BitRaser Mobile Eraser & Diagnostics

User Guide for version 3.0

Legal Notices | About Stellar | Contact Us

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

Table of Contents

1. GENERAL INFORMATION....2
    1.1. INTRODUCTION....3
    1.2. ABOUT THE GUIDE....6
    1.3. CONTACT INFORMATION....7
2. GETTING STARTED....8
    2.1. SYSTEM REQUIREMENTS....9
    2.2. INSTALLATION PROCEDURE....10
    2.3. CONNECTING TO THE INTERNET....15
    2.4. CREATING NEW USER PROFILE....21
    2.5. BUYING ADDITIONAL LICENSES....23
    2.6. UPDATING THE SOFTWARE....24
    2.7. GENERAL OVERVIEW OF USER INTERFACE....25
3. WORKING WITH BITRASER MOBILE ERASER & DIAGNOSTICS....27
    3.1. SETTINGS....28
    3.2. ERASURE STAGES....46
    3.2.1. ERASURE PROCESS....51
    3.2.1.1. ERASURE PROCESS FOR ANDROID DEVICES....53
    3.2.1.2. ERASURE PROCESS FOR iOS DEVICES....60
    3.2.1.3. ERASURE PROCESS FOR APPLE WATCHES....65
    3.3. DIAGNOSTIC STAGES....72
    3.3.1. DIAGNOSTIC PROCESS....77
    3.4. DETAILS SECTION....81
    3.5. WORKING ON REPORTS....86
    3.5.1. PREVIEW REPORT....90
    3.5.2. SAVE REPORT....92
    3.5.3. SEND REPORT TO BITRASER CLOUD....93
    3.5.4. CHANGE REPORT SETTINGS....94
    3.6. FORGOT LOGIN PASSWORD....96
    3.7. ENABLE USB DEBUGGING IN AN ANDROID DEVICE....98
4. FREQUENTLY ASKED QUESTIONS (FAQ)....103
5. LEGAL NOTICES....106
6. ABOUT STELLAR....113

1. GENERAL INFORMATION

1.1. About BitRaser Mobile Eraser & Diagnostics

1.2. About the Guide

1.3. Contact Information

1.1. INTRODUCTION

About BitRaser Mobile Eraser & Diagnostics

BitRaser Mobile Eraser & Diagnostics is a reliable application providing permanent Data Erasure and **Mobile Diagnostics** for mobile devices such as iPhones, iPads, Apple Watches, and Android devices.

Using the **BitRaser Data Erasure** process, data once erased cannot be recovered. This ensures that sensitive data does not fall in the wrong hands when mobile devices are disposed of, recycled, or sold. This software is used by organizations, refurbishers, and mobile data erasure companies to facilitate the safe disposal, reuse, or resale of mobile devices. 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 **Mobile Diagnostics** process enables quick identification of hardware problems for mobile devices running on iOS and Android. **BitRaser** diagnostics process helps determine the health status of various components such as the battery, camera, touch-pad, display, microphone, SIM card slots, RAM, internal memory, etc. of a mobile device through series of automated and assisted tests.

This application provides the user to generate an erasure or diagnostic report containing the result of the process. The report can be saved to a hard drive/external media or collected by the **BitRaser Cloud Console**.

BitRaser Mobile Eraser & Diagnostics is a product of **Stellar**.

Key Features of BitRaser Mobile Eraser & Diagnostics:

- Securely and permanently erase sensitive data from Android & iOS devices.
- Perform high-speed simultaneous erasure of up to 40 devices most efficiently.
- Cloud integration for user management, licenses & reports.
- Pay per use – No expiry of license.
- Provides an option to check the ESN Status of the mobile devices.
- Support to provide pre-report and asset details before the erasure/diagnostic process.
- Support to erase untrusted iOS devices.
- Option to erase device which has a Samsung Knox container.
- Device label printing available with the company logo and various parameters that can be customized as per requirement.
- Support for customizing general settings, user settings, iOS settings, Android settings, printer settings, and network settings.
- List view and Grid view option for the connected/erased/diagnosed devices.

- Provides an option to edit the USB port name for easy identification.
- Erases devices that are in recovery mode.
- Erase working iOS devices with broken screens.
- Supports 11 erasure methods:
    - NIST 800-88 Purge
    - Native OS Erasure
    - NIST 800-88 Clear
    - Zeroes (1 Pass)
    - Pseudo Random (2 passes)
    - US Department of Defense,DoD 5220.22-M (3 passes)
    - US Department of Defense,DoD 5200.22-M, ECE (7 passes)
    - B.Schneiers algorithm (7 passes)
    - Peter Gutmann (35 passes)
    - US Army AR 380-19 (3 passes)
    - US Air Force, AFSSI 5020 (3 passes)
    - British HMG IS5 (3 passes)
- Reporting:
    - Generate 100% secure and tamper-proof reports.
    - Provides an option to preview the runtime report.
    - Option to save erasure/diagnostic reports in various formats such as PDF, XML, and CSV.
    - Fast and user-friendly report searching (including search by date).
    - Automatically saves erasure reports on the same computer from which erasure is performed.
    - Automatic report delivering to **BitRaser Cloud Console**.
    - Option to customize report layout as per requirements.
    - Full visibility of hardware and erasure details for customized reporting.
- Devices Supported:
    - **Android**: All devices with Android OS version 5.0 and above
    - **iPhones**: iPhone 16, iPhone 16 Plus, iPhone 16 Pro, and iPhone 16 Pro Max, iPhone 15 pro max, iPhone 15 Pro, iPhone 15 Plus, iPhone 15, iPhone 14 Pro Max, iPhone 14 Pro, iPhone 14 plus, iPhone 14, iPhone 13 Pro Max, iPhone 13 Pro, iPhone 13, iPhone 13 Mini, iPhone 12 Pro Max, iPhone 12 Pro, iPhone 12, iPhone 12 Mini, iPhone SE (2nd Generation), iPhone 11 Pro Max, iPhone 11 Pro, iPhone 11, iPhone XS Max, iPhone XS, iPhone XR, iPhone X, iPhone 8, iPhone 8 Plus, iPhone 7, iPhone 7 Plus, iPhone 6S, iPhone 6S Plus, iPhone 6, iPhone 6 Plus, iPhone SE, iPhone 5S, iPhone 5C, iPhone 5, iPhone 4S

- **iPads**: iPad Air 4th Gen, iPad 8th Gen, iPad Pro 4th Gen, iPad 7th Gen, iPad Mini 5th Gen, iPad Air 3rd Gen, iPad Pro 3rd Gen, iPad 6th Gen, iPad Pro 2nd Gen, iPad 5th Gen, iPad Pro, iPad Mini 4, iPad Mini 3, iPad Air 2, iPad Mini 2, iPad Air, iPad Mini, iPad 4th Gen, iPad 3rd Gen, iPad 2
- **Apple Watches**: Apple Watch Series 1, 2, 3, 4, 5 and Series SE
- **iPod Touch**: All generations

1.2. ABOUT THE GUIDE

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

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

1. General Information
2. Getting Started
3. Working with BitRaser Mobile Eraser & Diagnostics
4. Frequently Asked Questions (FAQ)

This guide is intended for individuals who use **BitRaser Mobile Eraser & Diagnostics** to erase or diagnose mobile devices running iOS and Android.

- There are ***Cautions***, ***Notes***, and ***Tips*** in some topics of this guide for your understanding and ease of work. ***Cautions*** are given in yellow boxes and ***Notes*** and ***Tips*** are given in *italics* style for easy identification.

Definition of acronyms used in this guide:

ITEM	EXPLANATION
ECID	The ECID (Exclusive Chip Identification also referred to as Unique Chip ID in official Apple terms) is an identifier unique to every Apple device.
IMEI	IMEI (International Mobile Equipment Identity) is a 15- or 17-digit code that uniquely identifies mobile phone sets.
JPG or JPEG	Stands for Joint Photographic Experts Group. JPG or JPEG is a standard file format for compressing pictures so they can be stored or sent by e-mail more easily.
PDF	"Portable Document Format" is a file format designed to present documents consistently across multiple devices and platforms.
PNG	Portable Network Graphics (PNG) is a raster-graphics file-format for image compression.
User ID	Stands for User identification, which by default is the e-mail address of the user in this guide.
XML	"Extensible Markup Language" is a metalanguage that allows users to define their customized markup languages, especially to display documents on the Internet.

For any queries or feedback related to this guide, kindly contact us.

1.3. CONTACT INFORMATION

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

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

2. GETTING STARTED

2.1. System Requirements

2.2. Installation Procedure

2.3. Connecting to the Internet

2.4. Creating a New User Profile

2.5. Buying Additional Licenses

2.6. Updating the Software

2.7. General Overview of User Interface

2.1. SYSTEM REQUIREMENTS

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

Minimum System Requirements:

- **Processor**: x86 or x64 Processor
- **RAM**: 1 GB Minimum (4 GB Recommended)
- **Hard Disk**: 20 GB of free space
- **iOS Version for Device Erasure:** All versions supported
- i**OS Version for Device Diagnostics:** 12.0 and above
- **Android Version for Device Erasure or Diagnostics:** 5.0 and above
- **Devices Supported:**
  - **Android**: All devices with Android OS version 5.0 and above
  - **iPhones**: iPhone 16, iPhone 16 Plus, iPhone 16 Pro, and iPhone 16 Pro Max, iPhone 15 pro max, iPhone 15 Pro, iPhone 15 Plus, iPhone 15, iPhone 14 Pro Max, iPhone 14 Pro, iPhone 14 plus, iPhone 14, iPhone 13 Pro Max, iPhone 13 Pro, iPhone 13, iPhone 13 Mini, iPhone 12 Pro Max, iPhone 12 Pro, iPhone 12, iPhone 12 Mini, iPhone SE (2nd Generation), iPhone 11 Pro Max, iPhone 11 Pro, iPhone 11, iPhone XS Max, iPhone XS, iPhone XR, iPhone X, iPhone 8, iPhone 8 Plus, iPhone 7, iPhone 7 Plus, iPhone 6S, iPhone 6S Plus, iPhone 6, iPhone 6 Plus, iPhone SE, iPhone 5S, iPhone 5C, iPhone 5, iPhone 4S
  - **iPads**: iPad Air 4th Gen, iPad 8th Gen, iPad Pro 4th Gen, iPad 7th Gen, iPad Mini 5th Gen, iPad Air 3rd Gen, iPad Pro 3rd Gen, iPad 6th Gen, iPad Pro 2nd Gen, iPad 5th Gen, iPad Pro, iPad Mini 4, iPad Mini 3, iPad Air 2, iPad Mini 2, iPad Air, iPad Mini, iPad 4th Gen, iPad 3rd Gen, iPad 2
  - **Apple Watches**: Apple Watch Series 1, 2, 3, 4, 5 and Series SE
  - **iPod Touch**: All generations

***Note**: You need an active internet connection.*

***Caution**: Installing **BitRaser Mobile Eraser & Diagnostics** on your computer or laptop will format the hard drive to create partitions. Backup all your data from your computer before installing **BitRaser Mobile Eraser & Diagnostics**.*

2.2. INSTALLATION PROCEDURE

***Caution**: Installing **BitRaser Mobile Eraser & Diagnostics** on your computer or laptop will format the hard drive to create partitions. Backup all your data from your computer before installing **BitRaser Mobile Eraser & Diagnostics**.*

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

When you buy licenses for **BitRaser Mobile Eraser & Diagnostics**, you can receive the software in two ways: You can receive a **BitRaser Mobile Eraser & Diagnostics** bootable media (USB drive or DVD) from **Stellar**, or you can receive a link to download a **BitRaser Mobile Eraser & Diagnostics ISO file**.

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

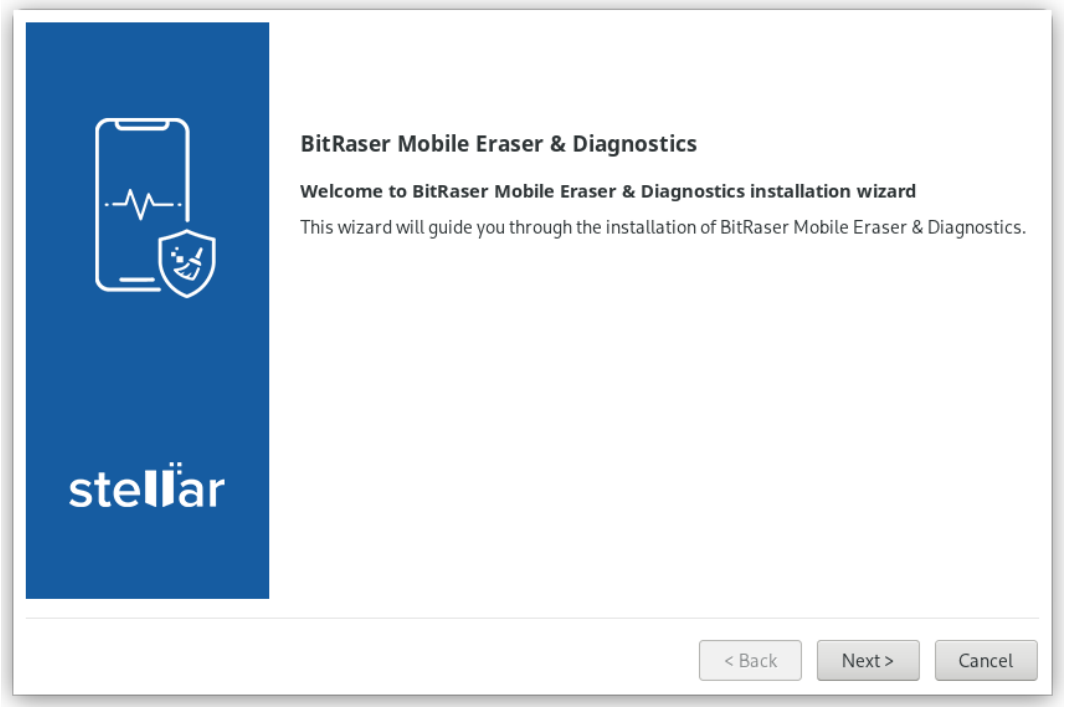
Installation Steps:

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

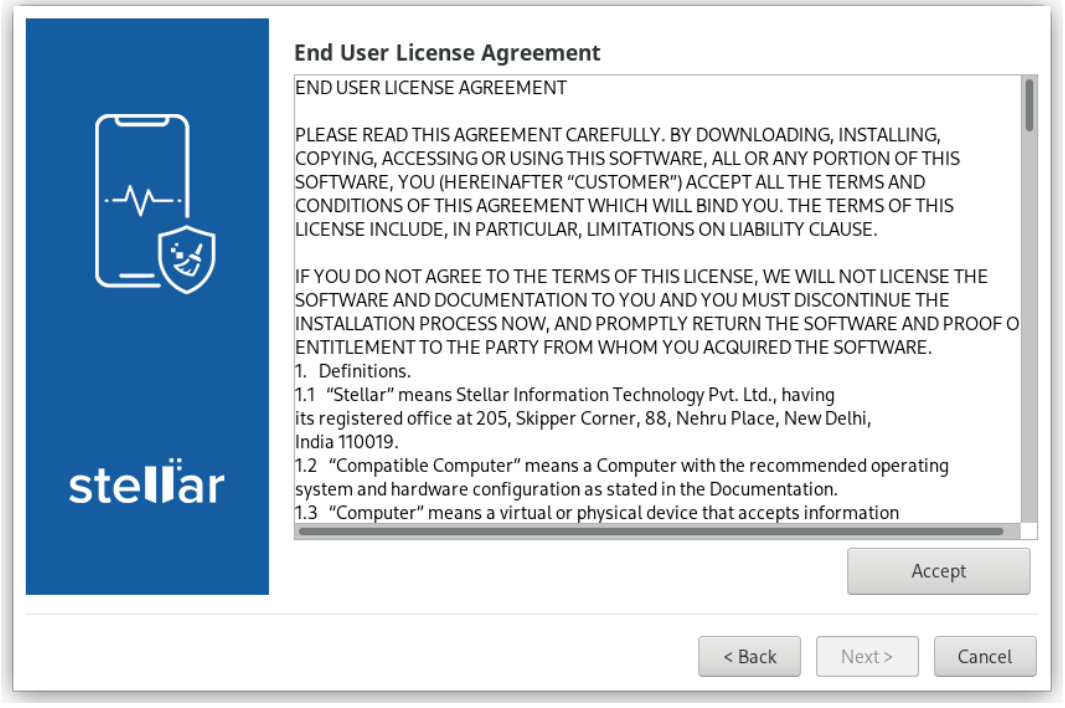
1. Power on your computer and check the BIOS boot options to boot from the bootable media (USB drive or DVD).

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

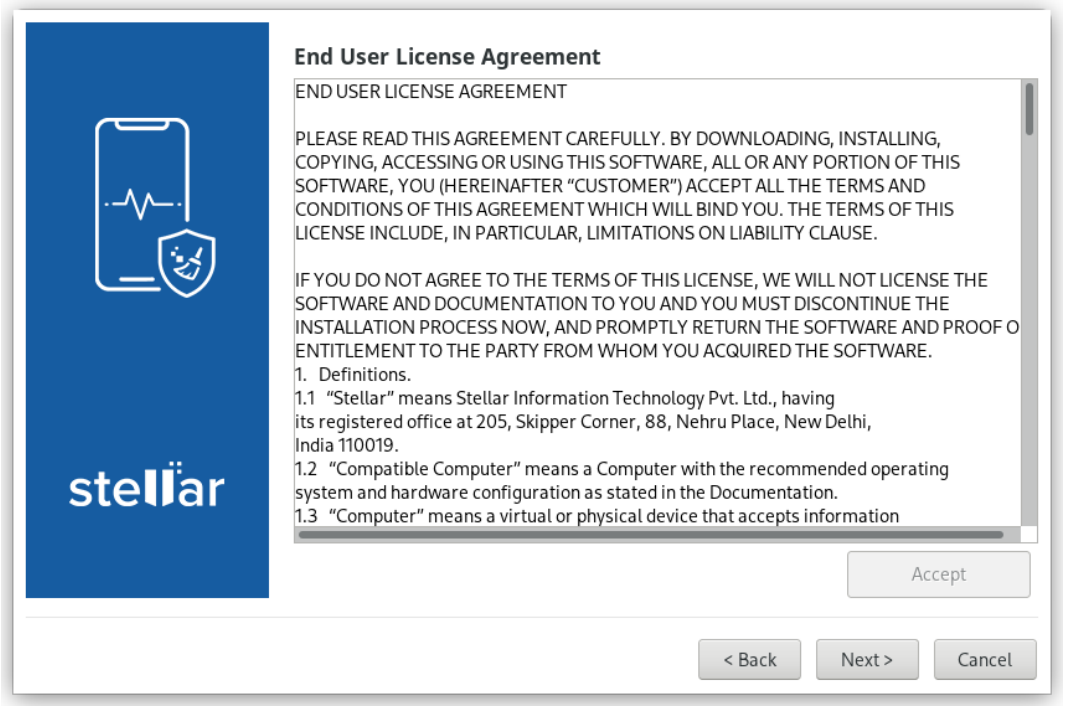
2. Once the computer boots, you will see the "**BitRaser Mobile Eraser & Diagnostics**" screen. Click **Next** to install **BitRaser Mobile Eraser & Diagnostics** on your computer.



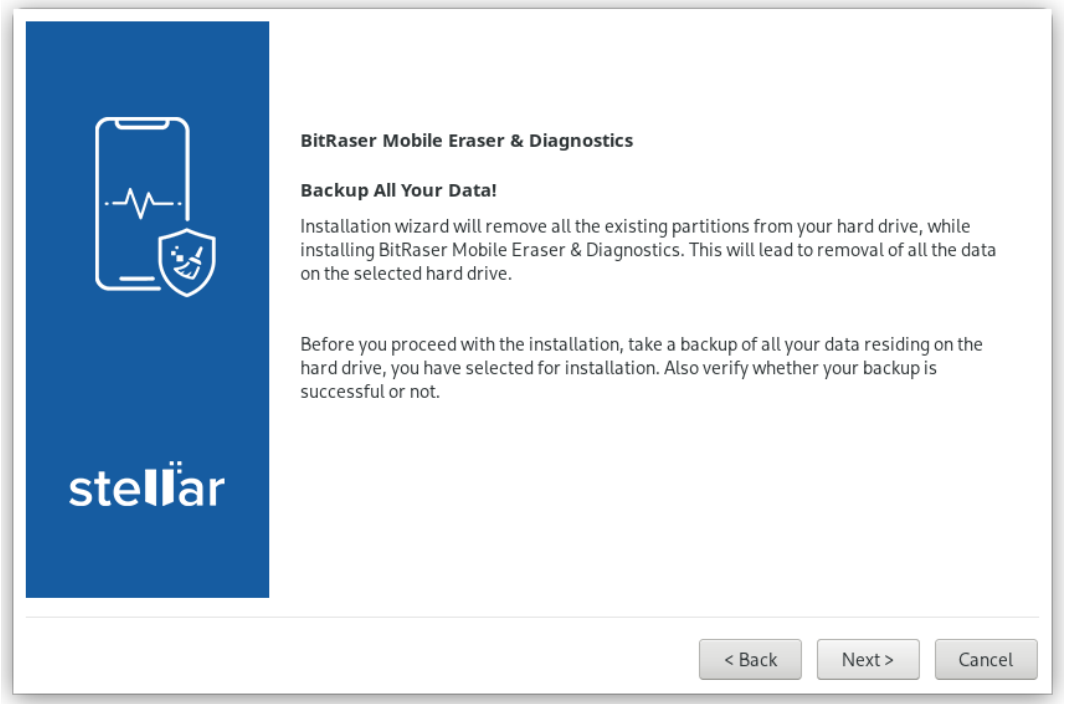
3. **End User License Agreement** screen is displayed. Click **Accept** to enable the **Next** button.



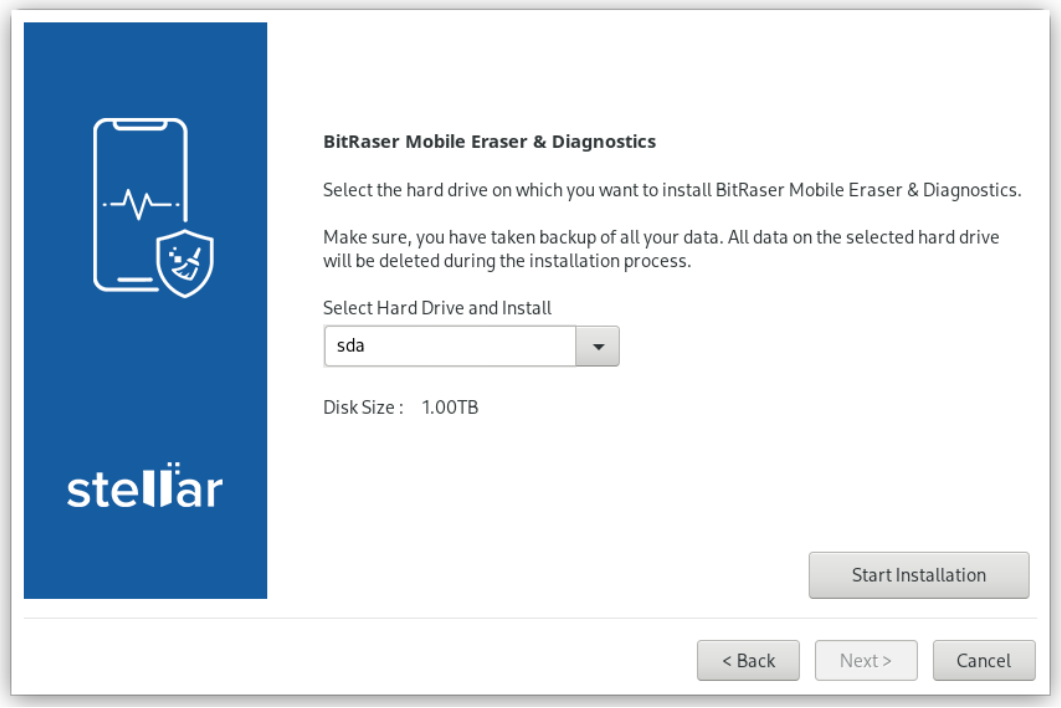
4. Click the **Next** button to proceed.



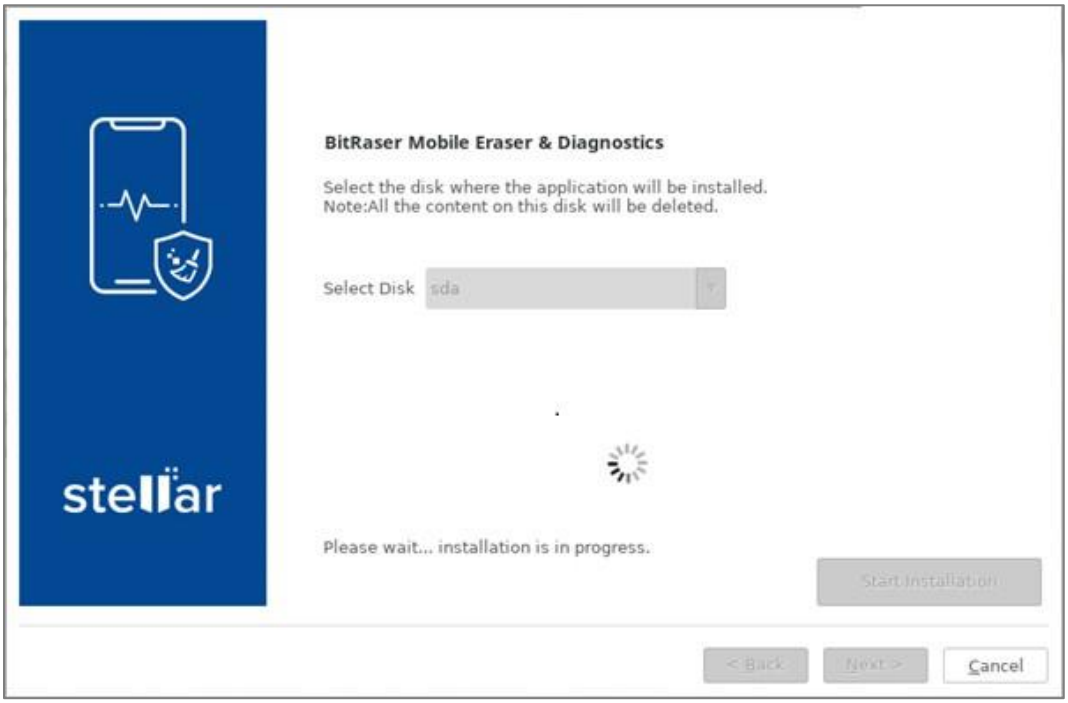
5. **Backup all your Data** window is displayed. Click **Next** to open **BitRaser Mobile Eraser & Diagnostics** screen.



6. Using the **Select Disk** drop-down option, click on the hard drive name on which you want to install **BitRaser Mobile Eraser & Diagnostics**.

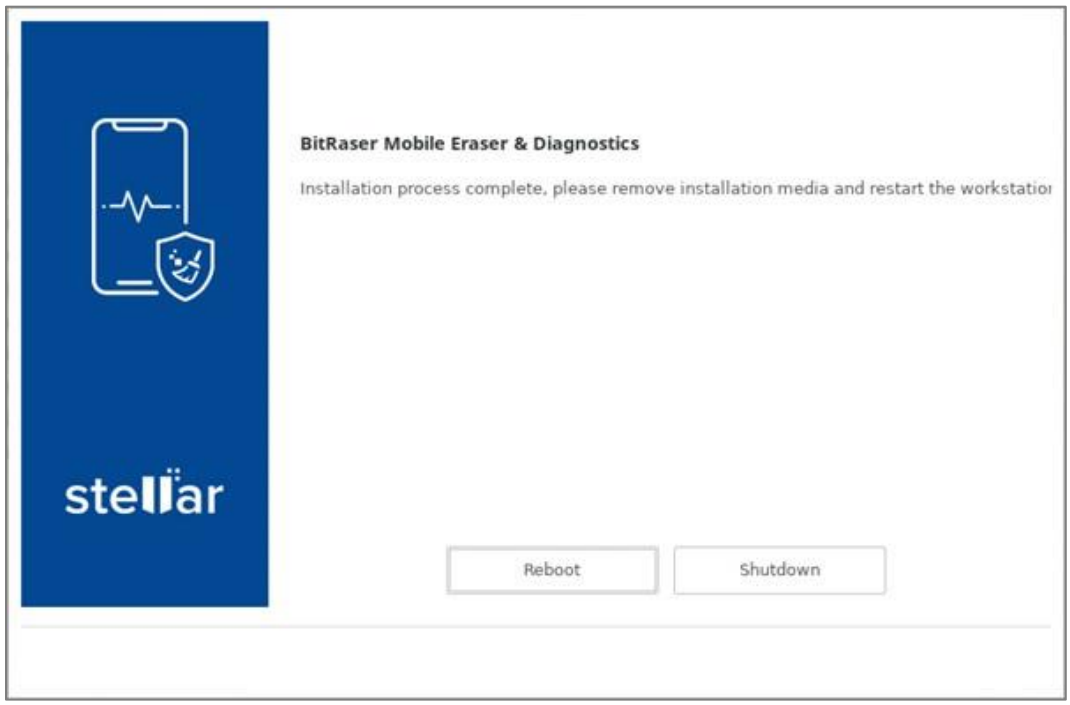


7. Click **Start Installation**. "**Please wait… installation is in progress"** message shows that the installation has started.



8. After the installation process is completed, a screen appears as shown below. Remove installation media from your system and click on **Reboot** button to restart the workstation.

   Note: *if you want to turn off your computer system, click* ***Shutdown*** *button.*



2.3. CONNECTING TO THE INTERNET

Once the **BitRaser Mobile Eraser & Diagnostics** is installed and started, it asks you to connect to the internet and the **Network Settings** dialog is displayed on startup:

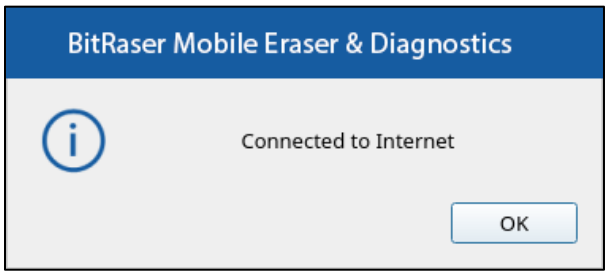
Network Settings has the following four tabs:

1. **Ethernet**: Use this tab to connect to the internet using the Ethernet or LAN connection of your computer. This tab has the following fields:

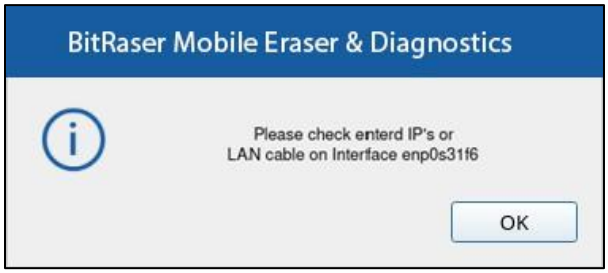
- **Network Device**: Use this field to select the Network Device from the drop down options, with which you wish to connect the **BitRaser Mobile Eraser & Diagnostics** application to the internet.

- **Configuration**: Use this field to select **Manual** or **Automatic** Internet Protocol (IP) configuration from the drop down options.
    - **Manual Configuration**: The Manual configuration is selected in this field by default. This configuration has the following fields to fill:
        - IP Address
        - Net Mask
        - Gateway
        - DNS Primary
        - DNS Secondary
    - **Automatic Configuration**: This configuration has the following fields to fill:
        - DHCP Hostname
        - Name Servers

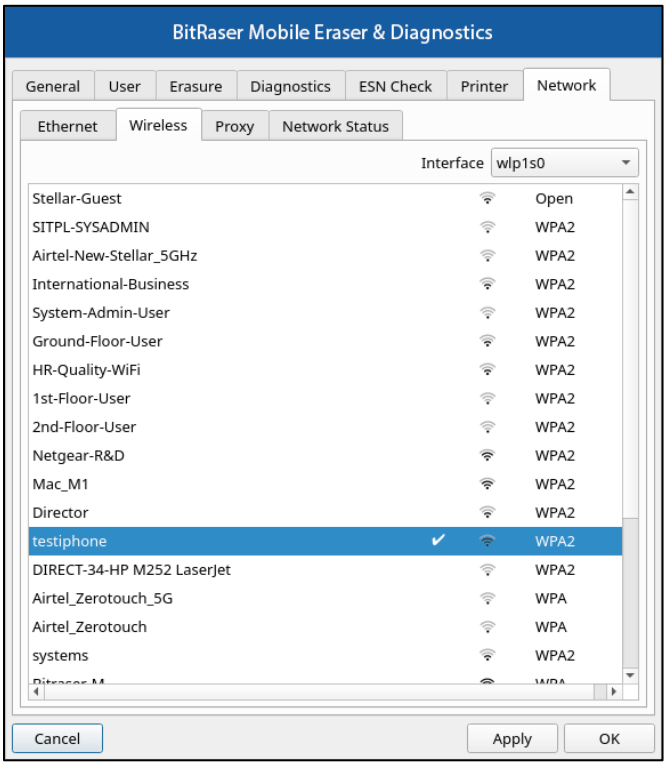
To connect to the internet through Ethernet, select the Network Device and Configuration. Enter the fields as given above and click **Connect**. The following dialog box shows that **BitRaser Mobile Eraser & Diagnostics** is successfully connected to the internet:



Alternatively, if the entered details are incorrect or the LAN cable is not connected, the following dialog box appears:

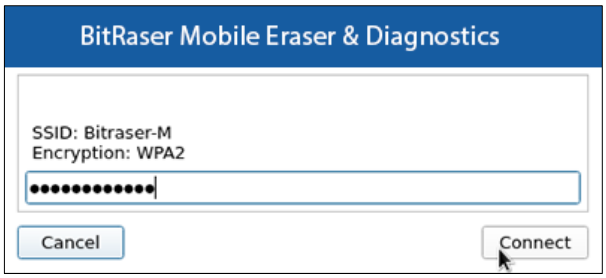


2. **Wireless**: BitRaser Mobile Eraser & Diagnostics also allows you to connect to the internet through the wireless device of your computer.

