Frequently Asked Questions

Should I defragment the SSDNow drive to maintain optimal performance?

SSDs do not require defragmentation. Since they do not contain a physical disk, there is no need to organise the data in order to reduce seek time. Therefore defragmenting an SSD is not effective. Also, defragmenting an SSD can put undue wear on specific areas of the drive. SSDs are designed to write data as evenly as possible over the entire drive to reduce undue wear to any one location. Defragmenting your SSD drive a couple of times will not harm it. However, if it is done continuously over a long period, it may reduce the life of the drive.

Why didn't my primary HDD transfer rate score in the Windows Experience

Index (WEI) go up after installing the new SSDNow drive?The Windows Experience Index (WEI) merely measures the relative capability of components. The WEI only runs for a short time and does not measure the interactions of components under a software load, but rather characteristics or your hardware.

The WEI does not therefore measure the performance of a system, but merely the relative hardware capabilities when running Windows 7. An article about the WEI can be found here: http://blogs.msdn.com/b/e7/archive/2009/01/19/engineering-the-windows-7-windows-experience-index.aspx

In Vista, the WEI scores ranged from 1.0 to 5.9. In Windows 7, the range has been extended upward to 7.9.

What is SMART and do the SSDNow drives support it?

Self-Monitoring Analysis and Reporting Technology (SMART) is a built-in monitoring capability in hard drives and SSDs. It can allow users to monitor the health of a device. It does this through monitoring software designed specifically for the SMART feature. All of our SSDNow drives support SMART.

Will the SSD experience a performance decrease? If so, is there a way to reset the drive to a factory default?

Performance decreases have been reported on some SSDNow drives. If you have an older SSD drive that does not have effective Garbage Collection, SSD drive performance will decrease over time. This is due to the way the system overwrites data that has been flagged for deletion.

Try using the Secure Erasetool like HDDErase to wipe the drive and restore it to its original condition.

What are TRIM and garbage collection?

Trim and garbage collection are technologies that modern SSDs incorporate to improve both their performance and endurance. When your SSD is fresh out of the box, all of the NAND blocks are empty so the SSD can write new data to the empty blocks in a single operation. Over time, most of the empty blocks will become used blocks that contain user data. In order to write new data to used blocks, the SSD is forced to perform a read-modify-write cycle. The read-modify-write cycle hurts the SSD's overall performance because it must now do three operations instead of a single operation. The read-modify-write cycle also causes write amplification, which hurts the SSD's overall endurance.

Trim and garbage collection can work together to improve SSD performance and endurance by freeing up used blocks. Garbage collection is a function built into the SSD controller that consolidates data stored in used blocks in order to free up more empty blocks. This process happens in the background and is completely handled by the SSD itself. However, the SSD may not know which blocks contain user data and which blocks contain stale data that the user has already deleted. This is where the trim function comes in. Trim allows the operating system to inform the SSD that data has been deleted so that the SSD can free up those previously used blocks. For trim to work, both the operating system and the SSD must support it. Most modern operating systems and SSDs support trim, although most RAID configurations do not.

Kingston SSDs take advantage of both garbage collection and trim technologies in order to maintain the highest possible performance and endurance over their lifetime.

When I connect my SSD as a secondary drive, it is seen as new hardware

but I cannot see it as a usable drive. How can I resolve this?

Open the Control Panel, open Administrative Tools and then open Computer Management. Click on Disk Management and see if the SSD drive is shown in the right window pane. If it is, right-click on where it is labelled as disk 1, disk 2, etc. and select "Initialize disk" (this may come up automatically when you go into Disk Management).

In XP, right click on the area to the right of that and choose "New Partition". Then choose "Primary Partition" in the partition wizard. Continue with the wizard by choosing the size, drive letter and formatting of the partition.

In Windows Vista and 7, right click on the area to the right of the disk label and choose "New Simple Volume". Continue with the wizard by choosing the size, drive letter and formatting of the partition.

In MacOS, a "disk insertion" window will appear. Click on the "Initialize" button. This will take you to the disk utility. Select the Kingston drive from the list of drives on the left side of the window. From the actions available, choose Partition. For the "Volume Scheme", choose "1 partition". For the format, choose MacOS extended for a permanent drive. Choose ExFAT for an external drive (available on MacOS 10.6.6 and above). Click Apply. A warning window will

appear stating that you will erase all data from the drive. Click on the partition button at the bottom.

