



SSD7000 Software Guide

V1.02- August 28, 2024

Copyright 2024 HighPoint Technologies, Inc.

All rights reserved

Table of Contents

1. Overview	6
1.1. General Features of the NVMe RAID AIC	6
1.2. Advanced Features of the NVMe RAID AIC	7
1.3. Technical Support	9
1.3.1. One-Click Diagnostic Feature	9
2. SafeStorage Encryption	10
2.1. Workflow	11
2.1.1. Enable Security	12
2.1.2. Change Security	13
2.1.3. Create a Secured RAID	13
2.1.4. Disable Security	13
2.1.5. Import SafeStorage Encryption	14
3. UEFI Command Line Utility	15
3.1. Start the UEFI Command Line Utility	17
3.2. Help Command	18
3.2.1. Show the Generic Help Command	18
3.3. Info Command	19
3.3.1. Show the Physical Device Information	19
3.3.2. Show the Logical Device Information	20
3.4. Quit Command	21
3.4.1. Quit the UEFI Command Line Utility	21
3.5. Exit Command	22
3.5.1. Exit the UEFI Command Line Utility	22
3.6. Create Command	23
3.6.1. Create a RAID Array	24
3.7. Delete Command	25
3.7.1. Delete a RAID Array	25
3.8. Flashing the UEFI	26
4. UEFI HII Utility	27
4.1. Start the UEFI HII Utility	27
4.2. UEFI HII Utility Menu View	29
4.2.1. View the Controller Information	29
4.2.2. View the Physical Device Information	30
4.2.3. View the Logical Device Information	30
4.2.4. Create a RAID array	31
4.2.5. Delete a RAID array	33
5. Install the HighPoint Software	34

5.1. Install the driver on Windows	38
5.1.1. Uninstall the driver on Windows	39
5.2. Install the RAID Management on Windows	41
5.2.1. Uninstall the RAID Management on Windows	41
5.3. Install the driver on Linux	42
5.3.1. Uninstall the driver on Linux	43
5.4. Install the RAID Management on Linux	44
5.4.1. Uninstall the RAID Management on Linux	44
5.5. Install the driver on macOS	45
5.5.1. Uninstall the driver on macOS	49
5.6. Install the RAID Management on macOS	50
5.6.1. Uninstall the RAID Management on macOS	51
6. Web RAID Management Interface	52
6.1. Start the WebGUI	52
6.2. Global View	53
6.2.1. HBA Properties	53
6.2.2. Storage Properties	53
6.3. Physical	54
6.3.1. Controller Information	54
6.3.2. Enclosure Information	55
6.3.3. Physical Devices Information	56
6.3.4. Update the Firmware	61
6.3.5. Secure Setting	62
6.3.6. Rescan the Physical Device	63
6.4. Logical	64
6.4.1. Logical Device Information	64
6.4.2. Physical Device Information	67
6.4.3. Create a RAID Array	68
6.4.4. Delete a RAID Array	70
6.4.5. Unplug a RAID Array	71
6.4.6. Verify a RAID Array	72
6.4.7. Add a Spare Disk	73
6.4.8. Remove a Spare Disk	74
6.5. Setting	75
6.5.1. System Setting	76
6.5.2. Password Setting	78
6.5.3. Email Setting	79
6.6. Event	85
6.6.1. View the Event Log	85
6.6.2. Save the Event Log	86
6.6.3. Event Log Icon Guide	87
6.7. SHI	88
6.7.1. View the SHI Information	88

6.7.2. View the SMART Information	89
6.7.3. Set the Temperature Threshold	90
6.7.4. Create a Health Inspector Scheduler	91
6.7.5. Create a New Verify Task	92
6.7.6. Delete a Task	93
6.8. Help	94
6.8.1. Online Help	94
6.8.2. Diagnostic View	94
6.8.3. Save the Diagnostic Log	95
7. Command Line Interface	100
7.1. Start the CLI	100
7.2. Query Commands	102
7.2.1. Query Controller	103
7.2.2. Query Enclosure	104
7.2.3. Query Device	105
7.2.4. Query Array	108
7.3. Init Commands	110
7.3.1. Init a Physical Disk	110
7.3.2. Init a RAID Array	111
7.4. Create Command	112
7.4.1. Create a RAID Array	114
7.4.2. Create a Spare Disk	114
7.5. Delete Command	115
7.5.1. Delete a RAID Array	115
7.5.2. Delete a Spare Disk	116
7.6. Rebuild Command	117
7.6.1. Rebuild a RAID array	117
7.6.2. Start Rebuilding the RAID Array	118
7.6.3. Stop Rebuilding the RAID Array	118
7.7. Verify Command	119
7.7.1. Start Verifying the RAID Array	119
7.7.2. Stop Verifying the RAID Array	119
7.8. Rescan Command	120
7.8.1. Rescan the Physical Devices	120
7.9. Lscard Command	121
7.9.1. Lscard all AICs	121
7.10. Events Command	122
7.10.1. View the Event Log	122
7.10.2. Save the Event Log	123
7.11. Mail Command	124
7.11.1. Add a Mail Recipient	125
7.11.2. List all Mail Recipients	125
7.11.3. Test the mail recipient	126

7.11.4. Delete a Mail Recipient	126
7.11.5. Add a Mail Server	127
7.11.6. List all Mail Servers	127
7.11.7. Set the Mail Server	127
7.12. Task Command	128
7.12.1. Create a New Rebuild Task	129
7.12.2. Create a New Verify Task	129
7.12.3. List all Tasks	129
7.12.4. Delete a Task	130
7.13. Set Command	131
7.13.1. Set Auto Rebuild	133
7.13.2. Set Continue Rebuilding On Error	134
7.13.3. Set Audible Alarm	134
7.13.4. Set Rebuild Priority	134
7.13.5. Set Restrict to localhost access	135
7.13.6. Set Temperature Threshold	135
7.13.7. Set Temperature Unit	135
7.13.8. Set Collecting System Logs	136
7.13.9. Set Password	136
7.13.10. Set AIC Fan Speed	136
7.14. Unplug Command	137
7.14.1. Unplug the Physical Device	137
7.14.2. Unplug a RAID Array	138
7.15. Secure Command	139
7.15.1. Enable AIC Security	140
7.15.2. Change AIC Security key	140
7.15.3. Disable AIC Security	141
7.15.4. Enable Disk Security	141
7.15.5. Change Disk Security key	142
7.15.6. Disable Disk Security	142
7.16. Diag Command	143
7.16.1. Collect the Diagnostic Information	143
7.17. Switch Command	144
7.17.1. Switch the AIC	144
7.18. Update Command	145
7.18.1. Update the Firmware	145
7.19. Help Command	146
7.19.1. Show the Generic Help Command	146
7.19.2. Show the Specific Command Help	147
7.20. Ver Command	148
7.20.1. Show the RAID Management Version	148
7.21. Exit Command	149
7.21.1. Exit the CLI	149
7.22. Clear Command	150

- 7.22.1. Clear the CLI screen 150
- 8. Troubleshooting151**
 - 8.1. Fail to compile gcc, make and other driver files151**
 - 8.1.1. For Debian 151
 - 8.1.2. For RHEL 153
 - 8.1.3. For Ubuntu 154
 - 8.1.4. For Proxmox 155
 - 8.2. No supporting host adapter is found 157**
 - 8.3. No supported controller detected157**
- 9. Glossary 158**
- 10. Revision History 161**
 - 10.1. Version 1.00, July 9, 2024 161**
 - 10.2. Version 1.01, August 13, 2024 161**
 - 10.3. Version 1.02, August 28, 2024 161**

1. Overview

This document is the primary reference and user guide for the HighPoint NVMe RAID AIC. This document contains the complete using the HighPoint Web RAID Management Interface (WebGUI), CLI (command line interface) utility, UEFI utility, and SafeStorage SED Solution.

1.1. General Features of the NVMe RAID AIC

- RAID levels: 0, 1, 10, Single
- Single-RAID or multi-RAID arrays per AIC
- Cross-Sync RAID solution across AICs
- Multiple RAID partitions supported
- TRIM RAID support
- Data RAID support
- WebGUI (Browser-Based management tool)
- CLI (Command Line Interface- scriptable configuration tool)
- API package
- Fast initialization for quick array setup
- Check Consistency for background data integrity
- Automatic and configurable RAID Rebuilding Priority
- Auto resume incomplete rebuilding after power on or reboot system
- Self-monitoring, Analysis, and Reporting Technology (S.M.A.R.T) support
- Storage Health Inspector
- SMTP Email Alert Notification
- Online Array Roaming
- Global Hot Spare Disk support

1.2. Advanced Features of the NVMe RAID AIC

The following table lists the advanced features and the NVMe RAID AICs that support them.

Table 1: Features and support NVMe RAID AICs

Advanced Features	Support NVMe RAID AICs
SSD HotPlug Support	SSD6780A/ SSD7580B/ SSD7580C
LED Indicators	SSD6444/ SSD6444M/ SSD6540/ SSD6540M/ SSD6780A/ SSD7749M/ RS6542AW/ RocketAIC7749MWSeries
Fan Control	SSD7101A-1/ SSD7104/ SSD7104F/ SSD7105/ SSD7140A/ SSD7180/ SSD7184/ SSD7202/ SSD7502/ SSD7505/ SSD7540/ SSD7580A/ SSD7580B/ SSD7580C/ SSD6444/ SSD6444M/ SSD6540/ SSD6540M/ SSD6780A/ RS6542AW/ RocketAIC7105HWSeries/ RocketAIC7140AWSeries/ RocketAIC7502HWSeries/ RocketAIC7505HWSeries/ RocketAIC7540HWSeries/ RS6542AW
SafeStorage Encryption	SSD7580C/ SSD7749M/ SSD7749M2/ SSD7749E/ SSD6780A/ RS6542AW/ RA7105HW-A04T0-03/ RA7502HW-A02T0-03/ RA7502HW-A04T0-00/ RA7502HW-A08T0-09/ RA7505HW-A04T0-03/ RA7505HW-A08T0-00/ RA7505HW-A04T0-0D/ RA7505HW-A08T0-0E/ RA7505HW-A16T0-0F/ RA7540HW-A16T0-00/ RA7540HW-A16T0-0E/ RA7540HW-A32T0-0F/ RA7749EW-K15T3-0A/ RA7749EW-K30T7-0B/ RA7749EW-K61T4-0C/ RA7749MW-A32T0-0F
Boot RAID Support	SSD7105/ SSD7202/ SSD7502/ SSD7505/ SSD7540/ SSD7580A/ SSD7580B/ SSD7580C/ SSD7749E/ SSD7749M/ SSD7749M2/ SSD6780A/ RS6542AW RocketAIC 7105HWSeries/ RocketAIC 7502HWSeries RocketAIC 7505HWSeries/ RocketAIC 7540HWSeries RocketAIC 7749EWSeries/ RocketAIC 7749MW Series RocketAIC7749M2WSeries
UEFI HII Utility	SSD7105/ SSD7202/ SSD7502/ SSD7505/ SSD7540/ SSD7580A/ SSD7580B/ SSD7580C/ SSD7749E/ SSD7749M/ SSD7749M2/ SSD6780A/ RS6542AW RocketAIC 7105HWSeries/ RocketAIC 7502HWSeries RocketAIC 7505HWSeries/ RocketAIC 7540HWSeries RocketAIC 7749EWSeries/ RocketAIC 7749MW Series RocketAIC7749M2WSeries
Flash ROM for Upgradeable UEFI	SSD7105/ SSD7202/ SSD7502/ SSD7505/ SSD7540/ SSD7580A/ SSD7580B/ SSD7580C/ SSD7749E/ SSD7749M/ SSD7749M2/ SSD6780A/ RS6542AW

	<p>RocketAIC 7105HWSeries/ RocketAIC 7502HWSeries</p> <p>RocketAIC 7505HWSeries/ RocketAIC 7540HWSeries</p> <p>RocketAIC 7749EWSeries/ RocketAIC 7749MW Series</p> <p>RocketAIC7749M2WSeries</p>
--	--

1.3. Technical Support

For assistance with using your HighPoint NVMe RAID AIC, please contact our [Technical Support Department](#).

1.3.1. One-Click Diagnostic Feature

One-Click Diagnostic is a unique feature of our HighPoint RAID Management. One-Click Diagnostic provides an information collection system for troubleshooting. It will gather all necessary hardware, software, and storage configuration data and compile it into a single file, which can be transmitted directly to our FAE Team via our [Online Support Portal](#).

2. SafeStorage Encryption

Overview

The SafeStorage Encryption (SED) service uses a secured key to encrypt data stored on SED-capable disks. Without the corresponding security key, the encrypted data becomes inaccessible. This approach ensures the confidentiality of data in the event of disk theft, loss, or removal.

The SafeStorage solution, developed by HighPoint, seamlessly integrates with industry-standard Self-Encrypted Drive (SED) technology and complies with OPAL v2.0. It supports M.2 and U.2/U.3 NVMe media, adhering to the specifications outlined by the OPAL SSC TCG (Trusted Computing Group). The objective is safeguarding data assets by preventing unauthorized access to stored information when physical drives are misplaced or stolen.

The SafeStorage solution applies to both single-disk and RAID configurations. Activation is facilitated through Disk Security, which can be easily managed via our HighPoint RAID Management.

Benefits

Numerous customers are actively seeking a comprehensive and efficient storage encryption solution to ensure the security of their data. To fulfill this urgent need, we recommend SafeStorage Encryption. By simply setting a security key, you can significantly reduce the risk of data loss and provide solid protection for valuable information assets.

In addition, SafeStorage Encryption also supports Cryptographic erase, which further enhances effective data erasure and disk reuse. We are confident that by adopting SafeStorage Encryption, you will be able to better meet the increasingly complex data security challenges and support your organization's robust development.

2.1. Workflow

Overview

The SafeStorage can be operated in WEBGUI. The specific operation process is as follows:

1. Use the disk that has SED (self-encrypting disk) capability.
2. [Enable AIC security](#) and create a security key that conforms to the security requirements.
3. [Enable disk security](#). The key used to secure the disk is the same as the key generated when the board is secured.
4. [Enable RAID security](#) when creating RAID with disks that have SED (self-encrypting disk) capability.

Please refer to the sections for the steps in the above process.

2.1.1. Enable Security

You can enable security on the AIC. To enable AIC security, you need to generate and configure a security key on the AIC. The security key is a unique identifier used to authenticate the AIC and protect from unauthorized access. The AIC security key you create will also serve as the disk security key, written to the disk or array.

After you enable AIC security, you can enable disk security using a security key.

Enable AIC Security

If you want to use SafeStorage, you must first enable AIC security option using the HighPoint RAID Management utility (WebGUI or CLI) and create a security Key.



Warning: Be sure to make a record of your AIC security key. If the security key is lost or forgotten, you will lose access to any encrypted data stored on the disk or RAID array.

Enable Disk Security

SafeStorage can only be used with storage media that has SED (self-encrypting disk) capability.

As mentioned previously, the disk security key is automatically generated when the AIC security key is created and will be written to the disk. These keys are identical. You only need to enable disk security.

There are two situations in which Disk Security can be enabled.

- Situation 1: Enabling Disk Security for disks with the Legacy status
- Situation 2: Enabling Disk Security when creating a RAID array

2.1.2. Change Security

You can change the security key on the AIC, and you can change the disk security key.

[Change AIC Security](#)

If you want to change the AIC security key, you must provide the old AIC security key.

When the AIC security key is changed to the new key, the disk security key is automatically changed to the same new key and written to the secured disk.

[Change Disk Security](#)

If the AIC and disk security keys do not match, you cannot access data stored on the disk or array. To resolve the password inconsistency, you need to change the disk security key to one that matches the current AIC so that you can access the data stored on the disk or RAID array.

To explain, there are two situations in which the AIC security key and disk security key will not match:

- Situation 1: The disk is from another AIC.
- Situation 2: The disk or array was not present when the AIC security key was changed.

2.1.3. Create a Secured RAID

Select the secured or unsecured disks to create a secure RAID and check the **secure** function.

2.1.4. Disable Security

If you disable security, there are two steps you need to follow.

1. Disable disk security using the Cryptographic Erase option.
2. Disable AIC security using the Disable Security option.

[Disable Disk Security](#)

If you want to disable disk security, use Cryptographic Erase.



Warning: Cryptographic erase will delete the Security (Encryption) key from the target disk/ array members. Data stored on these SSDs will no longer be accessible.

[Disable AIC Security](#)

We offer the “Disable Security” option to disable AIC security. The AIC security can only be disabled if the target AIC does not host any secured disks with the “legacy” status or secured arrays.



Warning: After disable AIC security, data stored on these secured disks will no longer be accessible.

2.1.5. Import SafeStorage Encryption

One of the features of all HighPoint RAID AIC is Online Array Roaming. Information about the RAID configuration is stored on the physical drives. So, if the AIC fails, you wish to use another AIC, or the drives to be moved to a different AIC, the RAID configuration data can still be read by another HighPoint RAID AIC. There are three situations:

- Situation 1: If the disks and HighPoint RAID AIC are not secured. You can do Online Array Roaming directly.
- Situation 2: If the disk security key and the HighPoint RAID AIC security key are the same. You can do Online Array Roaming directly.
- Situation 3: If the disks and HighPoint RAID AIC are secured and their security key does not match. You modify the AIC security key to match the disk security key or back up the data in the RAID, delete the RAID, and then create a new RAID on the AIC.

Note: The prerequisite for using this feature is that both AICs use the same AIC type. You can contact our FAE Team via our [Online Support Portal](#) for assistance.

3. UEFI Command Line Utility

Overview

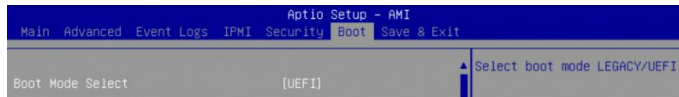
The UEFI (Unified Extensible Firmware Interface) command line utility is provided in a binary format, and no separate installation is required.

Prerequisites

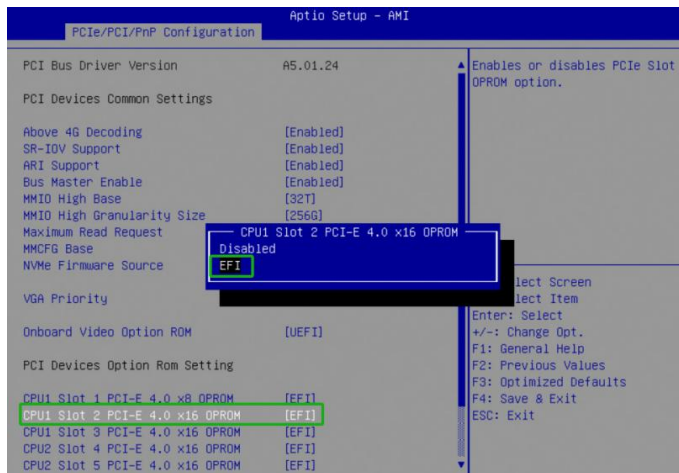
1. The AIC must be installed into a PCIe slot.
2. The motherboard needs to be booted into UEFI mode. Confirm that the motherboard boots in UEFI mode.

Example: SuperMicro X12DPi-N6 motherboard

1) Set **Boot Mode Select** to **UEFI**.



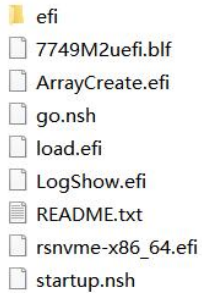
2) Set the **Slot** where the AIC is located to **EFI**.



3) Save changes and reboot.

3. A USB flash drive in FAT32 format. The UEFI package must be unzipped directly to the root directory of this flash drive. (Do not extract the contents in a new folder.)

Example: SSD7749M2

A file explorer view showing the contents of the 'efi' directory. The directory is represented by a yellow folder icon. Below it, several files are listed with their respective icons: a document icon for '7749M2uefi.blf', 'ArrayCreate.efi', 'go.nsh', 'load.efi', 'LogShow.efi', and 'startup.nsh'; a document icon with horizontal lines for 'README.txt'; and a document icon with a small square symbol for 'rsnvme-x86_64.efi'.

efi

- 7749M2uefi.blf
- ArrayCreate.efi
- go.nsh
- load.efi
- LogShow.efi
- README.txt
- rsnvme-x86_64.efi
- startup.nsh

- **7749M2uefi.blf** -- UEFI BLF file for SSD7749M2.
- **ArrayCreate.efi** -- EFI utility.
- **go.nsh** -- Batch file for flash loader.
- **load.efi** -- Flash utility for EFI environment.
- **LogShow.efi** -- EFI file for log.
- **README.txt** -- Includes an introduction to the UEFI, basic usage, etc.
- **rsnvme-x86_64.efi** -- EFI file for debug.
- **startup.nsh** -- Find USB driver.

3.1. Start the UEFI Command Line Utility

1. Insert the USB flash drive and NVMe RAID AIC into the motherboard and boot the system.
2. Enter the motherboard's BIOS and select the **UEFI: USB flash drive** in the BIOS startup item.

```
Boot Override
SanDisk
BRCM MBA Slot 4500 v20.14.2
UEFI: SanDisk, Partition 1
```

3. At the prompt, enter the following command to change the resolution:

mode 100 31

```
FS0:\> mode
Available modes for console output device.
Col   80 Row   25  *
Col   80 Row   50
Col  100 Row   31
Col  240 Row   56
FS0:\> mode 100 31_
```

Note: This command is used to adjust the screen resolution, please adjust it according to the actual situation of your motherboard.

4. Enter the following command to enter the UEFI command line:

ArrayCreate.efi

```
FS1:\> ArrayCreate.efi
Highpoint RAID utility for UEFI (version: 20230322)
Open handles: 1
=== Controller information:
Vendor: HighPoint Technologies, Inc.
Product: SSD7749M2 NVMe Controller (774a)
```

3.2.Help Command

```
>>> Please specify command to execute:
<<< help_
```

If you input an unknown or error command, you will be told that the command is unknown; you can use help commands to find the correct commands.

The following table lists and describes the properties of the help command.

Table 2: Properties for help Commands

cmd	Property Name	Description
H	N/A	This command shows generic help about this utility.
h		
help		

3.2.1.Show the Generic Help Command

<<<H/ h/ help

This command shows generic help about this utility.

Input example:

```
<<<help
```

```
create RAID0 * *
  create RAID0 array with all disks and with maximum capacity.
create RAID1 1/1,1/3 10
  create RAID1 array with disk 1/2 and 1/3 and with 10GB capacity.
create RAID10 *
  create RAID10 array with all disk and with maximum capacity.
create RAID5 * 40
  create RAID5 array with all disk and with 40GB capacity.
create RAID5 1/2,1/3,1/1 50
  create RAID5 array with disk 1/2,1/3 and 1/1 and with 50GB capacity.
create RAID50,4 1/1,1/2,1/3,1/4,1/5,1/6,1/7,1/8
  create RAID50 array with disk 1/1,1/2,1/3,1/4,1/5,1/6,1/7,1/8 and with sub member count
4.

delete ArrayIndex
  delete 1
    Delete the first array from Logical device list.
  delete 2
    Delete the second array from Logical device list.

info
  display physical device list and logical device list

Q/q/quit/exit
  quit the application

H/h/help
  this help message
```

3.3.Info Command

```
>>> Please specify command to execute:
<<< info
```

You can use the info command to view the NVMe RAID AIC status and disks information.

The following table lists and describes the properties of the info command.

Table 3: Properties for info Commands

cmd	Property Name	Description
info	N/A	This command shows the NVMe RAID AIC status and disks information.

3.3.1.Show the Physical Device Information

<<<info

Disks hosted by the AIC will appear here

Input example:

```
<<<info
```

```
<<< info
=====
==== Physical device list(count 4):
1/1 Samsung SSD 980 PRO 1TB-S5GXXN1W506237F, 1000204MB(MaxFree 0MB), Normal
1/2 KXG802N84T09 KIOXIA-4122X2BFA00WFU26, 4096805MB(MaxFree 0MB), Normal
1/3 HP-EM2802TOGHTCB58R-E264-2311270010002, 2000398MB(MaxFree 0MB), Normal
1/4 KXG602NV1T02 TOSHIBA-694S100MTV0Q, 1024209MB(MaxFree 0MB), Normal
```

- **Location** – The physical disk location (e.g., 1/2 represents the disk on AIC 1 port2)
- **Model** – The model number of the physical disk.
- **Capacity** – The total capacity of the physical disk.
- **Max Free** – The space on the physical disk is not configured in an array.
- **Status** – The status of the physical disk.

3.3.2. Show the Logical Device Information

<<<info

Disks and arrays you create and the properties associated with them will appear here.

Input example:

<<<info

```
==== Logical device list(count 1):
 1 [VD24-4] RAID0_000041A7 (RAID0), 4000493MB (Stripe 512KB), Normal
  1/1 Samsung SSD 980 PRO 1TB
  1/2 KXG80ZNB4T09 KIOXIA
  1/3 HP-EM2802T0GMTCB58R-E264
  1/4 KXG60ZNV1T02 TOSHIBA
```

- **Name** – The name of the arrays you created.
- **Type** – The RAID level of the arrays you created.
- **Capacity** – The total capacity of the array.
- **Stripe** – The block size of the arrays you created.
- **Status** – The status of the array.
- **Member disk** – The member disk of the array.

3.4. Quit Command

```
>>> Please specify command to execute:  
<<< quit_
```

Quit the UEFI Command Line Utility.

The following table lists and describes the properties of the quit command.

Table 4: Properties for quit Commands

cmd	Property Name	Description
Q	N/A	This command allows you to quit the UEFI Command Line Utility.
q		
quit		

3.4.1. Quit the UEFI Command Line Utility

<<<Q/ q/ quit

This command allows you to quit the UEFI Command Line Utility.

Input example:

```
<<<quit
```

3.5.Exit Command

```
>>> Please specify command to execute:  
<<< exit_
```

Exit the UEFI Command Line Utility.

The following table lists and describes the properties of the exit command.

Table 5: Properties for exit Commands

cmd	Property Name	Description
exit	N/A	This command allows you to exit the UEFI Command Line Utility.

3.5.1.Exit the UEFI Command Line Utility

<<<exit

This command allows you to exit the UEFI Command Line Utility.

Input example:

```
<<<exit
```

3.6. Create Command

```
>>> Please specify command to execute:
<<< create_
```

You can use create commands to create a new RAID array.

Note: RocketAIC series NVMe AIC SSDs are already pre-configured with RAID0. You can skip those steps. You can follow the steps if you want to use another type of RAID.

The following table lists and describes the properties of the create command.

Table 6: Properties for create Command

cmd	Property Name	Value Range	Description
create	ArrayType	RAID0 RAID1 RAID10	Specify the RAID level to be created. The AIC supports RAID levels 0, 1, and 10.
	disks	MemberDiskList	Specifies member disks that will compose a new array. disks=1/2,1/3...or disks=* * Indicates creation of RAID array using all member disks.
	capacity	capacity	Specify the capacity of the target array. capacity=10MB/1000MB...or capacity=* * Indicates creation of RAID array using all disk capacities.

3.6.1. Create a RAID Array

<<<create ArrayType (RAID0/RAID1/RAID10) MemberDiskList (1/1,1/2|*) Capacity(100|*)

This command allows you to create a new RAID array.

Input example:

```
<<<create RAID1 1/1,1/3 10
```

```
<<< create RAID1 1/1,1/3 10
  Creating array: RAID1_10D63AF1.
  Array created successfully.
=====
==== Physical device list(count 4):
1/1 Samsung SSD 980 PRO 1TB-S5GXNX1W506237F, 1000123MB(MaxFree 990123MB), Normal
1/2 KXGB02N84T09 KIOXIA-4122X2BFA00WFU26, 4096727MB(MaxFree 4096727MB), Normal
1/3 HP-EM2802TOGHTCB58R-E264-2311270010002, 2000313MB(MaxFree 1990313MB), Normal
1/4 KXG60ZNV1T02 TOSHIBA-694S100MTVDQ, 1024081MB(MaxFree 1024081MB), Normal
==== Logical device list(count 1):
1 [VD24-5] RAID1_10D63AF1 (RAID1), 10000MB (Stripe 512KB), Normal
  1/1 Samsung SSD 980 PRO 1TB
  1/3 HP-EM2802TOGHTCB58R-E264
```

3.7.Delete Command

```
>>> Please specify command to execute:
<<< delete_
```

You can use delete command to delete an existing RAID array.

After deletion, the original array and all data will be lost. All the member disks will be listed as available single disks.

The following table lists and describes the properties of the delete command.

Table 7: Properties for delete Command

cmd	Property Name	Value Range	Description
delete	{array_id}	The created RAID array	This command instructs the system to delete the array.

3.7.1.Delete a RAID Array

<<<delete {array_id}

This command allows you to delete an existing RAID array.

Input example:

```
<<<delete 1
```

```
1 [VD24-4] RAID0_000041A7 (RAID0), 4000493MB (Stripe 512KB), Normal
  1/1 Samsung SSD 980 PRO 1TB
  1/2 KXG802N84T09 KIOXIA
  1/3 HP-EM2802TOGMTCB58R-E264
  1/4 KXG602NV1T02 TOSHIBA
-----
>>> Please specify command to execute:
<< delete 1
  Deleting array: RAID0_000041A7 idx 0 5
<<<<< hpt_delete_array: id 5 options 2
  Array deleted successfully.
=====
=== Physical device list(count 4):
1/1 Samsung SSD 980 PRO 1TB-S5GXXN1W506237F, 1000123MB(MaxFree 1000123MB), Normal
1
1/2 KXG802N84T09 KIOXIA-4122X2BFA00WFU26, 4096727MB(MaxFree 4096727MB), Normal
1/3 HP-EM2802TOGMTCB58R-E264-2311270010002, 2000313MB(MaxFree 2000313MB), Normal
1/4 KXG602NV1T02 TOSHIBA-694S100MTVDQ, 1024081MB(MaxFree 1024081MB), Normal

==== Logical device list(count 0):
-----
```

3.8. Flashing the UEFI

You can flash the UEFI in the UEFI interface. This usually involves loading the latest UEFI package onto the motherboard to get the latest feature updates.

1. Enter the motherboard's BIOS and select the UEFI: USB flash drive in the BIOS startup item.

```
Boot Override
SanDisk
BRDM MBA Slot 4500 v20.14.2
UEFI: SanDisk, Partition 1
```

2. Enter the following command to flash the NVMe RAID AIC UEFI: **go.nsh**.

```
Shell> echo -off
Enter go.nsh to flash the UEFI rom.
FS1:\> go.nsh
```

3. When the message **Passed** appears, the flash is successful.

```
FS1:\> load.efi 7749M2uefi.blf /a /f
Load Utility for Flash EPROM v1.1.5
(built at Mar 28 2023 17:27:18)

Set flash size to 256K
Found adapter 0x75401103 at PCI 34:0:0
Offset address 0x0
EPROM Vendor: WINBOND W25X40BV
Erasing .....Succeeded
Flashing ....

Flashing Success (total retry 0)

Verifying ....

Passed !
```

4. Reboot to complete the update process.

4. UEFI HII Utility

Overview

The UEFI HII Utility is a powerful tool. It provides the most flexible and intuitive interface options available to the user and performs other configuration tasks in a BIOS environment. It provides rich functions to help users easily and conveniently query AIC and disk information and configure AIC.