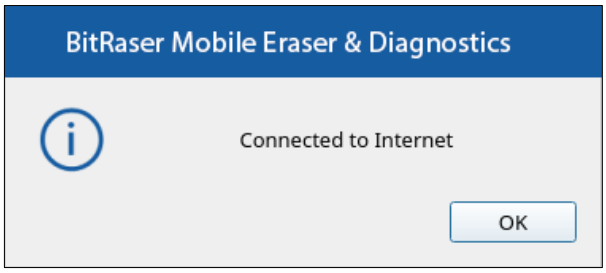


To do this:

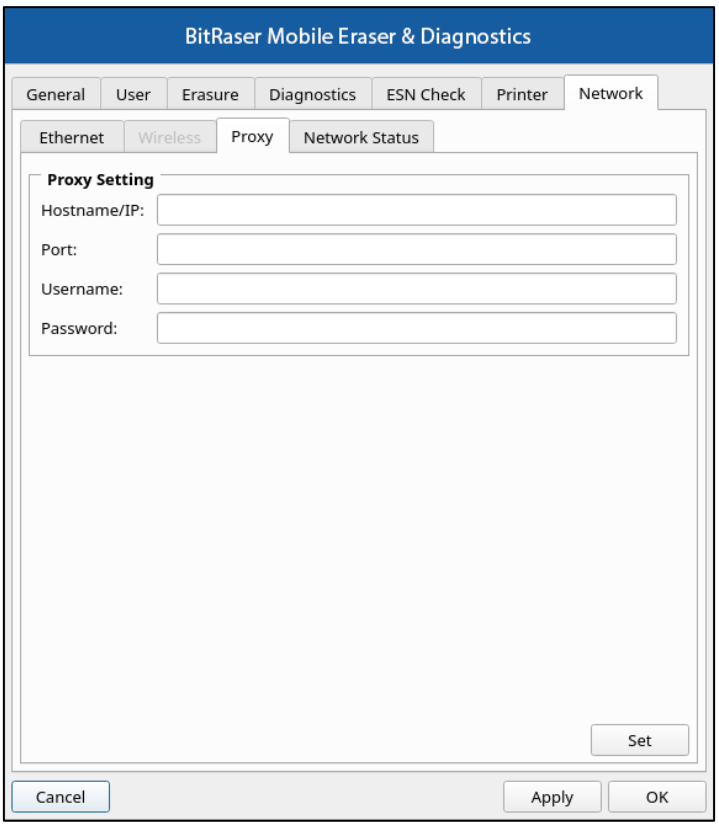
- Select the wireless device from the **Interface** drop-down option. BitRaser Mobile Eraser & Diagnostics automatically scan and displays the list of wireless networks available to connect.
- Double click on the wireless network from the list.
- If the network is secured, it asks you for the password. Enter the password and click **Connect:**



- The following dialog box shows that **BitRaser Mobile Eraser & Diagnostics** is successfully connected to the internet:



3. **Proxy**: BitRaser Mobile Eraser & Diagnostics gives an option to connect to a **Proxy** server if required.

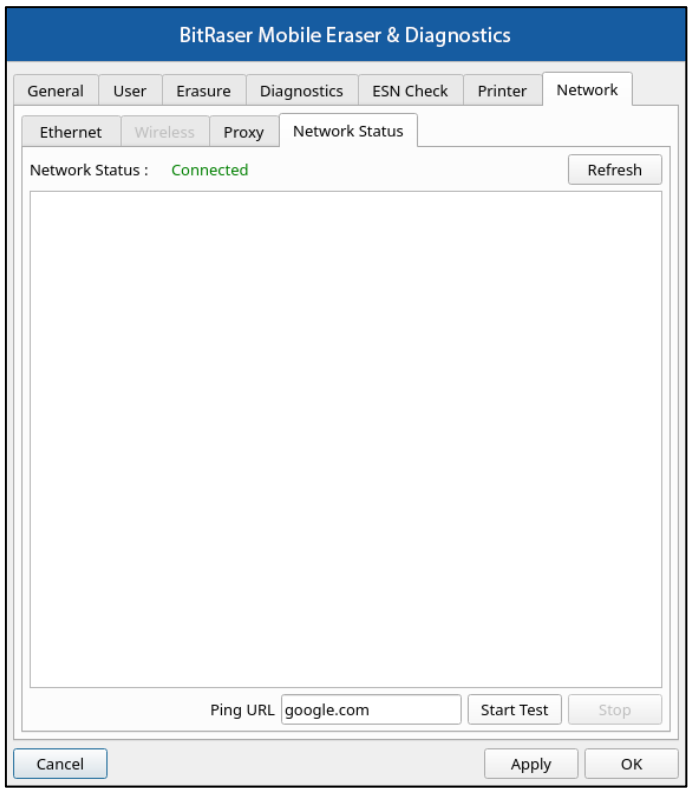


The following fields need to be filled:

FIELD NAME	DESCRIPTION
Hostname/IP	Enter the address of the proxy server.
Port	Enter the port number that the proxy server uses.
Username	Enter the proxy user name.
Password	Enter the authentication password of the proxy user.

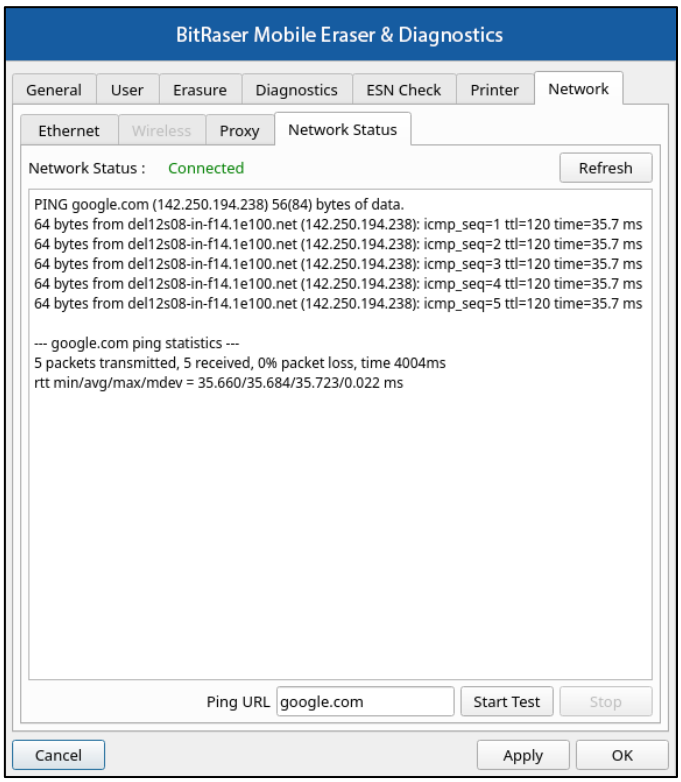
Click on **Set** to save your preferences.

4. **Network Status**: This tab shows the status of the network - **Connected** or **Disconnected**. The Refresh Button allows you to refresh the network status. This tab also has an option to ping a particular URL to check the network connectivity.



To ping a URL:

- Enter any URL, such as ***bitraser.com***, in the **Ping URL** field, and click on **Start Test**.
- If the network is connected successfully, this option will show a reply from the URL in bytes of data, similar to the screen given below:



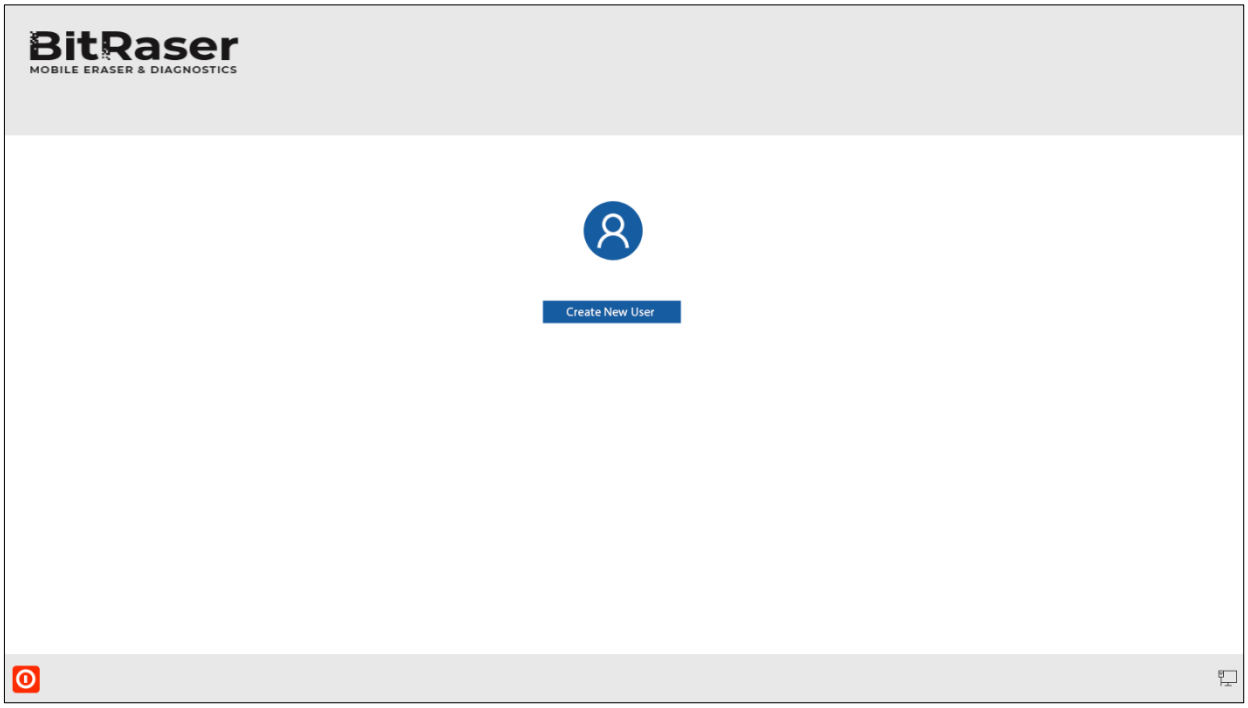
Click on **OK** to save the network settings and close the window or **Cancel** to close the window without saving.

Note: *At any point in time, if you wish to open the network settings again, double click on the Network icon in the bottom right of the screen.*

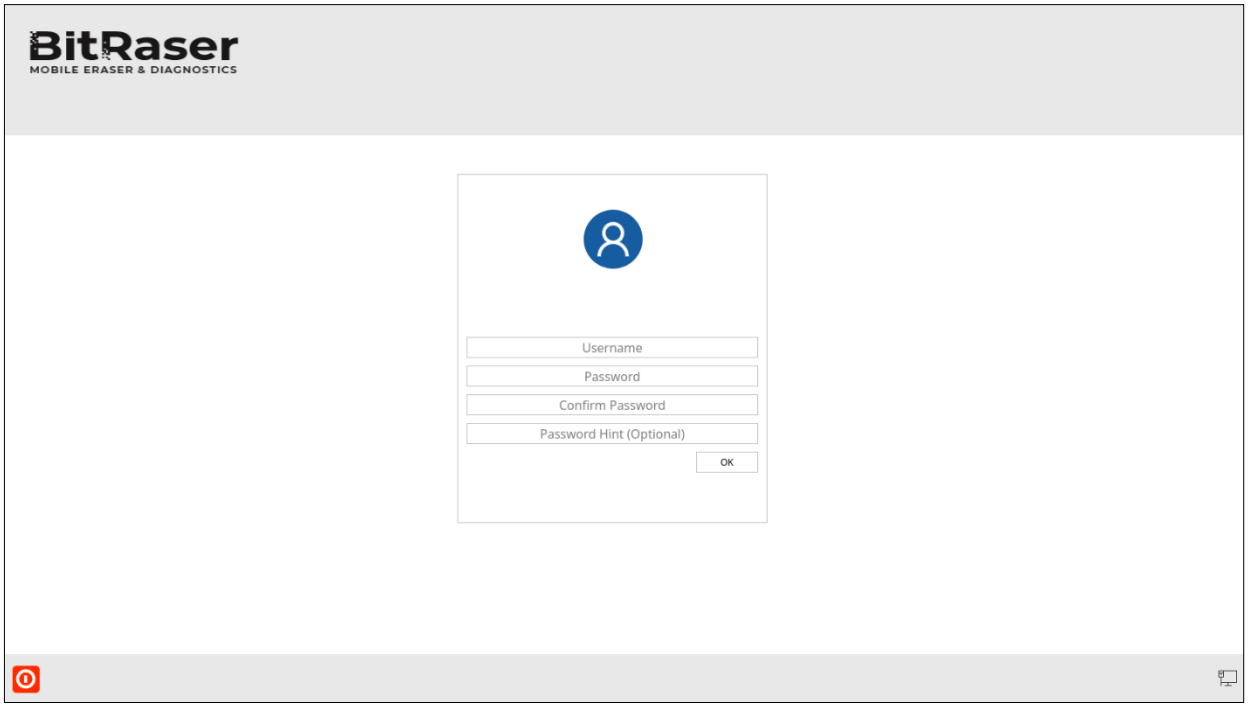
2.4. CREATING NEW USER PROFILE

When you run the **BitRaser Mobile Eraser & Diagnostics** for the first time, it asks you to create a new user profile. To create a new user profile, do the following steps:

1. Click on **Create New User** button.



2. The following screen appears with the fields to fill:



- Username
- Password
- Confirm Password
- Password Hint (Optional)

3. Fill in the above fields and click **OK.**
4. You can now login to **BitRaser Mobile Eraser & Diagnostics** using the new user credentials.

***Note**: The new user profile is only to log in to **BitRaser Mobile Eraser & Diagnostics** application. This option does not create a profile to login to **BitRaser Cloud**. The credentials to log in to **BitRaser Cloud** are created separately.*

2.5. BUYING ADDITIONAL LICENSES

You can purchase the additional licenses from https://www.bitraser.com. New licenses will be added to the registered account.

To purchase the licenses for BitRaser Mobile Eraser & Diagnostics, follow these steps:

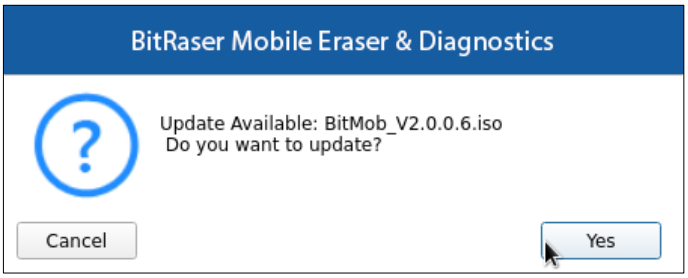
1. Go to https://www.bitraser.com/
2. Click **Buy Now** button.
3. Select the tab **BitRaser Mobile Eraser & Diagnostics**.
4. From the available license options, select the number of licenses you want to purchase.
5. Click **BUY NOW** button.
6. After you complete the payment and enter the required details, click **Buy Now** button. The licenses are sent on the e-mail address along with the BitRaser Cloud log-in credentials for license management and distribution.

***Note**: You need to use the same email-id given at the time of the first purchase to add the additional licenses to your account. In case a different email-id is entered, a new cloud log-in account will be created with the purchased licenses.*

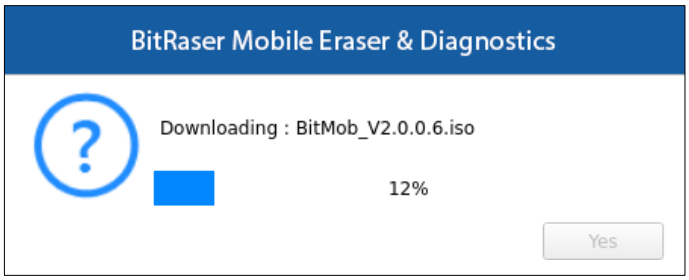
2.6. UPDATING THE SOFTWARE

Stellar releases periodical software updates for **BitRaser Mobile Eraser & Diagnostics** software. You can update the software to keep it up-to-date. These updates can add new functionality, feature, service, or any other information that can improve the software.

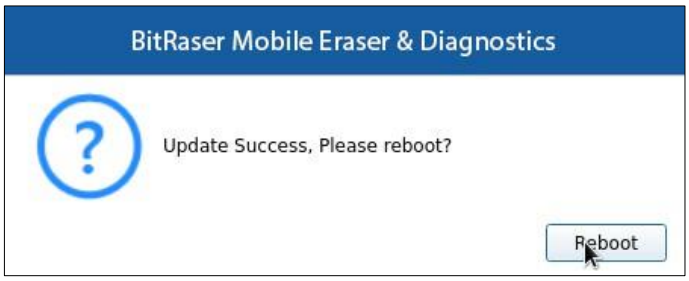
BitRaser Mobile Eraser & Diagnostics automatically check for software updates as soon as it is connected to the internet. If an update is available, **BitRaser Mobile Eraser & Diagnostics** will show a dialog to update the software as shown below:



1. Click **Yes** to start the ISO downloading process. The download dialog appears as follows:



2. Once the download is completed successfully, **Update Success** message appears as shown below:



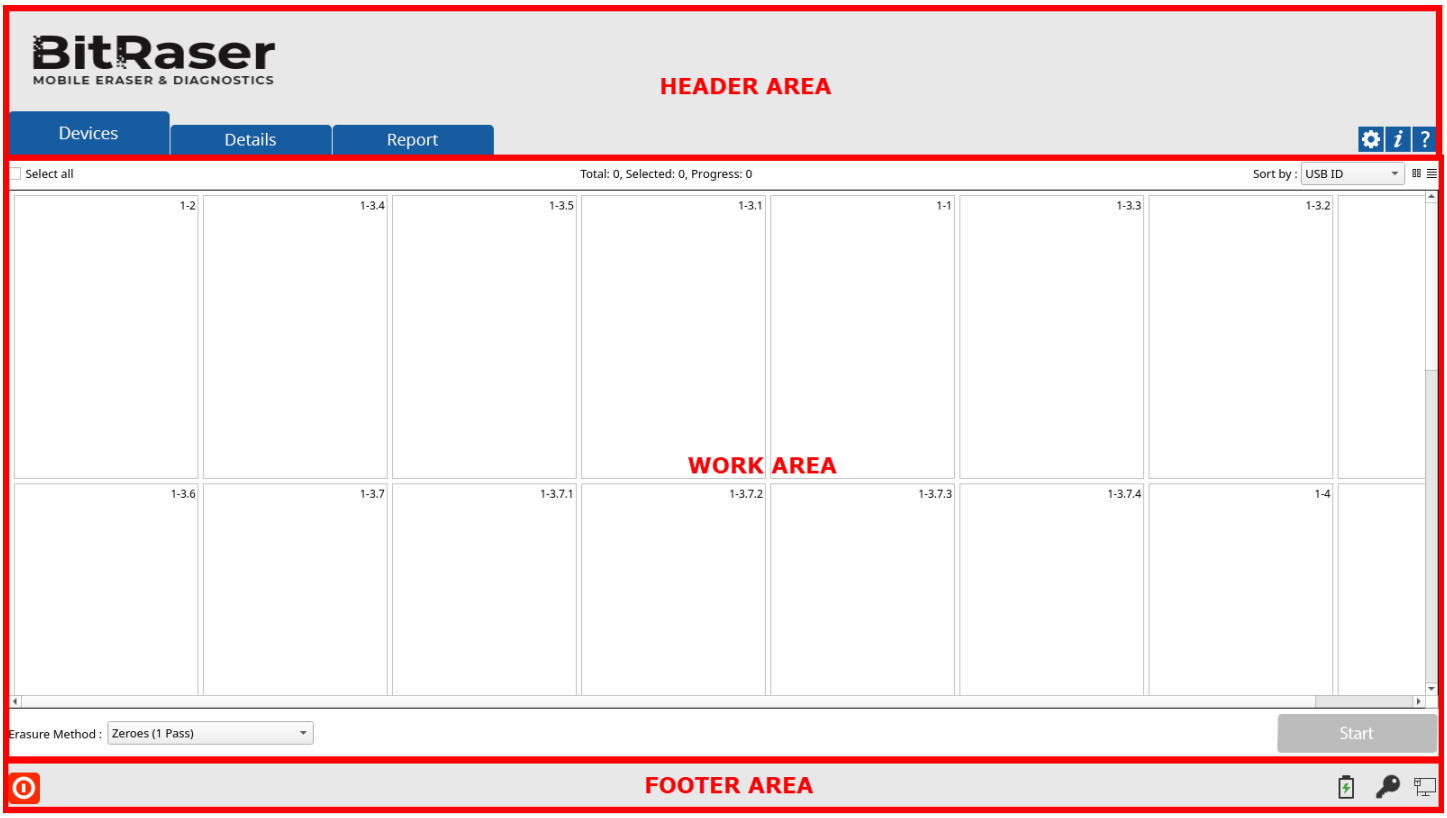
3. Click **Reboot** to install and update **BitRaser Mobile Eraser & Diagnostics**.

***Note**: **BitRaser Mobile Eraser & Diagnostics** also keep the previous version installed on your computer along with the latest version.*

2.7. GENERAL OVERVIEW OF USER INTERFACE

The user interface is divided into three main areas:

1. Header area
2. Work area
3. Footer area



1. **Header Area**: The header area contains the following tabs and buttons:

- **Devices Tab**

: This tab contains a list the connected devices in grid or list view and is used to perform erasure and diagnostic process.

- **Details Tab**

: This tab is used to enter various details to be included in reports. To know more, refer to the Details Section.

- **Report Tab**

: This tab provides a list of **BitRaser Mobile Eraser & Diagnostics** reports and various options for Working on Reports.

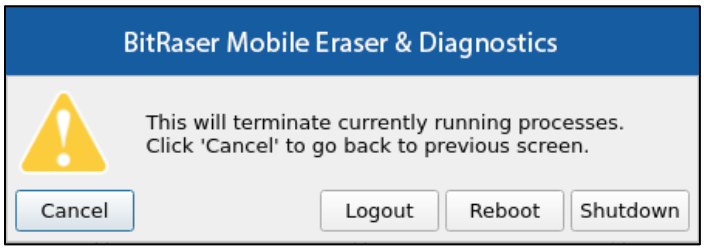
- **Settings Button** : Click this button to update various settings available for **BitRaser Mobile Eraser & Diagnostics**.

- **About Button** : Click this button to see information about **BitRaser Mobile Eraser & Diagnostics**.
- **Help Button** : Click this button to open this help guide from the application.

2. **Work Area**: The work area contains all the specific information and functionality of the selected tab or button.

3. **Footer Area**: The footer area contains the following buttons:

- **Power Button** : Click this button to logout, reboot, or shutdown **BitRaser Mobile Eraser & Diagnostics.** The following screen appears:



- **License Key Button** : Click this button to view the **BitRaser Mobile Eraser & Diagnostics** license information. If you are not connected to **BitRaser Cloud**, this button opens the **User Settings** for login authentication.
- **Network Button** or : Click this button to check the current status of the network. Double click to open the **Network Settings**. A red cross mark on this button shows that **BitRaser Mobile Eraser & Diagnostics** is not connected to the network.
- **Battery Icon** **:** This icon shows the battery status of the laptop.

  Note: *This feature is not available for PC's.*

3. WORKING WITH BITRASER MOBILE ERASER & DIAGNOSTICS

3.1. Settings

3.2. Erasure Stages

3.2.1. Erasure Process

3.3. Diagnostic Stages

3.3.1. Diagnostic Process

3.4. Details Section

3.5. Working on Reports

3.5.1. Preview Report

3.5.2. Save Report

3.5.3. Send Report to BitRaser Cloud

3.5.4. Change Report Settings

3.6. Forgot Login Password

3.7. Enable USB Debugging in an Android Device

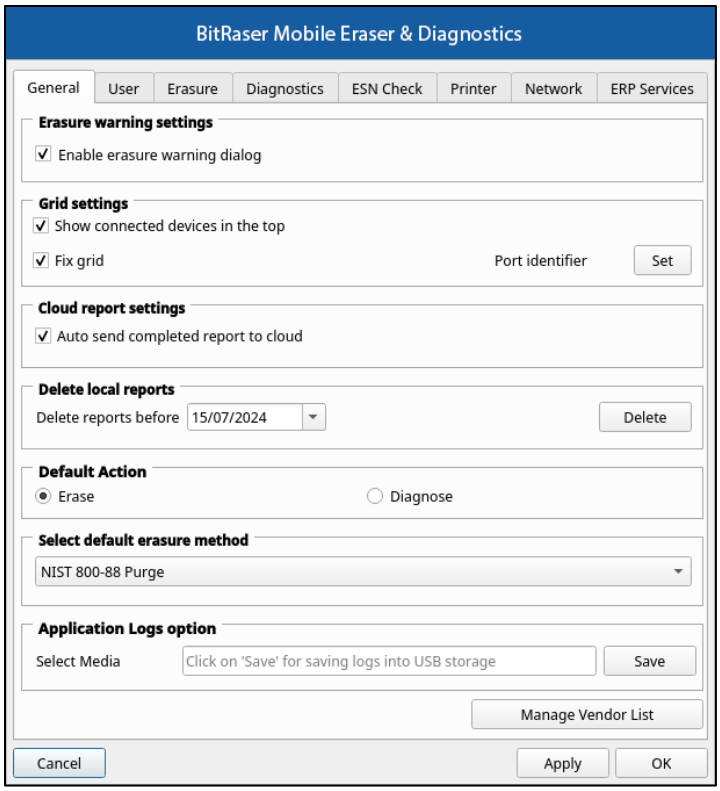
3.1. SETTINGS

Before starting an Erasure or a Diagnostic process, it is important to understand and configure various settings of **BitRaser Mobile Eraser & Diagnostics**. After the first login, the **Settings** window appears automatically. Alternatively, click on the **Settings** icon on the top right corner of the screen. Use this window to change the various general and default settings of the software. This window has the following tabs:

1. General Settings
2. User Settings
3. Erasure Settings
4. Diagnostic Settings
5. ESN Check
6. Printer Settings
7. Network Settings
8. ERP Services

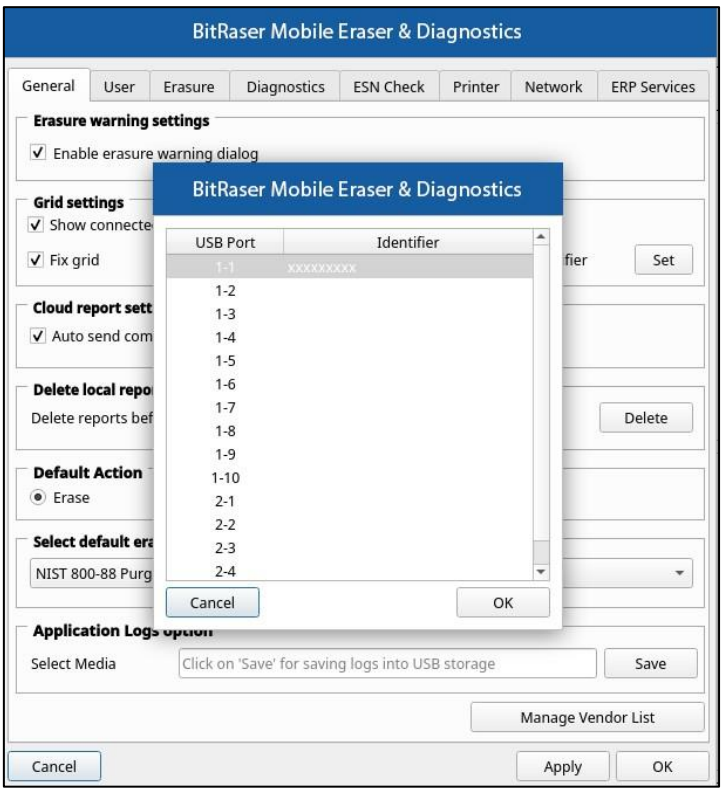
1. General Settings:

The General Settings tab allows you to configure erasure warning settings, grid settings, cloud report settings, delete the local reports and select the default erasure method.



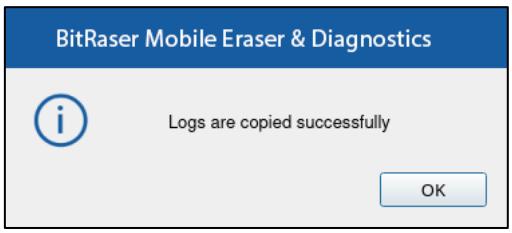
The following fields can be edited from this section:

- **Erasure Warning Settings:**
    - **Enable Erasure Warning Dialog:** Check this field to enable the warning message before the initiation of the erasure process.
- **Grid Settings**: This option allows you to set the layout of the grid which is shown when we connect the devices.
    - **Column**: Allows you to predefine the number of columns in a grid.
    - **Port Identifier**: Allows you to predefine name of each port to identify the port easily. Click on **Set**. The popup window shows a list of USB ports. Type the name against each port in the **Identifier** column and click **OK** to save or **Cancel** to exit without saving:



- **Show connected devices at the top of the grid**: Checking this field allows you to display the connected devices at the starting of the grid.
- **Fix Grid**: Checking this field allows you to fix the grid columns i.e., they cannot be moved.

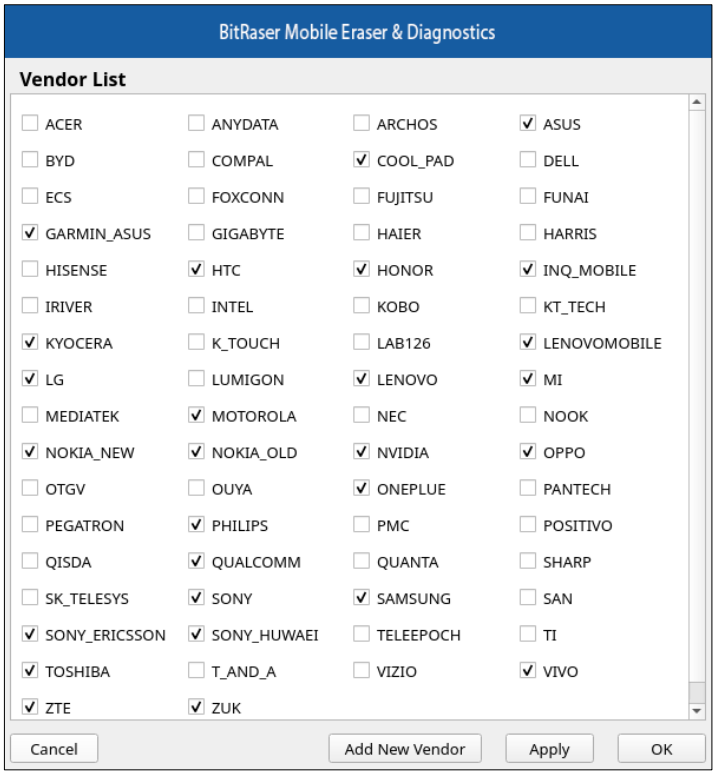
- **Cloud Report Settings**:
  - **Auto send report to cloud**: Checking this field allows you to auto-send the report to the cloud.
- **Delete Local Reports**:
  - **Delete Reports before**: This option allows you to delete the reports before a certain date. Specify the date from the calendar and click the **Delete** button. All the reports generated before the selected date will be deleted.
- **Default Action**: Select a default option of **Erase** or **Diagnose**, when you connect a device to **BitRaser Mobile Eraser & Diagnostics**.
- **Select Default Erasure Method**: Select any one of the erasure methods from the drop-down options to set the default erasure method for all devices.
- **Application Logs option**: This option allows you to save the log files at the desired destination path. Click **Save Logs** to select the path of a USB device where the log file will be saved. After selecting the path, the log files are copied to the destination and a message appears as shown below, click **OK**.



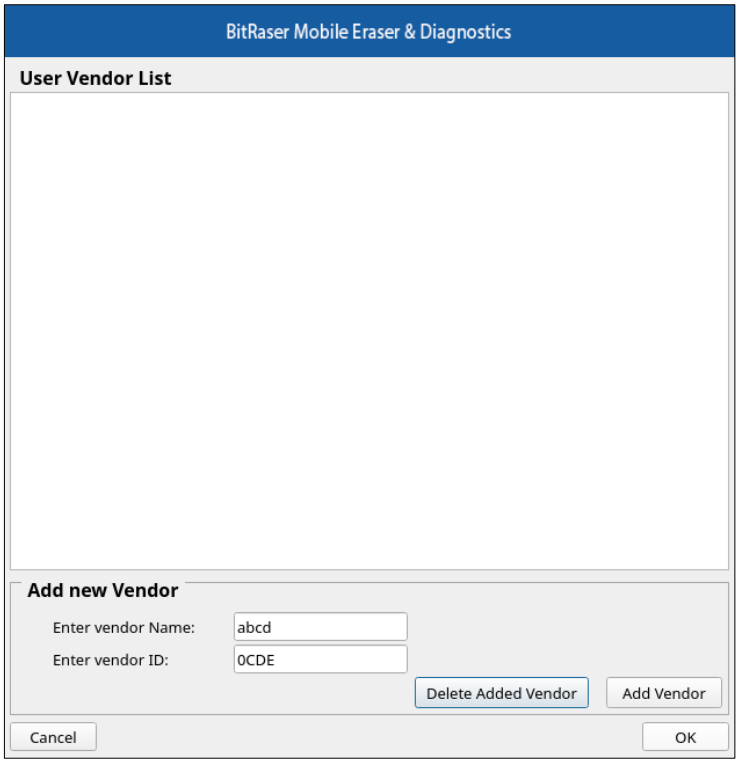
- **Manage Vendor List:** Click this button to add or list the mobile vendor manually, if mobile vendor is not recognized by the system.

  Steps to add mobile vendors name manually:

  - Click **Manage vendor list** located below right in the **General** tab.
  - **Vendor List** screen appears, this screen is displayed list of mobile vendors name.



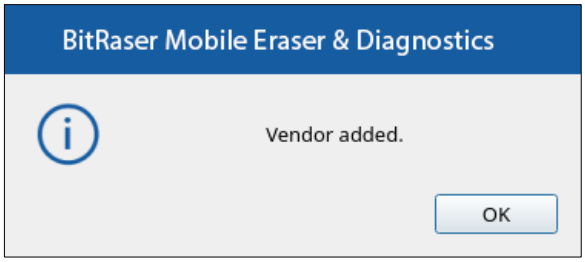
  - Check mobile vendor name from this screen, if the vendor name is available check that checkbox and click **Apply** to list mobile vendor name in the main user interface.
  - If mobile vendor name is not found in the **Vendor List** screen, click **Add New Vendor** button to add name of mobile vendor manually.
  - **User Vendor List** screen appears. In **Add new Vendor** section, enter vendor **Name** and **ID**.



- Click **Add Vendor** button to list the vendor name in **User Vendor List** section.

  ***Note**: If you wish to delete any vendor from the **User Vendor List** section, click **Delete Added Vendor** button.*

- **Vendor added** screen appears as shown below, click **OK** to continue.

