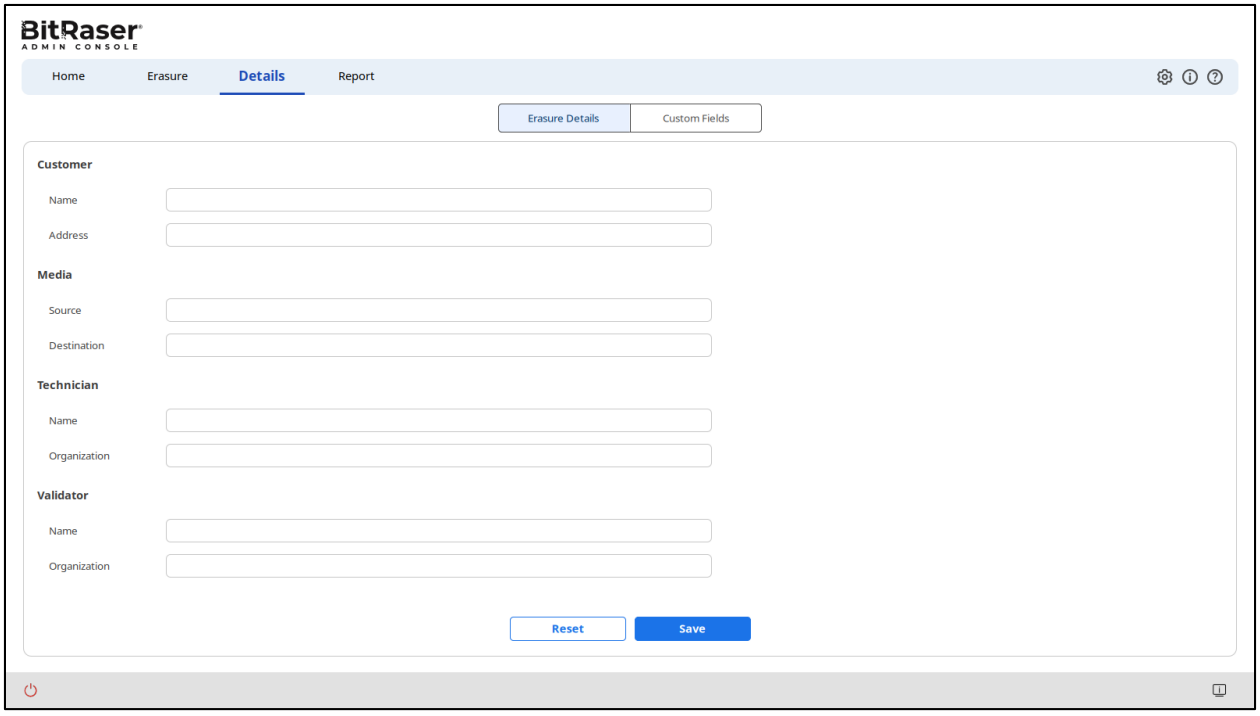
Configure the general information about the customer details and add custom fields as per the requirements. The information entered in this section will be added to the erasure report. The **Details** configuration is divided into two sub-sections:

- **Enter Erasure Details**: Erasure Details allows you to enter information like customer details, media details, technician details, and validator details.
- **Enter Custom Fields**: Custom Fields allows you to enter up to 20 sets of customized fields that can be added to the Erasure Reports.

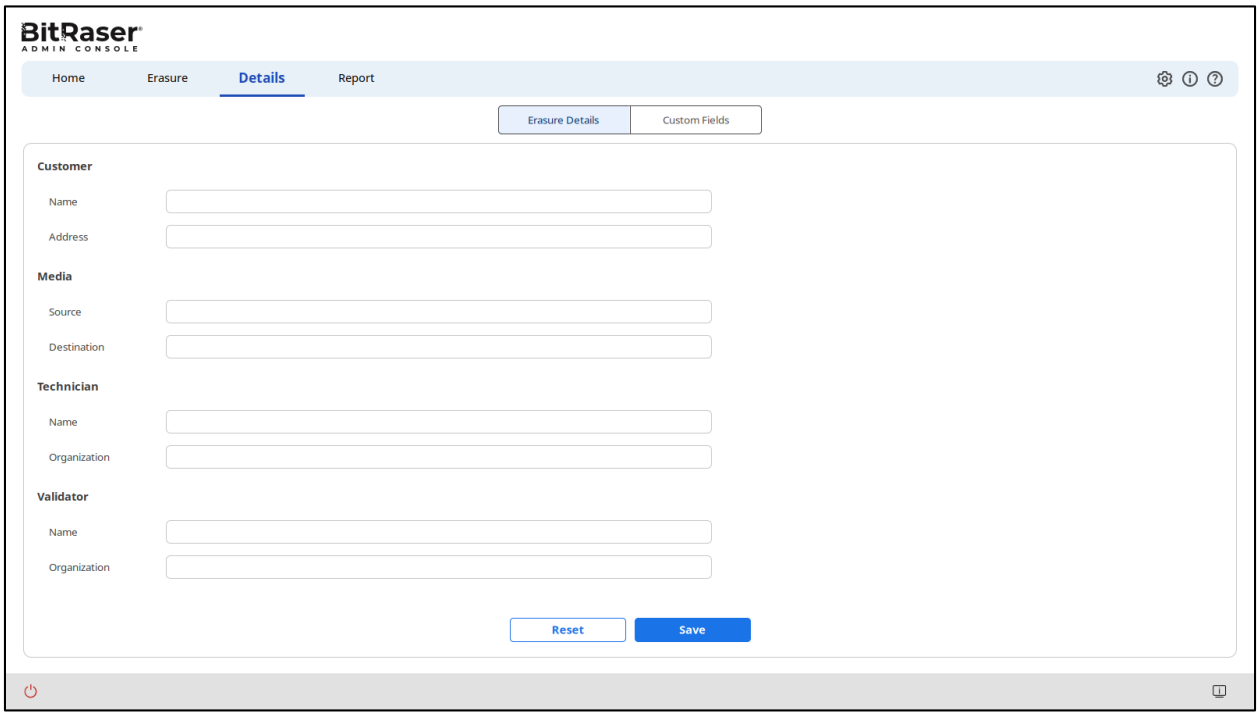
Note: *The erasure details should be filled in before starting the erasure process. These details are not mandatory, but if the client requires them to appear in the erasure report, they must be filled in and saved.*

3.2.1. ENTER ERASURE DETAILS

1. Run **BitRaser Admin Console**. Select the **Details** tab.



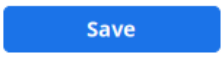
2. Click **Erasure Details**. A screen, as shown below, appears:



Specify the required details as mentioned below:

- **Customer Details**: Enter the details associated with the customer, such as Customer Name and Customer Address.
- **Media Details**: Enter the details associated with the media/machine, such as Media Source and Media Destination.
- **Technician Details**: Enter the details of the technician who would perform the erasure process. It contains fields Technician Name and Organization.
- **Validator Details**: Enter the details of the person who is validating the erasure process. It contains fields Validator Name and Organization.

3. Click

to reset the fields and enter the details again, if required.
4. Click 

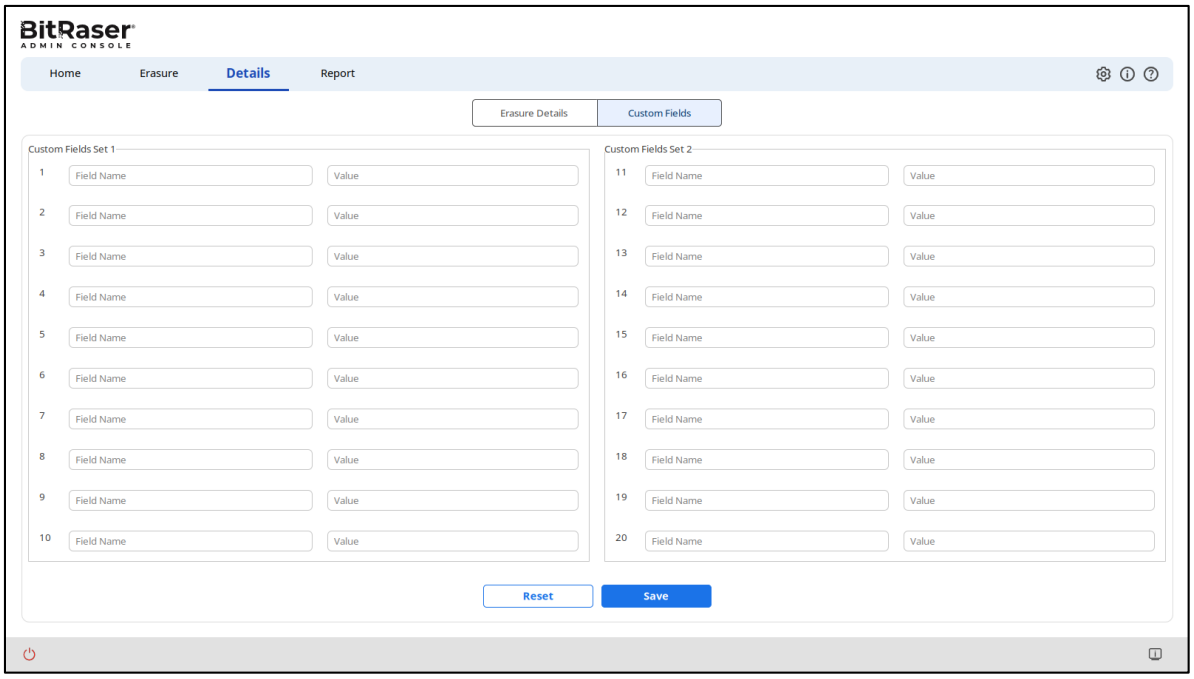
to save the information.