Prerequisites

1. The AIC must be installed into a PCIe slot.
2. The motherboard needs to be booted into UEFI mode. Confirm that the motherboard boots in UEFI mode.

4.1. Start the UEFI HII Utility

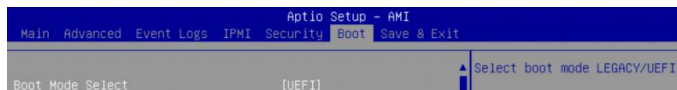
Follow these steps to start the UEFI HII Utility.

Step 1 Adjust System EFI Settings

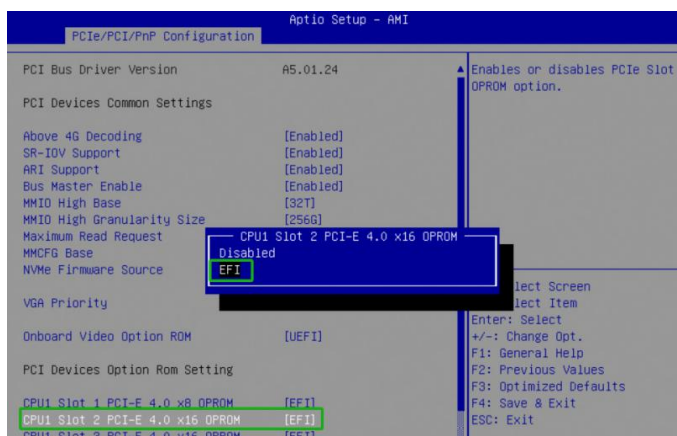
1. Insert the AIC into the motherboard, power on the system, and enter the BIOS.
2. Adjust the UEFI settings. Allow the option ROM settings for third-party devices to load.

Example: SuperMicro X12DPi-N6 motherboard

- 1) Set **Boot Mode Select** to **UEFI**.



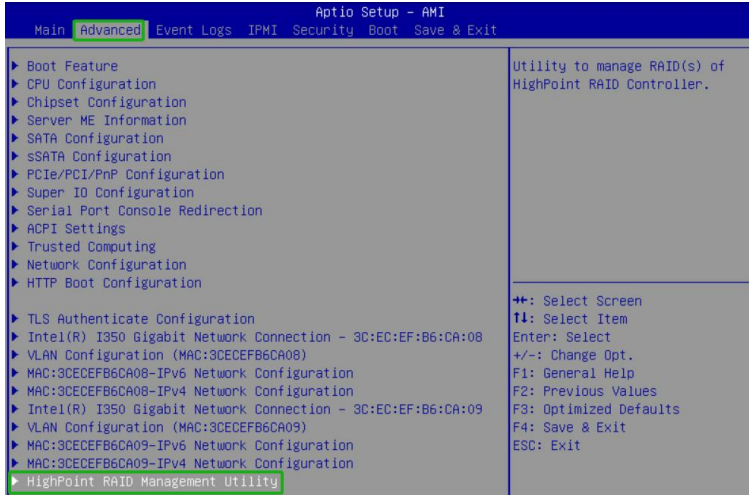
- 2) Set the **Slot** where the AIC is located to **EFI**.



3. Save changes and reboot.

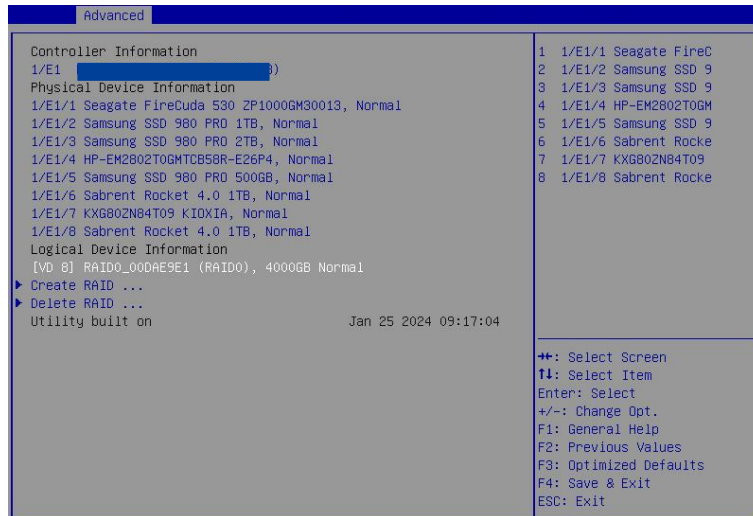
Step 2 Enter the UEFI HII Utility

1. Power up the system.
2. Press **Delete** to enter BIOS.
3. Find **Advanced**→**HighPoint RAID Management Utility** should appear under **Advanced** options.



4. Select **HighPoint RAID Management Utility** and enter it.

4.2.UEFI HII Utility Menu View



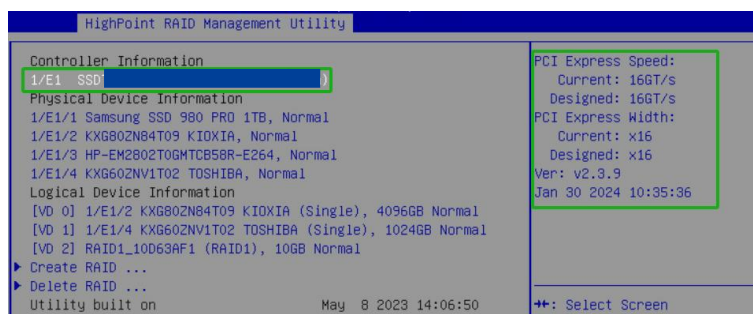
Keys

The UEFI HII Utility utilizes the following keys:

- **Arrow keys** – Use these to move between different menu items.
- **Enter** – Open the selected toolbar command/execute the selected command.
- **N or Esc** – Return to the previous menu, cancel the selected operation, or exit the BIOS Utility.

4.2.1.View the Controller Information

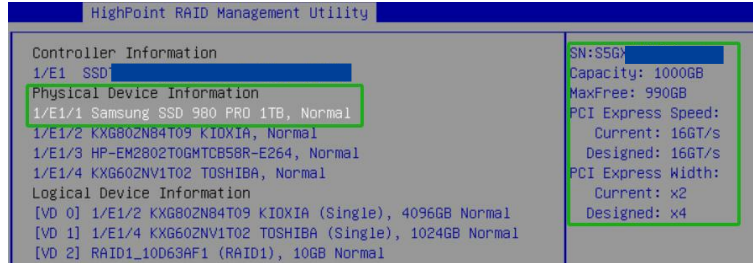
The UEFI HII Utility view allows you to view the Controller Information. The AIC that has been connected to the system will appear here.



- **Location** – The AIC location (example: 1/E1 represents the AIC1, AIC with ID 1)
- **Model** – The model name of the AIC connected.
- **PCI Express Speed** – The rate of current bandwidth and the rate of designed bandwidth.
- **PCI Express Width** – The current AIC occupies the PCIe width, and the designed AIC occupies the PCIe width.
- **Version** – The UEFI HII Utility version of the AIC.

4.2.2. View the Physical Device Information

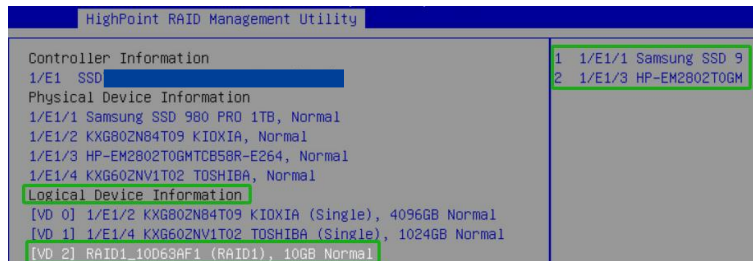
The UEFI HII Utility view allows you to view the Physical Device Information. The disks hosted by the AIC will appear here.



- **Location** – The disk location. (example: 1/E1/2 represents the AIC1, Port2)
- **Model** – The model number of the disk connected.
- **Status** – The (Normal) status of the disk.
- **SN** – The serial number of the physical disk.
- **Capacity** – The total capacity of the disk.
- **Max Free** – The total capacity that is not configured.
- **PCI Express Speed** – The current bandwidth rate and the designed rate.
- **PCI Express Width** – The current disk occupies the PCIe bandwidth, and the designed disk occupies the PCIe bandwidth.

4.2.3. View the Logical Device Information

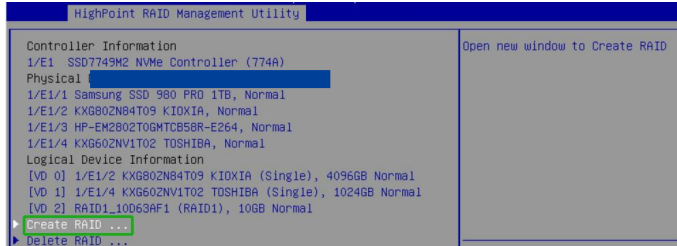
The UEFI HII Utility view allows you to view the Logical Device Information. The disks and arrays you create and their associated properties will appear here.



- **Name** – The name of the arrays you create.
- **Type** – The RAID level of the arrays you create.
- **Capacity** – The total capacity of the disk.
- **Status** – The (Normal, critical, disabled) status of the disk.
- **Member disk** – The member disk of the arrays.

4.2.4. Create a RAID array

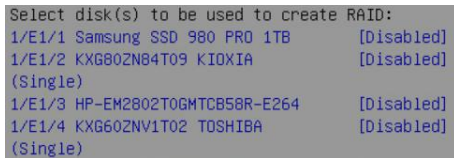
The UEFI HII Utility view allows you to create the RAID array.



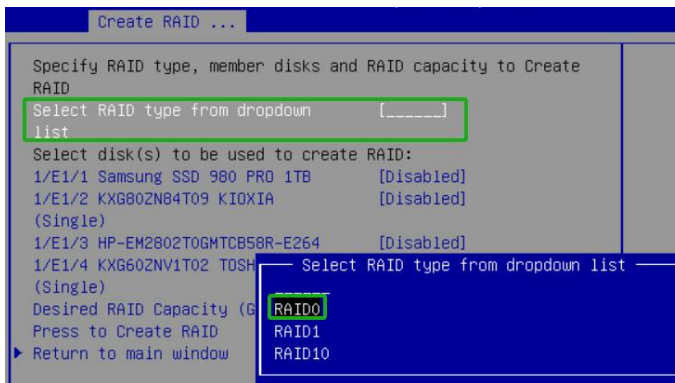
Note: RocketAIC series NVMe AIC SSDs are already pre-configured with RAID0. You can skip those steps. You can follow the steps if you want to use another type of RAID.

To create a RAID, perform the following steps:

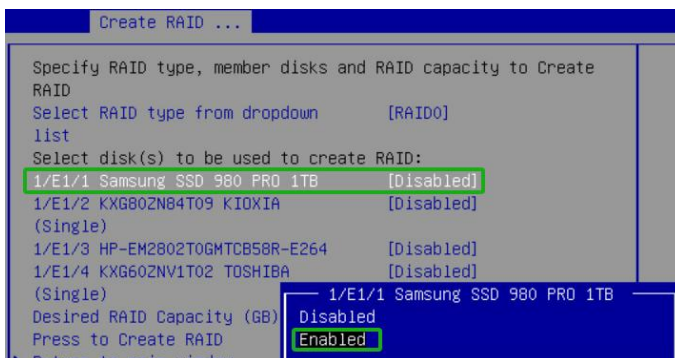
1. Select **Create RAID...** from the HighPint RAID Management Utility.
2. On the **Create** menu. A disk list will appear, and all available disks will be displayed.



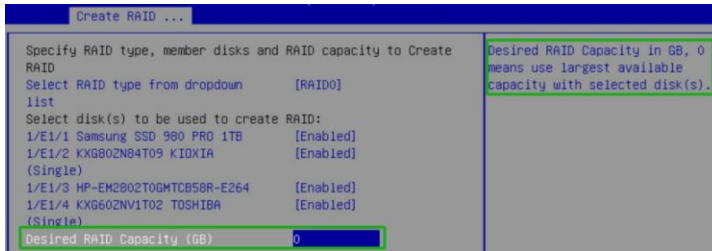
3. Select the **RAID type** from the dropdown list. Use the keyboard or mouse's up and down keys to select the RAID type and press **Enter**.



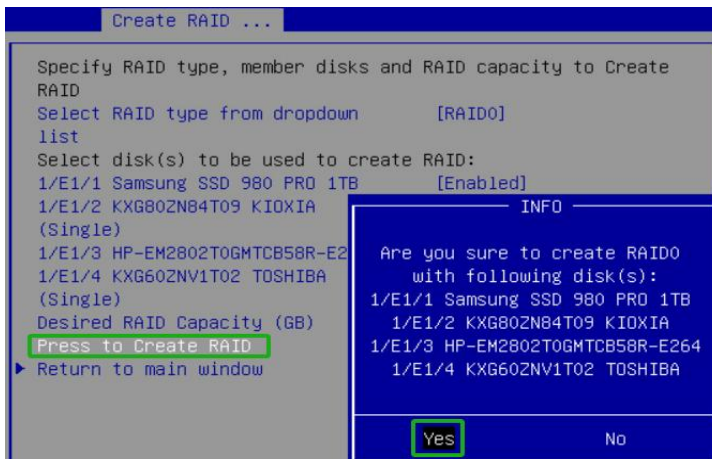
4. Select the disk that needs to create a RAID array and the status of the disk changes from **Disabled** to **Enabled**.



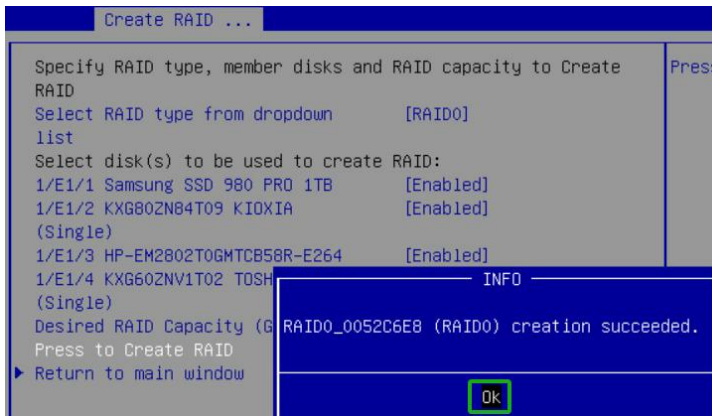
- Use the keyboard to input the space (GB) you want to set aside for this array. You can decide how much storage capacity will be assigned to the array.



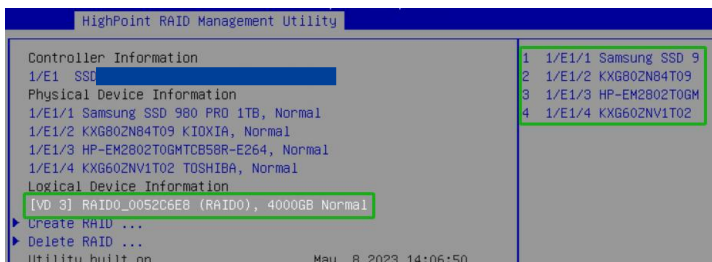
- Select and **press to create RAID** to complete the RAID Array creation. A pop-up window prompt: **Are you sure to create RAID0 with following disk(s)**. Press **Enter** to confirm.



- A pop-up window will state that **RAID*** creation succeeded**. Press **Enter** to confirm the operation again.

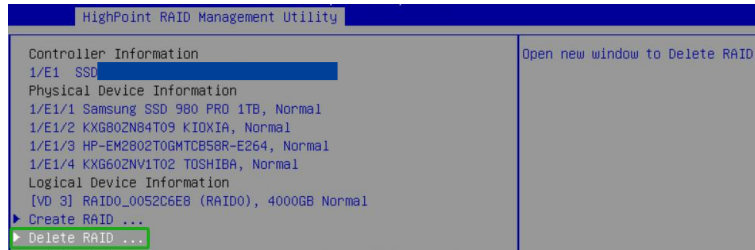


- The array you create, and its associated properties will appear under the **Logical Device Information**.



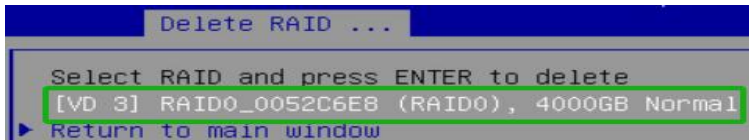
4.2.5. Delete a RAID array

The UEFI HII Utility view allows you to delete the created RAID array.



To delete a RAID, perform the following steps:

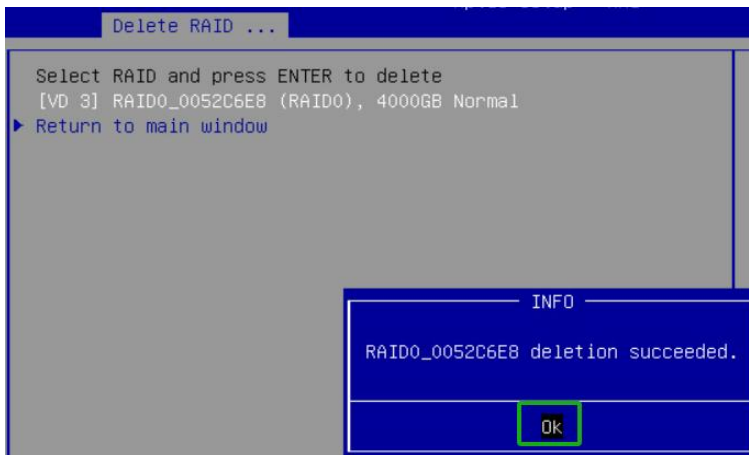
1. Select **Delete RAID...** from the HighPint RAID Management Utility.
2. Select the array you wish to delete and press **Enter**.



3. The utility will display a warning message. Press **Enter** to delete the array.



4. Press **Enter** to confirm the operation again.



5. Install the HighPoint Software

HighPoint Software Overview

The HighPoint Software includes the HighPoint driver and RAID Management.

- **HighPoint driver Overview**

The HighPoint driver is used for the AIC to communicate with the operating system. This driver enables the operating system to recognize AIC, ensuring that it loads and operates correctly in the operating system.

- **HighPoint RAID Management Overview**

The HighPoint RAID Management configures and monitors NVMe SSDs hosted by the AIC.

The HighPoint RAID Management includes two parts:

- Web RAID Management Interface (WebGUI)
- Command Line Interface (CLI)

The Web RAID Management Interface (WebGUI) is a simple and intuitive web-based management tool for Windows and Linux operating systems. It is an ideal interface for customers unfamiliar with RAID technology. The Wizard-like Quick Configuration menu allows even the most novice user to get everything up and running with a few simple clicks. Experienced users can fine-tune configurations for specific applications using the Setting Options menu.

The Command Line Interface (CLI) is a powerful, text-only management interface for advanced users and professional administrators. The universal command lines work with Linux and Windows platforms.

HighPoint Driver Prerequisites

1. The AIC must be installed into a PCIe slot.
2. Ensure any non-HighPoint drivers are uninstalled for SSDs hosted by the AIC. 3rd party software and manufacturer-provided drivers may prevent the AIC from functioning properly.
3. Download the appropriate driver from the AIC's Software Downloads webpage.
4. Secure Boot must be disabled.

- **For Linux operating system**

HighPoint Linux Driver capability has not been signed and certified. If Secure Boot is enabled, the driver will not load.

- 1) Boot the system and access the motherboard BIOS menu.

2) Set **Secure Boot** to **Disabled**.**Warnings:**

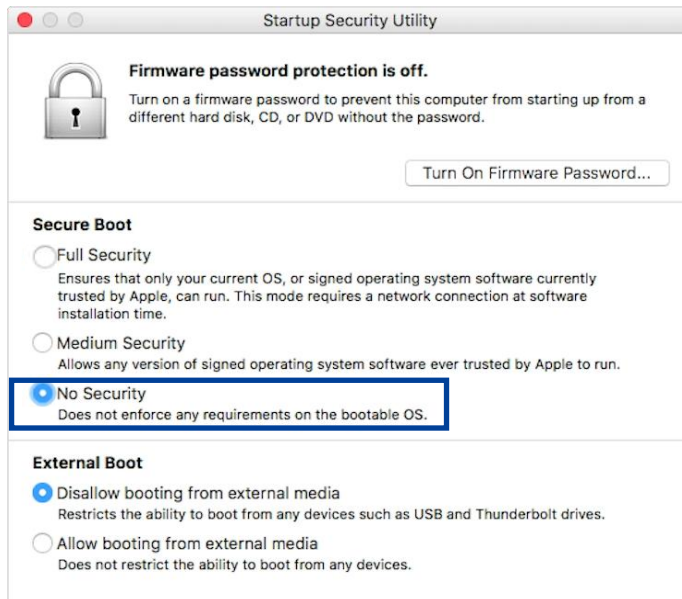
Failing to remove the AIC and SSDs when uninstalling the driver may result in data loss.

Always install the HighPoint NVMe driver before moving the AIC & RAID array to another operating system.

- **For Mac computers with the Apple T2 Security Chip**

The T2 security chip will need to disable the Secure Boot to load drivers for third-party devices. If Secure Boot is enabled, the driver will not load.

- 1) Boot the system and press the **Command (⌘)-R** keys to access the Startup Security Utility.
- 2) Set **Secure Boot** to **No Security**.

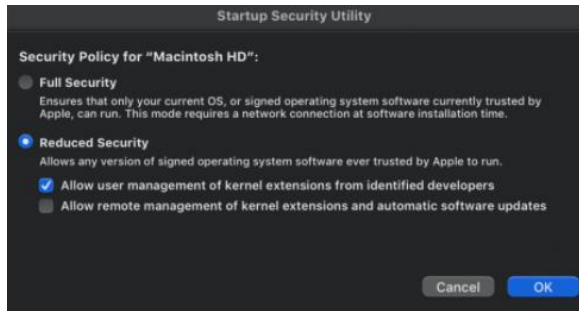


Note: For a list of products with the T2 Security Chipset, please visit the following website: [Mac computers that have the Apple T2 Security Chip](#).

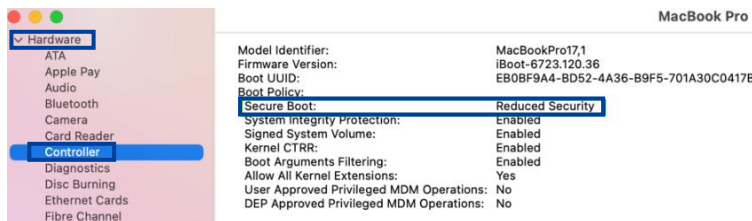
- **For Mac computers with the Apple M1 & M2 Chip**

The Apple M1 & M2 Chip must reduce the Security Policy to load drivers for third-party devices. If not, the driver will not load.

- 1) Turn the system off and hold down the **Power Button** until you see **Loading Startup Options**.
- 2) Set **Startup Security Utility** to **Reduced Security**.



- 3) Click the **Apple** logo in the upper left-hand corner of the desktop and select **Restart** to reboot the system.
- 4) Check the system's Security Policy settings: **System Information** → **Hardware** → **Controller** → **Boot Policy**.



Note: Mac computers with Apple M1 & M2 chips, please visit the following website:
[Mac computers that have the Apple M1 & M2 Chip](#)

- **For macOS 10.13x and earlier**

The SIP (System Integrity Protection) must be disabled. If the SIP is enabled, the older macOS versions prevent the driver from loading.

- 1) macOS enters System Recovery mode.
 - **For Mac with an Intel chip**

Boot the system and hold down the **Command (⌘)-R** keys until the macOS enters System Recovery mode.

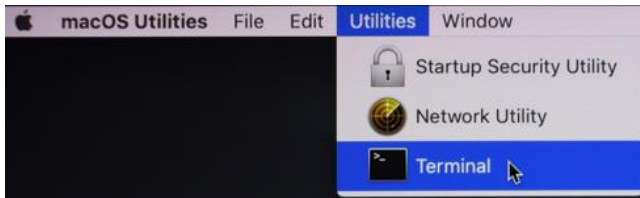


Note: Make sure you are using a wired keyboard and mouse for this procedure. Wireless devices may not be recognized or function properly when booting into the Recovery mode.

- **For Mac with an Apple M1/ M2 chip**

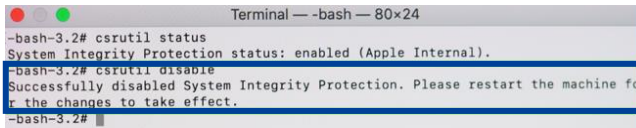
Turn the system off and hold down the **Power Button** until the macOS enters System Recovery mode.

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

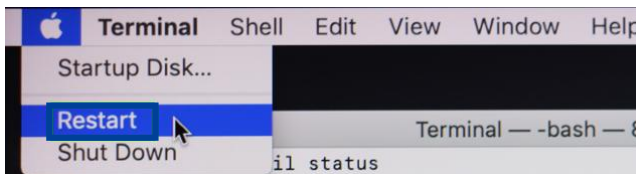


- 3) Enter the following command to set the SIP to disabled:

csrutil disable

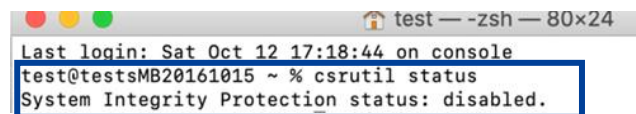


- 4) Click the **Apple** logo in the upper left-hand corner of the desktop and select **Restart** to reboot the system.



- 5) Enter the following command to check the SIP status:

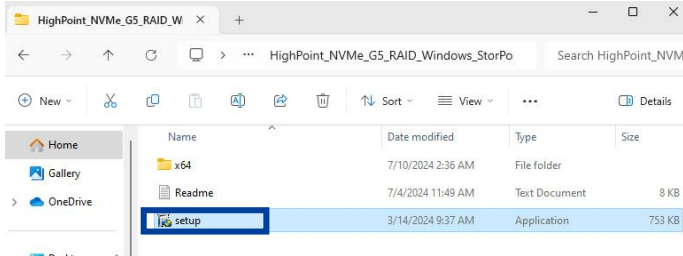
csrutil status



5.1. Install the driver on Windows

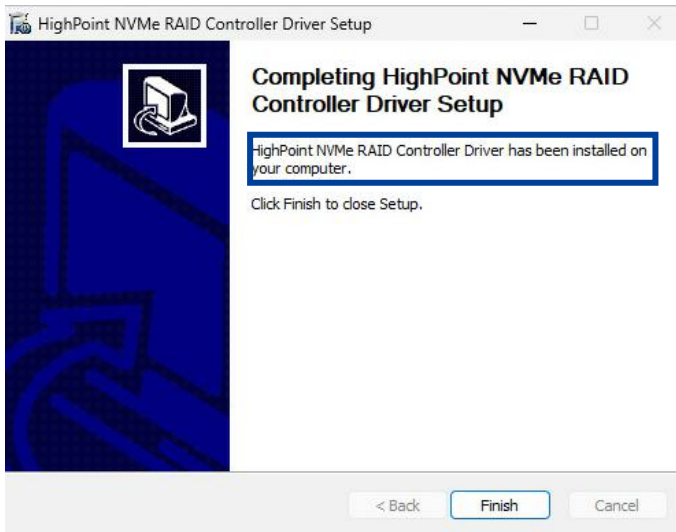
To install the HighPoint driver on the Windows operating system, perform the following steps.

1. Locate the HighPoint driver download and open the file.
2. Double-click **setup.exe**.



Note: If installation does not start, you may have to start setup using Administrator Privileges manually. Right-click setup, select Run as Administrator from the menu and confirm the pop-up window to proceed.

3. After the driver installation is complete, click **Finish** to proceed.



5.1.1. Uninstall the driver on Windows

Perform the following steps to uninstall the HighPoint driver on the Windows Operating System.

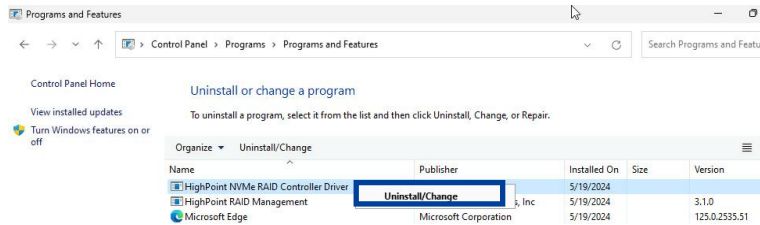
1. Power down the system and remove the AIC from the motherboard.

Notes:

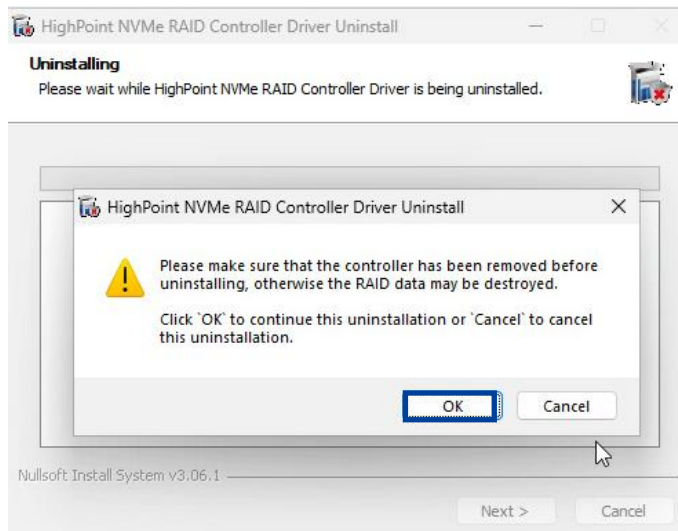
Failing to remove the AIC from the system during the uninstall process may result in data loss.

Whenever the driver is uninstalled, the Windows Operating System will attempt to install the default AIC, which may corrupt the RAID configurations and any data stored on SSDs hosted by the AIC.

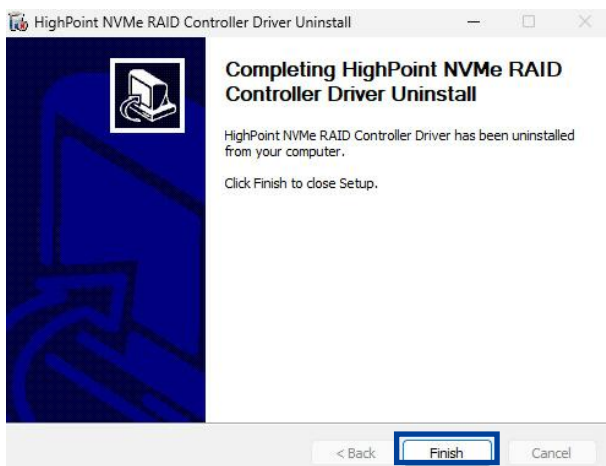
2. Power on the system and boot Windows.
3. Access **Control Panel** and select **Programs** → **Programs and Features**, and click on the **HighPoint NVMe RAID Controller Driver** entry.
4. Click **Uninstall/Change**.



