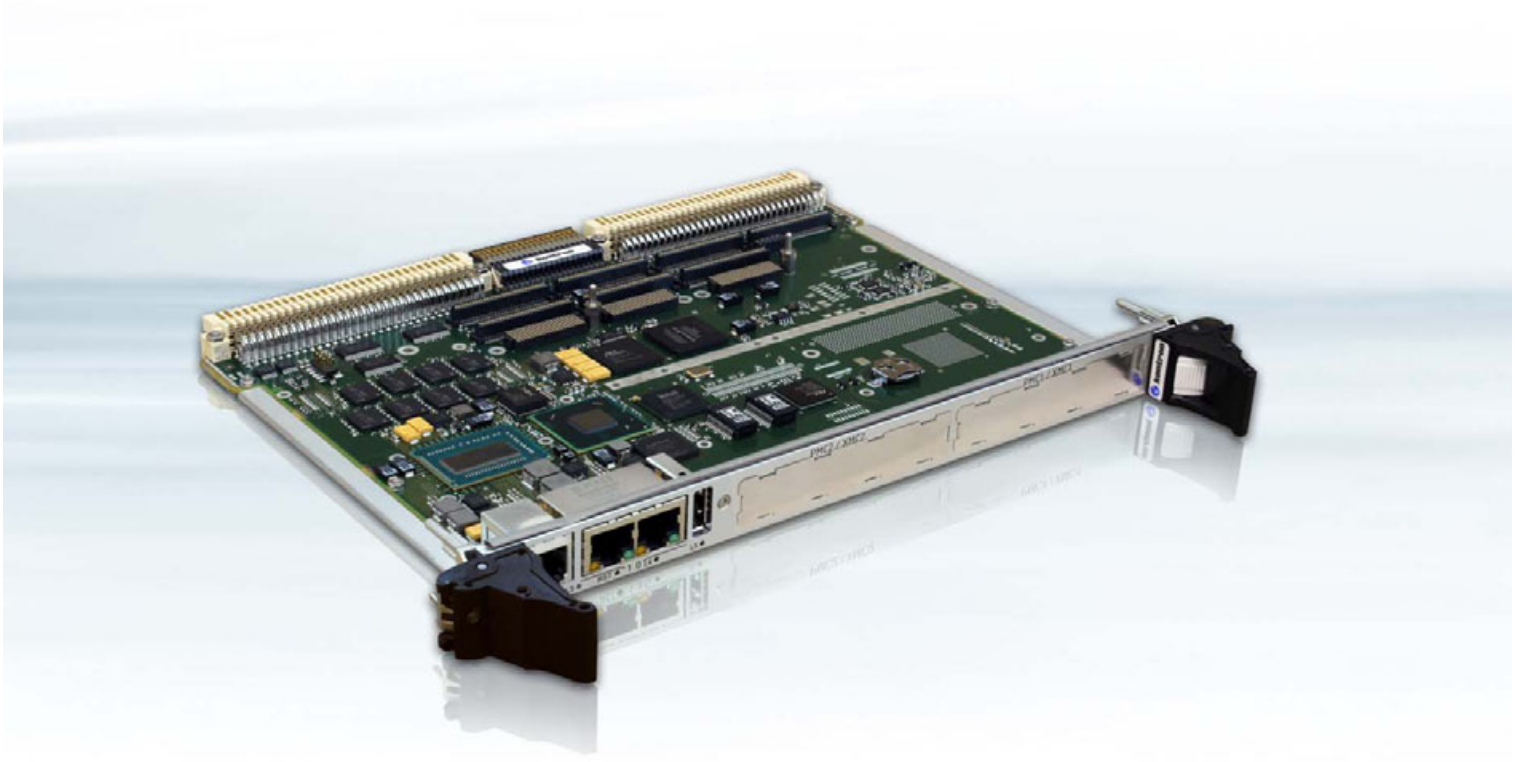
USER REFERENCE MANUAL



VM6052 & VM6054 AMI BIOS

SD.DT.G34-7e - May 2017

POSSIBILITIES START HERE kontron

VM6052/VM6054 AMI BIOS User Reference Manual

Disclaimer

Kontron would like to point out that the information contained in this manual may be subject to alteration, particularly as a result of the constant upgrading of Kontron products. This document does not entail any guarantee on the part of Kontron with respect to technical processes described in the manual or any product characteristics set out in the manual. Kontron assumes no responsibility or liability for the use of the described product(s), conveys no license or title under any patent, copyright or mask work rights to these products and makes no representations or warranties that these products are free from patent, copyright or mask work right infringement unless otherwise specified. Applications that are described in this manual are for illustration purposes only. Kontron makes no representation or warranty that such application will be suitable for the specified use without further testing or modification. Kontron expressly informs the user that this manual only contains a general description of processes and instructions which may not be applicable in every individual case. In cases of doubt, please contact Kontron.

Lise-Meitner-Str. 3-5

86156 Augsburg

Germany

www.kontron.com

REVISION HISTORY

PUBLICATION TITLE:	VM6052/VM6054 AMI BIOS User Reference Manual	
DOC. ID:	SD.DT.G34-7e	
Revision	Brief Description of Changes	Date of Issue
7e	New release ID17123 Updated section: - 11.2 Known problems table	05-2017
6e	New release ID17087 Updated sections: - 10.1.28 kvpd - 11.2 Known problems table New section: - 11.11 BIOS ID17087 Release Notes	04-2017
5e	Updated sections: - 10.1.27 ktemp - 11.1 Recommendations and Known Limitations	04-2016
4e	New section: 11.2 - Known Problems Table Section 5.11 -Thermal Configuration- Updated	03-2016
3e	New release ID 16008	01-2016
2e	Updated sections: - 6.1 Graphics Configuration - 11.1 Recommendations and Known Limitations - 11.7 BIOS ID15034 Release Notes New section: -10.2.2 Bootdelay	07-2015
1e	New release ID 15127	05-2015
0e	Initial Version	04-2014

Customer Support

Please contact our support team at support.KFR@kontron.com

Customer Service

As a trusted technology innovator and global solutions provider, Kontron extends its embedded market strengths into a services portfolio allowing companies to break the barriers of traditional product lifecycles. Proven product expertise coupled with collaborative and highly-experienced support enables Kontron to provide exceptional peace of mind to build and maintain successful products.

For more details on Kontron's service offerings such as: enhanced repair services, extended warranty, Kontron training academy, and more visit http://www.kontron.com/support-and-services/services.

Customer Comments

If you have any difficulties using this manual, discover an error, or just want to provide some feedback, contact Kontron support. Detail any errors you find. We will correct the errors or problems as soon as possible and post the revised manual on our website.

SYMBOLS

The following symbols may be used in this manual:

⚠DANGER	DANGER indicates a hazardous situation which, if not avoided, will result in death or serious injury.
⚠WARNING	WARNING indicates a hazardous situation which, if not avoided, could result in death or serious injury.
⚠CAUTION	CAUTION indicates a hazardous situation which, if not avoided, may result in minor or moderate injury.
NOTICE	NOTICE indicates a property damage message.
	**Electric Shock!** This symbol and title warn of hazards due to electrical shocks (> 60 V) when touching products or parts of them. Failure to observe the precautions indicated and/or prescribed by the law may endanger your life/health and/or result in damage to your material.
	**ESD Sensitive Device!** This symbol and title inform that the electronic boards and their components are sensitive to static electricity. Care must therefore be taken during all handling operations and inspections of this pro–duct in order to ensure product integrity at all times.
	**HOT Surface!** Do NOT touch! Allow to cool before servicing.
	**Laser!** This symbol inform of the risk of exposure to laser beam from an electrical device. Eye protection per manufacturer notice shall review before servicing.
	This symbol indicates general information about the product and the user manual. This symbol also indicates detail information about the specific product configuration.
	This symbol precedes helpful hints and tips for daily use.

FOR YOUR SAFETY

Your new Kontron product was developed and tested carefully to provide all features necessary to ensure its compliance with electrical safety requirements. It was also designed for a long fault-free life. However, the life expectancy of your product can be drastically reduced by improper treatment during unpacking and installation. Therefore, in the interest of your own safety and of the correct operation of your new Kontron product, you are requested to conform with the following guidelines.

High Voltage Safety Instructions

As a precaution and in case of danger, the power connector must be easily accessible. The power connector is the product's main disconnect device.

⚠CAUTION

Warning!
All operations on this device must be carried out by sufficiently skilled personnel only.

⚠CAUTION

Caution, Electric Shock!
Before installing a non hot-swappable Kontron product into a system always ensure that your mains power is switched off. This also applies to the installation of piggybacks. Serious electrical shock hazards can exist during all installation, repair, and maintenance operations on this product. The–refore, always unplug the power cable and any other cables which provide external voltages before performing any work on this product.
Earth ground connection to vehicle's chassis or a central grounding point shall remain connected. The earth ground cable shall be the last cable to be disconnected or the first cable to be connected when performing installation or removal procedures on this product.

Special Handling and Unpacking Instructions

ESD Sensitive Device!
Electronic boards and their components are sensitive to static electricity. Therefore, care must be taken during all handling operations and inspections of this product, in order to ensure product integrity at all times

Do not handle this product out of its protective enclosure while it is not used for operational purposes unless it is otherwise protected.

Whenever possible, unpack or pack this product only at EOS/ESD safe work stations. Where a safe work station is not guaranteed, it is important for the user to be electrically discharged before touching the product with his/her hands or tools. This is most easily done by touching a metal part of your system housing.

It is particularly important to observe standard anti-static precautions when changing piggybacks, ROM devices, jumper settings etc. If the product contains batteries for RTC or memory backup, ensure that the product is not placed on conductive surfaces, including anti-static plastics or sponges. They can cause short circuits and damage the batteries or conductive circuits on the product.

GENERAL INSTRUCTIONS ON USAGE

In order to maintain Kontron's product warranty, this product must not be altered or modified in any way. Changes or modifications to the product, that are not explicitly approved by Kontron and described in this manual or received from Kontron's Technical Support as a special handling instruction, will void your warranty.

This product should only be installed in or connected to systems that fulfill all necessary technical and specific environmental requirements. This also applies to the operational temperature range of the specific board version, that must not be exceeded. If batteries are present, their temperature restrictions must be taken into account.

In performing all necessary installation and application operations, only follow the instructions supplied by the present manual.

Keep all the original packaging material for future storage or warranty shipments. If it is necessary to store or ship the pro–duct then re-pack it in the same manner as it was delivered.

Special care is necessary when handling or unpacking the product. See Special Handling and Unpacking Instruction.

ENVIRONMENTAL PROTECTION STATEMENT

This product has been manufactured to satisfy environmental protection requirements where possible. Many of the com–ponents used (structural parts, printed circuit boards, connectors, batteries, etc.) are capable of being recycled.

Final disposition of this product after its service life must be accomplished in accordance with applicable country, state, or local laws or regulations.

Environmental protection is a high priority with Kontron.
Kontron follows the DEEE/WEEE directive.
You are encouraged to return our products for proper disposal.

The Waste Electrical and Electronic Equipment (WEEE) Directive aims to:

- Reduce waste arising from electrical and electronic equipment (EEE)
- Make producers of EEE responsible for the environmental impact of their products, especially when they become waste
- Encourage separate collection and subsequent treatment, reuse, recovery, recycling and sound environmental disposal of EEE

Improve the environmental performance of all those involved during the lifecycle of EEE

Table Of Contents

1 / Overview

This manual introduces the SETUP, EFI-SHELL of the AMI BIOS firmware available on Kontron VM6052/VM6054 boards.

The BIOS SETUP is a ROM-based configuration utility that displays the system's configuration status and provides users with a tool to set their system parameters. These parameters are stored in the non-volatile System Flash which saves this information even when the power is turned off. When the system is turned on, the system is configured with the last saved values. Using easy-to-use pull down menus, users can configure such items as:

- Date & Time
- Serial Port, Terminal Type, Console redirection
- USB keyboard layout
- Watchdog for OS boot
- PCI and VME configurations
- CPU configuration
- Boot method and boot device priority
- Security password
- Etc

This manual applies to the release ID16008 of the AMI BIOS*

* Enter SETUP/MAIN menu to get BIOS ID

1.1 Structure

1.2 Related Documents

VM6052/VM6054 Hardware

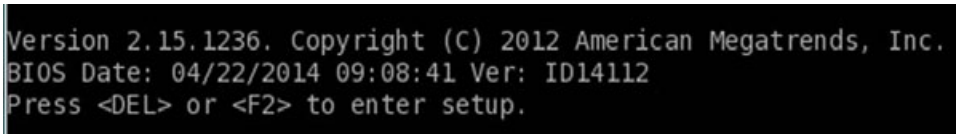
- VM6052/VM6054 User's Guide CA.DT.B19
- VM6052/VM6054 Hardware Release Notes CA.DT.B17

VM6052/VM6054 Software

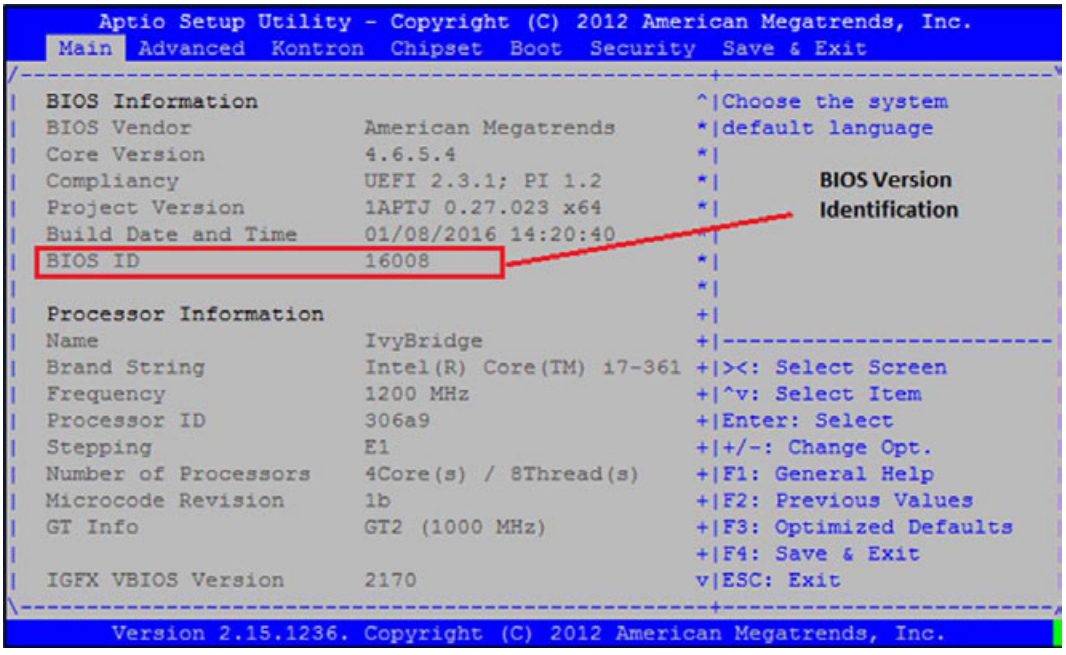
- Release Notes for BSP Fedora 16 . . . . . SD.DT.G11

2 / Accessing the SETUP Menu

To access the SETUP MENU, press <F2> during system boot when the message below is displayed :



A screen similar to the one shown below will appear:



The SETUP displays the system's current configuration settings. The top of the screen has a menu bar with various items (i.e., Main, Advanced, Kontron, etc.). The menu bar items are linked to submenus. Any submenu includes various items to configure the system or to perform specified tasks. For example, the Main menu contains a list of items such as setting the date and time or displaying the AMI BIOS version and ID ...

To get the SETUP menu from COM0 serial line, configure your terminal to 115200 baud. COM0 is available either via the front panel or via the backplane connector of the VM6052/VM6054 board.

The following chapter details the items that are available on Kontron VM6052/VM6054. Some of them are for future implementation, so are marked as reserved and should not be used.

The following chapters provide a sampling of menu items:

2.1 Working with First Level Menu Items

To access the menu of your choice:

- Use the < → > or < ← > keys to select the desired item Menu
- Use the < ↑ > or < ↓ > keys to highlight the desired setting or submenu in item
- Press < Enter > key to validate your choice.

Depending on the menu item selected, one of the following occurs:

- A pop-up window prompts users to enable/disable the selected item.
- A window appears with a list of options to choose from.
- A window appears prompting the user to supply input.
- Links to the submenu.

While the menu item is highlighted, its corresponding Help text is also displayed to help explain the purpose of the item.

- Use < ESC > to get out of the current menu item and jump to its parent item

2.2 Boot Manager Menu

To access the Boot Manager menu, press < F7 > during system boot up. The Boot Manager menu is used to select the boot device.

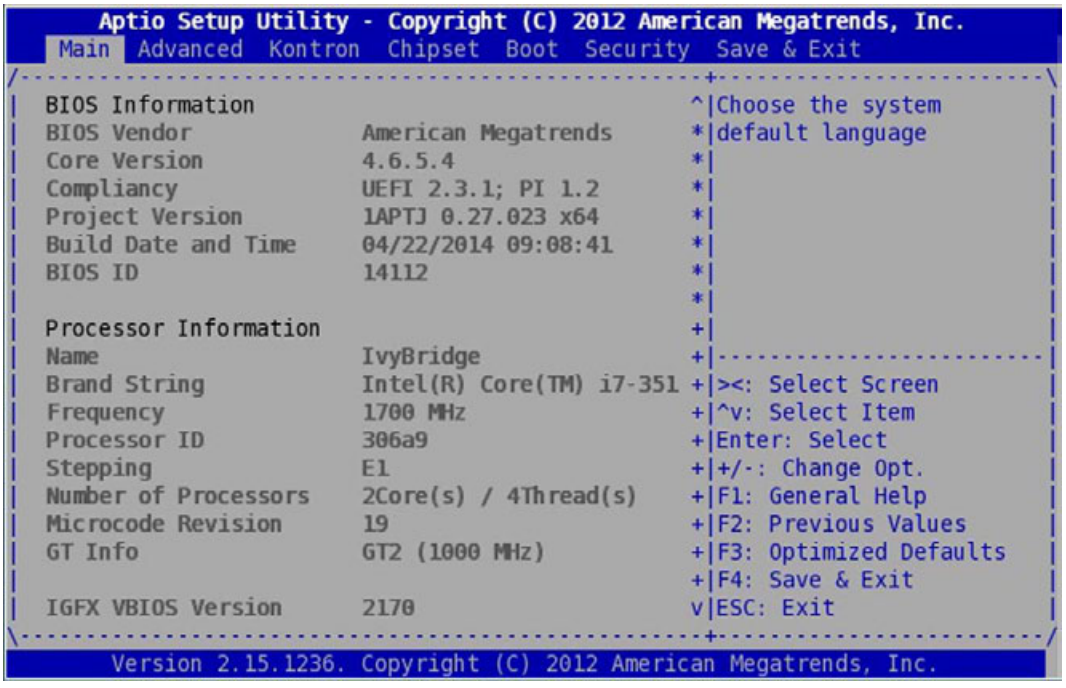
- Select a device from the list (Use the <↑> or <↓> to highlight the desired item)
- Press < ENTER > to boot the selected device or enter setup

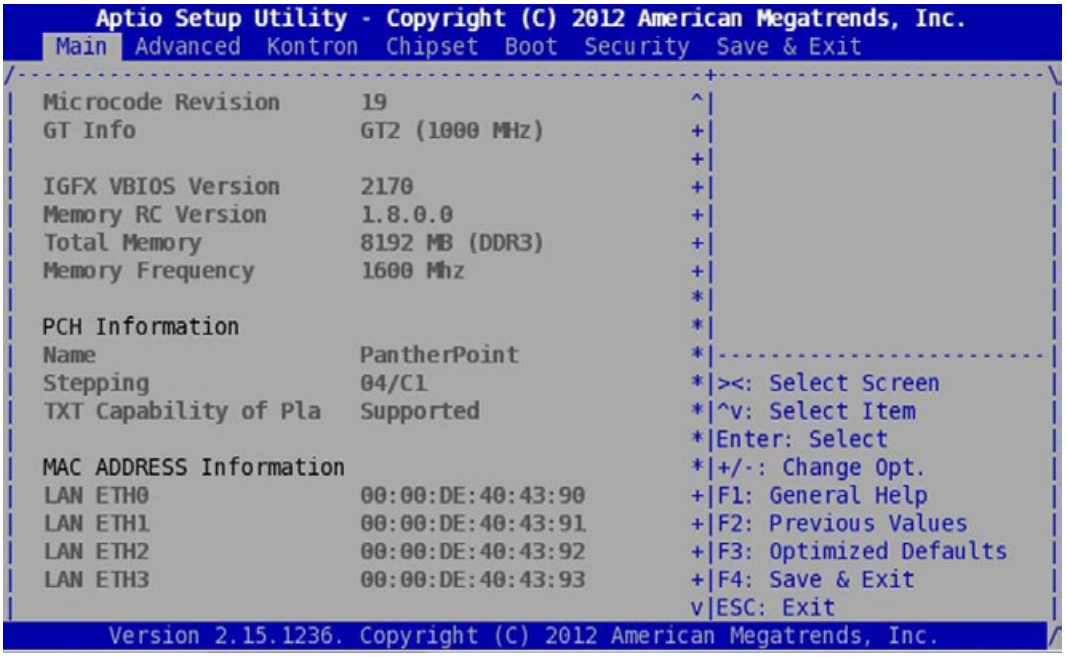
3 / Main Menu

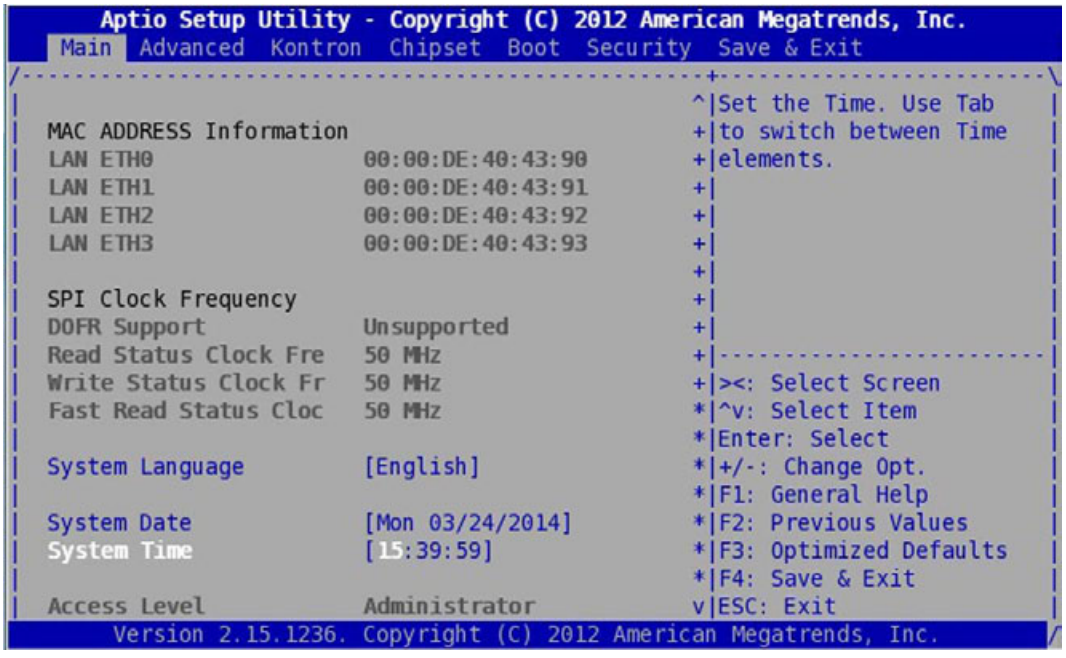
The Main Menu provides general system information and is the first accessible menu page.

Six sections are accessible from the main menu:

- BIOS Information
- Processor Information
- PCH Information
- MAC ADDRESS Information
- SPI Clock Frequency
- System Language
- System Date Time







The "**Information**" section displays:

- The BIOS ID and build date
- The board identity
- The processor name, frequency, stepping, number of cores and threads, graphic information, total memory size and frequency
- The PCH (Platform Controller Hub) name, stepping
- The MAC addresses of the 4 Ethernet interfaces

The entire display is accessible by scrolling down using the arrow key <↓>.

Only English is supported as System Language in this version.

The System Date and System Time fields allow the user to specify the month/day/year as well as the hour/minute/second of the system.

Time is represented in a 24-hour format.

To update the System Date, use the <+> or <-> keys to select the Month (<+> to increase / <-> to decrease the number of the month), and press the <Enter> key to validate your choice. Proceed in the same way for the day and finally for the year.

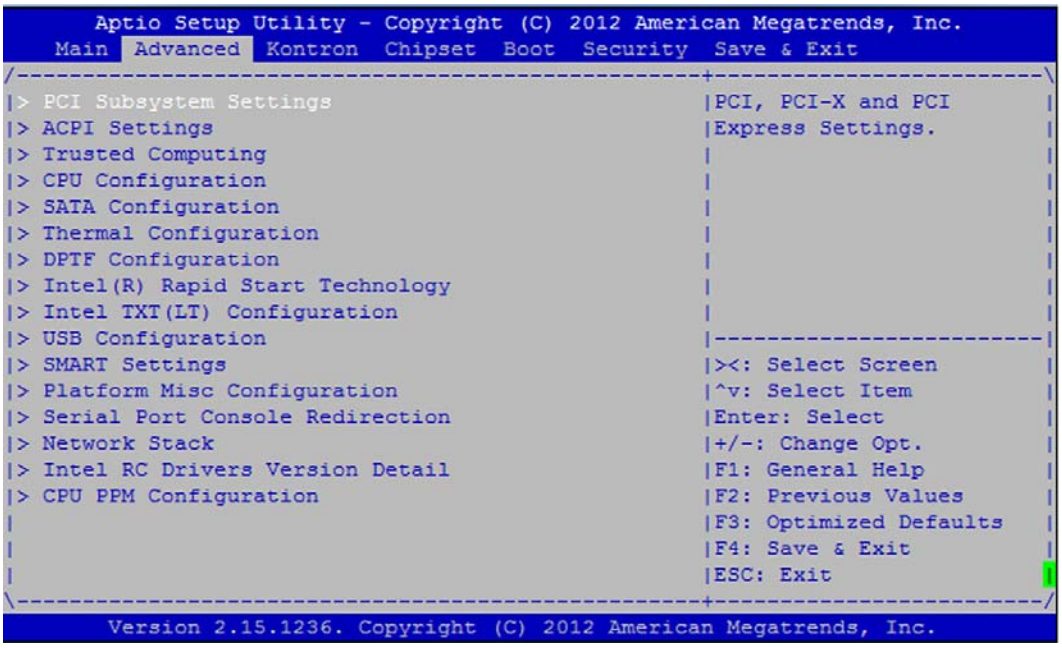
To update the Time, use the <+> or <-> keys to select the Hour (<+> to increase / <-> to decrease the hour), and press the <Enter> key to validate your choice. Proceed in the same way for the minutes and finally for the seconds.

The firmware always reads a RTC to display the date and time at each power-on. To keep the current date and time, the RTC needs to be supplied with the external battery otherwise System Date and System Time are initialized with the build date of the BIOS.

The VM6052/VM6054 board can operate safely without any battery fitted. In this case, the non-volatile board settings are managed this way:

- All the BIOS user settings are kept forever (in a specific area of the BIOS Flash)
- The Date/Time is lost at each Power-Down, and without battery fitted, the BIOS displays the BIOS build Date/Time instead of the current Date/Time.

4 / Advanced Menu



The Advanced menu provides system-level controls to configure the device settings in the following submenus:

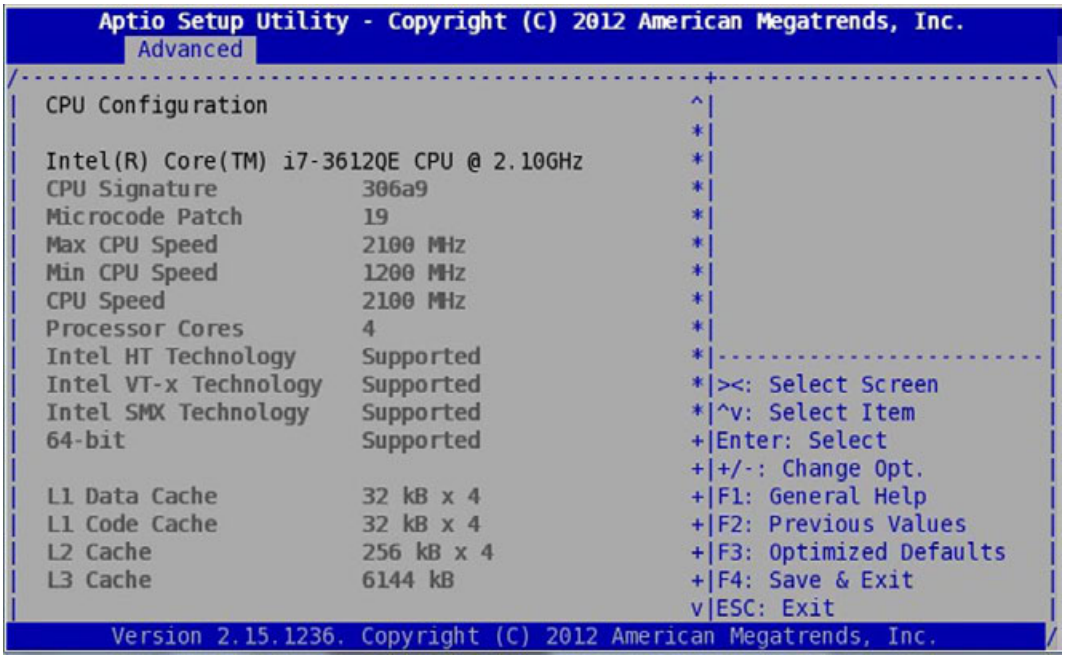
- **CPU Configuration** (hyper-threading, active cores) - Section 4.1 page 8
- **SATA Configuration** (mode selection, speed, port management) - Section 4.2 page 11
- **USB Configuration** (Legacy support) - Section 4.3 page 14
- **Serial Port Console Redirection** - Section 4.4 page 15
- **CPU PPM Configuration** (Turbo mode) - Section 4.5 page 17

The other submenus are Not intended to be changed.

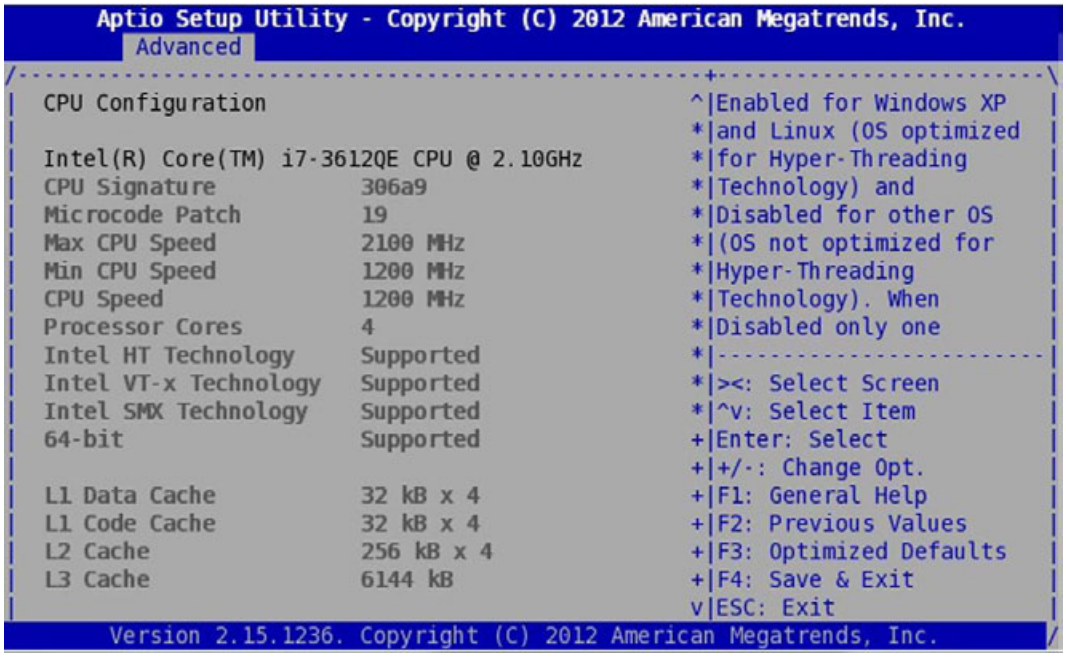
4.1 CPU Configuration

This menu displays information about the CPU speed capabilities and speed setting.

- On a VM6054 board:

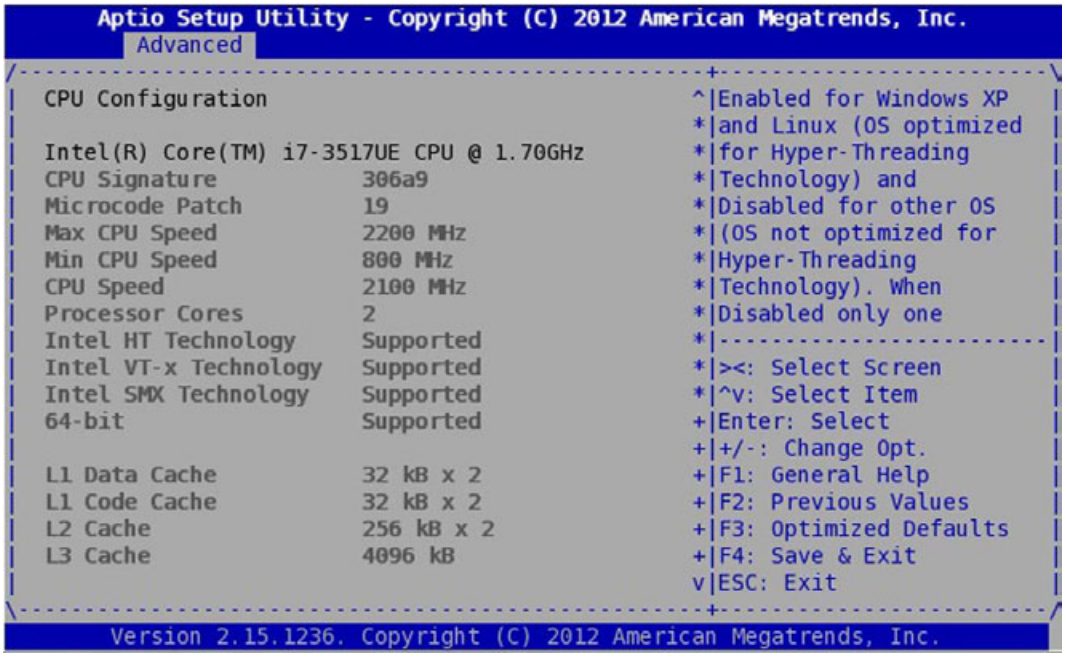


On a VM6054 board, the Thermal Design Power (TDP) is not configurable.
By default, the CPU speed corresponds to the frequency suitable for the maximum processor power 35W.
To force the CPU to its minimum power 28W/1.2 GHz, the microswitches SW2[3-4] must be set to ON.



Refer to the VM6052 and VM6054 - User's Guide - CA.DT.B19, section "Microswitch SW2 Description".

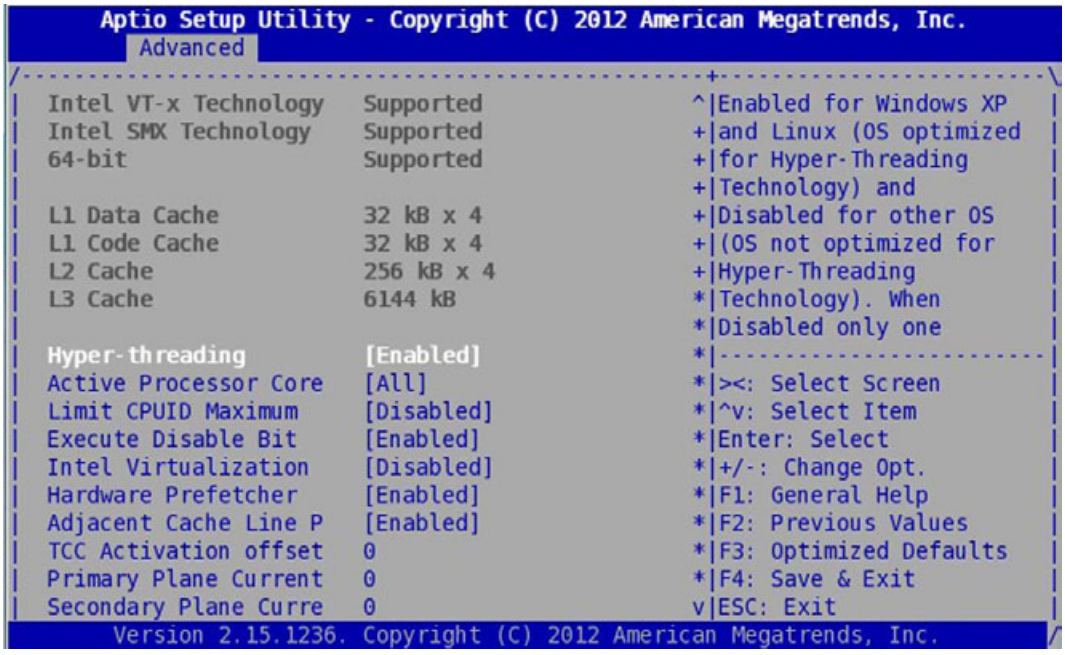
- On a VM6052 board:



On a VM6052 board, the Thermal Design Power (TDP) is configurable by the hardware microswitches SW2[3-4] (default) or by BIOS setup. By default (hardware switches SW2[3-4] set to off), the CPU speed corresponds to the frequency suitable for the TDP 25W.

