



R7000 Software Guide

V1.06 - December 26, 2025

Copyright 2025 HighPoint Technologies, Inc.

All rights reserved

Table of Contents

1. Overview.....	6
1.1. General Features of the NVMe RAID AIC	6
1.2. Advanced Features of the NVMe RAID AIC	7
1.3. Technical Support	8
1.3.1. One-Click Diagnostic Feature	8
2. SafeStorage Encryption.....	9
2.1. Workflow	10
2.1.1. Enable Security	11
2.1.2. Change Security	12
2.1.3. Create a Secured RAID	12
2.1.4. Disable Security	12
2.1.5. Import SafeStorage Encryption	13
3. UEFI HII Utility.....	14
3.1. Starting the UEFI HII Utility	14
3.2. UEFI HII Utility Menu View	16
3.2.1. View the Controller Information	16
3.2.2. View the Physical Device Information	17
3.2.3. View the Logical Device Information	17
3.2.4. Create a RAID array	18
3.2.5. Delete a RAID array	20
4. Install the HighPoint RAID Software.....	21
4.1. Install the Software on Windows	23
4.1.1. Uninstall the driver on Windows	24
4.1.2. Uninstall the RAID Management on Windows	25
4.2. Install the Software on Linux	26
4.2.1. Uninstall the driver on Linux	27
4.2.2. Uninstall the RAID Management on Linux	27
5. Web RAID Management Interface.....	28
5.1. Start the WebGUI	28
5.2. Global View	29
5.2.1. HBA Properties	29
5.2.2. Storage Properties	29
5.3. Physical	30
5.3.1. Controller Information	30
5.3.2. Enclosure Information	31
5.3.3. Vital Product Data Information	32
5.3.4. Physical Devices Information	33

5.3.5. Sensors Information	40
5.3.6. Update the Firmware	42
5.3.7. Secure Setting	43
5.3.8. Fan Setting	44
5.3.9. Hotplug Compatibility Mode Setting	45
5.3.10. LED On/Off Setting	46
5.3.11. Rescan the Physical Device	46
5.4. Logical	47
5.4.1. Logical Device Information	47
5.4.2. Physical Device Information	50
5.4.3. Create a RAID Array	51
5.4.4. Delete a RAID Array	54
5.4.5. Unplug a RAID Array	55
5.4.6. Verify a RAID Array	56
5.4.7. Add a Spare Disk	57
5.4.8. Remove a Spare Disk	58
5.5. Setting	59
5.5.1. System Setting	60
5.5.2. Password Setting	62
5.5.3. Email Setting	63
5.6. Event	69
5.6.1. View the Event Log	69
5.6.2. Save the Event Log	70
5.6.3. Event Log Icon Guide	71
5.7. SHI	72
5.7.1. View the SHI Information	72
5.7.2. View the SMART Information	73
5.7.3. View the TBW Information	73
5.7.4. Create a Health Inspector Scheduler	74
5.7.5. Create a New Verify Task	75
5.7.6. Delete a Task	76
5.8. Help	77
5.8.1. Online Help	77
5.8.2. Diagnostic View	77
5.8.3. Save the Diagnostic Log	78
6. Command Line Interface	82
 6.1. Start the CLI	82
 6.2. Query Commands	84
6.2.1. Query Controller	85
6.2.2. Query Enclosure	86
6.2.3. Query Device	88
6.2.4. Query Array	91
 6.3. Init Commands	93

6.3.1. Init a Physical Disk	93
6.3.2. Init a RAID Array	94
6.4. Create Command	95
6.4.1. Create a RAID Array	97
6.4.2. Create a Spare Disk	97
6.5. Delete Command	98
6.5.1. Delete a RAID Array	98
6.5.2. Delete a Spare Disk	99
6.6. Rebuild Command	100
6.6.1. Rebuild a RAID array	100
6.6.2. Start Rebuilding the RAID Array	101
6.6.3. Stop Rebuilding the RAID Array	101
6.7. Verify Command	102
6.7.1. Start Verifying the RAID Array	102
6.7.2. Stop Verifying the RAID Array	102
6.8. Rescan Command	103
6.8.1. Rescan the Physical Devices	103
6.9. Lscard Command	104
6.9.1. Lscard all AICs	104
6.10. Events Command	105
6.10.1. View the Event Log	105
6.10.2. Save the Event Log	106
6.11. Mail Command	107
6.11.1. Add a Mail Recipient	108
6.11.2. List all Mail Recipients	108
6.11.3. Test the mail recipient	109
6.11.4. Delete a Mail Recipient	109
6.11.5. Add a Mail Server	110
6.11.6. List all Mail Servers	110
6.11.7. Set the Mail Server	110
6.12. Task Command	111
6.12.1. Create a New Rebuild Task	112
6.12.2. Create a New Verify Task	112
6.12.3. List all Tasks	112
6.12.4. Delete a Task	113
6.13. Set Command	114
6.13.1. Set Auto Rebuild	118
6.13.2. Set Continue Rebuilding On Error	118
6.13.3. Set Audible Alarm	118
6.13.4. Set Beeper	119
6.13.5. Set Rebuild Priority	119
6.13.6. Set Temperature Unit	119
6.13.7. Set Collecting System Logs	120
6.13.8. Set Password	120

6.13.9. Set Identify LED	121
6.13.10. Set AIC Fan Speed.....	121
6.13.11. Set Hotplug Compatibility Mode	121
6.13.12. Set Status/ Fault/ SSD LED On/Off.....	122
6.13.13. Set Restrict to Localhost Access	123
6.14. Unplug Command	124
6.14.1. Unplug the Physical Device	124
6.14.2. Unplug a RAID Array	125
6.15. Secure Command	126
6.15.1. Enable AIC Security	127
6.15.2. Change AIC Security key	127
6.15.3. Disable AIC Security	128
6.15.4. Enable Disk Security	128
6.15.5. Change Disk Security key	129
6.15.6. Disable Disk Security	129
6.16. Diag Command	130
6.16.1. Collect the Diagnostic Information	130
6.17. Switch Command	131
6.17.1. Switch the AIC	131
6.18. Update Command	132
6.18.1. Update the Firmware	132
6.19. Help Command	133
6.19.1. Show the Generic Help Command	133
6.19.2. Show the Specific Command Help	134
6.20. Ver Command	135
6.20.1. Show the RAID Management Version	135
6.21. Exit Command	136
6.21.1. Exit the CLI	136
6.22. Clear Command	137
6.22.1. Clear the CLI screen	137
7. Format the RAID Array	138
7.1. Format the RAID Array in Windows	138
7.2. Format the RAID Array in Linux	140
7.3. Format the RAID Array in macOS	141
8. Trouble shooting	142
8.1. Fail to compile gcc, make and other driver files	142
8.1.1. For Debian	142
8.1.2. For RHEL	144
8.1.3. For Ubuntu	145
8.1.4. For Proxmox	146
8.2. Delete a drive partition in Windows	148
9. Glossary	149

10. Revision History	152
10.1. Version 1.00, June 24, 2024	152
10.2. Version 1.01, July 1, 2024	152
10.3. Version 1.02, January 3, 2025	152
10.4. Version 1.03, February 12, 2025	152
10.5. Version 1.04, April 11, 2025	153
10.6. Version 1.05, October 10, 2025	153
10.7. Version 1.06, December 26, 2025	153

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

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	R7628A/ R7528D/ RS6541AW/ R7624A/ R7528U/ R7628U
LED Indicators	R7628A/ R7608A/ R7528D/ RA7608AW/ RS6541AW/ R7604A/ R7624A/ R7528U/ R7628U
Fan Control	R7608A/ RA7608AW/ RS6541AW/ R7604A
Alarm Buzzer	R7628A/ R7608A/ R7528D/ RA7608AW/ RS6541AW/ R7604A/ R7624A/ R7528U/ R7628U
Boot RAID Support	R7628A/ R7608A/ R7528D/ RA7608AW/ RS6541AW/ R7604A/ R7624A/ R7528U/ R7628U
UEFI HII Utility	R7628A/ R7608A/ R7528D/ RA7608AW/ RS6541AW/ R7604A/ R7624A/ R7528U/ R7628U
Flash ROM for Upgradeable UEFI	R7628A/ R7608A/ R7528D/ RA7608AW/ RS6541AW/ R7604A/ R7624A/ R7528U/ R7628U
Global Hot Spare Disk support	R7628A/ R7608A/ R7528D/ RA7608AW/ RS6541AW/ R7604A/ R7624A/ R7528U/ R7628U

1.3. Technical Support

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

1.3.1. One-Click Diagnostic Feature

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

2. SafeStorage Encryption

Overview

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

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

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

Benefits

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

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

2.1. Workflow

Overview

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

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

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

2.1.1. Enable Security

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

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

Enable AIC Security

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



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

Enable Disk Security

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

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

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

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

2.1.2. Change Security

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

Change AIC Security

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

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

Change Disk Security

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

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

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

2.1.3. Create a Secured RAID

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

2.1.4. Disable Security

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

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

Disable Disk Security

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



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

Disable AIC Security

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



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

2.1.5. Import SafeStorage Encryption

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

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

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

3. UEFI HII Utility

Overview

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

Prerequisites

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

3.1. Starting the UEFI HII Utility

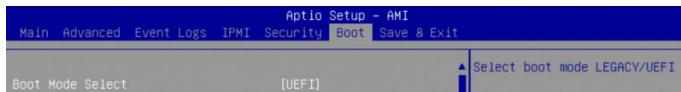
Follow these steps to start the UEFI HII Utility.

Step 1 Adjust System EFI Settings

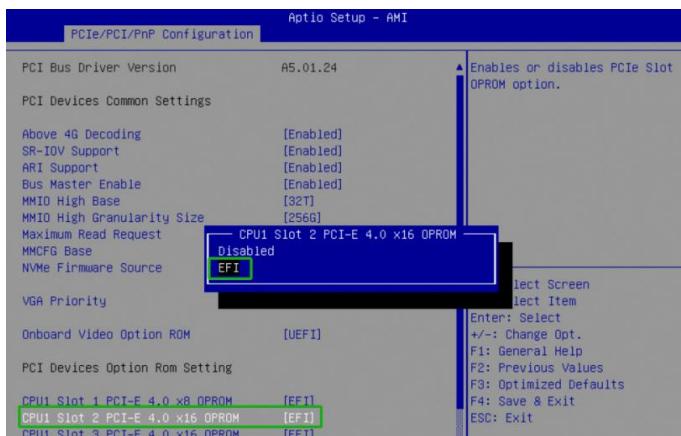
1. Insert the AIC into the motherboard, power on the system, and enter the BIOS.
2. Adjust the UEFI settings. Allow the option ROM settings for third-party devices to load.

Example: SuperMicro X12DPi-N6 motherboard

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



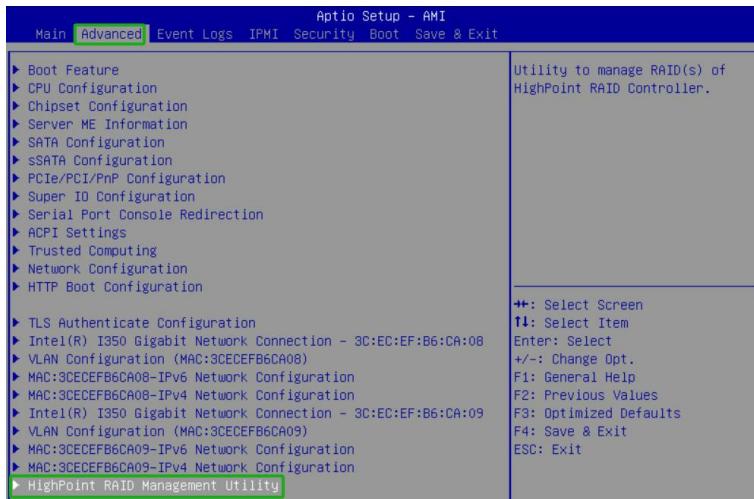
- 2) Set the **Slot** where the AIC is located to **EFI**.



3. Save changes and reboot.

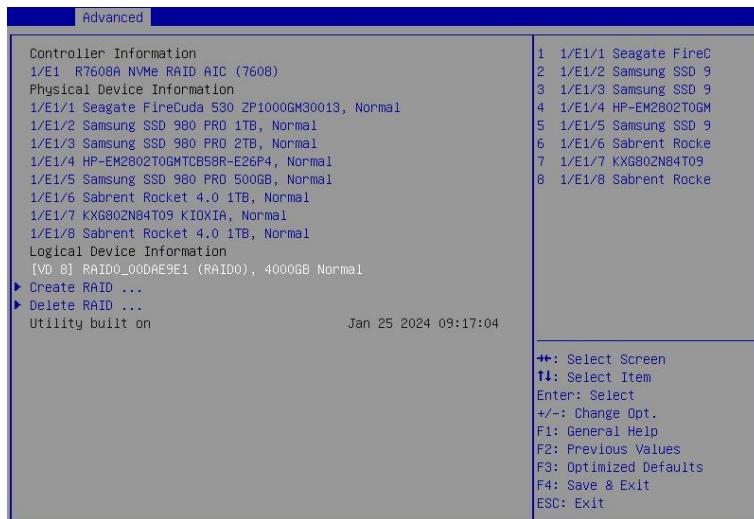
Step 2 Enter the UEFI HII Utility

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



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

3.2.UEFI HII Utility Menu View



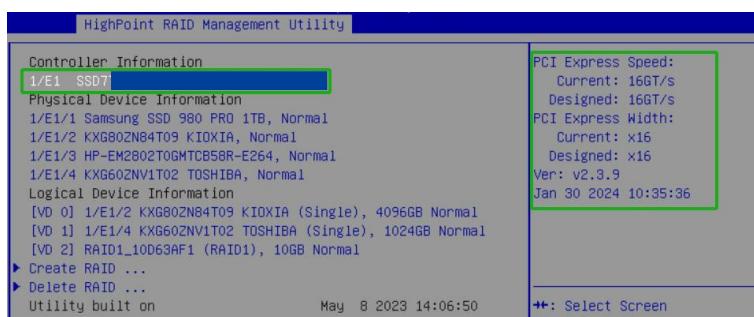
Keys

The UEFI HII Utility utilizes the following keys:

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

3.2.1. View the Controller Information

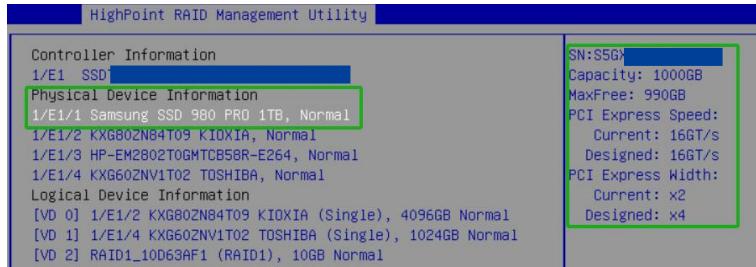
The UEFI HII Utility view allows you to view the Controller Information. The AIC that has been connected to the system will appear here.



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

3.2.2. View the Physical Device Information

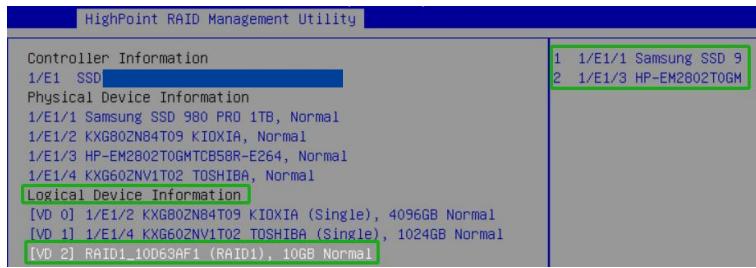
The UEFI HII Utility view allows you to view the Physical Device Information. The disks hosted by the AIC will appear here.



- **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.

3.2.3. View the Logical Device Information

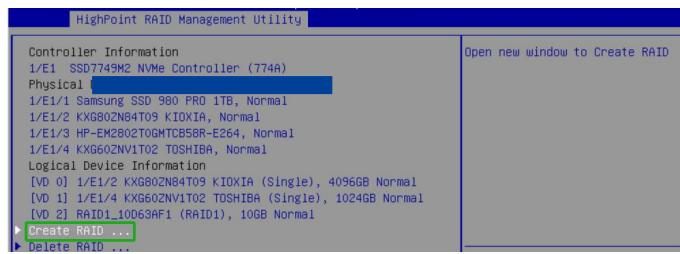
The UEFI HII Utility view allows you to view the Logical Device Information. The disks and arrays you create and their associated properties will appear here.



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

3.2.4. Create a RAID array

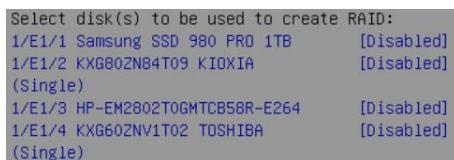
The UEFI HII Utility view allows you to create the RAID array.



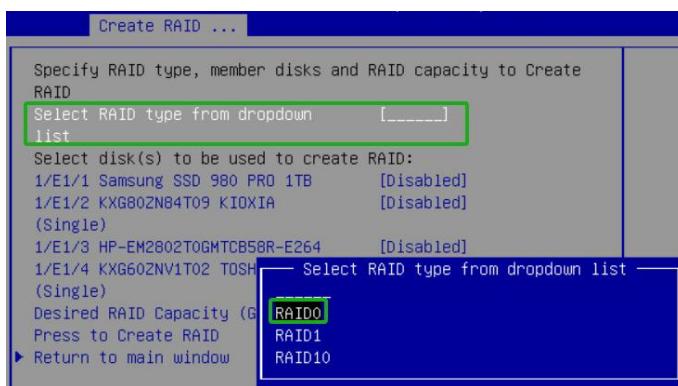
Note: RocketAIC series NVMe AIC SSDs are already pre-configured with RAID0. You can skip those steps. You can follow the steps if you want to use another type of RAID.

