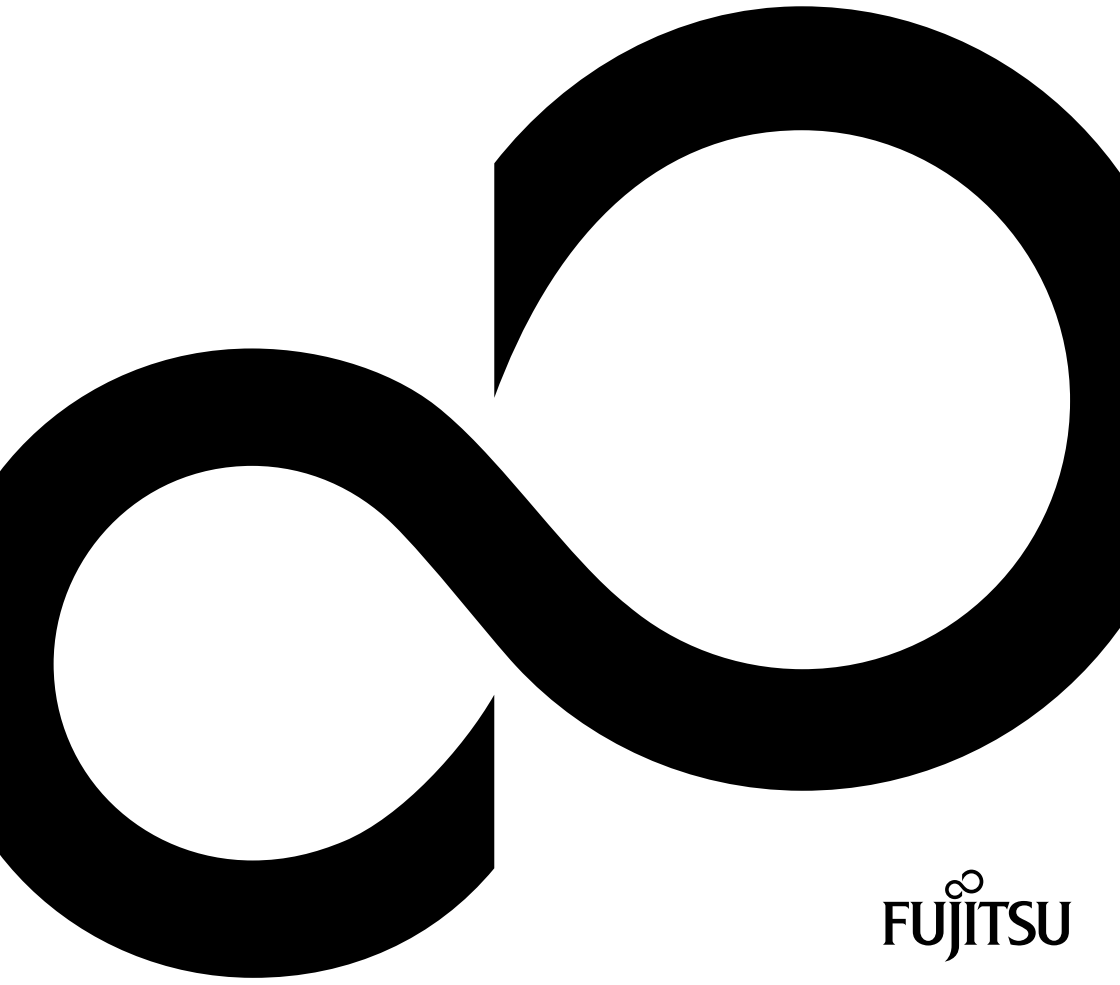# BIOS Manual for System Boards with 8th Generation Intel® 300 Series / C246 Chipset

FUJITSU

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/"

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

Should you have any technical questions, please contact:

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

We hope you enjoy working with your new Fujitsu system!

FUJITSU

BIOS Manual for System Boards with 8th Generation Intel® 300 Series / C246 Chipset

Manual

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.

