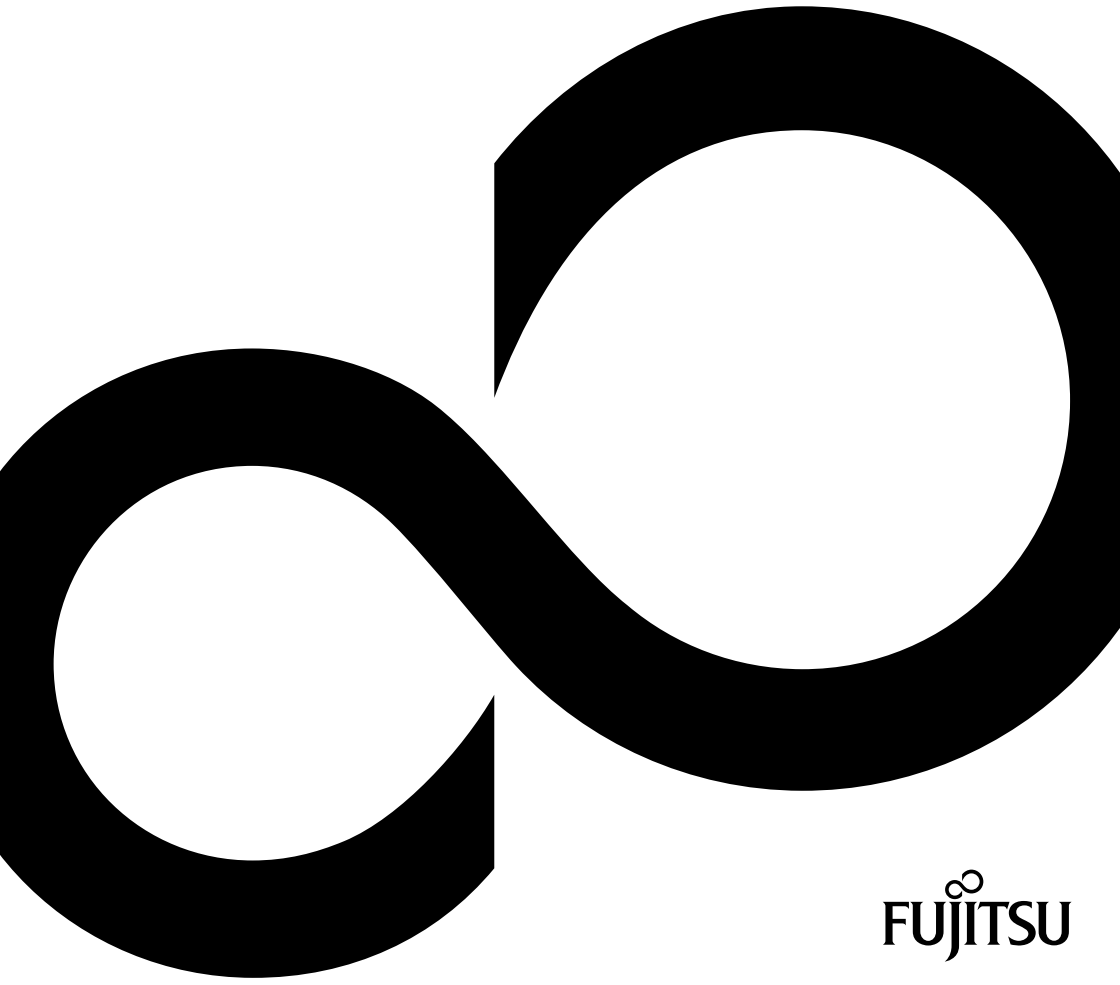


BIOS Manual for System Boards with Intel® 7 Series / C216 Chipset



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/)

For automatic driver updates, go to: ["http://support.ts.fujitsu.com/download"](http://support.ts.fujitsu.com/download)

Should you have any technical questions, please contact:

- our Hotline/Service Desk (see the Service Desk list or visit: ["http://support.ts.fujitsu.com/contact/servicedesk"](http://support.ts.fujitsu.com/contact/servicedesk))
- Your sales partner
- Your sales office

We hope you enjoy working with your new Fujitsu system!



Published by

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

Contact

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

Copyright

© Fujitsu Technology Solutions GmbH 2012. All rights reserved.

Publication Date

11/2012

Order No.: A26361-D3161-Z330-1-7619, edition 1

BIOS Manual for System Boards with Intel® 7 Series / C216 Chipset

Manual

Introduction	9
Navigating BIOS Setup	11
Main Menu – System functions	13
Advanced Menu – Advanced system configuration	15
Security Menu – Security Functions	40
Power Menu – Energy saving functions	50
Event Logs – Configuration and Display of the Event Log	54
Boot Menu – System boot	56
Save & Exit Menu – Finish BIOS Setup	61
BIOS Update	63
Index	65

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	11
If you wish to boot immediately from LAN	12
Navigating BIOS Setup	12
Exiting BIOS Setup	12
Main Menu – System functions	13
System Information	13
Board and Firmware Details	13
Network Controller Details	14
Processor Details	14
Memory Details	14
System Language	14
System Date / System Time	14
Access Level	14
Advanced Menu – Advanced system configuration	15
Erase Disk	15
PCI Subsystem Settings	17
PCI Common Settings	17
PCI Express Link Register Settings	18
TPM (Trusted Platform Module) Computing	18
TPM Support	18
TPM State	19
Pending TPM operation	19
Current TPM Status Information	19
CPU Configuration	20
Socket n CPU Information	20
Hyper-threading	20
Active Processor Cores	21
Limit CUID Maximum	21
Execute Disable Bit	21
Hardware Prefetcher	21
Adjacent Cache Line Prefetcher	22
Intel Virtualization Technology	22
VT-d	22
Enhanced SpeedStep	23
Turbo Mode	23
CPU C3 Report	23
CPU C6 Report	23
CPU C7 Report	23
Runtime Error Logging	24
ECC Memory Error Logging	24
PCI Error Logging	24
SATA Configuration	24
SATA Mode	24
Aggressive Link Power Management	24

