

SSD7000 Software Guide

V1.03- October 10, 2024

Copyright 2024 HighPoint Technologies, Inc.

All rights reserved

HighPoint Technologies, Inc

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	
1.3. Technical Support	
1.3.1. One-Click Diagnostic Feature	
2. SafeStorage Encryption	
2.1. Workflow	11
2.1.1. Enable Security	
2.1.2. Change Security	
2.1.3. Create a Secured RAID	
2.1.4. Disable Security	
2.1.5. Import SafeStorage Encryption	14
3. UEFI Command Line Utility	15
3.1. Start the UFEI Command Line Utility	
3.2. Help Command	
3.2.1. Show the Generic Help Command	
3.3. Info Command	19
3.3.1. Show the Physical Device Information	19
3.3.2. Show the Logical Device Information	
3.4. Quit Command	21
3.4.1. Quit the UEFI Command Line Utility	
3.5. Exit Command	22
3.5.1. Exit the UEFI Command Line Utility	
3.6. Create Command	
3.6.1. Create a RAID Array	24
3.7. Delete Command	
3.7.1. Delete a RAID Array	25
3.8. Flashing the UEFI	
4. UEFI HII Utility	
4.1. Start the UEFI HII Utility	27
4.2. UEFI HII Utility Menu View	29
4.2.1. View the Controller Information	
4.2.2. View the Physical Device Information	
4.2.3. View the Logical Device Information	
4.2.4. Create a RAID array	
4.2.5. Delete a RAID array	
5. Install the HighPoint Software	

	5.1. Install the driver on Windows	
	5.1.1. Uninstall the driver on Windows	
	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	
	5.3.1. Uninstall the driver on Linux	
	5.4. Install the RAID Management on Linux	
	5.4.1. Uninstall the RAID Management on Linux	
	5.5. Install the driver on macOS	
	5.5.1. Uninstall the driver on macOS	
	5.6. Install the RAID Management on macOS	
	5.6.1. Uninstall the RAID Management on macOS	
6.	. Web RAID Management Interface	
	6.1. Start the WebGUI	
	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	
	6.3.2. Enclosure Information	
	6.3.3. Physical Devices Information	
	6.3.4. Update the Firmware	61
	6.3.5. Secure Setting	
	6.3.6. Rescan the Physical Device	63
	6.4. Logical	
	6.4.1. Logical Device Information	
	6.4.2. Physical Device Information	
	6.4.3. Create a RAID Array	
	6.4.4. Delete a RAID Array	
	6.4.5. Unplug a RAID Array	
	6.4.6. Verify a RAID Array	
	6.4.7. Add a Spare Disk	
	6.4.8. Remove a Spare Disk	74
	6.5. Setting	75
	6.5.1. System Setting	
	6.5.2. Password Setting	
	6.5.3. Email Setting	
	6.6. Event	85
	6.6.1. View the Event Log	
	6.6.2. Save the Event Log	
	6.6.3. Event Log Icon Guide	
	6.7. SHI	
	6.7.1. View the SHI Information	

6.7.2. View the SMART Information	
6.7.3. Set the Temperature Threshold	
6.7.4. Create a Health Inspector Scheduler	
6.7.5. Create a New Verify Task	
6.7.6. Delete a Task	
6.8. Help	
6.8.1. Online Help	
6.8.2. Diagnostic View	
6.8.3. Save the Diagnostic Log	96
7. Command Line Interface	101
7.1. Start the CLI	
7.2. Query Commands	
7.2.1. Query Controller	
7.2.2. Query Enclosure	
7.2.3. Query Device	
7.2.4. Query Array	
7.3. Init Commands	
7.3.1. Init a Physical Disk	
7.3.2. Init a RAID Array	
7.4. Create Command	113
7.4.1. Create a RAID Array	
7.4.2. Create a Spare Disk	
7.5. Delete Command	
7.5.1. Delete a RAID Array	
7.5.2. Delete a Spare Disk	
7.6. Rebuild Command	118
7.6.1. Rebuild a RAID array	
7.6.2. Start Rebuilding the RAID Array	
7.6.3. Stop Rebuilding the RAID Array	
7.7. Verify Command	
7.7.1. Start Verifying the RAID Array	
7.7.2. Stop Verifying the RAID Array	
7.8. Rescan Command	121
7.8.1. Rescan the Physical Devices	
7.9. Lscard Command	
7.9.1. Lscard all AICs	
7.10. Events Command	
7.10.1. View the Event Log	
7.10.2. Save the Event Log	
7.11. Mail Command	
7.11.1. Add a Mail Recipient	
7.11.2. List all Mail Recipients	
7.11.3. Test the mail recipient	

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

7.22.1. Clear the CLI screen	151
8. Trouble shooting	152
8.1. Fail to compile gcc, make and other driver files	152
8.1.1. For Debian	
8.1.2. For RHEL	
8.1.3. For Ubuntu	
8.1.4. For Proxmox	
8.2. No supporting host adapter is found	
8.3. No supported controller detected	158
9. Glossary	
10. Revision History	
10.1. Version 1.00, July 9, 2024	
10.2. Version 1.01, August 13, 2024	
10.3. Version 1.02, August 28, 2024	
10.4. Version 1.03, October 10, 2024	

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/RS6542AW /RA6542AWW-S491T5-12
LED Indicators	SSD6444/ SSD6444M/ SSD6540/ SSD6540M/ SSD6780A/ SSD7749M/
	RS6542AW/ RocketAIC7749MWSeries/ RA6542AWW-S491T5-12
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/ RA6542AWW-S491T5-12
SafeStorage Encryption	SSD7580C/ SSD7749M/ SSD7749M2/ SSD7749E/ SSD6780A/ RS6542AW/
Salestor age Eneryption	
	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/RA6542AWW-S491T5-12
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/RA6542AWW-S491T5-12
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/RA6542AWW-S491T5-12
Flash ROM for Upgradeable UEFI	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/RA6542AWW-S491T5-12

1.3. Technical Support

For assistance with using your HighPoint NVMe RAID AIC, please contact our <u>Technical Support</u> <u>Department.</u>

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 <u>Online Support Portal</u>.

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. <u>Enable AIC security</u> and create a security key that conforms to the security requirements.
- 3. <u>Enable disk security</u>. The key used to secure the disk is the same as the key generated when the board is secured.
- 4. <u>Enable RAID security</u> 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.

Aptio Setup - AMI PCIe/PCI/PnP Configuration			
PCI Bus Driver Version PCI Devices Common Settings	A5.01.24	▲ Enables or disables PCIe Slot OPROM option.	
Above 4G Decoding SR-IOV Support ARI Support Bus Master Enable	[Enabled] [Enabled] [Enabled] [Enabled]		
MMIO High Base MMIO High Granularity Size	[32T] [256G] PU1 Slot 2 PCI-E 4.0	×15.0PR04	
	bled	lect Screen	
VGA Priority		lect Item	
Onboard Video Option ROM	[UEFI]	+/-: Change Opt.	
PCI Devices Option Rom Setting		F1: General Help F2: Previous Values F3: Optimized Defaults	
CPUI Slot 1 PCI-E 4.0 x8 OPROM CPUI Slot 2 PCI-E 4.0 x16 OPROM CPUI Slot 3 PCI-E 4.0 x16 OPROM	(EFI)	F4: Save & Exit ESC: Exit	
CPU2 Slot 4 PCI-E 4.0 ×16 OPROM CPU2 Slot 5 PCI-E 4.0 ×16 OPROM	[EFI] [EFI]		

3) Save changes and reboot.

SSD7000 Software Guide

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

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 UFEI 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:

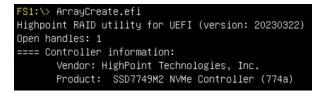
mode 100 31

FS0:\>	mode					
Availa	ole mo	odes	for co	nsole	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



3.2.Help Command

>>> Please specify command to execute: <<< help_</pre>

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
н	N/A	This command shows generic help about this utility.
h		
help		

3.2.1. Show the Generic Help Command

<u><<<H/ h/ help</u>

This command shows generic help about this utility.

Input example:

<<<help



3.3.Info Command

>>> Please specify command to execute: <<< info</p>

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

<u> <<<info</u>

Disks hosted by the AIC will appear here

Input example:

<<<info

<<< info
==== Physical device list(count 4):
1/1 Samsung SSD 980 PRO 1TB-S5GXNX1W506237F, 1000204MB(MaxFree OMB), Normal
1/2 KXG80ZN84T09 KIOXIA-4122X2BFA00WFU26, 4096805MB(MaxFree 0MB), Normal
1/3 HP-EM2802T0GMTCB58R-E264-2311270010002, 2000398MB(MaxFree OMB), Normal
1/4 KXG60ZNV1T02 TOSHIBA-694S10OMTVDQ, 1024209MB(MaxFree OMB), 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.

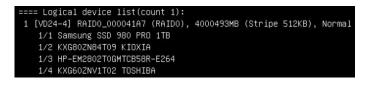
3.3.2. Show the Logical Device Information

<u> <<<info</u>

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

Input example:

<<<info



- 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_</pre>

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

<u><<<Q/ q/ quit</u>

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

<u> <<<exit</u>

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

Input example:

<<<exit

3.6.Create Command

>>> Please specify command to execute: <<< create_</p>

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

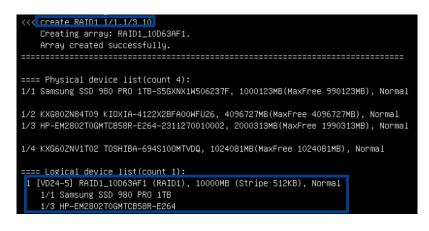
3.6.1. Create a RAID Array

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

This command allows you to create a new RAID array.

Input example:

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



3.7. Delete Command

>>> Please specify command to execute:
<<< delete_</pre>

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.

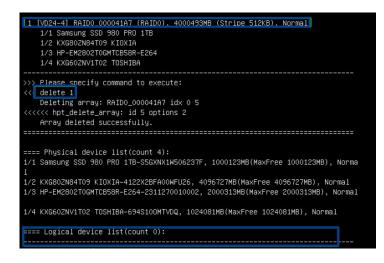
3.7.1. Delete a RAID Array

<<<delete {array id}</pre>

This command allows you to delete an existing RAID array.

Input example:

<<<delete 1



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.

