



# REFERENCE GUIDE

Preliminary

## Technical Reference for SMARTGuard

September 2013, Rev 1  
PN: 61-MANG000016



[www.smartstoragesys.com](http://www.smartstoragesys.com)



## 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.

## Preliminary Notice

As of the date of this document, the contents of these pages are in the preliminary stage, have not been verified, and are subject to change. Contact SMART Storage Systems for current information.

SMART Storage Systems, Inc.  
39870 Eureka Dr.  
Newark, CA 94560  
Tel: (510) 623-1231  
Fax: (510) 623-1434  
[www.smartstoragesys.com](http://www.smartstoragesys.com)

An ISO 9001 certified company.

## Disclaimer

No part of this document may be copied or reproduced in any form or by any means, or transferred to any third party, without the prior written consent of an authorized representative of SMART Storage Systems, Inc. ("SMART"). The information in this document is subject to change without notice. SMART assumes no responsibility for any errors or omissions that may appear in this document, and disclaims responsibility for any consequences resulting from the use of the information set forth herein. SMART makes no commitments to update or to keep current information contained in this document. The products listed in this document are not suitable for use in applications such as, but not limited to, aircraft control systems, aerospace equipment, submarine cables, nuclear reactor control systems and life support systems. Moreover, SMART does not recommend or approve the use of any of its products in life support devices or systems or in any application where failure could result in injury or death. If a customer wishes to use SMART products in applications not intended by SMART, said customer must contact an authorized SMART representative to determine SMART's willingness to support a given application. The information set forth in this document does not convey any license under the copyrights, patent rights, trademarks or other intellectual property rights claimed and owned by SMART. The information set forth in this document is considered to be "Proprietary" and "Confidential" property owned by SMART.

ALL PRODUCTS SOLD BY SMART ARE COVERED BY THE PROVISIONS APPEARING IN SMART'S TERMS AND CONDITIONS OF SALE ONLY, INCLUDING THE LIMITATIONS OF LIABILITY, WARRANTY AND INFRINGEMENT PROVISIONS. SMART MAKES NO WARRANTIES OF ANY KIND, EXPRESS, STATUTORY, IMPLIED OR OTHERWISE, REGARDING INFORMATION SET FORTH HEREIN OR REGARDING THE FREEDOM OF THE DESCRIBED PRODUCTS FROM INTELLECTUAL PROPERTY INFRINGEMENT, AND EXPRESSLY DISCLAIMS ANY SUCH WARRANTIES INCLUDING WITHOUT LIMITATION ANY EXPRESS, STATUTORY OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

The SMART Storage Systems logo, SMART Storage Systems, Optimus, XceedIOPS, Guardian, FlashGuard, EverGuard, and DataGuard are trademarks of SMART Storage Systems. All other trademarks and registered trademarks are the property of their respective owners.

## REVISION HISTORY

Date	Revision	Section(s)	Description
September 2013	01	All	Preliminary release.

Preliminary

**TABLE OF CONTENTS**

<b>1.0</b>	<b>Introduction</b> .....	<b>2</b>
<b>2.0</b>	<b>Installation</b> .....	<b>3</b>
<b>2.1</b>	<b>Installation Requirements</b> .....	<b>3</b>
<b>2.2</b>	<b>Editions</b> .....	<b>3</b>
<b>2.3</b>	<b>Installation Procedure</b> .....	<b>4</b>
<b>3.0</b>	<b>User Interface</b> .....	<b>6</b>
<b>3.1</b>	<b>Elements of User Interface</b> .....	<b>6</b>
<b>3.1.1</b>	<b>Device Bar</b> .....	<b>7</b>
<b>3.1.2</b>	<b>Quick Action Buttons</b> .....	<b>8</b>
<b>3.1.3</b>	<b>Device Health</b> .....	<b>8</b>
<b>3.1.4</b>	<b>Device Status Panels</b> .....	<b>9</b>
<b>3.1.5</b>	<b>Activity Log</b> .....	<b>10</b>
<b>3.1.6</b>	<b>Status and Progress Bar</b> .....	<b>10</b>
<b>3.2</b>	<b>Tool Bar</b> .....	<b>10</b>
<b>3.2.1</b>	<b>Toolbar Menu Options</b> .....	<b>10</b>
<b>3.2.2</b>	<b>Interface Specific Menus</b> ....	<b>15</b>
<b>3.3</b>	<b>Device Lock-out</b> .....	<b>15</b>
<b>3.4</b>	<b>Session Logging</b> .....	<b>15</b>
<b>4.0</b>	<b>Test Menu</b> .....	<b>16</b>
<b>4.1</b>	<b>Elements</b> .....	<b>16</b>
<b>4.2</b>	<b>Diagnostic Report</b> .....	<b>17</b>
<b>4.3</b>	<b>Event Log</b> .....	<b>18</b>
<b>4.4</b>	<b>Core Dump</b> .....	<b>18</b>
<b>4.5</b>	<b>Marking the Event Log</b> .....	<b>19</b>
<b>4.5</b>	<b>Panic Logs</b> .....	<b>19</b>
<b>4.5.1</b>	<b>Generate a Panic Log</b> .....	<b>19</b>
<b>4.5.2</b>	<b>Extract a Panic Log</b> .....	<b>19</b>
<b>4.5.3</b>	<b>Panic Log Seek</b> .....	<b>20</b>
<b>4.5.4</b>	<b>Panic Log Erase</b> .....	<b>20</b>
<b>4.6</b>	<b>Drive Self Test</b> .....	<b>21</b>
<b>4.4</b>	<b>Vendor-Unique Device Unlock</b> .....	<b>22</b>
<b>5.0</b>	<b>Command Menu</b> .....	<b>23</b>
<b>5.1</b>	<b>Elements</b> .....	<b>23</b>
<b>5.2</b>	<b>Refresh</b> .....	<b>23</b>
<b>5.3</b>	<b>Download Firmware</b> .....	<b>24</b>
<b>5.4</b>	<b>Format</b> .....	<b>24</b>
<b>5.5</b>	<b>Sequential Write and Read</b> .....	<b>24</b>
<b>5.6</b>	<b>Random Write and Read</b> .....	<b>25</b>
<b>5.7</b>	<b>Command Builder</b> .....	<b>25</b>
<b>6.0</b>	<b>SMART Menu</b> .....	<b>26</b>
<b>6.1</b>	<b>Elements</b> .....	<b>26</b>
<b>6.2</b>	<b>Read Attributes</b> .....	<b>27</b>
<b>6.2.1</b>	<b>SATA Read Attributes</b> .....	<b>27</b>
<b>6.2.2</b>	<b>SAS Read Attributes</b> .....	<b>27</b>
<b>6.3</b>	<b>SATA Return Status</b> .....	<b>27</b>
<b>6.4</b>	<b>SATA Disable</b> .....	<b>27</b>
<b>6.5</b>	<b>SATA Enable</b> .....	<b>27</b>
<b>6.6</b>	<b>SATA Read Log</b> .....	<b>27</b>
<b>6.7</b>	<b>SATA Write Log</b> .....	<b>28</b>
<b>6.7</b>	<b>SCT Command Transfer</b> .....	<b>28</b>
<b>6.8</b>	<b>SATA Self Test</b> .....	<b>29</b>
<b>7.0</b>	<b>SAS Menu</b> .....	<b>30</b>
<b>7.1</b>	<b>Elements</b> .....	<b>30</b>
<b>7.2</b>	<b>Inquiry</b> .....	<b>30</b>
<b>7.2.1</b>	<b>Standard Inquiry</b> .....	<b>30</b>
<b>7.2.2</b>	<b>Vital Product Data</b> .....	<b>31</b>
<b>7.3</b>	<b>Test Unit Ready</b> .....	<b>31</b>
<b>7.4</b>	<b>Read Capacity</b> .....	<b>31</b>
<b>7.5</b>	<b>Start Stop Unit</b> .....	<b>31</b>
<b>7.6</b>	<b>Mode Sense</b> .....	<b>32</b>
<b>7.6.1</b>	<b>Mode Sense Data</b> .....	<b>32</b>
<b>7.7</b>	<b>Log Sense</b> .....	<b>33</b>
<b>7.7.1</b>	<b>Log Sense Data</b> .....	<b>33</b>
<b>7.8</b>	<b>Read Defect Data</b> .....	<b>33</b>
<b>8.0</b>	<b>SATA Menu</b> .....	<b>34</b>
<b>8.1</b>	<b>Elements</b> .....	<b>34</b>
<b>8.2</b>	<b>Identify</b> .....	<b>34</b>
<b>8.3</b>	<b>SATA Power Management</b> .....	<b>35</b>
<b>8.4</b>	<b>Set Features</b> .....	<b>35</b>
<b>8.5</b>	<b>Security Feature Set</b> .....	<b>36</b>
<b>8.5.1</b>	<b>Security Unlock</b> .....	<b>36</b>
<b>8.5.1</b>	<b>Security Erase (Normal)</b> .....	<b>36</b>
<b>8.6</b>	<b>ATA Read Log</b> .....	<b>37</b>
<b>8.6.1</b>	<b>Log Addresses 3Eh</b> .....	<b>37</b>
<b>9.0</b>	<b>Tools Menu</b> .....	<b>38</b>
<b>9.1</b>	<b>Elements</b> .....	<b>38</b>
<b>9.2</b>	<b>Assign Firmware Package</b> .....	<b>38</b>
<b>9.3</b>	<b>Options</b> .....	<b>39</b>
<b>9.3.1</b>	<b>Environment Options</b> .....	<b>39</b>
<b>9.3.2</b>	<b>Device Control</b> .....	<b>39</b>
<b>9.3.3</b>	<b>Plug-Ins</b> .....	<b>40</b>
<b>9.3.4</b>	<b>HSAS and HSATA Plug-Ins</b> ...	<b>41</b>

## **1.0 INTRODUCTION**

This document is a technical reference for SMARTGuard and provides information about the installation, user interface, and diagnostic options of this product.

