

Sanitize Device Command

May ~~11~~13, 2009

Revision ~~6~~7

Technical Editor:

John Geldman
47300 Bayside Parkway
Fremont, CA 94538 USA
(510) 580-8715
jgeldman@lexar.com

Document Status

Revision History		
Rev	Date	Description
0	November 10, 2007	Initial draft
1	June 10, 2008	Initial draft in proposal form, presented in June 2008 Plenary
2	October 20, 2008	Clarified need to re-install file-system artifacts, reformed normal and error status, added hour/minutes/seconds unit choice for estimated time report (Incorporating feedback from June 2008 Plenary)
3	December 16, 2008	Much feedback from Oct 2008 Plenary, including command separation, Block Erase, Overwrite with pattern. Also added Sanitize Freeze lock and rewrote in the form of SMART
4	December 20, 2008	Clarified wording of the intent of Sanitization Operation (focus on the previously written contents), cleaned up lists, cleaned up output error lists, explicitly affected hidden areas and moved existing overview content to a feature set description
5	March 4, 2009	Replaced "Sanitize Prepare" two-step execution with signatures in additional fields: DWORD LBA signature to most operation commands (WORD for the OVERWRITE operation) and a 3-bit signature to the DEVICE field; specified required behavior to exit Sanitize Operation state, added new state diagram text description; added User Data Area definition; added ASC/ASCQ's and many editing clean-ups (non-technical related)
6	May 11, 2009	Extensive clarifications from Plenary (including state machine change to add additional completion states and explicitly call out hardware reset)
<u>7</u>	<u>May 13, 2009</u>	Editorial changes and State Machine label changes from May 13th Telecon

1. Introduction

There is a desire in the CF community to support a command (that is unrelated to SCT and to ATA security support) to sanitize (i.e., remove all visible and obscured) user data from a device. This command is intended to attempt to heroically sanitize all user data areas, included areas marked bad, spare or unallocated.

This command has several optional methods to allow a range of Sanitize quality (how much science & resources an attacker would need to recover user data) and the completion percentage of an ongoing Sanitize operation.

This command is intended to be independent of the type of media (rotating/solid-state/...) and to provide multiple options for the method used to sanitize the data (block erase, multiple overwrite, and cryptographic).

This command incorporates a command to fire the operation, as well as a status mechanism to discover supported sanitization methods, and to monitor operation progress.

This command also requires a new state machine that disables other commands until the sanitize operation is complete. This implies a non-volatile state machine that completes sanitization across power cycles.

2. Scope

This new feature is intended for inclusion in ACS-2.

3. Overview

There are two steps to complete a Sanitize operation.

1. [ExecuteProcess](#) a specific SANITIZE OPERATION START EXT command
2. Poll for status (note: time completion estimate available in status)

Sanitize Command capability identification

Capability Identification is performed by the host issuing an IDENTIFY DEVICE command to determine if the Sanitize command supported and which Sanitize Codes are supported.

Sanitize operations shall write over a hidden partition when hidden partitions are [enabled/available](#) using the Host Protected Area feature set. Automatic sector reassignment is permitted during the operation of this function.

4. Changes to ACS-2

4.1. Changes to Clause 2.4 (Other references)

Open NAND Flash Initiative Specification (ONFI)

For the Open NAND Flash Initiative Specification, contact them at <http://www.onfi.org>

<Editor's Note: add ONFI to Acronym list>

4.2. Changes to Clause 3.1 (Definitions and abbreviations)

Block Erase: A media operation supported by some media which sets a block of data to a vendor specific value, (replacing previous data), and may precondition the data for write operations (e.g. a block erase operation for FLASH memory (see ONFI)).

user data: <Editors Note: Already edited into ACS-2>

user data area:

~~Any area of the device's media that stores user data, which is addressable by the host from LBA 0 to the maximum of native max address, and DEVICE CONFIGURATION IDENTIFY data words 3..6. Any area of the device's media that is available to store user data, which can be addressed by the host from LBA 0 to the maximum of IDENTIFY DEVICE data words 100..103, native max address, IDENTIFY DEVICE data words 60..61, and DEVICE CONFIGURATION IDENTIFY data words 3..6.~~

~~<Editor's Note: Changed definition to include areas that aren't currently addressable, such as currently unallocated or spare physical sectors>~~

4.3. Changes to Clause 4 (Feature Set Definitions)

Add the Sanitize Device feature set to Table 15, Preserved Feature Sets and Settings

4.x Sanitize Device Feature Set

This SANITIZE DEVICE operation shall use one of the methods defined in this clause to make all previously written content in the user data area of the device unretrievable and shall only affect the following:

- a. user data areas;
- b. user data areas that are not currently allocated; and
- c. user data ~~held in~~ caches.

