ThinkSystem SN861 Read Intensive NVMe PCIe 5.0 SSDs

Product Guide

The ThinkSystem SN861 Read Intensive NVMe PCIe 5.0 SSDs, available in capacities up to 15.36TB, are general-purpose yet high-performance NVMe PCIe Gen 5 SSDs. Available in the 2.5-inch form factor, they are engineered for greater performance and endurance in a cost-effective design, and to support a broader set of workloads. These drives have SED encryption as standard to help ensure data security, even when the drive is removed from the server.

Figure 1. ThinkSystem SN861 Read Intensive NVMe PCIe 5.0 SSDs

Did you know?

The SN861 SSDs are part of the new family of PCIe 5.0 SSDs that match the performance of the ThinkSystem V4 family of servers. By having a Gen5 host interface, sequential performance is doubled compared to Gen4 SSDs. The NVMe host interface also maximizes flash storage performance and minimizes latency.

Lenovo Read Intensive SSDs like the SN861 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 part numbers and feature codes for ThinkSystem servers.

Table 1. Ordering information

Part number	Feature	Description	Vendor part number
2.5-inch hot-swap drives			
4XB7B10396	CFD6	ThinkSystem 2.5" U.2 SN861 1.92TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	SDS6BA119OSP9X7
4XB7B10397	CFD5	ThinkSystem 2.5" U.2 SN861 3.84TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	SDS6BA138OSP9X7
4XB7B10398	CFD4	ThinkSystem 2.5" U.2 SN861 7.68TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	SDS6BA176OSP9X7
4XB7B10399	CFD3	ThinkSystem 2.5" U.2 SN861 15.36TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	SDS6BA1A1OSP9X7

The part numbers include the following items:

- One solid-state drive
- Attached hot-swap tray (for hot-swap drives)
- 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 of the SN861 SSDs have direct PCIe 5.0 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 ThinkSystem SN861 Read Intensive NVMe PCIe 5.0 SSDs have the following features:

- Based on the SanDisk DC SN861 drives
- Available as 15mm 2.5-inch drives in a hot-swap tray
- 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.
- Also supports PCIe 4.0 and 3.0 host connection for previous-generation servers
- Based on SanDisk TLC flash memory
- Single-port design, optimized for data center class workloads
- Consistent performance and reliability for demanding 24x7 environments
- Designed for high-density storage deployments
- Power loss protection (PLP) and end-to-end data correction
- Supports Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T)
- SED support for TCG Opal v2.01 SSC

- Supports the following specifications:
  - PCI Express Base Specification, Revision 5.0
  - NVM Express Specification, Revision 2.0
  - NVM Express Management Interface (NVMe MI), Revision 1.2c

Read Intensive SSDs and Write Intensive SSDs have similar read IOPS performance, but the key difference between them is their endurance -- how long they can reliably perform write operations. Read Intensive SSDs have a better cost/IOPS ratio but lower endurance compared to Write Intensive SSDs. SSD write endurance is typically measured by the number of program/erase (P/E) write cycles that the drive incurs over its lifetime, listed as the total bytes of written data (TBW) in the device specification.

The TBW value assigned to a solid-state device is the total bytes of written data (based on the number of P/E cycles) that a drive can be guaranteed to complete (% of remaining P/E cycles = % of remaining TBW). Reaching this limit does not cause the drive to immediately fail. It simply denotes the maximum number of writes that can be guaranteed. A solid-state device will not fail upon reaching the specified TBW. At some point based on manufacturing variance margin, after surpassing the TBW value, the drive will reach the end-of-life point, at which the drive will go into a read-only mode.

Because of such behavior by Read Intensive solid-state drives, careful planning must be done to use them only in read-intensive or mixed up to 70% read/30% write environments to ensure that the TBW of the drive will not be exceeded before the required life expectancy.

For example, the 3.84 TB GB SN861 Read Intensive drive has an endurance of 7,008 TB of total bytes written (TBW). This means that for full operation over five years, write workload must be limited to no more than 3,840 GB of writes per day, which is equivalent to 1.0 full drive writes per day (DWPD). For the device to last three years, the drive write workload must be limited to no more than 6,400 GB of writes per day, which is equivalent to 1.7 full drive writes per day.

The benefits of drive encryption

All ThinkSystem SN861 Read Intensive NVMe PCIe 5.0 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 tables present the technical specifications for the SN861 SSDs. Note that the performance data and power consumption is based on a PCIe 5.0 host interface.

