Technical Note

Running Secure Erase on Micron SSDs

Introduction

This document describes how to run the ATA SECURITY ERASE command on Micron SATA solid state drives (SSDs) using the Linux utility Parted Magic. The utility is available for download at http://www.partedmagic.com.

Micron recommends but does not endorse Parted Magic as a utility that properly executes the ATA SECURITY ERASE command on SATA-based Micron SSDs. If secure erase is implemented improperly, potential issues with data security in some devices may occur. Make sure to follow the instructions described in this document.

Secure Erase Overview

The terms *secure erase* and *security erase* are often used interchangeably.

Secure erase is a term describing the operation of completely and irretrievably deleting user data from a storage device. It is often needed when all data on a storage device must be removed for reasons of privacy, confidentiality, and security.

Security erase is a term referring to the specific command or group of commands from the Advanced Technology Attachment (ATA) command set, also known as the ACS.

Executing an ATA SECURITY ERASE command using Parted Magic as described in this document deletes all user and host computer data from a Micron SATA SSD. The operation removes all partition and file system information, returning the entire user space to its erased state making it ready to accept new data.

Note: The ATA SECURITY ERASE command not only deletes data but also returns an SSD to its fresh-out-of-box (FOB) performance state. This can be useful when running performance and benchmark tests. See Micron's Differences in Personal vs. Enterprise SSD Performance technical marketing brief for more information. Writing all zeros or any data pattern across an entire SSD is not a proper or secure method of erasing data from an SSD. The ATA SECURITY ERASE command should be used for this purpose.

Secure Erase Operation

Before You Begin

Download and install Parted Magic on your system.

- Run the Parted Magic utility from a bootable CD or bootable USB drive as described in the utility's documentation.
- Select the boot time option to run the software from DRAM to enable access to all drives on SATA connection in the system.

Running the ATA SECURITY ERASE Command

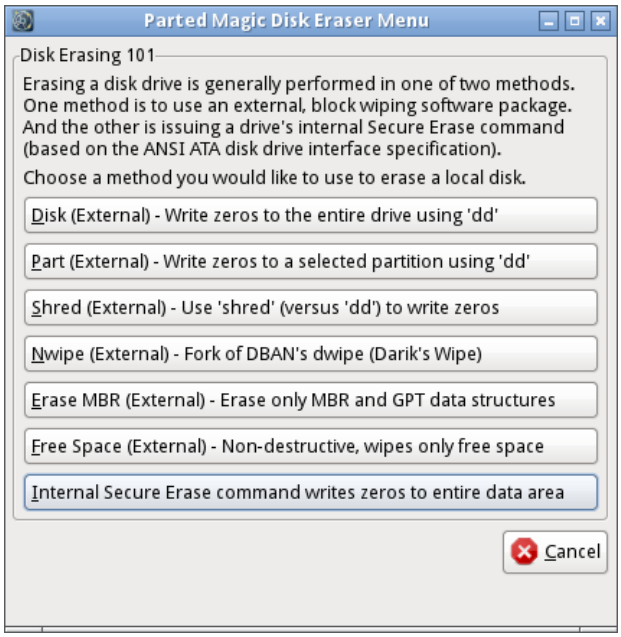
Parted Magic includes several utilities. **Erase Disk** is the utility to perform the ATA SECURITY ERASE command on Micron SSDs.

1. Double-click the **Erase Disk** icon, as shown in Figure 1.

Figure 1: Parted Magic Utility—Erase Disk

2. When prompted for a secure erase method, select **Internal Secure Erase command writes zeros to entire data area**, as shown in Figure 2.

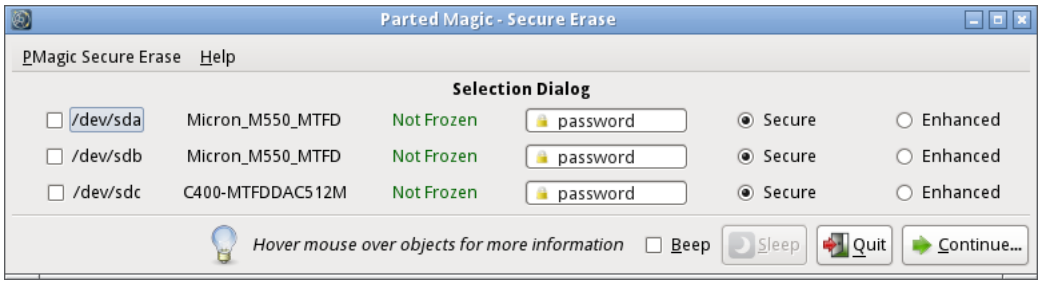
Figure 2: Secure Erase Method



This method issues the ATA SECURITY ERASE command and enables the target SSD to execute the command per the drive's design. Micron SATA SSDs are designed to send the BLOCK ERASE command to each NAND component.

