

FnL Series NVMe AIC RAID Drives MacOS Installation Guide

V1.00– Sep, 2021

Contents

Overview	3
Prerequisites	4
1. Disabling macOS Secure boot for T2 Systems.....	5
Disabling Secure Boot	5
2. Reduced Security Policy – For Apple M1 Platform.....	5

Reduced Security Policy	6
3. Disabling SIP (for macOS 10.13x and earlier)	6
4. Installing the Device Driver	9
macOS High Sierra 10.13 and Mojave10.14 and macOS Catalina 10.15 and macOS Big Sur 11.0 Driver Installation Procedure	9
5. Updating the Device Driver.....	12
6. Uninstalling the Device Driver.....	15
Uninstalling the Device Driver for macOS 10.13 and 10.14	15
Uninstalling the Device Driver for macOS 10.15 and macOS 11.0.....	16
7. Installing the FnL Monitor Software	16
8. Updating the FnL Monitor.....	18
9. Uninstalling the FnL Monitor.....	18
10. Trouble shooting.....	19
Unable to connect to the FnL Monitor	19
The FnL Monitor can't connect to a remote system	20
Appendix	21
Collecting the macOS version.....	21
Check the security & privacy.....	21
Verifying Product Installation.....	22
FnL Monitor Screenshots.....	23
FnL Monitor service restart.....	23
Checking the SIP Status	23
Systems with T2 chipsets – Secure Boot status	24
Apple M1 Platform – Reduced security policy	24
Checking the Driver status and Version.....	24
How to Collect System Logs.....	25

Overview

This guide includes important hardware/software requirements, installation & upgrade procedures, and troubleshooting tips for using FnL series NVMe AIC RAID Drives with a macOS operating system.

FnL series NVMe AIC RAID Drives:

SRD7104FDC/SRD7204DC/SRD7505DC
BRD7103DC/BRD7505DC
CRD7104FDC/CRD7505DC

Prerequisites

This section describes the base hardware and software requirements for FnL series NVMe AIC RAID Drives.

Driver Installation

This section covers driver installation, driver upgrade and driver uninstallation procedures for FnL series NVMe AIC RAID Drives in a macOS environment.

Troubleshooting

Please consult this section if you encounter any difficulties installing or using FnL series NVMe AIC RAID Drives. 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.

Prerequisites

- 1) The SRD7104FDC/SRD7505DC/BRD7103DC/BRD7505DC/CRD7104FDC/CRD7505DC NVMe device must be installed into a PCIe 3.0 or 4.0 slot with x16 dedicated lanes. The SRD7204 can be installed into a PCIe 3.0 x8 or x16 slot.

If you are using the FnL NVMe AIC RAID Drives via the RocketStor 6661A adapter, the RocketStor unit must be plugged into a Thunderbolt™ 3 port.
- 2) Operating System Support: macOS 10.13 or later
- 3) Before installing the driver and FnL Monitor RAID Management software, you should log into the system as a System Administrator.
- 4) Identify the system as either T2 or Non-T2 based – if the system has a T2 chip, make sure to follow [section 1](#) before attempting to install any software for the NVMe AIC RAID Drives.
- 5) If you're using the **Apple M1** Platform, make sure to follow [section 2](#) before attempting to install any software for the NVMe AIC RAID Drives.

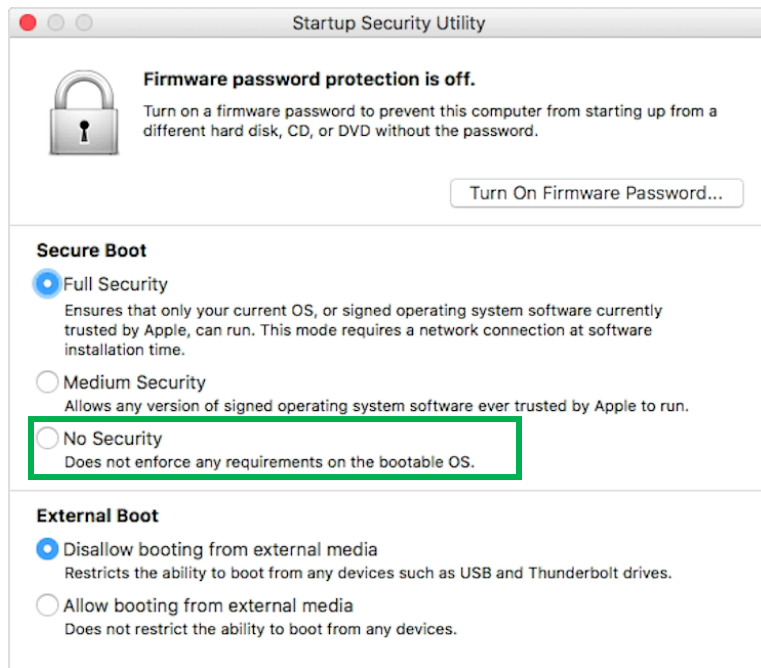
1. Disabling macOS Secure boot for T2 Systems

Customers working with Mac platforms manufactured in 2018 or later that feature a T2 security chip, will need to disable the **Secure Boot** in order to load drivers for third party devices.

For a list of products with the T2 Security Chipset, please visit the following website:
[Mac computers that have the Apple T2 Security Chip](#)

Disabling Secure Boot

In order to use these products with T2 systems, Secure Boot must be disabled. To disable this feature select "**No Security**" from the Startup Security Utility interface. You can access this menu by pressing the **Command (⌘)-R** keys after the Apple logo first appears during the boot-up process.



Instructions are available from Apple's website:
[About Secure Boot](#)

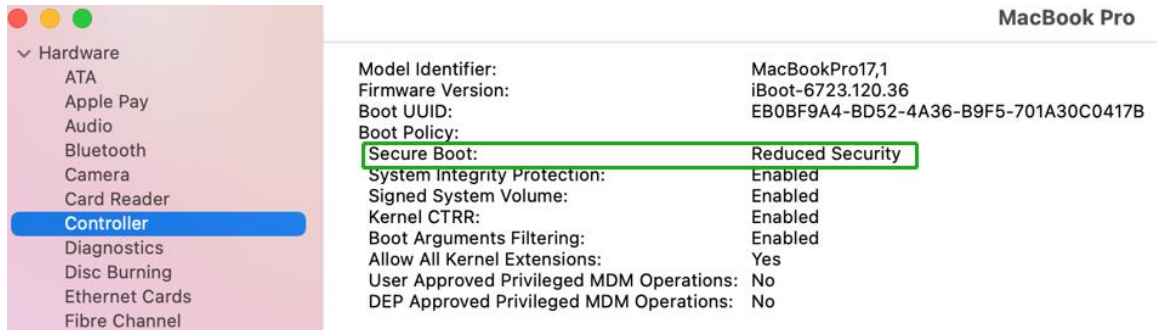
2. Reduced Security Policy – For Apple M1 Platform

Customers working with Apple M1 Platforms manufactured will need to **reduce the Security Policy** in order to load drivers for third party devices.

Mac computers with Apple M1 chip, please visit the following website:
[Mac computers that have the Apple M1 Chip](#)

Check Security Policy settings to determine if they need to be changed, **if Secure Boot is Full Security please set to Reduced Security:**

System Information -> Hardware -> Controller -> Boot Policy

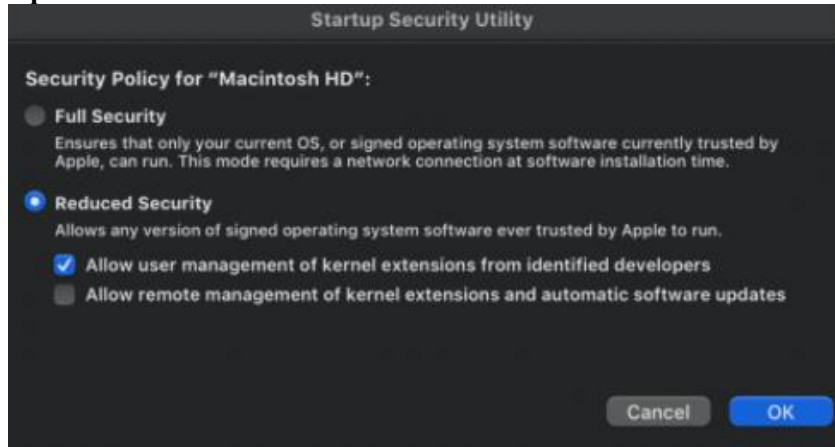


Reduced Security Policy

In order to use these products with Apple M1 Platform, Secure Boot must be **reduced Security**. Reduce this feature and select "**Allow user management of kernel extensions from Identified developers**" from the Startup Security Utility interface.

