# s846 Encrypted SAS SSD

## Frequently Asked Questions

HGST
a Western Digital company

# Frequently Asked Questions

**Q: How do I determine if an HGST s800 series SSD supports encryption?**

A: s842 series of products (up to 2TB) – non-encryption
s846 series of products (up to 2TB) – encryption
This classification applies to both 1.8" and 2.5" form factors.

**Q: What are the key advantages of using the new s846 self-encrypting drive SSDs?**

A: Hardware-based encryption ensures line speed encryption w/o any performance degradation.

- On-par or higher performance and lower latency
- Near-consistent performance between different capacities
- Optimized for lower 4KB block size
- Easily repurpose drives by using Cryptographic Erase

**Q: How does the s846 SED Encryption drive work? Is the SED built into the hardware?**

A: HGST SED SSDs come from our factory with encryption and authentication keys already generated. The default authentication key (MSID) is labeled on the drive.

These drives employ XTS-AES-256 with Cipher Text Stealing (CTS) data encryption mode to encrypt all data prior to being written on the media, and decrypt all data as it is read from the media. Built into the hardware, the encryption engines are always in operation and cannot be disabled. The user needs to take ownership of the drive and activate security in order to use the encryption feature See below for details.

**Q: How do I activate the security on the drive so that unauthorized users can't see the encrypted data??**

A: The security needs to be activated by the user on a newly manufactured drive. Although the user data is always encrypted during storage to the media, the decrypted data is initially immediately accessible through the host interface on this drive, as configured out of manufacturing. To activate the security, the drive should be taken through three steps:

- Taking Ownership of the SED
- Activate and Enroll the SED
- Configure the Locking Ranges

Explanation of these use cases is available in the TCG specification titled "TCG Storage Application Note: Encrypting Storage Devices Compliant with Enterprise SSC (Security Subsystem Classes)." SED management tools from ISVs are available in the market to automate these steps.

Once the security is activated, the drive will not honor any data READ or WRITE requests until the corresponding bands have been unlocked. This prevents user data from being accessed without the appropriate credentials when the drive has been power cycled or removed from its cabinet and installed in another system.

**Q: What do the acronyms XTS and AES stand for?**

A: "XTS" stands for XEX Tweakable Block Cipher with Ciphertext Stealing. "AES" stands for Advanced Encryption Standard.

The XTS-AES mode was designed for the cryptographic protection of data on storage devices that use fixed-length data units.

**Q: What are the default keys on the drive, and what are their functions when they leave the factory?**

A: There are two default set of keys that are set as default on the drive: DEK and MSID.

**DEK: Data Encryption Key**

The drive has in its hardware a true random number generator (TRNG) that is used to derive encryption keys. The 32-byte Data Encryption Key (DEK) is a random number generated by the drive. The DEK is inaccessible to the host system; it never leaves the drive, and is itself encrypted when stored on the media using the authentication key supplied by the user for the corresponding band. Note that for each band during manufacturing, a unique DEK is generated for a total of five DEKs.

**MSID Manufactured SID (SID- Security ID)**

A default password is used when the drive is shipped from the factory where all passwords are set to the value of a unique MSID labeled on the drive. Note that a unique MSID value is generated for each SED manufactured by HGST. This 32-byte random value can be read by the host electronically over the interface. After receipt of the drive, it is the responsibility of the owner to use the default MSID password as the authentication key to authenticate and change all passwords to unique owner-specified values.

**Q: Does HGST support key management of SED drives in a single or multi drive environment?**

A: HGST SSDs are compliant with TCG (Trusted Computing Group) Enterprise Security Subsystem Class specifications There are various Independent Software Vendors( ISVs) who traditionally manage encryption functions and can provide management of self-encrypting drives, both locally and remotely.

**Q: What happens to my data if I lose my AK (Authentication Key)?**

A: If the authentication key is lost, the owner has no recourse for gaining access to the encrypted data. However, security best practices dictate that sensitive or critical data, as well as critical parameters like security keys, should be backed up. The SED management tools from ISVs typically provide key recovery features as part of the management.

**Q: Do s846 drives use up extra user capacity to store keys?**

A: HGST SED SSDs do not need any extra capacity for the encryption engine and keys. The usable capacity of a drive is not reduced with SED, and security protection is maximized.

**Q: What happens to my data if the space upon which the keys are stored goes bad? What is the recovery?**

A: Good security practice dictates that important data is backed up at another location for recovery. To combat an occasional bad sector, HGST SED drives write the encrypted encrypting key to several locations within the drive, thus greatly minimizing the chance that all encrypted copies will be lost. This is the same protection given to all system parameters in an SSD.

As part of good data management practice, we recommend a regular data backup process.

**Q: I like the encryption feature, but don't have key management plans for actively managing the encryption feature. Can I just use this as a normal drive?**

A: Yes—as described in this document, the s846 SED drive can be used as a regular drive, as long as you don't take ownership of the drive. This drive can be used as a plug-and-play device in storage subsystems and servers, as the encryption happens in the background without impacting performance, and is seamless to the OS. Note that the drive will reject read long and write long commands.

**Q: How many bands does the s846 SED drive support?**

A: s846 SED drives support one Global band, and four user bands.

**Q:Does hardware encryption impact the SED performance?**

A: There is no degradation in SED performance, since the encryption engine is built into the drive hardware and works seamlessly while transparent to the user, OS and applications.

**Q: Is HGST hardware-based encryption more secure than software encryption?**

A: Yes. Hardware-based encryption can more effectively restrict unauthorized users from access. In addition, dedicated hardware can exhibit greater performance compared to software. Software-based encryption runs under an operating system that is vulnerable to viruses and data corruption.

**Q: Is HGST s846 SED OPAL compliant?**

A: OPAL is the TCG Specification for consumer drives. We are currently not compliant with OPAL. We are compliant with TCG Enterprise Specifications, the specification for enterprise drives, for XTS-AES 256-bit SED.

**Q: Do HGST s846 SED drives protect data in flight or at rest?**

A: HGST SED drives protect data at rest. Various proven technologies, such as SSL/TNS, protect data in flight.

**Q: Is it easier to repurpose the drive with secure cryptographic erase?**

A: Yes. A significant feature of HGST SED SSDs is the ability to perform a cryptographic erase. This involves the host telling the drive to change the data encryption key for a particular band. Once changed, the data will no longer be recoverable, since it was written with one key and will be read using a different key. Also note that the authentication key will be reverted to the value of MSID, the default password on the label.

HGST
a Western Digital company

FQ007-EN-US-0313-05