



HPE MSA storage array data-at-rest encryption

Contents

Executive summary	3
Audience	3
Secure data encryption standards.....	3
FIPS 140-2 standard	3
AES-256.....	3
Data encryption using SEDs.....	4
Benefits of using the MSA storage array with FIPS 140-2 SEDs.....	5
Self-encrypting disks.....	6
Supported storage components	7
Key management	7
SED management interfaces.....	7
Local key manager.....	7
Lock keys and encryption keys.....	7
Managing FDE settings.....	8
Changing FDE General Configuration	8
Repurposing disks.....	12
Setting FDE import lock key IDs.....	12
Loss of power scenarios.....	13
Power failure on the array	13
Powering down the array	13
Terminology.....	13

Executive summary

As the requirements for protecting stored customer data become more stringent, organizations are seeking storage manufacturers that provide a stored data protection method that is compliant with National Institute of Standards and Technology (NIST) standards and Federal Information Processing Standard (FIPS) 140-2.

To meet these needs, [Hewlett Packard Enterprise \(HPE\) MSA storage](#) arrays support FIPS 140-2 compliant self-encrypting drives (SEDs). These consist of a disk drive with an ASIC built into the drive controller's chipset, which automatically encrypts and decrypts all data sent to and from the drive media.

This white paper explains how the MSA storage array uses disk-based data encryption. It also provides an overview of data-at-rest encryption advantages, the various states of the MSA storage array, and instructions on managing data-at-rest encryption on the MSA storage array using SEDs.

Audience

This white paper is intended for MSA storage array administrators who have experience using the MSA storage array's graphical user interface, the Storage Management Utility (SMU).

Secure data encryption standards

Standards provide a means to assess the level of security a system or subsystem provides. Here's a quick overview of the two standards used in data-at-rest encryption on MSA storage arrays: FIPS 140-2 and Advanced Encryption Standard (AES)-256.

FIPS 140-2 standard

Federal Information Processing Standards are developed by the U.S. federal government for computer systems. FIPS 140-2 is issued by NIST. It describes the requirements for an encryption methodology and is used to accredit cryptographic modules, which include both hardware and software components.

Security levels within FIPS 140-2 standard

FIPS 140-2 defines four security levels which a product must adhere to:

- Level 1 is primarily used for software-only encryption; this level imposes very limited security requirements.
- Level 2 improves on Level 1 by requiring features that show evidence of tampering. SED disks typically include a tamperproof cover over the electronics section on the bottom of the disk and tamperproof seals placed on the mating surfaces of the disk drive.
- Level 3 adds physical tampering resistance to disassembly of the device; furthermore, if tampering is detected, the device must be able to erase critical security parameters (CSPs). Physical security mechanisms might include the use of strong enclosures and tamper detection response circuitry.
- Level 4 provides the highest level of security. The physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access.

All disk drives on encryption-ready MSA storage arrays are FIPS 140-2 Level 2 certified.

AES-256

The Advanced Encryption Standard is a specification for the encryption level of electronic data established by NIST in 2001. AES is a symmetric key algorithm, which uses the same key for encrypting and decrypting data on a disk drive.

Data encryption using SEDs

All data is encrypted by the disk drive mechanism before being written to disk, as illustrated in [Figure 1](#). Data enters the disk drive as readable clear text; upon being sent to the disk, the data enters a special chipset found on SED disk drives. This chipset encrypts the data before being written to the disk.



Figure 1. Data encryption

All data written to each FIPS 140-2 disk uses Full Disk Encryption (FDE), meaning all data encryption is handled at the drive level and no external software or hardware is needed to encrypt data. The benefits of FDE are:

- FDE uses government standard-based encryption and is an industry-wide standard.
- FDE uses AES-256.
- A dedicated engine provides full-speed encryption contained on every drive.
- The encryption key is unique and protected on the media.
- The encryption key itself is encrypted and stored on the media

MSA storage arrays use a passphrase, provided by the user, to generate a lock key ID. After the passphrase is provided and the lock key ID is generated, the system can be secured. When the system is secured, the lock key ID is used to unlock the SEDs in the system, allowing access to the data. The system cannot revert to an unsecured state without being repurposed, which performs an Instant Secure Erase on the disks. If the passphrase and generated lock key ID for a system are different from the passphrase and generated lock key ID associated with a disk, the system cannot access data on the disk, and shows the disk usage as UNUSABLE. Clearing the lock key IDs on a secured array and power cycling the array denies access to data on the disks until the passphrase is re-entered and the lock key IDs are regenerated. Individual disks in the system can be repurposed, which changes the encryption key on the disks, performing an Instant Secure Erase on them.

