Self-Encrypting Drives for System x

Product Guide (withdrawn product)

Data security is a growing requirement for businesses of all sizes today. While many companies have invested heavily in methods to thwart network-based attacks and other virtual threats, few effective safeguards have been readily available to protect against potentially costly exposures of proprietary data resulting from a hard drive being physically stolen, misplaced, retired, or redeployed.

Self-encrypting drives (SEDs) provide the ultimate in security for data-at-rest and help reduce IT drive retirement costs in the data center. When combined with the compatible RAID controllers, such as the ServeRAID M5015, M5014, and M1015 SAS/SATA Controllers with the appropriate Advanced Feature Key, the 6Gbps SAS SED drives in System x servers deliver superb performance per watt with a cost-effective, secure solution for businesses of all sizes. Self-encrypting drives are also an excellent choice if you need to comply with government or industry rules regarding data privacy and encryption.

These drives are the industry’s top-performing secure hard drives, capable of ensuring protection of data-at-rest against theft or when drives leave your control; reducing IT drive retirement costs and delivering more transactional performance density at the lowest power for environmentally friendly enterprise storage systems.

Figure 1. The IBM 146GB 15K SED Drive

Did you know?

The 128-bit AES security that self-encrypting drives provide can reduce drive retirement expenses while still protecting data and is one of the easiest, most cost-effective security measures you can implement.

Part number information

Table 1. Ordering part numbers and feature codes

Description	Part number	Feature code
IBM 146GB 15K 6Gbps SAS 2.5" SFF Slim-HS SED disk drive	44W2294	5412
IBM 300GB 10K 6Gbps SAS 2.5" SFF Slim-HS SED disk drive	44W2264	5413

The part numbers for each disk drive include the following items:

- One IBM 2.5" SED hard disk drive
- Product publication

Features and Benefits

Self-encrypting drives (SEDs) provide benefits in three main ways:

- By encrypting data on-the-fly at the drive level with no performance impact
- By providing instant secure erasure (cryptographic erasure, thereby making the data no longer readable)
- By enabling auto-locking to secure active data if a drive is misplaced or stolen from a system while in use

The following sections describe the benefits in more details.

Automatic encryption

It is vital that a company keep its data secure. With the threat of data loss due to physical theft or improper inventory practices, it is important that the data be encrypted. However, challenges with performance, scalability, and complexity have led IT departments to push back against security policies that require the use of encryption. In addition, encryption has been viewed as risky by those unfamiliar with key management, a process for ensuring a company can always decrypt its own data. Self-encrypting drives comprehensively resolve these issues, making encryption both easy and affordable.

When the self-encrypting drive is in normal use, its owner need not maintain authentication keys (otherwise known as credentials or passwords) in order to access the data on the drive. The self-encrypting drive will encrypt data being written to the drive and decrypt data being read from it, all without requiring an authentication key from the owner.

Drive retirement and disposal

When hard drives are retired and moved outside the physically protected data center into the hands of others, the data on those drives is put at significant risk. IT departments retire drives for a variety of reasons, including:

- Returning drives for warranty, repair, or expired lease agreements
- Removal and disposal of drives
- Repurposing drives for other storage duties

Nearly all drives eventually leave the data center and their owner's control. IBM estimates that 50,000 drives are retired from data centers daily. Corporate data resides on such drives, and when most leave the data center, the data they contain is still readable. Even data that has been striped across many drives in a RAID array is vulnerable to data theft because just a typical single stripe in today’s high-capacity arrays is large enough to expose, for example, hundreds of names and social security numbers.

In an effort to avoid data breaches and the ensuing customer notifications required by data privacy laws, companies use different methods to erase the data on retired drives before they leave the premises and potentially fall into the wrong hands. Current retirement practices that are designed to make data unreadable rely on significant human involvement in the process, and are thus subject to both technical and human failure.

