



OPEN

Compute Project

Datacenter NVMe[®] SSD Specification

Version 2.7 (01082026)

Author: Ross Stenfort, Meta

Author: Lee Prewitt, Tim Sharp, Microsoft

Author: Paul Kaler, HPE

Author: David Black, Colm Murphy, Dell Technologies

Author: Chris Sabol, Charles Kunzman, Google

Table of Contents

1	OCP	6
1.1	LICENSE OWF OPTION	6
1.2	SYSTEM FIRMWARE	6
2	OVERVIEW	6
3	SCOPE	6
4	NVM EXPRESS REQUIREMENTS	7
4.1	OVERVIEW	7
4.2	NVME RESET SUPPORTED	7
4.3	NVME CONTROLLER CONFIGURATION AND BEHAVIOR	7
4.4	NVME ADMIN COMMAND SET	9
4.4.1	Namespace Management/Attachment Commands	12
4.4.2	Namespace Utilization (NUSE)	12
4.4.3	UUID for DSSD Specific Information	13
4.4.4	DSSD Asynchronous Events	14
4.5	NVME I/O COMMAND SET	15
4.6	OPTIONAL NVME FEATURE SUPPORT	16
4.7	COMMAND TIMEOUT	18
4.8	LOG PAGE REQUIREMENTS	19
4.8.1	Standard Log Page Requirements	19
4.8.2	TCG Activity Events for Persistent Event Log	22
4.8.3	TCG Activity Event Format	23
4.8.4	DSSD Log Page Requirements	26
4.8.5	SMART / Health Information Requirements	27
4.8.6	SMART / Health Information Extended Log Page (Log Identifier C0h) Requirements	28
4.8.7	Error Recovery and the Error Recovery Log Page (Log Identifier C1h)	39
4.8.8	Latency Monitor Log Page and Feature Set Requirements	46
4.8.9	Latency Monitor Log Page (Log Identifier C3h) Requirements	48
4.8.10	Device Capabilities Log Page (Log Identifier C4h) Requirements	61
4.8.11	DSSD Power State Requirements	65
4.8.12	Unsupported Requirements Log Page (Log Identifier C5h) Requirements	66
4.8.13	Hardware Component Log Page (Log Identifier C6h) Requirements	67
4.8.14	TCG Configuration Log Page (Log Identifier C7h) Requirements	70
4.8.15	Telemetry String Log Page (Log Identifier C9h) Requirements	74
4.9	HOST AND CONTROLLER INITIATED TELEMETRY LOG PAGES	81
4.9.1	Theory of Operation	81
4.9.2	Data Partitioning Overview	81
4.9.3	Statistic Area	81
4.9.4	Event FIFO	81
4.9.5	Existing NVMe Log Pages	81
4.9.6	Debug Structure Overview Summary	82
4.9.7	Telemetry Data Requirements	82
4.9.8	Telemetry Reason Identifier Format	84
4.9.9	Debug Profiles	85
4.9.10	Statistic Descriptor	85
4.9.11	Statistic Identifiers	86
4.9.12	Context Statistic Descriptor	98
4.9.13	Statistic Descriptor Location	101
4.9.14	Statistic Requirements	102
4.9.15	Event FIFO Requirements	102

4.9.16	Event FIFO Location.....	121
4.9.17	Telemetry Data Area.....	122
4.10	DEVICE SELF-TEST REQUIREMENTS	130
4.11	FIRMWARE UPDATE REQUIREMENTS	133
4.12	FACTORY DEFAULT REQUIREMENTS	136
4.13	DEALLOCATION REQUIREMENTS.....	137
4.14	SECTOR SIZE AND NAMESPACE SUPPORT.....	138
4.15	SET/GET FEATURES REQUIREMENTS.....	138
4.15.1	General Feature Requirements.....	138
4.15.2	DSSD Feature Requirements.....	140
4.15.3	Event Injection (Feature Identifier C0h) Set Features.....	140
4.15.4	Event Injection (Feature Identifier C0h) Get Features	149
4.15.5	PLP Failure Mode (Feature Identifier C2h) Set Features.....	149
4.15.6	PLP Failure Mode (Feature Identifier C2h) Get Features	151
4.15.7	Clear PCIe Correctable Error Counters (Feature Identifier C3h) Set Features	152
4.15.8	Clear PCIe Correctable Error Counters (Feature Identifier C3h) Get Features.....	153
4.15.9	Enable IEEE1667 Silo (Feature Identifier C4h) Set Features	153
4.15.10	Enable IEEE1667 Silo (Feature Identifier C4h) Get Features	154
4.15.11	Latency Monitor (Feature Identifier C5h) Set Features	155
4.15.12	Latency Monitor (Feature Identifier C5h) Get Features.....	157
4.15.13	PLP Health Check Interval (Feature Identifier C6h) Set Features.....	158
4.15.14	PLP Health Check Interval (Feature Identifier C6h) Get Features	159
4.15.15	DSSD Power State (Feature Identifier C7h) Set Features	160
4.15.16	DSSD Power State (Feature Identifier C7h) Get Features	161
4.15.17	Telemetry Profile (Feature Identifier C8h) Set Features.....	162
4.15.18	Telemetry Profile (Feature Identifier C8h) Get Features	163
4.15.19	DSSD Asynchronous Event Configuration (Feature Identifier C9h) Set Features	164
4.15.20	DSSD Asynchronous Event Configuration (Feature Identifier C9h) Get Features.....	166
4.15.21	Idle Wake Up Time Configuration (Feature Identifier CAh) Set Features.....	167
4.15.22	Idle Wake Up Time Configuration (Feature Identifier CAh) Get Features.....	168
4.15.23	Max PCIe Interface Configuration (Feature Identifier CBh).....	169
4.15.24	Max PCIe Interface Configuration (Feature Identifier CBh) Get Features	171
5	PCIe REQUIREMENTS.....	172
5.1	BOOT REQUIREMENTS.....	175
5.2	PCIe ERROR LOGGING.....	175
5.3	LOW POWER MODES	176
5.4	PCIe EYE CAPTURE	176
6	OPTIONAL DEVICE FEATURES	176
6.1	FLEXIBLE DATA PLACEMENT REQUIREMENTS.....	176
6.1.1	Generic Flexible Data Placement Requirements.....	176
6.1.2	FDP Single Reclaim Group Configuration 1	177
6.1.3	FDP Single Reclaim Group Configuration 2	177
6.1.4	FDP Die Placement Configuration.....	177
6.2	DIX REQUIREMENTS	177
6.3	DIF REQUIREMENTS.....	178
7	RELIABILITY	179
7.1	UNCORRECTABLE BIT ERROR RATE.....	179
7.2	POWER ON/OFF REQUIREMENTS.....	179
7.2.1	Time to Ready and Shutdown Requirements	179
7.2.2	Incomplete/Unsuccessful Shutdown.....	180
7.3	END TO END INTERNAL DATA PROTECTION.....	182

7.4	BEHAVIOR ON FIRMWARE CRASH, PANIC OR ASSERT	183
7.5	ANNUAL FAILURE RATE (AFR).....	183
7.6	BACKGROUND DATA REFRESH	184
7.7	WEAR-LEVELING	184
7.8	POWER LOSS PROTECTION.....	185
7.9	DEVICE LIMITS.....	187
8	ENDURANCE	187
8.1	ENDURANCE DATA	187
8.2	RETENTION CONDITIONS.....	187
8.3	SHELF LIFE.....	188
8.4	END-OF-LIFE (EOL)	188
9	THERMAL.....	189
9.1	DATA CENTER ALTITUDE	189
9.2	THERMAL THROTTLING	189
9.3	TEMPERATURE REPORTING.....	191
9.4	THERMAL SHUTDOWN	192
10	FORM FACTOR REQUIREMENTS	192
10.1	GENERAL FORM FACTOR REQUIREMENTS.....	192
10.2	POWER CONSUMPTION MEASUREMENT METHODOLOGY	193
10.3	POWER LEVELS.....	193
10.4	M.2 FORM FACTOR REQUIREMENTS	194
10.5	E1.S FORM FACTOR REQUIREMENTS.....	195
10.6	E1.L FORM FACTOR REQUIREMENTS.....	196
10.7	E3 FORM FACTOR REQUIREMENTS	197
10.8	SFF-8639 (U.2/U.3) FORM FACTOR REQUIREMENTS	197
10.9	E2 FORM FACTOR REQUIREMENTS	198
11	MANAGEMENT SUPPORT	199
11.1	NVME BASIC MANAGEMENT COMMAND (APPENDIX A) REQUIREMENTS	199
11.2	NVME BASIC MANAGEMENT COMMAND (APPENDIX A) DATA FORMAT.....	200
11.3	NVME-MI REQUIREMENTS	204
11.4	VPD REQUIREMENTS.....	207
12	SECURITY	208
12.1	BASIC SECURITY REQUIREMENTS.....	208
12.2	SECURE BOOT	213
12.3	DMTF SECURITY PROTOCOL AND DATA MODEL (SPDM)	214
12.3.1	SPDM Certificates.....	216
12.3.2	SPDM Firmware Measurements.....	217
12.4	DATA ENCRYPTION AND ERADICATION	218
12.5	TCG IMPLEMENTATION REQUIREMENTS.....	218
12.5.1	TCG Version and Features.....	219
12.5.2	TCG Communication Layer.....	220
12.5.3	TCG Session Layer	220
12.5.4	TCG Transactions	221
12.5.5	TCG Authentication	221
12.5.6	TCG Crypto.....	221
12.5.7	TCG Locking Security Provider	222
12.5.8	TCG PSID Feature Set.....	222
13	DEVICE PROFILES	223

14	LABELING	224
14.1	LABEL REQUIREMENTS	225
15	COMPLIANCE.....	230
15.1	ROHS COMPLIANCE	230
15.2	ESD COMPLIANCE.....	230
15.3	EMC COMPLIANCE.....	230
16	SHOCK AND VIBRATION.....	230
17	SUSTAINABILITY REQUIREMENTS	231
18	LINUX NVME-CLI PLUG-IN REQUIREMENTS.....	231
18.1	NVME-CLI MANAGEMENT UTILITY.....	231
18.2	NVME-CLI PLUGIN REQUIREMENTS	231
18.2.1	<i>NVMe-CLI Plug-In Nomenclature/Functional Requirements.....</i>	<i>231</i>
18.2.2	<i>NVMe-CLI Plug-In FW Activation History Requirements</i>	<i>232</i>
19	REVISION HISTORY	232
20	META SPECIFIC ITEMS	236
20.1	CONFIGURATION SPECIFICS	236
20.2	PERFORMANCE REQUIREMENTS.....	238
20.3	TRIM RATE TARGETS.....	241
20.4	IO.GO BENCHMARK TARGETS	241
20.5	FILEAPPEND BENCHMARK TARGETS	241
20.6	SEQUENTIAL WRITE BANDWIDTH	242
20.7	CACHEBENCH TARGETS	242
20.8	BOOTBENCH TARGET.....	242
21	MICROSOFT SPECIFIC ITEMS.....	242
21.1	CONFIGURATION SPECIFICS	243
22	LATENCY MONITORING FEATURE SET THEORY OF OPERATION	243
22.1	OVERVIEW	243
22.2	FUNCTIONAL OPERATION	243
22.2.1	<i>Bucket Description Overview</i>	<i>244</i>
22.2.2	<i>Active Bucket Description.....</i>	<i>244</i>
22.3	PERSISTENCE ACROSS POWER CYCLES.....	250
22.4	DEBUG LOGS	250
22.5	LATENCY MONITORING FEATURE - EVENT HANDLING	251
22.5.1	<i>Power Off/On When Latency Monitoring Feature is Enabled</i>	<i>251</i>
22.5.2	<i>Latency Monitoring Feature Persistence.....</i>	<i>252</i>
22.5.3	<i>Moving Information from Active to Static Buckets.....</i>	<i>252</i>
22.5.4	<i>Firmware Update.....</i>	<i>252</i>
22.6	CONFIGURING LATENCY MONITORING	252
23	OCP TENANTS	252
24	ACKNOWLEDGEMENTS	253

1 OCP

1.1 License OWF Option

Contributions to this Specification are made under the terms and conditions set forth in Open Web Foundation Contributor License Agreement (“OWF CLA 1.0”) (“Contribution License”) by:

Meta
Microsoft
HPE
Dell Technologies
Google

Usage of this Specification is governed by the terms and conditions set forth in the Open Web Foundation Final Specification Agreement (“OWFa 1.0”).

Note: The following clarifications, which distinguish technology licensed in the Contribution License and/or Specification License from those technologies merely referenced (but not licensed), were accepted by the Incubation Committee of the OCP:

NONE

1.2 System Firmware

All products seeking OCP Accepted™ Product Recognition must complete the Open System Firmware (OSF) Tab in the OCP Open Platform Firmware [2021 Supplier Requirements Checklist](#). The completed checklist shall be uploaded and available

at: [https://github.com/opencomputeproject/OpenSystemFirmware/\[vendor_name\]/\[product_name\]/](https://github.com/opencomputeproject/OpenSystemFirmware/[vendor_name]/[product_name]/).

Note to author: replace [vendor_name] and [product_name] with actual company name and product identifier.

2 Overview

This document is to define the requirements for a Datacenter NVMe SSD (DSSD) for use in datacenters. The requirements in this document are in addition to the requirements in the underlying standards and may override some requirements in the underlying standards. The authors have attempted to note where requirements may be incompatible with the underlying standards.

If functionality in an underlying standard (e.g., a command) is not covered in this document, then the requirements in the underlying standard apply. For example, if an optional command in an underlying standard is not covered in this document, then that command remains optional.

Customers may impose additional requirements beyond those specified in this document.

3 Scope

This document covers PCIe-attached SSDs using NVM Express.

4 NVM Express Requirements

4.1 Overview

Requirement ID	Description
NVMe-1	The device shall comply with all required features of the NVM Express Base Specification Revision 2.2, the NVM Express NVM Command Set Specification Revision 1.1, and the NVM Express NVMe over PCIe Transport Specification Revision 1.2, or later except as overridden by this specification. Optional features in those three specifications shall be implemented per the requirements of this specification based on the three specifications above. The vendor shall provide an NVMe compliance report that demonstrates compliance.
NVMe-2	Any optional NVMe features supported by the device not described in this document shall be clearly documented and disclosed to the customer.
NVMe-3	Any vendor unique features supported by the device not described in this document shall be clearly documented and disclosed to the customer.

4.2 NVMe Reset Supported

Requirement ID	Description
NVMeR-1	NVM Subsystem Reset (NSSR) shall be supported via the NSSRC register.
NVMeR-2	NVMe Controller Reset (CC.EN cleared from 1b to 0b) shall be supported.

4.3 NVMe Controller Configuration and Behavior

Requirement ID	Description
NVMe-CFG-1	The default arbitration shall be Round-Robin. Weighted Round Robin with Urgent Class Priority shall be supported.
NVMe-CFG-2	The device shall support a Maximum Data Transfer Size (MDTS) value of at least 256 KiB.
NVMe-CFG-3	The device firmware shall support the use of CSTS.CFS.
NVMe-CFG-4	Obsolete. Replaced by LABL-11 .
NVMe-CFG-5	The minimum supported queue depth shall be 1,024 per submission queue.
NVMe-CFG-6	The minimum number of I/O Queue Pairs shall be 1,023.
NVMe-CFG-7	The single default namespace (see SECTOR-3) shall have a unique non-zero value in the EUI64 (Extended Unique Identifier) field in the Identify Namespace data structure. For each namespace that is created other than the initial namespace configured in the factory, the device shall clear the EUI64 field to 0h in the Identify Namespace data structure. This requirement is specific to the value of the EUI64 field in the Identify Namespace data structure and has no effect on the value of the NGUID field in that data structure.

Requirement ID	Description
NVMe-CFG-8	The device shall support a non-zero NGUID per Namespace and shall never reuse any NGUID value (i.e., the UIDREUSE bit in the Common Namespace Features field of the Identify Namespace data structure shall be set to 1b).
NVMe-CFG-9	The Doorbell Stride field in the Controller Capabilities data structure (CAP.DSTRD) shall be cleared to 0h.
NVMe-CFG-10	The device shall align the start of the Doorbells to a 4096-byte boundary as per the PCI Express Base Specification and the NVM Express Base Specification.
NVMe-CFG-11	If the Controller Memory Buffer (CMB) is supported, then the implementation shall comply with TP4054, which is included in the NVMe Express Base Specification 1.4 and subsequent versions (see NVMe-1). This includes the requirement that the CMB shall be disabled by default.
NVMe-CFG-12	The Controller Power Scope field in the Controller Capabilities property shall be set to a value of 11b to indicate it is NVM subsystem scope (i.e., the NVM subsystem does not support multiple power domains).
NVMe-CFG-13	The device shall support the NVM Command Set (i.e., in the Command Sets Supported field in the Controller Capabilities (CAP) property bit 0 shall be set to 1b, bit 6 shall be cleared to 0b, and bit 7 shall be cleared to 0b, and the Controller Type field in the Identify Controller data structure shall be set to 01h).
NVMe-CFG-14	The device shall support a maximum Submission Queue Entry Size of 64 bytes (i.e., bits 7:4 of the SQES field in the Identify Controller data structure shall be set to 6).
NVMe-CFG-15	The device shall support a maximum Completion Queue Entry Size of 16 bytes (i.e., bits 7:4 of the CQES field in the Identify Controller data structure shall be set to 4).
NVMe-CFG-16	The device shall clear the Memory Page Size Minimum (MPSMIN) field to 0h (4 KiB minimum page size).
NVMe-CFG-17	The device shall set the Memory Page Size Maximum (MPSMAX) field to a value of 1h or greater (8 KiB or greater maximum page size).
NVMe-CFG-18	The device shall support 256 Error Log Page Entries.
NVMe-CFG-19	The device shall clear the Host Memory Buffer Minimum Size field and the Host Memory Buffer Preferred Size field in the Identify Controller data structure to 0h (i.e., the Host Memory Buffer feature shall not be supported).
NVMe-CFG-20	The device shall clear the CAP.CRMS.CRIMS bit to 0b.
NVMe-CFG-21	The device shall support Power Measurement (See TP4199).
NVMe-CFG-22	The device shall not write to any memory in any Submission Queue (SQ).
NVMe-CFG-23	The device shall not read from any memory in any Completion Queue (CQ).
NVMe-CFG-24	The device shall meet full performance under the following conditions when not limited by host performance: • a single SQ/CQ pair with a max queue depth of 1024; • an Arbitration burst of at most 8 commands (RAB = 3);

Requirement ID	Description
	- a PCIe Payload Size of 512 bytes or less; and - device formatted to 4KiB LBAs.

4.4 NVMe Admin Command Set

The device shall support the following mandatory and optional NVMe Admin commands:

Requirement ID	Description
NVMe-AD-1	The device shall support all mandatory NVMe Admin commands.
NVMe-AD-2	Identify – In addition to supporting all the mandatory CNS values and the associated mandatory fields within the data returned for each mandatory CNS value, the following optional fields shall be supported: - Format progress indicator (FPI) with an update granularity of 1% in the Identify Namespace data structure in the NVM Command Set and in the I/O Command Set Independent Identify Namespace data structure. - I/O Performance and Endurance Hints: - bit 4 (OPTPERF) shall be set to 1b in the Namespace Features (NSFEAT) field in the Identify Namespace data structure for the NVM Command Set.
NVMe-AD-3	The Namespace Management command shall be supported.
NVMe-AD-4	The Namespace Attachment command shall be supported.
NVMe-AD-5	The Format NVM command shall be supported. Secure Erase Settings (SES) values 000b, 001b and 010b shall be supported.
NVMe-AD-6	The device shall support the NVMe-MI Receive and NVMe-MI Send commands (i.e., bit 6 in the Optional Admin Command Support field in the Identify Controller data structure shall be set to 1b). The device shall support all NVMe-MI commands that map to the NVMe-MI Receive command and that are mandatory using the in-band tunneling mechanism.
NVMe-AD-7	The device shall support the Sanitize command and the Sanitize Status Log Page (81h). The device shall support Block Erase (010b), Overwrite (011b), and Crypto Erase (100b) sanitize operations. The Sanitize Namespace command defined in TP4153 is optional for the device to support.
NVMe-AD-8	Once data is purged (see SEC-43) due to: - a Sanitize command that requests a sanitize operation and has the No-Deallocate After Sanitize bit cleared to 0b; - a Sanitize command that requests a Block Erase (SANACT=001b) or Crypto Erase (SANACT=100b) sanitize operation and has the No-Deallocate After Sanitize bit set to 1b but resulted in a deallocate for the reason specified in NVMe-AD-19; - a Format NVM command that specifies User Data Erase or Cryptographic Erase; or - a TCG Revert method, RevertSP method or GenKey method, the device shall deallocate all user data, enable reads to the purged/deallocated LBAs without generating errors, and return all zeroes for host reads to LBAs that have not been written since the last such purge completed.

Requirement ID	Description
	Once data is purged (see SEC-43) due to a Sanitize command that requests an Overwrite (SANACT=011b) sanitize operation, and has the No-Deallocate After Sanitize bit set to 1b, the device shall not deallocate any user data, shall enable reads to the overwritten LBAs without generating errors, and shall return the bytes written by the last overwrite pass for host reads to LBAs that have not been written since the last such purge completed.
NVMe-AD-9	Obsolete. Incorporated into NVMe-AD-8.
NVMe-AD-10	The device shall support Identify command UUID List functionality (CNS value 17h).
NVMe-AD-11	If the Namespace Identifier (NSID) is not used for a specific NVMe Admin command, and the host specifies a non-zero NSID, then the controller shall abort the command with status Invalid Field in Command.
NVMe-AD-12	The Device Self-test command shall be supported.
NVMe-AD-13	Obsolete. See SELFTEST-8 .
NVMe-AD-14	The device shall support the Lockdown command. For device profile specific requirements see DP-CFG-11 .
NVMe-AD-15	The Lockdown command shall support locking down all supported Admin commands on the in-band interface including the Lockdown command itself and all Admin commands not referenced in this specification.
NVMe-AD-16	The Lockdown command shall support locking down all supported Features on the in-band interface, including those not referenced in this specification.
NVMe-AD-17	The device shall set the No-Deallocate Modifies Media After Sanitize field to 01b in the Sanitize Capabilities in the Identify Controller data structure. Additional media modification after Sanitize is prohibited.
NVMe-AD-18	The device shall clear the No-Deallocate Inhibited bit to 0b in the Sanitize Capabilities in the Identify Controller data structure.
NVMe-AD-19	If the device cannot return logical block data due to checksum errors after a sanitize operation successfully completes that had been started by a Sanitize command with the No-Deallocate After Sanitize bit set to 1b, then the device shall instead perform a deallocation even though it was requested not to deallocate and shall set the Sanitize Status field to 100b in the Sanitize Status log page upon successful completion of the sanitize operation and deallocation. This behavior overrides the requirements in the NVM Express Base Specification.
NVMe-AD-20	Obsolete. Incorporated into NVMe-AD-8 .
NVMe-AD-21	The device shall not write data to any namespace user data in the NVM subsystem as part of a Crypto Erase sanitize operation, Block Erase sanitize operation, Format NVM Cryptographic Erase, Format NVM User Data Erase, or TCG Opal Revert/RevertSP/GenKey method.
NVMe-AD-22	The device shall be shipped from the factory with the Sanitize Status field in the Sanitize Status log page cleared to 000b indicating the NVM subsystem has never been sanitized and the Global Data Erased bit in the Sanitize Status field set to 1b.

Requirement ID	Description
NVMe-AD-23	The device shall support the Format NVM command on a per namespace basis (i.e., bit 0 and bit 1 shall be cleared to 00b in the Format NVM Attributes field in Identify Controller).
NVMe-AD-24	The device shall report a minimum value of 3 in the Asynchronous Event Request Limit field in the Identify Controller data structure to indicate support for at least 4 outstanding Asynchronous Event Request commands.
NVMe-AD-25	If asynchronous events occur for which reporting is enabled and there are no Asynchronous Event Request commands outstanding, then the controller shall retain the event information for those Asynchronous Event Types and use that information for responses to future Asynchronous Event Request commands. Queued duplicate Asynchronous events shall be reported once. This requirement does not apply to Immediate (asynchronous) events, as Immediate events are never queued.
NVMe-AD-26	The device shall support Media Verification for entire device sanitize operations initiated by the Sanitize command.
NVMe-AD-27	The device is not required to support the Get LBA Status command. The device shall support the related LBA Status Information log page, see STD-LOG-11 .
NVMe-AD-28	The device shall clear the DAE bit to 0b in the NSFEAT field in Identify Namespace to indicate that the device does not support the Deallocated or Unwritten Logical Block error for any namespace.
NVMe-AD-29	The device shall support both the 0b and 1b values of the No-Deallocate After Sanitize bit in the Sanitize command. If the No-Deallocate After Sanitize bit is cleared to 0b in a Sanitize command, then the device shall deallocate all LBAs upon completion of the sanitize operation, including media verification (see NVMe-AD-26), if performed as part of the sanitize operation.
NVMe-AD-30	The controller shall delete all queued Asynchronous Event Notifications upon Power Cycle or Controller Level Reset events.
NVMe-AD-31	For the DSSD Error Reporting asynchronous event, the default value for the DSSD Asynchronous Event Configuration feature (Feature Identifier C9h) shall be set to 1 (i.e., enabled). See GDAEC-2 .
NVMe-AD-32	For the DSSD Media Ready asynchronous event, the default value for the DSSD Asynchronous Event Configuration feature (Feature Identifier C9h) shall be cleared to 0 (i.e., disabled). See GDAEC-3 .
NVMe-AD-33	If the device is able to perform a Cryptographic Erase for a Format NVM command that requests User Data Erase (SES=001b), then the device shall: • support Cryptographic Erase functionality (SES=010b) for Format NVM commands; and • perform a cryptographic erase for any Format NVM command that requests User Data Erase.

4.4.1 Namespace Management/Attachment Commands

The namespace management command along with the attach/detach commands is used to increase device over-provisioning beyond the default minimum over-provisioning.

Requirement ID	Description	
NSM-1	The namespace management commands shall be supported on all namespaces.	
NSM-2	When creating a namespace, the default “Formatted LBA Size” parameter (FLBAS = 0) in the Identify Namespace Data Structure (byte 26) shall correspond to the default sector size set at the factory.	
NSM-3	The LBA Format 0 Support field shall correspond to the default sector size set at the factory (see DP-CFG-1).	
NSM-4	The device shall support a minimum of 16 Namespaces (see Section 13 Device Profiles).	
NSM-5	For some models (see Section 13 Device Profiles), the minimum number of namespaces shall be at least 128 Namespaces at 7 TiB based on 16 Namespaces per TB of usable capacity. The number of Namespaces shall be based on the device usable capacity as follows:	
	Device Usable Capacity	Minimum Number of Namespaces
	<= 1 TiB	16
	> 1 TiB but <= 2 TiB	32
	> 2 TiB but <= 3 TiB	48
	> 3 TiB but <= 4 TiB	64
	...	...
	> 7 TiB	128
NSM-6	The device shall report at least one Namespace Granularity Descriptor in the Namespace Granularity List.	
NSM-7	The device shall support the TNVMCAP and UNVMCAP fields in the Identify Controller Data Structure.	
NSM-8	The device shall not support extended LBA formats (i.e., the Extended LBA Formats Supported bit in the Controller Attributes register in the Identify Controller data structure shall be cleared to ‘0’).	

4.4.2 Namespace Utilization (NUSE)

Requirement ID	Description
NUSE-1	The NUSE shall be equal to the number of logical blocks currently allocated in the namespace. NUSE cannot be hardcoded to be equal to NCAP. Here is an example for a 200 GB device: After a Format NVM command User Data Erase (SES = 001b), NUSE would be zero. And the usage data would reflect that: 0.00 GB.

Requirement ID	Description
	- After writing 1 GB worth of data, the usage data is expected to show the following: 1.00 GB. - After filling the device, the usage data is expected to show the following: 200.00 GB. - If the host issues a 10 GB deallocate command and the device completes deallocation of the data, the usage data would show the following: 190.00 GB. Deallocation may occur in the background after completion of the deallocate command with NUSE updated accordingly as deallocation occurs.

4.4.3 UUID for DSSD Specific Information

A UUID has been defined for use in commands to ensure that the vendor specific Log Identifiers and Feature Identifiers used in this specification access the functionality defined in this specification (i.e., do not access other vendor specific functionality that may use the same vendor specific identifiers).

Requirement ID	Description																																		
UUID-1	The UUID List (NVMe-AD-10) shall contain a UUID List Entry that contains the UUID value C194D55BE0944794A21D29998F56BE6Fh in big endian format. The Identifier Association field in that UUID List Entry shall be cleared to 00b. For clarity: <table> <tr> <th>Byte Address</th><th>Value</th></tr> <tr><td>48</td><td>C1h</td></tr> <tr><td>49</td><td>94h</td></tr> <tr><td>50</td><td>D5h</td></tr> <tr><td>51</td><td>5Bh</td></tr> <tr><td>52</td><td>E0h</td></tr> <tr><td>53</td><td>94h</td></tr> <tr><td>54</td><td>47h</td></tr> <tr><td>55</td><td>94h</td></tr> <tr><td>56</td><td>A2h</td></tr> <tr><td>57</td><td>1Dh</td></tr> <tr><td>58</td><td>29h</td></tr> <tr><td>59</td><td>99h</td></tr> <tr><td>60</td><td>8Fh</td></tr> <tr><td>61</td><td>56h</td></tr> <tr><td>62</td><td>BEh</td></tr> <tr><td>63</td><td>6Fh</td></tr> </table>	Byte Address	Value	48	C1h	49	94h	50	D5h	51	5Bh	52	E0h	53	94h	54	47h	55	94h	56	A2h	57	1Dh	58	29h	59	99h	60	8Fh	61	56h	62	BEh	63	6Fh
Byte Address	Value																																		
48	C1h																																		
49	94h																																		
50	D5h																																		
51	5Bh																																		
52	E0h																																		
53	94h																																		
54	47h																																		
55	94h																																		
56	A2h																																		
57	1Dh																																		
58	29h																																		
59	99h																																		
60	8Fh																																		
61	56h																																		
62	BEh																																		
63	6Fh																																		
UUID-2	The Get Features and Set Features commands shall support UUID Index functionality.																																		

Requirement ID	Description
UUID-3	A Get Features command or a Set Features command with: - the UUID Index of the UUID (UUID-1) in the UUID List (NVMe-AD-10) or a zero UUID Index; and - a vendor-specific Feature Identifier that is used in this specification (see Section 4.15 Set/Get Feature Requirements) shall access the vendor specific Feature defined in this specification.
UUID-4	The Get Log Page command shall support UUID Index functionality.
UUID-5	A Get Log Page command with: - the UUID Index of the UUID (UUID-1) in the UUID List (NVMe-AD-10) or a zero UUID Index; and - a vendor-specific Log Page Identifier that is defined in this specification (see Section 4.8.4 DSSD Log Page Requirements) shall access the specified vendor specific log page defined in this specification.
UUID-6	The vendor-specific events in the Persistent Event log page shall support UUID Index functionality.

4.4.4 DSSD Asynchronous Events

This section describes the Asynchronous Event Notifications defined by this specification.

Requirement ID	Description
DSSD-AEN-1	If the device uses the Error Reporting AEN to report an error condition and the device encounters an error condition, then the device shall complete an Asynchronous Event Request (AER) command with an Asynchronous Event Notification (AEN) with Completion Queue Entry Dword 0 set as follows: - The Log Page Identifier field shall be set to C1h. - The Asynchronous Event Information field shall be set to 01h. - The Asynchronous Event Type field shall be set to 111b (Vendor Specific). - The device shall process an Error Reporting AEN as a Notice event (e.g., queued if there is not an outstanding AER command).
DSSD-AEN-2	If the device uses the Media Ready AEN to report that the media is ready to process commands and the Media Ready Event occurs, the device shall complete an Asynchronous Event Request (AER) command with an Asynchronous Event Notification (AEN) with Completion Queue Entry Dword 0 set as follows: - The Log Page Identifier field shall be cleared to 00h. - The Asynchronous Event Information field shall be set to 01h. - The Asynchronous Event Type field shall be set to 111b (Vendor Specific). The device shall process a Media Ready AEN as a One-Shot event (e.g., queued if there is no outstanding AER command).

4.5 NVMe I/O Command Set

Requirement ID	Description															
NVMe-IO-1	The device shall support all mandatory NVMe I/O commands.															
NVMe-IO-2	The device shall support the Dataset Management command. For additional information see TRIM-1 .															
NVMe-IO-3	Since the device is power fail safe (e.g., has Power Loss Protection (PLP)) the performance shall not be degraded by any of the following: - FUA – i.e., forced unit access shall not incur a performance penalty. - Flush Cache – i.e., flush cache shall have no effect as the PLP makes any cache non-volatile. - Volatile Write Cache (Feature Identifier 06h) Set Features to disable write-cache. This command shall fail as described in the NVM Express Base Specification as there is no volatile write cache.															
NVMe-IO-4	The device shall support the Write Zeroes command and shall set bit 3 of the ONCS field to 1b. The following bits of the Write Zeroes command shall be supported: - Deallocate (DEAC) bit. - Force Unit Access (FUA) bit.															
NVMe-IO-5	The Write Zeroes command shall have the following behavior:															
	<table><tr><th>DEAC</th><th>FUA</th><th>Behavior</th></tr><tr><td>0b</td><td>0b</td><td>The device shall follow the NVM Express NVM Command Set Specification, see NVMe-1.</td></tr><tr><td>0b</td><td>1b</td><td>The device shall follow the NVM Express NVM Command Set Specification, see NVMe-1.</td></tr><tr><td>1b</td><td>1b</td><td>The device shall follow the NVM Express NVM Command Set Specification, see NVMe-1.</td></tr><tr><td>1b</td><td>0b</td><td>See NVMe-IO-6.</td></tr></table>	DEAC	FUA	Behavior	0b	0b	The device shall follow the NVM Express NVM Command Set Specification, see NVMe-1 .	0b	1b	The device shall follow the NVM Express NVM Command Set Specification, see NVMe-1 .	1b	1b	The device shall follow the NVM Express NVM Command Set Specification, see NVMe-1 .	1b	0b	See NVMe-IO-6.
	DEAC	FUA	Behavior													
	0b	0b	The device shall follow the NVM Express NVM Command Set Specification, see NVMe-1 .													
	0b	1b	The device shall follow the NVM Express NVM Command Set Specification, see NVMe-1 .													
	1b	1b	The device shall follow the NVM Express NVM Command Set Specification, see NVMe-1 .													
1b	0b	See NVMe-IO-6.														
NVMe-IO-6	If the Write Zeroes DEAC bit is set to 1b and the FUA bit is cleared to 0b, the device shall deallocate the specified LBAs and shall return all zeros for any subsequent read to the specified LBAs until modified by a command (e.g., Write, Copy, etc.), regardless of the behavior of the Dataset Management command.															
NVMe-IO-7	With the DEAC bit set to 1b and the FUA bit cleared to 0b one or more Write Zeroes command(s) whose data size is the maximum value that is less than or equal to the data size: - indicated by the value of the Write Zeroes Size Limit (WZSL) field in the Identify Controller Data Structure for the NVM command set if that WZSL field is set to a non-zero value; or - that results from the maximum value of the NLB field in the Write Zeroes command for a namespace that uses the factory default sector size (see DP-CFG-1) if that WZSL field is cleared to zero,															

Requirement ID	Description
	shall be able to completely deallocate the entire device including updating the FTL map (e.g., in memory) so that subsequent reads return all zeroes as required by NVMe-IO-6 in less than one minute.
NVMe-IO-8	The device shall support the Compare command.
NVMe-IO-9	The device shall support the Compare and Write fused command pair.
NVMe-IO-10	For some models (see Section 13 Device Profiles), the device shall support the Write Uncorrectable command.
NVMe-IO-11	The Write Uncorrectable command shall support marking LBAs uncorrectable at a single LBA granularity regardless of the number of LBAs in the FTL indirection granularity.
NVMe-IO-12	The device shall not limit the number of LBAs that the host is able to specify in a Write Uncorrectable command beyond the minimum and maximum allowed by the NVM Express NVM Command Set Specification. The device shall support Write Uncorrectable commands that specify a single LBA.
NVMe-IO-13	There shall be no limit on the total media capacity that can be marked uncorrectable by Write Uncorrectable commands.
NVMe-IO-14	Uncorrectable errors (e.g., read errors) that are a consequence of a prior Write Uncorrectable command shall not be counted in the SMART / Health Information log page (Log Identifier 02h) Media and Data Integrity Errors field.
NVMe-IO-15	The device shall support SGLs for all I/O commands.
NVMe-IO-16	The device shall support SGL Descriptor Type 0, 1, 2 and 3.
NVMe-IO-17	The device shall configure SGLS (SGL Support) 2-bit field in the SGLS Dword field in the Identify Controller Data Structure to a value of 01b (byte alignment) or 10b (Dword alignment). Host code should use Dword alignment regardless of this field value.
NVMe-IO-18	The device shall set the MPTR SGL Descriptor Support (MSDS) bit to 1b in the Identify Controller Data Structure.

4.6 Optional NVMe Feature Support

The device shall also support the following NVMe features:

Requirement ID	Description
NVMe-OPT-1	Obsolete. Duplicate of STD-LOG-7 and STD-LOG-8 .
NVMe-OPT-2	The device shall support the Timestamp feature (Feature Identifier 0Eh). Timestamps are used to align the devices internal logs.
NVMe-OPT-3	Obsolete. See TEL-5 .
NVMe-OPT-4	If a timestamp has been set via Set Features for the Timestamp feature (Feature Identifier 0Eh), then: a) the device shall maintain the timestamp across all Controller Level Resets other than a Controller Level Reset caused by an NVM Subsystem Reset (i.e., if a

Requirement ID	Description
	timestamp has been set, then it is only permissible to clear the Timestamp Origin field to 000b due to an NVM Subsystem Reset and the device shall set the Timestamp Origin field to 001b for all Controller Level Resets other than NVM Subsystem Reset); and b) saving the timestamp across an NVM Subsystem Reset is optional.
NVMe-OPT-5	The device shall never set the Synch field bit to 1b in the Timestamp feature (Feature Identifier 0Eh).
NVMe-OPT-6	The device shall only generate a Telemetry Log Changed event on an error condition and shall not generate a Telemetry Log Changed event for periodic logging.
NVMe-OPT-7	The device shall report its Indirection Unit (IU) size in the Namespace Preferred Write Granularity (NPWG) field in the Identify Namespace data structure.
NVMe-OPT-8	The device shall support sending Telemetry Log Notices (i.e., bit 3 of the Log Page Attributes field shall be set to 1b).
NVMe-OPT-9	The device shall support the Namespace Attribute Changed asynchronous event and the associated Changed Namespace List log page (i.e., bit 8 of the Optional Asynchronous Events Supported field shall be set to 1b in the Identify Controller data structure). This event shall only be reported for namespaces that are attached to a controller.
NVMe-OPT-10	The device shall support the Firmware Activation Notices event (i.e., bit 9 shall be set to 1b in the Optional Asynchronous Events Supported field in the Identify Controller data structure).
NVMe-OPT-11	Obsolete. See NVMe-AD-24 .
NVMe-OPT-12	The device shall be composed of a single NVM subsystem (i.e., the CAP.CPS field shall be set to 11b in the CAP controller register, and the MDS bit shall be cleared to 0b in the Controller Attributes field in the Identify Controller data structure).
NVMe-OPT-13	The Timestamp feature (Feature Identifier 0Eh) shall not be saveable.
NVMe-OPT-14	The device shall ignore the values in reserved bits and fields received in commands or register writes (i.e., the device shall not generate an error because a reserved bit or field is not cleared to zero).
NVMe-OPT-15	Obsolete. See NVMe-OPT-7.
NVMe-OPT-16	The device shall support the Copy command and Source Range Entries Descriptor Format 0.
NVMe-OPT-17	The device shall set the Atomic Write Unit Power Fail (AWUPF) field in the Identify Controller data structure to a value that greater than or equal to the value of the Namespace Preferred Write Granularity (NPWG) field in every Identify Namespace data structure.
NVMe-OPT-18	The device shall support the Power Threshold feature (Feature Identifier 24h) defined in TP4199.
NVMe-OPT-19	The device shall support the Power Measurement feature (Feature Identifier 25h) defined in TP4199.

Requirement ID	Description
NVMe-OPT-20	The device shall support Tracking LBA Allocation with Granularity with a 64 KiB granularity or smaller.
NVMe-OPT-21	The device shall not support the Power Limit feature (Feature Identifier 23h) defined in TP4190.
NVMe-OPT-22	The device should coalesce writes smaller than Namespace Preferred Write Granularity (NPWG) to enable writing of NPWG sized chunks of data without read/modify/write.

4.7 Command Timeout

Requirement ID	Description
CTO-1	NVMe Admin commands and TCG commands shall take no more than 10 seconds from submission to completion. This CTO-1 requirement does not apply to the time taken by background operations (e.g., Device Self-test and Sanitize commands). This CTO-1 requirement does not apply to Asynchronous Event Request commands.
CTO-2	In addition to the Asynchronous Event Request command, the only other exception to the CTO-1 requirement shall be the Format NVM Command for non-Cryptographic Erase operations. Format NVM Cryptographic Erase and the TCG methods Revert, RevertSP and GenKey shall comply with the CTO-1 requirement.
CTO-3	Once the TTR-2 requirement is satisfied, an individual I/O command (submitted under Queue Depth 1) shall take no more than 8 seconds from submission to completion. Under full load the device shall not have more than 7 I/Os take more than 2 seconds in one hour.
CTO-4	I/O command processing time shall not be a function of device capacity.
CTO-5	The vendor shall disclose any I/O scenario that could violate the timeout requirements in CTO-1 through CTO-4.
CTO-6	The device shall set MDTS, the attributes of the Number of Queues feature (Feature Identifier 07h) and Maximum Queue Entries Supported such that the CTO-3 requirement cannot be violated.
CTO-7	A Crypto Erase sanitize operation, and any background activity initiated by a TCG command (e.g., as indicated by OutstandingData) shall complete within 10 seconds.
CTO-8	A Block Erase sanitize operation and a Format NVM command performing a User Data Erase shall each complete within 10 seconds per TB of device capacity (e.g., a Block Erase sanitize operation on a 4TB device shall complete within 40 seconds).
CTO-9	The device shall report the greater of the Sanitize Crypto Erase, Format NVM Cryptographic Erase, TCG Opal Revert, TCG Opal RevertSP, or TCG Opal GenKey time in the Estimated Time for Crypto Erase field in the Sanitize Status log page.
CTO-10	The device shall not set the Estimated Time fields in the Sanitize Status log page to a value of FFFFFFFFh for supported sanitize operations.

Requirement ID	Description
CTO-11	Formats between LBAF values with the Secure Erase Settings field cleared to 000b (No secure erase operation requested) or 2h (Cryptographic Erase) shall complete within 10 seconds.

4.8 Log Page Requirements

4.8.1 Standard Log Page Requirements

Requirement ID	Description	
STD-LOG-1	The device shall support the Error Information log page (Log Identifier 01h).	
STD-LOG-2	The device shall support the SMART / Health Information log page (Log Identifier 02h).	
STD-LOG-3	Under no conditions shall the Percentage Used field in the SMART / Health Information log page (Log Identifier 02h) decrease to a lower value than previously reported.	
STD-LOG-4	The Percentage Used field in the SMART / Health Information log page (Log Identifier 02h) shall be based on the average P/E cycle of the device. In addition, this field shall be based on the actual P/E cycle count of the media and not on the Power on Hours (POH) of the device.	
STD-LOG-5	The device shall support the Firmware Slot Information log page (Log Identifier 03h).	
STD-LOG-6	The device shall support the Commands Supported and Effects log page (Log Identifier 05h).	
STD-LOG-7	The device shall support the Telemetry Host-Initiated log page (Log Identifier 07h).	
STD-LOG-8	The device shall support the Telemetry Controller-Initiated log page (Log Identifier 08h).	
STD-LOG-9	The device shall support the Persistent Event log page (Log Identifier 0Dh).	
STD-LOG-10	The device shall support the following Persistent Event Log types:	
	Type	Event
	01h	SMART / Health Log Snapshot
	02h	Firmware Commit
	03h	Timestamp Change
	04h	Power-on or Reset
	05h	NVM Subsystem Hardware Error ¹
	06h	Change Namespace
	07h	Format NVM Start
	08h	Format NVM Completion
	09h	Sanitize Start
	0Ah	Sanitize Completion
	0Ch	Telemetry Log Created

Requirement ID	Description			
	ODh	Thermal Excursion		
	DEh	Vendor Specific This specification defines vendor specific events to report TCG command execution (see Section 4.8.2 TCG Events for Persistent Event Log and Section 4.8.3 TCG Activity Event Format).		
	Note(s): 1. The device shall not log PCIe Unsupported Request errors that are Advisory Non-Fatal.			
STD-LOG-11	The device shall support the LBA Status Information log page (Log Identifier 0Eh). The device is not required to support the related Get LBA Status command (see NVMe-AD-27).			
STD-LOG-12	The following behavior types are used to define the functional boundary condition behaviors for saturating or wrapping, under reset conditions and power cycles:			
	Behavior Type	Saturating Counter ¹	Reset ² Persistent	Power Cycle/PERST# Persistent
	0	Reserved		
	1	No	No	No (Volatile Value)
	2	No	Yes	Yes
	3	Yes	Yes	No
	4	Yes	Yes	Yes
	5	Yes	No	No
	6	No	Yes	No
	15-7	Reserved		
	Note(s): 1. See SLOG-2 for description of saturating counters. For a field or statistic that is not a counter, “Yes” indicates saturating behavior (i.e., report all F’s if the value exceeds the maximum possible value of the field or statistic). 2. All Controller Level Resets (e.g., Controller Reset, NVM Subsystem Reset, PCIe Function Level Reset, PCIe Conventional Reset, etc.). For Behavior Types 1 the counter shall reset to zero only on a Controller Level Reset, including any CLR caused by a Power Cycle or PERST#. For Behavior Type 6 the counter shall reset to zero only on a Power Cycle or PERST#.			
STD-LOG-13	The device shall support the Device Self-test log page (Log Identifier 06h).			
STD-LOG-14	The device shall support the Command and Feature Lockdown log page (Log Identifier 14h).			
STD-LOG-15	The device shall support the Physical Interface Receiver Eye Opening Measurement log page (Log Identifier 19h).			

Requirement ID	Description
STD-LOG-16	In addition to any receiver margining data and image plots, the device shall store information required to evaluate the signal integrity of the receiver such as equalization values like continuous time linear equalization (CTLE), variable gain amplifier (VGA), boost, and decision feedback equalization (DFE) settings in the Eye Data field of the Physical Interface Receiver Eye Opening Measurement log page.
STD-LOG-17	The device shall support the Endurance Group Information log page (Log Identifier 09h). The device shall use a single Endurance Group for the entire device. The device is not required to support the Endurance Group Event Aggregate log page (Log Identifier 0Fh).
STD-LOG-18	The device shall not support the SMART / Health Information log page (Log Identifier 02h) on a per namespace basis (i.e., bit 0 of the Log Page Attributes field in the Identify Controller data structure shall be cleared to 0b).
STD-LOG-19	The Persistent Event log page (Log Identifier 0Dh), Telemetry Host-Initiated log page (Log Identifier 07h), Telemetry Controller-Initiated log page (Log Identifier 08h), and Error Information log page (Log Identifier 01h) shall not contain user data, or the result of any computation performed on user data.
STD-LOG-20	The Persistent Event log page (Log Identifier 0Dh) events shall be ordered so that the more recent events are reported earlier in the log than older events (i.e., the most recent event is Persistent Event 0), and the events deemed less important by the vendor (e.g., old events, informational events, etc.) are removed first when the log is trimmed due to lack of space to store all events).
STD-LOG-21	The Persistent Event log page (Log Identifier 0Dh) reporting context shall be held until released by the host or until at least 5 minutes has elapsed since the last host access of the log unless the log fills and reporting context has to be released in order to remove events (see STD-LOG-20). New events that occur while the context is established shall not be dropped.
STD-LOG-22	The maximum size of the Persistent Event log page (Log Identifier 0Dh) reported in the Persistent Event Log Size (PELS) field in the Identify Controller data structure shall be 5 MiB or greater.
STD-LOG-23	The device shall not lose log page data for any reason, unless otherwise specified (e.g., see STD-LOG-20 and the purge exception in this requirement). Data that does not contain user data or data that could be used to derive user data including the Telemetry Host-Initiated log page (Log Identifier 07h), Telemetry Controller-Initiated log page (Log Identifier 08h), Persistent Event log page (Log Identifier 0Dh), Error Information log page (Log Identifier 01h), vendor-specific log pages, SMART / Health Information log page (Log Identifier 02h) including the Critical Warnings field, SMART / Health Information Extended log page (Log Identifier C0h), and backup energy source failure information shall be persisted across purge operations (see SEC-43). All log page data including the Telemetry Host-Initiated log page (Log Identifier 07h), Telemetry Controller-Initiated log page (Log Identifier 08h), Persistent Event log page (Log Identifier 0Dh), Error Information log page (Log Identifier 01h), vendor-specific log pages, SMART / Health Information log page (Log Identifier 02h) including the Critical Warnings field, SMART / Health Information Extended log page (Log Identifier C0h), and backup

Requirement ID	Description						
	energy source failure information shall be persisted across power loss, all resets, the Format NVM command, and the device entering any protected mode (e.g., read only or error mode). Issues with the device’s encryption engine shall not prevent access to the data specified by this requirement.						
STD-LOG-24	The device shall support the Power Measurement log page (Log Identifier 25h).						
STD-LOG-25	The device shall configure the Power Management Attributes (PMA) field in the Power Management Log as follows: • Clear the Estimated Power Flag (EPF) to 0b • Set the Maximum Interval Power Timestamp Support (MIPWRTS) to 1b						
STD-LOG-26	The following log pages shall be accessible via Get Log Page during a sanitize operation and processing of a Format NVM command. This requirement is in addition to the log pages that are required to be accessible by the NVMe specifications (see NVMe-1): <table><tr><th>Log Page</th><th>Log Page Identifier</th><th>Additional Restrictions for both Format NVM command and sanitize operations</th></tr><tr><td>Firmware Slot Information</td><td>03h</td><td>None</td></tr></table>	Log Page	Log Page Identifier	Additional Restrictions for both Format NVM command and sanitize operations	Firmware Slot Information	03h	None
Log Page	Log Page Identifier	Additional Restrictions for both Format NVM command and sanitize operations					
Firmware Slot Information	03h	None					
STD-LOG-27	The device shall support the Feature Identifiers Supported and Effects log page (Log Identifier 12h) and the NVMe-MI Commands Supported and Effects log page (Log Identifier 13h).						

4.8.2 TCG Activity Events for Persistent Event Log

This defines the requirements for recording TCG Activity Events in the Persistent Event Log as Event Type DEh (see [STD-LOG-10](#)).

Requirement ID	Description
TCGHST-PE-1	The device shall support recording at least 100 TCG Activity Events in the Persistent Event Log without deleting any TCG Activity Events to make room for new events.
TCGHST-PE-2	A TCG Activity Event entry shall be recorded in the Persistent Event Log whenever any of the following TCG activities occurs (the event is recorded upon completion of the activity): • Level 0 Discovery • Start Session • Authenticate method (entries only recorded when the authority specified is not locked out) • Close Session by the host when it sends an End-Of-Session token • Close Session due to timeout • Properties method • Stack Reset • TPer Reset • Hardware Reset • Get method

Requirement ID	Description
	• Set method • GenKey method • Random method • Activate method • Revert method • RevertSP method • Reactivate method • Erase method • Block SID Authentication • Assign method • Deassign method
TCGHST-PE-3	Redundant TCG activities shall not generate new TCG Command Event entries in the Persistent Event Log. A TCG activity shall be considered redundant if it meets ALL the following criteria with respect to a TCG Activity Event that is already recorded in the Persistent Event Log: • Power cycle count is the same; and • Active firmware revision is the same; and • TCG activity is the same as the most recent TCG Activity Event entry; and • Tper state remains the same (i.e., there has been no change either in the device behavior or host visible state); and • The Result field is the same. • The following are examples of TCG activities that do not generate a new TCG Activity Event entry: • Setting an attribute of a TCG Object to a value that is the same as the current value. • Getting or setting the value of an informative attribute of a TCG object (e.g., the CommonName of a Locking Object). • Getting data from or setting data to byte tables. • An unsuccessful authentication attempt that returns AUTHORITY_LOCKED_OUT status.
TCGHST-PE-4	TCG Activity Event entries shall not be removed for any TCG-specific reason (e.g., TCG Revert/RevertSP or TCG Manufactured-Inactive), except as required to make room in the Persistent Event Log for additional TCG Activity Event entries (see TCGHST-PE-1).
TCGHST-PE-5	TCG Activity Event format shall follow the requirements in the TCG Activity Event Format section.

4.8.3 TCG Activity Event Format

This defines the TCG Activity Event format for the Persistent Event Log when using Event Type DEh (see [STD-LOG-10](#) and [Section 4.8.2 TCG Activity Events for Persistent Event Log](#)).

Requirement ID	Byte Address	Field	# of Bytes	Field Description
TCGCE-1	0	Event Type	1	Shall be set to DEh to indicate a vendor-specific event.

Requirement ID	Byte Address	Field	# of Bytes	Field Description
TCGCE-2	1	Event Type Revision	1	Shall be set to 01h to indicate the revision in this specification.
TCGCE-3	2	Event Header Length (EHL)	1	Shall be set to 15h to indicate that 21 bytes of event header information follow and the total event header length (starting from byte 0) is 24 bytes.
TCGCE-4	3	Event Header Additional Information (EHAI)	1	Bits 7:2 are reserved and shall be cleared to 0h. Bits 1:0 shall be set to 01b if the event is associated with an NVM subsystem port and shall be set to 10b if the event is associated with a Management Endpoint.
TCGCE-5	5:4	Controller Identifier	2	Shall contain the NVMe controller identifier for the controller that is associated with the TCG activity.
TCGCE-6	13:06	Event Timestamp	8	Shall indicate the Timestamp of when the TCG activity was completed. This field contains an 8-byte data structure whose format matches the data structure returned by a Get Features command that specifies the Timestamp feature (Feature Identifier 0Eh).
TCGCE-7	15:14	Port Identifier (PELPID)	2	Shall contain a Port Identifier as specified in the definition of this field in the NVMe Express Base Specification.
TCGCE-8	19:16	Reserved	4	Shall be cleared to zero.
TCGCE-9	21:20	Vendor Specific Information Length	2	Shall be set to 04h to align the start of the Vendor Specific Event Data to an 8-byte multiple from the start of this data structure.
TCGCE-10	23:22	Event Length	2	Shall be set to 30h to indicate that 48 bytes of vendor specific information and vendor specific event data follow the event header.
TCGCE-11	27:24	Vendor Specific Information	4	Shall be cleared to zero for padding to align fields that follow.
TCGCE-12	29:28	Vendor Specific Event Code	2	Shall be set to 0001h.
TCGCE-13	30	Vendor Specific Event Data Type	1	Shall be set to 3h to indicate Binary data.
TCGCE-14	31	UUID Index	1	Shall be set to the UUID Index of the UUID (UUID-1) in the UUID List (NVMe-AD-10).

Requirement ID	Byte Address	Field	# of Bytes	Field Description
TCGCE-15	33:32	Vendor Specific Event Data Length (VSEDL)	2	Shall be set to 26h to indicate that the length of the vendor specific event data is 38 bytes.
TCGCE-16	35:34	Reserved	2	Shall be cleared to zero.
TCGCE-17	39:36	TCG Command Count	4	Shall increment every time a TCG command is completed regardless of the result, and an entry is recorded per TCGHST-PE-2 and TCGHST-PE-3 . This value shall be cleared to zero when the device is shipped from the factory.
TCGCE-18	47:40	Invoking ID	8	The 8-byte UID of the table, object, or SP associated with the event (e.g., for a method, this indicates the entity upon which the method is invoked).
TCGCE-19	55:48	Method ID	8	The 8-byte UID of the method being invoked.
TCGCE-20	57:56	ComID	2	The 2-byte ComID specified by the host in the command.
TCGCE-21	58	ProtocolID	1	The Protocol Id specified by the host in the command.
TCGCE-22	59	Status	1	The TCG status on completion of the command.
TCGCE-23	61:60	Process Time	2	Time in milliseconds it took to process the command.
TCGCE-24	71:62	TCG Activity Specific Context	10	Additional context for a TCG activity. If an activity has no additional context this field shall be cleared to 0h. Any unused bytes shall be cleared to 0h.

4.8.3.1 TCG Activity Specific Context

This defines the additional command specific context for specific TCG activities ([TCGCE-24](#)).

4.8.3.1.1 Authenticate Method

Requirement ID	Byte Address	Field	# of Bytes	Field Description
TCG-AUTHM-1	69:62	Authority ID	8	The 8-byte UID of the authority on which the authenticate method is being invoked.
TCG-AUTHM-2	70	Tries Count	1	The value of the Tries column of the C_PIN object corresponding to the authority after the authenticate method completes.
TCG-AUTHM-3	71	Reserved	1	Shall be cleared to zero.

4.8.3.1.2 Activate Method

Requirement ID	Byte Address	Field	# of Bytes	Field Description
TCG-ACT-1	62	Range Start Range Length Policy	1	The value of the RangeStartRangeLengthPolicy parameter passed to the Activate method.
TCG-ACT-2	71:63	Reserved	9	Shall be cleared to zero.

4.8.3.1.3 Reactivate Method

Requirement ID	Byte Address	Field	# of Bytes	Field Description
TCG-RACT-1	62	Range Start Range Length Policy	1	The value of the RangeStartRangeLengthPolicy parameter passed to the Reactivate method.
TCG-RACT-2	71:63	Reserved	9	Shall be cleared to zero.

4.8.3.1.4 Assign Method

Requirement ID	Byte Address	Field	# of Bytes	Field Description
TCG-ASGN-1	65:62	Namespace Id	4	The value of the NamespaceId parameter passed to the Assign method.
TCG-ASGN-2	71:66	Reserved	6	Shall be cleared to zero.

4.8.3.1.5 Block SID Authentication Command

Requirement ID	Byte Address	Field	# of Bytes	Field Description
TCG-BSID-1	62	Clear Events	1	The value of the Clear Events parameter passed to the Block SID Authentication command.
TCG-BSID-2	71:63	Reserved	9	Shall be cleared to zero.

4.8.4 DSSD Log Page Requirements

The following table defines the scope for all DSSD specific log pages:

Log Identifier	Scope	Log Page Name	Reference Section
C0h	Controller	SMART / Health Information Extended	4.8.6
C1h	NVM subsystem	Error Recovery	4.8.7
C2h	Obsolete		
C3h	Controller	Latency Monitor	4.8.8

Log Identifier	Scope	Log Page Name	Reference Section
C4h	NVM subsystem	Device Capabilities	4.8.10
C5h	NVM subsystem	Unsupported Requirements	4.8.12
C6h	NVM subsystem	Hardware Component	4.8.13
C7h	NVM subsystem	TCG Configuration	4.8.14
C8h	Reserved for future use		
C9h	NVM subsystem	Telemetry String	4.8.15
CAh	NVM subsystem	Latency Monitor Debug Telemetry	4.8.8

KEY:

- Namespace = The log page contains information about a specific namespace.
- Controller = The log page contains information about the controller that is processing the command.
- NVM subsystem = The log page contains information about the NVM subsystem.

The following table defines the interactions for all DSSD specific log pages with the Format NVM command and sanitize operations:

Requirement ID	Description
GLP-ACC-1	The DSSD log pages to which access is allowed during a Format NVM command or sanitize operations are listed below. Note that this requirement requires vendor-specific log pages to be accessible during a sanitize operation which overrides the requirement in the NVM Express Base Specification to prohibit access to vendor-specific log pages during a sanitize operation:
	DSSD Log Pages
	SMART / Health Information Extended (C0h)
	Error Recovery (C1h)
	Device Capabilities (C4h)
	Unsupported Requirements (C5h)
	Hardware Component (C6h)
	TCG Configuration (C7h)

4.8.5 SMART / Health Information Requirements

The requirements for the SMART / Health Information log page (Log Identifier 02h) and SMART / Health Information Extended log page (Log Identifier C0h) are in [Section 4.8.1 Standard Log Page Requirements](#) and the following table:

Requirement ID	Description
SLOG-1	All values in the DSSD log pages defined by this specification shall be persistent across power cycles unless otherwise specified.

Requirement ID	Description
SLOG-2	All counters defined by this specification shall be saturating counters (i.e., if the counter reaches the maximum allowable size, it stops incrementing and does NOT roll back to 0) unless otherwise specified.
SLOG-3	All fields in DSSD log pages shall be little endian format.
SLOG-4	A normalized counter defined by this specification, unless otherwise specified, shall be reported as the following: 100% shall represent the number at factory exit. 1% shall represent the minimum amount for the device to be reliable. A value of 0% means the device shall no longer be considered reliable. 100% shall be represented as 64h.
SLOG-5	The device shall support all fields in the SMART / Health Information log page.
SLOG-6	A Get Log Page command for either the SMART /Health Information log page (Log Identifier 02h) or SMART / Health Information Extended log page (Log Identifier C0h) shall not require an update of the SMART values other than the temperature values in SLOG-8 . It shall be a simple read of the current data and shall not block I/O.
SLOG-7	Unless otherwise specified, the device shall update the values of the SMART /Health Information log page (Log Identifier 02h) and SMART / Health Information Extended log page (Log Identifier C0h) in the background at least once every ten minutes.
SLOG-8	The composite and raw temperature sensor values shall be updated when the SMART / Health Information log page (Log Identifier 02h) is accessed.
SLOG-9	All assert events and controller-initiated log captures shall have an associated vendor-specific “Reason Identifier” that uniquely identifies the assert /controller condition.
SLOG-10	Obsolete (see STD-LOG-23).
SLOG-11	Obsolete (see STD-LOG-23).
SLOG-12	The device shall not set any bits in the Critical Warning field in the SMART / Health Information log page (Log Identifier 02h) solely due to the value in the Percentage Used field in the SMART/ Health Information log page (Log Identifier 02h).
SLOG-13	The device shall report lifetime energy in the Operational Lifetime Energy Consumed (OLEC) field in the SMART/ Health Information log page (Log Identifier 02h).
SLOG-14	The device shall configure the Interval Power Measurement (IPM) field in the SMART/ Health Information log page (Log Identifier 02h) as follows: • Clear the Power Measurement Type (PMT) to NVM Subsystem (0h). • Configure the Interval Power Measurement Scale (IPMS) field to 10b or 01b to report a scale value. • Report the Interval Power Measurement Value (IPMV) as a non-zero value.

4.8.6 SMART / Health Information Extended Log Page (Log Identifier C0h) Requirements

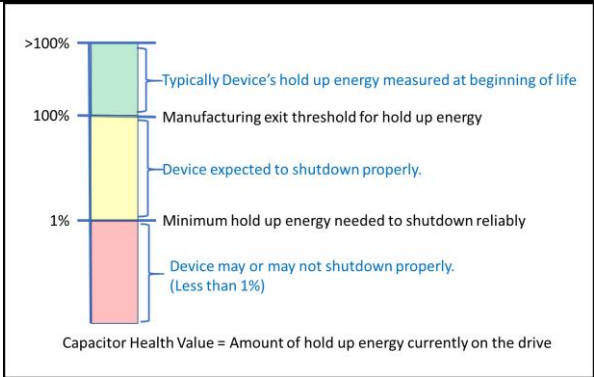
This log page shall be 512 bytes with the following functional requirements and field format:

Requirement ID	Byte Address	Field	# of Bytes	Field Description						
SMART-1	15:0	Physical Media Units Written	16	Shall contain the number of bytes written to the media; this value includes both user and metadata written to the user and system areas. It shall be possible to use this attribute to calculate the Write Amplification Factor (WAF).						
SMART-2	31:16	Physical Media Units Read	16	Shall contain the number of bytes read from the media from both the user and system areas.						
SMART-3	39:32	Bad User NAND Blocks	8	The Raw count specifies the number of user NAND blocks that have been retired for any reason (e.g., program fails, erase fails or other events). The Normalized value is the percentage of user spare blocks still available. The normalized value shall be set to 64h, and the Raw count shall be cleared to zero on factory exit. <table><tr><th>Byte Address</th><th>Byte Description</th></tr><tr><td>39:38</td><td>Normalized value</td></tr><tr><td>37:32</td><td>Raw count</td></tr></table> It should be noted that there are 2 bytes for normalized and 6 bytes for raw count. See SLOG-4 definition above.	Byte Address	Byte Description	39:38	Normalized value	37:32	Raw count
Byte Address	Byte Description									
39:38	Normalized value									
37:32	Raw count									
SMART-4	47:40	Bad System NAND Blocks	8	The Raw count specifies the number of system NAND blocks that have been retired for any reason (e.g., program fails, erase fails or other events). The Normalized value is the percentage of system spare blocks still available. The normalized value shall be set to 64h, and the Raw count shall be cleared to zero on factory exit. It should be noted that there are 2 bytes for normalized and 6 bytes for raw count. See SLOG-4 definition above. <table><tr><th>Byte Address</th><th>Byte Description</th></tr><tr><td>47:46</td><td>Normalized value</td></tr><tr><td>45:40</td><td>Raw count</td></tr></table> A value of FFFF_FFFF_FFFF_FFFFh indicates that the Bad User NAND block count field above represents all blocks on the device and Bad System NAND block count field is invalid.	Byte Address	Byte Description	47:46	Normalized value	45:40	Raw count
Byte Address	Byte Description									
47:46	Normalized value									
45:40	Raw count									

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
SMART-5	55:48	XOR Recovery Count	8	The total number of times XOR was invoked to recover data in NAND. This shall cover all reads from NAND. Data recovery may have succeeded or failed. This shall be cleared to zero on factory exit.	
SMART-6	63:56	Uncorrectable Read Error Count	8	Total count of NAND reads that were not correctable by read retries, all levels of ECC, or XOR. This shall be a count of the number of times data recovery fails and an uncorrectable read error is returned to the host.	
SMART-7	71:64	Soft ECC Error Count	8	Total count of NAND reads that were not correctable by first level ECC and requires invoking additional recovery. This shall cover all NAND read accesses. Data recovery may have succeeded or failed. If the device has more than one recovery level, then this counter only increments once per recovery action.	
SMART-8	79:72	End to End Correction Counts	8	The Detected Error count is a count of the detected errors by the end-to-end error protection mechanisms which includes DRAM, SRAM, or other storage element ECC/CRC protection mechanism (not NAND ECC). The Detected Error counter shall increment on all detected end-to-end errors regardless of if the error is corrected or uncorrectable.	
				Byte Address	Byte Description
				79:76	Corrected Errors
				75:72	Detected Errors
SMART-9	80	System Data % Used	1	A normalized cumulative count of the number of erase cycles per block since leaving the factory for the system (firmware and metadata) area. Starts at 0 and increments. 100 indicates that the estimated endurance has been consumed. Value may exceed 100 up to 255. This count shall increment regardless of what the backing media of the blocks are (e.g., SLC and TLC). If system data is split between media types, then this shall report the worst-case count so that the device wear out is clearly understood. This counter has a different behavior than the normalized counter definition in SLOG-4 , 100% (64h) represents the device may no longer function reliably as the max erase cycles has been hit.	
SMART-10	87:81	Refresh Counts	7	This is a count of the number of blocks that have been re-allocated to maintain data integrity. This counter	

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
				does not include creating free space due to garbage collection or block reallocation due to wear leveling.	
SMART-11	95:88	User Data Erase Counts	8	The maximum count and the minimum erase count across the user NAND blocks in the device. The host shall not be able to reset this counter. It should be noted there are 4 bytes for the maximum and 4 bytes for the minimum. The Minimum User Data Erase Count shall not include bad blocks. If a block goes bad, any subsequent attempts to recover the block shall not increment the Maximum User Data Erase Count field.	
				Byte Address	Byte Description
				95:92	Minimum User Data Erase Count
				91:88	Maximum User Data Erase Count
SMART-12	97:96	Thermal Throttling Status and Count	2	The current status of thermal throttling (throttled or not throttled) and a count of the number of thermal throttling initiation events independent of level. Note that there is 1 byte for the current status and 1 byte for the count. This shall be cleared to zero on factory exit.	
				Byte Address	Byte Description
				97	Current Throttling Status: • 00h = unthrottled • 01h = first level throttle • 02h = 2nd level throttle • 03h = 3rd level throttle • 04h – FFh = Reserved
				96	Number of thermal throttling events
SMART-13	103:98	DSSD Specification Version	6	Version of the DSSD Specification that this device conforms to:	
				Byte Address	Byte Description
				103	Major Version Field. Shall be 02h.
				102:101	Minor Version Field. Shall be 0007h.
				100:99	Point Version Field. Shall be 0000h.
98	Errata Version Field. Shall be 00h.				