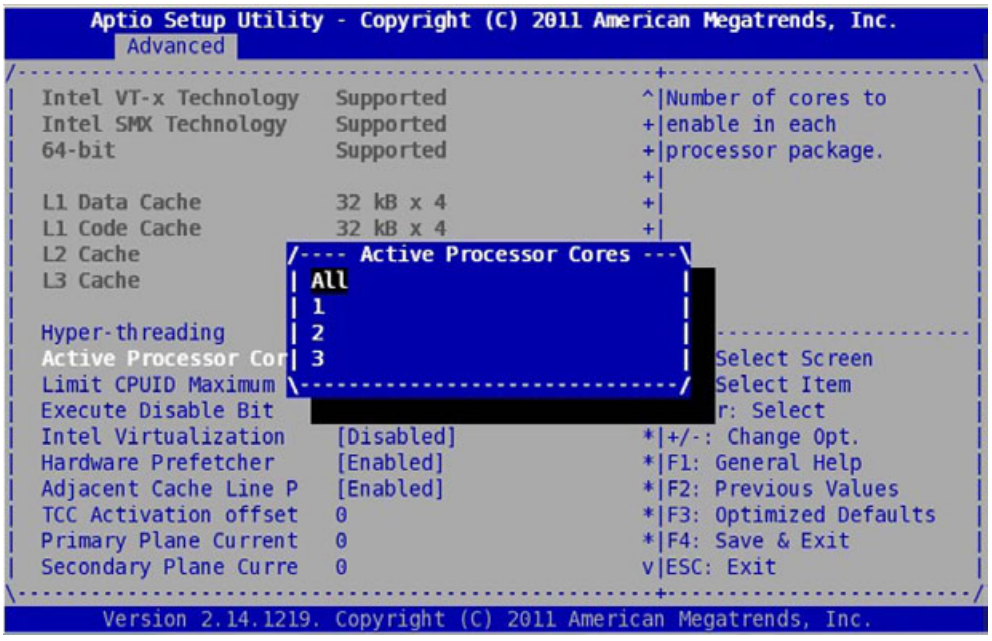
Note in configurable TDP, BIOS always programs the CPU Performance Ratio that corresponds to the Max Non Turbo Ratio. So, with Turbo mode enabled, for TDP 25W BIOS shall program ratio corresponding to 2100 MHz, higher ratio (corresponding to 2200 MHz) causing turbo.

This menu also allows the user to configure the number of active cores and to enable/disable the HyperThreading fea–ture.



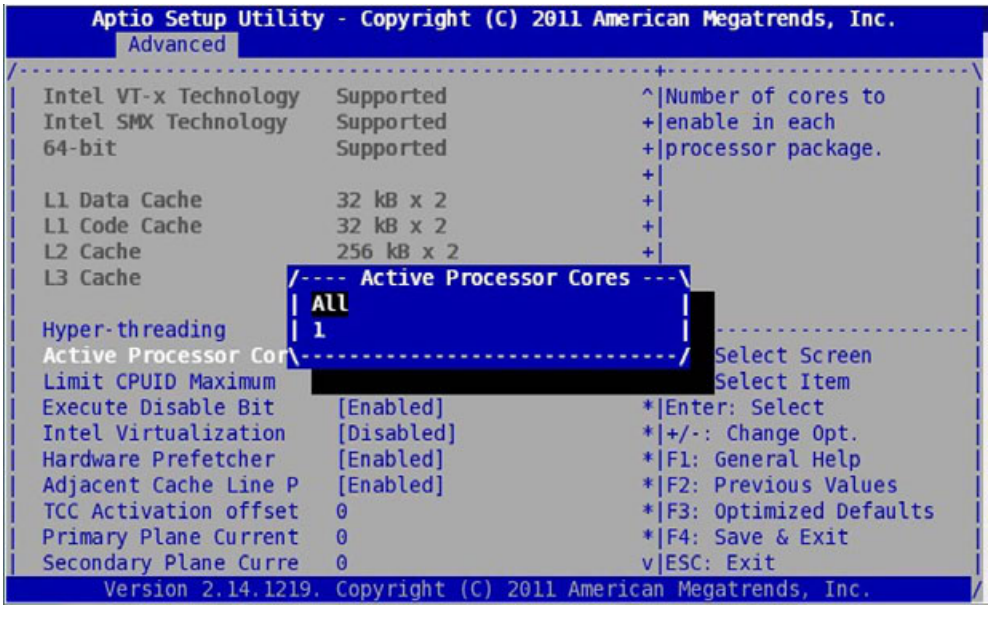
4.1.1 Active Processor Cores

- On a VM6054 board:



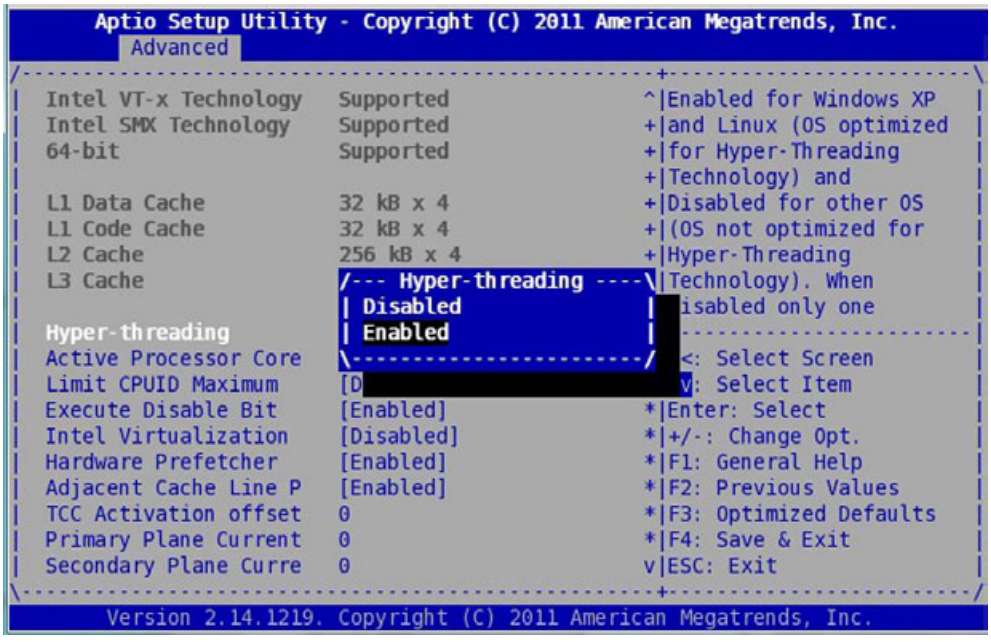
On a VM6054 board, up to 4 cores can be activated.

- On a VM6052 board:



On a VM6052 board, up to 2 cores can be activated.

4.1.2 Hyper-Threading

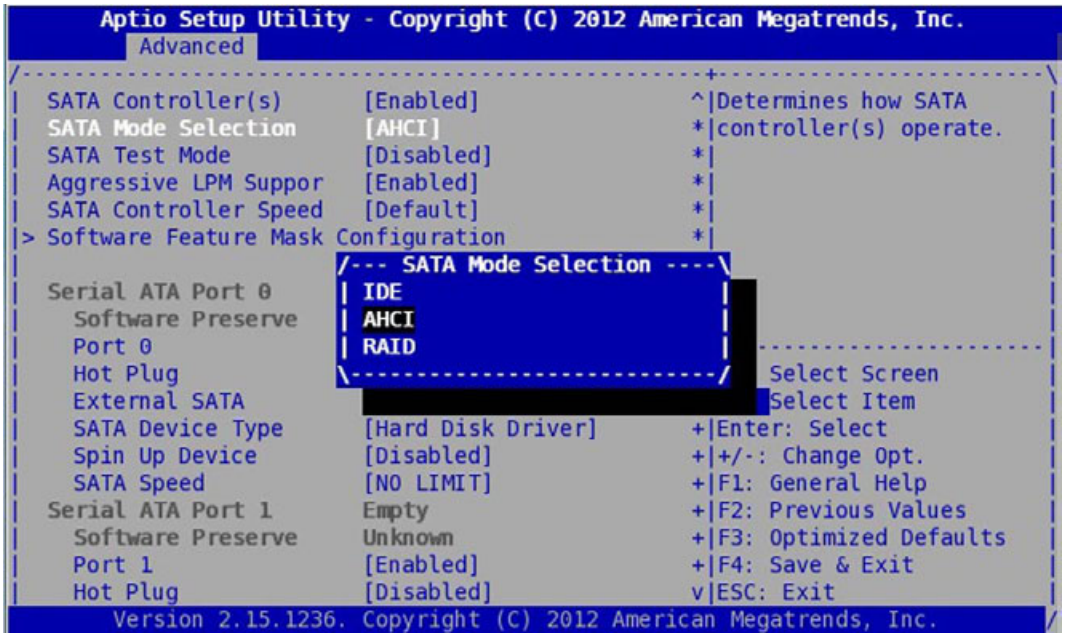


When **Hyper-Threading** is **Enabled**, 2 logical CPUs per core are present so there are up to 4 logical CPUs on a VM6052 board and up to 8 logical CPUs on a VM6054 board.

4.2 SATA Configuration

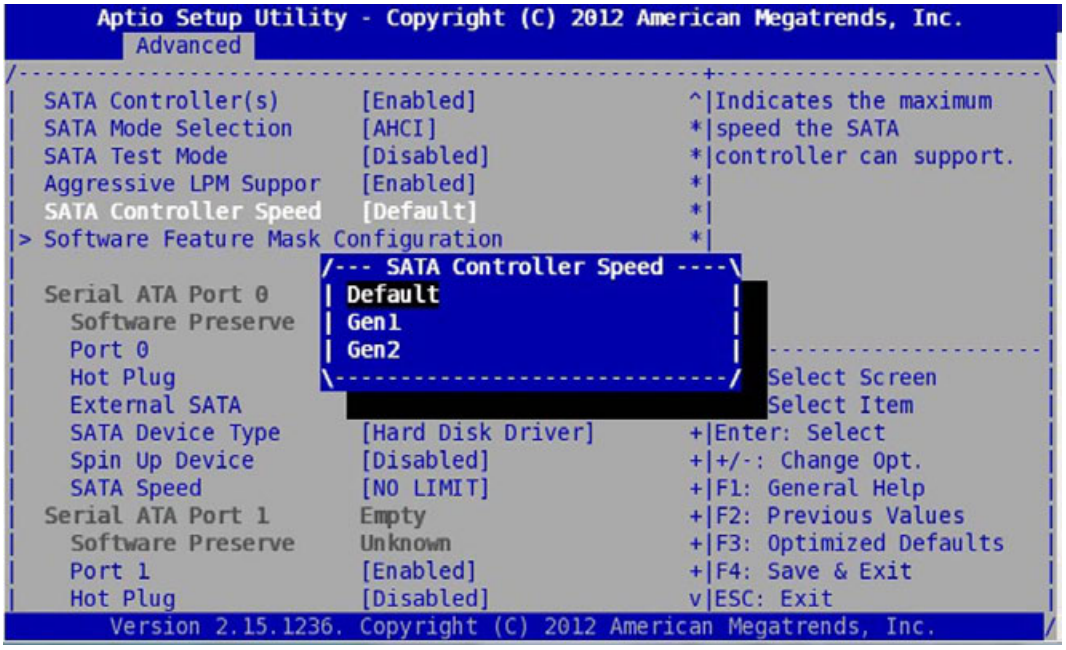
This menu can be used to :

- Select the SATA mode (AHCI or IDE)



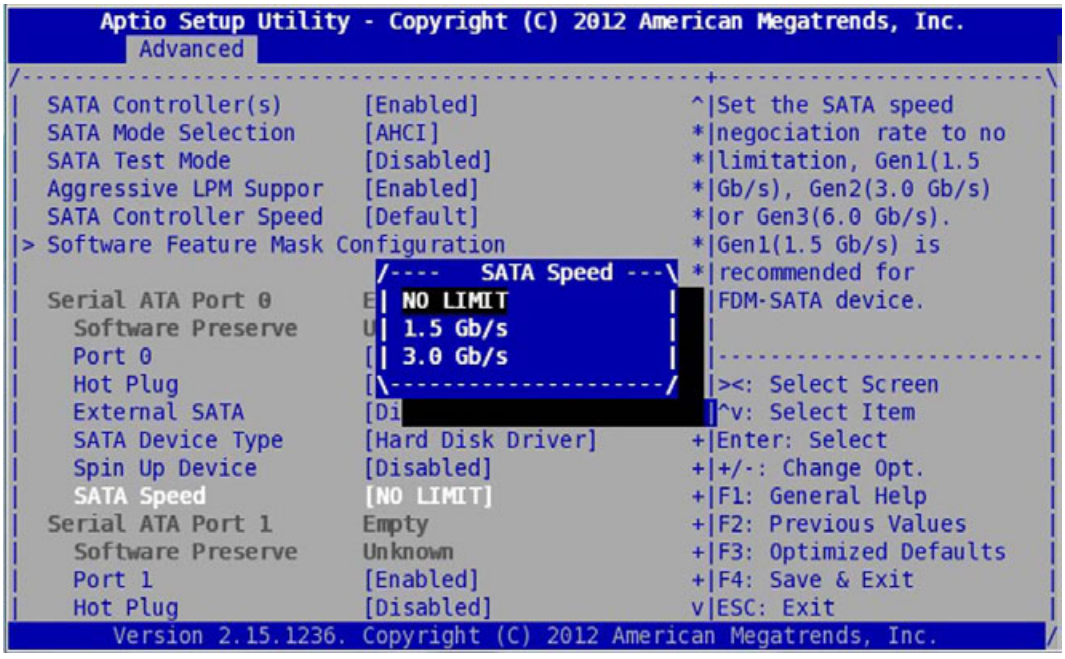
The SATA RAID mode is supported by the BIOS but has not been tested.

- Select the maximum speed supported by the SATA controller.

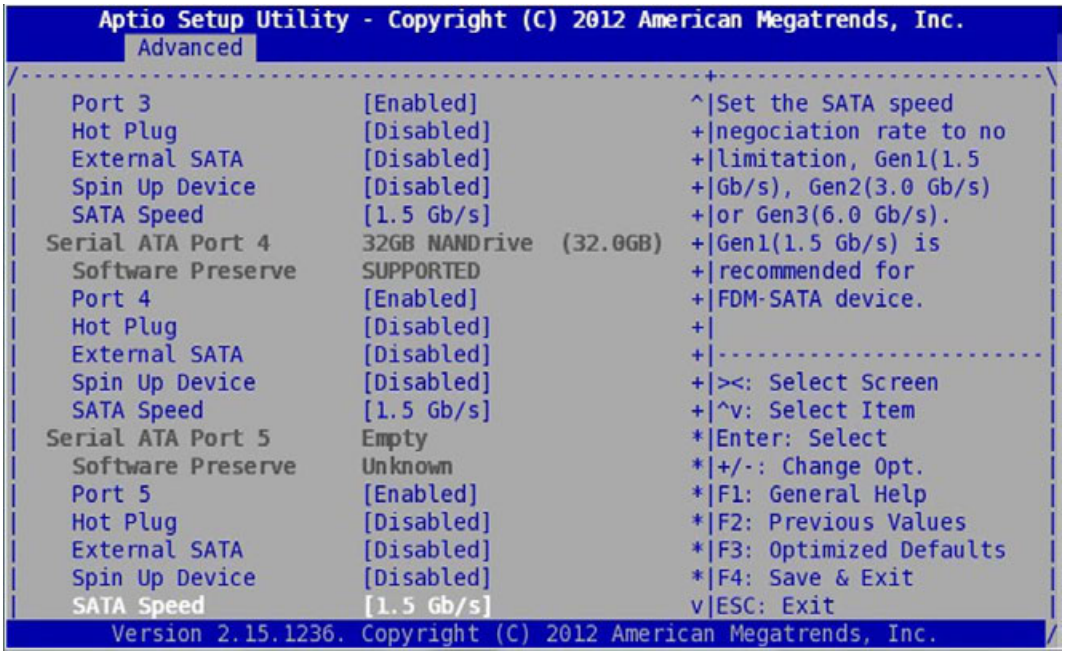


The SATA controller speed selection impacts all the SATA ports.

- Select the maximum speed for the SATA Ports:



By default, the SATA Speed for ports 0 and 1 is not limited (**`NO LIMIT`**) but can be forced to Gen1 (**`1.5 Gb/s`**) or Gen2 (**`3.0 Gb/s`**). The SATA Speed for the other ports is forced to Gen1 (**`1.5 Gb/s`**).



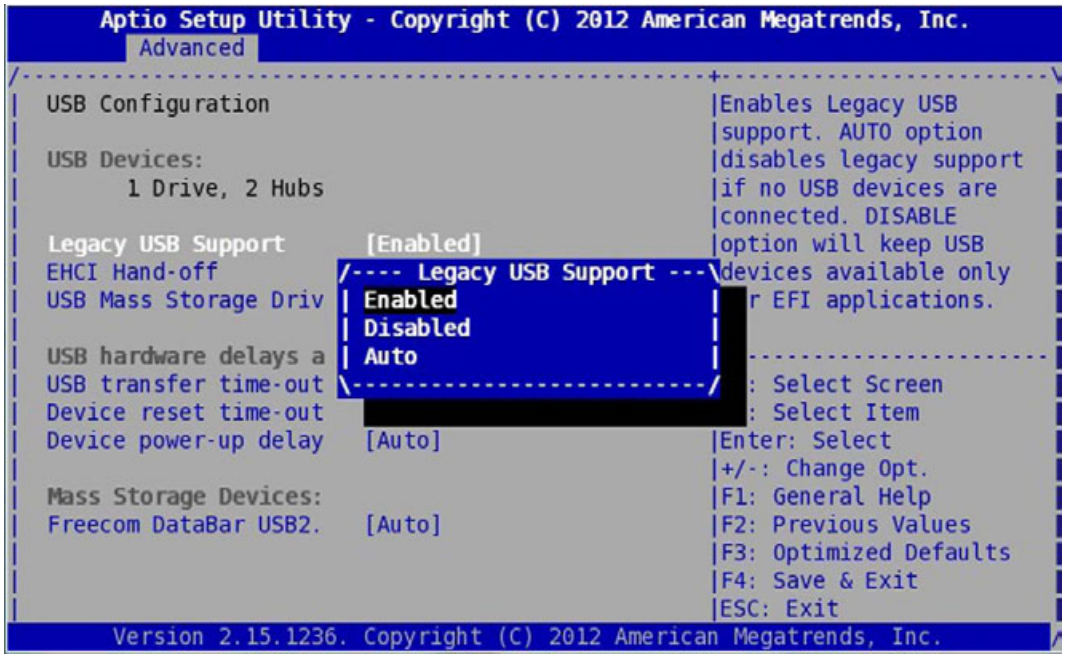
CAUTION:

1. In AHCI mode, the SATA controller speed takes precedence over the SATA speed by port.
2. In IDE Mode, only the SATA speed by port can be set.
3. In AHCI mode, usually, the operating system renegociates the SATA speed based on the capabilities registers. It is possible to force the SATA speed using the **`libata.force`** option at the kernel command line to boot Linux OS.

4.3 USB Configuration

This menu can be used to:

- Enable/disable the Legacy USB Support (such as DOS legacy environment).
- Avoid booting from a USB device when a USB device is connected.



Select the option **Legacy USB Support** to change it:

- **Enabled**
- **Disabled**
- **Auto**

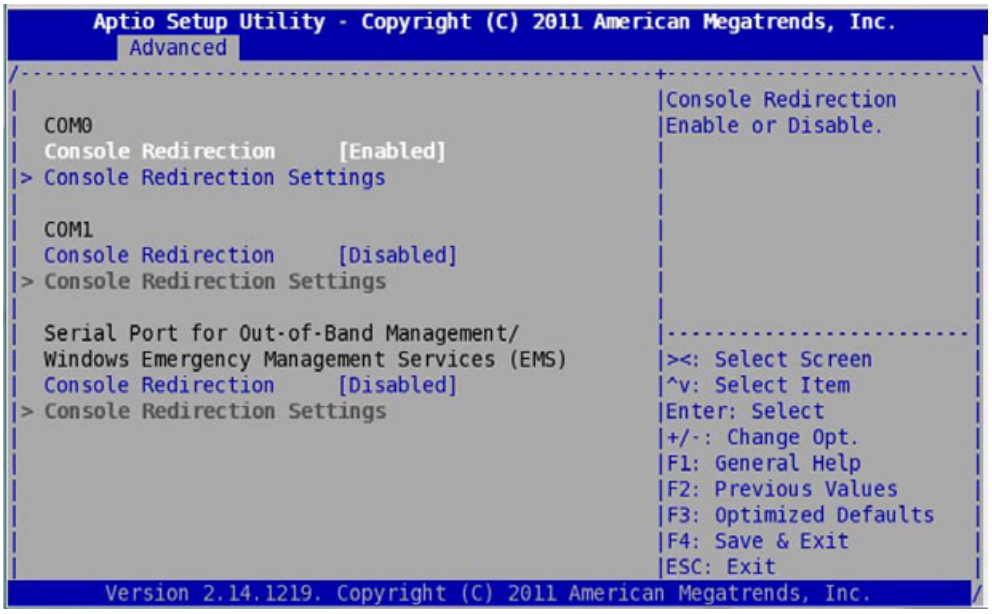
Auto option will disable the Legacy Support if no USB device is connected.

Disabled option will keep the USB device available for EFI application only.

The other options should Not be changed.

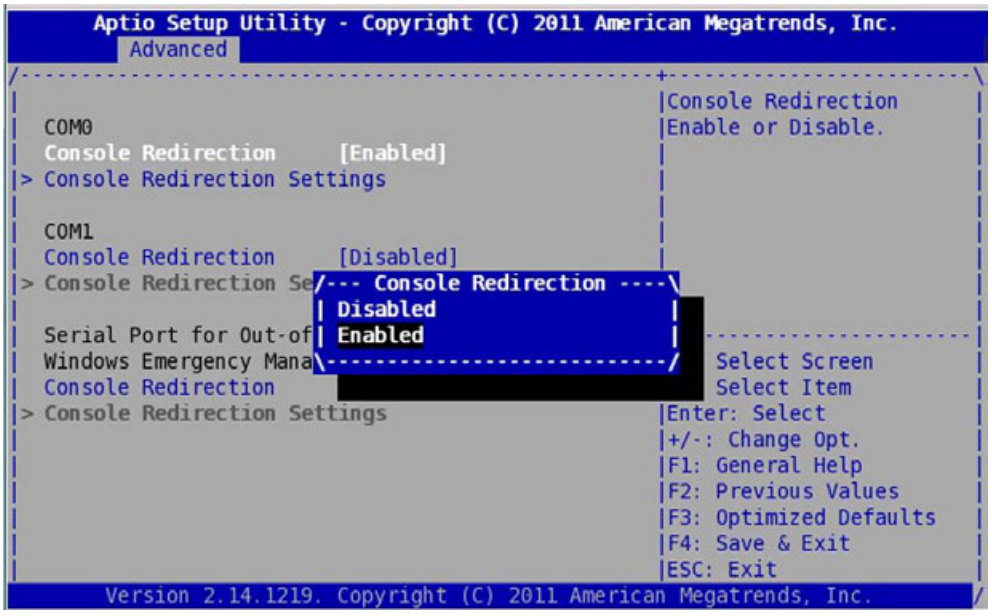
4.4 Serial Port Console Redirection

The BIOS console can be redirected to the serial COM0 and/or the serial COM1 with the Console Redirection menus. Also the characteristics of the COM0 or COM1 serial line can be modified with the Console Redirection Settings menus as described after:



4.4.1 COM0/COM1 Console Redirection

The user has the option to enable/disable the serial Console Redirection on COM0 or on COM1. COM0 is a serial line available on front panel or on rear of the VM6052/VM6054 and COM1 is available on the rear. To have SETUP displayed and EFI shell visible on a serial line it is necessary to enable the Console redirection on it. COM0 Console Redirection is enabled by default and COM1 is disabled by default.

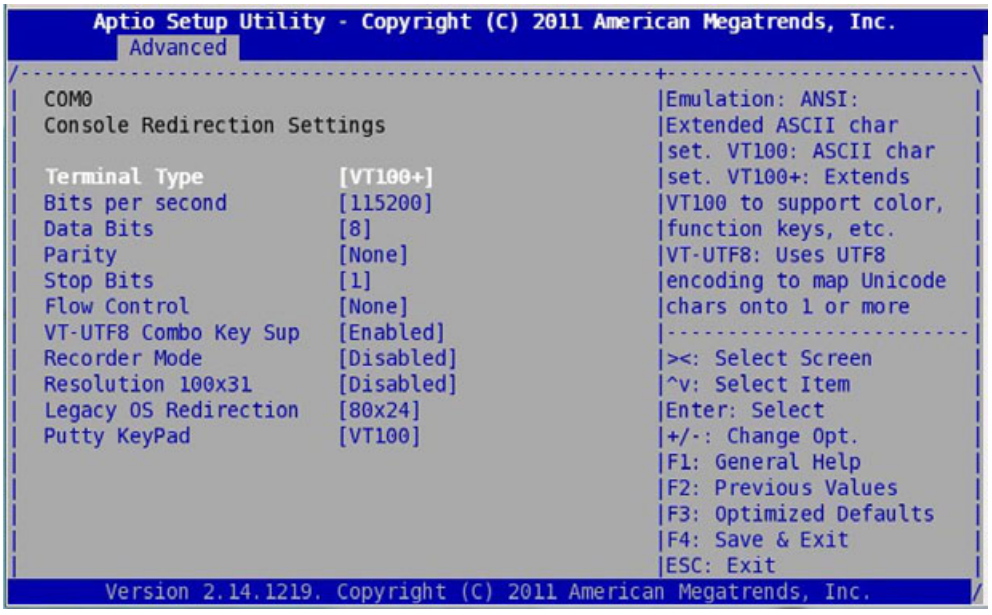


In case the user would like to display the PXE messages on serial COM1 instead of serial COM0, serial COM0 redirection must be disabled because only one serial port is selected by PXE.

4.4.2 COM0/COM1 Console Redirection Settings

This menu allows to configure several parameters for a serial line on which the console redirection has been enabled. The main configurable parameters are:

- Terminal Type
- Bits per second
- Data Bits
- Parity
- Stop Bits
- Flow Control

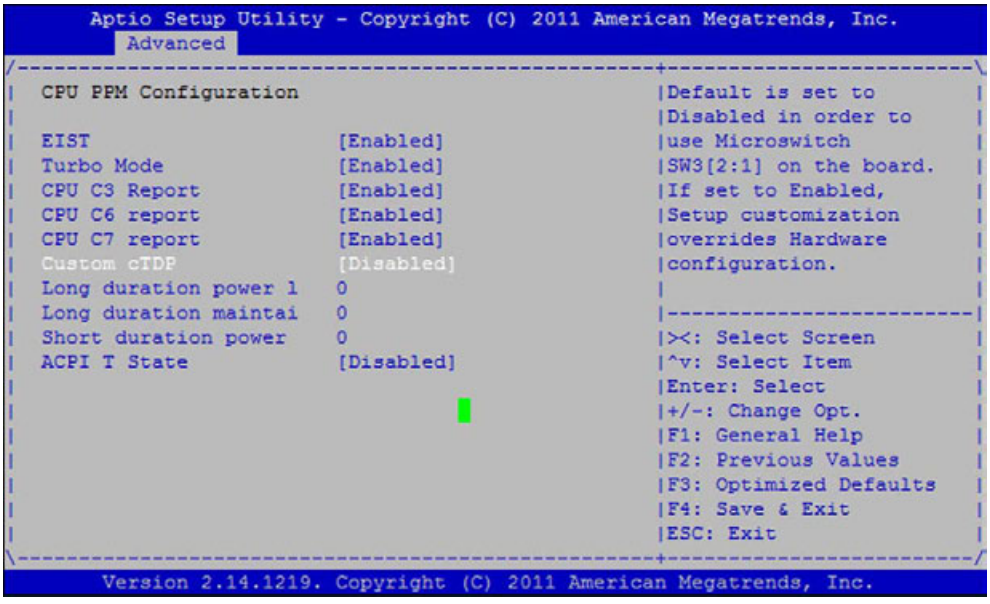


This shows the default settings.

4.5 CPU PPM Configuration

This menu can be used to:

- Enable/disable the EIST (Enhanced Intel Speed Step)
- Enable/disable the Turbo mode
- Configure the Thermal Design Power (TDP) (option only available on VM6052)

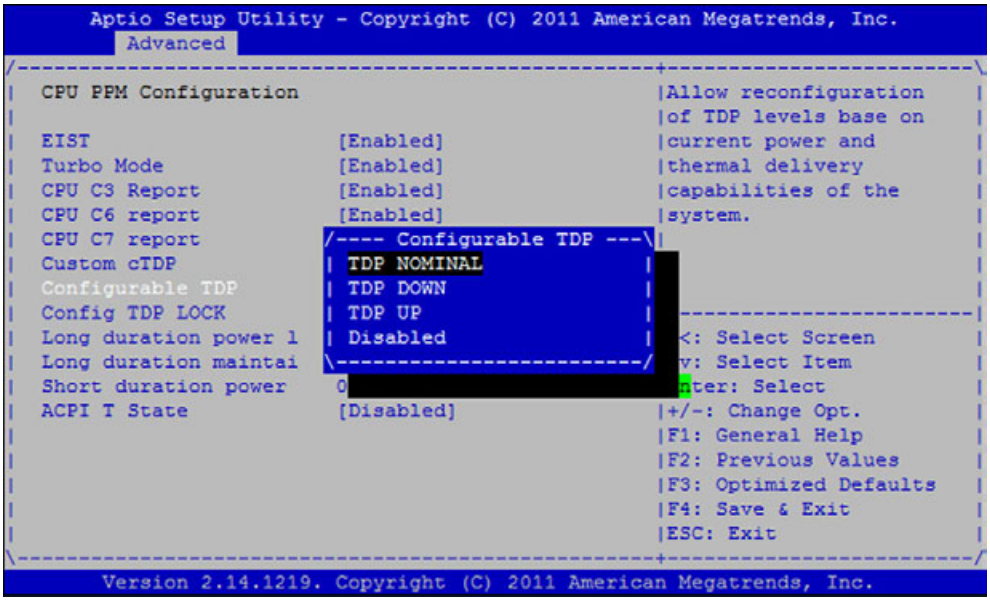


On VM6052 only:

By default the Custom cTDP option is set to **[Disabled]** in order to use the setting of the hardware microswitches SW2[3-4] on board.

By default, microswitches SW2.3 and SW2.4 are set to **[OFF:OFF]** to force TDP UP setting 25W.

Enabling this option allows the user to override the hardware switch configuration and allows a manual selection for the TDP as shown in the following paragraph.



Three **TDP** can be configured:

- **TDP Nominal** corresponding to 17W
- **TPD Down** corresponding to 14W
- **TPD Up** corresponding to 25W

The setting "**Disabled**" will force the **TDP** to the DOWN setting 14W.

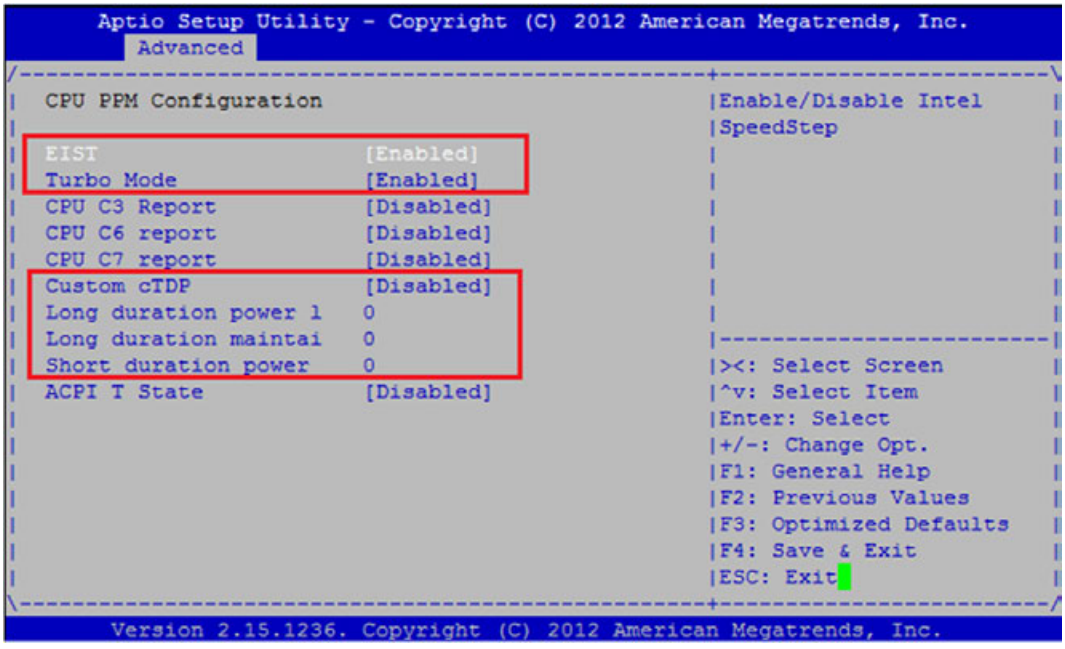
IMPORTANT NOTE about TURBO setting:

By default, Turbo mode is set to **[Disabled]**.

Setting EIST and Turbo Mode to **[Enabled]** displays 3 parameters corresponding to:

- Long duration power limit (PL1),
- Long duration maintain window (Tau),
- Short duration power limit (PL2):

On VM6052 board:



PL1, PL2 and Tau parameters in MSR and MMIO are set differently:

- MSR 610h reflects the highest level system supported (MAX PL1/PL2):

  As PACKAGE_MAX_POWER = No limit, PL1 is computed as follows:

  PL1 = MAX TDP Power = Power TDP-UP = 25 W

  As PACKAGE_MAX_POWER = No limit, PL2 is computed as follows:

  PL2 = 1.25 * MAX TDP Power = 31.25 W

  Tau must be less than PACKAGE_MAX_TIME.

  As PACKAGE_MAX_TIME = No limit, Tau is limited by Setup.

- MMIO reflects the current cTDP point selected (UP/DOWN/NOMINAL):

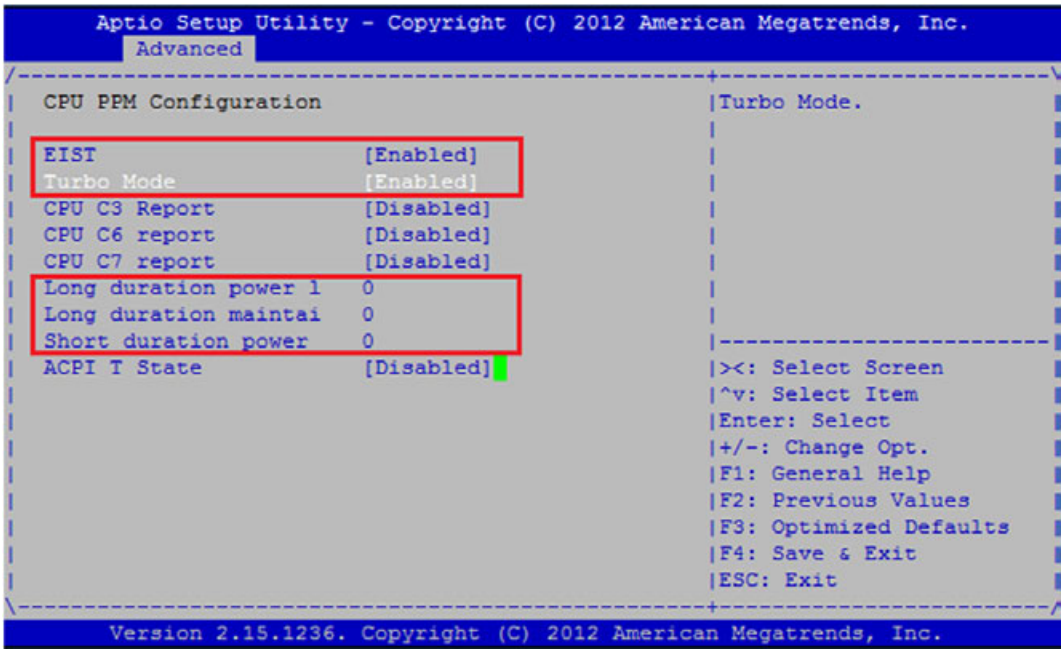
The default values set by BIOS in the setup (equal to 0 which means default') are summarized in following table:

TDP SELECTED	PL1 (W)	PL2 (W)	TAU (SEC)
UP	25W	31.25W	28 sec
NOMINAL	17W	21.25W	28 sec
DOWN	14W	21.25W	28 sec
Setup limit	0 ≤ PL1 ≤ 255	0 ≤ PL2 ≤ 255	0 ≤ Tau ≤ 120

Parameter Tau = PL1 time window is modified in both MSR 610h and MMIO registers.