You can access this menu by:

Shutdown the system, **pressing and holding the Power Button** until you see **Loading Startup Options**.



Instructions are available from Apple's website:

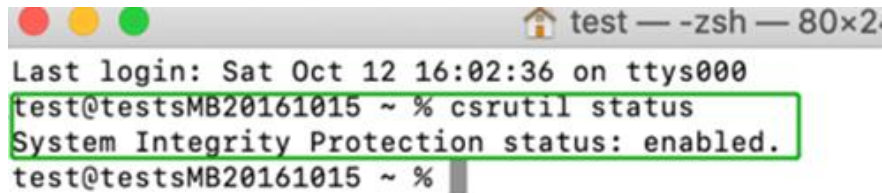
[About Secure Boot for M1](#)

3. Disabling SIP (for macOS 10.13x and earlier)

In addition, macOS 10.13x and earlier may require that **SIP** (System Integrity Protection) be disabled. If enabled, older versions of macOS may prevent the device drivers from loading. While macOS is running, open a terminal window to confirm whether System Integrity Protection (SIP) status is disabled.

If enabled, you will need to manually disable the setting. Open a terminal, and then enter the following command:

csrutil status



```
test — -zsh — 80x20
Last login: Sat Oct 12 16:02:36 on ttys000
test@testsmB20161015 ~ % csrutil status
System Integrity Protection status: enabled.
test@testsmB20161015 ~ %
```

The example screenshot shown above indicates that SIP is enabled.

To disable SIP

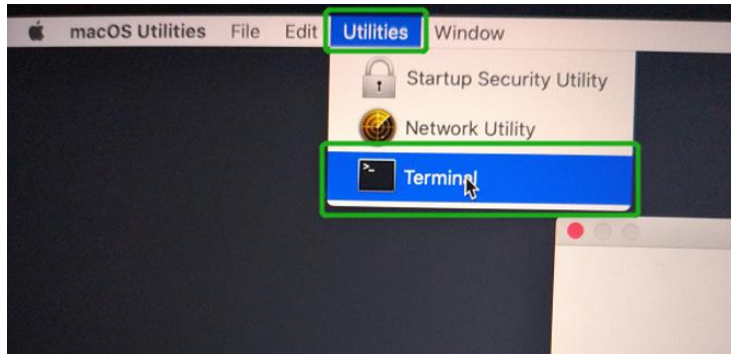
- 1) Restart the computer and hold down the “**Command + R**” buttons. Continue to hold these keys until macOS enters System Recovery mode.



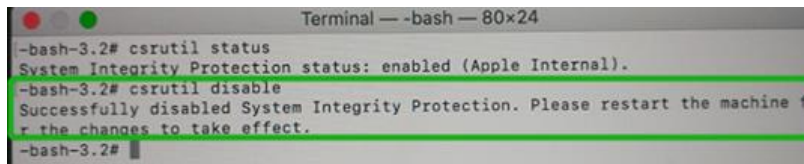
Note: *If you are unable to enter Recovery Mode to disable SIP: Make sure you are using a wired keyboard and mouse for this procedure. Wireless devices may not be recognized or function properly when booting into this mode.*



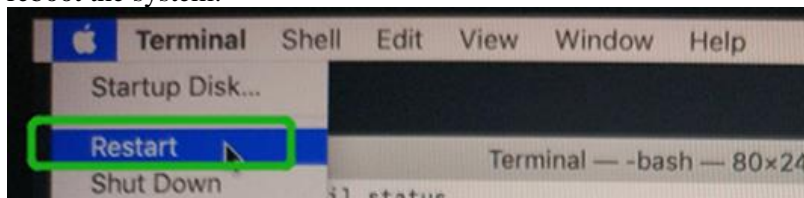
- 2) Click on Utilities in the upper left corner and select Terminal:



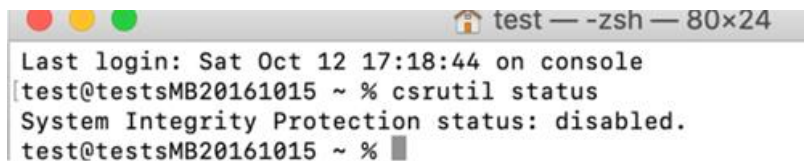
- 3) Set SIP to disabled in using Terminal. Enter the following command:
csrutil disable



- 4) Click the **Apple** logo in the upper left-hand corner of the desktop, and select **Restart** to reboot the system.



- 5) After rebooting, confirm that SIP is disabled. Open terminal and type the following command:
csrutil status



If the status is now reported as **disabled**, you can install the HighPoint NVMe driver.

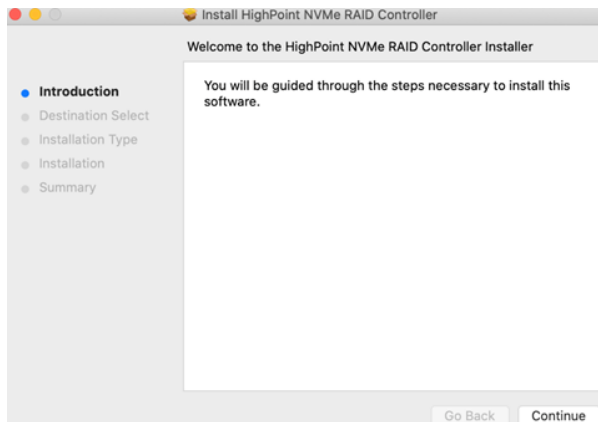
4. Installing the Device Driver

Current drivers can be downloaded from each product's **Software Downloads** webpage.

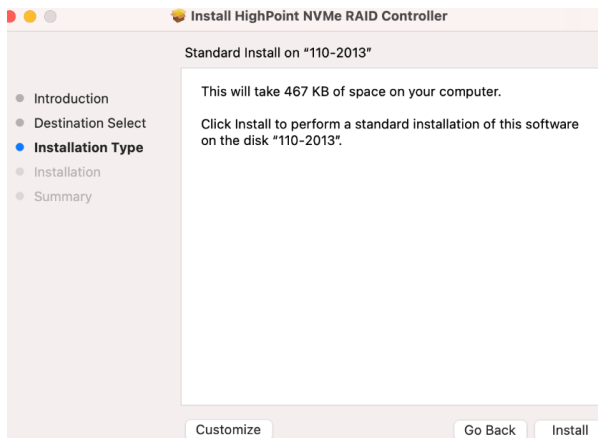
Product	Download Page
SRD7104FDC	https://www.fnlnvme.com/srd7104fdc-overview
SRD7204DC	https://www.fnlnvme.com/srd7204dc-overview
SRD7505DC	https://www.fnlnvme.com/srd7505dc-overview
BRD7103DC	https://www.fnlnvme.com/brd7103dc-overview
BRD7505DC	https://www.fnlnvme.com/brd7505dc-overview
CRD7104FDC	https://www.fnlnvme.com/crd7104fdc-overview
CRD7505DC	https://www.fnlnvme.com/crd7505dc-overview

macOS High Sierra 10.13 and Mojave10.14 and macOS Catalina 10.15 and macOS Big Sur 11.0 Driver Installation Procedure

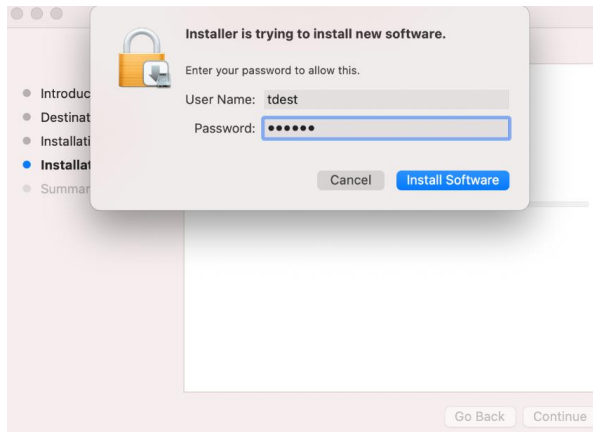
- 1) Locate the download and double click the **HighPointNVMe.pkg** package to start the installer. Click the **Continue** button:



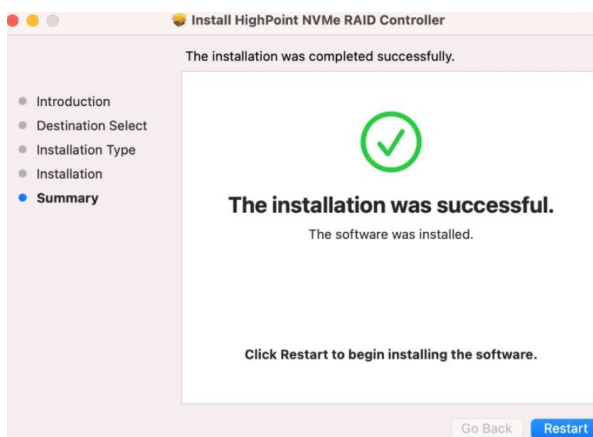
- 2) macOS will prompt you to install the driver. Click **Install** to proceed.



