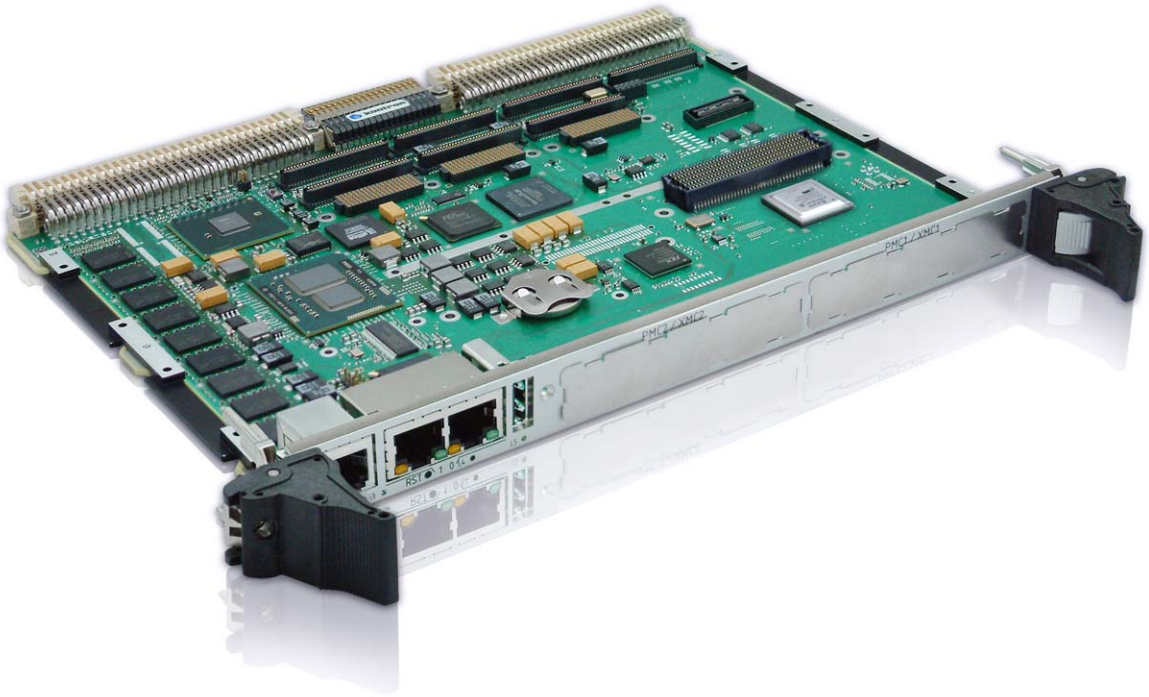
kontron

» VM6050 «



AMI BIOS User Reference Manual

SD.DT.F89-8e - August 2015

Revision History

Publication Title:	VM6050 AMI BIOS User Manual	
Doc. ID:	SD.DT.F89-8e	
Rev.	Brief Description of Changes	Date of Issue
8e	Updated section: 11.2 - Known Problems Table New section: 11.9 - BIOS ID15202 Release Notes	08-2015
7e	New sections: - 4.3 - S5 RTC Wake Settings - 10.1.25 - Kmac - 11.8 - BIOS ID14153 Updated sections: - 4 - Advanced Menu - 10-1 - EFI Shell Command - 11.2 - Know Problem Table	06-2014
6e	New sections: - 6.4 North Bridge & Memory Configuration - 11.7 BIOS ID13281 Release Notes Updated sections: - 10.1 EFI Shell Command - 11.2 Known Problem Table	10-2013
5e	New BIOS ID 13246 Update of section 11.2 - Know Problems Table	09-2013
4e	Update of section 11.2 - Know Problems Table	06-2013
3e	New BIOS ID 13078 Add of new section 6.3 - North Bridge and Display Hot Plug Configuration Update of section 11.2 - Know Problems Table	05-2013
2e	Update of Chapter 5 11.2.2 New items 11.4 New section	07-2012
1e	Chapter 5: New section - USC Misc Configuration Update of Board Misc Configuration Chapter 6: New section - South Bridge et Sata Configuration Chapter 11: Update of limitations	02-2012
0e	Initial Version	11-2011

Proprietary Note

This document contains information proprietary to Kontron. It may not be copied or transmitted by any means, disclosed to others, or stored in any retrieval system or media without the prior written consent of Kontron or one of its authorized agents.

The information contained in this document is, to the best of our knowledge, entirely correct. However, Kontron cannot accept liability for any inaccuracies or the consequences thereof, or for any liability arising from the use or application of any circuit, product, or example shown in this document.

Kontron reserves the right to change, modify, or improve this document or the product described herein, as seen fit by Kontron without further notice.

Trademarks

This document may include names, company logos and trademarks, which are registered trademarks and, therefore, proprietary to their respective owners.

Environmental Protection Statement

This product has been manufactured to satisfy environmental protection requirements where possible. Many of the components 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

Conventions

This guide uses several types of notice: Note, Caution, ESD.

Note: this notice calls attention to important features or instructions.


Caution: this notice alert you to system damage, loss of data, or risk of personal injury.


ESD: This banner indicates an Electrostatic Sensitive Device.

All numbers are expressed in decimal, except addresses and memory or register data, which are expressed in hexadecimal. The prefix `0x' shows a hexadecimal number, following the `C' programming language convention.

The multipliers `k', `M' and `G' have their conventional scientific and engineering meanings of $*10^3$, $*10^6$ and $*10^9$ respectively. The only exception to this is in the description of the size of memory areas, when `K', `M' and `G' mean $*2^{10}$, $*2^{20}$ and $*2^{30}$ respectively.

When describing transfer rates, `k' `M' and `G' mean $*10^3$, $*10^6$ and $*10^9$ *not $*2^{10}$ $*2^{20}$ and $*2^{30}$.*

In PowerPC terminology, multiple bit fields are numbered from 0 to n, where 0 is the MSB and n is the LSB. PCI and CompactPCI terminology follows the more familiar convention that bit 0 is the LSB and n is the MSB.

Signal names ending with an asterisk (*) or a hash (#) denote active low signals; all other signals are active high.

Signal names follow the PICMG 2.0 R3.0 CompactPCI Specification and the PCI Local Bus 2.3 Specification.

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


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


Caution, Electric Shock!
Before installing a not hot-swappable Kontron product into a system always ensure that your mains power is switched off. This applies also to the installation of piggybacks. Serious electrical shock hazards can exist during all installation, repair and maintenance operations with this product. Therefore, always unplug the power cable and any other cables which provide external voltages before performing work.

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 board 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 board.

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

In performing all necessary installation and application operations, please follow only 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 board, please re-pack it as nearly as possible in the manner in which it was delivered.

Special care is necessary when handling or unpacking the product. Please consult the special handling and unpacking instruction.

Table Of Contents

Chapter 1 - Overview

This manual introduces the SETUP, EFI-SHELL of the AMI BIOS firmware available on Kontron VM6050 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
- CPU Frequency
- Boot method and priority
- Security password

1.1 Structure

1.2 Related Documents

VM6050 Hardware

- VM6050 Hardware Release Notes CA.DT.A94
- VM6050 6U VME SBC User's Guide CA.DT.A93

VM6050 Software

- VM6050 - Release Notes for BSP Fedora 14 . . . . . SD.DT.F82
- Release Notes Fedora 16 on VX304x, VX3035, VM6050 and VM6052/54 . . SD.DT.G11

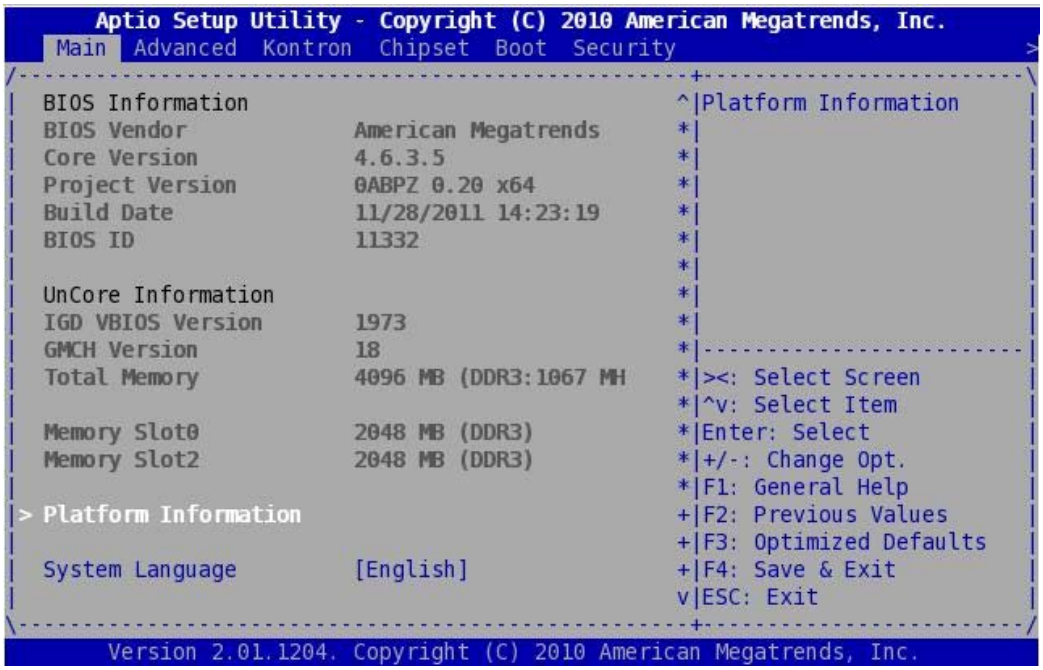
Chapter 2 - Accessing the SETUP Menu

To access the SETUP MENU, press:

<F2> during system boot when the message below is displayed :

```
Version 2.01.1204. Copyright (C) 2010 American Megatrends, Inc.
Press <DEL> or <F2> to enter setup. Press <F7> for BBS POPUP Menu.
```

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.

BIOS ID is the BIOS version identification.

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 VM6050 board.

The following chapter details the items that are available on Kontron VM6050. 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

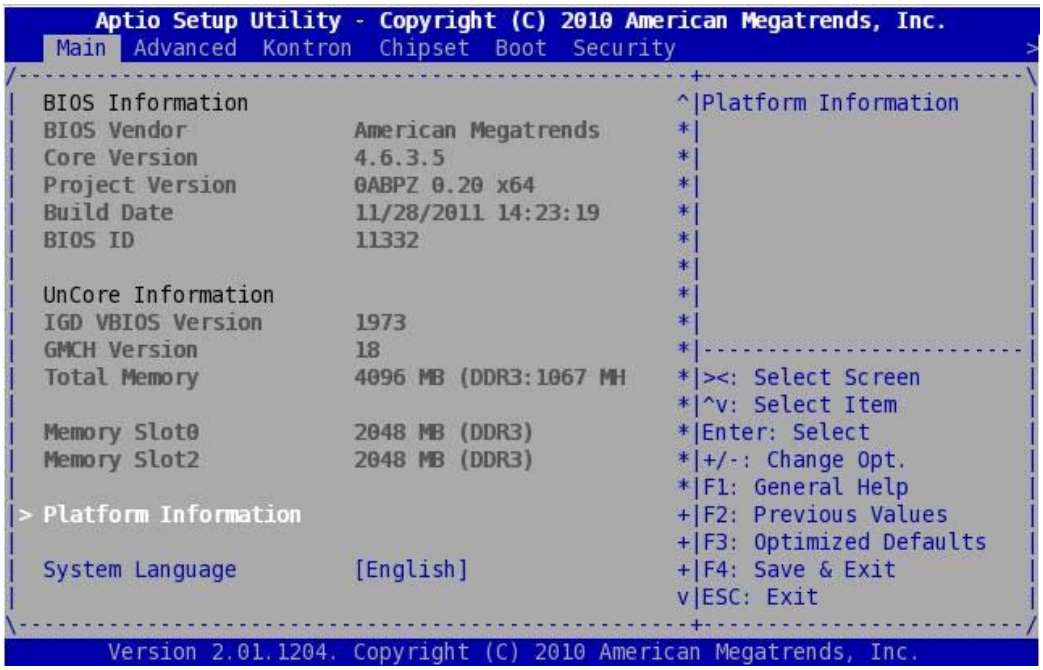
2.2 Boot Manager Menu

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

Chapter 3 - Main Menu

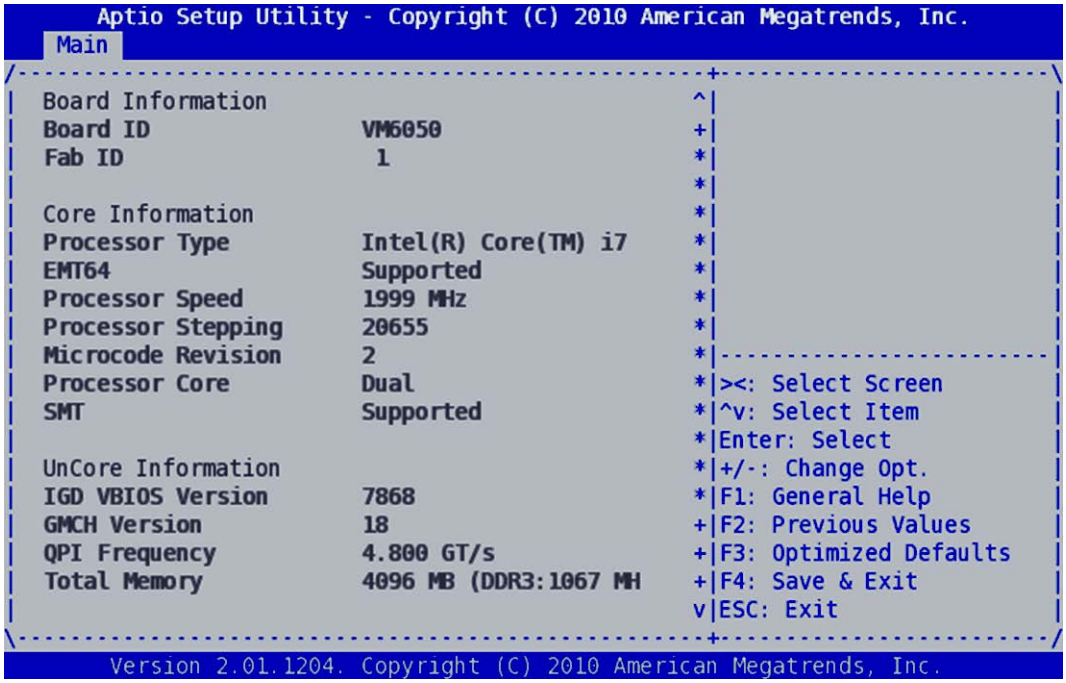
The Main Menu provides general system information and is the first accessible menu page.

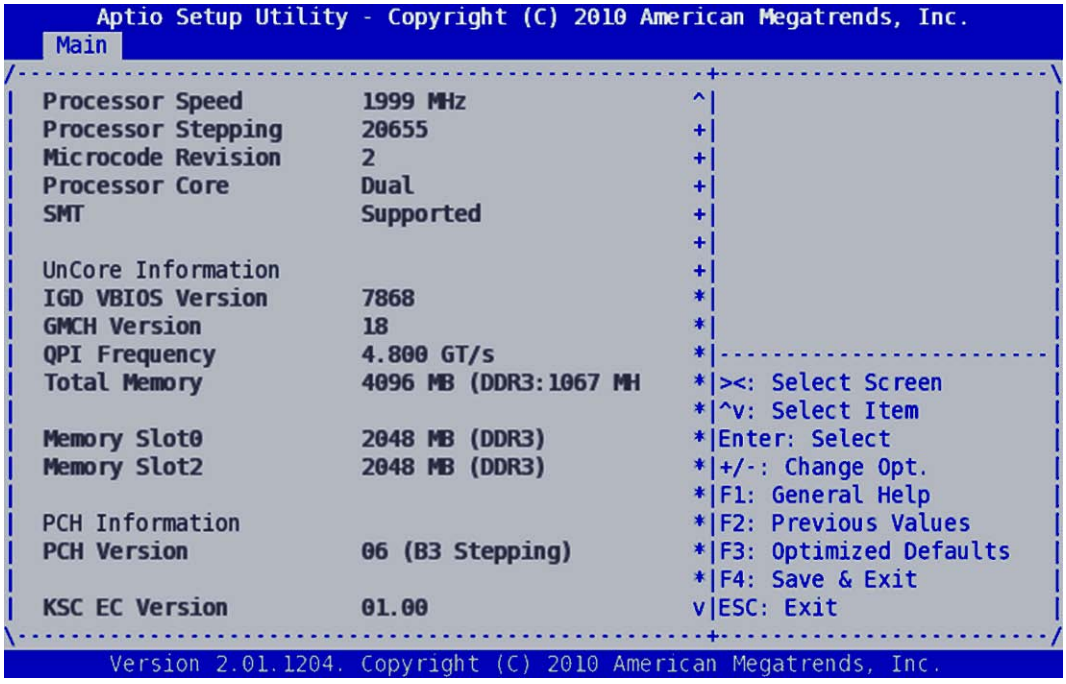


Three submenus or settings, described below, are available in the main menu:

- > Platform Information, section 3.1 page 5
- > System Language, section 3.2 page 6
- > System Date Time, section 3.3 page 6

3.1 Platform Information



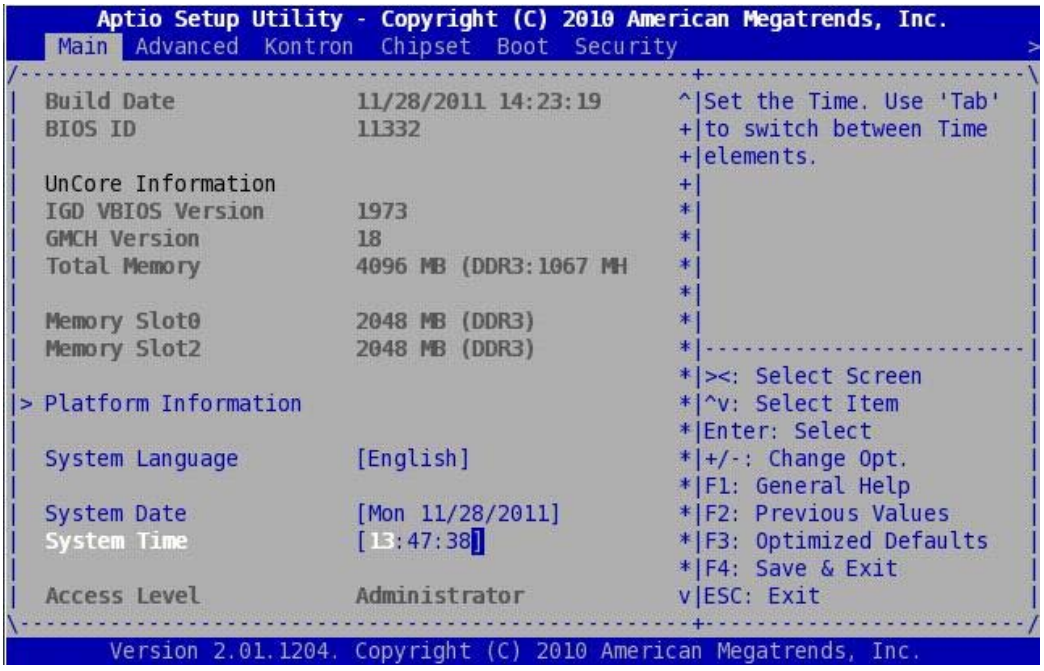


The platform information Menu displays the processor, graphic, memory and PCH (Platform Controller Hub) specific information. Platform information displays all contents by scrolling down using the arrow key <↓>.

3.2 System Language

Nothing can be changed in this menu. Only English language is supported in this version.

3.3 System Date and Time



The submenu is accessible from the Main menu by using <↓> and <↑> arrows keys. The System Date and Time window allows the user to specify the day, month,and year as well as the hour, minute, and second. The clock 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.

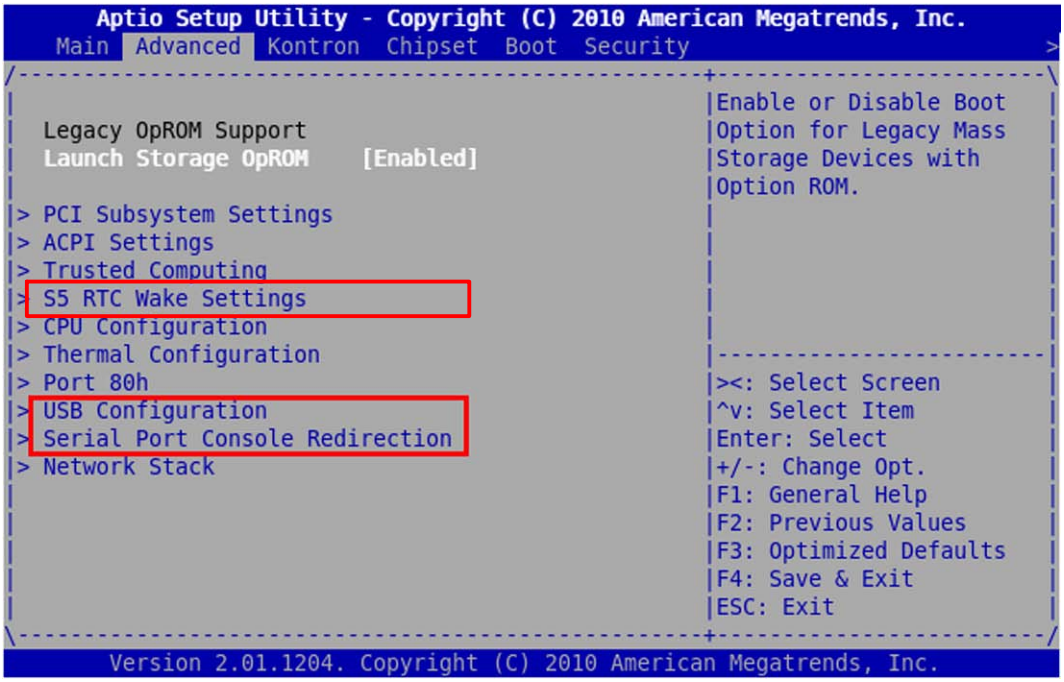
To update the Time, use the **<+>** or **<->**keys to select the Hour (**<+>** to increase / **<->** to decrease the hour), and press the **<Enter>** key to validate your choice. Proceed in the same way for the minutes and finally for the seconds.

The firmware always reads a RTC to display the date and time at each power-on. This RTC needs to be supplied by the external battery otherwise System Date and System Time are initialized with the build date of BIOS except if the power-off/power-on is lower than ~15s. In this case, System Date and System Time start with the power off value.

The VM6050 boards can operate safely without a battery fitted. In this case, the non-volatile board settings are managed this way:

- All 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.

Chapter 4 - Advanced Menu



The Advanced Menu provides system-level controls to configure device settings:

- USB Configuration (for Legacy support) - Section 4.1 page 8
- Serial Port Console redirection - Section 4.2 page 10
- S5 RTC Wake Settings - Section 4.3 page 22

Other following submenus are Reserved and Not to be used:

- PCI Subsystem Settings
- ACPI Settings
- Trusted Computing
- CPU Configuration
- ME Configuration
- Thermal Configuration
- Port 80h

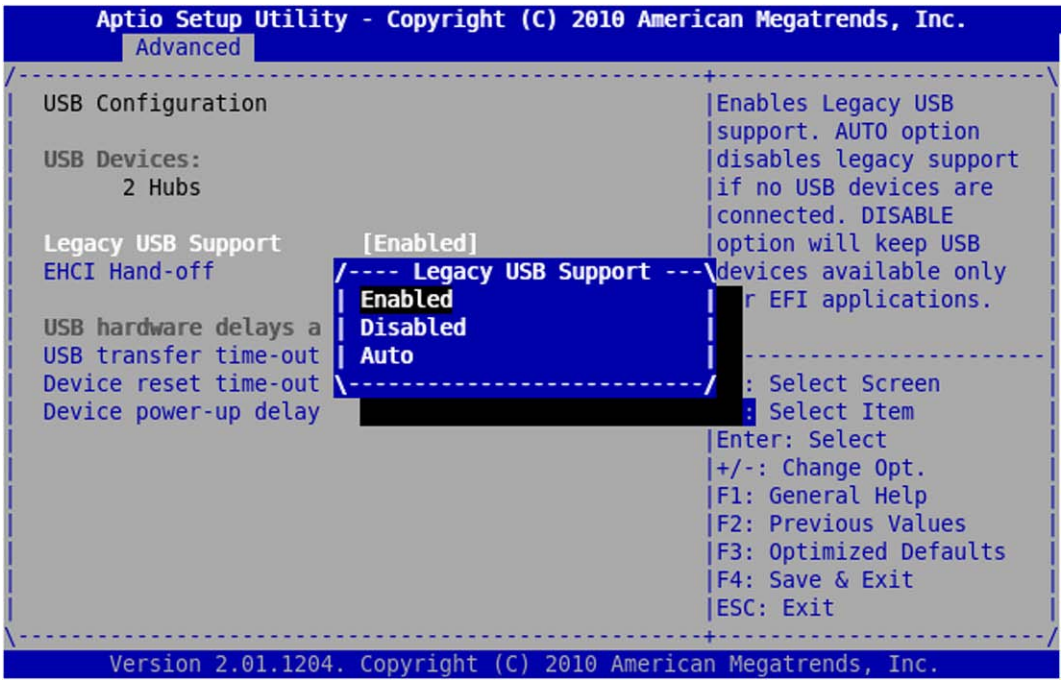
4.1 USB Configuration

This menu can be used to enable/disable the Legacy USB Support (such as DOS legacy environment) . It can be used to avoid booting on an USB device when an USB device is connected. This is the only option that is not reserved in the menu.

Other following options are Reserved and Not to be used:

- EHCI Hand-off
- USB transfer time-out [20 sec]
- Device reset time-out [20 sec]
- Device power-up delay [Auto]

4.1.1 Legacy USB Support



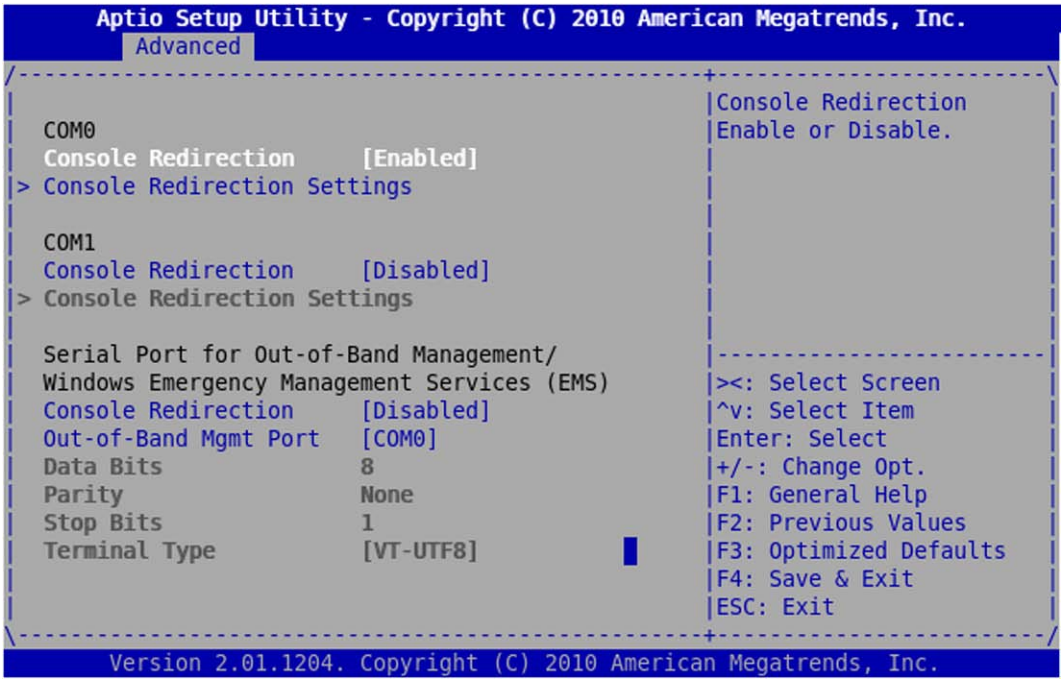
Select menu Legacy USB Support to change it. There are three options to choose from:

- Enabled
- Disabled
- Auto

`AUTO` option disables Legacy Support if no USB device is connected. `Disabled` option will keep USB device available for EFI application.