To create a RAID, perform the following steps:

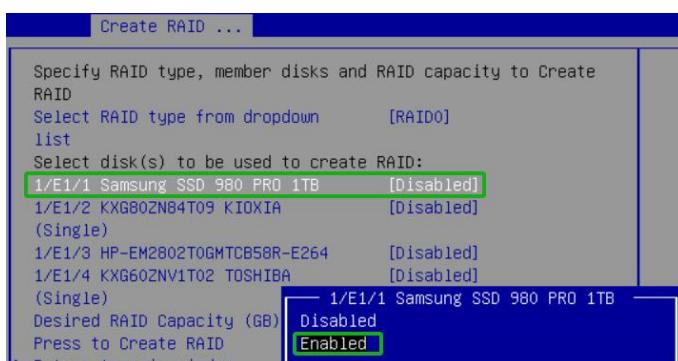
1. Select **Create RAID...** from the HighPint RAID Management Utility.
2. On the **Create** menu. A disk list will appear, and all available disks will be displayed.



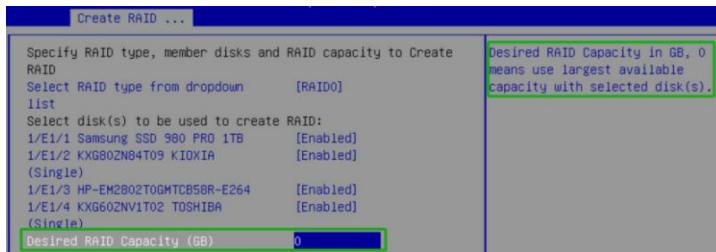
3. Select the **RAID type** from the dropdown list. Use the keyboard or mouse's up and down keys to select the RAID type and press **Enter**.



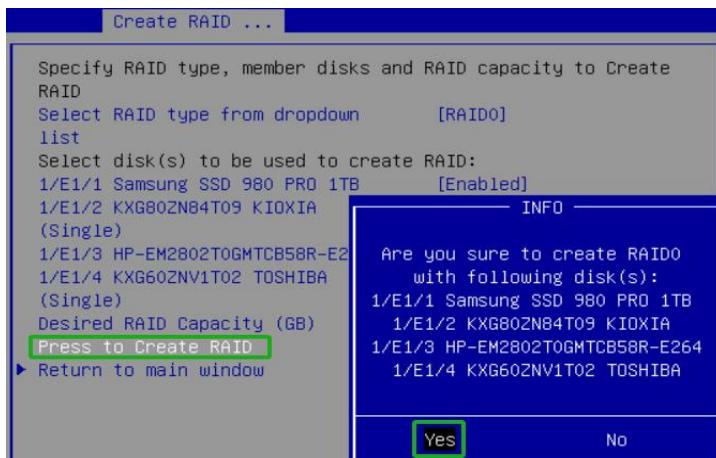
4. Select the disk that needs to create a RAID array and the status of the disk changes from **Disabled** to **Enabled**.



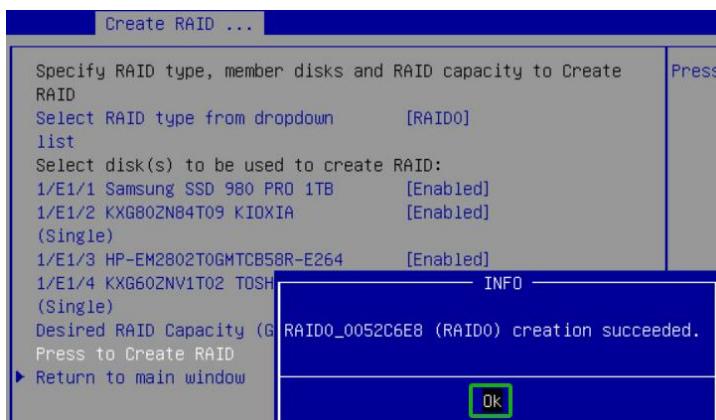
5. Use the keyboard to input the space (GB) you want to set aside for this array. You can decide how much storage capacity will be assigned to the array.



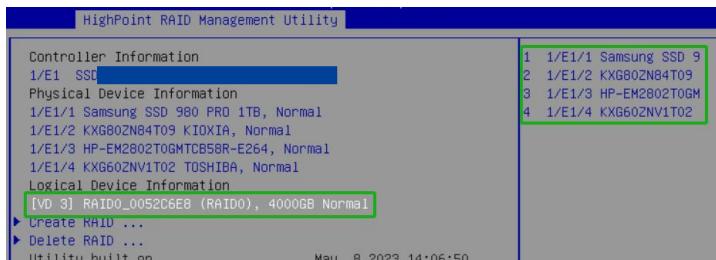
6. Select and **press to create RAID** to complete the RAID Array creation. A pop-up window prompt: **Are you sure to create RAID0 with following disk(s)**. Press **Enter** to confirm.



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

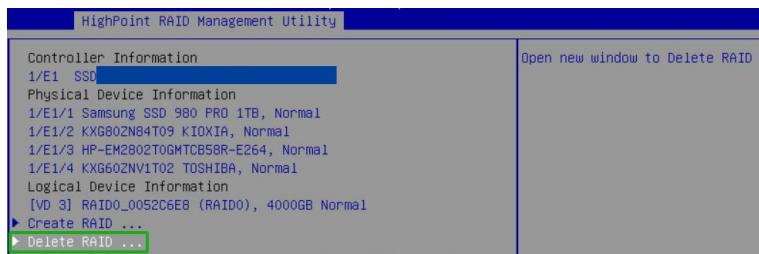


8. The array you create, and its associated properties will appear under the **Logical Device Information**.



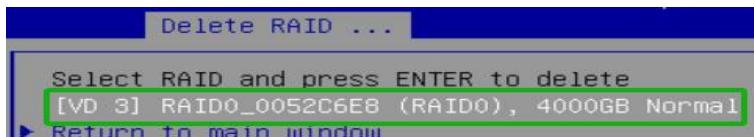
3.2.5. Delete a RAID array

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

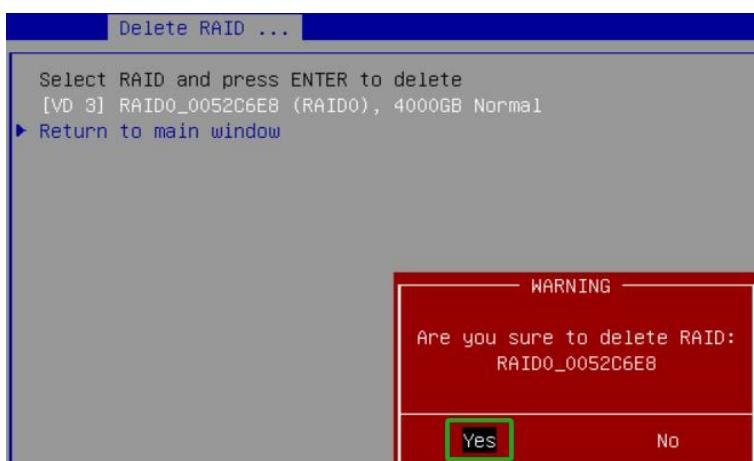


To delete a RAID, perform the following steps:

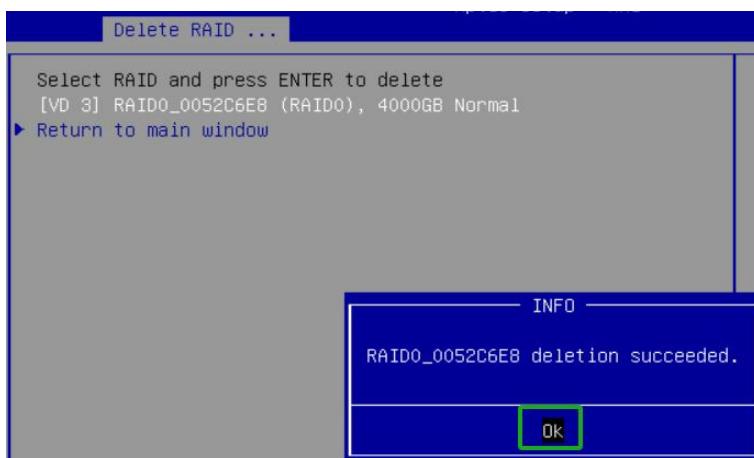
1. Select **Delete RAID...** from the HighPoint RAID Management Utility.
2. Select the array you wish to delete and press **Enter**.



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



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



4. Install the HighPoint RAID Software

HighPoint RAID Software Overview

The HighPoint RAID Software includes the HighPoint driver and RAID Management. You only need to run the **HighPoint RAID Software.exe** to install the HighPoint driver and RAID Management.

● HighPoint driver Overview

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

● HighPoint RAID Management Overview

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

The HighPoint RAID Management includes two parts:

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

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

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

HighPoint Driver Prerequisites

1. The AIC must be installed into a PCIe slot.
2. Ensure any non-HighPoint drivers are uninstalled for SSDs hosted by the AIC. 3rd party software and manufacturer-provided drivers may prevent the AIC from functioning properly.
3. Download the appropriate driver from the AIC's Software Downloads webpage.
4. Linux operating system Secure Boot must be disabled.
 - 1) HighPoint Linux Driver capability has not been signed and certified. If Secure Boot is enabled, the driver will not load.
 - a. Boot the system and access the motherboard BIOS menu.

b. Set Secure Boot to **Disabled.****Warnings:**

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

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

4.1. Install the Software on Windows

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

1. Locate the HighPoint RAID Software download and open the file.
2. Double-click **HighPoint NVMe G5 RAID Windows Software.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. Select the optional components you wish to install. Click **Install** to start the installation.



4. Click **Finish** to reboot Windows.



4.1.1. Uninstall the driver on Windows

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

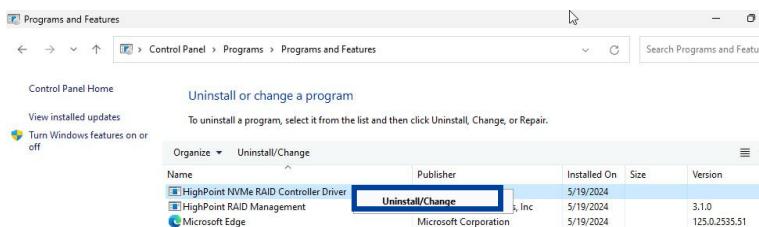
1. Power down the system and remove the AIC from the motherboard.

Notes:

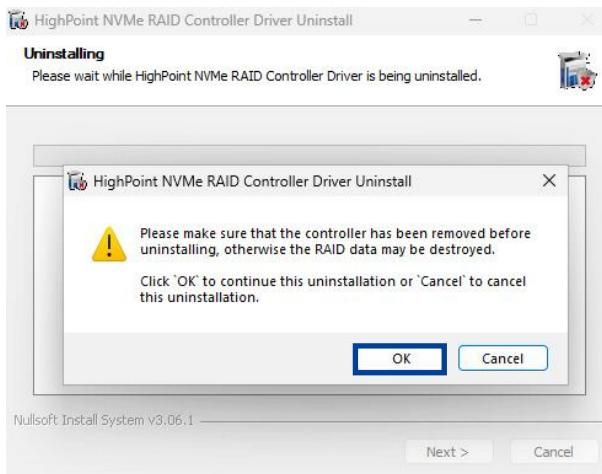
Failing to remove the AIC from the system during the uninstall process may result in data loss.

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

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



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



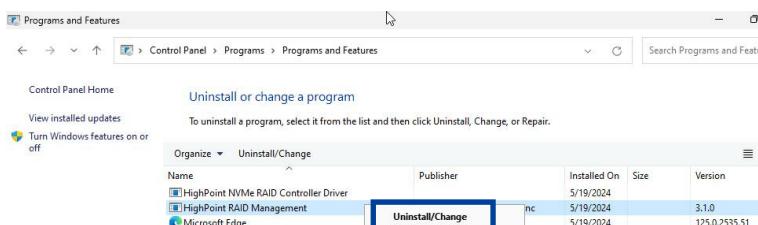
6. After uninstalling the driver, click **Finish**.



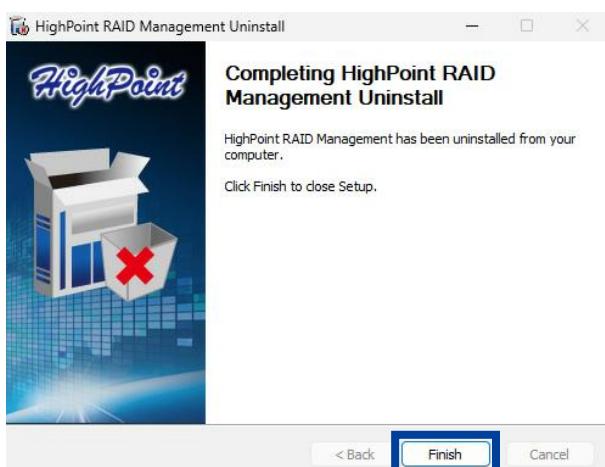
4.1.2. Uninstall the RAID Management on Windows

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

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



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



4.2. Install the Software on Linux

To install the HighPoint RAID Software 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 RAID Software is located.

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

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

3. Enter the following command to extract the HighPoint RAID Software package:

```
#tar zxvf HighPoint_NVMe_G5_Linux_Software_vx.x.xx_xx_xx_xx_xx.tar.gz
```

```
root@test-Z790M-AORUS-ELITE-AX:/home/test/Downloads# tar zxvf HighPoint_NVMe_G5_
RAID_Linux_Software_v1.8.0.0.0_24_05_27.tgz
setup.bin
README.txt
```

4. Enter the following command to install the HighPoint RAID Software.

```
#sh setup.bin (or ./setup.bin)
```

```
root@test-Z790M-AORUS-ELITE-AX:/home/test/Downloads# ./setup.bin
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.....
.....
sed: can't read /etc/init.d/udev: No such file or directory
sed: can't read /etc/init.d/udev: No such file or directory
Checking and installing required toolchain and utility ...
Installing program make ... done
Installing program gcc ... done
Found program perl (/usr/bin/perl)
Found program wget (/usr/bin/wget)
Sourcing file '/etc/default/grub'
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-6.8.0-31-generic
Found initrd image: /boot/initrd.img-6.8.0-31-generic
Found test86_64bit_EFI image: /boot/test86+x64.efi
Warning: os-prober will not be executed to detect other bootable partitions.
Systems on them will not be added to the GRUB boot configuration.
Check GRUB_DISABLE_OS_PROBER documentation entry.
Adding boot menu entry for UEFI Firmware Settings ...
done
Synchronizing state of hptdrv-monitor.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable hptdrv-monitor
update-rc.d: warning: enable action will have no effect on runlevel 1
SUCCESS: Driver hptnvm is installed successfully for kernel 6.8.0-31-generic.
Please restart the system for the driver to take effect.
If you want to uninstall the driver from the computer, please run hptuninhptnvm to uninstall the driver files.
Verifying archive integrity... All good.
Uncompressing HighPoint Web RAID Management Software package installer.....
.....
readline lib is already installed!
removing previous hptsvr(3.2.0)...
Waiting for hptsvr to be terminated...
Installing hptsvr(3.2.0)...
Installing related files...
Configuring service...
Starting hptsvr daemon.
```

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

4.2.1. Uninstall the driver on Linux

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

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

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

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

```
#hptuninhptnvme
```

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

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

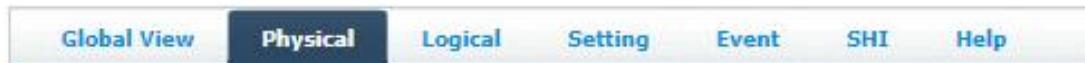
4.2.2. Uninstall the RAID Management on Linux

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

```
#hptuninhptsvr
```

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

5. Web RAID Management Interface



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

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

5.1. Start the WebGUI

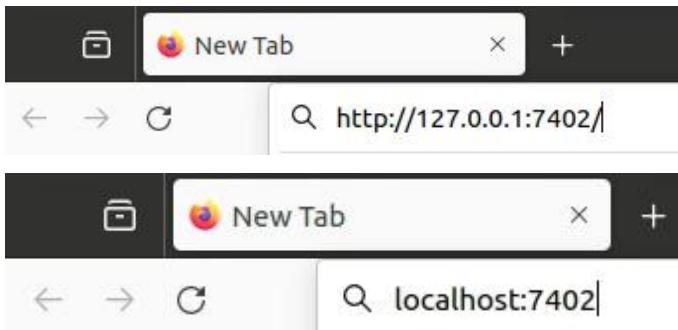
For Windows Users

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



For Linux Users

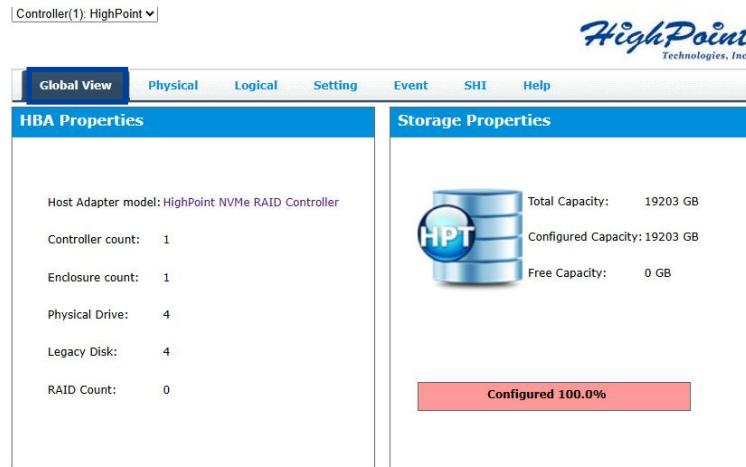
Open the browser and enter <http://127.0.0.1:7402> or localhost:7402 to log into WebGUI. 7402 is the WebGUI's Port Number, which can be modified.



