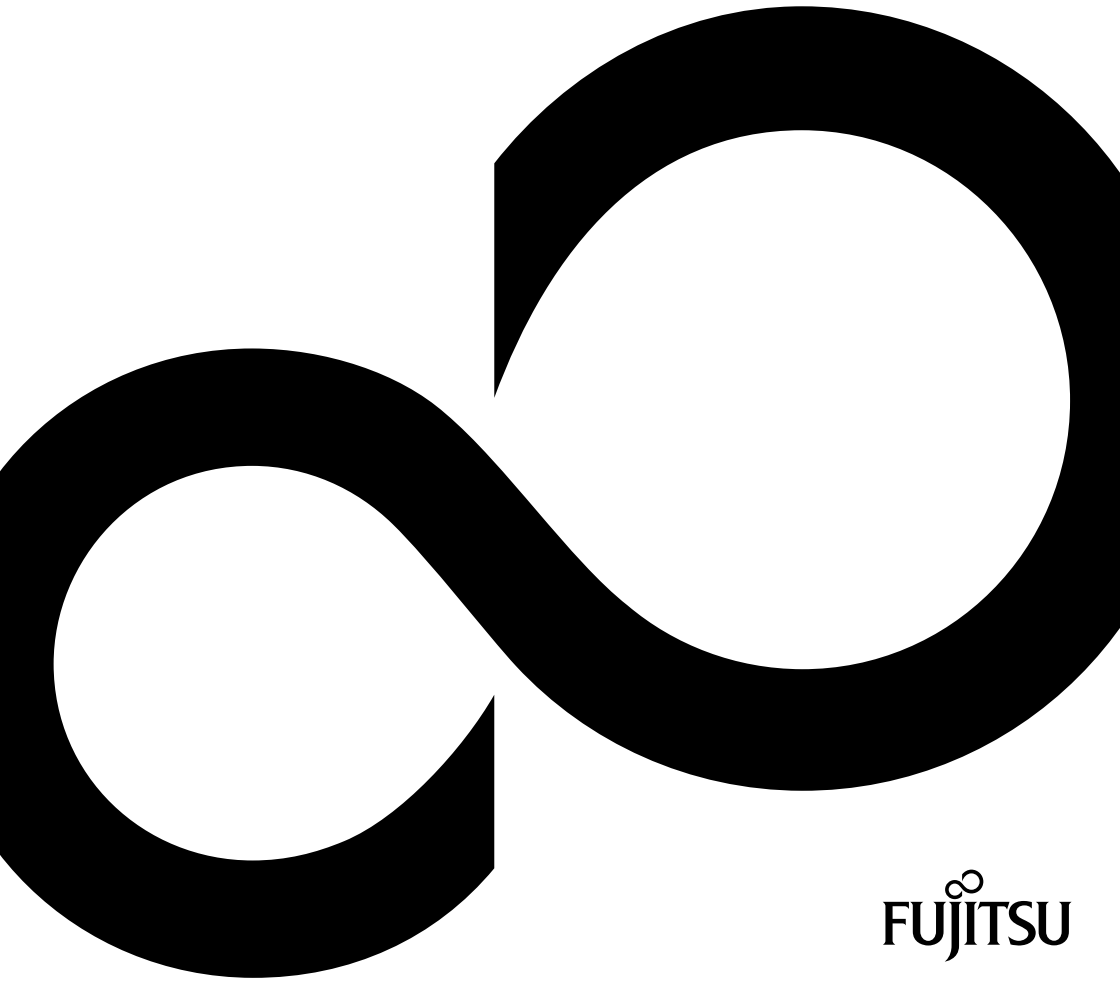


BIOS manual D3543/D3544



Congratulations on your purchase of an innovative product from Fujitsu.

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

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

Should you have any technical questions, please contact:

- our Hotline/Service Desk (["http://support.ts.fujitsu.com/contact/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 / Contact address in EU

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

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

Copyright

© Fujitsu Technology Solutions 2019. All rights reserved.