SATA PORT n	25
Staggered Spin-up	25
External SATA Port	25
Hot Plug	25
Acoustic Management Configuration	25
Acoustic Management	25
Acoustic Mode	26
Graphics Configuration	26
Primary Display	26
Internal Graphics	26
IGD Memory	27
DVMT/Fixed Memory	27
Intel TXT Configuration	27
Intel TXT Support	27
USB Configuration	28
USB Devices	28
xHCI Mode	28
Legacy USB Support	28
USB Transfer Time-Out	29
USB_INT1 Select	29
Mass Storage Devices	29
USB Port Security	30
USB Port Control	30
USB Device Control	30
System Monitoring	31
Controller Revision	31
Firmware Version	31
Chassis Type	31
TCV Version	31
Fan Control	31
Onboard Device Configuration	32
LAN controller	32
Audio Configuration	32
High Precision Event Timer Configuration	33
Super IO Configuration	33
Super IO Chip	33
Serial Port 0 Configuration	33
Serial Port	33
Device Settings	33
Parallel Port Configuration	33
Parallel Port	33
Device Settings	34
Device Mode	34
AMT Configuration	34
ME Version	34
Unconfigure AMT/ME	34
MEBx Mode	34
IFR Support	35
Serial Port Console Redirection	35
Console Redirection Settings (for COM0 and COM1)	35
Terminal Type	35
Bits per Second	35
Data Bits	36

Parity	36
Stop Bits	36
Flow Control	36
VT-UTF8 Combo Key Support	36
Recorder Mode	36
Resolution 100x31	37
Legacy OS Redirection Resolution	37
Serial Port for Out-of-Band Management / Windows Emergency Management Services (EMS)	37
Console Redirection (for Out of Band Management / EMS)	37
Console Redirection Settings (for Out of Band Management / EMS)	37
Out-of-Band Mgmt Port	37
Terminal Type	38
Bits per Second	38
Flow Control	38
Data Bits	38
Parity	38
Stop Bits	38
Network Stack	39
Ipv4 PXE Support	39
Ipv6 PXE Support	39
Security Menu – Security Functions	40
Password Description	41
Administrator Password	41
User Password	41
User Password on Boot	42
Cabinet Monitoring	42
Skip Password on WOL	42
FLASH Write	42
Smartcard SystemLock	43
Uninstall SystemLock	43
Single Sign On	43
Smartcard & PIN	43
Unblock Smartcard	44
Secure Boot	44
Platform Mode	44
Secure Boot	44
Secure Boot Control	44
Secure Boot Mode	45
Key Management	45
HDD Security Configuration	47
HDD Password on Boot	47
HDD n / HDD-ID	47
HDD Password Description	47
HDD Password Configuration	48
Security Supported	48
Security Enabled	48
Security Locked	48
Security Frozen	48
HDD User Password Status	48
HDD Master Password Status	48
Set User Password	48

Set Master Password	49
Power Menu – Energy saving functions	50
Power Settings	50
Zero Watt Mode	50
Power On Source	51
Low Power Soft Off	51
Power Failure Recovery – System status after a power failure	51
Hibernate like Soft Off	51
USB At Power Off	52
Wake-Up Resources	52
LAN	52
Wake On LAN Boot	52
Wake Up Timer	52
Hour	52
Minute	52
Second	53
Wake Up Mode	53
Wake Up Day	53
USB Keyboard	53
Event Logs – Configuration and Display of the Event Log	54
Change SMBIOS event log settings	54
SMBIOS Event Log	54
Erase Event Log	54
When Log is full	54
Log System Boot Event	54
MECI	54
METW	55
Log OEM Codes	55
Convert OEM codes	55
View SMBIOS Event Log	55
Boot Menu – System boot	56
Boot Configuration	56
Bootup NumLock State	56
Quiet Boot	57
Fast On	57
Skip USB	57
Skip PS2	58
Option ROM Messages	58
POST Errors	58
Boot Error Handling	58
Remove Invalid Boot Options	58
Boot Removable Media	59
Virus Warning	59
Boot option priorities	59
CSM Configuration	59
Save & Exit Menu – Finish BIOS Setup	61
Save Changes and Exit	61
Discard Changes and Exit – quit without saving	61
Save Changes and Reset	61
Discard Changes and Reset	62

Save Options	62
Save Changes	62
Discard Changes	62
Restore Defaults	62
Save as User Defaults	62
Restore User Defaults	62
Boot Override	62
BIOS Update	63
Flash BIOS update under Windows	63
Flash BIOS update with a USB stick	64
Flash Memory Recovery Update	64
Index	65

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 41](#).
- ↳ 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" or "ServerStart" CD/DVD.
 - Alternatively you can also use it to download the corresponding BIOS update file from the Internet (see "[BIOS Update](#)", [Page 63](#)).

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.