~~Note — Sanitize operations shall affect a hidden partition when hidden partitions are enabled using the Host Protected Area feature set.~~

Automatic sector reassignment is permitted during the operation of this function. A SANITIZE DEVICE operation shall return an Error if physical sectors that are ~~enabled-available~~ to be allocated for user data (i.e. allocated or unallocated physical sectors allowed by vendor-specific means to be usable for user data) were not successfully sanitized. ~~<Editor's Note: Note clarification of previous sentence>~~

To perform a SANITIZE DEVICE operation the host should issue:

- (1) one of the SANITIZE OPERATION START EXT commands; and
- (2) a SANITIZE STATUS EXT to check for completion.

After a device has started processing a SANITIZE DEVICE operation the device shall abort all commands other than IDENTIFY DRIVE, REQUEST SENSE and SANITIZE STATUS EXT. If a SANITIZE DEVICE operation is interrupted by a power cycle, the SANITIZE DEVICE operation shall continue to completion before reporting ready.

The SANITIZE STATUS EXT command returns information about the current sanitize operation, if any, and a percentage of completion if a sanitize operation is in progress.

An accepted SANITIZE DEVICE operation start command shall transition the device into the Sanitize Operation state. The device shall remain in this state until the device has responded to a SANITIZE STATUS EXT command with the Sanitize operation complete bit set to one and the Error bit cleared to zero (see Figure xx). ~~<Editor's Note: or Table xy?>~~

The SANITIZE FREEZE LOCK EXT command shall cause the device to transition to the Sanitize Frozen state and shall cause any subsequent SANITIZE OPERATION START EXT commands to be aborted. When the device processes a power on reset or a hardware reset, the device shall transition to the Sanitize Idle state.

A device implementing this feature set shall implement one or more of the following sanitization methods:

- a. Cryptographic Scramble;
- b. Block Erase; or
- c. Overwrite

The CRYPTOGRAPHIC SCRAMBLE method and BLOCK ERASE method make previously written contents in the user data area unretrievable.

The OVERWRITE method fills all user data with a four byte pattern passed within the LBA field of the command. Parameters for this method include a count for multiple overwrites and the option to invert the four byte pattern between consecutive overwrite passes.

Figure xx and the text in this subclause describe the operation of the Sanitize Device Feature set.

SD0: Sanitize Idle State: This state is entered when the device ~~executes a power cycle~~processes a power-on reset from SD0, SD1 or SD4.

Transition SD0a:SD0: When the device is in the Sanitize Idle state and it receives a hardware reset or power-on reset, the device shall remain in the SD0 Sanitize Idle state.

Transition SD0b:SD0: When the device is in the Sanitize Idle state and it receives a SANITIZE STATUS command, the device shall complete the command and remain in the SD0 Sanitize Idle state.

Transition SD0:SD1: When the device is in the Sanitize Idle state and it receives a SANITIZE FREEZE LOCK EXT command, the device shall transition to the SD1 Sanitize Frozen state.

Transition SD0:SD2: When the device is in the Sanitize Idle state and it receives a supported SANITIZE OPERATION START command, the device shall transition to the SD2 Sanitize Operation state.

SD1: Sanitize Frozen State: This state is entered from the SD0 Sanitize Idle state when the device receives a SANITIZE FREEZE LOCK EXT command.

Transition SD1:SD0: When the device is in the Sanitize Frozen state and it receives a hardware reset [or power-on reset](#), the device shall transition to the SD0 Sanitize Idle state.

Transition SD1:SD1: When the device is in the Sanitize Frozen state and it receives a SANITIZE STATUS EXT command, the device shall complete the command and remain in the SD1 Sanitize Frozen state.

SD2: Sanitize Operation State: This state is entered when:

- a) the device ~~processes a power-on reset executes a power cycle~~ from SD2; ~~;~~ or
- b) the device is in the SD0 Sanitize Idle state and a supported SANITIZE OPERATION START command is received.

Transition SD2a:SD2: When the device is in the Sanitize Operation state and it receives a hardware reset [or power-on reset](#), the device shall remain in the SD2 Sanitize Operation state.

Transition SD2b:SD2: When the device is in the Sanitize Operation state and it receives a SANITIZE STATUS EXT command, the device shall remain in the SD2 Sanitize Operation state.

Transition SD2:SD3: When the device is in the Sanitize Operation state and a Sanitize Operation completes with an error, the device shall transition to the SD3 Sanitize Operation Failed state.

Transition SD2:SD4: When the device is in the Sanitize Operation state and a Sanitize Operation completes without an error, the device shall transition to the SD4 Sanitize Operation Succeeded state.

SD3: Sanitize Operation Failed State: This state is entered when:

- a) the device ~~processes a power-on reset executes a power cycle~~ from SD3; ~~;~~ or
- b) the device is in the SD2 Sanitize Operation state and a Sanitize Operation completes with an error.

Transition SD3a:SD3: When the device is in the Sanitize Operation state and it receives a hardware reset [or power-on reset](#), the device shall remain in the SD3 Sanitize Operation state.

Transition SD3b:SD2: When the device is in the Sanitize Operation state and it receives a SANITIZE STATUS EXT command, the device shall remain in the SD2 Sanitize Operation state.

