Reference Manual - English

D3375 BIOS Setup Utility for FUJITSU Server PRIMERGY RX1330 M3

Reference Manual

Edition March 2017

Comments… Suggestions… Corrections…

The User Documentation Department would like to know your opinion of this manual. Your feedback helps us optimize our documentation to suit your individual needs.

Feel free to send us your comments by e-mail to manuals@ts.fujitsu.com.

Certified documentation according to DIN EN ISO 9001:2008

To ensure a consistently high quality standard and user-friendliness, this documentation was created to meet the regulations of a quality management system which complies with the requirements of the standard DIN EN ISO 9001:2008.

cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

Copyright and Trademarks

All hardware and software names used are trademarks of their respective manufacturers.

- The contents of this manual may be revised without prior notice.
- Fujitsu assumes no liability for damages to third party copyrights or other rights arising from the use of any information in this manual.
- No part of this manual may be reproduced in any form without the prior written permission of Fujitsu.

Microsoft, Windows, Windows Server, and Hyper V are trademarks or registered trademarks of Microsoft Corporation in the USA and other countries.

Intel and Xeon are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the USA and other countries.

Before reading this manual

For your safety

This manual contains important information for safely and correctly using this product.

Carefully read the manual before using this product. Pay particular attention to the accompanying manual "Safety Notes and Regulations" and ensure these safety notes are understood before using the product. Keep this manual and the manual "Safety Notes and Regulations" in a safe place for easy reference while using this product.

Radio interference

This product is a "Class A" ITE (Information Technology Equipment). In a domestic environment this product may cause radio interference, in which case the user may be required to take appropriate measures. VCCI-A

Aluminum electrolytic capacitors

The aluminum electrolytic capacitors used in the product's printed circuit board assemblies and in the mouse and keyboard are limited-life components. Use of these components beyond their operating life may result in electrolyte leakage or depletion, potentially causing emission of foul odor or smoke.

As a guideline, in a normal office environment (25°C) operating life is not expected to be reached within the maintenance support period (5 years). However, operating life may be reached more quickly if, for example, the product is used in a hot environment. The customer shall bear the cost of replacing replaceable components which have exceeded their operating life. Note that these are only guidelines, and do not constitute a guarantee of trouble-free operation during the maintenance support period.

High safety use

This product has been designed and manufactured to be used in commercial and/or industrial areas as a server.

When used as visual display workplace, it must not be placed in the direct field of view to avoid incommoding reflections (applies only to TX server systems).

The device has not been designed or manufactured for uses which demand an extremely high level of safety and carry a direct and serious risk of life or body if such safety cannot be assured.

These uses include control of nuclear reactions in nuclear power plants, automatic airplane flight control, air traffic control, traffic control in mass transport systems, medical devices for life support, and missile guidance control in weapons systems (hereafter, "high safety use"). Customers should not use this product for high safety use unless measures are in place for ensuring the level of safety demanded of such use. Please consult the sales staff of Fujitsu if intending to use this product for high safety use.

Measures against momentary voltage drop

This product may be affected by a momentary voltage drop in the power supply caused by lightning. To prevent a momentary voltage drop, use of an AC uninterruptible power supply is recommended.

(This notice follows the guidelines of Voltage Dip Immunity of Personal Computer issued by JEITA, the Japan Electronics and Information Technology Industries Association.)

Technology controlled by the Foreign Exchange and Foreign Trade Control Law of Japan

Documents produced by Fujitsu may contain technology controlled by the Foreign Exchange and Foreign Trade Control Law of Japan. Documents which contain such technology should not be exported from Japan or transferred to non-residents of Japan without first obtaining authorization in accordance with the above law.

Harmonic Current Standards

This product conforms to harmonic current standard JIS C 61000-3-2.

Only for the Japanese market:
About SATA hard disk drives

The SATA version of this server supports hard disk drives with SATA / BC-SATA storage interfaces. Please note that the usage and operation conditions differ depending on the type of hard disk drive used.

Please refer to the following internet address for further information on the usage and operation conditions of each available type of hard disk drive:

http://jp.fujitsu.com/platform/server/primergy/harddisk/

Content

1 Introduction 7

2 Navigating the BIOS setup 9

2.1 Open the BIOS setup 9

2.2 Open the Boot menu immediately 9

2.3 Screen design 11

2.4 Exiting the BIOS setup 12

3 Main menu 13

4 Advanced menu 15

4.1 Onboard Devices Configuration 18

4.2 PCI Status 19

4.3 PCI Subsystem Settings 19

4.4 CPU Configuration 21

4.5 Memory Status 25

4.6 SATA Configuration 26

4.7 CSM Configuration 26

4.8 Trusted Computing 28

4.9 USB Configuration 31

4.9.1 USB Port Security 33

4.10 Super IO Configuration 33

4.10.1 Serial Port 1 Configuration 33

4.11 Network Stack Configuration 34

4.12 Option ROM Configuration 35

4.13 VIOM Configuration 35

4.14 iSCSI Configuration 36
4.15 UEFI Device Driver Setup 36
4.16 Driver Health 36

5 Security menu 37

5.1 Secure Boot 40
5.1.1 Key Management 41

6 Power menu 45

6.1 Wake-Up Resources 46

7 Server Mgmt menu 47

7.1 iRMC LAN Parameters Configuration 52
7.2 Console Redirection 56

8 Boot menu 57

9 Save & Exit menu 61

10 Flash BIOS Update 63

10.1 Flash Memory Recovery Mode 65

Index 67

1 Introduction

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

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

- *Main* – System functions
- *Advanced* – Advanced system configuration
- *Security* – Security functions
- *Power* – Power management functions
- *Server Mgmt* – Server Management
- *Boot* – Configuration of the start-up sequence
- *Save & Exit* – Save and quit

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

Menus or certain setting options may therefore not be available in your system's BIOS setup, or the menus may be in a different place, depending on the BIOS revision.

Notational conventions

The meanings of fonts and symbols used in this manual are as follows:

Italics	Commands, menu items, path names, and file names
`fixed font`	System output
`semi-bold fixed font`	Text you have to enter via the keyboard
"Quotation marks"	Names of chapters and terms that are being emphasized
►	Activities that must be performed in the shown order
Abc	Key on the keyboard
ℹ	Additional information, notes and tips
⚠ **CAUTION!**	References, during their neglect your health, the operability of your system, or the security of your data is endangered

2 Navigating the BIOS setup

2.1 Open the BIOS setup

► Start the system and wait until the screen output appears.

► Press the F2 function key.

► If a password is assigned, enter this password and confirm with the Enter key.

The BIOS setup *Main* menu will be displayed on the screen.

► To show system specific information select *System Information* and press the Enter key.

The BIOS release information will be displayed:

- BIOS release (e.g. Version R1.3.0)
  The number of the system board (e.g. D3375-A1x) you will find under *Board*.
- Press the F1 function key.
  The General Help information will be displayed.

When the *Main* menu does not appear:

- If the *Main* menu does not appear by pressing the F2 function key, press the Ctrl + Alt + Delete keys at the same time to restart the system, then start up BIOS Setup Utility.

2.2 Open the Boot menu immediately

Use this function if you do not want to start your system from the first drive that is set in the *Boot* menu under the *Boot Option Priorities* menu item.

► Start the system and wait until the screen output appears.

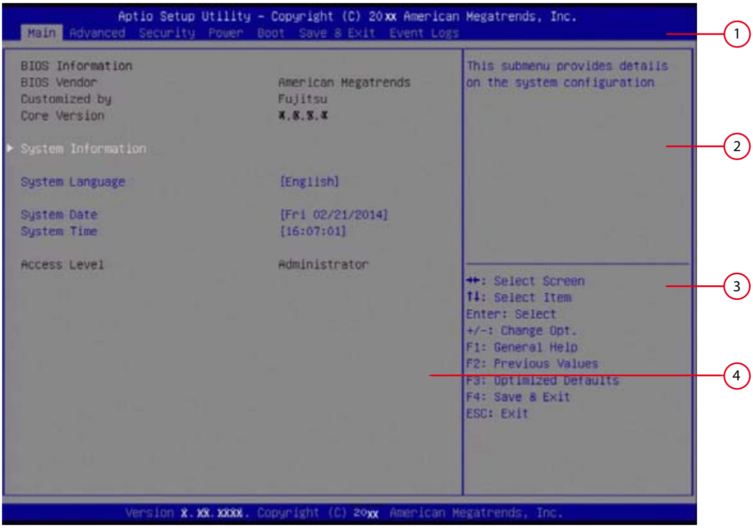
► Press the F12 function key.
The *Boot* menu will be displayed as a popup window.

► Use the ↑ or ↓ cursor keys to select the drive from which you want to start the operating system, and confirm your selection by pressing the Enter key. The selection options are the same as in the *Boot* menu.

ℹ The selected option applies to the current system start. The next time you start the system, the settings in the *Boot* menu will apply again.

► To start the BIOS setup, select the *Enter Setup* parameter and confirm your selection with the [Enter] key.

2.3 Screen design



```
        Aptio Setup Utility - Copyright (C) 20xx American Megatrends, Inc.
 Main  Advanced  Security  Power  Boot  Save & Exit  Event Logs

 BIOS Information                                     This submenu provides details
 BIOS Vendor                  American Megatrends     on the system configuration
 Customized by                Fujitsu
 Core Version                 x.x.x.x

▶ System Information

 System Language              [English]

 System Date                  [Fri 02/21/2014]
 System Time                  [16:07:01]

 Access Level                 Administrator
                                                      →←: Select Screen
                                                      ↑↓: Select Item
                                                      Enter: Select
                                                      +/-: Change Opt.
                                                      F1: General Help
                                                      F2: Previous Values
                                                      F3: Optimized Defaults
                                                      F4: Save & Exit
                                                      ESC: Exit

          Version x.xx.xxxx. Copyright (C) 20xx American Megatrends, Inc.
```

Figure 1: Example for a BIOS setup screen

The BIOS setup screen is divided into the following areas:

1 Menu bar

The menu bar is used to select the different BIOS setup menus.