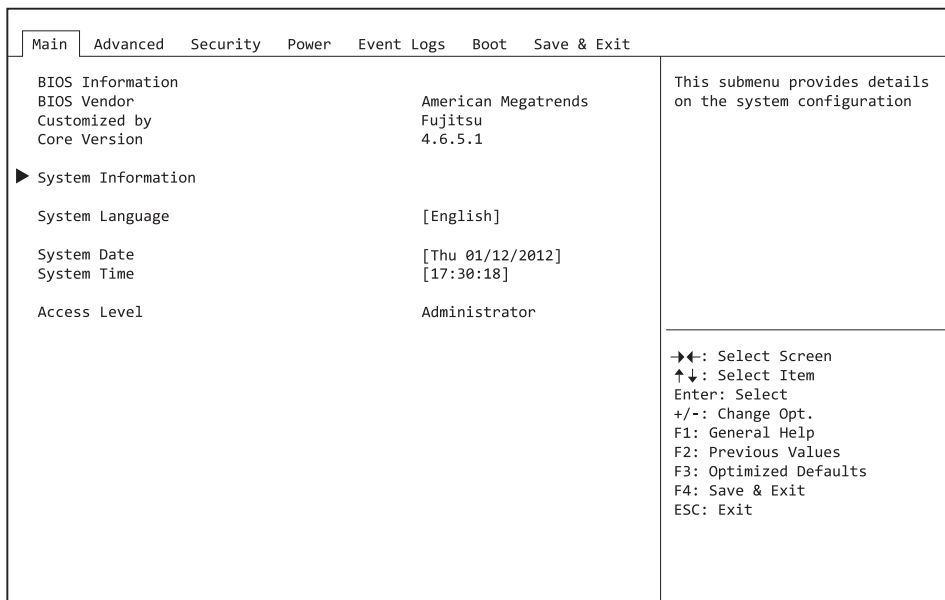
Navigating BIOS Setup

 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

This submenu contains descriptions of the system configuration. Some parameters are only available optionally.

Board and Firmware Details

Shows the current information on the installed system board and firmware.

<i>BIOS Revision</i>	Shows the current BIOS version.
<i>Build Date and Time</i>	Shows the date and time of the formation of the current BIOS.
<i>Board</i>	Shows information about the current system board.
<i>Ident Number</i>	Shows the identification number of the system.
<i>UUID</i>	Shows the 16-byte long Universal Unique ID, also known as the Globally Unique Identifier (GUID).

Network Controller Details

Shows the 6-byte long MAC address (Media Access Control) of the LAN controller.

Processor Details

<i>Processor Type</i>	Shows the CPU designation.
<i>CPU / Patch ID</i>	Shows the CPU ID and the current Patch ID.
<i>Processor Speed</i>	Shows the speed of the processor core.
<i>Cache Counts & Sizes</i>	Shows detailed information about the cache.
<i>Active Package, Core & Thread Count (maximum)</i>	Shows the number of active and maximum available CPU packages, cores and threads.

Memory Details

Shows details of the memory quantities.

<i>Memory Size / Frequency</i>	Shows the total memory in Megabytes and the memory frequency in MHz.
<i>DIMM n</i>	Shows the memory size in Megabytes for the corresponding memory slot.

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.

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.

Main	Advanced	Security	Power	Event Logs	Boot	Save & Exit
<ul style="list-style-type: none"> ▶ PCI Subsystem Settings ▶ Trusted Computing ▶ CPU Configuration ▶ Runtime Error Logging ▶ SATA Configuration ▶ Acoustic Management Configuration ▶ Graphics Configuration ▶ Intel TXT Configuration ▶ USB Configuration ▶ System Monitoring ▶ Onboard Device Configuration ▶ Super IO Configuration ▶ AMT Configuration ▶ Serial Port Console Redirection ▶ Network Stack 						PCI, PCI-X and PCI Express Settings.
						→←: 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 *Advanced* menu

Erase Disk

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

This function allows all the data on internal or external SATA hard disks connected via the eSATA connection to be irretrievably deleted, before disposal of the hard disks or the complete computer system. 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*).



Please note that data on solid state drives (SSD) cannot be deleted with total certainty.



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.

Proceed as follows to delete data from SATA hard disks:

- ▶ 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 *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 individually.



Erase Disk offers four deletion options, 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/cln_174/DE/Publikationen/publikationen_node.html"](https://www.bsi.bund.de/cln_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)

- ▶ Select the hard disk deletion algorithm which you wish to use.



The complete deletion process can be copied as an audit-compliant log onto an external USB drive, which must be formatted as FAT32. Just connect an external USB drive.

- ▶ 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.

PCI Subsystem Settings

PCI Common Settings

PERR# Generation

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

Disabled PCI parity errors will not be created.

Enabled PCI parity errors will be created.

SERR# Generation

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

Disabled PCI system errors will not be created.

Enabled PCI system errors will be created.

PCI Express Link Register Settings

ASPM Support

Configure Active State Power Management (ASPM) to gradually reduce the power consumption of the PCI Express Link and thus save energy. Even if ASPM is generally enabled by this selection, it is only then invoked for a particular connection if the corresponding PCI Express adapter card or the corresponding Onboard Controller also supports this.

<i>Disabled</i>	ASPM is disabled. The power consumption for PCI Express connections is not reduced. Best compatibility.
<i>Auto</i>	Configure maximum energy saving. Set the Low Power Mode of the PCI Express connections to L0s (uni-directional) or L1 (bi-directional).
<i>Limit to L0s</i>	Limit the Low Power Mode of the PCI Express connections to L0s (uni-directional). Compromise between compatibility and energy saving.
<i>Force L0s</i>	



The latency (delay) for PCI Express devices can increase if ASPM is not disabled. Even if ASPM is generally enabled by this selection, it is only then enabled for a particular connection if the corresponding PCI Express adapter card or the corresponding Onboard Controller also supports this. Various adapter cards do not support this function correctly, which can lead to an unpredictable system behaviour.

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).

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).

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.

<i>Disabled</i>	Trusted Platform Module is not available.
<i>Enabled</i>	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.

- 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.

- TPM SUPPORT OFF* Is displayed if the *TPM Support* is disabled.
- TPM Enabled Status* Indicates whether TPM can be used.
- TPM Active Status* Indicates whether TPM is enabled.
- TPM Owner Status* Indicates the TPM owner status.

CPU Configuration

Socket n CPU Information

The submenu opens to show information about the CPU in socket n.

