

Deleted: e07197r4

Sanitize Device Ext Command

March 4, 2009

Deleted: December 16, 2008

Revision 5

Deleted: 4

Technical Editor:

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

March 4, 2009

Page 1 of 16

Deleted: December 16, 2008

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)

Deleted: FreezeLock

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.

Deleted: An implementation alternative to that proposed here would be to edit an existing proposal to enhance the ATA Secure Erase command, e.g., extending the command with additional capabilities and removing the mandatory usage of ATA security)¶

Deleted: repetition sequence to prepare and

Deleted: December 16, 2008

March 4, 2009

Page 2 of 16

Deleted: e07197r4

2. Scope

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

3. Overview

There are two steps to complete a Sanitize operation.

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

Deleted: three

Deleted: <#>Execute a SANITIZE PREPARE EXT command¶

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 (see 7.18.7.xx).

Deleted: 16

Sanitize operations shall write over 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.

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>

Deleted: <Editors Comment: A request was made during a plenary review to further define what is meant by erase. However, erase already has two different meanings in ACS, such as when used in the CFA ERASE SECTORS command and when used in the SECURITY ERASE UNIT command. ¶ To resolve this, I've created a definition for "Block Erase" which could be applied to the CFA ERASE commands.>¶

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 media where user data may be stored.

Deleted: abbreviations

Deleted: (

Deleted:)

Deleted: A

Deleted: To be developed outside this proposal by Curtis

Deleted: <Editors Note: To be developed outside this proposal by Curtis>

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 uses one of several optional methods to make all previously written content of in the user data area of the device unretrievable. This includes User Data Areas which may currently hold User Data, or that have been marked as unusable and any hidden areas (e.g. hidden through the use of the DCO, see 4.8, or HPA, see 4.11, feature sets). This also includes any user data held in caches and any pin setting attributes (see 4.16). This does not include Logs, or SMART pages. (e.g., this includes all allocatable physical blocks of a storage device in the user data area, whether or not they are currently allocated as logically addressable or marked as bad). Automatic sector reassignment is permitted during the operation of this

Formatted: Bullets and Numbering

Deleted: any user data area

Deleted: not be in

Deleted: use

Deleted: has

Deleted: December 16, 2008

Deleted: e07197r4

function. A SANITIZE DEVICE operation shall return an Error if physical blocks that have not been marked bad were not successfully sanitized.

Deleted: not

To perform a SANITIZE DEVICE operation the host:

- (1) issues a SANITIZE_DEVICE_EXT command with the Feature field set to a supported SANITIZE_OPERATION_START_EXT command; and
- (2) issues a SANITIZE_DEVICE_EXT command with the Feature field set to SANITIZE_STATUS to check for completion.

Deleted: A SANITIZE DEVICE operation is intended to run to completion, aborting any commands other than Identify Drive and Sanitize Status. If a SANITIZE DEVICE operation is interrupted by a power cycle, the SANITIZE DEVICE operation shall continue to completion before reporting ready.

A SANITIZE DEVICE operation is intended to run to completion, aborting any 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.

Formatted: Bullets and Numbering

The SANITIZE_STATUS_EXT command returns both information on which sanitize methods are supported, if a sanitize operation is complete and a percentage of completion if a sanitize operation is in progress.

Deleted: PREPARE command¶ issues a SANITIZE_OPERATION_START with a specific SANITIZE method (one of the optional methods)

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 Command Complete bit set to one and the Error bit cleared to zero (see Figure xx).

Deleted: Until the Sanitize operation is complete, all other commands return command aborted.

Formatted: Font color: Blue

The SANITIZE_FREEZE_LOCK_EXT command shall cause subsequent SANITIZE_OPERATION_START_EXT commands to be aborted. The SANITIZE_FREEZE_LOCK state is volatile.

Deleted: SANITIZE_PREPARE and

Deleted: until the next power cycle

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

Deleted: may

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

The CRYPTOGRAPHIC_SCRAMBLE and BLOCK_ERASE methods 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, between 1 and 16, for multiple overwrites and the option to invert the four byte pattern between consecutive overwrite passes.

