Enabling an Intelligent Planet

Technical White Paper

January 22, 2013

Industrial Flash Storage Trends in Software and Security

Many flash storage devices in embedded applications are used to save data but also function as disks for the OS. Most users are blind to their operation and do not know when a memory device is wearing out, and often only remedy the problem after they have already been damaged. To cater to this demand, Advantech has developed a software package called SQFlash Utility, which can check the condition of the memory device at an early stage and inform users well in advance. When the life of the memory device is lower than the specified level, the software will warn users to backup and change to another device.

SQFlash Utility is a flash management software package that contains utilities and APIs to access and configure Advantech SQFlash products. Life Monitoring (S.M.A.R.T.) features help to optimize OS settings to better fit SQFlash and software protection (Security ID Read/Write) features are used for security purposes.

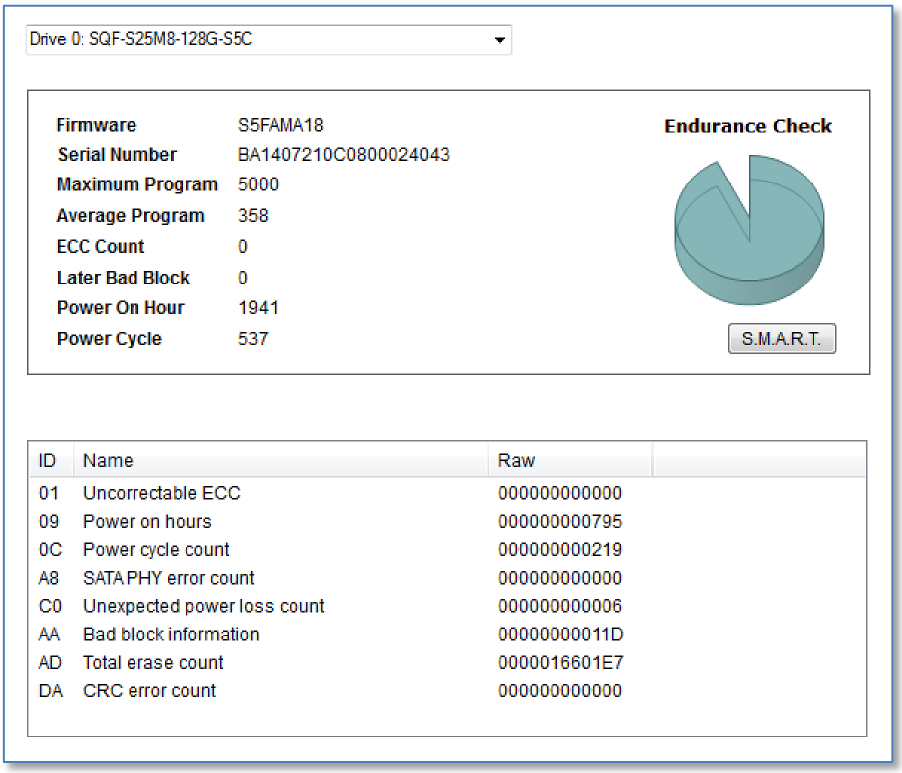
An "access code" protected package provides users with a safe environment, which not only protects the application itself but also prevents security information being read without the same access code.

* Once you type a valid access code with this utility, the system will keep a record and you won't need to type the same access code next time.

Disk Information

Basic disk information like model name, serial number, and firmware version will be revealed in this field. All available S.M.A.R.T. attributes are also displayed for users to monitor disk conditions.

- ❖ Max Program - Max program and erase cycles in SQFlash.
- ❖ Average Program - Average program and erase cycles in SQFlash.
- ❖ Power On Time - Power on accumulated time.
- ❖ ECC Count - Error correction code number of times counter.
- ❖ Endurance Check - Endurance (%) of remaining life is the result of (Average P/E cycles) / (Max P/E cycles).



