ThinkSystem 5200 Mainstream SATA 6Gb SED SSDs
Product Guide (withdrawn product)

The ThinkSystem 5200 Mainstream SATA 6Gb solid-state drives (SSDs) are high-performance self-encrypting drives (SEDs) that adhere to the Trusted Computing Group Enterprise Security Subsystem Class cryptographic standard (TCG Enterprise SSC). They use Micron NAND flash memory technology with a SATA 6Gbps interface to provide an affordable solution for secure mixed read/write workloads.

The 5200 Mainstream SATA SED SSD is shown in the following figure.

Figure 1. ThinkSystem 5200 Mainstream SATA 6Gb SED SSDs

Did you know?

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.

Rigorous testing of the 5200 Series SSDs by Lenovo through the ServerProven program assures a high degree of storage subsystem compatibility and reliability. Providing additional peace of mind, these drives are covered under Lenovo warranty.

Part number information

The following table lists the ThinkSystem part numbers.

Withdrawn: All drives described in this product guide are now withdrawn from marketing

Table 1. ThinkSystem ordering information

Part number	Feature	Description
2.5-inch hot-swap drives		
4XB7A14062	B6K1	ThinkSystem 2.5" 5200 960GB Mainstream SATA 6Gb Hot Swap SSD SED
4XB7A14063	B6K0	ThinkSystem 2.5" 5200 1.92TB Mainstream SATA 6Gb Hot Swap SSD SED
4XB7A13981	B93J	ThinkSystem 2.5" 5200 (Max) 1.92TB Mainstream SATA 6Gb Hot Swap SSD SED
4XB7A13982	B81X	ThinkSystem 2.5" 5200 3.84TB Mainstream SATA 6Gb Hot Swap SSD SED

The benefits of 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.

Features

The 5200 Mainstream SATA SED SSDs have the following features:

- Industry standard 2.5-inch form factor
- Compliant with the Trusted Computing Group Enterprise Security Subsystem Class cryptographic standard (TCG Enterprise SSC)
- Supports the SafeStore self-encrypting drive (SED) functionality of ThinkSystem RAID adapters
- Innovative 64-layer triple-level cell (TLC) 3D NAND technology
- Suitable for mixed read/write workloads
- 6 Gbps SATA host interface
- High reliability and enhanced ruggedness
- 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:
    - 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

SSDs have a huge but finite number of program/erase (P/E) cycles, which affect how long they can perform write operations and thus their life expectancy. Mainstream SSDs typically have a better cost per read IOPS ratio but lower endurance and performance compared to Performance 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 total bytes written (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. However, 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 1.92TB PRO mainstream drive has an endurance of 5,950 TB of total bytes written (TBW). This means that for full operation over five years, write workload must be limited to no more than 3,260 GB of writes per day, which is equivalent to 1.7 full drive writes per day (DWPD). For the device to last three years, the drive write workload must be limited to no more than 5,434 GB of writes per day, which is equivalent to 2.8 full drive writes per day.

Technical specifications

The following table presents technical specifications for the 5200 Mainstream SATA SED SSDs.

Tip: All drives listed in this product guide are the Lenovo versions of the Micron 5200 PRO SSD, except for the 1.92TB Max drive (4XB7A13981), which is a Micron 5200 MAX drive.