3.2.2. ENTER CUSTOM FIELDS

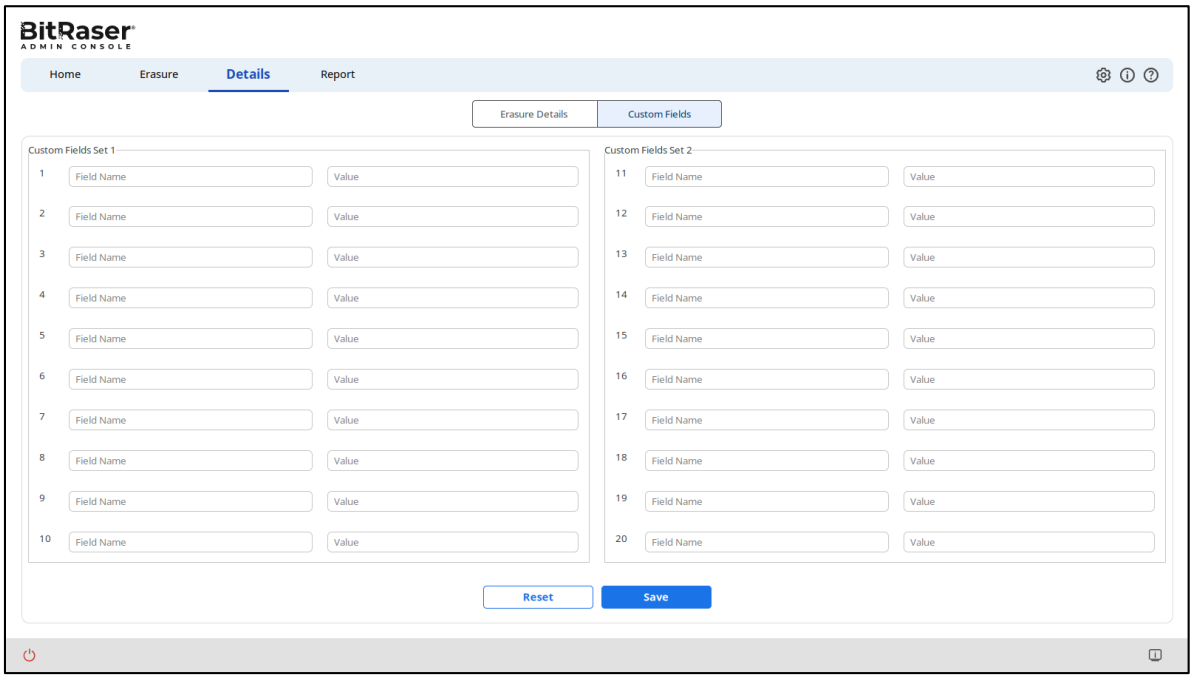
BitRaser Admin Console allows users to add up to 20 sets of customized fields to their erasure reports. These fields can be customized to capture specific data points relevant to the erasing process, such as department codes or asset classifications. This customization enables users to create more detailed and personalized reports that meet their organizational needs.

Follow these steps to add Custom Fields:

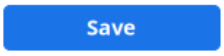
1. Run **BitRaser Admin Console**. Select the **Details** tab.



2. In the **Details** tab, click **Custom Fields**.



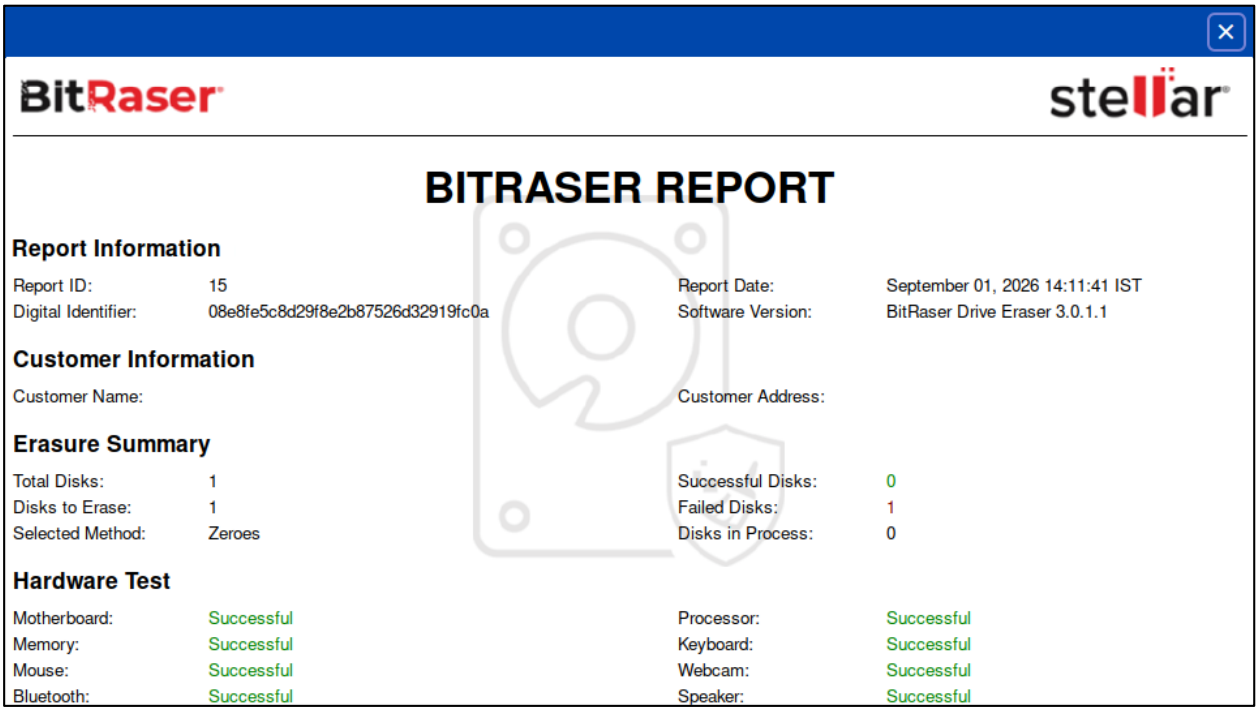
3. Upon selecting **Custom Fields**, a screen appears with fields to specify the **Field Name** and corresponding **Value**. Custom fields allow you to include specific information that may be relevant or unique to your erasure process and needs to be included in the report.
4. Click

to reset the fields and enter the details again, if required.
5. Click 

to save the information.

