SSD7103 NVMe RAID Controller
macOS Installation Guide
(Bootable RAID)

Version 1.00

Content

1. Overview

This guide includes important hardware/software requirements, installation & upgrade procedures, and troubleshooting tips for using the SSD7103 NVMe RAID controller with a macOS operating system.

Prerequisites
This section describes the base hardware and software requirements for the SSD7103 NVMe RAID controller.

Cloning the Boot Drive to the SSD7103 RAID Array
This section described how to clone an existing macOS boot drive to an array or NVMe SSD hosted by the SSD7103 NVMe RAID controller.

Driver Installation
This section covers driver installation and driver upgrade procedures for the SSD7103 NVMe RAID controller in a macOS environment.

Troubleshooting
Please consult this section if you encounter any difficulties installing or using the SSD7103 NVMe RAID controller with a Mac platform. It includes descriptions and solutions for commonly reported technical issues.

Appendix
This section describes how to collect trouble shooting information for support cases you have submitted via our Online Support Portal.

2. Prerequisites

1) Make sure at least one NVMe SSD's has been installed into the HighPoint NVMe controller or enclosure. The driver will not install properly unless NVMe SSD's are detected by the hardware environment.

2) Identify the system as either T2 or Non-T2 based – if the system has a T2 chip, make sure to follow section 3 before attempting to install any software for the HighPoint NVMe device.

3) The SSD7103 RAID controller must be installed into a PCIe 3.0 slot with x16 dedicated lanes.

4) Required Operating System Support: macOS 10.13 or later

5) Note: macOS cannot be installed directly to an array or NVMe SSD hosted by the SSD7103 controller – you will need to clone the existing OS to the array/SSD – this guide describes how to use Carbon Copy Clone to complete this procedure

6) Before installing the driver and RAID Management software for a non-bootable configuration, you should log into the system as a System Administrator.

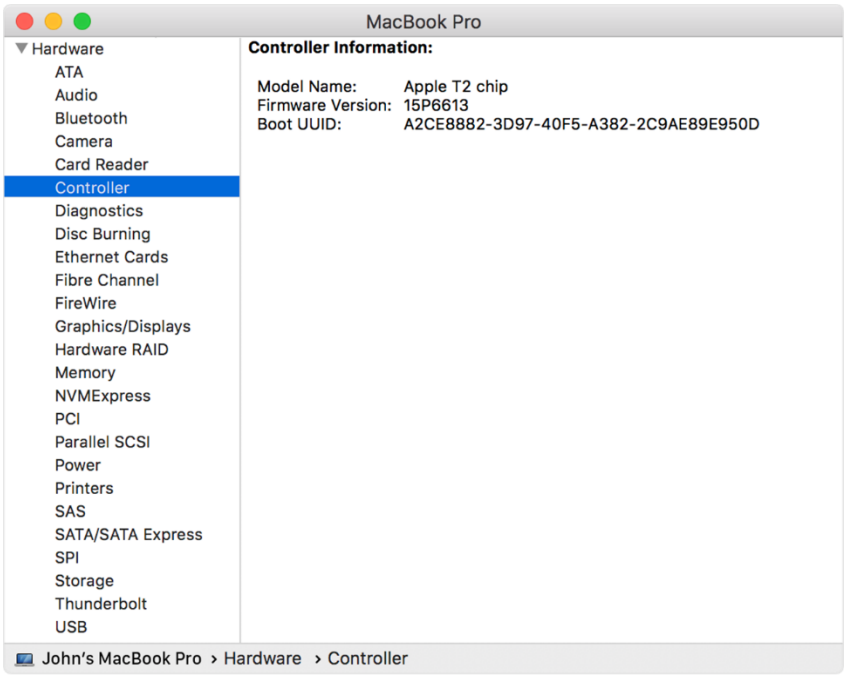
3. Apple T2 security Chip-Disable Secure boot and allowed boot media

Secure Boot must be disabled on the following products:
Learn more About the Apple T2 Security Chip：https://support.apple.com/en-us/HT208862

