# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTENTS</td>
<td>2</td>
</tr>
<tr>
<td>PREFACE</td>
<td>4</td>
</tr>
<tr>
<td>HISTORY</td>
<td>4</td>
</tr>
<tr>
<td>RUN THE PROGRAM</td>
<td>5</td>
</tr>
<tr>
<td>CHANGE THE NATIVE SIZE (HPA, DCO, AMAX, SCSI)</td>
<td>9</td>
</tr>
<tr>
<td>HPA AREA</td>
<td>9</td>
</tr>
<tr>
<td>Create hidden area HPA with SET MAX ADDRESS</td>
<td>9</td>
</tr>
<tr>
<td>Remove hidden area HPA</td>
<td>16</td>
</tr>
<tr>
<td>Remove hidden area HPA with SET MAX ADDRESS</td>
<td>16</td>
</tr>
<tr>
<td>Auto remove HPA area</td>
<td>19</td>
</tr>
<tr>
<td>Dump of HPA area</td>
<td>24</td>
</tr>
<tr>
<td>DCO AREA</td>
<td>27</td>
</tr>
<tr>
<td>Create hidden DCO area</td>
<td>27</td>
</tr>
<tr>
<td>Remove hidden DCO area</td>
<td>34</td>
</tr>
<tr>
<td>Remove hidden DCO area with DCO RESTORE</td>
<td>35</td>
</tr>
<tr>
<td>Auto remove DCO area</td>
<td>36</td>
</tr>
<tr>
<td>Dump of DCO area</td>
<td>38</td>
</tr>
<tr>
<td>AMAX AREA</td>
<td>41</td>
</tr>
<tr>
<td>Create AMAX area</td>
<td>41</td>
</tr>
<tr>
<td>Remove AMAX area</td>
<td>46</td>
</tr>
<tr>
<td>ADDRESS OFFSET AREA</td>
<td>49</td>
</tr>
<tr>
<td>Enable OFFS area</td>
<td>49</td>
</tr>
<tr>
<td>Disable OFFS area</td>
<td>59</td>
</tr>
<tr>
<td>SCSI CAPACITY</td>
<td>64</td>
</tr>
<tr>
<td>AUTO REMOVE HIDDEN AREAS</td>
<td>72</td>
</tr>
<tr>
<td>OVERVIEW OF HIDDEN AREAS</td>
<td>75</td>
</tr>
<tr>
<td>SECURITY LOCK THE DEVICE</td>
<td>85</td>
</tr>
<tr>
<td>SECURITY UNLOCK THE DEVICE</td>
<td>85</td>
</tr>
<tr>
<td>Unlock counter</td>
<td>85</td>
</tr>
<tr>
<td>Unlock and disable password</td>
<td>86</td>
</tr>
<tr>
<td>Unlock device</td>
<td>91</td>
</tr>
<tr>
<td>ERASE THE DEVICE</td>
<td>94</td>
</tr>
<tr>
<td>SECURITY ERASE THE DEVICE</td>
<td>94</td>
</tr>
<tr>
<td>SCT WRITE SAME</td>
<td>99</td>
</tr>
<tr>
<td>SEARCH THE DEVICE</td>
<td>116</td>
</tr>
<tr>
<td>Search for string</td>
<td>116</td>
</tr>
<tr>
<td>Search for empty sector</td>
<td>125</td>
</tr>
<tr>
<td>Search for non-empty sector</td>
<td>129</td>
</tr>
<tr>
<td>CHANGE THE LOGICAL SECTOR SIZE</td>
<td>131</td>
</tr>
<tr>
<td>SCSI DRIVES</td>
<td>131</td>
</tr>
<tr>
<td>SATA DRIVES</td>
<td>134</td>
</tr>
<tr>
<td>NVMe DRIVES</td>
<td>137</td>
</tr>
<tr>
<td>SMART</td>
<td>146</td>
</tr>
<tr>
<td>SMART self-tests</td>
<td>146</td>
</tr>
<tr>
<td>NVMe self-test</td>
<td>146</td>
</tr>
<tr>
<td>NVME DEVICE</td>
<td>154</td>
</tr>
<tr>
<td>Examples of some logs for NVMe devices</td>
<td>154</td>
</tr>
<tr>
<td>Examples of some commands for NVMe devices</td>
<td>159</td>
</tr>
</tbody>
</table>
Preface

This is the cookbook of program HDAT2 in pictures for beginners. **The document and images are for program version 7.4 except for updates.**

Images and texts may be subject to change during the development of the program.

There should be the answers in the pictures for questions "How can I do...?"

For a more detailed information see "User's Manual HDAT2".

I am sorry for my English.

---

History

v2.1 HDAT2 7.5 31.1.2022
Updates from version 7.5 have been applied: Address Offset Mode, SCSI Capacity

v2.0 HDAT2 7.4 29.9.2021

v1.1 HDAT2 4.9 8.9.2010

v1.0 HDAT2 4.9 8.9.2010
Run the program

Run the program without parameters:

C:\>hdat2

By pressing the setup key 'S' in the device list you can set the general parameters of the program.
After pressing the ENTER key in the device list you will get the main menu of allowed commands for the given device.

Run the program with the parameter 'd=0' to detect individual PCI controllers on the computer and detect devices only on the selected controller.

C:\>hdat2 /d=0
PCI controller

<table>
<thead>
<tr>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI controller</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Storage</th>
<th>1. SATA AHCI (AMD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage</td>
<td>2. NVMe (Samsung)</td>
</tr>
<tr>
<td>Storage</td>
<td>3. SATA AHCI (AMD)</td>
</tr>
</tbody>
</table>

PCI : Bus/Dev/Func=01h/00h/00h, Base/SubClass=01h/08h, PI=02h, Header=00h
HOST: Vendor=144Dh, Device=A808h, Revision=00h
NAME: Samsung

Detect devices on selected PCI controller.
PCI NVMe devices:
Controller init...
Device setup...

SAMSUNG MZVLB256HAHQ-000H1

Use these detected devices <Y/N> ?

Device list [SAMSUNG MZVLB256HAHQ-000H1]

<table>
<thead>
<tr>
<th>Type</th>
<th>Nr.</th>
<th>Device name</th>
<th>BIOS</th>
<th>LBA</th>
<th>Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>NVMe</td>
<td>1</td>
<td>SAMSUNG MZVLB256HAHQ-000H1</td>
<td></td>
<td></td>
<td>256.00 GB</td>
</tr>
</tbody>
</table>

CTRL=NVMe BAR=DOC0|0000h RAM base/size=2000|0000h/67.11 MB
Device=NVMe/NVMe [Direct Access]
SMART: O.K.
Supported: DST WZ FMT DSM CMP
Please consult the NVMe specification for details on how to use the parameters.
Change the native size (HPA, DCO, AMAX, SCSI)

The hidden area like Host Protected Area (HPA), Device Configuration Overlay (DCO) or Accessible Max Address (AMAX) area, is an area of a hard drive that is not normally visible to BIOS, an operating system, or user.

To create or remove Host Protected Area (HPA) is used the command SET MAX ADDRESS.

To create or remove DCO hidden area is used the command DCO MODIFY or DCO RESTORE.

To create or remove AMAX hidden area is used the command Set Accessible Max Address.

Note: To create or remove DCO area you must first remove an active HPA area. If you want to create both HPA and DCO area first you have to create DCO area without any HPA area. After power off/on you can create HPA area.

If HPA is not supported, the following message is displayed:

![Screenshot](image.png)

**HPA area**

Host Protected Area (HPA)

**Create hidden area HPA with SET MAX ADDRESS**

**Example:** We create HPA area with a size of 100 sectors (50 KB).
Main menu [ST3500413AS]

- Device tests menu
- File system menu
- Device data menu
- SMART/SCT menu
  - SET MAX (HPA) menu
- Device Configuration Overlay (DCO) menu
- Hidden areas menu
- Security menu
- Commands menu

Set Max Address
Set password
Lock
Unlock
Freeze Lock

↓↓ Move ENTER Select ESC Return

HDAT2 Cookbook (c) 2021 CBL

SET MAX (HPA) menu [ST3500413AS]

Set Max Address
Set password
Lock
Unlock
Freeze Lock

SET MAX status: HPA disabled

Allows to redefine the maximum address of the user accessible address space, to create or remove unlocked Host Protected Area (HPA). This command will be aborted in LOCKED or FROZEN mode until the power-on reset.

↓↓ Move ENTER Run ESC Return
By pressing the 'V' you can change so-called the volatile mode from hard settings to soft settings.
<table>
<thead>
<tr>
<th></th>
<th>LBA sectors</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>NATIVE</td>
<td>976,773,168</td>
<td>500.11 GB</td>
</tr>
<tr>
<td>USER</td>
<td>976,773,168</td>
<td>500.11 GB</td>
</tr>
<tr>
<td>HIDDEN</td>
<td>0</td>
<td>0.00 KB</td>
</tr>
<tr>
<td>NEW USER</td>
<td>976,773,068</td>
<td>500.11 GB</td>
</tr>
<tr>
<td>NEW HIDDEN</td>
<td>100</td>
<td>51.20 KB</td>
</tr>
</tbody>
</table>

Used command: SET MAX EXT (48-bits) (change it when an error occurs)
Volatile mode: YES -> hard settings
SET PERMANENTLY: Changes shall preserve over power-up or hardware reset.

Are you sure to run 'Set Max Address' <Y/N>?
HDAT2 Cookbook (c) 2021 CBL

Set Max Address [ST3500413AS]

<table>
<thead>
<tr>
<th>Current</th>
<th>LBA sectors</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>NATIVE</td>
<td>976,773,168</td>
<td>500.11 GB</td>
</tr>
<tr>
<td>USER</td>
<td>976,773,168</td>
<td>500.11 GB</td>
</tr>
<tr>
<td>HIDDEN</td>
<td>0</td>
<td>0.00 KB</td>
</tr>
<tr>
<td>NEW USER</td>
<td>976,773,068</td>
<td>500.11 GB</td>
</tr>
<tr>
<td>NEW HIDDEN</td>
<td>100</td>
<td>51.20 KB</td>
</tr>
</tbody>
</table>

Used command: SET MAX EXT (48-bits) (change it when an error occurs)
Volatile mode: YES -> hard settings
SET PERMANENTLY: Changes shall preserve over power-up or hardware reset.

AHCI CMD7 DEV6 HIGH5 MID4 LOW3 CNT2 FEA1
Before 0037h 0040h 0038h 005Fh 3AC8h 0001h 0000h
After 0050h 0040h 0038h 005Fh 3AC8h 0001h 0000h
Status 50h: BSY DRDY DFSE DWE DREQ ALGN SENS ERR
Error 00h: ICRC UNC MC IDNF MCR ABRT T0NF CCTO

Command completed successfully. Press any key...

HDAT2 Cookbook (c) 2021 CBL

Set Max Address
Set password
Lock
Unlock
Freeze Lock
Auto remove HPA area

SET MAX status: HPA enabled

Allows to redefine the maximum address of the user accessible address space, to create or remove unlocked Host Protected Area (HPA). This command will be aborted in LOCKED or FROZEN mode until the power-on reset.

Move ENTER Run ESC Return
This error message you will see if you try to call the second non-volatile command without power off (e.g. immediately after the first creation of HPA area). So we turn power off and on and try it again.

After pressing the keys 'S' and 'Y' and message 'Command completed successfully', the HPA area is set. The message 'Command aborted' means something is wrong, you can try using the command 'C' key to set 28-bit instead of 48-bit SET MAX command and repeat the procedure.

You can check the settings of hidden areas in the 'Hidden areas menu'.

Second SET MAX command: a power-on reset is required. Press any key...
Main menu [ST3500413AS]

- Device tests menu
- File system menu
- Device data menu
- SMART/SCT menu
- SET MAX (HPA) menu
- Device Configuration Overlay (DCO) menu
  - Hidden areas menu
  - Security menu
  - Commands menu

Overview of hidden areas
Auto remove hidden areas
Dump of HPA area
Detect BEER record

↓↓ Move ENTER Select ESC Return

Hidden areas menu [ST3500413AS]

- Overview of hidden areas
- Auto remove hidden areas
- Dump of HPA area
- Detect BEER record

Active areas: HPA

Summary of hidden areas (HPA, AMAX, DCO, Address Offset).

↓↓ Move ENTER Run ESC Return
Remove hidden area HPA

To remove HPA area you can use SET MAX ADDRESS command or menu option Auto Remove Hidden Areas.