<i>Processor Type</i>	Shows the CPU type.
<i>CPU Signature</i>	Shows the CPU ID.
<i>Microcode Patch</i>	Shows the CPU Micropatch ID.
<i>Max CPU Speed</i>	Shows the maximum speed of the processor core without turbo mode.
<i>Min CPU Speed</i>	Shows the minimum speed of the processor core.
<i>Processor Cores</i>	Shows the maximum number of available CPU cores.
<i>Intel HT Technology</i>	Shows whether Intel® Hyper Threading Technology is supported by the CPU.
<i>Intel VT-x Technology</i>	Shows whether Intel® VT-x (Virtualisation Technology) is supported by the CPU.
<i>Intel SMX Technology</i>	Shows whether Intel® SMX (Safer Mode Extensions) is supported by the CPU.
<i>L1 Data Cache</i>	Shows the memory size of the L1 Data Cache.
<i>L1 Code Cache</i>	Shows the memory size of the L1 instruction cache.
<i>L2 Cache</i>	Shows the memory size of the L2 cache.
<i>L3 Cache</i>	Shows the memory size of the L3 cache.

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.

<i>Disabled</i>	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.
<i>Enabled</i>	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.

<i>All</i>	All available processor cores are active and can be used.
<i>[1..n]</i>	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.

Limit CPUID Maximum

Specifies the number of CPUID functions which can be called from the processor. Some operating systems cannot process new CPUID commands which support more than three functions. This parameter should be enabled for these operating systems.

<i>Disabled</i>	All CPUID functions are supported.
<i>Enabled</i>	For reasons of compatibility with the operating system, only a reduced number of CPUID functions is supported by the processor.

Execute Disable Bit

Makes it possible to prevent the execution of programs in certain areas of memory (anti-virus protection). The function is only effective if it is also supported by the operating system. The eExecute Disable bit (XD bit) is also called the NX bit (No eExecute).

<i>Enabled</i>	Allows the operating system to switch on the Execute Disable function.
<i>Disabled</i>	Prevents the operating system from switching on the eExecute Disable function.

Hardware Prefetcher

If this function is enabled, an automatic prefetch of the memory content anticipated to be needed occurs when the memory bus is inactive. If the content is loaded from the cache and not from the memory, the latency is reduced. This particularly applies to applications with linear data access.



With this parameter you can make performance settings for non-standard applications. For standard applications, we recommend that the default settings are maintained.

<i>Disabled</i>	Deactivates the hardware prefetcher of the CPU.
<i>Enabled</i>	Activates the hardware prefetcher of the CPU.

Adjacent Cache Line Prefetcher

Available if the processor offers a mechanism by which an adjacent 64-byte cache line can also be loaded during each cache request. The number of hits in the cache increases as a result in the case of applications with high spatial locality.



With this parameter you can make performance settings for non-standard applications. For standard applications, we recommend that the default settings are maintained.

Disabled

The processor loads the requested cache line.

Enabled

The processor loads the requested cache line and the adjacent cache line.

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 by using 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.

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.

CPU C3 Report

Passes the processor C3 status as ACPI-C2/C3 status to the OSPM, if this is supported by the particular legacy operating system being used.

Disabled CPU C3 is not passed to the OSPM.

ACPI C-2 CPU C3 is passed as ACPI-C2 status to the OSPM.

ACPI C-3 CPU C3 is passed as ACPI-C3 status to the OSPM.

CPU C6 Report

Passes the processor C6 status as ACPI-C3 status to the OSPM to enable Processor Deep Power Down Technology.

Disabled CPU C6 is not passed as ACPI-C3 status to the OSPM.

Enabled CPU C6 is passed as ACPI-C3 status to the OSPM.

CPU C7 Report

Passes the processor C7 status as ACPI-C3 status to the OSPM, to enable Processor Deep Power Down Technology.

Disabled CPU C7 is not passed as ACPI-C3 status to the OSPM.

Enabled CPU C7 is passed as ACPI-C3 status to the OSPM.

Runtime Error Logging

ECC Memory Error Logging

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

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

PCI Error Logging

Specifies whether PCI errors will be entered in the SMBIOS 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 SMBIOS event log.
<i>Enabled</i>	PCI errors will be entered in the SMBIOS event log.

SATA Configuration

Opens the SATA configuration submenu.

SATA Mode

Specifies in which mode the SATA ports will be operated.

<i>IDE</i>	The SATA port is operated in IDE Mode.
<i>AHCI</i>	The SATA port is operated in AHCI Mode.
<i>RAID (if available)</i>	The SATA port is operated in RAID Mode.

Aggressive Link Power Management

In AHCI mode, makes it possible to allow Aggressive Link Power Management (ALPM) to save energy.

<i>Disabled</i>	ALPM is disabled.
<i>Enabled</i>	ALPM is enabled.

SATA PORT n

Specifies whether the SATA PORT n is available.

<i>Enabled</i>	The SATA PORT n is available.
<i>Disabled</i>	The SATA PORT n is not available.

Staggered Spin-up

Reduces the electrical load during boot up of systems with multiple SATA devices. The SATA devices run one after the other at the request of the HOST controller.

<i>Disabled</i>	Staggered Spin-up is disabled.
<i>Enabled</i>	Staggered Spin-up is enabled.

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.

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.

Graphics Configuration

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

Primary Display

Specifies the image source during the Power On Self Test (POST).

<i>Auto</i>	If the display adapter is inserted, this is used as the image source during the POST. Otherwise, the graphics device (IGD) integrated in the system board is used.
<i>IGD</i>	The Integrated Graphics Device (IGD) on the system board serves as the only image source during the POST.
<i>PEG</i>	If the PCI Express display adapter is inserted, this is used as the image source during the POST. Otherwise the IGD is used.
<i>PCI</i>	If the PCI display adapter is inserted, this is used as the image source during the POST. Otherwise the IGD is used.

