ThinkSystem U.2 6550 Read Intensive NVMe PCIe 5.0 x4 SSDs

Product Guide

The ThinkSystem 6550 Read Intensive NVMe SSDs are general-purpose yet high-performance drives with a PCIe 5.0 x4 interface. With performance optimizations for real-world IO conditions, the 6550 SSDs accelerate enterprise and cloud workloads such as AI/ML, HPC, databases, and general purpose servers, and deliver up to 90% IOPS consistency for the life of the drive.

SED support: All drives listed in this product guide include SED drive encryption.

Figure 1. ThinkSystem 6550 Read Intensive NVMe SSDs in 2.5-inch form factor (without the ThinkSystem hot-swap tray)

Did You Know?

The 6550 SSDs are part of the new family of PCIe 5.0 SSDs that match the performance of the ThinkSystem V3 and ThinkSystem V4 families of servers. By having a Gen 5 host interface, sequential performance is doubled compared to Gen 4 SSDs. The NVMe host interface also maximizes flash storage performance and minimizes latency.

Lenovo Read Intensive SSDs like the 6550 SSDs are suitable for read-intensive 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.

Part number information

The following table lists the ordering part numbers and feature codes for the 6550 SSDs.

Table 1. Ordering information

Part number	Feature	Description	Supplier part number
4XB7B08330	CBSW	ThinkSystem 2.5" U.2 6550 30.72TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	MTFDLAL30T7THL-1BK4JABYY
4XB7B08331	CBSX	ThinkSystem 2.5" U.2 6550 61.44TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	MTFDLAL61T4THL-1BK4JABYY

The part numbers for the drives include the following items:

- One drive with a hot-swap tray attached
- Publication package

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 significantly greater bandwidth and lower 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 6550 SSDs have the following key characteristics:

- Based on the Micron 6550 ION SSD Series
- PCIe 5.0 connection for each NVMe drive
- Compliant with Trusted Computing Group Opal 2.02 Security Subsystem Class cryptographic standard (TCG Opal 2.02 SSC)
- Micron 3D 232-layer TLC NAND Flash
- Suitable for read-intensive workloads
- Variable sector size and end-to-end data-path protection
- Enhanced power-loss data protection
- Thermal throttling and monitoring
- SMART health reporting
- Supports the following specifications:
    - PCI Express Base Specification Rev. 5.0
    - NVM Express Base Specification 2.0b
    - NVM Express Management Interface 1.2c

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 30.72 TB drive has an endurance of 16,500 TB of total bytes written (TBW). This means that for full operation over five years, write workload must be limited to no more than 9,041 GB of writes per day, which is equivalent to 0.3 full drive writes per day (DWPD). For the device to last three years, the drive write workload must be limited to no more than 15,068 GB of writes per day, which is equivalent to 0.5 full drive writes per day.

The benefits of drive encryption

All ThinkSystem 6550 Read Intensive 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

The following table present technical specifications for the 6550 SSDs.

Table 2. Technical specifications

Feature	**30.72 TB drive**	**61.44 TB drive**
Interface	PCIe 5.0 x4	PCIe 5.0 x4
Capacity	30.72 TB	61.44 TB
SED encryption	TCG Opal	TCG Opal
Endurance (drive writes per day over 5 years)	0.3 DWPD	0.3 DWPD
Endurance (total bytes written)	16.5 PB	33.5 PB
Data reliability	< 1 in 10^{17} bits read	< 1 in 10^{17} bits read
MTBF, hours	2,500,000	2,500,000
Performance & Power - PCIe 5.0 host interface		
IOPS read (4 KB blocks)	2,000,000	2,000,000
IOPS write (4 KB blocks)	70,000	70,000
Sequential read rate	14.0 GBps	14.0 GBps
Sequential write rate	8.0 GBps	8.0 GBps
Read access latency random*	70 µs	70 µs
Write access latency random*	25 µs	25 µs
Average power (Active Read / Active Write)	22 W / 23 W	23 W / 23 W
Environment		
Shock, non-operating	1,500 G (Max) at 0.5 ms	1,500 G (Max) at 0.5 ms
Vibration, non-operating	14.6 G_{RMS} (2-1200 Hz)	14.6 G_{RMS} (2-1200 Hz)

* Latency measured using 4 KB transfer size with queue depth = 1 on a random workload.

Server support

The following tables list the ThinkSystem servers that are compatible.

