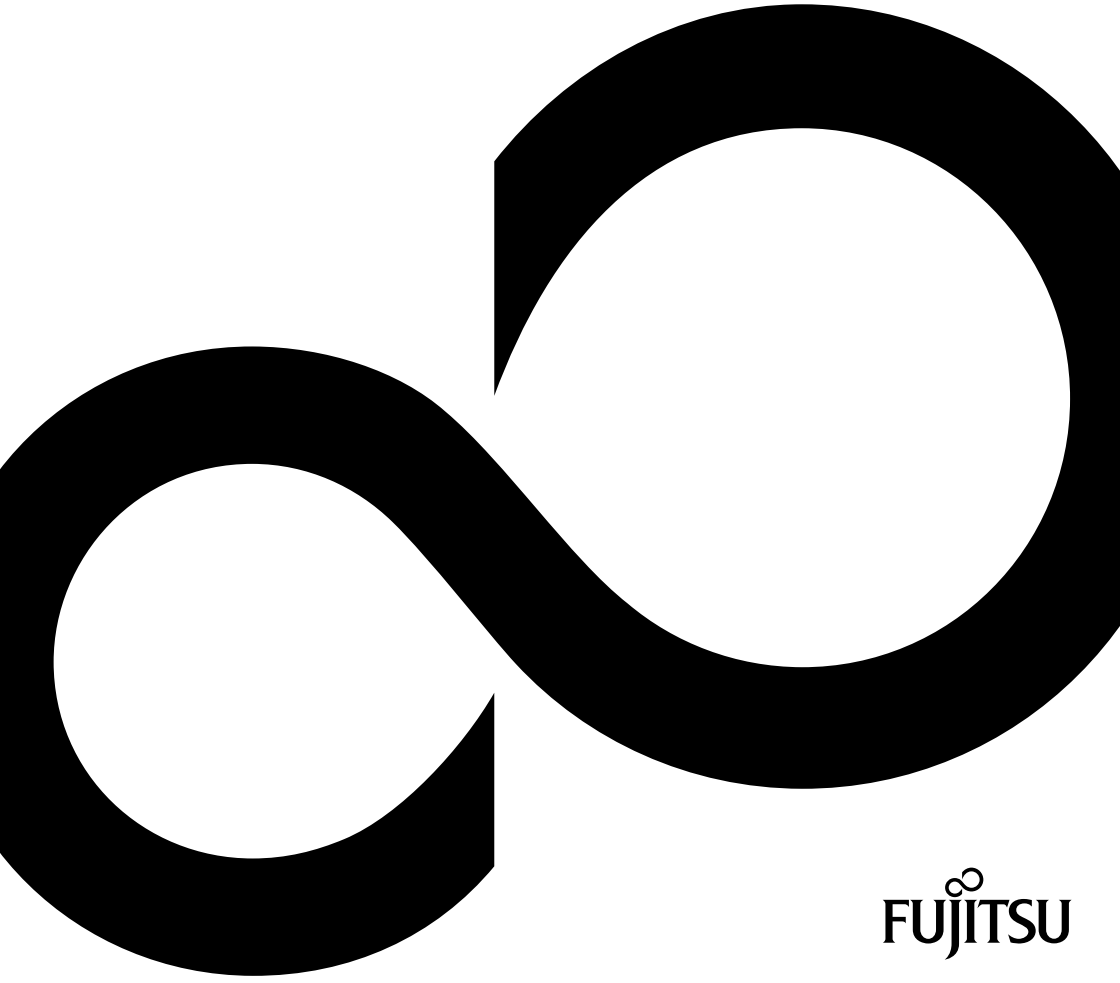
BIOS Handbuch D3118/D3128 (Ivy Bridge)



FUJITSU

Wir gratulieren Ihnen zum Kauf eines innovativen Produkts von Fujitsu.

Aktuelle Informationen zu unseren Produkten, Tipps, Updates usw. finden Sie im Internet: "http://www.fujitsu.com/fts/"

Treiber-Updates finden Sie unter: "http://support.ts.fujitsu.com/download"

Wenn Sie technische Fragen haben sollten, wenden Sie sich bitte an:

- unsere Hotline/Service Desk (siehe Service-Desk-Liste oder im Internet: "http://support.ts.fujitsu.com/contact/servicedesk")
- Ihren zuständigen Vertriebspartner
- Ihre Verkaufsstelle

Viel Freude mit Ihrem neuen Fujitsu-System!

Herausgegeben von / Kontaktadresse in der EU
Fujitsu Technology Solutions GmbH
Mies-van-der-Rohe-Straße 8
80807 München, Germany

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

Ausgabedatum
2013/11

Bestell-Nr.: A26361-D3118-Z335-1-19, Ausgabe 1

BIOS Handbuch D3118/D3128 (Ivy Bridge)

Handbuch

Einleitung	**7**
Bedienung des BIOS-Setup	**9**
Main Menu – Systemfunktionen	**12**
Advanced Menu – Erweiterte Systemkonfiguration	**15**
Security Menu - Sicherheitsfunktionen	**44**
Power Menu – Energiesparfunktionen	**52**
Event Logs – Konfiguration und Anzeige der Event Log	**56**
Boot Menu – Systemstart	**58**
Save & Exit Menu – BIOS-Setup beenden	**63**
BIOS-Update	**65**
Anlage	**68**
Stichwörter	**71**

Bemerkung

Hinweise zur Produktbeschreibung entsprechen den Designvorgaben von Fujitsu und werden zu Vergleichszwecken zur Verfügung gestellt. Die tatsächlichen Ergebnisse können aufgrund mehrerer Faktoren abweichen. Änderungen an technischen Daten ohne Ankündigung vorbehalten. Fujitsu weist jegliche Verantwortung bezüglich technischer oder redaktioneller Fehler bzw. Auslassungen von sich.

Warenzeichen

Fujitsu und das Fujitsu-Logo sind eingetragene Warenzeichen von Fujitsu Limited oder seiner Tochtergesellschaften in den Vereinigten Staaten und anderen Ländern.

Microsoft und Windows sind Warenzeichen bzw. eingetragene Warenzeichen der Microsoft Corporation in den Vereinigten Staaten und/oder anderen Ländern.

Intel und Pentium sind eingetragene Warenzeichen und MMX und OverDrive sind Warenzeichen der Intel Corporation, USA.

PS/2 und OS/2 Warp sind eingetragene Warenzeichen von International Business Machines, Inc.

Alle anderen hier genannten Warenzeichen sind Eigentum ihrer jeweiligen Besitzer.

Inhalt

Einleitung **7**
Darstellungsmittel 8

Bedienung des BIOS-Setup **9**
BIOS-Setup aufrufen 9
Wenn Sie sofort das Boot Menu aufrufen möchten 10
Wenn Sie sofort von LAN booten möchten 10
BIOS-Setup bedienen 11
BIOS-Setup beenden 11

Main Menu – Systemfunktionen **12**
System Information 12
Board und Firmware Details 12
Network Controller Details 13
Processor Details 13
Memory Details 13
System Language 13
System Date / System Time 13
Access Level 14

Advanced Menu – Erweiterte Systemkonfiguration **15**
Erase Disk 15
PCI Subsystem Settings 17
Above 4G Decoding 17
PCI Express Link Register Settings 18
TPM (Trusted Platform Module) Computing 19
TPM Support 19
TPM State 19
Pending TPM operation 19
Current TPM Status Information 20
CPU Configuration 20
Socket n CPU Information 20
Hyper Threading 21
Active Processor Cores 21
Limit CPUID Maximum 21
Execute Disable Bit 21
Hardware Prefetcher 22
Adjacent Cache Line Prefetcher 22
DCU (Data Cache Unit) Streamer Prefetcher 22
DCU Ip (Instruction pointer-based) Prefetcher 23
Intel Virtualization Technology 23
VT-d 23
Power Technology 23
Enhanced Speedstep 24
Turbo Mode 24
Energy Performance 24
P-State Coordination 25
CPU C3 Report 25
CPU C6 Report 25
CPU C7 Report 25
Package C State limit 26

QPI Link Frequency Select ... 26
Frequency floor override ... 26
Runtime Error Logging ... 26
ECC Memory Error Logging ... 26
PCI Error Logging ... 27
Memory Configuration ... 27
NUMA (nur D3118) ... 27
DDR Performance ... 27
Fast Patrol Scrub (nur D3118) ... 28
Refresh Rate Multiplier ... 28
SATA Configuration ... 28
SATA Mode ... 28
Aggressive LPM Support ... 28
Serial-ATA Controller 0 ... 29
Serial-ATA Controller 1 ... 29
Staggered Spin-up ... 29
External SATA Port ... 29
Hot Plug ... 29
Acoustic Management Configuration ... 30
Acoustic Management ... 30
Acoustic Mode ... 30
Intel TXT Configuration ... 31
Intel TXT Support ... 31
USB Configuration ... 31
USB Devices ... 31
Legacy USB Support ... 31
Mass Storage Devices ... 32
USB Port Security ... 32
USB Port Control ... 32
USB Device Control ... 32
System Monitoring ... 33
Controller Revision ... 33
Firmware Version ... 33
Chassis Type ... 33
TCV Version ... 33
Fan Control ... 33
Onboard Device Configuration ... 33
SCU Device ... 33
Audio Configuration ... 34
High Precision Event Timer Configuration ... 34
Memory Status ... 35
DIMM-xx ... 35
Auto BIOS Update ... 35
Nutzungsbedingungen ... 35
Automatic BIOS update ... 36
Server IP address ... 36
Silent update ... 36
Manually check for update ... 36
Super IO Configuration ... 36
Super IO Chip ... 36
Serial Port 0 Configuration ... 37
Serial Port ... 37
Device Settings ... 37

AMT Configuration ... 37
ME Version ... 37
ME Subsystem ... 37
Unconfigure AMT/ME ... 37
Execute MEBx ... 38
Serial Port Console Redirection ... 38
Console Redirection Settings (für COM0 und COM1) ... 38
Serial Port for Out-of-Band Management / Windows Emergency Management Services (EMS) ... 40
Console Redirection (für Out of Band Management / EMS) ... 40
Console Redirection Settings (für Out of Band Management / EMS) ... 40
Network Stack ... 41
Ipv4 PXE Support ... 42
Ipv6 PXE Support ... 42
PXE boot wait time ... 42
CPU Status (nur D3118) ... 42
CPU n ... 42
PCI Status ... 43
PCI Slot n ... 43
Option ROM Configuration ... 43
Launch Slot n OpROM ... 43

Security Menu - Sicherheitsfunktionen ... 44
Password Description ... 45
Administrator Password ... 45
User Password ... 45
User Password on Boot ... 46
Cabinet Monitoring ... 46
Skip Password on WOL ... 46
FLASH Write ... 46
Smartcard SystemLock ... 47
Uninstall SystemLock ... 47
Single Sign On ... 47
Smartcard & PIN ... 47
Unblock Smartcard ... 48
Secure Boot ... 48
Platform Mode ... 48
Secure Boot ... 48
Secure Boot Control ... 48
Secure Boot Mode ... 49
Key Management ... 49

Power Menu – Energiesparfunktionen ... 52
Power Settings ... 52
Power On Source ... 52
Low Power Soft Off ... 53
Power Failure Recovery – Systemzustand nach einem Stromausfall ... 53
Hibernate like Soft Off ... 53
USB At Power-off ... 53
Wake-Up Resources ... 54
LAN ... 54
Wake On LAN Boot ... 54
Wake Up Timer ... 54
Hour ... 54

Minute ... 54
Second ... 54
Wake Up Mode ... 55
Wake Up Day ... 55
USB Keyboard ... 55

Event Logs – Konfiguration und Anzeige der Event Log ... 56
Change Smbios Event Log Settings ... 56
Smbios Event Log ... 56
Erase Event Log ... 56
When Log is full ... 57
Log System Boot Event ... 57
MECI ... 57
METW ... 57
Log OEM Codes ... 57
Convert OEM Codes ... 57
View Smbios Event Log ... 57

Boot Menu – Systemstart ... 58
Boot Configuration ... 58
Bootup NumLock State ... 58
Quiet Boot ... 59
Check Controller Health Status ... 59
POST Errors ... 59
Remove Invalid Boot Options ... 59
Primary Display ... 59
Boot Removable Media ... 60
Virus Warning ... 60
Boot Option Priorities ... 60
CSM Configuration ... 60

Save & Exit Menu – BIOS-Setup beenden ... 63
Save Changes and Exit – Speichern und beenden ... 63
Discard Changes and Exit – Beenden ohne speichern ... 63
Save Changes and Reset ... 63
Discard Changes and Reset ... 64
Save Options ... 64
Save Changes ... 64
Discard Changes ... 64
Restore Defaults ... 64
Save as User Defaults ... 64
Restore User Defaults ... 64
Boot Override ... 64

BIOS-Update ... 65
Auto BIOS Update ... 65
Flash-BIOS-Update unter Windows ... 66
Flash-BIOS-Update mit einem USB-Stick ... 66
BIOS Recovery Update ... 67

Anlage ... 68
Nutzungsbedingungen ... 68

Stichwörter ... 71

Einleitung

Im *BIOS-Setup* können Sie Systemfunktionen und die Hardware-Konfiguration des Systems einstellen.

Die geänderten Einstellungen sind wirksam, sobald Sie die Einstellungen abspeichern und das *BIOS-Setup* beenden.

In den einzelnen Menüs des *BIOS-Setup* können Sie Einstellungen in folgenden Bereichen vornehmen:

Main:	Systemfunktionen
Advanced:	Erweiterte Systemkonfiguration
Security:	Sicherheitsfunktionen
Power:	Energiesparfunktionen
Event Logs:	Konfiguration und Anzeige der Event Log
Boot:	Konfiguration der Startreihenfolge
Save & Exit:	Speichern und beenden

Die Einstellmöglichkeiten hängen von der Hardware-Konfiguration Ihres Systems ab.

Es kann deshalb vorkommen, dass Menüs oder einige Einstellmöglichkeiten im *BIOS-Setup* Ihres Systems nicht angeboten werden oder die Lage der Menüs abhängig von der *BIOS-Revision* variiert.

Darstellungsmittel

	kennzeichnet Hinweise, bei deren Nichtbeachtung Ihre Gesundheit, die Funktionsfähigkeit Ihres Systems oder die Sicherheit Ihrer Daten gefährdet sind. Die Gewährleistung erlischt, wenn Sie durch Nichtbeachtung dieser Hinweise Defekte am System verursachen
	kennzeichnet wichtige Informationen für den sachgerechten Umgang mit dem System
►	kennzeichnet einen Arbeitsschritt, den Sie ausführen müssen
↳	kennzeichnet ein Resultat
`Diese Schrift`	kennzeichnet Eingaben, die Sie mit der Tastatur in einem Programm-Dialog oder in einer Kommandozeile vornehmen, z. B. Ihr Passwort (**`Name123`**) oder einen Befehl, um ein Programm zu starten (**`start.exe`**)
`Diese Schrift`	kennzeichnet Informationen, die von einem Programm am Bildschirm ausgegeben werden, z. B.: `Die Installation ist abgeschlossen!`
Diese Schrift	kennzeichnet • Begriffe und Texte in einer Softwareoberfläche, z. B.: Klicken Sie auf *Speichern*. • Namen von Programmen oder Dateien, z. B. *Windows* oder *setup.exe*.
"Diese Schrift"	kennzeichnet • Querverweise auf einen anderen Abschnitt z. B. "Sicherheitshinweise" • Querverweise auf eine externe Quelle, z. B. eine Webadresse: Lesen Sie weiter auf "http://www.fujitsu.com/fts/" • Namen von CDs, DVDs sowie Bezeichnungen und Titel von anderen Materialien, z. B.: "CD/DVD Drivers & Utilities" oder Handbuch "Sicherheit"
Abc	kennzeichnet eine Taste auf der Tastatur, z. B: F10

Bedienung des BIOS-Setup

BIOS-Setup aufrufen

► Schalten Sie das System ein.

↳ Warten Sie bis die Bildschirmausgabe erscheint.

► Drücken Sie die Funktionstaste F2.

► Wenn das System passwortgeschützt ist, müssen Sie nun das Passwort eingeben und mit der Taste Enter bestätigen. Details zur Passwortvergabe finden Sie unter "Password Description", Seite 45.

↳ Am Bildschirm wird das Menü Main des BIOS-Setup angezeigt.

► Um systemspezifische Informationen anzuzeigen, wählen Sie *System Information* und drücken Sie die Taste Enter.

↳ Die BIOS Release Information wird angezeigt:

- Der Ausgabestand (Revision) des BIOS (z. B. R1.3.0)

  Unter Board finden Sie die Nummer des System-Board (z. B. D3062-A11)

  Anhand der Nummer des System-Boards können Sie auf der CD/DVD "Drivers & Utilities" das entsprechende Technische Handbuch zum System-Board finden oder Sie können im Internet die entsprechende BIOS-Update Datei laden (siehe "BIOS-Update", Seite 65).