5.2. 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.



5.2.1. 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.

5.2.2. 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.

5.3. Physical

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



5.3.1. 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.

5.3.2. Enclosure Information

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

Enclosure Information	
Model:	HighPoint
Vendor:	1
ID:	5.15.12.0
Firmware Version:	2.5.1
UEFI Version:	1.1
PCB Version:	
Vendor ID:	0x1103
Device ID:	0x7604
Location:	PCI bus 5, device 0, function 0
Current Link Width:	x8
Current Link Speed:	8.0 GT/s
SN:	
Chip Temperature:	48 °C/118 °F
Board 3.3V Voltage:	3.252 V
Board 12V Voltage:	12.060 V
Power Consumption:	19.96 W
Fan Speed:	2250 RPM

- **Model** — The name of the AIC.
- **Vendor** — The manufacturer of the AIC.
- **ID** — The number of the AIC.
- **Firmware Version** — The firmware version of the AIC.
- **UEFI Version** — The UEFI HII Utility version of the AIC
- **PCB Version** — The hardware version of the AIC.
- **Vendor ID** - An AIC property indicating the vendor-assigned ID number of the AIC.
- **Device ID** - The device ID of the AIC.
- **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.
- **SN** — The serial number of the AIC.
- **Chip Temperature** — The temperature of the AIC's chip.
- **Board 3.3V Voltage** — The board 3.3V voltage of the AIC. When the voltage exceeds 3.3V ($\pm 8\%$), the voltage is displayed in red.

Note: If the Board 3.3V Voltage exceeds the threshold, the voltage here will be displayed in red.

- **Board 12V Voltage** — The board 12V voltage of the AIC. When the voltage exceeds 12V ($\pm 8\%$), the voltage is displayed in red.

Note: If the Board 12V Voltage exceeds the threshold, the voltage here will be displayed in red.

- **Power Consumption** — Total power consumption of the AIC, disks, and external power supply (provided by the PCIe host interface)
- **Fan Speed** — The current fan speed of the AIC.

5.3.3. Vital Product Data Information

The **Vital Product Data Information** section displays the following information.

Enclosure Information	
Model:	R7604A NVMe RAID AIC
Vendor:	HighPoint
ID:	1
Firmware Version:	5.15.12.0
UEFI Version:	2.5.1
PCB Version:	1.1
Vendor ID:	0x1103
Device ID:	0x7604
Location:	PCI bus 5, device 0, function 0
Current Link Width:	x8
Current Link Speed:	8.0 GT/s
SN:	2222229222222
Chip Temperature:	48 °C/118 °F
Board 3.3V Voltage:	3.252 V
Board 12V Voltage:	12.060 V
Power Consumption:	19.96 W
Fan Speed:	2250 RPM

Vital Product Data	
Product Name:	HighPoint
[PN] Part number:	R7604A-72C0000
[EC] Engineering changes:	0000
[MN] Manufacture ID:	1103
[SN] Serial number:	(redacted)
[V0] Vendor specific:	HighPoint Technologies
[V1] Vendor specific:	Broadcom PEX89048

- **Product Name** — The name of the AIC.
- **[PN] Part number** — The part number of the AIC.
- **[EC] Engineering changes** — The engineering change of the AIC.
- **[MN] Manufacture ID** — The manufacture ID of the AIC.
- **[SN] Serial number** — The serial number of the AIC.
- **[V0] Vendor specific** — The manufacturer of the AIC.
- **[V1] Vendor specific** — The chip model of the AIC.

5.3.4. Physical Devices Information

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



The screenshot shows the HighPoint Software interface with the 'Physical' tab selected. The main window displays a table titled 'Physical Devices Information' with the following data:

Model	Capacity
Device 1_E1_1 Model	1.92 TB
Device 1_E1_2 Model	1.92 TB
Device 1_E1_3 Model	7.68 TB
Device 1_E1_4 Model	7.68 TB

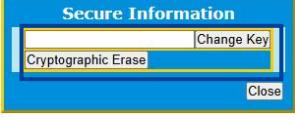
Below the table, there are additional details for the selected disk (Device 1_E1_4):

Unplug	Revision	E1MU2S1	PCIe Width	x4
	Location	1/E1/4	PCIe Speed	16.0 GT/s
	Max Free	0.00 GB		
	Status	Legacy		
	Serial Num	2316423C35A4	Identify LED	[ON] [OFF]
	Interface	NVME	Type	SSD
	SED Capable	No	SED Type	None
	Secured	No	Cryptographic Erase Capable	No

- **Model** – The model number of the physical disk.
- **Capacity** – The total capacity of the physical disk.
- **Revision** – The physical disk firmware revision number.
- **Location** – The physical disk location (e.g., Device 1_E1_1 represents the disk on AIC 1 port 1).
- **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.
- **Identify LED** – Identify the location of the disk. When **On** is selected, the disk LED will light up red to get the location of the disk. When **Off** is selected, the disk LED turns off.
- **Secured** – Whether the physical disk is secured.

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

Table 2: Secured Status & Description

Secured Status	Description
<p>Yes</p> 	<p>Indicates that security for the disk is enabled. The disk and AIC keys are the same, and the disk is initialized, and the disk is not reported to the system.</p> <p>Your optional option is:</p>  <ul style="list-style-type: none"> Cryptographic Erase <p>The Cryptographic Erase function will erase the secured key inside each disk, making it impossible to decrypt data stored on these devices.</p>
<p>Yes (Locked)</p> 	<p>Indicates that the security of the disk is enabled, but the disk's key does not match the key on the AIC.</p> <p>Your optional options are:</p>  <ul style="list-style-type: none"> Change key <p>Enter the disk's old password and click Change Key to unlock the Disk Security key.</p> <p>If you do not enter the correct disk key is not entered multiple times consecutively (the exact number of incorrect attempts leading to a lock is determined by the disk and may vary), this function will be locked, and you will need to power cycle to change the disk key, i.e., perform a one-time power failure on the disk, such as hot-swapping the disk or powering down the host system and Enclosure.</p> <ul style="list-style-type: none"> Cryptographic Erase <p>The Cryptographic Erase function will erase the secured key inside each disk, making it impossible to decrypt data stored on these devices.</p>
<p>No</p>	<p>Indicates that disk security is not enabled or not supported.</p>

 Device 1_E1_3 Model Micron_7450_MTFDKCC7T6TFR Capacity 7.68 TB Unplug Revision E2MU200 PCIe Width x4 Location 1/E1/3 PCIe Speed 16.0 GT/s Max Free 0.00 GB Status Legacy Serial Num 232641B4859A Interface NVME Identify LED [ON] [OFF] SED Capable No Type SSD Secured SED Type None Cryptographic Erase Capable No	
Yes  Device 1_E1_2 Model Samsung SSD 960 EVO 250GB Capacity 250.05 GB Revision 8B7QCXE7 PCIe Width x4 Location 1/E1/2 PCIe Speed 8.0 GT/s Max Free 0.00 GB Status Legacy Serial Num 53ESN0X0J503825P Interface NVME Identify LED [ON] [OFF] SED Capable Yes Type SSD Secured Yes SED Type OPAL Cryptographic Erase Capable Yes	<p>Indicates that security for the disk is enabled. Data can be accessed.</p>
Yes (Locked)  Device 1_E1_1 Model Samsung SSD 990 PRO 1TB Capacity 1.00 TB Unplug Revision 4B2QJXD7 PCIe Width x4 Location 1/E1/1 PCIe Speed 16.0 GT/s Max Free 0.00 GB Status Normal Serial Num S621N00W325847W Interface NVME Identify LED [ON] [OFF] SED Capable Yes Type SSD Secured Yes SED Type OPAL Cryptographic Erase Capable Yes(Locked)	<p>Indicates that the security of the disk is enabled, but the disk's key does not match the key on the AIC.</p>

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



Notes:

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

There is a limit to the number of times you can change the disk key. If you do not correct disk key is not entered multiple times consecutively (the exact number of incorrect attempts leading to a lock is determined by the disk and may vary), and you will need to power cycle to change the disk key, i.e., perform a one-time power failure on the disk, such as hot-swapping the disk or powering down the host system and Enclosure.

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

5.3.4.2. 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.

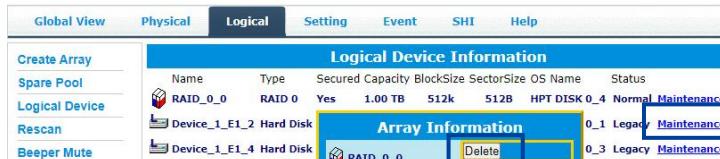
Note: When the disk is in Legacy status or is a RAID member disk, you cannot disable Disk Security directly. You need to initialize the legacy disk or delete the RAID.

To disable disk security, perform the following steps:

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



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



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



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

5.3.4.3. 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. Click the **Devices** tab.
4. Select the disk you want to unplug, and click **Unplug**.



Physical Devices Information				
<input type="checkbox"/> Device_1_E1_1 Model	Samsung SSD 983 DCT 960GB	Capacity	960.19 GB	
<input type="checkbox"/> Device_1_E1_2 Model	INTEL SSDPE21K375GA	Capacity	375.08 GB	
<input type="checkbox"/> Device_1_E1_3 Model	Samsung SSD 980 PRO 500GB	Capacity	500.10 GB	
<input type="checkbox"/> Unplug	Revision: 3B2QGXA7 Location: 1/E1/3 Max Free: 0.00 GB Status: Legacy Serial Num: S5GYNG0R206284E Interface: NVME SED Capable: Yes Secured: No	Identify LED: [ON] [OFF] Type: SSD SED Type: OPAL Cryptographic Erase Capable: Yes	PCIe Width: x4	PCIe Speed: 16.0 GT/s

5. Manually remove the disk.
6. 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**.

5.3.4.4. Identify the Physical Device LED

Identify the location of the disk. When **On** is selected, the disk LED will light up red to get the location of the disk. When **Off** is selected, the disk LED turns off.

1. Open the **WebGUI**.
2. Click the **Physical** tab.
3. Click the **Devices** tab.
4. Select the disk you want to unplug, and click **[ON]/ [OFF]**.

Physical Devices Information					
Device_1_E1_1 Model	Samsung SSD 983 DCT 960GB	Capacity	960.19 GB		
Device_1_E1_2 Model	INTEL SSDPE21K375GA	Capacity	375.08 GB		
Device_1_E1_3 Model	Samsung SSD 980 PRO 500GB	Capacity	500.10 GB		
Unplug	Revision Location Max Free Status Serial Num Interface SED Capable	3B2QGXA7 1/E1/3 0.00 GB Legacy S5GYNG0R206284E NVME Yes	PCIe Width PCIe Speed	x4 16.0 GT/s	
		Identify LED	[ON] [OFF]		
		Type	SSD		
		SED Type	OPAL		
		Cryptographic Erase Capable	Yes		

5.3.5. Sensors Information

The **Sensors Information** section displays the chip temperature, SSD temperature, power consumption and Fan Speed. The X-axis is time and the Y-axis is **Temperature/Fan Speed/Power Consumption**. Plot the information as a diagram line in different colors.



- **Last hour** – Display sensor information from the last hour.
- **Last day** – Display sensor information from the last day.
- **All** – Display messages from the last five days, up to 8,000 records.
- **Refresh** – Refresh to display the sensor's information. Refreshes and logs records once per minute.
- **Temperature (°C)** – The temperature diagram line of the chip and disk. (e.g., Port2 represents the disk on AIC port 2).

Notes:

Click **Chip (°C)** / **Port # (°C)** to adjust whether or not their diagram lines are displayed.

The unit of the temperature is confirmed by the **Setting**.

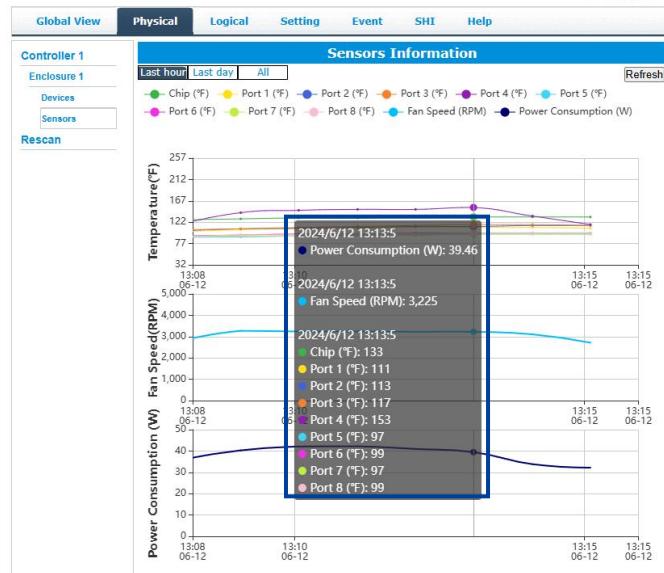
- **Fan Speed (RPM)** – The fan speed diagram line of the AIC.
- **Power Consumption (W)** – The power consumption diagram line of the AIC, disks and external power supply.

Notes:

For products using M.2 disks, the power is the sum of the power of the AIC, disks, and external power supply;

For products using U.2 disks, the power is the sum of the power of the AIC and the external power supply.

The cursor on the diagram line now shows the sensor information. The contents of the interval displayed can be zoomed in and out with the mouse wheel.



5.3.6. 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.



To update the AIC firmware, perform the following steps:

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

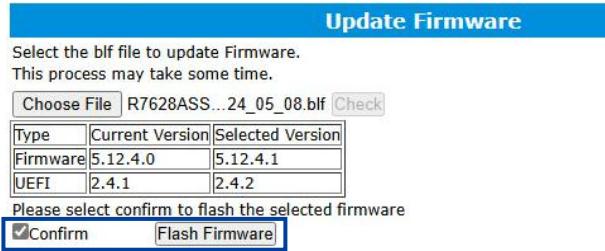


5. Click **Check**.

The current firmware version and the firmware version to be updated are displayed.



6. Select **Confirm** to flash the selected firmware.



7. Reboot the system to make the update take effect.



5.3.7. Secure Setting

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

The screenshot shows a 'Secure Setting' interface. It has two input fields: 'Password' and 'Confirm', both containing a series of dots representing masked text. Below these is a button labeled 'Enable Security'.

5.3.7.1. Enable AIC Security

To enable AIC security, perform the following steps:

1. Open the **WebGUI**.
2. Click the **Physical** tab.
3. Click the **Enclosure#** tab.
4. 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.
5. Set the password and click **Enable Security** to enable the AIC Security.

The screenshot shows the same 'Secure Setting' interface as before, but the 'Enable Security' button is highlighted with a blue border.



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

5.3.7.2. Change AIC Security

To change AIC security, perform the following steps:

1. Open the **WebGUI**.
2. Click the **Physical** tab.
3. Click the **Enclosure#** tab.
4. Enter the current password under the **Old Password** field.
5. 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.
6. After entering a new password, click **Change Security**.

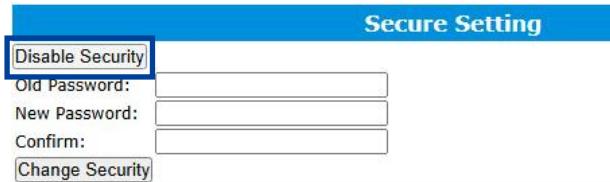
The screenshot shows the 'Secure Setting' interface with the 'Change Security' button highlighted.

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

5.3.7.3. Disable AIC Security

To disable AIC security, perform the following steps:

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



Secure Setting

Disable Security

Old Password:

New Password:

Confirm:

5.3.8. Fan Setting

This **Fan setting** supports different levels of fan speed. (default: Auto)



Fan Setting

Set Fan Speed

There are 5 levels [Auto, Off, Low, Medium, High, Full]



Fan Setting

Set Fan Speed

Hotplug compatibility mode

Parameter Setting

Disabled

Note: If you are using RS6541AW then here are the following 5 levels [Auto, Ultra Low, Low, Medium, High, Full]



Fan Setting

Set Fan Speed

Hotplug compatibility mode

Parameter Setting

Disabled

3.1.50
HighPoint Technologies, Inc. All Rights Reserved

To change AIC security, perform the following steps:

1. Open the **WebGUI**.
2. Click the **Physical** tab.
3. Click the **Enclosure#** tab.
4. Select the fan speed in the **Fan Setting-Set Fan Speed**.
5. Click **Submit**.

5.3.9. Hotplug Compatibility Mode Setting

This **Parameter Setting** supports setting the **Hotplug compatibility mode**. Enabled Hotplug compatibility mode causes performance degradation on all disks hosted by the AIC.

This setting needs to be adjusted to **Enabled** when the following situations occur.

- Connect disks with Payload=256k
- Inserting an older model disk into the system, but the system does not recognize the disk.



To change Hotplug compatibility mode, perform the following steps:

1. Open the **WebGUI**.
2. Click the **Physical** tab.
3. Click the **Enclosure#** tab.
4. Select **Disabled** or **Enabled** in the **Hotplug compatibility mode**.
5. Click **Submit**.

5.3.10. LED On/Off Setting

This **Parameter Setting** supports setting the Status LED/ Fault LED/ SSD LED On/Off. You can switch on and off the AIC Status LED, Fault LED and SSD LED.