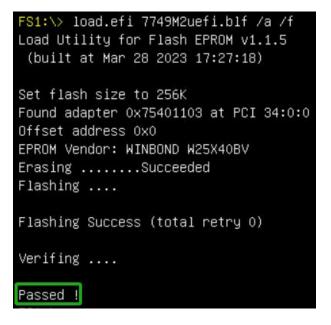
1. Enter the motherboard's BIOS and select the UEFI: USB flash drive in the BIOS startup item.

```
Boot Override
SanDisk
BRCM 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.



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.
- 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**.

Aptio Setup - AMI PCIe/PCI/PnP Configuration				
PCI Bus Driver Version	A5.01.24	Enables or disables PCIe Sid		
PCI Devices Common Settings				
Above 4G Decoding	[Enabled]			
SR-IOV Support	[Enabled]			
ARI Support	[Enabled]			
Bus Master Enable	[Enabled]			
MMIO High Base	[32T]			
MMIO High Granularity Size	[256G]			
Maximum Read Request	CPU1 Slot 2 PCI-E 4.0	×16 OPROM		
MMCFG Base Dis	sabled			
NVMe Firmware Source				
		lect Screen		
VGA Priority		lect Item		
		Enter: Select		
Onboard Video Option ROM	[UEFI]	+/-: Change Opt.		
		F1: General Help		
PCI Devices Option Rom Setting		F2: Previous Values		
		F3: Optimized Defaults		
CPU1 Slot 1 PCI-E 4.0 x8 OPROM	[EFI]	F4: Save & Exit		
CPU1 Slot 2 PCI-E 4.0 x16 OPROM	([EFI]	ESC: Exit		
CPUIT STOT 3 PCT_E 4 0 VIE OPPON				

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.

Aptio Setup – AMI Main <mark>Advanced</mark> Event Logs IPMI Security Boot Save & Exit	
 Boot Feature CPU Configuration Chipset Configuration Server ME Information SATA Configuration SATA Configuration PCIE-PCI/PhP Configuration Super ID Configuration Serial Port Console Redirection ACPT Settings Trusted Computing Network Configuration HTTP Boot Configuration 	Utility to manage RAID(s) of HighPoint RAID Controller.
 TLS Authenticate Configuration Intel(R) I350 Gigabit Network Connection - 3C:EC:EF:B6:CA:08 VLAN Configuration (MAC:3CECEF86CA08) MAC:3CECEF86CA08-IPv4 Network Configuration MAC:3CECEF86CA08-IPv4 Network Configuration Intel(R) I350 Gigabit Network Connection - 3C:EC:EF:B6:CA:09 VLAN Configuration (MAC:3CECEF86CA09) VAC:ACEFF86CA09-IPv4 Network Configuration MAC:3CECEF86CA09-IPv4 Network Configuration MBC:3CECEF86CA09-IPv4 Network Configuration MBC:3CECEF86CA09-IPv4 Network Configuration 	++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

4. Select HighPoint RAID Management Utility and enter it.

4.2. UEFI HII Utility Menu View



<u>Keys</u>

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

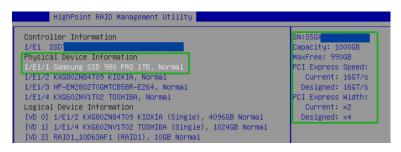
connected to the system will appear here.

Controller Information		PCI Express Speed:
1/E1 SSD	ð	Current: 16GT/s
Physical Device Information		Designed: 16GT/s
1/E1/1 Samsung SSD 980 PRO 1TB,	Normal	PCI Express Width:
1/E1/2 KXG80ZN84T09 KIOXIA, Nor	mal	Current: x16
1/E1/3 HP-EM2802T0GMTCB58R-E264	, Normal	Designed: x16
1/E1/4 KXG60ZNV1T02 TOSHIBA, No	rmal	Ver: v2.3.9
Logical Device Information		Jan 30 2024 10:35:36
[VD 0] 1/E1/2 KXG80ZN84T09 KIOX	IA (Single), 4096GB Normal	
[VD 1] 1/E1/4 KXG60ZNV1T02 TOSH	IBA (Single), 1024GB Normal	
[VD 2] RAID1_10D63AF1 (RAID1),	10GB Normal	
Create RAID		
Delete RAID		
Utility built on	May 8 2023 14:06:50	↔: Select Screen

- 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

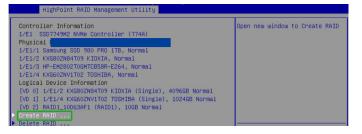
The UEFI HII Utility view allows you to view the Logical Device Information. The disks and arrays you create and their associated properties will appear here.

1/E1 SSD 2 1/E1/3 Physical Device Information 1/E1/1 Samsung SSD 980 PR0 1TB, Normal 1/E1/2 1/E1/1 Samsung SSD 980 PR0 1TB, Normal 1/E1/2 1/E002N84T05 1/E1/2 1/E1/2 KX6002N84T05 KIDXIA, Normal 1/E1/3 1/E1/3	HP-EM2802TOGM
1/E1/1 Samsung SSD 980 PRO 1TB, Normal 1/E1/2 KXG802N84T09 KIOXIA, Normal	
1/E1/2 KXG80ZN84T09 KIDXIA, Normal	
1/E1/3 HP-EM2802T0GMT0B58R-E264, Normal	
1/E1/4 KXG60ZNV1T02 TOSHIBA, Normal	
Logical Device Information	
[VD 0] 1/E1/2 KXG80ZN84T09 KIOXIA (Single), 4096GB Normal	
[VD 1] 1/E1/4 KXG60ZNV1T02 TOSHIBA (Single), 1024GB Normal	

- 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.

Select disk(s) to be used to create	RAID:
1/E1/1 Samsung SSD 980 PRO 1TB	[Disabled]
1/E1/2 KXG80ZN84T09 KIDXIA	[Disabled]
(Single)	
1/E1/3 HP-EM2802T0GMTCB58R-E264	[Disabled]
1/E1/4 KXG60ZNV1T02 TOSHIBA	[Disabled]
(Single)	

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**.

Create RAID	
Specify RAID type, member disks ar RAID	nd RAID capacity to Create
Select RAID type from dropdown list	[]
Select disk(s) to be used to creat	te RAID:
1/E1/1 Samsung SSD 980 PRO 1TB	[Disabled]
1/E1/2 KXG80ZN84T09 KIOXIA (Single)	[Disabled]
1/E1/3 HP-EM2802T0GMTCB58R-E264	[Disabled]
1/E1/4 KXG60ZNV1T02 TDSH (Single) Desired RAID Capacity (G Press to Create RAID ▶ Return to main window RAID10	ct RAID type from dropdown list ———

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

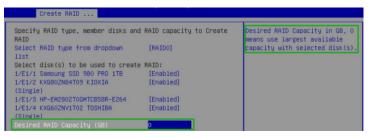
to Enabled.

Create RAID	
Specify RAID type, member disks an RAID	d RAID capacity to Create
Select RAID type from dropdown list	[RAIDO]
Select disk(s) to be used to creat	e RAID:
1/E1/1 Samsung SSD 980 PRO 1TB	[Disabled]
1/E1/2 KXG80ZN84T09 KIOXIA	[Disabled]
(Single)	
1/E1/3 HP-EM2802T0GMTCB58R-E264	[Disabled]
1/E1/4 KXG60ZNV1T02 TOSHIBA	[Disabled]
(Single) 1/E	1/1 Samsung SSD 980 PRO 1TB
Desired RAID Capacity (GB) Disabl	ed
Press to Create RAID	

SSD7000 Software Guide

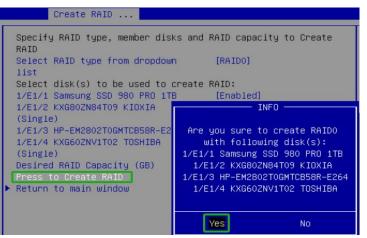
5. Use the keyboard to input the space (GB) you want to set aside for this array. You can decide how

much storage capacity will be assigned to the array.



6. 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.



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

operation again.

Create RAID		
Specify RAID type, member disks ar RAID	d RAID capacity to Create	Press
Select RAID type from dropdown list	[RAIDO]	
Select disk(s) to be used to creat	e RAID:	
1/E1/1 Samsung SSD 980 PRO 1TB	[Enabled]	
1/E1/2 KXG80ZN84T09 KIOXIA (Single)	[Enabled]	
1/E1/3 HP-EM2802T0GMTCB58R-E264	[Enabled]	
1/E1/4 KXG60ZNV1T02 TOSH (Single)		
Desired RAID Capacity (G RAIDO_005 Press to Create RAID	20668 (RAIDO) Creation succe	eaea.
Return to main window	Ok	

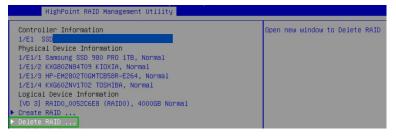
8. The array you create, and its associated properties will appear under the **Logical Device**

Information.

Controller Information			1	1/E1/1 Samsung SSD 9
1/E1 SSD			2	1/E1/2 KXG80ZN84T09
Physical Device Information			3	1/E1/3 HP-EM2802T0GM
1/E1/1 Samsung SSD 980 PRO 1TB	, Normal		4	1/E1/4 KXG60ZNV1T02
1/E1/2 KXG80ZN84T09 KIOXIA, No	rmal			
1/E1/3 HP-EM2802T0GMTCB58R-E26	4, Normal			
1/E1/4 KXG60ZNV1T02 TOSHIBA, N	ormal			
Logical Device Information				
	4000GB Normal			
Create RAID				
Delete RAID				
Utility built on	May 8 202	3 14:06:50		

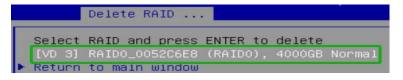
4.2.5. Delete a RAID array

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 and RAID Management need to be used together.

• 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.

System Mode	Audit	Secure Boot feature is
Vendor Keys	Active	Active if Secure Boot is
Secure Boot	Not Active	Enabled, Platform Key(PK) is
Secure Boot	[Disabled]	enrolled and the System is
Secure Boot Mode	[Custom]	The mode change requires
CSM Support	[Enabled]	platform reset



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** (**H**)-**R** keys to access the Startup Security Utility.
- 2) Set Secure Boot to No Security.

00	Startup Security Utility		
T	Firmware password protection is off. Turn on a firmware password to prevent this computer from starting up from a different hard disk, CD, or DVD without the password.		
	Turn On Firmware Password		
Secure Bo	ot		
trusted b installation	inat only your current OS, or signed operating system software currently y Apple, can run. This mode requires a network connection at software		
	by version of signed operating system software ever trusted by Apple to run.		
ONo Secu Does not	irity enforce any requirements on the bootable OS.		
External B	oot		
-	booting from external media the ability to boot from any devices such as USB and Thunderbolt drives.		
	boting from external media restrict the ability to boot from any devices.		

Note: For a list of products with the T2 Security Chipset, please visit the following website: <u>Mac</u> 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.

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



- 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.

• • •		MacBook Pro
✓ Hardware ATA Apple Pay Audio	Model Identifier: Firmware Version: Boot UUID: Boot Policy:	MacBookPro17,1 iBoot-6723.120.36 EB0BF9A4-BD52-4A36-B9F5-701A30C0417B
Bluetooth	Secure Boot:	Reduced Security
Camera	System Integrity Protection:	Enabled
Card Reader	Signed System Volume:	Enabled
Controller	Kernel CTRR:	Enabled
Diagnostics	Boot Arguments Filtering:	Enabled
Disc Burning	Allow All Kernel Extensions:	Yes
Ethernet Cards	User Approved Privileged MDM Operations:	
Fibre Channel	DEP Approved Privileged MDM Operations:	No

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.

	1 0 1 2							8	(9	1 0				delete
tab	Q	w	E	R	T	X	U	L.	0	1	2	1	}	$-\frac{1}{\lambda}$
• cape lock	A	s	D	F	G	н	L		ĸŢ	L]	1		Γ	return
10.01			x	с	v	в	N	м	< ,	>	3			shift
tn co	ntral apt		35 Inum)					X commar	7 100		•	•	•

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.

Ű	macOS Utilities	File	Edit	Utilities	Window
				S S	tartup Security Utility
				() N	letwork Utility
				≥ T	erminal 📡

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

csrutil disable

• • •	Terminal — -bash — 80×24
-bash-3.2# csrutil status System Integrity Protection	status: enabled (Apple Internal).
-bash-3.2# csrutil disable Successfully disabled Syste r the changes to take effec	n Integrity Protection. Please restart the machine fo

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

Ś	Term	ninal	Shell	Edit	View	Window	Help
St	artup I	Disk					
Re	estart				Terr	minal — -ba	sh — 8
Sł	nut Dov	wn	il	statu	s		

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

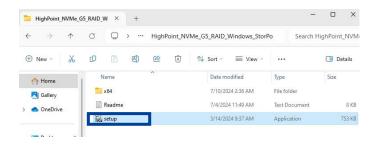
csrutil status

				1	tes	t — -zsh — 80×
Last]	login:	Sat Oct	12 17:	18:44	on	console
test@t	testsM	B2016101	5~%0	sruti	l st	tatus
System	n Inte	grity Pr	otectio	on stat	tus	: disabled.

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.

Completing HighF Controller Driver S		Me RAII	D
HighPoint NVMe RAID Control your computer.	ller Driver has	been installe	d on
Click Finish to dose Setup.			
< Back	Finish	Car	ncel

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.

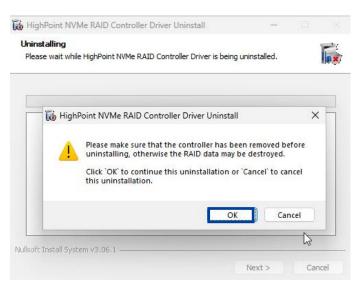
Notes:

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.

😰 Programs and Features			S		- 0
\leftarrow \rightarrow \checkmark \uparrow \blacksquare \diamond \diamond c	ntrol Panel > Programs > Programs and	Features	~ C	Search	Programs and Featu
Control Panel Home	Uninstall or change a progra	am the list and then click Uninstall, Change, or Repair.			
Turn Windows features on or off	1.2.1	the list and then eller officiation, change, of hepoil.			-
	Organize 👻 Uninstall/Change				≡ •
	Name	Publisher	Installed On	Size	Version
	HighPoint NVMe RAID Controller Driv	er	5/19/2024		
	HighPoint RAID Management	Uninstall/Change	5/19/2024		3.1.0
	C Microsoft Edge	Microsoft Corporation	5/19/2024		125.0.2535.51

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



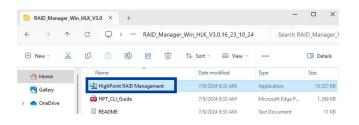
6. After uninstalling the driver, click **Finish**.

🐻 HighPoint NVMe RAID Co	ontroller Driver Uninstall			×
	Completing High Controller Driver HighPoint NVMe RAID Cont from your computer. Click Finish to close Setup.	Uninstall		
	< Back	Finish	Can	cel

5.2. Install the RAID Management on Windows

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

- 1. Make sure you have installed the HighPoint driver. If not, please refer here to install.
- 2. Locate the HighPoint RAID Management Software download and open the file.
- 3. Double-click HighPoint RAID Management.exe.

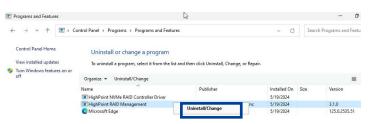


4. After the driver installation is complete, click Finish to proceed.

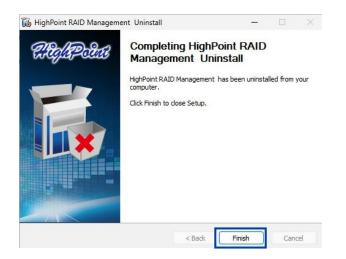
5.2.1. Uninstall the RAID Management on Windows

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

- 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/

	sudo su	
[sudo] password for test:		The second second second second
root@test-Super-Server:/home/test,	/Desktop#	cd /home/test/Downloads/
root@test-Super-Server:/home/test,	Download:	5#

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

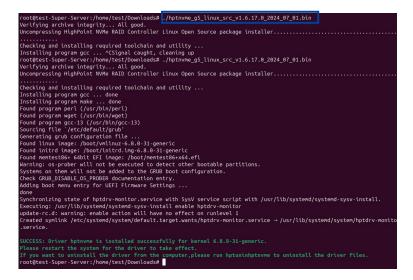
#tar zxvf HighPoint_NVMe_G5_Linux_Src_vx.x.xx_xx_xx_tar.gz



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

#sh hptnvme_g5_linux_sre_vxx.x.x_xx_xx.bin or

#./ hptnvme_g5_linux_sre_vxx.x.x_xx_xx_xx.bin



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

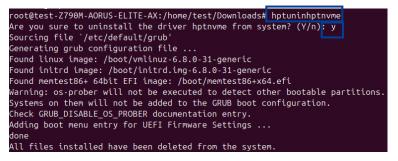
Perform the following steps to uninstall the HighPoint driver on the Linux Operating System.

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



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

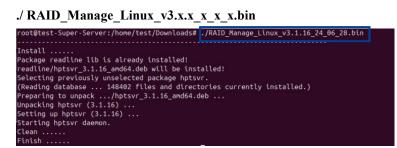
Install the RAID Management on Linux 5.4.

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

- 1. Make sure you have installed the HighPoint driver. If not, please refer here to install.
- 2. 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 x.tgz



Install the HighPoint RAID management software (WebGUI & CLI) using the following 3. command:

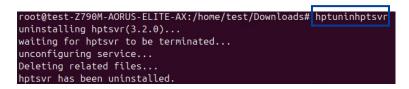


5.4.1. Uninstall the RAID Management on Linux

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

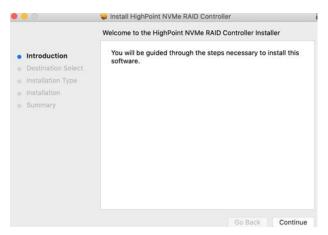


5.5. Install the driver on macOS

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.



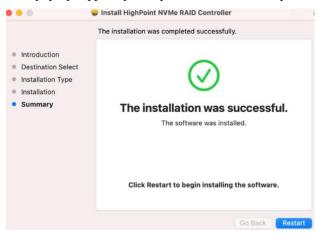
2. macOS will prompt you to install the driver. Click **Install** to proceed.

	Standard Install on "Untitled"	
Introduction	This will take 983 KB of space on your computer.	
 Destination Select Installation Type Installation Summary 	Click Install to perform a standard installation of this software on the disk "Untitled".	