Tau is set to 28 seconds by default on Intel® Mobile Ivy Bridge

On VM6054 board:



PL1, PL2 and Tau parameters are set ONLY in MSR because MMIO are reserved for TDP SKUs (Dual-Core Ivy Bridge):

- MSR 610h reflects the highest level system supported (MAX PL1/PL2):

  PL1 must be comprised between PACKAGE_MIN_POWER and PACKAGE_MAX_POWER defined in MSR 614h. If not, PL1 = PACKAGE_TDP_POWER = 35 W (default).

  Tau must be less than PACKAGE_MAX_TIME = 64 sec.

  Tau is set to 28 seconds by default on Intel® Mobile Ivy Bridge.

  PL2 must be greater than PACKAGE_MIN_POWER defined in MSR 614h.

  If not, PL2 = PACKAGE_MIN_POWER.

  PL2 default value is 1.25*PACKAGE_TDP_POWER = 1.25*35 = 43.75 W.

  MSR 610h is locked for non-TDP SKUs (Quad-Core Ivy Bridge).

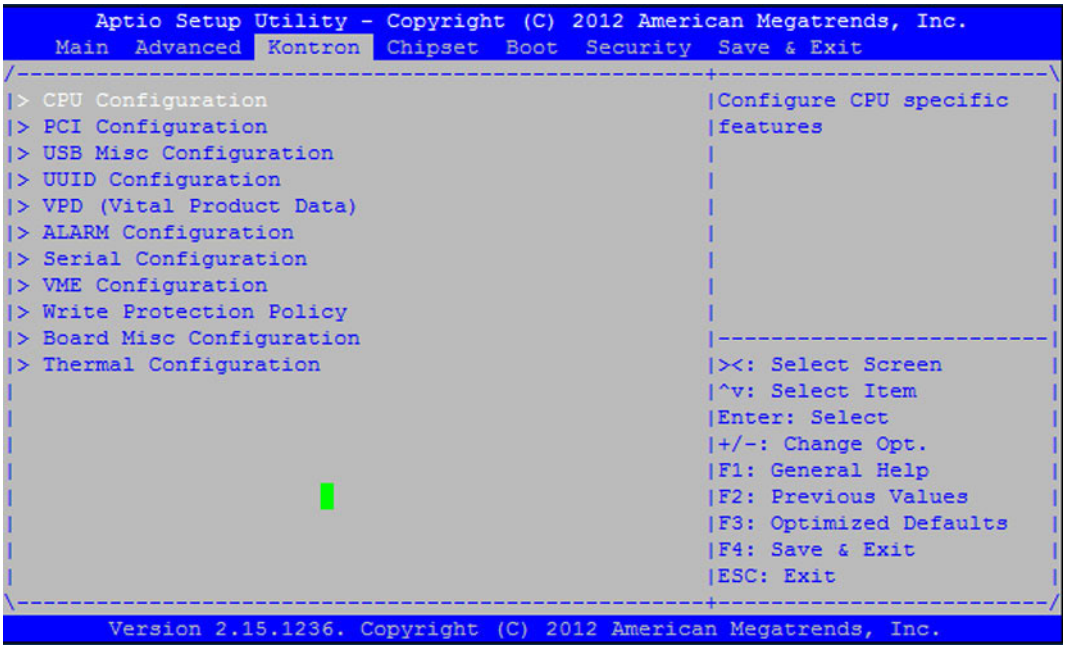
The default values set by BIOS in the setup (equal to 0 which means default') are summarized in following table:

PL1	PL2	TAU
35W	43.75W	28 sec
0 ≤ PL1 ≤ 255	0 ≤ PL2 ≤ 255	0 ≤ Tau ≤ 120

5 / Kontron Menu

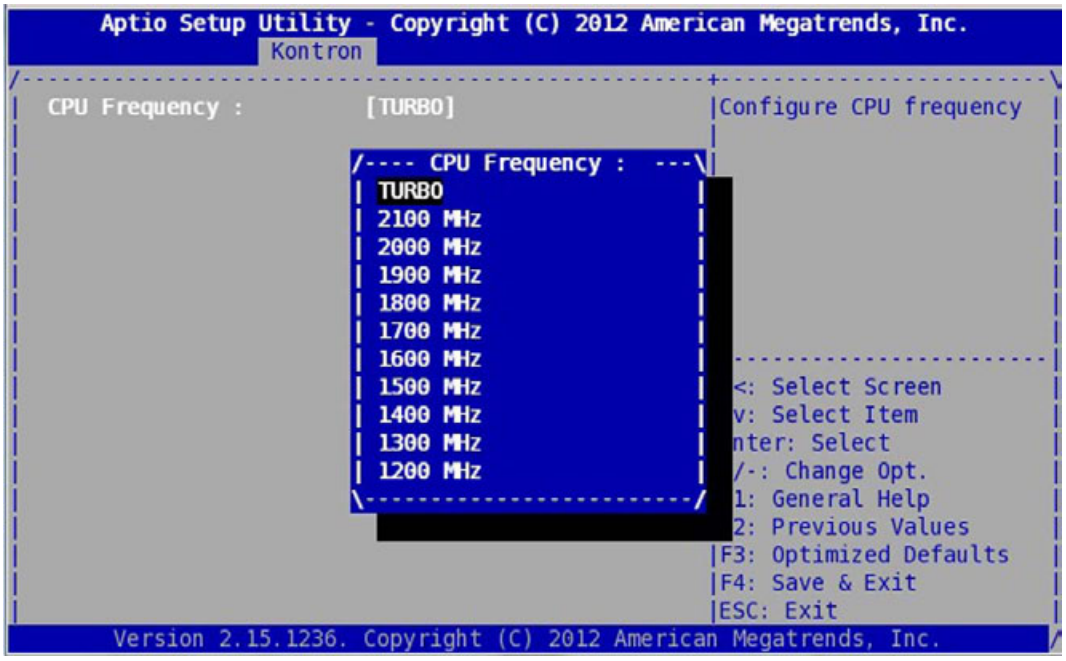
The Kontron Menu provides system-level controls to configure specific VM6052/VM6054 hardware design.

The different parameters are described in the following sections:



5.1 CPU Configuration

CAUTION: The following menu is used to configure the CPU speed on the VM6054 board only. This parameter only applies to the VM6054 boards as the processor does not support the Configurable TDP feature. Refer to section 4.5 page 17 for setting CPU configurable TDP for VM6052 board.



By default, the CPU speed option on the VM6054 board is set to "**2100 MHz**".

When "**TURBO**" is selected, the BIOS programs the ACPI _PSS table with P-state entries corresponding to the frequency range **[1200-2100] MHz** and the Turbo mode is automatically enabled (refer to the Advanced CPU PPM Configuration menu). Thus, BIOS allows the CPU to activate Intel® Turbo Boost Technologie in order to obtain higher performances.

When the CPU enters in idle state then the CPU speed is 1200 MHz by default, but when the CPU load increases, then the CPU speed can reach its maximum speed 2100 MHz and even higher in Turbo Boost with a maximum frequency of 3100 MHz for 1 core enabled and 2800 MHz for up to 4 cores enabled..

When the CPU must operate at a fixed frequency, the BIOS offers several CPU frequencies supported by the VM6054 board.

For example, to force the CPU to operate at the fixed CPU frequency 1700 MHz, select **1700 MHz** in the list, then move to the Save & Exit menu and select Save Changes and Reset.

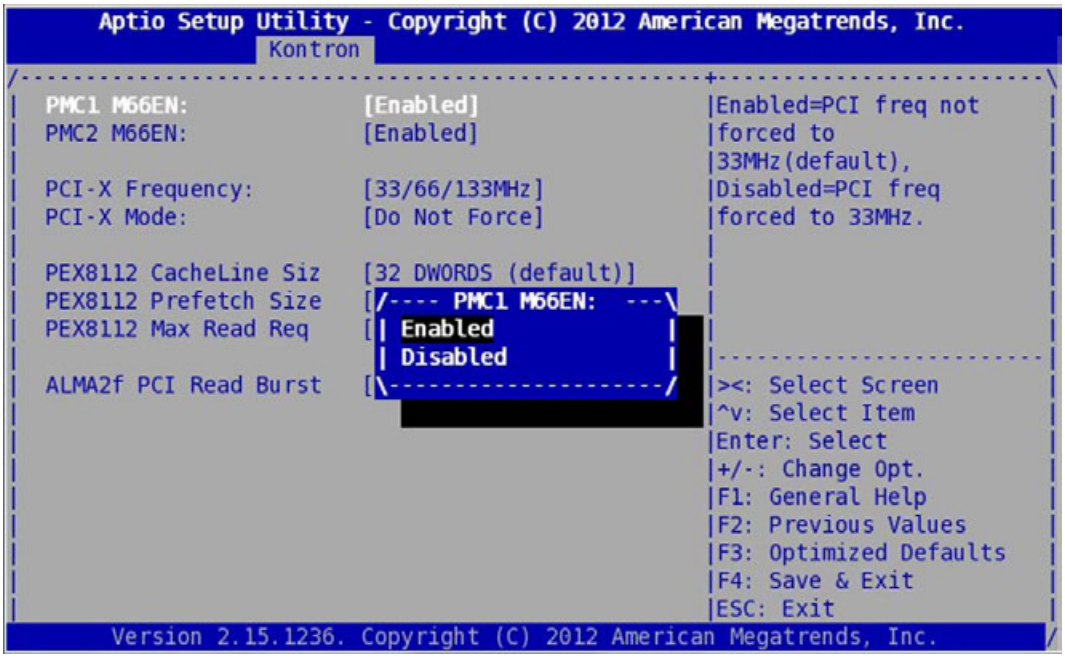
In a "**fixed frequency**" mode, the Turbo Mode is automatically set to Disabled by the BIOS in Advanced CPU PPM Configuration menu and programs the ACPI _PSS table with only one entry corresponding to the selected frequency.

Thus, the CPU speed does not oscillate under OS and will be set at the frequency specified in the BIOS Setup.

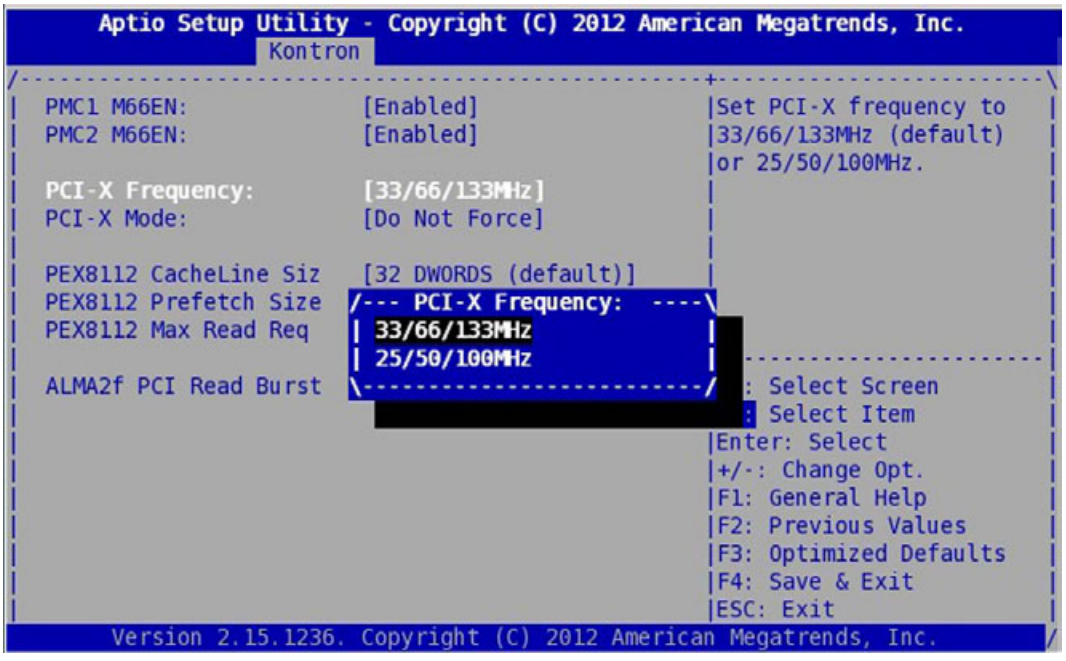
CAUTION: On a VM6054, setting the hardware microswitches SW2[3:4] to [on,on] force the CPU frequency to 1200 MHz (the other combinations have no impact on VM6054 but are used on VM6052). In this case, the CPU frequency selecting in the BIOS setup is no more relevant.

5.2 PCI Configuration

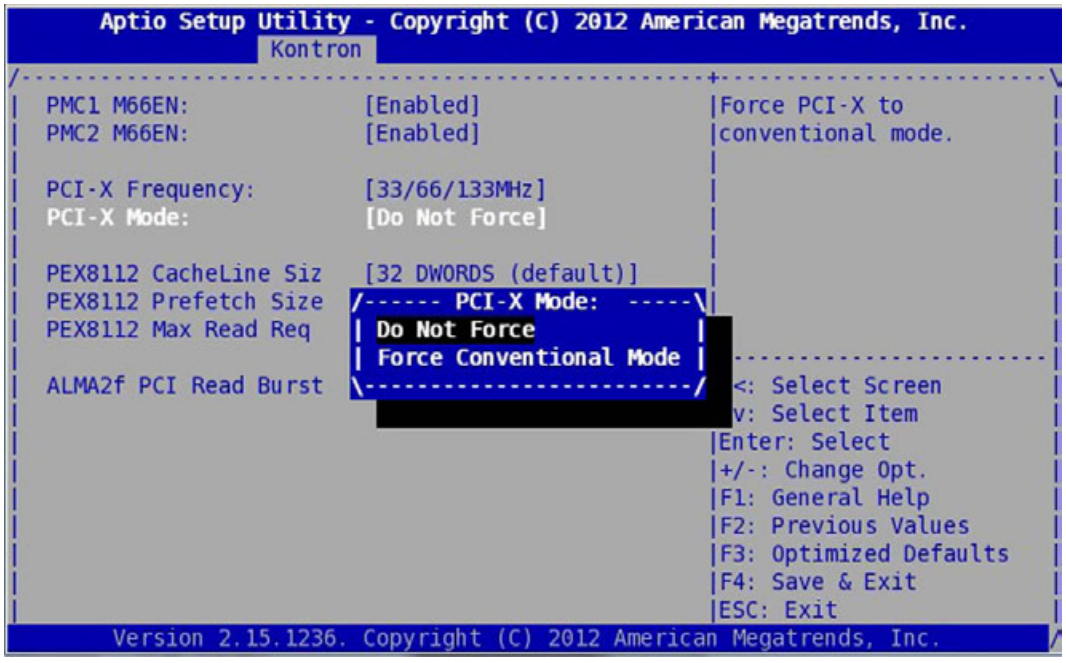
5.2.1 PCI 32 and PCI/PCIX 64 configuration



If set to "**Disabled**" the options "**PMC1 M66EN**" and "**PMC2 M66EN**" allow to force operation on the PCI bus at low frequency. Default setting is "**Enabled**".



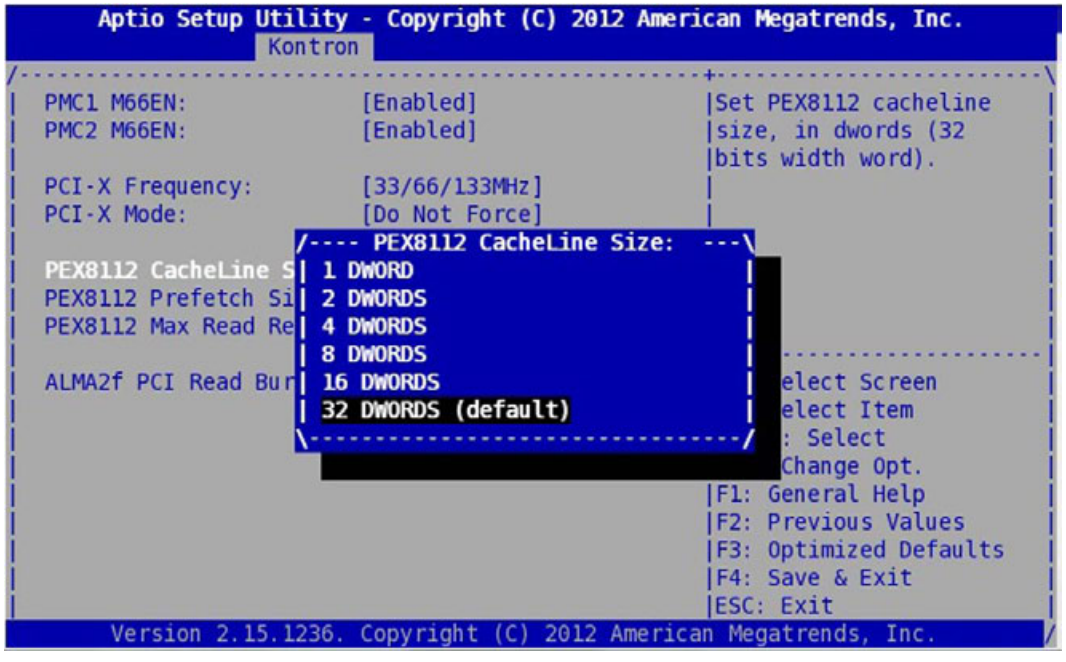
The option "**PCI-X Frequency**" allows to set the PCI-X bus either to **33/66/133 MHz** (default) or **25/50/100 Mhz**.



The option "**PCI-X Mode**" allows to force the PCI-X bus to the conventional mode.

5.2.2 PCIe-PCI Brigde PEX8112 Configuration

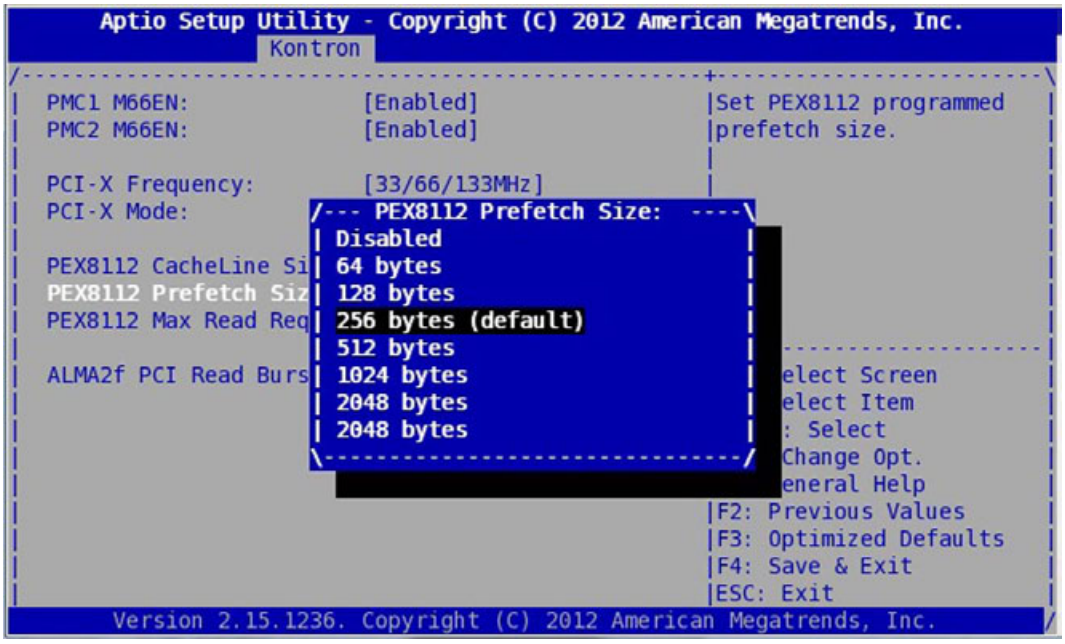
- Configuration of the CacheLine Size data in the PCI header of the PEX8112.



Default is set to **32 DWORDS**.

- **Configuration of the Programmed Prefetch Size bits of the PEX8112 PCI Control register (address offset 100Ch).**

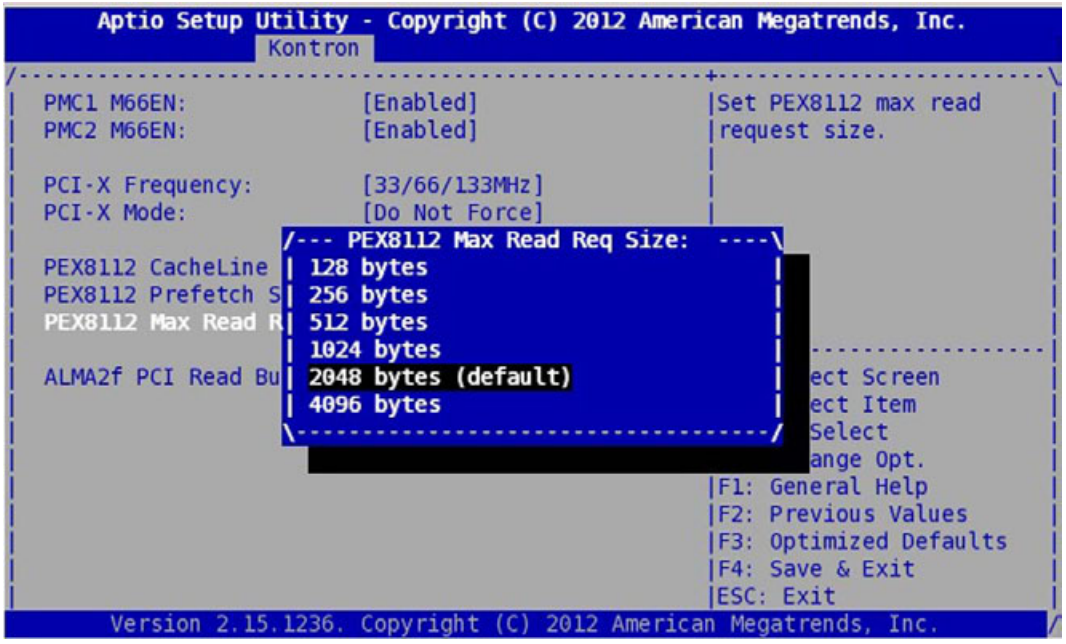
  It determines the number of bytes requested from the PCI Express interface as a result of a PCI-to-PCI Express Read.



  Default value is set to **256 bytes**.

- **Configuration of the Maximum Read Request Size bits of the PEX8112 PCI Express Device Control register (address offset 68h).**

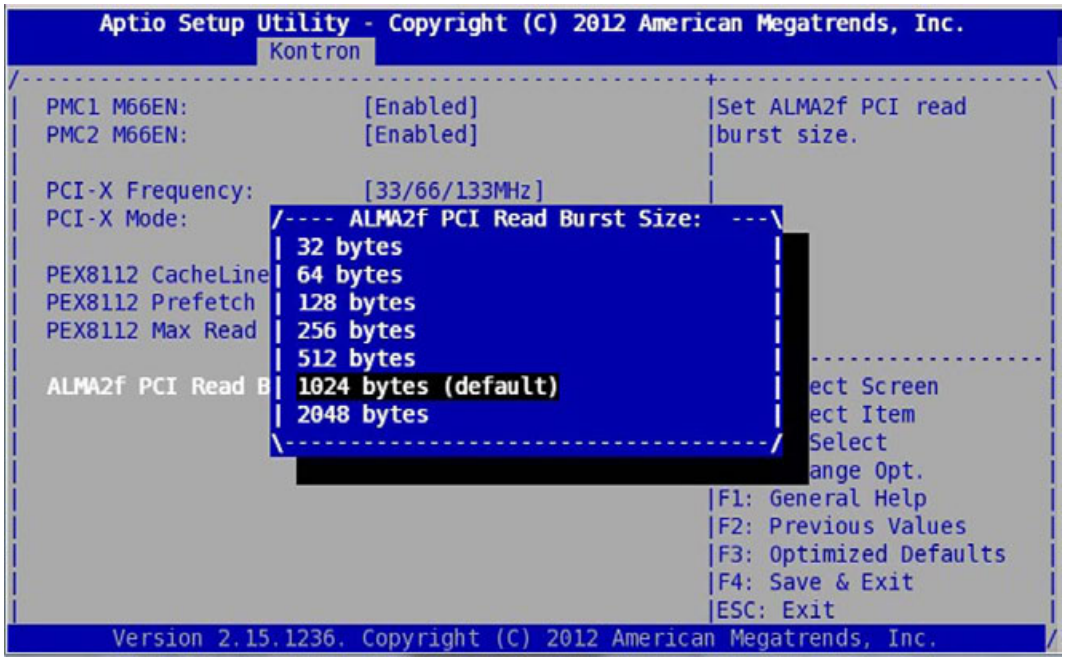
  It sets the Maximum Read Request Size for the Device as a Requester. The PEX 8112 must not generate Read requests with a size that exceeds the set value.



  Default value is set to **2048 bytes**.

5.2.3 PCI-VME Bridge ALMA2f Configuration

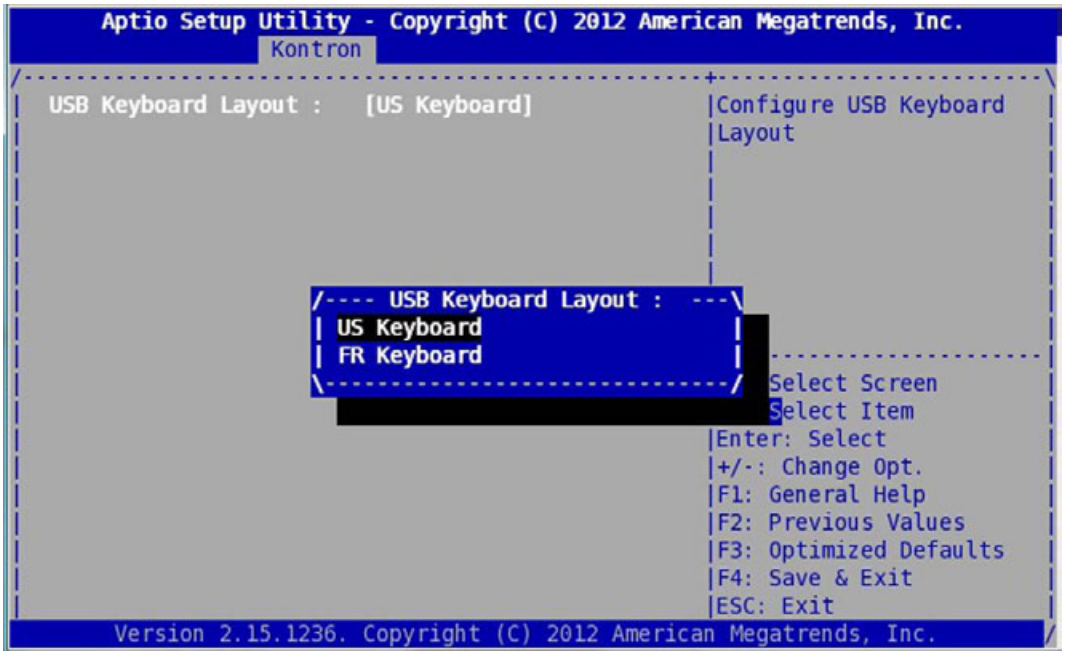
- Configuration of the PCI Read Burst Size bits of the ALMA2f VME Slave Read Control register (address offset 104h).



5.3 USB Misc Configuration

This menu is used to set the USB Keyboard Layout, Qwerty or Azerty.

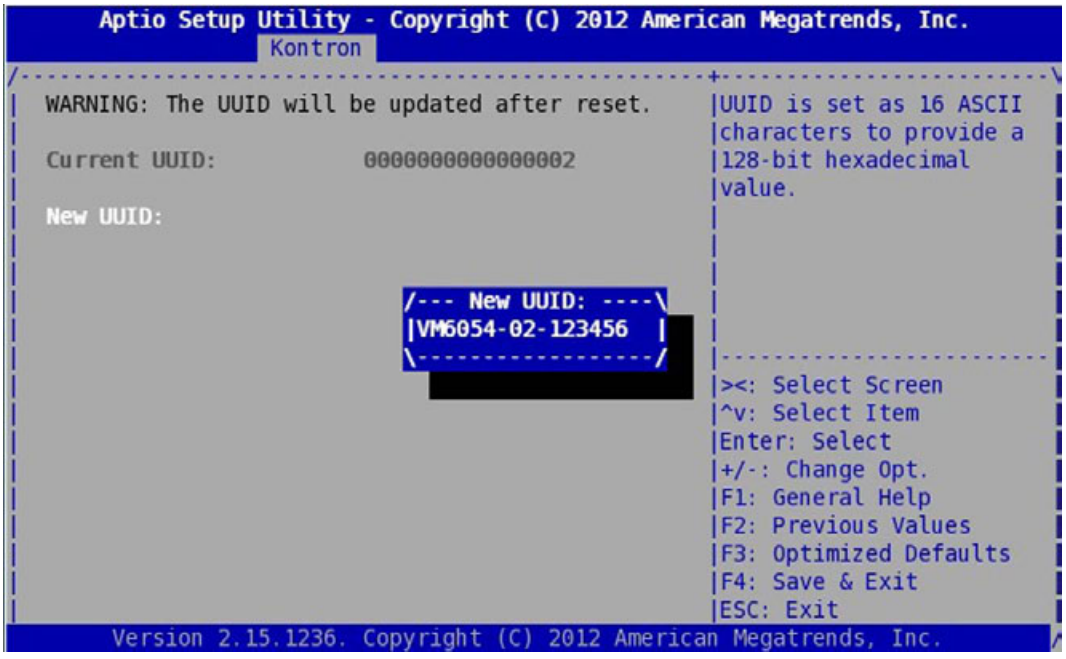
- US Keyboard
- FR Keyboard



Default is **US Keyboard**.

As only the English language is supported under BIOS, accented characters are not managed. Moreover, the characters ° £¤ µ and § are not displayed either.

5.4 UUID Configuration

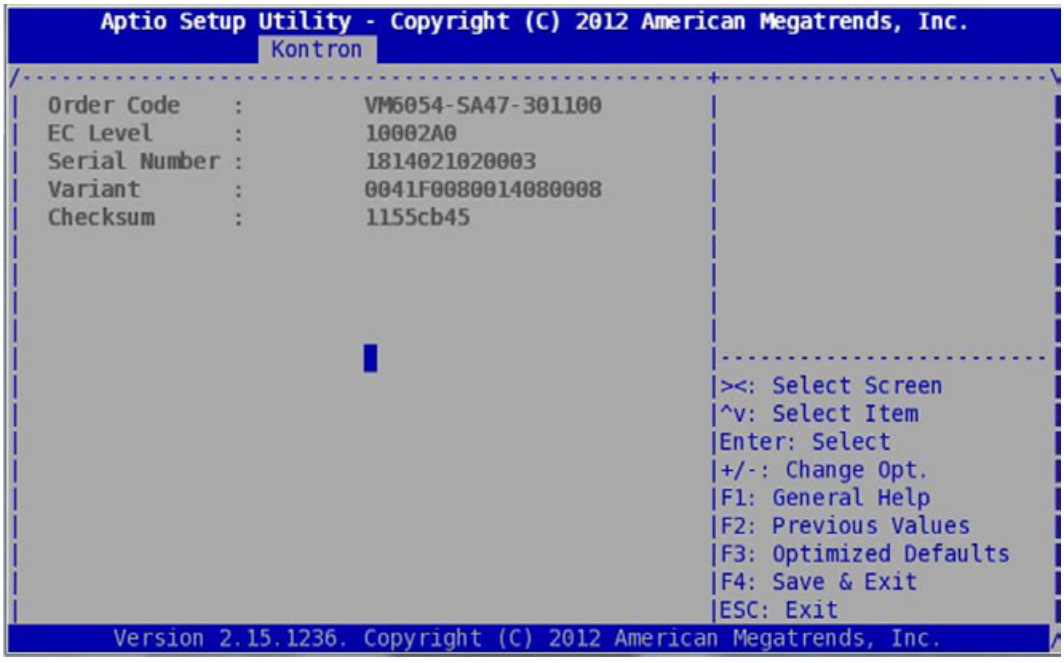


UUID stands for Universally Unique IDentifier also known as GUIDs (Globally Unique IDentifier). A UUID is 128 bits long, and can guarantee uniqueness across space and time. Please refer to RFC4122 documentation for more details about UUID.

The BIOS provides UUID to fill SMBIOS table and for PXE protocol. Default value of the UUID is set as an ASCII number equal to the Geographical Address of the board on the backplane.

This submenu provides ability for the user to modify the default value of the UUID (see picture above).

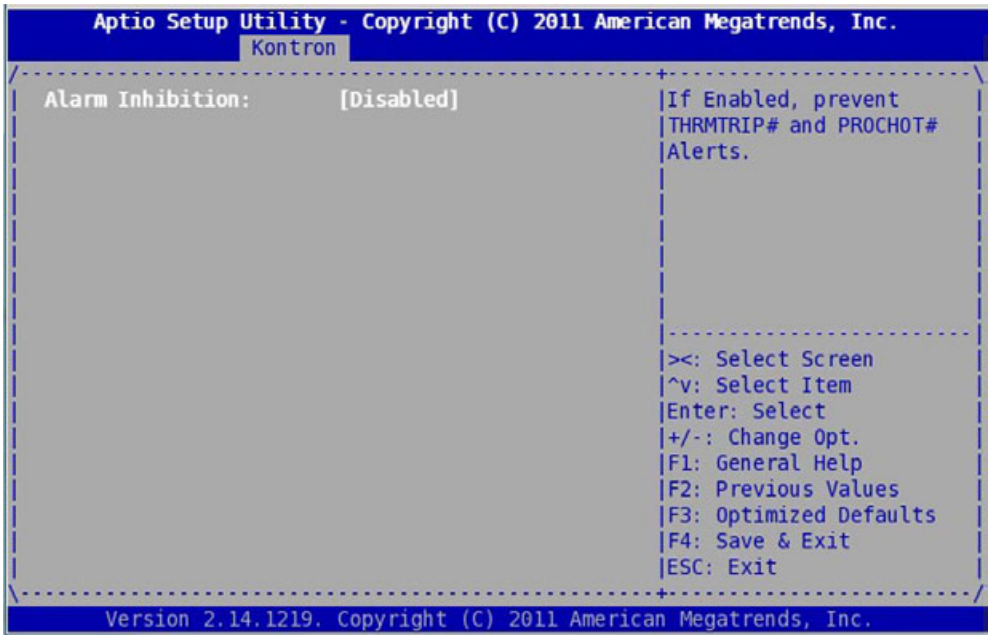
5.5 VPD – VITAL PRODUCT DATA



This menu displays the Vital Product Data (VPD) information for the board. VPD are stored in a EEPROM.

- **Order Code**: Ordering code defining the type of Board
- **EC Level**: Engineering Change Level, gives the hardware level identification
- **Serial Number**: Board Serial Number
- **Variant**: A define coding the exact hardware configuration
- **Checksum**: Checksum value of VPD area

5.6 ALARM Configuration

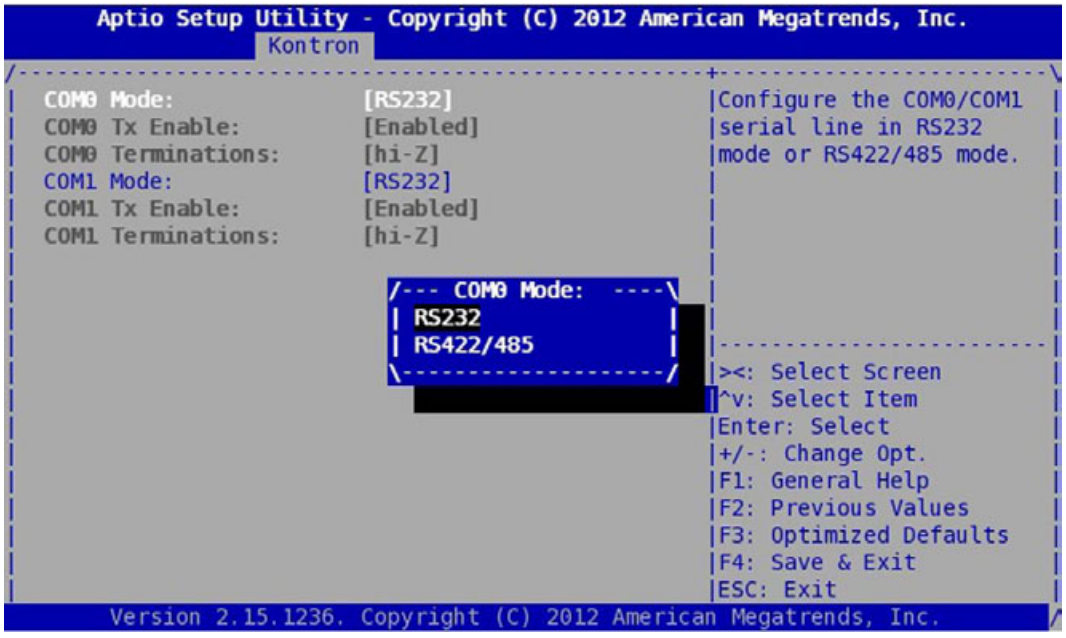


This menu allows user to prevent cPLD logic to turn off automatically the system in case of assertion of **THRMTRIP#** or **PROCHOT#** alerts.

CAUTION: it is highly recommended not to change the default setting for normal use. This parameter must be used with caution.