SMARTGuard is a Windows-client application intended for use only with SMART Storage products. SMARTGuard is a multi-device diagnostic tool which is user- and customer-configurable and is available to internal and external customers of SMART Storage Systems.

SMARTGuard is not a performance-benchmarking tool, nor is it based on HSAS/HSATA technology.

Preliminary

## 2.0 INSTALLATION

This section describes the installation requirements, various editions of SMARTGuard, and the installation procedure.

### 2.1 Installation Requirements

- **LSI 9200-series SAS/SATA HB-**
- **MS Windows XP and 7, 32-bit or 64 bit**
- **MS .NET Framework 4.0:** Included in each release folder
- **Released Installation Folder:** Can be found at the following link:
  - \\lsr-tew-data02\Groups\Test Engineering\Share-RW\Released\_Software\SMARTGuard

**NOTE:** Only external editions should ever be given to a customer. External editions include the OEM and CUST editions.

### 2.2 Editions

There are six editions of SMARTGuard which support six unique customer needs. The editions are as follows in descending order of features:

- **ENG:** Engineering Edition
- **FAE:** Field Support Edition
- **MFG:** Factory Support Edition
- **RMA:** RMA Edition
- **OEM:** Special Edition
- **CUST:** Standard Edition

Currently, only three editions of SMARTGuard are available: Engineering, Field Support, and Special (customer edition.) See the table below for the features included in each of the available editions.

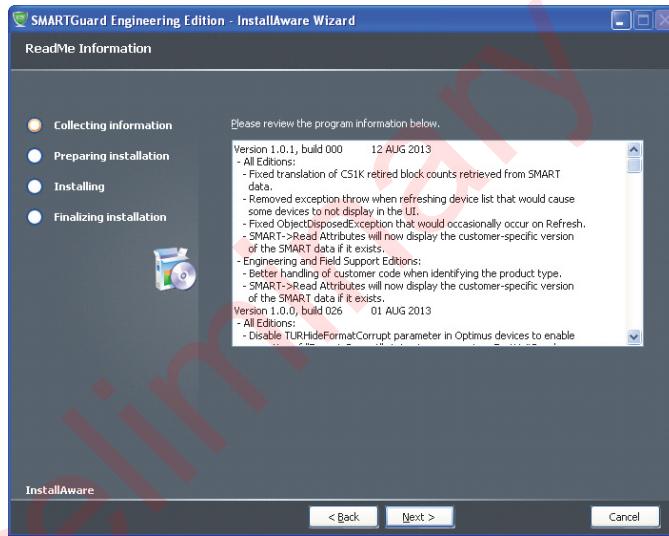
Features	Engineering	Field Support	Special
Internal Use Only	x	x	
External Use Only			x
Plug-Ins	x	x	
Automated Code Assignment	x		
Manual Code Assignment	x	x	
Device Unlock	x	x	
Diagnostic Reports	x	x	x
Command Builder	x	x	

Features	Engineering	Field Support	Special
Code Download	x	x	x
Write/Read	x	x	x

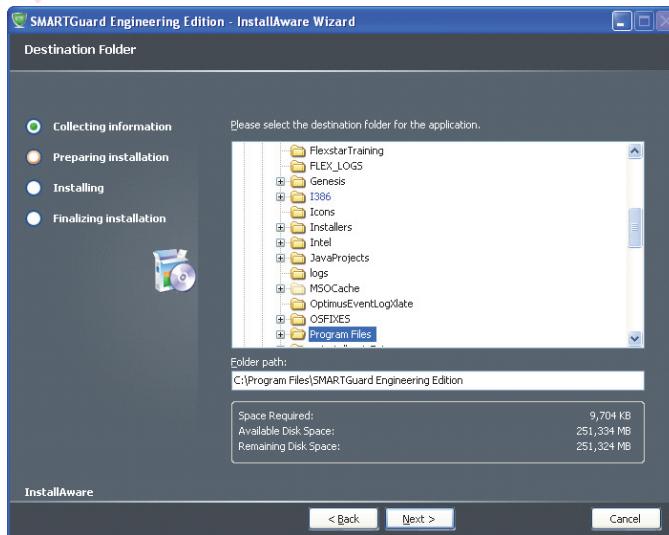
## 2.3 Installation Procedure

### To install SMARTGuard:

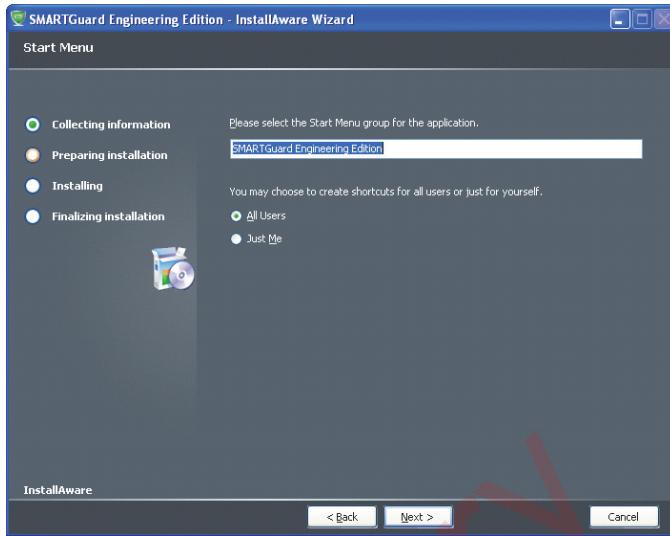
1. Double click the **SMARTGuard\_<edition>-<version>\_<internal\external>.exe** file.
2. Click **Next** at the welcome screen to continue.
3. Review the release notes to see the most recent changes. Then click **Next** to continue.



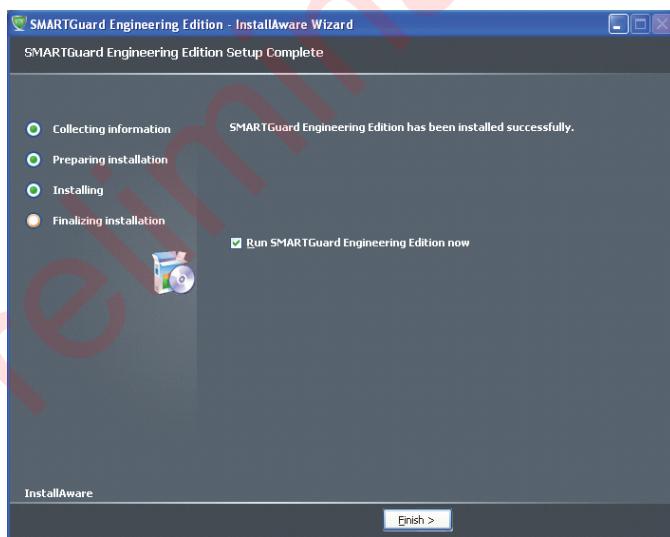
4. Select the location where you would like to install SMARTGuard or use the default location. Click **Next** to continue.



5. Enter the name of the SMART menu group and select whether shortcuts are for your account only or for all users. Click **Next** to continue.



6. Click **Next** again to begin the installation process.
7. When prompted, click **Finish**. You will have the option to launch SMARTGuard after you close the installer by checking the Run SMARTGuard box.

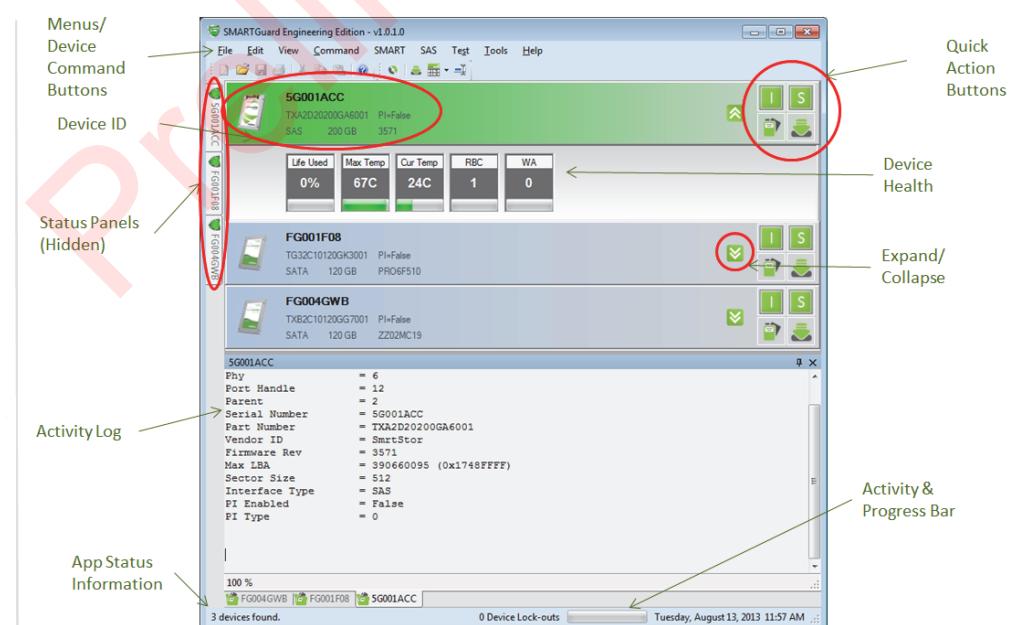


## 3.0 USER INTERFACE

### 3.1 Elements of the User Interface

The SMARTGuard interface provides options for querying, monitoring, and sending commands. The elements of the user interface are as follows:

- **Device Bar:** Contains device information and indicates whether the device is selected. The device bar also 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

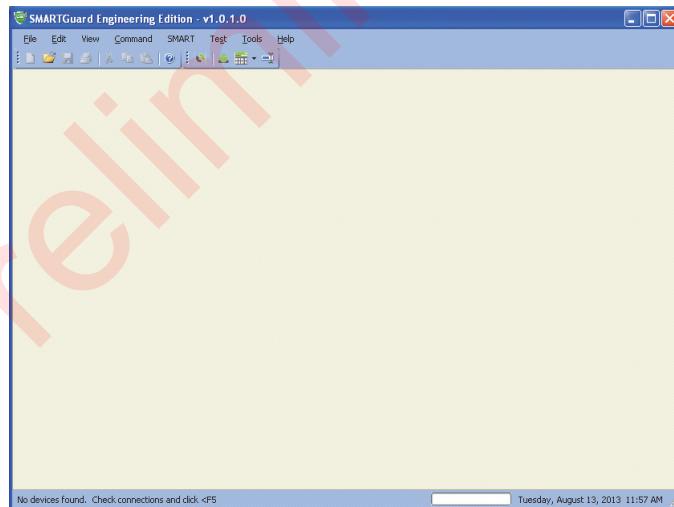
The device bar displays the connected devices as well as options for configuring and monitoring the devices. SMARTGuard will automatically search for connected devices when launched. To issue a command to a device, it must be selected. To select a device, left click the device bar. To select more than one device, hold CTRL while left clicking on the desired devices. A green bar signifies that the device is selected. Menu selections will only affect selected devices.



For each device displayed, the device bar also displays device health information and quick action buttons. See section 3.1.2 for quick action buttons and section 3.1.3 for device health.

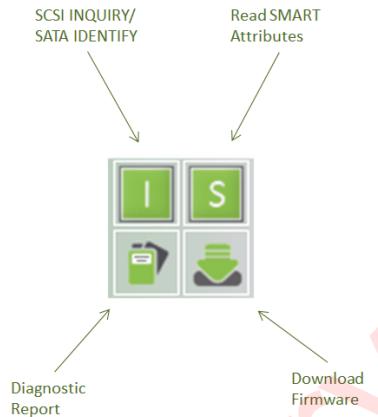
**NOTE:**

If SMARTGuard does not detect any devices connected, a blank screen will be displayed. In the case that a blank screen is displayed, check that devices are connected to an LSI HBA, the devices are powered on, and SMARTGuard is running as administrator. **Refresh** the page (**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 a SAS/SCSI device or Identify for a SATA/ATA  , Download Firmware  , Diagnostic Report  , and Read S.M.A.R.T. Attributes  .

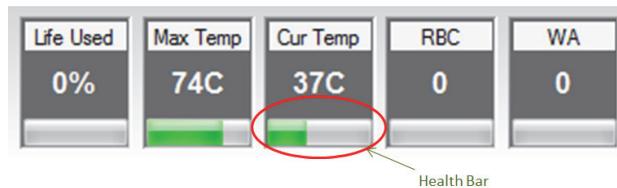


### 3.1.3 Device Health

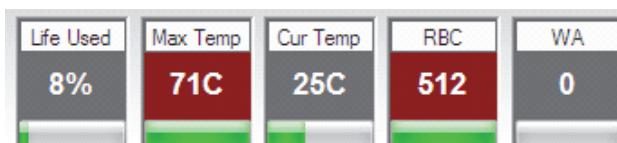
The SSD health information is displayed for all connected devices. The significance of each component of the device health is as follows:

- 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 S.M.A.R.T. threshold. The health information can be expanded or collapsed for each device by using the arrow  buttons on the device bar. To expand the health bar to be visible, click the down arrow  and to collapse it so that it becomes hidden, click the up arrow  .



If a device has tripped a S.M.A.R.T. threshold, the tripped attribute will turn red.

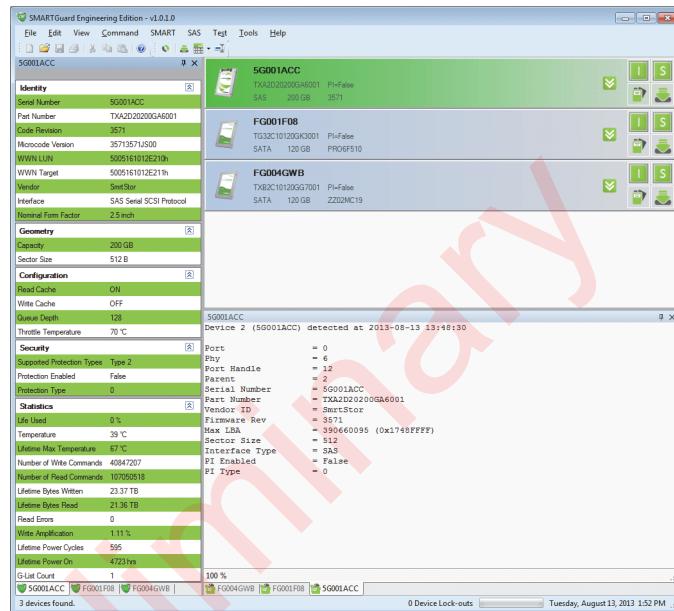


### 3.1.4 Device Status

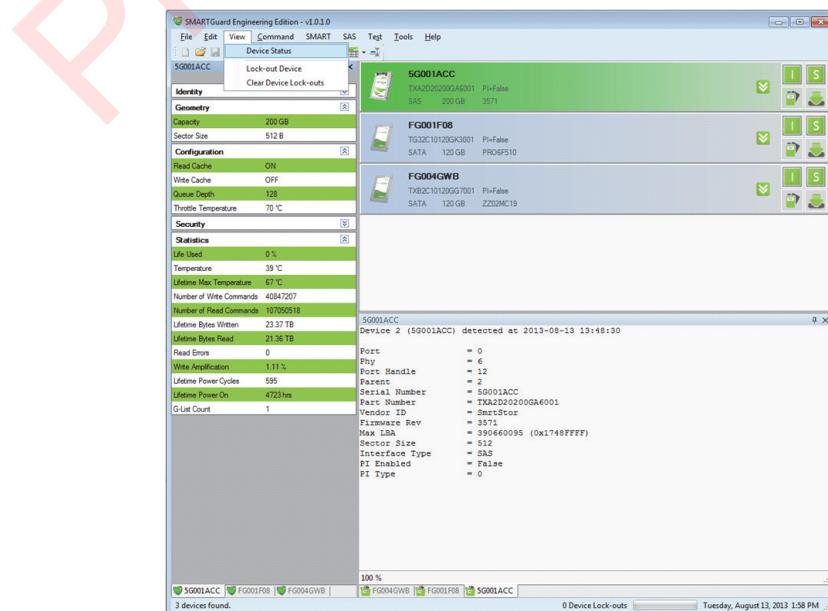
Device status panels display identifying, configuration, and status information about a device:

- Identity
- Geometry
- Configuration
- Security
- Statistics

Each category then contains applicable information. The 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.

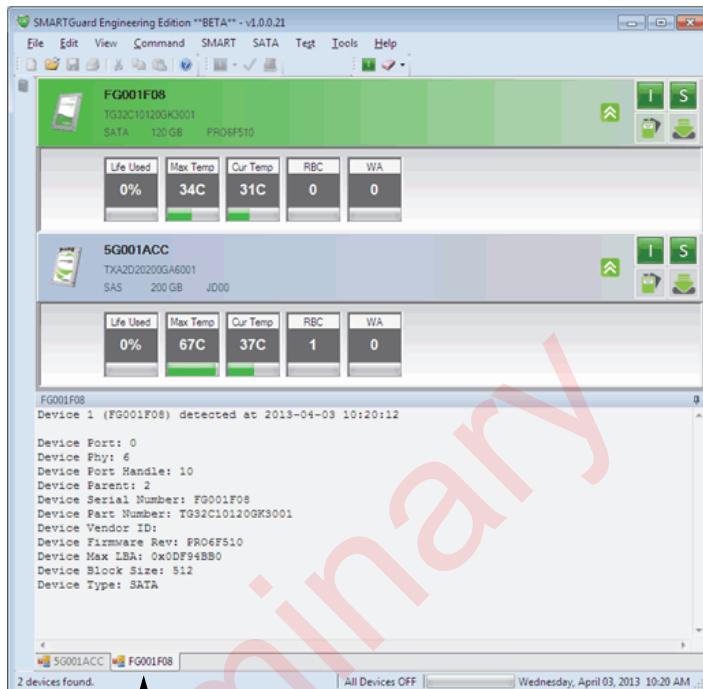


Each group is expandable and collapsible. To restore a hidden or closed status panel, select View > Device Panel