Requirement ID	Byte Address	Field	# of Bytes	Field Description
SMART-14	111:104	PCIe Correctable Error Count	8	This field is the summation counter of all PCIe correctable error counters (bad TLP, bad DLLP, receiver error, replay timeouts, replay rollovers) that have occurred over time and as defined in PCIe Error Logging . This count shall only increase during run time. The count shall not increase during training or power fail. The value in this field shall be cleared to zero on factory exit.
SMART-15	115:112	Incomplete Shutdowns	4	A count of the number of shutdowns that have occurred that did not completely flush all required user data and metadata to non-volatile memory for any reason. This shall be cleared to zero on factory exit.
SMART-16	119:116	Reserved	4	Shall be cleared to zero.
SMART-17	120	% Free Blocks	1	This field is the normalized counter of the number of NAND blocks which are currently erased and ready to be written with user data, out of the total number of NAND blocks in the spare area. i.e., this is the percentage of erased NAND blocks in spare area, where the spare area is defined as the NAND blocks that contain no valid user data, no valid system data, and are: • waiting to be erased for use to write user data; or • already erased and ready to be used to write user data. i.e., % Free Blocks = $A / (A + B)$ where A is the number of currently erased NAND blocks and B is the number of NAND blocks waiting to be erased.
SMART-18	127:121	Reserved	7	Shall be cleared to zero.
SMART-19	129:128	Capacitor Health	2	This field is an indicator of the capacitor health and represents the capacitor holdup energy margin during operation. If no PLP protection is present a value of FFFFh shall be reported. 100% represents the passing hold up energy threshold when a device leaves manufacturing. Thus, a device will typically report greater than 100% in this field after leaving manufacturing at the beginning of life. 1% is the minimum hold up energy required to conduct a proper shutdown reliably. A value of 0% may or may not result in a device failing to shut down properly. This value shall never go negative. Zero is the minimum.

Requirement ID	Byte Address	Field	# of Bytes	Field Description
				
SMART-20	130	NVM Express Base Errata Version	1	The device shall report the most recent NVM Express Base Specification Errata revision (a, b, c, etc.) in ASCII that the device has implemented backwards incompatible changes from. If the device does not implement any backwards incompatible changes due to errata, then this field shall be cleared to 0h.
SMART-32	131	NVM Command Set Errata Version	1	The device shall report the most recent NVM Express NVM Command Set Specification errata revision (a, b, c, etc.) in ASCII that the device has implemented backwards incompatible changes from. If the device does not implement any backwards incompatible changes due to errata, then this field shall be cleared to 0h.
SMART-34	132	NVMe over PCIe Transport Errata Version	1	The device shall report the most recent NVM Express NVMe over PCIe Transport Specification errata revision (a, b, c, etc.) in ASCII that the device has implemented backwards incompatible changes from. If the device does not implement any backwards incompatible changes due to errata, then this field shall be cleared to 0h.
SMART-35	133	NVM Express Management Interface Errata Version	1	The device shall report the most recent NVM Express Management Interface Specification errata revision (a, b, c, etc.) in ASCII that the device has implemented backwards incompatible changes from. If the device does not implement any backwards incompatible changes due to errata, then this field shall be cleared to zero.
SMART-30	135:134	Proactive Bad Die Retirement	2	This is a count of the number of dies that were taken offline by the device based on the device predicting that the die will become unusable for any reason. This is a saturating counter.

Requirement ID	Byte Address	Field	# of Bytes	Field Description
SMART-21	143:136	Unaligned I/O	8	This is a count of the number of write IOs performed by the device that are not aligned to the indirection unit size (IU) of the device. Alignment indicates only the start of each IO. The length does not affect this count. This counter shall reset on power cycle. This counter shall not wrap. This shall be cleared to zero on factory exit.
SMART-22	151:144	Security Version Number	8	This is the Security Version Number of the currently running firmware image. The value of this field shall be 0h for the initial release of firmware. The vendor shall increment this field by one any time a firmware includes a fix for a security issue or critical firmware fix that customer agrees rollback prevention is required.
SMART-23	159:152	Total NUSE	8	Total Namespace Utilization. For a device with a single Namespace, this shall be a copy of the Namespace Utilization (NUSE) field defined in the Identify Namespace Data Structure bytes 23:16. For a device with multiple Namespaces, this shall reflect the total utilization based on all the Namespaces.
SMART-24	175:160	PLP Start Count	16	This is a count of the number of times the device has initiated its power loss protection process due to supply voltage drop. This counter shall be incremented on the initial detection of the power loss condition. This does not include PLP health check operations.
SMART-25	191:176	Endurance Estimate	16	This field is an estimate of the total number of data bytes that may be written to the device over its lifetime assuming a write amplification of 1 (i.e., no increase in the number of write operations performed by the device beyond the number of write operations requested by a host). This value shall be equivalent to the Endurance Estimate field in the Endurance Group log page (Log Identifier 09h) but shall be in units of bytes.
SMART-29	199:192	PCIe Link Retraining Count	8	This is a count of the number of PCIe Link Retraining events (including link speed and link width changes). This count shall only increase while CC.EN=1. It shall not increase during training due to resets or power cycles. This shall be cleared to zero on factory exit.
SMART-31	207:200	Power State Change Count	8	Summation counter of the number of NVMe Power State changes whether host or device initiated, including NVMe Power State changes caused by DSSD Power State changes (see Section 4.8.11 DSSD Power State

Requirement ID	Byte Address	Field	# of Bytes	Field Description
				Requirements). This count shall only increase during run time. This shall be cleared to zero on factory exit.
SMART-33	215:208	Lowest Permitted Firmware Revision	8	This field indicates the value of the Firmware Revision field of the lowest firmware revision that is permitted to be rolled back to. If the currently running firmware image permits rollback to all prior firmware revision, then this field shall be cleared to 0h. If the currently running firmware image does not permit rollback to all prior firmware revisions, then this field shall indicate the value of the Firmware Revision field of the lowest firmware revision that has a Firmware Security Version equal to the Firmware Security Version of the currently running firmware image.
SMART-36	217:216	Total Media Dies	2	This field is the total number of media dies in the device.
SMART-37	219:218	Media Die Failure Tolerance	2	This field is the number of flash dies that are allowed to fail, and the device will continue to operate.
SMART-38	221:220	Media Dies Offline	2	This is a count of the number of media dies permanently offline (retired).
SMART-39	222	Max Temperature Recorded	1	This value shall report the highest composite temperature value recorded over the life of the device in degrees Celsius.
SMART-40	223	Form Factor	1	The device shall provide the Form Factor (FF) field in the NVMe MultiRecord Area in this byte as described in the NVM Express Management Interface Specification version 2.1 and TP6041 for E2.
SMART-41	231:224	NAND Avg. Erase Count	8	Average erase count of all flash blocks across entire device.
SMART-42	235:232	Command Timeouts	4	This is a count of the number of times a command with the limited retry (LR) bit set has exceeded the TLER value. This is a saturating count.
SMART-43	243:236	System Area Program Fail Count	8	The Raw count specifies the number of program failures in the system area. The Normalized value is the percentage of remaining allowable failures. The first four bytes shall be the raw value, the fifth byte the normalized value, and the last 3 bytes are reserved.

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
				Byte Address	Byte Description
				243:241	Reserved
				240	Normalized value
				239:236	Raw count
SMART-44	251:244	System Area Uncorrectable Read Count	8	The Raw count specifies the number of read failures (Uncorrectable Reads) in the system area. The Normalized value is the percentage of remaining allowable failures. The first four bytes shall be the raw value, the fifth byte the normalized value, and the last 3 bytes are reserved.	
				Byte Address	Byte Description
				251:249	Reserved
				248	Normalized value
SMART-45	259:252	System Area Erase Fail Count	8	The Raw count specifies the number of erase failures in the system area. The Normalized value is the percentage of remaining allowable failures. The first four bytes shall be the raw value, the fifth byte the normalized value, and the last 3 bytes are reserved.	
				Byte Address	Byte Description
				259:257	Reserved
				256	Normalized value
SMART-46	261:260	Max Peak Power Capability	2	The maximum peak power that the device is capable of measured in Watts over a 100 μ s window with a sampling interval of 4 μ s or smaller (see PCM-2). This is a static value based on the PS0 worst case.	
				255:252	Raw count
SMART-47	263:262	Current Average Power	2	The current device Average Power in Watts measured over a 1 second window with a recommended sampling rate of 2 ms or smaller. The sampling rate used shall be the same as reported in the Interval Power Measurement Sample Rate field. The value in this field shall be measured with the same methodology as the	

Requirement ID	Byte Address	Field	# of Bytes	Field Description
				value reported in the Interval Power Measurement field in SMART/Health Informational Log Page.
SMART-48	269:264	Lifetime Power Consumed	6	The total cumulative power consumed by the device in kWh based on the Current Average Power. This field shall be cleared to 0h from the factory. This is a saturating counter. The value in this field shall be measured with the same methodology as the value reported in the Operational Lifetime Consumed (OLEC) field in SMART/Health Informational Log Page.
SMART-49	277:270	DSSD Firmware Revision	8	The DSSD Firmware Revision field shall have the following format: <Major Revision>.<Minor Revision>.<Release Revision> where: • each sub-revision field (i.e., <Major Revision>, <Minor Revision>, and <Release Revision>) shall be a base-ten integer in the range 0 to 99, represented in ASCII; • the most significant sub-revision field (i.e., <Major Revision>) shall be on left; • each sub-revision field shall be separated by a period (ASCII 2Eh); • each sub-revision field of lesser significance shall reset to "0" (ASCII 30h) when a more significant sub-revision field increments (e.g., the next <Major Revision> release after 1.2.3 would be 2.0.0 and the next <Minor Revision> release after 1.2.3 would be 1.3.0); • the Firmware Revision field shall not contain padding of any kind at the start or in the middle of the string (e.g., zeroes or spaces); and • if the Firmware Revision field is less than 8 characters, then the Firmware Revision field shall be padded with spaces at the end of the string per the NVM Express Base Specification. Examples of legal values shown inside quotes: • "1.2.3 " (3 trailing spaces to make it 8 bytes) • "10.1.12 " (1 trailing space to make it 8 bytes) Examples of illegal values shown inside quotes: • "1.02.03" (leading zero before 2 and 3 is not allowed) • "1. 2. 3" (space before 2 and 3 is not allowed) • " 1.2.3" (space at start of string is not allowed)

Requirement ID	Byte Address	Field	# of Bytes	Field Description
				“1.2” (must have all three parts of the revision) Pre-production firmware shall have a <Major Revision> of “0”. The first production release of firmware shall have a <Major Revision> of “1”. The <Major Revision> shall be incremented by one whenever a major change is made to the firmware. Examples of major changes include: - the Security Firmware Revision is incremented; - major feature enhancements; - major architectural changes to the firmware code base; and - addition of support for major hardware changes. The first production release of firmware shall have a <Minor Revision> of “0”. The <Minor Revision> shall be incremented by one when only a minor change is made to the firmware. Examples of minor changes include: - minor feature enhancements; - performance enhancements; and - multiple bug fixes that, in aggregate, justify more than an increment to the <Release Revision>. The <Release Revision> shall be incremented by one for each firmware revision.
SMART-50	293:278	DSSD Firmware Build UUID	16	This field shall contain a UUID in the format specified for UUIDs by the NVM Express Base Specification that is unique for each firmware build.
SMART-51	357:294	DSSD Firmware Build Label	64	This field may contain a descriptive label for the firmware that provides additional information about the purpose of this revision of the firmware. For example, this field may be used for test or debug builds to describe the scope of the build. Examples: - Workaround for issue 12345 - Experimental new feature XYZ If a descriptive label is provided, then the label shall adhere to the rules for ASCII strings as defined by the NVM Express Base Specification; otherwise, this field shall be cleared to 0h.
SMART-52	365:358	Dies In Use Bad NAND Blocks	8	The Raw count specifies the number of NAND blocks that have been retired for any reason from the dies currently in use. (e.g., program fails, erase fails, etc.). Blocks in dies that have been taken offline (i.e., no

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
				longer used in the device) shall not be counted. The normalized value is the percentage of usable spare blocks still available. The normalized value shall be set to 64h, and the Raw count shall be cleared to zero on factory exit. It should be noted that there are 2 bytes for normalized and 6 bytes for raw count. See SLOG-4 definition above.	
				Byte Address	Byte Description
				47:46	Normalized value
				45:40	Raw count
				These values may decrease due to a die being marked as bad and going offline (See SMART-38).	
SMART-26	493:366	Reserved	128	Shall be cleared to zero.	
SMART-27	495:494	Log Page Version	2	This indicates the version of the mapping this log page uses. Shall be set to 0006h.	
SMART-28	511:496	Log Page GUID	16	Shall be set to AFD514C97C6F4F9CA4F2BFEA2810AFC5h.	

4.8.7 Error Recovery and the Error Recovery Log Page (Log Identifier C1h)

The requirements for the Error Recovery log page (Log Identifier C1h) log page are in the following tables:

Requirement ID	Description
EREC-AEN-1	Obsolete. Replaced by DSSD-AEN-1 .

4.8.7.1 Error Recovery Theory of Operations

Error Recovery Workflow using Asynchronous Event Notifications:

Requirement ID	Description
EREC-FUNC-1	The device shall make every attempt to transparently recover from errors without invoking any of the Error Recovery workflows described in the following tables.

Error Recovery Workflow – AEN with in-band recovery:

#	Task	Description
Pre-Failure Parameter Exchange		
1	Boot time controller initialization	During boot time controller initialization, the host reads the Error Recovery log page (Log Identifier C1h) and caches the Error Reset Wait Time and the Error Reset Action bitfield. The host also sends an Asynchronous Event

#	Task	Description
		Request (AER) command to device and waits for the device to complete the command when there is an asynchronous event.
Re-Establishing Communication When Failure Occurs		
2	Device hits error condition	The device detects error condition
3	Device saves error related data	The device saves the following information: • Error ID • Device Recovery Actions • Debug data for the Telemetry Controller-Initiated log page (Log Identifier 08h)
4	Device generates AEN*	The device generates the AEN to let the host know that an error was detected and then starts its error handling workflow. The device is not required to handle any NVMe command(s) sent via the Admin Submission Queue after sending the AEN. It is strongly recommended that the device continues to service commands sent via the out-of-band mechanism, if possible. The AEN Completion Queue Entry Dword 0 is filled in per DSSD-AEN-1. If the device is unable to send the AEN to the host (e.g., the Admin CQ is not usable), and If the device supports the CFS in-band error recovery workflow, then the device saves the AEN information and asserts CSTS.CFS and starts the CFS-based recovery workflow at step 4. If the device does not support the CFS-based recovery workflow, then the host falls back to the recovery functionality specified in the Controller Fatal Status Condition paragraph of the Error Reporting and Recovery section of the NVMe Base Specification (i.e., Controller Reset followed by an NVM Subsystem Reset if the Controller Reset does not recover). If the device recovers, the device waits for the host to send an AER and then completes the AEN using the previously saved AEN information and resumes this in-band error recovery workflow.
5	Host AEN handling	The host services the AEN and logs an event for the error condition.
6	Host waits for device error handling to complete	The host waits for Error Reset Wait Time to allow the device to finish its error handling workflow.
Extracting Debug Information After Failure and Recovery		
7	Host recovers device	The host tries one or more of the resets specified in the Error Reset Action bitfield to attempt to bring the device back to a state where it can service NVMe commands.
8	Host initiates controller initialization	The host starts controller initialization. If the controller fails to initialize, the host will attempt the next Error Reset Action as specified in the Error Reset Action bitfield.

#	Task	Description
9	Host reads the Error Recovery log page (Log Identifier C1h)	The host reads the Error Recovery log page (Log Identifier C1h) to retrieve the following information: • Last Error ID • Device Recovery Actions If the device is still in error mode, the device fails I/O commands if it cannot safely complete commands: • Status Code (SC) = 06h (Internal Error) • Status Code Type (SCT) = 00h (Generic Command Status)
10	Host retrieves Controller-Initiated Telemetry Log if device in error mode	Host retrieves Telemetry Controller-Initiated log page (Log Identifier 08h) for later use in debugging.
11	Device Recovery	The recommended Device Recovery Actions are taken. This is done during the offline recovery workflow.

Error Recovery Workflow – CFS with in-band recovery:

#	Task	Description
Pre-Failure Parameter Exchange		
1	Boot time controller initialization	During boot time controller initialization, driver reads the Error Recovery log page (Log Identifier C1h) and caches Error Reset Wait Time and Error Reset Action. Driver also saves information that Error CFS Supported is set.
Re-Establishing Communication When Failure Occurs		
2	Device hits error condition	Device detects error condition
3	Device saves error related data	Device saves the following information: • Error ID • Device Recovery Actions • Debug data for the Telemetry Controller-Initiated log page (Log Identifier 08h)
4	Device asserts CFS	Device asserts CFS to let host know that an error was detected and starts error handling workflow. Device is not expected to be able to handle any NVMe command(s) sent via the Admin Submission Queue after asserting CFS. It is strongly recommended that the device continues to service commands sent via the out-of-band mechanism, if possible.
5	Driver detects CFS after command timeout	On first command timeout after CFS bit is set, driver will check and detect CFS bit is set.
6	Driver waits for device error handling to complete	The driver waits for Error Reset Wait Time to allow the device to finish its error handling workflow.
Extracting Debug Information After Failure and Recovery		

#	Task	Description
7	Driver initiates a NVMe Controller Reset	The driver initiates an NVMe Controller Reset as recommended in the NVM Express Base Specification for CFS.
8	Driver resets device if NVMe Controller Reset fails	If prior NVMe Controller Reset fails, driver tries one or more resets specified in Error Reset Action to attempt to bring device back to a state that can service NVMe command(s).
9	Driver initiates controller initialization	Driver starts controller initialization. If controller fails to initialize, driver may attempt a different Error Reset Action.
10	Driver reads the Error Recovery log page (Log Identifier C1h)	Driver reads the Error Recovery log page (Log Identifier C1h) to retrieve the following information: • Last Error ID • Device Recovery Actions If the device is still in error mode, the device fails I/O commands if it cannot safely complete commands: • Status Code (SC) = 06h (Internal Error) • Status Code Type (SCT) = 0h (Generic Command Status)
11	Driver retrieves the Telemetry Controller-Initiated log page (Log Identifier 08h) if device in error mode	Driver retrieves the Telemetry Controller-Initiated log page (Log Identifier 08h) for sharing with IHV.
12	Device Recovery	The recommended Device Recovery Actions are taken. This is done during the offline recovery workflow.

4.8.7.2 Error Recovery Log Page (Log Identifier C1h) Requirements

This vendor-specific log page, C1h shall be 512 bytes with the following functional requirements and field format:

Requirement ID	Byte Address	Field	# of Bytes	Field Description
EREC-1	1:0	Error Reset Wait Time	2	The amount of time the host should wait for the device error workflow to complete in msec.
EREC-2	2	Error Reset Action	1	Bit field indicating potential reset actions that may need to be taken. If no reset action is needed, do not set any of the bits. More than 1 bit can be set, and it is up to the host to decide the sequence of action(s) to take. Instead of asserting and requiring the host to perform an NVMe Controller Reset to clear the assert condition, the device should reset itself using a methodology similar to what is used to perform a firmware activation without reset (e.g., pause command processing, set the Processing Paused bit to 1b, save current state, re-initialize firmware, restore saved state, resuming

Requirement ID	Byte Address	Field	# of Bytes	Field Description																
				processing, clear the Processing Paused bit to 0b). The device shall increment the Error Count field (see EREC-16) and shall log this event in the telemetry logs and include a vendor specific error code in the Error ID (see TELRI-1) whether or not it can autonomously recover. If autonomous recovery is not possible, then the assert condition shall be reported to the host (see EREC-5). The strongly preferred order of device advertised recovery is bit 0, 1, 2, 5, 3 then 4 which is based on least impactful to most impactful from a host perspective. <table><tr><th>Bit</th><th>Bit Description</th></tr><tr><td>7:6</td><td>Reserved. Shall be cleared to zero.</td></tr><tr><td>5</td><td>PCIe Conventional Hot Reset.</td></tr><tr><td>4</td><td>Main Power Cycle.</td></tr><tr><td>3</td><td>PERST#.</td></tr><tr><td>2</td><td>PCIe Function Level Reset.</td></tr><tr><td>1</td><td>NVM Subsystem Reset.</td></tr><tr><td>0</td><td>NVMe Controller Reset.</td></tr></table>	Bit	Bit Description	7:6	Reserved. Shall be cleared to zero.	5	PCIe Conventional Hot Reset.	4	Main Power Cycle.	3	PERST#.	2	PCIe Function Level Reset.	1	NVM Subsystem Reset.	0	NVMe Controller Reset.
Bit	Bit Description																			
7:6	Reserved. Shall be cleared to zero.																			
5	PCIe Conventional Hot Reset.																			
4	Main Power Cycle.																			
3	PERST#.																			
2	PCIe Function Level Reset.																			
1	NVM Subsystem Reset.																			
0	NVMe Controller Reset.																			
EREC-3	3	Device Recovery Action 1	1	The recovery action to take for handling a device error condition. Value is dependent on the error condition. The device shall set bit 0 to 1b if data integrity is intact. The device shall set bit 6 to 1b if the data integrity of some of the LBAs is compromised. The device shall only set bit 1, bit 2 or bit 5 to 1b if the data integrity of all of the LBAs is compromised. The device shall only set bit 3 to 1b or bit 4 to 1b if there is a persistent hardware failure. The device shall not set more than one bit to one in this field. If multiple recovery actions are possible, the device shall select the most effective recovery action to report in this field. <table><tr><th>Bit</th><th>Bit Description</th></tr><tr><td>7</td><td>Reserved. Shall be cleared to zero.</td></tr><tr><td>6</td><td>Device error has caused user data loss. The device shall populate LBA Status Information log page (Log Identifier 0Eh) with all of the lost/corrupted LBAs. If the device sets this bit to 1b, then the device shall also set at least one bit to 1b in Device Recovery Action 2, see EREC-14.</td></tr></table>	Bit	Bit Description	7	Reserved. Shall be cleared to zero.	6	Device error has caused user data loss. The device shall populate LBA Status Information log page (Log Identifier 0Eh) with all of the lost/corrupted LBAs. If the device sets this bit to 1b, then the device shall also set at least one bit to 1b in Device Recovery Action 2, see EREC-14.										
Bit	Bit Description																			
7	Reserved. Shall be cleared to zero.																			
6	Device error has caused user data loss. The device shall populate LBA Status Information log page (Log Identifier 0Eh) with all of the lost/corrupted LBAs. If the device sets this bit to 1b, then the device shall also set at least one bit to 1b in Device Recovery Action 2, see EREC-14.																			

Requirement ID	Byte Address	Field	# of Bytes	Field Description									
				5	Sanitize Required.								
				4	Device Replacement Required.								
				3	Vendor Physical Analysis Required.								
				2	Vendor Specific Command Required.								
				1	Format NVM Required (Any SES value, any supported combination of other parameters – PIL, PI, MSET, LBAF).								
				0	No Action Required.								
EREC-4	11:4	Error ID	8	A numeric value that uniquely identifies the exact error condition encountered. A value of zero indicates no error. The following Error ID values are reserved for Host defined fault codes for known error conditions: 00000000_00000000h – 00000000_0000FFFFh <table><tr><th>Byte Address</th><th>Byte Description</th></tr><tr><td>11:4</td><td> Error ID definition: 00000000_00000001h – Error caused by flush failures or data loss during power loss handling. </td></tr></table>		Byte Address	Byte Description	11:4	Error ID definition: 00000000_00000001h – Error caused by flush failures or data loss during power loss handling.				
Byte Address	Byte Description												
11:4	Error ID definition: 00000000_00000001h – Error caused by flush failures or data loss during power loss handling.												
EREC-5	15:12	Device Capabilities	4	Field to indicate device capabilities: <table><tr><th>Bit</th><th>Bit Description</th></tr><tr><td>31:2</td><td>Reserved: Shall be cleared to zero.</td></tr><tr><td>1</td><td>Error CFS Supported: If set, indicates device supports using CFS to notify host of an error condition¹.</td></tr><tr><td>0</td><td>Error Reporting AEN Supported: If set, indicates device supports using AEN to notify the host of an error condition¹.</td></tr></table> Note(s): It is valid for a device to indicate support for both Error Reporting AEN Supported and Error Controller Fatal Status Supported. If the device supports both, the device shall only use one of these in-band error notification mechanisms when reporting a given error event as		Bit	Bit Description	31:2	Reserved: Shall be cleared to zero.	1	Error CFS Supported: If set, indicates device supports using CFS to notify host of an error condition ¹ .	0	Error Reporting AEN Supported: If set, indicates device supports using AEN to notify the host of an error condition ¹ .
Bit	Bit Description												
31:2	Reserved: Shall be cleared to zero.												
1	Error CFS Supported: If set, indicates device supports using CFS to notify host of an error condition ¹ .												
0	Error Reporting AEN Supported: If set, indicates device supports using AEN to notify the host of an error condition ¹ .												

Requirement ID	Byte Address	Field	# of Bytes	Field Description																
				configured in the DSSD Asynchronous Event Configuration Feature (see SDAEC-14).																
EREC-6	16	Vendor Specific Recovery Opcode	1	Vendor-specific command opcode to recover device from the error condition. Only valid when bit 2 of the Device Recovery Action 1 field value is set to 1b. When bit 2 of the Device Recovery Action 1 field value is cleared to 0b, this field shall be cleared to zero.																
EREC-7	19:17	Reserved	3	Shall be cleared to zero.																
EREC-8	23:20	Vendor Specific Command CDW12	4	CDW12 value for the Vendor Specific command to recover device from the error condition. Only valid when bit 2 of the Device Recovery Action 1 field is set to 1b. When bit 2 of the Device Recovery Action 1 field value is cleared to 0b, this field shall be cleared to zero.																
EREC-9	27:24	Vendor Specific Command CDW13	4	CDW13 value for the Vendor Specific command to recover device from the error condition. Only valid when bit 2 of the Device Recovery Action 1 field value is set to 1b. When Device Recovery Action 1 field value is cleared to 0b, this field shall be cleared to zero.																
EREC-13	28	Vendor Specific Command Timeout	1	The amount of time the host should wait for the device to complete the recovery command in seconds.																
EREC-14	29	Device Recovery Action 2	1	Bit field indicating potential post reset actions that may need to be taken. If no reset action is needed, do not set any of the bits. More than 1 bit can be set, and it is up to the host to decide the sequence of action(s) to take. Use Bit 0 if possible. If Bit 0 is not possible then use Bit 1, etc.																
				<table><tr><th>Bit</th><th>Bit Description</th></tr><tr><td>7:6</td><td>Reserved. Shall be cleared to zero.</td></tr><tr><td>5</td><td>PCIe Conventional Hot Reset.</td></tr><tr><td>4</td><td>Main Power Cycle.</td></tr><tr><td>3</td><td>PERST#.</td></tr><tr><td>2</td><td>PCIe Function Level Reset.</td></tr><tr><td>1</td><td>NVM Subsystem Reset.</td></tr><tr><td>0</td><td>NVMe Controller Reset.</td></tr></table>	Bit	Bit Description	7:6	Reserved. Shall be cleared to zero.	5	PCIe Conventional Hot Reset.	4	Main Power Cycle.	3	PERST#.	2	PCIe Function Level Reset.	1	NVM Subsystem Reset.	0	NVMe Controller Reset.
				Bit	Bit Description															
				7:6	Reserved. Shall be cleared to zero.															
				5	PCIe Conventional Hot Reset.															
				4	Main Power Cycle.															
				3	PERST#.															
				2	PCIe Function Level Reset.															
1	NVM Subsystem Reset.																			
0	NVMe Controller Reset.																			

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
EREC-15	30	Device Recovery Action 2 Timeout	1	The amount of time the host should wait for the device to complete the Device Recovery Action 2 in seconds (overrides CAP.TO value).	
EREC-16	31	Error / Assert Count	1	The number of Errors the device has encountered during its lifetime. This is a saturating counter.	
EREC-17	63:32	Previous Error IDs	32	This set of fields reports the four most recent Error IDs not including the ID of the current error.	
				Byte Address	Byte Description
				39:32	Error ID N-1
				47:40	Error ID N-2
				55:48	Error ID N-3
63:56	Error ID N-4				
EREC-10	493:64	Reserved	430	Shall be cleared to zero.	
EREC-11	495:494	Log Page Version	2	This indicates the version of the mapping this log page uses. Shall be set to 0003h.	
EREC-12	511:496	Log Page GUID	16	Shall be set to 5A1983BA3DFD4DABAE3430FE2131D944h.	

4.8.8 Latency Monitor Log Page and Feature Set Requirements

The following are requirements for the Latency Monitor log page and Latency Monitor Feature Set. For more information about the Latency Monitoring Feature Set (see [Section 22 Latency Monitoring Feature Set Theory of Operation](#)).

Requirement ID	Description
LMLOG-1	All values in the Latency Monitor log page shall be persistent across power cycles and resets unless otherwise specified.
LMLOG-2	All counters shall be saturating counters (i.e., if the counter reaches the maximum allowable size, it stops incrementing and does NOT roll back to 0).
LMLOG-3	All values in the Latency Monitor log page shall be little endian format.
LMLOG-4	A read of the Latency Monitor log page shall be a simple read of the active data and shall not block IO.
LMLOG-5	Data in the Latency Monitor log page which is read by the host shall be no more than 10 minutes old.
LMLOG-6	When configuring the Latency Monitoring Feature with Set Features the Active Buckets and Static Buckets shall be reset.

Requirement ID	Description
LMLOG-7	When powering on, the counters shall run based on the previously configured values. If the values have never been configured, they shall run based on the default values.
LMLOG-8	The Latency Stamp shall be based on the NVMe timestamp set by the last Timestamp (Feature 0Eh) Set Features command if any. If a NVMe Timestamp (Feature 0Eh) Set Features command has not been received, then the Latency Stamp shall be based on the device power on hours.
LMLOG-9	When the device provides a Latency Stamp of latency outliers, the Latency Stamp shall be based on command completion.
LMLOG-10	When generating a Latency Monitoring log page (Feature Identifier C5h), the latency shall be no greater than the latency associated with generating a Telemetry Controller-Initiated log page (Feature Identifier 08h) or a Telemetry Host-Initiated log page (Feature Identifier 07h).
LMLOG-11	When configuring this feature, the thresholds shall always be configured such that Active Threshold A < Active Threshold B < Active Threshold C < Active Threshold D. If the host attempts to configure the device in such a way that violates the above rules, the device shall return Invalid Field in Command.
LMLOG-12	The device shall support the Latency Monitoring Feature Set.
LMLOG-13	The Latency Monitor Log page shall be 512 bytes.
LMLOG-14	Executing a Set Features command for Latency Monitor log page (Feature Identifier C5h) shall reset all the contents in the Active/Static Buckets.
LMLOG-15	If the Host Initiated Telemetry Format Supported bit is set to 1b (see LMDATA-1) then the Latency Monitor Debug Telemetry Log (CAh) shall follow: • The Host-Initiated Telemetry Log Format as defined NVM Express. • Telemetry Data Area 1, Data Area 2, Data Area 3 and Data Area 4 format as defined in this specification.
LMLOG-16	If the Host Initiated Telemetry Format Supported bit is set to 1b (see LMDATA-1) then the Latency Monitor Debug Telemetry Log page (CAh) shall only be cleared with Latency Monitor Set Features (C5h). See section 4.15.11.
LMLOG-17	If the Host Initiated Telemetry Format Supported bit is set to 1b, then there shall be no limits on the size of Data Area 1, 2, 3 or 4 beyond the NVM Express-defined limits. The Data Area size and performance limits in TEL-5 do not apply to the log in the Latency Monitor Debug Log page (Log Identifier CAh).
LMLOG-18	If the Host Initiated Telemetry Format Supported bit is set to 1b then the following bytes in the Latency Monitor Debug log page (Log Identifier CAh) shall be configured as shown: • Byte 00: Log Page Identifier (LID) shall be set to CAh. • Byte 380: Telemetry Host-Initiated Scope (THS) shall be set to 01h (Controller Scope).

4.8.9 Latency Monitor Log Page (Log Identifier C3h) Requirements

This log page shall be 512 bytes with the following functional requirements and field format (see [Section 22 Latency Monitoring Feature Set Theory of Operation](#) for additional details):

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
LMDATA-1	0	Latency Monitor Feature Status	1	Bit	Bit Description
				7:4	Reserved. Shall be cleared to zero.
				3	Host Initiated Telemetry Format Supported. When set to 1b the format of the Latency Monitor Debug Telemetry Log follows the Host Initiated Telemetry Log format. When cleared to 0b the Latency Monitor Debug Telemetry Log data format is not specified.
				2	Active Measured Latency Supported. When set to 1b the Active Measured Latency field is supported and shall be populated based on the Active Latency Configuration settings. When cleared to 0b the Active Measured Latency is not supported.
				1	Active Latency Configuration/Active Latency Mode 1 Supported. When set to 1b the device shall support the Active Latency Configuration with the Active Latency Mode = 1b. When cleared to 0b the device does not support Active Latency Mode =1b.
				0	Latency Monitoring Feature Enabled. This is a global feature enable. When set to 1b the Latency Monitoring Feature for this device is enabled. When cleared to 0b all features in the Latency Monitoring Log page are disabled for this device and can be ignored. When cleared to 0b the other fields in this log page are not power loss safe and may be lost.
The default value shall be 07h.					
LMDATA-2	1	Reserved	1	Shall be cleared to zero.	
LMDATA-3	3:2	Active Bucket Timer	2	The Active Bucket Timer is in 5-minute increments. Thus, a value of 0001h is 5 minutes and a value of 0002h is 10 minutes. This represents the amount of time the Active Buckets have been accumulating data. The Active	

Requirement ID	Byte Address	Field	# of Bytes	Field Description
				Bucket Timer will saturate at FFFFh. When the Active Bucket Timer reaches the Active Bucket Timer Threshold then the data specified in Section 22 Latency Monitoring Feature Set Theory of Operation is moved into the Static Buckets, the Active Bucket Timer is cleared to 0000h and restarts counting. If the Active Bucket Timer is running and there is a power cycle the Active Bucket Timer value from before the power cycle shall be restored into the Active Bucket Timer and the Active Bucket Timer shall continue when the device is powered on.
LMDATA-4	5:4	Active Bucket Timer Threshold	2	Active Bucket Timer Threshold is the threshold used to compare with the Active Bucket Timer. When cleared to 0000h this threshold is not used, the Active Bucket Timer will saturate, and the Static Buckets will not be loaded. This threshold is in 5-minute increments. The factory default value of the Active Bucket Timer Threshold shall be set to 07E0h.
LMDATA-5	6	Active Threshold A	1	This defines Active Threshold A. This is in 5 ms increments. A value of 00h represents 5 ms. The value FFh represents 1.280 seconds. The factory default is 05h.
LMDATA-6	7	Active Threshold B	1	This is in 5 ms increments. The factory default is 13h.
LMDATA-7	8	Active Threshold C	1	This is in 5 ms increments. The factory default is 1Eh.
LMDATA-8	9	Active Threshold D	1	This is in 5 ms increments. The factory default is 2Eh.
LMDATA-9	11:10	Active Latency Configuration	2	This configures how both the Active Latency Stamp, and the Active Measured Latency Fields are updated on a per I/O command (Read, Write, Deallocate) counter basis. When the Active Latency Mode is cleared to 0b the Active Latency Stamp and the Active Measured Latency will trigger and update the first time the associated command counter increments. Once this trigger happens the fields shall not be updated until the Active Latency Stamp and Active Measured Latency fields are reset based on the Active Bucket Timer expiring. When the Active Latency Mode is set to 1b the Active Latency Stamp and the Active Measured Latency fields

Requirement ID	Byte Address	Field	# of Bytes	Field Description																																																								
				shall update to show the largest measured latency based on the associated command counter.																																																								
				<table><tr><th>Bit</th><th>Bucket</th><th>Counter</th><th>Description</th></tr><tr><td>15:12</td><td>N/A</td><td>N/A</td><td>Reserved. Shall be cleared to zero.</td></tr><tr><td>11</td><td>3</td><td>Deallocate/TRIM</td><td>Active Latency Mode [11]</td></tr><tr><td>10</td><td>3</td><td>Write</td><td>Active Latency Mode [10]</td></tr><tr><td>9</td><td>3</td><td>Read</td><td>Active Latency Mode [9]</td></tr><tr><td>8</td><td>2</td><td>Deallocate/TRIM</td><td>Active Latency Mode [8]</td></tr><tr><td>7</td><td>2</td><td>Write</td><td>Active Latency Mode [7]</td></tr><tr><td>6</td><td>2</td><td>Read</td><td>Active Latency Mode [6]</td></tr><tr><td>5</td><td>1</td><td>Deallocate/TRIM</td><td>Active Latency Mode [5]</td></tr><tr><td>4</td><td>1</td><td>Write</td><td>Active Latency Mode [4]</td></tr><tr><td>3</td><td>1</td><td>Read</td><td>Active Latency Mode [3]</td></tr><tr><td>2</td><td>0</td><td>Deallocate/TRIM</td><td>Active Latency Mode [2]</td></tr><tr><td>1</td><td>0</td><td>Write</td><td>Active Latency Mode [1]</td></tr><tr><td>0</td><td>0</td><td>Read</td><td>Active Latency Mode [0]</td></tr></table>	Bit	Bucket	Counter	Description	15:12	N/A	N/A	Reserved. Shall be cleared to zero.	11	3	Deallocate/TRIM	Active Latency Mode [11]	10	3	Write	Active Latency Mode [10]	9	3	Read	Active Latency Mode [9]	8	2	Deallocate/TRIM	Active Latency Mode [8]	7	2	Write	Active Latency Mode [7]	6	2	Read	Active Latency Mode [6]	5	1	Deallocate/TRIM	Active Latency Mode [5]	4	1	Write	Active Latency Mode [4]	3	1	Read	Active Latency Mode [3]	2	0	Deallocate/TRIM	Active Latency Mode [2]	1	0	Write	Active Latency Mode [1]	0	0	Read	Active Latency Mode [0]
				Bit	Bucket	Counter	Description																																																					
				15:12	N/A	N/A	Reserved. Shall be cleared to zero.																																																					
				11	3	Deallocate/TRIM	Active Latency Mode [11]																																																					
				10	3	Write	Active Latency Mode [10]																																																					
				9	3	Read	Active Latency Mode [9]																																																					
				8	2	Deallocate/TRIM	Active Latency Mode [8]																																																					
				7	2	Write	Active Latency Mode [7]																																																					
				6	2	Read	Active Latency Mode [6]																																																					
				5	1	Deallocate/TRIM	Active Latency Mode [5]																																																					
				4	1	Write	Active Latency Mode [4]																																																					
				3	1	Read	Active Latency Mode [3]																																																					
				2	0	Deallocate/TRIM	Active Latency Mode [2]																																																					
				1	0	Write	Active Latency Mode [1]																																																					
				0	0	Read	Active Latency Mode [0]																																																					
The default value shall be 0FFh.																																																												
LMDATA-10	12	Active Latency Minimum Window	1	This is the minimum number of 100 ms increments between Latency Events for a single Active Latency Stamp and Active Measured Latency. When cleared to 00h this feature is disabled. This count is in 100 ms increments, thus a value of 01h is 100 ms and 02h is 200 ms. Once a Latency Stamp/Measured Latency is updated if the Active Latency Minimum Window time																																																								

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
				has not expired and an event that is configured to generate a Latency Stamp/Measured Latency occurs the Latency Stamp/Measured Latency will not be recorded. The default value of this field is 0Ah.	
LMDATA-11	31:13	Reserved	19	Shall be cleared to zero.	
LMDATA-12	47:32	Active Bucket Counter 0	16	Byte Address	Byte Description
				47:44	Read Command Counter.
				43:40	Write Command Counter.
				39:36	Deallocate/TRIM Command Counter.
				35:32	Reserved. Shall be cleared to zero.
LMDATA-13	63:48	Active Bucket Counter 1	16	Byte Address	Byte Description
				63:60	Read Command Counter.
				59:56	Write Command Counter.
				55:52	Deallocate/TRIM Command Counter.
				51:48	Reserved. Shall be cleared to zero.
LMDATA-14	79:64	Active Bucket Counter 2	16	Byte Address	Byte Description
				79:76	Read Command Counter.
				75:72	Write Command Counter.
				71:68	Deallocate/TRIM Command Counter.
				67:64	Reserved. Shall be cleared to zero.
LMDATA-15	95:80	Active Bucket Counter 3	16	Byte Address	Byte Description
				95:92	Read Command Counter.
				91:88	Write Command Counter.
				87:84	Deallocate/TRIM Command Counter.
				83:80	Reserved. Shall be cleared to zero.
LMDATA-16	191:96	Active Latency Stamp	96	This field contains a Timestamp for when a latency event occurred for each counter. A value of FFFFFFFF_FFFFFFFFh means the Latency Stamp is not valid. The Active Latency Stamp uses the data format for	

Requirement ID	Byte Address	Field	# of Bytes	Field Description																																																				
				Timestamp as defined in the NVM Express Base Specification: <table><tr><th>Byte Address</th><th>Bucket</th><th>Counter</th><th>Description</th></tr><tr><td>191:184</td><td>0</td><td>Read</td><td>Active Latency Stamp 0</td></tr><tr><td>183:176</td><td>0</td><td>Write</td><td>Active Latency Stamp 1</td></tr><tr><td>175:168</td><td>0</td><td>Deallocate/TRIM</td><td>Active Latency Stamp 2</td></tr><tr><td>167:160</td><td>1</td><td>Read</td><td>Active Latency Stamp 3</td></tr><tr><td>159:152</td><td>1</td><td>Write</td><td>Active Latency Stamp 4</td></tr><tr><td>151:144</td><td>1</td><td>Deallocate/TRIM</td><td>Active Latency Stamp 5</td></tr><tr><td>143:136</td><td>2</td><td>Read</td><td>Active Latency Stamp 6</td></tr><tr><td>135:128</td><td>2</td><td>Write</td><td>Active Latency Stamp 7</td></tr><tr><td>127:120</td><td>2</td><td>Deallocate/TRIM</td><td>Active Latency Stamp 8</td></tr><tr><td>119:112</td><td>3</td><td>Read</td><td>Active Latency Stamp 9</td></tr><tr><td>111:104</td><td>3</td><td>Write</td><td>Active Latency Stamp 10</td></tr><tr><td>103:96</td><td>3</td><td>Deallocate/TRIM</td><td>Active Latency Stamp 11</td></tr></table>	Byte Address	Bucket	Counter	Description	191:184	0	Read	Active Latency Stamp 0	183:176	0	Write	Active Latency Stamp 1	175:168	0	Deallocate/TRIM	Active Latency Stamp 2	167:160	1	Read	Active Latency Stamp 3	159:152	1	Write	Active Latency Stamp 4	151:144	1	Deallocate/TRIM	Active Latency Stamp 5	143:136	2	Read	Active Latency Stamp 6	135:128	2	Write	Active Latency Stamp 7	127:120	2	Deallocate/TRIM	Active Latency Stamp 8	119:112	3	Read	Active Latency Stamp 9	111:104	3	Write	Active Latency Stamp 10	103:96	3	Deallocate/TRIM	Active Latency Stamp 11
Byte Address	Bucket	Counter	Description																																																					
191:184	0	Read	Active Latency Stamp 0																																																					
183:176	0	Write	Active Latency Stamp 1																																																					
175:168	0	Deallocate/TRIM	Active Latency Stamp 2																																																					
167:160	1	Read	Active Latency Stamp 3																																																					
159:152	1	Write	Active Latency Stamp 4																																																					
151:144	1	Deallocate/TRIM	Active Latency Stamp 5																																																					
143:136	2	Read	Active Latency Stamp 6																																																					
135:128	2	Write	Active Latency Stamp 7																																																					
127:120	2	Deallocate/TRIM	Active Latency Stamp 8																																																					
119:112	3	Read	Active Latency Stamp 9																																																					
111:104	3	Write	Active Latency Stamp 10																																																					
103:96	3	Deallocate/TRIM	Active Latency Stamp 11																																																					
LMDATA-17	215:192	Active Measured Latency	24	This is the measured latency that caused the counter to increment. A value of 0000h means this field is invalid. A value of 0001h represents 1 ms. A value of 0002h represents 2 ms: <table><tr><th>Byte Address</th><th>Bucket</th><th>Counter</th><th>Description</th></tr><tr><td>215:214</td><td>0</td><td>Read</td><td>Active Measured Latency 0</td></tr></table>	Byte Address	Bucket	Counter	Description	215:214	0	Read	Active Measured Latency 0																																												
Byte Address	Bucket	Counter	Description																																																					
215:214	0	Read	Active Measured Latency 0																																																					

Requirement ID	Byte Address	Field	# of Bytes	Field Description			
				213:212	0	Write	Active Measured Latency 1
				211:210	0	Deallocate/TRIM	Active Measured Latency 2
				209:208	1	Read	Active Measured Latency 3
				207:206	1	Write	Active Measured Latency 4
				205:204	1	Deallocate/TRIM	Active Measured Latency 5
				203:202	2	Read	Active Measured Latency 6
				201:200	2	Write	Active Measured Latency 7
				199:198	2	Deallocate/TRIM	Active Measured Latency 8
				197:196	3	Read	Active Measured Latency 9
				195:194	3	Write	Active Measured Latency 10
				193:192	3	Deallocate/TRIM	Active Measured Latency 11
LMDATA-18	217:216	Active Latency Stamp Units	2	When bit is set to 1b, the Active Latency Stamp was based on receiving the NVMe Timestamp. When bit is cleared to 0b the Active Latency Stamp was based on power on hours since the NVMe Timestamp was not received.			
				Bit	Bucket	Counter	Description
				15:12	N/A	N/A	Reserved. Shall be cleared to zero.
				11	3	Deallocate/TRIM	Active Latency Stamp Unit [11]
				10	3	Write	Active Latency Stamp Unit [10]
				9	3	Read	Active Latency Stamp Unit [9]

Requirement ID	Byte Address	Field	# of Bytes	Field Description			
				8	2	Deallocate/TRIM	Active Latency Stamp Unit [8]
				7	2	Write	Active Latency Stamp Unit [7]
				6	2	Read	Active Latency Stamp Unit [6]
				5	1	Deallocate/TRIM	Active Latency Stamp Unit [5]
				4	1	Write	Active Latency Stamp Unit [4]
				3	1	Read	Active Latency Stamp Unit [3]
				2	0	Deallocate/TRIM	Active Latency Stamp Unit [2]
				1	0	Write	Active Latency Stamp Unit [1]
				0	0	Read	Active Latency Stamp Unit [0]
LMDATA-19	239:218	Reserved	22	Shall be cleared to zero.			
LMDATA-20	255:240	Static Bucket Counter 0	16	This is a snapshot of the Active Bucket Counter 0 which is moved to this field when the Active Bucket Timer equals the Active Bucket Timer Threshold:			
				Byte Address	Byte Description		
				255:252	Read Command Counter.		
				251:248	Write Command Counter.		
				247:244	Deallocate/TRIM Command Counter.		
				243:240	Reserved. Shall be cleared to zero.		
LMDATA-21	271:256	Static Bucket Counter 1	16	This is a snapshot of the Active Bucket Counter 1 which is moved to this field when the Active Bucket Timer equals the Active Bucket Timer Threshold:			
				Byte Address	Byte Description		
				271:268	Read Command Counter.		
				267:264	Write Command Counter.		

Requirement ID	Byte Address	Field	# of Bytes	Field Description			
				263:260	Deallocate/TRIM Command Counter.		
				259:256	Reserved. Shall be cleared to zero.		
LMDATA-22	287:272	Static Bucket Counter 2	16	This is a snapshot of the Active Bucket Counter 2 which is moved to this field when the Active Bucket Timer equals the Active Bucket Timer Threshold:			
				Byte Address	Byte Description		
				287:284	Read Command Counter.		
				283:280	Write Command Counter.		
				279:276	Deallocate/TRIM Command Counter.		
				275:272	Reserved. Shall be cleared to zero.		
LMDATA-23	303:288	Static Bucket Counter 3	16	This is a snapshot of the Active Bucket Counter 3 which is moved to this field when the Active Bucket Timer equals the Active Bucket Timer Threshold:			
				Byte Address	Byte Description		
				303:300	Read Command Counter.		
				299:296	Write Command Counter.		
				295:292	Deallocate/TRIM Command Counter.		
				291:288	Reserved. Shall be cleared to zero.		
LMDATA-24	399:304	Static Latency Stamp	96	This is a snapshot of the Active Latency Stamp which is moved to this field when the Active Bucket Timer equals the Active Bucket Timer Threshold. This field contains a timestamp for when a latency event occurred for each counter. A value of FFFFFFFF_FFFFFFFFh means the Latency Stamp is not valid. The Static Latency Stamp uses the Timestamp data format as defined in the NVM Express Base Specification:			
				Byte Address	Bucket	Counter	Description
				399:392	0	Read	Static Latency Stamp 0
				391:384	0	Write	Static Latency Stamp 1
				383:376	0	Deallocate/TRIM	Static Latency Stamp 2

Requirement ID	Byte Address	Field	# of Bytes	Field Description			
				375:368	1	Read	Static Latency Stamp 3
				367:360	1	Write	Static Latency Stamp 4
				359:352	1	Deallocate/TRIM	Static Latency Stamp 5
				351:344	2	Read	Static Latency Stamp 6
				343:336	2	Write	Static Latency Stamp 7
				335:328	2	Deallocate/TRIM	Static Latency Stamp 8
				327:320	3	Read	Static Latency Stamp 9
				319:312	3	Write	Static Latency Stamp 10
				311:304	3	Deallocate/TRIM	Static Latency Stamp 11
LMDATA-25	423:400	Static Measured Latency	24	This is a snapshot of the Active Measured Latency which is moved to this field when the Active Bucket Timer equals the Active Bucket Timer Threshold. A value of 0000h means this field is invalid. A value of 0001h represents 1 ms. A value of 0002h represents 2 ms.			
				Byte Address	Bucket	Counter	Description
				423:422	0	Read	Static Measured Latency 0
				421:420	0	Write	Static Measured Latency 1
				419:418	0	Deallocate/TRIM	Static Measured Latency 2
				417:416	1	Read	Static Measured Latency 3
				415:414	1	Write	Static Measured Latency 4
				413:412	1	Deallocate/TRIM	Static Measured Latency 5
				411:410	2	Read	Static Measured Latency 6

Requirement ID	Byte Address	Field	# of Bytes	Field Description			
				409:408	2	Write	Static Measured Latency 7
				407:406	2	Deallocate/TRIM	Static Measured Latency 8
				405:404	3	Read	Static Measured Latency 9
				403:402	3	Write	Static Measured Latency 10
				401:400	3	Deallocate/TRIM	Static Measured Latency 11
LMDATA-26	425:424	Static Latency Stamp Units	2	This is a snapshot of the Active Latency Stamp Units which is moved to this field when the Active Bucket Timer equals the Active Bucket Timer Threshold. When bit is set to 1b the Static Latency Stamp was based on receiving the NVMe Timestamp and the offset from this. When bit is cleared to 0b the Static Latency Stamp was based on power on hours since the NVMe Timestamp was not received.			
				Bit	Bucket	Counter	Description
				15:12	N/A	N/A	Reserved. Shall be cleared to zero.
				11	3	Deallocate/TRIM	Static Latency Stamp Unit [11]
				10	3	Write	Static Latency Stamp Unit [10]
				9	3	Read	Static Latency Stamp Unit [9]
				8	2	Deallocate/TRIM	Static Latency Stamp Unit [8]
				7	2	Write	Static Latency Stamp Unit [7]
				6	2	Read	Static Latency Stamp Unit [6]
				5	1	Deallocate/TRIM	Static Latency Stamp Unit [5]
				4	1	Write	Static Latency Stamp Unit [4]

Requirement ID	Byte Address	Field	# of Bytes	Field Description				
				3	1	Read	Static Latency Stamp Unit [3]	
				2	0	Deallocate/TRIM	Static Latency Stamp Unit [2]	
				1	0	Write	Static Latency Stamp Unit [1]	
				0	0	Read	Static Latency Stamp Unit [0]	
LMDATA-27	435:426	Reserved	10	Shall be cleared to zero.				
LMDATA-37	447:436	Latency Monitor Debug Telemetry Log Size	12	If the Host Initiated Telemetry Format Supported bit is cleared to 0b then this is the number of Dwords in the Latency Monitor Debug Log. This value is in Dwords. If the Host Initiated Telemetry Format Supported bit is set to 1b, then this field shall be reported as 0h and shall be ignored.				
LMDATA-28	449:448	Debug Log Trigger Enable	2	This controls what counters can cause a debug log event to be triggered. When set to 1b the first time the bucket/counter combination is incremented a debug log is triggered. When cleared to 0b a debug log will not be triggered when the bucket/counter combination is incremented.				
				Bit	Default Value	Bucket	Counter	Bit Description
				15:12	N/A	N/A	N/A	Reserved. Shall be cleared to zero.
				11	0b	3	Deallocate/TRIM	Active Log Enable [11]
				10	0b	3	Write	Active Log Enable [10]
				9	0b	3	Read	Active Log Enable [9]
				8	0b	2	Deallocate/TRIM	Active Log Enable [8]
				7	0b	2	Write	Active Log Enable [7]

Requirement ID	Byte Address	Field	# of Bytes	Field Description				
				6	0b	2	Read	Active Log Enable [6]
				5	0b	1	Deallocate/TRIM	Active Log Enable [5]
				4	0b	1	Write	Active Log Enable [4]
				3	0b	1	Read	Active Log Enable [3]
				2	0b	0	Deallocate/TRIM	Active Log Enable [2]
				1	0b	0	Write	Active Log Enable [1]
				0	0b	0	Read	Active Log Enable [0]
LMDATA-29	451:450	Debug Log Measured Latency	2	When a debug log is triggered, this is the measured latency for the Latency Stamp that caused the debug log to trigger. A value of 0000h means this field is invalid. A value of 0001h represents 1 ms. A value of 0002h represents 2 ms. A value of FFFFh means the Debug Log Measured Latency saturated at the max.				
LMDATA-30	459:452	Debug Log Latency Stamp	8	This is the Latency Stamp associated with the debug log.				
LMDATA-31	461:460	Debug Log Pointer	2	This shall be set to CAh.				
LMDATA-32	463:462	Debug Counter Trigger Source	2	When the Debug Counter Trigger Source bit is set to 1b the debug log is valid, and this is the counter that triggered the debug log. When the Debug Counter Trigger Source bit is cleared to 0b this is not the counter that triggered the debug log. No more than 1 bit in this field shall be set. When the Debug Counter Trigger Source is 0b the Debug Log Latency, Debug Log Latency Stamp, Debug Log Pointer, and Debug Counter Trigger Source is not valid. If the debug log has been cleared this field shall be cleared to zero.				
				Bit	Bucket	Counter	Bit Description	
				15:12	N/A	N/A	Reserved. Shall be cleared to zero.	

Requirement ID	Byte Address	Field	# of Bytes	Field Description			
				11	3	Deallocate/TRIM	Debug Counter Trigger Source 11
				10	3	Write	Debug Counter Trigger Source 10
				9	3	Read	Debug Counter Trigger Source 9
				8	2	Deallocate/TRIM	Debug Counter Trigger Source 8
				7	2	Write	Debug Counter Trigger Source 7
				6	2	Read	Debug Counter Trigger Source 6
				5	1	Deallocate/TRIM	Debug Counter Trigger Source 5
				4	1	Write	Debug Counter Trigger Source 4
				3	1	Read	Debug Counter Trigger Source 3
				2	0	Deallocate/TRIM	Debug Counter Trigger Source 2
				1	0	Write	Debug Counter Trigger Source 1
				0	0	Read	Debug Counter Trigger Source 0
LMDATA-33	464	Debug Log Stamp Units	1	Bit	Bit Description		
				7:1	Reserved. Shall be cleared to zero.		
				0	When set to 1b the Debug Latency Stamp was based on receiving the NVMe Timestamp and the offset from this. When cleared to 0b the Debug Latency Stamp was based on power on hours since the NVMe Timestamp was not received.		
LMDATA-34	493:465	Reserved	29	Shall be cleared to zero.			
LMDATA-35	495:494	Log Page Version	2	This indicates the version of this log page. Shall be set to 0005h.			
LMDATA-36	511:496	Log Page GUID	16	Shall be set to			

Requirement ID	Byte Address	Field	# of Bytes	Field Description
				85D45E58D4E643709C6C84D08CC07A92h.
LMDATA-38	4095:512	Reserved	3584	Reserved. Shall be cleared to 0h.

4.8.10 Device Capabilities Log Page (Log Identifier C4h) Requirements

This log page provides the host with a consolidated report of critical device-specific support information. This log page shall be 4096 bytes with the following functional requirements and field format:

Requirement ID	Byte Address	Field	# of Bytes	Field Description												
DCLP-1	1:0	PCI Express Ports	2	The number of physical PCI Express ports supported by the device.												
DCLP-2	3:2	OOB Management Support	2	Bit field indicating the OOB Management interfaces supported by the device: <table><tr><th>Bit</th><th>Bit Description</th></tr><tr><td>15</td><td>Shall be set to 1b if the device has been tested and found to comply with the OOB Management requirements of this specification.</td></tr><tr><td>14:3</td><td>Reserved. Shall be cleared to zero.</td></tr><tr><td>2</td><td>Shall be set to 1b to report that the NVMe Basic Management Command is supported. Some devices may not support (see DP-CFG-4).</td></tr><tr><td>1</td><td>Shall be set to 1b to report that MCTP over PCIe VDM is supported (see NVMe-MI-3).</td></tr><tr><td>0</td><td>Shall be set to 1b to report that MCTP over SMBus is supported (see NVMe-MI-2).</td></tr></table>	Bit	Bit Description	15	Shall be set to 1b if the device has been tested and found to comply with the OOB Management requirements of this specification.	14:3	Reserved. Shall be cleared to zero.	2	Shall be set to 1b to report that the NVMe Basic Management Command is supported. Some devices may not support (see DP-CFG-4).	1	Shall be set to 1b to report that MCTP over PCIe VDM is supported (see NVMe-MI-3).	0	Shall be set to 1b to report that MCTP over SMBus is supported (see NVMe-MI-2).
Bit	Bit Description															
15	Shall be set to 1b if the device has been tested and found to comply with the OOB Management requirements of this specification.															
14:3	Reserved. Shall be cleared to zero.															
2	Shall be set to 1b to report that the NVMe Basic Management Command is supported. Some devices may not support (see DP-CFG-4).															
1	Shall be set to 1b to report that MCTP over PCIe VDM is supported (see NVMe-MI-3).															
0	Shall be set to 1b to report that MCTP over SMBus is supported (see NVMe-MI-2).															
DCLP-3	5:4	Write Zeroes Command Support	2	Bit field indicating the Write Zeroes command requirements supported by the device. <table><tr><th>Bit</th><th>Bit Description</th></tr><tr><td>15</td><td>Shall be set to 1b if the device has been tested and found to comply with the Write Zeroes command requirements of this specification.</td></tr><tr><td>14:5</td><td>Reserved. Shall be cleared to zero.</td></tr><tr><td>4</td><td>Shall be set to 1b to report that the requirements of NVMe-IO-6 are met.</td></tr></table>	Bit	Bit Description	15	Shall be set to 1b if the device has been tested and found to comply with the Write Zeroes command requirements of this specification.	14:5	Reserved. Shall be cleared to zero.	4	Shall be set to 1b to report that the requirements of NVMe-IO-6 are met.				
Bit	Bit Description															
15	Shall be set to 1b if the device has been tested and found to comply with the Write Zeroes command requirements of this specification.															
14:5	Reserved. Shall be cleared to zero.															
4	Shall be set to 1b to report that the requirements of NVMe-IO-6 are met.															

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
				3	Shall be set to 1b to report that the requirements of NVMe-IO-5 are met.
				2	Shall be set to 1b to report that setting the FUA bit is supported (see NVMe-IO-4).
				1	Shall be set to 1b to report that setting the DEAC bit is supported (see NVMe-IO-4).
				0	Shall be set to 1b to report that the Write Zeroes command is supported (see NVMe-IO-4).
DCLP-4	7:6	Sanitize Command Support	2	Bit field indicating the Sanitize command requirements supported by the device:	
				Bit	Bit Description
				15	Shall be set to 1b if the device has been tested and found to comply with the Sanitize command requirements of this specification.
				14:5	Reserved. Shall be cleared to zero.
				4	Shall be set to 1b to report that deallocation after a sanitize operation is supported (see NVMe-AD-29).
				3	Shall be set to 1b to report that Overwrite is supported (see NVMe-AD-7).
				2	Shall be set to 1b to report that Block Erase is supported (see NVMe-AD-7).
				1	Shall be set to 1b to report that Crypto-Erase is supported (see NVMe-AD-7).
DCLP-5	9:8	Dataset Management Command Support	2	Bit field indicating the Dataset Management command requirements supported by the device:	
				Bit	Bit Description
				15	Shall be set to 1b if the device has been tested and found to comply with the Dataset Management command requirements of this specification.
				14:2	Reserved. Shall be cleared to zero.

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
				1	Shall be set to 1b to report that the Deallocate Attribute (i.e., Attribute – Deallocate (AD)) is supported (see TRIM-1).
				0	Shall be set to 1b to report that the Dataset Management command is supported (see NVMe-IO-2).
DCLP-6	11:10	Write Uncorrectable Command Support	2	If the device supports the Write Uncorrectable command (see DP-CFG-7), then the bits in this field indicates the Write Uncorrectable command requirements supported by the device. If the device does not support the Write Uncorrectable command, then this field shall be cleared to zero.	
				Bit	Bit Description
				15	Shall be set to 1b if the device has been tested and found to comply with the Write Uncorrectable command requirements of this specification if the Write Uncorrectable command is supported. Shall be cleared to 0b if the Write Uncorrectable command is not supported.
				14:4	Reserved. Shall be cleared to zero.
				3	Shall be set to 1b to report that the SMART / Health Information log page (Log Identifier 02h) requirements of NVMe-IO-14 are met if the Write Uncorrectable command is supported. Shall be cleared to 0b if the Write Uncorrectable command is not supported.
				2	Shall be set to 1b to report that the device supports setting uncorrectable on the maximum number of LBAs allowed by the NVM Express Base Specification (see NVMe-IO-12) if the Write Uncorrectable command is supported. Shall be cleared to 0b if the Write Uncorrectable command is not supported.
				1	Shall be set to 1b to report that the device supports setting uncorrectable on a single LBA (see NVMe-IO-11) if the Write Uncorrectable command is supported. Shall

Requirement ID	Byte Address	Field	# of Bytes	Field Description												
					be cleared to 0b if the Write Uncorrectable command is not supported.											
				0	Shall be set to 1b if the Write Uncorrectable command is supported (see DP-CFG-7).											
DCLP-7	13:12	Fused Operation Support	2	Bit field indicating the fused command pairs requirements supported by the device: <table><tr><th>Bit</th><th>Bit Description</th></tr><tr><td>15</td><td>Shall be set to 1b if the device has been tested and found to comply with the fused command pair support requirements of this specification.</td></tr><tr><td>14:1</td><td>Reserved. Shall be cleared to zero.</td></tr><tr><td>0</td><td>Shall be set to 1b to report that the Compare and Write fused command pair is supported (see NVMe-IO-9).</td></tr></table>		Bit	Bit Description	15	Shall be set to 1b if the device has been tested and found to comply with the fused command pair support requirements of this specification.	14:1	Reserved. Shall be cleared to zero.	0	Shall be set to 1b to report that the Compare and Write fused command pair is supported (see NVMe-IO-9).			
Bit	Bit Description															
15	Shall be set to 1b if the device has been tested and found to comply with the fused command pair support requirements of this specification.															
14:1	Reserved. Shall be cleared to zero.															
0	Shall be set to 1b to report that the Compare and Write fused command pair is supported (see NVMe-IO-9).															
DCLP-8	15:14	Minimum Valid DSSD Power State	2	Shall be set to the lowest numbered valid DSSD Power State. Setting a DSSD Power State less than this value results in Invalid Field in Command (see DSSDPSS-2).												
DCLP-9	143:16	DSSD Power State Descriptors	128	Byte 16 is reserved and shall be cleared to zero. The device shall populate bytes 17-143 with a single-byte DSSD Power State Descriptor for each DSSD Power State (see Section 4.8.11.1 DSSD Power State Descriptor) starting with DSSD Power State 1. The DSSD Power State Descriptors shall be populated in increasing order of power state number, i.e., byte 17 contains the descriptor for DSSD Power State 1, byte 18 contains the descriptor for DSSD Power State 2, etc. up to byte 143 which contains the descriptor for DSSD Power State 127.												
DCLP-13	145:144	FIPS 140 Validation	2	<table><tr><th>Bits</th><th>Description</th></tr><tr><td>15:4</td><td>Reserved. Shall be cleared to zero.</td></tr><tr><td rowspan="3">3:0</td><td>FIPS 140 Validation Status:<table><tr><th>Value</th><th>Description</th></tr><tr><td>Fh:5h</td><td>Reserved</td></tr><tr><td>4h</td><td>Device has a full FIPS 140 validation.</td></tr></table></td></tr></table>	Bits	Description	15:4	Reserved. Shall be cleared to zero.	3:0	FIPS 140 Validation Status: <table><tr><th>Value</th><th>Description</th></tr><tr><td>Fh:5h</td><td>Reserved</td></tr><tr><td>4h</td><td>Device has a full FIPS 140 validation.</td></tr></table>	Value	Description	Fh:5h	Reserved	4h	Device has a full FIPS 140 validation.
Bits	Description															
15:4	Reserved. Shall be cleared to zero.															
3:0	FIPS 140 Validation Status: <table><tr><th>Value</th><th>Description</th></tr><tr><td>Fh:5h</td><td>Reserved</td></tr><tr><td>4h</td><td>Device has a full FIPS 140 validation.</td></tr></table>	Value	Description	Fh:5h	Reserved	4h	Device has a full FIPS 140 validation.									
	Value	Description														
	Fh:5h	Reserved														
4h	Device has a full FIPS 140 validation.															

