Technical white paper

HP LaserJet Managed MFP Hard Disk Security

Contents

June 2019
Version 2.0

Public

Introduction

The HP LaserJet Managed MFP printers listed below have an additional processing board (Engine Controller Board) and associated hard disk drive (HDD) in addition to the device formatter HDD or eMMC. This whitepaper provides technical information regarding what data is stored on the Engine Controller board HDD and data stored on the formatter HDD or eMMC.

Products

HP LASERJET MANAGED MFP E724xx SERIES
HP LASERJET MANAGED MFP E725xx SERIES
HP LASERJET MANAGED FLOW MFP E725xx SERIES
HP COLOR LASERJET MANAGED MFP E778xx SERIES
HP COLOR LASERJET MANAGED MFP E774xx SERIES
HP COLOR LASERJET MANAGED FLOW MFP E778xx SERIES
HP LASERJET MANAGED MFP E825xx SERIES
HP LASERJET MANAGED FLOW MFP E825xx SERIES
HP COLOR LASERJET MANAGED MFP E876xx SERIES
HP COLOR LASERJET MANAGED FLOW MFP E876xx SERIES

Data Usage by Engine Controller Board and Formatter HDDs

Engine Controller Board HDD Data

The engine controller board HDD is part of the scan image pipeline. All scanner related job files or temporary job files are stored on this drive. This includes files required for the following job types:

- Copy
- Send to E-mail
- Send to USB drive
- Send to Network Folder
- Send to Fax
- Send to SharePoint
- Scanned Stored Jobs

All temporary files created as part of processing scan jobs are erased at the completion of the job and before the next job begins. The file erase used is dictated by the Managing Temporary Job Files setting located in the EWS or though Web Jetadmin.

Formatter HDD or eMMC Data

The formatter HDD or eMMC is part of the print image pipeline. All print related job files or temporary job files are stored on this drive. This includes files required for the following job types:

- Large print jobs
- Print jobs using Collation paper handling
- Stored Jobs (driver based)

All temporary files created as part of processing print jobs are erased at the completion of the. The file erase used is dictated by the Managing Temporary Job Files setting located in the EWS or though Web Jetadmin.

Note: See “Appendix C: Formatter and Engine Controller Board Storage Options” for models with eMMC storage.

Additional Data Stored on the Formatter HDD or eMMC

In addition to print job data, the formatter HDD or eMMC also manage the following system data:

- Configuration data - Contains administrator and user configured settings and system information.
- System data - Contains the HP FutureSmart Firmware operating system code.
- Repository - Contains a compressed copy of the device operating system installation code for system recovery.

Engine Controller Board eMMC Module

All HP LaserJet Managed MFP printers with an engine controller board scanning image pipeline include a separate eMMC module. This device stores the engine controller board firmware which executes from this eMMC.

- The eMMC is permanently mounted to the engine controller board and is not removable.
- Customer or job data is never stored on the engine controller board eMMC. The engine controller board eMMC is not encrypted.
- On a firmware upgrade a signed firmware package is downloaded to the engine controller board eMMC.
- The engine controller board firmware executes from this eMMC. The system will come to ready without a functioning engine controller board HDD, however scanner functions will be disabled in this scenario.

Secure Erase Commands

The secure HDD erase commands are executed by issuing standard ATA interface commands directly to the HDD embedded controller electronics. All secure erase commands are applied to both the formatter HDD and the engine controller board HDD when executed.

These erase modes are only accessible from the pre-boot menus. Performing secure HDD erase commands will render the device inoperable as the operating system will also be erased. A new firmware image must be installed before the device can be used again.

For both the Secure Erase and Erase/Unlock disk erase commands, the disk forces its encryption keys to be destroyed and new keys generated. This instantly renders all the encrypted data on the disk unreadable. There is no method to recover the encryption keys and no method to recover the encrypted data once the keys have been changed.

Secure Erase

This erase command securely erases all data on both the formatter and engine controller board hard disks by issuing the ATA command “Security Erase Unit” in “Normal” mode. This overwrites the entire HDD with binary 0s and regenerates the disk encryption key.