4.2 Serial Port Console Redirection

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



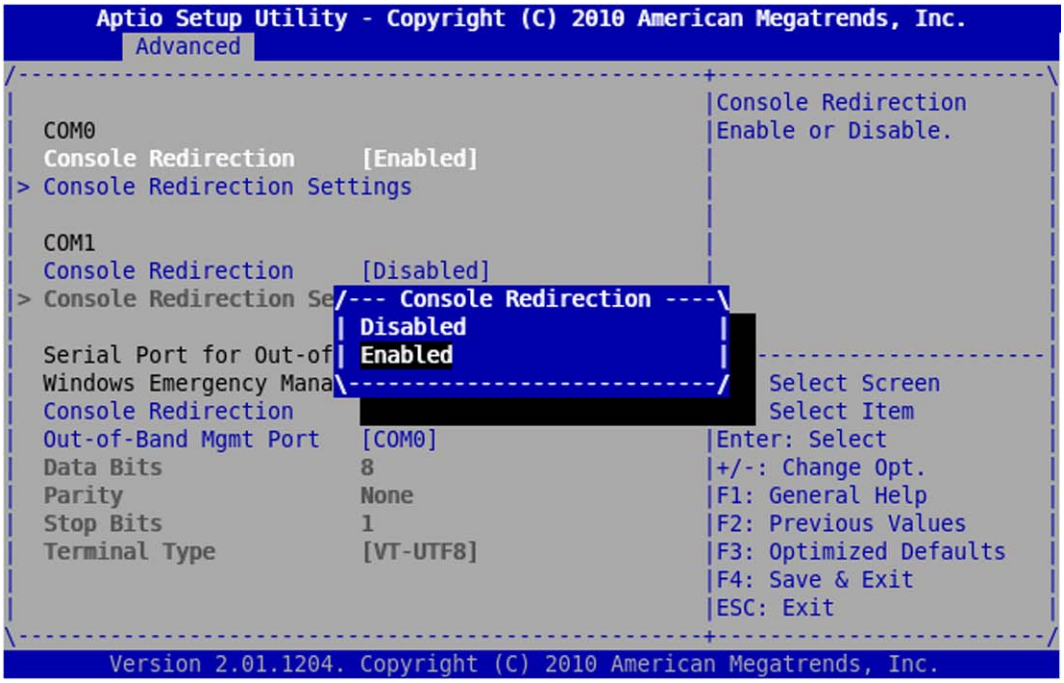
Other following options are Reserved and Not to be Used:

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

COM0/COM1 correspond respectively to the COM1/COM2 hardware serial lines.

4.2.1 COM0/COM1 Console Redirection

The user has the option to enable/disable serial Console Redirection on COM0 or on COM1. To have SETUP display 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.

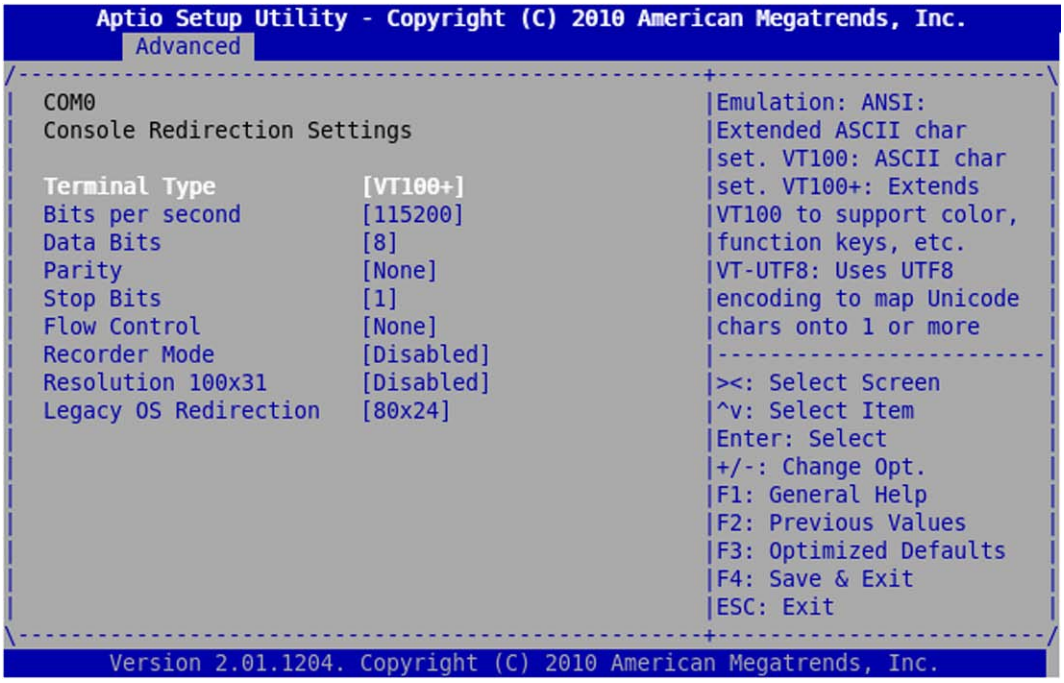


In case the user wants to display the PXE messages on serial COM1 instead of serial COM0, serial COM0 redirection must be disabled because only one serial port is selected by PXE.

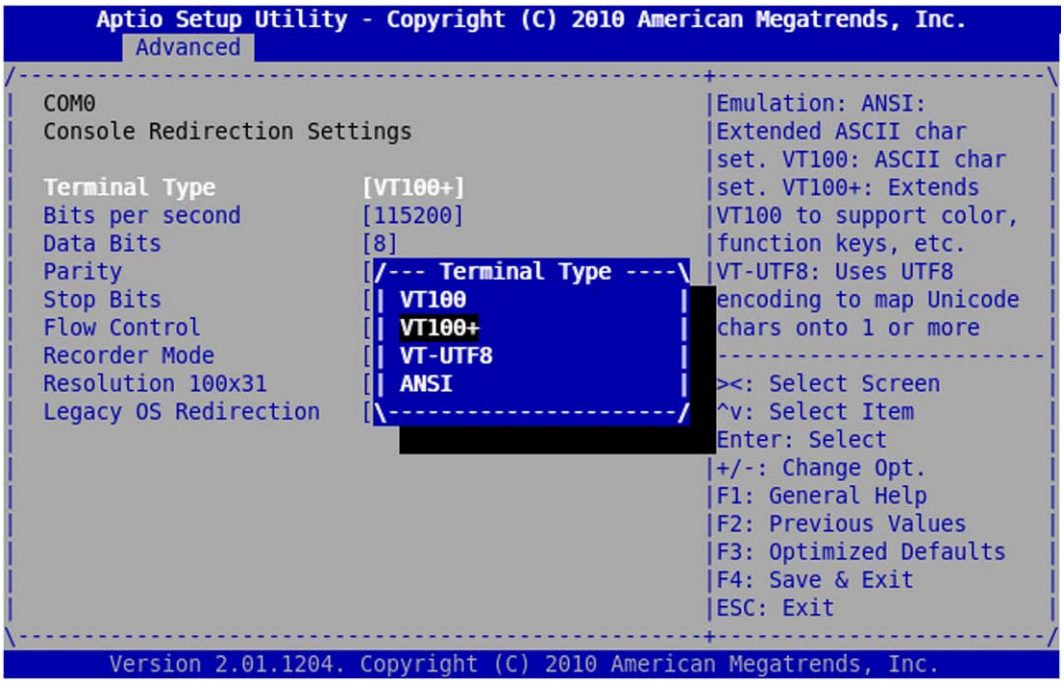
4.2.2 COM0/COM1 Console Redirection Settings

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

- Terminal Type
- Bits per second
- Data Bits
- Parity
- Stop Bits
- Flow Control
- Recorder Mode
- Resolution 100x31
- Legacy OS Redirection



4.2.2.1 Terminal Type

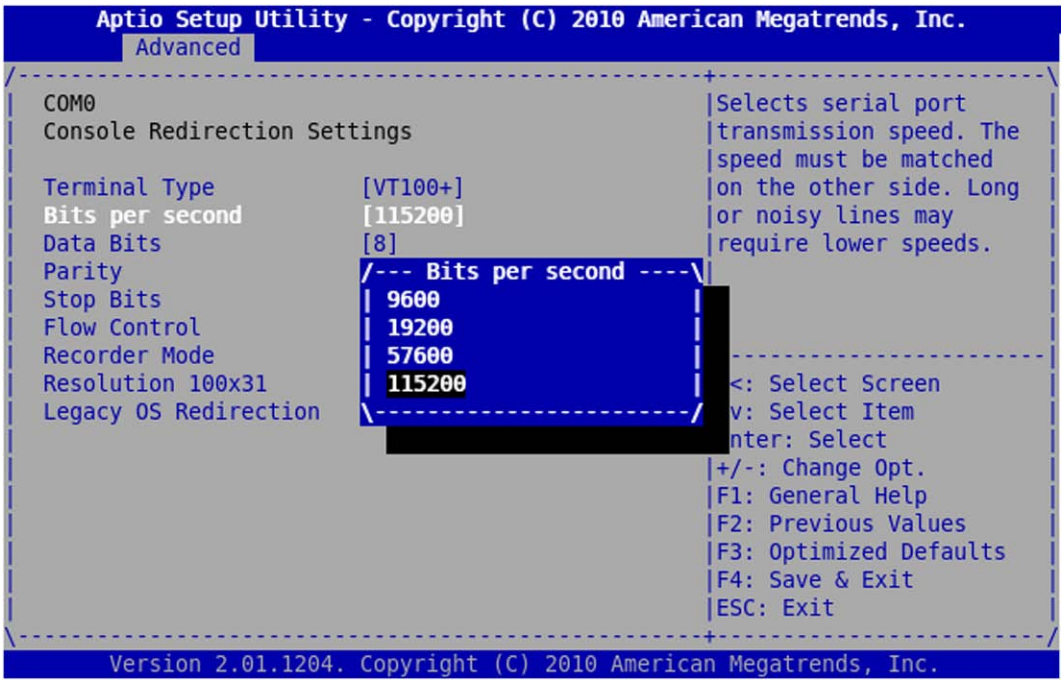


Set Terminal Type:

- VT100
  ASCII Char set
- VT100+
  Extends VT100 to support colours, functions keys
- VT-UTF8
  Uses UTF8 encoding to map Unicode onto 1 or more
- ASCII
  Extended ASCII char set

Default is VT100+

4.2.2.2 Bits per second

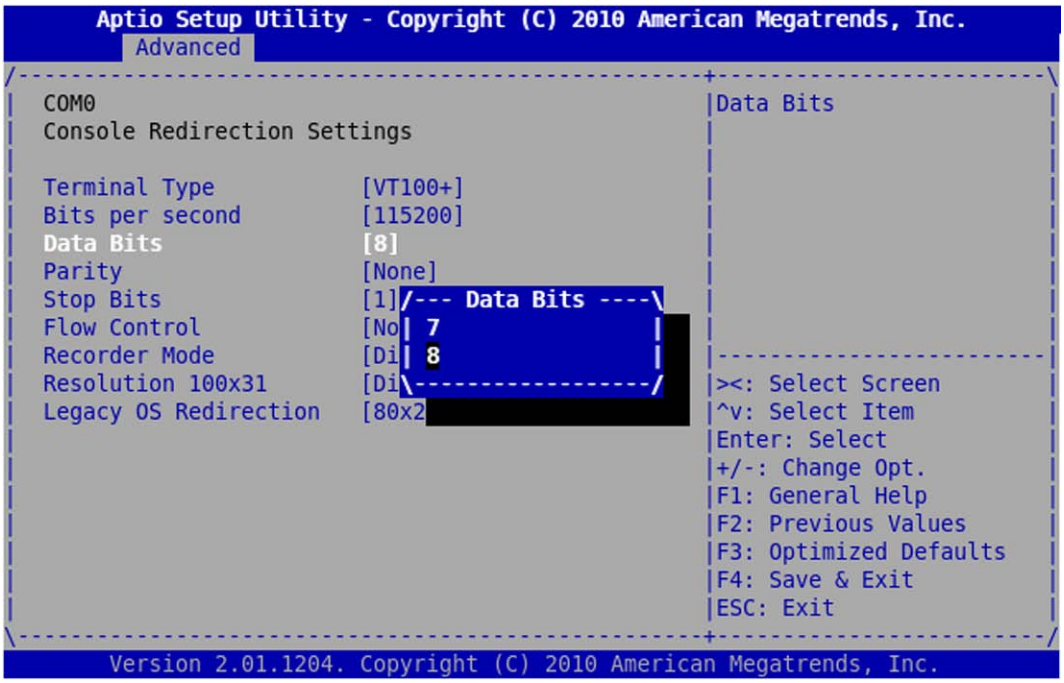


Set bits per second

- 9600
- 19200
- 57600
- 115200

Default and recommended value is 115200 bits per second for serial line baud rate on COM0 and COM1

4.2.2.3 Data Bits

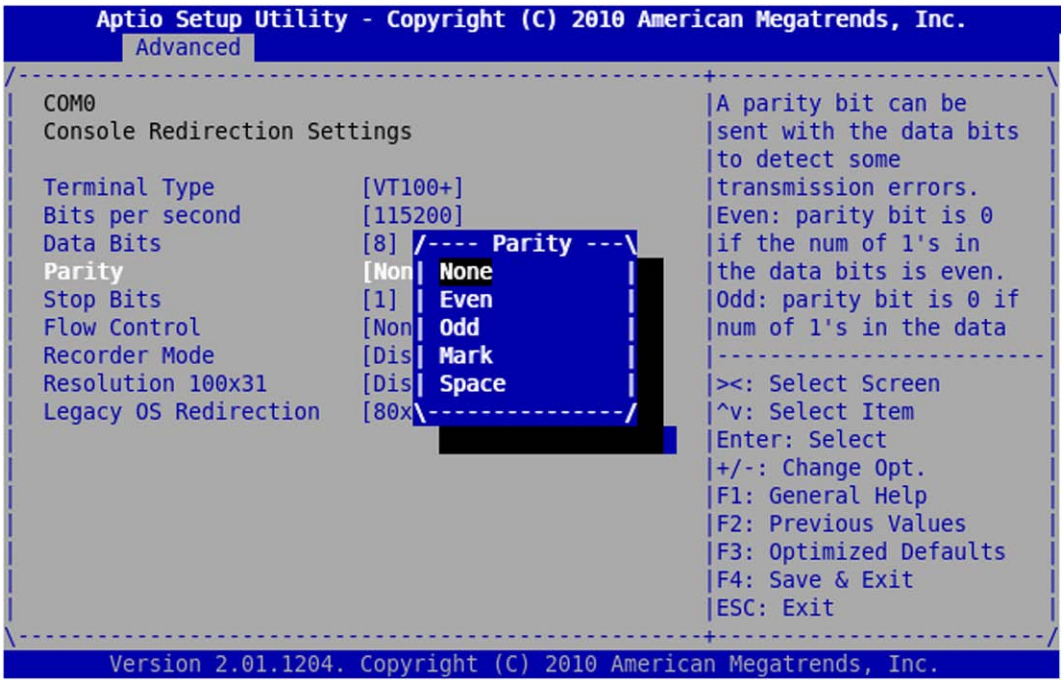


Set Data bit number for serial line COM0 or COM1

- 7
- 8

Default value is 8

4.2.2.4 Parity



Set Parity bit

- None
- Even
- Odd
- Mark
- Space

Default for parity bit is `None`

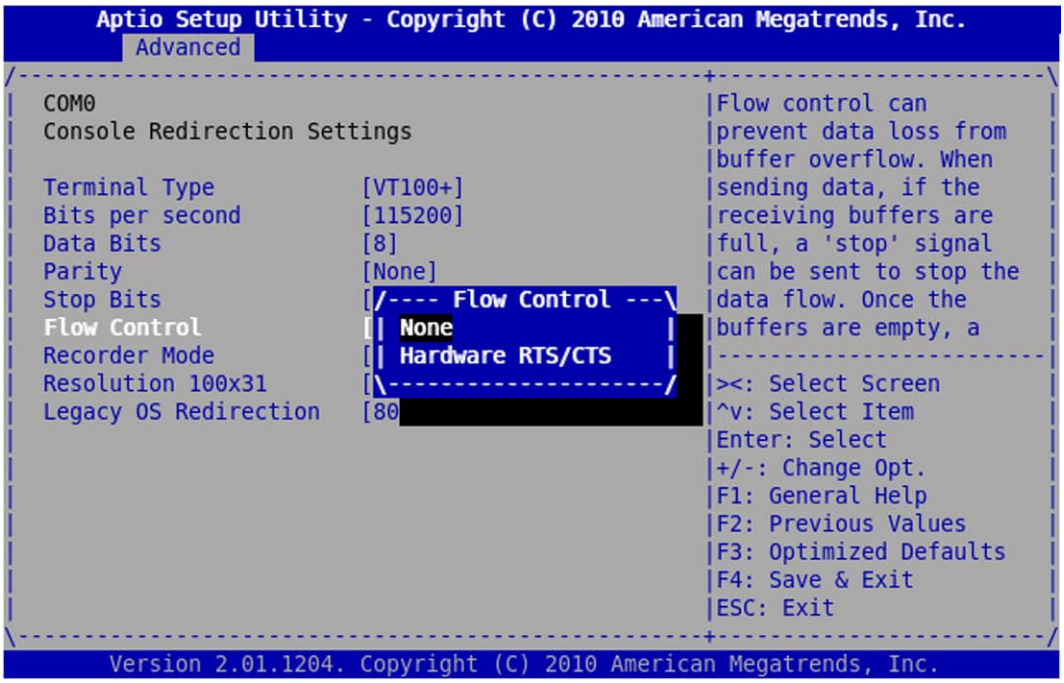
4.2.2.5 Stop Bits

Set Stop bit

- 1
- 2

Default for stop bit is 1

4.2.2.6 Flow Control

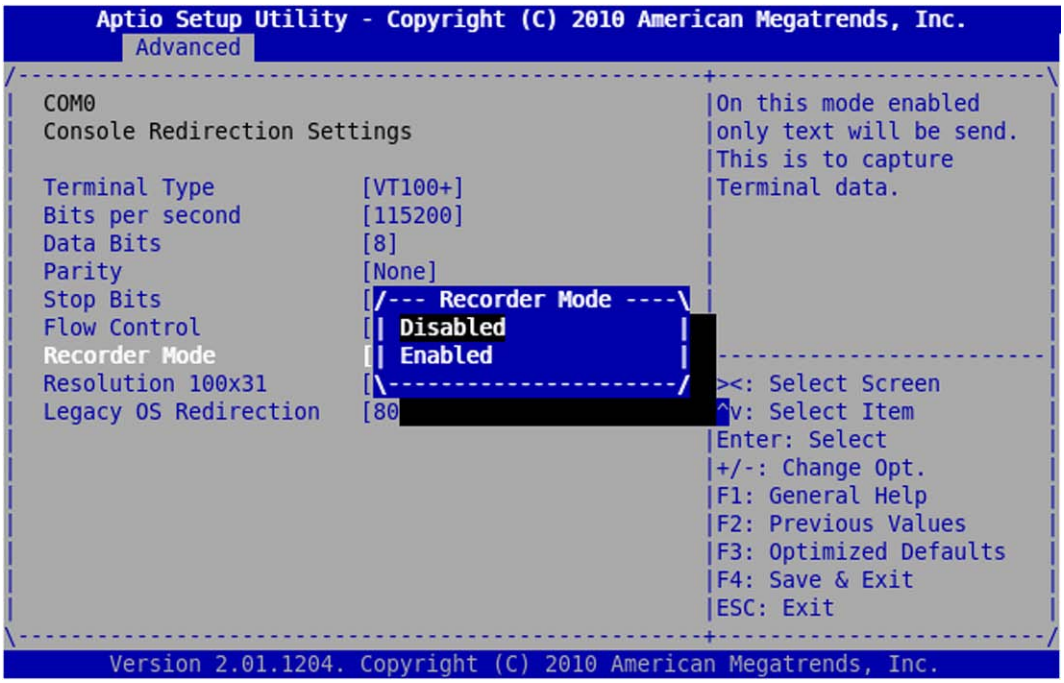


Set Flow Control or modem signals

- None
- Hardware RTS/CTS

Default for Flow Control setting is `None`

4.2.2.7 Recorder Mode



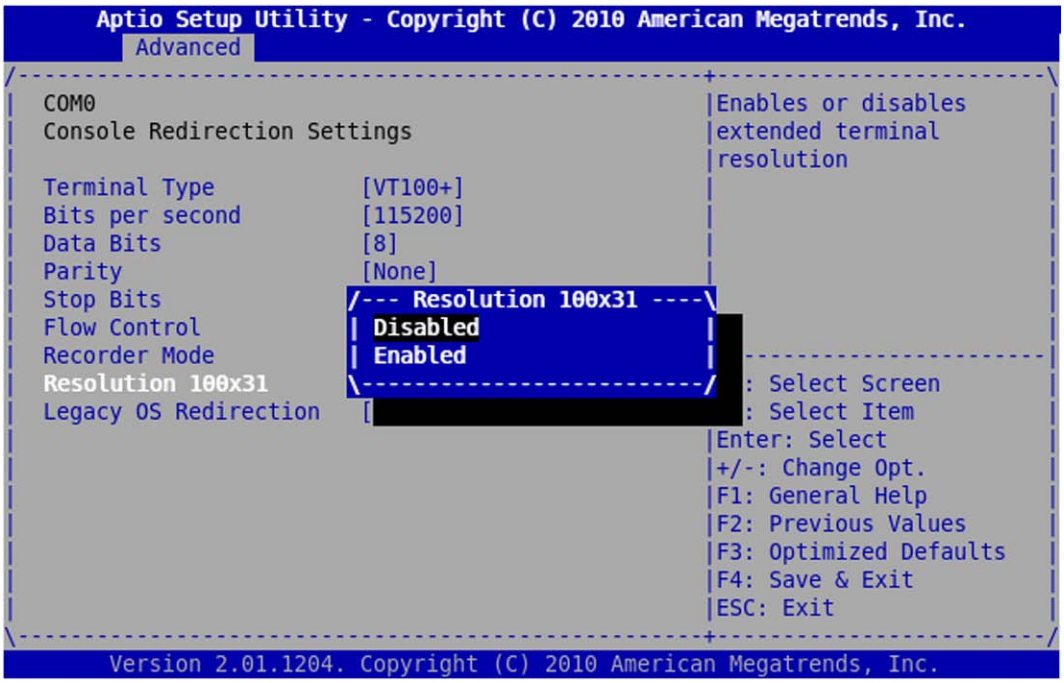
Set Recorder Mode. On this mode only text will be sent on the line. This allows to capture terminal data.

- Disabled
- Enabled

Default is `Disabled`

When this option is enabled it could be tricky to control the SETUP menu from the serial line. In case of difficulty graphical interface could be used to control SETUP menu.

4.2.2.8 Resolution

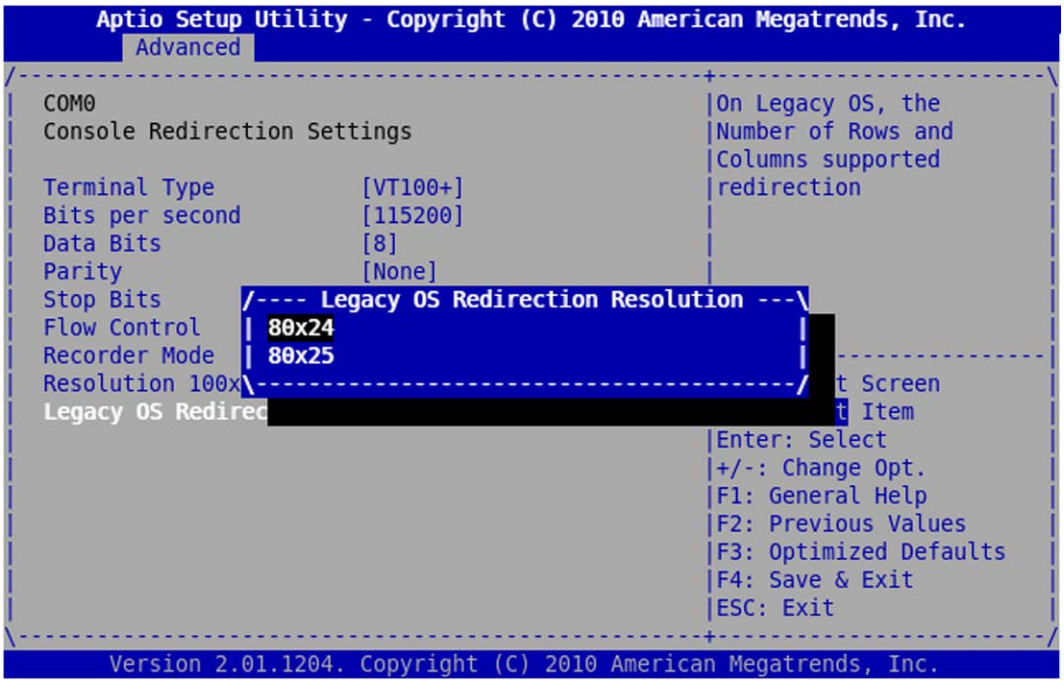


Set Resolution. This enables or disables the extended Terminal Resolution

- Disabled
- Enabled

Default is `Disabled`

4.2.2.9 Legacy OS Redirection



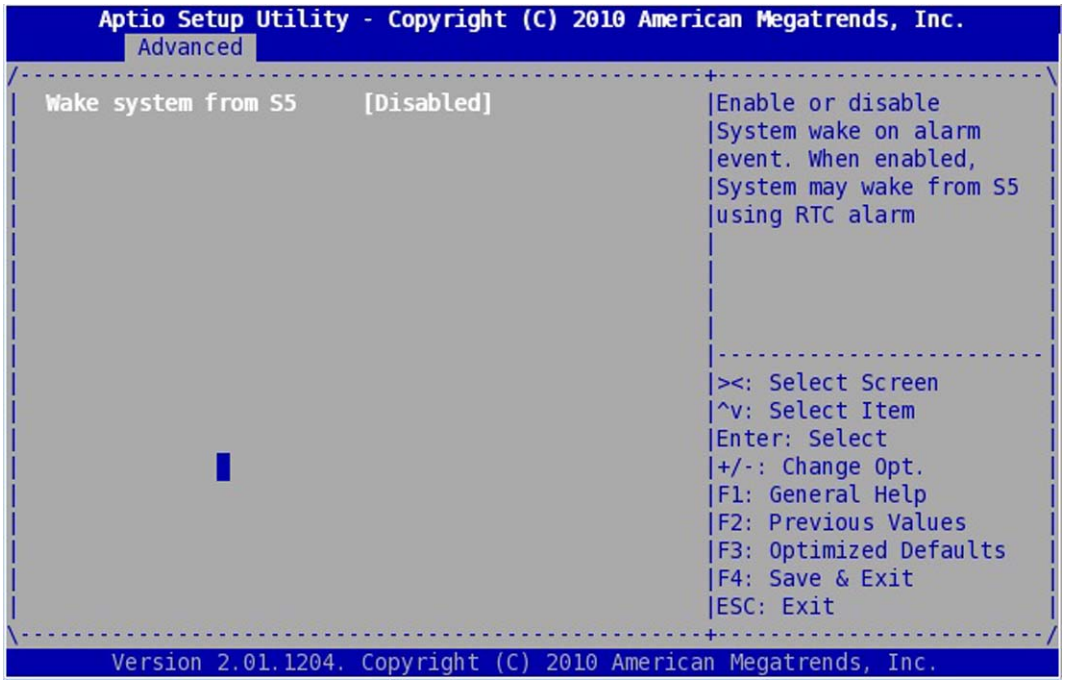
Legacy OS redirections indicates the number of Rows and Columns.

