THE POSSIBILITIES ARE INFINITE FUJITSU

PRODUCT FACTS

HDD Password

Issue May 2009
Product HDD Password

Pages 6

Brief Description

Fujitsu Technology Solutions mainboards support the “HDD Password” feature in the BIOS; this function can activate and manage the Security Mode Feature Set in hard disk drives according to ATA/ATAPI specification version 3 (Jan. 1997) or newer.

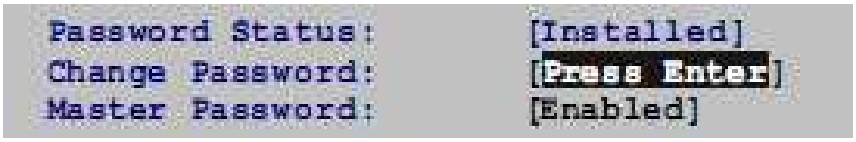
Data stored on such hard disk drives (HDD) can be protected against unauthorized access; the data is accessible only after entering the correct passwords during the system boot process. Each hard disk drive of a PC can be protected via an individual password.

For the feature HDD Password there is an option available called “Master Password”. In case the regular password entry fails due to a lost or forgotten password, the drive can only be accessed if the Master Password feature was enabled and the Master Password is entered correctly. Authorized personal from Fujitsu Technology Solutions can generate this Master Password on request by a customer. The customer has to proof the rightful ownership of the hard disk.

Benefits

- Protection of critical data on HDD’s, e.g. in case of theft or loss
- Easy password handling by built-in BIOS function; no additional software required
- Individual passwords possible for all HDD’s in the system
- With the Master Password feature enabled, the drive can still be unlocked by a Master Password in case of a lost or forgotten password; Fujitsu Technology Solutions can provide this HDD Master password.

HDD Password feature in the BIOS



Functional Description

The BIOS feature “HDD Password” supports the Security Mode Feature Set for hard disk drives according to ATA/ATAPI specification version 3 (January 1997) or newer. This feature was first introduced with notebooks and is now available also for desktop mainboards including mainboards for industrial use.

The Security Mode Feature Set is optional for hard disk drives. However, if implemented, all corresponding security commands must be implemented. The password is stored on the hard disk drive itself. A password protected hard disk drive which is installed in another system can only be accessed using the same password. The mainboard must support the feature in the same manner as the original system. The password feature protects all data stored on a hard disk drive. Each hard disk drive of a PC can be protected via an individual password.

An authorized user has the right to set or change the password for each drive separately.

The supervisor who is allowed to enter the BIOS setup can enable or disable the HDD Password feature.

If the password entry fails five times in a row, the HDD data is not accessible and the system must be switched off. For the feature HDD Password there is an option available called “Master Password”. In case, the Master Password option was set, authorized personal from Fujitsu Technology Solutions can generate a Master Password on request by a customer. The customer has to proof that he is the legitimate owner of the hard disk. This Master Password is capable of unlocking the HDD again in case of a forgotten or lost password. However, if the Master Password feature is disabled, there is no chance to recover the hard disk data.

The following description defines the HDD Password implementation of the Fujitsu Technology Solutions BIOS based on the Phoenix BIOS (currently TrustedCore and SecureCore). There might be a slightly different implementation in the individual BIOS for each mainboard.

Hard Disk Drive Password

The hard disk password will be stored in general on the storage disk of a hard disk drive. Therefore an exchange of the drive electronics will not give access to the password protected data of the hard disk. Note however, that the stored data itself is not encrypted by an encryption algorithm using a standard hard disk. Some special labs offer a service to recover protected hard disks, but a proof of ownership must be given to the labs before they start to recover the data. The rates of such a data recovery are high.

The BIOS supports the “Security Mode Feature Set” of hard disks. The BIOS sends the “Security Freeze Lock” command before booting the operating system. This prevents any application and also malware to change the customer hard disk password after booting.

The password must be 4 to 8 characters in length. All alphanumeric characters can be used, but no distinction is made between upper-case and lower-case characters. During BIOS POST (Power-On Self Test), each hard disk drive will be checked, whether it is locked or not.

Hard disk drives with different passwords have to be unlocked separately by the user. This means that the user has to enter up to 6 different passwords during system start-up. The number depends on the type of the mainboard and the number of hard disks installed in the system.

Besides entering the HDD password for each hard disk, the feature must be enabled in the BIOS Setup Security menu. The option “Password on boot” must be set to “First boot” or “Every Boot”.

Please note that beside the HHD password(s) the user will be asked to enter also the boot password (user password or supervisor password) when booting a system.

At Resume from Suspend, the BIOS automatically unlocks the locked drives which have been unlocked before.

If the password entry fails five times in a row, the HDD data is not accessible and the system must be switched off.