Internal Graphics

Use this option if you wish to use a PCI or PEG card as the primary image source and the graphics controller on the system board (IGD - Integrated Graphics Device) as the secondary image source.

<i>Auto</i>	If a PCI or PEG card is used as the first image source, the IGD is disabled and is not available to the operating system.
<i>Disabled</i>	If it is not used as the first image source, the IGD is disabled and is not available to the operating system.
<i>Enabled</i>	If the IGD is not used as the primary image source, it can be used for operation with several monitors after the POST.

IGD Memory

Configures the size of the main memory used for the graphics controller on the system board (Integrated Graphics Drive - IGD).

32M...1024M The set value specifies the size of the shared memory available to the integrated graphics in megabytes.

DVMT/Fixed Memory

Specifies the size of the system memory reserved for the graphics.

128MB 128 MB of the system memory is reserved for the graphics.

256MB 256 MB of the system memory is reserved for the graphics.

Maximum The size of the system memory reserved for the graphics is assigned dynamically in order to achieve an optimum balance between graphics performance and system performance.

Intel TXT Configuration

Opens the submenu for configuring the Intel® Trusted Execution Technology (TXT).

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 the BIOS update of the system is started.

Disabled TXT is disabled.

Enabled TXT is enabled.

USB Configuration

USB Devices

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

xHCI Mode

Specifies the mode in which USB devices are operated at the USB 3.0 sockets marked in blue.



If using operating systems that do not support USB 3.0 (e.g. Windows XP), it is recommended that you set xHCI mode to Disabled.

Smart Auto

Depending on whether or not the operating system used supports USB 3.0 (xHCI mode) or USB 2.0 (EHCI mode), the mode preset by the operating system is automatically used for any subsequent system boots, provided the system was not disconnected from the power supply. For the *Smart Auto* setting, it is recommended that you set the *Low Power Soft Off* setup point to *Disabled*.

Auto

During the BIOS POST, USB 3.0 devices work in USB 2.0 mode. Operating systems which support USB 3.0 switch to USB 3.0 during booting of the operating system.

Enabled

During the BIOS POST, all USB 3.0 devices are operated in USB 3.0 mode. For operating systems which do not support USB 3.0, these devices are no longer available in the operating system.

Disabled

USB 3.0 devices work in USB 2.0 mode both in the BIOS POST and under the operating system.

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.

Disabled

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.

Enabled

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.

Auto

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.

USB Transfer Time-Out

If USB devices are not detected during the POST, it is possible to increase the waiting time so that slower USB devices can also be detected.

1..5..20 sec Waiting time setting for USB devices in seconds.

USB_INT1 Select

Specifies whether the USB socket (type A connector) or the USB pin connector is used on the mainboard as a USB port.

Type A Connector The USB socket (type A connector) on the mainboard is used as USB_INT1.

Pin Connector The USB pin connector is routed to the outside via a connection cable and is used as USB_INT1.

Mass Storage Devices

List of USB Mass Storage Device(s)

Allows the user to force a particular device emulation. When set to *Auto*, the devices are emulated according to their media format. Optical drives are emulated as "CD ROM" and drives without data media according to the drive type.

Auto Emulation is chosen depending on the USB device.

Floppy Force USB floppy emulation.

Hard Disk Force USB hard disk emulation.

CD-ROM Force USB CD ROM emulation.

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.

<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 Monitoring

Controller Revision

Shows the version of the system monitoring controller.

Firmware Version

Shows the firmware version of the system monitoring controller.

Chassis Type

Displays the current chassis type.

TCV Version

Shows the TCV version (Temperature Characteristics Values).

Fan Control

Specifies whether the fan speed will be adjusted automatically.

Enabled

The fan speed is adjusted automatically.

Disabled

The fan speed is not adjusted automatically. All fans are operated at maximum speed.

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.

- Disabled* The onboard audio controller is disabled.
- Enabled* The onboard audio controller is enabled.

Azalia internal HDMI codec

Specifies whether audio output via HDMI (High Definition Multimedia Interface) or Display Port Monitor is available.

- Disabled* Audio output via HDMI or Display Port Monitor is not available.
- Enabled* Audio output via HDMI or Display Port Monitor is available.

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.

High Precision Event Timer Configuration

High Precision Timer

Provided that it is enabled, the operating system is able to make use of the High Precision Event Timer, which allows it to meet the requirements of time-critical applications. The advanced timer is also known as the Multimedia Timer.

<i>Disabled</i>	The High Precision Event Timer is disabled.
<i>Enabled</i>	The High Precision Event Timer is enabled.

Super IO Configuration

Super IO Chip

Shows information about the Super IO Chip.

Serial Port 0 Configuration

Opens the submenu to configure the serial port 0 (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.

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 Mbyte/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>Standard Parallel Port Mode</i>	The standard mode will be used for the parallel port.
<i>EPP Mode</i>	Fast transfer mode (up to 2 MByte/sec), data output and data reception are possible. The mode requires a peripheral device which supports the EPP (Enhanced Parallel Port) mode.
<i>ECP Mode</i>	Fast transfer mode (up to 2.4 MByte/sec), data output and data reception are possible. The mode requires a peripheral device which supports the ECP (Extended Capability Port) mode. The necessary DMA channel is determined by the system.
<i>EPP Mode & ECP Mode</i>	Both transfer modes are available.

AMT Configuration

Opens the submenu to configure Intel® Active Management Technology.

ME Version

Shows the current AMT/ME version.

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.

<i>Normal</i>	The message <input type="text" value="Ctrl + P"/> to open the MEBx Setup will be displayed during the POST.
<i>Enter MEBx Setup</i>	The MEBx Setup will be automatically called during the next POST.

