

## SanDisk Guard

Document Number: 80-11-80151

## Legal Disclaimer

The Western Digital Corporation or its affiliates general policy does not recommend the use of its products in life support applications wherein a failure or malfunction of the product may directly threaten life or injury. Without limitation to the foregoing, SanDisk shall not be liable for any loss, injury, or damage caused by use of its products in any of the following applications:

- Special applications such as military related equipment, nuclear reactor control, and aerospace.
- Control devices for transportation equipment including automotive vehicles, trains, ships, and traffic equipment.
- Safety systems for disaster prevention and crime prevention.
- Medical-related equipment (including medical measurement devices).

Accordingly, in any use of SanDisk products in life support systems or other applications where failure could cause damage, injury, or loss of life, the products should only be incorporated in systems designed with appropriate redundancy, fault tolerant, or back-up features. Per SanDisk Terms and Conditions of Sale, the user of SanDisk products in life support or other such applications assumes all risk of such use and agrees to indemnify, defend, and hold harmless Western Digital Corporation or its affiliates against all damages.

Security safeguards, by their nature, are capable of circumvention. SanDisk cannot, and does not, guarantee that data will not be accessed by unauthorized persons, and SanDisk disclaims any warranties to that effect to the fullest extent permitted by law.

this document and related material are for information use only and are subject to change without prior notice. Western Digital Corporation or its affiliates assumes no responsibility for any errors that may appear in this document or related material, nor for any damages or claims resulting from the furnishing, performance, or use of this document or related material. absent a written agreement signed by Western Digital Corporation or its affiliates or its authorized representative to the contrary, Western Digital Corporation or its affiliates explicitly disclaims any express and implied warranties and indemnities of any kind that may, or could, be associated with this document and related material, and any user of this document or related material agrees to such disclaimer as a precondition to receipt and usage hereof. Each user of this document expressly waives all guaranties and warranties of any kind associated with this document and/or related materials, whether expressed or implied, including without limitation, any implied warranty of merchantability or fitness for a particular purpose or infringement, together with any liability of Western Digital Corporation or its affiliates and its affiliates under any contract, profit or other incidental, punitive, indirect, special, or consequential damages, including without limitation physical injury or death, property damage, lost data, or costs of procurement of substitute goods, technology, or services.

This document and its contents, including diagrams, schematics, methodology, work product, and intellectual property rights described in, associated with, or implied by this document, are the sole and exclusive property of Western Digital Corporation or its affiliates and its applicable subsidiaries ("SanDisk"). No intellectual property license, express or implied, is granted by SanDisk associated with the document recipient's receipt, access and/or use of this document; SanDisk retains all rights hereto.

No work for hire, nor any form of joint ownership, is granted or implied by the document recipient's receipt, access and/or use of this document.

Any work requested (or implied by the document recipient to be requested) to SanDisk associated with this document and/or its contents, shall be the sole and exclusive property of SanDisk, except to the extent, if any, expressly agreed otherwise by SanDisk in writing referencing this document.

This document, and SanDisk's communications to the user associated therewith, shall be treated as SanDisk's proprietary and confidential information, protected by the recipient as such, and used by the recipient only for the purpose authorized in writing by SanDisk. This document shall be covered as SanDisk's confidential information under all applicable nondisclosure agreements between the recipient and SanDisk.

No part of this document may be reproduced, transmitted, transcribed, stored in a retrievable manner, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, without the prior written consent of an officer of Western Digital Corporation or its affiliates.

All parts of the SanDisk documentation are protected by copyright law and all rights are reserved. SanDisk and the SanDisk logo are registered trademarks of Western Digital Corporation or its affiliates, registered in the United States and other countries. Other brand names mentioned herein are for identification purposes only and may be the trademarks of their respective holder(s). Copyright 2016 Western Digital Corporation or its affiliates. All rights reserved.

## Revision History

Date	Revision	Section(s)	Description
July 2016	2	All	Western Digital corporate branding applied. No technical information was updated.
June 2015	1	All	Initial release.

## ESD Caution – Handling

Static electricity may be discharged through this disk subsystem. In extreme cases, this may temporarily interrupt the operation or damage components. To prevent this, make sure you are working in an ESD-safe environment. For example, before handling the disk subsystem, touch a grounded device, such as a computer case.



## Table of Contents

Contents	Pages
1.0 Introduction .....	7
2.0 Installation .....	7
2.1 Installation Requirements .....	7
2.2 Installation Procedure .....	7
3.0 User Interface .....	11
3.1 Elements of the User Interface .....	11
3.1.1 Device Bar .....	12
3.1.2 Quick Action Buttons .....	13
3.1.3 Device Health .....	13
3.1.4 Device Status .....	14
3.1.5 Activity Log .....	15
3.1.6 Status and Progress Bar .....	15
3.2 Toolbar .....	15
3.2.1 Toolbar Menu Options .....	16
3.2.2 Interface Specific Menu .....	19
3.3 Device Lockout .....	19
3.4 Session Logging .....	20
4.0 Test Menu .....	21
4.1 Elements .....	21
4.2 Diagnostic Report .....	21
4.3 Event Log .....	22
4.4 Core Dump .....	23
4.5 Panic Logs .....	23
4.5.1 Generate a Panic Log .....	23
4.5.2 Extract a Panic Log .....	23
4.5.3 Panic Log Seek .....	24
4.5.4 Panic Log Erase .....	25
4.6 Drive Self-test .....	26
5.0 Command Menu .....	27
5.1 Elements .....	27
5.2 Refresh .....	27
5.3 Update Firmware .....	28
5.4 Format .....	28
5.5 Sanitize .....	29
5.6 Sequential Write and Read .....	30
5.7 Random Write and Read .....	31

## Table of Contents

<b>Contents</b>	<b>Pages</b>
<b>6.0 SanDisk Menu</b> .....	<b>32</b>
6.1 Elements .....	32
6.2 Read Attributes .....	32
6.2.1 SATA Read Attributes .....	32
6.2.2 SAS Read Attributes .....	33
6.3 SMART Return Status .....	33
6.4 SMART Disable .....	33
6.5 SMART Enable .....	33
6.6 SMART Read Log .....	34
6.7 SMART Write Log .....	35
6.8 SMART Self-test .....	35
<b>7.0 SAS Menu</b> .....	<b>36</b>
7.1 Elements .....	36
7.2 Inquiry .....	36
7.2.1 Standard Inquiry .....	36
7.2.2 Vital Product Data Inquiry .....	37
7.3 Test Unit Ready .....	37
7.4 Read Capacity .....	37
7.5 Start Stop Unit .....	38
7.6 Mode Sense .....	39
7.6.1 Mode Sense Data .....	39
7.7 Log Sense .....	40
7.7.1 Log Sense Data .....	40
7.8 Read Defect Data .....	40
<b>8.0 SATA Menu</b> .....	<b>42</b>
8.1 Elements .....	42
8.2 Identify .....	42
8.3 SATA Power Management .....	42
8.4 Set Features .....	43
8.5 Security Feature Set .....	43
8.5.1 Security Unlock .....	44
8.5.2 Security Erase (Normal) .....	44
8.6 SATA Read Log .....	44
<b>9.0 Tools Menu</b> .....	<b>45</b>
9.1 Elements .....	45
9.2 Options .....	45

## Table of Contents

<b>Contents</b>	<b>Pages</b>
9.2.1 Environment Options .....	45
9.2.2 Device Control .....	46

## 1.0 Introduction

This user guide provides information about the installation, user interface, and diagnostic options of the SanDisk Guard tool.

SanDisk Guard is a Windows, client application intended for legacy products from SanDisk Corporation. SanDisk Guard is a configurable multi-device diagnostic tool that is available to SanDisk Corporation customers.

## 2.0 Installation

This section includes installation requirements and procedures, and various editions of SanDisk Guard.

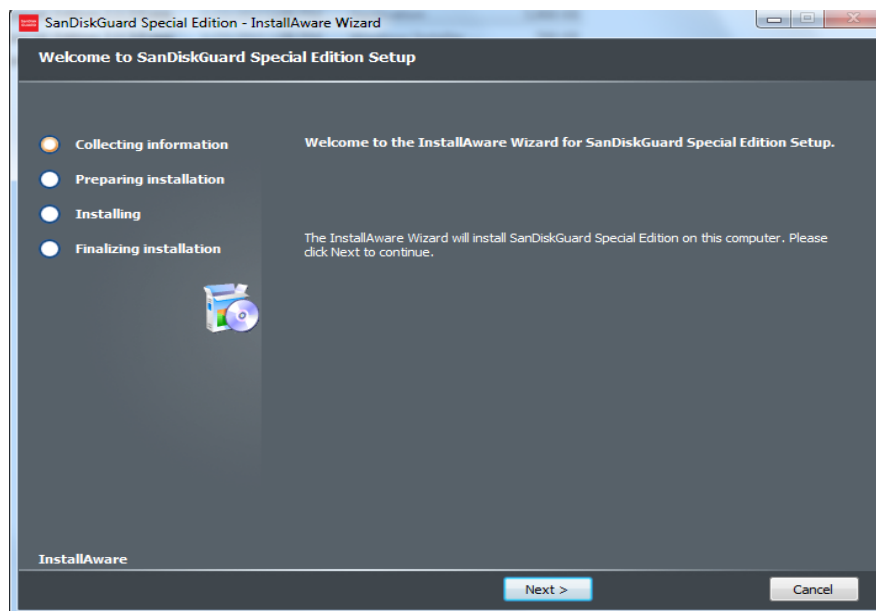
### 2.1 Installation Requirements

- LSI™ SAS 9207 series host bus adapter (HBA)
- Microsoft® Windows 7, 2008 R2, 2012 R2, 32-bit or 64-bit
- Microsoft .NET Framework 4.0

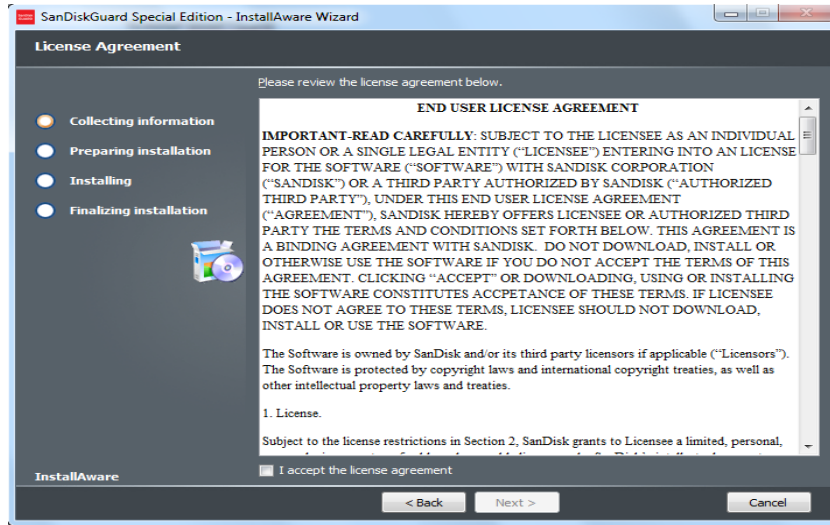
### 2.2 Installation Procedure

To install SanDisk Guard:

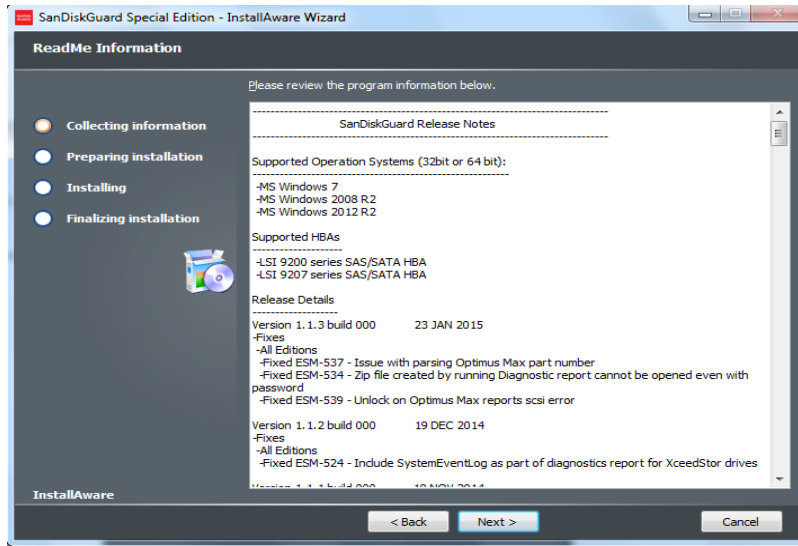
1. Double click `SanDiskGuard_Special_Edition_<version>.exe`.



2. Click **Next** at the welcome screen to continue.
3. Review and accept the licensing agreement.
4. Click **Next** to continue.



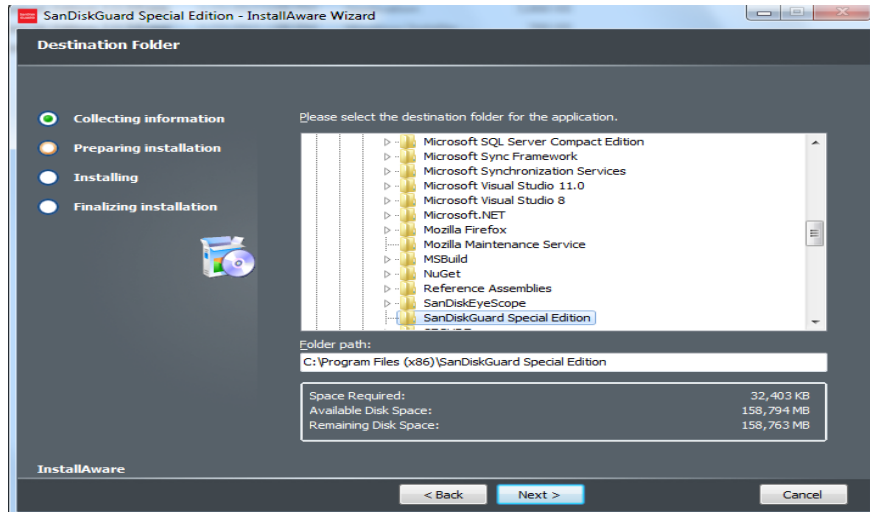
- 5. Review the release notes to see the most recent changes.
- 6. Click **Next** to continue.