Caution

Be sure to record the passphrase because it cannot be recovered if lost.

Benefits of using the MSA storage array with FIPS 140-2 SEDs

Each FIPS 140-2 SED disk, which is deployed within the MSA storage array, meets the Level 2 requirement of the FIPS 140-2 standard. This provides assurance that it uses sound security practices such as approved, strong encryption algorithms and methods. Benefits of these security practices include:

– Data-at-rest security

- SEDs automatically lock when powered off, protecting customer data from unauthorized access if drives are lost or stolen and when decommissioning failed drives.
- Whenever a drive is removed from the MSA storage array in which it was secured, the data residing on that drive is automatically protected and can only be accessed by returning it to the original system or through an import operation with a passphrase.

– Drive failure and replacement

- There is no need for special handling of failed drives; data is secure after it leaves the MSA array because the lock key remains with the array, not the drive.
- Rekeying the system helps ensure that a failed drive can never be unlocked, even in the secured system it came from.

– Repurpose and disposition

- The Instant Secure Erase feature changes the encryption key on the drive, making data permanently inaccessible.

– Performance

- SEDs offer full interface speed encryption, providing full-drive performance, which scales with additional drives.

– Secure key management

- Encryption keys are never exposed to the user; only the user-created passphrase is known.
- Encryption keys are never exposed outside the drive.
- Encryption keys are implemented with AES-256 strength.
- The local key manager (LKM) on the array creates the lock key by encrypting the passphrase.
- The array enforces passphrase strength.
- Encryption on the drive cannot be turned off.

– Secure transport

- The entire system can be locked, preventing unauthorized access while the system is transported from site to site.
- Access is restored only with a user-defined passphrase.

– Secure import and export

- Disk groups can be removed and imported from one secure system to another.
- After the system is initially secured, data on the removed disks is always secured and locked until unlocked by the import system.

– Securing system with existing data

- SEDs always encrypt data and therefore can be secured at any time without data loss.
- After an SED is secured by the system, it cannot be unsecured without repurposing the drive, which performs an Instant Secure Erase where all existing data is permanently inaccessible.

Self-encrypting disks

The SED is at the heart of data encryption and customer data security. Each SED in an [HPE MSA storage array](#) contains an ASIC used in the encryption and decryption of data.

Note

This ASIC is not the same as the MSA ASIC contained within the array controller, as illustrated in [Figure 2](#). Data encryption and decryption occur at the drive physical layer and are not part of the MSA firmware. The MSA storage array provides local key management for each disk, but does not participate in encrypting or decrypting the data.

When data is presented to the drive, as illustrated in [Figure 2](#), the drive will act upon the data as a normal data request. The drive electronics are responsible for checking and maintaining data integrity before the data enters the data encryption engine. Other parity generation and checks that occur within the drive electronics are outside the scope of this paper.

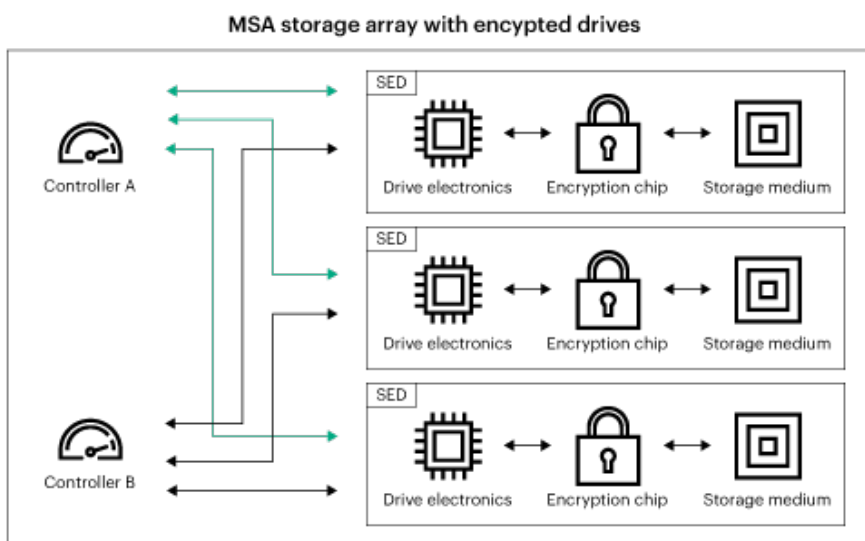


Figure 2. Data checks and encryption

The actual data encryption occurs within the logic of the encryption chip, as shown in [Figure 3](#). As previously mentioned, the encryption engine uses AES-256 when encrypting data being stored on the physical disk medium.