The drawbacks of today's drive retirement practices include the following:

- Overwriting drive data is expensive, tying up valuable system resources for days. No notification of completion is generated by the drive, and overwriting won't cover reallocated sectors, leaving that data exposed.
- Methods that include degaussing or physically shredding a drive are expensive. It is difficult to ensure the degauss strength is optimized for the drive type, potentially leaving readable data on the drive. Physically shredding the drive is environmentally hazardous, and neither practice allows the drive to be returned for warranty or expired lease.
- Some companies have concluded the only way to securely retire drives is to keep them in their control, storing them indefinitely in warehouses. But this is not truly secure because a large volume of drives coupled with human involvement inevitably leads to some drives being lost or stolen.
- Professional disposal services is an expensive option and includes the cost of reconciling the services as well as internal reports and auditing. Transporting of the drives also has the potential of putting the data at risk.

Self-encyrpting drives eliminate the need to overwrite, destroy, or store retired drives. When the drive is to be retired, it can be cryptographically erased, a process that is nearly instantaneous regardless of the capacity of the drive.

Instant secure erase

The self-encrypting drive provides instant data encryption key destruction via cryptographic erasure. When it is time to retire or repurpose the drive, the owner sends a command to the drive to perform a cryptographic erasure. Cryptographic erasure simply replaces the encryption key inside the encrypted drive, making it impossible to ever decrypt the data encrypted with the deleted key.

Self-encrypting drives reduce IT operating expenses by reducing asset control challenges and disposal costs. Data security with self-encrypting drives helps ensure compliance with privacy regulations without hindering IT efficiency. So called "Safe Harbor" clauses in government regulations allow companies to not have to notify customers of occurrences of data theft if that data was encrypted and therefore unreadable. Furthermore, self-encrypting drives simplify decommissioning and preserve hardware value for returns and repurposing by:

- Eliminating the need to overwrite or destroy the drive
- Securing warranty returns and expired lease returns
- Enabling drives to be repurposed securely

Auto-locking

Insider theft or misplacement is a growing concern for businesses of all sizes; in addition, managers of branch offices and small businesses without strong physical security face greater vulnerability to external theft. Self-encrypting drives include a feature called auto-lock mode to help secure active data against theft.

Using a self-encrypting drive when auto-lock mode is enabled simply requires securing the drive with an authentication key. When secured in this manner, the drive's data encryption key is locked whenever the drive is powered down. In other words, the moment the self-encrypting drive is switched off or unplugged, it automatically locks down the drive's data.

When the self-encrypting drive is then powered back on, it requires authentication before being able to unlock its encryption key and read any data on the drive, thus protecting against misplacement and theft.

While using self-encrypting drives just for the instant secure erase is an extremely efficient and effective means to help securely retire a drive, using self-encrypting drives in auto-lock mode provides even more advantages. From the moment the drive or system is removed from the data center (with or without authorization), the drive is locked. No advance thought or action is required from the data center administrator to protect the data. This helps prevent a breach should the drive be mishandled and helps secure the data against the threat of insider or outside theft.

Lower acquisition costs through standardization

These self-encrypting drives adhere to the Trusted Computing Group Enterprise Security Subsystem Class (TCG Enterprise SSC) specification, and this standardization promises lower acquisition cost. The world’s top six hard drive vendors collaborated to develop the final enterprise specification published by the Trusted Computing Group (TCG). This specification, created to be the standard for developing and managing self-encrypting drives, enables SEDs from different vendors to be interoperable. Such interoperability helps ensure greater market competition and lower prices for solution builders and end users alike. Historically, the hard drive industry has repeatedly shown that industry-wide standards increase volume, which in turn lowers costs. These economies of scale help ensure incremental logic in the ASICs remains a small portion of drive material costs.

Performance and power consumption

The hardware encryption engine on the drives matches the SAS port’s maximum speed and encrypts all data with no performance degradation. This performance scales linearly and automatically, with each drive added to the system. No CPU cycles from the host are necessary and I/Os occur without interruption.