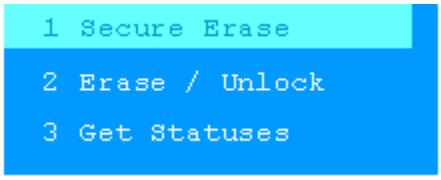

Figure 1: Secure Erase in device Pre - boot Menu

Erase / Unlock

This erase command securely erases all data on both the formatter and engine controller board hard disks by issuing the ATA command “Security Erase Unit” in “Enhanced” mode which regenerates the disk encryption key. This erase also clears the Disk Lock Key, which pairs the HDD to the printing device preventing reading of the data on another device. Clearing the Disk Lock Key allows the HDD to be relocated to a different printer.

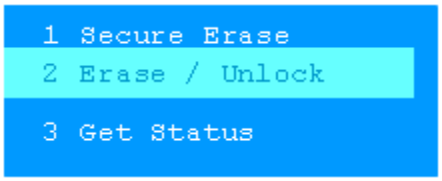

Figure 2: Erase / Unlock in device Pre - boot Menu

Customer Job Data Erase Commands

These erase options determine how files created as part of processing and storing print, copy, fax, or digital send jobs are erased. The commands are only available in the device EWS or Web Jetadmin.

Erase Job Data

This feature will erase and overwrite all job data files stored on the disk including:

- Stored Jobs, Stored Fax jobs
- Stored Personal, Quick Copy and Proof and Hold jobs
- Installed Solutions Job Data

The File Erase Modes available are:

- Non-secure Fast Erase (No overwrite)
- Secure Fast Erase (Overwrite 1 time)
- Secure Sanitizing Erase (Overwrite 3 times)

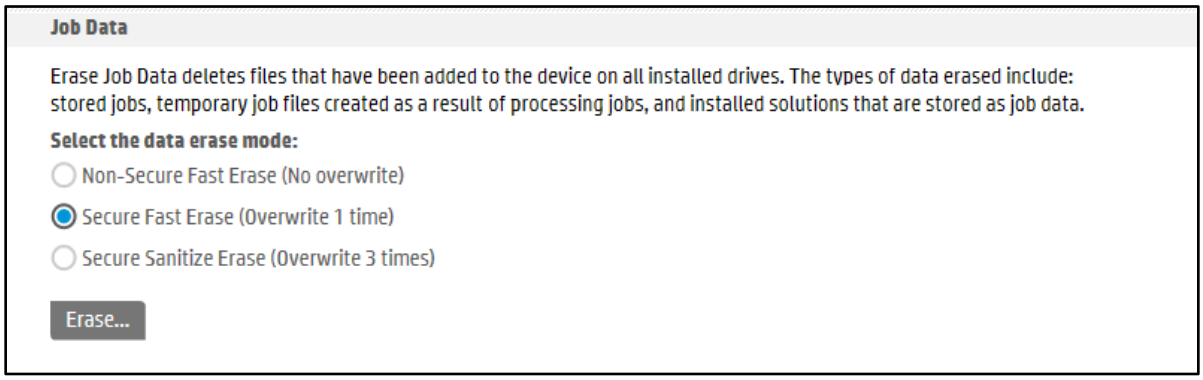

Figure 3: Erase Job Data settings in the Embedded Web Server

Note: For File Erase mode specifications see “Appendix A: Secure Erase Specifications”

Formatter eMMC Job Data

Formatter eMMC storage only allows Secure Cryptographic erase of job data. Selecting Erase will cryptographically erase the customer data area on the eMMC. The device will automatically reboot after the erase operation completes.

