

VPX6200 BIOS

User's Manual

Manual Rev.:	Rev. 1.0
Revision Date:	April 30, 2024
Part No.:	50M-31428-2000

Preface

Copyright © 2024 ADLINK Technology, Inc.

This document contains proprietary information protected by copyright. All rights are reserved. No part of this manual may be reproduced by any mechanical, electronic, or other means in any form without prior written permission of the manufacturer.

Disclaimer

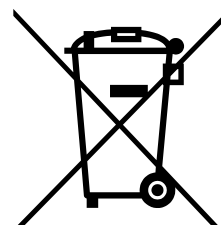
The information in this document is subject to change without prior notice in order to improve reliability, design, and function and does not represent a commitment on the part of the manufacturer.

In no event will the manufacturer be liable for direct, indirect, special, incidental, or consequential damages arising out of the use or inability to use the product or documentation, even if advised of the possibility of such damages.

Environmental Responsibility

ADLINK is committed to fulfill its social responsibility to global environmental preservation through compliance with the European Union's Restriction of Hazardous Substances (RoHS) directive and Waste Electrical and Electronic Equipment (WEEE) directive.

Environmental protection is a top priority for ADLINK. We have enforced measures to ensure that our products, manufacturing processes, components, and raw materials have as little impact on the environment as possible. When products are at their end of life, our customers are encouraged to dispose of them in accordance with the product disposal and/or recovery programs prescribed by their nation or company.



Trademarks

Product names mentioned herein are used for identification purposes only and may be trademarks and/or registered trademarks of their respective companies.

Revision History

Revision	Release Date	Description of Change(s)
1.0	2024-04-30	Initial release

Table of Contents

Preface	2
Table of Contents.....	3
1 BIOS Setup Menu	5
1.1 Introduction.....	5
1.2 Menu Selection Bar	5
1.3 Menu Conventions.....	5
2 Getting Started.....	6
2.1 BIOS Information	7
2.2 System Information.....	7
2.3 System Date/Time	8
2.4 Board Information.....	8
3 Advanced Menu	10
3.1 CPU Configuration.....	11
3.2 Power & Performance	12
3.2.1 CPU – Power Management Control	12
3.2.2 GT – Power Management Control.....	23
3.3 Power Management	24
3.3.1 Voltage Monitor.....	25
3.4 System Management.....	26
3.4.1 SEMA Flags	27
3.5 Thermal Management	28
3.5.1 CPU Thermal Configuration.....	29
3.5.2 Platform Thermal Configuration.....	30
3.5.3 Temperatures.....	33
3.6 Watchdog Timer	34
3.7 Super IO Configuration	35
3.7.1 NCT5104DSEC Super IO Configuration	35
3.8 VPX Configuration	37
3.9 USB Configuration.....	39
3.10 AMI Graphic Output Protocol Policy.....	40
3.11 Serial Port Console Redirection	41
3.12 Network Stack Configuration.....	42
3.13 Trusted Computing	43
4 Chipset Menu	45
4.1 System Agent (SA) Configuration	46
4.1.1 Memory Configuration	47
4.1.2 PEG Port Feature Configuration.....	48
4.1.3 VMD Setup Menu	48
4.1.4 PCI Express Configuration	49
4.2 PCH-IO Configuration.....	52
4.2.1 SATA and RST Configuration	54
4.2.2 Software Feature Mask Configuration	56
4.2.3 USB Configuration	57
4.2.4 Security Configuration	58
4.2.5 HD Audio Configuration	59

4.2.6	Serial IO Configuration	60
4.2.7	PCH Thermal Throttling Control	61
5	Server Mgmt Menu	62
5.1	System Event Log	63
5.2	View FRU Information.....	64
5.3	BMC Network Configuration	65
5.4	ADLINK IPMI Configuration	66
5.5	View System Event Log.....	67
5.6	BMC User Settings	67
6	Security Menu	68
6.1	Secure Boot.....	70
7	Boot Menu	71
8	Save & Exit.....	73
	Important Safety Instructions.....	74
	Getting Service	76

1 BIOS Setup Menu

1.1 Introduction

The BIOS setup utility is invoked by pressing <ESC> or keys. User can change BIOS settings during setup utility runs. A reset of system is required in order to make new settings take effect.

In BIOS setup utility, there are several hot keys designed for specific purposes. Hot keys are listed below.

- <F1>: General help in setup menu
- <F8>: Load previous BIOS values
- <F9>: Load BIOS default in setup utility
- <F10>: Save & Exit setup utility

1.2 Menu Selection Bar

The Menu Selection Bar is located at the top of the screen. It displays the top level available menus to the user:

- Main Menu
- Advanced Menu
- Chipset Menu
- Server Mgmt Menu
- Security Menu
- Boot Menu
- Save & Exit Menu

1.3 Menu Conventions

The appearance of setup menu listed in this chapter is a sample to describe the item list. It is shown on VT100 terminal via serial console. Followings are the menu conventions.

- Using color

The mandatory BIOS setup fields are in black. The BIOS setup fields currently not used are in grey. The display only strings are in black.

- Using brackets

Editable menu options are marketed with squares '[' and ']' to distinguish them from display only fields that can't be modified.

2 Getting Started

The Main Menu provides read-only information about system and also allows to set system's date and time. Refer to the tables below, it shows the screen shot of Main menu for detail, and submenus and settings as well.

Aptio Setup – AMI		
Main	Advanced	Chipset Server Mgmt Security Boot Save & Exit
BIOS Information		Set the Date. Use Tab to switch between Date elements.
BIOS Vendor	American Megatrends	
BIOS Version	0.14.10	
Build Date	04/9/2023	
SEMA Firmware Version	ADLINK 001	
BMC Firmware Version	1.04	
MRC Version	2.2.0.9	
GOP Version	17.0.1075	
ME FW Version	15.0.41.2142	
BIOS Boot Source	Primary BIOS	
System Information		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit
Project Name	VPX-6200	
Product ID	KX SKU	
System Node	A	
CPU Board Version	A1	
CPU Brand String	Intel(R) Xeon(R) W-1186 5MRE @ 2.60GHz	
CPU Frequency	2.6GHz	
Total Memory	32768 MB (DDR4)	
Memory Frequency	3200 MHz	
PCH SKU	H RM590E	
> Board Information		
System Date	[Thu 01/07/2022]	
System Time	[16:28:59]	
Access Level	Administrator	

2.1 BIOS Information

BIOS Item	Options	Description
BIOS Vendor	Info-only. American Megatrends	Display vendor name of system BIOS.
BIOS Version	Info-only. x.yy.zz	Display version of booting BIOS.
Build Date	Info-only. MM/DD/YYYY	It shows the date that BIOS was built.
SEMA Firmware Version	Info-only.	Display version of SEMA EC
BMC Firmware Version	Info-only.	Display version of IPMI
MRC Version	Info-only. w.x.y.z	Display the revision of MRC code which is implemented in BIOS.
GOP Version	Info-only. yyyy/x.y.zzzz	<i>GOP Version:</i> When video option ROM is set to "UEFI Only", it will show up.
ME FW Version	Info-only. ww.x.yy.zzzz	Display the version of Intel manageability firmware which is implemented in BIOS.
BIOS Boot Source	Info-only. Primary BIOS/Backup BIOS	It shows which BIOS flash boots the system. <i>Primary BIOS:</i> usually means that boots from SPI0 <i>Backup BIOS:</i> usually means that boots from SPI1

2.2 System Information

BIOS Item	Options	Description
Project Name	Info-only. VPX-6200	It shows the project name.
Product ID	Info-only.	It shows the Product ID. KX or KR SKU.
System Node	Info-only.	It shows the System Node. Node A or B.
CPU Board Version	Info-only. A1/A2/A3/...	It shows the CPU board HW version.
CPU Brand String	Info-only. Intel(R) Core, ...	It shows what CPU is booting the system.
CPU Frequency	Info-only. XXXX GHz	It shows CPU's frequency.
Total Memory	Info-only. XXXX MB (DDRx)	It shows total memory size used on the motherboard and memory type.
Memory Frequency	Info-only. XXXX MHz	It shows memory's frequency.
PCH SKU	Info-only. xxxx	It shows what PCH SKU is designed on motherboard.

2.3 System Date/Time

BIOS Item	Options	Description
System Date	MM/DD/YYYY	For configuring/showing system date. When setting the Date, use <Tab> key to switch between Date elements.
System Time	HH:MM:SS	For configuring/showing system time. When setting the Time, use <Tab> key to switch between Time elements.
Access Level	Info-only. Administrator/User	It shows what access level is used to enter BIOS setup menu.

2.4 Board Information

Aptio Setup – AMI

Main

Board Information		
Serial Number	N/A	
Manufacturing Date	N/A	
Last Repair Date	N/A	
MAC ID	N/A	
Runtime Statistics		
Total Runtime	12h 51m	
Current Runtime	0h 01m 29s	
Boot Cycles	198	
Boot Reason	Software-reset	
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
Serial Number	Info-only.	Display board's serial number.
Manufacturing Date	Info-only.	Display manufacturing date.
Last Repair Date	Info-only.	Display Last Repair Date.
MAC ID	Info-only.	Shows onboard Ethernet's MAC ID.
Total Runtime	Info-only.	The returned value specifies the total time in minutes the system is running in S0 state.
Current Runtime	Info-only.	The returned value specifies the time in

		seconds the system is running in S0 state. This counter is cleared when the system is removed from the external power supply.
Boot Cycles	Info-only.	The boot cycle is increased after a HW or SW reset or after a successful power-up.
Boot Reason	Info-only.	The boot reason is the event which causes the reboot of the system.

3 Advanced Menu

This menu contains the settings for most of the user interfaces in the system.

