SED (Self-Encrypting Drives) Operation Guide

Firmware

2.14 and above

Support RAID Model

TS-480xE/R, SS-450xE/R, 660xE/R, 880xE/R, Nova series

Revision History

Version	Date	Remarks
1.0	2010/4/28	Initial release
1.1	2010/5/7	Update content
1.2	2010/5/11	Update 2.4 SED Array Roaming Update Q&A
1.3	2010/6/17	Update Q&A
1.3a	2010/7/8	Update 2.2.1 Erase data in Hard Disk
1.4	2010/7/14	Official Release

Table of Content

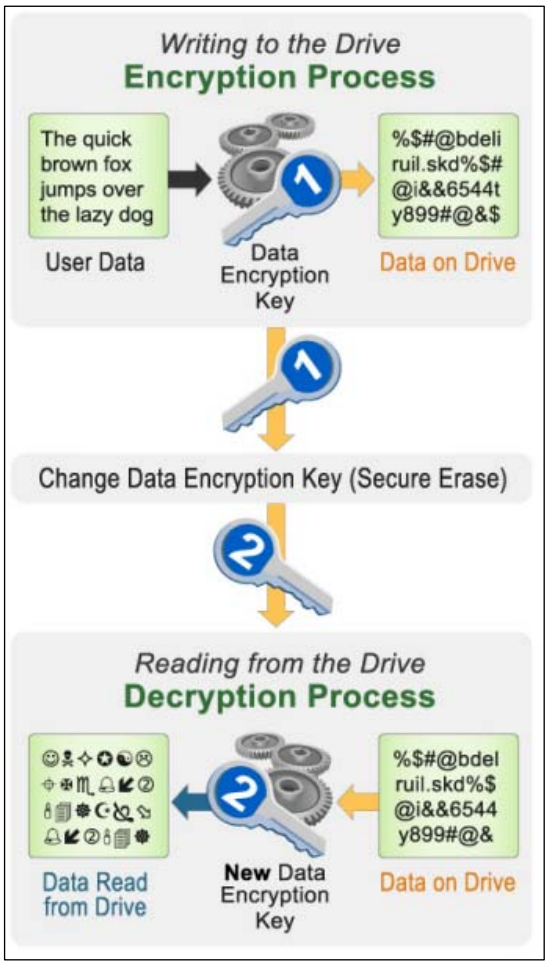
1. Overview

This guide teaches user how to create Self-Encrypting Drives (**SED**) array, and introduces SED Key management, Instant Secure Erase and SED array roaming.

RAID subsystem offers hardware based, disk drive integrated encryption for data that resides in the disks. All encryption executed by SED itself which provides simplest, most cost-effective and highest performance security storage. The SED implements FIPS approved AES-128 bit encryption algorithm; a government grade data security feature, no backdoor available.

1.1 Self-Encrypting Drives Technology

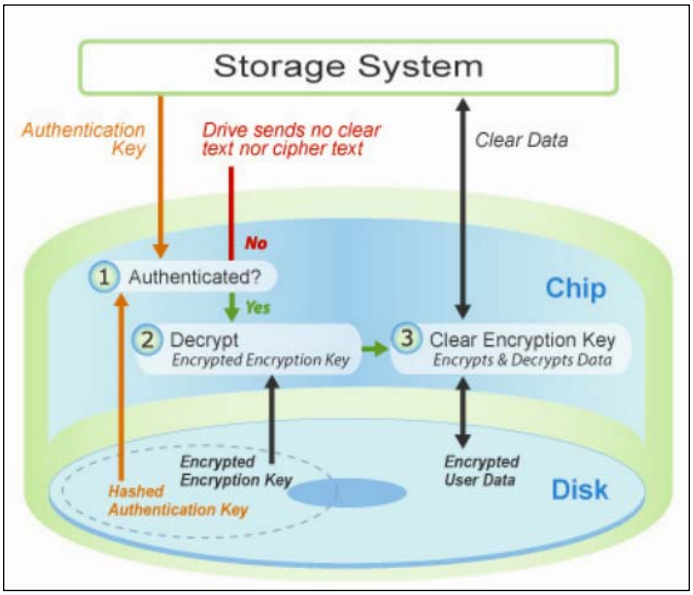
Each SED randomly generates an encryption key that is embedded on the drive. The SED automatically performs full disk encryption; when a write is performed, clear text enters the drive and is first encrypted (using the encryption key embedded within the drive) before being written to the disk. When a read is performed, the encrypted data on the disk is decrypted before leaving the drive. During normal operation an SED is completely transparent to the system, appearing to be the same as a non-encrypting drive. The SED is constantly encrypting - encryption cannot be accidentally turned off. When the owner acquires the drive, this embedded encryption key is in clear text form and will remain so until the drive is put in auto-lock mode, where an authentication key is introduced. The drive will encrypt and decrypt all data that it writes to and reads from the disk; however, without establishing an authentication key, anyone can write and read the clear text data on the disk. Setting up the system is quite simple. The owner must decide whether to use the SED in auto-lock mode or only for instant secure erase. Each use case is discussed below.