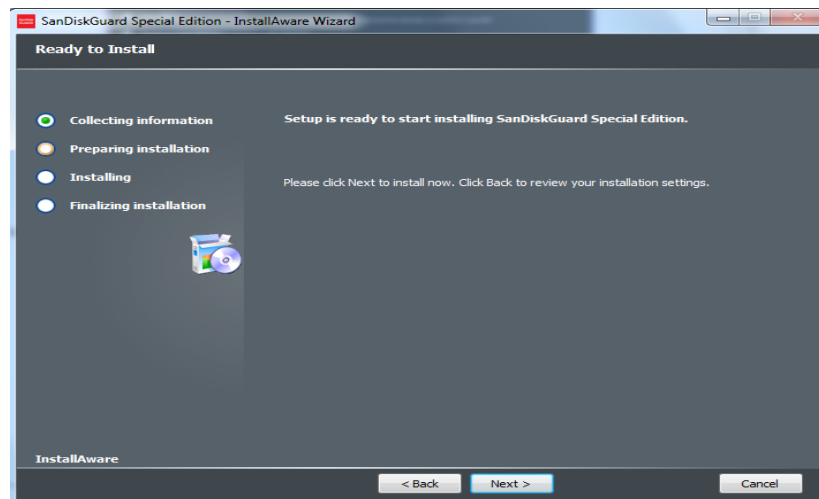
- 7. Select the location where you would like to install SanDisk Guard or use the default location.



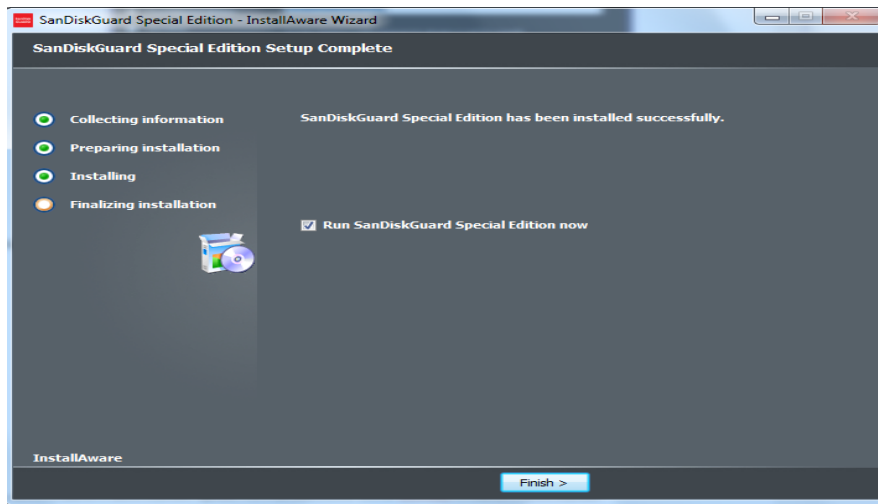
- Click **Next** to continue.



- Enter the name of the SanDisk menu group and select whether shortcuts are for your account only or for all users.
- Click **Next** to continue.
- Click **Next** to begin the installation process.



- When prompted, click **Finish**. You will have the option to launch SanDisk Guard after you close the installer by checking the Run SanDisk Guard box.

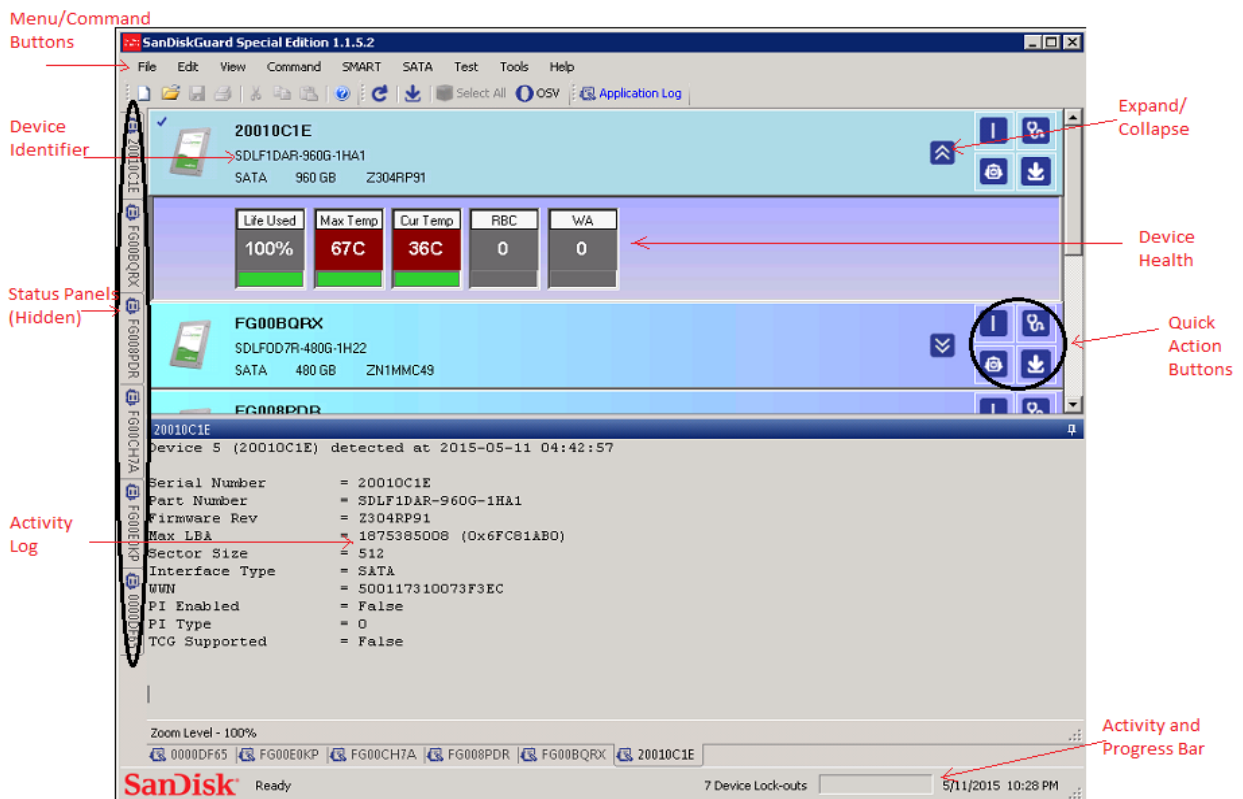


# 3.0 User Interface

## 3.1 Elements of the User Interface

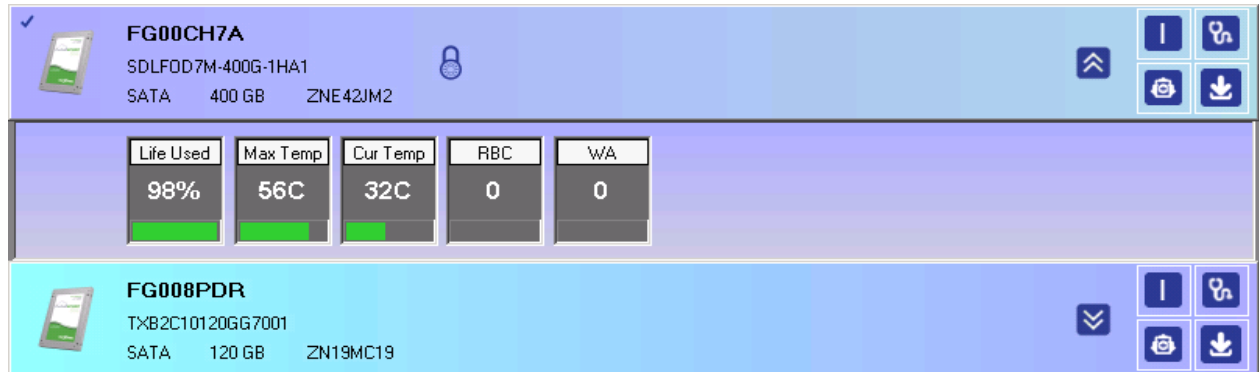
The SanDisk Guard user interface provides options for querying, monitoring, and sending commands. The user interface consists of the following:

- **Device Bar:** Contains device information and indicates whether the device is selected. The device bar contains quick action buttons for immediate access to frequently used commands.
- **Device Health:** Provides health information about the device through an expandable and collapsible panel:
  - Life Used
  - Maximum Temperature
  - Current Temperature
  - Retired Block Count
  - Write Amplification
- **Device Status Panels:** Displays more detailed information about a device. Device status panels are hidden by default.
- **Activity Log:** Displays the results of the most recent command or action.
- **Activity and Progress Bar:** Indicates the process of the current command or action and indicates the status of the connected device.
- **Menus and Device Command Buttons:** Contains both generic menus with options for all devices and device-specific menus with options exclusively applicable to the selected device type.



### 3.1.1 Device Bar

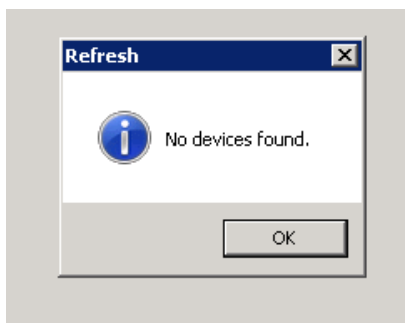
The device bar displays the connected devices as well as options for configuring and monitoring the devices. SanDisk Guard automatically searches for connected devices when launched. Select a device to issue a command. To select a device, **left click** the device bar. To select more than one device, click **CTRL** and **left-click** the desired devices. A purple bar indicates a device was selected. Menu selections only affect selected devices.







For each displayed device, the device bar displays device health information and quick action buttons. See [Quick Action Buttons, on page 13](#) and [Device Health, on page 13](#) for additional information.

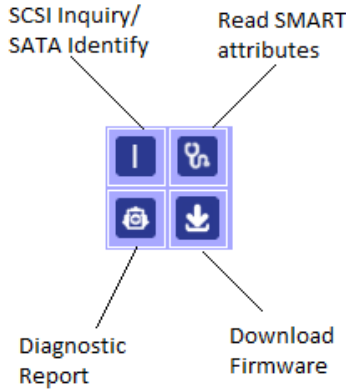
If SanDisk Guard does not detect connected devices, a blank screen displays. When a blank screen displays:

1. Check that devices are connected to an LSI HBA.
2. Check that devices are powered on.
3. Check that SanDisk Guard is running as administrator.
4. Click **Refresh (F5)**.



### 3.1.2 Quick Action Buttons



The quick action buttons allow for immediate access to the most common commands. The buttons are Inquiry for an SAS/SCSI device or Identify for an SATA/ATA , update Firmware , Diagnostic Report , and Read SMART Attributes .

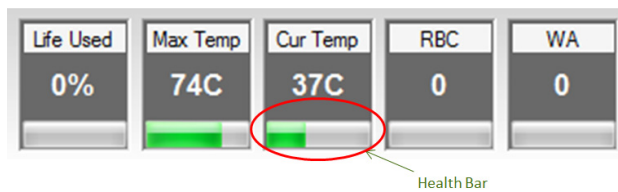


### 3.1.3 Device Health

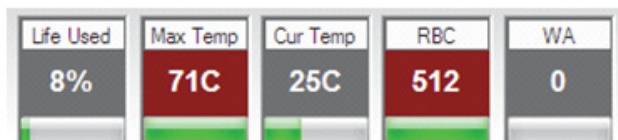
The SSD health information is displayed for all connected devices. The significance of each component of the device health is as follows:

- **Life Used:** The estimated total device life used shown as a percentage
- **Max Temp:** The maximum internal device temperature ever recorded in degrees Celsius
- **Cur Temp:** The current device temperature in degrees Celsius
- **RBC:** The total retired block count
- **WA:** The Write Amplification factor

The health bar graphically displays how close the current attribute is to the SMART threshold. The health information can be expanded or collapsed for each device by using the arrow buttons on the device bar. Click the down arrow  to expand the health bar to be visible. Click the up arrow  to collapse it so that it becomes hidden.



If a device has tripped a SMART threshold, the tripped attribute will turn red.