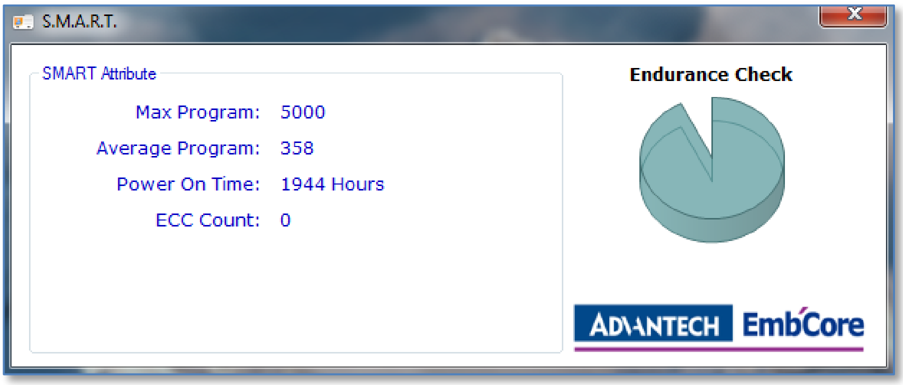
Drive 0: SQF-S25M8-128G-S5C

Firmware	S5FAMA18
Serial Number	BA1407210C0800024043
Maximum Program	5000
Average Program	358
ECC Count	0
Later Bad Block	0
Power On Hour	1941
Power Cycle	537

ID	Name	Raw
01	Uncorrectable ECC	000000000000
09	Power on hours	000000000795
0C	Power cycle count	000000000219
A8	SATA PHY error count	000000000000
C0	Unexpected power loss count	000000000006
AA	Bad block information	00000000011D
AD	Total erase count	0000016601E7
DA	CRC error count	000000000000

* Raw data of S.M.A.R.T. attributes can also be retrieved with this utility.

Disk health can be monitored directly via the SQFlash Utility or functions can be programmed into customized applications via the SQFlash API. A life-span detection mechanism can then be designed accordingly. The Standalone Life Monitoring utility is also available for easier access. Users are strongly recommended to evaluate with SQFlash Utility to make sure a suitable flash storage solution is chosen.



