Lenovo 12Gb SAS SSC+ Enterprise Performance FIPS SED SSDs

Product Guide (withdrawn product)

The 12 Gb SAS SSC+ Enterprise Performance FIPS SED solid-state drives (SSDs) are high-performance self-encrypting drives (SEDs) that adhere to the Federal Information Processing Standard 140-2 (FIPS 140-2) cryptographic standard. These drives are available in either 2.5-inch or 3.5-inch drive form factor for System x servers.

Self-encrypting drives 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, SED drives in Lenovo servers deliver 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.

The 12 Gb SAS Enterprise Performance FIPS SED SSD is shown in the following figure.

Figure 1. 12 Gb SAS Enterprise Performance FIPS SED SSD (hot-swap tray removed)

Did you know?

The 12 Gb SAS drives with 10 full drives writes per day (DWPD) are an excellent choice for applications demanding high write performance, such as High Performance Computing (HPC), High Definition Imaging and Video (HDIV), high data rate analytics and databases, large-scale virtualization, and video on demand content delivery.

Part number information

The following table lists the information for ordering part numbers and feature codes for System x servers.

Withdrawn: All drives listed in this product guide are withdrawn from marketing.

Table 1. Part number information - System x

Part number	Feature	Description
2.5-inch hot-swap drives		
01GR600	AUCC	HGST SSC+ 400GB 12Gb SAS FIPS SED 2.5" Enterprise G3HS SSD
01GR605	AUCD	HGST SSC+ 800GB 12Gb SAS FIPS SED 2.5" Enterprise G3HS SSD
01GR610	AUCE	HGST SSC+ 1.6TB 12Gb SAS FIPS SED 2.5" Enterprise G3HS SSD
3.5-inch hot-swap drives		
01GR615	AUCJ	HGST SSC+ 400GB 12Gb SAS FIPS SED 3.5" Enterprise HS SSD
01GR620	AUCK	HGST SSC+ 800GB 12Gb SAS FIPS SED 3.5" Enterprise HS SSD
01GR625	AUCL	HGST SSC+ 1.6TB 12Gb SAS FIPS SED 3.5" Enterprise HS SSD

The part numbers include the following items:

- One 2.5-inch SSD with either a 2.5-inch or 3.5-inch a hot-swap tray attached
- Support Flyer for SSDs
- Warranty flyer and Important Notices document

The benefits of drive encryption

Self-encrypting drives (SEDs) such as the 12 Gb SAS Enterprise Performance FIPS SED SSDs 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. 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 bank account 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.

Features

The 12 Gb SAS Enterprise Performance FIPS SED SSDs have the following features:

- Industry-standard 2.5-inch drive with 2.5-inch or 3.5-inch drive tray attached
- Compliant with the FIPS 140-2 Level 2 standard for cryptography modules
- Supports the SafeStore self-encyrpting drive (SED) functionality of ServeRAID adapters
- Based on proven HGST Ultrastar SSD1600MM drive technology
- Uses 20 nm Multi-Level Cell (MLC) NAND flash memory
- Endurance of 10 drive writes per day (DWPD) for 5 years. This equates to a total bytes written (TBW) value of:
    - 200 GB drive: 3.65 PB
    - 400 GB drive: 7.3 PB
    - 800 GB drive: 14.6 PB
    - 1.6 TB drive: 29.2 PB
- SAS MLC solid-state drive with high read performance and consistently low latencies to fulfill client needs in the enterprise space
- High reliability and enhanced ruggedness
- Energy saving, with 9 W typical power consumption per drive
- Absence of moving parts to reduce potential failure points in the server
- S.M.A.R.T. support
- Advanced Encrypting Standard (AES) 256-bit encryption
- Supports Sanitize Cryptographic Erase

- Full end-to-end data path protection:
    - T10 Data Integrity Field (DIF) standard
    - Extended error correction code (ECC)
    - Exclusive-OR (XOR) parity to protect against Flash die failure
    - Parity-checked internal data paths without an external write cache
    - Power loss data management without the need for a supercapacitor

The key difference between Enterprise Performance SSDs such as the 12Gb SAS SSDs described here and Enterprise Entry and Enterprise Mainstream SSDs, is their endurance (life expectancy). SSDs have a huge, but finite, number of program/erase (P/E) cycles, which determines how long the drives can perform write operations and thus their life expectancy. Enterprise Performance SSDs have better endurance than the Enterprise Mainstream and Enterprise Entry SSDs, but at a higher cost/IOPS ratio.