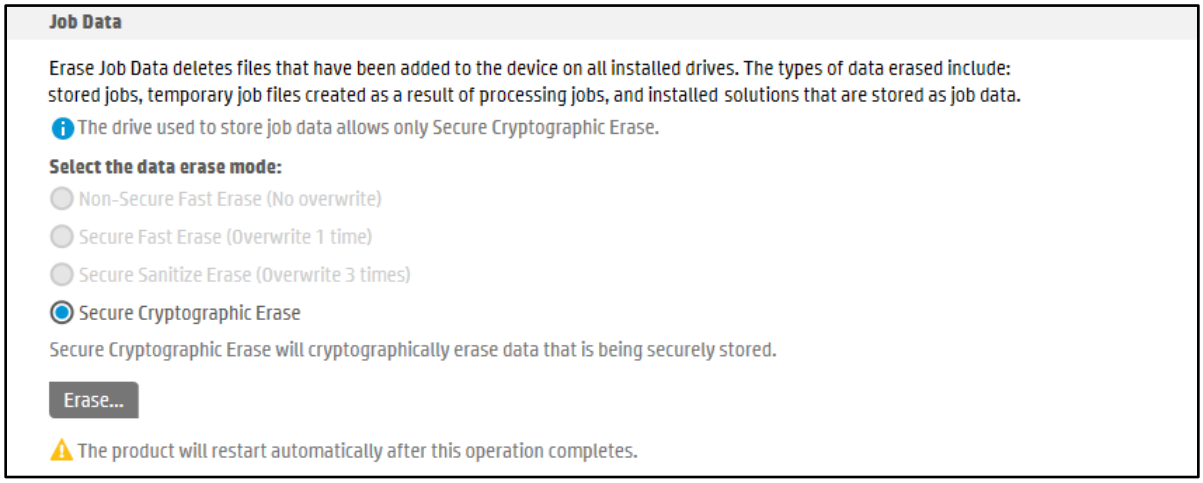

Figure 4: eMMC Erase Job Data settings in the Embedded Web Server

Note: For eMMC erase capabilities see "Appendix B: eMMC Security Characteristics"

Managing Temporary Job Files

This feature controls how temporary files created during the processing print, copy, fax, or digital send jobs are erased as part of completing the current job from both the engine controller board HDD and the formatter HDD.

The File Erase Modes available are:

- Non-secure Fast Erase (No overwrite)
- Secure Fast Erase (Overwrite 1 time)
- Secure Sanitizing Erase (Overwrite 3 times

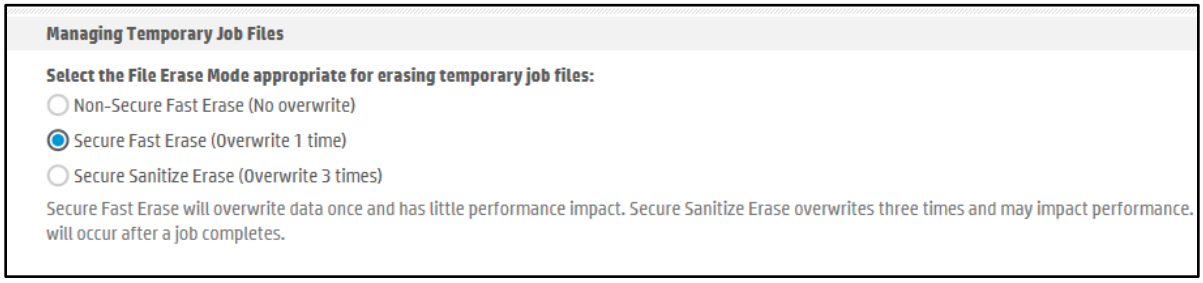

Figure 5: Managing Temporary Job Files settings in the EWS

Formatter eMMC Temporary Job Files

Formatter eMMC storage does not support Overwrite erase options. Only the Non-Secure Fast Erase option is available.

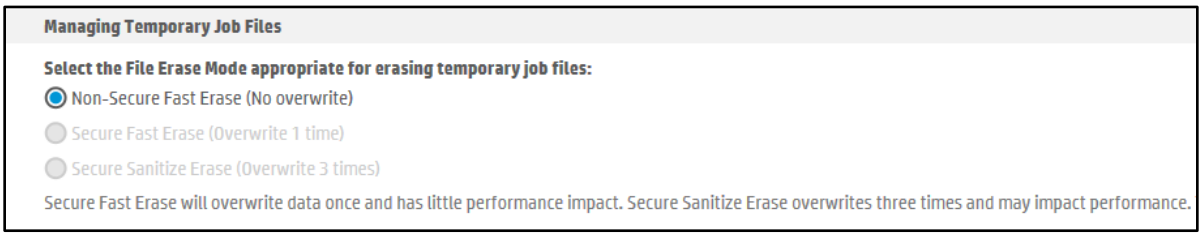

Figure 6: Managing Formatter eMMC Temporary Job Files settings with in the EWS

Note: For eMMC erase capabilities see “Appendix B: eMMC Security Characteristics”

Disk Initialization Commands

These commands reinitialize the hard disk or sections of the disk to provide troubleshooting and diagnostic capabilities. The commands are similar to disk formatting commands and do not provide sector level data overwrite. These erase command are not recommended for securely removing customer data.