Requirement ID	Byte Address	Field	# of Bytes	Field Description									
					<table><tr><td>3h</td><td>Device has an interim FIPS 140 validation.</td></tr><tr><td>2h</td><td>Device has been submitted for FIPS 140 validation and is not yet FIPS 140 validated.</td></tr><tr><td>1h</td><td>Device is intended to be FIPS 140 validated and has not yet been submitted for FIPS 140 validation.</td></tr><tr><td>0h</td><td>Device is not FIPS 140 validated and is not intended to be FIPS 140 validated.</td></tr></table>	3h	Device has an interim FIPS 140 validation.	2h	Device has been submitted for FIPS 140 validation and is not yet FIPS 140 validated.	1h	Device is intended to be FIPS 140 validated and has not yet been submitted for FIPS 140 validation.	0h	Device is not FIPS 140 validated and is not intended to be FIPS 140 validated.
3h	Device has an interim FIPS 140 validation.												
2h	Device has been submitted for FIPS 140 validation and is not yet FIPS 140 validated.												
1h	Device is intended to be FIPS 140 validated and has not yet been submitted for FIPS 140 validation.												
0h	Device is not FIPS 140 validated and is not intended to be FIPS 140 validated.												
				A review (i.e., NIST review or CST lab review) is considered to be in progress if the device is in the queue waiting for that review to begin. See SEC-53 for FIPS 140 compliance descriptor (see SEC-52) population requirements based on the status of FIPS 140 validation.									
DCLP-10	4077:146	Reserved	3932	Shall be cleared to zero.									
DCLP-11	4079:4078	Log Page Version	2	This indicates the version of the mapping this log page uses. Shall be set to 0002h.									
DCLP-12	4095:4080	Log Page GUID	16	Shall be set to B7053C914B58495D98C9E1D10D054297h.									

4.8.11 DSSD Power State Requirements

DSSD power states provide an alternative interface to NVMe power management. DSSD and NVMe Power States are numbered in opposite directions – higher numbered DSSD Power States consume more power than lower numbered DSSD Power States, whereas higher numbered NVMe Power States consume less power than lower numbered NVMe Power States.

Selecting a DSSD Power State via a Set Features command (see [Section 4.15.15 DSSD Power State \(Feature Identifier C7h\) Set Feature](#)) causes the device to run at the highest powered NVMe Power State whose Maximum Power (MP) in watts is less than or equal to the number of the DSSD Power State. For example, placing the device in DSSD Power State number 20 causes the device to enter the highest powered NVMe Power State whose Maximum Power (MP) is less than or equal to 20 watts.

In general, a device will have more DSSD Power States than NVMe Power States. Selecting a DSSD Power State whose number is not the Maximum Power (MP) in watts of an NVMe Power State causes the device to drop down to run at the highest powered NVMe Power State whose Maximum Power (MP) does not exceed the number of the DSSD Power State in watts.

For example, suppose that a device supports NVMe Power State 5 that consumes no more than 20 watts Maximum Power (MP) and NVMe Power State 6 that consumes no more than 16 watts Maximum Power (MP). Selecting DSSD Power State 18 (i.e., 18 watts Maximum Power (MP)) causes the device to enter NVMe Power State 6 and consume no more than 16 watts Maximum Power (MP). In this example the device reports 18 as its DSSD Power State and 6 as its NVMe Power State. Selecting NVMe Power State 6 causes the device to report 16 as its DSSD Power State and 6 as its NVMe Power State.

DSSD Power State 0 does not exist, as a device that is consuming 0 watts Maximum Power (MP) is powered off. DSSD Power States that represent a Maximum Power (MP) less than the lowest powered NVMe Power State are invalid. The lowest numbered valid DSSD Power State is indicated in [DCLP-8](#).

4.8.11.1 DSSD Power State Descriptor

The DSSD Power State Descriptor for each DSSD Power State has the following format:

Requirement ID	Bits	Field	Field Description
DSSDPSD-1	7	Valid DSSD Power State	Shall be set to 1b if the number of this DSSD Power State is greater than or equal to the Minimum Valid OCP Power State (see DCLP-8).
DSSDPSD-2	6:5	Reserved	Shall be cleared to zero.
DSSDPSD-3	4:0	NVMe Power State	Shall be set to the number of the highest powered NVMe Power State whose Maximum Power (MP) in watts is less than or equal to the number of this DSSD Power State.

4.8.12 Unsupported Requirements Log Page (Log Identifier C5h) Requirements

This log page provides a host with a consolidated report of all the Requirement IDs that the device does not support. This log page shall be 4096 bytes with the following functional requirements and field format:

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
URLP-1	1:0	Unsupported Count	2	The number of Unsupported Requirement IDs.	
URLP-2	15:2	Reserved	14	Shall be cleared to zero.	
URLP-3	4063:16	Unsupported Requirements List	4048	This structure shall be populated with between 0 and 253 16-byte zero padded ASCII strings. Each string shall be the Requirement ID of a requirement that the device does not support. Entries shall be in alphabetical order. Unused entries shall be cleared to zero.	
				Byte Address	Byte Description
				31:16	First Unsupported Requirement ID entry.
				47:32	Second Unsupported Requirement ID entry.
				...	...

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
				4063:4048	253 rd Unsupported Requirement ID entry.
URLP-4	4077:4064	Reserved	14	Shall be cleared to zero.	
URLP-5	4079:4078	Log Page Version	2	This indicates the version of the mapping this log page uses. Shall be set to 0001h.	
URLP-6	4095:4080	Log Page GUID	16	Shall be set to C7BB98B7D0324863BB2C23990E9C722Fh.	

4.8.13 Hardware Component Log Page (Log Identifier C6h) Requirements

This log page provides the host with information regarding the hardware components on the device. This log page is intended to enable customers to be able to parse this log when there are component issues to be able to find failing devices. This also enables customers to be able to parse this log for failing devices and not require device serial numbers to find the devices with component issues.

Requirement ID	Description
HWCOMP-1	A value of zero shall only be used if the corresponding component data is not available.
HWCOMP-2	Manufacturer codes shall be clearly documented and disclosed to the customer.
HWCOMP-3	This log shall contain the controller ASIC, PMICs, DRAM, NAND, PCB, and all other critical hardware components.
HWCOMP-4	This log shall contain the Device Serial Number.
HWCOMP-5	This log shall contain the Country of Origin.
HWCOMP-6	This log shall contain the Global Hardware Revision.
HWCOMP-7	The first Component Descriptor shall start at byte 64.
HWCOMP-8	The last Component Descriptor shall end at the byte address which is equal to the Hardware Component Log Size – 1
HWCOMP-9	There shall be no Dwords between two Component Descriptors.

4.8.13.1 Component Descriptor

The Hardware Component Log uses a component descriptor of the following format:

Requirement ID	Byte Address	Field	# of Bytes	Field Description
COMP-1	7:0	Component Date/Lot Size	8	Component Date/Lot Size in Dwords. This is a one-based value. A value of 0h means the Component Date/Lot Code field does not exist in the descriptor. A value of 1h means this field is 1 Dword in size.

Requirement ID	Byte Address	Field	# of Bytes	Field Description
COMPDP-2	15:8	Component Additional Information Size	8	Component Additional Information Size in Dwords. This is a one-based value. A value of 0h means the Component Additional Information field does not exist in the descriptor. A value of 1h means this field is 1 Dword in size.
COMPDP-3	19:16	Component Identifier	4	This is the type of component. This shall follow the Component Identifier Table.
COMPDP-4	27:20	Component Manufacture	8	The value in this field shall represent Component Manufacture. If this field is 0h then there is no component manufacture information provided. This value is in hex.
COMPDP-5	35:28	Component Revision	8	The value in this field shall represent the Component Revision. If this field is 0h then there is no Component Revision information provided. This value is in hex.
COMPDP-6	43:36	Component Manufacture Code	8	The value in this field shall represent the Component Manufacture Code. If this field is 0h then there is no Component Manufacture Code information provided. This value is in hex.
COMPDP-7	(Component Date/Lot Size * 4) + 43:44	Component Date/Lot Code	Component Date/Lot Size * 4	The value in this field shall represent a Component Date/Lot Code. If this field is 0h then there is no Component Date/Lot code provided. This value is in hex.
COMPDP-8	(Component Additional Information Size * 4) + (Component Date/Lot Size * 4) + 43:Component Date/Lot Size * 4) + 44	Component Additional Information	Component Additional Information Size * 4	The value in this field shall represent additional component information. If this field is 0h then there is no additional component information. This value is in hex unless otherwise noted in the component identifier.

4.8.13.2 Component Identifier Table

The following is a table of the Component Identifiers:

Requirement ID	Component Identifier	Description
CITYPE-1	0000h	Reserved
CITYPE-2	0001h	This is a Controller ASIC component
CITYPE-3	0002h	This is a NAND Component.
CITYPE-4	0003h	This is a DRAM Component.
CITYPE-5	0004h	This is a PMIC Component.
CITYPE-6	0005h	This is a PCB Component
CITYPE-7	0006h	This is a capacitor component.
CITYPE-8	0007h	This is a resistor component.
CITYPE-9	0008h	This is a case component.
CITYPE-10	0009h	Device Serial Number. The serial number shall go into the Additional Component Information field, and the other fields shall be 0h, except for the Component Identifier and Component Additional Information Size.
CITYPE-11	000Ah	Country of Origin. This is a UTF-8 string detailing the device Country of Origin. The Country-of-Origin value shall go into the Additional Component Information field, and the other fields shall be 0h, except for the Component Identifier and Component Additional Information Size.
CITYPE-12	000Bh	Global Device Hardware Revision. The Global Device Hardware Revision shall go into the Additional Component Information field, and the other fields shall be 0h, except for the Component Identifier and Component Additional Information Size. If a new revision of hardware is introduced during qualification, a new unique identifier shall be reported.
CITYPE-15	000Ch	Born on Date. The date on which the device was manufactured. ASCII string format is MMDDYYYY. The Born-on Date shall go into the Additional Component Information field, and the other fields shall be 0h, except for the Component Identifier and Component Additional Information Size.
CITYPE-13	000Dh-7FFFh	Reserved
CITYPE-14	8000h-FFFFh	Vendor Unique Component

4.8.13.3 Hardware Component Log Page

Requirement ID	Byte Address	Field	# of Bytes	Field Description
HWCLOG-1	1:0	Log Page Version	2	This indicates the version of the mapping this log page uses. Shall be set to 0002h.

Requirement ID	Byte Address	Field	# of Bytes	Field Description
HWCLOG-2	15:2	Reserved	14	Shall be cleared to zero.
HWCLOG-3	31:16	Log Page GUID	16	Shall be set to BCB6821F30CD4ED0B76B31B99F0F57DCh.
HWCLOG-4	47:32	Hardware Component Log Size	16	This is the size of the Hardware Component Log in bytes.
HWCLOG-5	63:48	Reserved	16	Reserved. Shall be cleared to 0h.
HWCLOG-6	Hardware Component Log Size – 1:64	Component Descriptions	Hardware Component Log Size – 64	This shall contain the hardware descriptors.

4.8.14 TCG Configuration Log Page (Log Identifier C7h) Requirements

TCG Configuration Log shall be 512 bytes in size. This log defines the data points related to TCG Opal Security Subsystem Class (SSC) that would be useful to collect for diagnostic purposes. These data points give point-in-time insight into the configuration and state of the device which can be used to explain either a device or host behavior.

TCG Log Behavior Type	Persistence Type
A	Persistent across TCG revert: PSID, Admin SP, Locking SP
B	Not persistent across TCG revert

Requirement ID	Byte Address	Field	# of Bytes	Field Description	Behavior Type	TCG Log Behavior Type
TCGL-1	0	State	1	Bit 0: C_PIN_SID Value indicates whether C_PIN_SID object's PIN column value is equal to MSID or not. 0 = MSID value 1 = Not MSID value Bit 1: C_PIN_SID Authentication Blocked indicates whether authentication of C_PIN_SID authority is blocked or not due to Block SID Authentication command. 0 = Not blocked	1	N/A

Requirement ID	Byte Address	Field	# of Bytes	Field Description	Behavior Type	TCG Log Behavior Type
				1 = Blocked Bit 2: Locking Enabled (feature code 0002h) indicates whether the Locking SP is currently in 'Manufactured-Inactive' or 'Manufactured' state. 0 = Locking SP not activated i.e., Manufactured-Inactive state 1 = Locking SP activated i.e., Manufactured state Bit 3: Single User Mode Owner indicates the ownership policy for the RangeStart and RangeLength columns of all Locking Objects in Single User Mode. 0 = User Authority 1 = Admins Authority All other bits shall be cleared to zero.		
TCGL-2	3:1	Reserved	3	Shall be cleared to zero.	N/A	N/A
TCGL-3	5:4	Locking SP Activation Count	2	Count of transitions of the Locking SP from 'Manufactured-Inactive' to 'Manufactured'.	2	A
TCGL-4	7:6	Tper Revert Count	2	Count of successful invocations of the Revert method on the Admin SP which causes the entire Tper to revert to Original Factory State.	2	A
TCGL-5	9:8	Locking SP Revert Count	2	Count of successful invocations of the Revert method on the Locking SP which causes the Locking SP to transition from 'Manufactured' to 'Manufactured-Inactive'.	2	A
TCGL-6	11:10	Number of Locking Objects	2	The number of Locking Objects supported in the Locking table, including the Global Locking Object. If the Locking SP is inactive, then this value shall be cleared to zero.	1	N/A

Requirement ID	Byte Address	Field	# of Bytes	Field Description	Behavior Type	TCG Log Behavior Type
TCGL-7	13:12	Number of Single User Mode Locking Objects	2	The current number of Locking Objects in the Locking table that are in Single User Mode including the Global Locking Object. If the Locking SP is inactive, then this value shall be cleared to zero.	1	N/A
TCGL-8	15:14	Number of Range Provisioned Locking Objects	2	The current number of non-Global Locking Objects with non-zero RangeLength value. If the Locking SP is inactive, then this value shall be cleared to zero.	1	N/A
TCGL-9	17:16	Number of Namespace Provisioned Locking Objects	2	The current number of non-Global Locking Objects with a non-zero NamespaceID value. If the Locking SP is inactive, then this value shall be cleared to zero. If there are more than 254 non-Global Locking Objects, then this field shall be set to FFh, and the device shall implement TCGL-23.	1	N/A
TCGL-10	19:18	Number of Read Locked Locking Objects	2	The current number of provisioned non-Global Locking Objects with ReadLockEnabled set to True and ReadLocked set to True. If the Locking SP is inactive, then this value shall be cleared to zero.	1	N/A
TCGL-11	21:20	Number of Write Locked Locking Objects	2	The current number of provisioned non-Global Locking Objects with WriteLockEnabled set to True and WriteLocked set to True. If the Locking SP is inactive, then this value shall be cleared to zero.	1	N/A
TCGL-12	23:22	Number of Read Unlocked Locking Objects	2	The current number of provisioned non-Global Locking Objects with ReadLockEnabled set to True and ReadLocked set to False. If the Locking SP is inactive, then this value shall be cleared to zero.	1	N/A

Requirement ID	Byte Address	Field	# of Bytes	Field Description	Behavior Type	TCG Log Behavior Type
TCGL-13	25:24	Number of Write Unlocked Locking Objects	2	The current number of provisioned non-Global Locking Objects with WriteLockEnabled set to True and WriteLocked set to False. If the Locking SP is inactive, then this value shall be cleared to zero.	1	N/A
TCGL-14	N/A	Reserved	0	Obsolete.	N/A	N/A
TCGL-15	29:26	SID Authentication Try Count	4	The Tries value for the C_PIN_SID Credential Object which indicates the number of failed authentication attempts for that object since the last power cycle, successful authentication or Tper revert.	1	N/A
TCGL-16	33:30	SID Authentication Try Limit	4	The TryLimit value for the C_PIN_SID Credential Object which indicates the maximum number of failed authentication attempts for that object.	1	N/A
TCGL-17	37:34	Programmatic TCG Reset Count	4	The count of Programmatic TCG Resets received by the device since the last power cycle.	3	A
TCGL-18	41:38	Programmatic Reset Lock Count	4	The count of state transitions for all provisioned non-Global Locking Objects in the following conditions: - Read Lock Transition when ReadLockedEnable = True and ReadLocked transitions from False to True. - Write Lock Transition when WriteLockedEnable = True and WriteLocked transitions from False True. The count shall increment for both explicit and implicit TCG Programmatic Resets since the last power cycle.	3	A

Requirement ID	Byte Address	Field	# of Bytes	Field Description	Behavior Type	TCG Log Behavior Type
TCGL-19	45:42	TCG Error Count	4	The count of TCG errors reported to the host.	3	A
TCGL-23	49:46	Number of Namespace Provisioned Locking Objects Extended	2	The current number of non-Global Locking Objects with a non-zero NamespaceID value. If the Locking SP is inactive, then this value shall be cleared to zero.	1	N/A
TCGL-20	493:450	Reserved	444	Shall be cleared to zero.	N/A	N/A
TCGL-21	495:494	Log Page Version	2	Shall be set to 0003h.	N/A	N/A
TCGL-22	511:496	Log Page GUID	16	Shall be set to 54E02A9DFA5447C083E6E07EBD 244006h.	N/A	N/A

4.8.15 Telemetry String Log Page (Log Identifier C9h) Requirements

The Telemetry String log page enables mapping of Statistic Identifiers, Debug Class/Event Identifiers and Debug Class/VU Event Identifier combinations to ASCII strings.

4.8.15.1 Telemetry String Log Page Requirements

Requirement ID	Description
TELSLG-1	All Statistic Identifiers contained in Data Area 1 and Data Area 2 shall be contained in this log page.
TELSLG-2	String Identifier Table entries shall be in numeric order such that the smallest Vendor Unique Statistic Identifier is at the lowest address.
TELSLG-3	All Debug Event Class/ Event Identifier combinations contained in Telemetry Data Area 1 and Telemetry Data Area 2 shall be contained in this log page.
TELSLG-4	All Debug Event Class/ VU Event Identifier combinations contained in Telemetry Data Area 1 and Telemetry Data Area 2 shall be contained in this log page.
TELSLG-5	String Event Table entries shall be in numeric order such that the smallest Debug event Class is at the lowest address.
TELSLG-6	String VU Event Table entries shall be in numeric order such that the smallest Debug event Class is at the lowest address.
TELSLG-7	String Event Table entries shall be in numeric order such that for a single Debug/Event Identifier combination the smallest Event Identifier is at the lowest address.
TELSLG-8	String VU Event Table entries shall be in numeric order such that for a single Debug/VU Event Identifier combination the smallest VU Event Identifier is at the lowest address.

Requirement ID	Description
TELSLG-9	In the ASCII table (See Section 4.8.15.2 Telemetry String Log Page Format), characters which are not valid (beyond the length of the ASCII length) shall be set to <space> (i.e., 20h).
TELSLG-10	The String Identifier Table shall have no gaps between this table and the String Event Table.
TELSLG-11	The String Event Table entry shall have no gaps between this table and the VU String Event Table.
TELSLG-12	The VU String Event Table and the ASCII table shall have no gaps between these tables.
TELSLG-13	The String Identifier Table Entries, The String Event Table Entries and the String VU Event Table Entries may point to the same ASCII Table Entry.
TELSLG-14	Statistic Identifiers (see Section 4.9.11 Statistics Identifiers) which are not vendor unique and Debug / Event Identifiers (see Section 4.9.15.2 Event Classes) which are not vendor unique and are defined by this specification are not required to be populated in the String Log if the OCP plugin for the nvme-cli tool is able to decode these due to the decodes being populated in the tool. This is an exception to TELSLOG-1 and TELSLOG-3.

4.8.15.2 Telemetry String Log Page Format

The Telemetry String log page enables mapping data constructs in Telemetry Data Area 1 and Telemetry Data Area 2 to ASCII strings. The size of the Telemetry String log page can be found in Telemetry Data Area 1 or in the Telemetry String log page. The following is the format of the Telemetry String log page:

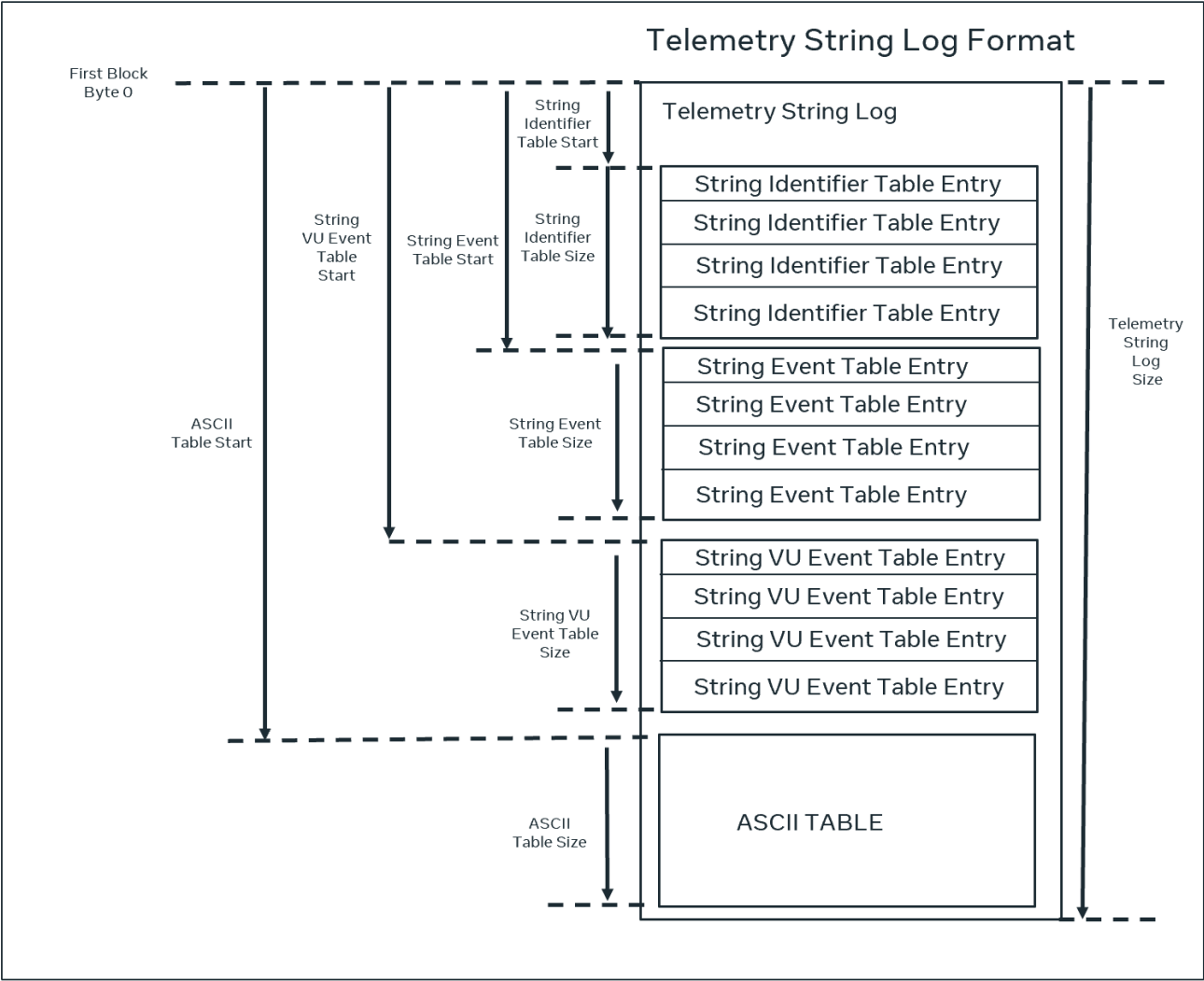
Requirement ID	Byte Address	Field	# of Bytes	Field Description
TELSTR-LOG-1	0	Log Page Version	1	Shall be set to 01h.
TELSTR-LOG-2	15:1	Reserved	15	Shall be cleared to zero.
TELSTR-LOG-3	31:16	Log Page GUID	16	Shall be set to B13A83691A8F408B9EA495940057AA44h.
TELSTR-LOG-4	39:32	Telemetry String Log Page Size (SLPS)	8	Shall be set to the number of Dwords in the Telemetry String log page.
TELSTR-LOG-5	63:40	Reserved	24	Shall be cleared to zero.
TELSTR-LOG-6	71:64	Statistics Identifier String Table Start (SITS)	8	Shall be set to the number of Dwords from byte 0 of this log page to the start of the Statistics Identifier String Table. This shall be set to 6Ch.
TELSTR-LOG-7	79:72	Statistics Identifier String Table Size (SITSZ)	8	Shall be set to the number of Dwords in the Statistics Identifier String Table. If there are no Statistic Descriptors that require strings and no vendor unique defined values this field shall be set to 0h.

Requirement ID	Byte Address	Field	# of Bytes	Field Description
TELSTR-LOG-8	87:80	Event String Table Start (ESTS)	8	Shall be set to the number of Dwords from byte 0 of this log page to the start of the Event String Table.
TELSTR-LOG-9	95:88	Event String Table Size (ESTSZ)	8	Shall be set to the number of Dwords in the Event String Table.
TELSTR-LOG-10	103:96	VU Event String Table Start (VUETS)	8	Shall be set to the number of Dwords from byte 0 of this log page to the start of the VU Event String Table.
TELSTR-LOG-11	111:104	VU Event String Table Size (VUESTZ)	8	Shall be set to the number of Dwords in the VU Event String Table.
TELSTR-LOG-12	119:112	ASCII Table Start (ASCTS)	8	This is the number of Dwords from byte 0 of this log page until the ASCII Table Starts.
TELSTR-LOG-13	127:120	ASCII Table Size (ASCTSZ)	8	This is the number of Dwords in the ASCII Table.
TELSTR-LOG-14	143:128	FIFO 1 ASCII String	16	This is the name of FIFO 1. If the FIFO has no string name this shall be populated with 0h.
TELSTR-LOG-15	159:144	FIFO 2 ASCII String	16	This is the name of FIFO 2. If the FIFO has no string name this shall be populated with 0h.
TELSTR-LOG-16	175:160	FIFO 3 ASCII String	16	This is the name of FIFO 3. If the FIFO has no string name this shall be populated with 0h.
TELSTR-LOG-17	191:176	FIFO 4 ASCII String	16	This is the name of FIFO 4. If the FIFO has no string name this shall be populated with 0h.
TELSTR-LOG-18	207:192	FIFO 5 ASCII String	16	This is the name of FIFO 5. If the FIFO has no string name this shall be populated with 0h.
TELSTR-LOG-19	223:208	FIFO 6 ASCII String	16	This is the name of FIFO 6. If the FIFO has no string name this shall be populated with 0h.
TELSTR-LOG-20	239:224	FIFO 7 ASCII String	16	This is the name of FIFO 7. If the FIFO has no string name this shall be populated with 0h.
TELSTR-LOG-21	255:240	FIFO 8 ASCII String	16	This is the name of FIFO 8. If the FIFO has no string name this shall be populated with 0h.
TELSTR-LOG-22	271:256	FIFO 9 ASCII String	16	This is the name of FIFO 9. If the FFO has no string name this shall be populated with 0h.

Requirement ID	Byte Address	Field	# of Bytes	Field Description
TELSTR-LOG-23	287:272	FIFO 10 ASCII String	16	This is the name of FIFO 10. If the FIFO has no string name this shall be populated with 0h.
TELSTR-LOG-24	303:288	FIFO 11 ASCII String	16	This is the name of FIFO 11. If the FIFO has no string name this shall be populated with 0h.
TELSTR-LOG-25	319:304	FIFO 12 ASCII String	16	This is the name of FIFO 12. If the FIFO has no string name this shall be populated with 0h.
TELSTR-LOG-26	335:320	FIFO 13 ASCII String	16	This is the name of FIFO 13. If the FIFO has no string name this shall be populated with 0h.
TELSTR-LOG-27	351:336	FIFO 14 ASCII String	16	This is the name of FIFO 14. If the FIFO has no string name this shall be populated with 0h.
TELSTR-LOG-28	367:352	FIFO 15 ASCII String	16	This is the name of FIFO 15. If the FIFO has no string name this shall be populated with 0h.
TELSTR-LOG-29	383:368	FIFO 16 ASCII String	16	This is the name of FIFO 16. If the FIFO has no string name this shall be populated with 0h.
TELSTR-LOG-30	431:384	Reserved	48	Shall be cleared to 0h.
TELSTR-LOG-31	(SITSZ * 4) + 431:432	Statistics Identifier String Table	SITSZ * 4	The format of the Statistics Identifier String Table can be seen in Section 4.8.15.3 Statistics Identifier String Table Entry .
TELSTR-LOG-32	(ESTSZ * 4) + (SITSZ * 4) + 431:SITSZ * 4) + 432	Event String Table	ESTSZ * 4	The format of the Event Identifier String Table can be seen in Section 4.8.15.4 Event Identifier String Table Entry .
TELSTR-LOG-33	(VUESTZ * 4) + (ESTSZ * 4) + (SITSZ * 4) + 431:ESTSZ * 4) + (SITSZ * 4) + 432	VU Event String Table	VUESTZ * 4	The format of the VU Event Identifier String Table can be seen in Section 4.8.15.5 VU Event Identifier String Table Entry .
TELSTR-LOG-34	(ASCTSZ * 4) + (VUESTZ * 4) +	ASCII Table	ASCTSZ * 4	The format of the ASCII table can be seen in Section 4.8.15.6 ASCII String Example .

Requirement ID	Byte Address	Field	# of Bytes	Field Description
	(ESTSZ * 4) + (SITSZ * 4) + 432: (VUESTZ * 4) + (ESTSZ * 4) + (SITSZ * 4) + 432			

A diagram of the Telemetry String log page format is as follows:



4.8.15.3 Statistics Identifier String Table Entry

The Statistic Identifier String Table enables translating from vendor unique statistic identifiers to ASCII labels. The format of an entry for the Statistic Identifier String Table Entry is in the following table:

Requirement ID	Byte Address	Field	# of Bytes	Field Description
STR-ID-1	1:0	Vendor Specific Statistic Identifier	2	Shall be set the Vendor Unique Statistic Identifier number.
STR-ID-2	2	Reserved	1	Shall be cleared to zero.
STR-ID-3	3	ASCII ID Length	1	Shall be set the number of ASCII Characters that are valid. This is a zero-based value so a value of 0h is 1 character.
STR-ID-4	11:4	ASCII ID offset	8	Shall be set to the offset from Dword 0/Byte 0 of the Start of the ASCII Table to the first character of the string for this Statistic Identifier string. This value is in Dwords.
STR-ID-5	15:12	Reserved	4	Shall be cleared to zero.

4.8.15.4 Event Identifier String Table Entry

The Event Identifier String Table enables translating from Event Identifier to ASCII labels. The format of an entry for the Event Identifier String Table Entry is in the following table:

Requirement ID	Byte Address	Field	# of Bytes	Field Description
STR-EV-1	0	Debug Event Class	1	Shall be set the Debug Class.
STR-EV-2	2:1	Event Identifier	2	Shall be set to the Event Identifier.
STR-EV-3	3	ASCII ID Length	1	Shall be set to the number of ASCII Characters that are valid. This is a zero-based value so a value of 0h is 1 character.
STR-EV-4	11:4	ASCII ID offset	8	This is the offset from Dword 0/ byte 0 of the start of the ASCII table to the ASCII data for this identifier. This value is in Dwords.
STR-EV-5	15:12	Reserved	4	Shall be cleared to zero.

4.8.15.5 VU Event Identifier String Table Entry

The VU Event Identifier String Table enables translating from VU Event Identifier to ASCII labels. The format of an entry for the VU Event Identifier String Table Entry is in the following table:

Requirement ID	Byte Address	Field	# of Bytes	Field Description
STR-VUEV-1	0	Debug Event Class	1	Shall be set the Debug Class.
STR-VUEV-2	2:1	VU Event Identifier	2	Shall be set to the VU Event Identifier.
STR-VUEV-3	3	ASCII ID Length	1	Shall be set to the number of ASCII Characters that are valid. This is a zero-based value so a value of 0h is 1 character.
STR-VUEV-4	11:4	ASCII ID offset	8	This is the offset from Dword 0/ byte 0 of the start of the ASCII table to the ASCII data for this identifier. This value is in Dwords.
STR-VUEV-5	15:12	Reserved	4	Shall be cleared to zero.

4.8.15.6 ASCII String Example

An ASCII ID Length/Decode example is shown in the following table:

Byte	Data Byte	ASCII Character
400	54h	T
401	45h	E
402	53h	S
403	54h	T
404	20h	<space>
405	45h	E
406	58h	X
407	41h	A
408	4Dh	M
409	50h	P
410	4Ch	L
411	45h	E
412	21h	!
413	20h	<space>
414	20h	<space>
415	20h	<space>

In this example the ASCII ID Length is 0Ch, which is 12 decimal. This is a zero-based count and thus there are 13 characters to print. The first 13 characters shall be part of the ASCII output. Thus, the message to print is:

“TEST EXAMPLE!”

The last three ASCII <space> characters are not part of the ASCII output. They are only used for padding the string to the next Dword boundary. The last three ASCII characters of <space> are not part of the next string.

4.9 Host and Controller Initiated Telemetry Log Pages

The following requirements define a standardized format for Telemetry Data Area 1 and Telemetry Data Area 2 for both Telemetry Host-Initiated log page (Log Identifier 07h) and Telemetry Controller-Initiated log page (Log Identifier 08h).

4.9.1 Theory of Operation

This feature is designed to enable both customers and vendors to have increased visibility into monitoring and debugging devices.

4.9.2 Data Partitioning Overview

The data provided by the device for debugging is broken into two categories. There is data that impacts I/O and data that does not impact I/O. The data generated by the device for monitoring and/or debugging which does not impact I/O (performance/latency) for active commands in progress goes into Telemetry Data Area 1. The data generated by the device for monitoring and/or debugging which impacts I/O (performance/latency) for active commands in progress goes into Telemetry Data Area 2. The data format in the Telemetry Host-Initiated log page and the Telemetry Controller-Initiated log page shall be the same format (see Section 4.6.16.1 Telemetry Data Format).

The information (i.e., statistics and events) reported in Telemetry Host-Initiated Data Areas 1 and 2 shall be the same as Telemetry Controller-Initiated Data Areas 1 and 2. There is no requirement that the data contents of Telemetry Host-Initiated Data Areas 1 and 2 be the same as the data contents of Telemetry Controller-Initiated Data Areas 1 and 2 because each log page is captured by different events, and each log page reports current data (e.g., counts of commands processed) at the time of capture. In addition, the order of statistic descriptors (see Section 4.9.10 Statistic Descriptor) and the order of event descriptors (see Section 4.9.14.1 Event Descriptor) are both allowed to differ between the two log pages.

4.9.3 Statistic Area

The Statistic Area contains a group of Statistic Descriptors. The Statistic Descriptors may be counters or other statistics where each statistic is a value with a statistic size. The attributes associated with each of these statistics are Statistic Identifier, Behavior Type (see [STD-LOG-12](#)) and the length of the data field associated with the Statistic Identifier.

4.9.4 Event FIFO

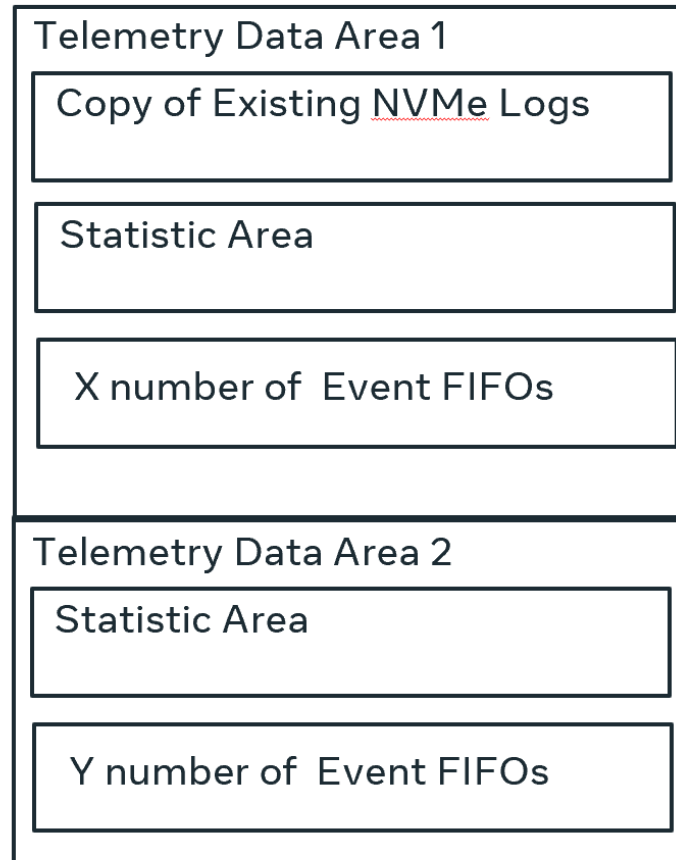
The Event FIFO is a queue that contains events that are generated. There is a total of up to 16 independent Event FIFO queues that may be configured between Telemetry Data Area 1 and Telemetry Data Area 2. It should be noted that the ordering relationship of events in the event FIFO is determined by the device.

4.9.5 Existing NVMe Log Pages

There are many existing NVMe log pages that are useful for monitoring the device. Some log pages have been overlaid into Telemetry Data Area 1 (see [TEL-23](#)). This is done to enable all the monitoring information to be gathered when polling Telemetry Data Area 1.

4.9.6 Debug Structure Overview Summary

The debug structure for Telemetry Data Area 1 and 2 can be seen in the following figure. The order of the Statistics and FIFOs are configurable, and both orders are acceptable.



4.9.7 Telemetry Data Requirements

The following applies to telemetry logging as the ability to quickly debug failures is required:

Requirement ID	Description
TEL-1	The device shall track the operational/event history and any critical parameters that can be used to debug issues.
TEL-2	The vendor shall provide a table that categorizes the reason identifiers that are a super set of the Error IDs in EREC-4 .
TEL-3	Obsolete. See STD-LOG-23 .
TEL-4	The Reason Identifier field (in the Telemetry Controller-Initiated log page and the Telemetry Host-Initiated log page) shall be the most recent failure identifier and shall not be cleared by a power cycle, reset, or any other mechanism.
TEL-5	The following table provides the specifications for the Telemetry Controller-Initiated log page and the Telemetry Host-Initiated log page Data Areas 1 and 2. Any vendor-specific data

Requirement ID	Description			
	required for root-cause analysis shall be included in Telemetry Data Area 3. If the vendor-specific data required for root-cause analysis does not fit within Telemetry Data Area 3, then the additional vendor-specific data shall be included in Telemetry Data Area 4. See TEL-26 for additional requirements that apply to use of Telemetry Data Area 4.			
	Telemetry Data Area	Purpose	Profile 0 Data Area Size	Latency Impact to IO
	1	Periodic logging for monitoring trends/problems	32,768 bytes	< 1 ms typical, < 5 ms max
	2	Logging for debug items that impact latency	-	Greater Telemetry Data Area 1 Requirement
	3	Optional Vendor Unique	-	-
	4	Optional Vendor Unique	-	-
TEL-6	The device shall set the Telemetry Host-Initiated Data Area 1 Last Block field of the Telemetry Host-Initiated log page (Log Identifier 07h) to 0040h as the factory default.			
TEL-7	The device shall set the Telemetry Controller-Initiated Data Area 1 Last Block field of the Telemetry Controller-Initiated log page (Log Identifier 08h) to 0040h as the factory default.			
TEL-8	Information that is used to populate Telemetry Data Area 1 shall be updated in the background at least once every ten minutes.			
TEL-9	If the device supports an encrypted log for debug this may be contained in Telemetry Data Area 3 and/or 4.			
TEL-10	The number of Timestamp Events inserted into the Event FIFOs shall be sufficient to debug.			
TEL-11	For any issue that causes the controller to generate the Telemetry Controller-Initiated log page, the complete contents of each of the Telemetry Controller-Initiated log page and Telemetry Host-Initiated log page shall contain all of the debug information needed to root cause the issue.			
TEL-12	Updating the Error ID in the TELRI-1 Reason Identifier field shall cause a Telemetry Log Changed event.			
TEL-13	When the device encounters a failure/error the Error ID in TELRI-1 shall be a non-zero value.			
TEL-14	Data in Telemetry Data Area 1 and Telemetry Data Area 2 as defined in this specification shall be decodable by the OCP plugin for the nvme-cli tool (version 2.10 or later) and shall meet the requirements for SEC-22 .			
TEL-15	Telemetry Data Area 1 and Telemetry Data Area 2 shall be supported per this specification.			
TEL-16	A minimum of two Telemetry Profiles shall be supported.			
TEL-17	Telemetry Profile 0 shall be the default profile from the factory.			
TEL-18	Telemetry Profile 1 shall be sized for maximum debuggability.			
TEL-19	The device shall support TP4109a to enable the host to access specific host telemetry.			

Requirement ID	Description
TEL-20	On a firmware update the Vendor Specific Statistics Identifier, the Debug Event Class/Events Identifier combinations and the Debug Class/VU Event Identifier combinations shall not be re-purposed or removed from the Telemetry String log page. This is to ensure on a firmware update that any existing Telemetry String log page is able to be decoded correctly.
TEL-21	Telemetry Controller-Initiated log pages shall only be generated (Telemetry Controller-Initiated Data Available transitions from 00h to 01h) for error conditions (e.g., they shall not be generated periodically, or in response to Percentage Used changes, etc.).
TEL-22	The Telemetry Controller-Initiated log page and Telemetry Host-Initiated log page shall be NVM subsystem in scope.
TEL-23	Statistics that are listed in the Description column in the table in Section 4.9.11 Statistic Identifiers as coming from the SMART / Health Extended log page (Log Identifier C0h), SMART / Health Information log page (Log Identifier 02h), or Endurance Group Information log page (Log Identifier 09h) shall be implemented and shall be in Data Area 1.
TEL-24	For the Statistics in TEL-23, the device shall populate the Telemetry String Log with strings that exactly match the text in the Statistic Specific Data Field column in the table in Section 4.9.11 Statistic Identifiers .
TEL-25	For the statistics in TEL-23, in the Statistic Information Field, the Host Hint Type shall be set to a value of Host Hint Type 1. For all other statistics descriptors, the Host Hint Type shall be set to a value of No Host Hint.
TEL-26	If the device uses Telemetry Data Area 4 (see TEL-5), then the device shall set the Data Area 4 Support bit to 1b in the Log Page Attributes field of Identify Controller. The host is required to set the Extended Telemetry Data Area 4 supported bit to 1b in the Host Behavior Support feature before requesting data from Telemetry Data Area 4.

4.9.8 Telemetry Reason Identifier Format

The format of the Reason Identifier shall be as follows:

Requirement ID	Byte Address	# of Bytes	Field	Field Description	
TELRI-1	63:0	64	Error ID	The device shall set a unique Error ID defining the persistent or transient error at the time of log capture.	
TELRI-2	71:64	8	File ID	File name or hash of the source file where the error occurred. Clear to zero if not applicable.	
TELRI-3	73:72	2	Line Number	Line Number in the source file where the error occurred. Clear to zero if not applicable.	
TELRI-4	74	1	Valid Flags	Bit	Bit Description
				7:4	Reserved. Shall be cleared to zero.
				3	VU Reason Extension Field is valid.

Requirement ID	Byte Address	# of Bytes	Field	Field Description	
				2	Shall be set to 1b if the Error ID is valid. Shall be cleared to 0b if Error ID is not valid.
				1	Shall be set to 1b if the File ID is valid. Shall be cleared to 0b if File ID is not valid.
				0	Shall be set to 1b if the Line Number is valid. Shall be cleared to 0b if Line Number is not valid.
TELRI-5	95:75	21	Reserved	Shall be cleared to zero.	
TELRI-6	127:96	32	VU Reason Extension	Vendor Unique reason code.	

4.9.9 Debug Profiles

There are many ways to configure Data Area 1, Data Area 2, the Statistics and Event FIFOs. Depending on the problem being investigated different configurations of these fields may be desired. Debug profiles are the mechanism that can address this challenge. The device will list the number of debug profiles supported. The host may then configure the profile based on the problem being investigated.

4.9.10 Statistic Descriptor

The format of the Statistic Descriptor is in the following table:

Requirement ID	Byte Address	Field	# of Bytes	Field Description		
STATF-1	1:0	Statistic Identifier	2	Shall contain the identifier that defines the data format of this entry.		
STATF-2	2	Statistic Information	1	Bit	Bit Description	
				7	Reserved. Shall be cleared to zero.	
				6	For Context Index Statistic Descriptors, this field shall be set to 1b. For all other descriptors this field shall be cleared to 0b.	
				5:4	Host Hint Type. The decode for Host Hint Type is as follows:	
					Value	Description
					0000h	No Host Hint
0001h	Host Hint Type 1					

Requirement ID	Byte Address	Field	# of Bytes	Field Description		
					0002h	Reserved
					0003h	Reserved
					This field is used for host decoding information. TEL-25 describes the requirements of what value shall be in this field.	
				3:0	Behavior Type (see STD-LOG-12)	
STATF-3	3	Namespace Information	1	Bit	Bit Description	
				7	Namespace Information Valid. When set to 1b the Namespace Identifier in STATF-3 and STATF-5 is valid. When cleared to 0b the Namespace Identifier is not valid	
				6:0	Namespace Identifier[6:0]. When Namespace Information Valid is set to 1b this is the Namespace Identifier (NS ID[6:0]). When Namespace Information Valid is cleared to 0b this field is not valid and shall be cleared to 0h.	
STATF-4	5:4	Statistic Data Size	2	Shall contain the number of Dwords that is used by the Statistic Specific Data field. Valid values for this field are 0h to FFFFh.		
STATF-5	7:6	Namespace Identifier[15:0]	2	When Namespace Information Valid is set to 1b this is the Namespace Identifier (NS ID[15:0]). When Namespace Information Valid is cleared to 0b this field is not valid and shall be cleared to 0h.		
STATF-6	(Statistic Data Size *4)+7:8	Statistic Specific Data	Statistic Data Size *4	Shall contain data specific extended information for this Statistic Data Entry type if this exists.		

4.9.11 Statistic Identifiers

The definitions of the Statistic Identifiers are in the following table. In addition to the Statistic Identifiers required elsewhere (e.g., [TEL-23](#)), any Statistic Identifiers that provide value to the vendor in debugging the device should be implemented.

Requirement ID	Statistic Identifier	Recommended Behavior Type	# of Dwords	Statistic Specific Data Field	Description
STATI-1	0000h	-	-	-	Reserved

Requirement ID	Statistic Identifier	Recommended Behavior Type	# of Dwords	Statistic Specific Data Field	Description
STATI-2	0001h	1	1	Outstanding Admin Commands	Number of outstanding Admin commands submitted by the host which have not been processed by the controller. Pulled from Submission Queue but not yet pushed to the Completion Queue. This count shall not include Asynchronous Event Request (AER) commands.
STATI-3	0002h	1	1	Host Write Bandwidth	The percentage of the current write bandwidth allowed to the NAND backend due to host writes.
STATI-4	0003h	1	1	GC Write Bandwidth	The percentage of the current write bandwidth allowed to the NAND backend due to internal writes. STATI-3 and STATI-4 shall add to 100%.
STATI-5	0004h	1	1	Active Namespaces	Shall be the number of Active Namespaces attached to the primary controller.
STATI-6	0005h	5	2	Internal Write Workload	Number of outstanding LBAs corresponding to the Internal Write Queue Depth (see STATI-8).
STATI-7	0006h	5	2	Internal Read Workload	Number of outstanding LBAs corresponding to the Internal Read Queue Depth (see STATI-9).
STATI-8	0007h	5	1	Internal Write Queue Depth	Number of outstanding Write commands submitted by the host which have not been processed by the controller. Pulled from Submission Queue but not yet pushed to the Completion Queue.
STATI-9	0008h	5	1	Internal Read Queue Depth	Number of outstanding Read commands submitted by the host which have not been processed by the controller. Pulled from Submission Queue but not yet pushed to the Completion Queue.
STATI-10	0009h	5	2	Pending Trim LBA Count	From a device perspective this is the current number of LBAs pending

Requirement ID	Statistic Identifier	Recommended Behavior Type	# of Dwords	Statistic Specific Data Field	Description
					completion of the background trim process due to host Dataset Management – Deallocate commands.
STATI-11	000Ah	4	2	Host Trim LBA Request Count	Number of LBAs that have been requested by Dataset Management – Deallocate command since last Telemetry Log collection. This shall not include other commands that result in de-allocation.
STATI-12	000Bh	1	1	Current NVMe Power State	Currently set NVMe Power State Descriptor at the time of this Telemetry Log collection.
STATI-13	000Ch	1	1	Current DSSD Power State	Currently set DSSD Power State Descriptor at the time of this Telemetry Log collection.
STATI-14	000Dh	4	2	Program Fail Count	The number of program operation failure events for the life of the device.
STATI-15	000Eh	4	2	Erase Fail Count	The number of erase operation failure events for the life of the device.
STATI-16	000Fh	4	4	Read Disturb Writes	Number of bytes written due to read disturb relocations for the life of the device.
STATI-17	0010h	4	4	Retention Writes	Number of bytes written due to retention relocation for the life of the device.
STATI-18	0011h	4	4	Wear Leveling Writes	Number of bytes written due to wear leveling for the life of the device.
STATI-19	0012h	4	2	Read Recovery Writes	Number of bytes written due to read recovery for the life of the device.
STATI-20	0013h	1	2	GC Writes	Number of bytes written due to garbage collection since last Telemetry Log collection using by reading either host-initiated or controller-initiated log.

Requirement ID	Statistic Identifier	Recommended Behavior Type	# of Dwords	Statistic Specific Data Field	Description										
STATI-21	0014h	4	1	SRAM Correctable Count	Total number of correctable errors due to device SRAM single error correction over the device lifetime.										
STATI-22	0015h	4	1	DRAM Correctable Count	Total number of correctable errors due to device DRAM single error correction over the life of the device.										
STATI-23	0016h	4	1	SRAM Uncorrectable Count	Total number of uncorrectable errors due to device SRAM double error detection.										
STATI-24	0017h	4	1	DRAM Uncorrectable Count	Total number of uncorrectable errors due to device DRAM double error detection.										
STATI-25	0018h	4	1	Data Integrity Error Count	Total number of data integrity errors due to FTL metadata integrity checks.										
STATI-26	0019h	4	1	Read Retry Error Count	The number of reads for the device lifetime performed on the flash because of error correction (e.g., Read retries, LDPC iterations, etc.).										
STATI-27	001Ah	4	1	PERST# Events Count	Number of PERST# events processed by the NVM Subsystem for the lifetime of the device. This count shall only increment if the CC.EN bit is set to 1b.										
STATI-28	001Bh	4	2	Max Die Bad Block	This information is based on a single die which has the largest number of bad blocks: <table><tr><th>Byte Address</th><th>Byte Description</th></tr><tr><td>0</td><td>Worst Die % of bad blocks, where the range is from 0-100%.</td></tr><tr><td>1</td><td>Reserved</td></tr><tr><td>3:2</td><td>Worst Die Raw Number of bad blocks</td></tr><tr><td>7:4</td><td>Reserved. Cleared to 0h.</td></tr></table>	Byte Address	Byte Description	0	Worst Die % of bad blocks, where the range is from 0-100%.	1	Reserved	3:2	Worst Die Raw Number of bad blocks	7:4	Reserved. Cleared to 0h.
Byte Address	Byte Description														
0	Worst Die % of bad blocks, where the range is from 0-100%.														
1	Reserved														
3:2	Worst Die Raw Number of bad blocks														
7:4	Reserved. Cleared to 0h.														

Requirement ID	Statistic Identifier	Recommended Behavior Type	# of Dwords	Statistic Specific Data Field	Description	
STATI-29	001Ch	4	2	Max NAND Channel Bad Block	This information is based on the dies in a single NAND channel which has the largest number of bad blocks:	
					Byte Address	Byte Description
					0	Worst NAND Channel % of bad blocks, where the range is 0-100%
					1	Reserved
					3:2	Worst NAND Channel Number of bad blocks
					7:4	Reserved. Cleared to 0h.
STATI-30	001Dh	4	2	Minimum NAND Channel Bad Block	This information is based on the dies in a single NAND channel which has the smallest number of bad blocks:	
					Byte Address	Byte Description
					0	Best NAND Channel % of bad blocks where the range is 0-100%
					1	Reserved
					3:2	Best NAND Channel Number of bad blocks
					7:4	Reserved. Cleared to 0h.
STATI-33	001Eh	4	4	Physical Media Units Written	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).	
STATI-34	001Fh	4	4	Physical Media Units Read	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).	
STATI-35	0020h	4	2	Bad User NAND Blocks	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).	
STATI-36	0021h	4	2	Bad System NAND Blocks	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).	

Requirement ID	Statistic Identifier	Recommended Behavior Type	# of Dwords	Statistic Specific Data Field	Description
STATI-37	0022h	4	2	XOR Recovery Count	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-38	0023h	4	2	Uncorrectable Read Error Count	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-39	0024h	4	2	Soft ECC Error Count	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-40	0025h	4	2	End to End Correction Counts	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-41	0026h	4	1	System Data % Used	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-42	0027h	4	2	Refresh Counts	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-43	0028h	4	2	User Data Erase Counts	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-44	0029h	4	1	Thermal Throttling Status and Count	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-45	002Ah	4	2	DSSD Specification Version	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-46	002Bh	4	2	PCIe Correctable Error Count	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-47	002Ch	4	1	Incomplete Shutdowns	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-48	002Dh	4	1	% Free Blocks	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).

Requirement ID	Statistic Identifier	Recommended Behavior Type	# of Dwords	Statistic Specific Data Field	Description
STATI-49	002Eh	4	1	Capacitor Health	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-50	002Fh	4	1	NVM Express Base Errata Version	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-51	0030h	4	1	NVM Command Set Errata Version	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-52	0031h	4	1	NVM Express Management Interface Errata Version	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-53	0032h	4	2	Unaligned I/O	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-54	0033h	4	2	Security Version Number	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-55	0034h	4	2	Total NUSE	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-56	0035h	4	1	PLP Start Count	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-57	0036h	4	4	Endurance Estimate	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-58	0037h	4	2	PCIe Link Retraining Count	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-59	0038h	4	2	Power State Change Count	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-60	0039h	4	4	Lowest Permitted Firmware Revision	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).

Requirement ID	Statistic Identifier	Recommended Behavior Type	# of Dwords	Statistic Specific Data Field	Description
STATI-61	003Ah	4	1	Log Page Version	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-62	003Bh	4	1	Media Dies Offline	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-63	003Ch	4	1	Max Temperature Recorded	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-64	003Dh	4	2	NAND Avg. Erase Count	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-65	003Eh	4	2	Command Timeouts	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-66	003Fh	4	2	System Area Program Fail Count	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-67	0040h	4	2	System Area Read Fail Count	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-68	0041h	4	2	System Area Erase Fail Count	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-69	0042h	4	1	Max Peak Power Capability	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-70	0043h	4	1	Current Average Power	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-71	0044h	4	2	Lifetime Power Consumed	This is the value of this field in the SMART / Health Extended log page (Log Identifier C0h).
STATI-72	0045h	4	1	Error / Assert Count	The number of Panics / Asserts the device has encountered during its lifetime. This is a saturating counter.
STATI-73	0046h	4	4	Device Busy Time	Contains the amount of time the device is busy with I/O commands.

Requirement ID	Statistic Identifier	Recommended Behavior Type	# of Dwords	Statistic Specific Data Field	Description
					The device is busy when there is a command outstanding to an I/O Queue (specifically, a command was issued via an I/O Submission Queue Tail doorbell write and the corresponding completion queue entry has not been posted yet to the associated I/O Completion Queue) on any NVMe controller. This value is reported in minutes.
STATI-74	0047h	4	1	Critical Warning	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-75	0048h	4	1	Composite Temperature	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-76	0049h	4	1	Available Spare	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-77	004Ah	4	1	Available Spare Threshold	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-78	004Bh	4	1	Percentage Used	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-79	004Ch	4	1	Endurance Group Critical Warning Summary	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-80	004Dh	4	4	Data Units Read	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-81	004Eh	4	4	Data Units Written	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-82	004Fh	4	4	Host Read Commands	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).

Requirement ID	Statistic Identifier	Recommended Behavior Type	# of Dwords	Statistic Specific Data Field	Description
STATI-83	0050h	4	4	Host Write Commands	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-84	0051h	4	4	Controller Busy Time	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-85	0052h	4	4	Power Cycles	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-86	0053h	4	4	Power On Hours	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-87	0054h	4	4	Unsafe Shutdowns	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-88	0055h	4	4	Media and Data Integrity Errors	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-89	0056h	4	4	Number Of Error Information Log Entries	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-90	0057h	4	1	Warning Composite Temperature Time	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-91	0058h	4	1	Critical Composite Temperature Time	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-92	0059h	4	1	Temperature Sensor 1	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-93	005Ah	4	1	Temperature Sensor 2	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).

Requirement ID	Statistic Identifier	Recommended Behavior Type	# of Dwords	Statistic Specific Data Field	Description
STATI-94	005Bh	4	1	Temperature Sensor 3	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-95	005Ch	4	1	Temperature Sensor 4	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-96	005Dh	4	1	Temperature Sensor 5	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-97	005Eh	4	1	Temperature Sensor 6	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-98	005Fh	4	1	Temperature Sensor 7	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-99	0060h	4	1	Temperature Sensor 8	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-100	0061h	4	1	Thermal Management Temperature 1 Transition Count	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-101	0062h	4	1	Thermal Management Temperature 2 Transition Count	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-102	0063h	4	1	Total Time For Thermal Management Temperature 1	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-103	0064h	4	1	Total Time For Thermal Management Temperature 2	This is the value of this field in the SMART / Health Information log page (Log Identifier 02h).
STATI-104	0065h	4	1	Endurance Estimate	This is the value of this field in the Endurance Group Information log page (Log Identifier 09h).

Requirement ID	Statistic Identifier	Recommended Behavior Type	# of Dwords	Statistic Specific Data Field	Description
STATI-105	0066h	4	4	Data Units Read	This is the value of this field in the Endurance Group Information log page (Log Identifier 09h).
STATI-106	0067h	4	4	Data Units Written	This is the value of this field in the Endurance Group Information log page (Log Identifier 09h).
STATI-107	0068h	4	4	Media Units Written	This is the value of this field in the Endurance Group Information log page (Log Identifier 09h).
STATI-108	0069h	4	4	Number of Error Information Log Entries	This is the value of this field in the Endurance Group Information log page (Log Identifier 09h).
STATI-109	006Ah	4	1	Form Factor	This is the value of this field in the SMART / Health Information log page (Log Identifier C0h).
STATI-110	006Bh	4	2	Dies In Use Bad NAND Blocks	This is the value of this field in the SMART / Health Information log page (Log Identifier C0h).
STATI-111	006Ch	4	1	Proactive Bad Die Retirement	This is the value of this field in the SMART / Health Information log page (Log Identifier C0h).
STATI-112	006Dh	1	2 + N	Namespace ID Context Statistic Descriptor	This Context Statistic Descriptor contains other Statistic Descriptors that describe the specified namespace (see Section 4.9.12.2.1 Namespace ID Context). The total size of this Context Statistic Descriptor is 2 Dwords plus the total size of the encapsulated Statistics Descriptors (N).
STATI-113	006Eh	1	2 + N	Controller ID Context Statistic Descriptor	This Context Statistic Descriptor contains other Statistic Descriptors that describe the specified controller (see Section 4.9.12.2.2 Controller ID Context). The total size of this Context Index Statistic Descriptor is 2 Dwords plus

Requirement ID	Statistic Identifier	Recommended Behavior Type	# of Dwords	Statistic Specific Data Field	Description
					the total size of the encapsulated Statistics Descriptors (N).
STATI-114	006Fh	1	2 + N	Queue ID Context Statistic Descriptor	This Context Statistic Descriptor contains other Statistic Descriptors that describe the specified queue attached to the specified controller (see Section 4.9.12.2.3 Queue ID Context). The total size of this Context Index Statistic Descriptor is 2 Dwords plus the total size of the encapsulated Statistics Descriptors (N).
STATI-31	0070h - 7FFFh	...	...	Reserved	Statistic Identifiers between 0070h and 7FFFh are reserved for future expansion.
STATI-32	8000h - FFFFh	...	...	Vendor Unique	Statistic Identifier's between 8000h and FFFFh are vendor unique.

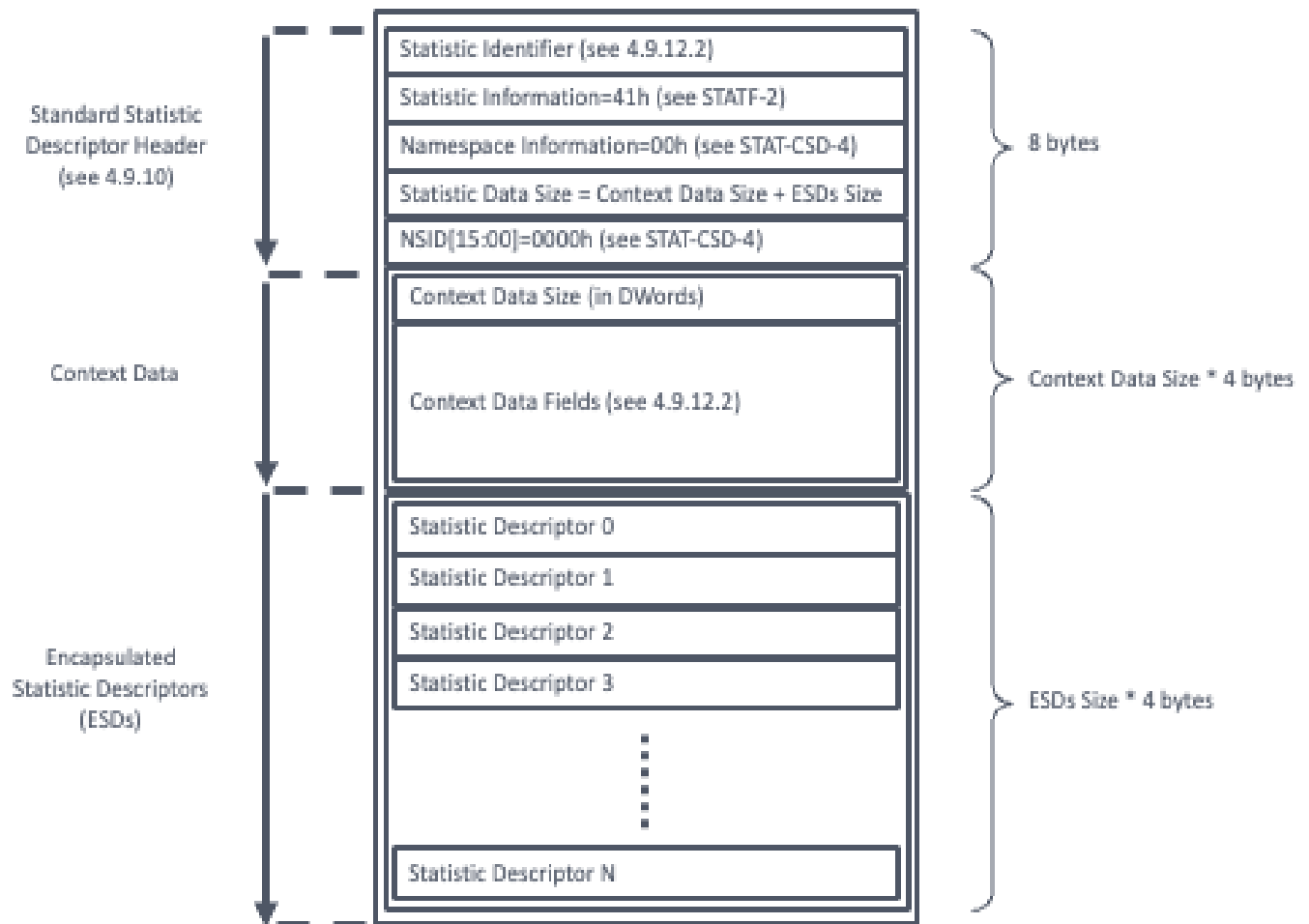
4.9.12 Context Statistic Descriptor

Context Statistic Descriptors encapsulate other Statistic Descriptors and provide additional context information about the source of the data. The Statistic Identifier value defines the type of context provided by the Context Statistic Descriptor, and the Context Value field(s) define the specific context for the encapsulated data. Statistic Descriptors for namespaces should continue to use the NSID field unless the identifier exceeds the 16-bit field limit of the NSID field.

