HP Secure Erase for SSDs & HDDs

Safely and effectively erase sensitive data from solid state and hard drives

HP Secure Erase[1] is a critical resource for IT administrators tasked with protecting sensitive data, and a key component of HP system security. HP Secure Erase makes it easy to sanitize local magnetic hard disk drives (HDD) or solid-state drives (SSDs) to industry standards before disposal or recycling.

Local storage sanitation—an important last step in the PC lifecycle

In an environment where sensitive user information is under attack at every stage of the system lifecycle, ensuring that data can be securely erased from a data storage device is paramount. Information can be vulnerable if left on a storage drive when a system is recycled, disposed of, or re-provisioned for another user. Properly sanitizing storage drives according to industry standards is a critical step in the PC lifecycle.

In addition to meeting industry standards for data erasure in standard magnetic hard disk drives (HDDs), HP has taken the additional step of extending HP Secure Erase to also support industry-standard solid state drives (SSDs). HP Sure Erase is a standard feature in all HP business notebooks, supporting the methods outlined in the National Institute of Standards and Technology Special Publication 800-88. Manufacturers of industry-standard SSDs approved for use in HP business notebook products have verified that running HP Secure Erase on their SSDs fully removes all user data so that it cannot be recovered.

Erasing SSDs vs. HDDs

Using HP Secure Erase on standard HDDs, data is overwritten using a data-removal algorithm that writes multiple patterns on every sector, cluster, and bit of the hard drive. This process is documented in the Department of Defense (DOD) 5220.22-M Chapter 8 specification.[2] This overwrite-based process is only effective on standard HDDs. Writing a predetermined data pattern to a NAND flash-based SSD does not result in an empty drive. Instead it results in a drive full of data that must be erased before new user data can be written, which massively shortens the service life.

Industry-standard disk sanitation

To securely erase all user data from an SSD and restore the drive to a fresh-out-of-box (FOB) performance state, the National Institute of Standards Technology (NIST) supports the following commands that meets the minimum guideline for media sanitization of SSDs (NIST SP800- 88 Rev. 1).

Block Erase is a function enabled only in SATA SSDs. Using the ATA command BLOCK ERASE EXT. Block Erase will instruct the SSDs controller to apply an erase voltage to all NAND cells of the device (including any cells which form blocks that have been retired, re-allocated, involved in garbage collection or over-provisioning or are part of a reserved pool of spare blocks). This functionality provides a very fast, complete and robust erasure of the SSD.

Crypto Erase is a function enabled only in SATA SED SSDs. Using the ATA command CRYPTO SCRAMBLE EXT, this function removes the encryption key effectively making it impossible to reconstruct any of the data on the storage device. Crypto Scramble is implemented on both HDD and SSD SED devices.

---

[1] For the methods outlined in the National Institute of Standards and Technology Special Publication 800-88 "Clear" sanitation method. Secure Erase does not support platforms with Intel® Optane™. HP Secure Erase does not support platforms with Intel® Optane.

[2] Specification 5220.22-M no longer exists. The DoD has subsequently decided that secure information must be destroyed to remain secure. The NIST guidelines restate in clear terms that a two-person rule (read human verification) shall be implemented but did not establish guidelines on the method of sanitization (it could be a single wipe with dual human verification, or a single destruction with the same).

4AA7-2608ENW, March 2019

Block Erase and Crypto Erase Sanitize Operation is a function enabled only in PCIe NVMe SSDs. NVMe does not follow conventional ATA feature sets. Instead, NVMe devices support a sanitization function, inside their FORMAT NVM command structure that includes BLOCK ERASE SANITIZE and CRYPTO ERASE SANITIZE operation. So, by setting some specific bits in this command structure, a function similar to Secure Erase can be carried out.

What data is not erased?

After deploying HP Secure Erase on an SSD, all data in the user space is completely and irretrievably erased, and every block in the user space is ready to accept new host-written data, which moves the drive to its highest performance state (FOB). However, some data must be left in place, including data required for normal drive operation: SSD firmware copies that reside in the NAND, all SMART data, and retired NAND block mapping tables.

Conclusion

Writing or overwriting data to drive is the accepted practice of securely eliminating data from an HDD. However, in the case of NAND flash-based SSDs, overwriting is redundant, unnecessary, and a potentially insecure method of eliminating data. By using HP Secure Erase, users can ensure that SSD drives are completely sanitized and meet the minimum industry standards HP Secure Erase is easily enabled through the standard F10 BIOS setup process on most HP business PCs.

Learn more

hp.com/go/computersecurity

4AA7-2608ENW, March 2019