Aptio Setup – AMI		
Main	Advanced	Chipset Server Mgmt Security Boot Save & Exit
> CPU Configuration > Power & Performance > Power Management > System Management > Thermal Management > Watchdog Timer > Super IO Configuration > VPX Configuration > USB Configuration > AMI Graphic Output Protocol Policy > Serial Port Console Redirection > Network Stack Configuration > Trusted Computing > TLS Auth Configuration > RAM Disk Configuration		CPU Configuration Parameters ><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
CPU Configuration	Submenu	For configuring CPU features/functions.
Power & Performance	Submenu	For configuring Power & Performance Options
Power Management	Submenu	
System Management	Submenu	
Thermal Management	Submenu	
Watchdog Timer	Submenu	
Super IO Configuration	Submenu	
VPX Configuration	Submenu	
USB Configuration	Submenu	
AMI Graphic Output Protocol Policy	Submenu	User Select Monitor Output by Graphic Output Protocol
Network Stack Configuration	Submenu	
Trusted Computing	Submenu	
TLS Auth Configuration	Submenu	
RAM Disk Configuration	Submenu	

3.1 CPU Configuration

Aptio Setup – AMI

Advanced

CPU Configuration		
Type	Intel(R) Xeon(R) W-11865MRE@2.60GHz	
Speed	2600 MHz	
ID	0x806D1	
Stepping	R0	
Number of Processors	8Core(s) / 8Thread(s)	
Microcode Revision	40	
GT Info	0x9A70	
eDRAM Size	N/A	
L1 Instruction Cache	32 KB x 8	
L2 Cache	1280 KB x 8	
L3 Cache	24MB	
L4 Cache	N/A	
VMX	Supported	
SMX/TXT	Supported	
Intel (VMX) Virtualization Technology	[Enable]	
Active Processor Cores	[All]	
Hyper-Threading	[Enabled]	
Intel Trusted Execution Technology	[Disabled]	

><: Select Screen
 ^v: Select Item
 Enter: Select
 +/-: Change Opt.
 F1: General Help
 F8: Previous Values
 F9: Optimized Default
 F10: Save & Exit
 ESC: Exit

BIOS Item	Options	Description
Type	Info-only.	It shows what detail CPU information
Speed	Info-only.	It shows what detail CPU information
ID	Info-only.	It shows what detail CPU information
Stepping	Info-only.	It shows what detail CPU information
Number of Processors	Info-only.	It shows what detail CPU information
Microcode Revision	Info-only.	It shows what detail CPU information
GT Info	Info-only.	It shows what detail CPU information
eDRAM Size	Info-only.	It shows what detail CPU information
L1 Instruction Cache	Info-only.	It shows what detail CPU information
L2 Cache	Info-only.	It shows what detail CPU information
L3 Cache	Info-only.	It shows what detail CPU information
L4 Cache	Info-only.	It shows what detail CPU information
VMX	Info-only.	It shows what CPU support feature.
SMX/TXT	Info-only.	It shows what CPU support feature.
Intel (VMX) Virtualization Technology	Enabled Disabled	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.
Active Processor Cores	All / 1 / 2 / 3 / 4 / 5	Number of cores to enable in each processor package.
Hyper-Threading	Enabled Disabled	Enable or Disable Hyper-Threading Technology.

Intel Trusted Execution Technology	Enabled Disabled	Enables utilization of additional hardware capabilities provided by Intel (R) Trusted Execution Technology. Changes require a full power cycle to take effect.
------------------------------------	----------------------------	---

3.2 Power & Performance

Aptio Setup – AMI

Advanced

>CPU – Power Management Control >GT – Power Management Control	CPU – Power Management Control Options
	><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
CPU – Power Management Control	Submenu	CPU – Power Management Control Options
GT – Power Management Control	Submenu	GT – Power Management Control Options

3.2.1 CPU – Power Management Control

Aptio Setup – AMI

Advanced

CPU – Power Management Control	CPU – Power Management Control Options
Boot performance mode Intel(R) SpeedStep(tm) Race To Halt (RTH) Intel(R) Speed Shift Technology Per Core P State OS control mode HwP Autonomous Per Core P State HwP Autonomous EPP Grouping EPB override over PECl HwP Fast MSR Support HDC Control > Config TDP Configurations	[Turbo Performance] [Disabled] [Enabled] [Enabled] [Enabled] [Enabled] [Enabled] [Disabled] [Enabled] [Enabled]

> CPU VR Settings		
Platform PL1 Enable	[Disabled]	
Platform PL2 Enable	[Disabled]	
Power Limit 4 Override	[Disabled]	
C states	[Disabled]	
Thermal Monitor	[Enabled]	
Interrupt Redirection Mode Selection	[Fixed Priority]	
Timed MWAIT	[Disabled]	
> Custom P-state Table		
Energy Performance Gain	[Disabled]	
EPG DIMM Idd3N		
EPG DIMM Idd3P		
> Power Limit 3 Settings		
> CPU Lock Configuration		

^v: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F8: Previous Values
F9: Optimized Default
F10: Save & Exit
ESC: Exit

BIOS Item	Options	Description
Boot performance mode	Max Battery Max Non-Turbo Performance Turbo Performance	Select the performance state that the BIOS will set starting from reset vector.
Intel(R) SpeedStep(tm)	Enabled Disabled	Allows more than two frequency ranges to be supported.
Race To Halt (RTH)	Enabled Disabled	Enable/Disable Race To Halt feature. RTH will dynamically increase CPU frequency in order to enter pkg C-State faster to reduce overall power. (RTH is controlled through MSR 1FC bit 20)
Intel(R) Speed Shift Technology	Enabled Disabled	Enable/Disable Intel(R) Speed Shift Technology support. Enabling will expose the CPPC v2 interface to allow for hardware controlled P-states.
Per Core P State OS control mode	Enabled Disabled	Enable/Disable Per Core P state OS control mode. Disabling will set Bit 31 = 1 command 0x06. When set, the highest core request is used for all other core requests.
HwP Autonomous Per Core P State	Enabled Disabled	Disable Autonomous PCPS (Bit 30 = 1, command 0x11) Autonomous will request the same value for all cores all the time. Enable PCPS (default Bit 30 = 0, command 0x11)
HwP Autonomous EPP Grouping	Enabled Disabled	Enable EPP grouping (default Bit 29 =0, command 0x11) Autonomous will request the same values for all cores with same EPP. Disable EPP grouping (Bit 29 =1 , command 0x11) autonomous will not necessarily request same values for all cores with same EPP.
EPB override over PECl	Enabled Disabled	Enable/Disable EPB override over PECl. Enable by sending pcode command 0x2b , subcommand 0x3 to 1. This will allow OOB EPB PECl override control

BIOS Item	Options	Description
HwP Fast MSR Support	Enabled Disabled	Enable/Disable HwP Fast MSR Support for IA32_HWP_REQUEST MSR.
HDC Control	Enabled Disabled	This option allows HDC configuration.
Config TDP Configurations	Submenu	
CPU VR Settings	Submenu	
Platform PL1 Enable	Enabled Disabled	Enable/Disable Platform Power Limit 1 programming. If this option is enabled, it activates the PL1 value to be used by the processor to limit the average power of given time window.
Platform PL2 Enable	Enabled Disabled	Enable/Disable Platform Power Limit 2 programming. If this option is disabled, BIOS will program the default values for Platform Power Limit 2.
Power Limit 4 Override	Enabled Disabled	Enable/Disable Power Limit 4 override. If this option is disabled, BIOS will leave the default values for Power Limit 4.
C states	Enabled Disabled	Enable/Disable CPU Power Management. Allows CPU to go to C states when it's not 100% utilized.
Thermal Monitor	Enabled Disabled	Enable/Disable Thermal Monitor
Interrupt Redirection Mode Selection	Fixed Priority Round robin Hash Vector No Change	Interrupt Redirection Mode Select for Logical Interrupts
Timed MWAIT	Enabled Disabled	Enable/Disable Timed MWAIT Support
Custom P-state Table	Submenu	
Energy Performance Gain	Enabled Disabled	Enable/disable Energy Performance Gain.
EPG DIMM Idd3N	26	Active standby current (Idd3N) in milliamps from datasheet. Must be calculated on a per DIMM basis.
EPG DIMM Idd3P	11	Active power-down current (Idd3P) in milliamps from datasheet. Must be calculated on a per DIMM basis.
Power Limit 3 Settings	Submenu	
CPU Lock Configuration	Submenu	

CPU – Power Management Control → Config TDP Configurations

Aptio Setup – AMI

Advanced

Config TDP Configurations	
Enable Configurable TDP	Applies to cTDP
Configurable TDP Boot Mode	Nominal
Configurable TDP Lock	Disabled

CTDP BIOS control	Disabled	
ConfigTDP Levels	2	
ConfigTDP Turbo Activation Ratio	25 (Unlocked)	
Power Limit 1	25.0W (MSR:35.0)	
Power Limit 2	56.250W (MSR:56.250)	
Custom Settings Nominal		
ConfigTDP Nominal	Ratio:26 TAR:25 PL1:45.0W	><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit
Power Limit 1	25000	
Power Limit 2	0	
Power Limit 1 Time Window*	[1]	
ConfigTDP Turbo Activation Ratio	0	
Custom Settings Down		
ConfigTDP Level1	Ratio:21 TAR:20 PL1:35.0W	
Power Limit 1	0	
Power Limit 2	0	
Power Limit 1 Time Window*	[0]	
ConfigTDP Turbo Activation Ratio	0	

BIOS Item	Options	Description
Enable Configurable TDP	Applies to non-cTDP Applies to cTDP	Applies TDP initialization settings based on non-cTDP or cTDP. Default is 1: Applies to cTDP; if 0 then applies non-cTDP and BIOS will bypass cTDP initialization flow
Configurable TDP Boot Mode	Nominal Down Up Deactivate	Configurable TDP Mode as Nominal/Up/Down/Deactivate TDP selection. Deactivate option will set MSR to Nominal and MMIO to Zero.
Configurable TDP Lock	Enabled Disabled	Configurable TDP Mode Lock sets the Lock bits on TURBO_ACTIVATION_RATIO and CONFIG_TDP_CONTROL. Note: When CTDP Lock is enabled Custom ConfigTDP Count will be forced to 1 and Custom ConfigTDP Boot Index will be forced to 0.
CTDP BIOS control	Enabled Disabled	Enables CTDP control via runtime ACPI BIOS methods. This "BIOS only" feature does not require EC or driver support.
ConfigTDP Levels	Info-only.	
ConfigTDP Turbo Activation Ratio	Info-only.	
Power Limit 1	Info-only.	
Power Limit 2	Info-only.	
ConfigTDP Nominal	Info-only.	
Power Limit 1	25000	Power Limit 1 in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Overclocking SKU:

BIOS Item	Options	Description
		Value must be between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). Other SKUs: This value must be between Min Power Limit and TDP
Power Limit 2	0	Power Limit 2 value in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Processor applies control policies such that the package power does not exceed this limit.
Power Limit 1 Time Window*	[0]	Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0 = default value (28 sec for Mobile and 8 sec for Desktop). Defines time window which TDP value should be maintained.
ConfigTDP Turbo Activation Ratio	0	Custom value for Turbo Activation Ratio. Needs to be configured with valid values from LFM to Max Turbo. 0 means don't use custom value.
ConfigTDP Level1	Info-only.	
Power Limit 1	0	Power Limit 1 in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Overclocking SKU: Value must be between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). Other SKUs: This value must be between Min Power Limit and TDP
Power Limit 2	0	Power Limit 2 value in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Processor applies control policies such that the package power does not exceed this limit.
Power Limit 1 Time Window*	[0]	Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0 = default value (28 sec for Mobile and 8 sec for Desktop). Defines time window which TDP value should be maintained.
ConfigTDP Turbo Activation Ratio	0	Custom value for Turbo Activation Ratio. Needs to be configured with valid values from LFM to Max Turbo. 0 means don't use custom value.