2 Help area

Brief information is displayed in the help area.

3 Operations area

The operations area lists the keys available for use with BIOS setup.

4 Working area

In the working area the parameters of the selected menu are displayed with their current values. You can modify the parameter values according to your requirements (if the appropriate fields are not greyed out).

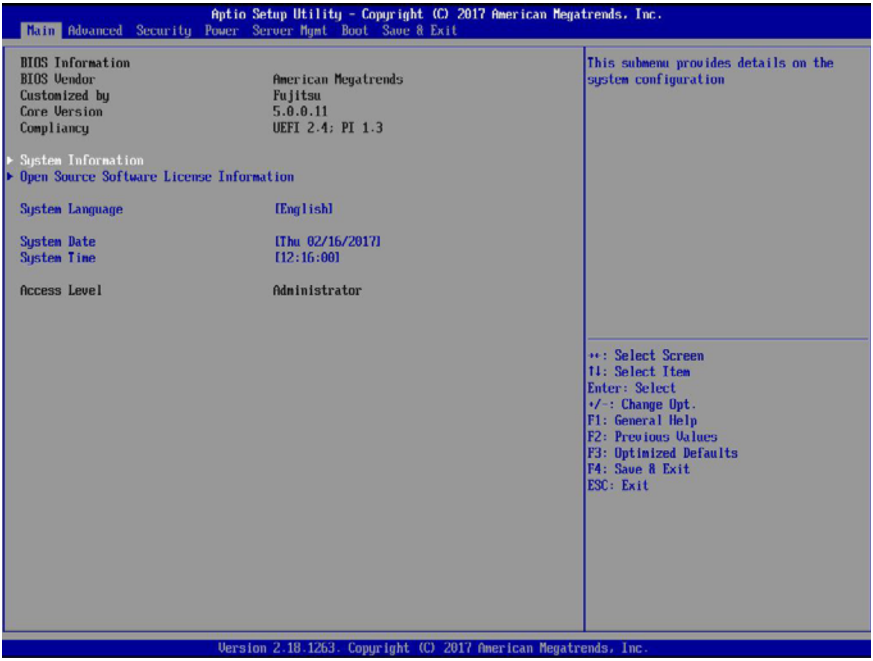
► Indicates parameters containing submenus

2.4 Exiting the BIOS setup

► In the *Save & Exit* menu select the required parameter and press the Enter key.

3 Main menu

The following parameters can be set in this menu. Some of them are only available under special preconditions.



```
Aptio Setup Utility - Copyright (C) 2017 American Megatrends, Inc.

BIOS Information                                     This submenu provides details on the
BIOS Vendor                  American Megatrends     system configuration
Customized by                Fujitsu
Core Version                 5.0.0.11
Compliancy                   UEFI 2.4; PI 1.3

► System Information
► Open Source Software License Information

System Language              [English]

System Date                  [Thu 02/16/2017]
System Time                  [12:16:00]

Access Level                 Administrator
                                                     →←: Select Screen
                                                     ↑↓: Select Item
                                                     Enter: Select
                                                     +/-: Change Opt.
                                                     F1: General Help
                                                     F2: Previous Values
                                                     F3: Optimized Defaults
                                                     F4: Save & Exit
                                                     ESC: Exit

Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```

Figure 2: Example for the "Main" menu

System Information

The *System Information* window displays an overview about the system configuration. This includes CPU, memory and LAN configuration data.

Open Source Software License Information

This submenu provides licenses information for open source software, used in this system board.

System Language

Defines the language used in BIOS setup utility.

System Date / System Time

Displays the current date/time set on the system.

The system time has the format *HH*:*MM*:*SS*, and the system date has the format *DOW (day of week)/MM/DD/YYYY*.

To change the current time/date settings enter the new time/date in the *System Time*/*System Date* fields respectively. Use the [Tab] key to move the cursor within the *System Time* and the *System Date* fields.

> If the system time and date are lost after you switch the system off and back on again, the lithium battery is empty and needs to be replaced.
>
> Refer to the "FUJITSU Server PRIMERGY RX1330 M3 Server Upgrade and Maintenance Manual" for information on how to replace the lithium battery.

Access Level

Displays the current *Access Level* in BIOS setup utility.

Administrator

In case Administrator password was entered or the system is not password protected the *Access Level* is Administrator.

User

If the User Password was set and User password was entered the user will have *User* level.

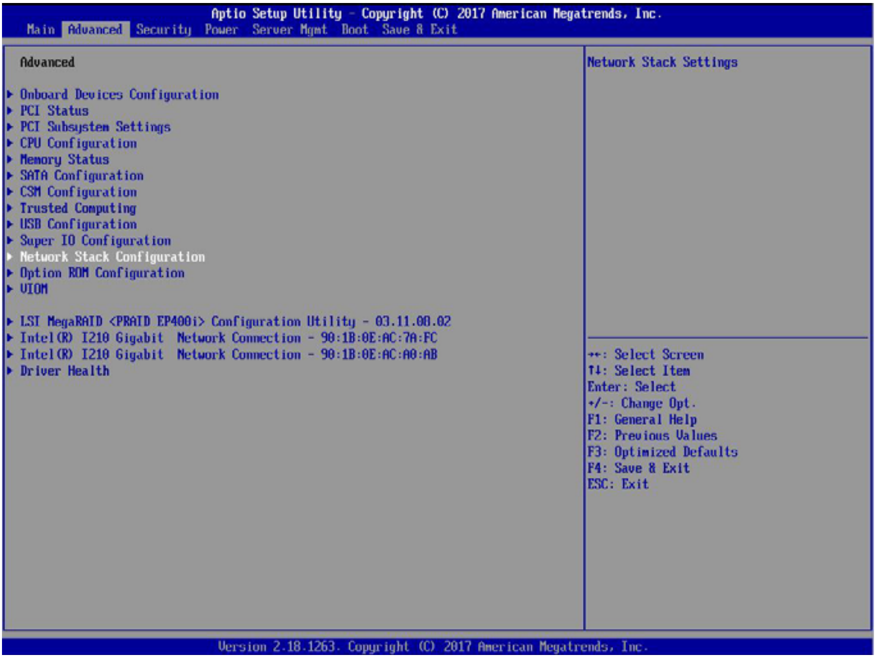
If Administrator and User password are assigned the *Access Level* depends on the password used for entering BIOS setup utility.

4 Advanced menu

CAUTION!

Only change the default settings if required for a special purpose. Incorrect settings in this menu can result in malfunctions on your computer!

Some settings depend on system configuration!



```
Aptio Setup Utility - Copyright (C) 2017 American Megatrends, Inc.
  Main  Advanced  Security  Power  Server Mgmt  Boot  Save & Exit

  Advanced                                              Network Stack Settings

► Onboard Devices Configuration
► PCI Status
► PCI Subsystem Settings
► CPU Configuration
► Memory Status
► SATA Configuration
► CSM Configuration
► Trusted Computing
► USB Configuration
► Super IO Configuration
► Network Stack Configuration
► Option ROM Configuration
► VIOM

► LSI MegaRAID <PRAID EP400i> Configuration Utility - 03.11.00.02
► Intel(R) I210 Gigabit  Network Connection - 90:1B:0E:AC:7A:FC   →←: Select Screen
► Intel(R) I210 Gigabit  Network Connection - 90:1B:0E:AC:A0:AB   ↑↓: Select Item
► Driver Health                                                   Enter: Select
                                                                  +/-: Change Opt.
                                                                  F1: General Help
                                                                  F2: Previous Values
                                                                  F3: Optimized Defaults
                                                                  F4: Save & Exit
                                                                  ESC: Exit

Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```

Figure 3: Example for the "Advanced" menu

Onboard Devices Configuration

Calls a submenu used to configure Onboard Devices. Some of them are only available under special preconditions (see "Onboard Devices Configuration" on page 18).

PCI Status

Calls a submenu used to watch the status of the PCI Express expansion cards (see "PCI Status" on page 19).

PCI Subsystem Settings

Calls a submenu used to set up the PCI slots and PCI components on the system board (see "PCI Subsystem Settings" on page 19).

CPU Configuration

Calls a submenu used to make additional processor settings (see "CPU Configuration" on page 21).

The adjustment options available in this submenu depend on the processor being used.

Memory Status

Calls a submenu used to watch the memory modules status (see "Memory Status" on page 25).

SATA Configuration

Calls a submenu containing the settings for the corresponding SATA controller (see "SATA Configuration" on page 26).

CSM Configuration

Opens the submenu for configuring the Compatibility Support Module (CSM) (see "CSM Configuration" on page 26).

Trusted Computing

Calls a submenu used to make additional system settings (see "Trusted Computing" on page 28).

USB Configuration

Calls a submenu used to set up the USB components on the system board (see "USB Configuration" on page 31).

Super IO Configuration

Calls a submenu used to configure System Super IO Chip parameters (see "Super IO Configuration" on page 33).

Network Stack Configuration

Calls a submenu used to set up the UEFI network stack (see "Network Stack Configuration" on page 34).

Option ROM Configuration

Calls a submenu to enable or disable the legacy Option ROMs of the PCI Express expansion cards (see "Option ROM Configuration" on page 35).

VIOM

Virtual IO-Manager can be disabled and its status is reported (see "VIOM Configuration" on page 35).

iSCSI Configuration

Calls a submenu used to configure a UEFI driver for a LAN controller (see "iSCSI Configuration" on page 36).

Driver Health

Calls a submenu used to display the health states of the UEFI drivers supporting the Driver Health interface (see "Driver Health" on page 36).

4.1 Onboard Devices Configuration

Opens the submenu to configure Onboard Devices. Some of them are only available under special preconditions.