5. Click **OK** to continue the driver uninstallation.



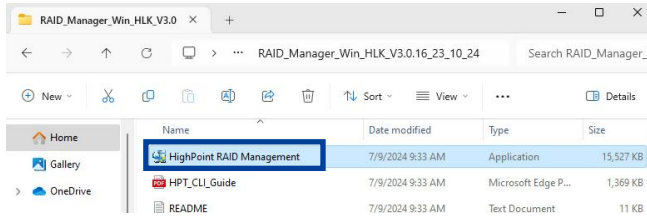
6. After uninstalling the driver, click **Finish**.



5.2. Install the RAID Management on Windows

To install the HighPoint RAID Management on the Windows operating system, perform the following steps.

1. Locate the HighPoint RAID Management Software download and open the file.
2. Double-click **HighPoint RAID Management.exe**.

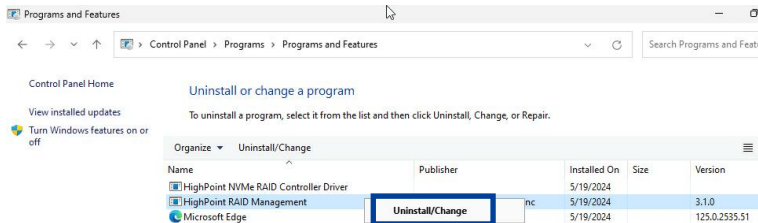


3. After the driver installation is complete, click **Finish** to proceed.

5.2.1. Uninstall the RAID Management on Windows

Perform the following steps to uninstall the HighPoint RAID Management on the Windows Operating System.

1. Access **Control Panel**, select **Programs** → **Programs and Features**, and right-click on the **HighPoint RAID Management** entry.
2. Click **Uninstall/Change**.



3. After uninstalling the HighPoint RAID Management, click **Finish**.



5.3. Install the driver on Linux

To install the HighPoint driver on the Linux operating system, perform the following steps.

1. Power on the system and boot the Linux distribution.
2. Open a terminal with root privileges and enter the following command to enter the path where the HighPoint driver is located.

```
#cd /home/test/Downloads/
```

```
test@test-Super-Server:~/Desktop$ sudo su
[sudo] password for test:
root@test-Super-Server:/home/test/Desktop# cd /home/test/Downloads/
root@test-Super-Server:/home/test/Downloads#
```

3. Enter the following command to extract the HighPoint driver:

```
#tar zxvf HighPoint_NVMe_G5_Linux_Src_vx.x.xx_xx_xx_xx.tar.gz
```

```
root@test-Super-Server:/home/test/Downloads# tar zxvf HighPoint_NVMe_G5_Linux_Src_v1.6.17.0_2024_07_01.tar.gz
hptnvme_g5_linux_src_v1.6.17.0_2024_07_01.bin
README
```

4. Enter the following command to install the HighPoint driver.

```
#sh hptnvme_g5_linux_sre_vxx.x.x_xx_xx_xx.bin or
```

```
#!/ hptnvme_g5_linux_sre_vxx.x.x_xx_xx_xx.bin
```

```
root@test-Super-Server:/home/test/Downloads# ./hptnvme_g5_linux_src_v1.6.17.0_2024_07_01.bin
Verifying archive integrity... All good.
Uncompressing HighPoint NVMe RAID Controller Linux Open Source package installer.....
.....
Checking and installing required toolchain and utility ...
Installing program gcc ... ^Csignal caught, cleaning up
root@test-Super-Server:/home/test/Downloads# ./hptnvme_g5_linux_src_v1.6.17.0_2024_07_01.bin
Verifying archive integrity... All good.
Uncompressing HighPoint NVMe RAID Controller Linux Open Source package installer.....
.....
Checking and installing required toolchain and utility ...
Installing program gcc ... done
Installing program make ... done
Found program perl (/usr/bin/perl)
Found program wget (/usr/bin/wget)
Found program gcc-13 (/usr/bin/gcc-13)
Sourcing file '/etc/default/grub'
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-6.8.0-31-generic
Found initrd image: /boot/initrd.img-6.8.0-31-generic
Found memtest86+ 64bit EFI image: /boot/memtest86+xx64.efi
Warning: os-prober will not be executed to detect other bootable partitions.
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
Adding boot menu entry for UEFI Firmware Settings ...
done
Synchronizing state of hptdrv-monitor.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable hptdrv-monitor
update-rc.d: warning: enable action will have no effect on runlevel 1
Created symlink /etc/systemd/system/default.target.wants/hptdrv-monitor.service → /usr/lib/systemd/system/hptdrv-monitor.service.
SUCCESS: Driver hptnvme is installed successfully for kernel 6.8.0-31-generic.
Please restart the system for the driver to take effect.
If you want to uninstall the driver from the computer, please run hptuninhptnvme to uninstall the driver files.
root@test-Super-Server:/home/test/Downloads#
```

5. After the HighPoint driver installation, the system will prompt you to restart to make the driver take effect. Manually restart the system.

5.3.1. Uninstall the driver on Linux

Perform the following steps to uninstall the HighPoint driver on the Linux Operating System.

1. Power down the system and remove the AIC from the motherboard.

Note: Failing to remove the NVMe product and SSDs when uninstalling the driver may result in data loss. The Linux distribution will load the default NVMe support after uninstalling the HighPoint Linux – this driver will only recognize the NVMe SSDs as separate disks.

2. Open the system terminal with root privileges.
3. Enter the following command to uninstall the driver, and press **Y/y** to confirm.

```
#hptuninhptnvme
```

```
root@test-Z790M-AORUS-ELITE-AX:/home/test/Downloads# hptuninhptnvme
Are you sure to uninstall the driver hptnvme from system? (Y/n): y
Sourcing file `'/etc/default/grub'
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-6.8.0-31-generic
Found initrd image: /boot/initrd.img-6.8.0-31-generic
Found memtest86+ 64bit EFI image: /boot/memtest86+x64.efi
Warning: os-prober will not be executed to detect other bootable partitions.
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
Adding boot menu entry for UEFI Firmware Settings ...
done
All files installed have been deleted from the system.
```

4. After uninstalling the driver, manually reboot the system.

5.4. Install the RAID Management on Linux

To install the HighPoint RAID Management on the Linux operating system, perform the following steps.

1. Using the system terminal with root privileges, browse to the directory where the software is downloaded and enter the following commands to extract the management software package:

```
tar zxvf RAID_Manage_Linux_v3.x.x_x_x_x.tgz
```

```
root@test-Super-Server:/home/test/Downloads# tar zxvf RAID_Manage_Linux_v3.1.16_24_06_28.tgz
HPT_CLI_Guide.pdf
README.txt
RAID_Manage_Linux_v3.1.16_24_06_28.bin
```

2. Install the HighPoint RAID management software (WebGUI & CLI) using the following command:

```
./RAID_Manage_Linux_v3.x.x_x_x_x.bin
```

```
root@test-Super-Server:/home/test/Downloads# ./RAID_Manage_Linux_v3.1.16_24_06_28.bin
.....
Install .....
Package readline lib is already installed!
readline/hptsvr_3.1.16_amd64.deb will be installed!
Selecting previously unselected package hptsvr.
(Reading database ... 148402 files and directories currently installed.)
Preparing to unpack .../hptsvr_3.1.16_amd64.deb ...
Unpacking hptsvr (3.1.16) ...
Setting up hptsvr (3.1.16) ...
Starting hptsvr daemon.
Clean .....
Finish .....
```

5.4.1. Uninstall the RAID Management on Linux

To uninstall the HighPoint RAID Management on the Linux operating system, perform the following steps.

1. Open the system terminal with root privileges.
2. Enter the following command to uninstall the RAID Management:

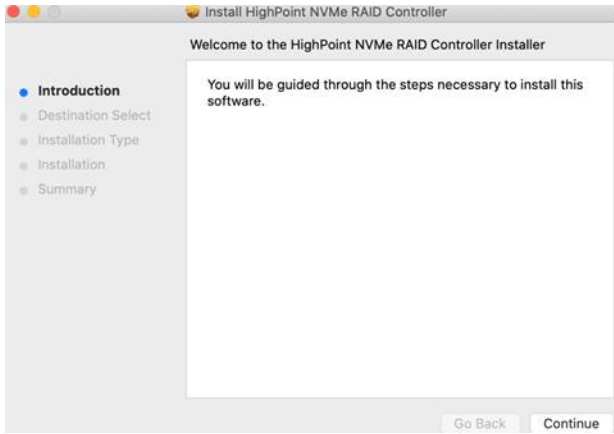
```
#hptuninhptsvr
```

```
root@test-Z790M-AORUS-ELITE-AX:/home/test/Downloads# hptuninhptsvr
uninstalling hptsvr(3.2.0)...
waiting for hptsvr to be terminated...
unconfiguring service...
Deleting related files...
hptsvr has been uninstalled.
```

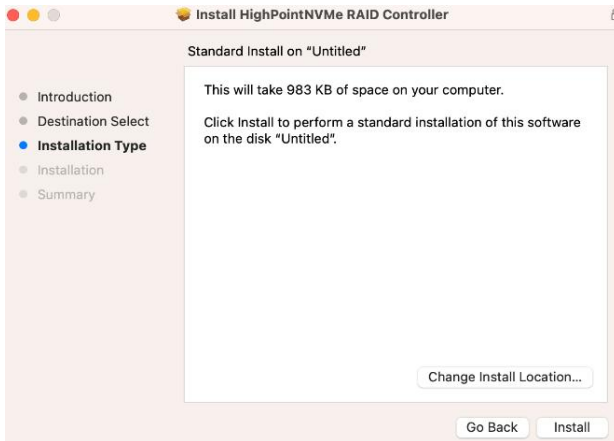
5.5. Install the driver on macOS

To install the HighPoint driver on the macOS, perform the following steps.

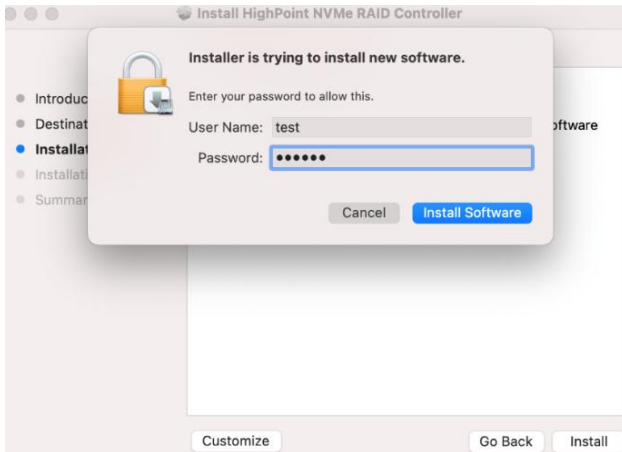
1. Locate the download and double-click the **HighPointNVMe.pkg** package to start the installer. Click the **Continue** button.



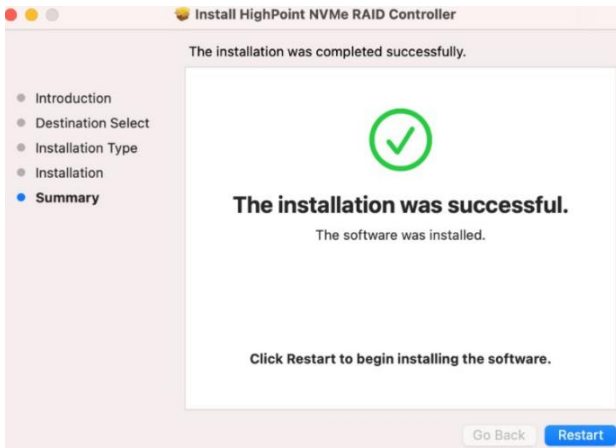
2. macOS will prompt you to install the driver. Click **Install** to proceed.



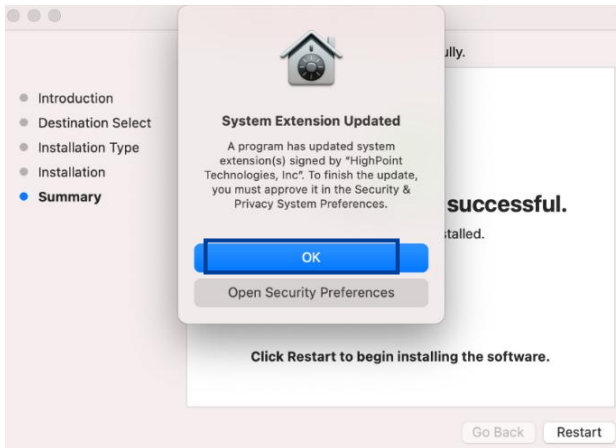
3. You will be prompted that the installer is trying to install new software; enter the *Administrator* Username and Password. Once these have been entered, Click **Install Software**.



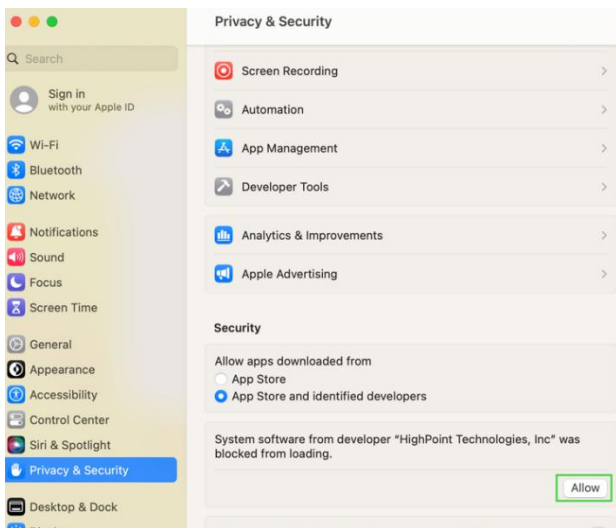
4. If no pop-ups appear, please proceed to the next step of installation. Click **Restart**.



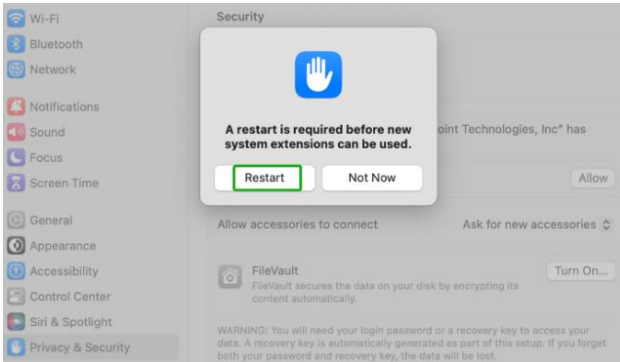
5. If you receive a popup window prompting you for permission, click **Open Security Preferences**.



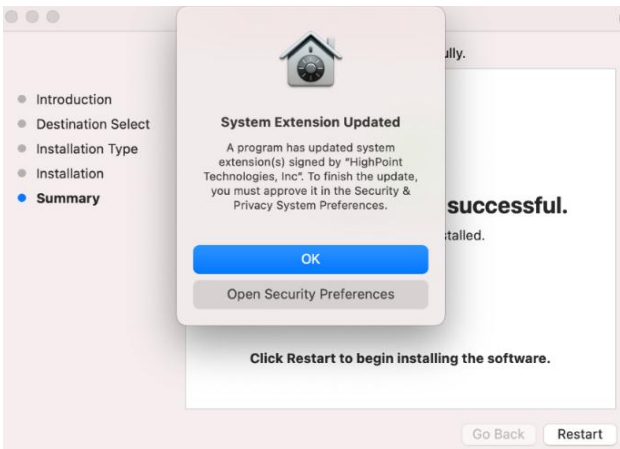
6. Make sure the **App Store and identified developers** is checked, and then click **Allow**.



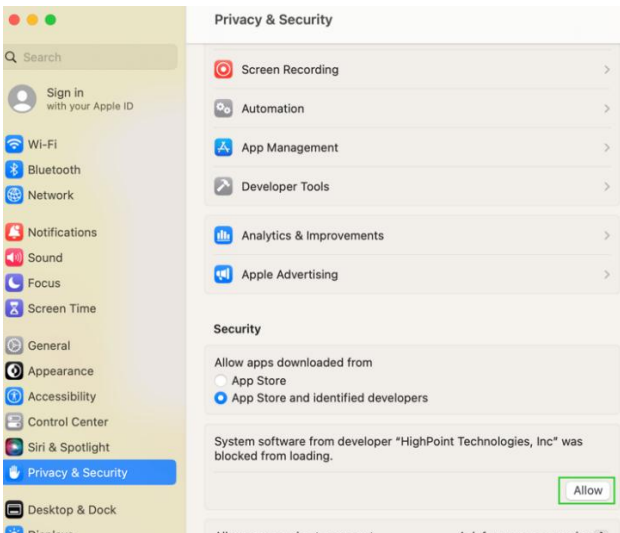
7. You will see a popup window prompting you to restart. Click **Restart**.



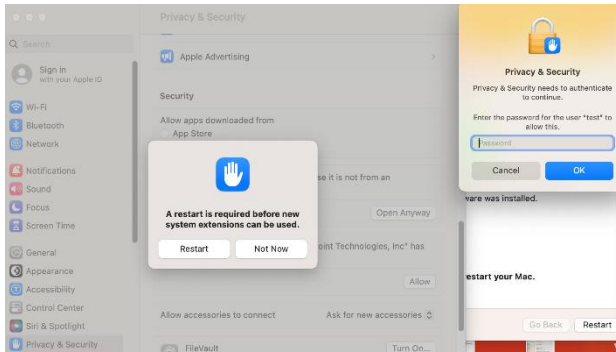
8. If you receive the permission prompt for the second time, click “**Open Security Preferences**” again.



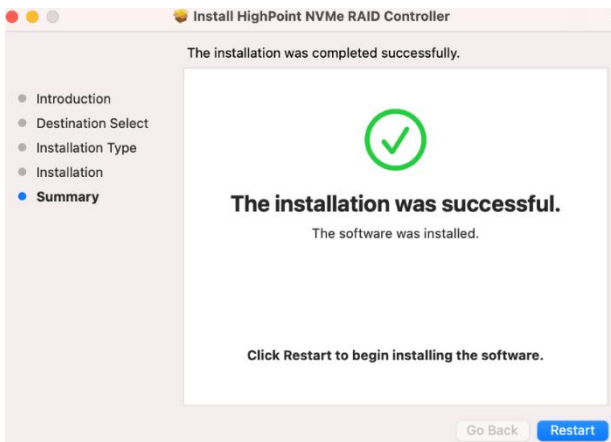
9. Make sure the **App Store and identified developers** is checked, and then click **Allow**.



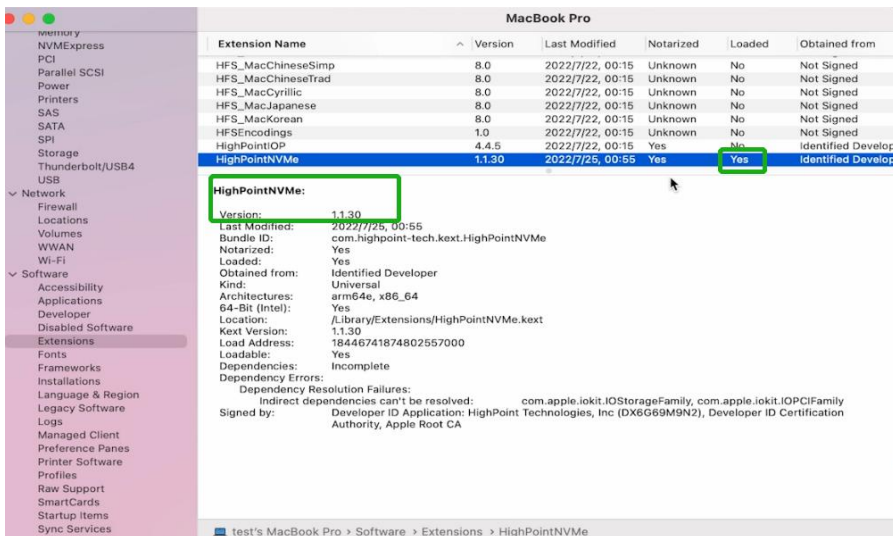
- You will see a popup window prompting you to restart. Enter the **Administrator** Username and Password and click **Restart**.



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



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



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

5.5.1. Uninstall the driver on macOS

To uninstall the HighPoint driver on the macOS, perform the following steps.

1. Power off the system and remove the NVMe product from the motherboard.

Notes:

Failing to remove the NVMe product and SSDs when uninstalling the driver may result in data loss.

The macOS will load the default NVMe support after the HighPoint driver has been uninstalled – this driver will only recognize the NVMe SSDs as separate disks.

2. To uninstall the NVMe driver, you will need to open the terminal window and enter the following command:

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

```
sudo kextcache -i /
```

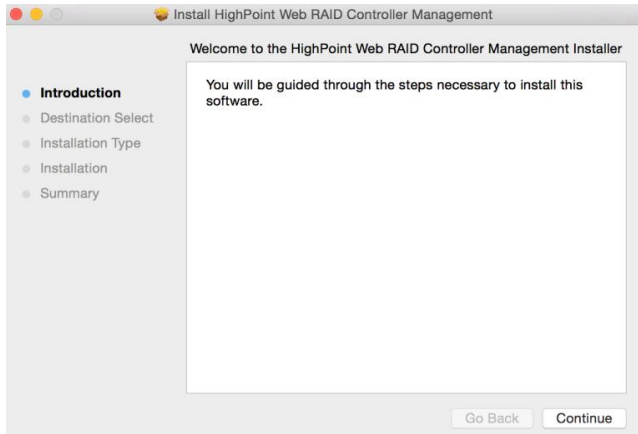
```
[test@testsMB01610152 ~] % sudo rm -rf /Library/Extensions/HighPointNVMe.kext
Password:
[test@testsMB01610152 ~] % sudo kextcache -i /
kextcache -i /
kextcache -arch x86_64 -local-root -all-loaded -kernel /System/Library/Kernels/k
kernel -prelinked-kernel /Library/Apple/System/Library/PrelinkedKernels/prelinked
kernel -volume-root / /Library/Extensions /AppleInternal/Library/Extensions /Lib
rary/Apple/System/Library/Extensions /System/Library/Extensions
KernelCache ID: 91AFAAB6216EDD61055A39A8E77A483C
test@testsMB01610152 ~ %
```

3. After uninstalling the driver, manually reboot the system.

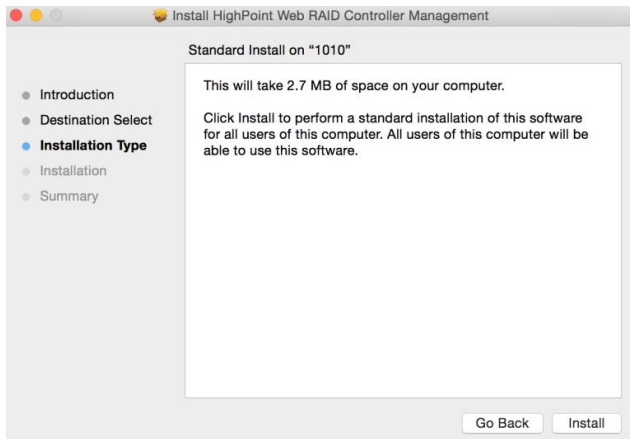
5.6. Install the RAID Management on macOS

To install the HighPoint RAID Management on the macOS, perform the following steps.

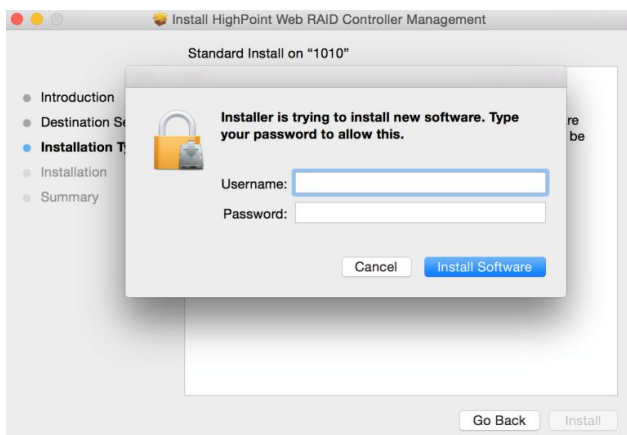
1. Double-click the package named **HighPointWebGUI.pkg** to start the installer. When the window appears, click the **Continue** button.



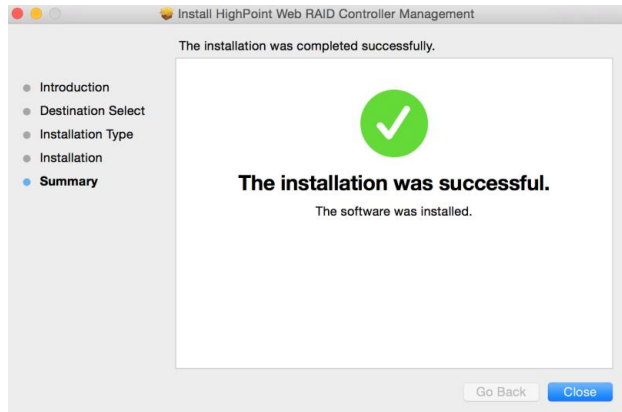
2. You will be promoted to click the **Install** button. Click **Install** to continue.



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



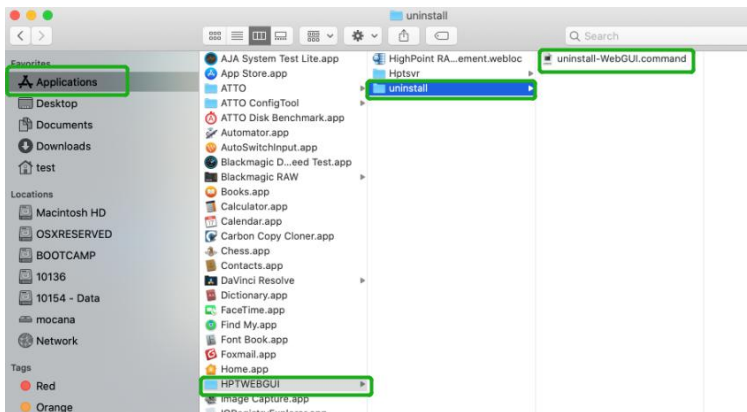
- The WebGUI Management software has been installed. Click **Close** to complete the procedure.



5.6.1. Uninstall the RAID Management on macOS

To uninstall the HighPoint RAID Management on the macOS, perform the following steps.

- Access **Applications**, click **HPTWEBGUI**.
- Select **uninstall**, and double-click the **uninstall-WEBGUI.command**. The uninstall command will automatically open a terminal and uninstall the software.



```

test — uninstall-WebGUI.command — 94x30
Last login: Thu Jul 2 13:34:32 on ttys000
/Applications/HPTWEBGUI/uninstall/uninstall-WebGUI.command ; exit;
test@tests-Pro2019 ~ % /Applications/HPTWEBGUI/uninstall/uninstall-WebGUI.command ; exit;

This script will attempt to uninstall HighPoint Web RAID Controller Manage 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/webservice.pkg
/Library/LaunchDaemons/HPTWebGUIDaemon.plist
/usr/share/hpt
/usr/bin/hptdaemonctl
/Library/LaunchDaemons/HPTWebGUIDaemon.plist: Operation now in progress
Process has completed.

[Process completed]

```

6. Web RAID Management Interface



Web RAID Management Interface is often referred to as WebGUI. While you are in the WebGUI view, if the WebGUI detects any new events, it checks and updates the AIC status, updates disk counts, updates disk group counts, updates virtual disk counts, and so on.

This section describes how to use the Web RAID Management Interface.

6.1. Start the WebGUI

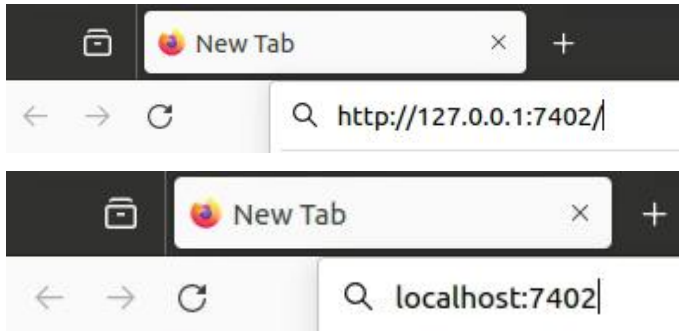
For Windows Users

Double-click the **HighPoint RAID Management** ICON to start the software using the system's default web browser. It will automatically log in to the WebGUI.



For Linux Users

Open the browser and enter <http://127.0.0.1:7402> or localhost:7402 to log into WebGUI. 7402 is the WebGUI's Port Number, which can be modified.



For macOS Users

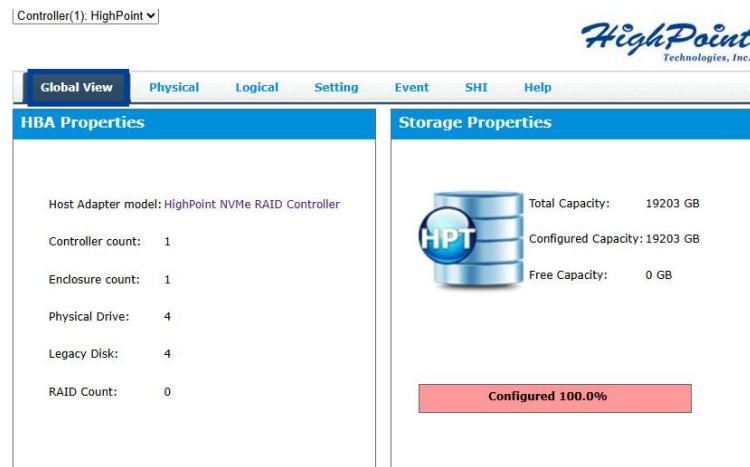
Double-click the **HighPoint RAID Management** ICON to start the software using the system's default web browser. It will automatically log in to the WebGUI.



6.2. Global View

The **Global view** provides an overview of what each AIC connected to your computer detects. It is also the first page you see when logging in.

A drop-down menu on the top left of the page lets you select which AIC you want to manage if you connect multiple HighPoint AICs.



6.2.1. HBA Properties

The **HBA Properties** section displays the following information.

- **Host Adapter model** — The name of the HighPoint product or solution.
- **Controller Count** — The number of the AICs detected.
- **Enclosure Count** — The number of external enclosures detected.
- **Physical Drives** — The number of disks hosted by the AIC.
- **Legacy Disk** — The number of Legacy disks connected.
- **RAID Count** — The number of RAID arrays.

6.2.2. Storage Properties

The **Storage Properties** section displays the following information.

- **Total capacity** — The combined capacity of each disk connected to the AIC.
- **Configured capacity** — The amount of space used for creating RAID arrays.
- **Free Capacity** — The total amount of space unused.

6.3. Physical

The **Physical** tab shows general and extended information about the AIC and any hosted NVMe SSDs.

Global View	Physical	Logical	Setting	Event	SHI	Help
Controller 1						
Enclosure 1						
Devices						
Rescan						
Controller Information						
Model Name:		HighPoint NVMe RAID Controller				
Vendor:		HighPoint Technologies, Inc.				

6.3.1. Controller Information

The **Controller Information** section displays the following information.