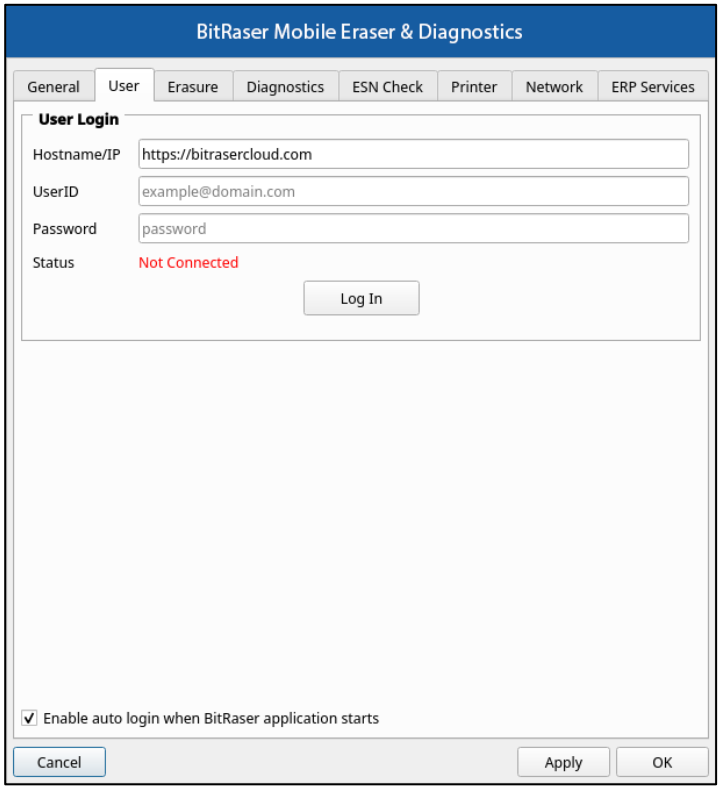


- After the vendor name is added under **User Vendor List**, click **OK** to continue further and **Cancel** to exit the screen.

Once the settings have been modified, click the **Apply** button to save the changes. **OK** applies all the changes to the software and closes the Settings menu, **Cancel** closes the Settings menu without saving the changes.

2. User Settings:

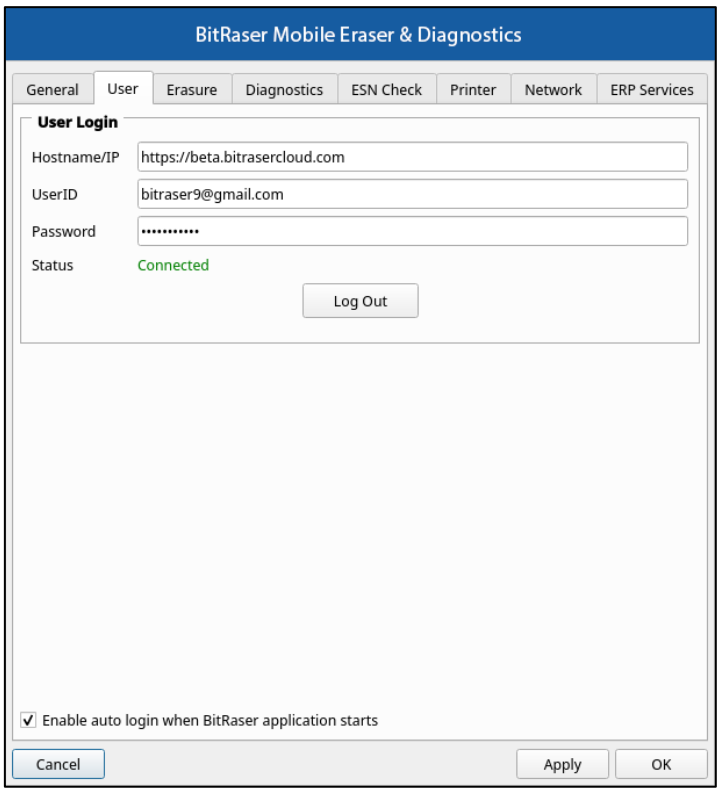
User settings allow you to connect **BitRaser Mobile Eraser & Diagnostics** application to the **BitRaser Cloud**. Connection to **BitRaser Cloud** is required to acquire the license information and to initiate the erasure or diagnostic process.



The following fields have to be filled:

FIELD NAME	DESCRIPTION
Hostname / IP	Hostname or IP address where the BitRaser Cloud Console is located.
UserID	UserID that is used to login to the BitRaser Cloud Console.
Password	Password which is used to login to the BitRaser Cloud Console.
Status	**Connected**: Shown when the connection to the BitRaser Cloud Console is active. **Not Connected**: Shown when there is no active connection to the BitRaser Cloud Console.

After you have entered the values in all the fields, click **Log In** to login to the **BitRaser Cloud Console**.



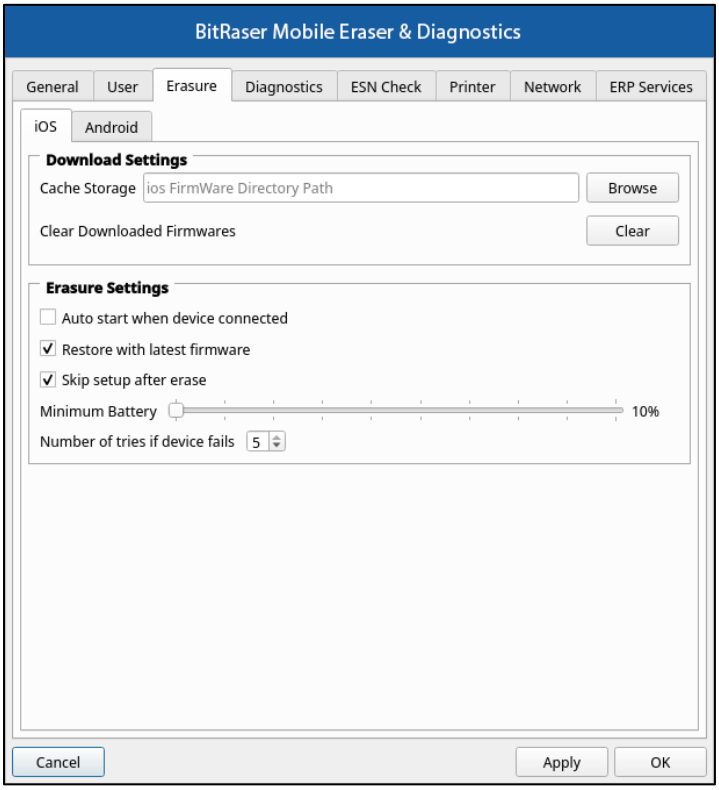
Checking **Enable auto login when BitRaser Mobile Eraser & Diagnostics starts** option allows you to automatically login to the **BitRaser Cloud Console** when you start **BitRaser Mobile Eraser & Diagnostics** application.

Once the settings have been modified, click **Apply** button to save the changes. **OK** applies all the changes to the software and closes the Settings menu, **Cancel** closes the Settings menu without saving the changes.

3. Erasure Settings:

The Erasure setting tab has the following two sub-tabs:

A. iOS Settings:



The iOS settings tab displays the firmware download and erasure settings. The following fields can be edited from this section:

- **Download Settings:**
  - **Cache Storage:** This option allows you to select the desired location where the firmware is located. Click **Browse** button and specify the path using **Look In** dialog box. After selecting the path, click **OK**.
  - Click **Clear** button to remove the downloaded iOS firmware from your hard drive.

- **Erasure Settings:**

  It has minimum battery and number of trials parameter which must be defined to erase the data:

  - **Auto start when device connected:** Checking this option allows you to automatically start the erasure process once device is connected.
  - **Restore with latest Firmware:** Checking this option allows you to erase an IOS device by restoring the latest firmware.

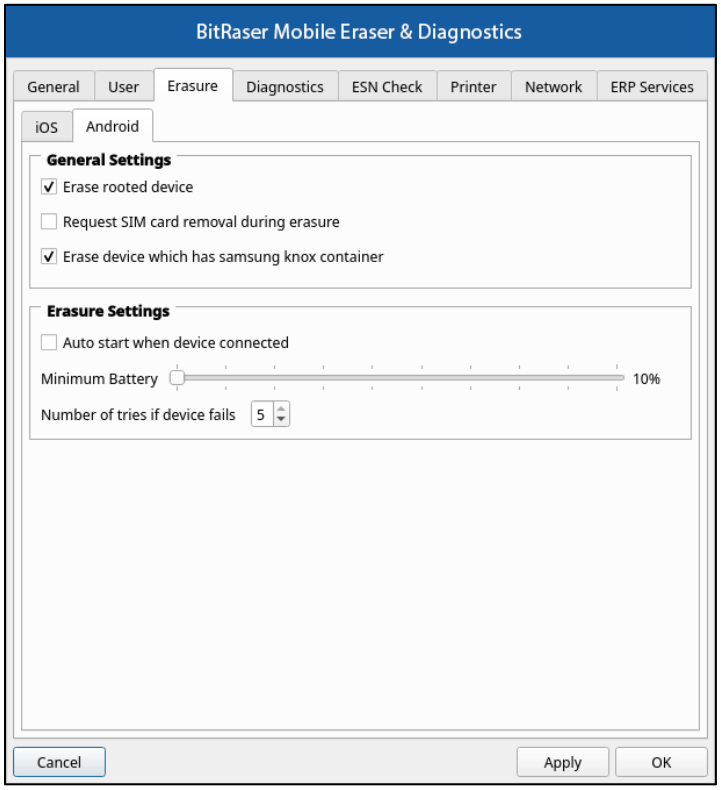
- **Skip Setup:** This checkbox is enabled by default, allowing you to activate the phone and bypass or skip the UI setup. You have the option to uncheck the box if you prefer not to skip setting up your device.

  ***Note**: The Skip Setup feature won't function when either FMIP or MDM is enabled on the device, or if the device is in recovery mode.*

- **Minimum Battery**: You can define the minimum battery percentage using the slider. This represents the minimum battery required to erase the device's data. For example: If you set the slider to 20 % it means that at least 20% battery should be there in your device for the Erase process to take place.
- **Number of tries if the device fails**: Allows you to define the maximum amount of retries/attempts for the erasure process to start if in case the device is disconnected/removed in the middle of the erasure process.

Once the settings have been modified, click **Apply** button to save the changes. **OK** applies all the changes to the software and closes the Settings menu, **Cancel** closes the Settings menu without saving the changes.

B. Android Settings:



The Android settings tab displays general and erasure settings. The following fields can be edited from this section:

- **General Settings:**

- **Erase rooted device:** Checking this option allows you to erase an Android device even if it is rooted.
- **Request SIM card removal during erasure**: Checking this option will show a message to remove the SIM card from the device before the erasure process starts.
- **Erase device which has Samsung Knox container**: Checking this option allows you to erase an Android device that has a Samsung Knox container.

- **Erasure Settings:**

  It has minimum battery and number of trials parameter which must be defined to erase the data:

  - **Minimum Battery**: You can define the minimum battery percentage using the slider. This represents the minimum battery required to erase the device's data. For example: If you set the slider to 20% it means that at least 20% battery should be there in your device for the Erase process to take place.

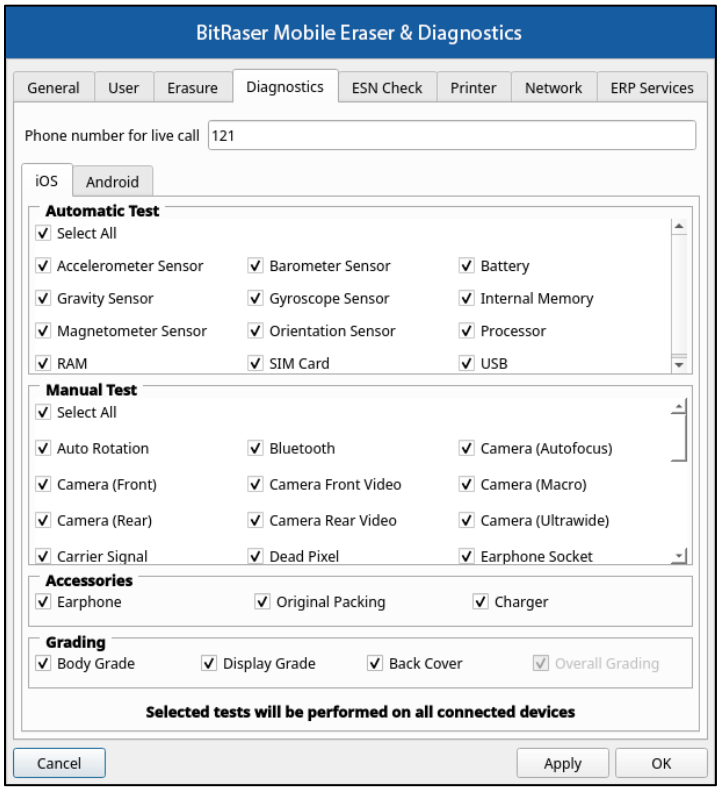
  - **Number of tries if the device fails**: Allows you to define the maximum amount of retries/attempts for the erasure process to start if in case the device is disconnected/removed in the middle of the erasure process.

Once the settings have been modified, click **Apply** button to save the changes. **OK** applies all the changes to the software and closes the Settings menu, **Cancel** closes the Settings menu without saving the changes.

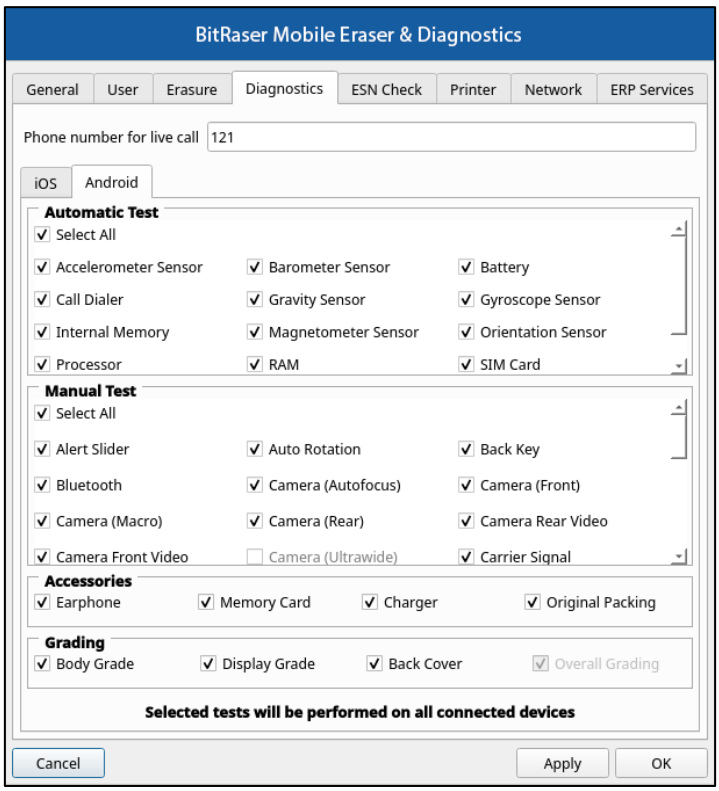
4. Diagnostic Settings:

The Diagnostic setting tab has the following two sub-tabs:

- **iOS Settings:**



- **Android Settings:**

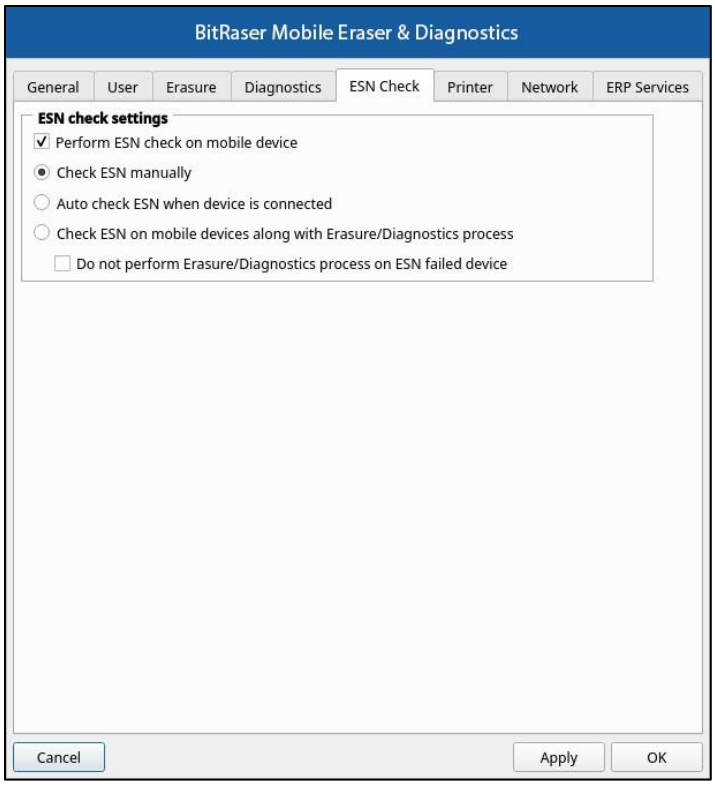


These tabs have lists of automatic tests, manual tests, accessories, and grading options. The tests which are checked will be performed on the connected devices.

Once the settings have been modified, click **Apply** button to save the changes. **OK** applies all the changes to the software and closes the Settings menu, **Cancel** closes the Settings menu without saving the changes.

5. ESN Check:

An ESN (Electronic Serial Number) check detects whether a phone is stolen, lost, or blacklisted. Using this tab you can choose a appropriate option for ESN check while performing Erasure/Diagnostics process.



The following fields can be selected from ESN check setting sections:

- **Perform ESN check on mobile device:** Check this field to enable the following options to perform ESN check on selected mobile devices.
  - **Check ESN manually:** Select this option to check the ESN status manually.
  - **Auto check ESN when device is connected:** Select this option to check the ESN status automatically, when the mobile devices is plugged-in.
  - **Check ESN on mobile devices along with Erasure/Diagnostics process:** Choose this option, if you want ESN to be checked automatically while performing Erasure/Diagnostics.
  - **Do not perform Erasure/Diagnostics process on ESN failed device:** Select this checkbox if you do not want to perform Erasure/Diagnostics process on ESN failed devices.

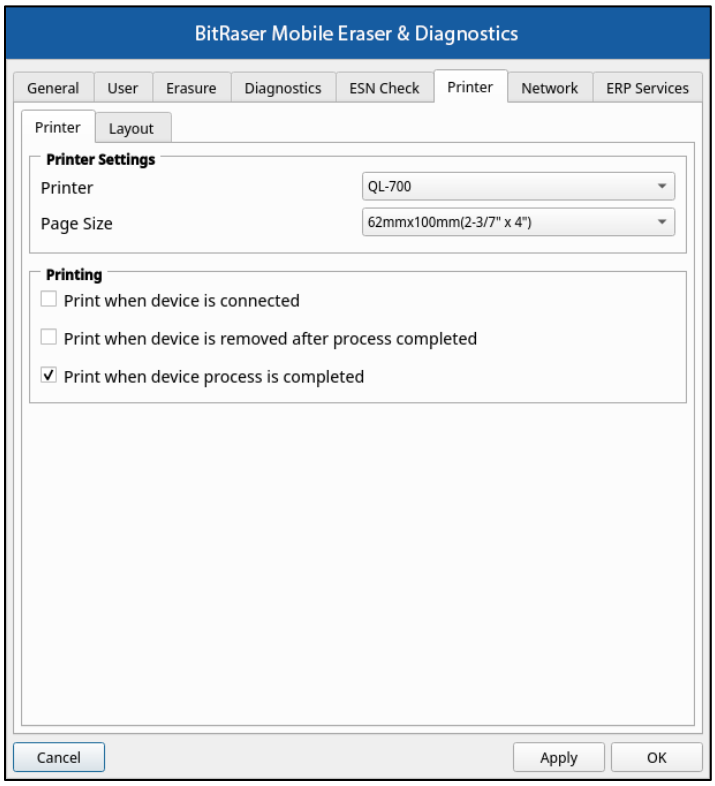
Once the settings have been modified, click the **Apply** button to save the changes. **OK** applies all the changes to the software and closes the Settings menu, **Cancel** closes the Settings menu without saving the changes.

6. Printer Settings:

This option allows you to print the information on the connected devices.

It has the following two tabs:

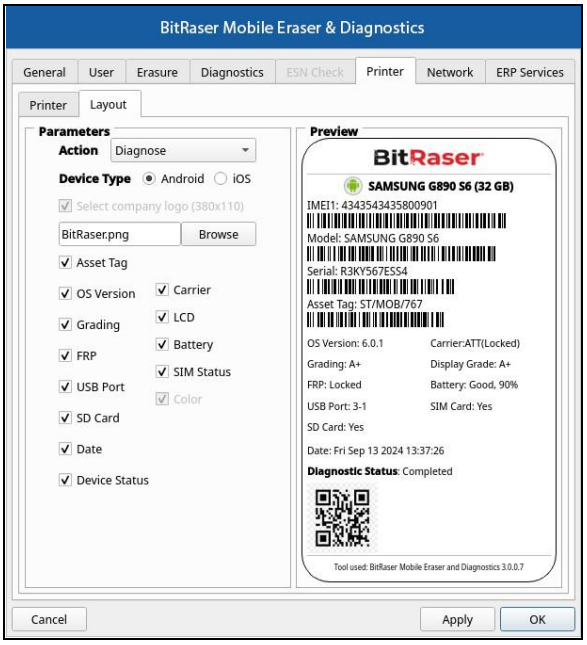
A. Printer:

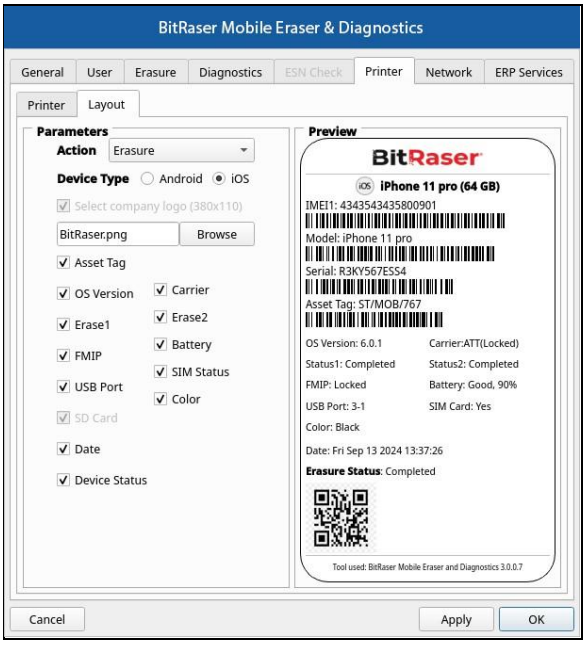


- **Printer Settings:**
  - **Printer:** Allows you to select a printer from the drop-down list.
  - **Page Size:** Choose the appropriate paper size from the drop-down list that you can print on.
- **Printing:**
  - To generate a print when you connect the device, select the option **Print when device is connected**.
  - To generate a print when you disconnect the device after the erasure or diagnostic process, select the option **Print when device is removed after process completed**.
  - To generate a print when the erasure or diagnostic process is completed, select the option **Print when device process is completed**.

B. Layout:

Android **iOS**





The layout tab allows you to select a list of parameters such as Action (Erasure or Diagnostics), Device Type (Android or iOS), Company Logo, Asset Tag, OS Version, and so on, for printing the device label. It also shows you the print preview of the label with all the device details selected by you.

The **QR code** displayed below the erasure / diagnostic completion status provides easy access to the report of the erased devices. Scan the QR code to instantly receive a **PDF** version of the report.

Once the settings have been modified, click **Apply** button to save the changes. **OK** applies all the changes to the software and closes the Settings menu; **Cancel** closes the Settings menu without saving the changes.

Note: BitRaser Mobile Eraser & Diagnostics *currently supports only* ***Brother QL-700*** *and the* ***Dymo Label Writer 450*** *brands of label makers. These labels are very useful for asset tagging and managing device inventory.*

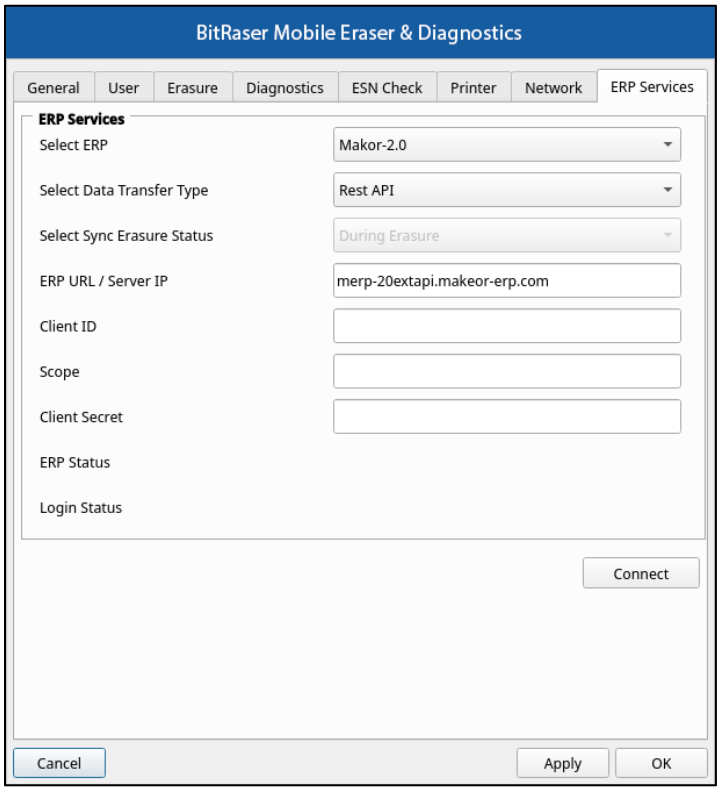
7. Network Settings:

The Network settings have been defined in the Connecting to the Internet section of this help guide.

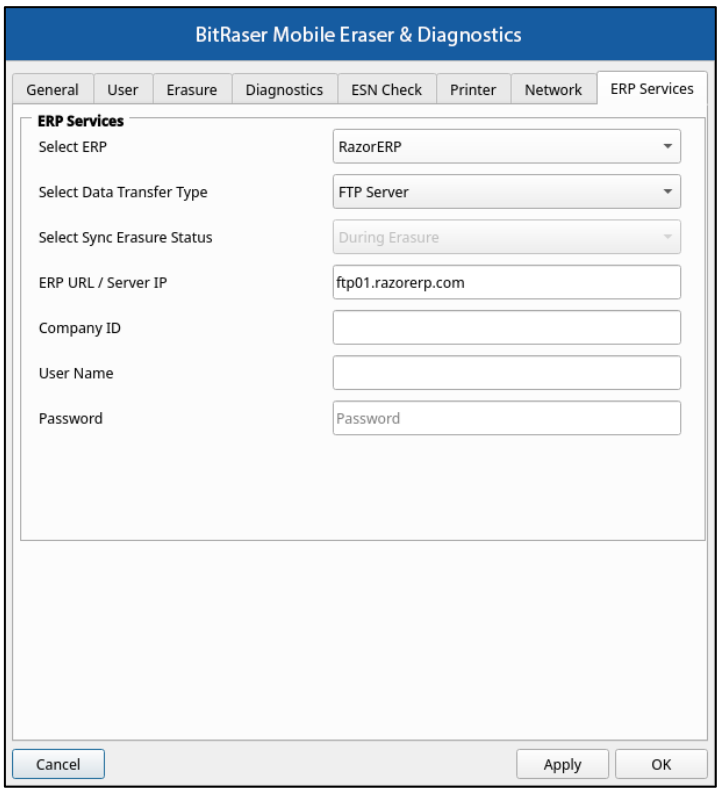
8. ERP Services:

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

Makor-2.0



RazorERP


BitRaser Mobile Eraser & Diagnostics
General
User
Erasure
Diagnostics
ESN Check
Printer
Network
ERP Services
ERP Services
Select ERP
RazorERP
Select Data Transfer Type
FTP Server
Select Sync Erasure Status
During Erasure
ERP URL / Server IP
ftp01.razorerp.com
Company ID
User Name
Password
Password
Cancel
Apply
OK

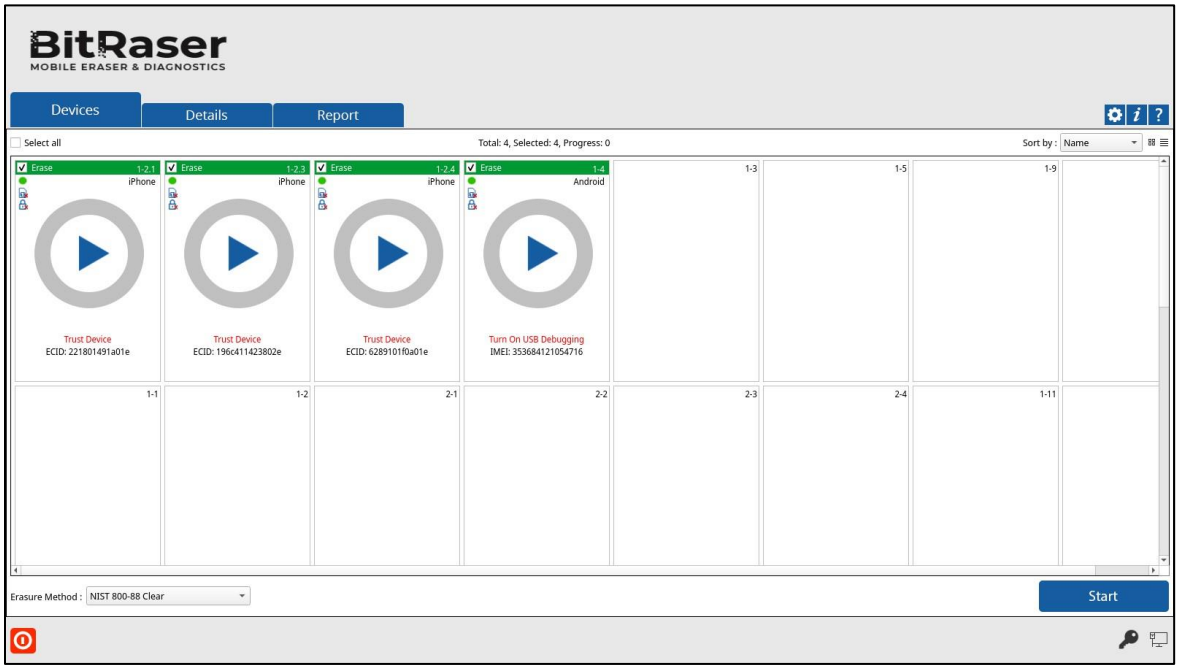
3.2. ERASURE STAGES

Before the completion of the erasure process, a series of steps take place while we erase a device. The erasure stages are as follows:

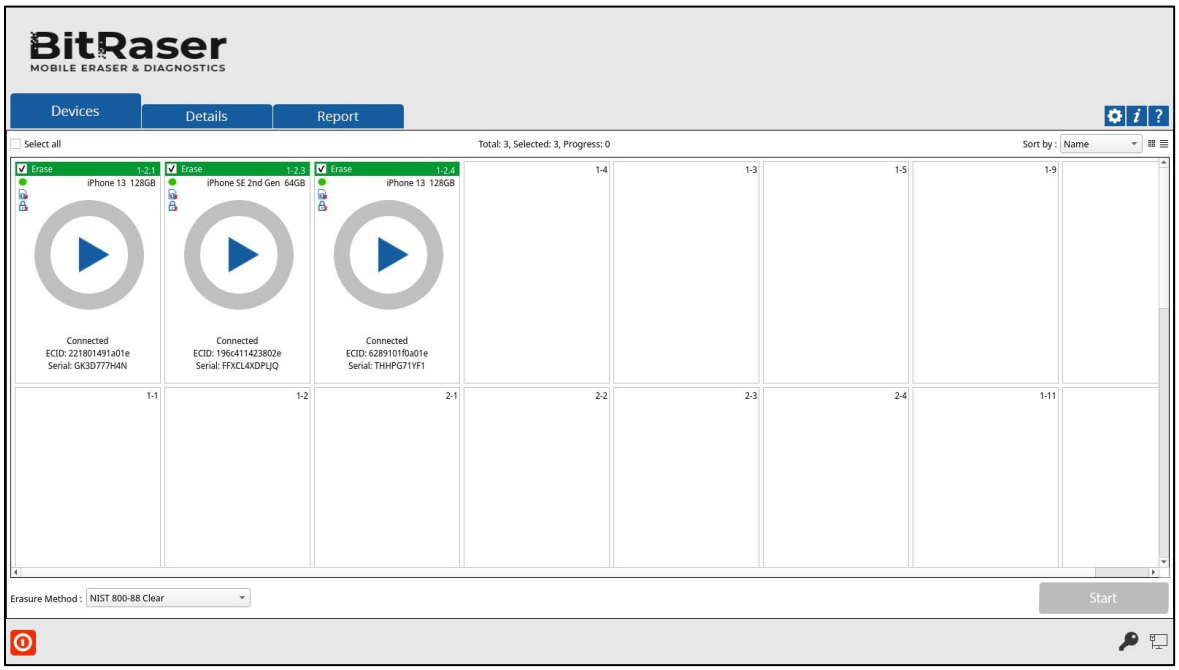
1. Device Connection
2. Initialization
3. Firmware Downloading
4. Restoration
5. Erasure

***Caution**: Make sure you do not interrupt the process by disconnecting the device or pressing the power button at any stage. Doing so might fail the process and harm your device.*

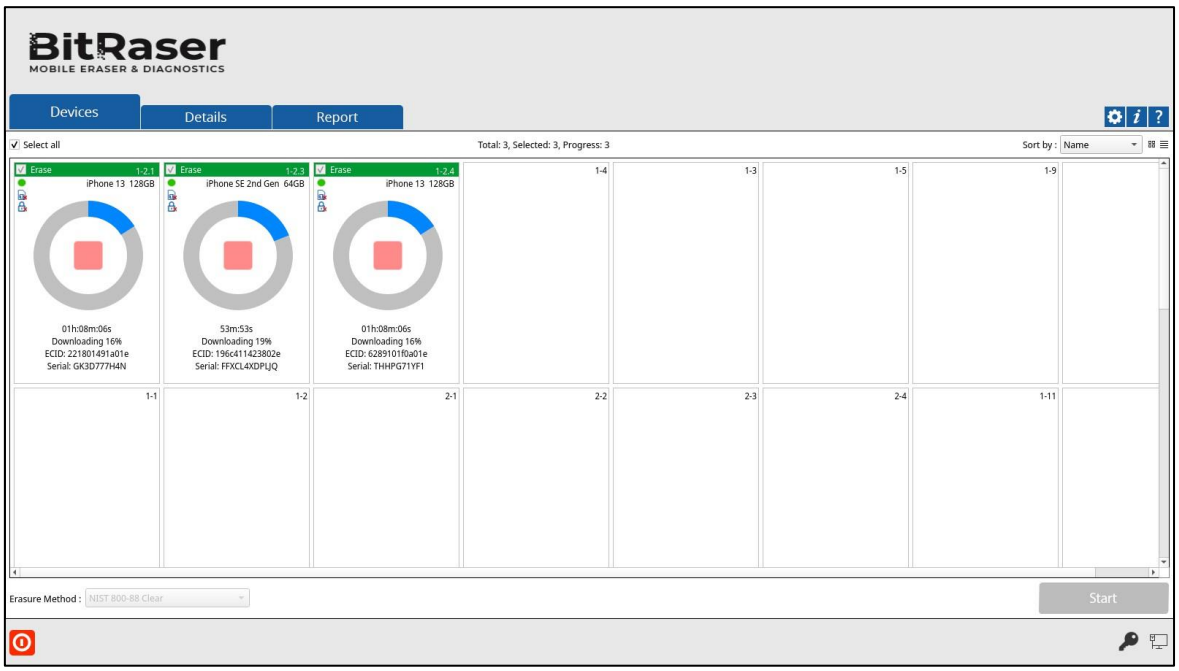
1. Device Connection: In this stage, the connection of the iOS/Android device which you want to erase is established.