Publication Date

01/2019

Order No.: A26361-D3544-Z330-1-7619, edition 1

BIOS manual D3543/D3544

Manual

Introduction	7
Navigating BIOS Setup	9
Main Menu – System functions	12
Advanced Menu – Advanced system configuration	14
Security Menu – Security Functions	37
Power Menu – Energy saving functions	47
Event Logs – Configuration and Display of the Event Log	51
Boot Menu – System boot	53
Save & Exit Menu – Finish BIOS Setup	56
Windows Recovery Environment	58
BIOS Update	59
Index	61

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	7
Notational conventions	8
Navigating BIOS Setup	9
Open BIOS Setup	9
If you want to open the Boot Menu immediately	10
If you wish to boot immediately from LAN	10
Navigating BIOS Setup	11
Exiting BIOS Setup	11
Main Menu – System functions	12
System Information	12
Open source software license information	12
System Language	12
System Date / System Time	13
Keyboard Layout	13
Access Level	13
Advanced Menu – Advanced system configuration	14
Erase Disk	15
Onboard Devices Configuration	17
LAN Controller	17
LAN 1 Controller	17
LAN 2 Controller	17
Audio Configuration	17
Auto BIOS Update	18
Terms of Use	18
Automatic BIOS update	18
Update Server address	19
Silent update	19
Manually check for update	19
PCI Subsystem Settings	19
PERR# Generation	19
SERR# Generation	20
Above 4G Decoding	20
CPU Configuration	20
Active Processor Cores	20
Intel Virtualization Technology	21
VT-d	21
Software Guard Extensions (SGX)	21
Enhanced SpeedStep	21
Package C State limit	22
Drive Configuration	22
(m)SATA Port n	22
Port n	22
Hot Plug	22
M.2 SATA Mode	22
SMART Settings	23
SMART Self Test	23
Trusted computing	23
TPM Support	23

Pending TPM operation	23
Current TPM Status Information	23
USB Configuration	24
USB Devices	24
Mass Storage Devices	24
USB Port Security	24
USB Port Control	24
USB Device Control	25
System Management	26
Fan Startup Check	26
Fan Control	26
Watchdog Timeout	26
Super IO Configuration	27
Serial Port 1 Configuration	27
Serial Port	27
Device Settings	27
Change Settings	27
Serial Port Mode	27
Termination	28
Fast Slew Rate	28
Serial Port 2 Configuration	28
Parallel Port Configuration	28
Parallel Port	28
Device Settings	28
Device Mode	29
Serial Port Console Redirection	29
Console Redirection Settings	29
Terminal Type	29
Bits per Second	30
Data Bits	30
Parity	30
Stop Bits	30
Flow Control	30
VT-UTF8 Combo Key Support	31
Recorder Mode	31
Resolution 100x31	31
Putty KeyPad	31
Network Stack Configuration	31
Network Stack	31
Ipv4 PXE Support	32
Ipv6 PXE Support	32
Graphics Configuration	32
Primary Display	32
Internal Graphics	32
DVMT Shared Memory Size	32
DVMT Total Graphics Memory Size	33
UEFI Device Driver Setup	33
LVDS Configuration	33
LVDS Support	33
Non-EDID Support	33
LVDS Panel Config Select	34
LVDS Mode	34
LVDS Channel Swap	34

LVDS Backlight-Enable Polarity	34
LVDS Brightness Control	34
LVDS Brightness	35
POST Screen Mode	35
LVDS Dual Channel Mode	35
Embedded Display Port Configuration	35
Power over Ethernet	36
PoE Support	36
Security Menu – Security Functions	37
Password Description	38
Administrator Password	38
User Password	38
Password Severity	39
Password on Boot	39
Housing Monitoring	39
Skip Password on automatic Wakeup	39
System Firmware Update	40
System Firmware Rollback	40
Easy PC Protection	40
HDD Security Configuration	41
HDD Password on Boot	41
HDD n / HDD-ID	41
HDD Password Description	41
HDD Password Configuration	41
Security Supported	41
Security Enabled	41
Security Locked	41
Security Frozen	41
HDD User Password Status	42
HDD Master Password Status	42
HDD User Password	42
HDD Master Password	42
Secure Boot Configuration	42
Platform Mode	42
Secure Boot	43
Vendor Keys	43
Secure Boot Control	43
Secure Boot Mode	43
Key Management	44
Factory Default Key Provisioning	44
Enrol All Factory Default Keys	44
Save All Secure Boot Variables	44
Device Guard Ready	44
Platform Key (PK)	45
Key Exchange Keys	45
Authorized Signatures	45
Forbidden Signatures	46
Authorized TimeStamps	46
OsRecovery Signatures	46
Power Menu – Energy saving functions	47
Power Settings	47
Power Failure Recovery – System status after a power failure	47