- 80x24
- 80x25

Default is 80x24 for resolution

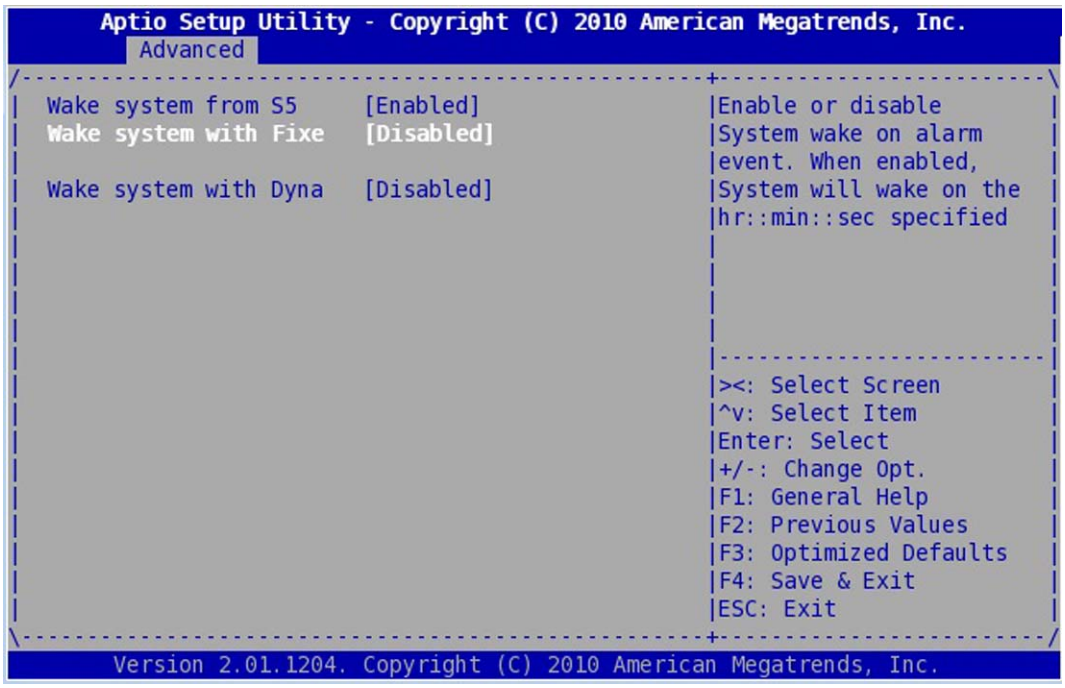
4.3 S5 RTC Wake Settings

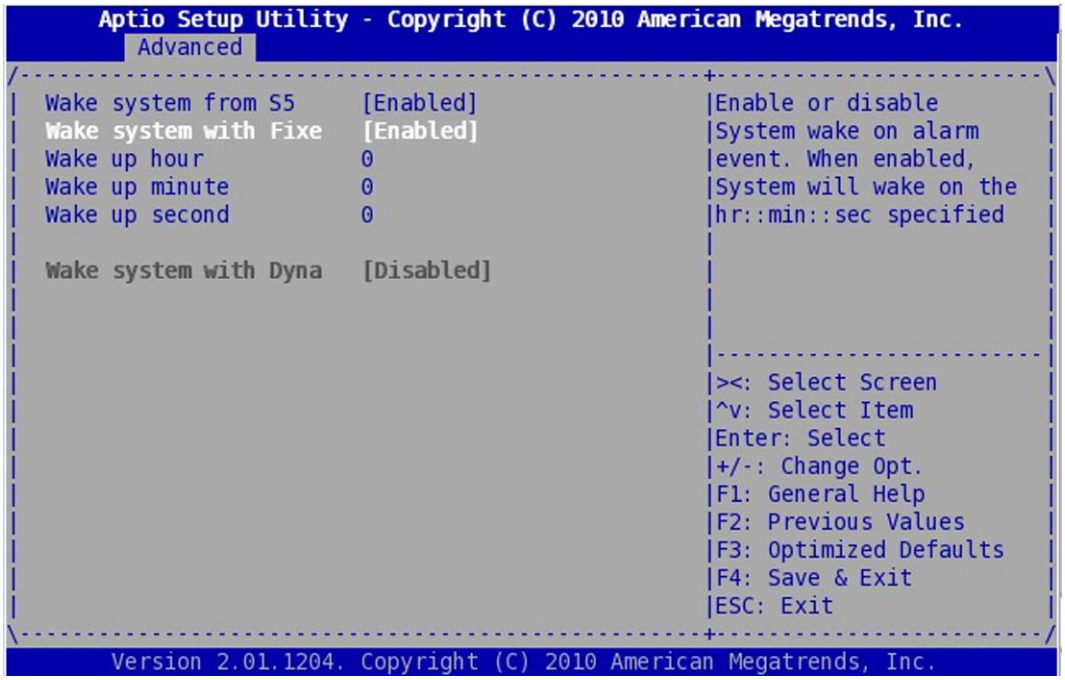
The menu enables or disables (default) the RTC wake-up feature.

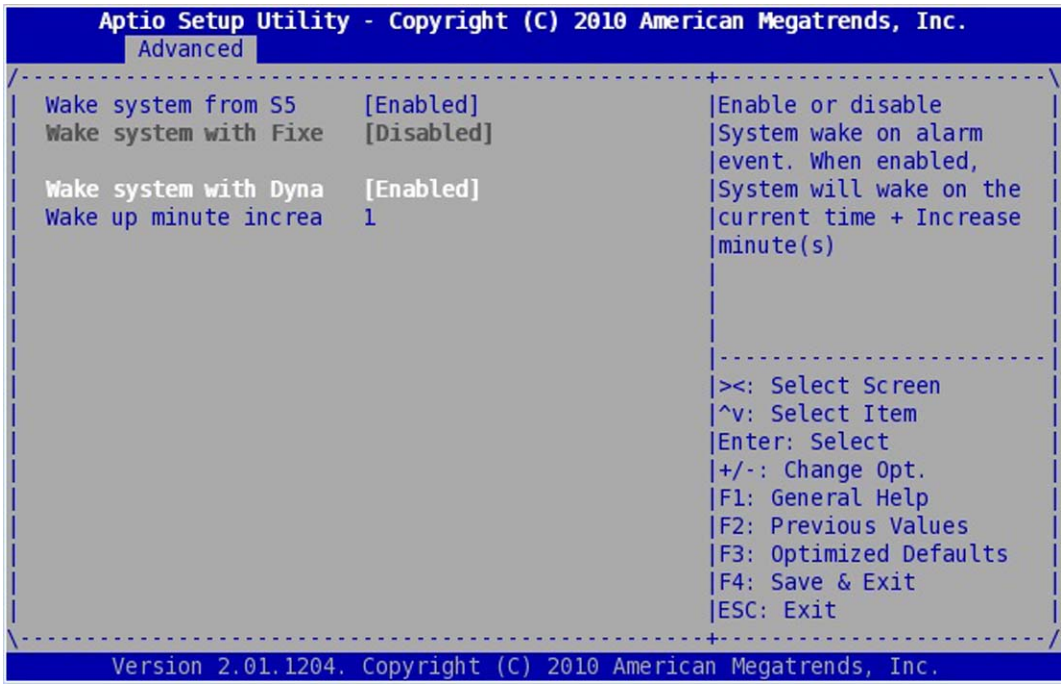


Enabling the feature allows the system to wake up from the S5 state by using the RTC alarm.

Either an absolute time or a relative time can be selected for wake-up:



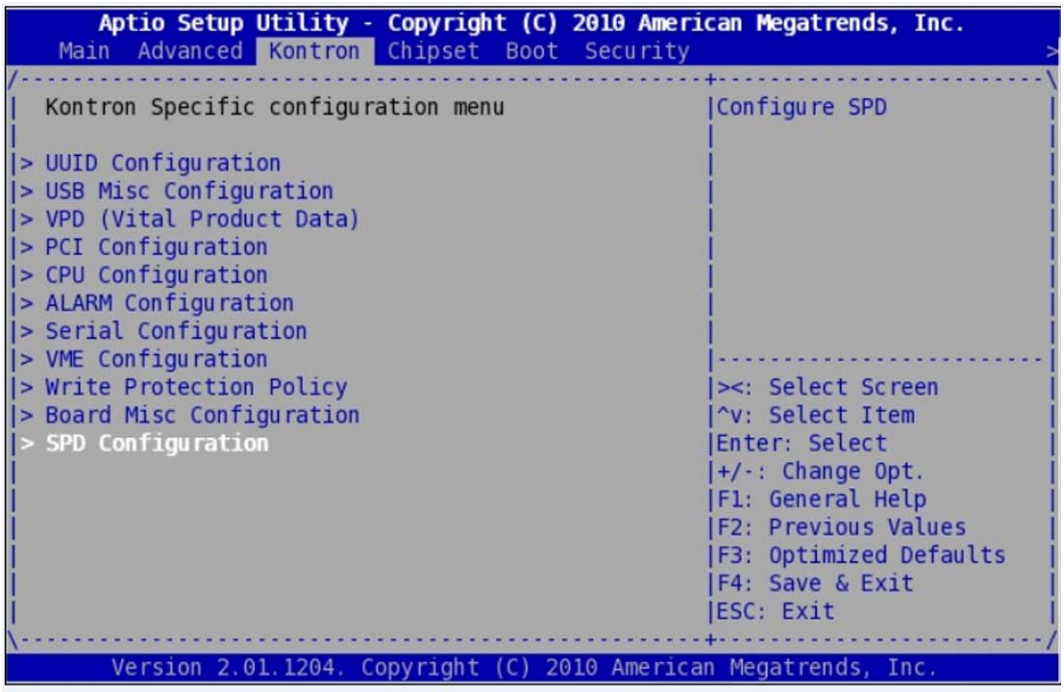

Aptio Setup Utility - Copyright (C) 2010 American Megatrends, Inc.
Advanced
Wake system from S5 [Enabled]
Wake system with Fixe [Enabled]
Wake up hour 0
Wake up minute 0
Wake up second 0
Wake system with Dyna [Disabled]
Enable or disable
System wake on alarm
event. When enabled,
System will wake on the
hr::min::sec specified
><: Select Screen
^v: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.01.1204. Copyright (C) 2010 American Megatrends, Inc.


Aptio Setup Utility - Copyright (C) 2010 American Megatrends, Inc.
Advanced
Wake system from S5 [Enabled]
Wake system with Fixe [Disabled]
Wake system with Dyna [Enabled]
Wake up minute increa 1
Enable or disable
System wake on alarm
event. When enabled,
System will wake on the
current time + Increase
minute(s)
><: Select Screen
^v: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.01.1204. Copyright (C) 2010 American Megatrends, Inc.

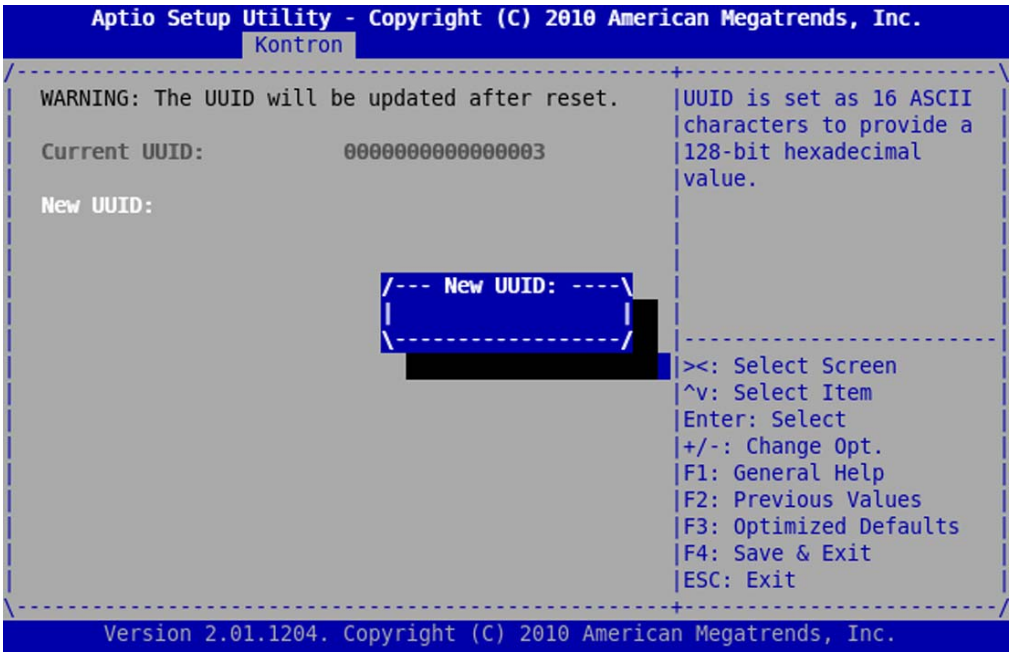
Chapter 5 - Kontron Menu

The Kontron Menu provides system-level controls to configure specific VM6050 hardware design.

The different parameters are described in the following sections:



5.1 UUID Configuration

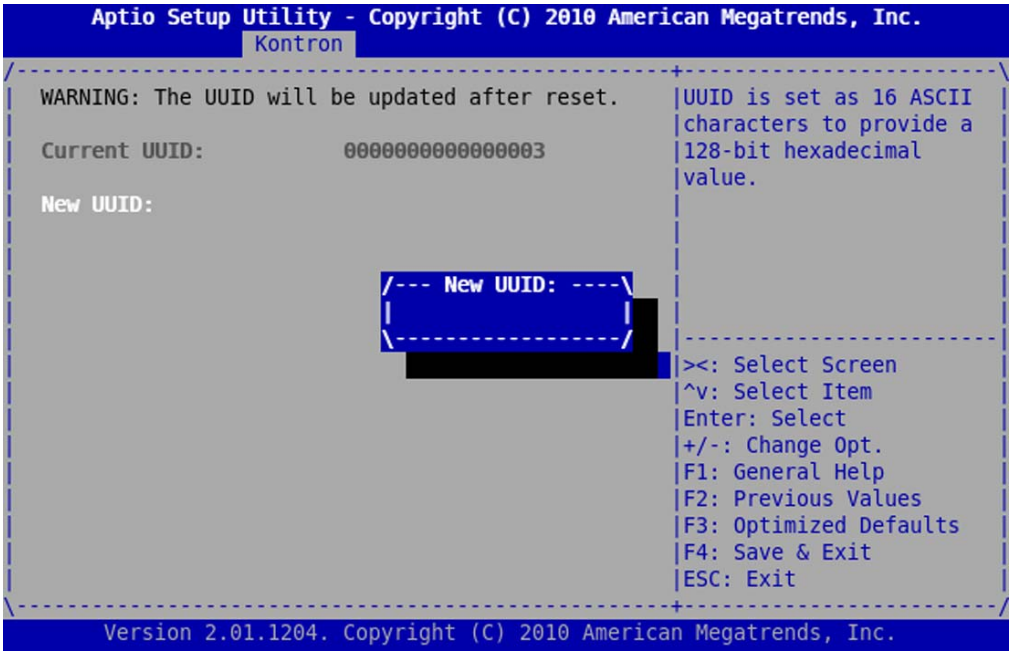


UUID stands for Universally Unique IDentifier also known as GUIDs (Globally Unique IDentifier). A UUID is 128 bits long, and can guarantee uniqueness across space and time. Please refer to RFC4122 documentation for more details about UUID.

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 to user to modify the default value of the UUID (see picture above).

Once the UUID is modified, it must be equal to exactly sixteen ASCII characters.
If not, an Error pop-up message appears on the screen (see picture below).
To cancel entering of a new UUID, type ESC key then enter key to close the pop-up message.



5.2 USB Misc Configuration

The following option is displayed :

Set the USB Keyboard Layout:

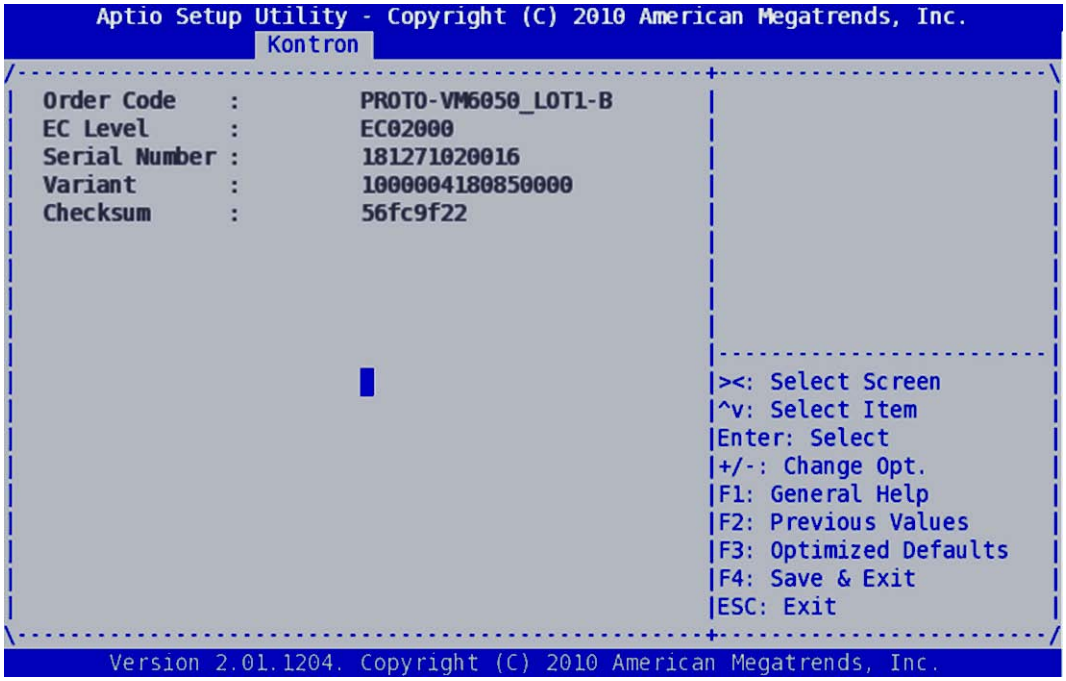
- US Keyboard
- FR Keyboard

Default is `US Keyboard`.

This option allows to set the type of USB keyboard used, Qwerty or Azerty.

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

5.3 VPD – VITAL PRODUCT DATA

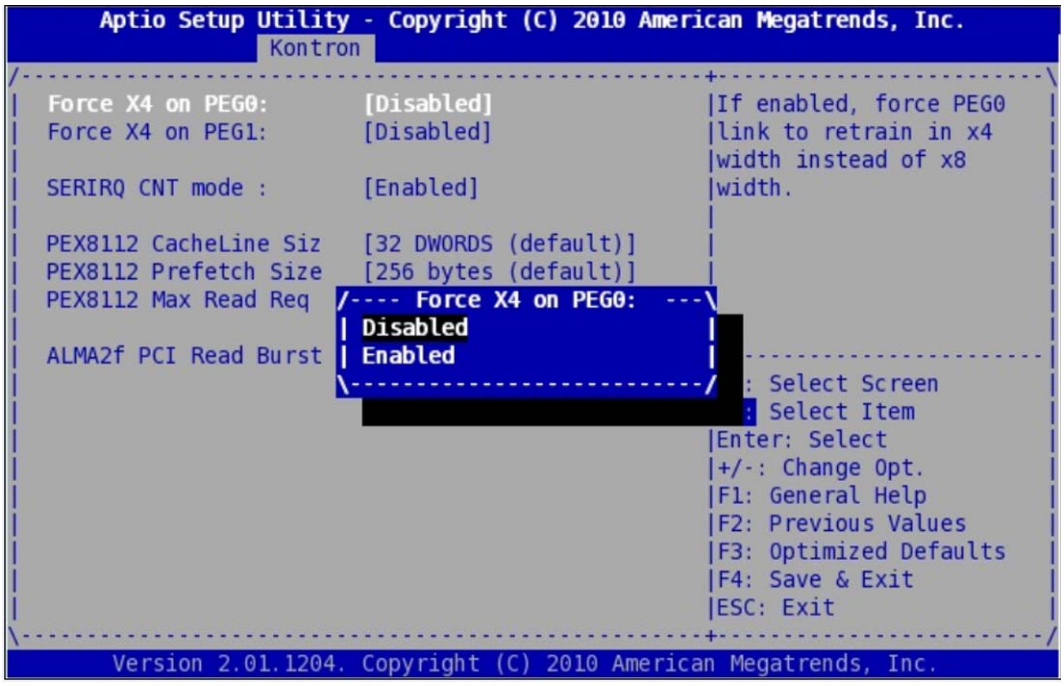


This menu only displays the Vital Product Data (VPD) information for VM6050. VPD are stored in VM6050 EEPROM.

- 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

5.4 PCI Configuration

5.4.1 PCI Express PEG0/PEG1 Links Configuration



Force x4 on PEG0/PEG1

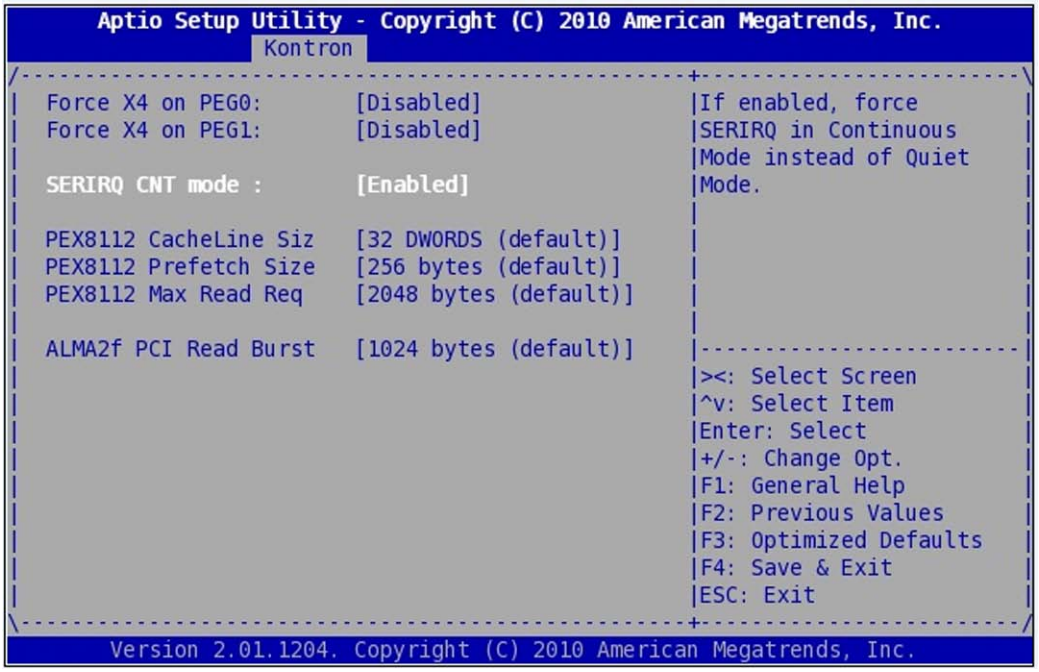
- Disabled
- Enabled

Default is `Disabled`

These settings allow to force the PCI Express links to XMC busses to x4. By default (disabled) these links are x8. This option can be used to support specific XMC device.

To take into account this feature, user should have to set this setting before using the XMC and should have to save changes before exiting Setup; then, plug the XMC device and power-up the board with the XMC and the correct setting.

5.4.2 LPC Serial IRQ Configuration



The serial IRQ protocol has two modes of operation which affect the start frame of the LPC interface in the PCH.

These two modes are:

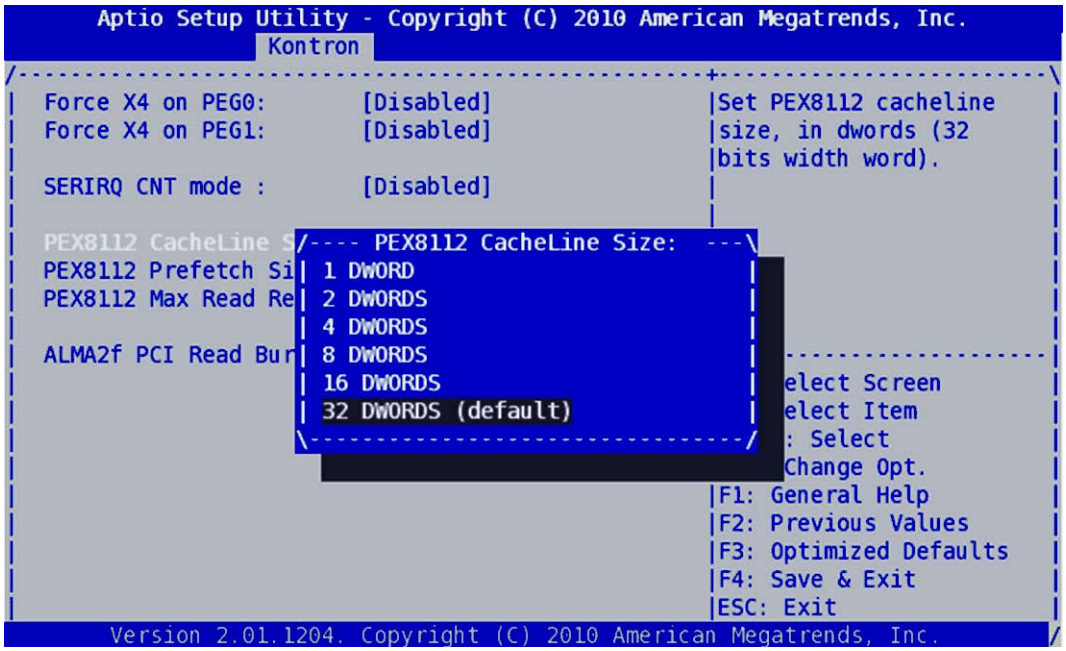
- Continuous, where the PCH is solely responsible for generating the start frame; and
- Quiet, where a serial IRQ peripheral is responsible for beginning the start frame.

The Continuous `Mode` is the `default` mode set by BIOS. It allows faster operations while `Quiet Mode` allows less power consumption.