Max Program: 5000

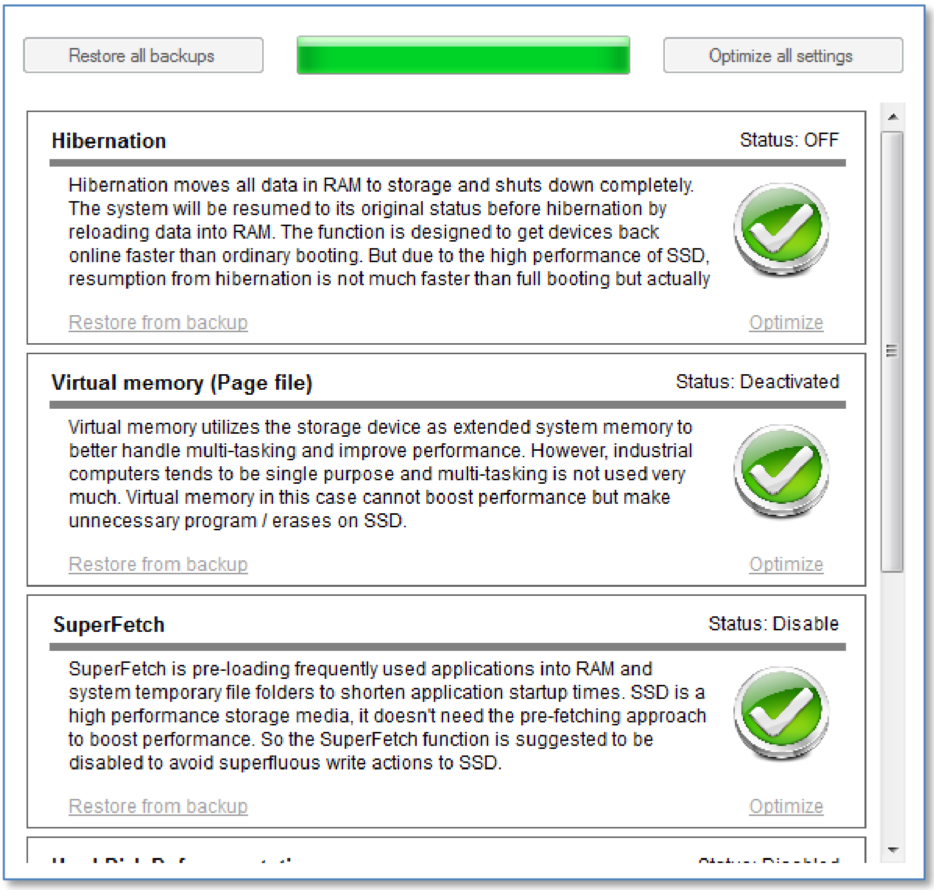
Average Program: 358

Power On Time: 1944 Hours

ECC Count: 0

OS optimizer

Basically, most OS nowadays supports SSD natively and are able to configure systems to fit SSD or HDD installation. However, some conventional OS (such as Windows XP) that are still widely adopted in the industrial computing market were designed only for HDD. So, users are required to check some OS configurations to make sure their SSD is working in optimal condition.



Hibernation Status: OFF

Hibernation moves all data in RAM to storage and shuts down completely. The system will be resumed to its original status before hibernation by reloading data into RAM. The function is designed to get devices back online faster than ordinary booting. But due to the high performance of SSD, resumption from hibernation is not much faster than full booting but actually

Virtual memory (Page file) Status: Deactivated

Virtual memory utilizes the storage device as extended system memory to better handle multi-tasking and improve performance. However, industrial computers tends to be single purpose and multi-tasking is not used very much. Virtual memory in this case cannot boost performance but make unnecessary program / erases on SSD.

SuperFetch Status: Disable