Remove hidden area HPA with SET MAX ADDRESS

Example: We try to remove created HPA area with 100 sectors. We use 48-bit SET MAX ADDRESS command.
SET MAX (HPA) menu [ST3500413AS]

Set Max Address
Set password
Lock
Unlock
Freeze Lock
Auto remove HPA area

SET MAX status: HPA enabled

Allows to redefine the maximum address of the user accessible address space, to create or remove unlocked Host Protected Area (HPA). This command will be aborted in LOCKED or FROZEN mode until the power-on reset.

↑↓ Move ENTER Run ESC Return

HDAT2 Cookbook (c) 2021 CBL
Set Max Address [ST3500413AS]

Current LBA sectors Size
NATIVE 976,773,168 500.11 GB
USER 976,773,068 500.11 GB
HIDDEN 100 51.20 KB <- HPA
NEW USER 976,773,168 500.11 GB <- full native size
NEW HIDDEN 0 0.00 KB <- OK.

Used command: SET MAX EXT (48-bits) (change it when an error occurs)
Volatile mode: YES -> hard settings
SET PERMANENTLY: Changes shall preserve over power-up or hardware reset.

↑↓/HOME/END Change INS Edit C Command V Volatile S Set ESC Abort
<table>
<thead>
<tr>
<th>Current</th>
<th>LBA sectors</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>NATIVE</td>
<td>976,773,168</td>
<td>500.11 GB</td>
</tr>
<tr>
<td>USER</td>
<td>976,773,068</td>
<td>500.11 GB</td>
</tr>
<tr>
<td>HIDDEN</td>
<td>100</td>
<td>51.20 KB &lt;- HPA</td>
</tr>
<tr>
<td>NEW USER</td>
<td>976,773,168</td>
<td>500.11 GB &lt;- full native size</td>
</tr>
<tr>
<td>NEW HIDDEN</td>
<td>0</td>
<td>0.00 KB &lt;- O.K.</td>
</tr>
</tbody>
</table>

Used command: SET MAX EXT (48-bits) (change it when an error occurs)
Volatile mode: YES -> hard settings
SET PERMANENTLY: Changes shall preserve over power-up or hardware reset.

Are you sure to run 'Set Max Address' <Y/N> ?

Command completed successfully. Press any key...
Now the HPA area is removed.

You get an error message 'Command aborted' if you try to remove HPA area with 48-bit SET MAX command, but HPA area was created with 28-bit SET MAX command. So you need to select 28-bit SET MAX command.

**Auto remove HPA area**

There are 2 options: 'Auto remove HPA area' in SET MAX menu or 'Auto remove hidden areas' in Hidden areas menu.
SET MAX (HPA) menu [ST3500413AS]

Set Max Address
Set password
Lock
Unlock
Freeze Lock
Auto remove HPA area

SET MAX status: HPA enabled

This command will be aborted in LOCKED or FROZEN mode until the power-on reset.

Are you sure to run 'SET MAX Auto remove HPA area' <Y/N>?
You can also use the option 'Auto remove hidden areas' in Hidden areas menu.
Overview of hidden areas
  Auto remove hidden areas
  Dump of HPA area
  Detect BEER record

Active areas: HPA

Are you sure to run 'Auto remove hidden areas' <Y/N>?
Removing hidden areas...

HPA area: detected

Using SET MAX command 4B-bits: O.K.
SET MAX full capacity was restored

AMAX area: not detected

DCO area: not detected

Press any key to continue...

Overview of hidden areas
Detect BEER record

Active areas: none

Summary of hidden areas (HPA, AMAX, DCO, Address Offset).
**Dump of HPA area**

**Example:** We have created an HPA area of 100 sectors, which starts at LBA sector 976,773,068. This option allows you to view the contents of this HPA area.
Overview of hidden areas
Auto remove hidden areas
**Dump of HPA area**
Detect BEER record

Active areas: HPA

To dump sectors the area will be temporarily disabled.

Do you want to temporarily disable HPA area <Y/N> ?
I saved the HPA text in the first sector of this area.
DCO area

Device Configuration Overlay (DCO)

Create hidden DCO area
If the device is in DCO frozen state the device shall return command aborted for all DCO commands. In this case see FAQ “How to bypass a Security and/or DCO frozen state?”

If the device is in security lock mode the device shall return command aborted for all DCO commands.

Example: We will try to create DCO area with a size of 50 sectors (25 KB) when device has a HPA area already.
To create or remove DCO area you must first remove an active HPA area. See an error message later.
We got an error message, because we tried to create DCO area with a previously created HPA area. We must first remove an active HPA area before creating DCO area.

**Example:** Now we create DCO area with a size 50 sectors (25 KB) without HPA area.
Show Identify
Modify
Restore
Freeze Lock
Check DCO structure

DCO status: disabled

Modify the set of optional commands, modes or feature sets supported by the device from DCO IDENTIFY command. Create and transfer an overlay to device that modifies some bits in words of IDENTIFY DEVICE.

↑↓ Move ENTER Run ESC Return

Multiword DMA modes: Multiword DMA 2
Ultra DMA modes: Ultra DMA 66/100/133
Maximum LBA sectors: 376,773,168 [500.11 GB] full capacity

1. Command/Feature set to (dis)allow Status from drive Action
SMART feature set enabled NONE
SMART self-test enabled NONE
SMART error logging enabled NONE
Security Mode feature disabled NONE
Automatic Acoustic Management (AAM) disabled NONE
Host Protected Area (HPA) enabled NONE
48-bit Addressing enabled NONE
Forced Unit Access (FUA) N/A INSTALL
SMART Selective self-test enabled NONE
SMART Conveyance self-test enabled NONE
Write-Read-Verify feature disabled NONE

↑↓ Move ← Select INS Edit F7 Restore PgDn/Up Next/Prev S Set ESC Return
### DCO Modify [ST3500413AS]

<table>
<thead>
<tr>
<th>Feature</th>
<th>Status from Drive</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMART feature set</td>
<td>enabled</td>
<td>NONE</td>
</tr>
<tr>
<td>SMART self-test</td>
<td>enabled</td>
<td>NONE</td>
</tr>
<tr>
<td>SMART error logging</td>
<td>enabled</td>
<td>NONE</td>
</tr>
<tr>
<td>Security Mode feature</td>
<td>disabled</td>
<td>NONE</td>
</tr>
<tr>
<td>Automatic Acoustic Management (AAM)</td>
<td>disabled</td>
<td>NONE</td>
</tr>
<tr>
<td>Host Protected Area (HPA)</td>
<td>enabled</td>
<td>NONE</td>
</tr>
<tr>
<td>48-bit Addressing</td>
<td>enabled</td>
<td>NONE</td>
</tr>
<tr>
<td>Forced Unit Access (FUA)</td>
<td>N/A</td>
<td>INSTALL</td>
</tr>
<tr>
<td>SMART Selective self-test</td>
<td>enabled</td>
<td>NONE</td>
</tr>
<tr>
<td>SMART Conveyance self-test</td>
<td>enabled</td>
<td>NONE</td>
</tr>
<tr>
<td>Write-Read-Verify feature</td>
<td>disabled</td>
<td>NONE</td>
</tr>
</tbody>
</table>

---

**Are you sure to run 'DCO Modify' <Y/N> ?**

---

**Command completed successfully. Press any key...**
DCO area is enabled now.

You can check the settings of hidden areas in the 'Hidden areas menu'.
Remove hidden DCO area

To remove DCO area you can use command DCO RESTORE or menu option Auto Remove Hidden Areas.
Remove hidden DCO area with DCO RESTORE

**Example:** We try to remove created DCO area of 50 sectors.
Auto remove DCO area

There are 2 options: 'Auto remove DCO area' in DCO menu or 'Auto remove hidden areas' in Hidden areas menu.
Device Configuration Overlay (DCO) menu [ST3500413AS]

Show Identify
Modify
Restore
Freeze Lock
Check DCO structure
Auto remove DCO area

DCO status: enabled

Auto remove DCO area using command DCO SET or DCO RESTORE.

Are you sure to run 'Auto remove DCO area' <Y/N> ?
The error message for the command DCO SET means that the original (native) capacity cannot be restored in this way. The DCO RESTORE command must be used.

**Dump of DCO area**

**Example:** We have created an DCO area of 50 sectors, which starts at LBA sector 976,773,118. This option allows you to view the contents of this DCO area.
Hidden areas menu [ST3500413AS]

Overview of hidden areas
Auto remove hidden areas
Dump of DCO area
Detect BEER record

Active areas: DCO

To dump sectors the area will be temporarily disabled.

↑↓ Move ENTER Run ESC Return

Dump of DCO area [ST3500413AS]

Overview of hidden areas
Auto remove hidden areas
Dump of DCO area
Detect BEER record

Active areas: DCO

To dump sectors the area will be temporarily disabled.

Do you want to remove DCO area using RESTORE <Y/N>?
I saved the DCO text in the first sector of this area.
**AMAX area**

Accessible Max Address (AMAX)

**Create AMAX area**

**Example:** We create AMAX area with a size of 100 sectors (50 KB).
Accessible Max Address (AMAX) menu [ADATA SD900]

Set Accessible Max Address
Freeze Accessible Max Address

AMAX status: disabled

Read/Write commands will be limited to LBA from zero to specified value. You can make only one successful command before a power-on reset is processed. This command will be aborted for AMAX in frozen state.

↑↓ Move ENTER Run ESC Return

Set Accessible Max Address [ADATA SD900]

<table>
<thead>
<tr>
<th>Current</th>
<th>LBA sectors</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>NATIVE</td>
<td>500,118,192</td>
<td>256.06 GB</td>
</tr>
<tr>
<td>USER</td>
<td>500,118,192</td>
<td>256.06 GB</td>
</tr>
<tr>
<td>HIDDEN</td>
<td>0</td>
<td>0.00 KB</td>
</tr>
<tr>
<td>NEW USER</td>
<td>500,118,192</td>
<td>256.06 GB (full native size)</td>
</tr>
<tr>
<td>NEW HIDDEN</td>
<td>0</td>
<td>0.00 KB</td>
</tr>
</tbody>
</table>

↑↓←→ Change INS Edit ESC Abort
<table>
<thead>
<tr>
<th>Current</th>
<th>LBA sectors</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>NATIVE</td>
<td>500,118,192</td>
<td>255.06 GB</td>
</tr>
<tr>
<td>USER</td>
<td>500,118,192</td>
<td>255.06 GB</td>
</tr>
<tr>
<td>HIDDEN</td>
<td>0</td>
<td>0.00 KB</td>
</tr>
</tbody>
</table>

| NEW USER   | 500,118,092 | 255.06 GB    |
| NEW HIDDEN | 100         | 51.20 KB     |

Are you sure to run 'Set Accessible Max Address' <Y/N> ?
Check AMAX area settings:
Main menu [ADATA SU900]

Device tests menu
File system menu
Device data menu
SMART/SCT menu
SET MAX (HPA) menu
Accessible Max Address (AMAX) menu
Hidden areas menu
Security (SEC) menu
Commands menu

Overview of hidden areas
Auto remove hidden areas
Detect BEER record

Hidden areas menu [ADATA SU900]

Overview of hidden areas
Auto remove hidden areas
Detect BEER record

Active areas: AMAX

Summary of hidden areas (HPA, AMAX, DCO, Address Offset).
Remove AMAX area
Overview of hidden areas
- Auto remove hidden areas
  - Detect BEER record

Active areas: AMAX

Are you sure to run 'Auto remove hidden areas' <Y/N> ?

Removing hidden areas...
HPA area: not detected
AMAX area: detected

Using SET AMAX command ERROR
AMAX full capacity was not restored
DCO area: not detected

Press any key to continue...
This error message you will see if you try to call the second SET AMAX command without power off (e.g. immediately after the first creation of AMAX area). So we turn power off and on and try it again.
ADDRESS OFFSET area

Address Offset mode Reserved Area Boot (OFFS)

Computer systems perform initial code loading (booting) by reading from a predefined address on a disk drive. To allow an alternate bootable operating system to exist in a system reserved area on a disk drive this feature provides a Set Features function to temporarily offset the drive address space. The offset address space wraps around so that the entire disk drive address space remains addressable in offset mode. Max LBA in offset mode is set to the end of the system reserved area to protect the data in the user area when operating in offset mode. The Max LBA can be changed by an Set Max Address command, but any commands which access sectors across the original native maximum LBA are rejected with error, even if this protection is removed by an Set Max Address command.

Enable OFFS area

Set Features subcommand code 09h Enable Address Offset Mode offsets address Cylinder 0, Head 0, Sector 1, and LBA 0, to the start of the non-volatile protected area established using the Set Max Address command. The offset condition is cleared by Subcommand 89h Disable Address Offset Mode, Hardware reset or Power on Reset. If Reverting to Power on Defaults has been enabled by Set Features command, it is cleared by Soft reset as well. Upon entering offset mode the capacity of the drive returned in the Identify Device data is the size of the former protected area. A subsequent Set Max Address command with the address returned by Read Max Address command allows access to the entire drive. Addresses wrap so the entire drive remains addressable.