Table 2. Technical specifications

Feature	**1.92 TB drive**	**3.84 TB drive**	**7.68 TB drive**	**15.36 TB drive**
Interface	PCIe 5.0 x4	PCIe 5.0 x4	PCIe 5.0 x4	PCIe 5.0 x4
Capacity	1.92 TB	3.84 TB	7.68 TB	15.36 TB
SED encryption	TCG Opal 2.01	TCG Opal 2.01	TCG Opal 2.01	TCG Opal 2.01
Endurance (drive writes per day for 5 years)	1 DWPD	1 DWPD	1 DWPD	1 DWPD
Endurance (total bytes written)	3504 TB	7008 TB	14,016 TB	28,032 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	2,500,000 hours	2,500,000 hours	2,500,000 hours	2,500,000 hours
Performance & Power - PCIe 5.0 host interface				
IOPS reads (4 KB blocks)	2,135,000	3,346,000	3,346,000	3,311,000
IOPS writes (4 KB blocks)	180,000	359,000	462,000	372,000
Sequential read rate (128 KB blocks)	13,700 MBps	13,700 MBps	13,700 MBps	13,700 MBps
Sequential write rate (128 KB blocks)	3,600 MBps	7,200 MBps	8,900 MBps	8,500 MBps
Latency (random R/W)	65 µs / 8 µs	65 µs / 8 µs	65 µs / 8 µs	65 µs / 8 µs
Power (random R/W)	14.2 W / 12.2 W	19.3 W / 17.5 W	20.8 W / 20.3 W	21.2 W / 19.9 W

Server support

The following tables list the ThinkSystem servers that are compatible.

Table 3. Server support (Part 1 of 5)

		AMD V3				2S Intel V3/V4						Multi Node V3			1S V3			
Part Number	Description	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)
4XB7B10396	ThinkSystem 2.5" U.2 SN861 1.92TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y	N	N	N	N
4XB7B10397	ThinkSystem 2.5" U.2 SN861 3.84TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y	N	N	N	N
4XB7B10398	ThinkSystem 2.5" U.2 SN861 7.68TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y	N	N	N	N
4XB7B10399	ThinkSystem 2.5" U.2 SN861 15.36TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y	N	N	N	N

Table 4. Server support (Part 2 of 5)

		4S 8S Intel V3/V4					GPU Rich							Edge					
Part Number	Description	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)	SR680a V4 (7DMK)	SE100 (7DGR)	SE350 (7Z46 / 7D1X)	SE350 V2 (7DA9)	SE360 V2 (7DAM)	SE450 (7D8T)	SE455 V3 (7DBY)
4XB7B10396	ThinkSystem 2.5" U.2 SN861 1.92TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	Y	Y	N	Y	Y	N	Y	N	N	N	N	N	N	N	N	N	N	N
4XB7B10397	ThinkSystem 2.5" U.2 SN861 3.84TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	Y	Y	N	Y	Y	N	Y	N	N	N	N	N	N	N	N	N	N	N
4XB7B10398	ThinkSystem 2.5" U.2 SN861 7.68TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	Y	Y	N	Y	Y	N	Y	N	N	N	N	N	N	N	N	N	N	N
4XB7B10399	ThinkSystem 2.5" U.2 SN861 15.36TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	Y	Y	N	Y	Y	N	Y	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)
4XB7B10396	ThinkSystem 2.5" U.2 SN861 1.92TB 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
4XB7B10397	ThinkSystem 2.5" U.2 SN861 3.84TB 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
4XB7B10398	ThinkSystem 2.5" U.2 SN861 7.68TB 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
4XB7B10399	ThinkSystem 2.5" U.2 SN861 15.36TB 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)
4XB7B10396	ThinkSystem 2.5" U.2 SN861 1.92TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	N	N	N	N	N	N	N	N	N	N	N	N	N	N
4XB7B10397	ThinkSystem 2.5" U.2 SN861 3.84TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	N	N	N	N	N	N	N	N	N	N	N	N	N	N
4XB7B10398	ThinkSystem 2.5" U.2 SN861 7.68TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	N	N	N	N	N	N	N	N	N	N	N	N	N	N
4XB7B10399	ThinkSystem 2.5" U.2 SN861 15.36TB 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)
4XB7B10396	ThinkSystem 2.5" U.2 SN861 1.92TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	N	N	N	N	N	N	N	N	N	N	N	N
4XB7B10397	ThinkSystem 2.5" U.2 SN861 3.84TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	N	N	N	N	N	N	N	N	N	N	N	N
4XB7B10398	ThinkSystem 2.5" U.2 SN861 7.68TB Read Intensive NVMe PCIe 5.0 x4 HS SSD	N	N	N	N	N	N	N	N	N	N	N	N
4XB7B10399	ThinkSystem 2.5" U.2 SN861 15.36TB 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.

PCIe 4.0 support: The SN861 SSDs offer a PCIe 5.0 host interface, however they are backward compatible with a PCIe 4.0 host interface. Note however that servers or NVMe retimer/switch adapters with a PCIe 4.0 host interface will not see the same performance levels (especially sequential read and write rates).