Wenn Sie sofort das Boot Menu aufrufen möchten

Diese Funktion können Sie nutzen, wenn Sie Ihr System nicht von dem Laufwerk starten möchten, das unter *Boot Option Priorities* im Menü *Boot* als erste Einstellung angegeben ist.

- ► Starten Sie das System und warten Sie bis die Bildschirmausgabe erscheint.
- ► Drücken Sie die Funktionstaste F12.
- ↳ Am Bildschirm werden die Boot-Optionen als Popup-Fenster angezeigt. Sie können nun auswählen, von welchem Laufwerk Sie das Betriebssystem starten möchten. Die Auswahlmöglichkeiten sind mit den möglichen Einstellungen unter *Boot Option Priorities* im Untermenü *Boot* identisch.
- ► Wählen Sie mit Hilfe der Cursor-Tasten ↑ oder ↓ aus, von welchem Laufwerk Sie das Betriebssystem jetzt starten möchten und bestätigen Sie Ihre Auswahl mit der Taste Enter.

Ihre Auswahl gilt nur für den aktuellen Systemstart. Beim nächsten Systemstart gelten wieder die Einstellungen im Menü *Boot*.

- ► Falls Sie das BIOS-Setup starten möchten, wählen Sie mit Hilfe der Cursor-Tasten ↑ oder ↓ den Eintrag *Enter Setup* aus und bestätigen Sie die Auswahl mit der Taste Enter.
- ► Falls Sie einen Basistests von CPU, Arbeitsspeicher und Festplatten durchführen wollen, wählen Sie mit Hilfe der Cursor-Tasten ↑ oder ↓ den Eintrag *Diagnostic Program* aus und bestätigen Sie die Auswahl mit der Taste Enter.

Wenn Sie sofort von LAN booten möchten

- ► Drücken Sie die Funktionstaste F11 wenn Sie direkt über LAN und nicht von dem Laufwerk starten möchten, das unter *Boot Option Priorities* im Menü *Boot* als erste Einstellung angegeben ist.

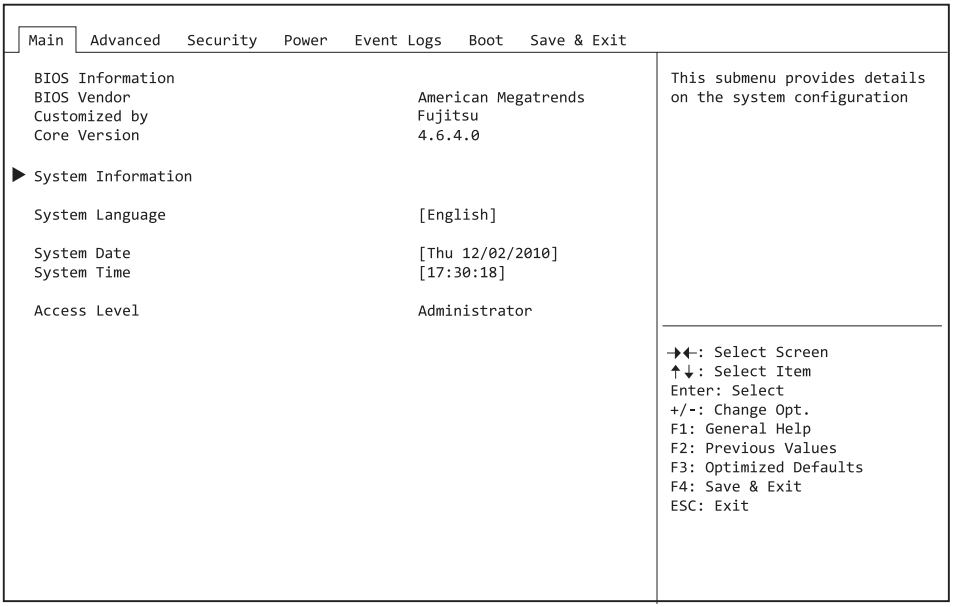
BIOS-Setup bedienen

Cursor-Tasten ← oder →	Menü aus der Menüleiste auswählen
Cursor-Tasten ↑ oder ↓	Feld auswählen - das ausgewählte Feld wird hervorgehoben dargestellt
Enter oder ESC	Untermenü (mit ► gekennzeichnet) öffnen Enter und verlassen ESC
Tasten + oder - (numerisches Tastaturfeld)	Eintrag für Feld ändern
Funktionstaste F3	Standardeinträge für alle Menüs einstellen
Funktionstaste F2	Einträge einstellen, die beim Aufruf des *BIOS-Setup* gültig waren

BIOS-Setup beenden

► Wählen Sie das Menü *Save & Exit* aus der Menüleiste um das *BIOS-Setup* zu beenden.
↳ Sie können dann entscheiden, ob Sie die geänderten Einstellungen speichern wollen.
► Wählen Sie die gewünschte Möglichkeit.
► Drücken Sie die Eingabetaste.

Main Menu – Systemfunktionen



Beispiel für das Menu *Main*.

Das *Main Menu* wird eingesetzt, um die grundlegende Systemkonfiguration festzulegen und sich eine Übersicht zu verschaffen. Einige der Parameter stehen nur unter bestimmten Voraussetzungen zur Verfügung.

System Information

Dieses Untermenü enthält Beschreibungen über die Systemkonfiguration. Einige Parameter stehen nur optional zur Verfügung.

Board und Firmware Details

Zeigt aktuelle Informationen zum verbauten System-Board und zur Firmware.

BIOS Revision	Zeigt die aktuelle BIOS Version an.
Build Date and Time	Zeigt das Datum und den Zeitpunkt der Entwicklung des aktuellen BIOS an.
Board	Zeigt Informationen zum aktuellen System-Board an.
Ident Number	Zeigt die Identifikationsnummer des Systems an.
UUID	Zeigt die 16 Byte lange, auch als Globally Unique Identifier (GUID) bezeichnete Universal Unique ID an.

Network Controller Details

Zeigt die 6 Byte lange MAC-Adresse (Media Access Control) des LAN-Controllers an.

Processor Details

Processor Type	Zeigt die CPU Bezeichnung an.
CPU-/Patch-ID	Zeigt die CPU-ID und die aktuelle Patch-ID an.
Processor Speed	Zeigt die Geschwindigkeit des Prozessorkerns an.
Cache Counts & Sizes	Zeigt ausführliche Informationen zum Cache an.
Active Package, Core & Thread Count (maximum)	Zeigt die Anzahl der aktiven und maximal verfügbaren CPU-Pakete, Kerne und Threads an.

Memory Details

Zeigt die Speichermengen Details an.

Memory Size / Frequency	Zeigt den Gesamtspeicher in Megabyte und die Speicherfrequenz in MHz an.
DIMM n	Zeigt die Speichergröße in Megabyte für den entsprechenden Speichersteckplatz an.

System Language

Legt die im *BIOS-Setup* verwendete Sprache fest.

System Date / System Time

Zeigt das aktuell eingestellte Datum / die aktuell eingestellte Uhrzeit des Systems an. Das Datum hat das Format "Tag der Woche, Monat/Tag/Jahr". Die Uhrzeit hat das Format "Stunde/Minute/Sekunde". Wenn Sie das aktuell eingestellte Datum / die aktuell eingestellte Uhrzeit verändern wollen, geben Sie das neue Datum im Feld *System Date* / die neue Uhrzeit im Feld *System Time* ein. Mit der Tabulatortaste können Sie den Cursor innerhalb der Felder *System Time* und *System Date* bewegen.

Wenn die Systemdatum/zeit -Felder beim Hochfahren des Computers häufig falsche Werte enthalten, ist die Lithium-Batterie möglicherweise leer und muss ersetzt werden. Die Vorgehensweise zum Wechseln der Lithium-Batterie ist im Handbuch des System-Board beschrieben.

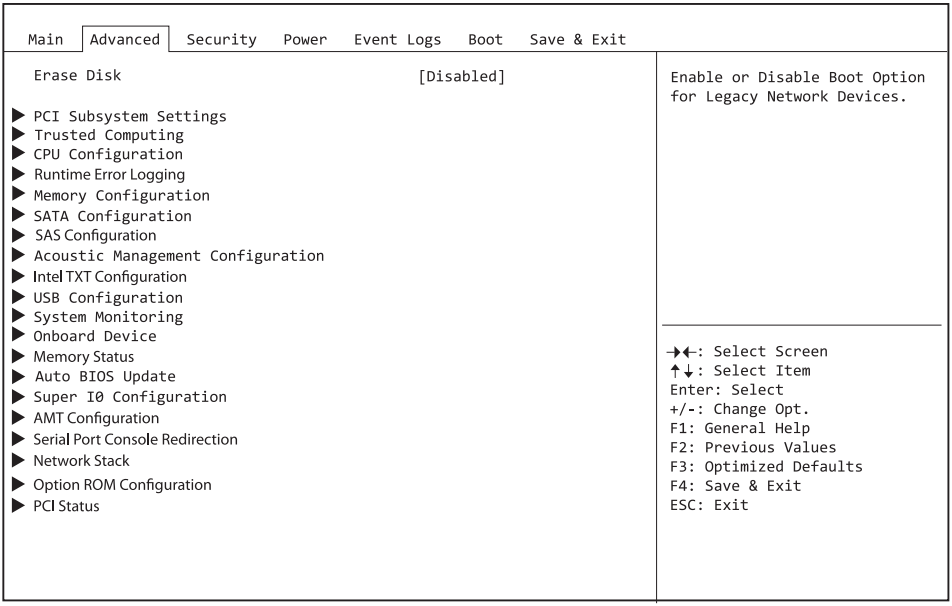
Access Level

Zeigt die aktuelle Zugriffsebene im *BIOS-Setup* an. Wenn das System nicht passwortgeschützt ist oder ein Administrator-Passwort vergeben wurde, ist die Zugriffsebene Administrator. Wenn das Administrator- und das User-Passwort vergeben sind, hängt der Access Level vom eingegebenen Passwort ab.

Advanced Menu – Erweiterte Systemkonfiguration

In diesem Menü für die erweiterte Systemkonfiguration werden die erweiterten Funktionen konfiguriert, die dem System zur Verfügung stehen.

Ändern Sie die Standardeinstellungen nur bei Spezialanwendungen. Falsche Einstellungen können zu Fehlfunktionen führen.



Beispiel für das Menü *Advanced*.

Erase Disk

Erase Disk ist eine in die Fujitsu Technology Solutions integrierte Firmware (*UEFI: Unified Extensible Firmware Interface*), um alle Daten von (einer) SATA-Festplatte(n) zu löschen.

Mit dieser Funktion können alle Daten von internen oder extern über den eSATA-Anschluss verbundenen SATA-Festplatten unwiederbringlich gelöscht werden, bevor die Festplatten entsorgt werden oder das komplette Computersystem veräußert wird. Die Funktion kann auch verwendet werden, wenn Festplatten komplett gelöscht werden sollen, z. B. vor dem Installieren eines neuen Betriebssystems.

Die Anwendung kann nur ausgewählt und ausgeführt werden, wenn ein Administrator-/Supervisorpasswort zugewiesen worden ist (*BIOS-Setup* -> *Security Menu*).

Bitte beachten Sie, dass Solid-State-Laufwerke (SSD) nicht sicher gelöscht werden können.

Um Festplatten in einem RAID-System zu löschen, muss der Modus des RAID-Controllers geändert werden, z. B. auf *IDE Mode* oder *AHCI Mode* im *SATA Configuration*-Untermenü des Menüs *Advanced*.

Zum Löschen von Daten von SATA-Festplatten gehen Sie folgendermaßen vor:

► Rufen Sie das *BIOS-Setup* mit dem Administrator-/Supervisorpasswort auf.

► Zum Starten der Anwendung wählen Sie *Erase Disk* (*BIOS-Setup* -> *Advanced* oder *BIOS-Setup* -> *Security*) und stellen Sie *Start after Reboot* ein.

► Wählen Sie dann *Save Changes and Exit* im Menü *Save & Exit* / *Exit*, um einen Neustart und Erase Disk einzuleiten.

Durch den Neustart wird das Menü *Erase Disk* gestartet. Sie haben die Möglichkeit den Vorgang während der Benutzerauswahl abzubrechen.

► Nach dem Start der Anwendung muss aus Sicherheitsgründen das Administrator-/Supervisorpasswort eingegeben werden.

↳ In einem eingeblendeten Dialogfeld können eine bestimmte, mehrere oder alle Festplatten zur Löschung ausgewählt werden – dies ist abhängig von der Anzahl der Festplatten in Ihrem System.

► Wählen Sie die zu löschende(n) Festplatte(n) aus.

↳ Die ausgewählte(n) Festplatte(n) wird/werden einzeln gelöscht.

Erase Disk bietet vier Löschoptionen, von "fast" (schnell) (mit einem Löschdurchlauf) bis "very secure" (sehr sicher) (mit 35 Löschdurchläufen). Je nach ausgewähltem Algorithmus kann der Vorgang zwischen ~10 Sek. und ~10 Min. pro GB dauern:

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

Weitere Informationen zu Löschalgorithmen finden Sie hier:

- "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"

► Wählen Sie den gewünschten Festplatten-Löschalgorithmus aus.

Der vollständige Löschvorgang kann als revisionssicheres Protokoll auf ein externes USB-Laufwerk kopiert werden, welches FAT32-formatiert sein muss. Schließen Sie nur ein externes USB-Laufwerk an.

► Wählen Sie, ob ein Statusreport auf das USB-Stick geschrieben werden soll.

Der Nutzer kann die folgenden Aufgaben auswählen, die nach dem Löschvorgang durch das System durchgeführt werden:

- *Reset administrator and user password* (Administrator- und Benutzerpasswort zurücksetzen)
- *Load BIOS setup defaults* (BIOS-Standardkonfiguration laden)
- *Shutdown the Computer* (Computer herunterfahren)
- *Exit Erase Disk with no additional options upon completion* (*Erase Disk* nach dem Durchlauf ohne weitere Optionen beenden)

► Wählen Sie die gewünschte Aufgabe aus.
↳ Der Löschvorgang beginnt.

Disabled	Erase Disk wird nach dem nächsten Neustart NICHT gestartet.
Start after Reboot	Erase Disk wird nach dem nächsten Neustart gestartet.

PCI Subsystem Settings

Above 4G Decoding

Legt fest, ob Speicher-Ressourcen über der 4-GB-Adress-Grenze PCI-Geräten zugeordnet werden können. Die Auswahl hängt vom Betriebssystem und von den Adapter-Karten ab.

Disabled	Nur Speicher-Ressourcen unter der 4-GB-Adress-Grenze werden den PCI-Geräten zugeordnet. Diese Auswahl wird bei 32-Bit-Betriebssystemen zwingend vorgenommen, aber auch von 64-Bit-Betriebssystemen unterstützt.
Enabled	Speicher-Ressourcen über der 4-GB-Adress-Grenze können PCIGeräten zugeordnet werden, wenn diese über 64-Bit-Adress-Dekodierung verfügen. Diese Auswahl wird nur von 64-Bit-Betriebssystemen unterstützt. Diese Auswahl kann notwendig sein, wenn die eingebauten PCI-Express-Geräte (z.B. Co-Prozessor-Adapter-Karten) einen großen Speicherbedarf haben, der nicht mehr in den Adressraum unterhalb von 4 GB hineinpasst.

Die PCI-Adress-Dekodierung ist bei 32-Bit-Betriebssystemen auf die 4-GB-Adress-Grenze begrenzt, auch wenn die verfügbaren PCI-Geräte die 64-Bit-Adress-Dekodierung unterstützen.

PERR# Generation

Legt fest, ob PERR# (PCI-Paritätsfehler) erzeugt werden.

Disabled	PCI-Paritätsfehler werden nicht erzeugt.
Enabled	PCI-Paritätsfehler werden erzeugt.

SERR# Generation

Legt fest, ob SERR# (PCI-Systemfehler) erzeugt werden.

Disabled	PCI-Systemfehler werden nicht erzeugt.
Enabled	PCI-Systemfehler werden erzeugt.

PCI Express Link Register Settings

ASPM Support

Konfigurieren Sie Active State Power Management (ASPM), um den Stromverbrauch des PCI Express Link schrittweise zu reduzieren und so Energie zu sparen. Auch wenn ASPM durch diese Auswahl allgemein aktiviert ist, wird es nur dann für eine bestimmte Verbindung aktiviert, wenn die entsprechende PCI Express-Adapterkarte oder der entsprechende Onboard-Controller dies ebenfalls unterstützt.

Disabled	ASPM ist deaktiviert. Der Stromverbrauch für PCI-Express-Verbindungen wird nicht reduziert. Beste Kompatibilität.
Auto	Maximale Energieeinsparung konfigurieren. Low-Power-Modus der PCI-Express-Verbindungen auf L0s (unidirektional) oder L1 (bidirektional) setzen.
Limit to L0s	Low-Power-Modus der PCI-Express-Verbindungen auf L0s (unidirektional) beschränken. Kompromiss zwischen Kompatibilität und Energieeinsparung.

Die Latenz (Verzögerung) für PCI-Express-Geräte kann sich erhöhen, wenn ASPM nicht deaktiviert wird. Verschiedene Adapterkarten unterstützen diese Funktion nicht korrekt, was zu einem undefinierten Systemverhalten führen kann.