Transition SD3:SD2: When the device is in the Sanitize Operation state and it receives a supported SANITIZE OPERATION START command, the device shall transition to the SD2 Sanitize Operation state.

SD4: Sanitize Operation Succeeded State: This state is entered when the device is in the SD2 Sanitize Operation state and a Sanitize Operation completes without an error.

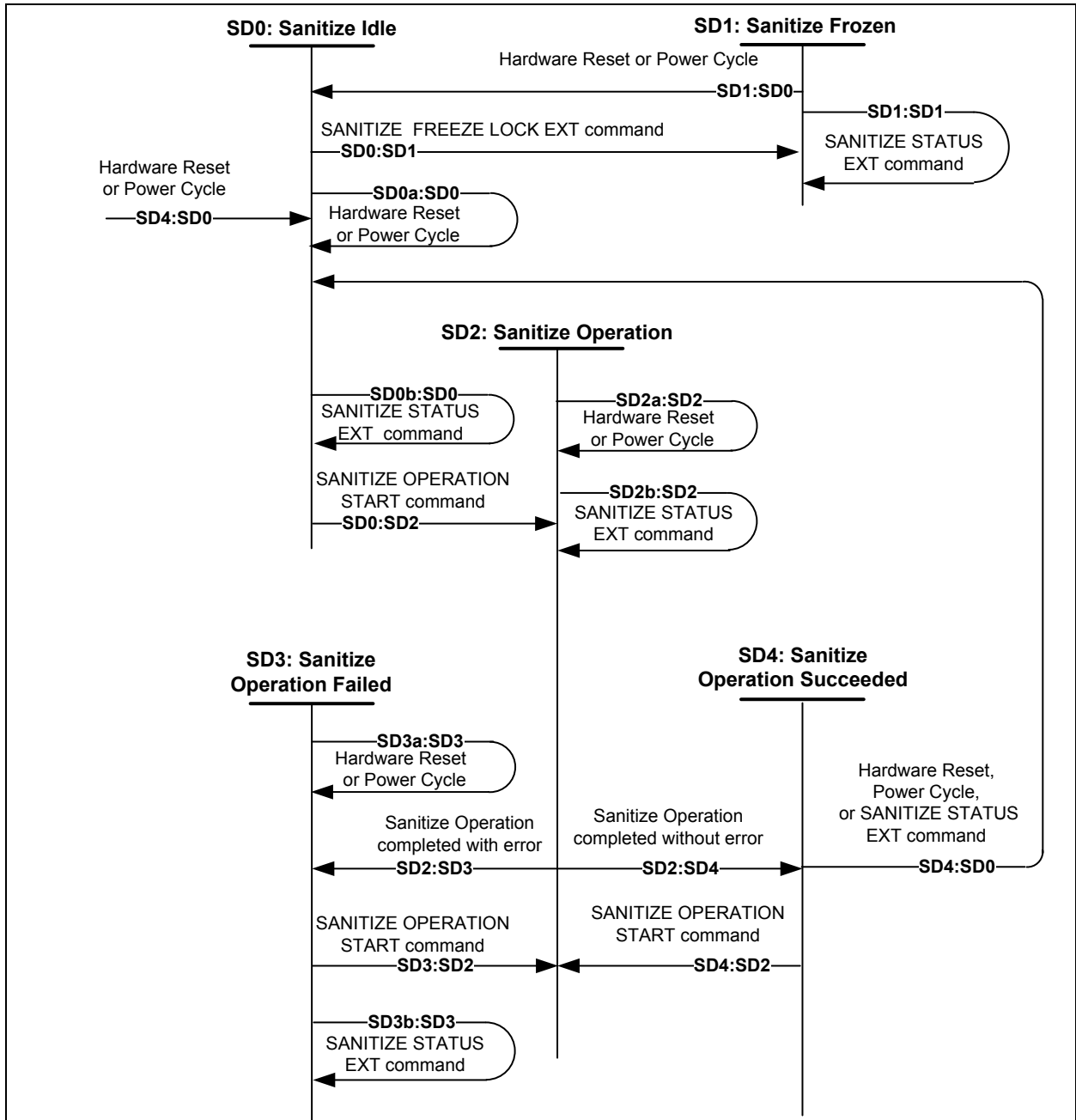
Transition SD4:SD0: When the device is in the Sanitize Operation state and it receives

- a) a hardware reset;
- a)b) [a power-on reset](#) or
- b)c) a SANITIZE STATUS EXT command

the device shall transition to the SD0 Sanitize Idle state.

Transition SD4:SD2: When the device is in the Sanitize Operation state and it receives a supported SANITIZE OPERATION START command, the device shall transition to the SD2 Sanitize Operation state.