3.3. WORK ON REPORT AND CERTIFICATE

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



BitRaser stellar

BITRASER REPORT

Report Information

Report ID:	15	Report Date:	September 01, 2026 14:11:41 IST
Digital Identifier:	08e8fe5c8d29f8e2b87526d32919fc0a	Software Version:	BitRaser Drive Eraser 3.0.1.1

Customer Information

Customer Name:		Customer Address:	

Erasure Summary

Total Disks:	1	Successful Disks:	0
Disks to Erase:	1	Failed Disks:	1
Selected Method:	Zeroes	Disks in Process:	0

Hardware Test

Motherboard:	Successful	Processor:	Successful
Memory:	Successful	Keyboard:	Successful
Mouse:	Successful	Webcam:	Successful
Bluetooth:	Successful	Speaker:	Successful

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, and the number of successful or failed 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 Admin Console**.
- **Erasure Results**: Erasure Results contain 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 Admin Console,** see Export Report**.**

BitRaser Admin Console Certificate:

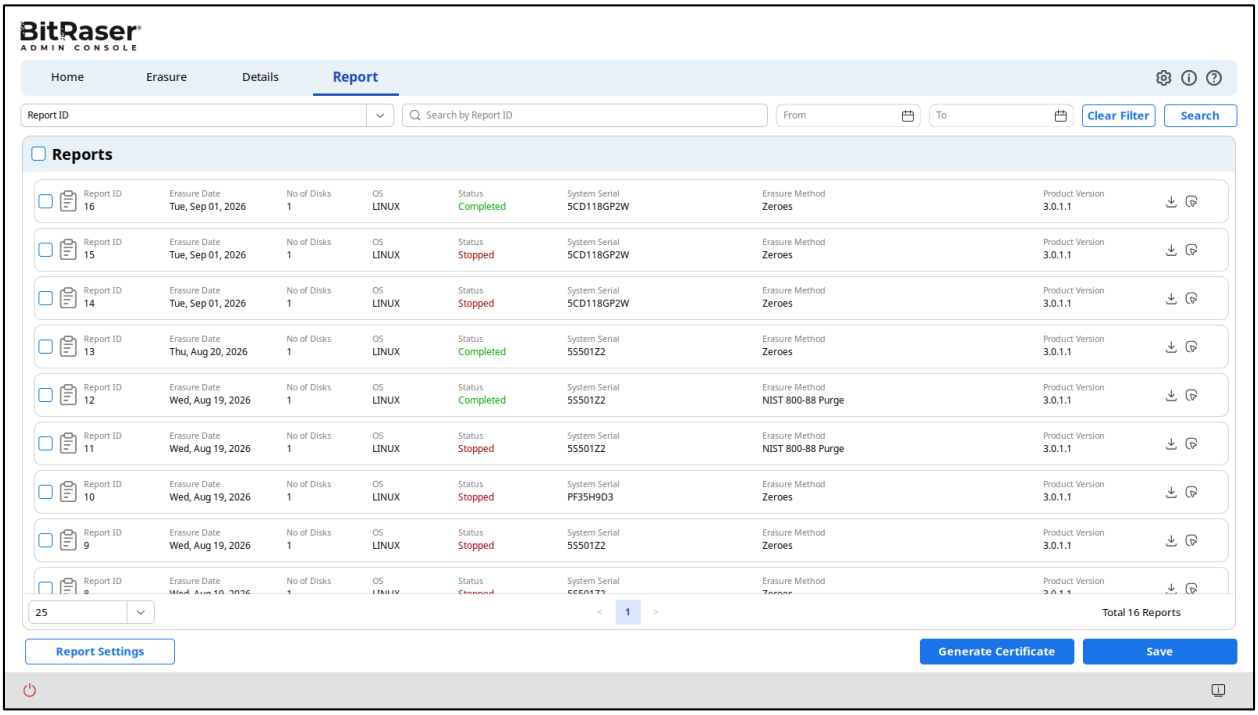
BitRaser Admin Console also provides you with a certificate of the erasure process performed. This certificate contains all the erasure details along with the signature and details of technician and validator performing the erasure process.

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

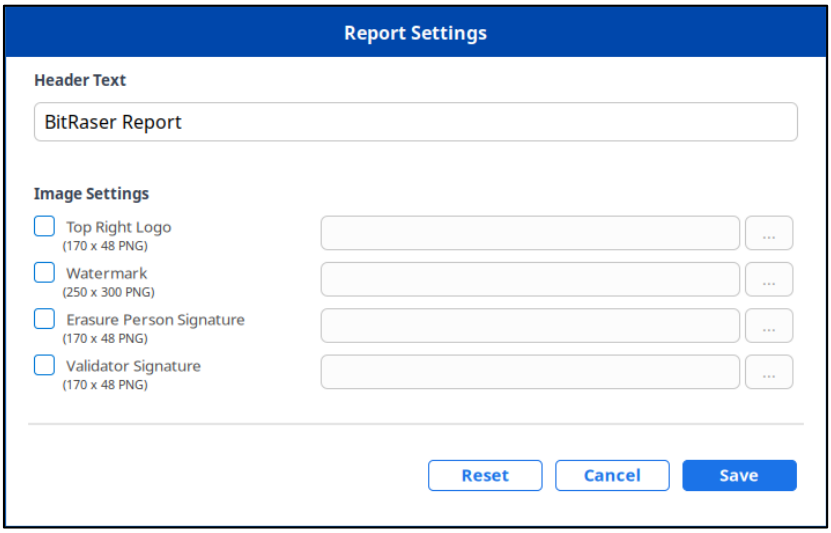
3.3.1. VIEW AND CUSTOMIZE REPORT

To view and customize BitRaser Admin Console report:

1. Boot and run **BitRaser Admin Console** and select the **Report** tab. All reports appear as shown below:



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



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

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

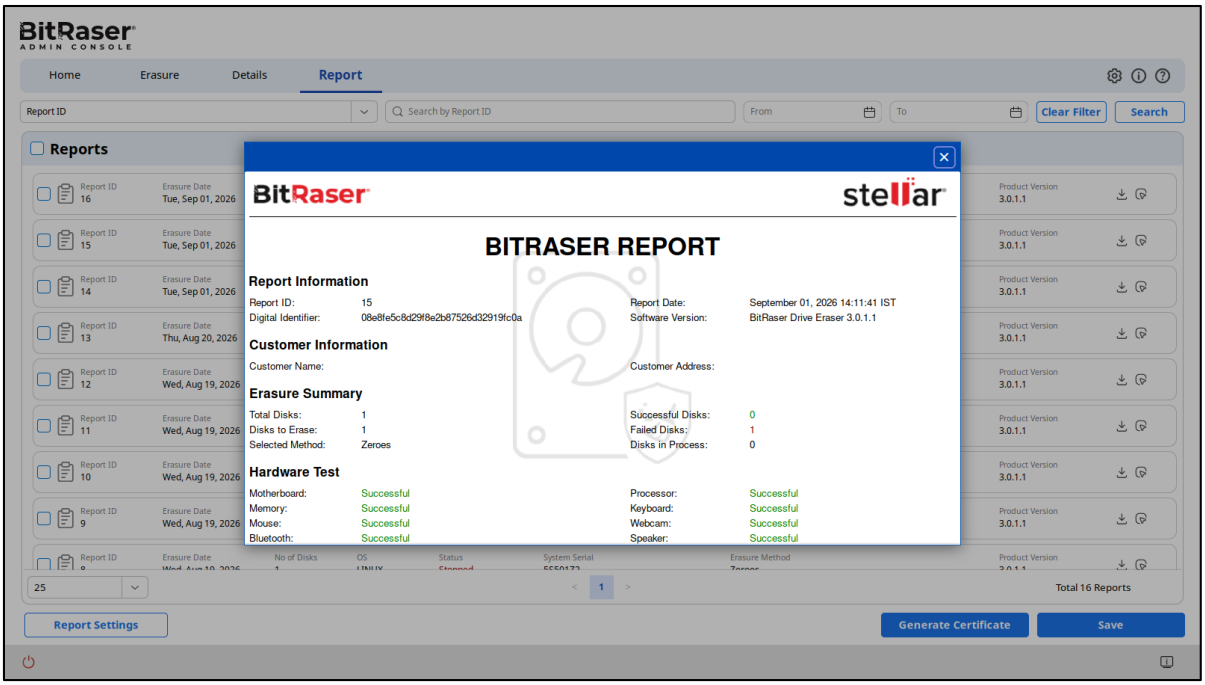
Sr. No.	Field Name	Description
1.	Enter report header text	Enter header text that appears on the header of the report (must be maximum of 30 characters)
2.	Select top right Logo	Select the check-box and click Browse to select the top-right logo of the report (image size and format - 170 x 48 PNG)
3.	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: *Top right logo, watermark, erasure person signature, and validation person signature image sizes need to be the same as specified in* ***Report Settings****. Top left logo, footer image, and text are set by default.* ***BitRaser Admin Console*** *will accept images with specified size and format only. In case of size mismatch,* ***BitRaser Admin Console*** *will continue to use the previously selected images.*

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

To preview the report

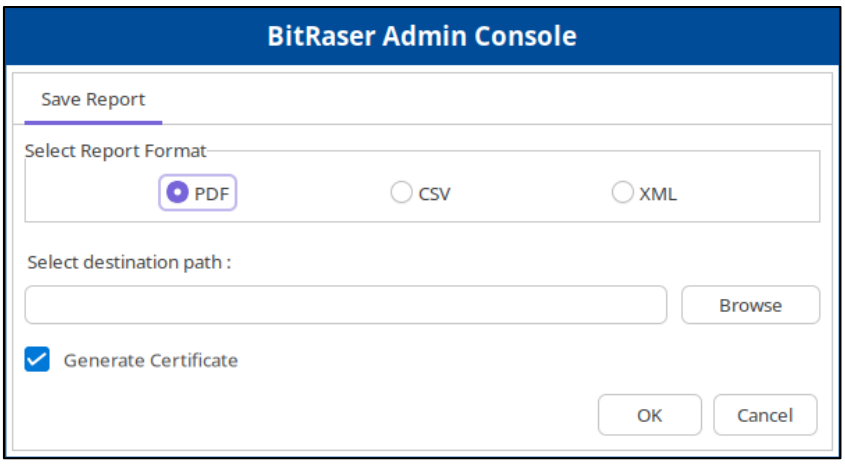
- Click this icon located in front of each report.
- The **BitRaser Report** screen appears.