These commands are only accessible from the device pre - boot menus.

Format Disk

Format Disk removes all data from the disk. This command will render the device inoperable. The device firmware must be re-installed to the disk before the device can be used again.

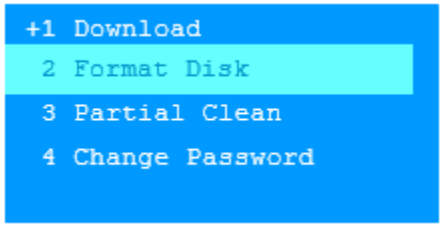

Figure 7: Format Disk in device Pre - boot Menu

Partial Clean

Partial Clean removes all data from the disk with the exception of the compressed operating system installation code in the repository and initiates a reload of the device operation system.

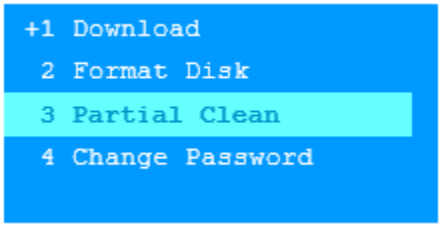

Figure 8: Partial Clean in device Pre - boot Menu

Government Erase Standards

These devices follow comply with current US Government requirements for clearing confidential data from a hard disk as specified in *Updated DSS Clearing and Sanitization Matrix AS OF June 28, 2007* and *NIST Special Publication 800-88, Guidelines for Media Sanitation.*

NIST 800-88 defines three levels of sanitization, from weakest to strongest:

- Clear Overwrite all storage space one or more times
- Purge Degauss the disk or execute the ATA Secure Erase command if the drive supports it (all hard disks used by HP support this command)
- Destroy Incinerate, crush, or chemically destroy the disk

Secure Erase Feature	NIST Sanitization Level
Managing Temporary Job Files	**Clear** when using Secure Fast Erase or Secure Sanitize Erase modes
Erase Job Data	**Clear**
Secure Disk Erase	**Clear** and **Purge**
Erase/Unlock encrypted disk	The cryptographic erase used by the HP High Performance Secure Hard Disk has been submitted to NIST for approval at the **Purge** level of sanitization. No decision has been made yet.

Appendix A: Secure Erase Specifications

Normally when a file is deleted from a HDD, the filename entry is erased from the disk's file allocation table, removing the file's presence. The file's data still exists in the disk's individual sectors and is overwritten only when that sector is allocated for a different file.

HP Secure Erase technology overwrites a deleted file's data from the individual sectors with random data using either a one pass or three pass overwrite, which conform to current US Government specifications.

Note: See the Government Erase Specifications section for further information

To enable Secure Erase using data overwrite, select the following options for "File Erase Mode" when available:

- Non-secure Fast Erase mode: Performs standard file system delete only (does not overwrite file data)
- Secure Fast Erase mode: Performs a one pass overwrite of all data
- Secure Sanitizing Erase mode: Performs a three pass overwrite of all data

Note: The system default is Non-Secure Fast Erase mode. Secure Fast Erase mode is recommended for best overwrite system performance.

Overwrite Specifications

Secure Fast Erase mode follows the National Institute of Standards and Technology Special Publication 800-88, Guidelines for Media Sanitization.

For Secure Fast Erase, each deleted file's data is overwritten once with:

- the hexadecimal character 0x48.

Secure Sanitizing Erase mode follows the U.S. Department of Defense 5220-22.M specification using a succession of multiple data overwrites.

For Secure Sanitizing Erase, each deleted file is overwritten with:

- the fixed character pattern (binary 01001000).
- the complement of the fixed character pattern (binary 10110111).
- a random character:
    - A 32k byte buffer of random characters is generated for each file delete operation using the device's unique uptime as the seed.
    - Each byte of file data uses a unique random character from the buffer.
    - The random character buffer is reused up to 32 times, and then regenerated using new random data.

To ensure successful completion of each overwrite operation, each overwritten byte is verified.