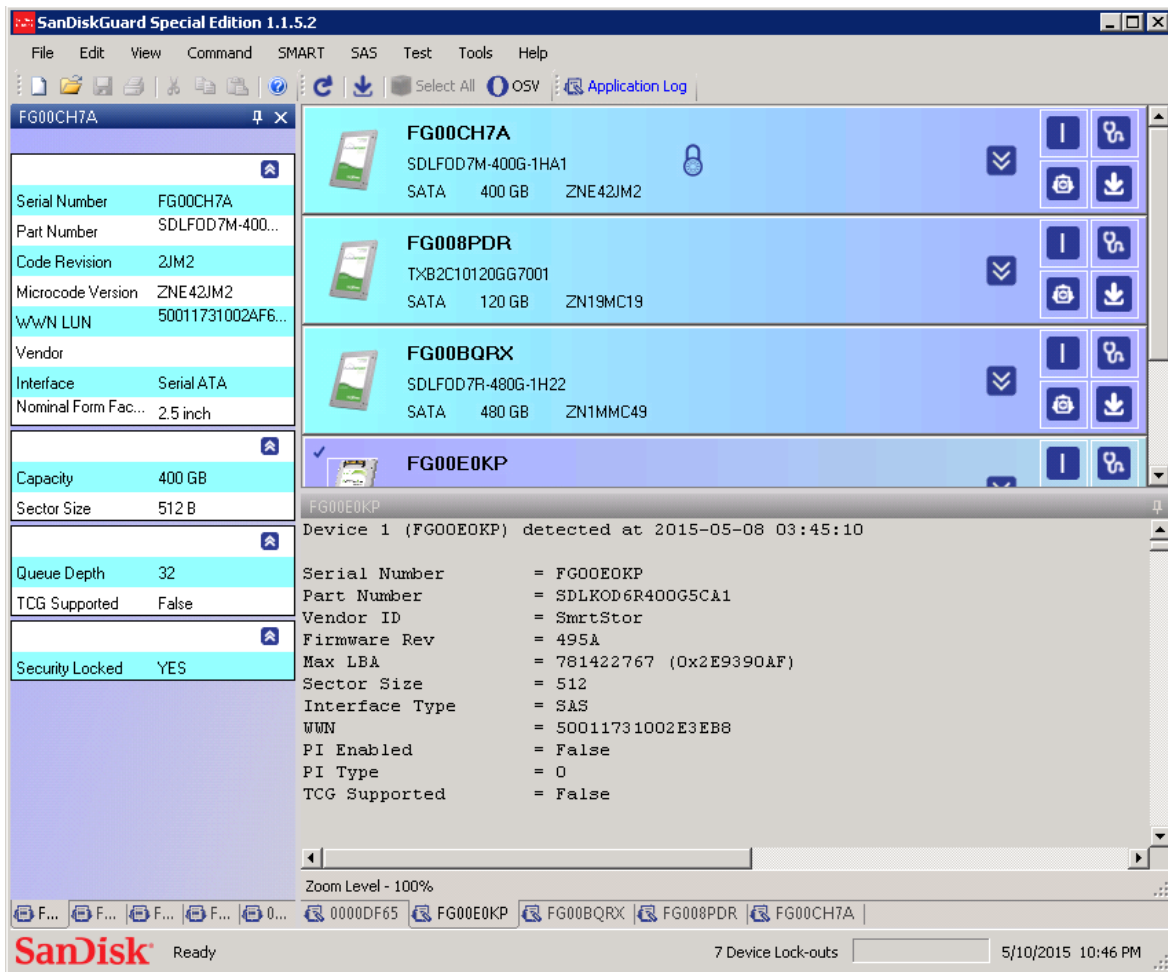


### 3.1.4 Device Status

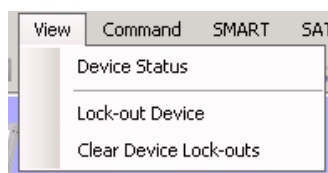
Device status panels display the following information about a device:

- Identity
- Geometry
- Configuration
- Security
- Statistics

Each category contains applicable information. Device status panels are hidden on the left-hand side of the user interface by default. The device panels can be pinned open by clicking on the pin icon.

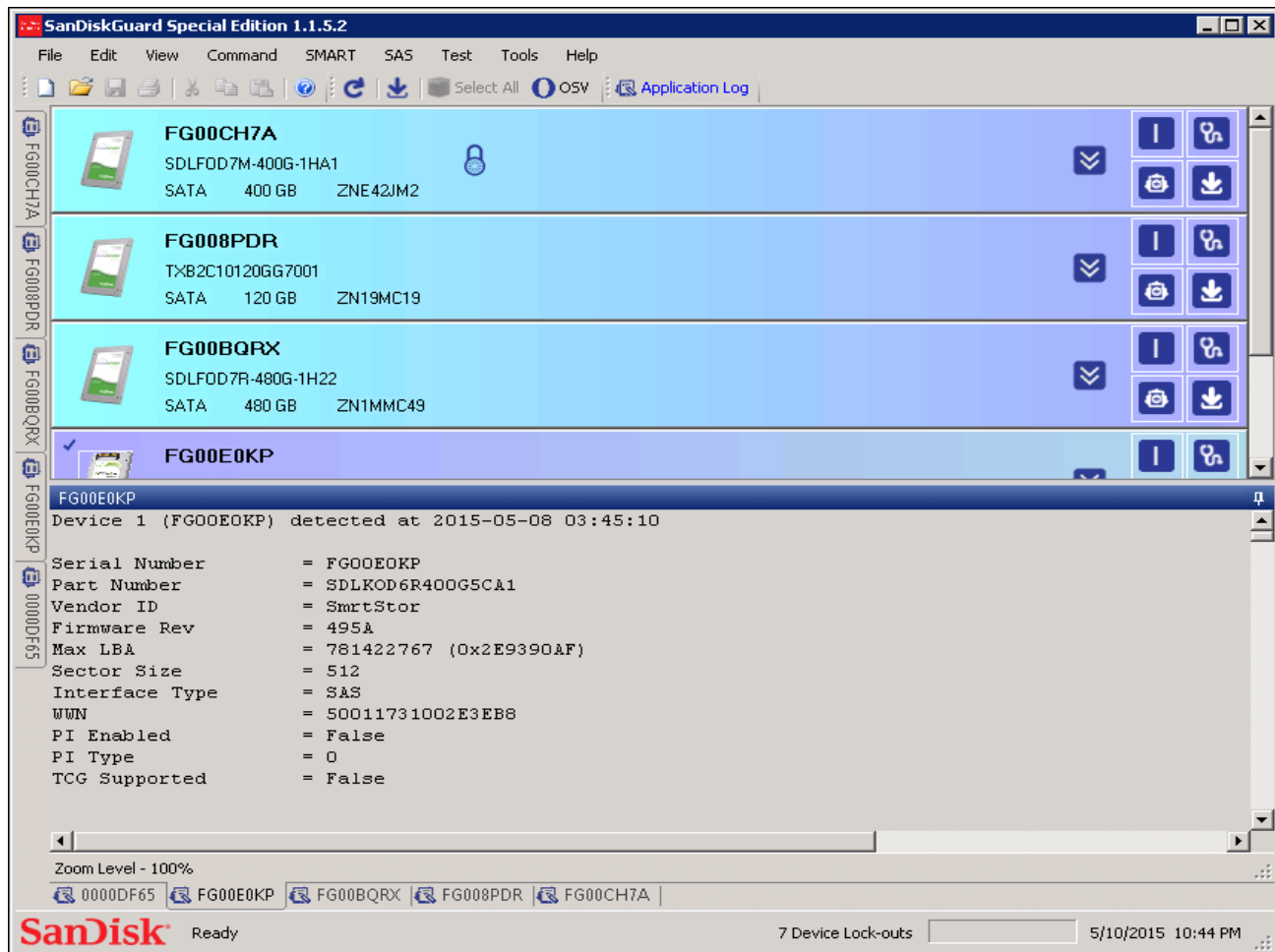


Each group is expandable and collapsible. To restore a hidden or closed status panel, select **View > Device Status**.



### 3.1.5 Activity Log

The activity log records and displays information about the most recent command for the selected drive(s). When multiple devices are connected, a tab is provided for each individual device. To view the activity log for a particular device, click the tab labeled with the drive serial number.



All activity logs are saved to MyDocuments\SanDiskGuard\Logs.

### 3.1.6 Status and Progress Bar

The status and progress bar is located at the bottom of the SanDisk Guard interface. The status and progress bar indicates how many devices are detected and the progress of any current long-running command or action. For example, it will cycle if a download firmware command has been issued until the command is completed. The status and progress bar also displays the date and time.






## 3.2 Toolbar

This section presents an overview of the toolbar menu options. The drop-down menus located on the toolbar provide access to commands, tests, and file operations.

### 3.2.1 Toolbar Menu Options









The following table lists the available menu options and identifies any shortcuts or buttons associated with the option.

**Table 1: Toolbar Menu Options**













Menu	Submenu	Command	Shortcut	Quick Access/Toolbar Button	Action	Page Ref	
File	New		CTRL + N		Opens a new SanDisk Guard application.		
	Open		CTRL + O		Lets you browse for and open an existing log file.		
	Exit		CTRL + Q		Closes the SanDisk Guard application.		
Test	Diagnostic Report		CTRL + D		Generates and saves a diagnostic report.	21	
	Event Log				Pulls the event log from the drive(s) and stores it in a specified location.	22	
	Core Dump				Retrieves the dump logs from the device(s) and stores it in a specified location.	23	
	Panic Log	Get Snapshot				Generates a panic log.	23
		Extract				Downloads all panic logs to the diagnostic report.	23
		Seek				Displays all available panic logs on LSI/SandForce based products.	24
		Erase				Erases all panic logs on LSI/SandForce-based products.	25
	Drive Self- test	Run				Runs a variety of tests and checks on the device(s).	26
		Report				Reports the results of the drive self-test.	



**Table 1: Toolbar Menu Options (Continued)**

Menu	Submenu	Command	Shortcut	Quick Access/ Toolbar Button	Action	Page Ref	
Command	Refresh		F5		Rescans the serial lanes for devices.	27	
	Update Firmware				Lets you select and update a firmware file onto the selected device(s).	28	
	Format	Current				Reformats the drive using the current drive configuration.	28
		512B/ 512B + PI				Reformats the drive to 512 Byte/sector optionally with Protection Information Type 2.	
		512B/ 512B + PI				Reformats the drive to 512 Byte/sector optionally with Protection Information Type 2.	
		528B				Reformats drive to 528 Byte/sector.	
		Sequential					30
	Random					31	
SMART	Read Attributes				Retrieves attributes data and reformats it into a readable version.	32	
	SATA Return Status				Reports whether a threshold has been exceeded.	33	
	SATA Disable				Disables operations on the drive.	33	
	SATA Enable				Enables operations on the drive.	33	
	SATA Read Log				Reads the specified log page using the Read Log command.	34	
	SATA Write Log				Writes data to the specified log page using the Write Log command.	35	
	SATA Self Test				Issues the SATA Self-test command.	35	

**Table 1: Toolbar Menu Options (Continued)**

Menu	Submenu	Command	Shortcut	Quick Access/ Toolbar Button	Action	Page Ref	
SAS	Inquiry	Standard Inquiry	CTRL + I		Returns standard device identifying and configuration data.	36	
		Vital Product Data			Returns detailed device identifying and configuration data.	37	
	TUR		CTRL + T		Issues the <b>Test Unit Ready</b> command to the selected device(s).	37	
	Read Capacity				Issues the <b>Read Capacity</b> command to the selected device(s).	37	
	Start-stop Unit	Start				Makes the media available for write and read access.	38
		Stop				Makes the media unavailable for write and read access.	
	Mode Sense					Reads device configuration parameters.	39
	Log Sense					Reads device statistics and metrics.	39
Read Defect	Defect Count				Returns the count of defects (grown and manufactured) from the selected device(s).	40	
SATA	Identify		CTRL + I		Returns the device identification and configuration data.	42	
	Standby Immediate				Moves the device(s) to standby.	42	
	Idle Immediate				Moves the device(s) to idle.	42	
	Sleep				Causes SATA interface to be inactive.	42	
	Check Power Mode				Returns the power-saving and performance mode of the device(s).	42	
	Set Features				Opens a dialog box that allows you to enable or disable various features.	43	
	Security Feature Set	Security Unlock				Sends the <b>Security Unlock</b> command to selected device(s).	43
		Security Erase				Performs a secure erase (encryption key only) operation on selected device(s).	
SATA Read Log					Lets you read selected logs.	44	

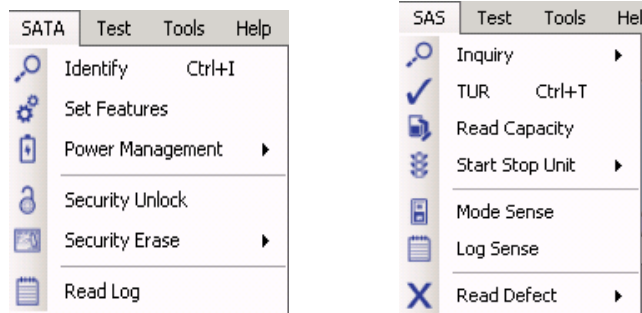
**Table 1: Toolbar Menu Options (Continued)**

Menu	Submenu	Command	Shortcut	Quick Access/ Toolbar Button	Action	Page Ref
Tools	Environment Options	Enable Sounds			Lets you enable sounds to alert the completion of a long-running command.	45
	Device Control				Lets you set the host bus adapter and access device error handling options.	45
Help	About			?	Displays information about the version of SanDisk Guard.	

### 3.2.2 Interface Specific Menu

The interface-specific menus contain commands unique to the communications protocol of the selected device. Only menus and commands relevant to the particular interface of the selected device(s) are visible. For example, only if an SAS device is selected will an SAS menu appear in the toolbar. The SAS menu provides options exclusively relevant to SAS devices.

Interface-specific menus are available in the toolbar. [See SAS Menu on page 36](#) [See SATA Menu on page 42](#).



### 3.3 Device Lockout

Device lockout hides devices from the user interface to prevent unintentional actions and commands.

To exclude devices from the user interface:

1. Select a device.
2. Select **View > Lock-out Device**.


The selected device will disappear from the list of available devices.

To restore the device to the user interface, select **View > Clear Device Lock-out**.

### 3.4 Session Logging

All device activity is logged with application status and error information. Session logging is saved to *MyDocuments\SanDiskGuard\Logs* at the end of every session. A session ends when SanDisk Guard is closed.

To view a log:

1. Select **File > Open**.
2. Click the open button  on the toolbar or **CTRL + O**.
3. Navigate to *MyDocuments* and select **SanDisk Guard > Logs**.
4. Click the desired log to open it.

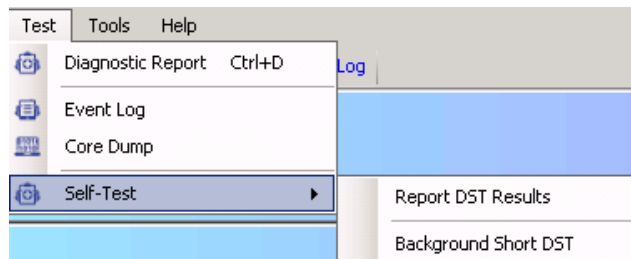
## 4.0 Test Menu

This section details the diagnostic options of SanDisk Guard located on the Test menu.