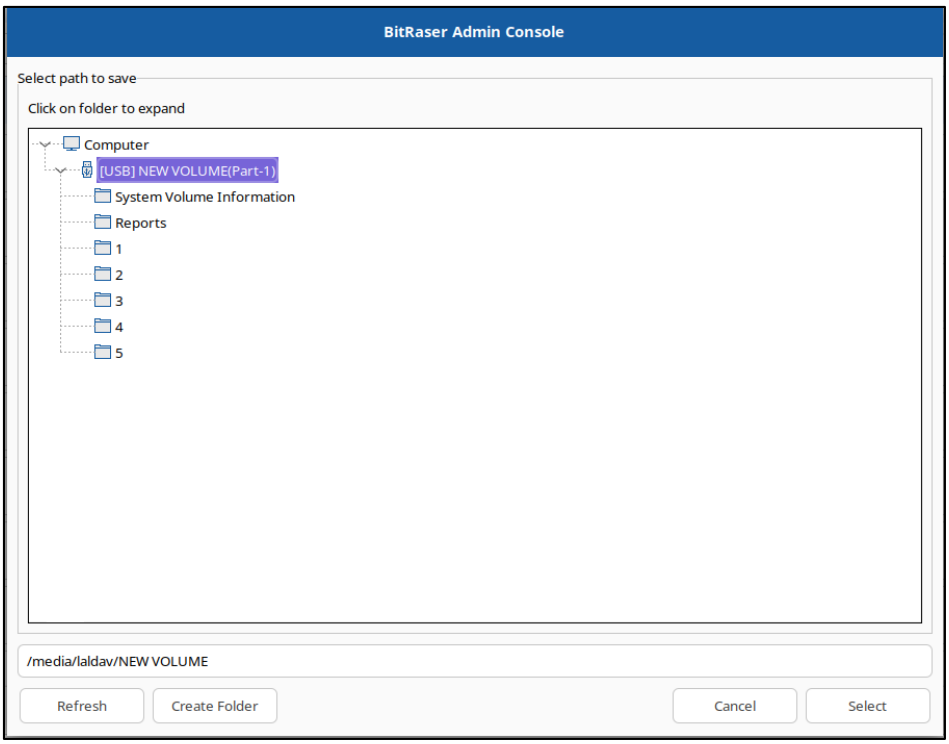
3.3.2. SAVE REPORT

To save a BitRaser Admin Console report:

1. Run **BitRaser Admin Console**. Select **Reports** tab.
2. Select the reports you want to save.
3. Click **Save** button located at the bottom right of the screen; the following dialog box appears:

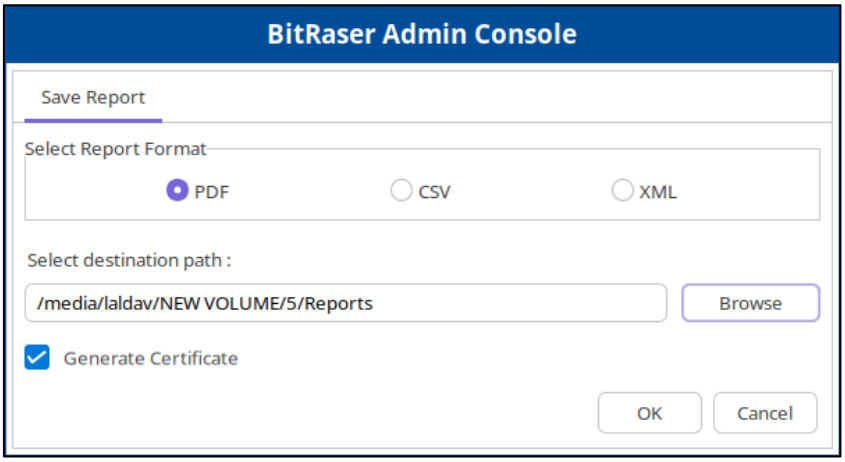


4. From the dialog box, select the format in which you want to save the reports, that is, either **PDF, CSV,** or **XML** format.
5. Click **Browse**. The following screen appears:

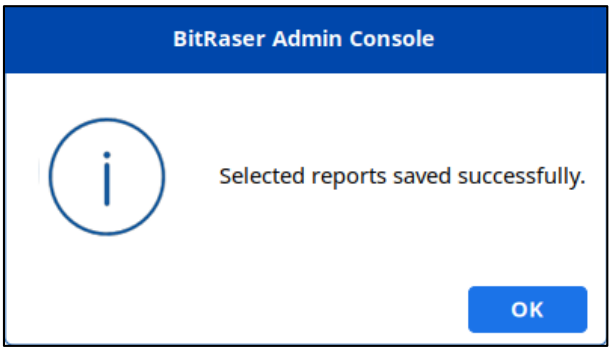


6. Select the destination folder where you want the file to be saved.

   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.*
7. Click **Select** to continue.



8. If you also wish to generate and save the certificates in the same path, select the check-box **Generate Certificate.**
9. Click **OK** and the report will be saved. "**Selected reports saved successfully**." message appears.



10. Click **Ok.**

3.3.3. EXPORT REPORT

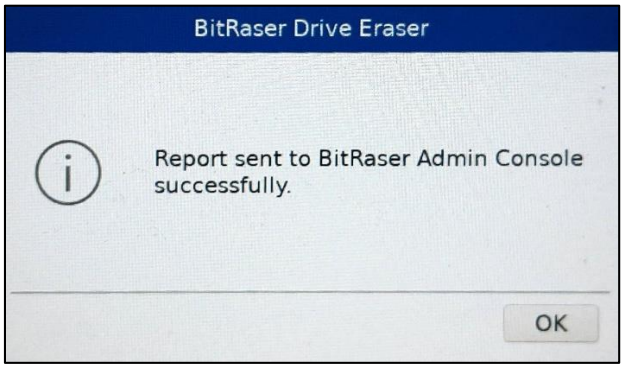
Export Report to BitRaser Admin Console from client side:

1. Click on **Export** button located at the bottom right of the screen.
2. Click **Send** to export the report to **BitRaser Admin Console.**

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

   Note: *Once the erasure process is completed, the erasure report is automatically sent to* ***BitRaser Admin Console.***
3. The icon in the bottom right corner of the report under **Report Tab** indicates that the report has been successfully sent to **BitRaser Admin Console**.