3. When the Selection Dialog appears (Figure 3), select the SSD(s) to be erased.

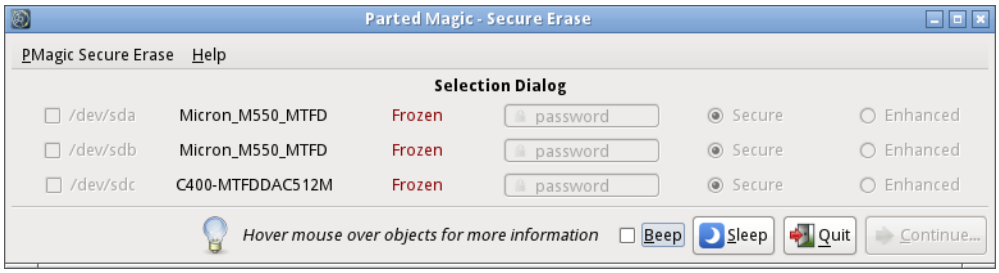
Figure 3: Selection Dialog



4. Click **Continue**.

If the selected SSD(s) appear with a "Frozen" state (as shown in Figure 4), unfreeze the drive(s) by placing the computer in sleep mode and then performing a restart.

Figure 4: Selection Dialog—SSDs in Frozen State

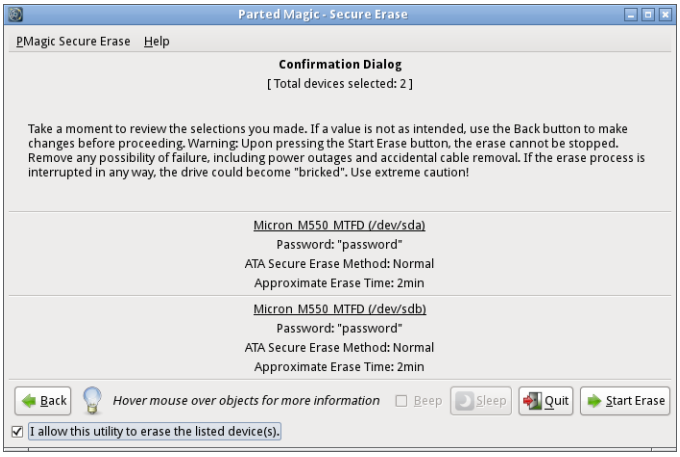


To place the computer in sleep mode, click the **Sleep** button on the Selection Dialog. After the computer enters sleep mode, press the power button to wake the computer.

When the operating system starts, restart the secure erase procedure from the beginning (step 1). The drives should appear in the "Not Frozen" state, enabling the secure erase command to be issued.

5. Confirm the SSDs you want to erase appear in the Confirmation Dialog (similar to Figure 5).

Figure 5: Confirmation Dialog—Start Erase



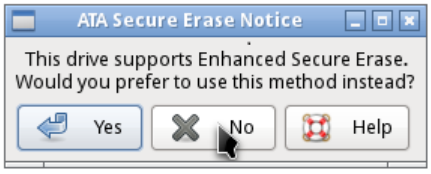
6. Click **Start Erase**.

Note: If supported by the SSD, the utility will prompt you to select the enhanced secure erase method.

On Micron M500, M510, and M550 SSDs, selecting the enhanced method will execute a cryptographic erase. This operation replaces the SSD's 256-bit encryption key, but will not actually erase any data. This effectively makes all user and operating system data unreadable because the data cannot be decrypted using the new encryption key. This method does not return the SSD to its FOB performance state.

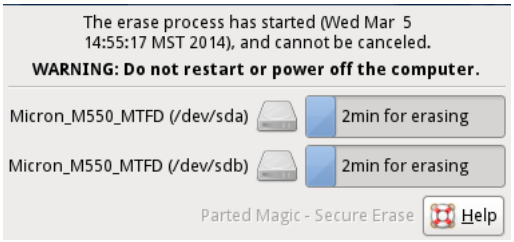
Select **Yes** or **No** to run enhanced secure erase, as shown in Figure 6.

Figure 6: Enhanced Secure Erase



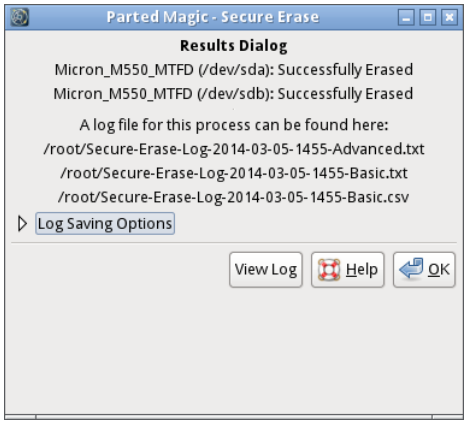
7. The secure erase operation starts. A status bar appears showing the progress of the operation (Figure 7). On Micron SSDs, the secure erase operation typically takes less than two minutes to complete.

Figure 7: Secure Erase Progress



8. The operation is finished when the Results Dialog appears (Figure 8).

Figure 8: Secure Erase Complete



9. Click **OK** to exit the utility and return to the desktop.

Revision History

Rev. A – 7/14

- Initial release

8000 S. Federal Way, P.O. Box 6, Boise, ID 83707-0006, Tel: 208-368-4000
www.micron.com/products/support Sales inquiries: 800-932-4992