Contents

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:

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

i
> 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.
i	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 (**start.exe**).
This font	Indicates information that is displayed on the screen by a program, e.g.: Installation is complete!.
This font	Indicates • terms and texts used in a software interface, e.g.: Click on *Save*. • names of programs or files, e.g. *Windows* or *setup.exe*.
"This font"	Indicates • 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.
Abc	Indicates a key on the keyboard, e.g: F10 .

Navigating BIOS Setup

Open BIOS Setup

► Switch the system on using the ON/OFF button and keep the button pressed for 2 seconds.

↳ The BIOS pauses during the POST and the message appears:

`Press <F2> to enter Setup or any other key to continue`

► 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 40.

↳ 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 61).

If you want to open the Boot Menu immediately

> **i** 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 cursor keys to select the drive from which you want to boot the operating system from now and confirm your selection with the Enter key.

> **i** 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 to select the *Enter Setup* entry and confirm your selection with the Enter key.
► If you want to perform a BIOS update, use the cursor keys to select the *FUJITSU Update Utility* entry and confirm your selection with the Enter key (see "Flash BIOS update with a USB stick ", Page 62).
► If you want to perform basic tests of the CPU, working memory and hard disks, use the cursor keys to select the *Diagnostic Program* entry and confirm your selection with the Enter key.
► If you want to start a Windows Recovery function, use the cursor keys to select the *Windows Recovery Environment* entry and confirm your selection with the Enter key (see "Windows Recovery Environment", Page 60).

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
Enter or ESC	Open submenu (marked by ►) Enter and leave ESC
+ or - keys (numeric keypad)	Change entry for field
F3 function key	Set default entries for all menus
F2 function key	Reset entries that were in use when *BIOS Setup* 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

```
┌─────────────────────────────────────────────────────────────────────────────────┐
│  Main   Advanced   Security   Power   Event Logs   Boot   Save & Exit           │
│ ┌──────┐                                                                         │
│   BIOS Information                                         This submenu provides details │
│   BIOS Vendor                    American Megatrends       on the system configuration   │
│   Customized by                  Fujitsu                                         │
│   Core Version 5.0.0.13                                                          │
│   Compliancy                     UEFI 2.6; PI 1.4                                │
│                                                                                 │
│ ▶ System Information                                                            │
│ ▶ Open Source Software License Information                                      │
│                                                                                 │
│   System Date                    [Thu 02/15/2018]                               │
│   System Time                    [10:20:13]                                     │
│   System Language                [English]                                      │
│                                                                    ──────────   │
│   Access Level                   Administrator          →←: Select Screen       │
│                                                         ↑↓: Select Item         │
│   Keyboard Layout                [English]              Enter: Select            │
│                                                         +/-: Change Opt.         │
│                                                         F1: General Help         │
│                                                         F2: Previous Values      │
│                                                         F3: Optimized Defaults    │
│                                                         F4: Save & Exit          │
│                                                         ESC: Exit                │
│                                                                                 │
└─────────────────────────────────────────────────────────────────────────────────┘
```

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 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 probably discharged and must be changed. The procedure for changing the lithium battery is described in the system board manual.

System Language

Specifies the language used in the *BIOS Setup*.

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.

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.