Controller Information	
Model Name:	HighPoint NVMe RAID Controller
Vendor:	HighPoint Technologies, Inc.

- **Model name** — The model name of the HighPoint AIC.
- **Vendor** — The manufacturer of the AIC.

6.3.2. Enclosure Information

The **Enclosure Information** section displays the following information.

Enclosure Information	
Model:	SSD7749M2 NVMe Controller
Vendor:	HighPoint
ID:	1
SN:	00000ce000000
Temperature:	43 (C)
PCI Location:	10:0:0
Current Link Width:	x16
Current Link Speed:	16.0 GT/s

- **Model** — The name of the AIC.
- **Vendor** — The manufacturer of the AIC.
- **ID** — The number of the AIC.
- **SN** — The serial number of the AIC.
- **PCI Location** — The PCI slot location where the AIC is located.
- **Current Link Width** — The PCIe width occupied by the current AIC.
- **Current Link Speed** — The current link bandwidth of the AIC.

6.3.3. Physical Devices Information

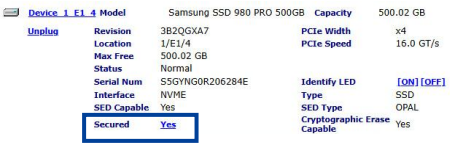
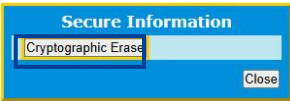
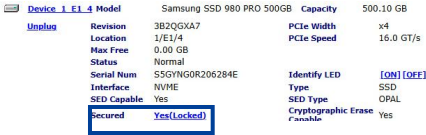
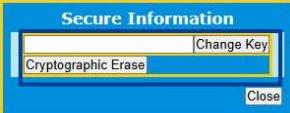
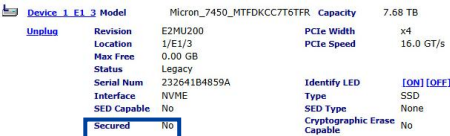
The **Devices Information** section displays the following information.

Global View		Physical	Logical	Setting	Event	SHI	Help
Controller 1		Physical Devices Information					
Enclosure 1	Device 1_E1_5		Model	Micron_7400_MTFDKCB7T6TDZ	Capacity	7.68 TB	
Devices	Unplug		Revision	E1MU23Y5	PCIe Width	x4	
Rescan			Location	1/E1/5	PCIe Speed	Gen 4	
			Max Free	0.00 GB			
			Status	Legacy			
			Serial Num	2316423C3572			
			Interface	NVME	Type	SSD	
			SED Capable	No	SED Type	None	
			Secured	No	Cryptographic Erase Capable	No	

- **Model** – The model number of the physical disk.
- **Capacity** – The total capacity of the physical disk.
- **Revision** – The physical disk firmware revision number.
- **Location** – The physical disk location (e.g., Device 1_E1_5 represents the disk on AIC 1 port 5).
- **Max Free** – The space on the physical disk is not configured in an array.
- **Status** – The status of the physical disk.
 - **Legacy:** The disk's status is legacy.
 - **Disabled:** The disk cannot be used. (May be related to disk failure)
 - **Normal:** The disk is a member of a RAID array.
 - **Spare:** The disk has been set as a spare disk.
- **Serial Number** – The serial number of the physical disk.
- **Interface** – The interface of the physical disk.
- **Type** – The type of the physical disk.
- **PCIe Width** – The PCIe width of the current physical disk.
- **PCIe Speed** – The PCIe speed of the current physical disk.
- **SED Capable** – Whether the physical disk supports the SED feature.
- **SED Type** – The current SED Type of the physical disk is OPAL.
- **Cryptographic Erase Capable** – Whether the physical disk supports the Cryptographic Erase feature.
- **Unplug** – Safely eject the selected disk.
- **Secured** – Whether the physical disk is secured.

The following table describes the **Secured** in detail.

Table 8: Secured Status & Description

Secured Status	Description
<p>Yes</p> 	<p>Indicates that security for the disk is enabled and unlocked. Data can be accessed.</p> <p>Your optional option is:</p>  <p>- Cryptographic Erase</p> <p>The Cryptographic Erase function will erase the secured key inside each disk, making it impossible to decrypt data stored on these devices.</p>
<p>Yes (Locked)</p> 	<p>Indicates that the security of the disk is enabled, but the disk's key does not match the key on the AIC.</p> <p>Your optional options are:</p>  <p>- Change key</p> <p>Enter the disk's old password and click Change Key to unlock the Disk Security key.</p> <p>If you do not enter the correct disk key five times, this function will be locked, and you will need to power cycle your system to change the disk key again.</p> <p>- Cryptographic Erase</p> <p>The Cryptographic Erase function will erase the secured key inside each disk, making it impossible to decrypt data stored on these devices.</p>
<p>No</p> 	<p>Indicates that disk security is not enabled or not supported.</p>

6.3.3.1. Change Disk Security

When the AIC Security Key and Disk Security Key do not match, the ability to change the Disk Security Key will be displayed. The secured disk is now in the **Yes (Locked)** state.

To change disk security, perform the following steps:

1. Click the **Physical** tab.
2. Under the **Physical Devices** section, click the name of each disk in blue text to view the Secured setting.
3. Click **Yes (Locked)**, a new pop-up window providing a Change Key option will be displayed.
4. Enter the disk's old password and click **Change Key** to unlock the Disk Security key.



Notes:

Change Key: Input the old Disk Security key to unlock the disk and write the AIC Security key on this disk.

There is a limit to the number of times you can change the disk key. If you do not enter the correct disk key **five times**, this function will be locked, and you will need to power cycle your system to change the disk key again.

5. After the system restarts, the secure attribute of the disk should change from **Yes (Locked)** to **Yes**.

6.3.3.2. Disable Disk Security

We use **Cryptographic Erase** to disable Disk Security. The **Cryptographic Erase** replaces the encryption key inside each disk; this makes it impossible to decrypt data stored on these devices. When executed, data is rendered inaccessible and considered cryptographically erased. The disks can then be reset to an unowned state and reused once a new Disk Security key is generated.



Warning: Cryptographic erase will delete the Security (Encryption) key from the target disk/array members. Data stored on these disks will no longer be accessible.

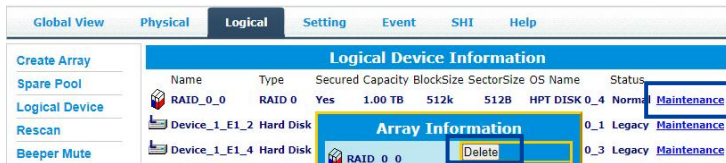
Note: When the disk is in Legacy status or is a RAID member disk, you cannot disable Disk Security directly. You need to initialize the legacy disk or delete the RAID.

To disable disk security, perform the following steps:

1. Click the **Physical** tab.
2. Click the **Maintenance**. There are two situations.
 - Situation 1: If the disk is in Legacy status, you can remove this by using the **Init** function.



- Situation 2: If the disk is a member disk in the secured RAID array, you can delete the array by using the **Delete** function.



3. Under the **Physical Devices** section of the Physical tab, check the **Secured** status of the target disk. If enabled, this will be displayed as **Yes** or **Yes (Locked)**;
4. Click the Secured status (blue text); a pop-up window will be displayed, providing a **Cryptographic Erase** button.



5. After the system restarts, the secure attribute of the disk should change from **Yes** to **No**.

6.3.3.3. Unplug the Physical Device

If you want to eject the disk while the system is working, you want to use the **Unplug** to keep the disk safe. Other methods of disk removal will trigger an alarm.

1. Open the **WebGUI**.
2. Click the **Physical** tab.
3. Select the disk you want to unplug, and click **Unplug**.



4. Manually remove the disk.
5. If you want to plug a new disk. Manually plug the disk, and click **Rescan**; the disk you just plugged in is displayed under **Physical Devices Information**.

6.3.4. Update the Firmware

You can upgrade to a newer version of the AIC firmware here. This help update the firmware version and the UEFI HII Utility version. The process may take some time.



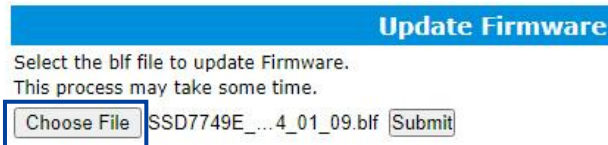
Update Firmware

Select the blf file to update Firmware.
This process may take some time.

No file chosen

To update the AIC firmware, perform the following steps:

1. Open the **WebGUI**.
2. Click the **Physical** tab.
3. Click **Choose File** to select the file with a suffix of blf you want to update the firmware.



Update Firmware

Select the blf file to update Firmware.
This process may take some time.

SSD7749E_...4_01_09.blf

4. Click **Submit**.
5. Reboot the system to make the update take effect.



Controller(1): HighPoint

localhost:7402 says
Firmware updated successfully, it will take effect after reboot.

Controller Information

Model Name:	HighPoint NVMe RAID Controller
Vendor:	HighPoint Technologies, Inc.

Global View

Controller 1

Enclosure 1

Devices

6.3.5. Secure Setting

This **Secure Setting** supports enable, disable and change AIC security key.

The screenshot shows a web interface titled "Secure Setting". It contains two input fields: "Password:" and "Confirm:". Below these fields is a button labeled "Enable Security".

6.3.5.1. Enable AIC Security

To enable AIC security, perform the following steps:

1. Open the **WebGUI**.
2. Click the **Physical** tab.
3. Under **Secure Setting**, Enter the password a second time for the **Confirm** field. The password length is 8-32 digits, and there is no limit to the valid complexity of the password.
4. Set the password and click **Enable Security** to enable the AIC Security.

The screenshot shows the "Secure Setting" interface with the "Password:" and "Confirm:" fields filled with dots. The "Enable Security" button is highlighted with a blue border.



Warning: If you forget the security key, you will lose access to your data.

6.3.5.2. Change AIC Security

To change AIC security, perform the following steps:

1. Open the **WebGUI**.
2. Click the **Physical** tab.
3. Enter the current password under the **Old Password** field.
4. Enter a new password under the **New Password** field. The password length is 8-32 digits, and there is no limit to the valid complexity of the password.
5. After entering a new password, click **Change Security**.

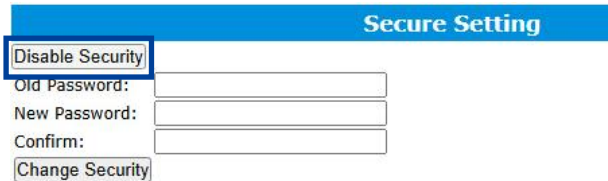
The screenshot shows the "Secure Setting" interface with the "Disable Security" button highlighted. It contains three input fields: "Old Password:", "New Password:", and "Confirm:". Below these fields is a button labeled "Change Security".

6. Confirm the change by clicking **OK** when the pop-up window is displayed.

6.3.5.3. Disable AIC Security

To disable AIC security, perform the following steps:

1. Open the **WebGUI**.
2. Click the **Physical** tab.
3. Under **Secure Setting**, click **Disable Security**.



The screenshot shows a web interface titled "Secure Setting" with a blue header. Below the header, there is a "Disable Security" button highlighted with a red box. Underneath this button are three input fields labeled "Old Password:", "New Password:", and "Confirm:". At the bottom of the form is a "Change Security" button.

6.3.6. Rescan the Physical Device

When the WebGUI initiates **Rescan**, the driver will immediately check and see whether the status of any disk has changed. If any changes occur, the disks and RAID array status will be updated to reflect this.

- **Disk Status** – if any disks were added or removed, or if a disk is no longer responding, the status will change.
- **RAID status** – the RAID array's status may change depending on the status of the disks.

6.4. Logical

The **Logical** tab is where you can create, delete, and maintain your RAID configurations and add disks to your spare pool.

Global View	Physical	Logical	Setting	Event	SHI	Help																																																							
Create Array Spare Pool Logical Device Rescan Beeper Mute	<table border="1"> <thead> <tr> <th colspan="7">Logical Device Information</th> </tr> <tr> <th>Name</th> <th>Type</th> <th>Secured</th> <th>Capacity</th> <th>BlockSize</th> <th>SectorSize</th> <th>OS Name</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td> Device_1_E1_1</td> <td>Hard Disk</td> <td>No</td> <td>960.19 GB</td> <td></td> <td></td> <td>HPT DISK 0_2</td> <td>Legacy Maintenance</td> </tr> <tr> <td> Device_1_E1_2</td> <td>Hard Disk</td> <td>No</td> <td>960.19 GB</td> <td></td> <td></td> <td>HPT DISK 0_3</td> <td>Legacy Maintenance</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th colspan="6">Physical Device Information</th> </tr> <tr> <th>Location</th> <th>Model</th> <th>Secured</th> <th>Capacity</th> <th>Max Free</th> <th></th> </tr> </thead> <tbody> <tr> <td> 1/E1/1</td> <td>KXD51RUE960G TOSHIBA</td> <td>No</td> <td>960.19 GB</td> <td>0.00 GB</td> <td></td> </tr> <tr> <td> 1/E1/2</td> <td>KXD51RUE960G TOSHIBA</td> <td>No</td> <td>960.19 GB</td> <td>0.00 GB</td> <td></td> </tr> </tbody> </table>						Logical Device Information							Name	Type	Secured	Capacity	BlockSize	SectorSize	OS Name	Status	Device_1_E1_1	Hard Disk	No	960.19 GB			HPT DISK 0_2	Legacy Maintenance	Device_1_E1_2	Hard Disk	No	960.19 GB			HPT DISK 0_3	Legacy Maintenance	Physical Device Information						Location	Model	Secured	Capacity	Max Free		1/E1/1	KXD51RUE960G TOSHIBA	No	960.19 GB	0.00 GB		1/E1/2	KXD51RUE960G TOSHIBA	No	960.19 GB	0.00 GB	
Logical Device Information																																																													
Name	Type	Secured	Capacity	BlockSize	SectorSize	OS Name	Status																																																						
Device_1_E1_1	Hard Disk	No	960.19 GB			HPT DISK 0_2	Legacy Maintenance																																																						
Device_1_E1_2	Hard Disk	No	960.19 GB			HPT DISK 0_3	Legacy Maintenance																																																						
Physical Device Information																																																													
Location	Model	Secured	Capacity	Max Free																																																									
1/E1/1	KXD51RUE960G TOSHIBA	No	960.19 GB	0.00 GB																																																									
1/E1/2	KXD51RUE960G TOSHIBA	No	960.19 GB	0.00 GB																																																									

6.4.1. Logical Device Information

The **Logical Device Information** tab is the default page when clicking the **Logical** tab of the WebGUI. The Logical Device Information section displays the following information.

Global View	Physical	Logical	Setting	Event	SHI	Help																															
Create Array Spare Pool Logical Device Rescan	<table border="1"> <thead> <tr> <th colspan="7">Logical Device Information</th> </tr> <tr> <th>Name</th> <th>Type</th> <th>Secured</th> <th>Capacity</th> <th>BlockSize</th> <th>SectorSize</th> <th>OS Name</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td> Device_1_E1_1</td> <td>Hard Disk</td> <td>No</td> <td>960.19 GB</td> <td></td> <td></td> <td>HPT DISK 0_2</td> <td>Legacy Maintenance</td> </tr> <tr> <td> Device_1_E1_2</td> <td>Hard Disk</td> <td>No</td> <td>960.19 GB</td> <td></td> <td></td> <td>HPT DISK 0_3</td> <td>Legacy Maintenance</td> </tr> </tbody> </table>						Logical Device Information							Name	Type	Secured	Capacity	BlockSize	SectorSize	OS Name	Status	Device_1_E1_1	Hard Disk	No	960.19 GB			HPT DISK 0_2	Legacy Maintenance	Device_1_E1_2	Hard Disk	No	960.19 GB			HPT DISK 0_3	Legacy Maintenance
Logical Device Information																																					
Name	Type	Secured	Capacity	BlockSize	SectorSize	OS Name	Status																														
Device_1_E1_1	Hard Disk	No	960.19 GB			HPT DISK 0_2	Legacy Maintenance																														
Device_1_E1_2	Hard Disk	No	960.19 GB			HPT DISK 0_3	Legacy Maintenance																														

- **Name** – The physical disk location (e.g., Device 1_E1_1 represents the disk on AIC 1 port 1).
- **Type** – The type of the physical disk.
- **Secured** – Whether the physical disk or RAID array is secured.
- **Capacity** – The total capacity of the physical disk or RAID array.
- **OS Name** – The name of the physical disk or RAID array in the system.
- **Status** – The status of the physical disk. (Normal, Disabled, Critical, Legacy, etc.)
- **Maintenance** – Once an array has been created, click maintenance for options to manage your array. Different array or disk statuses will have other maintenance options.

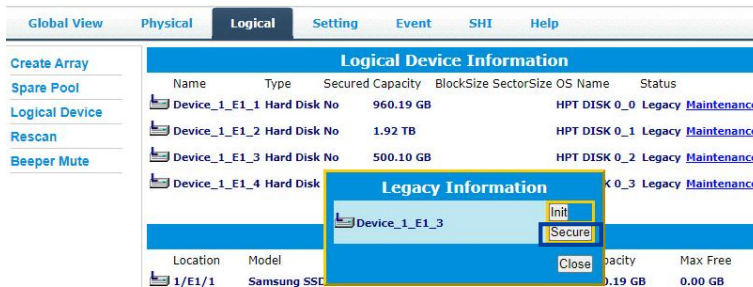
6.4.1.1.Enable Disk Security

To enable disk security, perform the following steps:

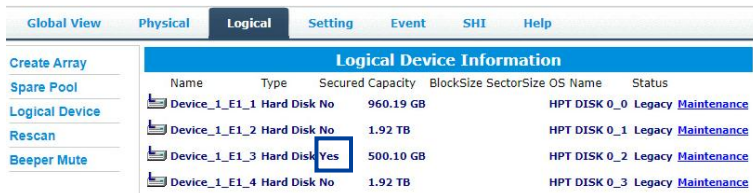
There are two methods to enable Disk Security.

- **Method 1: Enabling Disk Security for disks with the Legacy status**

1. Click the **Logical** tab and check the **Logical Device** section of the page.
2. Click the **Maintenance** option displayed on the right-hand side of each disk.
3. Click **Secure** to enable Disk Security.

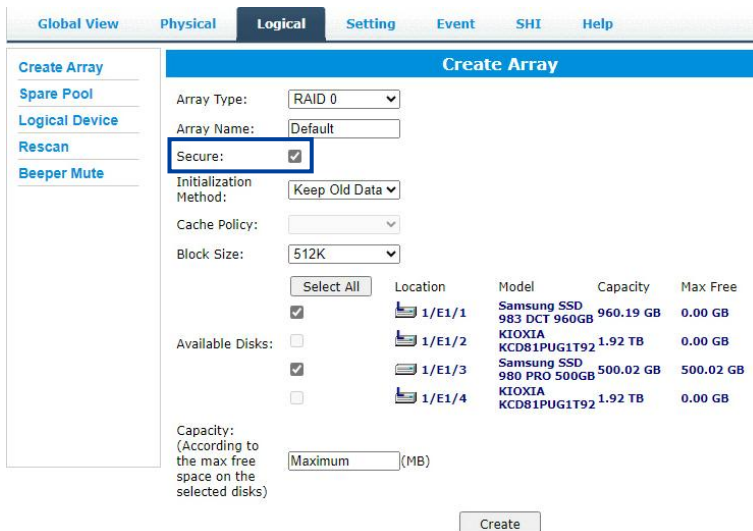


4. After Disk Security has been enabled.



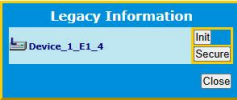
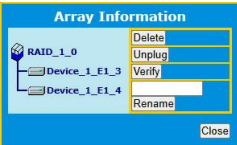
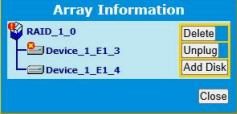
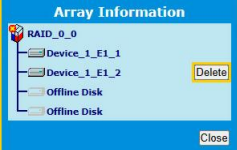
- **Method 2: Enabling Disk Security when creating a RAID array**

1. Click the **Logical** tab.
2. Check the box before the **Secure** option when creating a RAID array.



The following table describes the **Maintenance** in detail.

Table 9: Logical Device Status & Maintenance Options

Logical Device Status	Maintenance Options
<p>Legacy Status</p> 	<p>Disks with the Legacy status are healthy and functioning correctly.</p> <p>Your optional options in Maintenance are:</p> <ul style="list-style-type: none"> - init – Initialization of a disk sets all data bits to 0, clearing all the data on the disk. It is important to initialize disks as previous data physically stored on the disk may interfere with new data. - Secure – Enable Security for disks.
<p>Normal Status</p> 	<p>Arrays with the Normal status are healthy and functioning correctly.</p> <p>Your optional options in Maintenance are:</p> <ul style="list-style-type: none"> - Delete – Delete the selected RAID array. - Unplug – If you want to unplug the RAID array while the system works, use the Unplug first and then unplug the disks. - Verify – Verify the integrity of the RAID array. (RAID1/10 support only) - Rename – Rename the RAID array.
<p>Critical Status</p> 	<p>Arrays in the Critical status can be accessed and utilized but are no longer fault-tolerant. A Critical array should be rebuilt as soon as possible to restore redundancy.</p> <p>Your optional options in Maintenance are:</p> <ul style="list-style-type: none"> - Delete – deletes the selected RAID array. - Unplug – If you want to unplug the RAID array while the system works, use the Unplug first and then unplug the disks. - Add Disk – reinsert the same disk or insert a new disk. (RAID1/10 support only) <p>Reinserting the same disk should trigger the rebuilding status since data on the disk would be recognized.</p> <p>If you insert a new disk, clicking Add Disk will allow you to select and add it to the array.</p>
<p>Disabled Status</p> 	<p>An array with the Disabled status means that the RAID level does not have enough disks to function.</p> <p>Your optional option in Maintenance is:</p> <ul style="list-style-type: none"> - Delete – deletes the selected RAID array.

6.4.2. Physical Device Information

The **Physical Device Information** tab is the default page when clicking the **Logical** tab of the WebGUI. The Physical Device Information section displays the following information.

Global View Physical Logical Setting Event SHI Help								
Create Array Spare Pool Logical Device Rescan Beeper Mute	Logical Device Information							
	Name	Type	Secured	Capacity	BlockSize	SectorSize	OS Name	Status
	Device_1_E1_1	Hard Disk	No	960.19 GB			HPT DISK 0_2	Legacy Maintenance
	Device_1_E1_2	Hard Disk	No	960.19 GB			HPT DISK 0_3	Legacy Maintenance
	Physical Device Information							
	Location	Model	Secured	Capacity	Max Free			
	1/E1/1	KXD51RUE960G TOSHIBA	No	960.19 GB	0.00 GB			
	1/E1/2	KXD51RUE960G TOSHIBA	No	960.19 GB	0.00 GB			

- **Location** – The physical disk location (e.g., 1/E1/2 represents the disk on AIC 1 port 2).
- **Model** – The model number of the physical disk.
- **Secured** – Whether the physical disk is secured.
- **Capacity** – The total capacity of the physical disk or RAID array.
- **Max Free** – The space on the physical disk is not configured in an array.

6.4.3. Create a RAID Array

A RAID array is a collection of physical disks that will be one virtual disk by your Operating System. You need to follow the steps below to create a RAID array.

Note: RocketAIC series NVMe AIC SSDs are already pre-configured with RAID0. You can skip those steps. You can follow the steps if you want to use another type of RAID.

To create a RAID array, perform the following steps:

1. Open the **WebGUI**.
2. Select the proper **AIC** from the drop-down on the top left.
3. Click the **Logical** tab.
4. Click **Create Array**.

Location	Model	Capacity	Max Free
1/E1/1	KIOXIA KCD81PUG1T92	1.92 TB	0.00 GB
1/E1/2	KIOXIA KCD81PUG1T92	1.92 TB	0.00 GB

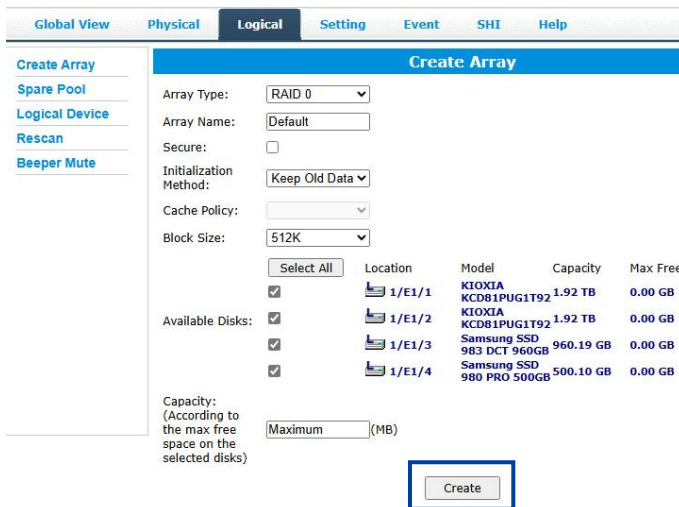
The following table describes the profile options.

Table 10: RAID Array Creation Profile Options

Property Name	Description
Array Type	Displays the RAID array level that is based on the profile selected. <ul style="list-style-type: none"> - RAID0 - RAID1 - RAID10
Array Name	Allows you to create the RAID array name. The name will be displayed on the Logical Device . (Default: RAID_ <level>_ <array number>)
Secure	Allows you to use the RAID array's SED capabilities. Only AIC that supports the SafeStorage Encryption feature will have this option.
Initialization Method	Displays the RAID array initialization setting. Default Initialization displays the following options: <ul style="list-style-type: none"> - Keep Old Data: This option skips the initialization process, and all data on each physical disk of the array will be untouched. - Quick Init: This option grants immediate access to the RAID array by skipping the

	<p>initialization process, but it will delete all data. (Recommended)</p> <ul style="list-style-type: none"> - Foreground: The array initialization process will be set to high priority. The array is inaccessible during this time, but the initialization process will complete faster. (Not recommended) - Background: The array initialization process will be set to low priority. The array is inaccessible during this time, but the initialization process will complete faster. (Not Recommended) <p>Important Note: The Foreground and Background Initialization options will cause NVMe SSD to result in TBW and performance degradation. Initialization of a disk sets all data bits to 0, clearing all the data on the disk. It is important to initialize disks as previous data physically stored on the disk may interfere with new data.</p>
Block Size	<p>It allows you to adjust the block size to fit your disk usage, thus improving performance.</p> <ul style="list-style-type: none"> - 128K - 256K - 512K (Default) <p>In a typical RAID configuration, virtual disk data is striped (or spread across) the physical disks. A smaller array block size will increase the likelihood of accessing all physical disks when processing large I/O requests. Multiple physical disks working in parallel increase the throughput, meaning better performance.</p>
Available Disks	Specifies member disks that will compose a new array.
Capacity	Displays the amount of RAID array storage space. By default, the maximum capacity available for the RAID array is displayed.

5. Select the creation profile options and click **Create**.



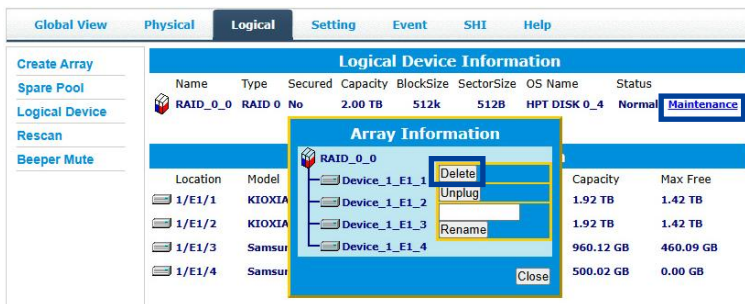
6. The created RAID array is displayed under **Logical Device Information**.

6.4.4. Delete a RAID Array

All data on a RAID array is lost when you delete it. Back up the data you want to keep before you delete a RAID array.

To delete a RAID array, perform the following steps:

1. Open the **WebGUI**.
2. Click the **Logical** tab.
3. Click **Maintenance**.
4. Click **Delete** to delete the RAID array.



5. A pop-up box pops up on the page. Click **OK** to confirm the RAID array deletion.
6. There is no deleted RAID array information at **Logical Device Information**, indicating that the RAID array deletion operation is complete.

Notes:

When the RAID array is in a rebuild, verify, foreground/background init status, deleting the RAID array will prompt in use. You can choose to stop the current operation and continue to delete it.

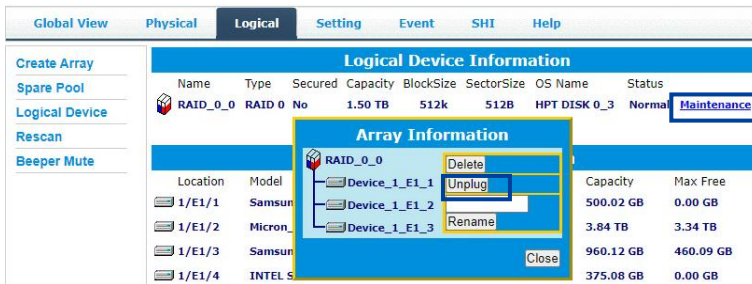
When the RAID array is mounted, deleting the RAID array will prompt in use. You can unmount it and continue to delete it.

6.4.5. Unplug a RAID Array

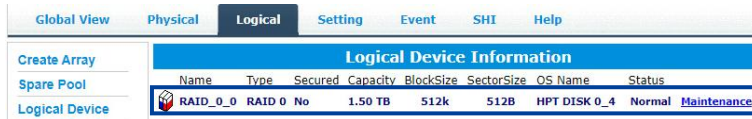
If you want to unplug the RAID array while the system works, use the Unplug first and then unplug the disks.

To unplug a RAID array, perform the following steps:

1. Open the **WebGUI**.
2. Click the **Logical** tab.
3. Click **Maintenance**.
4. Click **Unplug** to unplug the RAID array.



5. Manually remove all RAID member disks.
6. If you want to hot-plug the RAID member disks. Manually plug the disks, and click **Rescan**. The disks you just plugged in are displayed under **Logical Device Information**.

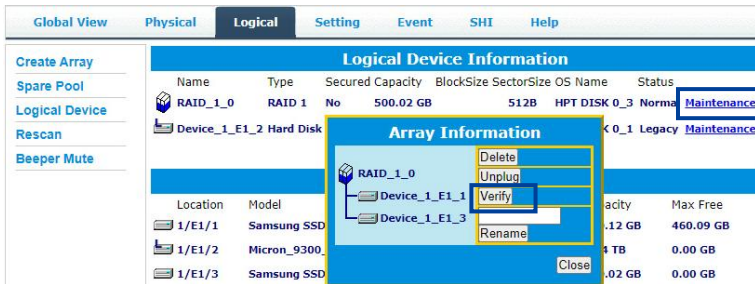


6.4.6. Verify a RAID Array

Check that the data spread across the disks of the array is consistent and ensure that the redundancy is the same between RAID members. (RAID1/10 support only)

To verify the integrity of the RAID array, perform the following steps:

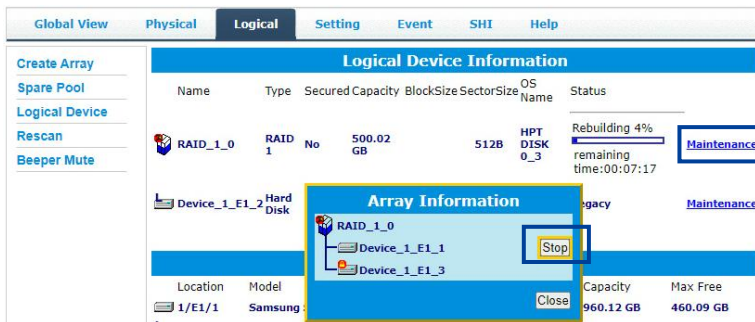
1. Open the **WebGUI**.
2. Click the **Logical** tab.
3. Click **Maintenance**.
4. Click **Verify** to verify the integrity of the RAID array.