	Change Install Location	

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**.

0	Installer is t	rying to install new software.	
Introduc	Enter your pas	sword to allow this.	
Destinat	User Name:	test	oftware
Installat	Password:	•••••	
Installati			
		Cancel 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**.

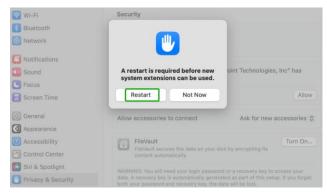
E

		ally.
Introduction		
Destination Select	System Extension Updated	
Installation Type	A program has updated system	
Installation	extension(s) signed by "HighPoint Technologies, Inc". To finish the update,	
Summary	you must approve it in the Security & Privacy System Preferences.	successful.
	ОК	indired.
	Open Security Preferences	
	Click Restart to begin insta	lling the software.
		Go Back Restart

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

•••	Privacy & Security
Q Search	O Screen Recording
Sign in with your Apple ID	Automation >
🛜 Wi-Fi	🛃 App Management >
Bluetooth	Developer Tools
Kotifications	Analytics & Improvements
 Sound Focus 	Apple Advertising
Screen Time	Security
6 General	Allow apps downloaded from
Appearance	O App Store
Accessibility Control Center	• App Store and identified developers
Siri & Spotlight	System software from developer "HighPoint Technologies, Inc" was blocked from loading.
🥑 Privacy & Security	Allow
🗖 Desktop & Dock	Allow
Displays	All

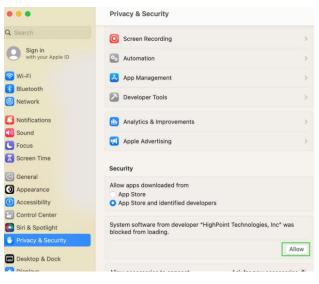
7. You will see a popup window prompting you to restart. Click Restart.



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

again.		
 Introduction Destination Select Installation Type Installation Summary 	Correction of the second secon	ully. successful. talled.
	Click Restart to begin insta	lling the software. Go Back Restart

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



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

			\cap
Q Search	Apple Advertising		
Sign in	Apple Advertising		Privacy & Security
Wi-Fi	Security		Privacy & Security needs to authenticate to continue.
Bluetooth	Allow apps downloaded from		Enter the password for the user "test" to
	App Store		ellow this.
Network			Password
Notifications		se it is not from an	Cancel OK
Cound Sound			vare was installed.
C Focus	A restart is required before new	Open Anyway	vare was installed.
Screen Time	system extensions can be used.	oparradium	1
General	Restart Not Now	oint Technologies, Inc* has	
O Appearance			estart your Mac.
Accessibility		Allow	
Control Center	Allow accessories to connect	Ask for new accessories C	
💽 Siri & Spotlight	Anow accessories to connect	Nok tor new docessories Q	Go Back Restart
Privacy & Security	FileVault		-

11. Return to the driver installation window. Click Restart to restart the system.

• • •	😺 Install HighPoint NVMe RAID Controller	E
	The installation was completed successfully.	
Introduction		
Destination Select		
Installation Type		
Installation		
Summary	The installation was successful.	
	The software was installed.	
	Click Restart to begin installing the software.	
	Go Back Resta	irt

12. 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:

			cBook Pro	(Pro			
NVMExpress	Extension Name	^	Version	Last Modified	Notarized	Loaded	Obtained from
PCI	HFS_MacChineseSimp		8.0	2022/7/22, 00:15	Unknown	No	Not Signed
Parallel SCSI	HFS_MacChineseTrad		8.0	2022/7/22, 00:15	Unknown	No	Not Signed
Power	HFS_MacCyrillic		8.0	2022/7/22, 00:15	Unknown	No	Not Signed
Printers	HFS_MacJapanese		8.0	2022/7/22, 00:15	Unknown	No	Not Signed
SAS	HFS_MacKorean		8.0	2022/7/22, 00:15	Unknown	No	Not Signed
SATA	HFSEncodings		1.0	2022/7/22, 00:15	Unknown	No	Not Signed
SPI			4.4.5			NO	
Storage	HighPointIOP HighPointNVMe		1.1.30	2022/7/22, 00:15	Yes		Identified Develo
Thunderbolt/USB4	HighPointNVMe		1.1.30	2022/7/25, 00:55	Yes	Yes	Identified Develo
USB					•		
Network	HighPointNVMe:				7		
Firewall							
Locations	Version: 1.1.3						
Volumes		7/25, 00:55		222			
WWAN	Bundle ID: com Notarized: Yes	highpoint-tech.kext.H	lighPointN	/Me			
Wi-Fi	Loaded: Yes						
Software		tified Developer					
Accessibility	Kind: Univ						
Applications		4e. x86 64					
Developer	64-Bit (Intel): Yes						
Disabled Software		ary/Extensions/HighP	ointNVMe.k	ext			
	Kext Version: 1.1.3						
Extensions		6741874802557000					
Fonts	Loadable: Yes						
Frameworks	Dependencies: Inco Dependency Errors:	nplete					
Installations	Dependency Errors: Dependency Resolution	o Epilurae:					
		cies can't be resolved		om.apple.iokit.IOStor	ageEamily cou	m annia iakit l	OPCIEamily
Language & Region							
Language & Region Legacy Software	Signed by: Deve	loper ID Application:	HighPoint T	echnologies. Inc (DX)			
		ority, Apple Root CA	HighPoint T	echnologies, Inc (DX	ogoamanz), t	veveloper ib c	entification
Legacy Software			HighPoint T	echnologies, Inc (DX	5G69M9N2), I	veveloper ib (ertification
Legacy Software Logs			HighPoint T	echnologies, Inc (DX	popamanz), r		ertification
Legacy Software Logs Managed Client			HighPoint T	echnologies, Inc (DX	oGoamanz), t	Jeveloper in C	eruncation
Legacy Software Logs Managed Client Preference Panes			HighPoint T	echnologies, Inc (DX	6669M9N2), I	Jeveloper in C	Leruncation
Legacy Software Logs Managed Client Preference Panes Printer Software Profiles			HighPoint T	echnologies, Inc (DXI	9069W3W2), I		Sertification
Legacy Software Logs Managed Client Preference Panes Printer Software Profiles Raw Support			HighPoint T	echnologies, Inc (DXI	обрамант2), Г		Sertification
Legacy Software Logs Managed Client Preference Panes Printer Software Profiles			HighPoint T	echnologies, Inc (DX	рорамант), Г		ernication

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 /

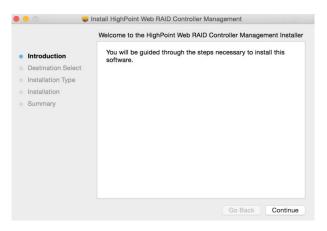


3. After uninstalling the driver, manually reboot the system.

5.6. Install the RAID Management on macOS

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

- 1. Make sure you have installed the HighPoint driver. If not, please refer here to install.
- 2. Double-click the package named **HighPointWebGUI.pkg** to start the installer. When the window appears, click the **Continue** button.



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

	Standard Install on "1010"
Introduction	This will take 2.7 MB of space on your computer.
Destination Select	Click Install to perform a standard installation of this software
Installation Type	for all users of this computer. All users of this computer will be able to use this software.
Installation	
Summary	

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

	Standard Install on "1010"	
Introduction Destination S Installation T Installation Summary	your password to allow this.	re be
	Go Back	

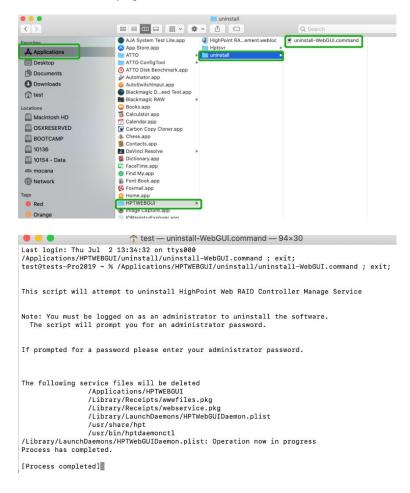
5. The WebGUI Management software has been installed. Click Close to complete the procedure.

••0	Install HighPoint Web RAID Controller Management
 Introduction Destination Select Installation Type Installation Summary 	The installation was completed successfully. The installation was successful. The software was installed.
	Go Back Close

5.6.1. Uninstall the RAID Management on macOS

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

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



6. Web RAID Management Interface

Global View	Physical	Logical	Setting	Event	SHI	Help	
-------------	----------	---------	---------	-------	-----	------	--

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

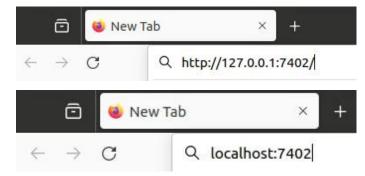
For Windows Users

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 <u>http://127.0.0.1:7402</u> or <u>localhost:7402</u> 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.

210 10 0

Controller(1): HighPoint V

Event SHI Help Storage Properties	Physical Logical Setting	lobal View
Storage imperites		
Total Capacity: 19203 G	el: HighPoint NVMe RAID Controller	Host Adapter mode
Configured Capacity: 19203 G	1	Controller count:
Free Capacity: 0 GB	1	Enclosure count:
	4	Physical Drive:
	4	Legacy Disk:
Configured 100.0%	0	RAID Count:

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			Co	ontroller	Inform	ation
Enclosure 1	Model Name:		HighPoint NVMe RAID Controller			
Devices	Vendor:		HighPoi	int Technolog	ies, Inc.	
Rescan						

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.

Global View	Physical Logical	Setting Event SHI He		
ontroller 1		Enclosure Information		
Enclosure 1	Model:	SSD7749M2 NVMe Controller		
cholo dato 1	Vendor:	HighPoint		
Devices	ID:	1		
Rescan	SN:	00000ce000000		
Kescan	Temperature:	43 (C)		
	PCI Location:	10:0.0		
	Current Link Width:	×16		
	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 Setti	ng Event S	HI Help	
Controller 1		P	hysical Devices	Information	
Enclosure 1	bevic	e 1 E1 5 Model	Micron_7400_MTFD	KCB7T6TDZ Capacity 7	.68 TB
Devices	Unplu	g Revision	E1MU23Y5	PCIe Width	x4
Rescan		Location	1/E1/5	PCIe Speed	Gen 4
Rescan		Max Free	0.00 GB		
		Status	Legacy		
		Serial Num	2316423C3572		
		Interface	NVME	Туре	SSD
		SED Capable	No	SED Type	None
		Secured	No	Cryptographic Eras Capable	e 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.

Secured Status	Description
Yes	Indicates that security for the disk is enabled and unlocked. Your optional option is: Secure Information [Cryptographic Erase Close - Cryptographic Erase The Cryptographic Erase function will erase the secured key inside each disk, making it impossible to decrypt data stored on these devices.
Yes (Locked)	Indicates that the security of the disk is enabled, but the disk's key does not match the key on the AIC. Your optional options are: Secure Information [Change Key] Change Key Enter the disk's old password and click Change Key to unlock the Disk Security 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. - Cryptographic Erase The Cryptographic Erase function will erase the secured key inside each disk, making it impossible to decrypt data stored on these devices.
No Device 1 E1 3 Model Micron_7450_MTFDKCC7T6TFR Capacity 7.68 TB Unables Revision E2MU200 PCLe Width x4 Location 1/E1/3 PCLe Speed 16.0 GT/s Max Free 0.00 GB Status Legacy Serial Num 23264184859A Identify LED IONI [OFF] Teteface NVME X Type S5D S5D Capabile No SED Capabile No	Indicates that disk security is not enabled or not supported.
Yes	Indicates that security for the disk is enabled and unlocked. Data can

Table 8: Secured Status & Description	Table 8:	Secured	Status &	b Description
---------------------------------------	----------	---------	----------	----------------------

Ŀ	Device 1 E1	7 Model	Samsung SSD 960 EVO 2500	SB Capacity 25	0.05 GB	be accessed.
		Revision Location Max Free Status Serial Num Interface SED Capable Secured	3B7QCXE7 1/E1/7 0.00 GB Legacy 53ESNX0J503825P NVME Yes Yes	PCIe Width PCIe Speed Identify LED Type SED Type Cryptographic Erase Capable	x4 8.0 GT/s SSD OPAL Yes	
Y	es (Locl	ked)				Indicates that the security of the disk is enabled, but the disk's key
	<u>Device 1 E1</u> <u>Unplug</u>	1 Model Revision Location Max Free Status Serial Num Interface SED Capable Secured	Samsung SSD 990 PRO 11B 482Q3XD7 1/E1/1 0.00 GB S007B S007B S02L1300W325847W NVME Yes Yes Yes(Locked)	Capacity 1. PCIe Width PCIe Speed Identify LED Type SED Type Cryptographic Erase Capable	00 TB x4 16.0 GT/s [ON][OFF] SSD OPAL Yes	does not match the key on the AIC.

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.

Controller 1			Р	hysical Devices Infor	nation	
Enclosure 1	5	Device 1 E1	1 Model	Samsung SSD 980 PRO 1TB	Capacity	1.00 TB
Devices	_	Device 1 E1	2 Model	Samsung SSD 980 PRO 1TB	Capacity	1.00 TB
Rescan			Revision Location Max Free Status Serial Num	5B2QGXA7 1/E1/2 0.00 GB Normal S5GXNG0N905305N	PCIe Width PCIe Speed	x4 Gen 4
			Interface SED Capable	NVME Yes	Type SED Type Cryptographic	SSD OPAL
			Secured	Yes(Locked) Secure Inform Composition Composition	Capable	Tes

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.

Global View	Physical	Logical	Setting	Even	t SHI	Hel	p	Sarchie Y	
Create Array		<u> </u>	Log	gical De	vice Info	rmatio	on		Ĩ
Spare Pool	Name	Туре	Secure	d Capacity	BlockSize S	ectorSize	OS Name	Status	
Logical Device	Device	_1_E1_1 Hard [Disk No	960.19 GE	3		HPT DISK 0_	0 Legacy	Maintenance
Rescan	Device	_1_E1_2 Hard [Disk No	1.92 TB			HPT DISK 0_	1 Legacy	Maintenance
Beeper Mute	Device	_1_E1_3 Hard [Disk Yes	500.10 GE	3		HPT DISK 0_	2 Legacy	Maintenance
	Device	_1_E1_4 Hard [Disk	Legac	y Inform	ation	K 0_	3 Legacy	Maintenance
				evice_1_E1	_3		Init		

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

Global View	Physical Log	jical S	etting	Event	SH	I H	elp		9194W	
Create Array			Logic	al Dev	vice In	format	ion			
Spare Pool	Name	Туре	Secured C	apacity E	BlockSize	SectorSiz	e OS Name		Status	
Logical Device	RAID_0_0	RAID 0	Yes 1	.00 TB	512k	512B	HPT DISK	0_4	Norma	Maintenance
Rescan	Device_1_E1	_2 Hard Disl		Array	/ Infor	mation		0_1	Legacy	Maintenance
Beeper Mute	Device_1_E1	_4 Hard Disl		000		Delete		0_3	Legacy	Maintenance

- 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.

Controller 1		Р	hysical Devices Inform	nation	
Enclosure 1	Devi	cc 1 E1 1 Model	Samsung SSD 980 PRO 1TB	Capacity	1.00 TB
Devices		Revision	5B2QGXA7	PCIe Width	x4
Rescan		Location Max Free Status	1/E1/1 1.00 TB Normal	PCIe Speed	Gen 4
		Serial Num Interface SED Capable	S5GXNG0N905360M NVME Yes	Type SED Type	SSD
		Secured	Yes	Cryptographic Capable	Erase Yes
	bevi	ice 1 E1 2 Model	Secure Inform	nation	1.00 TB
	Devi	ice 1 E1 3 Model	Cryptographic Erase		1.00 TB
	Devi	ice 1 E1 4 Model		Close	е 1.00 ТВ

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**.

Global View	Physical	Logical Setti	ng Event S	HI Help	
Controller 1		P	hysical Devices	Information	
Enclosure 1	Devic	e 1 E1 5 Model	Micron_7400_MTFD	KCB7T6TDZ Capacity 7.	68 TB
Devices	Unplu	g Revision	E1MU23Y5	PCIe Width	x4
Rescan		Location	1/E1/5	PCIe Speed	Gen 4
Rescan		Max Free	0.00 GB		
		Status	Legacy		
		Serial Num	2316423C3572		
		Interface	NVME	Туре	SSD
		SED Capable	No	SED Type	None
		Secured	No	Cryptographic Erase Capable	No