### 4.1 Elements

The Test menu generates information about the device(s) that is useful for debugging issues encountered with the drive(s). The Test menu includes the following interface- and device-specific diagnostic and test operations:


- Diagnostic Report
- Event Log Marking
- Core Dump



### 4.2 Diagnostic Report

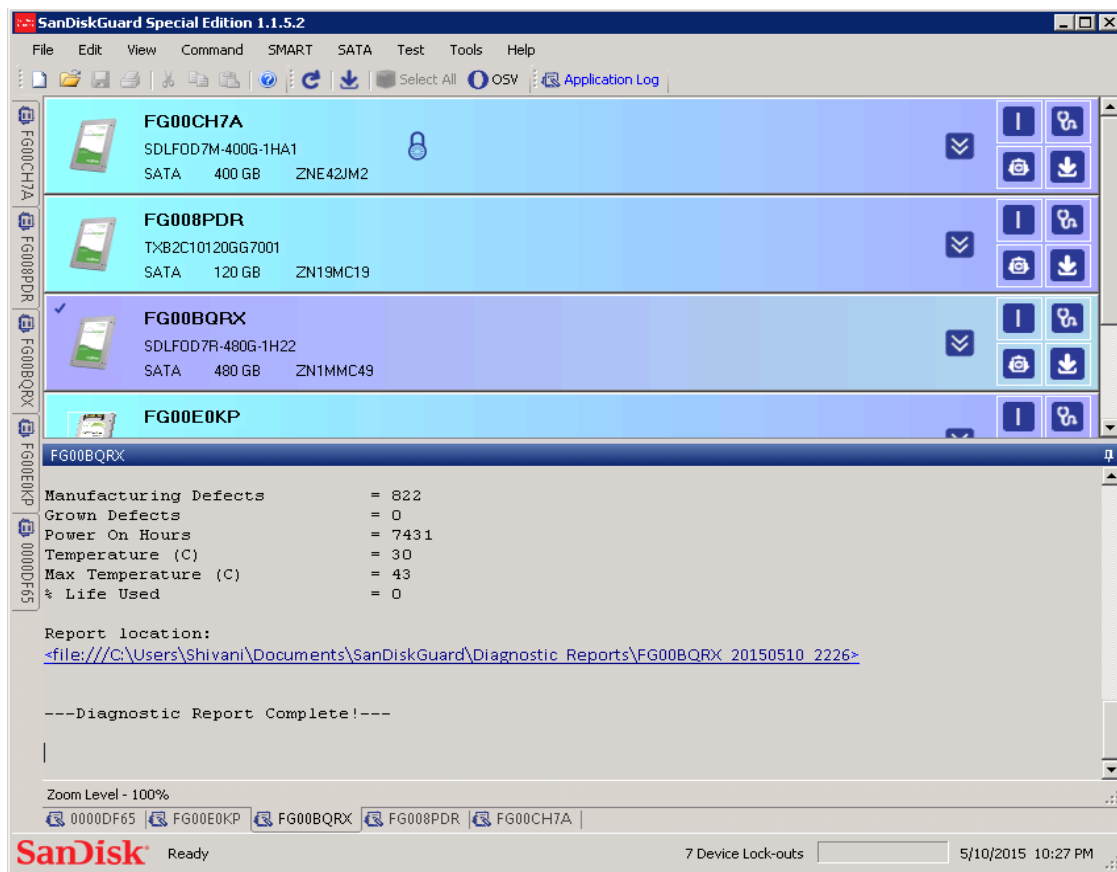
The diagnostic report retrieves all internal device logs, identification data, and device health data.

To generate a diagnostic report:

1. Select **Test > Diagnostic Report**.
2. Click the  quick action button or click **CTRL + D**.

If the device code is assigned, logs with format definitions will be parsed out and saved as text files. The diagnostic report can then be viewed by clicking on the hyperlink displayed in the activity log. The data and logs are written to files and archived to a zip file.

<b>NOTE:</b>	The password to the zip file is Sm@rtSt0r.
--------------	--



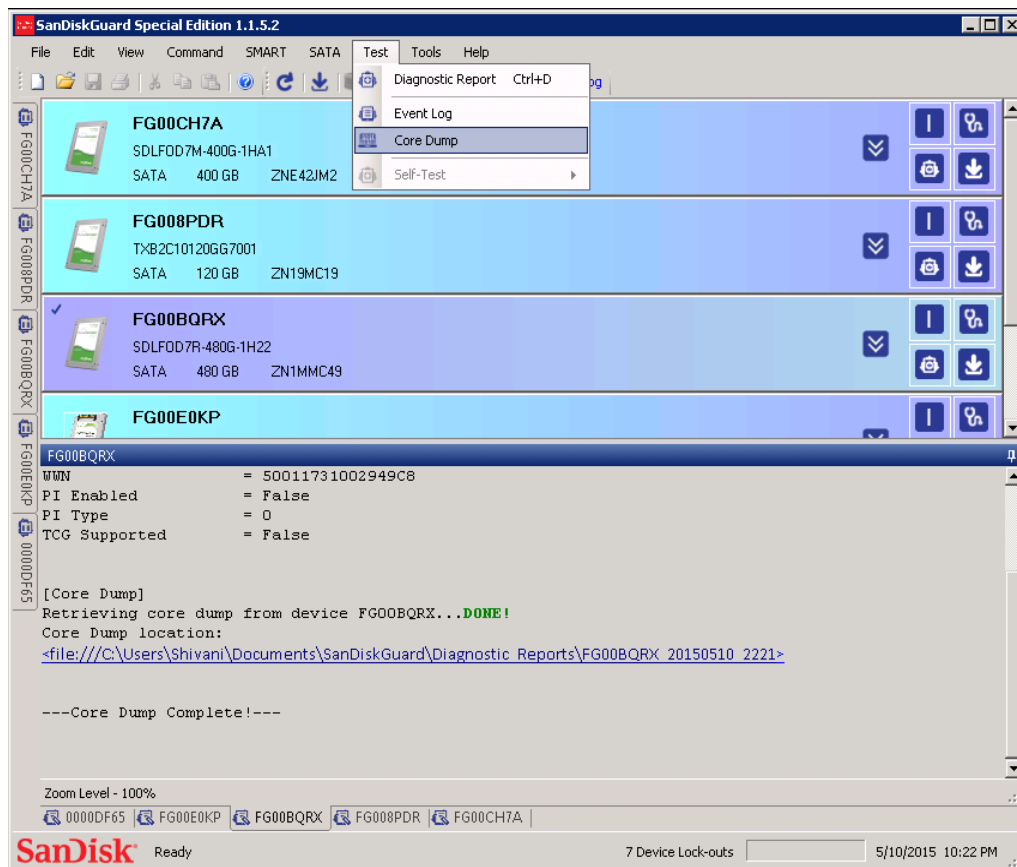
### 4.3 Event Log

To view the event log:

1. Select **Test > Event Log**.
2. Click the hyperlinks displayed in the activity log to view event logs. See first graphic under [Core Dump](#), on page 23.

## 4.4 Core Dump

1. Select **Test > Core Dump**.
2. Click the hyperlink displayed in the activity log to view core dumps.



## 4.5 Panic Logs

### 4.5.1 Generate a Panic Log

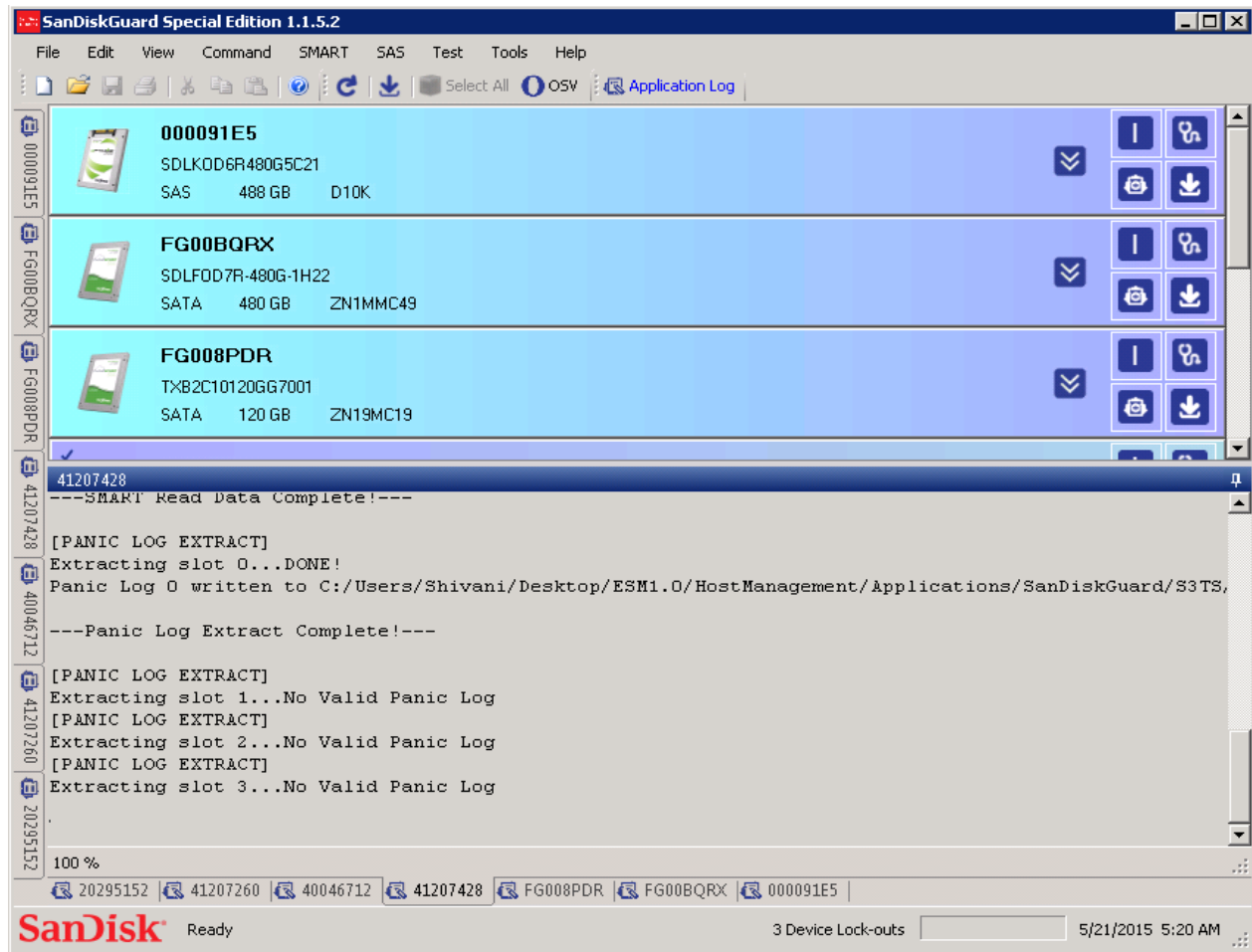
For LSI/SandForce-based products, GetSnapshot will generate a panic log. The device must be restarted to release SanDisk Guard from a paused state.

To generate a panic log, select **Test > Panic > Extract**.

### 4.5.2 Extract a Panic Log

Panic Log downloads are available for the Diagnostic Report folder in binary form.

Select **Test > Panic > Extract** to extract a panic log.

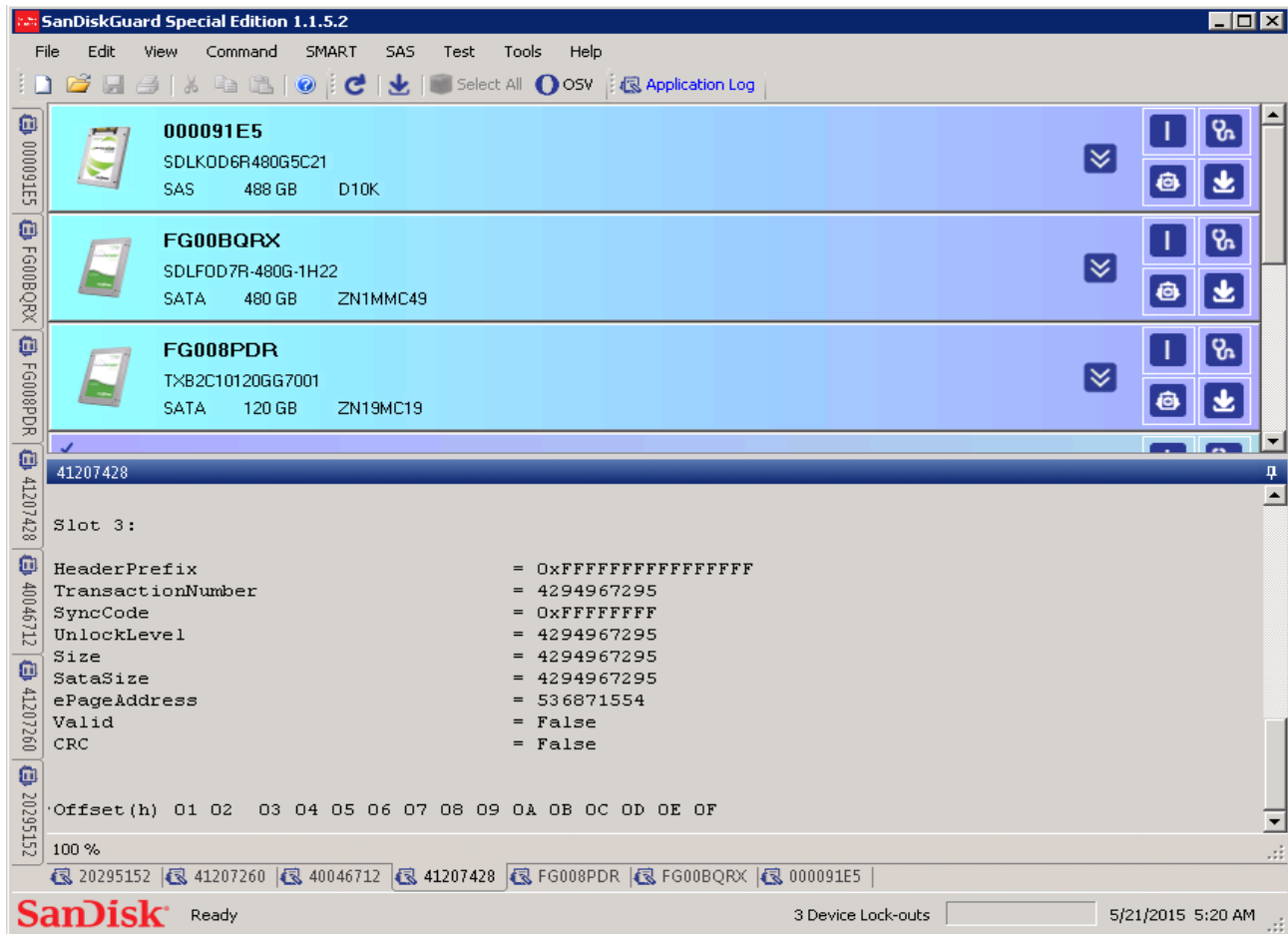


### 4.5.3 Panic Log Seek

Panic Log Seek lets you see what panic logs are available for LSI/SandForce-based products. The decoded headers for each panic slot are displayed along with the raw data returned.

