TECHNICAL WHITE PAPER

CONTENTS & NAVIGATION

ADDITIONAL HP SECURE ERASE OPTIONS ON HP DESKTOP WORKSTATIONS

HP SECURE ERASE PER NIST SP 800-88

Safely and effectively erase sensitive data from solid state and hard drives in accordance with NIST SP 800-88 Rev. 1

HP Secure Erase is a critical resource for IT administrators tasked with protecting sensitive data, and a key component of HP system security. HP Secure Erase is available on most HP Business PCs and all HP Desktop Workstations. It makes it easy to sanitize local magnetic hard disk drives (HDDs) or solid-state drives (SSDs) to industry standards before re-use, recycling, or disposal. Select HP Desktop Workstations have additional Secure Erase options to erase drives per NIST SP 800-88.

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 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.

HP Secure Erase is a standard feature on most HP Business PCs and all HP Desktop Workstations. Additional options to erase drives per National Institute of Standards and Technology Special Publication 800-88 are available on HP Z4 G4, Z6 G4, and Z8 G4 Desktop Workstations.

NIST SP 800-88 Compliance

Securely erasing storage drives can often become a choice between security, effectiveness and speed. The destination of the drive will also determine the appropriate methods of data erasure that should be performed on the drive. The National Institute of Standards Technology (NIST) outlines the proper techniques of securely erasing drives. These methods depend on if the drive will remain within an organization, or leave the organization following a successful erasure. HP Secure Erase has been extended to meet these requirements as a tool that presents smarter and NIST-compliant local storage sanitization options.

Industry-standard disk sanitation

To securely erase all user data from SSDs and HDDs and restore the drive to a fresh-out-of-box (FOB) performance state, the National Institute of Standards Technology (NIST) "Guidelines for Media Sanitization" (SP800-88 Rev. 1) defines several operations and outlines a verification process for media sanitization.

Clearing a drive

The following supported operations fall under the Clear category of NIST storage device sanitization guidelines and are intended to be performed on drives that will remain within an organization after being erased.

Secure Erase and *Enhanced Secure Erase* are functions supported on SATA SSDs and HDDs. Using the ATA command SECURITY ERASE UNIT EXT, with a specific bit set or cleared in the command structure, this function will instruct the drive's controller to perform Secure Erase by overwriting user data area with binary 0s or binary 1s, or to perform Enhanced Secure Erase, by overwriting user data area with a vendor specific pattern.

NVMe SSDs do not support conventional ATA feature sets. Instead, NVMe devices support drive clearing functions inside their FORMAT NVM command structure. So, by setting some specific bits in this command structure, a function similar to Secure Erase can be carried out.

Purging a drive

The following supported sanitization functions fall under the Purge category of NIST storage device sanitization guidelines and are intended to be performed on drives that will leave an organization after being sanitized.

Block Erase is a function supported in SATA SSDs. Using the ATA command BLOCK ERASE EXT, this function 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.

Overwrite is a function supported only in SATA HDDs. Using the ATA command OVERWRITE EXT, this function will instruct the HDD controller to overwrite the data across all user data area of the drive with 32-bit pattern that is repeated as necessary to fill each physical sector.

Crypto Erase is a function supported on SATA Self-Encrypting Drives (SEDs). Using the ATA command CRYPTO SCRAMBLE EXT, this function removes the encryption key on the drive, effectively making it impossible to reconstruct any of the data on the storage device.

NVMe devices support sanitize functions, such as BLOCK ERASE and CRYPTO ERASE operations by using the SANACT command. So, by setting some specific bits in this command structure, functions similar to these operations can be carried out.

Verification of Successful Sanitization

NIST outlines a verification process for media sanitization which, at a minimum, requires that at least 10% of user data area of a drive be checked for successful erasure, following a successful NIST operation. HP Secure Erase performs pseudo-random sector checks across the user data area of the drive, totaling to at least 10% of user data, after issuing a successful NIST supported Secure Erase command.

What data is not erased?

After performing a NIST-compliant Secure Erase operation on a local drive, all previously stored data in user space is completely and irretrievably erased on SSDs and overwritten on HDDs. User space is then ready to accept new host-written data, which moves the drive to its highest performance state (FOB). On SEDs and SSDs, the drive's encryption key is changed, effectively making it impossible to reconstruct any of the data on the storage device. 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

Proper sanitization through NIST SP 800-88 compliance is important when a system is being recycled, disposed of, or re-provisioned for another user. By using HP Secure Erase, users can ensure that SSD and HDD drives are completely sanitized and meet the current minimum industry standards. HP Secure Erase is easily enabled through the standard F10 BIOS setup process on most HP Workstation PCs.

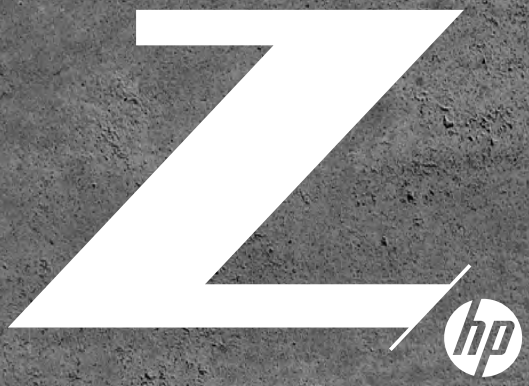
Learn More

https://www8.hp.com/us/en/solutions/computer-security.html

https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final

SIGN UP FOR UPDATES
HP.COM/GO/GETUPDATED

SHARE WITH COLLEAGUES



CONTACT US

© Copyright 2020 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

4AA7-8067ENW, July 2020