5.7 Serial Configuration

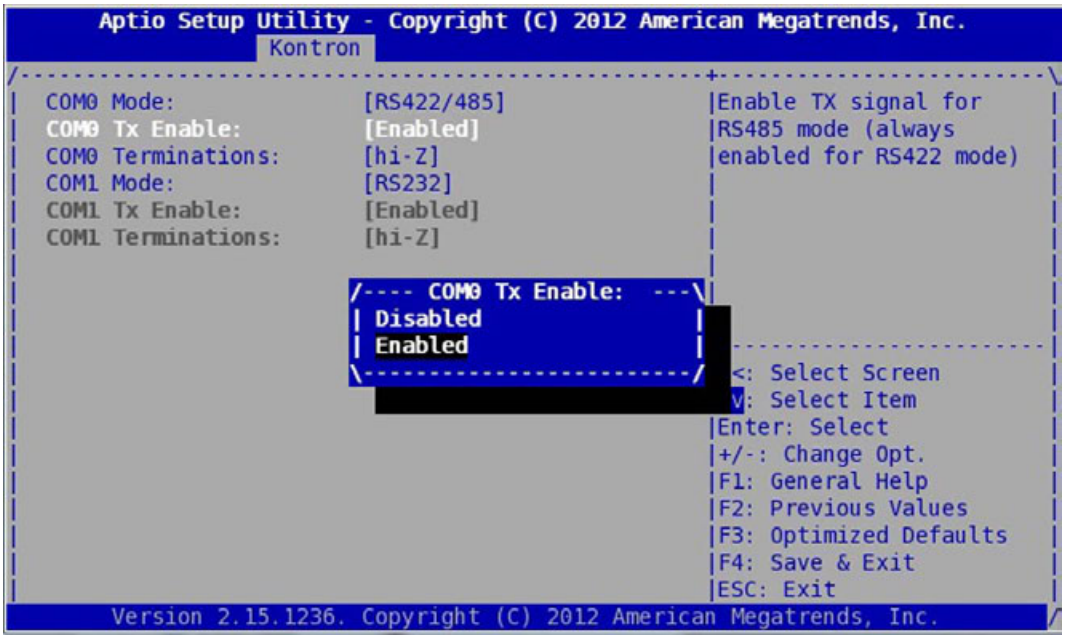
5.7.1 COM0/COM1 Mode



This option allows to select the mode for the COM0/COM1 serial ports: the supported modes are EIA-232 and EIA-422/485.

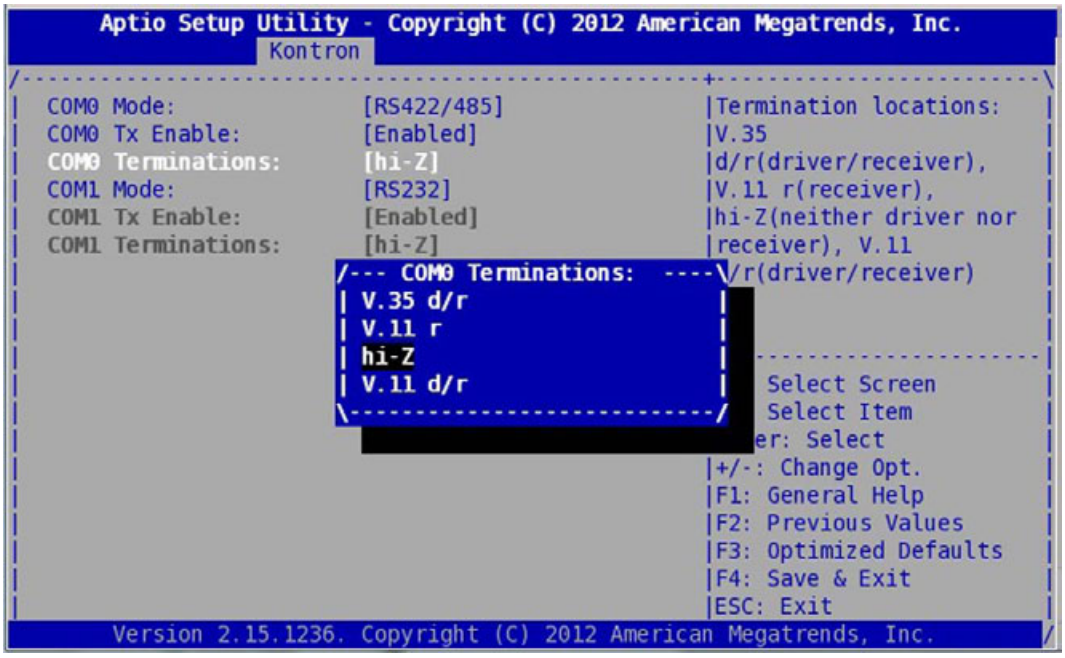
CAUTION: User must turn off the system to have the new Serial configuration taken into account. COM0/COM1 corresponds to the hardware COM1/COM2 lines

5.7.2 COM0/COM1 Tx Enable



This option allows to enable/disable transmit for the COM0/COM1 serial ports. Transmit should always be enabled in EIA-232 mode and only enabled when transmitting in EIA-422/485 mode.

5.7.3 COM0/COM1 Terminations

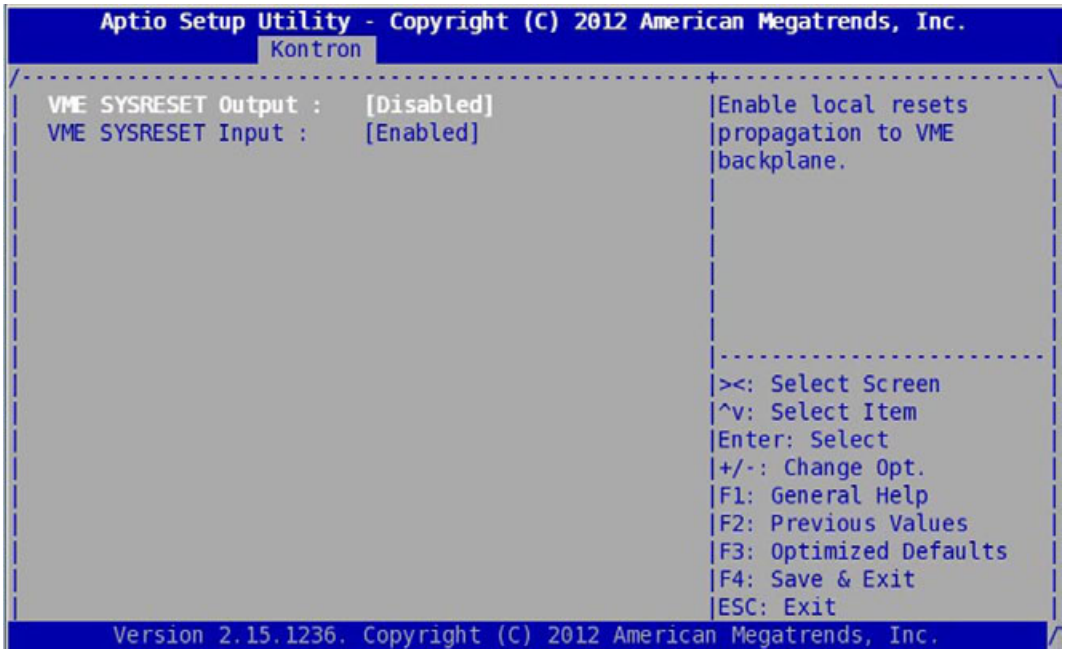


This option allows to select the terminations according to the selected mode:

- **V.35 d/r**: serial terminators used when the serial line is operating in EIA-422/485 mode with both driver and receiver terminated.
- **V.11 r**: serial terminators used when the serial line is operating in EIA-422/485 mode with only receiver terminated.
- **Hi-Z**: neither driver nor receiver is terminated. May be used for non-end point devices of a multi-drop bus, must be selected when the serial line is operating in EIA-232 mode or when the port is disabled.
- **V.11 d/r**: serial terminators used when the serial line is operating in EIA-422/485 mode with both driver and receiver terminated but no communication cable attached.

5.8 VME Configuration

This menu defines the VME SYSRESET# propagation policy in input and in output.

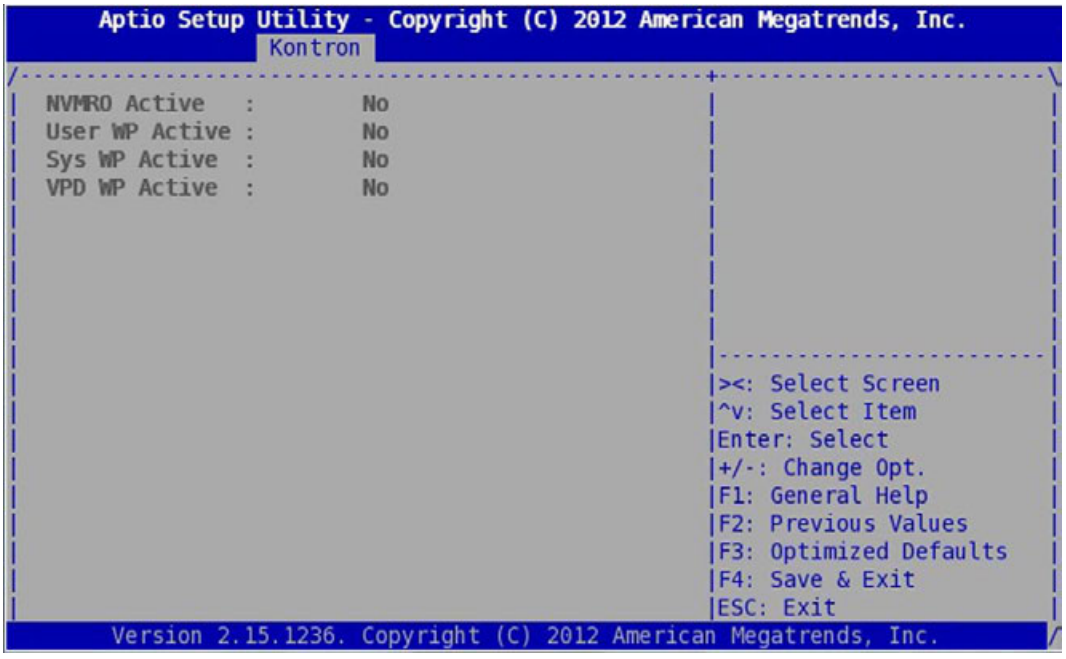


The default setting:

- Disables the local reset to propagate to the VME backplane,
- Enables the VME SYSRESET# to propagate to the local reset.

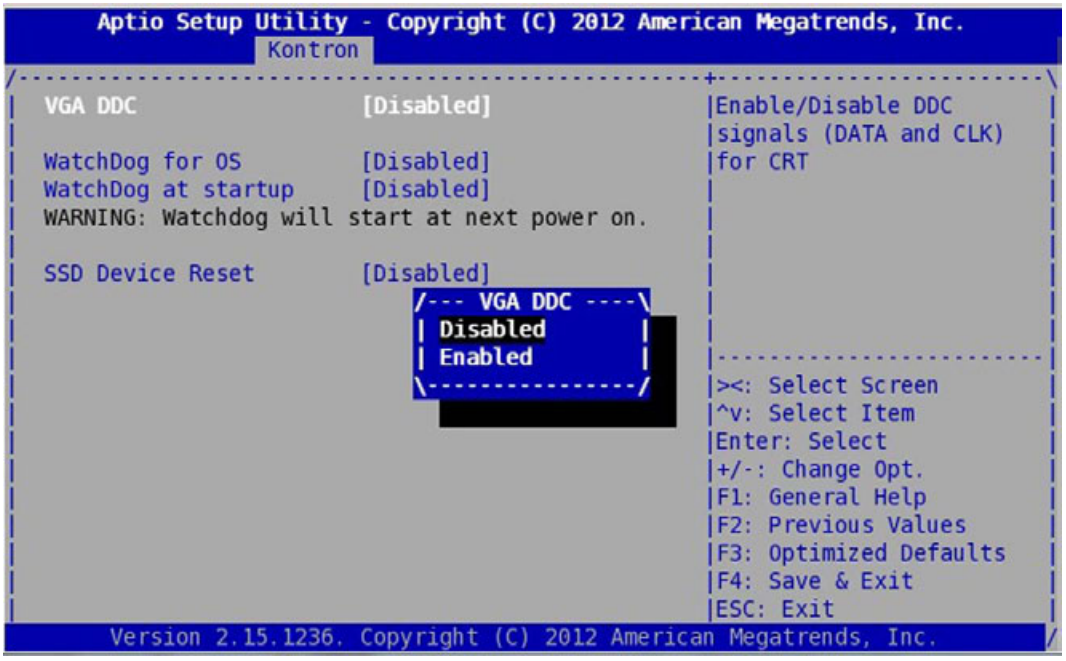
5.9 Write Protection Policy

This menu displays the NVMRO status and the configuration of the VPD EEPROM, System EEPROM and FRAM write protection switches on the hardware microswitch SW1.



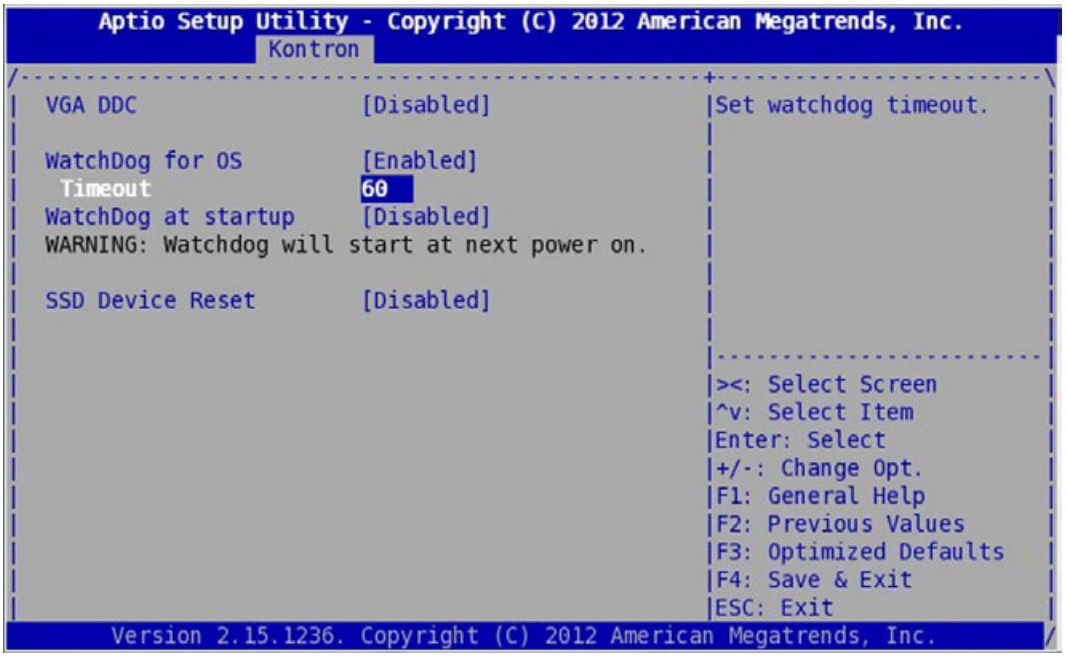
5.10 Board Misc Configuration

5.10.1 VGA DDC



This option enables/disables DDC signals for CRT detection.

5.10.2 Watchdog for OS boot



The "**WatchDog for OS**" option allows to disable (default setting) or enable the CPLD Watchdog Timer at OS boot time and to adjust the timeout value between 1 and 511 sec.

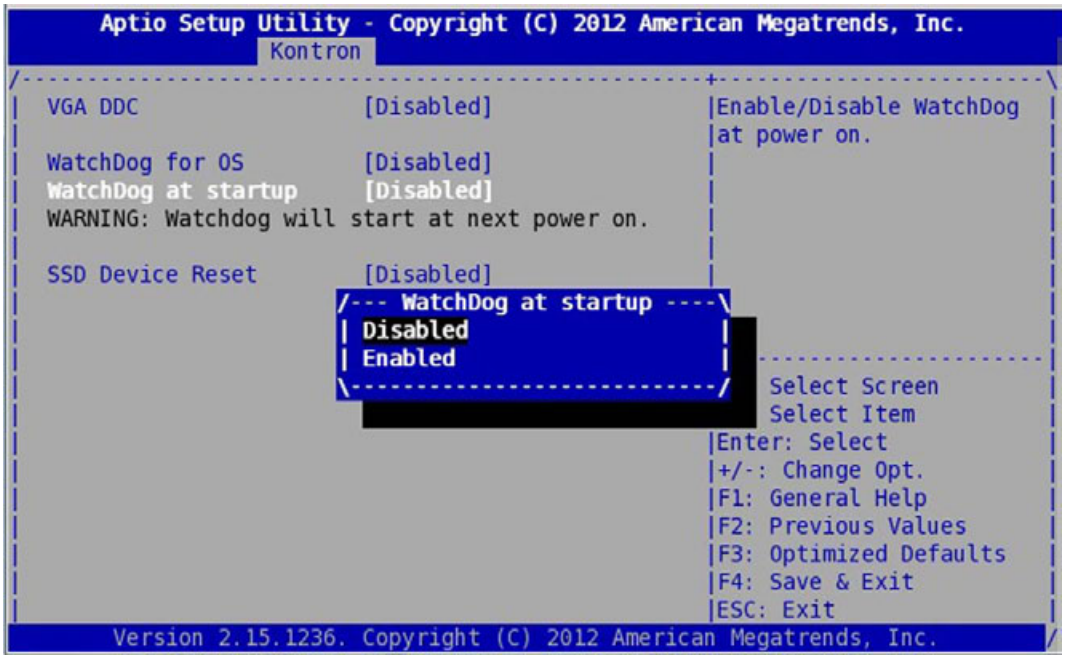
The timeout value can be changed by using the keys <+> or <->.

If enabled, the timer will be started at device boot time.

Only the power-cycle mode is handled. This mode performs a power-cycle of the board power supplies, switching the board temporarily to the standby power.

CAUTION: The WatchDog setting is kept even after a timeout has occurred.

5.10.3 Watchdog BIOS

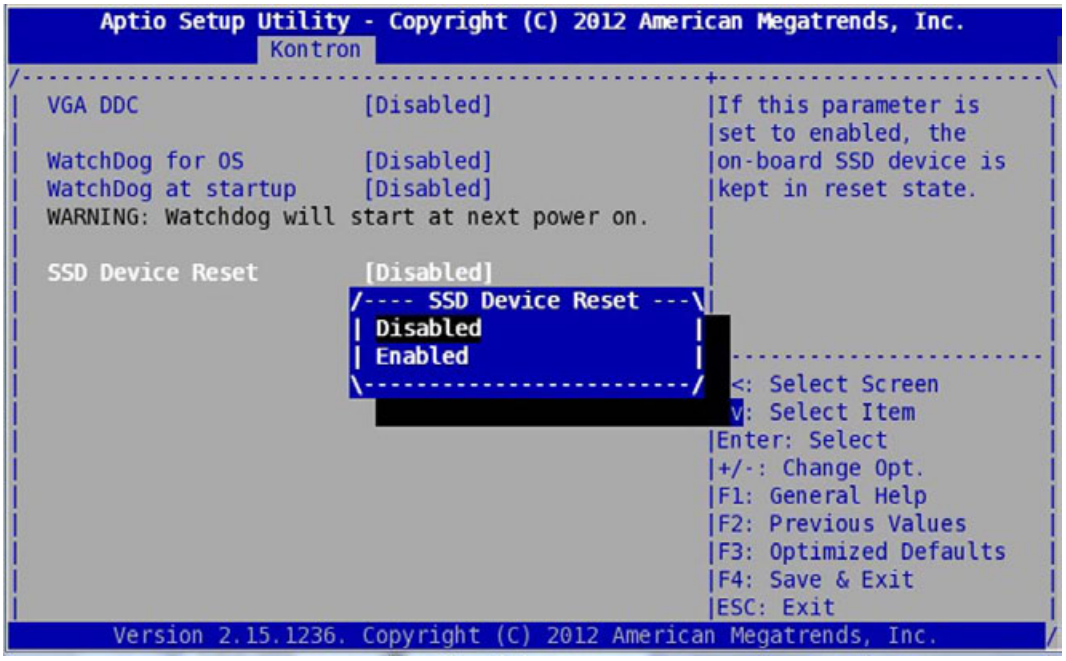


The "**WatchDog at Startup**" option allows to disable (default setting) or enable the CPLD Watchdog Timer at Power-on.

The default timeout is 21 sec and is not configurable in the setup.

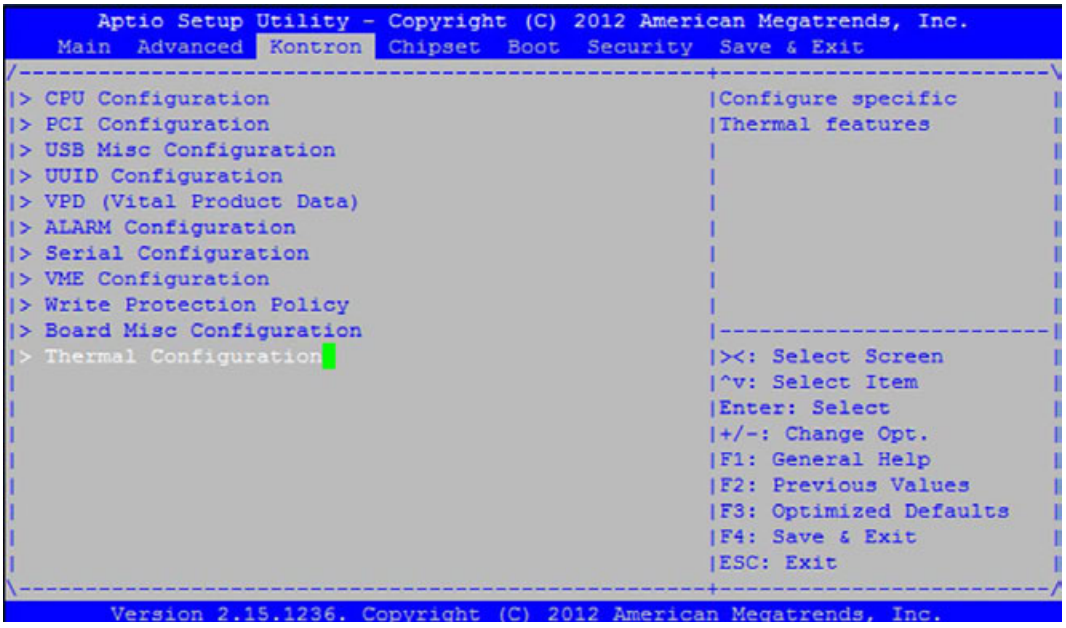
The Watchdog at Startup will start only at the next power-on of the board. Only the Power-cycle mode is handled.

5.10.4 SSD Device reset

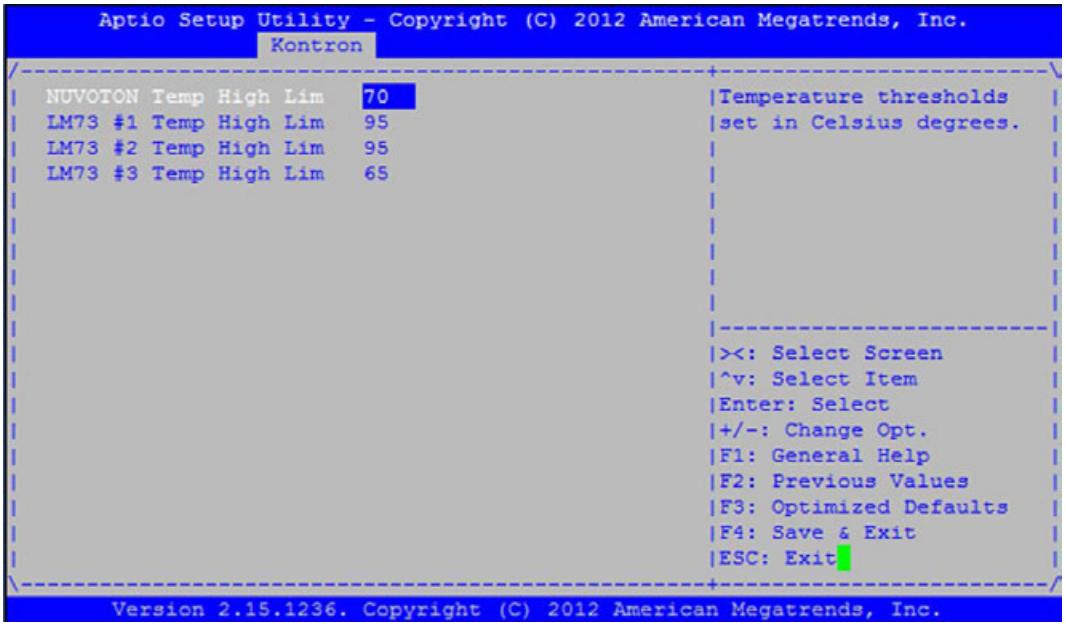


The "**SSD Device Reset**" option is used to keep the onboard SSD device in reset state. If the option is enabled, the onboard SSD device will not appear anymore in the Advanced -> SATA Configuration menu at the next power-on.

5.11 Thermal Configuration



This menu allows the user to change the high limit of the temperature sensors of the board programmed in device Nuvoton NCT7802Y and Texas Instruments LM73 #1, #2 and #3.

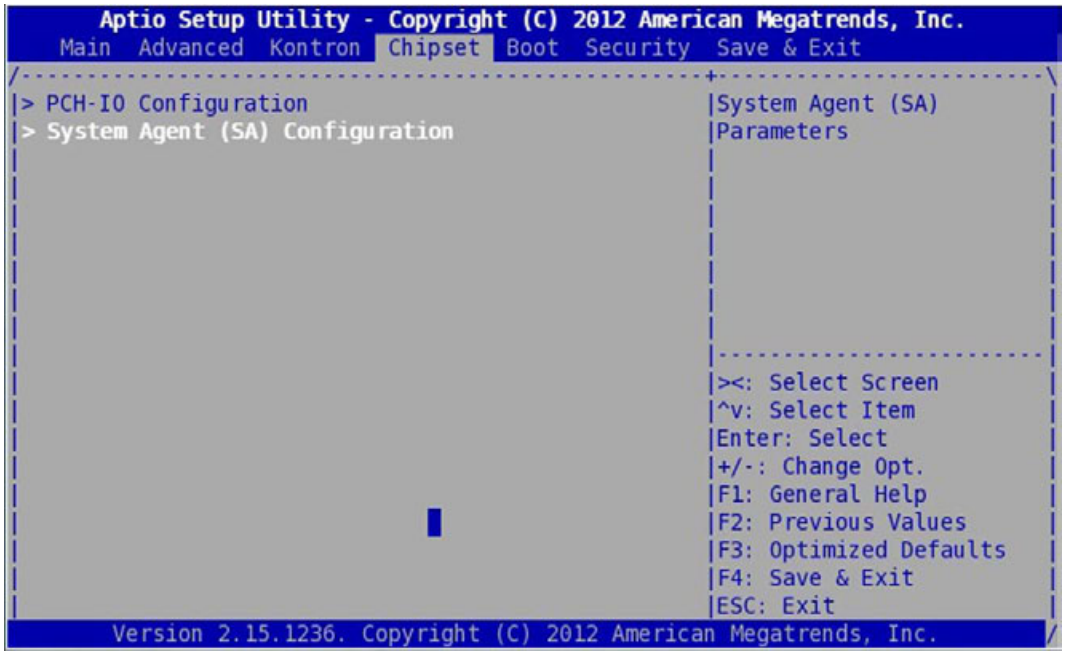


The value are positive in decimal format comprised between 0 and 255.

See VM6052/VM6054 User's Guide (CA.DT.B19) for Thermal Management on VM6052/VM6054 boards.

The temperature high limit thresholds can also be modified using ktemp EFI shell utility (see section 10.1.27 page 73). Refer to section 8 (11.1 Recommendations and Known Limitations page 100) for recommended temperature high limit thresholds regarding temperature classes.

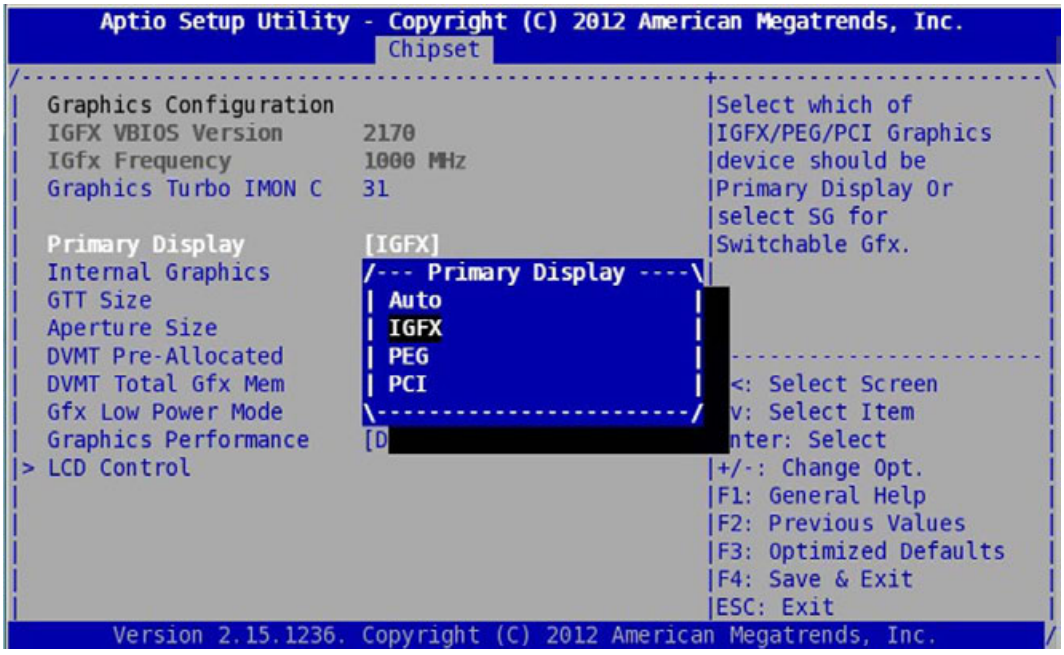
6 / Chipset Menu



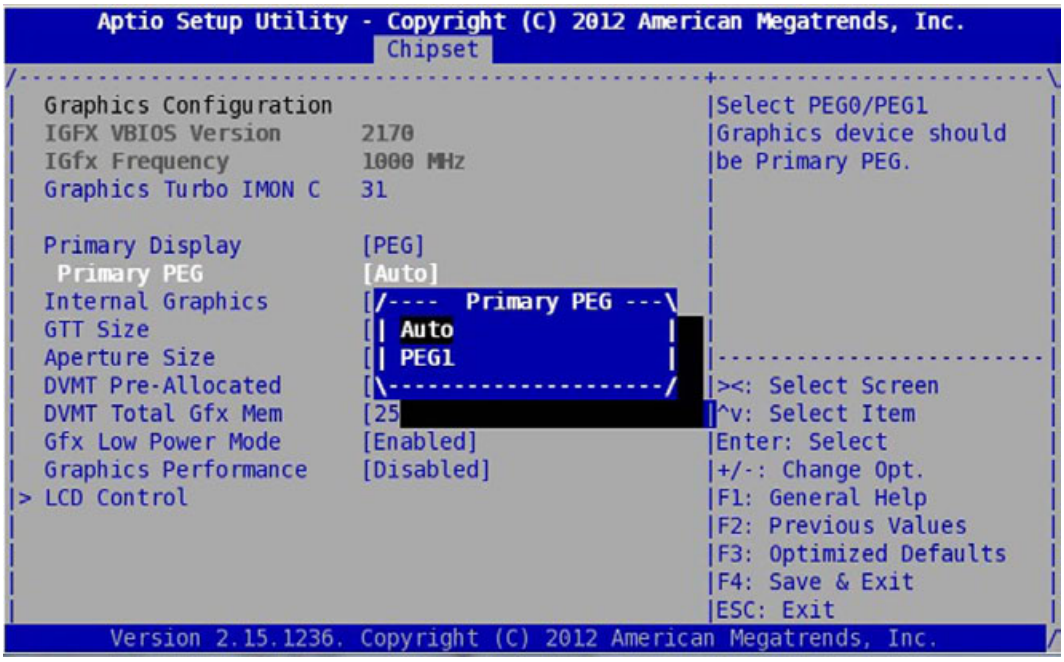
The **Chipset** menu provides system-level controls to configure the **chipset** devices settings.

The following paragraphs describe 2 examples for setting graphic device as primary display and to force memory refresh cycle.

6.1 Graphics Configuration



By default the internal video controller of the CPU, **IGFX** is selected as Primary Display.



When a graphic XMC is installed, then the Primary Display option must be set to **PEG**. If only one XMC is installed then the option Primary PEG can be let to **Auto** (default) whatever the XMC slot equipped.

If two XMCs are installed, then the XMC1 slot connected to PEG0 is selected when the option **Primary PEG** is set to **Auto**. To select the XMC2 slot connected to PEG1, the **Primary PEG** option must be changed into **PEG1**.

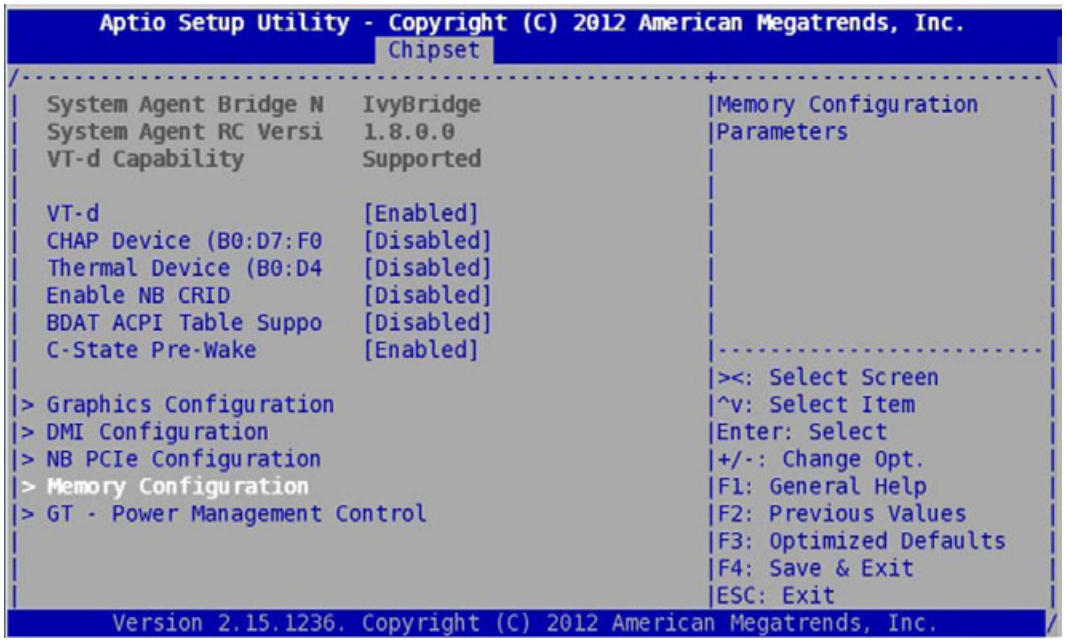
When a graphic PMC is installed into the PMC2 slot then the **Primary Display** option must be set to **PEG**. But when a graphic PMC is installed into the PMC1 slot then the **Primary Display** option must be set to **PCI**.

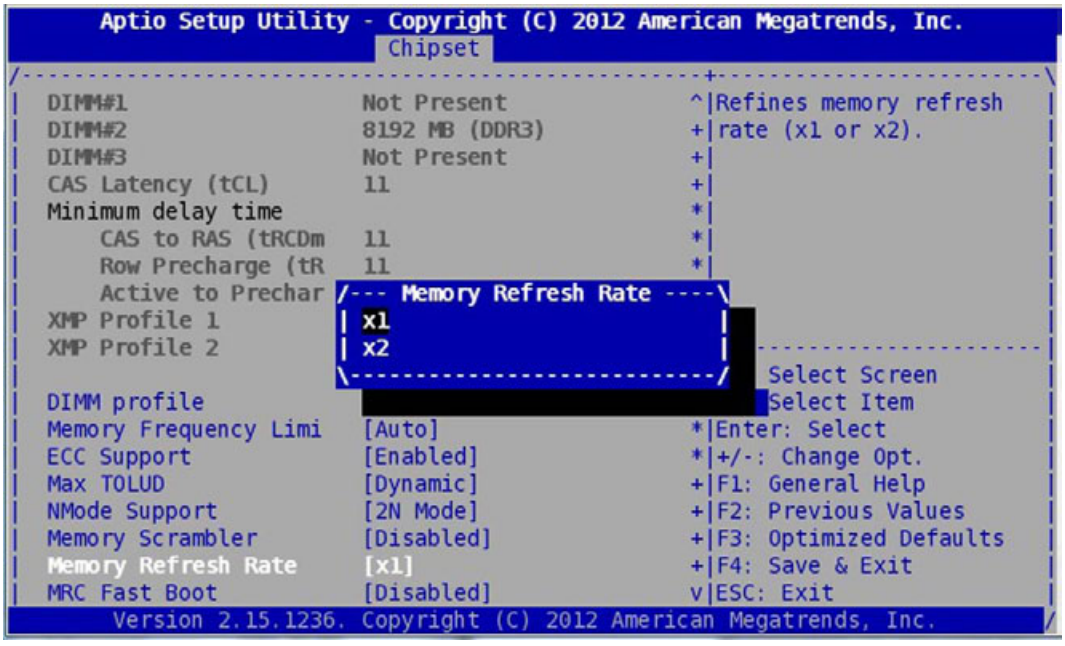
The following table summarizes the graphic configurations:

GRAPHIC SOURCE TO SELECT	PRIMARY DISPLAY	PRIMARY PEG (DEFAULT AUTO)
Internal Graphics	IGFX	Not applicable
XMC1	PEG	Auto
XMC2	PEG	PEG1 if graphic XMC1 exists
PMC1	PCI	Not applicable
PMC2	PEG	PEG1 if graphic XMC1 exists

If no graphic XMC or PMC is installed on the VM6052/VM6054 board, the BIOS force always the "Primary Display" parameter to "Auto".

