

Firmware Update Instructions for Crucial® Client SSDs

Overview

By using this guide, a user can perform a firmware update on Crucial® Client SSDs installed in a personal computing environment, referred to in this document as the host system. There are two methods to perform the update described in this guide, ranked in order of ease:

Method 1: Online update through Crucial® Storage Executive software (preferred)

When Storage Executive is running, it checks for firmware updates online and notifies the user if an update is available. The user can view the firmware change list and choose to perform the update within the Storage Executive user interface.

Method 2: Bootable ISO image provided by Crucial

Crucial provides a bootable ISO file that can perform the update without installing Storage Executive on the host machine. This method requires the user to load the provided image on a piece of bootable media such as a CD-R or USB flash drive. The user will then start the system with the bootable media to perform the update.

In each method, the final steps of the update are performed inside a secured boot environment on the host machine, which re-checks the applicability and integrity of the update materials before and during the download. Additionally, the update is performed on every applicable SSD in the host system.

It is highly recommended to use a stable power source and perform a full system backup prior to updating the firmware with any method. Although drive loss or corruption caused by an interrupted update is exceedingly rare, the update is performed at the user's own risk.

Update Method 1: Online update through Crucial® Storage Executive software (preferred)

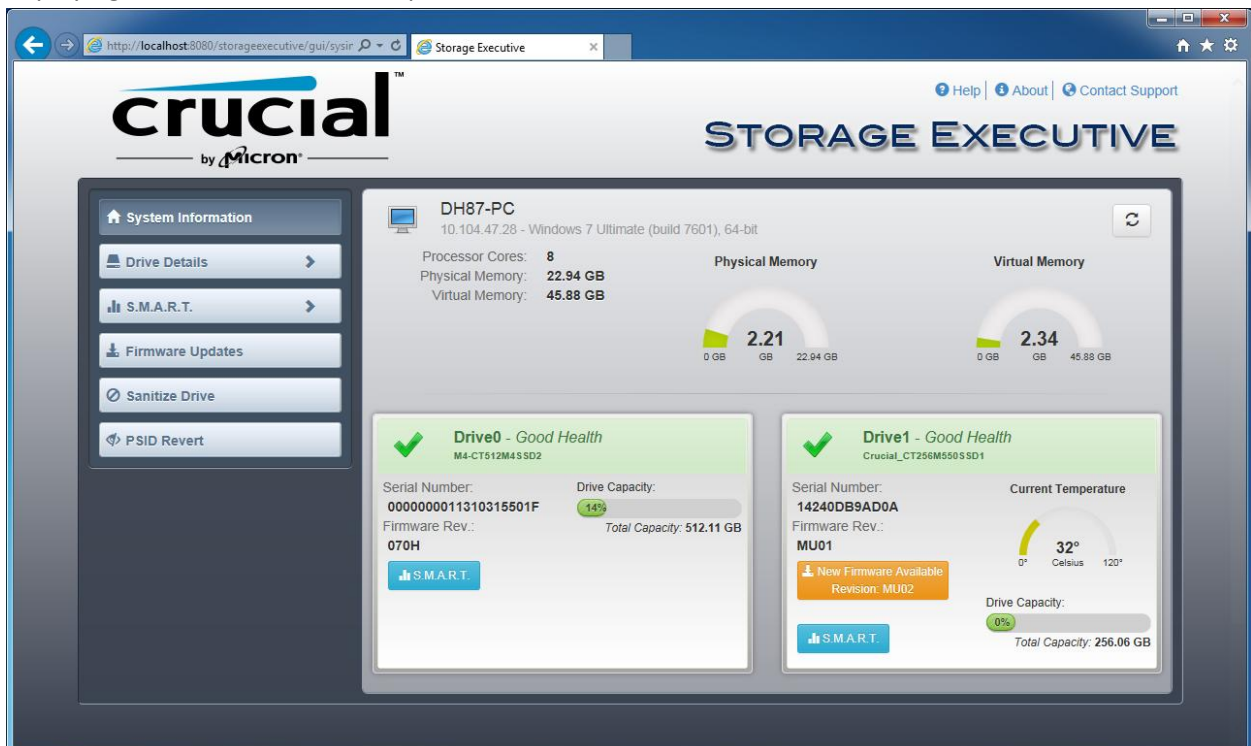
This method requires the Crucial Storage Executive to have been installed on the user's computer. More information on Storage Executive, a user's guide for the software, and a download link can be found at <http://www.crucial.com/usa/en/support-storage-executive>.