Slot n Link Speed

Ermöglicht es für einzelne PCIe-Steckplätze die maximal mögliche Link Speed zu begrenzen.

GEN1	Die maximal mögliche Link Speed wird auf GEN1 (2,5 GT/s) begrenzt.
GEN2	Die maximal mögliche Link Speed wird auf GEN2 (5 GT/s) begrenzt.
GEN3	Die maximal mögliche Link Speed wird auf GEN3 (8 GT/s) begrenzt.

TPM (Trusted Platform Module) Computing

Öffnet das Untermenü zum Aktivieren von TPM sowie zum Ändern der TPM-Einstellungen. Wenn dieses Setup-Menü verfügbar ist, enthält das System-Board einen Sicherheits- und Verschlüsselungs-Chip (TPM - Trusted Platform Module), der der TCG Spezifikation 1.2 entspricht. Dieser Chip ermöglicht die sichere Speicherung sicherheitsrelevanter Daten (Passwörter usw.). Der Einsatz von TPM ist standardisiert und wird von der Trusted Computing Group (TCG) spezifiziert.

TPM Support

Legt fest, ob die TPM-Hardware (Trusted Platform Module) verfügbar ist. Bei Deaktivierung von TPM verhält sich das System wie jedes andere System ohne TPM-Hardware.

Disabled	Trusted Platform Module ist nicht verfügbar.
Enabled	Trusted Platform Module ist verfügbar.

TPM State

Legt fest, ob TPM (Trusted Platform Module) vom Betriebssystem verwendet werden kann.

Disabled	Trusted Platform Module kann nicht verwendet werden.
Enabled	Trusted Platform Module kann verwendet werden.

Pending TPM operation

Legt eine TPM-Operation fest, die während des nächsten Bootvorgangs durchgeführt wird.

None	Es wird keine TPM-Operation durchgeführt.
Enable Take Ownership	Das Betriebssystem kann den Besitz des TPM übernehmen.
Disable Take Ownership	Das Betriebssystem kann den Besitz des TPM nicht übernehmen.
TPM Clear	TPM wird auf Werkseinstellung zurückgesetzt. Alle Schlüssel im TPM werden gelöscht.

Current TPM Status Information

Zeigt den aktuellen TPM-Status (Trusted Platform Module) an.

TPM SUPPORT OFF	Wird angezeigt, wenn der *TPM Support* deaktiviert ist.
TPM Enabled Status	Zeigt an, ob das TPM verwendet werden kann.
TPM Active Status	Zeigt an, ob das TPM aktiviert ist.
TPM Owner Status	Zeigt den TPM-Besitzerstatus an.

CPU Configuration

Öffnet das Untermenü *CPU Configuration*.

Socket n CPU Information

Öffent das Untermenü um Informationen der CPU im Sockel n anzuzeigen.

Processor Type	Zeigt die CPU Bezeichnung an.
CPU Signature	Zeigt die CPU-ID an.
Microcode Patch	Zeigt die CPU Micropatch ID an.
Max CPU Speed	Zeigt die maximale Geschwindigkeit des Prozessorkerns ohne Turbo-Modus an.
Min CPU Speed	Zeigt die Mindestgeschwindigkeit des Prozessorkerns an.
Processor Cores	Zeigt die maximale Anzahl verfügbarer CPU-Kerne an.
Intel HT Technology	Zeigt an, ob Intel® Hyper Threading Technology von der CPU unterstützt wird.
Intel VT-x Technology	Zeigt an, ob Intel® VT-x (Virtualisation Technology) von der CPU unterstützt wird.
Intel SMX Technology	Zeigt an, ob Intel® SMX (Safer Mode Extensions) von der CPU unterstützt wird.
L1 Data Cache	Zeigt die Speichergröße des L1 Daten-Cache an.
L1 Code Cache	Zeigt die Speichergröße des L1 Befehls-Cache an.
L2 Cache	Zeigt die Speichergröße des L2 Cache an.
L3 Cache	Zeigt die Speichergröße des L3 Cache an.

Hyper Threading

Die Hyper-Threading-Technologie lässt einen einzigen physikalischen Prozessor als mehrere logische Prozessoren erscheinen. Mit Hilfe dieser Technologie kann das Betriebssystem die internen Prozessor-Ressourcen besser nutzen, was eine Leistungssteigerung mit sich bringt. Die Vorteile dieser Technologie können nur von einem Betriebssystem genutzt werden, das ACPI unterstützt. Bei Betriebssystemen ohne ACPI-Unterstützung hat diese Einstellung keine Wirkung.

Disabled	Ein ACPI-Betriebssystem kann nur den ersten logischen Prozessor des physikalischen Prozessor verwenden. Diese Einstellung sollte nur dann gewählt werden, wenn das Betriebssystem die Hyper-Threading-Technologie nicht unterstützt.
Enabled	Ein ACPI-Betriebssystem kann alle logischen Prozessoren des physikalischen Prozessor verwenden.

Active Processor Cores

Bei Prozessoren, die mehrere Prozessorkerne enthalten, kann die Anzahl der aktiven Prozessorkerne eingeschränkt werden. Inaktive Prozessorkerne werden nicht genutzt und vor dem Betriebssystem verborgen.

All	Alle verfügbaren Prozessorkerne sind aktiv und können genutzt werden.
[1..n]	Nur die gewählte Anzahl der Prozessorkerne ist aktiv. Die übrigen Prozessorkerne sind deaktiviert.

Mit der hier getroffenen Auswahl lassen sich eventuell Probleme mit bestimmten Software-Paketen oder System-Lizenzen lösen.

Limit CPUID Maximum

Legt die Anzahl der CPUID-Funktionen fest, die vom Prozessor aufgerufen werden. Einige Betriebssysteme können neue CPUID Befehle, die mehr als drei Funktionen unterstützen, nicht verarbeiten. Dieser Parameter sollte für diese Betriebssysteme aktiviert werden.

Disabled	Alle CPUID-Funktionen werden unterstützt.
Enabled	Aus Gründen der Kompatibilität mit dem Betriebssystem wird nur eine reduzierte Anzahl von CPUID-Funktionen vom Prozessor unterstützt.

Execute Disable Bit

Erlaubt es, die Ausführung von Programmen in bestimmten Speicherbereichen zu verhindern (Virenschutz). Die Funktion ist nur wirksam, wenn sie auch vom Betriebssystem unterstützt wird. Das eXecute Disable-Bit (XD-Bit) wird auch als NX-Bit (No eXecute) bezeichnet.

Enabled	Ermöglicht es dem Betriebssystem, die Execute-Disable-Funktion einzuschalten.
Disabled	Verhindert, dass das Betriebssystem die eXecute-Disable-Funktion einschalten kann.

Hardware Prefetcher

Bei Aktivierung dieser Funktion erfolgt bei inaktivem Speicherbus ein automatischer Vorablesezugriff auf den voraussichtlich benötigten Speicherinhalt. Wenn Inhalte aus dem Cache und nicht aus dem Speicher geladen werden, verkürzt sich die Latenz. Dies gilt besonders für Anwendungen mit linearem Datenzugriff.

Mit diesem Parameter können Sie Leistungseinstellungen für nicht-standardisierte Anwendungen vornehmen. Bei Standardanwendungen wird empfohlen, die Standardeinstellungen beizubehalten.

Disabled	Deaktiviert den Hardware-Prefetcher der CPU.
Enabled	Aktiviert den Hardware-Prefetcher der CPU.

Adjacent Cache Line Prefetcher

Steht zur Verfügung, wenn der Prozessor einen Mechanismus bietet, mit dem während jeder Cache-Anforderung zusätzlich eine angrenzende 64 Byte Cache Line geladen werden kann. Hierdurch erhöht sich die Anzahl der Treffer im Cache bei Anwendungen mit hoher räumlicher Lokalität.

Mit diesem Parameter können Sie Leistungseinstellungen für nicht-standardisierte Anwendungen vornehmen. Bei Standardanwendungen wird empfohlen, die Standardeinstellungen beizubehalten.

Disabled	Der Prozessor lädt die angeforderte Cache-Line.
Enabled	Der Prozessor lädt die angeforderte und die angrenzende Cache-Line.

DCU (Data Cache Unit) Streamer Prefetcher

Mit dieser Option werden Dateninhalte, die wahrscheinlich benötigt werden, automatisch vorab in den L1-Daten-Cache geladen, wenn der Speicherbus inaktiv ist. Indem Inhalte aus dem Cache statt aus dem Speicher abgerufen werden, verringert sich die Latenz besonders für Anwendungen mit linearem Datenzugriff.

Mit diesem Parameter können Sie die Leistungseinstellungen für Nicht-Standardanwendungen ändern. Es wird empfohlen, die Standardeinstellungen für Standardanwendungen beizubehalten.

Enabled	Aktiviert die Funktion DCU Streamer Prefetcher der CPU.
Disabled	Deaktiviert die Funktion DCU Streamer Prefetcher der CPU.

DCU Ip (Instruction pointer-based) Prefetcher

Leistungssteigerungen sind zu erwarten, wenn der Code der Reihe nach und im zusammenhängenden Speicher verwendet wird.

Mit diesem Parameter können Sie die Leistungseinstellungen für Nicht-Standardanwendungen ändern. Es wird empfohlen, die Standardeinstellungen für Standardanwendungen beizubehalten.

Enabled	Aktiviert die Funktion DCU Streamer Prefetch der CPU.
Disabled	Aktiviert die Funktion DCU Streamer Prefetch der CPU.

Intel Virtualization Technology

Wird zur Unterstützung der Visualisierung von Plattform-Hardware und mehrerer Software-Umgebungen verwendet. Basiert auf Virtual Machine Extensions (VMX), um die Verwendung mehrerer Software-Umgebungen unter Nutzung virtueller Rechner zu unterstützen. Die Virtualisierungstechnik erweitert die Prozessorunterstützung für Virtualisierungszwecke auf die über 16 Bit und 32 Bit geschützten Modi und auf den Intel® Extended Memory 64 Technology (EM64T) Modus.

Im aktiven Modus kann ein Virtual Machine Monitor (VMM) die zusätzlichen Leistungsmerkmale der Vanderpool Technology-Hardware nutzen.

Disabled	Ein Virtual Machine Monitor (VMM) kann die zusätzlichen Leistungsmerkmale der Hardware nicht nutzen.
Enabled	Ein VMM kann die zusätzlichen Leistungsmerkmale der Hardware nutzen.

VT-d

VT-d (Intel Virtualization Technology for Directed I/O) ist eine Hardwareunterstützung für die gemeinsame Nutzung von E/A-Geräten durch mehrere virtuelle Maschinen. VMM-Systeme (Virtual-Machine-Monitor) können VT-d zur Verwaltung verschiedener virtueller Maschinen einsetzen, die auf das gleiche physikalische E/A-Gerät zugreifen.

Disabled	VT-d ist ausgeschaltet und für die VMMs nicht verfügbar.
Enabled	VT-d ist für die VMMs verfügbar.

Power Technology

Konfiguriert die CPU-Power-Management-Funktionen.

Disabled	Die CPU-Power-Management-Funktionen sind deaktiviert.
Energy Efficient	Die CPU-Power-Management-Funktionen sind auf Energieeffizienz optimiert.
Custom	Weitere Einstelloptionen für die CPU-Power-Management-Konfiguration stehen zur Verfügung.

Enhanced Speedstep

Legt die Spannung und Frequenz des Prozessors fest. EIST (Enhanced Intel SpeedStep® Technology) ist eine Energiesparfunktion.

Die Prozessorspannung wird an die jeweils benötigten Systemanforderungen angepasst. Eine Verringerung der Taktfrequenz führt dazu, dass das System weniger Energie benötigt.

Disabled	Die Enhanced SpeedStep-Funktionalität ist deaktiviert.
Enabled	Die Enhanced SpeedStep-Funktionalität ist aktiviert.

Turbo Mode

Der Prozessor darf schneller als mit der angegebenen Frequenz arbeiten, wenn das Betriebssystem den maximalen Leistungszustand anfordert (P0). Diese Funktion ist auch als Intel® Turbo Boost Technology bekannt.

Disabled	Der Turbo Mode ist deaktiviert.
Enabled	Der Turbo Mode ist aktiviert.

Energy Performance

Energieeffizienz-Vorgaben für den Prozessor bei Nicht-Legacy-Betriebssystemen. Der Prozessor erhält die Anweisung, Energieverbrauch und Performance anzupassen.

Performance	Optimierung mit Hinblick auf Performance, ggf. auf Kosten der Energieeffizienz.
Balanced Performance	Optimierung mit Hinblick auf die Performance bei guter Energieeffizienz.
Balanced Energy	Optimierung mit Hinblick auf Energieeffizienz bei guter Performance.
Energy Efficient	Optimierung mit Hinblick auf Energieeffizienz, ggf. auf Kosten der Performance.

Abhängig von der gewählten Energieoption wählt das Betriebssystem ggf. einen anderen Modus als den im Setup gewählten.

P-State Coordination

Prozessor-Performance-Koordinationsmodell, das ans OS-Power-Management (OSPM) kommuniziert wird.

HW_ALL	Die Prozessor-Hardware ist für die Koordination der Performance-Zustände aller logischen Prozessoren zuständig (empfohlen).
SW_ALL	OSPM ist für die Koordination der Performance-Zustände aller logischen Prozessoren zuständig. Performance-Übergänge müssen auf allen logischen Prozessoren initiiert werden (nicht empfohlen).
SW_ANY	OSPM ist für die Koordination der Performance-Zustände aller logischen Prozessoren zuständig. Performance-Übergänge können auf beliebigen logischen Prozessoren initiiert werden.

CPU C3 Report

Übergibt den Prozessor-C3-Status als ACPI-C2/C3-Status an das OSPM, wenn dies vom jeweilig verwendeten Legacy-Betriebssystem unterstützt wird.

Disabled	CPU C3 wird nicht an das OSPM übergeben.
ACPI C-2	CPU C3 wird als ACPI-C2-Status an das OSPM übergeben.
ACPI C-3	CPU C3 wird als ACPI-C3-Status an das OSPM übergeben.

CPU C6 Report

Übergibt den Prozessor-C6-Status als ACPI-C3-Status an das OSPM, um Processor Deep Power Down Technology zu aktivieren.

Disabled	CPU C6 wird nicht als ACPI-C3-Status an das OSPM übergeben.
Enabled	CPU C6 wird als ACPI-C3-Status an das OSPM übergeben.

CPU C7 Report

Übergibt den Prozessor-C7-Status als ACPI-C3-Status an das OSPM, um Processor Deep Power Down Technology zu aktivieren.

Disabled	CPU C7 wird nicht als ACPI-C3-Status an das OSPM übergeben.
Enabled	CPU C7 wird als ACPI-C3-Status an das OSPM übergeben.

Package C State limit

Ermöglicht es, das C State-Limit des Prozessors zu konfigurieren.

C0	Das C State-Limit lautet C0.
C1	Das C State-Limit lautet C1.
C6	Das C State-Limit lautet C6.
C7	Das C State-Limit lautet C7.
No limit	Ein beliebiger C-State kann aktiviert werden.

QPI Link Frequency Select

Stellt die Verbindung zwischen den Prozessoren her. Abhängig von den Prozessoren können QPI-Links mit unterschiedlichen Geschwindigkeiten arbeiten. Dieser Parameter steuert die Geschwindigkeit der QPI-Links Ihres Systems.

Auto	Das BIOS ermittelt abhängig von den Prozessoren in Ihrem System die Maximalgeschwindigkeit.

► Um die Geschwindigkeit der QPI-Links manuell festzulegen, wählen Sie einen der anderen Werte, falls dies von Ihrem System unterstützt wird.

Frequency floor override

Legt fest, ob die Frequenz des Prozessor unabhängig von den Systemanforderungen mit der maximalen Prozessorfrequenz betrieben wird. Dies erhöht die IO Performance und verkürzt die Antwortzeiten der CPU bei höherem Energiebedarf der CPU.

Disabled	Der Prozessor wird abhängig von den Systemanforderungen mit der maximalen Prozessorfrequenz betrieben.
Enabled	Der Prozessor wird permanent mit der maximalen Prozessorfrequenz betrieben.

Runtime Error Logging

ECC Memory Error Logging

Legt fest, ob ECC Speicherfehler erkannt und in die SMBIOS Eventlog eingetragen werden.

Enabled	Es werden sowohl Single-bit Speicherfehler als auch Multi-bit Speicherfehler in die SMBIOS Eventlog eingetragen.
Multi-bit Errors Only	Es werden nur Multi-bit Speicherfehler in die SMBIOS Eventlog eingetragen.
Disabled	Es werden keine Speicherfehler in die SMBIOS Eventlog eingetragen.

PCI Error Logging

Legt fest, ob PCI Fehler in die SMBIOS Eventlog eingetragen werden.

Um PCI Fehler erkennen zu können muss zuvor im Menü *PCI Subystem Settings* die Erzeugung von PERR# (PCI-Paritätsfehler) bzw. SERR# (PCI-Systemfehler) aktiviert werden.