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      │
 │                                                                              │
 │   Advanced                                              Onboard Devices Configuration
 │                                                                              │
 │   Erase Disk                          [Disabled]                             │
 │                                                                              │
 │ ▶ Onboard Devices Configuration                                              │
 │ ▶ Auto BIOS Update                                                           │
 │ ▶ PCI Subsystem Settings                                                     │
 │ ▶ CPU Configuration                                                          │
 │ ▶ Drive Configuration                                                        │
 │ ▶ SMART Settings                                                             │
 │ ▶ Trusted Computing                                                          │
 │ ▶ USB Configuration                                                          │
 │ ▶ System Management                                                          │
 │ ▶ Super IO Configuration                            →←: Select Screen        │
 │ ▶ Serial Port Console Redirection                   ↑↓: Select Item          │
 │ ▶ AMT Configuration                                 Enter: Select            │
 │ ▶ Network Stack Configuration                       +/-: Change Opt.         │
 │ ▶ Graphics Configuration                            F1: General Help         │
 │                                                     F2: Previous Values      │
 │                                                     F3: Optimized Defaults   │
 │ ▶ Intel(R) I210 Gigabit Network Connection -        F4: Save & Exit          │
 │   90:1B:0E:FF:01:B0                                 ESC: Exit                │
 │ ▶ Realtek PCIe GBE Family Controller (MAC:90:1B:0E:F7:39:92)                 │
 │                                                                              │
 └─────────────────────────────────────────────────────────────────────────────┘
```

Example showing the *Advanced* menu

Erase Disk

Erase Disk is a solution that is integrated into the firmware of the Fujitsu Computer (*UEFI: Unified Extensible Firmware Interface*), to delete all the data from a hard disk or solid state drive (SSD).

This function can be used to 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 disposed of. The function can also be used if hard disks need to be completely deleted, for example before installing a new operating system.

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

> **i** To delete hard disks in a system, the mode of the controller must be changed, for instance to *AHCI mode* in *the SATA configuration* sub-menu of the *Advanced* menu.

To erase data from 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.

> **i** 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.

| **i** | 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)

| **i** | You can find further information on the deletion algorithms here: |

- "https://www.bsi.bund.de/cln_174/DE/Publikationen/publikationen_node.html"
- "http://www.usaid.gov/policy/ads/500/d522022m.pdf"
- "http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html"

| **i** | 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.

| **i** | 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.

| **i** | 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 Devices 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.

LAN 1 Controller

Specifies whether the LAN 1 controller is available.

Disabled   The LAN 1 controller is not available.

Enabled   The LAN 1 controller is 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.

WLAN + Bluetooth

Enables the deactivation of an M.2 WLAN + Bluetooth combi module plugged into the system.

Disabled   M.2 WLAN + Bluetooth combi module is switched off.

Enabled   M.2 WLAN + Bluetooth combi module is switched on.

Card Reader Settings

PCIe card reader

Allows enabling of a PCIe card reader.

Disabled   The PCIe card reader is disabled.

Enabled   The PCIe card reader is enabled.

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.

i	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".

Decline   The Terms of Use were not accepted. The *Auto BIOS Update* function cannot be used.

Accept   The Terms of Use were accepted. The *Auto BIOS Update* function can be used.

i	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.

Disabled   BIOS updates are not automatically searched for.

Daily   BIOS updates are searched for daily.

Weekly   BIOS updates are searched for once per week.

Monthly   BIOS updates are searched for once per month.

Quarterly   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.

> **i** 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.

Disabled	It is possible to execute the BIOS update immediately, to skip it with this system boot or to ignore the new BIOS version.
Enabled	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.

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

Disabled	No BIOS update is searched for at the next system reboot.
Enabled	A BIOS update is searched for at the next system reboot.

PCI Subsystem 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

PCI Express Slot n

Enables or disables the selected PCIe slot.

Disabled	The PCIe slot is disabled and cannot be used.
Enabled	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.

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

Slot n Non-Compliance

Improves the identification of non-compliant PCI-Express cards. If enabled, this function increases the boot time of the system.

Disable	The identification of non-compliant PCIe cards is disabled.
Enable	The identification of non-compliant PCIe cards is enabled.

Above 4G Decoding

Defines whether memory resources can be assigned to PCI devices above the 4GB address limit. The selection depends on the operating system and the adapter cards.