If a non-volatile protected area has not been established before the device receives a Set Features Enable Address Offset Mode command, the command fails with Abort error status.

First we create non-volatile HPA area of 10000 sectors using SET MAX command.
For checking, we will list the contents of LBA sector 0.

For the follow-up check with dump sector, I filled the first sector of the HPA area (LBA 10000) with the text OFFS.
Main menu [HDT722525DLA380]

- Device tests menu
- File system menu
- Device data menu
- SMART menu
- ⬆️ SET MAX (HPA) menu
- Device Configuration Overlay (DCO) menu
- Hidden areas menu
- Security (SEC) menu
- ⬇️ Commands menu

↑↓ Move ENTER Select ESC Return

SET MAX (HPA) menu [HDT722525DLA380]

Set Max Address
Set password
Lock
Unlock
Freeze Lock

SET MAX status: HPA disabled

Allows to redefine the maximum address of the user accessible address space, to create or remove unlocked Host Protected Area (HPA). This command will be aborted in LOCKED or FROZEN mode until the power-on reset.

↑↓ Move ENTER Run ESC Return
<table>
<thead>
<tr>
<th></th>
<th>LBA sectors</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>NATIVE</td>
<td>488,397,168</td>
<td>250.06 GB</td>
</tr>
<tr>
<td>USER</td>
<td>488,397,168</td>
<td>250.06 GB</td>
</tr>
<tr>
<td>HIDDEN</td>
<td>0</td>
<td>0.00 KB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>LBA sectors</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEW USER</td>
<td>10,000</td>
<td>5.12 MB</td>
</tr>
<tr>
<td>NEW HIDDEN</td>
<td>488,387,168</td>
<td>250.05 GB</td>
</tr>
</tbody>
</table>

Used command: SET MAX EXT (48-bits) (change it when an error occurs)
Volatile mode: YES -> hard settings
SET PERMANENTLY: Changes shall preserve over power-up or hardware reset.

Are you sure to run 'Set Max Address' <Y/N>?
Check settings in 'Overview of hidden areas'.

Listing for setting disk sectors from 'Device data' after setting HPA area.
Now we enable Address Offset Mode feature.
Supported command/feature sets

ATA commands
SATA commands
Dump device sectors

Command/Feature sets supported by device.
Change of value is available for features with yellow color only.
WARNING! Restore is possible only until new detect or restart of program.

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Supported command/feature sets</th>
<th>Status</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Power-Up In Standby (PUIS) feature set</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>SET FEATURES required to spinup after power-up</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Address Offset Mode Reserved Area Boot</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>SET MAX security extension</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Automatic Acoustic Management (AAM) feature set</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>48-bit address feature set</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Device Configuration Overlay (DCO) feature set</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>FLUSH CACHE command</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>FLUSH CACHE EXT command</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>SMART error logging</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>SMART self-test</td>
<td>enabled</td>
<td></td>
</tr>
</tbody>
</table>

CAUTION! Setting could be dangerous!
The command is volatile and is reset on the next power cycle.
This command is not valid if DCO is active or MPA is not set.
RUN: change status to enabled
Check settings in 'Overview of hidden areas'.

---

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Supported command/feature sets</th>
<th>Status</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Power-Up In Standby (PUIS) feature set</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>SET FEATURES required to spinup after power-up</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Address Offset Mode Reserved Area Boot</td>
<td>enabled</td>
<td>O.K.</td>
</tr>
<tr>
<td>14</td>
<td>SET MAX security extension</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Automatic Acoustic Management (AAM) feature set</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>48-bit address feature set</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Device Configuration Overlay (DCO) feature set</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>FLUSH CACHE command</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>FLUSH CACHE EXT command</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>SMART error logging</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>SMART self-test</td>
<td>enabled</td>
<td></td>
</tr>
</tbody>
</table>

CAUTION! Setting could be dangerous!
The command is volatile and is reset on the next power cycle.
This command is not valid if DCO is active or HPA is not set.
**RUN:** change status to enabled

Are you sure to run 'Address Offset Mode Reserved Area Boot'? <Y/N>?
We will check the content of LBA sector 0 with 'Dump device sectors'. 
Now LBA sector 0 is set to the first sector of the HPA area (LBA 10000). The original LBA sectors in the range 0 to 9999 are now inaccessible.
Listing for setting disk sectors from 'Device data'.

<table>
<thead>
<tr>
<th>Source</th>
<th>Cylinders</th>
<th>Heads</th>
<th>Sectors</th>
<th>Total sectors</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATA LBA28</td>
<td>16383</td>
<td>16</td>
<td>63</td>
<td>268,435,455</td>
<td>137.44 GB</td>
</tr>
<tr>
<td>ATA LBA48</td>
<td>16383</td>
<td>16</td>
<td>63</td>
<td>488,387,168</td>
<td>250.05 GB</td>
</tr>
<tr>
<td>ATA CHS</td>
<td>16383</td>
<td>16</td>
<td>63</td>
<td>16,514,064</td>
<td>8.46 GB</td>
</tr>
<tr>
<td>INT13h/BIOS</td>
<td>1024</td>
<td>255</td>
<td>63</td>
<td>16,450,560</td>
<td>8.42 GB</td>
</tr>
<tr>
<td>*Ext.INT13h</td>
<td>955</td>
<td>255</td>
<td>63</td>
<td>488,397,168</td>
<td>250.06 GB</td>
</tr>
</tbody>
</table>

(* = CHS parameters are not valid)

| SET MAX size | HPA ACTIVE | 10,000 | 5.12 MB |
| DCO MAX size |            | 488,397,168 | 250.06 GB |
| OFFSET size  | ACTIVE     | 488,397,168 | 250.06 GB |

Device model [AHCI/SATA]  
Vendor                  
Translation/max. LBA mode 
Logical sector size     
Physical sector size    
Detect mode             
Removable device        

**Disable OFFS area**

Disable Address Offset Feature removes the address offset and sets the size of the drive reported by the Identify Device command back to the size specified in the last non-volatile Set Max Address command.

First we turn off the Address Offset Mode setting.
---

**Supported command/feature sets [HDT722525DLA388]**

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Supported command/feature sets</th>
<th>Status</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.</td>
<td>READ BUFFER command</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td>DOWNLOAD MICROCODE command</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td>Advanced Power Management (APM) feature set</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>11.</td>
<td>Power-Up In Standby (PUIS) feature set</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>12.</td>
<td>SET FEATURES required to spinup after power-up</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>13.</td>
<td>Address Offset Mode Reserved Area Boot</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>14.</td>
<td>SET MAX security extension</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>15.</td>
<td>Automatic Acoustic Management (AAM) feature set</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>16.</td>
<td>48-bit address feature set</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>17.</td>
<td>Device Configuration Overlay (DCO) feature set</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>18.</td>
<td>FLUSH CACHE command</td>
<td>enabled</td>
<td></td>
</tr>
</tbody>
</table>

**CAUTION! Setting could be dangerous!**
The command is volatile and is reset on the next power cycle.
This command is not valid if DCO is active or MPA is not set.
**RUN:** change status to disabled

---

**Address Offset Mode Reserved Area Boot [HDT722525DLA380]**

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Supported command/feature sets</th>
<th>Status</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.</td>
<td>READ BUFFER command</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td>DOWNLOAD MICROCODE command</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td>Advanced Power Management (APM) feature set</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>11.</td>
<td>Power-Up In Standby (PUIS) feature set</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>12.</td>
<td>SET FEATURES required to spinup after power-up</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>13.</td>
<td>Address Offset Mode Reserved Area Boot</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>14.</td>
<td>SET MAX security extension</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>15.</td>
<td>Automatic Acoustic Management (AAM) feature set</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>16.</td>
<td>48-bit address feature set</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>17.</td>
<td>Device Configuration Overlay (DCO) feature set</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>18.</td>
<td>FLUSH CACHE command</td>
<td>enabled</td>
<td></td>
</tr>
</tbody>
</table>

**CAUTION! Setting could be dangerous!**
The command is volatile and is reset on the next power cycle.
This command is not valid if DCO is active or MPA is not set.
**RUN:** change status to disabled

---

Are you sure to run 'Address Offset Mode Reserved Area Boot' <Y/N>?
### Address Offset Mode Reserved Area Boot [HDT722525DLA380]

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Supported command/feature sets</th>
<th>Status</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>READ BUFFER command</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>DOWNLOAD MICROCODE command</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Advanced Power Management (APM) feature set</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Power-Up In Standby (PUIS) feature set</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>SET FEATURES required to spinup after power-up</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Address Offset Mode Reserved Area Boot</td>
<td>disabled</td>
<td>O.K.</td>
</tr>
<tr>
<td>14</td>
<td>SET MAX security extension</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Automatic Acoustic Management (AAM) feature set</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>48-bit address feature set</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Device Configuration Overlay (DCO) feature set</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>FLUSH CACHE command</td>
<td>enabled</td>
<td></td>
</tr>
</tbody>
</table>

### AMCIC  CMD7  DEVI  HI GHS  MID4  LON5  CN T2  FEA1

Before 0060h 0040h 0000h 0020h 0000h 0000h 0000h 0000h
After 0050h 0040h 0000h 0000h 0000h 0100h 0000h

Status 50h: BSY  DRDY  DFSE  DME  DREQ  ALGN  SENS  ERR
Error 00h: ICRC  UNC  MC  IDNF  MCR  ABRT  T0NF  CCT0

---

### Supported command/feature sets [HDT722525DLA380]

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Supported command/feature sets</th>
<th>Status</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>READ BUFFER command</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>DOWNLOAD MICROCODE command</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Advanced Power Management (APM) feature set</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Power-Up In Standby (PUIS) feature set</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>SET FEATURES required to spinup after power-up</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Address Offset Mode Reserved Area Boot</td>
<td>disabled</td>
<td>O.K.</td>
</tr>
<tr>
<td>14</td>
<td>SET MAX security extension</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Automatic Acoustic Management (AAM) feature set</td>
<td>disabled</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>48-bit address feature set</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Device Configuration Overlay (DCO) feature set</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>FLUSH CACHE command</td>
<td>enabled</td>
<td></td>
</tr>
</tbody>
</table>

---

**CAUTION! Setting could be dangerous!**
The command is volatile and is reset on the next power cycle.
This command is not valid if DCO is active or HPA is not set.
**RUN:** change status to enabled

↓↓ Move F7 Restore all ENTER Run ESC Return
An error message appears when you try to remove the HPA area when the Address Offset is set.
An error message appears when you try to remove a non-volatile HPA area without restarting.

![Image]

This error message you will see if you try to call the second non-volatile command without power off (e.g. immediately after the first creation of HPA area). So we turn power off and on and try it again.

Status after removing HPA area and Address Offset Mode.
SCSI capacity

To change the sector size of SCSI disk see option [SCSI drives].
Main menu [WDIGTL ENTERPRISE]

- Device tests menu
- File system menu
- Device data menu
- SMART menu
  - Commands menu
  - Save to file menu

SCSI commands
Dump device sectors

Commands for SCSI devices.

↑ Move ENTER Select ESC Return
SCSI commands

1. SCSI Reset
2. Read Defect PLlist
3. Read Defect GList
4. Change capacity/sector size

Change capacity/sector size.
Not every disk supports changing the block size.

Move ENTER Run ESC Return

Main menu [wDIGTL ENTERPRISE]

- Device tests menu
- File system menu
- Device data menu
- SMART menu
- Commands menu
- Save to file menu

Move ENTER Select ESC Return
Commands for SCSI devices.

Read capacity: O.K.
Read mode sense page 01h: O.K.

Press any key to continue...
We will reduce the capacity of the SCSI disk.
Are you sure to run 'Change capacity' <Y/N> ?

Warning: read capacity and mode sense report different capacity.
Current: Set the current mode sense default values.
Restore: The logical unit shall be set to its maximum capacity.
Format: It can take from several minutes to hours, depending on the drive size.

Restore the original SCSI disk capacity using 'Restore'.
<table>
<thead>
<tr>
<th>Command</th>
<th>Current values</th>
<th>Sectors</th>
<th>Block size</th>
<th>Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>READ CAPACITY</td>
<td>8,515,100</td>
<td>512 bytes</td>
<td>4.36 GB</td>
<td></td>
</tr>
<tr>
<td>MODE SENSE</td>
<td>8,515,173</td>
<td>512 bytes</td>
<td>4.36 GB</td>
<td></td>
</tr>
</tbody>
</table>

Parameters savable: NO
Write-protected: NO

New capacity: 8515100 sectors [4.36 GB]
New block size: 512 bytes

Save mode pages (volatile): NO

Are you sure to run 'Restore' <Y/N> ?

