



SafeStore FAQ

What is FDE?

Full Disk Encryption is encrypting data at rest on a hard disk drive. Any of several methods can accomplish this, including software and host-based encryption.

What is SED?

Self Encrypting Drive is one method of implementing FDE. This method puts the encryption circuitry directly on the disk drive. SEDs encrypt everything written to the drive and de-encrypt everything read from the drive. Once a SED is secured, if the drive is ever powered down or removed, the SED becomes “locked” and the encryption key within that drive will not encrypt or decrypt data making the drive unreadable to an individual who does not have the correct authorizations. A security-enabled SED may be lost or stolen, but it will not expose its data to an unauthorized user.

Do all vendors use the term SED?

No. Some vendors may still refer to their drives as FDE. This is not incorrect; it is just not as descriptive as SED.

What are the alternatives to SED?

- Controller-based encryption (CBE)
- Host-based encryption
- Appliance-based encryption

What is Host-Based Encryption?

Host-based encryption is an application which runs on a server. Host-based encryption is very CPU intensive and its performance does not scale. Consequently, host-based encryption is typically used to encrypt a small percentage of the data. This requires rigorous data classification, which is time-consuming, difficult and error-prone.

What is CBE?

Controller-Based Encryption is one method of implementing FDE. This method puts the encryption engine on the RAID controller. LSI has selectively offered CBE, but does not do so in the Channel because of the performance advantages and ease of use of the SED solution

What is the TCG Opal Security Subsystem Class (SSC)?

Opal is the TCG SED specification for laptop/desktop environments. The requirements for this environment are quite different from the server/DAS space. We do not support TCG Opal SSC and have no plans to do so. We have tested several Opal drives and can verify they do NOT function properly with SafeStore Encryption Services within MSM.

What is Emerald??

Emerald is the TCG Enterprise SSC Revision 1.0, intended for enterprise server and storage environments. LSI urges enterprise drive vendors to implement Enterprise SSC and to move to Marble as soon as possible.

What is Marble?

Marble SSC (in development) is the next generation of TCG storage specification. It is not completely backwards compatible with either Enterprise or Opal, but is a converged specification. LSI urges enterprise drive vendors to implement Enterprise SSC and to move to Marble as soon as possible.

What specifications do we support?

LSI MegaRAID® Release 4.1 (i.e. Amicalola Falls) supports Trusted Computing Group (TCG) Enterprise SSC Revision 1.0 (i.e. Emerald).

What are SafeStore™ encryption services?

SafeStore encryption Services are a collection of features within LSI Storage Products that support FDE. SafeStore encryption services are available with LSI MegaRAID Release 4.1 and currently support Instant Secure Erase and Local Key Management.

What products will support SEDs?

SafeStore Encryption Services are offered on the LSI 6Gb/s MegaRAID SAS 9260DE-8i and 9280DE-8e products. Additional solution points will be added in the future. Note: the DE in the product name denotes Data Encryption/SafeStore.

Will SafeStore be offered on LSI 3Gb/s MegaRAID controllers?

LSI 3Gb/s MegaRAID SATA+SAS controllers will not support SEDs, as the firmware has not been built or validated with SED key management.

What services does SafeStore offer?

SEDs that are TCG Enterprise SSC compliant can be locked/unlocked through MegaRAID Storage Manager (MSM). The security wizard is simple to use and provides protection against disk drive theft, server theft, and simplifies drive disposal.

Is the “Instant Secure Erase” feature of SED drives supported by MegaRAID technology?

“Instant Secure Erase” means that an authorized administrator can overwrite the on-board encryption key, thereby rendering the encrypted data unreadable. The MegaRAID technology supports this feature on all 6Gb/s products (i.e. SafeStore products are NOT required).

What encryption algorithm is used by SEDs?

The Advanced Encryption Standard (AES) from NIST (National Institute of Standards and Technology) is implemented, with a 128-bit or 256-bit encryption key. AES is defined in the NIST publication FIPS 197 (Federal Information Processing Standard) and has been adopted internationally as an encryption standard. The Seagate implementation of AES in drive circuitry has received NIST certification through an independent laboratory, as tested against the FIPS 197 standard.

Does the SED functionality affect disk drive performance?

No. Since the AES algorithm was chosen by NIST as optimal for hardware implementations, and the SED has its AES engine built into the electronics, the throughput affect is imperceptibly small (a few millionths of a second). SED drives operate at the same throughput and response time levels as non-SED drives. Furthermore, the incorporation of the SED into the drives (vs other FDE implementations) means that encryption horsepower scales perfectly with the number of drives in the system.

Why was AES 128 implemented initially instead of AES 256?

Both the NSA and NIST have asserted that AES-128 provides sufficient protection. There are $2^{128} = 3.4 \times 10^{38}$ possible keys with 128 bits, which is a huge key space. NIST estimates that AES 128 is safe from key-search techniques for at least the next 30 years. In addition, AES 256 requires four more iterations of the core AES algorithm than does AES 128, which would slightly reduce the throughput and increase the cost of the product.