Table 2. Technical specifications

Feature	960 GB drive	1.92 TB PRO drive	1.92 TB MAX drive	3.84 TB drive
Interface	6 Gbps SATA	6 Gbps SATA	6 Gbps SATA	6 Gbps SATA
Capacity	960 GB	1.92 TB	1.92 TB	3.84 TB
Endurance (drive writes per day)	1.3 DWPD	1.7 DWPD	5.0 DWPD	2.5 DWPD
Endurance (total bytes written)	2,270 TB	5,950 TB	17520 TB	17,600 TB
Data reliability	< 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	3,000,000 hours	3,000,000 hours	3,000,000 hours	3,000,000 hours
IOPS reads (4 KB blocks)	95,000	95,000	95,000	95,000
IOPS writes (4 KB blocks)	32,000	32,000	70,000	24,500
Sequential read rate (128 KB blocks)	540 MBps	540 MBps	540 MBps	540 MBps
Sequential write rate (128 KB blocks)	520 MBps	520 MBps	520 MBps	520 MBps
Read latency (seq)	200 µs	200 µs	200 µs	200 µs
Write latency (seq)	300 µs	300 µs	300 µs	900 µs
Shock, non-operating	1,500 G (Max) at 0.5 ms	1,500 G (Max) at 0.5 ms	1,500 G (Max) at 0.5 ms	1,500 G (Max) at 0.5 ms
Vibration, non-operating	3.13 G_{RMS} (5-800 Hz)	3.13 G_{RMS} (5-800 Hz)	3.13 G_{RMS} (5-800 Hz)	3.13 G_{RMS} (5-800 Hz)
Typical power (Read / Write)	2.8 / 3.4 W	3.0 / 3.6 W	3.0 / 3.6 W	2.5 / 3.3 W

Server support

The following tables list the ThinkSystem servers that are compatible.

Table 3. Server support (Part 1 of 4)

Part Number	Description	AMD V3				2S Intel V3			4S 8S Intel V3			Multi Node			GPU Rich				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)	SR850 V3 (7D97 / 7D96)	SR860 V3 (7D94 / 7D93)	SR950 V3 (7DC5 / 7DC4)	SD535 V3 (7DD8 / 7DD1)	SD530 V3 (7DDA / 7DD3)	SD550 V3 (7DD9 / 7DD2)	SR670 V2 (7Z22 / 7Z23)	SR675 V3 (7D9Q / 7D9R)	SR680a V3 (7DHE)	SR685a V3 (7DHC)	ST50 V3 (7DF4 / 7DF3)	ST250 V3 (7DCF / 7DCE)	SR250 V3 (7DCM / 7DCL)
4XB7A14062	ThinkSystem 2.5" 5200 960GB Mainstream SATA 6Gb Hot Swap SSD SED	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
4XB7A14063	ThinkSystem 2.5" 5200 1.92TB Mainstream SATA 6Gb Hot Swap SSD SED	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
4XB7A13981	ThinkSystem 2.5" 5200 (Max) 1.92TB Mainstream SATA 6Gb Hot Swap SSD SED	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
4XB7A13982	ThinkSystem 2.5" 5200 3.84TB Mainstream SATA 6Gb Hot Swap SSD SED	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N

Table 4. Server support (Part 2 of 4)

Part Number	Description	Edge					Super Computing					1S Intel V2			2S Intel V2		
		SE350 (7Z46 / 7D1X)	SE350 V2 (7DA9)	SE360 V2 (7DAM)	SE450 (7D8T)	SE455 V3 (7DBY)	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)
4XB7A14062	ThinkSystem 2.5" 5200 960GB Mainstream SATA 6Gb Hot Swap SSD SED	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
4XB7A14063	ThinkSystem 2.5" 5200 1.92TB Mainstream SATA 6Gb Hot Swap SSD SED	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
4XB7A13981	ThinkSystem 2.5" 5200 (Max) 1.92TB Mainstream SATA 6Gb Hot Swap SSD SED	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
4XB7A13982	ThinkSystem 2.5" 5200 3.84TB Mainstream SATA 6Gb Hot Swap SSD SED	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N

Table 5. Server support (Part 3 of 4)

Part Number	Description	AMD V1					Dense V2				4S V2		8S	4S V1			1S Intel V1			
		SR635 (7Y98 / 7Y99)	SR655 (7Y00 / 7Z01)	SR655 Client OS	SR645 (7D2Y / 7D2X)	SR665 (7D2W / 7D2V)	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)
4XB7A14062	ThinkSystem 2.5" 5200 960GB Mainstream SATA 6Gb Hot Swap SSD SED	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
4XB7A14063	ThinkSystem 2.5" 5200 1.92TB Mainstream SATA 6Gb Hot Swap SSD SED	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
4XB7A13981	ThinkSystem 2.5" 5200 (Max) 1.92TB Mainstream SATA 6Gb Hot Swap SSD SED	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
4XB7A13982	ThinkSystem 2.5" 5200 3.84TB Mainstream SATA 6Gb Hot Swap SSD SED	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N