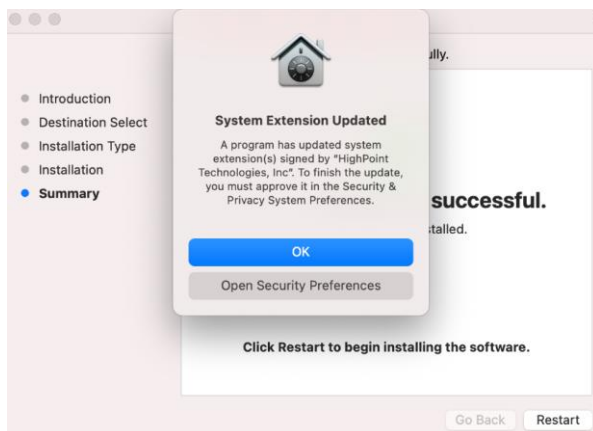
- 3) You will be prompted that installer is trying to install new software, enter the *Administrator* Username and Password. Once these have been entered, Click **Install Software**.



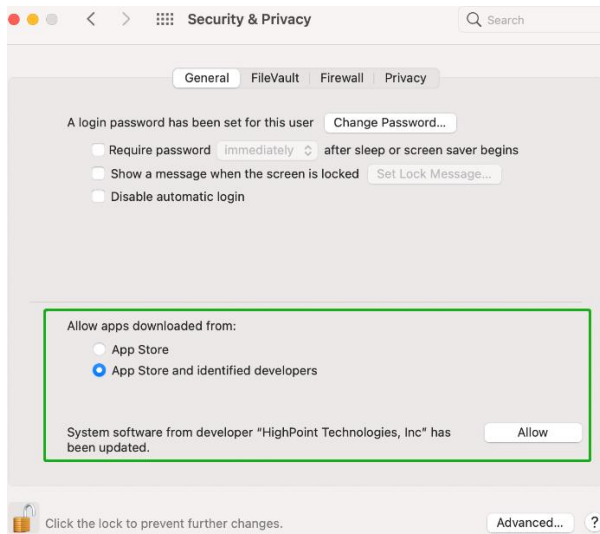
- 4) If no pop-ups appear, please proceed to the next step of installation. Click **Restart**.



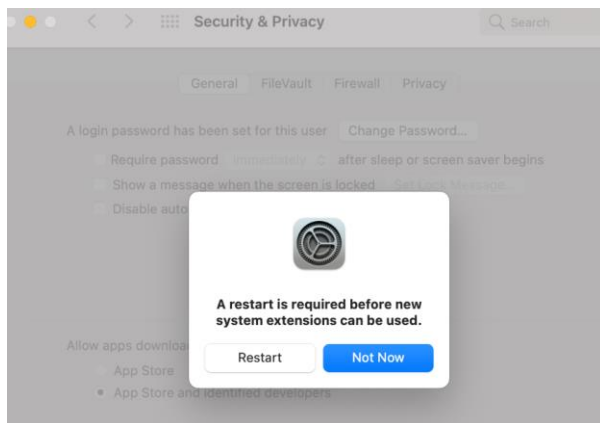
- 5) If you receive a popup window prompting you for permission, click **Open Security Preferences**.



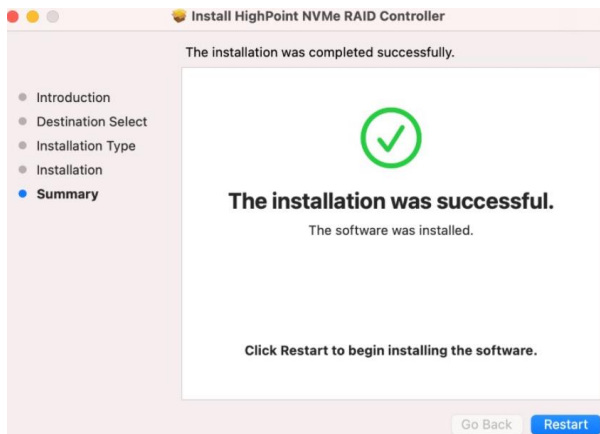
- 6) Make sure **App Store and identified developers** is checked, and then click **Allow**.



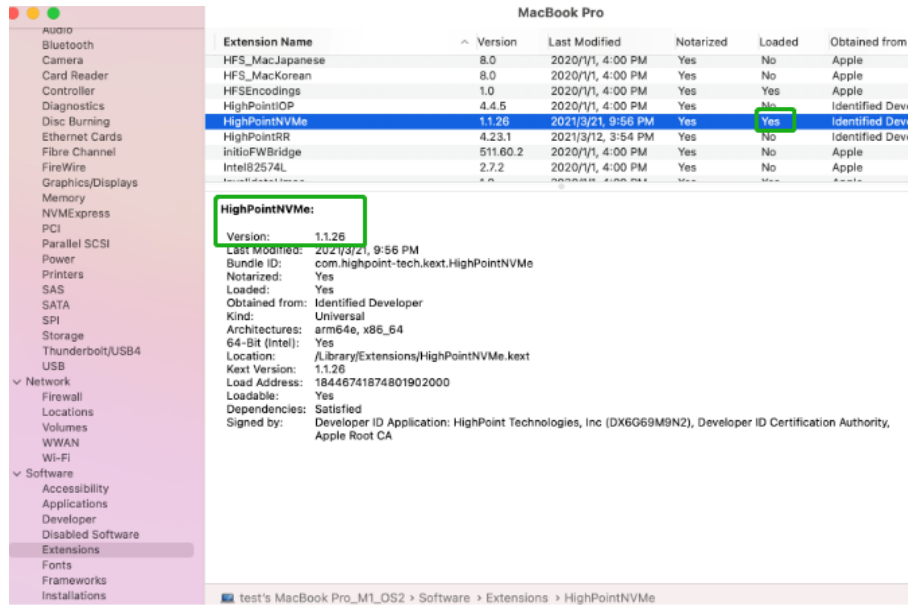
- 7) You will receive a popup window, prompting you to restart. Click **Not Now**.



- 8) Return to the driver installation window. Click **Restart** to restart the system.



- 9) After the system restarts, the driver's status can be viewed under **System Information**; The following screenshot shows the driver has been loaded:



Note: The driver revision shown in the screenshots may not correspond with current software releases. Please make sure to download the latest driver updates from the product's Software Updates page.

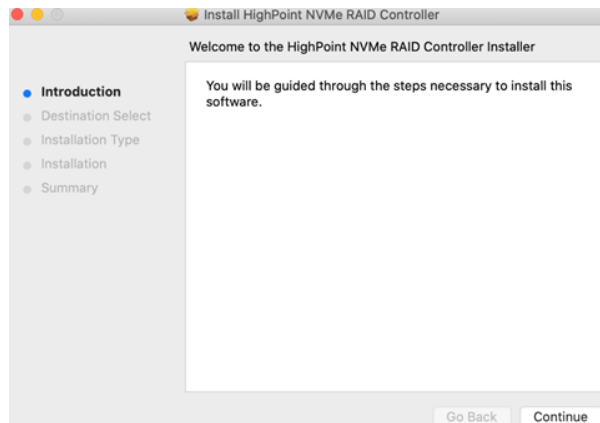
5. Updating the Device Driver

Note: Update the driver, please make sure the NVMe AIC RAID Drives is connected to the host.

