USER REFERENCE MANUAL

VX305x AMI BIOS

SD.DT.G50-5e - January 2018

POSSIBILITIES START HERE kontron

VX305x AMI BIOS User Reference Manual

Disclaimer

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

Kontron S&T AG

Lise-Meitner-Str. 3-5

86156 Augsburg

Germany

REVISION HISTORY

PUBLICATION TITLE:	VX305x AMI BIOS User Reference Manual	
DOC. ID:	SD.DT.G50-5e	
Revision	Brief Description of Changes	Date of Issue
5e	New BIOS ID17347 New sections: - 12.7 BIOS ID17347 Release Notes Updated sections: - 11 EFI Shell - 12.2 Known Problems Table	01-2018
4e	New BIOS ID17185 New sections: - 2.1 SETUP Menu - 2.2 Boot Manager Menu - 12.6 BIOS ID17185 Release Notes Updated sections: - 6.1.6 Watchdog Configuration - 11.1.7 kvpx - 12.1 Recommendations and Known Limitations - 12.2 Known Problems Table	07-2017
3e	New BIOS ID16182 New section: 12.2 Known Problems Table	07-2016
2e	New BIOS ID16133	05-2016
1e	Initial Issue	03-2016
0e	Preliminary version	02-2016

Customer Support

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

Customer Service

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

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

Customer Comments

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

SYMBOLS

The following symbols may be used in this manual:

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

FOR YOUR SAFETY

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

High Voltage Safety Instructions

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

⚠CAUTION

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

⚠CAUTION

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

Special Handling and Unpacking Instructions

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

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

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

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

GENERAL INSTRUCTIONS ON USAGE

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

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

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

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

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

ENVIRONMENTAL PROTECTION STATEMENT

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

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

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

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

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

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

TERMS AND CONDITIONS

Kontron warrants products in accordance with defined regional warranty periods. For more information about warranty compliance and conformity, and the warranty period in your region, visit http://www.kontron.com/terms-and-conditions

Kontron sells products worldwide and declares regional General Terms & Conditions of Sale, and Purchase Order Terms & Conditions. Visit http://www.kontron.com/terms-and-conditions

For contact information, refer to the corporate offices contact information on the last page of this user guide or visit our website CONTACT US.

Table Of Contents

1 / Overview

This manual introduces the SETUP and the additional EFI Kontron commands of the AMI BIOS firmware available on Kontron VX305x boards.

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

- Date & Time
- Serial Port, Terminal Type, Console redirection
- USB keyboard layout
- Watchdog for OS boot
- LAN routing, VPX configuration
- CPU active cores
- Boot method and boot device priority
- Security password

1.1 Structure

- Chapter 1 . . . . . "Overview"
- Chapter 2 . . . . . Enter the SETUP Menu
- Chapter 3 to Chapter 10 . . . "Sampling of menu items"
- Chapter 11 . . . . . "EFI SHELL"
- Chapter 12 . . . . . "BIOS Versions Description"
- Chapter 13 . . . . . "Use Cases"

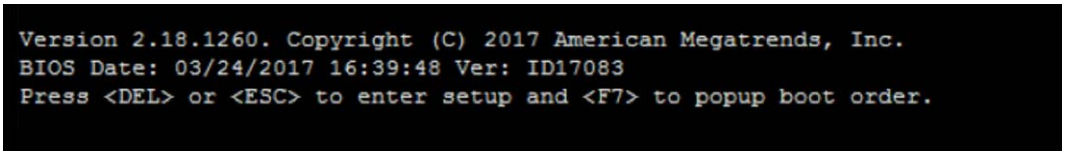
1.2 Related Documents

- VX305x User's Guide CA.DT.B25

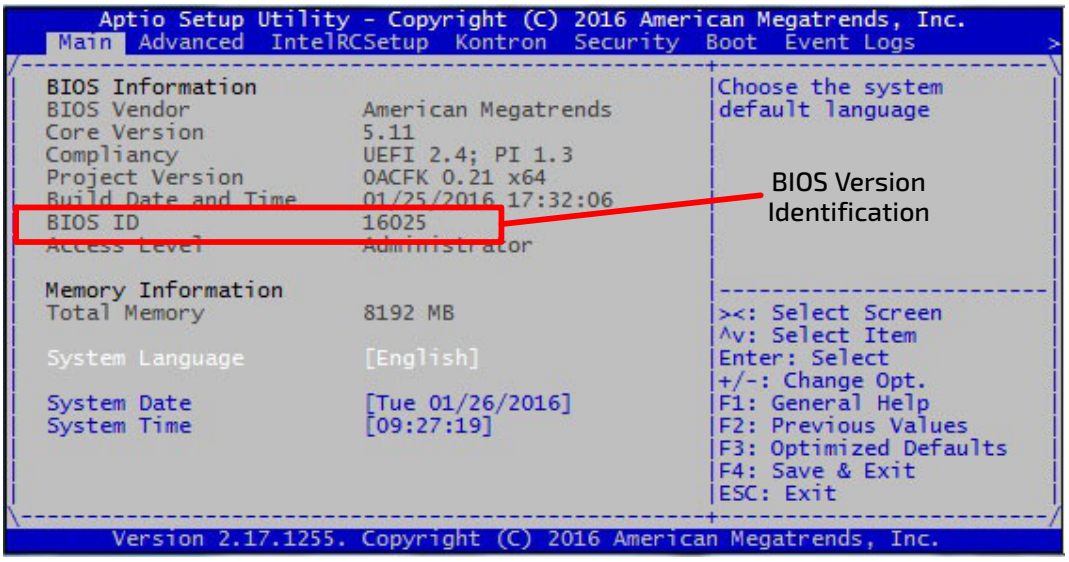
2 / Enter the SETUP

2.1 SETUP Menu

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



A screen similar to the one shown below will appear:



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

To get the SETUP menu from COM0 serial line, configure your terminal to 115200 baud. COM0 is available either via the front panel or via the backplane connector of the VX305x board.

The following chapter details the items that are available on Kontron VX305x. 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:

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.

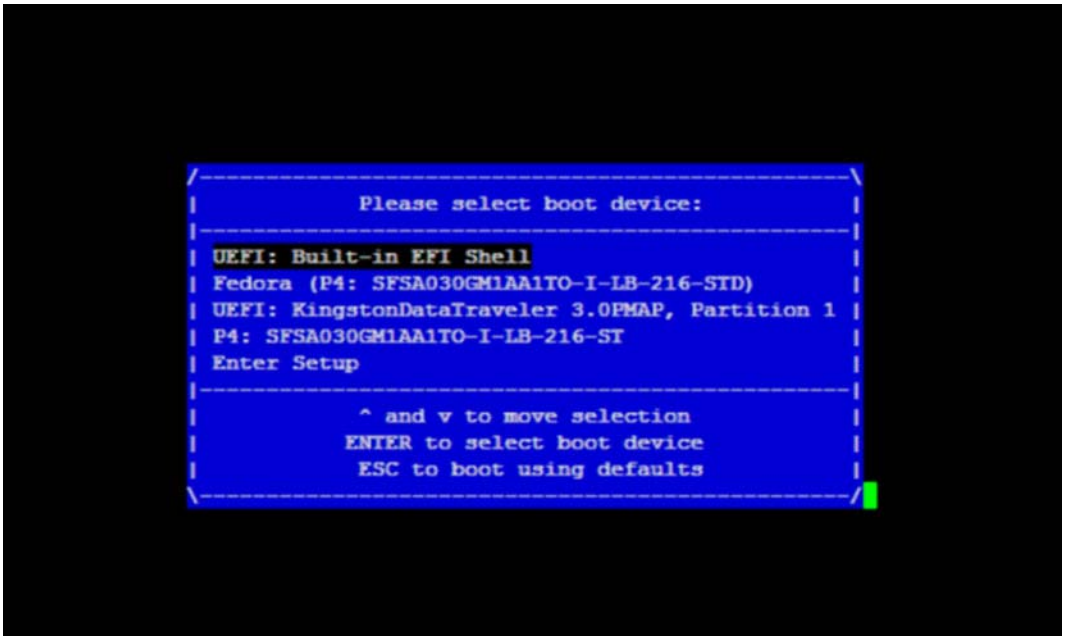
While the menu item is highlighted, its corresponding Help text is also displayed to help explain the purpose of the item.

- 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.

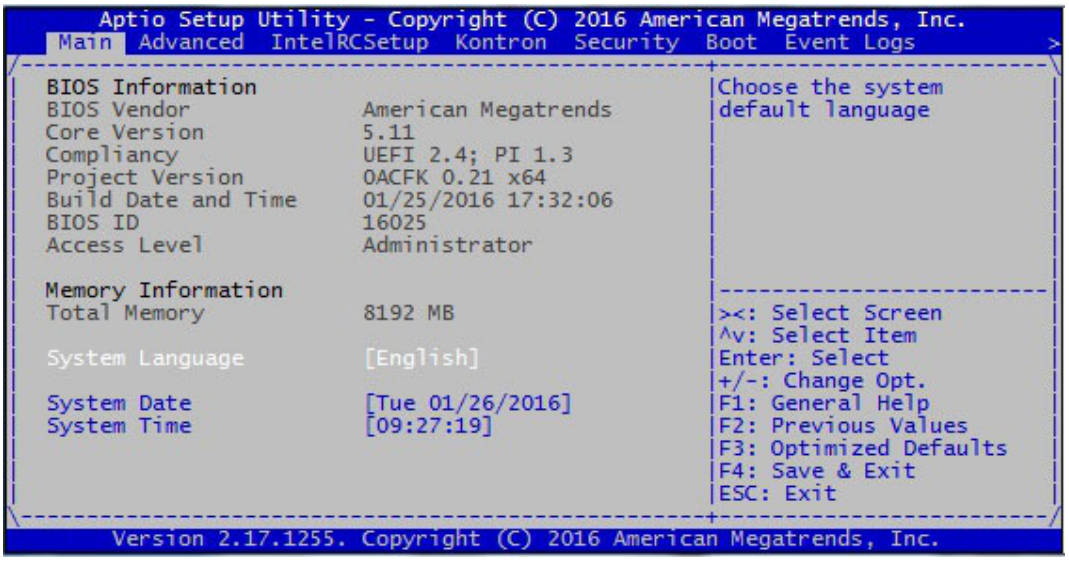
The Boot Manager menu is used to select the boot device.



Select a device from the list (Use the < ↑ > or < ↓ > to highlight the desired item).

Press < ENTER > to boot the selected device or enter the Setup Menus.

3 / Main Menu



The Main Menu is the first accessible setup page and provides BIOS information as the **BIOS ID** to identify the BIOS version and the **Build Date and Time**.

The total of initialized memory is also displayed.

Only English is supported as **System Language** in this version.

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

Time is represented in a 24-hour format.

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

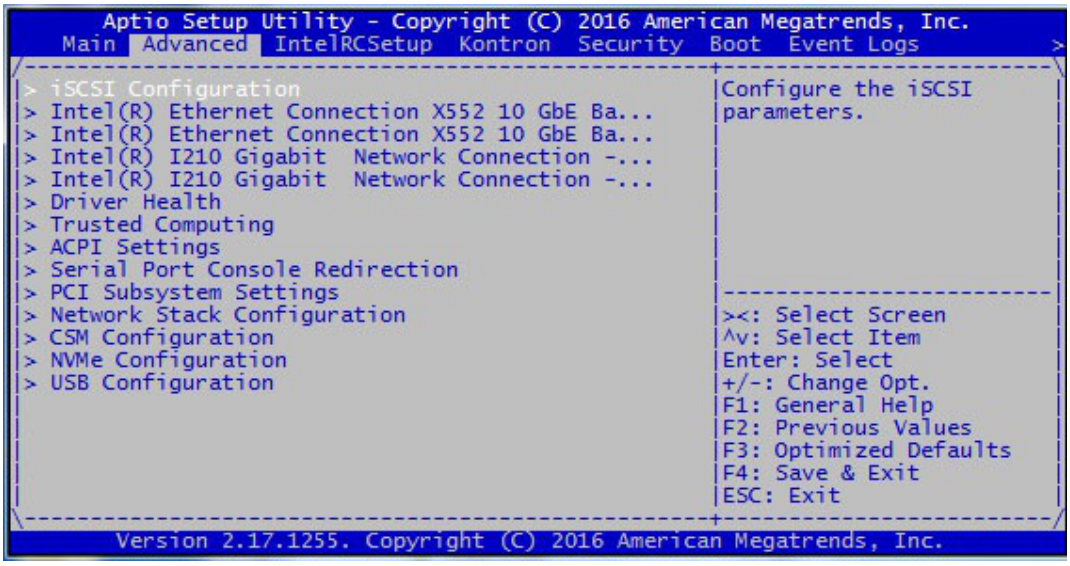
To update the **System Time**, use the <+> or <-> keys to select the Hour (<+> to increase / <-> to decrease the hour), and press the <Enter> key to validate your choice. Proceed in the same way for the minutes and finally for the seconds.

BIOS always reads a Real Time Clock to display the date and the time at each power-on.

To keep the current date and time, the RTC must be supplied by an external battery.

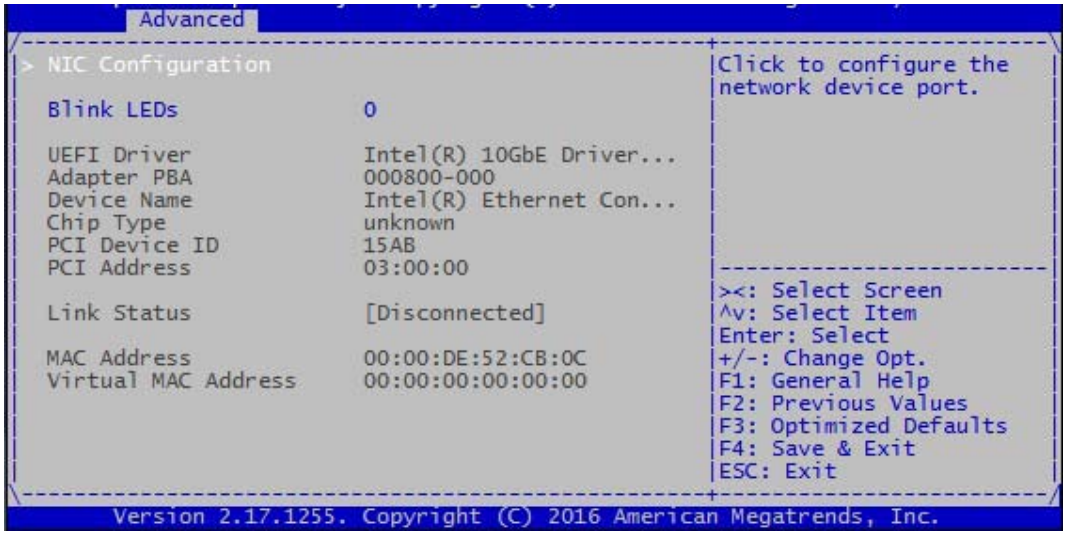
However, the VX305x board can operate safely without any battery fitted. In this case, the BIOS non-volatile settings and the user settings are stored in a specific area of the BIOS SPI Flash. The date/time are lost at each power-down and the BIOS initializes the RTC with the BIOS build date/time.

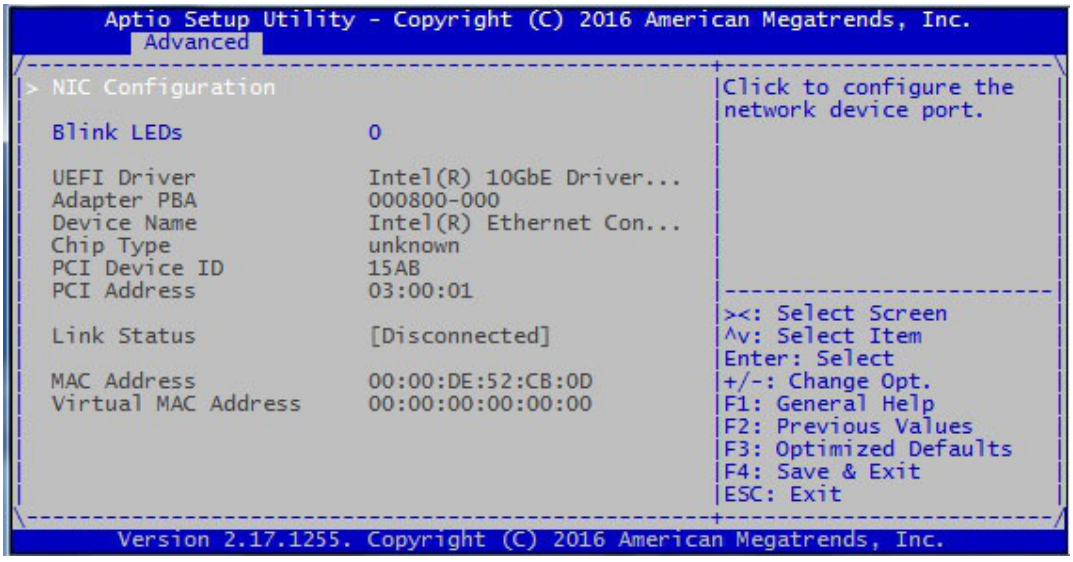
4 / Advanced Menu

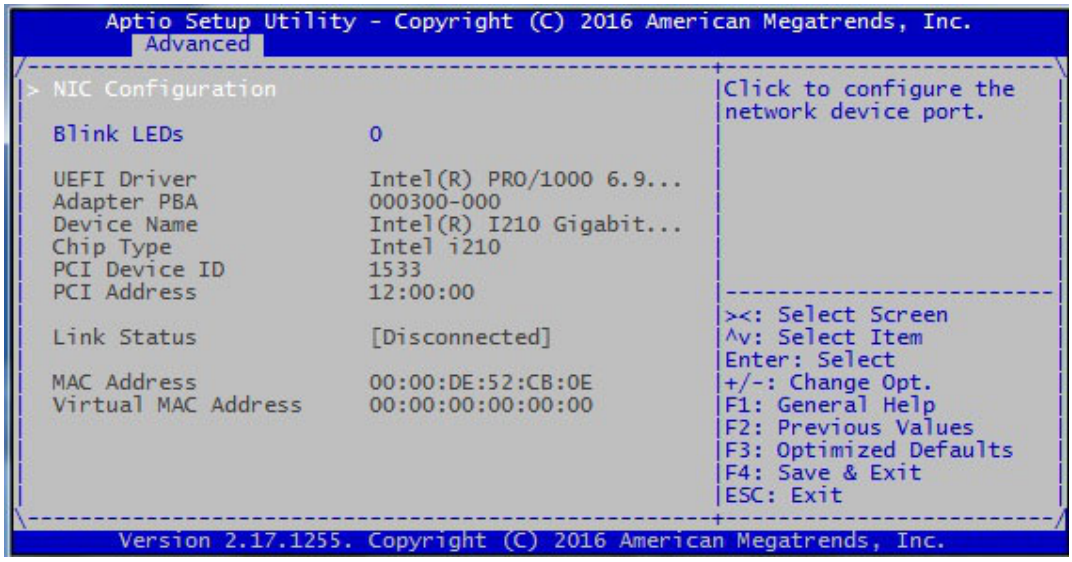


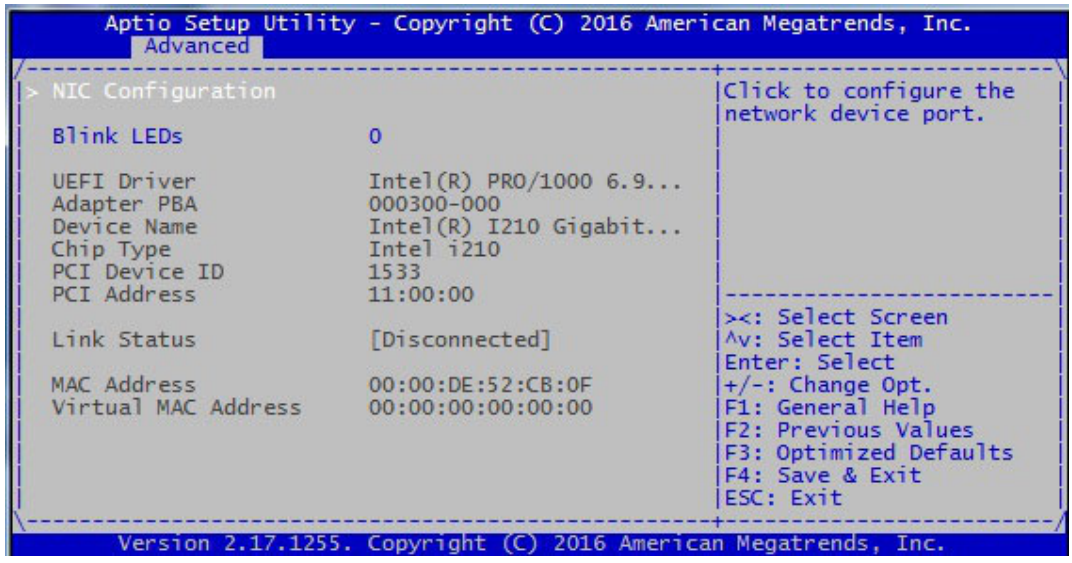
The Advanced menu provides information about the Ethernet interfaces of the board: the two 10GbE backplane interfaces of the X552 controller and the 1GbE interfaces of the two i210 controllers.