The following describes the steps that occur during the authentication process of a previously secured drive:

1. Authentication

The storage system gets the authentication key from the key management service and sends it to the correct locked drive. The drive hashes the authentication key and compares the result with the hash of the authentication key that's stored in a secure area of the disk. If the two hashed authentication key values do not match, the authentication process ends, and the drive will not permit reading data from the disk. The drive remains locked.



2. Decrypt the encrypted encryption key

If the two hashes match, the drive is then unlocked, and the drive uses the authentication key it received from the storage system to decrypt a copy of the encryption key (which was previously encrypted with the authentication key) that's stored in a secure area of the disk. Once the authentication process is completed, the drive is unlocked until the next time it is powered down. Note that authentication process only occurs when the drive is first powered on, it does not repeat with each read and write operation.

3. Clear encryption key encrypts and decrypts the data

The clear-text encryption key is then used to encrypt data to be written to the disk and to decrypt data that's being read from the disk. The drive now works in standard fashion during data transfers, with encryption and decryption transparently occurring in the background. Once the drive is put in auto-lock mode, it can be put back into secure erase-only mode only after a secure erase is performed. If an owner wishes to repurpose or retire the drive, the owner would simply perform a secure erase to replace the encryption key.

1.2 Self-Encrypting Drives Advantage

The advantages to use SED enabled as the encryption policy to prevent data theft from any unauthorized access would be:

- ✓ **Simplified key management**
- ✓ **Most cost-effective via standardized technology**
- ✓ **Maximum performance**
- ✓ **Superior security**
- ✓ **Eliminate re-encryption and re-purposing**

2. Workflow

2.1 Create SED Array

2.1.1 Preparation for SED array

a. The drive is compatible with RAID system. (Refer to **Appendix A**)

b. The member of SED array cannot mix with non-SED drive.

c. Firmware of RAID system is up to date.

d. In [RAID management]>[Hard Disk], check all SED drives are unused.

- **Auto Lock Mode**: off
- **SED State**: ERASE ONLY
- **Type**: UNUSED

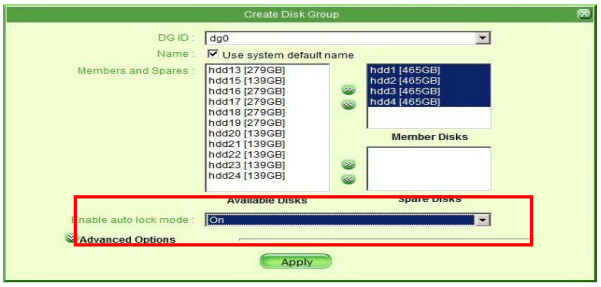
2.1.2 Create SED Array

2.1.2.1 Create DG (Disk Group)

a. In [RAID management] > [Disk Group], press **Create** to create a new DG.

b. Drag SED drives to Member Disk field.