- 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.	
Choose File No file chosen	Submit

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.



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

Controller(1): HighPoi	localhost:740	2 says ed successfully, it will take effect after reboot.
Global View		ок
Controller 1		Controller Information
Enclosure 1	Model Name:	HighPoint NVMe RAID Controller
Devices	Vendor:	HighPoint Technologies, Inc.

6.3.5. Secure Setting

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

	Secure Setting
Password:	
Confirm:	
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.

			Secure Setting
Password:	•••••		
Confirm:	•••••	Ŷ	
Enable Security			



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.

		Secure Setting
Disable Security		
Old Password:	******	
New Password:	******	
Confirm:	•••••••	
Change Security	1	

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.

	Secure Setting
Disable Security	
Old Password:	
New Password:	
Confirm:	
Change Security	

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.

Create Array		Logical De	vice Informatio	on	
Spare Pool	Name	Type Secured Capacity	BlockSize SectorSize	OS Name	Status
Logical Device	Device_1_	E1_1 Hard Disk No 960.19 GE		HPT DISK 0_2	Legacy Maintenance
	Davies 1	E1 2 Hard Disk No 960.19 GB		UDT DICK 0 2	Legacy Maintenance
Rescan	Device_1_	E1_2 Hard Disk No 960.19 GE		HPT DISK U_3	Legacy <u>Maintenance</u>
	Device_1_	E1_2 Hard Disk No 960.19 GE		HPT DISK 0_3	Legacy <u>Maintenance</u>
	Bevice_1_	-	evice Informati	-	Legacy <u>Maintenanc</u>
	Location	-		-	Max Free
Rescan Beeper Mute		- Physical De	evice Informati	on	

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	t SHI	Help		
Create Array			Log	ical De	vice Inform	nation		
Spare Pool	Name	Туре	Secured	Capacity	BlockSize Secto	orSize OS	Name	Status
Logical Device	Device_	1_E1_1 Hard Dis	c No	960.19 GE		HP	DISK 0_2	Legacy Maintenance
Rescan	Device_	1_E1_2 Hard Dis	c No	960.19 GE		HP	T 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.

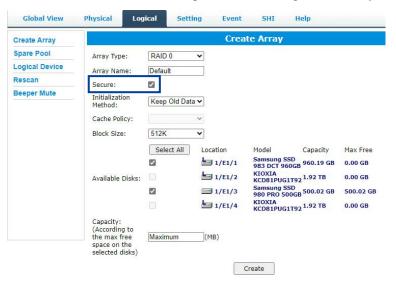
- Method 1: Enabling Disk Security for disks with the Legacy status
- 1. Click the Logical tab and check the Logical Device section of the page.
- 2. Click the Maintenance option displayed on the right-hand side of each disk.
- 3. Click Secure to enable Disk Security.

Create Array	7	Logical Device Informa	tion
Spare Pool	Name Type	Secured Capacity BlockSize SectorS	ze OS Name Status
Logical Device	Device_1_E1_1 Hard Disk	No 960.19 GB	HPT DISK 0_0 Legacy Maintenand
Rescan	Device_1_E1_2 Hard Disk	No 1.92 TB	HPT DISK 0_1 Legacy Maintenand
Beeper Mute	Device_1_E1_3 Hard Disk	No 500.10 GB	HPT DISK 0_2 Legacy Maintenand
	Device_1_E1_4 Hard Disk	Legacy Informatio	n K 0_3 Legacy <u>Maintenan</u>
		Device_1_E1_3	Init Secure
	Location Model		Close pacity Max Free
	1/E1/1 Samsung SSI		0.19 GB 0.00 GB

4. After Disk Security has been enabled.

Create Array			Log	jical De	vice Informatio	on		
Spare Pool	Name	Type	Secureo	l Capacity	BlockSize SectorSize	OS Name	Status	
Logical Device	Device_1_	E1_1 Hard Di	sk No	960.19 GE	3	HPT DISK 0_0	Legacy	Maintenance
Rescan	Device_1_	E1_2 Hard Di	sk No	1.92 TB		HPT DISK 0_1	Legacy	Maintenance
Beeper Mute	Device_1_	E1_3 Hard Di	sk Yes	500.10 GE	3	HPT DISK 0_2	Legacy	Maintenance
	Device 1	E1 4 Hard Di	sk No	1.92 TB		HPT DISK 0 3	Legacy	Maintenance

- 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 Statu	s & Maintenance Options
-------------------------------	-------------------------

Logical Device Status	Maintenance Options
Legacy Status	Disks with the Legacy status are healthy and functioning correctly.
Legacy Information	Your optional options in Maintenance are:
Device_1_E1_4 Secure Close	- 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.
Normal Status	Arrays with the Normal status are healthy and functioning correctly.
Array Information	Your optional options in Maintenance are:
RAID_1_0 Unplug Device_1_E1_3 Verify Device_1_E1_4	- Delete – Delete the selected RAID array.
Rename Close	- 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.
Critical Status	Arrays in the Critical status can be accessed and utilized but are no longer fault-tolerant. A
Array Information	Critical array should be rebuilt as soon as possible to restore redundancy.
Device_1_E1_3 Unplug Device_1_E1_4 Add Disk	Your optional options in Maintenance are:
Close	- 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)
	Reinserting the same disk should trigger the rebuilding status since data on the disk would
	be recognized.
	If you insert a new disk, clicking Add Disk will allow you to select and add it to the array.
Disabled Status	An array with the Disabled status means that the RAID level does not have enough disks to
Array Information	function.
Device_1_E1_1 Device_1_E1_2 Offline Disk	Your optional option in Maintenance is:
Offline Disk Offline Disk Close	- 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.

Create Array		Logical Dev	vice Informatio	n	
Spare Pool	Name	CHICK AND	BlockSize SectorSize	OS Name	Status
Logical Device	Device_1_E	E1_1 Hard Disk No 960.19 GB	0	HPT DISK 0_2	Legacy <u>Maintenan</u>
Rescan	Device_1_E	1_2 Hard Disk No 960.19 GB		HPT DISK 0_3	Legacy Maintenan
Rescan					10 The 10 Party 10
		Physical De	vice Informatio	on	
	Location	Physical De Model	vice Information Secured	Capacity	Max Free
Beeper Mute	Location				Max Free 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.



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.
	- 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="">)</array></level>
Secure	Allows you to use the RAID array's SED capabilities.
	Only AIC that supports the SafeStorage Encryption feature will have this option.
Initialization	Displays the RAID array initialization setting. Default Initialization displays the following options:
Method	- 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

	initialization process, but it will delete all data. (Recommended)
	- 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
	accessible during this time, but the initialization process will take much longer to complete.
	(Not Recommended)
	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.
Block Size	It allows you to adjust the block size to fit your disk usage, thus improving performance.
	- 128K
	- 256K
	- 512K (Default)
	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.
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.
L	

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

Create Array	Create Array								
Spare Pool	Array Type:	RAID 0	~						
Logical Device	Array Name:	Default							
Rescan	Secure:								
Beeper Mute	Initialization Method: Cache Policy:	Keep Old Data	•						
	Block Size:	512K	~						
		Select All	Location 1/E1/1 1/E1/2	Model KIOXIA KCD81PUG1T92 KIOXIA		Max Fre 0.00 GB 0.00 GB			
	Available Disks:		1/E1/2	KCD81PUG1T92 Samsung SSD 983 DCT 960GB		0.00 GB			
			1/E1/4	Samsung SSD 980 PRO 500GE	500.10 GB	0.00 GB			
	Capacity: (According to the max free space on the selected disks)	Maximum	(MB)						

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.

Create Array	Logical Device Information								
Spare Pool Logical Device	Name	Type Secu RAID 0 No	ured Capacity 2.00 TB	BlockSize 512k	SectorSize 512B	OS Name HPT DISK O	Status	al <u>Maintenance</u>	
Rescan			Arra	y Infor	nation				
Beeper Mute	Location 1/E1/1 1/E1/2 1/E1/2 1/E1/3 1/E1/4	Model KIOXIA KIOXIA Samsur Samsur	RAID_0_0 Device_1 Device_1 Device_1 Device_1 Device_1	L_E1_2	elete nplug ename	1.9 1.9 960	acity 2 TB 2 TB .12 GB .02 GB	Max Free 1.42 TB 1.42 TB 460.09 GB 0.00 GB	

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.

Global View	Physical I	ogical	Setting	Event	SHI	Help			
Create Array	Logical Device Information								
Spare Pool	Name		Secured Capacity	BlockSize	SectorSize	OS Name	Status		
Logical Device	RAID_0_0	RAID 0	No 1.50 TB	512k	512B	HPT DISK 0_3	Normal	Maintenanc	
Rescan			Агга	y Inform	nation				
Beeper Mute			RAID_0_0	D	elete				
	Location	Model	- Device_	1_E1_1 U	nplug	Capa	city	Max Free	
	= 1/E1/1	Samsu	Device_	1_E1_2		500.0	2 GB	0.00 GB	
	= 1/E1/2	Micron	Le Device_	1_E1_3 R	ename	3.84	тв	3.34 TB	
	= 1/E1/3	Samsu				Close 960.1	2 GB	460.09 GB	
	= 1/E1/4	INTEL S				375.0	8 GB	0.00 GB	

- 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**.

Global View	Physical	Logical	Set	ting	Event	SHI	Help		
Create Array	Logical Device Information								
Spare Pool	Name	Туре	Secured	Capacity	BlockSize	SectorSize	OS Name	Status	
Logical Device	RAID_0_0	RAID 0	No	1.50 TB	512k	512B	HPT DISK 0_4	Normal	Maintenance

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.

Create Array	Logical Device Information						
Spare Pool	Name			BlockSize SectorSiz	Second Second	Status 3 Norma	Maintenance
Rescan	Device_1_E	1_2 Hard Disk	Array	/ Information	< 0_	1 Legacy	Maintenanc
Beeper Mute	Location 1/E1/1 1/E1/2	Model Samsung SSD Micron_9300_	RAID_1_0		acity .12	GB 4	lax Free 60.09 GB .00 GB
	1/E1/3	Samsung SSD			Close .02	GB 0	.00 GB

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

Global View	Physical L	ogical	Set	tting Even	t SHI	Help		
Create Array				Logical De	vice Infor	matio	n	
Spare Pool	Name	Туре	Secu	red Capacity Bloc	kSize SectorSiz	e OS	Status	
Logical Device						Hume	-	
Rescan	RAID_1_0	RAID	No	500.02	512B	HPT	Rebuilding 4%	Maintenance
Beeper Mute	•	1		GB	5120	0_3	remaining time:00:07:17	. and change

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.

and all and the state of the			-	
Create Array			Spare Pool	
Spare Pool	Remove S	pare		
ogical Device			Available Disks	
Rescan		Device_1_E1_1	Micron_9300_MTFDHAL3T8TDP	3.84 TB
Beeper Mute		Device_1_E1_2	KCM61RUL960G	960.12 GB
		Device 1 E1 3	Samsung SSD 980 PRO 500GB	500.10 GB

- 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.



1 disk(s) will be added to spare pool. Do you want to continue?

- 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.**

Create Array			Spare Pool	
Spare Pool	0 🔛	Device_1_E1_3	Samsung SSD 980 PRO 500GB	500.02 GB
Logical Device	Remove \$	Spare		
Rescan			Available Disks	
Beeper Mute	0 🚍	Device_1_E1_1	Micron_9300_MTFDHAL3T8TDP	3.84 TB
		Device_1_E1_2	KCM61RUL960G	960.12 GB
	Add Spar	_	KCM61RUL960G	960.12 G

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.

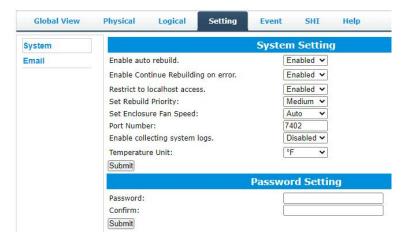
Physical	Logical	Setting	Event	SHI	Logout	Help	
			Spar	e Pool			
🛛 🔛	Device_1_E1_3	Sa	msung SSD 9	80 PRO 50	OGB		500.02 GB
				Spar	Spare Pool	Spare Pool	Spare Pool

- 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:

System		System Setting			
Email	Enable auto rebuild.	Enabled 🗸			
	Enable Continue Rebuilding on error.	Enabled 🗸			
	Restrict to localhost access.	Disabled ~			
	Set Rebuild Priority:	Medium v			
	Port Number:	7402			
	Submit				
	Password Setting				
	Password:				
	Confirm:				
	Submit				

• 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 V
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 ▼
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	(default: Enabled)			
on error	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:			
	- 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			
	You can adjust the audible alarm setting here.			
	Warning: Disabled audible alarm is permanently disabling the beeper, so			
	please proceed with caution!			
Restrict to localhost access	(default: Enabled)			

SSD7000 Software Guide				
	Remote access to the AIC will be restricted when enabled; other users in your network			
	cannot log in to the WebGUI remotely.			
	It is used as follows:			
	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	(default: Medium)			
	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]			
Set Enclosure Fan Speed	(default: Auto)			
	You can adjust the speed of the fan. There are 5 levels [Auto, Off, Low, Medium, High]			
Port Number	(default: 7402)			
	You may change it to any open port. (only for Windows)			
Enable collecting system logs	(default: Disabled)			
	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.			
	This setting is only supported by the Windows HighPoint RAID Management.			
	It is used as follows:			
	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	(default: °F)			
	The default temperature unit is Fahrenheit, and you can change it to Celsius.			
	This setting is only supported by the Windows HighPoint RAID Management.			
۰	·			

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:	
Submit	14

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.

System		S	MTP Setting		
Email	Enable Event Notification Server Address (name or IP): Mail From (E-mail address): Login Name: Password: SMTP Port: Support SSL:		25 Change Setting Recipients		
	E-mail	Name	Event Level		
	Add Recipient				
	E-mail: Name: Event Level: Add Test		Information Uarning Erro		

6.5.3.1.Add an Email Server

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

	SMTP Setting
Enable Event Notification	
Server Address (name or IP):	
Mail From (E-mail address):	
Login Name:	
Password:	
SMTP Port:	25
Support SSL:	
	Change 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)

Support SSL	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.

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: <u>https://accounts.google.com/Login</u>

G	
Sign in Use your Google Account	Enall or phone Forgot email?
	Not your computer? Use a private browsing window to sign in. Learn more about using Guest mode
	Create account Next
English (United States) -	Help Privacy Terms

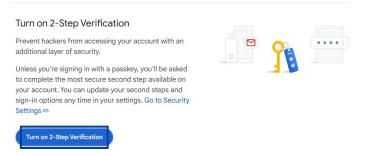
2) Click the Security and search for the 2-Step Verification.

	Go	ogle Account	٩	2-Step Verification
			Google	e Account Results
	٢	Home	F	2-Step Verification phones Security
	1	Personal info	E	2-Step Verification Security
_	•	Data & privacy		enter Articles
	₿	Security	E	Turn on 2-Step Verification
	ත්	People & sharing	E	Fix common issues with 2-Step Verification
	⊟	Payments & subscriptic	E	Turn off 2-Step Verification