The 146GB 15K 2.5" SED drive has the following performance and energy saving features:

- 115% improvement in system-level performance over 3.5-inch 15K drives
- Second-generation 2.5-inch 15K enterprise drive with field-proven reliability
- Seagate PowerTrim technology dynamically reduces power up to 70% over comparable 3.5-inch 15K drives
- IOPS/Watt are 2.5 times better than comparable 3.5-inch Tier 1 drives
- 70% smaller size than 3.5-inch drives reduces overall system cooling costs
- Supports 6 Gbps transfer rates and SAS 2.0 feature set, providing the next generation of signal and data integrity features

The 300GB 10K 2.5" SED drive has the following performance and energy saving features:

- 60% improvement in system-level performance over 3.5-inch 15K drives
- Third-generation 2.5-inch 10K-RPM enterprise drive with proven reliability
- Seagate PowerTrim technology dynamically reduces power
- 75% power savings over comparable 3.5-inch 300 GB capacity drives
- 70% smaller size over 3.5-inch drives reduces overall system cooling costs
- 40% reduction in $/IOPS over comparable 3.5-inch drives
- Supports 6 Gbps transfer rates and SAS 2.0 feature set, providing the next generation of signal and data integrity features

Specifications

Technical specifications for the drives are presented in Table 2.

Table 2. Specifications

Specification	146GB 15K 2.5" SED drive	300GB 10K 2.5" SED drive
Part number	44W2294	44W2264
Interface	6 Gbps SAS 2.0	6 Gbps SAS 2.0
Hot-swap drive	Yes	Yes
Form factor	2.5-inch SFF	2.5-inch SFF
Cache	16 MB	16 MB
Capacity	146 GB	300 GB
Encryption	Drive level AES 128-bit	Drive level AES 128-bit
Areal density (average)	237.1 Gbits/inch^2	252 Gbits/inch^2
Guaranteed sectors	286,749,488	585,937,500
Spindle speed	15,000 rpm	10,000 rpm
Average latency	2.0 msec	3.0 msec
Random read seek time	3.2 msec	4.2 msec
Random write seek time	3.5 msec	4.6 msec
MTBF	1,600,000 hours	1,600,000 hours
Annualized failure rate (AFR)	0.55%	0.55%
Current at +12V (max / typical)	1.12 Amps / 0.35 Amps	2.05 Amps / 0.40 Amps
Current at +5V (max / typical)	0.45 Amps / 0.39 Amps	0.72 Amps / 0.43 Amps
Power Idle	4.1 W	3.5 W

Physical specifications

The drives have the following physical specifications:

- Height: 15 mm (0.59 inches)
- Width: 70 mm (2.76 inches)
- Length: 100 mm (3.96 inches)
- Weight (typical): 227 grams (0.50 pounds)

Operating environment

The drives are supported in the following environment:

- Temperature Operating: 5 to 55°C
- Temperature Nonoperating: –40 to 70°C
- Shock, Operating - 2 ms: 60 Gs
- Shock, Nonoperating - 2 ms: 300 Gs
- Acoustics Idle (sound power): 146GB 10K drive: 3.3 bels; 300GB 15K drive: 3.1 bels
- Vibration, Operating: <400 Hz: 0.5 Gs
- Vibration, Nonoperating: <500 Hz: 2.4 Gs

Warranty

One-year, customer replaceable unit (CRU), limited warranty.

Supported RAID controllers

The self-encrypting drives require a supported RAID controller as listed in Table 3.

Table 3. Support RAID controllers

RAID controller	Part number	Support SEDs
ServeRAID M5015 SAS/SATA Controller	46M0829	Yes*
ServeRAID M5014 SAS/SATA Controller	46M0916	Yes*
ServeRAID M1015 SAS/SATA Controller	46M0831	Yes†
ServeRAID-MR10k SAS/SATA Controller	43W4280	No
ServeRAID-MR10i SAS/SATA Controller	43W4296	No
ServeRAID-MR10M SAS/SATA Controller	44E8825	No
ServeRAID-BR10i SAS/SATA Controller	44E8689	No
IBM 6Gb SSD Host Bus Adapter	7838-AC1 fc 3876	No
IBM 3Gb SAS HBA Controller v2	44E8700	No
IBM 6Gb SAS HBA	46M0907	No

* For SED support, the ServeRAID M5015 and M5014 require the ServeRAID M5000 Series Advanced Feature Key, part 46M0930.
† For SED support, the ServeRAID M1015 requires the ServeRAID M1000 Series Advanced Feature Key, part 46M0832.

The ServeRAID M5014 and M5015 controllers offer internal RAID 0, 1, 5, 10, and 50; the optional M5000 Series Advanced Feature Key (part number 46M0930, feature 5106) upgrade would be required for SED support as well as offering additional RAID 6 and 60 functionality.