LAN n Controller

Specifies if the respective onboard LAN controller is operational. If multiple onboard LAN controllers are present, each can be enabled/disabled individually.

Disabled

LAN controller is disabled.

Enabled

LAN controller is enabled.

LAN n Oprom

LAN controllers can be used as boot devices if a suitable Option ROM is started during BIOS POST. This parameter specifies whether an Option ROM should be started and if so which type of Option ROM.

Disabled

Do not start any Option ROM.

PXE

Starts the PXE Option ROM to provide the functionality for booting via PXE.

iSCSI

Starts the iSCSI Option ROM to provide the functionality for booting via iSCSI.

4.2 PCI Status

This submenu displays the current status of the expansion card in the slots.

PCI Slot n

Displays the current status of the expansion card in this slot.

Failed

An error was detected for this slot. The expansion card in this slot may have a problem.

ℹ After replacing the failing PCI card, please enable PCI slot again.

Enabled

No errors were reported for this slot. The expansion card in this slot can be used without restriction.

Empty

There is no expansion card in this slot.

4.3 PCI Subsystem Settings

The following parameters can be set in this menu. Some of them are only available under special preconditions.

ASPM Support

Active State Power Management (ASPM) is used to power-manage the PCI Express links, thus consuming less power. Even if ASPM is generally enabled by this selection, it will only be enabled for a specific link if the appropriate PCI Express expansion card or onboard controller supports it also.

Disabled

ASPM is disabled. Power consumption for PCI Express links is not reduced. Best compatibility.

Auto

Tries to configure maximum possible energy saving. Low power mode for PCI Express links is set to L0s (one direction) or L1 (bidirectional).

Force L0s

Low power mode for PCI Express links is set to L0s (one direction). Tradeoff between compatibility and energy saving.

The latency for PCI Express devices may increase if ASPM is not disabled. Several expansion cards do not support this feature correctly, which may lead to an undefined system behavior.

Above 4G Decoding

Specifies if memory resources above the 4 GB address boundary can be assigned to PCI devices. The selection depends on the operating system and the populated adapter cards.

Disabled

Only memory resources below the 4 GB address boundary will be assigned to the PCI devices. This selection is mandatory when using a 32-bit operating system, but is also supported on 64-bit operating systems.

Enabled

Memory resources above the 4 GB address boundary may be assigned to PCI devices, which are capable of 64-bit address decoding. This selection is supported only on 64-bit operating systems. It may be required if the populated PCI Express devices (e.g. coprocessors adapter cards) are claiming a huge amount of memory resources, which no longer fits into the address space below 4 GB.

The PCI address decoding of 32-bit operating systems is limited by the 4 GB address boundary, even if the available PCI devices would also support 64-bit address decoding.

DMI Control

Selects the speed of the bus connection between CPU and chipset. Lower speed means less power consumption but also lower system performance.

Auto

The bus connection between CPU and chipset is configured to run at highest possible speed.

GEN1

The bus connection between CPU and chipset is configured to run at 2.5GT/s.

GEN2

The bus connection between CPU and chipset is configured to run at 5.0GT/s.

GEN3

The bus connection between CPU and chipset is configured to run at 8.0GT/s.

4.4 CPU Configuration

The following parameters can be set in this menu. Some of them are only available under special preconditions.

Hyper-Threading

Hyper-threading technology allows a single physical processor core to appear as several logical processors. With this technology the operating system can better utilize the internal processor resources, which in turn leads to increased performance. The advantages of this technology can only be used by an operating system which supports ACPI. This setting has no effect on operating systems which do not support ACPI.

Disabled

An ACPI operating system can only use the first logical processor of a processor core. This setting should only be used if hyper-threading technology has not been correctly implemented in the ACPI operating system.

Enabled

An ACPI operating system can use all logical processors within a physical processor.

Active Processor Cores

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

0

All available processor cores are active and can be used.

1...n

Only the selected number of processor cores are active. The remaining processor cores are deactivated.

This selection may solve problems with specific software packages or system licenses.

Hardware Prefetcher

If activated memory content, that is likely required, is preloaded automatically to the cache when the memory bus is inactive. Fetching content form cache instead of memory reduces the latency especially for applications with linear data access.

With this parameter you can change the performance settings for non-standard applications. It is recommended that you should adhere to the default settings for standard applications.

Disabled

Deactivates the hardware prefetcher of the CPU.

Enabled

Activates the hardware prefetcher of the CPU.

Adjacent Cache Line Prefetch

Available if the processor offers a mechanism for loading an additional adjacent 64 Byte cache line during every cache request of the processor. This will increase cache hit ratio for applications with high spatial locality.

With this parameter you can change the performance settings for non-standard applications. It is recommended that you should adhere to the default settings for standard applications.

Disabled

The processor loads the requested cache line.

Enabled

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

DCU Streamer Prefetcher

If activated data content, that is likely required, is preloaded automatically to the L1 data cache when the memory bus is inactive. Fetching content from cache instead of memory reduces the latency especially for applications with linear data access.

With this parameter you can change the performance settings for non-standard applications. It is recommended that you should adhere to the default settings for standard applications.

Disabled

Deactivates the *DCU Streamer Prefetcher* of the CPU.

Enabled

Activates the *DCU Streamer Prefetcher* of the CPU.

Intel Virtualization Technology

Supports the virtualization of platform hardware and several software environments, based on VMX (Virtual Machine Extensions) to support the use of several software environments using virtual computers. Virtualization technology extends the processor support for virtualization purposes with the 16 Bit and 32 Bit protected modes and with the EM64T (Intel® Extended Memory 64 Technology) mode.

Disabled

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

Enabled

A VMM can use the additional hardware features.

VT-d

VT-d (Virtualization Technology for Directed I/O) provides hardware support for sharing I/O devices between multiple virtual machines. VMMs (Virtual Machine Monitors) can use VT-d for managing multiple virtual machines accessing the same physical I/O device.

Disabled

VT-d is disabled and not available for VMMs.

Enabled

VT-d for VMMs is enabled.

Intel TXT Support

Activates Trusted Execution Technology (TXT) Support. Intel® TXT is available if the populated CPU supports Secure Mode Extensions (SMX) and Virtualization Technology (VT) as well as VT-d are enabled within the CPU submenu.

i The Intel® TXT Support has to be disabled before the system BIOS update is initiated.

Disabled

TXT is deactivated.

Enabled

TXT is activated.

Enhanced SpeedStep

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

The processor voltage is adapted to the respective system requirements. A reduction in the clock frequency causes less power to be required by the system.

Disabled

Enhanced SpeedStep functionality is disabled.

Enabled

Enhanced SpeedStep functionality is enabled.

Turbo Mode

Allows the processor to run faster than the marked frequency if the OS requests the highest performance state (P0). This feature is also known as Intel® Turbo Boost Technology.

Disabled

Turbo Mode is disabled.

Enabled

Turbo Mode is enabled.

Package C State limit

Allows to configure processor C state limit.

C0

C0 is the C state limit.

C2

C1 is the C state limit.

C3

C1 is the C state limit.

C6

C6 is the C state limit.

C7

C7 is the C state limit.

C7S

C7S is the C state limit.

Auto

The C state limit is set to the lowest available C state.

4.5 Memory Status

DIMM-xx

Displays the current status of the memory modules.

Enabled

The system uses the memory module.

Disabled

The system does not use the memory module. It was manually disabled.

Failed

The system does not use the memory module. It was disabled automatically by the system after a memory error. If you have replaced a defective memory module, you must set the entry to *Enabled* again.

Empty

There is no memory module populated.

4.6 SATA Configuration

The following parameters can be set in this menu. Some of them are only available under special preconditions.

SATA Mode

Defines in which mode the SATA ports operate.

AHCI Mode

SATA interface is in AHCI Mode.

RAID Mode

SATA interface is in RAID Mode.

4.7 CSM Configuration

Opens the submenu of Compatibility Support Module (CSM) for configuration.

i This submenu is only available when the "Secure Boot Control" menu under Setup/Secure Boot Configuration is deactivated.

Launch CSM

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

Enabled

The CSM is executed so that a Legacy or UEFI operating system can be started.

Disabled

The CSM is not executed so that a only a UEFI operating system can be started.

Boot option filter

Specifies from which drives can be booted.

UEFI and Legacy

It is possible to boot with UEFI OS as well as with Legacy OS drives.

Legacy only

It is only possible to boot from drives with Legacy OS.

UEFI only

It is only possible to boot from drives with UEFI OS.

Launch PXE OpROM Policy

Specifies which PXE Option ROM will be started. For PXE boot there is available the normal (Legacy) PXE boot as well as a UEFI PXE boot.

Do not launch

No Option ROMs are started.

UEFI only

Only UEFI Option ROMs are started.

Legacy only

Only Legacy Option ROMs are started.

Launch Storage OpROM policy

Specifies which Storage Option ROM will be started.

Do not launch

No Storage Option ROMs are started.

UEFI only

Only UEFI Storage Option ROMs are started.

Legacy only

Only Legacy Storage Option ROMs are started.

Other PCI device ROM priority

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

UEFI only

Only UEFI Option ROMs are booted.

Legacy only

Only Legacy Option ROMs are booted.

4.8 Trusted Computing

Opens the submenu used to activate TPM and adjust TPM settings.

If this setup menu is available, the system board includes a security and encryption chip (TPM – Trusted Platform Module) that complies with TCG Specification 1.2 or 2.0. This chip allows security-relevant data (passwords etc.) to be stored securely. The use of TPM is standardised and is specified by the Trusted Computing Group (TCG).

TPM Support

Specifies whether the TPM (Trusted Platform Module) hardware is available.

If the TPM is disabled, the system behaves like any other system without TPM hardware.

Disabled

Trusted Platform Module is not available.

Enabled

Trusted Platform Module is available.

TPM State

Specifies if TPM (Trusted Platform Module) is useable by OS.

Disabled

Trusted Platform Module is not useable.