IFR Support

Specifies whether an automatic ME firmware update (Intel® Independent Firmware Recovery (IFR)) can be performed under an operating system via the ME driver.

<i>Disabled</i>	The automatic ME firmware update under the OS is not available.
<i>Enabled</i>	The automatic ME firmware update under the OS is available.

Serial Port Console Redirection

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 COM1)

Specifies the data exchange process of the host and remote system via the COM0 and COM1 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.

- Disabled* VT-UTF8 combination key support is not available.
- Enabled* VT-UTF8 combination key support is available.

Recorder Mode

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

- Disabled* Recorder mode is not available.
- Enabled* 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.

Serial Port for Out-of-Band Management / Windows Emergency Management Services (EMS)

Microsoft Windows Emergency Management Services (EMS) makes it possible to remotely manage a Windows Server operating system.

Console Redirection (for Out of Band Management / EMS)

Specifies whether a serial port for Out-of-Band Management / Windows Emergency Management Services (EMS) is available.

<i>Disabled</i>	EMS is not available.
<i>Enabled</i>	EMS is available.

Console Redirection Settings (for Out of Band Management / EMS)

Out-of-Band Mgmt Port

Assigns a serial port for Out-of-Band Management.

<i>COM0 (Disabled)</i>	Port COM0 will be used for Out-of-Band Management
<i>COM1 (Pci Dev0, Func0) (Disabled)</i>	Port COM1 will be used for Out-of-Band Management.

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.

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.

Software Xon/Xoff The interface transfer control is undertaken by the software.

Data Bits

Shows the number of data bits used to communicate with the host.

Parity

Specifies the use of parity bits for communication with the host.

Stop Bits

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

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.

<i>Disabled</i>	The UEFI Network Stack is not available.
<i>Enabled</i>	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.

<i>Disabled</i>	PXE UEFI Boot via Ipv4 is not available.
<i>Enabled</i>	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.

<i>Disabled</i>	PXE UEFI Boot via Ipv6 is not available.
<i>Enabled</i>	PXE UEFI Boot via Ipv6 is available.

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.

User Password on Boot

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

- On Every Boot* Entry of a user password is required before every boot process.
Disabled 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.

Cabinet Monitoring

Specifies whether opening of the casing should be monitored.

- Disabled* The system continues to operate normally even if the casing has been opened.
Enabled If the casing has been opened, then the boot process is suspended until the 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 WOL

Specifies whether a user password will be skipped or must be entered during a system boot via Wake on LAN.

- Disabled* The user password must be entered via using the keyboard during the system boot.
Enabled The user password is deactivated during the system boot with Wake On LAN.

FLASH Write

Supplies the system BIOS with write protection.

- Disabled* The system BIOS cannot be written. A flash BIOS update is not possible
Enabled The system BIOS can be written. A flash BIOS update is possible.

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.

No

Smartcard Security is not uninstalled.

Yes

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.

Disabled

Single Sign On is not available.

Enabled

Single Sign On is available.

Smartcard & PIN

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

Always Required

An authorised Smartcard is needed to access the system.

Ignore on WOL

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.

Secure Boot

Opens the submenu for configuring Secure Boot.

Platform Mode

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

<i>User</i>	In user mode, the Platform Key (PK) is installed. Secure Boot can be enabled or disabled via the <i>Secure Boot Control</i> menu option.
<i>Setup</i>	In setup mode, the Platform Key (PK) is not installed. Secure Boot is disabled and cannot be enabled via the <i>Secure Boot Control</i> menu option.

Secure Boot

Secure Boot indicates whether the Secure Boot function is active.

<i>Disabled</i>	Secure Boot is not active.
<i>Enabled</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, 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, DBX) in the system are deleted.

Install All Factory Default Keys

All keys and signature databases (PK, KEK, DB, DBX) in the system are reset to the default values. This menu option is only available when the PK is deleted.

Platform Key (PK)

Shows the current status of the Platform Key (PK).

<i>Installed</i>	The PK is installed. System is in user mode.
<i>Not Installed</i>	The PK is not installed. The system is in setup mode.

Set new PK

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

Delete PK

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

Key Exchange Key Database (KEK)

Shows the current status of the Key Exchange Key Database (KEK).

Installed The KEK Database is installed.

Not installed The KEK Database is not installed.

Set new KEK

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

Delete KEK

Deletes the Key Exchange Key Database (KEK)

Append Var to KEK

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

Authorized Signature Database (DB)

Shows the current status of the Authorized Signature Database (DB).

Installed The DB is installed.

Not installed The DB is not installed.

Set new DB

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

Delete DB

Deletes the Authorized Signature Database (DB).

Append Var to DB

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

Forbidden Signature Database (DBX)

Shows the current status of the Forbidden Signature Database (DBX).

<i>Installed</i>	The DBX is installed.
<i>Not installed</i>	The DBX is not installed.

Set new DBX

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

Delete DBX

Deletes the Forbidden Signature Database (DBX).

Append Var to DBX

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

Save Secure Boot Keys

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

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.

Power Menu – Energy saving functions



Example showing the *Power* menu.

Power Settings

Zero Watt Mode

Specifies whether the power consumption should be reduced to 0 Watts during system shutdown.



When Zero Watt Mode is enabled, remote management of the system is not possible and the system can only be switched on using the power button. The device cannot be switched on using the power button of a USB keyboard or a Wake-on-LAN signal.

- Enabled* The Zero Watt Mode is enabled. When the system is switched off, the power consumption reduces to 0 Watts. Remote management is not possible.
- Scheduled* The Zero Watt Mode is enabled except for a certain time period. Remote management is only possible during the specified time period.
- Disabled* The Zero Watt Mode is not enabled. Remote management is possible.

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.

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.

