HighPoint SafeStorage

User Manual

V1.06-Apr 8, 2024

Contents

1. Overview

HighPoint's SafeStorage solution was developed to work in conjunction with industry-standard SED (Self-encrypted drive) technology supported by OPAL v2.0 compliant M.2 and U.2/U.3 NVMe media, and is based on the OPAL SSC TCG (Trusted Computing Group) specifications. It is designed to protect data assets when physical drives are misplaced or stolen by preventing unauthorized access to stored data.

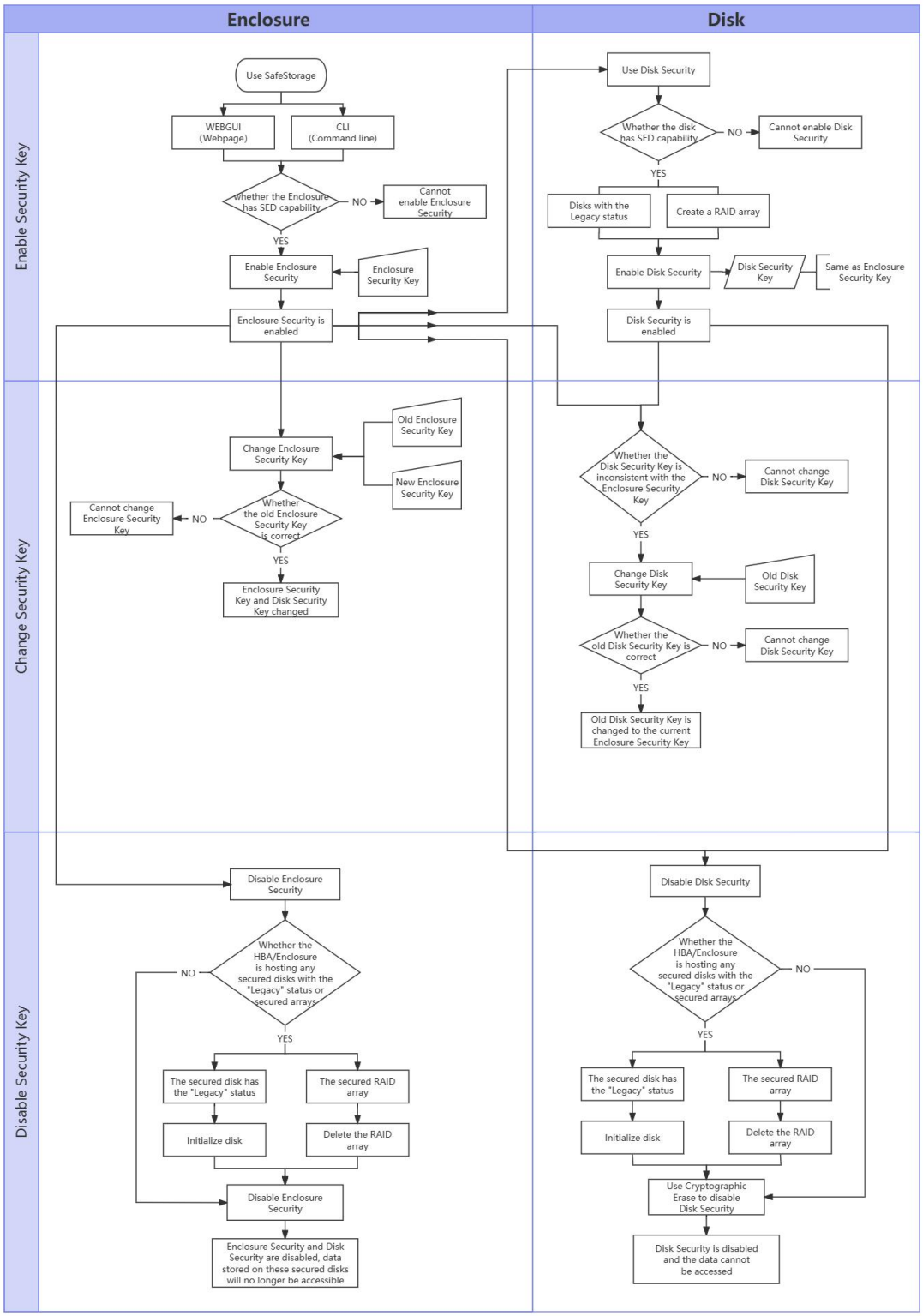
SafeStorage can be applied to single-disk and RAID configurations and is activated via a service known as Disk Security, which can be administered via our software management.

The following is a list of products that support SafeStorage.

Supported products	SSD7580C
	SSD7749M
	SSD7749E
	SSD6780A
	RA7105HW-A04T0-03
	RA7502HW-A02T0-03
	RA7502HW-A04T0-00
	RA7502HW-A08T0-09
	RA7505HW-A04T0-03
	RA7505HW-A08T0-00
	RA7505HW-A04T0-0D
	RA7505HW-A08T0-0E
	RA7505HW-A16T0-0F
	RA7540HW-A16T0-00
	RA7540HW-A16T0-0E
	RA7540HW-A32T0-0F
	RA7749EW-K15T3-0A
	RA7749EW-K30T7-0B
	RA7749EW-K61T4-0C
	RA7749MW-A32T0-0F
Supported disks	OPAL v2.0 compliant M.2 and U.2/U.3 NVMe media

Important Security Warning: *Enabling password protection for the WebGUI and CLI is highly recommended. By default, this security feature is disabled; administrators are not required to enter a name or password when starting the software. If this feature is not enabled, any user with access to the target platform can enable or disable Disk Security at will.*

2.SafeStorage Workflow



2.1 Enable Enclosure Security

To use SafeStorage, you must first enable the Enclosure Security option using the HighPoint RAID Management utility (WebGUI or CLI) and create an Enclosure Security Key.
Note: *The Enclosure Security Key you create will also be the Disk Security Key, written to the disk/ array*.

Warning: *Be sure to make a record of your Enclosure 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.*

2.2 Enable Disk Security

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

Once Enclosure Security has been enabled, you can use the disk/array's SED capabilities. As mentioned previously, the Disk Key is automatically generated when the Enclosure Key is created and will be written to the disk. These keys are identical.
There are two methods to enable Disk Security.
Method 1: Enabling Disk Security for disks with the Legacy status
Method 2: Enabling Disk Security when creating a RAID array

2.3 Change Enclosure Security key

If you want to change the Enclosure Security key, you must provide the old Enclosure Security key. If you don't know the old Enclosure Security key, you won't be able to change Enclosure Security key.
When the Enclosure Security key is changed to the new key, the Disk Security key is also changed to the same new key and written to the secured disk.

2.4 Change Disk Security key

If the Enclosure Security Key and Disk Security Key do not match, you cannot access data stored on the disk or array.
This ensures that the disk or array will remain inaccessible when removed from the system.
The administrator must input the original “old” Enclosure Security Key to access data.

To explain, there are two situations in which the Enclosure Security Key and Disk Security Key will not match:
Situation 1: The disk is from another Enclosure.
Situation 2: The disk/array was not present when the Enclosure Security Key was changed.

2.5 Disable Disk Security

If you do not want to encrypt the disks, use **Cryptographic Erase** to disable Disk Security.