Enabled

Trusted Platform Module is useable.

Pending TPM operation

Schedules a TPM operation to be executed during next boot.

ℹ These menu entries are only visible if a TPM1.2 is installed.

None

No TPM operation will be executed.

Enable Take Ownership

Allows the OS to take ownership of the TPM.

Disable Take Ownership

Disallows the OS to take ownership of the TPM.

TPM Clear

TPM will be reset to factory default. All keys within the TPM will be cleared.

ℹ These menu entries are only visible if a TPM2.0 is installed.

None

No TPM operation will be executed.

TPM Clear

TPM will be reset to factory default. All keys within the TPM will be cleared.

TPM 1.2 Device Found

A TPM device following the TCG specification version 1.2 has been found.

TPM 2.0 Device Found

A TPM device following the TCG specification version 2.0 has been found.

TPM Enabled Status:

Displays if the TPM is useable.

TPM Active Status:

Displays if the TPM is activated.

TPM Owner Status:

Displays TPM owner status.

4.9 USB Configuration

USB Devices

Displays number of available USB devices, USB keyboards, USB Mouse and USB Hubs.

Legacy USB Support

Specifies whether Legacy USB Support is available. This function has to be enabled or set to Auto if it may be necessary to boot the operating system from a USB device.

Disabled

Legacy USB Support is not available. A USB keyboard or USB mouse can only be used if supported by the operating system. The operating system cannot be booted from a USB device

Enabled

Legacy USB Support is available. The USB keyboard or USB mouse can also be used with operating systems that do not support USB. The operating system can be booted from a USB device.

Auto

Legacy USB Support will be disabled if no USB devices are connected.

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

Onboard USB Controllers

Allows the USB controllers on the system board to be enabled or disabled. If the onboard USB controllers are disabled, all USB devices connected are not available. Besides locally connected keyboard, mouse and mass storage, also keyboard, mouse and mass storage via iRMC and internally connected USB devices do not work.

Enabled

Onboard USB controllers are enabled and work as configured.

Disabled

Onboard USB controllers are disabled.

Mass Storage Device(s)

Allows the user to force a specific device emulation. If *Auto* is selected the devices are emulated according to their media format. Optical drives are emulated as *CD-ROM*, drives without media will be emulated according to the drive type.

Auto

Emulation is selected according to the USB device.

Floppy

Forces USB Floppy emulation.

Hard Disk

Forces USB Hard Disk emulation.

CD-ROM

Forces USB CD-ROM emulation.

4.9.1 USB Port Security

Opens the submenu to configure availability of USB Ports.

USB Port Control

Configures the usage of the USB ports. Any disabled USB ports are neither available during POST nor are they available under the operating system.

Enable all ports

All USB ports are enabled.

Enable front and internal ports

All front and internal USB ports are enabled.

Enable rear and internal ports

All rear and internal USB ports are enabled.

Enable internal ports only

Only the internal USB ports are enabled.

4.10 Super IO Configuration

Displays System Super IO Chip Parameters.

Super IO Chip

Displays information about Super IO Chip.

4.10.1 Serial Port 1 Configuration

Set Parameters of Serial Port 1 (COMA).

Serial Port

Specifies whether the serial port is available.

Disabled

The serial port is not available.

Enabled

The serial port is available.

Device Settings

Displays the base I/O address and the interrupt used to access the corresponding serial port, e.g. IO=3F8h; IRQ=4.

Change Settings

Selects the base I/O address and the interrupt used to access the corresponding serial port.

Auto
[*IO=3F8h; IRQ=4;*]
[*IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12;*]
[*IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12;*]
[*IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12;*]
[*IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;*]

The serial port uses the selected address and interrupt from the list above. In case of a resource conflict the setting might be changed to 'Auto'.

4.11 Network Stack Configuration

Network Stack

Configures whether the UEFI Network Stack is available for network access under UEFI. E.g.: is the UEFI Network Stack not available there is no UEFI installation possible via PXE.

Disabled

The UEFI Network Stack is not available.

Enabled

The UEFI Network Stack is available.

Ipv4 PXE Support

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

Disabled

PXE UEFI Boot via Ipv4 is not available.

Enabled

PXE UEFI Boot via Ipv4 is available.

Ipv6 PXE Support

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

Disabled

PXE UEFI Boot via Ipv6 is not available.

Enabled

PXE UEFI Boot via Ipv6 is available.

4.12 Option ROM Configuration

Launch Slot n OpROM

Controls if legacy Option ROMs of expansion cards mounted in this slot shall be started.

Disabled

Does not start Option ROMs of expansion cards in this slot.

Enabled

Starts Option ROMs of expansion cards in this slot.

4.13 VIOM Configuration

VIOM-flag

The Virtual IO-Manager flag is used to enable or disable the IO-virtualization. Being enabled, the Virtual IO-Manager software is able to provide so called profiles to virtualize IO addresses (WWNs and MAC) and to configure and deconfigure known onboard IO devices as well as expansion cards. The application of these profiles also allows to overwrite the boot sequence if desired.

Disabled

Virtual IO-Manager is not able to virtualize. Virtual IO-manager can be selected by the BIOS.

Enabled

Virtual IO-Manager may virtualize. Virtual IO-Manager can be selected by the Virtual IO-Manager only.

Within the setup it is only possible to disable this feature. Once disabled it has to be re-enabled again, using the OS based Virtual IO-Manager software.

4.14 iSCSI Configuration

If a UEFI driver for a LAN/CNA controller (onboard CNA or PCIe card) is loaded the parameter for booting via iSCSI can be configured here. The menu is intended for UEFI drivers only. The menu does not apply to legacy OpROMs.

If no UEFI driver for a LAN/CNA controller is loaded or there is no LAN/CNA controller present in the system, this menu is not used.

4.15 UEFI Device Driver Setup

An UEFI Device Driver might support an interface to UEFI FW Setup and provides a list of information and control items. Available UEFI Device Drivers are for example Intel® Ethernet Connection I217-LM and Intel® I210 Gigabit.

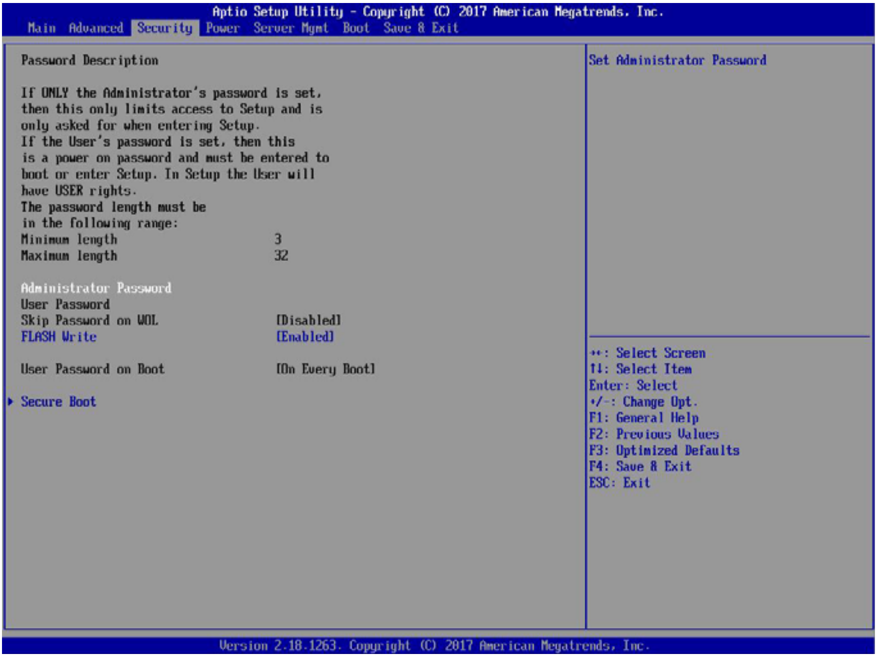
4.16 Driver Health

If a UEFI driver of a PCI express device supports the Driver Health Protocol, the UEFI firmware can query the UEFI driver for the health status of the devices it is managing.

The health states of the UEFI drivers supporting the Driver Health interface are displayed in this menu.