2. Initialization: In the initialization phase, the application starts analyzing the device you have connected. In case you have connected multiple devices, the application lists Device Status, Device Type, ECID/IMEI, and Serial Number of the connected devices. The erasure is also possible in case if the device gets into **Recovery mode**.

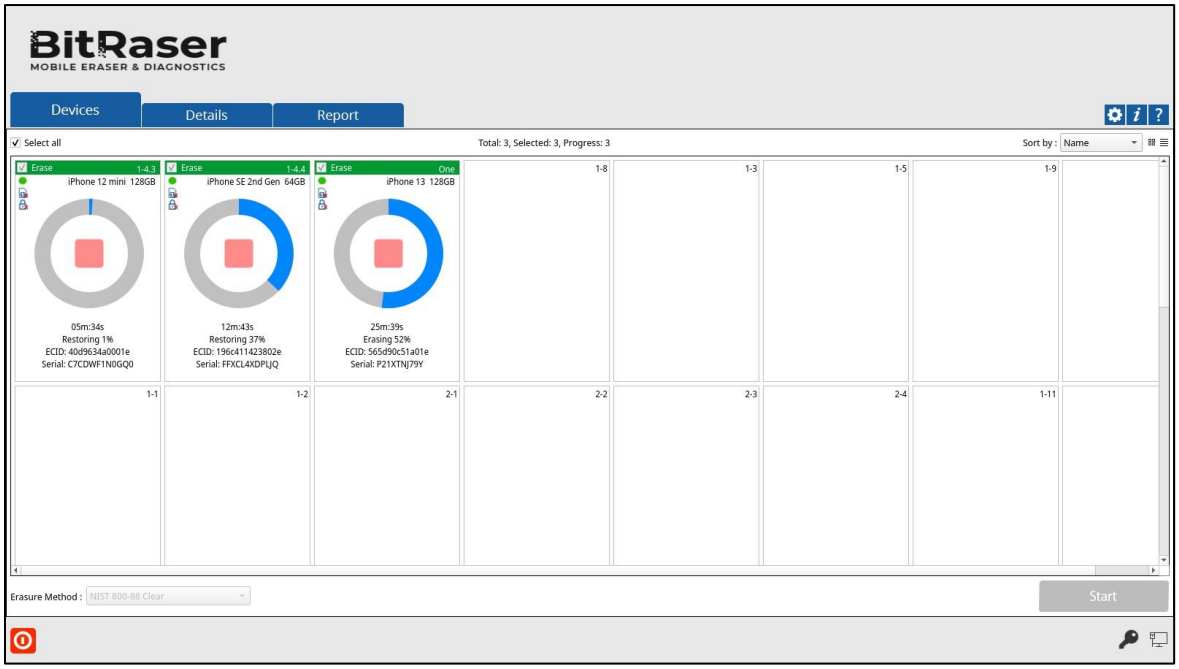


3. Firmware Downloading: Before the start of the erasure process for iOS devices, the firmware downloading process begins. In case, the firmware is already downloaded, the firmware's version will be checked and then the restoration process begins immediately. The percentage of download completed is displayed in a circular progress bar. If multiple devices are connected at a time, all of them show that their firmware is being downloaded.

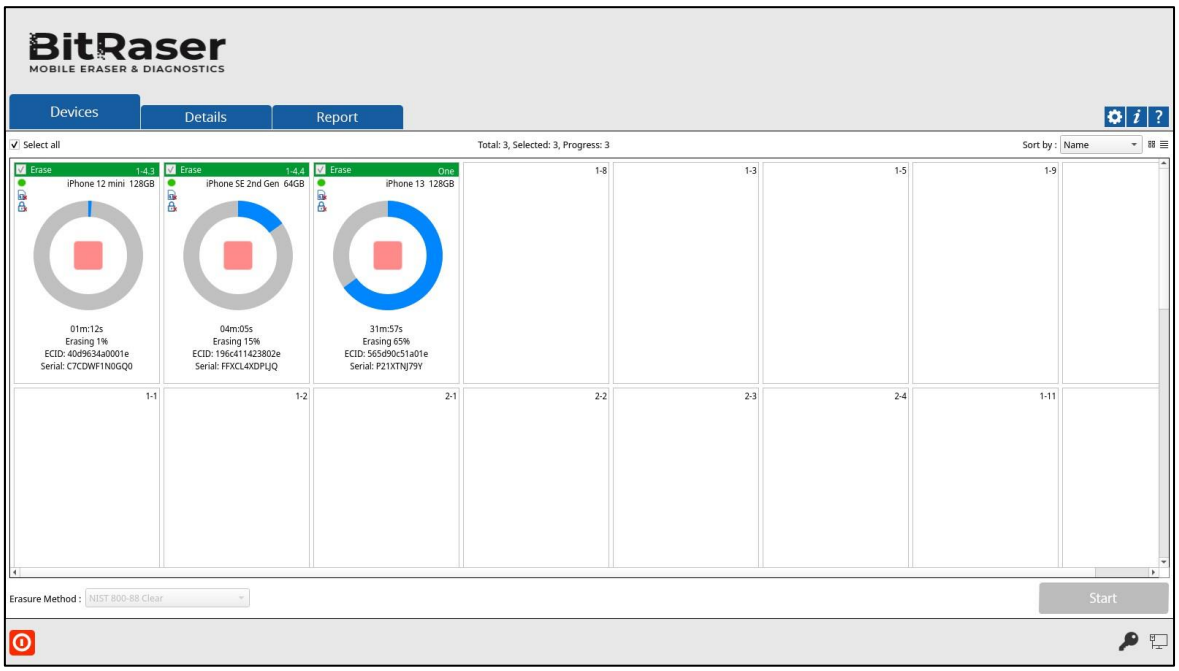


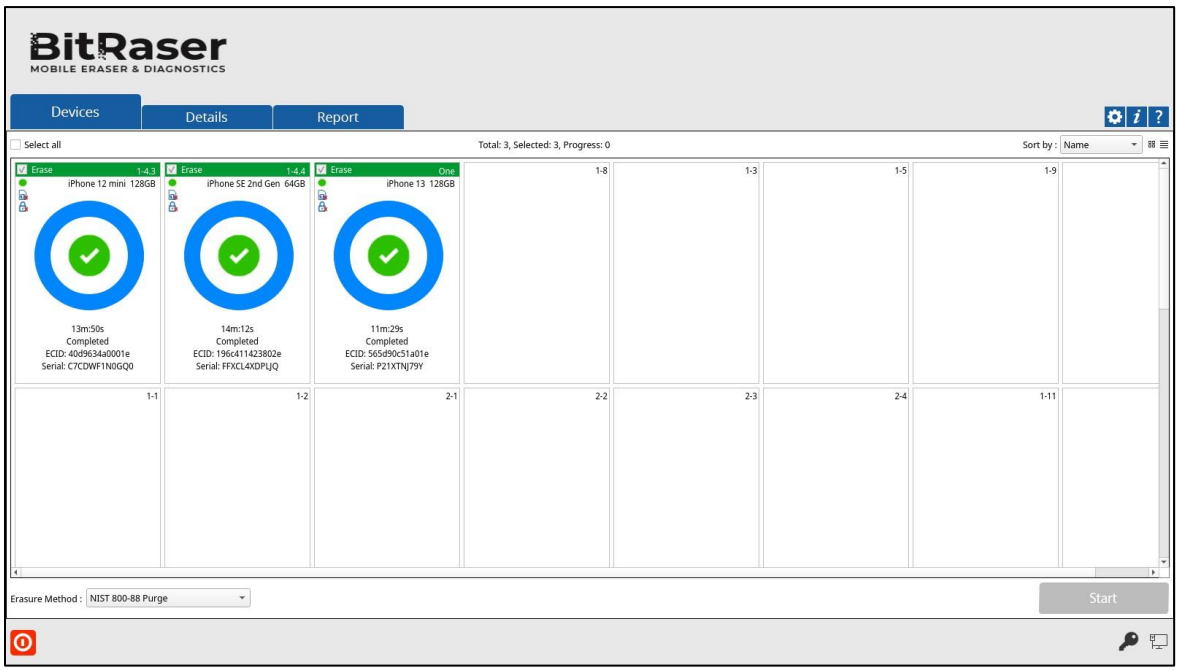
***Note**: For **Android** devices, the erasure will start immediately after the Initialization phase.*

4. Restoration: When the firmware downloading for the iOS devices gets complete, the firmware restoration process starts. Restoring your iOS device puts it into an almost completely factory-reset state that includes the erasure of all data. A '*Restoring Completed*' text appears after its successful completion.

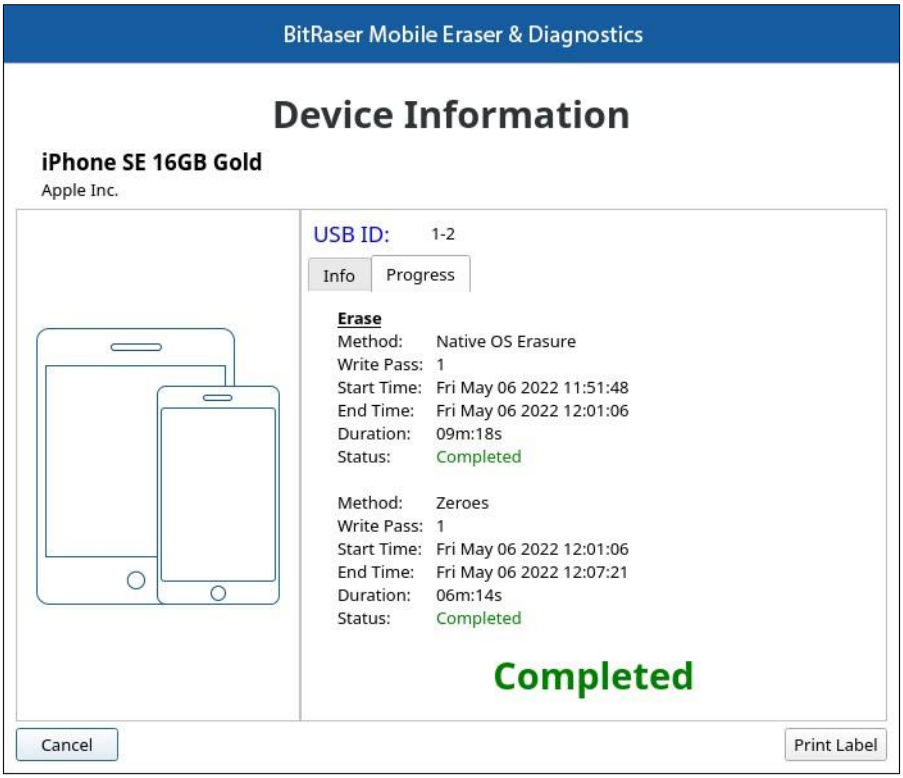


5. Erasure: The erasure process starts immediately after the completion of the restoring procedure. When the erasure is successfully completed, the icon displays a green color with the text '***Completed***'. The icon displays a red color with the text '***Failed***' in case of erasure failure.





You can view the progress of the erasure process at any time during the process by double-clicking on the device and clicking on the **Progress** tab from the **Device Information** dialog that opens:



Learn in detail about the erasure process for iOS and Android devices in the section Erasure Process.

3.2.1. ERASURE PROCESS

BitRaser Mobile Eraser & Diagnostics is a reliable application providing permanent **Data Erasure** for iPhones, iPads, Apple Watches and Android devices. Using the **BitRaser Data Erasure** process, data once erased cannot be recovered. This ensures that sensitive data does not fall into the wrong hands when mobile devices are disposed of, recycled, or sold. You can also generate an erasure report containing the results of the process. The report can be saved to a hard drive/external media or collected by the **BitRaser Cloud Console**. The application allows you to connect, erase, or diagnose multiple devices at once.

Read the data erasure process suitable for your device:

- Erasure Process for Android Devices
- Erasure Process for iOS Devices
- Erasure Process for Apple Watches

BitRaser Mobile Eraser & Diagnostics provides **11 data erasure methods**. You can select any one of the following erasure methods for both Android and iOS devices:

Erasure Methods	Description
NIST 800-88 Clear	This algorithm wipes data by overwriting the HDD or SSD drives using the Cryptographic Erase (CE) of a Self-Encrypting Drive (SED).
Native OS Erasure	This is the default algorithm available to the users in the device's OS.
Zeroes	This algorithm wipes data by overwriting it with zeros in a single pass. This is the fastest algorithm available to a user.
Pseudo-random (1 pass)	This algorithm wipes data by overwriting an entire device with randomly generated numbers in a single pass.
US Department of Defense, DoD 5220.22-M (3 passes)	This algorithm wipes data by overwriting the device in three passes. In the first pass, it overwrites data with zeros, then in the second pass, it overwrites the data with ones, and finally in the third pass overwrites the data with randomly generated bytes. This is a U.S. Department of Defense algorithm.
US Department of Defense, DoD 5200.22-M (ECE) (7 passes)	This algorithm wipes data by overwriting the device in seven passes. The first, fourth, and fifth pass are overwriting with a random byte, its 8 right-bit shift complement, and 16 right-bit shift complement; second and sixth passes are overwriting with zeros, and third and seventh pass with random data. This is a U.S. Department of Defense algorithm.

B.Schneier's algorithm (7 passes)	This algorithm wipes data in seven passes. In the first two passes, it overwrites the device with ones and then zeros, and in the next five passes, it overwrites data with random characters.
Peter Gutmann (35 passes)	This algorithm wipes data by overwriting it 35 times, making recovery of the wiped data by any tool impossible. This algorithm takes more time than other wiping algorithms.
US-Army AR 380-19 (3 passes)	This algorithm wipes data by overwriting the media in three passes. In the first pass, it overwrites data with random bytes, then in the second and third pass, it overwrites data with certain bytes and their complements. This is a U.S. Army algorithm.
US Air Force, AFSSI 5020(3 passes)	This algorithm wipes data by overwriting the media in three passes. First, it overwrites with zeros, then with ones, and finally with random characters.
British HMG IS5 (3 passes)	This algorithm is a three-pass overwriting algorithm, first pass - with zeros, the second pass–with ones and the last pass with random data.

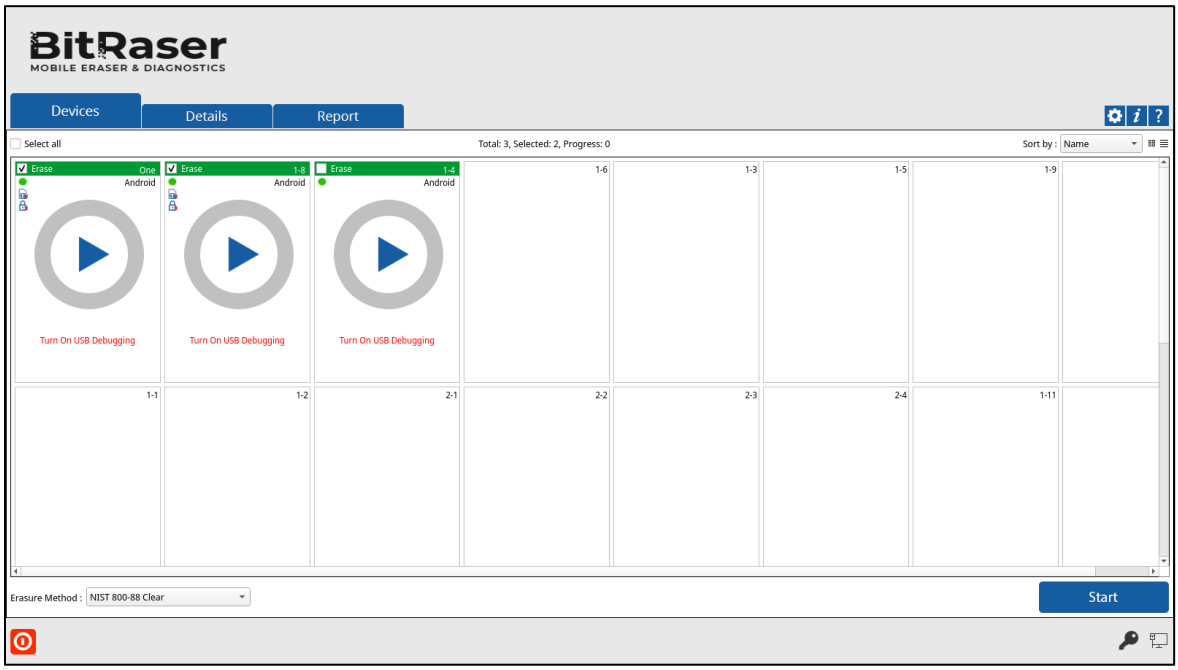
Note: *The algorithms mentioned above are not applicable for Apple Watches.*

3.2.1.1. ERASURE PROCESS FOR ANDROID DEVICES

You can securely erase data from your device by using the erasure feature of **BitRaser Mobile Eraser & Diagnostics**. You can choose an erasure method from a list of 11 data erasure methods. The software lists all of your connected devices. It allows you to perform erasure on multiple devices at once.

Steps to erase data using BitRaser Mobile Eraser & Diagnostics:

1. Run **BitRaser Mobile Eraser & Diagnostics**. Plug the Android device into the computer.
2. The **Devices** tab (which is selected by default) lists all the attached devices. The screen which appears is displayed below:



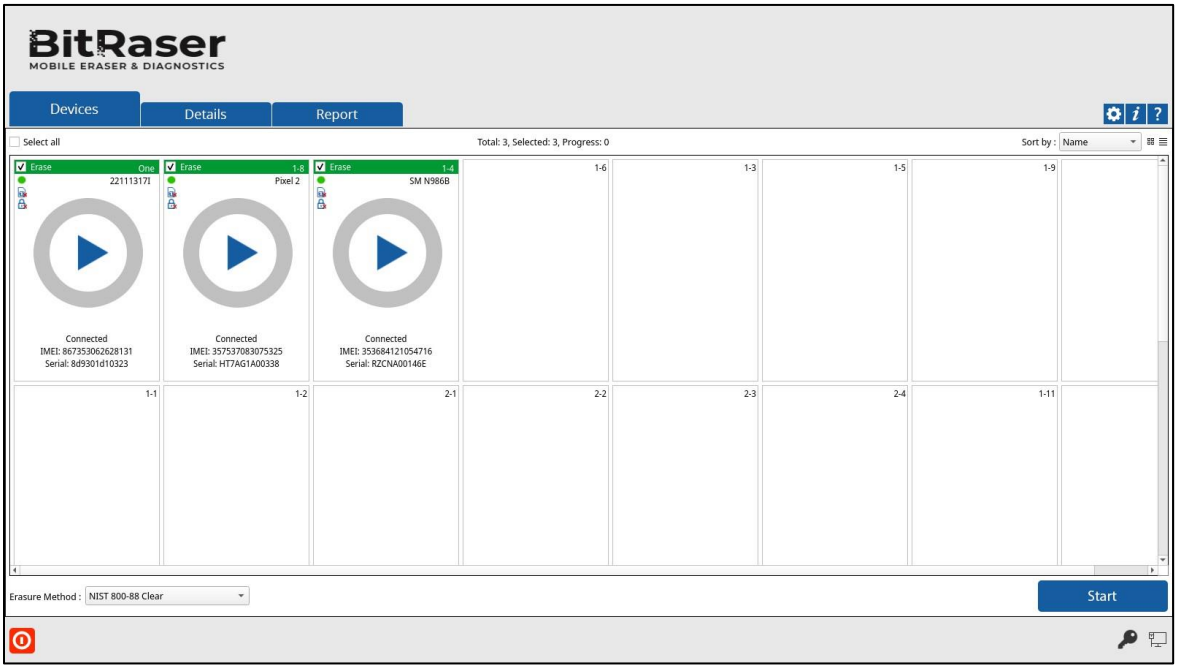
3. Your Android device appears with the message **'Turn On USB Debugging'** once it is connected. To continue from this stage, USB Debugging must be allowed from your Android device.

   Note: *Please refer to the section 'Enable USB Debugging in an Android device' to know how to turn on USB Debugging.*

4. All the devices along with their information like process (**Erase** or **Diagnose)**, USB port name, type, progress bar, status, ECID/IMEI, and serial number are displayed. You can also see icons for connectivity status, SIM card status, and FRP (Find my device) locked/unlocked status.

Note: *If you wish to change the process (**Erase** or **Diagnose**), click on the Diagnose (header area in orange color) to change the process to Erase (header area in green color) and vice versa.*

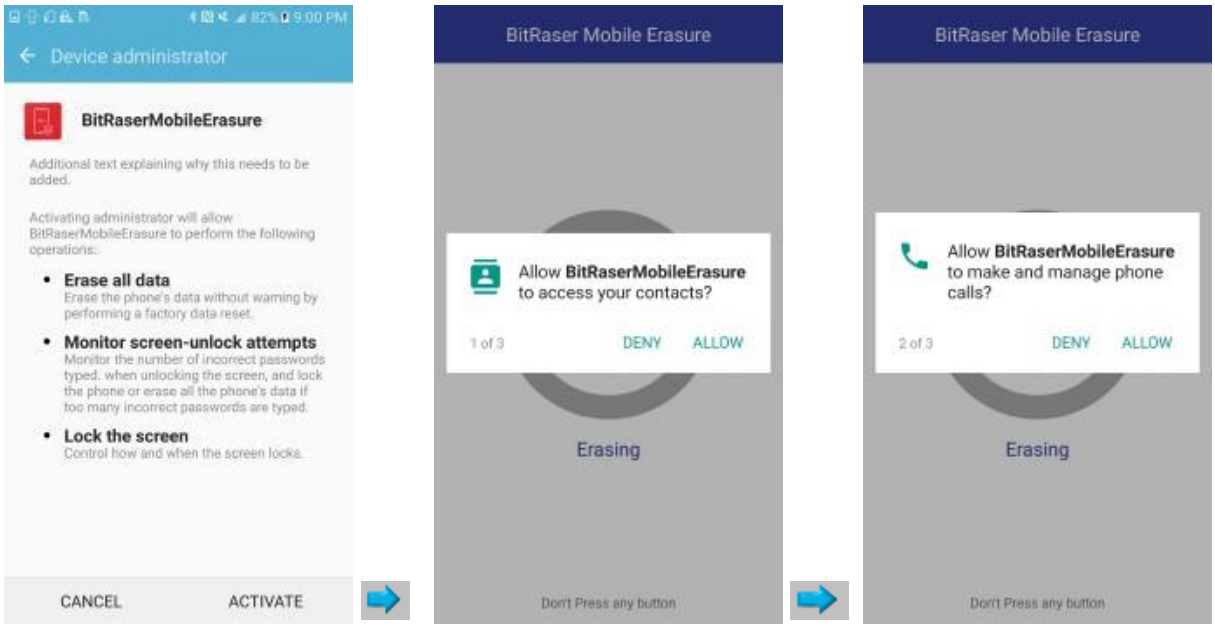
Note*: If you wish to check the ESN status of the mobile device prior to **Erase** process, click on the **ESN check** (Footer area in blue color). For more information on how to make prior settings for this feature, see ESN check.*

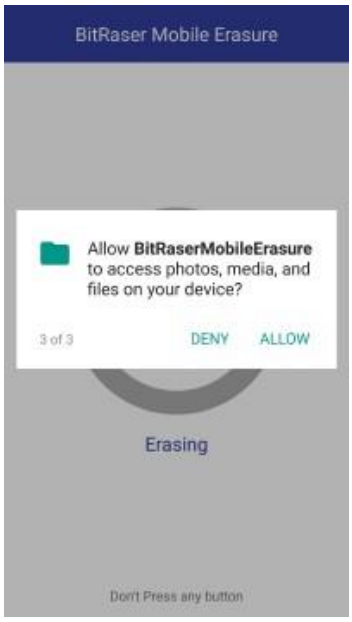


5. Select the device to erase by marking the check-box before every device. Mark **Select All** option to select every listed device for erasing.

   Tip: *When you install **BitRaser Mobile Eraser & Diagnostics** on a device running Android OS, you control which capabilities or information **BitRaser Mobile Eraser & Diagnostics** can access-known as **Permissions**. For example, the application might want permission to see your device's contacts or location. You can control which permissions the application can access after it installs on your device.*

6. **BitRaser Mobile Eraser & Diagnostics** prompts the user to **allow permissions** on the connected Android device. Click **Allow** on each of the permissions from your Android device to permit access to photos, media, files, and phone calls.



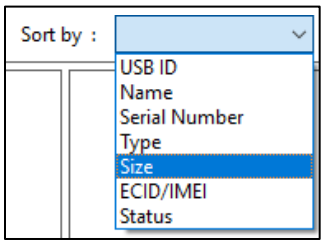


Note: *Keep in mind that turning off permissions may cause* ***BitRaser Mobile Eraser & Diagnostics*** *on your device to lose functionality.*

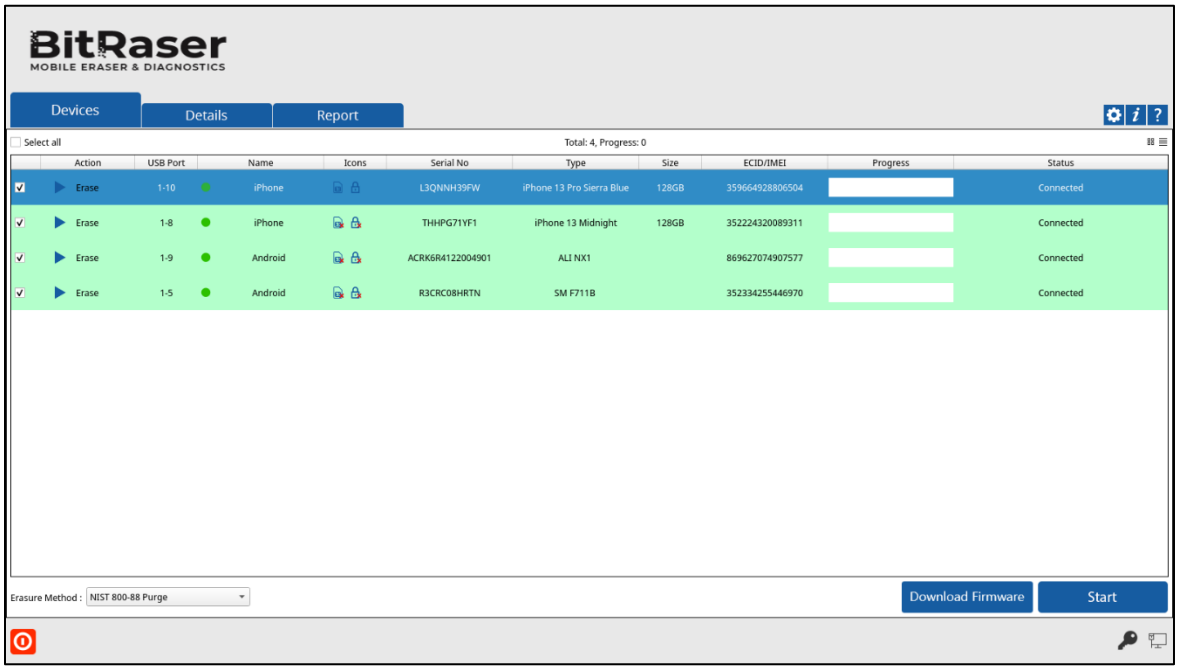
Note: *For Redmi devices, you need to install a* ***BitRaserAndroidErasure.apk*** *on your phone. See Procedure to installBitRaserAndroidErasure.apk on Redmi Phone.*

7. You can preview the device's information either in **Grid view** or **List view** .

- In the **Grid view**, the devices get displayed in a grid-like structure, and also the devices can be sort using the **Sort By** option. The **Sort By** option allows sorting the devices based on the following information/criteria: USB ID, Name, Serial Number, Type, Size, ECID/IMEI, and Status.

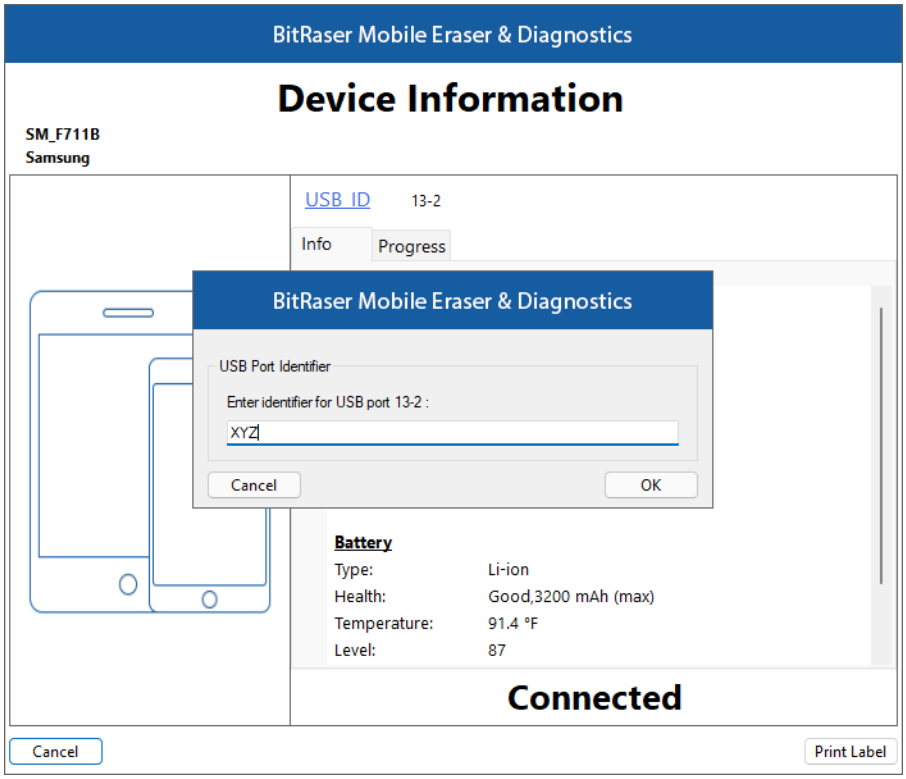


- In the **List view**, the devices get displayed in a list.

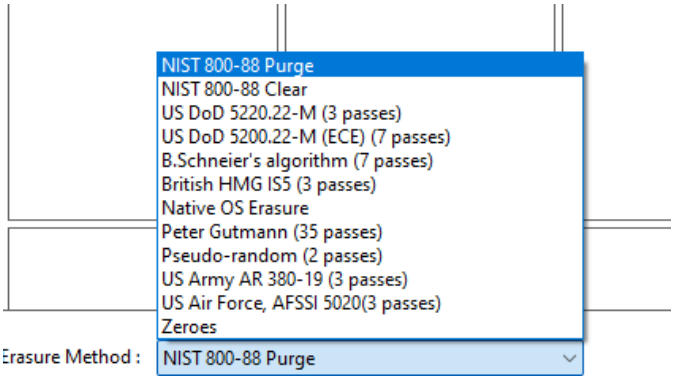


8. Double-clicking on any of the displayed devices will show the device information of the corresponding device. These details can be printed by clicking on the **Print Label** button.

9. From the dialog that appears, click on **USB ID** to change the identifier for the USB port. Click **OK.**



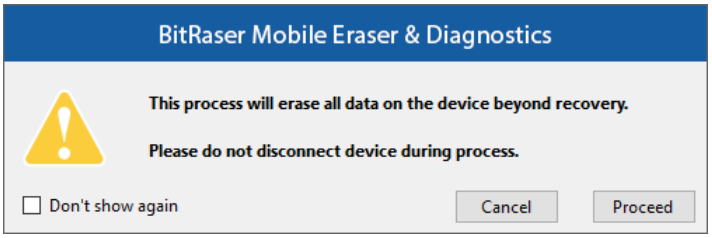
10. Select any one of the 11 erasure methods from the bottom of the screen by clicking on the drop-down menu.