Deleted: (

Deleted:)

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 powers-up and a sanitize operation is not in progress.

Transition SD0:SD0: When the device is in the Sanitize Idle State and it receives a SANITIZE_STATUS command, the device will 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 SD3 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.

Deleted: December 16, 2008

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

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

- a) the device powers-up and a sanitize operation is in progress, or
- b) the device is in the SD0 Sanitize Idle state and a supported SANITIZE OPERATION START command is received.

Transition SD2:SD2: When the device is in the Sanitize Operation State and it receives a REQUEST SENSE command, the device shall remain in the SD2 Sanitize Operation state.

Transition SD2:SD2: When the device is in the Sanitize Operation State and it receives a Identify Drive command, the device shall remain in the SD2 Sanitize Operation state.

Transition SD2:SD2: When the device is in the Sanitize Operation State,

- a) it receives a SANITIZE STATUS command, and
- b) the previous sanitize operation completed with an error status, then

the device shall remain in the SD2 Sanitize Operation state

Transition SD2:SD0: When the device is in the Sanitize Operation State,

- a) it receives a SANITIZE STATUS command, and
- b) the returned Sanitize status sanitize operation completed successfully, then

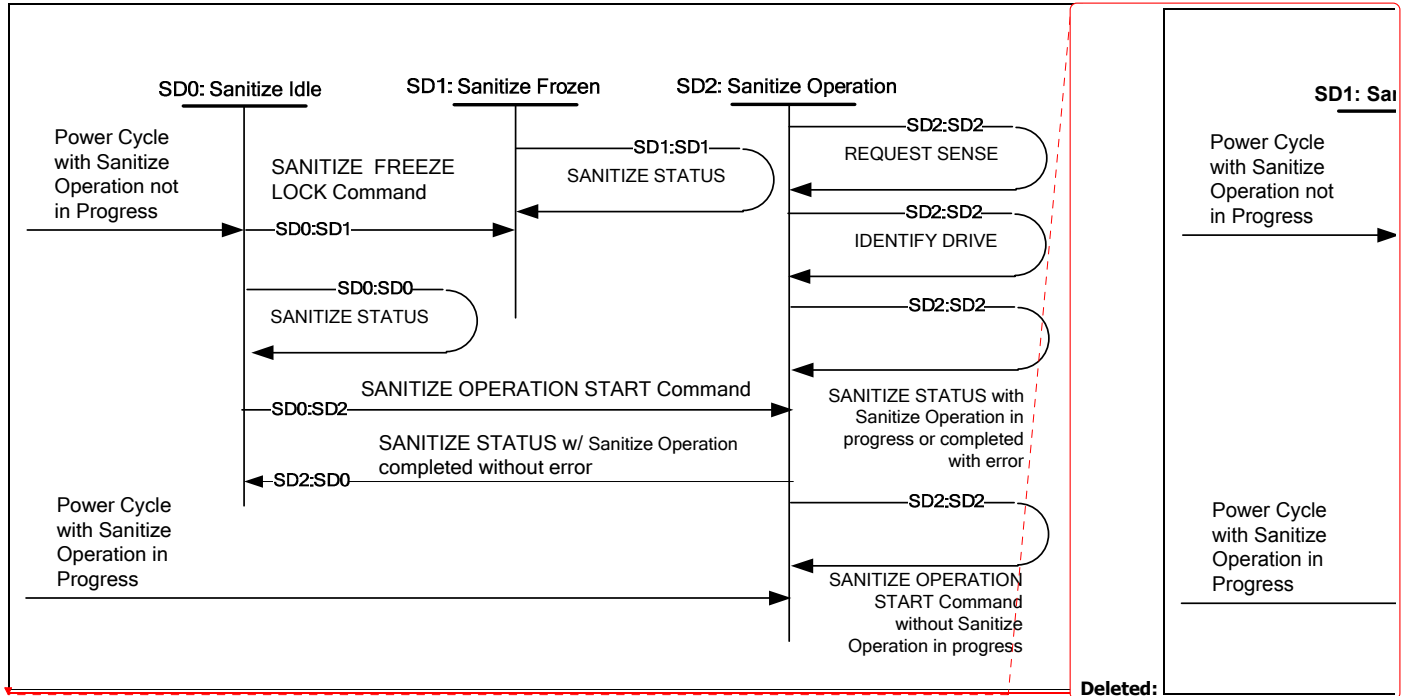
the device shall transition to the SD0 Sanitize Idle state