5.4.3 PCIe-PCI Brigde PEX8112 Configuration

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

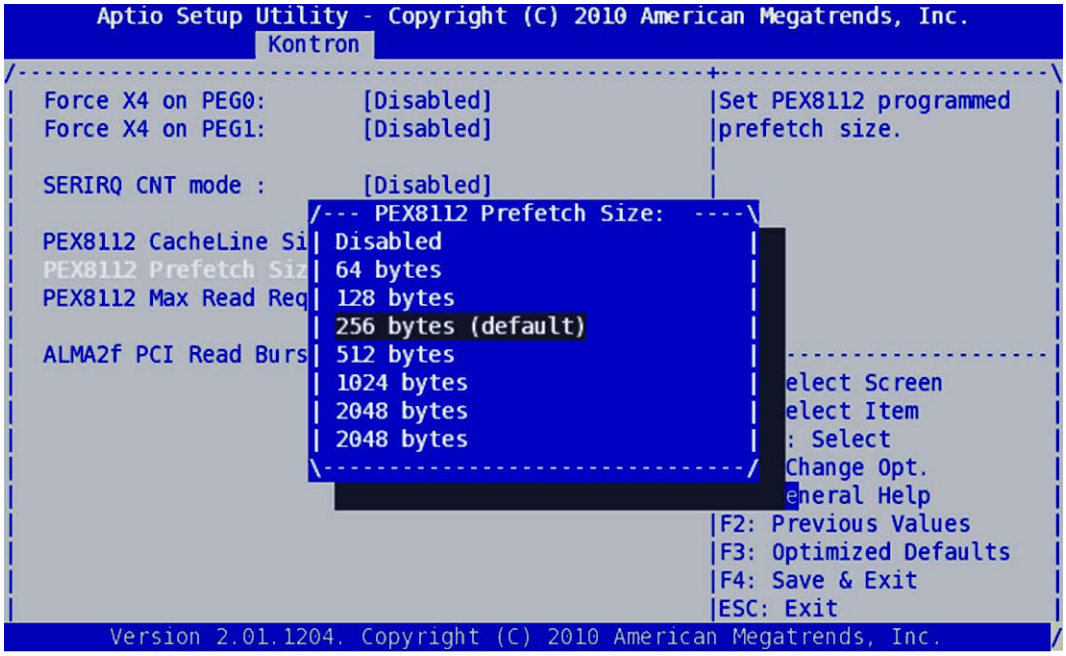
  Default is set to `32 DWORDS`.



- 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.

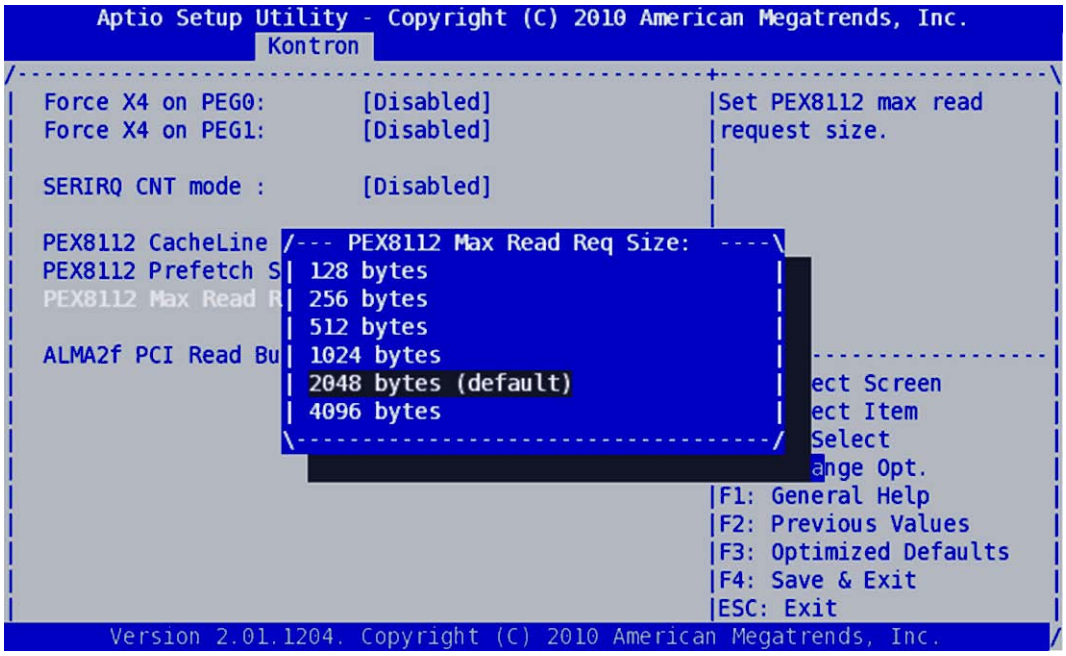
  Default value is set to `256 bytes`.



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

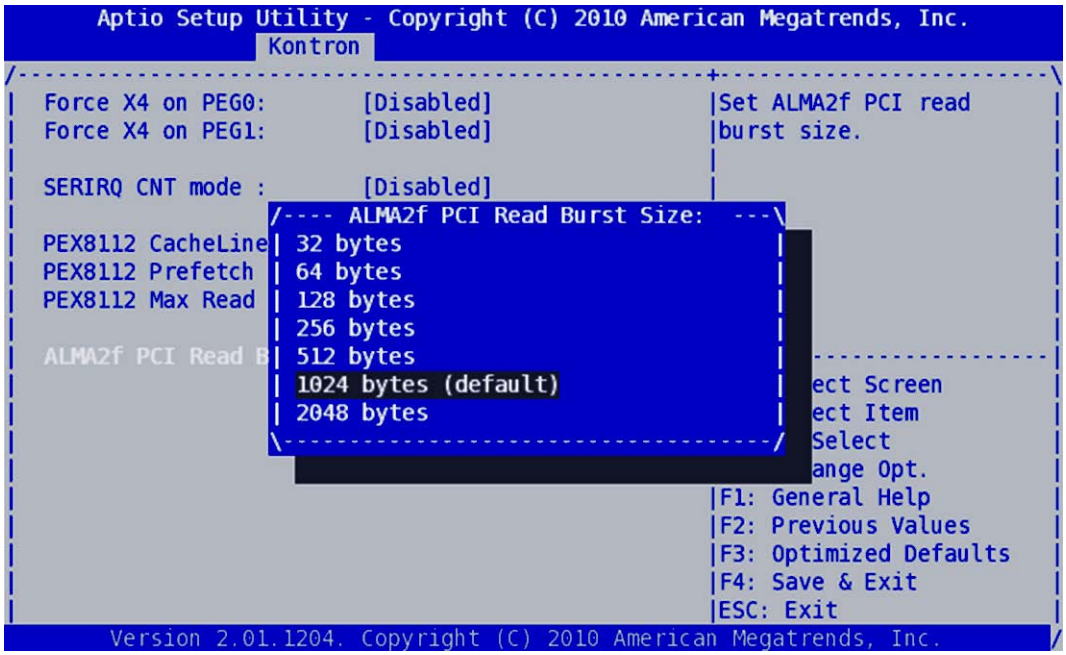
  It sets the Maximum Read Request Size for the Device as a Requester. The PEX 8112 must not generate Read requests with a size that exceeds the set value.

  Default value is set to `2048 bytes`.

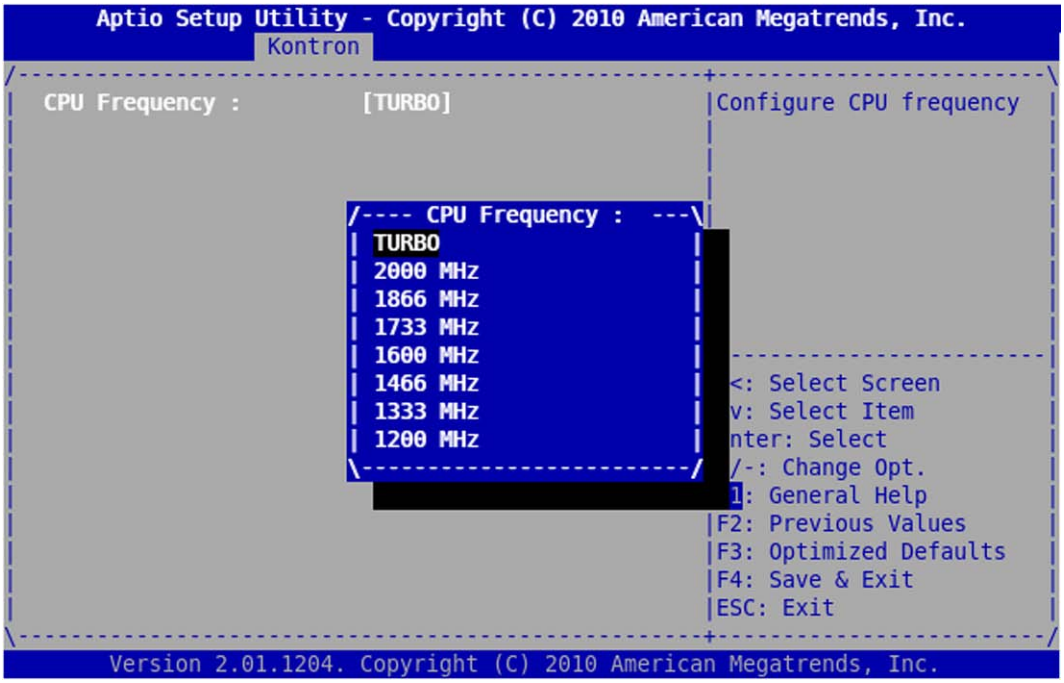


5.4.4 PCI-VME Bridge ALMA2f Configuration

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



5.5 CPU Configuration

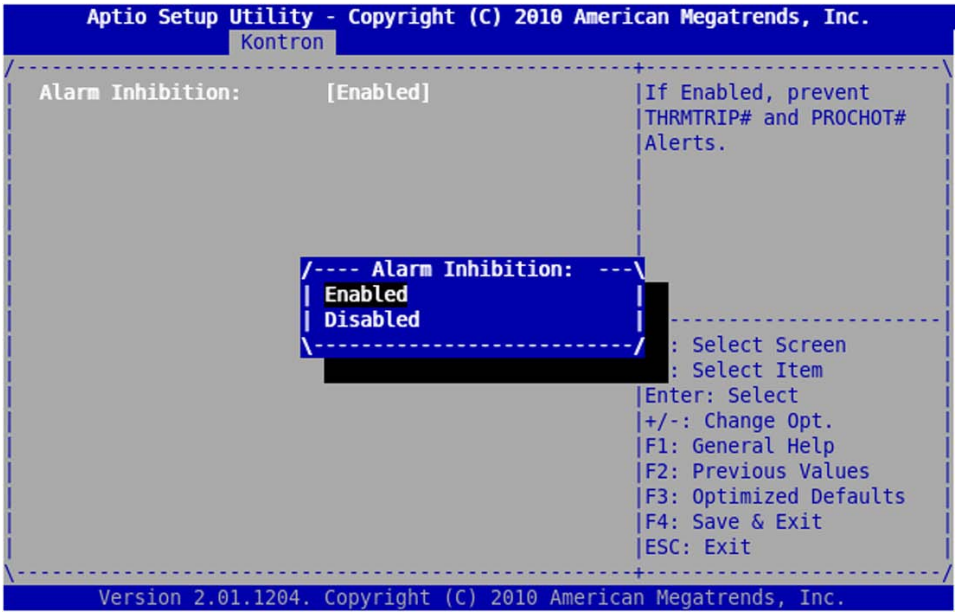


Set the CPU configuration. This option allows to configure the CPU frequency mode. The TURBO mode allows the CPU to boost its frequency between 2 and 3 GHz according to the CPU load and temperature. Other modes will force the CPU frequency to the indicated value, if TURBO mode is disabled in the Advanced / CPU Configuration / Power & Performance / Menu

- TURBO
- 2000 MHz
- 1866 MHz
- 1733 MHz
- 1600 MHz
- 1466 MHz
- 1333 MHz
- 1200 MHz

Default is 2000 MHz

5.6 ALARM Configuration

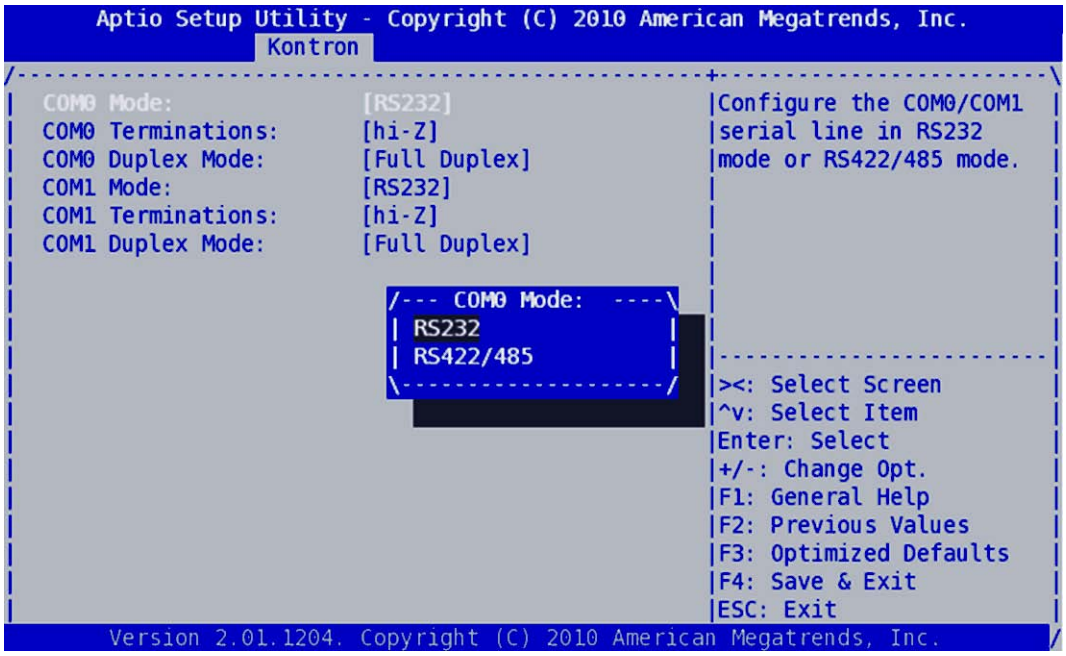


This menu allows user to prevent cPLD logic to turn off automatically the system in case of assertion of THRMTRIP# or PROCHOT# alerts.

It is strongly recommended not to disable this parameter for normal use. This parameter must be used with caution.

5.7 Serial Configuration

5.7.1 COM0/COM1 Mode

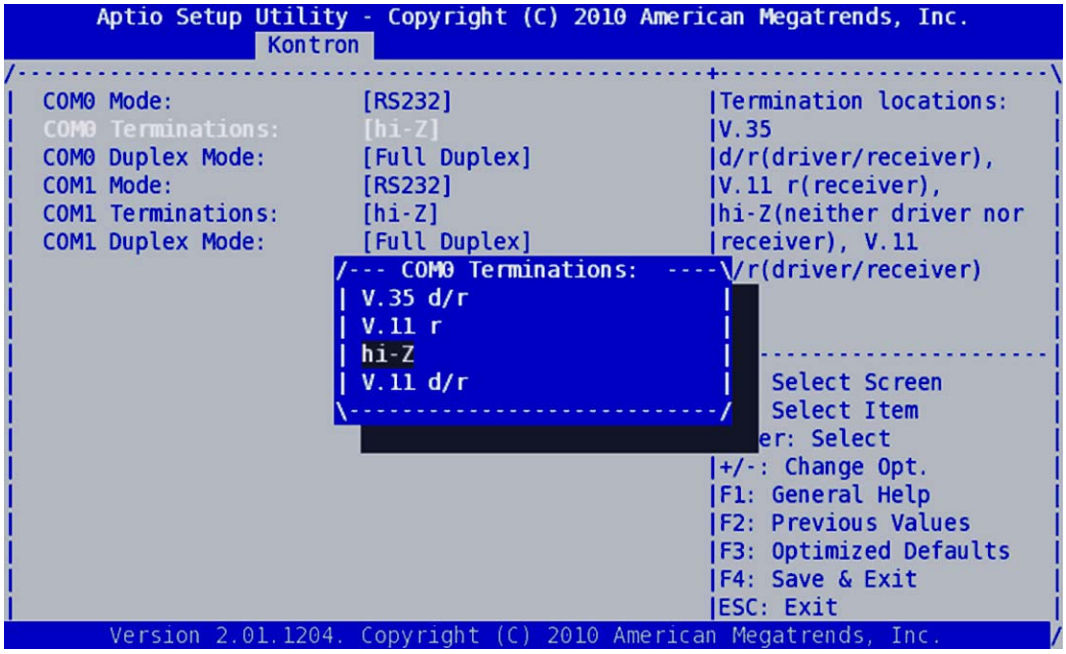


This menu allows user to select the mode for the COM0 serial port: the supported mode are EIA-232 and EIA-422/485.

User must turn off the system to have the new Serial configuration taken into account.

COM0/COM1 corresponds to the hardware COM1/COM2 lines

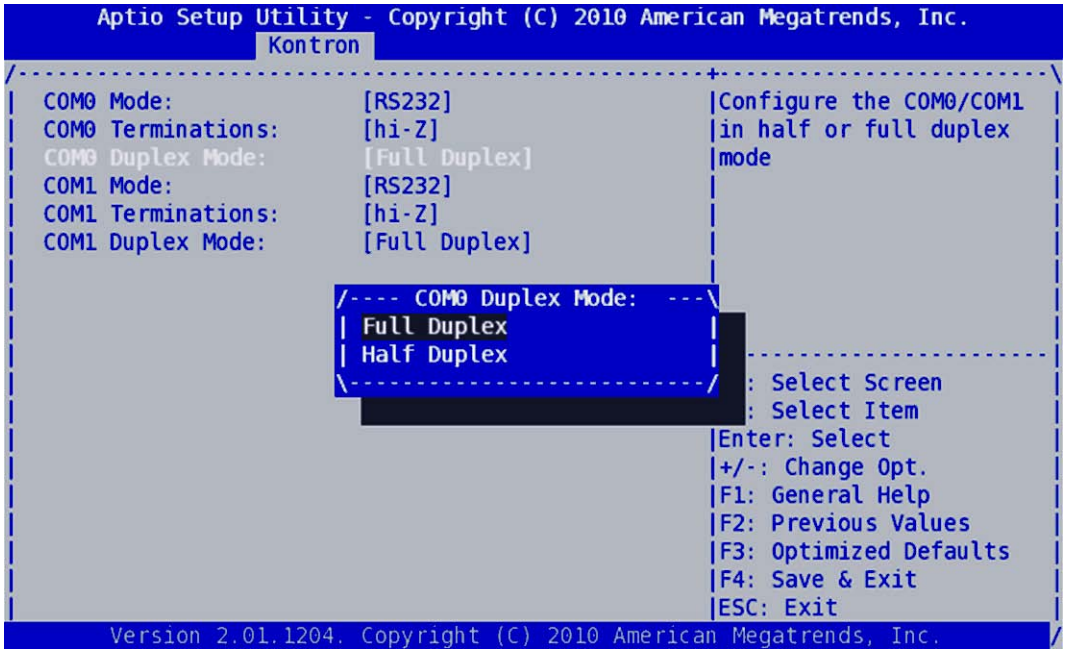
5.7.2 COM0/COM1 Terminations



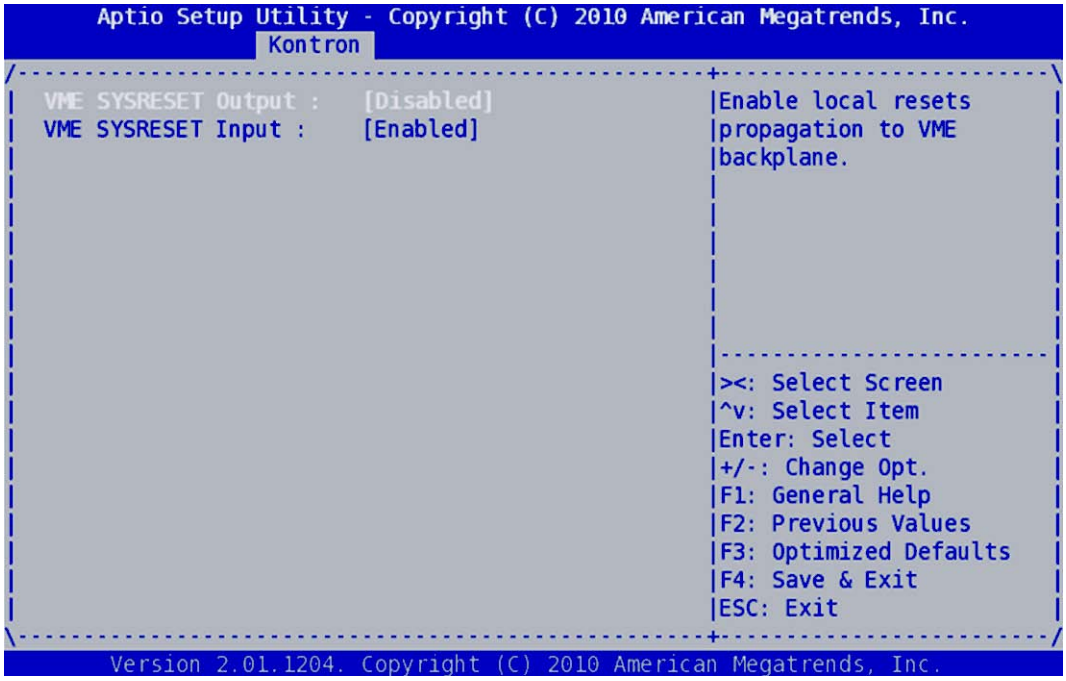
This allows the user to select the terminations according to the selected mode:

- V.35 d/r: serial terminators used when the serial line is operating in EIA-485 mode with both driver and receiver terminated.
- V.11 r: serial terminators used when the serial line is operating in EIA-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-485 mode with both driver and receiver terminated but no communication cable attached.

5.7.3 COM0/COM1 Duplex Mode



5.8 VME Configuration

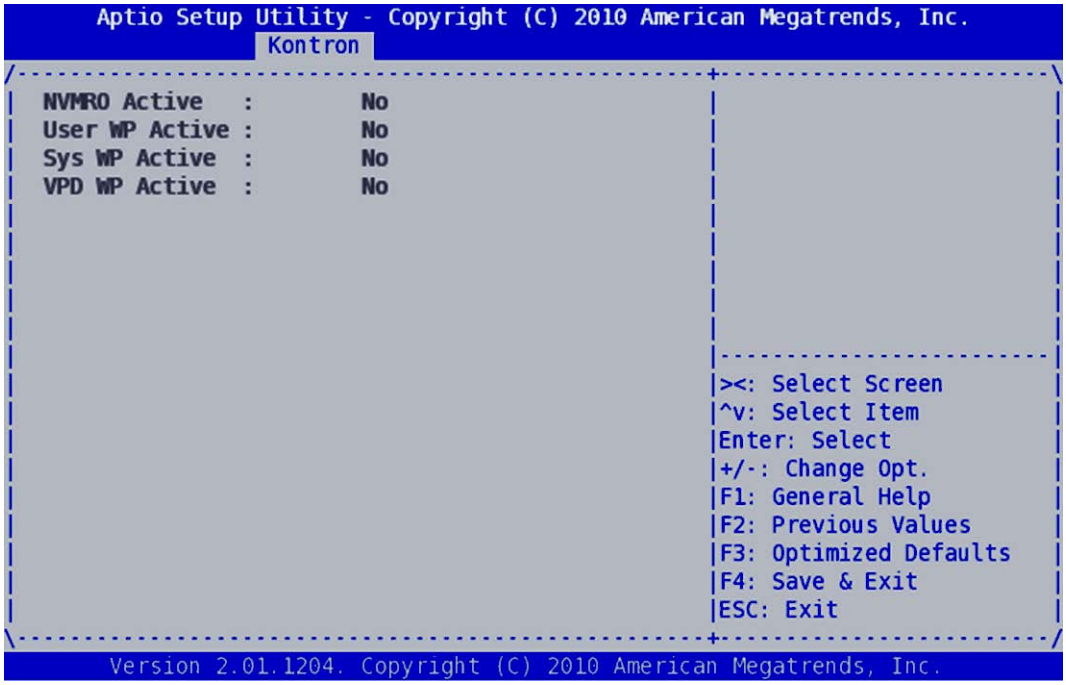


This menu defines the VME SYSRESET# propagation policy in input and in output.

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 SW1.

5.10 Board Misc Configuration

The following options are displayed to manage miscellaneous options of the board:

This menu is used to select the graphic ports D and B modes:

- Display Port,
- HDMI Port

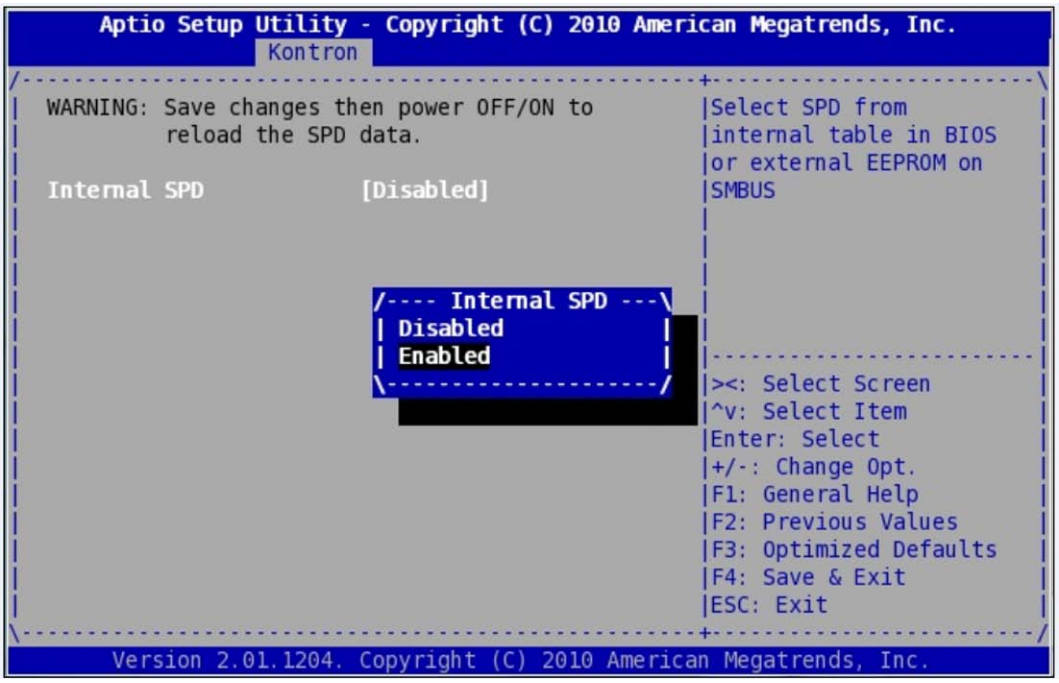
The WatchDog option allows to disable (default setting) or enable the CPLD Watchdog Timer and to define the timeout value.

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

Only the Reset mode is handled.

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

5.11 SPD Configuration

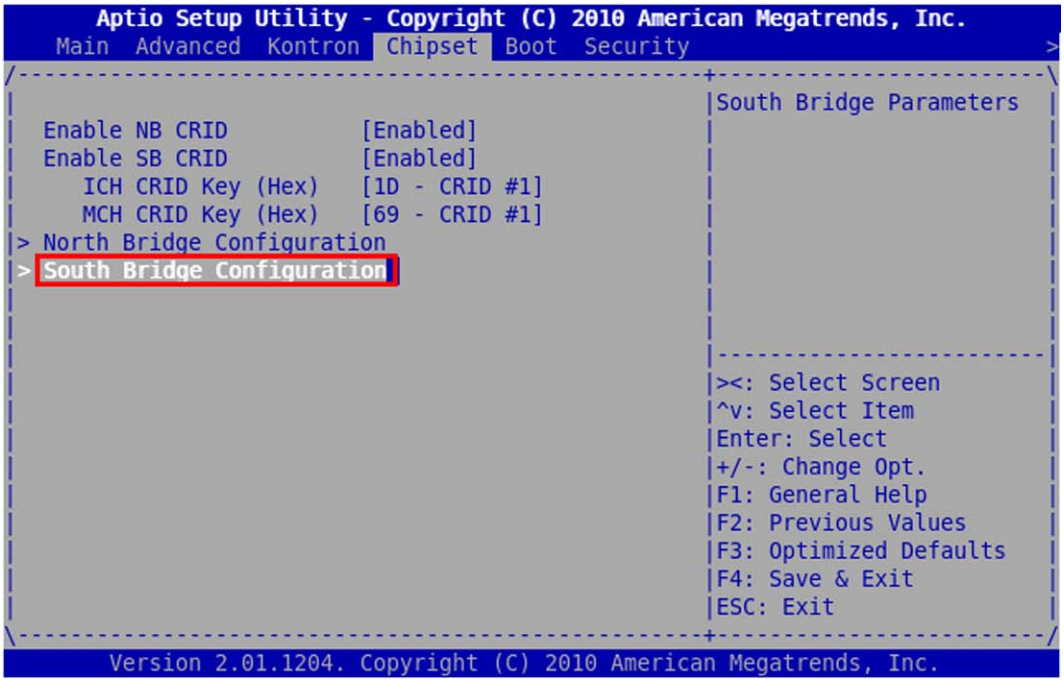


The SPD Configuration menu allows to select either the SPD data from BIOS internal tables or from the SPD EEPROMs accessible thru the PCH SMBus (default setting).