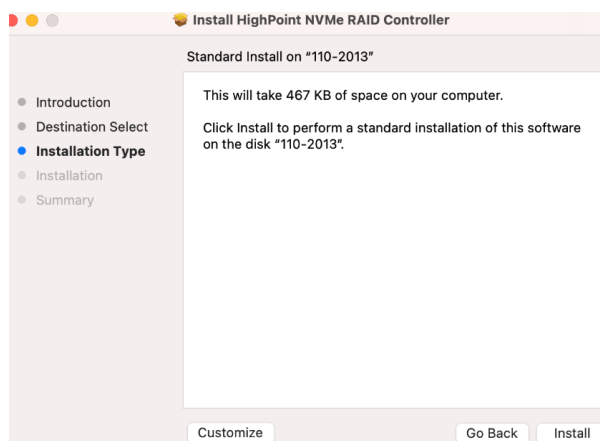
Current drivers can be downloaded from each product's **Software Downloads** webpage.

Product	Download Page
SRD7104FDC	https://www.fnlnvme.com/srd7104fdc-overview
SRD7204DC	https://www.fnlnvme.com/srd7204dc-overview
SRD7505DC	https://www.fnlnvme.com/srd7505dc-overview
BRD7103DC	https://www.fnlnvme.com/brd7103dc-overview
BRD7505DC	https://www.fnlnvme.com/brd7505dc-overview
CRD7104FDC	https://www.fnlnvme.com/crd7104fdc-overview
CRD7505DC	https://www.fnlnvme.com/crd7505dc-overview

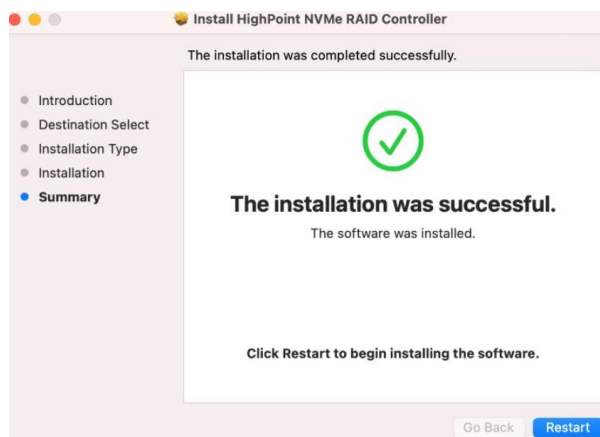
- 1) Locate the download and double click the **HighPointNVMe.pkg** package to start the installer. Click the **Continue** button:



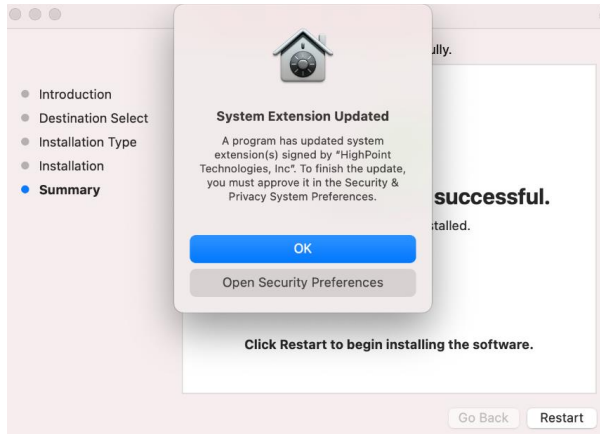
- 2) macOS will prompt you to install the driver. Click **Install** to proceed.



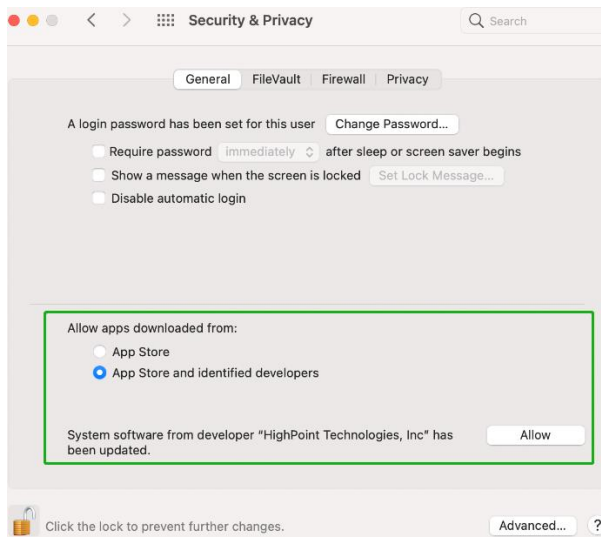
- 3) If no pop-ups appear, please proceed to the next step of installation. Click **Restart**.



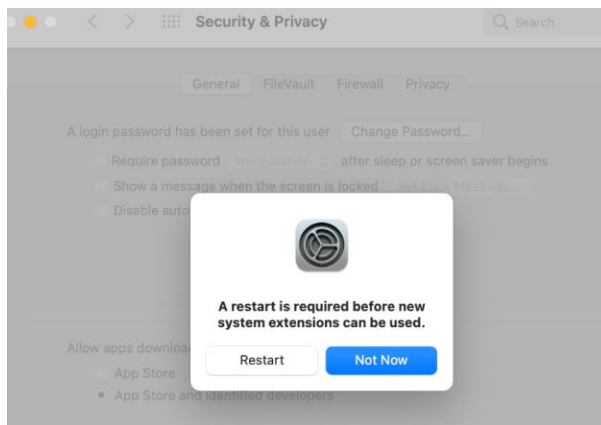
- 4) If you receive a popup window prompting you for permission, click **Open Security Preferences**.



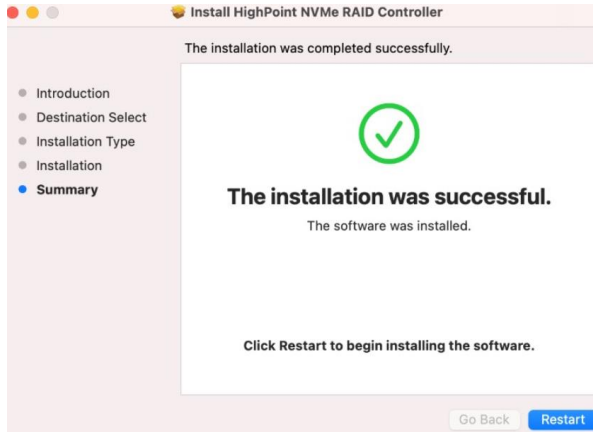
- 5) Make sure **App Store and identified developers** is checked, and then click **Allow**.



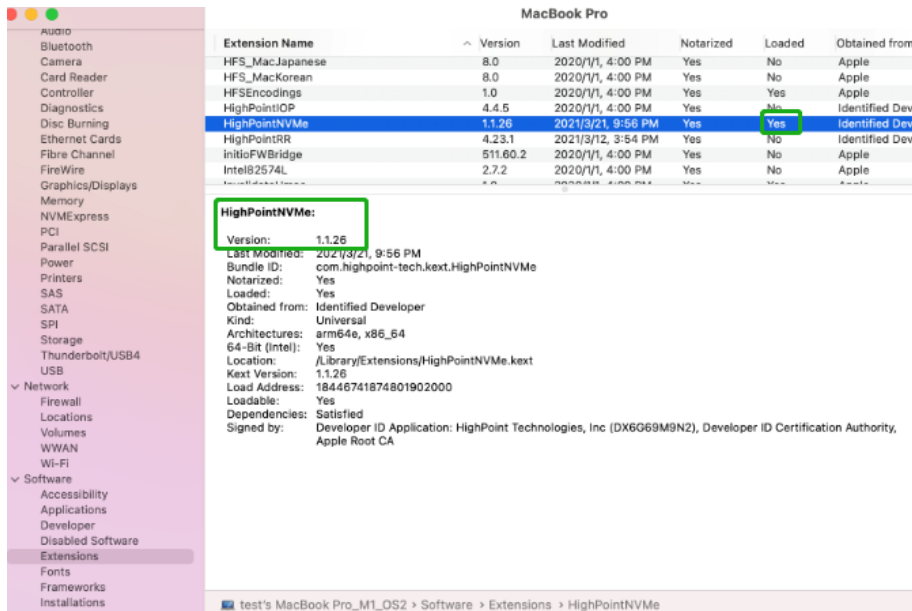
- 6) You will receive a popup window, prompting you to restart. Click **Not Now**.



- 7) Return to the driver installation window. Click **Restart** to restart the system.



