



# Supported RAID Controllers and Required Cables

Table 1:

Controller	Style	Maximum Front-Facing Drives Controlled	RAID Levels	Required Cables	SCPM <sup>1</sup>	Full Disk Encryption
ENCs-MRAID Controller	PCIe	SFF drives: 2 internal drives	0, 1, JBOD	Not required	Not Available	Yes <sup>3</sup>
<b>Note</b>	This controller cannot be ordered with FBWC. <sup>2</sup>					

1 SCPM = SuperCap power module (RAID backup unit).

2 FBWC: modular flash-based write cache.

3 When using SED drive.

## RAID Cabling

Cisco ENCS-MRAID card does not require additional cable to connect hard drives and RAID card. The flex cable connected to the mainboard can be used to connect to RAID card.

## RAID Card LED Indicator

When RAID card is installed, the LED indicator in the front bezel should turn in solid green.

- [RAID Card Firmware Compatibility, on page 2](#)
- [ENCs-MRAID Controller Considerations, on page 2](#)

- [Support Matrix For ENCS-MRAID Controller, on page 2](#)
- [Drive Types and Sizes Supported, on page 3](#)
- [ENCS-MRAID Drive and Predictive Failure Behavior, on page 3](#)
- [Setting the Preferred Boot Device Order for ENCS-MRAID, on page 3](#)
- [Mixing Drive Types in RAID Groups, on page 3](#)
- [Disks Replacement Considerations, on page 4](#)
- [RAID Backup Units, on page 5](#)
- [Installing ENCS-MRAID Drivers for NFVIS, on page 5](#)
- [RAID Configuration, on page 5](#)
- [Secured RAID Group Configuration, on page 7](#)
- [RAID Disk Group Rebuild, on page 9](#)
- [For More Information, on page 9](#)

## RAID Card Firmware Compatibility

The firmware on the RAID controller must be verified for compatibility with the current Cisco IMC (3.1.5) and BIOS (2.3) versions that are installed on the server. If not compatible, upgrade or downgrade the RAID controller firmware accordingly using the Host Upgrade Utility (HUU) for your firmware release to bring it to a compatible level.

See the HUU guide for your Cisco IMC release for instructions on downloading and using the utility to bring server components to compatible levels: [HUU Guides](#)

## ENCS-MRAID Controller Considerations

### Stripe-Size Limitation When No Flash-Backed Write Cache is Present

This controller does not have a FBWC, the only stripe size available is 64 KB.

### Write-Cache Policy for ENCS-MRAID Controller

This controller does not have SCPM, the default write-cache policy for the ENCS-MRAID controller is *Write Through*.

## Support Matrix For ENCS-MRAID Controller

the following table lists the support for the available controllers by server version.

**Table 2:**

ENCS Version	Boot SSD (Internal M.2) Supported?	ENCS-MRAID Controller Control Front-Facing Drives?
ENCS 5406	No	Yes
ENCS 5408		
ENCS 5412		

## Drive Types and Sizes Supported

- 480GB 2.5" SATA SSD (ENCS-SSD-480G)
- 960GB 2.5" SATA SSD (ENCS-SSD-960G)
- 1TB 2.5" SATA HDD (ENCS-SATA-1T)
- 2TB 2.5" SATA HDD (ENCS-SATA-2T)
- 1.2TB SAS HDD (ENCS-SAS-12T)
- 1.8TB SAS HDD (ENCS-SAS-18T)
- 1.2TB SED SAS HDD (ENCS-SED-12T)

## ENCS-MRAID Drive and Predictive Failure Behavior

- Good drive handling:
  - The physical drive is marked GOOD in the GUI/CLI interfaces and fault LED on the drive is off.
  - The virtual drive (RAID volume group) is marked GOOD in GUI/CLI interface. There is no LED for this.
- Bad/invalid/OMB drive handling:
  - The bad drive is marked BAD in the GUI/CLI interfaces and the fault LED on the drive is solid amber.
- Drive predictive failure:
  - If the drive is part of a RAID volume with a spare, the software performs an auto-copy backup and then marks the drive failed/BAD with the fault LED on the drive solid amber.

## Setting the Preferred Boot Device Order for ENCS-MRAID

The default boot device is internal SSD, disks connected to RAID card are only used as external datastores for VM images.

Refer to BIOS Boot order procedures to select the right boot device and make order of RAID adapter as low as possible.

## Mixing Drive Types in RAID Groups

The following table lists the technical capabilities for mixing hard disk drive (HDD) and solid state drive (SSD) types in a RAID group. However, see the recommendations that follow for the best performance.

Table 3: Drive Type Mixing

Mix of Drive Types in RAID Group	JBOD	RAID-1	RAID-0 (not in 3.6.1)
SATA HDD + SATA HDD	Yes	Yes	Yes
SATA SSD + SATA SSD	Yes	Yes	Yes
SAS HDD + SAS HDD	Yes	Yes	Yes
SAS SED HDD + SAS SED HDD	Yes <sup>1</sup>	Yes <sup>1</sup>	Yes <sup>1</sup>
SAS HDD + SATA HDD	Yes	Yes	Yes
SAS HDD + SAS SED HDD	Yes	Yes <sup>2</sup>	Yes <sup>2</sup>
HDD + SSD	Yes	No	No

<sup>1</sup> With or without encryption enabled.