4.9.12.1 Context Statistic Descriptor Requirements

Requirement ID	Description
STAT-CSD-1	The first Dword of the Statistic Specific Data field (see STATF-6) shall contain the number of Dwords in the Context Data and shall be greater than zero. The Context Data includes the Context Data Size field and the Context Data Fields, as shown in the Context Statistic Descriptor Layout Figure .
STAT-CSD-2	The size and format of the Context Data in a Context Statistic Descriptor are determined by the Statistic Identifier value. Context Data Fields are defined for each context type in Section 4.9.12.2 Context Types .
STAT-CSD-3	Encapsulated Statistic Descriptors within a Context Statistic Descriptor shall not include any Context Statistic Descriptors.
STAT-CSD-4	The Namespace Information field (see STATF-3) and Namespace Identifier[15:0] field (see STATF-5) in a Context Statistic Descriptor shall be cleared to 0h. Encapsulated Statistic Descriptors are able to use the Namespace Information and Namespace Identifier fields.

Context Statistic Descriptor Layout Figure



4.9.12.2 Context Types

This section defines the Index Context types that can be used to provide context information for Statistic Descriptors. These data structures follow the 2-Dword header for all Statistic Descriptors (see [Section 4.9.10 Statistic Descriptor](#)).

4.9.12.2.1 Namespace ID Context (Statistic Identifier 6Dh)

Requirement ID	Byte Address	Field	# of Bytes	Field Description
CTX-NS-1	1:0	Context Data Size	2	The number of Dwords in the context data, including this field. This field shall be set to 2h for this Context Type.

Requirement ID	Byte Address	Field	# of Bytes	Field Description
CTX-NS-2	3:2	Reserved	2	Shall be cleared to 0h.
CTX-NS-3	7:4	Namespace ID	4	This field shall be set to the Namespace ID of the namespace to which the encapsulated Statistic Descriptors apply.
CTX-NS-4	((Statistic Data Size – 2) * 4) + 7:8	Encapsulated Statistic Descriptors	((Statistic Data Size – 2) * 4)	This field shall contain one or more Statistic Descriptors whose data corresponds to the namespace indicated in the Namespace ID field.

4.9.12.2.2 Controller ID Context (Statistic Identifier 6Eh)

Requirement ID	Byte Address	Field	# of Bytes	Field Description
CTX-CTLR-1	1:0	Context Data Size	2	The number of Dwords in the context data, including this field. This field shall be set to 2h for this Context Type.
CTX-CTLR-2	5:2	Reserved	4	Shall be cleared to 0h.
CTX-CTLR-3	7:6	Controller ID	2	This field shall be set to the Controller ID of the controller to which the encapsulated Statistic Descriptors apply.
CTX-CTLR-4	((Statistic Data Size – 2) * 4) + 7:8	Encapsulated Statistic Descriptors	((Statistic Data Size – 2) * 4)	This field shall contain one or more Statistic Descriptors whose data corresponds to the controller indicated in the Controller ID field.

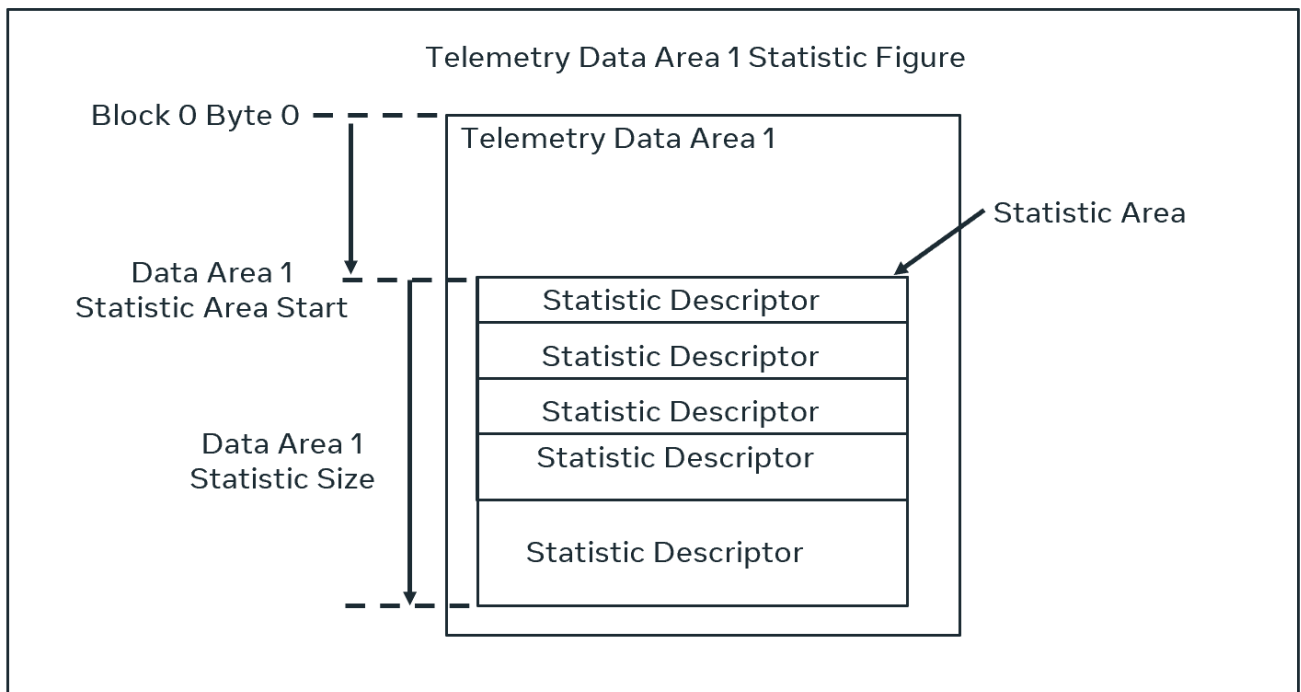
4.9.12.2.3 Queue ID Context (Statistic Identifier 6Fh)

Requirement ID	Byte Address	Field	# of Bytes	Field Description
CTX-QUEUE-1	1:0	Context Data Size	2	The number of Dwords in the context data, including this field. This field shall be set to 2h for this Context Type.
CTX-QUEUE-2	3:2	Reserved	2	Shall be cleared to 0h.
CTX-QUEUE-3	5:4	Controller ID	2	This field shall be set to the Controller ID of the controller that contains the queue identified in the Queue ID field.

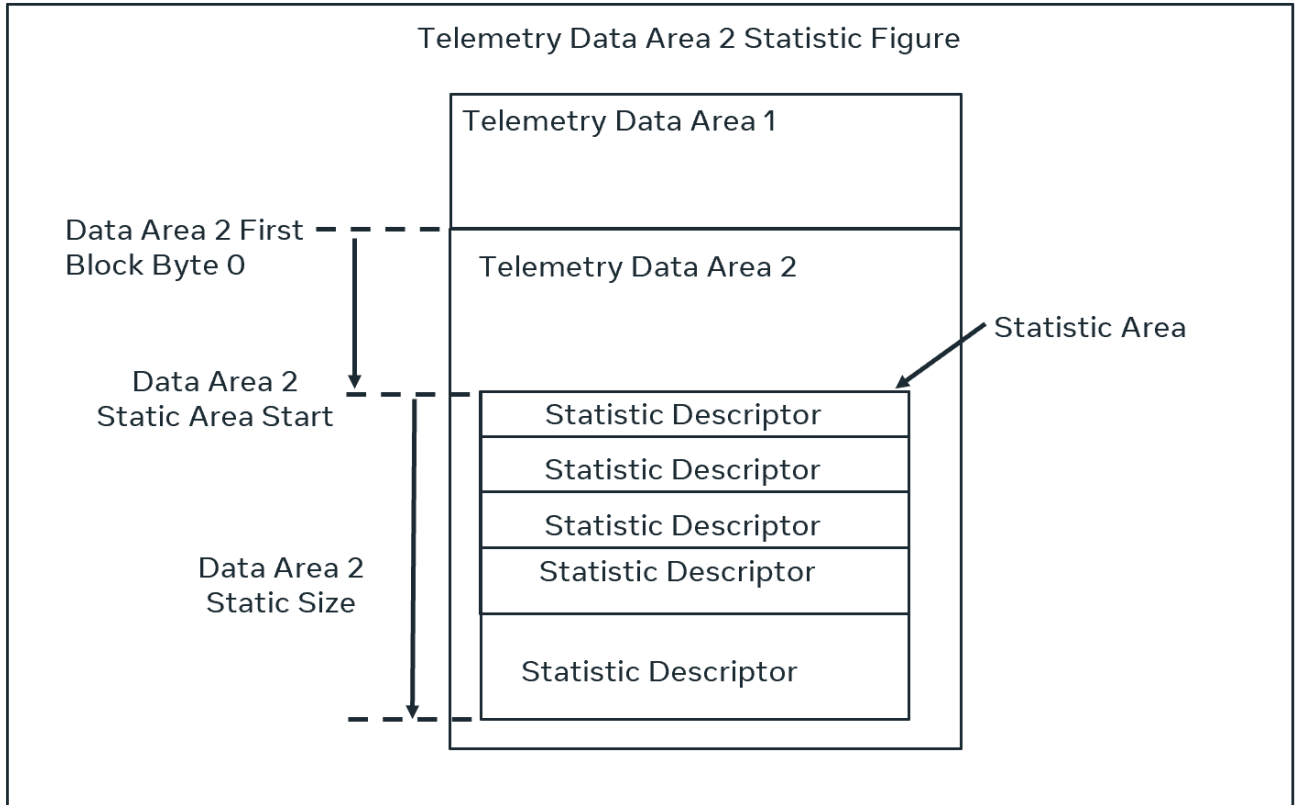
Requirement ID	Byte Address	Field	# of Bytes	Field Description
CTX-QUEUE-4	7:6	Queue ID	2	This field shall be set to the Queue ID of the queue to which the encapsulated Statistic Descriptors apply.
CTX-QUEUE-5	$((\text{Statistic Data Size} - 2) * 4) + 7:8$	Encapsulated Statistic Descriptors	$((\text{Statistic Data Size} - 2) * 4)$	This field shall contain one or more Statistic Descriptors whose data corresponds to the queue indicated in the Queue ID field.

4.9.13 Statistic Descriptor Location

The Statistic Area location in Telemetry Data Area 1 can be found by using the Data Area 1 Statistic Area 1 Start and Data Area 1 Statistic Area 1 Size. This can be seen in the following Data Area 1 Statistics Figure:



The Statistic Area location in Data Area 2 can be found by using the Data Area 2 Statistic Area Start and Data Area 2 Statistic Size. This can be seen in the following Data Area 2 Statistic Figure:



4.9.14 Statistic Requirements

Requirement ID	Description
SDL-1	Statistic Area 1 shall not cross from Telemetry Data Area 1 to Telemetry Data Area 2.
SDL-2	Bytes in the Statistics Areas that are not contained in a Statistic Descriptor shall be zero.
SDL-3	The decode of the Statistic Identifiers shall be provided to the customer via the Telemetry String log page.

4.9.15 Event FIFO Requirements

4.9.15.1 Event Descriptor

The Event Descriptor is used to log debug events in the Event FIFOs:

Requirement ID	Byte Address	Field	# of Bytes	Field Description
EVENTD-1	0	Debug Event Class Type	1	Shall contain the corresponding Event Class Type for this event.
EVENTD-2	2:1	Event Identifier	2	Shall contain the corresponding Event ID for this event.

Requirement ID	Byte Address	Field	# of Bytes	Field Description
EVENTD-3	3	Event Data Size	1	Shall contain the number of Dwords that is used by the Event Specific Data field.
EVENTD-4	(Event Data Size * 4) + 3:4	Event Specific Data	Event Data Size * 4	Shall contain event specific extended information for this event (if any).

4.9.15.2 Event Classes

This section defines the Event Class information that can be used to debug issues with the device.

4.9.15.2.1 Debug Event Class Types

Debug Event Class Code	Description
00h	Reserved
01h	Timestamp Debug Class
02h	PCIe Debug Class
03h	NVMe Debug Class
04h	Reset Debug Class
05h	Boot Sequence Debug Class
06h	Firmware Assert Debug Class
07h	Temperature Debug Class
08h	Media Debug Class
09h	Media Wear Class
0Ah	Statistic Snapshot Class
0Bh	Virtual FIFO Event Class
0Ch	SMBUS/I2C/I3C Event Class
0Dh	MCTP Event Class
7Fh-0Eh	Reserved
FFh-80h	Vendor Unique Class

4.9.15.2.2 Timestamp Debug Event Class Format

Requirement ID	Byte Address	Field	# of Bytes	Field Description
EVC-TS-1	0	Timestamp Debug Class	1	Shall be set to 01h.

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
EVC-TS-2	2:1	Event Identifier	2	Event ID	Description
				0000h	Host issued a Timestamp Set Feature Command (Feature ID Eh).
				0001h	Firmware initiated Timestamp Snapshot.
				0002h	Obsolete.
				0003h - 7FFFh	Reserved.
				8000h - FFFFh	Vendor Unique.
EVC-TS-3	3	Event Data Size	1	This field indicates the number of Dwords in the Event Specific Data field. If the VU Event Identifier field and VU data field do not exist then, then this field shall be set to 2h.	
Event Specific Data					
EVC-TS-4	11:4	Timestamp	8	Timestamp value based on Event ID, in the format defined in the NVM Express Base Specification.	
EVC-TS-5	13:12	VU Event Identifier	2	Vendor Unique Event Identifier. The VU Event Identifier that enables the VU Data field to be decoded.	
EVC-TS-6	(Event Data Size * 4) + 3:14	VU Data	(Event Data Size * 4) - 10	Vendor Unique Data. The size of this data is determined based on the Event Data Size if this field exists.	

4.9.15.2.3 PCIe Debug Event Class Format

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
EVC-PCI-1	0	PCIe Debug Class	1	Shall be set to 02h.	
EVC-PCI-2	2:1	Event Identifier	2	The device shall log PCIe Debug Events as follows:	
				Event ID	Description
				0000h	Link Up.
				0001h	Link Down.
				0002h	PCIe Error Detected.
				0003h	PERST# Asserted.
				0004h	PERST# De-asserted.

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
				0005h	Refclk Stable.
				0006h	Vmain Stable.
				0007h	Link Speed and Width Negotiated.
				0008h - 7FFFh	Reserved.
				8000h - FFFFh	Vendor Unique.
EVC-PCI-3	3	Event Data Size	1	This field indicates the number of Dwords in the Event Specific Data field. If the VU Event Identifier field and VU data field do not exist then, then this field shall be set to 1h.	
Event Specific Data					
EVC-PCI-4	7:4	PCIe Debug Event Data	4	For PCIe Debug Event ID 7, the device shall log the negotiated Link Speed and Width as follows:	
				Byte Address	Byte Description
				4	State changed flags: • 00h = Unchanged • 01h = Link Speed Changed • 02h = Link Width Changed • 03h - FFh = Reserved
				5	Link Speed: • 00h = Reserved • 01h = PCIe Gen1 • 02h = PCIe Gen2 • 03h = PCIe Gen3 • 04h = PCIe Gen4 • 05h = PCIe Gen5 • 06h = PCIe Gen6 • 07h = PCIe Gen7 • 08h - FFh = Reserved
6	Link Width: • 00h = Reserved • 01h = x1 • 02h = x2 • 03h = x4 • 04h = x8 • 05h = x16				

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
					06h - FFh = Reserved
				7	Reserved.
				For all other PCIe Debug Event IDs, this field shall be cleared to zero.	
EVC-PCI-5	9:8	VU Event Identifier	2	Vendor Unique Event Identifier. The VU Event Identifier that enables the VU data to be decoded.	
EVC-PCI-6	(Event Data Size * 4) + 3:10	VU Data	(Event Data Size * 4) – 6	Vendor Unique Data. The size of this data is determined based on the Event Data Size if this field exists.	

4.9.15.2.4 NVMe Debug Event Class Format

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
EVC-NVME-1	0	NVMe Debug Class	1	Shall be set to 03h.	
EVC-NVME-2	2:1	Event Identifier	2	The device shall log NVMe Debug Events as follows:	
				Event ID	Description
				0000h	CC.EN transitions from 0b to 1b.
				0001h	CC.EN transitions from 1b to 0b.
				0002h	CSTS.RDY transitions from 0b to 1b.
				0003h	CSTS.RDY transitions from 1b to 0b.
				0004h	Reserved
				0005h	Create I/O Submission Queue Command or Create I/O Completion Queue Command Processed successfully.
				0006h	In-band Admin Command Processed other than Create I/O Submission Queue Command or Create I/O Completion Queue Command Processed successfully.
				0007h	An Admin command returned a non-zero Status Code.
				0008h	An I/O Command Returned a Non-zero Status Code.
0009h	CSTS.CFS transitioned from 0b to 1b				

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
				000Ah	Admin Submission Queue Base Address Written (AQA) or Admin Completion Queue Based Address (ACQ) written.
				000Bh	Controller Configuration Register (CC) Changed except for the cases that are covered in 0000h and 0001h.
				000Ch	Controller Status Register (CSTS) Changed except for the cases that are covered in 0002h, 0003h, and 0009h.
				000Dh	Delete I/O Completion Queue Command or Delete I/O Submission Queue Command Processed.
				000Eh	Out-of-band Command Processed.
				000Fh	Out-of-band Asynchronous Event Message Transmitted.
				0010h	Error Reporting AEN was sent (see EREC-5).
				0011h - 7FFFh	Reserved.
				8000h - FFFFh	Vendor Unique.
EVC-NVME-3	3	Event Data Size	1	This field indicates the number of Dwords in the Event Specific Data field. If the VU Event Identifier field and VU data field do not exist then, then this field shall be set to 2h.	
Event Specific Data					
EVC-NVME-4	11:4	NVMe Debug Event Data	8	For NVMe Debug Event IDs 07h and 08h, the device shall log the NVMe Debug Event Data as follows:	
				Byte Address	Byte Description
				4	Command Opcode.
				6:5	The value of the Status field from CQE Dword 3 (DW3) shall be stored in bits 14:0 of this field and bit 15 of this field shall be cleared to 0b.
				8:7	Command Identifier (CID).
				10:9	Submission Queue Identifier (SQID).

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
				11	For Get Log Page, this field shall indicate the Log Page Identifier.
					For Get Features and Set Features, this field shall indicate the Feature Identifier.
					For NVMe-MI Send and NVMe-MI Receive, this field shall indicate the NVMe-MI Command Opcode.
					For all other commands, this field is reserved and shall be cleared to 0h.
				For NVMe Debug Event ID 0Bh the device shall log the NVMe Debug Event Data as follows:	
				Byte Address	Byte Description
				7:4	Controller Configuration Register.
				11:8	Reserved.
				For NVMe Debug Event ID 0Ch the device shall log the NVMe Debug Event Data as follows:	
				Byte Address	Byte Description
				7:4	Controller Status Register.
				11:8	Reserved.
				For NVMe Debug Event ID 0Eh the device shall log the NVMe Debug Event Data as follows:	
				Byte Address	Byte Description
				4	Command Opcode.
				6:5	For Admin Commands, the value of the Status field from CQEDW3 is stored in bits 14:0 of this field and bit 15 of this field shall be cleared to 0b. Cleared to 0h for all other commands.
				7	NVMe-MI Status Code.
				8	Byte 1 from the Request Message.
				9	Byte 2 from the Request Message.
				11:10	Reserved.

Requirement ID	Byte Address	Field	# of Bytes	Field Description				
				For NVMe Debug Event ID 0Fh the device shall log the NVMe Debug Event Data as follows:				
				<table><tr><th>Byte Address</th><th>Byte Description</th></tr><tr><td>11:4</td><td>Asynchronous Event Identifiers in the AEM for up to 8 Asynchronous Events where the first event that occurred is at offset 4, the second event that occurred is at offset 5, etc. If there are less than 8 AEs in the AEM, then unused bytes shall be cleared to 0h.</td></tr></table>	Byte Address	Byte Description	11:4	Asynchronous Event Identifiers in the AEM for up to 8 Asynchronous Events where the first event that occurred is at offset 4, the second event that occurred is at offset 5, etc. If there are less than 8 AEs in the AEM, then unused bytes shall be cleared to 0h.
				Byte Address	Byte Description			
11:4	Asynchronous Event Identifiers in the AEM for up to 8 Asynchronous Events where the first event that occurred is at offset 4, the second event that occurred is at offset 5, etc. If there are less than 8 AEs in the AEM, then unused bytes shall be cleared to 0h.							
For all other NVMe Debug Event IDs, this field shall be cleared to zero.								
EVC-NVME-5	13:12	VU Event Identifier	2	Vendor Unique Event Identifier. The VU Event Identifier that enables the VU data to be decoded.				
EVC-NVME-6	(Event Data Size * 4) + 3:14	VU Data	(Event Data Size * 4) – 10	Vendor Unique Data. The size of this data is determined based on the Event Data Size if this field exists.				

4.9.15.2.5 Reset Debug Event Class Format

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
EVC-RST-1	0	Reset Debug Class	1	Shall be set to 04h.	
EVC-RST-2	2:1	Event Identifier	2	The device shall log Reset Debug Events as follows:	
				Event ID	Description
				0000h	PCIe Conventional Hot Reset.
				0001h	Main Power Cycle.
				0002h	PERST#.
				0003h	PCIe Function Level Reset.
				0004h	NVM Subsystem Reset.
				0005h - 7FFFh	Reserved.
				8000h - FFFFh	Vendor Unique.

Requirement ID	Byte Address	Field	# of Bytes	Field Description
EVC-RST-3	3	Event Data Size	1	This field indicates the number of Dwords in the Event Specific Data field. If the VU Event Identifier field and VU data field do not exist then, then this field shall be set to 0h.
Event Specific Data				
EVC-RST-4	5:4	VU Event Identifier	2	Vendor Unique Event Identifier. The VU Event Identifier that enables the VU data to be decoded.
EVC-RST-5	(Event Data Size * 4) + 3:6	VU Data	(Event Data Size * 4) - 2	Vendor Unique Data. The size of this data is determined based on the Event Data Size if this field exists.

4.9.15.2.6 Boot Sequence Debug Event Class Format

Requirement ID	Byte Address	Field	# of Bytes	Field Description								
EVC-BS-1	0	Boot Sequence Debug Class	1	Shall be set to 05h.								
EVC-BS-2	2:1	Event ID	2	The device shall log Boot Sequence Debug Events as follows: <table><tr><th>Event ID</th><th>Description</th></tr><tr><td>0000h</td><td>Main Firmware Boot Complete. For a single controller subsystem, this is when all boot activities required to allow I/O commands to be processed are completed excluding the enablement of the controller. This is always after the FTL load from NVM Complete, FTL Rebuild Started and FTL Rebuild Completes events.</td></tr><tr><td>0001h</td><td>FTL Load from NVM Complete. This means the SSD downloaded the entire FTL table from NVM to internal memory (i.e., no journaling data is required to be loaded).</td></tr><tr><td>0002h</td><td>FTL Rebuild Started. This is after FTL Load from NVM has completed, if the FTL table is required to be rebuilt from journaling data, then mark the start.</td></tr></table>	Event ID	Description	0000h	Main Firmware Boot Complete. For a single controller subsystem, this is when all boot activities required to allow I/O commands to be processed are completed excluding the enablement of the controller. This is always after the FTL load from NVM Complete, FTL Rebuild Started and FTL Rebuild Completes events.	0001h	FTL Load from NVM Complete. This means the SSD downloaded the entire FTL table from NVM to internal memory (i.e., no journaling data is required to be loaded).	0002h	FTL Rebuild Started. This is after FTL Load from NVM has completed, if the FTL table is required to be rebuilt from journaling data, then mark the start.
Event ID	Description											
0000h	Main Firmware Boot Complete. For a single controller subsystem, this is when all boot activities required to allow I/O commands to be processed are completed excluding the enablement of the controller. This is always after the FTL load from NVM Complete, FTL Rebuild Started and FTL Rebuild Completes events.											
0001h	FTL Load from NVM Complete. This means the SSD downloaded the entire FTL table from NVM to internal memory (i.e., no journaling data is required to be loaded).											
0002h	FTL Rebuild Started. This is after FTL Load from NVM has completed, if the FTL table is required to be rebuilt from journaling data, then mark the start.											

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
				0003h	FTL Rebuild Complete. This means the FTL table is ready to fully support I/O commands.
				0004h - 7FFFh	Reserved.
				8000h - FFFFh	Vendor Unique.
EVC-BS-3	3	Event Data Size	1	This field indicates the number of Dwords in the Event Specific Data field. If the VU Event Identifier field and VU data field do not exist then, then this field shall be set to 0h.	
Event Specific Data					
EVC-BS-4	5:4	VU Event Identifier	2	Vendor Unique Event Identifier. The VU Event Identifier that enables the VU data to be decoded.	
EVC-BS-5	(Event Data Size * 4) +3:6	VU Data	(Event Data Size * 4) – 2	Vendor Unique Data. The size of this data is determined based on the Event Data Size if this field exists.	

4.9.15.2.7 Firmware Assert Debug Event Class Format

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
EVC-ASRT-1	0	Firmware Assert Debug Class	1	Shall be set to 06h.	
EVC-ASRT-2	2:1	Event Identifier	2	The device shall log Firmware Assert Debug Events as follows:	
				Event ID	Description
				0000h	Assert in NVMe Processing Code.
				0001h	Assert in Media Code.
				0002h	Assert in Security Code.
				0003h	Assert in Background Services Code.
				0004h	FTL Rebuild Failed.
				0005h	FTL Data Mismatch.
				0006h	Assert in Other Code.

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
				0007h - 7FFFh	Reserved.
				8000h - FFFFh	Vendor Unique.
EVC-ASRT-3	3	Event Data Size	1	This field indicates the number of Dwords in the Event Specific Data field. If the VU Event Identifier field and VU data field do not exist then, then this field shall be set to 0h.	
Event Specific Data					
EVC-ASRT-4	5:4	VU Event Identifier	2	Vendor Unique Event Identifier. The VU Event Identifier that enables the VU data to be decoded.	
EVC-ASRT-5	(Event Data Size * 4) +3:6	VU Data	(Event Data Size * 4) – 2	Vendor Unique Data. The size of this data is determined based on the Event Data Size if this field exists.	

4.9.15.2.8 Temperature Debug Event Class Format

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
EVC-TEMP-1	0	Temperature Debug Class	1	Shall be set to 07h.	
EVC-TEMP-2	2:1	Event Identifier	2	The device shall log Temperature Debug Events as follows:	
				Event ID	Description
				0000h	Composite Temperature decreases to (WCTEMP – 2).
				0001h	Composite Temperature increases to WCTEMP.
				0002h	Composite Temperature increases to reach CCTEMP.
				0003h - 7FFFh	Reserved.
				8000h - FFFFh	Vendor Unique.
Once the event is logged 2 degrees of hysteresis should be applied to avoid additional entries being generated.					

Requirement ID	Byte Address	Field	# of Bytes	Field Description
EVC-TEMP-3	3	Event Data Size	1	This field indicates the number of Dwords in the Event Specific Data field. If the VU Event Identifier field and VU data field do not exist then, then this field shall be set to 0h.
Event Specific Data				
EVC-TEMP-4	5:4	VU Event Identifier	2	Vendor Unique Event Identifier. The VU Event Identifier that enables the VU data to be decoded.
EVC-TEMP-5	(Event Data Size * 4) + 3:6	VU Data	(Event Data Size * 4) - 2	Vendor Unique Data. The size of this data is determined based on the Event Data Size if this field exists.

4.9.15.2.9 Media Debug Event Class Format

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
EVC-MEDIA-1	0	Media Debug Class	1	Shall be set to 08h.	
EVC-MEDIA-2	2:1	Event Identifier	2	The device shall log Media Debug Events as follows:	
				Event ID	Description
				0000h	XOR (or equivalent) Recovery Invoked.
				0001h	Uncorrectable Media Error.
				0002h	Block Marked Bad Due to Program Error.
				0003h	Block Marked Bad Due to Erase Error.
				0004h	Block Marked Bad Due to Read Error.
				0005h	Plane Failure Event.
				0006h - 7FFFh	Reserved.
8000h - FFFFh	Vendor Unique.				
EVC-MEDIA-3	3	Event Data Size	1	This field indicates the number of Dwords in the Event Specific Data field. If the VU Event Identifier field and VU data field do not exist then, then this field shall be set to 0h.	

Requirement ID	Byte Address	Field	# of Bytes	Field Description
Event Specific Data				
EVC-MEDIA-4	5:4	VU Event Identifier	2	Vendor Unique Event Identifier. The VU Event Identifier that enables the VU data to be decoded.
EVC-MEDIA-5	(Event Data Size * 4) + 3:6	VU Data	(Event Data Size * 4) – 2	Vendor Unique Data. The size of this data is determined based on the Event Data Size if this field exists.

4.9.15.2.10 Media Wear Event Class Format

Requirement ID	Byte Address	Field	# of Bytes	Field Description								
EVC-WEAR-1	0	Media Wear Class	1	Shall be set to 09h. This event shall be logged once every 24 hours.								
EVC-WEAR-2	2:1	Event Identifier	2	The device shall log Wear Debug Events as follows: <table><tr><th>Event ID</th><th>Description</th></tr><tr><td>0000h</td><td>Media Wear.</td></tr><tr><td>0001h - 7FFFh</td><td>Reserved.</td></tr><tr><td>8000h- FFFFh</td><td>Vendor Unique.</td></tr></table>	Event ID	Description	0000h	Media Wear.	0001h - 7FFFh	Reserved.	8000h- FFFFh	Vendor Unique.
Event ID	Description											
0000h	Media Wear.											
0001h - 7FFFh	Reserved.											
8000h- FFFFh	Vendor Unique.											
EVC-WEAR-3	3	Event Data Size	1	This field indicates the number of Dwords in the Event Specific Data field. If the VU Event Identifier field and VU data field do not exist then, then this field shall be set to 3h.								
Event Specific Data												
EVC-WEAR-4	15:4	Current Media Wear	12	For Wear Debug Event ID 00h, the device shall log the current wear as follows: <table><tr><th>Byte Address</th><th>Description</th></tr><tr><td>7:4</td><td>Host Terabytes Written.</td></tr><tr><td>11:8</td><td>Media Terabytes Written.</td></tr><tr><td>15:12</td><td>Media Terabytes Erased.</td></tr></table> For all other Wear Event IDs, this field shall be cleared to zero.	Byte Address	Description	7:4	Host Terabytes Written.	11:8	Media Terabytes Written.	15:12	Media Terabytes Erased.
Byte Address	Description											
7:4	Host Terabytes Written.											
11:8	Media Terabytes Written.											
15:12	Media Terabytes Erased.											

Requirement ID	Byte Address	Field	# of Bytes	Field Description
EVC-WEAR-5	17:16	VU Event Identifier	2	Vendor Unique Event Identifier. The VU Event Identifier that enables the VU data to be decoded.
EVC-WEAR-6	(Event Data Size * 4) + 3:18	VU Data	(Event Data Size * 4) – 14	Vendor Unique Data. The size of this data is determined based on the Event Data Size if this field exists.

4.9.15.2.11 Statistic Snapshot Class

For the Statistic Snapshot Class. This enables the device to take a snapshot of a statistic descriptor and store this value in the Event FIFO.

Requirement ID	Byte Address	Field	# of Bytes	Field Description
EVC-SNP-1	0	Statistic Snapshot Class	1	Shall be set to 0Ah. This is a statistic snapshot of a statistics descriptor.
EVC-SNP-2	3:1	Reserved	3	Reserved.
EVC-SNP-3	5:4	Statistic Identifier	2	This field shall contain the value in STATF-1 .
EVC-SNP-4	6	Statistic Information	1	This field shall contain the value in STATF-2 .
EVC-SNP-5	7	Namespace Information	1	This field shall contain the value in STATF-3 .
EVC-SNP-6	9:8	Statistic Data Size	2	This field shall contain the value in STATF-4 .
EVC-SNP-7	11:10	Namespace Identifier[15:0]	2	This field shall contain the value in STATF-5 .
Event Specific Data				
EVC-SNP-8	(Statistic Data Size * 4) + 11:12	Statistic Specific Data	Statistic Data Size * 4	This field shall contain the value in STATF-6 .

4.9.15.2.12 Virtual FIFO Event Class Format

For the Virtual FIFO Class the format of the data is:

Requirement ID	Byte Address	Field	# of Bytes	Field Description								
EVC-VF-1	0	Virtual FIFO Class	1	Shall be set to 0Bh.								
EVC-VF-2	2:1	Virtual FIFO Identifier	2	Virtual FIFO Event Identifier: <table><tr><th>Event ID</th><th>Description</th></tr><tr><td>0000h</td><td>Virtual FIFO Start.</td></tr><tr><td>0001h</td><td>Virtual FIFO End.</td></tr><tr><td>0002-FFFFh</td><td>Reserved.</td></tr></table>	Event ID	Description	0000h	Virtual FIFO Start.	0001h	Virtual FIFO End.	0002-FFFFh	Reserved.
Event ID	Description											
0000h	Virtual FIFO Start.											
0001h	Virtual FIFO End.											
0002-FFFFh	Reserved.											
EVC-VF-3	3	Virtual FIFO Data Size	1	This shall be set to 1h.								
EVC-VF-4	5:4	VU Virtual FIFO Identifier	2	This is the required format of the VU Virtual FIFO Identifier. <table><tr><th>Bit</th><th>VU Virtual FIFO Identifier Bit Description</th></tr><tr><td>15:11</td><td>This is the physical Event FIFO Number. Valid values are 1h to 10h. A value of 0h is not valid. An example physical event FIFO is TELDF-18 is event FIFO 1.</td></tr><tr><td>10:0</td><td>This is the virtual FIFO number within the physical FIFO. Note: Bits 7:0 are the LSB which is in byte 4.</td></tr></table>	Bit	VU Virtual FIFO Identifier Bit Description	15:11	This is the physical Event FIFO Number. Valid values are 1h to 10h. A value of 0h is not valid. An example physical event FIFO is TELDF-18 is event FIFO 1.	10:0	This is the virtual FIFO number within the physical FIFO. Note: Bits 7:0 are the LSB which is in byte 4.		
Bit	VU Virtual FIFO Identifier Bit Description											
15:11	This is the physical Event FIFO Number. Valid values are 1h to 10h. A value of 0h is not valid. An example physical event FIFO is TELDF-18 is event FIFO 1.											
10:0	This is the virtual FIFO number within the physical FIFO. Note: Bits 7:0 are the LSB which is in byte 4.											
EVC-VF-5	7:6	Reserved	2	This shall be set to 0h.								

This indicates the start/end of a virtual FIFO within a physical FIFO. The name of the virtual FIFO can be found in the String Log using the VU Virtual FIFO Identifier.

4.9.15.2.13 SMBUS/I2C/I3C Debug Event Class Format

For the SMBUS/I2C/I3C Debug Event Class the format of the data is:

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
EVC-SMBUS-1	0	SMBUS/I2C/I3C Debug Class	1	Shall be set to 0Ch.	
EVC-SMBUS-2	2:1	Event Identifier	2	Event ID	Description
				0000h	Timeout Errors.
				0001h	PEC Errors.
				0002h	Arbitration loss.
				0003h	NACK error.

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
				0004h-7FFFh	Reserved.
				8000h-FFFFh	Vendor Unique.
EVC-SMBUS-3	3	Event Data Size	1	This field indicates the number of Dwords in the Event Specific Data field. If the VU Event Identifier field and VU data field do not exist then, this field shall be set to 1h.	
Event Specific Data					
EVC-SMBUS-4	5:4	SMBUS Debug Event Data	2	For SMBUS/I2C/I3C Event ID 0003h, the device shall log the following events:	
				Event Data	Description
				0000h	Received invalid command or data.
				0001h	Device is busy.
				0002h	Requested data is not available.
				0003h-FFFFh	Reserved.
EVC-SMBUS-5	7:6	Reserved	2	Reserved.	
EVC-SMBUS-6	9:8	VU Event Identifier	2	Vendor Unique Event Identifier. The VU Event Identifier that enables the VU Data field to be decoded.	
EVC-SMBUS-7	(Event Data Size * 4) + 3:10	VU Data	(Event Data Size * 4) - 6	Vendor Unique Data. The size of this data is determined based on the Event Data Size if this field exists.	

4.9.15.2.14 MCTP Debug Event Class Format

For the MCTP Debug Event Class the format of the data is:

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
EVC-MCTP-1	0	MCTP Debug Class	1	Shall be set to 0Dh.	
EVC-MCTP-2	2:1	Event Identifier	2	Event ID	Description
				0000h	Dropped Packet.

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
				0001h	Dropped Message.
				0002h	Discovery and addressing errors.
				0003h	Error Status.
				0004h-7FFFh	Reserved.
				8000h-FFFFh	Vendor Unique.
EVC-MCTP-3	3	Event Data Size	1	This field indicates the number of Dwords in the Event Specific Data field. If the VU Event Identifier field and VU data field do not exist then, this field shall be set to 2h.	
Event Specific Data					
EVC-MCTP-4	5:4	MCTP Debug Event Data	2	For MCTP Event ID 0, the device shall log the following events:	
				Event Data	Description
				0000h	Unexpected middle or end packet.
				0001h	Bad packet data integrity or other physical layer error: Framing errors.
				0002h	Bad packet data integrity or other physical layer error: Byte alignment errors.
				0003h	Bad packet data integrity or other physical layer error: Invalid packet size.
				0004h	Unexpected or expired message tag.
				0005h	Unknown destination EID.
				0006h	Unsupported MCTP header version.
				0007h	Unsupported transmission unit size.
				0008h - FFFFh	Reserved.
				For MCTP Event ID 1, the device shall log the following events:	
				Event Data	Description
				0000h	Receipt of a new start packet.
				0001h	Timeout waiting for a packet + threshold.

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
				0002h	Out-of-sequence packet sequence number.
				0003h	Incorrect transmission unit.
				0004h	Bad message integrity check.
				0005h	Invalid message type received.
				0006h - FFFFh	Reserved.
				For MCTP Event ID 2, the device shall log the following events:	
				Event Data	Description
				0000h	Transport Binding specific bus enumeration errors.
				0001h	Transport Binding specific bus address assignment errors.
				0002h - FFFFh	Reserved.
				For MCTP Event ID 3, the device shall log the following events:	
				Event Data	Description
				0000h	Reserved.
				0001h	ERROR.
				0002h	ERROR_INVALID_DATA.
				0003h	ERROR_INVALID_LENGTH.
				0004h	ERROR_NOT_READY.
				0005h	ERROR_UNSUPPORTED_CMD.
				0006h	COMMAND_SPECIFIC.
				0007h - FFFFh	Reserved.
EVC-MCTP-5	6	MCTP Transport Protocol Information	1	Value	Description
				00h	PCIe VDM on device PCIe port 0.
				01h	PCIe VDM on device PCIe port 1. This value shall not be used if device PCIe port 1 does not exist.

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
				02h - 03h	Reserved.
				04h	I2C/SMBus.
				05h	I3C.
				06h - FFh	Reserved.
EVC-MCTP-6	7	MCTP Event Flags	1	Bits	Bit Description
				7	MCTP Transport Header Valid: Shall be set to 1b if the MCTP Transport Header field is valid in this event (see EVC-MCTP-7). Shall be cleared to 0b if the MCTP Transport Header field is not valid.
				6:0	Reserved.
EVC-MCTP-7	11:8	MCTP Transport Header	4	Shall contain the MCTP Transport Header captured from the MCTP packet associated with this event if the MCTP Transport Header Valid bit is set to 1b. Shall be cleared to zero if the MCTP Transport Header Valid bit is cleared to 0b. The 32-bit MCTP Transport Header follows the medium-specific header and precedes the MCTP packet payload, as specified in the Management Component Transport Protocol (MCTP) Base Specification, DMTF DSP0236. The device should capture the MCTP Transport Header unless prevented from doing so by a failure (e.g., integrity error).	
EVC-MCTP-8	13:12	VU Event Identifier	2	Vendor Unique Event Identifier. The VU Event Identifier that enables the VU Data field to be decoded.	
EVC-MCTP-9	(Event Data Size * 4) + 3:14	VU Data	(Event Data Size * 4) - 10	Vendor Unique Data. The size of this data is determined based on the Event Data Size if this field exists.	

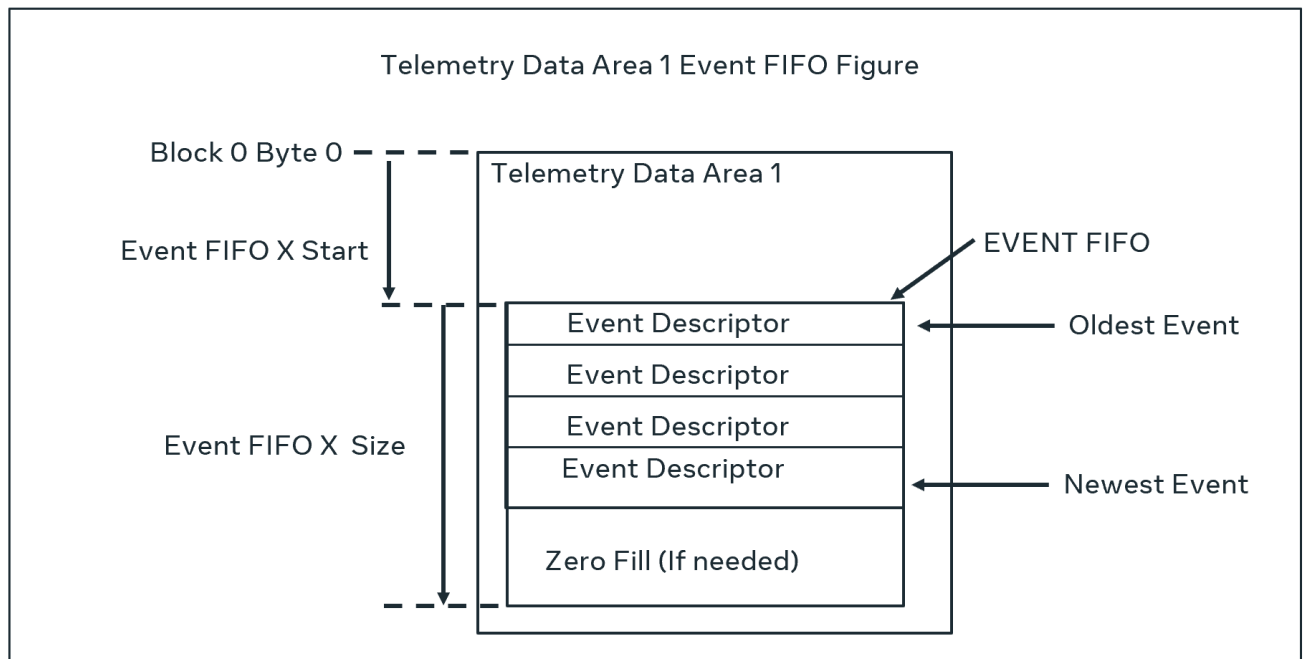
4.9.15.2.15 Vendor Unique Event Class Format

For the Vendor Unique debug class.

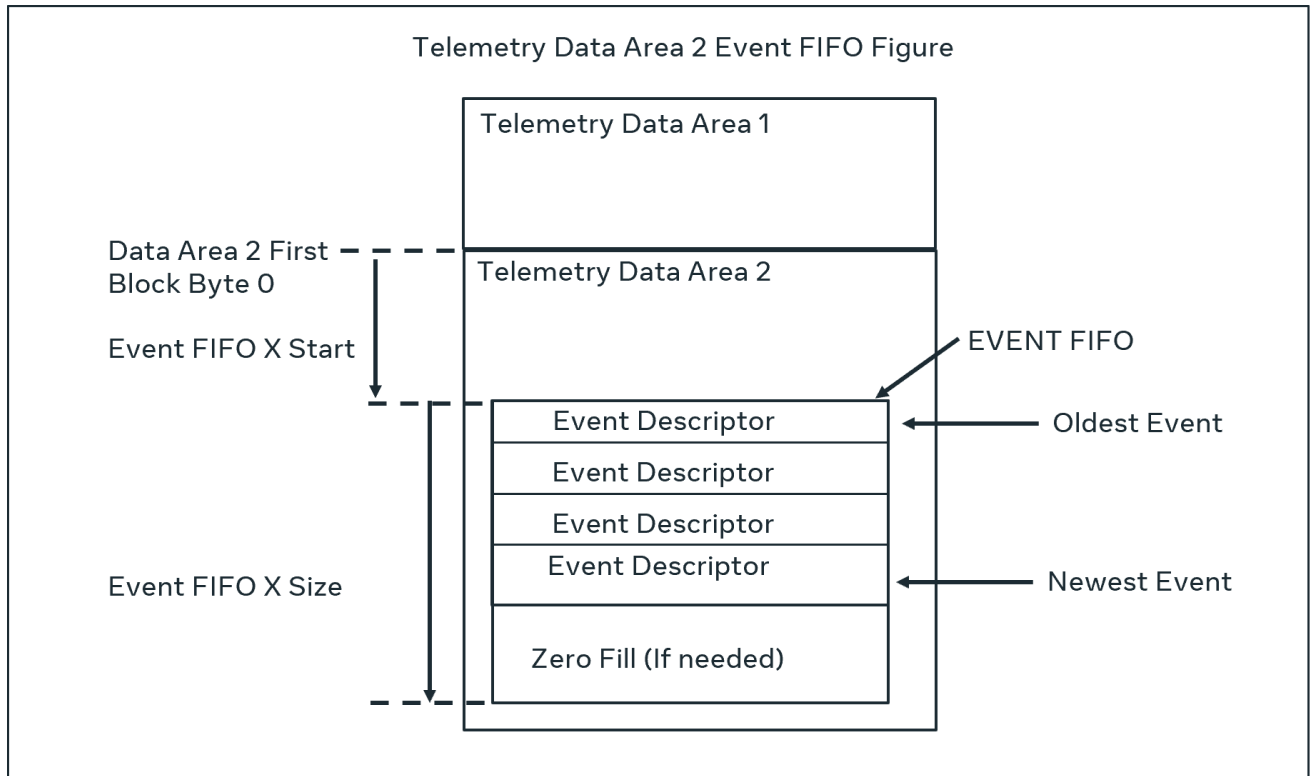
Requirement ID	Byte Address	Field	# of Bytes	Field Description
EVC-VU-1	0	Debug VU Class	1	Shall be set to a value in the range 80h to FFh.
EVC-VU-2	2:1	VU Event Identifier	2	Vendor Unique Event Identifier. The Vendor Unique event identifiers under the debug VU Class shall be in the range 0h to FFFFh.
EVC-VU-3	3	VU Event Data Size	1	This field indicates the number of Dwords in the Event Specific Data field. If the VU Specific Data field does not exist then, then this field shall be set to 0h. Valid values for this field are 0 to FF.
Event Specific Data				
EVC-VU-4	(VU vent Data Size * 4) + 3:4	VU Data	VU Event Data Size * 4	Vendor Unique Data. The size of this data is determined based on the Event Data Size if this field exists.

4.9.16 Event FIFO Location

The Event FIFO X location in Telemetry Data Area 1 can be found by using the Event FIFO X Start, Event FIFO X Size. This can be seen in the following Telemetry Data Area 1 Event FIFO Figure:



The Event FIFO location in Telemetry Data Area 2 can be found by using the Event FIFO X Start, Event FIFO X Data End. This can be seen in the following Telemetry Data Area 2 Event FIFO Figure:



4.9.16.1 Event FIFO Requirements

Requirement ID	Description
EVF-1	The oldest event descriptor shall be at the Event FIFO Start Address.
EVF-2	There shall be no gaps between the data in one descriptor and the next descriptor.
EVF-3	The event FIFO shall only have complete descriptors (i.e., no partial descriptors).
EVF-4	All data contained in the event FIFO that is not contained in an event descriptor shall be cleared to zero.
EVF-5	For a single FIFO, the Event FIFO Start and Event FIFO End shall be in the same Telemetry Data Area.
EVF-6	Event FIFO Start and End locations shall not overlap with the Statistic Descriptor locations.
EVF-7	The decode of the Event Class and Vendor Unique Event Class shall be provided to the customer via the Telemetry String log page.

4.9.17 Telemetry Data Area

4.9.17.1 Telemetry Data Format

Telemetry Data Area 1 has the following format. It should be noted that this is the format of Telemetry Data Area 1 in the Telemetry log, which does not start from byte 0/Dword 0.

Requirement ID	Byte Address	Field	# of Bytes	Field Description
TELDF-1	1:0	Major Version	2	This field shall be set to 0003h. A change of the Major Version number indicates that the changes to the Telemetry Data Area format decode are not host software backward compatible.
TELDF-2	3:2	Minor Version	2	This field shall be set to 0001h. A change of the Minor Version number indicates that the changes to the Telemetry Data Area format decode are host software backward compatible.
TELDF-3	7:4	Reserved	4	Shall be cleared to zero.
TELDF-4	15:8	Timestamp	8	Shall be set to the Timestamp when the Telemetry Log (Host Initiated or Controller Initiated) Get Log command was received by the device. The format of this field shall be as defined in Timestamp (Feature Identifier 0Eh) of the NVM Express Base Specification.
TELDF-5	31:16	Log Page GUID	16	This field shall be set to BA560A9C3043424CBC73719D87E64EFAh.
TELDF-6	32	Number Telemetry Profiles Supported	1	Shall be set to the number of Telemetry Profiles supported by the device. This is a 0's-based field (e.g., if this field is cleared to 0h then the device supports 1 Telemetry Profile).
TELDF-7	33	Telemetry Profile Selected (TPS)	1	Shall be set to the currently selected Telemetry Profile number.
TELDF-8	39:34	Reserved	6	Shall be cleared to zero.
TELDF-9	47:40	Telemetry String Log Page Size (SLPS)	8	Shall be set to the number of Dwords in the Telemetry String log page.
TELDF-10	55:48	Reserved	8	Shall be cleared to zero.
TELDF-11	63:56	Firmware Revision	8	Shall be set to the value of the Firmware Revision field in the Identify Controller data structure.
TELDF-12	95:64	Reserved	32	Shall be cleared to zero.
TELDF-13	103:96	Data Area 1 Statistic Start	8	This field shall contain the Dword offset of the start of the Statistic Buffer in Telemetry Data Area 1. This offset starts from Dword 0 / byte 0 in Telemetry Data Area 1. This field shall contain a zero-based value.

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
TELDF-14	111:104	Data Area 1 Statistic Size	8	This field shall contain the size of the Statistic Buffer in Data Area 1 in Dwords. If there are no Statistic Descriptors a value of 0h shall be reported.	
TELDF-15	119:112	Data Area 2 Statistic Start	8	This field shall contain the Dword offset of the start of the Statistic Buffer in Telemetry Data Area 2. This offset starts from Dword 0 / byte 0 in Telemetry Data Area 2. This field shall contain a zero-based value.	
TELDF-16	127:120	Data Area 2 Statistic Size	8	This field shall contain the size of the Statistic Buffer in Data Area 2 in Dwords. If there are no Statistic Descriptors a value of 0h shall be reported.	
TELDF-17	159:128	Reserved	32	Shall be cleared to zero.	
TELDF-18	160	Event FIFO 1 Data Area	1	Event FIFO Data Area	Description
				00h	Event FIFO 1 does not exist.
				01h	Event FIFO 1 exists in Telemetry Data Area 1.
				02h	Event FIFO 1 exists in Telemetry Data Area 2.
				03h - FFh	Reserved.
TELDF-19	161	Event FIFO 2 Data Area	1	Event FIFO Data Area	Description
				00h	Event FIFO 2 does not exist.
				01h	Event FIFO 2 exists in Telemetry Data Area 1.
				02h	Event FIFO 2 exists in Telemetry Data Area 2.
				03h - FFh	Reserved.
TELDF-20	162	Event FIFO 3 Data Area	1	Event FIFO Data Area	Description
				00h	Event FIFO 3 does not exist.
				01h	Event FIFO 3 exists in Telemetry Data Area 1.
				02h	Event FIFO 3 exists in Telemetry Data Area 2.
				03h - FFh	Reserved.

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
TELDf-21	163	Event FIFO 4 Data Area	1	Event FIFO Data Area	Description
				00h	Event FIFO 4 does not exist.
				01h	Event FIFO 4 exists in Telemetry Data Area 1.
				02h	Event FIFO 4 exists in Telemetry Data Area 2.
				03h - FFh	Reserved.
TELDf-22	164	Event FIFO 5 Data Area	1	Event FIFO Data Area	Description
				00h	Event FIFO 5 does not exist.
				01h	Event FIFO 5 exists in Telemetry Data Area 1.
				02h	Event FIFO 5 exists in Telemetry Data Area 2.
				03h - FFh	Reserved.
TELDf-23	165	Event FIFO 6 Data Area	1	Event FIFO Data Area	Description
				00h	Event FIFO 6 does not exist.
				01h	Event FIFO 6 exists in Telemetry Data Area 1.
				02h	Event FIFO 6 exists in Telemetry Data Area 2.
				03h - FFh	Reserved.
TELDf-24	166	Event FIFO 7 Data Area	1	Event FIFO Data Area	Description
				00h	Event FIFO 7 does not exist.
				01h	Event FIFO 7 exists in Telemetry Data Area 1.
				02h	Event FIFO 7 exists in Telemetry Data Area 2.
				03h - FFh	Reserved.

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
TELDf-25	167	Event FIFO 8 Data Area	1	Event FIFO Data Area	Description
				00h	Event FIFO 8 does not exist.
				01h	Event FIFO 8 exists in Telemetry Data Area 1.
				02h	Event FIFO 8 exists in Telemetry Data Area 2.
				03h - FFh	Reserved.
TELDf-26	168	Event FIFO 9 Data Area	1	Event FIFO Data Area	Description
				00h	Event FIFO 9 does not exist.
				01h	Event FIFO 9 exists in Telemetry Data Area 1.
				02h	Event FIFO 9 exists in Telemetry Data Area 2.
				03h - FFh	Reserved.
TELDf-27	169	Event FIFO 10 Data Area	1	Event FIFO Data Area	Description
				00h	Event FIFO 10 does not exist.
				01h	Event FIFO 10 exists in Telemetry Data Area 1.
				02h	Event FIFO 10 exists in Telemetry Data Area 2.
				03h - FFh	Reserved.
TELDf-28	170	Event FIFO 11 Data Area	1	Event FIFO Data Area	Description
				00h	Event FIFO 11 does not exist.
				01h	Event FIFO 11 exists in Telemetry Data Area 1.
				02h	Event FIFO 11 exists in Telemetry Data Area 2.
				03h - FFh	Reserved.

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
TELDf-29	171	Event FIFO 12 Data Area	1	Event FIFO Data Area	Description
				00h	Event FIFO 12 does not exist.
				01h	Event FIFO 12 exists in Telemetry Data Area 1.
				02h	Event FIFO 12 exists in Telemetry Data Area 2.
				03h - FFh	Reserved.
TELDf-30	172	Event FIFO 13 Data Area	1	Event FIFO Data Area	Description
				00h	Event FIFO 13 does not exist.
				01h	Event FIFO 13 exists in Telemetry Data Area 1.
				02h	Event FIFO 13 exists in Telemetry Data Area 2.
				03h - FFh	Reserved.
TELDf-31	173	Event FIFO 14 Data Area	1	Event FIFO Data Area	Description
				00h	Event FIFO 14 does not exist.
				01h	Event FIFO 14 exists in Telemetry Data Area 1.
				02h	Event FIFO 14 exists in Telemetry Data Area 2.
				03h - FFh	Reserved.
TELDf-32	174	Event FIFO 15 Data Area	1	Event FIFO Data Area	Description
				00h	Event FIFO 15 does not exist.
				01h	Event FIFO 15 exists in Telemetry Data Area 1.
				02h	Event FIFO 15 exists in Telemetry Data Area 2.
				03h - FFh	Reserved.

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
TELD-33	175	Event FIFO 16 Data Area	1	Event FIFO Data Area	Description
				00h	Event FIFO 16 does not exist.
				01h	Event FIFO 16 exists in Telemetry Data Area 1.
				02h	Event FIFO 16 exists in Telemetry Data Area 2.
				03h - FFh	Reserved.
TELD-34	183:176	Event FIFO 1 Start	8	Shall be set to the Dword offset of Event FIFO 1 starting from Dword 0 / byte 0 of the selected Telemetry Data Area.	
TELD-35	191:184	Event FIFO 1 Size	8	This field shall contain the size of Event FIFO 1 in Dwords.	
TELD-36	199:192	Event FIFO 2 Start	8	Shall be set to the Dword offset of Event FIFO 2 starting from Dword 0 / byte 0 of the selected Telemetry Data Area.	
TELD-37	207:200	Event FIFO 2 Size	8	This field shall contain the size of Event FIFO 2 in Dwords.	
TELD-38	215:208	Event FIFO 3 Start	8	Shall be set to the Dword offset of Event FIFO 3 starting from Dword 0 / byte 0 of the selected Telemetry Data Area.	
TELD-39	223:216	Event FIFO 3 Size	8	This field shall contain the size of Event FIFO 3 in Dwords.	
TELD-40	231:224	Event FIFO 4 Start	8	Shall be set to the Dword offset of Event FIFO 4 starting from Dword 0 / byte 0 of the selected Telemetry Data Area.	
TELD-41	239:232	Event FIFO 4 Size	8	This field shall contain the size of Event FIFO 4 in Dwords.	
TELD-42	247:240	Event FIFO 5 Start	8	Shall be set to the Dword offset of Event FIFO 5 starting from Dword 0 / byte 0 of the selected Telemetry Data Area.	
TELD-43	255:248	Event FIFO 5 Size	8	This field shall contain the size of Event FIFO 5 in Dwords	
TELD-44	263:256	Event FIFO 6 Start	8	Shall be set to the Dword offset of Event FIFO 6 starting from Dword 0 / byte 0 of the selected Telemetry Data Area.	

Requirement ID	Byte Address	Field	# of Bytes	Field Description
TELDF-45	271:264	Event FIFO 6 Size	8	This field shall contain the size of Event FIFO 6 in Dwords.
TELDF-46	279:272	Event FIFO 7 Start	8	Shall be set to the Dword offset of Event FIFO 7 starting from Dword 0 / byte 0 of the selected Telemetry Data Area.
TELDF-47	287:280	Event FIFO 7 Size	8	This field shall contain the size of Event FIFO 7 in Dwords.
TELDF-48	295:288	Event FIFO 8 Start	8	Shall be set to the Dword offset of Event FIFO 8 starting from Dword 0 / byte 0 of the selected Telemetry Data Area.
TELDF-49	303:296	Event FIFO 8 Size	8	This field shall contain the size of Event FIFO 8 in Dwords.
TELDF-50	311:304	Event FIFO 9 Start	8	Shall be set to the Dword offset of Event FIFO 9 starting from Dword 0 / byte 0 of the selected Telemetry Data Area.
TELDF-51	319:312	Event FIFO 9 Size	8	This field shall contain the size of Event FIFO 9 in Dwords.
TELDF-52	327:320	Event FIFO 10 Start	8	Shall be set to the Dword offset of Event FIFO 10 starting from Dword 0 / byte 0 of the selected Telemetry Data Area.
TELDF-53	335:328	Event FIFO 10 Size	8	This field shall contain the size of Event FIFO 10 in Dwords.
TELDF-54	343:336	Event FIFO 11 Start	8	Shall be set to the Dword offset of Event FIFO 11 starting from Dword 0 / byte 0 of the selected Telemetry Data Area.
TELDF-55	351:344	Event FIFO 11 Size	8	This field shall contain the size of Event FIFO 11 in Dwords.
TELDF-56	359:352	Event FIFO 12 Start	8	Shall be set to the Dword offset of Event FIFO 12 starting from Dword 0 / byte 0 of the selected Telemetry Data Area.
TELDF-57	367:360	Event FIFO 12 Size	8	This field shall contain the size of Event FIFO 12 in Dwords.
TELDF-58	375:368	Event FIFO 13 Start	8	Shall be set to the Dword offset of Event FIFO 13 starting from Dword 0 / byte 0 of the selected Telemetry Data Area.
TELDF-59	383:376	Event FIFO 13 Size	8	This field shall contain the size of Event FIFO 13 in Dwords.

Requirement ID	Byte Address	Field	# of Bytes	Field Description
TELD-60	391:384	Event FIFO 14 Start	8	Shall be set to the Dword offset of Event FIFO 14 starting from Dword 0 / byte 0 of the selected Telemetry Data Area.
TELD-61	399:392	Event FIFO 14 Size	8	This field shall contain the size of Event FIFO 14 in Dwords.
TELD-62	407:400	Event FIFO 15 Start	8	Shall be set to the Dword offset of Event FIFO 15 starting from Dword 0 / byte 0 of the selected Telemetry Data Area.
TELD-63	415:408	Event FIFO 15 Size	8	This field shall contain the size of Event FIFO 15 in Dwords.
TELD-64	423:416	Event FIFO 16 Start	8	Shall be set to the Dword offset of Event FIFO 16 starting from Dword 0 / byte 0 of the selected Telemetry Data Area.
TELD-65	431:424	Event FIFO 16 Size	8	This field shall contain the size of Event FIFO 16 in Dwords.
TELD-66	511:432	Reserved	80	Shall be cleared to zero.
TELD-67	1023:512	SMART / Health Information	512	This shall be a copy of the SMART / Health Information log page (Log Identifier 02h) of the controller that captured the Telemetry data.
TELD-68	1535:1024	SMART / Health Information Extended	512	This shall be a copy of the SMART / Health Information Extended log page (Log Identifier C0h) data of the controller that captured the Telemetry data.

The order and placement of the Event and Statistics FIFOs are vendor unique and shall be placed in the Telemetry log page Data Area 1 after byte offset 1535 up to the end of Data Area 1.

4.10 Device Self-test Requirements

To normalize the reporting of Device Self-test data, the following Segment Numbers are defined.

Requirement ID	Description		
SELFST-1	The device shall use the following segment numbers:		
	Segment	Test Performed	Failure Criteria
	0	Reserved.	N/A
	1 – SRAM Check	Write a test pattern to SRAM followed by a read and compare of original data. Shall test all internal and external SRAM devices.	Any uncorrectable error or data mis-compare.

Requirement ID	Description		
	2 – SMART Check	Check SMART or health status for Critical Warning bits set to 1b in SMART / Health Information log page.	Any Critical Warning bit set to 1b fails this segment, with the exception of bit 0 (spare capacity below threshold) and bit 1 (thermal excursions).
	3 – Volatile Memory Backup	Validate volatile memory backup solution health. Measure backup power source charge and/or discharge time. Shall perform backup test and not rely on previous results. During the test, the device shall not lose power loss protection.	Significant degradation in backup capability.
	4 – Non-User Data Validation	Confirm/validate all copies of non-user data (e.g., FTL, log pages, etc.).	Non-user data is corrupt and is not recoverable.
	5 – NVM Integrity	Write/read/compare to reserved areas of each NVM, if present. Ensure that every read/write channel of the controller is exercised and each NVM is accessed.	Data mis-compare or hardware failure.
	6 – Data Integrity	Perform background housekeeping tasks, prioritizing actions that enhance the integrity of stored data. Test CRC hardware, error correction hardware, including XOR, encryption engine, etc.	Any failure of the CRC hardware, error correction hardware, including XOR, encryption engine, etc. or any uncorrectable data error not caused by Write Uncorrectable command(s).
	7 – Media Check Extended	Perform reads from every mapped LBA. Shall include LBA 0 and MAXLBA, if mapped. Shall terminate segment when all mapped LBAs are read, or the Device Self-test completion time limit expires.	Any uncorrectable error not caused by Write Uncorrectable command(s).
	8 – DRAM check	Write a test pattern to DRAM followed by a read and compare of original data. Shall test all internal and external SRAM devices.	Any uncorrectable error or data mis-compare.
	9 – Temperature Sensor	Verify the temperature sensors are working correctly.	Temperature sensors are not reporting correctly.

Requirement ID	Description		
	10 – SMART Check	Same as 2-SMART Check. This check shall be performed after all other test segments in order to detect critical warnings caused by prior test segments.	Any Critical Warning bit set to 1b fails this segment, with the exception of bit 0 (spare capacity below threshold) and bit 1 (thermal excursions).
	200:11	Reserved.	N/A
	255:201	Vendor Unique. Any Vendor Unique Segment Numbers shall be clearly documented and disclosed to the customer.	
SELFTEST-2	A short device self-test operation (i.e., the STC field is set to 1h) shall complete in less than or equal to 2 minutes.		
SELFTEST-3	An extended device self-test operation (i.e., the STC field is set to 2h) shall complete in less than or equal to 30 minutes (i.e., the EDSTT field shall indicate a value of less than or equal to 30 minutes).		
SELFTEST-4	A vendor-specific self-test operation (i.e., the STC field is set to Eh) shall complete the test specified by SELFTEST-7 in less than or equal to 2 seconds.		
SELFTEST-5	A device self-test operation shall not fail if it is unable to complete within the specified completion time (e.g., due to concurrent host I/O activity). The device shall complete as many device self-test segments as possible within the allotted completion time.		
SELFTEST-6	For a Self-test Code (STC) of 2h, the device self-test operation shall terminate upon reading all allocated LBAs and completing all non-media related tests.		
SELFTEST-7	For a Device Self-test Code (STC) of 1h or Eh, the device self-test operation shall include at a minimum, segments 1 to 3 and 8, and as much as possible of segments 4 to 7, within the completion time specified for that specific operation.		
SELFTEST-8	Obsolete. See SELFTEST-1 segments 2 and 10.		
SELFTEST-9	The device vendor shall provide the minimum number of LBAs required to be written by the host to enable the extended device self-test operation to read from all physical non-volatile memory elements (e.g., NAND die). A segment shall not fail solely due to the host writing less than the minimum number of LBAs.		
SELFTEST-10	If the Device Self-test command is reissued after a previous Device Self-test command and operation different LBAs allocated LBAs, but only Self-test completion time, then the first run of the Device Self-test would scan LBAs 0h to 5FFFh, the next run would scan LBAs 6000h to		

Requirement ID	Description
	BFFFh and the 1FFFh, and so forth.
SELFTEST-11	The device self-test operation shall not be destructive to any user data (note that reading user data once during the device self-test operation is not considered destructive, because even though it technically causes read disturb, the effect is minimal).

