

BIOS manual for
industrial mainboards with
Intel® H110/Q170/C236 chipset



Congratulations on your purchase of an innovative product from Fujitsu.

The latest information about our products, tips, updates etc. can be found on the Internet at: ["http://www.fujitsu.com/fts/"](http://www.fujitsu.com/fts/)

You can find driver updates at: ["http://support.ts.fujitsu.com/download"](http://support.ts.fujitsu.com/download)

Should you have any technical questions, please contact:

- our Hotline/Service Desk (["http://support.ts.fujitsu.com/contact/service desk"](http://support.ts.fujitsu.com/contact/service desk))
- Your sales partner
- Your sales office

We hope you enjoy working with your new Fujitsu system!



Published by / Contact address in EU

Fujitsu Technology Solutions
Mies-van-der-Rohe-Straße 8
80807 Munich, Germany

<http://www.fujitsu.com/fts/>

Copyright

© Fujitsu Technology Solutions 2016. All rights reserved.

Publication Date

04/2016

Order No.: A26361-D3433-Z330-1-7619, edition 1

BIOS manual for industrial mainboards with Intel® H110/Q170/C236 chipset

Manual

Introduction	9
Navigating BIOS Setup	11
Main Menu – System functions	14
Advanced Menu – Advanced system configuration	16
Security Menu – Security Functions	42
Power Menu – Energy saving functions	53
Event Logs – Configuration and Display of the Event Log	57
Boot Menu – System boot	59
Save & Exit Menu – Finish BIOS Setup	62
BIOS Update	64
Index	67

Remarks

Product description information meets the design requirements of Fujitsu and is provided for comparison purposes. The actual results may differ due to several factors. Subject to technical changes without prior notification. Fujitsu rejects any responsibility with regard to technical or editorial errors or omissions.

Trademarks

Fujitsu and the Fujitsu logo are registered trademarks of Fujitsu Limited or its subsidiaries in the United States and other countries.

Microsoft and Windows are trademarks or registered trademarks of the Microsoft Corporation in the United States and/or other countries.

Intel and Pentium are registered trademarks and MMX and OverDrive are trademarks of Intel Corporation, USA.

PS/2 and OS/2 Warp are registered trademarks of International Business Machines, Inc.

Any other trademarks specified herein are the property of their respective owners.

Copyright

No part of this publication may be copied, reproduced or translated without the prior written consent of Fujitsu.

No part of this publication may be saved or transmitted by any electronic means without the written consent of Fujitsu.

Contents

Introduction	9
Notational conventions	10
Navigating BIOS Setup	11
Open BIOS Setup	11
If you want to open the Boot Menu immediately	12
If you wish to boot immediately from LAN	12
Navigating BIOS Setup	13
Exiting BIOS Setup	13
Main Menu – System functions	14
System Information	14
Open source software license information	14
System Language	14
System Date / System Time	15
Keyboard layout	15
Access Level	15
Advanced Menu – Advanced system configuration	16
Erase Disk	17
Onboard Device Configuration	19
LAN Controller	19
Audio Configuration	19
Auto BIOS Update	19
Terms of Use	20
Automatic BIOS update	20
Update Server address	20
Silent update	20
Manually check for update	21
PCI Subsystem Settings	21
PERR# Generation	21
SERR# Generation	21
PCI Express Slot n	21
Slot n Link Speed	21
CPU Configuration	22
Hyper-threading	22
Active Processor Cores	22
Intel Virtualization Technology	22
VT-d	23
Intel TXT Support	23
Enhanced SpeedStep	23
Turbo Mode	23
Package C State limit	24
Runtime Error Logging	24
ECC Memory Error Logging	24
PCI Error Logging	24
Drive Configuration	24
OffBoard Controller Configuration	25
OnBoard Controller Configuration	25
SMART Settings	26
SMART Self Test	26

Acoustic Management Configuration	26
Acoustic Management	26
Acoustic Mode	27
CSM Configuration	27
Launch CSM	27
Boot Option Filter	27
Launch PXE OpROM Policy	28
TPM (Trusted Platform Module) Computing	28
TPM Support	28
TPM State	28
Pending TPM operation	28
Current TPM Status Information	29
USB Configuration	29
USB Devices	29
Legacy USB Support	29
PS/2 Emulation	30
USB Port Security	30
System Management	31
Firmware Version	31
SMCS Version	31
Fan Startup Check	31
Fan Control	31
FAN 3 Wiring	31
Watchdog Timeout	31
Super IO Configuration	32
Serial Port 1 Configuration	32
Serial Port	32
Device Settings	32
Change Settings	32
Serial Port 2 Configuration	32
Serial Port	33
Device Settings	33
Change Settings	33
Parallel Port Configuration	33
Parallel Port	33
Device Settings	33
Device Mode	34
Serial Port Console Redirection	34
Console Redirection Settings (for COM0 and COM4)	34
Terminal Type	34
Bits per Second	35
Data Bits	35
Parity	35
Stop Bits	35
Flow Control	35
VT-UTF8 Combo Key Support	36
Recorder Mode	36
Resolution 100x31	36
Legacy OS Redirection Resolution	36
Putty KeyPad	36
Redirection After BIOS RESET	36
AMT Configuration	37
ME Version	37

Intel AMT	37
USB Provisioning of AMT	37
Unconfigure AMT/ME	37
MEBx Mode	38
Network Stack	38
Ipv4 PXE Support	38
Ipv6 PXE Support	38
Graphics Configuration	38
Primary Display	39
Internal Graphics	39
DVMT Shared Memory Size	39
DVMT Total Graphics Memory Size	39
UEFI Device Driver Setup	39
North Bridge LVDS Config Select	40
Non-EDID Support	40
LVDS Panel Config Select	40
LVDS Mode	40
LVDS Channel Swap	41
LVDS Backlight-Enable Polarity	41
POST Screen Mode	41
Security Menu – Security Functions	42
Password Description	43
Administrator Password	43
User Password	43
Password Severity	44
User Password on Boot	44
Housing Monitoring	44
Skip Password on automatic Wakeup	44
System Firmware Update	45
Smartcard SystemLock	45
Uninstall SystemLock	45
Single Sign On	45
Smartcard & PIN	46
Unblock Smartcard	46
Easy PC Protection	46
HDD Security Configuration	47
HDD Password on Boot	47
HDD n / HDD-ID	47
HDD Password Description	47
HDD Password Configuration	47
Security Supported	47
Security Enabled	47
Security Locked	47
Security Frozen	47
HDD User Password Status	48
HDD Master Password Status	48
Set User Password	48
Set Master Password	48
Secure Boot Configuration	48
Platform Mode	48
Secure Boot	49
Secure Boot Control	49

Secure Boot Mode	49
Key Management	49
Factory Default Key Provisioning	49
Delete All Secure Boot Variables	50
Enrol All Factory Default Keys	50
Save All Secure Boot Keys	50
Platform Key	50
Key Exchange Key	50
Authorized Signatures	51
Authorized TimeStamps	51
Forbidden Signatures	51
Authorized TimeStamps	52
Power Menu – Energy saving functions	53
Power Settings	53
Power Failure Recovery – System status after a power failure	53
USB Power	54
Power On Source	54
Hibernate like Soft Off	54
Low Power Soft Off	54
Wake-Up Resources	54
LAN	55
Wake On LAN Boot	55
USB Keyboard	55
Wake Up Timer	55
Hour	55
Minute	55
Second	56
Wake Up Mode	56
Wake Up Day	56
Event Logs – Configuration and Display of the Event Log	57
Change SMBIOS event log settings	57
SMBIOS Event Log	57
Erase Event Log	57
When Log is full	58
View SMBIOS Event Log	58
Boot Menu – System boot	59
Boot Configuration	59
Bootup NumLock State	59
Quiet Boot	60
Boot Error Handling	60
Keyboard Error Reporting	60
New Boot Option Policy	60
Power-on Beep	60
Boot Removable Media	60
Virus Warning	61
Boot option priorities	61
Save & Exit Menu – Finish BIOS Setup	62
Save Changes and Reset	62
Discard Changes and Reset	62
Save Changes and Power Off	62

Restore Defaults	63
Save as User Defaults	63
Restore User Defaults	63
Boot Override	63
Diagnostic Program	63
BIOS Update	64
Auto BIOS Update	64
Flash BIOS update under Windows	64
Flash BIOS update with a USB stick	65
BIOS Recovery Update	66
Index	67

Introduction

BIOS Setup provides settings for system functions and the hardware configuration for the system. Any changes you make to the settings take effect as soon as you save the settings and quit *BIOS Setup*.

The individual menus in *BIOS Setup* provide settings for the following areas:







<i>Main:</i>	System functions
<i>Advanced:</i>	Advanced system configuration
<i>Security:</i>	Security functions
<i>Power:</i>	Energy saving functions
<i>Event Logs:</i>	Configuration and display of the event log
<i>Boot:</i>	Configuration of the start-up sequence
<i>Save & Exit:</i>	Save and quit



The setting options depend on the hardware configuration of your system.

Some menus and certain settings may therefore not be available in *BIOS Setup* on your system, or the menus may be in a different place, depending on the *BIOS revision*.

Notational conventions

	Pay particular attention to texts marked with this symbol. Failure to observe this warning endangers your health, destroys the system, or may lead to loss of data. The warranty will be invalidated if the system becomes defective through failure to take notice of this warning.
	Indicates important information which is required to use the system properly.
	Indicates an activity that must be performed.
	Indicates a result.
This font	Indicates data entered using the keyboard in a program dialogue or command line, e.g. your password ((Name123) or a command used to start a program (<code>start.exe</code>).
This font	Indicates information that is displayed on the screen by a program, e.g.: Installation is complete!
<i>This font</i>	Indicates <ul style="list-style-type: none"> • terms and texts used in a software interface, e.g.: Click on <i>Save</i>. • names of programs or files, e.g. <i>Windows</i> or <i>setup.exe</i>.
"This font"	Indicates <ul style="list-style-type: none"> • cross-references to another section, e.g. "Safety information" • cross-references to an external source, e.g. a web address: For more information, go to "http://www.fujitsu.com/fts/" • names of CDs, DVDs and titles or designations for other materials, e.g.: "CD/DVD Drivers & Utilities" or "Safety" manual.
	Indicates a key on the keyboard, e.g:  .