Power Failure Recovery – System status after a power failure

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

- Always Off* The system switches on briefly, performs a status check (initialisation), and then switches off.
- Always On* The system switches on.
- Previous State* 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).
- Disabled* The system does not switch on.

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).

USB At Power Off

Enables/disables the power supply for the USB ports. This option is only available if Low Power Soft Off and Zero Watt mode are disabled.

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.

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.

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 or only once a month at the specified time.

- Daily* The system will be switched on daily at the time specified.
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.

USB Keyboard

Specifies whether the system can be switched on via the network key of a USB keyboard, if the keyboard supports this function.



Switching on the system via a USB keyboard is only available if *USB At Power-Off* is set to *Always On*.

- Disabled* The network key of the USB keyboard is disabled.
Enabled The network key of the USB keyboard is enabled.

Event Logs – Configuration and Display of the Event Log

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!

Log System Boot Event

Specifies whether every boot of the system is logged in the SMBIOS event log.

- Disabled* System boots are not recorded in the SMBIOS event log.
- Enabled* All system boots are recorded in the SMBIOS event log.

MECI

Multiple Event Count Increment: the number of double events which must occur before the multiple event counter is updated, including the associated log entry. The value is in the range between 1 and 255.

METW

Multiple Event Time Window: the number of minutes which must elapse between double event logs which use a multiple event counter. The value is in the range between 0 to 99 minutes.

Log OEM Codes

Enables or disables the log function of EFI codes as OEM codes (if not already legacy converted).

Convert OEM codes

Enabling or disabling the conversion of EFI status codes to standard SMBIOS types (not all may be translated).

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	[Off]
Quiet Boot	[Disabled]
Fast On	[Disabled]
Option ROM Messages	[Force BIOS]
POST Errors	[Enabled]
Boot error handling	[Continue]
Remove Invalid Boot Options	[Disabled]
Boot Removable Media	[Enabled]
Virus Warning	[Disabled]
Boot Option Priorities	
Boot Option #1	[IBA GE Slot 0700 v...]
Boot Option #2	[UEFI: Built-in EFI...]
	Select the keyboard NumLock state
	→←: 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.

Fast On

Fast On is intended to reduce the boot time for systems with a fixed configuration. Once a successful boot path has been established, enabling this function allows this boot path to be used for every subsequent boot process. This reduces the boot time, because only the components needed for booting are initialised. If the system configuration is changed, open the BIOS Setup once only to confirm the new configuration.



Due to the short boot time, it is not usually possible to enter the BIOS Setup by pressing key **F2**. To enter the BIOS Setup, power up the system with the on/off switch and keep pressing the on/off switch until you hear a beep. The BIOS Setup then opens.

Note that connected devices (e.g. SSD/HDD type & firmware, etc.) can increase the boot time.

To optimise the Fast On function, if possible configure as follows:

- Under First Boot Device, enter the preferred boot medium.
- Disable TPM.
- Disable the SMBIOS Eventlog function.
- Disable parallel and serial ports.

- Disabled* When the system is switched on, a complete initialisation is performed.
- Enabled* When the system is switched on, initialisation is performed only for the components needed for booting.

Skip USB

If this function is enabled, USB devices (including USB keyboard) are only available after the operating system has been booted.



Setup and operating system boot menus may not be usable if the function is enabled. This function has no effect if the function for entering a user password is enabled on every boot process.

- Disabled* USB components are available before the operating system has been booted.
- Enabled* USB components are not available before the operating system has been booted.

Skip PS2

Setup and operating system boot menus may not be usable if the function is enabled. This function has no effect if the function for entering a user password is enabled on every boot process.

Disabled PS/2 devices are available.

Enabled PS/2 devices are not available even after booting the operating system.

Option ROM Messages

Specifies whether Option ROM messages will be displayed during POST.

Force BIOS Option ROM messages will be displayed during POST.

Keep Current Option ROM messages will NOT be displayed during POST.

POST Errors

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

Disabled The system boot is not aborted. The error will be ignored, as far as this is possible.

Enabled If an error is detected during POST, the boot process is aborted and the system stopped.

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.

Remove Invalid Boot Options

Specifies whether UEFI boot settings for devices which are no longer connected to the system should be removed from the boot options priorities list.

Disabled UEFI boot settings are not removed from the boot options priorities list.

Enabled UEFI boot settings are removed from the boot options priorities list.

Boot Removable Media

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

<i>Disabled</i>	Bootting via a removable data storage device is disabled.
<i>Enabled</i>	Bootting 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.

<i>Disabled</i>	The boot sectors will not be checked.
<i>Enabled</i>	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 <i>Confirm</i> or disable the function.
<i>Confirm</i>	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*.

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* → *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.

<i>Do not launch</i>	No option ROMs are booted.
<i>UEFI only</i>	Only UEFI option ROMs are booted.
<i>Legacy only</i>	Only Legacy option ROMs are booted.
<i>Legacy first</i>	Legacy option ROMs are booted before the UEFI option ROMs.
<i>UEFI first</i>	UEFI option ROMs are booted before the Legacy option ROMs.

Launch Storage OpROM Policy

Specifies which Storage option ROM is booted.

<i>Do not launch</i>	No Storage option ROMs are booted.
<i>UEFI only</i>	Only UEFI Storage option ROMs are booted.
<i>Legacy only</i>	Only Legacy Storage option ROMs are booted.

Launch Video OpROM Policy

Specifies which Video option ROM is booted.

<i>UEFI only</i>	Only UEFI Video option ROMs are booted.
<i>Legacy only</i>	Only Legacy Video option ROMs are booted.

Other PCI Device ROM Priority

Specifies which option ROM is booted for devices other than the network, mass memory or video.

<i>UEFI OpROM</i>	Only UEFI option ROMs are booted.
<i>Legacy OpROM</i>	Only Legacy option ROMs are booted.