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

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 9. 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

The following tables list the ThinkSystem servers that support the FoD license upgrade.

Table 10. IBM SKLM Key Management license upgrade support (Part 1 of 5)

		AMD V3				2S Intel V3/V4						Multi Node V3			1S V3			
Part Number	**Description**	**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)**

Table 11. IBM SKLM Key Management license upgrade support (Part 2 of 5)

		4S 8S Intel V3/V4					GPU Rich							Edge					
Part Number	Description	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)	SR680a V4 (7DMK)	SE100 (7DGR)	SE350 (7Z46 / 7D1X)	SE350 V2 (7DA9)	SE360 V2 (7DAM)	SE450 (7D8T)	SE455 V3 (7DBY)

Table 12. IBM SKLM Key Management license upgrade support (Part 3 of 5)

		Super Computing							1S Intel V2			2S Intel V2			AMD V1			
Part Number	Description	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)

Table 13. IBM SKLM Key Management license upgrade support (Part 4 of 5)

		Dense V2				4S V2		8S	4S V1			1S Intel V1			
Part Number	Description	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)

Table 14. IBM SKLM Key Management license upgrade 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)

Warranty

The SN861 SSDs carry a one-year, customer-replaceable unit (CRU) limited warranty. When the SSDs are installed in a supported server, these drives assume the server'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 SN861 SSDs have the following physical specifications:

Dimensions and weight of the 2.5-inch drives (approximate, without the drive tray):

- Height: 15 mm (0.6 in.)
- Width: 70 mm (2.8 in.)
- Depth: 100 mm (4.0 in.)
- Weight: 140 g (1.92TB, 3.84TB), 142 g (7.68TB, 15.36TB)

Operating environment

The SN861 SSDs are supported in the following environment:

- Temperature
  - Operating: 0°C to 75°C
  - Shipping: -40°C to 85°C up to 15 days, 0°C to 60°C standard
  - Non-operating: -40°C to 70°C
- Relative humidity (non-condensing):
  - Operating: 10% to 90%
  - Shipping: 5 to 95%
  - Non-operating: 5% to 95%
- Maximum altitude:
  - Operating: up to 10,000 feet above sea level
  - Shipping: -305 m to +12,000 m
  - Non-operating: -305 m to +5,400 m
- Shock:
  - Operating 150 G / 6ms duration
  - Non-operating: 1,000 G / 0.5ms duration
- Vibration:
  - Operating: 3-500 Hz, 1.11 G_{RMS} spec, 30min/axis, along all 3 axes
  - Non-operating: 2-500 Hz, 2.92 G_{RMS} spec, 30min/axis, along all 3 axes

Agency approvals

The SN861 SSDs conform to the following regulations:

- Electromagnetic
  - CISPR 32 (Australia, New Zealand)
  - CNS 15396 (Taiwan)
  - EN 55032, EN 55035, EN 61000-3-2, EN 61000-3-3 (EU)
  - FCC Title 47 Part 15, Subpart B (USA)
  - ICES-003 (Canada)
  - VCCI 32-1 (Japan)
  - KSC 9832, KSC 9835 (Korea)
- Safety:
  - UL/cUL standards:
    - EN 60950-1:2006 with A11:2009, A1:2010, A2:2013/ EN 62368-1:2018.
    - IEC 63000-1:2018, Third Edition; Am 1:2009, A2:2013/ IEC 62368-1:2018 (Third Edition).
    - UL 60950-1, Second Edition, 2014-10-14/ UL 62368-1:2018 (Third Edition), USA.
    - CSA C22.2 No. 60950-1-07, Second Edition, 2014-10/ CAN/CSA-C22.2 No. 62368-1-14 2nd edition, Canada
  - European Standards Compliance:
    - EN 60950-1:2006 with A11:2009, A1:2010, A12:2011, A2:2013/ IEC 62368-1:2014 (Second Edition)

Related publications and links

For more information, see the following web pages:

- Lenovo ThinkSystem SSD Portfolio Comparison
  https://lenovopress.com/lp1261-lenovo-thinksystem-ssd-portfolio
- SanDisk product page for SN861 SSDs:
  https://shop.sandisk.com/products/ssd/internal-ssd/sandisk-dc-sn861-ssd

Related product families

Product families related to this document are the following:

- Drives

Notices

This document, LP2367, was created or updated on February 3, 2026.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  https://lenovopress.lenovo.com/LP2367
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at https://lenovopress.lenovo.com/LP2367.

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®
System x®
ThinkSystem®

The following terms are trademarks of other companies:

AMD is a trademark of Advanced Micro Devices, Inc.

Intel®, the Intel logo is a trademark of Intel Corporation or its subsidiaries.

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.