Table 6. Server support (Part 4 of 4)

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)
4XB7A14062	ThinkSystem 2.5" 5200 960GB Mainstream SATA 6Gb Hot Swap SSD SED	N	N	N	N	N	Y	Y	N	N	N	N	N
4XB7A14063	ThinkSystem 2.5" 5200 1.92TB Mainstream SATA 6Gb Hot Swap SSD SED	N	N	N	N	N	Y	Y	N	N	N	N	N
4XB7A13981	ThinkSystem 2.5" 5200 (Max) 1.92TB Mainstream SATA 6Gb Hot Swap SSD SED	N	N	N	N	N	Y	Y	N	Y	N	N	N
4XB7A13982	ThinkSystem 2.5" 5200 3.84TB Mainstream SATA 6Gb Hot Swap SSD SED	N	N	N	N	N	Y	Y	N	N	N	N	N

Storage controller support

SAS and SATA SED drives require a supported controller, either a SAS HBA or a RAID controller, with SED support. SED support of RAID adapters is via the MegaRAID SafeStore functionality of the adapter. SED support of the SAS HBAs (where supported) is by using software on the server (SED commands are passed through the HBA to the drives).

The following table lists which ThinkSystem controllers support the use of SED drives.

Note: Not all servers that support these drives also support all of the adapters supported here. Consult the individual server product guide for specific server support of the adapters.

Table 7. ThinkSystem controller support for SED drives

Part number	Description	SED Services
SAS HBAs for internal drives		
7Y37A01088	ThinkSystem 430-8i SAS/SATA 12Gb HBA	Host software pass-thru
4C57A16217	ThinkSystem SD530 430-8i SAS/SATA 12Gb Dense HBA Kit	Host software pass-thru
7Y37A01089	ThinkSystem 430-16i SAS/SATA 12Gb HBA	Host software pass-thru*
4Y37A72480	ThinkSystem 4350-8i SAS/SATA 12Gb HBA	Host software pass-thru*
4Y37A72481	ThinkSystem 4350-16i SAS/SATA 12Gb HBA	Host software pass-thru*
4Y37A09725	ThinkSystem 440-16i SAS/SATA PCIe Gen4 12Gb Internal HBA	Host software pass-thru
RAID adapters for internal drives		
None	Intel RSTe onboard controller	No
7M27A03918	ThinkSystem RAID 530-4i 2 Drive Adapter Kit for SN550	MegaRAID SafeStore
7M17A03932	ThinkSystem RAID 530-4i 4 Drive Adapter Kit for SN850	MegaRAID SafeStore
7Y37A01082	ThinkSystem RAID 530-8i PCIe 12Gb Adapter	MegaRAID SafeStore
4Y37A09727	ThinkSystem RAID 530-16i PCIe 12Gb Adapter	MegaRIAD SafeStore
4C57A16216	ThinkSystem SD530 HW RAID Kit	MegaRAID SafeStore
4Y37A72482	ThinkSystem RAID 5350-8i PCIe 12Gb Adapter	Supported*
7Y37A01083	ThinkSystem RAID 730-8i 1GB Cache PCIe 12Gb Adapter	No
4Y37A09722	ThinkSystem RAID 730-8i 2GB Flash PCIe 12Gb Adapter	MegaRAID SafeStore
7M27A03917	ThinkSystem RAID 930-4i-2GB 2 Drive Adapter Kit for SN550	MegaRAID SafeStore
7M17A03933	ThinkSystem RAID 930-4i-2GB 4 Drive Adapter Kit for SN850	MegaRAID SafeStore
7Y37A01084	ThinkSystem RAID 930-8i 2GB Flash PCIe 12Gb Adapter	MegaRAID SafeStore
7Y37A01085	ThinkSystem RAID 930-16i 4GB Flash PCIe 12Gb Adapter	MegaRAID SafeStore
4Y37A09721	ThinkSystem RAID 930-16i 8GB Flash PCIe 12Gb Adapter	MegaRAID SafeStore
7Y37A01086	ThinkSystem RAID 930-24i 4GB Flash PCIe 12Gb Adapter	MegaRAID SafeStore
4Y37A72483	ThinkSystem RAID 9350-8i 2GB Flash PCIe 12Gb Adapter	Supported*
4Y37A72485	ThinkSystem RAID 9350-16i 4GB Flash PCIe 12Gb Adapter	Supported*
4Y37A72484	ThinkSystem RAID 9350-8i 2GB Flash PCIe 12Gb Internal Adapter	Supported*
4Y37A72486	ThinkSystem RAID 9350-16i 4GB Flash PCIe 12Gb Internal Adapter	Supported*
4Y37A09728	ThinkSystem RAID 940-8i 4GB Flash PCIe Gen4 12Gb Adapter	MegaRAID SafeStore
4Y37A09729	ThinkSystem RAID 940-8i 8GB Flash PCIe Gen4 12Gb Adapter	MegaRAID SafeStore
4Y37A78600	ThinkSystem RAID 940-16i 4GB Flash PCIe Gen4 12Gb Adapter	MegaRAID SafeStore
4Y37A09730	ThinkSystem RAID 940-16i 8GB Flash PCIe Gen4 12Gb Adapter	MegaRAID SafeStore