- Never Off 48
- External Power Button Control 48
- USB Power 48
- USB/PS2 Power 48
- Wake-Up Resources 49
 - LAN 49
 - Wake On LAN Boot 49
 - USB Keyboard 49
 - Keyboard 49
 - Wake Up Timer 50
 - Hour 50
 - Minute 50
 - Second 50
 - Wake Up Mode 50
 - Wake Up Day 50
- Event Logs – Configuration and Display of the Event Log 51**
 - Change SMBIOS event log settings 51
 - SMBIOS Event Log 51
 - Erase Event Log 51
 - When Log is full 52
 - View SMBIOS Event Log 52
- Boot Menu – System boot 53**
 - Boot Configuration 53
 - Bootup NumLock State 53
 - Quiet Boot 54
 - Logo resolution 54
 - Boot Error Handling 54
 - Keyboard Error Reporting 54
 - Prefer USB Boot 54
 - New Boot Option Policy 55
 - POST Beep 55
 - Boot Menu 55
 - Boot Removable Media 55
 - Boot option priorities 55
- Save & Exit Menu – Finish BIOS Setup 56**
 - Save Changes and Reset 56
 - Discard Changes and Reset 56
 - Save Changes and Power Off 56
 - Restore Defaults 57
 - Boot Override 57
 - Diagnostic Program 57
- Windows Recovery Environment 58**
- BIOS Update 59**
 - Auto BIOS Update 59
 - Flash BIOS update under Windows 59
 - Flash BIOS update with a USB stick 60
 - BIOS Recovery Update 60
- Index 61**

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 ((N ame123) or a command used to start a program (s tart.exe).
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 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 38](#).
- ↳ 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 59](#)).

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 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.















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 60](#)).
- ▶ 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 58](#)).

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
 function key	Set default entries for all menus
 function key	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	Advanced	Security	Power	Event Logs	Boot	Save & Exit
<div>BIOS Information</div> <div>BIOS VendorAmerican Megatrends</div> <div>Customized byFujitsu</div> <div>Core Version5.0.0.13</div> <div>ComplianceUEFI 2.6; PI 1.4</div> <div>► System Information</div> <div>► Open Source Software License Information</div> <div>System Date[Thu 02/15/2018]</div> <div>System Time[10:20:13]</div> <div>System Language[English]</div> <div>Access LevelAdministrator</div> <div>Keyboard Layout[English]</div>						<div>This submenu provides details on the system configuration</div> <div>→←: Select Screen</div> <div>↑↓: Select Item</div> <div>Enter: Select</div> <div>+/-: Change Opt.</div> <div>F1: General Help</div> <div>F2: Previous Values</div> <div>F3: Optimized Defaults</div> <div>F4: Save & Exit</div> <div>ESC: Exit</div>

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.

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

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

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

Keyboard Layout

Specifies the keyboard layout used in the BIOS Setup.

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

Access Level

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

Advanced Menu – Advanced system configuration

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



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

MainAdvancedSecurityPowerEvent LogsBootSave & Exit

Advanced

Erase Disk [Disabled]

▶ Onboard Device Configuration

▶ Auto BIOS Update

▶ PCI Subsystem Settings

▶ CPU Configuration

▶ Drive Configuration

▶ SMART Settings

▶ Trusted Computing

▶ USB Configuration

▶ System Management

▶ LVDS Configuration

▶ Embedded Display Port Configuration

▶ Super IO Configuration

▶ Serial Port Console Redirection

▶ Network Stack Configuration

▶ Graphics Configuration

▶ Intel(R) I210 Gigabit Network Connection - 90:1B:0E:FF:01:B0

▶ Realtek PCIe GBE Family Controller (MAC:90:1B:0E:F7:39:92)

Onboard Devices 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 *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.



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



To delete hard disks in a 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*.



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

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



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

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



You can find further information on the deletion algorithms here:

- ["https://www.bsi.bund.de/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)



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

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



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

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



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

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

- Select the function which you require.

↳ The deletion process starts.

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

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

Onboard 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.

<i>Enabled</i>	The LAN controller on the system board is available.
<i>Disabled</i>	The LAN controller on the system board is not available.

LAN 1 Controller

Specifies whether the LAN 1 controller is available.

<i>Disabled</i>	The LAN 1 controller is not available.
<i>Enabled</i>	The LAN 1 controller is available.

LAN 2 Controller

Specifies whether the LAN 2 controller is available.

<i>Disabled</i>	The LAN 2 controller is not available.
<i>Enabled</i>	LAN 2 controller is available.

Audio Configuration

Azalia HD Audio

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

<i>Enabled</i>	The onboard audio controller is enabled.
<i>Disabled</i>	The onboard audio controller is disabled.