Navigating BIOS Setup



Open BIOS Setup

- ▶ Switch on the system.
- ↳ Wait until the screen output appears.
- ▶ Press function key **F2**.
- ▶ If the system is password protected, you must now enter the password and confirm with the **Enter** key. You will find details on password assignment under "[Password Description](#)", [Page 43](#).
- ↳ The BIOS Setup Main menu will be displayed on the screen.
- ▶ To display system-specific information, select *System Information* and press the **Enter** key.
- ↳ The BIOS release information will be displayed:
 - The revision of the BIOS (e.g. R1.3.0)
Under "Board" you will find the system board number (e.g. D3062-A11)
With the aid of the system board number you can locate the correct technical manual for the system board on the "Drivers & Utilities" CD/DVD. Alternatively you can also use it to download the corresponding BIOS update file from the Internet (see "[BIOS Update](#)", [Page 64](#)).

If you want to open the Boot Menu immediately





You can use this function if you do not wish to boot your system from the drive which is given as the first setting under *Boot Option Priorities* in the *Boot* menu.

- ▶ Start the system and wait until screen output appears.
- ▶ Press the function key **F12**.
- ↳ On the screen, the boot options are shown as a popup window. You can now select the drive from which you wish to boot the operating system. The selection options are the same as the possible settings given under *Boot Option Priorities* in the *Boot* submenu.
- ▶ Use the  and  cursor keys to select which drive you want to boot the operating system from now and confirm your choice with the **Enter** key.















Your selection is only valid for the current system boot. At the next system boot, the settings in the *Boot* menu are valid again.

- ▶ If you want to start the BIOS Setup, use the cursor keys  or  to select the *Enter Setup* entry and confirm your selection with the **Enter** key.

If you wish to boot immediately from LAN

- ▶ Press the function key **F11** if you wish to boot directly via LAN and not from the drive which is given as the first position under *Boot Option Priorities* in the *Boot* menu.

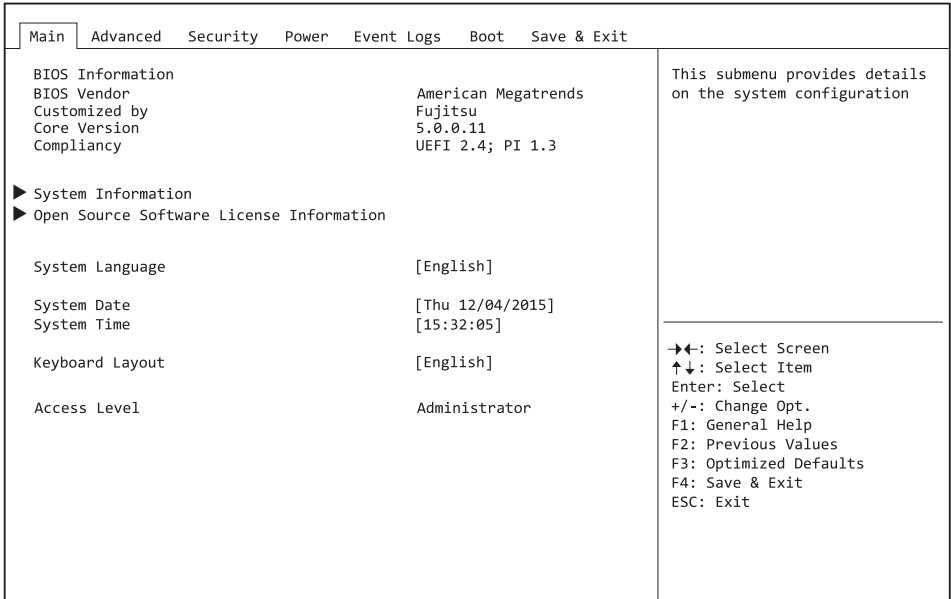
Navigating BIOS Setup

 or  cursor keys	Select menu from menu bar
 or  cursor keys	Select field - selected field is highlighted
 or 	Open submenu (marked by ►)  and leave 
 or  keys (numeric keypad)	Change entry for field
	Set default entries for all menus
	Reset entries that were in use when <i>BIOS Setup</i> was opened.

Exiting BIOS Setup

- ▶ Select the *Save & Exit* menu from the menu bar to end *BIOS Setup*.
- ↳ You can then decide whether you want to save the changed settings.
- ▶ Select the required option.
- ▶ Press the Enter key.

Main Menu – System functions



Example showing the *Main* menu

The *Main Menu* is entered, to determine the basic system configuration and to provide an overview. Some of the parameters are only available under certain conditions.

System Information

The *System Information* submenu gives you an overview of the system configuration. This includes information about the CPU, memory and LAN configuration.

Open source software license information

This submenu provides the licence information for the open source software that is used in this system board.

System Language

Specifies the language used in the *BIOS Setup*.

System Date / System Time

Shows the currently set date / the currently set time of the system. The date has the format "Day of the week, month/day/year". The time has the format "hours/minutes/seconds". If you wish to change the currently set date / the currently set time, enter the new date in the field *System Date* and the new time in the field *System Time*. Use the tab key to switch the cursor between the *System Time* and *System Date* fields.



If the system date & time fields are often set incorrectly when starting the computer, the lithium battery is possibly discharged and must be changed. The procedure for changing the lithium battery is described in the system board manual.

Keyboard layout

Specifies the keyboard layout used in the BIOS Setup.

This menu option can only be selected if no password has been configured, in order to prevent problems when entering a password.

Access Level

Shows the current access level in *BIOS Setup*. If the system is not protected by a password, or an administrator password has been allocated, the access level is Administrator. If administrator and user passwords are allocated, the access level depends on the password entered.

Advanced Menu – Advanced system configuration

The advanced functions which are available to the system are configured in this menu for the advanced system configuration.



Only change the default settings if required for a special purpose.
Incorrect settings can cause malfunctions.

Example showing the *Advanced* menu

Erase Disk

Erase Disk is a firmware incorporated in Fujitsu Technology Solutions (*UEFI: Unified Extensible Firmware Interface*), to erase all data from SATA hard disk(s) or SSDs.

The main purpose of this feature is to irretrievably delete all data from internal or external hard disks or SSDs connected via the eSATA port before the hard disks are discarded or the complete computer system is sold. The function can also be used if hard disks need to be completely deleted, for example before installing a new operating system.



The application can only be selected and run if an administrator/supervisor password has been assigned (*BIOS Setup -> Security Menu*).



To delete hard disks in a RAID system, the mode of the RAID controller must be changed, e.g. to *IDE Mode* or *AHCI Mode* in the *SATA Configuration* submenu of the *Advanced* menu.

To erase data from SATA hard disks or SSDs, proceed as follows:

- ▶ Call up the *BIOS Setup* with the administrator/supervisor password.
- ▶ To start the application, select *Erase Disk* (*BIOS Setup -> Advanced* or *BIOS Setup -> Security*) and set *Start after Reboot*.
- ▶ Then select *Save Changes and Exit* in the menu *Save & Exit / Exit* to initiate a reboot and start *Erase Disk*.



As a result of the reboot, the *Erase Disk* menu is started. You have the option of interrupting the process during the user selection.

- ▶ After the application starts, the administrator/supervisor password must be entered for security reasons.
- ↳ A dialogue field appears in which a particular, several or all the hard disks can be selected for deletion - this depends on the number of hard disks in your system.
- ▶ Select the hard disk(s) to be deleted.
- ↳ The selected hard disk(s) will be deleted one-by-one.



Erase Disk offers four deletion options for hard disks, from "fast" (with one deletion pass) to "very secure" (with 35 deletion passes). Depending on the algorithm chosen, the process can take between ~10 seconds and ~10 minutes per GB:

- *Zero Pattern* (1 pass)
- *German BSI/VSITR* (7 passes)
- *DoD 5220.22-M ECE* (7 passes)
- *Guttmann* (35 passes)



You can find further information on the deletion algorithms here:

- ["https://www.bsi.bund.de/clin_174/DE/Publikationen/publikationen_node.html"](https://www.bsi.bund.de/clin_174/DE/Publikationen/publikationen_node.html)
- ["http://www.usaid.gov/policy/ads/500/d522022m.pdf"](http://www.usaid.gov/policy/ads/500/d522022m.pdf)
- ["http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html"](http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html)



SSD drives are securely erased with the "Enhanced Secure Erase" ATA command integrated in the firmware.

- ▶ Select the desired deletion algorithm for the selected hard disks.



The complete deletion process can be recorded as an audit-compliant log and copied to an external USB stick, which must be formatted as FAT32. Please connect only one external USB stick.

- ▶ Select whether a status report should be written to the USB stick.



The user can select the following tasks which are run by the system after the deletion process:

- *Reset administrator and user password*
- *Load BIOS setup defaults*
- *Shutdown the computer*
- *Exit Erase Disk with no additional options upon completion*

- ▶ Select the function which you require.

↳ The deletion process starts.

Disabled Erase Disk will NOT be started after the next reboot.

Start after Reboot Erase Disk will be started after the next reboot.

Onboard Device Configuration

Opens the submenu to configure devices on the system board. Some of them are only available under certain conditions.

LAN Controller

Specifies whether the LAN controller on the system board is available.

Enabled The LAN controller on the system board is available.

Disabled The LAN Controller on the system board is not available.

Audio Configuration

Azalia HD Audio

Allows the onboard Azalia HD (High Definition) audio controller to be enabled.

Enabled The onboard audio controller is enabled.

Disabled The onboard audio controller is disabled.

Front Panel Audio

Makes it possible to use a legacy front audio connector (AC97). The automatic check of whether an audio connection is occupied is not supported with this setting.

High definition For the use of a high definition audio cable with automatic occupancy recognition.

Legacy For the use of a legacy audio cable without automatic occupancy recognition.

Auto BIOS Update

With Auto BIOS Update it is possible to check a Fujitsu server automatically to see if there is a new BIOS version for the system. For the update, no operating system or external storage medium is required.

To be able to use this function, the computer must have access to the Internet over a network. Access to the Internet must take place via a gateway and a DHCP server must be present in the network for the allocation of IP addresses.



Please also note the terms of use, which are included as an Annex to the BIOS manual or can be found on the Internet at "tou.ts.fujitsu.com".

Terms of Use

In order to be able to use the *Auto BIOS Update* function, you must accept the terms of use, which are included as an Annex to the BIOS manual or can be found on the Internet at "tou.ts.fujitsu.com".

<i>Decline</i>	The Terms of Use were not accepted. The <i>Auto BIOS Update</i> function cannot be used.
<i>Accept</i>	The Terms of Use were accepted. The <i>Auto BIOS Update</i> function can be used.



FLASH Write Support or the System Firmware Update must be enabled before the *Auto BIOS Update* function can be used.