Command completed successfully. Press any key...
Restoring the original SCSI disk capacity using 'Restore' does not work for some disks. In this case, you must set the capacity manually via the INS key (Edit).

<table>
<thead>
<tr>
<th>Command</th>
<th>Current values</th>
<th>Sectors</th>
<th>Block size</th>
<th>Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>READ CAPACITY</td>
<td>8,515,173</td>
<td>512 bytes</td>
<td>4.36 GB</td>
<td></td>
</tr>
<tr>
<td>MODE SENSE</td>
<td>8,515,173</td>
<td>512 bytes</td>
<td>4.36 GB</td>
<td></td>
</tr>
</tbody>
</table>

Parameters savable: NO  
Write-protected : NO

New capacity : 8515173 sectors [4.36 GB]  
New block size: 512 bytes 

Save mode pages (volatile): NO  

Current: Set the current mode sense default values.  
Restore: The logical unit shall be set to its maximum capacity.  
Format: It can take from several minutes to hours, depending on the drive size.
Auto remove hidden areas

Example: We have set both hidden HPA and DCO areas, which we will now try to remove.
### Overview of hidden areas [ST3500413AS]

<table>
<thead>
<tr>
<th>Type</th>
<th>Size</th>
<th>LBA Sectors</th>
<th>LBA Start</th>
<th>LBA End</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPA</td>
<td>51.20 KB</td>
<td>100</td>
<td>976,773,018</td>
<td>976,773,117</td>
</tr>
<tr>
<td>AMAX</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DCO</td>
<td>25.60 KB</td>
<td>50</td>
<td>976,773,118</td>
<td>976,773,167</td>
</tr>
<tr>
<td>OFFS</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FULL</td>
<td>500.11 GB</td>
<td>976,773,168</td>
<td>0</td>
<td>976,773,167</td>
</tr>
<tr>
<td>USER</td>
<td>500.11 GB</td>
<td>976,773,018</td>
<td>0</td>
<td>976,773,017</td>
</tr>
<tr>
<td>DIFF</td>
<td>76.80 KB</td>
<td>-150</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Hidden areas menu [ST3500413AS]

- Overview of hidden areas
- Auto remove hidden areas
- Dump of HPA area
- Dump of DCO area
- Detect BEER record

**Active areas:** HPA DCO
An error message *SET MAX full capacity was not restored* appears in the case we call the second non-volatile command SET MAX without power off. Turn off and turn on the computer and try again.

An error message *DCO full capacity was not restored* for the command DCO SET means that the original (native) capacity cannot be restored in this way. The DCO RESTORE command must be used.
An error message *'DCO full capacity was not restored'* for the command DCO RESTORE appears if the HPA area is not removed first.

Now are both hidden areas HPA and DCO disabled.

**Overview of hidden areas**

Disk status with no hidden HPA and DCO areas.
<table>
<thead>
<tr>
<th>Type</th>
<th>Size</th>
<th>LBA Sectors</th>
<th>LBA Start</th>
<th>LBA End</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPA</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AMAX</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DCO</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OFFS</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FULL</td>
<td>500.11 GB</td>
<td>976,773,168</td>
<td>0</td>
<td>976,773,167</td>
</tr>
<tr>
<td>USER</td>
<td>500.11 GB</td>
<td>976,773,168</td>
<td>0</td>
<td>976,773,167</td>
</tr>
<tr>
<td>DIFF</td>
<td>0.00 KB</td>
<td></td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

↑→ Move  S  Save ESC Return
Security Lock the device

The security system is enabled (the device in a locked state) by sending a user password to the device with the SECURITY SET PASSWORD command. Setting the master password does not enable security system.

When a user password is set, the drive automatically enters lock mode by the next powered-on. In locked mode, device rejects media access commands until a SECURITY UNLOCK command is successfully completed.

If the device is in security frozen state the device shall return command aborted for all security commands except 'Freeze lock'. In this case see FAQ “How to bypass a Security and/or DCO frozen state?”

Example: We set the user password “1234” with the high security mode.
Main menu [ST3500413AS]

- Device tests menu
- File system menu
- Device data menu
- SMART/SCT menu
- SET MAX (HPA) menu
- Device Configuration Overlay (DCO) menu
- Hidden areas menu
- Security menu
- Commands menu

Security (SEC) menu [ST3500413AS]

- Set password
- Erase unit
- Unlock
- Disable password
- Freeze lock
- Unlock device

SEC status: disabled
Master Password Revision Code: FFFeh
Sends USER or MASTER password in HIGH or MAXIMUM security level.
Master password may be used to unlock the device if User password is lost.
Setting the Master password does not enable the password system.
The locked mode will be active after reset.
After setting the password the lock mode shall be enabled from the next power-on or hardware reset. In lock mode you can use the commands erase unit, unlock or unlock device only.

When the device is security locked many other commands shall be aborted until the device is unlocked.
DEVELOP IS SECURITY LOCKED!

Set password
Erase unit
Unlock
Disable password
Freeze lock
Unlock device

SEC status: password/high/locked
Master Password Revision Code: FFFEh

Sends USER or MASTER password in HIGH or MAXIMUM security level.
Master password may be used to unlock the device if user password is lost.
Setting the master password does not enable the password system.
This command will be aborted!

DEVICE IS SECURITY LOCKED!
Set password
Erase unit
Unlock
Disable password
Freeze lock
Unlock device

SEC status: password/high/locked
Master Password Revision Code: FF Eh

CAUTION! This will OVERWRITE the data on your drive!
This command shall disable the device lock mode, however, the master password shall still be stored internally within the device and may be reactivated later when a new User password is set.
DEVICE IS SECURITY LOCKED!

**Move ENTER Run ESC Return**

Set password
Erase unit
Unlock
Disable password
Freeze lock
Unlock device

SEC status: password/high/locked
Master Password Revision Code: FF Eh

Identifier: User
Password: '1234'
Erase level: Normal
Erase time: 2 min.
Fill password: none

ERASING IN PROGRESS: DON'T TURN OFF POWER OR RESET SYSTEM!
Elapsed time: 00:00:04 hh:mm:ss 3%
Remaining time: 00:01:56 hh:mm:ss 97%
(check the status every 5 seconds)

A Abort (or wait for the command to finish)
Security (SEC) menu [ADATA SU000]

Set password
Erase unit
Unlock
Disable password
Freeze lock
Unlock device

SEC status: disabled
Master Password Revision Code: FFFEh

CAUTION! This will OVERWRITE the data on your drive!
This command shall disable the device lock mode, however, the master password shall still be stored internally within the device and may be reactivated later when a new User password is set.
The command requires a password to be set!
Security Unlock the device

In **High security mode**, the disk can be unlocked with either the User or Master password, using the **SECURITY UNLOCK** command.

In **Maximum security mode**, the disk can be unlocked with the User password only. Without the User password the device requires a **SECURITY ERASE PREPARE** command and a **SECURITY ERASE UNIT** command with the Master password to unlock. Execution of the **SECURITY ERASE UNIT** command erases all user data on the device. See [Security erase the device](#).

**Password lost**

If the user password is lost and High level security is set, the drive does not allow the user to access any data. However, the drive can be unlocked using the master password. If the user password is lost and Maximum security level is set, it is impossible to access data. However, the drive can be unlocked using the **ERASE UNIT** command with the master password. The drive will erase all user data and unlock the drive.

**Unlock counter**

If the password compare fails then the device shall return command aborted to the host and decrements the unlock counter. This counter shall be initially set to five and shall be decremented for each password mismatch when **SECURITY UNLOCK** is issued and the device is locked.

When this counter reaches zero then **SECURITY UNLOCK** and **SECURITY ERASE UNIT** commands shall be command aborted until a power-on reset or a hardware reset. **SECURITY UNLOCK** commands issued when the device is unlocked have no effect on the unlock counter.
**Unlock and disable password**

**Example:** To disable the high security mode of the device we have to unlock and disable password with the user password "1234".
Set password
Erase unit
Unlock
Disable password
Freeze lock
Unlock device

SEC status: password/high
Master Password Revision Code: FFFEH

Identifier: User
Password: '1234'
Fill password: none
HEX: 31 32 33 34

Are you sure to run 'Unlock'? <Y/N>?
Set password
Erase unit
Unlock
Disable password
Freeze lock
Unlock device

SEC status: password/high
Master Password Revision Code: FFEEh

Identifier: User
Password: '1234'
HEX: 31 32 33 34

Command completed successfully. Press any key...

SEC status: password/high [UNLOCKED mode]
Master Password Revision Code: FFEEh

SECURITY UNLOCK (unlock counter shall be initially set to 5).
With the correct password the device shall disable the lock mode.
The Master password shall not unlock the device in Security Level Maximum.
If the password compare fails then the device decrements the unlock counter.
SEC status: password/high [UNLOCKED mode]
Master Password Revision Code: FFFEh

SECURITY DISABLE PASSWORD - device shall be in Unlocked mode. With the correct password the device shall disable the lock mode. This command shall not change the Master password. The Master password shall be reactivated when a User password is set.

Identifier: User
Password: '1234'  Fill password: none
HEX: 31 32 33 34
Set password
Erase unit
Unlock
Disable password
Freeze lock
Unlock device

SEC status: password/high [UNLOCKED mode]
Master Password Revision Code: FFEEh

Identifier: User
Password: ‘1234’  
Fill password: none

HEX: 31 32 33 34

Are you sure to run 'Disable password' <Y/N>?

Command completed successfully. Press any key...
Unlock device

You can also use a special function **Unlock device** to unlock and then disable password.
Unlock device [ST3500413AS]

Set password
Erase unit
Unlock
Disable password
Freeze lock
Unlock device

SEC status: password/high
Master Password Revision Code: FFFEh

Identifier: User
Password : '1234'  Fill password : none

HEX: 31 32 33 34

Identifier P Password F Fill S Set ESC Abort

Are you sure to run 'Unlock device' <Y/N>?
Unlock device [ST3500413AS]

- Set password
- Erase unit
- Unlock
- Disable password
- Freeze lock
- Unlock device

SEC status: password/high
Master Password Revision Code: FFFEh

Identifier: User
Password: '1234'
Fill password: none
HEX: 31 32 33 34

Command completed successfully. Press any key...

Unlock device [ST3500413AS]

- Set password
- Erase unit
- Unlock
- Disable password
- Freeze lock
- Unlock device

SEC status: disabled
Master Password Revision Code: FFFEh

Unlock a locked device if you know a password (UNLOCK and DISABLE PASSWORD). The command requires a password to be set!

↑↑ Move ENTER Run ESC Return
Erase the device

Erase unit (wipe) does not mean delete or format. Data erasure is a method of software based overwriting. It uses an application to write patterns of data (like 00h or FFh) onto each of a hard drive's sectors on all areas of a hard drive.

To erase device you can use SECURITY ERASE UNIT command in Security Menu or, when supported, SCT Write Same command in SMART Menu.

Disk overwriting programs that cannot access the entire hard drive, including hidden areas like the Host Protected Area (HPA), Device Configuration Overlay (DCO), and remapped sectors, perform an incomplete erasure, leaving some of the data intact.

To use security erase command you should first set any password – we use password "1234".

Security erase the device

In Enhanced Erase mode, all previously written user data shall be overwritten, including sectors that are no longer in use due to reallocation.

SECURITY ERASE UNIT allow erase HPA (Host Protected Area) or DCO (Device Configuration Overlay) areas, if any, as well. But don't remove these areas.

Also in High security mode the SECURITY ERASE UNIT command can be used with either the User or Master password.
Set password
Erase unit
Unlock
Disable password
Freeze lock
Unlock device

SEC status: disabled
Master Password Revision Code: FFFEh

Sets USER or MASTER password in HIGH or MAXIMUM security level. 
Master password may be used to unlock the device if User password is lost. 
Setting the Master password does not enable the password system. 
The locked mode will be active after reset.

Identifier: User
Password : '1234'
Password level: High
Fill password : none
HEX: 31 32 33 34
Set password
Erase unit
Unlock
Disable password
Freeze lock
Unlock device

SEC status: disabled
Master Password Revision Code: FFFEh

Identifier: User
Password: '1234'
Password level: High
Fill password: none

HEX: 31 32 33 34

Are you sure to run 'Set password' <Y/N> ?

Command completed successfully. Press any key...
CAUTION! This will OVERWRITE the data on your drive!
This command shall disable the device lock mode, however, the Master password shall still be stored internally within the device and may be reactivated later when a new User password is set.
Erase unit [ADATA SU800]

Set password
Erase unit
Unlock
Disable password
Freeze lock
Unlock device

SEC status: password/high
Master Password Revision Code: FFFEh

Identifier: User
Password: '1234'

Erase level: Normal
Erase time: 2 min.
Fill password: none

Are you sure to run 'Erase unit' <Y/N> ?