Transition SD2:SD2: When the device is in the Sanitize Operation State,

- a) it receives a supported SANITIZE OPERATION START command, and
- b) a sanitize operation is not in progress, then

the device shall start the requested sanitize operation and shall remain in the SD2 Sanitize Operation state

Figure xx – SANITIZE DEVICE State Machine



Deleted:

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 1-byte Status field (see 6.2);
- a 1-byte Error field (see 6.3);
- 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
- 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 1-byte Status field (see 6.2);
- a 1-byte Error field (see 6.3);
- 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
- for certain commands (e.g., the READ FPDMA QUEUED command, the SANITIZE DEVICE EXT command and WRITE FPDMA QUEUED command), the Count (see 6.5), SATA Status (see 6.7), and SActive (see 6.6) fields.

Formatted: Space After: 6 pt

Deleted: December 16, 2008

4.5. Changes to Command Descriptions

7.18.7 Identify Device

Word	O M	S P	F V	Description
TBD	O	B	F	Bit 3: 1 = The Block Erase Sanitize operation is supported (see 7.x.4) 2: 1= The Overwrite Sanitize operation is supported (see 7.x.3) 1: 1 = The Cryptographic Scramble Sanitize operation is supported (see 7.x.2) 0: 1 = The Sanitize Feature Set is supported (see 4.x)

Formatted: Centered

Formatted: Left

Formatted: Font: (Default) ArialMT

Comment [JG1]: Since the Sanitize Status command reports the supported operations, these bits are redundant – remove them from here?

7.16.7.xx Word x: SANITIZE Commands

Bits 15:4 of word x are reserved.

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

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

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

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

7.x SANITIZE DEVICE EXT – xxh, non-data

7.x.1 Overview

Individual SANITIZE DEVICE EXT commands are identified by the value placed in the Feature field. Table xx shows these values.

Table xx – SANITIZE DEVICE EXT 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

Deleted: -

Deleted: FFFE

Deleted: FFFF

Deleted: SANITIZE PREPARE EXT

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.

Deleted: December 16, 2008

7.x.2.2 Description

If the Sanitize command is supported, the SANITIZE STATUS EXT command may be executed 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	<p>Bit Description</p> <p>7:5,101 (note: this signature is the inversion of non-Sanitize commands)</p> <p>4 Transport Dependent - See 6.2.12</p> <p>3:0 Reserved</p>				
Command	7:0 xxh				

Formatted: Indent: Left: 37 pt, Tabs: 70.75 pt, Left

Deleted: Obsolete

Deleted: 6 Shall be set to one
5 Obsolete

Deleted: 6.2.11

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 if at least one sector in the user data area, not including areas marked bad after the operation, have not been successfully sanitized (e.g. Cryptographically scrambled, Block Erased, or Overwritten).

See Table yz

Deleted: will

Deleted: (

Deleted:)

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. If the Sanitize Feature Set is supported, at least one SANITIZE OPERATION START EXT commands shall be supported.

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 are used for user

Deleted: December 16, 2008

data. The SANITIZE CRYPTOGRAPHIC SCRAMBLE operation shall 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 be reported as supported if all User Data would not be affected by changing internal encryption keys

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

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

- The SANITIZE_DEVICE feature set is supported,
- The CRYPTOGRAPHIC SCRAMBLE method is supported, and
- The device is in the SANITIZE IDLE state, or is in the SANITIZE OPERATION state without a sanitize operation in progress.