WLAN + Bluetooth

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

<i>Disabled</i>	M.2 WLAN + Bluetooth combi module is switched off.
<i>Enabled</i>	M.2 WLAN + Bluetooth combi module is switched on.

Auto BIOS Update

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

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



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

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



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

Automatic BIOS update

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

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

Update Server address

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

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



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

Silent update

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

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

Manually check for update

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



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

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

PCI Subsystem Settings

PERR# Generation

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

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

SERR# Generation

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

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

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.

<i>Disabled</i>	<p>Only memory resources below the 4GB address limit are assigned to the PCI devices.</p> <p>This selection must be made for 32-bit operating systems, but is also supported by 64-bit operating systems.</p>
<i>Enabled</i>	<p>Memory resources above the 4GB address limit can be assigned to PCI devices if they have 64-bit address decoding.</p> <p>This option is only supported by 64-bit operating systems.</p> <p>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.</p>



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.

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.

Intel Virtualization Technology

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



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

Disabled

A Virtual Machine Monitor (VMM) cannot use the additional performance features of the hardware.

Enabled

A VMM can use the additional performance features of the hardware.

VT-d

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

Disabled

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

Enabled

VT-d is available for the VMMs.

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.



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.

Package C State limit

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

<i>C0</i>	The C state limit is C0.
<i>C1</i>	The C state limit is C1.
<i>C2</i>	The C state limit is C2.

Drive Configuration

Opens the drive configuration submenu.

(m)SATA Port n

Indicates whether the (m)SATA port is available (not installed) or which drive is connected to the (m)SATA port.

Port n

Specifies whether the SATA port is available.

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

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.

M.2 SATA Mode

The M.2 interface can hold both SATA and PCIe modules. If a SATA module is plugged into the M.2 interface, you can select whether the SATA module (*Auto* option) or the SATA connector (*Disabled* option) is active.

<i>Auto</i>	If plugged in, the SATA module is active.
<i>Disabled</i>	The SATA connector is active.

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.

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.

<i>Auto</i>	Emulation is chosen depending on the USB device.
<i>Floppy</i>	Force USB floppy emulation.
<i>Forced FDD</i>	Force USB forced FDD emulation.
<i>Hard Disk</i>	Force USB hard disk emulation.
<i>CD-ROM</i>	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.



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

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

USB Device Control

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

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

System Management

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.

<i>Disabled</i>	The system does not wait for the fans to start up. A fan startup check is not executed.
<i>Enabled</i>	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.

<i>Enhanced (if available)</i>	The fan speed will be increased automatically so that the maximum CPU performance is achieved.
<i>Auto</i>	The fan speed is adjusted automatically. A compromise between system temperature and CPU performance.
<i>Full</i>	All fans are operated at maximum speed.

Watchdog Timeout

Determines the time after which a restart of the system takes place.

The permitted values are: 0 to 225

<i>0</i>	The Watchdog is deactivated. This setting is recommended to prevent an unintended restart of the system.
<i>1...255</i>	After expiry of the time set (in minutes), a restart of the system takes place if the Watchdog was not stopped in this timeframe by a tool in the OS or was continuously reset.

Super IO Configuration

Serial Port 1 Configuration

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

Serial Port

Specifies whether the serial port is available.

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

Device Settings

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

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

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



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

Serial Port Mode

Selects the protocol used for the corresponding serial port.

<i>Auto</i>	The protocol for the serial port is assigned automatically.
<i>RS-232</i>	The protocol for the serial port is RS-232.
<i>RS-485/422 Full Duplex</i>	The protocol for the serial port is RS-485/422 full duplex.
<i>RS-485 Half Duplex</i>	The protocol for the serial port is RS-485 half duplex.


Termination

Configures the line termination for RS-422 or RS-485 mode.

<i>Disabled</i>	The line termination for RS422/485 mode is disabled.
<i>Enabled</i>	The line termination for RS422/485 mode is enabled.

Fast Slew Rate

Configures the fast slew rate for RS-422 or RS-485 mode.



Enables fast slew rate for data rates above 250 kbps

<i>Disabled</i>	Slow slew rate is used for RS422/485 mode.
<i>Enabled</i>	Fast slew rate is used for RS422/485 mode.

Serial Port 2 Configuration

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

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 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)).



Both systems require identical or compatible settings.

Terminal Type

Specifies the type of terminal.

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



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

Bits per Second

Specifies the transfer rate for communication with the host.

