Blancco Drive Eraser version 6.2.0 has been released!

Drive Eraser 6.2.0 - Release Notes

Features:

- Erasure resume
  - Blancco Drive Eraser is able to resume an erasure that has been interrupted (due to a power loss, a human error, a system crash, etc.). Resuming an erasure from where it was left before the interruption will save time whenever erasing large servers with multiple drives.
  - For standards doing normal overwriting only. The erasure is resumed from the beginning of the step that was interrupted. The final verification will always be a full verification (100%) to catch any potential issue. No extra license is consumed.
  - Feature can be enabled with Blancco Drive Eraser Configuration Tool 2.2.0.
- eMMC purge
  - eMMC are light data storage devices that have become popular on netbooks and tablets. In addition to clearing them, Blancco Drive Eraser is capable of purging them. A purge-level erasure meets higher security requirements.
  - Requires using the erasure standards "NIST 800-88 Purge" or "Blancco SSD Erasure".
  - More information on the eMMC purge is available in the Blancco Drive Eraser user manual.
- Fill in custom fields remotely
  - This feature adds the ability for custom fields to be filled on a machine (running Blancco Drive Eraser) that is being remotely erased (from the Blancco Management Console user interface).
  - Custom fields and remote control can be configured via Blancco Drive Eraser Configuration Tool.
  - Requires Blancco Management Console 4.2.0 or higher.
- Input validation for custom fields
  - This feature adds the ability to set rules (regular expressions) on the value a custom field should have. It is now possible to define custom fields that should only have e.g. numbers only, letters only or any particular combination of both.
  - Requires Blancco Drive Eraser Configuration Tool 2.2.0.
- Threshold on write error count
  - This feature allows setting a configurable threshold on the write errors that may occur during the erasure. Once the threshold is reached, the erasure fails with a clear message.
  - Requires Blancco Drive Eraser Configuration Tool 2.2.0.
- Identify a headless machine remotely
  - Headless machines are usually rack servers without any screen or display. This feature adds the ability for a headless machine (running Blancco Drive Eraser) to be remotely identified (from the Blancco Management Console user interface).
  - Blancco Management Console sends an identification command to Blancco Drive Eraser; upon receiving it, BDE blinks all the drives connected to the machine.
  - Requires Blancco Management Console 3.7.0 or higher.
- Quick verification steps after every overwrite pass
  - When using an erasure standard with multiple overwriting passes, a quick verification will check that each overwrite wrote what it was meant to write. If unexpected patterns are found, the erasure will fail.
  - This quick verification is non-configurable and represents a tiny fraction of the drive capacity.
  - The erasure duration will not be affected (from a few seconds to a few minutes depending on the size of the drive and the read speed).
- NIST verification algorithm
  - All Blancco Drive Eraser verifications follow an algorithm similar to the one defined by NIST.
  - For instance, using a DoD 3-passes erasure with 10% verification will be compliant with NIST “clear”.
- CD boot on UEFI machines
  - Burn a CD and boot on any UEFI machine without problems.
  - CD booting worked before but the booted image used to lose all pre-configuration.
- Configure default report format
  - If you save reports locally, define what is the report format that should be used by default (PDF, XML or both).
  - Requires Blancco Drive Eraser Configuration Tool 2.2.0.
- Configure customized booting
  - Create a custom booting for Blancco Drive Eraser to match your erasure needs. Useful when erasing hardware requiring special booting parameters (Apple machines, some machines with NVMe drives, etc.).
  - Requires Blancco Drive Eraser Configuration Tool 2.2.0.
  - Requires Blancco USB Creator 3.1.0 or higher and/or Blancco Preinstall 2.4.0 or higher.

Bug fixes/Improvements:

- Better detection of erasure problems (example machine: Lenovo Thinkcentre M32 machines with JMicron "605 SSD" drives). Failing overwriting rounds are now detected via the quick verification steps executed after every overwriting.
- Fix for several overwriting issues on Apple machines with NVMe drives (example models: MacBookAir7,1 , MacBook8,1 , MacBook9,1). This was a known issue that resided in the kernel driver. Fixed by upgrading the kernel.
- Fix for a drive detection issue on MacBookPro11,3 ("A1398") machines. Erasure is also successful.
- Fix for some problems with the network connectivity (DNS settings were not retrieved from the DHCP server, captive portal detection was enabled).
- Fix for a problem on the "BSI-GS/E" erasure standards where the erasure did not necessarily fail in case hidden areas were not erased. This achieves a better compliance with the BSI standards.
- Fix for an erasure problem on Dell XPS 13 with a Samsung NVMe PM951. Drive is successfully erased with "Blancco SSD Erasure" or "NIST 800-88 Purge" as long as the booting parameter "flr=forced" is used.
- Fix for a booting problem where the freeze lock removal procedure was sometimes triggered when not required. This is a general booting improvement. In case the freeze lock removal is really needed, use the booting parameter "flr=forced".
- Fix for a problem where some hardware features (e.g. BIOS) failed to be detected and reported properly. This problem occurred with 6.1.x releases only.
- Fix for an erasure problem where an optional step (Cryptographic Erasure) was considered mandatory and failed the whole erasure. This occurred on NVMe drives supporting Cryptographic Erasure as well as Format NVMe and erased with "Blancco SSD Erasure".
- Fix for a problem where the user interface was not loaded properly on the "Report per drive" mode. This occurred if there were "per drive" custom fields defined.