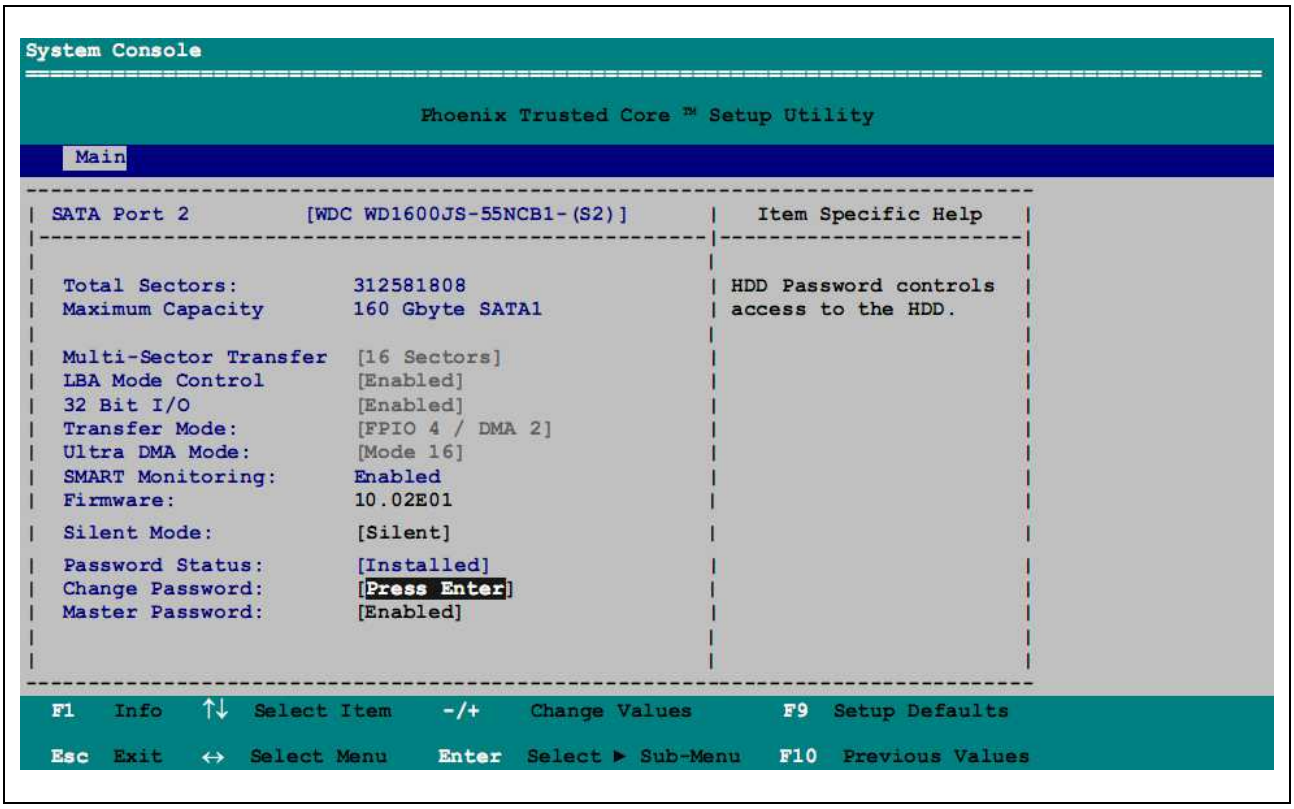
To set the HDD password it must be entered in the BIOS Setup. The BIOS Setup can only be entered if:

- No Supervisor Password is set or
- The Supervisor Password has been entered by the user

A user that does not have the supervisor rights is not allowed to enter the HDD password.

In the BIOS Setup main menu, please select the hard disk drive for which a hard disk password should be assigned. You will get a display similar to the figure below. There might be some slight differences due to the BIOS version and the drive(s) installed.

Figure BIOS Settings for HDD Password



Hard disk drive security setup

Any authorized user (supervisor), who is allowed to enter the BIOS Setup (press <F2> to enter BIOS Setup) is able to either set a password for each hard disk drive separately. The submenu of each hard disk shows the current state of the hard disk drive and allows setting or changing the password, if supported by the selected hard disk drive.

The arrangement of the menu items may vary depending on the BIOS version used. Please consult the actual BIOS manual for details.

Hard Disk Drive Security Status

The hard disk drive security status will be displayed in the BIOS setup for each installed hard disk.