Disabled   Only memory resources below the 4GB address limit are assigned to the PCI devices.

This selection must be made for 32-bit operating systems, but is also supported by 64-bit operating systems.

Enabled   Memory resources above the 4GB address limit can be assigned to PCI devices if they have 64-bit address decoding.

This option is only supported by 64-bit operating systems.

This selection can be necessary if the integrated PCI Express devices (e.g. co-processor adapter cards) have a large memory requirement that cannot fit into the address space below 4 GB.

> **i** PCI address decoding is limited to the 4GB address limit for 32-bit operating systems, even if the available PCI devices support 64-bit address decoding.

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.

> **i** 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.

> **i** 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 Intel® Virtualization Technology (VT) and VT-d are enabled in the CPU submenu.

Intel® TXT is only available if TPM (Trusted Platform Module) is enabled. The TPM function is located under the *Advanced* menu in the *Trusted Computing* sub-menu.

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

Disabled   TXT is disabled.

Enabled   TXT is enabled.

Software Guard Extensions (SGX)

Intel® SGX is a CPU extension that applications can use to create and access private memory areas.

Disabled   SGX is disabled and cannot be used by applications.

Enabled   SGX is enabled and can be used by applications. The reserved size of the private memory is specified by the BIOS.

Software Controlled   SGX is enabled and can be used by applications. The reserved size of the private memory is specified by the operating system (OS).

Enhanced SpeedStep

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

i	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.

Autonomous C-state Support

Enables the autonomous C-state clock control of the processor.

Disabled	C-states are controlled by the operating system with the aid of the available ACPI objects.
Enabled	C-states are controlled by the processor hardware without the use of ACPI.
	CPU HLT instructions are handled as MWAIT instructions. Based on internal statistics, the hardware demotes the C-state requests to a C-state with lower latency.

Package C State limit

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

C0	The C state limit is C0.
C0/C1	The C state limit is C0/C1.
C2	The C state limit is C2.
C3	The C state limit is C3.
C6	The C state limit is C6.
C7	The C state limit is C7.
C7s	The C state limit is C7s.
C8	The C state limit is C8.
C9	The C state limit is C9.
C10	The C state limit is C10.
Auto	The C state limit is set to the lowest available C state.
CPU default	The default C state limit set in the CPU is set.

Runtime Error Logging

ECC Memory Error Logging

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

Enabled	Both single-bit memory errors and multi-bit memory errors are entered in the event log.
Multi-bit Errors Only	Only multi-bit memory errors are entered in the event log.
Disabled	No memory errors are entered in the event log.

PCI Error Logging

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

i	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*.

Disabled   No PCI errors will be entered in the event log.

Enabled   PCI errors will be entered in the event log.

Drive Configuration

Opens the drive configuration submenu.

SATA Mode

Specifies in which mode the SATA ports will be operated.

AHCI   The SATA port is operated in AHCI Mode.

RST (if available) The SATA port is operated in Intel® RST mode.

i	Depending on the chip set and the CPU, one of the following functions may be available: • Intel RST Premium with Intel Optane System Acceleration • Intel RST with Intel Optane System Acceleration • Intel RST Premium (no Optane) • Intel RST (no Optane) Depending on the chip set, a RAID can be established via Intel Rapid Storage Technology (RST) option ROM.

Port n

Specifies whether the SATA port is available.

Disabled   The SATA port n is not available

Enabled   The SATA port is available.

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.

Enabled	The SMART self test is enabled during the POST.
Disabled	The SMART self test is disabled during the POST.

Trusted 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 2.0. 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.

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

Pending TPM operation

Specifies a TPM operation which will be performed during the next boot process.

None	No TPM operation will be performed.
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.

USB Configuration

USB Devices

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

USB 3.1 Gen 2 speed

To enhance the compatibility of third party USB devices that might not work as expected at USB 3.1 Gen 2 ports, the speed of all USB 3.1 Gen 2 ports can be reduced to USB 3.1 Gen 1. This setting does only affect USB Ports connected to the chipset.

Enabled	USB 3.1 Gen 2 ports run with 10 GBit/s.
Disabled	USB 3.1 Gen 2 ports speed is reduced to USB 3.1 Gen 1 (5 GBit/s).

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.
Forced FDD	Force USB forced FDD 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** During POST, a USB mouse and a USB keyboard are also available if
> the corresponding USB port is disabled.

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

Enable all devices	Those settings made under *USB Port Control* will be used without any limitation.
Enable Keyboard and Mouse only	Only USB keyboards and USB mice can be operated at the USB ports enabled under *USB Port Control*. 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.
Enable all devices except mass storage devices/Hubs	USB ports on which USB storage devices or USB hubs are connected will be disabled.

System Management

Temperatures, fan speeds and electrical voltages may also be shown on this page, depending on the system board.