### 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\SMARTGuard\Logs.

### 3.1.6 Status and Progress Bar

The status and progress bar is located at the bottom of the SMARTGuard 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 menu options found in the toolbar. The drop-down menus located in 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	Open		CTRL + O		Allows the user to browse for and open an existing log file.	
	Exit		CTRL + Q		Closes the SMARTGuard application.	
Edit	Select All		CTRL + A		Selects all connected devices.	
Test	Diagnostic Report		CTRL + D		Generates and saves a diagnostic report.	17
	Event Log				Pulls the event log from the drive(s) and stores it in a specified location.	18
	Core Dump				Retrieves the dump logs from the device(s) and stores it in a specified location.	18
	Marking the Event Log				Allows the user to mark the event log for diagnostic and testing purposes.	19
	Panic Log	Generate			Generates a Panic Log.	19
		Extract			Downloads all panic logs to the diagnostic report.	19
		Seek			Displays all available panic logs on LSI/SandForce based products.	20
		Erase			Erases all panic logs on LSI/SandForce based products.	20
	Drive Self Test	Run			Runs a variety of tests and checks on the device(s).	21
		Report			Reports the results of the drive self test.	
	Vendor-Unique Device Unlock				Unlocks the device to allow for many diagnostic logs and features.	22

Menu	Submenu	Command	Shortcut	Quick Access/ Toolbar Button	Action	Page Ref
Command	Refresh		F5	x	Rescans the serial lanes for devices.	23
	Download Firmware				Allows the user to select and download a firmware file onto the selected device(s).	24
	Format	Current			Reformats the drive using the current drive configuration.	24
		512B/ 512B + PI			Reformats the drive to 512 Byte/sector optionally with Protection Information Type 2.	
		520B/520B +PI			Reformats the drive to 520 Byte/sector optionally with protection Information Type 2.	
		528B			Reformats the drive to 528 Byte/sector.	
	Read/Write	Sequential				24
		Random				25
	Command Builder				Allows the user to issue commands not defined in SMARTGuard.	25
SMART	Read Attributes				Retrieves the S.M.A.R.T. attributes data and reformats it into a readable version.	27
	SATA Return Status				Reports whether a S.M.A.R.T. threshold has been exceeded.	27
	SATA Disable				Disables S.M.A.R.T. operations on the drive.	27
	SATA Enable				Enables S.M.A.R.T. operations on the drive.	27
	SATA Read Log				Reads the specified log page using the S.M.A.R.T. Read Log command.	27
	SATA Write Log				Writes data to the specified log page using the S.M.A.R.T. Write Log command.	27
	SCT Command Transport				Sends commands and data from the host to the device and returns data statuses from the device to the host.	28
	SATA Self Test				Issues a SATA Self-Test command.	28

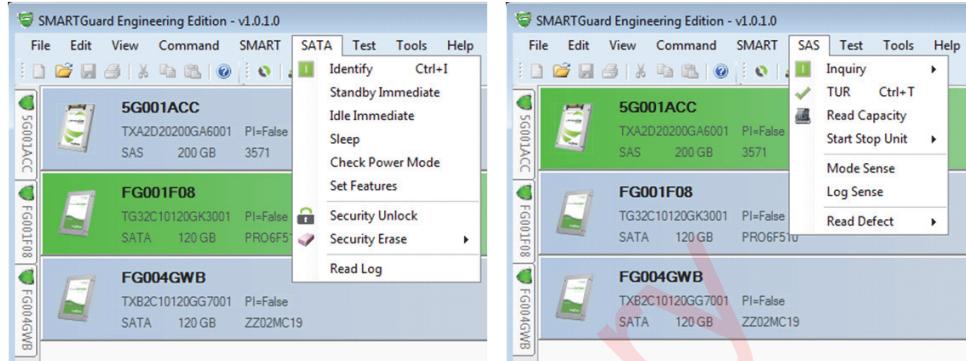
Menu	Submenu	Command	Shortcut	Quick Access/ Toolbar Button	Action	Page Ref
SAS	Inquiry	Standard Inquiry	CTRL + I		Returns standard device identifying and configuration data.	29
		Vital Product Data			Returns detailed device identifying and configuration data.	29
	TUR		CTRL + T		Issues a Test Unit Ready command to the selected device(s).	30
	Read Capacity				Issues a the Read Capacity command to the selected device(s).	30
	Start Stop Unit	Start			Makes the media available for write and read access.	30
		Stop			Makes the media unavailable for write and read access.	
	Mode Sense				Reads device configuration parameters.	31
	Log Sense				Reads device statistics and metrics.	32
SATA	Read Defect	Defect Count			Returns the count of defects (grown and manufacturing) from the selected device(s).	32
	Identify		CTRL + I		Returns the device identification and configuration data.	33
	Standby Immediate				Moves the device(s) to standby.	34
	Idle Immediate				Moves the device(s) to idle.	34
	Sleep				Causes SATA interface to be inactive.	34
	Check Power Mode				Returns the power-saving and performance mode of the device(s).	34
	Set Features				Opens a dialog box that allows you to enable or disable various features.	34
	Security Feature Set	Security Unlock			Sends the Security Unlock command to the selected device(s).	35
		Security Erase			Performs a secure erase (encryption key only) operation on the selected device(s).	
	ATA Read Log				Allows the user to read selected logs.	36

Menu	Submenu	Command	Shortcut	Quick Access/ Toolbar Button	Action	Page Ref
Tools	Assign Firmware Package				Enables decoding of device data.	37
	Environment Options	Enable Sounds			Allows the user to enable sounds to alert the completion of a long-running command.	38
	Device Control				Allows the user to set the host bus adapter and access device error handling options.	38
	Plug-Ins				Allows the user to extend the functionality and features of SMARTGuard.	39
Help	About				Displays information about the version of SMARTGuard.	

### 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 a SAS device is selected will a SAS menu appear in the toolbar. The SAS menu will then offer options exclusively relevant to SAS devices.

The interface-specific menus are available in the toolbar. See section 7.0 for the SAS menu and section 8.0 for the SATA menu.



### 3.3 Device Lock-out

Device lock-out hides devices from the user interface to prevent unintentional actions and commands.

**To exclude devices from the user interface,** select a device, 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 My Documents\SMARTGuard\Logs at the end of every session. A session ends when SMARTGuard is closed.

**To view a log:**

1. Select File > **Open** or;
- Use Open button  on the toolbar or;  
**CTRL + O**.
2. Navigate to My Documents and select SMARTGuard > **Logs**.
3. Click the desired log to open it.

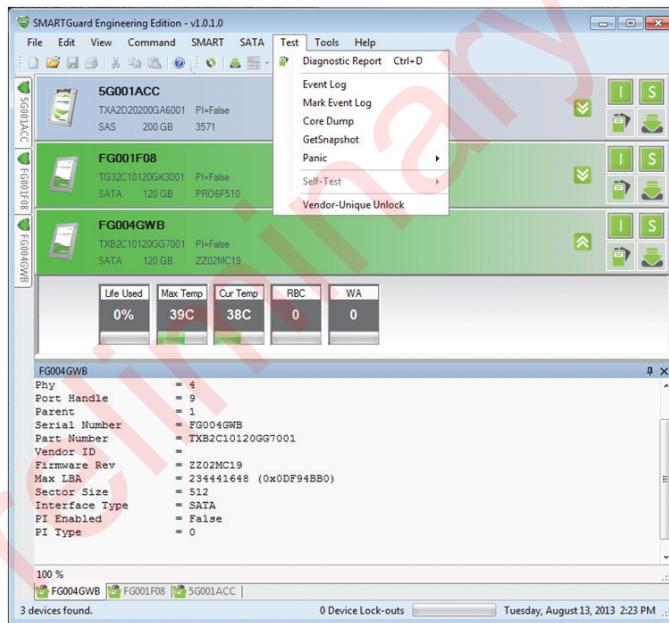
## 4.0 TEST MENU

This section details the diagnostic options of SMARTGuard located in the Test menu.

### 4.1 Elements

The test menu generates information about the device(s) which 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
- Event Log Marking
- Core Dump
- Panic Extraction



## 4.2 Diagnostic Report

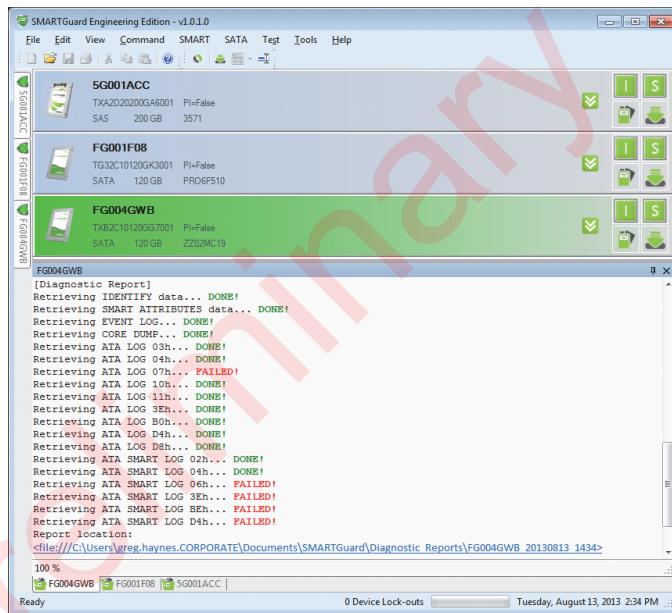
Diagnostic Report retrieves all internal device logs, identification data, and device health data.

**To generate a diagnostic report:**

- Select Test > **Diagnostic Report** or;
- Click the  quick action button or;
- **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.