Automatic BIOS update

Defines how frequently BIOS updates are searched for on the Fujitsu server. If the automatic BIOS update function is *disabled*, it is possible under *Manually check for update* to search for BIOS updates at the next system boot.

<i>Disabled</i>	BIOS updates are not automatically searched for.
<i>Daily</i>	BIOS updates are searched for daily.
<i>Weekly</i>	BIOS updates are searched for once per week.
<i>Monthly</i>	BIOS updates are searched for once per month.
<i>Quarterly</i>	BIOS updates are searched for once every three months.

Update Server address

Shows the address of the TFTP server on which BIOS updates are searched for.

The preset Fujitsu Update Server can be reached at the address "webdownloads.ts.fujitsu.com". With the fee-based advanced version of *Auto BIOS Update*, there is the option to use one's own TFTP server. Either a domain name or a direct IPv4 address of the desired update server can be entered.



The name resolution of a domain name occurs at first via the DNS server configured through DHCP. If no DNS server is configured or the DNS server cannot be reached, name resolution is attempted through the Google DNS server via IP address 8.8.8.8. The Neustar DNS service at IP address 156.154.70.1 is used as a second fallback.

Silent update

Defines if the BIOS update, if a new BIOS version is available, is executed automatically without an input request and only a notification is displayed.

<i>Disabled</i>	It is possible to execute the BIOS update immediately, to skip it with this system boot or to ignore the new BIOS version.
<i>Enabled</i>	The BIOS update is executed automatically without an input request.

Manually check for update

Defines if a BIOS update is searched for during the next system reboot.



This function is automatically reset to *disabled* after a search has been performed.

<i>Disabled</i>	No BIOS update is searched for at the next system reboot.
<i>Enabled</i>	A BIOS update is searched for at the next system reboot.

PCI Subsystem Settings

PERR# Generation

Specifies whether PERR# (PCI parity errors) are created.

<i>Disabled</i>	PCI parity errors will not be created.
<i>Enabled</i>	PCI parity errors will be created.

SERR# Generation

Specifies whether SERR# (PCI system errors) will be created.

<i>Disabled</i>	PCI system errors will not be created.
<i>Enabled</i>	PCI system errors will be created.

PCI Express Slot n

Enables or disables the selected PCIe slot.

<i>Disabled</i>	The PCIe slot is disabled and cannot be used.
<i>Enabled</i>	The PCIe slot is enabled and can be used.

Slot n Link Speed

Allows the maximum possible link speed to be limited for individual PCIe slots.

<i>Auto</i>	The card in the slot is operated at the maximum possible link speed.
<i>GEN1</i>	The maximum possible link speed will be limited to GEN1 (2,5 GT/s).
<i>GEN2</i>	The maximum possible link speed will be limited to GEN2 (5 GT/s).
<i>GEN3</i>	If supported by the slot. The maximum possible link speed is limited to GEN3 (8 GT/s).

CPU Configuration

Opens the *CPU Configuration* submenu. Some of the parameters are only available under certain conditions.

Hyper-threading

Hyper-threading technology allows a single physical processor to appear as several logical processors. With this technology, the operating system can better utilise the internal processor resources, which leads to an increase in performance. The advantages of this technology can only be used by an operating system that supports ACPI. This setting has no effect on operating systems without ACPI support.

- Disabled* An ACPI operating system can only use the first logical processor of the physical processor. This setting should therefore only be chosen if the operating system does not support hyper-threading technology.
- Enabled* An ACPI operating system can use all the logical processors of the physical processor.

Active Processor Cores

On processors which contain multiple processor cores, the number of active processor cores can be limited. Inactive processor cores will not be used and are hidden from the operating system.

- All* All available processor cores are active and can be used.
- 1..n* Only the selected number of processor cores is active. The other processor cores are disabled.



The choice made here allows possible problems with certain software packages or system licences to be solved.

Intel Virtualization Technology

Used to support the visualisation of platform hardware and multiple software environments. Based on Virtual Machine Extensions (VMX), to support the application of multiple software environments under the use of virtual computers. The virtualisation technology enhances the processor support for virtualisation purposes on the over 16 bit and 32 bit protected modes and on the Intel® Extended Memory 64 Technology (EM64T) mode.



In active mode, a Virtual Machine Monitor (VMM) can use the additional performance features of the Vanderpool Technology Hardware.

- Disabled* A Virtual Machine Monitor (VMM) cannot use the additional performance features of the hardware.
- Enabled* A VMM can use the additional performance features of the hardware.

VT-d

VT-d (Intel Virtualization Technology for Directed I/O) is a hardware support for the common use of I/O devices by several virtual machines. VMM systems (Virtual Machine Monitor) can use VT-d to manage various virtual machines which access the same physical I/O device.

Disabled VT-d is disabled and is not available for the VMMs.
Enabled VT-d is available for the VMMs.

Intel TXT Support

Enables Trusted Execution Technology (TXT) support. Intel® TXT is available if the CPU in use supports Secure Mode Extensions (SMX), and both Virtualization Technology (VT) and VT-d are enabled in the CPU submenu.



Intel TXT Support must be disabled before BIOS Update of the system is started.

Disabled TXT is disabled.
Enabled TXT is enabled.

Enhanced SpeedStep

Specifies the voltage and frequency of the processor. EIST (Enhanced Intel SpeedStep® Technology) is an energy-saving function.



The processor voltage is adapted to the particular system requirements which are needed at any one time. A reduction in the clock frequency causes the system to require less energy.

Disabled Enhanced SpeedStep functionality is disabled.
Enabled Enhanced SpeedStep functionality is enabled.

Turbo Mode

The processor may work faster than the specified frequency when the operating system requires the maximum performance state (P0). This function is also known as Intel® Turbo Boost Technology.

Disabled Turbo Mode is disabled.
Enabled Turbo Mode is enabled.

Package C State limit

Allows the C state limit of the processor to be configured.

<i>C0</i>	The C state limit is C0.
<i>C2</i>	The C state limit is C2.
<i>C3</i>	The C state limit is C3.
<i>C6</i>	The C state limit is C6.
<i>C7</i>	The C state limit is C7.
<i>C7s</i>	The C state limit is C7s.
<i>Auto</i>	The C state limit is set to the lowest available C state.

Runtime Error Logging

ECC Memory Error Logging

Specifies whether ECC memory errors will be recognised and entered in the event log.

<i>Enabled</i>	Both single-bit memory errors and multi-bit memory errors will be entered in the event log.
<i>Multi-bit Errors Only</i>	Only multi-bit memory errors will be entered in the event log.
<i>Disabled</i>	No memory errors will be entered in the event log.

PCI Error Logging

Specifies whether PCI errors will be entered in the event log.



To be able to recognise PCI errors, the creation of PERR# (PCI parity errors) or SERR# (PCI system errors) must be enabled in advance in the menu *PCI Subsystem Settings*.

<i>Disabled</i>	No PCI errors will be entered in the event log.
<i>Enabled</i>	PCI errors will be entered in the event log.

Drive Configuration

Opens the drive configuration submenu.

OffBoard Controller Configuration



Only visible if there is no OffBoard Controller.

PCIe Controller n Configuration

The PCIe SATA device is connected to the following PCIe device path.

SATA Mode

Specifies the mode in which the SATA ports should be operated.

AHCI The SATA port is operated in AHCI Mode.

RAID (if available) The SATA port is operated in RAID Mode.



To be able to start the RAID Setup during POST, the option *Quiet Boot* must be set to *Disabled*.

OnBoard Controller Configuration

SATA Mode

Specifies in which mode the SATA ports will be operated.

AHCI The SATA port is operated in AHCI Mode.

RAID (if available) The SATA port is operated in RAID Mode.



To be able to start the RAID Setup during POST, the option *Quiet Boot* must be set to *Disabled*.

SATA Port n

Indicates whether the SATA port is available, (*Not Installed*) or which drive is connected to the SATA port.

Port n

Specifies whether the SATA port is available.

Disabled The SATA port n is not available

Enabled The SATA port is available.

External SATA Port

Specifies whether the port will be operated internally as SATA or externally as eSATA.

<i>Disabled</i>	The port will be used internally as SATA.
<i>Enabled</i>	The port will be used as external SATA (eSATA).

Hot Plug

Specifies whether hot plug support of the port is enabled.

<i>Disabled</i>	The hot plug support of the port is disabled.
<i>Enabled</i>	The hot plug support of the port is enabled.

SMART Settings

Opens the submenu for enabling the hard disk self test.

SMART Self Test

Specifies whether the SMART (Self Monitoring, Analysis and Reporting Technology, S.M.A.R.T.) self test is enabled for all hard disks during the POST.

<i>Enabled</i>	The SMART self test is enabled during the POST.
<i>Disabled</i>	The SMART self test is disabled during the POST.

Acoustic Management Configuration

Open the submenu to set the noise level of hard disks or optical drives.

Acoustic Management

Specifies whether the functionality for setting the noise level of hard disks or optical drives (Automatic Acoustic Management) is available.

<i>Disabled</i>	Automatic Acoustic Management is not available.
<i>Enabled</i>	Automatic Acoustic Management is available.

Acoustic Mode

Specifies the noise level of the hard disk or the optical drive. The noise level of the drive is reduced by decreasing its rotational speed. This function must be supported by the drive.



If the functionality for setting the noise level (*Automatic Acoustic Management*) is disabled, the *Acoustic Mode* is *Not Available*. If the functionality for setting the noise level (*Automatic Acoustic Management*) is *enabled*, but is not supported by the connected SATA device, then *Acoustic Mode* is automatically set to *Not supported*.

<i>Bypass</i>	The drive is operated with its preset speed of rotation.
<i>Quiet</i>	The drive is operated with the slowest possible speed of rotation. The drive is operated with lower noise and limited performance.
<i>Medium Performance</i>	The drive is operated with a medium speed of rotation. The drive is operated with reduced noise and slightly reduced performance.
<i>High Performance</i>	The drive is operated at slightly less than the highest possible speed of rotation.
<i>Max Performance</i>	The drive is operated at the highest possible speed of rotation.

CSM Configuration

Opens the submenu for configuring the Compatibility Support Module (CSM).



This submenu is only available if *Secure Boot Control* is disabled under *Setup* → *Security* → *Secure Boot Configuration*.

Launch CSM

Specifies whether the Compatibility Support Module (CSM) is executed. A legacy operating system can only be booted if the CSM has been loaded.

<i>Enabled</i>	The CSM is executed so that a legacy or UEFI operating system can be booted.
<i>Disabled</i>	The CSM is not executed so that a only a UEFI operating system can be booted.

Boot Option Filter

Specifies the drives from which booting can be carried out.