Select **Test > Panic > Seek** to access panic logs.





#### 4.5.4 Panic Log Erase

You can erase all panic logs on an LSI/SandForce based product.

Select **Test > Panic > Erase** to erase panic logs.

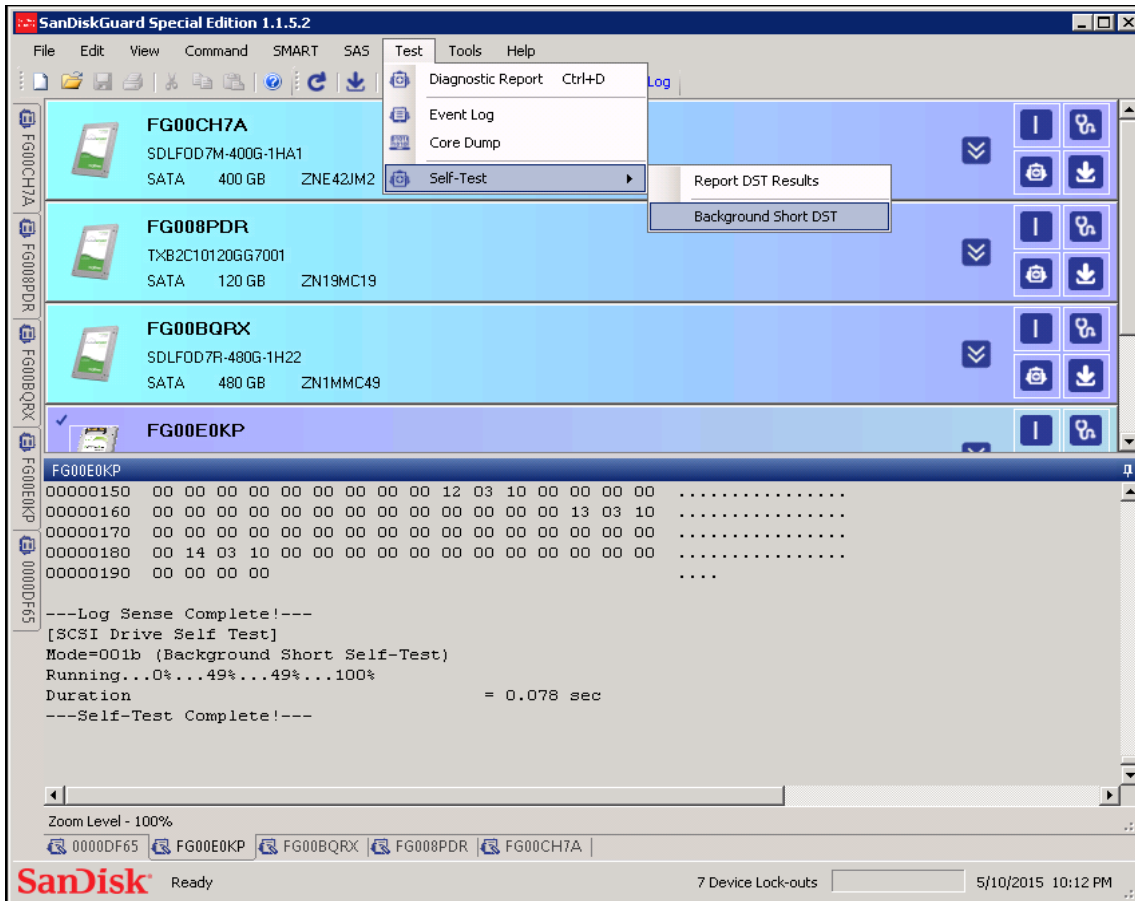
### 4.6 Drive Self-test

Drive self-test is part of the SCSI/ SAS standard. Run a drive self-test to perform the following operations:

- Run a sanity test on the FTL processor and its memory
- Test a section of DDR memory
- Test an area of shared memory
- Check for SMART attribute threshold trips

When the drive self-test completes, a command complete status is returned to you. If any failures occurred, the appropriate error status is returned.

1. Select **Test > DST > Run Background Short DST** to run SCSI DST.
2. Select **Test > DST > Report DST Results** to view DST results.

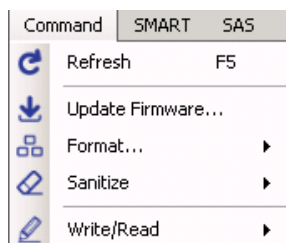


## 5.0 Command Menu

The command menu contains device commands and operations that are not interface-specific (SAS or SATA) and are available to all device types.

### 5.1 Elements

- Refresh
- Update Firmware
- Format
- Write/Read
- Sanitize



### 5.2 Refresh

The `Refresh` command rescans the serial lanes for devices. Powered off devices are removed from display when refreshed.

To refresh SanDisk Guard:

Select **Command > Refresh** or click **F5**.

**NOTE:**

Recently powered on devices may take several seconds to be recognized. If a device is not immediately recognized, wait a few seconds and refresh.

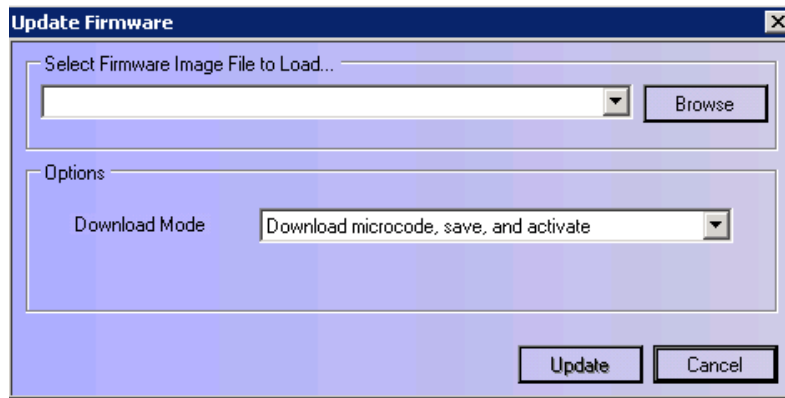
## 5.3 Update Firmware

SanDisk Guard lets you change the firmware for selected devices.

To upgrade device firmware:

1. Select **Command** > **Update Firmware** or click the  quick action button.

The Update Firmware dialog box opens.



2. Enter the path or click **Browse** for the firmware binary file to send to the device.
3. Click the down arrow to select the Download Mode.
4. Click **Update**.

The firmware binary file is transferred to the device using the appropriate commands for the device type. While the device processes the new code image, the progress bar will cycle to indicate background activity.

When the firmware update completes, the new firmware version is displayed in the device log and on the device bar. If sound is enabled, the completion will be signified by a beep.

```
[Update Firmware]
Download File   = D:\Shivani\D10k\optimus_eco_ex2_dell_D10K_480GB_fw.dob (407,552 B)
Xfer Mode      = Download microcode, save, and activate (05h)
Bytes per Xfer = 407552

Updating...DONE!

Updated Device Firmware Rev      = D10K
Duration                        = 5.928 sec
---Update Firmware Complete!---
```

## 5.4 Format

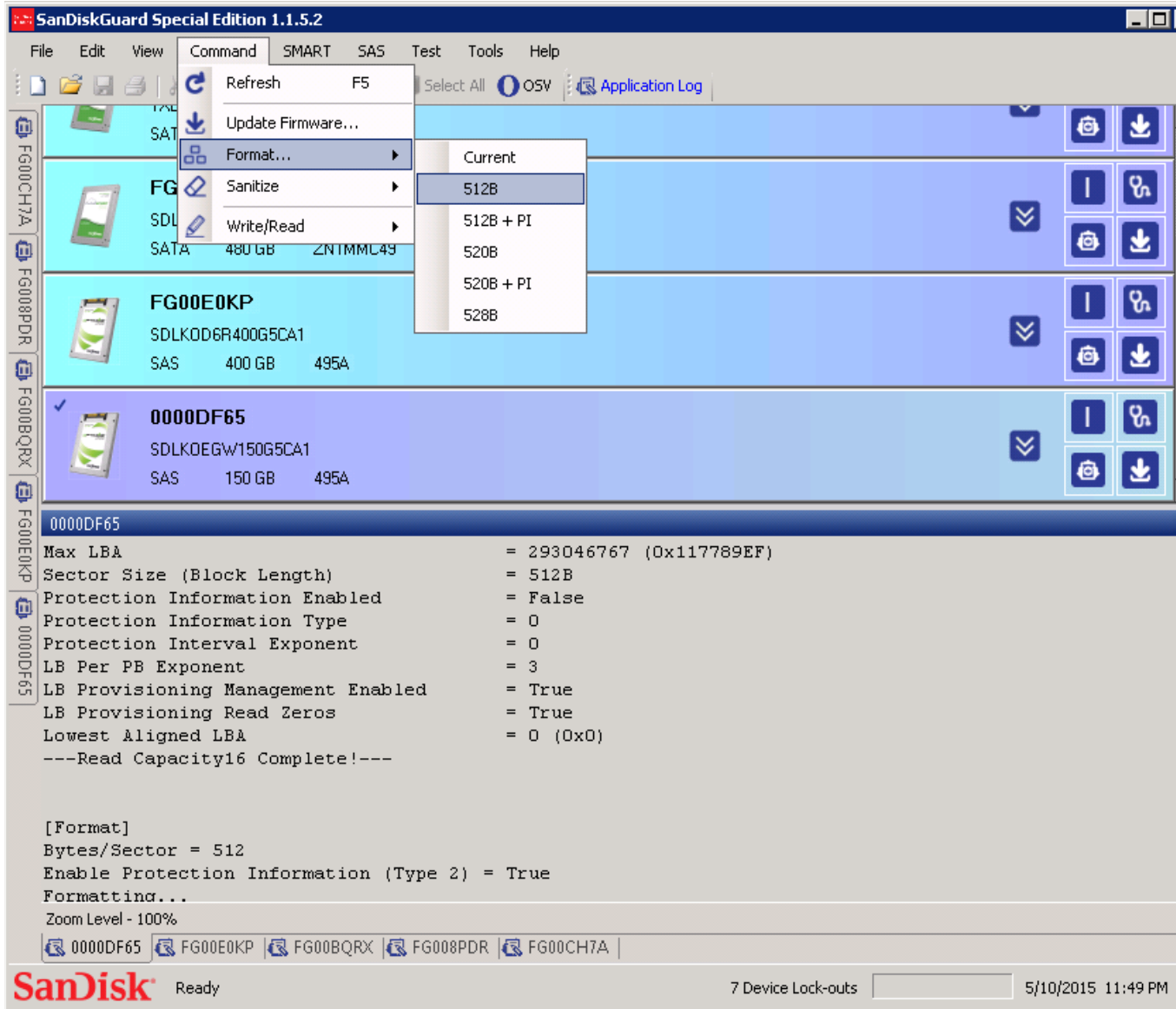
SanDisk Guard supports several different format options. These include:

- **Current:** Reformat current logical format
- **512B/512B + PI:** Format to 512 Byte/sector, optionally with Protection Information (PI) Type 2
- **520B/520B + PI:** Format to 520 Byte/sector, optionally with PI Type 2
- **528B:** Format to 528 Byte/sector

To format a SAS device, select **Command** > **Format** > **Option** where **Option** is the desired format type.

While a format is in progress, the progress bar cycles and indicates background activity. The percent complete is printed to the device log.

When a format completes, the duration is displayed and read capacity is issued and returns the new format and protection information status. If the PI state has changed, it will be reflected on the device bar.



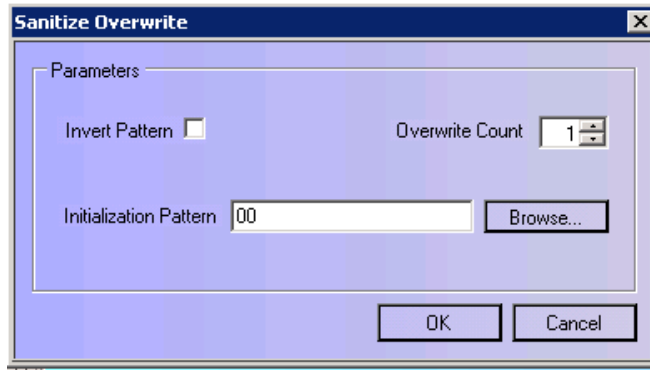
**NOTE:** Currently, format is only available for SCSI/SAS devices.

### 5.5 Sanitize

SanDisk Guard lets you perform the following operations:



- **Overwrite:** Causes the device server to alter information by writing a data pattern to the medium one or more times. You can set the initialization pattern, overwrite count, and invert pattern image.