6.2 Memory Configuration



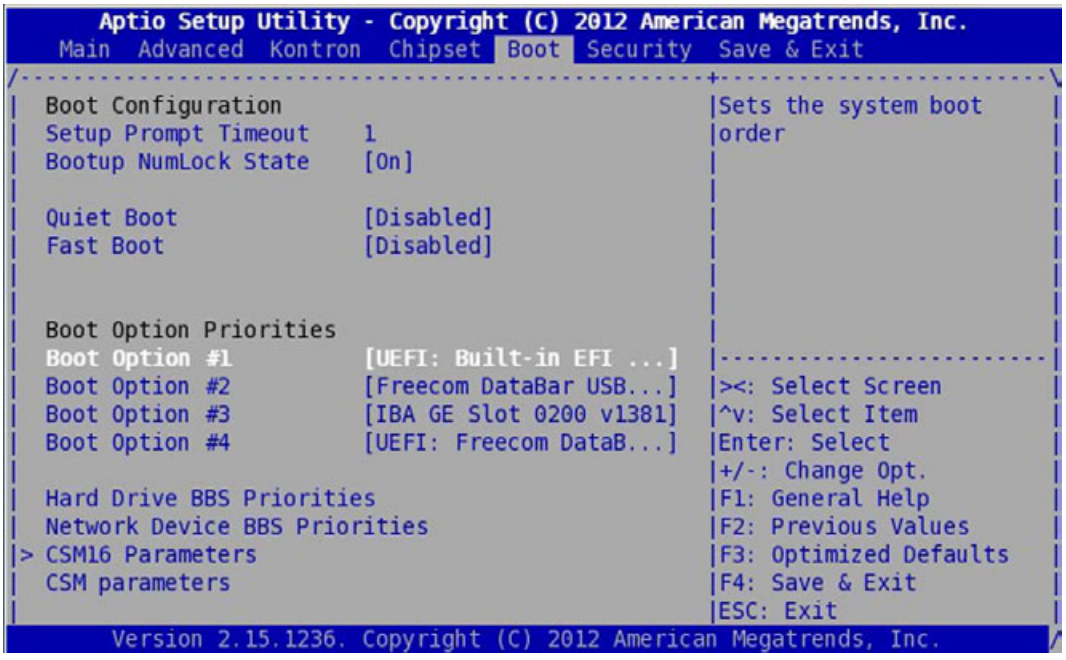


In this example, the Memory Refresh Rate refers to the DDR3 memory Refresh Rate mode which is by default set to ASR (Automatic Self-Refresh mode):

- if ASR is supported by memories part, the Refresh Rate is equal to 1X (64ms) if temperature is less than 85 °C and to 2X (32 ms) if temperature is above 85 °C.
- If the memories part does not support ASR, and temperature of the board exceed the 85 °C, it is necessary to refresh memory faster and so, user can set this parameter to **[Enabled]**: in this mode, the SRT (Self-Refresh Temperature) mode is used and the BIOS programs both the memory controller and DDR3 memories register to force SRT at 2X regardless of the temperature.

The other settings are Not intended to be changed.

7 / Boot Menu



The Boot Menu allows user to configure the boot mode and to select the boot sequence of the available boot devices. Possible Boot settings are:

- **Quiet boot**: Section 7.1 page 42
- **Setup Prompt Timeout**: Section 7.2 page 42
- **Bootup NumLock State**: Section 7.3 page 42
- **Boot Option Priorities**: Section 7.4 page 43
- **Network Device BBS Priorities**: Section 7.5 page 44
- **Hard Drive BBS Priorities**: Section 7.6 page 45
- **CSM parameters** (for OpROM execution and boot options filter): Section 7.7 page 46

The other submenus are Not to be used.

The VM6052/VM6054 boot time is about 9s after a reset and 11s after a power on, assuming boot time end is when the EFI shell prompt appears. The boot time may change depending on whether a USB device is connected or not.

7.1 Quiet boot

Quiet Boot setting when enabled allows to hide BIOS boot message such as:

```
Version 2.14.1219. Copyright (C) 2011 American Megatrends, Inc.
BIOS Date: 12/14/2012 14:37:25 Ver: 1APTJ
```

Press <DEL> or <F2> to enter setup.

7.2 Setup Prompt Timeout

Setup Prompt Timeout menu sets the number of tenth of a second for setup up activation key.

Setup Prompt Timeout

- Enter the number of tenth of a second. For example 60 for 6 seconds.

7.3 Bootup Numlock State

This menu selects the keyboard numlock state

Set **Bootup NumLock State**

- **On**
- **Off**

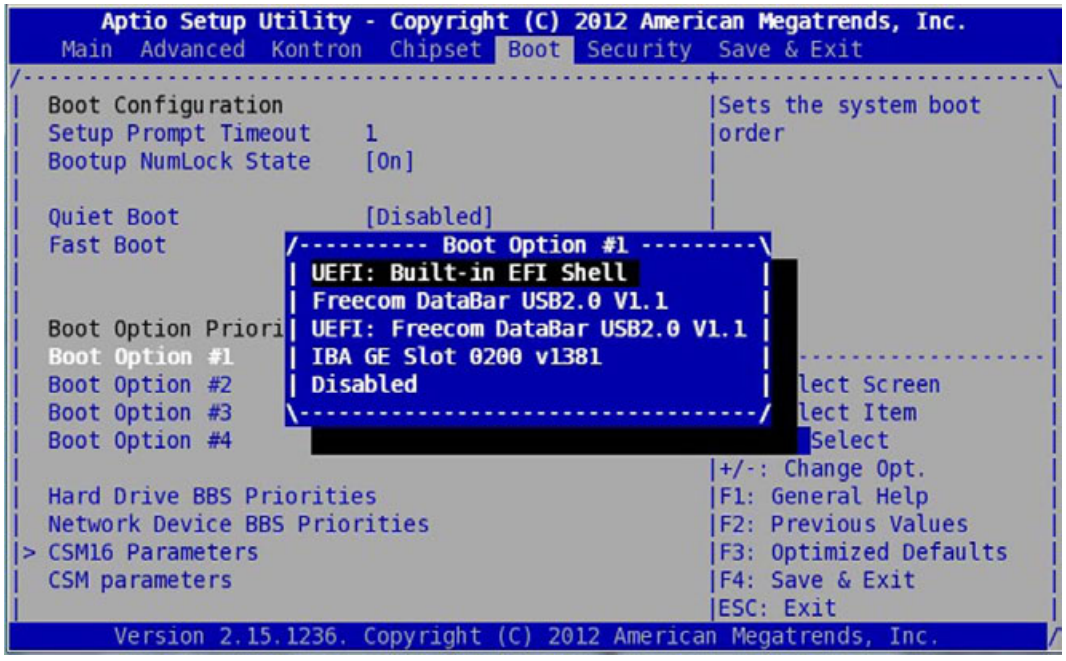
Default is **On**

7.4 Boot Option Priorities

This menu specifies the boot order from the available boot devices list.

The first device into the list is the first device that will be booted. If the boot is rejected (for example unsuccessful PXE boot) then the second device in the list will be used for boot and so on.

Here is a example of boot device list:



To change the boot device ordering

- Select a device from the list (Use the <↑> or <↓> to highlight the desired item)
- Use <+> or <-> control keys to move up/down the selected device item into the list

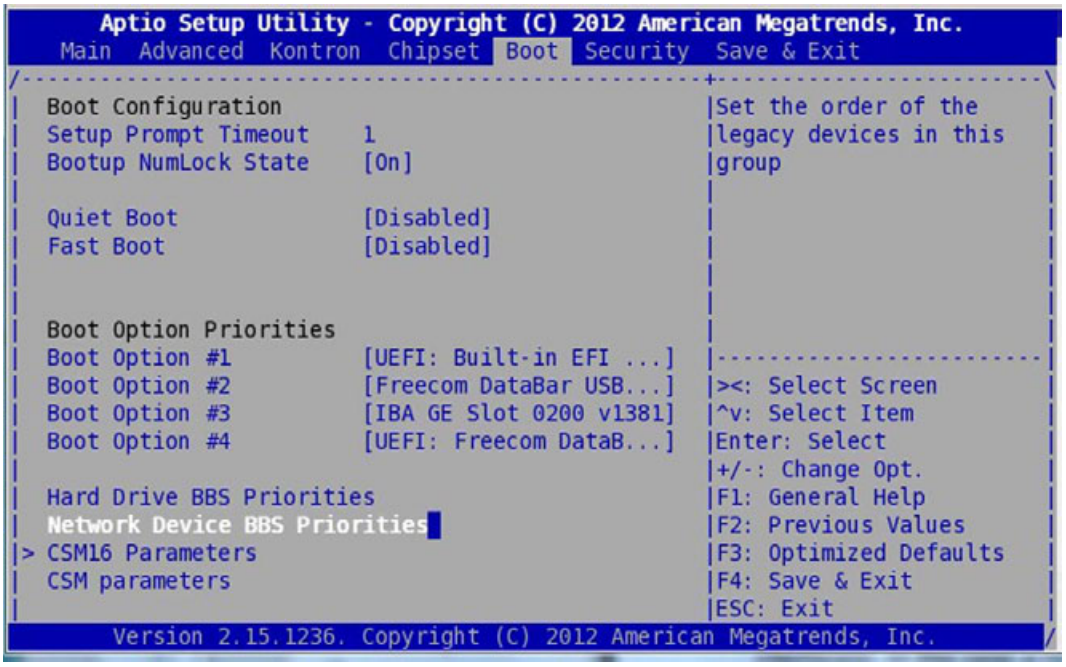
The possible family boot device can be SATA, USB or Gigabit Ethernet (Gbe). In the boot device item list only one item per family will appear. If more than one device is available for booting (for example 2 SATA disk or 3 Ethernets for PXE) then 2 new submenus can appear below the item list. So it can be:

- Hard Drive BBS Priorities This is the submenu for setting a SATA or USB boot order or deleting a SATA & USB boot possibility.
- Network Device BBS Priorities This is the submenu for setting a Gbe boot order or deleting a Gbe boot possibility

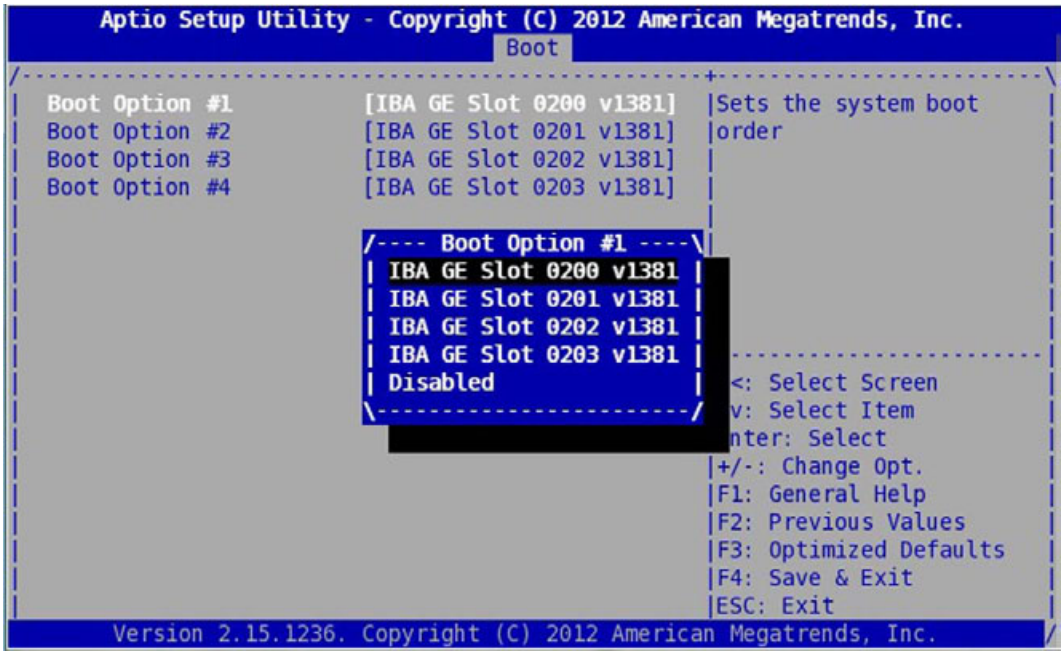
7.5 Network Device BBS Priorities (when PXE ROM Enabled)

When the PXE ROM option is enabled (refer to section 7.7 “CSM Parameters” page 46), Ethernet devices become available for PXE boot (4 Ethernet interfaces by default).

The following submenu “**Network Device BBS Priorities**” appears in the Boot Setup menu and allows to configure the Ethernet boot device sequence for PXE.



Select the submenu to display the available Ethernet devices and to change the boot order.



The network devices named as "**IBA GE Slot 0200 v1381**" are related to the Ethernet interfaces of the Intel 82580 controller.

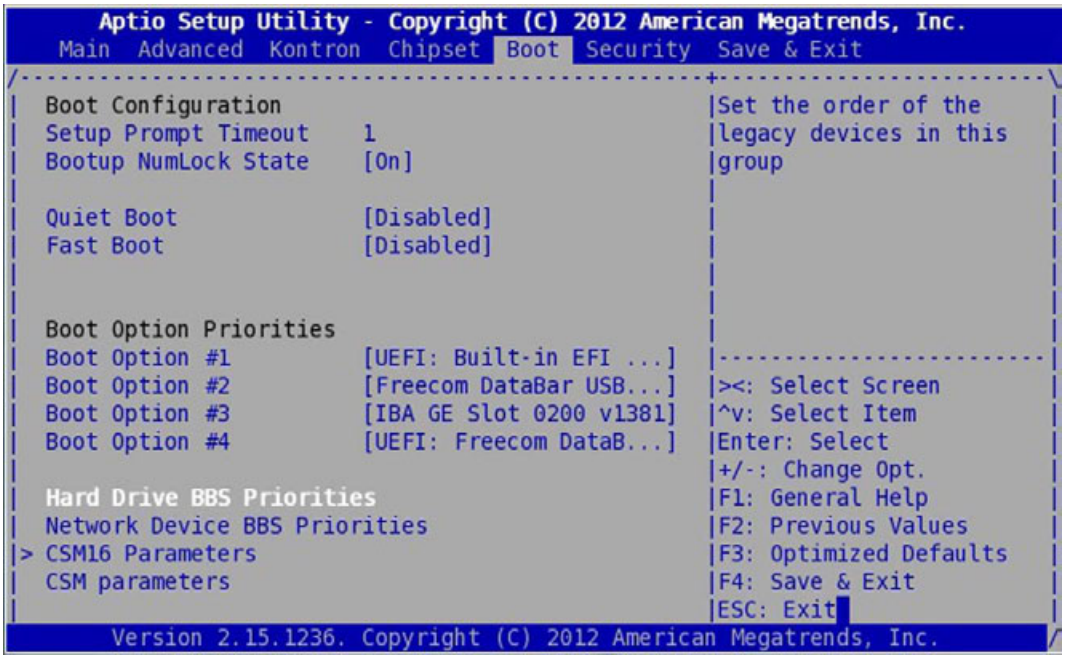
To change the boot device order, select a **Boot Option** number and then select the target device displayed in the list.

To disable a **Boot Option** entry, select “**Disabled**” in the list.

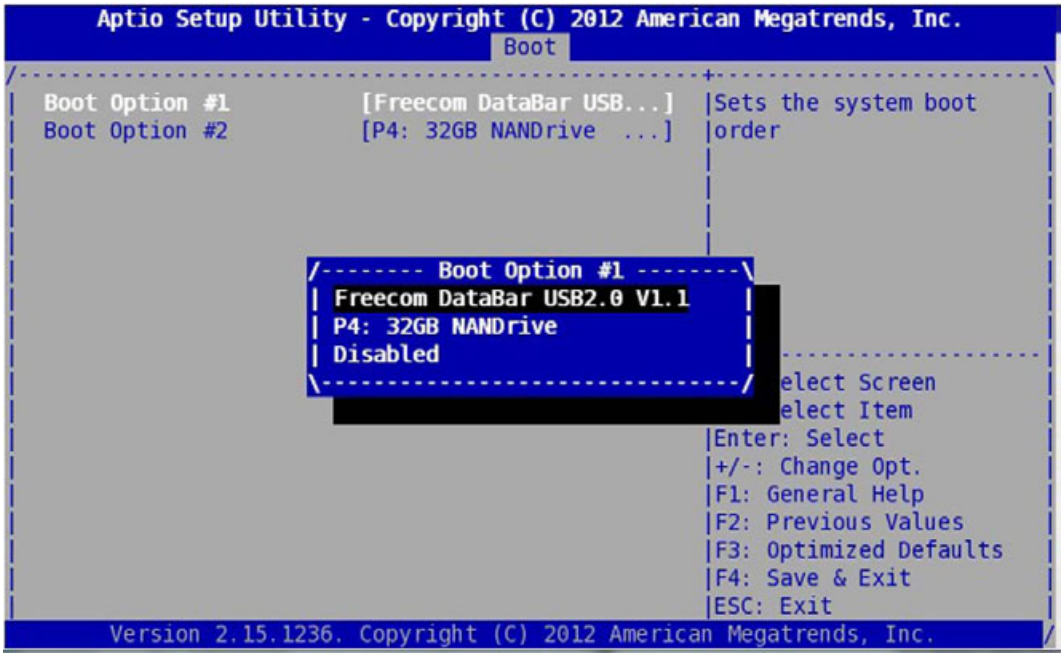
7.6 Hard Drive BBS Priorities

The following submenu appears in the Boot Setup menu when SATA or USB devices are connected.

It allows to configure the SATA/USB boot device sequence.



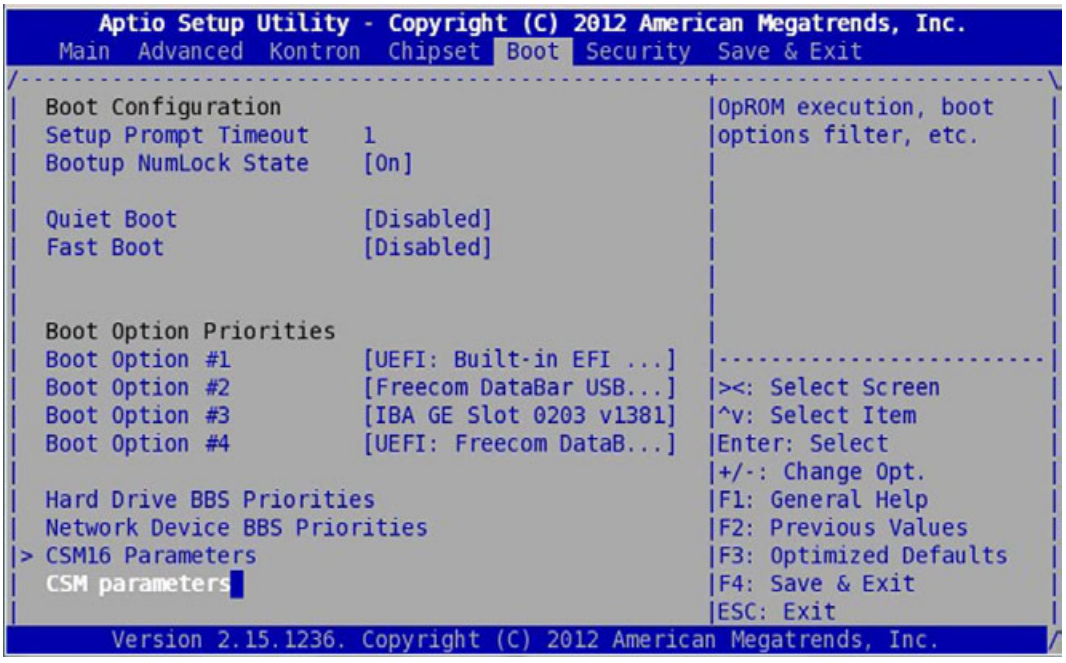
Select the submenu to display the available devices and to change the boot order.

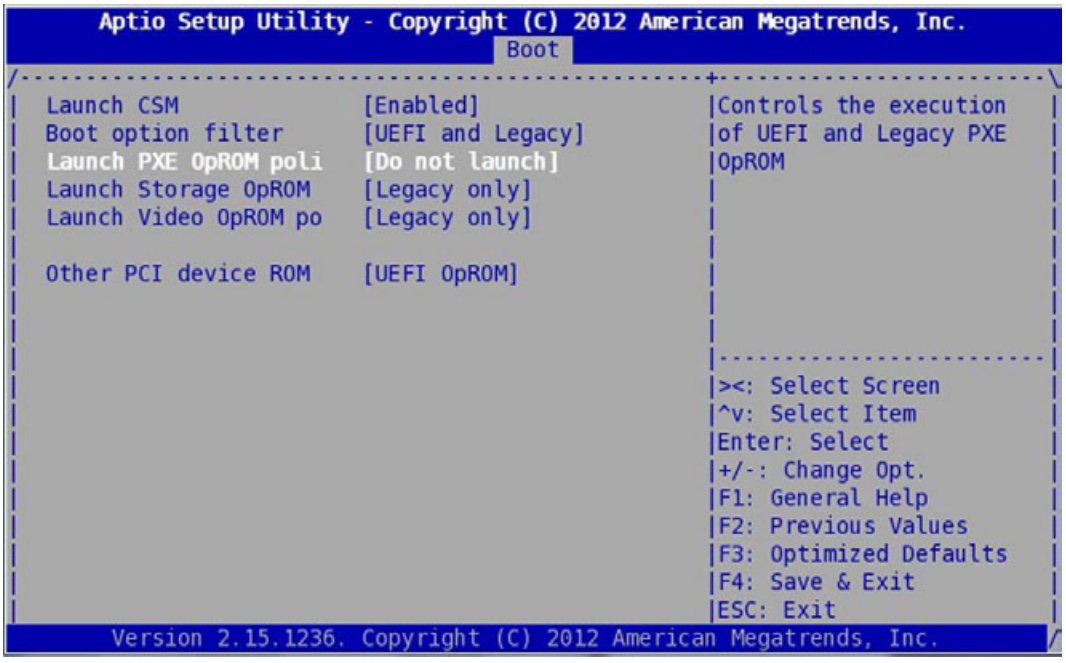


To change the boot device order, select a **`Boot Option`** number and then select the target device displayed in the list.

To disable a **`Boot Option`** entry, select "**`Disabled`**" in the list.

7.7 CSM Parameters





7.7.1 Launch CSM Parameter

This parameter must be set to **[Enabled]** to enable boot with Legacy devices.

7.7.2 Boot Option Filter

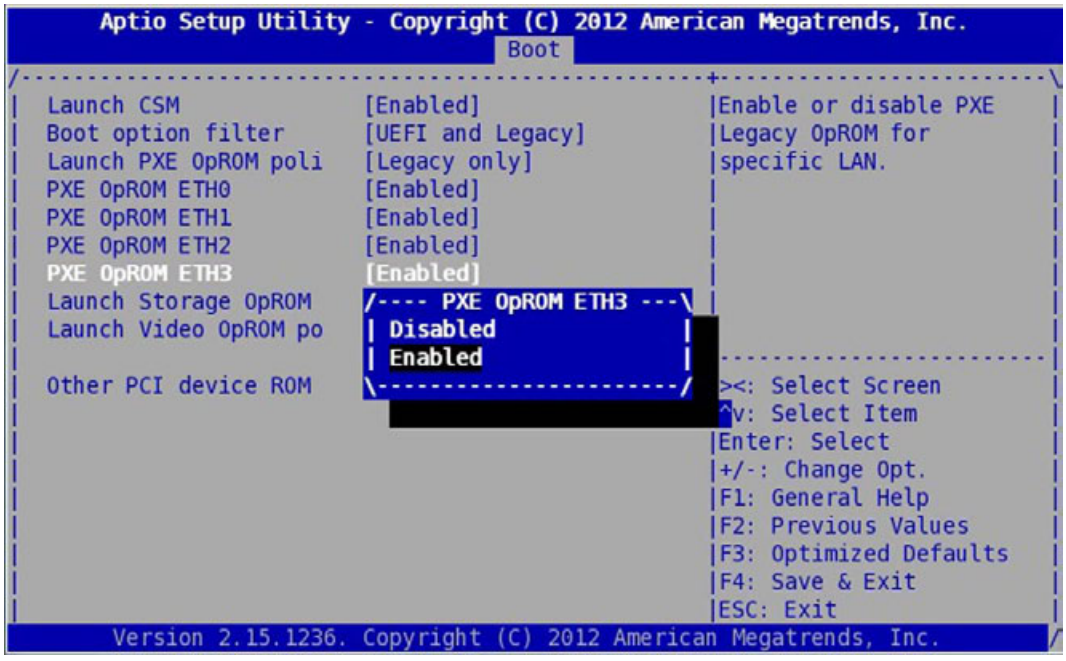
This parameter must be set to **[UEFI and Legacy]** in order to have bootable Legacy devices.

7.7.3 Launch PXE OpROM Policy

Defaut is **[Do not launch]**; set this parameter to **[Legacy Only]** to have Network Bootable Devices access in boot menu.

PXE Option ROM can be individually **Enabled** or **Disabled** for each Ethernet Interface.

By default, all PXE Option ROM are **Enabled**.



7.7.4 Launch Storage OpROM

Default is **[Legacy only]**; SATA RAID devices are allowed to boot to. Set to **[Do no launch]** if you want to disable boot to SATA RAID devices.

7.7.5 Launch Video OpROM Policy

This parameter must be set to **[Legacy Only]** to enable graphics on Legacy OSes.

7.7.6 Other PCI Device ROM

This parameter must be set to **[Legacy OpROM]** to enable Option ROM for Legacy PCI devices other than Network, Storage of Video Option ROMs.

8 / Security Menu

The **Security** Menu allows the user to set a password for SETUP or boot access.

If ONLY the Administrator's password is set, then this only limits access to Setup and is only asked for when entering Setup.

If ONLY the User's password is set, then this is a power on password and must be entered both to boot or enter Setup. In Setup, the User will have Administrator rights. If both passwords are set, then in setup the user will access as "View Only"

A HDD Security Configure submenu can appear when a SATA disk is connected.

This submenu is Reserved and Not To Be Used

8.1 Enter Administrator or user password

To enter the password:

- Select the administrator or user password item
- A pop-up window appears and proposes to create a new password
- Enter a password with lenght between 1 to 20 characters
- You will have to confirm the password
- The password will then be saved if the command "**Save changes**" is launched in **Save & Exit** Menu.

During the next reboot, if the <F2> key is pressed, then the password becomes mandatory to enter the SETUP menu.

When the user password is set, the password is required to enter setup menu and to execute the BIOS boot device selection.

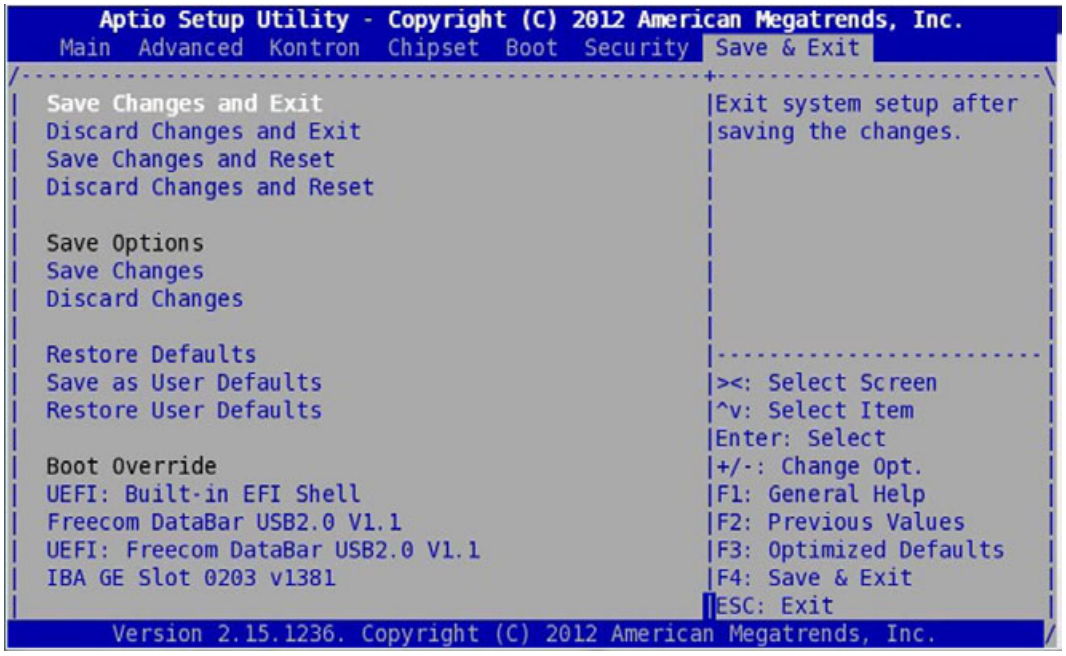
To suppress or change the password

- Select the administrator or user password item
- A pop-up window appears and proposes to enter a password
- Enter previous password
- A pop-up window appears and proposes to enter a new password
- Then type an empty password
- You will have to confirm empty password
- The password will be deleted if the command "**Save changes**" is launched in the **Save & Exit** Menu.

If the password is lost, the solution to unlock is to flash the BIOS again.

If an Administrator password is set, then it is required to create/suppress/change the User Pass–word

9 / Save & Exit Menu



This Menu is used to save a new SETUP configuration, discard changes, restore default SETUP values, record a customized SETUP and override the boot device sequence. This menu does not appear as the first window when entering SETUP. It is necessary to navigate from the main menu to find it.

Available submenus are

- **Save Changes and Exit**: section 9.1 page 52
- **Discard Changes and Exit**: section 9.1 page 52
- **Save Changes and Reset**: section 9.1 page 52
- **Discard Changes and Reset**: section 9.1 page 52
- **Save Changes**: section 9.2 page 52
- **Discard Changes**: section 9.2 page 52
- **Restore Defaults**: section 9.2 page 52
- **Save as User Defaults**: section 9.3 page 53
- **Restore User Defaults**: section 9.3 page 53
- **Boot Override**: section 9.4 page 53

9.1 Option with Exit or Reset

With one of the following options the user can choose to save or record the changes in SETUP and to reset or exit SETUP. Reset will perform a complete board reset while Exit will execute the Boot Device Selection for booting. To apply SETUP parameter modifications a reset is mandatory.

Select desired item and <Enter>

- Save Changes and Exit
- Discard Changes and Exit
- Saving the changes and reset
- Save Changes and Reset

9.2 Option to Save Discard Restore SETUP

SETUP modification can simply be Saved or Discarded without exiting BIOS SETUP. Also manufacturing default SETUP parameters can be restored with Restore Defaults menu.

Select desired item and <Enter>

- Save Changes
- Discard Changes
- Restore Defaults

CAUTION: For the RC class boards, the **`Restore Defaults`** option restores the specific SETUP parameters as follows:

SETTINGS FOR RC CLASS	VALUE FOR VM6052-RC	VALUE FOR VM6054-RC
Intel Speed Step (EIST)	ENABLED	ENABLED
Turbo Mode	DISABLED	DISABLED
C-STATES	DISABLED	DISABLED
Configurable TDP	NOMINAL	
CPU Frequency		2100 MHz(*)
DDR3 Double Refresh Rate Control	ENABLED	ENABLED
PEG2 Speed	GEN1	GEN1
Internal Graphics	ENABLED	ENABLED
Hyper-Threading	ENABLED	ENABLED
Launch PXE policy	Do not launch	Do not launch
VME Reset Ouput: Local reset propagation to VME	DISABLED	DISABLED

(*) For VM6054/WA class board, the CPU Frequency is set by default to 1200 MHz

CAUTION: For the WA and RC classes boards, the Restore Defaults option restores the default temperature high limit thresholds for SA class as defined in table section 8 (Recommended and Known Limitations page 100). User must restore temperature high limit thresholds according to the environmental conditions and board class in the Setup (see section 5.11 page 36) or using ktemp EFI shell utility (see section 10.1.27 page 73).

9.3 Saving a User Configuration

The current SETUP configuration can be saved as the user configuration and can be restored the same way as the default one.

Select desired item and <Enter>

- Save as User Defaults
- Restore User Defaults

9.4 Boot Override

The current sequence of boot devices can be overriden by this menu.

- Select a device from the list (Use the <↑> or <↓> to highlight the desired item
- <Enter> to immediately Boot on this device

10 / EFI SHELL

EFI Shell is a boot shell available on the VM6052/VM6054 that is accessible in the boot device list. EFI Shell is launched automatically if no other boot device is connected to the VM6052/VM6054. If EFI shell is not the primary boot device then it is necessary to enter the SETUP menu to access it. For this, enter <F2> during boot process to enter SETUP. Then navigate to **Save & Exit** Menu and select **UEFI shell** in Boot override menu.

EFI SHELL is available by default on the graphical display or serial line COM0 configured at 115200 bauds.

EFI SHELL implements a set of command utilities and can be used to access or display various resources, to flash a new BIOS image or execute a start-up script.

10.1 EFI Shell Command

The **Help** command or **(?)** displays all the available command. Use option **-b** to display command screen by screen. Use **help +** command (like **VM6052/VM6054> help help**) to have the detail of a command syntax

- VM6052/VM6054> help

COMMAND NAME	DESCRIPTION	SEE SECTION
?	Displays the EFI Shell command list or verbose command help	10.1.19 page 68
alias	Displays, creates, or deletes EFI Shell aliases	10.1.1 page 56
amlview	AML view utility	10.1.2 page 57
bcfg	Boot configuration utility	10.1.3 page 58
cd	Displays or changes the current directory	10.1.4 page 59
cls	Clears standard output and optionally changes background color	10.1.5 page 60
connect	Connects one or more EFI drivers to a device	10.1.6 page 60
cpuutil	CPU information utility	10.1.7 page 60
date	Displays or changes the current system date	10.1.8 page 61
devices	Displays the list of devices managed by EFI drivers	10.1.9 page 61
dh	Displays EFI handle information	10.1.10 page 62
disconnect	Disconnects one or more EFI drivers from a device	10.1.11 page 64
drivers	Displays the EFI driver list	10.1.12 page 64
dumpacpi	Prints ACPI Tables	10.1.13 page 65
dumpaml	Prints AML dump	10.1.14 page 65
echo	Controls batch file command echoing or displays a message	10.1.15 page 66
exit	Exits the EFI Shell environment	10.1.16 page 66
for	Executes commands for each item in a set of items	10.1.17 page 67
goto	Forces batch file execution to jump to specified location	10.1.18 page 68
help	Displays the EFI Shell command list or verbose command help	10.1.19 page 68
if	Executes commands in specified conditions	10.1.20 page 69
ifconfig	UEFI network modification utility	10.1.21 page 70

COMMAND NAME	DESCRIPTION	SEE SECTION
kdiag	Performs board diagnostics - Available ONLY if ordered.	10.1.22 page 70
kflash	Kontron SPI flasher	10.1.23 page 71
kmac	Kontron MAC Address viewer	10.1.24 page 71
kpld	Kontron PLD Commands	10.1.25 page 72
ksata	Kontron SATA Configurator	10.1.26 page 72
ktemp	Kontron Board Temperature	10.1.27 page 73
kvpd	Kontron VPD Information	10.1.28 page 75
ls	Displays a list of files and subdirectories in a directory	10.1.29 page 76
map	Displays or defines mappings	10.1.30 page 78
mem	Displays the contents of memory	10.1.31 page 82
memmap	Displays the memory map	10.1.32 page 84
mm	Displays or modifies MEM/MMIO/IO/PCI/PCIE address space	10.1.33 page 86
pause	Prints a message and waits for keyboard input	10.1.34 page 88
pci	Displays PCI device list or PCI function configuration space	10.1.35 page 90
reconnect	Reconnects one or more EFI drivers to a device	10.1.36 page 94
reset	Resets the system	10.1.37 page 94
set	Displays or modifies EFI Shell environment variables	10.1.38 page 94
shift	Shifts batch file input parameter positions	10.1.39 page 95
smbiosview	Displays SMBIOS information	10.1.40 page 96
smbutil	SMBus utility	10.1.41 page 96
time	Displays or changes the current system time	10.1.42 page 97
timezone	Displays or sets time zone information	10.1.43 page 97

10.1.1 alias

Displays, creates, or deletes aliases in the EFI Shell environment.

```
ALIAS [-d|-v] [sname] [value]
```

-d	Deletes an alias
-v	Volatile variable
sname	Alias name
value	Original name

1. '**sname**' should not be an internal EFI Shell command.
2. '**value**' can be an internal EFI Shell command, a script, or an EFI application. However, any other values are also acceptable.
3. **ALIAS** values are stored in EFI NVRAM and will be retained between boots unless the '**-v**' option is specified.
4. **ALIAS** will not add a nonvolatile alias when a volatile alias of the same name already exists, or vice versa.