- iMac Pro
- Mac Pro introduced in 2019
- Mac mini introduced in 2018
- MacBook Air introduced in 2018 or later
- MacBook Pro introduced in 2018 or later

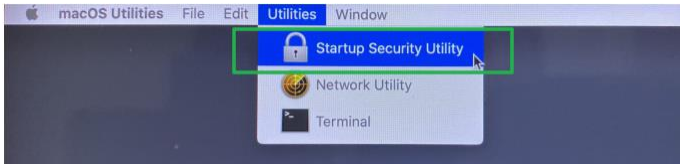
You can also use System Information to learn whether your Mac has this chip:

1. Press and hold the Option key while choosing Apple (□) menu > System Information.
2. In the sidebar, select either Controller or iBridge, depending on the version of macOS in use.
3. If you see "Apple T2 chip" on the right, your Mac has the Apple T2 Security Chip.



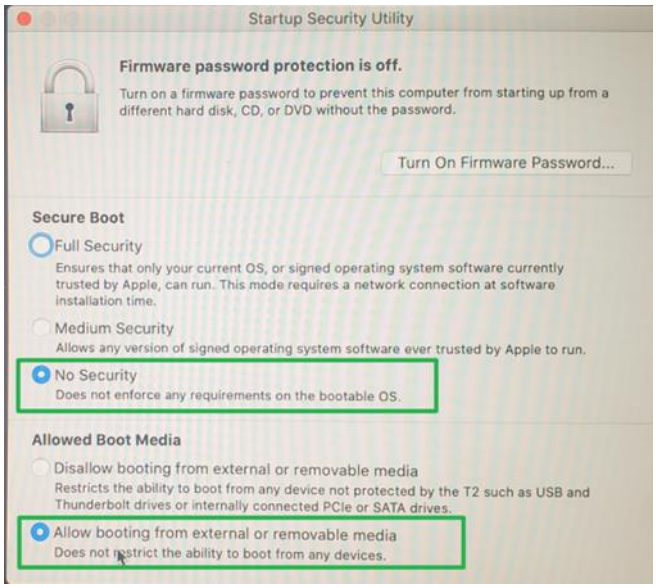
Disabling Secure Boot and Allowed Boot Media

1) Restart the computer and then press the **Command + R** keys simultaneously. Keep holding the keys down until the Apple Logo appears.
2) **When the menu bar says: "macOS Utilities"**, you have booted into Recovery mode. Launch the **Startup Security Utility** application by selecting it from the Utilities menu.



3) A dialog box will appear, telling you that you will need to authenticate as an Administrator to make changes, click **the Enter macOS Password…** button.

4) When the Startup Security Utility window appears, select **No Security** under the Secure Boot options.



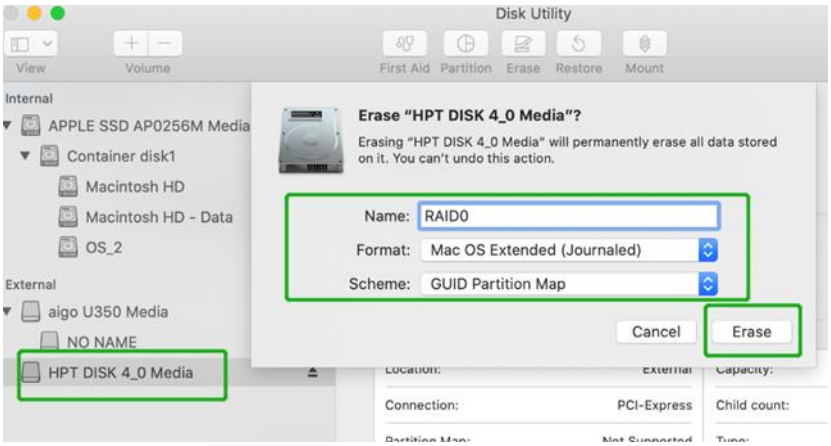
5) Select **Restart** from the Apple menu to restart your Mac, and wait for your normal Desktop to appear.

4. Install macOS to the SSD7103

1) Boot into macOS, install the SSD7103 driver and WebGUI (guides are available from the Software Downloads and Resources pages).