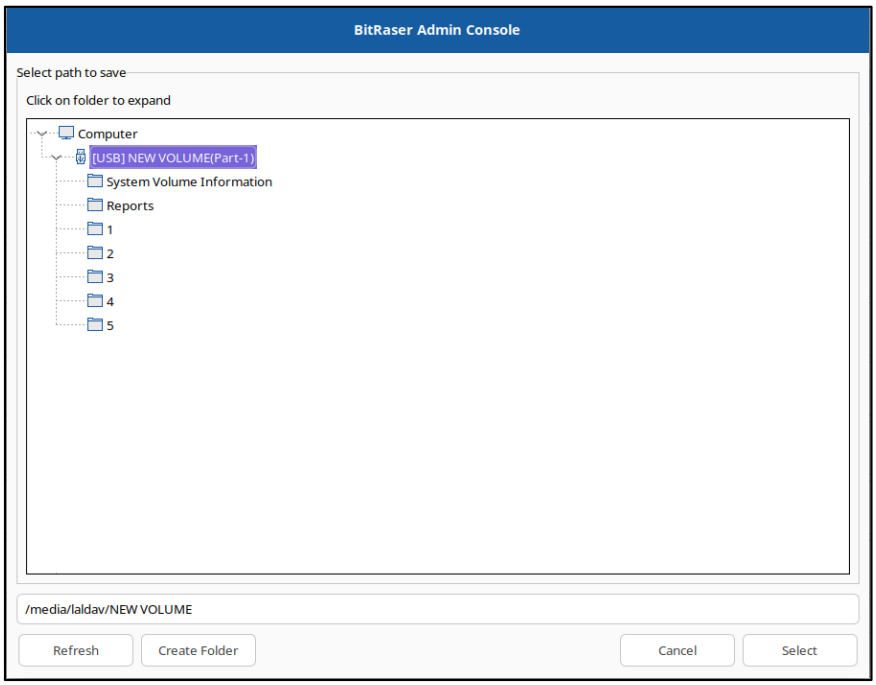
4. A dialog box appears with a message "**Report sent to BitRaser Admin Console successfully.**"



3.3.4. GENERATE AND SAVE CERTIFICATE

This option allows you to generate and save the erasure certificate to external media in PDF format. Follow the steps below:

1. Run **BitRaser Admin Console**. Select **Reports** tab.
2. Select the reports to generate certificates.
3. Click **Generate Certificate** button located at the bottom right of the screen. The following dialog box appears, as shown below:



4. Select the destination folder where you want the certificates to be saved.

   Note: *Use the* ***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.*

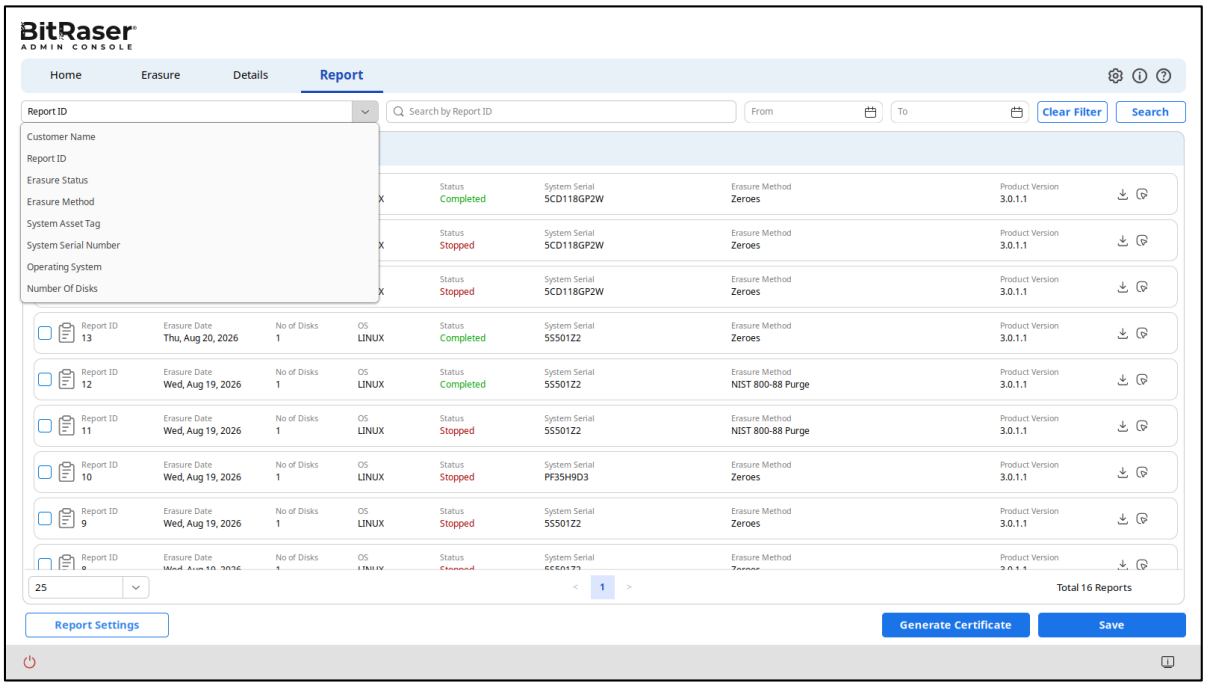
5. Click **Save** to continue.
   Note: *It is advisable to verify the saved certificate before closing the application.*

3.3.5. SEARCH REPORT

BitRaser Admin Console provides you with several filters to search your reports effortlessly. It consists of several filters.

1. **Search using filters**

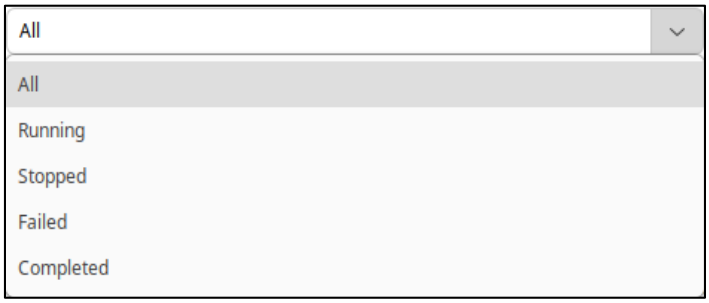
   To search the reports using filters, click the dropdown button.



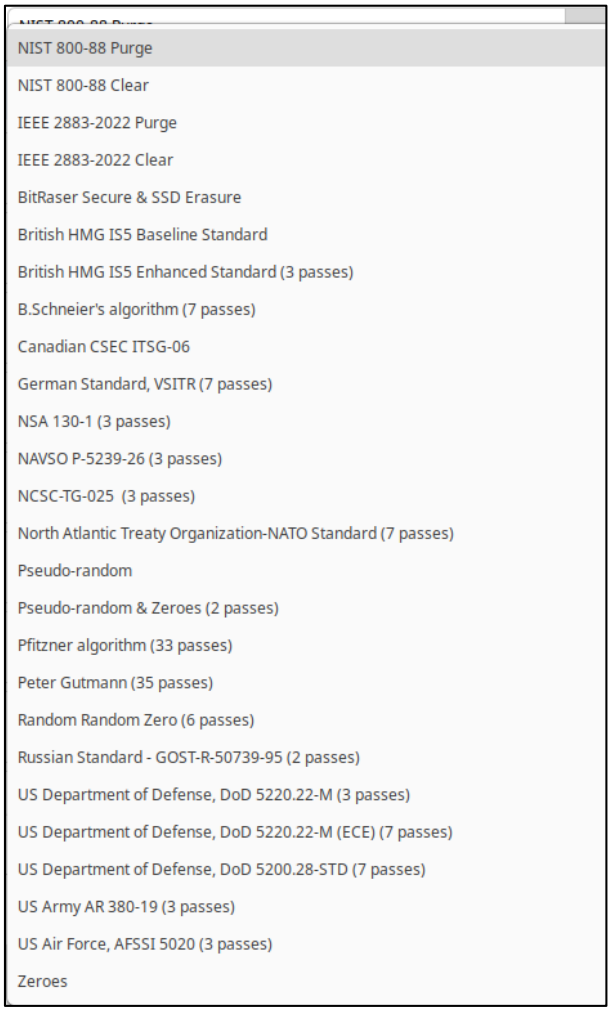
   It will provide the following options by which you can filter the report.

   - **Customer Name**: It will provide a list of all the reports for a particular customer name.
   - **Report ID**: Use this filter to search by entering the report ID of the report.

- **Erasure Status**: This filter will give another option to select a value. Select the desired value, i.e., All, Running, Stopped, Failed, or Completed, to generate a list of all reports, running reports, stopped reports, failed reports, or completed reports, respectively.



- **Erasure Method**: It will provide a list of all the reports for a particular erasure method.