Note: NIST SP-800-88 "Guidelines for Media Sanitization" (Sept 2006) supersedes the US DOD 5220-2.M (1997 edition) specification.

Appendix B: eMMC Security Characteristics

Embedded Multimedia Card (eMMC) Security Overview

Some models of HP printing devices use Embedded Multimedia Card (eMMC) mass storage devices as the system disk (See **Appendix C** for these models). SSD and eMMC 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 printing device operating system as a traditional Hard Disk Drive.

eMMCs have operational characteristics that affect some security features available in traditional HDD enabled devices. For high security environments and security sensitive applications, HP recommends

- Selecting models that include a HDD
- Adding an optional HDD when supported

Secure Erase Data Overwrite Functionality Not Supported on eMMC

Due to the nature of Flash memory operation, eMMC storage is not able to securely delete files by directly overwriting the data as can be done with a hard disk drive. The following eMMC read / write characteristics prevent the implementation of HP's Secure Erase Data Overwrite feature to securely delete files by overwriting the file data.

- eMMC controllers use a technique called "wear leveling" to evenly distribute data across all flash blocks in the storage device. 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.
- eMMC "write amplification" behavior also causes the memory 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.

Secure Volatile Storage Feature with eMMC

To protect customer data on devices using eMMC, HP uses firmware encryption to specific areas of the storage device containing customer job data. All files written to the customer job data disk areas are encrypted using AES-128 encryption. This can be configured to AES-256 encryption, if desired.

Data stored on the encrypted partition includes: Stored print jobs, temporary print job files, PJL and PostScript filesystem files including downloaded fonts, and extensibility customer data (if stored there by the extensibility solution).

Appendix C: Formatter and Engine Controller Board Storage Options

HP LaserJet Model	Formatter Storage		Engine Controller Board		B5L29A Secure HDD Accessory
	16 GB eMMC	320 - 500 GB HDD AES-256	16 GB eMMC	320 -500 GB HDD AES-256	500 GB FIPS, AES-256
HP LASERJET MANAGED MFP E724xx dn SERIES	Y		Y		Y
HP LASERJET MANAGED MFP E725xx dn SERIES	Y			Y	Y
HP LASERJET MANAGED FLOW MFP E725xx z SERIES		Y		Y	
HP COLOR LASERJET MANAGED MFP E774xx dn SERIES	Y		Y		Y
HP COLOR LASERJET MANAGED MFP E778xx dn SERIES	Y			Y	Y
HP COLOR LASERJET MANAGED FLOW MFP E778xx z SERIES		Y		Y	
HP LASERJET MANAGED MFP E825xx du SERIES		Y		Y	
HP LASERJET MANAGED MFP E825xx dn SERIES		Y		Y	
HP LASERJET MANAGED FLOW MFP E825xx z SERIES		Y		Y	
HP COLOR LASERJET MANAGED MFP E876xx du SERIES		Y		Y	
HP COLOR LASERJET MANAGED MFP E876xx dn SERIES		Y		Y	
HP COLOR LASERJET MANAGED FLOW MFP E876xxz SERIES		Y		Y	
HP LaserJet Model FIPS Compliant HDD SKUs	**Formatter Storage**		**Engine Controller Board**		**B5L29A Secure HDD Accessory**
	16 GB eMMC	500 GB FIPS, AES-256	16 GB eMMC	500 GB FIPS, AES-256	500 GB FIPS, AES-256
HP LASERJET MANAGED FLOW MFP E725xx z SERIES #201, #202 Gov't SKUs		Y		Y	
HP COLOR LASERJET MANAGED FLOW MFP E778xx z SERIES #201, #202 Gov't SKUs		Y		Y	
HP LASERJET MANAGED MFP E825xx du SERIES #201, #202 Gov't SKUs		Y		Y	
HP LASERJET MANAGED FLOW MFP E825xx z SERIES #201, #202 Gov't SKUs		Y		Y	
HP COLOR LASERJET MANAGED MFP E876xx du SERIES #201, #202 Gov't SKUs		Y		Y	
HP COLOR LASERJET MANAGED FLOW MFP E876xx z SERIES #201, #202 Gov't SKUs		Y		Y	

hp.com/go/support

Current HP driver, support, and security alerts delivered directly to your desktop

c05475902, Created April 2017; Updated June 2019
Version 2.0
Public