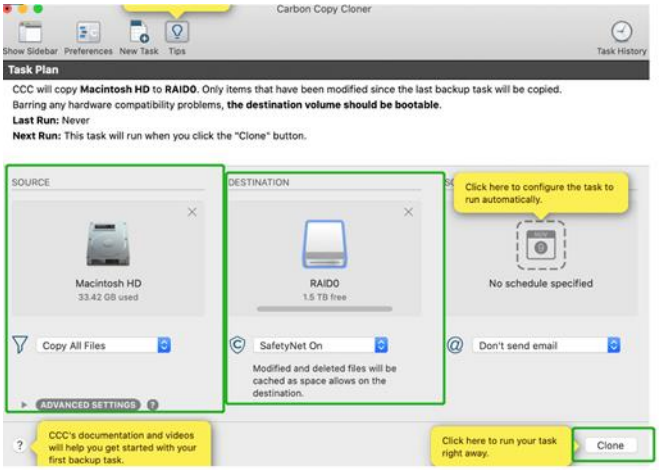
2) After the driver and management software are installed, start the WebGUI management software and create a RAID array.

3) Use 'Disk Utility' to format/partition the array (example shown below):



4) Clone the internal boot disk to the RAID array using 'Carbon Copy Cloner 5'

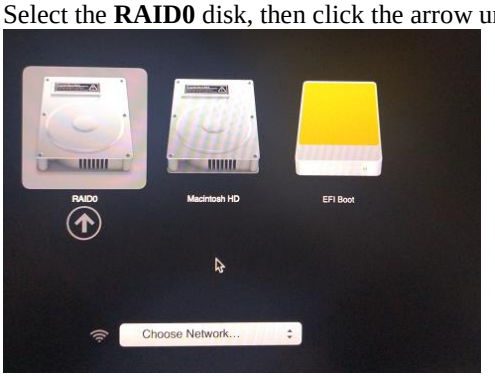
5) Open ‘Carbon Copy Cloner’. **SOURCE** = Select the disk you need to clone (the disk that contains the a bootable version of macOS). **DESTINATION** = select the RAID disk that you created using the EFI interface, then click ‘Clone’:



6) After cloning is complete, reboot the system.

5. Boot macOS after Cloning the Boot Drive

1) When the cloning procedure has completed, restart your Mac, then immediately press and hold the **Option (Alt)** keys.
2) Release the **Option** key when you see the Startup Manager window
3) Select the **RAID0** disk, then click the arrow under its icon, or press **Return**.



6. Troubleshooting

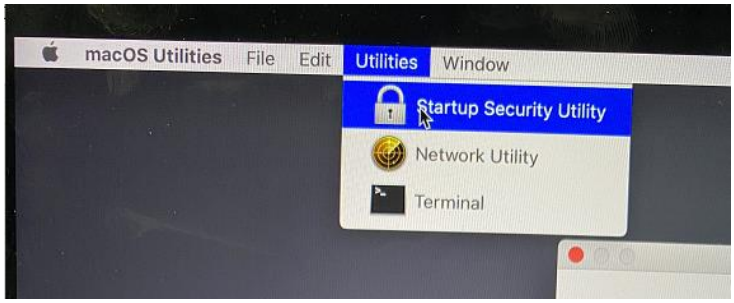
1. The startup disk is not visible in the Startup Manager

Problem: The RAID array that is hosting the cloned boot volume is not recognized by Startup Manager;

This problem can occur if the ROM file is not loaded. To resolve this issue, access the Startup Security Utility and check the following:

a) Restart the system, and press **"command+R"** to enter system recovery mode;

b) Select Utilities from the top menu, then choose **Startup Security Utility**.



c) Set Firmware password protection to OFF.

d) Restart the system, and press and hold the option key to enter the Startup Manager window.

e) Press and hold the Option-Shift-Command-Period keys for 10 seconds, then select the boot drive:

2. A RAID1 array cannot be set as the default boot drive

Problem: macOS displays an error when setting a RAID1 array as the system's default startup item:

To resolve this problem, try the following:

a) Shut down the system and remove the SSD7103 controller. Remove all SSD/s from the SSD7103, except the SSD's hosting the RAID 1 array.
b) Reinstall the SSD7103 into the Mac system and power on the system.
c) After rebooting, try setting the RAID1 array as the default startup item – macOS should no longer display an error.
d) Shut down the system once more and remove the SSD7103.
e) Reinstall all of the SSD's into the SSD7103, and then reinstall the SSD7103 into the Mac system.
f) Power on the system; it should now be able to boot from the RAID 1 array.