CPU – Power Management Control → CPU VR Settings

Aptio Setup – AMI

Advanced

CPU VR Settings		
PSYS Slope	0	
PSYS Offset	0	
PSYS Prefix	[+]	
PSYS PMax Power	0	
Min Voltage Override	[Disabled]	
> Acoustic Noise Settings		
> VccIn VR Settings		
> RFI Settings		
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
PSYS Slope	0	PSYS Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x9."
PSYS Offset	0	PSYS Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. PSYS Uses BIOS VR mailbox command 0x4.
PSYS Prefix	+ -	Sets the offset value as positive or negative.
PSYS PMax Power	0	PSYS PMax power, defined in 1/8 Watt increments. Range 0-8192. For a PMax of 125W, enter 1000. 0 = AUTO. Uses BIOS VR mailbox command 0xB.
Min Voltage Override	Enabled Disabled	Min Voltage Override. Enable to override minimum voltage for runtime and for C8.
Acoustic Noise Settings	Submenu	
VccIn VR Settings	Submenu	
RFI Settings	Submenu	

CPU – Power Management Control → CPU VR Settings→ Acoustic Noise Settings

Aptio Setup – AMI

Advanced

Acoustic Noise Settings		
Acoustic Noise Mitigation	[Disabled]	
Pre Wake Time	0	
Ramp Up Time	0	
Ramp Down Time	0	
VccIn VR Domain		
Disable Fast PKG C State Ramp for VccIn Domain	[FALSE]	
Slow Slew Rate for VccIn Domain	[Fast/2]	
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
Acoustic Noise Mitigation	Enabled Disabled	Enabling this option will help mitigate acoustic noise on certain SKUs when the CPU is in deeper C state
Pre Wake Time	0	Set the maximum Pre Wake randomization time in micro ticks. Range is 0-255. This is for acoustic noise mitigation Dynamic Periodicity Alteration (DPA) tuning.
Ramp Up Time	0	Set the maximum Ramp Up randomization time in micro ticks. Range is 0-255. This is for acoustic noise mitigation Dynamic Periodicity Alteration (DPA) tuning.
Ramp Down Time	0	Set the maximum Ramp Down randomization time in micro ticks. Range is 0-255. This is for acoustic noise mitigation Dynamic Periodicity Alteration (DPA) tuning.
Disable Fast PKG C State Ramp for VccIn Domain	TRUE FALSE	This option needs to be configured to reduce acoustic noise during deeper C states. False: Don't disable Fast ramp during deeper C states; True: Disable Fast ramp during deeper C state
Slow Slew Rate for VccIn Domain	Fast/2 Fast/4 Fast/8	Set VR VccIn Slow Slew Rate for Deep Package C State ramp time; Slow slew rate equals to Fast divided by number, the

BIOS Item	Options	Description
	Fast/16	number is 2, 4, 8, 16 to slow down the slew rate to help minimize acoustic noise

CPU – Power Management Control → CPU VR Settings→ VccIn VR Settings

Aptio Setup – AMI

Advanced

VccIn VR Domain		
VR Config Enable	[Enabled]	
Current AC Loadline	170	
Current DC Loadline	150	
Current Psi1 Threshold	80	
Current Psi2 Threshold	20	
Current Psi3 Threshold	4	
Current Imon Slope	100	
Current Imon Offset	1	
Current VR Current Limit	420	
Current Tdc Current Limit	488	
AC Loadline	0	
DC Loadline	0	
PS Current Threshold1	80	
PS Current Threshold2	20	
PS Current Threshold3	4	
PS3 Enable	[Enabled]	
PS4 Enable	[Enabled]	
IMON Slope	0	
IMON Offset	0	
IMON Prefix	[+]	
VR Current Limit	0	
TDC Enable	[Enabled]	
TDC Current Limit	0	
TDC Time Window	[1 ms]	
TDC Lock	[Disabled]	
VccIn Demotion Override Enable	[Disabled]	

><: Select Screen
 ^v: Select Item
 Enter: Select
 +/-: Change Opt.
 F1: General Help
 F8: Previous Values
 F9: Optimized Default
 F10: Save & Exit
 ESC: Exit

BIOS Item	Options	Description
VR Config Enable	Enabled Disabled	VR Config Enable
Current AC Loadline	170	
Current DC Loadline	150	
Current Psi1 Threshold	80	
Current Psi2 Threshold	20	
Current Psi3 Threshold	4	
Current Imon Slope	100	
Current Imon Offset	1	
Current VR Current Limit	420	
Current Tdc Current Limit	488	

BIOS Item	Options	Description
AC Loadline	0	AC Loadline defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. Range is 0-6249 (0-62.49 mOhms). 0 = AUTO/HW default. Uses BIOS mailbox command 0x2.
DC Loadline	0	DC Loadline defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. Range is 0-6249 (0-62.49 mOhms). 0 = AUTO/HW default. Uses BIOS mailbox command 0x2.
PS Current Threshold1	80	PS Current Threshold1, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3.
PS Current Threshold2	20	PS Current Threshold2, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3.
PS Current Threshold3	4	PS Current Threshold3, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. Uses BIOS VR mailbox command 0x3.
PS3 Enable	Enabled Disabled	PS3 Enable/Disable. 0 - Disabled, 1 - Enabled. Uses BIOS VR mailbox command 0x3.
PS4 Enable	Enabled Disabled	PS4 Enable/Disable. 0 - Disabled, 1 - Enabled. Uses BIOS VR mailbox command 0x3
IMON Slope	0	IMON Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x4.
IMON Offset	0	IMON Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. IMON Uses BIOS VR mailbox command 0x4.
IMON Prefix	[+]	Sets the offset value as positive or negative.
VR Current Limit	0	Voltage Regulator Current Limit (Icc Max). This value represents the Maximum instantaneous current allowed at any given time. The value is represented in 1/4 A increments. A value of 400 = 100A. 0 means AUTO. Uses BIOS VR mailbox command 0x6.
TDC Enable	Enabled Disabled	TDC Enable. 0- Disable, 1 - Enable

BIOS Item	Options	Description
TDC Current Limit	0	TDC Current Limit, defined in 1/8A increments. Range 0-32767. For a TDC Current Limit of 125A, enter 1000. 0 = 0 Amps. Uses BIOS VR mailbox command 0x1A.
TDC Time Window	1 ms, 2 ms, 3 ms, 4 ms, 5 ms, 6 ms, 7 ms, 8 ms, 10 ms	TDC Time Window, value in milliseconds. 1ms is default. Range from 1ms to 10ms, except for 9ms. 9ms has no valid encoding in the MSR definition.
TDC Lock	Enabled Disabled	TDC Lock
VccIn Demotion Override Enable	Enabled Disabled	Enable VccIn Demotion Override Configuration.

CPU – Power Management Control → CPU VR Settings→ RFI Settings

Aptio Setup – AMI

Advanced

RFI Domain	
RFI Current Frequency	140.400MHz
RFI Frequency	0
Spread Spectrum	[Enabled]
RFI Spread Spectrum	[1.5%]
RFI Mitigation	[Disabled]
><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit	

BIOS Item	Options	Description
RFI Current Frequency	140.400MHz	
RFI Frequency	0	Set desired RFI frequency, in increments of 100KHz. (For a frequency of 100.6MHz, enter 1006.)
Spread Spectrum	Enabled Disabled	Enable or Disable the Spread Spectrum
RFI Spread Spectrum	0.5%, 1%, 1.5% , 2%, 3%, 4%, 5%, 6%	Set the Spread Spectrum
RFI Mitigation	Enabled Disabled	Disable - DCM is the IO_N default; Enable - Enable IO_N DCM/CCM switching as RFI mitigation.

CPU – Power Management Control → Custom P-state Table

Aptio Setup – AMI

Advanced

Custom P-state Table		
Number of P states	0	
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
Number of P states	0	Sets the number of custom P-states. At least 2 states must be present.

CPU – Power Management Control → Power Limit 3 Settings

Aptio Setup – AMI

Advanced

Power Limit 3 Override	[Disabled]	
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
Power Limit 3 Override	Enabled Disabled	Enable/Disable Power Limit 3 override. If this option is disabled, BIOS will leave the hardware default values for Power Limit 3 and Power Limit 3 Time Window.