Parameter Setting	
Status LED:	Enable <input type="button" value="▼"/>
Fault LED:	Enable <input type="button" value="▼"/>
SSD LED:	Enable <input type="button" value="▼"/>
<input type="button" value="Submit"/>	Enable Disable

To change Status LED/ Fault LED/ SSD LED On/Off., perform the following steps:

1. Open the **WebGUI**.
2. Click the **Physical** tab.
3. Click the **Enclosure#** tab.
4. Select **Disable** or **Enable** in the **Status LED/ Fault LED/ SSD LED**.
5. Click **Submit**.

Notes:

Enable indicates: The Status LED/ Fault LED/ SSD LED functions works normally and provide status feedback on the disk, AIC bandwidth, and disk temperature, etc.

Disable indicates: The Status LED/ Fault LED/ SSD LED does not to work and cannot provide any status feedback on the disk, AIC bandwidth, and disk temperature, etc.

5.3.11. 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. When a disk drop triggers the beeper, the beeper can be turned off temporarily by **Rescan**.

- **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.

5.4. Logical

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

Name	Type	Secured Capacity	BlockSize	SectorSize	OS Name	Status
Device_1_E1_1	Hard Disk No	960.19 GB			HPT DISK 0_2	Legacy Maintenance
Device_1_E1_2	Hard Disk No	960.19 GB			HPT DISK 0_3	Legacy Maintenance

Location	Model	Secured	Capacity	Max Free
1/E1/1	KXD51RUE960G TOSHIBA	No	960.19 GB	0.00 GB
1/E1/2	KXD51RUE960G TOSHIBA	No	960.19 GB	0.00 GB

5.4.1. 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.

Name	Type	Secured Capacity	BlockSize	SectorSize	OS Name	Status
Device_1_E1_1	Hard Disk No	960.19 GB			HPT DISK 0_2	Legacy Maintenance
Device_1_E1_2	Hard Disk No	960.19 GB			HPT DISK 0_3	Legacy Maintenance

- **Name** – The physical disk location (e.g., Device 1_E1_1 represents the disk on AIC 1 port 1).
- **Type** – The type of the physical disk.
- **Secured** – Whether the physical disk or RAID array is secured.
- **Capacity** – The total capacity of the physical disk or RAID array.
- **BlockSize** – The block size of the array.
- **SectorSize** – The bytes per sector of the 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.

5.4.1.1. 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.

Logical Device Information

Name	Type	Secured Capacity	BlockSize	SectorSize	OS Name	Status
Device_1_E1_1 Hard Disk No	960.19 GB				HPT DISK 0_0	Legacy Maintenance
Device_1_E1_2 Hard Disk No	1.92 TB				HPT DISK 0_1	Legacy Maintenance
Device_1_E1_3 Hard Disk No	500.10 GB				HPT DISK 0_2	Legacy Maintenance
Device_1_E1_4 Hard Disk No					HPT DISK 0_3	Legacy Maintenance

Legacy Information

Device_1_E1_3	Init	Secure

Location 1/E1/1 **Model** Samsung SSD **Capacity** 960.19 GB **Max Free** 0.00 GB

4. After Disk Security has been enabled.

Logical Device Information

Name	Type	Secured Capacity	BlockSize	SectorSize	OS Name	Status
Device_1_E1_1 Hard Disk No	960.19 GB				HPT DISK 0_0	Legacy Maintenance
Device_1_E1_2 Hard Disk No	1.92 TB				HPT DISK 0_1	Legacy Maintenance
Device_1_E1_3 Hard Disk No	500.10 GB				HPT DISK 0_2	Legacy Maintenance
Device_1_E1_4 Hard Disk 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.

Create Array

Array Type: RAID 0 **Array Name:** Default **Secure:**

Initialization Method: Keep Old Data **Cache Policy:** **Block Size:** 512K

Available Disks:

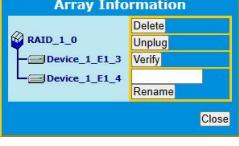
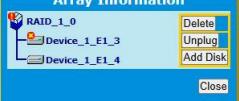
Location	Model	Capacity	Max Free
1/E1/1	Samsung SSD 983 DCT 960GB	960.19 GB	0.00 GB
1/E1/2	KIOXIA KCD81PUG1T92	1.92 TB	0.00 GB
1/E1/3	Samsung SSD 980 PRO 500GB	500.02 GB	500.02 GB
1/E1/4	KIOXIA KCD81PUG1T92	1.92 TB	0.00 GB

Capacity: (According to the max free space on the selected disks) **Maximum:** (MB)

Create

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

Table 3: Logical Device Status & Maintenance Options

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

5.4.2. 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.

Name	Type	Secured Capacity	BlockSize SectorSize	OS Name	Status
Device_1_E1_1	Hard Disk No	960.19 GB			HPT DISK 0_2 Legacy Maintenance
Device_1_E1_2	Hard Disk No	960.19 GB			HPT DISK 0_3 Legacy Maintenance

Location	Model	Secured	Capacity	Max Free
1/E1/1	KXD51RUE960G TOSHIBA	No	960.19 GB	0.00 GB
1/E1/2	KXD51RUE960G TOSHIBA	No	960.19 GB	0.00 GB

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

5.4.3. Create a RAID Array

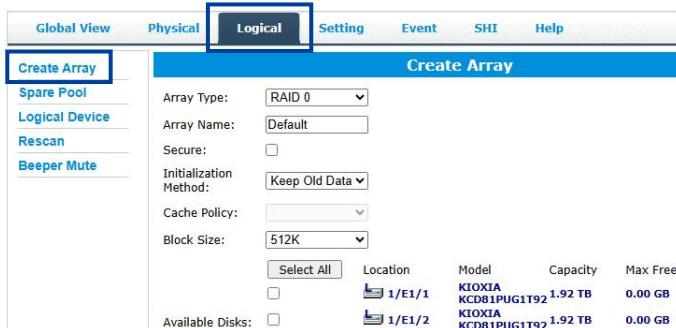
A RAID array is a collection of physical disks that will be one virtual disk by your Operating System. You need to follow the steps below to create a RAID array.

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.

5.4.3.1. Single AIC to create an array

To create a RAID array, perform the following steps:

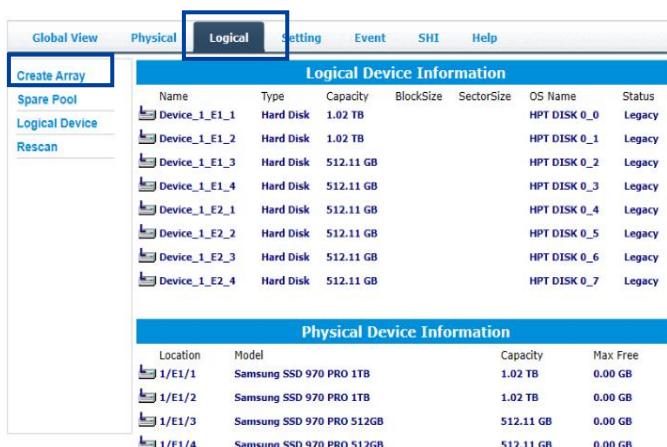
1. Open the **WebGUI**.
2. Select the proper **AIC** from the drop-down on the top left.
3. Click the **Logical** tab.
4. Click **Create Array**.



5.4.3.2. Use the Cross-Sync feature to create an array

To create a RAID array, perform the following steps:

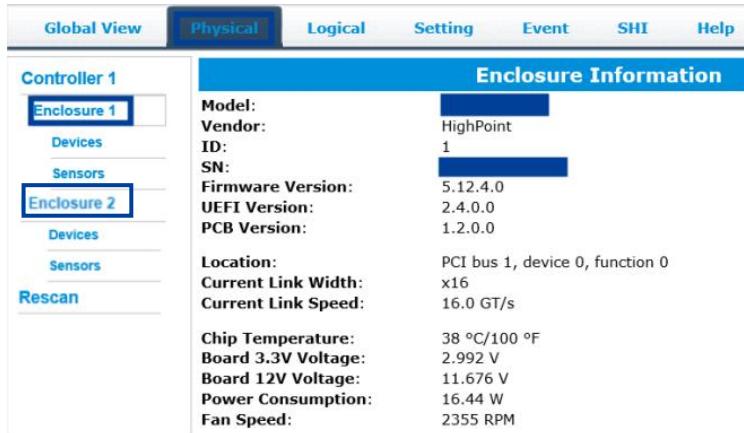
1. Open the **WebGUI**.
2. Select the proper **AIC** from the drop-down on the top left.
3. Click the **Logical** tab.
4. Click **Create Array**.



Notes:

You can view information about both controllers using the Physical tab.

The interface will refer to the controllers as "Enclosure 1" and "Enclosure 2".



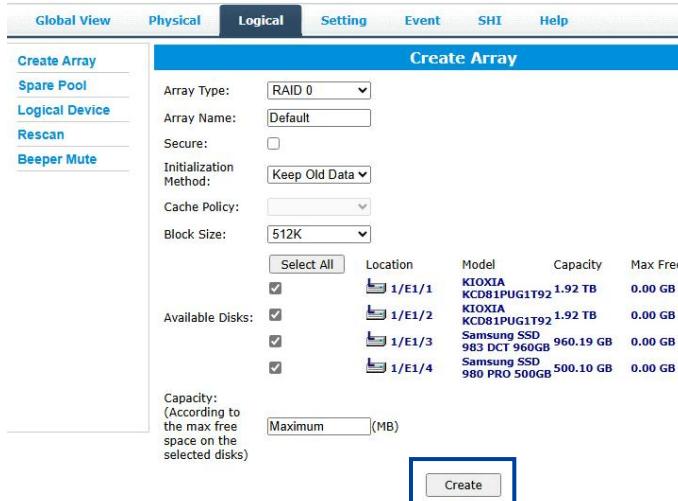
The following table describes the profile options.

Table 4: RAID Array Creation Profile Options

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

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

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



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

5.4.4. Delete a RAID Array

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

To delete a RAID array, perform the following steps:

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



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

Notes:

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

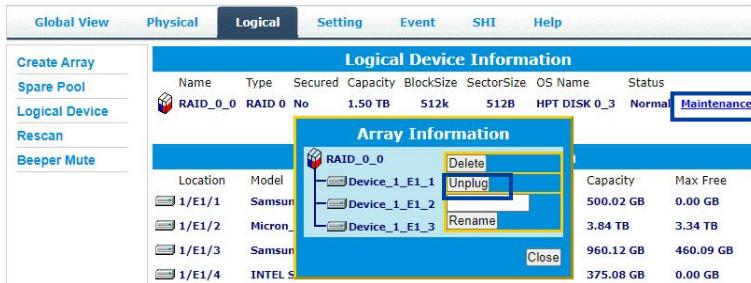
When the RAID array is mounted, deleting the RAID array will prompt in use. You can unmount it and continue to delete it.

5.4.5. Unplug a RAID Array

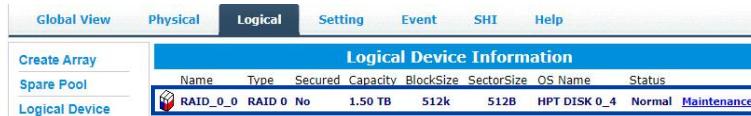
If you want to unplug the RAID array while the system works, use the Unplug first and then unplug the disks.

To unplug a RAID array, perform the following steps:

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



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



5.4.6. Verify a RAID Array

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

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

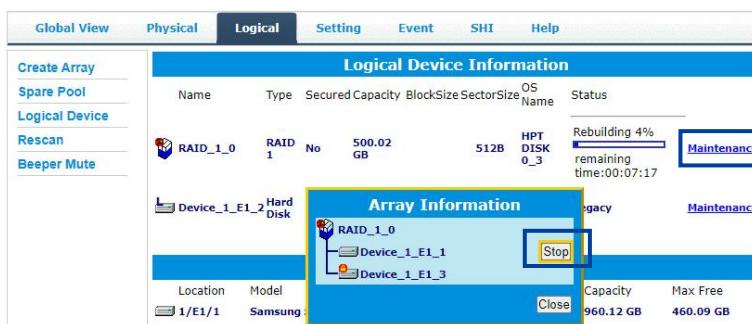
1. Open the **WebGUI**.
2. Click the **Logical** tab.
3. Click **Maintenance**.
4. Click **Verify** to verify the integrity of the RAID array.



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



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



5.4.7. 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**.

Available Disks			
<input type="checkbox"/>	Device_1_E1_1	Micron_9300_MTFDHAL3T8TDP	3.84 TB
<input type="checkbox"/>	Device_1_E1_2	KCM61RUL960G	960.12 GB
<input checked="" type="checkbox"/>	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**.

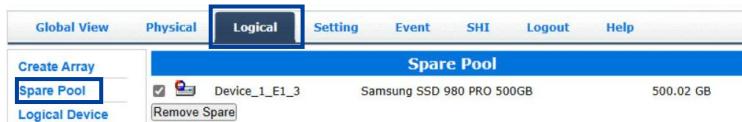
Available Disks			
<input type="checkbox"/>	Device_1_E1_1	Micron_9300_MTFDHAL3T8TDP	3.84 TB
<input type="checkbox"/>	Device_1_E1_2	KCM61RUL960G	960.12 GB

5.4.8. Remove a Spare Disk

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

To remove a spare disk, perform the following steps:

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



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

5.5. 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:**

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

Password Setting	
Password:	<input type="text"/>
Confirm:	<input type="text"/>
<input type="button" value="Submit"/>	

- **For Linux Users:**

System Setting	
Enable auto rebuild.	Enabled <input type="button" value="▼"/>
Enable Continue Rebuilding on error.	Enabled <input type="button" value="▼"/>
Enable audible alarm.	Enabled <input type="button" value="▼"/>
Restrict to localhost access.	Enabled <input type="button" value="▼"/>
Set Rebuild Priority:	Medium <input type="button" value="▼"/>
Port Number:	7402
Temperature Unit:	°F <input type="button" value="▼"/>
<input type="button" value="Submit"/>	

Password Setting	
Password:	<input type="text"/>
Confirm:	<input type="text"/>
<input type="button" value="Submit"/>	

5.5.1. System Setting

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

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

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

Table 5: System Setting Options

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

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

5.5.2. 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:	<input type="text"/>
Confirm:	<input type="text"/>
Submit	

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

5.5.3. Email Setting

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

5.5.3.1. Add an Email Server

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

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

Table 6: 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)

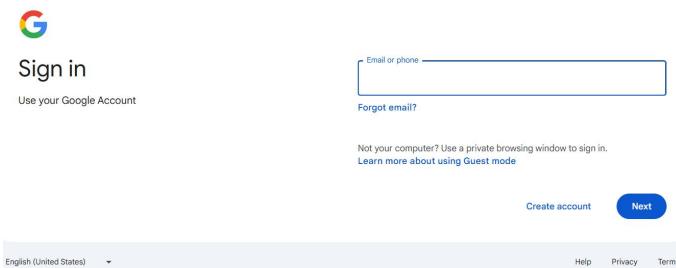
Support SSL	Check the Support SSL box if SSL is supported by your ISP (port value will change to 465; refer to your ISP if you have a specific SMTP port.)
--------------------	--

To add an email server, perform the following steps:

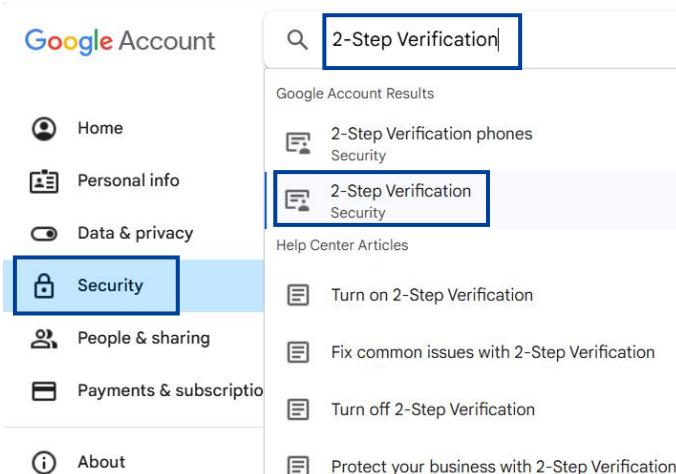
1. Open the **WebGUI**.
2. Click the **Setting** tab.
3. Check the **Enable Event Notification** box.
4. Enter the ISP server address or SMTP name in the **Server Address (name or IP)**.
5. Enter the email address of the sender (email account that is going to send the alert) in the **Mail From (E-mail 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: <https://accounts.google.com/Login>



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



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

← 2-Step Verification

Turn on 2-Step Verification

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



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

Turn on 2-Step Verification

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

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

← **App passwords**

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

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

[Learn more](#)

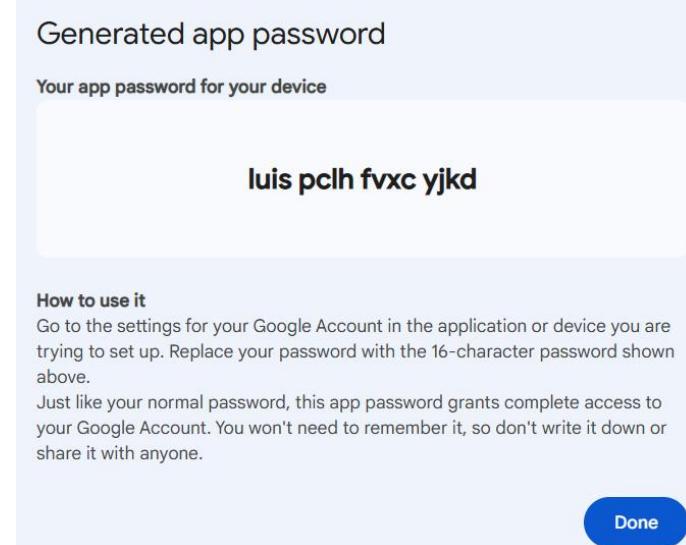
You don't have any app passwords.

