HP FutureSmart Firmware
Device Hard Disk Security

Summary:

This document discusses hard disk security for HP FutureSmart Firmware printing devices.

Contents:

October 2010
Version 1.0

Public

Overview

This document discusses secure erase options and hard disk security on HP FutureSmart Firmware printing devices. The section of the disk containing job data can now be securely erased on demand, instead of performing an entire disk wipe (See Erase Job Data). Industry standard ATA Secure Erase is an available option which securely wipes all data including spared and reallocated sectors for decommissioning devices (See Secure Disk Erase).

Secure Erase Commands

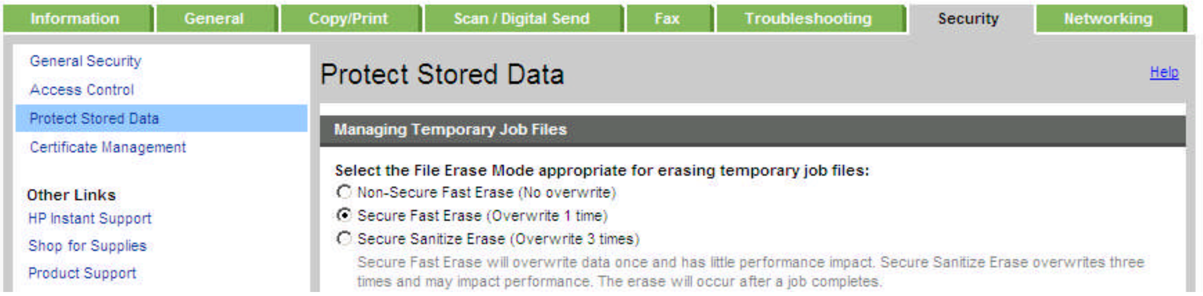
HP FutureSmart Firmware printing devices support four different data erase features to securely erase ongoing job data, and for device decommissioning or redeployment.

1. Managing Temporary Job Files

   The feature controls how temporary job files are erased at the completion of print, copy, fax, or digital send jobs.
   Temporary job files include:
   - Temporary data for print jobs
   - Temporary data for copy, fax, e-mail, and send to network folder jobs

   The File Erase Modes available are:
   - Non-secure Fast Erase (No overwrite)
   - Secure Fast Erase (Overwrite 1 time)
   - Secure Sanitizing Erase (Overwrite 3 times)

<u>Note</u>: For File Erase mode specifications see Appendix A



Protect Stored Data

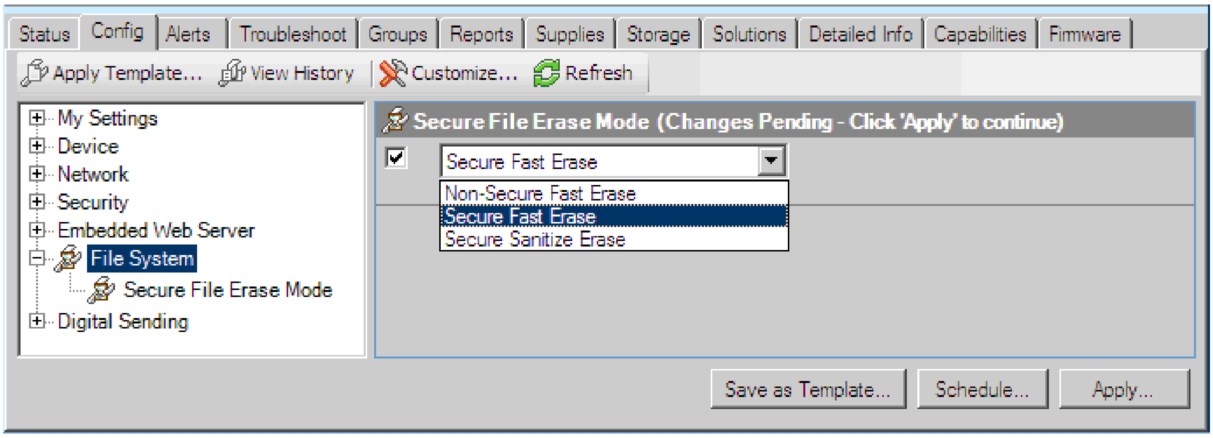
Managing Temporary Job Files

Select the File Erase Mode appropriate for erasing temporary job files:

○ Non-Secure Fast Erase (No overwrite)
● Secure Fast Erase (Overwrite 1 time)
○ Secure Sanitize Erase (Overwrite 3 times)

Secure Fast Erase will overwrite data once and has little performance impact. Secure Sanitize Erase overwrites three times and may impact performance. The erase will occur after a job completes.