SuperFetch is pre-loading frequently used applications into RAM and system temporary file folders to shorten application startup times. SSD is a high performance storage media, it doesn't need the pre-fetching approach to boost performance. So the SuperFetch function is suggested to be disabled to avoid superfluous write actions to SSD.

- **Disable Hibernation**

Hibernation moves all data in RAM to storage and powers down while retaining its state. The system will be resumed to its original status before hibernation by reloading data into RAM. The function is designed to get devices back online faster than a regular re-boot. But due to the high performance of SSD, resumption from hibernation is not much faster than a full boot but actually makes substantial data writes into SSD.

- **Disable Virtual Memory (page file)**

Virtual memory utilizes the storage device as extended system memory to better handle multi-tasking and improve performance. However, industrial computers tends to be single purpose and multi-tasking is not used very much. Virtual memory in this case cannot boost performance but make unnecessary program / erases on SSD.

- **Disable SuperFetch (PreFetch)**

SuperFetch is pre-loading frequently used applications into RAM and system temporary file folders to shorten application startup times. SSD is a high performance storage media, it doesn’t need the pre-fetching approach to boost performance. So the SuperFetch function is suggested to be disabled to avoid superfluous write actions to SSD.

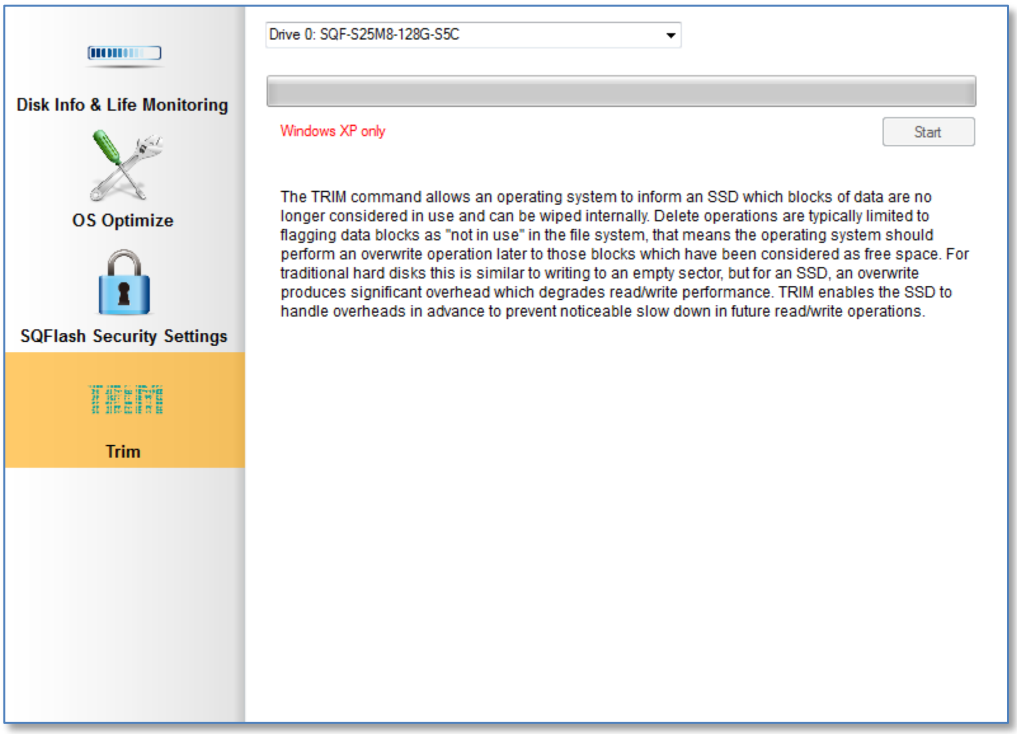
- **Cancel “Hard Disk Defragmentation” in task scheduler**