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

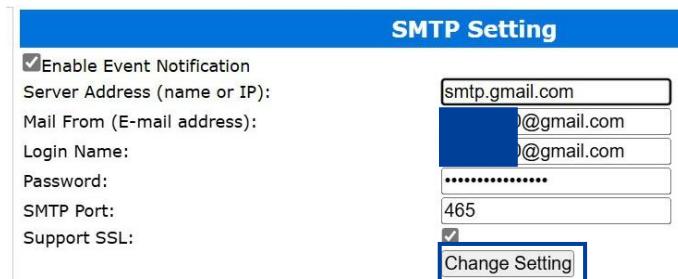
App name
HighPoint RAID Management

Create

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



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



The image shows a configuration screen titled 'SMTP Setting'. It includes the following fields:

- Enable Event Notification:**
- Server Address (name or IP):** smtp.gmail.com
- Mail From (E-mail address):** luis.perez@highpoint.com
- Login Name:** luis.perez@highpoint.com
- Password:** (redacted)
- SMTP Port:** 465
- Support SSL:**

At the bottom right is a blue 'Change Setting' button.

5.5.3.2. 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:	<input type="text"/>
Name:	<input type="text"/>
Event Level:	<input type="checkbox"/> Information <input type="checkbox"/> Warning <input type="checkbox"/> Error
<input type="button" value="Add"/> <input type="button" value="Test"/>	

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

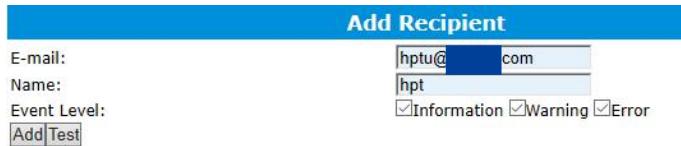
Table 7: Add Recipient Options

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 Recipient

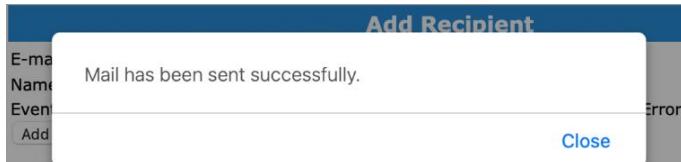
E-mail:

Name:

Event Level: Information Warning Error

Add **Test**

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



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

5.5.3.3. List all Email Recipients

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

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

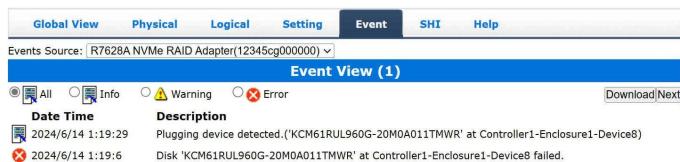
5.5.3.4. Delete an Email Recipient

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.

5.6. 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.



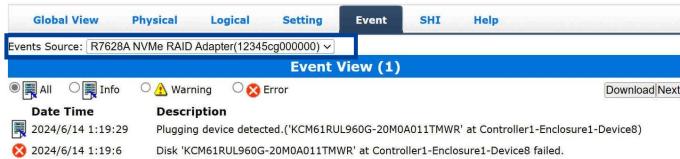
Event View (1)

Date Time	Description
2024/6/14 1:19:29	Plugging device detected.('KCM61RUL960G-20M0A011TMWR' at Controller1-Enclosure1-Device8)
2024/6/14 1:19:6	Disk 'KCM61RUL960G-20M0A011TMWR' at Controller1-Enclosure1-Device8 failed.

5.6.1. View the Event Log

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

You can switch between AIC event views by clicking on **Events Source**.



Event View (1)

Date Time	Description
2024/6/14 1:19:29	Plugging device detected.('KCM61RUL960G-20M0A011TMWR' at Controller1-Enclosure1-Device8)
2024/6/14 1:19:6	Disk 'KCM61RUL960G-20M0A011TMWR' at Controller1-Enclosure1-Device8 failed.

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

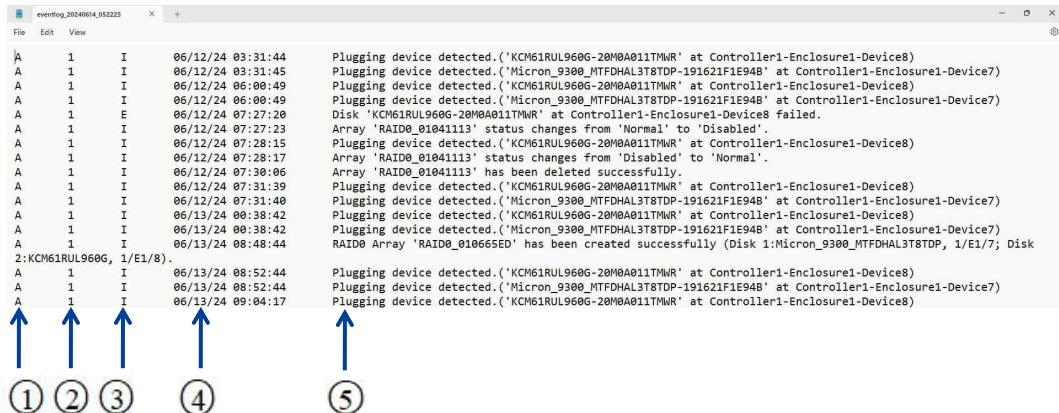
- **Prev** – View the previous log page
- **Next** – View the next log page

5.6.2. Save the Event Log

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



Open the downloaded event log.



The following table describes the Event Log.

Table 8: Event Log

No	Property Name	Description
①	Enclosure	Shows which specific Enclosure occurred the event.
②	Email delivery	Includes the followings: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> I – Information W – Warning E – Error
④	Event Time	Shows the exact time of the event.
⑤	Event Content	Shows the specifics of the event that occurred.

5.6.3. Event Log Icon Guide

The following table describes the Event Log Icon.

Table 9: Event Log Icon

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

5.7. 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.

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

5.7.1. 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.

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

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

5.7.2. View the SMART Information

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

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

Storage Health Inspector(SHI)						
Controller ID	Location#	Device Serial Number	RAID	°F	Total Bytes Written	S.M.A.R.T
1	E1_1	S48CNW0K400031X	RAID_1_0	91	192.85 TB	Detail
1	E1_2	XDR0A03D0UU1	RAID_0_0	95	14.80 TB	Detail
1	E1_3	S5GYNG0R206284E	RAID_1_0	86	109.04 TB	Detail
1	E1_4	XDR0A0370UU1	RAID_0_0	98	15.11 TB	Detail

NVME S.M.A.R.T Attributes	
Name	Value
Critical Warning	0x0
Composite Temperature (C)	37
Available Spare	100%
Available Spare Threshold	8%
Percentage Used	0%
Data Units Read	0x7af41cca
Data Units Written	0x1eef705
Host Read Commands	0x496eb26
Host Write Commands	0x1a2c25ca
Controller Busy Time	0xa14
Power Cycles	0xab
Power On Hours	0x7e
Unsafe Shutdowns	0x22
Media and Data Integrity Errors	0x0
Number of Error Information Log Entries	0x1
Warning Temperature Time	0x699
Critical Composite Temperature Time	0x0
Temperature Sensor 1 (C)	0
Temperature Sensor 2 (C)	0
Temperature Sensor 3 (C)	0
Temperature Sensor 4 (C)	0

5.7.3. View the TBW Information

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

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

1. Open the **WebGUI**.
2. Click the **SHI** tab.

Storage Health Inspector(SHI)						
Controller ID	Location#	Device Serial Number	RAID	°F	Total Bytes Written	S.M.A.R.T
1	E1_1	S48CNW0K400031X	RAID_1_0	91	192.85 TB	Detail
1	E1_2	XDR0A03D0UU1	RAID_0_0	95	14.80 TB	Detail
1	E1_3	S5GYNG0R206284E	RAID_1_0	86	109.04 TB	Detail
1	E1_4	XDR0A0370UU1	RAID_0_0	98	15.11 TB	Detail

5.7.4. Create a Health Inspector Scheduler

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

Storage Health Inspector(SHI)						
Controller ID	Location#	Device Serial Number	RAID	°F	Total Bytes Written	S.M.A.R.T
1	E1_3	S5GYNQGR206308X	RAID0_00A84D17	89	116.72 TB	Detail
1	E1_7	S5GYNQGR205478M	RAID0_00A84D17	82	322.93 TB	Detail

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

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

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

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

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

Health Inspector Scheduler

Task Name:

Occurs every: 1 Minute(s)

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

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

5.7.5. 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.

The screenshot shows a 'New Verify Task' dialog box. At the top, there is a radio button for 'Task Name' which is selected and contains the text 'RAID_1_0'. Below this, there is a radio button for 'Schedule' which is selected and contains the text 'Occurs every 1 Day(s) on Sunday at 2:00:00'. At the bottom of the dialog box is a 'Submit' button.

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

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

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

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

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

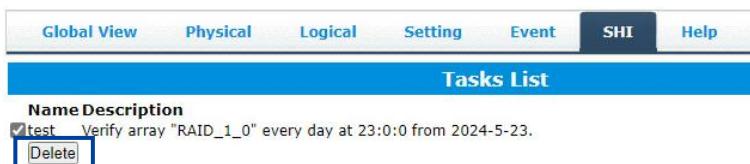
5.7.6. Delete a Task

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.



5.8. Help



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

5.8.1. Online Help

Online Help redirects you to the official HighPoint website.

5.8.2. Diagnostic View

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

Global View	Physical	Logical	Setting	Event	SHI	Help
Diagnostic View						
System				Product		
OS:	Microsoft Windows 11 Pro			Controller:	HighPoint NVMe RAID Controller	
Kernel:	10.0.22631			Driver Name:	hptnvme	
CPU:	AMD EPYC 7542 32-Core Processor			Driver Version:	1.5.0.0	
MotherBoard:	ASRockRack ROMED8-2T					
SystemModel:	To Be Filled By O.E.M. To Be Filled By O.E.M.					
BIOS:	American Megatrends Inc. P3.20 AMD - 3242016					
Disk:	Samsung SSD 860 PRO 256GB 238.467911GB					
Chipset:	Advanced Micro Devices					
Logs Location:	Logs have not been saved			<input type="button" value="Save Log"/>		

5.8.3. 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.

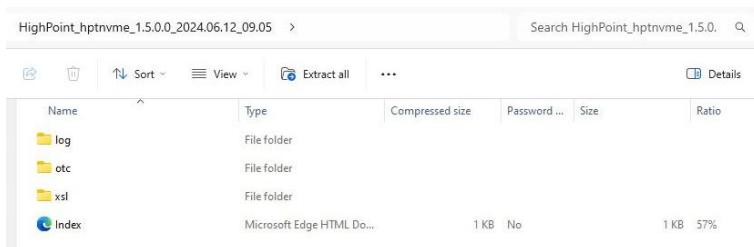
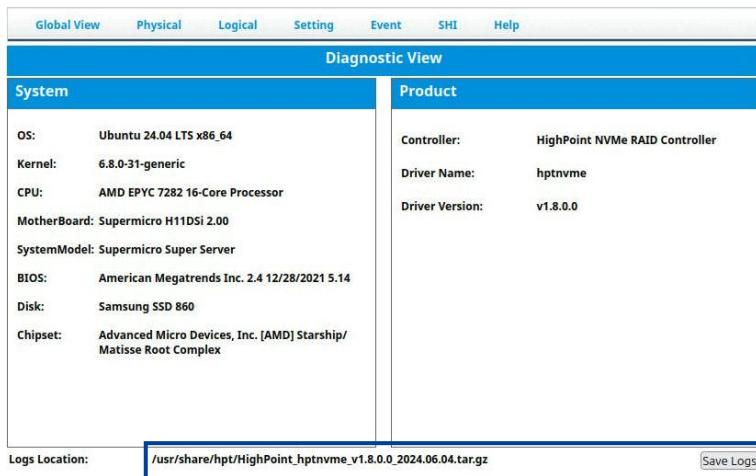


Table 10: Description of each folder in the log zip file (Windows)

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

● For Linux User



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

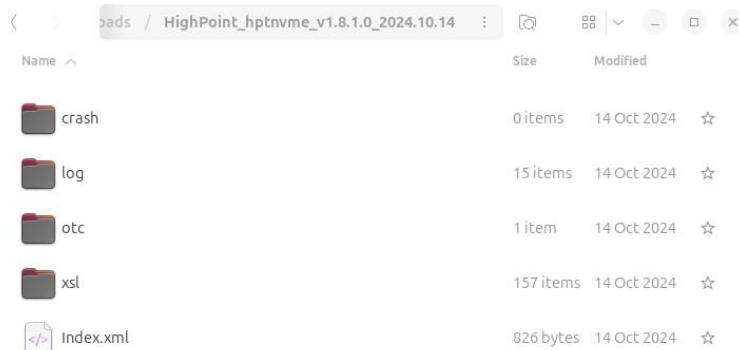


Table 11: Description of each folder in the log zip file (Linux)

Folder	Property	Description
log	cpu_info	CPU configuration of the current system.
	disk_info	Number and names of disks in the current system.
	dmesg_info	The kernel log for the current system boot.
	dmidecode_info	Instructions to view hardware information, BIOS, system, motherboard, processor, memory, cache, etc.
	hpt_xxxx.log	AIC log information, including creation/deletion of RAID and exception events. xxx is the SN number of AIC.
	hpt_diag.log	Collect the runtime logs of management software to detect any abnormalities.
	hpt_HighPoint.log	Collect the AIC log.
	hpt_temperature.log	Collects chip and disk temperature information to monitor thermal conditions.
	hptdrv.log	HighPoint driver installation log.

	hptdrv-cron.log	Collect HighPoint driver auto-upgrade log.
	hptsvr-install.log	Collect HighPoint RAID Management software installation log.
	kern.log	System kernel log.
	lsmod info	Record all driver information used in Linux.
	lspci_info	Information about the PCIe device connected to the motherboard.
	syslog	Collect kernel log and some other application log information.
Index.xml	RAID Management web page	<p>HTML webpage, record the screenshot information of each page of this WebGUI</p> <ul style="list-style-type: none"> ● Diagnostic View—CPU, Motherboard model, BIOS, driver version. ● Global view—Record disk and RAID utilization. ● Physical—Record the RAID Controller and disk PCIe width. ● Logical—Record the RAID status and the member of the RAID. ● Setting—Record the status of the WebGUI function setting. ● Event—Record activity log in WebGUI. ● SHI—Record the smart info of disks.
xsl	RAID Management web page	It contains components that allow local html files to be opened.
crash	N/A	It contains logs saved by the Linux system crash.
otc	0-switch	<ul style="list-style-type: none"> ● event.txt—Collect sensor information every minute, including power voltage, fan speed, and temperature. ● info.txt—Collect AIC information, including firmware, SN, firmware version, chip/board temperature, voltage/power, and fan speed. ● log.txt—AIC log, including RAID operation, disk drop, fan speed abnormal, temperature abnormal, voltage abnormal. ● Port.txt—AIC downstream port info, including width, speed, and PCIe configuration space. ● trace.txt—Collect firmware runtime log. ● {sn}.bin—AIC factory data, including the initial setup parameters.

6. 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, 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.

6.1. Start the CLI

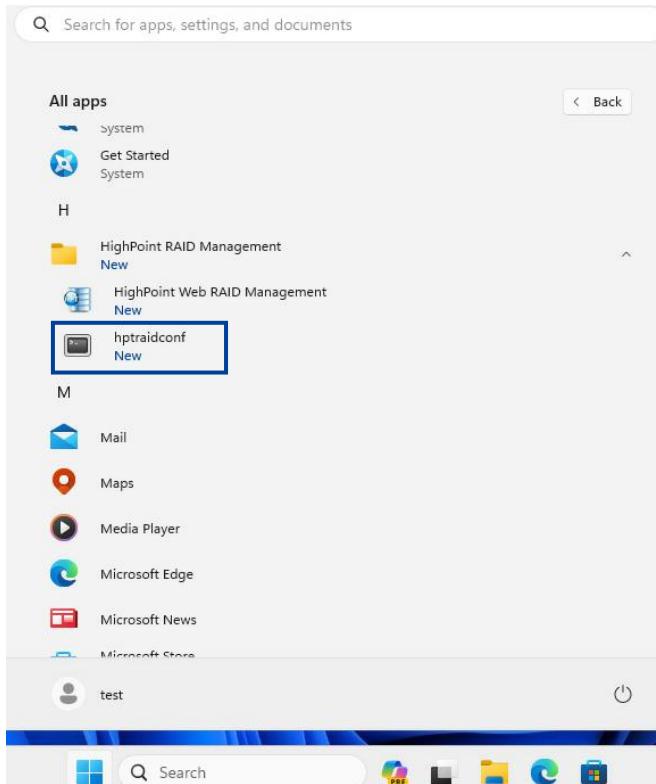
For Windows Users

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

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22631.3447]
(c) Microsoft Corporation. All rights reserved.