Is my data safe when I send my SSD back to Kingston for warranty replacement/repair?

Kingston realises the importance of keeping our customers' personal data and information confidential and secure. Kingston takes measures to ensure the security of all of our customers' personal information when a Solid State Drive (SSD) is returned to our RMA facility for warranty replacement or repair. When an SSD reaches our repair centre, it will undergo a thorough testing process. During the first phase of testing, an ATA Secure Erase is performed on the SSD, which erases all data and information. ATA Secure Erase is federally approved by the National Institute of Standards and Technology (NIST 800-88) for legal sanitisation of confidential user data. If the SSD is not in a functional state and not capable of undergoing an ATA Secure Erase, the SSD is dismantled and the NAND Flash Memory is destroyed.

Can I use two or more SSD drives in a RAID?

Any of our SSDs can be used in RAID. However, due to endurance specifications, only certain part numbers should be used in RAID. For servers, please contact Kingston to determine the best Kingston SSD to use for your workload.

How do I verify the TRIM command is enabled in Windows 7?

First, open an Elevated Command Prompt window.

To open an Elevated Command Prompt window: Click on Start Orb > Type "CMD.exe" in Search box > Right click on "CMD" and select "Run as Administrator" (If you receive a prompt confirmation, click YES)

To verify that the TRIM command is enabled, type the following and press enter in the Elevated command:

fsutil behavior query disabledeletenotify

The results will be as follows: DisableDeleteNotify = 1 (Windows TRIM commands are disabled) DisableDeleteNotify = 0 (Windows TRIM commands are enabled)

To enable the TRIM command,type the following and press enter in the Elevated command:

fsutil behavior set disabledeletenotify 0

To disable the TRIM command,type the following and press enter in the Elevated command:

fsutil behavior set disabledeletenotify 1

My new SSD is not being seen by the BIOS in my 2008 or older computer.

My older SATA drive is seen in the same port. Why?

Our SATA III (6Gbit/s) SSDs are tested to be backwards compatible to SATA II (3Gbit/s). They are not designed or tested to be backwards compatible with SATA I ports (1.5Gbit/s). Most systems made before 2008 used SATA I ports. Our SSDs will likely not work in these systems.

When I try to install Windows 7 from my installation disk, it will not detect the new SSD. However, the drive is seen in the BIOS. How do I resolve this?

When the SSD is recognised in the BIOS, but the Windows 7 installation does not detect the drive:
Follow these steps:

Disconnect any other hard drives or SSDs. Boot the Windows 7 installation disk. Choose repair, then advanced, then command prompt. Type: "diskpart" without quotes and press Enter. You will see a prompt labeled "diskpart". Type the following commands and press Enter after each one.

Diskpart > Select Disk 0
Diskpart > Clean
Diskpart > Create Partition Primary Align=1024
Diskpart > Format Quick FS=NTFS
Diskpart > List Partition
Diskpart > Active
Diskpart > Exit

Then, reboot the computer to the Windows 7 installation disk.

What is ESD?

ElectroStatic Discharge, ESD is simply the discharge of built-up static electricity. ESD should not be taken lightly as this is one of the few things that an individual can do to damage or destroy their computer or hardware components. It is like when you rub your feet on the carpet and you touch something metal. ESD can occur without the user feeling a shock and will occur when only working on the inside of the computer or handling hardware.

How to help prevent ESD
The best method of preventing ESD is to use an ESD wrist strap or an earthing mat or table. However, because most users do not have access to these items, we have included the below steps to help reduce the chance of ESD as much as possible.

- Standing – We recommend that you are standing at all times when working on the computer. Sitting on a chair can generate more electrostatic.
- Cables – Make sure that everything is removed from the back of the computer (power cable, mouse, keyboard, etc).
- Clothes – Do not wear any clothing that conducts a lot of Electrical Charge, such as a wool jumper.
- Accessories – To help reduce ESD and prevent other problems, it is also a good idea to remove all jewellery.
- Weather – Electrical storms can increase the ESD risk; unless absolutely necessary, try not to work on a computer during an electrical storm. In very dry areas, the air itself becomes a part of the electrostatic build-up mechanism every time there is an air flow (wind, air conditioning, blower) passing over an insulated surface. Do not let high humidity levels build false confidence, and beware of corrosion problems with interconnects and other electrical interfaces.