Table Parameter "HDD x Security Status"

Parameter HDD x Security Status	Function
Not supported	The hard disk drive does not support a password. The user cannot assign a password to this hard disk.
Not installed	No password has been assigned to this hard disk.
Installed	A password has just been assigned to the hard disk.
Count Expired	The maximum number of permissible attempts to enter the password has been exceeded. Switch off the system and retry. The maximum number of attempts is 5.
Locked	The hard disk is protected and a password must be entered to get access.
DCO	DCO (Device Configuration Overlay, Power Cycle) is blocked. Switch off the system and retry.
Frozen until Power Off	Restart the system to change the security status of the hard disk. Open the BIOS Setup during system boot and change the desired settings.

Hard Disk Drive Password "Change Password"

This field in the BIOS Setup allows the user to enter a password.

The hard disk password protects the data against unauthorized access. Only users who know the hard disk password can boot the operating system from the hard disk or access data on it.

The password must be 4 to 8 characters in length. All alphanumeric characters can be used, but no distinction is made between upper-case and lower-case characters. Passwords are not displayed during entry. The settings become effective immediately and will remain effective, regardless of the method used to exit the BIOS Setup later. The status of the hard disk password will be displayed according to the current settings (Installed/not installed).

Hard Disk Drive Password "Master Password"

This selection in the BIOS Setup allows the enabling or disabling of the Master Password feature.

The Master Password offers the option to recover from a lost password. If the user hard disk password is lost or forgotten, the access to the data can be obtained by using the master password. For this process, the drive doesn't need to be removed from the PC.

Disabling the Master Password option increases the security of the password protection, but if you lose your password, you will not be able to access your data anymore. All user data will then be lost.

The hard disk drive can be used again for data storage when special equipment is used. Using that special equipment and knowing the master password, special hard disk commands (Security Erase Prepare, Security Erase Unit) will be sent to the hard disk. The hard disk will erase all user data on the disks before allowing using the hard disk again.

The master password can be obtained by contacting Fujitsu Technology Solutions. A proof of rightful ownership of the hard disk must be given to Fujitsu Technology Solutions. The customer will be charged with a lump sum of 25 € + VAT for this service.

Hard Disk Drive Identification Number (HD-ID)

Each hard disk has an individual identification number. This 10-digit HD-ID is shown in the BIOS window for each hard disk when a password is requested.

Dedicated personal from Fujitsu Technology Solutions is authorized to generate a master password for each hard disk drive using this unique hard disk drive identification number (HD-ID). The customer needs to supply the proof for the rightful ownership of the hard disk. The customer will be charged with a lump sum of 25 € + VAT for this service. The master password feature will only work if enabled in the BIOS Setup. Otherwise the data stored on the hard disk is lost if the regular password has been lost or forgotten.

Hard Disk Drive Master Password Request

Please use the form on the next page to request a Master Password from Fujitsu Technology Solutions.

Limitations of HDD Password

Hard disk drives used in a RAID (Redundant Array of Independent Disks) cannot be secured by a password.

Additional information and downloads

- General Information:
  www.ts.fujitsu.com/mainboards
- Documentation and downloads:
  ftp.ts.fujitsu.com/pub/Mainboard-OEM-Sales/

Contact: Fujitsu Technolgy Solutions GmbH:
Peter Hoser / Director OEM Sales, Clients Group, Systemboard OEM
Phone: +49 (0) 821 - 804 3177
Fax: +49 (0) 821 – 804 3329
Email: Peter.Hoser@ts.fujitsu.com

To / An:
Fujitsu Technology Solutions
OEM Team
OEM-sales@ts.fujitsu.com
Fax ++49 (0) 821 804 3329

FUJITSU
THE POSSIBILITIES ARE INFINITE

HDD Password request for Mainboard
Anforderung HDD-Passwort für Mainboard

Techniker / *Field Engineer*:

Name, *First name, Last name*	
Support line-ID	
Telefon / *Phone*	
Fax	

Kunde / *Customer*:

Firma / *Company*	
Ansprechpartner / *Contact*	
Telefon / *Phone*	

Mainboard / *System*:

Typ / *Model*	
Ident-Nr./Serial-Nr.	
HD-ID	

Wird von Fujitsu Technology Solutions ausgefüllt /
Answer from Fujitsu Technology Solutions

HD-Password / *HD-Password*	

Der Kunde erklärt mit seiner Unterschrift, die **rechtmäßigen Eigentumsverhältnisse** an der Festplatte. Bitte **Belege beifügen**. Für die Erzeugung des Master-Passwords wird eine Unkostenpauschale von **25 Euro + MwSt**. berechnet.
The customer declares with his signature the rightful ownership of the hard disk drive. **Please add documents to proof ownership**. The charge for generating the master password is **25 Euro + VAT**.

Datum / *Date*	
Unterschrift / *Signature*	
Unterschrift / *Signature* Technical Support	

Published by department:

Fujitsu Technology Solutions GmbH
Clients Group, Systemboard OEM
Buergermeister-Ulrich-Str. 100
86199 Augsburg, Germany

Company stamp