Save & Exit Menu – Finish BIOS Setup

Main	Advanced	Security	Power	Boot	Save & Exit	Event Logs
Save Changes and Exit Discard Changes and Exit Save Changes and Reset Discard Changes and Reset Save Options Save Changes Discard Changes Restore Defaults Save as User Defaults Restore User Defaults Boot Override IBA GE Slot 0700 v1372 UEFI: Built-in EFI Shell						Exit system Setup after saving the changes. →←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

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

Save Changes and Exit

To save the current entries in the menus and exit the BIOS Setup, select *Save Changes and Exit* and then *Yes*. The new settings become effective and POST continues, provided a reboot is not necessary due to a changed option.

Discard Changes and Exit – quit without saving

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 & Exit* and *Yes*. BIOS Setup is terminated and POST continues.

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 Options

Save Changes

To save the changes made so far without leaving BIOS Setup, select *Save Changes* and *Yes*.

Discard Changes

To discard the changes made since calling the BIOS Setup or since the last time the function "Save Changes" was called, but without leaving the BIOS Setup, select *Save Changes* 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.

BIOS Update

Before you can perform a *flash BIOS update*, you must first download the required files from the Internet.



The BIOS is stored on a flash memory module. If an error occurs during the flash BIOS update procedure, the BIOS image may be destroyed. You can only then recreate the BIOS using *Flash Memory Recovery Update*, see "[Flash Memory Recovery Update](#)", [Page 64](#). 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
To "Flash BIOS Update under Windows", download the file *Flash BIOS Update – Desk Flash Instant*.
- ▶ Admin package – Compressed Flash Files
If you don't find in the selection the operating system which you are using, 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 settings in BIOS Setup.

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

Flash Memory 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 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 any 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.
- ▶ 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 14
 - Access Level 14
 - Acoustic Management 25
 - Acoustic Mode 26
 - Active Processor Cores 21
 - Adjacent Cache Line Prefetcher 22
 - Advanced menu 15
 - Aggressive Link Power Management 24
 - AMT Configuration 34
 - Audio Configuration 32
 - Authorized Signature Database (DB) 46
- B**
- BIOS Setup 11
 - navigating 12
 - settings 9
 - System configuration 13
 - System settings 15
 - BIOS Setup, security functions 40
 - BIOS update
 - under Windows 63
 - with a USB stick 64
 - BIOS Update 63
 - BIOS-Setup
 - opening 11
 - Boot menu 11–12
 - system boot 56
 - Boot Menu
 - Calling the 11
 - Boot Option Filter 60
- C**
- COM0 35
 - COM1 35
 - CPU C3 Report 23
 - CPU C6 Report 23
 - CPU C7 Report 23
 - CSM 59–60
- D**
- Date 14
 - Details
 - Firmware 13
 - Memory 14
 - Network Controller 14
 - Processor 14
 - Discard Changes and Exit 61
- DVMT Memory 27
- E**
- EMS 37
 - Enhanced SpeedStep 23
 - Erase Disk 15
 - Erase SATA hard disk 15
 - Error Logging 24
 - Event Log 54
 - Execute Disable Bit 21
 - Exit Menu 61
 - External SATA Port 25
- F**
- F12, function key 11
 - Fan speed 31
 - Finish
 - BIOS Setup 61
 - Fixed Memory 27
 - Flash Memory Recovery Update 64
 - Forbidden Signature Database (DBX) 47
- G**
- Graphics Configuration 26
- H**
- Hardware Prefetcher 21
 - High Precision Event Timer Configuration 33
 - Hot Plug 25
 - Hyper Threading 20
- I**
- IGD Memory 27
 - Independent Firmware Recovery 35
 - Intel Virtualization Technology 22
 - Internal Graphics 26
- K**
- Key Exchange Key (KEK) 46
 - Key Management 45–47
- L**
- LAN 12
 - LAN controller 32
 - Launch CSM 59
 - Launch PXE OpROM Policy 60
 - Launch Storage OpROM Policy 60

Launch Video OpROM Policy 60
Legacy USB Support 28
Limit CPUID Maximum 21
Link Speed 18

M

Main Menu 13
Mass Storage Devices 29
Memory Error 24

N

Network Stack 39
Noise level 25
NumLock 56

O

Onboard Device Configuration 32
Other PCI Device ROM Priority 60

P

Parallel Port 33
Parallel Port Configuration 33
Password 41
 Administrator Password 41
 Hard Disk Master Password 49
 Hard Disk User Password 47–48
 User Password 41–42
 User Password on Boot 42

PCI

 ASPM Support 18
 PCI parity errors 17
 PCI system errors 17
Platform Key 45–46
Platform Key (PK) 45
Platform Mode 44
Power consumption 50
Power failure, system reaction 51
Primary Display 26

R

Recovery Update 64

S

SATA Configuration 24
SATA PORT n 25
SATA ports 24
Save Changes and Exit 61
Secure Boot 44–45
Secure Boot Control 44

Secure Boot Keys 47
Secure Boot Mode 45
Security Menu 40
Serial interface 35
Setup,
 see BIOS Setup 11
Smartcard 43–44
Staggered Spin-up 25
Super IO Configuration 33
Switch on system
 network 52
System Date / System Time 14
System Information 13
System Language 14
System Monitoring 31
System power-on
 LAN controller 52
SystemLock 43

T

Time 14
Time-Out 29
Trusted Computing 18
Trusted Platform Module 18
 Pending TPM operation 19
 TPM State 19
 TPM Status Information 19
 TPM Support 18
Turbo Mode 23

U

USB 28–30
 USB keyboard 53
 USB ports 30
USB Transfer Time-Out 29
USB_INT1 Select 29

V

VT-d 22

W

Wake Up Mode 53
Wake Up Timer 52
Write protection 42

X

xHCI Mode 28