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.

Super IO Configuration

Serial Port Configuration

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

Device Settings

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

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

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

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

Serial Port 0 Configuration

Opens the submenu to configure the serial port 0 (COMA).

Serial Port

Specifies whether the serial port is available.

Disabled	The serial port is not available.
Enabled	The serial port is available.

Device Settings

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

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

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

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

Serial Port 1 Configuration

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

Serial Port

Specifies whether the serial port is available.

Disabled	The serial port is not available.
Enabled	The serial port is available.

Device Settings

Shows the base I/O address and the interrupt used for access to the particular serial 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.

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

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

> **i** 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.

Disabled	The parallel port is not available.
Enabled	The parallel port is available.

Device Settings

Shows the base I/O address and the interrupt which is used to access 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.

Standard Parallel Port Mode	The standard mode will be used for the parallel port.
EPP Mode	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.
ECP Mode	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.
EPP Mode & ECP Mode	Both transfer modes are 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

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

> **i** Both systems require identical or compatible settings.

Terminal Type

Specifies the type of terminal.

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

> **i** 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

> **i** 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	The 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.

Disabled	Enhanced terminal resolution is not available.
Enabled	Enhanced terminal resolution is available.

Legacy OS Redirection Resolution

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

80x24	Resolution 80x24 is used.
80x25	Resolution 80x25 is used.

Putty KeyPad

Sets FunctionKey and KeyPad to Putty.

VT100	Selects VT100.
LINUX	Selects LINUX.
XTERMR6	Selects XTERMR6.
SCO	Selects SCO.
ESN	Selects ESN.
VT400	Selects VT400.

Redirection After BIOS RESET

BootLoader	Legacy Console Redirection is disabled before Legacy OS is started.
Always Enable	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® Active Management Technology BIOS Extension (MEBx).

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

Disabled   Intel® AMT BIOS Extension (MEBx) is disabled.

Enabled   Intel® AMT BIOS Extension (MEBx) is enabled.

USB Provisioning

If this option is enabled, the settings of the AMT/ME configuration can be changed using a USB stick without starting the Intel® Active Management Technology BIOS Extension (MEBx).

Disabled   USB Provisioning from USB stick is disabled.

Enabled   USB Provisioning from USB stick is enabled.

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.

Disabled   Do not change the AMT/ME configuration.

Enabled   Start the reset of the AMT/ME configuration. The option is then automatically reset to *Disabled*.

MEBx Mode

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

Normal   MEBx Setup can be called by pressing the Ctrl + P key combination during POST.

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

Network Stack Configuration

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).

Auto   External display adapters are preferred. If there is no external display adapter, the internal display adapter is used.

Internal Graphics (if available)   The internal display adapter is used.

PCI Express for Graphics (PEG)   The display adapter in the PCI-Express slot for graphics is used.

PCI Express (PCIE)   The display adapter in a PCE Express slot is used.

Internal Graphics

Allows the internal graphics card to be switched on or off. With the *Auto* setting, the BIOS automatically determines the configuration.

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

DVMT Shared Memory Size

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

32 MB... *1024 MB*	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.

128 MB	128 MB of the main memory can be used by the internal display adapter.
256 MB	256 MB of the main memory can be used by the internal display adapter.
MAX	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.

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

   Password Description                              Set Administrator Password

   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.
   The password length must be
   in the following range:
   Minimum length              3
   Maximum length              32
   Minimum User Password length    3
                                                    →←: Select Screen
   Supervisor Password                              ↑↓: Select Item
   User Password                                    Enter: Select
   Password Severity          [Standard]            +/-: Change Opt.
   Password on Boot           [Disabled]            F1: General Help
   Skip Password on automatic Wakeup  [Disabled]    F2: Previous Values
                                                    F3: Optimized Defaults
   System Firmware Update     [Enabled]             F4: Save & Exit
   System Firmware Rollback   [Disabled]            ESC: Exit

   HDD Security Configuration:
```

