White Paper

HP Secure Disk Erase

June 2004

Document Version: 1

Imaging and Printing Group
Hewlett-Packard Company

Contents

Abstract:

To meet the needs for higher levels of Print and Imaging security, HP has implemented a disk erase feature which meets the U.S. Department of Defense 5220-22.M requirements for the clearing of disk media. This paper describes this capability and related information.

1 Introduction

To meet the needs for higher levels of Print and Imaging security, Hewlett-Packard has implemented a security feature in which print, scan, fax, and copy jobs can be securely erased from the hard disk drive. This is the secure disk erase feature provided as a standard feature on supported multifunction peripherals (MFPs).

The secure disk erase feature provides a choice of three different levels of disk security, which are configurable by an administrator and may be protected from unauthorized changes with a password.

- Sanitized Erase: Conforms to the DoD 5220-22.M specification for deletion of magnetically stored data. Using multiple data writes to eliminate trace magnetic data, Sanitized Erase prevents subsequent analysis of the hard disk drive's physical platters for the retrieval of data. See section 4, Specifications, for an explanation of the erase algorithm implemented.
- Secure Erase: Provides increased performance, overwriting the existing data once, and preventing software-based "undelete" operations to the data.
- Fast Erase: Provides the greatest performance, flagging the print job as deleted, and allowing the MFP's operating system to reclaim and subsequently overwrite the data when needed.

Unless otherwise specified, print job data is deleted from the disk at the completion of the print job. Multiple mechanisms are supported for the erasure of disk drive data.

2 Data Affected

Data affected by the secure disk erase feature includes temporary files created during the print, scan, fax and copying process, stored jobs, proof and hold jobs, disk-based fonts, and disk-based macros (e.g., forms). Stored jobs will only be securely overwritten when they have been deleted through the "Retrieve Job" menu on the device after the appropriate erase mode has been set. This feature will not impact data stored on flash-based printer non-volatile RAM that is used to store default printer settings, page counts, and so forth. This feature does not affect data stored in a system RAM disk (if utilized). This feature will not impact data stored on the flash-based system boot RAM.

Changing the secure disk erase mode does not overwrite previous data on the disk, nor does it immediately perform a full disk sanitization. Changing the secure disk erase mode changes how the MFP cleans up temporary data for jobs after the erase mode has been changed.

3 Default Setting

Prior to the introduction of Secure Disk Erase, all HP LJ9000, HP LJ9000L, and HP LJ4100 MFPs used the "Fast Erase" mode for all file delete operations. With the introduction of Secure Disk Erase, Fast Erase will continue to be the default erase mode.

4 Specifications

HP's Sanitized Erase mode implemented on the HP LJ9000, HP LJ9000L, and HP LJ4100 MFPs meets the U.S. Department of Defense 5220-22.M requirements for clearing disk media. Using

a succession of multiple data overwrites, including the validation of the success of those overwrites, Sanitized Erase can prevent the subsequent physical analysis of the hard disk drive's media for recovery of data:

1. Each byte of file data is overwritten with the fixed character pattern (binary 01001000).
2. Each byte of file data is overwritten with the compliment of the fixed character pattern (binary 10110111).
3. Each byte of file data is overwritten with a random character:
    a. A 32k byte buffer of random characters is generated for each file delete operation using the device's unique uptime as the seed.
    b. Each byte of file data uses a unique random character from the buffer.
    c. The random character buffer is reused up to 32 times, and then regenerated using new random data.
4. To ensure successful completion of the write operation, each overwritten byte is verified.

5 Common Usage Environment

The most common scenario under which administrators will use Sanitized Erase or Secure Erase modes is when devices are being used in a highly secure environment. The administrator will want to configure the MFP for Sanitized Erase or Secure Erase mode so that data is overwritten on an ongoing basis when data is deleted from the disk.

6 User Interface

Administrators interface with the secure disk erase feature from the Device List in HP Web Jetadmin (Figure 1).