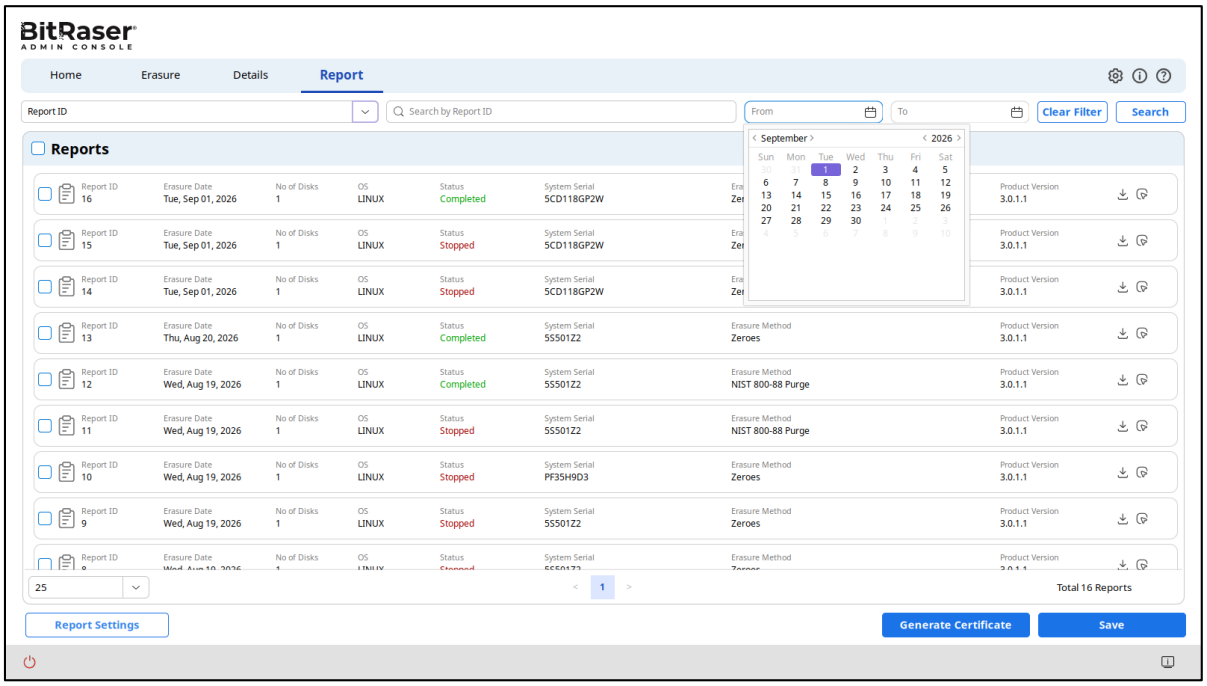
Note: *For details, refer to Erasure Methods.*

- **System Asset Tag**: Use this filter to search by entering the asset tag number of the system.
- **System Serial Number**: Use this filter to search by entering the serial number of the system.
- **Operating System**: Use this filter to search by entering the operating system of the device {eg: LINUX}
- **Number of Disks:** Use this filter to search by entering the number of disks erased.

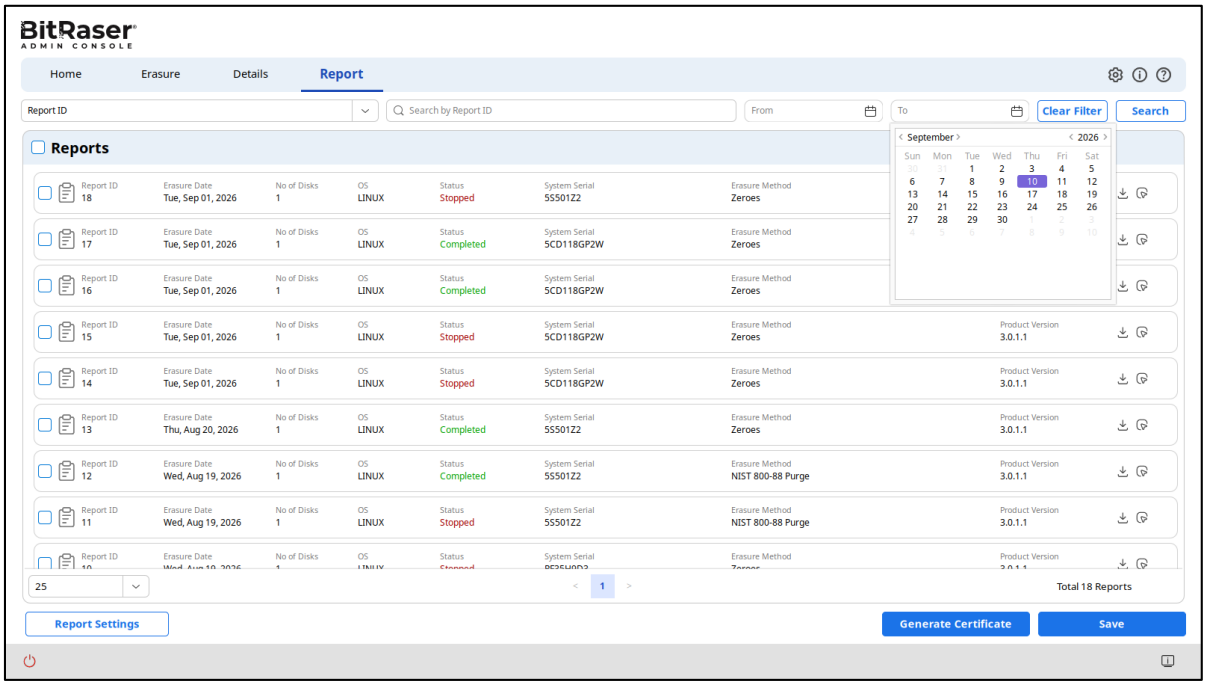
2. **Search by Date**

Use this filter to search records within a selected time period.

- **Calendar Icon**: Click calendar icon to open the date picker. Select the day, month, and year from the calendar.
- **Start Date (From):** Sets the first date for the search. Reports before this date are not shown.



- **End Date (To):** Sets the last date for the search. Reports after this date are not shown.



4. FREQUENTLY ASKED QUESTIONS

1. **What is Data Erasure?**

   Data erasure is a process of permanently erasing data from storage media devices 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 the impossibility of retrieving the data from an erased disk.

2. **What is BitRaser Admin Console and what are its main features?**

   BitRaser Admin Console is a portable application for permanent data erasure from connected devices. **BitRaser Admin Console** provides a centralized admin console for monitoring erasure and accessing reports and certificates repository on **BitRaser Admin Console Server** machine. The **BitRaser Admin Console** allows you to remotely control erasure on client machines over LAN and access tamper-free certificates and reports. This application erases data to prevent the recovery of sensitive data that is no longer required.

   Some of its main features are:

   - Securely and permanently erase sensitive data from machines and drives over a LAN network.
   - Provides complete centralized management of users, erasure, reports, and certificates.
   - Supports up to 100 drives for simultaneous erasure over a network.
   - Supports erasure of 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 26 world-class erasure methods, including NIST and IEEE erasure standards, with three options for erasure verification (No verification, Random verification, and Total verification).

3. **Where is the license information stored on BitRaser Admin Console and how to access the licenses?**

   BitRaser Admin Console needs access to license data for the erasure process. This license information is stored on a USB device called as **BitRaser Lock Key,** and this lock is required to be attached to the machine with OS during the transfer of the Licenses to the server using BitRaser Hardware Lock Manager to access the license information.

4. **I want to erase multiple systems and drives at a time; is it possible to do so using BitRaser Admin Console?**

   Yes, of course, you can erase multiple systems and drives at the same time. **BitRaser Admin Console** supports the erasure of up to 100 drives simultaneously.

5. **Can BitRaser Admin Console erase SSD drives?**

   Yes, **BitRaser Admin Console** supports SSD drive erasure.

6. **What is a fingerprint in BitRaser Admin Console?**

   The fingerprint acts as a unique identifier or signature to verify at a later stage that the drive has been erased using **BitRaser Admin Console** application. In **General Settings**, you can define the sector number on the drive where you want to add this unique identifier or the signature, and later verify the sector on the drive to make sure the software has performed the erasure satisfactorily.

7. **In how many formats can I save my erasure reports?**

   BitRaser Admin Console allows you to save the erasure reports in three formats. You can save your erasure reports in **PDF, CSV,** or **XML** format.

8. **Does BitRaser Admin Console support other languages?**

   BitRaser Admin Console is currently available in **English** only. However, the keyboard layout can be changed to your preferred language from the General Settings only on the client side.

9. **Is it possible to customize the erasure report?**

   Yes, you can customize the erasure reports of **BitRaser Admin Console** as per your requirement.

   To add details such as erasure and validator person details and to add custom fields, refer to Configure Details. To modify report settings such as logo, watermark, and erasure and validator person signature, refer to Report Settings.

10. **Does BitRaser Admin Console support data erasure from an SED?**
    Yes, **BitRaser Admin Console** supports data erasure from an SED. You can also erase data from multiple SEDs at once using the software. Refer to Erasure Process for the SED for detailed information.