[Figure 3](#) also shows the inner band where the secure encryption key resides if array encryption is enabled. The secure encrypted key generated by the [local key manager](#) (explained in the Local key manager section) secures the SED to the array in which the key was generated. Unauthorized removal of the disk drive locks the SED and no data access can be gained.

Destruction of the key permanently removes access to the data. All data on the disk drive remains encrypted, but without the key to decrypt the data, it is worthless.

Note

On SEDs, data is always encrypted on the storage medium; no license is necessary. Enabling encryption on the array protects the SEDs from any malicious intent by locking the disks to the array in which encryption is enabled. The same array encryption locking key is used for all disks within the same encrypted storage array.

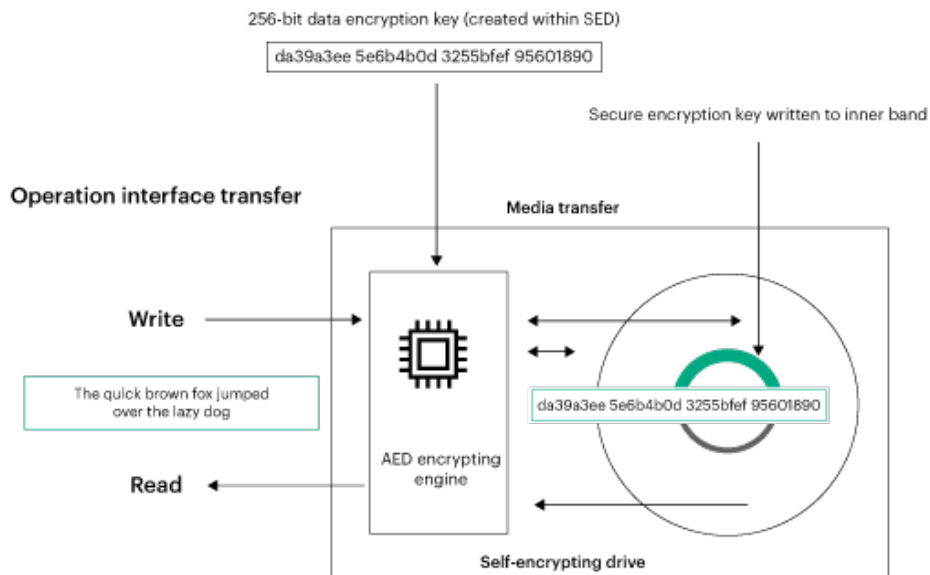


Figure 3. Drive encryption engine

Supported storage components

FDE is supported on all HPE MSA 2040 and HPE MSA 2050 storage arrays with supported SEDs; refer to the HPE MSA 2040 Storage QuickSpecs or the HPE MSA 2050 Storage QuickSpecs for details.

Key management

Management of the secure encryption key and SED access features is provided by an LKM, which is built into the MSA storage array. Specific management features allow control of encryption features including:

- Secure array system
- Rekey
- Lock system
- Import
- Instant Secure Erase or Repurpose

SED management interfaces

The FDE functionality can be managed using either the SMU, which is a target-based web user interface presented from the array, or the command line interface (CLI), which is accessible from a Secure Shell (SSH), telnet, or USB serial connection.

Local key manager

The LKM provides the functionality for securing and managing a system. As part of securing, unlocking, and importing self-encrypting drives, the LKM stores encrypted copies of the current and import lock keys. The current lock key is used to unlock the drives at power up. The import lock key is used when importing a disk set that was secured by another system.

Lock keys and encryption keys

The SEDs store a hash of the lock key and encryption key. The lock key hash is used to authenticate the lock key as part of the unlock operation performed by the LKM. The encryption key is used to encrypt and decrypt the data stored on the drive. The encryption key is stored in an encrypted format on the drive and does not change except when an Instant Secure Erase (repurpose) operation is performed.

Managing FDE settings

The SMU is a web-based interface for configuring, monitoring, and managing the storage system. For more information on accessing and using the SMU, visit the [HPE MSA 2040 User Guide](#) or the [HPE MSA 2050 User Guide](#).