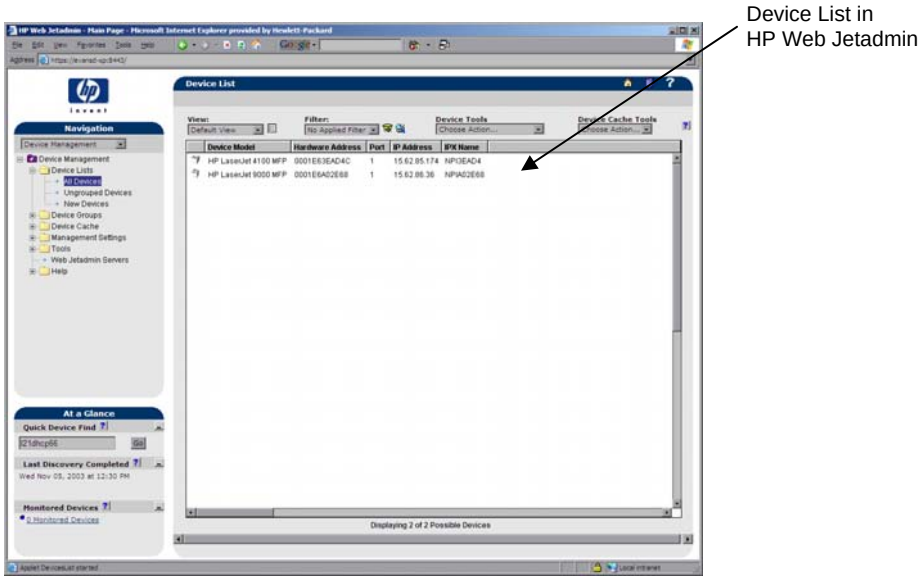

Figure 1: Device List in HP Web Jetadmin

Note: Administrators will use HP Web Jetadmin 7.5 or greater which contains the latest "plug-ins" for the HP LJ9000, HP LJ9000L, and HP LJ4100 MFP products. For more information about HP Web Jetadmin security plug-ins, see Questions and Answers later in this paper.)

The default disk erase mode is Non-Secure Fast Erase, and no file system access password is set. To set a password and the secure disk erase mode, the administrator will choose the device(s) through the Device List (double click on the device(s)) in HP Web Jetadmin (see Figure 1 earlier).

To set a system access password or select/change secure disk erase modes:

1. In the upper left of the window, choose "Configuration" from the drop-down list.
2. Click Security from the Configuration Categories list.
3. From here, administrators can:
   - Type or change a new file system access password (type the password, confirm the password, and then click Apply in the lower right corner).
   - Select or change the file system erase mode (type the password, choose the desired erase mode, and then click Apply in the lower right corner).
   - Password and secure disk erase modes can be set or changed on multiple devices simultaneously from the Device List page (select the devices, choose Configure under the Device Tools list, and then scroll to the file system access password and erase mode).

7 Impact to Performance

The Disk Erase feature does not affect printing and typical copying including simplex, duplex, enlargements, reductions, and n-up printing. Fast Erase is the fastest mode and is the default today. Secure Disk Erase is slower than Fast Erase because the file data gets overwritten. Sanitizing Erase is the most secure mode, but requires multiple overwrites of disk data and, therefore, results in the most impact to performance. Actual performance impacts will vary.

8 Availability

The new Secure Disk Erase features are available on the HP LJ9000, HP LJ9000L, and HP LJ4100 MFPs with firmware revision 03.779.0 or greater.

Customers who have a unit with firmware revision 03.757.0 or lower can upgrade their firmware via a remote firmware upgrade. These upgrades are available at the following locations:

HP LJ9000 MFP: www.hp.com/go/lj9000mfp_firmware

HP LJ9000L MFP: www.hp.com/go/lj9000Lmfp_firmware

HP LJ4100 MFP: www.hp.com/go/lj4100mfp_firmware

9 Questions and Answers

1. Question: Can the secure disk erase feature be accessed through the Embedded Web Server or via the MFP control panel?

   Answer: Access to the secure disk erase feature is controlled through HP Web JetAdmin.

2. Question: Where can HP Web JetAdmin be downloaded?

Answer: HP Web JetAdmin can be downloaded free from: http://www.hp.com/go/webjetadmin.

3. Question: What is the process to update to HP Web JetAdmin 7.5 with the security plug-ins?

   Answer: Secure Fast Erase and Secure Sanitizing Erase can only be enabled through HP Web JetAdmin 7.5, which has been updated with the latest plug-ins for HP LJ9000, HP LJ9000L, and HP LJ4100 MFPs.

   To install the security plug-ins:

   1. Start HP Web Jetadmin.
   2. Under Navigation in the left side bar, scroll down and click on Product Update.
   3. Under Product Update, click on Install (HP Web JetAdmin searches the web for the latest product updates).
   4. Highlight the plug-in for the HP LJ9000 and HP LJ4100 MFP products and click Install.

4. Question: How can the hard disk be physically secured?

   Answer: The hard disk may be physically secured from theft and tampering using an accessory lock. The accessory lock requires a physical key for hard disk drive removal.

10 Acronyms

MFPs: Multifunction peripherals.

RAM: Random access memory.

WJA: HP Web Jetadmin, which is a simple peripheral management software application for remotely installing, configuring, and managing a wide variety of HP and non-HP network peripherals using only a standard Web browser.