5. The status of the RAID array changes from **Normal** to **Rebuilding**, showing the duration of the verification process.



6. You can stop the process by clicking **Stop**.



6.4.7. Add a Spare Disk

You can use spare disks to replace failed or defective disks in the RAID array group. A new disk must be at least as large as the defective disk.

If a disk used in a RAID array fails, the spare disk automatically takes its place, and the data on the failed disk is rebuilt on the spare disk.

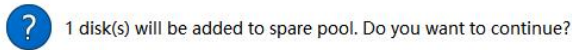
This feature minimizes the chances of data loss by reducing the time an array is in critical status.

To add a spare disk, perform the following steps:

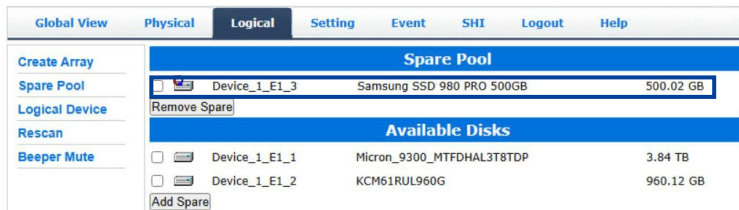
1. Open the **WebGUI**.
2. Click **Logical**.
3. Click **Spare Pool**.



4. Check the box for the disk you want as a spare under **Available Disks**.
5. Click **Add Spare** and confirm by selecting **OK** from the pop-up window.



6. The disk has now been assigned as a spare. Click **OK** to confirm.
7. The created spare disks are displayed under the **Spare Pool**.

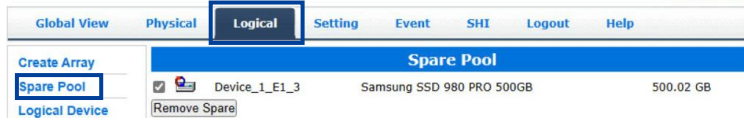


6.4.8. Remove a Spare Disk

Disks added to the spare pool will be displayed under the **Spare Pool**. You can also remove the spare disk from the Spare Pool.

To remove a spare disk, perform the following steps:

1. Open the **WebGUI**.
2. Click **Logical**.
3. Click **Spare Pool**.



4. Select the spare disk from the **Spare Pool**.
5. Click **Remove Spare**.
6. There is no deleted spare disk information at the **Spare Pool**, indicating that the spare disk has been successfully removed.

6.5. Setting

You can change the WebGUI settings in the **Setting** tab according to your preferred behavior and requirements. The **Setting** tab is divided into **System Setting**, **Password Setting** and **Email Setting**.

- **For Windows Users:**

- **For Linux Users:**

- **For macOS Users:**


6.5.1. System Setting

Using this tab, you can change the following system setting:

System Setting	
Enable auto rebuild.	Enabled ▾
Enable Continue Rebuilding on error.	Enabled ▾
Restrict to localhost access.	Enabled ▾
Set Rebuild Priority:	Medium ▾
Set Enclosure Fan Speed:	Auto ▾
Port Number:	7402
Enable collecting system logs.	Disabled ▾
Temperature Unit:	°F ▾
<input type="button" value="Submit"/>	

The following table enumerates the **System Setting** that you can adjust.

Table 11: System Setting Options

Option	Description
Enable auto rebuild	(default: Enabled) When a disk fails, the NVMe RAID AIC will take the disk offline. The NVMe RAID AIC will automatically rebuild the array after you have configured spare disks or replaced the disk, but only if the Enable auto rebuild option is enabled.
Enable continue rebuilding on error	(default: Enabled) When enabled, the rebuilding process will ignore bad disk sectors and continue rebuilding until completion. When the rebuild is finished, the data may be accessible but inconsistent due to any bad sectors that were ignored during the procedure. HighPoint recommends checking the event log periodically for bad sector warnings if this option is enabled.
Enable audible alarm	(default: Enabled) The audible alarm sounds when the following conditions occur: <ul style="list-style-type: none"> - Disk Dropped - Fan Speed lower than 600 RPM - SSD Temperature is higher than the SSD warning threshold - Broadcom Chipset Temperature is higher than 105°C <p>You can adjust the audible alarm setting here.</p>  <p>Warning: Disabled audible alarm is permanently disabling the beeper, so please proceed with caution!</p>
Restrict to localhost access	(default: Enabled)

	<p>Remote access to the AIC will be restricted when enabled; other users in your network cannot log in to the WebGUI remotely.</p> <p>It is used as follows:</p> <ol style="list-style-type: none"> 1. Set Restrict to localhost access to Disabled. 2. Click Submit. 3. Turn off the local firewall. 4. View the local IP address. 5. Use another system to access WebGUI remotely by typing http://IP address:port number in the browser.
Set Rebuild Priority	<p>(default: Medium)</p> <p>You can specify the amount of system resources you want to dedicate to rebuilding the array. There are 5 levels of priority [Lowest, Low, Medium, High, Highest]</p>
Set Enclosure Fan Speed	<p>(default: Auto)</p> <p>You can adjust the speed of the fan. There are 5 levels [Auto, Off, Low, Medium, High]</p>
Port Number	<p>(default: 7402)</p> <p>You may change it to any open port. (only for Windows)</p>
Enable collecting system logs	<p>(default: Disabled)</p> <p>You can set it to enable the collection of system logs at any time. The collected system logs are stored on C:/Windows/hpt_diagdriver. The maximum size of the collected system log is 840MB; anything over 840MB will be overwritten forward.</p> <p>This setting is only supported by the Windows HighPoint RAID Management.</p> <p>It is used as follows:</p> <ol style="list-style-type: none"> 1. Set Enable collecting system logs to Enabled. 2. Click Submit. 3. Reboot the system. 4. Duplicate the problems encountered. 5. Collect system logs with one click.
Temperature Unit	<p>(default: °F)</p> <p>The default temperature unit is Fahrenheit, and you can change it to Celsius.</p> <p>This setting is only supported by the Windows HighPoint RAID Management.</p>

6.5.2. Password Setting

Using this tab, you can set or change your WebGUI password. The password length is less than or equal to 8 bits, and there is no limit to the valid complexity of the password.

Password Setting

Password:

Confirm:

Type your new password, confirm it, then click **Submit**.

6.5.3. Email Setting

Using this tab, you can instruct the AIC to email the recipients of your choosing when certain events trigger.

6.5.3.1. Add an Email Server

To add an email server, complete the items in the **SMTP Setting**.

The following table enumerates the **SMTP Setting**.

Table 12: SMTP Setting Options

SMTP Setting Option	Description
Enable Event Notification	Check the Enable Event Notification box to use the Event Notification.
Server Address (name or IP)	Enter the ISP (Internet service provider) Server Address or SMTP name.
Mail From (E-mail address)	Enter the email address of the sender.
Login Name	Enter the email account name of the sender.
Password	Enter the sender's email account password.
SMTP Port	Enter the SMTP port. (default: 25)

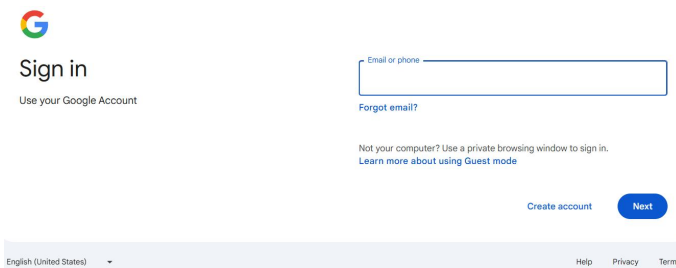
<p>Support SSL</p>	<p>Check the Support SSL box if SSL is supported by your ISP (port value will change to 465; refer to your ISP if you have a specific SMTP port).</p>
---------------------------	---

To add an email server, perform the following steps:

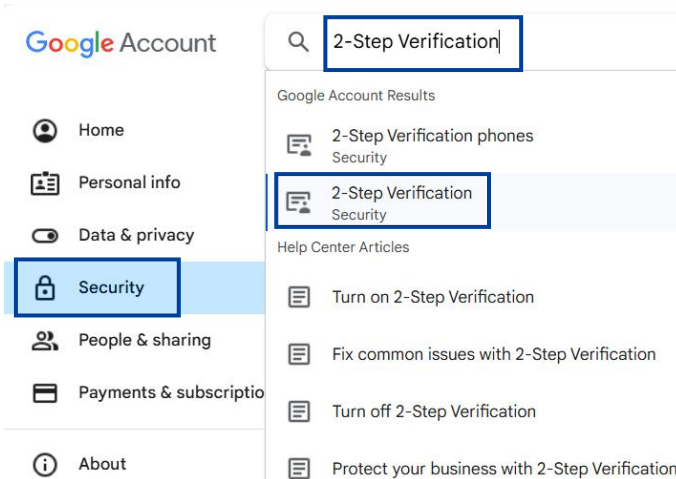
1. Open the **WebGUI**.
2. Click the **Setting** tab.
3. Check the **Enable Event Notification** box.
4. Enter the ISP server address or SMTP name in the **Server Address (name or IP)**.
5. Enter the email address of the sender (email account that is going to send the alert) in the **Mail From (E-mail address)**
6. Enter the account name of the sender in the **Login Name**.
7. Enter the sender's account password in the **Password**.

Example: Gmail

- 1) Sign in to Gmail and set it up, Login email address link: <https://accounts.google.com/Login>



- 2) Click the **Security** and search for the **2-Step Verification**.



- 3) Click the **Turn on 2-Step Verification** and follow Gmail’s prompts to complete the operation.

← 2-Step Verification

Turn on 2-Step Verification

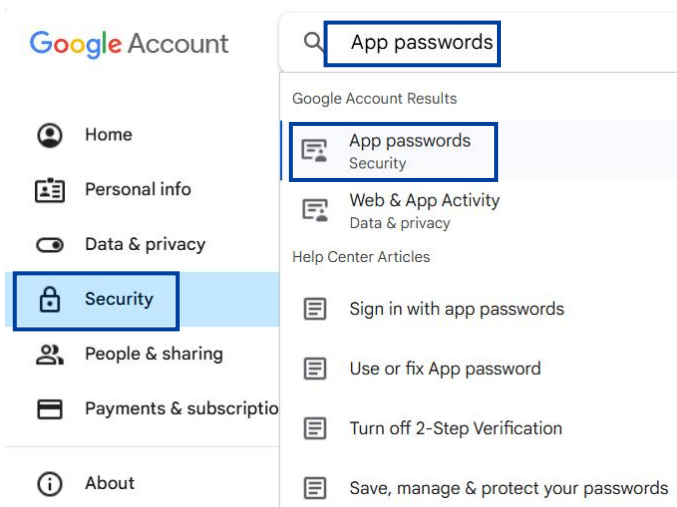
Prevent hackers from accessing your account with an additional layer of security.

Unless you’re signing in with a passkey, you’ll be asked to complete the most secure second step available on your account. You can update your second steps and sign-in options any time in your settings. [Go to Security Settings](#)



Turn on 2-Step Verification

- 4) Click the **Security** and search for the **App passwords**.



- 5) Click the **App passwords** and enter the app name.

← App passwords

App passwords help you sign into your Google Account on older apps and services that don’t support modern security standards.

App passwords are less secure than using up-to-date apps and services that use modern security standards. Before you create an app password, you should check to see if your app needs this in order to sign in.

[Learn more](#)

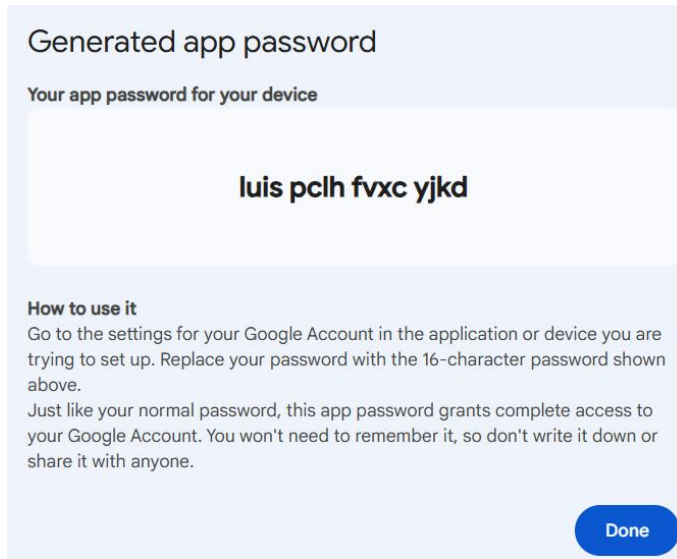
You don't have any app passwords.

To create a new app specific password, type a name for it below...

App name
HighPoint RAID Management

Create

- 6) Click **Create**, and you will get the new app-specific password. Enter this app-specific password into the **Password**.



8. Enter the SMTP port (default:25) in the **SMTP Port**.
9. Check the **Support SSL** box if your ISP supports SSL.
10. Click **Change Setting**.

6.5.3.2. Add an Email Recipient

To add multiple email addresses as notice receivers, you need to complete the items in **Add Recipient**.

Add Recipient

E-mail:

Name:

Event Level: Information Warning Error

The following table enumerates the **Add Recipient**.

Table 13: Add Recipient Options

Add Recipient Option	Description
E-mail	<p>Enter the email address of the recipient.</p> <p>If you want to receive notification mail using a Webmail account, you may need to modify the mailbox's permissions.</p>
Name	Enter the name of the recipient.
Event Level	<p>Check which type(s) of events will trigger an email in the respective Event Level check boxes.</p> <ul style="list-style-type: none"> - Inf (Information) - War (Warning) - Err (Error)
Add/ Test	<p>(Optional)</p> <ul style="list-style-type: none"> - Click Add to add the recipient. <p>The added recipient will be displayed under Recipients.</p> <p>The email will send your recipients the output recorded in the event log.</p> <ul style="list-style-type: none"> - Click Test to confirm settings are correct by sending a test email.

To add an email recipient, perform the following steps:

1. Open the **WebGUI**.
2. Click the **Setting** tab.
3. Type the email of the recipient in the **E-mail**.
4. Type the name of the recipient in the **Name**.

5. Select which type(s) of events will trigger an email using the respective **Event Level** check boxes.

6. **(Optional)** Click **test** to confirm the settings are correct by sending a test email.

7. Click **add** to add the email recipient to the recipient list.

6.5.3.3. List all Email Recipients

The added recipient will be displayed under **Recipients**.

Recipients		
E-mail	Name	Event Level
<input type="checkbox"/> hptu@ [redacted] .com <small>Delete</small>	hpt	Information , Warning , Error

6.5.3.4. Delete an Email Recipient

To delete an existing email recipient, perform the following steps:

1. Open the **WebGUI**.
2. Click the **Setting** tab.
3. Select the email recipient you want to delete under **Recipients**.
4. Click **Delete** to delete the email recipient.

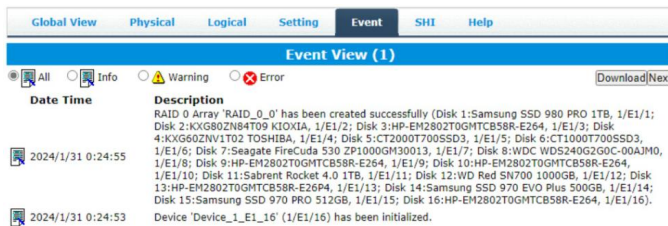
6.6. Event

The **Event View** is a basic error logging tool built into the HighPoint WebGUI. You can see log entries associated with the HighPoint device. The event log provides useful information when troubleshooting your setup.



6.6.1. View the Event Log

You can view the event log of RAID creation, RAID deletion, disk drop, disk up, etc.



You can switch between event views by clicking on **Prev** and **Next**.

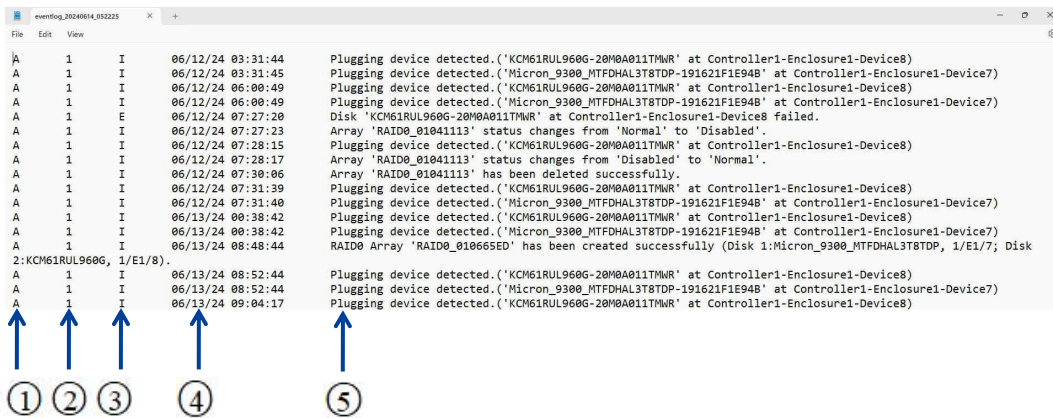
- **Prev** – View the previous log page
- **Next** – View the next log page

6.6.2. Save the Event Log

You can click **Download** to save the events log file on your system.



Open the downloaded event log.



The following table describes the Event Log.




Table 14: Event Log

No	Property Name	Description
①	Enclosure	Shows which specific Enclosure occurred the event.
②	Email delivery	0 Indicates that the event was not sent by Email. 1 Indicates that the event has been sent by Email.
③	Event Levels	Includes the following event levels: <ul style="list-style-type: none"> ● I – Information ● W – Warning ● E – Error
④	Event Time	Shows the exact time of the event.
⑤	Event Content	Shows the specifics of the event that occurred.

6.6.3. Event Log Icon Guide

The following table describes the Event Log Icon.

Table 15: Event Log Icon

Icon	Name	Definition
	Information	Includes general administrative tasks: <ul style="list-style-type: none"> ● Create/delete arrays ● Configuring spares ● Rebuilding arrays ● Configuring eventnotifications ● Configuring maintenance
	Warning	Alerts issued by the HostAdapter: <ul style="list-style-type: none"> ● High temperatures ● Sector errors ● Communication errors ● Verification errors
	Error	Hardware related problems: <ul style="list-style-type: none"> ● Disk failure ● Broken errors ● Memory failure

6.7.SHI

Storage Health Inspector (SHI) outputs information collected using SMART (Self-Monitoring Analysis and Reporting Technology) Disk Technology. The data provided on this tab helps you anticipate any disk failures based on various monitored disk properties.

Storage Health Inspector(SHI)						
Controller ID	Location#	Device Serial Number	RAID	°F	Total Bytes Written	S.M.A.R.T
1	E1_5	03F10707074404014589	None	91	268.34 TB	Detail
1	E1_6	694S10NBTVDQ	None	95	821.98 TB	Detail

HDD Temperature Threshold	
Set harddisk temperature threshold :	<input type="text" value="149"/> °F <input type="button" value="Set"/>

6.7.1. View the SHI Information

The **Storage Health Inspector (SHI)** tab is the default page when clicking the **SHI** tab of the WebGUI.

The **Storage Health Inspector (SHI)** section displays the following information.

Storage Health Inspector(SHI)						
Controller ID	Location#	Device Serial Number	RAID	°C	Total Bytes Written	S.M.A.R.T
1	E1_1	39US1018TR0Q	None	38	36.18 TB	Detail
1	E1_2	39US100MTR0Q	None	36	11.56 TB	Detail

- **Controller ID** – Controller ID where the disk is hosted.
- **Location** – The physical disk location (e.g., Device 1_E1_2 represents the disk on AIC 1 port 2).
- **Device Serial Number** – The serial number of the physical disk.
- **RAID** – The RAID array in which the disk resides.
- **°F/ °C** – Current temperature of the physical disk. Unit: °F/ °C.
- **Total Bytes Written** – The total number of bytes that can be written over the life of the SSD.
- **S.M.A.R.T** – Click **Detail** to display the SMART information of a single physical disk.

6.7.2. View the SMART Information

To access the SMART information of a single disk, perform the following steps:

1. Open the **WebGUI**.
2. Click the **SHI** tab.
3. Click the **Detail** on the desired disk.

Storage Health Inspector(SHI)						
Controller ID	Location#	Device Serial Number	RAID	%F	Total Bytes Written	S.M.A.R.T
1	E1_1	S48CNW0K400031X	RAID_1_0	91	192.85 TB	Detail
1	E1_2	XDR0A03D0UU1	RAID_0_0	95	14.80 TB	Detail
1	E1_3	S5GYNG0R206284E	RAID_1_0	86	109.04 TB	Detail
1	E1_4	XDR0A0370UU1	RAID_0_0	98	15.11 TB	Detail
Device Name		Device_1_E1_4				
Model Number		KIOXIA KC081PUG1T92				
Temperature		98°F				
Warning Composite Temperature Threshold		170°F				
Critical Composite Temperature Threshold		185°F				
NVME S.M.A.R.T Attributes						
Name						Value
Critical Warning						0x0
Composite Temperature (C)						37
Available Spare						100%
Available Spare Threshold						8%
Percentage Used						0%
Data Units Read						0x7af41cca
Data Units Written						0x1eef705
Host Read Commands						0x496eb2c6
Host Write Commands						0x1a2c25ca
Controller Busy Time						0xa14
Power Cycles						0xab
Power On Hours						0x7e
Unsafe Shutdowns						0x22
Media and Data Integrity Errors						0x0
Number of Error Information Log Entries						0x1
Warning Temperature Time						0x699
Critical Composite Temperature Time						0x0
Temperature Sensor 1 (C)						0
Temperature Sensor 2 (C)						0
Temperature Sensor 3 (C)						0
Temperature Sensor 4 (C)						0

Note: The TBW (Total Bytes Written) information can be used to monitor the lifespan of the NVMe disks.

6.7.3. Set the Temperature Threshold

To set the disks's temperature threshold, perform the following steps:

Notes:

This setting is not supported by the Linux HighPoint RAID Management.

149°F is the default. This setting can correspond with the disk manufacturer's official specifications.

1. Log in to the WebGUI.
2. Select the proper AIC using the drop-down menu on the top left.
3. Click the SHI tab.
4. Type temperature value.

HDD Temperature Threshold

Set harddisk temperature threshold : °F

If the temperature exceeds 149°F, it will display “Red”.

Storage Health Inspector(SHI)						
Controller ID	Location#	Device Serial Number	RAID	°F	Total Bytes Written	S.M.A.R.T
1	E1_1	S463NF0K409595F	None	150	1023.91 TB	Detail
1	E1_2	SSJYNS0N602754T	None	111	75.45 TB	Detail

HDD Temperature Threshold

Set harddisk temperature threshold : °F

6.7.4. Create a Health Inspector Scheduler

The **Health Inspector Scheduler (HIS)** enables you to schedule the disk and RAID array checkups to ensure they function optimally.

Storage Health Inspector (SHI)						
Controller ID	Location#	Device Serial Number	RAID	°F	Total Bytes Written	S.M.A.R.T
1	E1_3	S5GYNGOR206308X	RAID0_00A84D17	89	116.72 TB	Detail
1	E1_7	S5GYNGOR205478M	RAID0_00A84D17	82	322.93 TB	Detail

If you install the software for the first time, there will be a default check disk task here, which you can decide whether to keep or not, depending on your needs.

Tasks List	
Name	Description
<input type="checkbox"/> DefaultTask	Check all disks every 1 minute(s). Delete

When the operating temperature of the disk exceeds the temperature threshold, a Warning event will appear in the **Event** view.

To create a Health Inspector Scheduler, perform the following steps:

1. Open the **WebGUI**.
2. Click the **SHI** tab.
3. Set the **Task Name** and the time value in the **Occurs every**.

Health Inspector Scheduler

Task Name:

Occurs every:

4. After clicking **Submit**, your task will be shown under the **Task List**.

Tasks List	
Name	Description
<input type="checkbox"/> DefaultTask	Check all disks every 1 minute(s). Delete
<input type="checkbox"/> test	Check all disks every 1 minute(s). Delete

6.7.5. Create a New Verify Task

The Scheduler enables you to schedule disk/array checkups to ensure arrays are functioning optimally.

All redundant RAID arrays (RAID1/ RAID10) will appear under the New Verify Task.

To create a Health Inspector Scheduler, perform the following steps:

If you want to create a new verify task. You need to follow the steps below.

1. Open the **WebGUI**.
2. Select the proper AIC from the top left drop-down.
3. Click **SHI**.
4. Click **Schedule**.
5. Select the array you want to schedule the verify task.
6. Type the name in the **Task Name** entry box.
7. Choose whether you want to schedule.
8. One-time verify task on a specific date (YYYY-MM-DD) at (HH:MM:SS, 24-hr clock). Or a specific schedule you can adjust based on Daily, Weekly, or Monthly options.
9. Click **Submit**.
10. Your entry will appear under the **Tasks List**.

Tasks List	
Name	Description
<input type="checkbox"/> DefaultTask	Check all disks every 1 minute(s).
<input type="checkbox"/> test	Verify array "RAID_1_0" every day at 2:0:0 from 2024-5-21.

Note: The New Verify Task box only appears if you have normal status arrays. If you have a critical array, the New Rebuild Task will replace the New Verify Task.

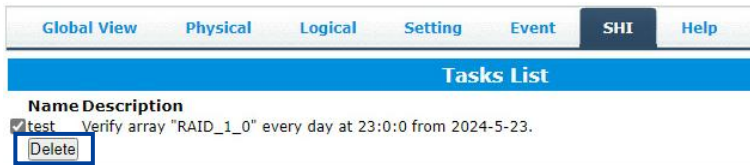
6.7.6. Delete a Task

The Scheduler enables you to schedule disk/array checkups to ensure arrays are functioning optimally.

All redundant RAID arrays (RAID1/ RAID10) will appear under the New Verify Task.

To delete an existing task, perform the following steps:

1. Open the **WebGUI**.
2. Click **SHI**.
3. Click **Schedule**.
4. Select the task you want to delete under the **Tasks List**.
5. Click **Delete** to delete the task.



6.8. Help



The **Help** displays help related to the WebGUI. The **Help** displays information about the AIC connection to the system and the AIC and driver status.

6.8.1. Online Help

Online Help redirects you to the official HighPoint website.

6.8.2. Diagnostic View

Diagnostic View provides a **1-click** information collection system for troubleshooting. It will gather and compile all necessary hardware, software, and storage configuration data into a single file.

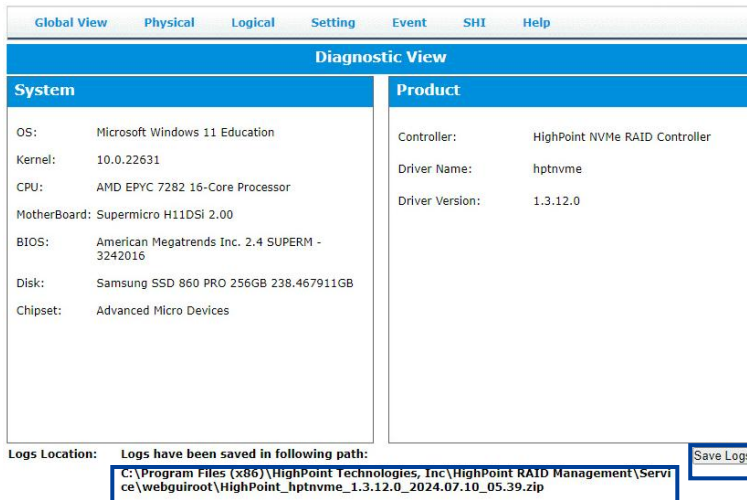
Global View		Physical		Logical		Setting		Event		SHI		Help	
Diagnostic View													
System							Product						
OS:	Microsoft Windows 11 Education						Controller:	HighPoint NVMe RAID Controller					
Kernel:	10.0.22631						Driver Name:	hptnvme					
CPU:	AMD EPYC 7282 16-Core Processor						Driver Version:	1.3.12.0					
MotherBoard:	Supermicro H11DSi 2.00												
BIOS:	American Megatrends Inc. 2.4 SUPERM - 3242016												
Disk:	Samsung SSD 860 PRO 256GB 238.467911GB												
Chipset:	Advanced Micro Devices												
Logs Location:				Logs have not been saved				Save Logs					

6.8.3. Save the Diagnostic Log

To save the Diagnostic log, perform the following steps:

1. Click the **Save Logs** button to create the diagnostic file.
2. **Logs Location** will display the location of the saving path.

- **For Windows User**



The following table lists and describes each folder in the log zip file.

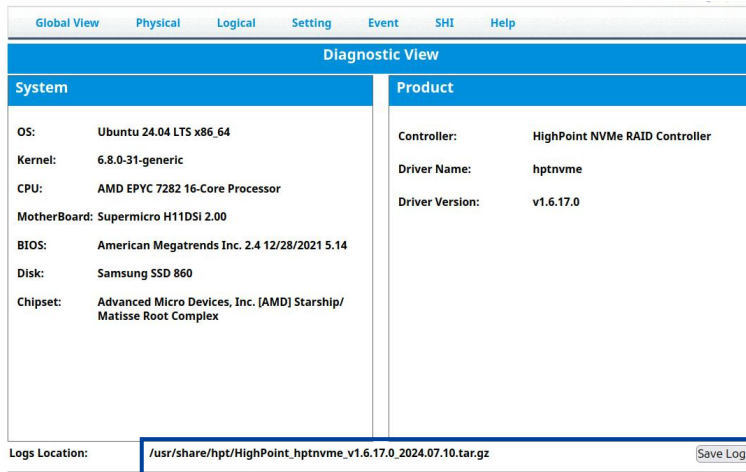
Name	Type	Compressed size	Password ...	Size	Ratio
log	File folder				
etc	File folder				
xsl	File folder				
Index	Microsoft Edge HTML Do...	1 KB	No	1 KB	57%

Table 16: Description of each folder in the log zip file (Windows)

Folder	Property	Description
Log	hpt CPU.txt	CPU configuration of the current system.
	hpt Disk.txt	Number and names of disks in the current system. You can also see the capacity of the disk.
	hpt driver.txt	Record all driver information used in Windows. Include the driver's name, version, and status.
	hpt Pci.txt	Information about all PCIe devices connected to the motherboard.
	hpt {drivename}.log	Record activity log in WebGUI. Collect driver runtime logs to check if the driver is working properly.
	hpt service.txt	Record the status of all services in the system.
	hpt diag.txt	Collect the runtime logs of management software to detect any abnormalities.
	drInst. {date}.dmp	Collect the crash logs of management software for analysis.
	hpt temperature.txt	Collects chip and disk temperature information to monitor thermal conditions.
	hpt_temperature.csv	
hpt_xxx.txt	AIC log information, including creation/deletion of RAID and exception	

		events. xxx is the SN number of AIC.
	hpt systemEvent.log	Event from Windows.
	MEMORY.DMP	Record information after system BSOD/Crash; you can just collect it in DataRAID.
	setupapi.dev.txt	Record the installation log of the driver. This is the log generated by the operating system itself. This can be used to check the log of the AIC installed driver showing an exclamation mark.
	hptnvmeco.txt	This is generated by HighPoint and is used to determine the reason for the exclamation mark when the NVMe driver is installed.
	hpt diagdriver.txt	Debug driver log information, including error information.
Index.xml	RAID Management web page	<p>On the HTML webpage, record the screenshot information for each page of this WebGUI.</p> <ul style="list-style-type: none"> ● Diagnostic View—CPU, Motherboard model, BIOS, driver version. ● Global view—Record disk and RAID utilization. ● Physical—Record the RAID Controller and disk PCIe width. ● Logical—Record the RAID status and the member of the RAID. ● Setting—Record the status of the WebGUI function setting. ● Event—Record activity log in WebGUI. ● SHI—Record the smart info of disks.
xsl	RAID Management web page	It contains components that allow local html files to be opened.
otc	0-switch	<ul style="list-style-type: none"> ● event.txt—Collect sensor information every minute, including power voltage, fan speed, and temperature. ● info.txt—Collect AIC information, including firmware, SN, firmware version, chip/board temperature, voltage/power, and fan speed. ● log.txt—AIC log, including RAID operation, disk drop, fan speed abnormal, temperature abnormal, voltage abnormal. ● Port.txt—AIC downstream port info, including width, speed, and PCIe configuration space. ● trace.txt—Collect firmware runtime log. ● {sn}.bin—AIC factory data, including the initial setup parameters.

