**Lexmark Printer and Multifunction Products:**
Hard Disk and Non-Volatile Memory Guide

This guide applies to the following Lexmark devices:

<table>
<thead>
<tr>
<th>Printers</th>
<th>Multifunction Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>C734</td>
<td>X463</td>
</tr>
<tr>
<td>C736</td>
<td>X464</td>
</tr>
<tr>
<td>C792</td>
<td>X466</td>
</tr>
<tr>
<td>C925</td>
<td>X651</td>
</tr>
<tr>
<td>T650</td>
<td>X652</td>
</tr>
<tr>
<td>T652</td>
<td>X654</td>
</tr>
<tr>
<td>T654</td>
<td>X656</td>
</tr>
<tr>
<td>W850</td>
<td>X658</td>
</tr>
<tr>
<td></td>
<td>X734</td>
</tr>
<tr>
<td></td>
<td>X736</td>
</tr>
<tr>
<td></td>
<td>X738</td>
</tr>
<tr>
<td></td>
<td>X792</td>
</tr>
<tr>
<td></td>
<td>X860</td>
</tr>
<tr>
<td></td>
<td>X862</td>
</tr>
<tr>
<td></td>
<td>X864</td>
</tr>
<tr>
<td></td>
<td>X925</td>
</tr>
<tr>
<td></td>
<td>X925</td>
</tr>
</tbody>
</table>

March 2011
Version 2.3
Overview

Lexmark provides a wide range of printing and imaging devices to help businesses of all sizes drive greater productivity—from the small business with a handful of employees to the world's largest enterprises. To meet today's complex printing requirements, Lexmark equips its devices with non-volatile memory to store essential system information when the devices are powered off. In addition, some Lexmark devices may also be equipped with a hard disk. The hard disk is used to buffer jobs, collate large jobs, or store forms, fonts or macros. To run some print apps or printer software solutions, a hard disk is required.

The use of non-volatile memory and hard disks are industry-standard methods for enhancing the performance of print and imaging devices. This document outlines how these memory types are implemented in Lexmark devices and the mechanisms that can be utilized to protect data stored on them.

About Non-Volatile Memory Technology on Lexmark Printers and MFPs

Lexmark devices use two forms of non-volatile memory: EEPROM and NAND. These components store the device operating system, device settings information, network information, embedded solution applications, various scanner settings and bookmark settings. No user-related print, copy and/or scan data is stored in non-volatile memory.

About Hard Disk Technology on Lexmark Printers and MFPs

Hard disks on Lexmark devices are designed for device-specific functionality and are not designed, nor can be used, as long-term storage for items unrelated to print and scan. The basic architecture of these devices disallows the capability for users to extract information, create folders, share the hard disk, create a network file share, or FTP information to the device’s hard disk directly from a client device.

The device hard disk is primarily designed to store print/image data, font data, forms data, macros, and in some cases, job data. In addition, Lexmark uses hard disks for temporarily buffering scan, fax, and copy data. In general, print-related data is processed in Random Access Memory (RAM) unless the job exceeds the amount of RAM on the device, or if the end user selects the confidential print and/or print and hold feature enabled through the print driver.
Hard Disk Encryption

Why is Hard Disk Encryption needed?
A common concern for print devices is that residual job data from the print, copy, fax, and scan processes will not be properly cleared prior to the device being removed from a secure area and/or decommissioned at the end of life. This concern has led many customers to look for additional hard disk protection mechanisms outside of disk wiping to secure information. Hard disk encryption adds an additional layer of security to a device's hard disk by encrypting all data that may be actively used by the device, sitting idle on a device, and/or used by the device in a previous job. Disk encryption provides the comfort that the hard disk can never be used in a device other than the one from which it was originally encrypted.

How does Hard Disk Encryption work?
Lexmark devices have the ability to encrypt all data on their hard disks to protect it from malicious access at all times. When this feature is enabled, all data written to the hard disk is encrypted. This protects not only residual data left over after jobs, but also protects data actively being used. This prohibits someone from maliciously powering off the device in the middle of a job and making use of data abruptly left on the hard disk. If an encrypted hard disk is removed and placed in another Lexmark device with hard disk encryption enabled, the hard disk will verify its encryption key with the device’s encryption key. If the verified encryption key on the hard disk is different from the device's encryption key, the device will reformat the hard disk with a new encryption key, destroying the existing encrypted data on the hard disk.

