LSI™ MegaRAID® SafeStore™ Software FAQ

What is LSI MegaRAID SafeStore Software?

LSI MegaRAID SafeStore software, together with self-encrypting drives (SEDs), secures a drive's data from unauthorized access or modification resulting from theft, loss or repurposing of drives.

What kind of real world security challenge does MegaRAID SafeStore software resolve?

Local key management using the Auto-lock feature locks the drive and secures data on the drive the moment a drive is removed from a system or a drive or system is stolen. Instant Secure Erase feature allows users to instantly and securely render data on SED drives unreadable, saving businesses time and money associated with secure drive erasure by simplifying decommissioning of drive and preserving hardware value for returns and repurposing.

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-crypt 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, and 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 SafeStore software solution.

How can I manage SafeStore software?

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 MegaRAID SATA+SAS products (i.e. MegaRAID SafeStore software is NOT required).

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 containing sensitive corporate data do move out of data centers, often not under the owner's direct control. The combination of MegaRAID SafeStore and SEDs 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.

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

Yes. But, non-SED drives 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 Auto-lock function, as the drives are always encrypting. The auto-lock function is configured by selecting the appropriate feature on the MegaRAID management console (MegaRAID Storage Manager) for those drives and defining a Security Key.

What specifications do we support?

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

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 effect on throughput is imperceptibly small (a few millionths of a second). SEDs operate at the same throughput and response time levels as non-SED drives. Furthermore, the incorporation of the encryption 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 x 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.

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.

What disk drives have been tested with SafeStore software on MegaRAID SATA+SAS controllers?

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. Please visit http://www.lsi.com/channel/support/marketing_resources for a complete list of tested SEDs.

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 will 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.

Which MegaRAID controllers support SafeStore software?

To obtain SafeStore software, channel customers currently have two options.

1) Since July 2009, LSI has offered 6Gb/s MegaRAID SATA+SAS controllers with SafeStore software pre-installed. These include the MegaRAID SAS 9260DE-8i and MegaRAID SAS 9280DE-8e.

2) For the initial launch of advanced software options, SafeStore software will also be offered as a physical key that can be installed on select MegaRAID SATA+SAS controllers. These include the MegaRAID SAS 9260-4i, 9260-8i, and 9280-4i4e. In the future, the advanced software options will be available via electronic licenses and will be supported on the full line of MegaRAID SAS 9260 and 9280 series controllers. At this time, the pre-configured MegaRAID "DE" boards will be phased out.

Will SafeStore software be offered on LSI 3Gb/s MegaRAID SATA+SAS 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 operating systems are supported with MegaRAID FastPath software?

All supported operating systems for given MegaRAID controller

Can I combine SafeStore software with other advanced software from LSI (ie Recovery, CacheCade, MegaRAID FastPath™, etc)?

The initial launch of advanced software, including SafeStore software, will utilize physical keys that are installed on select MegaRAID SATA+SAS controllers. Because the controller can only accept one key at a time, SafeStore software cannot be combined with other advanced software options at this time. There is one exception to this rule; if a customer purchases or already owns a MegaRAID 'DE' board that is pre-configured with SafeStore software, they can add a physical key for any of the other advanced software options (b/c the spot for the physical key is not being occupied already). In the future, with electronic license fulfillment, customers will have the ability to choose or combine as many advanced software options as they would like for their MegaRAID controller.

What does it cost and how do I buy SafeStore software?

MegaRAID SafeStore software has a suggested retail price of $89 and is available through the LSI worldwide network of distributors, integrators and VARs.

http://www.lsi.com/channel/WhereToBuy

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**