● For Linux User



The following table lists and describes each folder in the log zip file.

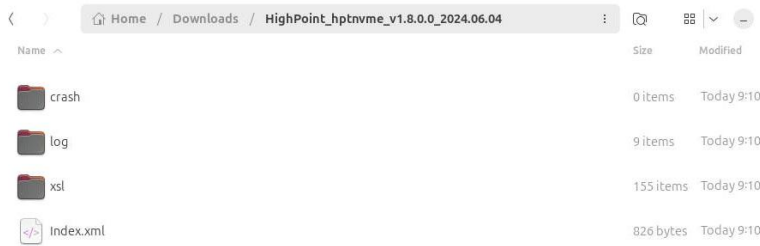
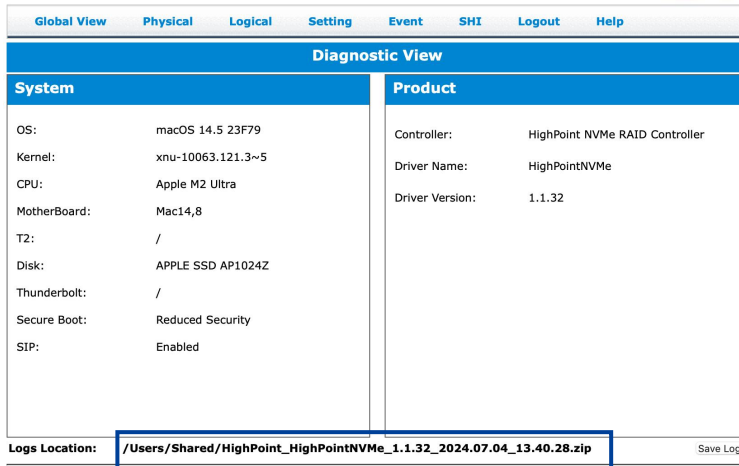


Table 17: Description of each folder in the log zip file (Linux)

Folder	Property	Description
log	cpu info.txt	CPU configuration of the current system.
	disk info.txt	Number and names of disks in the current system.
	dmesg info.txt	Kernel log in Linux.
	dmidecode info.txt	Instructions to view hardware information, BIOS, system, motherboard, processor, memory, cache, etc.
	hptdrv log	HighPoint driver installation log.
	lsmod info	Record all driver information used in Linux.
	kern.log	System kernel log.
	lspci info	Information about the PCIe device connected to the motherboard.
Index.xml	RAID Management web page	HTML webpage, record the screenshot information of each page of this WebGUI <ul style="list-style-type: none"> ● Diagnostic View—CPU, Motherboard model, BIOS, driver version. ● Global view—Record disk and RAID utilization. ● Physical—Record the RAID Controller and disk PCIe width.

		<ul style="list-style-type: none"> ● Logical—Record the RAID status and the member of the RAID. ● Setting—Record the status of the WebGUI function setting. ● Event—Record activity log in WebGUI. ● SHI—Record the smart info of disks.
xsl	RAID Management web page	It contains components that allow local html files to be opened.
crash	N/A	It contains logs saved by the Linux system crash.
otc	0-switch	<ul style="list-style-type: none"> ● event.txt—Collect sensor information every minute, including power voltage, fan speed, and temperature. ● info.txt—Collect AIC information, including firmware, SN, firmware version, chip/board temperature, voltage/power, and fan speed. ● log.txt—AIC log, including RAID operation, disk drop, fan speed abnormal, temperature abnormal, voltage abnormal. ● Port.txt—AIC downstream port info, including width, speed, and PCIe configuration space. ● trace.txt—Collect firmware runtime log. ● {sn}.bin—AIC factory data, including the initial setup parameters.

● For macOS User



The following table lists and describes each folder in the log zip file.

Index.xml	Jul 4, 2024 at 13:40	761 bytes	XML document
kernel.log	Jul 4, 2024 at 13:44	48.1 MB	Log File
> log	Jul 4, 2024 at 13:40	--	Folder
SystemInformation.spx	Jul 4, 2024 at 13:40	9.5 MB	System Report
> xsl	Jul 4, 2024 at 13:40	--	Folder

Table 18: Description of each folder in the log zip file (macOS)

Folder	Property	Description
log	DiagnosticReports	This is the crash log, including driver and WebGUI crashes in this directory, which have error file generation.
	Log	Mainly, system and application runtime logs
	Disk log	Number and names of disks in the current system.
	Ioreg log	Information about the Pcie device connected to the macOS.
Index.xml	RAID Management web page	HTML webpage, record the screenshot information of each page of this WebGUI <ul style="list-style-type: none"> ● Diagnostic View—CPU, Motherboard model, BIOS, driver version. ● Global view—Record disk and RAID utilization. ● Physical—Record the RAID Controller and disk PCIe width. ● Logical—Record the RAID status and the member of the RAID. ● Setting—Record the status of the WebGUI function setting. ● Event—Record activity log in WebGUI. ● SHI—Record the smart info of disks.
Kernel.log	N/A	Kernel log in macOS.
Systeminformation.spx	N/A	System report for macOS, including macOS version, CPU, pci log.
xsl	RAID Management web page	It contains components that allow local html files to be opened.

7. Command Line Interface

The Command Line Interface is often referred to as CLI. This section describes the various HighPoint CLI commands: query, create, delete, rebuild, verify, unplug, switch, lscard, rescan, init, events, mail, task, set, clear, diag, help, exit, ver, diag secure and update.



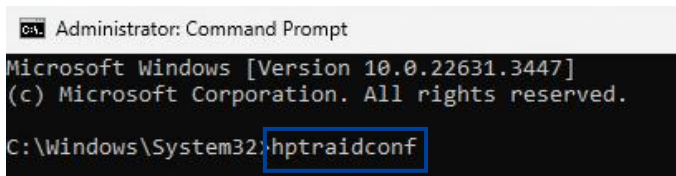
Warning: Using create/ delete commands may destroy data stored in the disks, and this lost data can never be recovered.

Please be cautious when executing these commands. The CLI utility will not prompt you before each command is executed.

7.1. Start the CLI

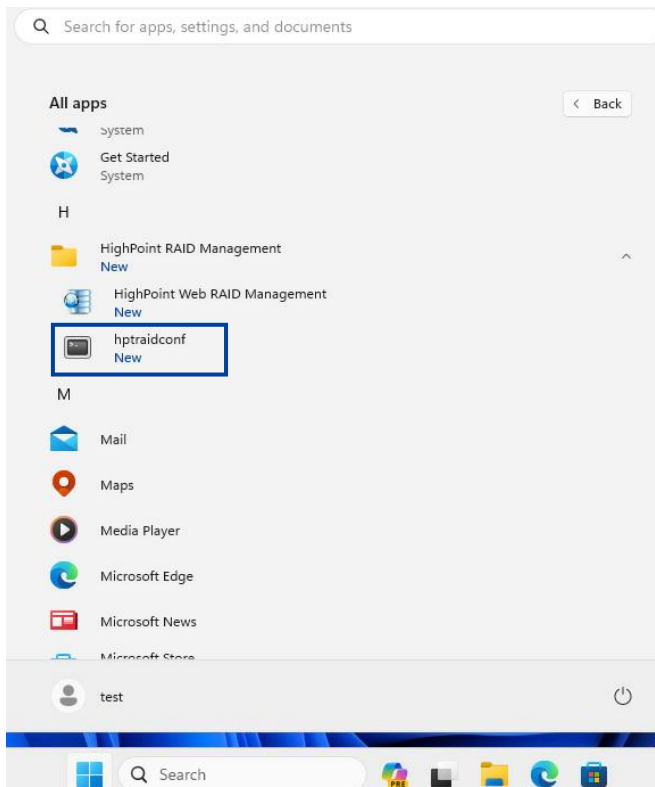
For Windows Users

- **Method 1:** Run **Command Prompt** as Administrator, enter **hptraidconf**, and press **Enter**.



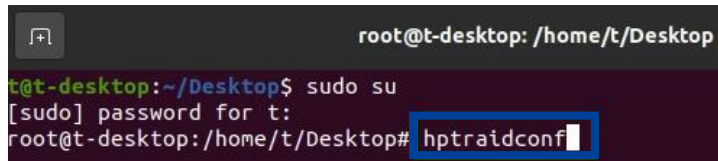
```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22631.3447]
(c) Microsoft Corporation. All rights reserved.
C:\Windows\System32>hptraidconf
```

- **Method 2:** Click **Start** to find the **HighPoint RAID Management** folder, and click on **hptraidconf**.

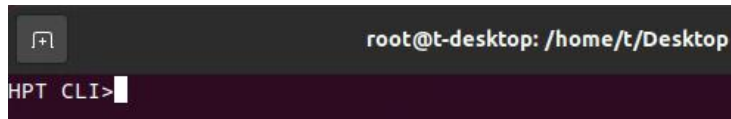


For Linux Users

1. Open the **Terminal** and enter root permissions.
2. Execute the command **hptraidconf** to enter the CLI.



```
root@t-desktop: /home/t/Desktop  
t@t-desktop:~/Desktop$ sudo su  
[sudo] password for t:  
root@t-desktop:/home/t/Desktop# hptraidconf
```



```
root@t-desktop: /home/t/Desktop  
HPT CLI>
```

7.2. Query Commands

```
HPT CLI > query
Query Command
    This command allows you to query devices or arrays' informations.
Syntax:
    query controllers
    query enclosures
    query devices
    query devices {device_id}
    query arrays
    query arrays {array_id}
Note:
    The query devices {device_id} has add S.M.A.R.T information in version 2.1.
```

You can use the query command to view the AIC status and disk information.

The following table lists and describes the properties of the query command.

Table 19: Properties for query Command

cmd	Property Name	Value Range	Description
query	controllers	N/A	This command reports AIC information
query	enclosures	N/A	This command reports AIC Product ID information.
		{enclosure_id}	This command presents information of the specified AIC.
query	devices	N/A	This command presents information of the physical disks hosted by the AIC.
		{device_id}	This command presents information for the specified physical disk.
query	arrays	N/A	This command lists information about each configured array, such as ID, capacity, RAID type, and status.
		{arrays_id}	This command presents information of each disk of a specified array.

7.2.1. Query Controller

HPT CLI>query controllers

This command reports AIC information.

Input example:

HPT CLI>query controllers

```
HPT CLI > query controllers
ID          Channel      Name
1           0            HighPoint NVMe RAID Controller
-----
```

- **ID** - The number of the AIC.
- **Channel** - The HighPoint NVMe AIC is a virtual device with a channel default of 0.
- **Name** - The AIC's model name.

7.2.2. Query Enclosure

HPT CLI>query enclosures

This command reports AIC Product ID information.

Input example:

HPT CLI>query enclosures

```
HPT CLI > query enclosures
ID      Secure  VendorID      ProductID      NumberOfPYH
-----
1/E1 No   HPT          SSD7749M2 NVMe Controller  16
```

- **ID** - An AIC ID is a string used to represent an AIC. It is in the format “1/AIC” for AICs.
- **Secure** - Whether the AIC is secured
- **VendorID** - An AIC property indicating the vendor-assigned ID number of the AIC.
- **ProductID** - The model name of the AIC.
- **NumberOfPYH** - The number of connected physical devices supported by the AIC.

7.2.3. Query Device

HPT CLI>query devices

This command will provide the status of each physical disk hosted by the AIC.

Input example:

HPT CLI>query devices

```
HPT CLI > query devices
ID      Secured   Capacity  MaxFree  Flag   Status  ModelNumber
-----
1/E1/1  No        960.13   460.10   RAID   NORMAL  Samsung SSD 983 DCT 960GB
1/E1/2  No        3840.76  0         SINGLE LEGACY  Micron_9300_MTFDHAL3T8TDP
1/E1/3  No        500.03   0         RAID   NORMAL  Samsung SSD 980 PRO 500GB
1/E1/4  Yes(locked) 375.08  0         SINGLE NORMAL  INTEL SSDPE21K375GA
-----
```

- **ID** - A disk ID is a string used to represent a disk. It is in the “AIC/port/ device” format for NVMe AICs. e.g., 1/E1/2 represents the disk on AIC 1 port 2.
- **Secured** - Whether the physical disk is secured.
- **Capacity** - The disk's capacity is GB.
- **MaxFree** - The maximum sequence free space on the disk can be used to create the array.
- **Flag** - Shows whether the disk is SINGLE or has been created RAID.
- **Status** - This will display the disk status (1 of 4 possible states):
 - **LEGACY**: The disk's status is legacy.
 - **DISABLED**: The disk cannot be used. (May be related to disk failure)
 - **NORMAL**: The disk is a member of a RAID array.
 - **SPARE**: The disk has been set as a spare disk.
- **ModelNumber** - The disk's model number.

HPT CLI>query devices {device_id}

This command presents information for the specified physical disk.

Input example:

HPT CLI>query devices 1/E1/6

```

HPT CLI > query devices 1/E1/6
Mode Number:      KXG60ZNV1T02 TOSHIBA
Serial Number:    ██████████
Firmware Version: AGGA4102
Capacity(GB):    1024.21      TotalFree(GB): 0
Status:          SINGLE      Flag:          LEGACY
SED Capable:     No          SED Type:      None
Secured:         No          Cryptographic Erase Capable: No
PCIe Width:      x4          PCIe Speed:    Gen 3
Temperature (F): 96
Warning Composite Temperature Threshold (F): 172
Critical Composite Temperature Threshold (F): 179
-----
                          S.M.A.R.T Attributes
S.M.A.R.T Status OK.
Name                Value
-----
Critical Warning    : 0x0
Composite Temperature (C) : 36
Available Spare     : 100%
Available Spare Threshold : 10%
Percentage Used     : 90%
Data Units Read    : 0x76d62aa9
Data Units Written  : 0x6936c6ab

```

- **Mode Number** - The disk's model number.
- **Serial Number** - The serial number of the physical disk.
- **Firmware Version** - The disk's Firmware version.
- **Capacity** - The disk's capacity.
- **TotalFree (GB)** - The total capacity that is not configured.
- **Status** - The disk's status.
 - **LEGACY:** The disk's status is legacy.
 - **DISABLED:** The disk cannot be used. (May be related to disk failure)
 - **RAID:** The disk is a member of a RAID array.
 - **SPARE:** The disk has been set as a spare disk.
- **Flag** - Shows whether the disk is single or has been created RAID.
- **SED Capable** - Whether the disk supports the SED feature.
- **SED Type** - The current SED Type of the physical disk is OPAL
- **Secured** - Whether the disk is secured.
- **Cryptographic Erase Capable** - Whether the disk supports the Cryptographic Erase feature.
- **PCIe Width** - The disk's PCIe width.
- **PCIe Speed** - The disk's PCIe speed.

- **Temperature** - The disk's temperature.
- **Warning Composite Temperature Threshold (F)** - The disk's warning composite temperature threshold.
- **Critical Composite Temperature Threshold (F)** - The disk's critical composite temperature threshold.
- **S.M.A.R.T Attributes** - S.M.A.R.T Attributes detailed information reported by disk.

7.2.4. Query Array

HPT CLI>query arrays

This command lists information about each configured array, such as array ID, secured status, capacity, RAID type, status, and array attributes.

Input example:

```
HPT CLI> query arrays
```

```
HPT CLI > query arrays
ID          Secured Capacity(GB)  Type      Status  Block  Sector  Cache      Name
-----
1           No           7681.01  RAID0    NORMAL  512k   512B     NONE      RAID_0_0
```

HPT CLI>query arrays {arrays id}

This command will present information of each disk of a specified array.

Input example:

```
HPT CLI>query arrays 1
```

```
HPT CLI > query arrays 1
ID: 1 Name: RAID10_0
Type: RAID10 Status: NORMAL
Capacity(GB): 1919.85 BlockSize: 512k
SectorSize: 512B CachePolicy: NONE
Progress: -- Secure: No
-----
ID          Secured Capacity(GB)  Type      Status  Block  Sector  Cache      Name
-----
1-1        No           239.98  RAID1    NORMAL  --     512B     NONE      [RAID10_0]
1-2        No           239.98  RAID1    NORMAL  --     512B     NONE      [RAID10_0]
1-3        No           239.98  RAID1    NORMAL  --     512B     NONE      [RAID10_0]
1-4        No           239.98  RAID1    NORMAL  --     512B     NONE      [RAID10_0]
1-5        No           239.98  RAID1    NORMAL  --     512B     NONE      [RAID10_0]
1-6        No           239.98  RAID1    NORMAL  --     512B     NONE      [RAID10_0]
1-7        No           239.98  RAID1    NORMAL  --     512B     NONE      [RAID10_0]
1-8        No           239.98  RAID1    NORMAL  --     512B     NONE      [RAID10_0]
```

- **ID** - The array's ID. A number generally represents an array ID.
- **Secured** - Whether the array is secured.
- **Capacity** - The capacity of the array is GB.
- **Type** - The array's type. (RAID0, RAID1, RAID10)
- **Status** - The array's status.
 - **NORMAL**: The array status is normal.
 - **CRITICAL**: The array is degraded (no data redundancy).
 - **DISABLED**: The array is disabled.
 - **REBUILDING**: The array is being rebuilt.
 - **VERIFYING**: The array is verifying.
 - **INIT(F)**: Initializing an array using Foreground mode.

- **INIT(B):** Initializing an array using Background mode.
- **UNINITIALIZED:** The array is not initialized.
- **Block** - The block size of the array.
- **Sector** - The bytes per sector of the array.
- **Name** - The name of the RAID array in the system.

7.3. Init Commands

```
HPT CLI > init
init command
    Init the array or device.
Syntax:
    init {device id| array id} {start|stop}
```

You can use init commands to initialize disks or arrays. A disk must be initialized first before being used to create arrays.

The following table lists and describes the properties of the init command.

Table 20: Properties for init Command

cmd	Property Name	Value Range	Description
init	{device_id}	The disk hosted by the AIC	This command initializes a disk for first use or a legacy disk on the AIC.
init	{array_id}	The created RAID array	This command starts/stops the initialization process of a redundant RAID array (RAID1).
	{start stop}	start/ stop	

7.3.1. Init a Physical Disk

HPT CLI>init {device id}

This command initializes a disk for first use or a legacy disk on the AIC.

Input example:

```
HPT CLI>init 1/E1/1
```

```
HPT CLI > query devices
ID      Secured  Capacity  MaxFree  Flag  Status  ModelNumber
-----
1/E1/1  No       960.13   460.10   RAID  NORMAL  Samsung SSD 983 DCT 960GB
1/E1/2  No       3840.64  0        SINGLE LEGACY  Micron_9300_MTFDHAL3T8TDP
1/E1/3  No       500.03   0        RAID  NORMAL  Samsung SSD 980 PRO 500GB
1/E1/4  Yes(lock) 375.08   0        SINGLE NORMAL  INTEL SSDPE21K375GA

HPT CLI > init 1/E1/2
Init device(1/E1/2) successfully!

HPT CLI > query devices
ID      Secured  Capacity  MaxFree  Flag  Status  ModelNumber
-----
1/E1/1  No       960.13   460.10   RAID  NORMAL  Samsung SSD 983 DCT 960GB
1/E1/2  No       3840.64  3840.64  SINGLE NORMAL  Micron_9300_MTFDHAL3T8TDP
1/E1/3  No       500.03   0        RAID  NORMAL  Samsung SSD 980 PRO 500GB
1/E1/4  Yes(lock) 375.08   0        SINGLE NORMAL  INTEL SSDPE21K375GA
```

7.3.2. Init a RAID Array

HPT CLI>init{array_id} {start|stop}

This command starts/stops the initialization process of a redundant RAID array (RAID1).

Input example:

HPT CLI>init 1 stop

```
HPT CLI > init 1 stop
```


7.4. Create Command

```

HPT CLI > create
Create Command
  This command allows you to create a new RAID array or add a spare disk.
Syntax:
  create {RAID0|RAID1|RAID3|RAID5|RAID6|RAID10|RAID50|JBOD|spare} [create-options]
create-option:
  disks=1/2,1/3... or disks=*
    Specify the disks used to create array.
  name=array name
    Specify the name of the array which will be created.
  src=source array ID
    If src argument is specified, OCE/ORLM will be started.
  cp=WB, WT or NONE
    Cache Policy option (WB: write back, WT: write through).
  init={foreground|background|keepdata|quickinit}
    Specifies array initialization option.
    foreground:
      Zero out all data on the array. The array is not
      accessible by the operating system until initialization is completed.
    background:
      Allow instant access to the array. Parity blocks
      will be generated in background.
  keepdata:
    Setup array information blocks on the drives only.
    Use this option for array recovery.
  quickinit:
    Setup array information blocks and zero out MBR data on the array.
  capacity=array capacity
    Specify the capacity (xxM,xxG) of the target array.
  matrix=n*m
    When create RAID50 to specify the matrix options.
    n : number of subarray's disk, m: number of subarray.
    For example: When create a RAID50 the option matrix
    can be matrix=3*2. That means 2 RAID5s each with 3 disks to form a RAID50
  bs=size
    Specify the block size (16k,32k,64k,128k,256k,512k,1024k)
  sector=size
    Specify the sector size (512B,1k,2k,4k)
  secure={y|n} {force}
    Specify if array is secured.
HPT CLI >

```

You can use create commands to create a new RAID array and add a spare disk.

Note: RocketAIC series NVMe AIC SSDs are already pre-configured with RAID0. You can skip those steps. You can follow the steps if you want to use another type of RAID.

The following table lists and describes the properties of the create command.

Table 21: Properties for create Command

cmd	Property Name	Value Range	Description
create	ArrayType	RAID0	Specify the RAID level to be created.
		RAID1	The AIC supports RAID levels 0, 1, and 10.
		RAID10	
	create-options	disks	Specifies member disks that will compose a new array. disks=1/2,1/3...or disks=* * Indicates creation of RAID array using all member disks.
	name	Specify the name of the array which will be created. (Default: RAID_ <level>_ <array number>)	
	src	Specifies an existing array to be expanded/migrated. All data on the	

			source array will be redistributed online to the target array. If this parameter is omitted, a new array is created.
		init	<p>Specifies array initialization option.</p> <ul style="list-style-type: none"> - foreground: Zero out all data on the array. The array is not accessible by the operating system until initialization is completed. (Not Recommended) - background: Allow instant access to the array. Parity blocks will be generated in the background. (Not Recommended) - keepdata: Setup array information blocks on the drives only. Use this option for array recovery. - quickinit: Setup array information blocks and zero out MBR data on the array. <p>Important Note: The Foreground and Background Initialization options will cause NVMe media to result in TBW and performance degradation. Initialization of a disk sets all data bits to 0, clearing all the data on the disk. It is important to initialize disks as previous data physically stored on the disk may interfere with new data.</p>
		capacity	<p>Specify the capacity of the target array.</p> <p>capacity=10MB/1000MB...or capacity=*</p> <p>* Indicates creation of RAID array using all disk capacities.</p>
		bs	<p>It allows you to adjust the block size to fit your disk usage, which can result in some performance gain.</p> <ul style="list-style-type: none"> - 128K - 256K - 512K (Default) <p>In a typical RAID configuration, virtual disk data is striped (or spread across) the physical disks. A smaller array block size will increase the likelihood of accessing all physical disks when processing large I/O requests. Multiple physical disks working in parallel increase the throughput, meaning better performance.</p>
		sector	<p>Specifies the target array's logical sector size in B/KB. This option is only valid for striped RAID levels.</p>

		secure	Allows you to use the RAID array's SED capabilities. Only AIC that supports the SafeStorage Encryption feature will have this option.
create	space	spare	This command allows you to add a spare disk.
	{device_id}	The disk hosted by the AIC	

7.4.1. Create a RAID Array

HPT CLI>create RAID{RAID0|RAID1|RAID10} [create-options]

This command allows you to create a new RAID array.

Input example:

HPT CLI>create RAID0 disks=* capacity=* init=quickinit bs=512k

```
HPT CLI > create RAID0 disks=* capacity=* init=quickinit bs=512k
Create array successfully.

HPT CLI > query arrays
ID          Secured Capacity(GB)  Type      Status  Block  Sector  Cache      Name
-----
0          No          1500.08  RAID0    NORMAL  512k   512B    NONE      RAID0_0
```

7.4.2. Create a Spare Disk

HPT CLI>create spare {device_id}

This command allows you to add a spare disk.

Input example:

HPT CLI>create spare disks=1/E1/1

```
HPT CLI > create spare disks=1/E1/1
Add spare disk successfully.

HPT CLI > query devices
ID          Secured  Capacity  MaxFree  Flag  Status  ModelNumber
-----
1/E1/1    No          1000.12  1000.12  SINGLE  SPARE    Samsung SSD 980 PRO 1TB
1/E1/2    No          4096.73  4096.73  SINGLE  NORMAL   KXG80ZN84T09 KIOXIA
1/E1/3    No          2000.31  2000.31  SINGLE  NORMAL   HP-EM2802T0GMCB58R-E264
1/E1/4    No          1024.08  1024.08  SINGLE  NORMAL   KXG60ZNV1T02 TOSHIBA
1/E1/5    No          2000.31  2000.31  SINGLE  NORMAL   CT2000T700SSD3
1/E1/6    No          1000.12  1000.12  SINGLE  NORMAL   CT1000T700SSD3
1/E1/7    No          1000.12  1000.12  SINGLE  NORMAL   Seagate FireCuda 530 ZP1000GH30013
1/E1/8    No          239.98   239.98   SINGLE  NORMAL   WDC WD5240CZG0C-00AJH0
1/E1/9    No          2000.31  2000.31  SINGLE  NORMAL   HP-EM2802T0GMCB58R-E264
1/E1/10   No          2000.31  2000.31  SINGLE  NORMAL   HP-EM2802T0GMCB58R-E264
1/E1/11   No          1000.12  1000.12  SINGLE  NORMAL   Sabrent Rocket 4.0 1TB
1/E1/12   No          1000.12  1000.12  SINGLE  NORMAL   WD Red SN700 1000GB
1/E1/13   No          2000.31  2000.31  SINGLE  NORMAL   HP-EM2802T0GMCB58R-E264
1/E1/14   No          500.03   500.03   SINGLE  NORMAL   Samsung SSD 970 EVO Plus 500GB
1/E1/15   No          512.04   512.04   SINGLE  NORMAL   Samsung SSD 970 PRO 512GB
1/E1/16   No          2000.31  2000.31  SINGLE  NORMAL   HP-EM2802T0GMCB58R-E264
```

7.5.Delete Command

```
HPT CLI > delete
Delete Command
  This command allows you to delete an existing RAID array or remove
  a spare disk. After deletion, the original array and all data on it
  will be lost. All the member disks will be listed as available single disks.
Syntax:
  delete {array id | spare id}
```

You can use delete commands to delete an existing RAID array or remove a spare disk.

After deletion, the original array and all data will be lost. All the member disks will be listed as available single disks.

The following table lists and describes the properties of the delete command.

Table 22: Properties for delete Command

cmd	Property Name	Value Range	Description
delete	{spare_id}	The added spare disk	This command instructs the system to delete the spare disk.
delete	{array_id}	The created RAID array	This command instructs the system to delete the array.

7.5.1.Delete a RAID Array

HPT CLI>delete {array id}

This command allows you to delete an existing RAID array.

Input example:

```
HPT CLI>delete 1
```

```
HPT CLI > query arrays
ID      Secured Capacity(GB)  Type      Status  Block  Sector  Cache      Name
-----
1       No                    1500.08  RAID0   NORMAL  512k   512B      NONE      RAID0_0
HPT CLI : delete 1
Delete array(1) successfully!
```

7.5.2. Delete a Spare Disk

HPT CLI>delete {spare_id}

This command allows you to delete an existing spare disk.