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



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

Data Bits

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

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

Parity

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

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

Stop Bits

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

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

Flow Control

This setting determines the transfer control over the interface.

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

VT-UTF8 Combo Key Support

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

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

Recorder Mode

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

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

Resolution 100x31

Indicates whether enhanced terminal resolution is available.

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

Putty KeyPad

Sets FunctionKey and KeyPad to Putty.

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

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.

<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.

- 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).

- Internal Graphics (if available)* The internal display adapter 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...* Memory size of the preset, shared main memory.
- 1,536 MB*

DVMT Total Graphics Memory Size

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

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

UEFI Device Driver Setup

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

LVDS Configuration

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

LVDS Support

Determines whether the LVDS interface is available.

<i>Disabled</i>	The LVDS interface is not available.
<i>Enabled</i>	The LVDS interface is available.

Non-EDID Support

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



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

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

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

<i>Disabled</i>	The LCD makes EDID available.
<i>Enabled</i>	The LCD does not make EDID available.

LVDS Panel Config Select

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



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

LVDS Mode

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



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

- | | |
|-------------------|---|
| <i>FPDI 8-bit</i> | The FPDI (Flat Panel Interface) 8-bit mode will be used. |
| <i>LDI 8-bit</i> | The LDI (LVDS Display Interface) 8-bit mode will be used. |
| <i>LDI 6-bit</i> | The LDI (LVDS Display Interface) 6-bit mode will be used. |

LVDS Channel Swap

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

- | | |
|-----------------|---|
| <i>Disabled</i> | The channels of the LVDS interface will not be swapped. |
| <i>Enabled</i> | The channels of the LVDS interface will be swapped. |

LVDS Backlight-Enable Polarity

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

- | | |
|--------------------|--|
| <i>Active High</i> | The polarity for switching on the background lighting of the LCD panel is Active High. |
| <i>Active Low</i> | The polarity for switching on the background lighting of the LCD panel is Active Low. |

LVDS Brightness Control

Determines whether the brightness of the LCD panel connected to the LVDS interface is controlled by the BIOS or operating system.

- | | |
|------------------------|--|
| <i>OS Controlled</i> | The brightness of the LCD panel connected to the LVDS interface is controlled by the operating system. |
| <i>BIOS Controlled</i> | The brightness of the LCD panel connected to the LVDS interface is controlled by the BIOS. |

LVDS Brightness

Specifies the brightness of the LCD panel connected to the LVDS interface.



Permitted values are: 0..255

Where 0 stands for the minimum (0 V) and 255 for the maximum brightness (4 V) voltage level at the corresponding inverter connection.

POST Screen Mode

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



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

Graphic Mode

During POST and BIOS Setup, the system is in graphics mode.

Text Mode

During POST and BIOS Setup, the system is in text mode.

LVDS Dual Channel Mode

Makes it possible also to enable dual channel mode for LVDS devices with a horizontal resolution ≤ 1366 pixels and a vertical resolution ≤ 800 pixels. Single channel mode is necessary for most of these devices with low resolution.

Use the *Disabled* setting by default for this option. Only use the *Enabled* setting for special LVDS devices that require dual channel mode regardless of low resolutions.

Disabled

The LVDS mode is set depending on the panel resolution. If the horizontal resolution is less than 1366 pixels or the vertical resolution is less than 800 pixels, dual channel mode is set, otherwise single channel mode is set.

Enabled

LVDS is permanently set to dual channel mode.

Embedded Display Port Configuration

Opens the submenu to configure the embedded display port.

eDP Brightness

Defines the brightness of the panel connected to the embedded display port.



The permitted values are: 1...14

Where 1 stands for the minimum and 14 for the maximum brightness.

Power over Ethernet

Opens the submenu to configure the power over Ethernet (PoE) if a power over the Ethernet module is plugged in.



With the help of a power over Ethernet module, the system can be operated via the LAN without an additional power supply. This requires a corresponding network infrastructure.



During operation via the power over Ethernet module, not all hardware configuration levels may be possible due to the limited power output.

PoE Support

Determines whether the plugged power over Ethernet module is active.

<i>Disabled</i>	The plugged power over Ethernet module is not active.
<i>Enabled</i>	The plugged power over Ethernet module is active.

Security Menu – Security Functions

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

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

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

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.