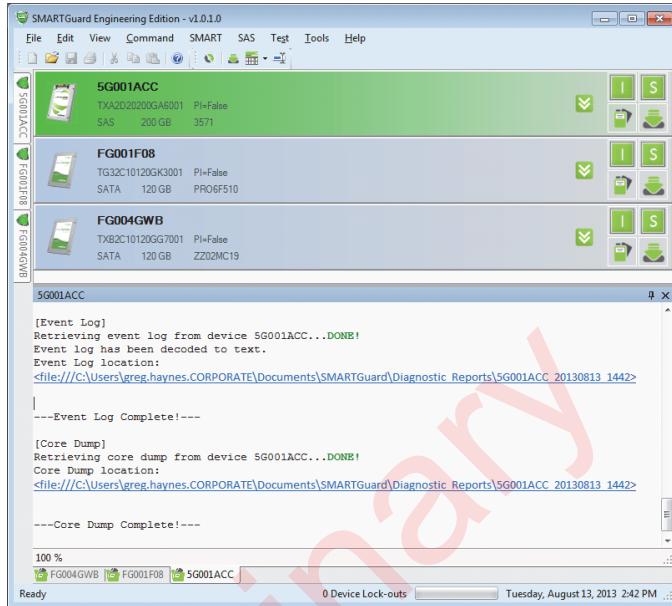
**NOTE:** The password to the zip file is Sm@rtSt0r.



## 4.3 Event Log

If a firmware package is assigned to the device, the event log will be decoded to text.

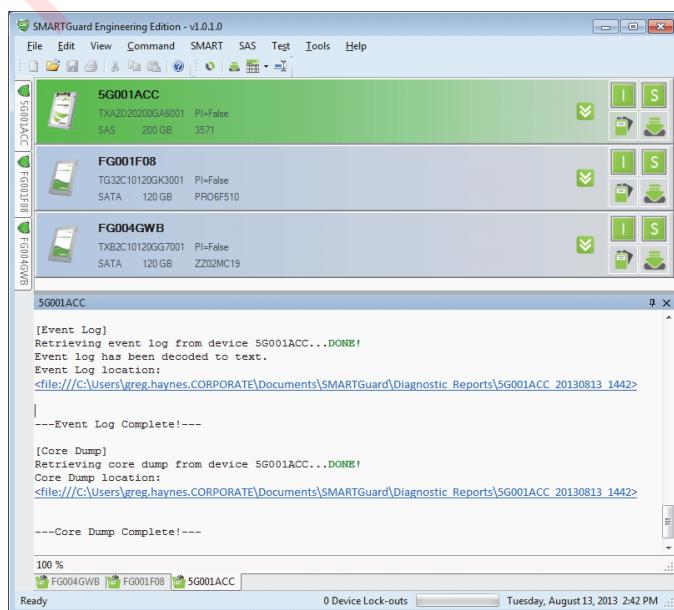
**To view the event log,** select Test > **Event Log**. Event logs can then be viewed by clicking the hyperlinks displayed in the activity log.



## 4.4 Core Dump

Core dumps are never decoded to text.

**To view the core dump,** select Test > **Core Dump**. Core dumps can then be viewed by clicking the hyperlink displayed in the activity log.

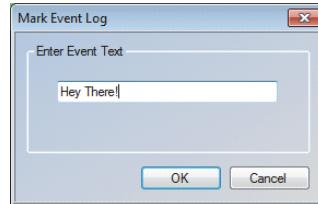


## 4.5 Marking the Event Log

The Optimus and Cloudspeed 1000 products have a mechanism for inserting messages (up to 16 characters) into the event log for debug and testing purposes.

**To mark an event log:**

1. Select Test > **Mark Event Log**.
2. Enter a message in the box.
3. Click **OK**.



The text will immediately be written to the event log.

25928 CPU0 4724:00:00 39 INFO System 0068 Checkpoint host scram information to SPI
25929 CPU0 4724:46:50 39 INFO System 0024 MARK: Hey There!

## 4.6 Panic Logs

### 4.6.1 Generate a Panic Log

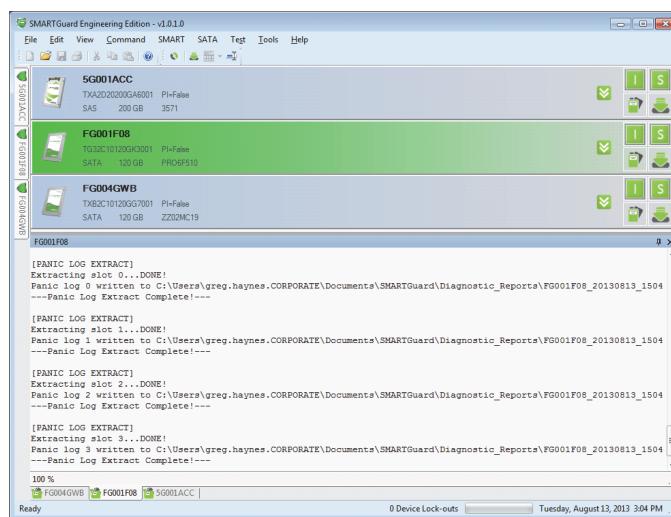
For LSI/SandForce based products, GetSnapshot will generate a panic log. The device must be restarted to release SMARTGuard from a paused state.

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

### 4.6.2 Extract a Panic Log

Extract Panic Log downloads all available panic logs to the Diagnostic\_Report folder in binary form.

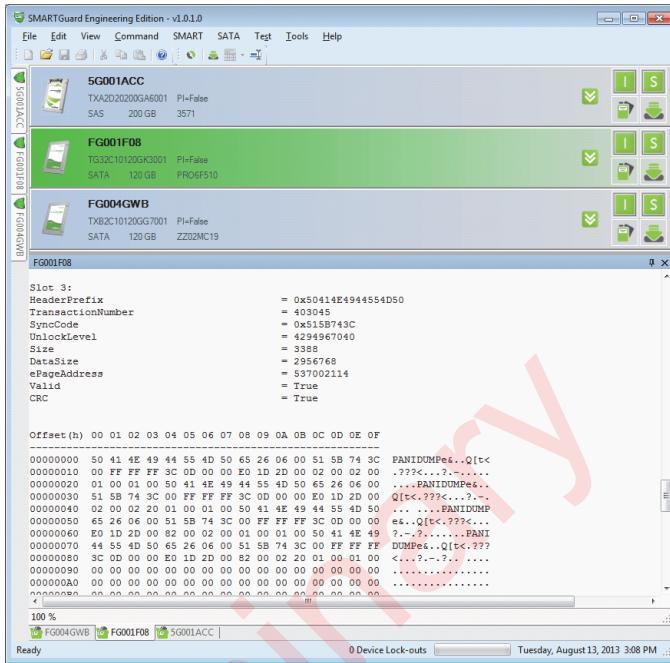
**To extract a panic log**, select Test > Panic > **Extract**.



### 4.6.3 Panic Log Seek

Panic Log Seek allows the user to see what panic logs are available for LSI/SandForce based products. The decoded headers for each panic slot will be displayed along with the raw data returned.

**To seek panic logs, select Test > Panic > Seek.**



### 4.6.4 Panic Log Erase

The user is able to erase all panic logs on an LSI/SandForce based product.

**To erase panic logs, select Test > Panic > Erase.**

## 4.7 Drive Self Test

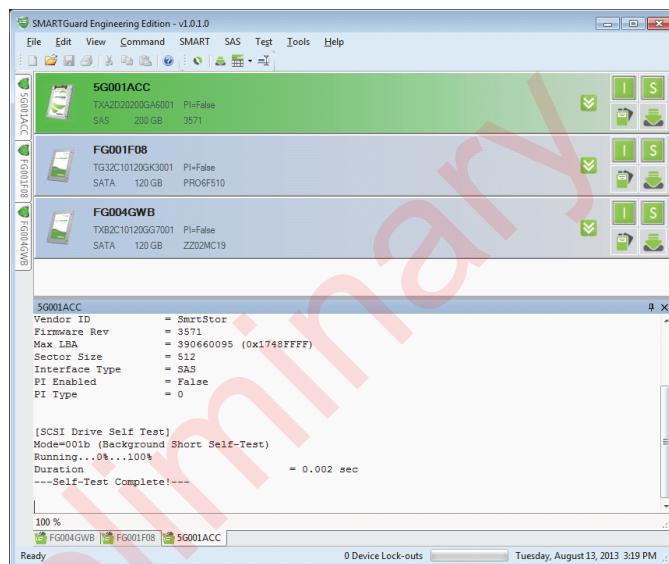
Drive Self Test is part of the SCSI/ SAS standard. Running a drive self test performs the following operations:

- Runs a sanity test on the FTL processor and its memory
- Tests a section of DDR memory
- Tests an area of shared memory
- Checks for S.M.A.R.T. attribute threshold trips

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

**To run SCSI DST,** select Test > DST > **Run Background Short DST.**

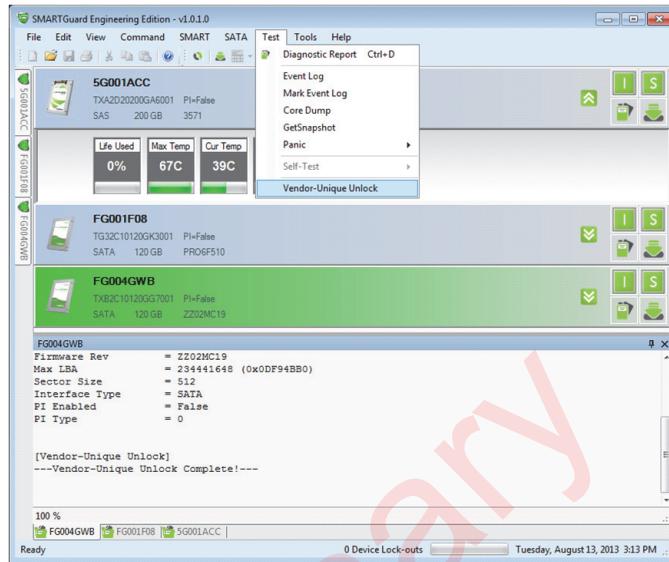
**To view DST results,** select Test > DST > **Report DST Results.**



## 4.8 Vendor-Unique Device Unlock

SATA products typically require an unlock command to allow access to many diagnostic logs and features.