In the Full Disk Encryption panel of the SMU interface, you can change settings for these tabs:

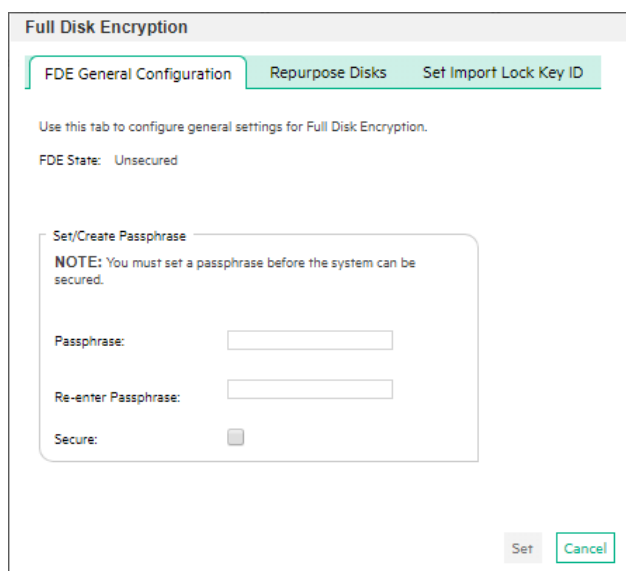
- FDE General Configuration
- Repurpose Disks
- Set Import Lock Key IDs

Changing FDE General Configuration

Use the FDE General Configuration tab of the Full Disk Encryption panel to:

- Set or create the passphrase used to generate the lock key.
- Clear lock keys to deny access to data on the disks after the system is power cycled.
- Secure the system so that data is not available without the lock key.
- Repurpose the system, which securely erases all data on the disk drives.

Figures 4 and 5 present the FDE General Configuration options depending on whether or not the passphrase is set.



Full Disk Encryption

FDE General Configuration Repurpose Disks Set Import Lock Key ID

Use this tab to configure general settings for Full Disk Encryption.

FDE State: Unsecured

Set/Create Passphrase

NOTE: You must set a passphrase before the system can be secured.

Passphrase:

Re-enter Passphrase:

Secure:

Set Cancel

Figure 4. FDE General Configuration (passphrase not set)

Full Disk Encryption

FDE General Configuration | Repurpose Disks | Set Import Lock Key ID

Use this tab to configure general settings for Full Disk Encryption.
Enter the current passphrase to enable access to the configurations below.

FDE State: Unsecured Current Passphrase:

Lock Key ID: 725A4636

Set/Create Passphrase
Sets or changes the lock key for the use of Full Disk Encryption. The lock key is derived from the passphrase and stored within the system. Ensure you record the passphrase and lock key ID returned by the command, as they are not recoverable if forgotten.

Passphrase:

Re-enter Passphrase:

Clear All FDE Keys
Clears all keys used with Full Disk Encryption.
One use of this command is to temporarily deny access to data on the disks during a period when the system will not be under your physical control.

Secure System
Changes the overall state of the system for the use of Full Disk Encryption.
Use this option to secure the system. In a secured system, each disk is secure and inaccessible outside the current system.

Figure 5. FDE General Configuration (passphrase set)

Setting the passphrase

You can set the FDE passphrase the system uses to generate a lock key ID to unlock the FDE-capable disks and allow read and write capabilities. If the passphrase and lock key ID for a system are different from the passphrase and lock key ID associated with a disk, the system cannot access data on the disks.

Caution

Be sure to record the passphrase because it cannot be recovered if lost.

To set or change the passphrase:

1. From the SMU, click the **System** topic.
2. Select **Action → Full Disk Encryption**. The Full Disk Encryption panel opens with the FDE General Configuration tab selected (see [Figure 4](#)).
3. Enter a passphrase in the Passphrase field. A passphrase is case-sensitive and can include 8–32 printable UTF-8 characters except for the following: ", < > \
4. Re-enter the passphrase.
5. Optional: Select the **Secure** checkbox to secure the system when the passphrase is set. If this is selected, the Set button changes to Set and Secure.
6. Click **Set** or **Set and Secure**; a dialog box confirms the passphrase was changed successfully.

Clearing lock keys to deny data access

Lock keys are generated from the passphrase and manage locking and unlocking the FDE-capable disks in the system. Clearing the lock keys and power cycling the system denies access to data on the disks. Use this procedure when the system will not be under your physical control.

If the lock keys are cleared while the system is secured, the system enters the FDE lock-ready state in preparation for being powered down and transported.