- Examples:
  - To display all aliases in the EFI Shell environment:

```
Shell> alias
               md   : mkdir
               rd   : rm
```

  - To create an alias in the EFI Shell environment:

```
Shell> alias myguid guid
Shell> alias
               md            : mkdir
               rd            : rm
               myguid        : guid
```

  - To delete an alias in the EFI Shell environment:

```
Shell> alias -d myguid
Shell> alias
               md   : mkdir
               rd   : rm
```

  - To add a volatile alias in the current EFI environment, which has a star * at the line head. This volatile alias will disappear at next boot.

```
Shell> alias -v fs0 floppy
Shell> alias
               md            : mkdir
               rd            : rm
               * fs0         : floppy
```

10.1.2 Amlview

Views ACPI1.0b, ACPI2.0, or ACPI3.0 AML in EFI Shell Environment.

```
usage: AMLView [<AML file>]
```

Also AmlView proposes its own shell syntax

```
Shell> amlview
Welcome to AmlView on EFI Shell (Version 0.01)
DefinitionBlock ("Dsdt.aml", "DSDT", 2, "ALASKA", "A M I", 24)
```

AmlView > help

```
EXEC     <NodeName>          : Prints the result of the method node.
CAT      <NodeName>          : Prints the node content.
LS [-R] [<NodeName>]         : Lists the node name. (-R means recursive)
CD      [<NodeName>]         : Changes current node dir.
QUIT                         : Quits Current Command Prompt.
HELP                         : Prints Help Information.
(NodeName format - [\]AAAA[.BBBB[...]])
```

10.1.3 bcfg

bcfg is an utility for boot configuration.

```
bcfg driver|boot [dump [-v]][add # file "desc"][rm #] [mv # #]
```

driver	selects boot driver list
boot	selects boot option list
dump	dumps selected list
-v	dumps verbose (includes load options)
add	adds '**file**' with '**desc**' at position **#**
addp	adds '**file**' with '**desc**' at position **#**.Use hard drive path
addh	adds '**handle**' with '**desc**' at position **#**.Use Handle
rm	removes **#**
mv	moves **#** to **#**

- **Example:**

The following example shows the ability to change boot device order without entering in BIOS setup.

```
Shell > bcfg boot dump
The boot option list is:
01. VenMedia(5023b95c-db26-429b-a648-bd47664c8012) "UEFI: Built-in EFI Shell " OPT
02. BBS(HD,,0x0) "Hard Drive " OPT
03.
PciRoot(0x0)/Pci(0x1,0x0)/Pci(0x0,0x0)/MAC(0000de404176,0x0)/IPv4(0.0.0.0,0x0,DHCP,0.0.0.0,0.0.0.0,0.0
.0.0) "UEFI: Intel(R) 10 Gigabit Network Connection" OPT
04.
PciRoot(0x0)/Pci(0x1,0x0)/Pci(0x0,0x1)/MAC(0000de404177,0x0)/IPv4(0.0.0.0,0x0,DHCP,0.0.0.0,0.0.0.0,0.0
.0.0) "UEFI: Intel(R) 10 Gigabit Network Connection" OPT
05.  PciRoot(0x0)/Pci(0x19,0x0)/MAC(0000de404175,0x0)/IPv4(0.0.0.0,0x0,DHCP,0.0.0.0,0.0.0.0,0.0.0.0)
"UEFI: Intel(R) 82579LM Gigabit Network Connection" OPT

Shell > bcfg boot mv 5 2
bcfg: boot option 5 moved to 2

Shell > bcfg boot dump
The boot option list is:
01. VenMedia(5023b95c-db26-429b-a648-bd47664c8012) "UEFI: Built-in EFI Shell " OPT
02.  PciRoot(0x0)/Pci(0x19,0x0)/MAC(0000de404175,0x0)/IPv4(0.0.0.0,0x0,DHCP,0.0.0.0,0.0.0.0,0.0.0.0)
"UEFI: Intel(R) 82579LM Gigabit Network Connection" OPT
03. BBS(HD,,0x0) "Hard Drive " OPT
04.
PciRoot(0x0)/Pci(0x1,0x0)/Pci(0x0,0x0)/MAC(0000de404176,0x0)/IPv4(0.0.0.0,0x0,DHCP,0.0.0.0,0.0.0.0,0.0
.0.0) "UEFI: Intel(R) 10 Gigabit Network Connection" OPT
05.
PciRoot(0x0)/Pci(0x1,0x0)/Pci(0x0,0x1)/MAC(0000de404177,0x0)/IPv4(0.0.0.0,0x0,DHCP,0.0.0.0,0.0.0.0,0.0
.0.0) "UEFI: Intel(R) 10 Gigabit Network Connection" OPT
```

10.1.4 cd

Displays or changes the current directory.

```
CD [path]
```

path The relative or absolute directory path

1. Type CD without parameters to display the current fs and directory.
2. There must be at least one blank space between CD and path.
3. The 'path' parameter supports certain special characters:
   - '**.**' refers to the current directory.
   - '**..**' refers to the parent directory.
   - '****' used at the beginning of the path refers to the root directory of the current filesystem.
4. CD can only be used to change directories in the current file system.

- Examples:
  - To change the current filesystem to the mapped fs0 filesystem:

```
Shell> fs0:
```

  - To change the current directory to subdirectory 'efi':

```
fs0:\> cd efi
```

  - To change the current directory to the parent directory (fs0:\):

```
fs0:\efi\> cd ..
```

  - To change the current directory to 'fs0:\efi\tools':

```
fs0:\> cd efi\tools
```

  - To change the current directory to the root of the current fs (fs0):

```
fs0:\efi\tools\> cd \
fs0:\>
```

  - To change volumes with cd will not work!! For example:

```
fs0:\efi\tools\> cd fs1:\  !!!! will not work !!!!
must first type fs1: then cd to desired directory
```

  - To move between volumes and maintain the current path.

```
fs0:\> cd \efi\tools
fs0:\efi\tools\> fs1:
fs1:\> cd tmp
fs1:\tmp> cp fs0:*.* .
copies all of files in fs0:\efi\tools into fs1:\tmp directory
fs0:\>
```

10.1.5 cls

Clears the standard output and optionally changes the background color.

```
CLS [color]
```

color	New background color
0	Black
1	Blue
2	Green
3	Cyan
4	Red
5	Magenta
6	Yellow
7	Light gray

1. If no parameters are specified, this command clears the standard output device. The background color is not changed.

- **Examples:**
  - To clear standard output without changing the background color:

```
fs0:\> cls
```

  - To clear standard output and change the background color to cyan:

```
fs0:\> cls 3
```

  - To clear standard output and change the background to the default color:

```
fs0:\> cls 0
fs0:\>
```

10.1.6 connect

Reserved - Not To be Used

10.1.7 cpuutil

Reserved - Not To be Used

10.1.8 date

Displays or changes the current system date.

```
date [mm/dd/[yy]yy]
```

mm	Month of date to set, range: 1 - 12
dd	Day of date to set, range: 1 - 31
yyyy	Year of date to set, range: 1998 - 2099

1. Short year format:
   yy: 98=1998, 99=1999, 00=2000, 01=2001, ..., 97=2097.
2. Long year format:
   yyyy: 1998 - 2099, other values are invalid.
3. EFI may behave unpredictably if illegal date values are used.

10.1.9 devices

Displays the list of devices managed by EFI drivers.

```
DEVICES [-b] [-l XXX]
```

-b	Displays one screen at a time
l XXX	Displays devices using the specified ISO 639-2 language

Display Format:

CTRL	The handle number of the EFI device
TYPE	The device type:
[R]	Root Controller
[B]	Bus Controller
[D]	Device Controller
CFG	A managing driver supports the Driver Configuration Protocol
DIAG	A managing driver supports the Driver Diagnostics Protocol
#P	The number of parent controllers for this device
#D	The number of drivers managing the device
#C	The number of child controllers produced by this device
DEVICE NAME	The name of the device from the Component Name Protocol

10.1.10 dh

Displays EFI handle information.

```
DH [-l lang] [handle | -p prot_id] [-d] [-v]
```

handle	Handles number in hexadecimal format
-p	Protocol ID
-d	Displays EFI Driver Model related information
-l	Displays information in the specified ISO 639-2 language
-v	Displays verbose information

1. When neither '**handle**' nor '**prot_id**' is specified, a list of all the device handles in the EFI environment is displayed.
2. The '**-d**' option displays EFI Driver Model related information including parent handles, child handles, all drivers installed on the handle, etc.
3. The '**-v**' option displays verbose information for the specified handle including all the protocols on the handle and their details.
4. If the '**-p**' option is specified, all handles containing the specified protocol will be displayed. Otherwise, the '**handle**' parameter has to be specified for display. In this case, the '**-d**' option will be enabled automatically if the '**-v**' option is not specified.

- **Examples:**
  - To display all handles one screen at a time:

```
Shell > dh -b
```

Handle dump

```
 1: Image(CORE_DXE)
 2:
 3: DevPath (..d(0xb,0xdaf51000,0xdaff0fff))
 4: DevPath (..d(0xb,0xdad90000,0xdafaffff))
 5: DevPath (..d(0xb,0xda6a5004,0xdad60003))
 6:
 7: DpathUtil DpathToText DpathFromText Decompress
 8:
 9:
 A:
 B: UnicodeCollation2
 C: HiiFont HiiString HiiDatabase HiiConfRouting
 D:
 E:
 F: Image(CpuDxe) ImageDevPath (..e536-4e88-b3a0-b77f78eb34fe))
10: Image(Runtime) ImageDevPath (..383a-41eb-a8ee-4498aea567e4))
11:
12:
(...)
```

- To display detailed information for handle 10:

```
Shell > dh 10
```

```
Handle 10 (D8576F98)
    Image (D87D9E40)   File:Runtime
        ParentHandle..: D931BF18
        SystemTable...: DA4B5F18
        DeviceHandle..: D930E918
        FilePath.....: FvFile(cbc59c4a-383a-41eb-a8ee-4498aea567e4)
        ImageBase.....: DA4FD000 - DA50F4C0
        ImageSize.....: 124C0
        CodeType.....: RT_code
        DataType.....: RT_data
    ImageDpath (D8576E98)
        Hardware Device Path for Memory Mapped
        Memory Type (11: DA6A5004-DAD60003)
        Media Device Path for PIWG FV
        AsStr: 'MemoryMapped(0xb,0xda6a5004,0xdad60003)/FvFile(cbc59c4a-383a-41eb-a8ee-
        4498aea567e4)
```

- To display all handles associated with the 'diskio' protocol:

```
Shell > dh -p diskio
```

```
Handle dump by protocol 'DiskIo'
    194: DevPath (../Pci(0x1f,0x2)/Sata(0x0,0x0))DiskIo BlkIo
    196: DevPath (..BR,0xed32b4ef,0x800,0xfa000))DiskIo BlkIo
    197: DevPath (..xed32b4ef,0xfa800,0x9408000))DiskIo BlkIo
    195: DevPath (../Pci(0x1f,0x2)/Sata(0x4,0x0))DiskIo BlkIo
    198: DevPath (..cd-5e2eaf41eed3,0x800,0x800))DiskIo BlkIo
    199: DevPath (..b1ac8b8cd38b,0x1000,0xfa000))DiskIo BlkIo ESP
    19A: DevPath (..06bd43318,0xfb000,0x3aa7800))DiskIo BlkIo
```

- To display all handles associated with the 'Image' protocol and break when the screen is full:

```
Shell > dh -p Image -b
```

```
Handle dump by protocol 'Image'
     1: Image(CORE_DXE)
     F: Image(CpuDxe) ImageDevPath (..e536-4e88-b3a0-b77f78eb34fe))
    10: Image(Runtime) ImageDevPath (..383a-41eb-a8ee-4498aea567e4))
    19: Image(AmiBoardInfo) ImageDevPath (..ae55-4288-829d-d22fd344c347))
    1B: Image(EBC) ImageDevPath (..73d0-11d4-b06b-00aa00bd6de7))DebugSupport EbcInterp
    1D: Image(CpuPolicyDxe) ImageDevPath (..00a9-4de7-b8e8-ed7afb88f16e))
    1E: Image(CpuSmmSaveRes) ImageDevPath (..2133-1ba2-800a-b9c00accb17d))
    1F: Image(MiscSubclassDxe) ImageDevPath (..55d9-4a33-93fc-5a3eb128de21))
    20: Image(SBRun) ImageDevPath (..056e-4888-b685-cfcd67c179d4))
    22: Image(ActiveBios) ImageDevPath (..fe0f-4251-b772-4b098a1aec85))
    24: Image(PchReset) ImageDevPath (..2e30-4793-9bed-74f672bc8ffe))
    26: Image(PchSerialGpio) ImageDevPath (..3466-4c06-b1cc-1c935394b5c2))
    28: Image(SmmControl) ImageDevPath (..ab78-491b-b583-c52b7f84b9e0))
    29: Image(WdtDxe) ImageDevPath (..f027-4ca7-bfd0-16358cc9e453))
    2A: Image(iFfsDxePolicyInit) ImageDevPath (..e3f3-4e9e-90a3-2a991270219c))
    2B: Image(AsfTable) ImageDevPath (..505b-4b50-99cd-a32467fa4aa4))
    2C: Image(PlatformInfo) ImageDevPath (..cb8d-421c-b854-06231386e642))
    2D: Image(IdeSMART) ImageDevPath (..809f-45cf-a377-d77bc0cb78ee))
    2F: Image(SmbiosGetFlashData64) ImageDevPath (..7e20-4f20-91a1-190439b04d5b))
    30: Image(S3Save) ImageDevPath (..4424-46a2-9943-cc4039ead8f8))
    31: Image(CpuInitDxe) ImageDevPath (..78cd-4480-8678-c6a2a797a8de))
    37: Image(PciHostBridge) ImageDevPath (..e55e-4d6a-a3a5-5e4d72ddf772))

Press <ENTER> to continue, 'q' to exit:  ...
```

10.1.11 disconnect

Reserved - Not To Be Used

10.1.12 drivers

Displays the EFI drivers list.

```
DRIVERS [-l XXX]
```

-l	Displays drivers using the specified ISO 639-2 language

Display Format:

DRV	Handles number of the EFI driver
TYPE	Driver type: **[B]** - Bus Driver **[D]** - Device Driver
CFG	Driver supports the Driver Configuration Protocol
DIAG	Driver supports the Driver Diagnostics Protocol
#D	Number of devices managed by the driver
#C	Number of child devices produced by the driver
DRIVER NAME	Name of the driver from the Component Name Protocol
IMAGE NAME	File path from which the driver was loaded

- **Example:**
  - To display the list:

```
Shell> drivers
            T   D
D           Y C I
R           P F A
V  VERSION  E G G #D #C DRIVER NAME                          IMAGE NAME
== ======== = = = == == ================================== ==================
3F 00000010 B - -  1  2 AMI Generic LPC Super I/O Driver    CORE_DXE
9C 000C03F4 ? - -  -  - Intel(R) GOP Driver [3.0.12.1012]   IntelIvbGopDriver
9D 001B03EF ? - -  -  - Intel(R) GOP Driver [1.0.27.1007]   IntelSnbGopDriver
9E 00010000 ? - -  -  - AMI File System Driver              FileSystem
A0 00020502 B - -  1 24 <UNKNOWN>                           PciBus
B7 00000010 D - -  1  - PCH Serial ATA Controller Initializ SataController
B9 00000001 B - -  1  2 AMI AHCI BUS Driver                 AHCI
BA 03011000 B - X  2  2 Intel(R) 10GbE Driver 3.1.10 EFIx64 E3110X4
BB 05001200 B X X  1  1 Intel(R) PRO/1000 5.0.12 PCI-E      IntelGigabitLanx64
C0 00000001 ? - -  -  - IDER Controller Init Driver         IdeRController
C1 00000010 ? - -  -  - PCI Serial Driver                   PciSerial
D4 00000010 B - -  2  2 <UNKNOWN>                           Terminal
D5 00000010 B - -  1  1 <UNKNOWN>                           Terminal
D8 0000000A B - -  3  3 ARP Network Service Driver          ArpDxe
D9 0000000A D - -  3  - Simple Network Protocol Driver      SnpDxe
DA 0000000A B - -  3 12 MNP Network Service Driver          MnpDxe
DB 0000000A D - - 21  - UEFI PXE Base Code Driver           UefiPxeBcDxe
DD 0000000A D - -  3  - TCP Network Service Driver          TcpDxe
DE 0000000A B - -  3  3 DHCP Protocol Driver                Dhcp4Dxe
DF 0000000A D - -  3  - IP4 CONFIG Network Service Driver   Ip4ConfigDxe
...
```

```
...
E0 0000000A B – –  3 21 IP4 Network Service Driver          Ip4Dxe
E1 0000000A B – –  6  3 MTFTP4 Network Service              Mtftp4Dxe
E2 0000000A B – – 18 15 UDP Network Service Driver          Udp4Dxe
E3 0000000A D – –  3  – DHCP6 Protocol Driver               Dhcp6Dxe
E4 0000000A B – –  3 12 IP6 Network Service Driver          Ip6Dxe
E5 0000000A D – –  3  – MTFTP6 Network Service Driver       Mtftp6Dxe
E6 0000000A B – –  9  6 UDP6 Network Service Driver         Udp6Dxe
E7 0000008A D – –  3  – AMI USB Driver                      UHCD
E9 0000008A B – –  3  2 USB bus                             UHCD
EA 00000001 ? – –  –  – USB Hid driver                      UHCD
EB 00000001 ? – –  –  – USB Mass Storage driver             UHCD
EC 00000001 ? – –  –  – AMI USB CCID driver                 UHCD
111 00000010 ? – –  –  – <UNKNOWN>                           BIOSBLKIO
112 00000024 B – –  1  1 BIOS[INT10] Video Driver            CsmVideo
113 00000010 ? – –  –  – <UNKNOWN>                           <UNKNOWN>
118 00000010 D – –  7  – <UNKNOWN>                           CORE_DXE
119 00000010 D – –  1  – <UNKNOWN>                           CORE_DXE
11A 00000010 B – –  2  2 <UNKNOWN>                           CORE_DXE
11C 00000010 B – –  2  5 <UNKNOWN>                           CORE_DXE
11D 00000010 ? – –  –  – AMI PS/2 Driver                    CORE_DXE
11E 00000001 ? – –  –  – AMI IDE BUS Driver                 CORE_DXE
```

10.1.13 dumpacpi

Dumps ACPI1.0b, ACPI2.0, or ACPI3.0 Table in EFI Shell Environment.

Usage:

```
DumpACPI [-d] [-v] [-p] [-b]
```

-d	Dumps ACPI Table Raw Data.
-v	Dumps ACPI Table Verbose Data.
-s	Dumps ACPI Table with signature being <SIGN>. The signature should be defined value in ACPI spec. One exception is RSDP, please use RSDP instead of 'RSD PTR '.
-p	Dumps the parsed AML Code.
-b	Displays one screen at a time.

10.1.14 dumpaml

Dumps ACPI1.0b, ACPI2.0, or ACPI3.0 AML in EFI Shell Environment.

Usage:

```
DumpAML [-b] <AML file>
DumpAML <AML file> -e <AML Method Name> [<Argument>...]
```

-b	Displays one screen at a time.
-e	Executes AML method.

<AML Method Name> format: \AAAA.BBBB.CCCC.

<Argument> format: memory content in string. (eg. 34120000 means 0x1234)

10.1.15 echo

Controls batch file command echoing or displays a message.

```
ECHO [-on|-off]
ECHO [message]
```

`-on`	Enables echo when executing batch file commands
`-off`	Disables echo when executing batch file commands
`message`	Displays a message string

1. `Echo -off` disables the echo feature when executing batch file commands. This command is not like the MS-DOS echo command.
2. `Echo` without a parameter shows the current echo setting.

- **Examples:**
  - To display the current echo setting:

```
fs0:\> echo
Echo is off
```

  - To enable command echoing:

```
fs0:\> echo -on
```

  - To disable command echoing:

```
fs0:\> echo -off
```

  - To execute HelloWorld.nsh batch file and echo commands when executing:

```
fs0:\> HelloWorld.nsh
+HelloWorld.nsh> echo Hello World
Hello World
```

  - To display a message string of 'Hello World':

```
fs0:\> echo Hello World
Hello World
```

10.1.16 exit

Exits the EFI Shell environment and returns control to the parent process. This command allows to exit the EFI shell and boot the next or first boot device in the boot list.

10.1.17 for

Executes one or more commands for each item in a set of items.

```
              FOR %indexvar IN set
      command [arguments]
      [command [arguments]]       ...
              ENDFOR
              FOR %indexvar RUN (start end[ step])
      command [arguments]
      [command [arguments]]      ...
              ENDFOR
```

`%indexvar`	Variable name used to index a set
`set`	Set to be searched
`command [arguments]`	Command to be executed with optional arguments

1. The **FOR** command is only available in batch script files.
2. **FOR** shall be matched with **ENDFOR**.
3. **Start** and **end** can be any integer. Up to 6 digits allowed.
4. **Step** can be any integer but zero. Up to 6 digits allowed.
5. **step** is optional, if step is not specified, step will be automatically determined as below:
   if start <= end, then step = 1
   if start > end, then step = -1

- Examples:

```
#
#  Sample for loop type contents of all *.txt files
#
for %a in *.txt
              type %a
              echo ===== %a done =====
endfor
#

#  To repeat operations, supporting multiple loop:
#
              for %a in 1 2 3 4 5 6 7 8 9
               for %b in a b c d e f g h i j k l m n o p q r s t u v w x y z
                alias %a a%a
                alias %b %b%a
              endfor
endfor
              for %a run (1 3)
               echo %a
              endfor
Output:
1
2
3
              for %a run (3 1)
               echo %a
              endfor
Output:
3
2
1
```

10.1.18 goto

Forces batch file execution to unconditionally jump to specified location.

```
GOTO label
```

`label`	Specifies a location in batch file

1. The **GOTO** command is only available in batch script files.
2. Execution of batch file will jump to the line immediately following the specified label name.
3. **GOTO** cannot jump from outside into a FOR cycle block.

- Example:

```
            #
#  Example script for "goto" command
#
goto Done
...
:Done
cleanup.nsh
```

10.1.19 help

Displays the EFI Shell command list or verbose help for specific commands.

```
HELP [cmd | pattern]
```

`cmd`	Shell command name
`pattern`	Wildmatch pattern

1. '**cmd -?**' also displays the verbose help of cmd, the same as '**help cmd**'.
2. If the specified command has no verbose help, its line help will be displayed instead.

- Examples:
  - To display the EFI Shell command list and break after one screen:

```
Shell> help -b
```

`?`	Displays the EFI Shell command list or verbose command help
`alias`	Displays, creates, or deletes aliases in the EFI Shell
`attrib`	Displays or changes the attributes of files or directories
`cd`	Displays or changes the current directory
`cls`	Clears the standard output with an optional background color
`connect`	Connects one or more EFI drivers to a device
`copy`	Copies one or more files or directories to another location

...

- To display help information for the ls shell command:

```
Shell> help ls
Shell> ? ls
Shell> ls -?
```

- To display the list of commands starting with the character 'p'

```
            Shell> help p*
pause       Prints a message and waits for keyboard input
pci
```

10.1.20 if

Executes one or more commands in specified conditions.

```
IF [NOT] EXIST file THEN
  command [arguments]
[ELSE
  command [arguments]]
ENDIF
IF [NOT] string1 == string2 THEN
    command [arguments]
    [command [arguments]]      ...
[ELSE
    command [arguments]
    [command [arguments]]      ...]
ENDIF
```

`EXIST file`	TRUE if file exists in the directory
`string1 == string2`	TRUE if the two stings are same

1. The **IF** command is only available in batch script files.
2. If condition is TRUE, commands between **IF** and **ELSE** will be executed.
3. If condition is FALSE but keyword 'NOT' is not prefixed, commands between **ELSE** and **ENDIF** will also be executed.

- **Example:**

```
            #
            #  Example script for "if" command
#
if exist fs0:\myscript.sc then
myscript myarg1 myarg2
endif
if %myvar% == runboth then
myscript1
myscript2
endif
```

10.1.21 ifconfig

Ifconfig© Intel Corporation 2006 modifies the default IP address of UEFI network stack.

- To list the current address:

```
IfConfig -l [Name]
```

Shows the configuration for all or the interface

- To set the default address use:

```
IfConfig -s <Name> dhcp [perment]
```

Uses the EFI_DHCP4_PROTOCOL to request address dynamically

```
IfConfig -s <Name> <static> <IP> <Mask> <Gateway> [perment]
```

Uses the static IP4 address configuration

perment is optional. If present, the configuration survives the network stack reload. Otherwise, it is for this time only.

- To clear the current address:

```
IfConfig -c [Name]
```

Clears the configuration for all or the interface. Although the configuration is cleared, the network stack will fall back to the DHCP as default.

- Other:

```
IfConfig -?
```

Shows this help message.

- **Example:**

```
IfConfig -s eth0 dhcp
IfConfig -l eth0
IfConfig -s eth0 static 192.168.0.5 255.255.255.0 192.168.0.1 perment
```

The “Network stack”must be enabled in the Advanced menu to have this command available.

10.1.22 kdiag

Performs board diagnostics. Available ONLY if ordered.

10.1.23 kflash

Kontron SPI flasher

Usage:

```
kflash [-ver] [ -p|-i|-v|-s|-h|-? ]  [-f] [-r] [file]
```

- Operation mode

-ver	Displays current BIOS ID
-p	Programs flash
-i	Shows information string and check CRC
-v	Verifies flashed image
-s	Saves current ROM image to file
-c	Clones flash content to second flash (Only in RESCUE mode)
-h	Shows this help

- Options

-f	Forces write

- Expert options: Not recommended for standard use

-r	Raw image mode (.bin, .rom)
-e	Erases all flash without preserving Ethernet area
-sp	Setup preserve NVRAM settings

10.1.24 kmac

Kontron MAC Address utility

Usage:

```
kmac [-h|-r|-dump] [-w value] [-save|-load [filename]]
```

- Operation mode

-h	Shows this help
-r | --read	Shows MAC Addresses
-w | --write	value : Update MAC Addresses value format = 0x0000DEaabbcc
-dump	Dumps the first 1024 words of the 82580 EEPROM
-save filename	Saves the 82580 EEPROM contents to <filename>
-load filename	Loads the 82580 EEPROM with the contents of <filename>

- **Example:**

```
Shell> kmac -r
MAC Address of Intel 82580 LAN0 = 00:00:DE:40:43:90
MAC Address of Intel 82580 LAN1 = 00:00:DE:40:43:91
MAC Address of Intel 82580 LAN2 = 00:00:DE:40:43:92
MAC Address of Intel 82580 LAN3 = 00:00:DE:40:43:93
```

10.1.25 kpld

Kontron PLD Command

Usage:

```
kpld [-h|-?] [-b] [-v] [-m] [-r Offset] [-w Offset Value]
kpld -i2cr busNum Add Offset Type [count]
kpld -i2cw busNum Add Offset Type Data [count]
```

- Operation mode

-h|-?	Shows this help
-v	Shows CPLD revision
-m	Boot Flash information
-r	Reads CPLD register -> kpld -r Offset
-w	Writes CPLD register -> kpld -w Offset Value
-i2cr	Reads Access to I2C bus -> kpld -i2cr busNum Add Offset Type [count]
-i2cw	Writes Access to I2C bus -> kpld -i2cw busNum Add Offset Type Data [count]

10.1.26 ksata

Kontron SATA Configurator

Usage:

```
ksata [-b|-h|-?] [-p <on|off> <num_port> [-f]]
```

-b	Enables page break
-h|-?	Shows this help

- Operation mode:

-p program Early Power-Down or Write-Protect mode on SATA device

Argument List:

on	Power-Down mode
off	Write-Protect mode
num_port	SATA port number on which SATA device is plugged on (4 = onboard SSD, 3=FDM-SATA)

-f Forces selected mode on SATA device

- **Example:**

```
Shell> ksata -p off 4 -f
Port 4: 32GB NANDrive
Program Write-Protect mode (FORCED) to SATA Port 4...OK
```

CAUTION: This command is not compatible with all SATA devices and must be used with caution. On VM6052 & VM6054 boards, only the onboard SSD connected to SATA Port 4 and the SATA mezzanine equipped with a Greenliant Model connected to SATA Port 3 are compatible.

If the **-f** parameter is not added to the command, only the devices connected to SATA Port 3 or Port 4 are allowed to be programmed. By default, the Write-Protect mode is programmed on devices supporting the Early Power Down feature but for VM6052 & VM6054 onboard SSD device, write protection is only enabled by switching ON the hardware switch SW1[5]. See CA.DT.B16 document for further information.

10.1.27 ktemp

Usage:

```
ktemp [-h|-?][-p|-mf]
```

- Operation mode
  - **-h** Shows this help
  - **-p** Prints temperature, power, voltages
  - **-mf** Modifies temperature thresholds

- Examples:

```
Shell> ktemp -mf

************* TEMPERATURE THRESHOLDS CONFIGURATION ***************

Enter NCT7802Y Threshold LTD MAX between 0 and 127 C (current = 70 C)
> 80
Enter LM73 #1(90h) Threshold UPPER LIMIT between 0 and 127 C (current = 95 C)
> 100
Enter LM73 #2(92h) Threshold UPPER LIMIT between 0 and 127 C (current = 95 C)
> 100
Enter LM73 #3(94h) Threshold UPPER LIMIT between 0 and 127 C (current = 65 C)
> 85

Current configuration:

  NCT7802Y     Threshold LTD MAX     : 80
  LM73 #1(90h) Threshold UPPER LIMIT : 100
  LM73 #2(92h) Threshold UPPER LIMIT : 100
  LM73 #3(94h) Threshold UPPER LIMIT : 85
Is this correct ?
    [n] No (re-enter Thresholds)
    [y] Yes
    [q] Exit no change
> y

=======> Please RESET the board to update THRESHOLDS on devices. <=======

Shell>
```

The temperature high limit thresholds can also be modified in the Setup (see section 5.11 page 36). Refer to section 8 (11.1 Recommendations and Known Limitations page 100) for recommended temperature high limit thresholds regarding temperature classes

```
Shell> ktemp -p
 Thermal Characteristic:
   TM1(TCC) is supported AND enabled.
   TM2 is NOT enabled.
=========================================================

+-------------------------+-------------+
| CPU Temperature         |    38 C     |
+-------------------------+-------------+
| PKG Temperature         |    48 C     |
+-------------------------+-------------+
| PCH Temperature         |    51 C     |
+-------------------------+-------------+
```

```
+-------------------------+-------------+
| PKG Power               |    7844  mW |
+-------------------------+-------------+
| Core0 Power             |    4236  mW |
+-------------------------+-------------+

NCT7802Y sensors:
+-------------------------+-------------+-------------+-------------+
|                         |    Value    |  High Limit |  Low Limit  |
+-------------------------+-------------+-------------+-------------+
| 3V3_SB Voltage          |    3308  mV |    3500  mV |    3200  mV |
+-------------------------+-------------+-------------+-------------+
| VCORE Voltage           |    870   mV |      -      |      -      |
+-------------------------+-------------+-------------+-------------+
| +3V3 Voltage            |    3408  mV |    3500  mV |    3200  mV |
+-------------------------+-------------+-------------+-------------+
| +5V Voltage             |    5176  mV |    5248  mV |    4872  mV |
+-------------------------+-------------+-------------+-------------+
| DDR3 Voltage            |    1510  mV |    1580  mV |    1420  mV |
+-------------------------+-------------+-------------+-------------+
| LTD Temp                |    +24  C   |    +85  C   |    -45  C   |
+-------------------------+-------------+-------------+-------------+

LM73 sensors:
+-------------------------+-------------+-------------+-------------+
|                         |    Value    |  Temp High  |  Temp Low   |
+-------------------------+-------------+-------------+-------------+
| LM73 CPU Temp (TOP)     |    +32  C   |    +95  C   |    -45  C   |
+-------------------------+-------------+-------------+-------------+
| LM73 SBC Temp           |    +22  C   |    +85  C   |    -45  C   |
+-------------------------+-------------+-------------+-------------+
| LM73 CPU Temp (BOTTOM)  |    +34  C   |    +95  C   |    -45  C   |
+-------------------------+-------------+-------------+-------------+
```

The Thermal Sensor Thermometer Read register of the PCH returns a value in the range 0x0-0x7F, 0x0 corresponding to the hottest temperature and 0x7F corresponding to the lowest.

Temperature in °C is calculated as the following: (0.0012*value^2) ...(0.8667*value) + 134.2

Thus the temperature range is between 43 °C to 134 °C.

Temperature below 43 °C will be truncated to 43 °C.

10.1.28 kvpd

Kontron VPD Information: displays Vital Product Information

Usage:

```
kvpd [-p|-m|-gp|-gm|-h|-?]
```

- Operation mode

-p	Displays motherboard VPD information
-m	Modifies or enters motherboard VPD information (production use only)
-gp	Display MOD-GXA VPD information
-gm	Modifles or enters MOD-GXA VPD information (production use only)
-h|-?	Shows this help

- **Example:**

```
Shell> kvpd -p

================ BOARD CONFIGURATION ==============

        Order Code     : VM6052-WA28-2538000P
        EC Level       : 48015A5
        Serial Number  : 1116271110192
        Variant        : 3802A80C09200C0078
        Check Sum      : 818BF64F

================ MAC ADDRESS ==============

        LAN ETH0: 00:00:DE:51:15:08
        LAN ETH1: 00:00:DE:51:15:09
        LAN ETH2: 00:00:DE:51:15:0A
        LAN ETH3: 00:00:DE:51:15:0B


Shell> kvpd -gp

================ MOD-GXA CONFIGURATION ==============

        Order Code     : MOD-GXA-SA-00
        EC Level       : EC1001
        Serial Number  : 181513101001
        PCB Version    : PCB A
        Check Sum      : CA3B9F38
```

10.1.29 ls

Displays a list of files and subdirectories in a directory.

```
LS [-b] [-r] [-a[attrib]] [file]
```

-b	Displays one screen at a time
-r	Displays recursively (including subdirectories)
-a	Displays files with attributes of type attrib
attrib	File attribute list:
a	Archive
s	System
h	Hidden
r	Read-only
d	Directory
file	Name of file or directory (wildcards are permitted)

1. Files and directories with the system and hidden attributes are not displayed unless the '**s**' and '**h**' attributes are specified.

- **Examples:**
  - To hide files by adding the hidden and system attributes:

```
fs0:\> attrib +h +s *.efi
    ASH  fs0:\IsaBus.efi
    ASH  fs0:\IsaSerial.efi
```

  - To display all files in the current directory:

```
fs0:\> ls
   Directory of: fs0:\
     06/18/01  09:32p                  153  for.nsh
     06/18/01  01:02p <DIR>            512  efi
     06/18/01  01:02p <DIR>            512  test1
     06/18/01  01:02p <DIR>            512  test2
     06/18/01  08:04p                   29  temp.txt
     06/18/01  08:05p <DIR>            512  test
     01/28/01  08:24p       r           29  readme.txt
             3 File(s)         211 bytes
             4 Dir(s)
```

- To display all files in the current directory:

```
fs0:\> ls -a
   Directory of: fs0:\
     06/18/01  09:32p                  153  for.nsh
     06/18/01  01:02p <DIR>            512  efi
     06/18/01  01:02p <DIR>            512  test1
     06/18/01  01:02p <DIR>            512  test2
     06/18/01  10:59p               28,739  IsaBus.efi
     06/18/01  10:59p               32,838  IsaSerial.efi
     06/18/01  08:04p                   29  temp.txt
     06/18/01  08:05p <DIR>            512  test
     01/28/01  08:24p       r           29  readme.txt
             5 File(s)      61,788 bytes
             4 Dir(s)
```

- To display all read-only files in the current directory:

```
   0fs0:\> ls -ar
00    Directory of: fs0:\
      06/18/01  11:14p       r           29  readme.txt
              1 File(s)          29 bytes
              0 Dir(s)     00
```

- To display the file '**isabus.efi**' with the system attribute:

```
    fs0:\> ls -as isabus.efi
    Directory of: fs0:\
      06/18/01  10:59p               28,739  IsaBus.efi
              1 File(s)      28,739 bytes
              0 Dir(s)
```

- To display all files in the **fs0:\efi** directory recursively:

```
    fs0:\> ls -r -a efi
```

- To display all files with the '***.efi**' extension recursively one screen at a time:

```
    fs0:\> ls -b -r -a *.efi
```

10.1.30 map

Displays or defines mappings between user defined names and device handles.

```
MAP [-d <sname>]
MAP [[-r][-v][-c][-f][-t <type[,type...]>][sname]]
MAP [sname handle | mapname]
```

-d	Deletes a mapping
-r	Resets to default mappings
-v	Displays verbose mapping information
sname	User defined mapping name (wildcards are permitted)
handle	The number of handle, which is same as dumped from '**dh**' command
-c	Displays the consistent mapping name
-f	Displays the normal mapping name(not consistent mapping)
-t	Displays the device mapping name according to the device type:
	fp Floppy
	hd Hard Disk
	cd CD-ROM
	Types can be combined by putting a comma between two types.
	Spaces are not allowed between types.
mapname	Mapped name for the device followed by a postfix ':'

1. The consistent mapping is persistent across the mapping reset and the system reboot.
2. Only characters and numbers are allowed inside of sname.
3. Redirection is not allowed when running map because we do not know the file system before mapping is done.
4. Output redirection is not supported for '**map -r**' usage.

