ThinkSystem CM893a Read Intensive SATA 6Gb SSDs
Product Guide

The ThinkSystem CM893a Read Intensive SATA SSDs are general-purpose SSDs that are engineered for greater performance and endurance in a cost-effective design, and to support a broader set of workloads. With SED encryption as standard, these drives help ensure data security, even when the drive is removed from the server.

SED support: All drives listed in this product guide include SED drive encryption. Our naming convention for new drives doesn't include SED in the name.

Figure 1. ThinkSystem CM893a Read Intensive SATA SSDs

Did you know?

Lenovo Read Intensive SSDs are suitable for read-intensive and general-purpose data center workloads. Overall, these SSDs provide outstanding IOPS/watt and cost/IOPS for enterprise solutions and are an excellent choice for applications such as web serving, hyperscale cloud, content delivery, caching, databases, and analytics.

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.

Table 1. Ordering part numbers and feature codes

Part number	Feature code	Description	Vendor part number
4XB7A89423	BXDY	ThinkSystem 2.5" CM893a 1.92TB Read Intensive SATA 6Gb HS SSD	MZ7L31T9HELA-00AV7

The part numbers include the following items:

- One 2.5-inch solid-state drive in a ThinkSystem hot-swap tray
- Documentation flyer

Features

The CM893a SSDs have the following features:

- Low cost, read-intensive SSD from Samsung
- 2.5-inch industry standard form factor with hot-swap tray
- 6 Gbps SATA interface
- TCG Opal SED drive encryption
- Advanced ECC Engine and End-to-End Data Protection
- Samsung V6 (128-layer) TLC V-NAND stacks the vertical NAND layers in three dimensions, solving the cell-to-cell interference that causes data corruption in planar NAND.
- Protect data integrity from unexpected power loss with Samsung's advanced power-loss protection (PLP) architecture
- Supports Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T).
- Dynamic Thermal Guard Protection protects the SSD from overheating by automatically controlling the speed of the CPU relative to its core temperature

Read-Intensive (Entry) SSDs and Write-Intensive (Performance) SSDs have similar read and write IOPS performance, but the key difference between them is their endurance (or lifetime) (that is, how long they can perform write operations because SSDs have a finite number of program/erase (P/E) cycles). 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) 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 mix-use up to 70% read/30% write environments to ensure that the TBW of the drive will not be exceeded before the required life expectancy.

The 1.92TB CM893a drive has an endurance of 3,504 TB of total bytes written (TBW). This means that for full operation over five years, write workload must be limited to no more than 1,920 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 3,200 GB of writes per day, which is equivalent to 1.7 full drive writes per day.

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.

Technical specifications

The following table lists the technical specifications of the CM893a SSDs.

Table 2. Technical specifications

Feature	**1.92 TB drive**
Interface	6 Gbps SATA
Capacity	1.92 TB
SED encyption	TCG Opal
Endurance (total bytes written)	3504 TB
Endurance (drive writes per day for 5 years)	1 DWPD
Data reliability (UBER)	< 1 in 10^{17} bits read
MTBF	2,000,000 hours
IOPS reads (4 KB blocks)	97,000
IOPS writes (4 KB blocks)	31,000
Sequential read rate (128 KB blocks)	560 MBps
Sequential write rate (128 KB blocks)	530 MBps
Read latency (random)	120 µs
Write latency (random)	40 µs
Shock, non-operating	1,500 G (Max) at 0.5 ms
Vibration, non-operating	20 G (20-2000 Hz)
Typical power (R/W)	2.2 W / 3.2 W

Server support

The following tables list the ThinkSystem servers that are compatible.

Table 3. Server support (Part 1 of 4)

Part Number	Description	2S 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)	ST250 V3 (7DCF / 7DCE)	SR250 V3 (7DCM / 7DCL)
4XB7A89423	ThinkSystem 2.5" CM893a 1.92TB Read Intensive SATA 6Gb HS SSD	N	N	Y	Y	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)
4XB7A89423	ThinkSystem 2.5" CM893a 1.92TB Read Intensive SATA 6Gb HS SSD	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y

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)
4XB7A89423	ThinkSystem 2.5" CM893a 1.92TB Read Intensive SATA 6Gb HS SSD	Y	Y	Y	Y	Y	N	N	N	N	Y	Y	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)
4XB7A89423	ThinkSystem 2.5" CM893a 1.92TB Read Intensive SATA 6Gb HS SSD	N	N	N	N	N	N	N	N	N	N	N	N

Operating system support

SATA 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 7. 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 8. 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 ThinkSystem CM893a Read Intensive SATA 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 CM893a SSDs have the following physical specifications:

Dimensions and weight (approximate, without the hot-swap tray):

- Height: 7 mm (0.3 in.)
- Width: 70 mm (2.8 in.)
- Depth: 100 mm (4.0 in.)
- Weight: 70 g (2.1 oz)

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

- Height: 63 mm (2.5 in.)
- Width: 133 mm (5.2 in.)
- Depth: 174 mm (6.9 in.)
- Weight (hot-swap): 433 g (1.0 lb)

Operating environment

The CM893a SSDs are supported in the following environment:

- Temperature: 0 to 70 °C (32 to 158 °F)
- Relative humidity: 5 to 95% (noncondensing)
- Maximum altitude: 3,050 m (10,000 ft)

Agency approvals

The CM893a SSDs conform to the following regulations:

- UL
- TUV
- FCC
- CE Mark
- C-Tick Mark
- BSMI (Taiwan)
- KCC (Korea EMI)

Related publications and links

For more information, see the following documents:

- Samsung Data Center SSDs product page:
  https://www.samsung.com/semiconductor/ssd/datacenter-ssd/
- Lenovo ThinkSystem storage options product web page
  https://lenovopress.com/lp0761-storage-options-for-thinksystem-servers
- Lenovo ThinkSystem SSD Portfolio comparison:
  https://lenovopress.com/lp1261-lenovo-thinksystem-ssd-portfolio
- Lenovo server options product page
  https://www.lenovo.com/us/en/data-center/options/
- 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

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, LP1789, was created or updated on August 8, 2023.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  https://lenovopress.lenovo.com/LP1789
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at https://lenovopress.lenovo.com/LP1789.

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:

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

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