	i	About	E	Protect your business with 2-Step Verification

3) Click the Turn on 2-Step Verification and follow Gmail's prompts to complete the

operation.

← 2-Step Verification



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

Go	ogle Account	٩	App passwords			
		Google	Account Results			
٢	Home	E	App passwords Security			
Ĩ	Personal info	E	Web & App Activity Data & privacy			
۲	Data & privacy		Help Center Articles			
₿	Security	E	Sign in with app passwords			
De	People & sharing	E	Use or fix App password			
	Payments & subscriptio	=	Turn off 2-Step Verification			
í	About	E	Save, manage & protect your passwords			

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

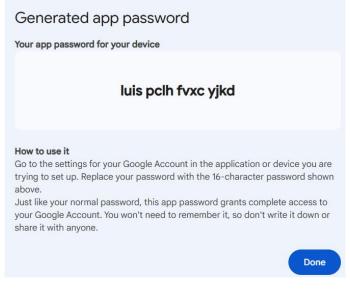
App passwords

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

op name				
ighPoint RA	D Managem	nent		

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.

	SMTP Setting
Enable Event Notification	
Server Address (name or IP):	smtp.gmail.com
Mail From (E-mail address):	@gmail.com
Login Name:)@gmail.com
Password:	•••••
SMTP Port:	465
Support SSL:	
	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: Add Test	Information Warning Error

The following table enumerates the Add Recipient.

Table 13: Add Recipient Options

Add Recipient Option	Description
E-mail	Enter the email address of the recipient.
	If you want to receive notification mail using a Webmail account, you may need to modify the mailbox's permissions.
Name	Enter the name of the recipient.
Event Level	Check which type(s) of events will trigger an email in the respective Event Level check boxes.
	- Inf (Information)
	- War (Warning)
	- Err (Error)
Add/ Test	(Optional)
	- Click Add to add the recipient.
	The added recipient will be displayed under Recipients.
	The email will send your recipients the output recorded in the event log.
	- 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.

	Add Recipi	ent	
E-mail:	hptu@	com	
Name:	hpt		
Event Level: Add Test	⊡Informa	ition 🖾 Warning 🛛	Erro

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

Add Recipient	-
Mail has been sent successfully.	Erro
Close	

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.



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.

	Event View (1)	
All 🔾 🜉 Info 🤇	🔾 🔥 Warning 🛛 🚫 Error	DownloadNex
Date Time	Description RAID 0 Array 'RAID_0_0' has been created successfully (I Disk 2:xXx5802XH84T00 K10XLA, J/E1/2; Disk 3:H+P-EM28 4:XXx5602XH84T00 K10XLA, J/E1/2; Disk 3:H+P-EM280 1/E1/6; Disk 7:Seagate FireCuda 530 ZP1000GM30013, 1/E1/8; Disk 7:H=PEM2802T0GMTCB58R-E264, J/E1/9; C 1/E1/10; Disk 1:Sabrert Rocket 4.0 1TB, J/E1/11; Disk 13:H+P=M2802T0GMTCB58R-E264, J/E1/12; Disk 14:Sa Disk 15:Samsung SSD 970 PR0 S1268, J/E1/15; Disk 14:	0270GMTCB58R-E264, 1/E1/3; Disk SSD3, 1/E1/5; Disk 6:CT10007700SSD3, /[f1/7; Disk 8:WDC WDS24062G0C-00AJM0, visk 10:HP-EM2802T0GMTCB58R-E264, 12:WD Red SN700 1000GB, 1/E1/12; Disk msung SSD 970 EVO Plus 500GB, 1/E1/14;

6.6.1. View the Event Log

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

Event View (1)								
🖲 🜉 All 🛛 🜉 Info	🔿 🔥 Warning 💦 🚫 😵 Error	Download Nex						
Date Time	Description RAID 0 Array 'RAID_0_0'has been created successfully Disk 2:KXG8027N47T05 KIOXIA, J/EJ/2; Disk 3:H0-EM4 4:KXG6027N41702 TOSHIBA, J/EJ/47 Disk 5:CT200177 J/EJ/6; Disk 7:Seagate FireCuda 530 ZP1000GM30013 J/EJ/8; Disk 7:Seagate FireCuda 530 ZP1000GM30013 J/EJ/8; Disk 1:Sabert Rocket 4.0 1TB, J/EJ/13; Disk 13:H0-EM2802T0GMTC358R-2264, J/EJ/13; Disk 1:43 Disk 15:Samsung SSD 370 PK0 51256, J/EJ/15; Disk	802T0GMTCB58R-E264, 1/E1/3; Disk 00SSD3, 1/E1/5; Disk 6:CT1000T700SSD3, 1/E1/7; Disk 6:CT1000T700SSD3, Disk 10:HP-EM2802T0GMTCB58R-E264, k 12:WD Red SN700 1000GB, 1/E1/12; Disk amsung SSD 970 EVO Plus 500GB, 1/E1/14;						
2024/1/31 0:24:53	Device 'Device_1_E1_16' (1/E1/16) has been initialized							

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.

Global View	hysical Logical Setting Event SHI Help	
	Event View (1)	
🛛 🜉 All 🛛 🜉 Info	O 🔥 Warning 🛛 😵 Error Downloa	ad I lex
Date Time	Description RAID 0 Array 'RAID_0_0' has been created successfully (Disk 1:Samsung SSD 980 PR0 1TB, I/EL Disk 2:AXX680Z184709 KIOXKA, J/EL/2; Disk 3:HP-EH2802T0GHTCE584-RE264, I/EL/3; Disk 4:XX660Z1NV102 TOSHIBA, J/EL/3; Disk 5:CT2000T7005SD3, J/EL/5; Disk 6:CT1000T7005SD3 J/EL/6; Disk 7:Seagate fireCuda 530 ZP100GH30013, J/EL/7; Disk 8:WDC VMDS2402G6C-004 J/EL/8; Disk 9:HP-EH2802T0GHTCE588-E264, J/EL/9; Disk 10:HP-EH2802T0GHTCE588-E264, J/EL/10; Disk 1:Saheret Rocket 4.0 1TB, J/EL/11; Disk 12:WD Red 8/T070 100065, J/EL/12; Disk 15:Samsung SSD 970 PR0 51268, J/EL/15; Disk 1:HS202T0GHTCE588-E264, J/EL/12; Disk 15:Samsung SSD 970 PR0 51268, J/EL/15; Disk 1:HS202T0GHTCE588-E264, J/EL/12; Disk 1:Saheret Rocho 51268, J/EL/12; Disk 1:HS202T0GHTCE588-E264, J/EL/12; Disk 1:Saheret Rocho 51268, J/EL/12; Disk 1:HS202T0GHTCE588-E264, J/EL/12; Disk 1:Saheret Rocho 51268, J/EL/12; Disk 1:HS202T0GHTCE588-E264,	3, AJMO, IISK 14;
2024/1/31 0:24:53	Device 'Device_1_E1_16' (1/E1/16) has been initialized.	

Open the downloaded event log.

8 e	eventlog_20240614_0	52225 ×	< +		-	0	×
ile I	Edit View						13
A	1	I	06/12/24 03:31:44	Plugging device detected.('KCM61RUL960G-20M0A011TMWR' at Controller1-Enclosure1-Device8)			
A	1	I	06/12/24 03:31:45	Plugging device detected.('Micron_9300_MTFDHAL3T8TDP-191621F1E94B' at Controller1-Enclosure1-Device7)			
4	1	I	06/12/24 06:00:49	Plugging device detected.('KCM61RUL960G-20M0A011TMWR' at Controller1-Enclosure1-Device8)			
4	1	I	06/12/24 06:00:49	Plugging device detected.('Micron_9300_MTFDHAL3T8TDP-191621F1E94B' at Controller1-Enclosure1-Device7)			
4	1	E	06/12/24 07:27:20	Disk 'KCM61RUL960G-20M0A011TMWR' at Controller1-Enclosure1-Device8 failed.			
4	1	I	06/12/24 07:27:23	Array 'RAID0 01041113' status changes from 'Normal' to 'Disabled'.			
	1	I	06/12/24 07:28:15	Plugging device detected.('KCM61RUL960G-20M0A011TMWR' at Controller1-Enclosure1-Device8)			
4	1	I	06/12/24 07:28:17	Array 'RAID0_01041113' status changes from 'Disabled' to 'Normal'.			
	1	I	06/12/24 07:30:06	Array 'RAID0 01041113' has been deleted successfully.			
	1	I	06/12/24 07:31:39	Plugging device detected.('KCM61RUL9606-20M0A011TMWR' at Controller1-Enclosure1-Device8)			
	1	I	06/12/24 07:31:40	Plugging device detected. ('Micron_9300_MTFDHAL3T8TDP-191621F1E94B' at Controller1-Enclosure1-Device7)			
	1	I	06/13/24 00:38:42	Plugging device detected. ('KCM61RUL960G-20M0A011TMWR' at Controller1-Enclosure1-Device8)			
	1	I	06/13/24 00:38:42	Plugging device detected. ('Micron_9300_MTFDHAL3T8TDP-191621F1E94B' at Controller1-Enclosure1-Device7)			
	1	I	06/13/24 08:48:44	RAID0 Array 'RAID0 010665ED' has been created successfully (Disk 1:Micron 9300 MTFDHAL3T8TDP, 1/E1/7	Di	sk	
:KC	M61RUL960	G, 1/E1/	8).				
A	1	I	06/13/24 08:52:44	Plugging device detected.('KCM61RUL960G-20M0A011TMWR' at Controller1-Enclosure1-Device8)			
	1	I	06/13/24 08:52:44	Plugging device detected. ('Micron 9300 MTFDHAL3T8TDP-191621F1E94B' at Controller1-Enclosure1-Device7)			
4	1	I	06/13/24 09:04:17	Plugging device detected.('KCM61RUL960G-20M0A011TMWR' at Controller1-Enclosure1-Device8)			
Α.							
r -	Т	T	T	<u>Т</u>			
·							
3	G	0	0				
D	(2)	(3)	(4)	(5)			
~	9		9				

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	Includes the followings:					
		• 0 – Indicates that the event was not sent by Email.					
		• 1 – Indicates that the event has been sent by Email or the event log can					
		not be sent because the mail is not set up recipients.					
		• 2 – Indicates that the mailbox recipient has been set up, but the event log					
		is in pending status, waiting for the mail to be sent.					
3	Event Levels	Includes the following event levels:					
		• I – Information					
		• W – Warning					
		• E – Error					
4	Event Time	Shows the exact time of the event.					

SSD7000 Software Guide								
(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
		Includes general administrative tasks:
1	Information	• Create/delete arrays
		Configuring spares
		Rebuilding arrays
		Configuring eventnotifications
		• Configuring maintenance
		Alerts issued by the HostAdapter:
	Warning	• High temperatures
		• Sector errors
		Communication errors
		Verification errors
		Hardware related problems:
8	Error	• 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.

						Sche
		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 Temperat	ture Three	shold		

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.

	Help	SHI	Event	Logical Setting	Physical	Global View
Schee						
	2	r(SHI)	Inspecto	Storage Health		
S.M.A.R.T	Total Bytes Written	°C	RAID	Device Serial Number	Location#	Controller ID
Detail	36.18 TB	38	None	39US1018TR0Q	E1_1	1
Detail	11.56 TB	36	None	39US100MTR00	E1 2	1

- 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 Hea	Ith Inspector	(SHI)				
Controller ID	Location#	Device Serial Number	RAID	۰F	Total Bytes Written	S.M.A.R.T		
	E1_1	S48CNW0K400031X	RAID_1_0	91	192.85 TB	Detai		
	E1_2	XDR0A03D0UU1	RAID_0_0	95	14.80 TB	Detai		
	E1_3	S5GYNG0R206284E	RAID_1_0	86	109.04 TB	Detai		
	E1_4	XDR0A0370UU1	RAID_0_0	98	15.11 TB	Detai		
Device Name		Device_1_E1_4						
Model Number		KIOXIA KCD81PU	G1T92					
Temperature		98°F						
Warning Com	osite Temperatur	e Threshold 170°F						
-		Threshold 185°F						
		NVME S.M	.A.R.T Attribu	ites				
Name		Sector and the sector sector			Value			
Critical Warnin					0×0			
Composite Temperature (C)					37			
Avaliable Spare					100%			
Avaliable Span					8%			
Precentage Us				0%				
Data Units Rea				0x7af41cca				
Data Units Wri				0x1eef705				
Host Read Con				0x496eb2c6				
Host Write Cor				0x1a2c25ca				
Controller Bus	y Time				0xa14			
Power Cycles				Oxab				
Power On Hou					0x7e			
Unsafe Shutdo					0x22			
	a Integrity Errors				0×0			
	or Information Lo	g Entries			0x1			
Warning Temp					0x699			
	site Temperature	Time			0×0			
Temperature S	ensor 1 (C)				0			
Temperature S					0			
Temperature S	ensor 3 (C)				0			
Temperature S	ensor 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 : 149
or Set

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

Global View	Physical	Logical Setting	Event	SHI	Help	
						Sched
		Storage Healt	h Inspecte	or(SHI)	
Controller ID	Location#	Device Serial Number	RAID	٩F	Total Bytes Written	S.M.A.R.T
1	E1_1	S463NF0K409595F	None	150	1023.91 TB	Detail
1	E1_2	S5JYNS0N602754T	None	111	75.45 TB	Detail
		HDD Temper	rature Thre	eshold		

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.

Global Vi	ew Phys	ical Logical	Setting	Event	SHI	b	Help	
					(0)17			Schedule
Controller ID	Location#	Stora Device Serial Numbe		h Inspecto	or(SHI) °F	Total Bytes Written	S.M.A.R.T
1	E1_3	S5GYNG0R206308X		ID ID0_00A84D1	7	89	116.72 TB	S.M.A.K.I Detail
1	E1_7	S5GYNG0R205478M	RA	ID0_00A84D1	7	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.

Global View Physical Logical	Setting	Event	SHI	Help
	Tasl	ks List		
Name Description DefaultTask Check all disks every 1 minute(s). Delete				

When the operating temperature of the disk exceeds the warning temperature threshold, or when the critical warning in the disk's smart message is not 0x0, a Warning event will appear in the **Event** view.

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

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:	1	Minute(s) V	
Submit			

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



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.

			New Verify	Task			
) Fask Name	RAID_1_0 :						
	Occurs one time on	2024 - 5	-[21] at [2	:0:0			
chedule:	Occurs every	1 Day(s)	✓ on Sunday	√ 1 at 2	:0	:0	
		Start date: 2024	- 5 - 21	OEnd date:	2024	- 5	- 21
Submit				No end da	te		

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
DefaultTa	sk Check all disks every 1 minute(s).
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.

	Tasks List	
Name Description test Verify array "RAID 1 0" every day at 23:0		

6.8.Help

Help	
Online Help	
Diagnostic	

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.

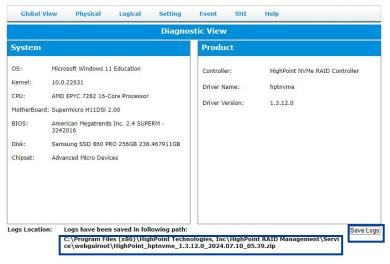
Diagnostic View				
System		Product		
OS: Kernel: CPU: MotherBoan BIOS: Disk: Chipset:	Microsoft Windows 11 Education 10.0.22631 AMD EPYC 7282 16-Core Processor rd: Supermicro H11DSi 2.00 American Megatrends Inc. 2.4 SUPERM - 3242016 Samsung SSD 860 PRO 256GB 238.467911GB Advanced Micro Devices	Controller: Driver Name: Driver Version:	HighPoint NVMe RAID Controller hptnvme 1.3.12.0	
ogs Locati	ion: Logs have not been save	ed	Save	

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	0	Туре	Compressed size	Password	Size		Ratio
🚞 log		File folder					
🚞 otc		File folder					
🚞 xsl		File folder					
C Index		Microsoft Edge HTML Do	1 KE	3 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 {drivername}.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	
	hpt_temperature.csv	conditions.	
	hpt_xxx.txt	AIC log information, including creation/deletion of RAID and exception	

SSD7000	Software	Guide
---------	----------	-------

		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	 On the HTML webpage, record the screenshot information for each page of this WebGUI. 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	 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

	Diagnostic View					
ystem	Product					
DS: Ubuntu 24.04 LTS x86_64 Gernel: 6.8.0-31-generic IPU: AMD EPYC 7282 16-Core Processor MotherBoard: Supermicro H11DSi 2.00 BIOS: American Megatrends Inc. 2.4 12/28/2021 5.14 Disk: Samsung SSD 860 Chipset: Advanced Micro Devices, Inc. [AMD] Starship/ Matisse Root Complex	Controller: Driver Name: Driver Version:	HighPoint NVMe RAID Controller hptnvme v1.6.17.0				

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

()	G Home / Downloads / HighPoint_hptnvme_v1.8.0.0_2024.06.04	:	ାହ	88 ~ -
Name 🔿			Size	ModiFied
Crash	1		0 items	Today 9:10
tog 🚺			9 items	Today 9:10
xsl			155 item	s Today 9:10
Index	c.xml		826 byte	s Today 9:10

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