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

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

Administrator Password

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



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

User Password

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



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

Password Severity

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

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

Password on Boot

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

<i>On Every Boot</i>	Entry of a password is required before every boot process.
<i>On First Boot</i>	Entry of a password is required during every cold start boot process.
<i>Disabled</i>	The system boots, without requiring a password to be entered.

Housing Monitoring

Specifies whether opening of the casing should be monitored.



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.

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

Skip Password on automatic Wakeup

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

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

System Firmware Update

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

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

System Firmware Rollback

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

<i>Disabled</i>	The system firmware (BIOS) cannot be flashed back to an older version.
<i>Enabled</i>	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.



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

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

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.

<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.

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.



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.

<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

Indicates whether the Secure Boot function is active.

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

Vendor Keys

Shows whether the Vendor Keys have been modified.

<i>Modified</i>	The Vendor Keys were modified.
<i>Not Modified</i>	The Vendor Keys were not modified.

Secure Boot Control

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



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

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

Secure Boot Mode

Specifies whether the Key Management submenu is available.

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

Key Management

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



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

Factory Default Key Provisioning

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

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

Enrol All Factory Default Keys

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



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

Save All Secure Boot Variables

Saves all Secure Boot Keys and Signature Databases to 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 the standard values.

Platform Key (PK)

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

<i>Details</i>	Displays details of the platform key (PK).
<i>Save To File</i>	Saves the Platform Key (PK) in a file on the selected drive.
<i>Set New Key</i>	Sets the Platform Key (PK). After selecting the drive, the corresponding file must be selected in the browser.
<i>Delete Key</i>	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).

<i>Details</i>	Displays the current status of the key exchange keys database (KEK).
<i>Save To File</i>	Saves the Key Exchange Keys Database (KEK) in a file on the selected drive.
<i>Set New Key</i>	Sets the Key Exchange Keys Database (KEK). After selecting the drive, the corresponding file must be selected in the browser.
<i>Append Key</i>	Adds an entry to the Key Exchange Keys Database (KEK). After selecting the drive, the corresponding file must be selected in the browser.
<i>Delete Key</i>	Deletes the Key Exchange Keys Database (KEK).



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

<i>Details</i>	Displays details of the authorized signatures database (DB).
<i>Save To File</i>	Backs up the authorized signatures database (DB) to a file on the selected drive.
<i>Set New Key</i>	Sets the authorized signatures database (DB). After selecting the drive, the corresponding file must be selected in the browser.
<i>Append Key</i>	Adds an entry to the authorized signatures database (DB). After selecting the drive, the corresponding file must be selected in the browser.
<i>Delete Key</i>	Deletes the authorized signatures database (DB).

Forbidden Signatures

Displays the current status of the forbidden signatures database (DBX).

<i>Details</i>	Displays details of the forbidden signatures database (DBX).
<i>Save To File</i>	Backs up the forbidden signatures database (DBX) to a file on the selected drive.
<i>Set New Key</i>	Sets the forbidden signatures database (DBX). After selecting the drive, the corresponding file must be selected in the browser.
<i>Append Key</i>	Adds an entry to the forbidden signatures database (DBX). After selecting the drive, the corresponding file must be selected in the browser.
<i>Delete Key</i>	Deletes the forbidden signatures database (DBX).

Authorized TimeStamps

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

<i>Set New Key</i>	Sets the authorized timestamps database (DBT). After selecting the drive, the corresponding file must be selected in the browser.
<i>Append Key</i>	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.

<i>Set New Key</i>	Sets the OsRecovery Signatures Database. After selecting the drive, the corresponding file must be selected in the browser.
<i>Append Key</i>	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: [Disabled] Remain Off. [Always Off] Switch Off. [Always On] Switch On. [Previous State] Switch to the state the system was in before power failure.
Power Failure Recovery	[Always On]	
Never Off	[Disabled]	
USB Power	[Always Off]	
External Power Button Control	[Enabled]	
Wake-Up Ressources		
LAN	[Enabled]	
Wake on LAN boot	[Boot Sequence]	
USB 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.

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

Never Off

Specifies whether the system can be switched off.



When the Never Off function is enabled, the system immediately switches on again if it is shutdown via the operating system or the network button on the casing. The system can only be shut down by disconnection from the power system.



If the Never Off function is enabled, Power Failure Recovery should be set to *Always On*.

- Disabled* The Never Off function is disabled.
- Enabled* The Never Off function is enabled.

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.

USB Power

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

- Always off* The USB ports are no longer supplied with power after the system is shut down.
- Always on* The USB ports continue to be supplied with power after the system is shut down.

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.

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.

