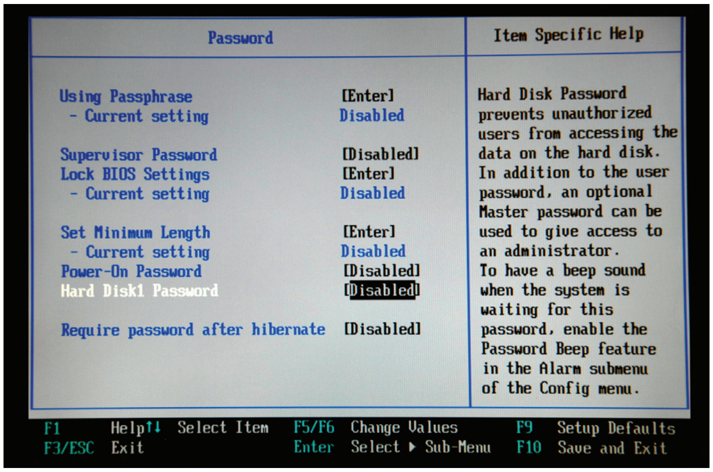
Whitepaper | May 2008

HGST Hard Drives With Bulk Data Encryption Technology — How To Guide

This guide is intended to OEM customers and system integrators help with the setup and use of HGST hard drives with the Bulk Data Encryption feature. It is not intended as an end-user manual.

Requirements to use a HGST hard drive with Bulk Data Encryption:

- BIOS that supports ATA security
- Minimum ATA command set:
  - Set password
  - Unlock drive
  - Disable password
  - Freeze lock
    NOTE: Without freeze lock, virus or malicious code could set a password and cause complete loss of data.
- Optional: Secure erase (no BIOS currently provides this)



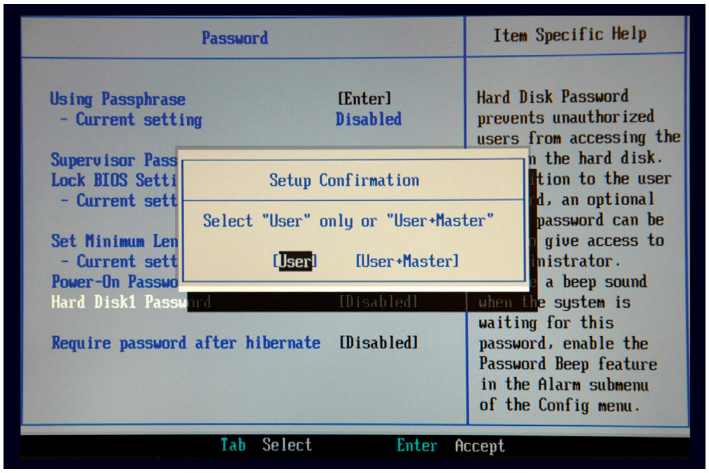
```
                    Password                              Item Specific Help

  Using Passphrase                       [Enter]      Hard Disk Password
   - Current setting                     Disabled     prevents unauthorized
                                                      users from accessing the
  Supervisor Password                    [Disabled]   data on the hard disk.
  Lock BIOS Settings                     [Enter]      In addition to the user
   - Current setting                     Disabled     password, an optional
                                                      Master password can be
  Set Minimum Length                     [Enter]      used to give access to
   - Current setting                     Disabled     an administrator.
  Power-On Password                      [Disabled]   To have a beep sound
  Hard Disk1 Password                    [Disabled]   when the system is
                                                      waiting for this
  Require password after hibernate       [Disabled]   password, enable the
                                                      Password Beep feature
                                                      in the Alarm submenu
                                                      of the Config menu.

F1      Help↑↓  Select Item    F5/F6  Change Values       F9   Setup Defaults
F3/ESC  Exit                   Enter  Select ▸ Sub-Menu   F10  Save and Exit
```

Figure 1: Enable HDD Security
(Security is currently disabled on this system.)

