ThinkSystem 7600 MAX Mixed Use NVMe PCIe 4.0 x4 SSDs

Product Guide

The ThinkSystem 7600 MAX Mixed Use NVMe SSDs are advanced data center SSDs optimized for mixed read-write performance, endurance, and strong data protection for Lenovo servers. With a PCIe 5.0 x4 interface, they are designed for greater performance and endurance in a cost-effective design, and to support a broader set of workloads. Now with SED encryption as standard, these drives help ensure data security, even when the drive is removed from the server.

Figure 1. ThinkSystem 7600 MAX Mixed Use NVMe SSDs

Did you know?

Lenovo Mixed Used SSDs like the 7600 MAX SSDs are suitable for mixed read-write and general-purpose data center workloads, however their NVMe PCIe interface means the drives also offer high performance. Overall, these SSDs provide outstanding IOPS/watt and cost/IOPS for enterprise solutions.

Self-encrypting drives (SEDs) provide benefits by encrypting data on-the-fly at the drive level with no performance impact, by providing instant secure erasure thereby making the data no longer readable, and by enabling auto-locking to secure active data if a drive is misplaced or stolen from a system while in use. These features are essential for many businesses, especially those storing customer data.

Part number information

The following table lists the part numbers and feature codes for the 7600 MAX SSDs.

Table 1. Part number information

Part number	Feature	Description	Supplier model
4XB7B15546	CGSM	ThinkSystem 2.5" U.2 7600 MAX 1.6TB Mixed Use NVMe PCIe 5.0 x4 HS SSD	MTFDLAL1T6THS-1BP1DFCYY
4XB7B15547	CGSL	ThinkSystem 2.5" U.2 7600 MAX 3.2TB Mixed Use NVMe PCIe 5.0 x4 HS SSD	MTFDLAL3T2THS-1BP1DFCYY
4XB7B15548	CGSK	ThinkSystem 2.5" U.2 7600 MAX 6.4TB Mixed Use NVMe PCIe 5.0 x4 HS SSD	MTFDLAL6T4THS-1BP1DFCYY
4XB7B15549	CGSJ	ThinkSystem 2.5" U.2 7600 MAX 12.8TB Mixed Use NVMe PCIe 5.0 x4 HS SSD	MTFDLAL12T8THS-1BP1DFCYY

The part numbers include the following items:

- One solid-state drive
- Hot swap drives include a hot-swap tray
- Documentation flyer

Features

Non-Volatile Memory Express (NVMe) is PCIe high performance SSD technology that provides high I/O throughput and low latency. NVMe interfaces remove SAS/SATA bottlenecks and unleash all of the capabilities of contemporary NAND flash memory. Each NVMe PCI SSD has direct PCIe x4 connection, which provides at least 2x more bandwidth and 2x less latency than SATA/SAS-based SSD solutions. NVMe drives are also optimized for heavy multi-threaded workloads by using internal parallelism and many other improvements, such as enlarged I/O queues.

The ThinkSystem 7600 MAX Mixed Use NVMe SSDs have the following features:

- NVMe SSD with PCIe 5.0 performance and a U.2 interface
- Based on the Micron 7600 MAX family of SSDs
- Compliant with FIPS 140-3 L2 encryption standard
- Micron 232-layer 3D TLC NAND
- Direct PCIe 5.0 x4 connection for each NVMe drive, resulting in up to 14 GBps overall throughput, compared to 7.5 GBps for a PCIe 4.0 connection.
- Advanced ECC Engine and End-to-End Data Protection
- Protect data integrity from unexpected power loss with advanced power-loss protection architecture
- Adaptive Thermal Monitoring to monitor the internal temperature of the drive with power adjustment to ensure operation within thermal limits
- Supports Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T).
- Enterprise-level security features:
    - Secure Execution Environment - dedicated security processing hardware with physical isolation

    - Asymmetric Roots of Trust - Enables authenticated revocation of root keys
    - Strong Asymmetric Key Support - Uses standard, NIST-approved algorithms with 208-bit/3072-bit RSA keys
    - RSA Delegation Key Support - Enables customers to maintain ownership of RSA keys
    - Secure Boot - Helps ensure firmware integrity on running platform
    - Key-Based Firmware Update - Validates firmware using public key-based authentication prior to firmware update
    - Key-Based Privileged Access - Protects against unauthorized privileged SSD function execution with public key-based authorization
- Supports the following specifications:
    - PCI Express Base Specification Rev. 5.0
    - NVM Express 2.0d
    - NVM Express Management Interface 1.2d

The key metric for solid state drives 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. Write Intensive SSDs have better endurance than Mixed Use SSDs, which in turn have better endurance than Read Intensive SSDs.