When hard disk encryption is activated, the encryption key used (256-bit AES symmetric encryption) is pseudo-randomly generated and stored in a proprietary fashion on the device. Note that the key is not stored on the hard disk itself, so if the hard disk were stolen from the device, the contents of the hard disk would remain indecipherable.

When the encryption function is activated, the hard disk is formatted and all data contained on the hard disk is lost. Encryption is then applied to all data placed on the hard disk, at all times.

Benefits of Hard Disk Encryption
- Increased security of active and residual data.
- The encryption is applied in real time, so there is no delay for cleanup or post-processing after jobs have completed.
- A dynamically generated encryption key stored on the device (not the hard disk) makes the data on an encrypted disk useless on any other device. Stealing the hard disk out of the device will not yield access to the data it contains.

How to Enable Hard Disk Encryption
The Disk Encryption menu can only be accessed by entering the Config Menu at the Lexmark device control panel.
Power off the device.

1. If your device has a touch screen, hold down the 2 and the 6 buttons, while powering on the device; hold the buttons down until a clock or bar indicator appears. If your device has a four line LCD display, hold down the check mark (✓) and the right arrow (►), while powering on the device; hold the buttons down until a clock or bar indicator appears. Once the clock or bar indicator appears, then you may release the buttons.
2. You should see the Config Menu appear on the device control panel.
3. To locate the Disk Encryption feature, press the down arrow until you see a feature that displays Disk Encryption. Select this feature.
4. The screen should change to a page that displays the header Disk Encryption.
5. The screen should only display two functions named Enable and Disable. If you would like to enable disk encryption, select the Enable function. If you already have disk encryption enabled and would like to disable the feature, select the Disable function. Please note either function will erase the contents of the disk.
6. After the appropriate feature has been selected, the screen should change to a confirmation page that displays the following prompt: Contents will be lost. Continue? The screen should also display two buttons with YES and NO. If you want to continue with the disk encryption, select the YES button and the disk encryption process will start. If you decide not to continue, press the NO button and you will be placed back to the previous screen.
7. When the process finishes, select the Back button.
8. Select the Exit Config Menu button and the device will return to a ready state.

The following graphic will appear when the encryption process is enabled:
The progress bar indicates the overall completion of the entire process by filling in throughout each separate stage.

The entire process is complete when the progress bar appears completely shaded and the percentage indicator shows 100%. After completion, the panel returns to the Disk Encryption menu.
Confirmation of Disk Encryption Activities
There are two ways to confirm that disk encryption has been enabled on the device:

1. You can review the Menu Settings Pages or launch the device’s embedded web server and follow these steps: Launch the EWS->Select Reports->Select Device Settings->Scroll down to Other Settings and look for the Disk Encryption entry.

Below is an illustration of the device Settings link on the EWS, showing Disk Encryption is enabled:

2. The second method to confirm that disk encryption has been enabled is via MarkVision Professional. A plug-in has been developed for MarkVision that will allow you to view the status of disk encryption on a fleet of devices.

Note: If you remove an encrypted disk from a device and then try to install another disk, the following message will appear on the device LCD: **Disk Corrupted. Reformat?** You can then format the newly installed disk or remove it from the device. If you choose to reformat the disk, the device will generate a new encryption key, and encrypt and format the new hard disk. At this point, the data from the previous hard disk will no longer be accessible by any machine.
Hard Disk Wiping

Why is Hard Disk Wiping Important?
Lexmark uses hard disks on our devices to temporarily buffer scan, fax, print, and copy data that exceeds the amount of Random Access Memory (RAM) installed on the device. Buffered data is deleted from the hard disk immediately after the original scan, fax, print, or copy job is complete. Additionally, devices will temporarily hold print jobs on a hard disk if the confidential print/print and hold features are enabled by the user and when fax jobs are received and sent. This data is held by the hard disk until the job is deleted by the end user, the document expires through the job expiration feature, or the document is printed by the end user.

When a data file is “deleted” from a hard disk, the data that is associated with that file is not actually deleted. This data remains on the hard disk and with substantial efforts, theoretically could be recovered. Lexmark devices support a mechanism for protecting residual data: hard disk wiping. Hard disk wiping actively overwrites the deleted job data with multiple passes of random data, removing all residue of prior information.

Intended Goals of a Hard Disk Wiping Solution
• Provide an advanced secure deletion solution.
• Reduce the user intervention required in the process to complete a disk wipe and still maintain a high level of security.
• Provide configuration options to suit individual user requirements.
• Ensure the disk wiping feature is efficient.