~~Deleted: Sanitize~~~~Deleted: Device~~~~Deleted: ¶
All user data will be affected by changing internal encryption keys,~~~~Deleted: <#>, and¶
The previously received command (without intervening commands) was a SANITIZE PREPARE EXT command.~~

7.x.3.3 Inputs

Name	Description
Feature	Value 0011h Action CRYPTOGRAPHIC SCRAMBLE
Count	Reserved
LBA	Bit Description <u>47:32</u> <u>Reserved</u> <u>31:0</u> <u>43727970h <Editor's Note: Cryp></u>
Device	Bit Description 7:5 101 (note: this signature is the inversion of these values for non-Sanitize commands), 4 Transport Dependent - See <u>6.2.12</u> 3:0 Reserved
Command	7:0 xxh

~~Formatted: Indent: Left: 37.05 pt~~~~Deleted: Reserved~~~~Deleted: Obsolete¶
6 Shall be set to one¶
5 Obsolete~~~~Deleted: 6.2.11~~

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.

~~Deleted: will~~~~Deleted: <#>A SANITIZE OPERATION START EXT command was not immediately preceded by a SANITIZE PREPARE EXT command;¶~~~~Deleted: , Sanitize Device Ext Error~~

See Table yz.

~~Deleted: December 16, 2008~~

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. If the Sanitize Feature Set is supported, at least one SANITIZE OPERATION START EXT commands shall be supported.

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 remove also any user data held in caches and any pin setting attributes (see 4.16).

Deleted: b

Deleted: e

The SANITIZE OPERATION START EXT- BLOCK ERASE shall not be reported as supported unless 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 if:

- The Sanitize Device feature set is supported.
- The BLOCK ERASE method is supported, and
- The device is in the SANITIZE IDLE state, or is in the SANITIZE OPERATION state without a sanitize operation in progress.

Deleted: ¶
The internal media supports block erase operations (e.g. NAND FLASH, see [ONFI])

Deleted: , and¶
The previously received command (without intervening commands) was a SANITIZE PREPARE EXT command

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	<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								

Formatted: Indent: Left: 35.1 pt

Deleted: Reserve

Deleted: d

Deleted: Obsolete¶
6 Shall be set to one¶
5 Obsolete

Deleted: 6.2.11

Deleted: December 16, 2008

Deleted: e07197r4

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.

Deleted: will

Deleted: <#>a SANITIZE OPERATION START EXT command was not immediately preceded by a SANITIZE PREPARE EXT command;¶

See Table yz.

Deleted: , Sanitize Device Ext Error

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. If the Sanitize Feature Set is supported, at least one SANITIZE OPERATION START EXT commands shall be supported.

Comment [JG2]: An alternative is to make overwrite mandatory as part of the optional feature set, and make Crypto Scramble and Block Erase optional commands in the feature set

7.x.5.2 Description

The SANITIZE OPERATION START EXT – OVERWRITE command shall start a sanitize operation which fills all user data with a four byte pattern passed in the LBA field of the command. Parameters for this method include a count, between 1 and 16, for multiple overwrites and the option to invert the four byte pattern between consecutive overwrite passes. The SANITIZE OVERWRITE operation shall remove also any user data held in caches and any pin setting attributes (see 4.16).

Deleted: (

Deleted:)

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

The SANITIZE OPERATION START EXT –OVERWRITE shall only be executed 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, or is in the SANITIZE OPERATION state without a sanitize operation in progress.

Deleted: , and¶
The previously received command (without intervening commands) was a SANITIZE PREPARE EXT command

7.x.5.3 Inputs

Deleted: December 16, 2008

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				

Deleted:

Deleted: (

Deleted:)

Deleted: 47:33 Reserved

Comment [JG3]: ACK ACK short signature

Deleted: ¶

Deleted: 2

 Deleted: Obsolete¶
 6 Shall be set to one¶
 5 Obsolete

Deleted: 6.2.11

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.