There is an opportunity to set two different passwords: user and master. If you want a system administrator to have the capability of recovering data on a hard disk drive (HDD), then you must have this person set a master password which should be different than the user password.



```
                    Password                              Item Specific Help

  Using Passphrase                       [Enter]      Hard Disk Password
   - Current setting                     Disabled     prevents unauthorized
                                                      users from accessing the
  Supervisor Pass                                    n the hard disk.
  Lock BIOS Setti        Setup Confirmation          tion to the user
   - Current sett                                    d, an optional
                   Select "User" only or "User+Master"  password can be
  Set Minimum Len                                      give access to
   - Current sett       [User]     [User+Master]     nistrator.
  Power-On Passwo                                      a beep sound
  Hard Disk1 Password                    [Disabled]   when the system is
                                                      waiting for this
  Require password after hibernate       [Disabled]   password, enable the
                                                      Password Beep feature
                                                      in the Alarm submenu
                                                      of the Config menu.

                    Tab  Select            Enter  Accept
```

Figure 2: Set User Password

Securing your data

Remember, your drive is not locked until a hard drive password is set.

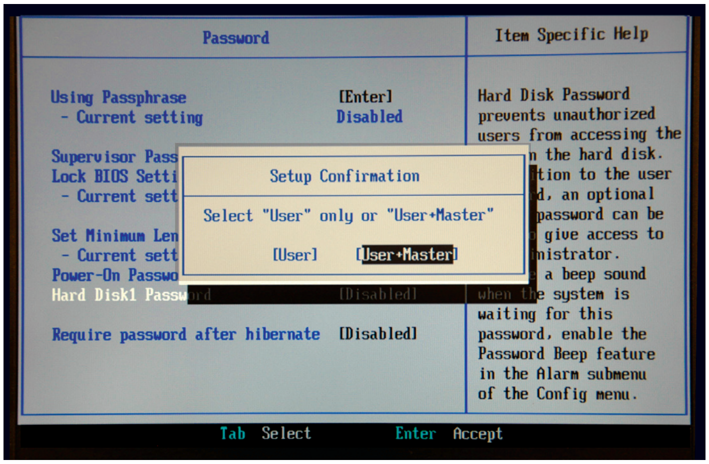
To set the password if you are an end user:

1. Install the drive in a personal computer.
2. Boot system and enter BIOS setup. For help, refer to your PC system manual.
3. Find the security portion of your BIOS (Figure 1) and enable the HDD user password (Figure 2), NOT the BIOS password. Enter the password when prompted. Be sure to remember this password. NOTE: If you lose it, you will lose all access to the programs and data on the computer!
4. Reboot the computer when prompted and enter the user password to allow the computer to start.

Securing your data, continued:

To set the password if you are a system administrator:

1. Install the drive in the personal computer.
2. Boot system and enter BIOS setup. For help, refer to your PC system manual.
3. Find the security portion of your BIOS and enable the HDD (Figure 3) master password in accordance with your corporate IT policy. This password should be recorded and securely stored to allow recovery of the drive hardware. NOTE: Data recovery services cannot recover data from an encrypted drive if the password is lost.
4. Shut down the PC.
5. Provide the PC to the end user and recommend that s/he set the user password in the BIOS per your corporate IT policy (see above).



```
                    Password                         Item Specific Help

 Using Passphrase                  [Enter]         Hard Disk Password
  - Current setting                Disabled        prevents unauthorized
                                                   users from accessing the
 Supervisor Pass                                  n the hard disk.
 Lock BIOS Setti      Setup Confirmation          tion to the user
  - Current sett                                  d, an optional
                 Select "User" only or "User+Master"  password can be
 Set Minimum Len                                   give access to
  - Current sett      [User]    [User+Master]     nistrator.
 Power-On Passwo                                    a beep sound
 Hard Disk1 Password               [Disabled]      when the system is
                                                   waiting for this
 Require password after hibernate  [Disabled]      password, enable the
                                                   Password Beep feature
                                                   in the Alarm submenu
                                                   of the Config menu.

              Tab  Select            Enter  Accept
```

Figure 3: Set Master Password

Security modes

There are multiple security modes. Not all modes are supported in every BIOS such as the one used in these figures. You should discuss the security mode options with your BIOS provider. The security modes with the encrypted drives are no different than those provided with standard HDDs. The difference is that the data is not recoverable without the HDD password.