Figure xx – SANITIZE DEVICE State Machine



4.4. Changes to Clause 6 (Status and Error fields)

6.1 Was:

The normal outputs (see 9.2) and error outputs (see 9.3) for each command shall include:

- a) a 1-byte Status field (see 6.2);
- b) a 1-byte Error field (see 6.3);
- c) for certain commands (e.g., PACKET, READ DMA QUEUED, READ DMA QUEUED EXT, WRITE DMA QUEUED, and WRITE DMA QUEUED EXT), a 1-byte Interrupt Reason field (see 6.4); and
- d) for certain commands (e.g., the READ FPDMA QUEUED command and WRITE FPDMA QUEUED command), the Count (see 6.5), SATA Status (see 6.7), and SActive (see 6.6) fields.

6.1 s/b:

The normal outputs (see 9.2) and error outputs (see 9.3) for each command shall include:

- a) a 1-byte Status field (see 6.2);
- b) a 1-byte Error field (see 6.3);
- c) for certain commands (e.g., PACKET, READ DMA QUEUED, READ DMA QUEUED EXT, WRITE DMA QUEUED, and WRITE DMA QUEUED EXT), a 1-byte Interrupt Reason field (see 6.4); and
- d) for certain commands (e.g., the READ FPDMA QUEUED command, [the Sanitize Device commands](#) and WRITE FPDMA QUEUED command), the Count (see 6.5), SATA Status (see 6.7), and SActive (see 6.6) fields.

4.5. Changes to Command Descriptions

7.18.7 Identify Device

Word	O M	S P	F V	Description
TBD	O	B	F	Bit TBD3: 1 = The Block Erase Sanitize operation is supported (see 7.x.4) TBD2: 1= The Overwrite Sanitize operation is supported (see 7.x.3) TBD1: 1 = The Cryptographic Scramble Sanitize operation is supported (see 7.x.2) TBD0: 1 = The Sanitize Feature Set is supported (see 4.x)

7.16.7.xx Word x: SANITIZE Commands

If bit 3 of word TBD is set to one the device supports the Overwrite Sanitize Method (see xx).

If bit 2 of word TBD is set to one the device supports the Block Erase Sanitize Method (see xx).

If bit 1 of word TBD is set to one the device supports the Cryptographic Scramble Method (see xx).

If bit 0 of word TBD is set to one the device supports the SANITIZE DEVICE EXT Command including the SANITIZE STATUS actions.

7.x Sanitize Device– xxh, non-data

7.x.1 Overview

Individual Sanitize Device commands are identified by the value placed in the Feature field. Table xx shows these values.

Table xx – Sanitize Device Feature Field Values

Value	Command
-------	---------

0000	SANITIZE STATUS EXT
0001..0010	Reserved
0011	SANITIZE OPERATION START EXT – CRYPTOGRAPHIC SCRAMBLE
0012	SANITIZE OPERATION START EXT – BLOCK ERASE
0013	Reserved
0014	SANITIZE OPERATION START EXT – OVERWRITE
0015..001F	Reserved
0020	SANITIZE FREEZE LOCK EXT
0021..FFFF	Reserved

7.x.2 SANITIZE STATUS EXT

7.x.2.1 Feature Set

This 48-bit command is mandatory for devices that implement the Sanitize Feature Set.

7.x.2.2 Description

If the Sanitize command is supported, the SANITIZE STATUS EXT command may be ~~executed~~processed at any phase in the Sanitize Device command sequence.

7.x.2.3 Inputs

Name	Description				
Feature	<table border="1"> <thead> <tr> <th>Value</th> <th>Command</th> </tr> </thead> <tbody> <tr> <td>0000h</td> <td>STATUS</td> </tr> </tbody> </table>	Value	Command	0000h	STATUS
Value	Command				
0000h	STATUS				
Count	Reserved				
LBA	<table border="1"> <thead> <tr> <th>Bit</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>47:0</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Description	47:0	Reserved
Bit	Description				
47:0	Reserved				
Device	<table border="1"> <thead> <tr> <th>Bit Description</th> </tr> </thead> <tbody> <tr> <td>7:5 101 (note: this signature is the inversion of non-Sanitize commands)</td> </tr> <tr> <td>4 Transport Dependent - See 6.2.12</td> </tr> <tr> <td>3:0 Reserved</td> </tr> </tbody> </table>	Bit Description	7:5 101 (note: this signature is the inversion of non-Sanitize commands)	4 Transport Dependent - See 6.2.12	3:0 Reserved
Bit Description					
7:5 101 (note: this signature is the inversion of non-Sanitize commands)					
4 Transport Dependent - See 6.2.12					
3:0 Reserved					
Command	7:0 xxh				

7.x.2.4 Normal Outputs

See Table xy.

7.x.2.5 Error Outputs

The abort bit shall be set to one after the completion of a SANITIZE DEVICE operation physical sectors that are ~~enabled~~available to be allocated for user data (i.e. allocated or unallocated physical sectors allowed by vendor-specific means to be usable for user data) were not successfully sanitized (e.g. Cryptographically scrambled, Block Erased, or Overwritten) .<Editor's Note: Note clarification of previous sentence>

See Table yz

7.x.3 SANITIZE OPERATION START EXT – CRYPTOGRAPHIC SCRAMBLE

7.x.3.1 Feature Set

This 48-bit command is optional for devices that implement the Sanitize Feature Set.