- Examples:
  - To reset the mapping table to the default mappings:

```
Shell> map -r
Device mapping table
  fs0  :Removable HardDisk - Alias hd29b0b0b blk0
        PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x1,0x0)/HD(1,MBR,0x000b9400,0x38,0x7ce10)
  blk0 :Removable HardDisk - Alias hd29b0b0b fs0
        PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x1,0x0)/HD(1,MBR,0x000b9400,0x38,0x7ce10)
  blk1 :HardDisk - Alias (null)
        PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x0,0x0)/HD(1,MBR,0xed32b4ef,0x800,0xfa000)
  blk2 :HardDisk - Alias (null)
        PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x0,0x0)/HD(2,MBR,0xed32b4ef,0xfa800,0x9408000)
  blk3 :HardDisk - Alias (null)
PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x4,0x0)/HD(1,GPT,b2d5d098-ba66-4477-9ccd-5e2eaf41eed3,0x800,0x800)
  blk4 :HardDisk - Alias (null)
        PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x4,0x0)/HD(2,GPT,439ced9e-fdd2-408c-8bd4-b1ac8b8cd38b,0x1000,0xfa000)
  blk5 :HardDisk - Alias (null)
        PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x4,0x0)/HD(3,GPT,4e5b73d4-90b5-46ce-909a-3bf06bd43318,0xfb000,0x3aa7800)
```

```
  blk6 :BlockDevice - Alias (null)
        PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x0,0x0)
  blk7 :BlockDevice - Alias (null)
        PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x4,0x0)
  blk8 :Removable BlockDevice - Alias (null)
        PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x1,0x0)
  hd29b0b0b :Removable HardDisk - Alias fs0 blk0
             PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x1,0x0)/HD(1,MBR,0x000b9400,0x38,0x7ce10)
```

- To display all mappings in the device mapping table:

```
Shell> map
Device mapping table
  fs0  :Removable HardDisk - Alias hd29b0b0b blk0
         PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x1,0x0)/HD(1,MBR,0x000b9400,0x38,0x7ce10)
  blk0 :Removable HardDisk - Alias hd29b0b0b fs0
         PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x1,0x0)/HD(1,MBR,0x000b9400,0x38,0x7ce10)
  blk1 :HardDisk - Alias (null)
        PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x0,0x0)/HD(1,MBR,0xed32b4ef,0x800,0xfa000)
  blk2 :HardDisk - Alias (null)
        PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x0,0x0)/HD(2,MBR,0xed32b4ef,0xfa800,0x9408000)
  blk3 :HardDisk - Alias (null)
         PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x4,0x0)/HD(1,GPT,b2d5d098-ba66-4477-9ccd-5e2eaf41eed3,0x800,0x800)
  blk4 :HardDisk - Alias (null)
         PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x4,0x0)/HD(2,GPT,439ced9e-fdd2-408c-8bd4-b1ac8b8cd38b,0x1000,0xfa000)
  blk5 :HardDisk - Alias (null)
         PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x4,0x0)/HD(3,GPT,4e5b73d4-90b5-46ce-909a-3bf06bd43318,0xfb000,0x3aa7800)
  blk6 :BlockDevice - Alias (null)
        PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x0,0x0)
  blk7 :BlockDevice - Alias (null)
        PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x4,0x0)
  blk8 :Removable BlockDevice - Alias (null)
        PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x1,0x0)
  hd29b0b0b :Removable HardDisk - Alias fs0 blk0
             PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x1,0x0)/HD(1,MBR,0x000b9400,0x38,0x7ce10)
```

- To display verbose mapping table information:

```
Shell> map -v
Device mapping table
  fs0   Consistent Name hd29b0b0b
        Other Name   blk0
        Handle       1A2: Fs DiskIo BlkIo
        Media Type   HardDisk
        Removable   YES
        Current Dir  \
         PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x1,0x0)/HD(1,MBR,0x000b9400,0x38,0x7ce10)
  blk0  Consistent Name hd29b0b0b
        Other Name   fs0
        Handle       1A2: Fs DiskIo BlkIo
        Media Type   HardDisk
        Removable   YES
        Current Dir  \
         PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x1,0x0)/HD(1,MBR,0x000b9400,0x38,0x7ce10)
```

```
  blk1  Consistent Name (null)
        Other Name   (null)
        Handle       196: DiskIo BlkIo
        Media Type   HardDisk
        Removable    NO
        Current Dir  \
         PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x0,0x0)/HD(1,MBR,0xed32b4ef,0x800,0xfa000)
  blk2  Consistent Name (null)
        Other Name   (null)
        Handle       197: DiskIo BlkIo
        Media Type   HardDisk
        Removable    NO
        Current Dir  \
         PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x0,0x0)/HD(2,MBR,0xed32b4ef,0xfa800,0x9408000)
(...)
```

- To assign fs0 another name:

```
Shell > map floppy fs0:
Device mapping table
  floppy :Removable HardDisk - Alias hd29b0b0b fs0 blk0
           PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x1,0x0)/HD(1,MBR,0x000b9400,0x38,0x7ce10)
```

- To display information about the mapped name:

```
Shell > map floppy
Device mapping table
  floppy :Removable HardDisk - Alias hd29b0b0b fs0 blk0
           PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x1,0x0)/HD(1,MBR,0x000b9400,0x38,0x7ce10)
```

- To operate with the mapped name:

```
Shell > floppy:
floppy:\> ls
Directory of: floppy:\
(...)
```

- To delete a mapped name:

```
floppy:\> map -d floppy
Shell > map
Device mapping table
  fs0  :Removable HardDisk - Alias hd29b0b0b blk0
         PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x1,0x0)/HD(1,MBR,0x000b9400,0x38,0x7ce10)
  blk0 :Removable HardDisk - Alias hd29b0b0b fs0
         PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x1,0x0)/HD(1,MBR,0x000b9400,0x38,0x7ce10)
  blk1 :HardDisk - Alias (null)
         PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x0,0x0)/HD(1,MBR,0xed32b4ef,0x800,0xfa000)
  blk2 :HardDisk - Alias (null)
         PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x0,0x0)/HD(2,MBR,0xed32b4ef,0xfa800,0x9408000)
```

```
  blk3 :HardDisk - Alias (null)
         PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x4,0x0)/HD(1,GPT,b2d5d098-ba66-4477-9ccd-5e2eaf41eed3,0x800,0x800)
  blk4 :HardDisk - Alias (null)
         PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x4,0x0)/HD(2,GPT,439ced9e-fdd2-408c-8bd4-b1ac8b8cd38b,0x1000,0xfa000)
  blk5 :HardDisk - Alias (null)
         PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x4,0x0)/HD(3,GPT,4e5b73d4-90b5-46ce-909a-3bf06bd43318,0xfb000,0x3aa7800)
  blk6 :BlockDevice - Alias (null)
        PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x0,0x0)
  blk7 :BlockDevice - Alias (null)
        PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x4,0x0)
  blk8 :Removable BlockDevice - Alias (null)
        PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x1,0x0)
  hd29b0b0b :Removable HardDisk - Alias fs0 blk0
              PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x1,0x0)/HD(1,MBR,0x000b9400,0x38,0x7ce10)
```

- To display all the mapped names starting with **'b'**:

```
Shell> map b*
Device mapping table
  blk0   :Removable HardDisk - Alias hd29b0b0b fs0 floppy
           PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x1,0x0)/HD(1,MBR,0x000b9400,0x38,0x7ce10)
  blk1   :HardDisk - Alias (null)
           PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x0,0x0)/HD(1,MBR,0xed32b4ef,0x800,0xfa000)
  blk2   :HardDisk - Alias (null)
           PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x0,0x0)/HD(2,MBR,0xed32b4ef,0xfa800,0x9408000)
  blk3   :HardDisk - Alias (null)
           PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x4,0x0)/HD(1,GPT,b2d5d098-ba66-4477-9ccd-5e2eaf41eed3,0x800,0x800)
  blk4   :HardDisk - Alias (null)
           PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x4,0x0)/HD(2,GPT,439ced9e-fdd2-408c-8bd4-b1ac8b8cd38b,0x1000,0xfa000)
  blk5   :HardDisk - Alias (null)
           PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x4,0x0)/HD(3,GPT,4e5b73d4-90b5-46ce-909a-3bf06bd43318,0xfb000,0x3aa7800)
  blk6   :BlockDevice - Alias (null)
          PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x0,0x0)
  blk7   :BlockDevice - Alias (null)
          PciRoot(0x0)/Pci(0x1f,0x2)/Sata(0x4,0x0)
  blk8   :Removable BlockDevice - Alias (null)
          PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x1,0x0)
```

10.1.31 mem

Displays the contents of system or device memory.

```
MEM [-b] [Address] [Size] [-MMIO]
```

-b	Displays one screen at a time
address	Starting address in hexadecimal format
size	Number of bytes to display in hexadecimal format
-MMIO	Forces address cycles to the PCI bus

1. All units are in hexadecimal format.
2. Address must be aligned on an even processor address boundary.
3. If the 'address' parameter is not specified, DMEM will display the all system table pointer entries by default.

- Examples:
  - To display the EFI system table pointer entries:

```
Shell> mem
 Memory Address 000000007ADB7F18 200 Bytes
 7ADB7F18: 49 42 49 20 53 59 53 54-00 00 02 00 78 00 00 00  *IBI SYST....x...*
 7ADB7F28: 51 E1 C4 FF 00 00 00 00-00 B6 59 7A 00 00 00 00  *Q.........Yz....*
 7ADB7F38: 7B 02 04 00 00 00 00 00-18 EE AF 01 00 00 00 00  *.................*
 7ADB7F48: F0 9A 1A 12 00 00 00 00-18 EE AF 01 00 00 00 00  *.................*
 7ADB7F58: C0 9B 1A 12 00 00 00 00-18 EE AF 01 00 00 00 00  *.................*
 7ADB7F68: A0 EB 59 7A 00 00 00 00-18 7E DB 7A 00 00 00 00  *..Yz.......z....*
 7ADB7F78: 40 D2 59 7A 00 00 00 00-06 00 00 00 00 00 00 00  *@.Yz............*
 7ADB7F88: 18 5E DB 7A 00 00 00 00-70 74 61 6C 98 00 00 00  *.^.z....ptal....*
 7ADB7F98: 7A 85 16 BB 02 1A 70 DB-64 75 FC 1F 63 C5 DE 0B  *z.....p.du..c...*
 7ADB7FA8: 6B C6 2B 63 56 7E 6B 5A-69 46 2C 40 DD 98 F3 E0  *k.+cV.kZiF,@....*
 7ADB7FB8: F4 41 B6 4E C3 BA 08 D1-36 6D 03 05 CF E8 1D 0C  *.A.N....6m......*
 7ADB7FC8: D7 37 16 91 DD 4B 10 45-4C FF 38 3D 01 B8 87 2A  *.7...K.EL.8=...**
 7ADB7FD8: E6 21 D6 6B 02 89 8A BD-FE ED 76 FA 3C A6 67 3D  *.!.k......v.<.g=*
 7ADB7FE8: 97 B7 7C 7F 6B B1 4C 9E-ED 50 D2 FC 75 9B 34 3E  *....k.L..P..u.4>*
 7ADB7FF8: 96 5E 4F 60 BE AD 1A 81-00 00 00 00 00 00 00 00  *.^O`............*
 7ADB8008: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
 7ADB8018: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
 7ADB8028: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
 7ADB8038: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
 7ADB8048: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
 7ADB8058: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
 7ADB8068: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
 7ADB8078: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
 7ADB8088: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
 7ADB8098: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
 7ADB80A8: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
 7ADB80B8: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
 7ADB80C8: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
```

```
7ADB80D8: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
7ADB80E8: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
7ADB80F8: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
7ADB8108: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*

Valid EFI Header at Address 000000007ADB7F18
------------------------------------------
System: Table Structure size 00000078 revision 00020000
ConIn (01AFEE18) ConOut (01AFEE18) StdErr (01AFEE18)
Runtime Services     000000007ADB7E18
Boot Services        000000007A59D240
ACPI 2.0 Table       000000007AFFFF98
SMBIOS Table         00000000000F0480
```

- To display memory contents from **7adbf18** with size of 16 bytes:

```
Shell> mem 7ADB7F18 16
Memory Address 000000007ADB7F18 10 Bytes
7ADB7F18: 49 42 49 20 53 59 53 54-00 00 02 00 78 00 00 00  *IBI SYST....x...*
```

- To display memory mapped IO contents from **7adbf18** with size of 16 bytes:

```
Shell> mem 7ADB7F18 16 -MMIO
 Memory Address 000000007ADB7F18 10 Bytes
7ADB7F18: 49 42 49 20 53 59 53 54-00 00 02 00 78 00 00 00  *IBI SYST....x...*
```

10.1.32 memmap

Displays the memory map maintained by the EFI environment.

```
MEMMAP [-b]
```

-b Displays one screen at a time

1. The EFI environment keeps track of all the physical memory in the system and how it is currently being used.
2. Total memory is the physical memory size, **MemMapIO** and **MemPortIO** not included.
3. Refer to the EFI specification for memory type definitions.

- Example:
  - To display the system memory map:

```
Shell> memmap

Type       Start            End              # Pages          Attributes
BS_code    0000000000000000-0000000000007FFF  0000000000000008 000000000000000F
available  0000000000008000-000000000005DFFF  0000000000000056 000000000000000F
BS_data    000000000005E000-000000000005FFFF  0000000000000002 000000000000000F
BS_code    0000000000060000-000000000009EFFF  000000000000003F 000000000000000F
RT_data    000000000009F000-000000000009FFFF  0000000000000001 800000000000000F
available  0000000000100000-0000000001436FFF  0000000000001337 000000000000000F
LoaderData 0000000001437000-000000000144CFFF  0000000000000016 000000000000000F
LoaderCode 000000000144D000-0000000001552FFF  0000000000000106 000000000000000F
available  0000000001553000-0000000001FFFFFF  0000000000000AAD 000000000000000F
LoaderData 0000000002000000-00000000020FFFFF  0000000000000100 000000000000000F
available  0000000002100000-000000001FFFFFFF  000000000001DF00 000000000000000F
reserved   0000000020000000-00000000201FFFFF  0000000000000200 000000000000000F
available  0000000020200000-0000000040003FFF  000000000001FE04 000000000000000F
reserved   0000000040004000-0000000040004FFF  0000000000000001 000000000000000F
available  0000000040005000-00000000BC691FFF  000000000007C68D 000000000000000F
BS_data    00000000BC692000-00000000BC89DFFF  000000000000020C 000000000000000F
available  00000000BC89E000-00000000BC90AFFF  000000000000006D 000000000000000F
BS_data    00000000BC90B000-00000000BC932FFF  0000000000000028 000000000000000F
available  00000000BC933000-00000000BC935FFF  0000000000000003 000000000000000F
BS_data    00000000BC936000-00000000C82DFFFF  000000000000B9AA 000000000000000F
available  00000000C82E0000-00000000C8B01FFF  0000000000000822 000000000000000F
BS_code    00000000C8B02000-00000000C8D8CFFF  000000000000028B 000000000000000F
ACPI_NVS   00000000C8D8D000-00000000C8DCFFFF  0000000000000043 000000000000000F
BS_data    00000000C8DD0000-00000000C8F1FFFF  0000000000000150 000000000000000F
BS_code    00000000C8F20000-00000000C9570FFF  0000000000000651 000000000000000F
BS_data    00000000C9571000-00000000C958CFFF  000000000000001C 000000000000000F
BS_code    00000000C958D000-00000000C95A6FFF  000000000000001A 000000000000000F
BS_data    00000000C95A7000-00000000C95ADFFF  0000000000000007 000000000000000F
RT_data    00000000C95AE000-00000000C97F8FFF  000000000000024B 800000000000000F
BS_data    00000000C97F9000-00000000C9806FFF  000000000000000E 000000000000000F
available  00000000C9807000-00000000CA416FFF  0000000000000C10 000000000000000F
reserved   00000000CA417000-00000000CA427FFF  0000000000000011 000000000000000F
reserved   00000000CA428000-00000000CA429FFF  0000000000000002 000000000000000F
reserved   00000000CA42A000-00000000CA438FFF  000000000000000F 000000000000000F
reserved   00000000CA439000-00000000CA43DFFF  0000000000000005 000000000000000F
reserved   00000000CA43E000-00000000CA492FFF  0000000000000055 000000000000000F
```

```
ACPI_NVS   00000000CA493000-00000000CA855FFF  00000000000003C3 000000000000000F
ACPI_NVS   00000000CA856000-00000000CABF8FFF  00000000000003A3 000000000000000F
RT_data    00000000CABF9000-00000000CAE9EFFF  00000000000002A6 800000000000000F
RT_data    00000000CAE9F000-00000000CAECEFFF  0000000000000030 800000000000000F
RT_data    00000000CAECF000-00000000CAED0FFF  0000000000000002 800000000000000F
RT_data    00000000CAED1000-00000000CAF6CFFF  000000000000009C 800000000000000F
RT_code    00000000CAF6D000-00000000CAF8DFFF  0000000000000021 800000000000000F
RT_code    00000000CAF8E000-00000000CAFF0FFF  0000000000000063 800000000000000F
available  00000000CAFF1000-00000000CAFF1FFF  0000000000000001 000000000000000F
BS_data    00000000CAFF2000-00000000CAFFCFFF  000000000000000B 000000000000000F
RT_data    00000000CAFFD000-00000000CAFFEFFF  0000000000000002 800000000000000F
BS_data    00000000CAFFF000-00000000CAFFFFFF  0000000000000001 000000000000000F
available  0000000100000000-00000002305FFFFF  0000000000130600 000000000000000F
reserved   00000000CB000000-00000000CF9FFFFF  0000000000004A00 0000000000000000
MemMapIO   00000000F8000000-00000000FBFFFFFF  0000000000004000 8000000000000001
MemMapIO   00000000FEC00000-00000000FEC00FFF  0000000000000001 8000000000000001
MemMapIO   00000000FED00000-00000000FED03FFF  0000000000000004 8000000000000001
MemMapIO   00000000FED1C000-00000000FED1FFFF  0000000000000004 8000000000000001
MemMapIO   00000000FEE00000-00000000FEE00FFF  0000000000000001 8000000000000001
MemMapIO   00000000FF000000-00000000FFFFFFFF  0000000000001000 8000000000000001

  reserved  :  19,581 Pages (80,203,776)
  LoaderCode:     262 Pages (1,073,152)
  LoaderData:     278 Pages (1,138,688)
  BS_code   :   2,365 Pages (9,687,040)
  BS_data   :  48,493 Pages (198,627,328)
  RT_code   :     132 Pages (540,672)
  RT_data   :   1,474 Pages (6,037,504)
  available : 2,022,510 Pages (8,284,200,960)
  ACPI_NVS  :   1,961 Pages (8,032,256)
  MemMapIO  :  20,490 Pages (83,927,040)
Total Memory: 8,115 MB (8,509,337,600) Bytes
```

10.1.33 mm

Displays or modifies **MEM/MMIO/IO/PCI/PCIE** address space.

```
MM Address [Value] [-w 1|2|4|8] [-MEM | -MMIO | -IO | -PCI | -PCIE] [-n]
```

Address	Starting address
Value	The value to write
-MEM	Memory Address type
-MMIO	Memory Mapped IO Address type
-IO	IO Address type
-PCI	PCI Configuration Space Address type: Address format: **0x000000ssbbddffrr** **ss** Segment **bb** Bus **dd** Device **ff** Function **rr** Register
-PCIE	PCIE Configuration Space Address type: Address format: **0x00000ssbbddffrrr** **ss** Segment **bb** Bus **dd** Device **ff** Function **rrr** Register
-w	Unit size accessed in bytes: **1** 1 byte **2** 2 bytes **4** 4 bytes **8** 8 bytes
-n	Non-interactive mode

1. If the address type parameter is not specified, address type defaults to the '**MEM**' type.
2. If the '**Value**' parameter is specified, the '**-n**' option will be used automatically. In this case, this command will write the value to the specified address in non-interactive mode. If the '**Value**' parameter is not specified, only the current contents in the address are displayed.
3. If the '**-w**' option is not specified, unit size defaults to 1 byte.
4. If the PCI address type is specified, the '**Address**' parameter should follow the PCI Configuration Space Address format above. The '**PCI**' command can be used to determine the address for a specified device. It is listed in the PCI configuration space dump information, in the following format: "**[EFI 0x000000ssbbddffxx]**".
5. If the PCIE address type is specified, the '**Address**' parameter should follow the PCIE Configuration Space Address format above.
6. In interactive mode, type a hex value to modify, '**q**' or '**.**' to exit. If the '**-n**' option is specified, it will run in non-interactive mode which supports batch file operation without user intervention.
7. Not all PCI configuration register locations are writable.
8. MM will only write the specified value. Read-modify-write operations are not supported.
9. The '**Address**' parameter should be aligned on a boundary of the specified width.
10. Not all addresses are safe to access. Access to any improper address can bring unexpected results.

- Examples:
  - To display or modify memory:

```
Address 0x1b07288, default width=1 byte:
    fs0:\> mm 1b07288
    MEM  0x0000000001B07288 : 0x6D >
    MEM  0x0000000001B07289 : 0x6D >
    MEM  0x0000000001B0728A : 0x61 > 80
    MEM  0x0000000001B0728B : 0x70 > q
    fs0:\> mm 1b07288
    MEM  0x0000000001B07288 : 0x6D >
    MEM  0x0000000001B07289 : 0x6D >
    MEM  0x0000000001B0728A : 0x80 >        *Modified
    MEM  0x0000000001B0728B : 0x70 > q
```

  - To modify memory:

```
    Address 0x1b07288, width = 2 bytes:
    Shell> mm 1b07288 -w 2
    MEM  0x0000000001B07288 : 0x6D6D >
    MEM  0x0000000001B0728A : 0x7061 > 55aa
    MEM  0x0000000001B0728C : 0x358C > q
    Shell> mm 1b07288 -w 2
    MEM  0x0000000001B07288 : 0x6D6D >
    MEM  0x0000000001B0728A : 0x55AA >      *Modified
    MEM  0x0000000001B0728C : 0x358C > q
```

  - To display IO space:

```
    Address 80h, width = 4 bytes:
    Shell> mm 80 -w 4 -IO
    IO  0x0000000000000080 : 0x000000FE >
    IO  0x0000000000000084 : 0x00FF5E6D > q
```

  - To modify IO space using non-interactive mode:

```
    Shell> mm 80 52 -w 1 -IO
    Shell> mm 80 -w 1 -IO
    IO  0x0000000000000080 : 0x52 > FE    *Modified
    IO  0x0000000000000081 : 0xFF >
    IO  0x0000000000000082 : 0x00 >
    IO  0x0000000000000083 : 0x00 >
    IO  0x0000000000000084 : 0x6D >
    IO  0x0000000000000085 : 0x5E >
    IO  0x0000000000000086 : 0xFF >
    IO  0x0000000000000087 : 0x00 > q
```

- To display PCI configuration space, ss=00, bb=00, dd=00, ff=00, rr=00:

```
Shell> mm 0000000000 -PCI
PCI  0x0000000000000000 : 0x86 >
PCI  0x0000000000000001 : 0x80 >
PCI  0x0000000000000002 : 0x30 >
PCI  0x0000000000000003 : 0x11 >
PCI  0x0000000000000004 : 0x06 >
PCI  0x0000000000000005 : 0x00 > q
```

These contents can also be displayed by 'PCI 00 00 00'.

- To display PCIE configuration space, ss=00, bb=06, dd=00, ff=00, rrr=000:

```
Shell> mm 00060000000 -PCIE
PCIE  0x0000000060000000 : 0xAB >
PCIE  0x0000000060000001 : 0x11 >
PCIE  0x0000000060000002 : 0x61 >
PCIE  0x0000000060000003 : 0x43 >
PCIE  0x0000000060000004 : 0x00 > q
```

10.1.34 pause

Prints a message and waits for keyboard input.

```
PAUSE [-q]
```

-q Does not display notification message

1. The PAUSE command is only available in batch script files.
2. The prompt message is "**Enter ´q´ to quit, any other key to continue**".

- **Examples:**
  - To pause the system after displaying the date and time:

```
fs0:\> type pause.nsh
File: fs0:\pause.nsh, Size 204
#
#  Example script for ´pause´ command
#
echo pause.nsh begin..
date
time
pause
echo pause.nsh done.
```

  - To execute the script with **echo on**:

```
+pause.nsh> echo pause.nsh begin..
pause.nsh begin..
+pause.nsh> date
06/19/2001
+pause.nsh> time
00:51:45
+pause.nsh> pause
Enter ´q´ to quit, any other key to continue:
+pause.nsh> echo pause.nsh done.
pause.nsh done.
fs0:\> pause.nsh
```

- To execute the script with **echo off**:

```
fs0:\> echo -off
fs0:\> pause.nsh
pause.nsh begin..
06/19/2001
00:52:50
Enter ´q´ to quit, any other key to continue: q
fs0:\>
```

10.1.35 pci

Displays PCI device list or PCI function configuration space.

```
PCI [Bus Dev [Func] [-s Seg] [-i]]
```

Bus	Bus number
Dev	Device number
Func	Function number
-s	Optional segment number specified
Seg	Segment number
-i	Information interpreted

1. If no parameters are specified all PCI devices will be listed.
2. If the Bus and Device number parameters are specified while the Function or Segment parameters are not, Function or Segment will be set as default value 0.
3. The '**-i**' option can be used to display verbose information for the specified PCI device. The PCI configuration space for the specified device will be dumped with a detailed interpretation.

- Examples on VM6052/VM6054:
  - To display all PCI devices in the system:

```
Shell> pci
   Seg  Bus  Dev  Func
   ---  ---  ---  ----
    00   00   00    00 ==> Bridge Device - Host/PCI bridge
              Vendor 8086 Device 0154 Prog Interface 0
    00   00   01    00 ==> Bridge Device - PCI/PCI bridge
              Vendor 8086 Device 0151 Prog Interface 0
    00   00   01    02 ==> Bridge Device - PCI/PCI bridge
              Vendor 8086 Device 0159 Prog Interface 0
    00   00   02    00 ==> Display Controller - VGA/8514 controller
              Vendor 8086 Device 0166 Prog Interface 0
    00   00   1A    00 ==> Serial Bus Controllers - USB
              Vendor 8086 Device 1E2D Prog Interface 20
    00   00   1C    00 ==> Bridge Device - PCI/PCI bridge
              Vendor 8086 Device 1E10 Prog Interface 0
    00   00   1C    06 ==> Bridge Device - PCI/PCI bridge
              Vendor 8086 Device 1E1C Prog Interface 0
    00   00   1D    00 ==> Serial Bus Controllers - USB
              Vendor 8086 Device 1E26 Prog Interface 20
    00   00   1F    00 ==> Bridge Device - PCI/ISA bridge
              Vendor 8086 Device 1E55 Prog Interface 0
    00   00   1F    02 ==> Mass Storage Controller - UNDEFINED
              Vendor 8086 Device 1E03 Prog Interface 1
    00   00   1F    03 ==> Serial Bus Controllers - System Management Bus
              Vendor 8086 Device 1E22 Prog Interface 0
```

```
    00   00   1F    06 ==> Data Acquisition & Signal Processing Controllers - Ot
              Vendor 8086 Device 1E24 Prog Interface 0
    00   02   00    00 ==> Network Controller - Ethernet controller
              Vendor 8086 Device 150E Prog Interface 0
    00   02   00    01 ==> Network Controller - Ethernet controller
              Vendor 8086 Device 150E Prog Interface 0
    00   02   00    02 ==> Network Controller - Ethernet controller
              Vendor 8086 Device 150E Prog Interface 0
    00   02   00    03 ==> Network Controller - Ethernet controller
              Vendor 8086 Device 150E Prog Interface 0
    00   04   00    00 ==> Bridge Device - PCI/PCI bridge
              Vendor 10B5 Device 8112 Prog Interface 0
    00   05   09    00 ==> Bridge Device - Other bridge type
              Vendor 1059 Device 9035 Prog Interface 0
```

- To display the configuration space of the PCIe-PCI Bridge PEX8112 (Bus 4, Device 0, Function 0):

```
VM6054> pci 4 0 0 -i
  PCI Segment 00 Bus 04 Device 00 Func 00 [EFI 80000000000000004CAFC000000000000]
  00000000: B5 10 12 81 07 00 10 00-AA 00 04 06 20 00 01 00  *............ ...*
  00000010: 0C 00 00 E0 00 00 00 00-04 05 05 20 F0 00 20 22  *........... .. "*
  00000020: 00 E8 00 F0 F0 FF 00 00-00 00 00 00 00 00 00 00  *................*
  00000030: 00 00 00 00 40 00 00 00-00 00 00 00 12 01 10 00  *....@...........*

  00000040: 01 50 02 5A 00 00 00 00-12 28 0E 00 00 00 00 00  *.P.Z.....(......*
  00000050: 05 60 80 00 00 00 00 00-00 00 00 00 00 00 00 00  *.`..............*
  00000060: 10 00 71 00 00 00 90 05-00 40 0B 00 11 4C 02 00  *..q......@...L..*
  00000070: 03 00 11 00 80 0C 00 00-00 00 40 00 00 00 00 00  *..........@.....*
  00000080: 00 00 00 00 00 00 00 00-33 00 00 00 00 00 00 00  *........3.......*
  00000090: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000A0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000B0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000C0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000D0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000E0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  000000F0: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*

Vendor ID(0): 10B5                    Device ID(2): 8112

Command(4): 0007
  (00)I/O space access enabled:       1  (01)Memory space access enabled:    1
  (02)Behave as bus master:           1  (03)Monitor special cycle enabled:  0
  (04)Mem Write & Invalidate enabled: 0  (05)Palette snooping is enabled:    0
  (06)Assert PERR# when parity error: 0  (07)Do address/data stepping:       0
  (08)SERR# driver enabled:           0  (09)Fast back-to-back transact...:  0

Status(6): 0010
  (04)New Capabilities linked list:   1  (05)66MHz Capable:                  0
  (07)Fast Back-to-Back Capable:      0  (08)Master Data Parity Error:       0
  (09)DEVSEL timing:               Fast  (11)Signaled Target Abort:          0
  (12)Received Target Abort:          0  (13)Received Master Abort:          0
  (14)Signaled System Error:          0  (15)Detected Parity Error:          0
```

```
Revision ID(8):     AA                BIST(0F):  Incapable
Cache Line Size(C): 20                Latency Timer(D): 00
Header Type(0E):    01, Single function, P2P bridge
Class: Bridge Device - PCI/PCI bridge -
Base Address Registers(10):     Start_Address  Type  Space    Prefetchable?     Size
      Limit
  ------------------------------------------------------------------------------
  00000000E0000000  Mem   64 bits  YES    0000000000010000  00000000E000FFFF
  ------------------------------------------------------------------------------
No Expansion ROM(38)

(Bus Numbers)  Primary(18)     Secondary(19)   Subordinate(1A)
               ---------------------------------------------------
               04               05               05
Secondary Latency Timer(1B):       20

Secondary Status(1E): 2220
  (04)New Capabilities linked list:   0  (05)66MHz Capable:                  1
  (07)Fast Back-to-Back Capable:      0  (08)Master Data Parity Error:       0
  (09)DEVSEL timing:             Medium  (11)Signaled Target Abort:          0
  (12)Received Target Abort:          0  (13)Received Master Abort:          1
  (14)Received System Error:          0  (15)Detected Parity Error:          0

Resource Type                             Base                    Limit
-------------------------------------------------------------------------
I/O(1C)                              0000F000                00000FFF
Memory(20)                           E8000000                F00FFFFF
Prefetchable Memory(24)    00000000FFF00000         00000000000FFFFF

Capabilities Ptr(34):   40

Bridge Control(3E)     0010
  (00)Parity Error Response:          0  (01)SERR# Enable:                   0
  (02)ISA Enable:                     0  (03)VGA Enable:                    0
  (05)Master Abort Mode:              0  (06)Secondary Bus Reset:           0
  (07)Fast Back-to-Back Enable:       0  (08)Primary Discard Timer:       2^15
  (09)Secondary Discard Timer:     2^15  (10)Discard Timer Status:          0
  (11)Discard Timer SERR# Enable:     0

Interrupt Line(3C)      12             Interrupt Pin(3D):       01

Pci Express device capability structure:
CapID( 0):          10            NextCap Ptr( 1):    00
Cap Register( 2):             0071
  Capability Version(3:0):          0x0001
  Device/PortType(7:4):             PCI Express to PCI/PCI-X Bridge
  Interrupt Message Number(13:9):   0x00000
Device Capabilities( 4):      05900000
  Max_Payload_Size Supported(2:0):          128 bytes
  Phantom Functions Supported(4:3):         0
  Extended Tag Field Supported(5):          5-bit Tag field supported
  Role-based Error Reporting(15):           0
Device Control( 8):           4000
  Correctable Error Reporting Enable(0):    0
  Non-Fatal Error Reporting Enable(1):      0
  Fatal Error Reporting Enable(2):          0
  Unsupported Request Reporting Enable(3):  0
  Enable Relaxed Ordering(4):               0
```

```
  Max_Payload_Size(7:5):                    128 bytes
  Extended Tag Field Enable(8):             0
  Phantom Functions Enable(9):              0
  Auxiliary (AUX) Power PM Enable(10):      0
  Enable No Snoop(11):                      0
  Max_Read_Request_Size(14:12):             2048 bytes
  Bridge Configuration Retry Enable(15):  0
Device Status( A):            000B
  Correctable Error Detected(0):            1
  Non-Fatal Error Detected(1):              1
  Fatal Error Detected(2):                  0
  Unsupported Request Detected(3):          1
  AUX Power Detected(4):                    0
  Transactions Pending(5):                  0
Link Capabilities( C):        00024C11
  Supported Link Speeds(3:0):                           2.5 GT/s supported
  Maximum Link Width(9:4):                              x1
  Active State Power Management Support(11:10):         L0s and L1 Supported
  L0s Exit Latency(14:12):                              512ns to less than 1us
  L1 Exit Latency(17:15):                               8us to less than 16us
  Clock Power Management(18):                           0
  Surprise Down Error Reporting Capable(19):            0
  Data Link Layer Link Active Reporting Capable(20):  0
  Link Bandwidth Notification Capability(21):           0
  Port Number(31:24):                                   0x00
Link Control(10):             0003
  Active State Power Management Control(1:0):           L0s and L1 Entry Enabled
  Read Completion Boundary (RCB)(3):                    64 byte
  Common Clock Configuration(6):                        0
  Extended Synch(7):                                    0
  Enable Clock Power Management(8):                     0
  Hardware Autonomous Width Disable(9):                 0
  Link Bandwidth Management Interrupt Enable(10):       0
  Link Autonomous Bandwidth Interrupt Enable(11):       0
Link Status(12):              0011
  Current Link Speed(3:0):                              2.5 GT/s
  Negotiated Link Width(9:4):                           x1
  Link Training(11):                                    0
  Slot Clock Configuration(12):                         0
  Data Link Layer Link Active(13):                      0
  Link Bandwidth Management Status(14):                 0
  Link Autonomous Bandwidth Status(15):                 0
Slot Capabilities(14):        00000C80
Slot Control(18):             0000
Slot Status(1A):              0040
Root Control(1C):             0000
Root Capabilities(1E):        0000
Root Status(20):              00000000

Start dumping PCIex extended configuration space (0x100 - 0xFFF).

  00000100: 04 00 01 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000110: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000120: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000130: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000140: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000150: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
```

10.1.36 reconnect

Reserved - Not To Be Used

10.1.37 reset

Resets the system.

```
RESET [-w [string]]
RESET [-s [string]]
```

`-w`	Performs a warm reset
`-s`	Performs a shutdown
`string`	String to be passed to reset service

1. Reset will be guaranteed to reset the chipset as well as the processor when cold reset is called.
2. This command does not support output redirection.

10.1.38 set

Displays, creates, changes, or deletes EFI Shell environment variables.

```
SET [-v] [sname [value]]
SET [-d <sname>]
```

`-d`	Deletes the environment variable
`-v`	Volatile variable
`sname`	Environment variable name
`value`	Environment variable value

1. SET values are stored in EFI NVRAM and will be retained between boots unless the option `-v` is specified.

- Examples:
  - To add an environment variable:

```
Shell> set DiagnosticPath fs0:\efi\diag;fs1:\efi\diag
```

  - To display all environment variables:

```
Shell> set
                * path           : .
                diagnosticPath : fs0:\efi1.1\diag;fs1:\efi1.1\diag
```

  - To delete an environment variable:

```
Shell> set -d diagnosticpath
Shell> set
                * path           : .
```

- To change an environment variable:

```
fs0:\> set src efi
fs0:\> set
              * path : .;fs0:\efi\tools;fs0:\efi\boot;fs0:\
                src  : efi
fs0:\> set src efi1.1
fs0:\> set
              * path : .;fs0:\efi\tools;fs0:\efi\boot;fs0:\
                src  : efi1.1
```

- To append an environment variable:

```
Shell> set
              * path          : .
Shell> set path %path%;fs0:\efi\tools;fs0:\efi\boot;fs0:\
Shell> set
              * path          : .;fs0:\efi\tools;fs0:\efi\boot;fs0:\
```

- To set a volatile variable that will disappear at the next boot:

```
Shell> set -v EFI_SOURCE c:\project\EFI1.1
Shell> set
              * path       : .;fs0:\efi\tools;fs0:\efi\boot;fs0:\
              * EFI_SOURCE : c:\project\EFI1.1
```

10.1.39 shift

Shifts batch file input parameter positions.

```
SHIFT
```

1. The SHIFT command is only available in batch script files.
2. Each time the SHIFT command is executed the parameters are shifted one position higher, giving you access to more than ten parameters.