After the system has been transported and powered up, the system and disks enter the secured, locked state. As a result, disk group status becomes quarantined offline (QTOF), pool health becomes Degraded, and volumes become inaccessible.

To restore access to data, enter the passphrase for the system's lock key ID. After providing the passphrase, disk groups are dequarantined, pool health is restored, and volumes become accessible.

Note

The FDE tabs are dynamic. In the FDE General Configuration tab, the Clear All FDE Keys option is not available until the current passphrase is entered in the Current Passphrase field. If there is no passphrase, set one by using the procedure described in [Setting the passphrase](#).

To clear lock keys:

1. From the SMU, click the **System** topic.
2. Select **Action → Full Disk Encryption**; the Full Disk Encryption panel opens with the FDE General Configuration tab selected (refer to [Figure 5](#)).
3. Enter the passphrase in the Current Passphrase field.
4. In the Clear All FDE Keys section, click **Clear**; a dialog box is displayed:
 - a. To clear the keys, click **OK**.
 - b. To cancel the request, click **Cancel**.

Securing the system

An FDE-capable system must be secured to enable FDE protection.

Note

The FDE tabs are dynamic. In the FDE General Configuration tab, the Secure option is not available until the current passphrase is entered in the Current Passphrase field. If there is no passphrase, set one by using the procedure described in [Setting the passphrase](#).

To secure the system:

1. From the SMU, click the **System** topic.
2. Select **Action → Full Disk Encryption**; the Full Disk Encryption panel opens with the FDE General Configuration tab selected (refer to [Figure 5](#)).
3. Enter the passphrase in the Current Passphrase field.
4. In the Secure System section, click **Secure**.

Repurposing the system

Repurpose a system to return its FDE state to unsecure.

Caution

Repurposing a system erases all disks in the system.

Note

The FDE tabs are dynamic. In the FDE General Configuration tab, the Repurpose System option is not available until the system is secure and all disk groups have been removed from the system.

Full Disk Encryption

FDE General Configuration | Repurpose Disks | Set Import Lock Key ID

Use this tab to configure general settings for Full Disk Encryption.
Enter the current passphrase to enable access to the configurations below.

FDE State: Secured Current Passphrase:

Lock Key ID: CA632F5A

Set/Create Passphrase
Sets or changes the lock key for the use of Full Disk Encryption. The lock key is derived from the passphrase and stored within the system. Ensure you record the passphrase and lock key ID returned by the command, as they are not recoverable if forgotten.

Passphrase:

Re-enter Passphrase:

Clear All FDE Keys
Clears all keys used with Full Disk Encryption.
One use of this command is to temporarily deny access to data on the disks during a period when the system will not be under your physical control.

Repurpose System
Repurposes the system, which secure erases all disks and leaves the system in an unsecured state. Before starting this action, all data (including volumes and disk groups) must be deleted from the system.

Figure 6. FDE General Configuration (secured)

To repurpose the system:

1. Delete all disk groups in the system; removing disk groups effectively deletes all data on the disks but does not securely erase them.
2. From the SMU, click the **System** topic.
3. Select **Action → Full Disk Encryption**; the Full Disk Encryption panel opens with the FDE General Configuration tab selected (see [Figure 6](#)).
4. In the Repurpose System section, click **Repurpose**; a dialog box is displayed:
 - a. To repurpose the system, click **OK**.
 - b. To cancel the request, click **Cancel**.

Repurposing disks

You can repurpose a disk that is no longer part of a disk group. Repurposing a disk resets the encryption key on the disk, effectively deleting all data on the disk. After a disk is repurposed in a secured system, the disk is secured using the system lock key ID and the new encryption key on the disk, making the disk usable to the system.

Caution

Repurposing a disk changes the encryption key on the disk. This is known as an Instant Secure Erase, which effectively deletes all data on the disk. Repurpose a disk only if you no longer need the data on the disk.