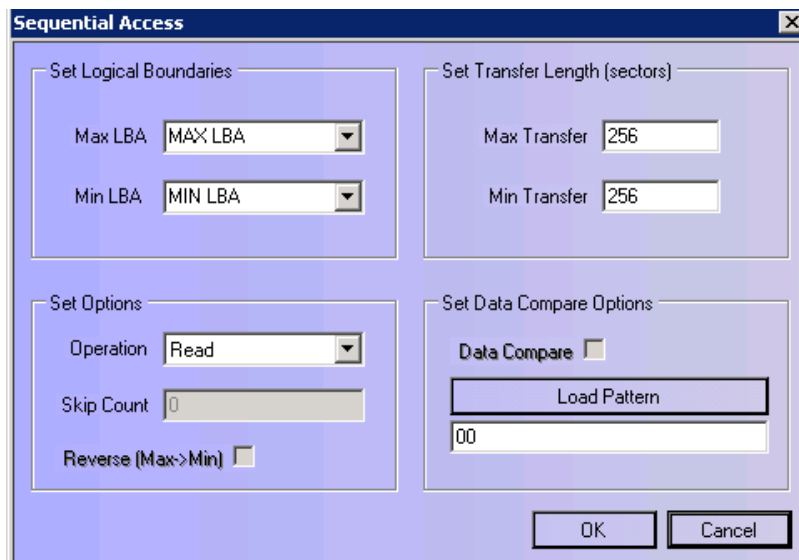
- **Block Erase:** Causes the device server to alter information by setting the physical blocks to a vendor specific value.
- **Cryptographic Erase:** Causes the device server to alter information by changing the encryption keys, which may cause protection information, if any, to be indeterminate.

## 5.6 Sequential Write and Read

Sequential Write and Read has several options which lets you do the following:

- Set the logical boundaries
  - Use pre-defined boundaries such as MAX Lock Block Address (LBA), or enter a number
- Set the transfer length
  - Each transfer randomized between Max and Min
  - Set Max = Min to use a fixed transfer length
- Set operation
  - Write/Read/Verify/Write Verify
- Set data compare options
  - If writing, load or enter a data pattern to use each transfer
  - Read data compare is currently disabled

To access Sequential Write and Read, select **Command > Write/Read > Sequential**.



## 5.7 Random Write and Read

Random Write and Read options let you do the following:

- Set the logical boundaries
  - Set the transfer length
  - Set operation
    - Write/Read/Verify/Write Verify
    - Enter the number of random commands
- Set data compare options
  - If writing, load or enter a data pattern to use each transfer
  - Read Data compare is currently disabled

To access Random Write and Read, select **Command > Write/Read > Random**.

**Random Access**

Set Logical Boundaries

Max LBA MAX LBA

Min LBA MIN LBA

Set Transfer Length (sectors)

Max Transfer 256

Min Transfer 256

Set Options

Operation Read

Commands 1

Set Data Compare Options

Data Compare

Load Pattern

00

OK Cancel

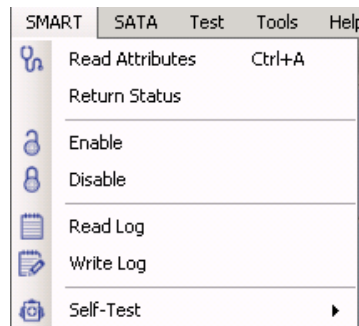
## 6.0 SanDisk Menu

The SMART menu contains tools for working with data. SMART is a native element of the ATA/SATA standard and has additional features and commands not found in SCSI/SAS.

### 6.1 Elements

- Read Attributes
- Return Status
- Enable
- Disable
- Read Log
- Write Log
- Self Test

**NOTE:** Read Attributes is the only SMART menu command available for SAS devices.



### 6.2 Read Attributes


The `Read Attributes` command reads the attribute data, reformats it, and returns it in a readable version.

#### 6.2.1 SATA Read Attributes

On a SATA device, `Read Attributes` send a SMART read data command to the device to read the attribute data. The `Read Data` command returns the SMART attribute data and reformats it into a readable version.

The formats may vary between different SATA devices.

To issue a SATA `Read Attributes` command, you must have a SATA device selected on the device bar.

Select **SMART > Read Attributes** or select the  quick action button.




### 6.2.2 SAS Read Attributes

On a SAS device, Read Attributes send a `Log Sense` command to the device to read the relevant log page containing the SMART attributes data. The `Log Sense` command returns the SMART attribute data and reformats it into a readable version.

Read Attributes is the only SMART menu option for SAS devices.

To issue the SAS `Read Attributes` command, you must select a SAS device on the device bar:

Select **SMART > Read Attributes** or select the  quick action button.

### 6.3 SMART Return Status

SATA Return Status reports whether a SMART attribute threshold has been exceeded.

To view SATA Return Status, select **SMART > Return Status**.

If a SMART threshold has been exceeded, use Read Attributes to view the status of each attribute and identify the exceeded threshold. See [Read Attributes, on page 32](#).

### 6.4 SMART Disable

SMART Disable turns off SMART attribute measurements and reporting. SMART commands will report an error if disabled.

To use SATA Disable, select **SMART > Disable**.

### 6.5 SMART Enable

SMART Enable restores SMART reporting if disabled.

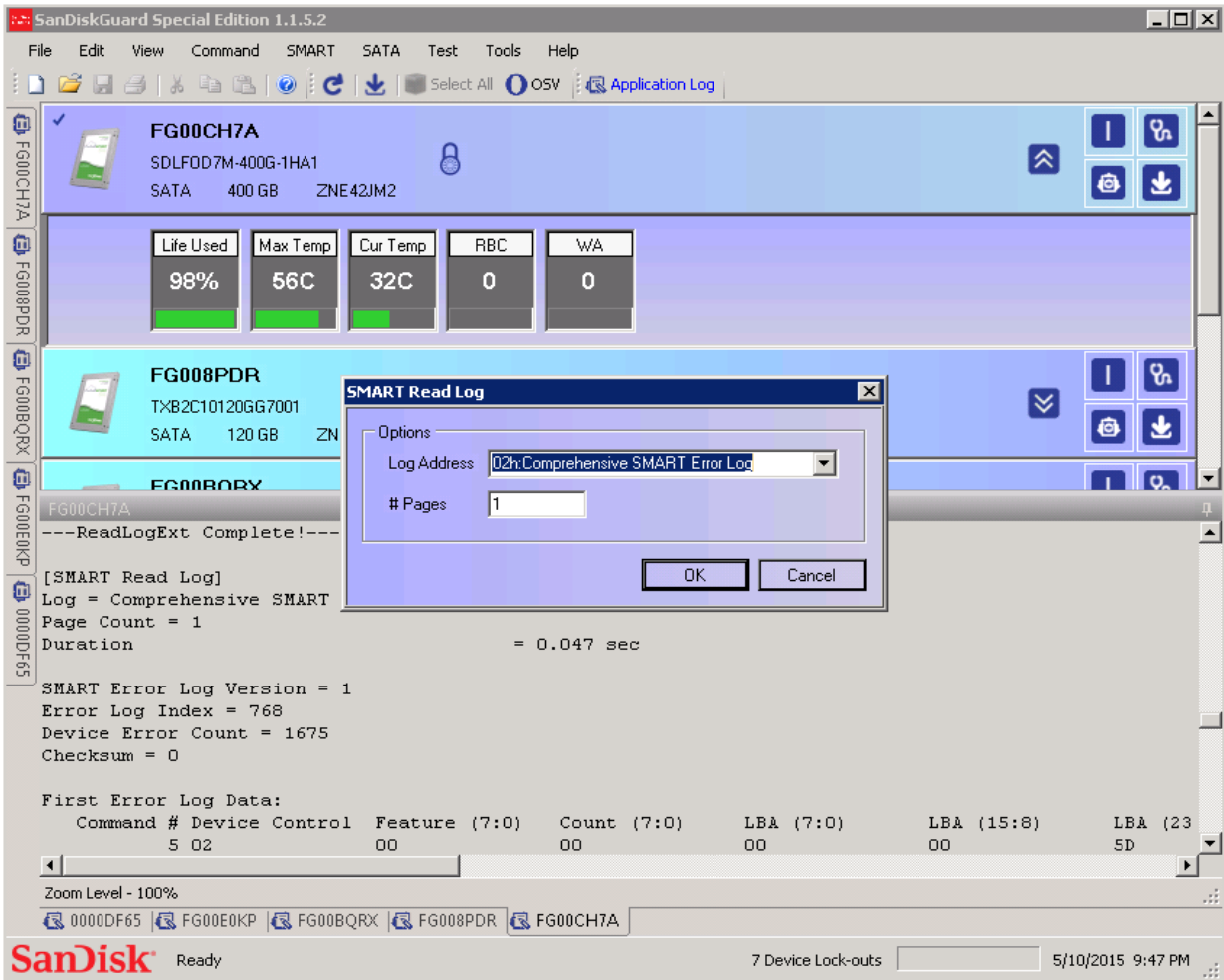
To use SATA Enable, select **SMART > Enable**.

## 6.6 SMART Read Log

SATA devices have a set of SMART log addresses for device data and SMART Command Transport. See section [SMART Self-test, on page 35](#) for SMART Command Transport.

SanDisk Guard displays a list of all SMART logs on the selected device. A custom log number may be entered if the desired log is not listed.

To access SATA Read Log, select **SMART > Read Log**.



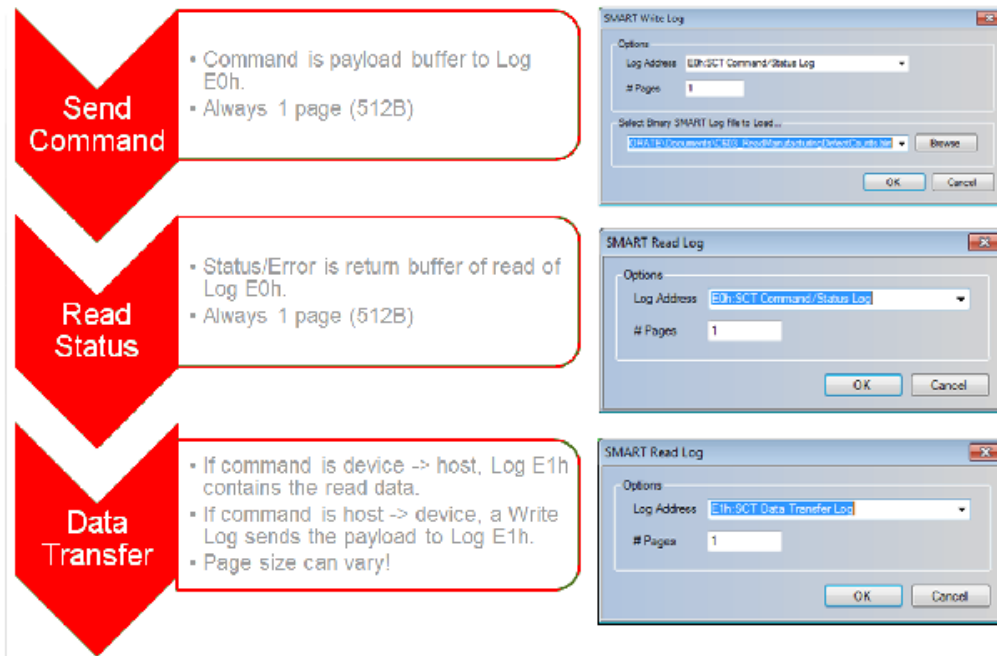
## 6.7 SMART Write Log

SATA write log is mostly used for SMART Command Transport. Select a predefined binary file (created externally to SanDisk Guard) to write to the selected log address.

To access SATA Write log, select **SMART > Write Log**.

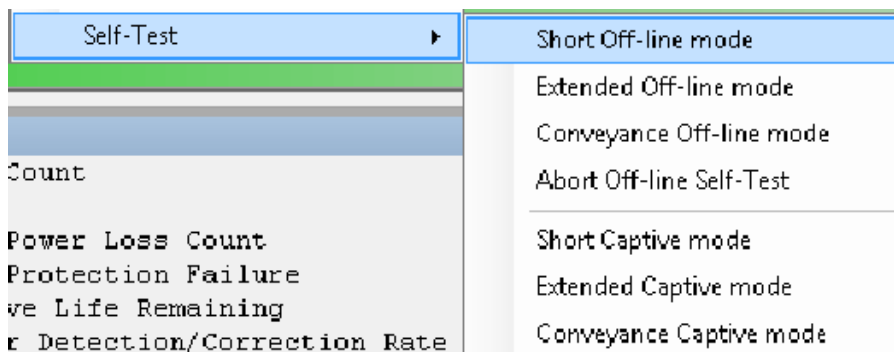
### 6.7.1.0 SMART Command Transport

The SMART Command Transport is a method for a host to send commands and data to a device, and for a device to send data and status to a host using the SMART logs.



## 6.8 SMART Self-test

Using the `Execute Off-line Immediate` command, SanDisk Guard executes SMART self-tests. The `Execute Off-line Immediate` command causes the device to initiate a sequence of events that collects SMART data in an off-line mode and then preserves this data across power and reset events; or processes a vendor specific self-diagnostic test routine in either captive or offline mode.



SATA self-test progress is reported in the device log. The progress bar cycles to indicate background activity. The SMART self-test status displays when complete.

To issue a SMART `Execute Off-line Immediate` command, select **SMART > Self Test > Short Off-line mode**.

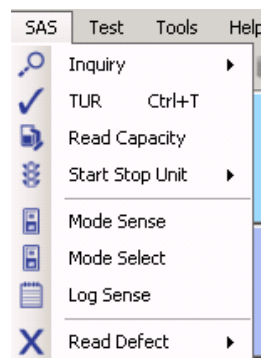
## 7.0 SAS Menu

The SAS menu offers options exclusively available for SAS (SCSI) devices, and lets you run common SAS commands.

### 7.1 Elements

The elements of the SAS menu are as follows:

- Inquiry
  - Standard
  - Vital Product Data
- Test Unit Ready (TUR)
- Read Capacity
- Start Stop Unit
- Mode Sense
- Log Sense
- Read Defect



### 7.2 Inquiry


Inquiry returns identification and configuration device data.