The BIOS internal tables are based on an hardware configuration and on the VPD (Vital Product Data).

This feature allows to bypass SMBus access on PCH in order to speed up and secure the boot process in case of reset during I2C EEPROM access.

Chapter 6 - Chipset Menu



The Chipset Menu provides system-level controls to configure the chipset device settings.

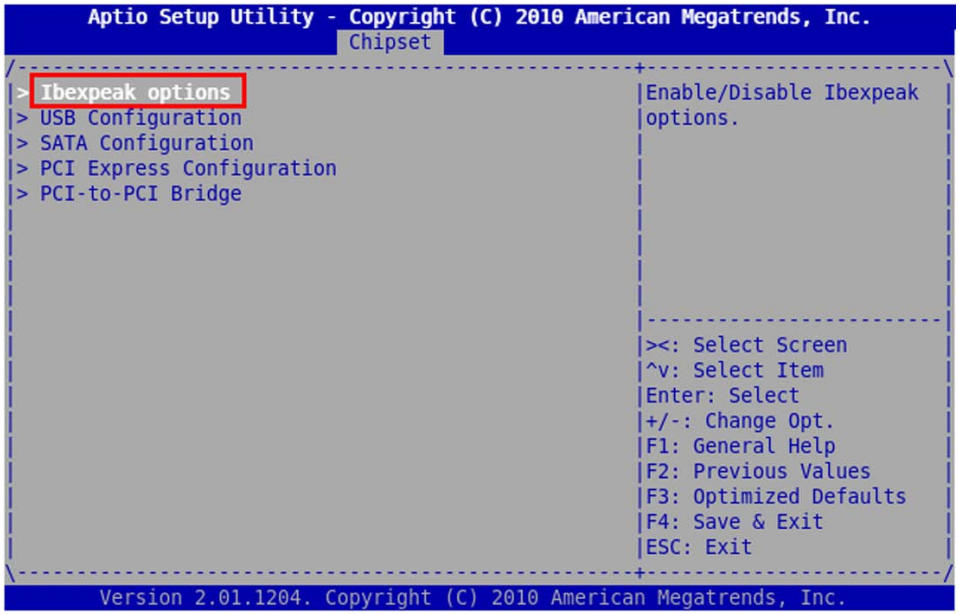
In particular the South Bridge Configuration menu will be used to enable the Pre-boot Execution Environment (PXE) ROM and also to manage the SATA Configuration.

Other following submenus are Reserved and Not to be used !

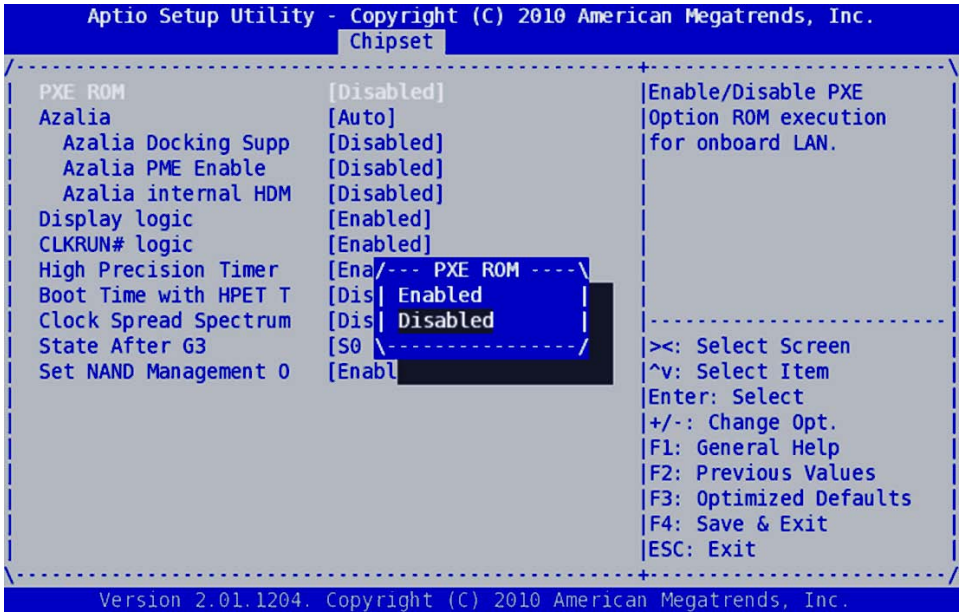
- Enable CRID
- North Bridge Configuration

6.1 South Bridge & PXE ROM configuration

To reach PXE ROM setting, select `South Bridge Configuration` setting in `Chipset` menu then select `Ibexpeak Options`.



Then select `PXE ROM`. This option allows to enable/disable the PXE ROM. Other settings are reserved and not to be used.



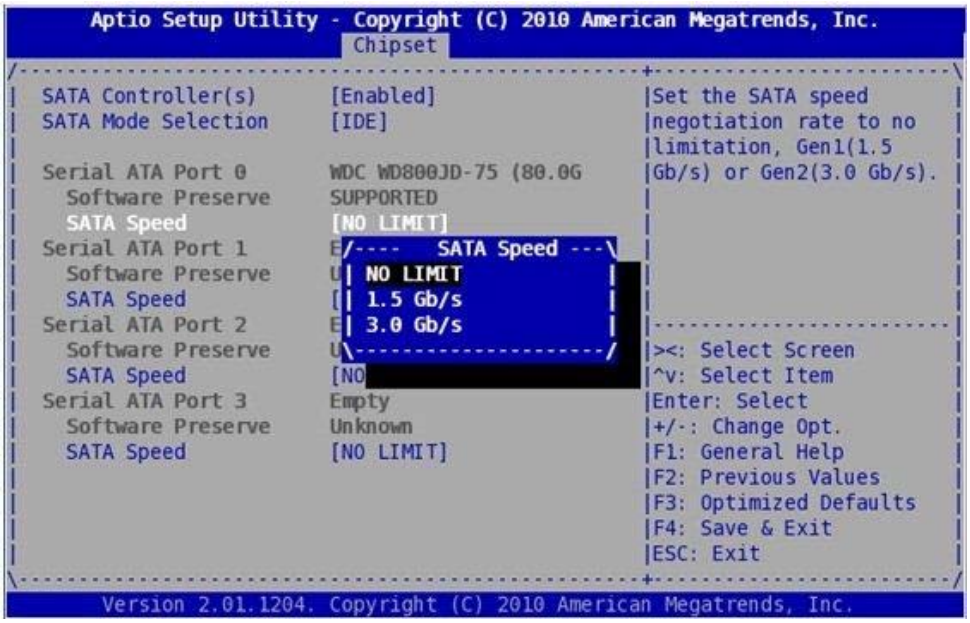
Set PXE ROM

- Disabled
- Enabled

Default is `Disabled`

6.2 South Bridge & SATA Configuration

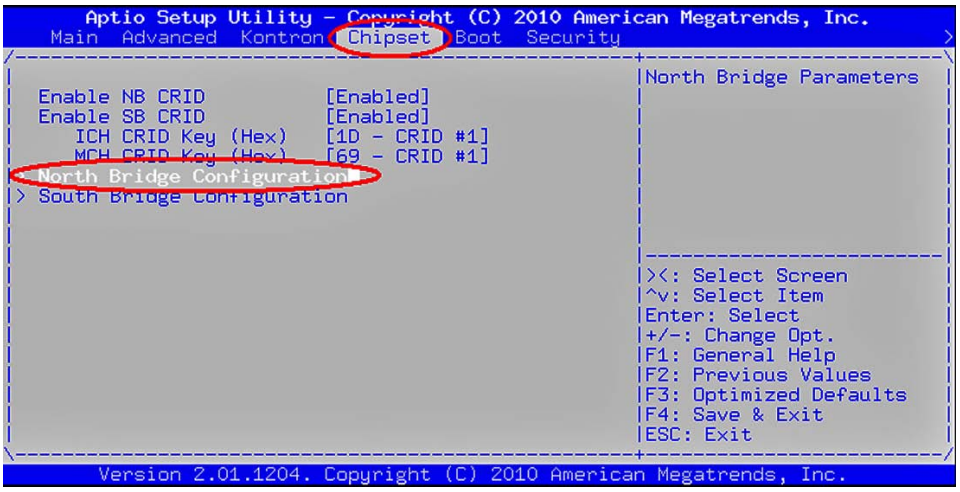
To manage the SATA configuration select the sub-menus South Bridge Configuration and then SATA Configuration.

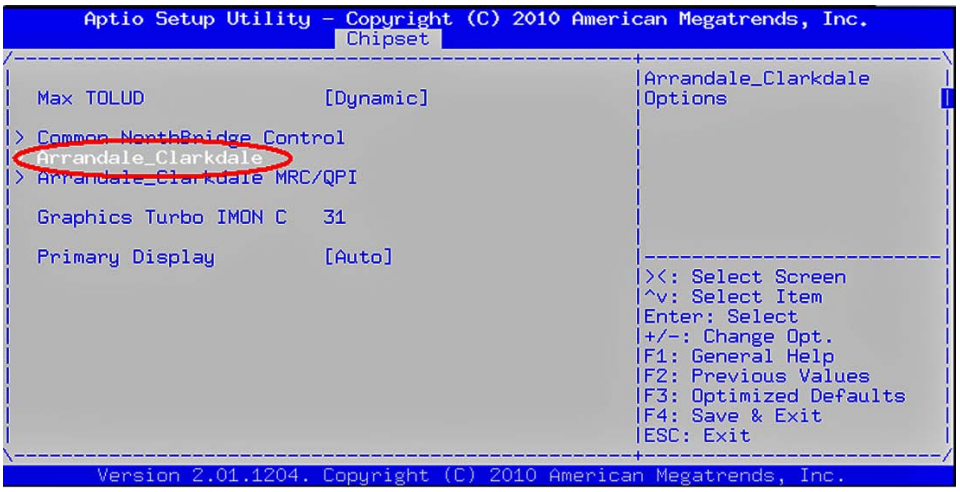


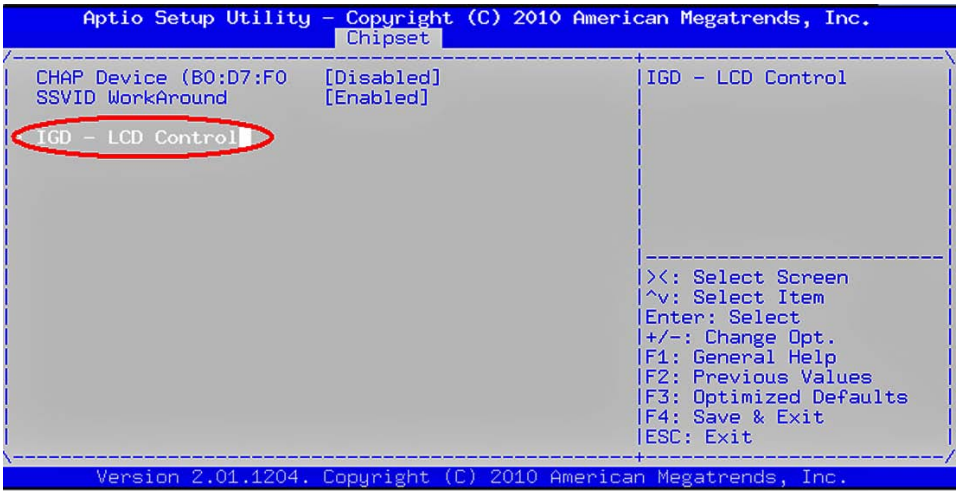
By default, the SATA controllers are enabled and the SATA mode is IDE. No speed limitation is selected.

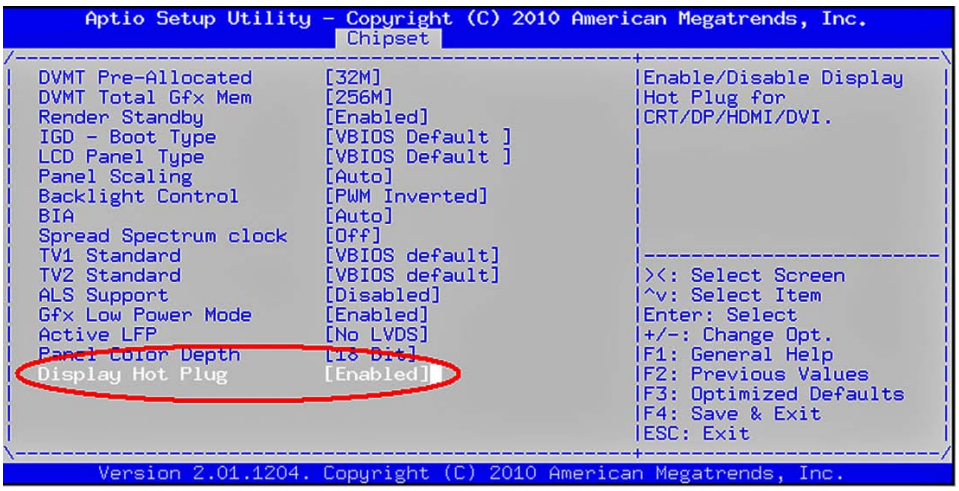
6.3 North Bridge & Display Hot Plug configuration

To manage display hot plug (for fixing CRP #4072), a new menu has been added in North Bridge Configuration
`-> Arrandale_Clarkdale -> IGD - LCD Control -> Display Hot Plug`

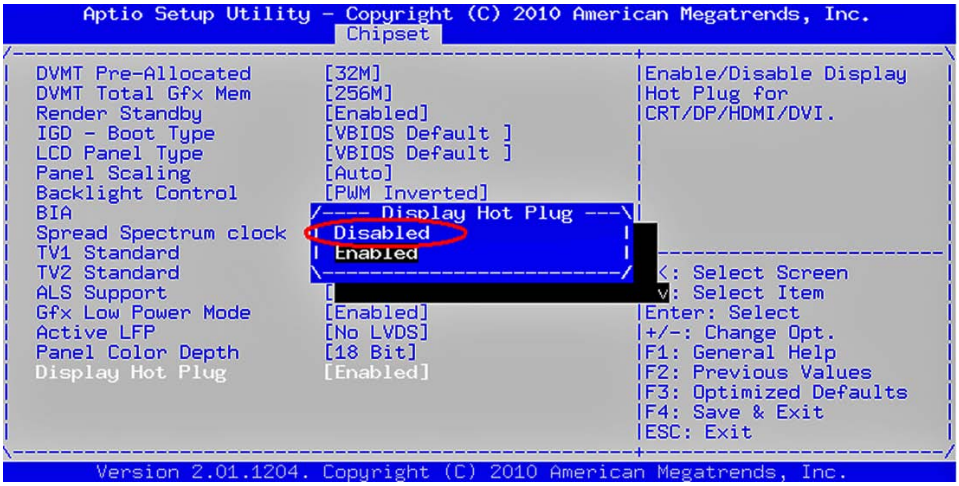






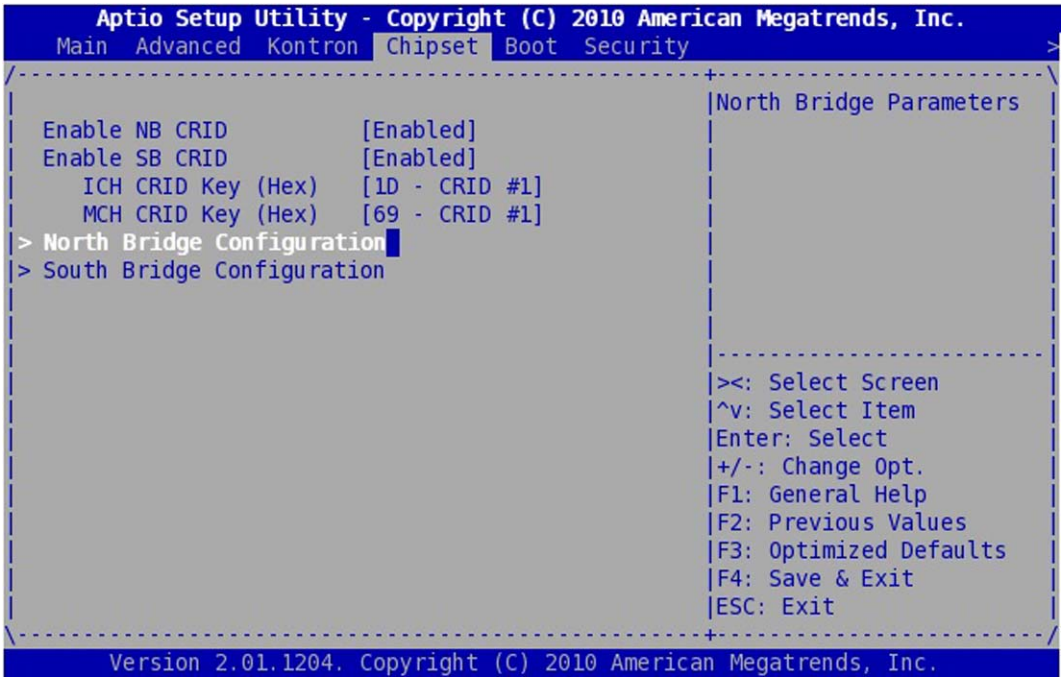


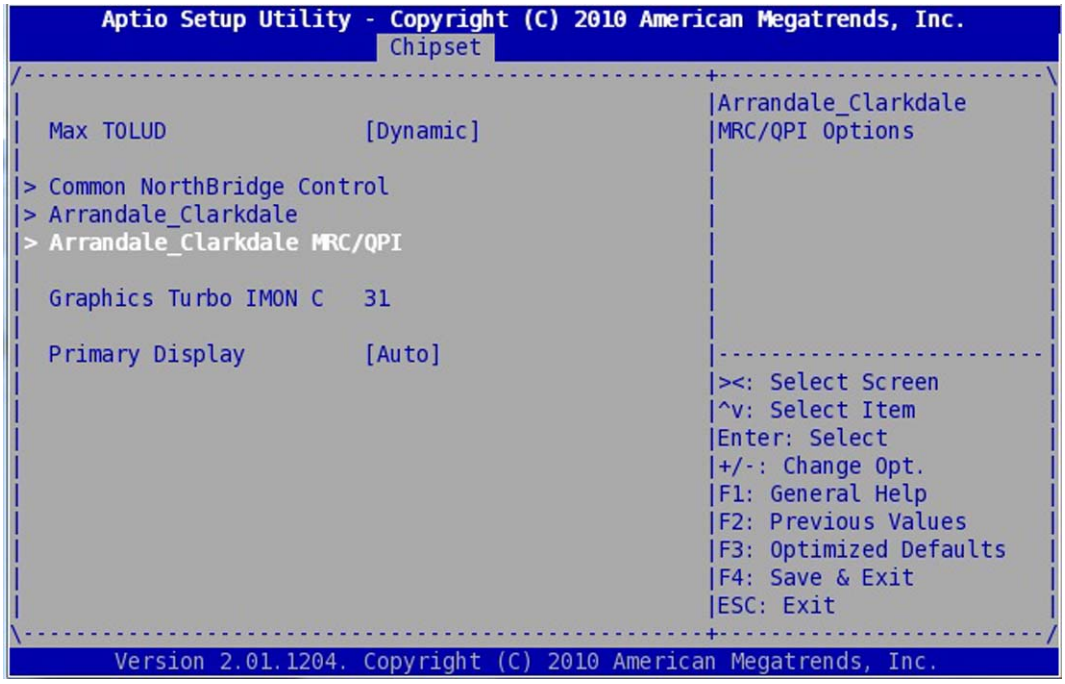
To fix CRP #4072, we have to disable display hot plug in order to not generate IRQ that causes USB 2.0 unworkable as shown in following picture:

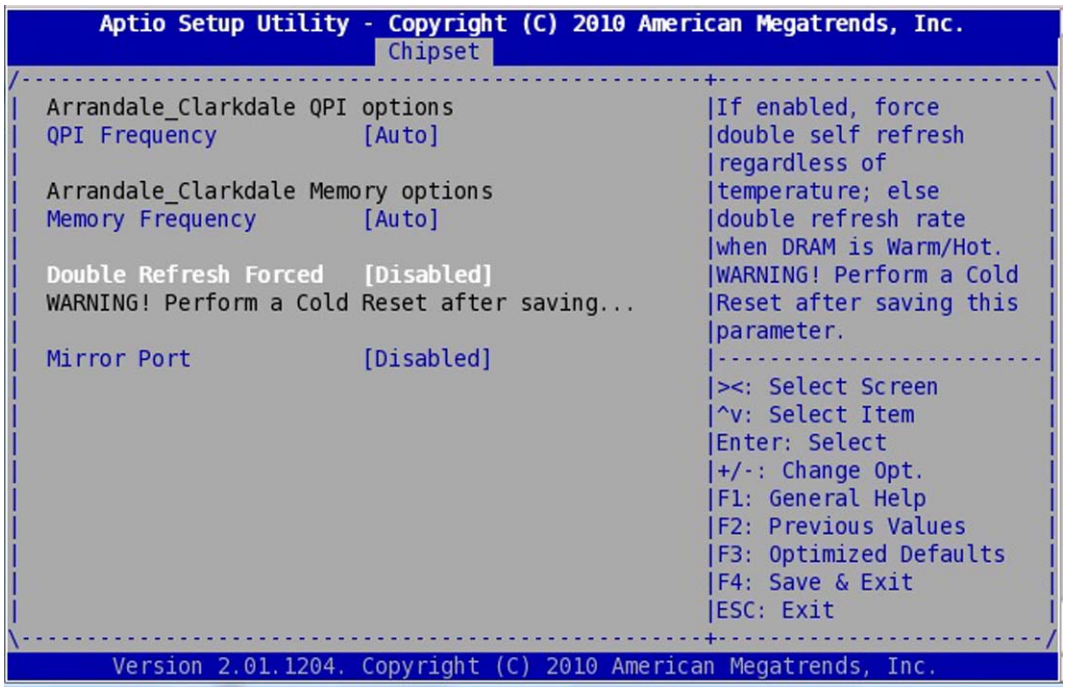


6.4 North Bridge & Memory Configuration

To manage the DDR3 refresh rate for the extended temperature range (above +85°C) a new option has been added in `North Bridge Configuration` -> `Arrandale_Clarkdale MRC/QPI` -> `Double Refresh Forced`







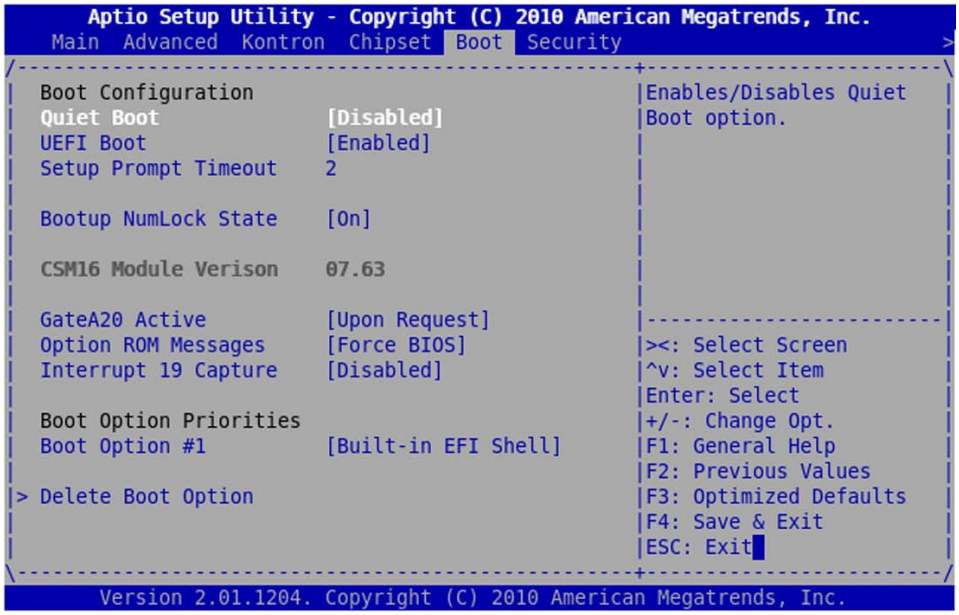
By default the option is disabled and the DDR3 refresh rate managed by the Memory Controller is suitable for the normal temperature range (up to +85°C).

When operating in the extended temperature range (above +85°C) it may be needed to double the refresh rate. Note the Automatic Self Refresh feature is supported by the DDR3 components.

The Double Refresh Forced option will be activated only after a cold reset because the BIOS needs to re-init the memory controller.

The other settings are Not intended to be changed.

Chapter 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 51
- UEFI boot: Section 7.2 page 51
- Setup prompt timeout: Section 7.3 page 51
- Bootup NumLock State: Section 7.4 page 51
- Boot Option Priorities: Section 7.5 page 52
- Network Device BBS Priorities: Section 7.6 page 53
- Hard Drive BBS Priorities: Section 7.7 page 55
- Delete Boot Option: Section 7.8 page 57

Other following submenus are Reserved and Not to be used !

- GateA20 Active
- Option ROM Messages
- Interrupt 19 Capture
- Add New Boot Option

The VM6050 boot time is about 5 seconds after power on.

7.1 Quiet boot

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

```
Version 2.00.1204. Copyright (C) 2010 American Megatrends, Inc.
```

Press <DEL> or <F2> to enter setup. Press <F7> for BBS POPUP Menu.

Set Quiet boot

- Disabled
- Enabled

Default is `Disabled`

7.2 UEFI boot

UEFI Boot setting allows to enable or disable UEFI boot from disk

Set UEFI Boot

- Disabled
- Enabled

Default is `Enabled`

7.3 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.