4.11 Firmware Update Requirements

This defines the requirements for firmware update in the device.

Requirement ID	Description
FWUP-1	Obsolete. See STD-LOG-10 .
FWUP-2	Other than media end-of-life, devices shall not have any restrictions on the number of firmware downloads supported.
FWUP-3	The Firmware Commit command with the following Commit Action (CA) codes shall be supported: • 000b – Download only. • 001b – Download and activate upon reset. • 010b – Activate upon reset. • 011b – Activate immediately without reset.
FWUP-4	Firmware Image Download command shall be supported and shall not cause any performance impact.
FWUP-5	Obsolete.
FWUP-6	The device shall support a minimum of 2 read/write slots for firmware update and may support up to 7.
FWUP-7	The controller shall set the Maximum Time for Firmware Activation (MTFA) field to a value that is less than or equal to Ah (1s). This time limit applies only to Commit Action 011b (firmware activation without reset) of the Firmware Commit command, see FWUP-30.
FWUP-8	If a Firmware Commit command is processed that specifies a firmware image that has a Security Firmware Revision (see SMART-22) that is less than the Security Firmware Revision of the currently running firmware image, then the device shall abort that Firmware Commit command with a status code of Firmware Activation Prohibited (13h). See SEC-3 for additional firmware anti-rollback requirements.
FWUP-9	The firmware image in each valid firmware slot shall have multiple copies of that firmware image on separate physical non-volatile memory devices (e.g., NAND die, NAND RAID stripe) for reliability.
FWUP-10	Firmware activation shall not cause or require data (e.g., user data, log page contents, etc.) to be lost or destroyed.
FWUP-11	Firmware activation without reset shall occur seamlessly on a running system:

Requirement ID	Description
	- The device shall preserve the current state of the device (e.g., Opal locking state, current value of each Feature, Timestamp, I/O Submission/Completion Queue setup, NVMe-MI state such as MCTP Transmission Unit Size, SMBus/I2C/I3C Frequency, and MCTP state such as the MCTP endpoint ID, LBA format, PCIe state, etc.). - The PCIe link state shall not be impacted.
FWUP-12	The firmware image shall contain the firmware for all the device's controllers (NVMe controllers, management controllers, etc.).
FWUP-13	The VPD/FRU Data shall be a part of the device's firmware update image and shall be field upgradable using the standard NVMe Firmware Image Download/Firmware Commit commands. VPD fields that are unique to the device (e.g., Serial Number) shall be preserved during a firmware update.
FWUP-14	The size of the firmware shall be 6 MiB or less in order to facilitate firmware update via low-bandwidth interfaces (e.g., NVMe-MI over SMBus).
FWUP-15	Requiring a reset of any type to activate firmware under any condition shall be avoided. If a reset is unavoidable, the device vendor shall request a waiver from the end customer. In cases where waivers are granted, a Controller Level Reset is preferred over a Conventional Reset. Firmware Activation requiring an NVMe Subsystem Reset should always be avoided.
FWUP-16	All firmware updates shall be allowed to be performed by the system vendor or end user without any outside assistance from NVMe device vendor employees or anyone else and shall not require any additional vendor-specific actions or equipment (such as dongles, debug cables, etc.) unless otherwise noted in this specification. This includes both pre-production and production firmware.
FWUP-17	Firmware updates shall not require an intermediate firmware update or "bridge code" to update from one firmware version to the next subsequent version (e.g., N-1 firmware revision to bridge firmware to N firmware is prohibited). This includes both pre-production and production firmware.
FWUP-18	The device shall not be left in an unusable state due to any reset or loss of power during a firmware update. Depending on where in the device's firmware activation process the reset or loss of power occurs, the device shall either: - abort the firmware activation and continue running with the firmware revision that was running at the start of the firmware update process; or - complete the firmware activation and start running with the new firmware revision.
FWUP-19	For production-level firmware, all means of updating the firmware besides the Firmware Image Download/Firmware Commit commands (e.g., via MMIO or any vendor-proprietary mechanisms) shall be disabled.
FWUP-20	The device shall support a read-only firmware slot (slot 1). If a firmware image is successfully activated to a read-write slot that increases the Security Version Number (see SMART-22), then the device shall also update the read-only slot 1 with that firmware image.

Requirement ID	Description
FWUP-21	If the Firmware Slot field in the Firmware Commit command is cleared to 0h, then the device shall commit the firmware image to a firmware slot that does not contain the currently running firmware image.
FWUP-22	If the current active firmware image is corrupt, then the device shall automatically fail over to another backup copy of that firmware image until all backup copies of that firmware image are exhausted. The device shall not automatically fail over to another revision of firmware in a different firmware slot; this overrides the NVM Express Base Specification. The vendor should follow the guidelines in NIST SP 800-193.
FWUP-23	A single firmware image shall cover all the devices in a product family. For example, devices with the same model but different capacity points, endurance or form factor shall have one firmware image that works on all devices. A single firmware image shall cover all TCG Opal capable and non-TCG Opal capable devices in a given product family. An exception is that the firmware for a family of FIPS 140-3 compliant devices is different than the firmware for the same family of non-FIPS 140-3 compliant devices. In particular, the firmware for the family of FIPS 140-3 compliant devices shall contain the FIPS 140 compliance descriptor (see SEC-52) whereas the firmware for the family of non-FIPS 140-3 compliant devices shall not contain the FIPS 140 compliance descriptor. Other than the FIPS 140 compliance descriptor, the firmware for the family of FIPS 140-3 compliant devices should be the same as the firmware for the same family of non-FIPS 140-3 compliant devices.
FWUP-24	Every firmware image shall have a firmware signature that meets the requirements of SBT-1 and SBT-4 . The device shall check the firmware signature as part of processing any Firmware Commit command that commits a firmware image to a firmware slot. If the firmware signature check fails, the device shall abort the Firmware Commit command with Invalid Firmware Image status.
FWUP-25	If a Firmware Commit command activates a firmware image from the same firmware slot as the currently running firmware image (where the currently running firmware image is the firmware that processed the Firmware Commit command), then: - the device shall keep a copy of the currently running firmware image until the newly activated firmware image completes initialization successfully at least once; and - if the firmware image that is being activated is unable to complete initialization successfully for any reason, then the device shall revert to the firmware that processed the Firmware Commit command; and - once the newly activated firmware image successfully completes initialization at least once, the firmware image for the firmware that processed the Firmware Commit command is permitted to be discarded.
FWUP-26	For a successful Firmware Commit command with Commit Action 001b or 010b (firmware is activated at the next Controller Level Reset) and for a Firmware Commit command with Commit Action 011b (activate firmware without reset) that is aborted with Firmware Activation Requires Controller Level Reset status, the device shall complete the firmware activation process within 5 seconds from the start of the Controller Level Reset.

Requirement ID	Description
FWUP-27	For an active slot firmware update, upon completing the firmware activate of the new firmware, the firmware slot shall only contain multiple copies of the active firmware with no other additional information. When updating a firmware slot which is not active, upon completing the Firmware Commit command, the firmware slot being updated shall only contain multiple copies of the committed firmware with no other additional information.
FWUP-28	For a FIPS 140-3 device: - if the Cryptographic Module Boundary encompasses the entire physical device, then the Firmware Version value(s) in the FIPS 140-3 certification shall match the value(s) indicated by the Firmware Revision field in the Identify Controller data structure; and - if the Cryptographic Module Boundary does not encompass the entire physical device, then there is no requirement that the Firmware Version value(s) in the FIPS 140-3 certification match the value(s) indicated by the Firmware Revision field in the Identify Controller data structure. SEC-47 strongly recommends that the Cryptographic Module Boundary not encompass the entire physical device. All FIPS 140-3 devices are required to provide FIPS 140 compliance information, see SEC-52.
FWUP-29	The device shall set the Firmware Update Granularity (FWUG) field to 01h indicating and firmware update granularity of 4,096 bytes.
FWUP-30	For a Firmware Commit command with Commit Action 011b (firmware activation without reset), the device shall complete the firmware activation process within MTFA seconds after submission of the Firmware Commit command to an empty Admin Queue, see FWUP-7.
FWUP-31	The device shall be ready to accept host I/O and NVMe Admin commands upon completion of the Firmware Commit Command.
FWUP-32	The device shall reject any attempt to commit or activate any firmware image that is not appropriate for the device (e.g., a firmware image for a FIPS 140-3 compliant device may or may not be appropriate for a device that is not FIPS 140-3 compliant, see FWUP-23). Rejection of a firmware image shall neither render the device inoperable nor impair device functionality. The means of firmware image rejection is device-specific, e.g., if different keys are used to sign firmware images for different devices, then attempting to commit or activate an inappropriate firmware image fails because the device is unable to validate the firmware image signature.

4.12 Factory Default Requirements

This section defines additional requirements for the state of the device as shipped from the factory. In addition to the factory default requirements in this section, factory default requirements listed in other sections of this document are also required (e.g., [NVMe-AD-22](#)).

Requirement ID	Description
FDEF-1	All firmware slots shall contain the most recent production firmware revision.
FDEF-2	All logical blocks shall be deallocated.

Requirement ID	Description
FDEF-3	The following SMART / Health Information log page (Log Identifier 02h) fields shall be cleared to 0h: Critical Warning, Endurance Group Critical Warning Summary, Data Units Read, Data Units Written, Host Read Commands, Host Write Commands, Controller Busy Time, Power Cycles, Power On Hours, Unsafe Shutdowns, Media, and Data Integrity Errors, Percentage Used, and Number of Error Information Log Entries.
FDEF-4	The Available Spare field in the SMART / Health Information log page (Log Identifier 02h) shall be set to a value of 100.
FDEF-5	The Total Number of Events field in the Persistent Event log page (Log Identifier 0Dh) shall be cleared to 0h.
FDEF-6	All features that are saveable shall not have a saved value unless otherwise specified. This requirement applies to features in the NVM Express Specifications and this specification.

4.13 Deallocation Requirements

Requirement ID	Description
TRIM-1	The device shall support the Deallocate attribute of the Dataset Management command.
TRIM-2	Once the device has deallocated a logical block, a read of that logical block shall return all bytes cleared to 0h until that logical block has been modified by a command (e.g., Write, Copy, etc.) (i.e., bits 2:0 = 001b in the Deallocate Logical Block Features (DLFEAT) field in the Identify Namespace data structure).
TRIM-3	Obsolete (see TRIM-2).
TRIM-4	Device deallocated logical blocks shall provide the performance and reliability benefits of overprovisioned space.
TRIM-5	The device shall support Garbage Collection during periods of no I/O (Idle GC).
TRIM-6	Processing of deallocation requested by a Dataset Management command shall not cause read latency for LBAs that are outside the LBA ranges being deallocated to change by more than 5% from baseline.
TRIM-7	If Read I/O occurs while Idle GC is active, then Read latency shall not increase more than 5% from baseline.
TRIM-8	If any device deallocated logical blocks have been subsequently read or written to, then the contents of those logical blocks shall not change as a consequence of an unsafe power down event.
TRIM-9	The device shall deallocate data to the maximum extent possible provided that it does not violate TRIM-6 or TRIM-7. Background deallocate processing is allowed provided that it does not violate TRIM-8.

4.14 Sector Size and Namespace Support

Requirement ID	Description
SECTOR-1	Obsolete. Replaced by SECTOR-4.
SECTOR-2	Obsolete. Replaced by SECTOR-4.
SECTOR-3	A new device shipped from the factory shall have one active Namespace whose size in bytes and capacity in bytes are the same and consume the maximum capacity that is listed on the device label (see SECTOR-5).
SECTOR-4	The device shall support 512-byte and 4096-byte logical block sizes.
SECTOR-5	The capacity listed on the device label (see the capacity row in LABL-1) and the maximum number of logical blocks that the device is able to allocate to a single namespace (i.e., the maximum possible value of NCAP) shall comply with the latest revision of the SFF-8447 Specification for LBA Count for Disk Drives: • for all form factors, including form factors not explicitly listed in the SFF-8447 Specification; and • for all LBA Formats supported by the device.
SECTOR-6	A device that has 128TB raw NAND capacity shall list a capacity of 122.88 TB or greater on the device label. A device that has 256TB raw NAND capacity shall list a capacity of 245.76 TB or greater on the device label. Some devices are required to list exactly 122.88 TB capacity or exactly 245.76 TB capacity on the device label, i.e., listing a greater capacity is prohibited, see DP-CFG-12 .

4.15 Set/Get Features Requirements

This section describes features defined by this specification. Unless otherwise specified, the device shall support all the features defined in this section.

4.15.1 General Feature Requirements

Requirement ID	Description
GETF-1	For any Feature Identifier defined in this section, Selection (SEL) values 00b to 11b in Dword 10 of the Get Features command shall be supported.
GETF-2	If the feature requested by Set Features or by Get Features is not supported, then a status error code of 02h (Invalid Field in Command) shall be returned.
GETF-3	The device shall not implement a Feature with Feature Identifier D0h.
GETF-4	For any Feature Identifier defined in this section that is not Namespace scoped, the host should either clear the Namespace Identifier (NSID) field in the Get Features command to zero or set that field to FFFFFFFFh. In addition, the host may set that field to a valid NSID if the feature is Namespace scoped. The device shall return the appropriate status based on the NVM Express Specifications.

Requirement ID	Description		
GETF-5	If the SEL field is set to 11b (i.e., Supported Features) in a Get Features command for any Feature Identifier defined in this section, then the following capabilities for that Feature Identifier shall be returned in CQE Dword 0:		
	Bit	Bit Name	Bit Value
	7:3	Reserved	0b
	2	Changeable (CHANG)	1b
	1	NS Specific (NSSPEC)	See below
	0	Saveable (SVBL)	See below
	If the scope of the Feature (see Section 4.15.2 DSSD Feature Requirements) is Namespace, then the NSSPEC bit shall be set to 1b, otherwise, the NSSPEC bit shall be cleared to 0b. If the Feature is saveable (see Section 4.15.2 DSSD Feature Requirements), then the SVBL bit shall be set to 1b, otherwise the SVBL bit shall be cleared to 0b.		

4.15.2 DSSD Feature Requirements

The following table defines the scope and persistence for all DSSD specific Features:

Feature Identifier	Scope	Persistence	Feature Name	Reference Section
C0h	NVM subsystem	No	Event Injection	4.15.3
C1h	NVM subsystem	N/A	Obsolete	N/A
C2h	NVM subsystem	Saveable	EOL/PLP Failure Mode	4.15.5
C3h	Controller	No	Clear PCIe Correctable Error Counters	4.15.7
C4h	NVM subsystem	Saveable	Enable IEEE1667 Silo	4.15.9
C5h	Controller	Saveable	Latency Monitor	4.15.11
C6h	NVM subsystem	Saveable	PLP Health Check Interval	4.15.13
C7h	NVM subsystem	Saveable	DSSD Power State	4.15.15
C8h	NVM subsystem	Saveable	Telemetry Profile	4.15.17
C9h	Controller	No	DSSD Asynchronous Event Configuration	4.15.19
CAh	NVM subsystem	Saveable	Idle Wake Up Time Configuration	4.15.21
CBh	NVM subsystem	Saveable	Max PCIe Interface Configuration	4.15.23

Scope KEY:

- Namespace = The Set Feature affects a specific namespace.
- Controller = The Set Feature affects the controller that is processing the command.
- NVM subsystem = The Set Feature affects the NVM subsystem.

Persistence KEY:

- Yes = Current setting persists across power cycles and resets, and the Feature is not saveable.
- No = Current setting does not persist across power cycles and resets, and the Feature is not saveable.
- Saveable = Current setting does not persist across power cycles and resets, and the Feature is saveable.

The device shall support the following additional vendor unique Set/Get Features Identifiers.

4.15.3 Event Injection (Feature Identifier C0h) Set Features

Feature to inject an event to be simulated and reported by the device for the purpose of exercising the event behavior or error handling and recovery functionality in the device and the host. For injected errors, the device is not required to actually undergo the injected error (e.g. perform an unsafe shutdown or corrupt the FTL), but the device is required to behave as if the injected error has occurred.

If multiple Set Features commands for this feature are sent by the host, then only information from the most recent successful command is retained (i.e., subsequent commands replace information provided by previous commands).

Requirement ID	Dword	Field	Bits	Field Description
SERRI-1	0	Command Identifier (CID)	31:16	Should be set as defined in the NVM Express Base Specification.

Requirement ID	Dword	Field	Bits	Field Description
SERRI-2	0	PRP or SGL for Data Transfer (PSDT)	15:14	Should be cleared to 00b to specify that PRPs are used.
SERRI-3	0	Reserved	13:10	Should be cleared to zero.
SERRI-4	0	Fused Operation (FUSE)	9:8	Should be cleared to 00b.
SERRI-5	0	Opcode (OPC)	7:0	Should be set to 09h.
SERRI-6	1	Namespace Identifier (NSID)	31:0	See GETF-4 .
SERRI-7	3:2	Reserved	All	Should be cleared to zero.
SERRI-8	5:4	Metadata Pointer (MPTR)	All	Should be cleared to zero.
SERRI-9	9:6	Data Pointer (DPTR)	All	Should contain one or two PRPs that specify a physically contiguous 4096-byte address range containing 0 to 127 Event Injection Data Structure Entries.
SERRI-10	10	Save (SV)	31	The device shall not support setting this bit to 1b. If the controller receives this Set Features command with the bit set to 1b, then the device shall abort the command with a status of Feature Identifier Not Saveable.
SERRI-11	10	Reserved	30:8	Should be cleared to zero.
SERRI-12	10	Feature Identifier (FID)	7:0	Should be set to C0h.
SERRI-13	11	Reserved	31:7	Should be cleared to zero.
SERRI-14	11	Number of Event Injections	6:0	The host sets this field to 000001b to indicate there is a valid Event Injection Data Entry described in the address range pointed to by the Data Pointer (DPTR) field. The host clears this field to 0b to clear an untriggered injected event if any. If the host sets this field to any other value, the device shall abort the Set Features command with Invalid Field in Command status.
SERRI-15	13:12	Reserved	All	Should be cleared to zero.
SERRI-16	14	UUID Index	31:0	Should be set per UUID-3 .
SERRI-17	15	Reserved	31:0	Should be cleared to zero.

Requirement ID	Description
ERRI-1	The number of entries in the Number of Event Injections field shall be 1.
ERRI-2	A value of 0000000b in the Number of Event Injections field shall clear the untriggered event injection, if any.
ERRI-3	Obsolete.
ERRI-4	The host shall clear any unused entries in the Event Injection data structure to zero and the device shall ignore all zeroed entries. The device shall check at least the first four bytes of each Event Injection Entry data structure to determine if it is zeroed.
ERRI-5	The device shall abort the Event Injection Set Features command if the request contains an event injection type that is not supported.
ERRI-6	Once the trigger conditions specified in an Event Injection Entry are met, the device shall inject the defined error event such that the host can detect the error through device behavior, e.g., an AEN being sent, the CFS bit being set, delayed receipt of command completion, or command being aborted. The device is not required to cause the injected error to occur (e.g., injecting an Incomplete Shutdown error requires the device to behave as if an Incomplete Shutdown occurred, but does not require the device to perform an Incomplete Shutdown).
ERRI-7	Obsolete.
ERRI-8	The device shall clear the triggered event, if any, at the next power cycle (i.e., next power cycle reverts device behavior to have no injected event) unless otherwise specified for a specific injected event in Section 4.15.3.3 Event Definition Table (e.g., see the definition of Recovery Type 4 in EVTREC-4).

4.15.3.1 Event Injection Entry Data Structure

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
ERRIE-1	0	Event Flags	1	Event Flags definition:	
				Bit	Bit Description
				7:2	Reserved. Shall be cleared to zero.
				1	Single Instance: Required to be set to 1b to indicate a single instance event injection. If cleared to 0b, the device shall abort the command with Invalid Field in Command status.
				0	Event Injection Enable: Required to be set to 1b to indicate that event injection is enabled. If cleared to 0b, the device shall abort the command with Invalid Field in Command status.
ERRIE-2	1	Reserved	1	Shall be cleared to zero.	

Requirement ID	Byte Address	Field	# of Bytes	Field Description
ERRIE-3	3:2	Event Injection Type	2	See the Event Definition Table for additional information (see Section 4.15.3.3).
ERRIE-4	31:4	Event Injection Type Specific Definition	28	Event Injection Type specific definition (see Section 4.15.3.4 Device Event Injection Type).

4.15.3.2 Event Injection Recovery Types

Requirement ID	Recovery Type	Description
EVTREC-1	1	These events require the device to: 1. Either send the Error Recovery AEN (C1h) or set the CFS bit to 1b; 2. Populate the Error Recovery log page; 3. Perform error recovery in conjunction with the host; and 4. Exit event injection only upon successful completed of error recovery (step 3) or power cycle.
EVTREC-2	2	These are non-persistent single shot events that remain outstanding until the event is performed. Once the event has been performed, the device automatically exits event injection.
EVTREC-3	3	These are persistent condition events that require the device to exit event injection in order to clear the persistent behavior (see SERRI-14).
EVTREC-4	4	These are persistent condition events that require an event-specific action for the device to exit event injection in order to clear the persistent behavior. The event-specific action is described in the event entry in the Event Definition Table. The mechanism to exit event injection defined in SERRI-14 has no effect on the persistent behavior that results from injecting one of these events.

4.15.3.3 Event Definition Table

Requirement ID	Event ID	Event Name	Event Definition	Recovery Type
EVTDEF-1	0000h	Reserved	The device shall not support this Error ID value and shall abort a command that contains this value with Invalid Field In Command status.	N/A
EVTDEF-2	0001h	CPU/Controller Hang	The device shall respond to this event injection by simulating a hardware logic hang condition.	1
EVTDEF-3	0002h	NAND Hang	The device shall respond to this event injection by simulating a NAND logic hang condition.	1

Requirement ID	Event ID	Event Name	Event Definition	Recovery Type
EVTDEF-4	0003h	PLP Defect	The device shall respond to this event injection by simulating a PLP failure condition. The device shall enter the ROWTM state defined by the current setting of the ROWTM feature (C2h), shall set the appropriate critical warning bits in the SMART/Health and Information log page (Log Identifier 02h), and shall complete the required AERs to the host.	3
EVTDEF-5	0004h	Logical Firmware Error	The device shall respond to this event injection by simulating a firmware assert condition.	1
EVTDEF-6	0005h	DRAM Corruption Critical Path	The device shall respond to this event injection by simulating DRAM corruption on the critical data path that is not correctable by ECC (e.g., SECEDED).	1
EVTDEF-7	0006h	DRAM Corruption Non-Critical Path	The device shall respond to this event injection by simulating DRAM corruption not on the data path that is not correctable by ECC (e.g., SECEDED).	1
EVTDEF-8	0007h	NAND Corruption	The device shall respond to this event injection by simulating NAND corruption that is not correctable. Reads to affected LBAs shall return Uncorrectable read errors.	3
EVTDEF-9	0008h	SRAM Corruption	The device shall respond to this event injection by simulating SRAM corruption on the critical data path that is not correctable by ECC (e.g., SECEDED).	1
EVTDEF-10	0009h	HW Malfunction	The device shall respond to this event injection by simulating a hardware hang condition.	1
EVTDEF-11	000Ah	No More NAND Spares Available	The device shall respond to this event injection by simulating an EOL condition where the device has insufficient NAND blocks to continue to support Write operations (see GROWTM-2 and EOL-5). The device shall enter Read Only Mode, shall set the appropriate critical warning bits in the SMART/Health and Information log page (Log Identifier 02h) and complete any required AERs to the host.	3
EVTDEF-12	000Bh	Incomplete Shutdown	The device shall respond to this event injection by simulating an incomplete shutdown condition on the next power cycle where the device shall behave as if the device was not able to flush all its metadata to stable storage.	2

Requirement ID	Event ID	Event Name	Event Definition	Recovery Type
EVTDEF-13	000Ch	Metadata Corruption	The device shall respond to this event injection by simulating an unrepairable corruption of a metadata structure (e.g., FTL).	1
EVTDEF-14	000Dh	Critical Garbage Collection	The device shall respond to this event injection by behaving as if the amount of erased usable NAND has dropped below a threshold that causes the device to prioritize garbage collection and NAND erasure to avoid having to reject writes because no NAND is available to be written.	3
EVTDEF-15	000Eh	Latency Spike	The device shall respond to this event injection by inserting a delay in the first IO after the number of reads specified in NRTDE. The length of the delay is specified in the Latency Duration field of Event Injection Type Specific Definition in the (see ERRIEDP-4).	2
EVTDEF-16	000Fh	I/O command failure	The device shall respond to this event injection by returning a failure status code on the next I/O command after the number of reads specified in NRTDE have completed.	2
EVTDEF-17	0010h	I/O command timeout	The device shall respond to this event injection by not returning a CQE on the next I/O command after the number of reads specified in NRTDE have completed.	2
EVTDEF-18	0011h	Admin command failure	The device shall respond to this event injection by returning a failure status code on the next Admin command after the number of reads specified in NRTDE have completed.	2
EVTDEF-19	0012h	Admin command timeout	The device shall respond to this event injection by not returning a CQE on the next Admin command after the number of reads specified in NRTDE have completed.	2
EVTDEF-20	0013h	Thermal Throttle Engaged	The device shall respond to this event injection by setting the Temperature Threshold Condition (TTC) bit (I.e., bit 1) to 1b in the Critical Warning field in the SMART / Health Information log page (Log Identifier 02h), completing an appropriately populated AER to send a Temperature Threshold AEN (event 01h for Asynchronous Event Type 01h) to the host and engaging first level thermal throttling. This condition shall persist until the device is reset by any Controller Level Reset	4

Requirement ID	Event ID	Event Name	Event Definition	Recovery Type
			(including a CLR caused by a power cycle), or the device receives a Thermal Throttle Disengaged (see EVTDEF-21)) Event Injection.	
EVTDEF-21	0014h	Thermal Throttle Disengaged	If the device is thermally throttling due to an active Thermal Throttle Engaged (see EVTDEF-20) Event Injection, the device shall respond to this event injection by sending the Temperature Threshold AEN (event 01h for Asynchronous Event Type 01h), disengaging thermal throttling, and exiting event injection. If the device is not thermally throttling due to an active Thermal Throttle Engaged Event Injection, then injecting this event has no effect.	2
EVTDEF-22	0015h	Critical Temperature Event	The device shall respond to this event injection by setting bit-1 of the Critical Warning field in the SMART / Health Information log page (Log Identifier 02h), completing an appropriately populated AER to the host, engaging first level thermal throttling and performing an emergency shutdown of the controller. This condition shall persist until the device is power cycled.	4
EVTDEF-23	0016h	NAND Die Offline	The device shall respond to this event injection by simulating the loss of a NAND die.	3
EVTDEF-24	0017h	Sanitize Command Failure	The device shall respond to this event injection by returning status code (1Ch, Sanitize Failed) for the next Sanitize command that is submitted to this controller.	3
EVTDEF-25	0018h	Reserved	Reserved for future use	
EVTDEF-26	0019h	Require Format NVM Use User Data Erase	If the device supports using the Crypto Erase option (SES=010b) instead of the User Data Erase option (SES=001b) when User Data Erase is requested in a Format NVM command, then the device shall respond to this error injection by using User Data Erase when requested in the next Format NVM command submitted to this controller.	2
EVTDEF-27	001Ah	Inject PCIe Correctable Errors	The device shall respond to this event injection by reporting randomly chosen PCIe Correctable Errors in the PCIe Correctable Error Status Register (Offset 10h).	3

Requirement ID	Event ID	Event Name	Event Definition	Recovery Type
EVTDEF-28	001Bh	Inject PCIe Uncorrectable Errors	The device shall respond to this event injection by reporting randomly chosen PCIe Uncorrectable Errors in the PCIe Uncorrectable Error Status Register (Offset 04h).	3
EVTDEF-29	001Ch	Clear the Persistent Event Log	The device shall respond to this event injection by clearing the Persistent Event Log to contain no entries. The device shall remain in this state until the device exits event injection mode. Upon exiting event injection mode, the device may or may not restore the original PEL contents prior to injection of this event.	3
EVTDEF-30	001Dh	Sanitize Operation Failure	The device shall respond to this event injection by completing the next Sanitize command submitted to this controller with successful status and then completing the Sanitize operation with the status value 011b in the Sanitize Status Log Page.	3
EVTDEF-31	001Eh	Random I/O Latency Spikes Over Time	The device shall respond to this event injection by starting to induce latency spikes on subsequent I/O commands. The latency spikes shall occur on commands randomly over time with a minimum occurrence of 100 spikes per minute until event injection is exited. The latency value to delay each command shall also be randomly chosen within a range of 5 ms – 30 ms.	3
EVTDEF-32	001Fh	Reset To Factory Default Settings	The device shall respond to this event injection by simulating the restoration of the device to its factory default state.	3
EVTDEF-33	0020h	Supply Voltage Drop	The device shall respond to this event injection by initiating the power loss protection processing that should occur due to a sudden supply voltage drop. This event shall also cause the PLP Start Count (SMART-24) value reported in the SMART/Health Information Extended log page (Log Identifier C0h) to increment.	2
EVTDEF-34	0021h	Available Spare Threshold	The device shall respond to this event injection by simulating the Available Spare Capacity falling below the Available Spare Threshold (see EOL-8).	3
EVTDEF-35	0022h	Volatile Memory Backup Failure	The device shall respond to this event injection by simulating volatile memory backup device failure	3

Requirement ID	Event ID	Event Name	Event Definition	Recovery Type
EVTDEF-36	0023h - FFFFh	Reserved Range	The device shall not support Event ID values in this range and shall respond with Invalid Field In Command if an Event ID value in this range is sent by the host.	N/A

4.15.3.4 Device Event Injection Type

The device shall inject a device event that the host can detect through device behavior, e.g., an AEN being sent, the CFS bit being set, delayed receipt of command completion, or command being aborted.

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
ERRIEDP-1	0	Event Entry Flags	1	Device Event Entry Flags:	
				Bit	Bit Description
				7:2	Reserved.
				1	Shall be set to 1b.
				0	Shall be set to 1b.
ERRIEDP-2	1	Reserved	1	Shall be cleared to zero.	
ERRIEDP-3	3:2	Event Injection Type	2	Shall be set to a value defined in Section 4.15.3.3 Event Definition Table .	
ERRIEDP-4	31:4	Event Injection Type Specific Definition	28	Device Event Injection information:	
				Byte Address	Byte Description
				31:10	Reserved.
				11:8	Latency Duration: If this Event Injection Type is Latency Spike (000Eh) then this field indicates the number of microseconds the device will delay the triggered IO. For all other Event Injection Types, this field is reserved.
				7:6	Reserved.
5:4	Number of Reads to Trigger Device Event (NRTDE): Indicates the number of Read commands the device shall process and complete before performing the injected event. If this field is cleared to 0h, the event occurs immediately. For all values of this field, the event remains outstanding until the event is performed.				

Requirement ID	Byte Address	Field	# of Bytes	Field Description
				The completed Read command that triggers occurrence of the injected device event is not affected by that device event (i.e., the Read command is completed before that device event occurs).

4.15.4 Event Injection (Feature Identifier C0h) Get Features

This Get Features returns the event injection that is enabled on the device if any, GETF-4 specifies the acceptable values of the NSID field in the Get Features command. The attributes specified in Section 4.15.3.4 - Device Event Injection Type are returned in Dword 0 of the completion queue entry and the Event Injection data structure specified in Section 4.15.3.1 - Event Injection Entry Data Structure is returned for the event injection in the data buffer for that command. If there are no currently enabled event injections, the data buffer returned shall contain all zeroes. The device shall clear to zero all unused entries in the Event Injection data structure.

4.15.4.1 Event Injection – Get Features Completion Queue Entry Dword 0

Requirement ID	Field	Bits	Field Description
GERRI-1	Reserved	31:7	Shall be cleared to zero.
GERRI-2	Number of Event Injections (NUME)	6:0	The returned value depends on the contents of the Select (SEL) field in the Get Features command. Current value (Select (SEL) field cleared to 000b): This field indicates if there is an untriggered event injection. If so, information about that outstanding event injection is returned in the command data buffer (see Section 4.15.3.1 Event Injection Entry Data Structure for the format of the entry). Default value (Select (SEL) field set to 001b) or saved value (Selection (SEL) set to 010b): This field shall be cleared to 00h. This feature is not saveable (see SERRI-10), so a request for the saved value returns the default value. Capabilities (Select (SEL) field set to 011b): See GETF-5.

4.15.5 PLP Failure Mode (Feature Identifier C2h) Set Features

This Set Features defines the mode to which the device shall transition to on failure of the Power Loss Protection (PLP) circuitry:

Requirement ID	Description
ROWTM-1	The device shall default from the factory to Read Only Mode (ROM) (01b). This requirement applies regardless of whether the PLP Failure Mode feature is enabled or disabled (see DP-CFG-6).

Requirement ID	Dword	Field	Bits	Field Description	
SROWTM-1	0	Command Identifier (CID)	31:16	Shall be set as defined in NVM Express Base Specification.	
SROWTM-2	0	PRP or SGL for Data Transfer (PSDT)	15:14	Shall be cleared to 00b to specify that PRPs are used.	
SROWTM-3	0	Reserved	13:10	Shall be cleared to zero.	
SROWTM-4	0	Fused Operation (FUSE)	9:8	Shall be cleared to 00b.	
SROWTM-5	0	Opcode (OPC)	7:0	Shall be set to 09h.	
SROWTM-6	1	Namespace Identifier (NSID)	31:0	See GETF-4 .	
SROWTM-7	3:2	Reserved	All	Shall be cleared to zero.	
SROWTM-8	5:4	Metadata Pointer (MPTR)	All	Shall be cleared to zero.	
SROWTM-9	9:6	Data Pointer (DPTR)	All	Shall be cleared to zero.	
SROWTM-10	10	Save (SV)	31	This bit specifies that the controller shall save the End-of-Life Behavior state so that the state persists through all power states and resets. The device shall support setting this bit to 1b.	
SROWTM-11	10	Reserved	30:8	Shall be cleared to zero.	
SROWTM-12	10	Feature Identifier (FID)	7:0	Shall be set to C2h.	
SROWTM-13	11	End of Life Behavior	31:30	Field to indicate device write behavior at End of Life (EOL) or in the event of loss of PLP functionality. See EOL-5 for definition on EOL.	
				Value	Description
				00b	Reserved.
				01b	The device shall transition to Read Only Mode (ROM) in the event of PLP failure or at EOL.
				10b	The device shall transition to Write Through Mode (WTM) in the event of PLP failure and transition to Read Only Mode (ROM) at EOL.

Requirement ID	Dword	Field	Bits	Field Description	
				11b	The device shall continue to operate as normal in the event of PLP failure and transition to Read Only Mode (ROM) at EOL where EOL is defined as the device no longer has enough spare blocks to support Write commands.
SROWTM-14	11	Reserved	29:0	Shall be cleared to zero.	
SROWTM-15	13:12	Reserved	All	Shall be cleared to zero.	
SROWTM-16	14	UUID Index	31:0	Shall be set per UUID-3 .	
SROWTM-17	15	Reserved	31:0	Shall be cleared to zero.	

4.15.6 PLP Failure Mode (Feature Identifier C2h) Get Features

[GETF-4](#) specifies the acceptable values of the NSID field in the Get Features command. Dword 0 of command completion queue entry:

Requirement ID	Field	Bits	Field Description								
GROWTM-1	Reserved	31:3	Shall be cleared to zero.								
GROWTM-2	End of Life Behavior	2:0	Field to indicate what the device write behavior is configured for at End of Life (EOL) or in the event of loss of PLP functionality. The following tables define the required return values for each value of the Select (SEL) field in the Get Features command. All other bit values are reserved. Current value (Select (SEL) field cleared to 000b):								
			<table><tr><th>Value</th><th>Description</th></tr><tr><td>001b</td><td>The device will transition to Read Only Mode (ROM) in the event of PLP failure or at EOL.</td></tr><tr><td>010b</td><td>The device will transition to Write Through Mode (WTM) in the event of PLP failure and transition to Read Only Mode (ROM) at EOL.</td></tr><tr><td>011b</td><td>The device will continue to operate as normal in the event of PLP failure and transition to Read Only Mode (ROM) at EOL.</td></tr></table>	Value	Description	001b	The device will transition to Read Only Mode (ROM) in the event of PLP failure or at EOL.	010b	The device will transition to Write Through Mode (WTM) in the event of PLP failure and transition to Read Only Mode (ROM) at EOL.	011b	The device will continue to operate as normal in the event of PLP failure and transition to Read Only Mode (ROM) at EOL.
			Value	Description							
			001b	The device will transition to Read Only Mode (ROM) in the event of PLP failure or at EOL.							
			010b	The device will transition to Write Through Mode (WTM) in the event of PLP failure and transition to Read Only Mode (ROM) at EOL.							
			011b	The device will continue to operate as normal in the event of PLP failure and transition to Read Only Mode (ROM) at EOL.							
			Default value (Select (SEL) field set to 001b):								
			<table><tr><th>Value</th><th>Description</th></tr><tr><td>001b</td><td>Read Only Mode (ROM) is the factory default.</td></tr><tr><td>010b</td><td>The Write Through Mode (WTM) is the factory default.</td></tr><tr><td>011b</td><td>Normal operation is the factory default for PLP failure. Read Only Mode (ROM) is the factory default at EOL.</td></tr></table>	Value	Description	001b	Read Only Mode (ROM) is the factory default.	010b	The Write Through Mode (WTM) is the factory default.	011b	Normal operation is the factory default for PLP failure. Read Only Mode (ROM) is the factory default at EOL.
			Value	Description							
			001b	Read Only Mode (ROM) is the factory default.							
010b	The Write Through Mode (WTM) is the factory default.										
011b	Normal operation is the factory default for PLP failure. Read Only Mode (ROM) is the factory default at EOL.										

Requirement ID	Field	Bits	Field Description	
			Saved value (Select (SEL) field set to 010b):	
			Value	Description
			001b	The saved state is Read Only Mode (ROM).
			010b	The saved state is Write Through Mode (WTM).
			011b	The saved state is to operate as normal in the event of PLP failure and Read Only Mode (ROM) at EOL.
			Capabilities (Select (SEL) field set to 011b): See GETF-5 .	

4.15.7 Clear PCIe Correctable Error Counters (Feature Identifier C3h) Set Features

Requirement ID	Dword	Field	Bits	Field Description
CPCIE-1	0	Command Identifier (CID)	31:16	Shall be set as defined in NVM Express Base Specification.
CPCIE-2	0	PRP or SGL for Data Transfer (PSDT)	15:14	Shall be cleared to 00b to specify that PRPs are used.
CPCIE-3	0	Reserved	13:10	Shall be cleared to zero.
CPCIE-4	0	Fused Operation (FUSE)	9:8	Shall be cleared to 00b.
CPCIE-5	0	Opcode (OPC)	7:0	Shall be set to 09h.
CPCIE-6	1	Namespace Identifier (NSID)	31:0	See GETF-4 .
CPCIE-7	3:2	Reserved	All	Shall be cleared to zero.
CPCIE-8	5:4	Metadata Pointer (MPTR)	All	Shall be cleared to zero.
CPCIE-9	9:6	Data Pointer (DPTR)	All	Shall be cleared to zero.
CPCIE-10	10	Save (SV)	31	The device shall not support setting this bit to 1b. If the controller receives this Set Features command with the bit set to 1b, then the device shall abort the command with a status of Feature Identifier Not Saveable.
CPCIE-11	10	Reserved	30:8	Shall be cleared to zero.
CPCIE-12	10	Feature Identifier (FID)	7:0	Shall be set to C3h.

Requirement ID	Dword	Field	Bits	Field Description
CPCIE-13	11	Clear PCIe Error Counters	31	Set to 1b to clear all PCIe correctable error counters in the SMART / Health Information Extended log page (Log Identifier C0h). This clears the counters for the following PCIe correctable errors: bad TLP, bad DLLP, receiver error, replay timeouts, replay rollovers. The OCP nvme-cli plugin command “clear-pcie-correctable-errors” can also perform this operation.
CPCIE-14	11	Reserved	30:0	Shall be cleared to zero.
CPCIE-15	13:12	Reserved	All	Shall be cleared to zero.
CPCIE-16	14	UUID Index	31:0	Shall be set per UUID-3 .
CPCIE-17	15	Reserved	31:0	Shall be cleared to zero.

4.15.8 Clear PCIe Correctable Error Counters (Feature Identifier C3h) Get Features

A Get Features command for Feature Identifier C3h should not be issued because no useful information is returned. [GETF-4](#) specifies the acceptable values of the NSID field in a Get Features command.

Requirement ID	Description
GPCIE-1	The returned value depends on the value of the Select (SEL) field in the Get Features command. If the Select (SEL) field is cleared to 000b (current value), set to 001b (default value), or set to 010b (saved value), then the device shall clear Dword 0 of the completion queue entry to zero. This feature is not saveable (see CPCIE-10), so a request for the saved value returns the default value. If the Select (SEL) field is set to 011b (i.e., Capabilities), see GETF-5.

4.15.9 Enable IEEE1667 Silo (Feature Identifier C4h) Set Features

This Set Features shall return an error if the OPAL Security state is not Manufactured Inactive.

Requirement ID	Dword	Field	Bits	Field Description
S1667-1	0	Command Identifier (CID)	31:16	Shall be set as defined in NVM Express Base Specification.
S1667-2	0	PRP or SGL for Data Transfer (PSDT)	15:14	Shall be cleared to 00b to specify that PRPs are used.
S1667-3	0	Reserved	13:10	Shall be cleared to zero.
S1667-4	0	Fused Operation (FUSE)	9:8	Shall be cleared to 00b.
S1667-5	0	Opcode (OPC)	7:0	Shall be set to 09h.

Requirement ID	Dword	Field	Bits	Field Description
S1667-6	1	Namespace Identifier (NSID)	31:0	See GETF-4 .
S1667-7	3:2	Reserved	All	Shall be cleared to zero.
S1667-8	5:4	Metadata Pointer (MPTR)	All	Shall be cleared to zero.
S1667-9	9:6	Data Pointer (DPTR)	All	Shall be cleared to zero.
S1667-10	10	Save (SV)	31	This bit specifies that the controller shall save the IEEE1667 Silo Enable/Disable state so that the state persists through all power states and resets. The device shall support setting this bit to 1b.
S1667-11	10	Reserved	30:8	Shall be cleared to zero.
S1667-12	10	Feature Identifier (FID)	7:0	Shall be set to C4h.
S1667-13	11	Enable IEEE1667 Silo	31	If set to 0b, the IEEE1667 silo shall be disabled no later than the next power cycle. If set to 1b, the IEEE1667 silo shall be enabled no later than the next power cycle.
S1667-14	11	Reserved	30:0	Shall be cleared to zero.
S1667-15	13:12	Reserved	All	Shall be cleared to zero.
S1667-16	14	UUID Index	31:0	Shall be set per UUID-3 .
S1667-17	15	Reserved	31:0	Shall be cleared to zero.

4.15.10 Enable IEEE1667 Silo (Feature Identifier C4h) Get Features

[GETF-4](#) specifies the acceptable values of the NSID field in the Get Features command. Dword 0 of command completion queue entry.

Requirement ID	Field	Bits	Field description	
G1667-1	Reserved	31:3	Shall be cleared to zero.	
G1667-2	IEEE1667 Silo Enabled	2:0	The following tables define the required return values for each value of the Select (SEL) field in the Set Features command. All other values are illegal.	
			Current value (Select (SEL) field cleared to 000b):	
			Value	Description
			000b	The IEEE1667 silo is currently disabled.
			001b	The IEEE1667 silo is currently enabled.

Requirement ID	Field	Bits	Field description	
			Default state (Select (SEL) field set to 001b):	
			Value	Description
			000b	The IEEE1667 silo factory default is disabled. Unless otherwise specified, the device shall set the default value of the IEEE1667 silo to 000b (disabled).
			001b	The IEEE1667 silo factory default is enabled.
			Saved state (Select (SEL) field set to 010b):	
			Value	Description
			000b	The IEEE1667 silo saved state is disabled.
			001b	The IEEE1667 silo saved state is enabled.
			Capabilities (Selection (SEL) field set to 011b): See GETF-5 .	

4.15.11 Latency Monitor (Feature Identifier C5h) Set Features

This configures the Latency Monitor Feature.

Requirement ID	Dword	Field	Bits	Field Description
LMSF-1	0	Command Identifier (CID)	31:16	Shall be set as defined in NVM Express Base Specification.
LMSF-2	0	PRP or SGL for Data Transfer (PSDT)	15:14	Shall be cleared to 00b to specify that PRPs are used.
LMSF-3	0	Reserved	13:10	Shall be cleared to zero.
LMSF-4	0	Fused Operation (FUSE)	9:8	Shall be cleared to 00b.
LMSF-5	0	Opcode (OPC)	7:0	Shall be set to 09h.
LMSF-6	1	Namespace Identifier (NSID)	31:0	See GETF-4 .
LMSF-7	3:2	Reserved	All	Shall be cleared to zero.
LMSF-8	5:4	Metadata Pointer (MPTR)	All	Shall be cleared to zero.
LMSF-9	9:6	Data Pointer (DPTR)	All	Shall contain one PRP that specifies a physically contiguous 4096-byte address range that is 4096-byte aligned (see Section 4.15.11.1 Latency Monitoring Data Structure Entry).

Requirement ID	Dword	Field	Bits	Field Description
LMSF-10	10	Save (SV)	31	This bit specifies that the controller shall save the data pointed to by the Data Pointer in LMSF-9 (Data Pointer (DPTR)) so that the data persists through all power states and resets. The device shall support setting this bit to 1b. The host should set this bit to 1b. The device shall ignore the value of this bit and process the Set Features command for this feature as if this bit is set to 1b.
LMSF-11	10	Reserved	30:8	Shall be cleared to zero.
LMSF-12	10	Feature Identifier (FID)	7:0	Shall be set to C5h.
LMSF-13	11	Reserved	31:0	Shall be cleared to zero.
LMSF-14	12:13	Reserved	All	Shall be cleared to zero.
LMSF-15	14	UUID Index	31:0	Shall be set per UUID-3 .
LMSF-16	15	Reserved	31:0	Shall be cleared to zero.

4.15.11.1 Latency Monitoring Data Structure Entry

This data structure is 4096 bytes with the following functional requirements and field format:

Requirement ID	Byte Address	Field	# of Bytes	Field Description
LMDS-1	1:0	Active Bucket Timer Threshold	2	This is the value that loads the Active Bucket Timer Threshold.
LMDS-2	2	Active Threshold A	1	This is the value that loads into the Active Threshold A
LMDS-3	3	Active Threshold B	1	This is the value that loads into the Active Threshold B
LMDS-4	4	Active Threshold C	1	This is the value that loads into the Active Threshold C
LMDS-5	5	Active Threshold D	1	This is the value that loads into the Active Threshold D
LMDS-6	7:6	Active Latency Config.	2	This is the value that loads into the Active Latency Configuration.
LMDS-7	8	Active Latency Minimum Window	1	This is the value that loads into the Active Latency Minimum Window.

Requirement ID	Byte Address	Field	# of Bytes	Field Description	
LMDS-8	10:9	Debug Log Trigger Enable	2	This is the value that loads into the Debug Log Trigger Enable.	
LMDS-9	11	Discard Debug Log	1	Value	Description
				00h	When cleared to 00h the debug log, if it exists, will not be cleared.
				01h	When set to 01h the debug log will be discarded so another log can be triggered. In addition to this, all the fields in the Set Features Data structure are valid, which will cause the Latency Monitor feature to be reset and loaded with the values from the Set Features command. This shall discard the Debug Log regardless of whether the Latency Monitoring Feature is enabled or disabled.
				02h	When set to 02h the debug log will be discarded so another log can be triggered. In addition to this none of the other fields of the Set Features Data structure are valid. Thus, only the debug log is discarded, and the Latency Monitor feature is not reset or loaded with any new values from the Set Features command. This shall discard the Debug Log regardless of whether the Latency Monitoring Feature is enabled or disabled.
				03h - FFh	Reserved. Shall be cleared to zero.
LMDS-10	12	Latency Monitor Feature Enable	1	When set to 01h the Latency Monitor Feature is enabled. When cleared to 00h the Latency Monitor Feature is disabled. All other values are reserved.	
LMDS-11	4095:13	Reserved	4083	Shall be cleared to zero.	

4.15.12 Latency Monitor (Feature Identifier C5h) Get Features

A Get Features command for Feature Identifier C5h should not be issued because no useful information is returned. [GETF-4](#) specifies the acceptable values of the NSID field in a Get Features command.

Requirement ID	Description
LMGF-1	The returned value depends on the contents of the Select (SEL) field in the Get Features command. If the Select (SEL) field is cleared to 000b (current value), set to 001b (default value), or set to 010b (saved value), then the device shall clear Dword 0 of the completion queue entry to zero. If the Select (SEL) field is set to 011b (i.e., Capabilities), see GETF-5.

4.15.13 PLP Health Check Interval (Feature Identifier C6h) Set Features

This Set Features defines the test interval that the device shall use to test that its Power Loss Protection (PLP) circuitry is healthy.

Requirement ID	Dword	Field	Bits	Field Description
SPLPI-1	0	Command Identifier (CID)	31:16	Shall be set as defined in NVM Express Base Specification.
SPLPI-2	0	PRP or SGL for Data Transfer (PSDT)	15:14	Shall be cleared to 00b to specify that PRPs are used.
SPLPI-3	0	Reserved	13:10	Shall be cleared to zero.
SPLPI-4	0	Fused Operation (FUSE)	9:8	Shall be cleared to 00b.
SPLPI-5	0	Opcode (OPC)	7:0	Shall be set to 09h.
SPLPI-6	1	Namespace Identifier (NSID)	31:0	See GETF-4 .
SPLPI-7	3:2	Reserved	All	Shall be cleared to zero.
SPLPI-8	5:4	Metadata Pointer (MPTR)	All	Shall be cleared to zero.
SPLPI-9	9:6	Data Pointer (DPTR)	All	Shall be cleared to zero.
SPLPI-10	10	Save (SV)	31	This bit specifies that the controller shall save the PLP Health Check Interval so that the time interval persists through all power states and resets. The device shall support setting this bit to 1b.
SPLPI-11	10	Reserved	30:8	Shall be cleared to zero.
SPLPI-12	10	Feature Identifier (FID)	7:0	Shall be set to C6h.

Requirement ID	Dword	Field	Bits	Field Description
SPLPI-13	11	PLP Health Check Interval	31:16	The time interval between PLP health checks in minutes. If cleared to 0000h, then the health check is disabled.
SPLPI-14	11	Reserved	15:0	Shall be cleared to zero.
SPLPI-15	13:12	Reserved	All	Shall be cleared to zero.
SPLPI-16	14	UUID Index	31:0	Shall be set per UUID-3 .
SPLPI-17	15	Reserved	31:0	Shall be cleared to zero.

4.15.14 PLP Health Check Interval (Feature Identifier C6h) Get Features

[GETF-4](#) specifies the acceptable values of the NSID field in the Get Features command. Dword 0 of command completion queue entry.

Requirement ID	Field	Bits	Field description						
GPLPI-1	Reserved	31:16	Shall be cleared to zero.						
GPLPI-2	PLP Health Check Interval	15:0	The following tables define the required return values for each value of the Select (SEL) field in the Get Features command. All other values are illegal. Current value (Select (SEL) field cleared to 000b):						
			<table><tr><th>Value</th><th>Description</th></tr><tr><td>0000h</td><td>The PLP Health Check is currently disabled.</td></tr><tr><td>xxxxh</td><td>The PLP Health Check Interval is currently xxxxh minutes.</td></tr></table>	Value	Description	0000h	The PLP Health Check is currently disabled.	xxxxh	The PLP Health Check Interval is currently xxxxh minutes.
			Value	Description					
			0000h	The PLP Health Check is currently disabled.					
			xxxxh	The PLP Health Check Interval is currently xxxxh minutes.					
			Default value (Select (SEL) field set to 001b):						
			<table><tr><th>Value</th><th>Description</th></tr><tr><td>0000h</td><td>The PLP Health Check Interval factory default is disabled.</td></tr><tr><td>000Fh</td><td>The PLP Health Check Interval factory default is 000Fh minutes.</td></tr></table>	Value	Description	0000h	The PLP Health Check Interval factory default is disabled.	000Fh	The PLP Health Check Interval factory default is 000Fh minutes.
			Value	Description					
			0000h	The PLP Health Check Interval factory default is disabled.					
			000Fh	The PLP Health Check Interval factory default is 000Fh minutes.					
			Saved value (Select (SEL) field set to 010b):						
			<table><tr><th>Value</th><th>Description</th></tr><tr><td>0000h</td><td>The PLP Health Check Interval saved state is disabled.</td></tr><tr><td>xxxxh</td><td>The PLP Health Check Interval saved state is xxxxh minutes.</td></tr></table>	Value	Description	0000h	The PLP Health Check Interval saved state is disabled.	xxxxh	The PLP Health Check Interval saved state is xxxxh minutes.
Value	Description								
0000h	The PLP Health Check Interval saved state is disabled.								
xxxxh	The PLP Health Check Interval saved state is xxxxh minutes.								
Capabilities (Select (SEL) field set to 011b): See GETF-5 .									

4.15.15 DSSD Power State (Feature Identifier C7h) Set Features

Requirement ID	Description
DSSDPSS-1	If the host selects an DSSD Power State via a DSSD Power State (Feature Identifier C7h) Set Feature command, the device shall accept the command and run at the highest powered NVMe Power State whose Maximum Power (MP) is less than or equal to the number of the DSSD Power State in watts (see DCLP-9 and DSSDPSD-3).
DSSDPSS-2	If the host selects a DSSD Power State via DSSD Power State (Feature Identifier C7h) Set Features command and the number of that DSSD Power State is less than the Minimum DSSD Power State (see DCLP-8), the device shall abort the Set Features command with Invalid Field in Command status.

This Set Features causes the device to move to the given DSSD Power State:

Requirement ID	Dword	Field	Bits	Field Description
SDSSDPS-1	0	Command Identifier (CID)	31:16	Shall be set as defined in NVM Express Base Specification.
SDSSDPS-2	0	PRP or SGL for Data Transfer (PSDT)	15:14	Shall be cleared to 00b to specify that PRPs are used.
SDSSDPS-3	0	Reserved	13:10	Shall be cleared to zero.
SDSSDPS-4	0	Fused Operation (FUSE)	9:8	Shall be cleared to 00b.
SDSSDPS-5	0	Opcode (OPC)	7:0	Shall be set to 09h.
SDSSDPS-6	1	Namespace Identifier (NSID)	31:0	See GETF-4 .
SDSSDPS-7	3:2	Reserved	All	Shall be cleared to zero.
SDSSDPS-8	5:4	Metadata Pointer (MPTR)	All	Shall be cleared to zero.
SDSSDPS-9	9:6	Data Pointer (DPTR)	All	Shall be cleared to zero.
SDSSDPS-10	10	Save (SV)	31	This bit specifies that the controller shall persist the DSSD Power State through all power cycles and resets. The device shall support setting this bit to 1b.
SDSSDPS-11	10	Reserved	30:8	Shall be cleared to zero.
SDSSDPS-12	10	Feature Identifier (FID)	7:0	Shall be set to C7h.
SDSSDPS-13	11	Reserved	31:7	Shall be cleared to zero.

Requirement ID	Dword	Field	Bits	Field Description
SDSSDPS-14	11	DSSD Power State	6:0	DSSD Power State to set in watts.
SDSSDPS-15	13:12	Reserved	All	Shall be cleared to zero.
SDSSDPS-16	14	UUID Index	31:0	Shall be set per UUID-3 .
SDSSDPS-17	15	Reserved	31:0	Shall be cleared to zero.

4.15.16 DSSD Power State (Feature Identifier C7h) Get Features

Requirement ID	Description
DSSDPSG-1	If a DSSD Power State (Feature Identifier C7h) Get Features command is executed and the current NVMe Power State was selected because of a DSSD Power State Set Features command, the device shall report the DSSD Power State selected by that command (see Section 4.8.11 DSSD Power State Requirements for an example).
DSSDPSG-2	If a DSSD Power State (Feature Identifier C7h) Get Features command is executed and the current NVMe Power State was not selected because of a DSSD Power State Set Features command, the device shall report the lowest power DSSD Power State whose number is greater than or equal to the Maximum Power in watts of the current NVMe Power State (see Section 4.8.11 DSSD Power State Requirements for an example).

[GETF-4](#) specifies the acceptable values of the NSID field in the Get Features command. Dword 0 of command completion queue entry.

Requirement ID	Field	Bits	Field Description				
GDSSDPS-1	Reserved	31:7	Shall be cleared to zero.				
GDSSDPS-2	DSSD Power State	6:0	The following tables define the required return values for each value of the Select (SEL) field in the Get Features command. All other values are illegal. Current value (Select (SEL) field cleared to 000b):				
			<table><tr><th>Value</th><th>Description</th></tr><tr><td>xx</td><td>The DSSD Power State is currently xx watts as specified by DSSDPSG-1 and DSSDPSG-2.</td></tr></table>	Value	Description	xx	The DSSD Power State is currently xx watts as specified by DSSDPSG-1 and DSSDPSG-2 .
			Value	Description			
			xx	The DSSD Power State is currently xx watts as specified by DSSDPSG-1 and DSSDPSG-2 .			
			Default value (Select (SEL) field set to 001b):				
			<table><tr><th>Value</th><th>Description</th></tr><tr><td>xx</td><td>The DSSD Power State factory default is xx watts.</td></tr></table>	Value	Description	xx	The DSSD Power State factory default is xx watts.
			Value	Description			
			xx	The DSSD Power State factory default is xx watts.			
			Saved value (Select (SEL) field set to 010b):				
			<table><tr><th>Value</th><th>Description</th></tr><tr><td>xx</td><td>The DSSD Power State saved state is xx watts.</td></tr></table>	Value	Description	xx	The DSSD Power State saved state is xx watts.
Value	Description						
xx	The DSSD Power State saved state is xx watts.						
Capabilities (Selection (SEL) field set to 011b): See GETF-5 .							

4.15.17 Telemetry Profile (Feature Identifier C8h) Set Features

4.15.17.1 Telemetry Profiles

Telemetry profiles enable the following to be configured:

- Data Area 1 Last Block
- Data Area 2 Last Block
- Statistic Area Location and Size
- Event FIFO Start and End locations and number of Event FIFOs

In the Telemetry Controller-Initiated log page and Telemetry Host-Initiated log page there is the Number of Telemetry Profiles Supported field. This field enables the device to report the number of Telemetry Profiles supported. There is also a Telemetry Profile Selected field. This reports what profile is currently selected. The Telemetry Profile Selected field can be changed through Set Features. The Telemetry Controller-Initiated log page and Telemetry Host-Initiated log page can then be read to see the format of the Telemetry Profile. Having different profiles enables the device to optimize debug for different situations.

4.15.17.2 Telemetry Profile (Feature Identifier C8h) Set Features

Set Features to set the Telemetry Profile.

Requirement ID	Dword	Field	Bits	Field Description
TEL-CFG-SF-1	0	Command Identifier (CID)	31:16	Shall be set as defined in NVM Express Base Specification.
TEL-CFG-SF-2	0	PRP or SGL for Data Transfer (PSDT)	15:14	Shall be cleared to 00b to specify that PRPs are used.
TEL-CFG-SF-3	0	Reserved	13:10	Shall be cleared to zero.
TEL-CFG-SF-4	0	Fused Operation (FUSE)	9:8	Shall be cleared to 00b.
TEL-CFG-SF-5	0	Opcode (OPC)	7:0	Shall be set to 09h.
TEL-CFG-SF-6	1	Namespace Identifier (NSID)	31:0	See GETF-4 .
TEL-CFG-SF-7	3:2	Reserved	All	Shall be cleared to zero.
TEL-CFG-SF-8	5:4	Metadata Pointer (MPTR)	All	Shall be cleared to zero.
TEL-CFG-SF-9	9:6	Data Pointer (DPTR)	All	Shall be cleared to zero.
TEL-CFG-SF-10	10	Save (SV)	31	This bit specifies that the controller shall save the Telemetry Profile Select (TPS) value (see TEL-CFG-14) so that the selection of a Telemetry Profile persists through

Requirement ID	Dword	Field	Bits	Field Description
				all power states and resets. The device shall support setting this bit to 1b. The host should set this bit to 1b. The device shall ignore the value of this bit and process the Set Features command for this feature as if this bit is set to 1b.
TEL-CFG-SF-11	10	Reserved	30:8	Shall be cleared to zero.
TEL-CFG-SF-12	10	Feature Identifier (FID)	7:0	Shall be set to C8h.
TEL-CFG-SF-13	11	Reserved	31:8	Shall be cleared to zero.
TEL-CFG-SF-14	11	Telemetry Profile Select (TPS)	7:0	The device shall collect debug data per the specified profile number.
TEL-CFG-SF-15	13:12	Reserved	All	Shall be cleared to zero.
TEL-CFG-SF-16	14	UUID Index	31:0	Shall be set per UUID-3 .
TEL-CFG-SF-17	15	Reserved	31:0	Shall be cleared to zero.

4.15.18 Telemetry Profile (Feature Identifier C8h) Get Features

This Get Features returns the telemetry profile that is currently selected on the device, [GETF-4](#) specifies the acceptable values of the NSID field in a Get Features command. Dword 0 of command completion queue entry.

Requirement ID	Field	Bits	Description												
TEL-CFG-GF-1	n/a	n/a	Obsolete. See TEL-CFG-SF-2 and TEL-CFG-SF-3 .												
TEL-CFG-GF-2	Reserved	31:8	Shall be cleared to 0.												
TEL-CFG-GF-3	Telemetry Profile Select (TPS)	7:0	The following tables define the required return values for each value of the Select (SEL) field in the Get Features command. All other values are illegal. Current value (Select (SEL) field cleared to 000b): <table><tr><th>Value</th><th>Description</th></tr><tr><td>xx</td><td>The current Telemetry Profile is xx.</td></tr></table> Default value (Select (SEL) field set to 001b): <table><tr><th>Value</th><th>Description</th></tr><tr><td>xx</td><td>The default Telemetry Profile is xx.</td></tr></table> Saved field (Select (SEL) field set to 010b): <table><tr><th>Value</th><th>Description</th></tr><tr><td>xx</td><td>The saved Telemetry Profile is xx.</td></tr></table>	Value	Description	xx	The current Telemetry Profile is xx.	Value	Description	xx	The default Telemetry Profile is xx.	Value	Description	xx	The saved Telemetry Profile is xx.
Value	Description														
xx	The current Telemetry Profile is xx.														
Value	Description														
xx	The default Telemetry Profile is xx.														
Value	Description														
xx	The saved Telemetry Profile is xx.														

Requirement ID	Field	Bits	Description
			Capabilities (Select (SEL) field set to 011b): See GETF-5 .

4.15.19 DSSD Asynchronous Event Configuration (Feature Identifier C9h) Set Features

This Feature controls the DSSD events that cause an asynchronous event notification to be sent to the host. If the condition for an event is true when the corresponding notice indicated in Command Dword 11 is enabled and there's an outstanding Asynchronous Event Request command, then that event is sent to the host. If the notice indicated in Command Dword 11 is disabled, then that event is not sent to the host.

Requirement ID	Dword	Field	Bits	Field Description
SDAEC-1	0	Command Identifier (CID)	31:16	Shall be set as defined in NVM Express Base Specification.
SDAEC-2	0	PRP or SGL for Data Transfer (PSDT)	15:14	Shall be cleared to 00b to specify that PRPs are used.
SDAEC-3	0	Reserved	13:10	Shall be cleared to zero.
SDAEC-4	0	Fused Operation (FUSE)	9:8	Shall be cleared to 00b.
SDAEC-5	0	Opcode (OPC)	7:0	Shall be set to 09h.
SDAEC-6	1	Namespace Identifier (NSID)	31:0	See GETF-4 .
SDAEC-7	3:2	Reserved	All	Shall be cleared to zero.
SDAEC-8	5:4	Metadata Pointer (MPTR)	All	Shall be cleared to zero.
SDAEC-9	9:6	Data Pointer (DPTR)	All	Shall be cleared to zero.
SDAEC-10	10	Save (SV)	31	The device shall not support setting this bit to 1b. If the controller receives this Set Features command with the bit set to 1b, then the device shall abort the command with a status of Feature Identifier Not Saveable.
SDAEC-11	10	Reserved	30:8	Shall be cleared to zero.
SDAEC-12	10	Feature Identifier (FID)	7:0	Shall be set to C9h.
SDAEC-13	11	Reserved	31:2	Shall be cleared to zero.
SDAEC-14	11	Enable Error Reporting AENs	0	This bit specifies whether an asynchronous event notification is sent to the host for an error event (see EREC-5).

Requirement ID	Dword	Field	Bits	Field Description
				If this bit is set to 1b, then: - the Error Reporting AEN is sent to the host as a consequence of an error event unless the device is unable to send that AEN because: - the device is unable to generate command completions; or - there is no outstanding Asynchronous Event command, and the device is unable to process commands submitted to the Admin Queue; and - the Controller Fatal Status bit in the in-band Controller Status property shall not be set to 1b when an error occurs; however, the Controller Fatal Status bit in the out-of-band Controller Health Data Structure shall still be set to 1b. Error Reporting AENs are processed as Notice (asynchronous) events (see DSSD-AEN-1). If this bit is cleared to 0b, or the controller is unable to complete an Error Reporting AEN, then: - the Error Reporting AEN shall not be sent to the host; and - the Controller Fatal Status bit in the in-band Controller Status property and in the in-band and out-of-band Controller Health Data Structure shall be set to 1b when an error event occurs.
SDAEC-18	11	Enable Media Ready AENs	1	This bit specifies whether an Asynchronous Event Notification is sent to the host for a DSSD Media Ready Event. The DSSD Media Ready Event occurs during device initialization when the device is ready to successfully respond to Admin commands that access media and IO commands. This event shall occur within the timespan defined by TTR-2. If this bit is set to 1b, then the Media Ready AEN is sent to the host. That Media Ready AEN is processed as a One-Shot (asynchronous) event (see DSSD-AEN-2). If this bit is cleared to 0b, then the Media Ready AEN is not sent to the host.
SDAEC-15	13:12	Reserved	All	Shall be cleared to zero.
SDAEC-16	14	UUID Index	31:0	Shall be set per UUID-3 .