- Fix for several issues occurring with CD-booting on UEFI machines (the pre-configuration was always lost). The CD-boot improvements on UEFI machines have fixed these issues.
- Fix for some localization issues in the user interface (strings remained in English).
- Improved identification of the default booting option. Any booting option pre-configured to be the default one is followed with a " [DEFAULT]" label.
    - Requires Blancco Drive Eraser Configuration Tool 2.2.0.
    - Requires Blancco USB Creator 3.1.0 or higher and/or Blancco Preinstall 2.4.0 or higher.
- Fix for a problem where the presence of an old file (RUNNING_PID) prevented the DECT from starting. Problem existed in Windows O.S. only.
    - Available in Blancco Drive Eraser Configuration Tool 2.2.0.
- Fix for a problem where the configuration of the CD tray ejection was lost. Problem existed since version DECT1.8.0.
    - Available in Blancco Drive Eraser Configuration Tool 2.2.0.
- Fix for a problem where temporary ISO files were left in the system. Problem existed in Windows O.S. only.
    - Available in Blancco Drive Eraser Configuration Tool 2.2.0.
- Fix for a problem where the DECT service name was still "Blancco 5 Configuration Tool". Replaced with "Blancco Drive Eraser Configuration Tool". Problem existed in Windows O.S. only.
    - Available in Blancco Drive Eraser Configuration Tool 2.2.0.
- Fix for a problem where enabling the memory test in DECT did not enable it in Drive Eraser.
    - Available in Blancco Drive Eraser Configuration Tool 2.2.0.

Things to know:

- The erasure resume has been designed to work mainly on physical drives that are identified via a serial number and are erased as a whole. The erasure resume will not necessarily work on drives that are not physical (e.g. logical drives) or drives that are partially erased (e.g. drives where only some specific partitions are erased). For the time being, it is advised not to activate partition erasure or recovery partition preservation from the UI if the erasure resume is enabled. The erasure resume will include more cases in the next releases.
- USB stick must be plugged in during the erasure.
    - File with the erasure information is saved to the USB device and that file is used to resume the erasure. Generally, a few KB of free space is required per erased disk.
- When an erasure is resumed:
    - The erasure progress shown in the user interface starts from 0%, although in reality the erasure is being restarted from where it was interrupted.
    - The estimated erasure duration may look too high and the erasure speed may look too low. These values become correct after a while. This can be confusing at first sight. This will be fixed in the next releases.
- When an erasure is resumed:
    - Only the erasure standards doing normal overwriting are resumed.
    - Those standards doing more complex operations (e.g. "Blancco SSD Erasure", "NIST 800-88 Clear", "NIST 800-88 Purge", "BSI-GS", "BSI-GSE") are not automatically resumed and should be restarted manually. This can be confusing at first sight. This will be fixed in the next releases.
- When an erasure is resumed:
    - Only the drives that have a valid serial number are resumed.
    - Drives that do not have any serial number are not automatically resumed and should be restarted manually. Drives where the erasure is resumed need to be identified in a unique manner to prevent resuming the wrong drive. The drive unique identification will be improved in the next releases.
- When an erasure is resumed:
    - It is resumed from the beginning of the step that was interrupted.
    - The verification percentage used in the last verification is always 100% to catch any potential problem that may have occurred during the resume process. Therefore, the duration of a resumed erasure may be longer than expected. The erasure will be restarted from the last known position in the next releases. The high percentage of the final verification is not a bug, it is there by design.

Known issues:

- Some SSDs and NVMes available on Apple machines do not implement any firmware-based erasure command. Therefore, these data storage devices cannot be purged but only cleared via normal overwriting methods.
    - The known models were this happens:
        - MacBook9,1 , MacBook8,1 , MacBookAir7,1 (all with NVMe drives)
        - MacBookPro11,1 (with OWC Aura SSD)
    - This appears to be an Apple customization. Since the commands are simply missing, there is nothing Blancco can do about it.
- On rare occasions, saving a report (normal report or issue report) on a USB stick can take longer than expected (up to several minutes). We suspect this problem is connected to the USB stick were the report is saved, feel free to replace the USB stick if you witness this problem. The report saving works in the end, so this is more of an annoyance.
- Some ATA SSDs that implement the Sanitize Crypto Erase command fail the erasure when handled with "Blancco SSD Erasure" if the verification percentage is below 100%.
    - This is a known issue that is going to be fixed in the 6.2.1 release coming before the end of October 2017.
    - There is a workaround: setting a verification percentage of 100% will prevent this from happening.
- Some ATA SSDs that implement the Secure Erase command fail the erasure when handled with "NIST 800-88 Clear" if the verification percentage is between 11% and 99%.
    - This is a known issue that is going to be fixed in the 6.2.1 release coming before the end of October 2017.
    - There is a workaround: setting either a verification percentage of 10% (or less) or equal to 100% will prevent this from happening.