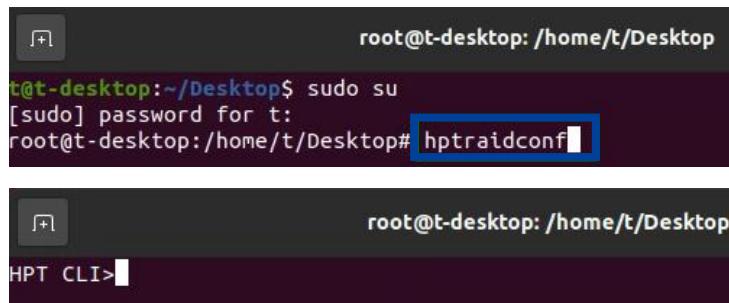
C:\Windows\System32\hptraidconf
```

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



For Linux Users

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



The image consists of two vertically stacked screenshots of a Linux terminal window. The terminal has a dark background with light-colored text. The top screenshot shows the command line with the prompt `t@t-desktop:~/Desktop$`, followed by the command `sudo su`, and then the password prompt `[sudo] password for t:`. The bottom screenshot shows the command line with the prompt `root@t-desktop:~/Desktop#`, followed by the command `hptraidconf`. A blue rectangular box highlights the `hptraidconf` command in the bottom screenshot. The terminal window has a small icon in the top-left corner and a tab labeled `root` in the top-right corner.

6.2. Query Commands

```

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

```

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

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

Table 12: Properties for query Command

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

6.2.1. Query Controller

HPT CLI>query controllers

This command reports AIC information.

Input example:

```
HPT CLI>query controllers
```

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

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

6.2.2. Query Enclosure

HPT CLI>query enclosures

This command reports AIC Product ID information.

Input example:

```
HPT CLI>query enclosures
```

ID	Secure	VendorID	ProductID	NumberOfPYH
1/E1	Yes	HPT	R7628A NVMe RAID Adapter	8
1/E2	Yes	HPT	R7628A NVMe RAID Adapter	8

- **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.

HPT CLI>query enclosures {enclosure_id}

This command presents information of the specified AIC.

Input example:

```
HPT CLI>query enclosures 1/E1
```

HPT CLI>query enclosures 1/E1	
Model:	██████████
Vendor:	HighPoint
ID:	1/E1
Vendor ID:	0x1103
Device ID:	0x7604
Location:	PCI bus 5, device 0, function 0
Current Link Width:	x8
Current Link Speed:	8.0 GT/s
SN:	██████████
Firmware Version:	5.15.12.0
UEFI Version:	2.5.1
Chip Temperature:	48 (C)/118 (F)
PCB Version:	1.1
Board 3.3V Voltage:	3.252 V
Board 12V Voltage:	12.068 V
Power Consumption:	19.52 W
Fan Speed:	Auto(2310 RPM)

Vital Product Data	
Product Name:	HighPoint ██████████
[PN] Part number:	R7604A-72C0000
[EC] Engineering changes:	0000
[MN] Manufacture ID:	1103
[SN] Serial number:	██████████
[V0] Vendor specific:	HighPoint Technologies
[V1] Vendor specific:	Broadcom PEX89048

- **Model** — The name of the AIC.
- **Vendor** — The manufacturer of the AIC.
- **ID** — An AIC ID is a string used to represent an AIC. It is in the format “1/AIC” for AICs.
- **Vendor ID** - An AIC property indicating the vendor-assigned ID number of the AIC.
- **Device ID** - The device ID of the AIC.
- **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.
- **SN** — The serial number of the AIC.
- **Firmware Version** — The firmware version of the AIC.
- **UEFI Version** — The UEFI version of the AIC
- **PCB Version** — The hardware version of the AIC.
- **Chip Temperature** — The temperature of the AIC’s chip.
- **Board 3.3V Voltage** — The board 3.3V voltage of the AIC. When the voltage exceeds 3.3V ($\pm 8\%$), the voltage is displayed in red.
- **Board 12V Voltage** — The board 12V voltage of the AIC. When the voltage exceeds 12V ($\pm 8\%$), the voltage is displayed in red.
- **Power Consumption** — Total power consumption of the AIC, disks, and external power supply (provided by the PCIe host interface)
- **Fan Speed** — The current fan speed of the AIC.

Vital Product Data

- **Product Name** — The name of the AIC.
- **[PN] Part number** — The part number of the AIC.
- **[EC] Engineering changes** — The engineering change of the AIC.
- **[MN] Manufacture ID** — The manufacture ID of the AIC.
- **[SN] Serial number** — The serial number of the AIC.
- **[V0] Vendor specific** — The manufacturer of the AIC.
- **[V1] Vendor specific** — The chip model of the AIC.

6.2.3. 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_MTFDHAL3T8TDP
1/E1/3	No	500.03	0	RAID	NORMAL	Samsung SSD 980 PRO 500GB
1/E1/4	Yes(locked)	375.08	0	SINGLE	NORMAL	INTEL SSDPE21K375GA
1/E2/1	No	960.13	460.10	RAID	NORMAL	Samsung SSD 983 DCT 960GB
1/E2/2	No	3840.76	0	SINGLE	LEGACY	Micron_9300_MTFDHAL3T8TDP
1/E2/3	No	500.03	0	RAID	NORMAL	Samsung SSD 980 PRO 500GB
1/E2/4	Yes(locked)	375.08	0	SINGLE	NORMAL	INTEL SSDPE21K375GA

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

HPT CLI>query devices {device_id}

This command presents information for the specified physical disk.

Input example:

HPT CLI>query devices 1/E1/1

```
HPT CLI > query devices 1/E1/1
Mode Number:      Samsung SSD 983 DCT 960GB
Serial Number:   [REDACTED]
Firmware Version: EDA5102Q
Capacity(GB):    960.13      TotalFree(GB): 460.10
Status:          RAID        Flag:      NORMAL
SED Capable:    Yes         SED Type:  OPAL
Secured:        No          Cryptographic Erase Capable: Yes
PCIe Width:     x4          PCIe Speed: 8.0 GT/s
Temperature (F): 96
Warning Composite Temperature Threshold (F): 188
Critical Composite Temperature Threshold (F): 190
-----
S.M.A.R.T Attributes
Name                  Value
-----
Critical Warning      : 0x0
Composite Temperature (C) : 36
Available Spare       : 100%
Available Spare Threshold : 10%
Percentage Used       : 2%
Data Units Read       : 0x5abab7f0
Data Units Written    : 0x18af2e09
Host Read Commands   : 0x36d452ab7
Host Write Commands  : 0xba7fefef9
Controller Busy Time : 0x4c6a
Power Cycles          : 0xecb
Power On Hours        : 0xab8
Unsafe Shutdowns      : 0xadd
Media and Data Integrity Errors : 0x0
Number of Error Information Log Entries : 0x43d2
Warning Temperature Time : 0x0
Critical Composite Temperature Time : 0x0
Temperature Sensor 1 (C) : 36
Temperature Sensor 2 (C) : 40
Temperature Sensor 3 (C) : 45
Temperature Sensor 4 (C) : 0
Temperature Sensor 5 (C) : 0
Temperature Sensor 6 (C) : 0
Temperature Sensor 7 (C) : 0
Temperature Sensor 8 (C) : 0
```

- **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.

6.2.4. 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

ID	Secured	Capacity(GB)	Type	Status	Block	Sector	Cache	Name
1	No	7681.01	RAID0	NORMAL	512k	512B	NONE	RAID_0_0

HPT CLI>query arrays {arrays_id}

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

Input example:

HPT CLI>query arrays 1

ID	Secured	Capacity(GB)	Type	Status	Block	Sector	Cache	Name
1	No	239.98	RAID1	NORMAL	--	512B	NONE	[RAID10_0]
1-2	No	239.98	RAID1	NORMAL	--	512B	NONE	[RAID10_0]
1-3	No	239.98	RAID1	NORMAL	--	512B	NONE	[RAID10_0]
1-4	No	239.98	RAID1	NORMAL	--	512B	NONE	[RAID10_0]
1-5	No	239.98	RAID1	NORMAL	--	512B	NONE	[RAID10_0]
1-6	No	239.98	RAID1	NORMAL	--	512B	NONE	[RAID10_0]
1-7	No	239.98	RAID1	NORMAL	--	512B	NONE	[RAID10_0]
1-8	No	239.98	RAID1	NORMAL	--	512B	NONE	[RAID10_0]

- **ID** - The array's ID. A number generally represents an array ID.
- **Secured** - Whether the array is secured.
- **Capacity** - The capacity of the array in 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.

6.3. Init Commands

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

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

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

Table 13: Properties for init Command

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

6.3.1. Init a Physical Disk

HPT CLI>init {device_id}

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

Input example:

HPT CLI>init 1/E1/1

```
HPT CLI > query devices
ID Secured Capacity MaxFree Flag Status ModelNumber
-- 
1/E1/1 No 960.13 460.10 RAID NORMAL Samsung SSD 983 DCT 960GB
1/E1/2 No 3840.76 0 SINGLE LEGACY Micron 9300_MTFDHAL3T8TDP
1/E1/3 No 500.03 0 RAID NORMAL Samsung SSD 980 PRO 500GB
1/E1/4 Yes(locked) 375.08 0 SINGLE NORMAL INTEL SSDPE21K375GA
-- 

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

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

6.3.2. 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
```

6.4. Create Command

```

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

```

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

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

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

Table 14: Properties for create Command

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

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

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

6.4.1. Create a RAID Array

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

This command allows you to create a new RAID array.

Input example:

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

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

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

6.4.2. Create a Spare Disk

HPT CLI>create spare {device_id}

This command allows you to add a spare disk.

Input example:

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

HPT CLI > create spare disks=1/E1/1						
Add spare disk successfully.						
HPT CLI > query devices						
ID	Secured	Capacity	MaxFree	Flag	Status	ModelNumber
1/E1/1	No	1000.12	1000.12	SINGLE	SPARE	Samsung SSD 980 PRO 1TB
1/E1/2	No	4096.73	4096.73	SINGLE	NORMAL	KXG80ZNN84T09 KIOXIA
1/E1/3	No	2000.31	2000.31	SINGLE	NORMAL	HP-EM2802T0GMTCBS8R-E264
1/E1/4	No	1024.08	1024.08	SINGLE	NORMAL	KXG60ZNV1T02 TOSHIBA
1/E1/5	No	2000.31	2000.31	SINGLE	NORMAL	CT2000T7085SD
1/E1/6	No	1000.12	1000.12	SINGLE	NORMAL	CT1000T7085SD
1/E1/7	No	1000.12	1000.12	SINGLE	NORMAL	Seagate FireCuda 530 2TB 1000GM30013
1/E1/8	No	239.98	239.98	SINGLE	NORMAL	WDC WD5240G260C-00AJM0
1/E1/9	No	2000.31	2000.31	SINGLE	NORMAL	HP-EM2802T0GMTCBS8R-E264
1/E1/10	No	2000.31	2000.31	SINGLE	NORMAL	HP-EM2802T0GMTCBS8R-E264
1/E1/11	No	1000.12	1000.12	SINGLE	NORMAL	Sabrent Rocket 4.0 1TB
1/E1/12	No	1000.12	1000.12	SINGLE	NORMAL	WD Red SN700 1000GB
1/E1/13	No	2000.31	2000.31	SINGLE	NORMAL	HP-EM2802T0GMTCBS8R-E26P4
1/E1/14	No	500.03	500.03	SINGLE	NORMAL	Samsung SSD 970 EVO Plus 500GB
1/E1/15	No	512.04	512.04	SINGLE	NORMAL	Samsung SSD 970 PRO S12GB
1/E1/16	No	2000.31	2000.31	SINGLE	NORMAL	HP-EM2802T0GMTCBS8R-E264

6.5. 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 15: 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.

6.5.1. Delete a RAID Array

HPT CLI>delete {array id}

This command allows you to delete an existing RAID array.

Input example:

HPT CLI>delete 1

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

HPT CLI > delete 1
Delete array(1) successfully!
```

6.5.2. 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	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	KXG60ZN1V1T02 TOSHIBA
/E1/5	No	2000.31	2000.31	SINGLE	NORMAL	CT2000T7005SD3
/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 WDS240G2G0C-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

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

ID	Secured	Capacity	MaxFree	Flag	Status	ModelNumber
/E1/1	No	1000.12	1000.12	SINGLE	NORMAL	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	KXG60ZN1V1T02 TOSHIBA
/E1/5	No	2000.31	2000.31	SINGLE	NORMAL	CT2000T7005SD3
/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 WDS240G2G0C-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

6.6. Rebuild Command

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

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

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

Table 16: Properties for rebuild Command

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

6.6.1. Rebuild a RAID array

HPT CLI>rebuild {array_id} {device_id}

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

Input example:

HPT CLI>rebuild 1 1/E1/4

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

HPT CLI > rebuild 1 1/E1/4

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

6.6.2. Start Rebuilding the RAID Array

HPT CLI>rebuild {array id} {start}

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

Input example:

```
HPT CLI>rebuild 1 start
```

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

6.6.3. 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!
```

6.7. 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 17: Properties for verify Command

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

6.7.1. Start Verifying the RAID Array

HPT CLI>verify {array_id} {start}

This command starts the verification process on the specified array.

Input example:

HPT CLI>verify 1 start

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

6.7.2. Stop Verifying the RAID Array

HPT CLI>verify {array_id} {stop}

This command stops the verification process on the specified array.

Input example:

HPT CLI> verify 1 stop

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

6.8. 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 18: Properties for rescan Command

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

6.8.1. Rescan the Physical Devices

HPT CLI>rescan

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

Input example:

HPT CLI> rescan

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

6.9. Lscard Command

```

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

```

The lscard command is used to list multiple AICs.

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

Table 19: Properties for lscard Command

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

6.9.1. Lscard all AICs

HPT CLI>lscard

This command displays the list of multiple AICs.

Input example:

HPT CLI>lscard

```

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

```

6.10. Events Command

HPT CLI > events

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 20: Properties for events Command

cmd	Property Name	Value Range	Description
events	{enclosure_id}	The AIC in use	<p>This command will display the events log for the selected page number, displaying 20 log messages per page.</p> <p>Event Level:</p> <ul style="list-style-type: none"> - Inf (Information) - War (Warning) - Err (Error)
	pages	0~*	
events	save=	N/A	This command will save all the logged events as a plain text file.
	{enclosure_id}	The specified AIC	
	{file_name}	File path	

6.10.1. View the Event Log

[HPT CLI>events {enclosure_id} pages=*](#)

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

Input example:

HPT CLI>events 1/E1 page=0

```
HPT CLI > events 1/E1 page=0
1 Inf [05/22/2024 22:44:01]           Array 'RAID_1_0' status changes from 'Verifying' to 'Normal'.
2 War [05/22/2024 22:44:00]           Array 'RAID_1_0' verifying aborted.
3 Inf [05/22/2024 22:43:34]           Array 'RAID_1_0' status changes from 'Normal' to 'Verifying'.
4 Inf [05/22/2024 22:43:33]           Array 'RAID_1_0' verifying started.
5 Inf [05/22/2024 22:43:22]           Array 'RAID_1_0' status changes from 'Rebuilding' to 'Normal'.
6 Inf [05/22/2024 22:43:20]           Array 'RAID_1_0' rebuilding completed.
```

6.10.2. Save the Event Log

HPT CLI>events {enclosure_id} save={file_name}

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

Input example:

```
HPT CLI> events 1/E1 save=C:/raidlog.txt
```

```
HPT CLI > events 1/E1 save=C:/raidlog.txt
The event log C:/raidlog.txt has been saved.
```

6.11. Mail Command

```

APT CLI > mail
Mail Commands
  Set a mail recipient to get the e-mail from system.

Syntax:
  mail recipient
  mail recipient add {recipient_name} {mail_address} [Inf|War|Err]
  mail recipient delete {recipient_name}
  mail recipient test {recipient_name}
  mail server
  mail server set {server_address} {port} {ssl} {e|d} {from_address} {username} {password}
  mail server set {a|p|s|m|u|t} {value}

```

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

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

Table 21: Properties for mail Commands

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

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

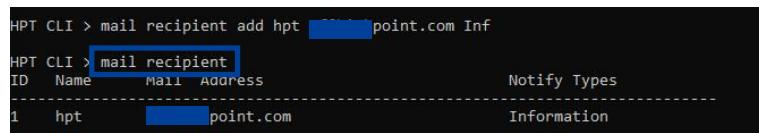
6.11.1. Add a Mail Recipient

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
```



ID	Name	Mail Address	Notify Types
1	hpt	[REDACTED]point.com	Information

6.11.2. List all Mail Recipients

HPT CLI>mail recipient

This command will display a list of all mail recipients.

Input example:

```
HPT CLI> mail recipient
```



ID	Name	Mail Address	Notify Types
1	hpt	[REDACTED]point.com	Information

6.11.3. 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
```

6.11.4. Delete a Mail Recipient

HPT CLI>mail recipient delete {recipient_name}

This command will delete an existing mail recipient.

Input example:

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

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

HPT CLI > mail recipient delete hpt

HPT CLI > mail recipient
ID  Name      Mail Address          Notify Types
-----
```

6.11.5. 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
```



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

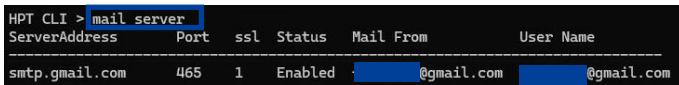
6.11.6. List all Mail Servers

HPT CLI>mail server

This command will configure mail server settings.

Input example:

```
HPT CLI> mail server
```



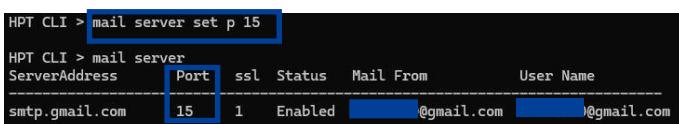
6.11.7. Set the Mail Server

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
```



6.12. Task Command

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

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

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

Table 22: 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}	<p>This command allows you to schedule a specified array.</p> <p><i>Note: When you add a task to rebuild a selected array once, the parameter {day} should be omitted.</i></p>
task	verify	{options}	<p>This command allows you to schedule a verification task.</p>
	{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	<p>The task start date.</p> <ul style="list-style-type: none"> - yyyy - year - dd - day - mm - month - hh - hour - mm - minute - ss - second
		end=mm/dd/yyyy time=hh:mm:ss	The task end date.