To learn more about ESD and how to protect your electronics, please refer to the below site.

ESD Association
http://www.esda.org/aboutESD.html

FAQ: KTC-Gen-ESD
During the OS installation, go to UTILITIES / TERMINAL

In terminal type:

diskutil list

Then press RETURN. Scroll up to top and verify the Kingston SSD disk (i.e. disk0, disk1, etc).

Then type:

diskutil mountDISK disk0 (or whichever ddisk is the Kingston SSD).

Then press RETURN. It should show "mounted successfully".

Then type:

diskutil eraseDISK apfs YOURDRIVENAME disk0 (or whichever disk is the Kingston SSD)

Warning – This step (eraseDISK command) will delete all data on the target drive. Confirm that you have selected the drive you wish to delete and then continue.

Then press RETURN. It should show "successful". Then exit terminal and proceed with the normal installation of the OS. FAQ: KSD-092917-GEN-21
Kingston SSD Manager (KSM) is ending support for Microsoft Windows 7. The latest version of KSM with Windows 7 support is v1.1.2.5. If you are using Windows 7 and experience

complications with KSM, please make sure you have AHCI mode enabled in BIOS and install the latest Intel RST storage driver provided by your system manufacturer. If you still need assistance, feel free to contact our Kingston Technical Support department. FAQ: KSM-001125-001-00
Kingston SSD Manager 1.1.2.6 will not offer firmware updates for NVMe SSDs until IEEE 1667 support has been disabled. In order to complete the firmware update you must do the following:

1. First, we recommend you backup your data.
2. Then use a secondary system to complete a REVERT using the PSID on the drive label. **Note: Performing a REVERT will securely erase all data on the drive.**
3. Disable IEEE 1667 support
4. The firmware update will become available upon refresh or restart of KSM FAQ: KSM-001125-001-01

Secure Erase User Guide for Linux
This guide will walk you through securely erasing your Kingston SSD using Linux tools

SATA Secure Erase Procedure

Warning
Please make sure to have a full backup of any important data before you proceed!

Prerequisites
• You must have root privileges.
• You must have your SSD connected to the system as a secondary (non-OS) drive.
• You must have lsscsi and hdparm installed. You may need to install them with your distribution's package manager.
• Your drive must not be in a security freeze.
• Your drive must not be password protected.

Instructions
1. Find the device name (/dev/sdX) of the drive you wish to erase:
lsscsi

2. Make sure drive security is not frozen:
hdparm -I /dev/sdX | grep frozen

If the output shows "frozen" (instead of "not frozen") then you cannot continue to the next step. You must try to remove the security freeze by trying one of the following methods:

Method 1: Put the system to sleep (suspend to RAM) and wake it up. On most distributions the command to suspend is:
systemctl suspend

Now issue the hdparm command again. If it worked the output will show "not frozen" (instead of "frozen").
Method 2: Hot plug the drive. This is done by physically unplugging the SATA power cable

from the drive and plugging it back in while the system is powered on. You may need to enable hot plug in BIOS. Not all systems support hot plug.