5 Security menu

The following parameters can be set in this menu. Some of them are only available under special preconditions.



```
                 Aptio Setup Utility - Copyright (C) 2017 American Megatrends, Inc.
   Main  Advanced  Security  Power  Server Mgmt  Boot  Save & Exit

 Password Description                                    Set Administrator Password

 If ONLY the Administrator's password is set,
 then this only limits access to Setup and is
 only asked for when entering Setup.
 If the User's password is set, then this
 is a power on password and must be entered to
 boot or enter Setup. In Setup the User will
 have USER rights.
 The password length must be
 in the following range:
 Minimum length                    3
 Maximum length                    32

 Administrator Password
 User Password
 Skip Password on WOL              [Disabled]
 FLASH Write                       [Enabled]
                                                         →←: Select Screen
 User Password on Boot             [On Every Boot]       ↑↓: Select Item
                                                         Enter: Select
▸ Secure Boot                                            +/-: Change Opt.
                                                         F1: General Help
                                                         F2: Previous Values
                                                         F3: Optimized Defaults
                                                         F4: Save & Exit
                                                         ESC: Exit

                 Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```

Figure 4: Example for the "Security" menu

Neither administrator nor user password is assigned

Entering BIOS setup utility as well as booting the system are unrestricted.

Only administrator password is assigned

If ONLY administrator password is assigned solely the BIOS setup utility is protected. Booting the system is unrestricted. In case of entering BIOS setup utility with administrator password you will obtain administrator level and have full access to BIOS setup utility. Entering BIOS setup utility without password results in limited BIOS setup utility access as you only obtain user level.

Only user password is assigned

If ONLY user password is assigned the BIOS setup utility as well as booting the system are protected by user password. In case of entering BIOS setup utility with user password the user obtains administrator level and has full access to BIOS setup utility. Entering the BIOS setup utility without password is prohibited.

Administrator AND user password are assigned

If administrator and user password are assigned the BIOS setup utility rights depend on the entered password. Entering BIOS setup utility with administrator password results in full BIOS setup utility access, typing the user password results in limited access. Booting the system is possible with user password as well as with administrator password.

> ℹ Deleting Administrator Password clears the User Password as well.

The system shuts down after three times password attempts. If this happens, turn off the server, turn it back on, and then enter the correct password.

Administrator Password

When you press the Enter key, a window opens where you can define the administrator password. Enter a character string to define a password. If you confirm an empty password field, the password will be deleted.

> ℹ To call up the complete BIOS setup utility, you need the administrator access level. If the administrator password is assigned the user password allows only a very limited access to the BIOS setup utility.

User Password

When you press the Enter key, a window opens where you can define the user password. Enter a character string to define a password. The user password prevents unauthorized access to your system.

Skip Password on WOL

Establishes whether the user password is bypassed or must be entered when booting with Wake On LAN.

Disabled

The user password must be entered via the keyboard when booting the operating system.

Enabled

The user password is deactivated when booting with Wake On LAN.

FLASH Write

Assigns write protection to the system BIOS.

Disabled

The system BIOS cannot be written. Flash-BIOS update is not possible.

Enabled

The system BIOS can be written. Flash BIOS update is possible.

Password on Boot

Specifies whether a User Password prompt appears when booting.

On every Boot

The password prompt appears on all boot.

On first Boot

Entering the user password is required before each cold boot.

Disabled

The password is always taken from non-volatile storage and there is no password prompt displayed.

Secure Boot

Calls a submenu used to define a firmware authentication process (see "Secure Boot" on page 40).

5.1 Secure Boot

Opens the submenu for configuring *Secure Boot*.

Secure Boot defines a firmware execution authentication process.

As an industry standard, *Secure Boot* defines how platform firmware manages certificates, authenticates firmware, and how the operating system interfaces with this process.

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

System Mode

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

User

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

Setup

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

Platform Mode

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

User

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

Setup

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

Secure Boot Control

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

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

Disabled

All boot loaders / OpROMs (Legacy / UEFI) can be executed.

Enabled

Only booting of signed boot loaders / UEFI OpROMs is permitted.

Secure Boot Mode

Specifies whether the *Key Management* submenu is available.

Standard

The *Key Management* submenu is not available.

Custom

The *Key Management* submenu is available.

5.1.1 Key Management

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

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

Provision Factory Default Keys

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

Disabled

The available Secure Boot key and signature databases remain unchanged.

Enabled

If the PK, KEK, DB, DBT, DBX signature databases are not available, the default Secure Boot key and signature databases will be installed after rebooting the system.

Enroll All Factory Default Keys

This menu item is only visible when *Provision Factory Default Keys* is set to *Enabled*.

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

Delete All Secure Boot Variables

> i This menu item is only visible when *Provision Factory Default Keys* is set to *Disabled*.

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

Save All Secure Boot Keys

Saves all keys and signature databases to the selected drive.

Secure Boot variable

Displays the size and key of the current security key.

Platform Key

Displays the popup window *Key Management*.

Set new key

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

Delete key

Deletes the *Key Exchange Key Database (KEK)*.

Key Exchange Keys

Displays the popup window *Key Management*.

Set new key

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

Append key

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

Delete key

Deletes the *Key Exchange Key Database (KEK)*.

Authorized Signatures

Displays the popup window *Key Management*.

Set new key

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

Append key

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

Delete key

Deletes the *Key Exchange Key Database (KEK)*.

Forbidden Signatures

Displays the popup window *Key Management*.

Set new key

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

Append key

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

Delete key

Deletes the *Key Exchange Key Database (KEK)*.

Authorized TimeStamps

Displays the popup window *Key Management*.

Set new key

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

Append key

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

OsRecovery Signatures

Displays the popup window *Key Management*.

Set new key

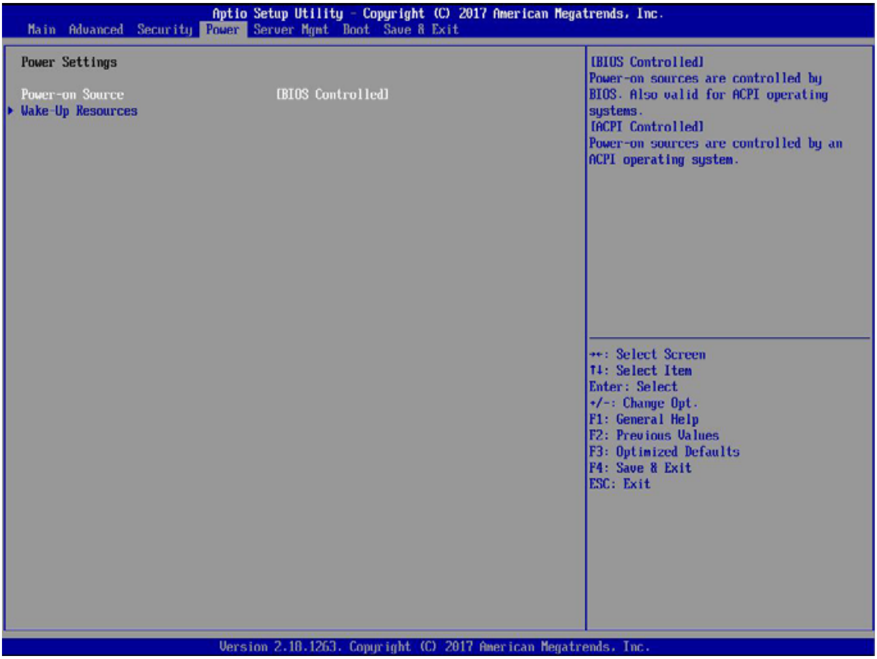
Sets the *Key Exchange Key Database (KEK)*. After selecting the drive, the corresponding file must be selected in the browser.

Append key

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

6 Power menu

The following parameters can be set in this menu. Some of them are only available under special preconditions.



```
             Aptio Setup Utility - Copyright (C) 2017 American Megatrends, Inc.
   Main  Advanced  Security  Power  Server Mgmt  Boot  Save & Exit

 Power Settings                                      [BIOS Controlled]
                                                     Power-on sources are controlled by
 Power-on Source              [BIOS Controlled]     BIOS. Also valid for ACPI operating
▸ Wake-Up Resources                                  systems.
                                                     [ACPI Controlled]
                                                     Power-on sources are controlled by an
                                                     ACPI operating system.

                                                     →←: Select Screen
                                                     ↑↓: Select Item
                                                     Enter: Select
                                                     +/-: Change Opt.
                                                     F1: General Help
                                                     F2: Previous Values
                                                     F3: Optimized Defaults
                                                     F4: Save & Exit
                                                     ESC: Exit

             Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```

Figure 5: Example for the "Power" menu

Power-on Source

Specifies whether the switch on sources for the system are managed by the BIOS or the ACPI operating system.

BIOS Controlled

The switch on sources are managed by the BIOS.

ACPI Controlled

The switch on sources are managed by the ACPI operating system.

6.1 Wake-Up Resources

LAN

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

Disabled

The system cannot be switched on via a LAN controller.

Enabled

The system can be switched on via a LAN controller.

Wake On LAN boot

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

Boot Sequence

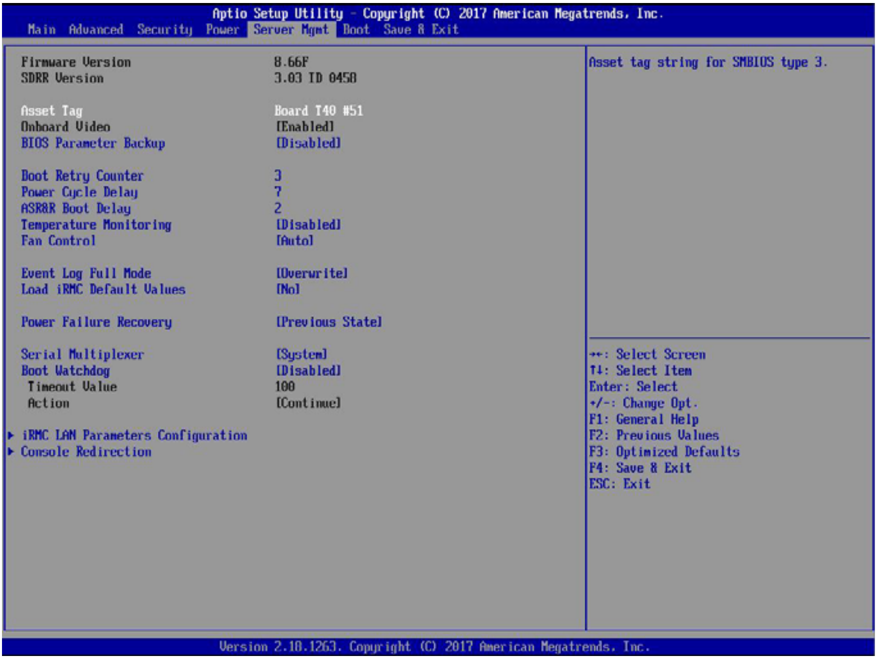
The system boots up according to the device sequence specified in the Boot menu when switched on via LAN.

Force LAN Boot

The system is booted remotely via LAN when switched on via LAN.