- 8) After the system restarts, the driver's status can be viewed under **System Information**; The following screenshot shows the driver has been loaded:



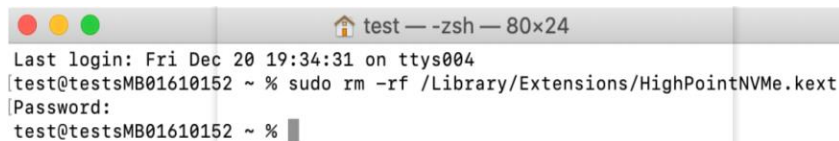
Note: The driver revision shown in the screenshots may not correspond with current software releases. Please make sure to download the latest driver updates from the product's Software Updates page.

6. Uninstalling the Device Driver

Uninstalling the Device Driver for macOS 10.13 and 10.14

To uninstall the NVMe driver, you will need to open a **Terminal** window and enter the following command:

```
sudo rm -rf /Library/Extensions/HighPointNVMe.kext
```

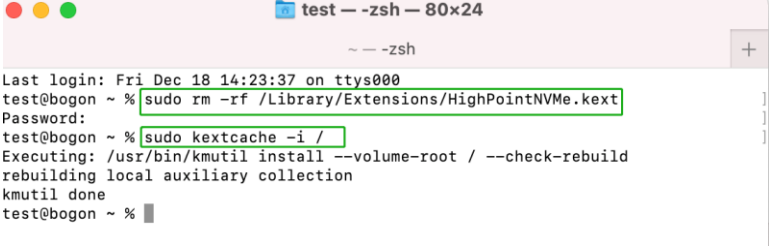


Uninstalling the Device Driver for macOS 10.15 and macOS 11.0

To uninstall the Nvme driver, you will need to open a Terminal window and enter the following command:

```
sudo rm -rf /Library/Extensions/HighPointNVMe.kext
```

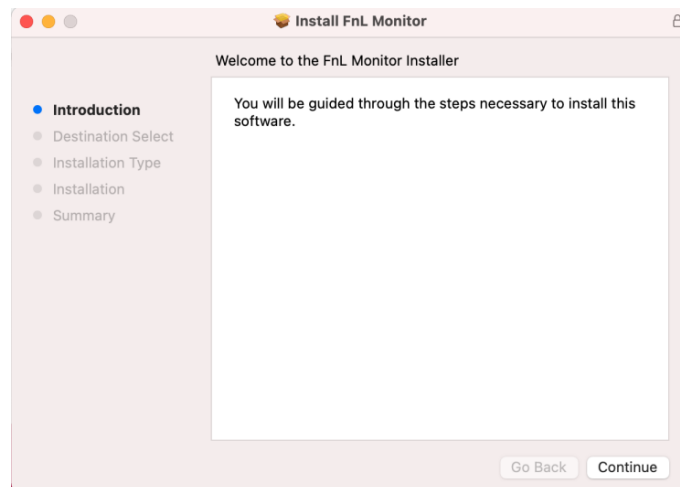
```
sudo kextcache -i /
```



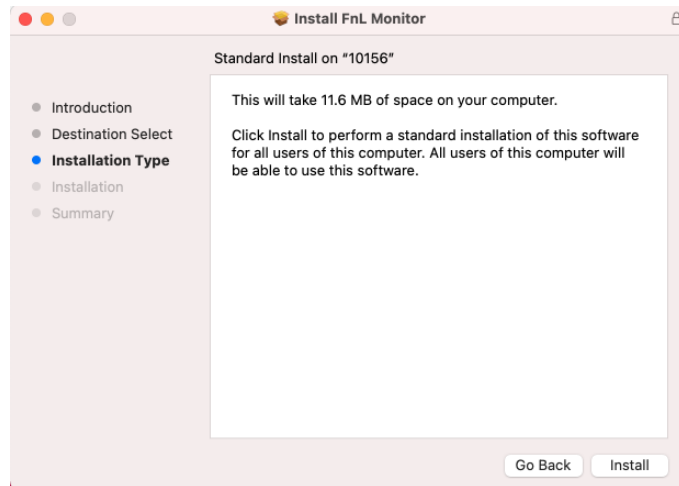
```
test --zsh -- 80x24
~ --zsh
Last login: Fri Dec 18 14:23:37 on ttys000
test@bogon ~ % sudo rm -rf /Library/Extensions/HighPointNVMe.kext
Password:
test@bogon ~ % sudo kextcache -i /
Executing: /usr/bin/kmutil install --volume-root / --check-rebuild
rebuilding local auxiliary collection
kmutil done
test@bogon ~ %
```

7. Installing the FnL Monitor Software

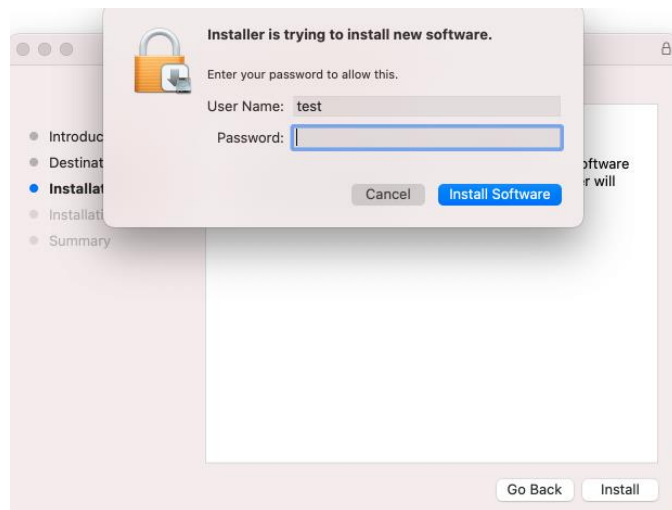
- 1) Double click the package named **HighPointWebGUI.pkg** to start the installer. When the window appears, click the **Continue** button.



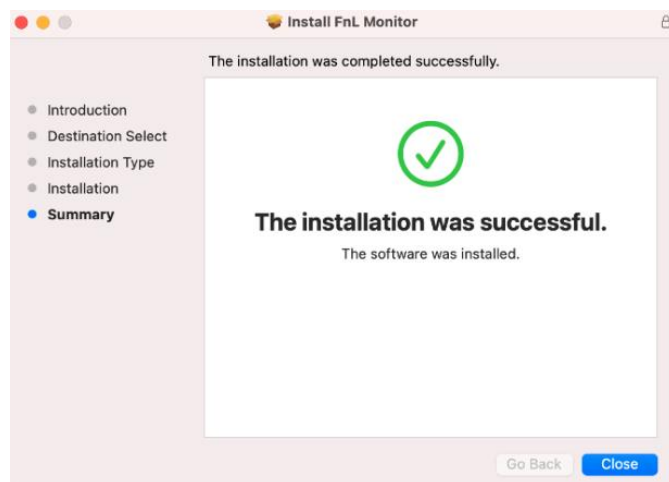
- 2) You will be promoted to click the **Install** button. Click **Install** to continue.



- 3) You will then be promoted to enter the *Administrator* Username and Password. Once these have been entered, click **Install Software** to continue.



- 4) The FnL Monitor software has been installed. Click **Close** to complete the procedure.

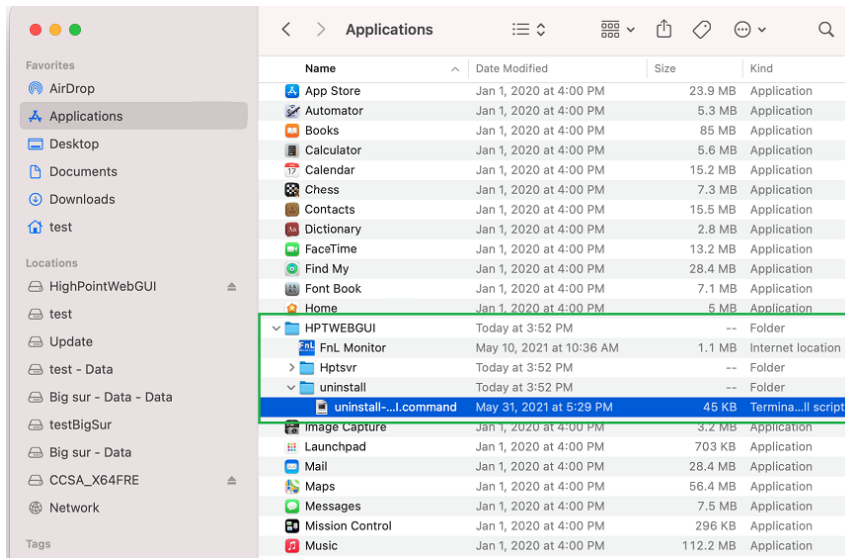


8. Updating the FnL Monitor

- 1) First, uninstall the current FnL Monitor. Please refer to [Uninstalling the FnL Monitor](#).
- 2) Once the system has rebooted, download the latest version of the FnL Monitor from the appropriate Software Downloads webpage.
- 3) Locate the download and double click the package named **HighPointWEBGUI.pkg** to start the installer. Please refer to [Installing the FnL Monitor](#) for more information.