Disabled	Es werden keine PCI Fehler in die SMBIOS Eventlog eingetragen.
Enabled	PCI Fehler werden in die SMBIOS Eventlog eingetragen.

Memory Configuration

Öffnet das Untermenü *Memory Configuration*.

NUMA (nur D3118)

NUMA (Non-Uniform Memory Access) ist eine Speicherarchitektur für Multiprozessor-Systeme. Jeder Prozessor verfügt über seinen eigenen lokalen Speicher, kann jedoch ebenfalls auf den lokalen Speicher des anderen Prozessor zugreifen (Shared Memory, gemeinsamer Speicher). Der Zugriff auf den lokalen Speicher ist schneller als der Zugriff auf den gemeinsamen Speicher.

Disabled	Der gesamte Systemspeicher wird in viele kleine, ineinander verzahnte Bereiche von lokalem und gemeinsamen Speicher aufgeteilt. Verwenden Sie diese Option, wenn das Betriebssystem NUMA nicht unterstützt.
Enabled	Der gesamte Systemspeicher wird in wenige, große, nicht ineinander verzahnte Bereiche von lokalen und gemeinsamen Speicher aufgeteilt. Dadurch erzielen Sie bei einem ACPI-Betriebssystem, das NUMA unterstützt, beste Ergebnisse mit Hinblick auf die Performance.

DDR Performance

Die Speichermodule können mit verschiedenen Geschwindigkeiten (Frequenzen) arbeiten.

Die Leistung erhöht sich bei höheren Geschwindigkeiten, die Energieeinsparung erhöht sich hingegen bei geringeren Geschwindigkeiten. Die möglichen Speichergeschwindigkeiten richten sich nach der jeweiligen Speichermodul-Konfiguration.

Low-Voltage optimized	Höchstmögliche Geschwindigkeit bei geringer Spannung.
Energy optimized	Geringstmögliche Geschwindigkeit, um Energie zu sparen.
Performance optimized	Höchstmögliche Geschwindigkeit für beste Performance.

Fast Patrol Scrub (nur D3118)

Bestimmt die Patrol-Scrub-Rate. Eine höhere Patrol-Scrub-Rate führt zu einer höheren Zuverlässigkeit des Speichers, aber auch zu einem erhöhten Stromverbrauch und einer verminderten Leistung.

Disabled	Eine Überprüfung des Speichers des gesamten Systems im Hintergrund kann einen ganzen Tag dauern, führt dafür aber zu einer höheren Leistung und einem verminderten Stromverbrauch.
Enabled	Eine Überprüfung des Speichers des gesamten Systems im Hintergrund dauert nur wenige Minuten, führt dafür aber zu einer höheren Zuverlässigkeit.

Refresh Rate Multiplier

Wählt den Multiplikator für die Standard DRAM Refresh Rate aus. Ein höherer Multiplikator erhöht die Zuverlässigkeit des Speichers, führt aber auch zu einem höheren Stromverbrauch und einer verminderten Leistung.

1x	Standard DRAM Refresh Rate, führt zu einer höheren Performance und einem reduzierten Stromverbrauch.
2x...4x	Multiplikator für die Standard DRAM Refresh Rate, führt zu einer höheren Zuverlässigkeit Beispiel: Wenn *2x* ausgewählt ist, wird das DRAM doppelt so oft in einem Zeitabschnitt aktualisiert wie sonst, verglichen mit der Standard DRAM Refresh Rate.

SATA Configuration

Öffnet das Untermenü SATA Configuration.

SATA Mode

Legt fest, in welchem Modus die SATA-Schnittstellen betrieben werden.

Disabled	Die SATA-Schnittstelle ist deaktiviert.
IDE	Die SATA-Schnittstelle wird im IDE-Modus betrieben.
AHCI	Die SATA-Schnittstelle wird im AHCI-Modus betrieben.

Aggressive LPM Support

Ermöglicht es im AHCI-Modus das Aggressive Link Power Management (ALPM) zuzulassen, um Energie zu sparen.

Disabled	ALPM ist deaktiviert.
Enabled	ALPM ist aktiviert.

Serial-ATA Controller 0

Legt im IDE-Modus fest, in welchem Modus der SATA-Controller 0 betrieben wird.

Disabled	Der SATA-Controller 0 ist deaktiviert.
Enhanced	Die dem SATA-Controller 0 zugewiesenen Ressourcen sind nicht auf die Legacy-Ressourcen begrenzt. Je nach Betriebssystem kann die Leistung höher sein, als im kompatiblen Modus.
Compatible	Nur vordefinierte Legacy-Ressourcen (E/A-Schnittstellen, IRQ) werden dem SATA Controller 0 zugeordnet. Dieser Modus ist besonders für ältere Betriebssysteme geeignet, wenn der Enhanced- oder AHCI-Modus nicht unterstützt wird.

Serial-ATA Controller 1

Legt im IDE-Modus fest, in welchem Modus der SATA-Controller 1 betrieben wird.

Disabled	Der SATA-Controller 1 ist deaktiviert.
Enhanced	Die dem SATA-Controller 1 zugewiesenen Ressourcen sind nicht auf die Legacy-Ressourcen begrenzt. Je nach Betriebssystem kann die Leistung höher sein, als im kompatiblen Modus.

Staggered Spin-up

Reduziert die elektrische Last beim Start von Systemen mit mehreren SATA-Geräten. Die SATA-Geräte laufen nacheinander auf Anforderung des HOST-Controller an.

Disabled	Staggered Spin-up ist deaktiviert.
Enabled	Staggered Spin-up ist aktiviert.

External SATA Port

Legt fest, ob die Schnittstelle intern als SATA oder extern als eSATA betrieben wird.

Disabled	Der Port wird intern als SATA verwendet.
Enabled	Der Port wird extern als external SATA (eSATA) verwendet.

Hot Plug

Legt fest, ob die Hot Plug-Unterstützung der Schnittstelle aktiviert ist.

Disabled	Die Hot Plug-Unterstützung der Schnittstelle ist deaktiviert.
Enabled	Die Hot Plug-Unterstützung der Schnittstelle ist aktiviert.

Acoustic Management Configuration

Öffnet das Untermenü zur Einstellung des Geräuschpegel von Festplatten bzw. optischen Laufwerken.

Acoustic Management

Legt fest, ob die Funktionalität zur Einstellung des Geräuschpegel von Festplatten bzw. optischen Laufwerken (Automatic Acoustic Management) verfügbar ist.

Disabled	Automatic Acoustic Management ist nicht verfügbar.
Enabled	Automatic Acoustic Management ist verfügbar.

Acoustic Mode

Legt den Geräuschpegel der Festplatte bzw. des optischen Laufwerks fest. Der Geräuschpegel des Laufwerks wird gesenkt, indem seine Drehzahl verringert wird. Diese Funktion muss vom Laufwerk unterstützt werden.

Wenn die Funktionalität zur Einstellung des Geräuschpegel (*Automatic Acoustic Management*) deaktiviert (Disabled) ist, steht der *Acoustic Mode* nicht zur Verfügung (*Not Available*). Wird die Funktionalität zur Einstellung des Geräuschpegel (*Automatic Acoustic Management*) aktiviert (*Enabled*), aber vom angeschlossenen SATA-Gerät nicht unterstützt, so wird der *Acoustic Mode* automatisch auf *Not supported* gesetzt.

Bypass	Das Laufwerk wird mit seiner voreingestellten Drehzahl betrieben.
Quiet	Das Laufwerk wird mit der kleinsten möglichen Drehzahl betrieben. Das Laufwerk wird mit geringerer Geräuschentwicklung und eingeschränkter Leistung betrieben.
Medium Performance	Das Laufwerk wird mit einer mittleren Drehzahl betrieben. Das Laufwerk wird mit geringerem Geräuschpegel und leicht eingeschränkter Leistung betrieben.
High Performance	Das Laufwerk wird etwas unter der höchsten möglichen Drehzahl betrieben.
Max Performance	Das Laufwerk wird mit der höchsten möglichen Drehzahl betrieben.

Intel TXT Configuration

Öffnet das Untermenü, um Intel® Trusted Execution Technology (TXT) zu konfigurieren.

Intel TXT Support

Aktiviert die Trusted Execution Technology (TXT) Unterstützung. Intel® TXT ist verfügbar, wenn die verwendete CPU Secure Mode Extensions (SMX) unterstützt und Virtualization Technology (VT) sowie VT-d im CPU-Untermenü aktiviert sind.

Intel TXT Support muss deaktiviert sein, bevor das BIOS-Update des Systems eingeleitet wird.

Disabled	TXT ist deaktiviert.
Enabled	TXT ist aktiviert.

USB Configuration

USB Devices

Zeigt die Anzahl der verfügbaren USB-Geräte, USB-Tastaturen, USB-Mäuse und USB-Hubs an.

Legacy USB Support

Legt fest, ob Legacy USB Support verfügbar ist. Diese Funktion sollte immer aktiviert oder auf *Auto* gesetzt sein, damit das Betriebssystem bei Bedarf von einem USB-Gerät gebootet werden kann.

Disabled	Legacy USB Support ist nicht verfügbar. Eine USB-Tastatur oder -Maus kann nur verwendet werden, wenn dies vom Betriebssystem unterstützt wird. Das Booten des Betriebssystems von einem USB-Gerät ist nicht möglich.
Enabled	Legacy USB Support ist verfügbar. Eine USB-Tastatur oder -Maus kann auch dann verwendet werden, wenn das Betriebssystem USB nicht unterstützt. Das Booten des Betriebssystems von einem USB-Gerät ist möglich.
Auto	Legacy USB Support wird deaktiviert, wenn keine USB-Geräte angeschlossen werden.

Legacy USB Support sollte deaktiviert werden, wenn das Betriebssystem USB unterstützt und Sie das Betriebssystem nicht von USB-Geräten booten wollen.

Mass Storage Devices

List of USB Mass Storage Device(s)

Ermöglicht es dem Benutzer, eine bestimmte Geräteemulation zu erzwingen. Bei Einstellung auf *Auto* werden die Geräte entsprechend ihres Medien-Format emuliert. Optische Laufwerke werden als "CD-ROM" und Laufwerke ohne Datenträger nach Laufwerkstyp emuliert.

Auto	Emulation wird abhängig vom USB-Gerät gewählt.
Floppy	USB-Floppy-Emulation erzwingen.
Hard Disk	USB-Festplatten-Emulation erzwingen.
CD-ROM	USB-CD-ROM-Emulation erzwingen.

USB Port Security

Öffnet das Untermenü *USB Port Security* um auf dem Mainboard vorhandene USB-Schnittstellen zu konfigurieren.

USB Port Control

Konfiguriert die Nutzung der USB-Schnittstellen. Deaktivierte USB-Schnittstellen stehen weder während des POST, noch unter dem Betriebssystem zur Verfügung.

Enable all ports	Alle USB-Schnittstellen werden aktiviert.
Disable all ports	Alle USB-Schnittstellen werden deaktiviert.
Enable front and internal ports	Alle USB-Schnittstellen an der Geräterückseite werden deaktiviert.
Enable rear and internal ports	Alle USB-Schnittstellen an der Gerätevorderseite werden deaktiviert.
Enable internal ports only	Alle externen USB-Schnittstellen werden deaktiviert.
Enable used ports	Alle nicht genutzten USB-Schnittstellen werden deaktiviert.

USB Device Control

Für einige Einstellungen, die unter *USB Device Control* vorgenommen wurden stehen hier zusätzliche Optionen zur Verfügung.

Enable all devices	Die unter *USB Port Control* getätigten Einstellungen werden uneingeschränkt verwendet.
Enable Keyboard and Mouse only	An den unter *USB Port Control* aktvierten USB-Schnittstellen können ausschließlich USB-Tastatur und -Maus betrieben werden. Alle Anschlüsse, an denen keine USB-Tastatur oder -Maus angeschlossen ist, werden deaktiviert.
Enable all devices except mass storage devices/Hubs	USB-Schnittstellen, an denen USB-Hubs oder USB-Speichermedien angschlossen sind werden deaktiviert.

System Monitoring

Controller Revision

Zeigt die Version des System Monitoring Controllers an.

Firmware Version

Zeigt die Firmware-Version des System Monitoring Controllers an.

Chassis Type

Zeigt den aktuellen Gehäusetyp an.

TCV Version

Zeigt die TCV-Version (Temperature Characteristics Values) an.

Fan Control

Steuert die Drehzahl der Lüfter. Je nach Systemausbau und den verwendeten Anwendungen kann der voreingestellte Modus geändert werden. Bei Vollausbau des Systems ist der Silent-Modus nicht empfehlenswert.

Enhanced	Die Lüfterdrehzahl wird automatisch erhöht, um die maximale CPU-Leistung zu erreichen.
Auto	Die Lüfterdrehzahl wird automatisch angepasst. Ein Kompromiss zwischen Systemtemperatur und CPU-Leistung.
Disabled	Alle Lüfter werden mit maximaler Drehzahl betrieben.

Onboard Device Configuration

Öffnet das Untermenü um Geräte auf dem System-Board zu konfigurieren. Einige davon sind nur unter bestimmten Voraussetzungen vorhanden.

SCU Device

Legt fest, ob die an der Storage Controller Unit (SCU) angeschlossenen SAS und SATA Geräte zur Verfügung stehen.

Disabled	Die an der SCU ngeschlossenen SAS und SATA Geräte stehen nicht zur Verfügung.
Enabled	Die an der SCU ngeschlossenen SAS und SATA Geräte stehen zur Verfügung.

Audio Configuration

Azalia HD Audio

Ermöglicht die Aktivierung des Onboard Azalia HD (High Definition) Audio-Controllers.

Disabled	Der Onboard-Audio-Controller ist deaktiviert.
Enabled	Der Onboard-Audio-Controller ist aktiviert.

Front Panel Audio

Ermöglicht die Verwendung eines Legacy-Front-Audiosteckers (AC97). Bei dieser Einstellung wird die automatische Belegungsprüfung für Audioanschlüsse nicht unterstützt.

High definition	Für die Verwendung eines High-Definition-Audio-Kabels mit automatischer Belegungserkennung.
Legacy	Für die Verwendung eines Legacy-Audio-Kabels ohne automatische Belegungserkennung.

High Precision Event Timer Configuration

High Precision Timer

Um den Anforderungen von zeitkritischen Applikationen zu genügen, kann das Betriebssystem den High Precision Event Timer verwenden, wenn dieser aktiviert ist. Dieser erweiterte Timer wird auch Multimedia Timer genannt.

Disabled	Der High Precision Event Timer ist deaktiviert.
Enabled	Der High Precision Event Timer ist aktiviert.

LAN 1

Legt fest, ob der LAN 1 Controller verfügbar ist.

Disabled	LAN 1 Controller ist nicht verfügbar.
Enabled	LAN 1 Controller ist verfügbar.

Launch Legacy OpROM

LAN-Controller können als Boot-Geräte genutzt werden, wenn ein geeignetes Option ROM während BIOS POST gestartet wurde. Dieser Parameter legt fest ob ein Option ROM für LAN 1 oder LAN 2 (nur D3118) gestartet werden soll.

Disabled	Startet kein Option ROM.
PXE	Startet das PXE Option ROM, um über PXE booten zu können.

LAN 2 (nur D3118)

Legt fest, ob der LAN 2 Controller verfügbar ist.

Disabled	LAN 2 Controller ist nicht verfügbar.
Enabled	LAN 2Controller ist verfügbar.

Memory Status

In diesem Untermenü können Speichermodule als fehlerhaft markiert werden. Fehlerhafte Speichermodule werden beim Systemneustart nicht mehr verwendet, vorausgesetzt, es ist noch mindestens eine fehlerfreie Bank vorhanden. Der Speicherausbau verringert sich entsprechend.

DIMM-xx

Zeigt den aktuellen Zustand der Speichermodule an.

Failed	Das Speichermodul wird nicht vom System verwendet. Es wurde nach einem Speicherfehler automatisch vom System deaktiviert. Wenn Sie ein defektes Speichermodul ausgetauscht haben, müssen Sie den Eintrag wieder auf *Enabled* setzen.
Disabled	Das Speichermodul wird nicht vom System verwendet. Es wurde manuell deaktiviert.
Enabled	Das System verwendet das Speichermodul.
Empty	Es ist kein Speichermodul bestückt.

Auto BIOS Update

Mit Auto BIOS Update besteht die Möglichkeit auf einem Fujitsu-Server automatisch zu prüfen, ob für das System eine neue BIOS-Version zur Verfügung steht. Für die Aktualisierung ist weder ein Betriebssystem noch ein externes Speichermedium nötig.

Bitte beachten Sie dazu die Nutzungsbedingungen, die Sie als Anlage im BIOS-Handbuch oder im Internet unter "http://support.ts.fujitsu.com/content/tou.asp" finden.

Nutzungsbedingungen

Um die Funktion *Auto BIOS Update* verwenden zu können müssen die Nutzungsbedingungen, die in der Anlage im BIOS-Handbuch oder im Internet unter "http://support.ts.fujitsu.com/content/tou.asp" zu finden sind, akzeptiert werden.