Appendix

When submitting s support ticket via our Online Support Portal, the following information will help our Support Department diagnose and resolve your issue as quickly and efficiently as possible.

If you encounter any problem while collecting this information, please contact our Customer Support Department:

Web Support: http://www.highpoint-tech.com/websupport/

Collecting the WebGUI information

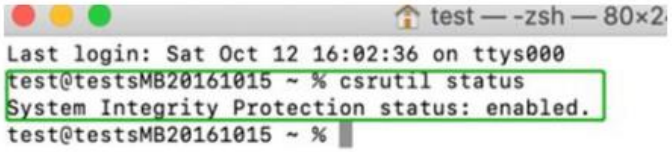
Please take screenshots of each Tab (such as Physical, Logical, Event, etc.) and upload these to your support case. In addition, check the Event log tab and save a copy of the current log – please upload this to the support case.

Collecting the SIP Status

Open Terminal and enter the following command:

csrutil status

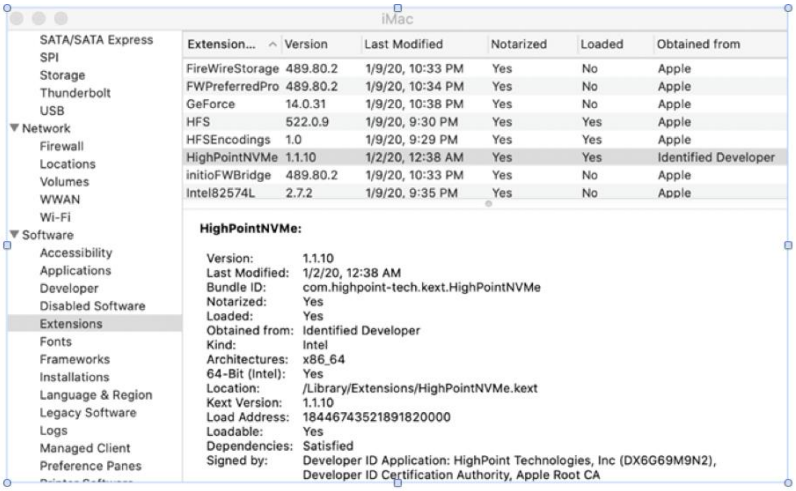
Please take a screenshot and attach it to this support case (see example below – the setting is enabled in this case):



Collecting the driver status and version screenshots

1) Click on the **Apple** logo located near the upper left-hand portion of the Desktop, and select "**About this Mac**".

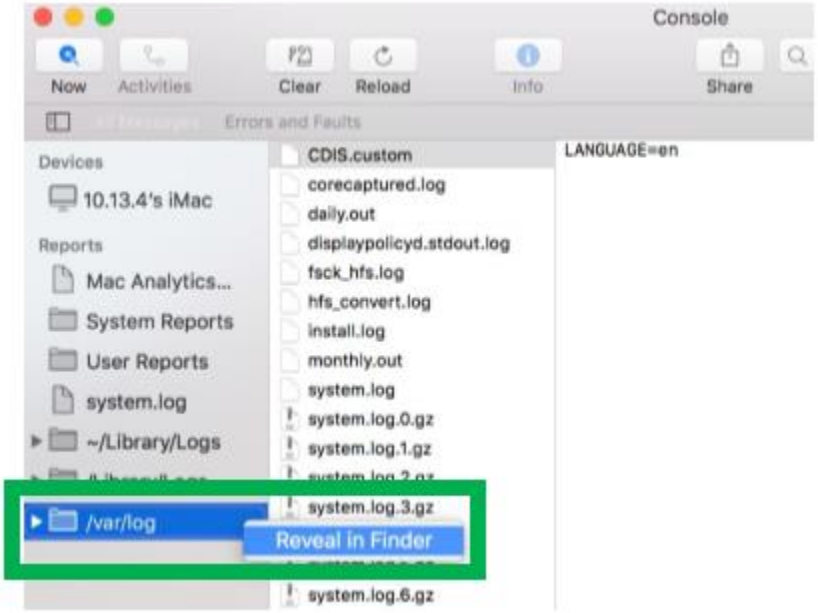
2) Click on **Extensions**, and then click on **HighPoint NVMe** entry – please take a screenshot and attach it this support case (see the example below)