**To unlock a device,** select Test > **Vendor-Unique Unlock**. The device-specific unlock command/procedure will be sent to the selected device(s).

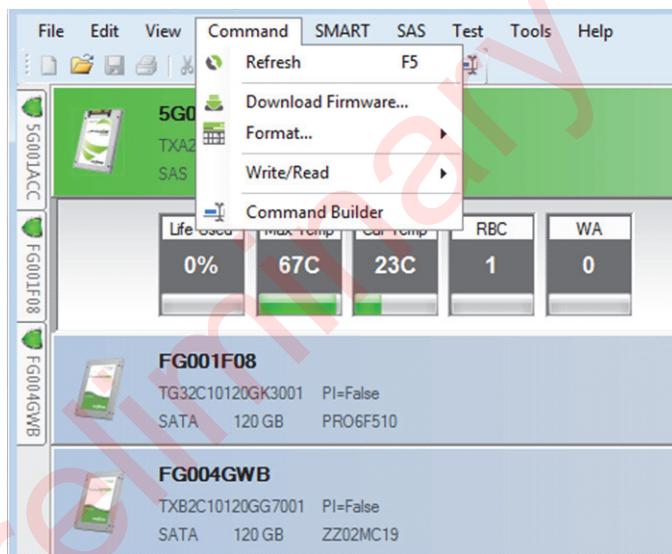


## 5.0 COMMAND MENU

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
- Download Firmware
- Format
- Write/Read
- Command Builder



### 5.2 Refresh

Refresh rescans the serial lanes for devices. Powered off devices will be removed from display when refreshed.

**To refresh SMARTGuard:**

- Select Command > **Refresh** or;
- **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.

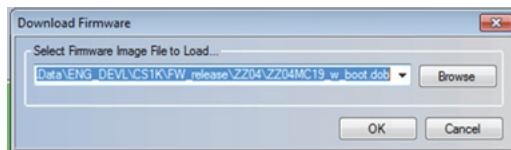
## 5.3 Download Firmware

SMARTGuard allows the user to change the firmware for selected devices.

**To upgrade device firmware:**

1. Select Command > **Download Firmware** or;

Click the  quick action button. The Download Firmware dialog box opens.



2. Enter the path or browse for the firmware binary file to send to the device.
3. Click **OK**.

The firmware binary file will be 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. See section 9.3 to enable sounds.

## 5.4 Format

SMARTGuard supports several different format options. These include:

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

<b>NOTE:</b>	Currently, Format is only available for SCSI/SAS devices.
--------------	---

## 5.5 Sequential Write and Read

Sequential Write and Read has several options which allow the user to:

- Set the logical boundaries
  - Use pre-defined boundaries like "MAX 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/WriteVerify

- 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**.

## 5.6 Random Write and Read

Random Write and Read has several options which allow the user to:

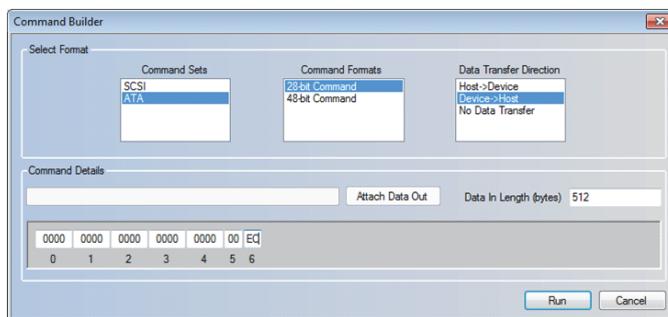
- Set the logical boundaries
- Set the transfer length
- Set operation
  - Write/Read/Verify/WriteVerify
  - Enter the number of random commands
- Set data compare options
  - If writing, load or enter a data pattern to use each transfer
  - Read Data compare is currently disabled

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

## 5.7 Command Builder

Command Builder allows the user to enter any command from an applicable standard or any vendor-unique standard and send it to a device.

- Select any command from the command set, format, and transfer direction to configure the command requirements.
- Enter the command bytes and data out (data going to device) or data in length (data coming from device) if applicable.



To use **Command Builder**:

1. Select Command > **Command Builder**.
2. Enter the desired command information in the fields.
3. Click **Run**.

## 6.0 SMART MENU

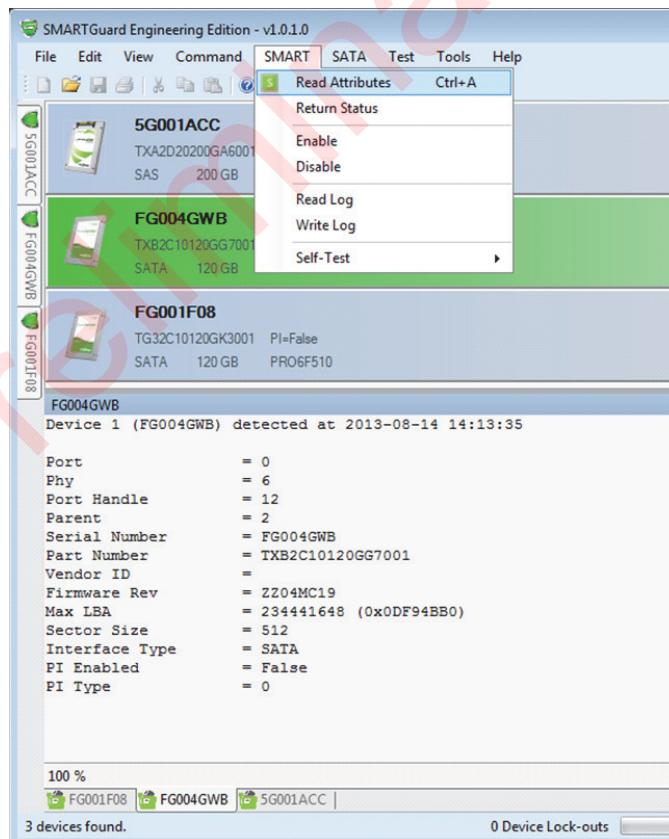
The SMART menu contains tools for working with S.M.A.R.T. data. S.M.A.R.T. is a native element of the ATA/SATA standard and has additional features and commands not found in SCSI/SAS.

### 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 sends a S.M.A.R.T. read data command to the device to read the attribute data. The read data command returns the S.M.A.R.T. 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;
- Use the  quick action button.

### 6.2.2 SAS Read Attributes

On a SAS device, Read Attributes sends a log sense command to the device to read the relevant log page containing the S.M.A.R.T. attributes data. The log sense command returns the S.M.A.R.T. attribute data and reformats it into a readable version.

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

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

- Select SMART > **Read Attributes** or;
- Use the  quick action button.

## 6.3 SATA Return Status

SATA Return Status reports whether a S.M.A.R.T. attribute threshold has been exceeded.

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

If a S.M.A.R.T. threshold has been exceeded, use Read Attributes to view the status of each attribute and identify the exceeded threshold. See section 6.2.

## 6.4 SATA Disable

SMART Disable turns off S.M.A.R.T. attribute measurements and reporting. S.M.A.R.T. commands will report an error if disabled.

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

## 6.5 SATA Enable

SMART Enable restores S.M.A.R.T. reporting if disabled.

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

## 6.6 SATA Read Log

SATA devices have a set of SMART log addresses for device data and SCT command transport. See section 6.8 for SCT Command Transport.

SMARTGuard 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**.

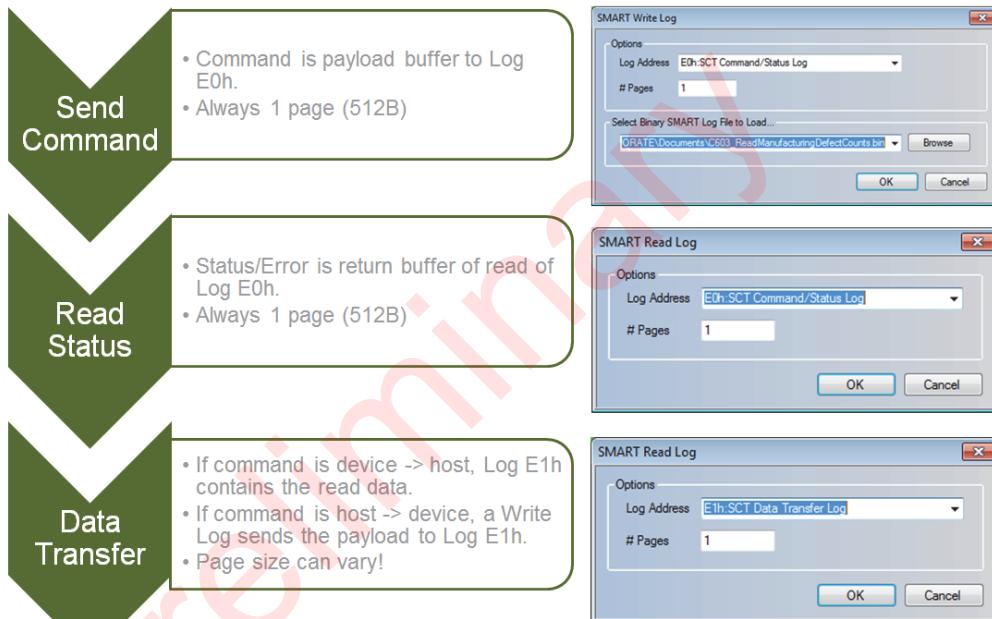
## 6.7 SATA Write Log

SATA write log is mostly used for SCT command transport. Select a pre-defined binary file (created externally to SMARTGuard) to write to the selected log address.

