Handling encrypted drives

Created date	Updated date	Affects version	Fix version
29 Jun 2018	08 Oct 2021	Drive Eraser - All versions	N/A

A drive (HDD, SSD, NVMe…) can be encrypted in multiple different ways:

Encryption via software

The machine's OS (e.g. Windows via BitLocker) encrypts the content of the drive, but otherwise the drive does not have any encryption itself.

Blancco Drive Eraser can erase these drives without a problem since it overrides the machine's original OS.

Encryption via hardware

The drive encrypts itself and does not require the machine's OS or any other utility. The drive has an encryption mechanism that does not depend on the machine's OS, such drive usually supports the Sanitize Crypto Erase command which—if executed—changes the encryption key of the drive rendering its content nonsensical and any existing data unrecoverable. These drives are also known as self-encrypting drives or SED.

As per version 6.18.0, Blancco Drive Eraser can erase these drives (ATA, SCSI/SAS, NVMe) without problems, either via traditional overwriting or via executing the Sanitize Crypto Erase command (used in standards such as "NIST 800-88 Purge", "Blancco SSD Erasure", "Sanitize Cryptographic Erasure").

Encryption via a combination of software and hardware

The drive supports a special locking/encrypting security feature that needs to be enabled via a utility provided by the drive manufacturer. The most popular security features are developed by the Trusted Computer Group or TCG (e.g. the OPAL security feature), such features lock/encrypt a drive to prevent any unauthorized person from accessing the data. It can be enabled either by the computer manufacturer or by the computer owner. These drives are also considered self-encrypting drives or SED.

As per version 6.18.0, Blancco Drive Eraser can erase these drives (ATA, SCSI/SAS, NVMe) without problems, either via traditional overwriting or via executing the TCG Crypto Erase command (used in standards such as "NIST 800-88 Purge", "Blancco SSD Erasure", "TCG Cryptographic Erasure"). In case the TCG feature set has been used to lock the drive, the drive can still be unlocked and erased via a procedure called "PSID Revert" (more information about this in this article).