7 Server Mgmt menu

The following parameters can be set in this menu. Some of them are only available under special preconditions.



```
                 Aptio Setup Utility - Copyright (C) 2017 American Megatrends, Inc.
   Main  Advanced  Security  Power  Server Mgmt  Boot  Save & Exit

 Firmware Version                    8.66F                      Asset tag string for SMBIOS type 3.
 SDRR Version                        3.03 ID 0458

 Asset Tag                           Board T40 #51
 Onboard Video                       [Enabled]
 BIOS Parameter Backup               [Disabled]

 Boot Retry Counter                  3
 Power Cycle Delay                   7
 ASR&R Boot Delay                    2
 Temperature Monitoring              [Disabled]
 Fan Control                         [Auto]

 Event Log Full Mode                 [Overwrite]
 Load iRMC Default Values            [No]

 Power Failure Recovery              [Previous State]
                                                                →←: Select Screen
 Serial Multiplexer                  [System]                   ↑↓: Select Item
 Boot Watchdog                       [Disabled]                 Enter: Select
  Timeout Value                      100                        +/-: Change Opt.
  Action                             [Continue]                 F1: General Help
                                                                F2: Previous Values
▶ iRMC LAN Parameters Configuration                             F3: Optimized Defaults
▶ Console Redirection                                           F4: Save & Exit
                                                                ESC: Exit

                 Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```

Figure 6: Example for the "Server Mgmt" menu

Asset Tag

Displays the *Asset Tag* field of SMBIOS Type 3 (system housing or chassis). For changing or inserting the *Asset Tag* select this setup option and press the [Enter] key. A window opens and you can type a character string or change the existing character string. Only alpha-numeric entries are allowed.

BIOS Parameter Backup

Specifies whether the BIOS setup parameters are automatically transferred to the iRMC at each system start. Allows to backup the BIOS parameters to a file on a local system similar to the iRMC's settings. The BIOS parameter file can be edited afterwards. A restore operation, i.e. uploading it back to the iRMC, applies the changed parameters to the BIOS with the next reboot.

Disabled

The BIOS setup parameters are not automatically transferred to the iRMC at each system start. A particular request of the iRMC to the BIOS is necessary to get the BIOS setup parameters on the next system start.

Enabled

The BIOS setup parameters are automatically transferred to the iRMC at each system start. This may increase the time for the system start for some seconds.

Onboard Video

The graphics controller on the system board can be deactivated if a display card is installed in the system.

Disabled

The graphics controller on the system board is disabled.

Enabled

The graphics controller on the system board is enabled.

Boot Retry Counter

Specifies the maximum number of attempts to boot the operating system. Each failed attempt is followed by a system reboot after the time set in *Boot Watchdog* has expired. Other critical system errors also result in a system reboot and a counter decrement. After the last attempt, the system is ultimately powered off.

Allowed values are: *0* to *7* number of possible retries

Pressing the + key or the - key increases or decreases this value.

Power Cycle Delay

Specifies the minimum time that must be expired before the system can be switched on again after it has been switched off.

Allowed values are: 0 sec. to 15 sec.

Pressing the + key or the - key increases or decreases this value.

ASR&R Boot Delay

Specifies the system reboot delay after the system shuts down as a result of an error (e.g. excessively high temperature). The system is rebooted after the set wait time has expired.

Allowed values are: 1 min. to 30 min.

Pressing the + key or the - key increases or decreases this value.

Temperature Monitoring

Specifies if a system power-on request is executed, depending on the ambient temperature.

Disabled

A system power-on request is executed independent of the ambient temperature.

Enabled

Prevents a system power-on if the ambient temperature is above the upper threshold value or below the lower threshold value.

Fan Control

Controls the speed of the fans. Depending on the system configuration and applications used, you can change the preset mode.

Auto

The fan speed is adjusted automatically. Trade-off between system temperature and CPU performance.

Full

All fans are set to full speed.

Event Log Full Mode

Specifies whether or not the System Event Log can be overwritten.

Overwrite

If the System Event Log is full, additional events overwrite the oldest entries in the System Event Log. In this case, newer events are more important than older events.

Maintain

If the System Event Log is full, no further events are entered. The System Event Log file must be cleared first before additional events can be entered. In this case, older events are more important than newer events.

Load iRMC Default Values

Specifies whether the iRMC default values are loaded or not.

No

No action is taken.

Yes

The iRMC default values are loaded when you choose *Save Changes and Exit* to exit the BIOS setup utility. Any BIOS setup utility settings that affect the iRMC are not lost by this setting. They are sent to the iRMC after the iRMC default values are loaded and therefore overwrite the corresponding values again.

The setting is automatically set to *No* after the default values are loaded.

Power Failure Recovery

Specifies the system restart behavior after a power failure.

Always Off

The system performs a status check and then switches off.

Previous State

The system performs a status check and then returns the mode it was in before the power failure occurred (*On* or *Off*).

Always On

The system performs a status check and then switches on.

For the UPS scheduled operation, set it to *Always On*. Otherwise, the server may not be turned on at the set time.

ℹ All wake up sources are reconfigured during the short initialization process. The system can be woken up via LAN etc.

Serial Multiplexer

Specifies whether the serial interface can be used by the system.

System

The serial interface can be used by the system or the operating system.

iRMC

The serial interface can only be used by the iRMC. The operating system cannot use this serial interface.

Boot Watchdog

Specifies whether the system is restarted if the server management process (ServerView Agent) is unable to establish a connection with the iRMC. After a successful operating system start-up the ServerView Agent starts the communication with the iRMC within a specified period.

The iRMC assumes a start-up error if a timeout occurs and may restart the system to recover from this error.

Disabled

The iRMC does not restart the system on *Boot Watchdog Timeout Value*. This selection must be used if ServerView is not installed to avoid inadvertently system restarts by the iRMC.

Enabled

The iRMC restarts the system on *Boot Watchdog Timeout Value*, because it assumes an operating system start-up error.

If Enabled is set, the server may not operate as intended. For example, the server may automatically turn off or restart without any commands.

– When starting up the system by using ServerView Suite, be sure to disable the *Boot Watchdog*, even when ServerView Agent has been installed on the system. If the system starts up with this item enabled, the server may not operate as intended. For example, the server may automatically turn off or restart without any commands.

– When setting this function, refer to ServerView Suite manuals.

Timeout Value

Specifies the time after which the system is rebooted if enabled via *Boot Watchdog.*
Allowed values are 0...100

0

Time monitoring is disabled.

1...100

The system is rebooted after the selected time (in minutes) has expired.

Pressing the + key or the - key increases or decreases this value.

Action

Determines the action taken after the boot watchdog expires.

Continue

The system continues to run.

Reset

The system is restarted by a system reset.

Power Cycle

The system is restarted by a power cycle.

iRMC LAN Parameters Configuration

Calls a submenu used to make settings for the Remote Management Controller (see "iRMC LAN Parameters Configuration" on page 52).

Console Redirection

Calls a submenu used to make settings for the terminal communication (see "Console Redirection" on page 56).

7.1 iRMC LAN Parameters Configuration

The following parameters can be set in this menu. Some of them are only available under special preconditions.

Management LAN

Enables the LAN interface, which can be used by the iRMC.

Disabled

The iRMC LAN interface is disabled.

Enabled

The iRMC LAN interface is enabled.

iRMC MAC Address

Shows the MAC address of the iRMC. The iRMC MAC address is divided in blocks, separated by colons.

Management LAN Port

Specifies which LAN interface can be used by the iRMC. The iRMC and the onboard LAN can share the LAN interface or the iRMC can use a separate LAN interface. The Management LAN interface is indicated by a screw-wrench icon.

Management

The iRMC uses a separate LAN interface.

Shared

The iRMC and the onboard LAN share the LAN interface.

Management LAN Speed

Specifies the speed for the management LAN port.

Auto

The speed is automatically negotiated by the LAN controller.

100 Mbit/s Full Duplex

Maximum speed at 100 Mbit/s. Simultaneous transmission in both directions is possible.

100 Mbit/s Half Duplex

Maximum speed at 100 Mbit/s. Transmission is only possible in one direction at a time.

10 Mbit/s Full Duplex

Fixed speed at 10 Mbit/s. Simultaneous transmission in both directions is possible.

10 Mbit/s Half Duplex

Fixed speed at 10 Mbit/s. Transmission is only possible in one direction at a time.

1000 Mbit/s

Maximum speed at 1000 Mbit/s.

Management VLAN

Enables the support of IEEE 802.1q VLAN (virtual LAN) headers for IPMI over IP sessions on IEEE 802.3 Ethernet.

Enabled

Enables the support of IEEE 802.1q VLAN (virtual LAN) headers for IPMI over IP sessions on IEEE 802.3 Ethernet.

Disabled

Disables the support of IEEE 802.1q VLAN (virtual LAN) headers for IPMI over IP sessions on IEEE 802.3 Ethernet.

VLAN ID

Value the VLAN headers are tagged with.
Allowed values are: *0 ... 4094*

VLAN Priority

Value for the VLAN user priority field to be used.
Allowed values are: *0 ... 7*

iRMC IPv4 LAN Stack

Configures whether the *IPv4 LAN Stack* is available for the iRMC.

Disabled

The *IPv4 LAN Stack* is not available for the iRMC.

Enabled

The *IPv4 LAN Stack* is available for the iRMC.

IP configuration

Specifies whether DHCP (Dynamic Host Configuration Protocol) support for the iRMC is used. An IP address can automatically be assigned to iRMC from a DHCP server in the network via the DHCP network protocol.

use DHCP

The DHCP support for the iRMC is used. Local IP Address, Subnet Mask, and Gateway Address will be requested from the DHCP server.

use static configuration

The DHCP support for the iRMC is disabled. Local IP Address, Subnet Mask, and Gateway Address have to be entered manually.

IP Address

Specifies IP address of the iRMC.
Numeric values from 0 to 255 are possible.

Subnet Mask

Specifies the subnet mask of the iRMC. Uses the same subnet mask as in the operating system.
Numeric values from *0 to 255* are possible.

Gateway Address

Specifies the gateway address of the iRMC.
Numeric values from *0 to 255* are possible.

iRMC IPv6 LAN Stack

Configures if the *IPv6 LAN Stack* of the iRMC is available.

Disabled

The *IPv6 LAN Stack* of the iRMC is not available.

Enabled

The *IPv6 LAN Stack* of the iRMC is available.

Unique Local Address

Displays the IPv6 address. The IP address is split into blocks separated by colons.

Link Local address

Displays the IPv6 address. The IP address is split into blocks separated by colons.

IPv6 Router

Displays the address of the IPv6 router. The IP address is split into blocks separated by colons.

IPv6 Gateway

Displays the address of the IPv6 gateway. The IP address is split into blocks separated by colons.

7.2 Console Redirection

The following parameters can be set in this menu. Some of them are only available under special preconditions.

Console Redirection

Specifies the interface used for communication with the terminal.

Disabled

The terminal interface is disabled.

Serial 1

The terminal uses the first serial interface.

Baud Rate

Specifies the transfer rate for communication with the terminal. This setting must be identical on both terminal and server.

Allowed values are:
9600, 19.2 k, 38.4 k, 57.6 k, 115.2 k

The data is transferred to the terminal at the rate set.

Protocol

Shows the assigned console type.
This setting must be identical on both the terminal and the server.

Allowed values are:
VT100, PC ANSI, VT100+, VT-UTF8

The assigned console is used to transfer the data to the terminal.

Flow Control

This setting determines how the transfer via the interface is controlled. This setting must be identical on both terminal and server.

None

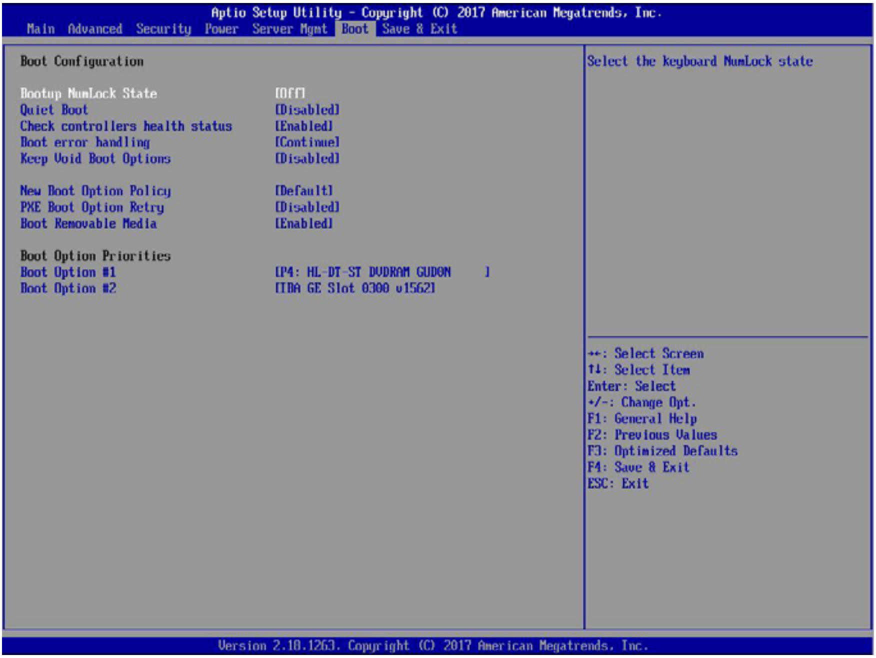
The interface is operated without transfer control.

CTS/RTS

The transfer control is performed by the hardware. This mode must also be supported by the cable.

8 Boot menu

The following parameters can be set in this menu. Some of them are only available under special preconditions.