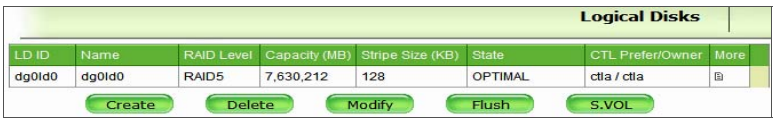
c. Select “Enable auto lock mode” to **On**.



Note: Support SED JBOD drive as well. If you want to configure SED JBOD drive, select the “Enable auto lock mode” to **On** while JBOD creating.

2.1.2.2 Create LD (Logical Disk)

In [RAID management] > [Logical Disk], create a Logical Disk.

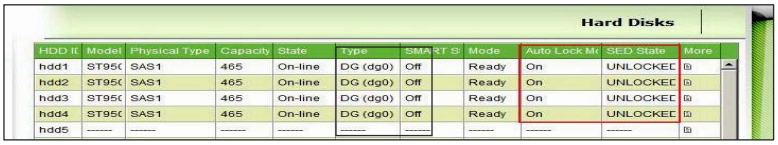


Note: Follow the standard procedure to set host LUN Mapping, please see software manual chapter Storage Provisioning for detail.

2.1.3 Check SED is enabled

In [RAID management] > [Hard Disk], check all SED drives has enabled.

- **Auto Lock Mode**: On
- **SED State**: Unlocked
- **Type**: DG (dg0)

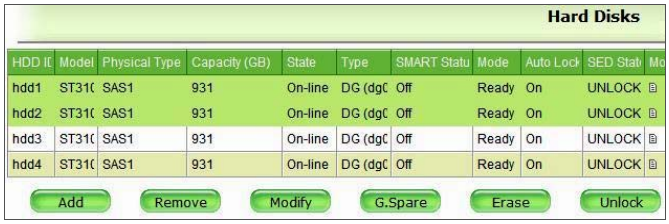


2.2 Instant Secure Erase

Drive retirement is always a headache for data sensitive enterprises such as banks, insurance companies, hospitals, they have to follow governmental laws and regulations to handle drive retirement and it is expensive, time-consuming and error-prone. Instant Secure Erase technology has implemented to instantaneous “rapid” erase for secure disposal or re-purposing. Instant Secure Erase could be performed by Hard Disk or Disk Group. Follow steps below to perform Instant Secure Erase.

2.2.1 Erase data in Hard Disk

a. In [RAID management]>[Hard Disk], left-click the HDD ID to select hard disks wanted to erase, and then press “**Erase**”.



b. In the popup window, click “**Force to erase**” and press “**Confirm**” to erase data instantly.

2.2.2 Erase in Disk Group

a. In [RAID management]>[Disk Group], left-click to select a DG ID wanted to erase, and then press “**Delete**”

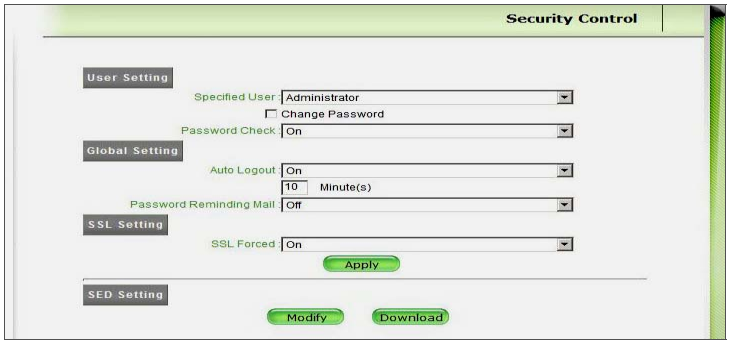
b. In the popup window, click “**Instant Erase**” and press “**Confirm**” to erase data instantly.

2.3 SED Key Management

SED key is managed by RAID controller which used for SED array maintenance (e.g. array roaming), default SED key is “00000000” (eight zero’s) while DG created with SED function enable. It is recommended to administrator to modify (or auto regenerate) the SED key at first time DG is created. The key is also downloadable and be saved at personal computer. Follow steps below to perform SED key management.