7.4 Bootup Numlock State

This menu selects the keyboard numlock state

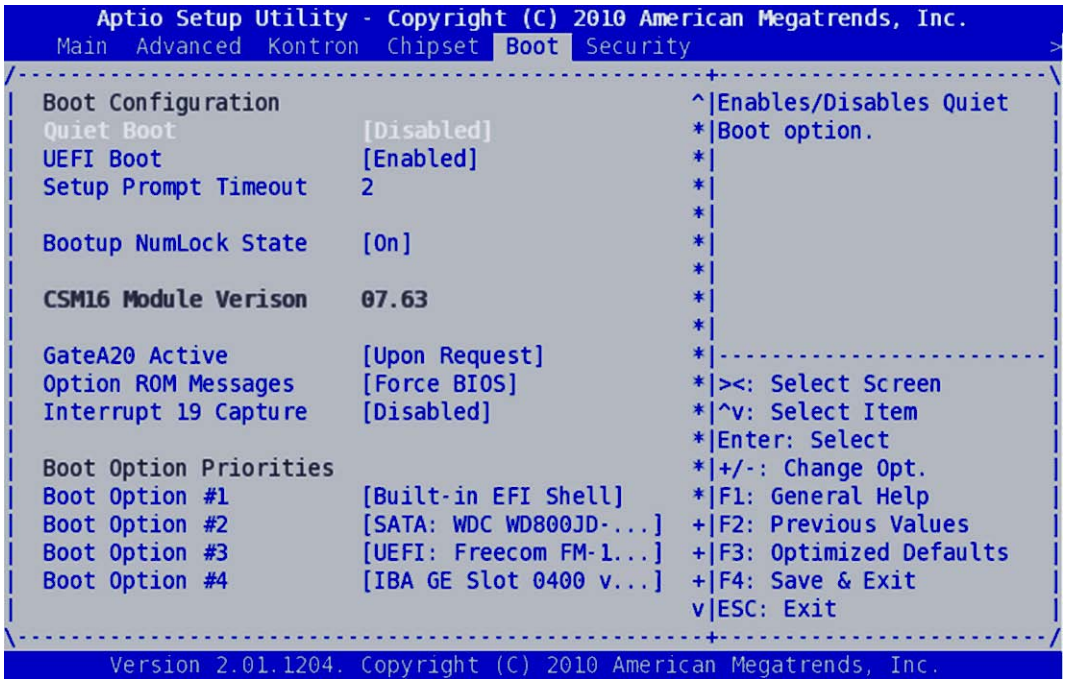
Set Bootup NumLock State

- On
- Off

Default is `On`

7.5 Boot Option Priorities

This menu specifies the boot sequence from the available boot devices. The first device into the list is the primary device that will be booted first. If the boot is rejected (for example unsuccessful PXE boot) then the second device will be used for boot and so on. Here is an example of a boot devices list:



To change the boot devices order:

- 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

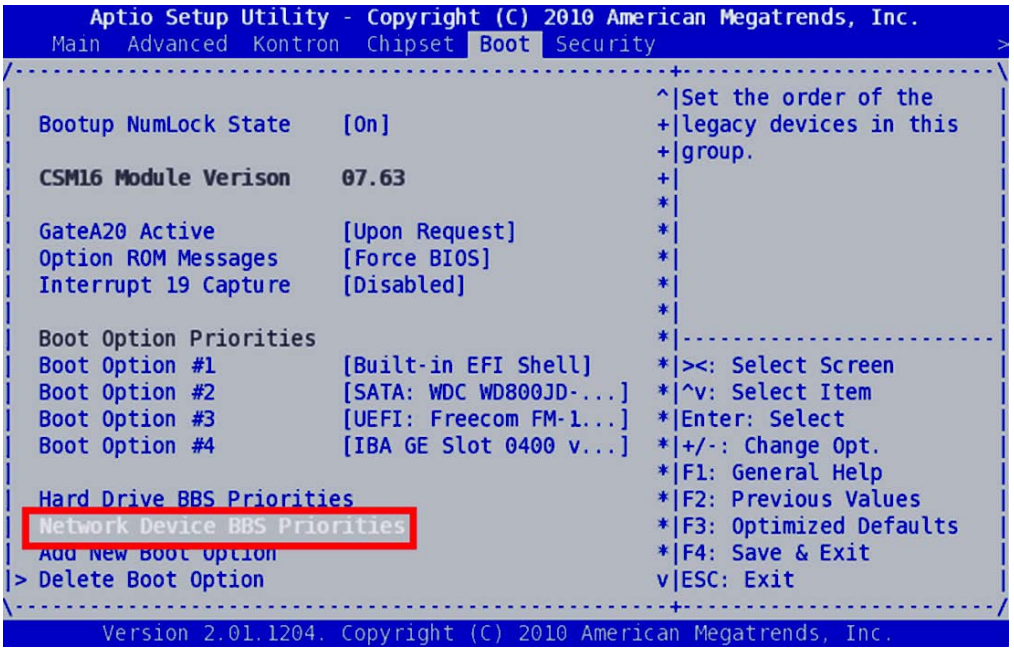
The possible family boot device can be SATA-USB or Gigabyte Ethernet (Gbe). In the boot device items list only one item per family will appear. If more than one device is available for booting (for example 2 SATA disk or 4 Ethernets for PXE) then 2 new submenus can appear below the item list. So it can 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 BSS Priorities → This is the submenu for setting a Gbe boot order or deleting a Gbe boot possibility

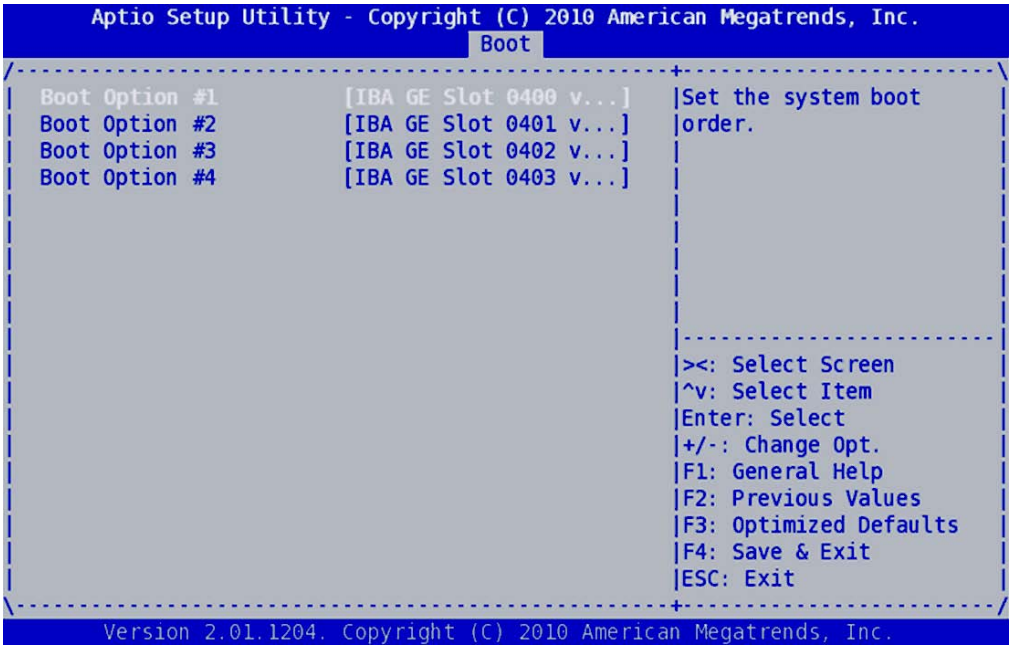
7.6 Network Device BSS Priorities (when PXE ROM Enabled)

The setting allows to configure the Ethernet boot device sequence for PXE.

When PXE ROM has been enabled, Ethernet devices become available for PXE booting (4 Ethernets interfaces). In this case a new submenu is displayed in Boot Setup menu. See image below:



Select this parameter to display available Ethernet Device.



The network device “IBA GE Slot 040X …” corresponds to the Ethernet interface X of the Intel® 82580 BartonHills.

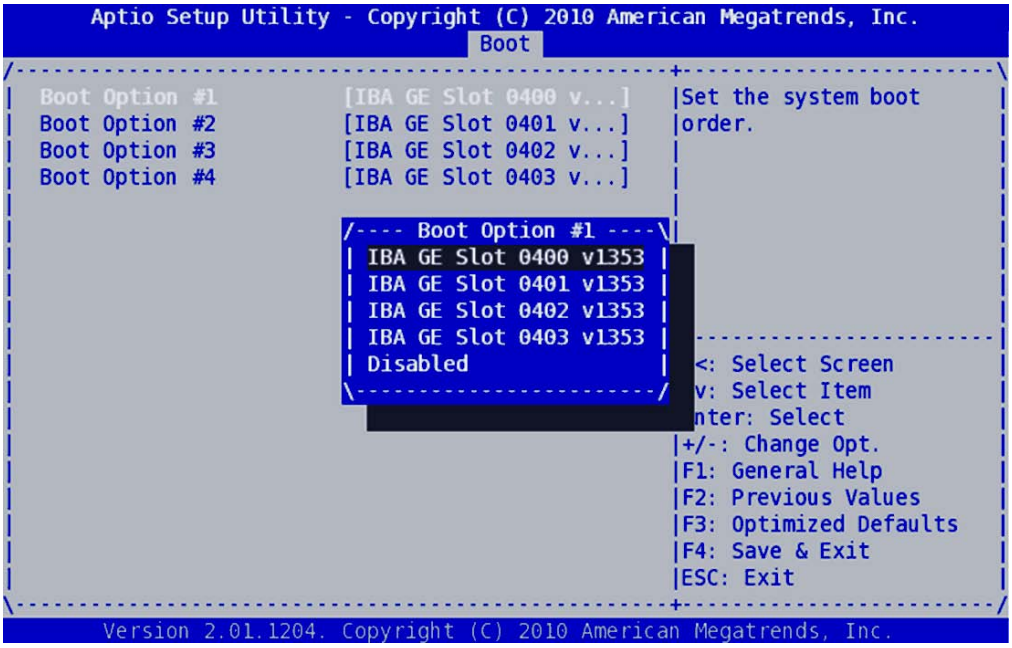
To change the PXE boot devices order:

- 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 in the list

To disable one of the PXE boot device

- Select a device from the list (Use the <↑> or <↓> to highlight the desired item)
- **<Enter>** to validate the choice

A new submenu appears (see image) , select `Disabled` to disable the PXE device



When a PXE boot device is disabled this does not disable the PXE OpROm loading for the concerned boot device. So this following message will appear 4 times in any case when PXE ROM is enabled for South Bridge:

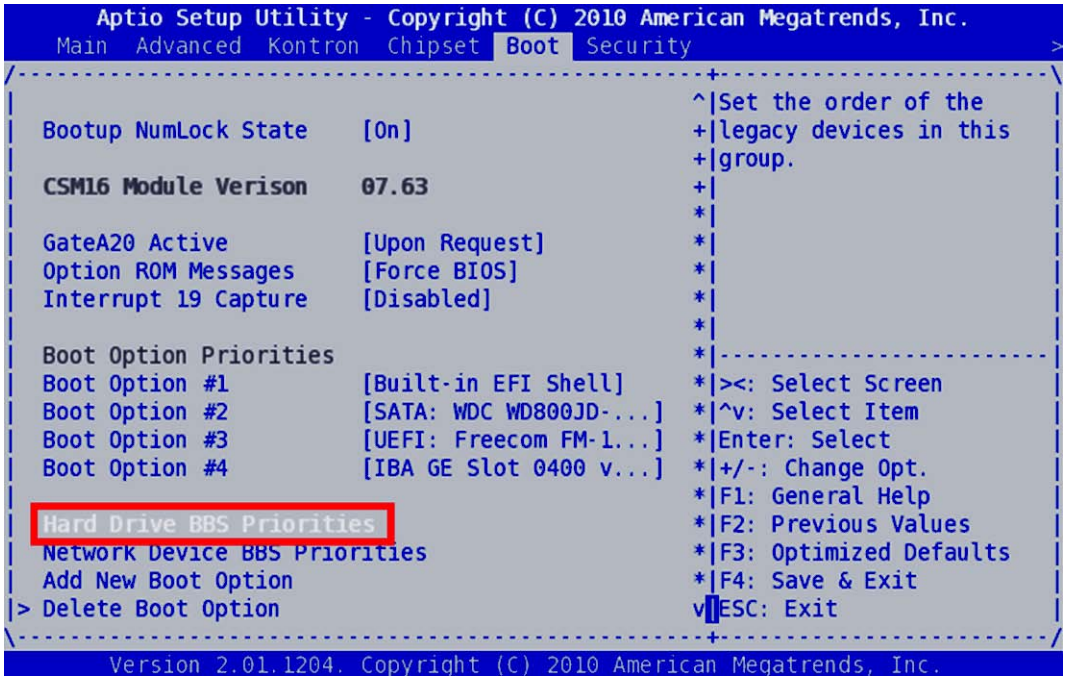
```
Initializing Intel(R) Boot Agent GE v1.3.53
        PXE 2.1 Build 089 (WfM 2.0)
```

Press **<Ctrl>+<S>** to enter the Setup Menu..

7.7 Hard Drive BBS Priorities

The setting allows to configure the SATA, USB boot device sequence.

This submenu appears when several SATA disk or USB device are present. See image:



Select this menu to see the available SATA and USB boot device and to be able to disable it or to reorganize the boot sequence.

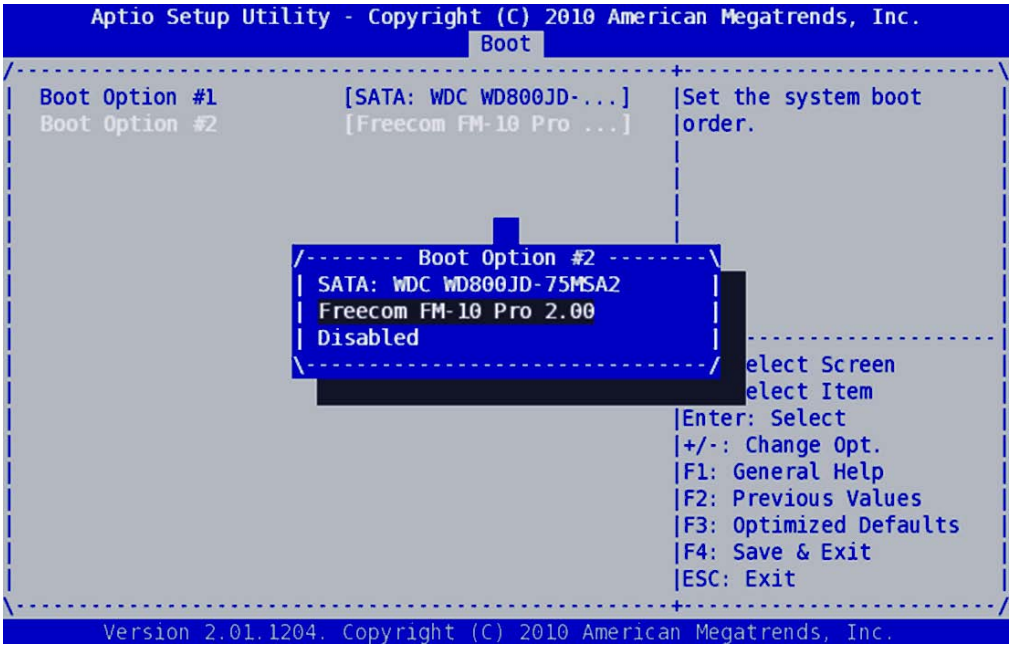
To change the boot device ordering

- 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 in the list

To disable one of the boot device

- Select a device from the list (Use the <↑> or <↓> to highlight the desired item
- <Enter> to validate the choice

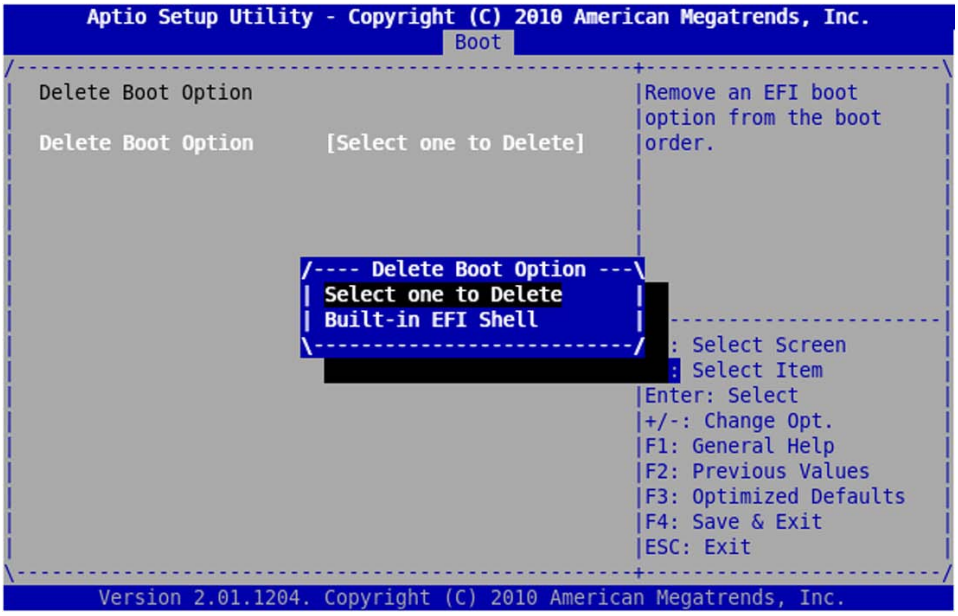
A new submenu appears (see image) , select `Disabled` to disable the SATA or USB device



7.8 Delete Boot Option

The setting allows to delete a boot device from the available boot device list.

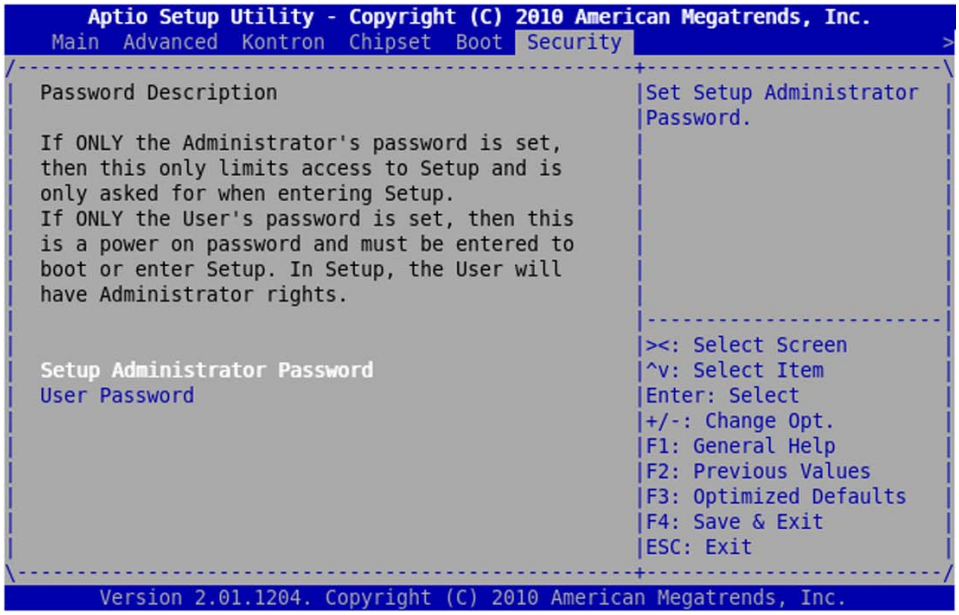
In particular Built-In EFI shell can be deleted.



To delete a boot device like EFI Shell

- Select a device from the list (Use the <↑> or <↓> to highlight the desired item)
- **<Enter>** to validate the choice

Chapter 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.

A HDD security configure submenu can appear when a SATA disk is connected.

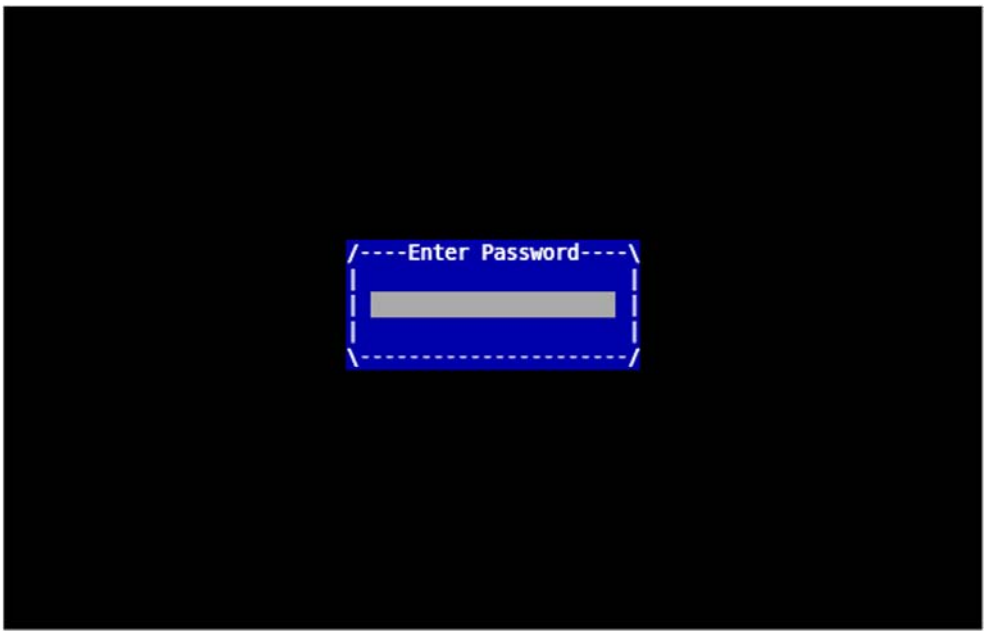
This submenu is Reserved and Not To Be Used

8.1 Enter Administrator or user password

To enter password:

- Select the administrator or user password item
- A pop-up window appears and proposes to you to create a new password
- Enter a password from 1 to 20 characters
- Confirm password
- Then the new password will be recorded if save change is launch in Save & Exit Menu.

At next reboot if <F2> key is pressed then entering password is mandatory to enter SETUP



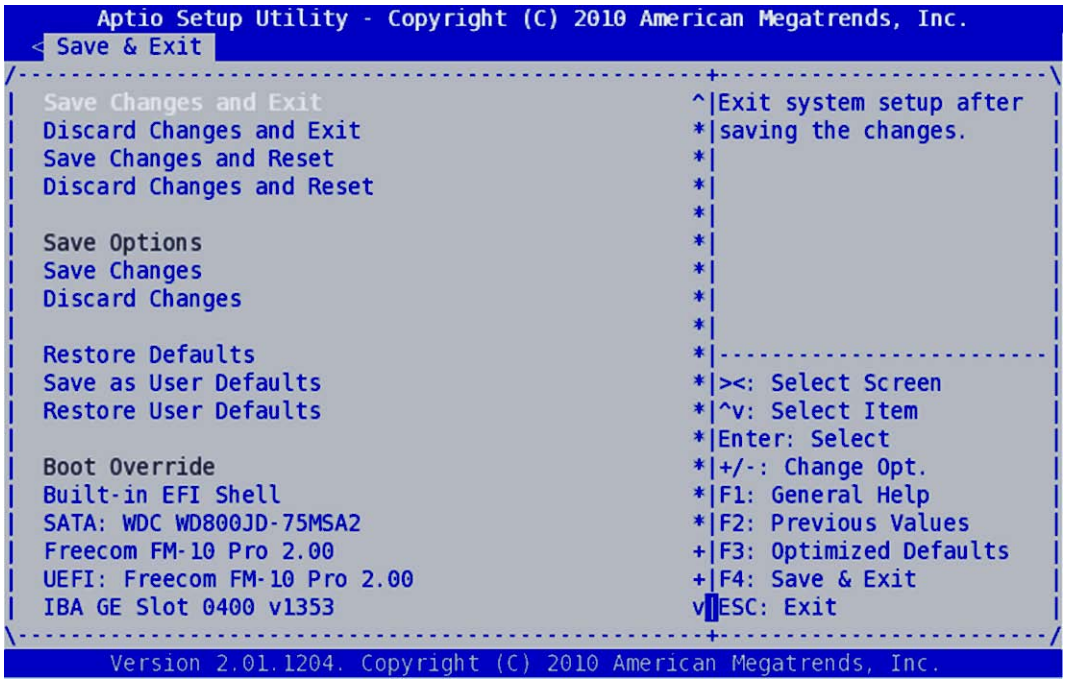
When User password has been set the password will be required to entering SETUP and to to execute the BIOS boot device selection .

To suppress password

- Select the administrator or user password item
- A pop-up window appears and proposes to you to enter a password
- Enter previous password
- A pop-up window appears and proposes to you to enter a new password
- Then type an empty password
- Confirm empty password
- Password will be deleted if save change is launch in Save & Exit Menu.

If password is lost the solution to unlock it will be to flash the BIOS or to flash the SETUP BIOS part.

Chapter 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 62
- Discard Changes and Exit: section 9.1 page 62
- Save Changes and Reset: section 9.1 page 62
- Discard Changes and Reset: section 9.1 page 62
- Save Changes: section 9.2 page 62
- Discard Changes: section 9.2 page 62
- Restore Defaults: section 9.2 page 62
- Save as User Defaults: section 9.3 page 62
- Restore User Defaults: section 9.3 page 62
- Boot Override: section 9.4 page 62

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

9.3 Saving a user configuration

Current SETUP configuration can be saved as user configuration and can be restored the same way the default configuration.

Select desired item and **<Enter>**

- Save as User Defaults
- Restore User Defaults

9.4 Boot Override

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

Chapter 10 - EFI SHELL

EFI Shell is a boot shell available on the VM6050 that is accessible in the boot device list. EFI Shell is launched automatically if no other boot device is connected to the VM6050. 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 `VM6050> help help`) to have the detail of a command syntax

» VM6050> help

Command Name	Description	See Section
`?`	Displays the EFI Shell command list or verbose command help	10.1.20 page 80
`alias`	Displays, creates, or deletes EFI Shell aliases	10.1.1 page 65
`amlview`	AML view utility	10.1.2 page 66
`bcfg`	Boot configuration utility	10.1.3 page 67
`cd`	Displays or changes the current directory	10.1.4 page 68
`cls`	Clears standard output and optionally changes background color	10.1.5 page 69
`connect`	Connects one or more EFI drivers to a device	10.1.6 page 69
`cpuutil`	CPU information utility	10.1.7 page 69
`date`	Displays or changes the current system date	10.1.8 page 70
`devices`	Displays the list of devices managed by EFI drivers	10.1.9 page 70
`dh`	Displays EFI handle information	10.1.10 page 71
`disconnect`	Disconnects one or more EFI drivers from a device	10.1.11 page 72
`drvcfg`	Invokes the Driver Configuration Protocol	10.1.12 page 73
`drivers`	Displays the EFI driver list	10.1.13 page 75
`dumpacpi`	Print ACPI Tables	10.1.14 page 76
`dumpaml`	Print AML dump	10.1.15 page 76
`echo`	Controls batch file command echoing or displays a message	10.1.16 page 77
`exit`	Exits the EFI Shell environment	10.1.17 page 77
`for`	Executes commands for each item in a set of items	10.1.18 page 78
`goto`	Forces batch file execution to jump to specified location	10.1.19 page 79
`help`	Displays the EFI Shell command list or verbose command help	10.1.20 page 80

Command Name	Description	See Section
`if`	Executes commands in specified conditions	10.1.21 page 81
`ifconfig`	UEFI network modification utility	10.1.22 page 82
`kdiag`	Perform board diagnostics - **Available ONLY if ordered.**	10.1.23 page 82
`kflash`	Kontron SPI flasher	10.1.24 page 83
`kmac`	Kontron MAC Address utility	10.1.25 page 83
`kpld`	Kontron PLD Commands	10.1.26 page 84
`kuuid`	Kontron UUID Configurator	10.1.26 page 70
`kvpd`	Kontron VPD Information	10.1.28 page 86
`ls`	Displays a list of files and subdirectories in a directory	10.1.29 page 87
`map`	Displays or defines mappings	10.1.30 page 89
`mem`	Displays the contents of memory	10.1.31 page 92
`memmap`	Displays the memory map	10.1.32 page 94
`mm`	Displays or modifies MEM/MMIO/IO/PCI/PCIE address space	10.1.33 page 95
`mv`	Moves one or more files or directories to another location	10.1.34 page 97
`pause`	Prints a message and waits for keyboard input	10.1.35 page 99
`pci`	Displays PCI device list or PCI function configuration space	10.1.36 page 100
`ping`	Target IP ping utility	10.1.37 page 102
`reconnect`	Reconnects one or more EFI drivers to a device	10.1.38 page 102
`reset`	Resets the system	10.1.39 page 102
`set`	Displays or modifies EFI Shell environment variables	10.1.40 page 103
`shift`	Shifts batch file input parameter positions	10.1.41 page 104
`smbiosview`	Displays SMBIOS information	10.1.42 page 105
`smbutil`	SMBus utility	10.1.43 page 106
`time`	Displays or changes the current system time	10.1.44 page 106

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

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

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

Also AmlView propose its own shell syntax

```
fs0:\> AmlView
Welcome to AmlView on EFI Shell (Version 0.01)
DefinitionBlock ("Dsdt.aml", "DSDT", 1, "ALASKA", "A M I", 0)
```

AmlView > help

```
EXEC      <NodeName>          : Print the result of the method node.
CAT       <NodeName>          : Print the node content.
LS [-R] [<NodeName>]          : List the node name. (-R means recursive)
CD       [<NodeName>]         : Change current node dir.
QUIT           :               Quit Current Command Prompt.
HELP                          : Print 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     add ´file´ with ´desc´ at position #
  addp    add ´file´ with ´desc´ at position #.Use hard drive path
  addh    add ´handle´ with ´desc´ at position #.Use Handle
  rm      remove #
  mv      move # to #
```

> Example:

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

```
VM6050> bcfg boot dump
The boot option list is:
01.  VenMedia(5023B95C-DB26-429B-A648-BD47664C8012)
/C57AD6B7-0515-40A8-9D21-551652854E37 "Built-in EFI Shell"
02. BBS-Harddrive() "Hard Drive"
03. Acpi(PNP0A03,0)/Pci(1D|0)/Usb(1, 0)/Usb(1, 0)/HD(Part1,Sig000B9400) "UEFI: Freecom FM-10 Pro 2.00"
04. BBS-Net() "Network Card" OPT

VM6050> bcfg boot mv 4 2
bcfg: boot option 4 moved to 2

VM6050> bcfg boot dump
The boot option list is:
01.  VenMedia(5023B95C-DB26-429B-A648-BD47664C8012)
/C57AD6B7-0515-40A8-9D21-551652854E37 "Built-in EFI Shell"
02. BBS-Net() "Network Card" OPT
03. BBS-Harddrive() "Hard Drive"
04. Acpi(PNP0A03,0)/Pci(1D|0)/Usb(1, 0)/Usb(1, 0)/HD(Part1,Sig000B9400) "UEFI: Freecom FM-10 Pro 2.00"
```

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	Display one screen at a time
l XXX	Display 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	Handle number in hexadecimal format
-p	Protocol ID
-d	Display EFI Driver Model related information
-l	Display information in the specified ISO 639-2 language
-v	Display 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(DXE Core)

2: FwVol FwFileSys FwVolBlk DevPath(MemMap(11:1B50000-1D4FFC8))

3: Image(Ebc)

4: DevPath(MemMap(11:1CA0000-1CB0000))

5: Image(WinNtThunk)

6: WinNtThunk DevPath(..76F3-11D4-BCEA-0080C73C8881))

7: Image(WinNtBusDriver) DriverBinding

...