SSD write endurance is typically measured by the number of program/erase cycles that the drive can incur over its lifetime, which is listed as TBW in the device specification. The TBW value that is assigned to a solid-state device is the total bytes of written data that a drive can be guaranteed to complete. Reaching this limit does not cause the drive to immediately fail; the TBW simply denotes the maximum number of writes that can be guaranteed.

A solid-state device does not fail upon reaching the specified TBW, but at some point after surpassing the TBW value (and based on manufacturing variance margins), the drive reaches the end-of-life point, at which time the drive goes into read-only mode. Because of such behavior, careful planning must be done to use SSDs in the application environments to ensure that the TBW of the drive is not exceeded before the required life expectancy.

For example, the 800 GB drive has an endurance of 14,600 TB (14.6 PB) of total bytes written (TBW). This means that for full operation over five years, write workload can be up to 8 TB of writes per day, which is equivalent to 10.0 full drive writes per day (DWPD). For the device to last three years, the drive write workload must be limited to no more than 13.3 TB of writes per day, which is equivalent to 16.7 full drive writes per day.

Technical specifications

The following table presents technical specifications for the 12 Gb SAS Enterprise Performance FIPS SED SSDs.

Table 2. Technical specifications

Feature	**400 GB drive**	**800 GB drive**	**1.6 TB drive**
Part number - 2.5" G3HS	01GR600	01GR605	01GR610
Part number - 3.5" HS	01GR615	01GR620	01GR625
Interface	12 Gbps SAS	12 Gbps SAS	12 Gbps SAS
Capacity	400 GB	800 GB	1.6 TB
Endurance (drive writes per day over 5 years)	10 DWPD	10 DWPD	10 DWPD
Endurance (total bytes written)	7.3 PB	14.6 PB	29.2 PB
Data reliability	1 in 10^{17} bits read	1 in 10^{17} bits read	1 in 10^{17} bits read
MTBF	2,500,000 hours	2,500,000 hours	2,500,000 hours
IOPS reads (4 KB blocks)	130,000	130,000	130,000
IOPS writes (4 KB blocks)	100,000	100,000	100,000
Sequential read rate (64 KB blocks)	1100 MBps	1100 MBps	1100 MBps
Sequential write rate (64 KB blocks)	765 MBps	765 MBps	765 MBps
Read latency (seq)	100 µs	100 µs	100 µs
Write latency (seq)	45 µs	45 µs	45 µs
Shock, operating	1,000 G (Max) at 0.5 ms	1,000 G (Max) at 0.5 ms	1,000 G (Max) at 0.5 ms
Vibration, operating	2.16 G_{RMS} (5-700 Hz)	2.16 G_{RMS} (5-700 Hz)	2.16 G_{RMS} (5-700 Hz)
Typical power	8.47 W	8.47 W	8.47 W

Server support

The following tables list the Lenovo servers that are compatible.

Support for System x and dense servers with Xeon E5/E7 v4 and E3 v5 processors

Table 3. Support for System x and dense servers with Xeon E5/E7 v4 and E3 v5 processors

Part number	Description	x3250 M6 (3943)	x3250 M6 (3633)	x3550 M5 (8869)	x3650 M5 (8871)	x3850 X6/x3950 X6 (6241, E7 v4)	nx360 M5 (5465, E5-2600 v4)	sd350 (5493)
01GR600	HGST SSC+ 400GB 12Gb SAS FIPS SED 2.5" Enterprise G3HS SSD	N	N	Y	Y	N	N	N
01GR605	HGST SSC+ 800GB 12Gb SAS FIPS SED 2.5" Enterprise G3HS SSD	N	N	Y	Y	N	N	N
01GR610	HGST SSC+ 1.6TB 12Gb SAS FIPS SED 2.5" Enterprise G3HS SSD	N	N	Y	Y	N	N	N
01GR615	HGST SSC+ 400GB 12Gb SAS FIPS SED 3.5" Enterprise HS SSD	N	N	N	N	N	N	N
01GR620	HGST SSC+ 800GB 12Gb SAS FIPS SED 3.5" Enterprise HS SSD	N	N	N	N	N	N	N
01GR625	HGST SSC+ 1.6TB 12Gb SAS FIPS SED 3.5" Enterprise HS SSD	N	N	N	N	N	N	N