Benefits of Hard Disk Wiping
• The benefits of a hard disk wiping solution include:
  • Increased security of residual data.
  • Elimination of the need to remove or process the hard disk when the device is to be retired, recycled, or otherwise removed from a customer’s secure environment.

Disk Wiping Methods
The disk wiping menus are included in this document to outline the functions, capabilities, and flexibility of the disk wiping methods.

<table>
<thead>
<tr>
<th>Menu Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automatic Method</strong></td>
<td>Disk Wiping erases only job data from the device hard disk that is not currently in use by the file system. All permanent data on the device hard disk is preserved, such as downloaded fonts, macros and held jobs.</td>
</tr>
<tr>
<td>Off (default)</td>
<td></td>
</tr>
<tr>
<td>On</td>
<td></td>
</tr>
<tr>
<td>Single Pass (default)</td>
<td></td>
</tr>
<tr>
<td>Multiple Pass</td>
<td>Automatic Wiping marks all disk space used by a previous job and does not permit the file system to reuse this space until it has been sanitized. Only Automatic Wiping enables users to</td>
</tr>
</tbody>
</table>
activate disk wiping without having to take the device offline for an extended amount of time.

Notes:
• This menu item appears only if a formatted, non-defective device hard disk is installed.
• Off and Single Pass are the default settings.
• Highly confidential information should be wiped using the Multiple Pass method only.
• Due to the large amount of resources required for Automatic Wiping, activating this option may decrease device performance, especially if the device requires hard disk space faster than it can be wiped and returned to service.

### Scheduled Method

<table>
<thead>
<tr>
<th>Single pass (default)</th>
<th>Disk Wiping erases only job data from the device hard disk that is not currently in use by the file system. All permanent data on the device hard disk is preserved, such as downloaded fonts, macros and held jobs. Both the Manual Method and the Scheduled Method allow the file system to reuse marked disk space without first having to wipe it.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple pass</td>
<td></td>
</tr>
</tbody>
</table>

Notes:
• This menu item appears only if a formatted, non-defective device hard disk is installed.
• Single pass is the default setting.
• Highly confidential information should be wiped using the Multiple Pass method only.
• Scheduled wipes are initiated without displaying a user warning or confirmation message.

### Manual Method

<table>
<thead>
<tr>
<th>Do Not Start Now (default)</th>
<th>Disk Wiping erases only job data from the device hard disk that is not currently in use by the file system. All permanent data on the device hard disk is preserved, such as downloaded fonts, macros and held jobs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Now</td>
<td></td>
</tr>
<tr>
<td>Single pass (default)</td>
<td>Manual Wiping overwrites all disk space that has been used to hold data from a print job that has been processed (i.e. printed). This type of wipe does not erase any information related to an unprocessed print job.</td>
</tr>
<tr>
<td>Multiple pass</td>
<td></td>
</tr>
</tbody>
</table>

Both the Manual Method and the Scheduled Method allow the file system to reuse marked disk space without first having to wipe it.
**Notes:**
- This menu item appears only if a formatted, non-defective device hard disk is installed.
- "Do Not Start Now" and Single Pass are the default settings.
- Highly confidential information should be wiped using the Multiple Pass method only.
- If the Disk Wiping access control is activated, then a user must successfully authenticate and have the required authorization in order to initiate the disk wipe.

**How to Enable Disk Wiping**
The disk wiping menu can only be accessed from the device’s Embedded Web Server or the device’s control panel.

The device control panel is either the four-line LCD display as shown in the photo below on the left, or a touch screen as shown on the right.

Below is an illustration of the disk wiping menu located on the Embedded Web Server:
Automatic Method

1. **To enable using the Embedded Web Server:** Locate the IP address of the device (Menus > Reports > Network Setup Page) and type it into your Web browser. This will bring up the device’s embedded Web page. Next, select Settings > Security > Disk Wiping, and then change the Wiping Mode to Auto and select Submit.

2. **To enable from the device control panel:** While standing at the device, perform the following tasks using the device control panel. Select Menus > Security > Disk Wiping, and then change the Wiping Mode to Auto and select Submit.

Scheduled Method

1. **To enable using the Embedded Web Server:** Locate the IP address of the device (Menus > Reports > Network Setup Page) and type it into your Web browser. This will bring up the device’s embedded Web page. Next, select Settings > Security > Disk Wiping, and then change the Wiping Mode to Manual and select Submit.