ERASING IN PROGRESS: DON'T TURN OFF POWER OR RESET SYSTEM!
Elapsed time: 00:00:03 hh:mm:ss 2%
Remaining time: 00:01:57 hh:mm:ss 98%
(check the status every 5 seconds)

Abort (or wait for the command to finish)
SCT Write Same

When device supports SMART Command Transport (SCT) you can use the SCT function Write Same – LBA Repeat Write Pattern or LBA Repeat Write Sector.

Example: We will overwrite sectors from LBA 0 with hexadecimal pattern "0000|0000h".
SMART Command Transport (SCT) menu [ST3500413AS]

- Error Recovery Control (ERC) menu
- Feature Control menu
- Data Table menu
- Write Same
- Long Sector Access menu
- SCT Status page (E0h)

Drive state: Active waiting for a command
Last command: Background SCT operation terminated: interrupt of host command

HDAT2 Cookbook (c) 2021 CBL

Write Same [ST3500413AS]

- LBA Repeat Write Pattern
- LBA Repeat Write Sector

Drive state: Active waiting for a command
Last command: Background SCT operation terminated: interrupt of host command

Writes a 32-bit pattern repeatedly to the media. Automatic sector reassignment is permitted. It will not write over HPA area. All user data shall be overwritten!
Drive state: Active waiting for a command
Last command: Background SCT operation terminated: interrupt of host command

Command mode: background
Start LBA: 0
Last LBA: 976773157 [976,773,168 sector(s) = 500.11 GB]
Fill pattern: 0000|0000h - -

Are you sure to run 'LBA Repeat Write Pattern' <Y/N> ?

CAUTION! This will OVERWRITE the data on your drive! ARE YOU SURE <Y/N> ?

Page 102
I interrupted the command with the 'A' key.
LBA Repeat Write Pattern
LBA Repeat Write Sector

Drive state: SCT command processing in background
Last command: SCT command processing in background

SCT command processing: background
Drive state: SCT command processing in background
Action: Write Same
Function: Write pattern background
Current LBA: 4,480,284 [2.30 GB] 0%
Elapsed time:
(check the status every 5 seconds)

Command aborted. Press any key...

Write Same [ST3500413AS]

LBA Repeat Write Pattern
LBA Repeat Write Sector

Drive state: Active waiting for a command
Last command: Background SCT operation terminated: interrupt of host command

Writes a sector data in data buffer repeatedly to the media.
Automatic sector reassignment is permitted. It will not write over HPA area.
All user data shall be overwritten!

11 Move S Setup ENTER Run ESC Return
LBA Repeat Write Pattern

LBA Repeat Write Sector

Drive state: Active waiting for a command
Last command: Background SCT operation terminated: interrupt of host command

Command mode: background
Start LBA: 0
Last LBA: 976773167 [976,773,168 sector(s) = 500.11 GB]
Fill pattern: 000000000h - '

Are you sure to run 'LBA Repeat Write Sector' <Y/N>?
### Drive state: Active waiting for a command

Last command: Background SCT operation terminated: interrupt of host command

**Command mode:** background

**Start LBA:** 0
**Last LBA:** 976773167

[976,773,168 sector(s) - 500.11 GB]

**Fill pattern:** 0000|0000h - '

---

CAUTION! This will OVERWRITE the data on your drive! ARE YOU SURE <Y/N>? 

---

**Command completed successfully. Press any key...**
I interrupted the command with the 'A' key.
Now we change the write pattern 0000|0000h to ABCDh.

How to change 'Fill pattern':

Use the 'M' key to select the type of input ASCII or HEX and use the 'INS' key to enter the desired pattern.
Drive state: Active waiting for a command
Last command: Background SCT operation terminated: interrupt of host command

Command mode: foreground
Start LBA: 0
Last LBA: 976773167 [976,773,168 sector(s) = 500.11 GB]
Fill pattern: ^ - 0000 0000h
Sector buffer filler that is written on the media.

INPUT: INS Insert F8 Clear ENTER Set ESC Cancel
LBA Repeat Write Pattern
LBA Repeat Write Sector

Drive state: Active waiting for a command
Last command: Background SCT operation terminated: interrupt of host command

Command mode: foreground
Start LBA: 0
Last LBA: 976773167 [976,773,168 sector(s) = 500.11 GB]
Fill pattern: 'ABCD' - 4142|4344H
Sector buffer filler that is written on the media.

Are you sure to run 'LBA Repeat Write Sector' <Y/N>?
I interrupted the command with the 'A' key.
Using 'Dump device sectors' we will verify the written pattern into sectors.
You can also check command status in SCT status page.
HDAT2 Cookbook (c) 2021 CBL

Main menu [ST3500413AS]

- Device tests menu
- File system menu
- Device data menu
- SMART/SCT menu
- SET MAX (HPA) menu
- Device Configuration Overlay (DCO) menu
- Hidden areas menu
- Security (SEC) menu
- Commands menu
- SMART Command Transport (SCT)
- Read Log menu
- Routine menu
- Command menu
- SMART Attributes
- SMART Capability
- Dump SMART Attribute Data
- Dump SMART Attribute Thresholds

SMART: enabled, status: WARNING, GPL: supported

↑↓ Move ENTER Select ESC Return
SMART Command Transport (SCT) menu [ST3500413AS]

- Error Recovery Control (ERC) menu
- Feature Control menu
- Data Table menu
- Write Same
- Long Sector Access menu

SCT Status page (E0h)

Drive state: Active waiting for a command
Last command: Command complete without error

Read the SCT Command/Status log with HDA temperature.

---

SCT Status page (E0h) [ST3500413AS]

- Format version 0003h
- SCT version (vendor specific) 020Ah
- SCT level 0001h

Status flags
Segment Initialized bit:
- Any user LBA is written, even if write cache is enabled
- Active waiting for a command
- Command complete without error
- Write Same
- Write pattern background

Current LBA of SCT command n/a

Head/disk assembly (HDA) temperature
- Current 38°C/100.4°F
- Power cycle minimum 31°C/87.8°F
- Power cycle maximum 38°C/100.4°F

Move S Setup ENTER Run ESC Return
Search the device

Types of searched objects: string, empty sector, non-empty sector or time stamp.

In setup menu (with a key 'S') you can select type of search object: string, empty sector, non-empty sector or time stamp.

When overwriting a bad sector, a **time stamp** is stored in the sector at a fixed location.

**Search for string**

You can search a string with these parameters:

- case or non-case sensitive
- string type (ASCII or UNICODE)
- position in sector

**Example 1:** On NVMe device Samsung I want to search for a string 'U¬' (hexadecimal 55h and AAh), in non-case sensitive mode and only when this string is on fixed position 510 in sector. This could be e.g. master boot record (MBR) or boot sector.
Press a key 'S' for setup, set the parameter 'STRING: position in sector' to 510 and press 'ENTER' to accept.
By pressing 'ALT-F' and then 'ALT-H' you can insert any hexadecimal value.
Press a key 'F' to search for the next occurrence.
Example 2: On NVMe device Samsung I want to search for a string 'NTFS', in non-case sensitive mode and regardless of position in the sector.

Press a key 'S' for setup, set the parameter 'STRING: position in sector' to 'anywhere' and press 'ENTER' to accept.
Press a key 'ALT+F', write 'ntfs' in the STRING field and press 'ENTER' to accept.

Press a key 'F' to search.
Example 3: On NVMe device Samsung I want to search for a string ‘MFT’, in non-case sensitive mode and regardless of position in the sector. Text ‘MFT’ (NTFS Master File Table) is stored as Unicode string.

Press a key ‘S’ for setup, set the parameter ‘STRING: position in sector’ to ‘UNICODE’ and ‘ENTER’ to accept.
Press a key 'ALT+F', write 'mft' in the STRING field and press 'ENTER' to accept.

Press a key 'F' to search.
Search for empty sector

This is usable if you are looking for empty sector (with binary 00h) on device.
ASCII/HEX dump of sector blocks with search and save options. You can dump/save sectors in either text or binary forms.
Press a key 'S' for setup, set the parameter 'STRING: type of object' to 'empty sector' and 'ENTER' to accept.

Press a key 'F' to search.
Search for non-empty sector

This is usable if you are looking for any data on device.

Press a key 'S' for setup, set the parameter 'STRING: type of object' to 'non-empty sector' and 'ENTER' to accept.

Press a key 'F' to search.
**Change the logical sector size**

On some hard drives you can change the size of the logical sector.

For SATA and NVMe drives the values for logical sector size can be set to 512 or 4096, if the disks support those values. The default value is platform dependent.

The current sector size settings can be checked in the device data menu.

**SCSI drives**
SCSI commands
Dump device sectors

Commands for SCSI devices.

1. SCSI Reset
2. Read Defect PList
3. Read Defect GList
4. Change capacity/sector size

Change capacity/sector size.
Not every disk supports changing the block size.
Check the current sector size setting:

- Read capacity: O.K.
- Read mode sense page 01h: O.K.

Change capacity [WDIGTL ENTERPRISE]

Command - Current values | Sectors       | Block size | Capacity
--------------------------|--------------|------------|---------
READ CAPACITY             | 8,515,173    | 512 bytes  | 4.36 GB
MODE SENSE                | 8,515,173    | 512 bytes  | 4.36 GB

Parameters savable: NO
Write-protected: NO

New capacity: 8515173 sectors [4.36 GB]
New block size: 512 bytes

Save mode pages (volatile): NO

Current: Set the current mode sense default values.
Restore: The logical unit shall be set to its maximum capacity.
Format: It can take from several minutes to hours, depending on the drive size.
### SATA drives

The image shows a computer screen displaying information about a SATA drive. The screen contains a table showing device data, including the device model, vendor, logical sector size, physical sector size, and detect mode. There is also a section indicating the extended INT13h status and major/extension version.

The main menu of the software includes options such as file system menu, device data menu, SMART/SCT menu, SET MAX (HPA) menu, device configuration overlay (DCO) menu, hidden areas menu, security menu, commands menu, and save to file menu.
Supported command/feature sets
ATA commands
SATA commands
Dump device sectors

Commands for SATA devices.

1. Set sector configuration

CAUTION! This will OVERWRITE the data on your drive!
Perform the conversion from 512e to 4Kn logical sector size and vice versa. This command sets the device logical block length and number of logical sectors per physical sector.
Check the current sector size setting:

- Logical sector size 4,096 bytes
- Logical sector size 4,160 bytes
- Logical sector size 4,224 bytes
- Logical sector size 512 bytes
- Logical sector size 520 bytes
- Logical sector size 528 bytes

Descriptor 0
CURRENT sector size: logical 512 bytes, physical 4,096 bytes
SELECTED sector size: logical 4,096 bytes (0000|1000h)
Relationship: 0 - 1 logical sector(s) per physical sector
Descriptor check: 0200h
NVMe drives

First we will display the current settings.
Main menu [SK hynix BC501 HFM256GDJTNQ-8310A]

- Device tests menu
- File system menu
- Device data menu
- LOG menu
- Commands menu
- Save to file menu

NSID: 0000|0001h

Move ENTER Select ESC Return

Device data menu [SK hynix BC501 HFM256GDJTNQ-8310A]

- Device data
- PCI controller data
- PCI NVMe Registers
- Dump Namespace Identify
- Dump Controller Identify

NSID: 0000|0001h

Data about the device.