11. Click **Start** to begin the erasing process.

Note: *If you wish to erase a single device, you can start the process by simply clicking the play button in the middle.*

12. A warning message appears asking to proceed to the erasure process. Click **Proceed**.

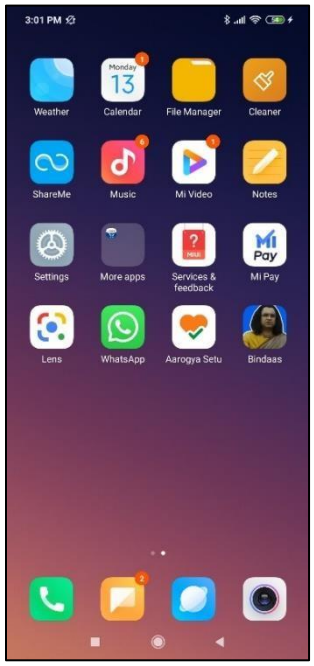


Note: *If you do not wish to see the warning message the next time you erase a device, mark* ***Don't Show Again*** *check-box.*

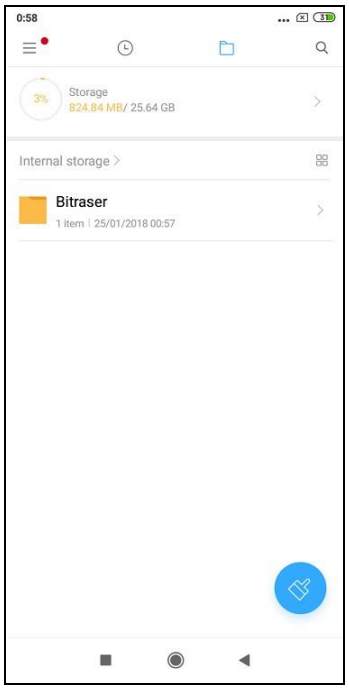
Note*: At this stage,* ***BitRaser Mobile Eraser & Diagnostics*** *acquire license information from* ***BitRaser Cloud,*** *and licenses are consumed depending upon the number of devices you have selected for erasure. Therefore, you need an active internet connection to start the erasing process.*

Procedure to Install BitRaserAndroidErasure.apk on Redmi Devices:

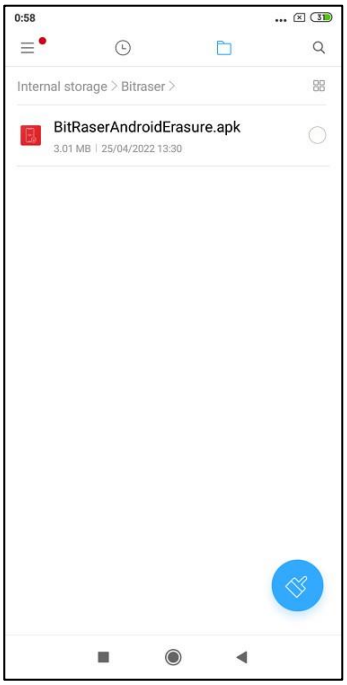
1. Open **File Manager** on your **Redmi** phone



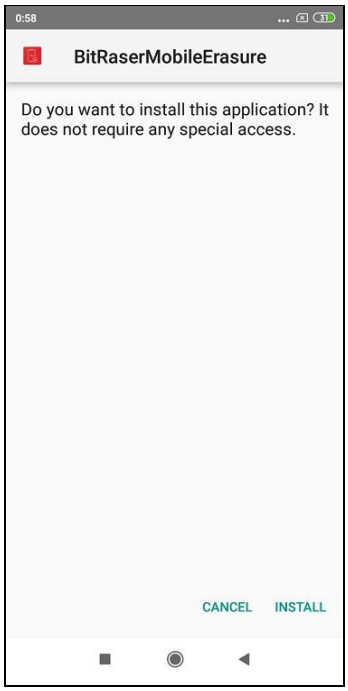
2. Locate and open **Bitraser** folder



3. Select and open **BitRaserAndroidErasure.apk**

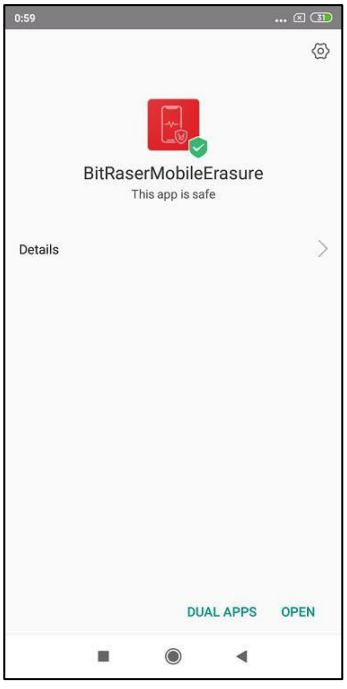


4. Click **Install** to begin the installation process



5. Wait while the device installs the **.apk** file

6. **BitRaserMobileErasure** is installed successfully



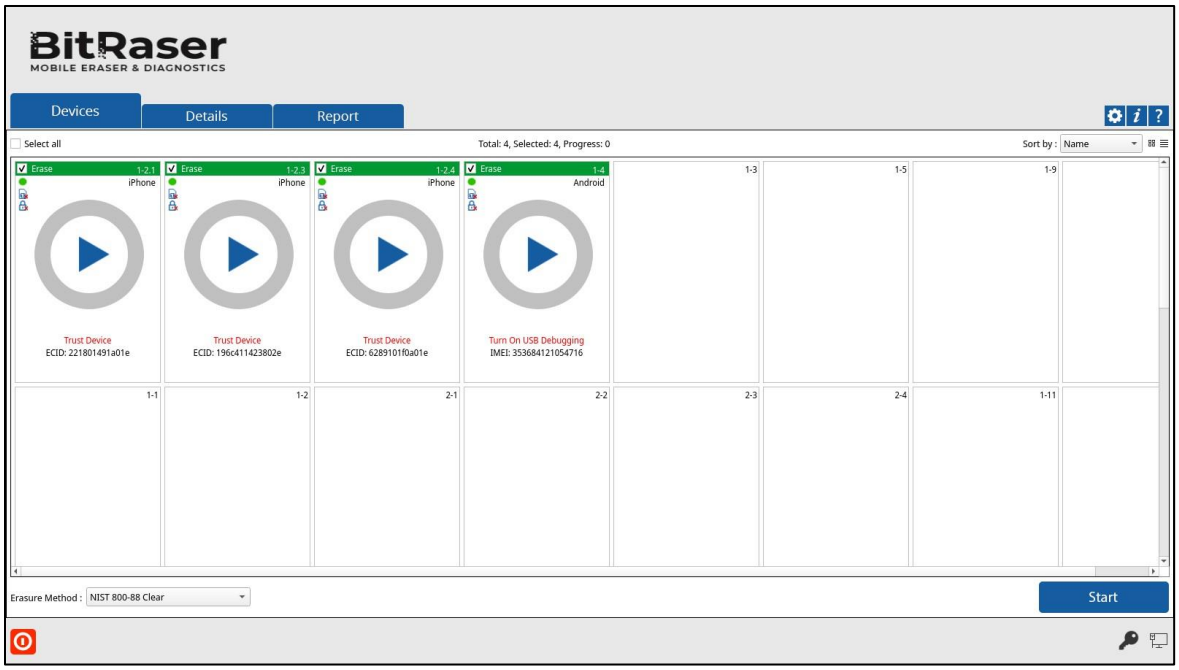
3.2.1.2. ERASURE PROCESS FOR iOS DEVICES

BitRaser Mobile Eraser & Diagnostics allows you to erase your data from all of your iOS devices like iPhones and iPads. It also supports complete data erasure from Apple Watches. The software provides you a list of 11 data erasure methods for erasing your data. **BitRaser Mobile Eraser & Diagnostics** lists all of your connected devices and allows you to perform erasure on multiple devices simultaneously.

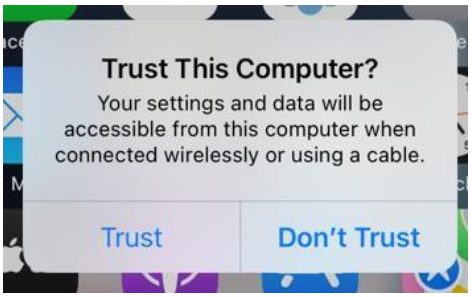
Steps To erase data using BitRaser Mobile Eraser & Diagnostics:

1. Run **BitRaser Mobile Eraser & Diagnostics**. Plug the iOS device into the computer.

2. The **Devices** tab (which is selected by default) lists all the attached devices. The screen which appears is displayed below:



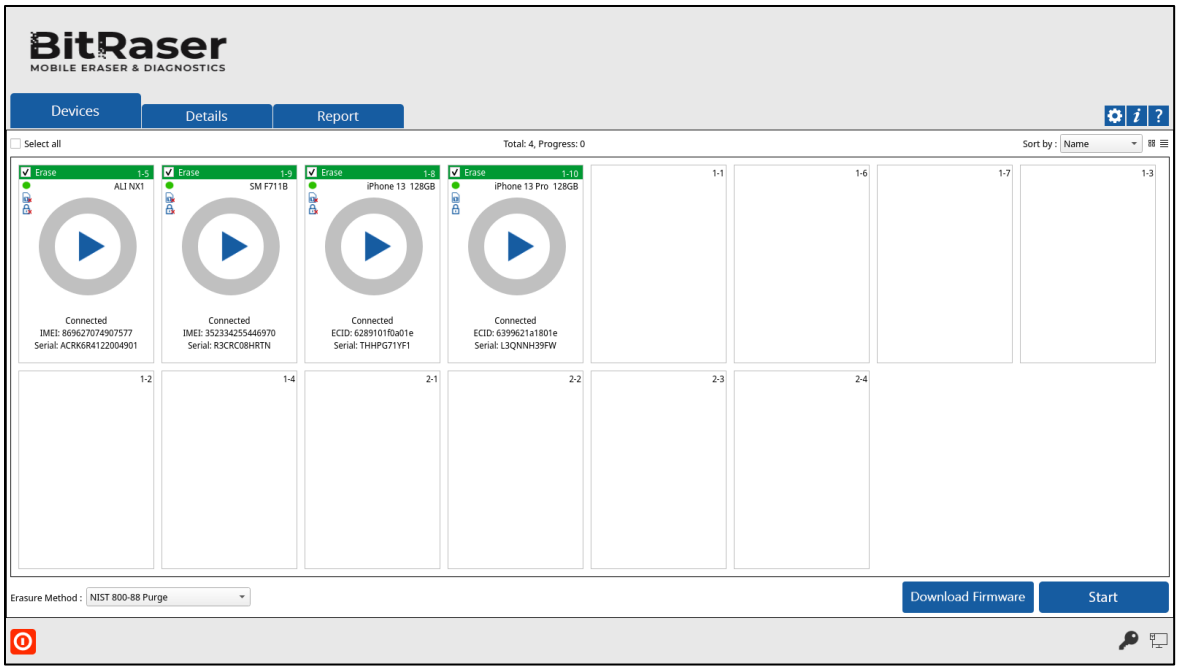
3. Your iOS device appears with a message **'Trust this Computer?'**. Click on **'Trust'** button to proceed further.



Note: *You need to Trust the computer to enable sync and data transfer between your connected iOS device and the computer. Keep in mind that clicking on* ***'Don't Trust'*** *instead of* ***'Trust'*** *may cause* ***BitRaser Mobile Eraser & Diagnostics*** *on your device to lose functionality.*

4. All the devices along with their information like process (**Erase** or **Diagnose)**, USB port name, type, progress bar, status, ECID/IMEI, and serial number are displayed. You can also see icons for connectivity status, SIM card status, and FMIP locked/unlocked status.

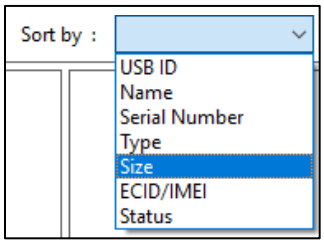
Note: *If you wish to change the process (****Erase*** *or* ***Diagnose****), click on the Diagnose (header area in orange color) to change the process to Erase (header area in green color) and vice versa.*



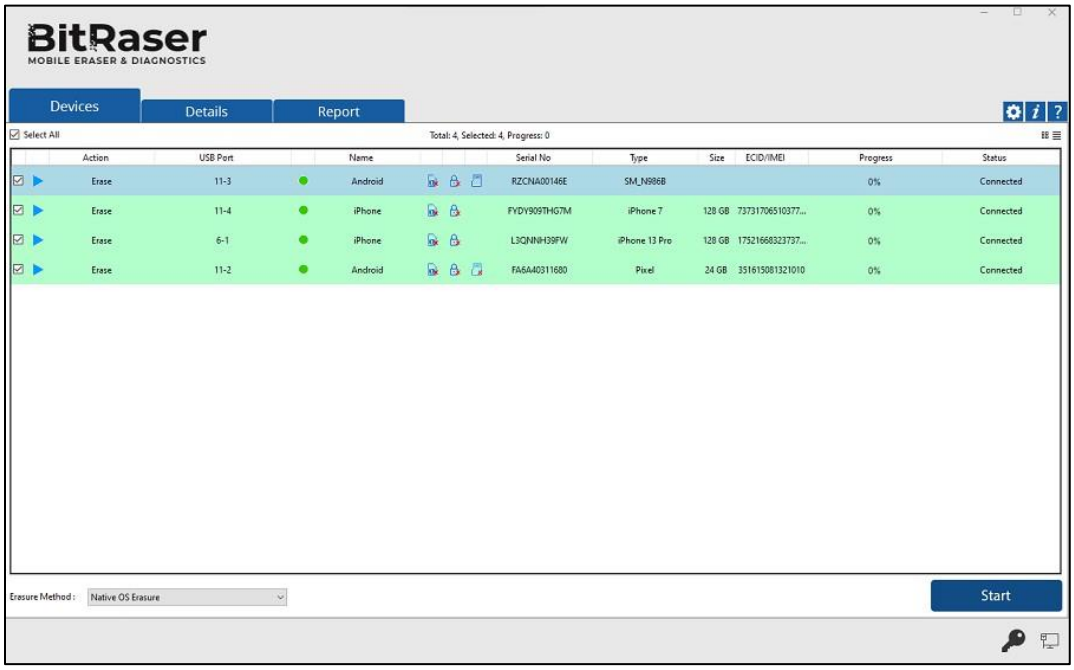
5. Select the device to erase by marking the check-box before every device. You can mark **Select All** option for selecting every listed device at once.

6. You can preview the device's information either in **Grid view** or **List view** .

- In the **Grid view**, the devices get displayed in a grid-like structure, and also the devices can be sort using the **Sort By** option. The **Sort By** option allows sorting the devices based on the following information/criteria: USB ID, Name, Serial Number, Type, Size, ECID/IMEI, and Status.

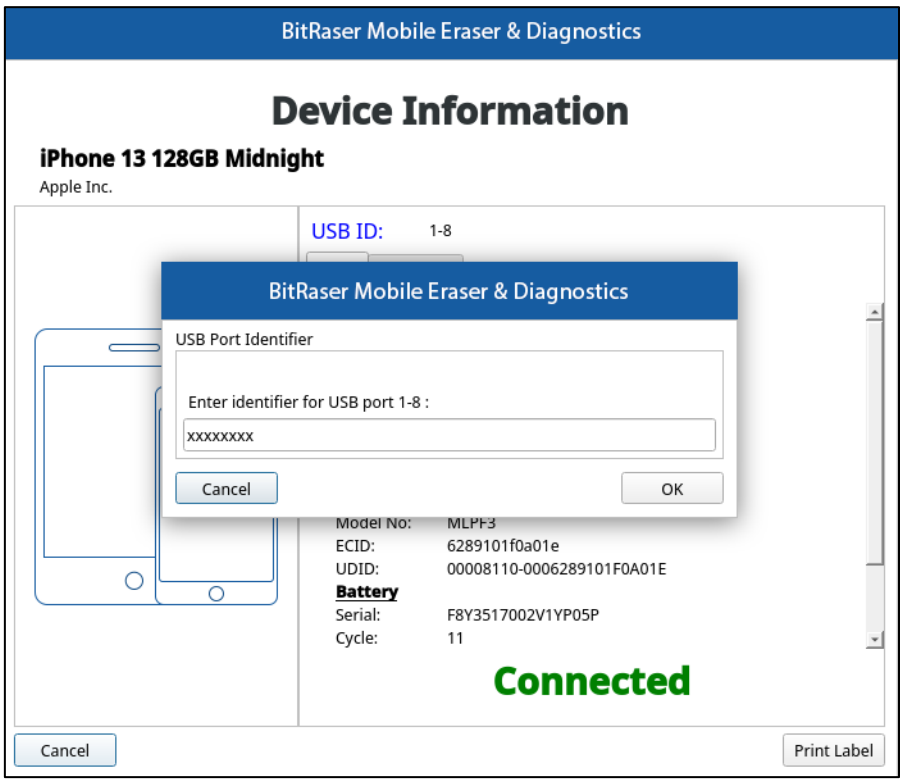


- In the **List view**, the devices get displayed in a list.

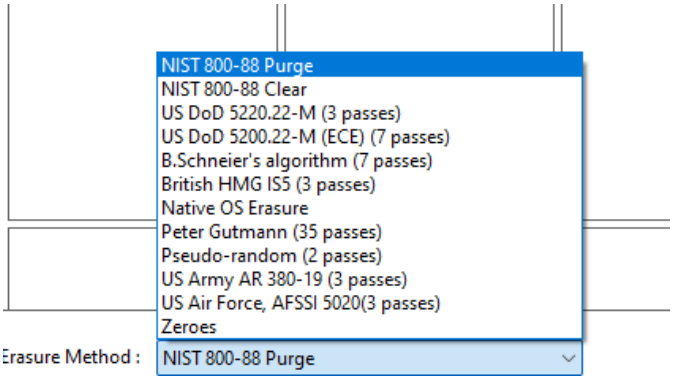


7. Double-clicking on any of the displayed devices will show the device information of the corresponding device. These details can be printed by clicking on the **Print Label** button.

8. From the dialog that appears, click on **USB ID** to change the identifier for the USB port. Click **OK**.



9. Select any one of the [11 erasure methods] from the bottom of the screen by clicking on the drop-down menu.

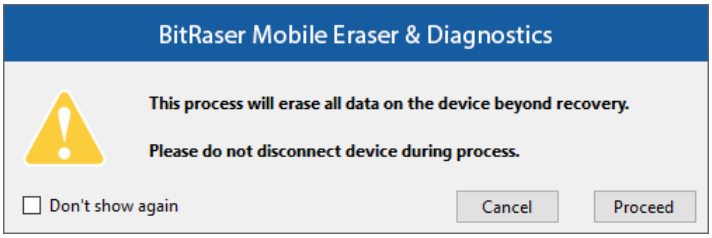


Note: *The algorithms shown above are not applicable for Apple Watches. You have to manually [erase data from the Apple Watch].*

10. Click **Start** to initiate the erasing process.

Note: *If you wish to erase a single device, you can start the process by simply clicking the play button in the middle.*

11. A warning message appears asking to proceed to the erasure process. Click **Proceed**.



Note: *If you do not wish to see the warning message the next time you erase a device, select the* ***Don't show again*** *check-box.*

Note: *At this stage,* ***BitRaser Mobile Eraser & Diagnostics*** *acquires license information from* ***BitRaser Cloud,*** *and licenses are consumed depending upon the number of devices you have selected for erasure. Therefore, you need an active internet connection to start the erasing process.*

3.2.1.3. ERASURE PROCESS FOR APPLE WATCHES

BitRaser Mobile Eraser & Diagnostics is efficiently capable of not only erasing data from iPhones, iPads, and Android devices but also from Apple Watches. It supports data erasure from Apple Watch Series 1, 2, 3, 4, 5 and Series SE. Your Apple Watch should have a minimum of 10% battery backup for successful data erasure. **BitRaser Mobile Eraser & Diagnostics** allows you to see your connected Apple Watch's information like process (Erase), USB port name, type, progress bar, status, ECID/IMEI, and serial number. You can also see icons for connectivity status, SIM card status, and FMIP locked or unlocked status. You can preview this information either in Grid view or List view. The software allows you to securely erase data from both activated and non-activated Apple Watches.

Steps to erase data when the Apple Watch is activated:

1. Run **BitRaser Mobile Eraser & Diagnostics**.

2. Detach the bands from the Apple Watch.

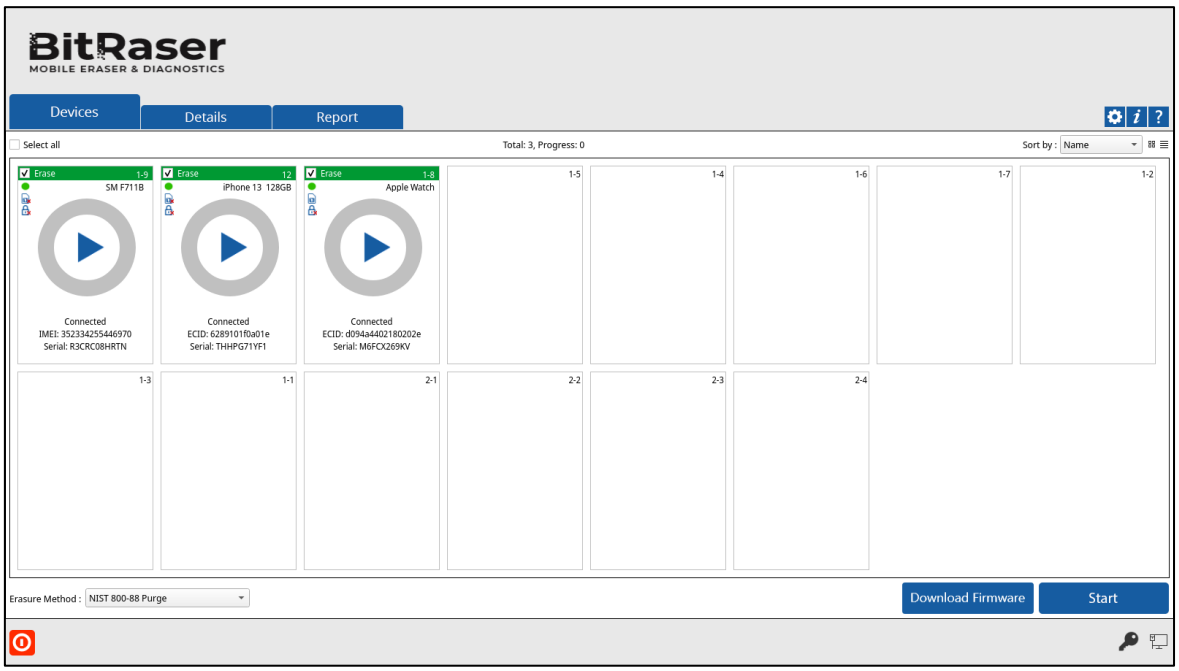
3. Remove the cap shielding the pin on the Apple Watch using a small pin or similar tool.

4. Connect your Apple Watch to the iBUS adapter, ensuring that the iBUS text is positioned towards the front of the Apple Watch's display, then plug the adapter into the computer using a USB cable.

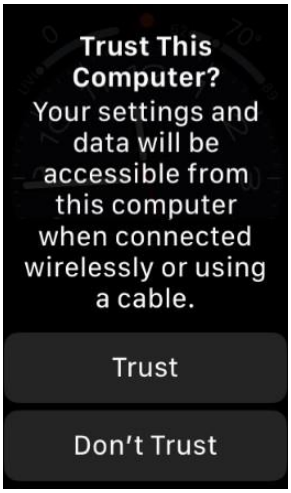
***Note**: If the device item isn't visible in BitRaser, attempt flipping the lightning cable upside down.*

***Note**: You need to pair Apple Watch to iPhone and then perform a manual factory reset from the Apple Watch's menu.*

5. The **Devices** tab (which is selected by default) lists all the attached devices. The screen which appears is displayed below:



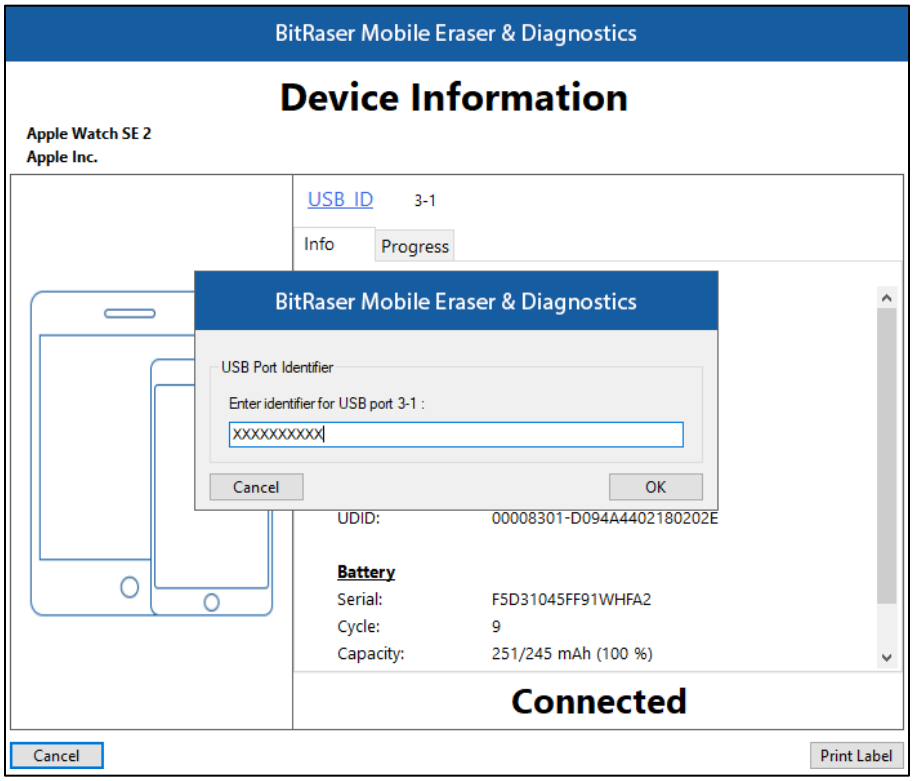
6. Your Apple Watch appears with a message **'Trust this Computer'**. Click on **'Trust'** button to proceed further.



Note: *You need to Trust the computer to enable sync and data transfer between your connected Apple Watch and the computer. Keep in mind that clicking on* ***'Don't Trust'*** *instead of* ***'Trust'*** *may cause* ***BitRaser Mobile Eraser & Diagnostics*** *on your device to lose functionality.*

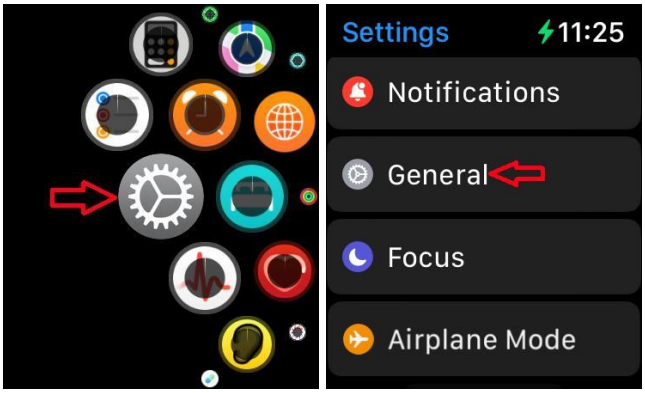
7. You can see your connected Apple Watch's information by double-clicking on its icon. These details can be printed by clicking on the **Print Label** button.

Note: *From the dialog box that appears, click on* ***USB ID*** *if you wish to change the identifier of the USB port, and then click* ***OK****.*

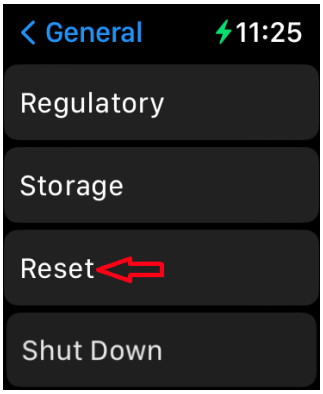


8. Press the Digital Crown of your Apple Watch for two seconds to open the Home Screen.

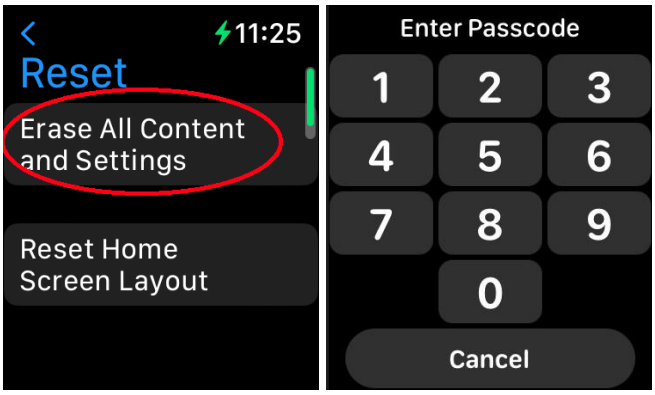
9. Tap on the **"Settings"** app from your Apple Watch's Home Screen and click on **"General"** button.



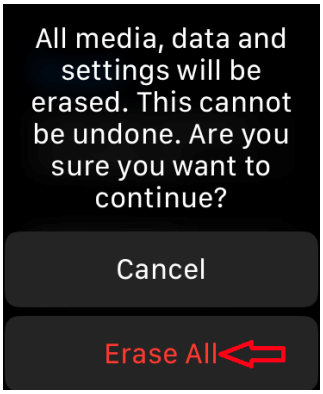
10. Scroll down and tap **"Reset"**.



11. Select **"Erase All Content and Settings"**. It prompts you to enter your Apple Watch's passcode if it is passcode protected.



12. A dialog box appears telling you to confirm whether you want to erase your media, data, and settings or not. Tap on **"Erase All"** to initiate the erasure process.



Note: *You will need to first unpair your Apple Watch before erasing if you wish to remove the activation lock.*

Steps to erase data when the Apple Watch is not activated:

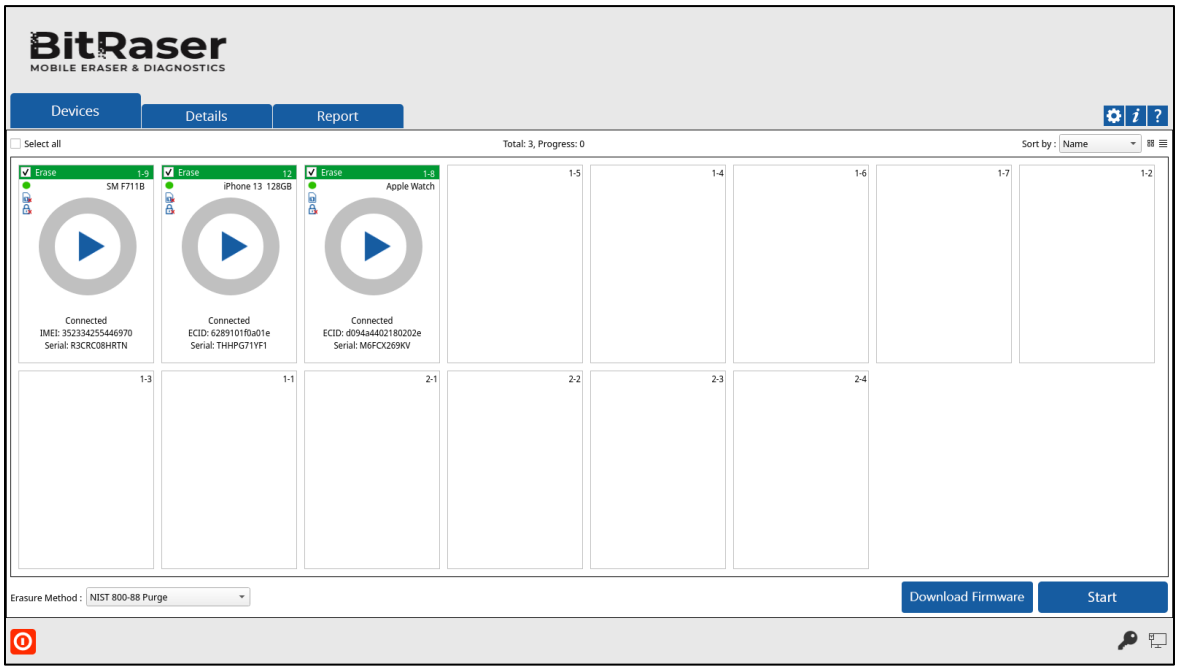
1. Run **BitRaser Mobile Eraser & Diagnostics**.

2. Detach the bands from the Apple Watch.

3. Remove the cap shielding the pin on the Apple Watch using a small pin or similar tool.

4. Connect your Apple Watch to the iBUS adapter, ensuring that the iBUS text is positioned towards the front of the Apple Watch's display, then plug the adapter into the computer using a USB cable.

5. The **Devices** tab (which is selected by default) lists all the attached devices. The screen which appears is displayed below:



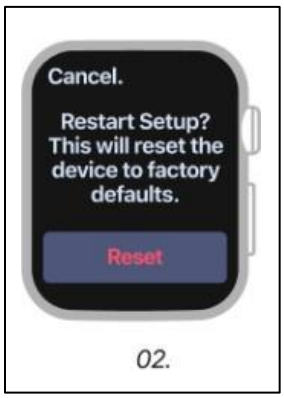
6. You can see your non-activated Apple Watch's information by double-clicking on its icon, just like the activated Apple Watch. Click on the Print Label button to print these details.

Note: *From the dialog box that appears, click on* ***USB ID*** *if you wish to change the identifier of the USB port, and then click* ***OK****.*

7. Press and hold the Digital Crown your Apple Watch.

01.

8. A dialog box appears telling you to confirm whether you want to reset your Apple Watch or not. Tap on **"Reset"** button to begin the erasure process.



02.