The corresponding forms display information as the **`Hardware MAC address`** and the **`PCI address`** or **`PCI device ID`** (also returned by the **`pci`** EFI shell command):




Aptio Setup Utility - Copyright (C) 2016 American Megatrends, Inc.
Advanced
> NIC Configuration
Blink LEDs 0
UEFI Driver Intel(R) 10GbE Driver...
Adapter PBA 000800-000
Device Name Intel(R) Ethernet Con...
Chip Type unknown
PCI Device ID 15AB
PCI Address 03:00:01
Link Status [Disconnected]
MAC Address 00:00:DE:52:CB:0D
Virtual MAC Address 00:00:00:00:00:00
Click to configure the network device port.
><: Select Screen
^v: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.17.1255. Copyright (C) 2016 American Megatrends, Inc.


Aptio Setup Utility - Copyright (C) 2016 American Megatrends, Inc.
Advanced
> NIC Configuration
Blink LEDs 0
UEFI Driver Intel(R) PRO/1000 6.9...
Adapter PBA 000300-000
Device Name Intel(R) I210 Gigabit...
Chip Type Intel i210
PCI Device ID 1533
PCI Address 12:00:00
Link Status [Disconnected]
MAC Address 00:00:DE:52:CB:0E
Virtual MAC Address 00:00:00:00:00:00
Click to configure the network device port.
><: Select Screen
^v: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.17.1255. Copyright (C) 2016 American Megatrends, Inc.


Aptio Setup Utility - Copyright (C) 2016 American Megatrends, Inc.
Advanced
> NIC Configuration
Blink LEDs 0
UEFI Driver Intel(R) PRO/1000 6.9...
Adapter PBA 000300-000
Device Name Intel(R) I210 Gigabit...
Chip Type Intel i210
PCI Device ID 1533
PCI Address 11:00:00
Link Status [Disconnected]
MAC Address 00:00:DE:52:CB:0F
Virtual MAC Address 00:00:00:00:00:00
Click to configure the network device port.
><: Select Screen
^v: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.17.1255. Copyright (C) 2016 American Megatrends, Inc.

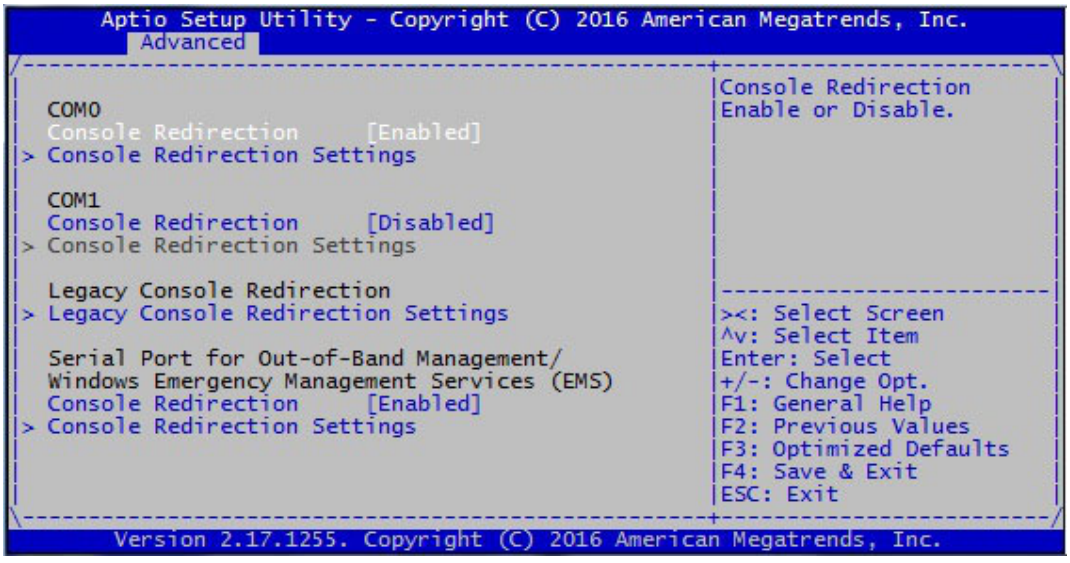
The Advanced setup page also provides configuration menus as:

- Serial Port Console Redirection - Section 4.1 page 7
- CSM Configuration - Section 4.2 page 9
- USB Configuration (Legacy support) - Section 4.3 page 10

The other submenus should NOT be modified

4.1 Serial Port Console Redirection

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



4.1.1 COM0/COM1 Console Redirection

COM0 is the serial line available on the front panel or at rear of the VX305x.

COM1 is only available at rear.

Without graphic option, it is necessary to enable the **Console Redirection** on one serial line to access the BIOS setup and the EFI shell.

Console Redirection may be enabled or disabled on each serial line independently.

By default the redirection is enabled on COM0 and disabled on COM1.

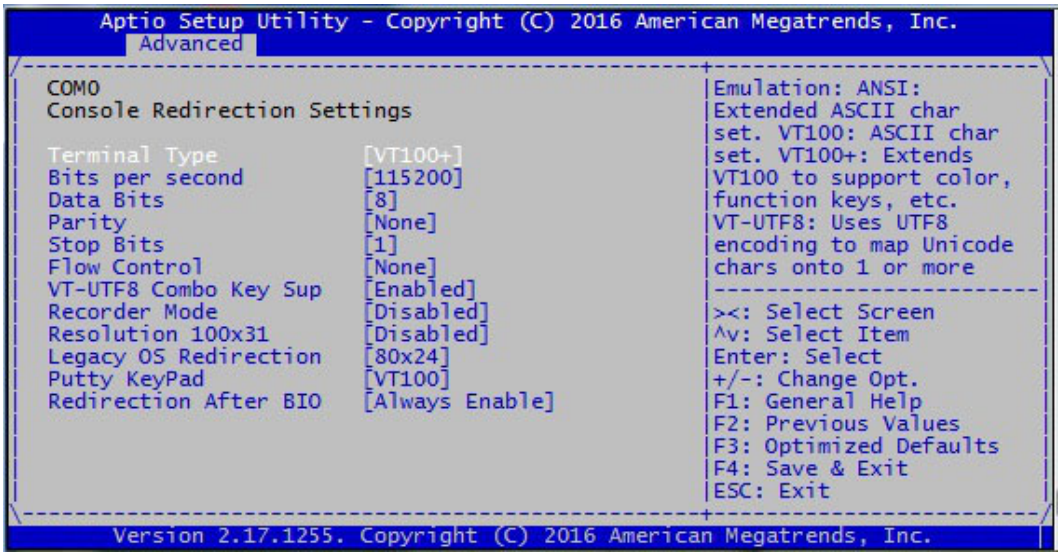
To display the PXE messages on the COM1 serial line instead of COM0, change the **Legacy Serial Redirection** option to **COM1** in the **Legacy Console Redirection Settings** submenu.
However, OS will need to use this line as console also.

4.1.2 COM0/COM1 Console Redirection Settings

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

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

This shows the default settings:

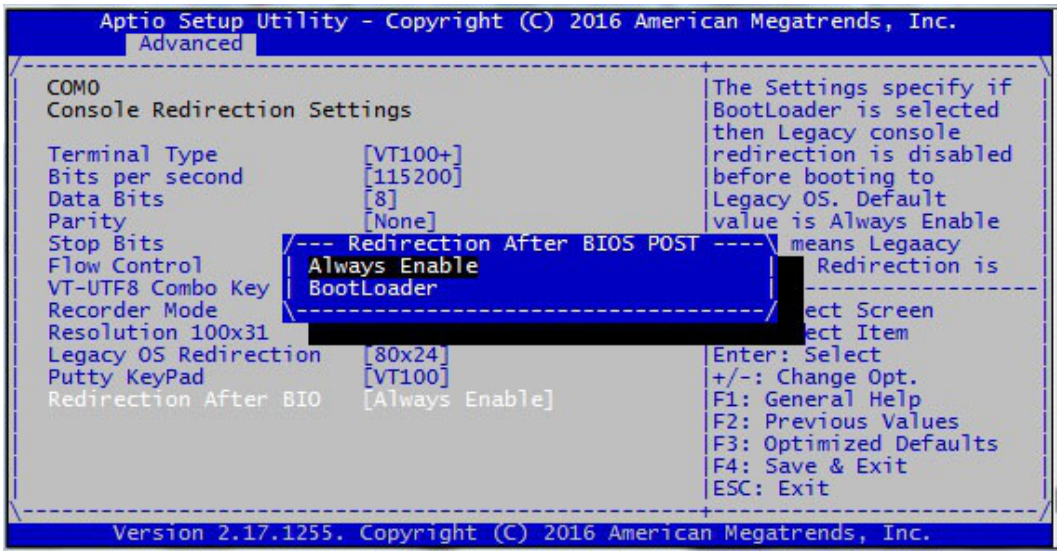


The **`Redirection after BIOS`** option is used to keep or disable the legacy console redirection before booting OS.

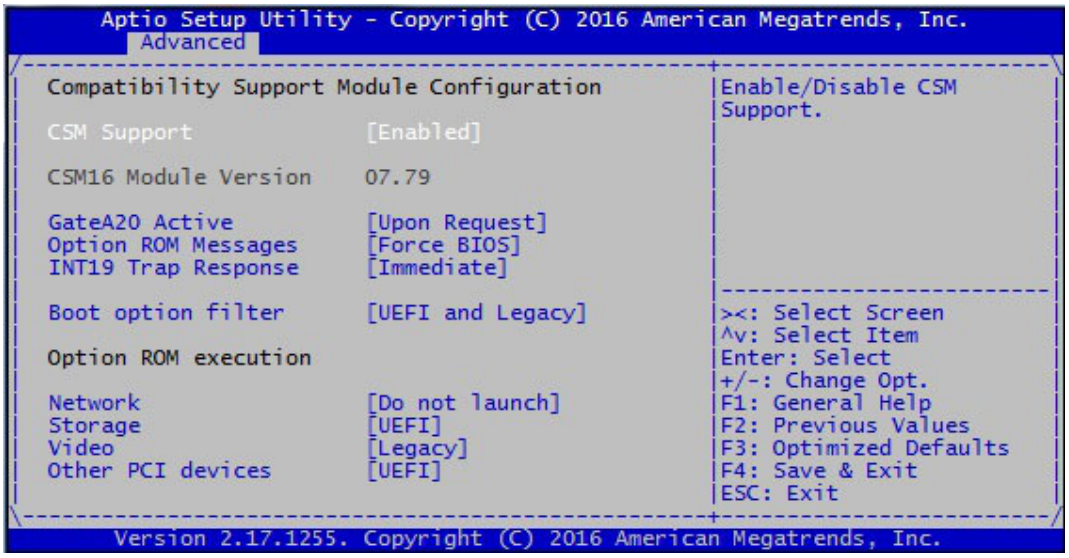
For example, set the option to **`Bootloader`** (default value) if Grub bootloader is booted to prevent any double display on the serial line.

Thus, only the bootloader will control the line.

If PXE boot is used, you must set the option to **`Always Enable`** to get the PXE boot messages.

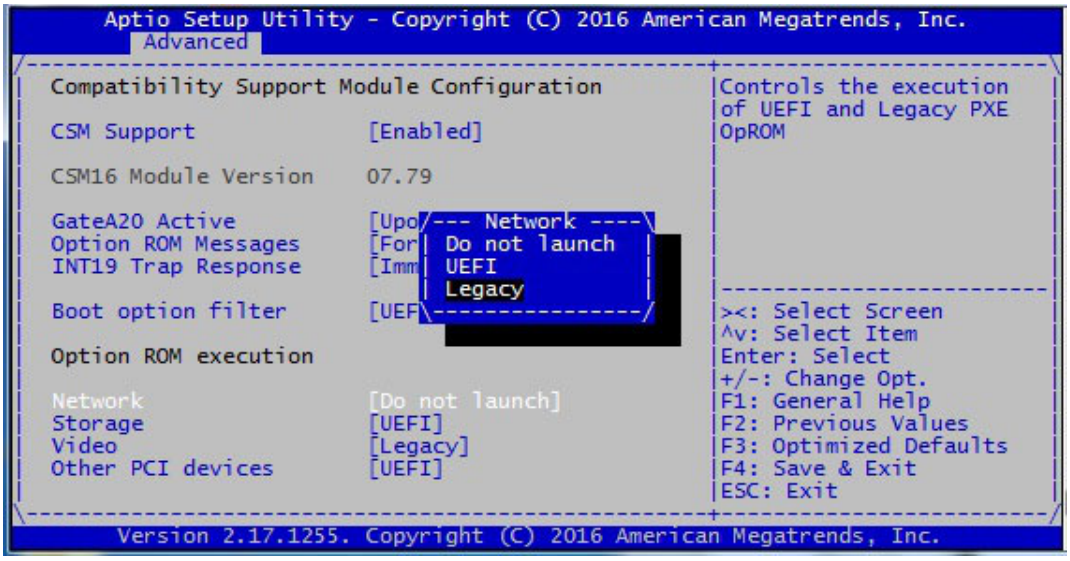


4.2 CSM Configuration



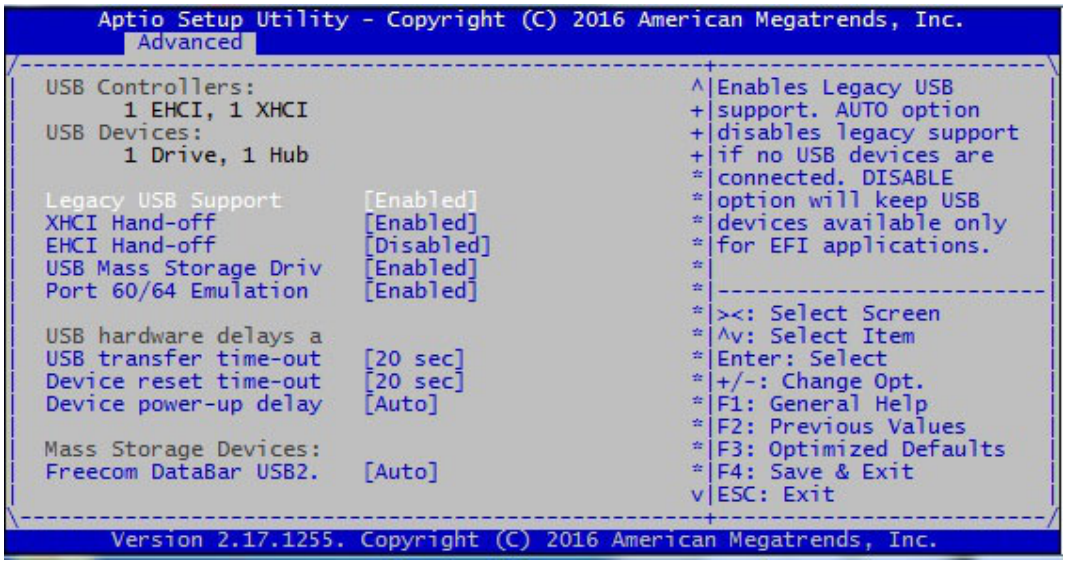
The **Network option** is used to enable/disable the execution of the network device OpROMs.

Set the option to **Legacy** to enable PXE boot.



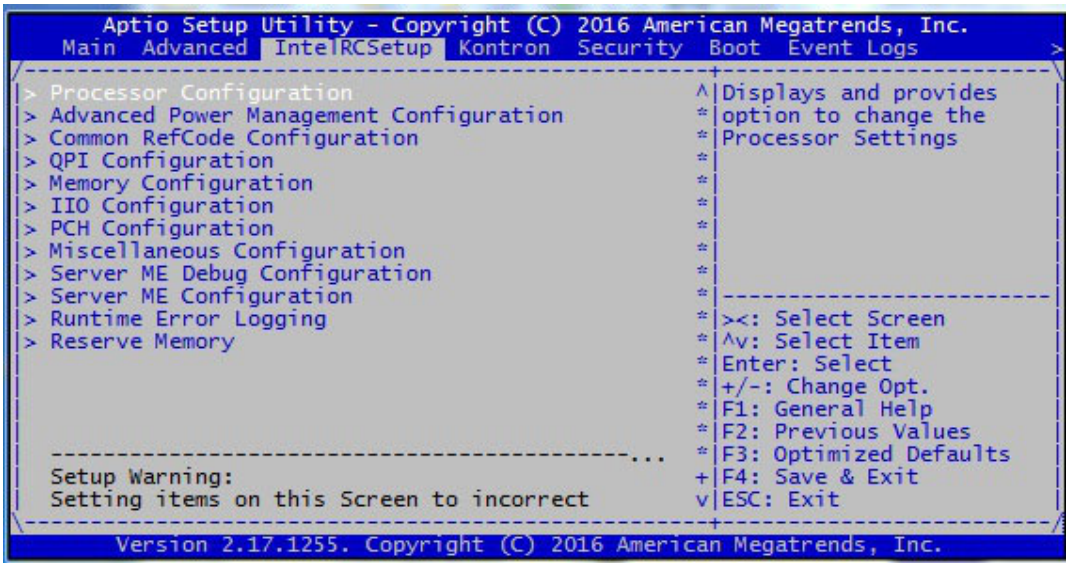
4.3 USB Configuration

This menu is used to enable/disable the **Legacy USB Support** (such as DOS legacy environment) and avoid boot from a USB device.