7.x.3.2 Description

The SANITIZE OPERATION START EXT – CRYPTOGRAPHIC SCRAMBLE command shall start a sanitize operation which shall change the internal encryption keys ~~which that~~ are used for user data. The SANITIZE CRYPTOGRAPHIC SCRAMBLE operation shall also remove ~~also any~~ user data held in caches and ~~any~~ pin setting attributes (see 4.16).

The SANITIZE OPERATION START EXT- CRYPTOGRAPHIC SCRAMBLE shall ~~not only~~ be reported as supported if all user data ~~would is not be~~ affected by changing internal encryption keys.

After a successful cryptographic scramble, the contents of the user data area ~~are may be in an~~ indeterminate ~~state~~.

The SANITIZE OPERATION START EXT – CRYPTOGRAPHIC SCRAMBLE shall only be ~~executed~~processed if:

- a) the SANITIZE DEVICE feature set is supported;
- b) the CRYPTOGRAPHIC SCRAMBLE method is supported; and
- c) the device is in the Sanitize Idle state, the Sanitize Operation Failed state, or the Sanitize Operation Succeeded state .

7.x.3.3 Inputs

Name	Description	
Feature	Value 0011h	Action CRYPTOGRAPHIC SCRAMBLE
Count	Reserved	
LBA	Bit 47:32 31:0	Description Reserved 43727970h <Editor's Note: Cryp>

Device	<p>Bit Description</p> <p>7:5 101 (note: this signature is the inversion of these values for non-Sanitize commands)</p> <p>4 Transport Dependent - See 6.2.12</p> <p>3:0 Reserved</p>
Command	7:0 xxh

7.x.3.4 Normal Outputs

See Table xy.

7.x.3.5 Error Outputs

The abort bit shall be set to one if:

- the Sanitize Device Cryptographic Scramble method is not supported; or
- a SANITIZE DEVICE FREEZE LOCK EXT command had been previously successfully completed.

See Table yz.

7.x.4 SANITIZE OPERATION START EXT – BLOCK ERASE

7.x.4.1 Feature Set

This 48-bit command is optional for devices that implement the Sanitize Feature Set.

7.x.4.2 Description

The SANITIZE OPERATION START EXT – BLOCK ERASE command shall start a sanitize operation which shall cause Block Erase operations on all user data. The SANITIZE BLOCK ERASE operation shall also remove ~~also any~~ user data held in caches and ~~any~~ pin setting attributes (see 4.16).

The SANITIZE OPERATION START EXT- BLOCK ERASE shall ~~not only~~ be reported as supported unless if the internal media supports Block Erase operations (e.g. NAND FLASH, see [ONFI]).

After a successful SANITIZE BLOCK ERASE operation, the contents of the user data area are ~~in an~~ indeterminate state.

The SANITIZE OPERATION START EXT – BLOCK ERASE shall only be ~~executed~~processed if:

- the Sanitize Device feature set is supported;
- the BLOCK ERASE method is supported; and
- the device is in the Sanitize Idle state, the Sanitize Operation Failed state, or the Sanitize Operation Succeeded state .

7.x.4.3 Inputs

Name	Description						
Feature	<table border="1"> <thead> <tr> <th>Value</th> <th>Command</th> </tr> </thead> <tbody> <tr> <td>0012h</td> <td>BLOCK ERASE</td> </tr> </tbody> </table>	Value	Command	0012h	BLOCK ERASE		
Value	Command						
0012h	BLOCK ERASE						
Count	Reserved						
LBA	<table border="1"> <thead> <tr> <th>Bit</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>47:32</td> <td>Reserved</td> </tr> <tr> <td>31:0</td> <td>426b4572h <Editor's Note: BkEr></td> </tr> </tbody> </table>	Bit	Description	47:32	Reserved	31:0	426b4572h <Editor's Note: BkEr>
Bit	Description						
47:32	Reserved						
31:0	426b4572h <Editor's Note: BkEr>						
Device	<p>Bit Description</p> <p>7:5 101 (note: this signature is the inversion of these values for non-Sanitize commands)</p> <p>4 Transport Dependent - See 6.2.12</p> <p>3:0 Reserved</p>						
Command	7:0 xxh						

7.x.4.4 Normal Outputs

See Table xy.

7.x.4.5 Error Outputs

The abort bit shall be set to one if:

- a. the Sanitize Device Block Erase method is not supported; or
- b. A SANITIZE DEVICE FREEZE LOCK EXT command had been previously successfully completed.

See Table yz.

7.x.5 SANITIZE OPERATION START EXT – OVERWRITE

7.x.5.1 Feature Set

This 48-bit command is optional for devices that implement the Sanitize Feature Set.