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 has been 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, 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 since 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.

> **i**
> 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.

> **i**
> 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.

Password Severity

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

Standard   A forgotten password can be deleted using the Password skip jumper.

Strong   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.

Stringent   It is not possible to use the Password skip jumper. If a password has been forgotten, the system remains permanently unusable.

Password on Boot

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

On Every Boot   Entry of a password is required before every boot process.

On First Boot   Entry of a password is required during every cold start boot process.

Disabled   The system boots, without requiring a password to be entered.

Housing Monitoring

Specifies whether opening of the casing should be monitored.

> **i**
>
> This menu item is only visible if a switch for cover monitoring is present.
>
> This menu item is greyed out if no administrator password has been assigned.

Disabled   The system continues to operate normally, even if the casing was opened.

Enabled   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.

Disabled   The user password is not requested during automatic start processes.

Enabled   The user password is requested.

System Firmware Update

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

Disabled　　　　　　The system firmware (BIOS) cannot be written. A flash BIOS update is not possible.

Restricted　　　　　The system firmware (BIOS) can only be updated via FUJITSU Tools, automatic update via Windows Update (WU) is prevented.

Enabled　　　　　　The system firmware (BIOS) can be updated both via FUJITSU Tools and automatically via Windows Update (WU).

System Firmware Rollback

Specifies whether a Flash BIOS update to an older version of the system firmware (BIOS) is possible.

Disabled　　　　　　The system firmware (BIOS) cannot be flashed back to an older version.

Enabled　　　　　　The system firmware (BIOS) can be flashed back to an older version.

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.

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

Disabled　　　　　　Easy PC Protection is not available.

Enabled　　　　　　Easy PC Protection is available.

Effective configuration settings:

- Server IP address, e.g. 192.168.1.1
  The TFTP server IP address provides the boot grant configuration data
- Schedule, e.g. Development_Department
  System identification name
- Configuration file name, e.g. Dev_Dep.csv
  CSV file name with the boot grant configuration, provided by the TFTP server

HDD Security Configuration

HDD Password on Boot

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

Disabled   It is not necessary to enter a hard disk user password during the boot process.
Enabled   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.

HDD 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.

i	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.

HDD 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.

Not active	Secure Boot is not active.
Active	Secure Boot is active.

Vendor Keys

Shows whether the Vendor Keys have been modified.

Modified	The Vendor Keys were modified.
Not Modified	The Vendor Keys were not modified.

Secure Boot Control

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

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

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

Secure Boot Mode

Specifies whether the Key Management submenu is available.

Default	The *Key Management* submenu is not available.
Custom	The *Key Management* submenu is available.

Key Management

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

> **i** 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.

Disabled   The available Secure Boot key and signature databases remain unchanged.

Enabled   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.

Enrol All Factory Default Keys

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

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

Save All Secure Boot Keys

Backs up all key and signature databases on the selected drive.

Device Guard Ready

Remove 'UEFI CA' from DB

Removes the "UEFI CA 2011" certificate from the Authorized Signature database (DB).

Restore DB Defaults

The Authorized Signature database (DB) is reset to its default values.

Platform Key

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

Details   Shows details of the Platform Key (PK).

Save To File   Backs up the Platform Key (PK) in a file on the selected drive.

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 Keys

Shows the current status of the Key Exchange Keys database (KEK).

Details   Shows the details of the Key Exchange Keys Database (KEK).

Save To File   Backs up the Key Exchange Keys Database (KEK) in a file on the selected drive.

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

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

Delete Key   Deletes the Key Exchange Keys database (KEK)

> **i** The system has high security standards. Various keys and signatures are present in the system to ensure maximum security. These functions are reserved for experts and administrators.
>
> Detailed descriptions of the security standards can be found on the Internet, e.g.: UEFI Specification Version 2.6.

Authorized Signatures

Details   Shows details of the Authorized Signatures database (DB).

Save To File   Backs up the Authorized Signatures database (DB) in a file on the selected drive.

Set New Key   Sets the Authorized Signatures database (DB). After selecting the drive, the corresponding file must be selected in the browser.