		• 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 t 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	• 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

System			
		Product	
DS: Kernel: CPU: MotherBoard: f2: Disk: Disk: Chunderbolt: Secure Boot: SiP:	macOS 14.5 23F79 xnu-10063.121.3~5 Apple M2 Ultra Mac14,8 / APPLE SSD AP1024Z / Reduced Security Enabled	Controller: Driver Name: Driver Version:	HighPoint NVMe RAID Controller HighPointNVMe 1.1.32

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	HTML webpage, record the screenshot information of each page of	
	page	this WebGUI	
		• 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	It contains components that allow local html files to be opened.	
	page		

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.



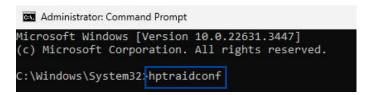
Warning: Using create/ delete commands may destroy data stored in the disks, and this lost data can never be recovered.

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

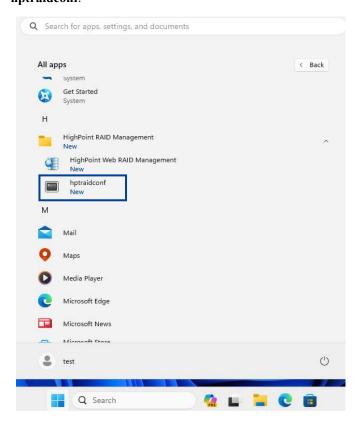
7.1.Start the CLI

For Windows Users

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

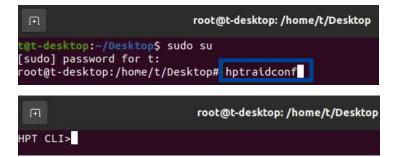


• Method 2: Click Start to find the HighPoint RAID Management folder, and click on hptraidconf.



For Linux Users

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



7.2. Query Commands



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.

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.	
query		{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.	
query		{arrays_id}	This command presents information of each disk of a specified array.	

Table 19: Properties for query Command

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 Control

- **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



- 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

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 MTFDHAL3T8TDF
L/E1/3	No	500.03	0	RAID	NORMAL	Samsung SSD 980 PRO 500GE
L/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):
 - LEAGACY: 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 > quer	y devices 1/E1/6				
	KXG60ZNV1T	2 TOSHIBA			
Serial Number:					
Firmware Versi	on: AGGA4102				
Capacity(GB):	1024.21	TotalFree(GB)	: 0		
Status:			LEGACY		
SED Capable:	No	SED Type:	None		
Secured:	No	Cryptographic	Erase Capable:	No	
PCIe Width:	x4	PCIe Speed:			
Temperature (F):		96		
Warning Compos	ite Temperature	Threshold (F):	172		
Critical Composite Temperatu					
		S.M.A.R.T Attribu	 tes		
S.M.A.R.T Stat	us OK.	Still Alter Activities			
Name		Value			
Critical Warni	 ng	: 0x0			
Composite Temp		: 36			
Available Spar		: 100%			
Available Spare Threshold		: 10%			
Percentage Used		: 90%			
Data Units Rea		: 0x76d			
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 CL: ID	I > query Secured	arrays Capacity(GB)	Туре	Status	Block	Sector	Cache	Name
1	No	7681.01	RAIDØ	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

D:			Name		RAID10	0		
ype:		RAID10	Stat	us:	NORMAL			
apac	ity(GB):	1919.85	Bloc	kSize:	512k			
ecto	rSize:	512B	Cach	ePolicy:	NONE			
rogr	ess:		Secu	re:	No			
	Secured	Capacity(GB)	Туре	Status	Block	Sector	Cache	Name
-1	No	239.98	RAID1	NORMAL		5128	NONE	- [RAID10 0]
-2	No	239.98	RAID1	NORMAL		512B	NONE	[RAID10 0]
	No	239.98	RAID1	NORMAL		512B	NONE	[RAID10 0]
-4	No	239.98	RAID1	NORMAL		512B	NONE	[RAID10_0]
	No	239.98	RAID1	NORMAL		512B	NONE	[RAID10 0]
-6	No	239.98	RAID1	NORMAL		512B	NONE	[RAID10 0]
	No	239.98	RAID1	NORMAL		512B	NONE	[RAID10_0]
-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



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): Prope	rties for	init Co	mmand
----------	----------	-----------	---------	-------

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
	{start stop}	start/ stop	redundant RAID array (RAID1).

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

	Secured	Capacity	MaxFree	Flag	Status	ModelNumber
/E1/1	No	960.13	460.10	RAID	NORMAL	Samsung SSD 983 DCT 960GE
/E1/2	No	3840.76	0	SINGLE	LEGACY	Micron_9300_MTFDHAL3T8TDF
/E1/3	No	500.03	0	RAID	NORMAL	Samsung SSD 980 PRO 500GE
/E1/4	Yes(locked)	375.08	0	SINGLE	NORMAL	INTEL SSDPE21K375GA
nit de	> init 1/E1 vice(1/E1/2)	successful	ly!			
nit de		successful ices	ly! MaxFree	Flag	Status	ModelNumber
nit de IPT CLI D	vice(1/E1/2) > query dev Secured	successful ices Capacity	MaxFree			
nit de IPT CLI D /F1/1	vice(1/E1/2) > query dev Secured No	successful ices Capacity 960 13	MaxFree	RATD	NORMAI	Samsung SSD 983 DCT 960GE
nit de IPT CLI	vice(1/E1/2) > query dev Secured	successful ices Capacity	MaxFree		NORMAI	ModelNumber Samsung SSD 983 DCT 96066 Micron 9300 MTFDHAL3T8TD Samsung SSD 980 PRO 50066

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:	
<pre>create {RAID0 RAID1 RAID3 RAID5 RAID6 RAID10 RAID50 JBOD spare} [create-options]</pre>	
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.	
ADT CLT S	

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.

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=1/2,1/3or 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="">)</array></level>
		src	Specifies an existing array to be expanded/migrated. All data on the

Table 21: Properties for create Command

source array will be redistributed online to the target array. If this parameter is omitted, a new array is created. init Specifies array initialization option. - foreground: Zero out all data on the array. The array is not accessible by the operating system until initialization is complet (Not Recommended) - background: Allow instant access to the array. Parity blocks be generated in the background. (Not Recommended)	is			
init Specifies array initialization option. - foreground: Zero out all data on the array. The array is not accessible by the operating system until initialization is comple (Not Recommended) - background: Allow instant access to the array. Parity blocks				
 foreground: Zero out all data on the array. The array is not accessible by the operating system until initialization is comple (Not Recommended) background: Allow instant access to the array. Parity blocks 		parameter is omitted, a new array is created.		
accessible by the operating system until initialization is comple (Not Recommended) - background: Allow instant access to the array. Parity blocks		Specifies array initialization option.	init	
(Not Recommended) - background: Allow instant access to the array. Parity blocks	not	- foreground: Zero out all data on the array. T		
- background: Allow instant access to the array. Parity blocks	ompleted.	accessible by the operating system until initiali		
		(Not Recommended)		
be generated in the background. (Not Recommended)	locks will	- background: Allow instant access to the arr		
		be generated in the background. (Not Recomm		
- keepdata: Setup array information blocks on the drives only.	only. Use	- keepdata: Setup array information blocks on		
this option for array recovery.		this option for array recovery.		
- quickinit: Setup array information blocks and zero out MBR	MBR data	- quickinit: Setup array information blocks an		
on the array.		on the array.		
Important Note: The Foreground and Background Initialization op	on options	Important Note: The Foreground and Background		
will cause NVMe media to result in TBW and performance degrade	egradation.	will cause NVMe media to result in TBW and perfe		
Initialization of a disk sets all data bits to 0, clearing all the data of	lata on the	Initialization of a disk sets all data bits to 0, clearing		
disk. It is important to initialize disks as previous data physically stor	y stored on	disk. It is important to initialize disks as previous dat		
the disk may interfere with new data.		the disk may interfere with new data.		
capacity Specify the capacity of the target array.		Specify the capacity of the target array.	capacity	
capacity=10MB/1000MBor capacity=*		capacity=10MB/1000MBor capacity=*		
* Indicates creation of RAID array using all disk capacities.		* Indicates creation of RAID array using all disk capa		
bs It allows you to adjust the block size to fit your disk usage, which car	ch can	It allows you to adjust the block size to fit your disk to	bs	
result in some performance gain.		result in some performance gain.		
- 128K		- 128K		
- 256K		- 256K		
- 512K (Default)		- 512K (Default)		
In a typical RAID configuration, virtual disk data is striped (or spread	spread	In a typical RAID configuration, virtual disk data is s		
across) the physical disks. A smaller array block size will increase the	ise the	across) the physical disks. A smaller array block size		
likelihood of accessing all physical disks when processing large I/O	I/O	likelihood of accessing all physical disks when proce		
requests. Multiple physical disks working in parallel increase the	e	requests. Multiple physical disks working in parallel		
throughput, meaning better performance.		throughput, meaning better performance.		
sector Specifies the target array's logical sector size in B/KB. This option is	ion is only	Specifies the target array's logical sector size in B/KE	sector	
valid for stripped RAID levels.		valid for stripped RAID levels.		
secure Allows you to use the RAID array's SED capabilities.		Allows you to use the RAID array's SED capabilities	secure	

SSD7000 Software Guide

			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 > c Create arra				capacity=*	init=quick	init	bs=512k		
IPT CLI > q ID Sec		arrays Capacity	y(GB)	Туре	Status	Bloc	k Sector	Cache	Name
1	No	15(20.08	RAIDØ	NORMAL	512	k 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

IPT CLI	> query de	evices				
	Secured	Capacity	MaxFree	Flag	Status	ModelNumber
/E1/1	No	1000.12	1000.12	SINGLE	SPARE	Samsung SSD 980 PRO 1TB
/E1/2	No	4096.73	4096.73	SINGLE	NORMAL	KXG80ZN84T09 KIOXIA
/E1/3	No	2000.31	2000.31	SINGLE	NORMAL	HP-EM2802T0GMTCB58R-E264
/E1/4	No	1024.08	1024.08	SINGLE	NORMAL	KXG60ZNV1T02 TOSHIBA
/E1/5	No	2000.31	2000.31	SINGLE	NORMAL	CT2000T700SSD3
/E1/6	No	1000.12	1000.12	SINGLE	NORMAL	CT1000T7005SD3
/E1/7	No	1000.12	1000.12	SINGLE	NORMAL	Seagate FireCuda 530 ZP1000GM30013
/E1/8	No	239.98	239.98	SINGLE	NORMAL	WDC WD5240G2G0C-00AJM0
/E1/9	No	2000.31	2000.31	SINGLE	NORMAL	HP-EM2802T0GMTCB58R-E264
/E1/10	No	2000.31	2000.31	SINGLE	NORMAL	HP-EM2802T0GMTCB58R-E264
/E1/11	No	1000.12	1000.12	SINGLE	NORMAL	Sabrent Rocket 4.0 1TB
/E1/12	No	1000.12	1000.12	SINGLE	NORMAL	WD Red SN700 1000GB
/E1/13	No	2000.31	2000.31	SINGLE	NORMAL	HP-EM2802T0GMTCB58R-E26P4
/E1/14	No	500.03	500.03	SINGLE	NORMAL	Samsung SSD 970 EVO Plus 500GB
/E1/15	No	512.04	512.04	SINGLE	NORMAL	Samsung SSD 970 PRO 512GB
/E1/16	No	2000.31	2000.31	SINGLE	NORMAL	HP-EM2802T0GMTCB58R-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



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

ID	> query dev Secured	vices Capacity	MaxFree	Flag	Status	ModelNumber
/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-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-00AJM0
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		1000.12	1000.12	SINGLE		Sabrent Rocket 4.0 1TB
1/E1/12		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		Samsung SSD 970 EVO Plus 500GB
1/E1/15		512.04	512.04	SINGLE		Samsung SSD 970 PRO 512GB
1/E1/16	No	2000.31	2000.31	SINGLE	NORMAL	HP-EM2802T0GMTCB58R-E264
HPT CLI ID	> query dev Secured	vices				
	Secureu	Capacity	MaxFree	Flag	Status	ModelNumber
/F1/1		Capacity		ĭ		
/E1/1 1/E1/2	No	Capacity 1000.12	1000.12	SINGLE	NORMAL	Samsung SSD 980 PRO 1TB
1/E1/2	No No	Capacity 1000.12 4096.73	1000.12 4096.73	SINGLE SINGLE	NORMAL NORMAL	Samsung SSD 980 PRO 1TB KXG80ZN84T09 KIOXIA
	No	Capacity 1000.12 4096.73 2000.31	1000.12 4096.73 2000.31	SINGLE	NORMAL NORMAL NORMAL	Samsung SSD 980 PRO 1TB
1/E1/2 1/E1/3 1/E1/4	No No No No	Capacity 1000.12 4096.73 2000.31 1024.08	1000.12 4096.73 2000.31 1024.08	SINGLE SINGLE SINGLE SINGLE	NORMAL NORMAL NORMAL NORMAL	Samsung SSD 980 PRO 1TB KXG80ZN84T09 KIOXIA HP-EM280ZT06MTCBS8R-E264 KXG60ZNV1T02 TOSHIBA
1/E1/2 1/E1/3 1/E1/4 1/E1/5	No No No	Capacity 1000.12 4096.73 2000.31 1024.08 2000.31	1000.12 4096.73 2000.31 1024.08 2000.31	SINGLE SINGLE SINGLE SINGLE SINGLE	NORMAL NORMAL NORMAL NORMAL NORMAL	Samsung SSD 980 PRO 1TB KXG802N84T69 KIOXIA HP-EM2802T0GMTCBS8R-E264
1/E1/2 1/E1/3 1/E1/4	No No No No No	Capacity 1000.12 4096.73 2000.31 1024.08	1000.12 4096.73 2000.31 1024.08	SINGLE SINGLE SINGLE SINGLE	NORMAL NORMAL NORMAL NORMAL NORMAL	Samsung SSD 980 PRO 1TB KXG802N84T09 KIOXIA HP-EM2802T0GMTCG58R-E264 KXG602INV1T02 TOSHIBA CT2000T7095SD3
1/E1/2 1/E1/3 1/E1/4 1/E1/5 1/E1/6	No No No No No No	Capacity 1000.12 4096.73 2000.31 1024.08 2000.31 1000.12	1000.12 4096.73 2000.31 1024.08 2000.31 1000.12	SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE	NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL	Samsung SSD 980 PRO 1T8 KXG802N84T09 KIOXIA HP-EM2802T064TCESSR-E264 KXG602NV1102 TOSHIBA CT2000T7005SD3 CT1000T7005SD3
1/E1/2 1/E1/3 1/E1/4 1/E1/5 1/E1/6 1/E1/7	No No No No No No No	Capacity 1000.12 4096.73 2000.31 1024.08 2000.31 1000.12 1000.12	1000.12 4096.73 2000.31 1024.08 2000.31 1000.12 1000.12	SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE	NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL	Samsung SSD 980 PRO 1TB KXG80ZN8AT09 KIOXIA HP-EM2802T0GMTCG5S8R-E264 KXG60ZNV1102 TOSHIBA CT2000T7005SD3 CT1000T7005SD3 Seagate FireCuda 530 ZP1000GM30013
1/E1/2 1/E1/3 1/E1/4 1/E1/5 1/E1/6 1/E1/7 1/E1/8	No No No No No No No No No	Capacity 1000.12 4096.73 2000.31 1024.08 2000.31 1000.12 1000.12 239.98	1000.12 4096.73 2000.31 1024.08 2000.31 1000.12 1000.12 239.98	SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE	NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL	Samsung SSD 980 PRO 1TB KXG802N84T09 KIOXIA HP-EM2802T0GMTCB58R-E264 KXG602NV1T02 TOSHIBA CT2006T7005SD3 Seagate FireCuda 530 ZP1000GM30013 MDC WDS24062c06C-00AJM0