7.x.5.2 Description

The SANITIZE OPERATION START EXT – OVERWRITE command shall start a sanitize operation which fills the user data area with a four byte pattern passed in the LBA field of the command. Parameters for this method include a count for multiple overwrites and the option to invert the four byte pattern between consecutive overwrite passes. The SANITIZE OVERWRITE operation shall also remove ~~also any~~ user data held in caches and ~~any~~ pin setting attributes (see 4.16).

After a successful SANITIZE OVERWRITE operation affected data blocks shall contain valid ECC.

The SANITIZE OPERATION START EXT – OVERWRITE shall only be executed/processed if:

- a) the Sanitize Device feature set is supported;
- b) the OVERWRITE method is supported; and

- c) the device is in the Sanitize Idle state, the Sanitize Operation Failed state, or the Sanitize Operation Succeeded state.

7.x.5.3 Inputs

Name	Description				
Feature	<table border="1"> <thead> <tr> <th>Value</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>0014h</td> <td>OVERWRITE</td> </tr> </tbody> </table>	Value	Action	0014h	OVERWRITE
Value	Action				
0014h	OVERWRITE				
Count	Bit Description 15:8 Reserved 7 Invert pattern between overwrite operations 6:5 Reserved 4:0 Count of OVERWRITE operations, a count of zero requests sixteen overwrites				
LBA	Bit Description 48:32 4f57h <Editor's Note: OW> 31:0 Overwrite Pattern				
Device	Bit Description 7:5 101 (note: this signature is the inversion of these values for non-Sanitize commands) 4 Transport Dependent - See 6.2.12 3:0 Reserved				
Command	7:0 xxh				

7.x.5.4 Normal Outputs

See Table xy.

7.x.5.5 Error Outputs

The abort bit shall be set to one if:

- the Sanitize Device Overwrite method is not supported; or
- a SANITIZE DEVICE FREEZE LOCK EXT command had been previously successfully completed.

See Table yz.

7.x.6 SANITIZE FREEZE LOCK EXT

7.x.6.1 Feature Set

This 48-bit command is mandatory for devices that implement the Sanitize Feature Set.

7.x.6.2 Description

The SANITIZE FREEZE LOCK EXT command shall set the device to the Sanitize Frozen state. After command completion all Sanitize commands other than SANITIZE STATUS EXT shall be command aborted. Sanitize Frozen state shall be disabled by power-off or hardware reset. If a SANITIZE FREEZE LOCK EXT command is issued when the device is in the Sanitize Frozen state, the command ~~executes is~~ processed and the device shall remain in Sanitize Frozen state.

7.x.6.3 Inputs

Name	Description								
Feature	<table border="1"> <thead> <tr> <th>Value</th> <th>Command</th> </tr> </thead> <tbody> <tr> <td>0020h</td> <td>SANITIZE FREEZE LOCK</td> </tr> </tbody> </table>	Value	Command	0020h	SANITIZE FREEZE LOCK				
Value	Command								
0020h	SANITIZE FREEZE LOCK								
Count	Reserved								
LBA	<table border="1"> <thead> <tr> <th>Bit</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>47:32</td> <td>Reserved</td> </tr> <tr> <td>31:0</td> <td>46724c6bh <Editor's Note: FrLk></td> </tr> </tbody> </table>	Bit	Description	47:32	Reserved	31:0	46724c6bh <Editor's Note: FrLk>		
Bit	Description								
47:32	Reserved								
31:0	46724c6bh <Editor's Note: FrLk>								
Device	<table border="1"> <thead> <tr> <th>Bit</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>7:5</td> <td>101 (note: this signature is the inversion of these values for non-Sanitize commands)</td> </tr> <tr> <td>4</td> <td>Transport Dependent - See 6.2.12</td> </tr> <tr> <td>3:0</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Description	7:5	101 (note: this signature is the inversion of these values for non-Sanitize commands)	4	Transport Dependent - See 6.2.12	3:0	Reserved
Bit	Description								
7:5	101 (note: this signature is the inversion of these values for non-Sanitize commands)								
4	Transport Dependent - See 6.2.12								
3:0	Reserved								
Command	7:0 xxh								

7.x.6.4 Normal Outputs

See Table xy.