- To display detailed information for handle 0x30:

```
Shell> dh 30
```

Handle 30 (01AF5308)

IsaIo

ROM Size.....: 00000000

ROM Location..: 00000000

ISA Resource List :

IO : 000003F8-000003FF Attr : 00000000

INT : 00000004-00000000 Attr : 00000000

dpath

PNP Device Path for PnP

HID A0341D0, UID 0

Hardware Device Path for PCI

PNP Device Path for PnP

HID 50141D0, UID 0

AsStr: 'Acpi(PNP0A03,0)/Pci(1F|0)/Acpi(PNP0501,0)'

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

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

Handle dump by protocol 'Diskio'

15: DiskIo BlkIo DevPath(..i(3|1)/Ata(Secondary,Master))

16: DiskIo BlkIo DevPath(..,1)/PCI(0|0)/Scsi(Pun0,Lun0))

44: DiskIo BlkIo fs DevPath(..ABD0-01C0-507B-9E5F8078F531)) ESP

45: DiskIo BlkIo fs DevPath(..i(Pun0,Lun0)/HD(Part4,SigG0)) ESP

17: DiskIo BlkIo DevPath(..PCI(3|1)/Ata(Primary,Master))

- 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(DXE Core)

5: Image(WinNtThunk)

7: Image(WinNtBusDriver) DriverBinding

8: Image(Metronome)

A: Image(IsaBus) DriverBinding

B: Image(WinNtConsole) DriverBinding ...

10.1.11 disconnect

Reserved - Not To Be Used

10.1.12 drvcfg

Invokes the Driver Configuration Protocol.

```
DRVCFG [-l XXX] [-c] [-f Type|-v|-s]
       [DriverHandle [DeviceHandle [ChildHandle]]]
```

`-l`	Configure using the specified ISO 639-2 language
`-c`	Configure all child devices
`-f`	Force defaults
`-v`	Validate options
`-s`	Set options
`Type`	The type of default configuration options to force on the controller specified by ControllerHandle and ChildHandle: `0` - Safe Defaults. `1` - Manufacturing Defaults. `2` - Custom Defaults. `3` - Performance Defaults.
`DriverHandle`	Handle of the driver to configure
`DeviceHandle`	Handle of a device that DriverHandle is managing
`ChildHandle`	Handle of a device that is a child of DeviceHandle

Note:

1. Default Type.
   0. Safe Defaults. Places a controller in a safe configuration with the greatest probability of functioning correctly in a platform.
   1. Manufacturing Defaults. Optional type that places the controller in a configuration suitable for a manufacturing and test environment.
   2. Custom Defaults. Optional type that places the controller in a custom configuration.
   3. Performance Defaults. Optional type that places the controller in a configuration that maximizes the controller's performance in a platform.

   Other Value - Depends on the driver's implementation.

> Examples:

- To display the list of devices available for configuration:

```
Shell> drvcfg
```

- To display the list of devices and child devices available for configuration:

```
Shell> drvcfg -c
```

- To force defaults on all devices:

```
Shell> drvcfg -f 0
```

- To force defaults on all devices managed by driver 0x17:

```
Shell> drvcfg -f 0 17
```

- To force defaults on device 0x28 which is managed by driver 0x17:

```
Shell> drvcfg -f 0 17 28
```

- To force defaults on all child devices of device 0x28 which is managed by driver 0x17:

```
Shell> drvcfg -f 0 17 28 -c
```

- To force defaults on child device 0x30 of device 0x28 which is managed by driver 0x17:

```
Shell> drvcfg -f 0 17 28 30
```

- To validate options on all devices:

```
Shell> drvcfg -v
```

- To validate options on all devices managed by driver 0x17:

```
Shell> drvcfg -v 17
```

- To validate options on device 0x28 which is managed by driver 0x17:

```
Shell> drvcfg -v 17 28
```

- To validate options on all child devices of device 0x28 which are managed by driver 0x17:

```
Shell> drvcfg -v 17 28 -c
```

- To validate options on child device 0x30 of device 0x28 which is managed by driver 0x17:

```
Shell> drvcfg -v 17 28 30
```

- To set options on device 0x28 which is managed by driver 0x17:

```
Shell> drvcfg -s 17 28
```

- To set options on child device 0x30 of device 0x28 which is managed by driver 0x17:

```
Shell> drvcfg -s 17 28 30
```

- To set options on device 0x28 which is managed by driver 0x17, in English:

```
Shell> drvcfg -s 17 28 -l eng
```

- To set options on device 0x28 which is managed by driver 0x17, in Spanish:

```
Shell> drvcfg -s 17 28 -l spa
```

10.1.13 drivers

Displays the EFI driver list.

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

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

Display Format:

DRV	Handle 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

> Examples:

- To display the list:

```
VM6050> drivers
            T   D
D           Y C I
R           P F A
V  VERSION  E G G #D #C DRIVER NAME                          IMAGE NAME
== ======== = = = == == ================================== ==================
6F 00010000 D - -  1  - AMI File System Driver              FileSystem
71 00020200 B - -  1 25 <UNKNOWN>                          PciBus
7D 00000001 D - -  2  - PCH Serial ATA Controller Initializ SataController
7F 00000001 ? - -  -  - AMI AHCI BUS Driver                AHCI
81 04001500 B X X  4  4 Intel(R) PRO/1000 4.0.15 PCI-E      IntelGigabitLanx64
84 00000010 ? - -  -  - <UNKNOWN>                          BIOSBLKIO
85 00000024 B - -  1  1 BIOS[INT10] Video Driver            CsmVideo
86 00000010 ? - -  -  - <UNKNOWN>                          <UNKNOWN>
87 00000000 ? - -  -  - BIOS[UNDI] Simple Network Protocol  BiosSnp
88 00000010 ? - -  -  - MNP   Network Service Driver        Mnp
89 00000010 ? - -  -  - ARP   Network Service Driver        Arp
8A 00000010 ? - -  -  - IP4  Network Service Driver         Ip4
8B 00000010 ? - -  -  - DHCP Protocol Driver                Dhcp4
8C 00000010 ? - -  -  - UDP   Network Service Driver        Udp4
8D 00000010 ? - -  -  - Tcp   Network Service Driver        Tcp4
8E 00000010 ? - -  -  - MTFTP4 Network Service              Mtftp4
8F 00000010 ? - -  -  - IP4 CONFIG Network Service Driver   Ip4Config
96 00000010 B - -  2  2 AMI Serial I/O Driver               Terminal
97 00000010 B - -  1  1 AMI Terminal Driver                 Terminal
98 00000089 D - -  2  - AMI USB Driver                     UHCD
9A 00000089 B - -  2  4 USB bus                            UHCD
9B 00000001 ? - -  -  - USB Keyboard driver                UHCD
9C 00000002 D - -  1  - USB Mouse driver                   UHCD
9D 00000001 D - -  1  - USB Mass Storage driver            UHCD
```

```
C3 00000010 D - -  5  - <UNKNOWN>                          CORE_DXE
C4 00000010 D - -  1  - <UNKNOWN>                          CORE_DXE
C5 00000010 B - -  3  3 <UNKNOWN>                          CORE_DXE
C7 00000010 B - -  2  3 <UNKNOWN>                          CORE_DXE
C8 00000010 ? - -  -  - AMI PS/2 Driver                    CORE_DXE
C9 00000010 ? - -  -  - AMI Floppy Driver                  CORE_DXE
CA 00000001 B - -  2  1 AMI IDE BUS Driver                 CORE_DXE
CB 00000010 B - -  1  2 AMI Generic LPC Super I/O Driver    CORE_DXE
```

10.1.14 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.

10.1.15 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	Execute AML method.

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

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

10.1.16 echo

Controls batch file command echoing or displays a message.

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

`-on`	Enable echo when executing batch file commands
`-off`	Disable echo when executing batch file commands
`message`	Display 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
```

10.1.17 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.

10.1.18 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
```

10.1.19 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.

> Examples:

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

10.1.20 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
```

10.1.21 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.

> Examples:

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

10.1.22 ifconfig

`IfConfig` © Intel Corporation 2006

Modify 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 configure 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 user has to enable “Network stack” in Advanced menu to have this command available.

10.1.23 kdiag

This command is fully described in the document SD.DT.F88 “VM6050 PBIT User's Guide”.

10.1.24 kflash

Kontron SPI flasher

Usage:

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

- Operation mode
  - `-p` program flash
  - `-i` show information string and check CRC
  - `-v` verify flashed image
  - `-s` save current ROM image to file
  - `-c` clone flash content to second flash (Only in RESCUE mode)
  - `-h` Show this help
- Options
  - `-f` force write
- Expert options: Not recommended for standard use
  - `-r` raw image mode (.bin, .rom)
  - `-e` erase all flash without preserving Ethernet area
  - `-sp` setup preserve NVRAM settings

10.1.25 kmac

Kontron MAC Address utility

Usage:

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

- Operation mode
  - `-h` Show this help
  - `-r | --read` Show MAC Address (82580 chipset)
  - `-w | --write value` Update MAC Address of the 82580 chipset
    value format = 0x0000DEaabbcc
  - `-prog` Program the 82580 EEPROM with a predefined image (not fully tested)
  - `-dump` Dump the first 1024 words of the 82580 EEPROM
  - `-save filename` Save the 82580 EEPROM contents to <filename>
  - `-load filename` Load the 82580 EEPROM with the contents of <filename>

> Example:

```
Shell> kmac -r
Quad link Gbe 82580 configuration
MAC Address of Intel 82580 LAN0 = 00:00:DE:52:1B:9C
MAC Address of Intel 82580 LAN1 = 00:00:DE:52:1B:9D
MAC Address of Intel 82580 LAN2 = 00:00:DE:52:1B:9E
MAC Address of Intel 82580 LAN3 = 00:00:DE:52:1B:9F
```

10.1.26 kpld

Kontron PLD Commands: this command allows basics accesses to internal PLD registers and I2C device (EEPROM, Thermal sensors)

Usage:

```
kpld [ -h|-? ]
```

- Operation mode

  `-h` Show this help

  `-v` Show cpld revision

  `-m` Memory information protection -r : Read cpld register

  -> kpld -r Offset

  `-w` Write cpld register

  -> kpld -w Offset Value

  `-i2cr` Read Access to I2C bus

  -> kpld -i2cr busNum Add Offset Type

  `-i2cw` Write Access to I2C bus

  -> kpld -i2cw busNum Add Offset Type Data

10.1.27 kuuid

Kontron UUID configurator: this command allows user to change the default UUID value of the board and overcome the value set on the setup (See §5.1).

Usage:

kuuid [-a|-r|-p|-h]

- Operation mode

  -a | --ascii : Store UUID in ASCII format

  -r | --raw : Store UUID in RAW format

  -p | --print : Print UUID

  -h | --help : Show this help

> Example:

```
VM6050> kuuid -r

Enter UUID[15-8]:0000000000000000
Enter UUID[7-0]:0000000000000000
Current UUID: 0000000000000001
New     UUID: 00000000000000000000000000000000


Is this correct ?
                [n] No (re-enter UUID)
                [y] Yes
                [q] Exit no change
y

VM6050> kuuid -p

Current UUID (RAW)  : 00000000-0000-0000-0000000000000000

VM6050> reset
```

It is mandatory to perform a reset at the end of the process to update UUID in SMBIOS table.

10.1.28 kvpd

Kontron VPD Information: displays Vital Product Information

Usage:

```
kvpd [ -p|-m|-h ]
```

- Operation mode
  - `-p` Display VPD information
  - `-m` Modify or enter VPD information (Rescue Only)
  - `-h` Show this help

> Example

```
 VM6050> kvpd -p

Current configuration:
              Order Code     : PROTO-VM6050_LOT1-B
              EC Level       : ECO2000
              Serial Number  : 181271020016
              Variant        : 1000004180850000
              Check Sum      : 56FC9F22
```

10.1.29 ls

Displays a list of files and subdirectories in a directory.

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

-b	Display one screen at a time
-r	Display recursively (including subdirectories)
-a	Display 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:

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

- 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	Delete a mapping
-r	Reset to default mappings
-v	Display 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	Display the consistent mapping name
-f	Display the normal mapping name(not consistent mapping)
-t	Display 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 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

f4            UnknownDevice - Alias fs0 blk0
              Device Path  VenHw(58C518B1-76F3-11D4-BCEA-0080C73C8881)/VenHw(0C95A92F
-A006-11D4-BCFA-0080C73C8881)
  fs0:        UnknownDevice - Alias f4 blk0
              Device Path  VenHw(58C518B1-76F3-11D4-BCEA-0080C73C8881)/VenHw(0C95A92F
-A006-11D4-BCFA-0080C73C8881)
  blk0:       UnknownDevice - Alias f4 fs0
              Device Path  VenHw(58C518B1-76F3-11D4-BCEA-0080C73C8881)/VenHw(0C95A92F
-A006-11D4-BCFA-0080C73C8881)
```

- To display all mappings in the device mapping table:

```
Shell> map
Device mapping table
  f4    :UnknownDevice - Alias fs0 blk0
         Device Path  VenHw(58C518B1-76F3-11D4-BCEA-0080C73C8881)/VenHw(0C95A92F
-A006-11D4-BCFA-0080C73C8881)
  fs0   :UnknownDevice - Alias f4 blk0
         Device Path  VenHw(58C518B1-76F3-11D4-BCEA-0080C73C8881)/VenHw(0C95A92F
-A006-11D4-BCFA-0080C73C8881)
  blk0  :UnknownDevice - Alias f4 fs0
         Device Path  VenHw(58C518B1-76F3-11D4-BCEA-0080C73C8881)/VenHw(0C95A92F
-A006-11D4-BCFA-0080C73C8881)
```

- To display verbose mapping table information:

```
Shell> map -v
Device mapping table
  f4     Consist Name f4
         Other Name   fs0 blk0
         Handle       5F: Fs DiskIo BlkIo WinNtDriverIo
         Media Type   UnknownDevice
         Removable    NO
         Current Dir  \
         Device Path  VenHw(58C518B1-76F3-11D4-BCEA-0080C73C8881)/VenHw(0C95A92F
-A006-11D4-BCFA-0080C73C8881)
  fs0    Consist Name f4
         Other Name   blk0
         Handle       5F: Fs DiskIo BlkIo WinNtDriverIo
         Media Type   UnknownDevice
         Removable    NO
         Current Dir  \
         Device Path  VenHw(58C518B1-76F3-11D4-BCEA-0080C73C8881)/VenHw(0C95A92F
-A006-11D4-BCFA-0080C73C8881)
  blk0   Consist Name f4
         Other Name   fs0
         Handle       5F: Fs DiskIo BlkIo WinNtDriverIo
         Media Type   UnknownDevice
         Removable    NO
         Current Dir  \
         Device Path  VenHw(58C518B1-76F3-11D4-BCEA-0080C73C8881)/VenHw(0C95A92F
-A006-11D4-BCFA-0080C73C8881)
```

- To assign fs0 another name:

```
Shell> map floppy fs0:
  floppy:UnknownDevice - Alias f4 fs0 blk0
         Device Path  VenHw(58C518B1-76F3-11D4-BCEA-0080C73C8881)/VenHw(0C95A92F
-A006-11D4-BCFA-0080C73C8881)

* To display information about the mapped name:
Shell> map floppy
  floppy:UnknownDevice - Alias f4 fs0 blk0
         Device Path  VenHw(58C518B1-76F3-11D4-BCEA-0080C73C8881)/VenHw(0C95A92F
-A006-11D4-BCFA-0080C73C8881)
```

- To operate with the mapped name:

```
Shell> floppy:
floppy:\> ls
```

- To delete a mapped name:

```
Shell> map -d floppy
Shell> map
Device mapping table
  f4    :UnknownDevice - Alias fs0 blk0
         Device Path  VenHw(58C518B1-76F3-11D4-BCEA-0080C73C8881)/VenHw(0C95A92F
-A006-11D4-BCFA-0080C73C8881)
  fs0   :UnknownDevice - Alias f4 blk0
         Device Path  VenHw(58C518B1-76F3-11D4-BCEA-0080C73C8881)/VenHw(0C95A92F
-A006-11D4-BCFA-0080C73C8881)
  blk0  :UnknownDevice - Alias f4 fs0
         Device Path  VenHw(58C518B1-76F3-11D4-BCEA-0080C73C8881)/VenHw(0C95A92F
-A006-11D4-BCFA-0080C73C8881)
```

- To display all the mapped names starting with 'f':

```
Shell> map f*
Device mapping table
  f4    :UnknownDevice - Alias fs0 blk0
         Device Path  VenHw(58C518B1-76F3-11D4-BCEA-0080C73C8881)/VenHw(0C95A92F
-A006-11D4-BCFA-0080C73C8881)
  fs0   :UnknownDevice - Alias f4 blk0
         Device Path  VenHw(58C518B1-76F3-11D4-BCEA-0080C73C8881)/VenHw(0C95A92F
-A006-11D4-BCFA-0080C73C8881)
```

10.1.31 mem

Displays the contents of system or device memory.

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

-b	Display 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:

```
fs0:\> mem
Memory Address 000000003FF7D808 200 Bytes
3FF7D808: 49 42 49 20 53 59 53 54-02 00 01 00 78 00 00 00  *IBI SYST....x...*
3FF7D818: 5C 3E 6A FE 00 00 00 00-88 2E 1B 3F 00 00 00 00  *\>j........?....*
3FF7D828: 26 00 0C 00 00 00 00 00-88 D3 1A 3F 00 00 00 00  *&..........?....*
3FF7D838: A8 CE 1A 3F 00 00 00 00-88 F2 1A 3F 00 00 00 00  *...?.......?....*
3FF7D848: 28 EE 1A 3F 00 00 00 00-08 DD 1A 3F 00 00 00 00  *(..?.......?....*
3FF7D858: A8 EB 1A 3F 00 00 00 00-18 C3 3F 3F 00 00 00 00  *...?..........*
3FF7D868: 00 4B 3F 3F 00 00 00 00-06 00 00 00 00 00 00 00  *.K............*
3FF7D878: 08 DA F7 3F 00 00 00 00-70 74 61 6C 88 00 00 00  *...?....ptal....*
3FF7D888: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
3FF7D898: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
3FF7D8A8: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
3FF7D8B8: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
3FF7D8C8: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
3FF7D8D8: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
3FF7D8E8: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
3FF7D8F8: 00 00 00 00 00 00 00 00-70 68 06 30 88 00 00 00  *........ph.0....*
3FF7D908: 65 76 6E 74 00 00 00 00-02 02 00 60 00 00 00 00  *evnt.......`....*
3FF7D918: 18 6F 1A 3F 00 00 00 00-10 E0 3F 3F 00 00 00 00  *.o.?.........*
3FF7D928: 10 00 00 00 00 00 00 00-40 C0 12 3F 00 00 00 00  *........@..?....*
3FF7D938: 10 80 13 3F 00 00 00 00-00 00 00 00 00 00 00 00  *...?............*
3FF7D948: 00 00 00 00 00 00 00 00-40 7D 3F 3F 00 00 00 00  *........@.....*
3FF7D958: 50 6F 1A 3F 00 00 00 00-00 00 00 00 00 00 00 00  *Po.?............*
3FF7D968: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
3FF7D978: 00 00 00 00 00 00 00 00-70 74 61 6C 88 00 00 00  *........ptal....*
```

```
3FF7D988: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
3FF7D998: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
3FF7D9A8: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
3FF7D9B8: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
3FF7D9C8: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
3FF7D9D8: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
3FF7D9E8: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
3FF7D9F8: 00 00 00 00 00 00 00 00-70 68 06 30 A0 00 00 00  *........ph.0....*
Valid EFI Header at Address 000000003FF7D808
 ------------------------------------------
System: Table Structure size 00000078 revision 00010002
ConIn (3F1AD388) ConOut (3F1AF288) StdErr (3F1ADD08)
Runtime Services 000000003F3FC318
Boot Services    000000003F3F4B00
SAL System Table 000000003FF22760
ACPI Table       000000003FFD9FC0
ACPI 2.0 Table   00000000000E2000
MPS Table        000000003FFD0000
SMBIOS Table     00000000000F0020
```

- To display memory contents from 1af3088 with size of 16 bytes:

```
Shell> mem 1af3088 16

Memory Address 0000000001AF3088 16 Bytes

01AF3088: 49 42 49 20 53 59 53 54-00 00 02 00 18 00 00 00 *IBI SYST........*

01AF3098: FF 9E D7 9B 00 00                               *......*
```

- To display memory mapped IO contents from 1af3088 with size of 16 bytes:

```
Shell> mem 1af3088 16 -MMIO
```

10.1.32 memmap

Displays the memory map maintained by the EFI environment.

```
MEMMAP [-b]
```

-b Display one screen at a time

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

> Examples:

- To display the system memory map:

```
    fs0:\> memmap
Type      Start      End          # Pages      Attributes
available  0000000000750000-0000000001841FFF  00000000000010F2 0000000000000009
LoaderCode 0000000001842000-00000000018A3FFF  0000000000000062 0000000000000009
available  00000000018A4000-00000000018C1FFF  000000000000001E 0000000000000009
LoaderData 00000000018C2000-00000000018CAFFF  0000000000000009 0000000000000009
BS_code    00000000018CB000-0000000001905FFF  000000000000003B 0000000000000009
BS_data    0000000001906000-00000000019C9FFF  00000000000000C4 0000000000000009   ...
RT_data    0000000001B2B000-0000000001B2BFFF  0000000000000001 8000000000000009
BS_data    0000000001B2C000-0000000001B4FFFF  0000000000000024 0000000000000009
reserved   0000000001B50000-0000000001D4FFFF  0000000000000200 0000000000000009
  reserved  :     512 Pages (2,097,152)
  LoaderCode:      98 Pages (401,408)
  LoaderData:      32 Pages (131,072)
  BS_code   :     335 Pages (1,372,160)
  BS_data   :     267 Pages (1,093,632)
  RT_data   :      19 Pages (77,824)
  available :   4,369 Pages (17,895,424)
Total Memory: 20 MB (20,971,520) 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 mv

Moves one or more files or directories to another location.

```
MV src [src...] [dst]
```

`src` Source file/directory name (wildcards are permitted)

`dst` Destination file/directory name (wildcards not permitted)

1. If the 'dst' parameter is not specified, the current directory is assumed to be the destination.
2. If there is more than one argument in the command line, the last one will be taken as 'dst' unconditionally. If there is more than one source file or directory to move, the 'dst' should be an existing directory.
3. Attempting to move a read-only file or directory is not allowed.
4. Moving a directory that contains read-only file(s) is allowed.
5. You cannot move a directory into itself or its subdirectories.
6. You cannot move a directory if the current directory is itself or its subdirectory.
7. Redirecting output to a file under a directory to be moved is not allowed.
8. If an error occurs, the remaining files or directories will still be moved.

> Examples:

- To rename a file:

```
fs0:\> mv IsaBus.efi Bus.efi
moving fs0:\IsaBus.efi -> \Bus.efi
 - [ok]
```

- To move a directory to the current directory:

```
fs0:\> mkdir test1\temp
fs0:\> mv test1\temp
moving fs0:\test1\temp -> \.\temp
 - [ok]
```

- To rename a directory:

```
fs0:\> mv efi efi1.1
moving fs0:\efi -> \efi1.1
 - [ok]
```

- To move multiple directories at a time:

```
fs0:\> mv test1 test2 test
moving fs0:\test1 -> \test\test1
 - [ok]
moving fs0:\test2 -> \test\test2
 - [ok]
```

- Moving a read-only directory will result a failure:

```
fs0:\test> attrib +r temp1
DA  R fs0:\test\temp1
fs0:\test> mv temp1 temp2
moving fs0:\test\temp1 -> \test\temp2
 - [error] - Write Protected
```

10.1.35 pause

Prints a message and waits for keyboard input.