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 7600 MAX 1.6TB drive has an endurance of 8,700 TB of total bytes written (TBW). This means that for full operation over five years, write workload must be limited to no more than 4,800 GB of writes per day, which is equivalent to 3.00 full drive writes per day (DWPD). For the device to last three years, the drive write workload must be limited to no more than 8,000 GB of writes per day, which is equivalent to 5.0 full drive writes per day.

The benefits of drive encryption

All ThinkSystem 7600 MAX Mixed Use NVMe SSDs support drive encryption.

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. 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-encrypting 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.

Technical specifications

Table 2. Technical specifications

Feature	1.6 TB drive	3.2 TB drive	6.4 TB drive	12.8 TB drive
Interface	PCIe 5.0 x4	PCIe 5.0 x4	PCIe 5.0 x4	PCIe 5.0 x4
Capacity	1.6 TB	3.2 TB	6.4 TB	12.8 TB
SED encryption	FIPS 140-3 L2	FIPS 140-3 L2	FIPS 140-3 L2	FIPS 140-3 L2
Endurance (drive writes per day for 5 years)	3.0 DWPD	3.0 DWPD	3.0 DWPD	3.0 DWPD
Endurance (total bytes written)	8700 TB	17,500 TB	35,000 TB	70,000 TB
Data reliability (UBER)	< 1 in 10^{17} bits read	< 1 in 10^{17} bits read	< 1 in 10^{17} bits read	< 1 in 10^{17} bits read
MTBF	2,000,000 hours	2,000,000 hours	2,000,000 hours	2,000,000 hours
IOPS reads (4 KB blocks)	1,800,000	2,100,000	2,100,000	2,100,000
IOPS writes (4 KB blocks)	300,000	560,000	675,000	675,000
Sequential read rate (128 KB blocks)	12,000 MBps	12,000 MBps	12,000 MBps	12,000 MBps
Sequential write rate (128 KB blocks)	3,300 MBps	6,500 MBps	7,000 MBps	7,000 MBps
Latency (random R/W)	55 µs / 15 µs	55 µs / 15 µs	55 µs / 15 µs	55 µs / 15 µs
Typical power (R/W)	18 / 19 W	18 / 19 W	19 / 20 W	23 / 23 W

Server support

These drives are supported in ThinkAgile servers. See each ThinkAgile server product guide for details.

Storage controller support

NVMe PCIe SSDs require a NVMe drive backplane and some form of PCIe connection to processors. PCIe connections can take the form of either an adapter (PCIe Interposer or PCIe extender) or simply a cable that connects to an onboard NVMe connector.

Consult the relevant server product guide for details about required components for NVMe drive support.

Operating system support

The following tables list the supported operating systems:

Tip: These tables are automatically generated based on data from Lenovo ServerProven.

Table 3. Operating system support for ThinkSystem 2.5" U.2 7600 MAX 3.2TB Mixed Use NVMe PCIe 5.0 x4 HS SSD, 4XB7B15547

Operating systems	SR645 V3	SR635 V3	SR655 V3	SR630 V4	SR650 V4/SR650a V4
Microsoft Windows 10	Y	Y	Y	N	N
Microsoft Windows 11	Y	Y	Y	N	N
Microsoft Windows Server 2022	Y	Y	Y	Y	Y
Microsoft Windows Server 2025	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.6	Y	Y	Y	N	N
Red Hat Enterprise Linux 8.7	Y	Y	Y	N	N
Red Hat Enterprise Linux 8.8	Y	Y	Y	N	N
Red Hat Enterprise Linux 8.9	Y	Y	Y	N	N
Red Hat Enterprise Linux 8.10	Y	Y	Y	N	N
Red Hat Enterprise Linux 9.0	Y	Y	Y	N	N
Red Hat Enterprise Linux 9.1	Y	Y	Y	N	N
Red Hat Enterprise Linux 9.2	Y	Y	Y	N	N
Red Hat Enterprise Linux 9.3	Y	Y	Y	N	N
Red Hat Enterprise Linux 9.4	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 9.5	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 9.6	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 9.7	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 10.0	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 10.1	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP4	Y	Y	Y	N	N
SUSE Linux Enterprise Server 15 SP5	Y	Y	Y	N	N
SUSE Linux Enterprise Server 15 SP6	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP7	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 16	Y	Y	Y	Y	Y
Ubuntu 20.04.5 LTS or later with HWE kernel	Y	Y	Y	N	N
Ubuntu 22.04.5 LTS or later with HWE kernel	Y	Y	Y	Y	Y
Ubuntu 22.04 LTS or later with HWE kernel	Y	Y	Y	N	N
Ubuntu 24.04 LTS or later with HWE kernel	Y	Y	Y	Y	Y