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

2.6 Disable Enclosure Security

If you do not want to use the SafeStorage, we provide options to disable Enclosure Security.
The Enclosure Security can only be disabled if the target HBA/ enclosure does not host any secured disks with the “Legacy” status or secured arrays.
Disable Enclosure Security will perform a Cryptographic Erase operation to disable Disk Security for all secured disks on the Enclosure.

***Warning**: After disable Enclosure Security, data stored on these secured disks will no longer be accessible.*

3. How to use SafeStorage with the WebGUI

Web RAID Management (WebGUI) is a simple and intuitive web-based management tool.

3.1 Enable Enclosure Security

1. Click the **Physical** tab, then click the appropriate "**Enclosure**" on the left-hand side of the interface.

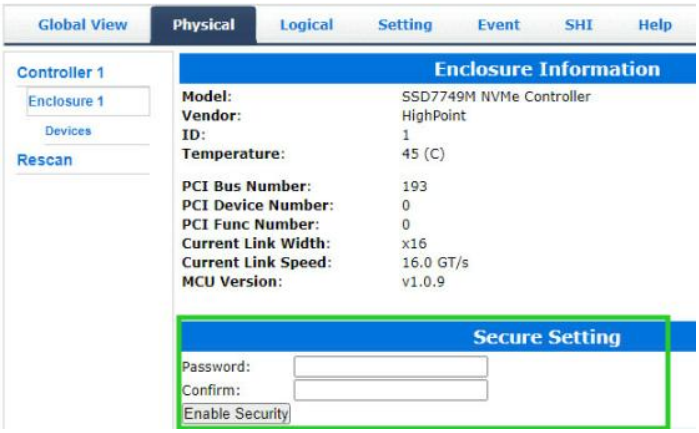
   Note: *"Enclosure X" in this instance refers to each SSD series RAID HBA, RocketAIC series NVMe drive, or RocketStor enclosure that is currently installed into the system. For example, if you work with a single SSD7749M, the default option is "Enclosure 1".*

2. Next, create a password under **Secure Setting**. The password must be between 8 and 32 characters in length. Enter the password a second time for the "**Confirm**" field.

3. After setting the password, click **Enable Security** to enable the Secure settings.

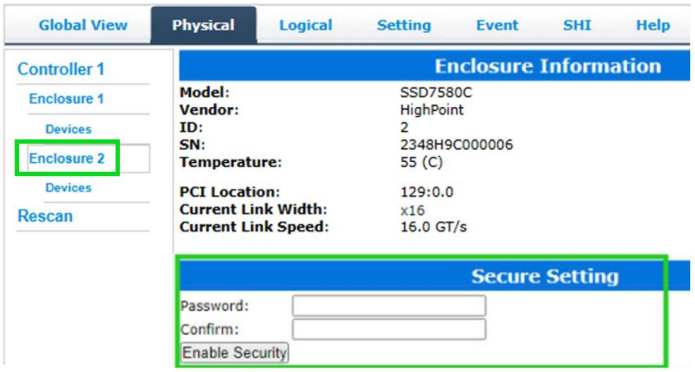
   Note: *The steps for enable single Enclosure* Security *and enable dual Enclosure* Security *are the same.*

   Example 1 (before enable single Enclosure Security setting):

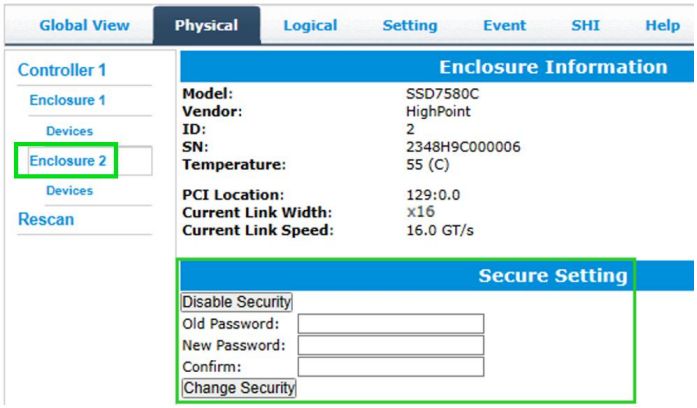


   Example 2 (after enable single Enclosure Security setting):

Example 3 (before enable dual Enclosure Security setting):



Example 4 (after enable dual Enclosure Security setting):



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

3.2 Enable Disk Security

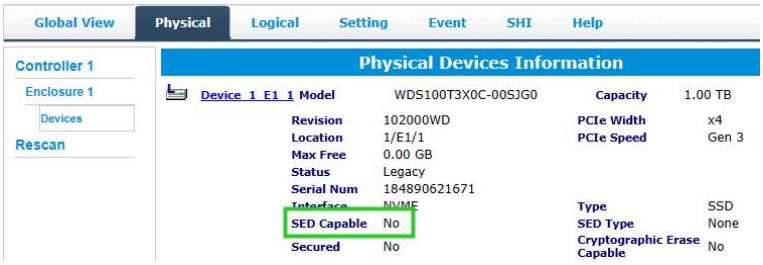
Notes:

Disk security can only be enabled only if you have enabled Enclosure Security.

First, confirm if your disk supports SED functions. SafeStorage will only work with SED-capable storage media.

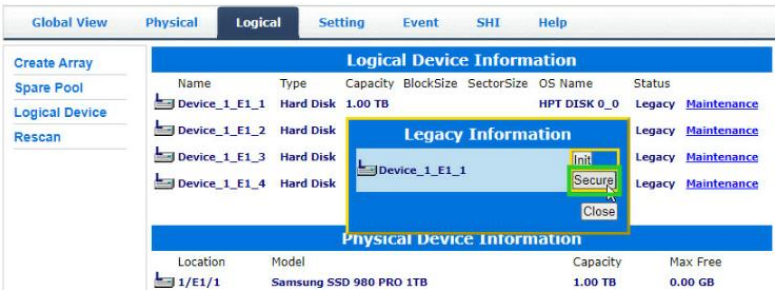
Example 1 (The device supports SED functions; **SED Capable** is **Yes**):

Example 2 (The device does not support SED functions, **SED Capable** is **No**):



There are two methods to enable Disk Security.

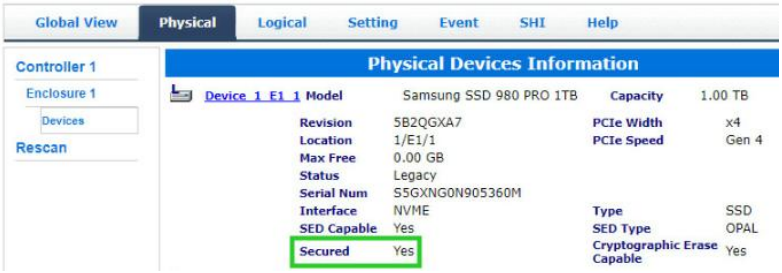
1. **Method 1: Enabling Disk Security for disks with the Legacy status**
   1) Click the **Logical tab** and check the **Logical Device** section of the page**.**
   2) Click the **Maintenance** option displayed on the right-hand side of each disk.
   3) Click **Secure** to enable Disk Security.



4) Repeat steps 1) through 3) for the remaining disks.