Part number	Description	SED Services
4Y37A09735	ThinkSystem RAID 940-16i 8GB Flash PCIe Gen4 12Gb Internal Adapter	MegaRAID SafeStore
4Y37A09733	ThinkSystem RAID 940-32i 8GB Flash PCIe Gen4 12Gb Adapter	MegaRAID SafeStore

* A firmware update may be required for SED support

For more information, see the RAID adapter and HBA product guides:

- RAID controllers: https://lenovopress.com/servers/options/raid
- SAS HBAs: https://lenovopress.com/servers/options/hba

To compare the capabilities of these adapters, see the Lenovo ThinkSystem RAID Adapter and HBA Reference:
https://lenovopress.com/LP1288

Operating system support

SSDs operate transparently to users, storage systems, applications, databases, and operating systems.

Operating system support is based on the controller used to connect to the drives. Consult the controller propduct guide for more information:

- RAID controllers: https://lenovopress.com/servers/options/raid
- SAS HBAs: https://lenovopress.com/servers/options/hba

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 8. 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 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 are compatible.

Table 10. IBM SKLM Key Management support (Part 1 of 4)

		AMD V3				2S Intel V3			4S 8S Intel V3			Multi Node			GPU Rich				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)	SR850 V3 (7D97 / 7D96)	SR860 V3 (7D94 / 7D93)	SR950 V3 (7DC5 / 7DC4)	SD535 V3 (7DD8 / 7DD1)	SD530 V3 (7DDA / 7DD3)	SD550 V3 (7DD9 / 7DD2)	SR670 V2 (7Z22 / 7Z23)	SR675 V3 (7D9Q / 7D9R)	SR680a V3 (7DHE)	SR685a V3 (7DHC)	ST50 V3 (7DF4 / 7DF3)	ST250 V3 (7DCF / 7DCE)	SR250 V3 (7DCM / 7DCL)
A5U1	SKLM for System x w/SEDs - FoD per Install w/1Yr S&S	N	N	Y	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	Y	Y
AS6C	SKLM for System x w/SEDs - FoD per Install w/3Yr S&S	N	N	Y	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	Y	Y

Table 11. IBM SKLM Key Management support (Part 2 of 4)