The other options should not be changed.

5 / IntelRCSetup Menu

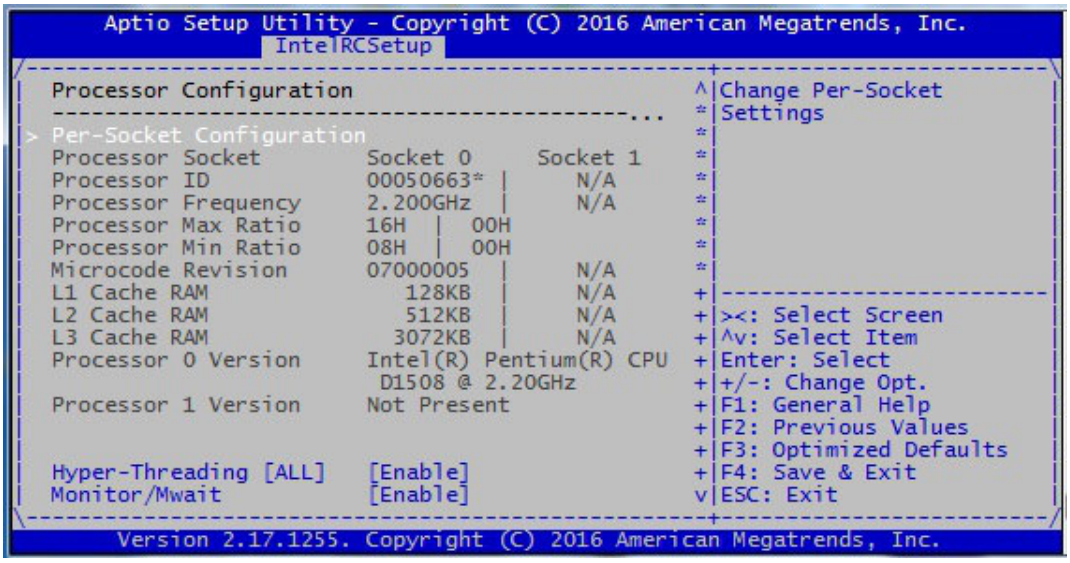


The following chapters describe the settings tested on VX305x.
All the other settings should not be modified to prevent malfunction.

5.1 Processor Configuration

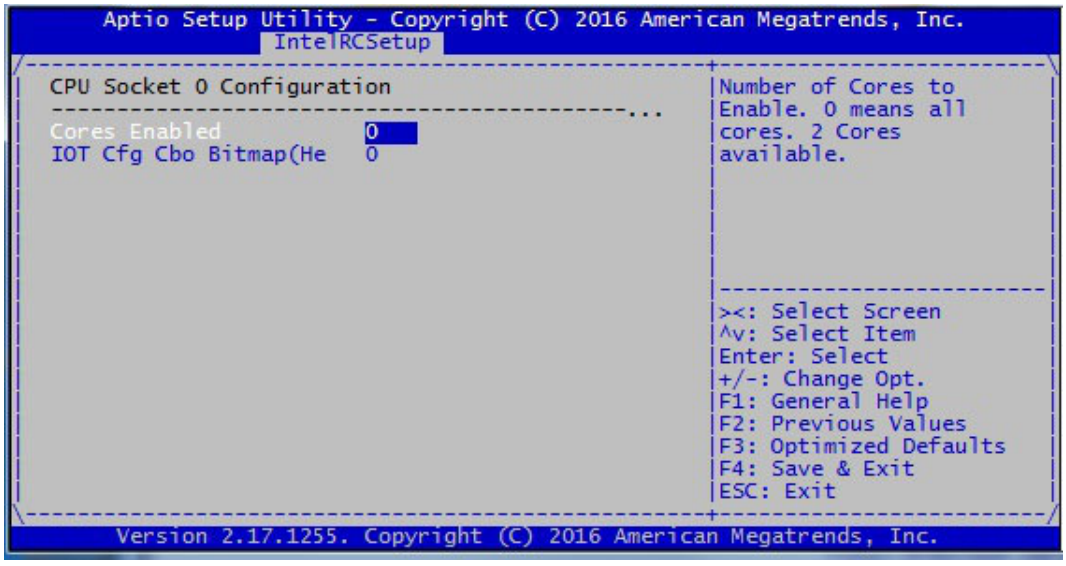
This menu displays the CPU configuration.

On VX305x boards, only one socket (0) is equipped.

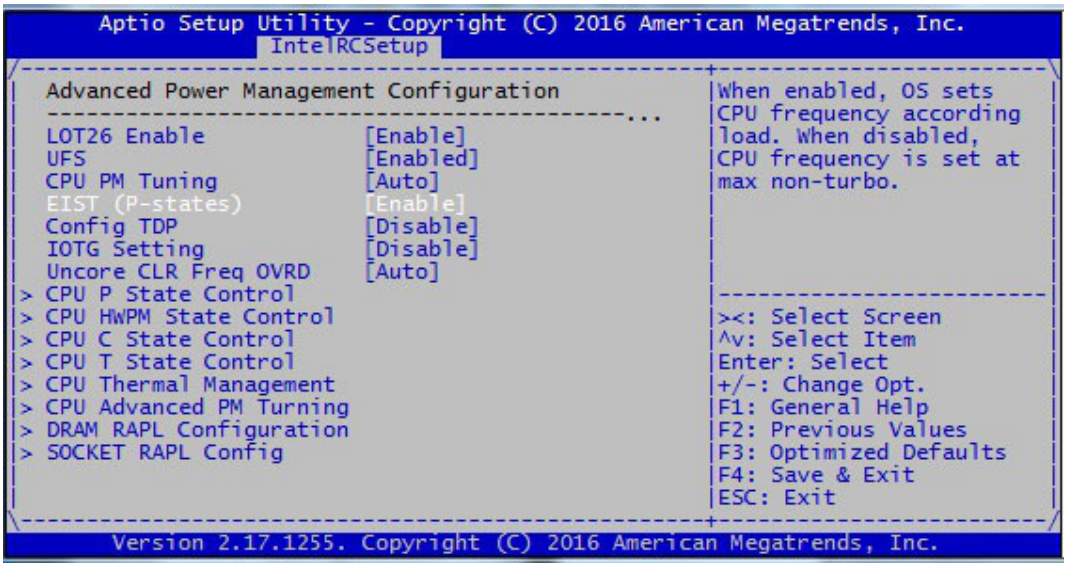


The **Hyper-Threading** option is used to enable/disable the logical processor threads globally (2 logical threads per core).

In the **Per-Socket Configuration** submenu for socket 0 , the **Cores Enabled** option defines the number of cores to activate, 0 meaning all cores (default).



5.2 Advanced Power Management Configuration



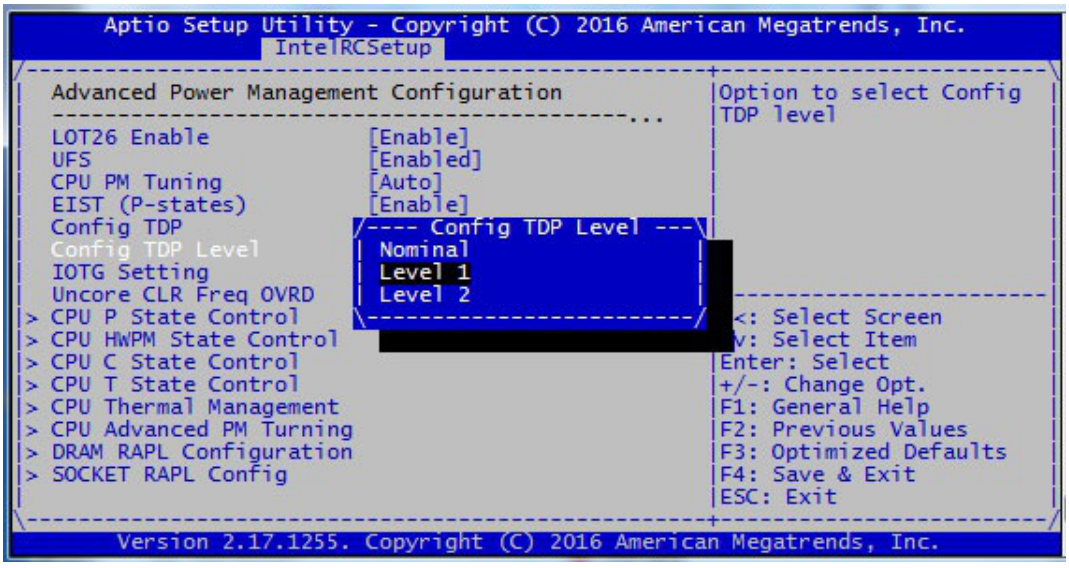
5.2.1 EIST

The **EIST (P-states)** option enables/disables the Enhanced Intel Speed Step feature. Default is Enabled. When enabled, the OS can set the CPU frequency according to load. When disabled, the CPU frequency is set at the Max non-Turbo frequency.

Refer to the VX305x-SA User s Guide for CPU frequency information according to the processor version.

5.2.2 Config TDP

When **EIST** is enabled, the **Config TDP** option allows to select the **TDP level** (Thermal Design Power). Each TDP level allows the OS to set the CPU frequency ratio within a specific range [Min Ratio, Max Ratio].



For example, the Nominal TDP level for a Xeon D-1508 processor @ 2.2 GHz sets the Min Ratio to 8 and the Max Ratio to 22, meaning the minimum frequency can be set to 800 MHz/8W and the maximum non turbo frequency can be set to 2200 MHz/25W. The Level1 TDP level sets the Min Ratio to 8 and the Max Ratio to 16, meaning the minimum frequency can be set to 800 MHz/8W and the maximum non turbo frequency can be set to 1600 MHz/20W.

5.2.3 Turbo Mode

When **EIST** is enabled, the **Turbo Mode** option can be enabled/disabled in the **CPU PState Control** submenu.

Turbo mode allows the CPU to operate at a higher frequency for a while when enough power is available.

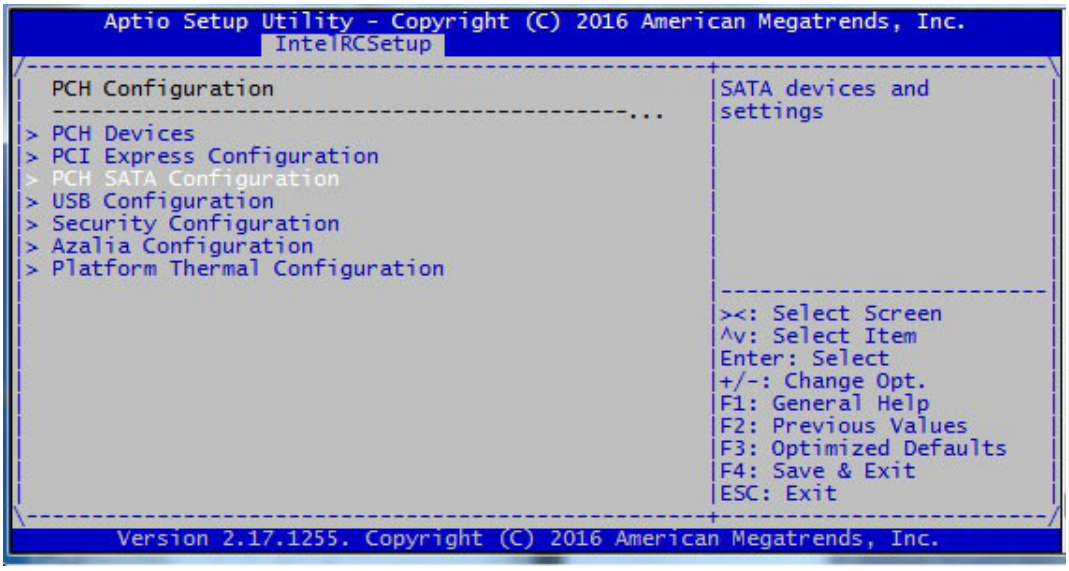
The following timings associated with **Turbo Mode** can be configured in the **SOCKET RAPL Configuration** submenu: Long Duration Power Limit, Long Duration Time Window, Short Duration Power Limit. For more information, please refer to the Intel® Turbo Boost Technology documentation.

5.2.4 C States

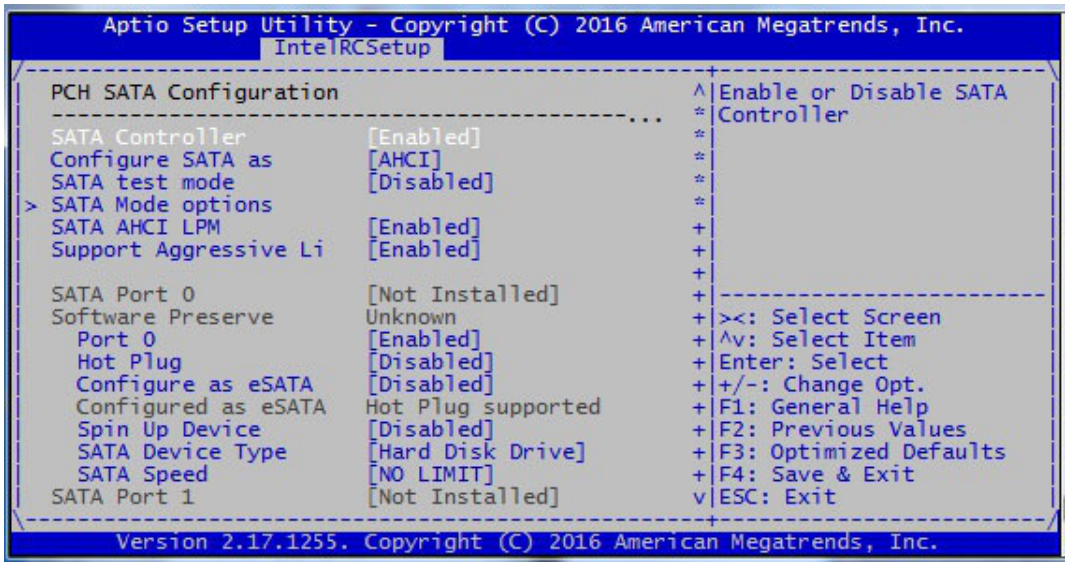
The **Enhanced Cx State** is enabled by default and can be disabled in the **CPU C State Control** submenu.

BUT to guarantee the minimal C1 state on the core when the CPU is in IDLE mode, the setup option **Monitor/MWAIT** must also be disabled in the **Processor Configuration** submenu. Disabling this option will automatically disable C states.

5.3 PCH Configuration

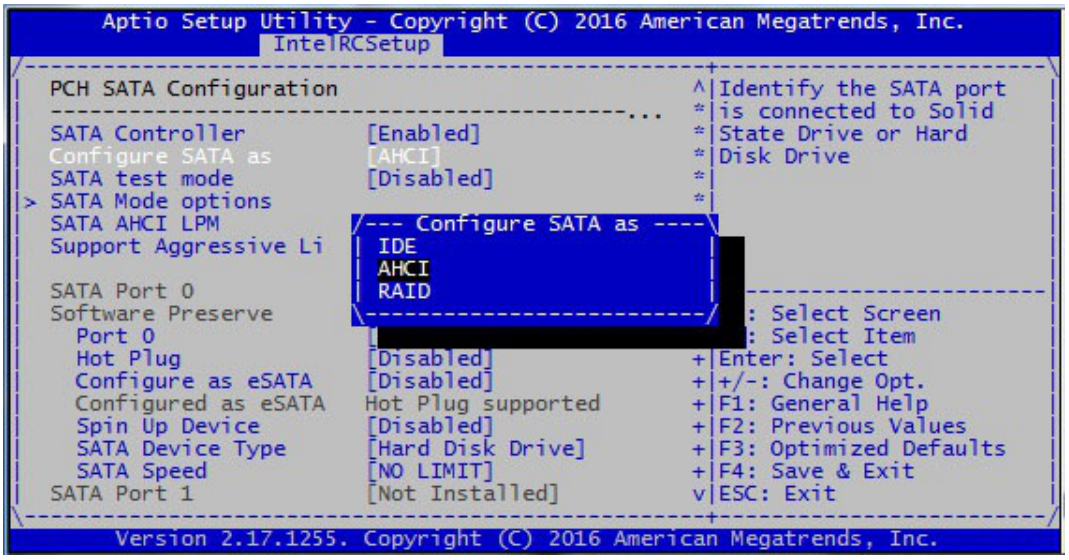


5.3.1 SATA Configuration



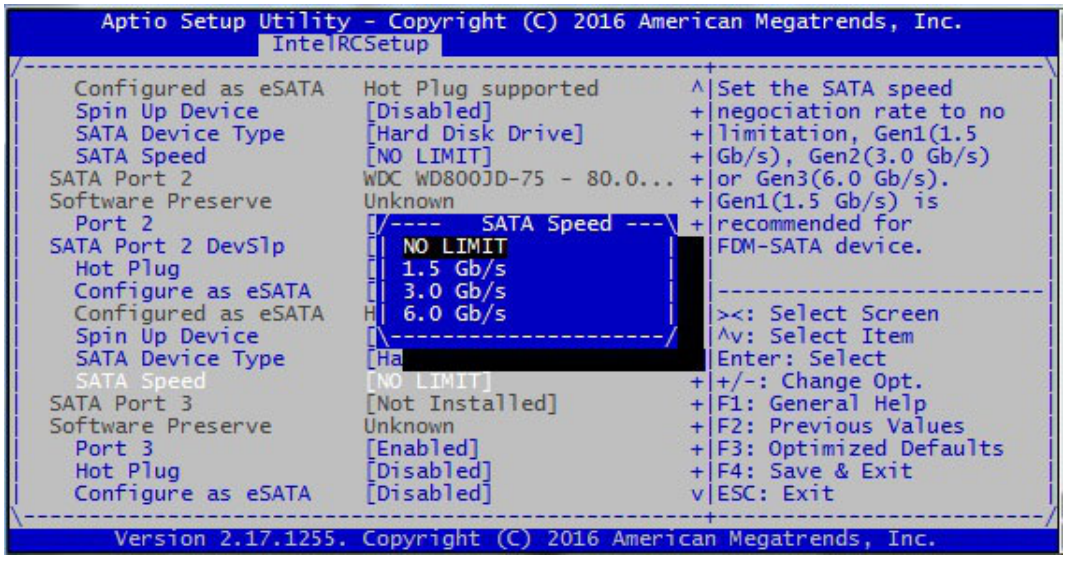
This menu can be used to :

- Select the SATA mode (AHCI or IDE)



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

- Select the maximum speed for each SATA port:

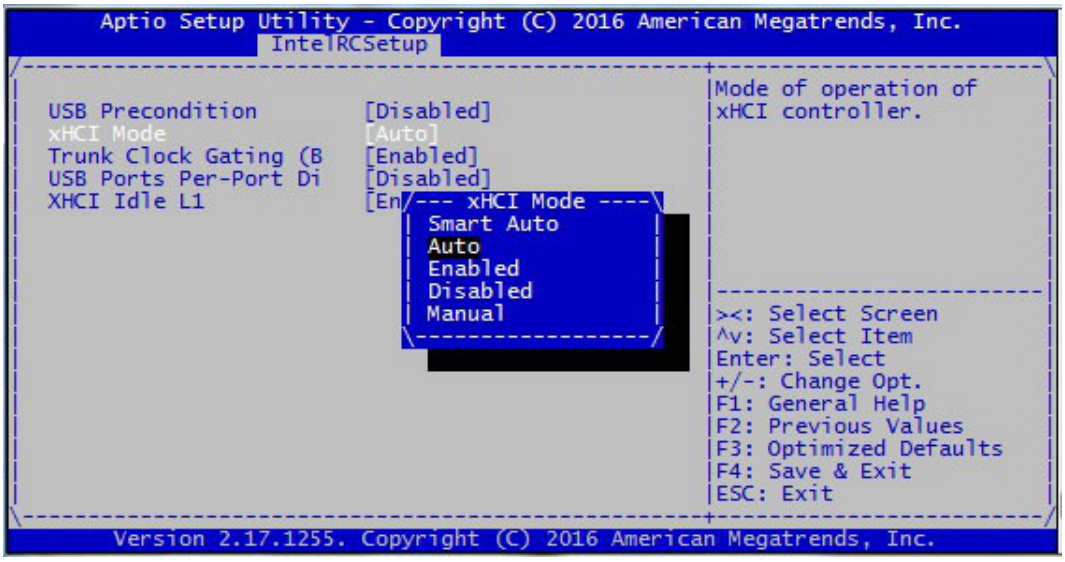


By default, the SATA Speed for each Port is not limited (**NO LIMIT**).