Have the SEDs received FIP 140-2 certification, which is a standard for “cryptographic modules”?

No. The TCG Storage WorkGroup has developed the SED specifications for a variety of drive types and environments (eg, laptop, enterprise, optical). The TCG has been working with NIST and the NSA (National Security Agency) on the challenge that the “cryptographic module” implementing the AES algorithm inside the drive is tightly integrated (for efficiency, cost savings, and added security) with the remaining drive controller electronics. This integration makes FIPS 140 testing especially challenging, since the traditional view is that cryptographic modules are standalone. In addition, the short life cycles of a given drive model are contrary to the relatively long testing time for FIPS 140. Alternatives are being pursued. In the meantime, the NSA has issued an ‘acceptance’ letter to Seagate for their SED laptop drive: suitable for sensitive and classified national security data.

If MegaRAID controllers are deployed into data centers, which are “secure”, why is the additional protection of SED needed?

SEDs protect stored data-at-rest whenever the drive leaves the owner’s control. Drives are being re-purposed, repaired, or de-commissioned every day. A recent Seagate study showed 50,000 drives leaving data centers daily. Moreover, a study by one of the world’s largest computer system companies found that 90 percent of the drives returned as “failed” were readable to some extent! Drives do move out of data centers, often not under the owner’s direct control, containing sensitive corporate data. The combination of drive locking and data encryption provides, at minimal cost, the additional protection needed for the data in the event a drive leaves the data center. Also, the “rapid erase” feature makes de-commissioning a drive both simple and inexpensive.

Are there “backdoors” to the SEDs?

No. There is no way to circumvent the security measures provided by the drive. For example, if the Security Key is lost, the owner has no recourse for gaining access to the encrypted data. But, security best practices dictate that sensitive or critical data should be backed up, as well as critical parameters like Security Keys.

Can I have SED and non-SEDs mixed in an environment powered by a single MegaRAID controller?

Yes. But, non-SEDs cannot be part of an encryption-protected RAID set. SEDs can be used in non-encryption-protected RAID groups. This means that a customer could purchase all SEDs and turn on the encryption protection, as desired. Of course this actually means turning on the locking function, as the drives are always encrypting. The locking function is configured by selecting the appropriate feature on the MegaRAID management console for those drives and defining a Security Key.

What disk drives have been tested?

To date, we have validated our solution with TCG Enterprise SSC compliant Seagate SEDs. It is our intent to validate with as many TCG compliant drives as possible.

When a secure volume is deleted, does the drive security remain enabled?

Yes. The only way to disable security is to perform an instant secure erase, which will re-provision those drives.

With instant secure erase, what can I erase...an individual drive, a volume group?

Instant secure erase is on a drive-by-drive basis. It is not possible to erase a secure drive that is part of a secure volume group. You must first delete the volume group. Once the volume group is deleted and the drive then becomes unassigned, the drive can then be instantly secure erased.

Can an unauthorized user boot a system with SEDs?

Yes, the server can be configured to pause during the MegaRAID boot sequence for a password. If the appropriate password is not entered in three attempts, the server will still boot but the data on the SEDs will be inaccessible.

What if the boot volume itself is encrypted?

If the OS boot partition is secured, the server can be configured to pause during the MegaRAID boot sequence for a password. If the appropriate password is not entered in three attempts, the server not boot.

Is the data on the MegaRAID controller's cache secure with SED and SafeStore encryption services?

No. As this is a security issue of the physical access to the hardware. It is recommended that the administrator take precautions to maintain physical control and security of the server itself.

Do SEDs have lower usable capacity because the data is encrypted or because capacity is needed for the encryption engine and keys?

No. The usable capacity of a drive is not reduced with SED.

Do all MegaRAID controllers support SEDs?

No. SafeStore Encryption Services are only available on LSI 6Gb/s MegaRAID products. Instant Secure Erase is available on all 6Gb/s products. The lock or "auto-lock" function (local key management) is only available on boards which contain the DE designation (i.e. MegaRAID SAS 9260DE-8i and SAS 9280DE-8e).

Do all Seagate drives support SEDs?

No. Seagate markets specific SKUs, which support SED functionality

For more information and sales office locations, please visit the LSI web sites at: lsi.com lsi.com/contacts
Phone: 1.866.574.5741 or 1.610.712.4323

LSI, the LSI logo, MegaRAID and SafeStore are trademarks or registered trademarks of LSI Corporation.

All other brand and product names may be trademarks of their respective companies. LSI Corporation reserves the right to make changes to any products and services herein at any time without notice. LSI does not assume any responsibility or liability arising out of the application or use of any product or service described herein, except as expressly agreed to in writing by LSI; nor does the purchase, lease, or use of a product or service from LSI convey a license under any patent rights, copyrights, trademark rights, or any other of the intellectual property rights of LSI or of third parties.

Copyright ©2009 by LSI Corporation. All rights reserved.
August 2009