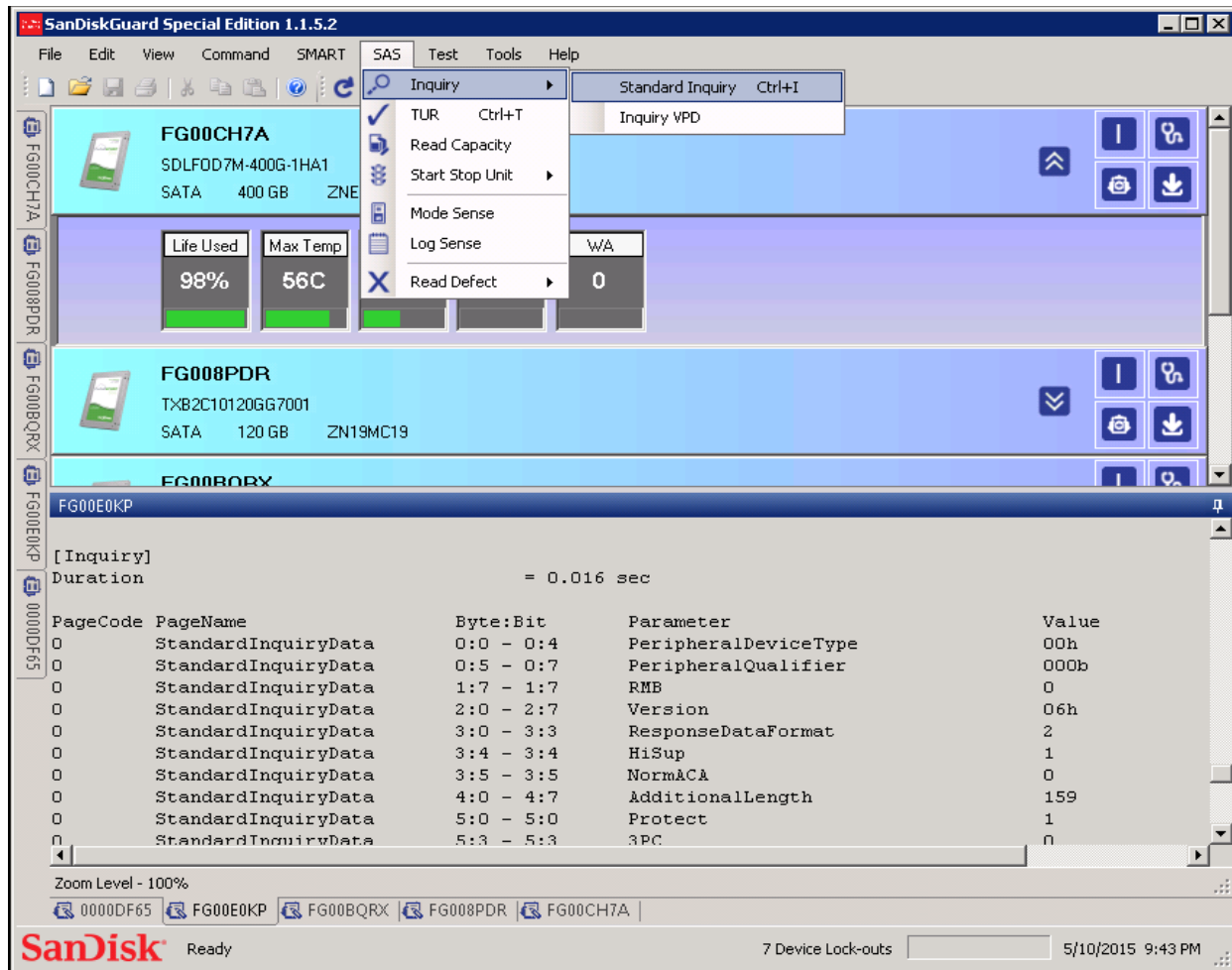
#### 7.2.1 Standard Inquiry

Standard Inquiry returns the following identification and configuration device data:

- Serial Number
- Model Number
- Firmware Version
- Device Type

To open Standard Inquiry, you must select a SAS device:

- Select **SAS > Inquiry > Standard** or
- Click the  quick action button.



## 7.2.2 Vital Product Data Inquiry

Vital Product Data (VPD) is an additional set of inquiry pages containing more detailed identifying and configuration data.

To open Vital Product Data Inquiry, you must select a SAS device.

Select **SAS > Inquiry > Vital Product Data**

## 7.3 Test Unit Ready

Test Unit Ready (TUR) returns the operational and media status of a SAS device.

To view Test Unit Ready:

1. Select **SAS > TUR**.
2. Click **CTRL + T**.

## 7.4 Read Capacity

Read Capacity returns the geometric configuration of the device:

- Max logical block address
- Sector (block) sizes
- Protection information status
- Logical block provisioning

To view the Read Capacity:

1. Select **SAS > Read Capacity**.
2. Click the toolbar button.

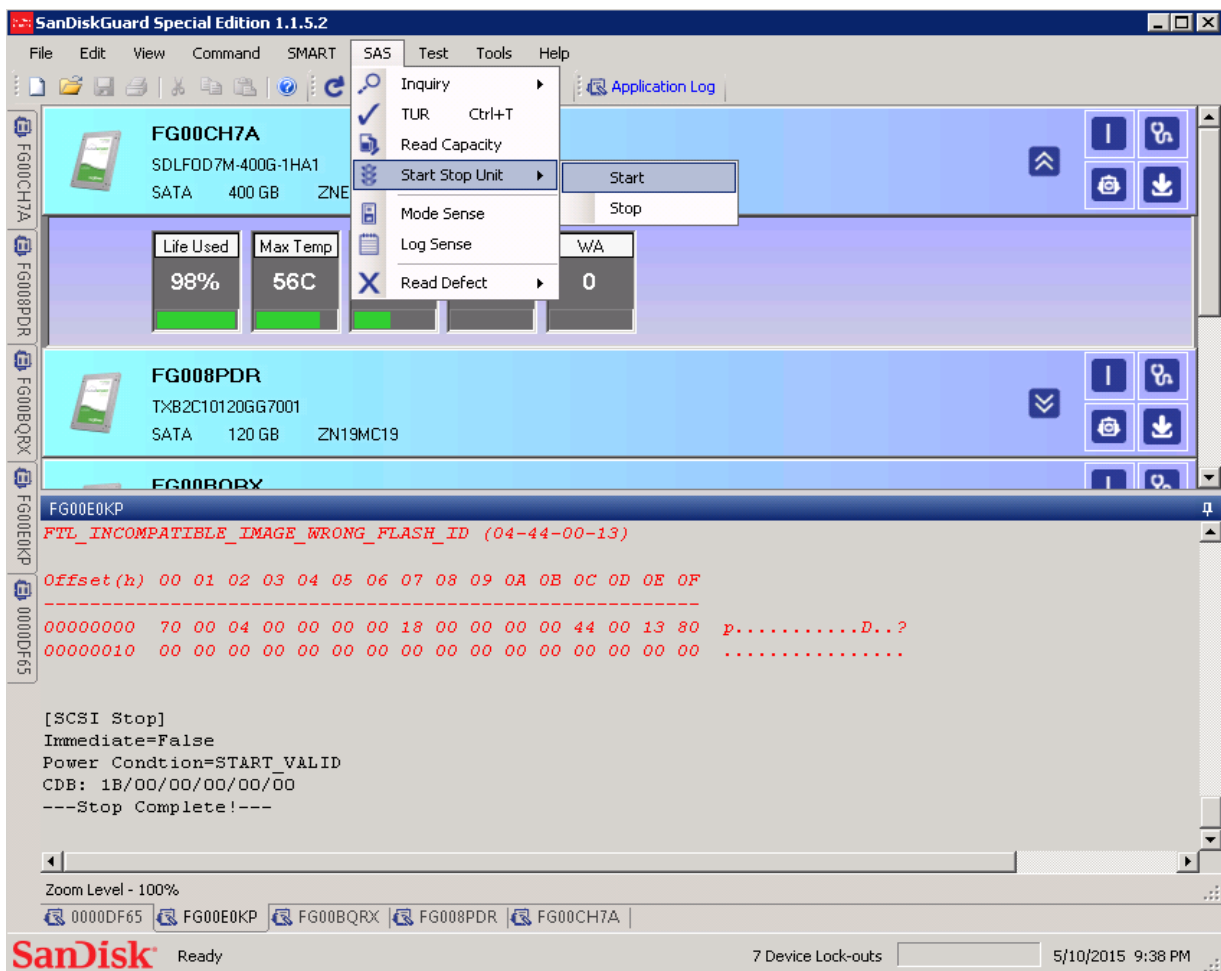
### 7.5 Start Stop Unit

The `Start Stop Unit` command with spinning hard disk drives physically stops (spin down) or starts (spin up) the disk stack to disable or enable access to the medium. SSDs typically implement the `Start Stop Unit` command for legacy installations.

The `Start` command makes the media available for read and write access. If the `Start` command fails, attempts to access the media will also fail.

1. To issue a `Start` command, select **SAS > Start Stop Unit > Start**.
2. To issue a `Stop` command, select **SAS > Start Stop Unit > Stop**.

The `Stop` command makes the media unavailable for read and write access. A stopped device reports a Not Ready error until the device is started.

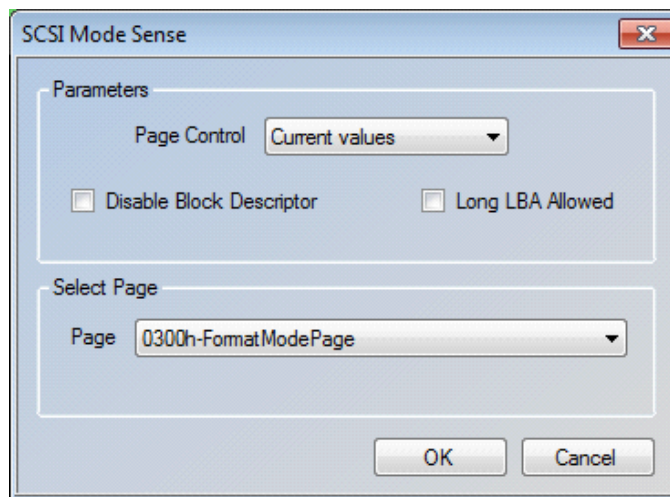


## 7.6 Mode Sense

SCSI Mode Sense is used to read device configuration parameters.

To issue the Mode Sense command:

1. Select **SAS > Mode Sense**.
2. Select the type of value to read:
  - **Current:** Read the current mode page values
  - **Changeable:** Read only the mode page values that can be modified
  - **Default:** Read the mode page values as defined by the current firmware
  - **Saved:** Read the last set of mode page values saved to the device
3. Select a mode page/subpage number from the drop-down list.
4. Click **OK**.



### 7.6.1 Mode Sense Data

Standard SCSI mode pages are decoded for easy reading.

If there is no decoding, select **Tools > Assign Firmware Package**. Then reissue the Mode Sense command.

```
[Mode Sense]
Page = 03h
SubPage = 00h
Duration = 0.001 sec

PageCode PageName ParameterName Value
0x0300 FormatModePage TracksPerZone 0
0x0300 FormatModePage ReplacementSectorsPerZone 0
0x0300 FormatModePage ReplacementTracksPerZone 0
0x0300 FormatModePage ReplacementTracksPerLun 0
0x0300 FormatModePage SectorsPerTrack 1
0x0300 FormatModePage DataBytesPerSector 512
0x0300 FormatModePage Interleave 0
0x0300 FormatModePage TrackSkew 0
0x0300 FormatModePage CylinderSkew 0
0x0300 FormatModePage SURF 0
0x0300 FormatModePage RMB 0
0x0300 FormatModePage HSEC 1
0x0300 FormatModePage SSEC 0

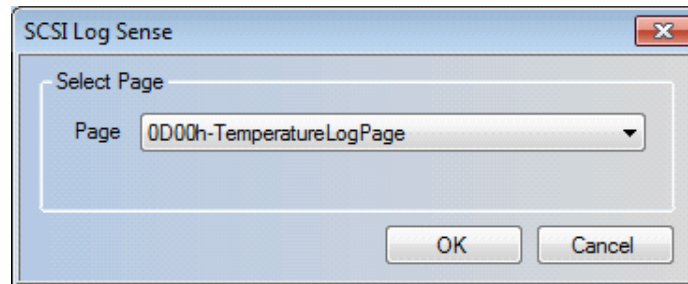
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
----- 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
4
```

## 7.7 Log Sense

SCSI Log Sense reads device statistics and metrics stored in various pages.

To issue a Log Sense command:

1. Select **SAS > Log Sense**.
2. Select a page/subpage combination on the drop-down menu.
3. Click **OK**.



For SAS devices, SMART attributes are stored in the log pages.

### 7.7.1 Log Sense Data

Standard SCSI log pages are decoded for easy reading.