Requirement ID	Dword	Field	Bits	Field Description
SDAEC-17	15	Reserved	31:0	Shall be cleared to zero.

4.15.20 DSSD Asynchronous Event Configuration (Feature Identifier C9h) Get Features

[GETF-4](#) specifies the acceptable values of the NSID field in the Get Features command. Dword 0 of command completion queue entry.

Requirement ID	Field	Bits	Field description										
GDAEC-1	Reserved	31:2	Shall be cleared to zero.										
GDAEC-2	Error Reporting AEN Enabled	0	The following tables define the required return values for each value of the Select (SEL) field in the Get Features command. All other values are illegal. Current value (Select (SEL) field cleared to 000b): <table><tr><th>Value</th><th>Description</th></tr><tr><td>0b</td><td>An Error Reporting AEN is not sent to the host for an error event (see SDAEC-14 and EREC-5).</td></tr><tr><td>1b</td><td>An Error Reporting AEN is sent to the host for an error event.</td></tr></table> Default value (Select (SEL) field set to 001b): <table><tr><th>Value</th><th>Description</th></tr><tr><td>1b</td><td>The default behavior following a Controller Level Reset is that an Error Reporting AEN is sent to the host for an error event.</td></tr></table> Saved field (Select (SEL) field set to 010b): This feature is not saveable (see SDAEC-10), so the default value (0b) is returned. Capabilities (Select (SEL) field set to 011b): See GETF-5.	Value	Description	0b	An Error Reporting AEN is not sent to the host for an error event (see SDAEC-14 and EREC-5).	1b	An Error Reporting AEN is sent to the host for an error event.	Value	Description	1b	The default behavior following a Controller Level Reset is that an Error Reporting AEN is sent to the host for an error event.
Value	Description												
0b	An Error Reporting AEN is not sent to the host for an error event (see SDAEC-14 and EREC-5).												
1b	An Error Reporting AEN is sent to the host for an error event.												
Value	Description												
1b	The default behavior following a Controller Level Reset is that an Error Reporting AEN is sent to the host for an error event.												
GDAEC-3	Media Ready AEN Enabled	1	The following tables define the required return values for each value of the Select (SEL) field in the Get Features command. All other values are illegal. Current value (Select (SEL) field cleared to 000b): <table><tr><th>Value</th><th>Description</th></tr><tr><td>0b</td><td>A Media Ready AEN is not sent to the host when a Media Ready event occurs (see SDAEC-18 and DSSD-AEN-2).</td></tr><tr><td>1b</td><td>A Media Ready AEN is sent to the host when a Media Ready event occurs.</td></tr></table> Default value (Select (SEL) field set to 001b):	Value	Description	0b	A Media Ready AEN is not sent to the host when a Media Ready event occurs (see SDAEC-18 and DSSD-AEN-2).	1b	A Media Ready AEN is sent to the host when a Media Ready event occurs.				
Value	Description												
0b	A Media Ready AEN is not sent to the host when a Media Ready event occurs (see SDAEC-18 and DSSD-AEN-2).												
1b	A Media Ready AEN is sent to the host when a Media Ready event occurs.												

Requirement ID	Field	Bits	Field description	
			Value	Description
			0b	The default behavior following a Controller Level Reset is that an Error Reporting AEN is not sent to the host for an error event.
			Saved field (Select (SEL) field set to 010b): This feature is not saveable (see SDAEC-10), so the default value (0b) is returned.	
			Capabilities (Select (SEL) field set to 011b): See GETF-5 .	
			Value	Description
			0b	A Media Ready AEN is not sent to the host when a Media Ready Event occurs.
			1b	A Media Ready AEN is sent to the host when a Media Ready Event occurs.

4.15.21 Idle Wake Up Time Configuration (Feature Identifier CAh) Set Features

This Set Features defines the amount of time the device has to wake up to complete a 4 KiB read command from being in a low power idle mode which is transparent to the host assuming the device is in the L0 state. If the Phy is not in the L0 state, the time to transition to L0 is not included in the wake-up time. This functionality is independent of the 5 W idle requirement (see [PWR-6](#)).

Requirement ID	Dword	Field	Bits	Field Description
SIDLE-1	0	Command Identifier (CID)	31:16	Shall be set as defined in NVM Express Base Specification.
SIDLE-2	0	PRP or SGL for Data Transfer (PSDT)	15:14	Shall be cleared to 00b to specify that PRPs are used.
SIDLE-3	0	Reserved	13:10	Shall be cleared to zero.
SIDLE-4	0	Fused Operation (FUSE)	9:8	Shall be cleared to 00b.
SIDLE-5	0	Opcode (OPC)	7:0	Shall be set to 09h.
SIDLE-6	1	Namespace Identifier (NSID)	31:0	See GETF-4 .
SIDLE-7	3:2	Reserved	All	Shall be cleared to zero.
SIDLE-8	5:4	Metadata Pointer (MPTR)	All	Shall be cleared to zero.
SIDLE-9	9:6	Data Pointer (DPTR)	All	Shall be cleared to zero.

Requirement ID	Dword	Field	Bits	Field Description
SIDLE-10	10	Save (SV)	31	This bit specifies that the controller shall save the Idle Wake Up Time so that the time interval persists through all power states and resets. The device shall support setting this bit to 1b.
SIDLE-11	10	Reserved	30:8	Shall be cleared to zero.
SIDLE-12	10	Feature Identifier (FID)	7:0	Shall be set to CAh.
SIDLE-13	11	Reserved	31:16	Shall be cleared to zero.
SIDLE-14	11	Idle Wake Up Time	15:0	This field specifies the maximum amount of time in milliseconds that the device is allowed to complete a 4 KiB read command starting from being in a low power idle mode. With the exception of I/O timeouts, this is transparent to the host assuming the device phy is in the L0 state and the device is in an operational NVMe power state. If the device phy is not in the L0 state, the time to transition to L0 is not included in the wake-up time. If this value is cleared to 0000h, then this feature is disabled. If this Idle Wake Up Time field contains a value less than the minimum value the device supports, the device shall set the IdleWake Up Time to the minimum value the device supports. The minimum value the device supports can be found using Get Features to retrieve the factory default value.
SIDLE-15	13:12	Reserved	All	Shall be cleared to zero.
SIDLE-16	14	UUID Index	31:0	Shall be set per UUID-3 .
SIDLE-17	15	Reserved	31:0	Shall be cleared to zero.

4.15.22 Idle Wake Up Time Configuration (Feature Identifier CAh) Get Features

[GETF-4](#) specifies the acceptable values of the NSID field in the Get Features command. Dword 0 of command completion queue entry is specified in the following table.

Requirement ID	Field	Bits	Field Description	
GIDLE-1	Reserved	31:16	Shall be cleared to zero.	
GIDLE-2	Idle Wake Up Time	15:0	The following tables define the required return values for each value of the Select (SEL) field in the Get Features command. All other values are illegal.	
			Current value (Select (SEL) field cleared to 000b):	
			Value	Description
			0000h	The Idle Wake Up Time is currently disabled.

Requirement ID	Field	Bits	Field Description	
			xxxxh	The Idle Wake Up Time is currently xxxxh milliseconds.
			Default value (Select (SEL) field set to 001b):	
			Value	Description
			0000h	The Idle Wake Up Time factory default is disabled.
			xxxxh	The Idle Wake Up Time factory default is xxxxh.
			The factory default value shall be set to the minimum value supported by the device.	
			Saved value (Select (SEL) field set to 010b):	
			Value	Description
			0000h	The Idle Wake Up Time saved state is disabled.
			xxxxh	The Idle Wake Up Time saved state is xxxxh milliseconds.
			Capabilities (Select (SEL) field set to 011b): See GETF-5 .	

4.15.23 Max PCIe Interface Configuration (Feature Identifier CBh)

This Set Features enables limiting the max number of PCIe lanes and/or the max speed of these lanes to something less than the max the device supports.

Requirement ID	Dword	Field	Bits	Field Description
MPCS-1	0	Command Identifier (CID)	31:16	Shall be set as defined in NVM Express Base Specification.
MPCS-2	0	PRP or SGL for Data Transfer (PSDT)	15:14	Shall be cleared to 00b to specify that PRPs are used.
MPCS-3	0	Reserved	13:10	Shall be cleared to zero.
MPCS-4	0	Fused Operation (FUSE)	9:8	Shall be cleared to 00b.
MPCS-5	0	Opcode (OPC)	7:0	Shall be set to 09h.
MPCS-6	1	Namespace Identifier (NSID)	31:0	See GETF-4 .
MPCS-7	3:2	Reserved	All	Shall be cleared to zero.
MPCS-8	5:4	Metadata Pointer (MPTR)	All	Shall be cleared to zero.

Requirement ID	Dword	Field	Bits	Field Description										
MPCS-9	9:6	Data Pointer (DPTR)	All	Shall be cleared to zero.										
MPCS-10	10	Save (SV)	31	This bit specifies that the controller shall save the Max PCIe Interface Configuration such that this persists through all power states and resets. The device shall support setting this bit to 1b. The host should set this bit to 1b. The device shall ignore the value of this bit and process the Set Features command for this feature as if this bit is set to 1b.										
MPCS-11	10	Reserved	30:8	Shall be cleared to zero.										
MPCS-12	10	Feature Identifier (FID)	7:0	Shall be set to CBh.										
MPCS-13	11	Reserved	31:16	Shall be cleared to zero.										
MPCS-14	11	Max PCIe Interface Configuration	15:0	This field specifies the PCIe lane configuration. <table><tr><th>Bit</th><th>Description</th></tr><tr><td>15:9</td><td>Reserved.</td></tr><tr><td>8</td><td>Factory Default Revert: When set to 1b the device shall revert to the factory default and all other fields in the Max PCIe Interface Configuration field shall be ignored. When cleared to 0b this field shall have no effect.</td></tr><tr><td>7:4</td><td>Max Number of PCIe Lanes: F-4h: Reserved 3h: x8 2h: x4 1h: x2 0h: x1</td></tr><tr><td>3:0</td><td>Max PCI Interface Speed: F-5h: Reserved 4h: PCIe Gen 7 3h: PCIe Gen 6 2h: PCIe Gen 5 1h: PCIe Gen 4 0h: PCIe Gen 3</td></tr></table> This field shall only take effect after the next power cycle of the device after this set features. For unsupported combinations of Max Number of PCIe Lanes and/or Max PCIe Interface Speed the device shall select the next	Bit	Description	15:9	Reserved.	8	Factory Default Revert: When set to 1b the device shall revert to the factory default and all other fields in the Max PCIe Interface Configuration field shall be ignored. When cleared to 0b this field shall have no effect.	7:4	Max Number of PCIe Lanes: F-4h: Reserved 3h: x8 2h: x4 1h: x2 0h: x1	3:0	Max PCI Interface Speed: F-5h: Reserved 4h: PCIe Gen 7 3h: PCIe Gen 6 2h: PCIe Gen 5 1h: PCIe Gen 4 0h: PCIe Gen 3
Bit	Description													
15:9	Reserved.													
8	Factory Default Revert: When set to 1b the device shall revert to the factory default and all other fields in the Max PCIe Interface Configuration field shall be ignored. When cleared to 0b this field shall have no effect.													
7:4	Max Number of PCIe Lanes: F-4h: Reserved 3h: x8 2h: x4 1h: x2 0h: x1													
3:0	Max PCI Interface Speed: F-5h: Reserved 4h: PCIe Gen 7 3h: PCIe Gen 6 2h: PCIe Gen 5 1h: PCIe Gen 4 0h: PCIe Gen 3													

Requirement ID	Dword	Field	Bits	Field Description
				lowest value of Max Number of PCIe Lanes and/or Max PCIe Interface Speed which is supported. Limits imposed by this feature shall affect all PCIe registers that report PCIe link capabilities, including the Link Capabilities 2 register (e.g., if the Max PCIe interface speed is set to Gen 4 on a Gen 5 device, then the device shall behave as a Gen 4 device).
MPCS-15	13:12	Reserved	All	Shall be cleared to zero.
MPCS-16	14	UUID Index	31:0	Shall be set per UUID-3 .
MPCS-17	15	Reserved	31:0	Shall be cleared to zero.

4.15.24 Max PCIe Interface Configuration (Feature Identifier CBh) Get Features

[GETF-4](#) specifies the acceptable values of the NSID field in the Get Features command. Dword 0 of command completion queue entry is specified in the following table.

Requirement ID	Field	Bits	Field Description												
MPCSG-1	Reserved	31:16	Shall be cleared to zero.												
MPCSG-2	Max PCIe Interface Configuration	15:0	The following tables define the required return values for each value of the Select (SEL) field in the Get Features command. All other values are illegal. Current value (Select (SEL) field cleared to 000b): <table><tr><th>Value</th><th>Description</th></tr><tr><td>xxxxh</td><td>This is the Max PCIe Interface Configuration Value which the device is currently operating with.</td></tr></table> Default value (Select (SEL) field set to 001b): <table><tr><th>Value</th><th>Description</th></tr><tr><td>xxxxh</td><td>This is the Max PCIe Interface Configuration Value which is the factory default</td></tr></table> Saved value (Select (SEL) field set to 010b): <table><tr><th>Value</th><th>Description</th></tr><tr><td>xxxxh</td><td>This is the Max PCIe Interface Configuration Value which is saved and will be used for the next power cycle.</td></tr></table> Capabilities (Select (SEL) field set to 011b): See GETF-5.	Value	Description	xxxxh	This is the Max PCIe Interface Configuration Value which the device is currently operating with.	Value	Description	xxxxh	This is the Max PCIe Interface Configuration Value which is the factory default	Value	Description	xxxxh	This is the Max PCIe Interface Configuration Value which is saved and will be used for the next power cycle.
Value	Description														
xxxxh	This is the Max PCIe Interface Configuration Value which the device is currently operating with.														
Value	Description														
xxxxh	This is the Max PCIe Interface Configuration Value which is the factory default														
Value	Description														
xxxxh	This is the Max PCIe Interface Configuration Value which is saved and will be used for the next power cycle.														

5 PCIe Requirements

The following are PCIe requirements:

Requirement ID	Description
PCI-1	The device shall support a PCIe Maximum Payload Size (MPS) of 512 bytes or larger. When the device transmits data, the device shall use the largest MPS possible. Changes to the MPS shall take effect immediately without requiring a Controller Reset or any other type of reset.
PCI-2	The device shall support modification of PCIe TLP completion timeout range as defined by the PCI Express Base Specification.
PCI-3	The vendor shall disclose the vendor-specific timeout range definition in the “Completion Timeout Ranges Supported” field in the PCI Express Base Specification.
PCI-4	The device shall support disabling PCIe Completion Timeout.
PCI-5	The device shall perform a PCIe Fundamental Reset when PERST# is asserted, and main power has not been removed even if firmware is hung. The device firmware shall initialize when PERST# is de-asserted, regardless of whether the device firmware was hung when PERST# was asserted.
PCI-6	PCIe Function Level Reset shall be supported.
PCI-7	Obsolete. See PCI-5.
PCI-8	The device shall not expose a BAR4 or a BAR5 if neither CMB nor PMR is supported.
PCI-9	The device shall support MSI-X.
PCI-10	The MSI-X table shall reside in BAR0.
PCI-11	If implemented, the MSI capability structure in configuration space shall be 4-byte aligned.
PCI-12	Any optional PCI features supported by the device not described in this document shall be clearly documented and disclosed to the customer.
PCI-13	The device shall support Completion Timeout Ranges A, B and C.
PCI-14	The device shall support Relaxed Ordering.
PCI-15	The device shall not set the Relaxed Ordering bit in transactions it initiates as a Requester that require strong ordering (i.e., transactions that would violate the NVMe protocol or result in data corruption if re-ordered shall clear the Relaxed Ordering bit to 0b). For example, the Enable Relaxed Ordering bit in transactions initiated by the device as a Requester shall be cleared to 0b in MSI/MSI-X writes, writes to the Completion Queue Entry, etc.
PCI-16	The device shall set the Relaxed Ordering bit in data DMAs, if Relaxed Ordering is enabled.
PCI-17	The device shall support all link speeds between the lowest link speed and the highest link speed, inclusive (e.g., a device compliant with the PCI Express Base Specification Revision 6.2 shall support link speeds of 2.5 GT/s, 5.0 GT/s, 8 GT/s, 16 GT/s, 32 GT/s, and 64 GT/s).

Requirement ID	Description
PCI-18	The device shall not require Device Specific Initialization (DSI).
PCI-19	The device shall not perform a soft reset when transitioning from D3hot to D0 (i.e., No_Soft_Reset bit in the Power Management Control/Status Register shall be set to 1b).
PCI-20	The device shall not support BARs that map to I/O Space.
PCI-21	All BARs that map to Memory Space shall be 64-bit capable (i.e., bits 2:1 of the BAR shall be set to 10b) and shall support the full 64-bit address space.
PCI-22	The sum of the size of all BARs for a single non-SR-IOV function or SR-IOV Physical Function that maps to Memory Space shall be less than or equal to 1 MiB if neither CMB nor PMR is supported.
PCI-23	The device shall require a maximum of one PCI bus number (e.g., no PCIe switches are allowed).
PCI-24	The device's DMA engines shall support the full 64-bit address space with uniform performance across the entire address range.
PCI-25	The Device Serial Number Extended Capability shall be supported except for virtual functions. All functions on all ports of a device that implement this capability shall return the same serial number value. The serial number shall be unique for each device and independent from all other unique identifiers on the device (e.g., for namespaces, controllers, etc.).
PCI-26	The device shall support the Advanced Error Reporting Extended Capability.
PCI-27	The device shall silently discard (following normal data link layer processing) without logging or signaling an error, any PCIe VDMs targeting a Function while it is in Function Level Reset (FLR). When an FLR is initiated for a Function, any already-received PCIe VDMs still being processed by that Function shall be silently discarded. This requirement prohibits non-silent-discard behavior during an FLR that is allowed by the PCI Express Base Specification.
PCI-28	The device shall support Address Translation Services (ATS).
PCI-29	While any one or more Functions on the device are in the D3hot power state, MCTP over PCIe VDM processing shall be fully operational and the device shall not generate errors for valid MCTP over PCIe VDMs received while in this state. For example, while in this state, the device shall be able to successfully process MCTP over PCIe VDM requests, transmit the response, and shall be able to transmit MCTP messages for any asynchronous events that occur and are enabled. This requirement applies to all supported MCTP message types (e.g., NVMe-MI, SPD, etc.).
PCI-30	PCIe non-Fundamental Resets (e.g., Function Level Reset, hot reset, or reset due to a link down/link disabled condition) shall not clear the device's captured PCIe bus number(s) or MCTP Endpoint ID(s). This is required so that devices can continue to communicate via MCTP over PCIe VDM following these types of resets without having to be re-initialized.

Requirement ID	Description
	PCIe Fundamental Resets shall clear the captured PCIe bus number(s) as required by the PCI Express Base Specification and shall clear the MCTP Endpoint ID(s) as required by the MCTP PCIe Transport Binding Specification.
PCI-31	If an MCTP over PCIe VDM would otherwise signal Unsupported Request (e.g., ID Routed Message targeting a Function that is not implemented) is received, then the device shall silently discard that message.
PCI-32	In addition to responding to Broadcast from Root Complex as required by the MCTP PCIe VDM Binding Specification, a PCIe VDM Management Endpoint shall respond to Route by ID Message Requests for the following MCTP control messages: • Prepare for Endpoint Discovery; and • Endpoint Discovery.
PCI-33	PERST# shall not be treated as a power cycle. For example, PERST#: • shall not cause TCG Opal devices to go to the Read Locked/Write Locked state (i.e., PERST# maps to the TCG reset type of Hardware Reset, not a Power Cycle, as defined by the TCG Storage Interface Interactions Specification) if the host has not configured a TCG HW Reset as one of the Reset Types that can lock the device's locking ranges on LockOnReset in addition to Power Cycle; and • shall not cause commands prohibited via the NVMe Lockdown command to be unprohibited.
PCI-34	PERST# shall not cause RW1CS bits defined by the PCI Express Base Specification (e.g., bits in the Uncorrectable Error Status and Correctable Error Status registers) to be cleared.
PCI-35	The device shall not support either the D1 or the D2 power management states.
PCI-36	If any power-of-two-sized access, up to 8-bytes in size, to the memory pointed to by any of the NVMe device's BARs (e.g., access to controller registers) is aligned to a power-of-two boundary equal to the size of the access (e.g., a 2-byte access aligned to a 2-byte boundary, a 4-byte access aligned to a 4-byte boundary, etc.), then the access shall not be considered a restricted programming model violation (i.e., the access shall be processed successfully unless some other error unrelated to a restricted programming model violation is encountered). Support is optional for any accesses greater than 8-bytes in size to the memory pointed to by NVMe BAR0/BAR1 (e.g., access to controller registers). The restricted programming model for the memory pointed to by BARs other than BAR0/BAR1 may support additional access sizes as required by the device vendor. For any access that results in a restricted programming model violation, the request shall be handled as an Unsupported Request or Completer Abort as permitted for restricted programming model violations as defined by the PCI Express Base Specification (e.g., the device firmware shall not hang due to a restricted programming model violation).
PCI-37	If the device receives an MCTP over PCIe VDM that is invalid due to an MCTP base layer error or MCTP message-type layer (e.g., NVMe-MI, SPD) error, then the error shall be reported, if possible, at the MCTP base layer or MCTP message-type layer respectively; otherwise, the invalid MCTP over PCIe VDM shall be silently discarded.

Requirement ID	Description
	This requirement applies to all supported MCTP message types (e.g., NVMe-MI, SPD, etc.).
PCI-38	A Function Level Reset to a Function other than the Function associated with the MCTP endpoint shall have no impact on MCTP traffic on the Function associated with the MCTP endpoint.
PCI-39	The device shall perform a PCIe Conventional Reset per the PCI Express Base Specification (e.g., resetting PCIe-defined state machines, setting PCIe-defined registers to default, etc.) when main power has not been removed and any of the following conditions occur, even if the firmware is not functioning (e.g., has asserted or is otherwise non-responsive): - the PCIe link is disabled; or - the device is reset by a PCIe hot reset.
PCI-40	The device shall comply with PCI-SIG requirements for supported TLP sizes, including support for TLP writes to PRP memory addresses with 64-byte alignment and 64-byte granularity.
PCI-41	MCTP over PCIe VDM shall be supported by PCIe Function 0 on each port and shall not be supported by any other PCIe Function.
PCI-42	For PCIe Gen6 devices, L0p shall be supported.

5.1 Boot Requirements

Requirement ID	Description
BOOT-1	The device shall support the UEFI 2.0 and all later versions of the Tianocore EDKII NVMe driver.
BOOT-2	The device shall neither support nor include an option ROM.

5.2 PCIe Error Logging

The following table indicates where the PCIe physical layer error counters shall be logged. This is in addition to the aggregated PCIe error counters defined in SMART / Health Information Extended log page (Log Identifier C0h).

Requirement ID	Event	Logging Mechanism
PCIERR-1	Unsupported Request Error Status (URES)	Uncorrectable Error Status Register (Offset 04h) in PCI Express Base Specification. The host is able to read and clear the contents of this register as appropriate.
PCIERR-2	ECRC Error Status (ECRCES)	
PCIERR-3	Malformed TLP Status (MTS)	
PCIERR-4	Receiver Overflow Status (ROS)	
PCIERR-5	Unexpected Completion Status (UCS)	
PCIERR-6	Completer Abort Status (CAS)	
PCIERR-7	Completion Timeout Status (CTS)	
PCIERR-8	Flow Control Protocol Error Status (FCPES)	

Requirement ID	Event	Logging Mechanism
PCIERR-9	Poisoned TLP Status (PTS)	
PCIERR-10	Data Link Protocol Error Status (DLPES)	
PCIERR-11	Advisory Non-Fatal Error Status (ANFES)	Correctable Error Status Register (Offset 10h) in PCI Express Base Specification.
PCIERR-12	Replay Timer Timeout Status (RTS)	The total number of these errors shall be reported in the PCIe Correctable Error Count in the SMART / Health Information Extended log page (Log Identifier C0h) (see SMART-14).
PCIERR-13	REPLAY_NUM Rollover Status (RRS)	
PCIERR-14	Bad DLLP Status (BDS)	
PCIERR-15	Bad TLP Status (BTS)	
PCIERR-16	Receiver Error Status (RES)	

5.3 Low Power Modes

Requirement ID	Description
LPWR-1	ASPM shall be disabled after a power cycle or PCIe resets as defined by the PCI Express Base Specification.
LPWR-2	The device shall support the PCIe ASPM L1 power state.

5.4 PCIe Eye Capture

Requirement ID	Description
EYE-1	A utility shall be provided that takes the entire Physical Interface Receiver Eye Opening Measurement log page as an input and decodes the Eye Data field of each lane in the log page.

6 Optional Device Features

Features in this section are optional. If the feature is implemented, it shall follow the requirements in this section.

6.1 Flexible Data Placement Requirements

If Flexible Data Placement is supported, then the Generic Flexible Data Placement Requirements and a minimum of one of the Flexible Data Placement configurations shall be supported:

6.1.1 Generic Flexible Data Placement Requirements

Requirement ID	Description
FDPG-1	Obsolete (see NVMe-OPT-16).

Requirement ID	Description
FDPG-2	It shall be clearly disclosed to the customer which FDP Event Types are supported and what additional fields related to this are supported with each event type (FDP Event Flags, PID, NSID, Reclaim Group Identifier, Reclaim Unit Handle Identifier, etc.)

6.1.2 FDP Single Reclaim Group Configuration 1

Requirement ID	Description
FDPSRG-1	The number of advertised reclaim groups (NRG) shall be 1.
FDPSRG-2	The device shall support a minimum of 8 reclaim unit handles.
FDPSRG-3	The device shall set Volatile Write Cache Present to 0b (not supported).
FDPSRG-4	The device shall support an FDP configuration with a minimum of 8 reclaim unit handles of Reclaim Unit Handle Type Initially Isolated.
FDPSRG-5	Obsolete. Moved to FDPSRG2-2.
FDPSRG-6	Single reclaim group configurations shall support a minimum of 8 namespaces.
FDPSRG-7	Single reclaim group configurations shall support SECTOR-4 and DIX-1 in an FDP configuration.

6.1.3 FDP Single Reclaim Group Configuration 2

Requirement ID	Description
FDPSRG2-1	The device shall support all the requirements in FDP Single Reclaim Group Configuration 1 section 6.1.2 except FDPSRG-4.
FDPSRG2-2	The device shall support an FDP configuration with a minimum of 8 reclaim unit handles of Reclaim Unit Handle Type Persistently Isolated.

6.1.4 FDP Die Placement Configuration

Requirement ID	Description
FDPDP-1	The number of advertised reclaim groups (NRG) shall match the number of flash dies in the NVM subsystem.
FDPDP-2	The configuration shall support a minimum of 8 reclaim unit handles. In other words, it shall be possible to utilize (NRG) x 8 placement identifiers simultaneously.

6.2 DIX Requirements

If DIX is supported, then the following shall be supported:

Requirement ID	Description
DIX-1	The following DIX configuration shall be supported.

Requirement ID	Description	
	Field	Value
	PIL (Protection Information Location)	0b
	PI (Protection Information)	011b (Type 3)
	MSET (Metadata Settings)	0b (DIX)
	LBAF (LBA Format)	4K+64 ¹
	LBAFEE (LBA Format Extension Enable)	0b
	PRACT (Protection Information Action)	0b and 1b
	PRCHK (Protection Information Check): Guard Check (bit 2)	1b
	PRCHK (Protection Information Check): Application Tag Check (bit 1)	0b
	PRCHK (Protection Information Check): Reference Tag check (bit 0)	0b
	STC (Storage Tag Check)	0b ²
	Note(s): 1. 4 KiB logical blocks, each of which has an additional 64 bytes of metadata. 2. The Storage Tag does not exist because LBAFEE is cleared to 0b.	

6.3 DIF Requirements

If DIF is supported, then the following shall be supported:

Requirement ID	Description	
DIF-1	The following DIF configuration shall be supported.	
	Field	Value
	PIL (Protection Information Location)	0b
	PI (Protection Information)	010b (Type 2)
	MSET (Metadata Settings)	1b
	LBAF (LBA Format)	512+8 ¹
	LBAFEE (LBA Format Extension Enable)	0b
	PRACT (Protection Information Action)	0b and 1b
	PRCHK (Protection Information Check): Guard Check (bit 2)	0b and 1b
	PRCHK (Protection Information Check): Application Tag Check (bit 1)	0b and 1b
	PRCHK (Protection Information Check): Reference Tag check (bit 0)	0b and 1b
	STC (Storage Tag Check)	0b ²
	Note(s): 1. 512-byte logical blocks, each of which has an additional 8 bytes of metadata	

Requirement ID	Description
	2. The Storage Tag does not exist because LBAFEE is cleared to 0b.

7 Reliability

7.1 Uncorrectable Bit Error Rate

Requirement ID	Description
UBER-1	The device shall support an Uncorrectable Bit Error Rate (UBER) of < 1 sector per 10^{18} bits read. Physical device testing is only required to demonstrate an Uncorrectable Bit Error Rate (UBER) of < 1 sector per 10^{17} bits read (as per JESD218B method).

7.2 Power On/Off Requirements

7.2.1 Time to Ready and Shutdown Requirements

Requirement ID	Description
TTR-1	The device shall be able to process the Identify command with a successful completion within 1 second of CC.EN being set to 1b provided a Shutdown is not in progress when CC.EN is set to 1b. Some models may allow a longer time (see Section 13 Device Profiles).
TTR-2	The device shall be able to process I/O and Admin commands that require access to media with a successful completion within 20 seconds after CC.EN has been set to 1b. Some models require a different time (see Section 13 Device Profiles). See TTR-22 for additional requirements for time to ready after PCIe Conventional Reset.
TTR-3	The device shall be able to process Admin commands with a successful completion as soon as CSTS.RDY = 1. Slower processing of Admin commands that require media access is acceptable while the media is becoming ready.
TTR-4	The device shall keep CSTS.RDY = 0 until the device is able to process Admin commands. Some models may have additional requirements before CSTS.RDY can be set to 1 (see Section 13 Device Profiles).
TTR-5	The Shutdown Notification completion (i.e., the CSTS.SHST set to 10b) shall be received within 10 seconds after the start of a normal shutdown (i.e., after CC.SHN is set to 01b).
TTR-6	The device shall support both the CC.SHN Normal and Abrupt Shutdown Notifications.
TTR-7	After a normal shutdown is completed successfully, the device shall not enter a rebuild/recovery mode on the next power on.
TTR-8	A normal shutdown shall trigger flushing to non-volatile memory of any content within the device's internal cache(s) (e.g., SRAM/DRAM), if present, which is required to be non-volatile.
TTR-9	Obsolete. See NVMe-CFG-3 .
TTR-10	Obsolete. Moved to PLP-1 .

Requirement ID	Description
TTR-11	Obsolete. Moved to PLP-2 .
TTR-12	Metadata rebuild due to any reason (e.g., unexpected power loss) shall not exceed 120 seconds and the device shall meet its latency requirements after this.
TTR-13	Obsolete. Moved to PLP-3 .
TTR-14	Obsolete. Moved to PLP-4 .
TTR-15	In case of a successful Normal shutdown operation (CC.SHN = 1 set by the NVMe device driver), no data loss is tolerated even if PLP has failed.
TTR-16	Any shutdown event shall not make the device non-functional under any conditions.
TTR-17	Obsolete. Moved to PLP-5 .
TTR-18	Obsolete. Moved to PLP-6 .
TTR-19	When the CC.SHN register is written to notify the device to shut down it shall not be assumed that power will be lost even after CC.EN is cleared to 0. Under these conditions the device shall continue to function properly based on the NVMe and PCIe Specifications.
TTR-20	The device shall be able to successfully respond to Configuration space accesses within 1s from de-assertion of PERST#.
TTR-21	Obsolete, see GDAEC-2 and GDAEC-3 .
TTR-22	Upon completion of a PCIe Conventional Reset, the device shall start initializing the media and within 20 seconds from the completion of the PCIe Conventional Reset shall be able to successfully process: in-band I/O and Admin commands requiring media access, assuming CC.EN has been set to 1b; and out-of-band Admin commands requiring media access, including prior to the in-band host enabling the controller. Some models require a different time (see Section 13 Device Profiles) If a PCIe Conventional Reset occurs while a device is shutdown (i.e., the CSTS.SHST field is set to 10b), then this requirement may cause the device to transition to a state where a power loss would be unexpected. This requirement overrides the requirement in the NVM Express Base specification for the controller to be ready to be powered off until CC.EN transitions from 0b to 1b following a controller shutdown.
TTR-23	The device shall not support NVM Subsystem Shutdown.

7.2.2 Incomplete/Unsuccessful Shutdown

An incomplete/unsuccessful shutdown is a Normal or Abrupt power down that did not complete 100% of the shutdown sequence for any reason that causes the device to be unable to guarantee data/metadata integrity (e.g., firmware hang/crash, capacitor failure, PLP circuit failure, etc.).

Requirement ID	Description
INCS-1	When the power-loss protection mechanism fails for any reason while power is applied, the device shall:

Requirement ID	Description
	- set Critical Warning bit 4 to 1b in the SMART / Health Information log page (Log Identifier 02h); - send an NVM subsystem Reliability SMART / Health Status AEN, if that AEN is enabled; and - transition to the write behavior as defined in the PLP Failure Mode (see Section 4.15.5 PLP Failure Mode (Feature Identifier C2h Set Features)).
INCS-2	The device shall incorporate a shutdown checksum or flag as the very last piece of data written to flash to detect incomplete shutdown.
INCS-3	The checksum or flag in INCS-2 shall be used on power-up to confirm that the previous shutdown was 100% successful.
INCS-4	An incomplete/unsuccessful shutdown that causes the device to be unable to guarantee data/metadata integrity shall result in an increase in the Incomplete Shutdowns field (SMART-15) in the SMART / Health Information Extended log page (Log Identifier C0h). on the subsequent power up, the device shall set bit 3 of the Critical Warning field in the SMART / Health Information log page (Log Identifier 02h) to 1b.
INCS-5	If the device is in read-only mode (i.e., bit 3 in the Critical Warning field is set to 1b in the SMART / Health Information log page (Log Identifier 02h)) for any reason, then the device shall still support NVMe Admin commands, including commands that result in a purge (see SEC-43).
INCS-6	If the Error Recovery log page (Log Identifier C1h) is supported, when the device increments the Incomplete Shutdowns field in SMART / Health Information Extended log page (Log Identifier C0h), it shall use the following recovery procedure at the next power up: <pre> graph TD A[Incomplete Shutdown Occurs] --> B[Device detects the event on next power up and increments the Incomplete Shutdowns field (See SMART-15)] B --> C[Device enters into panic state (see Section 7.4), returns errors for all I/O commands without accessing the media and reports the Device Recovery Action needed in Error Recovery (Log Identifier C1h) with Device Recovery Action 1 set to 02h (i.e., bit 1 set to 1b and all other bits cleared to 0). See EREC-3.] C --> D[Host executes the specified Error Recovery Action (Format NVM)] D --> E{Was the Error Recovery Action successful?} E -- Yes --> F[Device returns to normal operational state] E -- No --> C </pre>
INCS-7	If the Error Recovery log page (Log Identifier C1h) is not supported, when the device increments the Incomplete Shutdowns field in SMART / Health Information Extended log page (Log Identifier C0h), it shall use the following recovery procedure at the next power up:

Requirement ID	Description
	<pre> graph TD A[Drive incomplete Shutdown occurs] --> B[FW needs to detect that the event occurred on next time the drive powers up] B --> C["Drive enters into a degraded state: - Visible to host - Reject reads/writes - Allow Format command (For NVMe, use Secure erase settings - value = 1) - Allow get log command and any vendor-unique commands to grab drive log - Sends NVMe async event notification to host"] C --> D[Drive power cycle or any event that causes a reset of the controller/FW] D --> E{Was secure erase performed on prior power cycle?} E -- Yes --> F["- Drive boots into normal operational state - Don't send any async event"] E -- No --> C </pre>

7.3 End to End Internal Data Protection

Requirement ID	Description
E2E-1	All user data and metadata shall be protected using overlapping protection mechanisms throughout the entire read and write path in the device including all storage elements (registers, caches, SRAM, DRAM, NAND, etc.).
E2E-2	At least one bit of correction and 2 bits of detection is required for all memories. This shall be for all memories regardless of function.
E2E-3	The entire DRAM addressable space shall be protected with at least one-bit correction and 2 bits of detection scheme (SECCDED). This includes but is not limited to the following: - Flash translation layer (FTL). - Mapping tables (including metadata related to deallocated LBAs). - Journal entries. - Firmware scratch pad. - System variables. - Firmware code.
E2E-4	Silent data corruption shall not be tolerated under any circumstances.
E2E-5	The device shall include a mechanism to protect against returning the data from the wrong logical block address (LBA), including previous copies from the same LBA, to the host. It is acceptable if the device stores additional/modified information to provide protection against returning wrong data to the host. Device shall perform host LBA integrity checking on all transfers to and from the media.
E2E-6	All device metadata, firmware, firmware variables, and other device system data shall be protected by at least a single bit detection scheme.
E2E-7	Any memory buffers that are utilized to accelerate data transfer (read-ahead buffers for example) shall follow the protection scheme outlined in E2E-5.

7.4 Behavior on Firmware Crash, Panic or Assert

Requirement ID	Description
CRASH-1	While the device is in a failed state in which it can no longer accept Write commands (e.g., firmware crash, error, or assert), the device shall allow read access only if it can guarantee data integrity.
CRASH-2	While the device is in a failed state, that is not a controller failure (e.g., firmware crash, HW error, or assert), the device shall still support NVMe Admin commands including the ability to read any failure logs from the device to determine the nature of the failure. After a controller failure, the device may fail Admin commands sent by the host prior to completion of the Error Reset Action in the Error Recovery workflow (see EREC-2).
CRASH-3	Upon device completion of the actions specified in Error Reset Action (see EREC-2) and Device Recovery Action (see EREC-3), if the device is successfully recovered from a failed state, then the device shall function normally as specified in this specification including read and write access at full performance.
CRASH-4	Obsolete.
CRASH-5	The device shall have a mechanism (e.g., watchdog timer) to allow recovery from hangs of the firmware and hardware. The timeout interval of this mechanism shall be less than 2 seconds.

7.5 Annual Failure Rate (AFR)

Requirement ID	Description		
REL-1	The device shall meet an MTBF of 2.5 million hours (AFR of <= 0.35% per JEDEC JESD 218) under the following environmental conditions:		
	Specification	Environment	Requirement
	Temperature	Operational	● 0°C to 50°C (32°F to 122°F) ● < 20°C (68°F) per hour gradient
		Non-Operational	● -40°C to 70°C (-40°F to 158°F) ● < 30°C (86°F) per hour gradient
	Humidity	Operational	● 10% to 90% non-condensing ● Yearly weighted average: < 80% RH ○ 90% of year: < 80% ○ 10% of year: 80% to 90% ● Maximum dewpoint: 29.4°C (85°F)
		Non-Operational	● 5% to 95% non-condensing ● 38°C (100.4°F) maximum wet bulb temperature
REL-2	The device shall meet an MTBF of 2.0 million hours (AFR of <= 0.44% per JEDEC JESD 218) under the following environmental conditions:		

Requirement ID	Description		
	Specification	Environment	Requirement
	Temperature	Operational	● 0°C to 55°C (32°F to 131°F) ● < 20°C (68°F) per hour gradient
		Non-operational	● -40°C to 70°C (-40°F to 158°F) ● < 30°C (86°F) per hour gradient
	Humidity	Operational	● 10% to 90% non-condensing ● Maximum dewpoint: 29.4°C (85°F)
		Non-operational	● 5% to 95% non-condensing ● 38°C (100.4°F) maximum wet bulb temperature
REL-3	The vendor shall provide the temperature conditions used to determine the MTBF.		
REL-4	The vendor shall provide AFR de-rating curves for the Temperature range shown in requirement REL-2 for up to 70°C (158°F).		
REL-5	The AFR targets in REL-1 (MTBF of 2.5 million hours) and REL-2 (MTBF of 2.0 million hours) shall be maintained up to a continuous reported composite temperature of 77°C (170°F) (WCTEMP) with less than 1% of the device power on time above WCTEMP.		
REL-6	The device shall have no exposed raw copper on any component. All copper surfaces, pads, fingers, etc. on all components shall be covered with a minimally reactive coating (e.g., resin packaging material on ICs, gold plating on PCB connectors/pads, silver-tin coatings on component leads and IC balls).		

7.6 Background Data Refresh

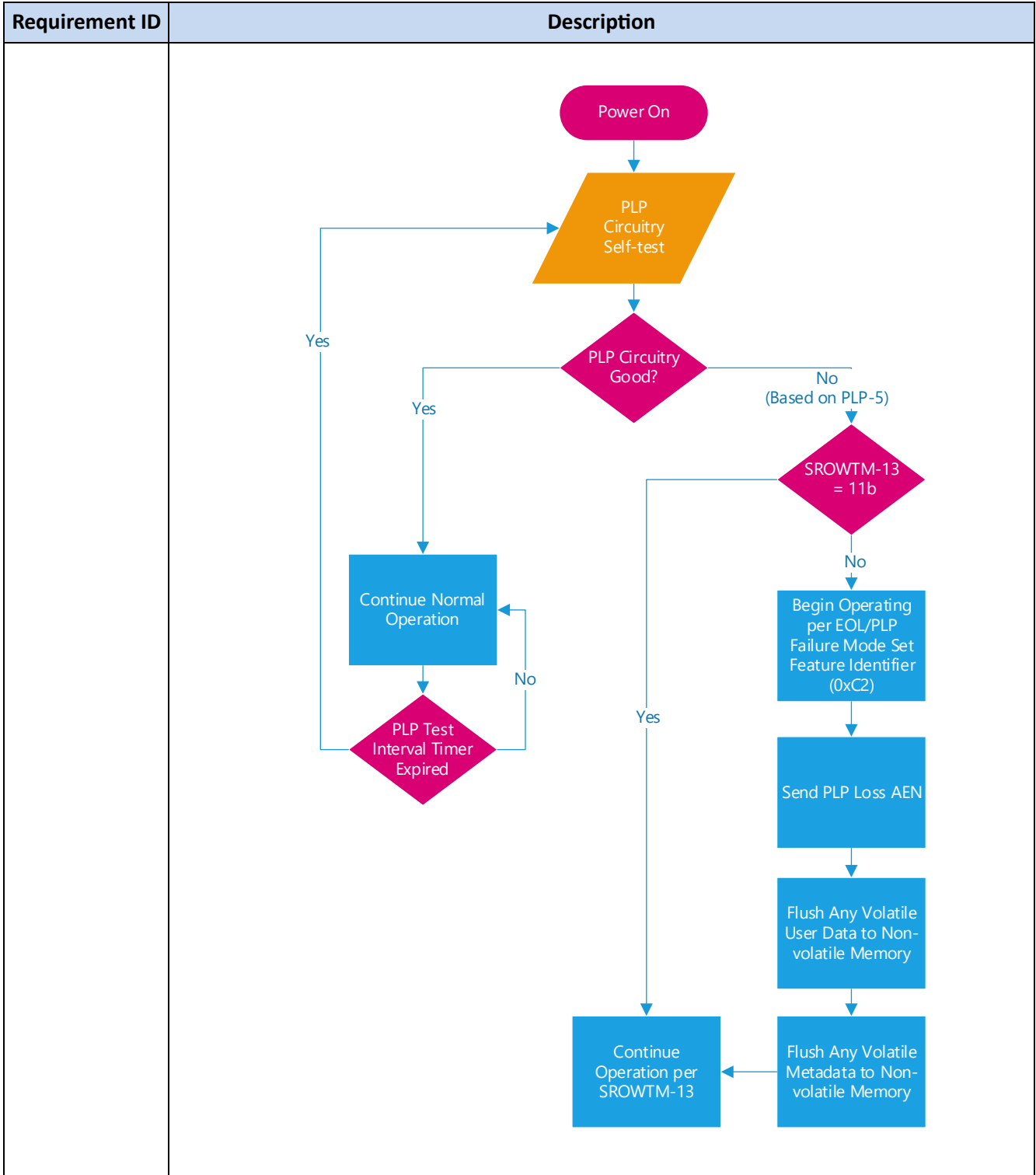
Requirement ID	Description
BKGND-1	The device shall support background data refresh while the device is powered on to ensure there is no data-loss due to power-on retention issues.
BKGND-2	The device shall be designed and tested to support the normal NAND operating temperature.
BKGND-3	Background data refresh shall cover the entire device and be designed to continuously run in the background and not just during idle periods.

7.7 Wear-leveling

Requirement ID	Description
WRL-1	The device shall utilize the entire Endurance Group media capacity range whenever the device needs to wear-level a block. The device shall not restrict the wear-leveling range to a subset of the Endurance Group media capacity unless otherwise specified. If the device does not support Endurance Groups, it shall wear-level across the entire physical media.

7.8 Power Loss Protection

Requirement ID	Description
PLP-1	The device shall support full power-loss protection for all acknowledged data and metadata.
PLP-2	The Power-loss protection health check shall not impact I/O latency and performance.
PLP-3	Power-loss protection health check shall be performed by the device at power-on (prior to accepting any writes) and at least once every time interval as specified in SPLPI-13 .
PLP-4	While performing the power-loss protection health check, the device shall still have enough energy to be able to handle an abrupt power loss properly.
PLP-5	The firmware/hardware algorithm shall deploy safeguards to prevent false detection of power loss protection failure. Example of a false detection would be a glitch in any of the power loss circuitry readings which would cause a transient event to trigger a false power loss protection failure when the power loss protection hardware is healthy.
PLP-6	The device shall implement a power-loss protection (PLP) health check which can detect the capacitor holdup energy margin reported in the Capacitor Health field specified in SMART-19 in SMART / Heath Information Extended log page (Log Identifier C0h). The PLP health check shall not just check for open/short capacitor conditions but shall measure the true available margin energy.
PLP-7	The factory default PLP Health Check Interval shall be 15 minutes (see GPLPI-2).
PLP-8	The default PLP Health Check Interval of 15 minutes (see GPLPI-2) shall not cause the device to violate REL-1 or REL-2 .
PLP-9	The device shall use the following workflow for the PLP Health Check (see INCS-1 for PLP Loss details):



7.9 Device Limits

Requirement ID	Description
DEVLMT-1	The device shall not have any architectural restrictions, other than P/E cycle restrictions of the NAND, on the number of times any of the following events can occur: • Firmware downloads and activation supported (see FWUP-2); or • Changing password when taking/changing ownership via TCG; or • Commands that result in a purge (see SEC-43); or • Power cycles; or • Set Features command/Get Features command (including power state changes); or • Log page or debug log retrievals. This is not meant to be a test until fail requirement.

8 Endurance

8.1 Endurance Data

Requirement ID	Description
ENDUD-1	The device documentation shall include the number of physical bytes able to be written to the device assuming a write amplification of 1. The units should be gigabytes (10^9 bytes).
ENDUD-2	The preconditioning steps to test device performance at end-of-life are: • 50/50 Read/Write workload (by number of I/Os). • 4 KiB Read accesses aligned to 4 KiB boundaries. • 128 KiB Write accesses aligned to 128 KiB boundaries. • Random pattern of Read addresses. • Sequential pattern of Write addresses. • 100% active range. • 80% full device (80% data, 20% free space). • 0% compressible data. • Ambient temperature 35°C (95°F). • Short-stroked device if capacity is 2 TB or greater (see EOL-2).
ENDUD-3	The Percentage Used in the SMART / Health Information log page (Log Identifier 02h) shall track linearly with bytes written and at 100% it shall match the EOL value specified in ENDUD-1.

8.2 Retention Conditions

Since there are several factors that impact the device endurance, the following table provides the requirements for the datacenter environment:

Requirement ID	Description
RETC-1	Non-Operational (Powered-off) device data retention time (end of life) shall be at least 1 month at 40°C (104°F). See Section 13 Device Profiles for specific retention requirements. Specific Devices Profiles may have longer data retention time requirements.
RETC-2	Operating (Powered-on) data retention shall be at least 7 years. For purposes of this requirement, the assumption is that the Terabytes Written (TBW) capability of the devices is used linearly over the lifetime. This requirement does not imply any specific warranty period.
RETC-3	The device shall not throttle its performance based on the endurance metric (endurance throttling).

8.3 Shelf Life

Requirement ID	Description
SLIFE-1	A new device may be kept as a datacenter spare and therefore shall be fully functional even if it sits on the shelf for at least 5 years at 25°C (77°F) before getting installed in the server. The device shall be new in box factory state.
SLIFE-2	Shelf-life shall be documented and provided to the customer.

8.4 End-of-Life (EOL)

Requirement ID	Description
EOL-1	Several types of samples are required for EOL testing: a. Beginning of Life (Short stroked if required by EOL-2). b. End of Life (Short stroked if required by EOL-2). c. End of Life (Not short stroked if different than item b). EOL is defined as the Total Bytes Written (TBW) specification has been surpassed (see ENDUD-1) or the non-volatile media endurance limit (e.g., NAND cycling limit causes the block to be unwritable) has been reached; whichever is earliest.
EOL-2	On 2 TB or larger devices, there shall be a method to “short stroke” the device. Media reserved for background operations shall be proportionally adjusted. Short Stroke firmware capacity shall be reduced to a range of 10% to 3% of full capacity. Short stroke shall cover all the channels/dies/planes while maintaining the native performance of the device.
EOL-3	Obsolete.
EOL-4	The device shall continue to operate in a read/write mode until the conditions in EOL-5 are reached or until another type of error causes the device to be unable to continue to operate in read/write mode (e.g., the device enter read-only mode due to the conditions in INCS-4).
EOL-5	The device shall switch to Read Only Mode (ROM) when the Available Spare field in the SMART / Health Information log page (Log Identifier 02h) reaches 0%. A value of 0% represents the device state where there is an insufficient number of spare blocks to support Host writes. The Available Spare field shall report a value of 0% before the device exhausts

Requirement ID	Description
	all available spare blocks so that there are still sufficient available spare blocks remaining to handle blocks going bad during read operations. When the device switches to ROM due to this condition, bit 2 and bit 3 of the Critical Warning field in the SMART / Health Information log page (Log Identifier 02h) shall be set to 1b. If the value reported in the Available Spares field falls below the value reported in the Available Spare Threshold field, then the device shall set bit 0 of the Critical Warning field in the SMART / Health Information log page to 1b and generate a SMART / Health Status event if that event is enabled and an Asynchronous Event Request command is outstanding.
EOL-6	The device shall have enough spare blocks so that the Percentage Used field value in the SMART / Health Information log page (Log Identifier 02h) reaches 100% prior to the Available Spare field value falling below the Available Spare Threshold field value. See ENDUD-1 and ENDUD-3 for related Percentage Used field value requirements.
EOL-7	The update granularity for the Percentage Used field and Available Spare field in the SMART / Health Information log page (Log Identifier 02h) shall be 1%.
EOL-8	The Available Spare Threshold shall be set such that the Available Spare does not reach 0% for at least three days after crossing the Available Spare Threshold assuming a worst-case write workload.

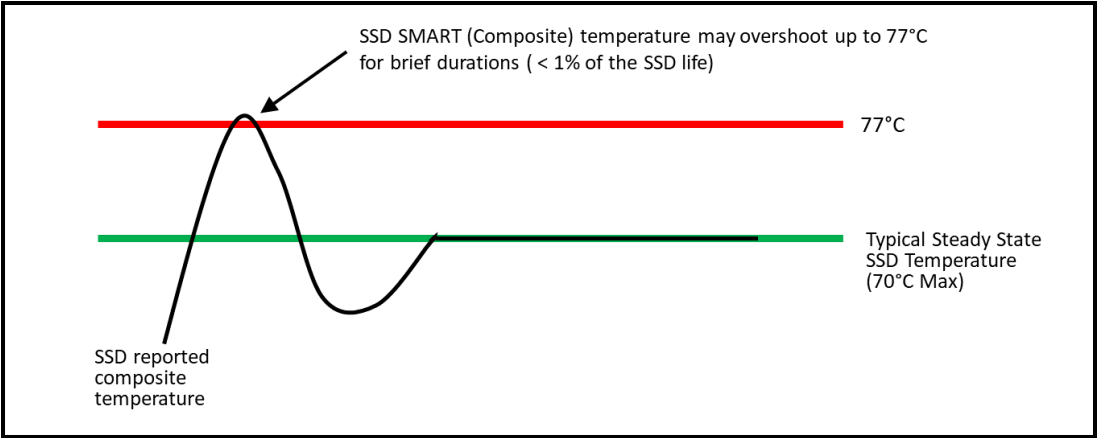
9 Thermal

9.1 Data Center Altitude

Requirement ID	Description
THERM-1	Support for devices in data centers located at an altitude of up to 10,000 feet above sea level is required (e.g., thermals, cosmic rays, etc.). When considering thermals, there shall be no de-rating up to 6,000 feet above sea level. Above 6,000 feet the derating shall be 0.9°C (1.6°F)/1000ft.
THERM-2	A thermal study with each platform is required and shall be provided to the customer. The thermal design shall be validated up to 35°C (95°F) ambient temperature for the platform with a worst-case airflow of 1.5 meters per second at sea level.
THERM-3	The device shall operate normally with relative humidity to be between 10% and 90%.

9.2 Thermal Throttling

Requirement ID	Description
TTHROTTLE-1	The device shall implement a thermal throttling mechanism to protect the device in case of a failure or an excursion that causes the device's temperature to increase above its maximum specified temperature. This mechanism shall check device temperature at a

Requirement ID	Description
	frequency sufficient to ensure that the thermal throttling mechanism protects the device. This temperature check frequency shall be at least once per second.
TTHROTTLE-2	When the device begins throttling performance due to an over temperature condition, an Asynchronous Event Request shall be completed with the Asynchronous Event Type field set to 001b (SMART / Health status) and the Asynchronous Event Information field set to 01h (Temperature Threshold), if that event is enabled and an Asynchronous Event Request command is outstanding. The device shall set bit 1 of the SMART / Health Information log page (Log Identifier 02h) Critical Warning field to 1b.
TTHROTTLE-3	Thermal throttling shall only be engaged under conditions that are able to cause significant reduction in device service life, such as excessive server ambient temperature. The required behavior is illustrated in the following figure: 
TTHROTTLE-4	The firmware algorithm shall deploy safeguards to prevent a false activation of either thermal throttling or thermal shutdown. An example of a false activation would be a glitch in any of the sensor readings which would cause the composite temperature to reach the thermal throttling or thermal shutdown limit.
TTHROTTLE-5	A composite temperature of 77°C (170.6°F) shall be used to start throttling. Single stage and multi-stage throttling are both allowed.
TTHROTTLE-6	Thermal throttling shall not start based on the rate of temperature increase or slew rate.
TTHROTTLE-7	When the device is in the thermal throttling state and the temperature drops back down below 75°C (167°F), the device shall exit the thermal throttling state and an Asynchronous Event Request shall be completed with the Asynchronous Event Type field set to 001b (SMART / Health status) and the Asynchronous Event Information field set to 01h (Temperature Threshold), if that event is enabled and an Asynchronous Event Request command is outstanding. The device shall clear bit 1 of the SMART / Health Information log page (Log Identifier 02h) Critical Warning field to 0b.
TTHROTTLE-8	When the device reaches a critical temperature on any component it shall report a composite temperature of 85°C (185°F) and an Asynchronous Event Request shall be completed with the Asynchronous Event Type field set to 001b (SMART / Health status) and the Asynchronous Event Information field set to 01h (Temperature Threshold), if that event

Requirement ID	Description
	is enabled and an Asynchronous Event Request command is outstanding, before the device shuts off to protect itself.
TTHROTTLE-9	The device shall report a value of 015Eh (77°C) (170.6°F) in the Warning Composite Temperature Threshold (WCTEMP) field of the Identify Controller Data structure.
TTHROTTLE-10	The device shall report a value of 0166h (85°C) (185°F) in the Critical Composite Temperature Threshold (CCTEMP) field of the Identify Controller Data structure.
TTHROTTLE-11	If the Composite Temperature is greater than or equal to 77°C (170.6°F), the device shall update the Warning Composite Temperature Time field of the SMART / Health Information log page (Log Identifier 02h) once per minute until one of the following occurs: • The device Composite Temperature falls below 75°C (167°F); or • The device shuts down due to an over Critical Temperature condition; or • The device is power cycled.
TTHROTTLE-12	The temperature limits of internal components within the device shall govern the thermal throttling algorithms. In addition, the thermal throttling algorithms shall prevent excessive case temperature (see TTHROTTLE-14).
TTHROTTLE-13	In all throttling states including the lowest throttle state, the device shall not enter a read-only mode and shall continue to attempt to process all commands, including commands that write media, unless the device shuts down, e.g., due to a Critical Temperature condition.
TTHROTTLE-14	The critical device case (i.e., touch) temperature shall be the TS2 limits as specified in IEC 62368-1 3rd Edition or later. For non-case devices the hottest surface shall be used for the device touch temperature. The TS2 100°C limit is prohibited for some form factors (see FFM2-15, FFE1S-13, and FFE1L-13).

9.3 Temperature Reporting

Requirement ID	Description
TRPT-1	The device shall expose the current raw sensor readings from all the sensors on the device.
TRPT-2	A device shall report a composite temperature that has an accuracy better than or equal to +/-1°C (1.8°F) degrees. As a consequence, two devices of the same model shall not report a composite temperature greater than 2°C (3.6°F) apart under the same environmental conditions, slot location, and workload.
TRPT-3	A device shall use temperature sensors that have an accuracy better than or equal to +/-1°C (1.8°F) degrees.
TRPT-4	The vendor shall provide the customer the equation, settings, and thresholds used to calculate the composite temperature.
TRPT-5	When calculating the composite temperature, the device shall take into account the temperature of all of the major thermal components (SOC, DRAM, NAND, PMIC, etc.).

Requirement ID	Description
TRPT-6	The reported composite temperature shall be the same for all controllers in the NVM subsystem.

9.4 Thermal Shutdown

Requirement ID	Description
THRMS-1	The device shall shut down to protect itself against data loss or damage due to extreme temperatures. The shutdown temperature value shall be at a composite temperature of 85°C (185°F). Shutdown shall preserve all user data.
THRMS-2	The device shall not process NVM I/O commands while in thermal shutdown. If it is safe to do so, the device shall process Admin commands (in-band and out-of-band), NVMe-MI Command Set commands, and PCIe Command Set commands while in thermal shutdown.
THRMS-3	The device shall only come out of thermal shutdown as a result of a main power cycle or PWRDIS cycling internal device power.

10 Form Factor Requirements

10.1 General Form Factor Requirements

Requirement ID	Description
GFF-1	The device shall be compliant to PCI Express Base Specification, Revision 5.0, Version 1.0 (or later).
GFF-2	The vendor shall provide a PCIe compliance report that demonstrates compliance.
GFF-3	The device shall support lane reversal with all lanes connected or partially connected lanes on both the lower-numbered lanes and higher-numbered lanes of the device (e.g., a x4 device shall support lane reversal for x4, x2, and x1 connections on both the lower-numbered lanes and higher-numbered lanes of the device).
GFF-4	The device shall train to x1 when the upstream device provides only one lane, to x2 when 2 lanes are provided and to x4 when 4 lanes are provided. This requirement applies to both the lower-numbered lanes and higher-numbered lanes of the device.
GFF-5	The device shall support hot swap on form factors that support hot swap.
GFF-6	A CAD file of each supported form factor shall be provided to the customer.
GFF-7	For the purpose of determining when to blink the LED, host-requested activity consists of processing one or more of the following: - any I/O command; - any Admin command whose processing is expected to take more than one second; or - any background activity that was initiated by an Admin command if that background processing is expected to take more than one second.

Requirement ID	Description
	The LED effects of Admin command processing are independent of whether an Admin command was submitted in-band or out-of-band.
GFF-8	For the purpose of determining when to blink the LED, the following activities are not host-requested activity: - internally initiated background activity; - maintenance activity that is not requested by the host; - NVMe Basic Management command activity (see Section 11.1 NVMe Basic Management Command (Appendix A) Requirements); and - NVMe-MI activity (see Section 11.3 NVMe-MI Requirements) with the exception of NVMe Admin commands submitted via NVMe-MI.

10.2 Power Consumption Measurement Methodology

Requirement ID	Description
PCM-1	The device Max Average Power (MAP) consumption for any workload shall not exceed the Maximum Power (MP) of the current NVMe Power State measured over a 1 second window with a sampling rate of 2 ms or less. The measurement duration shall be at least 15 minutes on a pre-conditioned device. This requirement defines the measurement methodology for Maximum Sustained Device Power as defined in SFF-TA-1009 revision 3.0.
PCM-2	The device peak power for any workload shall be measured over a 100 uS window with a sampling interval of 4 uS or less. The measurement duration shall be at least 15 minutes on a pre-conditioned device.
PCM-3	For devices whose max average power consumption is less than or equal to 25 W, the peak power shall be no more than 1.5x the max average power. For devices whose max average power consumption is greater than 25 W but less than or equal to 29W the peak power shall be no more than 37.5 W. For devices whose max average power consumption is greater than 29 W, the peak power shall be no more than 1.3x the max average power. The max average power is defined in PCM-1.
PCM-4	The Maximum Power field in each NVMe Power State Descriptor data structure in the Identify Controller data structure shall indicate (for the described power state) the maximum allowed value of the device Max Average Power (MAP) where MAP is measured as specified by PCM-1.

10.3 Power Levels

Requirement ID	Description
PWR-1	The Power Management (Feature Identifier 02h) shall be supported and the NVMe Power State Descriptor table in Identify Controller Data Structure bytes 3071:2048 shall be filled out per the NVM Express Base Specification.
PWR-2	Obsolete. See DCLP-9 and Section 4.8.11.1 DSSD Power State Descriptor .

Requirement ID	Description
PWR-3	The method of measurement for Maximum Average Power (MAP) is defined in PCM-1 . MAP values are reported in the Maximum Power (MP) field of NVMe Power State Descriptors.
PWR-4	Power state entries above the maximum rated power envelope of the device shall not be populated in the NVMe Power State Descriptor table in Identify Controller Data Structure bytes 3071:2048.
PWR-5	The Set Features for Power Management (Feature Identifier 02h) with the SV bit 31 in Command Dword 10 shall be supported so that the power level can be set and will be saved across power cycles.
PWR-6	The device, regardless of form factor or capacity, shall have an idle power of 5 W or less per European Lot 9 regulation without use of the Idle Wake Up Time Configuration Feature (see Section 4.15.21 Idle Wake Up Time Configuration (Feature Identifier CAh) Set Features). Devices shall automatically reduce power consumption to 5 W or less when idle without impacting latency or performance.
PWR-7	The device shall not consume more power than the PCI-SIG Slot Capabilities register Slot Power Limit regardless of other settings (e.g., DSSD Power State, NVMe Power State).
PWR-8	The device shall not use the same Maximum Power (MP) value in more than one supported NVMe Power State Descriptor unless otherwise specified.
PWR-9	The device shall not support Non-Operational Power State Permissive Mode (i.e., bit 1 of the Controller Attributes field in the Identify Controller data structure shall be cleared to 0b).

10.4 M.2 Form Factor Requirements

Requirement ID	Description
FFM2-1	The device shall adhere to the M.2 specification with a size of 22 mm x 110 mm or 22 mm x 80 mm.
FFM2-2	The bottom-side height shall not exceed 1.5 mm.
FFM2-3	The top-side height shall not exceed 3.2 mm. Some models may need to be thinner (see Section 13 Device Profiles).
FFM2-4	The device shall use an M key.
FFM2-5	The device shall support a minimum of PCIe Gen4 x4.
FFM2-6	The device shall support driving an activity LED through the connector via LED_1#.
FFM2-7	The LED should be lit solidly while power is applied, and the device is not performing host-requested activity (see GFF-8). The LED should blink while the device is performing host-requested activity (see GFF-7).
FFM2-8	The device shall not use any pins that are defined in the M.2 specification for vendor unique functionality.

Requirement ID	Description
FFM2-9	The device shall support a protection scheme that protects against NAND block level failures.
FFM2-10	The protection scheme must also support NAND plane level failures without data or metadata loss.
FFM2-11	The Label shall be placed on the top side of the device.
FFM2-12	The device's SMBus electricals shall comply with version 3.2 (see http://www.smbus.org/specs/SMBus_3_2_20220112.pdf) and in PCI Express M.2 Revision 4.2 or later.
FFM2-13	The device's SMBus protocol shall comply with version 3.2 (see http://www.smbus.org/specs/SMBus_3_2_20220112.pdf).
FFM2-14	The default max average power for M.2 devices shall not exceed 8.25 W and the peak power shall comply to PCM-3 .
FFM2-15	The case (i.e., touch) temperature shall not exceed 80°C (176°F). The 100°C (212°F) TS2 limit does not apply (see TTHROTTLE-14).

10.5 E1.S Form Factor Requirements

Requirement ID	Description
FFE1S-1	The device shall adhere to the latest revision of SFF-TA-1006.
FFE1S-2	At a minimum, the device shall support PCIe Gen4 x4.
FFE1S-3	The device shall support activity and error LEDs.
FFE1S-4	The activity LED shall be lit solidly while power is applied, and the device is not performing host-requested activity (see GFF-8). The activity LED shall blink while the device is performing host-requested activity (see GFF-7).
FFE1S-5	The device shall support a protection scheme that protects against NAND block level failures.
FFE1S-6	The protection scheme must also support NAND plane level failures without data or metadata loss.
FFE1S-7	The amber LED shall meet the requirements specified in SFF-TA-1009. The functioning of the Amber LED shall be independent of the 12 V, 3.3 Vaux and the state of the PWRDIS pin.
FFE1S-8	The thermal performance of the 9.5 mm, 15 mm, and 25 mm cases and their associated pressure drops shall be provided.
FFE1S-9	The PWRDIS pin shall be supported.
FFE1S-10	The SMBus electrical connections shall follow the "DC Specification For 3.3 V Logic Signaling" as defined in SFF-TA-1009 revision 4.1 or later. Including Vih1 with a max of 3.465 V.

