

How Does the "Resume erasure if interrupted" option work in Drive Eraser

Created date	Updated date	Affects version	Fix version
01 Sep 2023	01 Sep 2023	Drive Eraser 6.2.2 (and newer)	N/A

Problem

If you checked the 'Resume eraser if interrupted' option in the Drive Eraser Configuration Tool for a Drive Eraser ISO, and if you are using an erasure standard that has two or more overwriting passes, the erasure will continue automatically even after the event of power loss and/or system failure before the erasure completes. When enabled no extra licenses will be consumed after the resumed erasure after the failure.

Note that this option works only with the magnetic standard having two and more than two overwriting passes.

In the event of power loss and/or system failure, Drive Eraser will get the interrupted session's information from that USB and continue the erasure. The erasure is resumed at the beginning of the execution step where the interruption took place. For example, if an erasure was started with the 'HMG Infosec Standard 5, Higher Standard' (3 overwriting rounds) selected and the erasure was interrupted at say 70% through overwriting pass 3 (Overwrite with random byte), then the erasure will resume at the beginning of the pass 3. The erasure is resumed at the beginning of the execution step where the interruption took place.

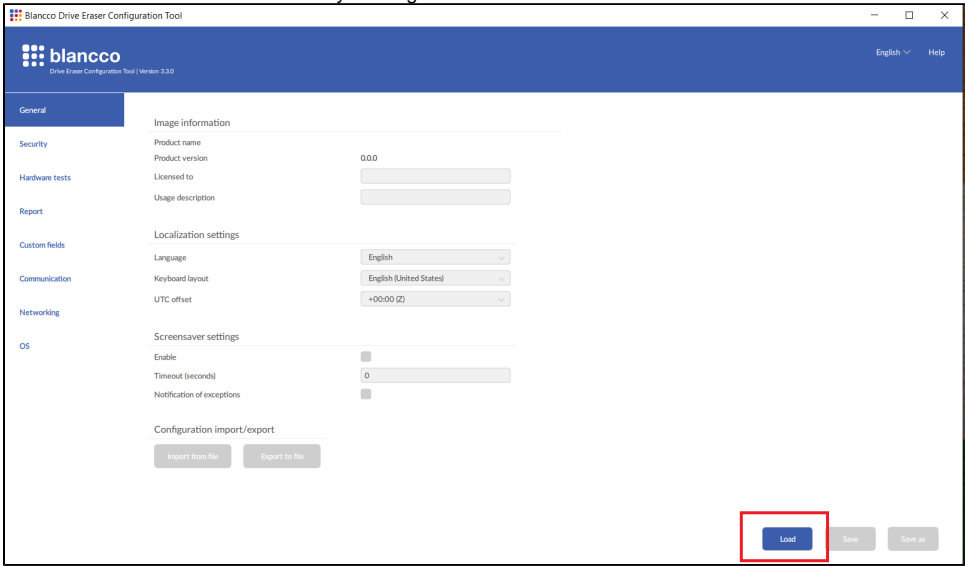
Requirements

1. The feature must be activated via the Drive Eraser Configuration Tool.
2. A USB flash drive, which is not full, must be plugged in during the erasure. A tar file with the erasure information is saved to the USB device and that file is used to resume the erasure after the event of erasure failure.

How to enable "Resume erasure if interrupted" option

Follow the below steps to enable the 'Resume erasure if interrupted' option in Blancco Drive Eraser.

1. Load the desired BDE ISO in DECT by clicking on the Load button in the DECT.



2. Go to the 'Security' Tab and 'in the 'Security options' section.

Blancco Drive Eraser Configuration Tool

blancco
Drive Eraser Configuration Tool | Version 3.3.0

General

Security

Hardware tests

Report

Custom fields

Communication

Networking

OS

Connected devices

Report per connected device ☐

Hotplug ☐ Timeout (seconds) 30

Chromebook support ☐ Port 80

Security options

Erase standard HMG Infosec Standard 5, Lower Sta...

Enforce Blancco SSD method on SSDs ☐

Enable fallback from NIST Purge to NIST Clear ☐

Fail erasure if write errors ☒ Fail threshold 5

Fail erasure if read errors ☒ Fail threshold 5

Remove hidden areas ☐

Erase remapped sectors ☐

Fail erasure if the number is too high ☐ Fail threshold 0

Fail erasure if unsuccessful ☐

Fail erasure if the speed is too low (MB/s) ☐ Fail threshold 0

Execute self-tests on drives None

Fail erasure if unsuccessful ☐

Erase verification level 1

3. Check the 'Resume erasure if interrupted' option.

Blancco Drive Eraser Configuration Tool

blancco
Drive Eraser Configuration Tool | Version 3.3.0

General

Security

Hardware tests

Report

Custom fields

Communication

Networking

OS

Chromebook support ☐ Port 80

Security options

Erase standard HMG Infosec Standard 5, Lower Sta...

Enforce Blancco SSD method on SSDs ☐

Enable fallback from NIST Purge to NIST Clear ☐

Fail erasure if write errors ☒ Fail threshold 5

Fail erasure if read errors ☒ Fail threshold 5

Remove hidden areas ☐

Erase remapped sectors ☐

Fail erasure if the number is too high ☐ Fail threshold 0

Fail erasure if unsuccessful ☐

Fail erasure if the speed is too low (MB/s) ☐ Fail threshold 0

Execute self-tests on drives None

Fail erasure if unsuccessful ☐

Erase verification level 1

Logical disk (RAID) Show

Preserve recovery partition ☐

Resume erasure if interrupted ☒

Lock the erasure settings ☐

4. Now if you click on the Save button, it will save those latest changes in that ISO directly. If you click on Save as a button, then the DECT tool will allow you to create a new configured ISO with the latest changes and you can name that ISO file as per your wish.

Blancco Drive Eraser Configuration Tool

English Help

General

Security

Hardware tests

Report

Custom fields

Communication

Networking

OS

Device enrollment detection

Persistent software

Format settings

Format drive after erasure

File system type

Power saving settings

Spin down idle disks

Erase remapped sectors

Fail erasure if the number is too high

Fail erasure if unsuccessful

Fail erasure if the speed is too low (MB/s)

Execute self-tests on drives

Fail erasure if unsuccessful

Erasure verification level

Logical disk (RAID)

Preserve recovery partition

Resume erasure if interrupted

Lock the erasure settings

Fail threshold 0

Fail threshold 0

None

1

Show

NTFS

Load Save Save as