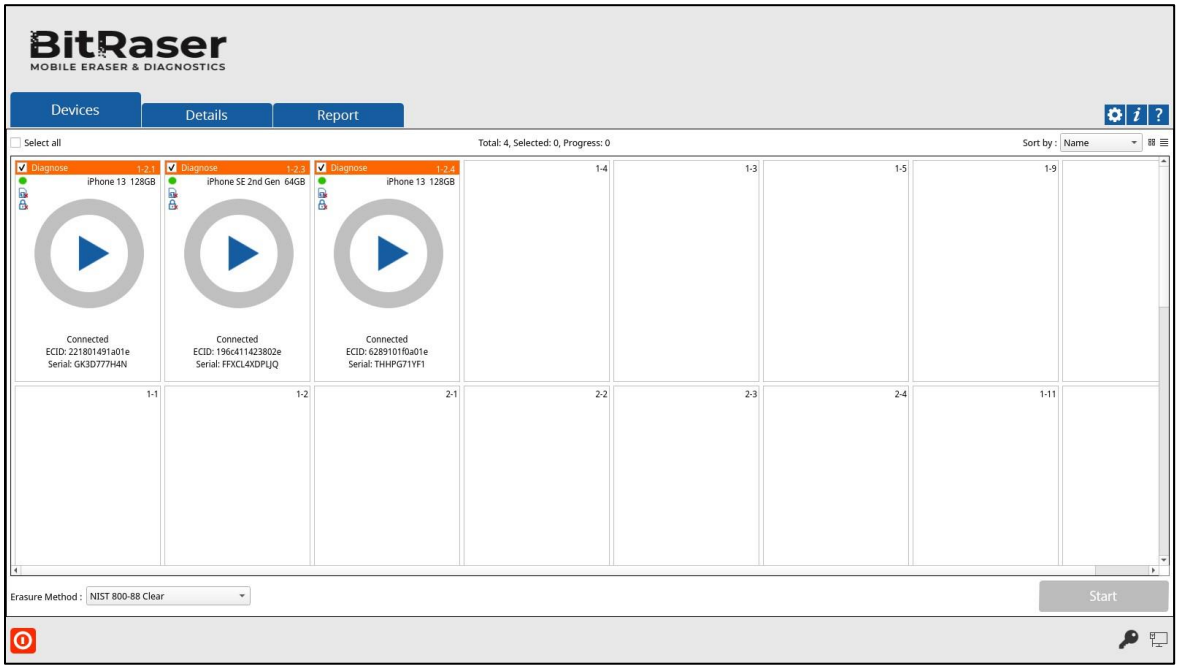
3.3. DIAGNOSTIC STAGES

Before the completion of the diagnostic process, a series of steps take place while we diagnose a device. The diagnostic stages are as follows:

1. Device Connection
2. Initialization
3. Automatic Diagnostic Tests
4. Manual Diagnostic Tests
5. Accessories and Grading

Caution: *Make sure you do not interrupt the process by disconnecting the device or pressing the power button at any stage. Doing so might fail the process and harm your device.*

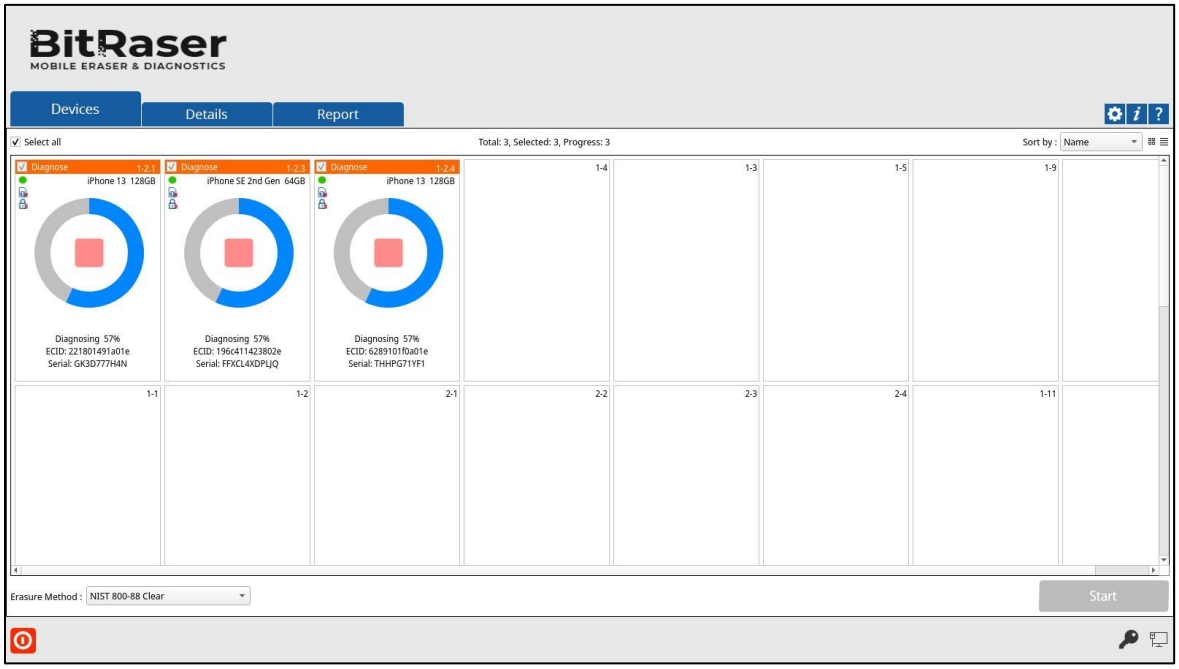
1. Device Connection: In this stage, the connection of the iOS/Android device that you want to diagnose is established.

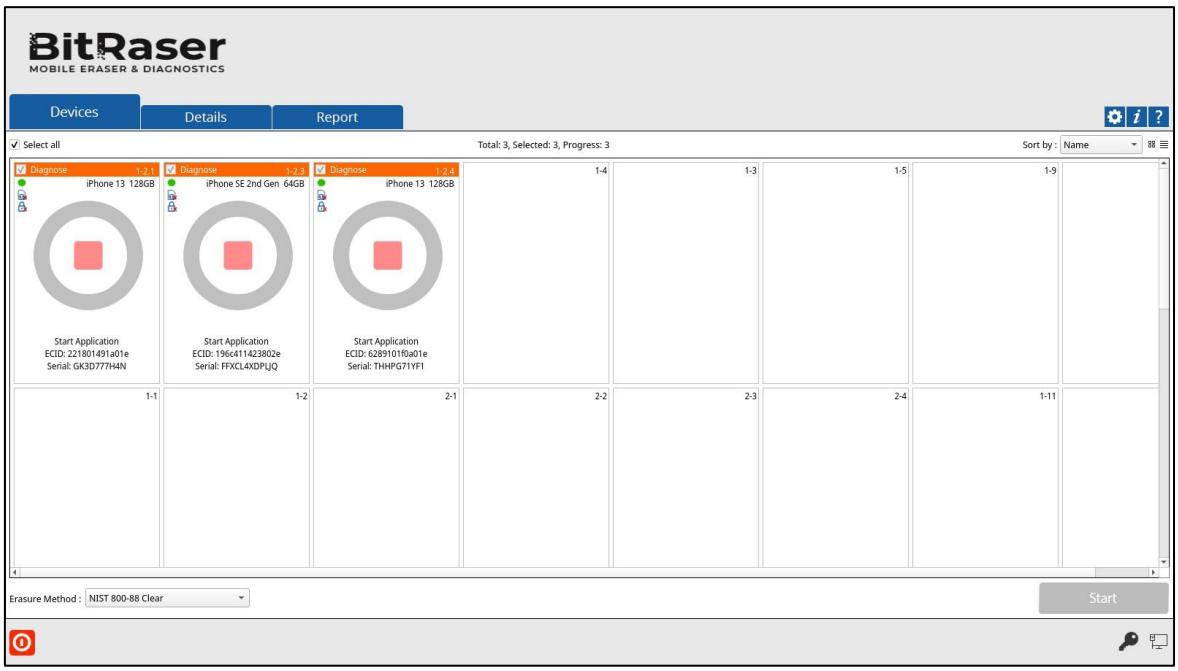


2. Initialization: In the initialization phase, the application starts analyzing the device you have connected. In case you have connected multiple devices, the application lists Device Status, Device Type, ECID/IMEI, and Serial Number of the connected devices.

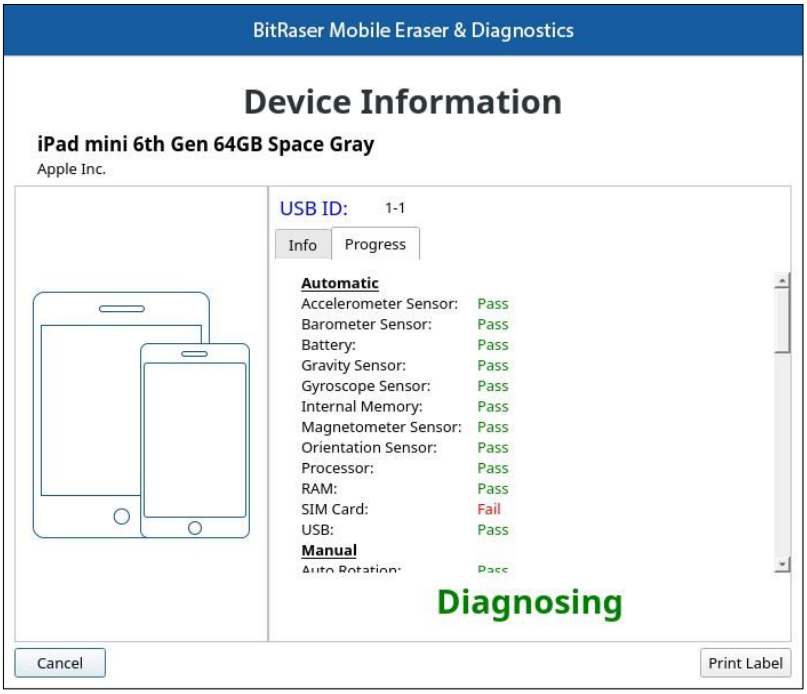
The application prompts the user to **Install App from device** for **Redmi** devices and Allow Permissions on other android devices. Proceed to this process on the device as required by the application.

***Note**: For **Redmi** devices, you need to install a **BitraserMobileDiagnostics.apk** on your phone. See Procedure to install BitraserMobileDiagnostics.apk on Redmi Phone to know the required steps.*





3. Automatic Diagnostic Tests: The automatic diagnostic tests starts immediately after the diagnostic procedure is initiated. The device at this stage goes through a series of automatic tests. You can view the progress of the diagnostic process by double-clicking on the device and clicking on the **Progress** tab from the **Device Information** dialog that opens:

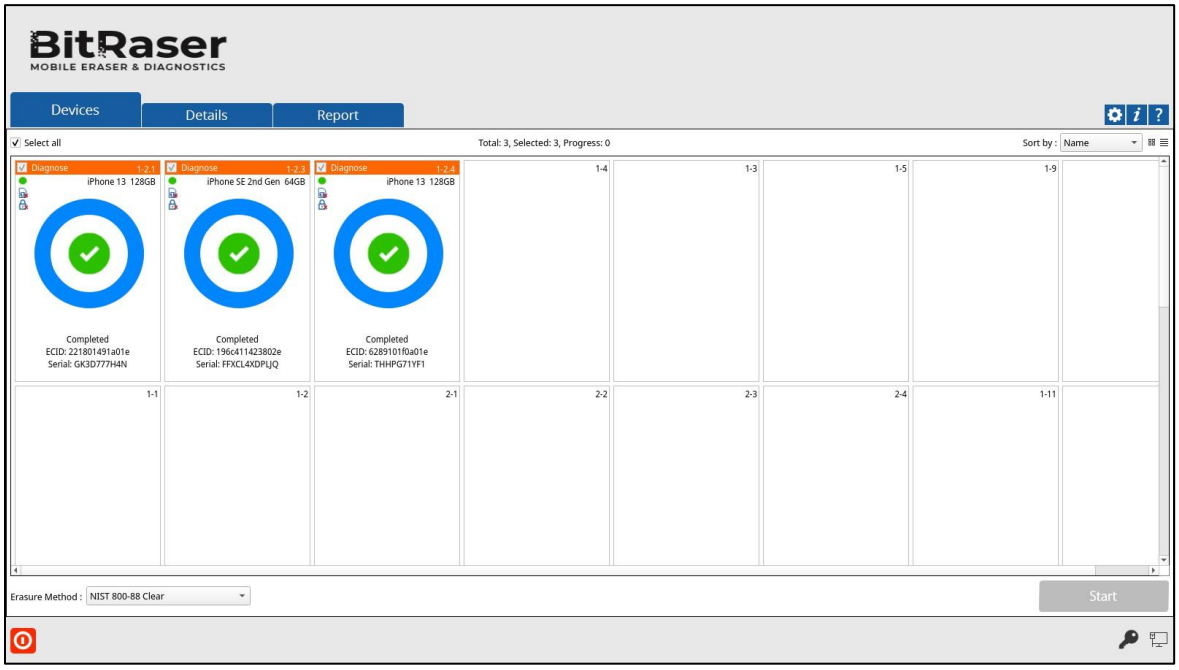


4. Manual Diagnostic Tests: At this stage, the device goes through a series of manual tests. These are a series of easy tests that you need to perform manually on the device. Follow the simple instructions on the device to perform these tests.

5. Accessories and Grading: After the completion of manual tests, the device gives you an option to enter the accessories such as charger, earphone, memory card, original packing, etc. that are available with the device. Mark the check-boxes for the accessories if they are available.

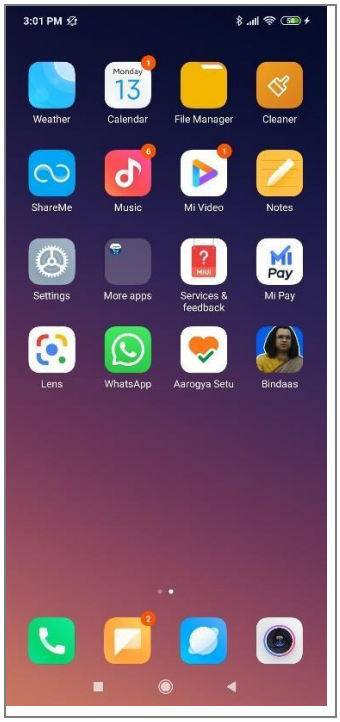
The device also asks you to grade the back cover, body, display, and overall grading on a scale of A+, A, B, and C with A+ being the highest grading and C being the lowest.

When the diagnose gets successfully completed, the icon displays a green color with the text '***Completed***'. The icon displays a red color with the text '***Failed***' in case of diagnose failure.

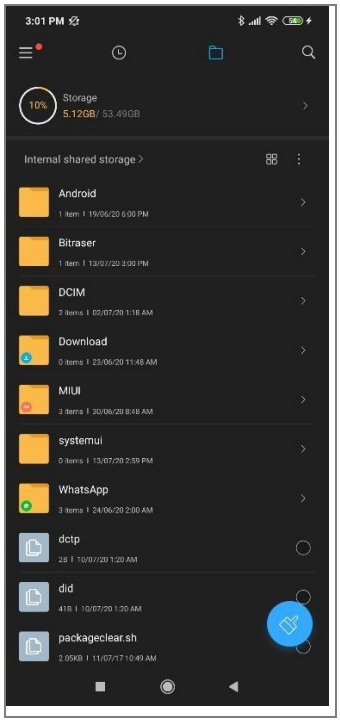


Procedure to Install BitraserMobileDiagnostics.apk on Redmi Devices:

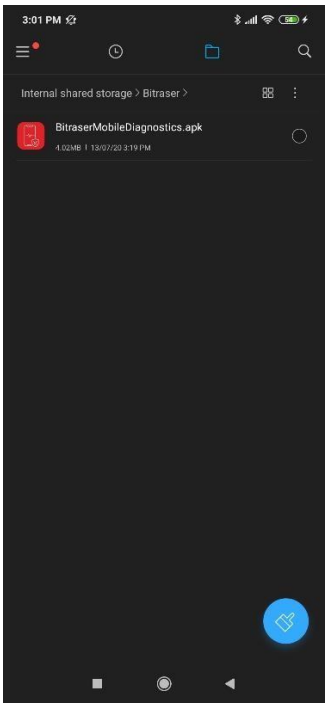
1. Open **File Manager** on your **Redmi** phone
2. Locate and open **Bitraser folder**
3. Select and open **BitraserMobileDiagnostics.apk**



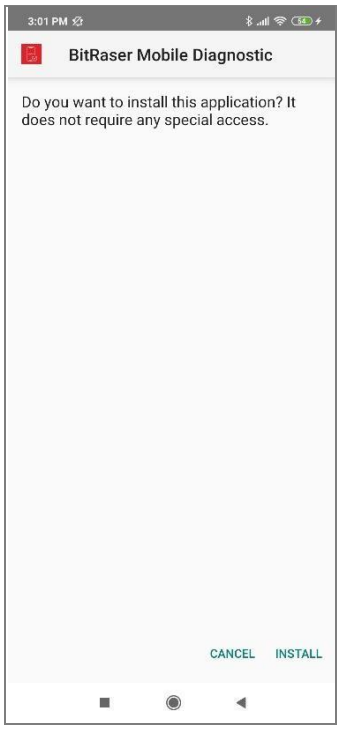
4. Click **Install** to begin the installation process

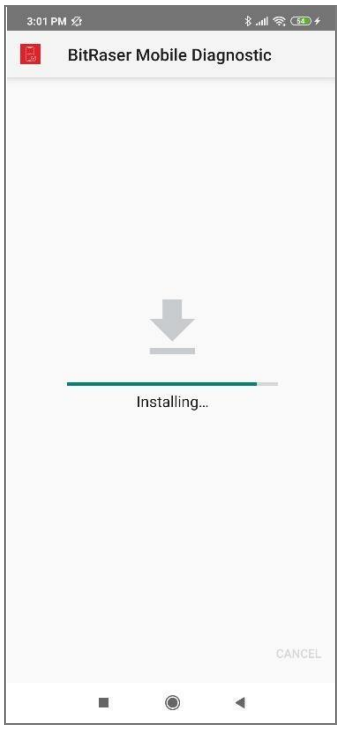


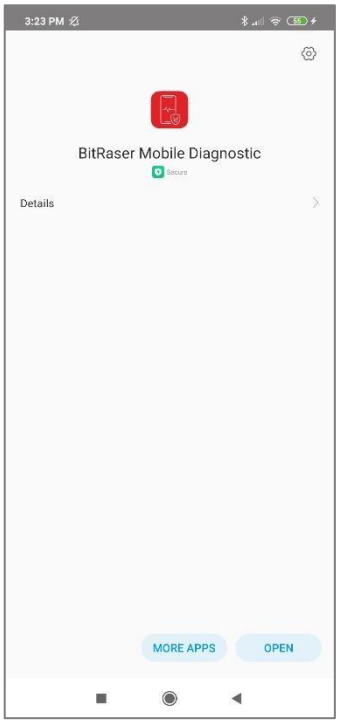
5. Wait while the device installs the **.apk** file



6. **BitRaser Mobile Diagnostic** is installed successfully







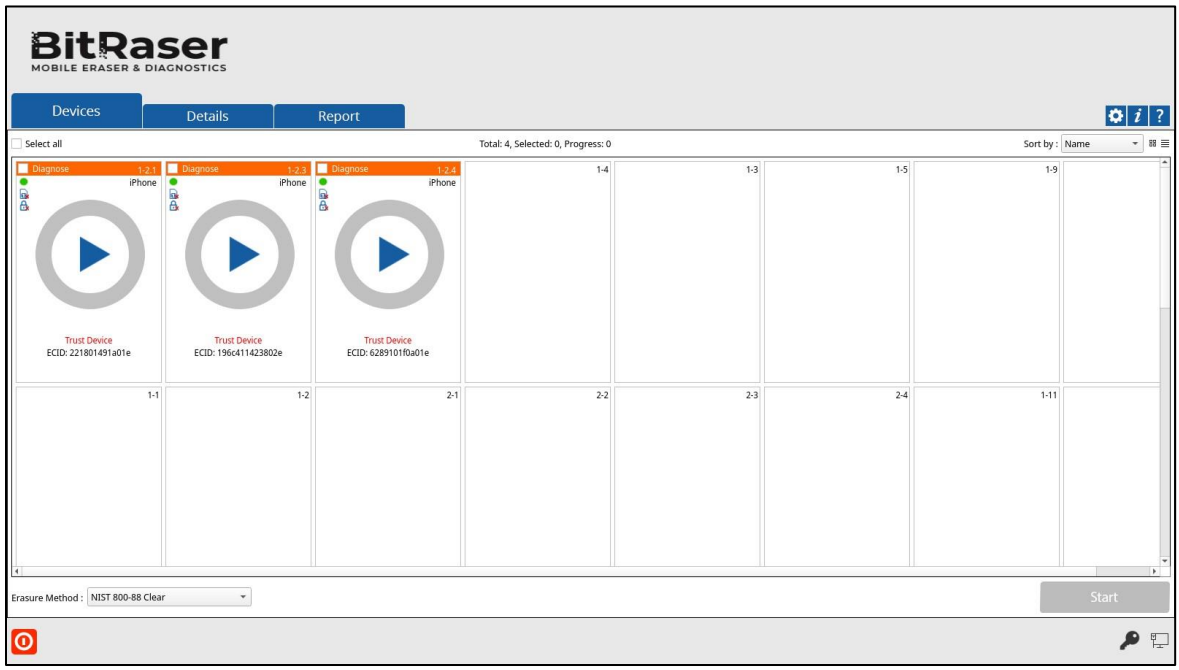
Learn in detail about the diagnostic process for iOS and Android devices in the section Diagnostic Process.

3.3.1. DIAGNOSTIC PROCESS

You can diagnose your device by using the diagnose feature of **BitRaser Mobile Eraser & Diagnostics**.

Steps to diagnose a device using BitRaser Mobile Eraser & Diagnostics:

1. Run **BitRaser Mobile Eraser & Diagnostics**. Plug the iOS/Android device into the computer.
2. The **Devices** tab (selected by default) lists all the attached iOS/Android devices. The screen which appears is displayed below:



A device message appears after its connection. **For example**: In the above screen, an Android device shows the message '**Turn On USB Debugging**' and iOS device shows '**Trust Device**'. To continue from this stage, USB Debugging must be allowed on the Android device's end and Trust Device must be allowed on the iOS device's end.

***Note**: For more information, please refer to the section 'Enable USB Debugging in an Android device'.*

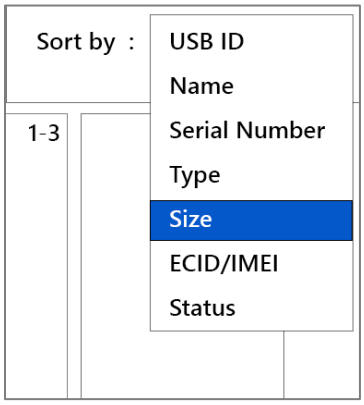
3. All the devices along with their information like process (**Erase** or **Diagnose)**, USB port name, type, progress bar, status, ECID/IMEI, and serial number are displayed. You can also see icons for connectivity status, SIM card status, and FMD (Find my device) locked/unlocked status.

***Note**: If you wish to change the process (**Erase** or **Diagnose**), click on the Erase (header area in green color) to change the process to Diagnose (header area in orange color) and vise versa.*

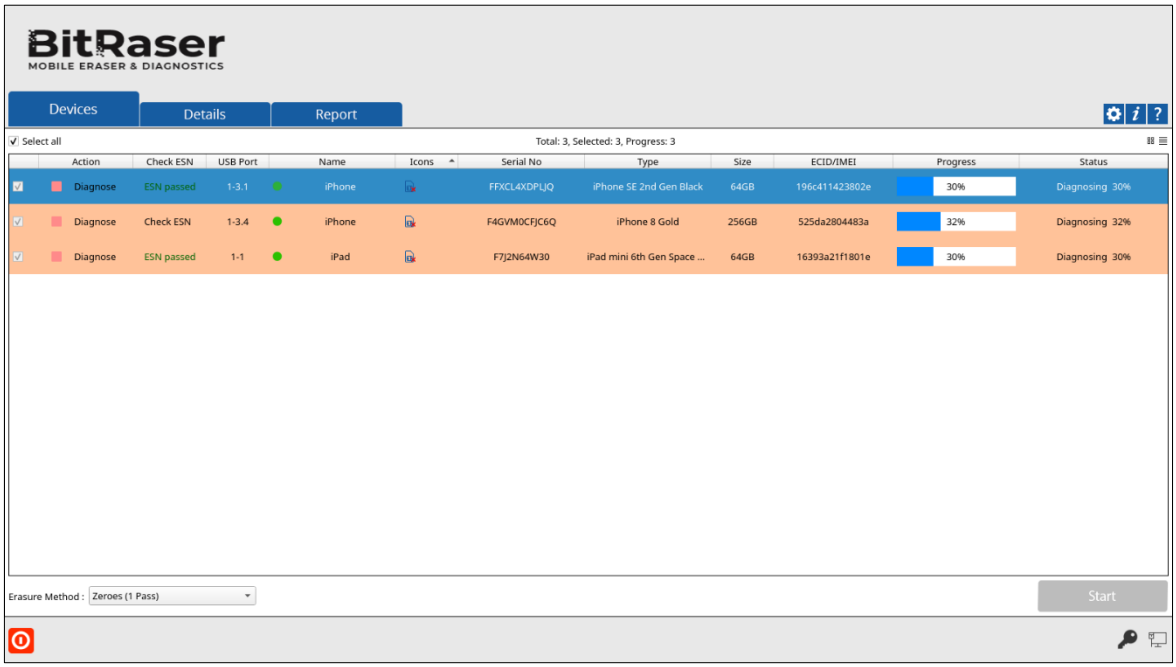
***Note**: If you wish to check the ESN status of the mobile device prior to **Diagnose** process, click on the **ESN check** (Footer area in blue color). For more information on how to make prior settings for this feature, see ESN check.*

4. You can preview the device's information either in a **Grid view** or **List view**.

   - In the **Grid view**, the devices get displayed in a grid-like structure, and also the devices can be sort using the **Sort By** option. The **Sort By** option allows sorting the devices based on the following information/criteria: USB ID, Name, Serial Number, Type, Size, ECID/IMEI, and Status.

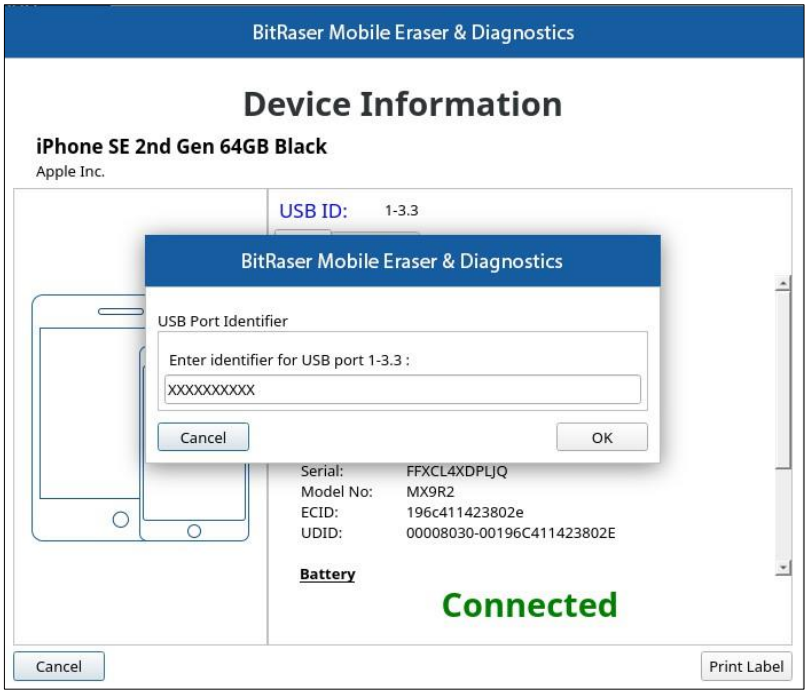


   - In the **List view**, the devices get displayed in a list.



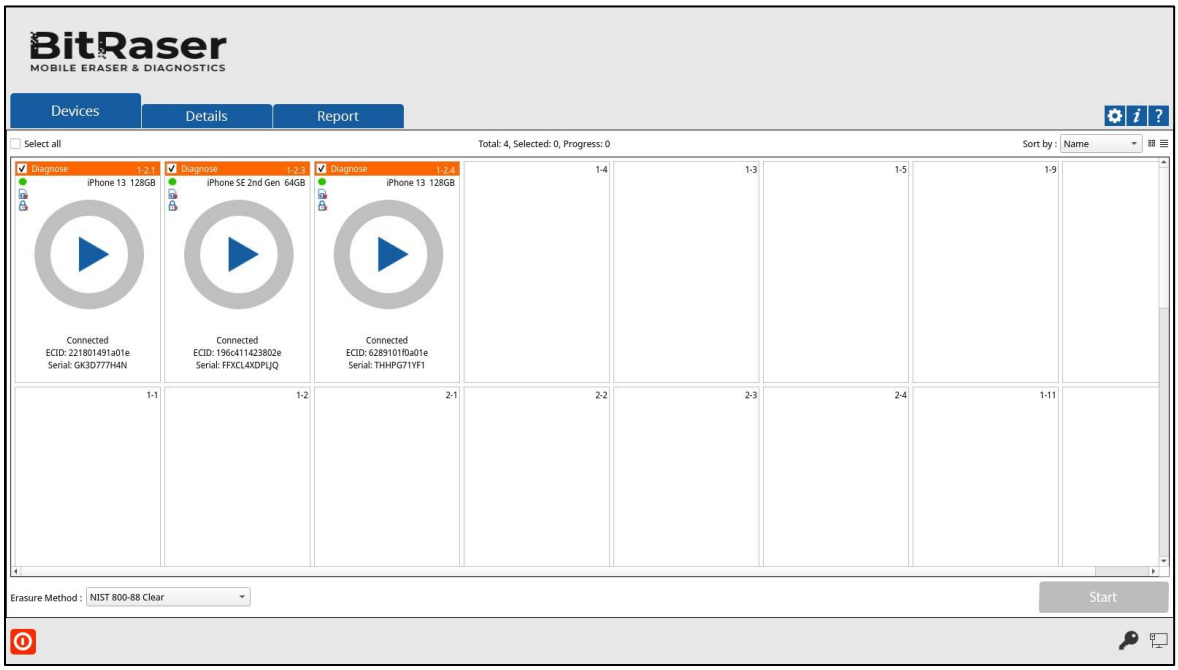
5. Clicking on any of the following devices will show device information of the corresponding device. These details can be printed by clicking on the **Print Label** button.

6. From the dialog that appears, click on **USB ID** to change the identifier for the USB port. Click **OK**.



7. Select the devices to diagnose by marking the check-box before every device.

   ***Note**: Mark **Select All** option to select every listed device for diagnosing.*



8. Click **Start** to start diagnosing the device.

***Note:** If you wish to diagnose a single device, you can start the process by simply clicking the play button in the middle.*

***Note**: At this stage, **BitRaser Mobile Eraser & Diagnostics** acquire license information from **BitRaser Cloud,** and licenses are consumed depending upon the number of devices you have selected for diagnostics. Therefore, you need an active internet connection to start the diagnostic process.*

***Tip:** It is recommended to enable Bluetooth, GPS (location services), and Wi-Fi on your device before starting the diagnostic process, to diagnose these services on your device.*

***Note:** On your iOS device, make sure you have enabled the Bluetooth from the Control Centre of your device. This is required to diagnose the Bluetooth service successfully.*

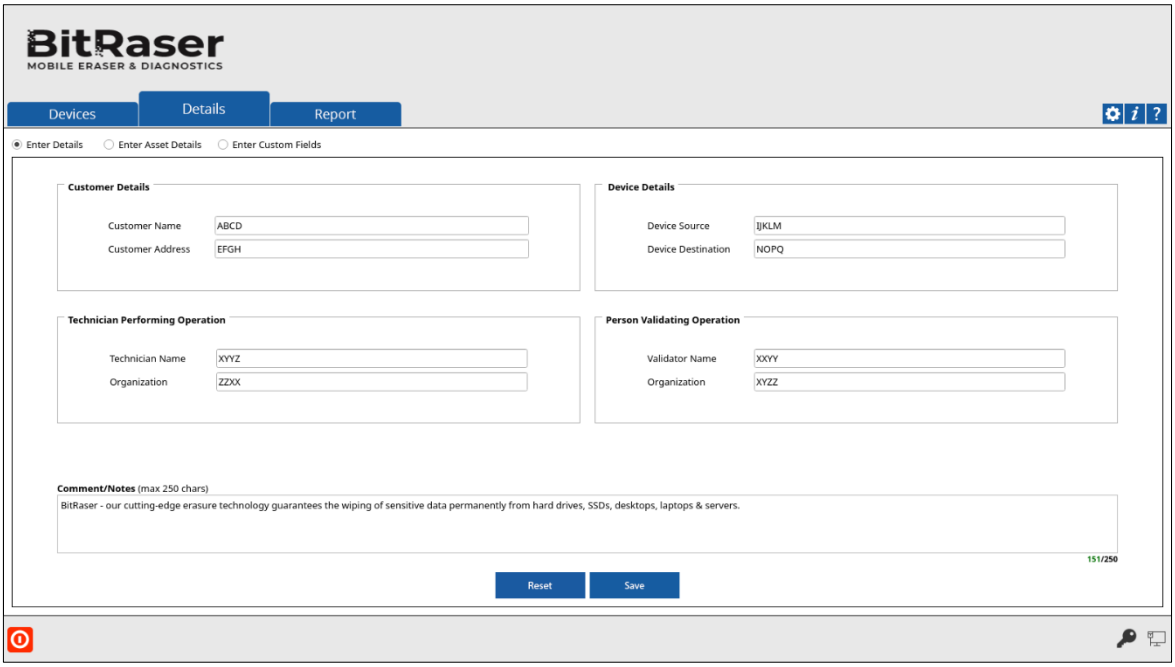
3.4. DETAILS SECTION

The **Details** section allows you to fill in the generic information related to the customer. These details must be entered by the user which can later be modified if required.

The information mentioned in these fields will be added to the **Report**. The **Details** section have the following three sub-sections:

1. **Enter Details**

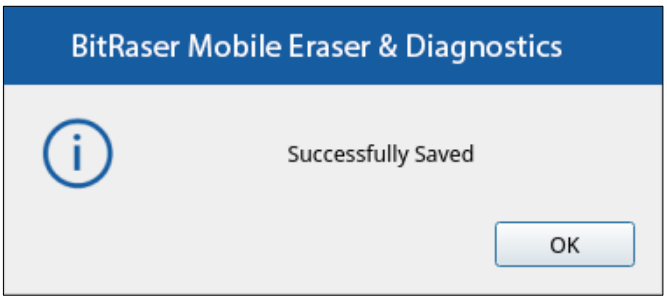
FIELD NAME	DESCRIPTION
Customer Details	This section allows you to enter the details of the customer.
Customer Name Customer Address	Name of the customer for whom the erasure or diagnosis is to be done. Location of the customer for whom the erasure or diagnosis is to be done.
Device Details	This section allows you to enter the details of the device.
Device Source Device Destination	You get an option to record the source (user who has handed over the device) and destination (user who will be assigned the device after erasure or diagnosis) of the device.
Technician Performing Erasure	This section allows you to enter the details of the technician who is going to perform the process.
Technician Name Organization	Name of the technician processing the device. Name of the organization providing the service.
Person Validating Erasure	This section allows you to enter the details of the person validating the process.
Validator Name Organization	Name of the person validating the process. Name of the organization validating the process.
Comment/Notes	This section allows you to enter any other comments or notes that you want to include in the report. You can enter up to a maximum of 250 characters.



You can reset these fields using the **Reset** button located at the bottom of the **Details** dialog box.

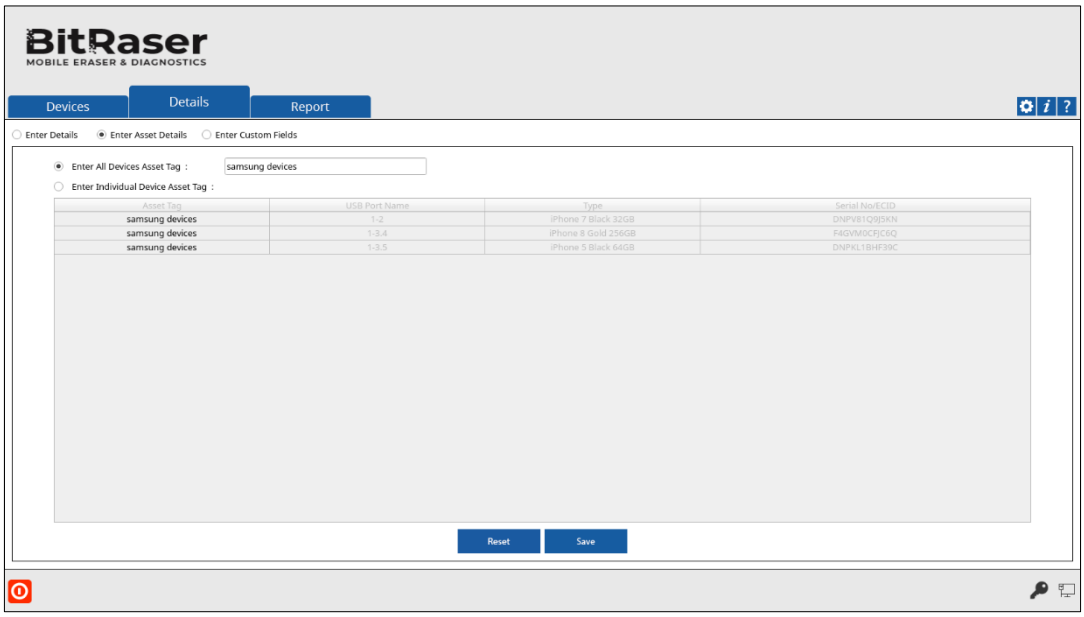
After making the required changes to **Details**, click **Save** to continue.