Figure 1: Managing Temporary Job Files settings in the Embedded Web Server (EWS)



Secure File Erase Mode (Changes Pending - Click 'Apply' to continue)

☑ Secure Fast Erase

Non-Secure Fast Erase
Secure Fast Erase
Secure Sanitize Erase

Figure 2: Secure File Erase Mode settings in Web Jetadmin
<u>Note</u>: This setting corresponds to Managing Temporary Job Files setting in EWS

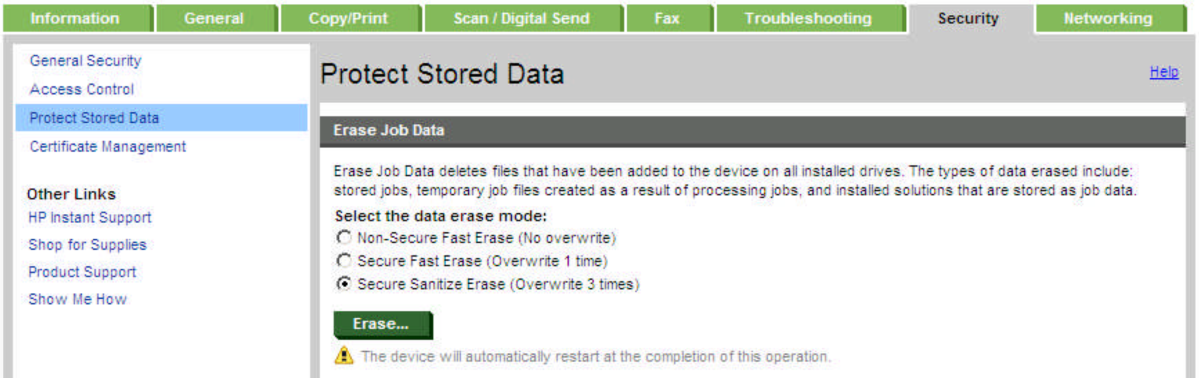
2. Erase Job Data

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

- Temporary data for print jobs
- Temporary data for copy, fax, e-mail, and send to network folder jobs
- Stored Jobs, Stored Fax jobs

The File Erase Modes available are:

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



Protect Stored Data

Erase Job Data

Erase Job Data deletes files that have been added to the device on all installed drives. The types of data erased include: stored jobs, temporary job files created as a result of processing jobs, and installed solutions that are stored as job data.

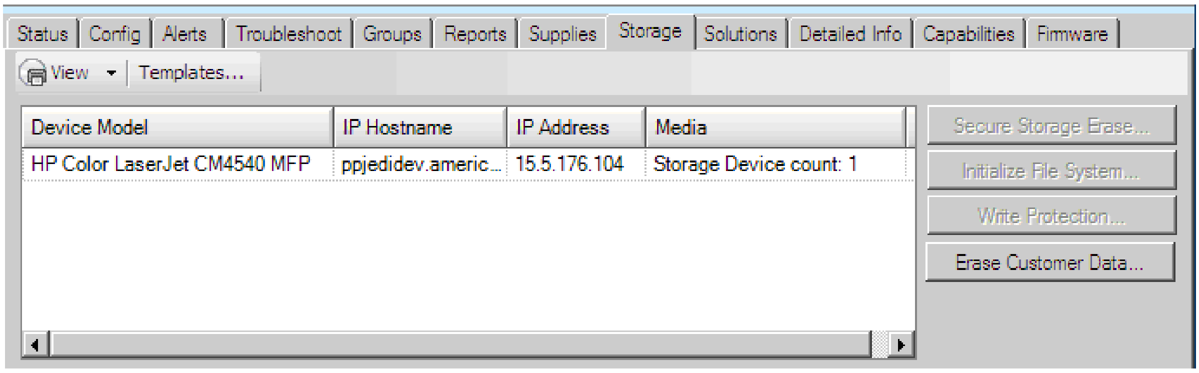
Select the data erase mode:

○ Non-Secure Fast Erase (No overwrite)
○ Secure Fast Erase (Overwrite 1 time)
● Secure Sanitize Erase (Overwrite 3 times)

Erase...

⚠ The device will automatically restart at the completion of this operation.

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



Device Model	IP Hostname	IP Address	Media
HP Color LaserJet CM4540 MFP	ppjedidev.americ...	15.5.176.104	Storage Device count: 1

Figure 4: Erase Customer Data settings in Web Jetadmin
Note: This setting corresponds to Erase Job Data setting in EWS

3. Secure Disk Erase

This feature securely erases all data on the hard disk, including disk sectors spared and relocated sectors. This erase operation, also known as ATA Erase, is executed directly by the hard disk controller.

