SILICON MECHANICS
SERVERS • STORAGE • HPC

Expert included.

Drive Options:

			Requires		
Type	**Use Case**	**Encryption Used**	**SafeStore***	**TPM**	**Password**
SE	Data wipe: Overwrite only	On-board cryptographically secure pseudorandom number generator	N	Optional	No
ISE	Data Wipe: Instant Data Deletion	Encrypts all data with a built-in factory key	N	Optional	No
SED/TCG-E	Encryption: Data-at-rest protection	AES-256	Recommended	Optional	Yes
SED-BDE	Encryption: Data-at-rest protection	AES- 128, ATA Security Commands	Recommended	Optional	Yes
SED-FIPS/TCG-FIPS	Encryption + Tamper-resistant seal	AES-256	Recommended	Optional	Yes

LSI SafeStore Key: Recommended for encryption key management for multiple drives in RAID array.

SafeStore helps to create and locally manage SED authentication keys. Provides high level of security for self-encrypting drives attached to MegaRAID controller cards.

Type	Hardware Key	Software Key
Downtime	Zero downtime. In the event of controller failure, remove hardware key and plug it into new card with no downtime	Some downtime involved- In the event of controller failure, you need to get the safe ID from the controller BIOS and the serial # and associate it with a controller name. Then another code is generated which you type into the BIOS.
Activation Key	Hardware Key needs to be shipped	Comes instantly with purchase

Requirements to activate LSI SafeStore:

- LSI MegaRAID controller: Hardware/Software key available for 9361-4i/8i. Software key available for 9380-8e.
- Self-encrypting drives
- Silicon Mechanics installs LSI SafeStore license and Customer sets password.

LSI SafeStore, together with self-encrypting drives (SEDs), secures a drive’s data from unauthorized access or modification resulting from theft, loss or repurposing of drives. Auto-Lock feature locks the drive and secures the data on the drive the moment a drive is removed from a system or a drive or system is stolen.

TPM (Trusted Platform Module): Locks complete system data

TPM hardware can be used on motherboard for additional data security. Drives removed from existing system, don't work when placed in new system.

The TPM and the SED are not required to interact. However, depending on the software authentication, secrets held within the TPM could be used to authenticate or help authenticate to the SED. Please note that in the event of system failure, if the user wants to move the SED to a new system, the management software would have to support moving it from one TPM to another. Otherwise the SED can’t be unlocked, as it is in part controlled by the TPM in the dead system.

Glossary:

- SE (Secure Erase): With SE, drive overwrites data (including inaccessible areas), and this process takes hours.
- ISE (Instant Secure Erase): With ISE, drive simply deletes key from memory/makes it inaccessible.
- SED (Self-Encrypting Drive): Encrypts/decrypts data-at-rest and not data-in-flight. Supports AES 128/256.
- BDE (Block Data Encryption): Standard available in HGST SATA drives only.
- FIPS (Federal Information Processing Standard): U.S Government security standard used to approve cryptographic modules. To know if your drive is FIPS certified, check this link: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

Disclaimer: Information presented in this article is from manufacturers’ websites and other Internet sources.