A ***Saved Successfully*** dialog appears. Click **OK**.



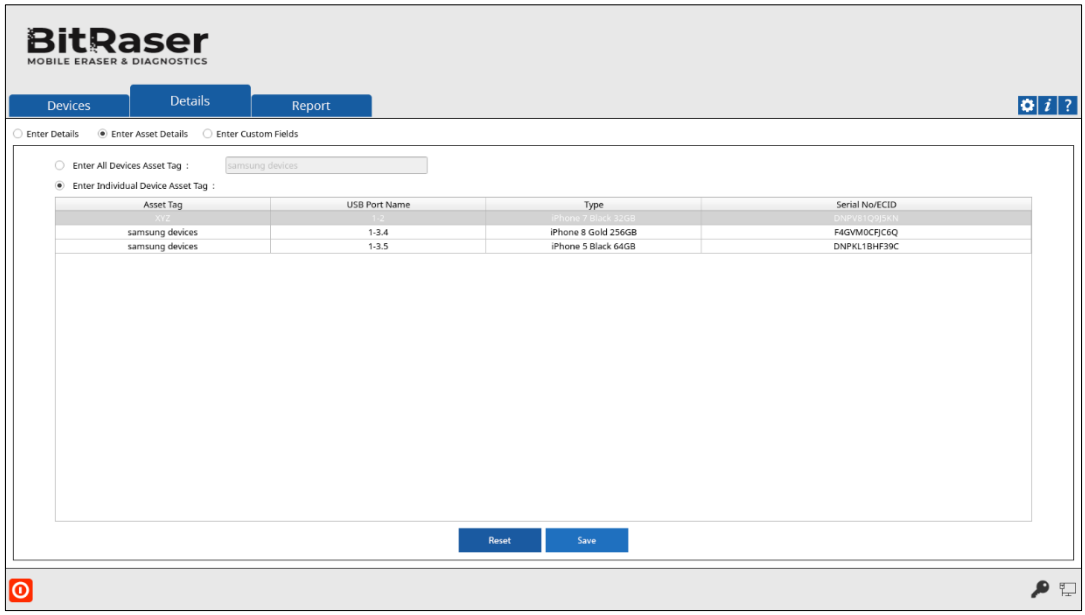
2. **Enter Asset Details**

- To set a particular asset tag for all the devices, select the radio button '**Enter all Devices Asset Tag**' and enter the asset tag in the corresponding text box.



- To set an individual asset tag for the device, select the radio button '**Enter individual Device Asset Tag**' and enter the **Asset Tag** for each device, this section has the following fields:

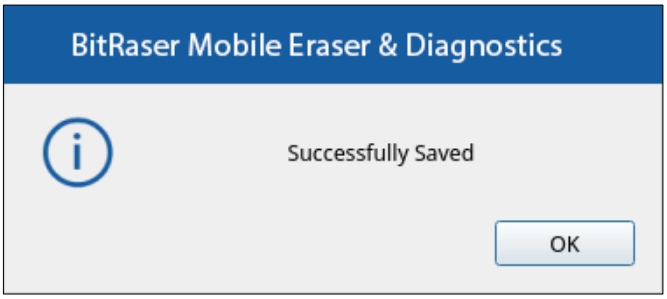
FIELD NAME	DESCRIPTION
Asset Tag	Enter the Asset Tag associated with the device.
USB Port Name	The USB Port name is set by default.
Type	The Device Type is set by default.
Serial No/ECID	The Serial No/ECID associated with the device is set by default.



You can reset the asset tags that you entered using the **Reset** button located at the bottom of the **Details** dialog box.

After making the required changes to **Details**, click **Save** to continue.

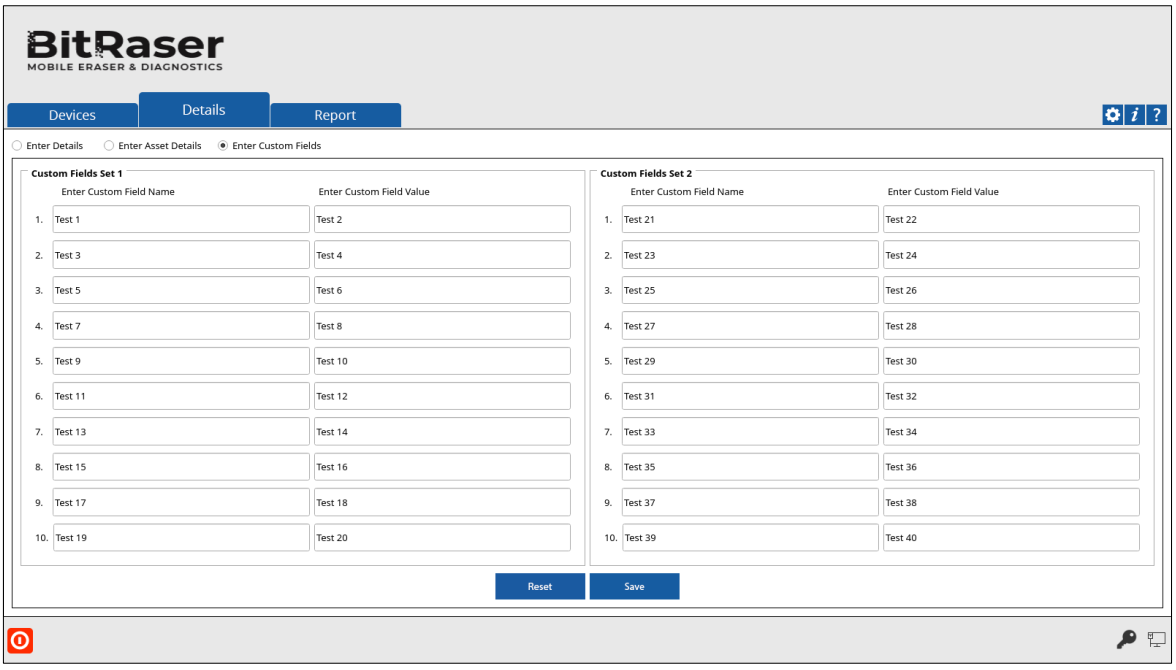
A ***Saved Successfully*** dialog appears. Click **OK**.



3. **Enter Custom Fields**:

   BitRaser Mobile Eraser & Diagnostics also allows you to create custom fields to enter in the Reports. You can create up to two sets of custom fields with each Custom Field Set containing up to 10 custom fields. The following two fields are available for each set:

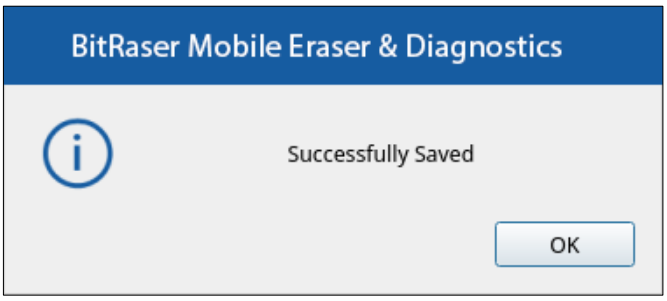
   - **Enter Custom Field Name**: Allows you to enter the name of the custom field.
   - **Enter Custom Field Value**: Allows you to enter the value of the custom field.



You can reset these fields using the **Reset** button located at the bottom of the **Details** dialog box.

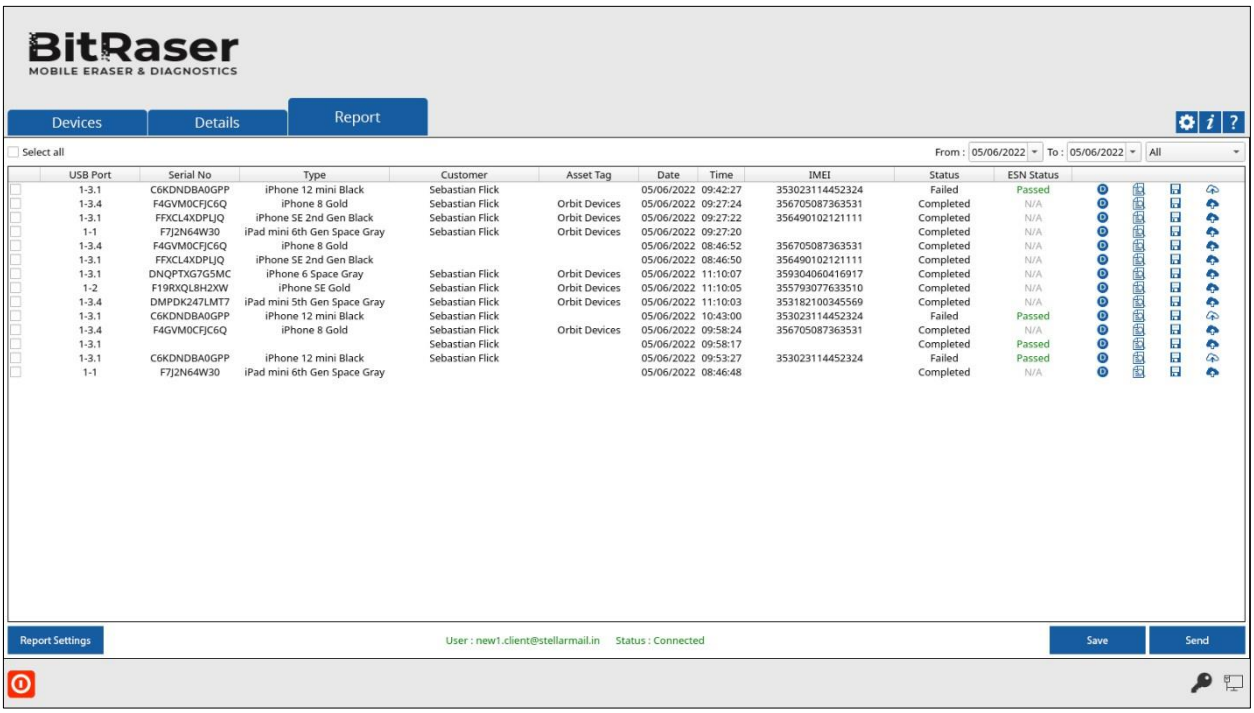
After making the required changes to **Details**, click **Save** to continue.

A ***Saved Successfully*** dialog appears. Click **OK**.



3.5. WORKING ON REPORTS

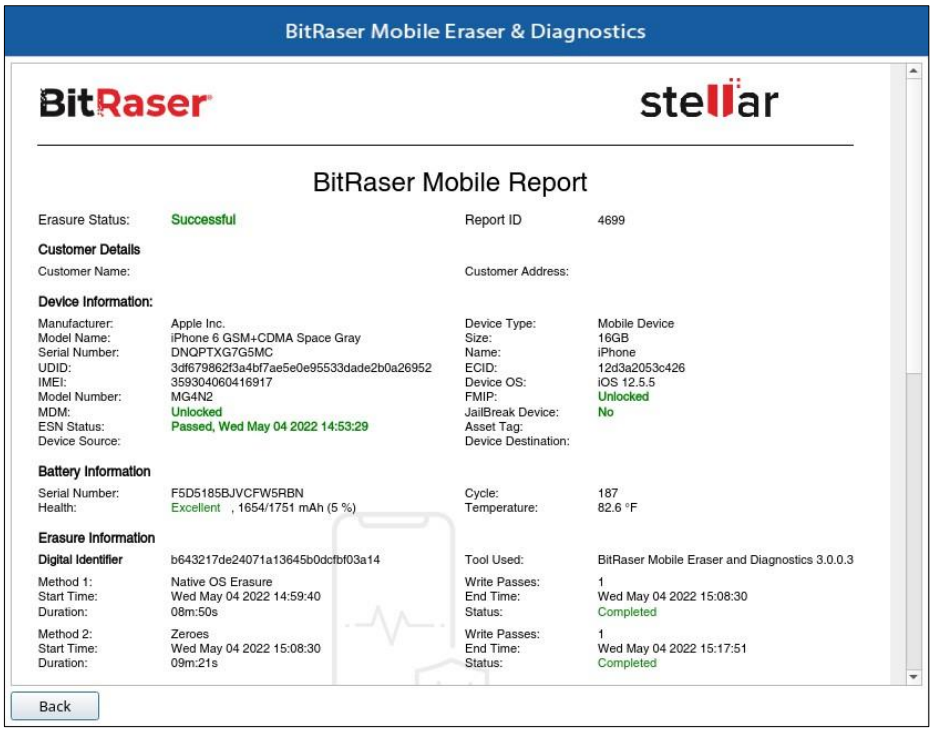
The **Report** tab in the **BitRaser Mobile Eraser & Diagnostics** application displays all of the erasure and diagnostic processes that either have been completed or failed.



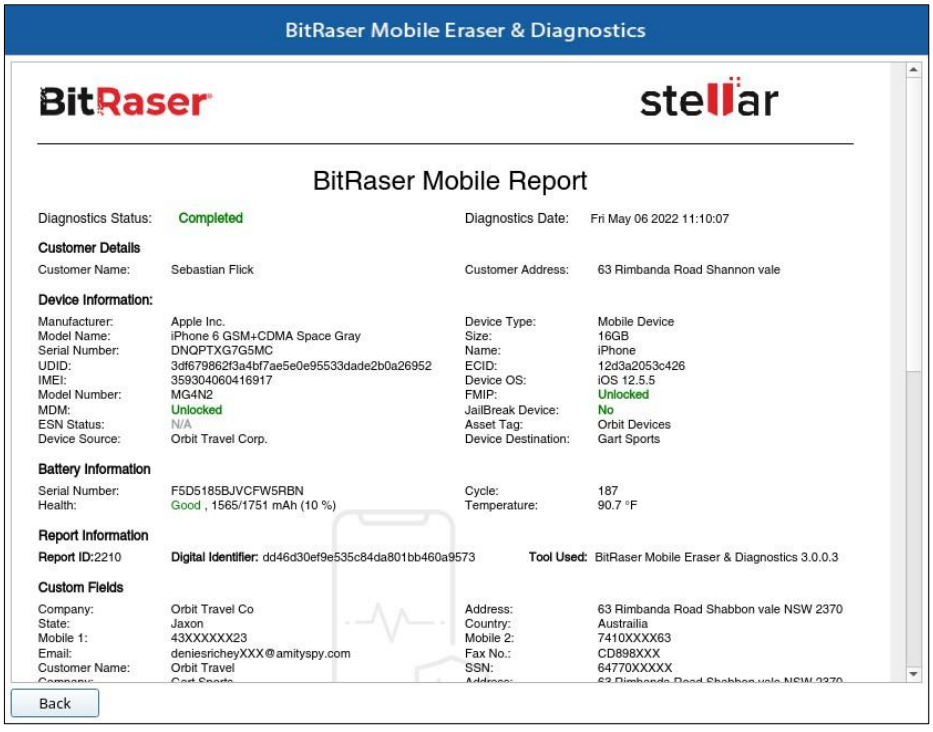
BitRaser Mobile Eraser & Diagnostics gives an option to search reports for the processes performed. Based on the specification of records, different filters help in fetching records more quickly. You can search for multiple reports using certain search criteria. This makes the search operation efficient as the user can straight away find the intended result.

BitRaser Mobile Eraser & Diagnostics provides you with erasure and diagnostic reports as follows:

- An erasure report provides information such as Customer Details, Device Information, Battery Information, Erasure Information, Erasure & Validation Details. A sample erasure report is given as follows:

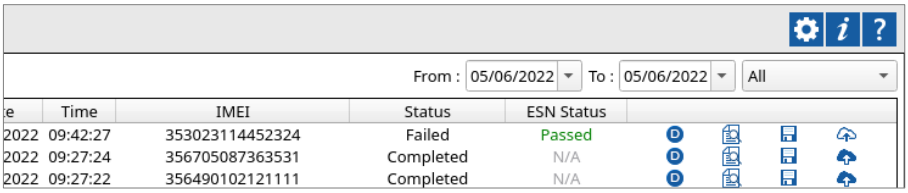


- A diagnostic report provides information such as Customer Details, Device Information, Battery Information, Diagnostic Information, Diagnostic & Validation Details. A sample diagnostic report is given as follows:



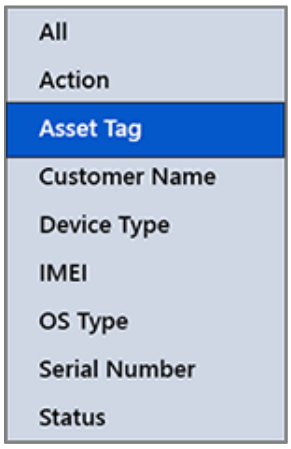
To search BitRaser Mobile Eraser & Diagnostics reports:

1. Run **BitRaser Mobile Eraser & Diagnostics**. Select the **Report** tab.
2. The upper right pane of the screen, shows the criteria to be entered. This can be set up depending on what the user wants.



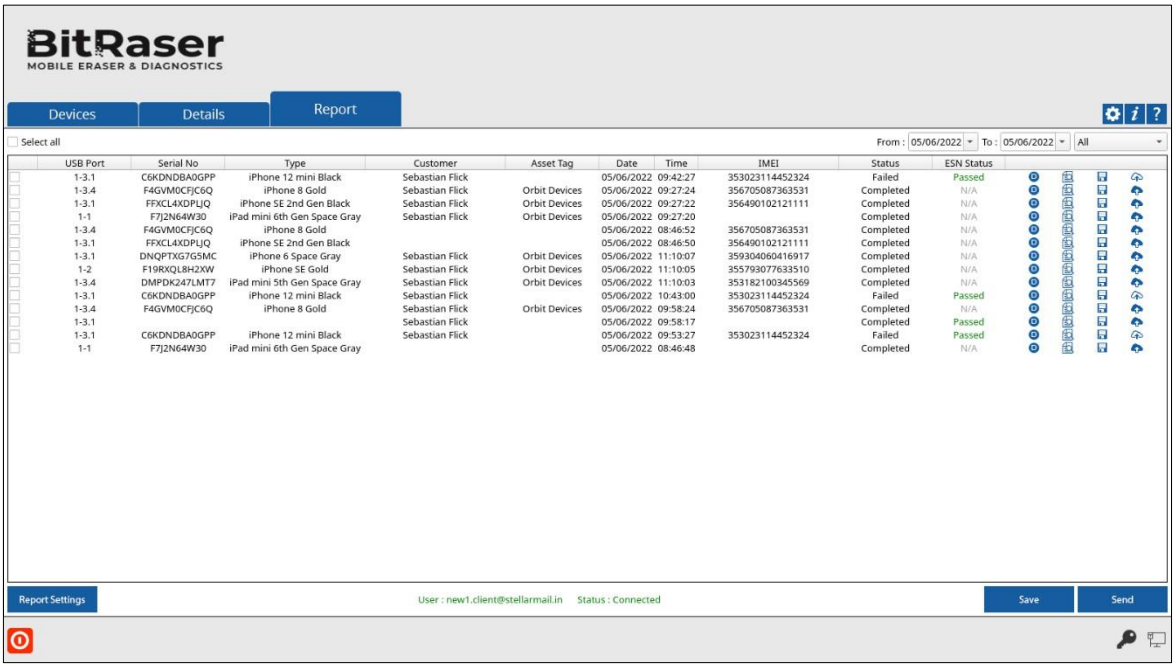
Specify the date range in the **From** and **To** fields, if you want to search reports for processes performed from a specific period i.e., between two dates.

The '**All**' drop-down button displays:



- **Action:** This option enables you to filter data based on the type of process (Diagnose or Erase).
- **Asset Tag**: Select this option if you know the asset tag assigned to a device.
- **Customer Name**: Select this option if you know the person who performed the erasure process.
- **Device Type**: This option enables you to filter data based on the type of device and/or its model.
- **IMEI**: Select this option if you know the IMEI number of a device.
- **OS Type**: This option enables you to filter data based on the type of operating system on your device.
- **Serial Number**: Select this option if you know the serial number of a device.
- **Status**: Select this option if you know the process status i.e., Completed, Failed, or Running.

3. The application will show all the reports fulfilling the search criteria. A list of all the reports generated on the specific time period mentioned, along with the information like USB Port, Serial No, Type, Customer Name, Asset Tag, Date, Time, IMEI, Status, and Action are displayed.



4. The **Action** tab provides the shortcuts to perform the following functions:
   - **Process icon** or : This shows an icon indicating the Erasure or Diagnostic process.
   - **Preview** : This function enables you to see how the **Report** looks like before you save or print it.
   - **Save** : This option allows you to save the **Report** in PDF, XML, and CSV formats. The reports can be saved to an external storage device, not to the device where **BitRaser Mobile Eraser & Diagnostics** application is launched.
   - **Send to Cloud** : This option allows you to send the reports over the **BitRaser Cloud**.
5. In case you want to customize the report, select the **Report Settings** button

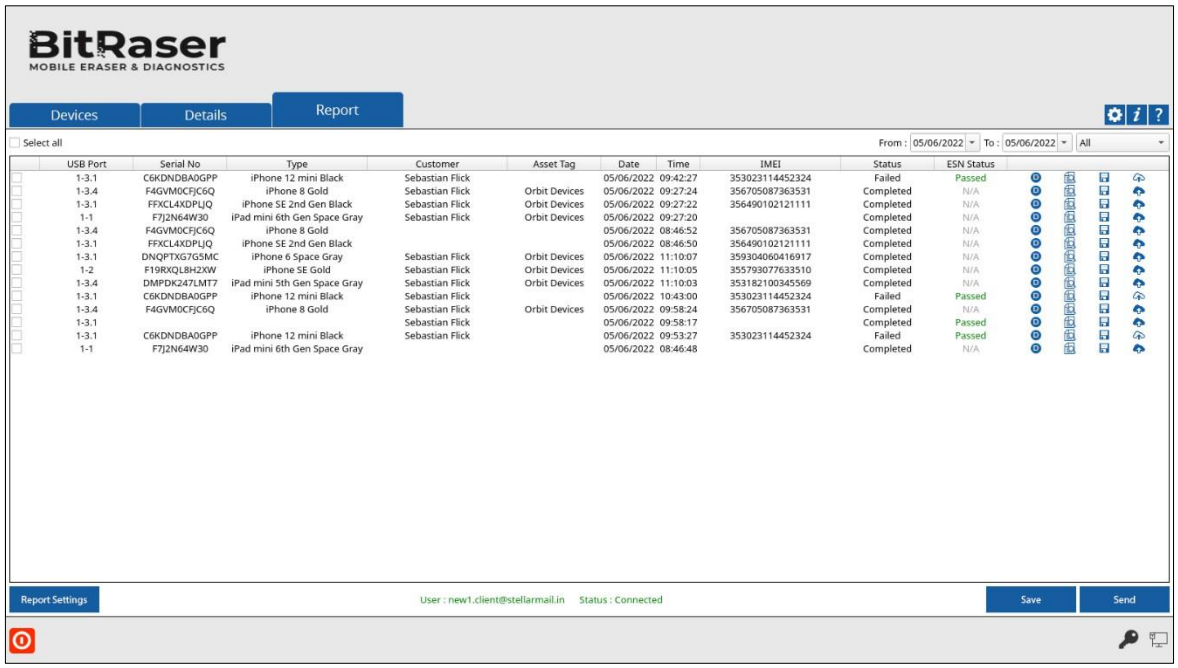
located at the bottom left of the screen.

3.5.1. PREVIEW REPORT

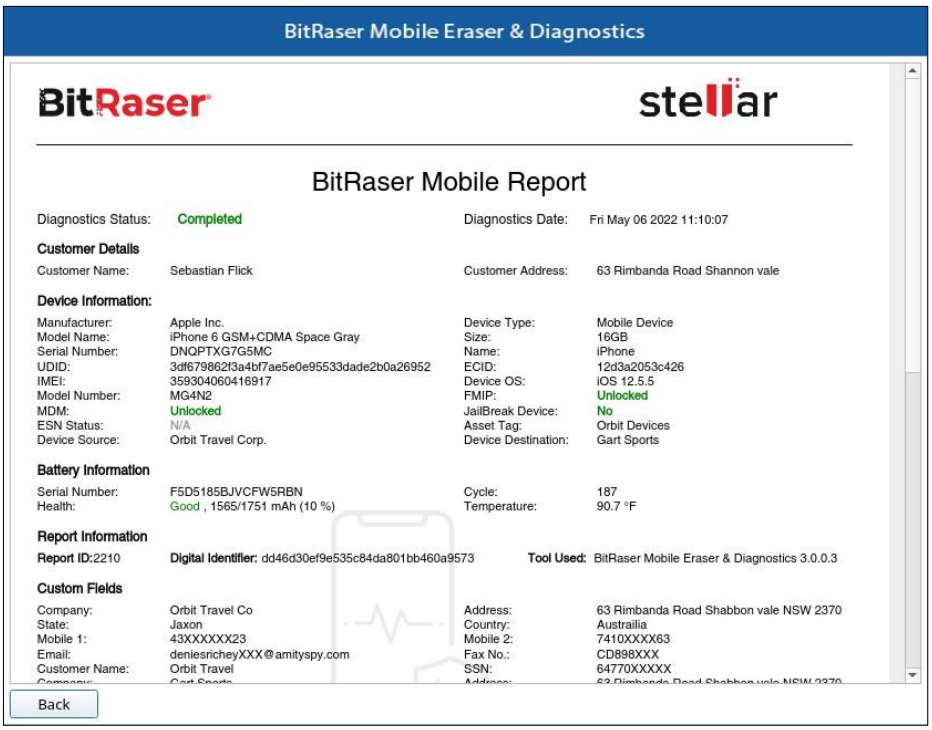
BitRaser Mobile Eraser & Diagnostics allows you to preview a report after it has been generated. This function enables you to see how the report looks like before you save/print it. You cannot make any changes in preview mode. The report contains information like Customer Details, Device Information, Erasure or Diagnostic Information, Technician performing the process, and Person validating the process.

To preview a report:

1. Select the **Report** tab.
2. Click **Preview** button from the **Action** tab of the report that you want to preview.



3. The report will be displayed in a new window as shown below.



***Note**: You cannot preview more than one report at a time.*

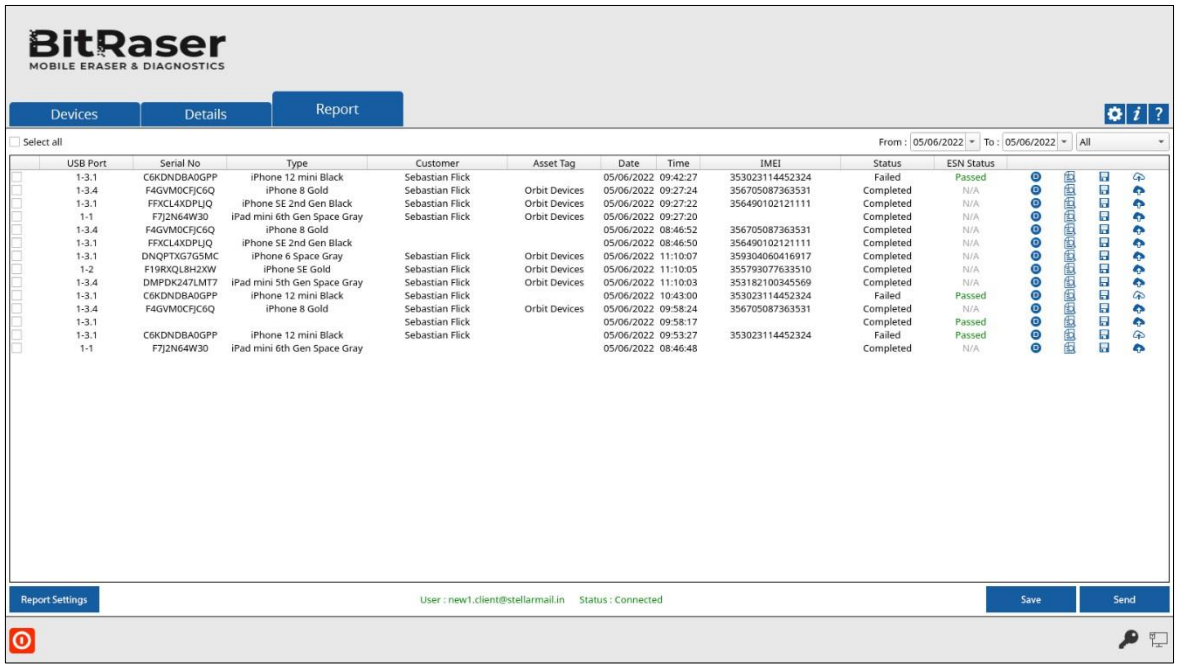
3.5.2. SAVE REPORT

You can save a report for future use once it has been generated. The report can be saved in PDF, XML, or CSV format.

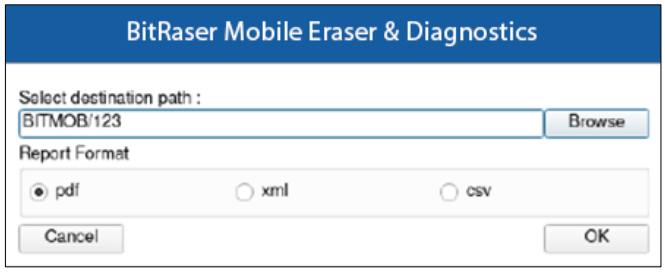
To Save an erasure Report:

1. Select the **Report** tab.

2. Select the desired reports which you want to save by checking on the check-boxes. You can click **Select All** to select all the files.



3. Click on the **Save** button at the lower pane of your screen to save all the selected reports. Alternatively, you can click **Save** button from the **Action** tab to save one report at a time. A dialog prompts as illustrated below:



4. Click **Browse** to select a destination to save the report file in external media.

5. Select the desired format as **PDF**, **XML, or CSV**. Click **OK** to proceed.

***Note**: The report cannot be saved to the hard drive where **BitRaser Mobile Eraser & Diagnostics** is launched.*

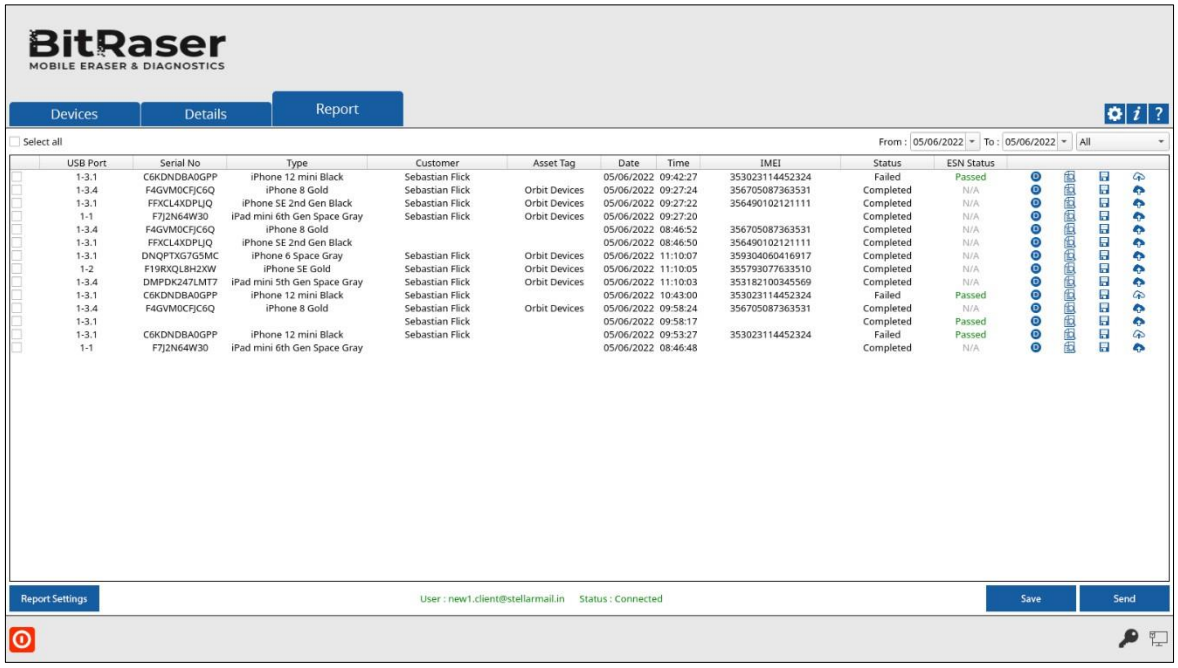
3.5.3. SEND REPORT TO BITRASER CLOUD

BitRaser Mobile Eraser & Diagnostics provides you with an option to send the selected reports to the **BitRaser Cloud**. This requires that the connection to the Cloud Console is working i.e., the user must be connected to the Cloud.

Note: *Checking the '**Auto send completed report to cloud**' option in the General Settings section of the **Settings** window automatically sends the report to the BitRaser Cloud Console.*

To send reports to the cloud:

1. Select the **Report** tab.
2. Select the desired reports which you want to send.



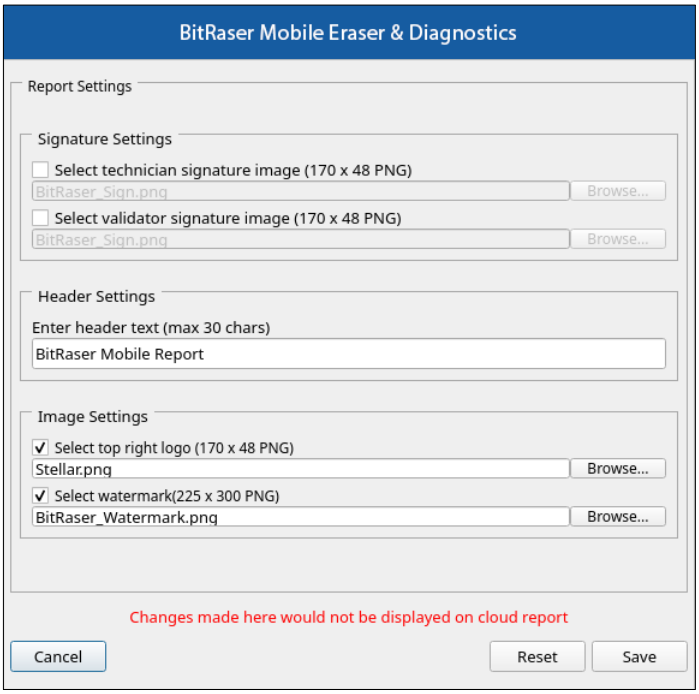
3. Click on **Send** button located at the lower pane of your screen to send the selected reports over **BitRaser Cloud**. Alternatively, click button from the **Action** tab of the report that you wish to send.