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
-----
00000000 11 00 00 08 00 01 03 04 00 00 00 00  .....
---Log Sense Complete!---

[Log Sense]
Page = 0Dh
SubPage = 00h
Duration          = 0.000 sec

PageCode PageName          Parameter ParameterName Value
0D00     TemperatureLogPage      0D00     Temperature      37
0D00     TemperatureLogPage      0D01     ReferenceTemperature 80

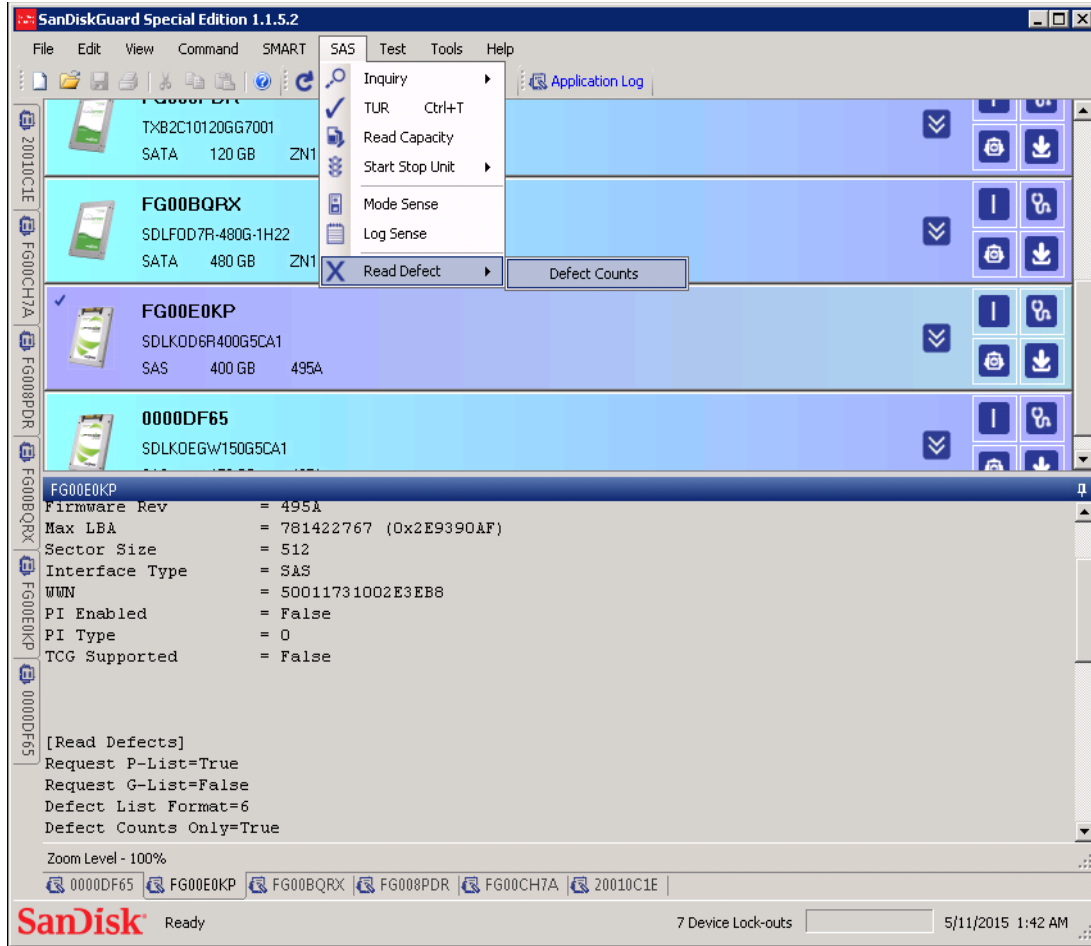
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
-----
00000000 0D 00 00 0C 00 00 02 02 00 25 00 01 02 02 00 50  .....N.....P
---Log Sense Complete!---
```

## 7.8 Read Defect Data

The `Read Defect Data` command requests device transfer of medium defect parameter data from the P-LIST and/or the G-LIST. Defect list entries are decoded to identify defect locations.

To issue a read defect command, select **SAS > Read Defect** <option> where <option> is the desired location of the read defect.





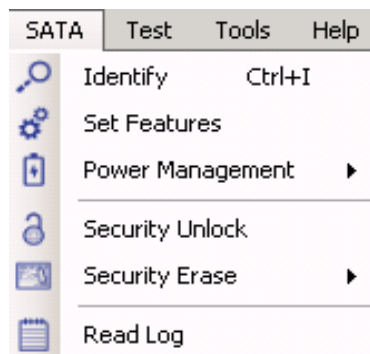
## 8.0 SATA Menu

The SATA Menu contains commands exclusively available for SATA (ATA) devices.

### 8.1 Elements

The elements of the SATA menu are as follows:

- Identify
- Set Features
- Power Management
  - Standby Immediate
  - Idle Immediate
  - Sleep
  - Check Power Mode
- Security Unlock
- Security Erase
- Read Log




### 8.2 Identify

Identify returns device identifying and configuration data:

- Serial Number
- Model Number
- Firmware Version
- Maximum LBA
- Security Status

To view the SATA Identify information:

1. Select **SATA > Identify**.
2. Click the  quick action button or click **CTRL + I**.

### 8.3 SATA Power Management

The SATA `power management` command set features let you control the power condition mode of the device. The power management command set features includes:

- **Standby:** Moves a device to standby and flushes cached data transfers to non-volatile storage. SATA interface remains active. To issue a `Standby Immediate` command, select **SATA > Standby Immediate**.
- **Idle:** Moves a device to idle and flushes cached data transfers to non-volatile storage. SATA interface remains active.

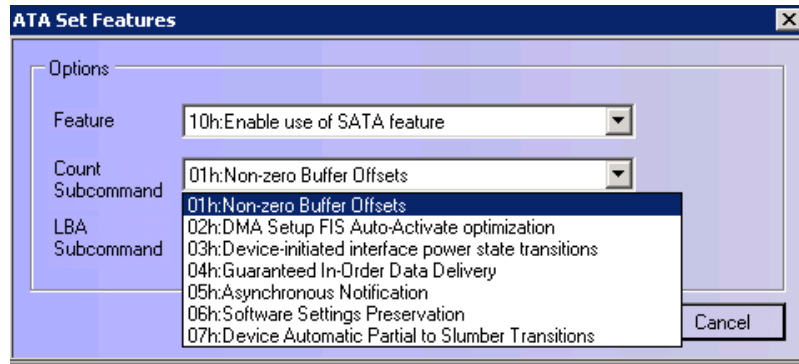
To issue an `Idle Immediate` command, select **SATA > Idle Immediate**.

- **Sleep:** Causes the SATA interface to be inactive. Only a power cycle or hardware reset will restore the SATA interface. To issue a `Sleep` command, select **SATA > Sleep**.
- **Check Power Mode:** Returns the current power-saving and performance mode of the drive. To issue a `Check Power Mode` command, select **SATA > Check Power Mode**.

### 8.4 Set Features

Set Features enables control of several ATA device features and options.

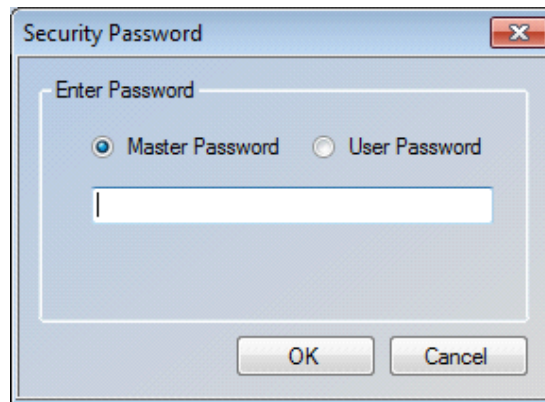
1. Select **SATA > Set Features**.
2. Select a feature.
3. If applicable, select a feature-specific parameter.
4. Click **OK**.



### 8.5 Security Feature Set

The Security Feature Set includes unlock and erase. To issue security commands, the password must be entered. There are two passwords:

- **Master:** Used to unlock the device if the user password is lost or if an administrator requires access (for example, to repurpose a device).
- **User:** Creates a lock to block processing of some commands, including preventing access to all user data on the device. It is used to unlock the device to allow access.



### 8.5.1 Security Unlock

Security Unlock allows access to the device user data and clears the security status field in the identify device.

To issue a security unlock, select **SATA > Security Unlock**.

### 8.5.2 Security Erase (Normal)

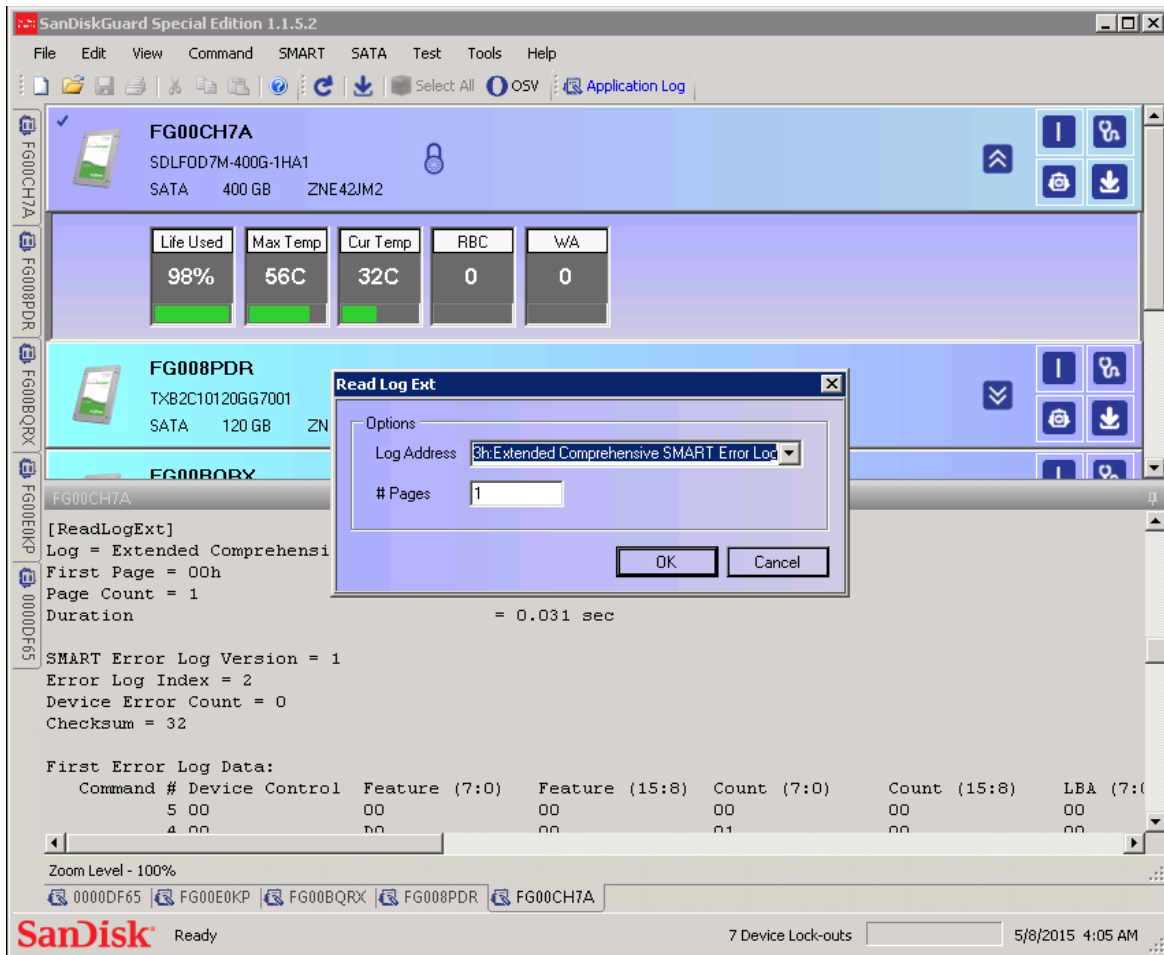
After setting the password, Security Erase (Normal) will replace the contents of LBA 0 to the native max address with all binary zeros or all binary ones. Security will also be disabled, unlocking the device.

To issue a Security Erase (Normal), select **SATA > Security Erase > Normal**.

**NOTE:** Normal is the only Security Erase type currently available.

## 8.6 SATA Read Log

Read Log lets you read standard and vendor-unique logs in a SATA device.



To view the SATA Read Log:

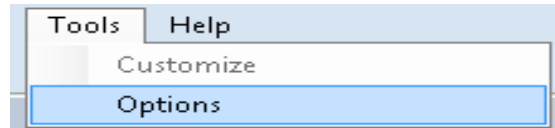
1. Select **SATA > Read Log**.
2. Select a log from the drop-down menu or enter a log address and the length.
3. Click **OK**.

## 9.0 Tools Menu

The tools menu has features for configuring SanDisk Guard behavior and capabilities with the following features:

### 9.1 Elements

The elements of the tools menu are as follows:



### 9.2 Options

Options configures the operating and user interface elements of SanDisk Guard.

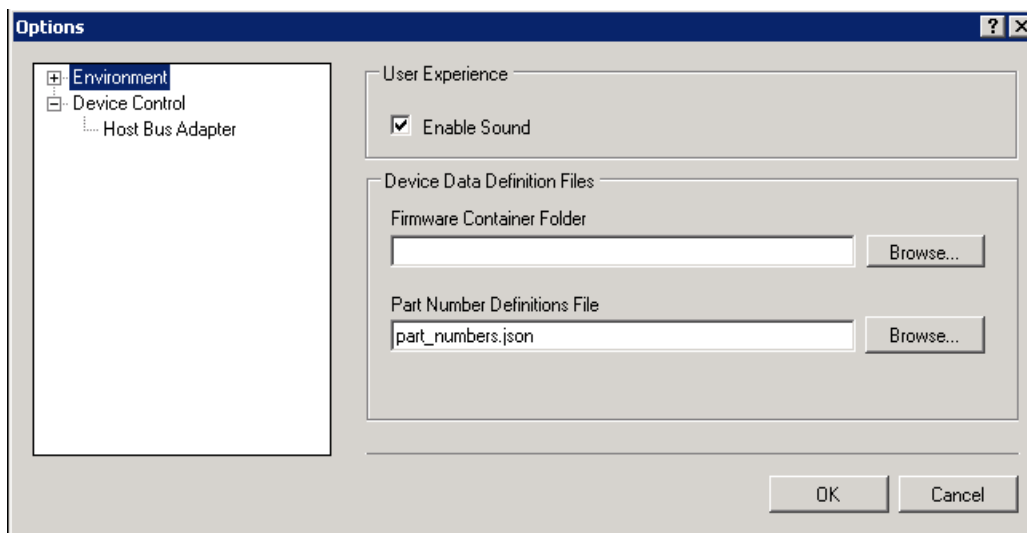
#### 9.2.1 Environment Options

Environment Options let you customize the user interface elements and behaviors.

To access the environment options:

1. Select **Tools > Options**.
2. Check the options you want to enable.
3. Click **OK**.

Currently, the only available customization is Enable Sounds, which when checked, causes SanDisk Guard to beep upon the completion of a long running process, such as downloading firmware. You can select the device data definition files.



## 9.2.2 Device Control

Device Control lets you set the host bus adapter and access device error handling options.

To access the Device Control menu:

1. Select **Tools > Options**.
2. Select **Device Control**.
3. Browse for the current selected HBA.
4. Click **OK**.

Currently, there are no options available. Only LSI 9200 series HBAs may be used.