Move S Setup ENTER Run ESC Return
Now we change the sector size from 512 to 4096 bytes.
Press a key 'S' for setup and select the parameter 'LBA Format (LBAF)' to another LBA data size, if supported.
HDAT2 Cookbook (c) 2021 CBL

Format Menu [SK hynix BC501 HFM256GDJTN9-8310A]

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Namespace Identifier (NSID)</td>
<td>0000</td>
</tr>
<tr>
<td>2.</td>
<td>LBA Format (LBAF)</td>
<td>0h</td>
</tr>
<tr>
<td>3.</td>
<td>Secure Erase (SES)</td>
<td>0h - 0000b</td>
</tr>
<tr>
<td>4.</td>
<td>Metadata Settings (MSET)</td>
<td>not supported</td>
</tr>
<tr>
<td>5.</td>
<td>Protection Information (PI)</td>
<td>0h = 0000b</td>
</tr>
</tbody>
</table>

LBA format: selected 0h (active 0h, max. number 1h)
Performance: best
LBA data size: 512 bytes
Metadata size: 0 bytes

↑↓ Move ← Change D Defaults ENTER Accept ESC Cancel

HDAT2 Cookbook (c) 2021 CBL

Format Menu [SK hynix BC501 HFM256GDJTN9-8310A]

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Namespace Identifier (NSID)</td>
<td>0000</td>
</tr>
<tr>
<td>2.</td>
<td>LBA Format (LBAF)</td>
<td>1h</td>
</tr>
<tr>
<td>3.</td>
<td>Secure Erase (SES)</td>
<td>0h - 0000b</td>
</tr>
<tr>
<td>4.</td>
<td>Metadata Settings (MSET)</td>
<td>not supported</td>
</tr>
<tr>
<td>5.</td>
<td>Protection Information (PI)</td>
<td>0h = 0000b</td>
</tr>
</tbody>
</table>

LBA format: selected 1h (active 0h, max. number 1h)
Performance: best
LBA data size: 4,096 bytes
Metadata size: 0 bytes

↑↓ Move ← Change D Defaults ENTER Accept ESC Cancel
## LBA Format Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Erase</td>
<td>disabled</td>
</tr>
<tr>
<td>Protection Information</td>
<td>disabled</td>
</tr>
<tr>
<td>Metadata Settings</td>
<td>not supported</td>
</tr>
<tr>
<td>LBA format</td>
<td>active-0h selected-1h</td>
</tr>
<tr>
<td>Performance</td>
<td>best</td>
</tr>
<tr>
<td>LBA data size</td>
<td>512</td>
</tr>
<tr>
<td>Metadata size</td>
<td>0</td>
</tr>
</tbody>
</table>

NSID: 0000|0001h

**CAUTION! This will OVERWRITE the data on your drive!**

Change the LBA format may require re-partition and re-format the drive.

Format NVM Attributes (FNA): 00h - 00000000b

Format Progress Indicator (FPI): not supported

**FORMAT: S Setup ENTER Run ESC Return**

---

**CAUTION! This will OVERWRITE the data on your drive! ARE YOU SURE <Y/N> ?**
CAUTION! This will OVERWRITE the data on your drive!
Change the LBA format may require re-partition and re-format the drive!
Format NVMe Attributes (FNA): 00h = 00000000
Format Progress Indicator (FPI): not supported

Are you sure to run 'Format Menu' <Y/N>?

Command completed successfully. Press any key...
Now we list the new current settings.
<table>
<thead>
<tr>
<th>Source</th>
<th>Cylinders</th>
<th>Heads</th>
<th>Sectors</th>
<th>Total sectors</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>NVMe</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>62,514,774</td>
</tr>
</tbody>
</table>

**Device model [NVMe/NVMe]**
- Vendor: SK hynix
- Logical sector size: 4,096 bytes
- Physical sector size: 4,096 bytes [4Kn]
- Detect mode: NVMe

**Identify Controller data (CNS=01h)**

- **PCI Vendor ID (VID):** 1C5Ch
- **PCI Subsystem Vendor ID (SSVID):** 1C5Ch
- **Model number:** SK hynix BC501 HFM256GDJTN9-01
- **Serial number:** 0123456789
- **Firmware:** 80002C00
- **NVMe version:** 00010201h = 1.2.1
- **Controller ID:** 0001h
- **IEEE OUI identifier:** ACF42Eh
- **Maximum data transfer size (MDTS):** 05h

---

Page 145
SMART

SMART self-tests

NVMe self-test
Feature Menu
- Self-Test Menu
- Dataset Management Menu
- Format Menu
- Shutdown Menu
- Dump device sectors

NSID: 0000|0001h

Execute built-in Drive Self-Test (DST) running in the background.

↓↓ Move ENTER Run ESC Return

Short Self-Test
Extended Self-Test
Vendor Self-Test
Abort Self-Test
Self-Test Log

NSID: FFFF|FFFFh

Current operation: no test in progress
Last test result: completed without error

5 Setup ENTER Run ESC Return
### Self-Test Log (NSID=FFFF|FFFFh, 564 bytes)

<table>
<thead>
<tr>
<th>Current DST Operation</th>
<th>no test in progress</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current DST Completion</td>
<td>0%</td>
</tr>
</tbody>
</table>

1. Result data (the last one)

<table>
<thead>
<tr>
<th>DST status</th>
<th>10h = 00010000b</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-test code</td>
<td>short test</td>
</tr>
<tr>
<td>Self-test result</td>
<td>completed without error</td>
</tr>
<tr>
<td>Segment number</td>
<td>0</td>
</tr>
<tr>
<td>Valid diagnostics information</td>
<td>00h = 0000000b</td>
</tr>
<tr>
<td>Power on hours (POH)</td>
<td>27 hours (1:03 dd:hh)</td>
</tr>
<tr>
<td>Vendor specific</td>
<td>0000h</td>
</tr>
</tbody>
</table>

2. Result data

entry not used

3. Result data

entry not used

4. Result data

1→→ Move S→→ Save D Dump ESC Return

### Self-Test Menu [SAMSUNG MZVLB256HAHQ-000H1]

- Short Self-Test
- Extended Self-Test
- Vendor Self-Test
- Abort Self-Test
- Self-Test Log

NSID: 0000|0001h

Current operation : no test in progress
Last test result : completed without error
Short Self-Test
Extended Self-Test
Vendor Self-Test
Abort Self-Test
Self-Test Log

NSID: 0000|0001h

Current operation: no test in progress
Last test result: completed without error

Are you sure to run 'Short Self-Test' <Y/N> ?

Short Self-Test
Extended Self-Test
Vendor Self-Test
Abort Self-Test
Self-Test Log

NSID: 0000|0001h

Current operation: short test in progress [scope controller]
Current completion: 21%, remains 79%
(status updates every 5 seconds)

5 Setup ENTER Run A Abort ESC Return
The running test can be interrupted by pressing the 'A' key.
Self-Test Menu [SAMSUNG MZVLB256HAHQ-000H1]

Short Self-Test
Extended Self-Test
Vendor Self-Test
Abort Self-Test
Self-Test Log

NSID: 0000|0001h

Current operation: extended test in progress [scope controller]
Time to complete: 00h:00m:35 s
Current completion: 7%, remains 93%
(status updates every 5 seconds)

Command completed successfully. Press any key...

NSID: 0000|0001h

Current operation: no test in progress
Time to complete: 00h:00m:35 s
Last test result: aborted by self-test command

5 Setup ENTER Run ESC Return
Self-Test Menu [SAMSUNG MZVLB256HAH-Q000H1]

Short Self-Test
Extended Self-Test
Vendor Self-Test
Abort Self-Test
Self-Test Log

NSID: FFFF|FFFFh

Current operation: no test in progress
Last test result: aborted by self-test command

Self-Test Log (NSID=FFFF|FFFFh, 564 bytes)

Current DST Operation: no test in progress
Current DST Completion: 0%

1. Result data (the last one)
DST status: 21h = 00100001b
Self-test code: extended test
Self-test result: aborted by self-test command
Segment number: 7
Valid diagnostics Information: 00h = 00000000b
Power on hours (POH): 870 hours (36:06 dd:hh)
Vendor specific: 0000h

2. Result data
DST status: 10h = 00010000b
Self-test code: short test
Self-test result: completed without error
Segment number: 0
Valid diagnostics Information: 00h = 00000000b
Power on hours (POH): 870 hours (36:06 dd:hh)

↑→ Move S* Save D Dump ESC Return
NVMe device

Examples of some logs for NVMe devices

```plaintext
The controller should clear this log page by removing all entries on power cycle and reset.
```

Page 154
Error (01h) (NSID=FFFF|FFFFh, 16,384 bytes)

Log entry 1 of 256
<empty>

↓↓ Move S ▶ Save D Dump ESC Return

HDAT2 Cookbook (c) 2021 CBL

LOG menu [SAMSUNG MZVLB256HAH0-000H1]

Error (01h)
SMART/Health (02h)
Firmware Slot Information (03h)
Commands supported (05h)
Self-Test (06h)
Telemetry Host (07h)
Telemetry Controller (08h)
Sanitize status (01h)
List of supported log pages

NSID: FFFF|FFFFh

The SMART and health information log is retained across power cycles.

↑↑ Move S Setup ENTER Run ESC Return
SMART/Health (02h) (NSID=FFFF|FFFFh, 512 bytes)

Critical Warning: 00h = 00000000b
Composite Temperature: 0146h
- 326K = 52.85°C = 127.13°F

Available Spare: 100%
Available Spare Threshold: 5%
Percentage Used: 0%
Data Units Read [1,000 units of 512 bytes]: 3,845,130 [1.97 TB]
Data Units Written [1,000 units of 512 bytes]: 4,110,027 [2.10 TB]
Host Read Commands: 178,651,795
Host Write Commands: 119,150,732
Controller Busy Time [min]: 410
Power Cycles: 779
Power On Hours: 870
- 36:06 dd:hh
Unsafe Shutdowns: 84
Media and Data Integrity Errors: 0
Number of Error Information Log Entries: 4,972
Warning Composite Temperature Time: 0 min.
Critical Composite Temperature Time: 0 min.

Move S Setup ENTER Run ESC Return

LOG menu [SAMSUNG MZVLB256HAHQ-000H1]

Error (01h)
SMART/Health (02h)
Firmware Slot Information (03h)
Commands supported (05h)
Self-Test (06h)
Telemetry Host (07h)
Telemetry Controller (08h)
Sanitize status (09h)
List of supported log pages

NSID: FFFF|FFFFh

Move S Setup ENTER Run ESC Return
Firmware Slot Information (03h) (NSID=FFFF|FFFFh, 512 bytes)

Active Firmware Info (AFI)
  -> Running firmware slot: 1
  -> Firmware slot activated next reset: n/a
Firmware Revision for Slot 1 (FRS1) 'EXD70H1Q'
Firmware Revision for Slot 2 (FRS2) ..
Firmware Revision for Slot 3 (FRS3) ..
Firmware Revision for Slot 4 (FRS4) ..
Firmware Revision for Slot 5 (FRS5) ..
Firmware Revision for Slot 6 (FRS6) ..
Firmware Revision for Slot 7 (FRS7) ..

Commands supported (05h)
Self-Test (06h)
Telemetry Host (07h)
Telemetry Controller (08h)
Sanitize status (01h)
List of supported log pages

NSID: FFFF|FFFFh

↑↓→ Move S Setup ENTER Run ESC Return
### Commands supported (05h) (NSID=FFFF|FFFFh, 4096 bytes)

<table>
<thead>
<tr>
<th>Command</th>
<th>CSUPP</th>
<th>LBCC</th>
<th>NCC</th>
<th>NIC</th>
<th>CCC</th>
<th>CSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 (00h)</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>no restriction</td>
</tr>
<tr>
<td>1 (01h)</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>no restriction</td>
</tr>
<tr>
<td>2 (02h)</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>no restriction</td>
</tr>
<tr>
<td>3 (03h)</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>no restriction</td>
</tr>
<tr>
<td>4 (04h)</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>no restriction</td>
</tr>
<tr>
<td>5 (05h)</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>no restriction</td>
</tr>
<tr>
<td>6 (06h)</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>no restriction</td>
</tr>
<tr>
<td>7 (07h)</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>no restriction</td>
</tr>
<tr>
<td>8 (08h)</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>no restriction</td>
</tr>
<tr>
<td>9 (09h)</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>no restriction</td>
</tr>
<tr>
<td>10 (0Ah)</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>no restriction</td>
</tr>
<tr>
<td>11 (0Bh)</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>no restriction</td>
</tr>
<tr>
<td>12 (0Ch)</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>no restriction</td>
</tr>
<tr>
<td>13 (0Dh)</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>no restriction</td>
</tr>
<tr>
<td>14 (0 Eh)</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>no restriction</td>
</tr>
<tr>
<td>15 (0Fh)</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>no restriction</td>
</tr>
<tr>
<td>128 (80h)</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>any namespace</td>
</tr>
<tr>
<td>129 (81h)</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>any namespace</td>
</tr>
</tbody>
</table>

**List of supported log pages**

Error (01h)
SMART/Health (02h)
Firmware Slot Information (03h)
Commands supported (05h)
Self-Test (06h)
Telemetry Host (07h)
Telemetry Controller (08h)
Sanitize status (09h)
Examples of some commands for NVMe devices
Feature Menu
Self-Test Menu
Dataset Management Menu
Format Menu
Shutdown Menu
Dump device sectors

NSID: 0000|0001h

Move ENTER Run ESC Return

Dataset Management range parameters

Range set definition : 1
Starting LBA : 0
Length in logical blocks: 1 [block 512 bytes]
Command Access Size : 0
Write Prepare : disabled
Sequential Write : disabled
Sequential Read : disabled
Access Latency : 0
Access Frequency : 0

NSID: 0000|0001h

Number of range sets: 1
Deallocation attribute: disabled
Deallocated logical blocks returns: not reported

DSM: ← Select range S Setup F Full ENTER Run ESC Return
Dataset Management Menu [SAMSUNG MZVLB256HAHQ-000H1]

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Namespace Identifier (NSID)</td>
<td>0000</td>
</tr>
<tr>
<td>2.</td>
<td>Deallocate (AD) TRIM/UNMAP</td>
<td>disabled</td>
</tr>
<tr>
<td>3.</td>
<td>Integral Dataset for write (IDW)</td>
<td>disabled</td>
</tr>
<tr>
<td>4.</td>
<td>Integral Dataset for read (IDR)</td>
<td>disabled</td>
</tr>
<tr>
<td>5.</td>
<td>Number of range sets (NR)</td>
<td>1</td>
</tr>
<tr>
<td>6.</td>
<td>Select range set definition</td>
<td>1</td>
</tr>
<tr>
<td>7.</td>
<td>Starting LBA</td>
<td>0</td>
</tr>
<tr>
<td>8.</td>
<td>Length in logical blocks</td>
<td>1</td>
</tr>
<tr>
<td>9.</td>
<td>Command Access Size</td>
<td>0</td>
</tr>
<tr>
<td>10.</td>
<td>Write Prepare</td>
<td>disabled</td>
</tr>
<tr>
<td>11.</td>
<td>Sequential Write range</td>
<td>disabled</td>
</tr>
</tbody>
</table>

NSID 00000000h specifies only the controller without any namespaces.
NSID FFFFFFFFh is a broadcast value that is used to specify all namespaces.
Other value specifies the namespace.