   Note: *icon shows that the report has been sent to BitRaser Cloud successfully and shows that the report has not been sent to BitRaser Cloud.*

4. The desired reports will be sent to the **BitRaser Cloud Console**.

3.5.4. CHANGE REPORT SETTINGS

To customize the report, select the **Report Settings** button located at the bottom left of the screen.



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

Field Name	Description
Report Settings	This section allows you to customize Reports like signature settings, header settings, top-right logo, and watermark.
Signature Settings	This section allows you to add a signature image of the technician and validator.
Select technician signature image (170 x 48 PNG) Select validator signature image (170 x 48 PNG)	You can change the technician's signature image here. You can change the validator's signature image here.

Header Settings	You can either enter Header information like header text or header image here.
Enter header text (max 30 characters)	Enter the header text.
Image Settings	This section allows you to add the top-right logo and watermark image.
Select top right logo (170 x 48 PNG) Select watermark (225 x 300 PNG)	You can change the top-right logo image of the report here. You can change the watermark image of the report here.

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

***Note**: Signature images, Logo, and Watermark image size needs to be the same as specified in Report Settings. **BitRaser Mobile Eraser & Diagnostics** will accept images with a specified size only. In the case of a size mismatch, **BitRaser Mobile Eraser & Diagnostics** will continue to use the previously selected images.*

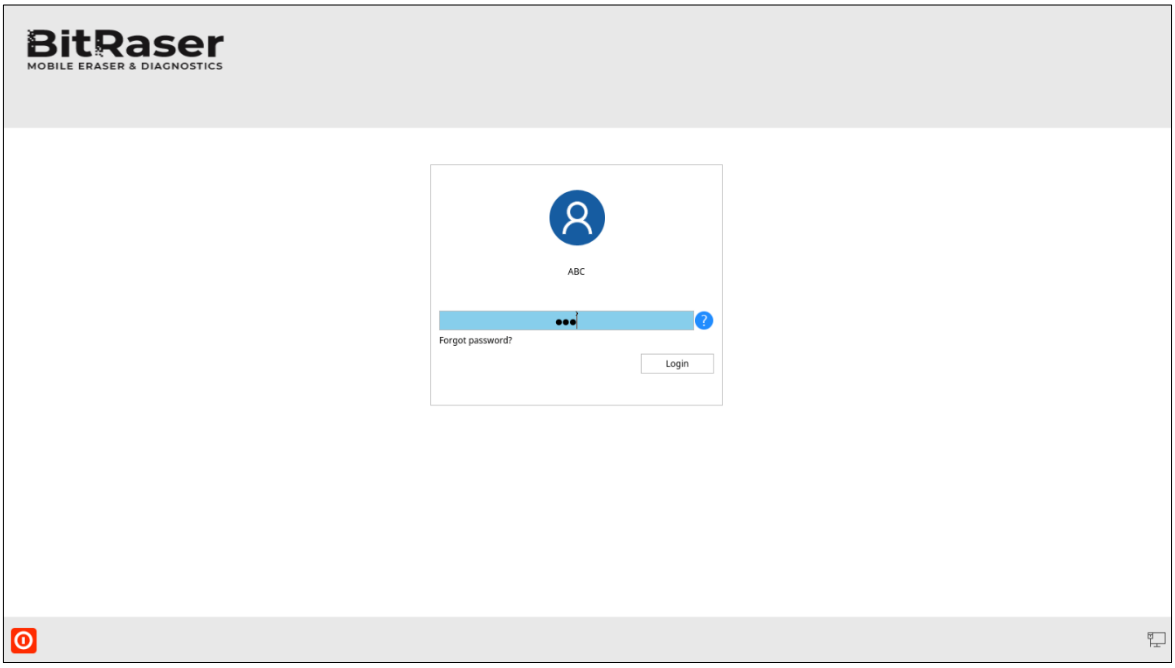
- After making the required changes to **Report Settings**, click **Save** to update settings.

***Note**: Changes made to reports settings in **BitRaser Mobile Eraser & Diagnostics** application will not be updated on the **BitRaser Cloud** report.*

3.6. FORGOT LOGIN PASSWORD

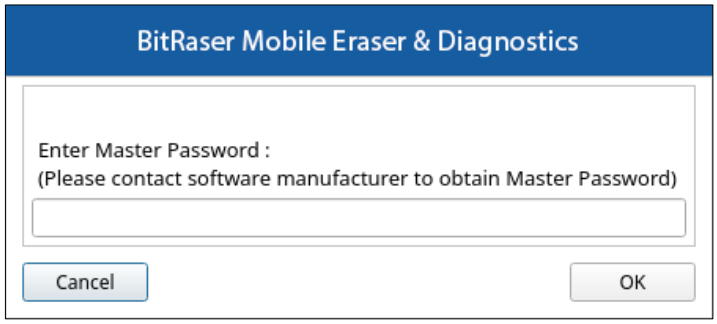
BitRaser Mobile Eraser & Diagnostics provides an option to reset your login password if you forget it. The software also has an option to set and view a **Password Hint** to help you remember your old password.

If you have set a **Password Hint** at the time of Creating New User Profile, you can view the hint by hovering your mouse cursor over **Password Hint Icon** on the **User Login** screen:



If you don't remember your password, use the following steps to reset it:

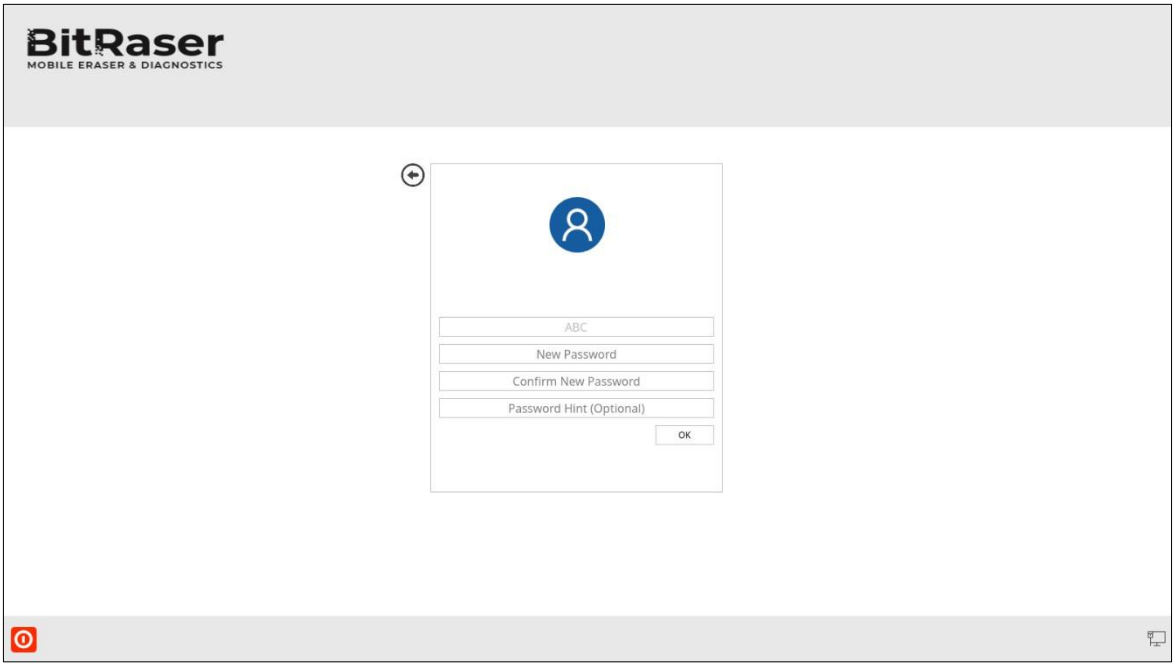
1. On the **User Login** screen, click on **Forgot password?**. The **Enter Master Password** screen appears as shown below:



2. Enter the Master Password that you received along with **BitRaser Mobile Eraser & Diagnostics** software from Stellar and click **OK.**
   ***Note**: The master password is a unique password sent to you by Stellar along with the **BitRaser Mobile Eraser & Diagnostics** software.*

3. The Reset password screen appears if the master password that you have entered is correct. The screen has the following fields:

    - New Password
    - Confirm New Password
    - Password Hint (Optional)



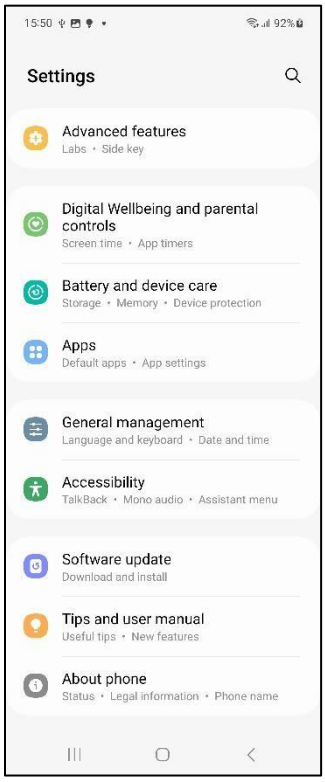
4. Fill in the above fields and click **OK** to reset the password.

3.7. ENABLE USB DEBUGGING IN AN ANDROID DEVICE

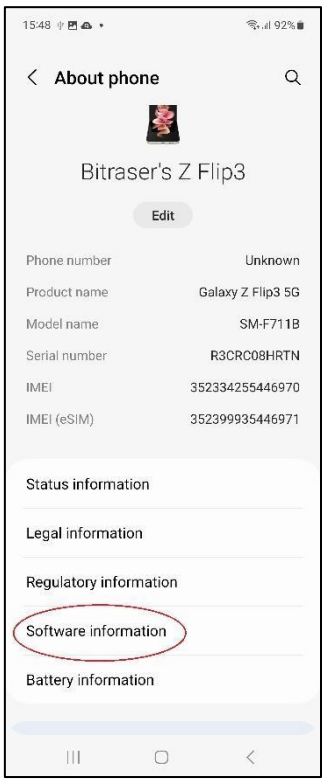
In order to initiate the erasure process on an android device, the **USB Debugging** must be in **ENABLE** mode for the device you are connecting.

Follow the steps below to enable USB Debugging:

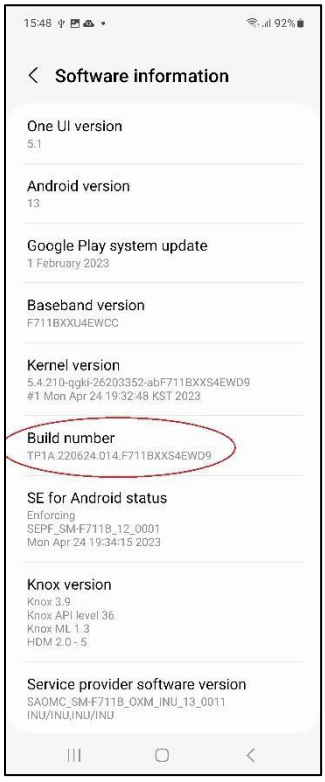
1. Go to settings in your android device and click **"About phone"** option.



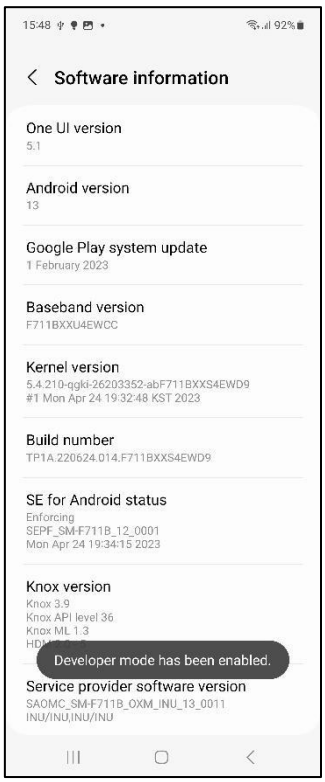
2. Select **"Software information"** from the about device page.



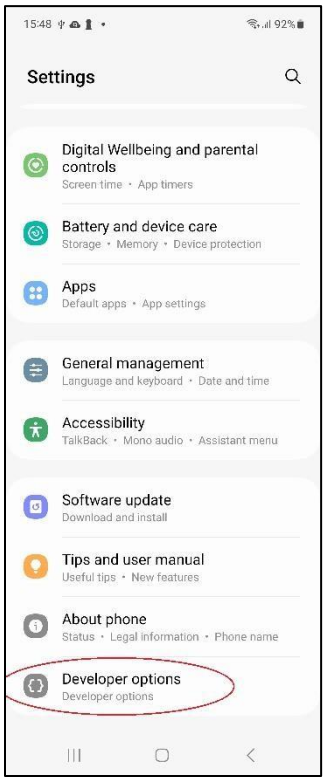
3. Tap the **Build number** eight times to make **Settings** > **Developer Options** available.



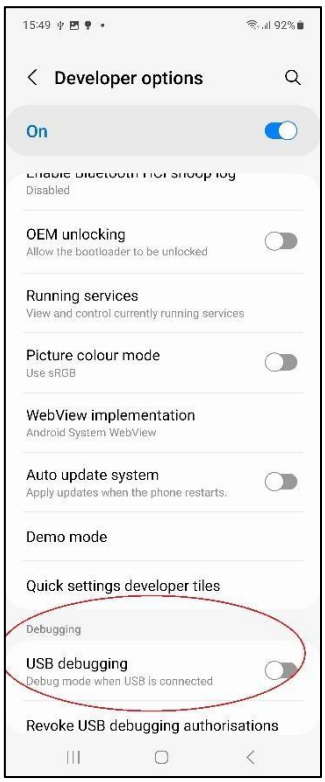
4. A notification saying **"Developer mode has been enabled"** appears.



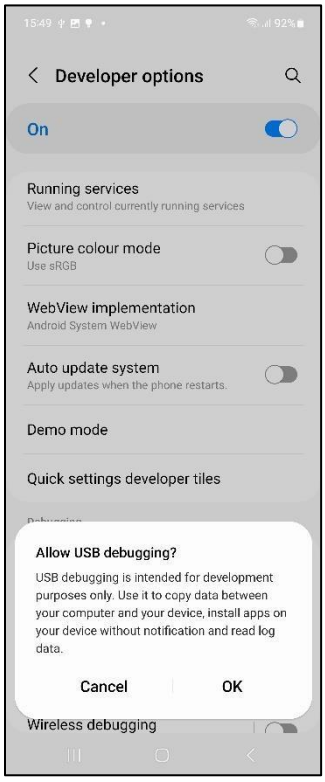
5. Go back to the setting page and scroll down until you see "**Developer options**". Select **Developer options**.



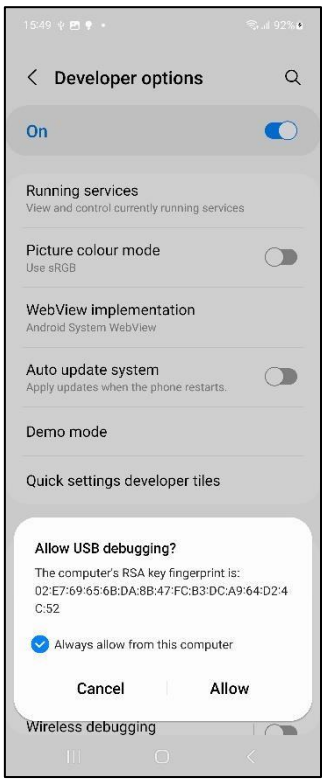
6. On the Developer Options page scroll down and enable **USB debugging**.



7. Once you enable **USB debugging**, A dialog box asking **"Allow USB debugging?"** appears. Click **OK** to confirm.



8. For final confirmation, the dialog box asking **"Allow USB debugging?"** with your computer's information appears. Click **Allow**.



Note: *select* ***"Always allow from this computer"*** *checkbox to avoid repeating the process again.*

4. FREQUENTLY ASKED QUESTIONS (FAQ)

1. **I want to erase or diagnose multiple iOS devices at a time, is it possible to do so using BitRaser Mobile Eraser & Diagnostics?**

   Yes, **BitRaser Mobile Eraser & Diagnostics** allows you to erase or diagnose multiple iOS devices at the same time.

2. **Does BitRaser Mobile Eraser & Diagnostics support other languages?**

   BitRaser Mobile Eraser & Diagnostics is currently available in the **English** language only.

3. **Is it possible to edit the existing fields of the report?**

   Yes, you can edit existing fields from the report of **BitRaser Mobile Eraser & Diagnostics** as per your requirement.

4. **Is it possible to edit the USB Identifier for the USB Port of a particular device?**

   Yes, **BitRaser Mobile Eraser & Diagnostics** allows you to change the identifier for the USB port.

5. **Why do iOS devices need a firmware update and Android devices do not?**

   iOS uses Cryptographic Erasure. In this process, the firmware is downloaded and restored on the device. Encryption keys are changed and the data on the device is rendered inaccessible. After this, other overwrite methods may be applied. In the case of **Android** devices, a traditional overwrite of all storage and a factory reset is done, thus a new firmware is not needed.

6. **When I erase an android device, the erasure process comes to a standstill at 8 percent. Why does this happen?**

   When you install **BitRaser Mobile Eraser & Diagnostics** on a device running Android OS, you control which capabilities or information **BitRaser Mobile Eraser & Diagnostics** can access—known as **Permissions**. Thus, the user needs to grant all the required permissions for the erasure process to proceed.

7. **When I try to erase or diagnose a device, I get a failed status. What could be the problem?**

   Failure of the process mostly occurs due to the following reasons:

   - There might be some issues with internet connectivity. Make sure that your internet connection is active.
   - Your USB cable has probably disconnected or is not supported. Make sure you are using a genuine USB cable provided by your device manufacturer. Reconnect your device and then try to erase or diagnose it again.
   - The USB port on your computer is loose or not functioning properly. Change the USB port and try again.

8. **I got failed status while performing erasure or diagnostic process but the license was consumed. Will another license be consumed if I start another process?**

   No, you can perform the erasure or diagnostic process again within 24hrs without consuming another license for the same device.

9. **Which algorithm should I choose for the best erasure?**

   It depends upon how many times an algorithm overwrites the data precisely or the number of passes used to erase the data. More the passes used by the algorithm, the more effective it is. Each algorithm performs a different set of features from where you can choose the suitable algorithm as per the requirement.

10. **I want to perform a diagnostics process on my Redmi phone. After connecting my phone, the software is asking me to install an app on my device. How to install the app?**

    BitRaser Mobile Eraser & Diagnostics need a **BitraserMobileDiagnostics.apk** (application) to be installed manually on **Redmi** phones, to perform the diagnostic process. See Procedure to install **BitraserMobileDiagnostics.apk** on **Redmi** Phone to know the required steps.

11. **The application is taking too long to erase the data. Why does this happen?**

    It depends on the size of the data you are erasing, the configuration of the system, and the algorithm you are using to erase the data. A large amount of data, lesser configuration, and more number of passes may consume more time for erasure.

12. **Can I erase data from MDM (Mobile device management) from my mobile device?**

    Yes, **BitRaser Mobile Eraser & Diagnostics** can erase data from MDM (Mobile Device Management) Apple Inc. mobile (iPhones, iPads and iPod Touch) devices only.

13. Can I erase data from Jailbreak mobile devices?

Yes, **BitRaser Mobile Eraser & Diagnostics** can erase data from Jailbreak Apple Inc. mobile (iPhones, iPads and iPod Touch) devices only.

14. Why do I need to check the ESN status of the mobile device before Erasure/Diagnostics process?

ESN check gives you a precise information if the device is reported, blacklisted or a genuine product. This way, you can rest assured that you can perform data Diagnostics/Erasure on a genuine product. Refer to ESN Check for more details.

5. LEGAL NOTICES

PLEASE READ THIS EULA CAREFULLY.

This End User License Agreement (hereinafter called "EULA" or "AGREEMENT" contains important terms and conditions relating to the use and license of the software.

BY DOWNLOADING, INSTALLING, COPYING, ACCESSING OR USING THIS SOFTWARE, ALL OR ANY PORTION OF THIS SOFTWARE "YOU" OR "CUSTOMER" OR "LICENSEE" ACCEPT & AGREE TO BE BOUND BY ALL THE TERMS AND CONDITIONS OF THIS EULA; INCLUDING IN PARTICULAR THE LIMITATIONS & LIABILITY CLAUSE.

IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, WE WILL NOT LICENSE THE SOFTWARE AND DOCUMENTATION TO YOU AND YOU MUST DISCONTINUE THE INSTALLATION PROCESS NOW, AND PROMPTLY RETURN THE SOFTWARE AND PROOF OF ENTITLEMENT TO THE PARTY FROM WHOM YOU ACQUIRED THE SOFTWARE.

This EULA is a legal and binding agreement between you, being either an individual or a single entity (Herein after referred to as "you" or "your" or "customer" or "licensee") and Stellar Information Technology Pvt. Ltd., having its registered address at 205, Skipper Corner, 88, Nehru Place, New Delhi, India 110019 & its subsidiaries (Herein after referred to as "Stellar" or "We" or "Licensor").

1. DEFINITIONS

1.1. "Computer" means a virtual or physical device that accepts information in digital or similar form and manipulates it for a specific result based on a sequence of instructions, including without limitation desktop computers, laptops, tablets, mobile devices, telecommunication devices, Internet-connected devices, and hardware products capable of operating a wide variety of productivity, entertainment, or other software applications.

1.2. "Compatible Computer" means a computer with the recommended operating system and hardware configuration as stated in the Documentation contained in the Software.

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

1.4. "License" means the limited right given by Stellar to use the Software for specific purpose in accordance with this EULA.

1.5. "Permitted Number" means one (1) in number unless otherwise indicated under a valid license (e.g., volume license) granted by Stellar.

1.6. "Software" means (a) all of the information with which this agreement is provided, including but not limited to: (i) all software files and other computer information; (ii) any proprietary scripting logic embedded within exported file formats (iii)images, sounds, clip art, video and other works bundled with Stellar software or made available by Stellar on

Stellar's website for use with the Stellar software and not obtained from Stellar through a separate service (unless otherwise noted within that service) or from another party ("Content Files"); (iv) related explanatory written materials, help manuals and files ("Documentation"); and (v) any modified versions and copies of, and upgrades, updates, and additions to, such information, provided to you by Stellar at any time, to the extent not provided under separate terms (collectively, "Updates").

2. LICENSE GRANT

Right to use the Software: Subject to the terms and conditions of this Agreement, Stellar grants you a non-exclusive, non-transferable, non-perpetual, revocable and limited right to use the Software on a single computer or workstation for your internal purposes in accordance with the license type.

3. LICENSE TYPES

3.1. Pay Per Use License: This license requires you to pay for every license consumed. License will be consumed on every use of the software to perform a task such as drive erasure, mobile erasure or device diagnostics and one license is deducted from your total pool of purchased licenses.

3.2. Subscription License: This License allows you unlimited use of the software for a defined period of time (annually or monthly basis) on Permitted Number of computers. Upon expiration, the subscription must be renewed to continue using the software. Subscriptions may be set to renew automatically unless you opt out. Ongoing access to a Subscription License requires an uninterrupted Internet connection to activate, renew, and validate the license. If Stellar does not receive the recurring subscription payment or cannot validate the license periodically, then the Software may become inactive without additional notice until Stellar receives the payment or validates the license. You agree that Stellar may change the type of Software (such as specific components, versions, platforms, languages, etc.) included in the Subscription License at any time and shall not be liable to you whatsoever for such change.

4. SOFTWARE SUPPORT

Support will be provided to you for a period of 1 Year from the date of purchase. Free Technical Support is provided for 1 Year from the date of purchase, if your license term is greater than 1 year then you may avail Technical Support by paying an additional fee applicable at that time. Stellar will not assist you for any technical support request after 3 years from the date of purchase of the software.

5. INTELLECTUAL PROPERTY OWNERSHIP

Stellar has proprietary rights in the Software, its source code and Documentation which are protected by copyright and other intellectual property laws of India, United States and other countries, and by international treaty provisions. Stellar shall at all times retain all rights, title, interest, including intellectual property rights, in the Software or Documentation. Customer acknowledges that, all intellectual property rights in the Software belong to and/or are Licensed to Stellar. The rights granted to Customer in the Software are only licensed (and not sold), and Customer have no rights in, or to, the Software or the Documentation other than the right to use them in accordance with the terms of this EULA. All rights not expressly granted are reserved by Stellar.

6. LICENSEE RESTRICTIONS & REQUIREMENTS

6.1. Proprietary Notices. Any permitted copy of the Software (including without limitation Documentation) that Customer makes must contain the same copyright and other proprietary notices that appear on or in the Software.

6.2. Use Obligations. You agree that you will not use the Software other than as permitted by this agreement and that you will not use the Software in a manner inconsistent with its design or Documentation.

6.3. No Modifications. You shall not modify, adapt, tamper with, translate or create derivative works in any form whatsoever of the Software or the Documentation contained therein; combine or merge any part of the

Software or Documentation with or into any other software or documentation; or refer to or otherwise use the Software as part of any effort to develop software (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; except with Stellar's prior written permission, publish any performance or benchmark tests or analysis relating to the Software.

6.4. No Reverse Engineering. You shall not reverse engineer, decompile, disassemble, or otherwise attempt to discover the source code of the Software.

6.5. No Unbundling. The Software may include various applications and components, may allow access to different Stellar Online Channels, may support multiple platforms and languages, and may be provided to you on multiple media or in multiple copies. Nonetheless, the Software is designed and provided to you as a single product to be used as a single product on Computers as permitted herein. Unless otherwise permitted in the Documentation, you are not required to install all component parts of the Software, but you shall not unbundle the component parts of the Software for use on different Computers.

6.6. You will not remove, erase, obscure or tamper with any copyright or any other product identification or proprietary rights notices, seal or instructional label printed or stamped

on, affixed to, or encoded or recorded in or on any Software or Documentation; or fail to preserve all copyright and other proprietary notices in all copies Company makes of the Software and Documentation.

6.7. You will not run or operate the Software in a cloud, Internet-based computing or similar on-demand computing environment unless the software specifications permit such use.

6.8. No Transfer. You will not rent, lease, sell, sub-license, assign, or transfer its rights in the software (including without limitation, software obtained through a web download), or authorize any portion of the software to be copied onto another individual or legal entity's computer except as may be expressly permitted herein.

7. WARRANTIES

The licensed software (excluding the media on which it is distributed) and all Stellar related websites and services are provided to licensee 'AS IS' and "AS AVAILABLE," and Stellar and its suppliers and licensors make NO WARRANTY as to their use or performance. Stellar and its suppliers and licensors make NO WARRANTIES OR REPRESENTATIONS (express or implied, whether by statute, common law, custom, usage, or otherwise) as to any matter including without limitation to quality, availability, performance or functionality of the licensed software or any related Stellar websites or services; quality or accuracy of any information obtained from or available through use of the licensed software or related Stellar websites or services; any representation or warranty that the use of the licensed software or any related Stellar websites or services will be uninterrupted or always available (whether due to internet failure or otherwise), error-free, free of viruses or other harmful components or operate on or with any particular hardware, platform or software; merchantability, integration, satisfactory quality, or fitness for any particular purpose, except for, and only to the extent, that a warranty may not be excluded or limited by applicable law in licensee's jurisdiction.

8. INDEMNIFICATION

Subject to the Customer using the Software in the manner prescribed, Stellar warrants that its software does not infringe the intellectual property rights of the third parties. Stellar may at its option will defend or indemnify and hold you harmless against any claims arising out of and resulting from Stellar's infringement of third-party intellectual property rights. You will give Stellar notice of any claims within 3 business days of the receipt of the same, provided that any failure to notify within the time stated, shall relieve Stellar to the extent prejudiced.

You may participate in the defense of any claim with counsel of its own choosing at your own expense. You will not settle any claim without Stellar's written consent, which shall not be unreasonably withheld. You will not make any statement contradictory to the interests of Stellar in connection with such claim.

9. LIMITATIONS & LIABILITY

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

Notwithstanding anything contained in this agreement, the maximum liability of Stellar is limited to the amount actually paid by you in the preceding 12 months.

10. DATA PROTECTION

You understand that by using the Licensed Software, you accord, consent and agree to the collection and use of certain information about you and your use of the Licensed Software in accordance with Stellar's Privacy Policy, which is available at https://www.bitraser.com/privacy-policy.php. You further consent and agree that Stellar may collect, use, transmit, process and maintain information related to your Account, and any devices or computers registered thereunder, for purposes of providing the Licensed Software, and any features therein, to you. Information collected by Stellar when you use the Licensed Software may also include technical or diagnostic information related to your use that may be used by Stellar to support, improve and enhance Stellar's products and services. You further understand and agree that this information may be transferred to the United States, India and/or other countries for storage, processing and use by Stellar, its affiliates, and/or their service providers. You hereby agree and consent to Stellar's and its partners' and licensors' collection, use, transmission, processing and maintenance of such location and account data to provide and improve such features or services in accordance with Stellar Privacy policy.

11. DATA PRIVACY

11.1 Internet Connection: The Software may cause your computer, without notice, to automatically connect to the Internet and to communicate with Stellar website or Stellar domain for purposes such as license validation and providing you with additional information, features, or functionality. Unless otherwise specified in Sections 11.2 through 11.5, the following provisions apply to all automatic Internet connections by the Software:

11.1.1 Whenever the Software makes an Internet connection and communicates with a Stellar website, whether automatically or due to explicit user request, the Privacy Policy shall apply. Stellar Privacy Policy allows tracking of website visits and it

addresses in detail the topic of tracking and use of cookies, web beacons, and similar devices.

11.1.2 Whenever the Software connects to Stellar website or Stellar owned domains over the Internet, certain Customer information is collected and transmitted by the Software to Stellar pursuant to the Stellar Privacy Policy. If Customer accesses Stellar Online Service or activates or registers the Software, then additional information such as Customer's ID, user name, and password may be transmitted to and

stored by Stellar pursuant to the Privacy Policy.

11.1.3 Stellar, unless barred under applicable law, may (a) send Customer transactional messages to facilitate the Stellar Online Service or the activation or registration of the Software or Stellar Online Service, or (b) deliver in-product marketing to provide information about the Software and other Stellar products and Services using information including but not limited to platform version, version of the Software, license status, and language.

11.2 Updating. The Software may cause Customer's Computer, without additional notice, to automatically connect to the Internet (intermittently or on a regular basis) to (a) check for Updates that are available for download to and installation on the computer and (b) notify Stellar of the results of installation attempts.

11.3 Activation. The Software may require Customer to (a) obtain Stellar Software Activation Key, (b) activate or reactivate the Software, (c) register the software, or (d) validate the . Such requirement may cause Customer's Computer to connect to the Internet without notice on install, on launch, and on a regular basis thereafter. Once connected, the Software will collect and transmit information to Stellar. Software or Customer may also receive information from Stellar related to Customer's license or subscription. Stellar may use such information to detect or prevent fraudulent or unauthorized use not in accordance with a valid license or subscription. Failure to activate or register the Software, validate the subscription or license, or a determination by Stellar of fraudulent or unauthorized use of the Software may result in reduced functionality, inoperability of the Software, or a termination or suspension of the subscription or license.

11.4 Use of Online Services. The Software may cause Customer's Computer, without additional notice and on an intermittent or regular basis, to automatically connect to the Internet to facilitate Customer's access to content and services that are provided by Stellar or third parties. In addition, the Software may, without additional notice, automatically connect to the Internet to update downloadable materials from these online services so as to provide immediate availability of these services even when Customer is ofline.

11.5 Digital Certificates. The Software uses digital certificates to help Customer identify downloaded files (e.g., applications and/or content) and the publishers of those files. For example, Stellar uses digital certificates to help Customer identify the publisher of Stellar applications. Customer's Computer may connect to the Internet at the time of validation of a digital certificate.

12. TERMINATION

If you breach this EULA, and fails to cure any breach within 30 calendar days after request from Stellar, Stellar may terminate this EULA, whereupon all rights granted to you shall immediately cease including but not limited to the license granted to you to use the software, which shall also stand revoked. Furthermore, upon termination, you shall return to Stellar all copies of the Licensed Software or verify in writing that all copies of the Licensed Software have been destroyed and failure of the customer to do so would entitle Stellar to sue for relief in equity and damages.

13. JURISDICTION AND LAW

13.1. This EULA is subject to and will be governed by and construed in accordance with the substantive laws applicable to the state of Delhi (India). Courts at Delhi (India) alone shall have the jurisdiction to entertain any dispute arising out of the terms and conditions of this EULA or the use of the Software or license and Customer consent to urisdiction of the courts at Delhi, India.

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

14. GENERAL

14.1. This License is the complete statement of the agreement between the parties on the subject matter and merges and supersedes all other or prior understandings, purchase orders, agreements and arrangements.

14.2. The exclusions of warranties and liability limitations shall survive the termination of this EULA, howsoever caused; but this survival shall not imply or create any continued right to use the Licensed Software after termination of this EULA.

14.3. Licensee shall not ship, transfer, or export Licensed Software into any country or use Licensed Software in any manner prohibited by the applicable export control laws, notably where applicable, the United States Export Administration Act, restrictions, or regulations (collectively the 'Export Laws'.) All rights to use the Licensed Software are granted on condition that Licensee complies with the Export Laws, and all such rights are forfeited if Licensee fails to comply with the Export Laws.

14.4. Stellar reserves all rights not expressly granted to the Licensee by this EULA All rights are reserved and protected under the copyright laws of India and/or of other countries, to Stellar Information Technology Pvt Ltd, having its registered office at 205, Skipper Corner, 88, Nehru Place, New Delhi, India 110019.

14.5. There are no third-party beneficiaries of any promises, obligations or representations made by Stellar herein.

14.6. Any waiver by Stellar of any violation of this License by Customer shall not constitute nor contribute to a waiver by Stellar of any other or future violation of the same provision or any other provision of this License.

14.7. This EULA constitutes the entire agreement between Customer and Stellar and it supersedes all prior or contemporaneous representations, discussions, undertakings, communications, agreements, arrangements, advertisements, and understandings regulating the Licensed Software. This EULA is binding on and made for the benefit of the parties and their successors and permitted assigns.

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

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

6. ABOUT STELLAR

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

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

For more information about us, please visit www.stellarinfo.com.