Table 3. Server support (Part 1 of 5)

Part Number	Description	AMD V3				2S Intel V3/V4						Multi Node V3			1S V3			
		SR635 V3 (7D9H / 7D9G)	SR655 V3 (7D9F / 7D9E)	SR645 V3 (7D9D / 7D9C)	SR665 V3 (7D9B / 7D9A)	ST650 V3 (7D7B / 7D7A)	SR630 V3 (7D72 / 7D73)	SR650 V3 (7D75 / 7D76)	SR630 V4 (7DG8 / 7DG9)	SR650 V4 (7DGC / 7DGD)	SR650a V4 (7DGC / 7DGD)	SD535 V3 (7DD8 / 7DD1)	SD530 V3 (7DDA / 7DD3)	SD550 V3 (7DD9 / 7DD2)	ST45 V3 (7DH4 / 7DH5)	ST50 V3 (7DF4 / 7DF3)	ST250 V3 (7DCF / 7DCE)	SR250 V3 (7DCM / 7DCL)
4XB7B08330	ThinkSystem 2.5" U.2 6550 30.72TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	N	Y	Y	Y	N	Y	Y	N	N	N	N	N	N	N	N	N	N
4XB7B08331	ThinkSystem 2.5" U.2 6550 61.44TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	N	Y	Y	Y	N	Y	Y	N	N	N	N	N	N	N	N	N	N

Table 4. Server support (Part 2 of 5)

Part Number	Description	4S 8S Intel V3/V4					GPU Rich						Edge					
		SR850 V3 (7D97 / 7D96)	SR860 V3 (7D94 / 7D93)	SR950 V3 (7DC5 / 7DC4)	SR850 V4 (7DJT / 7DJS)	SR860 V4 (7DJQ / 7DJN)	SR670 V2 (7Z22 / 7Z23)	SR675 V3 (7D9Q / 7D9R)	SR680a V3 (7DHE)	SR680a V3 B200 (7DM9)	SR685a V3 (7DHC)	SR780a V3 (7DJ5)	SE100 (7DGR)	SE350 (7Z46 / 7D1X)	SE350 V2 (7DA9)	SE360 V2 (7DAM)	SE450 (7D8T)	SE455 V3 (7DBY)
4XB7B08330	ThinkSystem 2.5" U.2 6550 30.72TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
4XB7B08331	ThinkSystem 2.5" U.2 6550 61.44TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N

Table 5. Server support (Part 3 of 5)

Part Number	Description	Super Computing							1S Intel V2			2S Intel V2			AMD V1			
		SC750 V4 (7DDJ)	SC777 V4 (7DKA)	SD665 V3 (7D9P)	SD665-N V3 (7DAZ)	SD650 V3 (7D7M)	SD650-I V3 (7D7L)	SD650-N V3 (7D7N)	ST50 V2 (7D8K / 7D8J)	ST250 V2 (7D8G / 7D8F)	SR250 V2 (7D7R / 7D7Q)	ST650 V2 (7Z75 / 7Z74)	SR630 V2 (7Z70 / 7Z71)	SR650 V2 (7Z72 / 7Z73)	SR635 (7Y98 / 7Y99)	SR655 (7Y00 / 7Z01)	SR645 (7D2Y / 7D2X)	SR665 (7D2W / 7D2V)
4XB7B08330	ThinkSystem 2.5" U.2 6550 30.72TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
4XB7B08331	ThinkSystem 2.5" U.2 6550 61.44TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N

Table 6. Server support (Part 4 of 5)

Part Number	Description	Dense V2				4S V2		8S	4S V1			1S Intel V1			
		SD630 V2 (7D1K)	SD650 V2 (7D1M)	SD650-N V2 (7D1N)	SN550 V2 (7Z69)	SR850 V2 (7D31 / 7D32)	SR860 V2 (7Z59 / 7Z60)	SR950 (7X11 / 7X12)	SR850 (7X18 / 7X19)	SR850P (7D2F / 2D2G)	SR860 (7X69 / 7X70)	ST50 (7Y48 / 7Y50)	ST250 (7Y45 / 7Y46)	SR150 (7Y54)	SR250 (7Y52 / 7Y51)
4XB7B08330	ThinkSystem 2.5" U.2 6550 30.72TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	N	N	N	N	N	N	N	N	N	N	N	N	N	N
4XB7B08331	ThinkSystem 2.5" U.2 6550 61.44TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	N	N	N	N	N	N	N	N	N	N	N	N	N	N

Table 7. Server support (Part 5 of 5)

Part Number	Description	2S Intel V1								Dense V1			
		ST550 (7X09 / 7X10)	SR530 (7X07 / 7X08)	SR550 (7X03 / 7X04)	SR570 (7Y02 / 7Y03)	SR590 (7X98 / 7X99)	SR630 (7X01 / 7X02)	SR650 (7X05 / 7X06)	SR670 (7Y36 / 7Y37)	SD530 (7X21)	SD650 (7X58)	SN550 (7X16)	SN850 (7X15)
4XB7B08330	ThinkSystem 2.5" U.2 6550 30.72TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	N	N	N	N	N	N	N	N	N	N	N	N
4XB7B08331	ThinkSystem 2.5" U.2 6550 61.44TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	N	N	N	N	N	N	N	N	N	N	N	N

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/switch adapter) 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 6550 SSDs support the operating systems listed in the following tables.