This method also requires the system to have access to the internet so the Storage Executive can connect to the Crucial server. If the host system is connected to the internet through a network proxy, Storage Executive may not be able to connect to the Crucial server, even though the user may have internet access.

Step 1: Start Storage Executive

- In Windows® 7 or a previous version, open the Start menu and click All Programs, click Storage Executive, then click Storage Executive Client
- In Windows 8, press the Windows logo key+S and the Search bar will appear. Type "Storage Executive Client" in the Search bar, then click on the Crucial Storage Executive app

When Storage Executive starts, the System Information screen appears in your default browser. Within the System Information window, the availability of firmware updates for each of the Crucial SSDs in the host system is displayed in the drive status boxes. An example of a System Information window displaying an available firmware update is shown below:



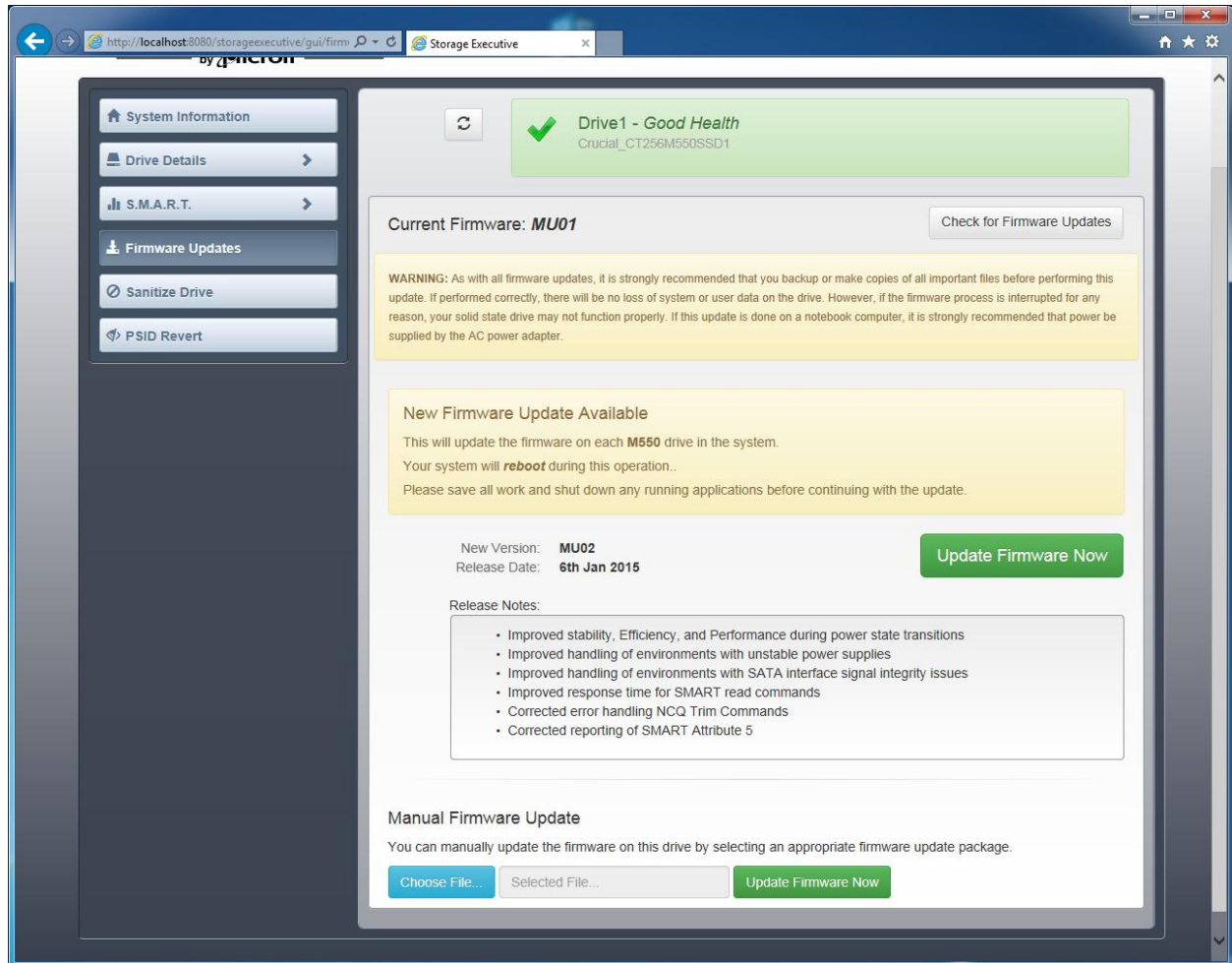
The screenshot displays the Crucial Storage Executive web interface in a browser window. The interface is titled "crucial by Micron STORAGE EXECUTIVE". On the left, there is a navigation menu with options: System Information, Drive Details, S.M.A.R.T., Firmware Updates, Sanitize Drive, and PSID Revert. The main content area shows system information for a PC named "DH87-PC" (10.104.47.28, Windows 7 Ultimate, 64-bit). It displays Processor Cores: 8, Physical Memory: 22.94 GB, and Virtual Memory: 45.88 GB. Two drive status boxes are shown:

- Drive0 - Good Health** (M4-CT512M4S SD2): Serial Number: 000000011310315501F, Firmware Rev.: 070H, Drive Capacity: 14% (512.11 GB Total Capacity). A "SMART" button is visible.
- Drive1 - Good Health** (Crucial_CT256M550S SD1): Serial Number: 14240DB9AD0A, Firmware Rev.: MU01, Current Temperature: 32° Celsius, Drive Capacity: 0% (256.06 GB Total Capacity). A "New Firmware Available" notification for Revision: MU02 is shown, along with a "SMART" button.

Step 2: Select the update to perform

This step can be performed by either clicking the orange update button for the drive in question, or by clicking on the Firmware Updates button on the left and selecting the drive to update.

Once performed, information regarding the update will be displayed on the screen, as shown in the example below:



Step 3: Perform the update

There are a few things to keep in mind before performing a firmware update:

- It is recommended to save files and close other programs before performing the update.
- The update will be performed on every compatible drive on the host system.
- The system will reboot into a Storage Executive environment when performing the update.
- After the update has finished, the system will automatically restart into the normal operating environment.

Information on the firmware version, the release date, and the release notes will be shown on the screen. After reviewing them, click Update Firmware Now.

Method 2: Bootable ISO image provided by Crucial

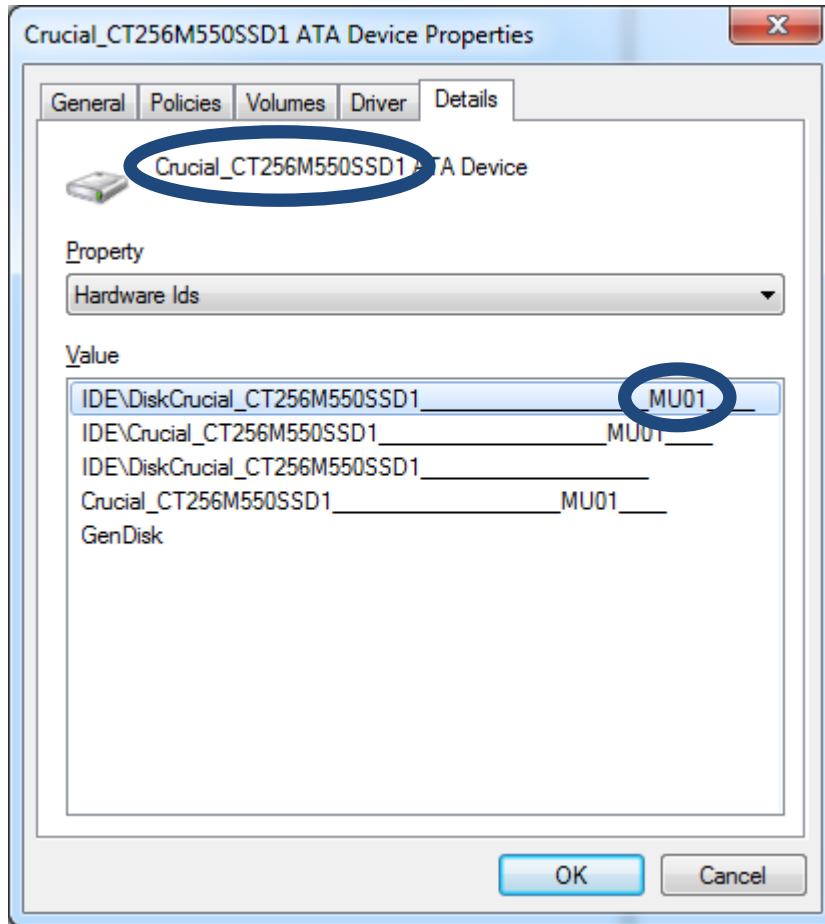
This method does not require installing Storage Executive, or a working internet connection on the host system to perform. However, it is more complicated and has a greater chance of user error than the first method. The process for determining applicable updates, starting up into the update environment, and verifying the update was successful are more complicated without Storage Executive.