Example 1 (before Disk Security has been enabled):

Example 2 (after Disk Security has been enabled):

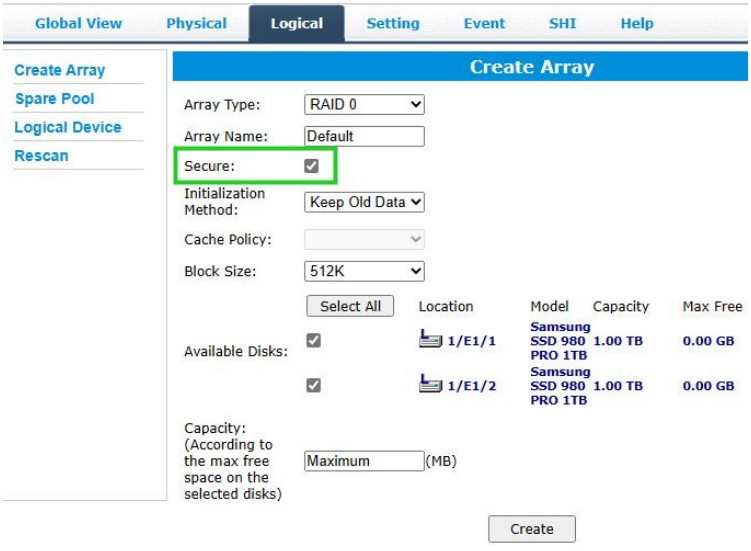


2. Method 2: Enabling Disk Security when creating a RAID array

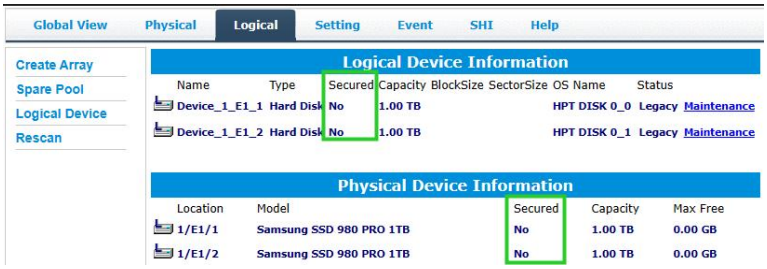
Note: *this feature is enabled when the array is created. Disk Security cannot be added to an existing array.*

1) Click the **Logical** tab.

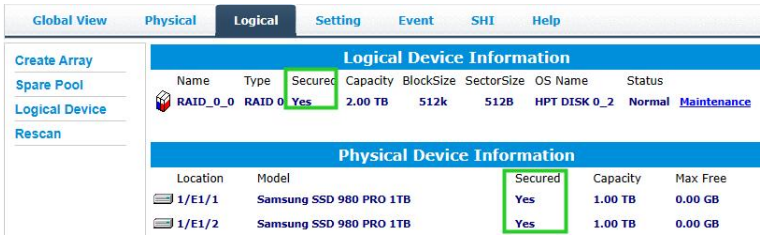
2) When creating a RAID array, check the box before the **Secure** option.



Example 1 (before Disk Security has been enabled):

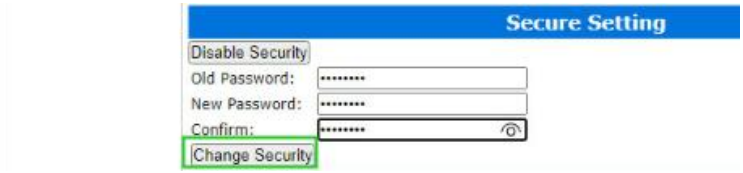


Example 2 (after Disk Security has been enabled):

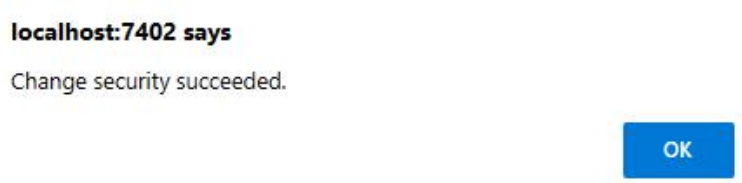


3.3 Change Enclosure Security key

1. Click the **Physical** tab and the target **Enclosure** entry on the left side of the interface.
2. Enter the current password under the "**Old Password**" field.
3. Enter a new password under the "**New Password**" field (must contain 8 to 32 characters).
4. After entering a new password, click **Change Security**.



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



Notes:

*Changing the **Enclosure Security key** will automatically change the **Disk Security Key.***

The steps for change single Enclosure Security and change dual Enclosure Security are the same.

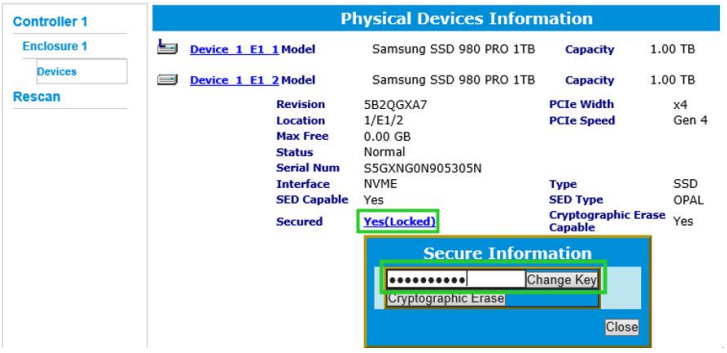
3.4 Change Disk Security key

Note: *When the Enclosure 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.*

1. Click the **Physical** tab.
2. Under the **Physical Devices** section, click the name of each disk in blue text to view the Secured setting. Yes (Locked).

   Note: ***Security:*** *Yes (Locked) indicates that the security of the disk is enabled, but the unlock action failed because the disk's key does not match the key on the controller. This status will prevent access to data stored on the disk.*
3. Click Yes (Locked), a new pop-up window providing a **Change Key** option will be displayed.
4. Enter the disk's **old password** and click **Change Key** to unlock the Disk Security key.

   Example:



   Note: ***Change Key:*** *Input the old Disk Security key to unlock the disk and write the Enclosure Security key on this disk.*
5. After the system restarts, the secure attribute of the disk should change from Yes (Locked) **to** Yes, and the disk password is now consistent with the enclosure's password.

   Note: ***Secured:*** *Yes indicates that security for the disk is enabled and unlocked. Data can be accessed.*

3.5 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.

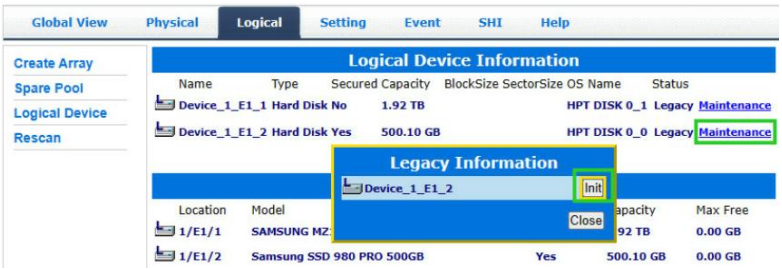
***Warning**: **Cryptographic erase** will delete the Security (Encryption) key from the target disk/ array members. Data stored on these disks will no longer be accessible.*

Notes:

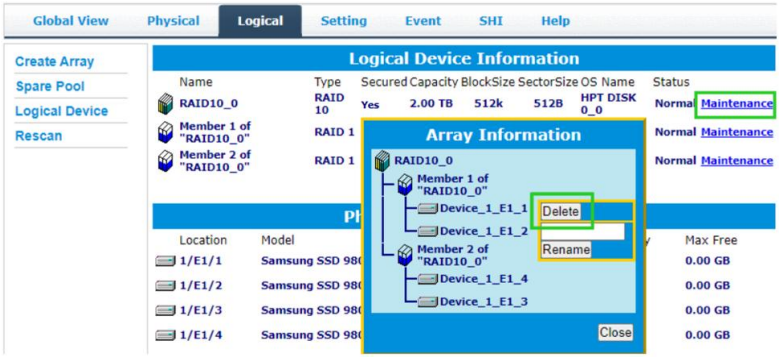
Disabling Disk Security will destroy data on the target disk or RAID array. Please make sure to back up any important data before using this option.