   Once the page refreshes, select Disk Wiping and click on the Scheduled Disk Wiping link (shown in blue on the picture below), then add your entry(s) and select Submit.

2. **To enable from the control panel:** While standing at the device, perform the following tasks using the device control panel. Select Menus > Security > Disk Wiping, and then change the Wiping Mode to Manual and select Submit.

   Once the page refreshes, select Disk Wiping > Schedule Disk Wiping, then add your entry(s) and select Submit.

**Notes:**
A device can be set for an Automatic disk wipe or a Scheduled disk wipe, but it cannot be set for both at the same time.

On single-function devices, certain configuration options may be limited at the device control panel because of usability, such as configuring a schedule entry.
Manual Method

1. **To enable using the Embedded Web Server:** Locate the IP address of the device (Menus > Reports > Network Setup Page) and type it into your Web browser. This will bring up the device’s embedded Web page. Next, select Settings > Security > Disk Wiping, and then change the Wiping Mode to Manual and select Submit.

   To initiate the manual disk wiping process, you will need to perform this task while at the device control panel. Select Menus > Security > Disk Wiping > Manual Wiping and then click Start.

2. **To enable from the control panel:** While standing at the device, perform the following tasks using the device control panel. Select Menus > Security > Disk Wiping, and then change the Wiping Mode to Manual and select Submit.

   To initiate the manual disk wiping process, you will need to perform this task while at the device control panel. Select Menus > Security > Disk Wiping > Manual Wiping and then click Start.

Single Pass Disk Wipe or Multi Pass Disk Wipe

Each disk wiping method (Automatic, Scheduled or Manual) can perform either a Single Pass or Multi Pass wipe. The Single Pass wipe is a simple zeroing of the data, whereas the Multi Pass wipe is currently defined to meet NIST/DOD/DOE standards.

To Confirm Disk Wipe Activities

To confirm that an automatic or scheduled disk wipe is functioning, check the device Audit Log for disk wipe entries, as shown in this example:

```
<37>Mar  3 17:00:31 ET0021B700BAB9 lxkwiped: 80,2009-03-03T17:00:31.5,"lxkwiped",,,,-1,-1,,0xFFFFFFFF,,"Disk Wipe Initiated","0.02Mb to be wiped"
<37>Mar  3 17:00:31 ET0021B700BAB9 lxkwiped: 81,2009-03-03T17:00:31.5,"lxkwiped",,,,-1,-1,,0xFFFFFFFF,,"Manual/Scheduled Wipe Completed",
```

Meeting DOD/DOE/NIST Guidelines for Magnetic Media Sanitization

The U.S. Department of Defense clearing and sanitizing matrix (DoD 5220.22-M, Section 8-306, Maintenance) recommends that the sanitization of a magnetic removable rigid disk should be done by one of the following:

- Overwrite all addressable locations with a character, its complement, then a random character and verify.
- Degauss with a Type I degausser.
- Degauss with a Type II degausser.
- Destroy – disintegrate, incinerate, pulverize, shred or melt.

A Multi Pass wipe using either the Automatic, Schedule or Manual Methods is currently defined to meet NIST/DOD/DOE standards.
Securing the Memory Before Moving or Decommissioning Lexmark Printers and MFPs

There are several circumstances under which Lexmark recommends you erase the contents of the memory components installed in your Lexmark printer or MFP. These include:

- The printer is being decommissioned
- The printer hard disk is being replaced
- The printer is being moved to a different department or location
- The printer is being serviced by someone from outside your organization
- The printer is being removed from your premises for service

The following sections explain the recommended steps to ensure confidential data is erased.

How to Perform a Complete or Out of Service Disk Wipe (Wipe Disk Feature)
The Wipe Disk feature is accessed via the device Config Menu and is different from the disk wiping functionality previously described in this document. The Wipe Disk feature provides you with a tool for erasing all contents of a disk. Two options are available: Wipe Disk (Fast) and Wipe Disk (Secure). Wipe Disk (Secure) initiates a three-pass overwrite that can take up to nine hours to complete depending on the device.

Steps to Enable the Wipe Disk Feature
The Wipe Disk menu can only be accessed by entering the Config Menu at the Lexmark device control panel.

Warning: Wipe Disk removes a disk's data in such a way that it cannot be recovered.