Append Key   Adds an entry to the Authorized Signatures database (DB). After selecting the drive, the corresponding file must be selected in the browser.

Delete Key   Deletes the Authorized Signatures database (DB).

Forbidden Signatures

Shows the current status of the Forbidden Signatures database (DBX).

Details	Shows details of the Forbidden Signatures database (DBX).
Save To File	Backs up the Forbidden Signatures (DBX) in a file on the selected drive.
Set New Key	Sets the Forbidden Signatures database (DBX). After selecting the drive, the corresponding file must be selected in the browser.
Append Key	Adds an entry to the Forbidden Signatures database (DBX). After selecting the drive, the corresponding file must be selected in the browser.
Delete Key	Deletes the Forbidden Signatures database (DBX).

Authorized TimeStamps

Shows the current status of the Authorized TimeStamps Database (DBT).

Set New Key	Sets the Authorized TimeStamps database (DBT). After selecting the drive, the corresponding file must be selected in the browser.
Append Key	Adds an entry to the Authorized TimeStamps database (DBT). After selecting the drive, the corresponding file must be selected in the browser.

OsRecovery Signatures

Shows the current status of the OsRecovery Signatures Database.

Set New Key	Sets the OsRecovery Signatures Database. After selecting the drive, the corresponding file must be selected in the browser.
Append Key	Adds an entry to the OsRecovery Signatures Database. 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:
   Power Failure Recovery              [Always On]            [Disabled]
   System Power Limitation             [Disabled]             Remain Off.
   USB/PS2 Power                       [Always Off]           [Always Off]
   USB Type-C Connector Power Limit    [Disabled]             Switch Off.
                                                              [Always On]
   Wake-Up Ressources                                         Switch On.
                                                              [Previous State]
   LAN                                 [Enabled]              Switch to the state the system
   Wake on LAN boot                    [Boot Sequence]        was in before power failure.
   External Power Button Control       [Disabled]
   Keyboard                            [Disabled]
   Wake Up Timer                       [Disabled]
                                                              →←: 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.

Always Off   The system switches itself on briefly (initialisation by the wake sources)

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.

System Power Limitation

The system maximum power is limited so that the requirements according to JIS-T-2014 IEC 60602-1-2:2014 4th Edition are met. If the function is enabled, an extra restart is required.

Disabled   No restart is performed.

Enabled   The system restarts as soon as the system power is above the system maximum power limit.

USB/PS2 Power

Enables and disables the power supply to the USB and PS2 ports when the system is switched off.

Always off   The USB and PS2 ports are no longer supplied with power after the system is shut down.

Always on   The USB and PS2 ports continue to be supplied with power after the system is shut down.

USB Type-C Connector Power Limit

Limits the maximum power provided via the USB type C connector. Limiting the maximum power can improve system stability when many USB devices are used.

max. 3A / 15W   Limits the output power at the USB type C connector to max. 3A

max. 1.5A / 7.5W   Limits the output power at the USB type C connector to max. 1.5A

max. 900mA / 4.5W   Limits the output power at the USB type C connector to max. 900mA

OFF (no power supply)   The power supply at the USB type C connector is switched off and the connector cannot be used.

Wake-Up Resources

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.

External Power Button Control

Determines the behaviour of an externally connected power button that is connected via the PS/2 interface.

Disabled   The system can neither be switched on nor switched off using the externally connected power button.

Power On only   The system can only be switched on using the externally connected power button.

Enabled   The system can both be switched on and switched off using the externally connected power button.

Keyboard

Determines whether the system can be switched on via a keyboard (power key, any key or left CTRL + right CTRL).

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

Disabled   Keyboard switch-on is disabled.

Enabled   Switch-on via any key on the keyboard is enabled.

Special Key Only   Switch-on via a special key or key combination is enabled.