<i>UEFI and Legacy</i>	Booting is possible both from drives with UEFI OS and from drives with Legacy OS.
<i>Legacy only</i>	Booting is only possible from drives with Legacy OS.
<i>UEFI only</i>	Booting is only possible from drives with UEFI OS.

Launch PXE OpROM Policy

Specifies which PXE option ROM is booted. For the PXE boot, both the normal (Legacy) PXE boot and a UEFI PXE boot are available.

- Do not launch* No option ROMs are booted.
- UEFI only* Only UEFI option ROMs are booted.
- Legacy only* Only Legacy option ROMs are booted.

TPM (Trusted Platform Module) Computing

Opens the submenu for enabling TPM and changing the TPM settings. If this setup menu is available, the system board contains a security and encryption chip (TPM - Trusted Platform Module) which complies with TCG specification 1.2. This chip allows security-related data (passwords, etc.) to be stored securely. The use of TPM is standardised and is specified by the Trusted Computing Group (TCG).



For systems that support both TPM 1.2 and TPM 2.0, version switching is not possible in the BIOS Setup. This should prevent operating errors associated with loss of keys. Switching is carried out via Deskview Tools.

TPM Support

Specifies whether the TPM (Trusted Platform Module) hardware is available. If the TPM is disabled, the system behaves like any other system without TPM hardware.

- Disabled* Trusted Platform Module is not available.
- Enabled* Trusted Platform Module is available.

TPM State

Specifies whether TPM (Trusted Platform Module) can be used by the operating system.

- Disabled* Trusted Platform Module cannot be used.
- Enabled* Trusted Platform Module can be used.

Pending TPM operation

Specifies a TPM operation which will be performed during the next boot process. Versions TPM 1.2 and TPM 2.0 are available. TPM 2.0 also has HashPolicy: SHA-1 / SHA-2.

- None* No TPM operation will be performed.
- Enable Take Ownership* The operating system can assume ownership of the TPM.
- Disable Take Ownership* The operating system cannot assume ownership of the TPM.
- TPM Clear* TPM is reset to the factory setting. All keys in the TPM will be deleted.

Current TPM Status Information

Shows the current TPM (Trusted Platform Module) status.

<i>TPM SUPPORT OFF</i>	Is displayed if the <i>TPM Support</i> is disabled.
<i>TPM Enabled Status</i>	Indicates whether TPM can be used.
<i>TPM Active Status</i>	Indicates whether TPM is enabled.
<i>TPM Owner Status</i>	Indicates the TPM owner status.
<i>TPM 2.0</i>	Is displayed if <i>TPM 2.0</i> is available.

USB Configuration

USB Devices

Shows the number of available USB devices, USB keyboards, USB mice and USB hubs.

Legacy USB Support

Specifies whether legacy USB support is available. This function should always be enabled or set to *Auto* so that the operating system can be booted from a USB device if required.

<i>Disabled</i>	Legacy USB support is not available. A USB keyboard or USB mouse can only be used if this is supported by the operating system. Booting the operating system from a USB device is not possible.
<i>Enabled</i>	Legacy USB support is available. A USB keyboard or USB mouse can also be used if the operating system does not support USB. Booting the operating system from a USB device is possible.
<i>Auto</i>	Legacy USB support will be disabled if no USB devices are connected.



Legacy USB support should be disabled if the operating system supports USB and you do not want to boot the operating system from USB devices.

PS/2 Emulation

Enables the use of USB keyboards and mice under operating systems such as Windows 7, which do not support XHCI.

<i>Disabled</i>	PS/2 Emulation is not available. A USB keyboard or USB mouse can only be used if it is supported by the operating system.
<i>Enabled</i>	PS/2 Emulation is available. A USB keyboard or USB mouse can be used even if the operating system does not support USB.

USB Port Security

Opens the *USB Port Security* submenu in order to configure the USB interfaces present on the mainboard.

USB Port Control

Configures the use of the USB ports. Disabled USB ports are only available during the POST, but are no longer available under the operating system.



During POST, a USB mouse and a USB keyboard are also available if the corresponding USB port is disabled.

<i>Enable all ports</i>	All USB ports are enabled.
<i>Disable all ports</i>	All USB ports are disabled.
<i>Enable front and internal ports</i>	All USB ports on the rear of the device are disabled.
<i>Enable rear and internal ports</i>	All USB ports on the front of the device are disabled.
<i>Enable internal ports only</i>	All external USB ports are disabled.
<i>Enable used ports</i>	All unused USB ports are disabled.

USB Device Control

For the *Enable front and internal ports*, *Enable rear and internal ports* and *Enable used ports* settings, which were made under *USB Port Control*, there are additional options available here.

<i>Enable all devices</i>	Those settings made under <i>USB Port Control</i> will be used without any limitation.
<i>Enable Keyboard and Mouse only</i>	Only USB keyboards and USB mice can be operated at the USB ports enabled under <i>USB Port Control</i> . Any ports to which no USB keyboards or USB mice are connected are disabled. Keyboards with an integrated hub result in deactivation of the port.
<i>Enable all devices except mass storage devices/Hubs</i>	USB ports on which USB storage devices or USB hubs are connected will be disabled.

System Management

Firmware Version

Shows the firmware version of the system monitoring controller.

SMCS Version

Shows the SMCS version (Systemboard Management Configuration Settings).

Fan Startup Check

Allows you to check the start-up of fans at system boot. This can prolong the duration of the system boot by a few seconds.

Disabled The system does not wait for the fans to start up. A fan startup check is not executed.

Enabled The system waits for the fans to start up. The fan startup check is executed.

Fan Control

Controls the speed of the fan. The preset mode can be changed depending on the system configuration and the applications used.

Enhanced (if available) The fan speed will be increased automatically so that the maximum CPU performance is achieved.

Auto The fan speed is adjusted automatically. A compromise between system temperature and CPU performance.

Full All fans are operated at maximum speed.

FAN 3 Wiring

Determines whether a three-wire or four-wire fan is connected to fan connector FAN 3.

3 wires A three-wire fan is connected.

4 wires A four-wire fan is connected.

Watchdog Timeout

Specifies the time after which a system restart is performed, if this is enabled by Boot Watchdog.

The permitted values are: 0 to 225

0...225 The system is restarted after the set time (minutes) has elapsed.

Super IO Configuration

Serial Port 1 Configuration

Opens the submenu for configuration of the serial port 1 (COMA).

Serial Port

Specifies whether the serial port is available.

<i>Disabled</i>	The serial port is not available.
<i>Enabled</i>	The serial port is available.

Device Settings

Shows the base I/O address and the interrupt used for access to the parallel port.

Change Settings

Specifies which base I/O addresses and which interrupts can be used for the particular serial port by the BIOS or the operating system.

<i>Auto</i>	The base I/O address and the interrupt are automatically assigned.
<i>IO=3F8h; IRQ=4;</i>	The base I/O address 3F8h and the interrupt 4 are permanently assigned.
<i>IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12;</i>	The base I/O address is permanently assigned.
<i>IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12;</i>	
<i>IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12;</i>	
<i>IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;</i>	

The values given in the list are available for the interrupt for automatic selection by the BIOS or the operating system.



If conflicts with other devices occur, this option should be converted to *Auto*.

Serial Port 2 Configuration

Opens the submenu for configuration of the serial port 2 (COMA).

Serial Port

Specifies whether the serial port is available.

<i>Disabled</i>	The serial port is not available.
<i>Enabled</i>	The serial port is available.

Device Settings

Shows the base I/O address and the interrupt used for access to the parallel port.

Change Settings

Specifies which base I/O addresses and which interrupts can be used for the particular serial port by the BIOS or the operating system.

<i>Auto</i>	The base I/O address and the interrupt are automatically assigned.
<i>IO=2F8h; IRQ=3;</i>	The basic I/O address 2F8h and the Interrupt 3 are firmly allocated.
<i>IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12;</i>	The base I/O address is permanently assigned.
<i>IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12;</i>	
<i>IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12;</i>	
<i>IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;</i>	

The values given in the list are available for the interrupt for automatic selection by the BIOS or the operating system.



If conflicts with other devices occur, this option should be converted to *Auto*.

Parallel Port Configuration

Opens the submenu to configure the parallel port (LPT).

Parallel Port

Specifies whether the parallel port is available.

<i>Disabled</i>	The parallel port is not available.
<i>Enabled</i>	The parallel port is available.

Device Settings

Shows the base I/O address and the interrupt used for access to the parallel port.

Device Mode

Specifies whether the parallel port should be used as an input/output port or just as an output port. The ECP and EPP transfer modes permit higher transfer speeds of 2 or 2.4 MB/sec. These modes can however only be used on devices which also support these modes. In addition, for EPP the I/O address of the parallel port must be set to 378 h or 278 h.

<i>STD Printer Mode</i>	Switches to STD printer mode.
<i>SPP Mode</i>	The standard mode will be used for the parallel port.
<i>EPP-1.9 and SPP Mode</i>	Standard and fast transfer mode (up to 2 MB/sec), data output and data reception are possible. The mode requires a peripheral device which supports the EPP (Enhanced Parallel Port) mode.
<i>EPP-1.7 and SPP Mode</i>	Standard and fast transfer mode (up to 2 MB/sec), data output and data reception are possible. The mode requires a peripheral device which supports the EPP (Enhanced Parallel Port) mode.

Serial Port Console Redirection

<i>Disabled</i>	Serial Port Console Redirection is not available.
<i>Enabled</i>	Serial Port Console Redirection is available.

The parameters for terminal communication via Serial Port Console Redirection can be shown and set in this submenu. Some parameters are only available under certain conditions.

Console Redirection Settings (for COM0 and COM4)

Specifies the data exchange process of the host and remote system via the COM0 and COM4 ports (iAMT/SOL (Serial overLAN)).



Both systems require identical or compatible settings.

Terminal Type

Specifies the type of terminal.

Permitted values: VT100, VT100+, VT-UTF8, ANSI



The terminal type allocated will be used to transfer data to the host.

Bits per Second

Specifies the transfer rate for communication with the host.

Permitted values: 9600, 19200, 38400, 57600, 115200



The data will be transferred to the host at the transfer rate set.

Data Bits

Shows the number of data bits used for communication with the host.

- 7 Seven data bits are used for the communication.
- 8 Eight data bits are used for the communication.

Parity

Specifies the use of parity bits for communication with the host. Parity bits are used for error detection.

- None* No parity bits are used. Error detection is not possible.
- Even* Parity bit is 0 if the number of ones in the data bit is an even number.
- Odd* Parity bit is 0 if the number of ones in the data bit is an odd number.
- Mark* Parity bit is always 1.
- Space* Parity bit is always 0.