Disabling Disk Security can only be disabled if the target HBA/ enclosure is not hosting any secured disks with the "Legacy" status or secured arrays.

If the disk (or disks) has the "Legacy" status, you can remove this by using the "Init" function (initialize).



If you have the secured array, you can delete the array by using the "delete" function.



1. 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);
2. Click the Secured status (blue text); a pop-up window will be displayed, providing a **Cryptographic Erase** button.

3. Click the secure attribute of the **Cryptographic Erase** disk from Yes/Yes (Locked) to **No**.

Example 1 (click "Yes", popup window, then click "**Cryptographic Erase**"):

Example 2 (click "Yes (Locked)", popup window, then click "**Cryptographic Erase**"):

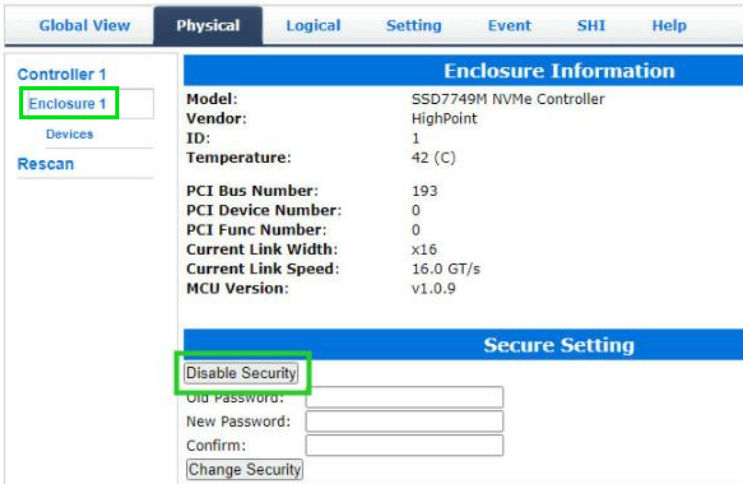
3.6 Disable Enclosure Security

Note: *This setting can only be disabled if the target HBA/ enclosure does not host any secured disks with the "Legacy" status or secured arrays.*

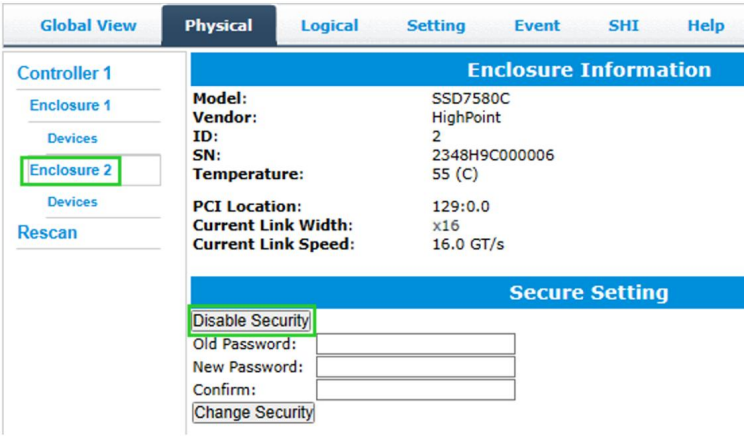
1. Click the **Physical** tab, then click the target Enclosure entry on the left side of the interface.
2. Under **Secure** Setting, click **Disable Security**.

   Note: *The steps for disable single Enclosure* Security *and disable dual Enclosure* Security *are the same.*

   Example 1 (disable single Enclosure Security setting):



   Example 2 (disable dual Enclosure Security setting):



4.How to use SafeStorage with the CLI

The **CLI** (command line interface) is a powerful, text-only management interface for advanced users and professional administrators.

Secure command reference:

```
HPT CLI > help secure
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 >
```

4.1 Enable Enclosure Security

Syntax:

secure {enclosure id} enable key={password}

The command is used to enable Enclosure Security.

Example1: enable single Enclosure Security

secure 1/E1 enable key=00000000

```
HPT CLI > query enclosures
ID    Secure      VendorID       ProductID                                NumberOfPYH
-----------------------------------------------------------------------------------
1/E1  No          HPT             A1005784                                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             A1005784                                8
```

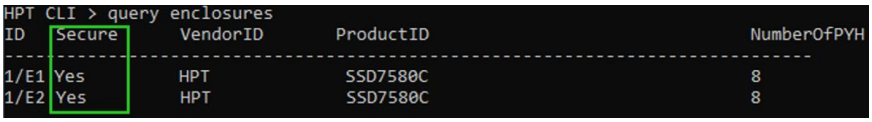
Example2: enable dual Enclosure Security

secure 1/E1 enable key=00000000

secure 1/E2 enable key=11111111

```
HPT CLI > query enclosures
ID    Secure      VendorID       ProductID                                NumberOfPYH
-----------------------------------------------------------------------------------
1/E1  No          HPT             SSD7580C                                8
1/E2  No          HPT             SSD7580C                                8

HPT CLI > secure 1/E1 enable key=00000000
Enable security successfully.
HPT CLI > secure 1/E2 enable key=11111111
Enable security successfully.
```



Notes:

The steps for enable single Enclosure Security *and enable dual Enclosure* Security *are the same.*

You can check if enable Enclosure Security is in effect with the command: ***query enclosures****. The secure status of enable Enclosure Security is* ***Yes,*** *and the secure status of disable Enclosure Security is* ***No.***

4.2 Enable Disk Security

Notes:

Disk security is enabled only if you have enabled Enclosure Security. If you don't enable Enclosure Security first, you will enable Disk Security failure.

First, confirm if your disk supports SED functions. SafeStorage can only be used with SED-capable storage media.

Example 1 (*Support SED function, SED Capable is Yes*):

```
HPT CLI > query devices 1/E1/2
Mode Number:          Samsung SSD 980 PRO 500GB
Serial Number:        S5GYNG0R205478M
Firmware Version:     3B2QGXA7
Capacity(GB):    500.03              TotalFree(GB):  500.03
Status:          SINGLE              Flag:           NORMAL
SED Capable:     Yes                 SED Type:       OPAL
Secured:         No                  Cryptographic Erase Capable:  No
PCIe Width:      x4                  PCIe Speed:     Gen 4
Temperature (F):                                    89
Warning Composite Temperature Threshold (F):        179
Critical Composite Temperature Threshold (F):       185
```

Example 2 *(Not support SED function, SED Capable is No*):

```
HPT CLI > query devices 1/E1/1
Mode Number:          WDS100T3X0C-00SJG0
Serial Number:        184890621671
Firmware Version:     102000WD
Capacity(GB):    1000.20             TotalFree(GB):  0
Status:          SINGLE              Flag:           LEGACY
SED Capable:     No                  SED Type:       None
Secured:         No                  Cryptographic Erase Capable:  No
PCIe Width:      x4                  PCIe Speed:     Gen 3
Temperature (F):                                    89
Warning Composite Temperature Threshold (F):        176
Critical Composite Temperature Threshold (F):       185
```

There are two methods to enable Disk Security.