- **Examples:**
  - To execute a batch file named **MySript.nsh**:

```
fs0:\> MyScript.nsh X1 X2 X3 X4 X5 X6 X7 X8 X9 X10
```

The parameters available when **MyScript.nsh** initially begins execution will be set as follows:

%1 = X1
%2 = X2
%3 = X3
%4 = X4
%5 = X5
%6 = X6
%7 = X7
%8 = X8
%9 = X9

- To shift the parameters one position inside the batch file:

```
shift
```

The parameters available in **MyScript.nsh** are changed as follows:

%1 = X2
%2 = X3
%3 = X4
%4 = X5
%5 = X6
%6 = X7
%7 = X8
%8 = X9
%9 = X10

10.1.40smbiosview

Displays SMBIOS information.

```
SMBIOSVIEW [-t SmbiosType]|[-h SmbiosHandle]|[-s]|[-a]
```

-t	Displays all structures of SmbiosType
SmbiosType	SMBIOS structure type
-h	Displays structure of SmbiosHandle
SmbiosHandle	SMBIOS structure unique 16-bit handle
-s	Displays statistics table
-a	Displays all information

1. The SmbiosType parameter supports the following types:
   - 0 - BIOS Information
   - 1 - System Information
   - 2 - Base Board Information
   - 4 - Processor Information
   - 7 - Cache Information
   - 11 - OEM Strings
   - 16 - Physical Memory Array
   - 17 - Memory Device
   - 18 - 32-bit Memory Error Information
   - 19 - Memory Array Mapped Address
   - 20 - Memory Device Mapped Address
   - 21 - Built-in Pointing Device
   - 22 - Portable Battery
   - 26 - Voltage Probe
   - 27 - Cooling Device
   - 28 - Temperature Probe
   - 29 - Electrical Current Probe
   - 32 - System Boot Information
   - 34 - Management Device
   - 35 - Management Device Component
   - 36 - Management Device Threshold Data
   - 39 - System Power Supply
2. The SmbiosHandle parameter can be specified in either decimal or hexadecimal format. Use the '**0x**' prefix format for hexadecimal values.

10.1.41 smbutil

Reserved - Not To Be Used

10.1.42 time

Displays or changes the current system time.

```
time [hh:mm[:ss]]
```

hh	Hour of time to set, range: **0 - 23**
mm	Minute of time to set, range: **0 - 59**
ss	Second of time to set, range: **0 - 59**

1. Hour and minute are required to set the time.
2. If second is not specified, 0 will be used as default.

10.1.43 timezone

Displays or sets time zone information.

```
TIMEZONE [-s hh:mm | -l] [-b] [-f]
```

-s hh:mm	Sets time zone associated with **hh:mm** offset from GMT
-l	Displays list of all time zones
-b	Displays one screen at a time
-f	Displays full information for specified timezone

- Example:

```
VM6052/VM6054> timezone -s +1:00

VM6052/VM6054> timezone -f
GMT+01:00, Amsterdam, Berlin, Bern, Rome, Paris, West Central Africa
```

The current time is not modified by this command; it is only an information about the time zone displayed with the command time.

10.2 Environment Variables

EFI shell allows user to set environment variables.

Three environment variables are available on VM6052/VM6054 board to control the behavior of EFI shell as described hereafter.

10.2.1 Bootcmd

The environment variable "**bootcmd**" allows the end user to run automatically an EFI command at startup of the EFI shell without typing any command on the keyboard.

- Examples:

1. To set **bootcmd** to run the "**pci**" command on EFI shell:

```
VM6052/VM6054> set bootcmd "pci"
```

2. To check if the **bootcmd** variable is set on EFI shell:

```
VM6052/VM6054> set
bootcmd: pci
```

3. To clear the **bootcmd** variable on EFI shell:

```
VM6052/VM6054> set -d bootcmd
```

10.2.2 Bootdelay

The environment variable "**bootdelay**" defines a delay in seconds before executing the bootstring defined in 10.2.1 "**Bootcmd**" (0 means no delay).

- Examples:

1. To set bootdelay with a delay of 2 seconds:

```
set bootdelay 2
```

2. To clear bootdelay variable:

```
set -d bootdelay
```

10.2.3 StartupAuto

The environment variable "**StartupAuto**" allows user to run the EFI shell script file "**startup.nsh**" present for example on a USB Flash drive plugged on the board.

- Examples:

1. To set **StartupAuto** variable on EFI shell:

```
VM6052/VM6054> set StartupAuto 1
```

2. To clear **StartupAuto** variable on EFI shell:

```
VM6052/VM6054> set -d StartupAuto
```

10.2.4 StartupDelay

The environment variable "**StartupDelay**" allows user to set a timeout delay before running the EFI shell script file "startup.nsh" present for example on a USB Flash drive plugged on the board.

The value of "**StartupDelay**" is a number that represents a delay in seconds.

- **Examples:**

1. To set a 2 seconds delay in **StartupDelay** variable on EFI shell:

```
VM6052/VM6054> set StartupDelay 2
```

2. To clear **StartupDelay** variable on EFI shell:

```
VM6052/VM6054> set -d StartupDelay
```

By default, the startup delay before running the EFI shell script **startup.nsh** is equal to 5 seconds.

11 / BIOS Versions Description

11.1 Recommendations and Known Limitations

1. Reserved Setup settings

CAUTION: All the settings that are not described in this documentation are reserved and should not be changed. Changing any of these settings may cause system dysfunction or failure.

2. After BIOS upgrades

It is recommended to turn the system off and do a power-on after upgrading the BIOS with the EFI shell "**kflash**" command or another utility.

3. Display Port hot plug

The BIOS does not support hot plug for Display Port. The user has to plug the Display Port device before switching the board on.

4. ACPI warnings under Linux OS

Some ACPI warnings are logged under the Linux Fedora operating system using the "**dmesg**" utility. Those messages are not errors and should be ignored.

5. HEST and ERST ACPI tables are not supported

Currently, the BIOS does not implement the Hardware Error Source Table (HEST) and the Error Record Serialization Table (ERST) in the ACPI atbles. So, the operating system cannot retrieve error information as the PCI-Express Advanced Error reporting (AER).

6. "kflash" command limitation

The "**-i**", "**-v**" and "**-sp**" options of the "**kflash**" command are not operational.

7. Intel® vPro™

Intel® vPro' technology is a set of security and manageability capabilities built into the 3rd generation Intel® Core vPro' processor family like Intel "Ivy Bridge".

Currently, the BIOS supports only the Intel Virtualization feature as part of the Intel® vPro' technology and this feature is disabled by default into the setup.

8. Thresholds voltage and temperature for device NCT7208Y are set by BIOS during initialization phase.

Thresholds for voltage sensors in device NCT7802Y cannot be changed by end-user and are are summerized in the table below:

VOLTAGE SENSORS	HIGH LIMIT	LOW LIMIT
3V3_SB Voltage	3500 mV	3200 mV
+3V3 Voltage	3600 mV	3120 mV
+5V Voltage	5440 mV	4720 mV
+1.5V DDR3 Voltage	1580 mV	1420 mV
+1.35V DDR3 Voltage	1450 mV	1280 mV

The default value programmed by BIOS for high limit thresholds are summerized in the table below:

TEMPERATURE SENSORS	SA CLASS	WA CLASS	RC CLASS
NUVOTON Temp High Limit	70 °C	80°C	90°C
LM73 #1 Temp High Limit	95 °C	95 °C	95°C
LM73 #2 Temp High Limit	95 °C	95 °C	95 °C
LM73 #3 Temp High Limit	65°C	75°C	85°C

The temperature high limit thresholds can be modified in the Setup (see section 5.11 page 36) or using ktemp EFI shell utility (see section 10.1.27 page 73) in order to take into account the environmental condition and also according to the board class

CAUTION: Default temperature high limit threshold parameters were restored with Restore Defaults menu, user must restore these parameters according to class of board in the Setup (see section 5.11 page 36) or using ktemp EFI shell utility (see section 10.1.27 page 73).

A System Management Interrupt (SMI) is generated by the NCT7208Y and passed to CPLD on PECI_ALERT signal each time a threshold is out of range.

The BIOS does not clear this CPLD alert signal and pass the information to OSes in CPLD registers.

The BIOS also transmit thresholds and current value of sensors through SMBIOS tables.

Note that no ACPI tables are updated by this alert to be coherent with ACPI standard. It is up to OSes to trap this signal on CPLD registers and handle it.

9. **NCT7802Y and LM73 low limit thresholds are set by BIOS and cannot be modified by end-user.**

To take into account the fact that OSes works on polling mode, the low limit threshold is set to -45 °C by the BIOS and cannot be modified by end-user.

11.2 Known Problems Table

The following table lists the BIOS relative known problems.

11.2.1 How to Use the Table:

1. Get the BIOS ID associated to your board. Refer to Chapter 3 "Main Menu" page 4 of this document.
2. Check for a specific item in the table rows:
   2.1. A "X" (cross) in the BIOS ID column indicates this item applies to this BIOS release (problem is not solved).
   2.2. No "X" (cross) in the BIOS ID column indicates this item does not apply to this release (problem is fixed).
3. A full description associated to a specific problem is available in the next section.

Item	CRP	Description	BIOS ID			
			ID15127	D16008	ID17087	ID17123
1	4280	Update voltage thresholds on NCT7802Y for VSEN2/VSEN3	X			
2	4281	PBIT does not display the COM2 modem signal errors in complex mode	X			
3	4282	PBIT detect undervoltage on sensor 1V0 on ADS7830 component	X			
4	4283	BIOS cannot read Variant in VPD EEPROM during PEI phase	X			
5	4284	XMC-401 does not boot on PXE on VM6052/VM6054 boards	X			
6	4285	BIOS hangs sometimes on ERROR code with a power cycle endurance test.	X	X	X	
7	4309	ACPI Warnings under dmesg	X	X	X	
8	4310	PBIT: Sometimes COM2 test fails with an incorrect rate error	X	X	X	
9	27082	XMC PBIT test for slot B fails in simple mode	X	X		
10	27175	Need separated kvpd options for motherboard and MOD-GXA VPD management	X	X		
11	27177	GPIO 7&8 on P2 option not implemented in CPLD PBIT test for production	X	X		
12	27764	PBIT: XMC-401 in complex mode is not correctly recognized	X	X	X	
13	28187	PBIT: XMC-ETH2 in PMC mode is not correctly recognized	X	X	X	

11.2.2 Detailed Description of the Problems

Item #1 Update voltage thresholds on NCT7802Y for VSEN2/VSEN3 - CRP 4280

Description: Thresholds voltage and temperature for device NCT7208Y are set by BIOS and cannot be modified by end-user. The current value programmed in BIOS does not take into account the tolerance of passive components and device itself, so thresholds must be updated with the values described in section 11.1 page 100.

Workaround: None

Item #2 PBIT does not display the COM2 modem signal errors in complex mode - CRP 4281

Description: Customer does not see any message when running "**`serial`**"(16) test FAILED due to an error on Modem signals (RTS/CTS,...).

Workaround: Use the PBIT "**`kdiag verbose`**" command to add verbosity.

Item #3 PBIT detect undervoltage on sensor 1V0 on ADS7830 component - CRP 4282

Description: Issue is present on Test 48 with "**`kdiag run 1000000`**" command.
Occurence is 8 FAILED on 2750 loops with following messages:

```
PBIT "voltage" (fast,simple)
Voltage value for 1V0 3U is out of range (937 mV)
It should be between 950..1050 mV
FAILED
```

or:

```
Voltage value for 1V0 3U is out of range (947 mV)
It should be between 950..1050 mV
FAILED
```

Thresholds for ADS7830 device must be updated in PBIT according to tolerance and accuracy of the device and passive components on the board.

Workaround: None

Item #4 BIOS cannot read Variant in VPD EEPROM during PEI phase - CRP 4283

Description: Running PBIT serial(16) test, with option COM2 PENTXM2 Compatibility (Full-Modem) in variant, is FAILED on VM6052 in complex mode. This is due to a bad read of the variant in PEI phase. The solution is to increase the number of retry on internal I2C in PEI phase to read VPD EEPROM for COM2 initialization based on variant.

Workaround: None

Item #5 XMC-401 does not boot on PXE on VM6052/VM6054 boards- CRP 4284

Description: PXE boot on XMC-401 is not possible on VM6052/VM6054 boards. BIOS does not integrate a LOM image for 10G Ethernet devices. It is not really a bug but an enhancement because the LOM image is normally provided by OS driver by the XMC board vendor.

Workaround: None

Item #6 BIOS hangs sometimes on ERROR code with a power cycle endurance test - CRP 4285

Description: In rare cases, at power-on, the BIOS may hang on following message:

```
ERROR: Type:2; Severity:90; Class:3; Subclass:5; Operation: 100E
```

This error is due to an internal error related to the USB driver and is very difficult to reproduce.

Impact: VM605x board does not boot.

Workaround: None

Item #7 ACPI Warnings under dmseg - CRP 4309

Description: On VM6052/VM6054 boards, booting Linux with dmesg shows following ACPI Warnings:

```
[    7.251775] ACPI Warning: 0x000000000000f040-0x000000000000f05f SystemIO
conflicts with Region \_SB_.PCI0.SBUS.SMBI 1 (20120320/utaddress-251)
[    7.362543] ACPI Warning: 0x0000000000000420-0x000000000000042f SystemIO
conflicts with Region \PMIO 1 (20120320/utaddress-251)
[    7.362560] ACPI Warning: 0x0000000000000404-0x0000000000000405 SystemIO
conflicts with Region \PMIO 1 (20120320/utaddress-251)
[    7.362570] ACPI Warning: 0x0000000000000540-0x000000000000054f SystemIO
conflicts with Region \GPIO 1 (20120320/utaddress-251)
[    7.362578] ACPI Warning: 0x0000000000000530-0x000000000000053f SystemIO
conflicts with Region \GPIO 1 (20120320/utaddress-251)
[    7.362586] ACPI Warning: 0x0000000000000500-0x000000000000052f SystemIO
conflicts with Region \GPIO 1 (20120320/utaddress-251)
```

Impact: No impact

Workaround: None

Item #8 PBIT: Sometimes COM2 test fails with an incorrect rate error - CRP 4310

Description: On VM6052/VM6054 board, in rare cases, an error may occur on COM2 serial test with the following message:

```
<06/13/15 21:46:09.73> PBIT "core_dmi" (fast,simple)  PASSED
<06/13/15 21:46:09.79> PBIT "tpm" (fast,simple)   TPM NOT EQUIPPED PASSED
<06/13/15 21:46:09.84> PBIT "serial" (fast,simple)  COM2 Serial Line Measured
rate is incorrect (5783 instead of 9600)
<06/13/15 21:46:10.09> FAILED
<06/13/15 21:46:10.09> PBIT "rtc" (fast,simple)  PASSED
```

This error is triggered by PBIT when the rate is 70 % below the theorical speed rate of 9600 bauds equivalent to 6720 bauds.

The serial speed of the UART is computed from the CPU clock (TSC).

Impact: PBIT COM2 “serial” test fails

Workaround: None

Item #9 XMC PBIT test for slot B fails in simple mode – KDP 27082

Description: With PBIT version 1.10 ID15329, the PBIT test pmcB_xmc_check(78) fails if a XMC other than XMC-401 is plugged in slot B.

Workaround: None

Item #10 Need separated kvpd options for motherboard and MOD-GXA VPD management – KDP 27175

Description: `kvpd -p, -m` commands currently manage both the motherboard and the MOD-GXA VPD. We need to implement other options for managing the MOD-GXA VPD separately: `-gp`, `-gm`.

Workaround: None

Item #11 GPIO 7&8 on P2 option not implemented in CPLD PBIT test for production – KDP 27177

Description: The "GPIO 7&8 on P2" option is not taken into account in the GPIO test of the CPLD PBIT test for production (complex mode).

The additional test will require an hardware connection between the 2 signals on P2: PMC1 IO 63/GPIO8 and PMC1 IO 64/GPIO7.

Workaround: None

Item #12 PBIT: XMC-401 in complex mode is not correctly recognized – KDP 27764

Description: Tests 77 "pmcA_xmc_see" and 79 "pmcB_xmc_see" are FAILED in complex mode (OK in simple mode).

Workaround: Configure the tests 77 and 79 in simple mode.

Item #13 PBIT: XMC-ETH2 in PMC mode not correctly recognized – KDP 28187

Description: The PBIT tests 76 is FAILED in complex mode with an XMC-ETH2 with a wrong reason: "PMC bus is not at 133 Mhz (reg 58h = 0x00036807)"
This is due to the presence of the bridge 8112 on the XMC-ETH2 that the PBIT does not take into account in the test.

Workaround: None

11.3 BIOS ID14112 Release Notes

The following lists the evolutions or enhancements relative to this BIOS release:

- **Accessible by setup:**
  - Serial Port Console Redirection on COM0 and/or COM1 - Section 5.7 page 30
  - PCI Configuration - Section 5.2 page 23
  - VME Configuration - Section 5.8 page 32
  - USB keyboard configuration - Section 5.3 page 26
  - UUID Configuration - Section 5.4 page 27
  - Watchdog timer implementation at OS boot time - Section 5.10 page 33
  - Vital Product Data display - Section 5.5 page 28

- **Accessible by Kontron EFI commands (Refer to chapter 10 page 54 for details):**
  - **`kdiag`**, Board diagnostics (feature available only if ordered)
  - **`kflash`**, SPI flasher.
  - **`kmac`**, Gigabit Ethernet Controller i82580 MAC address management.
  - **`kpld`**, CPLD register and I2C device access
  - **`ktemp`**, Board temperature and voltage sensors display.
  - **`kvpd`**, Vital Product Data information

11.4 BIOS ID14210 Release Notes

The following lists the evolutions or enhancements relative to this BIOS release:

- Fix bug#7050: Suppress checking for SPI Write-Protection microswitch SW1.3 in **kmac** utility since no PCH GbE LAN is present on the board
- Fix bug#7090: Security password does not protect all the setup
- Fix bug#7129: 3.3V high threshold set to 3.450V is too short on new rack; 3V3 and 3V3SB high threshold set to 3.500V in SMBIOS table
- Fix bug#7130: EFI shell command **cpuutil** hangs without arguments
- Enhancement: display UUID in setup and SMBIOS table following RFC4122
- Enhancement: udpate Intel Microcode for Ivy Bridge to Revision 0x1B
- Enhancement: add 'info' option to cpuutil to display CPU information

This release also includes the PBIT software(*) V1.4 ID14204 implementing the following evolutions:

- System test evolutions (following Fixed CPLD bug#6926 and BIOS bug#7009): only probe backplane SMBus0 with I2C addresses range 0x18 to 0x2C which correspond to VME boards and SMBUS1 is reserved for custom device.
- Limitation: SMBUS test not fully supported.
- Fix bug#6947: restore default Watchdog mode and countdown value after PBIT
- Fix bug#7096: kdiag system command not allowed if PBIT not activated
- Fix bug#7115: wrong value displayed if 3.3V low limit threshold overrange
- Fix bug#7126: PBIT edit system: edit problem with pci options p or pa
- Fix bug#7129: 3.3V high threshold set to 3.450 V is too short on new rack; 3V3 and 3V3SB high threshold are set to 3.500 V in BIOS and 'hwmon' test
- Fix bug#7132: PBIT learn system: the number of detected devices is not correct
- Fix bug#7133: PBIT edit system: if SMBUS is ignored, "unknown type dans constructeur" messages are displayed
- Fix bug#7134: PBIT system test does not detect PMC/XMC presence correctly

(*) PBIT - Power on Built In Test - is a software developed by Kontron. It is an optional product.

For more information, please contact your field representative.

11.5 BIOS ID14288 Release Notes

The following lists the evolutions or enhancements relative to this BIOS release:

- Fix bug#7141: default VGA DDC signals to Enabled in Setup
- Fix bug#7142: PBIT hwmon test always fails after Power-on with a message related to Nuvoton
- Fix bug#7146: GPIO71 must be programmed by BIOS in GPI instead of GPO
- Fix bug#7150: Handle are not correct in SMBIOS table DMI Type 35
- Enhancement: add 3rd LM73 in ktemp utility and SMBIOS table for PCB B
- Enhancement: add thresholds in ktemp utility
- Enhancement: add new options in kpld utility for testing LED
- Enhancement: add option in kmac utility for checking CRC in 82580 EEPROM
- Enhancement: add option in kmac utility for programming 82580 EEPROM
- Enhancement: update cpuutil /info
- Enhancement: add PXE selection in Kontron configurator utility for MANUFACTURING
- Enhancement: add MOD-GXA VPD EEPROM support in kvpd utility

This release also includes the PBIT software(*) V1.5 ID14287 implementing the following evolutions:

- Evolution bug#7085: PBIT activation lost after RMA
- Evolution bug#7127: add a mecanism to bypass PBIT from OS
- Fix bug#7145: Do not bypass PBIT for MANUFACTURING if PBIT Customer bypassed
- Enhancement: Add 3rd LM73 in test temperature (32)
- Enhancement: Add default test sata4_dev_see (67) for on-board SDD

(*) PBIT - Power on Built In Test - is a software developed by Kontron. It is an optional product.

For more information, please contact your field representative.

11.6 BIOS ID14332 Release Notes

The following lists the evolutions or enhancements relative to this BIOS release:

- Fix bug#7154: default is Turbo disabled and C-States disabled in CPU PPM Configuration menu. CPU speed is set to Max Non-Turbo Frequency (2100 MHz) in Kontron CPU Configuration menu for SA/RC class.
- Enhancement: add SMBIOS table compatibility with PCB A
- Enhancement: change "DDR3-1V5" by "DDR3-1V50" in SMBIOS Table and add a "DDR3-1V35" voltage probe if DDR3 Low Voltage Memory parts are equipped
- Enhancement: grayout CPU Configuration -> CPU Frequency in Kontron menu if Ivy Bridge CPU supports TDP (VM6052 board)

This release also includes the PBIT software(*) V1.6 ID14296 implementing the following evolutions:

- Enhancement: check CRC of 82580 EEPROM in ethernet tests 55 to 58
- Enhancement: check CRC of SPD EEPROM in memory tests 1 to 9
- Enhancement: check coherency between VPD and SPD in memory tests 1 to 9
- Enhancement: add MOD-GXA test(15) if MOD-GXA module is equipped

(*) PBIT - Power on Built In Test - is a software developed by Kontron. It is an optional product.

For more information, please contact your field representative.

11.7 BIOS ID14349 Release Notes

The following lists the evolutions or enhancements relative to this BIOS release:

- Fix bug#7163: Product Name field in SMBIOS table DMI Type 1 not correct

This release also includes the PBIT software(*) V1.7 ID14344 implementing the following evolutions:

- Fix bug#7168: PBIT customer test pmcA_xmc_check(76) fail if PMC PCI-X plugged is not 133 MHz capable

(*) PBIT - Power on Built In Test - is a software developed by Kontron. It is an optional product.

For more information, please contact your field representative.

11.8 BIOS ID15034 Release Notes

The following lists the evolutions or enhancements relative to this BIOS release:

- Fix bug#7123: CPU Frequency not set correctly on VM6054 board (Quad-core)
- Fix bug#7159: SMBIOS table last handle type 127 is wrong
- Fix bug#7177/bug#7178: Fix bug on **`krcconfig`** utility used for Manufacturing only

This release also includes the PBIT software(*) V1.8 ID14351 implementing the following evolutions:

- Fix bug#7170: PBIT test usb1_dev_see() is always PASSED if USB drive is plugged on rear P0 USB2 port
- Fix bug#7171: sata4_dev_see(67) test is seen as simple mode instead of complex mode
- Fix bug#7172: usb1_dev_see(81) test is seen as complex mode instead of simple mode
- Fix bug#7173: for temperature(32) test, do not probe 3rd LM73 if board is PCB A

(*) PBIT - Power on Built In Test - is a software developed by Kontron. It is an optional product.

For more information, please contact your field representative.

11.9 BIOS ID15127 Release Notes

The following lists the evolutions or enhancements relative to this BIOS release:

- Fix bug#7182: SPI Flash Write-Protect not set correctly
- Fix bug#7192: Add support for new SPI Flash NUMONYX(Micron) N25Q064
- Fix bug#7194: PL1/PL2 settings from Setup for VM6052 boards is not working
- Fix bug#7197: CPU straps for FLEX ratio must not be set for VM6052 boards ; consequence is that Max Non-Turbo frequency is 2100 MHz instead of 2200 MHz for a VM6052 board configured in TDP UP.
- Fix bug#7199: Improve alternate access mode in RTC to avoid infinite loop on read RTC REGA
- Fix bug#7200: Write Boot mode 0x04 (OS-BOOT) in CPLD register before booting OS
- Fix bug#7201: slva alma2f register does not get the GA value
- Fix bug#7206: COM2 port is not correctly configured for OS using ACPI

This release also includes the PBIT software(*) V1.9 ID15119 implementing the following evolutions:

- Fix bug#7198: Cold/Warm Reset status is done by CPLD.
  PBIT must check Cold/Warm status in CPLD instead of PCH register.
- Fix bug#7205: P0 connector option is not correctly processed by PBIT.
- Fix bug#7207: set LM73 high/low limits for polling under Linux and set Nuvoton and LM73 temperature limits according to board class.

(*) PBIT - Power on Built In Test - is a software developed by Kontron. It is an optional product.

For more information, please contact your field representative.

11.10 BIOS ID16008 Release Notes

The following lists the evolutions or enhancements relative to this BIOS release:

- Fix CRP#4284/Bug#7184: PXE boot on XMC-401 is supported.
- Fix CRP#4280/Bug#7213: update voltage thresholds on NCT7802Y for VSEN2/VSEN3 3.120 V <= VSEN2 <= 3.600 V and 4.720 V <= VSEN3 <= 5.440 V
- Fix CRP#4283/Bug#7220: increase number of retries on internal I2C Bus in PEI phase to read VPD EEPROM for COM2 initialization based on variant bit D[28].
- Fix Bug#7255(HW WORK-AROUND): PCIe Link Speed forced to Gen1 (1.5 Gb/s) for PEG2 connected to chipset Ethernet Intel 82580 on RA/WA/RC class board.
- Fix Bug#7256: FOR MANUFACTURING ONLY, to enter VPD on MOD-GXA EEPROM.
- Fix Bug#7263: SMBIOS table are not correct for LM73 devices and update NCT7802Y thresholds.
- Fix Bug#7269: CPU speed not set correctly in Setup using Restore Defaults for RC class board.
- Fix Bug#7270: display a message in setup and for manufacturing utility if SPI Flash is Write-Protected.
- Enhancement: boot 1s faster with default boot time set to zero by default.
- Enhancement: Add support for RA/RC/WA class board.
- Enhancement: Add support for UEFI Shell Protection (PBIT)

This release also includes the PBIT software(*) V1.10 ID15329 implementing the following evolutions:

- Fix CRP#4281/Bug#7209: PBIT does not display the COM2 modem signal errors in complex mode.
- Fix CRP#4280/Bug#7213: PBIT hwmon(61) updated with new thresholds.
- Fix CRP#4282/Bug#7217: PBIT undervoltage detected on ADS7830 (update thresholds).
- Fix Bug#7220: PBIT serial(16) failed due to short number of I2C retries to read correctly the serial COM2 mode defined in VPD EEPROM.
- Fix Bug#7260: Test MOD-GXA(15) must not run if MOD-GX is plugged instead of MOD-GXA graphic board.

(*) PBIT - Power on Built In Test - is a software developed by Kontron. It is an optional product.

For more information, please contact your field representative.

11.11 BIOS ID17087 Release Notes

The following lists the evolutions or enhancements relative to this BIOS release:

- Fix kdp#27175: Need separated **kvpd** options for motherboard and MOD-GXA VPD management.

This release also includes the PBIT software(*) V1.11 ID17086 implementing the following evolutions:

- Fix kdp#27082: XMC PBIT test for slot B fails in simple mode.
- Fix kdp#27177: GPIO 7&8 on P2 option not implemented in CPLD PBIT test for production.

(*) PBIT - Power on Built In Test - is a software developed by Kontron. It is an optional product.

For more information, please contact your field representative.

11.12 BIOS ID17123 Release Notes

The following lists the evolutions or enhancements relative to this BIOS release:

- No changes for the BIOS, only for new PBIT version embedded.

This release also includes the PBIT software(*) V1.12 ID17117 implementing the following evolutions:

- Fix kdp#27764: XMC-401 in complex mode is not correctly recognized
- Fix kdp#28187: XMC-ETH2 in PMC mode is not correctly recognized

(*) PBIT - Power on Built In Test - is a software developed by Kontron. It is an optional product.

For more information, please contact your field representative.

12 / Use Cases

This chapter gives some advise for following pratical cases:

- DEPLOY : How to deploy VM6052/VM6054 - BIOS, section 12.1 page 113
- DEVEL: How to develop applications with VM6052/VM6054 - BIOS, section 12.2 page 114
- EVAL: How to benchmark VM6052/VM6054 - BIOS, section 12.3 page 114
- TROUBLESHOOT: How to troubleshoot VM6052/VM6054 - BIOS, section 12.4 page 114

12.1 DEPLOY: How to deploy VM6052/VM6054 - BIOS

Deploying with VM6052/VM6054 boards usually requires to handle the following tasks:

- Cloning a board,
- Managing a pool of deployed boards.

12.1.1 Cloning a board:

To be able to replace a VM6052/VM6054 with another one in a system, cloning allows to duplicate VM6052/VM6054 settings in the new board prior to replacement. This is how to proceed with VM6052/VM6054:

- **On Original VM6052/VM6054**

Duplicate the hardware settings. (see VM6052/VM6054 User's Guide: chapter Configuration)

Duplicating BIOS settings:

BIOS and BIOS settings are stored in the BIOS FLASH device itself. See Annex A.3 page 116 of this document to know how to save a BIOS ROM image.

- **New VM6052/VM6054**

Check the Board EC level to insure the BIOS + Settings you are going to install are compatible with the hardware evolution.

See Annex A.1 page 115 on how to program the new BIOS + settings.

Boot the board and set the Date Time to the correct date/time.

Now the new board is a functional clone ot the initial VM6052/VM6054.

Once the system has been qualified, it may be a good idea to save the image of the BIOS + Settings for later use.

In the case of removable storage like USB or SATA FLASH mezzanine, refer to VM6052/VM6054 User's Guide (CA.DT.A95) for details of removal and fitting operations.

For large programs, Kontron can contribute with high level software to automate this cloning task. Contact support-kom-sa@kontron.com for details.

12.1.2 Managing a pool of VM6052/VM6054:

To manage a pool of boards, the main task is to identify and track board using serial number, E.C. Level, BIOS version, MAC addresses, etc... possibly without having to take the system apart to look at its labels.

See chapter 2.2 of VM6052/VM6054 User's Guide about the board identifcation labels.

See section 5.5 page 28 on VPD of this document to retrieve the board serial number and E.C. level.

See VPD Tool in the Linux BSP document to know how to get this information from a Linux OS running on the board.

The BIOS information is also transmitted from the BIOS to the OS using a software table in memory, use the **`dmidecode`** command to retrieve this information from Linux.

Kontron maintains a database of all the boards sold to customers. This includes customer, program, system and any information you may wish to have maintained by us, allowing to retrieve an exact board pool status, whenever needed.

Contact support-kom-sa@kontron.com for details.

12.2 DEVEL: How to develop applications with VM6052/VM6054 - BIOS

TBD

12.3 EVAL: How to benchmark VM6052/VM6054 - BIOS

TBD

12.4 TROUBLESHOOT: How to troubleshoot VM6052/VM6054 - BIOS

SETUP not accessible

If setup is not accessible, make sure the board is operational in rescue mode (boot from the rescue SPI flash) or try a BIOS Failsafe boot.

Refer to the VM6052-VM6054 User's Guide section 2.4.2 SW2 Microswitch Description.

SETUP accessible but OS not booting

Enter setup by pressing the <F2> key as indicated at BIOS boot time and check if the boot device is visible in the boot device list. See chapter 7 page 41 “Boot Method and Priority” of this document

It could be worth restoring the default manufacturing setup configuration.

Appendix A - How to Update and Restore the BIOS

A.1 Update BIOS from UEFI Shell using USB device

This section details the update of the AMI BIOS Firmware on a VM6052/VM6054 board. An USB key with the BIOS image to flash will be used.

Operating Mode

- Copy the BIOS image under the USB device
- Boot VM6052/VM6054 on UEFI shell. If necessary enter the BIOS SETUP pressing <F2> during the boot sequence. Then navigate to Save & Exit Menu and select UEFI shell in Boot override menu and boot under UEFI shell. Plug the USB device on the concerned USB interface
- Enter command

```
map -r
```

- fs0: file system must become visible, then Enter

```
fs0:
```

- Eventually use cd command to reach a directory where the Bios image is stored. Use ls to display file list

  If BIOS image is named **VM6052/VM6054_IDYYXXX.bin** then flash the BIOS entering command

```
VM6052/VM6054 > kflash -p -r  VM6052/VM6054_IDYYXXX.bin
```

CAUTION: Do not turn off nor reset the board until the end of the command. This prevent the system to boot at next power on.

- Wait about 1 minutes and 30 seconds and check if message "**image are equal**" is displayed. If not, do again the flash update. When upgrade is finished without any errors, then turn off the system and do a fresh cold start in order to boot with the new BIOS.

The serial console displays a toolbar **[======]** during Flash process to show the progression of the Flash update while the graphical screen not.

A.2 Restore or Update BIOS from Rescue BIOS

A rescue BIOS is available on any VM6052/VM6054 CPU. It is possible to boot on rescue BIOS and update the main BIOS with the rescue BIOS.

When board is powered off, set micro switch SW2 function 1 to ON. Then Boot on Rescue BIOS and EFI-Shell. If necessary enter BIOS SETUP with F2 in boot sequence and then navigate to Save & Exit Menu and select UEFI shell in Boot override menu. Check if EFI-Shell prompt is VM6052/VM6054-RESCUE.

- Enter command:

```
VM6052/VM6054-RESCUE> kflash -c
```

CAUTION: Do not power down the board during update process. This behavior will prevent the board to boot.

- Wait about 1 minutes and 30 seconds the command end.

  The BIOS is restored. Power off the board, set micro switch SW2 function 1 to Off then boot on Main BIOS.

A.3 Record BIOS image ROM and setting from UEFI Shell using USB device

This section details the record of the AMI BIOS Firmware and its setting of a VM6052/VM6054 board. An USB key will be used to store the BIOS image

Operating Mode

- Boot VM6052/VM6054 on UEFI shell. If necessary enter BIOS SETUP with F2 in boot sequence. Then navigate to Save & Exit Menu and select UEFI shell in Boot override menu and boot under UEFI shell. Plug the USB device on the concerned USB interface
- Enter command

```
map -r
```

- fs0: file system must become visible, then Enter

```
fs0:
```

- Eventually use cd command to reach a directory where the Bios image is stored. Use ls to display file list

  If BIOS image is named **VM6052/VM6054_CLONE.bin** then copy the BIOS image entering command

```
VM6052/VM6054> kflash -s  VM6052/VM6054_CLONE.bin
```

- Wait 20 seconds. When finished without error then the BIOS ROM image is stored onto the USB device.

About Kontron

Kontron, a global leader in embedded computing technology and trusted advisor in IoT, works closely with its customers, allowing them to focus on their core competencies by offering a complete and integrated portfolio of hardware, software and services designed to help them make the most of their applications.

With a significant percentage of employees in research and development, Kontron creates many of the standards that drive the world's embedded computing platforms; bringing to life numerous technologies and applications that touch millions of lives. The result is an accelerated time-to-market, reduced total-cost-of-ownership, product longevity and the best possible overall application with leading-edge, highest reliability embedded technology

Kontron is a listed company. Its shares are traded in the Prime Standard segment of the Frankfurt Stock Exchange and on other exchanges under the symbol "KBC".
For more information, please visit: **www.kontron.com**

CORPORATE OFFICES

FRANCE

150, rue Marcelin Berthelot
ZI de Toulon-Est . BP 244
83078 Toulon Cedex 9 - France
Tel: +33 4 98 16 34 00
Fax: +33 4 98 16 34 01
sales.KFR@kontron.com

HEAD OFFICE

Lise-Meitner-Str. 3-5
86156 Augsburg
Germany
Tel.: + 49 821 4086-0
Fax: + 49 821 4086-111
info@kontron.com

NORTH AMERICA

14118 Stowe Drive
Poway, CA 92064-7147
USA
Tel.: + 1 888 294 4558
Fax: + 1 858 677 0898
info@us.kontron.com

ASIA PACIFIC

1~2F, 10 Building, No. 8 Liangshuihe 2nd Str.
Economical & Technological Develop. Zone,
Beijing, 100176, P.R. China
Tel.: + 86 10 63751188
Fax: + 86 10 83682438
info@kontron.cn