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

5.3.2 USB Configuration

This menu is used to configure the xHCI controller mode.

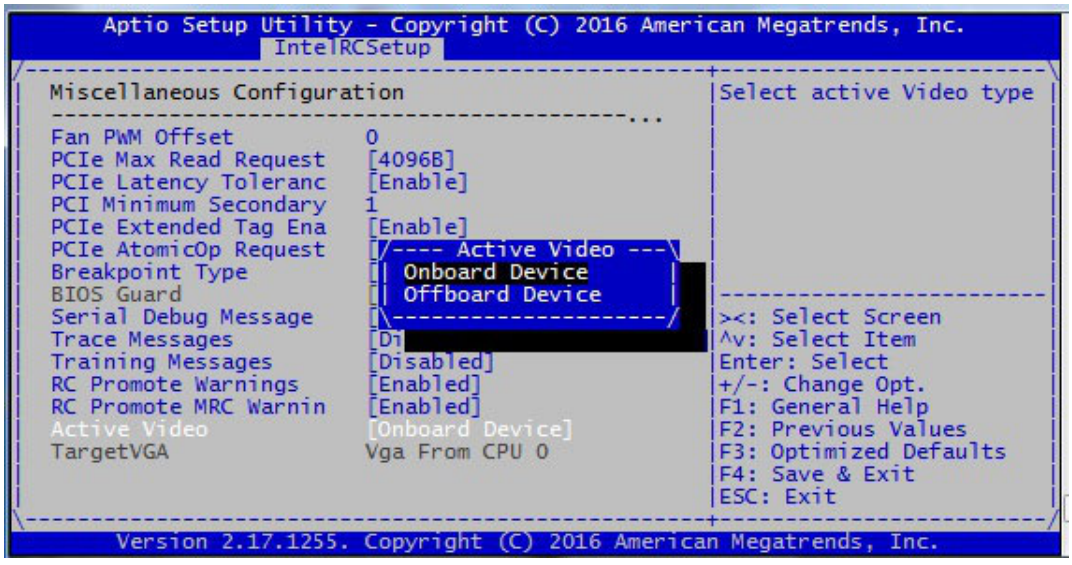


When the **xHCI mode** option is **Enabled**, it allows USB 3.0 SuperSpeed devices to be supported in BIOS and OS. The xHCI controller is turned on. All the VX305x USB ports (USB 2.0 and USB 3.0) are routed to the xHCI controller.

When the **xHCI mode** option is **Auto**, this mode uses ACPI protocol to provide an option to enable the xHCI controller and reroute the USB ports via the _OSC ACPI method call. With this mode, USB 2.0 devices work in BIOS and OS. USB 3.0 SuperSpeed does not work but should work as High Speed Devices.

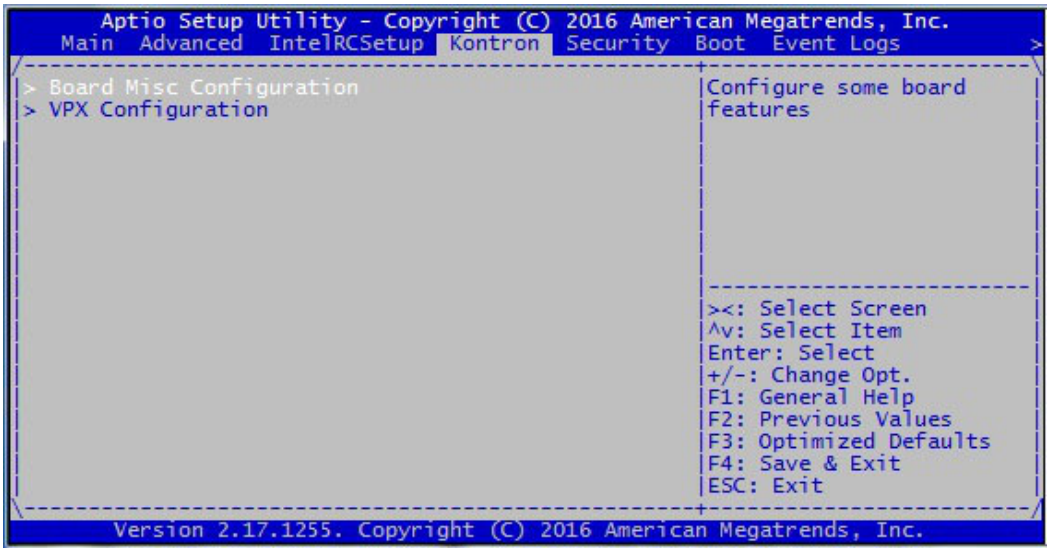
5.4 Miscellaneous Configuration

In this menu, the **Active Video** option is used to select the video either from the **Onboard device** (2-D graphic M.2 module based on the Silicon Motion SM750 graphic controller) or from a **Offboard device** (graphic card connected on the VPX backplane).

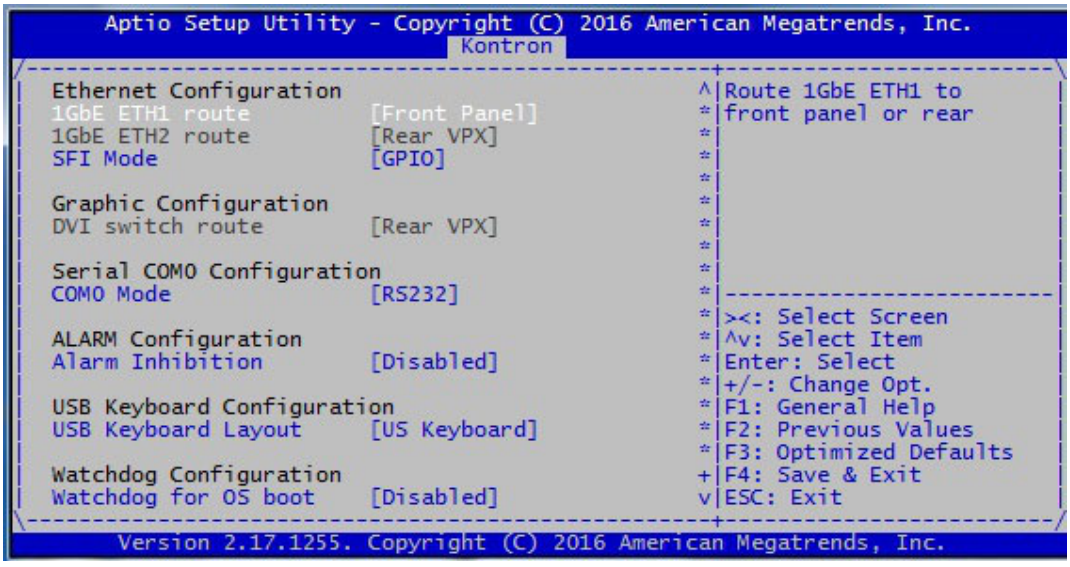


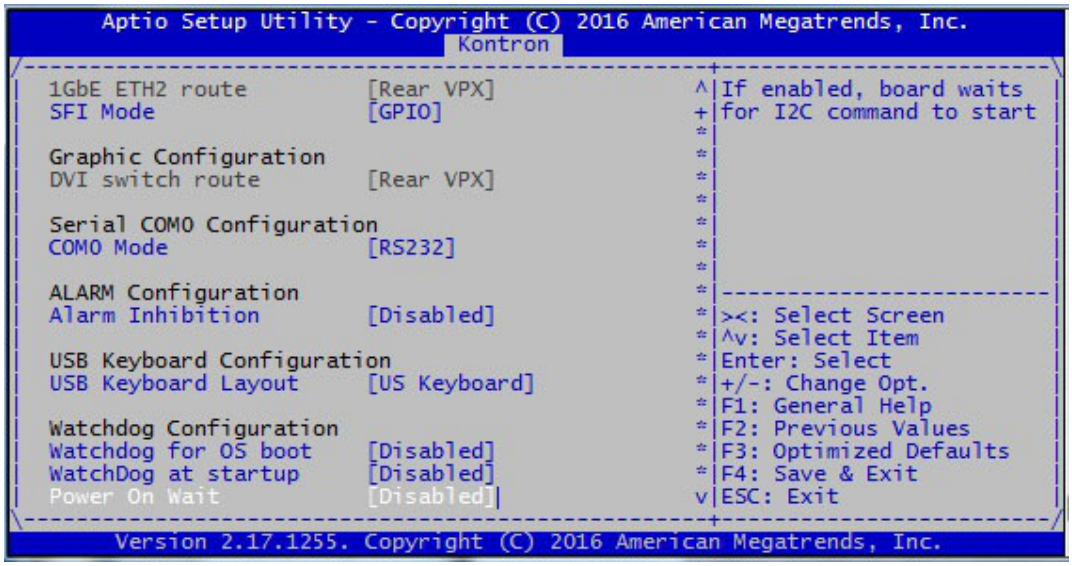
6 / Kontron Menu

This menu is used to configure specific VX305x hardware design.

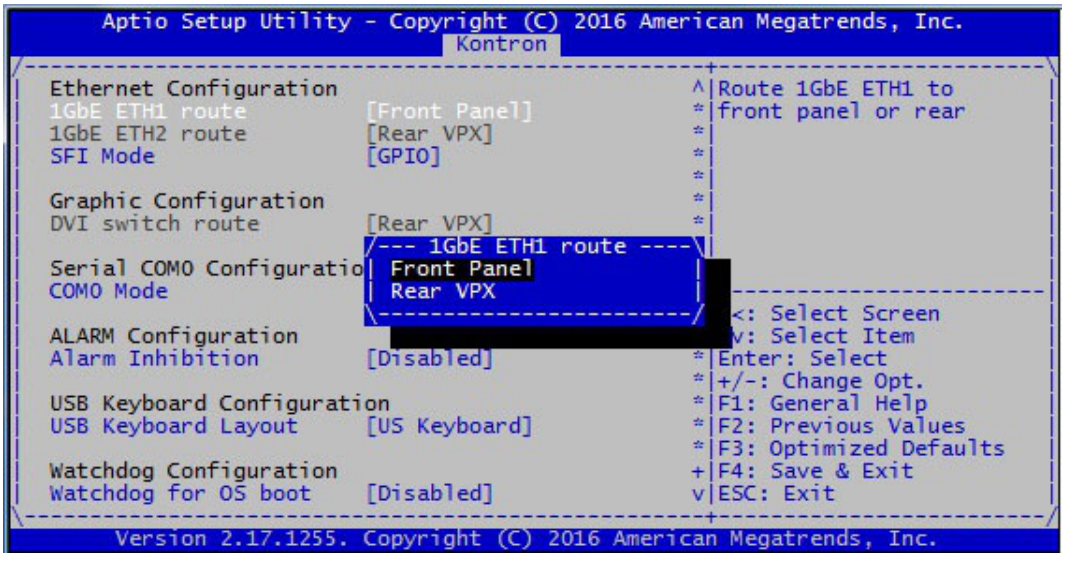


6.1 Board Misc Configuration





6.1.1 Ethernet Configuration



- The **`1GbE ETH1 route`** option is used to physically route the i210 ETH1(*) ethernet interface (also called LAN2) to the front panel or to the rear VPX.

  `Front panel` is the default setting for a SA class board.

- The **`1GbE ETH2 route`** option is used to physically route the i210 ETH2(*) ethernet interface (also called LAN3) to the front panel or to the rear VPX.

  `Rear VPX` is the default setting for a board without the Front-IO module option for Ethernet interface (*).

(*) Refer to the block diagram in the VX305x-SA User s Guide

By default, the SFI mode is set to GPIO and should not be modified.

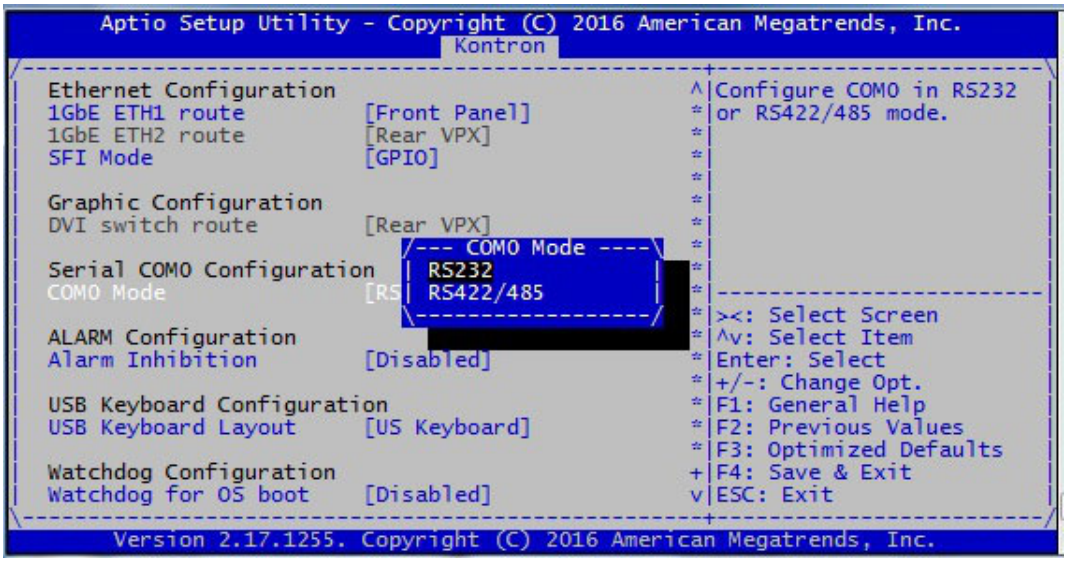
6.1.2 Graphic Configuration

The **DVI switch route** option is used to physically route the graphic interface (if it exists) to the front panel or to the rear VPX (refer to the block diagram in the VX305x-SA User s Guide).

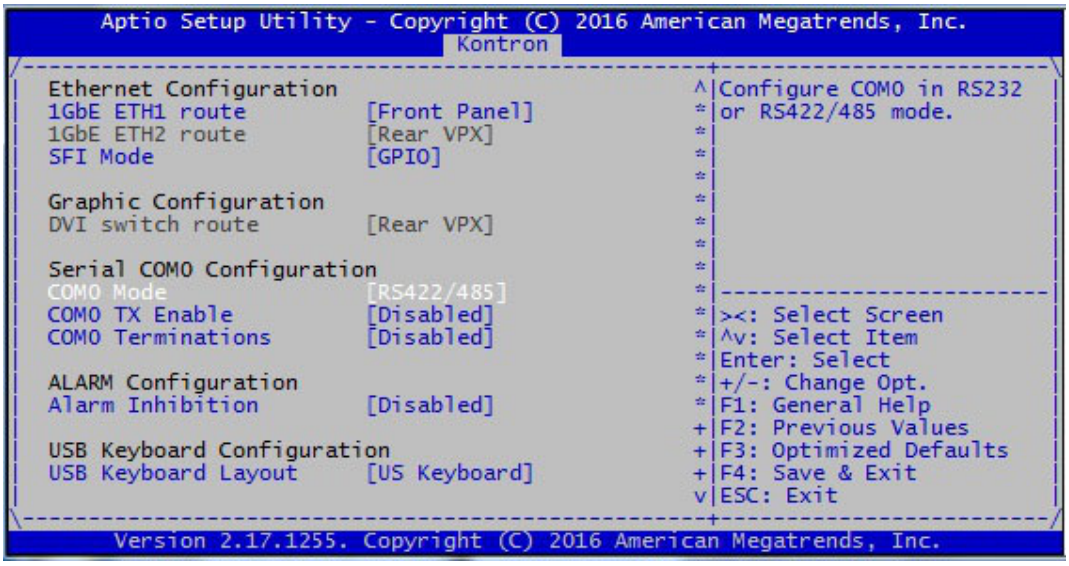
Rear VPX is the default setting for a board without a Front-IO module option for DVI/HDMI interface .

6.1.3 Serial COM0 Configuration

The **COM0 Mode** option is used to select the serial line mode to **RS232** or **RS422/485**.



If **RS422/485** mode is selected, then the **COM0 TX Enable** and **COM0 Terminations** options are available to adapt the line to the configuration used.



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

When COM0 Mode is set to RS422/485, then COM1 is not operational anymore.

6.1.4 Alarm Configuration

The **Alarm Inhibition** option is used to prevent the cPLD logic to turn off automatically the system in case of THRMTRIP# or PROCHOT# alerts assertion.

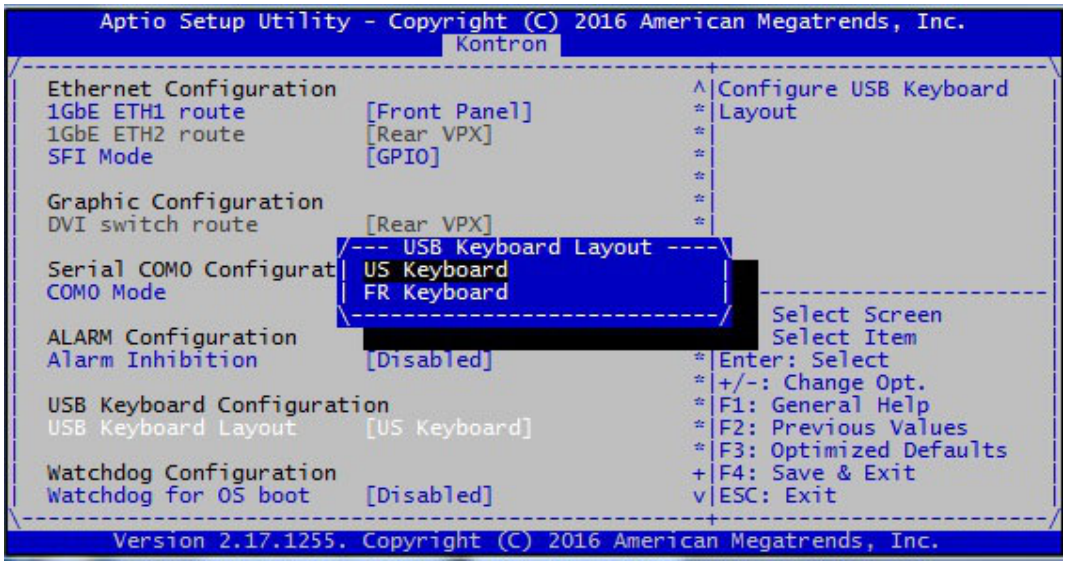
By default, alarms are enabled.