The ServeRAID M1015 controller provides internal RAID 0, 1, and 10; the optional ServeRAID M1000 (part number 46M0832, feature 9749) Series Advanced Feature Key upgrade would be required for SED support and also provides additional RAID 5 and 50 capabilities.

Figure 2 shows the ServeRAID M5000 Series Advanced Feature Key attached to the ServeRAID M5015 controller.

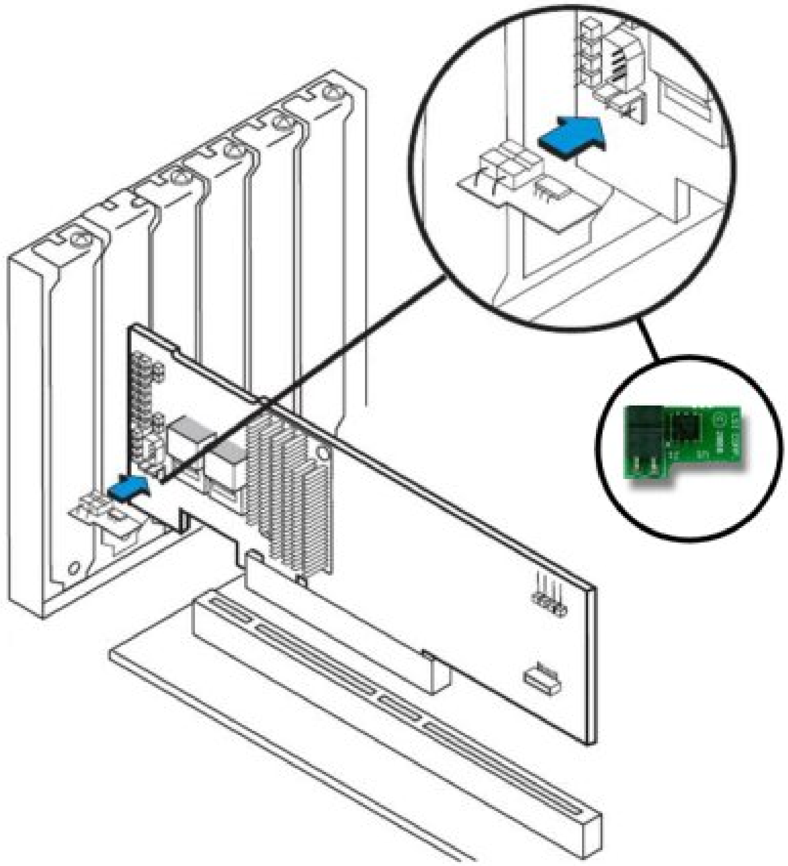

Figure 2. ServeRAID M5000 Series Advanced Feature Key

Supported servers

The self-encrypting drives and supported RAID controllers can be installed in the System x servers identified in Table 4.

Table 4. Supported servers

	x3200 M2	x3200 M3	x3250 M2	x3250 M3	x3350	x3400	x3400 M2	x3455	x3500	x3500 M2	x3550	x3550 M2	x3650	x3650 T	x3650 M2	x3655	x3755	x3850 M2	x3950 M2
ServeRAID M5015	N	Y	N	Y	N	N	Y	N	N	Y	N	Y	N	N	Y	N	N	N	N
ServeRAID M5014	N	N	N	N	N	N	Y	N	N	Y	N	Y	N	N	Y	N	N	N	N
ServeRAID M1015	N	Y	N	Y	N	N	Y	N	N	Y	N	Y	N	N	Y	N	N	N	N

See the IBM ServerProven Web site for the latest information about the adapters supported by each System x server type: http://ibm.com/servers/eserver/serverproven/compat/us/.

Supported operating systems

The self-encrypting drives operate transparently to end users, storage systems, applications, databases, and the operating systems. The SafeStore feature in the ServeRAID controllers uses simple and intuitive configuration menus that are imbedded in the Storage Manager volume management interface.