Deleted: will

Deleted: <#>A SANITIZE OPERATION START EXT command was not immediately preceded by a SANITIZE PREPARE EXT command;¶

See Table yz.

Deleted: , Sanitize Device Ext Error

Deleted: FREEZELOCK

Formatted: Bullets and Numbering

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

Deleted: FREEZELOCK

7.x.6.3 Inputs

Deleted: December 16, 2008

Deleted: e07197r4

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	<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						

Deleted: FREEZELOCK

Formatted: Indent: Left: 37.05 pt

Deleted: Reserved

Deleted: Obsolete¶
6 Shall be set to one¶
5 Obsolete

Deleted: 6.2.11

7.x.6.4 Normal Outputs

See Table xy.

7.x.6.5 Error Outputs

See Table yz

4.6. Changes to Normal Outputs

Deleted: <#>SANITIZE PREPARE EXT ¶
<#>Description¶
The SANITIZE PREPARE EXT command must be executed immediately before a Sanitize operation is executed. If a SANITIZE OPERATION START EXT command is received without a preceding SANITIZE PREPARE EXT command, the SANITIZE OPERATION START EXT command shall be aborted. If a SANITIZE PREPARE EXT command is received during a Sanitize operation, the SANITIZE PREPARE EXT command shall be aborted.¶
¶
<#>Inputs¶
¶
Name

... [1]

Deleted: December 16, 2008

Reference 7.x

Table xy: Normal Outputs Sanitize Device Ext Commands

Name	Description																		
Error	N/A																		
Count	<p>Sanitize Status and Supported Sanitize Methods</p> <p>Bits 15:8: Sanitize Status</p> <table border="1"> <thead> <tr> <th>Bit</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>15</td> <td>Sanitize <u>operation complete</u></td> </tr> <tr> <td>14</td> <td>Sanitize <u>operation in progress</u></td> </tr> <tr> <td>13:8</td> <td>Reserved</td> </tr> </tbody> </table> <p>Bits 7:0: Supported Sanitize Methods</p> <table border="1"> <thead> <tr> <th>Bit</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>7:3</td> <td>Reserved</td> </tr> <tr> <td>2</td> <td>Cryptographic Scramble</td> </tr> <tr> <td>1</td> <td>Block Erase</td> </tr> <tr> <td>0</td> <td>Overwrite</td> </tr> </tbody> </table>	Bit	Description	15	Sanitize <u>operation complete</u>	14	Sanitize <u>operation in progress</u>	13:8	Reserved	Bit	Description	7:3	Reserved	2	Cryptographic Scramble	1	Block Erase	0	Overwrite
Bit	Description																		
15	Sanitize <u>operation complete</u>																		
14	Sanitize <u>operation in progress</u>																		
13:8	Reserved																		
Bit	Description																		
7:3	Reserved																		
2	Cryptographic Scramble																		
1	Block Erase																		
0	Overwrite																		
LBA	<p>Sanitize Progress Indication</p> <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 <u>sanitize operation</u> 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 <u>sanitize operation</u> 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 <u>sanitize operation</u> 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 <u>6.2.12</u></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 <u>6.2.12</u>	3:0	Reserved						
Bit	Description																		
7	Obsolete																		
6	N/A																		
5	Obsolete																		
4	Transport Dependent - See <u>6.2.12</u>																		
3:0	Reserved																		
Status	<table border="1"> <tbody> <tr> <td>7:6</td> <td>Transport Dependent - See <u>6.2.12</u></td> </tr> <tr> <td>5</td> <td>Device Fault - See <u>6.2.7</u></td> </tr> <tr> <td>4</td> <td>N/A</td> </tr> <tr> <td>3</td> <td>Transport Dependent - See <u>6.2.12</u></td> </tr> <tr> <td>2:1</td> <td>N/A</td> </tr> <tr> <td>0</td> <td>Error - See <u>6.2.9</u></td> </tr> </tbody> </table>	7:6	Transport Dependent - See <u>6.2.12</u>	5	Device Fault - See <u>6.2.7</u>	4	N/A	3	Transport Dependent - See <u>6.2.12</u>	2:1	N/A	0	Error - See <u>6.2.9</u>						
7:6	Transport Dependent - See <u>6.2.12</u>																		
5	Device Fault - See <u>6.2.7</u>																		
4	N/A																		
3	Transport Dependent - See <u>6.2.12</u>																		
2:1	N/A																		
0	Error - See <u>6.2.9</u>																		