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

Table 8. Operating system support for ThinkSystem 2.5" U.2 6550 30.72TB Read Intensive NVMe PCIe 5.0 x4 HS SSD, 4XB7B08330

Operating systems	SR630 V3 (4th Gen Xeon)	SR630 V3 (5th Gen Xeon)	SR645 V3	SR650 V3 (4th Gen Xeon)	SR650 V3 (5th Gen Xeon)	SR655 V3	SR665 V3
Microsoft Windows 10	N	Y	Y	Y	Y	Y	Y
Microsoft Windows 11	Y	Y	Y	Y	Y	Y	Y
Microsoft Windows Server 2019	Y	Y	Y	Y	Y	Y	Y
Microsoft Windows Server 2022	Y	Y	Y	Y	Y	Y	Y
Microsoft Windows Server 2025	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 8.6	Y	N	Y	Y	N	Y	Y
Red Hat Enterprise Linux 8.10	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 9.0	Y	N	Y	Y	N	Y	Y
Red Hat Enterprise Linux 9.1	Y	N	Y	Y	N	Y	Y
Red Hat Enterprise Linux 9.2	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 9.3	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 9.4	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 9.5	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 9.6	Y	Y	Y	Y	Y	Y	Y
Red Hat Enterprise Linux 10.0	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP4	Y	N	Y	Y	N	Y	Y
SUSE Linux Enterprise Server 15 SP5	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP6	Y	Y	Y	Y	Y	Y	Y
SUSE Linux Enterprise Server 15 SP7	Y	Y	Y	Y	Y	Y	Y
Ubuntu 20.04.5 LTS	N	N	Y	N	N	Y	Y
Ubuntu 20.04 LTS	Y	Y	N	Y	Y	N	N
Ubuntu 22.04.3 LTS	N	Y	N	N	Y	N	N
Ubuntu 22.04.5 LTS	N	N	Y	N	N	Y	Y
Ubuntu 22.04 LTS	Y	N	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 8.0	Y	N	Y	Y	N	Y	Y
VMware vSphere Hypervisor (ESXi) 8.0 U1	Y	N	Y	Y	N	Y	Y
VMware vSphere Hypervisor (ESXi) 8.0 U2	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 8.0 U3	Y	Y	Y	Y	Y	Y	Y
VMware vSphere Hypervisor (ESXi) 9.0	Y	Y	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. Certain Lenovo servers support Features on Demand (FoD) license upgrades that enable SKLM support.

The following table lists the part numbers and feature codes to enable SKLM support in the management processor of the server.

Table 9. FoD upgrades for SKLM support

Part number	Feature code	Description
Security Key Lifecycle Manager - FoD (United States, Canada, Asia Pacific, and Japan)		
00D9998	A5U1	SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/1Yr S&S
00D9999	AS6C	SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/3Yr S&S
Security Key Lifecycle Manager - FoD (Latin America, Europe, Middle East, and Africa)		
00FP648	A5U1	SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/1Yr S&S
00FP649	AS6C	SKLM for System x/ThinkSystem w/SEDs - FoD per Install w/3Yr S&S

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

Table 10. 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 6550 SSDs carry a 1-year, customer-replaceable unit (CRU) limited warranty. When installed in a supported Lenovo server, these drives assume the system’s base warranty and any warranty upgrade.

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 6550 SSDs have the following physical dimensions and weight:

- Height: 15 mm
- Width: 70 mm
- Depth: 100 mm
- Weight: 198 g (30.72TB drive), 178 g (61.44TB drive)

Operating environment

The 6550 SSDs are supported in the following environment:

- Temperature
  - Operating: 0 to 70 °C (32 to 158 °F) at 0 to 3,048 m (0 to 10,000 ft)
  - Non-operating: -40 to 85 °C (-40 to 185 °F)
- Relative humidity: 5 to 90% (non-condensing)
- Maximum altitude (operational): 3,048 m (10,000 ft)

Agency approvals

The 6550 SSDs 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
- BSMI: CNS 13438
- KCC Article 11.1
- RoHS DIRECTIVE 2011/65/EU
- WEEE Directive 2002/96/EC

Related publications and links

For more information, see the following documents:

- Lenovo ThinkSystem SSD Portfolio
  https://lenovopress.lenovo.com/lp1261-lenovo-thinksystem-ssd-portfolio
- ServerProven
  https://serverproven.lenovo.com/
- Micron 6550 ION product page
  https://www.micron.com/products/storage/ssd/data-center-ssd/6550-ion

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, LP2285, was created or updated on August 26, 2025.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  https://lenovopress.lenovo.com/LP2285
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at https://lenovopress.lenovo.com/LP2285.

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®
ThinkSystem®

The following terms are trademarks of other companies:

AMD is a trademark of Advanced Micro Devices, Inc.

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.

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.