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

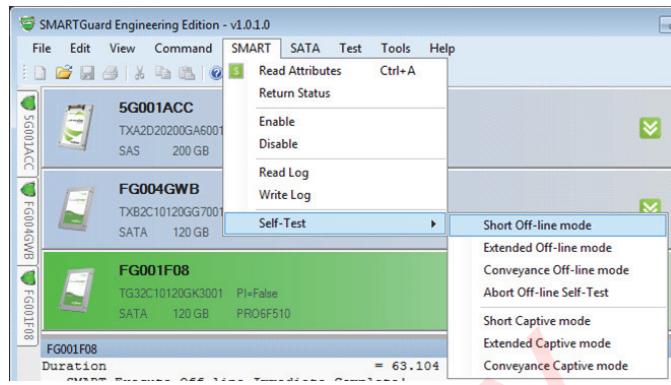
## 6.8 SCT Command Transport

SCT 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.



## 6.9 SATA Self-Test

Using the SMART Execute Off-line Immediate command, SMARTGuard can execute S.M.A.R.T. Self-Tests. The Execute Off-line Immediate command causes the device to initiate a sequence of events that collects S.M.A.R.T. 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 off-line mode.



SATA self-test progress will be reported in the device log. The progress bar will cycle to indicate background activity. When complete, the S.M.A.R.T. self-test status is displayed.

**To issue a SMART Execute Off-line Immediate command,** you must select a SATA device. Select SMART >Self Test > **Short Off-line mode**.

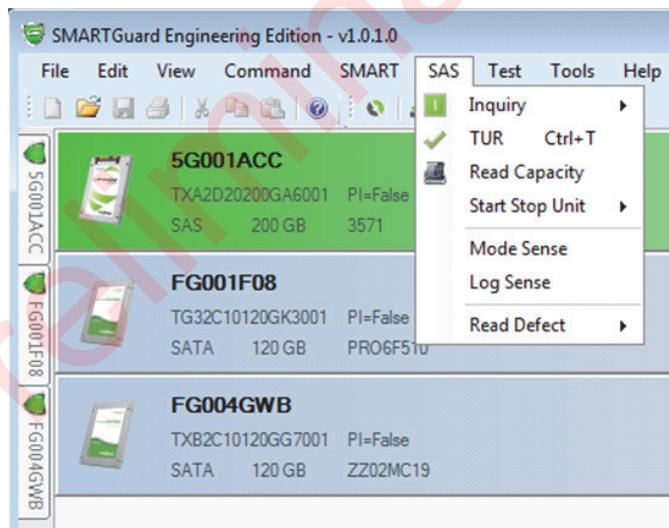
## 7.0 SAS MENU

The SAS menu offers options exclusively available for SAS (SCSI) devices. It allows the user to 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 device identifying and configuration data.

#### 7.2.1 Standard Inquiry

Standard Inquiry returns standard device identifying and configuration 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** or;
- Click the  quick action button.

## 7.3 Test Unit Ready

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

**To view Test Unit Ready:**

- Select SAS > **TUR** or;
- Click the  toolbar button or;
- **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:**

- Select SAS > **Read Capacity** or;
- Click the  toolbar button.

## 7.5 Start Stop Unit

A Start Stop Unit command with spinning hard disk drives would physically stop (spin down) or start (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.

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

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

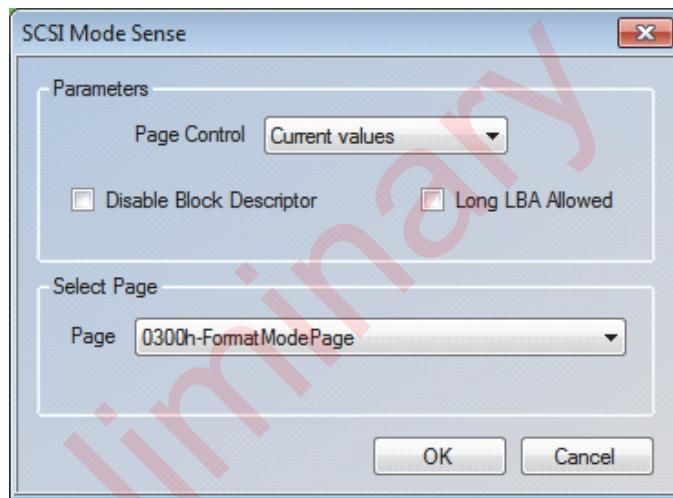
**To issue a Stop command**, select SAS > Start Stop Unit > **Stop**.

## 7.6 Mode Sense

SCSI Mode Sense is used to read device configuration parameters.

**To issue a 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

Mode page data is decoded for easy reading.

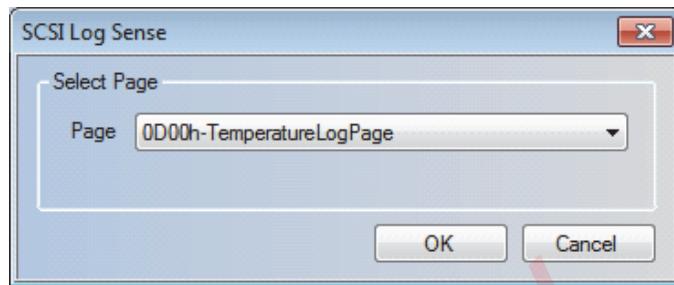
If there is no decoding, select Tools > **Assign Firmware Package**. Then re-issue the Mode Sense command.

## 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, S.M.A.R.T. Attributes are stored in the Log Pages.

### 7.7.1 Log Sense Data

Log page data is decoded for easy reading.

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

## 7.8 Read Defect Data

The Read Defect Data command requests that the device transfer the 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.

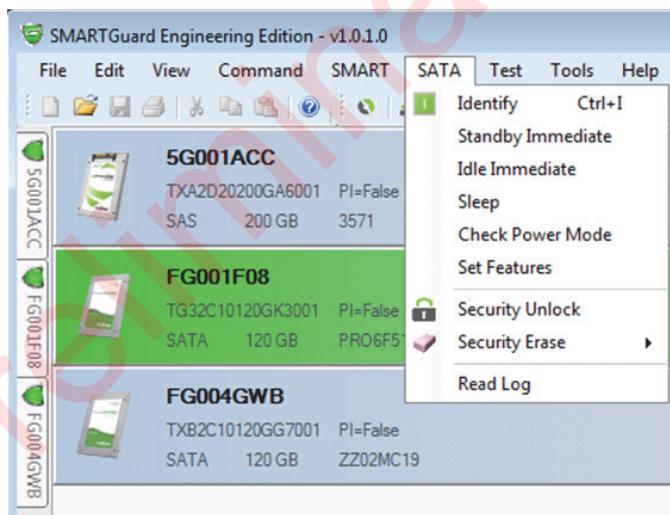
## 8.0 SATA MENU

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

### 8.1 Elements

The elements of the SATA menu are as follows:

- Identify
- Standby Immediate
- Sleep
- Check Power Mode
- Set Features
- 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:**

- Select SATA > **Identify** or;
- Click the quick action button or;

- **CTRL + I.**

## 8.3 SATA Power Management

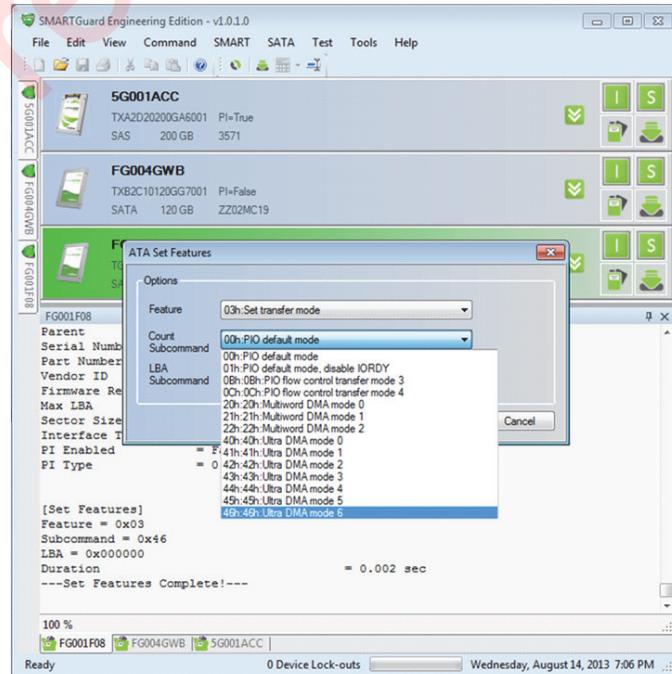
The SATA power management command set features allow the user to control the power condition mode of the device. The power management command set features includes:

- **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 (e.g. 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)

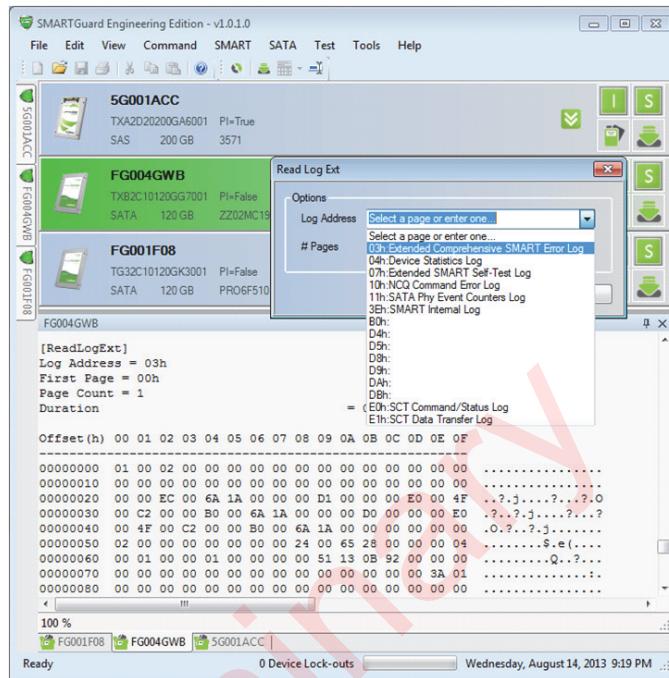
After setting the password, Security Erase Normal will replace the contents of LBA 0 to the native max address with all binary zeros or all binary ones. Security will also be disabled, unlocking the device.