CPU – Power Management Control → CPU Lock Configuration

Aptio Setup – AMI

Advanced

CFG Lock	[Enabled]	
Overclocking Lock	[Enabled]	
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
CFG Lock	Enabled Disabled	Configure MSR 0xE2[15], CFG Lock bit
Overclocking Lock	Enabled Disabled	Enable/Disable Overclocking Lock (BIT 20) in FLEX_RATIO(194) MSR

3.2.2 GT – Power Management Control

Aptio Setup – AMI

Advanced

GT – Power Management Control		
RC6(Render Standby)	[Enabled]	
Maximum GT frequency	[Default Max Frequency]	
Disable Turbo GT frequency	[Enabled]	
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
RC6(Render Standby)	Enabled Disabled	Check to enable render standby support.
Maximum GT frequency	Default Max Frequency , 100Mhz, 150Mhz, 200Mhz, 250Mhz, 300Mhz, 350Mhz, 400Mhz, 450Mhz, 500Mhz, 550Mhz, 600Mhz, 650Mhz, 700Mhz, 750Mhz, 800Mhz, 850Mhz, 900Mhz, 950Mhz, 1000Mhz, 1050Mhz, 1100Mhz, 1150Mhz, 1200Mhz	Maximum GT frequency limited by the user. Choose between 350MHz (RPN) and 1350MHz (RP0). Value beyond the range will be clipped to min/max supported by SKU
Disable Turbo GT frequency	Enabled Disabled	Enabled: Disables Turbo GT frequency. Disabled: GT frequency is not limited

3.3 Power Management

Aptio Setup – AMI

Advanced

Power Management	
> Voltage Monitor	
	><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
Voltage Monitor	Submenu	

3.3.1 Voltage Monitor

Aptio Setup – AMI

Advanced

Voltage Monitor			
RTC	XXX V		
5VSB	XXX V		
VIN	XXX V		
3.3V	XXX V		
VMEM	XXX V		
3.3VSB	XXX V		
VCORE	XXX V		
			><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
RTC	Info-only	
5VSB	Info-only	
VIN	Info-only	
3.3V	Info-only	
VMEM	Info-only	
3.3VSB	Info-only	
VCORE	Info-only	

3.4 System Management

Aptio Setup – AMI

Advanced

System Management			
SEMA Firmware Version	ADLINK	001	
> SEMA Flags SEMA Features: System Restart Event 4096 Bytes User-Flash Runtime Watchdog Temperatures Voltage Monitor Power-up Watchdog Boot Counter Dual-BIOS I2C Bus 2 AT/ATX Mode ACPI Thermal Trigger Ext - GPIO I2C Bus 3 Other BMC Error Log Parameter Memory Ext-GPIO Input Interrupt Support			><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
SEMA Firmware Version	Info-only	
SEMA Flags	Submenu	
SEMA Features	Info-only	If this item is shown below, it means SEMA supports it.

3.4.1 SEMA Flags

Aptio Setup – AMI

Advanced

SEMA Flags		
SEMA Flags	0x00	
BMC Select	Standard BIOS	
ATX/AT-Mode	AT Mode	
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
Flags	Info-only	
SEMA Flags	Read only	Show current SEMA settings.
BMC Select	Read only	Display current boot BIOS ROM chip.
ATX/AT-Mode	Read only	Display current power mode setting, AT or ATX mode.

3.5 Thermal Management

Aptio Setup – AMI

Advanced

Thermal Management > CPU Thermal Configuration > Platform Thermal Configuration > Temperatures	><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit
--	--

BIOS Item	Options	Description
CPU Thermal Configuration	Submenu	
Platform Thermal Configuration	Submenu	
Temperatures	Submenu	

3.5.1 CPU Thermal Configuration

Aptio Setup – AMI

Advanced

Cpu Thermal Configuration		
DTS SMM	[Enabled]	
Tcc Activation Offset	0	
Tcc Offset Time Window	[Disabled]	
Tcc Offset Clamp Enable	[Disabled]	
Tcc Offset Lock Enable	[Enabled]	
Bi-directional PROCHOT#	[Enabled]	
Disable PROCHOT# Output	[Enabled]	
Disable VR Thermal Alert	[Disabled]	
PROCHOT Response	[Disabled]	
PROCHOT Lock	[Disabled]	
ACPI T-States	[Disabled]	
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
DTS SMM	Enabled Disabled	Disabled: ACPI thermal management uses EC reported temperature values.
Tcc Activation Offset	0	Offset from factory set Tcc activation temprature at which the Thermal Control Circuit must be activated. Tcc will be activated at: Tcc Activation Temp - Tcc Activation Offset. Tcc Activation Offset range is 0 to 63.
Tcc Offset Time Window	Disabled , 5 ms, 10 ms, 55 ms, 156 ms, 375 ms, 500 ms, 750 ms, 1 sec, 2 sec, 3 sec, 4 sec, 5 sec, 6 sec, 7 sec, 8 sec, 10 sec, 12 sec, 14 sec, 16 sec, 20 sec, 24 sec, 28 sec, 32 sec, 40 sec, 48 sec, 56 sec, 64 sec, 80 sec, 96 sec, 112 sec, 128 sec, 160 sec, 192 sec, 224 sec, 256 sec, 320 sec, 384 sec, 448 sec	Tcc Offset Time Window for Running Average Temperature Limit(RATL) feature. The Tcc offset time window can range from 5ms to 448s.

Tcc Offset Clamp Enable	Enabled Disabled	Tcc Offset Clamp bit Enable for Running Average Temperature Limit(RATL) feature to allow CPU to throttle below P1.
Tcc Offset Lock Enable	Enabled Disabled	Lock Enable for Running Average Temperature Limit(RATL) feature to lock Temperature Target MSR.
Bi-directional PROCHOT#	Enabled Disabled	When a processor thermal sensor trips (either core), the PROCHOT# will be driven.
Disable PROCHOT# Output	Enabled Disabled	Enable/Disable PROCHOT# Output
Disable VR Thermal Alert	Enabled Disabled	Enable/Disable VR Thermal Alert
PROCHOT Response	Enabled Disabled	Enable/Disable PROCHOT Response
PROCHOT Lock	Enabled Disabled	Enable/Disable PROCHOT Lock
ACPI T-States	Enabled Disabled	Enable/Disable ACPI T-States.

3.5.2 Platform Thermal Configuration

Aptio Setup – AMI

Advanced

Platform Thermal Configuration		
Critical Trip Point	[Disabled]	
Passive Trip Point	[95 C]	
Passive TC1 Value	1	
Passive TC2 Value	5	
Passive TSP Value	10	
Passive Trip Points	[Enabled]	
Critical Trip Points	[Disabled]	
PCH Temp Read	[Enabled]	><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit
CPU Energy Read	[Enabled]	
CPU Temp Read	[Enabled]	
Alert Enable Lock	[Disabled]	
CPU Temp	72	
Boot DTS Read	[Disabled]	

BIOS Item	Options	Description
Critical Trip Point	Disabled , 80 C, 90 C, 95 C, 100 C	This value controls the temperature of the ACPI Critical Trip Point - the point in which the OS will shut the system off.

Passive Trip Point	Disabled, 15 C, 23 C, 31 C, 39 C, 47 C, 55 C, 63 C, 71 C, 79 C, 87 C, 95 C , 103 C, 111 C, 119 C (POR)	This value controls the temperature of the ACPI Passive Trip Point - the point in which the OS will begin throttling the processor.
Passive TC1 Value	1	This value sets the TC1 value for the ACPI Passive Cooling Formula. Range 1 - 16
Passive TC2 Value	5	This value sets the TC2 value for the ACPI Passive Cooling Formula. Range 1 - 16
Passive TSP Value	10	This item sets the TSP value for the ACPI Passive Cooling Formula. It represents in tenths of a second how often the OS will read the temperature when passive cooling is enabled. Range 2 - 32
Passive Trip Points	Enabled Disabled	Disable Passive Trip Points
Critical Trip Points	Enabled Disabled	Disable Critical Trip Points
PCH Temp Read	Enabled Disabled	PCH Temperature Read Enable
CPU Energy Read	Enabled Disabled	CPU Energy Read Enable
CPU Temp Read	Enabled Disabled	CPU Temperature Read Enable
Alert Enable Lock	Enabled Disabled	Lock all Alert Enable settings
CPU Temp	72	Fail Safe temp that EC will use if OS is hung
Boot DTS Read	Enabled Disabled	Read PCH, CPU DTS Temperature and publish via SMBIOS table

Aptio Setup – AMI

Advanced

Temperatures and Fan Speed		
CPU Temperature		
Current	xx C	
Startup	xx C	
Min	xx C	
Max	xx C	
At the Front Edge Temperatures		
Current	xx C	
Startup	xx C	
Min	xx C	
Max	xx C	
Close to 10G Temperatures		
Current	xx C	
Startup	xx C	
Under M.2 Temperatures		
Current	xx C	
Startup	xx C	
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
CPU Temperature Current/Startup/Min/Max	Info-only	
At the Front Edge Temperatures Current/Startup/Min/Max	Info-only	.
Close to 10G Temperatures Current/Startup	Info-only	
Under M.2 Temperatures Current/Startup	Info-only	

3.6 Watchdog Timer

Aptio Setup – AMI

Advanced

Watchdog Timer		
Power-Up Watchdog	[Disabled]	
ATTENTION: Pressing F12 during start up disables the Power Up Watchdog.		
RunTime Watchdog	[Disabled]	
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
Power-Up Watchdog	Enabled Disabled	The Power Up Watchdog resets the system after a certain amount of time after power up.
RunTime Watchdog	Enabled Disabled	The RunTime Watchdog resets the system after a certain amount of time after power up.

3.7 Super IO Configuration

Aptio Setup – AMI

Advanced

Super IO Configuration	
> NCT5104DSEC Super IO Configuration	
	><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
NCT5104DSEC Super IO Configuration	Submenu	

3.7.1 NCT5104DSEC Super IO Configuration

Aptio Setup – AMI

Advanced

NCT5104DSEC Super IO Configuration	
Super IO Chip	NCT5104DSEC
> Serial Port 1 Configuration > Serial Port 2 Configuration > Serial Port 3 Configuration	
	><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
Super IO Chip	Info-only	
Serial Port x Configuration	Submenu	

NCT5104DSEC Super IO Configuration → Serial Port x Configuration

Aptio Setup – AMI.

Advanced

Serial Port x Configuration		
Serial Port	[Enabled]	
Device Settings	IO=240; IRQ=4;	
Change Settings	[Auto]	
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
Serial Port	Disabled Enabled	Enable or disable serial port (COMx).
Device Setting	Info-only	
Change Settings	Auto IO=248h;IRQ=7; IO=240h;IRQ=3,4,5,6,7,10,11,12 IO=248h;IRQ=3,4,5,6,7,10,11,12 IO=250h;IRQ=3,4,5,6,7,10,11,12 IO=258h;IRQ=3,4,5,6,7,10,11,12	Select an optimal setting for Super IO device.