9. Uninstalling the FnL Monitor

To uninstall the FnL Monitor, access Applications, click on **HPTWEBGUI**, select **uninstall**, and double-click the **uninstall-FnL Monitor.command**. The uninstall command will automatically open a terminal and uninstall the software:



Enter the macOS password, uninstall the software:

```
test — uninstall-WebGUI.command — 101x34
Last login: Thu Sep  2 16:04:21 on console
/Applications/HPTWEBGUI/uninstall/uninstall-WebGUI.command ; exit;
test@test-Mac-Pro-10156 ~ % /Applications/HPTWEBGUI/uninstall/uninstall-WebGUI.command ; exit;

This script will attempt to uninstall FnL Monitor Service

Note: You must be logged on as an administrator to uninstall the software.
The script will prompt you for an administrator password.

If prompted for a password please enter your administrator password.

The following service files will be deleted
/Applications/HPTWEBGUI
/Library/Receipts/wwwfiles.pkg
/Library/Receipts/websservice.pkg
/Library/LaunchDaemons/HPTWebGUIDaemon.plist
/usr/share/hpt
/usr/bin/hptdaemonctl

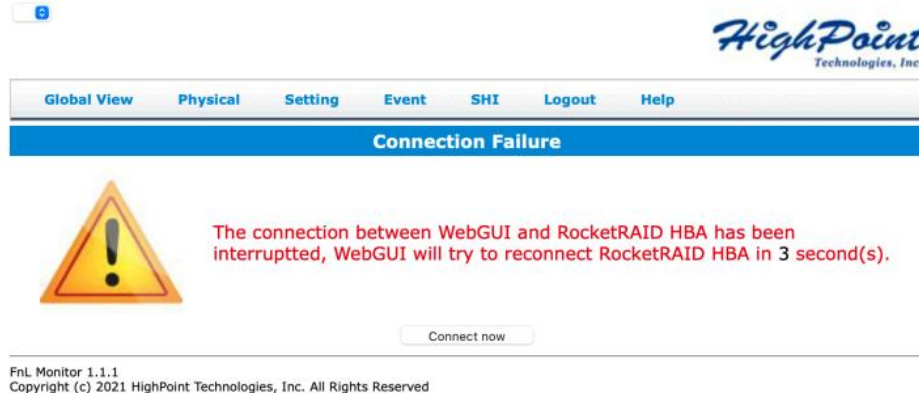
Password:
Process has completed.
Saving session...
...copying shared history...
...saving history...truncating history files...
...completed.

[Process completed]]
```

10. Trouble shooting

Unable to connect to the FnL Monitor

After the driver and management software are installed, the management software displays a "Connection Failure" warning when attempting to start the interface:



This error can be triggered by one of the following issues

01. The NVMe AIC RAID Drives hardware is not recognized by macOS
02. The NVMe AIC RAID Drives device driver is not installed or is not loading properly.
03. FnL Monitor service is not running.
04. The system's SIP status is incorrect.
05. If you are using a T2 system, Secure Boot may not be 'Disabled'.
06. If you are using Apple M1 system, Security Policy may not be 'Reduced'.

01. Verifying the NVMe AIC RAID Drives hardware

Please refer to the [Appendix – Verifying Product Installation](#) to make sure the NVMe AIC RAID Drives device is properly recognized by macOS.

Note: If you are using the RocketStor 6661A-NVMe:

If you are using the RocketStor 6661A-NVMe (RS6661A-NVMe), or another FnL series Drives via our RocketStor 6661A adapter and a Thunderbolt™ 3 connection, refer to the [first screenshot](#) displayed under - **Appendix – Verifying Product Installation**. If the RS6661A entry is present, proceed to screenshot #2.

If the RocketStor 6661A entry is not displayed, this may be related to a connection problem – move the RS6661A to another Thunderbolt™ 3 port or replace the cable and recheck the entry.

02. Make sure the NVMe AIC RAID Drives Driver is loaded

Please refer to the [Appendix - Checking the Driver status and Version](#) to make sure the NVMe AIC RAID Drives driver is installed properly.

If the HighPoint NVMe driver is not loading, proceed to step 2 – [Check the security & privacy status](#). If HighPoint software is blocked in the permission, you need to click Allow.

If the driver is loading properly, but the FnL Monitor is still unable to start, please try to restart the FnL Monitor service. Please refer to [Appendix – FnL Monitor service restart](#) make settings.

If FnL Monitor is still not connected, please contact our [Support Department](#) to open a support ticket. Please make sure to include any screenshots and system information you are able to collect (see the Appendix for more information).

03. Check the SIP status

Please refer to the [Appendix - Checking the SIP Status](#) .

If the settings are not correct for your system, please refer to the driver installation manual for each system to reset the SIP status.

04. For T2 Systems: Make sure Secure Boot is disabled

Please refer to the [Disabling Secure Boot](#). If the setting is incorrect, you will need to reboot the system to change the setting.

05. For Apple M1 Platform: Make sure Security Policy is reduced

Please refer to the [Reduced Security Policy](#) . If the setting is incorrect, you will need to shutdown the system to change the setting.

If you encounter any problems while checking items 1-6, please refer to the [Appendix](#) to collect information about your system and configuration, and submit a support ticket to our Customer Support department using our Online Support Portal: <https://www.highpoint-tech.com/websupport/main.php>

The FnL Monitor can't connect to a remote system

If you can't connect to a remote system, make sure **raidman-httpsd** is running on the target system, and confirm that you can access the remote system via a TCP/IP connection. If you have a firewall configured, make sure TCP port 7406 is not blocked.

Appendix

When submitting a 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.

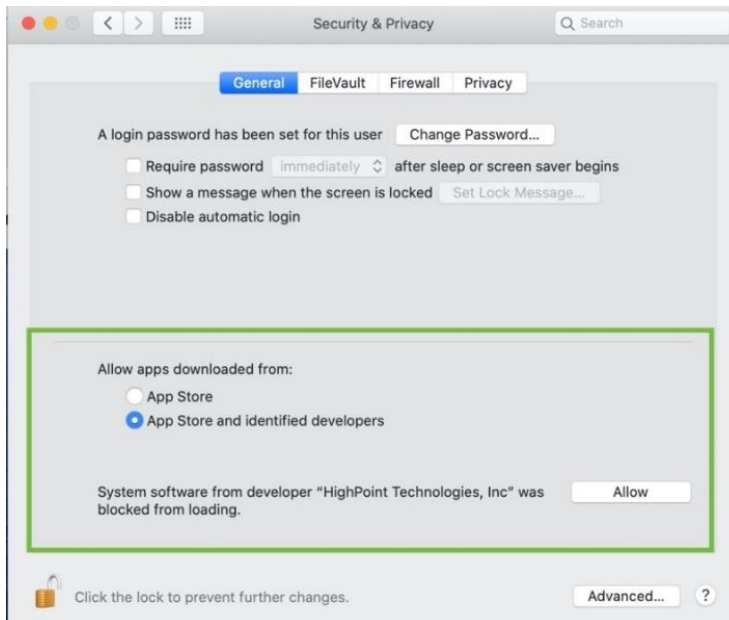
Collecting the macOS version

- 1) Click on the Apple logo located near the upper left-hand portion of the Desktop, and click “Version”. Then the version number of the system will all be displayed.