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

   Syntax:

   secure {device id} legacy

   The command is used to enable Disk Security for disks with the Legacy status.

   Example:

   secure 1/E1/1 legacy

```
HPT CLI > query devices
ID      Secured    Capacity    MaxFree     Flag    Status    ModelNumber
-------------------------------------------------------------------------------
1/E1/1  No         1000.20     0           SINGLE  LEGACY    Samsung SSD 980 PRO 1TB
1/E1/2  No         1000.20     0           SINGLE  LEGACY    Samsung SSD 980 PRO 1TB
-------------------------------------------------------------------------------

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

HPT CLI > query devices
ID      Secured    Capacity    MaxFree     Flag    Status    ModelNumber
-------------------------------------------------------------------------------
1/E1/1  Yes        1000.20     0           SINGLE  LEGACY    Samsung SSD 980 PRO 1TB
1/E1/2  No         1000.20     0           SINGLE  LEGACY    Samsung SSD 980 PRO 1TB
```

   Note: *You can check if enable Disk Security is in effect with the command:* ***query devices****. The secured status of enable Disk Security is* ***Yes,*** *and the secured status of disable Disk Security is* ***No.***

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

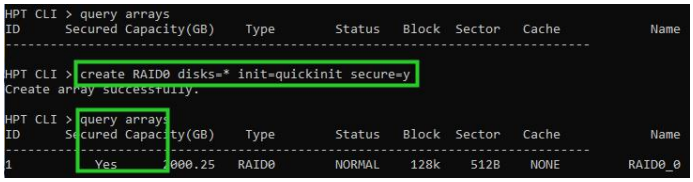
Syntax:

create RAID* disks=* init=* secure=y

The command is used to enable Disk Security when creating a RAID array.

Example:

create RAID0 disks=* init=quickinit secure=y



Note: *You can check if enable Disk Security is in effect with the command* ***query arrays****. The secured status of enable Disk Security is* ***Yes,*** *and the secured status of disable Disk Security is* ***No.***

4.3 Change Enclosure Security key

Syntax:

secure {enclosure id} change oldkey={old password} key={new password}

The command is used to change Enclosure Security key.

Example:

secure 1/E1 change oldkey=0000000 key=11111111

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

Notes:

*Changing the **Enclosure Security ke**y will automatically change the **Disk Security Key.***

The steps for change single Enclosure Security and change dual Enclosure Security are the same.

4.4 Change Disk Security key

Syntax:

secure {devices-id} changekey key={old password}

The command is used to change the Disk Security key to be consistent with all other Disk Security key on the enclosure.

Example:

secure 1/E1/2 changekey key=00000000

```
HPT CLI > query devices
ID      Secured      Capacity     MaxFree      Flag     St
-------------------------------------------------------------
1/E1/1  Yes          1920.25      1820.25      RAID     NO
1/E1/2  Yes(locked)  1920.38      0            SINGLE   NO
1/E1/3  Yes          1920.25      1800.25      RAID     NO
1/E1/4  Yes          1920.25      1900.25      RAID     NO
```

```
HPT CLI > secure 1/E1/2 changekey key=00000000
Change key successfully.Please restart to take effect.
```

```
HPT CLI > query devices
ID      Secured      Capacity     MaxFree      Flag     S
-------------------------------------------------------------
1/E1/1  Yes          1920.25      1920.25      SINGLE   N
1/E1/2  Yes          1920.25      1920.25      SINGLE   N
1/E1/3  Yes          1920.25      1920.25      SINGLE   N
1/E1/4  Yes          1920.25      1920.25      SINGLE   N
```

Note:** You can check if the change Disk Security key is in effect with the query devices command. The secured status of successfully change Disk Security key is **Yes,** and the secured status of not successfully change Disk Security is **Yes(locked).

4.5 Disable Disk Security

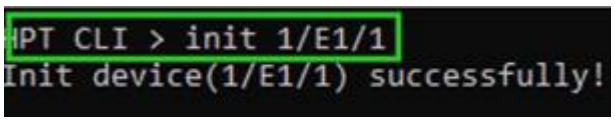
Syntax:

secure {devices-id} secureerase force

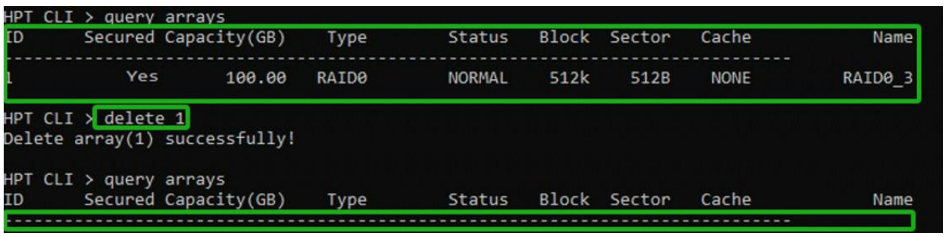
The command is used to erase the Disk Security configuration and securely erase data.

Note: *Disabling Disk Security can only be disabled if the target HBA/ enclosure is not hosting any secured disks with the "Legacy" status or secured arrays.*

If the disk (or disks) has the "Legacy" status, you can remove this by using the "Init" function (initialize).

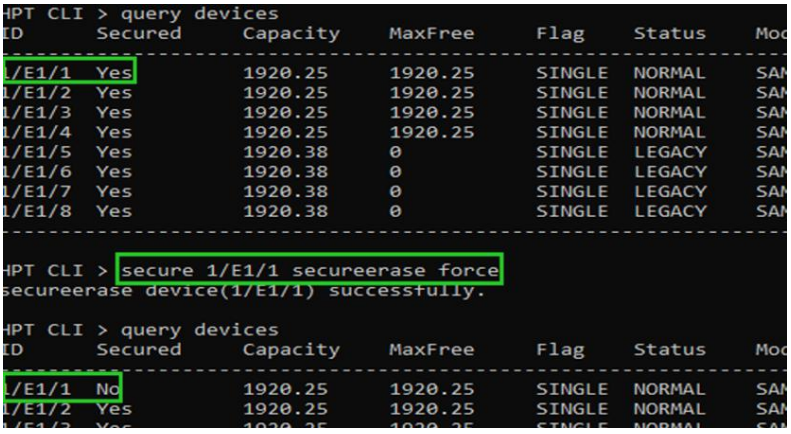


If you have the secured array, you can delete the array by using the "delete" function.



Example:

secure 1/E1/1 secureerase force



Note: *You can check if disable Disk Security is in effect with the command:* ***query devices****. The secured status of enable Disk Security is* ***Yes,*** *and the secured status of disable Disk Security is* ***No.***

4.6 Disable Enclosure Security

Note: *This setting can only be disabled if the target HBA/ enclosure does not host any secured disks with the "Legacy" status or secured arrays.*

Syntax:

secure {enclosure id} disable

The command is used to disable Enclosure Security.