Step 1: Identify the drive model and current firmware

This can often be performed using system configuration utilities installed on the running operating system.

The following steps can be used in Windows 7:

- Click the Start button, then click Computer.
- Right-click on the disk icon that represents your drive, then click Properties.
- Click the Hardware tab.
- The “All disk drives:” list contains a list of all physical drives in the system. Highlight the chosen drive and click Properties.
 - Note: There may be multiple entries in the list, and each entry may appear as an ATA device or a SCSI device depending on the drivers installed in the system.
- Click the Details tab, click the Property drop-down list, then select Hardware Ids. A display similar to what is shown on the following page will appear.
 - Note: The format of the information below may change depending on if the drive appeared as an ATA device or a SCSI device.



- The drive model and current firmware are circled in the example above.

Step 2: Download the appropriate ISO image from Crucial.com

On a system with a working internet connection, go to the following URL to find update packages:
<http://www.crucial.com/usa/en/support-ssd-firmware>.

Search for a firmware update ISO image that matches the first several characters of the drive model. There may be multiple packages that match the drive model. If there are, choose the ISO that is most recent and is similar in format to the firmware revision currently on the drive. In the example above, MU01 was loaded on a Crucial M550 drive, so a Crucial M550 firmware update package for MU02 or MU03 would be appropriate.

There are some cases where multiple firmware types exist for the same product line, but are not compatible. In these cases, the firmware revisions will appear distinct from each other. For example, a standard Crucial M550 has the self-encrypting drive (SED) feature supported, but there are also Crucial M550s which do not have this feature supported, and the two require separate firmware. In that case, the standard Crucial M550 would contain standard firmware (ex. MU01) and a non-SED version would contain non-SED firmware (ex. MUN1).

Before proceeding to Step 3, make sure the correct ISO image has been downloaded.

Step 3: Create bootable media with the ISO

This step may be performed using a CD burner and a CD-R, or by creating a bootable USB drive. Select which option makes the most sense based on the connectivity of the host system.

Option 1: Burn a bootable CD

The ISO image can be burned onto a CD-R or CD-RW. To do this in Windows, place an unused CD-R into a CD-R capable optical drive, then right-click the downloaded ISO file and click "Burn disk image." Selecting the slowest burn speed is generally advised to ensure proper recording.

Option 2: Create a bootable USB drive

1. Start with an empty and newly formatted USB drive.
2. Open a USB installer program. If you do not have a USB installer program, you may install a USB installer program such as the Universal USB Installer available for free at www.pendrivelinux.com/universal-usb-installer-easy-as-1-2-3/.
3. Using the Universal USB Installer:
 - In the Step 1 drop-down list, select Try Unlisted Linux ISO
 - Find the firmware ISO previously downloaded
 - Create the bootable USB with the Format drive option selected

Shut down the host system with the newly created bootable media attached.

Step 4: Boot into the created media to perform the update

This step may first require disabling drive passwords, or changing the boot order using the host system's BIOS or UEFI configuration utility. Consult the host system's owner's manual to perform these actions.

When the system is started from the bootable media created using the ISO, the update will be performed on all compatible drives on the host system.

The user is informed of the progress of the update through text displayed on a screen similar to what is shown below:

```
Micron Storage Executive
Loading ... Done.

Upgrading drive /dev/sdb [Serial No. 14210CC52AD7] from firmware MU01 to MU02
.....
Device Name   : /dev/sdb
Firmware Update on /dev/sdb Succeeded!
CMD_STATUS   : Success
STATUS_CODE  : 0
Your system will now reboot back into Windows.
-
```

Step 5: Remove the bootable media and restart into the normal operating environment

To prevent the host system from starting up into the ISO again, remove the bootable media from the host system.

The host system should function normally after being restarted.