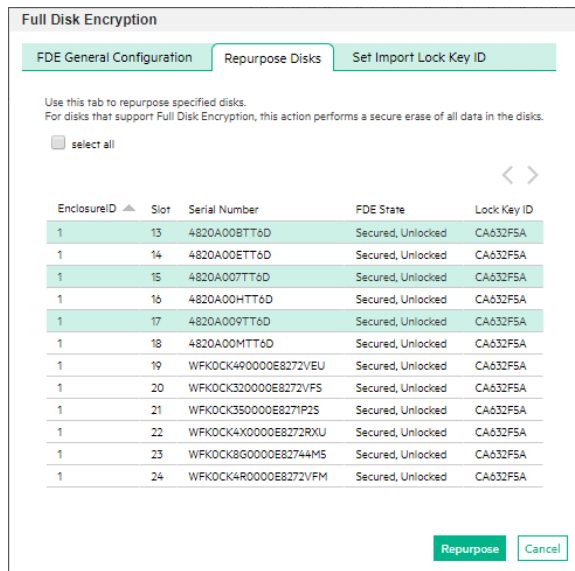


Figure 7. Full Disk Encryption—Repurpose Disks

To repurpose a disk:

1. From the SMU, click the **System** topic.
2. Select **Action** → **Full Disk Encryption**; the Full Disk Encryption panel opens with the FDE General Configuration tab selected (refer to [Figure 5](#)).
3. Select the **Repurpose Disks** tab (see [Figure 7](#)).
4. Select the disks to repurpose, or click the **Select all** checkbox to repurpose all FDE disks in the system. Multiple disk selection is not available on the HPE MSA 2040 storage array.
5. Click **Repurpose**; a dialog box is displayed:
 - a. To repurpose the selected disk, click **OK**.
 - b. To cancel the request, click **Cancel**.

Setting FDE import lock key IDs

You can set the passphrase associated with an import lock key to unlock FDE-secured disks that are inserted into the system from a different secure system. If the correct passphrase is not entered, the system cannot access data on the disk. After importing disks into the system, the disks become associated with the system lock key ID and data is no longer accessible using the import lock key. This effectively transfers security to the local system passphrase.

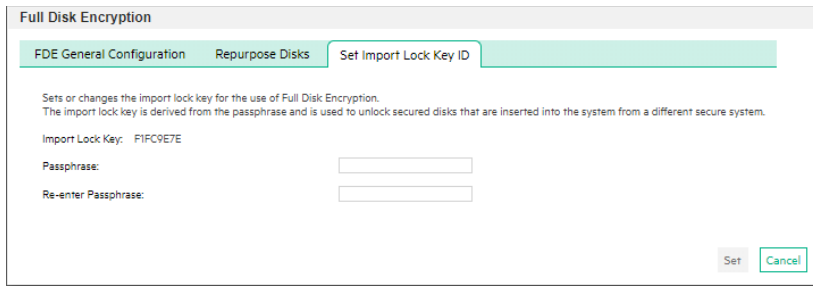


Figure 8. Full Disk Encryption—Set Import Lock Key ID

To set or change the import passphrase:

1. From the SMU, click the **System** topic.
2. Select **Action → Full Disk Encryption**; the Full Disk Encryption panel opens with the FDE General Configuration tab selected (see [Figure 5](#)).
3. Select the **Set Import Lock Key ID** tab (refer to [Figure 8](#)).
4. In the Passphrase field, enter the passphrase associated with the displayed lock key.
5. Re-enter the passphrase.
6. Click **Set**; a dialog box confirms the passphrase was changed successfully.

Loss of power scenarios

A power loss can affect access to data on a secured array in different ways depending on whether it is planned or not. Both scenarios are briefly detailed in this section.

Power failure on the array

In the event of a power failure within the data center, each drive is protected by a unique encryption key and data cannot be accessed without that unique key. Drives cannot be removed and put into another array for data retrieval without importing them into another encrypted array. Having a unique passphrase for each encrypted array within the same data center is recommended. After power is restored to the data center, a normal start up of the array restores access to data stored on the array by the host systems.

Powering down the array

Users should follow standard procedures in powering down an array. When the array is powered back on, the local key manager unlocks access to the host data. If the FDE keys have been cleared before shutdown of the array, the passphrase is required to gain access to the drives and data.

Terminology

Key definitions related to encryption of HPE MSA storage arrays include:

- **CSP:** Critical security parameters
- **FDE:** Full Disk Encryption
- **FIPS:** Federal Information Processing Standard
- **LKM:** Local key manager
- **NIST:** National Institute of Standards and Technology
- **SED:** Self-encrypting drive

Resources

[HPE MSA 2040 SAN Storage](#)

[HPE MSA 2050 SAN Storage](#)

Learn more at

[HPE MSA Storage](#)

Visit [HPE.com](#)

[Chat now](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

a00050848ENW, Rev. 1

HEWLETT PACKARD ENTERPRISE

[hpe.com](#)