Commands menu [SAMSUNG MZVLB256HAHQ-000H1]

- Feature Menu
- Self-Test Menu
- Dataset Management Menu
- Format Menu
- Shutdown Menu
- Dump device sectors

NSID: 0000|0001h

Move ENTER Run ESC Return
1. Arbitration
2. Power Management
3. LBA Range Data
4. Temperature Threshold Feature
5. Error Recovery
6. Volatile Write Cache
7. Number of Queues
8. Interrupt Coalescing

NSID: 0000|0001h, selected: current
FID 03h: saveable, namespace, changeable

Indicates the type and attributes of LBA ranges that are part of the specified namespace.
1. Arbitration
2. Power Management
3. LBA Range Data
4. Temperature Threshold Feature
5. Error Recovery
6. Volatile Write Cache
7. Number of Queues
8. Interrupt Coalescing

NSID: 0000|0000h, selected: current
FID 04h: not saveable, not namespace, changeable

Over and under temperature threshold for composite temperature and temperature sensors.

↑↓ Move S Setp ENTER Run ESC Return
Frequently Asked Questions

1. I received a 40 GB drive in replacement for a 20 GB model in PC. The drive is reported as 20 GB capacity. How can I get full capacity?
2. How to bypass a Security and/or DCO frozen state?
3. Can I remove non-existent bad sectors from the file table FAT?
4. Connecting ATA/IDE Hard Drives
5. What are the differences between master/slave and cable select?
6. Host Protected Area (HPA) vs. 28/48-bit LBA mode
7. Change of DCO Modify item is always aborted (abort command)
8. What is Spread Spectrum Clocking (SSC)?
9. SATA NCQ / eSATA / xSATA
10. Can I cut down size of hard drive?
11. How can I determine supported media format of CD/DVD drive?
12. Portable computer with Windows Vista has problem with power consumption.
13. Host Protected Area (HPA) from BIOS.
14. The Hidden Protected Area (hidden partition).
15. I cannot remove Host Protected Area (HPA) on Dell notebook (Media Direct HPA).
16. I cannot read SMART for USB/FireWire hard drives.
17. Western Digital WD5000KS does not spin-up (firmware bug).
18. How to non-destructively convert dynamic disks to basic disks.
19. Hard disk does not spin-up - PUIS (Power-Up In Standby).
20. Windows support for logical units larger than 2 TB.
21. GUID partition table (GPT) disks.
22. Physical/Logical sector size 512 bytes or 4096 bytes (8*512 = 4 KB).
23. Error Page Fault when the program starts.

Q1: I received a 40 GB drive in replacement for a 20 GB model in PC. The drive is reported as 20 GB capacity. How can I get full capacity?

A1: If you see in 'Device List' menu at your disk drive a notice '!SET MAX: HPA IS ACTIVE', use 1. method, otherwise use 2. method.
In program HDAT2 select your disk drive and press Enter to show 'Main Menu'.

1. method:
In 'Device List' menu at your disk drive you see notice '!SET MAX: HPA IS ACTIVE'.
Select 'SET MAX (HPA) Menu', then select 'Set Max Address' and press Enter. By default is set so called native size of disk drive and you can just press a key 'S' to setup original capacity of hard drive and remove HPA area.
If the command is aborted, try change 'LBA mode' from 28 to 48 or vice versa (if disk supports 48-bit LBA mode).

2. method:
Select 'Device Configuration Menu', then select 'Restore' and press Enter. If you don't see any error message, in 'Device List' menu press a key 'D' to make new detection of devices or simple make restart of PC's and check capacity of your hard drive.
If you see any error message or in 'Device List' menu at your disk you see a notice '!DCO: FROZEN', then it is possible that BIOS was sent a command DCO Freeze and all subsequent DCO commands will be aborted now. How to try bypass this state see answer no. 2.

Q2: How to bypass a Security and/or DCO frozen state?
A2: Turn off PC, remove ribbon (data) cable from this hard drive (not the power cable),
turn on PC and after boot from floppy you can connect ribbon (data) cable back to hard
drive and start up HDAT2. Don't worry - program can detect this device.
Notice: this is valid only for PATA drivers, not for SATA drivers.
If you have SATA drive in Security and/or DCO frozen state, simple solution is connect
this drive to PC with BIOS which does not set security mode.

Q3: Can I remove non-existent bad sectors from the file table FAT?
A3: Yes, with file-system version program HDAT2FS or HDAT2 you can test FAT12/16/32.

- select your drive and press Enter to run Menu
- select 'File Level Tests Menu' and press Enter
- select 'Read File System from MBR' and press Enter
- for item 'All' press 'C' to check detected items
- go to 'Table' item and 2-times press Enter to run Utility menu
- press 'T' to setup test for file table FAT
- if you want to update file table press 'W' for update

This procedure will first compare both FAT copies and second tests all FAT entries for bad
sectors. If program will find 'bad sector' entry, then all sectors in this cluster will be
tested. If all these sectors are not bad program will remove this record of bad sectors.

Q4: Connecting ATA/IDE Hard Drives
A4: ATA/IDE devices use a ribbon cable to connect to each other. Ribbon cables have all
of the wires laid flat next to each other instead of bunched or wrapped together in a
bundle. IDE ribbon cables have either 40 or 80 wires. There is a connector at each end
of the cable and another one about two-thirds of the distance from the motherboard
connector. This cable cannot exceed 18 inches in total length (12 inches from first to
second connector, and six inches from second to third) to maintain signal integrity.

40-wire Cables

On the slower older 40-wire ATA cables, the Slave device, usually a CD-ROM or CD-ROM
recorder/burner still goes on the END, but you need to set the jumpers as Slave. This is
true even if you don't have a hard drive in the Master position. The Master for 40-wire
cables goes on the Middle connector.

If you want to use the cable select with the older drive on a 40-wire cable, you'll have to
consult the maker of the drive for the instructions.

80-wire Cables

On the ATA66/100/133 standard 80-wire cable, the Master hard drive or your boot hard
drive goes on the END of the cable. This is true whether or not you use the Master/Slave
style or the Cable Select style.

The 40-pin 80-conductor cable is orientation specific. The cable connectors are color-
coded: blue for the host connector, black and gray for the primary and secondary disk
drives. The blue connector should be installed into the Primary IDE connector.

The blue connector attaches to the motherboard.
The black connector attaches to the primary, or master, drive.
The gray connector attaches to the secondary, or slave, drive.

Along one side of the cable is a stripe. This stripe tells you that the wire on that side is
attached to Pin 1 of each connector. Wire 20 is not connected to anything. In fact, there
is no pin at that position. This position is used to ensure that the cable is attached to the
drive in the correct position. Another way that manufacturers use to make sure that the
cable is not reversed is by using a cable key. The cable key is a small plastic square on
top of the connector on the ribbon cable that fits into a notch on the connector of the device. This allows the cable to attach in only one position.

Q5: What are the differences between master/slave and cable select?

A5: Two different protocols can be used for jumper ATA devices, including hard disk drives. One is the master-slave relationship. With this protocol, one device is jumpered as master and the other is jumpered as slave. The second protocol is cable select. With this protocol, both devices are jumpered as cable select and their position on the cable dictates which is the master and which is the slave. The end device is master while the device on the middle of the cable is slave. You can use either of these protocols but you cannot mix them on the same data cable.

Computers that use cable-select determine the master and slave drives by selecting or deselecting pin 28, CSEL, on the interface bus. Master and slave drives are determined by their physical position on the cable.

Configuration Using Cable Select

Cable Select is defined in the ATA-2 and ATA-3 specifications and is part of the ATA PnP standard and Microsoft's PC97 standard.

The standard 40-wire ATA ribbon cable and the 80-wire cable give different drive behavior when using Cable Select. If using the standard 40-wire cable, the Master goes in the middle connector and the Slave goes in the end connector. If using the 80-wire cable, attach the blue end connector to the system board or host controller, the gray middle connector to the Slave, and the black end connector to the Master.

All newer ATA hard drives can be jumpered as Cable Select (CS or CSEL). This is an alternate way to indicate which drive is master and which drive is slave (instead of jumper one drive as master and one drive as slave). Cable Select jumper requires a special IDE cable with wire 28 not connected to one of the drive connectors, which would configure the drive attached to that connector as the slave drive.

In order to use Cable Select jumper, several conditions must be met. Both drives on a channel must support CSEL, both drives must be jumpered as CSEL, a CSEL cable must be used, and the host interface connector must support CSEL. For the host interface to support Cable Select, wire 28 must be grounded.

Although the Cable Select specification may simplify things in the future, there will probably be lots of confusion, especially on legacy systems, as this starts to be introduced. One problem will be in selecting the correct cable. Supposedly, the cables used for Cable Select will be clearly marked, with each connector labeled as Device 0 (or Master) or Device 1 (or Slave). If not clearly marked, it may not be easy to identify a CSEL cable visually. Wire 28 can be checked for continuity.

A Cable Select cable can be constructed in various ways. Pin 28 may be not connected to the connector at the end of the cable or to the connector in the middle of the cable. Another design would have the host interface connector in the middle and the two drives would plug into each end of the cable, with the connector at one of the ends not connected to pin 28.

If both drives are set for CSEL and the host interface supports CSEL, but a regular cable is used, both drives will be seen as master.

A Cable Select cable can be used with master/slave drive jumper.

Another problem will be with host interfaces on legacy motherboards and controller cards. If pin 28 is not grounded on the host interface, drives connected to either connector on the CSEL cable will be seen as slave. It will be common to find that pin 28 is open or high on many older IDE interfaces. This can be checked with a voltmeter.
Q6: Host Protected Area (HPA) vs. 28/48-bit LBA mode

A6: There is a problem of incompatibility on some hard drives (e.g. Seagate and/or in an external Maxtor One Touch) when you are using 48-bit command for removing Host Protected Area (HPA) created with 28-bit command. 48-bit command cannot remove HPA created with 28-bit command and vice-versa. Following solution is for disk supports 48-bit LBA mode only and if you have HPA greater than 127 GB.

Solution:

"Some vendor-specific external drive enclosures (Maxtor) are known to use HPA to limit the capacity of unknown replacement hard drives installed into the enclosure. When this occurs, the drive may appear to be limited in size (e.g. 128 GB). In this case, one must use software utilities that use READ NATIVE MAX ADDRESS and SET MAX ADDRESS to change the drive's reported size back to its native size."

Q7: Change of DCO Modify item is always aborted (abort command)

A7: Some hard drives (Maxtor) allow to modify DCO always, the other hard drives (Seagate) allow to modify DCO one times only.

Example of the restrictions on changing of bits:

If a user attempts to change maximum LBA address (SET or RESTORE) after establishing a protected area with SET MAX address, the device will abort that command.

If the user attempts to disable Security feature when the device is enabled and the Security feature is set, the device will abort that command.

If you always got an error message (aborted command) when you want to change any item in DCO Modify menu, you should first run a 'Restore' item to restore default settings and then you can go to Modify menu.

Q8: What is Spread Spectrum Clocking (SSC)?

