HP Secure Erase for SSDs & HDDs

Safely and effectively erase sensitive data

HP Secure Erase is a critical resource for IT

IT administrators are tasked with protecting sensitive data on business PCs, even after devices are recycled, disposed of, or reprovisioned. HP Secure Erase[1] makes it easy to sanitize local magnetic hard disk drives (HDDs) or solid-state drives (SSDs) to industry standards before disposal or recycling.

Table of Contents

Local storage sanitization – 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 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 reprovisioned for another user. Properly sanitizing storage devices, while being compliant with 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 Secure Erase is a built in standard feature in HP business-class PC's supporting the methods outlined in the National Institute of Standards and Technology Special Publication 800-88 Rev. 1[4]. Manufacturers of industry standard SSDs approved for use in HP business-class PC 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 each 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 a fully erased 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 product life.

INDUSTRY-STANDARD DISK SANITIZATION

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 meet the minimum guideline for media sanitization of SSDs (NIST SP800- 88R1).

- BLOCK ERASE
  Is a function enabled only in SATA SEDs, using the ATA command BLOCK ERASE EXT. Block Erase will instruct the SSD 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 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.

- 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'S NEW?

HP Secure Erase can be found on HP business-class PC's, but the ability to support NIST 800-88R1 erasure types can vary by the drive manufacturer or drive-type in the PC. In the Fall of 2024, HP updated the BIOS on HP business-class PC's to include multiple new HP Secure Erase capabilities. The improved features can be acquired simply, by updating to the latest HP BIOS[3].

SUMMARY OF HP SECURE ERASE UPDATES

1. Improved User Interface within the HP BIOS – HP Secure Erase provides additional data about the drive type in the system. This includes the drive type (HDD or SSD), manufacturer, capacity, serial number and more, compliant with NIST 800-88R1 guidelines.

2. By adding improved detection of drive types, HP Secure Erase will now present to the Administrator or User the most Secure method of drive sanitization. (E.g., Level 1-Clear or Level 2-Purge). HP Secure Erase will default to the highest level or, most secure method of sanitization.

3. At the conclusion of the sanitization event, HP Secure Erase will present the IT Admin or User the opportunity to save a digital record of the sanitization to a USB drive, connected to one of the USB ports on the PC.

   HP Secure Erase will create a NIST 800-88R1 compliant document of completion, containing the details of the sanitization event. This includes, but is not limited to:
   - Date of the Sanitization of the drive
   - Time of the Sanitization of the drive
   - Drive Model Number
   - Drive Serial Number
   - Media Type
   - Type of Sanitization performed (Clear or Purge)
   - PC data (Model and Serial Number of the PC the drive was connected to)
   - HP BIOS version that performed the Sanitization
   - Sanitization result
   - Proof that data were effectively erased from the drive

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 data, which moves the drive to its highest performance state.

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.

Writing or overwriting data to a 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.

Conclusion

HP Secure Erase is easily enabled through the standard F10 BIOS setup process on most HP business-class PCs. By using HP Secure Erase, users can ensure that SSDs are completely sanitized and meet the NIST 800-88R1 industry standards.

Learn more at hp.com/wolf or hp.com/securityresources

1. For the methods outlined in the National Institute of Standards and Technology Special Publication 800-88R1 "Clear" or "Purge" sanitization methods. Drive types and the ability to support "Clear" or "Purge" can vary. 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).

3. HP G9 or newer Business PC's - includes HP Notebook, Desktop, Workstation and Mobile Workstations.

4. https://csrc.nist.gov/pubs/sp/800/88/r1/final

4AA7-2608ENW, January 2025