Decline	Die Nutzungsbedingungen wurden nicht akzeptiert. Die Funktion *Auto BIOS Update* kann nicht verwendet werden.
Accept	Die Nutzungsbedingungen wurden akzeptiert. Die Funktion *Auto BIOS Update* kann verwendet werden.

Automatic BIOS update

Legt fest, wie häufig auf dem Fujitsu-Server nach BIOS-Updates gesucht wird. Ist die automatische BIOS-Update-Funktion deaktiviert (*Disabled*), besteht unter *Manually check for update* die Möglichkeit einmalig beim nächsten Systemneustart nach BIOS-Updates zu suchen.

Disabled	Es wird nicht automatisch nach BIOS-Updates gesucht.
Daily	Es wird täglich nach BIOS-Updates gesucht.
Weekly	Es wird einmal wöchentlich nach BIOS-Updates gesucht.
Monthly	Es wird einmal monatlich nach BIOS-Updates gesucht.
Quaterly	Es wird einmal vierteljährlich nach BIOS-Updates gesucht.

Server IP address

Zeigt die IP-Adresse des Fujitsu-Server an, auf dem nach BIOS-Updates gesucht wird.

Silent update

Legt fest, ob das BIOS-Update, falls eine neue BIOS-Version verfügbar ist, ohne Eingabeaufforderung automatisch ausgeführt und nur ein Hinweis angezeigt wird.

Disabled	Es besteht die Möglichkeit das BIOS-Update sofort auszuführen, bei diesem Systemstart zu überspringen oder die neue BIOS-Version zu ignorieren.
Enabled	Das BIOS-Update wir ohne Eingabeaufforderung automatisch ausgeführt.

Manually check for update

Legt fest, ob einmalig während des nächsten Systemneustart nach einem BIOS-Update gesucht wird.

Diese Funktion wird nach erfolgter Suche automatisch wieder auf *Disabled* gesetzt.

Disabled	Beim nächsten Systemneustart wird nicht nach einem BIOS-Update gesucht.
Enabled	Beim nächsten Systemneustart wird einmalig nach einem BIOS-Update gesucht.

Super IO Configuration

Super IO Chip

Zeigt Informationen zum Super IO Chip an.

Serial Port 0 Configuration

Öffnet das Untermenü zur Konfiguration der seriellen Schnittstelle 0 (COMA).

Serial Port

Legt fest, ob die serielle Schnittstelle verfügbar ist.

Disabled	Die serielle Schnittstelle steht nicht zur Verfügung.
Enabled	Die serielle Schnittstelle steht zur Verfügung.

Device Settings

Zeigt die Basis-E/A-Adresse und den Interrupt an, der zum Zugriff auf die parallele Schnittstelle verwendet wird.

AMT Configuration

Öffnet das Untermenü zur Konfiguration der Intel® Active Management Technology.

ME Version

Zeigt die aktuelle AMT/ME-Version an.

ME Subsystem

Legt fest, ob die Intel® AMT/ME (Management Engine) aktiv ist.

Bei Deaktivierung verändern sich möglicherweise die Systemeigenschaften.

Disabled	Intel® AMT/ME ist deaktiviert.
Enabled	Intel® AMT/ME ist aktiviert.

Unconfigure AMT/ME

Wenn diese Option aktiviert wird, erscheint beim nächsten Neustart eine Abfrage der MEBx (Management Engine BIOS eXtension), ob die AMT/ME-Konfiguration auf die Standardwerte zurückgesetzt werden soll.

Disabled	AMT/ME-Konfiguration nicht ändern.
Enabled	Zurücksetzen der AMT/ME-Konfiguration einleiten. Die Option wird anschließend automatisch auf *Disabled* zurückgesetzt.

Execute MEBx

Legt fest, ob das MEBx (Management Engine BIOS eXtension) Setup während des Neustartes aufgerufen werden kann.

Disabled	Das MEBx-Setup kann während des POST nicht aufgerufen werden.
Enabled	Das MEBx-Setup kann während des POST aufgerufen werden. Die Meldung Strg + P zum Öffnen des MEBx-Setup wird während des POST angezeigt.

Serial Port Console Redirection

In diesem Untermenü können die Parameter für die Terminal-Kommunikation via Serial Port Console Redirection angezeigt und eingestellt werden. Einige Parameter stehen nur unter bestimmten Voraussetzungen zur Verfügung.

Console Redirection Settings (für COM0 und COM1)

Bestimmt den Datenaustauschablauf von Host- und Remotesystem über COM0- und COM1-Port (iAMT/SOL (Serial overLAN)).

Beide Systeme benötigen identische oder kompatible Einstellungen.

Terminal Type

Legt den Terminal-Typ fest.

Zugelassene Werte: VT100, VT100+, VT-UTF8, ANSI

Der zugewiesene Terminal-Typ wird für die Übertragung der Daten an den Host verwendet.

Bits per Second

Gibt die Übertragungsrate für die Kommunikation mit dem Host an.

Zugelassene Werte: 9600, 19200, 38400, 57600, 115200

Die Daten werden mit der eingestellten Übertragungsrate an den Host übermittelt.

Data Bits

Gibt die Anzahl an Datenbits an, die für die Kommunikation mit dem Host verwendet werden.

7	Sieben Datenbits werden für die Kommunikation verwendet.
8	Acht Datenbits werden für die Kommunikation verwendet.

Parity

Gibt die Verwendung von Paritätsbits für die Kommunikation mit dem Host an. Paritätsbits werden zur Fehlererkennung verwendet.

None	Es werden keine Paritätsbits verwendet. Keine Fehlererkennung möglich.
Even	Paritätsbit ist 0, wenn die Anzahl von Einsen im Datenbit eine gerade Zahl annimmt.
Odd	Paritätsbit ist 0, wenn die Anzahl von Einsen im Datenbit eine ungerade Zahl annimmt.
Mark	Paritätsbit ist immer 1.
Space	Paritätsbit ist immer 0.

Stop Bits

Gibt die Anzahl der verwendeten Stoppbits an, die das Ende eines seriellen Datenpakets angeben.

1	Es wird ein Stoppbit verwendet.
2	Es werden zwei Stoppbits verwendet.

Flow Control

Diese Einstellung bestimmt die Transfersteuerung über das Interface.

None	Das Interface wird ohne Transfersteuerung bedient.
Hardware CTS/RTS	Die Transfersteuerung wird von der Hardware übernommen. Dieser Modus muss auch vom Kabel unterstützt werden.

VT-UTF8 Combo Key Support

Gibt an, ob die VT-UTF8 Combination key-Unterstützung für ANSI/VT100 Terminals zur Verfügung steht.

Disabled	Die VT-UTF8 Combination key-Unterstützung ist nicht verfügbar.
Enabled	Die VT-UTF8 Combination key-Unterstützung ist verfügbar.

Recorder Mode

Gibt an, ob nur Text gesendet wird. Dies dient der Erfassung von Terminal-Daten.

Disabled	Recorder Mode ist nicht verfügbar.
Enabled	Recorder Mode ist verfügbar

Resolution 100x31

Gibt an, ob eine erweiterte Terminal-Auflösung verfügbar ist.

Disabled	Erweiterte Terminal-Auflösung ist nicht verfügbar.
Enabled	Erweiterte Terminal-Auflösung ist verfügbar.

Legacy OS Redirection Resolution

Gibt die Anzahl von Zeilen und Spalten für die Lecacy OS Redirection an.

80x24	Auflösung 80x24 wird verwendet.
80x25	Auflösung 80x25 wird verwendet.

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

Microsoft Windows Emergency Management Services (EMS) ermöglicht die Remote-Verwaltung eines Windows Server Betriebssystems.

Console Redirection (für Out of Band Management / EMS)

Gibt an, ob eine serielle Schnittstelle für Out-of-Band-Management / Windows Emergency Management Services (EMS) verfügbar ist.

Disabled	EMS ist nicht verfügbar.
Enabled	EMS ist verfügbar.

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

Out-of-Band Mgmt Port

Weist eine serielle Schnittstelle für Out-of-Band-Management zu.

COM0 (Disabled)	Port COM0 wird für Out-of-Band-Management verwendet
COM1 (Pci Dev0, Func0) (Disabled)	Port COM1 wird für Out-of-Band-Management verwendet.

Terminal Type

Legt den Terminal-Typ fest.

Zugelassene Werte: VT100, VT100+, VT-UTF8, ANSI

Der zugewiesene Terminal-Typ wird für die Übertragung der Daten an den Host verwendet.

Bits per Second

Gibt die Übertragungsrate für die Kommunikation mit dem Host an.

Zugelassene Werte: 9600, 19200, 38400, 57600, 115200

Die Daten werden mit der eingestellten Übertragungsrate an den Host übermittelt.

Flow Control

Diese Einstellung bestimmt die Transfersteuerung über das Interface.

None	Das Interface wird ohne Transfersteuerung bedient.
Hardware CTS/RTS	Die Transfersteuerung wird von der Hardware übernommen. Dieser Modus muss auch vom Kabel unterstützt werden.
Software Xon/Xoff	Die Interface-Transfersteuerung wird von der Software übernommen.

Data Bits

Gibt die Anzahl an Datenbits an, die für die Kommunikation mit dem Host verwendet werden.

Parity

Gibt die Verwendung von Paritätsbits für die Kommunikation mit dem Host an.

Stop Bits

Gibt die Anzahl der verwendeten Stoppbits an, die das Ende eines seriellen Datenpakets angeben.

Network Stack

Legt fest, ob der UEFI Network Stack zum Netzwerkzugriff unter UEFI zur Verfügung steht. Wird der UEFI Network Stack Disabled ist z. B. keine UEFI Installation über PXE möglich.

Disabled	Der UEFI Network Stack steht nicht zur Verfügung.
Enabled	Der UEFI Network Stack steht zur Verfügung.

Ipv4 PXE Support

Legt fest, ob der PXE UEFI Boot via Ipv4 zur Installation von Betriebssysstemen im UEFI Modus zur Verfügung steht.

Disabled	Der PXE UEFI Boot via Ipv4 steht nicht zur Verfügung.
Enabled	Der PXE UEFI Boot via Ipv4 steht zur Verfügung.

Ipv6 PXE Support

Legt fest, ob der PXE UEFI Boot via Ipv6 zur Installation von Betriebssysstemen im UEFI Modus zur Verfügung steht.

Disabled	Der PXE UEFI Boot via Ipv6 steht nicht zur Verfügung.
Enabled	Der PXE UEFI Boot via Ipv6 steht zur Verfügung.

PXE boot wait time

Legt die Wartezeit fest, in der der PXE Boot durch Drücken der Taste ESC abgebrochen werden kann.

[0..5] sec	Wartezeit zum Abbruch des PXE Boot.

CPU Status (nur D3118)

Dieses Untermenü zeigt den aktuellen Zustand der CPUs in den Sockeln an.

CPU n

Gibt an, ob der Prozessor genutzt werden kann. Deaktivieren Sie einen Prozessor nur dann, wenn eine interne Fehlfunktion aufgetreten ist. Die Fehlfunktion wird in der Error Log eingetragen, die Sie sich mit den Programmen SCU (ServerConfiguration Utility), RemoteView oder ServerView anzeigen lassen können.

Failed	Das Betriebssystem kann den Prozessor nicht verwenden. Der Prozessor wurde nach einer internen Fehlfunktion automatisch deaktiviert.
Disabled	Das Betriebssystem kann den Prozessor nicht verwenden. Der Prozessor wurde manuell deaktiviert.
Enabled	Das Betriebssystem kann den Prozessor verwenden.
Empty	Es ist kein Prozessor eingebaut.

PCI Status

Dieses Untermenü zeigt den aktuellen Zustand der Erweiterungskarten in den Steckplätzen an.

PCI Slot n

Zeigt den aktuellen Zustand der Erweiterungskarten in diesem Steckplatz an.

Failed	Für diesen Steckplatz wurde ein Fehler erkannt. Die Erweiterungskarte in diesem Steckplatz hat möglicherweise ein Problem.
Enabled	Für diesen Steckplatz wurden keine Fehler gemeldet. Die Erweiterungskarte in diesem Steckplatz kann uneingeschränkt verwendet werden.
Empty	In diesem Steckplatz steckt keine Erweiterungskarte.

Option ROM Configuration

Ruft das Untermenü *Option ROM Configuration* auf.

Launch Slot n OpROM

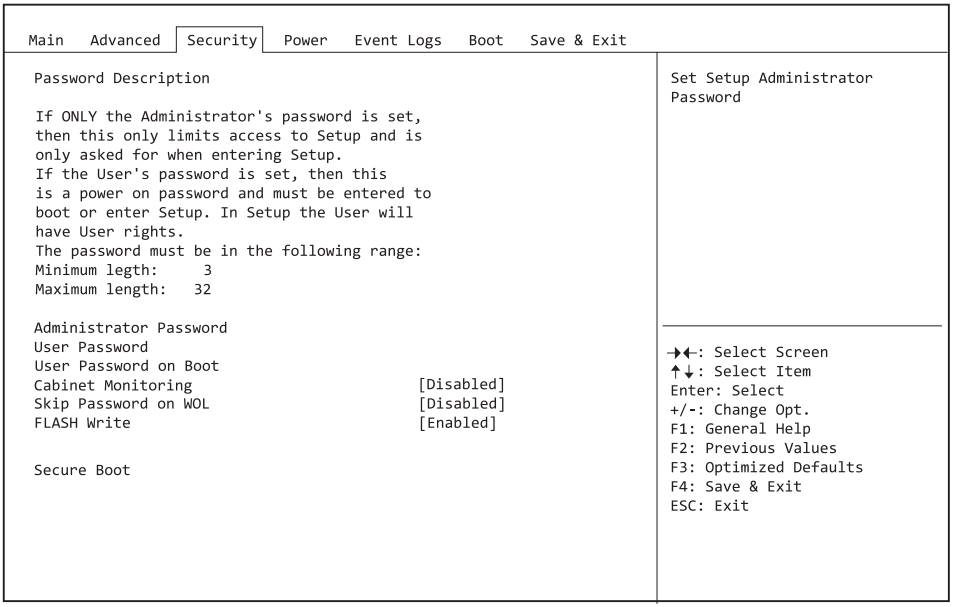
Legt fest, ob Option ROMs für Erweiterungskarten, die in diesem Steckplatz gesteckt sind, gestartet werden sollen.

Disabled	Startet keine Option ROMs für Erweiterungskarten in diesem Steckplatz.
Enabled	Startet Option ROMs für Erweiterungskarten in diesem Steckplatz.

Security Menu - Sicherheitsfunktionen

Das Menü *Security* bietet Ihnen verschiedene Möglichkeiten, Ihre persönlichen Daten gegen unbefugten Zugriff zu schützen. Sie können diese Möglichkeiten auch sinnvoll kombinieren, um einen optimalen Schutz Ihres Systems zu erreichen.

Die folgenden Sicherheitseinstellungen können in diesem Menü eingestellt werden. Einige davon stehen nur unter bestimmten Voraussetzungen zur Verfügung.



Password Description

Weder ein Administrator- noch ein User-Passwort wurde vergeben

Das Öffnen des BIOS-Setup und das Booten des Systems sind uneingeschränkt möglich.

Nur das Administrator-Passwort wurde vergeben

Wenn NUR ein Administrator-Passwort vergeben wurde, ist nur das BIOS-Setup geschützt. Das Booten des Systems ist uneingeschränkt möglich. Beim Zugriff auf das BIOS-Setup mit einem Administrator-Passwort wird Ihnen die Zugriffsebene Administrator zugewiesen und Sie besitzen uneingeschränkten Zugang zum BIOS-Setup. Beim Zugriff auf das BIOS-Setup ohne Passwort wird der Zugriff auf das BIOS-Setup eingeschränkt, da Ihnen nur die Zugriffsebene User zugewiesen wird.

Administrator- UND User-Passwort wurden vergeben

Wenn Administrator- und User-Passwort vergeben wurden, hängt die Berechtigungsstufe im BIOS-Setup vom eingegebenen Passwort ab. Beim Zugriff auf das BIOS-Setup mit Administrator-Passwort ist der Zugriff auf das BIOS-Setup uneingeschränkt möglich, die Eingabe des User-Passworts führt zu eingeschränktem Zugriff. Das Booten des System ist sowohl mit Administrator- als auch mit User-Passwort möglich.

Beim Löschen des Administrator-Passworts wird das User-Passwort ebenfalls gelöscht.

Nach dreimaliger Falscheingabe des Passworts hält das System an. Schalten Sie in diesem Fall das System aus und wieder ein und geben Sie das korrekte Passwort ein.

Administrator Password

Wenn Sie die Eingabetaste drücken, öffnet sich ein Fenster, in dem Sie das Adminstrator-Passwort vergeben können. Geben Sie eine Zeichenfolge ein, um das Passwort zu definieren. Wenn Sie ein leeres Passwort-Feld bestätigen, wird das Passwort gelöscht.