Stop Bits

Shows the number of stop bits used to indicate the end of a serial data packet.

- 1 One stop bit is used.
- 2 Two stop bits are used.

Flow Control

This setting determines the transfer control over the interface.

- None* The interface is operated without transfer control.
- Hardware CTS/RTS* The transfer control is undertaken by the hardware. This mode must also be supported by the cable.

VT-UTF8 Combo Key Support

Specifies whether VT-UTF8 combination key support for ANSI/VT100 terminals is available.

<i>Disabled</i>	VT-UTF8 combination key support is not available.
<i>Enabled</i>	The VT-UTF8 combination key support is available.

Recorder Mode

Specifies whether only text will be sent. This is used to capture terminal data.

<i>Disabled</i>	Recorder mode is not available.
<i>Enabled</i>	Recorder mode is available.

Resolution 100x31

Indicates whether enhanced terminal resolution is available.

<i>Disabled</i>	Enhanced terminal resolution is not available.
<i>Enabled</i>	Enhanced terminal resolution is available.

Legacy OS Redirection Resolution

Specifies the number of lines and columns for the legacy OS redirection.

<i>80x24</i>	Resolution 80x24 is used.
<i>80x25</i>	Resolution 80x25 is used.

Putty KeyPad

Sets FunctionKey and KeyPad to Putty.

<i>VT100</i>	Selects VT100.
<i>LINUX</i>	Selects LINUX.
<i>XTERMR6</i>	Selects XTERMR6.
<i>SCO</i>	Selects SCO.
<i>ESN</i>	Selects ESN.
<i>VT400</i>	Selects VT400.

Redirection After BIOS RESET

<i>BootLoader</i>	Legacy Console Redirection is disabled before Legacy OS is started.
<i>Always Enable</i>	Legacy Console Redirection is enabled for Legacy OS.

AMT Configuration

Opens the submenu to configure Intel® Active Management Technology.

ME Version

Shows the current AMT/ME version.

Intel AMT

Enables/disables Intel (R) Active Management Technology BIOS Extension.



iAMT H/W is always enabled. This option simply controls the execution of the BIOS Extension.

If this option is enabled, an MBEx (Management Engine BIOS eXtension) query occurs at the next reboot to establish whether the AMT/ME configuration should be reset to the default values.

<i>Disabled</i>	Do not change the AMT/ME configuration.
<i>Enabled</i>	Start the reset of the AMT/ME configuration. The option is then automatically reset to <i>Disabled</i> .

USB Provisioning of AMT

Enables/disables AMT-USB provisioning.

If this option is enabled, an MBEx (Management Engine BIOS eXtension) query occurs at the next reboot to establish whether the AMT/ME configuration should be reset to the default values.

<i>Disabled</i>	Do not change the AMT/ME configuration.
<i>Enabled</i>	Start the reset of the AMT/ME configuration. The option is then automatically reset to <i>Disabled</i> .

Unconfigure AMT/ME

If this option is enabled, an MBEx (Management Engine BIOS eXtension) query occurs at the next reboot to establish whether the AMT/ME configuration should be reset to the default values.

<i>Disabled</i>	Do not change the AMT/ME configuration.
<i>Enabled</i>	Start the reset of the AMT/ME configuration. The option is then automatically reset to <i>Disabled</i> .

MEBx Mode

Configure how the MEBx (Management Engine BIOS eXtension) behaves during the reboot.

Normal The message **Ctrl + P** to open the MEBx Setup will be displayed during the POST.

Enter MEBx Setup The MEBx Setup will be automatically called during the next POST.

Network Stack

Specifies whether the UEFI Network Stack is available for network access under UEFI. If the UEFI Network Stack is disabled, UEFI installation via PXE is not possible, for example.

Disabled The UEFI Network Stack is not available.

Enabled The UEFI Network Stack is available.

Ipv4 PXE Support

Specifies whether PXE UEFI Boot via Ipv4 is available for installation of operating systems in UEFI mode.

Disabled PXE UEFI Boot via Ipv4 is not available.

Enabled PXE UEFI Boot via Ipv4 is available.

Ipv6 PXE Support

Specifies whether PXE UEFI Boot via Ipv6 is available for installation of operating systems in UEFI mode.

Disabled PXE UEFI Boot via Ipv6 is not available.

Enabled PXE UEFI Boot via Ipv6 is available.

Graphics Configuration

Opens the submenu for configuring the graphics controller on the system board.

Primary Display

Specifies which display adapter is connected to the primary monitor. The primary monitor is used during system boot (POST).

<i>Auto</i>	External display adapters are preferred. If there is no external display adapter, the internal display adapter is used.
<i>Internal Graphics (if available)</i>	The internal display adapter is used.
<i>PCI Express for Graphics (PEG)</i>	The display adapter in the PCI-Express slot for graphics is used.
<i>PCI Express (PCIe)</i>	The display adapter in a PCE Express slot is used.

Internal Graphics

Allows you to switch the internal display adapters on or off. With the Auto setting, the BIOS automatically determines the configuration. Specifies which display adapter is connected to the primary monitor. The primary monitor is used during system boot (POST).

<i>Auto</i>	The BIOS determines the configuration automatically and switches the internal display adapter on or off.
<i>Disabled</i>	The internal display adapter is switched off.
<i>Enabled</i>	The internal display adapter is switched on.

DVMT Shared Memory Size

Defines the memory size that can be used by the internal display adapter.

<i>32 MB... 1,536 MB</i>	Memory size of the preset, shared main memory.
--------------------------	--

DVMT Total Graphics Memory Size

Defines the total size of the memory that can be used by the internal display adapter.

<i>128 MB</i>	128 MB of the main memory can be used by the internal display adapter.
<i>256 MB</i>	256 MB of the main memory can be used by the internal display adapter.
<i>MAX</i>	The size of the main memory that can be used by the internal display adapter is dynamically allocated.

UEFI Device Driver Setup

A UEFI device driver can support the interface to UEFI-FW Setup and makes information and menu items available. Available UEFI device drivers are, for example, Intel® Ethernet Connection I217-LM and Intel® I210 Gigabit.

North Bridge LVDS Config Select

Opens the submenu to configure the LVDS interface for direct connection of an LCD panel.

Non-EDID Support

There is no EDID (Extended Display Identification Data) available for LCD panels which do not support DDC (Display Data Channel).



Enabled must be set for an LCD panel without EDID support.

For installation of a Linux operating system, despite a connected LVDS panel without DDC support, it may be necessary to first select *Non-EDID Support = Disabled*.

After the Linux and driver installation has been completed, *Non-EDID Support = Enabled* can then be set again.

Disabled

The LCD makes EDID available.

Enabled

The LCD does not make EDID available.

LVDS Panel Config Select

Specifies the resolution of the LVDS (Low Voltage Differential Signaling) interface. The selected resolution should correspond to that of the connected LCD panel.



By using the OEM tool *LVDS*, an additional entry *LVDS Adjusted Parameters* can be created, which makes it possible to use freely configurable LVDS parameters.

LVDS Mode

The selected mode of the LVDS interface must be supported by the LCD panel used.



A faulty representation of colours often means an incorrectly set LVDS mode.

FPDI 8-bit

The FPDI (Flat Panel Interface) 8-bit mode will be used.

FPDI 6-bit

The FPDI (Flat Panel Interface) 6-bit mode will be used.

LDI 8-bit

The LDI (LVDS Display Interface) 8-bit mode will be used.

LDI 6-bit

The LDI (LVDS Display Interface) 6-bit mode will be used.

LVDS Channel Swap

Depending on the LCD panel connected, the channels of the LVDS interface can be swapped.

- Disabled* The channels of the LVDS interface will not be swapped.
Enabled The channels of the LVDS interface will be swapped.

LVDS Backlight-Enable Polarity

The polarity for switching on the background lighting can be set depending on the LCD panel connected.

- Active High* The polarity for switching on the background lighting of the LCD panel is Active High.
Active Low The polarity for switching on the background lighting of the LCD panel is Active Low.

POST Screen Mode

Specifies whether the output during POST is in graphics mode or text mode.



For LCD panels with a resolution less than 800 x 600, text mode must be selected to see the output during POST.

- Graphic Mode* During POST and BIOS Setup, the system is in graphics mode.
Text Mode During POST and BIOS Setup, the system is in text mode.

Security Menu – Security Functions

The *Security* menu offers various options for protecting your system and personal data from unauthorised access. Using a sensible combination of these options will help you achieve maximum protection for your system.

The following security settings can be made in this menu. Some of them are only available under certain conditions.

Main	Advanced	Security	Power	Event Logs	Boot	Save & Exit
<p>Password Description</p> <p>If the Administrator's password is set, then this limits access to Setup and is asked during boot or when entering Setup. If the User's password is set, then this is a power on password and must be entered to boot or enter Setup. In Setup the User will have USER rights.</p> <p>The password length must be in the following range:</p> <p>Minimum length 3</p> <p>Maximum length 32</p> <p>Administrator Password</p> <p>User Password</p> <p>Password Severity [Standard]</p> <p>Password on Boot [Disabled]</p> <p>Skip Password on automatic Wakeup [Disabled]</p> <p>System Firmware Update</p> <p>HDD Security Configuration:</p> <p>HDD Password on Boot [Enabled]</p>						<p>Set Administrator Password</p> <hr/> <p>→←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit</p>

Password Description

Neither an administrator password nor a user password has been allocated

Opening the BIOS Setup and booting the system are possible without restriction.

Only the administrator password was allocated

If ONLY an administrator password was allocated, only the BIOS Setup is protected. Booting the system can be performed without restriction. When you access the BIOS Setup with an administrator password, the Administrator access level is assigned to you and you have unrestricted access to the BIOS Setup. If you access the BIOS Setup without a password, access to the BIOS Setup is limited because you are only assigned the User access level.

Administrator AND user passwords were allocated

If administrator and user passwords were allocated, the authorisation level in the BIOS Setup depends on the password entered. If you access the BIOS Setup with the administrator password, unlimited access to the BIOS Setup is possible, entry of the user password results in limited access. Booting the system is possible both with the administrator and also with the user password.



If the administrator password is deleted, the user password will also be deleted.

The system will stop after an incorrect password has been entered three times. If this happens, switch off the system and then back on again, and enter the correct password.

Administrator Password

If you press the enter key, a window will open in which you can assign the administrator password. Enter a character string to define the password. If you confirm an empty password field, the password will be deleted.