Requirement ID	Description
FFE1S-11	The device's SMBus protocol shall comply to version 3.2 (see http://www.smbus.org/specs/SMBus_3_2_20220112.pdf).
FFE1S-12	A x4 device shall only have a 1C connector.
FFE1S-13	The case (touch) temperature shall not exceed 80°C (176°F). The 100°C (212°F) TS2 limit does not apply (see TTHROTTLE-14).
FFE1S-14	The device shall support the amber LED and the green LED. The device shall not support any other LED colors.
FFE1S-15	The device shall be designed to support air cooling.
FFE1S-16	The 9.5mm enclosure shall be designed to support a cold plate connecting to the secondary side of the device. Nothing in the design shall preclude an optional additional cold plate on the primary side of the device.

10.6 E1.L Form Factor Requirements

Requirement ID	Description
FFE1L-1	The device shall adhere to the latest revision of SFF-TA-1007.
FFE1L-2	At a minimum, the device shall support PCIe Gen4 x4.
FFE1L-3	The device shall support activity and error LEDs.
FFE1L-4	The activity LED shall be lit solidly while power is applied, and the device is not performing host-requested activity (see GFF-8). The activity LED shall blink while the device is performing host-requested activity (see GFF-7).
FFE1L-5	The device shall support a protection scheme that protects against NAND block level failures.
FFE1L-6	The protection scheme must also support NAND plane level failures without data or metadata loss.
FFE1L-7	The amber LED shall meet the requirements specified in SFF-TA-1009. The functioning of the Amber LED shall be independent of the 12 V, 3.3 Vaux and the state of the PWRDIS pin.
FFE1L-8	The thermal performance of the 9.5 mm and 18 mm cases and their associated pressure drops shall be provided.
FFE1L-9	The PWRDIS pin shall be supported.
FFE1L-10	The SMBus electrical connections shall follow the "DC Specification For 3.3 V Logic Signaling" as defined in SFF-TA-1009 revision 4.1 or later. Including Vih1 with a max of 3.465 V.
FFE1L-11	The device's SMBus protocol shall comply to version 3.2 (see http://www.smbus.org/specs/SMBus_3_2_20220112.pdf).
FFE1L-12	A x4 device shall only have a 1C connector.

Requirement ID	Description
FFE1L-13	The case (touch) temperature shall not exceed 80°C. The 100°C TS2 limit does not apply (see TTHROTTLE-14).
FFE1L-14	The device shall support the amber LED and the green LED. The device shall not support any other LED colors.

10.7 E3 Form Factor Requirements

Requirement ID	Description
FFE3-1	The device shall adhere to the latest revision of SFF-TA-1008.
FFE3-2	The device shall adhere to the latest revision of SFF-TA-1009.
FFE3-3	The device shall support Separate Reference Clocks with Independent SSC (SRIS) requirements of the PCI Express Base Specification. Devices shall support SRIS detection and switching as described in SFF-TA-1009 and support the full jitter specified by the PCI Express Base Specification (see FFE3-4). The device shall support switching between SRIS and common clock on a power cycle and on assertion/de-assertion of PERST# with or without a power cycle as described in SFF-TA-1009 and shall not switch clocking modes under any other conditions.
FFE3-4	The device shall be compliant to PCI Express Base Specification, Revision 5.0, Version 1.0 (or later).
FFE3-5	The activity LED shall be lit solidly while power is applied, and the device is not performing host-requested activity (see GFF-8). The activity LED shall blink while the device is performing host-requested activity (see GFF-7).
FFE3-6	For Gen6 (64 GT/s) devices, they shall be compliant to PCI Express Base Specification, Revision 6.2 (or later)

10.8 SFF-8639 (U.2/U.3) Form Factor Requirements

Requirement ID	Description
FF8639-1	The device shall adhere to SFF-TA-1001 revision 1.1 or later and the PCI Express SFF-8639 Module Specification, Revision 4.0, Version 1.0 (or later).
FF8639-2	The device shall support Separate Reference Clocks with Independent SSC (SRIS) requirements of the PCI Express Base Specification. Devices shall support SRIS detection and switching as described in the PCI Express SFF-8639 Module Specification (see FF8639-1) and support the full jitter specified by the PCI Express Base Specification Revision 4.0. The device shall support switching between SRIS and common clock on a power cycle and on assertion/de-assertion of PERST# with or without a power cycle and shall not switch clocking modes under any other conditions.

Requirement ID	Description
FF8639-3	All 2.5" SFF NVMe devices shall support the activity LED function on Pin 11 of the SFF-8639 connector. Pin 11 shall assert/de-assert (see FF8639-4) while the device is performing host-requested activity (see GFF-7). Once asserted due to command processing, pin 11 shall remain asserted for 50 ms and then shall be de-asserted for 50 ms. This assert/de-assert behavior shall continue while command processing continues (i.e., the LED is usually off, but flashes on and off while commands are processed). Once pin 11 is de-asserted for 50 ms, it shall remain de-asserted as long as there is no command processing activity.
FF8639-4	Active State (pin asserted and LED on) is defined as logic "0" (i.e., < 0.3 V) on Pin 11. Inactive State is defined as logic "1" (i.e., > 3.3 V) on Pin 11. Device activity other than host-requested activity (e.g., internally initiated background activity or maintenance routine that is not commanded to be performed from the host) shall not cause the LED to be in the Active State (logic "0" level). See GFF-8.

10.9 E2 Form Factor Requirements

Requirement ID	Description
FFE2-1	The device shall adhere to the latest revision of SFF-TA-1042.
FFE2-2	At a minimum, the device shall support PCIe Gen5 x4.
FFE2-3	The device shall support activity and error LEDs.
FFE2-4	The activity LED shall be lit solidly while power is applied, and the device is not performing host-requested activity (see GFF-8). The activity LED shall blink while the device is performing host-requested activity (see GFF-7).
FFE2-5	The device shall support a protection scheme that protects against NAND block level failures.
FFE2-6	The protection scheme shall support NAND plane level failures without data or metadata loss.
FFE2-7	The protection scheme shall support NAND die level failures without data or metadata loss.
FFE2-8	The amber LED shall meet the requirements specified in SFF-TA-1009. The functioning of the Amber LED shall be independent of the 12 V, 3.3 Vaux and the state of the PWRDIS pin.
FFE2-9	The PWRDIS pin shall be supported.
FFE2-10	The SMBus electrical connections shall follow the "DC Specification For 3.3 V Logic Signaling" as defined in SFF-TA-1009 revision 4.1 or later. Including Vih1 with a max of 3.465 V.
FFE2-11	The device's SMBus protocol shall comply to version 3.2 (see http://www.smbus.org/specs/SMBus_3_2_20220112.pdf).

Requirement ID	Description
FFE2-12	The case (touch) temperature shall not exceed 80°C (176°F). The 100°C (212°F) TS2 limit does not apply (see TTHROTTLE-14).
FFE2-13	The device shall support the amber LED and the green LED. The device shall not support any other color LEDs.
FFE2-14	The device shall be designed to support air cooling.
FFE2-15	The device shall be designed to support a cold plate connecting to the secondary side of the device. Nothing in the design shall preclude an optional additional cold plate on the primary side of the device.
FFE2-16	A x4 device shall only have a 1C connector.

11 Management Support

11.1 NVMe Basic Management Command (Appendix A) Requirements

Requirement ID	Description						
SMBUS-1	If the device supports the NVMe Basic Management Command (see DP-CFG-4), then the device shall support that command as defined in Appendix A of the NVM Express Management Interface Specification, Revision 2.0: (https://nvmexpress.org/wp-content/uploads/NVM-Express-Management-Interface-Specification-Revision-2.0-2024.08.05-Ratified.pdf).						
SMBUS-2	SMBus Block Read protocol and Byte Read protocol shall be supported. As an override of the NVM Express Management Interface Specification, SMBus Block Write protocol and Byte Write protocol shall also be supported.						
SMBUS-3	The device shall implement the SMBus format as show in Section 11.2 - NVMe Basic Management Command (Appendix A) Data Format .						
SMBUS-4	Unless otherwise noted, the default value for the Firmware Update Flags field (byte 91) in the SMBus Data structure shall be set to FFh.						
SMBUS-5	The Secure Boot Failure Feature Reporting Supported bit at offset 243 shall be supported and set to 1b.						
SMBUS-6	When there is a secure boot failure the device shall report the failure with the following behavior:						
	<table><tr><th>Bit</th><th>Bit Description</th></tr><tr><td>7</td><td>Shall be set to 1b. See Command Code 242 for the definition of Secure Boot Failure Reporting.</td></tr><tr><td>6</td><td>Shall be set to 1b. See Command Code 242 for the definition of Secure Boot Failure Reporting.</td></tr></table>	Bit	Bit Description	7	Shall be set to 1b. See Command Code 242 for the definition of Secure Boot Failure Reporting.	6	Shall be set to 1b. See Command Code 242 for the definition of Secure Boot Failure Reporting.
	Bit	Bit Description					
7	Shall be set to 1b. See Command Code 242 for the definition of Secure Boot Failure Reporting.						
6	Shall be set to 1b. See Command Code 242 for the definition of Secure Boot Failure Reporting.						

Requirement ID	Description	
	5	Shall be set to 1b and a valid Recovery code shall be entered in byte 244. These codes are defined in the Platform Root-of-Trust for Recovery . Use of these codes is explained in the OCP Hardware Secure Boot White Paper .
	4:0	Reserved. Shall be cleared to zero.
SMBUS-7	The device shall take no longer than the CAP.TO timeout value to produce stable SMBus output through the NVMe Basic Management Command (if supported).	
SMBUS-8	If the device has set a non-zero value in the Error ID field (Command Code 154, byte 01h), then the device shall clear the Drive Functional field to 0b (Command Code 0, byte 01h, Bit 5b).	
SMBUS-9	The device shall generate the PEC values specified for each command code in the SMBus data format described in Section 11.2 - NVMe Basic Management Command (Appendix A) Data Format when the host issues a Block Read.	
SMBUS-10	The device shall check the PEC value sent when the host issues a Block Write and only process the message if the PEC value matches the SMBus data format specified value described in Section 11.2 - NVMe Basic Management Command (Appendix A) Data Format . The device is encouraged to issue a NACK if the PEC value is not correct.	
SMBUS-11	All data returned by the NVMe Basic Management Command shall be returned in big-endian format unless otherwise noted.	

11.2 NVMe Basic Management Command (Appendix A) Data Format

Command Code (Decimal)	Byte Offset (Decimal)	Description	
0	0	Defined in the NVM Express Management Interface Specification.	
8	8	Defined in the NVM Express Management Interface Specification.	
32	32	Payload length of Command Code 32: This is the number of bytes until the PEC code. This shall be set to 10h.	
	48:33	GUID: This is a 16-byte Global Unique Identifier:	
		Byte Address	Value
		33	73h
		34	89h
		35	20h
		36	E5h
		37	6Bh
		38	EEh

Command Code (Decimal)	Byte Offset (Decimal)	Description
		39
		42h
		40
		58h
		41
		9Ah
		42
		7Ah
		43
		CEh
		44
		BDh
		45
		B3h
		46
		5Fh
		47
		00h
		48
		85h
	49	PEC: An 8-bit CRC calculated over the SMBus address, command code, second SMBus address and returned data. The algorithm is defined in the SMBus Specification.
50	50	Payload length of Command Code 50: Indicated the number of additional bytes to read before encountering PEC. Shall be set to 26h.
	51	Temperature Flags: This field reports the effect of temperature on the device's performance. Temperature Throttling – Bit 7 is set to 1b when the device is throttling performance to prevent overheating. Clear to 0b when the device is not throttling. Bits 6:0 shall be set to 111111b.
	52	Max Power Supported: This shall denote the Max Average Power (MAP) supported by this device rounded to the nearest watt (e.g., a 50W device is 32h, a 25W device is 19h, a 15W device is 0Fh, an 8.25W device is 8W which is 08h).
	84:53	Configured NVMe Power State: This is a copy of the NVMe Power State Descriptor Data Structure of the currently configured Power State and is laid out in little-endian format.
	88:85	Total NVM Capacity: This field indicates the total usable NVM capacity in the NVM subsystem in GB in Hex (2048 GB in total capacity = 0000800h). This field is equivalent to the TNVMCAP field in the Identify Controller Data Structure.
	89	PEC: An 8-bit CRC calculated over the SMBus address, command code, second SMBus address and returned data. The algorithm is defined in the SMBus Specification.
90	90	Payload length of Command Code 90: Indicates number of additional bytes to read before encountering PEC. Shall be set to 04h.

Command Code (Decimal)	Byte Offset (Decimal)	Description																
	91	Firmware Update Flags: This field allows the host to control whether the current firmware allows new firmware images to be downloaded and committed via the in-band interface (see Section 12 Security for more information).																
		<table><tr><th>Bit</th><th>Bit Description</th></tr><tr><td rowspan="2">7</td><td>Written by host, read by device:<table><tr><td>1b</td><td>Unlock Firmware Update: Device shall enable Firmware Image Download and Firmware Commit commands both in-band and out-of-band via NVMe-MI.</td></tr><tr><td>0b</td><td>Lock Firmware Update: Device shall block and error on in-band Firmware Image Download and Firmware Commit commands. The device shall allow out-of-band Firmware Image Download and Firmware Commit commands via NVMe-MI.</td></tr></table></td></tr><tr><td rowspan="2">6</td><td>Written by device, read by host:<table><tr><td>1b</td><td>Firmware Update Unlocked: Device allows Firmware Image Download and Firmware Commit commands both in-band and out-of-band via NVMe-MI.</td></tr><tr><td>0b</td><td>Firmware Update Locked: Device blocks and errors on in-band Firmware Image Download and Firmware Commit commands. The device allows out-of-band Firmware Image Download and Firmware Commit commands via NVMe-MI.</td></tr></table></td></tr><tr><td>5:0</td><td>Shall be set to 111111b.</td></tr></table>	Bit	Bit Description	7	Written by host, read by device: <table><tr><td>1b</td><td>Unlock Firmware Update: Device shall enable Firmware Image Download and Firmware Commit commands both in-band and out-of-band via NVMe-MI.</td></tr><tr><td>0b</td><td>Lock Firmware Update: Device shall block and error on in-band Firmware Image Download and Firmware Commit commands. The device shall allow out-of-band Firmware Image Download and Firmware Commit commands via NVMe-MI.</td></tr></table>	1b	Unlock Firmware Update: Device shall enable Firmware Image Download and Firmware Commit commands both in-band and out-of-band via NVMe-MI.	0b	Lock Firmware Update: Device shall block and error on in-band Firmware Image Download and Firmware Commit commands. The device shall allow out-of-band Firmware Image Download and Firmware Commit commands via NVMe-MI.	6	Written by device, read by host: <table><tr><td>1b</td><td>Firmware Update Unlocked: Device allows Firmware Image Download and Firmware Commit commands both in-band and out-of-band via NVMe-MI.</td></tr><tr><td>0b</td><td>Firmware Update Locked: Device blocks and errors on in-band Firmware Image Download and Firmware Commit commands. The device allows out-of-band Firmware Image Download and Firmware Commit commands via NVMe-MI.</td></tr></table>	1b	Firmware Update Unlocked: Device allows Firmware Image Download and Firmware Commit commands both in-band and out-of-band via NVMe-MI.	0b	Firmware Update Locked: Device blocks and errors on in-band Firmware Image Download and Firmware Commit commands. The device allows out-of-band Firmware Image Download and Firmware Commit commands via NVMe-MI.	5:0	Shall be set to 111111b.
		Bit	Bit Description															
		7	Written by host, read by device: <table><tr><td>1b</td><td>Unlock Firmware Update: Device shall enable Firmware Image Download and Firmware Commit commands both in-band and out-of-band via NVMe-MI.</td></tr><tr><td>0b</td><td>Lock Firmware Update: Device shall block and error on in-band Firmware Image Download and Firmware Commit commands. The device shall allow out-of-band Firmware Image Download and Firmware Commit commands via NVMe-MI.</td></tr></table>	1b	Unlock Firmware Update: Device shall enable Firmware Image Download and Firmware Commit commands both in-band and out-of-band via NVMe-MI.	0b	Lock Firmware Update: Device shall block and error on in-band Firmware Image Download and Firmware Commit commands. The device shall allow out-of-band Firmware Image Download and Firmware Commit commands via NVMe-MI.											
			1b	Unlock Firmware Update: Device shall enable Firmware Image Download and Firmware Commit commands both in-band and out-of-band via NVMe-MI.														
0b	Lock Firmware Update: Device shall block and error on in-band Firmware Image Download and Firmware Commit commands. The device shall allow out-of-band Firmware Image Download and Firmware Commit commands via NVMe-MI.																	
6	Written by device, read by host: <table><tr><td>1b</td><td>Firmware Update Unlocked: Device allows Firmware Image Download and Firmware Commit commands both in-band and out-of-band via NVMe-MI.</td></tr><tr><td>0b</td><td>Firmware Update Locked: Device blocks and errors on in-band Firmware Image Download and Firmware Commit commands. The device allows out-of-band Firmware Image Download and Firmware Commit commands via NVMe-MI.</td></tr></table>	1b	Firmware Update Unlocked: Device allows Firmware Image Download and Firmware Commit commands both in-band and out-of-band via NVMe-MI.	0b	Firmware Update Locked: Device blocks and errors on in-band Firmware Image Download and Firmware Commit commands. The device allows out-of-band Firmware Image Download and Firmware Commit commands via NVMe-MI.													
	1b	Firmware Update Unlocked: Device allows Firmware Image Download and Firmware Commit commands both in-band and out-of-band via NVMe-MI.																
0b	Firmware Update Locked: Device blocks and errors on in-band Firmware Image Download and Firmware Commit commands. The device allows out-of-band Firmware Image Download and Firmware Commit commands via NVMe-MI.																	
5:0	Shall be set to 111111b.																	
The device shall revert to the default Unlock/Lock state on the next power cycle. If the host attempts to issue an in-band Firmware Image Download command or Firmware Commit when the device is in the Firmware Update Locked state, the device shall fail the command with status Operation Denied.																		
94:92	Reserved. Shall be cleared to zero.																	
95	PEC: An 8-bit CRC calculated over the SMBus address, command code, second SMBus address and returned data. The algorithm is defined in the SMBus Specification.																	
96	96	Payload length of Command Code 96: Indicates number of additional bytes to read before encountering PEC. Shall be set to 38h.																
	104:97	Firmware Version Number: This field shall indicate the activated firmware version that is running on the device after the firmware activation took place. The format of this field shall be as defined in the Firmware Revision (FR) field in the Identify Controller data structure.																

Command Code (Decimal)	Byte Offset (Decimal)	Description							
	112:105	Security Version Number: This is the Security Version Number of the currently running firmware image. The vendor increments this number any time a firmware includes a fix for a security issue or critical firmware fix that customer agrees rollback prevention is required. This is a copy of SMART-22 Security Version Number.							
	152:113	Model Number: This shall be a copy of the data in the Model Number field of Identify Controller Data Structure (CNS 01h, byte offset 63:24).							
	153	PEC: An 8-bit CRC calculated over the SMBus address, command code, second SMBus address and returned data. The algorithm is defined in SMBus Specification.							
154	154	Payload length of Command Code 154: Indicates number of additional bytes to read before encountering PEC. Shall be set to 0Bh.							
	155	Error Rest Action: See EREC-2 .							
	156	Device Recovery Action 1: See EREC-3 .							
	164:157	Error ID: See EREC-4 .							
	165	Device Recovery Action 2: See EREC-14 .							
	166	PEC: An 8-bit CRC calculated over the SMBus address, command code, second SMBus address and returned data. The algorithm is defined in the SMBus Specification.							
167	167	Payload length of Command Code 167: Indicates number of additional bytes to read before encountering PEC. Shall be set to 20h.							
	199:168	Error Context Buffer: Vendor may record additional information about the Error ID reported in Command Code 154. Any unused bytes shall be cleared to zero.							
	200	PEC: An 8-bit CRC calculated over the SMBus address, command code, second SMBus address and returned data. The algorithm is defined in the SMBus Specification.							
201	241:201	Reserved. Shall be cleared to zero.							
242	242	Payload length of Command Code 242: Indicates number of additional bytes to read before encountering PEC. Shall be set to 04h.							
	243	Secure Boot Failure Reporting:							
			<table><tr><th>Bit</th><th>Bit Description</th></tr><tr><td>7</td><td>Secure Boot Failure Feature Reporting Supported: When set to 1b the secure boot feature reporting is supported. When cleared to 0b the secure boot failure feature reporting is not supported.</td></tr><tr><td>6</td><td>Secure Boot Failure Status: When cleared to 0b there is no secure boot failure. When set to 1b there is a secure boot failure. This bit shall only</td></tr></table>	Bit	Bit Description	7	Secure Boot Failure Feature Reporting Supported: When set to 1b the secure boot feature reporting is supported. When cleared to 0b the secure boot failure feature reporting is not supported.	6	Secure Boot Failure Status: When cleared to 0b there is no secure boot failure. When set to 1b there is a secure boot failure. This bit shall only
		Bit	Bit Description						
7	Secure Boot Failure Feature Reporting Supported: When set to 1b the secure boot feature reporting is supported. When cleared to 0b the secure boot failure feature reporting is not supported.								
6	Secure Boot Failure Status: When cleared to 0b there is no secure boot failure. When set to 1b there is a secure boot failure. This bit shall only								

Command Code (Decimal)	Byte Offset (Decimal)	Description	
			be set if the Secure Boot Feature Supported bit is set to 1b and there is a secure boot failure.
		5	OCP Recovery/ Platform Root-of-Trust for Recovery: When set to 1b, OCP Recovery/ Platform Root-of-Trust for Recovery codes are supported in byte 244. When cleared to 0b OCP Recovery/ Platform Root-of-Trust for Recovery codes are not supported and byte 244 shall be cleared to zero.
		4:0	Reserved. Shall be cleared to zero.
	244	Recovery Code: OCP Recovery/Platform Root-of-Trust for Recovery code.	
	246:245	Reserved. Shall be cleared to zero.	
	247	PEC: An 8-bit CRC calculated over the SMBus address, command code, second SMBus address and returned data. The algorithm is defined in the SMBus Specification.	
	248	248	Payload length of Command Code 248: Indicates number of additional bytes to read before encountering PEC. Shall be set to 06h.
250:249		Data Format Version Number: Indicates the version of this mapping used in the device. Shall be set to 0004h.	
254:251		Reserved. Shall be cleared to zero.	
255		PEC: An 8-bit CRC calculated over the SMBus address, command code, second SMBus address and returned data. The algorithm is defined in the SMBus Specification.	

11.3 NVMe-MI Requirements

Requirement ID	Description
NVMe-MI-1	The device shall support NVM Express Management Interface Specification, Revision 2.0 or later, including all mandatory requirements. The vendor shall provide an NVMe-MI compliance report that demonstrates compliance.
NVMe-MI-2	The device shall support all NVMe-MI functionality required by this specification over SMBus, even when the PCIe link is not active (as required by the NVM Express Management Interface Specification).
NVMe-MI-3	The device shall support NVMe-MI over PCIe VDM (see NVMe-MI-1).
NVMe-MI-4	The device shall support SMBus Fixed and Discoverable.
NVMe-MI-5	The device shall NACK any SMBus addresses not listed in the NVM Express Management Interface Specification.
NVMe-MI-6	The device shall support the Get UDID command per the SMBus Specification.
NVMe-MI-7	Obsolete, see FRU-1 .

Requirement ID	Description
NVMe-MI-8	Obsolete, see NVMe-MI-2.
NVMe-MI-9	Obsolete, see NVMe-MI-3.
NVMe-MI-10	All mandatory NVMe Admin commands and the following optional NVMe Admin commands shall be supported by MCTP over SMBus, and by MCTP over PCIe VDM. • Firmware Commit • Firmware Image Download • Format NVM • Lockdown • Sanitize • Security Send for TCG devices • Security Receive for TCG devices • Device Self-test • Set Features
NVMe-MI-11	All mandatory Log Identifiers, all Log Identifiers defined in this specification, and the following optional Log Identifiers shall be supported by MCTP over SMBus, and by MCTP over PCIe VDM. • Device Self-test (06h) • Telemetry Host-Initiated (07h) • Telemetry Controller-Initiated (08h) • Persistent Event Log (0Dh) • Command and Feature Lockdown (14h) • Sanitize Status (81h) • SMART / Health Information Extended (C0h)
NVMe-MI-12	Obsolete. See NVMe-MI-11.
NVMe-MI-13	All mandatory Feature Identifiers, all Feature Identifiers defined in this specification, and the following Feature Identifiers shall be supported by MCTP over SMBus, and by MCTP over PCIe VDM. • Power Management (02h) • Timestamp (0Eh) • Temperature Threshold (04h)
NVMe-MI-14	The device shall support locking down all supported Admin commands and all supported Features on the in-band interface via a Lockdown command issued out-of-band via MCTP over SMBus, and by MCTP over PCIe VDM. This includes the Lockdown command itself, and all Admin commands and Features not referenced in this specification.
NVMe-MI-15	The following commands are prohibited and shall return an NVMe-MI Response Message Status of Invalid Command Opcode: • PCIe Memory Write • PCIe Memory Read • PCIe I/O Write • PCIe I/O Read

Requirement ID	Description
	Support for the PCIe Configuration Read command is optional.
NVMe-MI-16	Access to user data is prohibited via out-of-band NVMe-MI (e.g., vendor-specific commands shall not access user data).
NVMe-MI-17	The device shall support SMBus/I2C Frequencies of 100 KHz and 400 KHz.
NVMe-MI-18	For SMBus, the device shall support all possible MCTP Transmission Unit Size values up to the largest (250 bytes).
NVMe-MI-19	For PCIe VDM, the NVMe device shall support all possible MCTP Transmission Unit Size values up to the PCIe Max Payload Size Supported.
NVMe-MI-20	NVMe devices shall support a minimum throughput of 50 MiB/s for data transfer in each direction over the MCTP over PCIe VDM interface under the assumptions that: a) there is no delay between Request Messages from the Management Controller for transfers that require multiple Request/Response Messages; and b) there is a single data transfer and no other MCTP over PCIe VDM activity at the device. This is a sustained throughput requirement for large transfers of 1 MiB or more (e.g., transfer a firmware image to the device, transfer a telemetry log page from the device) that does not include the overhead to start and end a transfer.
NVMe-MI-21	Any TCG method invoked via NVMe-MI that takes longer than 100 ms shall run in the background using the OutstandingData mechanism (preferred) or the More Processing Required mechanism.
NVMe-MI-22	The device shall support NVMe-MI over SPDMM Secured Messages (see SPDM-7).
NVMe-MI-23	The device shall support the following Asynchronous Event Messages per TP6035a and shall support the following Asynchronous Events: • Controller Fatal Status (Asynchronous Event ID 01h) • Shutdown Status (Asynchronous Event ID 02h) • Namespace Attribute Changed (Asynchronous Event ID 04h) • Firmware Activated (Asynchronous Event ID 05h) • Composite Temperature (Asynchronous Event ID 06h) • Percentage Drive Life Used (Asynchronous Event ID 07h) • Available Spare (Asynchronous Event ID 08h) • SMART Warnings (Asynchronous Event ID 09h) • Telemetry Controller-Initiated Data Available (Asynchronous Event ID 0Ah) • PCIe Link Active (Asynchronous Event ID 0Bh) • Sanitize Failure Mode (Asynchronous Event ID 0Ch)
NVMe-MI-24	If the device is in SMBus mode, and the SMBus clock is low for longer than $t_{\text{TIMEOUT,MIN}}$ (refer to the SMBus Specification), then the device shall perform SMBus clock-low recovery even if firmware is hung. Refer to section 4.2.2 of the SMBus specification version 3.3.1 – the behavior that is “highly recommended” (including the communication interface reset) is mandatory in this specification.

Requirement ID	Description
NVMe-MI-25	The device shall support retrieval of log pages greater than 4 KiB as required by the NVM Express Management Interface Specification.
NVMe-MI-26	For devices that support auxiliary power, the device shall be fully functional including NVMe-MI over SMBus/I2C as long as main power is present even if auxiliary power is absent.
NVMe-MI-27	For form factors that support I3C, the device shall support I3C Basic Specification v1.1.1 as specified in the NVM Express Management Interface Specification and SFF-TA-1009 Enterprise and Datacenter Standard Form Factor Pin and Signal Specification.
NVMe-MI-28	The device shall support the PCIe Configuration Write command for a single-byte-sized PCIe Configuration Write to the Power Management Control/Status Register (Offset 04h) in the PCI Power Management Capability Structure. PCIe Configuration Writes to any register other than the Power Management Control/Status Register and PCIe Configuration Writes that access any byte offset other than 4h (e.g., a multi-byte write that starts at offset 4h) shall be aborted with a status code of Access Denied.
NVMe-MI-29	The device shall support multiple NVMe-MI Management Endpoints per 2-wire port (i.e., I2C or I3C port) via MCTP bridging for Endpoint Identifier assignment so that multiple Management Controllers are able to manage the device via NVMe-MI. This device support for multiple Management Endpoints shall include support for TP6034a, which is included in NVMe-MI 2.0, see NVMe-MI-1. If the device is unable to use MCTP bridging for Endpoint Identifier assignment on a 2-wire port (e.g., because the device is unable to obtain Endpoint Identifiers for MCTP bridging to assign to multiple NVMe-MI Management Endpoints), then the device shall use a single NVMe-MI Management Endpoint for that 2-wire port.
NVMe-MI-30	If the device is in I3C mode and the I3C Clock is low for longer than the T2wrst min time (see the SFF-TA-1009 specification), then the device shall switch to SMBus mode, even if the firmware is hung. See NVMe-MI-24 for required behavior if the SMBus clock remains low after switching to SMBus mode.
NVMe-MI-31	A device that supports I3C shall support I3C Basic SDR with a frequency of 12.5 MHz.
NVMe-MI-32	A device that supports I3C shall support I3C Basic HDR-DDR with a frequency of 12.5 MHz.

11.4 VPD Requirements

Requirement ID	Description
FRU-1	The device shall have a VPD that is accessible over SMBus and supports IPMI Platform Management FRU Information. The VPD shall support all required elements that are defined in the NVM Express Management Interface Specification.
FRU-2	The device shall support a FRU Information Device Size of at least 512 bytes.
FRU-3	The device shall support the NVMe MultiRecord (i.e., Record Type ID 0Bh). The length of MultiRecord shall be set to 20h to remove reserved bytes.

Requirement ID	Description
FRU-4	The device shall support the NVMe PCIe MultiRecord (i.e., Record Type ID 0Ch). The length of MultiRecord shall be set to 8h to remove reserved bytes.
FRU-5	The device shall support the following Topology MultiRecords (i.e., Record Type ID 0Dh): - Upstream Connector Element Descriptor (i.e., Element Descriptor Type 2h); - NVM Subsystem Element Descriptor (i.e., Element Descriptor Type 7h); and - FRU Information Device Element Descriptor (i.e., Element Descriptor Type 8h).
FRU-6	The Maximum Power field in the Upstream Connector Element Descriptor shall indicate maximum average power measured required by PCM-1 .

12 Security

12.1 Basic Security Requirements

Requirement ID	Description
SEC-1	All device firmware images shall be signed with both a classical (see SBT-1) and PQC (see SBT-4) algorithm. The device shall validate both signatures successfully before the device completes processing a Firmware Commit command that commits a firmware image and before a firmware image is activated. Both device firmware image signatures shall be validated on every reboot and during firmware update.
SEC-2	The device shall support XTS-AES-256 (as specified in NIST SP 800-38E, which references IEEE STD 1619) or AES-256-GCM (as specified in NIST SP 800-38D) hardware-based data encryption for performance and to prevent firmware tampering with the encryption mechanism. AES-256-GCM is the preferred mode. The combination of AES-256-CTR (as specified in NIST SP 800-38A) with HMAC-SHA256 (where the HMAC is calculated on the ciphertext) is an acceptable alternative.
SEC-3	The device shall support anti-rollback protection for firmware. If the Security Version Number (see SMART-22) of the firmware being committed or activated is greater or equal to the Security Version Number of the currently running firmware, then the firmware is allowed to be committed or activated. If the Security Version Number of the firmware being committed or activated is less than the Security Version Number of the currently running firmware, then the firmware shall not be committed or activated. If firmware activation occurs as a result of a power cycle, then the term “currently running firmware” in this requirement refers to the firmware that was running immediately prior to that power cycle. See FWUP-8 for additional Firmware Commit command requirements.
SEC-4	The device shall support Crypto Erase (see NVMe-AD-5) and NVMe-AD-7).
SEC-5	The device shall support Secure Boot (see Section 12.2 Secure Boot).
SEC-6	The device shall have a method of identifying a secure boot failure which does not require physical access to the device.

Requirement ID	Description
SEC-7	The device's cryptographic module shall be FIPS 140-3 level 2 capable per CMVP and shall follow the NIST 800-90 (A, B and C) specification.
SEC-8	The device shall only implement NIST approved cryptographic algorithms and shall be designed to achieve FIPS-140-3 validation (see SEC-7).
SEC-9	The device shall support key revocation allowing a new key to be used for firmware verification. The device shall support at least 4 key revocations, and key revocation shall not make the device unbootable (i.e., the device supports at least 5 keys).
SEC-10	Obsolete. Moved to TCG-FEATURE-1 .
SEC-11	Obsolete. Moved to TCG-FEATURE-2 .
SEC-12	Obsolete. Moved to TCG-FEATURE-3 .
SEC-13	TCG devices shall support the IEEE1667 Probe (100h) and the TCG Storage Transport (104h) silos. See SEC-50 and SEC-51 for additional IEEE1667 requirements.
SEC-14	The vendor shall follow the Security Development Lifecycle (SDL), and provide a report with the following for each qualification-ready or production-ready firmware version: • The Threat Model. • Fuzz & Pen Tests. • Static Analysis. • Build Logs and Compiler Security Settings. Additional information about the SDL is available here: https://www.microsoft.com/en-us/sdl/default.aspx
SEC-15	A firmware audit of the initial firmware released to customer intended for qualification and any subsequent firmware release intended for production use shall be performed using OCP SAFE, Framework v1.0 or later. A Scope 1 audit is the minimum requirement. The detailed report for each firmware release delivered to the customer shall be provided to the customer. The customer may choose to put the firmware release into production use ahead of the vendor delivering the completed SAFE audit results (e.g., deploy hotfix firmware before the incremental SAFE audit for that hotfix firmware is received).
SEC-16	All signing keys shall be stored in a Hardware Security Module (HSM) that is either FIPS 140-2 Level 3 (or greater) certified or FIPS 140-3 Level 3 (or greater) certified.
SEC-17	Access/use of signing keys should be restricted to a small set of developers, following the principle of least privilege. The number of people with access and their corresponding roles shall be provided.
SEC-18	All debug ports shall be disabled before the device leaves the factory. Alternatively, the ports shall only be accessible in the field after a successful exchange of a challenge-response mechanism using an asymmetric crypto scheme (see NIST SP 800-63). The state shall be reset to inaccessible on any reset or power cycle.
SEC-19	All vendor unique commands, log pages or set features that are not explicitly defined in this specification or approved of in writing by the customer shall be disabled before the device

Requirement ID	Description
	leaves the factory. Alternatively, the commands/log pages/set features shall only be accessible in the field after a successful exchange of a challenge-response mechanism using an asymmetric crypto scheme (see NIST SP 800-63). The state shall be reset to inaccessible on any reset or power cycle.
SEC-20	Adversarial testing using red teams shall be conducted before the start of customer qualification of the initial product and any major firmware or hardware revision. A report of items attempted, and results shall be provided to the customer.
SEC-21	The vendor shall provide timely notification to the customer of security issues and delivery of fixes to the customer: • The vendor shall document all security fixes with each firmware update. • The vendor shall notify end customer within 7 days of discovering security issues in the device hardware or firmware. • Notification of issues shall include the process and timeline of the vendor's commitment to fix the issue: ○ For privately disclosed vulnerabilities, the duration shall be no longer than 90 days. ○ For publicly disclosed vulnerabilities, the duration shall be no longer than 7 days. ○ Vendors shall notify the customers about the known CVEs and security issues and provide security-related updates before public announcement.
SEC-22	The Telemetry Controller-Initiated log page, Telemetry Host-Initiated log page, shall be designed so that the contents of Data Area 1 and Data Area 2 are human readable after decoding via the OCP plugin for the nvme-cli, see TEL-14 . Telemetry Data Areas 3 and 4 should be human readable after decoding via a vendor-specific tool. The contents of Data Area 1 and Data Area 2 shall be sufficient for debugging.
SEC-23	The device shall not include user data, passwords, keys, or any secret or sensitive information in any Telemetry or debug log pages.
SEC-24	All public keys shall be revocable.
SEC-25	Secure Boot Flow shall be based upon a hardware root of trust. All mutable key(s), certificate(s), and/or firmware shall be cryptographically bound to the hardware root of trust. See Section 12.2 Secure Boot .
SEC-26	The device shall only update firmware via a secure firmware update flow that shall be based upon immutable public keys.
SEC-27	Obsolete. Moved to TCG-CRYPTO-1 .
SEC-28	The device shall purge all symmetric keys and all private asymmetric keys from volatile memory as soon as they are no longer needed for operation during the current power on state.
SEC-29	The device shall only store, even if temporarily, host provided passwords, host provided keys, or any host provided secret information in non-volatile memory in an encrypted form. The encryption key(s) for this protection shall not be stored in non-volatile memory. Device

Requirement ID	Description
	shall not store plaintext/cleartext secrets in any non-volatile memories. The device shall protect all such stored passwords, keys, and secrets from unauthorized modification.
SEC-30	The vendor must deliver key management and encryption flow diagram details (not source code) which includes: • Encryption algorithms and modes (e.g., RNG, wrapping function, key derivation function). • Key size and password length. • Any crypto information that is stored in nonvolatile memory. • Critical Security Parameters. Complete details about algorithm inputs (e.g., Initialization vector source and size, salt source and size, unique per device/product line/vendor)
SEC-31	The vendor shall provide industry certification reports, once they are available such as FIPS and OCP SAFE for device and device components such as TRNG, RNG, Crypto engine etc.
SEC-32	Log data and user data (data transferred from the Host in Write Commands) shall be stored on physically separate areas on the device. For example, in the system area and the user data area, respectively.
SEC-33	The vendor shall provide a comprehensive list of what is included in the logs covering both the standard logs and vendor-unique logs. The list shall identify any defined optional events or items that are not logged by the device.
SEC-34	Obsolete.
SEC-35	All telemetry and debug logs shall only be writable by device firmware that has been verified as part of a secure boot.
SEC-36	Obsolete. Moved to TCG-AUTH-3 .
SEC-37	Obsolete. Moved to NVME-MI-2 and NVME-MI-10 .
SEC-38	Obsolete. Moved to TCG-FEATURE-4 .
SEC-39	The device shall not allow the host to read firmware or boot code from the device.
SEC-40	All device firmware packages shall be encrypted based on a symmetric encryption algorithm. See SEC-2 for acceptable algorithms and SEC-29 for key storage requirements.
SEC-41	If the device does not support Caliptra, the device shall only support activation of encrypted firmware images.
SEC-42	If the device does not support Caliptra, the device shall only store firmware in encrypted format when stored in non-volatile memory to protect against physical disassembly of drive to extract stored firmware from media.
SEC-43	Sanitize, Format NVM User Data Erase/Cryptographic Erase, and TCG Revert/RevertSP/GenKey functionality shall comply with the IEEE 2883-2022 Purge requirements.
SEC-44	Any command that changes the media encryption key(s) as part of its operation (e.g., Sanitize command with Crypto Erase (100b), TCG Revert, TCG RevertSP, etc.), shall purge, as

Requirement ID	Description
	defined in IEEE 2883-2022, all copies of the previous key(s) before the device completes the operation. If the device cannot guarantee that all copies of the previous media encryption key(s) have been purged, then the device shall fail the operation.
SEC-45	Any optional security features supported by the device and not described in this document shall be clearly documented and disclosed to the customer.
SEC-46	TCG devices shall support the Security Receive and Security Send commands in-band (i.e., bit 0 in the Optional Admin Command Support field in the Identify Controller data structure shall be set to 1b).
SEC-47	The Cryptographic Module Boundary should be defined to minimize the size and scope of the Cryptographic Module, and in particular the Cryptographic Module Boundary should not encompass the entire physical device. This enables FIPS certification of the Cryptographic Module to be leveraged across multiple device configurations and versions. To facilitate a timelier NIST certification approval process, any revalidations made to the Cryptographic Module Boundary should be Non-Security Relevant. The Cryptographic Module Boundary shall include all relevant cryptographic functions within the boundary itself, such as the data at rest encryption algorithms per FIPS 197 and digital signature algorithms for firmware authentication per FIPS 186-5. The device is required to provide compliance information that enables the host to obtain FIPS certification information that is associated with the Cryptographic Module, see SEC-52.
SEC-48	At a minimum, the device shall support the following signature and hashing algorithms for secure boot, firmware update, CoRIM, and SPDm implementations: • ECDSA P384 or other asymmetric key signature algorithms that meet at least 192-bits of security strength as documented in NIST SP 800-57 Part 1 Revision 5 (Table 2). The device may also support RSA 3072 instead. • SHA-384, SHA3-384, or other hashing algorithms that meet at least 192-bits of security strength as documented in NIST SP 800-57 Part 1 Revision 5 (Table 3). • ML-KEM-1024 as specified in FIPS 203. • ML-DSA-87 as specified in FIPS 204 or one of LMS or XMSS as specified in NIST SP800-208. ○ ML-DSA-87 is preferred.
SEC-49	The device shall not reveal secrets (including passwords, asymmetric private keys, symmetric keys, and any other secret information) even in encrypted form via programmatic methods, logging operations (including debug outputs), and within externally accessible configuration files or settings.
SEC-50	After power on, for a given ComID, any IEEE1667 functionality that is different than what is specified by the TCG specifications (e.g., the Command Sequencing Reset differences) shall only take effect if IEEE1667 support is enabled (see G1667-2) and the device receives a Security Send or Security Receive command with the Security Protocol field set to a value of EEh on that ComID only (i.e., IEEE1667). Once the device receives a Security Send or Security Receive command with the Security Protocol field set to a value of EEh on a given ComID, then the device shall behave as

Requirement ID	Description
	specified by the IEEE1667 Specification for that ComID until the next Controller Level Reset when the device shall switch back to TCG-compliant behavior for all ComIDs.
SEC-51	If IEEE1667 support is enabled and the host completes taking ownership of the device (refer to the TCG Storage Application Note: Encrypting Drives Compliant with Opal SSC) via the Security Send/Security Receive commands with the Security Protocol field set to a value of 01h to 06h (i.e., TCG), then the device shall go into a mode where Security Send or Security Receive command with the Security Protocol field set to a value of EEh is prohibited and results in an error status code of Access Denied being returned for any Security Send or Security Receive command with the Security Protocol field set to a EEh. If the device is in the mode where Security Send or Security Receive command with the Security Protocol field set to a value of EEh is prohibited, then a Revert shall cause the device to switch back to a mode where Security Send or Security Receive command with the Security Protocol field set to a value of EEh is allowed.
SEC-52	A FIPS 140 device shall support retrieval of the FIPS 140 compliance descriptor for the active firmware via the Security Receive command with Security Protocol 00h and an SP Specific value of 0002h, as specified in the SFSC (Security Features for SCSI Commands) SCSI standard. For a FIPS 140 validated device, the contents of the FIPS 140 compliance descriptor shall match the FIPS 140 certificate for that FIPS 140 device. This requirement applies to all FIPS 140 devices, independent of whether or not the Cryptographic Module Boundary encompasses the entire physical device (see SEC-47).
SEC-53	For a FIPS 140 device, the FIPS 140 compliance descriptor shall be populated with accurate and complete information reflecting the device's FIPS 140 certification information in devices that are intended for customer qualification (i.e., Qualification Samples), production devices, and any device that has been submitted for FIPS 140 validation (see DCLP-13). For a FIPS 140 device, the FIPS 140 compliance descriptor shall be populated with accurate and complete information reflecting the device's FIPS 140 certification information in any device that is intended to be FIPS 140 validated, but has not yet been submitted for FIPS 140 validation, e.g., Engineering Samples for which the expected contents of the FIPS 140 compliance descriptor are known (see DCLP-13). These requirements override any requirements in the SCSI SFSC standard to only populate the FIPS 140 compliance descriptor for a device that is FIPS 140 validated.

12.2 Secure Boot

The device shall support Secure Boot. There are two fundamental things to address for secure boot:

- Secure boot rooted in hardware.
- Core Root of Trust Measurement.

The vendor should follow the recommendations in the [TCG Hardware Requirements for a Device Identifier Composition Engine](#) and the guidelines in NIST SP 800-193. DICE coupled with [TCG Implicit Identity Based Device Attestation](#) and Source for [RIOT Reference Architecture](#) can help implement Cryptographic Identity with implicit attestation.

Requirement ID	Description
SBT-1	The device shall comply with the FIPS 186-5 Digital Signature Standard (DSS) and relevant NIST standards for PQC Digital Signatures (see SBT-4) and the OCP Hardware Secure Boot v1.0 or later specification. This requirement does not require implementation of the OCP Attestation of System Components specification.
SBT-2	For Core Root of Trust measurement, each device shall have a Cryptographic Device Identity.
SBT-3	The TCG Hardware Requirements for a Device Identifier Composition Engine v1.0 R0.91 or later standard or an alternative hardware based cryptographic identity shall be implemented.
SBT-4	The device shall implement at least one of the Digital Signature PQC algorithms as specified in the Commercial National Security Algorithm Suite 2.0 no later than 2025.
SBT-5	Secure boot flow shall be immutable for exploitation and use immutable public keys.
SBT-6	The next version of this specification will require full implementation of the OCP Secure Firmware Recovery specification.

12.3 DMTF Security Protocol and Data Model (SPDM)

The vendor should follow the guidelines in NIST SP 800-193.

Requirement ID	Description
SPDM-1	The device shall comply with the Security Protocol and Data Model (SPDM) Specification, Version 1.4 or later. The device shall be backwards compatible with the Security Protocol and Data Model (SPDM) Specification, Version 1.1 and later.
SPDM-2	The device shall comply with the revised PCI-SIG Component Measurement and Authentication (CMA-SPDM) ECN that was published on September 20, 2023.
SPDM-3	The device shall support SPDM-1 and SPDM-2 via MCTP over SMBus/I2C.
SPDM-4	The device shall support SPDM-1 and SPDM-2 via MCTP over PCIe VDM.
SPDM-5	The device shall support SPDM-1 and SPDM-2 via PCI-SIG Data Object Exchange (DOE) Revision 1.1.
SPDM-6	Obsolete. See CERT-1 .
SPDM-7	The device shall comply with the Secured Messages using SPDM over MCTP Binding Specification, Version 1.1.1 or later.
SPDM-8	The device shall comply with the Secured Messages using SPDM Specification, Version 1.1.1 or later. Mutual authentication is not required.
SPDM-9	The device shall comply with the Security Protocol and Data Model (SPDM) over MCTP Binding Specification, Version 1.0.2 or later.
SPDM-10	The device shall not drop the response if the device does not receive RESPOND_IF_READY within WT_{Max} amount of time after sending an ERROR message with an ErrorCode equal to ResponseNotReady.

Requirement ID	Description		
SPDM-11	The device shall be ready to respond to SPDM requests within a maximum of 2 second after main power is applied.		
SPDM-12	The device’s SPDM MCTP interpacket delay shall be less than 40 ms.		
SPDM-13	The device shall have a unique and immutable hardware identity based on an asymmetric key pair, and DeviceCert that includes hardware identity information as defined in the SPDM Specification.		
SPDM-14	The device shall support a DataTransferSize of at least 4 KiB.		
SPDM-15	The device shall comply with the SPDM requirements in the following table:		
	Response	Code	Requirement
	DIGESTS	01h	Required
	CERTIFICATE	02h	Required
	CHALLENGE_AUTH	03h	Required
	VERSION	04h	Required
	CHUNK_SEND_ACK	05h	Optional
	CHUNK_RESPONSE	06h	Optional
	MEASUREMENTS	60h	Required
	CAPABILITIES	61h	Required
	SUPPORTED_EVENT_TYPES	62h	Required
	ALGORITHMS	63h	Required
	KEY_EXCHANGE_RSP	64h	Required
	FINISH_RSP	65h	Required
	PSK_EXCHANGE_RSP	66h	Optional
	PSK_FINISH_RSP	67h	Optional
	HEARTBEAT_ACK	68h	Required
	KEY_UPDATE_ACK	69h	Required
	ENCAPSULATED_REQUEST	6Ah	Optional
	ENCAPSULATED_RESPONSE_ACK	6Bh	Optional
	END_SESSION_ACK	6Ch	Required
	CSR	6Dh	Recommended
	SET_CERTIFICATE_RSP	6Eh	Recommended
	MEASUREMENT_EXTENSION_LOG	6Fh	Required
	SUBSCRIBE_EVENT_TYPES_ACK	70h	Required

Requirement ID	Description		
	EVENT_ACK	71h	Required
	VENDOR_DEFINED_RESPONSE	7Eh	Optional
	1) ERROR	7Fh	Required
SPDM-16	The device shall comply with the CHALLENGE_AUTH response requirements in the following table:		
	CHALLENGE_AUTH Response		Requirement
	0h = No Measurement Summary Hash		Required
	1h = TCB Component Measurement Hash		Required
	FFh = All measurements Hash		Required
SPDM-17	Signature endianness shall follow the requirements in Security Protocol and Data Model (SPDM) Specification, Version 1.2.2 or later even in the case that an older SPDM version is supported by the device. For example, on ECDSA signatures, the byte order for r and s shall be big endian order. When placing ECDSA signatures into an SPDM signature field, r shall come first, followed by s.		
SPDM-18	A device that is not ready to accept a new request message shall respond with an ERROR response message with an ErrorCode of Busy (3h) (i.e., the device shall not silently discard the request message). This requirement does not apply while a device is becoming ready to respond to SPDM requests after application of main power (see SPDM-11).		
SPDM-19	If a request is received out of order, then the device shall respond with an ERROR response message with an ErrorCode of RequestResynch (i.e., 43h) for that request and for all subsequent requests until a GET_VERSION command is received and processed (i.e., the device shall not silently discard requests due to an out of order request).		
SPDM-20	The device shall support at least two SPDM banks in order to support both a classical (e.g., RSA, ECDSA) certificate chain and a CNSA 2.0 compliant certificate chain (e.g., ML-DSA-87).		
SPDM-21	For form factors that support I3C, the device shall support SPDM-1 and SPDM-2 via MCTP over I3C.		

12.3.1 SPDM Certificates

Requirement ID	Description
CERT-1	The leaf certificate shall include a Subject Alternative Name certificate extension otherName field using the DMTF OID as defined in the Security Protocol and Data Model (SPDM) Specification with the following settings: - the DMTF-serialNumber shall be set to same value reported in the Serial Number field of the Identify Controller data structure; - the DMTF-product shall be set to same value reported in the Model Number field of the Identify Controller data structure; and

Requirement ID	Description
	the DMTF-manufacturer shall be set to a value reported in the PCI Vendor ID field using the ASCII representation of the hexadecimal value without a leading “0x” or trailing “h”.
CERT-2	The Root CA Trusted Certificate Authority shall be the device vendor and shall be the same across all device models developed by the device vendor.
CERT-3	Device self-signed certificates are prohibited.
CERT-4	The device shall support the AliasCert or DeviceCert model in slot 0. An AliasCert in slot 0 is permitted while running regardless of which version of the SPDM Specification is negotiated (e.g., AliasCert in slot 0 is permitted running in SPDM 1.1 mode).
CERT-5	The AliasCert chain shall contain an immutable hardware identity certificate and hardware identity OID (refer to the SPDM Specification) shall be used to indicate hardware identity certificate(s).
CERT-6	A Mutable certificate OID (refer to the SPDM Specification) shall be used to indicate mutable certificates.

12.3.2 SPDM Firmware Measurements

Requirement ID	Description	
SFM-1	The device shall be able to generate signed measurements (i.e., MEAS_CAP field shall be set to 10b) and shall support the following Measurement block types:	
	DMTFSpecMeasurementValueType	Requirement
	[7] - 0b: Digest, 1b: Raw Bit Stream	Digest Required
	[6:0] = 00h: immutable ROM	Recommended
	[6:0] = 01h: mutable firmware	Required
	[6:0] = 02h: hardware configuration, such as straps, debug modes	Recommended
	[6:0] = 03h: firmware configuration (e.g., configurable firmware policy)	Recommended
	[6:0] = 04h: Measurement manifest	Required
	[6:0] = 05h: Structured representation of debug and device mode	Optional
	[6:0] = 06h: Mutable firmware’s version number	Optional
	[6:0] = 07h: Mutable firmware’s security version number, which should be formatted as an 8-byte unsigned integer	Optional
SFM-2	The device shall always return measurements of the most recently activated firmware and current configuration without requiring a power cycle or any type of NVMe or PCIe reset. Measurements of the activated firmware image are acceptable.	
SFM-3	The device shall report the same measurements blocks and values for all devices in a product family (e.g., devices with the same model but different capacity points, endurance, or form factor).	

Requirement ID	Description
SFM-4	The device vendor shall provide a Reference Integrity Manifest (RIM) for the firmware modules and configuration settings for components using the CoRIM schema as defined by IETF (refer to the latest version of draft-ietf-rats-corim - Concise Reference Integrity Manifest or the RFC (if any) published from that Internet-Draft).
SFM-5	The reference measurements in the CoRIM schema may be expressed using the CoMID tags and/or the CoSWID tags. If the CoRIM has reference measurements from sub-components from different manufacturers, then the reference values of the sub-components shall be captured in CoSWID tags with their individual signatures.
SFM-6	The RIM shall apply to all devices in a product family (e.g., devices with the same model but different capacity points, endurance, or form factor). The RIM shall not include any instance specific information (e.g., any device specific identifiers such as Serial Number, UUID, etc.).
SFM-7	The RIM shall be signed by the device manufacturer using the COSE schema (refer to RFC 9052 - CBOR Object Signing and Encryption (COSE): Structures and Process (ietf.org) and RFC 9053 - CBOR Object Signing and Encryption (COSE): Initial Algorithms (ietf.org)). The device manufacturer shall use an approved digital signature algorithm (see SEC-48).
SFM-8	The device manufacturer shall provide the customer with a digital certificate with the public key that is able to be used to verify the RIM signatures. This digital certificate shall validate (e.g., via direct signature or certificate chain) to the Root CA Trusted Certificate Authority (see CERT-2).
SFM-9	The RIM shall contain the hash values of each firmware module using an approved hashing algorithm (see SEC-48). ASCII text string values in the RIMs are acceptable if the string length is less than 128 bytes and the string is descriptive (e.g., a module identifier string, a product identifier string, or firmware revision string).

12.4 Data Encryption and Eradication

Requirement ID	Description
DATAE-1	Obsolete. Duplicate of SEC-2 .

12.5 TCG Implementation Requirements

Devices that support TCG functionality (i.e., TCG devices) shall implement the specifications in accordance with the additional requirements in this section.

Feature/Parameters		Value	Requirement ID
SSC Feature Descriptor		Opal 2 (0203h)	TCG-FEATURE-1
SID	# of SIDs	1	TCG-FEATURE-1
	TryLimit	10	TCG-AUTH-3
	Persistence	FALSE	TCG-AUTH-5
	Admin authorities	4 (min)	TCG-LOCKING-6

Feature/Parameters		Value	Requirement ID
Number of Locking SP	User authorities	8 (min)	TCG-LOCKING-1 also see TCG-LOCKING-2
Number of Locking Ranges	Global	1	TCG-FEATURE-1
	Additional	8 (min)	TCG-LOCKING-1
DataStore size		10 MiB (min)	TCG-FEATURE-7
MBR Table		Mandatory	TCG-FEATURE-1
Configurable Access Control		Mandatory	TCG-FEATURE-1
Life Cycle support		Mandatory	TCG-FEATURE-1
Repurpose (Revert/ Revert SP)		Mandatory	TCG-FEATURE-1
Shadow MBR		Mandatory (and disabled by default)	TCG-FEATURE-8
Feature Sets	Single User Mode	Mandatory	TCG-FEATURE-2
	PSK Secure Messaging	Strongly Discouraged	TCG-FEATURE-9
	PSID	Mandatory	TCG-FEATURE-1
	Block SID	Mandatory	TCG-FEATURE-1
	Additional Data Store Tables	Mandatory	TCG-FEATURE-7

12.5.1 TCG Version and Features

Requirement ID	Description
TCG-FEATURE-1	TCG devices shall support TCG Storage Security Subsystem Class: Opal Version 2.02, Revision 1.0 or later, and all mandatory feature sets (e.g., Additional DataStore, Block SID Authentication, and PSID feature sets).
TCG-FEATURE-2	TCG devices shall support TCG Single User Mode feature set Version 1.00, Revision 2.00 or later.
TCG-FEATURE-3	TCG devices shall support TCG Configurable Locking for NVMe Namespaces and SCSI LUNs feature set Version 1.02, Revision 1.16 or later with mandatory support for the Namespace Global Range Locking object. The Namespace Non-Global Range Locking object may be supported.
TCG-FEATURE-4	Obsolete, see TCG-FEATURE-1.
TCG-FEATURE-5	The current TCG feature set configuration settings, if any, shall persist through a download and activation of firmware code (e.g., TPer Lock State, Single User Mode configuration, no C_PIN Reset). This is required regardless of the “default setting state” of the new code being downloaded.
TCG-FEATURE-6	The device shall support the Data Removal Mechanism Feature Descriptor (Feature Code 0404h). The Data Removal Time Format bit shall be set to 0 to indicate the Data Removal

Requirement ID	Description
	Time value is stored in (value x 2) seconds. The Data Removal Time shall be less than or equal to 10 seconds per CTO-1 .
TCG-FEATURE-7	The device shall support at least 8 Additional DataStore Tables, each with a minimum size of 128 KiB. The required size of these tables is in addition to the 10 MiB minimum required for the DataStore Table.
TCG-FEATURE-8	The device shall support Shadow MBR functionality and shall disable that functionality by default in the MBRControl Table as specified by the TCG Opal SSC standard (see TCG-FEATURE-1).
TCG-FEATURE-9	The device should not support TCG Opal PSK Secure Messaging.

12.5.2 TCG Communication Layer

Requirement ID	Description
TCG-COMM-1	The device shall support ComID management, and the Level 0 Discovery TPer Feature Descriptor shall report ComID Mgmt supported.
TCG-COMM-2	The device shall support at least 2 Static ComIDs.
TCG-COMM-3	The device should support at least 2 Dynamic ComIDs.
TCG-COMM-4	MaxComIDTime shall be at least 120 seconds.
TCG-COMM-5	MaxComIDTime shall be greater than DefSessionTimeout.

12.5.3 TCG Session Layer

Requirement ID	Description
TCG-SES-1	A single Read-Write Session shall be supported per SP and shall be indicated by MaxSessions. MaxSessions shall indicate the maximum number of simultaneous sessions supported (Read-Write + Read-Only). It is not required to support an active RW session on the AdminSP at the same time as sessions on other SPs, because this would violate the TCG Storage Architecture Core Specification.
TCG-SES-2	At least 2 Read-Only Sessions shall be supported per SP and shall be indicated by MaxReadSessions. SET methods and other TCG commands that modify the TCG configuration state shall be rejected during a Read Only session.
TCG-SES-3	DefSessionTimeout shall be included in the Properties Method response from the device.
TCG-SES-4	The DefSessionTimeout value shall be 90,000 ms.
TCG-SES-5	The MaxSessionTimeout value shall be 0. This value indicates that there is no limit.
TCG-SES-6	The MinSessionTimeout value should be 500 ms.
TCG-SES-7	The SessionTimeout parameter of the StartSession method call shall be used to configure the session timeout.
TCG-SES-8	Support for setting the SPSessionTimeout column of the SPInfo table is recommended.

12.5.4 TCG Transactions

Requirement ID	Description
TCG-TRAN-1	TCG devices shall support TCG Transactions.
TCG-TRAN-2	TCG Nested Transactions may be supported. If TCG Nested Transactions are supported, all supported transactions including any nested transactions shall be reflected in the MaxTransactionLimit property.

12.5.5 TCG Authentication

Requirement ID	Description
TCG-AUTH-1	TCG devices shall enforce a minimum password length (C-PIN PinLength of 16) of 16 bytes for all TCG Opal authorities.
TCG-AUTH-2	TCG devices shall allow a password length (C-PIN PinLength of 32) of at least 32 bytes for all TCG Opal authorities.
TCG-AUTH-3	TCG devices shall set the default TryLimit to 10 for all TCG Opal authorities. The value of the Tries column shall only be cleared to 0 for the mandatory reasons specified in the TCG Storage Architecture Core Specification (e.g., do not clear the Tries column via the Set method, do clear it upon successful authentication or power cycle).
TCG-AUTH-4	Authentication of each C_PIN shall be delayed in order to limit how fast the next authentication of that C_PIN can occur. • The delay shall be at least 100 ms and should not exceed 250 ms and I/O shall not be blocked during this time. • The delay shall apply regardless of whether the authentication is successful. • The device manufacturer shall supply documentation with the implemented delay value. • The time limit should be enforced cryptographically (e.g., by tuning the number of PBKDF iterations to reach the target time).
TCG-AUTH-5	The Persistence column shall be set to false for all C_PIN rows.

12.5.6 TCG Crypto

Requirement ID	Description
TCG-CRYPTO-1	If TCG Opal Locking SP has been activated and the host has supplied at least one authority password, the device shall use at least one authority password as an added source of randomness for its Deterministic Random Number Generator (DRNG). For example, the device may use KDF (PBKDF2) on the user provided locking range password to generate an output of equal length to the required locking range key length plus DRNG seed length. This output can then be utilized in parts, one part as Opal locking range key and the other part as an additional input to the DRNG. If the DRNG implementation does not allow the use of additional input, then an alternative option would be to XOR this output (e.g., from PBKDF2 operation) with initial DRNG seed.

12.5.7 TCG Locking Security Provider

Requirement ID	Description
TCG-LOCKING-1	The number of Additional Locking Ranges supported shall be at least 8 and shall be greater than or equal to the maximum number of NVMe namespaces supported on the device.
TCG-LOCKING-2	The Locking SP of the device shall support at least one User per Locking Range.
TCG-LOCKING-3	The K_AES_256 Table shall be supported.
TCG-LOCKING-4	The K_AES_256 Table's Key columns shall not be readable by the host or be accessible outside the device in any manner.
TCG-LOCKING-5	Any attempt to remove the Power Cycle reset type from a LockOnReset column set value shall be rejected.
TCG-LOCKING-6	The Locking SP of the device shall support at least 4 Admins.

12.5.8 TCG PSID Feature Set

Requirement ID	Description
TCG-PSID-1	The PSID shall not be deterministic, shall comprise at least 160 bits of entropy. The entropy shall be unique for each device. The PSID shall not be derived from any information that is available without physical access to the device. For example, the PSID shall not be the same as the MSID, the PSID shall not be derived from the device serial number or the date of manufacture because these can be read via the device interface or obtained from other documentation. The PSID shall not be the serial number of the drive hashed with a secret string shared with any other device or among all devices, because the entropy shall be unique for each device. The presence of the PSID on the device label does not violate this requirement.
TCG-PSID-2	The PSID shall consist of 32 ASCII characters. The allowed ASCII characters are upper case letters, lower case letters and the digits 0-9. The characters 'I', 'l', 'O' and 'o' (i.e., 49h, 6Ch, 4Fh and 6Fh) and the digits '0' and '1' (i.e., 30h and 31h) shall not be used to limit possible visual confusion.
TCG-PSID-3	The generation method for the PSID shall be documented and provided to the customer.
TCG-PSID-4	After the PSID is provisioned in manufacturing, the PSID shall not be persistently stored in a form that makes retrieval or reconstruction of the PSID by firmware possible, either on the drive or outside the drive (e.g., it is acceptable to store the PSID on the drive hashed via a cryptographic hash or KDF such that the hashed PSID can only be used to verify a PSID input from the host). The presence of the PSID on the device label does not violate this requirement.
TCG-PSID-5	Once manufacturing is complete, the PSID shall not be stored anywhere other than on the physical drive label.

13 Device Profiles

The following are device profiles. This section is intended to be firmware-based configuration settings configured by device vendors when manufacturing a device. A device may be configured with a mix of A and/or B settings. Each customer shall provide their A/B preference for each configuration setting.

The following conventions are used for the Device Profile Table:

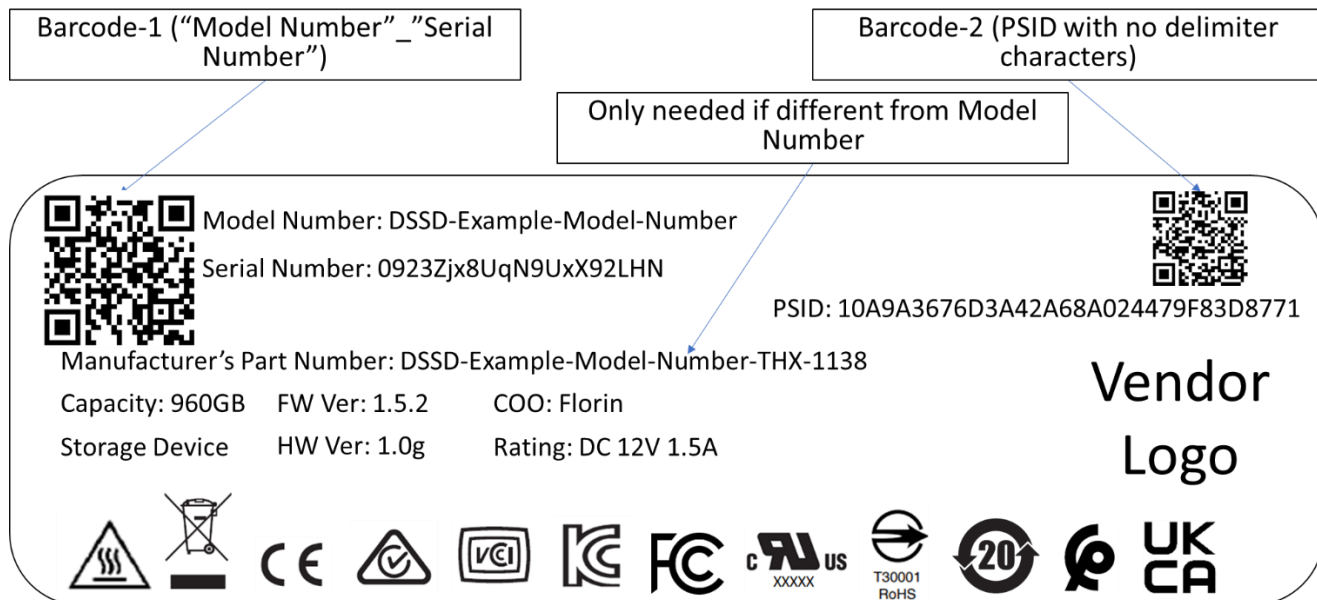
Convention	Definition
R	Required. This shall be supported.
O	Optional. This may be supported.
P	Prohibited. This shall not be supported.

