HP High Performance Secure Hard disk

Abstract:

Many customers store sensitive information on their Imaging and Printing Device hard disks. In high security installations, such as government facilities and large enterprises, detrimental consequences could result if this information fell into the wrong hands. As a result, customers have requested that critical information stored on the hard disk be encrypted. The industry has coined a term for confidential data on storage media, it is called "data at rest".

Notice:

©2008 Hewlett-Packard Company

Microsoft®, Windows®, and Windows NT® are trademarks of Microsoft Corporation in the U.S. and/or other countries. UNIX® is a trademark of The Open Group in the U.S. and/or other countries. Intel® and Itanium® are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the U.S. and other countries. Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California. All other product names mentioned herein may be the trademarks of their respective companies.

Neither HP, nor any of its subsidiaries, shall be liable for technical or editorial errors or omissions contained herein. The information in this publication is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for HP products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.
1 Introduction

Many customers store sensitive information on their Imaging and Printing Device hard disks. In high security installations, such as government facilities and large enterprises, detrimental consequences could result if this information fell into the wrong hands. As a result, customers have requested that critical information stored on the hard disk be encrypted. The industry has coined a term for confidential data on storage media, it is called "data at rest".

2 Customer experience

The encrypted hard disk will be a customer-installed option. Both internal and EIO hard disks will be available allowing for flexibility in deployment:

• An internal hard disk may replace an existing MFP internal hard disk.

• An EIO hard disk may be added to an MFP or SFP, or replace an existing hard disk.

Hard disk encryption will be supported in most shipping products; however for legacy devices it will be necessary to update the device’s firmware before hard disk encryption can be utilized.

To prevent ambiguity of data security, only one encrypted hard disk may be “locked” to a device at a time, and any additional installed hard disks will be disabled from access.

By default, a printer will automatically configure a newly installed encrypted hard disk, requiring no customer intervention. The customer can validate encryption is enabled using status pages or the Embedded Web Server (EWS).

Migration of data, including installed applications, digital sending and security settings, will not be available in the first phase release, and the customer will be responsible for reinstalling any needed settings or applications. A migration procedure is being developed, and will be published on the product website when available.

If the printer detects an encrypted hard disk that is configured for a different printer, or if the printer is configured for encryption and the correct hard disk is not present, manual intervention by the administrator will be required to re-enable the hard disk.

3 Installation

Installing the internal hard disk option requires replacing the existing hard disk by removing the printer’s side panel and transferring the data and power cables. EIO hard disks are inserted into an open EIO slot.
The two hard disk types with part numbers are:
HP High-Performance Secure Hard disk (J8018A).

![HP High-Performance Secure Hard disk (J8018A)]

HP High-Performance Secure EIO Hard disk (J8019A).

![HP High-Performance Secure EIO Hard disk (J8019A)]

For added physical security, the secure EIO hard disk (J8019A) includes an EIO lock adapter, shown here with the secure EIO hard disk. The adapter can be outfitted with a Kensington-type lock (with or without a cable).

![EIO lock adapter with Kensington-type lock]
By default, at start-up, a newly discovered and unused encrypted hard disk will be automatically configured and “locked” to the device. The Drive Lock Key is a software-based key, not a physical key. An administrator may configure the device to not automatically lock newly discovered encrypted hard disks, in which case the hard disk will act as an unencrypted hard disk. The hard disk may be manually locked to the printer at a later time.

4 Multiple Hard disks

If multiple hard disks are present, the following priority will be used in determining which hard disk is utilized.

1. Internal, encrypted
2. EIO, encrypted
3. Internal, unencrypted
4. EIO, unencrypted

Once an encrypted hard disk is locked to a printer, all additional hard disks (internal and EIO) installed in the printer will be disabled from use. For example, if an EIO encrypted hard disk is installed in an MFP with an internal hard disk, the internal hard disk will be disabled from use.

Disabled hard disks will be reported as being physically present in the management interfaces, however they will not be accessible for any read/write operations by the printer or users.

5 Encryption

A Seagate FDE hard disk is used that continuously encrypts every write operation and decrypts every read operation without user intervention. The hard disk uses an internally controlled encryption key for the encryption and decryption processes and this encryption key is not accessible by the printer or printer user. The hard disk uses 128 bit Advanced Encryption Standard (AES) data encryption and decryption.

This solution protects data stored on a printer’s hard disk from unauthorized access when the hard disk is removed from the printer to which it is “locked.” The “Lock Password” is either randomly generated by the printer or manually specified by the customer at installation.
6 Status & Configuration

The status of the hard disk system will be available remotely using the EWS and WJA interfaces, as well as locally using the Control Panel and Internal/Configuration Pages. Current status will include the present state of hard disk encryption (Enabled, Disabled), as well as a concise status message for any warning or error condition.

The EWS screen above shows the following information:

- Internal Hard disk is a standard non-encryptable hard disk, and is disabled.
- The external EIO hard disk is an encryptable secure hard disk, and is enabled.
- The MFP supports HP encrypted Hard disks, and is actively encrypting data.
- The encrypted hard disk is paired to this printer, and must be Reinitialized to be used in a different MFP or printer.
7 Unlocking and Crypto-Erasing Hard disks

A locked hard disk may be unlocked from a printer. To prevent the risk of subsequent unauthorized access to the hard disk’s stored data, the hard disk’s internally managed encryption keys will be reset causing a “Crypto-Erase”, effectively erasing the entire hard disk contents.

If an installed hard disk is detected to be locked to a different printer, the administrator will be warned of the condition, and the correct hard disk can be reinstalled.

Alternatively, the administrator is given the option to reinitialize the hard disk, losing all stored data, and create a new lock to the printer.

An unlocked hard disk may be re-locked to the existing printer, or moved to a new HP printer.

8 Availability

The HP High Performance Secure Hard disk will be available in Fall of 2008. Devices that will support the HP High Performance Secure EIO Hard disk (J8019A)

- HP Color LaserJet CP3525
- HP LaserJet M3027 MFP, M3035 MFP, M4345 MFP, M5025 MFP, M5035 MFP, M9040 MFP, M9050 MFP
- HP Color LaserJet CM3530 MFP, CM4730 MFP, CM6030 MFP, CM6040 MFP
- HP Digital Sender DS9250

Devices that will support the HP High Performance Secure Hard disk (J8018A)

- HP LaserJet M4345 MFP, M5025 MFP, M5035 MFP, M9040 MFP, M9050 MFP; HP Color LaserJet CM3530 MFP; HP Digital Sender DS9250