Secure Disk Erase meets the "Purge" erase standard defined in *NIST Special Publication 800-88, Guidelines for Media Sanitation.*

Note: See the Government Erase Specifications section

This erase mode is only accessible from the pre - boot menus for the main system disk. It is available for accessory disks in EWS and Web Jetadmin. If the erased disk contained the system firmware, performing an Erase/Unlock will render the device inoperable, and a new firmware image must be installed to the disk before the device can be used again.

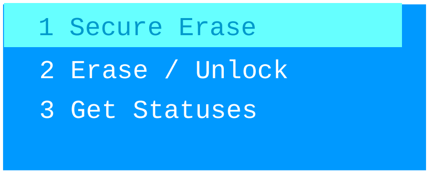


Figure 5: Secure Disk Erase in device Pre - boot Menu

4. Erase / Unlock Encrypted Disk

The HP High Performance Secure Hard Disk supports a special erase referred to as a "Crypto Erase". Selecting the Erase/Unlock option for one of these disks 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.

This erase mode is only accessible from the pre - boot menus for the main system disk. It is available for accessory disks in EWS and Web Jetadmin. If the erased disk contained the system firmware, performing an Erase/Unlock will render the device inoperable, and a new firmware image must be installed to the disk before the device can be used again.

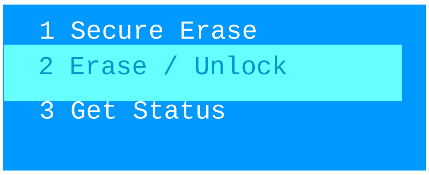
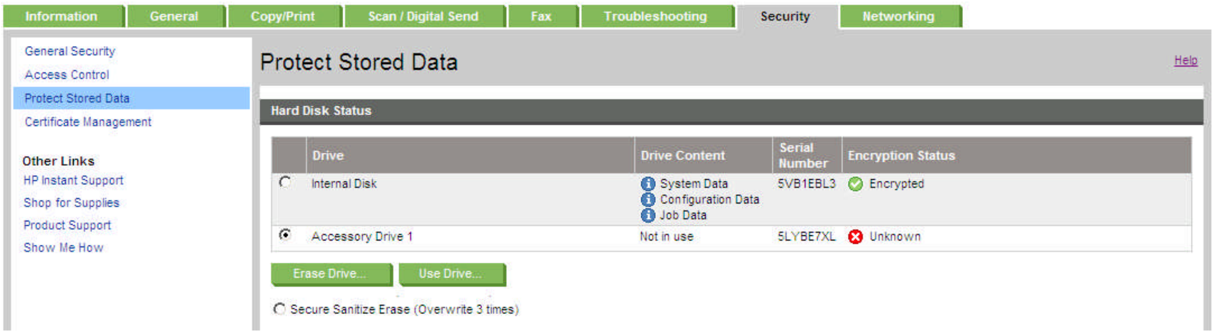


Figure 6: Erase / Unlock in device Pre - boot Menu

Accessory Drive

A second hard drive can be added to the device to store all customer job data. Once the drive is installed, it is enabled by selecting the drive and clicking the Use option. All existing customer job data is then transferred to the external drive automatically. From that point forward all job data including temporary files for print and scan jobs use the accessory drive instead of the main system drive.



Protect Stored Data

Hard Disk Status

	Drive	Drive Content	Serial Number	Encryption Status
○	Internal Disk	System Data Configuration Data Job Data	5VB1EBL3	✓ Encrypted
●	Accessory Drive 1	Not in use	5LYBE7XL	✗ Unknown

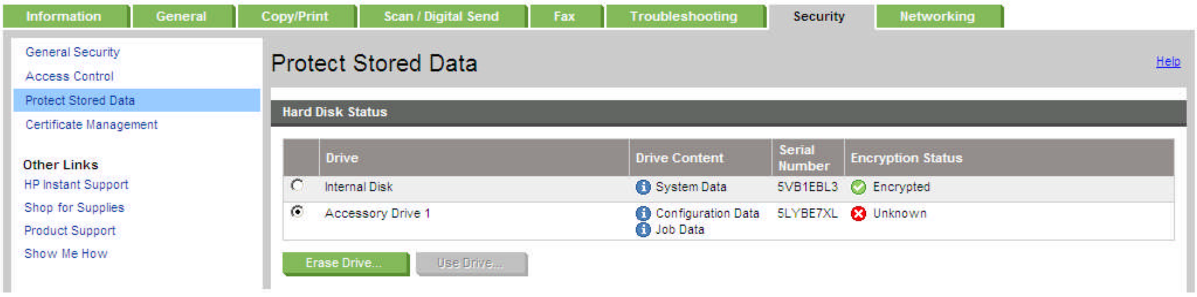
○ Secure Sanitize Erase (Overwrite 3 times)

Figure 7: Accessory Drive settings in the Embedded Web Server (EWS)

The accessory drive can be securely erased independently of the system drive. Two erase operations are available.