2.3.1 Modify SED Key

a. In [System management] > [Security Control] > [SED Setting], click “ **Modify** “.



b. Type in old Key Code in **Old Key** field. (Default: 00000000)

c. Type in new Key Code in **New Key** field or click “ **Gen. Key** ” to auto-generate a Key Code.

Note: SED Key Code must be at least 8 characters and combination of mixing a~z, A~Z and 0~9.

d. Type new Key again in **Confirmed Key** field and click “ **Apply** “.

e. Click “ **Confirm** “ to make new Key available.

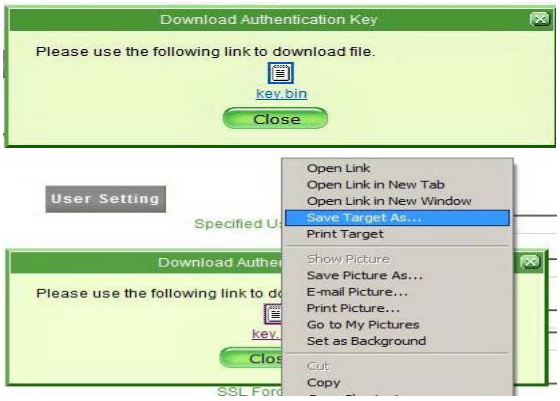
2.3.2 Download SED Key

SED key could export to a context file to save at outside backup which will be used for array maintenance if needed.

a. In [System management]>[Security Control]>[SED Setting], click " **Download** ".

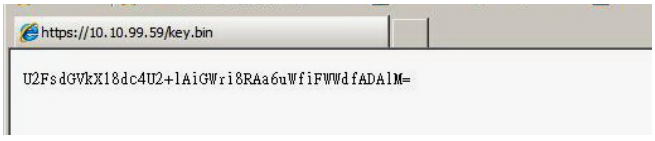
b. Click " **Confirm** " to download the key file. (Option: click **Set password** to give a password to the file)

c. Right-click **key.bin** to save file.



d. Open the file with IE, you will find the SED key.

Note: If SED key file is given a password, it will not possible to read correct SED key by IE browser directly.



2.4 SED Array Roaming

For maintenance purpose, you may need to roam SED Array from original RAID system to another new one. SED Array is allowed to be recognized by new RAID system with the correct SED key. Follow steps below to perform SED Array roaming.

2.4.1 Preparation of new RAID system

a. Confirming the **Firmware/Bootcode** versions are the same with original RAID system.

b. Change **SED key** to match original, refer to chapter 2.3.1 for details.

c. **Online array roaming control** set to " **On** ". (In [Maintenance]>[Miscellaneous].)

2.4.2 Unlock SED drives

a. Insert four SED drives into slot hdd1~4 from the other RAID subsystem.

b. In [RAID management]>[Hard Disk], you will find all SED drives have been locked.

- **Auto Lock Mode**: On
- **SED State**: Locked
- **Type**: Unknown

c. Left-click to select SED drives hdd1~4 and click **Unlock** to unlock all SED drives.

d. Type in correct SED Key code. (Go to next step if you want to load SED key file instead.)

e. Click **Use authentication key file** to load SED key file.

2.4.3 Array Roaming

a. In [Maintenance]>[Array Roaming], the original DG information will appear. Confirm the DG/LD information and then click " **Import** ".

b. Drag the SED drives to **Selected Members** field, press " **Apply** ".

c. SED Array roaming is done!

Appendix A – Certification list of SED drives

Below table contains a list of self-encrypting drive recommended for use in SED Array creating.

2.5inch type: (RAID model: TS-480xE/R)

Vendor	Model	Size	RPM	Speed	Category	SED
Seagate	ST9500431SS	500GB	7200	6Gb/s	SAS	Yes

3.5inch type: (RAID model: SS-450xE/R, 660xE/R, 880xE/R)

Vendor	Model	Size	RPM	Speed	Category	SED
Seagate	ST3300557SS	300GB	15000	6Gb/s	SAS	Yes
Seagate	ST31000425SS	1000GB	7200	6Gb/s	SAS	Yes

Appendix B – Q&A

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 Redundant series (SS-880x, SS-660x, SS-450x 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.

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.

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