It is highly recommended to not change the default setting for normal use.

This parameter must be used with caution.

6.1.5 USB Keyboard Configuration

The **USB Keyboard Layout** option is used to choose either a qwerty or an azerty keyboard map.



As only the English language is supported under BIOS, accented characters of the French key' board cannot be managed. Moreover, the characters °, £, ¤, µ and § are not displayed either.

6.1.6 Watchdog Configuration

The **WatchDog for OS boot** option allows to enable/disable the cPLD Watchdog Timer at OS boot time.

The timeout value can range between 1 sec and 511 sec. This can be adjusted up and down by using the keys <+> or <->.

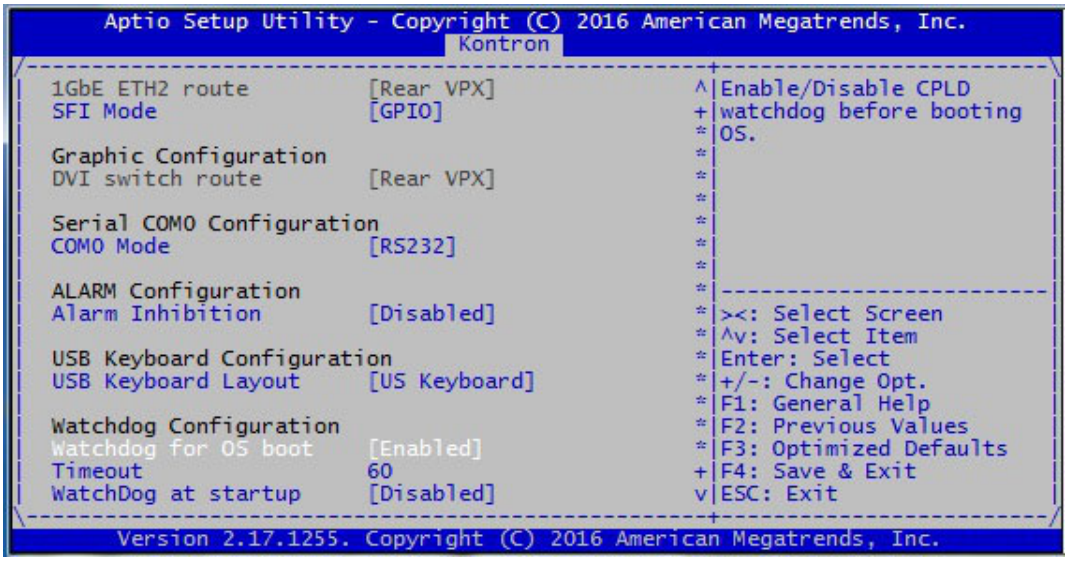
If enabled, the timer will start to count down at device boot time.

Only the Power-cycle mode is handled.

The WatchDog for OS setting is kept by the Setup even after a timeout has occurred.

Since BIOS version ID17185 the watchdog feature is applied not only to legacy boots but also to UEFI boots.
As the UEFI shell is a UEFI boot device, the watchdog is operational under the shell also.

See recommendation 9 in section 12.1 page 42



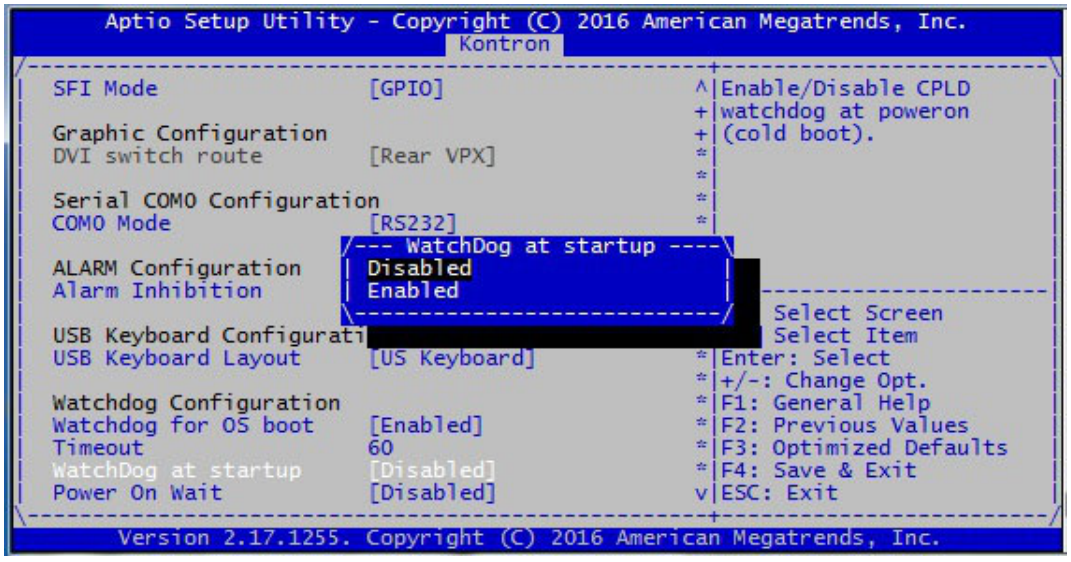
The **WatchDog at Startup option** enable/disable the cPLD Watchdog Timer at Power-On.

The timeout value is set to 31 sec and is not configurable.

After enabling the feature, the timer will start only at the next board Power-On.

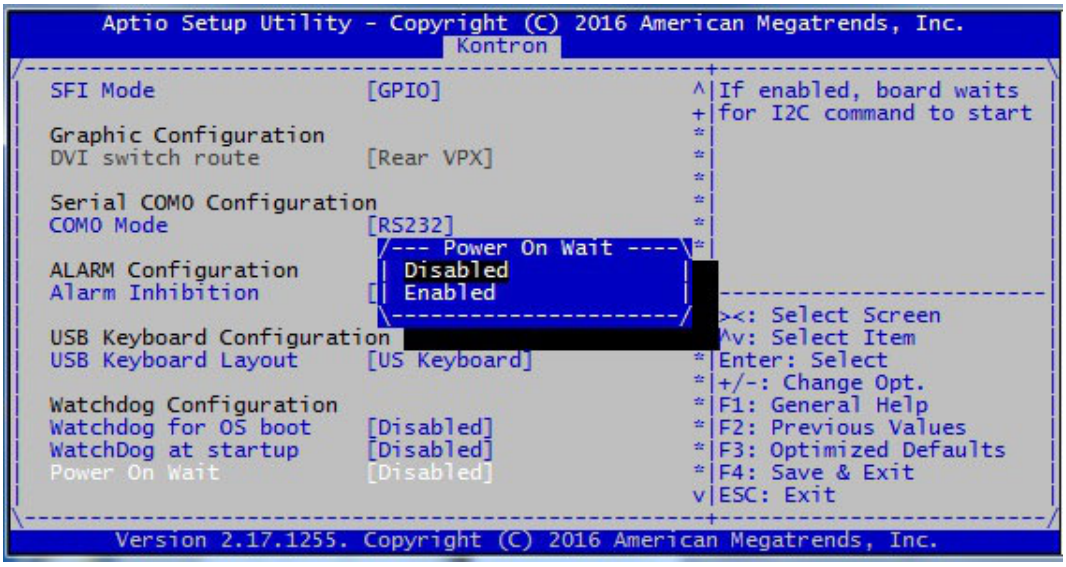
Only the Power-cycle mode is handled.

In case of failure, the board startup can be retried 6 times.

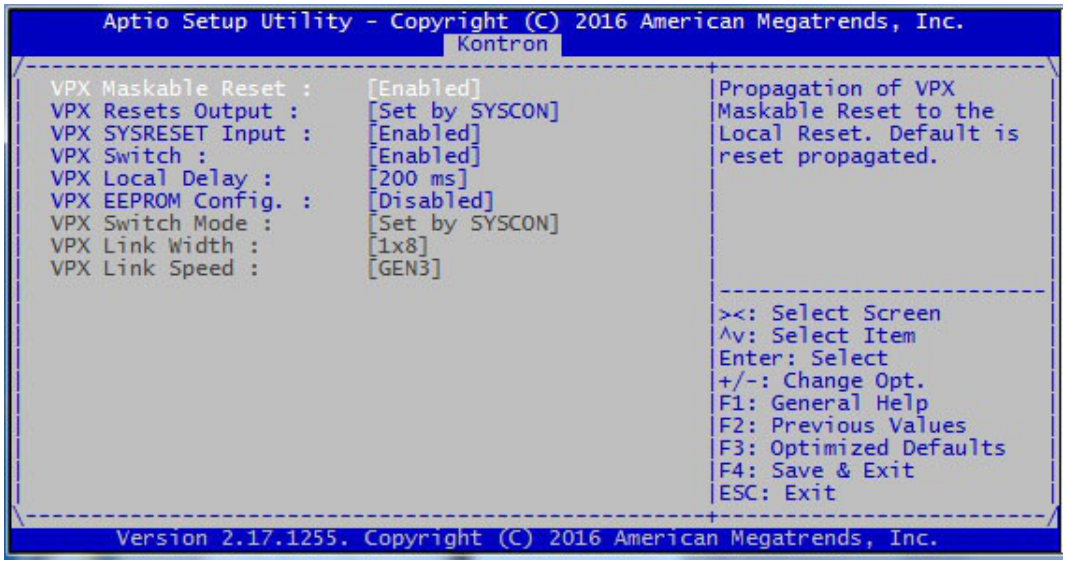


The **Power On Wait** option allows an external equipment to power-on the board remotely by using the I2C backplane.

This feature is reserved for specific hardware. DO NOT USE for normal operation.



6.2 VPX Configuration



6.2.1 VPX Maskable Reset

The **VPX Maskable Reset** option allows to propagate or not the Maskable Reset from the VPX backplane to the board.

By default reset is **propagated**.

6.2.2 VPX Reset Propagation to VPX Backplane

The **VPX Resets Output** parameter allows to propagate the local resets of the board to the VPX backplane disregarding the state of the **VPX SYSCON#** signal.

By default only the VPX System Controller board can control the propagation of the local reset to the **VPX SYSRESET#** signal on VPX backplane.

Caution when using this parameter in a multi-boards system because ALL boards plugged on the VPX backplane can be affected by the **VPX SYSRESET#** signal.

This parameter can be used in conjunction with the parameter **VPX SYSRESET** Input.

6.2.3 VPX SYSRESET Input

The **VPX SYSRESET Input** parameter allows to propagate or not the **VPX SYSRESET#** signal from the VPX backplane to the board.

If this parameter is set to **[Disabled]**, VPX backplane reset has no effect on the board.

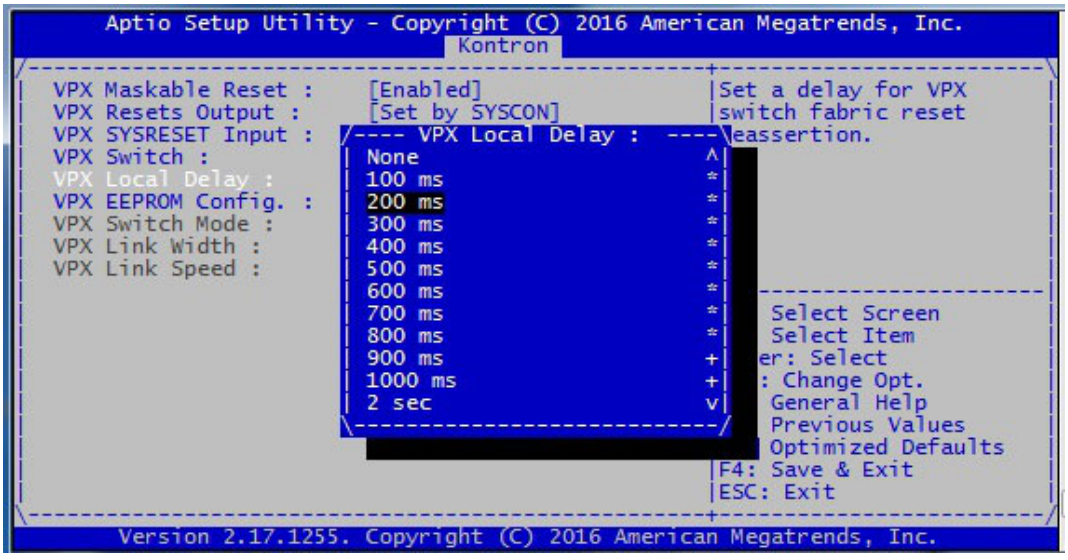
In a multi-boards configuration system, this parameter can be used in conjunction with the VPX Resets Output parameter.

6.2.4 VPX Switch

If set to **Disabled**, the **VPX Switch** option allows to maintain the PCI-E switch PEX8725 component in reset state.

By default, this option is enabled and access to the backplane PCI-E can be performed.

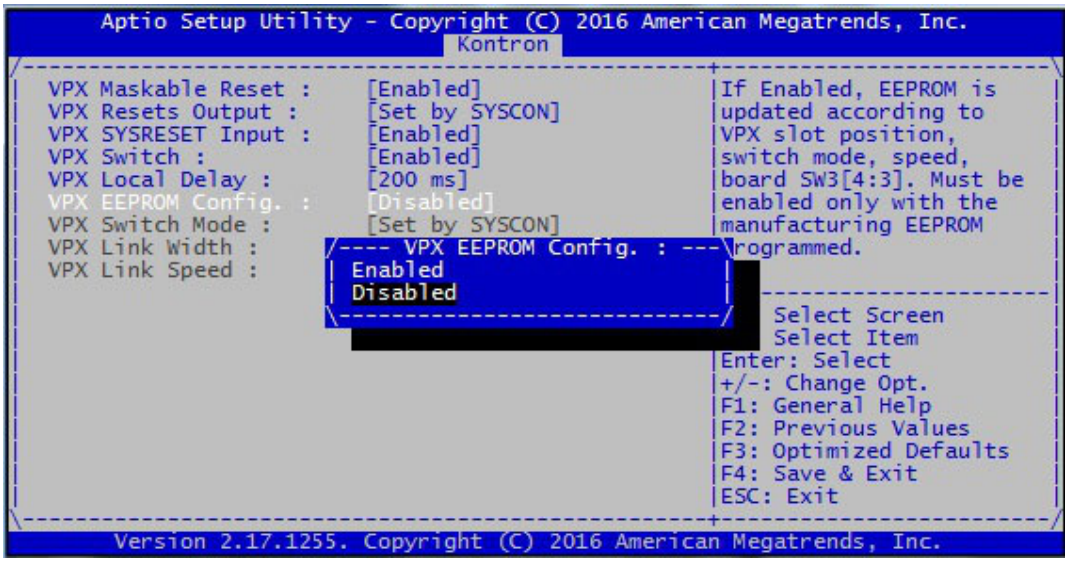
6.2.5 VPX Local Delay



The **VPX Local Delay** option set a delay for the PCI-E switch PEX8725 reset deassertion.

This can be useful in a multi CPU board system to delay the backplane PCI-E discovery for the System Controller board and adjust the boot sequence.

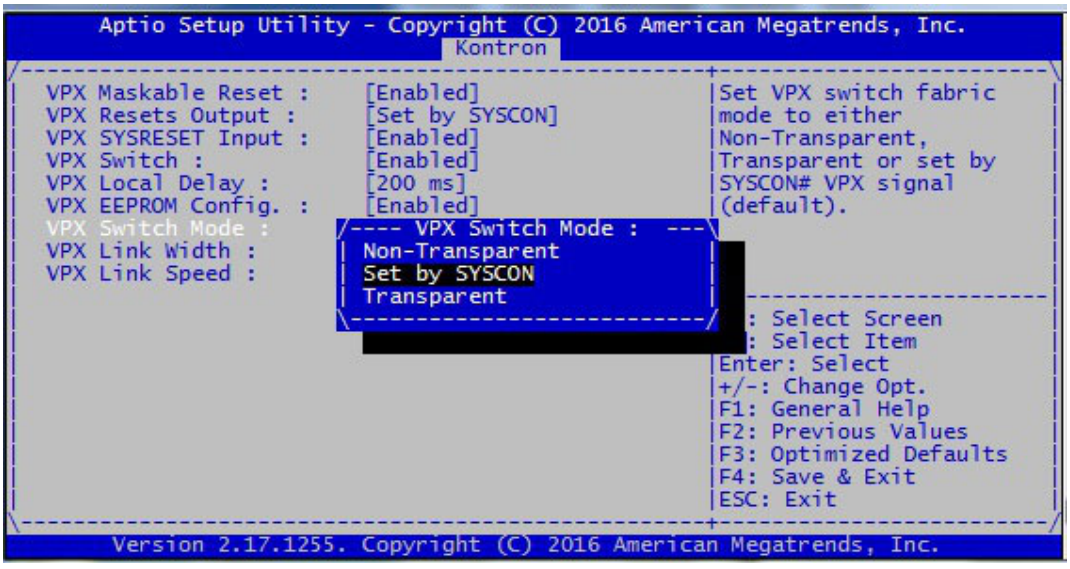
6.2.6 VPX EEPROM Configuration



The VPX Switch Fabric EEPROM can be configured dynamically by enabling this feature. By default, this parameter is set to **[Disabled]**: the EEPROM is programmed during manufacturing with a default binary image that configures the PCI-E switch in Non-Transparent mode, VPX port speed at Gen3 and a VPX link width of 1x8.