```
                 Aptio Setup Utility - Copyright (C) 2017 American Megatrends, Inc.
   Main  Advanced  Security  Power  Server Mgmt  Boot  Save & Exit

 Boot Configuration                                       Select the keyboard NumLock state

 Bootup NumLock State              [Off]
 Quiet Boot                        [Disabled]
 Check controllers health status   [Enabled]
 Boot error handling               [Continue]
 Keep Void Boot Options            [Disabled]

 New Boot Option Policy            [Default]
 PXE Boot Option Retry             [Disabled]
 Boot Removable Media              [Enabled]

 Boot Option Priorities
 Boot Option #1                    [P4: HL-DT-ST DVDRAM GUD0N      ]
 Boot Option #2                    [IBA GE Slot 0300 v1562]
                                                          ++: Select Screen
                                                          ↑↓: Select Item
                                                          Enter: Select
                                                          +/-: Change Opt.
                                                          F1: General Help
                                                          F2: Previous Values
                                                          F3: Optimized Defaults
                                                          F4: Save & Exit
                                                          ESC: Exit

                 Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```

Figure 7: Example for the "Boot" menu

This menu can be used to define the sequence of the drives from which the system is booted. Up to eight drives (and also, for example, USB interfaces) can be listed.

For references to the operation please see the help area in this menu.

Bootup NumLock State

Determines the setting of the NumLock function when the system is started up. NumLock controls the usage of the numeric keypad.

On

NumLock is enabled and the numeric keypad can be used.

Off

NumLock is disabled and the cursor functions of the numeric keys can be used.

The Num indicator on the keyboard reports the current Bootup NumLock State. The Num key on the keyboard allows to toggle between On and Off.

Quiet Boot

The boot logo is displayed on the screen instead of the POST startup information.

Disabled

The POST startup information will be displayed on the screen.

Enabled

The boot logo is displayed.

Check Controllers Health Status

If a UEFI driver option ROM of a PCIe devices supports the Controller Health interface, the UEFI FW can query the UEFI driver option ROM for the health status of the devices it is managing.

Disabled

The controller health status is not checked by the UEFI FW.

Enabled

The UEFI FW checks the controller health status.

Boot error handling

Defines whether the system boot process is paused and the system halted when an error is detected.

Continue

The system boot is not paused. The error is ignored as far as possible.

Pause and wait for key

If an error is detected during POST the system boot pauses.

Keep Void Boot Options

Specifies if UEFI and legacy Boot Options for devices, which are no longer connected to the system will be removed from "Boot Option Priority" list. If enabled the void Boot Options will be preserved in the "Boot Option Priorities" list. This is useful to keep the boot order of the devices, that are temporarily disconnected from the system.

The difference between the two Setup questions “Keep Void Boot Options” and “Remove Invalid Boot Options” is the following:

The question “Keep Void Boot Options” will change only the policy of the UEFI and legacy boot options created by the system BIOS.

The question “Remove Invalid Boot Options” will change only the policy of the UEFI boot options created by parties outside of the BIOS (e.g. UEFI Windows).

Disabled

Boot Options will be removed from the "Boot Option Priority" list.

Enabled

Boot Options will not be removed from "Boot Option Priority" list.

New Boot Option Policy

Configures the rule of the Boot Option Priority list positioning for new boot options.

Default

No rule is applied which position is chosen for new boot devices.

Place First

New boot options are positioned at the beginning.

Place Last

New boot options are positioned at the end.

PXE Boot Option Retry

Specifies if NON-EFI based PXE boot options will be retried without waiting for user input.

Disabled

NON-EFI boot options would not be retried without waiting for user input.

Enabled

NON-EFI boot options will be retried without waiting for user input.

Boot Removable Media

Specifies if support for booting to removable devices such as USB-Stick is available.

Disabled

Booting to removable devices is deactivated.

Enabled

Booting to removable devices is activated.

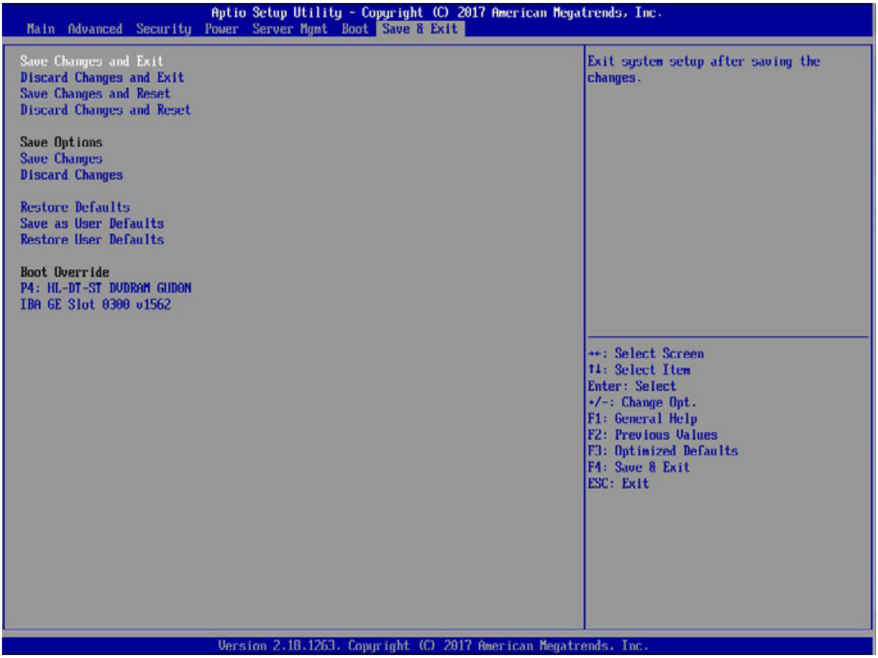
Boot Option Priorities

Displays the current boot order.

- ► Press the cursor keys [↑] or [↓] to select the device for which you want to change the boot order.
- ► Press the [+] key to increase the priority and the [-] key to decrease the priority for the selected device.
- ► Press the [Enter] key and select *Disabled* to remove the selected device from the boot order.