Hard Disk Defragmentation is an operation to optimize HDD performance that consolidates fragmented file sectors to become consecutive file sectors. This action reduces “seek times” for the HDD actuator. However, the action is not needed for SSD since SSD doesn’t have an actuator. Also, the action would relocate files and additional program / erases would occur to diminish the life of SSD.

TRIM

TRIM command allows an operating system to inform an SSD which blocks of data are no longer considered in use and can be wiped internally. Delete operations are typically limited to flagging data blocks as "not in use" in the file system, that means the operating system should perform an overwrite operation later to those blocks which have been considered as free space. For traditional hard disks this is similar to writing to an empty sector, but for an SSD, an overwrite produces significant overhead which degrades read/write performance. TRIM enables the SSD to handle overheads in advance to prevent noticeable slow down in future read/write operations.

However, TRIM is only supported by Windows versions later than “Vista / 7.” To benefit older Windows versions, a TRIM tool is designed for SQFlash. It will detect if the operating SQFlash supports TRIM and make sure the utility is running with the correct Windows version. The disk can then be optimized with a single click.



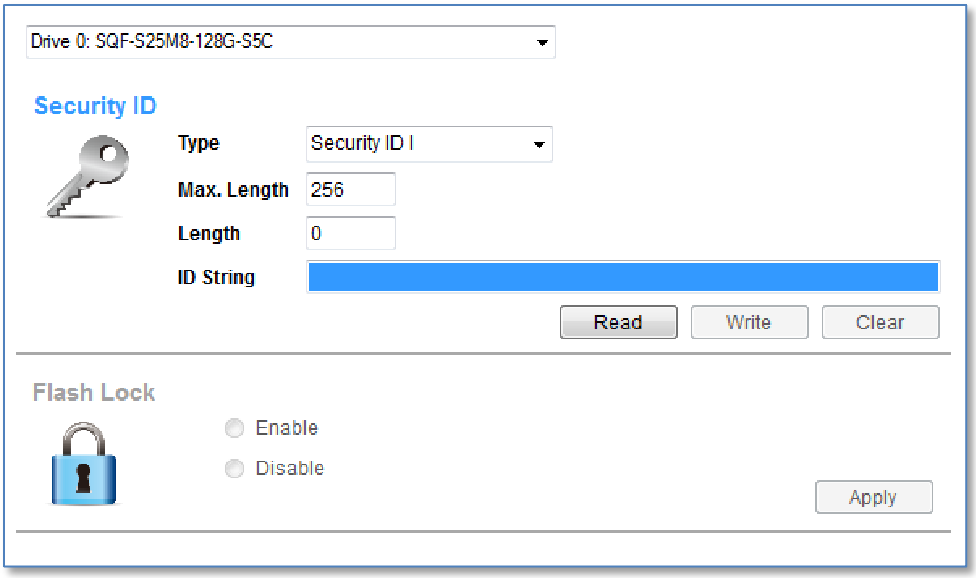
Drive 0: SQF-S25M8-128G-S5C

Windows XP only

The TRIM command allows an operating system to inform an SSD which blocks of data are no longer considered in use and can be wiped internally. Delete operations are typically limited to flagging data blocks as "not in use" in the file system, that means the operating system should perform an overwrite operation later to those blocks which have been considered as free space. For traditional hard disks this is similar to writing to an empty sector, but for an SSD, an overwrite produces significant overhead which degrades read/write performance. TRIM enables the SSD to handle overheads in advance to prevent noticeable slow down in future read/write operations.

SQFlash Integrated Software Security Features

In order to help protect customers' intellectual property, Advantech has designed in a Security ID feature for Advantech SQFlash. Customers can easily implement security functions on their applications based on an encrypted utility and library. The Flash Lock feature helps users to lock SQFlash with the motherboard it operates on to protect flash data from being read.



Drive 0: SQF-S25M8-128G-S5C

Security ID

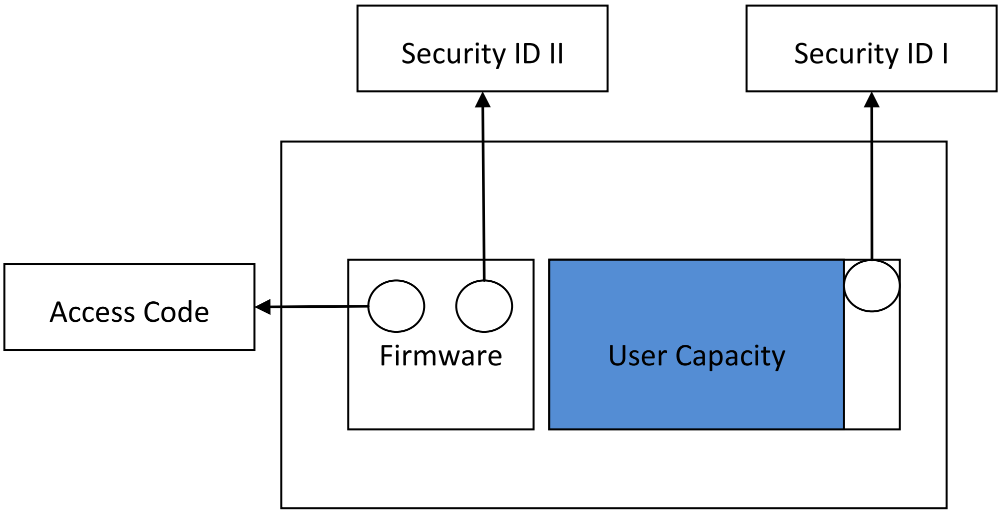
Type: Security ID I

Max. Length: 256

Length: 0

ID String:

Security ID



❖ Security ID I

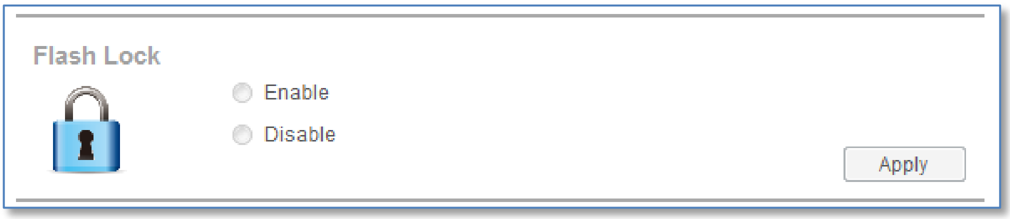
Security ID I can be a full run-time configuration. All read/write access can be performed immediately. After Security ID I is enabled, all disk management access would be disabled, e.g. Format, fdisk, ghost, etc. This is because the SQFlash controller protects the SID area and does not allow any disk I/O to read or write to this area. If any tool or command tries to access this area, it will return a fail instruction.

- **Security ID II**

  This SID will be located into the firmware zone and all disk management access will maintain the same behavior.