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

6.12.1. Create a New Rebuild Task

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

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

Input example:

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

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

6.12.2. Create a New Verify Task

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

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

Input example:

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

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

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

6.12.3. List all Tasks

HPT CLI>task

This command displays detailed information about all scheduled tasks.

Input example:

HPT CLI>task

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

6.12.4. Delete a Task

HPT CLI>task delete {task_id}

This command allows you to delete a scheduled task.

Input example:

```
HPT CLI>task delete 2
```

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

6.13. Set Command

```

set Command
  Set the system, device or array's param.

Syntax:
  set
    show the system parameters
  set {name=}
    set AR=[y|n]          Auto Rebuild
    set CE=[y|n]           Continue Rebuild On Error
    set AA=[y|n]           Audible Alarm
    set SS=[y|n]           Staggered spinup
    set DS=[seconds]      Delay between spinup (seconds)
    set ND=[number]       Number of drives per spinup
    set IT=[y|n]           INT 13 support
    set SB=[y|n]           Single BCV entry
    set NC=[y|n]           NCQ
    set BP=[y|n]           Beeper
    set RP=[1-100]          Rebuild Priority
    set BR=[1-100]          Background Rate
    set SD=[minutes]       Spindown Idle Disk (minutes)
    set TU=[C|F]           Temperature Unit
    set PS                 set Password
    set RL=[y|n]           Restrict to localhost access
    set PUIS=[y|n] disks={device_id}      set disk's PUIS feature
    set LED=[y|n] disk={device_id}  identify LED on(y) or off(n)
  set {device id} {name=}
    set tcq=[y|n]          set TCO enable or disable.
    set ncq=[y|n]           set NCQ enable or disable.
    set wc=[y|n]            set Write Cache enable or disable.
    set ra=[y|n]            set Read Ahead enable or disable.
    set smart=[y|n]          set smart enable or disable.
  set {array id} name={name} cp=[wt|wb|none]
    name   Set the array's name.
    cp     Set array's cache policy.
  set {enclosure id} FS=[Auto|ULow|Low|Medium|High|Full]      Enclosure Fan Speed
  set {enclosure id} Param          display all enclosure parameter settings
  set {enclosure id} Param {ID}={Option}  set enclosure parameter

```

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

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

Table 23: Properties for set Commands

cmd	Property	Value Range	Description
set	AR	[y n]	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	[y n]	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

		<p>the procedure. HighPoint recommends checking the event log periodically for bad sector warnings if this option is enabled.</p>
AA	[y n]	<p>Set enable or disable to the [Audible Alarm] parameter.</p> <p>The audible alarm sounds when the following conditions occur:</p> <ul style="list-style-type: none"> - Disk Dropped - Fan Speed lower than 600 RPM - SSD Temperature is higher than the SSD warning threshold - Broadcom Chipset Temperature is higher than 105°C <p> Warning: Disabled audible alarm is permanently disabling the beeper, so please proceed with caution!</p>
BP	[y n]	<p>Set enable or disable [Beeper].</p> <p>When a disk drop triggers the beeper.</p>
RP	[1-100]	<p>Change [Rebuilding Priority]. If an AIC is not specified, this command will set the global rebuilding priority.</p> <p>[1-12] Lowest</p> <p>[13-37] Low</p> <p>[38-67] Medium</p> <p>[68-87] High</p> <p>[>88] Highest</p>
TU	[C F]	<p>Set the [Temperature Unit] to Celsius or Fahrenheit.</p> <p>This setting is only supported by the Windows HighPoint RAID Management.</p>
CL	[y n]	<p>Set enable or disable [Collecting System Logs].</p> <p>You can set it to enable the collection of system logs at any time. The collected system logs are stored on C:/Windows/hpt_diagdriver. The maximum size of the collected system log is 840MB; anything over 840MB will be overwritten forward.</p> <p>This setting is only supported by the Windows HighPoint</p>

			<p>RAID Management.</p> <p>It is used as follows:</p> <ol style="list-style-type: none"> 1. Set CL to Enabled. 2. Reboot the system. 3. Duplicate the problems encountered. 4. Collect system logs with one click.
PS	{password}		<p>Set or change your [Password]. The password is ≤ 8 characters.</p>
RL	[y n]		<p>Set enable(y) or disable(n) [Restrict to localhost access].</p> <p>Remote access to the AIC will be restricted when enabled; other users in your network cannot log in to the WebGUI remotely.</p> <p>It is used as follows:</p> <ol style="list-style-type: none"> 1. Set RL=n. 2. Reboot the system. 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.
LED	LED={y n}		<p>Set the identify the [LED] on(y) or off(n).</p>
	disks={device_id}		<p>Identify the location of the disk. When the LED is set to y, the disk LED will light up red to get the location of the disk. When the LED is set to n, the disk LED turns off.</p>
FS	{enclosure_id}=		<p>Change the AIC Fan Speed. This supports setting different levels of fan speed {Auto Off Low Medium High Full}</p> <p>Note: If you are using RS6541AW then here are the following 5 levels [Auto, Ultra Low, Low, Medium, High, Full]</p>
Param	{enclosure_id}		<p>Display or set the AIC parameter settings.</p>
	Parameter ID	2001	<p>This Parameter Setting supports setting the Hotplug compatibility mode and LED (Status/ Fault/ SSD) on/off.</p>

			2003	Status LED	<p>Notes:</p> <p>Enabled Hotplug compatibility mode causes performance degradation on all disks hosted by the AIC.</p> <p>LED Enable indicates: The Status LED/ Fault LED/ SSD LED functions works normally and provide status feedback on the disk, AIC bandwidth, and disk temperature, etc.</p> <p>LED Disable indicates: The Status LED/ Fault LED/ SSD LED does not work and cannot provide any status feedback on the disk, AIC bandwidth, and disk temperature, etc.</p>
			2004	Fault LED	
			2005	SSD LED	
			{Option}={Enable Disable}		
smart	[y n]				Set smart enable or disable.

6.13.1. Set Auto Rebuild

HPT CLI>set AR=[y|n]

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

Input example:

```
HPT CLI>set AR=y
```

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

6.13.2. Set Continue Rebuilding On Error

HPT CLI>set CE=[y|n]

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

Input example:

```
HPT CLI>set CE=y
```

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

6.13.3. Set Audible Alarm

HPT CLI>set AA=[y|n]

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

Input example:

```
HPT CLI>set AA=n
```

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

6.13.4. Set Beeper

HPT CLI>set BP=[y|n]

Set enable or disable **beeper**.

Input example:

```
HPT CLI>set BP=n
```

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

6.13.5. Set Rebuild Priority

HPT CLI>set RP=[1-100]

Change rebuilding priority.

Input example:

```
HPT CLI>set RP=60
```

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

6.13.6. Set Temperature Unit

HPT CLI>set TU=[C|F]

Set the temperature unit to Celsius or Fahrenheit.

Input example:

```
HPT CLI>set TU=C
```

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

6.13.7. Set Collecting System Logs

HPT CLI>set CL=[y|n]

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

It is used as follows:

1. Set CL to Enabled(y).

Input example:

HPT CLI>set CL=y

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

2. Reboot the system.
3. Duplicate the problems encountered.
4. Collect system logs with one click.

6.13.8. Set Password

HPT CLI>set PS={password}

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

Input example:

HPT CLI>set PS=00000000

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

6.13.9. Set Identify LED

HPT CLI>set LED={y|n} disk={device id}

Identify the location of the disk. When the LED is set to **y**, the disk LED will light up red to get the location of the disk. When the LED is set to **n**, the disk LED turns off.

Input example:

```
HPT CLI>set LED=y disk=1/E1/4
```

```
HPT CLI > set LED=y disk=1/E1/4
```

6.13.10. Set AIC Fan Speed

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

Change the AIC Fan Speed.

Input example:

```
HPT CLI>set 1/E1 FS=Low
```

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

6.13.11. Set Hotplug Compatibility Mode

HPT CLI>set {enclosure id} Param {ID}={Option}

This Parameter Setting supports setting the **Hotplug compatibility mode**.

Input example:

```
HPT CLI>set 1/E1 Param 2001=Enabled
```

```
HPT CLI > set 1/E1 Param 2001=Enabled  
Parameter set successfully! It will take affect after reboot.
```

```
HPT CLI > set 1/E1 Param  
ID: 2001  
Name: Hotplug compatibility mode  
Option: Disabled/Enabled  
Value: Enabled  
Description: If you experience issues when hot-plugging NVMe devices, please try enabling this option to resolve the problem.
```

6.13.12. Set Status/ Fault/ SSD LED On/Off

HPT CLI>set {enclosure id} Param {ID}={Option}

This **Parameter Setting** supports setting the **Status LED/ Fault LED/ SSD LED On/Off**. You can switch on and off the AIC LED.

Notes:

Enable indicates: The Status LED/ Fault LED/ SSD LED functions works normally and provide status feedback on the disk, AIC bandwidth, and disk temperature, etc.

Disable indicates: The Status LED/ Fault LED/ SSD LED does not work and cannot provide any status feedback on the disk, AIC bandwidth, and disk temperature, etc.

Input example:

HPT CLI>set 1/E1 Param 2003=Disable

```
HPT CLI > set 1/E1 param
ID: 2003
Name: Status LED
Option: Enable/Disable
Value: Enable
Description: Enable: turn on the Status LED control function; Disable: turn off the Status LED control function and the LED is off by default.
ID: 2004
Name: Fault LED
Option: Enable/Disable
Value: Enable
Description: Enable: turn on the Fault LED control function; Disable: turn off the Fault LED control function and the LED is off by default.
ID: 2005
Name: SSD LED
Option: Enable/Disable
Value: Enable
Description: Enable: turn on the SSD LED control function; Disable: turn off the SSD LED control function and the LED is off by default.

HPT CLI > set 1/E1 Param 2003=Disable
Parameter set successfully! It will take affect after reboot.

HPT CLI > set 1/E1 param
ID: 2003
Name: Status LED
Option: Enable/Disable
Value: Disable
Description: Enable: turn on the Status LED control function; Disable: turn off the Status LED control function and the LED is off by default.
ID: 2004
Name: Fault LED
Option: Enable/Disable
Value: Enable
Description: Enable: turn on the Fault LED control function; Disable: turn off the Fault LED control function and the LED is off by default.
ID: 2005
Name: SSD LED
Option: Enable/Disable
Value: Enable
Description: Enable: turn on the SSD LED control function; Disable: turn off the SSD LED control function and the LED is off by default.
```

6.13.13. Set Restrict to Localhost Access

HPT CLI>set RL=[y|n]

Set enable(y) or disable(n) **[Restrict to localhost access]** parameter.

Remote access to the AIC will be restricted when enabled; other users in your network cannot log in to the RAID Management software remotely.

It is used as follows:

1. Set **RL=n**.

Input example:

HPT CLI>set RL=n

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

2. Reboot the system.
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.

6.14. Unplug Command

```
Unplug Command
  This command allows you to unplug an existing RAID array or device.
  After you have unplugged the array or device, you can hot plug it.
  Also by running the rescan command you can find it back.
  Please refer to 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 24: Properties for unplug Commands

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

6.14.1. Unplug the Physical Device

HPT CLI>unplug {device id}

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

Input example:

HPT CLI>unplug 1/E1/6

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

HPT CLI > unplug 1/E1/6
Unplug device(1/E1/6) successfully!

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

6.14.2. Unplug a RAID Array

HPT CLI>unplug {array id}

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

Input example:

```
HPT CLI>unplug 1
```

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

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

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

6.15. Secure Command

```
Secure Command
  This command is used to set device security.

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

HPT CLI > .
```

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

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

Table 25: Properties for secure Commands

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

6.15.1. 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
```



The screenshot shows a terminal window with the following text:

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

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

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

The 'Secure' column for the first row (1/E1) is highlighted in blue, and the command 'secure 1/E1 enable key=00000000' is highlighted in blue in the second line of the terminal.

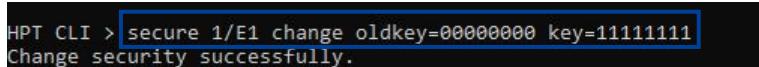
6.15.2. Change AIC Security key

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}
```



The screenshot shows a terminal window with the following text:

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

The command 'secure 1/E1 change oldkey=00000000 key=11111111' is highlighted in blue in the terminal.

6.15.3. Disable AIC Security

HPT CLI>secure {enclosure id} disable

This command allows you to disable AIC security.

Input example:

HPT CLI>secure 1/E1 disable

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

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

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

6.15.4. Enable Disk Security

HPT CLI>secure {device id} legacy

This command allows you to enable disk security.

Input example:

HPT CLI>secure 1/E1/5 legacy

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

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

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

6.15.5.Change Disk Security key

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

This command allows you to change the AIC security key.

Input example:

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

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

Note: There is a limit to the number of times you can change the disk key. If you do not correct disk key is not entered multiple times consecutively (the exact number of incorrect attempts leading to a lock is determined by the disk and may vary), and you will need to power cycle to change the disk key, i.e., perform a one-time power failure on the disk, such as hot-swapping the disk or powering down the host system and Enclosure.

6.15.6.Disable Disk Security

HPT CLI>secure {device_id} secureerase {force}

This command allows you to disable disk security.

Input example:

HPT CLI>secure 1/E1/5 secureerase force

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

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

6.16. 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 26: Properties for diag Command

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

6.16.1. Collect the Diagnostic Information

HPT CLI>diag

This command allows you to collect the diagnostic information.

Input example:

```
HPT CLI>diag
```

- **For Windows User**

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

- **For Linux User**

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

6.17. Switch Command

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

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

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

Table 27: 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.

6.17.1. Switch the AIC

HPT CLI>switch {card_id}

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

Input example:

HPT CLI>switch 1

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

6.18. Update Command

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

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

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

Table 28: Properties for update Command

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

6.18.1. 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\R7628ASSW_HLK_v5.12.4.1_v2.4.1.2_2024_05_08.blf
```

```
HPT CLI > update 1/E1 fw=C:\Users\test\Desktop\R7628ASSW_HLK_v5.12.4.1_v2.4.1.2_2024_05_08.blf
Current Firmware version: 5.12.5.0, Selected Firmware version: 5.12.4.1
Current UEFI version: 2.4.1, Selected UEFI version: 2.4.2

Are you sure to flash firmware? Please input 'Y' or 'N' : Y
Firmware updated successfully, it will take effect after reboot.
```

6.19. 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|update|ver|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 29: 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.

6.19.1. Show the Generic Help Command

HPT CLI>help

This command shows generic help about this utility.

Input example:

HPT CLI>help

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

6.19.2. Show the Specific Command Help

HPT CLI>help {command}

Show help about a specific command.

Input example:

HPT CLI>help delete

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

6.20. Ver Command

```
HPT CLI>ver
```

Shows the version of RAID Management currently in use. This is only supported by the Linux HighPoint RAID Management.

6.20.1. Show the RAID Management Version

HPT CLI>ver

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

Input example:

```
HPT CLI>ver
```

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

6.21. Exit Command

```
HPT CLI > exit
```

Exit from the interactive mode and close the window.

6.21.1. Exit the CLI

HPT CLI>exit

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

Input example:

HPT CLI>exit

6.22. Clear Command

```
HPT CLI > clear
```

This command is used to clear the screen.

6.22.1. Clear the CLI screen

HPT CLI>clear

This command allows you to clear the screen.

Input example:

```
HPT CLI>clear
```

7. Format the RAID Array

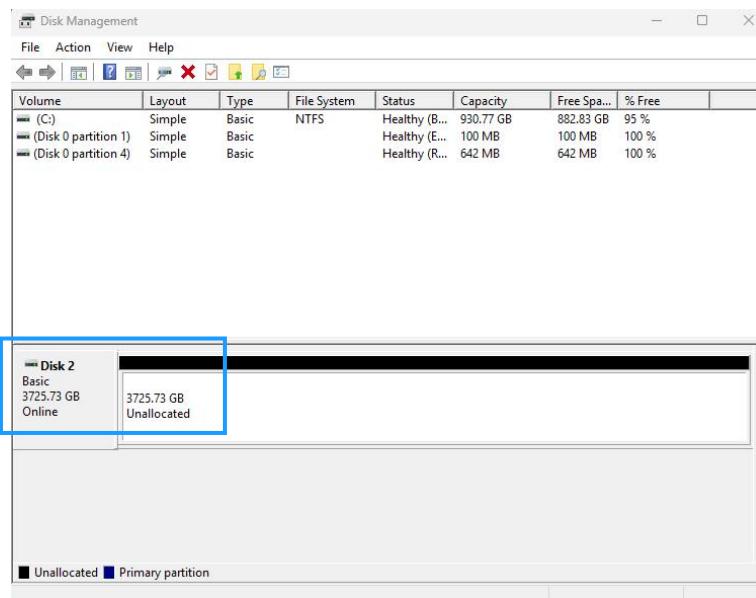
The section provides a comprehensive guide on formatting the RAID arrays in Windows, Linux, and macOS.