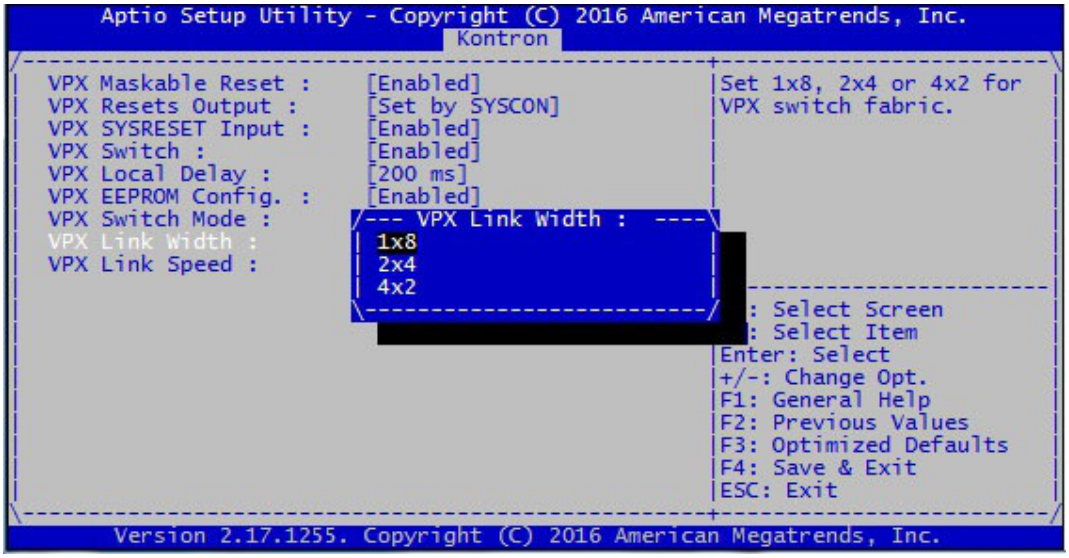
If this parameter is set to **[Enabled]**, the following features can be configured:

1. The Transparent Mode of the Switch Fabric:
   a. **Transparent**: the Switch Fabric is forced in Transparent Mode
   b. **Non-Transparent**: the Switch Fabric is forced in Non-Transparent Mode
   c. **Set by SYSCON**: the Switch Fabric is in Transparent Mode if the board is System Controller, and Non-transparent otherwise.



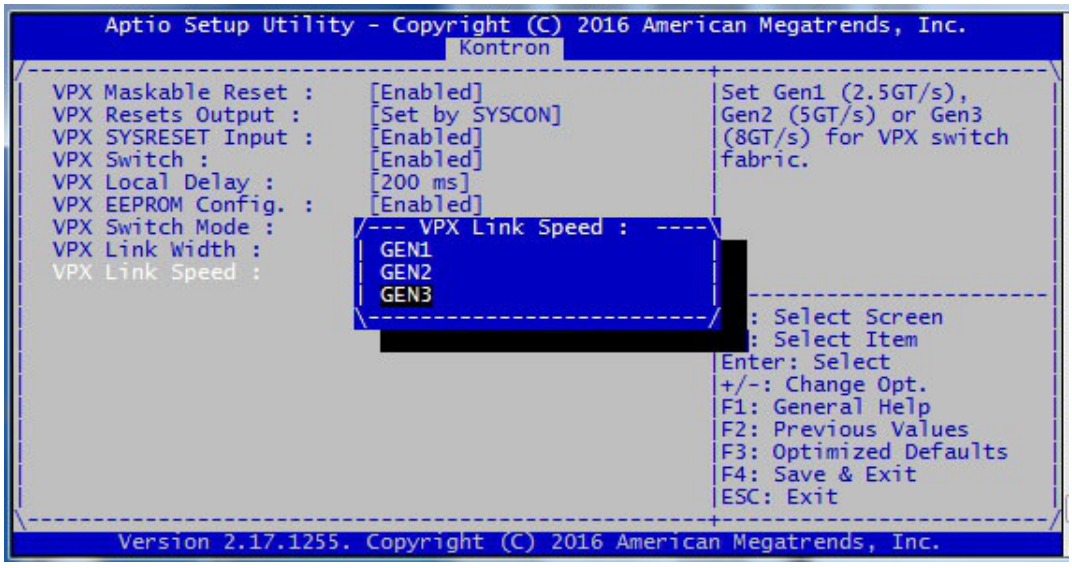
2. The VPX width of the Link

a. 1x8
b. 2x4
c. 4x2



3. The VPX speed of the Link:

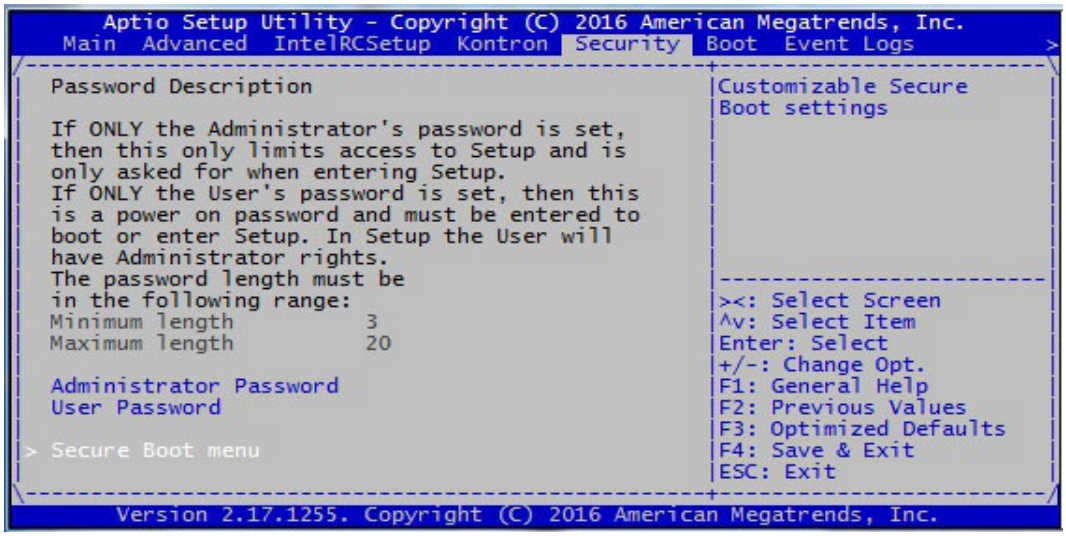
a. **GEN1**: the speed is limited to 2.5 GT/s
b. **GEN2**: the speed is limited to 5 GT/s
c. **GEN3**: the speed is limited to 8 GT/s



7 / Security Menu

The **Security** menu provides both **Administrator** and **User password**.

The Administrator and User passwords activate two different levels of password security as written in the following description:



If ONLY the User s password is set, then it must be entered to boot or to enter Setup and in Setup the User will have Administrator rights.

So to protect the BIOS settings at User level, it is required to also set an Administrator s pass' word. In this case, the user does not have Administrator rights anymore.

When both passwords are set, user will have limited access to the Setup as changing the system date and time, selecting boot devices or change the devices boot order. <F4> key to **Save and Exit** is used to save the limited changes, <F3> key to **Load Optimized Defaults** is not allowed.

Note that if an Administrator s password is set, the user cannot change the User s password. This is only possible with the Administrator rights.

To enter the password:

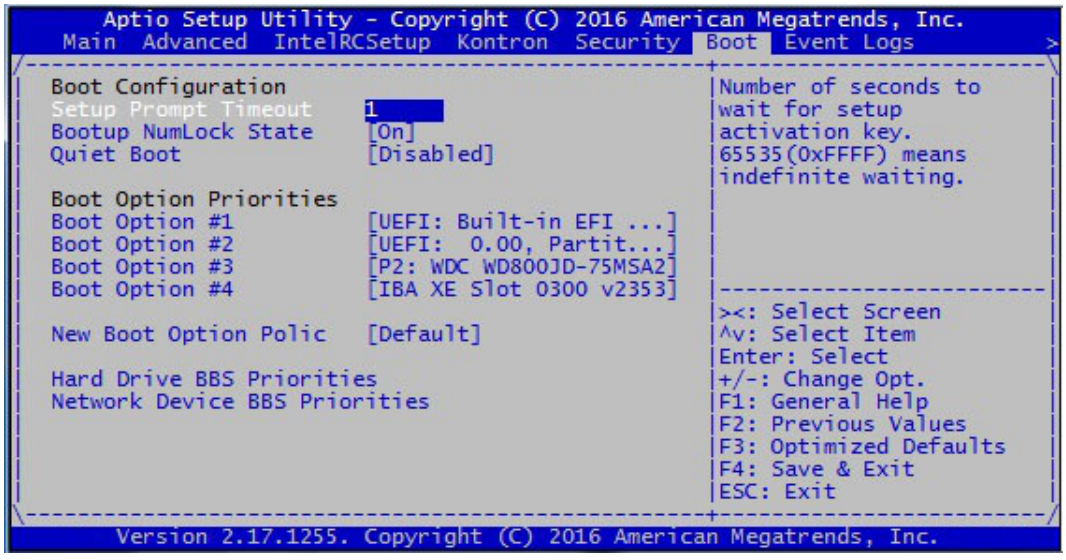
- Select the administrator or user password item
- A pop-up window appears to create a new password
- Enter the password (from 3 up to 20 characters)
- A new pop-up window appears to confirm the password
- Save the password by selecting **Save Changes** in the **Save & Exit** menu.

To suppress or change the password:

- Select the Administrator or User password item
- A pop-up window appears to enter the current password
- A new pop-up window appears to enter a new password
- Type the new password or enter <CR> to suppress the password
- Confirm the new password or confirm you want to clear the password
- Save the changes by selecting **Save Changes** in the **Save & Exit** menu.

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

8 / Boot Menu



The Boot Menu is used to select the boot sequence of the available boot devices.

Boot settings are:

- **Setup Prompt Timeout**: Section 8.1 page 27
- **Bootup NumLock State**: Section 8.2 page 27
- **Boot Option Priorities**: Section 8.3 page 28
- **Network Device BBS Priorities**: Section 8.4 page 29
- **Hard Drive BBS Priorities**: Section 8.5 page 30

The VX305x boot time is about 17s after a reset and 20s after a power-on, assuming network OpROMs are not launched and boot time ends when the EFI shell prompt appears.
Boot time may also change depending a USB device is connected or not.

8.1 Setup Prompt Timeout

This option sets the time to wait (in second) for the setup activation key.

Default value is **1 sec**.

8.2 Bootup Numlock State

Set this option to **On** allows the Number Lock on the keyboard to be automatically enabled during boot up.

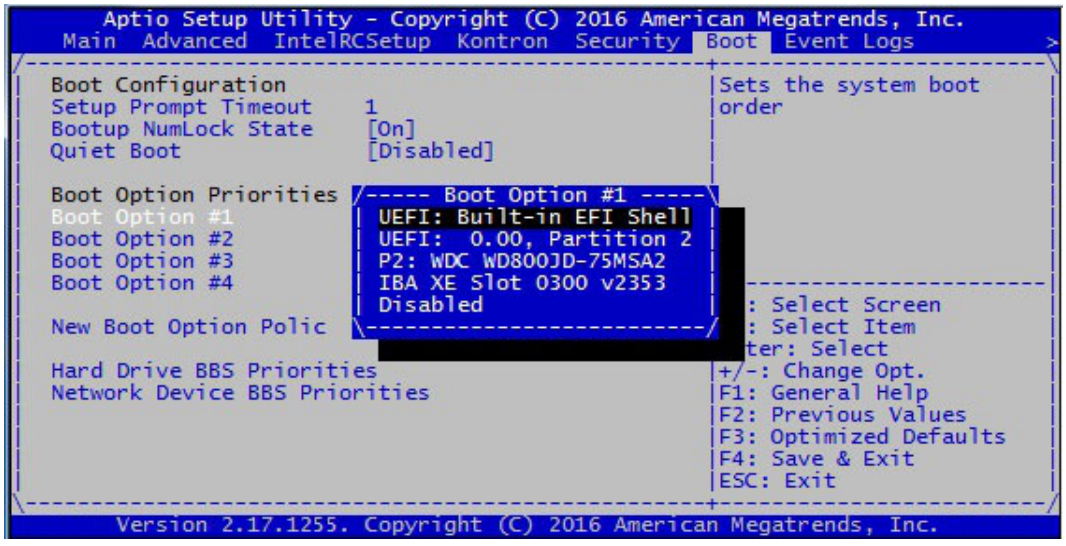
Default is **On**.

8.3 Boot Option Priorities

The **Boot Options Priorities** specify the boot order of the available boot devices.

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

Here is a example of boot device list:



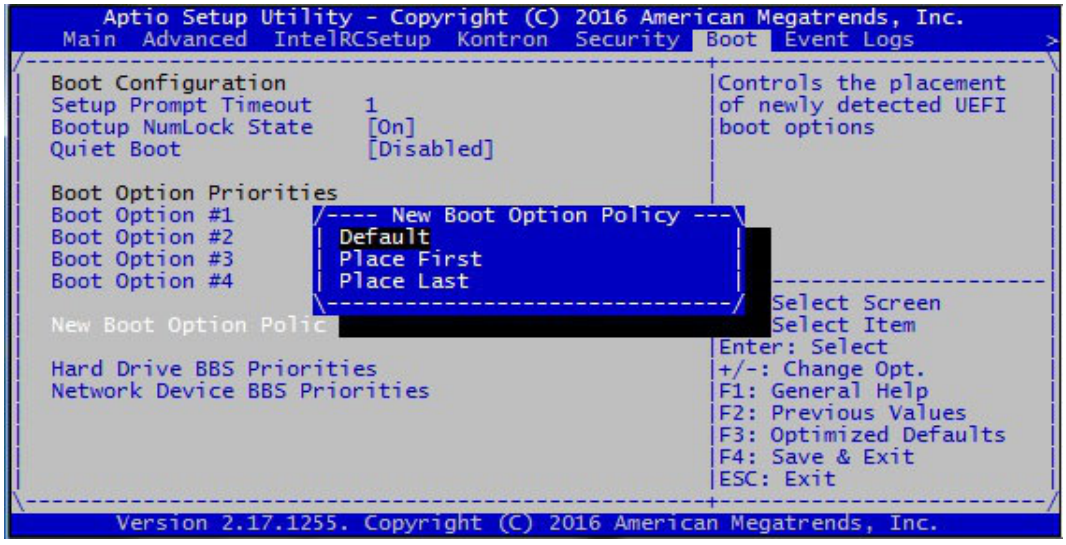
To change the boot device ordering

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

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

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

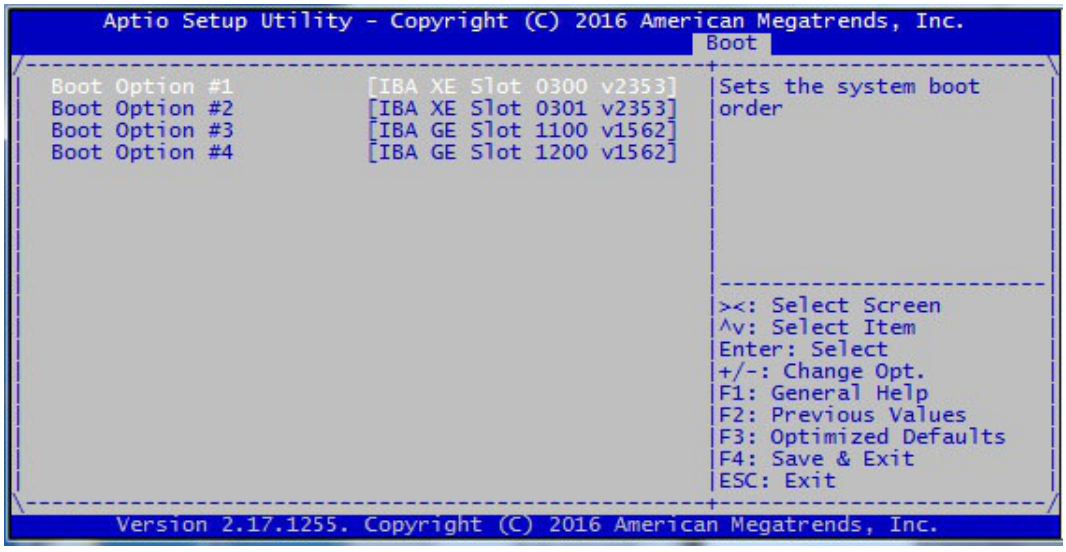
The **New Boot Option Policy** option can be used to control the placement of the newly detected UEFI boot options.



8.4 Network Device BBS Priorities

If the **Network OpROM** option in the Advanced/CSM Configuration menu has been set to **Legacy**, all the Ethernet interfaces become available for PXE boot.

Then, a new entry is displayed in the Boot menu. The **Network Device BBS Priorities** allows to configure the Ethernet boot devices order for PXE boot.



The entries "**IBA XE Slot 0300**" and "**IBA XE Slot 0301**" correspond to the 10 GbE interfaces of the Broadwell-DE, respectively LAN0 and LAN1.

The entries "**IBA GE Slot 1100**" and "**IBA GE Slot 1200**" correspond to the 1 GbE interfaces of the i210 controllers, respectively LAN3 and LAN2 (Pay attention to the LAN2 and LAN3 order in the list because LAN3 PCI device is detected first when scanning the PCI busses).

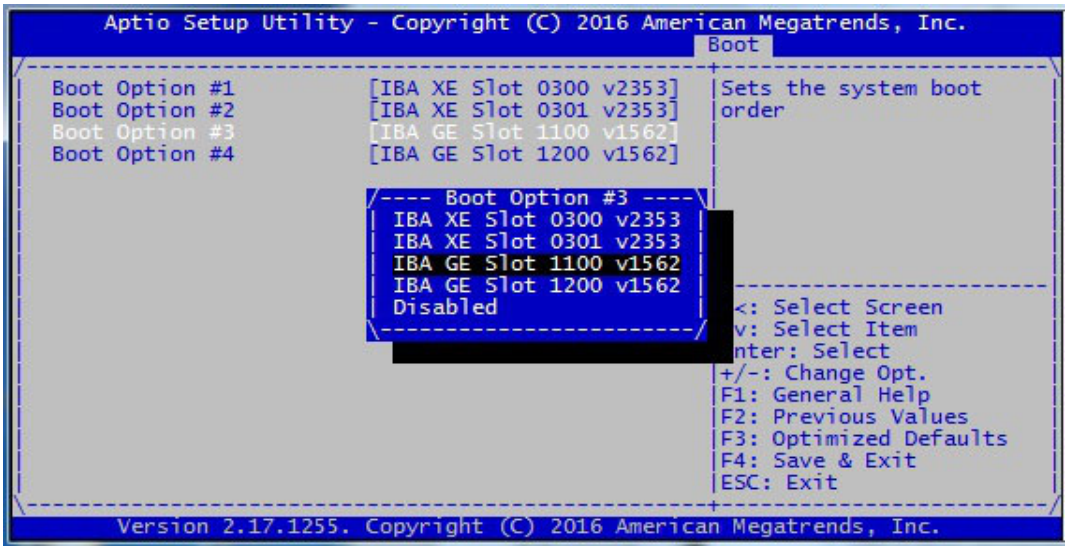
To change the PXE boot device ordering

- 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 PXE boot device

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

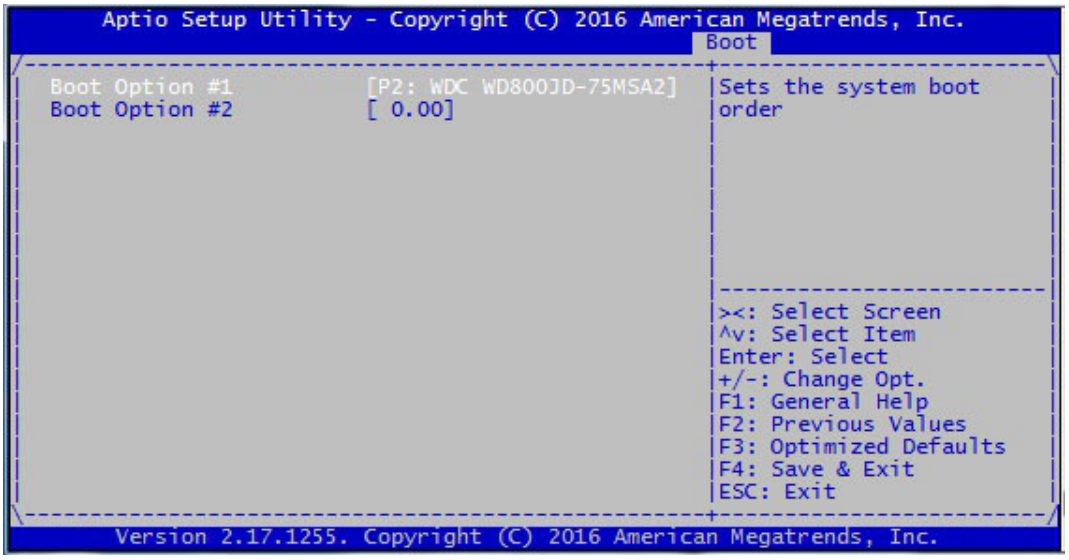
A new submenu appears (see image) , select **Disabled** to disable the PXE device



8.5 Hard Drive BBS Priorities

The **Hard Drive BBS Priorities** entry appears when SATA or USB devices are present.