Deleted: ..

Deleted: Operation

Deleted: Complete

Deleted: Operation

Deleted: Process

Deleted: 13 Sanitize Prepare Received]

Deleted: ..

Deleted: Sanitize

Deleted: Operation

Deleted: E

Deleted: 6.2.11

Deleted: 6.2.11

Deleted: 6.2.6

Deleted: 6.2.11

Deleted: 6.2.8

Deleted: December 16, 2008

Deleted: e07197r4

4.7. Changes to Error Outputs

The device shall return command aborted if:

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

The device shall return an Error if:

- a. 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 EXT Error

Name	Description
Error	Bit Description 7:3 N/A 2 Abort - See 6.3.2 1:0 N/A
Count	N/A
LBA	Value Description FF FFFFh..00 0004h Reserved 00 0003h Sanitize Sequence Error (Sanitize Frozen) – 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	Bit Description 7 Obsolete 6 N/A 5 Obsolete 4 Transport Dependent - See 6.2.12 3:0 Reserved
Status	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

Deleted: not immediately preceded by a SANITIZE PREPARE EXT command; ¶ A SANITIZE PREPARE EXT command was

Deleted: during a Sanitize operation

Formatted: Bullets and Numbering

Deleted: Sanitize

Deleted: operation

Deleted: requested

Deleted: (

Deleted:)

Deleted: xxx, Sanitize Device Ext Error

Deleted: Rerence

Deleted: Sanitize

Deleted: Operation

Deleted: Requested

Deleted: 6.2.11

Deleted: 6.2.11

Deleted: 6.2.6

Deleted: 6.2.4

Deleted: 6.2.8

Deleted: December 16, 2008

Deleted: e07197r4

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

<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.

Deleted: user data area

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)

Table with 4 columns: ASC, ASCQ, DTLPWROMAEBKVF, Description. Rows include LOGICAL UNIT NOT READY - SANITIZE OPERATION IN PROGRESS and LOGICAL UNIT NOT READY - SANITIZE OPERATION COMPLETED.

Deleted: To be done?
Add words to state machine?
Add in DCO language?
Describe what happens on restart (busy or not-busy)?

Deleted: December 16, 2008

SANITIZE PREPARE EXT

Description

The SANITIZE PREPARE EXT command must be executed immediately before a Sanitize operation is executed. If a SANITIZE OPERATION START EXT command is received without a preceding SANITIZE PREPARE EXT command, the SANITIZE OPERATION START EXT command shall be aborted. If a SANITIZE PREPARE EXT command is received during a Sanitize operation, the SANITIZE PREPARE EXT command shall be aborted.

Inputs

Name	Description				
Feature	<table border="1"> <thead> <tr> <th>Value</th> <th>Command</th> </tr> </thead> <tbody> <tr> <td>FFFFh:</td> <td>SANITIZE PREPARE</td> </tr> </tbody> </table>	Value	Command	FFFFh:	SANITIZE PREPARE
Value	Command				
FFFFh:	SANITIZE PREPARE				
Count	Reserved				
LBA	Reserved				
Device	<p>Bit Description</p> <ul style="list-style-type: none"> 7 Obsolete 6 Shall be set to one 5 Obsolete 4 Transport Dependent - See 6.2.11 3:0 Reserved 				
Command	7:0 xxh				

Normal Outputs

See Table xy.

Error Outputs

See Table yz