Um das komplette BIOS-Setup aufzurufen, benötigen Sie die Zugriffsebene Administrator. Wenn ein Administrator-Passwort vergeben ist, ermöglicht das User-Passwort lediglich einen stark eingeschränkten Zugriff auf das BIOS-Setup.

User Password

Wenn Sie die Eingabetaste drücken, öffnet sich ein Fenster, in dem Sie das User-Passwort vergeben können. Geben Sie eine Zeichenfolge ein, um das Passwort zu definieren. Mit dem User-Passwort können Sie den unautorisierten Zugang zu Ihrem System verhindern.

Um das User-Passwort vergeben zu können muss bereits ein Administrator-Passwort vergeben sein.

User Password on Boot

Legt fest, ob das User-Passwort vor dem Bootvorgang eingegeben werden muss.

On Every Boot	Die Eingabe des User-Passwort ist vor jedem Bootvorgang erforderlich.
Disabled	Das System startet, ohne dass die Eingabe des User-Passwort erforderlich ist.

Wenn das Adminstrator- und das User-Passwort vergeben wurden und für diesen Punkt die Einstellung *Disabled* gewählt wurde, genügt zum Zugriff auf das BIOS-Setup mit der Zugriffsebene USER das Drücken der Eingabetaste. Das User-Passwort muss in diesem Fall nicht eingegeben werden.

Cabinet Monitoring

Legt fest, ob ein Öffnen des Gehäuses überwacht werden soll.

Disabled	Das System arbeitet normal weiter, auch wenn das Gehäuse geöffnet wurde.
Enabled	Sollte das Gehäuse geöffnet gewesen sein, wird der Boot-Prozess solange unterbrochen bis das BIOS-Setup aufgerufen wurde. Sollte das BIOS-Setup mit einem Passwort geschützt sein muss dieses eingegeben werden. Ein SMBIOS Eventlog-Eintrag wird generiert.

Skip Password on WOL

Legt fest, ob das User-Passwort beim Systemstart über Wake on LAN übergangen wird oder eingegeben werden muss.

Disabled	Das User-Passwort muss beim Systemstart über die Tastatur eingegeben werden.
Enabled	Das User-Passwort ist beim Systemstart mit Wake On LAN deaktiviert.

FLASH Write

Versieht das System-BIOS mit einem Schreibschutz.

Disabled	Das System-BIOS kann nicht beschrieben werden. Ein Flash-BIOS-Update ist nicht möglich.
Enabled	Das System-BIOS kann beschrieben werden. Ein Flash-BIOS-Update ist möglich.

Smartcard SystemLock

Mit SystemLock (Smartcard Pre-boot Authentication - PBA) kann der PC nur mit initialisierter Smartcard und persönlicher Geheimnummer (PIN) gestartet werden. Smartcard und PIN werden bereits beim Systemstart im BIOS geprüft, also noch vor dem Betriebssystemstart.

Zur Initialisierung der Smartcard(s) wird die OS Applikation SystemLock Manager verwendet. Systeme ohne den Menüpunkt *Smart Card System Lock* unterstützen die Funktion SystemLock nicht.

Nur mit einer Admin-Smartcard können Einstellungen im Menü *Smartcard SystemLock* geändert werden.

Wenn die Smartcard defekt oder nicht verfügbar ist, kann sich der Anwender für einen Bootvorgang entweder beim lokalen Administrator oder beim Fujitsu Service Desk freischalten lassen.

Uninstall SystemLock

Deinstalliert die Funktion *Smartcard Security*.

Eine erneute Installation von SystemLock erfordert die Re-Initialisierung Ihrer Smartcards!

No	Smartcard Security wird nicht deinstalliert.
Yes	Smartcard Security wird während des nächsten Boot-Vorgangs deaktiviert.

Single Sign On

Mit der Funktion *Single Sign On* kann das BIOS während der Anmeldung an das Betriebssystem mit einer anderen Anwendung kommunizieren, um Smartcard-Zugriffsrechte zu ermitteln.

Disabled	Single Sign On ist nicht verfügbar.
Enabled	Single Sign On ist verfügbar.

Smartcard & PIN

Legt fest, ob eine autorisierte Smartcard für den Zugriff auf das System erforderlich ist.

Always Required	Für den Zugriff auf das System ist eine autorisierte Smartcard erforderlich.
Ignore on WOL	Wenn die Funktion Wakeup On LAN aktiviert ist, wird die Funktion Smartcard Security umgangen.

Unblock Smartcard

Zur Vergabe einer neuen PIN, wenn die PIN nicht bekannt oder die Smartcard gesperrt ist.

Die Smartcard wird durch die dreimalige, falsche Eingabe der PIN gesperrt und durch die zehnmalige, falsche Eingabe der PUK unwiderruflich gesperrt. Bitte beachten Sie, dass bei einer neuen Smartcard die PIN und PUK im Auslieferzustand immer 12345678 ist. Diese PIN / PUK muss aus Sicherheitsgründen geändert werden.

Prohibited	Es kann keine neue PIN vergeben werden.
Allowed	Es kann eine neue PIN vergeben werden.

Secure Boot

Öffnet das Untermenü um Secure Boot zu konfigurieren.

Platform Mode

Zeigt an, ob sich das System im User- oder Setup-Mode befindet.

User	Im User-Mode ist der Platform Key (PK) installiert. Secure Boot kann über den Menüpunkt *Secure Boot Control* aktiviert bzw. deaktiviert werden.
Setup	Im Setup-Mode ist der Platform Key (PK) nicht installiert. Secure Boot ist deaktiviert und kann auch nicht über den Menüpunkt *Secure Boot Control* aktiviert werden.

Secure Boot

Secure Boot Zeigt an, ob die Funktion Secure Boot aktiv ist.

Disabled	Secure Boot ist nicht aktiv.
Enabled	Secure Boot ist aktiv.

Secure Boot Control

Legt fest, ob das Starten von nicht signierten Bootloadern / UEFI-OpROMs erlaubt wird.

Die zugehörigen Signaturen sind im BIOS hinterlegt oder können im Untermenü *Key Management* nachgeladen werden.

Disabled	Alle Bootloader / OpROMs (Legacy / UEFI) können ausgeführt werden.
Enabled	Ausschließlich das Starten signierter Booloader / UEFI-OpROMs wird erlaubt.

Secure Boot Mode

Legt fest, ob das Untermenü Key Managment zur Verfügung steht.

Standard	Das Untermenü *Key Management* steht nicht zur Verfügung.
Custom	Das Untermenü *Key Management* steht zur Verfügung.

Key Management

Untermenü zum Löschen, Ändern und Hinzufügen der für Secure Boot notwendigen Schlüssel und Signaturdatenbanken.

Ohne installierten Platform Key (PK) befindet sich das System im Setup-Mode (Secure Boot ist deaktiviert). Sobald der PK installiert ist befindet sich das System im User-Mode (Secure Boot kann aktiviert werden).

Factory Default Key Provisioning

Befindet sich das System im Setup-Mode (es ist kein Public Key installiert) besteht die Möglichkeit die Standard-Secure-Boot-Schlüssel und Signaturdatenbanken zu installieren.

Disabled	Die vorhandenen Secure-Boot-Schlüssel und Signaturdatenbanken bleiben unverändert.
Enabled	Falls die Signaturdatenbanken PK, KEK, DB, DBX nicht vorhanden sind werden die Standard-Secure-Boot-Schlüssel und Signaturdatenbanken nach dem Neustart des Systems installiert.

Delete All Secure Boot Variables

Versetzt das System in den Setup-Mode (Secure Boot wird deaktiviert). Alle im System befindlichen Schlüssel und Signaturdatenbanken (PK, KEK, DB, DBX) werden gelöscht.

Install All Factory Default Keys

Alle im System befindlichen Schlüssel und Signaturdatenbanken (PK, KEK, DB, DBX) werden auf die Standardwerte zurückgesetzt. Dieser Menüpunkt steht nur bei gelöschtem PK zur Verfügung.

Platform Key (PK)

Zeigt den aktuellen Status des Platform Key (PK) an.

Installed	Der PK ist installiert. Das System befindet sich im User-Mode.
Not Installed	Der PK ist nicht installiert. Das System befindet sich im Setup-Mode.

Set new PK

Setzt den Platform Key (PK). Nach der Auswahl des Laufwerks muss die entsprechende Datei im Browser ausgewählt werden.

Delete PK

Löscht den Platform Key (PK), wodurch das System in den Setup-Mode versetzt und Secure Boot deaktiviert wird.

Key Exchange Key Database (KEK)

Zeigt den aktuellen Status der Key Exchange Key Database (KEK) an.

Installed	Die KEK Database ist installiert.
Not Installed	Die KEK Database ist nicht installiert.

Set new KEK

Setzt die Key Exchange Key Database (KEK). Nach der Auswahl des Laufwerks muss die entsprechende Datei im Browser ausgewählt werden.

Delete KEK

Löscht die Key Exchange Key Database (KEK).

Append Var to KEK

Ergänzt einen Eintrag zur Key Exchange Key Database (KEK). Nach der Auswahl des Laufwerks muss die entsprechende Datei im Browser ausgewählt werden.

Authorized Signature Database (DB)

Zeigt den aktuellen Status der Authorized Signature Database (DB) an.

Installed	Die DB ist installiert.
Not Installed	Die DB ist nicht installiert.

Set new DB

Setzt die Authorized Signature Database (DB). Nach der Auswahl des Laufwerks muss die entsprechende Datei im Browser ausgewählt werden.

Delete DB

Löscht die Authorized Signature Database (DB).

Append Var to DB

Ergänzt einen Eintrag zur Authorized Signature Database (DB). Nach der Auswahl des Laufwerks muss die entsprechende Datei im Browser ausgewählt werden.

Forbidden Signature Database (DBX)

Zeigt den aktuellen Status der Forbidden Signature Database (DBX) an.

Installed	Die DBX ist installiert.
Not Installed	Die DBX ist nicht installiert.

Set new DBX

Setzt die Forbidden Signature Database (DBX). Nach der Auswahl des Laufwerks muss die entsprechende Datei im Browser ausgewählt werden.

Delete DBX

Löscht die Forbidden Signature Database (DBX).

Append Var to DBX

Ergänzt einen Eintrag zur Forbidden Signature Database (DBX). Nach der Auswahl des Laufwerks muss die entsprechende Datei im Browser ausgewählt werden.

Save Secure Boot Keys

Sichert die Secure-Boot-Schlüssel und Schlüsseldatenbanken auf dem ausgewählten Laufwerk.

Power Menu – Energiesparfunktionen

Beispiel für das Menu *Power*.

Power Settings

Power On Source

Legt fest, ob die Einschaltquellen für das System über das BIOS oder über ein ACPI-Betriebssystem verwaltet werden.

BIOS Controlled	Die Einschaltquellen werden über das BIOS verwaltet.
ACPI Controlled	Die Einschaltquellen werden über das ACPI-Betriebssystem verwaltet.

Low Power Soft Off

Verringert den Energieverbrauch bei ausgeschaltetem System.

Wenn Low Power Soft Off aktiviert ist, kann das System nur mit der Netztaste am Gehäuse eingeschaltet werden. Das Gerät kann nicht mit der Netztaste einer USB-Tastatur oder einem Wake-on-LAN-Signal eingeschaltet werden.

Disabled Low Power Soft Off ist nicht aktiv.

Enabled Low Power Soft Off ist aktiv.

Power Failure Recovery – Systemzustand nach einem Stromausfall

Legt fest, wie sich das System bei einem durch Stromausfall bedingten Neustart verhält.

Always Off Das System schaltet sich kurz ein, prüft seinen aktuellen Zustand (Initialisierung) und schaltet sich wieder ab.

Always On Das System schaltet sich ein.

Previous State Das System schaltet sich kurz ein, prüft seinen aktuellen Zustand und kehrt in den Zustand zurück, in dem es sich vor dem Stromausfall befand (ON oder OFF).

Disabled Das System schaltet sich nicht ein.

Hibernate like Soft Off

Um auch im Ruhezustand (S4) den Energieverbrauch zu verringern wird das System beim Ausschalten stattdessen in den Low Power Soft Off- oder Zero-Watt-Mode gebracht (S5). Der Energieverbrauch sinkt aber nur, falls Low Power Soft Off oder Zero-Watt-Mode aktiviert sind.

Disabled Das System wird in den Ruhezustand (S4) gebracht.

Enabled Das System wird statt in den Ruhezustand (S4) in den Low Power Soft Off- oder Zero-Watt-Mode gebracht (S5).

USB At Power-off

Aktiviert/deaktiviert die Stromversorgung an den USB-Schnittstellen. Diese Option steht nur zur Verfügung, falls Low Power Soft Off oder Zero-Watt-Mode deaktviert sind.

Always off Die USB-Schnittstellen werden nach dem Ausschalten des Systems nicht mehr mit Spannung versorgt.

Always on Die USB-Schnittstellen werden nach dem Ausschalten des Systems weiterhin mit Spannung versorgt.

Wake-Up Resources

Dieses Untermenü steht nur zur Verfügung, wenn weder *Zero-Watt Mode* noch *Low Power Soft Off* aktiviert sind.

LAN

Legt fest, ob das System über einen LAN-Controller (auf dem System-Board oder Erweiterungskarte) eingeschaltet werden kann.

Enabled	Das System kann über einen LAN-Controller eingeschaltet werden.
Disabled	Das System kann nicht über einen LAN-Controller eingeschaltet werden.

Wake On LAN Boot

Legt das Verhalten beim Einschalten des Systems über Netzwerksignale fest.

Boot Sequence	Nach dem Einschalten über LAN startet das System gemäß der im Boot Menü vorgegebenen Gerätefolge.
Force LAN Boot	Nach dem Einschalten über LAN wird das System über LAN remote gestartet.

Wake Up Timer

Hier kann der Zeitpunkt zu dem das System eingeschaltet werden soll, festgelegt werden.

Disabled	Wake Up Timer ist nicht aktiviert.
Enabled	Wake Up Timer ist aktiviert. Das System wird zur angegebenen Zeit eingeschaltet.

Hour

Legt die Stunde des Einschaltzeitpunkts fest.

Minute

Legt die Minute des Einschaltzeitpunkts fest.

Second

Legt die Sekunde des Einschaltzeitpunkts fest.

Wake Up Mode

Legt fest, ob das System täglich oder nur einmal monatlich zum festgelegten Zeitpunkt eingeschaltet werden soll.

Daily	Das System wird täglich zum festegelegten Zeitpunkt eingeschaltet.
Weekly	Das System wird an den ausgewählten Wochentagen zum festgelegten Zeitpunkt eingeschaltet.
Monthly	Das System wird einmal monatlich zum festgelegten Zeitpunkt eingeschaltet.

Wake Up Day

Legen Sie den Monatstag fest, an dem das System eingeschaltet werden soll. Zulässige Werte sind 1..31.

USB Keyboard

Legt fest, ob das System über die Netztaste einer USB-Tastatur eingeschaltet werden kann, wenn die Tastatur diese Funktion unterstützt.

Das Einschalten des Systems über eine USB-Tastatur ist nur verfügbar, wenn *USB At Power-Off* auf *Always On* eingestellt ist.

Disabled	Die Netztaste der USB-Tastatur ist deaktiviert.
Enabled	Die Netztaste der USB-Tastatur ist aktiviert.

Event Logs – Konfiguration und Anzeige der Event Log

Beispiel für das Menu *Event Logs*.

Change Smbios Event Log Settings

Smbios Event Log

Legt fest, ob die Smbios-Event-Log aktiviert ist.

Disabled	Die Smbios-Event-Log ist deaktiviert.
Enabled	Die Smbios-Event-Log ist aktiviert.

Erase Event Log

Legt fest, ob die Smbios-Event-Log gelöscht werden soll.

No	Die Smbios-Event-Log wird nicht gelöscht.
Yes, Next reset	Die Smbios-Event-Log wird beim nächsten Neustart einmalig gelöscht. Danach wird diese Option automatisch wieder auf *No* zurückgesetzt.
Yes, Every reset	Die Smbios-Event-Log wird bei jedem Neustart gelöscht.

When Log is full

Legt die Vorgehensweise für den Fall fest, dass die Smbios-Event-Log voll ist.

Do Nothing	Wenn die Smbios-Event-Log vollständig belegt ist, werden keine weiteren Einträge hinzugefügt. Die Smbios-Event-Log muss zuerst gelöscht werden, bevor neue Einträge hinzugefügt werden können.
Erase Immediately	Wenn die Smbios-Event-Log vollständig belegt ist, wird diese sofort zurückgesetzt. Alle vorhandenen Einträge werden gelöscht!

Log System Boot Event

Gibt an, ob jedes Booten des Systems in der Smbios-Event-Log protokolliert wird.

Disabled	System-Boots werden nicht im Smbios-Event-Log aufgezeichnet.
Enabled	Alle System-Boots werden im Smbios-Event-Log aufgezeichnet.

MECI

Mutiple Event Count Increment: Die Anzahl der Doppel-Events die stattfinden muss, bevor der Multiple-Event Zähler einschließlich zugehörigen Logeintrag aktualisiert wird. Der Wertebereich liegt zwischen 1 und 255.