Support for System x and dense servers with Intel Xeon v3 processors

Table 4. Support for servers with Intel Xeon v3 processors

Part number	Description	x3100 M5 (5457)	x3250 M5 (5458)	x3500 M5 (5464)	x3550 M5 (5463)	x3650 M5 (5462)	x3850 X6/x3950 X6 (6241, E7 v3)	nx360 M5 (5465)
01GR600	HGST SSC+ 400GB 12Gb SAS FIPS SED 2.5" Enterprise G3HS SSD	N	N	N	N	N	N	N
01GR605	HGST SSC+ 800GB 12Gb SAS FIPS SED 2.5" Enterprise G3HS SSD	N	N	N	N	N	N	N
01GR610	HGST SSC+ 1.6TB 12Gb SAS FIPS SED 2.5" Enterprise G3HS SSD	N	N	N	N	N	N	N
01GR615	HGST SSC+ 400GB 12Gb SAS FIPS SED 3.5" Enterprise HS SSD	N	N	N	N	N	N	N
01GR620	HGST SSC+ 800GB 12Gb SAS FIPS SED 3.5" Enterprise HS SSD	N	N	N	N	N	N	N
01GR625	HGST SSC+ 1.6TB 12Gb SAS FIPS SED 3.5" Enterprise HS SSD	N	N	N	N	N	N	N

Support for Flex System compute nodes

Table 5. Support for Flex System servers

Part number	Description	x240 (8737, E5-2600 v2)	x240 (7162)	x240 M5 (9532)	x440 (7167)	x880/x480/x280 X6 (7903)	x280/x480/x880 X6 (7196)	Storage Expansion Node
01GR600	HGST SSC+ 400GB 12Gb SAS FIPS SED 2.5" Enterprise G3HS SSD	N	N	N	N	N	N	N
01GR605	HGST SSC+ 800GB 12Gb SAS FIPS SED 2.5" Enterprise G3HS SSD	N	N	N	N	N	N	N
01GR610	HGST SSC+ 1.6TB 12Gb SAS FIPS SED 2.5" Enterprise G3HS SSD	N	N	N	N	N	N	N
01GR615	HGST SSC+ 400GB 12Gb SAS FIPS SED 3.5" Enterprise HS SSD	N	N	N	N	N	N	N
01GR620	HGST SSC+ 800GB 12Gb SAS FIPS SED 3.5" Enterprise HS SSD	N	N	N	N	N	N	N
01GR625	HGST SSC+ 1.6TB 12Gb SAS FIPS SED 3.5" Enterprise HS SSD	N	N	N	N	N	N	N

Storage controller support

The 12 Gb SAS Enterprise Performance FIPS SED SSDs require a supported SAS controller, either a SAS HBA or a RAID controller with SED support. The following table lists the controllers and the servers that support those controllers.

SED support of the ServeRAID adapters is with the addition of the MegaRAID SafeStore FoD upgrade. SED support of the SAS HBAs is by using software on the server (SED commands are passed through the HBA to the drives).

Table 6. Controllers for supported servers

Part number	Description	SED Services	x3550 M5 (8869)	x3650 M5 (8871)	sd350 (5493)
46C9114	ServeRAID M1215 Controller	MegaRAID SafeStore*	Y	Y	N
46C9110	ServeRAID M5210 Controller	MegaRAID SafeStore*	Y	Y	N
00YD430	H701-L 6Gb HBA Mezz Card	Host software pass-thru	N	N	Y
47C8675	N2215 SAS/SATA HBA	Host software pass-thru	Y	Y	N

* ServeRAID RAID controllers require the MegaRAID SafeStore upgrade for SED support. This is a Features on Demand upgrade. See the relevant product guide for details.

For more information, see these Lenovo Press product guides:

- ServeRAID M5210 product guide
  https://lenovopress.com/tips1069
- ServeRAID M1215 product guide
  https://lenovopress.com/tips1174
- H701-L HBA Mezz Card (see Controllers for internal storage section of sd350 product guide)
  https://lenovopress.com/lp0095#controllers-for-internal-storage
- Lenovo Press product guide for N2215 HBA
  https://lenovopress.com/tips1075

Operating system support

SSDs operate transparently to users, storage systems, applications, databases, and operating systems. The SAS controllers that are supported by the servers listed in the Server support section are also supported by the following operating systems:

- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Red Hat Enterprise Linux 6 Server x64 Edition
- Red Hat Enterprise Linux 7
- SUSE LINUX Enterprise Server 11 for AMD64/EM64T
- SUSE LINUX Enterprise Server 11 with Xen for AMD64/EM64T
- VMware vSphere 5.5 (ESXi)
- VMware vSphere 6.0 (ESXi)

For the latest information about the specific supported operating system versions and service packs, see ServerProven:
http://www.lenovo.com/us/en/serverproven/xseries/controllers/matrix.shtml

Select the check mark box that is associated with the controller and server combination in question to see the details about operating system support.

