# NVME SSD's: NVME Secure Erase

ATA and NVME drives use different communication specs, and as such the secure erase/sanitize commands are different. Sanitize overwites all data

## Linux:

Best, Sanitize. Source: NVME Sanitize on tinyapps.org

1. Install `nvme-cli`
2. list NVME drives with `nvme list`
3. Check device is supported with `nvme id-ctrl -H /dev/nvmeX`. Check the 'fna' section, if any features have a '0x1'instead of a '0', sanitize is supported. Otherwise use Secure Erase.
4. Run the command `nvme sanitize -a Y /dev/nvmeX` where `Y` is 1, 2, 3, or 4 depending on supported sanitize features:
   a) 1 = exit failure mode
   b) 2 = Block Erase (Does a hi-low pulse on all blocks to reset them all to 0)
   c) 3 = Overwrite (random data overwrite)
   d) 4 = Crypto Erase (delete/change crypto keys, only on encrypted drives)
5. Check Status with `nvme sanitize-log /dev/nvmeX`. Completed when SPROG=65535, and SSTAT=0x101

Alternate, Secure Erase. Source: NVME Secure Erase on tinyapps.org

1. Install `nvme-cli`
2. list NVME drives with `nvme list`
3. Check device is supported with `nvme id-ctrl -H /dev/nvmeX`. if 'oacs' section, option [1:1] is set, Secure erase is supported. If 'fna' section, option [2:2] is set, then cryptographic secure erase is supported as well.
4. trigger the secure erase with `nvme format /dev/nvmeX --ses=Y` where `Y` is 0, 1, or 2, depending on supported features:
   a) 0 = no secure erase
   b) 1 = User Data Erase (random data overwrite)
   c) 2 - Cryptographic Erase (delete/change crypto keys, only on encrypted drives)

## Windows:

See the Windows section under the SATA page, method is the same.

Revision #1
Created 14 January 2023 23:51:49 by Dev
Updated 15 January 2023 00:31:46 by Dev