A8: Spread Spectrum Clocking is a way to lower electromagnetic interference or EMI. This is important for storage solutions that are required to pass FCC and other agency certifications. Today, some Serial ATA disk drives implement SSC, some allow you to turn this feature on/off, and some do not implement SSC; it is anticipated that all will implement this feature in the near future.

The technique of modulating the operating frequency of a circuit slightly to spread its radiated emissions over a range of frequencies rather than just one tone. This reduction in the maximum emission for a given frequency helps meet FCC requirements.

Newer Serial ATA (3Gbps SATA) interface disc drives may employ a standard technology called Spread Spectrum Clocking (SSC) which helps to reduce electronic emissions (EMI) in large, multi-drive systems. Single drive environments do not need SSC to meet EMI requirements.
3Gbps means doubled interface speeds, which also means greater signal noise and electromagnetic emissions. As in the processor settings in many motherboard's BIOS, spread spectrum clocking can reduce emissions to meet regulations.

In a single-drive environment, it's not necessary, but when you've got two or more drives, and they're all running at 3Gbps, that's when you've got a lot of electrical noise going on, and the spread spectrum feature is recommended. This is more for safety than reducing data errors, which most drives' ECC code will correct automatically.

A small number of SATA host products do not support this SSC standard feature. Similarly, RAID controllers may need to enable SSC on drive configurations with SSC disabled by default to reduce EMI.

Disable SSC: Host products that do not support SSC cannot detect the presence of the disc drive. Therefore, in order to disable SSC the drive must be attached to another host platform that does support SSC so that the feature can be disabled. Once SSC is turned off, the drive can be returned to the original host system.

Enable SSC: If the drive has SSC turned off by default and SSC is required for a large multi-drive environment, the target system is usually supported by the SSC software. RAID controllers, however, can pose a barrier to communicating with the SATA at the low hardware level required to make the SSC change. If your RAID controller is not supported then a more standard SATA system may be needed to toggle SSC on the drive. Once SSC is turned on, the drive can be returned to the original RAID controller.

There are many accounts on the Internet about problems arising from HBAs (Host Bus Adapter) not supporting SSC as required. Disk drive vendors that tried turning on SSC have had to provide consumers special programs or jumpers to turn SSC off so they will work in non-compliant systems.

Intel
Apple
Apple discussions
SeriTek controller.Hitachi hard disks
Seagate
Western Digital
Hitachi

Due to this problem, users believe that SATA 3Gb/s HDD’s are not compatible with SATA 1.5Gb/s controllers. This is inaccurate as the technology is definitely backwards compatible.

**Q9: SATA NCQ / eSATA / xSATA**

**A9: NCQ:** NCQ (Native Command Queuing) debuted in many 1.5Gbps drives as a refinement of earlier CQ schemes used in SCSI drives. When a supporting controller sends NCQ-enabled commands to a drive, the drive will intelligently prioritize up to 32 of those commands before performing the reads/writes. Because the controller triggers CQ, the user can enable/disable it in the OS, as from Windows XP's Device Manager. That applications that take advantage of the multithreading features of dual-core and/or Hyper-Threaded processors should complement NCQ for faster throughput.

Explains Native Command Queuing (NCQ) Seagate

eSATA: More of a cable and connector redesign than a fundamental change, eSATA means data cables with better shielding and connectors that are harder to accidentally dislodge or break. The external drive’s power is still supplied separately, eSATA headers are rectangular instead of L-shaped, so eSATA cables won't work inside most PCs. The working group came up with eSATA to address the fact that users were already connecting SATA drives externally because the interface outpaces USB 2.0 and FireWire

Page 168
800Mbps. Shielding that was adequate for use inside a computer case, wasn't good enough outside the box.

xSATA: This option allows the use of much longer external data cables of up to 8 meters in length.

**Q10: Can I cut down size of hard drive?**

A10: Yes. In 'Device List' menu select your disk drive. Select 'SET MAX (HPA) Menu', then select 'Set Max Address' and press Enter. Now you can choose your required size of hard drive. It should be smaller as native (maximal) size of drive, of course. See also question no. 1.

**Q11: How can I determine supported media format of CD/DVD drive?**

A11: In 'Device List' menu select your CD/DVD drive. Select 'Device Information Menu', then select 'Get Configuration' and press Enter. Now you will see list of supported profiles of your drive.

**Q12: Portable computer with Windows Vista has problem with power consumption.**

A12: Power consumption may be slightly more than expected on a portable Windows Vista-based computer that uses a SATA hard disk that does not support Host-Initiated Link Power Management. This problem may occur if the SATA hard disk does not support HIPM. In this case, Windows Vista may not use DIPM for power management. Therefore, the Windows Vista power management feature is less able to efficiently manage power consumption. See MS Article ID: 932079.

**Q13: Host Protected Area (HPA) from BIOS.**

A13: Some motherboards has incorporated the HPA feature in the BIOS. This feature allows information contained in the first partition of the Hard Drive to be copied to a hidden HPA partition on the same drive where it is immune from attack. If the HPA is removed from the HD the area of use will be available at the end of the drive as 'Unallocated'. E.g. Gigabyte's Xpress Recovery.

**Q14: The Hidden Protected Area (hidden partition).**

A14: The Hidden Protected Area is a special area (hidden partition) (usually a few gigabytes in size) located at the end of a hard disk. It is preinstalled on the hard disks of some PC's (e.g. IBM). It is normally hidden to the software running on this PC. It includes all the software and data needed to recover the preloaded state of the PC. This HPA also includes some diagnostic tools and a backup tool. Some vendors are using the HPA instead of providing rescue media. It is referred to as the Predesktop Area in the BIOS Setup Utility. That hidden partition is not an HPA.

**Q15: I cannot remove Host Protected Area (HPA) on Dell notebook (Media Direct HPA).**

A15: With HDAT2 program you did the first half of the fix but missed the second part. The Dell MBR (Master Boot Record at sector 0) calls special code in LBA sector 3 to re-enable the HPA anytime you boot from the hard disk. After you unhide the HPA, in order for it to stay unhidden you need to either get rid of the Dell MBR (so LBA-3 does not get called) or you need to disable LBA-3 (wipe LBA sector 3). (search on Google for 'dell hpa mediadirect')

**Q16: I cannot read SMART for USB/FireWire hard drives.
A16: It all depends on the chip your USB/FireWire enclosures with drive have. The protocol USB-IDE bridge between the USB and ATA protocols should support SMART data and correctly send SMART data over those interfaces. If you cannot see the SMART menu, your drive cannot send SMART data.
Supported bridge chips: Cypress, JMicron and Oxford.
E.g. Western Digital Passport is using Cypress AT2+ USB/ATA interface.

Q17: Western Digital WD5000KS does not spin-up (firmware bug).

A17: Taken over from Google Notebook.
If any controller or software you have enables the "Power-up in Standby" feature on these drives, you cannot disable it. In fact, once that mode is enabled, the drive reports conflicting information.
Western Digital said on the phone the KS line of drives are not a high-enough priority for them to fix the firmware.

Q18: How to non-destructively convert dynamic disks to basic disks.

A18: Read this instruction disk_probe.pdf.

Q19: Hard disk does not spin-up - PUIS (Power-Up In Standby).

A19: The optional Power-Up In Standby (PUIS) feature set allows devices to be powered-up into the Standby power management state to minimize current at power-up and to allow the host to sequence the spin-up of devices.
This optional feature set may be enabled or disabled via the SET FEATURES command or may be enabled by use of a jumper, or both. When enabled by a jumper, this feature set shall not be disabled via the SET FEATURES command.

Once this feature is enabled in a device, the device shall not disable the feature as a result of processing a power-on reset, a hardware reset, or a software reset.

If the device implements this SET FEATURES subcommand and power-up into Standby is enabled, the device shall remain in Standby until the SET FEATURES subcommand is received.

If the device does not implement the SET FEATURES subcommand to spin-up the device after power-up and PUIS is enabled, the device shall spin-up upon receipt of the first command that requires the device to access the media, except the IDENTIFY DEVICE command or the IDENTIFY PACKET DEVICE command.

Solution for HDAT2 program: if you have a hard disk with enabled PUIS (cannot spin up and BIOS cannot recognize this drive) run program with parameter /W Wake/Spin-up the drive:

HDAT2 /W

Without the parameter /W, when PUIS is detected on the disk, the program asks you to turn off PUIS.

List of parameters: HDAT2 /? or HDAT2 /h.

Q20: Windows support for logical units larger than 2 TB.

A20: Disk devices with more than 2 TB of disk space must be converted to GPT format for all of the disk space to be usable. If the device uses MBR format, the disk space beyond 2 TB will be unusable.

Q21: GUID partition table (GPT) disks.
A21: A GPT disk uses the GUID partition table (GPT) disk partitioning system. A GPT disk offers these benefits:

- Allows up to 128 primary partitions. (MBR disks can support up to four primary partitions and an infinite number of partitions inside an extended partition.)
- Allows a much larger volume size - greater than 2 TB, which is the limit for MBR disks.
- Provides greater reliability due to replication and cyclical redundancy check (CRC) protection of the partition table.
- Can be used as a storage volume on all x64-based platforms, including platforms running Microsoft Windows XP Professional x64 Edition. Windows Server 2003 SP1 also enables support for GPT in x86 versions of the Windows Server 2003 family.

Notes:
- Unlike Windows support for the Intel Itanium platform, Windows x64 Edition and Windows Server 2003 SP1 operating systems support the use of GPT drives only as data volumes. Because the x64 and x86 architectures do not provide support for an EFI boot partition, you cannot use a GPT drive to boot an x64-based computer or an x86-based computer with a legacy BIOS. Therefore, computers running these operating systems must be equipped with more than one physical driver to allow the use of the GPT disk format.

On Intel Itanium platforms, Windows supports the use of GPT drives as boot drives or data volumes.

You can convert only empty, unpartitioned disks (raw drives or empty MBR drives) to the GPT format. To convert a volume that contains data, you must first manually delete the partition.

GPT is part of the EFI specification.

Extensible Firmware Interface (EFI) describes an interface between the operating system and the platform firmware.

Unified Extensible Firmware Interface (UEFI) [https://uefi.org/](https://uefi.org/)

UEFI computers require at least three GPT partitions:

1. An EFI system partition (ESP) to store the boot applications and other related information (EFI drivers). Windows does not assign a driver letter to the ESP. This partition should not be used for any user or application data files.

2. A Microsoft reserved (MSR) partition, which must be located between the ESP and the Windows operating system partitions.

3. A Windows system partition.

Q22: Physical/Logical sector size 512 bytes or 4096 bytes (8*512 = 4 KB).

A22: Starting in December 2009, hard disk manufacturers began introducing disks that use 4096-byte sectors rather than the more common 512-byte sectors. Although this change is masked by firmware that breaks the 4096-byte physical sectors into 512-byte logical sectors for the benefit of the operating system, the use of larger physical sectors has implications for disk layout and system performance.

(e.g. "Advanced Format Technology" from Western Digital)

The physical medium is organized in 4 KB sectors but the firmware on the drive will present it as if the drive is composed of 512 byte sectors thus making the drive behave as before, so if the driver asks the hard drive to read 64 sectors from LBA 2048, the firmware will translate it and read 8 4 KB sectors from hardware sector 256. As a result, the hard drive now has two sector sizes - the physical one which the physical media is actually organized in, and the logical one which the firmware presents to the outside world.
Some of the existing BIOSs and/or drivers can't cope with drives which report 4 KB physical sector size. To work around this, some drive models lie that its physical sector size is 512 bytes when the actual configuration is 4 KB without offsetting.

Therefore the information about sector size from ATA IDENTIFY DEVICE command returns an incorrect value (e.g. WD, Samsung).

**Q23: Error Page Fault when the program starts.**

A23: If you start the program HDAT2, you can get the following error:

**Page Fault**
cr2=00400000 at eip=419; flags=3206 Eax=00000300 ebx=00330021 ecx=000000a6 edx=bfeb00bf esi=00000000 edi=00000000 Ebp=00000001 esp=00003ffa cs=87 ds=bf es=b7 fs=0 gs=0 ss=a7 **error=0006**

**In this case you have to use another DPMI server HDPMI32.EXE.**

If you are using a distribution version from HDAT2 web just type HDAT2x instead of HDAT2. It will load the DPMI server HDPMI32, run HDAT2 and then unload HDPMI32 server from memory.

If you are using another version or only single EXE file on e.g. USB device, you have to download the HDPMI32.EXE file, copy this file to your boot medium and run these commands:

```
hdpmi32 -r
hdat2
hdpmi32 -u
```

To get help run

```
hdpmi32 -?
```

License: HDPMI is part of the HX DOS extender runtime, which is freeware. It may be used for any purpose.