Warranty

The 12 Gb SAS Enterprise Performance FIPS SED SSDs carry a one-year, customer-replaceable unit (CRU) limited warranty. When the SSDs are installed in a supported server, these drives assume the system's base warranty and any warranty upgrades.

Solid State Memory cells have an intrinsic, finite number of program/erase cycles that each cell can incur. As a result, each solid state device has a maximum amount of program/erase cycles to which it can be subjected. The warranty for Lenovo solid state drives (SSDs) is limited to drives that have not reached the maximum guaranteed number of program/erase cycles, as documented in the Official Published Specifications for the SSD product. A drive that reaches this limit may fail to operate according to its Specifications.

Physical specifications

The 12 Gb SAS Enterprise Performance FIPS SED SSDs have the following physical specifications.

Dimensions and weight (approximate, without drive tray):

- Height: 15 mm (0.6 in.)
- Width: 70 mm (2.8 in.)
- Depth: 100 mm (4.0 in.)
- Weight: 187 g (6.6 oz lb)

Shipping dimensions and weight - 2.5-inch drives (approximate):

- Height: 63 mm (2.5 in.)
- Width: 174 mm (6.9 in.)
- Depth: 133 mm (5.2 in.)

Shipping dimensions and weight- 3.5-inch drives (approximate):

- Height: 95 mm (3.7 in.)
- Width: 257 mm (10.1 in.)
- Depth: 193 mm (7.6 in.)

Operating environment

The 12 Gb SAS Enterprise Performance FIPS SED SSDs are supported in the following environment:

- Temperature, operational: 0 to 70° C (32 to 158° F)
- Temperature, storage: -40 to 85° C (-40 to 185° F)
- Relative humidity: 5 to 90% (noncondensing)
- Maximum altitude: 3,050 m (10,000 ft)

Agency approvals

The 12 Gb SAS Enterprise Performance FIPS SED SSDs conform to the following encyrption standards:

- Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2)
- Trusted Computing Group (TCG) SSC: Enterprise Specification

The following documents provide further information:

- National Institute of Standards and Technology (NIST) summary for FIPS 140-2 certification of the 12 Gb SAS FIPS SED SSD offerings:
  http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2016.htm#2716
- FIPS 140-2 Security Policy for the 12 Gb SAS FIPS SED SSD offerings:
  http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2716.pdf

The 12 Gb SAS Enterprise Performance FIPS SED SSDs also conform to the following regulations:

- FCC Title 47, Part 15B, Class B
- CA/CSA-CEI/IEC CISPR 22:02
- EN 55024: 1998
- EN 55022: 2006
- EN-60950-1 2nd Edition
- UL/CSA EN-60950-1 2nd Edition
- Low Voltage Directive 2006/95/EC
- C-Tick: AS/NZS3584
- VCCI V-3/2013-04 Class B
- CNS 13438: 2006
- KCC Article 11.1
- RoHS DIRECTIVE 2011/65/EU
- REACH 1907/2006
- WEEE Directive 2002/96/EC

Related publications and links

For more information, see the following documents:

- Lenovo System x storage options product page
  https://www3.lenovo.com/us/en/data-center/servers/server-options/system-x-options/server-storage/c/system-x-storage
- HGST Ultrastar SSD1600MM SAS SSD product page
  https://www.hgst.com/products/solid-state-solutions/ultrastar-ssd1600mm
- ServerProven for SSDs
  http://www.lenovo.com/us/en/serverproven/xseries/storage/hssdmatrix.shtml
- Lenovo Press book, *Centrally Managing Access to Self-Encrypting Drives in Lenovo System x Servers*
  https://lenovopress.com/sg248247

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.

This document, LP0614, was created or updated on August 21, 2018.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  https://lenovopress.lenovo.com/LP0614
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at https://lenovopress.lenovo.com/LP0614.

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®
Flex System
ServeRAID
ServerProven®
System x®

The following terms are trademarks of other companies:

Intel® and Xeon® are trademarks of Intel Corporation or its subsidiaries.

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.