The self-encrypting drives and supported RAID controllers support the following operating systems:

- Microsoft Windows Server 2003, Web Edition
- Microsoft Windows Server 2003/2003 R2, Datacenter Edition
- Microsoft Windows Server 2003/2003 R2, Datacenter x64 Edition
- Microsoft Windows Server 2003/2003 R2, Enterprise Edition
- Microsoft Windows Server 2003/2003 R2, Enterprise x64 Edition
- Microsoft Windows Server 2003/2003 R2, Standard Edition
- Microsoft Windows Server 2003/2003 R2, Standard x64 Edition
- Microsoft Windows Server 2008/2008 R2, Datacenter x64 Edition
- Microsoft Windows Server 2008/2008 R2, Datacenter x86 Edition
- Microsoft Windows Server 2008/2008 R2, Enterprise x64 Edition
- Microsoft Windows Server 2008/2008 R2, Enterprise x86 Edition
- Microsoft Windows Server 2008/2008 R2, Standard x64 Edition
- Microsoft Windows Server 2008/2008 R2, Standard x86 Edition
- Microsoft Windows Server 2008/2008 R2, Web x64 Edition
- Microsoft Windows Server 2008/2008 R2, Web x86 Edition
- Microsoft Windows Small Business Server 2003/2003 R2 Premium Edition
- Microsoft Windows Small Business Server 2003/2003 R2 Standard Edition
- Microsoft Windows Storage Server 2003/2003 R2, Enterprise Edition x64
- Microsoft Windows Storage Server 2003/2003 R2, Standard Edition
- Microsoft Windows Storage Server 2003/2003 R2, Standard Edition x64
- Microsoft Windows Storage Server 2003/2003 R2, Workgroup Edition x64
- Red Hat Enterprise Linux 4 AS for AMD64/EM64T
- Red Hat Enterprise Linux 4 AS for x86
- Red Hat Enterprise Linux 5 Server Edition
- Red Hat Enterprise Linux 5 Server Edition with Xen
- Red Hat Enterprise Linux 5 Server with Xen x64 Edition
- Red Hat Enterprise Linux 5 Server x64 Edition
- SUSE LINUX Enterprise Server 10 for AMD64/EM64T
- SUSE LINUX Enterprise Server 10 for x86
- SUSE LINUX Enterprise Server 10 with Xen for AMD64/EM64T
- SUSE LINUX Enterprise Server 10 with Xen for x86
- SUSE LINUX Enterprise Server 11 for AMD64/EM64T
- SUSE LINUX Enterprise Server 11 for x86
- SUSE LINUX Enterprise Server 11 with Xen for AMD64/EM64T

See the IBM ServerProven Web site for the latest information about the specific versions and service packs supported: http://ibm.com/servers/eserver/serverproven/compat/us/. Click **System x servers**, then **Disk controllers** to see the support matrix. Click the check mark that is associated with the System x server in question to see the details of the operating system support.

Related publications

For more information refer to the following documents:

- IBM US Announcement Letter:
  http://ibm.com/common/ssi/cgi-bin/ssialias?infotype=dd&subtype=ca&&htmlfid=897/ENUS109-590
- Lenovo Press product guide for ServeRAID M5015 and M5014 SAS/SATA Controllers
  http://lenovopress.com/tips0738
- Lenovo Press product guide for ServeRAID M1015 SAS/SATA Controller
  http://lenovopress.com/tips0740
- ServeRAID M5015 and M5014 SAS/SATA Controllers User's Guide
  http://ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5082936
- ServeRAID software matrix:
  http://ibm.com/support/entry/portal/docdisplay?lndocid=SERV-RAID

Related product families

Product families related to this document are the following:

- Drives

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service. Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION ”AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary. Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk. Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

© Copyright Lenovo 2024. All rights reserved.

This document, TIPS0761, was created or updated on February 18, 2010.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  https://lenovopress.lenovo.com/TIPS0761
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at https://lenovopress.lenovo.com/TIPS0761.

Trademarks

Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. A current list of Lenovo trademarks is available on the Web at https://www.lenovo.com/us/en/legal/copytrade/.

The following terms are trademarks of Lenovo in the United States, other countries, or both:
Lenovo®
ServeRAID
ServerProven®
System x®

The following terms are trademarks of other companies:

Linux® is the trademark of Linus Torvalds in the U.S. and other countries.

Microsoft®, Windows Server®, and Windows® are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.