11. **What will happen if I proceed with the erasure process with an incorrect password for an SED?**

    If you save and erase with an incorrect password for an SED, the software will not be able to access the drive; hence, it will lead to a failed erasure attempt.

12. **Can I start the erasure procedure for an 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 NOTICE

This End User License Agreement (hereinafter called “EULA” or “AGREEMENT” contains important terms and conditions governing the use and licensing of the BitRaser software.

This EULA is a legal and binding agreement between YOU (“CUSTOMER”, or “LICENSEE”, or “YOU”) and Stellar Information Technology Pvt. Ltd., (“Stellar” or “We” or “Licensor”), having its registered address at 205, Skipper Corner, 88, Nehru Place, New Delhi, India 110019.

PLEASE READ THIS EULA CAREFULLY.

BY DOWNLOADING, INSTALLING, COPYING, ACCESSING OR USING THIS SOFTWARE, IN WHOLE OR IN PART, **YOU ACKNOWLEDGE AND AGREE** TO BE BOUND BY ALL TERMS AND CONDITIONS OF THIS EULA, INCLUDING THE LIMITATIONS OF LIABILITY AND **WARRANTY CLAUSE**.

IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, STELLAR DOES NOT GRANT TO YOU ANY RIGHTS TO THE

SOFTWARE. YOU MUST IMMEDIATELY DISCONTINUE THE INSTALLATION OR USE OF THE SOFTWARE AND PROMPTLY RETURN THE SOFTWARE AND PROOF OF ENTITLEMENT TO THE PARTY FROM WHOM YOU ACQUIRED THE SOFTWARE.

---

1. DEFINITIONS

1.1. **“Computer”** means any physical or virtual device capable of processing information, including, without limitation PCs, laptops, smartphones, tablets, embedded systems & hardware products on which the software is installed or accessed.

1.2. **“Compatible Computer”** means a computer with the recommended operating system and hardware configuration set out in the documentation contained in the Software.

1.3. **“Customer”, “You”, or “Licensee”** means any individual, body, corporate or legal entity that has been granted rights to use the Software for its own internal purposes in accordance with the terms and conditions contained in this EULA.

1.4. **“License”** means the limited non-exclusive right granted by Stellar to use the Software for specific purpose and in the manner permitted under this EULA.

1.5. **"Permitted Number"** means one (1), unless a different quantity is expressly authorized under a valid license (e.g., volume license) granted by Stellar

1.6. **"Software"** means

1.6.1. all of the information provided with this agreement, including but not limited to:

1.6.1.1. all software files, programs, executables, and other computer information;

1.6.1.2. any proprietary scripting logic embedded within exported file formats

1.6.1.3. images, sounds, clip art, video and other works included with Stellar software or made available by Stellar on it's website for use with the Stellar software and not obtained from Stellar through a separate service or from another party ("Content Files");

1.6.1.4. related explanatory written materials, help manuals and files ("Documentation"); and

1.6.2. any modified versions, copies, upgrades, updates, patches, enhancements, and additions to the foregoing provided by Stellar at any time, unless supplied under separate terms (collectively, "Updates").

2. LICENSE GRANT TERMS

2.1. **Right to use the Software:** Subject to the terms and conditions of this Agreement, Stellar grants Customer a non-exclusive, non-transferable, non-perpetual, revocable and limited right to use the Software on a 'Permitted Number' of computers solely for internal purposes in accordance with the license type.

2.2. **Scope.** Stellar provides license for usage of the Software only. The Software runs locally on Customer-controlled devices to perform media-sanitization, diagnostics or other related functions.

2.3. **No Services.** Stellar does not provide media sanitization services, managed services, data-center services, operational services, or any other services under this EULA.

3. LICENSE TYPES

3.1. **Pay Per Use License:** License is consumed each time the Software performs a task (including drive erasure, mobile erasure, or diagnostics). One license is deducted per use from the Customer's available pool.

3.2. **Subscription License:** Subscription License permits the Customer to use the Software during the active subscription term on Permitted Number of Computers. Software may require periodic Internet-based license validation unless deployed in approved offline modes. Failure to complete required validation or failure to pay applicable subscription fees may result in suspension or inactivation of the Software. Subscription license will renew automatically unless cancelled by the Customer in accordance with the applicable renewal terms. Stellar may modify, replace, or update Software components included in a subscription, provided such changes do not materially reduce the core functionality of the Software.

4. TECHNICAL SUPPORT

Free Technical Support is provided for one (1) year from the date of purchase. Support beyond one year requires additional fees. Stellar will not provide Support after three (3) years from the date of purchase.

5. INTELLECTUAL PROPERTY OWNERSHIP

Stellar owns and retains all rights, title, and interest in and to the Software, its source code, the Documentation, and all related intellectual property, whether registered or unregistered, and whether existing now or in the future; and are protected by the copyright and intellectual property laws of India, and other applicable jurisdictions, as well as by international treaties. Customer acknowledges that all intellectual property rights in the Software and Documentation belong to, and/or are licensed to Stellar. The License granted under this EULA provides only a limited right to use the Software; it does not constitute a sale or transfer of any ownership rights. Except for the limited rights expressly granted in this EULA, no other rights are conveyed, and all rights not expressly granted are reserved by Stellar.

6. LICENSEE RESTRICTIONS & REQUIREMENTS

6.1. **Use Obligations:** Customer shall use the Software solely as permitted under this EULA and strictly in accordance with the Software's intended design, and Documentation.

6.2. **No Modifications or Derivative Works:** Customer shall not, and shall not permit any third party to:

6.2.1. modify, adapt, translate, tamper with, or create derivative works of the Software or Documentation;

6.2.2. combine or merge any part of the Software or Documentation with or into any other software or Documentation;

6.2.3. use the Software in any manner to develop, train, or improve competing software, scripts, routines, or programs (including any routine, script, code, or program) having any functional attributes, visual expressions or other features similar to those of the Software to compete with Stellar;

6.2.4. publish or disclose performance results, benchmark tests, or comparative analysis of the Software without Stellar's prior written consent.

6.3. **No Reverse Engineering.** Customer shall not reverse engineer, decompile, disassemble, or otherwise attempt to derive or access the source code, underlying algorithms, or structural design of the Software.

6.4. **No Unbundling.** The Software is licensed and provided as a single integrated product. Although Customer is not required to install all components, Customer shall not unbundle, separate, or use individual components on different Computers unless expressly permitted in the Documentation.

6.5. **Prohibited Cloud or On-Demand Use.** Customer shall not run, host, or operate the Software in any cloud, Internet-based, virtualized, or on-demand computing environment unless the Documentation expressly permits such deployment.

6.6. **No Transfer or Unauthorized Distribution.** Customer shall not rent, lease, sell, sublicense, assign,

transfer, distribute, or otherwise convey any rights in the Software, nor authorize any portion of the Software to be copied or installed on another individual's or entity's computer, except as expressly permitted under this EULA.

7. WARRANTIES

Except as expressly stated in this Section 7, the Software (excluding the physical media on which it may be delivered), and all Stellar-related websites, content, and services, are provided to Customer **"**AS IS" and "AS AVAILABLE." Stellar and its licensors and suppliers make NO WARRANTIES OR REPRESENTATIONS of any kind, whether express, implied, statutory, or otherwise, including without limitation any warranties of merchantability, satisfactory quality, fitness for a particular purpose, accuracy, availability, performance, non-infringement, interoperability , or that the Software or related websites or services will operate uninterrupted, error-free, free of viruses, securely, or in combination with any particular hardware, software, platform, or environment. These disclaimers apply to the maximum extent permitted by applicable law. Nothing herein limits any warranty that cannot be excluded under applicable law.

Customer's sole and exclusive remedy for breach of any warranty is repair, replacement, or re-delivery of the Software at Stellar's option.

8. INDEMNIFICATION

8.1. **Intellectual Property (IP) Infringement Indemnity.** Subject to Customer's proper use of the Software strictly in accordance with this Agreement and the Documentation, Stellar warrants that the unmodified Software, as provided by Stellar, does not infringe any third party's intellectual property rights. Stellar will, at its sole discretion, defend and indemnify Customer against any third-party claim alleging such infringement, and will pay only those damages and reasonable attorneys' fees finally awarded or payable under a settlement approved in writing by Stellar. This is Customer's sole and exclusive remedy for any IP infringement claim.

8.2. **Conditions.** Customer must notify Stellar of any IP infringement claim within **five (5) business days** of becoming aware of it. Any delay relieves Stellar of its obligations to the extent it is prejudiced. Customer must provide full cooperation and grant Stellar **exclusive control** over the defense and settlement. Customer may participate with its own counsel at its own expense but will not settle any claim or make any statement inconsistent with Stellar's interests without Stellar's prior written consent.