Requirement ID	Description	Configuration Setting	
		A	B
DP-CFG-1	Factory Default Sector Size.	4096-byte	512-byte
DP-CFG-2	Number of Namespaces Supported.	16 Namespaces (see NSM-4)	16 Namespaces per TB (see NSM-5)
DP-CFG-3	Retention Time based on RETC-1 .	1 Month	3 Months
DP-CFG-4	NVMe Basic Management Command Supported.	R	P
DP-CFG-5	Max M.2 top side height.	2.0 mm	3.2 mm
DP-CFG-6	EOL/PLP Failure Mode (Feature Identifier C2h).	Enabled	Disabled (Default specified in ROWTM-1 shall be used)
DP-CFG-7	Write Uncorrectable command support.	O	R
DP-CFG-8	Time-to-Identify-Ready based on TTR-1 .	<= 1 second	<= 10 seconds after a normal shutdown <= 60 seconds after an abrupt shutdown
DP-CFG-9	Time-to-I/O-Ready based on TTR-2 and TTR-22 .	<= 10 seconds (The device shall set CAP.TO to 10 seconds at most.) ²	<= 10 seconds after a normal shutdown <= 60 seconds after an abrupt shutdown (The device shall set CAP.TO to 60 seconds at most.) ²
DP-CFG-10	In addition to the requirements in TTR-4 , the device shall keep CSTS.RDY = 0 until the device is able to service I/O commands and	p ¹	R

Requirement ID	Description	Configuration Setting	
		A	B
	Admin commands that require media access successfully.		
DP-CFG-11	Support for the Lockdown command on the in-band interface. If the Lockdown command is prohibited, then the Lockdown command shall not be supported in-band (e.g., bit 10 of the Optional Admin Command Support field in the Identify Controller data structure shall be cleared to 0b).	R	P
DP-CFG-12	A device that contains 128TB or 256TB (raw NAND capacity) is allowed to list a capacity on the device label that is greater than the minimum capacity values specified in SECTOR-6 .	R	p ³
DP-CFG-13	The device supports the Max PCIe Interface Configuration (Feature Identifier CBh).	R	P
Note(s): 1. This requirement overrides the NVM Express Base Specification requirement to operate in Controller 2. Ready With Media Mode when CAP.CRMS.CRIMS is cleared to 0b as required by NVMe-CFG-20. 3. Shall list the exact values specified in SECTOR-6. If the device cannot meet the required CAP.TO time, then the device shall report the actual value.			

14 Labeling

The following sample label is meant to be used to refer to the label requirements in [Section 14.1 Label Requirements](#). It is not a model label and any markings on it are informative only. See the specifics in [Section 14.1 Label Requirements](#) for actual requirements:



14.1 Label Requirements

Requirement ID	Description				
LABL-1	The following fields are required information that shall be placed on the label:				
	Item	Format	Text Required	Barcode Required	Barcode Type
	Barcode-1	'Model Number' 'Underscore' 'Serial Number' \n.	No	Yes	2d
	Model Number	See LABL-11 (Model Number shall match).	Yes	No	N/A
	Serial Number	See LABL-12 (Serial Number shall match), LABL-15 (certification logos), and LABL-17 (Serial Number format).	Yes	No	N/A
	Manufacturer's Part Number	Number used for ordering.	Yes, if different from Model Number	No	N/A
	Capacity	Number of GB or TB. See SECTOR-5.	Yes	No	N/A
	STORAGE DEVICE	Text shall be "STORAGE DEVICE".	Yes	No	N/A
	PSID	TCG Storage Security Subsystem Class: Opal Specification	Yes	No	N/A

Requirement ID	Description				
	Barcode-2	'PSID' \n	No	Yes	2d
	HW Revision		Yes	No	N/A
	Firmware Name & Revision		No	No	N/A
	Regulatory Mark	See LABL-15 (certification logos).		No	N/A
	Country Certification Numbers	See LABL-15 (certification logos).		No	N/A
	Certification Logos	See LABL-15 (certification logos).		No	N/A
	RoHS/ Green	See LABL-15 (certification logos).		No	N/A
LABL-2	The Model Number on the shipping label shall match the Model Number used during qualification.				
LABL-3	The minimum font size shall be 3 points, and the typical size should be 6 points.				
LABL-4	For the Capacity field, if there are space constraints, the manufacturer may remove "Capacity:" and just show "960GB" or "60TB" for example.				
LABL-5	To distinguish Model Number and Serial Number, Barcode-1 shall have an underscore " _ " between the Model Number portion and the Serial Number portion. Example: Model Number: DSSD-Example-Model-Number Serial Number: 0923Zjx8UqN9UxX92LHN Barcod-1 Readout: DSSD-Example-Model-Number_0923Zjx8UqN9UxX92LHN				
LABL-6	There shall be a line with the text "STORAGE DEVICE".				
LABL-7	The following fields are optional information that can be placed on the label at the discretion of the device maker. Placement is also at the device makers' discretion if such information does not interfere with the mandatory information above. No additional barcode shall be present.				
	Item	Format	Text Required	Barcode Required	Barcode Type
	Processor Code (BA)		Optional	No	N/A
	Maker Logo		Optional	No	N/A
	Rated Voltage & Current		Optional	No	N/A
	Production Date	DDMMYYYY: DD (Date), MM (Month), YYYY (Year)	Optional	No	N/A

Requirement ID	Description				
	Weekly Code	YYWW: YY (Year), WW (Week)	Optional	No	N/A
	Warranty VOID IF REMOVED		Optional	No	N/A
	Makers Own Label Material Number		Optional	No	N/A
	Website, Company Address		Optional	No	N/A
	SSD		Optional	No	N/A
	Product Series Name		Optional	No	N/A
	SA: Value used within manufacturing		Optional	No	N/A
	PBA: Physical Board Address (identifies the physical configuration of the device)		Optional	No	N/A
	WWN: World Wide Number (unique for each device)		Optional	No	N/A
LABL-8	To ensure that datacenter operations personnel can quickly and easily identify devices that have been ticketed for field replacement, it is mandatory to have the proper identifying fields on the label(s), in the format specified in this table.				
LABL-9	The label shall not degrade over the standard SSD lifetime under standard operating conditions.				
LABL-10	For each form factor, the label shall be placed as follows: • M.2: the label shall be placed on the top side of the device as defined in the PCI-SIG M.2 form factor specification. • E1.S: the label shall be placed on the Primary side of the device as defined in the SFF-TA-1006 form factor specification. • E1.L: the label shall be placed on either the Primary or Secondary side of the device as defined in the SFF-TA-1007 form factor specification. • E3: the primary label shall contain the drive information (e.g., model number, serial number, manufacturing info, firmware revision) and be placed on the top label area as defined in the SFF-TA-1008 form factor specification. If more space is needed a label may also be placed on the bottom label area with regulatory marks.				

Requirement ID	Description																								
LABL-11	The Model Number in Barcode-1, the Model Number printed on the label and the Model Number returned in Identify Controller Data Structure (CNS 01h, byte offset 63:24) shall all match unless exempted in writing by the customer.																								
LABL-12	The Serial Number in Barcode-1, the Serial Number printed on the label and the Serial Number returned in Identify Controller Data Structure (CNS 01h, byte offset 23:04) shall all match.																								
LABL-13	The Hardware Revision printed on the label and returned by the nvme-cli utility shall match.																								
LABL-14	All other electronically readable information shall also match their counterparts printed on the label.																								
LABL-15	The following certification logos and their corresponding certifications are required, unless explicitly specified as “Optional” in this table: <table> <tr> <th>Regulatory Mark/Text</th><th>Description</th></tr> <tr> <td>Regulatory Model Number</td><td>Unique regulatory Identifier.</td></tr> <tr> <td>Made in</td><td>Country of Origin.</td></tr> <tr> <td>Manufacturer or Brand name</td><td>Identification of the responsible party for placing the device into the market.</td></tr> <tr> <td>Address of the Manufacturer</td><td>Required for devices with the CE mark or UKCA mark.</td></tr> <tr> <td>Date of Manufacture</td><td>Not needed if embedded in the Serial Number.</td></tr> <tr> <td>Serial Number</td><td>Alpha-Numeric, 12-20 digits.</td></tr> <tr> <td></td><td>[Europe] Compliance with EU WEEE directive 2010/19/EU.</td></tr> <tr> <td></td><td>[Europe] Compliance with EU EMC directive 2014/30/EU and RoHS directive 2011/65/EU.</td></tr> <tr> <td></td><td>[Australia, New Zealand] Compliance with requirements of the relevant Australian ACMA Standards, under the Radiocommunications Act 1992 and the Telecommunications Act 1997.</td></tr> <tr> <td></td><td>[Japan] Compliance with Japan VCCI requirements.</td></tr> <tr> <td></td><td>[Korea] Compliance with requirements of the Radio Research Laboratory Ministry of Information and Communication Republic of Korea.</td></tr> </table>	Regulatory Mark/Text	Description	Regulatory Model Number	Unique regulatory Identifier.	Made in	Country of Origin.	Manufacturer or Brand name	Identification of the responsible party for placing the device into the market.	Address of the Manufacturer	Required for devices with the CE mark or UKCA mark.	Date of Manufacture	Not needed if embedded in the Serial Number.	Serial Number	Alpha-Numeric, 12-20 digits.		[Europe] Compliance with EU WEEE directive 2010/19/EU.		[Europe] Compliance with EU EMC directive 2014/30/EU and RoHS directive 2011/65/EU.		[Australia, New Zealand] Compliance with requirements of the relevant Australian ACMA Standards, under the Radiocommunications Act 1992 and the Telecommunications Act 1997.		[Japan] Compliance with Japan VCCI requirements.		[Korea] Compliance with requirements of the Radio Research Laboratory Ministry of Information and Communication Republic of Korea.
Regulatory Mark/Text	Description																								
Regulatory Model Number	Unique regulatory Identifier.																								
Made in	Country of Origin.																								
Manufacturer or Brand name	Identification of the responsible party for placing the device into the market.																								
Address of the Manufacturer	Required for devices with the CE mark or UKCA mark.																								
Date of Manufacture	Not needed if embedded in the Serial Number.																								
Serial Number	Alpha-Numeric, 12-20 digits.																								
	[Europe] Compliance with EU WEEE directive 2010/19/EU.																								
	[Europe] Compliance with EU EMC directive 2014/30/EU and RoHS directive 2011/65/EU.																								
	[Australia, New Zealand] Compliance with requirements of the relevant Australian ACMA Standards, under the Radiocommunications Act 1992 and the Telecommunications Act 1997.																								
	[Japan] Compliance with Japan VCCI requirements.																								
	[Korea] Compliance with requirements of the Radio Research Laboratory Ministry of Information and Communication Republic of Korea.																								

Requirement ID	Description
	CAN ICES-3(*)/NMB-3(*) [Canada] Compliance with Canada standard ICES 003. Where * is either A or B.
	 [USA] Optional. Compliance with United States Federal Communications Commission requirements.
	 [USA] Compliance with UL standards and Canadian Safety Standards.
	 [Taiwan] Compliance with Taiwan EMC and RoHS.
	 [China] Compliance with Chinese environmental requirements. The number inside the circle is usually 10 or 20.
	 [Morocco] Compliance with Moroccan EMC standards.
	 [United Kingdom] Optional. Compliance with United Kingdom standards. Guidance to UKCA marking.
LABL-16	If the surface of any component or casing will reach a temperature of 70°C (158°F) or greater the following warning logo shall be either printed on the label or placed separately on the device:  In addition, instructional safeguards shall be provided in accordance with IEC 62368-1 3rd Edition or later.
LABL-17	The format of the Serial Number shall have no leading spaces (e.g., 1234567890123456).
LABL-18	The Model Number shall have no leading spaces.
LABL-19	Barcodes shall be printed using Datamatrix ECC200 or Model 2 QR code only.
LABL-20	QR codes shall use a minimum of ECC Level M (15%).
LABL-21	The density of the barcode shall be 10 mil or larger.
LABL-22	The label shall only be printed on Polyester or Plastic labels using a Wax/Resin ribbon.
LABL-23	The PSID shall be printed on the label in its direct 32-character alphanumeric representation without any ancillary delimiting characters (e.g., underscore, dash, backslash, forward slash, etc.) and shall exactly match the readout of Barcode-2 (see the label example at the top of this section).

15 Compliance

15.1 ROHS Compliance

Requirement ID	Description
ROHS-1	The vendor shall provide component-level reporting on the use of listed materials by concentration (ppm) for all homogenous materials.

15.2 ESD Compliance

Requirement ID	Description
ESD-1	Device manufacturer shall provide ESD immunity level (HBM - Human Body Model) measured in accordance with IEC-61000-4-2.

15.3 EMC Compliance

Requirement ID	Description
EMC-1	The device shall comply with the requirements of FCC / EN55032 Class B Radiated Emissions.

16 Shock and Vibration

The shock and vibration specifications for storage devices are in the following table:

Requirement ID	Description
SV-1	The non-operational shock requirement is 700G, half-sine, 0.5 ms, total 6 shocks, along all three axes (+/-).
SV-2	The vibration requirement during operation is: 1.8G _{rms} , 5-500-5 Hz, Random Vibe, 20 min along all three axes.
SV-3	The vibration requirement during non-operation is: 3.13G _{rms} , 5-800-5 Hz, total 6 sweeps along all three axes, 20 minutes per sweep.
SV-4	Validation flow for Shock and Vibration: 1. UUT (Unit Under Test), test fixture should be visually inspected and ensured that everything is torqued or secured as needed. Pictures of test fixture with and w/o UUT should be provided. 2. Baseline performance of device should be gathered and used as a reference against post S&V data to ensure no performance impact incurred. 3. Once S&V testing is completed, repeat visual inspection to the UUT and test fixture to ensure no physical damage or performance impact has occurred to the UUT or test fixture.

Requirement ID	Description
	4. Re-run stress test on the UUT in case of non-op test and provide data indicating no performance impact incurred to the unit.

17 Sustainability Requirements

The following are the sustainability requirements for devices.

Requirement ID	Description
SUS-1	A Life Cycle Assessment (LCA) aligned with ISO 14040 for the device shall be provided to the customer.
SUS-2	Recycled content information per material type shall be provided to the customer.

18 Linux NVMe-CLI Plug-In Requirements

18.1 NVMe-CLI Management Utility

The nvme-cli utility (<https://github.com/linux-nvme/nvme-cli/tree/master/plugins/ocp>) shall be used as one of the management utilities for NVMe devices.

Requirement ID	Description
UTIL-1	The vendor must test their SSDs with this utility and ensure compatibility with their device and functionality supported by OCP plugin for the nvme-cli (version 2.10 or later) (e.g., Format, Secure Erase, Firmware Update, etc.).

18.2 NVMe-CLI Plugin Requirements

Requirement ID	Description
UTIL-PI-1 through UTIL-PI-7	Obsolete. See Section 18.1 NVMe-CLI Management Utility .

18.2.1 NVMe-CLI Plug-In Nomenclature/Functional Requirements

Requirement ID	Description
UTIL-NM-1 through UTIL-NM-10	Obsolete. See Section 18.1 NVMe-CLI Management Utility .

18.2.2 NVMe-CLI Plug-In FW Activation History Requirements

Requirement ID	Description
UTIL-FWHST-1 Through UTIL-FWHST-15	Obsolete. See Section 18.1 NVMe-CLI Management Utility .

19 Revision History

Revision	Date	Release Notes	
1.0	03/16/2020	Initial release based on feedback from the industry.	
1.0a	06/26/2020	Errata.	
2.0	05/18/2021	Additional major features and requirements, including Latency Monitoring, Device Capabilities, Unsupported Requirements, Datacenter SSD Power States, Multiple Namespaces, Sanitize, NVMe-MI, Write Zeroes, Compare, Fused, Write Uncorrectable, Device Profiles, SPDM and additional security requirements, etc.	
2.5	09/22/2023	Additional major features and requirements including Telemetry Data Area 1 & 2, Hardware Component log, FDP, DIX, security requirements, etc.	
2.6	09/11/2024	Errata and other updates in most sections.	
2.7	10/24/2025	Note: The authors have made every attempt to make the lists below complete and accurate on a best effort basis, some changes may have been missed. Reader discretion is advised. List of new requirements:	
		Section/Requirement Change	Summary
		Section 4.4.4 DSSD Asynchronous Events	New section.
		Section 4.9.12 Context Statistic Descriptor	New section.
		Section 4.9.15.2.13 SMBUS/I2C/I3C Debug	New section.
		Section 4.9.15.2.14 MCTP Debug	New section.
		Section 4.15.3.2 Event Injection Recovery Types	New section.
		Section 4.15.3.3 Event Definition Table	New section; events starting with EVTDEF-24 are new to this version.
		Section 4.15.21 Idle Wake Up Time Configuration Set Feature	New feature.
		Section 4.15.22 Idle Wake Up Time Configuration Get Feature	New feature.

Revision	Date	Release Notes	
		Section 4.15.23 Max PCIe Interface Configuration Set Feature	New feature.
		Section 4.15.24 Max PCIe Interface Configuration Get Feature	New feature.
		Section 6.3 DIF Requirements	New section.
		Section 10.9 E2 Form Factor Requirements	New section.
		DCLP-13	New requirement.
		DP-CFG-12	New requirement.
		ERRI-8	New requirement.
		FDPSRG2-1 , FDPSRG2-2	New requirements.
		FFE1S-15 , FFE1S-16	New requirements.
		FFE3-5 , FFE3-6	New requirements.
		FWUP-28	New requirement.
		FWUP-30 to FWUP-32	New requirements.
		GDAEC-3	New requirement.
		GFF-1 , GFF-7 , GFF-8	New requirements.
		LMDATA-38	Log size change.
		LMLOG-15 to LMLOG-18	New requirements.
		MS-CONF-9	New requirement.
		NVMe-AD-29 to NVMe-AD-31	New requirements.
		NVMe-CFG-21 to NVMe-CFG-25	New requirements.
		NVMe-IO-15 to NVMe-IO-18	New requirements.
		NVMe-MI-29 to NVMe-MI-32	New requirements.
		NVMe-OPT-17 to NVMe-OPT-22	New requirements.
		PCI-40 to PCI-42	New requirements.
		SBT-6	New requirement.
		SDAEC-18	New requirement.
		SEC-52 , SEC-53	New requirements.
		SECTOR-6	New requirement.
		SLOG-13 , SLOG-14	New requirements.
		SMART-30 , SMART-40 , SMART-52	New requirements.
		SPDM-20 , SPDM-21	New requirements.

Revision	Date	Release Notes	
		STATI-109 to STATI-114	New requirements.
		STD-LOG-24 to STD-LOG-27	New requirements.
		TCG-FEATURE-8 , TCG-FEATURE-9	New requirements.
		TEL-26	New requirement.
		TELSLG-14	New requirement.
		List of modified requirements:	
		Section/Requirement Change	Summary
		Section 4.8.14 TCG Configuration Log	Expanded field sizes.
		Section 4.15.3 Event Injection	Modified to only allow one event at a time.
		DCLP-11	Modified requirement.
		DP-CFG-9	Modified requirement.
		EREC-AEN-1	Modified Requirement (Obsolete).
		ERRI-1	Modified Requirement.
		ERRI-3	Modified Requirement (Obsolete).
		ERRI-6	Modified Requirement.
		ERRI-7	Modified Requirement (Obsolete).
		ERRIE-1	Modified Requirement.
		ERRIE-3	Modified Requirement.
		ERRIEDP-3	Modified Requirement.
		ERRIEDP-4	Modified Requirement.
		FDPSRG-5	Modified Requirement (Obsolete).
		FDPSRG-7	Modified Requirement.
		FF8639-1	Modified Requirement.
		FFE1L-10	Modified Requirement.
		FFE1S-10	Modified Requirement.
		FWUP-7	Modified Requirement.
		GDAEC-1	Modified Requirement.
		GERRI-2	Modified Requirement.

Revision	Date	Release Notes	
		LABL-15	Modified Requirement.
		LMDATA-1	Modified Requirement (added Bit 3).
		LMDATA-35	Modified Requirement (bumped version).
		LMDATA-37	Modified Requirement.
		LMSF-10	Modified Requirement.
		NVMe-AD-6 to NVMe-AD-8	Modified Requirements.
		NVMe-AD-19	Modified Requirement.
		NVMe-AD-26	Modified Requirement.
		NVMe-CFG-6	Modified Requirement.
		NVMe-MI-11	Modified Requirement.
		NVMe-MI-12	Modified Requirement (Obsolete).
		NVMe-MI-13	Modified Requirement.
		NVMe-MI-24	Modified Requirement.
		NVMe-MI-27	Modified Requirement.
		NVMe-OPT-15	Modified Requirement (Obsolete).
		PCI-5	Modified Requirement.
		PCI-17	Modified Requirement.
		SDAEC-13	Modified Requirement.
		SEC-1	Modified Requirement.
		SEC-3	Modified Requirement.
		SEC-15	Modified Requirement.
		SECTOR-3	Modified Requirement.
		SECTOR-5	Modified Requirement.
		SERRI-14	Modified Requirement.
		SMART-13	Modified Requirement (Minor Version updated).
		SMART-43 to SMART-45	Modified Requirements (fixed byte addresses).
		SMART-47 to SMART-48	Modified Requirements.

Revision	Date	Release Notes	
		SMBUS-1	Modified Requirement.
		SPDM-1	Modified Requirement.
		SPDM-15	Modified Requirement.
		STATF-2	Modified Requirement.
		STATI-31	Modified Requirement.
		TCG-FEATURE-7	Modified Requirement.
		TCGHST-PE-2	Modified Requirement (added Hardware Reset).
		TCGL-21	Modified Requirement (bumped version).
		TCG-SES-1	Modified Requirement.
		TEL-5	Modified Requirement.
		TEL-14	Modified Requirement.
		TRIM-6	Modified Requirement.
		TTR-21	Modified Requirement (Obsolete).
		UBER-1	Modified Requirement.
		UTIL-1	Modified Requirement.

20 META Specific Items

The following items apply specifically to devices delivered to Facebook.

20.1 Configuration Specifics

Requirement ID	Description		
META-CONF-1	NVMe-MI Basic Management - SMBus byte 91 bit 6, Firmware Update Unlocked bit shall be set to 1b by default from the factory.		
META-CONF-2	Devices shall not support Event Injection (Feature Identifier C0h) Set Feature.		
META-CONF-3	Devices shall not support Event Injection (Feature Identifier C0h) Get Feature.		
META-CONF-4	Devices shall not support Error Recovery log page (Log Identifier C1h).		
META-CONF-5	For devices less than 128TB the default power state shall conform to the following table:		
	Form Factor	Capacity	Default Power State Upon Factory Exit
	E1.S 25mm	1 TB	8 (10 W)

Requirement ID	Description		
		2 TB	7 (12 W)
		4 TB	6 (14 W)
		8 TB	5 (16 W)
		16 TB	3 (20 W)
	E1.S 9.5mm	1 TB	9 (8.25 W)
		2 TB	8 (10 W)
		4 TB	6 (14W)
		8 TB	5 (16 W)
		16 TB	3 (20 W)
META-CONF-6	For devices less than 128TB the power state table on the device shall be the following:		
	Power State		Maximum Average Power (MAP)
	0		35 W
	1		30 W
	2		25 W
	3		20 W
	4		18 W
	5		16 W
	6		14 W
	7		12 W
	8		10 W
	9		8.25 W
META-CONF-7	Devices shall be configured to Configuration Setting A as shown in Section 13 Device Profiles .		
META-CONF-8	DIX-1 shall be supported.		
META-CONF-9	FDPSRG-1 to FDPSRG-7 shall be supported with support for 4K, 4K+64 (DIX-1), and 512-byte sector sizes.		
META-CONF-10	For GROWTM-2 the default end of life behavior shall be 11b. It shall be noted that EOL is defined in EOL-4 , EOL-5 and EOL-6 and is not based on the life curve.		
META-CONF-11	The PLP Failure Mode (Feature Identifier C2h) shall set the factory default value of the End-of-Life Behavior to 11b (see SROWTM-13 for additional information).		
META-CONF-12	For 128TB devices the following power states shall be supported.		

Requirement ID	Description	
	Power State	Power (W)
	0	30
	1	22
	2	20 (Default)
	3	18
	4	16
	5	14
	6	12
	7	10
META-CONF-13	For 256TB devices the following power states shall be supported.	
	Power State	Power (W)
	0	40
	1	32
	2	30 (Default)
	3	28
	4	26
	5	24
	6	22
	7	20
	8	18
	9	16
	10	14
	11	12
	12	10
META-CONF-14	For devices 128TB or greater the preferred Indirection Unit (IU) Size 16KB.	
META-CONF-15	For devices 128TB or greater the Maximum Data Transfer Size (MDTS) reported shall be 1 MiB or greater. The reported MDTS value shall not contain the meta data bytes.	

20.2 Performance Requirements

The following numbers are the Meta performance targets for SSDs across all form factors up to 32TB. They are provided to serve as guidance for SSD Vendors. Performance scripts can be found on GitHub at <https://github.com/facebookincubator/FioSynth>. The targets are broken down into the following segments:

Requirement ID	Description
META-PERF-1	FB-FIO Synth Flash Targets (for all capacities).
META-PERF-2	fb-FIOSynthFlash TRIM Rate targets.
META-PERF-3	IO.go benchmark target.
META-PERF-4	Fileappend benchmark target.
META-PERF-5	Sequential write bandwidth.
META-PERF-6	Cache Bench target.
META-PERF-7	All targets shall be achieved by using “none” as the I/O scheduler.
META-PERF-8	Obsolete
META-PERF-9	BootBench Target
META-PERF-10	All tests shall be executed on Kernel 6.11.1 FBK13 or later versions with support for io_uring engine.
META-PERF-11	All performance data shall be provided to Meta based on the following configuration in Figure 1.
META-PERF-12	All SSD Capacities are required to pass all the benchmarks as outlined in the META-PERF section with the following configuration: • User capacity: default OP • Power state: Set to default power state • SSD Configuration: 1xSSD PCIe Config: Max capability (i.e. If the drive is capable of Gen5, then use Gen5.)

Tool	Workload	Job	LBAF	IO Type	IOPS	Bandwidth (MB/s per TB)	Latency (ms)			
							P99	P99.99	P99.9999	Max
FB-FioSynthFlash	HE_Flash_Short_wTRIM_1H25	4K_L2R6DWD_wTRIM	4k	Read	-	74.8	0.3	2	5	5.5
FB-FioSynthFlash	HE_Flash_Short_wTRIM_1H25	4K_L2R6DWD_wTRIM	4k	Write	-	79.2	-	1.5	6	7
FB-FioSynthFlash	HE_Flash_Short_wTRIM_1H25	4K_L2R6DWD_wTRIM	4k	Trim	-	128.7	-	-	-	-
FB-FioSynthFlash	HE_Flash_Short_wTRIM_1H25	4K_L2R9DWD_wTRIM	4k	Read	-	74.8	0.3	2	5	7
FB-FioSynthFlash	HE_Flash_Short_wTRIM_1H25	4K_L2R9DWD_wTRIM	4k	Write	-	102.3	-	2	7	8
FB-FioSynthFlash	HE_Flash_Short_wTRIM_1H25	4K_L2R9DWD_wTRIM	4k	Trim	-	171.6	-	-	-	-
FB-FioSynthFlash	HE_Flash_Short_wTRIM_1H25	MyRocks_Heavy_wTRIM	4k	Read	-	231	1	2.5	4	5
FB-FioSynthFlash	HE_Flash_Short_wTRIM_1H25	MyRocks_Heavy_wTRIM	4k	Write	-	111.1	-	3	5	7
FB-FioSynthFlash	HE_Flash_Short_wTRIM_1H25	MyRocks_Heavy_wTRIM	4k	Trim	-	24.2	-	-	-	-
FB-FioSynthFlash	HE_Flash_Short_wTRIM_1H25	FLeaf_wTRIM	4k	Read	-	352	1	2.5	3.5	5
FB-FioSynthFlash	HE_Flash_Short_wTRIM_1H25	FLeaf_wTRIM	4k	Write	-	95.7	-	2.5	6	6.5
FB-FioSynthFlash	HE_Flash_Short_wTRIM_1H25	FLeaf_wTRIM	4k	Trim	-	97.9	-	-	-	-
FB-FioSynthFlash	Cache_1H25	B_Cache	4k	Read	-	180.4	0.5	2	8	10
FB-FioSynthFlash	Cache_1H25	B_Cache	4k	Write	-	105.6	-	7	10	11
FB-FioSynthFlash	Cache_1H25	B_Cache	4k	Trim	-	-	-	-	-	-
FB-FioSynthFlash	Search_1H25	SearchLM_wTRIM	4k	Read	-	2805	1.5	3	5	9
FB-FioSynthFlash	Search_1H25	SearchLM_wTRIM	4k	Write	-	13.2	-	5	9	10
FB-FioSynthFlash	Search_1H25	SearchLM_wTRIM	4k	Trim	-	143	-	-	-	-
FB-FioSynthFlash	WSCache_1H25	WSCache_1H22	4k	Read	-	236.5	10	15	20	30
FB-FioSynthFlash	WSCache_1H25	WSCache_1H22	4k	Write	-	99	-	50	85	100
FB-FioSynthFlash	WSCache_1H25	WSCache_1H22	4k	Trim	-	-	-	-	-	-
FB-FioSynthFlash	WSF_1H25	wsf-ll-normal	4k	Read	-	85.8	1	5	10	25
FB-FioSynthFlash	WSF_1H25	wsf-ll-normal	4k	Write	-	37.4	-	10	15	25
FB-FioSynthFlash	WSF_1H25	wsf-ll-normal	4k	Trim	-	31.9	-	-	-	-
FB-FioSynthFlash	TrimRate	TrimRate 64M	4k	Trim	See targets in "Trim Rate Targets"					
FB-FioSynthFlash	TrimRate	TrimRate 3G	4k	Trim						
OCP Autoval SSD	IO.go	#N/A	4k	Read	See targets in "IO.go Benchmark Targets"					
OCP Autoval SSD	IO.go	#N/A	4k	Write						
OCP Autoval SSD	IO.go	#N/A	4k	Trim						
OCP Autoval SSD	Fileappend	#N/A	4k	Read	See targets in "Fileappend Benchmark Targets"					
OCP Autoval SSD	Fileappend	#N/A	4k	Write						
OCP Autoval SSD	Fileappend	#N/A	4k	Trim						
FB-FioSynthFlash	HE_Flash_Short_wTRIM_Sweep_1H25	<all>	4k	Read	-	-	-	-	-	35
FB-FioSynthFlash	HE_Flash_Short_wTRIM_Sweep_1H25	<all>	4k	Write	-	-	-	-	-	40
FB-FioSynthFlash	HE_Flash_Short_wTRIM_Sweep_1H25	<all>	4k	Trim	-	-	-	-	-	-
FB-FioSynthFlash	Cache_Sweep_1H25	<all>	4k	Read	-	-	-	-	-	35
FB-FioSynthFlash	Cache_Sweep_1H25	<all>	4k	Write	-	-	-	-	-	40
FB-FioSynthFlash	Cache_Sweep_1H25	<all>	4k	Trim	-	-	-	-	-	-
FB-FioSynthFlash	Search_Sweep_1H25	<all>	4k	Read	-	-	-	-	-	35
FB-FioSynthFlash	Search_Sweep_1H25	<all>	4k	Write	-	-	-	-	-	40
FB-FioSynthFlash	Search_Sweep_1H25	<all>	4k	Trim	-	-	-	-	-	-

Tool	Workload	Job	LBAF	IO Type	IOPS	Bandwidth (MB/s per TB)	Latency (ms)			
							P99	P99.99	P99.9999	Max
FB-FioSynthFlash	UDB_Boot	UDB_BOOT	512	Read	-	-	5	20	-	500
FB-FioSynthFlash	UDB_Boot	UDB_BOOT	512	Write	-	-	100	200	-	400
FB-FioSynthFlash	UDB_Boot	UDB_BOOT	512	Trim	-	-	-	-	-	-
FB-FioSynthFlash	Warmstorage_HXFS_SSD	<all>	512	Read	-	-	5	20	-	500
FB-FioSynthFlash	Warmstorage_HXFS_SSD	<all>	512	Write	-	-	40	100	-	400
FB-FioSynthFlash	Warmstorage_HXFS_SSD	<all>	512	Trim	-	-	-	-	-	-
FB-FioSynthFlash	Twshahred_Pkg_Boot	twshahred-pkg	512	Read	210	51	60	90	-	100
FB-FioSynthFlash	Twshahred_Pkg_Boot	twshahred-pkg	512	Write	600	62	30	60	-	250
FB-FioSynthFlash	Twshahred_Pkg_Boot	twshahred-pkg	512	Trim	-	-	-	-	-	-
FB-FioSynthFlash	Rsw_Cp_wTRIM	rsw_cp_wTRIM	512	Read	119	27	15	30	-	80
FB-FioSynthFlash	Rsw_Cp_wTRIM	rsw_cp_wTRIM	512	Write	700	80	30	60	-	120
FB-FioSynthFlash	Rsw_Cp_wTRIM	rsw_cp_wTRIM	512	Trim	-	60	-	-	-	-
FB-FioSynthFlash	TwI_Iris	twi_iris	512	Read	420	45	10	50	-	150
FB-FioSynthFlash	TwI_Iris	twi_iris	512	Write	65	6	40	200	-	400
FB-FioSynthFlash	TwI_Iris	twi_iris	512	Trim	-	2.4	-	-	-	-
FB-FioSynthFlash	iDyNo_Boot	idyno_boot	512	Read	-	75	25	50	-	90
FB-FioSynthFlash	iDyNo_Boot	idyno_boot	512	Write	-	15	30	45	-	60
FB-FioSynthFlash	iDyNo_Boot	idyno_boot	512	Trim	-	0.1	-	-	-	-
FB-FioSynthFlash	Stacking	stacking	512	Read	-	120	10	50	-	120
FB-FioSynthFlash	Stacking	stacking	512	Write	-	64	0.6	60	-	350
FB-FioSynthFlash	Stacking	stacking	512	Trim	-	18	-	-	-	-
FB-FioSynthFlash	Twshahred_Pkg_Boot_FullSweep	<all>	512	Read	-	-	-	-	-	100
FB-FioSynthFlash	Twshahred_Pkg_Boot_FullSweep	<all>	512	Write	-	-	-	-	-	250
FB-FioSynthFlash	Twshahred_Pkg_Boot_FullSweep	<all>	512	Trim	-	-	-	-	-	-
FB-FioSynthFlash	iDyNo_Boot_FullSweep	<all>	512	Read	-	-	-	-	-	90
FB-FioSynthFlash	iDyNo_Boot_FullSweep	<all>	512	Write	-	-	-	-	-	60
FB-FioSynthFlash	iDyNo_Boot_FullSweep	<all>	512	Trim	-	-	-	-	-	-
FB-FioSynthFlash	BootBench	#N/A	512	Read	See targets in "BootBench Target"					
FB-FioSynthFlash	BootBench	#N/A	512	Write						
FB-FioSynthFlash	BootBench	#N/A	512	Trim						

Note: Search_1H25 Bandwidth is MB/s per drive

Performance Test Drive Configuration

20.3 Trim Rate Targets

- This test measures raw trim performance with no background I/O.
- 64M trim ≥ 50 GiB/s & ≤ 10 ms P99 trim latency.
- 3GB trim ≥ 500 GiB/s & ≤ 10 ms P99 trim latency.

20.4 IO.go Benchmark Targets

- This test measures how long the file system is blocked from writing/overwriting a file while a different file is deleted.
- Less than 4 file sizes total with latency outliers > 10 ms.
- No more than 2 latency outliers per file size.
- No single latency outlier above 15 ms.
- The IO.go targets will be met with XFS, EXT-4 & BTRFS file systems.

20.5 Fileappend Benchmark Targets

- This test measures how long the file system is blocked from appending to a file while a different file is deleted.
- No measurable stalls reported by this tool.
- Max acceptable latency outlier is 10 ms when deleting 1 GiB or 2 GiB file.
- Test should be executed for xfs, ext4 and btrfs file systems.

20.6 Sequential Write Bandwidth

- Full device (all available user capacity, all namespaces) must be written/filled in 180 minutes or less.
- Simple single-threaded sequential write FIO script to fill device.

20.7 CacheBench Targets

- A benchmarking tool that is a supplement for FB FIO Synth Flash tool on measuring performance for cache applications. This is different than the “B Cache” workload in FB FIO Synth Flash.
- Two workloads need to be tested:
 - Graph Cache Leader
 - Kvcache WC
- The final allocator and throughput stats from the benchmark will be used to see if the targets are met.
- Send SSD latency versus time file to Facebook using one of the following methods:
 - Send the raw results log file.
 - Run the “extract_latency.sh script and return the raw results log file, “.tsv” and “.png” files.
- Vendor nvme-cli plugin with “physical NAND bytes written” metric in the SMART / Health Information Extended log page (Log Identifier C0h) needs to be working to get the write amplification.

Workload	Get Rate	Set Rate	Read Latency (us)						Write Amp
			P50	P90	P99	P99.9	P99.99	Max	
Graph Cache Leader	87,000	16,000	100	300	800	N/A	3,000	12,000	1.3
Kvcache WC	3,200	1,500	300	700	2,000	9,000	14,000	15,000	1.4
Workload	Get Rate	Set Rate	Write Latency (us)						Write Amp
			P50	P90	P99		P99.99	P100	
Graph Cache Leader	87,000	16,000	30	50	100	N/A	700	8,000	1.3
Kvcache WC	3,200	1,500	100	200	400	9,000	7,000	8,000	1.4

20.8 BootBench Target

This test measures load on a Boot Device in a stacked environment.

- Download the tool from: github.com/liu-song-6/bootbench.
- Execute ./run.py . FIO 3.20 or newer must be installed as a prerequisite.
- Look at the final_result.txt file for output at the end of the run!

Workload	Read IOPS (sustained)	Overall Result
BootBench	At least 60K	Pass, without any errors.

21 Microsoft Specific Items

The following items apply specifically to Microsoft.

21.1 Configuration Specifics

Requirement ID	Description			
MS-CONF-1	M.2 and E1.S devices shall come from the factory with logical block size formatted per DP-CFG-1 Configuration B, i.e., 512-byte sectors.			
MS-CONF-2	E1.L devices shall come from the factory with logical block size formatted per DP-CFG-1 Configuration A, i.e., 4096-byte sectors.			
MS-CONF-3	Obsolete.			
MS-CONF-4	Obsolete.			
MS-CONF-5	Obsolete.			
MS-CONF-6	For all devices, SMBus byte 91 bit 6, Firmware Update Enabled bit shall be set to 1b (Firmware Update is Enabled) by default from the factory.			
MS-CONF-7	Vendor devices targeting the Microsoft Azure Cloud shall support the configuration A settings for device profile requirements DP-CFG-2 through DP-CFG-13 . Devices shall set the DP-CFG-1 setting on a form factor specific basis per requirements MS-CONF-1 and MS-CONF-2 above.			
MS-CONF-8	The device shall come from the factory supporting the following configuration:			
	<table><tr><th>Requirement ID</th><th>Description</th></tr><tr><td>ROWTM-1</td><td>The device shall default from the factory to 10b for SROWTM-13 which sets the device to transition to Write Through Mode (WTM) in the event of PLP failure and Read Only Mode (ROM) at EOL.</td></tr></table>	Requirement ID	Description	ROWTM-1
Requirement ID	Description			
ROWTM-1	The device shall default from the factory to 10b for SROWTM-13 which sets the device to transition to Write Through Mode (WTM) in the event of PLP failure and Read Only Mode (ROM) at EOL.			
MS-CONF-9	The device shall meet the TRIM Rate requirements specified in META-PERF-2.			

22 Latency Monitoring Feature Set Theory of Operation

22.1 Overview

Latency outliers are very undesirable in the data center. The goal of this feature is to allow production monitoring of SSD QOS outliers and to debug outlier issues in production. This feature will allow vendors and hyperscale companies to clearly understand if the outliers are caused by the SSD or other components in the Host system. This feature enables vendors to effectively debug latency issues efficiently. This feature will enable predicting when latency outliers are growing and likely to impact hyperscale customers. This feature enables many use cases involving understanding and debugging latency issues at scale in a production environment.

22.2 Functional Operation

Latency Monitoring Feature Description

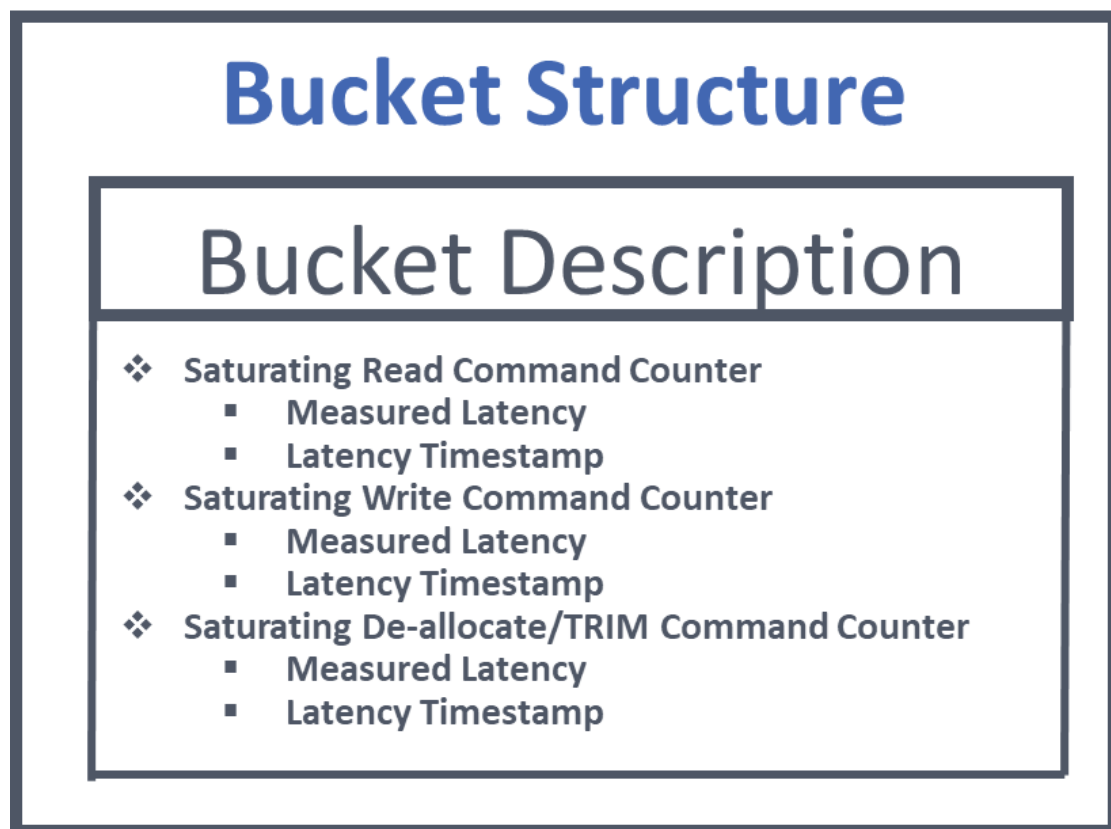
Following is the high-level theory of operation describing how the Latency Monitoring feature works. The latency of an individual command shall be measured from the time a controller fetches the command from the SQ to the time when controller writes the CQ entry for the SQ entry it fetched.

22.2.1 Bucket Description Overview

There are two types of buckets Active Buckets and Static Buckets. Active Buckets are buckets that are updated in real time. Static Buckets are buckets which are loaded with snapshots from the Active Buckets. This is a move from the Active Buckets to the Static Buckets, thus the old values in the Static Buckets are discarded. The Static Buckets allow hyperscale users to sample the Static Buckets over a fixed time period to gather statistics.

22.2.2 Active Bucket Description

The high-level concept is to create 4 real time buckets groups of active latency tracking command counters. Each bucket will count latency events which exceed a configured latency threshold. A description of each bucket is in the following figure:



Each bucket contains the following:

- Saturating Read Command Counter with an associated Measured Latency and Latency Timestamp.
- Saturating Write Command Counter with an associated Measured Latency and Latency Timestamp.
- Saturating Deallocate/TRIM Command Counter with an associated Measured Latency and Latency Timestamp.

For clarity, the opcode to Counter mapping is in the following table:

Bucket Counter	Opcode	Command
Read Command Counter	02h	Read
Write Command Counter	01h	Write

Bucket Counter	Opcode	Command
Deallocate/TRIM Command Counter	09h with Attribute – Deallocate (AD) = 1	Dataset Management

In addition to the command counters there is a Measured Latency data structure, and a Latency Timestamp data structure associated with each command counter. The Measured Latency and Latency Timestamp have a direct relationship such that both are updated, or neither are updated. The Measured Latency and Latency Timestamp will be described later in this document.

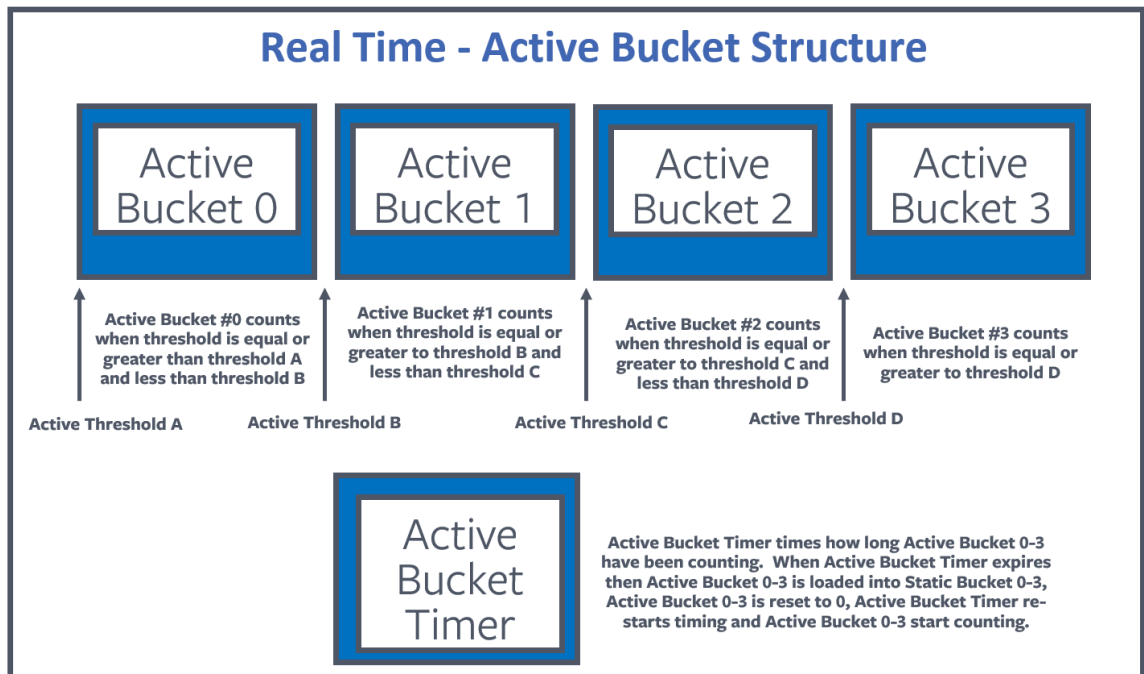
22.2.3.1 Active Command Counter Behavior

The active command counters count Read commands, Write commands, and Deallocate/TRIM commands which exceed a configured latency threshold. These active command counters count until the command counter saturates or the Active Bucket Timer expires. The behavior for each of these events is as follows:

- Active Command Counter Saturation:
 - If the Command Counter saturates, the counter shall maintain the active value and not wrap.
- Active Bucket Timer Expiration:
 - If the Active Bucket Timer Expires, then the following occurs:
- The Active Bucket Command Counter values and associated information are moved into Static Bucket Command Counters; the Active Bucket Command Counters are then cleared to zero and re-start counting.
- The active command counters shall count regardless of how the Active Latency Minimum Window is configured.

22.2.3.2 Active Bucket Thresholds

There are multiple Active Command Counter Buckets. The configured latency thresholds determine which Bucket the command counter shall be incremented in. The following figure shows how there are multiple Buckets and thresholds for each Bucket:



If the Read, Write, Deallocate/TRIM command completion time is below Threshold A then no counter is incremented. If the threshold is equal or greater than A and less than B, then the corresponding command counter in Active Bucket 0 increments. If it is equal to or greater than B and less than threshold C, then the corresponding command counter in Active Bucket 1 increments. If it is equal to or greater than C and less than threshold D, then the corresponding command counter in Active Bucket 2 increments. If it is equal to or greater than threshold D, then the corresponding command counter in Active Bucket 3 increments. By following this process all latencies greater than threshold A are counted for Read, Write and Deallocate/TRIM commands. When configuring the Latency Monitor Feature the thresholds shall always be configured such that Active Threshold A < Active Threshold B < Active Threshold C < Active Threshold D.

22.2.3.3 Active Bucket Timer Behavior

The Active Bucket Timer times how long the Bucket Command Counters have been counting. When the Active Bucket Timer is equal to the Active Bucket Timer Threshold then the following operations shall occur:

- The following data is moved:
 - Active Bucket Counters 0 - 3 are moved to Static Bucket Counters 0 - 3.
 - Active Latency Timestamps are moved to Static Latency Timestamps.
 - Active Measured Latencies are moved to Static Measured Latencies.
 - Active Latency Timestamp Units are moved to Static Latency Timestamp Units.
- The Active Bucket items shall then be updated as follows:
 - Active Bucket Counters 0 - 3 are cleared to zero.
 - Active Latency Timestamps are set to invalid (FFFF_FFFF_FFFF_FFFFh).
 - Active Measured Latencies are cleared to zero.
 - Active Latency Timestamp Units are cleared to zero.
 - The Active Latency Minimum Window, if it is running, may be reset or continue to count.
 - Active Bucket Timer is cleared to zero and starts the process of counting over.

- When looking at the data structures in the Latency Monitor log page (Log Identifier C3h) it should be noted that the data in item #1 and #2 above is 16-byte aligned, and the data can be moved simply by doing a data move of the entire data structure.

22.2.3.4 Active Latency Timestamp Format

The format of the Latency Timestamp follows the Timestamp data structure which is defined in the NVM Express Base Specification. The Latency Timestamp allows an understanding of where a latency excursion occurred in terms of wall clock time. The Latency Timestamp time reported shall be based on CQ completion.

If the device receives a Timestamp Set Features (Feature Identifier 0Eh), then the device shall use this baseline wall clock time plus the time in milliseconds since the Timestamp was set to determine the Latency Timestamp of the latency event. If the device receives multiple Timestamp Set Features (Feature Identifier 0Eh) the most recent Timestamp shall be used as the baseline.

If the device does not receive Set Features with a Timestamp, then the Latency Timestamp shall be generated based on Power on Hours.

If the device receives a Set Features with a Timestamp and then the device is powered off. When the device is powered on it shall use the most recent Timestamp it received even if this Timestamp was from before the device was powered off.

The Active Latency Timestamp Units shall be populated when the Latency Timestamp is updated to indicate if the Latency Timestamp used Timestamp with Power on Hours to generate the Latency Timestamp or if only Power on Hours were used to generate the Latency Timestamp.

22.2.3.5 Active Measured Latency and Active Latency Timestamp Updates

The Active Measured Latency is the latency measured from fetching the command in the SQ to updating the CQ. The Active Measured Latency data structure and the Active Latency Timestamp data structure shall be updated atomically. They shall not update independently. Each Command Counter (Read/Write/Deallocate) has an Active Measured Latency, and an Active Latency Timestamp structure associated with it. The Active Latency Configuration is used to configure this feature.

When the Latency Mode in the Active Latency Configuration is cleared to zero then the following behavior shall be followed:

- The Active Measured Latency and Active Latency Timestamp will be loaded the first time the command counter associated with it increments.
- The Active Measured Latency and Active Latency Timestamp will not be loaded again until the Active Measured Latency is reset.

If the Latency Mode is set to 0001h in the Active Latency Configuration, then every time the associated command counter is incremented the Active Measured Latency will report the largest measured latency based on the associated command counter. The Active Latency Timestamp will report the time when the largest latency occurred.

The Active Latency Minimum window also affects when the Active Measured Latency and the Active Latency Timestamp are updated. This is described in the section on Active Latency Minimum Window.

22.2.3.6 Active Latency Minimum Window

This affects both the Active Measured Latency and the Active Latency Timestamp. This defines the minimum time between updating the Active Measured Latency and the Active Latency Timestamp for a single Active Bucket/Counter combination. The feature is only used if the Active Latency Mode is set to 0001h.

If the Active Latency Minimum Window timer is running and the Measured Latency and Latency Timestamp have been updated, then the Latency Timestamp and Active Measured Latency will not be updated again until the Active Latency Minimum Window timer has expired. Some examples of this are as follows:

Example 1:

Assume:

- Active Latency Minimum Window of 5 seconds.
- Latency Mode is Configured for Largest Latency.
- Bucket 2 has a threshold range of 40 ms to 400 ms.

Time in seconds	Read Counter Bucket 2 Latency Event	Active Read Counter Bucket 2 Value	Actual Latency	Active Measured Latency	Latency Stamp	Comment
0	N	0	-	-	FFFF_FFFF_FFFF_FFFFh	Actual Latency and Active Measured latency are invalid.
0.5	Y	1	50 ms	50 ms	0.5 Seconds	First Latency Event. This starts the Active Latency Minimum window. New latency events will not be recorded until the 5 second Active Minimum Window expires at 5.5 seconds.
5.25	Y	2	100 ms	50 ms	0.5 Seconds	Measured Latency and Latency Timestamp is not updated due to Minimum Window is not expired; however, the Active Read Counter is updated.
6	Y	3	75 ms	75 ms	6 Seconds	Minimum Window is expired and 75ms is greater than the previous number of 50ms, so the Active Measured Latency and Latency Timestamp are updated.

Example 2:

Assume:

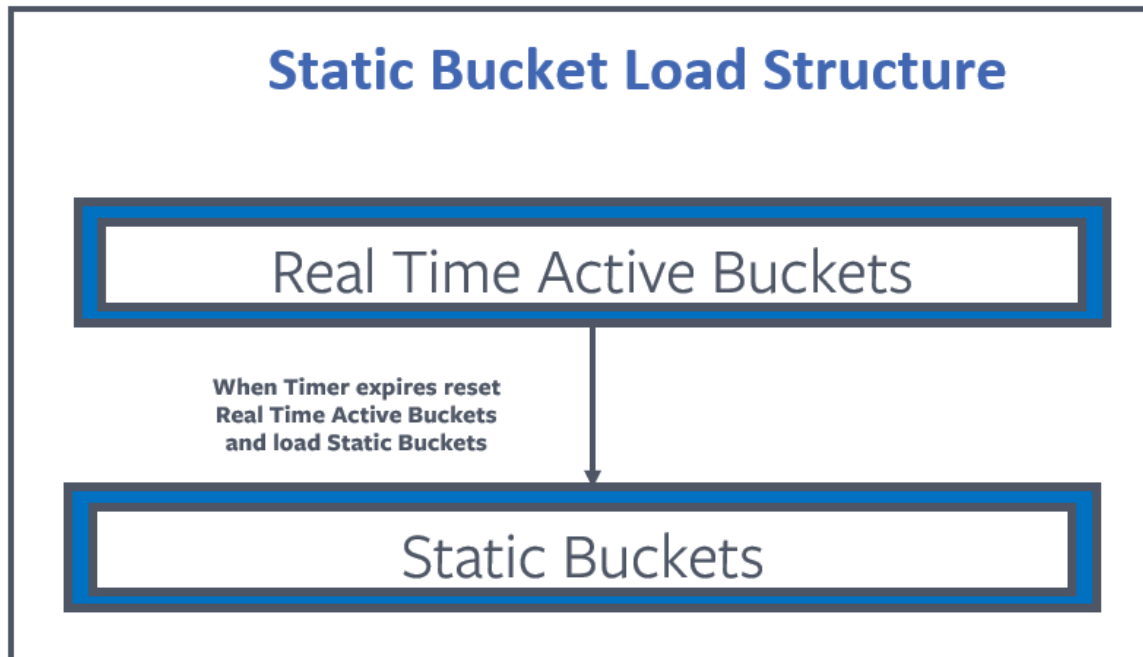
- Active Latency Minimum Window of 5 seconds.
- Latency Mode is Configured for First Latency Event.
- Bucket 2 has a threshold range of 40 ms to 400 ms.

Time in seconds	Read Counter Bucket 2 Latency Event	Active Read Counter Bucket 2 Value	Actual Latency	Active Measured Latency	Latency Stamp	Comment
0	N	0	-	-	FFFF_FFFF_FFFF_FFFFh	Actual Latency and Active Measured latency are invalid.
0.5	Y	1	150 ms	150 ms	0.5 Seconds	First Latency Event.
10	Y	2	200 ms	150 ms	0.5 Seconds	Since the device is in First Latency Event mode, no additional events are recorded.
15	Y	3	75 ms	150 ms	0.5 Seconds	Since the device is in First Latency Event mode, no additional events are recorded.

The Active Latency Minimum Window acts as a filter to ensure there are not a large number of events to update the Active Measured Latency and the Latency Timestamp. Thus, if the queue depth is 128 commands deep and there is a latency event, then there are not 128 updates to these data structures. Rather the first event is recorded, and the rest of the events are filtered out. It should be noted that the Active Latency Window is not enforced across power cycles. Thus, after a power cycle the Active Latency Window shall not start until a Bucket Counter is incremented.

22.2.3.7 Static Bucket Description

In addition to the real-time buckets there are static buckets. When the Active Bucket Timer reaches its configured threshold (Active Bucket Timer Threshold) the active real time buckets shall be loaded into the static buckets and the active real time buckets shall be reset and start counting from 0. The following figure describes this:



22.3 Persistence Across Power Cycles

When either a safe or unsafe power transition happens the counters and associated Latency Monitoring Information shall be saved such that they can be restored on the next power up transition and continue from where the power cycle left off. There are additional details about this in the C.5 Latency Monitoring Feature - Challenging Event Handling section.

22.4 Debug Logs

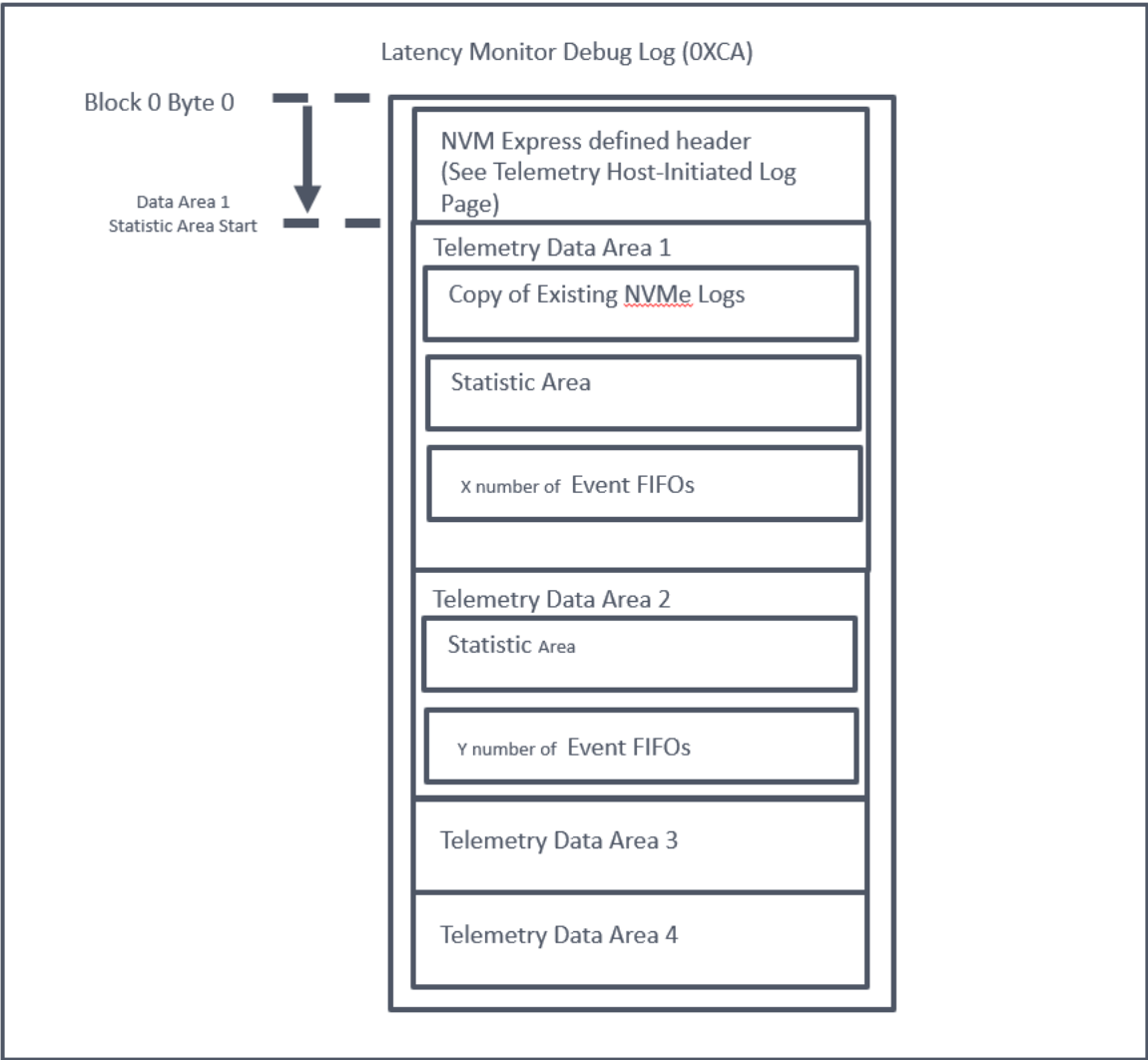
The Latency Monitoring Feature can also enable debug logs to trigger. The Debug Log Trigger Enable configures which counters shall trigger a debug log the first time the Bucket/Counter combination is incremented. Only a single debug log shall be generated. Once a Latency Monitor debug log is generated, until the Latency Monitor debug log is discarded another Latency Monitor debug log cannot be generated.

If the Host Initiated Telemetry format supported bit is cleared to 0b then the host is able to discard the Latency Monitor debug log by using Set Features for the Latency Monitor or by reading the Latency Monitor Debug Log. If the Host Initiated Telemetry format supported bit is set to 1b then the host is only able to discard the Latency Monitor debug log by using Set Features for the Latency Monitor. Reading the Latency Monitor Debug Log does not clear the log.

The Set Features for the Latency Monitor has two mechanisms for discarding the Debug Log. One method discards the debug log and resets the Latency Monitor feature to a new set of configured values based on the fields in Set Features. The other method discards the Debug Log and has no effect on any of the other features associated with the Latency Monitor Feature. Thus, the Latency Monitor Feature will keep running undisturbed when the Debug Log is discarded.

When the Latency Monitor debug log trigger event happens, the following data shall be captured: Debug Log Measured Latency, Debug Log Latency Timestamp, Debug Log Trigger Source, Debug Log Timestamp Units, Debug Log Pointer as well as internal information required to debug the issue to root cause.

When the Host Initiated Telemetry format supported bit is set to 1b then the format of the Latency Monitor shall follow the Host and Controller Initiated Log format.



22.5 Latency Monitoring Feature - Event Handling

22.5.1 Power Off/On When Latency Monitoring Feature is Enabled

When powering off, the Active Bucket Information (Counters, Measured Latency, Latency Timestamp, Active Bucket Timer) may be slightly off due to concerns with flushing data with unsafe power down. The Active Bucket Information shall maintain coherency compared to itself when flushing data with unsafe power down. When the device powers back on the Latency Monitoring Feature shall restore the Active/Static Bucket/Debug Information including loading the Active Bucket Counter. Once the restoration is complete then the device shall resume the Latency Monitor functionality. The device shall start capturing latency data within 2 minutes of power on. Thus, commands for the first 2 minutes may not be monitored. The Active Latency Window is not enforced across power cycles. Thus, after a power cycle the Active Latency Window shall not start until a Bucket Counter is incremented.

22.5.2 Latency Monitoring Feature Persistence

The Latency Monitoring Feature disabled/enabled state shall be persistent across all resets and power cycles. When the Latency Monitor Feature is enabled the associated Latency Monitor configuration information in the Latency Monitor log page shall persist across all resets and power cycles.

22.5.3 Moving Information from Active to Static Buckets

When moving data from the active buckets to static buckets it can be challenging to track all the information. The Active counter shall restart counting no longer than 3 seconds from moving data from Active to Static Counters.

22.5.4 Firmware Update

When activating new firmware, if the Latency Monitoring Feature is enabled, the firmware activation shall reset the Latency Monitoring Feature just as if a Set Features command to enable the feature was received. The Latency Monitoring Log shall start updating properly within 2 minutes of firmware activation completing. Thus, there are command latencies which could be missed after initially activating new firmware.

22.6 Configuring Latency Monitoring

The Set Features command is used to configure this feature. When the Set Features command is used to configure this feature all the data structures in both the Active and Static Buckets are reset. The debug log and related debug information is reset based on the Discard Debug Log Field.

23 OCP Tenants

OCP Tenant	Description
Efficiency	Enables common design that can be used across multiple end users which reduces the number of SKU's.
Scaleability	Simpler design allows for scale, manageability and reliability.
Openness	Provides an open specification for datacenter SSD requirements.
Impact	This contribution provides the community a public SSD specification for SSD users and providers to focus on. Enables a more robust supply chain and increased quality. Enabling the eco-system to have an open component specification thus enabling innovation.
Sustainability	Sustainability requirements are contained in specification (LCA aligned to ISO 14040 and recycled content information)

24 Acknowledgements

We recognize and thank the contributions of former authors in the development of current and previous versions of this specification:

Name	Company
Austin Bolen	Dell Technologies
David Derosa	HPE
William Lynn	Dell Technologies