To call up the complete BIOS Setup, you need the administrator level of access. If an administrator password is allocated, the user password only allows very limited access to the BIOS Setup.

User Password

If you press the enter key, a window will open in which you can assign the user password. Enter a character string to define the password. With the user password, you can prevent unauthorised access to your system.



In order to be able to assign a user password, an administrator password must already have been assigned.

Password Severity

Defines ways to access the system if the password has been forgotten.

<i>Standard</i>	A forgotten password can be deleted using the Password skip jumper.
<i>Strong</i>	It is not possible to use the Password skip jumper. If a password has been forgotten, only the certified, technical support team can enable it.
<i>Stringent</i>	It is not possible to use the Password skip jumper. If a password has been forgotten, the system remains permanently unusable.

User Password on Boot

Specifies whether a user password must be entered before the boot process.

<i>On Every Boot</i>	Entry of a user password is required before every boot process.
<i>On First Boot</i>	The user password must be entered with every cold start boot process.
<i>Disabled</i>	The system starts without requiring the entry of a user password.



If the administrator password and the user password have been assigned and the setting *Disabled* has been chosen for this item, simply press Enter to get USER access to the BIOS Setup. In this case the user password does not have to be entered.

Housing Monitoring

Specifies whether opening of the casing should be monitored.

<i>Disabled</i>	The system continues to operate normally, even if the casing was opened.
<i>Enabled</i>	If the casing has been opened, then the boot process is suspended until BIOS Setup is called. If the BIOS Setup is protected with a password, then this must be entered. An SMBIOS event log entry will be generated.

Skip Password on automatic Wakeup

Specifies whether the user password is skipped or requested when the system is started automatically.

<i>Disabled</i>	The user password is not requested during automatic start processes.
<i>Enabled</i>	The user password is requested.

System Firmware Update

Defines how the system firmware (BIOS) update is carried out.

<i>Disabled</i>	The system firmware (BIOS) cannot be written. A flash BIOS update is not possible.
<i>Restricted</i>	The system firmware (BIOS) can only be updated via FUJITSU Tools, automatic update via Windows Update (WU) is prevented.
<i>Enabled</i>	The system firmware (BIOS) can be updated both via FUJITSU Tools and automatically via Windows Update (WU).

Smartcard SystemLock

With SystemLock (Smartcard Pre-boot Authentication - PBA), the PC can only be started with an initialised Smartcard and personal identification number (PIN). Smartcard and PIN are already checked during system booting in the BIOS, i.e. before the operating system is booted.

The OS application SystemLock Manager is used to initialise the Smartcard(s). Systems without the menu item *Smart Card System Lock* do not support the SystemLock function.



Settings in the *Smartcard SystemLock* menu can only be changed with an Admin Smartcard.



If the Smartcard is defective or unavailable, the user can get authorisation for a boot process either from the local administrator or from the Fujitsu Service Desk.

Uninstall SystemLock

Uninstalls the *Smartcard Security* function.



To reinstall SystemLock it will be necessary to reinitialise your Smartcards.

<i>No</i>	Smartcard Security is not uninstalled.
<i>Yes</i>	Smartcard Security is disabled during the next boot process.

Single Sign On

The *Single Sign On* function allows the BIOS to communicate with a different application during logon to the operating system, in order to determine the Smartcard access rights.

<i>Disabled</i>	Single Sign On is not available.
<i>Enabled</i>	Single Sign On is available.

Smartcard & PIN

Determines whether an authorised Smartcard is needed for access to the system.

<i>Always Required</i>	An authorised Smartcard is needed to access the system.
<i>Ignore on WOL</i>	If the Wakeup On LAN function is enabled, the Smartcard Security function is bypassed.

Unblock Smartcard

To assign a new PIN if the PIN is not known or the Smartcard is blocked.



The Smartcard becomes blocked after 3 incorrect attempts to enter the PIN, and it will be blocked permanently after 10 incorrect attempts to enter the PUK. Please note that the default PIN and PUK for a new Smartcard is always 12345678. This PIN/PUK must be changed for security reasons.

<i>Prohibited</i>	No new PIN can be assigned.
<i>Allowed</i>	A new PIN can be assigned.

Easy PC Protection

Easy PC Protection bypasses the start password, if the start permission confirmation is issued via the local network (LAN).

If the system is connected to the corporate LAN, the start configuration will be read from the TFTP server. All required data (name of start configuration file, IP address of TFTP server, name of system) is saved in the *System Data* area.



To set the *Easy PC Protection* function to *Enabled*, the *Network Stack* function must first be set to *Enabled*.

<i>Disabled</i>	Easy PC Protection is not available.
<i>Enabled</i>	Easy PC Protection is available.

Current Configuration set:

- Server IP address, e.g. 192.168.1.1
TFTP server IP address providing the boot grant configuration data
- Schedule, e.g. Development_Department
System identification name
- Configuration file name e.g. Dev_Dep.csv
TFTP server hosted CSV file name containing the boot grant configuration

HDD Security Configuration

HDD Password on Boot

Specifies whether a hard disk user password must be entered during every boot process.

<i>Disabled</i>	It is not necessary to enter a hard disk user password during the boot process.
<i>Enabled</i>	Entry of a hard disk user password is required during every boot process.

HDD n / HDD-ID

Opens a submenu with information on the hard disk user password.

HDD Password Description

Allows the hard disk user and master passwords to be set, changed and deleted. The hard disk user password must be set up before the Enabled Security setting can be carried out. The hard disk master password can only be changed if you have successfully unlocked it in POST with the hard disk master password.

HDD Password Configuration

Shows the current security status of the hard disk.

Security Supported

Yes is shown here if the device supports use of a hard disk user password. In this case it is possible to assign a password to the hard drive.

Security Enabled

Yes is shown here if either a hard disk user password or a hard disk master password has been assigned to the hard disk.

Security Locked

The hard disk is locked if it was not unlocked with the valid password.

Security Frozen

If *Yes* is displayed, then a hard disk user password cannot be set up, changed or deleted. To change the security frozen status to *No*, the system must have been shut down before the BIOS Setup is called. Only then can a hard disk user password be set up, changed or deleted.

HDD User Password Status

Shows whether a hard disk user password was allocated or not.

HDD Master Password Status

Shows whether a hard disk master password was allocated or not.

Set User Password

The hard disk user password protects the hard disk(s) from unauthorised access. Booting the operating system from the hard disk or accessing the data on the hard disk can only be carried out by those people who know the hard disk user password. The hard disk user password can be up to 32 characters long. The settings become effective immediately and also remain so, regardless of how you later end the BIOS Setup. The hard disk user password is requested during the POST.



If you press the Enter key, a window will open in which you can assign the hard disk user password. Enter a character string to define the password. If you confirm an empty password field, the password will be deleted.

Set Master Password

If a hard disk user password has been forgotten, it can be deleted using the hard disk master password. This option is only available if an incorrect hard disk user password has been entered three times when the system is booting during POST. The hard disk master password for your hard disk can be obtained from the certificated technical support service, but only if the particular HDD-ID is provided together with a valid proof of purchase.

Secure Boot Configuration

Opens the submenu for configuring Secure Boot.

An authentication process for the firmware version is defined with *Secure Boot Configuration*.

Secure Boot defines the industry standard method by which platform firmware certificates are managed, firmware is authenticated and in which the operating system is integrated in this process.

Secure Boot Configuration is based on the PKI process (Public Key Infrastructure), to authenticate modules before they are allowed to be executed.

Platform Mode

Shows whether the system is in user mode or setup mode.

User In user mode, the Platform Key (PK) is installed. Secure Boot can be enabled or disabled via the *Secure Boot Control* menu option.

Setup In setup mode, the Platform Key (PK) is not installed. Secure Boot is disabled and cannot be enabled via the *Secure Boot Control* menu option.

Secure Boot

Indicates whether the Secure Boot function is active.

<i>Not active</i>	Secure Boot is not active.
<i>Active</i>	Secure Boot is active.

Secure Boot Control

Specifies whether booting of unsigned boot loaders/UEFI OpROMs is permitted.



The associated signatures are saved in the BIOS or can be reloaded in the *Key Management* submenu.

<i>Disabled</i>	All boot loaders / OpROMs (Legacy / UEFI) can be executed.
<i>Enabled</i>	Only booting of signed boot loaders/UEFI OpROMs is permitted.

Secure Boot Mode

Specifies whether the Key Management submenu is available.

<i>Default</i>	The <i>Key Management</i> submenu is not available.
<i>Custom</i>	The <i>Key Management</i> submenu is available.

Key Management

Submenu for deleting, changing and adding the key and signature databases required for Secure Boot.



Without the installed Platform Key (PK), the system is in setup mode (Secure Boot is disabled). As soon as the PK is installed, the system switches to user mode (Secure Boot can be enabled).

Factory Default Key Provisioning

If the system is in setup mode (no Public Key is installed), it is possible to install the default Secure Boot key and signature databases.

<i>Disabled</i>	The available Secure Boot key and signature databases remain unchanged.
<i>Enabled</i>	If the PK, KEK, DB, DBT, DBX signature databases are not available, the default Secure Boot key and signature databases will be installed after rebooting the system.

Delete All Secure Boot Variables

Puts the system in setup mode (Secure Boot is disabled). All keys and signature databases (PK, KEK, DB, DBT, DBX) in the system are deleted.



This menu item is only available if *Factory Default Key Provisioning* is set to *Disabled*.

Enrol All Factory Default Keys

All keys and signature databases (PK, KEK, DB, DBT, DBX) in the system are reset to the default values.



This menu item is only available if *Factory Default Key Provisioning* is set to *Enabled*.

Save All Secure Boot Keys

Saves all Secure Boot Keys and Key Databases to the selected drive.

Platform Key

Set new key

Sets the Platform Key (PK). After selecting the drive, the corresponding file must be selected in the browser.

Delete key

Deletes the Platform Key (PK), which puts the system in setup mode and disables Secure Boot.

Key Exchange Key

Set new key

Sets the Key Exchange Key Database (KEK). After selecting the drive, the corresponding file must be selected in the browser.

Append key

Adds an entry to the Key Exchange Key Database (KEK). After selecting the drive, the corresponding file must be selected in the browser.

Delete key

Deletes the Key Exchange Key Database (KEK)

Authorized Signatures

Set new key

Sets the Authorized Signature Database (DB). After selecting the drive, the corresponding file must be selected in the browser.

Append key

Adds an entry to the Authorized Signature Database (DB). After selecting the drive, the corresponding file must be selected in the browser.

Delete key

Deletes the Authorized Signature Database (DB).