Operating systems	SR645 V3	SR635 V3	SR655 V3	SR630 V4	SR650 V4/SR650a V4
VMware vSphere Hypervisor (ESXi) 7.0 U3	Y	Y	Y	N	N
VMware vSphere Hypervisor (ESXi) 8.0	Y	Y	Y	N	N
VMware vSphere Hypervisor (ESXi) 8.0 U1	Y	Y	Y	N	N
VMware vSphere Hypervisor (ESXi) 8.0 U2	Y	Y	Y	N	N
VMware vSphere Hypervisor (ESXi) 8.0 U3	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 9.0	Y	Y	Y	Y	Y

IBM SKLM Key Management support

To effectively manage a large deployment of SEDs in Lenovo servers, IBM Security Key Lifecycle Manager (SKLM) offers a centralized key management solution.

The IBM Security Key Lifecycle Manager software is available from Lenovo using the ordering information listed in the following table.

Table 5. IBM Security Key Lifecycle Manager licenses

Part number	Description
7S0A007FWW	IBM Security Key Lifecycle Manager Basic Edition Install License + SW Subscription & Support 12 Months
7S0A007HWW	IBM Security Key Lifecycle Manager For Raw Decimal Terabyte Storage Resource Value Unit License + SW Subscription & Support 12 Months
7S0A007KWW	IBM Security Key Lifecycle Manager For Raw Decimal Petabyte Storage Resource Value Unit License + SW Subscription & Support 12 Months
7S0A007MWW	IBM Security Key Lifecycle Manager For Usable Decimal Terabyte Storage Resource Value Unit License + SW Subscription & Support 12 Months
7S0A007PWW	IBM Security Key Lifecycle Manager For Usable Decimal Petabyte Storage Resource Value Unit License + SW Subscription & Support 12 Months

Warranty

The 7600 MAX 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 7600 MAX SSDs have the following physical specifications:

Dimensions and weight (approximate, without the drive tray):

- Height: 15 mm (0.6 in.)
- Width: 70 mm (2.8 in.)
- Depth: 100 mm (4.0 in.)
- Weight: 180 g (2.5 oz)

Operating environment

The 7600 MAX SSDs are supported in the following environment:

- Temperature:
  - Operating: 0 to 70 °C (32 to 158 °F)
  - Storage: -40 to 85 °C (-40 to 185 °F)
- Relative humidity, Non-operating: 5 to 90% (noncondensing)
- Maximum altitude: 3,050 m (10,000 ft)
- Shock, non-operating: 1,500 G (Max) at 0.5 ms
- Vibration, non-operating: 3.3 G_{RMS} (5-800 Hz)

Agency approvals

The 7600 MAX SSDs conform to the following regulations:

- CE (Europe): EN55032, EN55035 Class A, RoHS
- FCC: CFR Title 47, Part 15, Class B
- UL/cUL: approval to UL 62368-1
- BSMI (Taiwan): approval to CNS 15936-2016, CNS 15663-2013
- RCM (Australia, New Zealand): AS/NZS CISPR32 Class A
- KC RRL (Korea): approval to KS C 9832 Class A, KS C 9835 Class A
- W.E.E.E.: Compliance with EU WEEE directive 2012/19/EC.
- TUV (Germany): approval to EN62368
- VCCI (Japan): CISPR 32 Class A
- IC (Canada): ICES-003 Class A
- Morocco: EN55032, EN55035 Class A
- UkrSEPRO (Ukraine): EN55032, EN55035 Class A, EN62368, RoHS (Resolution 2017 No. 139)
- UKCA (UK): SI 2016/1091 Class A and SI 2012/3032 RoHS

Related publications and links

For more information, see the following documents:

- Lenovo ThinkSystem storage options product web page
  https://lenovopress.com/lp0761-storage-options-for-thinksystem-servers
- Micron 7600 product page
  https://www.micron.com/products/storage/ssd/data-center-ssd/7600-ssd

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, LP2447, was created or updated on May 26, 2026.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  https://lenovopress.lenovo.com/LP2447
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at https://lenovopress.lenovo.com/LP2447.

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®
ServerProven®
System x®
ThinkAgile®
ThinkSystem®

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.

IBM® and IBM Security® are trademarks of IBM in the United States, other countries, or both.

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