Note: *The steps for disable single Enclosure* Security *and disable dual Enclosure* Security *are the same.*

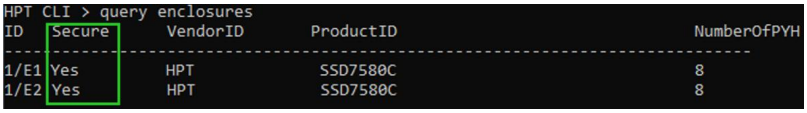
Example 1 (disable single Enclosure Security setting):

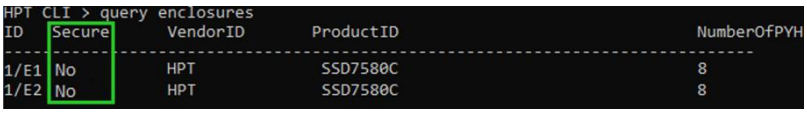
secure 1/E1 disable

Example 2 (disable dual Enclosure Security setting)**:**

secure 1/E1 disable

secure 1/E2 disable





Note: *You can check if disable Enclosure Security is in effect with the command:* ***query enclosures****. The secure status of enable Enclosure Security is* ***Yes,*** *and the secure status of disable Enclosure Security is* ***No.***

5. How Online Array Roaming

One of the features of all HighPoint RAID Enclosure and RAID controllers is Online Array Roaming. Information about the RAID configuration is stored on the physical drives. So, if the RAID Enclosure or RAID controller fails or you wish to use another RAID Enclosure or RAID controller, or you wish the drives to be moved to a different Enclosure or controller, the RAID configuration data can still be read by another HighPoint RAID Enclosure or RAID controller.

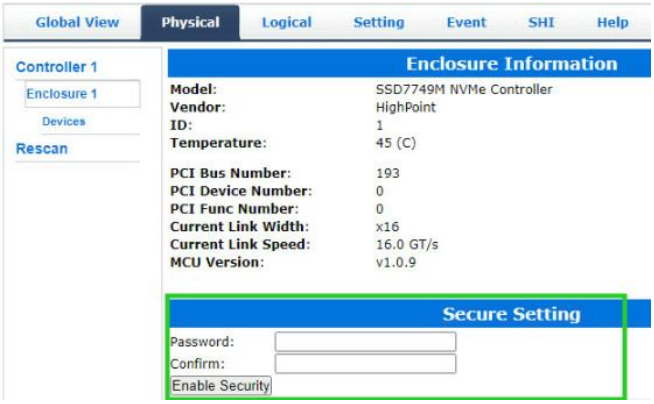
Note: *The prerequisite for using this feature is that both RAID Enclosures and RAID controllers use the same type of driver.*

5.1 Online Array Roaming: Moving an array from secured Enclosure A to the unsecured Enclosure B

Suppose you want to move an array from a secured Enclosure ("A" for this example) to an unsecured Enclosure ("B" for this example). In that case, you must **enable Enclosure B's Security Key** using a key that is consistent with Enclosure A's Security Key.

Example1 (**enable Enclosure B Security** in the WebGUI):

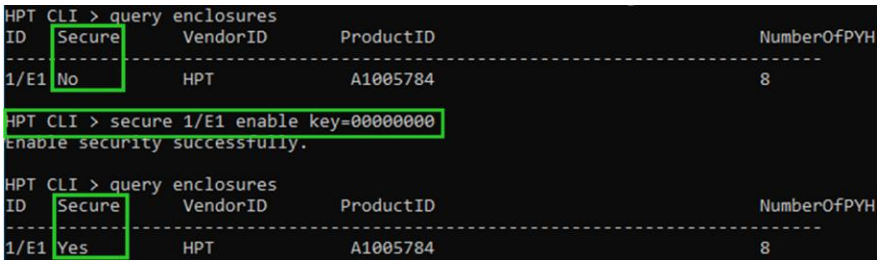
1. Click the **Physical** tab and the appropriate "**Enclosure**".
   Note: *"Enclosure X" in this instance refers to each SSD series RAID HBA, RocketAIC series NVMe drive, or RocketStor enclosure that is currently installed into the system. For example, if you work with a single SSD7749M, the default option is "Enclosure 1".*
2. Next, create a password under **Secure Setting**. The password must be between 8 and 32 characters in length. Enter the password a second time for the "**Confirm**" field.
3. After setting the password, click **Enable Security** to enable the Secure settings.



4. This will allow you to access data stored on the array using Enclosure B.

Example2 (**enable Enclosure B Security** in the CLI):

1. Enter the following command to enable Enclosure B Security**: HPT>s secure {enclosure_id} enable key={password}**



Note: *You can check if enable Enclosure Security is in effect with the command:* ***query enclosures****. The secure status of enable Enclosure Security is* ***Yes,*** *and the secure status of disable Enclosure Security is* ***No.***

2. This will allow you to access data stored on the array using Enclosure B.

5.2 Moving an array from secured Enclosure “A” to the secured Enclosure “B”

There are two situations where the keys for secured Enclosure A and secured Enclosure B are consistent or inconsistent. For these two situations, we need to take different measures.

5.2.1 The secured Enclosure A and the secured Enclosure B have the same key

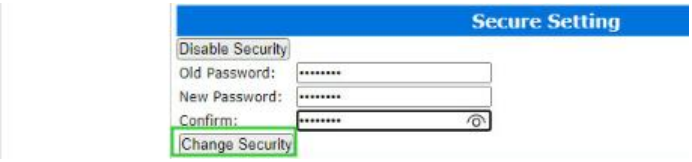
If the secured Enclosure A and the secured Enclosure B have the same key, you can access data stored on the array directly after Moving the disks to Enclosure B.

5.2.2 The secured Enclosure A and the secured Enclosure B have different Keys

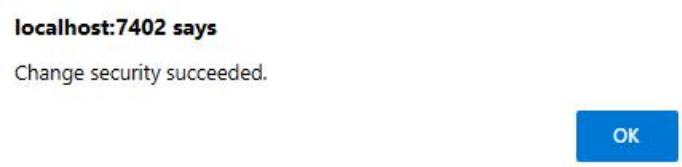
If the secured Enclosure A and the secured Enclosure B have different keys, you will not be able to access data after moving the array.
To access data, the administrator must **change Enclosure B’s Security key** to match Enclosure A’s Security key.

Example1 (**Changing Enclosure B Security Key** in the WebGUI):

1. Click the **Physical** tab and the target **Enclosure** entry on the left side of the interface.
2. Enter the current password under the “**Old Password**” field.
3. Enter a new password under the “**New Password**” field (must contain 8 to 32 characters).
4. After entering a new password, click **Change Security**.