Authorized TimeStamps

Set new key

Sets the Authorized Signature Database (DBT). After selecting the drive, the corresponding file must be selected in the browser.

Append key

Adds an entry to the Authorized Signature Database (DBT). After selecting the drive, the corresponding file must be selected in the browser.

Delete key

Deletes the Authorized Signature Database (DBT).

Forbidden Signatures

Set new key

Sets the Forbidden Signature Database (DB). After selecting the drive, the corresponding file must be selected in the browser.

Append key

Adds an entry to the Forbidden Signature Database (DBX). After selecting the drive, the corresponding file must be selected in the browser.

Delete key

Deletes the Forbidden Signature Database (DB).

Authorized TimeStamps

Set new key

Sets the Authorized Signature Database (DBT). After selecting the drive, the corresponding file must be selected in the browser.

Append key

Adds an entry to the Authorized Signature Database (DBT). After selecting the drive, the corresponding file must be selected in the browser.

Power Menu – Energy saving functions

Main	Advanced	Security	Power	Event Logs	Boot	Save & Exit
Power Settings						After recovery from power failure: [Disabled] Remain Off. [Always Off] Switch Off. [Always On] Switch On. [Previous State] Switch to the state the system was in before power failure.
Power Failure Recovery				[Always On]		
USB Power				[Always Off]		
Power-On Source				[BIOS Controlled]		
Hibernate like Soft Off				[Enabled]		
Low Power Soft Off				[Enabled]		
Wake-Up Ressources						
LAN				[Enabled]		
Wake on LAN boot				[Boot Sequence]		
USB Keyboard				[Disabled]		
▶ Wake Up Timer						→←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Example showing the *Power* menu.

Power Settings

Power Failure Recovery – System status after a power failure

Specifies how the system behaves during a reboot following a power failure.

<i>Always Off</i>	The system switches on briefly, performs a status check (initialisation), and then switches off.
<i>Always On</i>	The system switches on.
<i>Previous State</i>	The system switches on briefly, performs a status check, and then returns the mode it was in before the power failure occurred (ON or OFF).
<i>Disabled</i>	The system does not switch on.

USB Power

Enables and disables the power supply to the USB ports when the system is switched off.

Always off The USB ports are no longer supplied with power after the system is shut down.

Always on The USB ports continue to be supplied with power after the system is shut down.

Power On Source

Specifies whether the switch-on sources for the system are managed via BIOS or via an ACPI operating system.

BIOS Controlled The switch-on sources are managed via BIOS.

ACPI Controlled The switch-on sources are managed via the ACPI operating system.

Hibernate like Soft Off

In order to also reduce the energy consumption in hibernate mode (S4), the system will instead be brought into Low Power Soft Off or Zero Watt mode (S5) when it is switched off. However, the energy consumption will only reduce if Low Power Soft Off or Zero Watt mode is enabled.

Disabled The system will be brought into hibernate mode (S4).

Enabled Instead of going into hibernate mode (S4), the system will be brought into Low Power Soft Off or Zero Watt mode (S5).

Low Power Soft Off

Reduces the energy consumption of a system which is switched off.



When Low Power Soft Off is enabled, the system can only be switched on with the power button on the casing. The device cannot be switched on using the power button of a USB keyboard or a Wake-on-LAN signal.

Disabled Low Power Soft Off is disabled.

Enabled Low Power Soft Off is enabled.

Wake-Up Resources



This submenu is only available if neither *Zero-Watt mode* nor *Low Power Soft Off* is enabled.

LAN

Determines whether the system can be switched on via a LAN controller (on the system board or expansion card).

Enabled The system can be switched on via a LAN controller.

Disabled The system cannot be switched on via a LAN controller.

Wake On LAN Boot

Specifies the system behaviour when switched on by means of network signals.

Boot Sequence After being switched on via the LAN, the system boots up according to the device sequence specified in the boot menu.

Force LAN Boot After being switched on via the LAN, the system is booted remotely via the LAN.

USB Keyboard

Specifies whether the system can be switched on via a USB keyboard (power button or any desired button).



It is only possible to switch the system on via a USB keyboard if *USB At Power-Off* is set to *Always On* and the keyboard is directly connected to the system.

From BIOS version 1.11.0, the system can be switched on via any key on a USB keyboard.

Disabled The network key of the USB keyboard is disabled.

Enabled The network key of the USB keyboard is enabled.

Wake Up Timer

The time at which the system should be switched on can be specified here.

Disabled Wake Up Timer is not enabled.

Enabled Wake Up Timer is enabled. The system is switched on at the time specified.

Hour

Specifies the hour of the switch-on time.

Minute

Specifies the minute of the switch-on time.

Second

Specifies the second of the switch-on time.

Wake Up Mode

Specifies whether the system should be switched on daily, on selected week days or only once a month at the specified time.

- Daily* The system will be switched on daily at the time specified.
- Weekly* The system is switched on at the specified time on the selected week days.
- Monthly* The system will be switched on once a month at the time specified.

Wake Up Day

Specifies the day of the month on which the system is to be switched on. Permitted values are 1..31.

Event Logs – Configuration and Display of the Event Log



Example showing the *Event Logs*.

Change SMBIOS event log settings

SMBIOS Event Log

Specifies whether the SMBIOS event log is enabled.

Disabled The SMBIOS event log is disabled.

Enabled The SMBIOS event log is enabled.

Erase Event Log

Specifies whether the SMBIOS event log should be deleted.

No The SMBIOS event log will not be deleted.

Yes, next reset The SMBIOS event Log is deleted once during the next system boot up. Afterwards, this option is automatically reset to *No*.

Yes, every reset The SMBIOS event log is deleted every time the system is booted.

When Log is full

Specifies the course of action to be taken when the SMBIOS event log is full.

Do Nothing When the SMBIOS event log is full, no further entries are added. The SMBIOS event log must first be deleted before new entries can be added.

Erase Immediately When the SMBIOS event log is full, it will be erased immediately. All existing entries will be deleted!

View SMBIOS Event Log

Opens the submenu to show all SMBIOS event log entries present.

Boot Menu – System boot

Main	Advanced	Security	Power	Event Logs	Boot	Save & Exit
Boot Configuration Bootup NumLok State [On] Quiet Boot [Enabled] Logo Resolution [Native Resolution] Boot error handling [Continue] Keyboard Error Reporting [Enabled] New Boot Option Policy [Place First] Power-on Beep [Disabled] Boot Menu [Enabled] Boot Removable Media [Enabled] Virus Warning [Disabled]						Select the keyboard Numlock state
Boot Option Priorities Boot Option #1 [Windows Boot Manager (P3: WDC WD5000AAKX-07U6AA0)] Boot Option #2 [P2: TSSTcorp DVD-ROM SH-116CB] Boot Option #3 [Realtek PXE B01 D00] Boot Option #4 [P3: WDC WD5000AAKX-07U6AA0] Boot Option #5 [USB DISK 3.0 PMAP]						→←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

The sequence of the drives from which booting is to occur can be specified here.

Up to eight drives (can include USB ports, for example) can be listed here.

Boot Configuration

Bootup NumLock State

The setting of the NumLock function after a system boot is provided here. NumLock controls the functionality of the numeric keypad.

On NumLock is enabled, the numeric keypad can be used.

Off NumLock is disabled, the numeric keypad keys can be used to control the cursor.



The Num indicator light on your keyboard shows the current boot up NumLock state. The **Num** key on the keyboard can be used to toggle between ON and OFF.

Quiet Boot

The boot logo is shown on the screen instead of the POST boot up information.

- Enabled* The boot logo is displayed.
- Disabled* The POST boot up information is shown on the screen.

Boot Error Handling

Specifies whether the system boot process is interrupted and the system stopped when an error is detected.

- Continue* The system boot is not aborted. The error will be ignored, as far as this is possible.
- Pause and wait for key* If an error is detected during POST, the boot process is interrupted and the system stopped.

Keyboard Error Reporting

- Disabled* No keyboard error message is displayed.
- Enabled* A keyboard error message is displayed.

New Boot Option Policy

Configures the placement rule for new boot options in the boot options priorities list.

- Default* No placement rule is applied to new boot options.
- Place First* New boot options are placed at the beginning.
- Place Last* New boot options are placed at the end.

Power-on Beep

Activates or deactivates signalling of system boot by means of a short beep.

- Disabled* No acoustic signalling.
- Enabled* A short beep is output at system boot.

Boot Removable Media

Specifies whether booting via a removable data storage device such as a USB stick is supported.

- Disabled* Booting via a removable data storage device is disabled.
- Enabled* Booting via a removable data storage device is enabled.

Virus Warning

Checks the boot sectors of the hard disks for changes since the last system boot. If the boot sectors have been changed without any apparent reason, a suitable virus detection program should be run.






Disabled The boot sectors will not be checked.

Enabled If the boot sector has been changed since the last system boot (e.g. new operating system or a virus attack), a warning notice is displayed. The warning notice remains on the screen until you confirm the changes by going into BIOS Setup and setting this item to *Confirm* or disable the function.

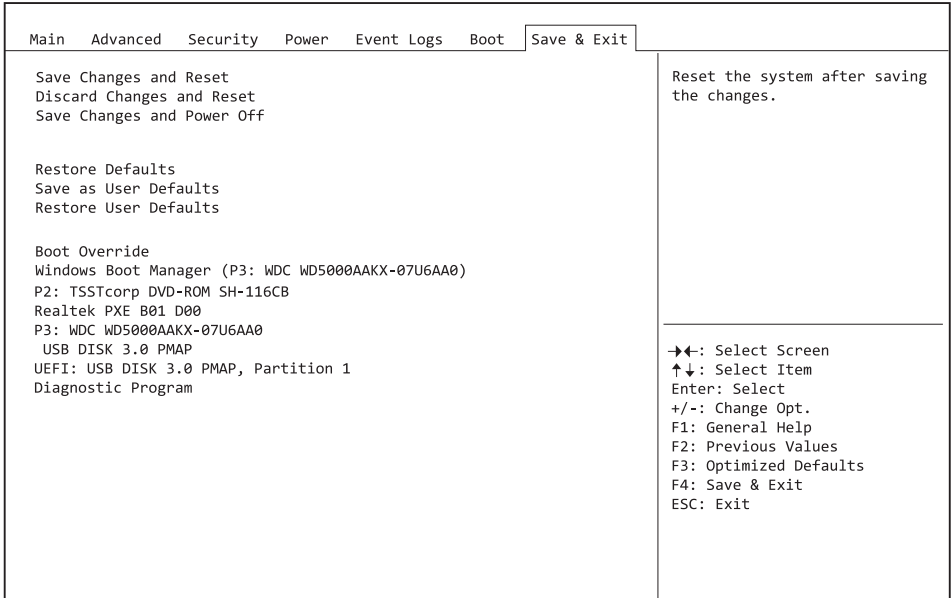
Confirm Confirm a required change to a boot sector (e.g. new operating system).