<sup>2</sup> Virtual disk encryption cannot be enabled.

### Mixing Drive Types in RAID Groups

For the best performance, follow these guidelines:

- Use either all SAS or all SATA drives in a RAID group.
- Use the same capacity for each drive in the RAID group.
- Never mix HDDs and SSDs in the same RAID group.
- Never mix SAS and SED SAS.

## Disks Replacement Considerations

For the best compatibility with NFVIS, follow these guidelines:

- When replace a faulty unit, make sure the replacement unit does not have existing partitions.
- Do not swap the drives between Slot-0 and Slot-1.
- Do not swap or replace drives used by other ENCS system without reformatting it beforehand.
- OIR ( Online Insertion/ Removal ) is not supported in ENCS system.
- Do not attempt to swap or replace drives used by other ENCS systems.

## RAID Backup Units

ENCS-MRAID does not support RAID backup units.

## Installing ENCS-MRAID Drivers for NFVIS

NFVIS 3.6.1 already includes the required drivers and there is no need to install additional driver for this RAID controller.

## RAID Configuration

RAID configuration is done through CIMC Web GUI unless specified otherwise. Though ENCS-MRAID controller can support multiple RAID modes, the physical limitation of ENCS chassis (two physical drives) restrict ENCS-MRAID controller only supporting JBOD and RAID-1 modes under NFVIS 3.6.1.

### JBOD Mode

When a brand new drive is inserted, the drive's status is either **Unconfigured Good** or **JBOD**. If drive is in **Unconfigured Good** status, use the following steps to enable JBOD mode:

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	Log into CIMC.	
<b>Step 2</b>	choose <b>Storage</b> tab on the left pane.	
<b>Step 3</b>	Choose <b>Physical Drive Info</b> tab in middle pane.	
<b>Step 4</b>	Highlight the drive which is in <b>Unconfigured Good</b> status.	
<b>Step 5</b>	Click <b>Set State as JBOD</b> in the <b>Actions</b> field.	
<b>Step 6</b>	Reboot NFVIS to use the new installed drive.	

For existing ENCS with external drives inserted but no RAID card installed, the drives will be set to JBOD mode without further configuration after RAID card installed..

### RAID-1 Mode

After both drives are in **Unconfigured Good** state, use the following steps to create virtual disk (under WebGUI):

### Before you begin

To enable RAID-1 virtual disk on ENCS, refer to **Mixing Drives Types in RAID Groups** for hard drive compatibility and best practice for performance. Before creating virtual disk, both drives must be in **Unconfigured Good** status. If drive is on other status, use CIMC Web GUI/CLI and do the following:

- If disk is in JBOD state: go to **Storage** tab > **Physical Drive Info** tab, choose **Set State as Unconfigured Good** link for this drive.
- If disk is in **Foreign Config** state, go to **Storage** tab > **Controller Info** tab, choose **Clear Foreign Config** in **Action** field.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	Click on <b>Storage</b> tab in left-pane.	
<b>Step 2</b>	Click on <b>Controller Info</b> tab in mid-pane.	
<b>Step 3</b>	Click on <b>Create Virtual Drive</b> from <b>Unused Physical Drives</b> in <b>Action</b> field. Wait for a new pop-up window to open.	
<b>Step 4</b>	<p>In the <b>Create Virtual Drive</b> from <b>Unused Physical Drives</b> pop-up, choose the following:</p> <ul style="list-style-type: none"> <li>• <b>RAID Level:</b> 1</li> <li>• <b>Enable Full Disk Encryption:</b> un-checked</li> <li>• <b>Create Drive Groups:</b> select the physical drives, and click &gt;&gt; to add both disks into Drive Groups.</li> <li>• Fill the following <b>Virtual Drive Properties</b> and click <b>Create Virtual Drive</b> button: <ul style="list-style-type: none"> <li>• <b>Virtual Drive Name:</b> RAID1_12 (auto-assign by GUI)</li> <li>• <b>Strip Size:</b> 64k (default)</li> <li>• <b>Write Policy:</b> Write Through (default)</li> <li>• <b>Access Policy:</b> Read Write (default)</li> <li>• <b>Read Policy:</b> No Read Ahead (default)</li> <li>• <b>Cache Policy:</b> Direct IO (default)</li> <li>• <b>Disk Cache Policy:</b> Unchanged (default)</li> <li>• <b>Size:</b> xxxxxxxx (auto-filled by GUI)</li> </ul> </li> </ul>	
<b>Step 5</b>	Click on <b>Virtual Drive Info</b> tab in mid-pane to verify virtual drive is in <b>Optimal</b> state and health is <b>Good</b> .	