5. Confirm the change by clicking “**OK**” when the pop-up window is displayed.

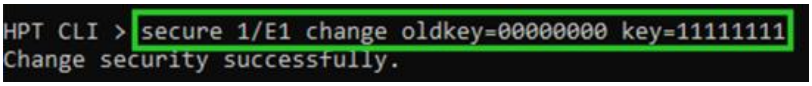


Note: *Changing the **Enclosure Security key** will automatically change the **Disk Security Key.***

6. This will allow you to access data stored on the array using Enclosure B.

Example2 (**Changing Enclosure B Security Key** in the CLI):

1. Enter the following command to change Enclosure A Security Key**: HPT> secure {enclosure id} change oldkey={old password} key={new password}**



Note: *Changing the* ***Enclosure Security key*** *will automatically change the* ***Disk Security Key.***

2. This will allow you to access data stored on the array using Enclosure B.

5.3 Moving an Array from an unsecured Enclosure to a secured Enclosure

Array from an unsecured Enclosure (“A”) can be moved directly to a secured Enclosure (“B”). Disk Security cannot be added to an existing array. If you want to protect data stored on the array at a later date, you can only back up the important data on the array, delete the array, and enable Disk Security when creating a new RAID array.

Notes:

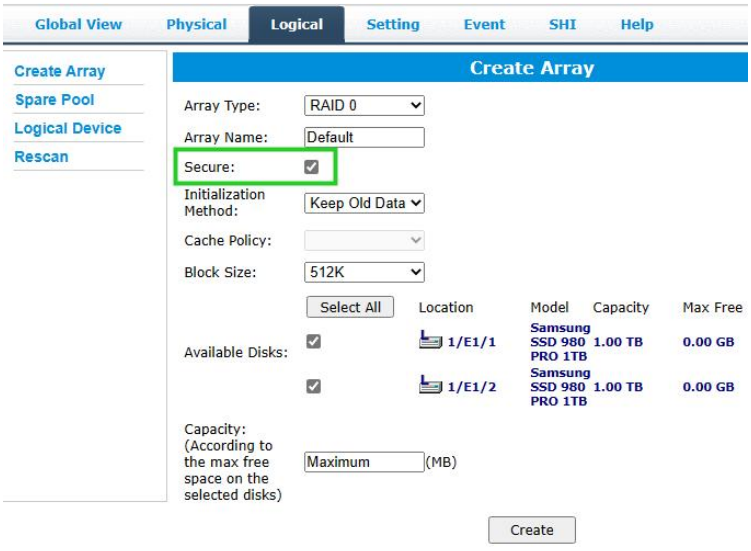
First, confirm if your disk supports SED functions. SafeStorage can only be used with SED-capable storage media.

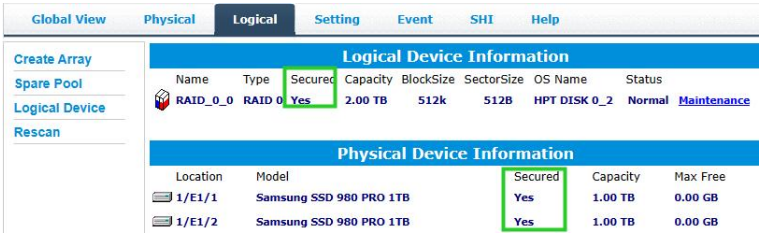
The Disk Key is automatically generated when the Enclosure B Security Key is used, and it will be written to the disk.

1. Back up the important data on the array.
2. Open the **WebGUI**. Click the **Logical→Maintenance**.
3. Click **Delete** to delete the RAID array on the Enclosure A.
4. Online Array Roaming from the unsecured Enclosure A to the secured Enclosure B.
5. Enable Disk Security when creating a RAID array.

   Example1 (enable Disk Security when creating a RAID array in the WebGUI):

   1) Click the **Logical** tab.
   2) When creating a RAID array, check the box before the **Secure** option.

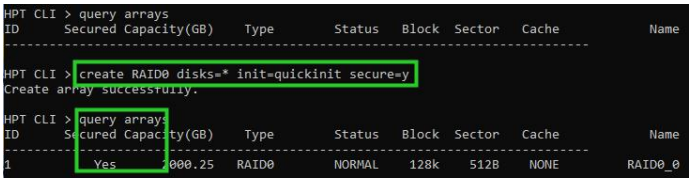




Example2 (enable Disk Security when creating a RAID array in the CLI):

1) Enter the following command to enable Disk Security f when creating a RAID array**:**

HPT> create RAID* disks=* init=* secure=y



6. You can protect data stored on the array.

6.Troubleshooting

6.1 Why does enable Disk Security fail?

There are two possible causes:

1. A motherboard BIOS setting is incorrect.
2. The proper procedure was not followed, which will result in a “Disk Security fail” status.

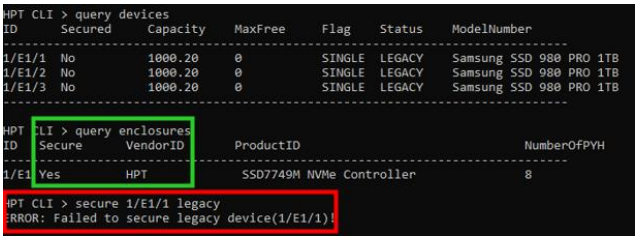
6.1.1 Improper motherboard BIOS settings cause enable Disk Security to fail

1. Description of the Problem:

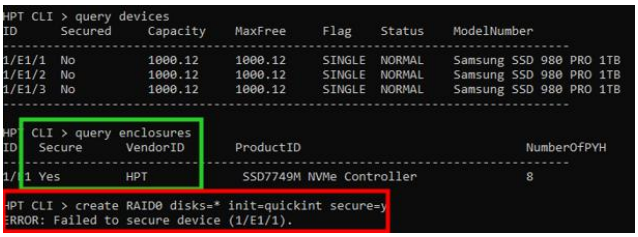
You have enabled Enclosure Security successfully, but the interface reports that Disk Security has failed.

1) As reported by the CLI:

a Failed to enable Disk Security for disks with the Legacy status

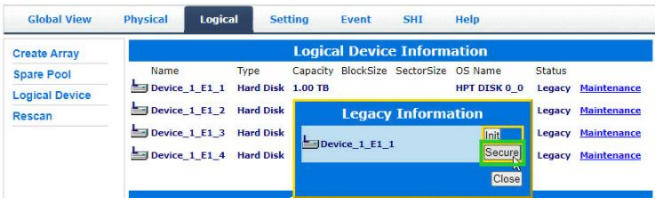


b Failed to enable Disk Security when creating a RAID array



2) As reported by the WebGUI

a Failed to enable Disk Security for disks with the Legacy status



b Failed to enable Disk Security when creating a RAID array

2. Cause of the Issue:

The system could not load the controller UEFI due to one or more incorrect motherboard BIOS settings.