3.8 VPX Configuration

Aptio Setup – AMI

Advanced

VPX Configuration		
Watchdog ACPI Event Shutdown	[Disabled]	
COM1 port mode	[RS232]	
COM2 port mode	[RS232]	
CPU TDP Power Limit 1 Config	[25W]	
PCIe Scan Delay	0	
EC GPIO Options		
GPIO Pin Direction	[Input Mode]	
GPIO Interrupt Setting	[No interrupt]	
EC_GPIO	[Interrupt trigger]	
EC_GPI1	[Interrupt trigger]	
EC_GPI2	[Interrupt trigger]	><: Select Screen
EC_GPI3	[Interrupt trigger]	^v: Select Item
EC_GPI4	[Interrupt trigger]	Enter: Select
EC_GPI5	[Interrupt trigger]	+/-: Change Opt.
EC_GPI6	[Interrupt trigger]	F1: General Help
EC_GPI7	[Interrupt trigger]	F8: Previous Values
EC_GPO0	[Low]	F9: Optimized Default
EC_GPO1	[Low]	F10: Save & Exit
EC_GPO2	[Low]	ESC: Exit
EC_GPO3	[Low]	
EC_GPO4	[Low]	
EC_GPO5	[Low]	
EC_GPO6	[Low]	
EC_GPO7	[Low]	
COM2 port mode	[RS232]	
Maintenance port mode	[UART]	
DP++ manual mode	[Displayport]	
PCIe Scan Delay	0	

BIOS Item	Options	Description
Watchdog ACPI Event Shutdown	Disabled Enabled	Watchdog ACPI Event Shutdown Enabled/Disabled
COM1 port mode	RS232 RS422	COM1 port mode
COM2 port mode	RS232 RS422	COM2 port mode
CPU TDP Power Limit 1 Config	25W, 35W, 45W	To config CPU TDP
PCIe Scan Delay	0-60	System delay before PCIe scan. Unit is second and maximum value is 60 seconds
EC GPIO Options		

GPIO Pin Direction	Input Mode Output Mode	Indicates whether the GPIO Pin is interrupted. Write 0x00 to clear the interrupt and EC_GPIO_INT will be changed to high level
GPIO Interrupt Setting	No interrupt, Interrupt for both edge trigger, Low level trigger, High level trigger	When GPIO Pin is input mode, it supports edge trigger and level trigger
EC_GPIx	No Interrupt Interrupt trigger	Indicates whether the GPIO Pin is interrupted. Write 0x00 to clear the interrupt and EC_GPIO_INT will be changed to high level
EC_GPOx	Low High	Indicates whether the GPIO Pin is interrupted. Write 0x00 to clear the interrupt and EC_GPIO_INT will be changed to high level

3.9 USB Configuration

Aptio Setup – AMI

Advanced

USB Configuration		
USB Module Version	26	
USB Controllers: 1 XHCI		
USB Devices: 1 Drive, 1 Keyboard, 1 Mouse, 1 Hub		
Legacy USB Support	[Enabled]	
XHCI Hand-off	[Enabled]	
USB Mass Storage Driver Support	[Enabled]	
USB hardware delays and time-outs:		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit
USB transfer time-out	[20 sec]	
Device reset time-out	[20 sec]	
Device power-up delay	[Auto]	

BIOS Item	Options	Description
USB Module Version	Info-only	
USB Controllers	Info-only	
USB Devices	Info-only	
Legacy USB Support	Enabled Disabled	Enables Legacy USB support. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications.
XHCI Hand-off	Enabled Disabled	This is a workaround for Oses without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support	Enabled Disabled	Enable/Disable USB Mass Storage Driver Support.
USB transfer time-out	1 sec, 5 sec, 10 sec, 20 sec	The time-out value for Control, Bulk, and Interrupt transfers.
Device reset time-out	10 sec, 20 sec , 30 sec, 40 sec	USB mass storage device Start Unit command time-out.

BIOS Item	Options	Description
Device power-up delay	Auto , Manual	Maximum time the device will take before it properly reports itself to the Host Controller. 'Auto' uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub descriptor.

3.10 AMI Graphic Output Protocol Policy

Aptio Setup – AMI

Advanced

Intel(R) Graphics Controller Intel(R) GOP Driver [17.0.1075] Output Select [HDMI3[ACTIVE]]		
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
Intel(R) GOP Driver	Info-only	
Output Select	HDMI3[ACTIVE]	Output Interface

3.11 Serial Port Console Redirection

Aptio Setup – AMI

Advanced

COM0		
Console Redirection	[Disabled]	
> Console Redirection Settings		
COM1		
Console Redirection	[Disabled]	
> Console Redirection Settings		
COM2		
Console Redirection	[Disabled]	
> Console Redirection Settings		
Serial Port for Out-of-Band Management/ Windows Emergency Management Services (EMS)		
Console Redirection EMS	[Disabled]	
> Console Redirection Settings		
		><: Select Screen
		^v: Select Item
		Enter: Select
		+/-: Change Opt.
		F1: General Help
		F8: Previous Values
		F9: Optimized Default
		F10: Save & Exit
		ESC: Exit

BIOS Item	Options	Description
Console Redirection	Disabled Enabled	To enable or disable console redirection of COMx.
Console Redirection Settings	Submenu	The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings.

3.12 Network Stack Configuration

Aptio Setup – AMI

Advanced

Network Stack	[Disabled]	
IPv4 PXE Support	[Disabled]	
IPv4 HTTP Support	[Disabled]	
IPv6 PXE Support	[Disabled]	
IPv6 HTTP Support	[Disabled]	
PXE boot wait time	0	
Media detect count	1	
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
Network Stack	Disabled Enabled	Enable/Disable UEFI Network Stack
IPv4 PXE Support	Disabled Enabled	Enable/Disable IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available.
IPv4 HTTP Support	Disabled Enabled	Enable/Disable IPv4 HTTP boot support. If disabled, IPv4 HTTP boot support will not be available.
IPv6 PXE Support	Disabled Enabled	Enable/Disable IPv6 PXE boot support. If disabled, IPv6 PXE boot support will not be available.
IPv6 HTTP Support	Disabled Enabled	Enable/Disable IPv6 HTTP boot support. If disabled, IPv6 HTTP boot support will not be available.
PXE boot wait time	0	Wait time in seconds to press ESC key to abort the PXE boot. Use either +/- or numeric keys to set the value.
Media detect count	1	Number of times the presence of media will be checked. Use either +/- or numeric keys to set the value.

3.13 Trusted Computing

Aptio Setup – AMI

Advanced

TPM 2.0 Device Found		
Firmware Version:	7.85	
Vendor:	IFX	
Security Device Support	[Enabled]	
Active PCR banks	SHA256	
Available PCR banks	SHA256	
SHA256 PCR Bank	[Enabled]	
Pending operation	[None]	
Platform Hierarchy	[Enabled]	
Storage Hierarchy	[Enabled]	
Endorsement Hierarchy	[Enabled]	
Physical Presence Spec Version	[1.3]	
TPM 2.0 InterfaceType	[TIS]	
Device Select	[Auto]	
Disable Block Sid	[Disabled]	
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
Firmware Version	Info-only	
Vendor	Info-only	
Security Device Support	Disable Enable	Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.
Active PCR banks	Info-only	
Available PCR banks	Info-only	
SHA256 PCR Bank	Disable Enable	Enable or Disable SHA256 PCR Bank
Pending operation	None TPM Clear	Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change State of Security Device.
Platform Hierarchy	Disable Enable	Enable or Disable Platform Hierarchy
Storage Hierarchy	Disable Enable	Enable or Disable Storage Hierarchy
Endorsement Hierarchy	Disable Enable	Enable or Disable Endorsement Hierarchy
Physical Presence Spec	1.2	Select to Tell O.S. to support PPI Spec

BIOS Item	Options	Description
Version	1.3	Version 1.2 or 1.3. Note some HCK tests might not support 1.3.
TPM 2.0 InterfaceType	CRB TIS	Select the Communication Interface to TPM 2.0 Device.
Device Select	TPM 1.2 TPM 2.0 Auto	TPM 1.2 will restrict support to TPM 1.2 devices, TPM 2.0 will restrict support to TPM 2.0 devices, Auto will support both with the default set to TPM 2.0 devices if not found, TPM 1.2 devices will be enumerated
Disable Block Sid	Disable Enable	Override to allow SID authentication in TCG Storage device.

4 Chipset Menu

This menu contains the settings for most of the chipset I/O in the system.

Aptio Setup – AMI	
Main	Advanced
Chipset Server Mgmt Security Boot Save & Exit > System Agent (SA) Configuration > PCH-IO Configuration	><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
System Agent (SA) Configuration	Submenu	System Agent (SA) Parameters
PCH-IO Configuration	Submenu	PCH Parameters

4.1 System Agent (SA) Configuration

Aptio Setup – AMI		
Chipset		
System Agent (SA) Configuration		
VT-d	Supported	
> Memory Configuration > Graphics Configuration > PEG Port Feature Configuration > VMD setup menu		
Stop Grant Configuration	[Auto]	
VT-d	[Enabled]	
X2APIC Opt Out	[Disabled]	
DMA Control Guarantee	[Enabled]	
Above 4GB MMIO BIOS assignment	[Enabled]	
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
VT-d	Info-only	
> Memory Configuration	Submenu	
> PEG Port Feature Configuration	Submenu	
> VMD setup menu	Submenu	
> PCI Express Configuration	Submenu	
Stop Grant Configuration	Auto Manual	Automatic/Manual stop grant configuration
VT-d	Disabled Enabled	VT-d capability
X2APIC Opt Out	Disabled Enabled	Enable/Disable X2APIC_OPT_OUT bit
DMA Control Guarantee	Disabled Enabled	Enable/Disable DMA_CONTROL_GUARANTEE bit
Above 4GB MMIO BIOS assignment	Disabled Enabled	Enable/Disable above 4GB MemoryMappedIO BIOS assignment

4.1.1 Memory Configuration

Aptio Setup – AMI

Chipset

Memory Configuration		
Memory RC Version	2.0.2.9	
Memory Speed	3200 MT/s	
Memory Timings (tCL-tRCD-tRP-tRAS)	22-22-22-52	
Controller 0 Channel 0 Slot 0	Populated & Enabled	
Size	16384 MB (DDR4)	
Number of Ranks	1	
Manufacturer	Micron	
Controller 1 Channel 0 Slot 0	Populated & Enabled	
Size	16384 MB (DDR4)	><: Select Screen
Number of Ranks	1	^v: Select Item
Manufacturer	Micron	Enter: Select
Memory Test on Warm Boot	[Enabled]	+/-: Change Opt.
Maximum Memory Frequency	[Auto]	F1: General Help
ECC Support	[Enabled]	F8: Previous Values
Max TOLUD	[Dynamic]	F9: Optimized Default
In-Band ECC Support	[Disabled]	F10: Save & Exit
		ESC: Exit

BIOS Item	Options	Description
Memory RC Version	Info-only	
Memory Speed	Info-only	
Memory Timings (tCL-tRCD-tRP-tRAS)	Info-only	
Controller X Channel X Slot X	Info-only	
Size	Info-only	
Number of Ranks	Info-only	
Manufacturer	Info-only	
Memory Test on Warm Boot	Disabled Enabled	Enable Or Disable Base Memory Test Run on Warm Boot
Maximum Memory Frequency	Auto	Maximum Memory Frequency Selections in Mhz.
ECC Support	Disabled Enabled	Enable/disable DDR Ecc Support
Max TOLUD	Dynamic, 1 GB, 1.25 GB, 1.5 GB, 1.75 GB, 2 GB, 2.25 GB, 2.5 GB, 2.75 GB, 3 GB, 3.25 GB, 3.5 GB	Maximum Value of TOLUD. Dynamic assignment would adjust TOLUD automatically based on largest MMIO length of installed graphic controller
In-Band ECC Support	Disabled, Enabled	Enable/Disable In-Band ECC. Either the IBECC or the TME can be enabled.