# Secured RAID Group Configuration

ENCS-MRAID controller support Full Disk Encryption (FDE) feature in hardware level when using supported Self-Encryption Drive (SED). To use secured RAID group feature, first you must enable security on RAID controller before you enable security on drives. Use CIMC CLI to enable security with following steps:

## SUMMARY STEPS

1. Log into CIMC.
2. Under CIMC CLI shell, issues the following CLI:
3. Verify that controller's security is enabled.

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	Log into CIMC.	
<b>Step 2</b>	Under CIMC CLI shell, issues the following CLI:	<pre> ENCS5408-FGL210310KJ# ENCS5408-FGL210310KJ# scope chassis ENCS5408-FGL210310KJ /chassis # scope storageadapter SLOT-5 ENCS5408-FGL210310KJ /chassis/storageadapter # ENCS5408-FGL210310KJ /chassis/storageadapter # ENCS5408-FGL210310KJ /chassis/storageadapter # enable-controller-security Use generated key-id 'UCSC-MRAIDC460__21313526'? (y or n)--&gt; y Use suggested security-key 'i7mbSmYjqbXicAFOOb44yeKCGLLdoFlB'? (y or n)--&gt; y ENCS5408-FGL210310KJ /chassis/storageadapter # </pre>
<b>Step 3</b>	Verify that controller's security is enabled.	<pre> ENCS5408-FGL210310KJ /chassis/storageadapter # show detail PCI Slot SLOT-5: Health: Good Controller Status: Optimal ROC Temperature: 60 degrees C Product Name: MegaRAID SAS 3108 R Serial Number: Firmware Package Build: 24.12.1-0039 Product ID: LSI Logic Battery Status: BBU Not Supported NVRAM Size: 32 KB Memory Size: 0 MB Flash Memory Size: 16 MB Cache Memory Size: 0 MB Boot Drive: 0 Boot Drive is PD: false TTY Log Status: Not Downloaded Controller is Secured: 1 </pre>

## JBOD Secured Mode

When controller security feature is enabled, we can verify and configure SED drive. To verify drive is security (FDE) capable, use the following:

- From CIMC web GUI, go to **Storage tab > Physical Drive Info** tab, select the drive, check **General field** in the mid-pane, you should see **Security Capable: Yes**.
- From CIMC CLI, issue the following CLI:

```
ENCS5408-FGL210310KJ /chassis/storageadapter # show physical-drive 1 detail
Physical Drive Number 1:
  Controller: SLOT-5
  Health: Good
  Status: JBOD
  Boot Drive: false
  Manufacturer: HGST
  Model: HUC101812CSS205
  Predictive Failure Count: 0
  Drive Firmware: D703
  Coerced Size: 1143455 MB
  Type: HDD
  Block Size: 512
  Link Speed: 12.0 Gb/s
  Locator LED: false
  FDE Capable: 1
  FDE Enabled: 0
  FDE Secured: 0
  FDE Locked: 0
  FDE Locked Foreign Config: 0
```

To enable FDE feature, do the following:

1. From CIMC web GUI, go to **Storage tab > Physical Drive Info** tab, select the drive, check **General field** in the mid-pane, click on **Enable Secure Drive** from **Actions** field.
2. To verify, similar action is taken
  - From CIMC Web, check **Security Enabled: Yes** string.
  - From CIMC CLI, check the following:

```
ENCS5408-FGL210310KJ /chassis/storageadapter # show physical-drive 1 detail
Physical Drive Number 1:
  Controller: SLOT-5
  Health: Good
  Status: JBOD
  Boot Drive: false
  Manufacturer: HGST
  Model: HUC101812CSS205
  Predictive Failure Count: 0
  Drive Firmware: D703
  Coerced Size: 1143455 MB
  Type: HDD
  Block Size: 512
  Link Speed: 12.0 Gb/s
  Locator LED: false
  FDE Capable: 1
  FDE Enabled: 1
  FDE Secured: 1
```



```
FDE Locked: 0
FDE Locked Foreign Config: 0
```

## RAID-1 Secured Mode

To enable FDE on RAID-1 virtual disk, the steps are similar to previous RAID-1 virtual disk creation, the only difference is on Step 4 when **Create Virtual Drive** from **Unused Physical Drives** pop-up appears, check **Enable Full Disk Encryption** option to enable FDE on virtual disk level.

### Component Replacement Consideration

Unlike the security-disabled configuration, different controller has different encryption key, please advise your system administrator with the following conditions:

- Replacing ENCS-MRAID controller will render FDE-enabled disks data un-retrievable on same host.
- FDE-enabled disks cannot be swapped between systems.
- FDE-enabled disks can be re-used by clear its foreign config and set its state to **Unconfigured Good**.

## RAID Disk Group Rebuild

RAID-1 Disk Group is the only mode can be rebuilt under ENCS-MRAID controller. To rebuild the disk group, you must provide the disk with same type, equal or larger size than virtual disk.

## For More Information

The LSI utilities have help documentation for more information about using the utilities.

For basic information about RAID and for using the utilities for the RAID controller cards that are supported in Cisco servers, see the [Cisco UCS Servers RAID Guide](#).

Full Avago Technologies/LSI documentation is also available:

- For hardware SAS MegaRAID - [Avago Technologies/LSI 12 Gb/s MegaRAID SAS Software User's Guide, Rev. F](#)
- For embedded software MegaRAID - [LSI Embedded MegaRAID Software User Guide](#)

For More Information