Input example:

```
HPT CLI>delete 1/E1/1
```

```
HPT CLI > query devices
ID      Secured  Capacity  MaxFree  Flag  Status  ModelNumber
-----
1/E1/1  No       1000.12  1000.12  SINGLE SPARE   Samsung SSD 980 PRO 1TB
1/E1/2  No       4096.73  4096.73  SINGLE NORMAL  KXG80ZM84T09 KIOXIA
1/E1/3  No       2000.31  2000.31  SINGLE NORMAL  HP-EM2802T0GMTCB58R-E264
1/E1/4  No       1024.08  1024.08  SINGLE NORMAL  KXG60ZNV1T02 TOSHIBA
1/E1/5  No       2000.31  2000.31  SINGLE NORMAL  CT2000T700SSD3
1/E1/6  No       1000.12  1000.12  SINGLE NORMAL  CT1000T700SSD3
1/E1/7  No       1000.12  1000.12  SINGLE NORMAL  Seagate FireCuda 530 ZP1000GM30013
1/E1/8  No       239.98   239.98   SINGLE NORMAL  WDC WDS240G2G0C-00A2M0
1/E1/9  No       2000.31  2000.31  SINGLE NORMAL  HP-EM2802T0GMTCB58R-E264
1/E1/10 No       2000.31  2000.31  SINGLE NORMAL  HP-EM2802T0GMTCB58R-E264
1/E1/11 No       1000.12  1000.12  SINGLE NORMAL  Sabrent Rocket 4.0 1TB
1/E1/12 No       1000.12  1000.12  SINGLE NORMAL  WD Red SN700 1000GB
1/E1/13 No       2000.31  2000.31  SINGLE NORMAL  HP-EM2802T0GMTCB58R-E26P4
1/E1/14 No       500.03   500.03   SINGLE NORMAL  Samsung SSD 970 EVO Plus 500GB
1/E1/15 No       512.04   512.04   SINGLE NORMAL  Samsung SSD 970 PRO 512GB
1/E1/16 No       2000.31  2000.31  SINGLE NORMAL  HP-EM2802T0GMTCB58R-E264

HPT CLI > delete 1/E1/1
Spare delete '1/E1/1' successfully!

HPT CLI > query devices
ID      Secured  Capacity  MaxFree  Flag  Status  ModelNumber
-----
1/E1/1  No       1000.12  1000.12  SINGLE NORMAL  Samsung SSD 980 PRO 1TB
1/E1/2  No       4096.73  4096.73  SINGLE NORMAL  KXG80ZM84T09 KIOXIA
1/E1/3  No       2000.31  2000.31  SINGLE NORMAL  HP-EM2802T0GMTCB58R-E264
1/E1/4  No       1024.08  1024.08  SINGLE NORMAL  KXG60ZNV1T02 TOSHIBA
1/E1/5  No       2000.31  2000.31  SINGLE NORMAL  CT2000T700SSD3
1/E1/6  No       1000.12  1000.12  SINGLE NORMAL  CT1000T700SSD3
1/E1/7  No       1000.12  1000.12  SINGLE NORMAL  Seagate FireCuda 530 ZP1000GM30013
1/E1/8  No       239.98   239.98   SINGLE NORMAL  WDC WDS240G2G0C-00A2M0
1/E1/9  No       2000.31  2000.31  SINGLE NORMAL  HP-EM2802T0GMTCB58R-E264
1/E1/10 No       2000.31  2000.31  SINGLE NORMAL  HP-EM2802T0GMTCB58R-E264
1/E1/11 No       1000.12  1000.12  SINGLE NORMAL  Sabrent Rocket 4.0 1TB
1/E1/12 No       1000.12  1000.12  SINGLE NORMAL  WD Red SN700 1000GB
1/E1/13 No       2000.31  2000.31  SINGLE NORMAL  HP-EM2802T0GMTCB58R-E26P4
1/E1/14 No       500.03   500.03   SINGLE NORMAL  Samsung SSD 970 EVO Plus 500GB
1/E1/15 No       512.04   512.04   SINGLE NORMAL  Samsung SSD 970 PRO 512GB
1/E1/16 No       2000.31  2000.31  SINGLE NORMAL  HP-EM2802T0GMTCB58R-E264
```

7.6.Rebuild Command

```
HPT CLI > rebuild
Rebuild Commands
  You can use rebuild commands to rebuild a RAID1 RAID5 RAID6,
  when it is critical or broken.
Syntax:
  rebuild {array_id} {device_id}
  rebuild {array_id} {start|stop}
```

You can use rebuild commands to rebuild a RAID array when it is critical or broken.

The following table lists and describes the properties of the rebuild command.

Table 23: Properties for rebuild Command

cmd	Property Name	Value Range	Description
rebuild	{array_id}	The created RAID array	This command allows you to add the specified disk to a critical RAID array and rebuild it.
	{device_id}	The disk hosted by the AIC	
rebuild	{array_id}	The created RAID array	This command lets you start or stop the rebuilding process on the specified array.
	{start stop}	start/ stop	

7.6.1.Rebuild a RAID array

HPT CLI>rebuild {array id} {device id}

This command allows you to add the specified disk to a critical RAID array and rebuild it.

Input example:

HPT CLI>rebuild 1 1/E1/4

```
HPT CLI > query arrays
ID      Secured Capacity(GB)  Type      Status  Block Sector  Cache      Name
-----
1      No      500.03    RAID1    CRITICAL  --  512B  NONE      RAID_1_0

HPT CLI > rebuild 1 1/E1/4

HPT CLI > query arrays 1
ID: 1      Name: RAID_1_0
Type: RAID1      Status: REBUILDING
Capacity(GB): 500.03      BlockSize: --
SectorSize: 512B      CachePolicy: NONE
Progress: 1.30%      Secure: No
ID      Secured Capacity  MaxFree  Flag  Status  ModelNumber
-----
1/E1/4 No      960.13  460.10  NORMAL CRITICAL Samsung SSD 983 DCT 960GB
1/E1/3 No      500.03  0        NORMAL RAID    Samsung SSD 980 PRO 500GB
```

7.6.2. Start Rebuilding the RAID Array

HPT CLI>rebuild {array_id} {start}

This command allows you to start the rebuilding process on the specified array.

Input example:

HPT CLI>rebuild 1 start

```
HPT CLI > rebuild 1 start
Start rebuild array(1) successfully!
```

7.6.3. Stop Rebuilding the RAID Array

HPT CLI>rebuild {array_id} {stop}

This command allows you to stop the rebuilding process on the specified array. After you stop a rebuilding process, you can resume it later with the rebuild start command.

Input example:

HPT CLI>rebuild 1 stop

```
HPT CLI > rebuild 1 stop
Stop rebuild array(1) successfully!
```

7.7. Verify Command

```
HPT CLI > verify
Verify Command
This command starts or stops the verifying process on the specified array.
Syntax:
verify {array_id} {start|stop}
```

You can use the verify command to start or stop the verifying process on the specified array.

The following table lists and describes the properties of the verify command.

Table 24: Properties for verify Command

cmd	Property Name	Value Range	Description
verify	{array_id}	The created RAID array	This command starts or stops the verifying process on the specified array.
	{start stop}	start/ stop	

7.7.1. Start Verifying the RAID Array

HPT CLI>verify {array_id} {start}

This command starts the verification process on the specified array.

Input example:

```
HPT CLI>verify 1 start
```

```
HPT CLI > verify 1 start
Start verify array(1) successfully!

HPT CLI > query arrays
ID      Secured Capacity(GB)  Type  Status  Block  Sector  Cache  Name
-----
1       No                    500.03  RAID1  VERIFYING  --  512B  NONE  RAID_1_0
```

7.7.2. Stop Verifying the RAID Array

HPT CLI>verify {array_id} {stop}

This command stops the verification process on the specified array.

Input example:

```
HPT CLI> verify 1 stop
```

```
HPT CLI > verify 1 stop
Stop verify array(1) successfully!

HPT CLI > query arrays
ID      Secured Capacity(GB)  Type  Status  Block  Sector  Cache  Name
-----
1       No                    500.03  RAID1  NORMAL  --  512B  NONE  RAID_1_0
```


7.8. Rescan Command

```
HPT CLI > rescan
```

When the CLI initiates **Rescan**, the driver will immediately check and see whether the status of any disk has changed. If any changes occur, the disks and RAID array status will be updated to reflect this. When a disk drop triggers the beeper, the beeper can be turned off temporarily by rescan command.

- **Disk Status** – if any disks were added or removed, or if a disk is no longer responding, the status will change.
- **RAID status** – the RAID array’s status may change depending on the status of the disks.

The following table lists and describes the properties of the rescan command.

Table 25: Properties for rescan Command

cmd	Property Name	Description
rescan	N/A	This command rescans all of the physical devices attached to the AIC.

7.8.1. Rescan the Physical Devices

HPT CLI>rescan

This command rescans all of the physical devices attached to the AIC.

Input example:

```
HPT CLI> rescan
```

```
HPT CLI > rescan
Rescan successfully.
```

7.9.Lscard Command

```
lscard Command
    This command show your card(s).
syntax:
    lscard
```

The lscard command is used to list multiple AICs.

The following table lists and describes the properties of the lscard command.

Table 26: Properties for lscard Command

cmd	Property Name	Description
lscard	N/A	<p>This command displays the list of multiple AICs.</p> <p>Active: Indicates the AIC you are using.</p> <p>Inactive: Indicates another AIC connected to the system but not in use.</p>

7.9.1.Lscard all AICs

HPT CLI>lscard

This command displays the list of multiple AICs.

Input example:

HPT CLI>lscard

```
HPT CLI > lscard
CARD_ID      NAME                                ACTIVED
-----
0             Controller(1): HighPoint           Active
1             Controller(2): RR3720              Inactive
```

7.10. Events Command

```

Events Commands
The CLI system will auto record three types of events: Information
(shortened to 'Inf'), Warning (shortened to 'War'), and Error
(shortened to 'Err') on the screen output. These commands allow you to
query, save the logged events.
Syntax:
events
events save {file_name}

```

The CLI system will automatically record three types of events on the screen output. Events commands allow you to view and save the logged events.

The following table lists and describes the properties of the events command.

Table 27: Properties for events Command

cmd	Property Name	Value Range	Description
events	N/A	N/A	This command will display the events log for the selected page number, displaying 20 log messages per page. Event Level: <ul style="list-style-type: none"> - Inf (Information) - War (Warning) - Err (Error)
events	save	N/A	This command will save all the logged events as a plain text file.
	{file_name}	File path	

7.10.1. View the Event Log

HPT CLI>events

This command will display a list of all the logged events.

Input example:

HPT CLI>events

```

HPT CLI > events
1 Inf [07/10/2024 05:18:03] Plugging device detected.('Sabrent Rocket 4.0 1TB-03F10707074404014589' at Controller
1-Enclosure1-Device5)
2 Inf [07/10/2024 05:18:03] Plugging device detected.('KXG60ZNV1T02 TOSHIBA-694S10NBTVDO' at Controller1-Enclosur
e1-Device6)
3 Inf [07/10/2024 05:08:56] RAID 1 Array 'RAID_1_0' has been created successfully (Disk 1: Micron_7400_MTFDKCB7T6T
DZ, 1/E1/5; Disk 2: Micron_7450_MTFDKCC7T6TFR, 1/E1/6).
4 Inf [07/10/2024 05:08:41] Array 'RAID_0_0' has been deleted successfully.
5 Inf [07/10/2024 05:08:26] RAID 0 Array 'RAID_0_0' has been created successfully (Disk 1: Micron_7400_MTFDKCB7T6T
DZ, 1/E1/5; Disk 2: Micron_7450_MTFDKCC7T6TFR, 1/E1/6; Disk 3: INTEL_SSDPF2X076TZO, 1/E1/7; Disk 4: INTEL_SSDPF2X08TZO, 1/E1/
8).
6 Inf [07/10/2024 05:08:25] Device 'Device_1_E1_8' (1/E1/8) has been initialized.

```

7.10.2. Save the Event Log

HPT CLI>events save {file_name}

This command will save all the logged events as a plain text file.

Input example:

HPT CLI> events save C:/raidlog.txt

```
HPT CLI > events save C:/raidlog.txt
The event log C:/raidlog.txt has been saved.
```

7.11. Mail Command

```

HPT CLI > mail
Mail Commands
Set a mail recipient to get the e-mail from system.
syntax:
mail recipient
mail recipient add {recipient_name} {mail_address} [Inf|War|Err]
mail recipient delete {recipient_name}
mail recipient test {recipient_name}
mail server
mail server set {server_address} {port} {ssl} {e|d} {from_address} [username] [password]
mail server set {a|p|s|m|u|t} {value}

```

The mail command instructs the AIC to email your chosen recipients when certain events trigger.

The following table lists and describes the properties of the mail command.

Table 28: Properties for mail Commands

cmd	Property Name	Value Range	Description
mail	recipient	N/A	Use this command to list all of the mail recipients.
mail	add	{options}	Use this command to add a new recipient.
mail	test	{options}	Use this command to send a test email to a specified recipient.
mail	delete	{options}	Use this command to delete an existing recipient.
	{options}	{recipient_name}	The name of the recipient.
		{mail_address}	The email address of the recipient.
		[Inf War Err]	The type(s) of events will trigger an email in the respective Event Level. <ul style="list-style-type: none"> - Inf (Information) - War (Warning) - Err (Error)
mail	server	N/A	Use this command to display the SMTP server information.
mail	set	{options}	Use this command to configure mail server settings.
	options	{server_address}	The SMTP server address.
		{port}	The SMTP port is generally 25.
		{ssl}	1 for enable and port needs 465, 0 for disabled.
		{e d}	Enable Event Notification status, e for enabled or d for disabled.
		{from_address}	The mail from address.
		[username]	The mail username.

	[password]	The mail password.
	{a p m u t} {value}	Use this command to set your mail server value. <ul style="list-style-type: none"> - a - The SMTP server address. - p - The SMTP port is generally 25. - s - Enable Event Notification status, e for enabled or disabled. - m - The mail from the address. - u - The mail username. - t - The mail password. - value - Setting parameters.

7.11.1. Add a Mail Recipient

HPT CLI>recipient add {recipient_name} {mail_address} [Inf|War|Err]

This command will add a new recipient.

Input example:

HPT CLI> mail recipient add hpt admin@highpoint-tech.com Inf

```
HPT CLI > mail recipient add hpt [REDACTED]point.com Inf
HPT CLI > mail recipient
ID  Name      Mail Address      Notify Types
-----
1   hpt      [REDACTED]point.com  Information
```

7.11.2. List all Mail Recipients

HPT CLI>mail recipient

This command will display a list of all mail recipients.

Input example:

HPT CLI>mail recipient

```
HPT CLI > mail recipient
ID  Name      Mail Address      Notify Types
-----
1   hpt      [REDACTED]hpoint.com  Information
```

7.11.3. Test the mail recipient

HPT CLI>mail recipient test {recipient_name}

This command will send a test email to a specified recipient.

Input example:

```
HPT CLI> mail recipient test hpt
```

```
HPT CLI > mail recipient test hpt
```

7.11.4. Delete a Mail Recipient

HPT CLI>mail recipient delete {recipient_name}

This command will delete an existing mail recipient.

Input example:

```
HPT CLI> mail recipient delete hpt
```

```
HPT CLI > mail recipient
ID  Name      Mail Address      Notify Types
-----
1   hpt       yf@highpoint.com  Information
HPT CLI > mail recipient delete hpt
HPT CLI > mail recipient
ID  Name      Mail Address      Notify Types
-----
```

7.11.5. Add a Mail Server

HPT CLI>mail server set {server address}{port} {ssl} {e|d} {from address} [username] [password]

This command will configure mail server settings.

Input example:

HPT CLI> mail server set smtp.gmail.com 465 1 e name@somecompany.com name@somecompany.com password

```
HPT CLI > mail server set smtp.gmail.com 465 1 e [redacted]@gmail.com [redacted]@gmail.com lui:[redacted]
```

Note: Gmail requires dual authentication and logging in with the app-specific password. Please refer to [step 7](#) to get the app-specific password.

7.11.6. List all Mail Servers

HPT CLI>mail recipient delete {recipient name}

This command will configure mail server settings.

Input example:

HPT CLI> mail server

```
HPT CLI > mail server
ServerAddress      Port  ssl  Status  Mail From      User Name
-----
smtp.gmail.com    465  1    Enabled [redacted]@gmail.com [redacted]@gmail.com
```

7.11.7. Set the Mail Server

HPT CLI>mail server set {a|p|m|u|t} {value}

This command will separate and set your mail server value.

Input example:

HPT CLI> mail server set p 15

```
HPT CLI > mail server set p 15
HPT CLI > mail server
ServerAddress      Port  ssl  Status  Mail From      User Name
-----
smtp.gmail.com    15   1    Enabled [redacted]@gmail.com [redacted]@gmail.com
```


7.12. Task Command

```

Task Commands
  Set tasks for the server.
Syntax:
task
task {rebuild|verify} {array_id} {name=} {once|daily|monthly|weekly}={day}
{interval}={interval} start=mm/dd/yyyy end=mm/dd/yyyy time=hh:mm:ss
task delete {task_id}

```

When an array requires regular verification or rebuilding, you can use the task commands to automate this process in the background. You can add new tasks and modify or delete existing tasks.

The following table lists and describes the properties of the task command.

Table 29: Properties for task Commands

cmd	Property Name	Value Range	Description
task	N/A	N/A	This command displays detailed information about all scheduled tasks.
task	rebuild	{options}	This command allows you to schedule a specified array. <i>Note: When you add a task to rebuild a selected array once, the parameter {day} should be omitted.</i>
task	verify	{options}	This command allows you to schedule a verification task.
	{options}	{array_id}	The created RAID array.
		{once daily monthly weekly}={day}	Schedule the frequency as once, daily, weekly, or monthly.
		interval={interval}	Intervals between task executions.
		start=mm/dd/yyyy time=hh:mm:ss	The task start date. - yyyy - year - dd - day - mm - month - hh - hour - mm - minute - ss - second
		end=mm/dd/yyyy time=hh:mm:ss	The task end date.

task	delete {task_id}	The created task	This command allows you to delete a scheduled task.
-------------	------------------	------------------	---

7.12.1. Create a New Rebuild Task

HPT CLI>task rebuild {array_id} {name=} {once|daily|weekly|monthly}={day} interval={interval} start=mm/dd/yyyy end=mm/dd/yyyy time=hh:mm:ss

This command allows you to schedule the frequency as once, daily, weekly, or monthly, and the detailed time range to rebuild a specified array. The first mm/dd/yyyy specifies the task start date, while the second mm/dd/yyyy specifies the task end date.

Input example:

```
HPT CLI>task rebuild 1 name=test daily=1 start=5/25/2024 end=5/31/2024
```

```
HPT CLI > task rebuild 1 name=test daily=1 start=5/25/2024 end=5/31/2024
Add task(test) successfully!
```

7.12.2. Create a New Verify Task

HPT CLI>task verify {array_id} {name=} {once|daily|weekly|monthly}={day} interval={interval} start=mm/dd/yyyy end=mm/dd/yyyy time=hh:mm:ss

This command allows you to schedule a verification task. The usage of this command is the same as adding a rebuild task schedule.

Input example:

```
HPT CLI>task verify 1 name=test daily=1 start=6/1/2024 end=6/30/2024
```

```
HPT CLI > task verify 1 name=test daily=1 start=6/1/2024 end=6/30/2024
Add task(test) successfully!
```

Note: Verify Task can only be created if the RAID1 array is in a normal status.

7.12.3. List all Tasks

HPT CLI>task

This command displays detailed information about all scheduled tasks.

Input example:

```
HPT CLI>task
```

```
HPT CLI > task
ID   Name      Start-Date  End-Date    S-F    Description
----
test 05/25/2024 05/31/2024  E-D    Rebuild raid RAID_1_0 (created by )
test 06/01/2024 06/30/2024  E-D    Verify raid RAID_1_0 (created by )
```

7.12.4.Delete a Task

HPT CLI>task delete {task_id}

This command allows you to delete a scheduled task.

Input example:

HPT CLI>task delete 2

```
HPT CLI > task
ID Name Start-Date End-Date S-F Description
-----
1 test 05/25/2024 05/31/2024 E-D Rebuild raid RAID_1_0 (created by )
2 test 06/01/2024 06/30/2024 E-D Verify raid RAID_1_0 (created by )
HPT CLI task delete 2
Delete task(test) successfully!
HPT CLI > task
ID Name Start-Date End-Date S-F Description
-----
1 test 05/25/2024 05/31/2024 E-D Rebuild raid RAID_1_0 (created by )
```

7.13. Set Command

```

set Command
  Set the system, device or array's param.
Syntax:
set
  show the system parameters
set {name=}
  set AR=[y|n]           Auto Rebuild
  set CE=[y|n]           Continue Rebuild On Error
  set AA=[y|n]           Audible Alarm
  set SS=[y|n]           Staggered spinup
  set DS=[seconds]      Delay between spinup (seconds)
  set ND=[number]       Number of drives per spinup
  set IT=[y|n]          INT 13 support
  set SB=[y|n]          Single BCV entry
  set NC=[y|n]          NCQ
  set BP=[y|n]          Beeper
  set FS=[Auto|Off|Low|Medium|High] Enclosure Fan Speed
  set RP=[1-100]        Rebuild Priority
  set BR=[1-100]        Background Rate
  set SD=[minutes]     Spindown Idle Disk (minutes)
  set TT=[20-100]      Temperature threshold
  set TU=[C|F]         Temperature Unit
  set CL=[y|n]         Collect system logs
  set PS               Set Password
set {device id} {name=}
  set tcq=[y|n]        set TCQ enable or disable.
  set ncq=[y|n]        set NCQ enable or disable.
  set wc=[y|n]        set Write Cache enable or disable.
  set ra=[y|n]        set Read Ahead enable or disable.
  set smart=[y|n]     set smart enable or disable.
set {array id} name={name} cp=[wt|wb|none]
  name               Set the array's name.
  cp                 Set array's cache policy.


```

You can change the CLI settings by setting commands according to your preferred behavior and requirements.

The following table lists and describes the properties of the set command.

Table 30: Properties for set Commands

cmd	Property Name	Description
set	AR	Set enable or disable to the [Auto Rebuild] parameter. When a disk fails, the NVMe RAID AIC will take the disk offline. The NVMe RAID AIC will automatically rebuild the array after you have configured spare disks or replaced the disk, but only if the Enable auto rebuild option is enabled.
	CE	Set enable or disable to the [Continue Rebuilding On Error] parameter. When enabled, the rebuilding process will ignore bad disk sectors and continue rebuilding until completion. When the rebuild is finished, the data may be accessible but inconsistent due to any bad sectors that were ignored during the procedure. HighPoint recommends checking the event log periodically for bad sector warnings if this option is enabled.
	AA	Set enable or disable to the [Audible Alarm] parameter.

		<p>The audible alarm sounds when the following conditions occur:</p> <ul style="list-style-type: none"> - Disk Dropped - Fan Speed lower than 600 RPM - SSD Temperature is higher than the SSD warning threshold - Broadcom Chipset Temperature is higher than 105°C <p> Warning: Disabled audible alarm is permanently disabling the beeper, so please proceed with caution!</p>
	BP	<p>Set enable or disable [Beeper].</p> <p>When a disk drop triggers the beeper.</p>
	RP	<p>Change [Rebuilding Priority]. If an AIC is not specified, this command will set the global rebuilding priority.</p> <p>[0-12] Lowest</p> <p>[13-37] Low</p> <p>[38-67] Medium</p> <p>[68-87] High</p> <p>[>88] Highest</p>
	RL	<p>(default: Enabled)</p> <p>Remote access to the AIC will be restricted when enabled; other users in your network cannot log in to the WebGUI remotely.</p> <p>It is used as follows:</p> <ol style="list-style-type: none"> 1. Set Restrict to localhost access to n. 2. Turn off the local firewall. 3. View the local IP address. 4. Use another system to access WebGUI remotely by typing http://IP address:port number in the browser.
	TT	<p>Set the disks's temperature threshold.</p> <p>Notes:</p> <p>This setting is not supported by the Linux HighPoint RAID Management.</p> <p>149° F is the default. This setting can correspond with the disk manufacturer's official specifications.</p>

TU	<p>Set the [Temperature Unit] to Celsius or Fahrenheit.</p> <p>This setting is only supported by the Windows HighPoint RAID Management.</p>
CL	<p>Set enable or disable [Collecting System Logs].</p> <p>You can set it to enable the collection of system logs at any time. The collected system logs are stored on C:/Windows/hpt_diagdriver. The maximum size of the collected system log is 840MB; anything over 840MB will be overwritten forward.</p> <p>This setting is only supported by the Windows HighPoint RAID Management.</p> <p>It is used as follows:</p> <ol style="list-style-type: none"> 1. Set CL to Enabled. 2. Reboot the system. 3. Duplicate the problems encountered. 4. Collect system logs with one click.
PS	Set or change your [Password] . The password is ≤ 8 characters.
FS	<p>Change the AIC Fan Speed. This supports setting different levels of fan speed {Auto Off Low Medium High Full}</p> <p>This setting is only supported by the Windows HighPoint RAID Management.</p>

7.13.1. Set Auto Rebuild

HPT CLI>set AR=[y|n]

Set enable or disable to the **[Auto Rebuild]** parameter.

Input example:

HPT CLI>set AR=y

```
HPT CLI > set AR=y
Set param successfully!
```

7.13.2. Set Continue Rebuilding On Error

HPT CLI>set CE=[y|n]

Set enable or disable to the [Continue Rebuilding On Error] parameter.

Input example:

HPT CLI>set CE=y

```
HPT CLI > set CE=y
Set param successfully!
```

7.13.3. Set Audible Alarm

HPT CLI>set AA=[y|n]

Set enable or disable to the [Audible Alarm] parameter.

Input example:

HPT CLI>set AA=n

```
HPT CLI > set AA=n
Set param successfully!
```

7.13.4. Set Rebuild Priority

HPT CLI>set RP=[0-100]

Change rebuilding priority.

Input example:

HPT CLI>set RP=60

```
HPT CLI > set RP=60
Set param successfully!
```

7.13.5. Set Restrict to localhost access

HPT CLI>set RL= [v|n]

Set enable or disable restrict localhost access.

Input example:

HPT CLI>set RL=y

```
HPT CLI>set RL=y
Set param successfully!
```

7.13.6. Set Temperature Threshold

To set the disks's **temperature threshold**.

Input example:

HPT CLI>set BP=n

```
HPT CLI > set BP=n
Set param successfully!
```

Notes:

This setting is not supported by the Linux HighPoint RAID Management.

149°F is the default. This setting can correspond with the disk manufacturer's official specifications.

7.13.7. Set Temperature Unit

HPT CLI>set TU=[C|F]

Set the temperature unit to Celsius or Fahrenheit.

Input example:

HPT CLI>set TU=C

```
HPT CLI > set TU=C
Set param successfully!
```


7.13.8. Set Collecting System Logs

HPT CLI>set CL=[y|n]

Set enable or disable to the [Collecting System Logs] parameter.

Input example:

HPT CLI>set CL=y

```
HPT CLI > set CL=y
Set param successfully!
```

7.13.9. Set Password

HPT CLI>set PS={password}

You can set or change your HighPoint RAID Management password. The password length is less than or equal to 8 bits, and there is no limit to the valid complexity of the password.

Input example:

HPT CLI>set PS=00000000

```
HPT CLI > set PS=00000000
Password :*****
Confirm  :*****
Password has been changed, please login with your new password.
HighPoint Windows CLI, Please Input
Password:
```

7.13.10. Set AIC Fan Speed

HPT CLI>set {enclosure_id} FS=[Auto|Off|Low|Medium| High|Full]

Change the AIC Fan Speed.

Input example:

HPT CLI>set 1/E1 FS=Low

```
HPT CLI > set 1/E1 FS=Low
Set param successfully!
```

7.14. Unplug Command

```

Unplug Command
  This command allows you to unplug an existing RAID array or device.
  After you have unplugged the array or device, you can hot plug it.
  Also by running the rescan command you can found it back.
  Please refering the rescan command help.
Syntax:
  unplug {array_or_device_ID}

```

To ensure data security, if you want to unplug an existing RAID array or disks while the system works, use the unplug command first and then unplug the disks.

The following table lists and describes the properties of the unplug command.

Table 31: Properties for unplug Commands

cmd	Property Name	Value Range	Description
unplug	{device_id}	The disk hosted by the AIC	This command allows you to unplug the disk.
unplug	{array_id}	The created RAID array	This command allows you to unplug the array.

7.14.1. Unplug the Physical Device

HPT CLI>unplug {device_id}

This command allows you to unplug the disk. After the command, manually remove the disk.

Input example:

```
HPT CLI>unplug 1/E1/6
```

```

HPT CLI > query devices
ID      Secured  Capacity  MaxFree  Flag  Status  ModelNumber
-----
1/E1/5  No        500.03   0        RAID  NORMAL  Samsung SSD 980 PRO 500GB
1/E1/6  No        7681.50  0        SINGLE LEGACY  Micron 7450 MTFDKCC7T6TFR
1/E1/8  No        3840.64  3340.61  RAID  NORMAL  Micron_9300_MTFDHAL3T8TDP
-----
HPT CLI > unplug 1/E1/6
Unplug device(1/E1/6) successfully!

HPT CLI > query devices
ID      Secured  Capacity  MaxFree  Flag  Status  ModelNumber
-----
1/E1/5  No        500.03   0        RAID  NORMAL  Samsung SSD 980 PRO 500GB
1/E1/8  No        3840.64  3340.61  RAID  NORMAL  Micron_9300_MTFDHAL3T8TDP
-----

```

7.14.2. Unplug a RAID Array

HPT CLI>unplug {array_id}

This command allows you to unplug the array. After the command, manually remove the member disks.

Input example:

```
HPT CLI>unplug 1
```

```
HPT CLI > query arrays
ID      Secured Capacity(GB)  Type      Status  Block  Sector  Cache      Name
-----
1       No          500.03    RAID1    NORMAL  --     512B     NONE      RAID_1_0

HPT CLI > unplug 1
Unplug array(1) successfully!

HPT CLI > query arrays
ID      Secured Capacity(GB)  Type      Status  Block  Sector  Cache      Name
-----
```

7.15. Secure Command

```

secure Command
  This command is used to set device security.
syntax:
  secure {enclosure id} enable key={password}  Enable device security on the enclosure.
  secure {enclosure id} disable                Disable device security on the enclosure.
  secure {enclosure id} change oldkey={old password} key={new password}  Change all devices' security key on the enclosure.
  secure {device id} legacy                    Secure legacy device.
  secure {device id} changekey key={old password}  Change the device's security key to be consistent with all other devices' key on the enclosure.
  secure {device id} secureerase {force}       Erase the device's security configuration and securely erases data.
HPT CLI >

```

This Secure commands supports enable, disable and change AIC/ disks security key.

The following table lists and describes the properties of the secure command.

Table 32: Properties for secure Commands

cmd	Property Name	Value Range	Description
secure	{enclosure_id}	The AIC in use	This command allows you to enable AIC security.
	enable	N/A	
	key	{password}	
secure	disable	N/A	This command allows you to disable AIC security.
secure	change	N/A	This command allows you to change the AIC security key.
	oldkey	{old password}	
	key	{new password}	
secure	{device_id}	The disk hosted by the AIC	This command allows you to enable legacy disk security.
	legacy	The disk is in the legacy	
secure	changekey	N/A	The command changes the disk security key to be consistent with the AIC security key.
	key	{old password}	
secure	secureerase	{force}	This command allows you to disable disk security.

7.15.1.Enable AIC Security

HPT CLI>secure {enclosure_id} enable key={password}

This command allows you to enable AIC security. The password length is 8-32 digits, and there is no limit to the valid complexity of the password.

Input example:

```
HPT CLI>secure 1/E1 enable key=00000000
```

```
HPT CLI > query enclosures
ID   Secure  VendorID      ProductID      NumberOfPYH
-----
1/E1 No       HPT           R7628A NVMe RAID Adapter  8

HPT CLI > secure 1/E1 enable key=00000000
Enable security successfully.

HPT CLI > query enclosures
ID   Secure  VendorID      ProductID      NumberOfPYH
-----
1/E1 Yes       HPT           R7628A NVMe RAID Adapter  8
```

7.15.2.Change AIC Security key

HPT CLI>secure {enclosure_id} change oldkey={old password} key={new password}

This command allows you to change the AIC security key. The password length is 8-32 digits, and there is no limit to the valid complexity of the password.

Input example:

```
HPT CLI>secure 1/E1 change oldkey={00000000} key={11111111}
```

```
HPT CLI > secure 1/E1 change oldkey=00000000 key=11111111
Change security successfully.
```

7.15.3. Disable AIC Security

HPT CLI>secure {enclosure_id} disable

This command allows you to disable AIC security.