Part Number	Description	Edge					Super Computing					1S Intel V2			2S Intel V2		
		SE350 (7Z46 / 7D1X)	SE350 V2 (7DA9)	SE360 V2 (7DAM)	SE450 (7D8T)	SE455 V3 (7DBY)	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)
A5U1	SKLM for System x w/SEDs - FoD per Install w/1Yr S&S	N	N	N	N	N	N	N	N	N	N	N	Y	Y	N	Y	Y
AS6C	SKLM for System x w/SEDs - FoD per Install w/3Yr S&S	N	N	N	N	N	N	N	N	N	N	N	Y	Y	N	Y	Y

Table 12. IBM SKLM Key Management support (Part 3 of 4)

Part Number	Description	AMD V1					Dense V2				4S V2		8S	4S V1			1S Intel V1			
		SR635 (7Y98 / 7Y99)	SR655 (7Y00 / 7Z01)	SR655 Client OS	SR645 (7D2Y / 7D2X)	SR665 (7D2W / 7D2V)	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)
A5U1	SKLM for System x w/SEDs - FoD per Install w/1Yr S&S	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	N	N	N	N	N
AS6C	SKLM for System x w/SEDs - FoD per Install w/3Yr S&S	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	N	N	N	N	N

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

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)
A5U1	SKLM for System x w/SEDs - FoD per Install w/1Yr S&S	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N
AS6C	SKLM for System x w/SEDs - FoD per Install w/3Yr S&S	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	N

Warranty

The 5200 Mainstream SATA 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 drives have the following physical specifications (approximate, without the tray):

- Height: 7 mm (0.3 in.)
- Width: 70 mm (2.8 in.)
- Depth: 100 mm (4.0 in.)
- Weight: 70 g (2.5 oz)

Shipping dimensions and weight - 2.5-inch drives (approximate, including the tray):

- Height: 63 mm (2.5 in.)
- Width: 174 mm (6.9 in.)
- Depth: 133 mm (5.2 in.)
- Weight: 434 g (1.0 lb)

Operating environment

The SSDs are supported in the following environment:

- Operating temperature: 0 to 70°C (32 to 158°F)
- Non-operating temperature: -40 to 85°C (-40 to 185°F)
- Relative humidity: 5 to 95% (non-condensing)

Agency approvals

The 5200 Mainstream SATA SED SSDs conform to the following regulations:

- Micron Green Standard
- Built with sulfur resistant resistors
- CE (Europe): EN 55032 Class B, RoHS
- FCC: CFR Title 47, Part 15 Class B
- UL: UL-60950-1, 2nd Edition
- BSMI (Taiwan): approval to CNS 13438
- RCM (Australia, New Zealand): AS/NZS CISPR32 Class B
- KCC RRL (Korea): approval to KN 32 Class B, KN 35 Class B
- W.E.E.E.: Compliance with EU WEEE directive 2002/96/EC.
- TUV (Germany): approval to IEC60950/EN60950
- VCCI (Japan): 2015-04 Class B
- IC (Canada): CISPR32 Class B: Canadian ICES-003:2016

Related publications and links

For more information, see the following documents:

- Product Guide for ThinkSystem 5200 Mainstream SATA 6Gb SSDs
  https://lenovopress.com/LP0926
- Lenovo ThinkSystem storage options product page
  https://lenovopress.com/lp0761-storage-options-for-thinksystem-servers
- ServerProven for SSDs
  http://www.lenovo.com/us/en/serverproven
- Lenovo RAID Introduction
  https://lenovopress.com/lp0578-lenovo-raid-introduction
- Lenovo RAID Management Tools and Resources
  https://lenovopress.com/lp0579-lenovo-raid-management-tools-and-resources
- ServeRAID Adapter Quick Reference
  http://lenovopress.com/tips0054

Related product families

Product families related to this document are the following:

- Drives
- Security Key Lifecycle Manager

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, LP1173, was created or updated on November 22, 2021.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  https://lenovopress.lenovo.com/LP1173
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at https://lenovopress.lenovo.com/LP1173.

Trademarks

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

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

The following terms are trademarks of other companies:

AMD is a trademark of Advanced Micro Devices, Inc.

Intel® is a trademark of Intel Corporation or its subsidiaries.

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