```
PAUSE [-q]
```

-q Do 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:\>
```

10.1.36 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 numbers 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 VM6050:

- To display all PCI devices in the system:

```
VM6050> pci
   Seg  Bus  Dev  Func
   ---  ---  ---  ----
    00   00   00    00 ==> Bridge Device - Host/PCI bridge
              Vendor 8086 Device 006A Prog Interface 0
    00   00   01    00 ==> Bridge Device - PCI/PCI bridge
              Vendor 8086 Device 0045 Prog Interface 0
    00   00   06    00 ==> Bridge Device - PCI/PCI bridge
              Vendor 8086 Device 0047 Prog Interface 0
    00   00   16    00 ==> Simple Communications Controllers - Other communicati
              Vendor 8086 Device 3B64 Prog Interface 0
    00   00   16    01 ==> Simple Communications Controllers - Other communicati
              Vendor 8086 Device 3B65 Prog Interface 0
    00   00   16    02 ==> Mass Storage Controller - IDE controller
              Vendor 8086 Device 3B66 Prog Interface 85
    00   00   16    03 ==> Simple Communications Controllers - Serial controller
              Vendor 8086 Device 3B67 Prog Interface 2
    00   00   1A    00 ==> Serial Bus Controllers - USB
              Vendor 8086 Device 3B3C Prog Interface 20
    00   00   1C    00 ==> Bridge Device - PCI/PCI bridge
              Vendor 8086 Device 3B42 Prog Interface 0
    00   00   1C    04 ==> Bridge Device - PCI/PCI bridge
              Vendor 8086 Device 3B4A Prog Interface 0
    00   00   1C    06 ==> Bridge Device - PCI/PCI bridge
              Vendor 8086 Device 3B4E Prog Interface 0
    00   00   1D    00 ==> Serial Bus Controllers - USB
              Vendor 8086 Device 3B34 Prog Interface 20
    00   00   1E    00 ==> Bridge Device - PCI/PCI bridge
              Vendor 8086 Device 2448 Prog Interface 1
    00   00   1F    00 ==> Bridge Device - PCI/ISA bridge
              Vendor 8086 Device 3B07 Prog Interface 0
    00   00   1F    02 ==> Mass Storage Controller - IDE controller
              Vendor 8086 Device 3B2E Prog Interface 8F
    00   00   1F    03 ==> Serial Bus Controllers - System Management Bus
              Vendor 8086 Device 3B30 Prog Interface 0
```

```
    00   00   1F    05 ==> Mass Storage Controller - IDE controller
              Vendor 8086 Device 3B2D Prog Interface 85
    00   01   00    00 ==> Display Controller - VGA/8514 controller
              Vendor 1002 Device 94CB Prog Interface 0
    00   04   00    00 ==> Network Controller - Ethernet controller
              Vendor 8086 Device 150E Prog Interface 0
    00   04   00    01 ==> Network Controller - Ethernet controller
              Vendor 8086 Device 150E Prog Interface 0
    00   04   00    02 ==> Network Controller - Ethernet controller
              Vendor 8086 Device 150E Prog Interface 0
    00   04   00    03 ==> Network Controller - Ethernet controller
              Vendor 8086 Device 150E Prog Interface 0
    00   05   00    00 ==> Bridge Device - PCI/PCI bridge
              Vendor 10B5 Device 8112 Prog Interface 0
    00   06   09    00 ==> Bridge Device - Other bridge type
              Vendor 1059 Device 9035 Prog Interface 0
```

- To display the configuration space of Bus 0, Device 16, Function 0:

```
 VM6050> pci 0 16 0 -i -b
 PCI Segment 00 Bus 00 Device 16 Func 00 [EFI 0000160000]
  00000000: 86 80 64 3B 00 00 10 00-06 00 80 07 00 00 80 00  *..d;............*
  00000010: 04 60 60 F1 00 00 00 00-00 00 00 00 00 00 00 00  *.``............*
  00000020: 00 00 00 00 00 00 00 00-00 00 00 00 86 80 64 3B  *............d;*
  00000030: 00 00 00 00 50 00 00 00-00 00 00 00 0B 01 00 00  *....P...........*

  00000040: 05 02 11 EA 00 00 01 80-1F 00 0B 00 00 00 00 00  *................*
  00000050: 01 8C 03 C8 08 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000060: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000070: 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  *................*
  00000080: 00 00 00 00 00 00 00 00-00 00 00 00 05 00 80 00  *................*
  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 02 00 00 40  *...............@*
  000000C0: DA DA AB 31 43 73 B2 86-57 AF 74 FC 9B FC 20 04  *...1Cs..W.t... .*
  000000D0: 98 B5 AA D7 CD B6 F1 25-F8 0B 26 1E 0D B3 9D 55  *.......%..&....U*
  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): 8086                     Device ID(2): 3B64

Command(4): 0000
  (00)I/O space access enabled:       0  (01)Memory space access enabled:    0
  (02)Behave as bus master:           0  (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):     06                  BIST(0F):  Incapable
Cache Line Size(C): 00                  Latency Timer(D): 00
Header Type(0E):    80, Multi-function, PCI device
Class: Simple Communications Controllers - Other communication device -
```

```
Base Address Registers(10):
     Start_Address  Type  Space    Prefetchable?     Size             Limit
   ------------------------------------------------------------------------
  00000000F1606000  Mem   64 bits  No      0000000000000010  00000000F160600F
   ------------------------------------------------------------------------
Expansion ROM Disabled(30)

Cardbus CIS ptr(28):   00000000
Sub VendorID(2C):          8086      Subsystem ID(2E):      3B64
Capabilities Ptr(34):        50
Interrupt Line(3C):          0B      Interrupt Pin(3D):       01
Min_Gnt(3E):                 00      Max_Lat(3F):             00
```

10.1.37 ping

Usage:

```
Ping [-n count] [-l size] TargetIp
```

Options:

`-n count` Number of echo requests to send.

`-l size` Send buffer size.

The user has to enable “Network stack” in Advanced menu to have this command available.

10.1.38 reconnect

Reserved - Not To Be Used

10.1.39 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.

10.1.40 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
```

10.1.41 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

10.1.42 smbiosview

Displays SMBIOS information.

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

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

1. The SmbiosType parameter supports the following types:
   0 - BIOS Information
   1 - System Information
   3 - System Enclosure
   4 - Processor Information
   5 - Memory Controller Information
   6 - Memory Module Information
   7 - Cache Information
   8 - Port Connector Information
   9 - System Slots
   10 - On Board Devices Information
   15 - System Event Log
   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
   34 - Management Device
   37 - Memory Channel
   38 - IPMI Device Information
   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.
3. Internal commands:
   :q -------- quit smbiosview
   :0 -------- Change smbiosview display NONE info
   :1 -------- Change smbiosview display OUTLINE info
   :2 -------- Change smbiosview display NORMAL info
   :3 -------- Change smbiosview display DETAIL info
   /? -------- Show help

10.1.43 smbutil

EFI SMBUS Utility . NOT RECOMMENDED

Usage:

```
smbutil /rspd [/pec]
 smbutil /rdbyte Address Length Command [/pec]
 smbutil /rdword Address Length Command [/pec]
 smbutil /rdblock Address Length Command [/pec]
 smbutil /wtbyte Address Length Command /o Filename [/pec]
 smbutil /wtword Address Length Command /o FileName [/pec]
 smbutil /wtblock Address Length Command /o FileName [/pec]
 smbutil /testrw Address Length Command /o TestFileName [/pec]
   Address, Length, Command in HEX
```

`Address` is the device address on SMBUS

`Length` is the amount of data to transfer

`Command` is the offset to reach into the device

`wbyte wword wblock` will change and the EEPROM contents of the device. They are not RECOMMENDED and can cause a malfunction of the board.

`testrw` can corrupt the EEPROM contents of the device and can cause a malfunction of the board.

10.1.44 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.

10.2 Environment Variables

EFI shell allows user to set environment variables.

Actually, 3 environment variables are used on VM6050 board to control the behavior of EFI shell as described hereafter.

10.2.1 Bootcmd

The environment variable "`bootcmd`" allows user to run automatically a EFI command into EFI shell at startup of EFI shell without typing any command on keyboard.

> Examples:

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

```
VM6050> set bootcmd "pci"
```

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

```
VM6050> set
bootcmd: pci
```

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

```
VM6050> set -d bootcmd
```

10.2.2 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:

```
VM6050> set StartupAuto 1
```

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

```
VM6050> set -d StartupAuto
```

10.2.3 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:

```
VM6050> set StartupDelay 2
```

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

```
VM6050> set -d StartupDelay
```

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

Chapter 11 - BIOS Versions Description

11.1 Recommendations and Known Limitations

1. Reserved Setup settings

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 fresh Cold Boot 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. "`kflash`" command limitation

The "`-sp`" option of the "`kflash`" command is used to preserve the BIOS parameters. However the boot devices order is not preserved by this option.

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							
			11332	12044	12184	13078	13246	13281	14153	15202
1	3964	No video on XMC-G72 when plugged in XMC side slot								
2	3916	SATA speed for Gen1/Gen2	X							
3	-	PCH PCIe Port 8 is not enabled – Bugzilla 6493	X							
4	3998	VM6050 does not boot up to the BIOS/EFI prompt	X	X						
5	-	Double reset issue, board blocked – Bugzilla 6564	X	X						
6	4126	Critical Temperature Status not properly managed at low temperature	X	X	X					
7	-	The SATA speed Port 3 is set by default to 1.5 Gb/s for FDM-SATA device	X	X	X					
8	4066	Wrong VME sysreset management	X	X	X					
9	4141	Additionnal Graphic board on PCIe not detected as primary graphic display	X	X	X	X				
10	4183	Wrong value on Min Refresh Recover Time Delay tRFC in DDR3 SPD table	X	X	X	X	X			
11	-	Double refresh not set by default for RC board	X	X	X	X	X			
12	4202	Random reboot during a halt on Linux	X	X	X	X	X	X		
13	4225	COM2 serial line programmation error in BIOS PEI phase	X	X	X	X	X	X		
14	4226	I2C arbitration lost not managed	X	X	X	X	X	X		
15	4231	kuuid command erases some setup parameters	X	X	X	X	X	X	X	

11.2.2 Detailed description of the problems

Item # 1 No video on XMC-G72 when plugged in XMC side slot – CRP #3964

Description: Graphic XMC-G72 is not operational when it is plugged in the XMC side slot of the VM6050 board.

The XMC is detected and listed in the PCI devices list but there is no video output.

Workaround: This problem is fixed by the hardware E.C. Level 02034

Item # 2 SATA speed for Gen1/Gen2 – CRP #3916

Description: Some hard disk devices are not correctly recognized by BIOS. BIOS has to implement a setup option to select the SATA speed between GEN1 and GEN2 in order to work-around this limitation in case of the HDD has no mean to select the speed itself, for example with SSD devices.

Workaround: In AHCI mode, usually operating system re-negociate the SATA speed based on the capabilities registers. It is possible to force the SATA speed by using the `libata.force` option at the kernel command line to boot Linux.

Item # 3 PCH PCIe port 8 is not enabled – Bugzilla #6493

Description: The PCH PCIe Port #8 is not enabled and so the connection to the FPGA FMC is not operational.

Workaround: None

Item # 4 VM6050 does not boot up to the BIOS/EFI prompt – CRP #3998

Description: BIOS prompt is not available 5 out of 1000 power-on

Workaround: None

Item # 5 Double reset issue, board blocked – Bugzilla #6564

Description: The VM6050 CPU board is vulnerable to some reset timing.
If a second reset occurs in a period from 5 to 8 seconds after the first one, the board will reach a frozen state.

Workaround: The only solution to recover is to power cycle the system.

Item # 6 Critical Temperature Status not properly managed at low temperature - CRP 4126

Description: **1- Description: ACPI temperature overview:**

The ACPI returns the CPU Temperature to the OS as follows:

> CPU Temperature is the maximum temperature of all CPU IA cores

> CPU Temperature may be obtained from multiple sources, on Arrandale CPUs:

- Source 1: EC via PCH SMBus read if PCH SMBus thermal reporting is enabled
- Source 2: PCH MMIO Registers
- Source 3: Direct Comparison of CPU DTS temperature values from all Cores.

Source 1 and Source 2 need EC (Embedded Controller) that does not exist on our design.

So, the only method is Source 3. When Linux reaches the Critical Trip Point Critical, it initiates a shutdown, Trip Point can be set to a default value by BIOS, it is set to 100°C in Setup. This value is reported in ACPI under "Critical Trip Points" and for Arrandale CPU, this value is equal to 100°C.

2- Issue Analysis:

When the Processor is not able to perform the temperature computation or when the value is not valid, the ACPI returns to the OS a default value (Those default values are some ‘defines’ in the BIOS sources). This case occurs if the following MSR bits are reached those values:

> Case 1 : MSR 19Ch bit 31 = 0 => Reading Valid is not set

> Case 2 : MSR 19Ch bit 4 = 1 => Critical Temperature Status is set

The ‘case 1’ is a common problem below -15°C, we treated this issue during our board validation, all BIOS official release from ID11332 to ID12184 have the default value set to -56 °C.

The ‘case 2’ is not properly treated today, if this MSR bit is set, the temperature returned is 255°C, it is above the critical trip point, consequences: the OS initiates a shutdown.

Solution: BIOS returns - 56 °C as invalid temperature instead of 255°C for 'case 2'.

Workaround: None

Item # 7 The SATA speed Port 3 is set by default to 1.5 Gb/s for FDM-SATA device

Description: Some SATA II 3 Gb/s devices like FDM-SATA plugged on SATA Port 3 are not detected by BIOS.

Workaround: Set SATA speed for Port 3 to 1.5 Gb/s for those devices (see section 6.2 page 45).

Item # 8 Wrong VME sysreset management – CRP 4066

Description: VME sysreset from backplane to local reset is unmaskable, then, a VME sysreset will always generate a local reset despite the setting in VME BIOS (see section 5.8 page 38).
A local reset to VME sysreset is not propagated to the backplane if LOC2VME bit is not set in ALMA2f UTIL_RST register, this in spite of VME BIOS setting.

Workaround: To propagate local reset to VME bus, enable local to VME sysreset propagation in BIOS setup (see section 5.8 page 38) and set bit 0 UTIL_RST_LOC2VME in Alma register @ BAR+0x64 (UTIL_RST).

No workaround to mask VME sysreset propagation to local reset.

Item # 9 Additionnal Graphic Board on PCIe not detected as Primary Graphic Display – CRP 4141

Description: On XMC slot 1 of VM6050 an additional graphic card is never selected by BIOS as VGA display.

Workaround: Use XMC slot 2 instead of XMC slot 1.

Item # 10 Wrong value on Min Refresh Recover Time Delay tRFC in DDR3 SPD table – CRP 4183

Description: A wrong value has been noted in DDR3 SPD table on VM6050 board. Minimum Refresh Recover Time Delay (tRFC) has been set to 110 ns instead of 160 ns for 2 Gb DDR3 memory.

Workaround: Update BIOS with ID13281 and program SPD EEPROM using following command under BIOS prompt:

```
VM6050> smbutil /wtbyte A0 96 0
VM6050> smbutil /wtbyte A4 96 0
```

To check that SPD EEPROM are correctly programmed.

Read the EEPROM using following EFI shell command and check that the underlined result bytes are right:

- `VM6050> smbutil /rdbyte A0 20 0`

  Read Device at Address 0xA0:

  `0x92 0x10 0x0B 0x02 0x03 0x19 0x00 0x01 0x0B 0x52 0x01 0x08 0x0F 0x00 0x1E 0x00`

  `0x69 0x78 0x69 0x3C 0x69 0x11 0x2C 0x95 0x00 0x05 0x3C 0x3C 0x01 0x2C 0x82 0x05`

- `VM6050> smbutil /rdbyte A4 20 0`

  Read Device at Address 0xA4:

  `0x92 0x10 0x0B 0x02 0x03 0x19 0x00 0x01 0x0B 0x52 0x01 0x08 0x0F 0x00 0x1E 0x00`

  `0x69 0x78 0x69 0x3C 0x69 0x11 0x2C 0x95 0x00 0x05 0x3C 0x3C 0x01 0x2C 0x82 0x05`

Item # 11 Double refresh not set by default for RC board

Description: Double refresh is not set by default for RC board where DDR3 memory device can exceed temperature higher than 85°C. But DDR3 memory datasheet recommend to double the refresh cycle when the ambient temperature is higher than 85°C.

Workaround: Force double refresh for RC board (see section 6.4 - North Bridge & Memory Configuration page 48)

Item # 12 Random reboot after a halt on Linux – CRP 4202

Description: Depending on the Linux configuration, the board may restart after a halt command, due to a RTC wake-up event.

Workaround: Disable the RTC wake-up feature in BIOS setup to avoid restart after halt.

Item # 13 COM2 serial line programmation error in BIOS PEI phase – CRP 4225

Description: The BIOS programmation of the serial line COM2 is not correct just after reset and causes a 500ms pulse on TX2 signal at startup.

Workaround: None

Item # 14 I2C arbitration lost not managed – CRP 4226

Description: The BIOS does not manage the I2C Arbitration Lost, mainly on the 2 backplane I2C busses.

This can provoke errors when the PBIT system is run on a multiboard system or a system equipped with the Chassis Monitoring Board.

This management also requires a cPLD supporting the I2C multimaster feature (version 0xE at least).

Workaround: None

Item # 15 kuuid command erases some setup parameters – CRP 4231

Description: `kuuid` EFI utility command must not be used because some setup parameters are modified. If this command is used, then all parameters in Kontron menu and Advanced -> CPU Configuration menu previously set must be re-entered after using this command.

Workaround: Set UUID graphically using SETUP

11.3 BIOS ID12044 Release Notes

The identified or the fixed problems relative to this release are described in the section 11.2 - Known Problems Table page 110.

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

1. Watchdog under BIOS

The CPLD Watchdog function can be enabled with a configurable timeout value to control the OS boot.

The option is accessible in the Kontron/Board Misc Configuration menu under the BIOS Setup.

The watchdog timer is disabled by default.

Only the Reset mode is handled.

The watchdog setting is kept even after a timeout has occurred.

2. Azerty USB keyboard support

The USB French keyboard is now supported.

The option is accessible in the Kontron/USB Misc Configuration menu under the BIOS Setup.

The US keyboard is set by default.

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

3. Support of new PXE version

The Legacy Option ROM for the i82580 (Barton Hills) has been updated.

This fixes a potential problem with the EEPROM reset.

11.4 BIOS ID12184 Release Notes

The identified or the fixed problems relative to this release are described in the section 11.2 - Known Problems Table page 110.

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

1. Evolution Serial IRQ protocol mode

The Serial IRQ protocol mode is now set by default to the Continuous mode instead of the Quiet mode to give priority to the operational speed instead of power consumption. Also, compatibility with other Kontron Arrandale platforms is kept.

2. This release includes the PBIT software(*) V2.0 ID12180 implementing a new test at system level.

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

   For more information, please contact your field representative.

11.5 BIOS ID13078 Release Notes

The identified or the fixed problems relative to this release are described in the section 11.2 - Known Problems Table page 110.

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

1. **PBIT Evolution**

   A new PBIT version is included into BIOS 13078 with the following evolution

   PBIT v2.3 ID13078:

   - System test completed to check CPLD information, SETUP crc, SMBUS scan, PCI device ID, PCIe Bridge width and speed link
   - Added system_edit command Menu
   - Added kdiag deleteall command
   - kdiag loop mode behaviour improvement
   - kdiag promptonfail on loop mode corrected
   - Correction on PBIT result status in write protect mode on EEPROM
   - Test CPLD (debug mode enabled + correction delay in watchdog test)
   - Memory test correction when logging faulty addresses
   - Command behaviour modification: kdiag cfg “runflag” => it just modify the flag of current test list instead of adding all the missing test in “runflag” mode
   - Reset type is supported in PBIT execution mode (WARM, COLD)
   - Correction of bug on command with clearstatus + test num
   - Add feature to be able to activate pbit with a key
   - Serial rate test: avoid dividing by zero (if rate is zero) and improve line state restoring.
   - Endurance test in loop mode corrected

2. **Enhancement:**

   Add warnings when saving setup if the CPU frequency or Turbo mode is not suitable with the board class (WA, RA, RC)

3. **Add Display Hot Plug feature** to enable/disable Hot plug IT for CRT/DP/HDMI/DVI (see chapter 6.3 page 46)

11.6 BIOS ID13246 Release Notes

The identified or the fixed problems relative to this release are described in the section 11.2 - Known Problems Table page 110.

This release is produced for CRP #4141 correction.

The PBIT release V2.3 ID13078 is unchanged.

11.7 BIOS ID13281 Release Notes

The identified or the fixed problems relative to this release are described in the section 11.2 - Known Problems Table page 110.

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

1. Updates the SPD table for the DDR3 2Gb components.
2. Adds support to double the DDR3 refresh rate for the extended temperature range (above +85°C). New option in the North Bridge menu.
3. Includes PBIT(*) V2.4 ID13280 that improves the system test management: new system_edit menus and choice for prints and error reporting added.

(*) 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 ID14153 Release Notes

The identified or the fixed problems relative to this release are described in the section 11.2 - Known Problems Table page 110.

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

1. Fixed CRP #4202/Bug #7104: Random reboot after a halt on Linux.

   New option "Wake system from S5" added in Advanced setup menu to enable/disable the RTC wakeup event in S5 sleep state after Linux "`halt`" command.

2. Fixed CRP# 4225/Bug #7069: COM2 serial line programmation error in BIOS PEI phase.

   Wrong TX2 polarity for COM2 at reset. Set TX2 polarity to high level (inactive) when IR MUX is selected for UART2 mode in SMSC1007 device.

3. Fixed CRP #4226/Bug #7009: I2C arbitration lost not managed

   
   This feature requires at least CPLD version 0xE.
   Without this CPLD version, I2C multi-master is not supported by hardware.

4. Fixed Bug #7050: i82580 EEPROM write protection.

   BIOS controls the i82580 EEPROM write protection but with a wrong board switch. So the EEPROM is effectively write protected by the hardware but the BIOS still tries to write.

5. BIOS change due to CPLD CRP #4206/Bug #6878 fix: glitches on serial lines at power-on and reset.

   CPLD version 0xE fixes this issue and DXEN signal defaults to 0 but to enable debug messages on COM1 serial console, the BIOS has to program COM1 transmit enable in CPLD register 0x07 very early in the code.

   
   In RESCUE Flash or with FACTORY mode enabled, the CPLD drives the DXEN signal to 1 automatically.

6. `kmac` EFI command added: mainly used to read/write MAC addresses in i82580 EEPROM.

   
   "`prog`" option not tested on a blank EEPROM.

BIOS ID14153 also includes the PBIT software(*) V2.5 ID14146 with the following changes:

1. PBIT system test evolution (following fixed CPLD bug #6926 and BIOS bug #7009)

   Only probe backplane SMBus0: only I2C board addresses (range 0x18 to 0x2C). Don't probe Chassis Monitoring Board at 0x6F.

   Probing customer devices at other addresses or connected on SMBus1 may cause malfunction.

2. Misc: add the number of each test listed in the "`kdiag stat`" output.

(*) 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 ID15202 Release Notes

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

BIOS update:

- Supports new Flash type N25Q032.
- Fixes CRP#4231: `kuuid` command erases some setup parameters. `kuuid` EFI utility command must not be used because some setup parameters are modified.

  If this command is used, then all parameters in Kontron menu and Advanced -> CPU Configuration menu previously set must be re-entered after using this command.
- Fixes Bug#7201: VME Geographical address register not set correctly. VME conflit may occurs on VME bus if the operating system does not take care of it.
- Enhancement: Updates Intel Microcode from 0x2 to 0x4 for Arrandale processor.
- Fixes Bugzilla#7139: Board configuration is not always applied immediatly after setup is updated.
- Enhancement: Sets default boot timeout to 0 instead of 2th of second.
- Fixes bug #7182: SPI Flash protection does not work (correction concerns `kflash` and `krconfig` command).

Information on Flash Write Protect:

- The flash write protect is effective after the next boot following the switch SW1-3 activation. This is because the non-volatile Flash lock bits are set by software during the BIOS boot phase.

BIOS ID15202 also includes the PBIT software(*) V2.6 ID15190 with the following changes:

- Adds `kdiag` bypass option
- Bug #7198 - Problem with `normalreset`/`poweronreset` option status: status information is now taken from CPLD.
- Bug #7132 - PBIT learn system: the number of detected devices is not correct.
- Bug #7133 - PBIT edit system: if SMBUS is ignored, "`unknown type in constructor`" messages are displayed
- Bug #7168 - PBIT test pmcA_xmc_check(76) fails 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.

Chapter 12 - Use Cases

This chapter gives some advise for following pratical cases:

> DEPLOY : How to deploy VM6050 - BIOS, section 12.1 page 122

> DEVEL: How to develop applications with VM6050 - BIOS, section 12.2 page 123

> EVAL: How to benchmark VM6050 - BIOS, section 12.3 page 123

> TROUBLESHOOT: How to troubleshoot VM6050 - BIOS, section 12.4 page 123

12.1 DEPLOY: How to deploy VM6050 - BIOS

Deploying with VM6050 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 VM6050 with another one in a system, cloning allows to duplicate VM6050 settings in the new board prior to replacement. This is how to proceed with VM6050:

> On Original VM6050

Duplicate the hardware settings. (see VM6050 Users Documentation: “Configuration” chapter)

Duplicating BIOS settings:

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

> New VM6050

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

See Annex A 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 of the initial VM6050.

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 FLASH mezzanine or HDD fitted on the board, refer to VM6050 User's Guide (CA.DT.A93) for details on 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 VM6050:

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

See chapter 2.2 of VM6050 User's Guide about the board identifcation labels.

See section 5.3 page 28 on VPD into SETUP Kontron Menu in this document on where to retrieve the board SN and EC level using the BIOS

See VPDTool in the Linux BSP document on 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 software table in memory, use the **`dmidecode`** command to retrieve this information from Linux.

Kontron maintains a database of all 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 VM6050 - BIOS

TBD

12.3 EVAL: How to benchmark VM6050 - BIOS

TBD

12.4 TROUBLESHOOT: How to troubleshoot VM6050 - BIOS

» SETUP not accessible

If setup is not accessible, make sure the board is operational in rescue mode (see VM6050 User'sGuide for Rescue Boot).

» SETUP accessible but OS not booting

If setup can be accessed, then enter setup (see chapter 2 page 2 ”Accessing the Setup Menu”) and check if the boot device is visible in the boot device list. See chapter 7 page 50 “Boot Method and Priority” in this document

Eventually restore default manufacturing setup configuration. See chapter 9 page 61 “Save and Exit Menu” to restore setup.

Appendix A - How to Update and Restore BIOS

A.1 Update BIOS from UEFI Shell using USB device

This section details the update of the AMI BIOS Firmware on a VM6050 board. An USB key with the BIOS image to flash will be used.

Operating Mode

> Copy the BIOS image under the USB device

> Boot VM6050 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 `VM6050_IDYYXXX.bin` then flash the BIOS entering command

```
VM6050 > kflash -p -r  VM6050_IDYYXXX.bin
```

Do not turn off nor reset the board before the end of the command. Otherwise, this could prevent the system to boot at next power on.

> Wait for about 1 minute and 30 seconds and check if the message "`image are equal`" is displayed. If not, proceed with the flash update again. When update is finalized without any errors, then turn off the system and do a fresh cold start in order to boot with the new BIOS.

Unlike the graphical screen, the serial console displays a toolbar [======] during the Flash process to show the progress of the Flash update.

A.2 Restore or Update BIOS from Rescue BIOS

A rescue BIOS is available on each VM6050 CPU. It is possible to boot on the rescue BIOS and to update the main BIOS with the rescue BIOS.

When the 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 VM6050-RESCUE.

> Enter command:

```
VM6050-RESCUE> kflash -c
```

Do not power down the board during the update process. Otherwise, this could prevent the board to boot.

> The command lasts around 1 minute and 30 seconds. Then 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 VM6050 board. A USB key will be used to store the BIOS image

Operating Mode

> Boot VM6050 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:
```

> If necessary use cd command to reach a directory where the Bios image is stored. Use ls to display file list

If BIOS image is named `VM6050_CLONE.bin` then copy the BIOS image entering command

```
VM6050> kflash -s  VM6050_CLONE.bin
```

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

MAILING ADDRESS
Kontron Modular Computers S.A.S.
150 rue Marcelin Berthelot - BP 244
ZI TOULON EST
83078 TOULON CEDEX - France

TELEPHONE AND E-MAIL
+33 (0) 4 98 16 34 00
Sales: Order-ATD-Toulon@Kontron.com
Support: GSS-ATD-Toulon@Kontron.com

For further information about other Kontron products, please visit our Internet web site: www.kontron.com.