1/E1/2 1/E1/3 1/E1/4 1/E1/5 1/E1/6 1/E1/7 1/E1/8 1/E1/9	No No No No No No No No No	Capacity 1000.12 4096.73 2000.31 1024.08 2000.31 1000.12 1000.12 239.98 2000.31	1000.12 4096.73 2000.31 1024.08 2000.31 1000.12 1000.12 239.98 2000.31	SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE	NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL	Samsung SSD 980 PR0 1TB KXG802N84T09 KIOXIA HP-EM2802T0GMTCBS8R-E264 KXG602NV1102 TOSHIBA CT2000T7005SD3 CT1000T7005SD3 Seagate FireCuda 530 ZP1000GM30013 WDC WDS2406206C-000JN0 HP-EM2802T06MTCB58R-E264
1/E1/2 1/E1/3 1/E1/4 1/E1/5 1/E1/6 1/E1/7 1/E1/8 1/E1/9 1/E1/10	No No No No No No No No No No	Capacity 1000.12 4096.73 2000.31 1024.08 2000.31 1000.12 1000.12 239.98 2000.31 2000.31	1000.12 4096.73 2000.31 1024.08 2000.31 1000.12 1000.12 239.98 2000.31 2000.31	SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE	NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL	Samsung SSD 980 PRO 1TB KXG802N84T09 KIOXIA HP-EM2802T0GMTCBS8R-E264 KXG602NW1702 TOSHIBA CT2000T7005SD3 CT1000T7005SD3 Seagate FineCuda S30 ZP1000GM30013 WDC WDS240G260C-000JM0 HP-EM2802T0GMTCB58R-E264 HP-EM2802T0GMTCB58R-E264
1/E1/2 1/E1/3 1/E1/4 1/E1/5 1/E1/6 1/E1/7 1/E1/8 1/E1/9 1/E1/10 1/E1/11	No No No No No No No No No No No	Capacity 1000.12 4096.73 2000.31 1024.08 2000.31 1000.12 1000.12 239.98 2000.31 2000.31 1000.12	1000.12 4096.73 2000.31 1024.08 2000.31 1000.12 1000.12 239.98 2000.31 2000.31 1000.12	SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE	NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL	Samsung SSD 980 PR0 1TB KXG6827N84T09 KIOXIA HP-EM280210GMTCBS8R-E264 KXG6027N1702 TOSHIBA CT2000T7005SD3 CT1000T7005SD3 Seagate FireCuda 530 ZP1000GM30013 MDC WD524062C60C-000A7M6 HP-EM2802T0GMTCBS8R-E264 HP-EM2802T0GMTCBS8R-E264 Sabrent Rocket 4.0 ITB
1/E1/2 1/E1/3 1/E1/4 1/E1/5 1/E1/6 1/E1/7 1/E1/8 1/E1/9 1/E1/10 1/E1/11 1/E1/12	No No No No No No No No No No No No	Capacity 1000.12 4096.73 2000.31 1024.08 2000.31 1000.12 239.98 2000.31 2000.31 2000.31 1000.12 1000.12	1000.12 4096.73 2000.31 1024.08 2000.31 1000.12 1000.12 239.98 2000.31 2000.31 1000.12 1000.12	SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE	NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL	Samsung SSD 980 PRO 1TB KXG802N84T09 KTOXIA HP-EM2802T0GMTCG5S8R-E264 KXG602NV1702 TOSHIBA CT2000T7005SD3 Seagate FireCuda S30 ZP1000GM30013 MDC MDS240G200C-000JM0 HP-EM2802T0GMTCB58R-E264 HP-EM2802T0GMTCB58R-E264 Sabrent Rocket 4.0 1TB MD Red SN700 1000G0
1/E1/2 1/E1/3 1/E1/4 1/E1/5 1/E1/6 1/E1/7 1/E1/8 1/E1/9 1/E1/10 1/E1/11 1/E1/12 1/E1/13	No No No No No No No No No No No No No N	Capacity 1000.12 4096.73 2000.31 1024.08 2000.31 1000.12 1000.12 1000.12 239.98 2000.31 2000.31 1000.12 2000.31	1000.12 4096.73 2000.31 1024.08 2000.31 1000.12 1000.12 239.98 2000.31 2000.31 1000.12 1000.12 2000.31	SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE SINGLE	NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL NORMAL	Samsung SSD 990 PRO 1TB KXG802N84T09 KIOXIA HP-EM2802T064TCG588R-E264 KXG602NV102 TOSHIBA CT2000T7005SD3 CT1000T7005SD3 Seagate FireCuda 530 ZP10006M30013 MDC WD524062G60-000A3M0 HP-EM2802T06MTCB58R-E264 Sabrent Rocket 4.0 1TB MD Red SN700 100068 HP-EM2802T06MTCB58R-E264 Sabrent Rocket 4.0 1TB MD Red SN700 100068

7.6. Rebuild Command

	> 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
	{device_id}	The disk hosted by the AIC	critical RAID array and rebuild it.
rebuild	{array_id}	The created RAID array	This command lets you start or stop the rebuilding process on
	{start stop}	start/ stop	the specified array.

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

ID CL.	I > query Secured	Capacity(GB)	Туре	Status	Block	Sector	Cache		Name
1	No	500.03	RAID1	CRITICAL		512B	NONE	RAI	ID_1_6
IPT CL	I > rebuil	ld 1 1/E1/4							
	I > query	arrays 1	Name		RAID 1				
ID:		RAID1	Stat		REBUILD				
Type:	ty(GB):	500.03		kSize:	REBUILD.	LING			
Sector		512B		ePolicy:	NONE				
rogre		1.30%	Secu		No				
inogre:	Secured	Capacity	MaxFree	Flag	Status	ModelN	umbon		
		cupucity							
	No	960.13	460.10	NORMAL	CRITICAL	Samsun	g SSD 98	3 DCT 966	GB
/E1/4			0	NORMAL	RAID			0 PRO 500	

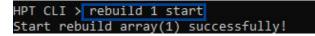
7.6.2. Start Rebuilding the RAID Array

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



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
	{start stop}	start/ stop	specified array.

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

	LI > verify 1 verity array		fully!					
HPT C ID	LI > query ar Secured Ca		Туре	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

	LI > verify 1 verity array(:		ully!					
HPT C ID	LI > query arı Secured Caj		Туре	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.

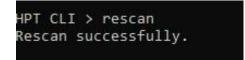
7.8.1. Rescan the Physical Devices

HPT CLI>rescan

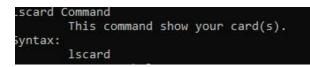
This command rescans all of the physical devices attached to the AIC.

Input example:

HPT CLI> rescan



7.9.Lscard Command



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 Iscard Command

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

7.9.1. Lscard all AICs

HPT CLI>lscard

This command displays the list of multiple AICs.

Input example:

HPT CLI>lscard

HPT CLI > 1	scard	
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.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:
			- 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] 1-Enclosure1-Device5)	Plugging device detected.('Sabrent Rocket 4.0 1TB-03F10707074404014589' at Controller
2 Inf [07/10/2024 05:18:03] e1-Device6)	Plugging device detected.('KXGG02NVIT02 TOSHIBA-694S10NBTVDQ' at Controller1-Enclosur
3 Inf [07/10/2024 05:08:56] DZ, 1/E1/5; Disk 2:Micron_7450_MTF	RAID 1 Arnay 'RAID_1_0' has been created successfully (Disk 1:Micron_7400_MTFDKCB7T6T DKCC7TGTFR, 1/E1/6).
4 Inf [07/10/2024 05:08:41]	Array 'RAID_0_0' has been deleted successfully.
	RAID 0 Array 'RAID_00' has been created successfully (Disk 1:Micron_7400_MTFDKCB7T6T DKCC7T6TFR, 1/E1/6; Disk 3:INTEL SSDPF2KW276T20, 1/E1/7; Disk 4:INTEL SSDPF2KW038T20, 1/E1/
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

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

7.11. Mail Command

HPT CLI Mail Com	
	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}
	<pre>mail recipient test {recipient_name}</pre>
	mail server
	<pre>mail server set {server_address} {port} {ssl} {e d} {from_address} [username] [password]</pre>
	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.	
			- 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}	_address} The mail from address.	
		[username]	The mail username.	

SSD7000 Soft	ware Guide	1
	[password]	The mail password.
	a p s m u t	Use this command to set your mail server value.
	{value}	- 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 recipier	nt add hpt	point.com Inf	
HPT CLI ID Nam	> mail recipier e Mail AG	AND ADDRESS OF ADDRESS		Notify Types
1 hpt	F	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 ID		il recipient Mail Address	Notify Types
1	hpt	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

	CLI > mail Name	recipient Mail Address	Notify Types
1	hpt	yf@highpoint.com	Information
нрт с	CLI > mail	recipient delete hpt	
	CLI > mail Name	recipient 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____@gmail.com____@gmail.com luis

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 server

This command will configure mail server settings.

Input example:

HPT CLI> mail server



7.11.7. Set the Mail Server

HPT CLI>mail server set {a|p|s|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 se	rver set	p 15			
HPT CLI > mail se ServerAddress	rver Port	ssl	Status	Mail From	User Name
smtp.gmail.com	15	1	Enabled	@gmail.com	@gmail.com

7.12. Task Command

Task Co	mmands Set tasks for the server.
Syntax:	
	task
	<pre>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</pre>
	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. Note: When you add a task to rebuild a selected array once, the parameter {day} should be omitted.
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.

k_id} The created task

7.12.1.Create a New Rebuild Task

<u>HPT CLI>task rebuild {array_id} {name=} {once|daily|weekly|monthly={day} interval={interval}</u> 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



7.12.2. Create a New Verify Task

<u>HPT CLI>task verify {array_id} {name=} {once|daily|weekly|monthly}={day} interval={interval}</u> 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

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 > ta	sk			
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
2	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

reated by)
eated by)
reated by)

7.13. Set Command

set Com	mand		
	Set	the system, device or arr	ay's param.
Syntax:			
5	set		
		show the system param	eters
	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	
		set RP=[1-100]	
		set BR=[1-100]	
		set SD=[minutes]	
		set TT=[20-100]	Temperature threshold
		set TU=[C F]	Temperature Unit
		set CL=[y n]	Collect system logs
	or an	set PS	Set Password
	set	{device id} {name= }	
		set tcq=[y n] set T	
		set ncq=[y n] set N	
			rite Cache enable or disable. ead Ahead enable or disable.
			mart enable or disable.
	cot	: {array id} name={name} cp	
	Jer	name Set the array	
		cp Set array's c	

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.

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.

Table 30: Properties for set Commands

	The audible alarm sounds when the following conditions occur:
	- 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
	Warning: Disabled audible alarm is permanently disabling
	the beeper, so please proceed with caution!
BP	Set enable or disable [Beeper].
	When a disk drop triggers the beeper.
RP	Change [Rebuilding Priority]. If an AIC is not specified, this command
	will set the global rebuilding priority.
	[0-12] Lowest
	[13-37] Low
	[38-67] Medium
	[68-87] High
	[>88] Highest
RL	(default: Enabled)
	Remote access to the AIC will be restricted when enabled; other users in
	your network cannot log in to the WebGUI remotely.
	It is used as follows:
	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	Set the disks's temperature threshold.
	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.
TU	Set the [Temperature Unit] to Celsius or Fahrenheit.

SSD7000 Software Guide

	This setting is only supported by the Windows HighPoint RAID Management.
CL	Set enable or disable [Collecting System Logs].
	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.
	This setting is only supported by the Windows HighPoint RAID
	Management.
	It is used as follows:
	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	Change the AIC Fan Speed. This supports setting different levels of fan
	speed {Auto Off]Low Medium High Full}
	This setting is only supported by the Windows HighPoint RAID
	Management.

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



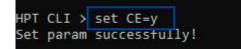
7.13.2. Set Continue Rebuilding On Error

HPT CLI>set CE=[y|n]

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

Input example:

HPT CLI>set CE=y



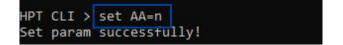
7.13.3.Set Audible Alarm

HPT CLI>set AA=[y|n]

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

Input example:

HPT CLI>set AA=n



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= [y|n]

Set enable or disable restrict localhost access.

Input example:

HPT CLI>set RL=y

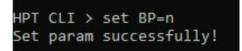


7.13.6. Set Temperature Threshold

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

Input example:

HPT CLI>set BP=n



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.

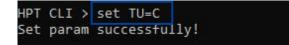
7.13.7. Set Temperature Unit

HPT CLI>set TU=[C|F]

Set the temperature unit to Celsius or Fahrenheit.

Input example:

HPT CLI>set TU=C



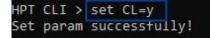
7.13.8.Set Collecting System Logs

HPT CLI>set CL=[y|n]

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

Input example:

HPT CLI>set CL=y



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



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



7.14. Unplug Command

Unplug	Command This command allows you to unplug an existing RAID array or device.
	After you have unpluged 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

D	Secured	Capacity	MaxFree	Flag	Status	ModelNumber
/E1/5	No	500.03	0	RAID	NORMAL	Samsung SSD 980 PRO 500GB
/E1/6	No	7681.50	0	SINGLE	LEGACY	Micron 7450 MTFDKCC7T6TFR
/E1/8	No	3840.64	3340.61	RAID	NORMAL	Micron 9300 MTFDHAL3T8TDP
	>unplug : device(1/E:	1/E1/6 1/6) successf	ully!			
inplug c		1/6) successf	ully!			
Inplug d	device(1/E	1/6) successf	ully! MaxFree	Flag	Status	ModelNumber
Inplug c IPT CLI D	device(1/E > query de	1/6) successf evices		Flag RAID	Status NORMAL	ModelNumber

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 CL ID	I > query arı Secured Cap		Туре	Status	Block	Sector	Cache	Name
1	No	500.03	RAID1	NORMAL		512B	NONE	RAID_1_0
	.I > unplug 1 g array(1) sug							
HPT CL ID	I > query ar	rays Dacity(GB)	Туре	Status	Block	Sector	Cache	Name

7.15. Secure Command

tax:		
	e {enclosure id} enable key={password}	Enable device security on the enclosure.
securi	e {enclosure id} disable	Disable device security on the enclosure.
secur	e {enclosure id} change oldkey={old passw	ord} key={new password} Change all devices' security key on the enclosure.
secur	e {device id} legacy	Secure legacy device.
secur	e {device id} changekey key={old password	} Change the device's security key to be consistent with all other devices' key on the enclosure
securi	e {device id} secureerase {force}	Erase the device's security configuration and securely erases data.

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
	key	{old password}	with the AIC security key.
secure	secureerare	{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



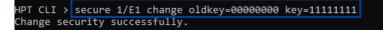
7.15.2. Change AIC Security key

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}
```



