Erasure failing for SSD/NVMe drives due to erasure commands failing or not being supported

Created date	Updated date	Affects version	Fix version
15 Sep 2021	15 Sep 2021	Drive Eraser - All version	N/A

Problem

Erasure of SSD and NVMe drives fails due to certain firmware based erasure commands failing or not being supported.

For example you can see one of the below mentioned failures being mentioned in the erasure report:

Exception message
ENHANCED SECURE ERASE command failed
SECURE ERASE command failed
FORMAT UNIT command failed
BLOCK ERASE EXT command failed
OVERWRITE EXT command failed
Cryptographic erasure has failed

Cause

Certain erasure standards (and erasure settings) incorporate firmware based erasure rounds which are mandatory in order to successfully complete the erasure. In some cases the drive may not support these required firmware commands (due to lack of the implementation on drive's firmware) or the drive might be in a locked state which prevents using these type of commands.

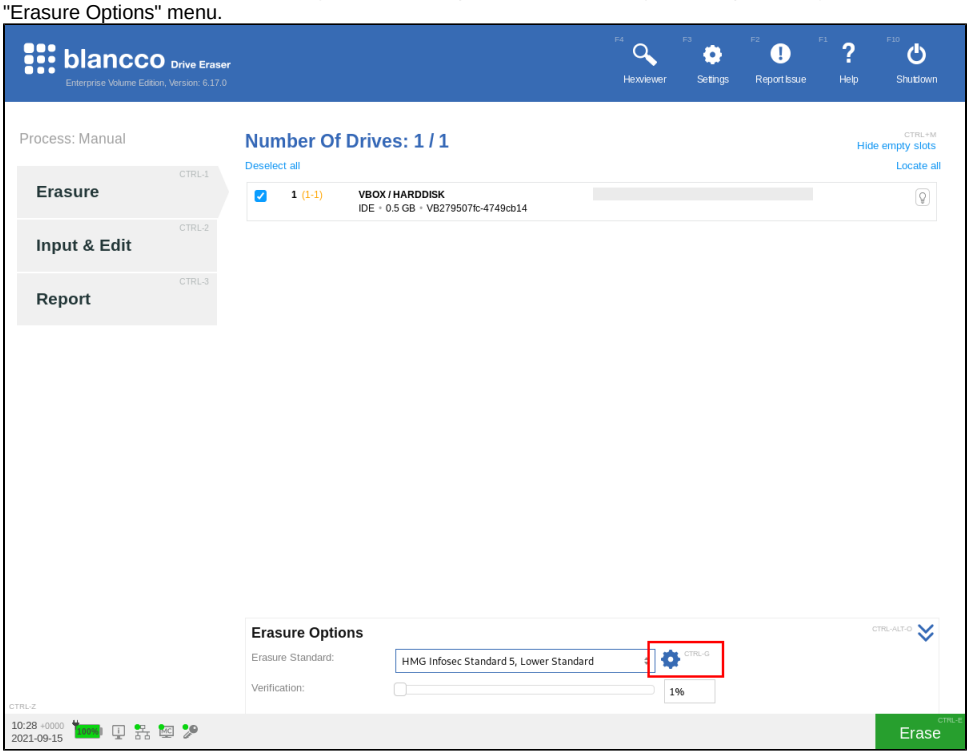
The commands used are dependent on the details of the target drive, selected erasure settings and erasure standard.

Resolution

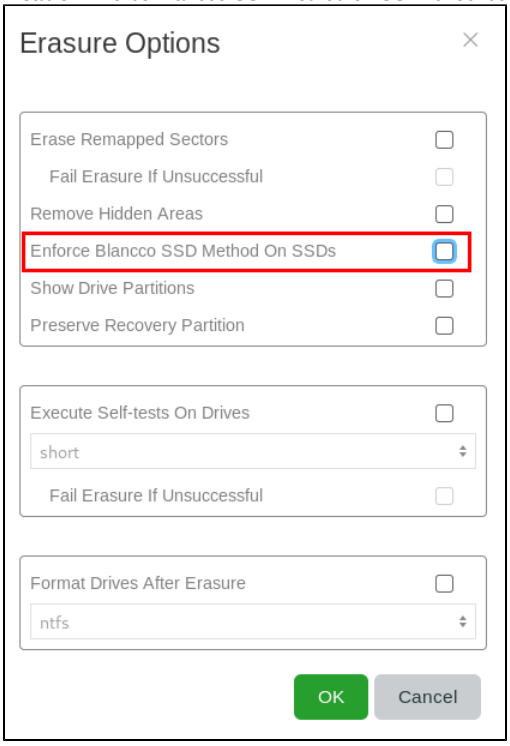
As a workaround, such drives can be erased using erasure settings which do not include firmware based erasure rounds during the process. Note that this type of erasure process will provide a clear level erasure results which protects against non-invasive data recovery methods.

To do this follow below steps:

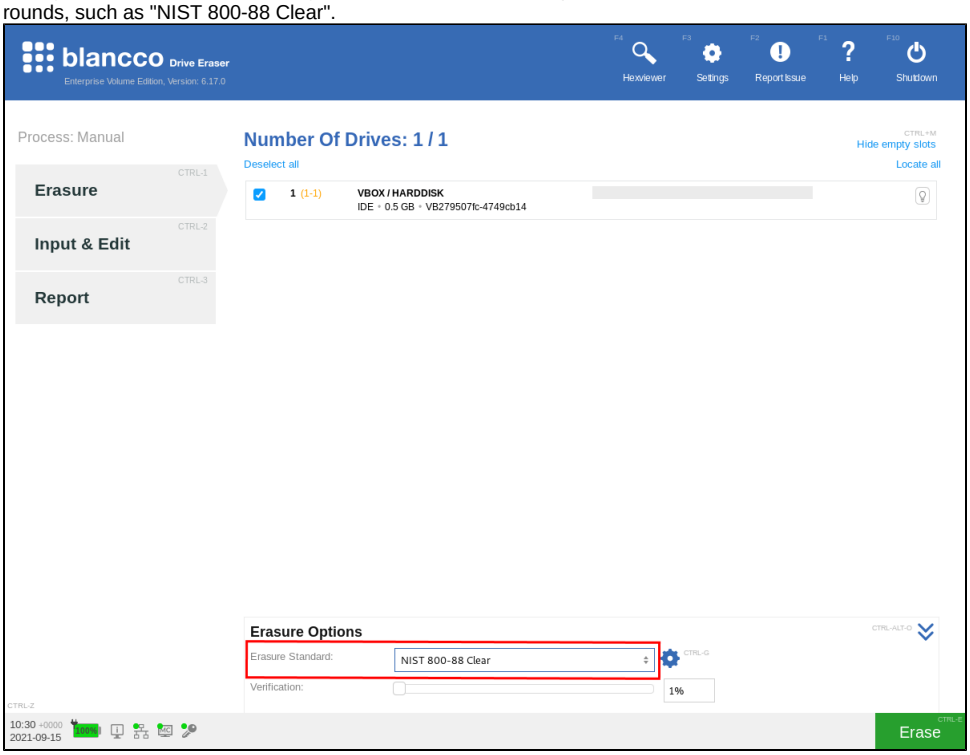
1. On Drive Eraser user interface navigate "Erasure Options" and click the gear-icon (or use keyboard combination CTRL+G) to open additional "Erasure Options" menu.



2. Disable “Enforce Blancco SSD method on SSD” checkbox and click on “OK” to save the settings.



3. Change the erasure standard using the "Erasure Standard" dropdown menu. Select a standard which does not include firmware based erasure rounds, such as "NIST 800-88 Clear".



4. Run the erasure.