Drive Security for Xerox® Devices with Solid State Drives (SSD)

How Xerox keeps your data safe

Version 1.0
November 11, 2016

SSD Security Overview

Introduction

Xerox printing devices will have Solid State Drive (SSD) mass storage devices as the system disk on selected models. Solid State Drives are mass storage devices that use NAND-based Flash memory instead of spinning disks used in traditional hard disk drives (HDD). These memory based drives appear to the device operating system as a traditional HDD but are faster and not as susceptible to mechanical issues.

SSDs have operational characteristics that affect some security features available in traditional HDD enabled devices. This whitepaper describes how these security features differ in devices with SSDs.

Overwrite Functionality Not Supported on SSD

Due to the nature of Flash memory operation, SSDs are not able to securely delete files by directly overwriting their data as can be done with a hard disk drive. The following SSD read / write characteristics prevent the implementation of the Overwrite (both Immediate and Disk) feature to securely delete files.

- SSD controllers use a technique called “wear leveling” to evenly distribute data across all Flash blocks in the SSD. This causes data previously written to be moved dynamically to different locations when writing new data. The previous data locations cannot be tracked for overwriting.
- SSD “write amplification” behavior also causes the SSD controller to dynamically relocate previously written data. Data is written to Flash locations using 4 to 8 KB pages, but must be erased in blocks of typically 256KB. Existing data is relocated to free entire blocks for erasure, as Flash needs to be erased before it can be written again.

Drive Encryption

Xerox has long offered the ability to encrypt the user data partition of the system disk in its devices. This disk encryption feature, using industry-standard AES-256 encryption, protects all user files associated with print, network scan, internet fax, network fax, and e-mail jobs. Xerox devices with SSD have the same drive encryption that is available on devices with HDD.

Drive encryption defaults to enabled on devices with SSD and on some devices cannot be disabled. While this feature is optional on older devices with HDD, Xerox recommends that it always be enabled regardless of the type of disk in use.

Additional SSD Security Features

In addition to the disk encryption feature Xerox devices with SSDs also have the TRIM feature enabled. TRIM allows the operating system to mark a section of the SSD as deleted. Once enough pages are marked for deletion, the TRIM command performs a "garbage collection" operation. This action deletes large "blocks" of data all at once, allocating free space on the drive.

This feature makes it even more difficult to recover erased data and is enabled at the hardware level. It runs in the background on the SSD controller and does not significantly impact system performance.

Changes to the User Interface

Since SSDs do not support overwrite, the following settings are not available on devices with SSD.

- Immediate Job Overwrite
- Disk Overwrite

Since these functions are not available, no entries for them will be made in the Audit Log.

Optional Hard Drive Kit

For customers who require disk overwrite that conforms to NIST Special Publication 800-88 Rev1 Xerox offers an optional hard drive kit for some devices that replaces the SSD with a traditional HDD. A link will be provided in the future for more details on this offering.

Models with Standard SSD

A list of Xerox devices that have SSDs for their standard system disk will appear below when they are available.

Models with Optional SSD Kit

A list of Xerox devices that have an option SSD kit will appear below when they are available.

©2016 Xerox Corporation. All rights reserved. Xerox® and Xerox and Design® are trademarks of Xerox Corporation in the United States and/or other countries. BR20365