Input example:

```
HPT CLI>secure 1/E1 disable
```

```
HPT CLI > query enclosures
ID   Secure  VendorID  ProductID  NumberOfPYH
-----
1/E1 Yes      HPT       R7628A NVMe RAID Adapter  8

HPT CLI > secure 1/E1 disable
Disable security successfully.

HPT CLI > query enclosures
ID   Secure  VendorID  ProductID  NumberOfPYH
-----
1/E1 No      HPT       R7628A NVMe RAID Adapter  8
```

7.15.4. Enable Disk Security

HPT CLI>secure {device_id} legacy

This command allows you to enable disk security.

Input example:

```
HPT CLI>secure 1/E1/5 legacy
```

```
HPT CLI > query devices
ID   Secured  Capacity  MaxFree  Flag  Status  ModelNumber
-----
1/E1/5 No       500.11    0        SINGLE LEGACY  Samsung SSD 980 PRO 500GB
1/E1/6 No       7681.50   0        SINGLE LEGACY  Micron_7450_MTFDKCC7T6TFR
1/E1/8 No       3840.76   0        SINGLE LEGACY  Micron_9300_MTFDHAL3T8TDP

HPT CLI > secure 1/E1/5 legacy
Secure legacy device(1/E1/5) successfully

HPT CLI > query devices
ID   Secured  Capacity  MaxFree  Flag  Status  ModelNumber
-----
1/E1/5 Yes       500.11    0        SINGLE LEGACY  Samsung SSD 980 PRO 500GB
1/E1/6 No       7681.50   0        SINGLE LEGACY  Micron_7450_MTFDKCC7T6TFR
1/E1/8 No       3840.76   0        SINGLE LEGACY  Micron_9300_MTFDHAL3T8TDP
```

7.15.5. Change Disk Security key

HPT CLI>secure {devices id} changekey key={old password}

This command allows you to change the AIC security key.

Input example:

```
HPT CLI>secure 1/E1/5 changekey key=00000000
```

```
HPT CLI > query devices
ID      Secured  Capacity  MaxFree  Flag  Status  ModelNumber
-----
1/E1/5  Yes(locked) 500.11    0        SINGLE NORMAL  Samsung SSD 980 PRO 500GB
1/E1/6  No         7681.50   0        SINGLE LEGACY  Micron_7450_MTFDKCC7T6TFR
1/E1/8  No         3840.76   0        SINGLE LEGACY  Micron_9300_MTFDHAL3T8TDP
-----
HPT CLI > secure 1/E1/5 changekey key=00000000
Change key successfully.Please restart to take effect.
```

Note: There is a limit to the number of times you can change the disk key. If you do not enter the correct disk key **five times**, this function will be locked, and you will need to power cycle your system to change the disk key again.

7.15.6. Disable Disk Security

HPT CLI>secure {device id} secureerase {force}

This command allows you to disable disk security.

Input example:

```
HPT CLI>secure 1/E1/5 secureerase force
```

```
HPT CLI > query devices
ID      Secured  Capacity  MaxFree  Flag  Status  ModelNumber
-----
1/E1/5  Yes      500.03    500.03   SINGLE NORMAL  Samsung SSD 980 PRO 500GB
1/E1/6  No       7681.50   0        SINGLE LEGACY  Micron_7450_MTFDKCC7T6TFR
1/E1/8  No       3840.76   0        SINGLE LEGACY  Micron_9300_MTFDHAL3T8TDP
-----
HPT CLI > secure 1/E1/5 secureerase force
secureerase device(1/E1/5) successfully.
HPT CLI > query devices
ID      Secured  Capacity  MaxFree  Flag  Status  ModelNumber
-----
1/E1/5  No       500.03    500.03   SINGLE NORMAL  Samsung SSD 980 PRO 500GB
1/E1/6  No       7681.50   0        SINGLE LEGACY  Micron_7450_MTFDKCC7T6TFR
1/E1/8  No       3840.76   0        SINGLE LEGACY  Micron_9300_MTFDHAL3T8TDP
-----
```

7.16. Diag Command

Diagnostic Command
 This command is used to diagnose and save HighPoint driver and controller information.
Syntax:
 If you have any questions, please send the compressed package saved by this command to support.

This command allows you to collect the diagnostic information.

The following table lists and describes the properties of the diag command.

Table 33: Properties for diag Command

cmd	Property Name	Description
diag	N/A	This command allows you to collect the diagnostic information. The saving path will be displayed after entering this command.

7.16.1. Collect the Diagnostic Information

HPT CLI>diag

This command allows you to collect the diagnostic information.

Input example:

HPT CLI>diag

- **For Windows User**

```
HPT CLI > diag
The diagnostic information will be saved in C:\Program Files\HighPoint Technologies, Inc\HighPoint RAID Management\Service\ce\webguiroot\HighPoint_hptnvme_1.4.0.0_2024.05.23_23.59.zip.It may take a few minutes to be ready.
```

- **For Linux User**

```
HPT CLI>diag
The diagnostic information has been saved in /usr/share/hpt/HighPoint_hptnvme_v1.8.0.0_2024.06.04.tar.gz
```


7.17. Switch Command

```
Switth Command
  This command allows you switch card.
Syntax:
  switch {card_id}
```

When you use the R7000 series AICs with other series AICs, you can switch the AICs you want to use with this command.

The following table lists and describes the properties of the switch command.

Table 33: Properties for switch Command

cmd	Property Name	Value Range	Description
switch	{card_id}	AICs connected to the system	This command allows you to switch the use of the AIC.

7.17.1. Switch the AIC

HPT CLI>switch {card_id}

This command allows you to switch the use of the AIC.

Input example:

HPT CLI>switch 1

```
HPT CLI > lscard
CARD_ID      NAME                               ACTIVED
-----
0             Controller(1): HighPoint           Active
1             Controller(2): RR3720              Inactive
HPT CLI > switch 1

HPT CLI > lscard
CARD_ID      NAME                               ACTIVED
-----
0             Controller(1): HighPoint           Inactive
1             Controller(2): RR3720              Active
```

7.18. Update Command

```
HPT CLI > update
Update Command
  This command is used to update Firmware by the specified file.
  This process may take some time.
Syntax:
  update {controller_id | enclosure_id} fw={file_path}. Select the blf file to update Firmware.
```

You can upgrade to a newer version of firmware here. This help update the firmware version and the UEFI HII Utility version. The process may take some time.

The following table lists and describes the properties of the update command.

Table 34: Properties for update Command

cmd	Property Name	Value Range	Description
update	{enclosure_id}	The AIC in use	This command allows you to select the blf file to update AIC firmware.
	fw=	{file_path}	

7.18.1. Update the Firmware

HPT CLI>update {controller_id enclosure_id} fw={file path}

This command allows you to select the blf file to update the AIC firmware.

Input example:

```
HPT CLI>update 1/E1 fw=C:\Users\test\Desktop\SSDxxxx_HLK_v5.12.4.1_v2.4.1.2_2024_05_08.blf
```

```
HPT CLI > update 1/E1 fw=C:\Users\test\Desktop\SSDxxxx_HLK_v5.12.4.1_v2.4.1.2_2024_05_08.blf
```

7.19. Help Command

```
HPT CLI > help
help [query|create|delete|OCE/ORLM|rebuild|verify|unplug|switch|lscard
rescan|init|events|mail|task|set|clear|help|exit|diag|secure]
```

If you input an unknown or error command, you will be told that the command is unknown; you can use help commands to find the correct commands.

```
HPT CLI > HELP
ERROR: Unknown command HELP .
You can input 'help' for more commands.
```

The following table lists and describes the properties of the help command.

Table 35: Properties for help Commands

cmd	Property Name	Description
help	N/A	This command shows generic help about this utility.
help	{command}	This command shows help about a specific command.

7.19.1. Show the Generic Help Command

HPT CLI>help

This command shows generic help about this utility.

Input example:

```
HPT CLI>help
```

```
HPT CLI > help
help [query|create|delete|OCE/ORLM|rebuild|verify|unplug|switch|lscard
rescan|init|events|mail|task|set|clear|help|exit|diag|secure]
```

7.19.2. Show the Specific Command Help

HPT CLI>help {command}

Show help about a specific command.

Input example:

```
HPT CLI>help delete
```

```
HPT CLI > help delete
Delete Command
  This command allows you to delete an existing RAID array or remove
  a spare disk. After deletion, the original array and all data on it
  will be lost. All the member disks will be listed as available single disks.
Syntax:
  delete {array id | spare id}
```

7.20. Ver Command

```
HPT CLI>ver
```

Shows the version of RAID Management currently in use.

7.20.1.Show the RAID Management Version

HPT CLI>ver

This command shows you the version of RAID Management currently in use.

Input example:

```
HPT CLI>ver
```

```
HPT CLI>ver  
hptsvr: v3.2.0
```

7.21. Exit Command

```
HPT CLI > exit
```

Exit from the interactive mode and close the window.

7.21.1.Exit the CLI

HPT CLI>exit

This command lets you exit the interactive mode and close the window.

Input example:

```
HPT CLI>exit
```

7.22. Clear Command

```
HPT CLI > clear
```

This command is used to clear the screen.

7.22.1. Clear the CLI screen

HPT CLI>clear

This command allows you to clear the screen.

Input example:

```
HPT CLI>clear
```

8. Trouble shooting

8.1. Fail to compile gcc, make and other driver files

8.1.1. For Debian

1. Description of the Problem

When installing the driver, due to various factors, driver files such as **gcc** and **make** cannot be compiled, thus interrupting the driver installation process:

```
root@debian:/home/test/Documents# ./hptnvme_g5_linux_src_v1.4.4_2022_06_13.bin
Verifying archive integrity... All good.
Uncompressing HighPoint NVMe RAID Controller Linux Open Source package installer.....
Checking and installing required toolchain and utility ...
Installing program make ... (failed)
Installing program gcc ... (failed)
Found program perl (/usr/bin/perl)
Found program wget (/usr/bin/wget)
old pcie_ahci=off iommu=off intel_iommu=off amd_iommu=off
new pcie_ahci=off iommu=off intel_iommu=off amd_iommu=off
Synchronizing state of hptdrv-monitor.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable hptdrv-monitor
update-rc.d: warning: enable action will have no effect on runlevel 1
Toolchain to build the driver is incomplete, please install the missing package to build the driver.
Exit.
```

2. Cause of the Problem

The system is not connected to a network (internet connection).

3. Solution

- a. Ensure that the network is properly connected.
- b. Reinstall the HighPoint software.

If the following occurs after the network connection and reinstall driver:

```
Verifying archive integrity... All good.
Uncompressing HighPoint NVMe G5 RAID Linux Software package installer.....
Verifying archive integrity... All good.
Uncompressing HighPoint NVMe RAID Controller Linux Open Source package installer.....
Checking and installing required toolchain and utility ...
Installing program gcc ...
Media change: please insert the disc labeled
'Debian GNU/Linux 12.5.0_Bookworm_ - Official amd64 DVD Binary-1 with firmware 20240210-11:28'
in the drive '/media/cdrom/' and press [Enter]
```

This problem can be caused by a lack of dependency packages:

Solution:

- a. To install using the CD-ROM: insert the CD-ROM back and press **Enter**.
- b. To install using the USB flash drive:
 - a) The system needs to be resourced. For details, please refer to the official website file:

<https://www.debian.org/doc/manuals/debian-faq/uptodate.en.html>
 - b) Open the system terminal with root privileges.
 - c) Enter the following command:

```
#nano /etc/apt/sources.list
```


- d) Replace the contents of the file with the following.

```
deb https://mirrors.tuna.tsinghua.edu.cn/debian/ bookworm main contrib non-free non-
free-firmware
# deb-src https://mirrors.tuna.tsinghua.edu.cn/debian/ bookworm main contrib non-free
non-free-firmware
deb https://mirrors.tuna.tsinghua.edu.cn/debian/ bookworm-updates main contrib non-free
non-free-firmware
# deb-src https://mirrors.tuna.tsinghua.edu.cn/debian/ bookworm-updates main contrib
non-free non-free-firmware
deb https://mirrors.tuna.tsinghua.edu.cn/debian/ bookworm-backports main contrib non-free
non-free-firmware
# deb-src https://mirrors.tuna.tsinghua.edu.cn/debian/ bookworm-backports main contrib
non-free non-free-firmware
```

Note: See the mirror list at <https://www.debian.org/mirror/list> for more information.

- c. Enter the following command: **#apt-get update**

```
root@test:/home/test/Documents# nano /etc/apt/sources.list
root@test:/home/test/Documents# apt-get update
Get:1 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye InRelease [116 kB]
Get:2 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye-updates InRelease [44.1 kB]
Get:3 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye-backports InRelease [49.0 kB]
Get:4 https://mirrors.tuna.tsinghua.edu.cn/debian-security bullseye-security InRelease [48.4 kB]
Get:5 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye/non-free Sources [81.2 kB]
Get:6 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye/main Sources [8,633 kB]
Get:7 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye/contrib Sources [43.2 kB]
Get:8 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye/main amd64 Packages [8,184 kB]
Get:9 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye/main Translation-en [6,239 kB]
Get:10 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye/main amd64 DEP-11 Metadata [4,049 kB]
Get:11 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye/main DEP-11 48x48 Icons [3,478 kB]
Get:12 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye/main DEP-11 64x64 Icons [7,315 kB]
Get:13 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye/contrib amd64 Packages [50.6 kB]
Get:14 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye/contrib Translation-en [46.9 kB]
Get:15 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye/contrib amd64 DEP-11 Metadata [13.6 kB]
Get:16 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye/contrib DEP-11 48x48 Icons [47.2 kB]
Get:17 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye/contrib DEP-11 64x64 Icons [93.3 kB]
Get:18 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye/non-free amd64 Packages [97.7 kB]
Get:19 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye/non-free Translation-en [92.4 kB]
Get:20 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye/non-free amd64 DEP-11 Metadata [17.9 kB]
Get:21 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye/non-free DEP-11 48x48 Icons [741 B]
Get:22 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye/non-free DEP-11 64x64 Icons [27.7 kB]
Get:23 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye-updates/main Sources [3,588 B]
Get:24 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye-updates/main amd64 Packages [6,344 B]
Get:25 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye-updates/main Translation-en [5,890 B]
Get:26 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye-backports/main Sources [314 kB]
Get:27 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye-backports/non-free Sources [3,996 B]
Get:28 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye-backports/contrib Sources [2,712 B]
Get:29 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye-backports/main amd64 Packages [341 kB]
Get:30 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye-backports/main Translation-en [281 kB]
Get:31 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye-backports/contrib amd64 Packages [4,400 B]
Get:32 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye-backports/contrib Translation-en [4,320 B]
Get:33 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye-backports/non-free amd64 Packages [11.5 kB]
Get:34 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye-backports/non-free Translation-en [8,960 B]
Get:35 https://mirrors.tuna.tsinghua.edu.cn/debian-security bullseye-security/main Sources [160 kB]
Get:36 https://mirrors.tuna.tsinghua.edu.cn/debian-security bullseye-security/non-free Sources [632 B]
Get:37 https://mirrors.tuna.tsinghua.edu.cn/debian-security bullseye-security/main amd64 Packages [189 kB]
Get:38 https://mirrors.tuna.tsinghua.edu.cn/debian-security bullseye-security/main Translation-en [119 kB]
Get:39 https://mirrors.tuna.tsinghua.edu.cn/debian-security bullseye-security/non-free amd64 Packages [528 B]
Get:40 https://mirrors.tuna.tsinghua.edu.cn/debian-security bullseye-security/non-free Translation-en [344 B]
Fetched 40.2 MB in 3min 13s (288 kB/s)
Reading package lists... Done
root@test:/home/test/Documents#
```

- d. Reinstall the HighPoint software.

8.1.2. For RHEL

1. Description of the Problem

When installing the driver, due to various factors, driver files such as **gcc** and **make** cannot be compiled, thus interrupting the driver installation process:

```
[root@localhost Documents]# ./hptnvme_g5_linux_src_v1.4.1_2022_03_04.bin
Verifying archive integrity... All good.
Uncompressing HighPoint NVMe RAID Controller Linux Open Source package installer.....
Checking and installing required toolchain and utility ...
Installing program make ... (failed)
Installing program gcc ... (failed)
```

Or a prompt with **subscription-manager repos**:

```
compile:default boot kernel: /boot/vmlinuz-XXXXXXXXXX.x86_64
dumpkernels:kernel installed
kernel-XXXXXXXXXX.x86_64
dumpkernels:kernel-devel installed
kernel-devel-XXXXXXXXXX.x86_64
dumpkernels:repo list kernel-devel

dumpkernels:end
installlib_centos elfutils-libelf-devel
There are no enabled repos.
Run "yum repolist all" to see the repos you have.
To enable Red Hat Subscription Management repositories:
  subscription-manager repos --enable <repo>
To enable custom repositories:
  yum-config-manager --enable <repo>
compile:some build tools are missing.
/var/lock/subsys/hptdrv-monitor:
```

2. Cause of the Problem

The system is not connected to a network (internet connection) or this is not registered.

3. Solution

- a. Ensure that the network is properly connected.
- b. Go to the Red Hat website and register an account: [Register for | Red Hat IDP](#)
- c. Open the system terminal with root privileges.
- d. Enter the following command to log in:

```
#subscription-manager register --username=*** --password=*** --auto-attach
```

```
[root@localhost Documents]# subscription-manager register --username=XXXXXXXXXX --password=XXXXXXXXXX --auto-attach
Registering to: subscription.rhsm.redhat.com:443/subscription
The system has been registered with ID: 963XXXXXXXXXXf
The registered system name is: localhost.localdomain
```

- e. Reinstall the HighPoint software.

```
[root@localhost Documents]# ./setup.bin
Verifying archive integrity... All good.
Uncompressing HighPoint NVMe RAID Controller Linux Open Source package installer....
.....
Checking and installing required toolchain and utility ...
Installing program make ... done
Installing program gcc ... done
```

8.1.3. For Ubuntu

1. Description of the Problem

When installing the driver, due to various factors, driver files such as **gcc** and **make** cannot be compiled, thus interrupting the driver installation process:

```
root@testlu-Super-Server:/home/testlu/Desktop# ./hptnvme_g5_linux_src_v1.6.2.0_2023_06_21.bin
Verifying archive integrity... All good.
Uncompressing HighPoint NVMe RAID Controller Linux Open Source package installer.....
.....
Checking and installing required toolchain and utility ...
Installing program make ... (failed)
Installing program gcc ... (failed)
Found program perl (/usr/bin/perl)
Found program wget (/usr/bin/wget)
Sourcing file '/etc/default/grub'
```

2. Cause of the Problem & Solution

- **The system is not connected to a network (internet connection).**

Solution:

- a. Ensure that the network is properly connected.
- b. Reinstall the HighPoint software.

- **The system process is occupied/ busy.**

Solution:

- a. Open the system terminal with root privileges and enter the following command:

```
#apt-get update
```

- b. Release the process and update the download source.
- c. Reinstall the HighPoint software.

8.1.4. For Proxmox

1. Description of the Problem

When installing the driver, due to various factors, driver files such as **gcc** and **make** cannot be compiled, thus interrupting the driver installation process:

```
Verifying archive integrity... All good.
Uncompressing HighPoint NVMe RAID Controller Linux Open Source package installer.....
Checking and installing required toolchain and utility ...
Found program make (/usr/bin/make)
Installing program gcc ... (failed)
Found program perl (/usr/bin/perl)
Found program wget (/usr/bin/wget)
old pcie_aspm=off l3mmu=off intel_l3mmu=off amd_l3mmu=off
new pcie_aspm=off l3mmu=off intel_l3mmu=off amd_l3mmu=off
Synchronizing state of hptdrv-monitor.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable hptdrv-monitor
update-rc.d: warning: enable action will have no effect on runlevel 1
Toolchain to build the driver is incomplete, please install the missing package to build the driver.
Exit.
```

2. Cause of the Problem & Solution

- The system is not connected to a network (internet connection).

Solution:

- Ensure that the network is properly connected.
- Reinstall the HighPoint software.

- The system process is occupied/ busy.

Solution:

- Open the system terminal with root privileges and enter the following command:

```
#apt-get update
```

- Release the process and update the download source.
- Reinstall the HighPoint software.

- If you are using a completely new system, the following error occurs when installing the driver or apt-get update. This problem can be caused by a lack of dependency packages:

```
Verifying archive integrity... All good.
Uncompressing HighPoint NVMe RAID Controller Linux Open Source package installer.....
Checking and installing required toolchain and utility ...
Found program make (/usr/bin/make)
Installing program gcc ... (failed)
Found program perl (/usr/bin/perl)
Found program wget (/usr/bin/wget)
old pcie_aspm=off l3mmu=off intel_l3mmu=off amd_l3mmu=off
new pcie_aspm=off l3mmu=off intel_l3mmu=off amd_l3mmu=off
Synchronizing state of hptdrv-monitor.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable hptdrv-monitor
update-rc.d: warning: enable action will have no effect on runlevel 1
Toolchain to build the driver is incomplete, please install the missing package to build the driver.
Exit.
root@test:/home# apt-get update
Hit:1 http://ftp.debian.org/debian bullseye InRelease
Temporary failure resolving 'ftp.debian.org'
Hit:2 http://ftp.debian.org/debian bullseye-updates InRelease
Temporary failure resolving 'ftp.debian.org'
Hit:3 https://security.debian.org bullseye-security InRelease
Temporary failure resolving 'security.debian.org'
Hit:4 https://enterprise.proxmox.com/debian/pve bullseye InRelease
Temporary failure resolving 'enterprise.proxmox.com'
Reading package lists... Done
** failed to fetch http://ftp.debian.org/debian/updates/bullseye/updates InRelease Temporary failure resolving 'ftp.debian.org'
```

Solution:

- The system needs to be resourced. For details, please refer to the official website file: https://pve.proxmox.com/wiki/Downloads#Update_a_running_Proxmox_Virtual_Environment_8.x_to_latest_8.2

- Open the system terminal with root privileges.
- Enter the following command:

```
#nano /etc/apt/sources.list
```

- c) Replace the contents of the file with the following.

```
# deb http://ftp.debian.org/debian bookworm main contrib
# deb http://ftp.debian.org/debian bookworm-updates main contrib
# deb http://security.debian.org bookworm-security main contrib
# deb http://download.proxmox.com/debian/pve bookworm pve-no-subscription
deb http://mirrors.ustc.edu.cn/debian bookworm main contrib non-free-firmware
deb http://mirrors.ustc.edu.cn/debian bookworm-updates main contrib non-free-firmware
deb http://mirrors.ustc.edu.cn/debian-security bookworm-security main contrib
non-free-firmware

deb https://mirrors.ustc.edu.cn/proxmox/debian/pve bookworm pve-no-subscription
```

- d) Enter the following command to edit the source file: /etc/apt/sources.list.d/pve-enterprise.list

```
#nano /etc/apt/sources.list.d/pve-enterprise.list
```

- e) Enter the following command to modify proxmox software source.

```
# deb https://enterprise.proxmox.com/debian/pve bookworm pve-enterprise
```

- f) Enter the following command to edit the source file: /etc/apt/sources.list.d/ceph.list

```
#nano /etc/apt/sources.list.d/ceph.list
```

- g) Enter the following command to modify proxmox ceph source.

```
# deb https://enterprise.proxmox.com/debian/ceph-quincy bookworm enterprise
deb https://mirrors.ustc.edu.cn/proxmox/debian/ceph-quincy bookworm no-subscription
```

- h) Enter the following command to /usr/share/perl5/PVE/CLI/pveceph.pm.

```
#cp /usr/share/perl5/PVE/CLI/pveceph.pm /usr/share/perl5/PVE/CLI/pveceph.pm_back
#sed -i 's|http://download.proxmox.com|https://mirrors.ustc.edu.cn/proxmox|g'
/usr/share/perl5/PVE/CLI/pveceph.pm
```

- i) Enter the following command to modify proxmox lxc source.

```
#cp /usr/share/perl5/PVE/APLInfo.pm /usr/share/perl5/PVE/APLInfo.pm_back
#sed -i 's|http://download.proxmox.com|https://mirrors.ustc.edu.cn/proxmox|g'
/usr/share/perl5/PVE/APLInfo.pm
```

Note: See the mirror list at <https://www.debian.org/mirror/list> for more information.

- j) Enter the following command to restart the service.

```
#systemctl restart pvedaemon
```

- b. apt-get update

```
root@pve:~# apt-get update
Hit:1 http://mirrors.ustc.edu.cn/debian bookworm InRelease
Hit:2 http://mirrors.ustc.edu.cn/debian bookworm-updates InRelease
Hit:3 http://mirrors.ustc.edu.cn/debian-security bookworm-security InRelease
Hit:4 https://mirrors.ustc.edu.cn/proxmox/debian/pve bookworm InRelease
Get:5 https://mirrors.ustc.edu.cn/proxmox/debian/ceph-quincy bookworm InRelease [3,470 B]
Get:6 https://mirrors.ustc.edu.cn/proxmox/debian/ceph-quincy bookworm/no-subscription amd64 Packages [41.5 kB]
Fetched 45.0 kB in 1s (70.4 kB/s)
Reading package lists... Done
root@pve:~#
```

- c. Reinstall the HighPoint software.

8.2.No supporting host adapter is found

1. Description of the Problem

Run the command “go.nsh” in the UEFI command line, the procedure does not start and the message **No supporting host adapter is found** is displayed.

```
FS0:\> go.nsh
FS0:\> load.efi 7540uefi.b1f /a /f
Load Utility for Flash EPROM v1.1.5
(built at Mar 28 2023 17:27:18)

Set flash size to 256K
No supporting host adapter is found.
```

2. Cause of the Problem

The system does not detect the NVMe RAID AIC.

3. Solution

- a. Shut down the system.
- b. Move the AIC to another PCIe slot and re-enter the command.

If the problem still occurs, please provide a [UEFI log](#). You can submit a support ticket using our [Online Support Portal](#) and include a problem description in as much detail as possible.

8.3.No supported controller detected

1. Description of the Problem

Run the command “ArrayCreate.efi” in the UEFI command line, the procedure does not start and the message **No supported controller detected** is displayed.

```
FS0:\SSD7505-uefi\> ArrayCreate.efi
Highpoint RAID utility for UEFI (version: 20200306)
No supported controller detected.
FS0:\SSD7505-uefi\> _
```

2. Cause of the Problem

The OPROM is not configured correctly, which prevents the UEFI driver from loading correctly.

3. Solution

- a. Check whether the [Storage option ROM](#) is Enabled in the system EFI setting.
- b. Check whether NVMe is connected to the NVMe RAID AIC.
- c. Replace the motherboard slot and re-enter the command.

If none of the above methods work, please provide a [UEFI log](#). You can submit a support ticket using our [Online Support Portal](#) and include a problem description in as much detail as possible.

9. Glossary

This glossary defines the terms that are used in this document.

Glossary	Description
Array	RAID (Redundant Array of Independent Drives) array is a system that combines multiple disks to improve data storage performance and redundancy. The RAID array can provide data redundancy backup, improve read/write speed, increase storage capacity, and perform other functions.
AIC	AIC (Add-in Card) Insert the card into the computer motherboard expansion slot to achieve a specific function of the hardware device.
Background	Background initialization means the array will still be created, and you can still write new data onto the array. But when your array requires rebuilding, residual data left behind may interfere with the process.
BIOS	BIOS is an acronym for Basic Input/Output System, a type of firmware that is solidified on a computer's motherboard and used to initialize hardware devices and boot the operating system. The BIOS connects the communication between computer hardware and the operating system and provides basic input/output functions.
Cache	A cache refers to a cache area in a computer system that stores data temporarily. When a computer accesses data on a disk, that data is temporarily stored in the disk cache to speed up subsequent accesses.
Capacity	A property that indicates the amount of storage space on a disk or virtual disk.
CLI	The Command Line Interface (CLI) is a powerful, text-only management interface for advanced users and professional administrators. The universal command lines work with Linux and Windows platforms.
Controller	A chip that controls data transfer between the microprocessor and memory or between the microprocessor and a peripheral device.
Diagnostic	A diagnostic view will appear when the Driver or HPT card has no effect; you can see the system and HPT Product information in this view.
Disk	A disk generally refers to a storage device used to store files and data. This includes solid-state disks (SSDs), both used to store data and allow computers to read and write data.
Enclosure	Enclosure refers to the SSD series RAID AIC currently installed in the system.

Foreground	Foreground initializing the array will completely zero out the data on the disks, meaning the disk will be completely wiped, and every bit on the disk will be set to 0.
Firmware	Firmware is a class of embedded systems software typically stored in the device's non-volatile memory and controls the device's hardware operations. It provides the device with a basic operating system and is usually preinstalled.
HBA	A Host Bus Adapter is a hardware device used to connect a computer host to a storage device. It acts as an interface between the host computer and the storage device, enabling them to communicate directly. It provides high-speed data transfer, improving the storage device's performance and reliability.
Host interface	The host interface is through which a computer system or device communicates with other devices outside the system. The host interface can transfer data, receive commands, control devices, and perform other operations, allowing different devices to interact and communicate.
Initialization	The process of making a redundant virtual disk consistent.
Legacy Disk	The newly inserted disk is configured as a legacy disk.
Link Speed	Connection speed of the port.
Link Width	Connection width of the port.
Mirroring	The process of providing complete data redundancy with two disks by maintaining an exact copy of one disk's data on the second disk.
N/A	N/A means nothing is entered in the CLI (command line interface)
Offline	The system has marked a disk or storage device as offline, meaning the computer cannot access the data and files on that disk.
PCI Location	The Location of the AIC in the system.
Rebuild	The regeneration of all data to a replacement disk in a redundant virtual disk after a disk failure. A disk rebuild normally occurs without interrupting normal operations on the affected virtual disk, though some performance degradation of the disk subsystem can occur.
Rebuild Priority	The priority of rebuilding data onto a new disk after a disk in a storage configuration has failed.
SHI	Storage Health Inspector is used to assess and monitor the health of a storage system and ensure its proper functioning and security.
SMTP	The Simple Mail Transfer Protocol (SMTP) is the standard protocol for sending and receiving email online. It transfers email from the sender to the receiver's mail

	server and allows communication between mail servers.
Temperature	The degree of heat present in the supercapacitors, which is measured in Celsius
Vendor ID	An AIC property indicating the vendor-assigned ID number of the AIC
Virtual disk	A storage unit created by a RAID AIC from one or more disks. Although a virtual disk can be created from several disks, the operating system sees it as a single disk. Depending on the RAID level used, the virtual disk can retain redundant data if there is a disk failure.
WebGUI	The Web RAID Management Interface (WebGUI) is a simple and intuitive web-based management tool for Windows and Linux operating systems. It is an ideal interface for customers unfamiliar with RAID technology. The Wizard-like Quick Configuration menu allows even the most novice user to get everything up and running with a few simple clicks. Experienced users can fine-tune configurations for specific applications using the Setting Options menu.

10. Revision History

10.1. Version 1.00, July 9, 2024

Initial version.

10.2. Version 1.01, August 13, 2024

Add RocketAIC 7749M2W Series support.

10.3. Version 1.02, August 28, 2024

Update [Install the driver on macOS](#), add description of Secure boot and SIP.