- If the drive is an HP Secure Disk encrypted hard drive, a cryptographic erase can be performed. (See the Erase / Unlock section in the Secure Erase section)

- Secure Disk Erase selects the most secure method to remove the drives data, other than a cryptographic erase. The method will either be a Secure Erase using data overwrite or an ATA Secure Disk Erase
(See the Secure Disk Erase topic in the Secure Erase Command section)

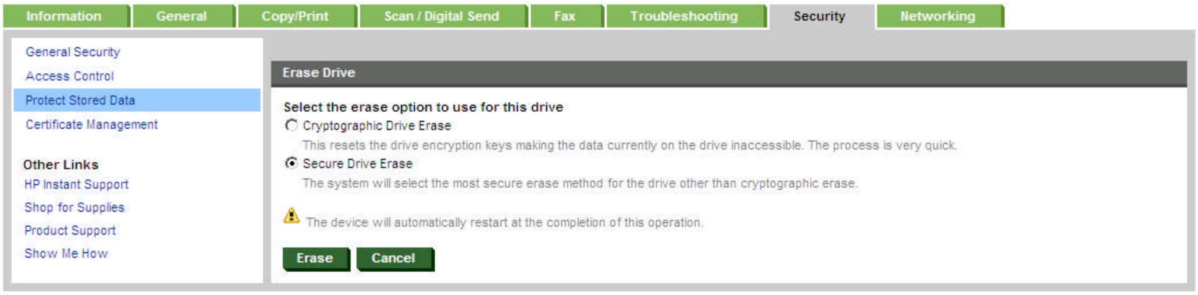


Protect Stored Data

Hard Disk Status

	Drive	Drive Content	Serial Number	Encryption Status
○	Internal Disk	System Data	5VB1EBL3	Encrypted
●	Accessory Drive 1	Configuration Data Job Data	5LYBE7XL	Unknown

Figure 8: Accessory Drive Erase command in Hard Disk Status of EWS



Erase Drive

Select the erase option to use for this drive

○ Cryptographic Drive Erase
This resets the drive encryption keys making the data currently on the drive inaccessible. The process is very quick.

● Secure Drive Erase
The system will select the most secure erase method for the drive other than cryptographic erase.

The device will automatically restart at the completion of this operation.

Figure 9: Erase options for accessory drive in the Embedded Web Server (EWS)

Disk Architecture

The printing device Hard Disk is divided into different sections for different classes of data

- Job Data: Contains all job data, including temporary files for print and scan jobs, and Stored Jobs.

- Configuration Data: Contains printing device dependant configuration settings and system information. Information stored here includes printing defaults, authentication configuration, and some customer specific configuration settings.

- System Data: Contains the HP FutureSmart Firmware operating system code. This code must be present on the hard disk for the printing device to boot. Previous HP printing device operating systems booted from a compressed image stored in non-volatile memory.

- Repository: This area contains a compressed copy of the device operating system installation code, providing a way to restore a corrupted operating system image or recover from a failed firmware upgrade.

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 <u>not</u> recommended for securely removing customer data.

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

- <u>Clean Disk</u> 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.

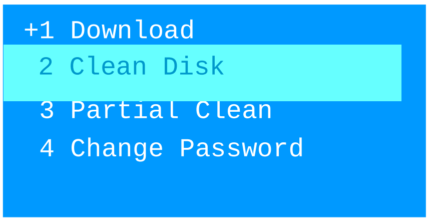


Figure 10: Clean Disk in device Pre - boot Menu

- <u>Partial Clean</u> removes all data from the disk with the except the compressed operating system installation code in the repository and initiates a reload of the device operation system.

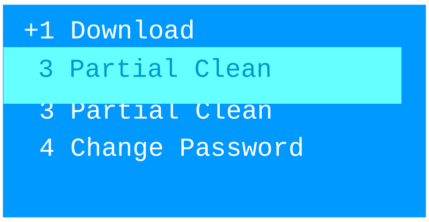


Figure 11: Partial Clean in device Pre - boot Menu

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:

- <u>Clear</u> Overwrite all storage space one or more times
- <u>Purge</u> Degauss the disk or execute the ATA Secure Erase command if the drive supports it (all hard disks used by HP support this command)
- <u>Destroy</u> 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 Data Overwrite and 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: Device List

The devices support HP FutureSmart Firmware functionality:

HP Color LaserJet CM4540 MFP
HP Color LaserJet CP5525

October 2010
Version 1.0