MaxTronic International Co., Ltd.
Tel: 886-2-2218 4875 Fax: 886-2-2218 4896 4F., 529, Zhongzheng Rd., Xindian Dist. New Taipei City 231, Taiwan

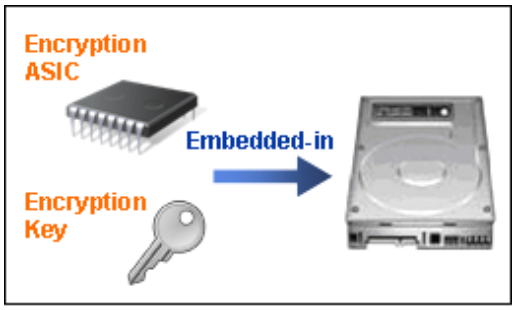
Introduction about SED (Self Encryption Drives)

SED Advantage

- Reduced Cost via Standardized Technology
- Reduced control headaches and disposal costs
- Optimum Storage Efficiency
- Reduced Re-Encryption
- Superior Security

What is SED (Self-Encrypting Drives):

- Encryption controller (ASIC) & Encryption Key are both embedded on hard drive itself. SED encryption is automatic and transparent without performance degradation. An encryption key is generated randomly from factory by each SED.



How SED works?

- SED automatically performs full disk encryption when a Write is performed by using the embedded encryption key before the data is written to the disk. When a Read is performed, the encrypted data is decrypted before leaving the drives.
- When the new SED is acquired, the embedded encryption key is in clear text form, until the user evokes the authentication key. The SED will still encrypt – decrypt all write or read data on the disk if the authentication key is not evoked, but anyone can also write and read the clear text data on the disk.
- There are two major functions for SED: ***" Secure Erase"*** and ***"Auto Lock".***

Instant Secure Erase

- The owner just simply begins using SED in normal operation; eliminate the need to manage the authentication key. When owner decides to repurpose or dispose the drives, simply perform the "Instant Secure Erase", which would implement a "key erase" to replace the existing encryption key with a new encryption key which generated randomly within the drives.
- All the data that had been written with the previous key are garbled when decrypted with the new encryption key. The drives would leave as the original factory default SED, ready for the owner to use it as a "Secure Erase only" mode or in "Auto Lock" mode as new ones.

Benefit of using "Instant Secure Erase"

- Eliminating the need to overwrite or destroy data.
- Securing warrant and expired lease return
- Enabling drives to be repurposed securely.
- However data are not secured while drives are stolen.

Auto Lock:

Authentication manage of SED in "auto-lock" mode

1. Evoke authentication key by outer source (F/W or application)
2. Decrypt (unlock) the encrypted encryption key, clear encryption key and encrypts or decrypt the data

Headquarters
MaxTronic International Co., Ltd.
sales@maxtronic.com.tw

America
Arena-MaxTronic Inc.
sales@maxtronic.com

3. When Authentication is completed during powered on, encryption is fully transparent to the storage system and performs its traditional functions normally.
4. The drive's data encryption key would be **"auto-locked"** whenever the drive is powered down or disconnected.
5. When system is powered on again, the SED requires an authentication key before being able to unlock its encryption key and read any data on the drive.
6. If the authentication is matched, the drive would be unlocked and use the authentication from storage system to decrypt a copy of the encryption key stored in the specific area of the disk.
7. Once the authentication process is completed, the drive is unlocked until the next power down.
8. The authentication process only required on first power on, would not repeat with each read and write.
9. The clear-text encryption key is used to encrypt-decrypt the data write and read from the disk.
10. Drives would work in standard fashion during data transfer, and the encryption and decryption would transparently work on the background.

When and How to use SED?

- SED is good for securing data resident in disks while drives leave the owner's control, preventing data been accessed while drives are retired, stolen, return for warranty or repurposed.
- SED would not secure data in transit or preventing data been hacked by outer attack while systems are on, or unauthorized access if systems are stolen or return for repair. Enterprise would apply different encryption or security policy to protect data from above threatens.
- It would be highly recommended to use Arena RAID solutions incorporate with SED in following manners:
  - To Use "Instant Erase" for newly acquired HDDs to replace the factory default encryption keys.
  - Evoke "Auto Lock" function by using the "SED Key" management
  - Conduct "Instant Erase" again if HDDs are retired, disposed, repurposed or returned for warranty, but before that be sure to backup the data which still need to be maintained.

==========

FAQ:

Can I use SED in regular equipment? Or do I need special H/W or F/W to use SED?

SED can be used in standard drives form in regular equipment, however the unique "Instant Secure Erase" and "Auto Lock" mode support by SED would only effected by special F/W or application S/W. Currently the above 2 features (MaxSure) support by all Arena Janus II series (SS-880x, SS-660x, SS-4501x, TS-4801E/R) and NOVA series.

What are "*MaxSure*" features mean?

MaxSure encryption service is unique function in Arena RAID solutions for supporting SED, which include 2 features: "Instant Secure Erase" and "Authentication Key management"

Does the SED functionality affect disk drive performance?

No, since the algorithm and the engine are built into the ASIC, the impact on throughput is relatively small. SED drives operate at the same throughput and response time as non-SED drives.

Headquarters
MaxTronic International Co., Ltd.
sales@maxtronic.com.tw

America
Arena-MaxTronic Inc.
sales@maxtronic.com

Are there backdoors to the SED?

No, there is no way to retrieve the encryption made by drives. If the authentication key is lost, the owner would have no source to access the encryption data while the controller is faulty or disk groups been removed. However, in the best practice the sensitive and critical data should be backup as well as the critical information like authentication key.

Would the data been accessed by some of the data rescue tools or from the disc platter?

No, if the HDDs evoked by “Auto Lock” or running “Instant Erase”, there is no chance to retrieve the encryption key to decrypt the encrypted data resident in HDD, nor any chance to source data from the disc platters.

Can I have SED and non-SED mix in an environment using Arena RAID solutions?

Yes, you can have SED and non-SED drives in same environment, but they could not mix in same Disk Group. The user could use both SED and non-SED in the environment to setup tiers storage by level of data sensitivity.

Which disk drives have been tested?

Currently there are 3 SED models supply by Seagate Technology approved by Arena RAID solutions:

ST3500425SS	3.5” 1TB 6Gb/s SAS 7200rpm 16MB SED
ST3300557SS	3.5” 300GB 6Gb/s SAS 15000rpm 16MB SED
ST9500431SS	2.5” 500GB 6Gb/s SAS 7200rpm 16MB SED

When a volume group is deleted, does the drive security still enabled?

Yes, the only way to erase authentication key is to run the “Instant Secure Erase” to return to the original factory default.

Does the use of SED lowering the usable capacity because data is encrypted?

No, the usable capacity of the drives would not be reduced with SED.

Can I download the SED key?

Yes, SED key is managed by RAID controller, and the key can be downloaded out of RAID system as a text file for backup.

How many SED key could be configured?

There is only one SED key would be generated in one RAID system.

When would the SED key been requested?

There are 3 circumstances need to use SED (authentication) key:

1. Create SED array.
2. Modify SED key
3. SED array roaming

Headquarters
MaxTronic International Co., Ltd.
sales@maxtronic.com.tw

America
Arena-MaxTronic Inc.
sales@maxtronic.com