Boot option priorities

Displays the current boot sequence.

- ▶ Use the cursor keys  or  to select the device whose boot sequence you would like to change.
- ▶ To increase the priority for the selected device, press the  key. To decrease the priority, press the  key.
- ▶ To remove the selected device from the boot sequence, press the  key and select *Disabled*.

Save & Exit Menu – Finish BIOS Setup



The *Exit* menu provides options for saving settings and exiting *BIOS Setup*.

Save Changes and Reset

To save the current entries in the menus and exit BIOS Setup, select *Save Changes and Reset* and *Yes*. The system reboots and the new settings take effect.

Discard Changes and Reset

To discard the changes made since calling up the BIOS Setup or since the last time the function "Save Changes" was called, select *Discard Changes and Reset* and *Yes*. BIOS Setup is closed and the system reboots.

Save Changes and Power Off

To save the current entries in the menus and then exit the system, select *Save Changes and Power Off* and *Yes*.

Restore Defaults

To reset all the menus of the BIOS setup to the default values, select *Restore Defaults* and *Yes*. If you wish to leave the BIOS Setup with these settings, select *Save Changes and Exit* and *Yes*.



Save as User Defaults

To save the changes made so far as user default settings, select *Save as User Defaults* and *Yes*.

Restore User Defaults

To reset all the menus of the BIOS Setup to the user default settings, select *Restore User Defaults* and *Yes*. If you wish to leave the BIOS Setup with these settings, select *Save Changes and Exit* and *Yes*.


Boot Override

Use the cursor keys  and  to select the drive from which the operating system should be booted. Press the Enter key to start the boot process from the selected drive.

Diagnostic Program

- ▶ To perform a basic test of the CPU, working memory and hard disks, select *Diagnostic Program* and press the Enter key.
- ↳ If a problem occurs during the test, the relevant Error Code and a brief explanation (Diagnostic Result) will be displayed. In addition, the Error Code is entered in the Smbios Event Log.



Diagnostic Program can also be called up directly in the Boot Menu by pressing the  key in the POST.

BIOS Update

To carry out a *Flash BIOS Update*, you can use the *Auto BIOS Update* function ("[Auto BIOS Update](#)", [Page 19](#)) or must first download the necessary files from the Internet.



The BIOS is installed on a flash memory module. If an error occurs during the flash BIOS update procedure, the BIOS image may be destroyed. You can then only recover the BIOS using *BIOS Recovery Update*, see "[BIOS Recovery Update](#)", [Page 66](#). If this is not possible, the Flash memory module must be replaced. If this is the case, please contact the Service Desk of Customer Services.

- ▶ On the Internet, go to "<http://www.fujitsu.com/de/support/index.html>".
- ▶ Use *MANUAL PRODUCT SELECTION* to select your device or look for your device under *SELECT PRODUCT USING SERIAL/IDENT NO.* using the serial/ident. no. or the product name.
- ▶ Click on *Drivers & Downloads* and select your operating system.
- ▶ Select *Flash BIOS*.
- ▶ Flash BIOS Update – Desk Flash Instant: For "Flash-BIOS Update under Windows", download the file *Flash-BIOS Update – Desk Flash Instant*.
- ▶ Admin package – Compressed Flash Files: If you cannot find the operating system which you are using in the selection, select an operating system of your choice and download the file *Admin package – Compressed Flash Files* to "Flash-BIOS Update using a USB stick".
- ▶ For safety reasons, make a note of the settings in the BIOS Setup before you perform the Flash-BIOS update. Normally, a Flash-BIOS update does not damage the BIOS Setup.

Auto BIOS Update

With *Auto BIOS Update* it is possible to check a Fujitsu server automatically to see if there is a new BIOS version for the system. For the update, no operating system or external storage medium is required. For details on the *Auto BIOS Update* function, see the manual, "[Auto BIOS Update](#)", [Page 19](#).

Flash BIOS update under Windows

- ▶ Start your system and boot Windows.
- ▶ Open Windows Explorer, then under *Flash-BIOS Update – Desk Flash Instant* select the file which was downloaded and start the Flash-BIOS update with a double-click. Follow the instructions on the screen.



Administrator rights are necessary to run "Desk Flash Instant".

- ↳ After the Flash-BIOS Update has terminated successfully, the system will restart automatically and boot up with the new version of BIOS.

Flash BIOS update with a USB stick



- ▶ Have a boot-capable USB stick ready.



If your USB stick is not boot-capable, you will find the necessary files for it under *Admin package – Compressed Flash Files* under the item *Installation description* then selecting the item *Further information*. Follow the instructions.



When a boot-capable USB stick is created, all the files on the stick are irretrievably deleted. Please therefore make certain that all files from the USB stick are backed up elsewhere beforehand.

- ▶ Unzip the ZIP files which were downloaded under *Admin package – Compressed Flash Files* and copy the files and directories into the root directory of your boot-capable USB stick.
- ▶ Restart your system and wait until screen output appears. Press the function key **[F12]** and use the cursor keys  or  to select the boot-capable USB stick.
- ▶ Use *cd DOS* to change directory, launch Flash BIOS Update with the command *DosFlash* and follow the further instructions.
- ↳ After the Flash-BIOS Update has terminated successfully, the system will restart automatically and boot up with the new version of BIOS.

BIOS Recovery Update

- ▶ Prepare a boot-capable USB stick as described under "Flash BIOS update with a USB stick".
- ▶ Switch off the system and unplug it from the mains supply.
- ▶ Open the casing and enable *Recovery* using the jumper / DIP switch on the system board. You will find details on this in the technical manual for the system board.
- ▶ Connect the prepared USB stick and remove all other bootable USB devices.



If the Admin package on the prepared USB stick does not match the BIOS version of the system (e.g. Admin package for BIOS R1.2.0, but BIOS R1.3.0 is enabled on the system), no screen outputs will be possible in recovery mode. The Recovery Update will be carried out automatically in this case.

During the Recovery Update, a recurring short signal tone will sound. Recovery of the system has succeeded if you hear the repeated signal sequence "short-short-long-long" after a long signal tone. The Recovery process can take a few minutes.

- ▶ Connect the system to the mains supply again and switch it on.
- ▶ Use *cd DOS* to change directory, launch BIOS Recovery Update with the command *DosFlash* and follow the further instructions.
- ▶ After the recovery process has finished, switch off the system and disconnect it from the mains supply.
- ▶ Remove the USB stick.
- ▶ For all jumpers / DIP switches which were changed, return them to their original positions and close the casing.
- ▶ Connect the system to the mains supply again and switch it on.
- ↳ The system will now boot up with the new version of BIOS.
- ▶ Check the settings in the BIOS Setup. If necessary, configure the settings once again.

Index

A

Access 15
 Access Level 15
 Acoustic Management 26
 Acoustic Mode 27
 Active Processor Cores 22
 Advanced menu 16
 AMT Configuration 37
 Audio Configuration 19
 Authorized Signature Database (DB) 51
 Authorized Signature Database (DBT) 51–52
 Automatic BIOS Update 19–20

B

BIOS Recovery Update 66
 BIOS Setup 11
 navigating 13
 settings 9
 System configuration 14
 System settings 16
 BIOS Setup,
 security functions 42
 BIOS update
 under Windows 64
 with a USB stick 65
 BIOS Update 64
 BIOS-Setup
 opening 11
 Boot menu 12
 system boot 59
 Boot Menu
 Calling the 12
 Boot Option Filter 27

C

COM0 34
 COM1 34
 CSM 27–28

D

Date 15
 Details
 Keyboard 15
 Drive configuration
 OffBoard Controller 25
 ONBoard Controller 25
 DVMT
 Shared Memory Size 39
 Total Graphics Memory Size 39

E

Easy PC Protection 46
 EDID 40
 Enhanced SpeedStep 23
 Erase Disk 17
 Erase SATA hard disk 17
 Error Logging 24
 Event Log 57
 Exit Menu 62
 Express Slot n 21
 External SATA Port 26

F

F12, function key 12
 Finish
 BIOS Setup 62
 Forbidden Signature Database (DBX) 51

G

Graphics Configuration 38

H

Hot Plug 26
 Hyper Threading 22

I

Intel Virtualization Technology 22
 Internal Graphics 39

K

Key Exchange Key (KEK) 50
 Key Management 49–52

L

LAN 12
 LAN controller 19
 Launch CSM 27
 Launch PXE OpROM Policy 28
 Legacy USB Support 29
 Link Speed 21
 LVDS channels 41
 LVDS interface 40–41
 background lighting 41
 LVDS Interface 40
 LVDS Mode 40

M

Main Menu 14
Memory Error 24

N

Network Stack 38
Noise level 26
NumLock 59

O

Onboard Device Configuration 19
Open source software license information 14

P

Package C State limit 24
Parallel Port 33
Parallel Port Configuration 33
Password 43

- Administrator Password 43
- automatic Wakeup 44
- Hard Disk Master Password 48
- Hard Disk User Password 47–48
- Housing Monitoring 44
- Password Severity 44
- User Password 43
- User Password on Boot 44

PCI

PCI parity errors 21
PCI system errors 21

PCIe 21

Platform Key 50
Platform Key (PK) 50
Platform Mode 48

POST

Graphics Mode 41
Power failure, system reaction 53
Primary Display 39
PS/2 Emulation 30
Putty KeyPad 36

R

Recovery Update 66
Redirection After BIOS RESET 36

S

SATA

- Drive Configuration 24

SATA Port n 25
SATA ports 25
Secure Boot 48–49
Secure Boot Control 49
Secure Boot Keys 50
Secure Boot Mode 49
Security Menu 42
Serial interface 34
Server address 20
Setup,

- see BIOS Setup 11

Smartcard 45–46
Switch on system

- network 55

System Date / System Time 15
System Information 14
System Language 14
System power-on

- LAN controller 55

SystemLock 45

T

Terms of Use 20
Time 15
Trusted Computing 28
Trusted Platform Module 28

- Pending TPM operation 28
- TPM State 28
- TPM Status Information 29
- TPM Support 28

Turbo Mode 23

U

Update 20–21, 64

- System Firmware 45

USB 29–30

- USB keyboard 55
- USB ports 30

V

VT-d 23

W

Wake Up Mode 56
Wake Up Timer 55