7.x.6.5 Error Outputs

See Table yz

4.6. Changes to Normal Outputs

Reference 7.x

Table xy: Normal Outputs Sanitize Device Commands

Name	Description												
Error	N/A												
Count	Sanitize Status and Supported Sanitize Methods Bits 15:0: Sanitize Status <table border="1"> <thead> <tr> <th>Bit</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>15</td> <td>Sanitize operation complete</td> </tr> <tr> <td>14</td> <td>Sanitize operation in progress</td> </tr> <tr> <td>13:0</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Description	15	Sanitize operation complete	14	Sanitize operation in progress	13:0	Reserved				
Bit	Description												
15	Sanitize operation complete												
14	Sanitize operation in progress												
13:0	Reserved												
LBA	Sanitize Progress Indication <table border="1"> <thead> <tr> <th>Bit</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>47:16</td> <td>Reserved</td> </tr> <tr> <td>15:0</td> <td>Sanitize Progress Indication: This is a percent complete indication of the total operation in progress. This value shall be FFFFh if a sanitize operation is not in process. The returned value is a numerator that has 65 536 (10000h) as its denominator.</td> </tr> </tbody> </table> <p>NOTE - The progress indication should be time related, however this is not an absolute requirement. (e.g., since format time varies with the number of defects encountered, etc., it is reasonable for the device server to assign values to various steps within the process. The granularity of these steps should be small enough to provide reasonable assurances to the application client that progress is being made.)</p>	Bit	Description	47:16	Reserved	15:0	Sanitize Progress Indication: This is a percent complete indication of the total operation in progress. This value shall be FFFFh if a sanitize operation is not in process. The returned value is a numerator that has 65 536 (10000h) as its denominator.						
Bit	Description												
47:16	Reserved												
15:0	Sanitize Progress Indication: This is a percent complete indication of the total operation in progress. This value shall be FFFFh if a sanitize operation is not in process. The returned value is a numerator that has 65 536 (10000h) as its denominator.												
Device	<table border="1"> <thead> <tr> <th>Bit</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>7</td> <td>Obsolete</td> </tr> <tr> <td>6</td> <td>N/A</td> </tr> <tr> <td>5</td> <td>Obsolete</td> </tr> <tr> <td>4</td> <td>Transport Dependent - See 6.2.12</td> </tr> <tr> <td>3:0</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Description	7	Obsolete	6	N/A	5	Obsolete	4	Transport Dependent - See 6.2.12	3:0	Reserved
Bit	Description												
7	Obsolete												
6	N/A												
5	Obsolete												
4	Transport Dependent - See 6.2.12												
3:0	Reserved												
Status	<table border="1"> <tbody> <tr> <td>7:6</td> <td>Transport Dependent - See 6.2.12.</td> </tr> <tr> <td>5</td> <td>Device Fault - See 6.2.7</td> </tr> <tr> <td>4</td> <td>N/A</td> </tr> <tr> <td>3</td> <td>Transport Dependent - See 6.2.12.</td> </tr> <tr> <td>2:1</td> <td>N/A</td> </tr> <tr> <td>0</td> <td>Error - See 6.2.9</td> </tr> </tbody> </table>	7:6	Transport Dependent - See 6.2.12.	5	Device Fault - See 6.2.7	4	N/A	3	Transport Dependent - See 6.2.12.	2:1	N/A	0	Error - See 6.2.9
7:6	Transport Dependent - See 6.2.12.												
5	Device Fault - See 6.2.7												
4	N/A												
3	Transport Dependent - See 6.2.12.												
2:1	N/A												
0	Error - See 6.2.9												

4.7. Changes to Error Outputs

The device shall return command aborted if:

- a) ~~A-a~~ SANITIZE OPERATION START EXT command was received after a SANITIZE FREEZE LOCK EXT command; or
- b) ~~An-an~~ unsupported SANITIZE OPERATION START command was received.

~~If physical sectors that are available for user data (i.e. allocated or unallocated physical sectors allowed by vendor-specific means to be usable for user data) were not successfully sanitized, then the device shall return an Error.~~

~~if:~~

~~The user data area, not including areas marked bad after the operation, has not been successfully overwritten.~~

See Table yz.