1. Power off the device.
2. If your device has a touch screen, hold down the 2 and the 6 buttons, while powering on the device. Hold the buttons down until a clock or bar indicator appears. If your device has a four-line LCD display, hold down the check mark (✓) and the right arrow (>), while powering on the device. Hold the buttons down until a clock or bar indicator appears. Once the clock or bar indicator appears, then you may release the buttons.
3. You should see the Config Menu appear on the device control panel.
4. To locate the Wipe Disk feature, press the down arrow until you see a feature that displays Disk Wipe. Select this feature.
5. The screen should change to a page that displays the header Wipe Disk. The screen should only display two functions named Wipe Disk (Fast) and Wipe Disk (Secure). Select the feature that you would like to enable.
6. After the appropriate feature has been selected, the screen should change to a confirmation page that displays the following prompt: Contents will be lost. Continue? or The Wipe Disk (Secure) operation takes many hours and content will be lost. The confirmation screen will allow you to continue or cancel the wipe disk operation.
7. When the process finishes, select the Back button.
8. Select the Exit Config Menu button and the device will return to a ready state.

How to Perform a Complete Settings Wipe (Wipe All Settings Feature)
The Wipe All Settings feature provides you with a tool for erasing all contents stored on the various forms of non-volatile memory contained on the device. The Wipe All Settings feature is accessed via the device Config Menu and is different from the disk wiping functionality and the Wipe Disk feature previously described in this document. The Wipe All Settings feature is a complete clearing of all settings, solutions, jobs and faxes on the device.

Steps to Enable the Wipe All Settings Feature
The Wipe All Settings menu can only be accessed by entering the Config Menu at the Lexmark device control panel.

Warning: Wipe All Settings removes device settings, solution, job, and fax data in such a way that it cannot be recovered.

1. Power off the device.
2. If your device has a touch screen, hold down the 2 and the 6 buttons, while powering on the device. Hold the buttons down until a clock or bar indicator appears. If your device has a four-line LCD display, hold down the check mark (✓) and the right arrow (>), while powering on the device. Hold the buttons down until a clock or bar indicator appears. Once the clock or bar indicator appears, then you may release the buttons.
3. You should see the Config Menu appear on the device control panel.
4. To locate the Wipe All Settings feature, press the down arrow until you see a feature that displays Wipe All Settings. Select this feature.
5. The screen should change to a page that displays a warning message. Warning: This will clear all settings, solutions, jobs, and faxes on this device. The device will reboot during this process. The bottom of the screen should only display buttons Yes and No. Select the Yes button to continue with the Wipe All Settings and continue to step 6 or No button to cancel out of this menu.
6. The device will begin clearing all settings on the device and during the process it will reboot several times.
7. When the process finishes, select the Back button.
8. Select the Exit Config Menu button and the device will return to a ready state.
Summary

Lexmark printers and multifunction devices are equipped with non-volatile memory. In addition, some devices are equipped with internal hard disks. These devices have a number of standard and advanced security mechanisms to enhance the security of data that is stored on or passes through them, including:

- **Hard disk encryption** using the Advanced Encryption Standard (AES), which provides the following protections:
  - 256-bit AES.
  - When encryption is activated, the encryption key is pseudo-randomly generated and stored on the device.
  - Encryption applies not only to residual data left over after jobs, but also to data that is actively being used.

- **Disk wiping** ensures that any residual data on the hard disk cannot be recovered if the encryption key is compromised.
  - Automatic disk wiping: This method wipes residual data immediately following the completion of a print, copy, fax, or scan job.
  - Scheduled disk wiping: A wipe that is set up by a device administrator to be conducted at specific time(s) and date(s).
  - Manual disk wiping: A manually activated process that wipes all residual data from the device when invoked from the device’s operator panel.
  - Complete or Out of Service disk wiping: This feature is designed to completely wipe the entire contents (active and residual data) of the hard disk. It is highly recommended if the device is being taken out of service or removed from a secure location.

The wiping methods mentioned above provide two levels of disk wiping: fast and secure.
  - A fast disk wipe is a single overwrite pass with a random bit pattern.
  - A secure disk wipe uses three overwrite passes with different bit patterns followed by a verify pass; this is otherwise known as a NIST or U.S. Department of Defense compliant wipe.

- **Wipe All Settings** provides you with a tool for erasing all contents stored on the various forms of non-volatile memory contained on the device.
  - Removes device settings, solution, job, and fax data in such a way that it cannot be recovered.
  - Recommended when the Lexmark device is to be retired, recycled, or otherwise removed from a secure environment.