USB Keyboard

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

With ordinary keyboards, the system can be switched on using any key. With keyboards that have a special power button, the system can only be switched on using this button.



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* A USB keyboard cannot switch the system on.
- Enabled* The system can be switched on using a USB keyboard.

Keyboard

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



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

Wake Up Day

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

Event Logs – Configuration and Display of the Event Log



Example showing the *Event Logs*.

Change SMBIOS event log settings

SMBIOS Event Log

Specifies whether the SMBIOS event log is enabled.

- Disabled* The SMBIOS event log is disabled.
- Enabled* The SMBIOS event log is enabled.

Erase Event Log

Specifies whether the SMBIOS event log should be deleted.

- No* The SMBIOS event log will not be deleted.
- Yes, next reset* The SMBIOS event Log is deleted once during the next system boot up. Afterwards, this option is automatically reset to *No*.
- Yes, every reset* The SMBIOS event log is deleted every time the system is booted.

When Log is full

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

- | | |
|--------------------------|--|
| <i>Do Nothing</i> | 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. |
| <i>Erase Immediately</i> | 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.



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]	
Prefer USB Boot	[Disabled]	
New Boot Option Policy	[Place First]	
POST Beep	[Disabled]	
Boot Menu	[Enabled]	
Boot Removable Media	[Enabled]	
Boot Option Priorities		→←: Select Screen
Boot Option #1	[Windows Boot Manager (P1: M.2 (S42) 3ME4)]	↑↓: Select Item
Boot Option #2	[UEFI: JetFlashTranscend 16GB 1100]	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.

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.

<i>Disabled</i>	The POST boot up information is shown on the screen.
<i>Enabled</i>	The boot logo is displayed.

Logo resolution

Configures the screen resolution.

<i>Default resolution</i>	The default screen resolution is used.
<i>Native resolution</i>	The native resolution of the display is used.
<i>Static resolution</i>	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.

<i>Continue</i>	The system boot is not aborted. The error will be ignored, as far as this is possible.
<i>Pause and wait for key</i>	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.

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

Prefer USB Boot

Determines whether USB devices should be preferred in the boot sequence.

<i>Enabled</i>	USB devices will be preferred to other devices in the boot sequence.
<i>Disabled</i>	USB devices will not be treated with preference in the boot sequence.

New Boot Option Policy

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

<i>Default</i>	No placement rule is applied to new boot options.
<i>Place First</i>	New boot options are placed at the beginning.
<i>Place Last</i>	New boot options are placed at the end.

POST Beep

Configures the signalling with a short beep tone during the POST.

<i>Disabled</i>	No acoustic signalling.
<i>At start of POST</i>	A short beep tone sounds at the start of the POST.
<i>At end of POST</i>	A short beep tone sounds at the end of the POST.
<i>At start and end of POST</i>	A short beep tone sounds at the start and at the end of the POST.

Boot Menu

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

<i>Enabled</i>	The <i>Boot</i> menu can be called up during the POST.
<i>Disabled</i>	The <i>Boot</i> 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.

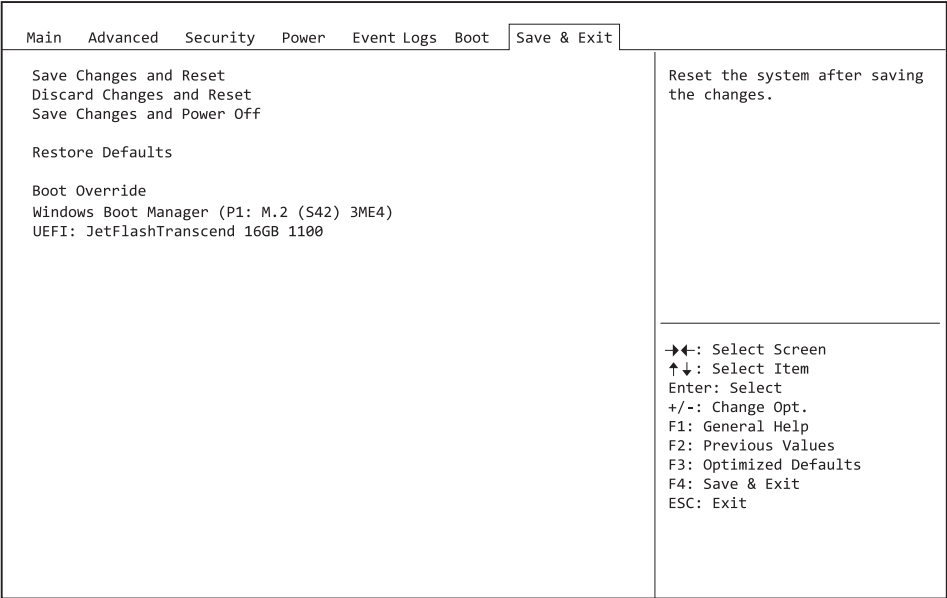
<i>Disabled</i>	Booting via a removable data storage device is disabled.
<i>Enabled</i>	Booting via a removable data storage device is enabled.