Check the security & privacy

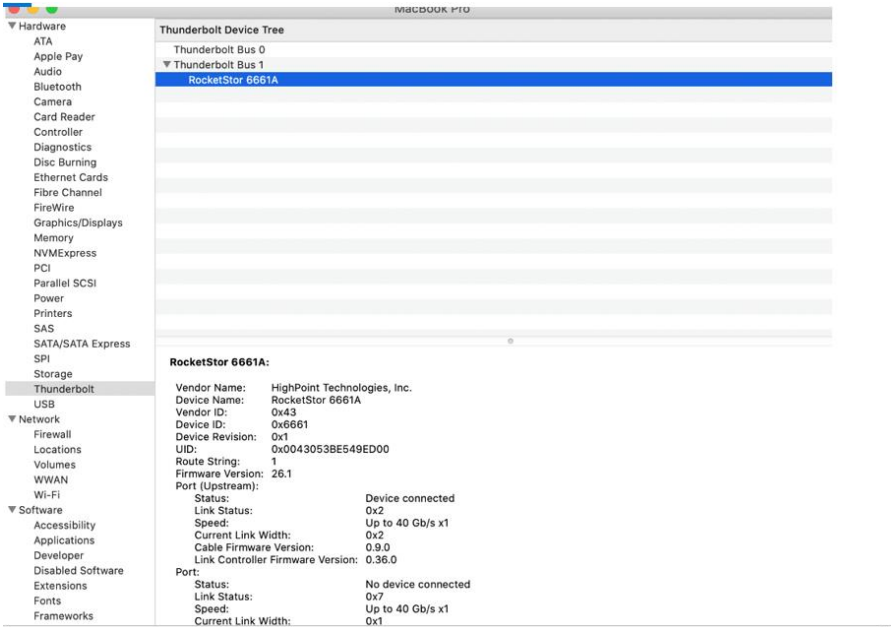
- 1) Check if there is HighPoint software blocked in the permission, if it is blocked, you need to click “Allow”.



Verifying Product Installation

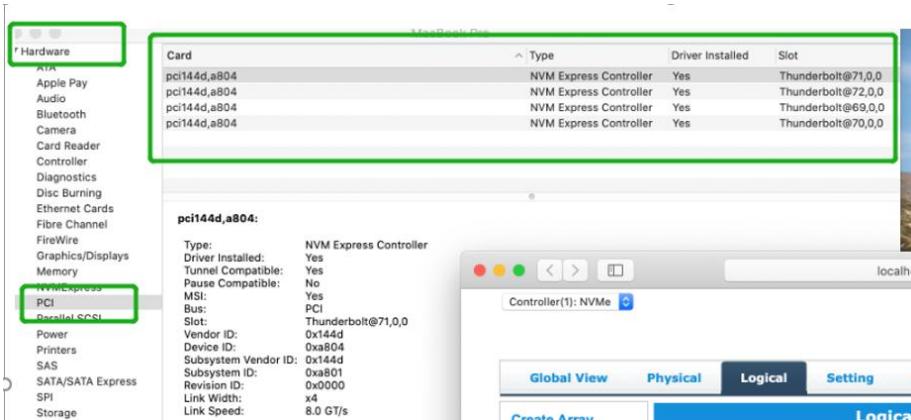
- 1) Click on the **Apple** logo located near the upper left-hand portion of the Desktop, and select “**About this Mac**”.

RocketStor 6661A-NVMe (Thunderbolt entry):

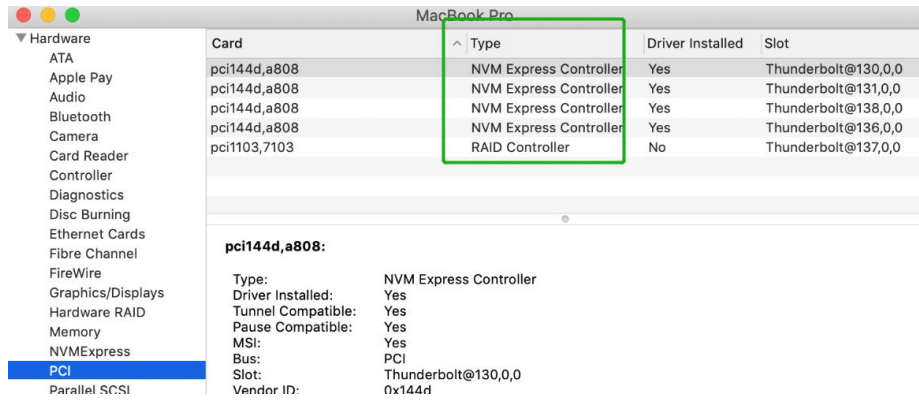


- 2) If you are using a NVMe AIC RAID Drives, check under **Hardware, PCI**. Reference screenshots for each product are show below.

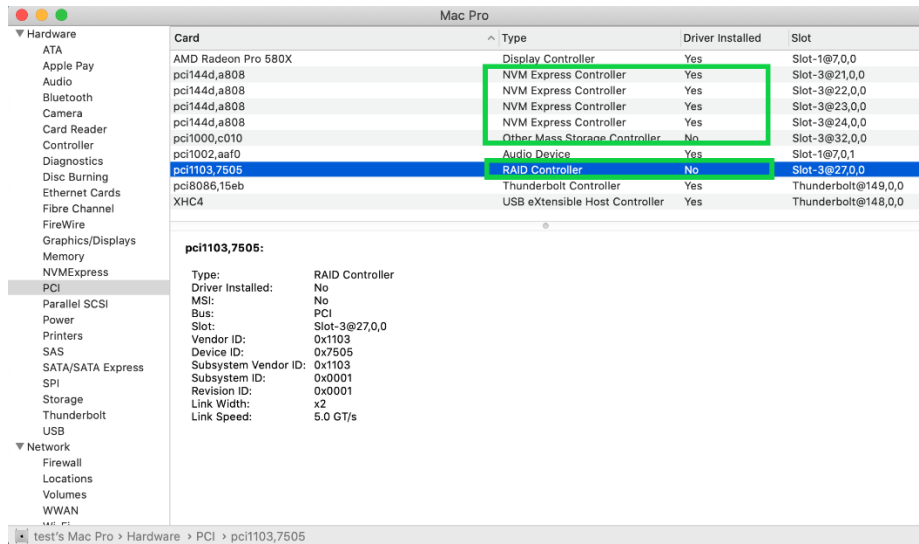
SRD7104DC / SRD7204DC / CRD7104FDC or RS6661A-NVMe:



BRD7103DC:



SRD7505DC / BRD7505DC / CRD7505DC:



FnL Monitor Screenshots

Please take screenshots of FnL Monitor 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.

FnL Monitor service restart

If you can't connect to the FnL Monitor, please check if a process named raidman-httpsd is running on the system. If it is not running, you can start it manually by opening a terminal window and running the command: “**sudo hptdaemonctl restart**”.

Checking the SIP Status

Open a Terminal window and enter the following command:

csrutil status

Please take a screenshot of the output, and attach it to a support case (see example below):

```
test — zsh — 80x2
Last login: Sat Oct 12 16:02:36 on ttys000
test@testsmB20161015 ~ % csrutil status
System Integrity Protection status: enabled.
test@testsmB20161015 ~ %
```

The status will vary depending on which version of macOS you are using:

MacOS Version	SIP Status	Driver Status
10.13.x	Disable	Loaded
10.14.x	Enable	Loaded
10.15.x	Enable	Loaded
11.x	Enable	Loaded

Systems with T2 chipsets – Secure Boot status

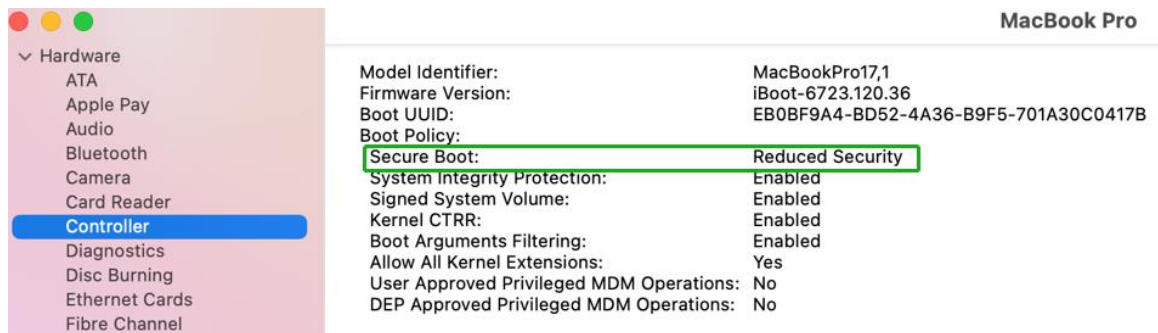
You will need reboot the system and enter Recovery Mode to check the Secure Boot status. This setting should remain disabled.