METW

Mutiple Event Time Window: Die Anzahl der Minuten die zwischen Doppel-Event-Logs vergehen muss, die einen Multiple-Event Zähler verwenden. Der Wertebereich liegt zwischen 0 und 99 Minuten.

Log OEM Codes

Aktivieren oder Deaktivieren der Logfunktion von EFI Status Codes als OEM Codes (falls nicht bereits legacy-konvertiert).

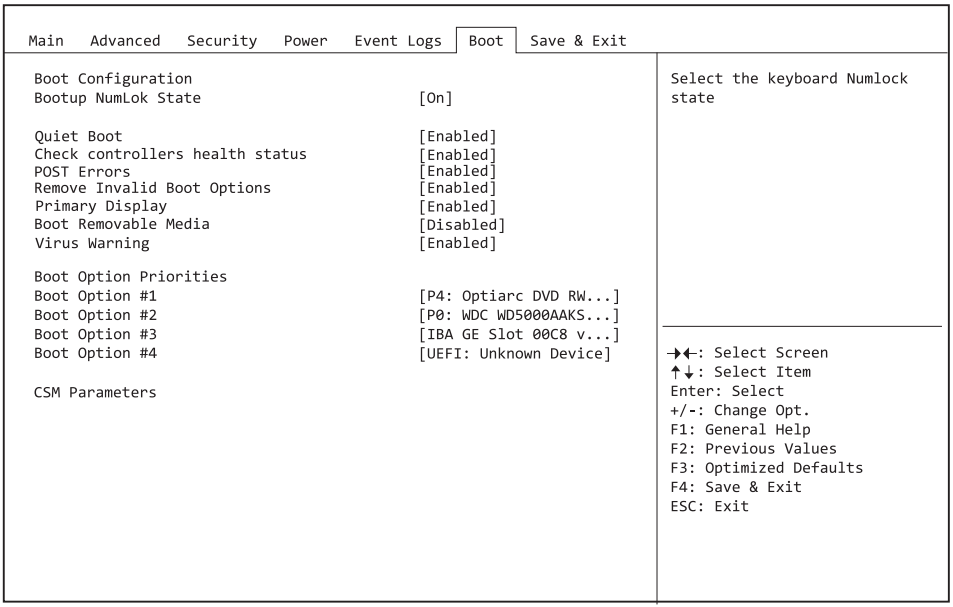
Convert OEM Codes

Aktivieren oder Deaktivieren der Konvertierung von EFI Status Codes zu Standard Smbios Typen (evtl. sind nicht alle übersetzt).

View Smbios Event Log

Öffnet das Untermenü um alle vorhandenen Smbios Event Log Einträge anzuzeigen.

Boot Menu – Systemstart



Hier kann die Reihenfolge der Laufwerke, von denen gebootet werden soll, festgelegt werden.

Bis zu acht Laufwerke (auch z. B. USB-Schnittstellen) können hier gelistet sein.

Boot Configuration

Bootup NumLock State

Hier wird die Einstellung der NumLock-Funktion nach dem Systemstart vorgegeben. Über NumLock wird die Funktionsweise des Zahlenblock gesteuert.

On	NumLock ist aktiviert, der Zahlenblock kann verwendet werden.
Off	NumLock ist deaktiviert, die Zahlenblocktasten können zur Cursorsteuerung verwendet werden.

Die Num-Kontrollleuchte auf der Tastatur zeigt den aktuellen Bootup NumLock-Zustand an. Mit der Num -Taste auf der Tastatur kann zwischen ON und OFF umgeschaltet werden.

Quiet Boot

Auf dem Bildschirm wird an Stelle der POST-Startinformationen das Boot-Logo angezeigt.

Enabled	Das Boot-Logo wird angezeigt.
Disabled	Die POST-Startinformationen werden auf dem Bildschirm angezeigt.

Check Controller Health Status

Wenn ein UEFI-Treiber-Option-ROM eines PCI-Express-Geräts Controller Health unterstützt, kann die UEFI-Firmware das UEFI-Treiber-Option-ROM über den Zustand der Geräte abfragen, die sie verwaltet.

Disabled	Der Controller Health Status wird von der UEFI FW nicht abgefragt.
Enabled	Die UEFI FW fragt den Controller Health Status ab.

POST Errors

Legt fest, ob der Bootvorgang des System abgebrochen und das System nach einem erkannten Fehler angehalten wird.

Disabled	Der Bootvorgang des Systems wird nicht abgebrochen. Der Fehler wird ignoriert, soweit dies möglich ist.
Enabled	Wenn während des POST ein Fehler erkannt wird, wird der Bootvorgang abgebrochen und das System angehalten.

Remove Invalid Boot Options

Gibt an, ob UEFI-Boot-Einstellungen für Geräte, die nicht mehr an das System angeschlossen sind, aus der Boot-Optionen-Prioritätenliste entfernt werden.

Disabled	UEFI-Boot-Einstellungen werden nicht aus der Boot-Optionen-Prioritätenliste entfernt.
Enabled	UEFI-Boot-Einstellungen werden aus der Boot-Optionen-Prioritätenliste entfernt.

Primary Display

Legt fest, welche Grafik-Steckkarte während des Einschalt-Selbsttests (POST) als Bildquelle dient.

Slot n	Wählen Sie den Steckplatz der Grafik-Steckkarte, die während des POST als Bildquelle dienen soll.

Boot Removable Media

Gibt an, ob ein Booten über Wechseldatenträger, wie z. B. USB-Sticks, unterstützt wird.

Disabled	Das Booten über Wechseldatenträger ist deaktiviert.
Enabled	Das Booten über Wechseldatenträger ist aktiviert.

Virus Warning

Überprüft die Boot-Sektoren der Festplatten auf Änderungen seit dem letzten Systemstart. Wenn die Boot-Sektoren ohne ersichtlichen Grund geändert wurden, sollte ein geeignetes Erkennungsprogramm für Computer-Viren durchgeführt werden.

Disabled	Die Boot-Sektoren werden nicht geprüft.
Enabled	Wenn der Boot-Sektor seit dem letzten Systemstart geändert wurde (z. B. neues Betriebssystem oder Virus-Angriff), wird ein Warnhinweis angezeigt. Der Warnhinweis verbleibt auf dem Bildschirm, bis Sie die Änderungen bestätigen, indem Sie in das BIOS-Setup gehen und diesen Punkt auf *Confirm* stellen oder die Funktion deaktivieren.
Confirm	Eine erforderliche Änderung an einem Bootsektor bestätigen (z. B. neues Betriebssystem).

Boot Option Priorities

Zeigt die aktuelle Boot-Reihenfolge an.

- ► Um das Gerät auszuwählen, dessen Boot-Reihenfolge Sie ändern möchten, verwenden Sie die Cursor-Tasten ↑ oder ↓.
- ► Um die Priorität für das gewählte Gerät zu erhöhen, drücken Sie die Taste + . Um die Priorität zu verringern, drücken Sie die Taste - .
- ► Um das gewählte Gerät aus der Boot-Reihenfolge zu entfernen, drücken Sie die Taste Enter und wählen Sie *Disabled* (Deaktiviert). Wenn ein oder mehr Geräte deaktiviert wurden, wird der letzte Eintrag der Boot-Reihenfolge auf *Disabled* gesetzt.

CSM Configuration

Öffnet das Untermenü um das Compatibility Support Module (CSM) zu konfigurieren.

Dieses Untermenü ist nur vorhanden, wenn *Secure Boot Control* unter *Setup –> Secure Boot Configuration* deaktiviert ist.

Launch CSM

Legt fest, ob das Compatibility Support Module (CSM) ausgeführt wird. Ein Legacy-Betriebssystem kann nur gestartet werden wenn das CSM geladen wurde.

Enabled	Das CSM wird ausgeführt, so dass ein Legacy- oder UEFI-Betriebssystem gestartet werden kann.
Disabled	Das CSM wird nicht ausgeführt, so dass nur ein UEFI-Betriebssysstem gestartet werden kann.

Boot option filter

Legt fest, von welchen Laufwerken gebootet werden kann.

UEFI and Legacy	Es kann sowohl von Laufwerken mit UEFI- als auch mit Legacy-OS gebootet werden.
Legacy only	Es kann nur von Laufwerken mit Legacy-OS gebootet werden.
UEFI only	Es kann nur von Laufwerken mit UEFI-OS gebootet werden.

Launch PXE OpROM Policy

Legt fest, welcher PXE Option-ROM gestartet wird. Für den PXE boot stehen sowohl der normale (Legacy) PXE boot sowie auch ein UEFI PXE boot zur Verfügung.

Do not launch	Es werden keine Option-ROMs gestartet.
UEFI only	Es werden nur UEFI Option-ROMs gestartet.
Legacy only	Es werden nur Legacy Option-ROMs gestartet.

Launch Storage OpROM policy

Legt fest, welcher Storage Option-ROM gestartet wird.

Do not launch	Es werden keine Storage Option-ROMs gestartet.
UEFI only	Es werden nur UEFI Storage Option-ROMs gestartet.
Legacy only	Es werden nur Legacy Storage Option-ROMs gestartet.

Launch Video OpROM policy

Legt fest, welches Video Option-ROM gestartet wird.

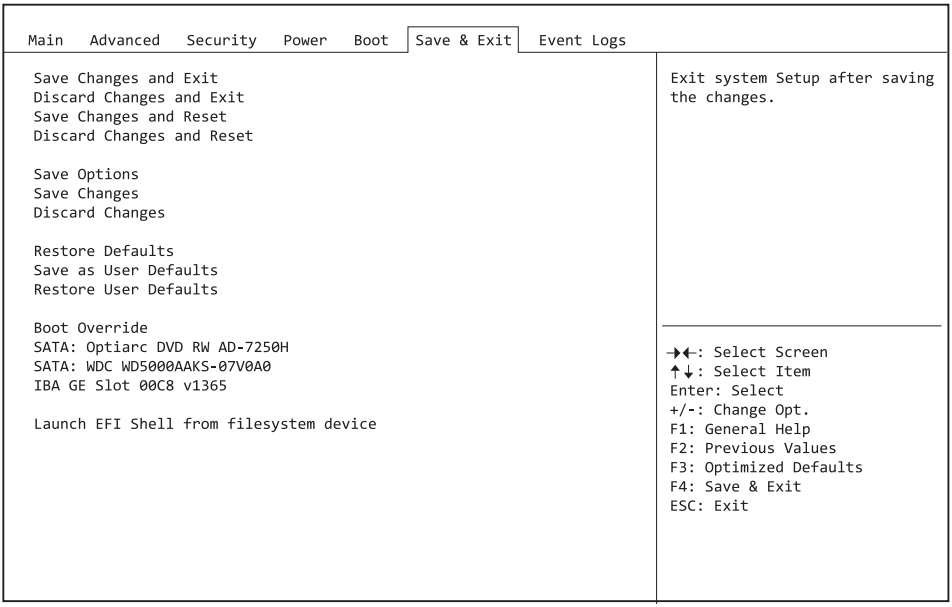
UEFI only	Es werden nur UEFI Video Option-ROMs gestartet.
Legacy only	Es werden nur Legacy Video Option-ROMs gestartet.

Other PCI device ROM priority

Legt fest, welches Option-ROM für Geräte außer Netzwerk, Massenspeicher oder Video gestartet wird.

UEFI OpROM	Es werden nur UEFI Option-ROMs gestartet.
Legacy OpROM	Es werden nur Legacy Option-ROMs gestartet.

Save & Exit Menu – BIOS-Setup beenden



Im Menü *Exit* können Sie Einstellungen speichern und das *BIOS-Setup* beenden.

Save Changes and Exit – Speichern und beenden

Um die aktuellen Einträge in den Menüs zu speichern und das BIOS-Setup zu beenden, wählen Sie *Save Changes and Exit* und dann *Yes*. Die neuen Einstellungen treten in Kraft und der POST wird fortgesetzt, solange kein Neustart aufgrund einer geänderten Option erforderlich ist.

Discard Changes and Exit – Beenden ohne speichern

Um die Änderungen seit dem Aufrufen des BIOS-Setups bzw. seit dem letzen Aufruf der Funktion "Save Changes" zu verwerfen, wählen Sie *Discard Changes & Exit* und *Yes*. Das BIOS-Setup wird beendet und der POST fortgesetzt.

Save Changes and Reset

Um die aktuellen Einträge in den Menüs zu speichern und das BIOS-Setup zu beenden, wählen Sie *Save Changes and Reset* und *Yes*. Es erfolgt ein Neustart und die neuen Einstellungen treten in Kraft.

Discard Changes and Reset

Um die Änderungen seit dem Aufrufen des BIOS-Setups bzw. seit dem letzen Aufruf der Funktion "Save Changes" zu verwerfen, wählen Sie *Discard Changes and Reset* und *Yes*. Das BIOS-Setup wird beendet und es erfolgt ein Neustart.

Save Options

Save Changes

Um die bisherigen Änderungen zu speichern, ohne das BIOS-Setup zu beenden, wählen Sie *Save Changes* und *Yes*.

Discard Changes

Um die Änderungen seit dem Aufrufen des BIOS-Setups bzw. seit dem letzen Aufruf der Funktion "Save Changes" zu verwerfen, ohne jedoch das BIOS-Setup zu verlassen, wählen Sie *Save Changes* und *Yes*.

Restore Defaults

Um alle Menüs des BIOS-Setups auf die Standardwerte zurückzusetzen, wählen Sie *Restore Defaults* und *Yes*. Wenn Sie das BIOS-Setup mit diesen Einstellungen verlassen möchten, wählen Sie *Save Changes and Exit* und *Yes*.

Save as User Defaults

Um die bisher vorgenommenen Änderungen als Benutzer-Standardeinstellungen zu speichern, wählen Sie *Save as User Defaults* und *Yes*.

Restore User Defaults

Um alle Menüs des BIOS-Setups auf die Benutzer-Standardeinstellungen zurückzusetzen, wählen Sie *Restore User Defaults* und *Yes*. Wenn Sie das BIOS-Setup mit diesen Einstellungen verlassen möchten, wählen Sie *Save Changes and Exit* und *Yes*.

Boot Override

Wählen Sie mit den Cursor-Tasten  und  das Laufwerk aus, von dem das Betriebssystem gestartet werden soll. Drücken Sie die Eingabetaste, um den Bootvorgang vom ausgewählten Laufwerk zu starten.

BIOS-Update

Um einen *Flash-BIOS-Update* durchzuführen können Sie die *Auto BIOS Update* Funktion verwenden ("Auto BIOS Update", Seite 35) oder müssen zuerst die dafür notwendigen Dateien aus dem Internet herunterladen.

Das BIOS wird auf einem Flash-Speicherbaustein gespeichert. Tritt während der Flash-BIOS-Updateprozedur ein Fehler auf, wird das BIOS-Image möglicherweise zerstört. Sie können das BIOS dann nur mit dem *BIOS Recovery Update* wieder herstellen, siehe "BIOS Recovery Update", Seite 67. Falls dies nicht möglich ist, muss der Flash-Speicherbaustein ersetzt werden. Kontaktieren Sie in diesem Fall den Service Desk des Kundenservice.

- Rufen Sie im Internet die Seite "http://www.fujitsu.com/de/support/index.html" auf.
- Wählen Sie über *MANUELLE PRODUKTAUSWAHL* Ihr Gerät aus oder suchen Sie Ihr Gerät unter *PRODUKTAUSWAHL ÜBER SERIEN-/IDENTNUMMER* über die Serien-/Identnummer oder den Produktnamen.
- Klicken Sie auf *Treiber & Downloads* und wählen Sie ihr Betriebssystem aus.
- Wählen Sie *Flash-BIOS*.
- Flash BIOS Update – Desk Flash Instant: Zum "Flash-BIOS-Update unter Windows" laden Sie die Datei *Flash BIOS Update – Desk Flash Instant* herunter.
- Admin package – Compressed Flash Files: Sollte sich das von Ihnen verwendete Betriebssystem nicht in der Auswahl befinden, wählen Sie ein beliebiges Betriebssystem aus und laden die Datei *Admin package – Compressed Flash Files* zum "Flash-BIOS-Update mit einem USB-Stick" herunter.
- Notieren Sie sich vorsorglich die Einstellungen im BIOS-Setup bevor Sie das Flash-BIOS-Update durchführen.Normalerweise beschädigt ein Flash-BIOS-Update die Einstellungen im BIOS-Setup nicht.

Auto BIOS Update

Mit *Auto BIOS Update* besteht die Möglichkeit auf einem Fujitsu-Server automatisch zu prüfen, ob für das System eine neue BIOS-Version zur Verfügung steht. Für die Aktualisierung ist weder ein Betriebssystem noch ein externes Speichermedium nötig. Details zu der Funktion *Auto BIOS Update* finden Sie im Handbuch unter "Auto BIOS Update", Seite 35.

Flash-BIOS-Update unter Windows

► Starten Sie Ihr System und booten Windows.

► Öffnen Sie den Windows-Explorer, wählen Sie die unter *Flash BIOS Update – Desk Flash Instant* heruntergeladene Datei aus und starten das Flash-BIOS-Update mit einem Doppelklick. Folgen Sie den Bildschirmanweisungen.