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  key and select *Disabled*.

Save & Exit Menu – Finish BIOS Setup



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

Save Changes and Reset

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

Discard Changes and Reset

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.



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



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 60](#). 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.



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

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



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

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

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

Index

A

- Access 13
- Access Level 13
- Active Processor Cores 20
- Advanced menu 14
- Audio Configuration 17
- Authorized Signatures Database (DB) 45
- Authorized TimeStamps Database (DBT) 46
- Automatic BIOS Update 18

B

- BIOS Recovery Update 60
- BIOS Setup 9
 - navigating 11
 - settings 7
 - System configuration 12
 - System settings 14
- BIOS Setup,
 - security functions 37
- BIOS update
 - under Windows 59
 - with a USB stick 60
- BIOS Update 59
- BIOS-Setup
 - opening 9
- Bluetooth 17
- Boot menu 10
 - system boot 53
- Boot Menu
 - Calling the 10

C

- COM0 29
- COM4 29

D

- Date 13
- Decoding
 - 4G 20
- Details
 - Keyboard 13
- Display Port
 - eDP Brightness 35
- DVMT
 - Shared Memory Size 32
 - Total Graphics Memory Size 33

E

- Easy PC Protection 40

EDID 33

- Enhanced SpeedStep 21
- Erase Disk 15
- Erase SATA hard disk 15
- Event Log 51
- Exit Menu 56

F

- F12, function key 10
- Finish
 - BIOS Setup 56
- Forbidden Signatures Database (DBX) 46

G

- Graphics Configuration 32

H

- Hot Plug 22

I

- Intel Virtualization Technology 21
- Internal Graphics 32

K

- Key Exchange Keys (KEK) 45
- Key Management 44–46

L

- LAN 10, 17
- LAN controller 17
- LVDS channels 34
- LVDS interface 33–34
 - background lighting 34
 - LVDS brightness 35
- LVDS Interface 33–34
 - Brightness LCD 34
 - Dual Channel Mode 35
- LVDS Mode 34
- LVDS Support 33

M

- M.2 interface 22
- Main Menu 12
- Mass Storage Devices 24

N

- Network Stack 31

NumLock 53

O

Onboard Devices Configuration 17
Open source software license information 12
OsRecovery Signatures 46

P

Package C State limit 22
Parallel Port 28
Parallel Port Configuration 28
Password 38
 Administrator Password 38
 automatic Wakeup 39
 Hard Disk Master Password 42
 Hard Disk User Password 41–42
 Housing Monitoring 39
 Password on Boot 39
 Password Severity 39
 User Password 38

PCI

 PCI parity errors 19
 PCI system errors 20

Platform Key 45

Platform Mode 42

PoE Support 36

POST 55

 Graphics Mode 35

POST Beep 55

Power

 external Power Button 48

Power failure, system reaction 47

Power over Ethernet 36

Primary Display 32

Putty KeyPad 31

R

Recovery Update 60

Rollback

 System Firmware 40

S

SATA

 Drive Configuration 22

SATA Configuration 22

SATA module 22

SATA Port n 22

Secure Boot 42–44

Secure Boot Control 43

Secure Boot Mode 43

Secure Boot Variables 44

Security Menu 37

Serial interface 29

serial port 27

Server address 19

Setup,

 see BIOS Setup 9

Software Guard Extensions (SGX) 21

Switch on system

 network 49

System boot 55

System Date / System Time 13

System Information 12

System Language 12

System power-on

 LAN controller 49

T

Tastatur 49

Terms of Use 18

Time 13

Trusted Computing 23

Trusted Platform Module 23

 Pending TPM operation 23

 TPM Status Information 23

 TPM Support 23

U

Update 18–19, 59

 System Firmware 40

USB 24–25

 USB keyboard 49

 USB ports 24

V

Vendor Keys 43

VT-d 21

W

Wake Up Mode 50

Wake Up Timer 50

WLAN 17