9 Save & Exit menu

The following parameters can be set in this menu.



```
Aptio Setup Utility - Copyright (C) 2017 American Megatrends, Inc.
Main  Advanced  Security  Power  Server Mgmt  Boot  Save & Exit

Save Changes and Exit                          Exit system setup after saving the
Discard Changes and Exit                       changes.
Save Changes and Reset
Discard Changes and Reset

Save Options
Save Changes
Discard Changes

Restore Defaults
Save as User Defaults
Restore User Defaults

Boot Override
P4: HL-DT-ST DVDRAM GUD0N
IBA GE Slot 0300 v1562
                                               →←: Select Screen
                                               ↑↓: Select Item
                                               Enter: Select
                                               +/-: Change Opt.
                                               F1: General Help
                                               F2: Previous Values
                                               F3: Optimized Defaults
                                               F4: Save & Exit
                                               ESC: Exit

Version 2.18.1263. Copyright (C) 2017 American Megatrends, Inc.
```

Figure 8: Example for the "Save & Exit" menu

Save Changes and Exit

To save the current menu entries and exit the BIOS setup utility, select *Save Changes and Exit* followed by *Yes*.
The new settings will be effective and the POST continues as long as no changed option requires a reset.

Discard Changes and Exit

Select *Discard Changes and Exit* followed by *Yes* to discard the changes you have made since entering BIOS setup utility or since invoking *Save Changes*.
The BIOS setup utility will be closed and the POST continues.

Save Changes and Reset

To save the current menu entries and exit the BIOS setup utility, select *Save Changes and Reset* followed by *Yes*.

A reset is initiated and the new settings will be effective.

Discard Changes and Reset

Select *Discard Changes and Reset* followed by *Yes* to discard the changes you have made since entering BIOS setup utility or since invoking *Save Changes*.
The BIOS setup utility will be closed and a reset is initiated.

Save options

Save Changes

Select *Save Changes* followed by *Yes* to safe the changes you have made so far without leaving BIOS setup utility.

Discard Changes

Select *Discard Changes* followed by *Yes* to discard the changes you have made since entering BIOS setup utility or since invoking *Save Changes* without leaving BIOS setup utility.

Restore Defaults

To reset all BIOS setup utility menus to use default values, select *Restore Defaults* followed by *Yes*.
If you want to exit BIOS setup utility with these settings, select *Save Changes and Exit* followed by *Yes*.

Save as User Defaults

Select *Save as User Defaults* followed by *Yes* to save the changes you have done so far as user defaults.

Restore User Defaults

To reset all BIOS setup utility menus to use user default values, select *Restore User Defaults* followed by *Yes*. If you want to exit BIOS setup utility with these settings, select *Save Changes and Exit* followed by *Yes*.

Boot Override

Use the ↑ and ↓ cursor keys to select the drive from which you want to start the operating system. Press Enter to initiate the boot from the selected drive.

10 Flash BIOS Update

To perform a Flash BIOS update you must first download the necessary files from the internet.

CAUTION!

The BIOS is stored in a flash memory device. If an error occurs during the Flash BIOS update procedure, the BIOS image in the flash memory may be destroyed. You can then only restore the BIOS using the *Flash Memory Recovery Mode*, see "Flash Memory Recovery Mode" on page 65. If this is also not possible, the flash memory device has to be replaced. Contact your customer support Service Desk.

- ► Preventively note down the settings in the BIOS setup utility. A Flash BIOS update does not normally affect the settings in the BIOS setup utility.
- ► Call up the following internet page: *http://support.ts.fujitsu.com/Download*

For the Japanese market please use the URL:

http://jp.fujitsu.com/platform/server/primergy/bios/

- ► Select your system via *Select Product* or look under *Product Search by Serial-/Identnumber* for your system.
- ► Click on *Driver & Downloads* and then select your operating system.
- ► Select *Flash-BIOS*.

Flash BIOS Update - Desk Flash Instant

- ► Download the file *Flash BIOS Update - Desk Flash Instant* for a Flash BIOS Update under Windows.

Admin package - Compressed Flash Files

- ► If the operating system which you use is not selectable select any operating system and download the file *Admin package - Compressed Flash Files* for a Flash BIOS Update with a USB stick.

Flash BIOS Update under Windows

- ► Boot the operating system.

The execution of *Desk Flash Instant* is limited to Administrator Privileges.

- Open the Windows explorer, select the downloaded *Flash BIOS Update - Desk Flash Instant* and start the Flash BIOS Update with a double click. Then follow the instructions on the screen.
- After the Flash BIOS Update the system is restarted automatically. It will be booted with the new BIOS revision.
- Check the settings in the BIOS setup utility. If necessary, reconfigure the settings again.

Flash BIOS Update with a USB stick

- Make sure, that you have a bootable USB stick.

> If your USB stick is not bootable proceed as follows:
>
> - Select under *Admin package - Compressed Flash Files* the menu item *Installation Description - More information*.
> - Follow the instructions.
>
>   You need a USB stick on which the BIOS update files will be stored. The data on the USB stick will be fully erased and overwritten.
>
>   Make sure, that all data are saved before.
> - Unzip the downloaded zip file from *Admin package - Compressed Flash Files* and copy all files and directories to the root of your bootable USB stick.

- Boot the system from the inserted bootable USB stick.
- Wait until the screen output appears.
- Press the function key [F12] and select the bootable USB stick with the arrow keys [↑] and [↓].
- Change the directory with `cd DOS` and start the Flash BIOS Update with the command `DosFlash`. Then follow the instructions on the screen.
- After the Flash BIOS Update the system is restarted automatically. The system will be booted with the new BIOS revision.
- Check the settings in the BIOS setup utility. If necessary, reconfigure the settings again.

10.1 Flash Memory Recovery Mode

- Prepare a bootable USB stick as described in section *Flash BIOS Update with a USB stick*.
- Switch off the system and disconnect the power plug.
- Open the chassis and switch on "Recovery" (BIOS-RCVR) using the jumper / DIP switch on the system board.
- Reconnect the power plug and boot the system with the inserted bootable USB stick.
- Boot the system from the inserted bootable USB stick.
- Change the directory with `cd DOS` and start the Flash BIOS Update with the command `DosFlash`. Then follow the instructions on the screen.
- Observe the update process on the screen, until it is finished. The recovery update may take several minutes.
- Switch-off the system and disconnect the power plug.
- Remove the USB stick.
- Return the "Recovery" (BIOS-RCVR) jumper / DIP switch which have been changed to the initial position.
- Reconnect the power plug and switch on the system.
  The system will be booted with the new BIOS revision.
- Check the settings in the BIOS setup utility. If necessary, reconfigure the settings again.

Index

13

A
Above 4G Decoding 20
Access Level 14
Action 51
Active Processor Cores 21
Adjacent Cache Line Prefetch 22
Administrator Password 38
ASPM Support 19
ASR&R Boot Delay 49
Asset Tag 47
Authorized Signatures 43
Authorized TimeStamps 43

B
Baud Rate 56
BIOS Parameter Backup 48
BIOS setup
  exiting 12
  menu overview 7
  open 9
Boot error handling 58
Boot menu
  open immediately 9
Boot option filter 26
Boot Option Priorities 60
Boot Override 62
Boot Removable Media 60
Boot Retry Counter 48
Boot Watchdog 50
Bootup NumLock State 58

C
Change Settings 34
Check Controller Health Status 58
Console Redirection 52, 56

D
DCU Streamer Prefetcher 22
Delete All Secure Boot Variables 42
Device Settings 33
DIMM-xx 25
Discard Changes 62
Discard Changes and Exit 61
Discard Changes and Reset 62
DMI Control 20

E
Enhanced SpeedStep 24
Enroll All Factory Default Keys 41
Event Log Full Mode 49

F
Fan Control 49
FLASH Write 39
Flow Control 56
Forbidden Signatures 43

G
Gateway Address 54

H
Hardware Prefetcher 22
Hyper-Threading 21

I
Intel TXT (LT) Support 23
Intel Virtualization Technology 23
IP Address 54
IP configuration 54
Ipv4 PXE Support 34
IPv6 Gateway 55
Ipv6 PXE Support 34
IPv6 Router 55
iRMC IPv4 LAN Stack 53
iRMC IPv6 LAN Stack 54
iRMC LAN Parameters
  Configuration 52
iRMC MAC Address 52

K
Keep Void Boot Options 59
Key Exchange Keys 42

L
LAN n Controller 18
LAN n Oprom 18
Launch CSM 26
Launch PXE OpROM Policy 27
Launch Slot n OpROM 35
Launch Storage OpROM policy 28
Link Local Address 54
Load iRMC default Values 49

M
Management LAN 52
Management LAN Port 52
Management LAN Speed 52
Management VLAN 53
Mass Storage Device(s) 32

N
Network Stack 34
New Boot Option policy 59

O
Onboard USB Controllers 31
Onboard Video 48
OsRecovery Signatures 44
Other PCI device ROM priority 28

P
Package C State limit 25
PCI Slot n 19, 35
Pending TPM operation 29
Platform Key 42
Platform Mode 40
Power Cycle Delay 48
Power Failure Recovery 50
Power-on Source 45
Protocol 56
Provision Factory Default Keys 41
PXE Boot Option Retry 59

Q
Quiet Boot 58

R
Restore Defaults 62
Restore User Defaults 62

S
SATA Mode 26
Save as User Defaults 62
Save Changes 62
Save Changes and Exit 61
Save Changes and Reset 61
Save Secure Boot Keys 42
Secure Boot 40
Secure Boot Mode 41
Serial Multiplexer 50
Serial Port 33
Skip Password on WOL 39
Subnet Mask 54
Super IO Chip 33
System 40
System Date 14
System Information 13
System Language 13
System Time 14

T
Temperature Monitoring 49
Timeout Value 51
TPM 1.2 Device Found 30
TPM 2.0 Device Found 30
TPM Active Status 30
TPM Enabled Status 30
TPM Owner Status 30
TPM State 29
TPM Support 28
Turbo Mode 24

U
Unique Local Address 54
USB Devices 31
USB Legacy Support 31
USB Port Control 33

User Password 38

V

VLAN ID 53

VLAN Priority 53

VT-d (Virtualization Technology) 23

W

Wake-Up resource

- LAN 46

Wake-Up Resource Wake On LAN

- boot 46