4.1.2 PEG Port Feature Configuration

Aptio Setup – AMI	
Chipset	
PEG Port Feature Configuration	
Detect Non-Compliance Device	[Disabled]
><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit	

BIOS Item	Options	Description
Detect Non-Compliance Device	Disabled Enabled	Detect Non-Compliance PCI Express Device in PEG

4.1.3 VMD Setup Menu

Aptio Setup – AMI	
Chipset	
VMD Configuration	
Enable VMD controller	[Disabled]
Enabled VMD Global Mapping	[Enabled]
Map this Root Port under VMD	[Enabled]
Root Port BDF details	SATA Controller
RAID0	[Enabled]
RAID1	[Enabled]
RAID5	[Enabled]
Intel(R) Optane™ Memory	[Enabled]
><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit	

ESC: Exit

BIOS Item	Options	Description
Enable VMD controller	Disabled Enabled	Enable/Disable to VMD controller
Enabled VMD Global Mapping	Disabled Enabled	Enable/Disable to VMD Global Mapping
Map this Root Port under VMD	Disabled Enabled	Enable/Disable to Map this Root Port under VMD
Root Port BDF details	Info-only	
RAID0	Disabled Enabled	Enable/Disable to RAID0
RAID1	Disabled Enabled	Enable/Disable to RAID1
RAID5	Disabled Enabled	Enable/Disable to RAID5
Intel(R) Optane™ Memory	Disabled Enabled	Enable/Disable System Acceleration with Intel(R) Optane™ Memory feature.

4.1.4 PCI Express Configuration

Aptio Setup – AMI
Chipset

PCI Express Configuration PCI Express Clock Gating [Enabled] PCI Express Power Gating [Enabled] PCIe function swap [Enabled] > PCI Express Root Port 1 > PCI Express Root Port 2 > PCI Express Root Port 3 > PCI Express Root Port 4		
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
PCI Express Clock Gating	Disabled	PCI Express Clock Gating Enable/Disable

	Enabled	for each root port.
PCI Express Power Gating	Disabled Enabled	PCI Express Power Gating Enable/Disable for each root port.
PCIe function swap	Disabled Enabled	When Disabled, prevents PCIe rootport function swap. If any function other than 0th is enabled, 0th will become visible.
> PCI Express Root Port 1	Submenu	
> PCI Express Root Port 2	Submenu	
> PCI Express Root Port 3	Submenu	
> PCI Express Root Port 4	Submenu	

PCI Express Configuration → PCI Express Root Port X

Aptio Setup – AMI

Chipset

PCI Express Root Port 1	[Enabled]	
Connection Type	[Slot]	
ASPM	[Disabled]	
L1 Substates	[L1.1 & L1.2]	
Gen3 Eq Phase3 Method	[Hardware]	
Gen4 Eq Phase3 Method	[Hardware]	
ACS	[Enabled]	
PTM*	[Enabled]	
DPC	[Enabled]	
FOM Scoreboard Control Policy	[Auto]	
VC	[Enabled]	
Multi-VC	[Disabled]	
EDPC	[Enabled]	
URR	[Disabled]	
FER	[Disabled]	
NFER	[Disabled]	
CER	[Disabled]	
CTO	[Disabled]	
SEFE	[Disabled]	
SENF	[Disabled]	
SECE	[Disabled]	
PME SCI	[Disabled]	
Hot Plug	[Disabled]	
Advanced Error Reporting	[Enabled]	
PCIe Speed	[Auto]	
IOTG Mode	[Enabled]	
Transmitter Half Swing	[Disabled]	
Detect Timeout	0	
P2P Support	[Disabled]	
SA PCIe LTR Configuration		
LTR	[Enabled]	
Snoop Latency Override	[Auto]	
Non Snoop Latency Override	[Auto]	
Force LTR Override	[Disabled]	

><: Select Screen

LTR Lock	[Disabled]	^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit
CPU PCIe Gen3 HWEQ Config		
UPTP	7	
DPTP	7	
CPU PCIe Gen4 HWEQ Config		
UPTP	8	
DPTP	9	

BIOS Item	Options	Description
PCI Express Root Port 1	Disabled, Enabled	Control the PCI Express Root Port.
Connection Type	Built-in, Slot	Built-In: a built-in device is connected to this root port. Slot Implemented bit will be clear. Slot: this root port connects to user-accessible slot. Slot Implemented bit will be set.
ASPM	Disabled, L1	Set the ASPM Level:
L1 Substates	Disabled, L1.1, L1.1 & L1.2	PCI Express L1 Substates settings. L1SS cannot be enabled when CLKREQMSG is disabled
Gen3 Eq Phase3 Method	Hardware, Static Coeff.	PCIe Gen3 Equalization Phase 3 Method
Gen4 Eq Phase3 Method	Hardware, Static Coeff.	PCIe Gen3 Equalization Phase 3 Method
ACS	Disabled, Enabled	Enable/Disable Access Control Services Extended Capability
PTM*	Disabled, Enabled	Enable/Disable Precision Time Measurement
DPC	Disabled, Enabled	Enable/Disable Downstream Port Containment
FOM Scoreboard Control Policy	Auto, Gen3, Gen4, Gen3/Gen4	Select the FOM Scoreboard Control Policy, when set to Auto, speed is based on TLS
VC	Disabled, Enabled	Enable/Disable Virtual Channel
Multi-VC	Disabled, Enabled	Enable/Disable Multi Virtual Channel
EDPC	Disabled, Enabled	Enable/Disable Rootport extensions for Downstream Port Containment
URR	Disabled, Enabled	PCI Express Unsupported Request Reporting Enable/Disable.
FER	Disabled, Enabled	PCI Express Device Fatal Error Reporting Enable/Disable.
NFER	Disabled, Enabled	PCI Express Device Non-Fatal Error Reporting Enable/Disable.
CER	Disabled, Enabled	PCI Express Device Correctable Error Reporting Enable/Disable.
CTO	Disabled, Enabled	PCI Express Completion Timer TO Enable/Disable.
SEFE	Disabled, Enabled	Root PCI Express System Error on Fatal Error Enable/Disable.
SENF	Disabled, Enabled	Root PCI Express System Error on Non-Fatal Error Enable/Disable.
SECE	Disabled, Enabled	Root PCI Express System Error on Correctable

		Error Enable/Disable.
PME SCI	Disabled, Enabled	PCI Express PME SCI Enable/Disable.
Hot Plug	Disabled, Enabled	PCI Express Hot Plug Enable/Disable.
Advanced Error Reporting	Disabled, Enabled	Advanced Error Reporting Enable/Disable.
PCIe Speed	Auto, Gen1, Gen2, Gen3, Gen4	Configure PCIe Speed
IOTG Mode	Disabled, Enabled	IOTG Mode Enable/Disable
Transmitter Half Swing	Disabled, Enabled	Transmitter Half Swing Enable/Disable.
Detect Timeout	[Max-Value, Min-Value, Step-Value] = [0xFFFF, 0x0000, 0x0001]	The number of milliseconds reference code will wait for link to exit Detect state for enabled ports before assuming there is no device and potentially disabling the port.
P2P Support	Disabled, Enabled	Program P2P Support Registers according to setup option
LTR	Disabled, Enabled	SA PCIE Latency Reporting Enable/Disable
Snoop Latency Override	Disabled, Manual, Auto	Snoop Latency Override for SA PCIE.
Non Snoop Latency Override	Disabled, Manual, Auto	Non Snoop Latency Override for SA PCIE.
Force LTR Override	Disabled, Enabled	Force LTR Override for SA PCIE.
LTR Lock	Disabled, Enabled	PCIE LTR Configuration Lock
UPTP	[Max-Value, Min-Value, Step-Value] = [0x0A, 0x00, 0x01]	Upstream Port Transmitter Preset
DPTP	[Max-Value, Min-Value, Step-Value] = [0x0A, 0x00, 0x01]	Downstream Port Transmitter Preset

4.2 PCH-IO Configuration

Aptio Setup – AMI

Chipset

PCH-IO Configuration		
> SATA And RST Configuration > USB Configuration > Security Configuration > HD Audio Configuration > Seriallo Configuration > Pch Thermal Throttling Control > TSN GBE Configuration		
Port 80h Redirection	[LPC Bus]	><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit
Enhance Port 80h LPC Decoding	[Enabled]	
Enable TCO Timer	[Enabled]	
Enable Timed GPIO0	[Disabled]	
Enable Timed GPIO1	[Disabled]	
WOL From S5	[ON]	

BIOS Item	Options	Description
> SATA And RST Configuration	Submenu	
> USB Configuration	Submenu	
> Security Configuration	Submenu	
> HD Audio Configuration	Submenu	
> Seriallo Configuration	Submenu	
> Pch Thermal Throttling Control	Submenu	
> TSN GBE Configuration	Submenu	
Port 80h Redirection	LPC Bus PCIE Bus	Control where the Port 80h cycles are sent.
Enhance Port 80h LPC Decoding	Disabled Enabled	Support the word/dword decoding of port 80h behind LPC

Enable TCO Timer	Disabled Enabled	Enable/Disable TCO timer. When disabled, it disables PCH ACPI timer, stops TCO timer, and ACPI WDAT table will not be published.
Enable Timed GPIO0	Disabled Enabled	Enable/Disable Timed GPIO0. When disabled, it disables cross time stamp time-synchronization as extension of Hammock Harbor time synchronization.
Enable Timed GPIO1	Disabled Enabled	Enable/Disable Timed GPIO1. When disabled, it disables cross time stamp time-synchronization as extension of Hammock Harbor time synchronization.
WOL From S5	OFF ON	This Config to control power on/off LAN in S5 State by SEMA(EC).