Flash Lock

Flash Lock is a mechanism to lock SQFlash with the motherboard through the BIOS and make SQFlash only operate with the corresponding platform. This can help to prevent data being stolen by reading the SQFlash with other computers and card readers. Since the feature is a mechanism between the SQFlash firmware and BIOS, it can work only on Advantech products. If the target platform doesn't support this feature, Flash Lock buttons will be grayed out as follows.

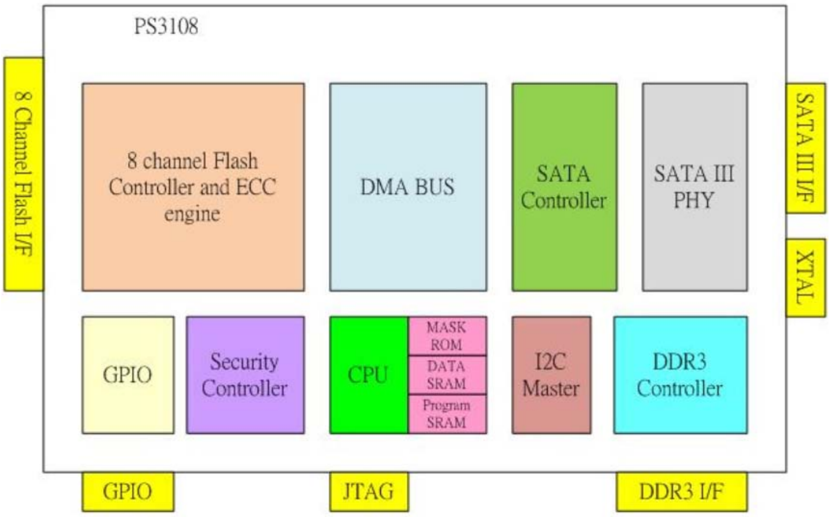


Advanced Hardware Security Functions

SQFlash 820 series SATA III SSD is designed with the Opal Compliant disk encryption standard, which supports in-drive AES 256-bit encryption. For even more critical applications that may need emergency erase, the SSD is equipped with hardware GPIO pins for triggering a high security level erase-at-once command.

AES 256-bit Encryption Key

PS3108 is optionally embedded with a security controller to generate an AES (Advanced Encryption Standard) encryption key for real-time data encryption before storing data into NAND flash. Since data is fully hashed with the 256-bit encryption key, once the controller or firmware has failed, there is no way to access data stored in the NAND flash.



One Touch Emergency Erase

One Touch Emergency Erase is a hardware emergency erase. The low level erase command executed by the controller will be triggered once the GPIO has detected signal interruption. Three different erase levels could be made with SQFlash 820 series products.

- ❖ **Data Erase:** Firmware is kept intact in this mode so the drive is still usable after an erase. It takes around 70 seconds to thoroughly wipe out user data on a 256 GB SSD. However, if the erase process is interrupted, data will not be fully deleted, and remaining data could possibly be accessed after reactivating the device.
- ❖ **Firmware Erase:** The drive will immediately become unusable after execution since firmware will be destroyed in just a few milliseconds. AES is enabled and the encryption key is stored in the firmware, none of the data can be decrypted or recovered in such condition.
- ❖ **Global Elimination:** This is the highest security level erase mode, which is implemented on SQFlash 820 series. Once the erase command is triggered, the controller will proceed with a firmware erase first and follow up with a data erase to make sure the drive is completely wiped and no data is left on the storage media.

SQFlash Offering

Advantech is dedicated to continuously develop security software which protects intellectual property. Advantech's SQFlash Utility software package is a flash management package that contains utilities and API to access and configure Advantech flash storage. It supports Software Protection (Security ID Read/Write) and Life Monitoring (S.M.A.R.T.) features. A product key protected package provides users with a safe environment which not only protects the application itself but also prevents Security ID being read without the same product key while writing. The S.M.A.R.T. attribute contains Max/Average Program and Erase Cycles, Power On Time, ECC count and Life Endurance utilities. Users can monitor directly via the SUSI-SQFlash utility or implement functions into the application via the SUSI-SQFlash API, and a life-span detection mechanism can be designed from the Life Endurance information.