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

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

## 8.6 ATA Read Log

Read Log allows the user to read standard and vendor-unique logs in a SATA device.



### To view the ATA Read Log:

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

### 8.6.1 Log Addresses 3Eh

SMART Storage maintains a log address at 3Eh with SMART Storage unique data. This is decoded for internal versions of SMARTGuard.

**To view the 3Eh Read Log**, select SATA > Read Log > **3Eh**.

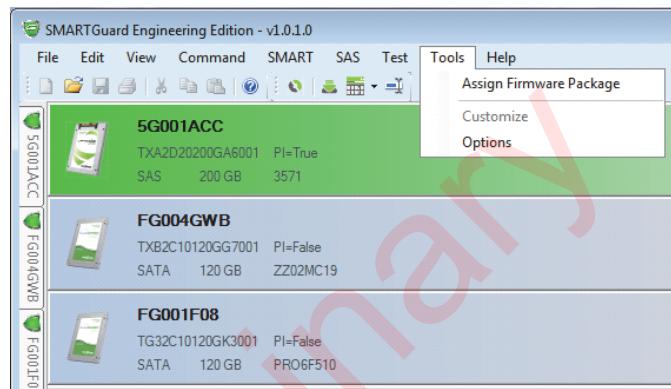
## 9.0 TOOLS MENU

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

### 9.1 Elements

The elements of the Tools menu are as follows:

- Assign Firmware Package
- Options



### 9.2 Assign Firmware Package

Assign Firmware Package enables decoding of device data for the selected device. The firmware package for Optimus and CloudSpeed 1000 devices must be assigned to decode device data. SMARTGuard uses the following files to decode the binary data and format it to readable text:

- `scsi.xml` (`sata.xml` for SATA devices)
- `scsihandler.xml`
- `scsisensecodes.xml`
- `dump_event_log.exe` (decoding of event logs)

**To Assign a firmware package:**

1. Select Tools > **Assign Firmware Package**.
2. Select a firmware zip package or select the desired set of `.xml` files and `dump_event_log.exe`.
3. Click **Open**.

**NOTE:** This process is automatic in the Engineering edition.

## 9.3 Options

Options configures the operating and user interface elements of SMARTGuard.

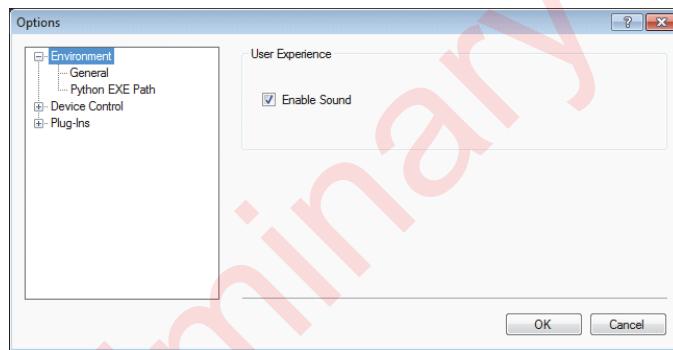
### 9.3.1 Environment Options

Environment Options allow the user to customize the user interface elements and behaviors.

**To access the environment options:**

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

Currently, the only available customization is Enable Sounds, which when checked, will cause SMARTGuard to beep upon the completion of a long running process (e.g. download firmware.)

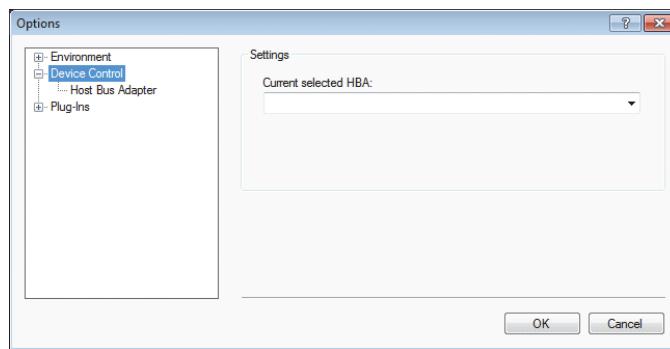


### 9.3.2 Device Control

Device Control allows the user to 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.

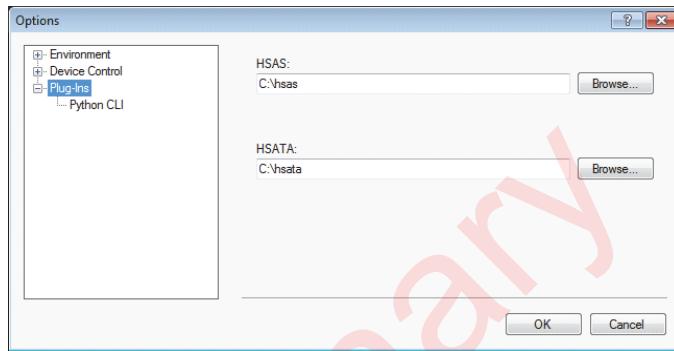
### 9.3.3 Plug-Ins

Plug-Ins allows the user to extend the functionality and features of SMARTGuard with external tools.

Currently SMARTGuard can only be extended with HSAS and HSATA.

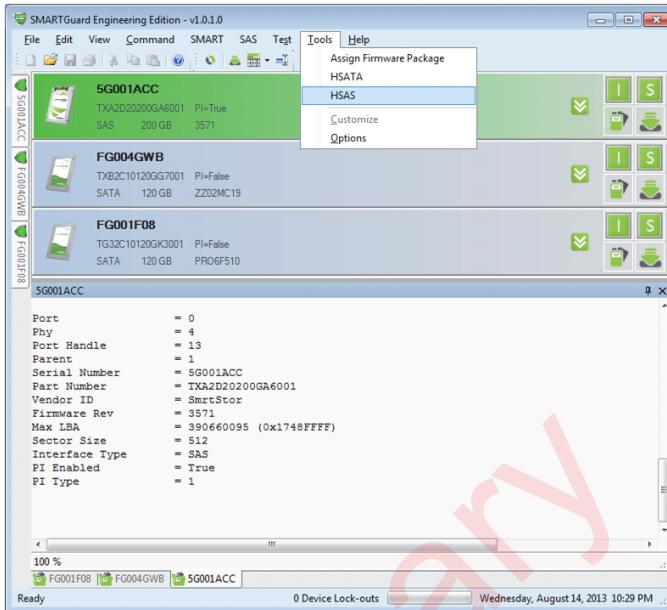
**To use Plug-Ins:**

1. Select Tools > **Options**.
2. Select Plug-Ins.
3. Browse for the desired Plug-in under HSAS or HSATA.
4. Click **OK**.

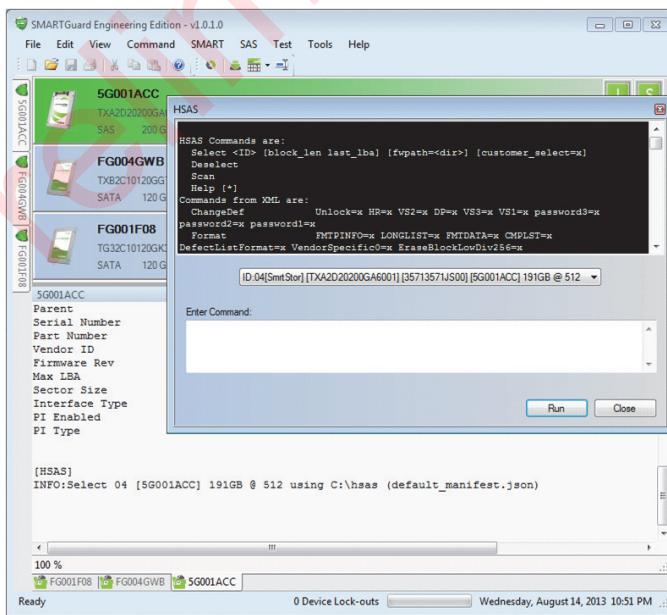


### 9.3.4 HSAS and HSATA Plug-In

After the path has been set to HSAS or HSATA, the menu options become available under Tools.



1. Select the HSAS or HSATA option to launch the CLI tool user interface. When the HSAS or HSATA user interface opens, it automatically scans for devices and displays the HSAS or HSATA Help menu.
2. To select a device in HSAS or HSATA, select it from the drop down list.
3. Once a device is selected, enter any command.



4. Click **Run** to execute the command. The results will print out in the device log.