4.2.1 SATA and RST Configuration

Aptio Setup – AMI Chipset

SATA And RST Configuration		
SATA Controller(s)	[Enabled]	
SATA Mode Selection	[AHCI]	
SATA Test Mode	[Disabled]	
> Software Feature Mask Configuration		
Aggressive LPM Support	[Enabled]	
SATA Controller Speed	[Gen3]	
Serial ATA Port X	XXXX	
Software Preserve	Unknown	
Port X	[Enabled]	
Hot Plug	[Disabled]	
Configured as eSATA	Hot Plug supported	><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit
External	[Disabled]	
Spin Up Device	[Disabled]	
SATA Device Type	[Hard Disk Drive]	
Topology	[Unknow]	
SATA Port 0 DevSlp	[Enabled]	
DITO Configuration	[Disabled]	
DITO Value	625	
DM Value	15	

BIOS Item	Options	Description
SATA Controller(s)	Disabled Enabled	Enable/Disable SATA Device.
SATA Mode Selection	AHCI Intel RST Premium With Intel Optane System Acceleration	Determines how SATA controller(s) operate.
SATA Test Mode	Disabled Enabled	Test Mode Enable/Disable (Loop Back).
> Software Feature Mask Configuration	Submenu	
Aggressive LPM Support	Disabled Enabled	Enable PCH to aggressively enter link power state.
SATA Controller Speed	Default, Gen1, Gen2, Gen3	Indicates the maximum speed the SATA controller can support.
Serial ATA Port X	Info-only	
Software Preserve	Info-only	
Port X	Disabled Enabled	Enable or Disable SATA Port
Hot Plug	Disabled Enabled	Designates this port as Hot Pluggable.
Configured as eSATA	Info-only	
External	Disabled Enabled	Marks this port as external.
Spin Up Device	Disabled Enabled	If enabled for any of ports Staggered Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	Hard Disk Drive Solid State Drive	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive
Topology	Unknown ISATA Direct Connect Flex M2	Identify the SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2
SATA Port X DevSlp	Disabled Enabled	Enable/Disable SATA Port X DevSlp. For DevSlp to work, both hard drive and SATA port need to support DevSlp function, otherwise an unexpected behavior might happen. Please check board design before enabling it.
DITO Configuration	Disabled Enabled	Enable/Disable DITO Configuration
DITO Value	625	DITO Value
DM Value	15	DM Value

4.2.2 Software Feature Mask Configuration

Aptio Setup – AMI	
Chipset	
Software Feature Mask Configuration	
HDD Unlock	[Enabled]
LED Locate	[Enabled]
><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit	

BIOS Item	Options	Description
HDD Unlock	Disabled Enabled	If enabled, indicates that the HDD password unlock in the OS is enabled.
LED Locate	Disabled Enabled	If enabled, indicates that the LED/SGPIO hardware is attached and ping to locate feature is enabled on the OS.

4.2.3 USB Configuration

Aptio Setup – AMI
Chipset

USB Configuration		
xDCI Support	[Disabled]	
USB2 PHY Sus Well Power Gating	[Enabled]	
USB3 Link Speed Selection	[GEN1]	
USB PDO Programming	[Enabled]	
XHCI LTR Mode	[Enabled]	
USB Overcurrent	[Enabled]	
USB Overcurrent Lock	[Enabled]	
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
xDCI Support	Disabled Enabled	Enable/Disable xDCI (USB OTG Device).
USB2 PHY Sus Well Power Gating	Disabled Enabled	Select 'Enabled' to enable SUS Well PG for USB2 PHY. This option has no effect on PCH-H
USB3 Link Speed Selection	GEN1 GEN2	This option is to select USB3 Link Speed GEN1 or GEN2
USB PDO Programming	Disabled Enabled	Select 'Enabled' if Port Disable Override functionality is used.
XHCI LTR Mode	Disabled Enabled	Enable/Disable XHCI LTR Mode
USB Overcurrent	Disabled Enabled	Select 'Disabled' for pin-based debug. If pin-based debug is enabled but USB overcurrent is not disabled, USB DbC does not work.
USB Overcurrent Lock	Disabled Enabled	Select 'Enabled' if Overcurrent functionality is used. Enabling this will make xHCI controller consume the Overcurrent mapping data

4.2.4 Security Configuration

Aptio Setup – AMI

Chipset

Security Configuration		
RTC Memory Lock	[Enabled]	
BIOS Lock	[Disabled]	
Force unlock on all GPIO pads	[Disabled]	
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
RTC Memory Lock	Disabled Enabled	Enable will lock bytes 38h-3Fh in the lower/upper 128-byte bank of RTC RAM
BIOS Lock	Disabled Enabled	Enable/Disable the PCH BIOS Lock Enable feature. Required to be enabled to ensure SMM protection of flash.
Force unlock on all GPIO pads	Disabled Enabled	If Enabled BIOS will force all GPIO pads to be in unlocked state

4.2.5 HD Audio Configuration

Aptio Setup – AMI
Chipset

HD Audio Subsystem Configuration Settings	
HD Audio	[Enabled] ><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
HD Audio	Disabled Enabled	Control Detection of the HD-Audio device.

4.2.6 Serial IO Configuration

Aptio Setup – AMI
Chipset

SerialIo Configuration UART0 Controller [Disabled]	><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit
--	--

BIOS Item	Options	Description
UART0 Controller	Disabled Enabled Communication port (COM)	Enables/Disables SerialIo Controller

4.2.7 PCH Thermal Throttling Control

Aptio Setup – AMI
Chipset

Thermal Throttling Level	[Suggested Setting]	
DMI Thermal Setting	[Suggested Setting]	
SATA Thermal Setting	[Suggested Setting]	
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
Thermal Throttling Level	Suggested Setting Manual	Determine if use Intel suggested setting
DMI Thermal Setting	Suggested Setting Manual	Determine if use Intel suggested setting
SATA Thermal Setting	Suggested Setting Manual	Determine if use Intel suggested setting

5 Server Mgmt Menu

This menu contains the settings for IPMI BMC in the system.

Aptio Setup – AMI						
Main	Advanced	Chipset	Server Mgmt	Security	Boot	Save & Exit
BMC Self Test Status			PASSED			
BMC Device ID			18			
BMC Device Revision			80			
BMC Firmware Revision			0.04			
IPMI Version			2.0			
IPMI BMC Interface			KCS			
BMC Support			[Enabled]			
>System Event Log					><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit	
>View RFU information						
>BMC network configuration						
>ADLINK IPMI configuration						
>View System Event Log						
>BMC User Setting						

BIOS Item	Options	Description
BMC Self Test Status	Info-only	
BMC Device ID	Info-only	
BMC Device Revision	Info-only	
BMC Firmware Revision	Info-only	
IPMI Version	Info-only	
IPMI BMC Interface	Info-only	
BMC Support	Disabled Enabled	Enable/Disable interfaces to communicate with BMC
>System Event Log	Submenu	
>View RFU information	Submenu	
>BMC network configuration	Submenu	
>ADLINK IPMI configuration	Submenu	
>View System Event Log	Submenu	Enter to check SEL.
>BMC User Setting	Submenu	Enter to modify BMC user setting.

5.1 System Event Log

Aptio Setup – AMI
Server Mgmt

Enabling/Disabling Options SEL Components	[Enabled]	
Erasing Settings Erase SEL	[No]	
When SEL is Full	[Do Nothing]	
Custom EFI Logging Options Log EFI Status Codes	[Error code]	
NOTE: All values changed here do not take effect until computer is restarted.		
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
SEL Components	Disabled Enabled	Change this to enable or disable event logging for error/progress codes during boot.
Erase SEL	No Yes, On next reset Yes, On every reset	Choose options for erasing SEL.
When SEL is Full	Do Nothing Erase Immediately	Choose options for reactions to a full SEL.
Log EFI Status Codes	Disabled Both Error code Progress code	Disable the logging of EFI Status Codes or log only error code or only progress code or both.

5.2 View FRU Information

Aptio Setup – AMI
Server Mgmt

FRU information		
Board Manufacturer	ADLINK	
Board Product	VPX6200	
Board Serial Number	PPS0000001	
Board Part Number	55-31129	
Product Manufacturer	ADLINK	
Product Name	VPX6200	
Product Part Number	91-31129	
Product Version	Rev A2	
Product Serial Number	0000001	
NOTE: No FRU information for fields indicate information needs to be filled by O.E.M		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
Board Manufacturer	Info-only	
Board Product	Info-only	
Board Serial Number	Info-only	
Board Part Number	Info-only	
Product Manufacturer	Info-only	
Product Name	Info-only	
Product Part Number	Info-only	
Product Version	Info-only	
Product Serial Number	Info-only	

5.3 BMC Network Configuration

Aptio Setup – AMI
Server Mgmt

--BMC network configuration-- ***** Configure IPv4 support ***** LAN channel 1 Configuration Address source [Unspecified] Current Configuration Address StaticAddress source Station IP address xxx.xxx.xxx.xxx Subnet mask xxx.xxx.xxx.xxx Station MAC address xx-xx-xx-xx-xx-xx Router IP address xxx.xxx.xxx.xxx		
LAN channel 2 Configuration Address source [Unspecified] Current Configuration Address StaticAddress source Station IP address xxx.xxx.xxx.xxx Subnet mask xxx.xxx.xxx.xxx Station MAC address xx-xx-xx-xx-xx-xx Router IP address xxx.xxx.xxx.xxx		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
Configuration Address source	Unspecified Static	Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase
Current Configuration Address source	Info-only	
Station IP address	Info-only	
Subnet mask	Info-only	
Station MAC address	Info-only	
Router IP address	Info-only	

5.4 ADLINK IPMI Configuration

Aptio Setup – AMI Server Mgmt

PCB Version	A1	><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit
Geographical Address	0x1E	
System Controller	Host	
NVMRO Signal	Non Protect	
NVMRO item Control	[Non-Protect]	
SYS_RESET Support	[Enabled]	
GA Status	It's GA 17	
SBC Control Status	3x SBC (GA17/18/19)	
SBC Control	[3x SBC (GA17/18/19)]	

BIOS Item	Options	Description
PCB Version	Info-only	
Geographical Address	Info-only	
System Controller	Info-only	
NVMRO Signal	Info-only	
NVMRO item Control	Protect Non-Protect	Enable or disable NVMRO Control support.
SYS_RESET Support	Disabled Enabled	Enable or disable SYS_RESET support.
SBC Control Status	Info-only	Show the SBC control Status from IPMC
SBC Control	1x SBC (GA17) 2x SBC (GA17/18) 3x SBC (GA17/18/19)	Send SBC control Status to IPMC

5.5 View System Event Log

Aptio Setup – AMI
Server Mgmt

No. of log entries in SEL : xxx			
DATE	TIME	SENSOR TYPE	
			><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
System Event Log	Info-only	To display System Event Logs (SEL).