Please refer to: [Disabling Secure Boot](#)

Apple M1 Platform – Reduced security policy

Check if Secure Boot is **Reduced Security**

System Information -> Hardware -> Controller -> Boot Policy

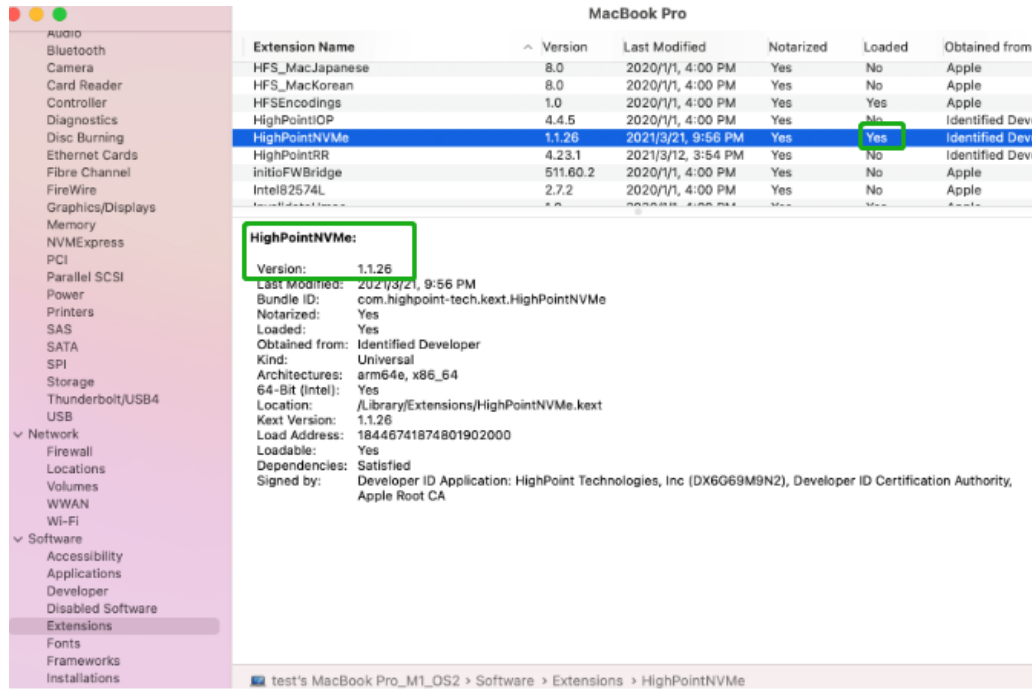


Secure Boot must be **reduced Security** in order to load drivers for third party devices, if change please refer to: [Reduced Security Policy](#)

Checking the Driver status and Version

- 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):

System Information→Software→Extensions→HighPointNVMe



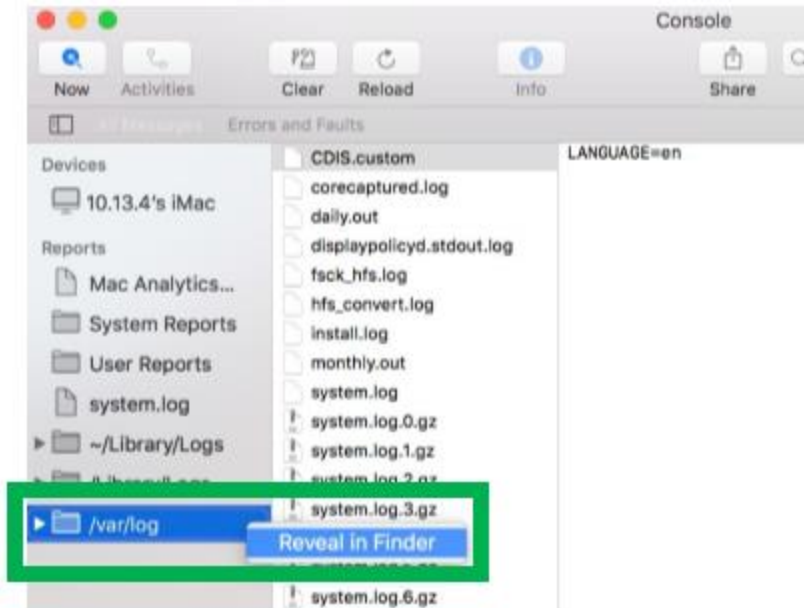
How to Collect System Logs

- 1) Please attach a copy of the /var/log folder to your support ticket.

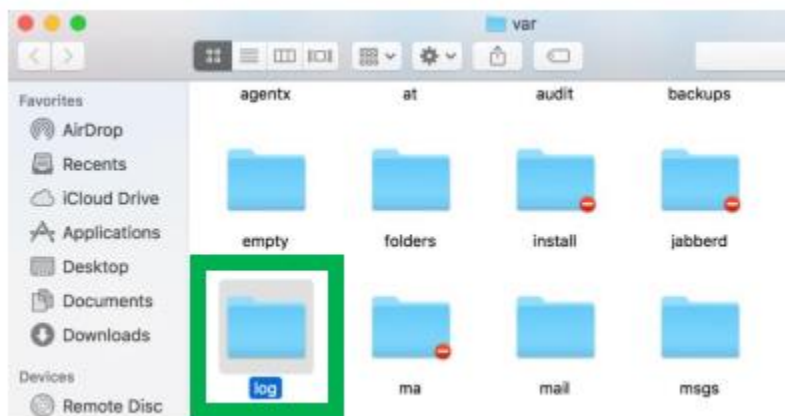
To locate the /var/log Folder: 1. Go to **Applications** → **Utilities** → **Console**:



- 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:

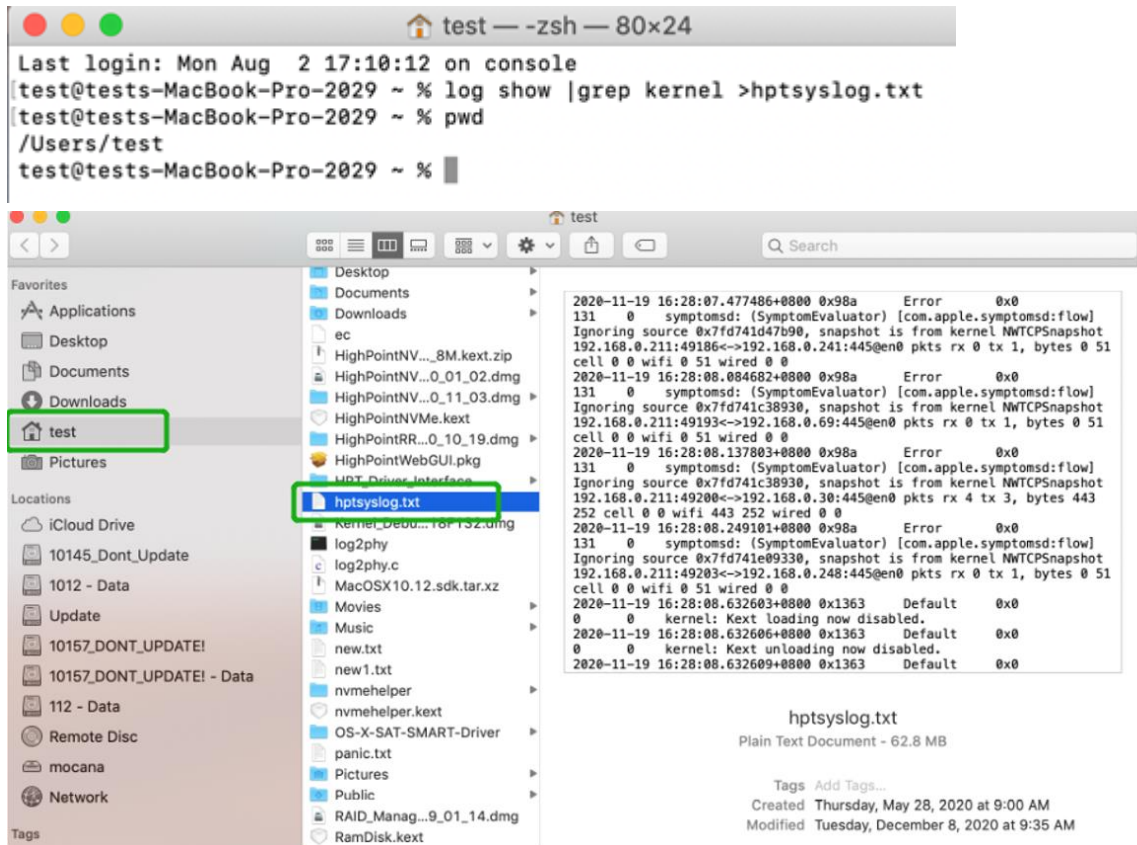
log show |grep kernel > hptsyslog.txt

Note:

It takes about 5-10minutes to respond after this command is entered, please don't worry, this is because your log file is relatively large, so it takes a lot of time.

- b. Enter the following command to view the path where the log is stored.

pwd



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