7.1. Format the RAID Array in Windows

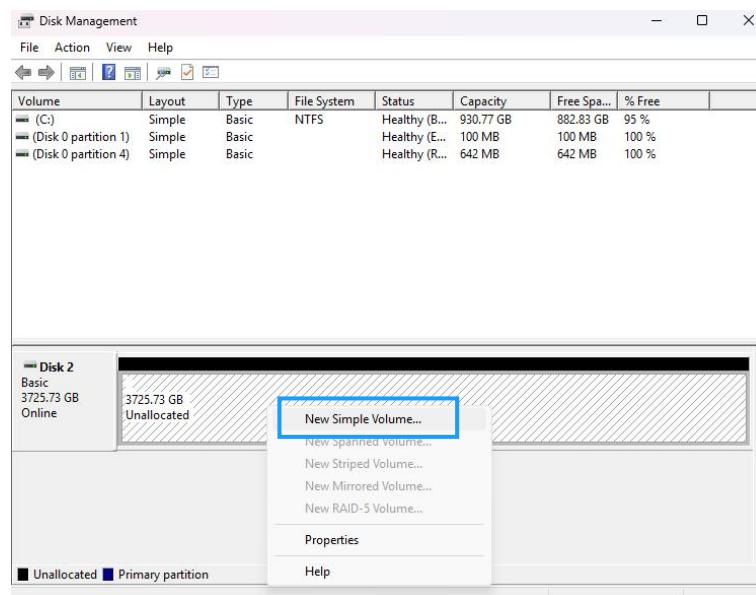
1. Create a RAID array using the [WebGUI](#) or [CLI](#).

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.

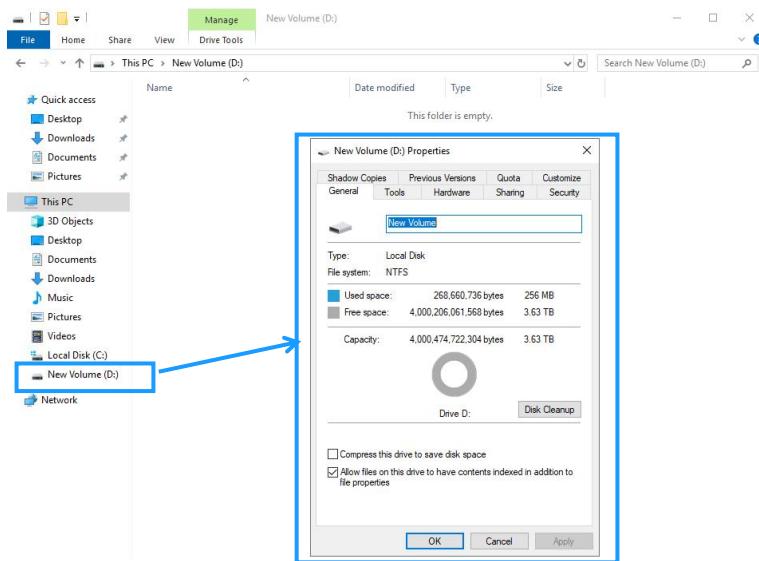
2. Access **Disk Management**, and partition/format the RAID array.



3. Click the array icon and select "New simple volume" to format the array.



4. Once complete, it will be available for use.



7.2. Format the RAID Array in Linux

1. Create a RAID array using the [WebGUI](#) or [CLI](#).

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.

2. Run the **Terminal** as Administrator.
3. Use the following command to format the RAID array.

```
#mkfs.ext4 /dev/hptblock0n* -E lazy_itable_init=0,lazy_journal_init=0
```

```
root@t-System-Product-Name:/home/t/Desktop# mkfs.ext4 /dev/hptblock0n4p -E lazy_itable_init=0,lazy_journal_init=0
mke2fs 1.47.0 (5-Feb-2023)
Discarding device blocks: done
Creating filesystem with 976683008 4k blocks and 244170752 inodes
Filesystem UUID: 6f254775-66c8-4197-8a77-a58e4b9a936a
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000, 7962624, 11239424, 20480000, 23887672, 71663616, 78675968,
    102400000, 214990848, 512000000, 550731776, 644972544

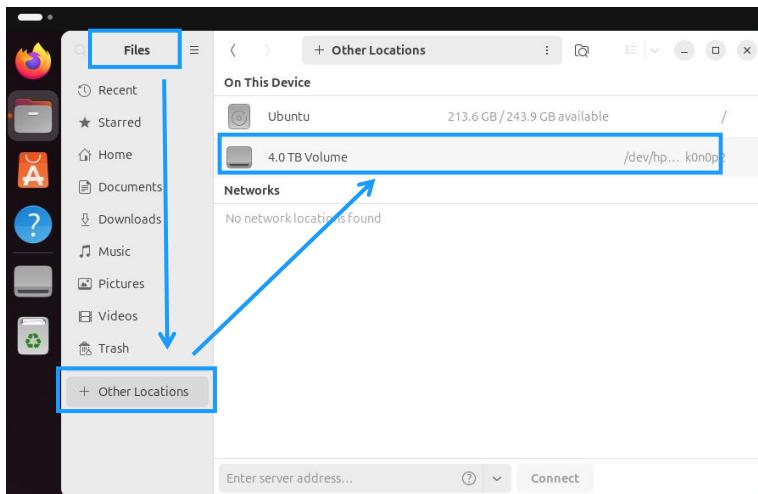
Allocating group tables: done
Writing inode tables: done
Creating journal (262144 blocks): done
Writing superblocks and filesystem accounting information: done
```

4. Use the following command to mount the RAID array.

```
#mount /dev/hptblock0n* /mnt
```

```
root@t-System-Product-Name:/home/t/Desktop# mount /dev/hptblock0n4p /mnt
root@t-System-Product-Name:/home/t/Desktop# lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
loop0      7:0    0  73.9M  1 loop /snap/core22/1748
loop1      7:1    0  73.9M  1 loop /snap/core22/1981
loop2      7:2    0    4K  1 loop /snap/bare/5
loop3      7:3    0  258M  1 loop /snap/firefox/5751
loop4      7:4    0  11.1M 1 loop /snap/firmware-updater/167
loop5      7:5    0  516M  1 loop /snap/gnome-42-2204/202
loop6      7:6    0  91.7M 1 loop /snap/gtk-common-themes/1535
loop7      7:7    0  10.8M 1 loop /snap/snap-store/1248
loop8      7:8    0  50.9M 1 loop /snap/snapd/24505
loop9      7:9    0  568K  1 loop /snap/snapd-desktop-integration/253
loop10     7:10   0  44.4M 1 loop /snap/snapd/23545
nvme0n1    259:0   0 232.9G  0 disk
└─nvme0n1p1 259:1   0    1G  0 part /boot/efi
└─nvme0n1p2 259:2   0 231.8G  0 part /
hptblock0n4p 259:3   0   3.6T  0 disk /mnt
root@t-System-Product-Name:/home/t/Desktop#
```

5. Once complete, it will be available for use.

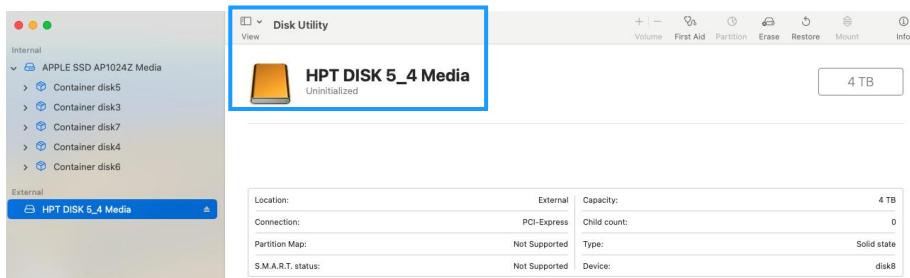


7.3. Format the RAID Array in macOS

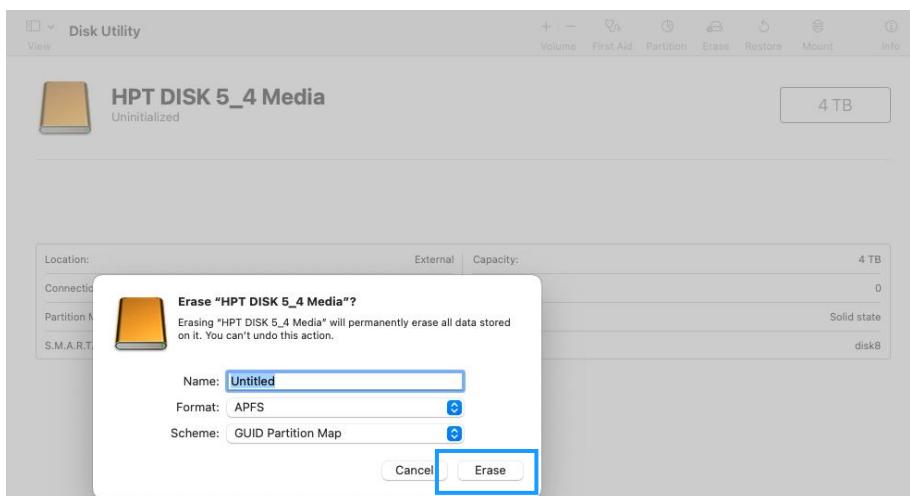
1. Create a RAID array using the [WebGUI](#).

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.

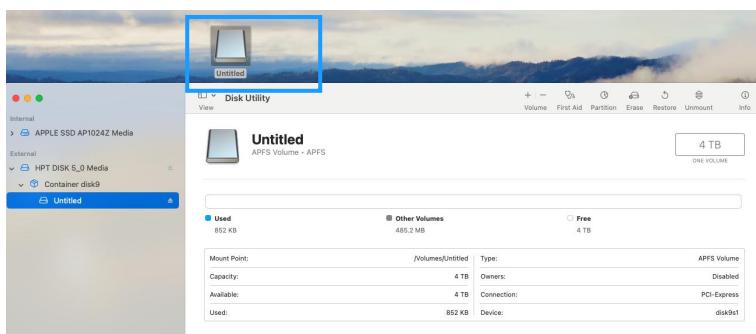
2. Access the **Disk Utility**.



3. Click "Erase" and wait for completion. Format the RAID array. Name, partition and format the array as desired.



4. Once complete, it will mount on the desktop and be available for use.



8. Trouble shooting

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

8.1.1. For Debian

1. Description of the Problem

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

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

2. Cause of the Problem

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

3. Solution

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

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

```
root@debian:/home/test/Documents# ./setup.bin
Verifying archive integrity... All good.
Uncompressing HighPoint NVMe GS 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:

- To install using the CD-ROM: insert the CD-ROM back and press **Enter**.
- To install using the USB flash drive:
 - 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>
 - Open the system terminal with root privileges.
 - Enter the following command:
#nano /etc/apt/sources.list

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

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

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

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

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

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

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

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

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

```
root@test:~/home/test/Documents$ nano /etc/apt/sources.list
root@test:~/home/test/Documents$ apt-get update
Get:1 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye InRelease [116 kB]
Get:2 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye-updates InRelease [44.1 kB]
Get:3 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye-backports InRelease [49.0 kB]
Get:4 https://mirrors.tuna.tsinghua.edu.cn/debian-security bullseye-security InRelease [48.4 kB]
Get:5 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye/non-free Sources [81.2 kB]
Get:6 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye/main Sources [1.1 kB]
Get:7 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye/contrib Sources [49.2 kB]
Get:8 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye/main amd64 Packages [8,184 kB]
Get:9 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye/main Translation-en [6,239 kB]
Get:10 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye/main amd64 DEP-11 Metadata [4,649 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 DEP-11 48x48 Icons [13.6 kB]
Get:16 https://mirrors.tuna.tsinghua.edu.cn/debian bullseye/contrib DEP-11 64x64 Icons [47.7 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 kB]
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-backports/main Sources [160 kB]
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-security/bullseye-security/main Sources [160 kB]
Get:35 https://mirrors.tuna.tsinghua.edu.cn/debian-security/bullseye-security/main Sources [160 kB]
Get:36 https://mirrors.tuna.tsinghua.edu.cn/debian-security/bullseye-security/non-free Sources [632 B]
Get:37 https://mirrors.tuna.tsinghua.edu.cn/debian-security/bullseye-security/main amd64 Packages [189 kB]
Get:38 https://mirrors.tuna.tsinghua.edu.cn/debian-security/bullseye-security/main Translation-en [119 kB]
Get:39 https://mirrors.tuna.tsinghua.edu.cn/debian-security/bullseye-security/non-free amd64 Packages [528 B]
Get:40 https://mirrors.tuna.tsinghua.edu.cn/debian-security/bullseye-security/non-free Translation-en [344 B]
Fetched 40.2 MB in 3min 13s (208 kB/s)
Reading package lists... Done
```

d. Reinstall the HighPoint software.

8.1.2. For RHEL

1. Description of the Problem

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

```
[root@localhost Documents]# ./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 ... (failed)
Installing program gcc ... (failed)
```

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

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

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

2. Cause of the Problem

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

3. Solution

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

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

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

- Reinstall the HighPoint software.

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

8.1.3. For Ubuntu

1. Description of the Problem

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

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

2. Cause of the Problem & Solution

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

Solution:

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

- The system process is occupied/ busy.

Solution:

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

```
#apt-get update
```

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

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 ...
  Checking for required toolchain and utility ...
  Found program make (/usr/bin/make).
  Installing program gcc... (failed)
  Found program perl (/usr/bin/perl).
  Found program wget (/usr/bin/wget).
  Old package(s) lommu=off intel_lommu=off amd_lommu=off
  New package(s) lommu=off intel_lommu=off intel_lommu=off amd_lommu=off
  Synchronizing state of hptdrv-monitor.service with SysV service script with /lib/systemd/systemd-sysv-install.
  Executing: /lib/systemd/systemd-sysv-install enable hptdrv-monitor
  update-rc.d: warning: enable action will have no effect on runlevel 1
  Toolchain to build the driver is incomplete, please install the missing package to build the driver.
  Exit.
```

2. Cause of the Problem & Solution

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

Solution:

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

- The system process is occupied/ busy.

Solution:

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

```
#apt-get update
```

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

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

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

root@test:/home apt-get update
rr1: http://ftp.debian.org/debian buster InRelease
Temporary failure resolving 'ftp.debian.org'
rr2: http://ftp.debian.org/debian buster-updates InRelease
Temporary failure resolving 'ftp.debian.org'
rr3: http://security.debian.org buster-security InRelease
Temporary failure resolving 'security.debian.org'
rr4: http://proxmox.com/debian/buster InRelease
Temporary failure resolving 'proxmox.com'
Temporary failure resolving 'enterprise.proxmox.com'
Reading package lists... Done
* failed to fetch http://ftp.debian.org/debian/dists/buster/main/binary-amd64/Temporary failure resolving 'ftp.debian.org'
```

Solution:

- The system needs to be resourced. For details, please refer to the official website file:

https://pve.proxmox.com/wiki/Downloads#Update_a_running_Proxmox_Virtual_Environment_8.x_to_latest_8.2

- Open the system terminal with root privileges.

- Enter the following command:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

j) Enter the following command to restart the service.

```
#systemctl restart pvedaemon
```

b. apt-get update

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

c. Reinstall the HighPoint software.

8.2. Delete a drive partition in Windows

1. Search for **cmd** in the Start menu, right-click the **Command Prompt**, and select **Run as administrator**.
2. Type **diskpart** to launch the disk utility.

```
Microsoft Windows [Version 10.0.26100.1742]
(c) Microsoft Corporation. All rights reserved.

X:\sources>diskpart

Microsoft DiskPart version 10.0.26100.1150

Copyright (C) Microsoft Corporation.
On computer: MININT-FSDNPII
```

3. Type **list disk** to view all disk listings and confirm the target disk number.

```
DISKPART> list disk

Disk ###  Status       Size     Free     Dyn  Gpt
-----  -----
Disk 0    Online       238 GB  1024 KB   *    
Disk 1    Online       1863 GB 1863 GB   *    
Disk 2    Online       931 GB  931 GB   *    
```

Note: The system will list all available disks and assign each a number, such as Disk 0, Disk 1, etc.

4. Type **select disk X** (where X is the target disk number) to select the disk.

```
DISKPART> select disk 1

Disk 1 is now the selected disk.
```

5. Type **clean** to erase all partitions and data.

```
DISKPART> clean

DiskPart succeeded in cleaning the disk.
```

Note: This operation will permanently delete all data on the disk. Back up important data beforehand.

9. Glossary

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

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

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

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

10. Revision History

10.1. Version 1.00, June 24, 2024

Initial version.

10.2. Version 1.01, July 1, 2024

1. Add RA7608AW support
2. Update [Sensors Information](#)
3. Update [Password Setting](#)
4. Update [Secure Setting](#)

10.3. Version 1.02, January 3, 2025

1. Add RA6541AW support.
2. Update background initialization description.
3. Add secured status.
4. Update [Event Log](#).
5. Add BlockSize and SectorSize in [Logical Device Information](#).
6. Update Linux otc file in [Save the Diagnostic Log](#).
7. Remove Add RS6542AW/ RA6542AWW-S491T5-12 support.
8. Change the description of “power cycle”.
9. Add RA6541AW Fan Speed “Ultra Low/ULow”.
10. Update [5.3Physical](#) steps.

10.4. Version 1.03, February 12, 2025

1. Add [5.3.9 LED On/Off Setting](#)
2. Add [6.13.12 Set Status/ Fault/ SSD LED On/Off](#)

10.5. Version 1.04, April 11, 2025

1. Add R7604A support
2. Add [Using the Cross-Sync feature to create an array](#)
3. Add [View the TBW Information](#)
4. Add [Vital Product Data Information](#)
5. Change: the number of times the disk password limit is changed from 5 times to be determined by the disk itself
6. Add description of LED settings Enable and Disable

10.6. Version 1.05, October 10, 2025

1. Add R7624A support
2. Add [Format the RAID Array in Windows](#)
3. Add [Format the RAID Array in Linux](#)
4. Add [Format the RAID Array in macOS](#)
5. Add [Delete a drive partition in Windows](#)

10.7. Version 1.06, December 26, 2025

1. Add R7528U support
2. Add R7628U support