5.6 BMC User Settings

Aptio Setup – AMI
Server Mgmt

BMC User Settings			
> Add User			
> Delete User			
> Change User Settings			
			><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
BMC User Settings	Info-only	To config BMC user settings.

6 Security Menu

This menu contains the settings for security in the system.

Aptio Setup – AMI	
Main	Advanced
Chipset	Boot
Security	Save & Exit
Password Description 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 to boot or enter Setup. In Setup the user will have Administrator rights. The password length must be in the following range: Minimum length 3 Maximum length 20 Administrator Password User Password HDD Security Configuration > Secure Boot menu	
><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit	

BIOS Item	Options	Description
Administrator Password	Enter to set password	Configure/Clear Administrator Password. When pressing enter, a menu will be popped up for creating new password. When password installed, press enter without inputting password, it will clear password.
User Password	Enter to set password	Configure/Clear User Password. When pressing enter, a menu will be popped up for creating new password. When password installed, press enter without inputting password, it will clear password.
HDD Security Configuration	Submenu	For HDD security, it will list all HDD detected on motherboard. Select the HDD and then press enter can figure/clear HDD password.

BIOS Item	Options	Description
Secure Boot menu	Submenu	

When selecting a HDD to configure passwords, BIOS will enter another new BIOS setup page like below. The method of configuring HDD password is the same as BIOS passwords. Once password is set, it will reflect the status on the screen, like 'INSTALLED' change on 'HDD User Pwd Status'. When there is no HDD user password installed, you can always change master password without confirming the latest installed password. Once HDD user password is installed, HDD master password is not allowed changing.

Aptio Setup – AMI

Security

HDD Password Description		
Allows Access to Set, Modify and Clear HardDisk User and Master Passwords. User Password need to be installed for Enabling Security. Master Password can be Modified only when successfully unlocked with Master Password in POST		
HDD PASSWORD CONFIGURATION		
Security Supported	Yes	
Security Enabled	Yes	
Security Locked	No	
Security Frozen	No	
HDD User Pwd Status	INSTALLED	
HDD Master Pwd Status	INSTALLED	
Set User Password		
Set Master Password		
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

6.1 Secure Boot

Aptio Setup – AMI

Security

System Mode	User	
Secure Boot	[Disabled] Not Active	
Secure Boot Mode	[Standard]	
> Restore Factory Keys		
> Reset To Setup Mode		
> Key Management		
		><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
System Mode	Info-only	
Secure Boot	Disabled Enabled	Secure Boot feature is Active if Secure Boot is Enabled,
Secure Boot Mode	Standard Custom	Secure Boot mode options

7 Boot Menu

This menu contains the settings for bootable devices in the system.

Aptio Setup – AMI.		
Main	Advanced	Chipset Server Mgmt Security Boot Save & Exit
Boot Configuration		
Setup Prompt Timeout	1	
Bootup NumLock State	[On]	
Quiet Boot	[Enabled]	
Fast Boot	[Disabled]	
Boot mode select	[UEFI]	
Boot Configuration		
Boot Option #1	[Hard Disk]	
Boot Option #2	[NVMe]	
Boot Option #3	[Built-in EFI Shell]	
Boot Option #4	[CD/DVD]	
Boot Option #5	[SD]	><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit
Boot Option #6	[USB Hard Disk]	
Boot Option #7	[USB CD/DVD]	
Boot Option #8	[USB Key]	
Boot Option #9	[USB Floppy]	
Boot Option #10	[USB Lan]	
Boot Option #11	[Network]	

BIOS Item	Options	Description
Setup Prompt Timeout	1	Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting.
Bootup NumLock State	On Off	Select the keyboard NumLock state after system boot.
Quiet Boot	Disabled Enabled	Enabled: will show splash screen during POST. Disabled: will show boot message during POST.
Fast Boot	Disabled Enabled	Enable or disabled Fast boot feature. Most probes are skipped to reduce time cost during boot.
Boot mode select	LEGADY UEFI	Select boot mode, LEGACY/UEFI.

Boot Option #1~#11	Hard Disk NVME CD/DVD SD USB Hard Disk USB CD/DVD USB Key USB Floppy USB Lan Network Disabled	Set system boot order.
--------------------	---	------------------------

8 Save & Exit

Aprio Setup – AMI	
Main	Advanced
Save Options Save Changes and Exit Discard Changes and Exit Save Changes and Reset Discard Changes and Reset Save Changes Discard Changes Default Options Restore Defaults Save as User Defaults Restore User Defaults Boot Override Launch EFI Shell from filesystem device	Exit system setup after saving the changes. ><: Select Screen ^v: Select Item Enter: Select +/-: Change Opt. F1: General Help F8: Previous Values F9: Optimized Default F10: Save & Exit ESC: Exit

BIOS Item	Options	Description
Save Changes and Exit	Enter	Save changed settings and exit BIOS setup utility.
Discard Changes and Exit	Enter	Skip changed setting and exit BIOS setup utility.
Save Changes and Reset	Enter	Save all changed settings and let system do reset to boot system.
Discard Changes and Reset	Enter	Discard all changed settings and let system do reset to boot system.
Save Changes	Enter	Save all changed settings.
Discard Changes	Enter	Discard changes done so far to any of the setup options.
Restore Default	Enter	Load the default made when BIOS was built.
Save as User Default	Enter	Save all changed done so far as User Defaults.
Restore User Default	Enter	Load the default that user save as user defaults.
Boot Override	Info-only	

Important Safety Instructions

For user safety, please read and follow all **instructions**, **WARNINGS**, **CAUTIONS**, and **NOTES** marked in this manual and on the associated equipment before handling/operating the equipment.

1. Read these safety instructions carefully.
2. Keep this user's manual for future reference.
3. Read the specifications section of this manual for detailed information on the operating environment of this equipment.
4. The equipment can be operated at an ambient temperature of 40°C.
5. When installing/mounting or uninstalling/removing equipment; or when removal of the chassis lid required for user servicing (Section 3.1-3.5):
 - Turn off power and unplug any power cords/cables, and
6. To avoid electrical shock and/or damage to equipment:
 - Keep equipment away from water or liquid sources;
 - Keep equipment away from high heat or high humidity;
 - Keep equipment properly ventilated (do not block or cover ventilation openings);
 - Make sure to use recommended voltage and power source settings;
 - Always install and operate equipment near an easily accessible electrical socket-outlet;
 - Secure the power cord (do not place any object on/over the power cord);
 - Only install/attach and operate equipment on stable surfaces and/or recommended mountings;
 - If the equipment will not be used for long periods of time, turn off and unplug the equipment from its power source.
 - The power cord must be connected to a socket or outlet with a ground connection.
7. Never attempt to fix the equipment. Equipment should only be serviced by qualified personnel.

8. This equipment is not suitable for use in locations where children are likely to be present.
9. Equipment must be serviced by authorized technicians when:
 - The power cord or plug is damaged;
 - Liquid has penetrated the equipment;
 - It has been exposed to high humidity/moisture;
 - It is not functioning or does not function according to the user's manual;
 - It has been dropped and/or damaged; and/or,
 - It has an obvious sign of breakage.
10. Please pay strict attention to all warnings and advisories appearing on the device, to avoid injury or damage.
11. It is recommended that equipment be installed only in a server room or computer room where access is:
 - Restricted to qualified service personnel or users familiar with restrictions applied to the location, reasons therefor, and any precautions required;
 - Only afforded by the use of a tool or lock and key, or other means of security, and is controlled by the authority responsible for the location.
12. Suitable for installation in Information Technology Rooms in accordance with Article 645 of the National Electrical Code and NFPA 75.

Getting Service

Ask an Expert: <https://www.adlinktech.com/en/Askanexpert>

ADLINK Technology, Inc.

Address: No. 66, Huaya 1st Rd., Guishan District
Taoyuan City 333411, Taiwan
333411 桃園市龜山區華亞一路 66 號
Tel: +886-3-216-5088
Fax: +886-3-328-5706
Email: service@adlinktech.com

Ampro ADLINK Technology, Inc.

6450 Via Del Oro, San Jose, CA 95119-1208, USA
Tel: +1-408-360-0200
Toll Free: +1-800-966-5200 (USA only)
Fax: +1-408-600-1189
Email: info@adlinktech.com

ADLINK Technology (China) Co., Ltd.

Address: 上海市浦东新区张江高科技园区芳春路 300 号 (201203)
300 Fang Chun Rd., Zhangjiang Hi-Tech Park, Pudong New Area
Shanghai, 201203 China
Tel: +86-21-5132-8988
Fax: +86-21-5132-3588
Email: market@adlinktech.com

ADLINK Technology GmbH

Address: Hans-Thoma-Strasse 11, D-68163, Mannheim, Germany
Tel: +49-621-43214-0
Fax: +49-621 43214-30
Email: emea@adlinktech.com

Please visit the Contact page at www.adlinktech.com for information on how to contact the ADLINK regional office nearest you.