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

ID Secure	VendorID	ProductID	NumberOfPYH
1/E1 Yes	HPT	R7628A NVMe RAID Adapter	8
Disable secur	ure 1/E1 disable ity successtully		
	ry enclosures		NumberOfPY
HPT CLI > que ID Secure	VendorTD	ProductID	

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

D	Secured	Capacity	MaxFree	Flag	Status	ModelNumber
/E1/5	No	500.11	0	SINGLE	LEGACY	Samsung SSD 980 PRO 500GE
/E1/6	No	7681.50		SINGLE	LEGACY	Micron_7450_MTFDKCC7T6TFF
/E1/8	No	3840.76	0	SINGLE	LEGACY	Micron 9300 MTFDHAL3T8TDF
Secure	le <mark>gacy dev</mark> i	l/E1/5 legacy ice(1/E1/5) s				
iecure IPT CLI	legacy devi	ice(1/E1/5) s evices	uccessfully	Flor	Status	Modol Wumbon
ecure	le <mark>gacy dev</mark> i	ice(1/E1/5) s		Flag	Status	ModelNumber
ecure IPT CLI D	legacy devi	ice(1/E1/5) s evices	uccessfully	Flag SINGLE	Status	ModelNumber
ecure	legacy devi > auerv de Secured	ice(1/E1/5) s evices Capacity	MaxFree			

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

D	Secured	Capacity	MaxFree	Flag	Status	ModelNumber
/E1/5	Yes(locked)	500.11	0	SINGLE	NORMAL	Samsung SSD 980 PRO 500GE
L/E1/6	No	7681.50	0	SINGLE	LEGACY	Micron_7450_MTFDKCC7T6TFR
/E1/8	No	3840.76	0	SINGLE	LEGACY	Micron 9300 MTFDHAL3T8TDF

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

[D	Secured	Capacity	MaxFree	Flag	Status	ModelNumber
L/E1/5	Yes	500.03	500.03	SINGLE	NORMAL	Samsung SSD 980 PRO 500GE
L/E1/6	No	7681.50	0	SINGLE	LEGACY	Micron 7450 MTFDKCC7T6TFF
L/E1/8	No	3840.76	0	SINGLE	LEGACY	Micron 9300 MTFDHAL3T8TDF
		1/E1/5 secure e(1/E1/5) suc				
ecuree		e(1/E1/5) suc evices	cesstully.			
ecuree	era <mark>se devic</mark>	e(1/E1/5) suc		Flag	Status	ModelNumber
ecuree IPT CLI ID	<pre>se device > query de Secured</pre>	e(1/E1/5) suc evices	cesstully.	Flag SINGLE	Status	ModelNumber Samsung SSD 980 PRO 500GE
securee	<pre>se device > query de Secured</pre>	e(1/E1/5) suc evices Capacity	Cesstully. MaxFree			

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

he diagnostic information will be saved in C:\Program Files\HighPoint Technologies, Inc\HighPoint RAID Management\Serv

• For Linux User

HPT CLI><mark>diag</mark> 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



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 > 1:	scard	
CARD_ID	NAME	ACTIVED
0	Controller(1): HighPoint	Active
1	Controller(2): RR3720	Inactive
HPT CLI > s		
HPT CLI > 1		
CARD_ID	NAME	ACTIVED
0	Controller(1): HighPoint	Inactive
1	Controller(2): RR3720	Active

7.18. Update Command



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_____V_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



7.19.2. Show the Specific Command Help

HPT CLI>help {command}

Show help about a specific command.

Input example:

HPT CLI>help delete



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



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

Description of the Problem 1.

When installing the driver, due to various factors, driver files such as gcc and make cannot be

compiled, thus interrupting the driver installation process:

Cause of the Problem 2.

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 bullseve 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 bullseve-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 bullseve/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 bullseve/contrib Sources [43.2 kB]
Get:8 https://mirrors.tuna.tsinghua.edu.cn/debian bullseve/main amd64 Packages [8.184 kB]
Get:9 https://mirrors.tuna.tsinghua.edu.cn/debian bullseve/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 bullseve-security/main Sources [160 kB]
det:35 https://mirrors.tuna.tsingnua.edu.cn/debian-security buttseye-security/main sources [100 kB] Get:36 https://mirrors.tuna.tsinghua.edu.cn/debian-security buttseye-security/non-free Sources [632 B]
det:36 https://mirrors.tuna.tsingnda.edu.cn/debian-security bullseve-security/main amd64 Packages [189 kB]
det:3/ https://mirrors.tuna.tsinghua.edu.cn/debian-security bullseve-security/main Translation-en [119 kB]
Get:30 https://mirrors.tuma.tsinghua.edu.cn/debian-security bullseve-security/non-free amd64 Packages [528 B]
det:39 https://mirrors.tuna.tsinghua.edu.cn/debian-security bullseve-security/non-free Translation-en [34 B]
Fetched 40.2 MB in 3min 13s (208 kB/s)
Reading package listsDone
rootoff pickage trass pointer in the second

d. Reinstall the HighPoint software.

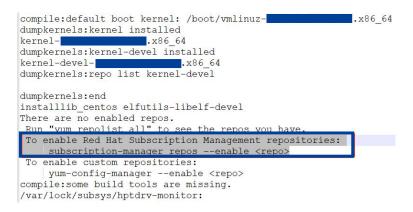
8.1.2. For RHEL

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:



Or a prompt with subscription-manager repos:



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<mark>s</mark>--password=<mark>--auto-attach</mark> Registering to: subscription.rhsm.redhat.com:443/subscription The system has been registered with 10: 963 The registered system name is: localhost.localdomain

e. Reinstall the HighPoint software.

[root@localnost 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:



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 (/usc/hio/make) Installing program wace (failed)	
jound program per 1 (/usr/bio/per1)	
Found program wget (/usr/bir/uget) old pcle_aspmeoff ionmu=off intel_ionmu=off and_ionmu=off new pcle_aspmeoff ionmu=off intel_ionmu=off and_ionmu=off Synchronizing state of hptdrv=monitor.service with SysV service script with /lib/systemd/systemd- Executing: 'lib/systemd/systemd-sysv=install enable hptdrv=monitor wpdate=rc.d: wærning: enable action will have no effect on runlevel 1 Toolchain to built the driver is incomplete, please install the missing package to build the driv Exit.	

- 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.
- 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:

Veritying archive integrity All good.	
Uncompressing HighPoint NVMe RAID Controller Linux Open Source package	Installer
Checking and installing required toolchain and utility	DISTURE
Found program make (/usr/bin/make)	
Installing program gcc (failed)	
Found program per1 (/usr/bin/per1)	
Found program wget (/usr/bin/wget)	
old pcle_aspm=off lommu=off intel_lommu=off amd_lommu=off	
new pcle_aspm=off iomnu=off intel_iomnu=off amd_iomnu=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 built the driver is incomplete, please install the missin	g package to build the driver.
oot@test:/home# apt-get update	
rr:1 http://ftp.debian.org/debian bullseye InRelease Temporary failure resolving 'ftp.debian.org'	
rr:2 http://ftp.debian.org/debian buliseye-updates InRelease	
Temporary failure resolving 'fto.debian.org'	
rr:3 http://security.debian.org bullseye-security InRelease	
Temporary failure resolving 'security.debian.org'	
rr:4 https://enterprise.proxmox.com/debian/pve_bullseve_InRelease	
Temporary failure resolving 'enterprise.proxmox.com'	
leading package lists Done	
w: railed to tetch http://ttp.debian.org/debian/dists/bullseye/inkelea	se Temporary failure resolving 'ftp.debian.org'

Solution:

- a. The system needs to be resourced. For details, please refer to the official website file: <u>https://pve.proxmox.com/wiki/Downloads#Update_a_running_Proxmox_Virtual_Environmen</u> <u>t_8.x_to_latest_8.2</u>
 - a) Open the system terminal with root privileges.
 - b) 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-updates main contrib non-free-firmware
 deb http://mirrors.ustc.edu.cn/debian-security bookworm-security main contrib non-free-firmware
 deb http://mirrors.ustc.edu.cn/debian-security bookworm-security main contrib non-free-firmware
 deb http://mirrors.ustc.edu.cn/debian-security bookworm-security main contrib non-free-firmware
- 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

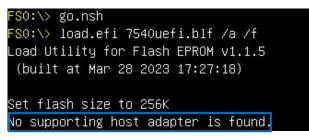
root@pue:"# apt-get update	
Hit:1 http://mirrors.ustc.edu.cn/debian bookworm InRelease	
Hit:2 http://mirrors.ustc.edu.cn/debian bookworm-updates InRelease	
Hit:3 http://mirrors.ustc.edu.cn/debian-security bookworm-security InRelease	
Hit:4 https://mirrors.ustc.edu.cn/proxmox/debian/pue_bookworm_InRelease	
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@pue:"#	

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.



2. Cause of the Problem

The system does not detect the NVMe RAID AIC.

3. Solution

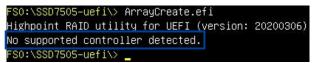
- a. Shut down the system.
- b. Move the AIC to another PCIe slotand re-enter the command.

If the problem still occurs, please provide a <u>UEFI log</u>. You can submit a support ticket using our <u>Online Support Portal</u> 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.



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 <u>UEFI log</u>. You can submit a support ticket using our <u>Online Support Portal</u> and include a problem description in as much detail as possible.

9. Glossary

Glossary	Description
Аттау	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.

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

SSD7000 Software Guide

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.
НВА	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

SSD7000 Software Guide

SSD7000 Software Guide	
	server and allows communication between mail servers.
Temperature	The degree of head 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

Updade Install the driver on macOS, add description of Secure boot and SIP.

10.4. Version 1.03, October 10, 2024

- 1. Update Install the RAID Management on Windows
- 2. Update Install the RAID Management on Linux
- 3. Update Install the RAID Management on macOS
- 4. Add RA6542AWW-S491T5-12 support.
- 5. Update background initialization description.
- 6. Add <u>Secured status</u>.