It allows to configure the SATA and USB boot devices order.

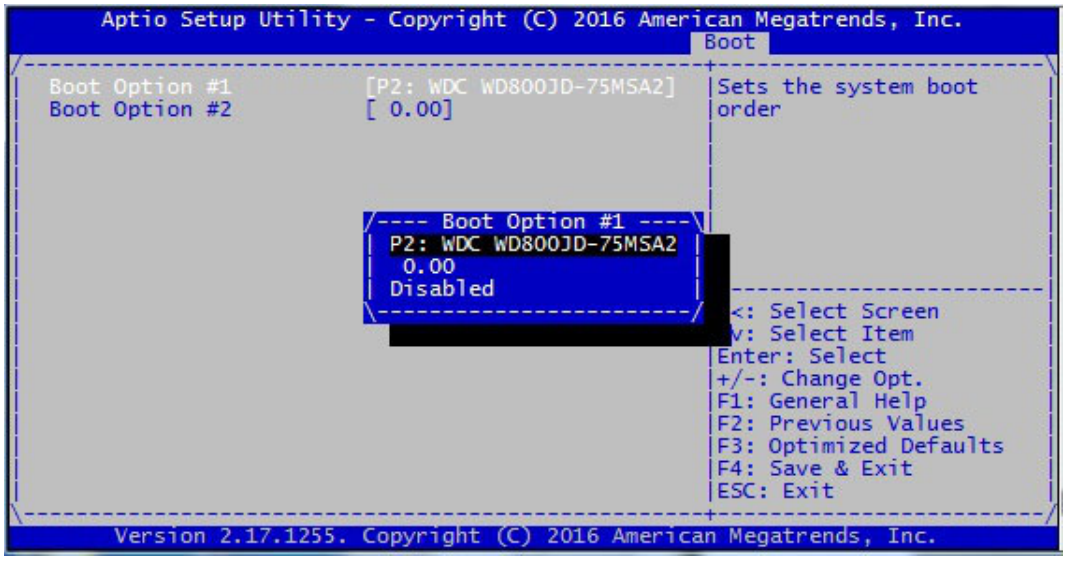


To change the boot devices ordering

- 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 devices

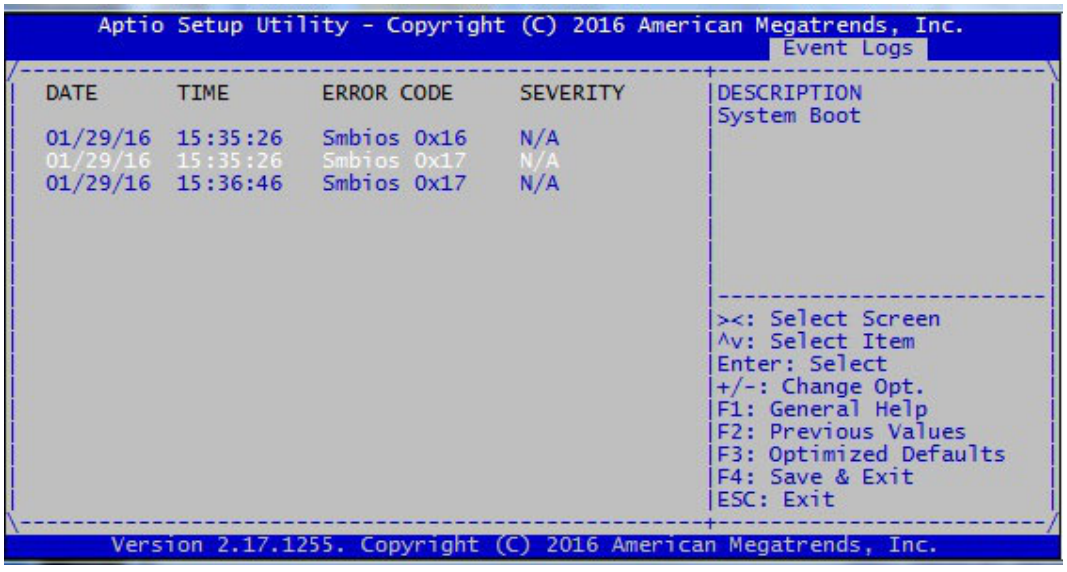
- Select a device from the list (Use the <↑> or <↓> to highlight the desired item
- <Enter> to validate the choice



9 / Event Logs Menu

System events logged by the BIOS are displayed in the page **View Smbios Event Log**.

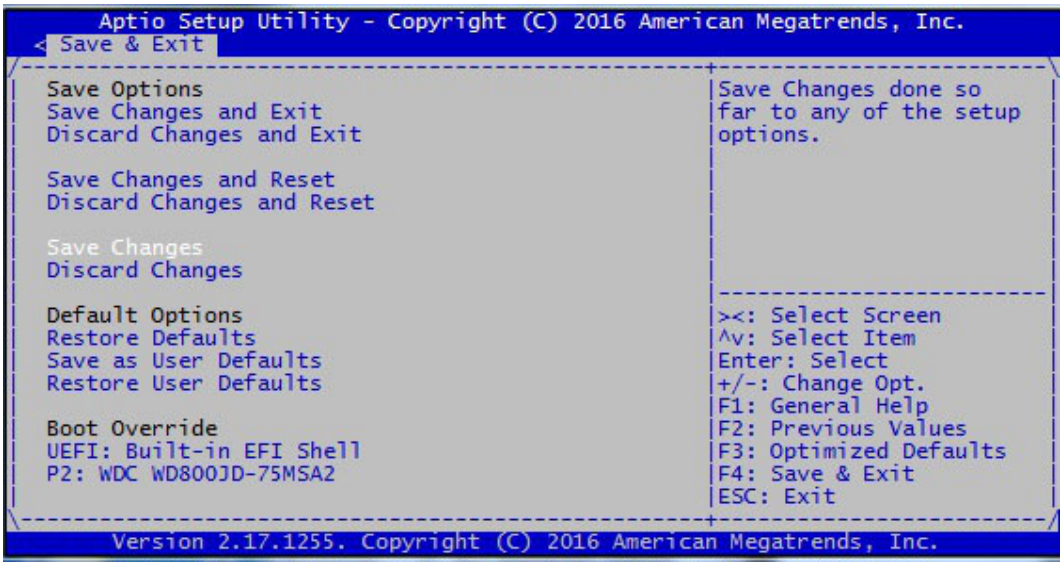
For example, it is possible to trace each time the system has been powered on or reset. System errors are also logged.



The page **Change Smbios Event Log Settings** is used for basic logging management.

10 / Save & Exit Menu

This menu does not appear when entering SETUP, it is necessary to navigate from the Main menu with <→> or <←> keys to find it.



The possible actions are

- **Save Changes and Exit**: section 10.1 page 32
- **Discard Changes and Exit**: section 10.1 page 32
- **Save Changes and Reset**: section 10.1 page 32
- **Discard Changes and Reset**: section 10.1 page 32
- **Save Changes**: section 10.2 page 33
- **Discard Changes**: section 10.2 page 33
- **Restore Defaults**: section 10.2 page 33
- **Save as User Defaults**: section 10.3 page 33
- **Restore User Defaults**: section 10.3 page 33
- **Boot Override**: section 10.4 page 33

10.1 Save/Discard Options with Exit/Reset Actions

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

10.2 Save/Discard/Restore Default Options

SETUP modification can simply be Saved or Discarded without exiting BIOS SETUP.

Also manufacturing default SETUP parameters can be restored with the **`Restore Defaults`** option.

Select the desired item and <Enter>

- Save Changes
- Discard Changes
- Restore Defaults

10.3 Saving a User Configuration

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

Select desired item and <Enter>

- Save as User Defaults
- Restore User Defaults

10.4 Boot Override

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

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

11 / EFI SHELL

EFI Shell is a boot shell available on the VX305x that is accessible in the boot device list. EFI Shell is launched automatically if no other boot device is connected to the VX305x. If EFI shell is not the primary boot device then it is necessary to enter the SETUP menu to access it. For this, enter <DEL> 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.

Only the additional Kontron Shell commands are developed in the next chapter.

Since BIOS ID17347, the Admin password also applies when accessing the Shell.

11.1 Kontron Command

The **`Help`** command or **`(?)`** displays all the available command. Use option **`-b`** to display command screen by screen. Use **`help +`** command (like **`VX305x> help help`**) to have the detail of a command syntax

COMMAND NAME	DESCRIPTION	SEE SECTION
`kdiag`	Performs board diagnostics - Available ONLY if ordered.	11.1.1 page 35
`kflash`	Kontron SPI flasher	11.1.2 page 35
`kmac`	Kontron MAC Address viewer	11.1.3 page 36
`kpld`	Kontron PLD Commands	11.1.4 page 37
`ksensor`	Kontron sensor utility	11.1.5 page 37
`kvpd`	Kontron VPD Information	11.1.6 page 38
`kvpx`	Kontron VPX Configurator	11.1.7 page 38

11.1.1 kdiag

Performs board diagnostics. Available ONLY if ordered.

11.1.2 kflash

Kontron SPI flasher

- **Usage:**

```
kflash -p -r filename
kflash -s filename
kflash -v filename
kflash -c
kflash -ver
kflash -h|-?
```

- **Options**

`-p`	Program flash image file
`-r`	Raw image mode (.bin, .rom)
`-s`	Read flash and save content to a file
`-c`	Clone RESCUE flash on MAIN flash
`-v`	Verify flash image file and check flash CRC
`-ver`	Display BIOS version of current flash
`-h|-?`	Display this help

- **Description**

Program/Manage SPI flash on Kontron board.

To save current BIOS flash content to file named image.bin:

```
Shell> kflash -s image.bin
```

To program file image.bin:

```
Shell> kflash -r -p image.bin
```

To display current BIOS version in SPI flash:

```
Shell> kflash -ver
```

11.1.3 kmac

Kontron MAC Address utility

- **Usage:**

```
kmac [-h|-r|-v|-stat] [-dump lan] [-w value]
```

- **Options**

`-h`	Shows this help
`-r`	Shows the MAC Address for each LAN
`-w value`	Updates all the LAN MAC Addresses by auto-increment LAN0 (SOC 10G LAN0) = value LAN1 (SOC 10G LAN1) = value+1 LAN2 (i210 frontpanel) = value+2 LAN3 (i210 frontIO) = value+3 value is a 6-bytes hexa number prefixed with "0x"
`-dump [0|1|2|3]`	Dumps the first 1024 words of the NVM of each LAN (same NVM for LAN0 and LAN1)
`-stat`	Displays LAN0 and LAN1 (SOC 10G) link status information

- **Description**

Manages SOC 10GbE and i210T LAN MAC addresses.

To display the MAC addresses:

```
Shell> kmac -r
MAC Address LAN ETH0 (SOC 10GbE LAN0) = 00:00:DE:52:CB:0C
MAC Address LAN ETH1 (SOC 10GbE LAN1) = 00:00:DE:52:CB:0D
MAC Address LAN ETH2 (i210T ETH1) = 00:00:DE:52:CB:0E
MAC Address LAN ETH3 (i210T ETH2) = 00:00:DE:52:CB:0F
```

11.1.4 kpld

Kontron PLD Utility

- **Usage:**

```
kpld [-h] [-b] [-v] [-m] [-r addr] [-w addr data]
kpld -i2cr i2cbusnum addr offset accesstype [count]
kpld -i2cw i2cbusnum addr offset accesstype data [count]
```

- **Options**

`-h`	Displays help
`-v`	Shows CPLD revision
`-m`	Boot Flash information
`-r`	Reads CPLD register address <addr>
`-w`	Writes <data> into cpld register address <addr>
`-i2cr`	Reads I2C device address <addr>, bus number <i2cbusnum>, offset address <offset>, with access type <1 or 2 bytes>
`-i2cw`	Writes <data> into I2C device address <addr>, bus number <i2cbusnum>, offset address <offset>, with access type <1 or 2 bytes>

All parameters must be raw hexadecimal values (without prefix)

- **Description**

Manages read/write access to the CPLD registers or to devices connected to CPLD I2C busses.

I2C device write protection is not controlled before write access.

11.1.5 ksensor

Kontron sensor utility

- **Usage:**

```
ksensor [-h]
```

- **Options**

`-h`	Shows this help

- **Description**

Displays the board sensors.

11.1.6 kvpd

Kontron VPD Information

- Usage:

```
kvpd -p
kvpd -m
kvpd -h
```

- Options

`-p`	Displays VPD information
`-m`	Modifies or enters VPD information
`-h`	Displays this help

- Description

Displays the Vital Product Data of the Kontron board: order code, hardware level, serial number, variant.

11.1.7 kvpx

Kontron VPX Configurator

- Usage:

```
kvpx -plx_eeprom [prog|dump|conf|ver] [0|1|2|3|filename] [-b] [-h|-?]
```

- Options

`-b`: Enables page break

`-h|-?`: Shows this help

`-plx_eeprom`: Manages PCIe switch serial EEPROM

- Suboptions:

`prog`: Programs PCIe switch serial EEPROM

`dump`: Dumps PCIe switch serial EEPROM

`conf`: Displays PCIe switch configuration

`ver`: Displays version of PCIe switch serial EEPROM

- Parameters:

`prog`:

`0 - SYSCON`: Programs PLX EEPROM in TRANSPARENT mode x8 Gen3 or Gen2 (RC Class)

`1 - PERIPH`: Programs PLX EEPROM in NON-TRANSPARENT mode x8 Gen3 or Gen2 (RC Class)

`2 - PERIPH`: Programs PLX EEPROM in NON-TRANSPARENT mode x4 Gen3 or Gen2 (RC Class)

`3 - PERIPH`: Programs PLX EEPROM in NON-TRANSPARENT mode x2 Gen3 or Gen2(RC Class)

`filename`: Customs configuration filename in binary format

`dump`:

`w/o argument`: Displays on screen

`filename`: Filename of PLX EEPROM content in binary format

- **Description**

Manage PLX EEPROM on Kontron board.

- **Examples:**

To save current PLX EEPROM content to file named plx_image.bin:

```
Shell> kvpx -plx_eeprom dump plx_image.bin
```

To program file plx_image.bin:

```
Shell> kvpx -plx_eeprom prog plx_image.bin
```

To program PCIe switch in NON-TRANSPARENT mode x8 Gen3

```
Shell> kvpx -plx_eeprom prog 1
```

To display current PCIE switch configuration:

```
Shell> kvpx -plx_eeprom conf
```

To display current PLX EEPROM version:

```
Shell> kvpx -plx_eeprom ver
```

11.2 Environment Variables

EFI shell allows the user to set environment variables.

The following variables are available on the VX305x board to control the board boot behavior.

WARNING: Variable names are case sensitive.

11.2.1 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.

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

```
VX305x> set StartupAuto 1
```

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

```
VX305x> set -d StartupAuto
```

11.2.2 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.

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

```
VX305x> set StartupDelay 2
```

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

```
VX305x> set -d StartupDelay
```

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

11.2.3 BootCmd

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

1. To set **BootCmd** to run automatically the command "**pci 0 1F 0**":

```
VX305x> set BootCmd "pci 0 1F 0"
```

2. To control the **BootCmd** variable is correctly set:

```
VX305x> set
BootCmd = pci 0 1F 0
    path = .\;FS0:\efi\tools\;FS0:\efi\boot\;FS0:\
profiles = ;Install;Debug1;Driver1;network1;
```

```
uefishellsupport = 3
uefishellversion = 2.0
uefiversion = 2.40
debuglasterror = 0x0
lasterror = 0x0
```

3. To clear the **BootCmd** variable:

```
VX305x> set -d BootCmd
```

11.2.4 BootDelay

The environment variable "**BootDelay**" is used to set a timeout delay before running the command defined in the **BootCmd** variable.

1. To set **BootDelay** to 10 seconds:

```
VX305x> set BootDelay 10
```

2. To clear the **BootDelay** variable:

```
VX305x> set -d BootDelay
```

By default (ie. if **BootDelay** variable does not exist) the delay applied before **BootCmd** execution is equal to 5 seconds.

11.2.5 StopEfiShell

The environment variable "**StopEfiShell**" is used to stop the boot sequence after the **BootCmd** execution.

1. To set **StopEfiShell**:

```
VX305x> set StopEfiShell 1
```

2. To clear the **StopEfiShell** variable:

```
VX305x> set -d StopEfiShell
```

12 / BIOS Versions Description

12.1 Recommendations and Known Limitations

1. Reserved Setup settings

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

The **Bios Lock** and **Host Flash Lock-Down** options must remain **Disabled** in the IntelRCSetup/PCH Configuration/Security Configuration setup menu.

It is required for the **kflash** command.

2. After BIOS Upgrades

Just after upgrading the BIOS with the **kflash** command, the system must be turned off.

BIOS upgrade shall be completed in flash at the next power-on.

3. Kmac Command

The **kmac** command cannot be used to program the SPI flashes associated to the 10G X552 and the i210IT controllers.

It only manages the NVM areas through a Shadow RAM to change the MAC addresses and CRCs.

4. USB3.0 Super Speed

The VX305x USB 3.0 port can operate in Super Speed mode under BIOS if the xHCI controller configuration is set to **Enabled** instead of **Auto** in the IntelRCSetup/PCH Configuration/USB Configuration menu setup menu.

Refer to section 5.3.2 USB Configuration page 16 for more information.

5. UUID Setting

Full UUID management is not supported.

By default, UUID is set to NodeID depending on the VPX slotID.

6. Fast Boot

BIOS boot sequence may be speeded up by enabling the options **Attempt Fast Boot** and **Attempt Fast Cold Boot** in the **IntelRCSetup/Memory Configuration** menu. Then if it is possible, BIOS tries to use the fast path of the Memory Reference Code.

Default setting **Auto** enables the options.

7. PXE boot

When booting through PXE, set the option **Redirection After BIOS** to **Always Enabled** in the **Serial Redirection Configuration** menu to get the Intel Boot Agent messages.