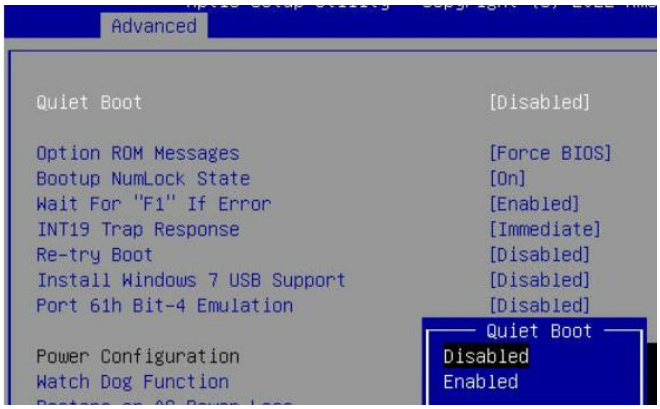
3. Solution:

Two motherboard BIOS menus will be used to explain this issue:

1) Changing the BIOS setting (SuperMicro H12SSL-i motherboard)

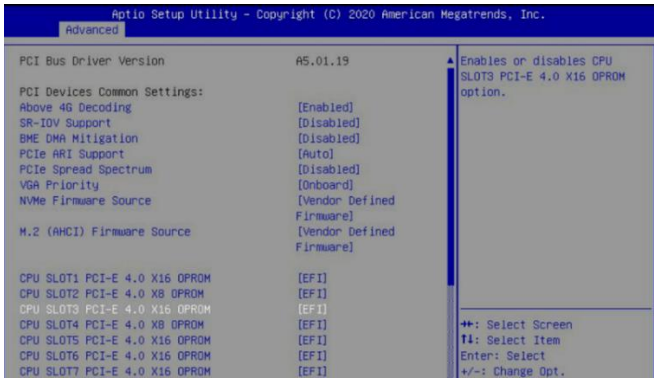
a. **Quiet Boot** is **Disabled**.

Under **Advanced→Boot Feature**, change "**Quiet Boot**" to "**Disabled**".



b. CPU Slot x PCI-E **OPROM** is **EFI.**

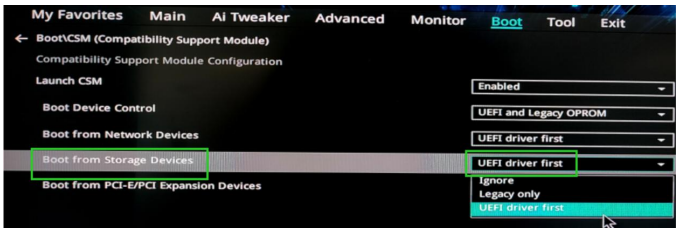
Under **Advanced → PCIe/PCI/PnP Configuration**, change "**CPU Slot x PCI-E OPROM**" to "EFI". "x" represents the PCIE slot assignment.



2) Changing the BIOS setting (WS WRX80-E SAGE SE WI-FI motherboard)

a. **Boot from Storage Devices** is **UEFI driver first**.

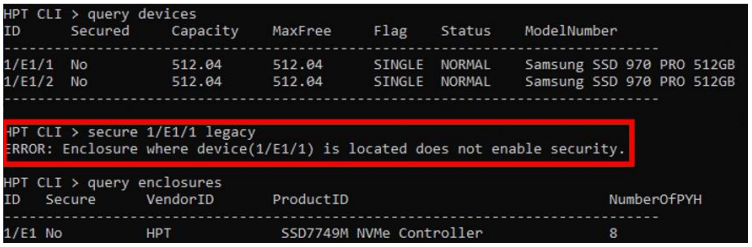
Under **Boot→CSM**, change "**Boot from Storage Devices**" to "**UEFI driver first**".



6.1.2 Enabling Disk Security using the CLI causes enable Disk Security to fail

1. **Description of the Problem:**

   When you enter the command directly in CLI to enable Disk Security, you cannot enable Disk Security successfully. CLI prompts, "**Enclosure, where device(1/E1/1) is located, does not enable security**".



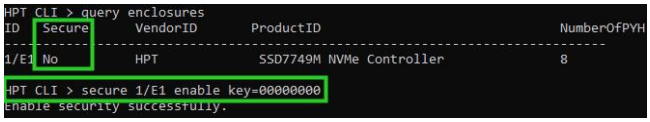
   Note: This issue will only occur when Disk Security is enabled for disks with the "Legacy" status.

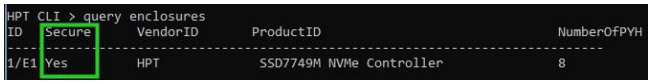
2. **Cause of the Issue:**

   You did not enable Enclosure Security before enabling Disk Security.

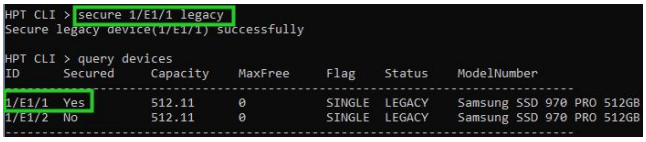
3. **Solution:**

   1) First, enable Enclosure Security. (click here to learn more)





   2) Then enable Disk Security. (click here to learn more)

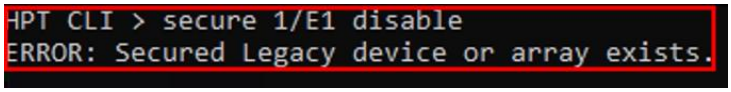


6.2 Why does disable Enclosure Security fail?

1. **Description of the Problem:**

   1) **As reported by the CLI**

   When you enter the command directly in the CLI to **disable Enclosure Security**, you cannot enable Enclosure Security successfully. CLI will report that "**ERROR: Secured Legacy device or array exists**".



   2) **As reported by the WebGUI**

   The process will fail when the WebGUI is used to disable Enclosure Security. A pop-up will prompt, **"Operation not allowed. Secured Legacy device or array exists"**.

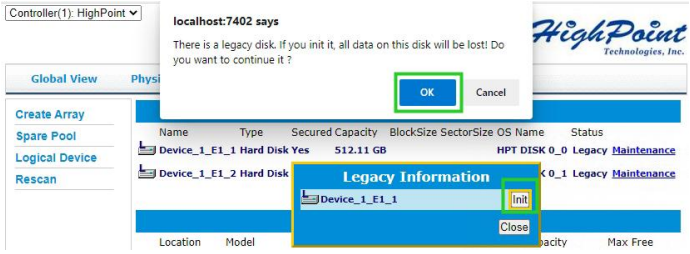
2. **Cause of the Issue:**

   The target enclosure hosts secured disks with the "Legacy" status or a secured array with Disk security enabled before disabling Enclosure Security.

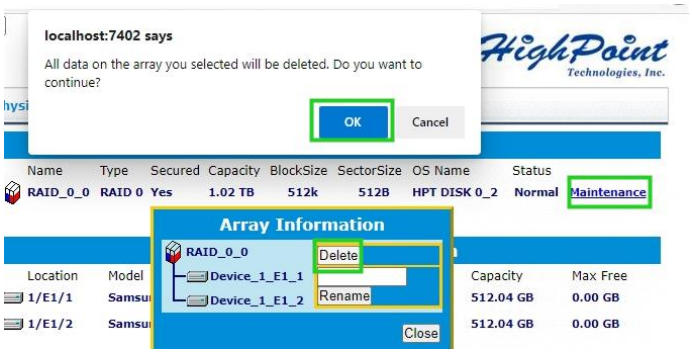
3. **Solution:**

   1) **Solution (WebGUI):**

   a. Init the Legacy disks

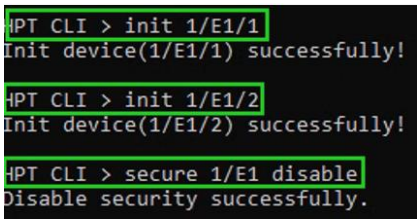


   b. Delete the existing RAID array



2) Solution (CLI):

a. Init the legacy disks



b. Delete the existing RAID array