Wake-Up Resources

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

```
   Main    Advanced    Security    Power    Event Logs    Boot    Save & Exit

▶ Change Smbios Event Log Settings                          Press <Enter> to change the
▶ View Smbios Event Log                                     Smbios Event Log configuration.




                                                            ──────────────────────

                                                            →←: 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 *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.

i   An explanation can be shown in the top right window for each log entry.
         To do this, select the entry using the cursor keys.

Boot Menu – System boot

```
  Main   Advanced   Security   Power   Event Logs   Boot   Save & Exit

  Boot Configuration                                              Select the keyboard NumLock
                                                                  state
  Bootup NumLock State              [On]
  Quiet Boot                        [Enabled]
  Logo Resolution                   [Native Resolution]
  Boot error handling               [Continue]
  Keyboard Error Reporting          [Enabled]


  New UEFI OS Boot Option Policy    [Place First]
  POST Beep                         [Disabled]
  Boot Menu                         [Enabled]
  Boot Removable Media              [Enabled]

                                                                 →←: Select Screen
  Boot Option Priorities                                         ↑↓: Select Item
  Boot Option #1                    [Windows Boot Manager        Enter: Select
                                    (P1: M.2 (S42) 3ME4)]        +/-: Change Opt.
  Boot Option #2                    [UEFI:                       F1: General Help
                                    JetFlashTranscend 16GB       F2: Previous Values
                                    1100]                        F3: Optimized Defaults
                                                                 F4: Save & Exit
                                                                 ESC: Exit
```

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

> **i** 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.

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

Logo resolution

Configures the screen resolution.

Default resolution	The default screen resolution is used.
Native resolution	The native resolution of the display is used.
Static resolution	Limit the screen resolution to 800 x 600.

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

Specifies whether a keyboard error message is displayed and entered in the event log.

Disabled	No keyboard error message is displayed nor entered in the event log.
Enabled	A keyboard error message is displayed and is entered in the event log.

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 Menu

Specifies whether the Boot menu can be called up by pressing the F12 key during the POST process.

Enabled   The *Boot* menu can be called up during the POST.
Disabled   The *Boot* menu cannot be called up during the POST.

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.

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 Enter key and select *Disabled*.

Save & Exit Menu – Finish BIOS Setup

```
 Main   Advanced   Security   Power    Event Logs  Boot   Save & Exit

   Save Changes and Reset                               Reset the system after saving
   Discard Changes and Reset                            the changes.
   Save Changes and Power Off

   Restore Defaults

   Boot Override
   Windows Boot Manager (P1: M.2 (S42) 3ME4)
   UEFI: JetFlashTranscend 16GB 1100

   Diagnostic Program

                                                        →←: 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 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

In order to discard the changes made since calling up the BIOS Setup, 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 shut down 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*.

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.

> **i** Diagnostic Program can also be called up directly in the Boot Menu by pressing the F12 key in the POST.

Windows Recovery Environment

If Windows 10 is installed on your system, you can reset your operating system at the push of a button. This *Windows Recovery Environment* function reinstalls the operating system. All user data and settings can either be deleted or retained.

If your system does not boot correctly, you can access the Windows Recovery Environment as follows:

► Start the system and wait until screen display appears.

► Press the function key ⌷F12⌷.

► Use the cursor keys to select the *Windows Recovery Environment* entry and confirm your selection with the ⌷Enter⌷ key.

↳ The system starts in the Windows Recovery Environment.

BIOS Update

To carry out a *Flash BIOS Update*, you can use the *Auto BIOS Update* function ("Auto BIOS Update", Page 18) or must first download the necessary files from the Internet.

i	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 63. 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 18.

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.

> **i** 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

► Unzip the ZIP files which were downloaded under *Admin package – Compressed Flash Files* and copy the files and directories to the root directory of your USB stick.
► Restart your system and wait until screen display appears.
► Press the function key ⌐F12 .⌐
► Using the cursor keys, select the entry *FUJITSU Update Utility*.
► Press the *Enter* button to confirm your selection.
↳ The automatic update starts.
► Using the cursor keys, select the entry ⌐y⌐.
↳ The system is restarted and the Flash BIOS update is performed.

BIOS Recovery Update

► Unzip the ZIP files which were downloaded under *Admin package – Compressed Flash Files* and copy the files and directories to the root directory of your 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.

► Insert the prepared USB stick.

> 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.

► 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