8. 10G Ethernet Links

10G KR only supports auto-negotiation, forcing speed is not possible.

SFI is not operational.

9. Watchdog and UEFI Shell

Since BIOS version ID17185 the watchdog feature is applied not only to legacy boots but also to UEFI boots. As the shell is a UEFI boot device, the watchdog operates under the shell also.

Note the PBIT will save the watchdog settings before running the built-in tests (to apply its own settings) and restore them for the next boot entry, usually OS boot but also the Shell command loop.

PBIT **`haltonfail`** and **`promptonfail`** events will stop the watchdog.

If the watchdog is enabled, then a warning message is displayed before the shell prompt display for recall.

Also, to prevent any damage due to reset timeout during flash access, the **`kflash`** commands are denied. To temporary disable the watchdog without entering the setup you can type the following commands to access the CPLD WDG_CONTROL register @0x56 and reset bit0 WDG_Enb:

```
Shell> kpld -r 56
READ : @0x9 = 0x87
Shell> kpld -w 56 86
```

10. RC class board settings

On VX305x RC boards the following settings are applied by default:

- Nuvoton HW monitor: temperature high limit set to 95°C, critical temperature set to 100°C
- DDR4 Refresh Rate x2
- EIST and Turbo mode disabled (can be changed in setup)
- Cstates disabled, Monitor/MWAIT disabled (can be changed in setup)
- SATA ports speed Gen2 (can be changed in setup)
- Backplane PCIe Link speed Gen2 (can be changed in setup)

12.2 Known Problems Table

The following table lists the BIOS/PBIT relative known problems.

12.2.1 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	KDP Issue	Description	BIOS ID			
			16133	16182	17185	17347
1	22865	PCIe Port0/DMI link width trained to x2 instead of x4	X			
2	22901	**kvpx** commands with PCIE SWITCH in FAILSAFE MODE are not working correctly		X		
3	25776	Watchdog feature not supported for EFI boots	X	X		
4	26443	VPD EEPROM error under Linux	X	X		
5	26635	PXE issue after PBIT run	X	X		
6	27081	Boot menu is not available	X	X		
7	30052	PBIT Ethernet test, watchdog timeout if Ethernet SPI flash corrupted	X	X		
8	33523	SPI boot flash is not correctly protected	X	X	X	
9	30740	SPD check failure during PBIT memory tests with DDR4 2400			X	

12.2.2 Detailed Description of the Problems

Item #1 PCIe Port0/DMI link width trained to x2 instead of x4- KDP 22865

Description: The PCIe Port0/DMI link bandwidth is degraded to x2 instead of x4.

This causes poor performance on SATA and USB links.

Workaround: Disable the CPU to PCH Throttle option in the IntelRCSetup/Advanced Power Management Configuration/CPU Thermal Management setup menu.

Fixed in the BIOS versions > ID16133.

Item #2 kvpx commands with PCIE SWITCH in FAILSAFE MODE are not working correctly - KDP 22901

Description: If the PCIe Switch Failsafe Mode SW2.3 is set to ON, then the `kvpx -plx_eeprom prog/conf/dump/ver` commands are not working correctly. The command attempts PCIe instead of I2C access to the PLX EEPROM.

Workaround: Set manually the CPLD register 0x71 at 0x10 instead of 0x11 by using the command `kpld -w 71 10`, then run the `kvpx` command.

When PLX is in Maintenance mode, the EEPROM is not accessible, so the command '`kvpx -plx_eeprom conf`' displays:

```
kvpx: PCIe Switch is in FailSafe mode.
ERROR : PCI Express Switch PLX not found.
```

This is a normal behaviour.

The other command `kvpx -plx_eeprom` '`dump/prog/ver`' are working correctly with this work-around.

Item #3 Watchdog feature not supported for EFI boots - KDP 25776

Description: There is no timeout when enabling the watchdog under BIOS and blocking UEFI boot (for instance staying under grub). It does not occur on Legacy boot.

This feature is implemented in BIOS for Legacy boots but not for UEFI boots.

Workaround: None

Item #4 VPD EEPROM error under Linux - KDP 26443

Description: Linux `vpdtool` returns an error on VX305x RC boards.

This is due to the CPLD register PWON_STATUS layout managed by BIOS that is no more compatible with Linux tool.

Workaround: None

Item #5 PXE issue after PBIT run - KDP 26635

Description: After "`kdiag run`", PXE is not functional anymore and returns the following error:

`PXE-EC8`: !PXE structure was not found in UNDI driver code segment.

`PXE-M0F`: Exiting Intel Boot Agent.

Workaround: None

Item #6 Boot menu is not available - KDP 27081

Description: No BBS menu available by pressing function key <F7> as usual.

Workaround: None

Item #7 PBIT Ethernet test, watchdog timeout if Ethernet SPI flash corrupted - KDP 30052

Description: If the SPI flash of an Ethernet interface is corrupted, then running the PBIT Ethernet test causes a watchdog timeout.

This is due to the dump of the flash data that takes a long time.

Workaround: None

Item #8 SPI boot flash is not correctly protected - KDP 33523

Description: The Block Protect bits of the Write Status register are not correctly managed when using the kflash command.

Workaround: None

Item #9 SPD check failure during PBIT memory tests with DDR4 2400- KDP 30740

Description: PBIT memory tests fail with SPD check error if the board is equipped with DDR4-2400 devices.

Workaround: None

12.3 BIOS ID16064 Release Notes

This is the first BIOS production release.

This release is based on the AMI Grangeville_022 release including the Intel Reference Code 2.0.0 Production Release and the SPS firmware v3.0.3.20.

It also updates the processor microcode into the 07000009 version (for processor V2).

The following lists the Kontron specifics implemented in the release .

- Accessible by setup:
  - 1Gb Ethernet Front/Rear Configuration - Section 6.1.1 page 18
  - Graphic Front/Rear Configuration - Section 6.1.2 page 19
  - Serial COM0 RS232/RS485 Configuration - Section 6.1.3 page 19
  - USB keyboard US/FR Configuration - Section 6.1.5 page 20
  - Watchdog at Startup and for OS boot Configuration - Section 6.1.6 page 20
  - VPX Reset and PCIe Switch Configuration - Section 6.2 page 22

- Accessible by Kontron EFI commands (Refer to chapter 11 page 34 for details):
  - kdiag, Board diagnostics (only if ordered)
  - kflash, SPI boot flasher.
  - kmac, MAC address management utility
  - kpld, PLD management utility
  - ksensor, sensor utility
  - kvpd, Vital Product Data information
  - kvpx, VPX PCIe Switch configurator

12.4 BIOS ID16133 Release Notes

- Updated with AMI Grangeville_023 release including Intel Reference Code 2.0.0 Production Release and SPS firmware v3.0.3.23
- Updated versions of Ethernet UEFI drivers for PBIT:
  - for 10GbE: v5.1.1 x64 -> 5.2.05 x64
  - for i210: v6.9.07 PCI-E -> 7.0.06 PCI-E
- Updated CSM module version 10: fixes Intel Boot Agent header display on serial redirection when OpRom is loaded.
- Set CSM16 INT19 retry feature when PXE boot is enabled to loop on legacy boot.
  Useful on diskless system to enable slave boards waiting for the server.
- Updated i210 LOM file with Intel BootAgent version 1.5.78: 10G LOM file suppressed as NVM in flash includes PXE software already.
- Added setup options to enable/disable PXE OpRom loading individually on each LAN.
  Useful to reduce boot time in a PXE configuration.
- Enabled RAID management (RSTE_SUPPORT token).
- Fixed issue on FRAM access: low speed I2C clock instead of fast speed.
- Fixed issue on backplane SMBUS access: bad write-protection check.
- Improved "**`kmac -v`**" to get more info about 10G NVM version.
- Improved "**`kvpd -m`**" to manage backspace key.

Includes PBIT(*) v1.4 ID16081:

- Added cpld(24), eeprom(71), smbus0(26), smbus1(27), fram(40), sysflash(22), m2_bottom(14), m2_top(15) and tpm(11) tests.
- Added system(89) test and "**`kdiag edit system`**" command to customize the system test.
- Improved SATA controllers test in customer mode as controllers are automatically disabled if no device is connected.

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

For more information, please contact your field representative.

12.5 BIOS ID16182 Release Notes

- Updated with AMI Grangeville_026 release including Intel Reference Code 2.2.0, SPS firmware 3.0.3.25, microcode 0700000C.
- Added SPD support for DDR4 2133MT/s 8Gb single die devices.
- Workaround for KDP#21928/CRP#xxxxx: DMI link width x2 instead of x4 involving poor performance on SATA and USB links. GPIO4 is forced to GPO at level 0 to override hardware setting.
- Set default Fast Boot setup options (Auto) to Enable instead of Disable for warm and cold boot to reduce boot time.
- Hide IOU0 configuration in setup to follow Grangeville override.

Includes PBIT(*) v1.5 ID16150:

- Memory test improved with ECC error registers reported in case of correctable ECC errors. Applied to PBIT memory unitary tests and Early Memory Test in factory mode.
- PBIT m2_top and m2_bottom tests improved to control the CPLD register M.2 Slots Configuration @0xB against VPD.
- Do not print LocateHandle error message if no SATA or USB device is detected while learning the system configuration (kdiag learn system). However the error message is still consistent for the unitary SATA and USB tests that require to detect a device. Also, detect the configuration where no SATA device is connected as controllers are automatically disabled then.

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

For more information, please contact your field representative.

12.6 BIOS ID17185 Release Notes

This BIOS/PBIT version supports the VX305x RC boards (EFT).

- Code updated with AMI Grangeville_029 release: Intel Reference Code 2.3.0, SPS fw 3.0.3.25, microcode V2 0700000C
- Kdp#22901 fixed: PEX8725 EEPROM programmation issue in PCIe Failsafe mode
- Write protection warning added for FRAM at 0xA6.
- Image execution policy override options added in **SecureBoot** menu.
- **MaskableReset** configuration added in CPLD config data in OS EEPROM at offset @0x6100.
- Enable Built-in EFI Shell even with Secure Boot enabled to allow PBIT execution.
- Kdp#26443 fixed: in CPLD reg @0x3 move boardclass bits to 6-5 instead of 5-4 for Linux BSP compatibility.
- Kdp#27081 fixed: add BBS popup menu, accessible with function key <F7>.
- Kdp#25776 fixed: watchdog feature now supported for EFI boots.

  Caution, the EFI shell is then also involved. Refer to section 12.1, recommendation 9.
- Warning added before shell prompt if watchdog is enabled and **kflash** commands denied to prevent any reset timeout during flash updates.
- Support for Samsung 8Gb K4A8G085WB-BIRC.
- Support of VX305x RC.

  Set default DDR4 refresh rate to x2 (tREFI 3.9µs) for RC class board. Refer to section 12.1, recommendation 10.

  New PEX8725 EEPROM ID17164 for setting backplane PCIe Link Speed. Update **kvpx** utility with new EEPROM and set default PCIe Link Speed Gen2/Gen3 according to board class SA/RC.

Includes PBIT(*) v1.6 ID17185:

- Improved sata controllers test in IDE mode and sata dev tests according to controller presence.
- Kdp#26635 fixed: PXE issue after running PBIT memory tests.
- Kdp#25776 fixed: watchdog feature now supported for EFI boots. "**kdiag run**" saves the watchdog settings and restores them for the next boot entry.

  promptonfail/**haltonfail** events stops the watchdog.
- Added warning in **kdiag run** if the SYSTEM EEPROM is write protected.
- In cpld test do not stop the test in case of error to check all the features.
- Kdp#30052 fixed: in Ethernet test, prevent watchdog timeout if Ethernet SPI flash is corrupted.
- Update **pcie_vpx_switch** test for checking the backplane PCIe link speed Gen2/Gen3 according to board class SA/RC.

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

For more information, please contact your field representative.

12.7 BIOS ID17347 Release Notes

- Source code updated with AMI Grangeville_036 release: Intel Reference Code 2.5.0, SPS firmware 3.0.3.31, microcode V2 0700000E
- Password authentication added on Shell access if an Admin password has been set for BIOS setup access.
- Password now supports case sensitive characters.
- Kdp#33523 fixed: SPI boot flash is not correctly protected.
- If the SPI boot flash is write protected, prevent error messages at startup when managing Nvram variables.
- Update SMBIOS tables types 28 and 36 for Temperature Probe according to the board class SA/RC.

Includes PBIT(*) V1.7 ID17320:

- Fixed kdp#30740 issue in PBIT memory test with DDR4-2400 devices. An error is returned when checking the SPD EEPROMs content.

(*) 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.

13 / Use Cases

This chapter gives some advise for following pratical cases:

- DEPLOY : How to deploy VX305x - BIOS, section 13.1 page 52
- DEVEL: How to develop applications with VX305x - BIOS, section 13.2 page 53
- EVAL: How to benchmark VX305x - BIOS, section 13.3 page 53
- TROUBLESHOOTING: Useful Tips, section 13.4 page 53

13.1 DEPLOY: How to deploy VX305x - BIOS

Deploying with VX305x boards usually requires to handle the following tasks:

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

13.1.1 Cloning a board

To be able to replace a VX305x with another one in a system, cloning allows to duplicate the VX305x settings onto the new board prior replacement:

- **On the initial VX305x**
  - Get the hardware settings: refer to the VX305x User's Guide: section 2.3 Board Configuration
  - Get the BIOS settings: BIOS software and settings are stored in the BIOS SPI flash device itself. Use `kflash -s` command to retrieve the flash content in a file.
- **On the new VX305x**
  - Check the board ECLevel to be sure the BIOS and Settings you are going to download are compatible with the hardware evolution.
  - Flash the binary file by using `kflash -p -r` command. Powercycle the board and set the Date/Time.

The new VX305x board is now a functional clone of the initial one.

Once the system has been qualified, it should be worth saving the image of the BIOS and Settings for a later use. For large programs, Kontron can contribute with high level software to automate this cloning task.

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

13.1.2 Managing a pool of VX305x

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

Refer to section 2.2 of VX305x User's Guide about the board identification labels.

Also use the `kvpd -p` command to retrieve the Vital Product Data.

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

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

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

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

13.2 DEVEL: How to develop applications with VX305x - BIOS

TBD

13.3 EVAL: How to benchmark VX305x - BIOS

TBD

13.4 TROUBLESHOOTING: Useful Tips

SETUP is not accessible

If trouble occurred after changing the setup, it should be worth booting in BIOS FailSafe Mode(*) to force the default settings to be reloaded at startup. Then, save the reloaded settings (see Save and Exit menu). Power off, reconfigure the board in Normal Mode(*) and power on.

If BIOS does not boot in Normal Mode(*), make sure the board is still operational in Rescue Mode(*). In Rescue Mode, you can then clone the rescue boot flash into the normal boot flash by using the `kflash -c` shell command.

SETUP is accessible but OS does not boot

Enter setup by pressing the <DEL> key as indicated at BIOS boot time and check if the boot device is visible in the boot device list. See section 8.3 page 28 Boot Option Priorities in this document.

If the device is still not present, it should be worth restoring the manufacturing settings. Select the **`Restore Defaults`** option in the **`Save and Exit`** menu, then Save and Reset, and verify if the boot device is now visible.

No 1GbE link

Verify the Ethernet route option (front/rear) for the corresponding 1GbE interface in the Kontron menu.

No video

Verify the video route option (front/rear) in the Kontron menu.

If there are several graphic components connected in the system (onboard M.2 GFX module and others), verify the Active Video Device selection is correct.

See chapter 5.4 page 16.

No 10G Ethernet backplane link

Verify the LANs configuration with the `kmac -conf` shell command. 10G LANs must be configured in KR mode. The link status can be verified with the `kmac -stat` command. May be negotiation with the link partner has been done at 1Gb.

Verify also the Ethernet routing layout of your backplane.

No messages on the serial line.

COM0 line is accessible on front or at rear without any setup selection. Note that when COM0 is configured in RS422/RS485, COM1 line (rear only) is not accessible any more.

If the Serial Redirection on COM0 has been unintentionally disabled, boot the board in BIOS FailSafe Mode(*) to force the default settings to be reloaded at startup. By default COM0 line mode will be RS232.

(*) VX305x User's Guide, section Board Configuration to change the boot modes by selecting the board switches.

Backplane PCIe dysfunction

If trouble occurs with the backplane PCIe discovery, you can reprogram the PCIe Switch EEPROM by using the **`kvpx -plx_eeprom prog <num>`** command according to the location of the board in the system (System Controller slot or Peripheral slot).

Then, in the Kontron menu, you can select the wanted PCIe link width and speed, enable the VPX EPROM Configuration option and reset the board.

It is not recommended to keep the VPX EPROM Configuration option enabled.

Appendix A - How to Update and Restore the BIOS

A.1 Update BIOS from UEFI Shell using USB device

This section details the update of the AMI BIOS Firmware on a VX305x board. An USB key with the BIOS image to flash will be used:

- Copy the BIOS image under the USB device
- Boot VX305x on UEFI shell. If necessary enter the BIOS SETUP. 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

```
VX305x> map -r
```

- fs0: file system must become visible, then Enter

```
VX305x> 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 **VX305x_IDYYXXX.bin** then flash the BIOS entering command

```
VX305x> kflash -p -r  VX305x_IDYYXXX.bin
```

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

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

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

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

A.2 Restore or Update BIOS from Rescue BIOS

A rescue BIOS is available on any VX305x CPU. It is possible to boot on rescue BIOS and update the main BIOS with the rescue BIOS.

When board is powered off, set micro switch SW2 function 1 to ON. Then Boot on Rescue BIOS and EFI-Shell. If necessary enter BIOS SETUP and then navigate to Save & Exit Menu and select UEFI shell in Boot override menu. Check if EFI-Shell prompt is VX305x-RESCUE.

- Enter command:

```
VX305x-RESCUE> kflash -c
```

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

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

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

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

This section details the record of the AMI BIOS Firmware and its setting of a VX305x board. An USB key will be used to store the BIOS image:

- Boot VX305x on UEFI shell. If necessary enter BIOS SETUP. 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

```
VX305x> map -r
```

- fs0: file system must become visible, then Enter

```
VX305x> 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 **VX305x_CLONE.bin** then copy the BIOS image entering command

```
VX305x> kflash -s  VX305x_CLONE.bin
```

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

About Kontron - An S&T Company

Kontron is a global leader in IoT/Embedded Computing Technology (ECT). As a part of technology group S&T, Kontron offers a combined portfolio of secure hardware, middleware and services for Internet of Things (IoT) and Industry 4.0 applications. With its standard products and tailor-made solutions based on highly reliable state-of-the-art embedded technologies, Kontron provides secure and innovative applications for a variety of industries. As a result, customers benefit from accelerated time-to-market, reduced total cost of ownership, product longevity and the best fully integrated applications overall.

For more information, please visit: **www.kontron.com**

CORPORATE OFFICES

FRANCE

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

GLOBAL HEADQUARTERS

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

NORTH AMERICA

9477 Waples Street, Suite 150
San Diego, CA 92121
USA
Tel.: + 1 888 294 4558
Fax: + 1 858 677 0898
info@us.kontron.com

ASIA PACIFIC

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