Reference: 7.x

Table yz – Sanitize Device Error

Name	Description														
Error	<table border="1"> <thead> <tr> <th>Bit</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>7:3</td> <td>N/A</td> </tr> <tr> <td>2</td> <td>Abort - See 6.3.2</td> </tr> <tr> <td>1:0</td> <td>N/A</td> </tr> </tbody> </table>	Bit	Description	7:3	N/A	2	Abort - See 6.3.2	1:0	N/A						
Bit	Description														
7:3	N/A														
2	Abort - See 6.3.2														
1:0	N/A														
Count	N/A														
LBA	<table border="1"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>FF FFFFh..00 0004h</td> <td>Reserved</td> </tr> <tr> <td>00 0003h</td> <td>Sanitize Frozen Error – A SANITIZE OPERATION START command was received after a SANITIZE FREEZE LOCK EXT command was received or when a sanitize operation was already in progress</td> </tr> <tr> <td>00 0002h</td> <td>Unsupported SANITIZE OPERATION START received – A SANITIZE OPERATION START command for an unsupported method was received</td> </tr> <tr> <td>00 0001h</td> <td>Sanitize Command Unsuccessful – SANITIZE OPERATION completed with User Data still retrievable from User Data Area (specifically in areas not marked defective)</td> </tr> <tr> <td>00 0000h</td> <td>Reserved</td> </tr> </tbody> </table>	Value	Description	FF FFFFh..00 0004h	Reserved	00 0003h	Sanitize Frozen Error – A SANITIZE OPERATION START command was received after a SANITIZE FREEZE LOCK EXT command was received or when a sanitize operation was already in progress	00 0002h	Unsupported SANITIZE OPERATION START received – A SANITIZE OPERATION START command for an unsupported method was received	00 0001h	Sanitize Command Unsuccessful – SANITIZE OPERATION completed with User Data still retrievable from User Data Area (specifically in areas not marked defective)	00 0000h	Reserved		
Value	Description														
FF FFFFh..00 0004h	Reserved														
00 0003h	Sanitize Frozen Error – A SANITIZE OPERATION START command was received after a SANITIZE FREEZE LOCK EXT command was received or when a sanitize operation was already in progress														
00 0002h	Unsupported SANITIZE OPERATION START received – A SANITIZE OPERATION START command for an unsupported method was received														
00 0001h	Sanitize Command Unsuccessful – SANITIZE OPERATION completed with User Data still retrievable from User Data Area (specifically in areas not marked defective)														
00 0000h	Reserved														
Device	<table border="1"> <thead> <tr> <th>Bit</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>7</td> <td>Obsolete</td> </tr> <tr> <td>6</td> <td>N/A</td> </tr> <tr> <td>5</td> <td>Obsolete</td> </tr> <tr> <td>4</td> <td>Transport Dependent - See 6.2.12</td> </tr> <tr> <td>3:0</td> <td>Reserved</td> </tr> </tbody> </table>	Bit	Description	7	Obsolete	6	N/A	5	Obsolete	4	Transport Dependent - See 6.2.12	3:0	Reserved		
Bit	Description														
7	Obsolete														
6	N/A														
5	Obsolete														
4	Transport Dependent - See 6.2.12														
3:0	Reserved														
Status	<table border="1"> <thead> <tr> <th>Bit</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>7:6</td> <td>Transport Dependent - See 6.2.12.</td> </tr> <tr> <td>5</td> <td>Device Fault - See 6.2.7</td> </tr> <tr> <td>4</td> <td>N/A</td> </tr> <tr> <td>3</td> <td>Data Request - See 6.2.5</td> </tr> <tr> <td>2:1</td> <td>N/A</td> </tr> <tr> <td>0</td> <td>Error - See 6.2.9</td> </tr> </tbody> </table>	Bit	Description	7:6	Transport Dependent - See 6.2.12.	5	Device Fault - See 6.2.7	4	N/A	3	Data Request - See 6.2.5	2:1	N/A	0	Error - See 6.2.9
Bit	Description														
7:6	Transport Dependent - See 6.2.12.														
5	Device Fault - See 6.2.7														
4	N/A														
3	Data Request - See 6.2.5														
2:1	N/A														
0	Error - See 6.2.9														

Change to 4.21.10, Security Command Actions Table

SANITIZE	Command Aborted	Executable	Executable
----------	-----------------	------------	------------

Change to Long Logical Sector Size <Editor' s Note: Annex C or E?>**Changes to ANNEX B, Command Codes Tables**

SANITIZE	Optional for ATA devices	Prohibited for Packet Devices	ND	48-bit
----------	--------------------------	-------------------------------	----	--------

Changes to ANNEX B, Historical Commands Table**Changes to Annex E**

<ACS-2 Editor's Note: Editor shall update Figure E.5 Typical HDD Layout Using A Master Boot Record, to change the label "USER DATA Area" to "File Data Area">

E.5.3 File System Formatting

There are many file systems that cluster sectors together to create an allocation unit larger than a single 512-byte sector. These file systems generally implement a table to associate clusters with files, commonly called a File Allocation Table (FAT). A typical cluster size is 4,096 bytes or eight 512-byte sectors. Even if the Partition is properly aligned, there is an issue where the size of the FAT may cause the individual clusters in the File Data Area (see Figure E.5) to be unaligned relative to the physical sectors on the media. This also results in performance degradation.

Additions to ASC/ASCQs

- D – Direct Access Block Device (SBC-3) Device Column key
- T – Sequential Access Device (SSC-3) blank = code not used
- L – Printer Device (SSC) not blank = code used
- P – Processor Device (SPC-2)
- W – Write Once Block Device (SBC)
- R – C/DVD Device (MMC-6)
- O – Optical Memory Block Device (SBC)
- M – Media Changer Device (SMC-3)
- A – Storage Array Device (SCC-2)
- E – SCSI Enclosure Services device (SES)
- B – Simplified Direct-Access (Reduced Block) device (RBC)
- K – Optical Card Reader/Writer device (OCRW)
- V – Automation/Device Interface device (ADC)
- F – Object-based Storage Device (OSD)

ASC	ASCQ	DTLPWROMAEBKVF	Description
04h	yyh	D A	LOGICAL UNIT NOT READY – SANITIZE OPERATION IN PROGRESS
04h	zzh	D A	LOGICAL UNIT NOT READY – SANITIZE OPERATION COMPLETED