- *High*: User and master password have the same capabilities in terms of data access. The data on the HDD can be unlocked using either password.
- *Maximum*: The user password is required to unlock the data on the HDD. Without the user password, a system administrator, with only the master password, cannot access the data. S/he can only re-purpose the drive by issuing a "secure erase" command.

Some computer companies offer a password escrow service where a user can save a copy of his password. This may be useful in the event of the user forgetting his or her password. You may want to consider offering this sort of service to your customers of encrypted drives as a value-added service.

Note that the access method to the drive is stored in an encrypted form in redundant locations on the drive.

Secure erase

For more information about secure erase (sanitization), please refer to the National Institute of Standards & Technology (NIST) publication 800-88 "Guidelines for Media Sanitization". HGST hard drives with Bulk Data Encryption implement two recommended methods by the NIST for disk purge: normal secure erase, and enhanced secure erase.

What it does:

1. *Normal mode* writes zeros on every sector on the drive and can take hours to complete. NOTE: the computer must be left on for the entire duration of the secure erase process. Sectors that had been reassigned may not be erased.
2. *Enhanced mode* overwrites the old encryption key. This takes seconds and effectively erases all data on the HDD, including the original sectors that had been reassigned. While the data is physically still present on the drive, it is secured by AES encryption and is inaccessible by all known means since the encryption key is unknown.

How to use it:

User:
You need to have a BIOS that supports secure erase. Since most BIOS' issue a freeze lock to the security state of the drive, a stand-alone application cannot be used to perform the secure erase on the boot drive.

System administrator:
One way is to install the drive into a PC with a BIOS that does not freeze lock the drive. Use PC software that performs the secure erase command, such as HDDErase from the Center for Magnetic Recording Research (CMRR) at the University of California at San Diego (UCSD).

or

Obtain an external enclosure that passes ATA security commands (some USB external enclosures that support SAT (SCSI / ATA Translation) and all eSATA enclosures are suitable). Install the drive into the enclosure and plug it into a PC. Use PC software to perform the secure erase command (referenced above).

Disable security

For an end user to disable security (i.e., turn off the password access control):

1. Enter the BIOS and unlock the drive (when required, BIOS dependent).
2. Find the security portion of your BIOS and disable the HDD user password, NOT the BIOS password. The master password is still set.

For a system administrator to disable security (i.e., turn off the password access control):

1. In high security mode, follow the user mode instructions above.
2. In maximum security mode, disabling security is not available. Only secure erase can return the drive to the security disabled state.

NOTE: All data on the hard drive will be accessible. A secure erase should be performed before disposing or redeploying the drive to avoid inadvertent disclosure of data.

Information and Technical Support

www.hgst.com (Main Web site)
www.hgst.com/partners (Partner Web site)

North America
support_usa@hgst.com
Toll free: 1 888 426-5214,

Asia Pacific
support_ap@hgst.com
65 6840 959

EMEA and UK
support_uk@hgst.com
44 20 7133 0032

Germany
support_uk@hgst.com
49 6929 993601

Program Support
Partners First™ Program
channelpartners@hgst.com

HGST trademarks are intended and authorized for use only in countries and jurisdictions in which HGST has obtained the rights to use, market and advertise the brand. Contact HGST for additional information. HGST shall not be liable to third parties for unauthorized use of this document or unauthorized use of its trademarks.

References in this publication to HGST products, programs, or services do not imply that HGST intends to make these available in all countries in which it operates. Some countries have laws that may affect encryption-enabled devices. HGST assumes no responsibility for compliance with laws that apply to our products after they are sold or outside of our control. Accordingly, we suggest that you review all laws of the countries where you conduct business.

Product specifications provided are sample specifications and do not constitute a warranty. Information is true as of the date of publication and is subject to change. Actual specifications for unique part numbers may vary. Please visit the Support section of our website, www.hgst.com/support, for additional information on product specifications. Photographs may show design models.

HGST, a Western Digital company
3403 Yerba Buena Road
San Jose, CA 95135 USA

Produced in the United States 09/07. Revised 05/08.
All rights reserved.