Zur Ausführung von "Desk Flash Instant" sind Administratorrechte notwendig.

↳ Nachdem das Flash-BIOS-Update erfolgt ist wird das System automatisch neu gestartet und mit der neuen BIOS-Version hochgefahren.

Flash-BIOS-Update mit einem USB-Stick

► Halten Sie einen bootfähigen USB-Stick bereit.

Falls Ihr USB-Stick nicht bootfähig ist finden Sie die dafür notwendigen Dateien, wenn Sie unter *Admin package – Compressed Flash Files* beim Punkt *Installationsbeschreibung* den Punkt *Weitere Informationen* auswählen. Folgen Sie den Anweisungen.

Bei der Erstellung eines bootfähigen USB-Stick werden alle Dateien auf dem Stick unwiederbringlich gelöscht. Tragen Sie bitte dafür Sorge, dass alle Dateien des USB-Stick zuvor gesichert werden!

► Entpacken Sie die unter *Admin package – Compressed Flash Files* heruntergeladenen ZIP-Datei und kopieren Sie die Dateien und Verzeichnisse in das Root-Verzeichnis Ihres bootfähigen USB-Stick.

► Starten Sie Ihr System neu und warten bis die Bildschirmausgabe erscheint. Drücken Sie die Funktionstaste F12 und wählen mit Hilfe der Cursortasten ↑ oder ↓ den bootfähigen USB-Stick aus.

► Wechseln Sie mit *cd DOS* das Verzeichnis und starten durch das Kommando *DosFlash* das Flash-BIOS-Update und folgen den weiteren Anweisungen.

↳ Nachdem das Flash-BIOS-Update erfolgt ist wird das System automatisch neu gestartet und mit der neuen BIOS-Version hochgefahren.

BIOS Recovery Update

- ► Bereiten Sie wie unter "Flash-BIOS-Update mit einem USB-Stick" beschrieben einen bootfähigen USB-Stick vor.
- ► Schalten Sie das System aus und nehmen Sie es vom Stromnetz.
- ► Öffnen Sie das Gehäuse und schalten Sie *Recovery* mittels Jumper / DIP-Switch auf dem System-Board ein. Details hierzu finden Sie im technischen Handbuch für das System-Board.
- ► Stecken Sie den vorbereiteten USB-Stick und entfernen alle anderen bootfähigen USB-Geräte.

Sollte das Admin package auf dem vorbereiteten USB-Stick nicht zur BIOS-Version des Systems passen (z. B. Admin package vom BIOS R1.2.0, aber BIOS R1.3.0 ist auf dem System aktiv) sind im Recovery-Modus keine Bildschirmausgaben möglich. Das Recovery-Update wird in diesem Fall automatisch durchgeführt.

Während des Recovery-Update wird ein sich wiederholender kurzer Signalton ausgegeben. Das Wiederherstellen des Systems war erfolgreich, wenn Sie nach einem langen Signalton die sich wiederholende Tonfolge "kurz-kurz-lang-lang" hören. Der Recovery-Vorgang kann einige Minuten dauern.

- ► Verbinden Sie das System wieder mit dem Stromnetz und schalten Sie es ein.
- ► Wechseln Sie mit *cd DOS* das Verzeichnis und starten durch das Kommando *DosFlash* das BIOS-Recovery-Update und folgen den weiteren Anweisungen.
- ► Wenn der Recovery-Vorgang beendet ist, schalten Sie das System aus und nehmen es vom Stromnetz.
- ► Entfernen Sie den USB-Stick.
- ► Setzen Sie alle Jumper / DIP-Switches, die geändert wurden, auf die ursprüngliche Position zurück und schließen das Gehäuse.
- ► Verbinden Sie das System wieder mit dem Stromnetz und schalten Sie es ein.
- ↳ Das System wird nun mit der neuen BIOS-Version hochgefahren.
- ► Prüfen Sie die Einstellungen im BIOS-Setup. Wenn nötig, konfigurieren Sie die Einstellungen noch einmal.

Anlage

Nutzungsbedingungen

Allgemeine Bedingungen für den kostenlosen Download von Software auf Portalen von Fujitsu Technology Solutions

1. Anwendungsbereich, Gegenstand

Diese „Allgemeinen Bedingungen für den kostenlosen Download von Software auf Portalen von Fujitsu Technology Solutions“ („Bedingungen“) gelten für den kostenlosen Download von Software auf allen Portalen von Fujitsu Technology Solutions („FTS“). Die von FTS zum Herunterladen bereitgehaltenen Downloadprodukte inklusive Updates, Upgrades, Patches etc. („Software“) wurden sorgfältig ausgewählt, eingestellt und – soweit sie von Dritten („Lizenzgebern“) stammen – unverändert übernommen. Eine Verpflichtung von FTS zum Angebot kostenloser Software oder zur kostenlosen Bereitstellung von Updates oder Upgrades etc. wird hierdurch nicht begründet. Jedes Angebot von Software zum kostenlosen Download kann von FTS jederzeit ohne Angabe von Gründen eingestellt werden.

2. Umfang der Nutzung

Mit dem Download der Software erhält der jeweils Herunterladende („Nutzer“) das nicht ausschließliche Recht, die Software in unveränderter Form auf der eigenen Systemeinheit zu nutzen. Soweit nicht zwingende Rechtsvorschriften entgegenstehen, ist es dem Nutzer untersagt, die Software zu verändern, zu ergänzen, zurück zu entwickeln, zu übersetzen, in anderer Weise zu überarbeiten oder Programmteile herauszulösen. Soweit die Software von Lizenzgebern stammt, verpflichtet sich der Nutzer mit dem Download der Software, die einschlägigen Bedingungen des Lizenzgebers vollumfänglich einzuhalten. Soweit die Vervielfältigung der Software gestattet ist, hat der Nutzer alphanumerische Kennungen, Metadaten, Marken und Urheberrechtsvermerke etc. unverändert mit zu vervielfältigen.

3. Nutzungsberechtigung

Alle Rechte an der Software, insbesondere alle Urheber-, Patent- und Markenrechte, verbleiben bei FTS bzw. den jeweiligen Lizenzgebern. Diese Rechte werden weder durch noch im Zusammenhang mit dem Download der Software auf den Nutzer übertragen. Eine Verwertung ist nur mit Zustimmung von FTS bzw. des jeweiligen Inhabers der Rechte an der Software zulässig. Rechtsverletzungen werden zivilrechtlich und strafrechtlich verfolgt. Der Nutzer darf die Software Dritten nur zur Verfügung stellen oder sonst zugänglich machen, wenn sich der Dritte ausdrücklich zur Einhaltung dieser Bedingungen verpflichtet hat. Gleiches gilt für die Übertragung des Rechts zur Nutzung der Software auf Dritte.

Das Recht des Nutzers zur Nutzung der Software erlischt automatisch, wenn und sobald der Nutzer gegen diese Bedingungen verstößt.

4. Mängel der Software

Soweit nicht beim Download der Software von FTS ausdrücklich anders beschrieben, stellt FTS die Software unentgeltlich und ausschließlich in dem zum Download bereitgestellten Zustand und ohne eine ausdrückliche oder indirekte Zusicherung von bestimmten Eigenschaften (z.B. eine bestimmte Spezifikation etc.) zur Verfügung. Soweit nicht zwingende Rechtsvorschriften entgegenstehen übernimmt FTS keinerlei Haftung für Mängel jeder Art, es sei denn der Mangel wurde von FTS vorsätzlich oder grob fahrlässig verursacht oder arglistig verschwiegen. FTS haftet insbesondere

nicht für Übermittlungsfehler und/oder Störungen des Datenaustausches während des Downloads, z.B. Leitungsausfall, Verbindungsunterbrechungen, Serverausfälle, Datenkorruption oder ähnliches.

5. Haftung

Der Download der Software durch den Nutzer erfolgt vollumfänglich auf eigene Gefahr des Nutzers.

FTS übernimmt keinerlei Verantwortung dafür, dass die Software und/oder Dokumentation am Ort des Nutzers abgerufen oder heruntergeladen werden kann bzw. dass die Software und/oder Dokumentation am Ort des Nutzers heruntergeladen werden darf. Der Nutzer ist ausschließlich selbst für die Einhaltung der nach dem anwendbaren Landesrecht jeweils einschlägigen Vorschriften verantwortlich. Der Nutzer ist insbesondere für die Überprüfung der Verwendbarkeit der Software für seine Zwecke sowie der Verträglichkeit mit seinen Systemen ausschließlich selbst verantwortlich. Soweit der Download der Software gegen einschlägige Rechtsvorschriften verstößt, ist der Download der Software und/oder Dokumentation ausdrücklich untersagt. FTS haftet nicht für Schäden, die dem Nutzer mittelbar oder unmittelbar aus dem Download der Software entstehen, es sei denn soweit FTS den Schaden Schäden vorsätzlich oder grob fahrlässig herbeigeführt hat. FTS übernimmt insbesondere keine Verantwortung für Schäden, die im Zusammenhang damit entstehen, dass der Nutzer keine tagesaktuelle Datensicherung in geeigneter Form angefertigt oder sonst eine zeitnahe und kostengünstige Wiederherstellung von Daten sichergestellt hat. FTS ersetzt insbesondere nicht den Aufwand für die Wiederbeschaffung verlorener Daten und Informationen.

Weitergehende als die in diesen Bedingungen ausdrücklich genannten Ansprüche des Nutzers gegen FTS, gleich aus welchem Rechtsgrund, insbesondere wegen Betriebsunterbrechung, entgangenen Gewinn, Verlust von Informationen und Daten etc. oder Mangelfolgeschäden sind ausgeschlossen.

Im Übrigen haftet FTS nur diejenige Sorgfalt, die der üblichen Sorgfalt in eigenen Angelegenheiten von FTS entspricht.

Vorstehende Beschränkung der Haftung von FTS gilt nicht, soweit zwingende Rechtsvorschriften entgegenstehen.

6. Ausfuhr- und Einfuhrbeschränkungen, personenbezogene Daten des Nutzers

Der Export und/oder Reexport einschließlich der nicht gegenständlichen Übermittlung von Gütern kann - z.B. aufgrund der Art oder des Verwendungszwecks - der Genehmigungspflicht unterliegen. Die Einholung dieser Genehmigungen insbesondere gemäß der geltenden Exportkontrollvorschriften der Bundesrepublik Deutschland, der Europäischen Union, der United States of America (USA) und/oder nach dem Recht irgend eines anderen Landes, das durch einen solchen Tatbestand berührt ist oder einen solchen regelt, liegt in der Verantwortung des Nutzers.

Downloads, Exporte, Reexporte und die Erbringung von Dienstleistungen in Zusammenhang mit dieser Software dürfen nicht erfolgen, wenn Grund zu der Annahme besteht, dass eine Nutzung im Zusammenhang mit chemischen, biologischen oder Kernwaffen oder Flugkörpern für derartige Waffen erfolgt.

Der Nutzer wird die einschlägigen Sanktionslisten der Europäischen Union, der Deutschen Bundesregierung, der US-Exportbehörden, der japanischen Exportbehörden oder anderer relevanter Länder, z.B. European Sanctions List, Denied Persons List, sowie sonstige Warnhinweise der zuständigen Behörden in der jeweils aktuellsten Fassung beachten und danach handeln.

Downloads sind grundsätzlich nicht zulässig für Länder und Staatsangehörige der Country-Group E gemäß US Export Administration Regulations (z.B. Iran, Syrien, Nord Korea, Sudan, Kuba).

FTS ist nicht verpflichtet, Lieferungen zu tätigen und/oder andere Verpflichtungen aus diesem Vertrag zu erfüllen, soweit FTS an entsprechenden Lieferungen bzw. der Erfüllung entsprechender Verpflichtungen aufgrund von Exportvorschriften (insbesondere z.B. diejenigen der Bundesrepublik Deutschland, der Europäischen Union, der USA oder Japan) gehindert ist.

Insbesondere aufgrund einschlägiger Ausfuhr- und/oder Einfuhrbeschränkungen kann es erforderlich sein, dass FTS bestimmte personenbezogene Daten des Nutzers (z.B. Vor- und Nachname, IP-Adresse etc.) erhebt, speichert, verarbeitet oder an Dritte weitergibt (z.B. bei entsprechendem Auskunftsersuchen einer Behörde). Die Speicherung besagter Daten erfolgt nur dann, wenn „hochverschlüsselte SW-Produkte“ heruntergeladen werden. Mit dem Download erklärt sich der Nutzer hiermit ausdrücklich einverstanden.

7. Sonstiges

Sollten einzelne Bestimmungen dieser Bedingungen ganz oder teilweise unwirksam sein, so berührt dies die Wirksamkeit der Bedingungen im Übrigen nicht, es sei denn, das Festhalten hieran stellt auch unter Berücksichtigung der ergänzend angewandten gesetzlichen Vorschriften eine unzumutbare Härte dar.

Es gilt das deutsche Recht. Ausschließlicher Gerichtsstand ist München, soweit ein solcher Gerichtsstand zulässigerweise mit dem Nutzer vereinbart werden darf.

Stichwörter

A
Access Level 14
Acoustic Management 30
Acoustic Mode 30
Active Processor Cores 21
Adjacent Cache Line Prefetcher 22
Advanced Menü 15
Aggressive Link Power Management 28
AMT Configuration 37
Audio Configuration 34
Authorized Signature Database (DB) 50
Automatic BIOS Update 35–36

B
BIOS Recovery Update 67
BIOS-Setup 9
  aufrufen 9
  bedienen 11
  beenden 63
  Einstellungen 7
  Sicherheitsfunktionen 44
  Systemeinstellungen 15
  Systemkonfiguration 12
BIOS-Update 65
  mit USB-Stick 66
  unter Windows 66
Boot Menü 10
  aufrufen 10
  Systemstart 58
Boot option filter 61

C
COM0 38
COM1 38
CPU 20, 42
CPU C3 Report 25
CPU C6 Report 25
CPU C7 Report 25
CSM 60–62

D
Data Cache Unit 22–23
Datum 13
DDR Performance 27
Decoding
  4G 17
Details
  Firmware 12
  Memory 13
  Network Controller 13
  Processor 13
Discard Changes and Exit 63

E
EMS 40
Energy Performance 24
Enhanced Speedstep 24
Erase Disk 15
Error Logging 26
Erweiterungskarten 43
Event Log 56
Execute Disable Bit 21
Exit Menü 63
External SATA Port 29

F
F12, Funktionstaste 10
Fast Patrol Scurb 28
Forbidden Signature Database (DBX) 51
Frequenz 27–28

G
Geräuschpegel 30
Geschwindigkeit 27–28

H
Hardware Prefetcher 22
High Precision Event Timer Configuration 34
Hot Plug 29
Hyper Threading 21

I
Intel Virtualization Technology 23
IP Adresse 36

K
Key Exchange Key (KEK) 50
Key Management 49–51

L
LAN 10, 34–35
Launch CSM 61
Launch Legacy OpROM 34
Launch PXE OpROM Policy 61
Launch Storage OpROM policy 61
Launch Video OpROM policy 61

Legacy USB Support 31
Limit CPUID Maximum 21
Link Speed 18

M
Main Menü 12
Mass Storage Devices 32
Memory Konfiguration 27

N
Network Stack 41
NUMA 27
NumLock 58
Nutzungsbedingungen 35

O
Onboard Device Configuration 33
Other PCI device ROM priority 62

P
P-State Coordination 25
Package C State limit 26
Password 45
  Administrator Password 45
  User Password 45–46
  User Password on Boot 46
PCI 43
  ASPM Support 18
  PCI-Paritätsfehler 18
  PCI-Systemfehler 18
Platform Key 49–50
Platform Key (PK) 49
Platform Mode 48
Power Technology 23
PXE Boot 42

R
Recovery Update 67
Refresh Rate Multiplier 28

S
SATA Konfiguration 28
SATA-Festplatte löschen 15
SATA-Schnittstellen 28
Save Changes and Exit 63
Schreibschutz 46
Secure Boot 48–49
Secure Boot Control 48
Secure Boot Keys 51
Secure Boot Mode 49
Security Menü 44
Serial-ATA Controller 0 29
Serial-ATA Controller 1 29
Serielle Schnittstelle 38
Setup,
  siehe BIOS-Setup 9
Smartcard 47–48
Speicherfehler 26
Staggered Spin-up 29
Steckplätze 43
Stromausfall, Verhalten des Systems 53
Super IO Configuration 36
System Date / System Time 13
System einschalten
  LAN-Controller 54
  Netzwerk 54
System Information 12
System Language 13
System Monitoring 33
SystemLock 47

T
Terms of Use 35
Trusted Computing 19
Trusted Platform Module 19
  Pending TPM operation 19
  TPM State 19
  TPM Status Information 20
  TPM Support 19
Turbo Mode 24

U
Uhrzeit 13
Update 35–36, 65
USB 31
  USB-Schnittstellen 32
  USB-Tastatur 55

V
VT-d 23

W
Wake Up Mode 55
Wake Up Timer 54

Z
Zugriff 14