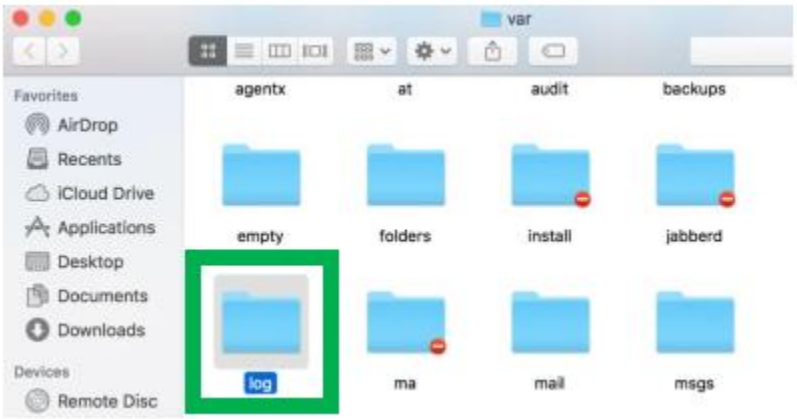
Collecting System Logs

1) Please attach a copy of the /var/log folder to your support ticket.
   To locate the /var/log Folder: 1. Go to **Applications → Utilities → Console**:

2) On the left side of the Console application, right-click on the /var/log folder and select Reveal in Finder:

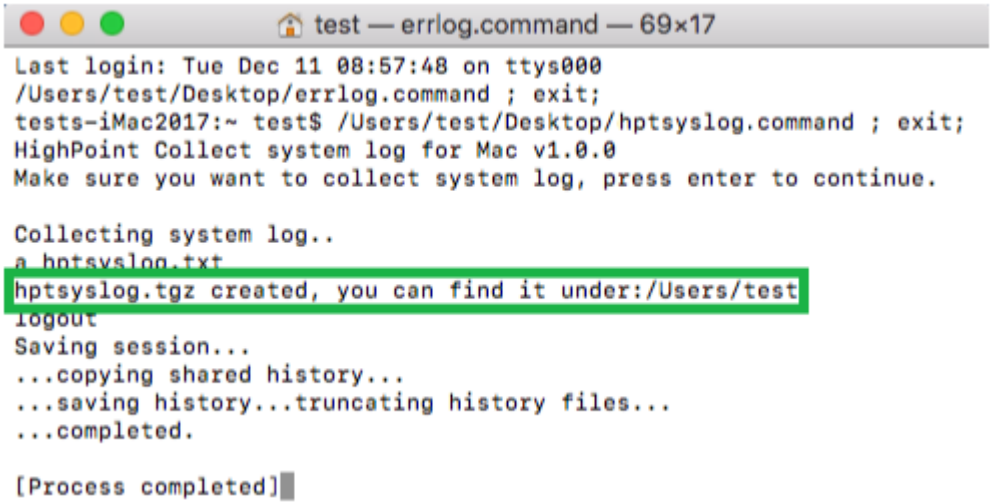


3) You should then be automatically directed to the log folder in the var directory. Please remember when sending the folder to zip file, you should first direct it to a separate location (such as the desktop).



4) In addition to /var/log Folder detailed above, please attach a copy of the errlog.txt file:

   a. Open terminal and type the following, then press Enter:
   log show |grep kernel > hptsyslog.txt



5) Please attach the hptsyslog.txt to your support ticket.