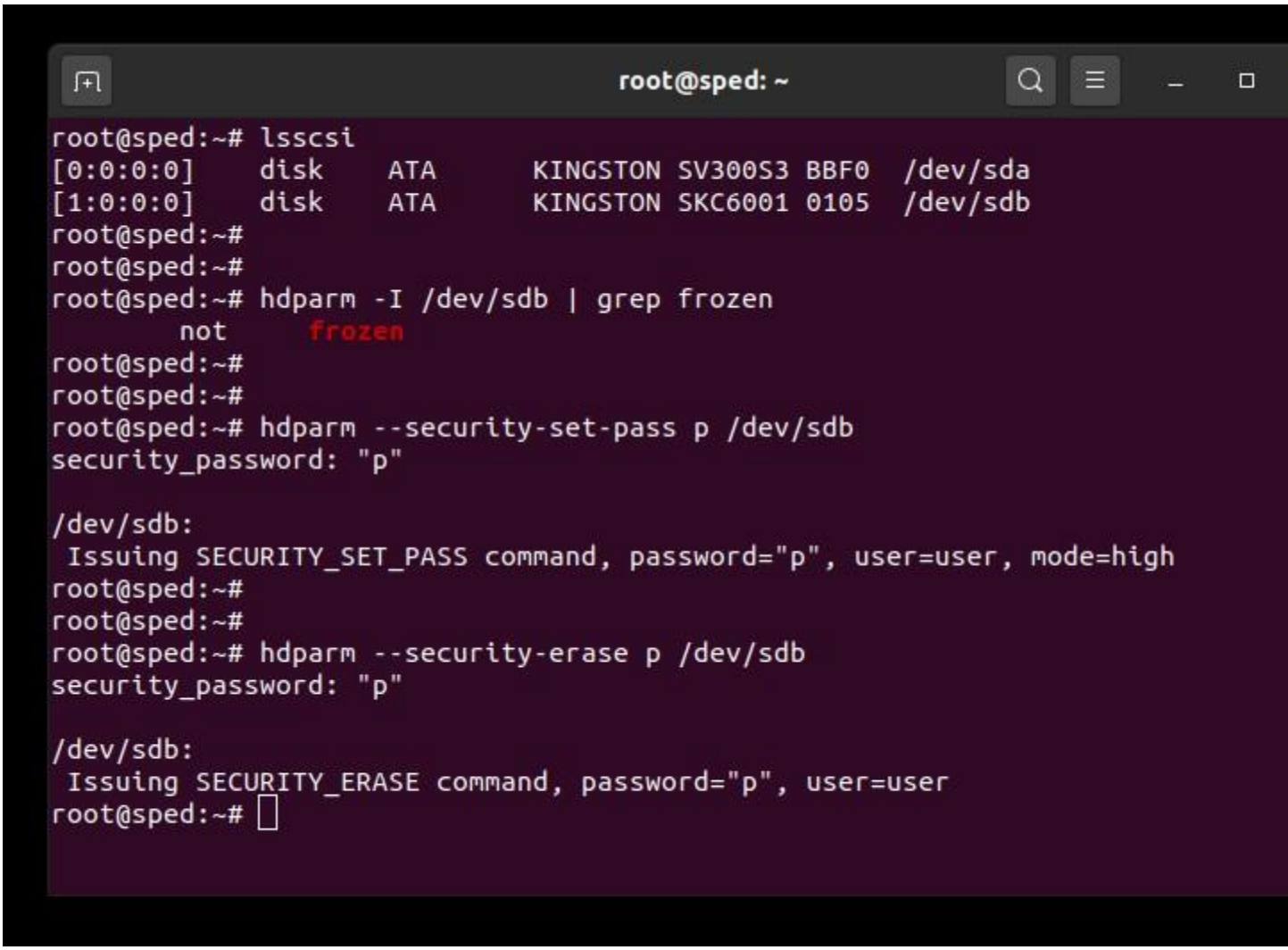
Now issue the hdparm command again. If it worked the output will show “not frozen” (instead of “frozen”).

3. Set a user password on the drive. The password can be anything. Here we are setting the password to “p”:
hdparm --security-set-pass p /dev/sdX

4. Issue the secure erase command to the drive using the same password:
hdparm --security-erase p /dev/sdX

This command may take a few minutes to complete. The drive password is removed upon successful completion.
If the secure erase is interrupted or otherwise fails your drive may become security locked. In this case you can remove the security lock using the command below and then try the secure erase procedure again:
hdparm --security-disable p /dev/sdX

SATA Secure Erase Example



NVMe Secure Erase Procedure

Warning
Please make sure to have a full backup of any important data before you proceed!

Prerequisites
• You must have root privileges.
• You must have your SSD connected to the system as a secondary (non-OS) drive.
• You must have nvme-cli installed. You may need to install it with your distribution's package manager.
• Your drive must not be password protected.

Instructions
1. Find the device name (/dev/nvmeXn1) of the drive you wish to erase:
nvme list

2. Issue the format command to the drive. Here we set the secure erase setting to 1 which indicates a user data erase:
nvme format /dev/nvmeXn1 --ses=1

This command may take a few minutes to complete.

NVMe Secure Erase Example