8.3. **Exclusions.** Stellar has no obligation for claims arising from: (a) use of the Software in violation of this Agreement or the Documentation; (b) use with hardware, software, not approved by Stellar; (c) modifications or alterations not made by Stellar; (d) use of outdated, unsupported, or non-current versions of the Software; or (e) Customer's environment, systems, configurations, or Customer-provided content or materials.

8.4. **Remedies.** If an infringement claim arises, Stellar may, at its discretion: (a) secure the right for Customer to continue using the Software; (b) modify or replace the Software; or (c) terminate the affected license and refund the unused portion of fees.

9. LIMITATIONS & LIABILITY

9.1. **Excluded Damages.** To the fullest extent permitted by law, Stellar is not liable for indirect, incidental, special, punitive, or consequential damages; loss of profits, revenue, business, or data; business interruption; or costs of replacement services, even if advised of the possibility.

9.2. **Maximum Liability.** Stellar's total aggregate liability for all claims under this Agreement, including indemnity claims, will not exceed the License fees Customer paid in the 12 months before the event giving rise to the claim.

9.3. **No Liability for Customer Environment.** Stellar is not responsible for issues caused by Customer's systems, data, configurations, third-party software, or use outside a Supported Environment.

9.4. **Mandatory Carve-Out.** Nothing in this Section limits liability that cannot be excluded under applicable law.

10. Data Collection, Privacy & Confidentiality

10.1. **Consent to Data Collection and Use. By using the Licensed Software,** Customer agrees that Stellar may collect, use, process, transmit, and store information relating to Customer's Account, devices, system interactions, and use of the Software, in accordance with Stellar's Privacy Policy available at **https://www.BitRaser.com/privacy-policy.php**. Such information may include

technical, diagnostic, and usage data used to provide, maintain, support, improve, and enhance the Software.

Customer further agrees that such information may be transferred to and processed in any **other jurisdiction** by Stellar, its affiliates, and service providers.

10.2. **No Storage of Customer Confidential or Personal Data (Except as Stated).** The Software does not access, store, save, or transmit Customer confidential information or personal data, except as expressly described in this Agreement or the Privacy Policy. Customer is solely responsible for ensuring that no sensitive or regulated data is introduced into the Software except as permitted.

10.3. **Data Security.** Stellar will maintain administrative, physical, and technical safeguards designed to protect the confidentiality, integrity, and availability of Customer data processed by Stellar, to the extent within Stellar's control and only as required for Stellar's performance under this Agreement.

10.4. **Data Storage & Handling on BitRaser Cloud Console.** If Customer uses the BitRaser Cloud Console, the Cloud Console stores and processes only system-generated outputs and metadata (e.g., device identifiers, erasure reports, certificates, logs, and license usage data) and does not store Customer business data or end-user content. Such outputs may constitute Customer-provided Confidential Information to the extent they contain information supplied by the Customer. Authentication credentials (e.g., username and email address), usage records, and reports may be stored and processed on BitRaser Cloud, which is hosted on BitRaser's approved cloud infrastructure providers.

10.5. **Liability Alignment.** All obligations under this Section 10 are subject to the limitations, exclusions, and maximum liability set out in Section 9 (Limitation of Liability).

11. CONNECTIVITY

11.1. 11.1. **Internet Connectivity**. The Software may cause Customer's computer, without additional notice, to automatically connect to the Internet and communicate with BitRaser Cloud Console, Stellar websites or server for purposes including license validation, activation, registration, updates, security checks, feature delivery. When the Software connects to Stellar website whether

automatically or by user action; Stellar's Privacy Policy applies. Such connections may transmit technical, diagnostic, usage, and system‑related information, and, where applicable, Customer credentials used for activation or access to BitRaser Cloud Console. Unless prohibited by applicable law, Stellar may send transactional messages or in‑product information related to the Software or other Stellar Software.

11.2. **Updates.** The Software may automatically connect to the Internet, intermittently or regularly, to check for, download, install, and report on Updates.

11.3. **Activation and License Validation.** The Software may require Customer to obtain an activation key, activate or reactivate the Software, register the Software, or validate a subscription or license. These processes may trigger automatic Internet connections on installation, launch, or periodically thereafter. Information transmitted may be used to detect or prevent unauthorized or fraudulent use. Failure to activate or validate may result in reduced functionality, inoperability, or suspension of the license or subscription.

11.4. **Digital Certificates.** The Software may use digital certificates to identify downloaded files and their publishers. Validation of such certificates may require Internet connectivity.

11.5. **Offline Variant.** The Offline variant of the Software is delivered on a USB drive along with a USB port accessible License 'Lock key'. This variant does not require any Internet connection for core functionality and does not access BitRaser Cloud Console.

12. TERMINATION

12.1. **Termination for Cause.** If Customer breaches this EULA and fails to cure such breach within **thirty (30) calendar days** after receiving written notice from Stellar, Stellar may terminate this EULA. Upon termination, **all rights granted to Customer immediately cease**, including the license to use the Software, which shall stand revoked without further action.

12.2. **Return or Destruction of Software.** Upon termination, Customer shall **return or destroy** all copies of the Licensed Software and, upon Stellar's request,

provide **written certification** confirming such destruction. Failure to return or destroy the Software, or failure to provide certification, entitles Stellar to pursue **equitable relief and damages**.

13. JURISDICTION AND LAW

13.1. **Governing Law and Forum.** This EULA is governed by, and will be construed in accordance with, the substantive laws applicable in the **State of Delhi, India**. The **courts at Delhi, India,** shall have **exclusive jurisdiction** over any dispute arising out of or relating to this EULA, the Software, or the license granted hereunder. Customer irrevocably consents to the jurisdiction of the courts at Delhi, India.

13.2. **Exclusions.** This EULA will not be governed by any conflict-of-law principles or by the **United Nations Convention on Contracts for the International Sale of Goods,** the application of which is expressly excluded.

14. GENERAL

14.1. **Entire Agreement.** This EULA constitutes the **entire agreement** between the parties with respect to the Licensed Software and supersedes all prior or contemporaneous understandings, purchase orders, agreements, communications, or arrangements relating to its subject matter.

14.2. **Survival.** The exclusions of warranties, limitations of liability, and any provisions that by their nature should survive, shall continue in effect after termination of this EULA. Such survival does not grant Customer any continued right to use the Licensed Software after termination.

14.3. **Export Compliance.** Customer shall not ship, transfer, export, or use the Licensed Software in any manner prohibited by applicable export control laws, including, where applicable, the United States Export Administration Act and related regulations (“Export Laws”). All rights granted under this EULA are conditioned upon Customer’s compliance with the Export Laws, and such rights are automatically forfeited upon any non-compliance.

14.4. **Reservation of Rights.** All rights not expressly granted to Customer under this EULA are reserved by Stellar. The Licensed Software is protected by the copyright laws of India and other applicable jurisdictions. All ownership rights belong to

Stellar Information Technology Pvt. Ltd., 205 Skipper Corner, 88 Nehru Place, New Delhi 110019, India.

14.5. **No Third-Party Beneficiaries.** This EULA does not create any rights for, or confer any benefits upon, any third party.

14.6. **No Waiver.** Any waiver by Stellar of a breach of this EULA shall not constitute a waiver of any other or future breach of the same or any other provision.

14.7. **Binding Effect.** This EULA is binding upon, and inures to the benefit of, the parties and their respective successors and permitted assigns. It supersedes all prior or contemporaneous representations, discussions, undertakings, communications, agreements, advertisements, and understandings relating to the Licensed Software.

14.8. **Amendments.** This EULA may be modified, supplemented, or amended only by a written instrument signed by an authorized officer of Stellar.

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

6. ABOUT STELLAR

Stellar is a leading data care corporation headquartered in India, with a strong presence in the USA and Europe. An ISO 9001 & ISO 27001 certified organization, Stellar specializes in Data Recovery, Data Erasure, Mailbox Conversion, and File Repair software and services.

BitRaser, is our data erasure software that helps organizations wipe drives and devices securely to maintain compliance.

Our software products are recognized for their ease of use, innovation, and value, offering practical features to meet both specialized and broad user needs.

For over 30 years, Stellar has consistently focused on developing future-ready solutions that are unrivalled in capability and built with the core purpose of delivering comprehensive data care to consumers and enterprises worldwide.

For more information about us, please visit our corporate website www.stellarinfo.com or product website www.BitRaser.com.