AV710

Intel®Core™ i7-6822EQ Processor

User's Manual

Revision Date: July. 16. 2020

Safety Information

Electrical safety

- To prevent electrical shock hazard, disconnect the power cable from the electrical outlet before relocating the system.
- When adding or removing devices to or from the system, ensure that the power cables for the devices are unplugged before the signal cables are connected. If possible, disconnect all power cables from the existing system before you add a device.
- Before connecting or removing signal cables from the motherboard, ensure that all power cables are unplugged.
- Seek professional assistance before using an adapter or extension cord. These devices could interrupt the grounding circuit.
- Make sure that your power supply is set to the correct voltage in your area.
- If you are not sure about the voltage of the electrical outlet you are using, contact your local power company.
- If the power supply is broken, do not try to fix it by yourself. Contact a qualified service technician or your local distributor.

Operation safety

- Before installing the motherboard and adding devices on it, carefully read all the manuals that came with the package.
- Before using the product, make sure all cables are correctly connected and the power cables are not damaged. If you detect any damage, contact your dealer immediately.
- To avoid short circuits, keep paper clips, screws, and staples away from connectors, slots, sockets and circuitry.
- Avoid dust, humidity, and temperature extremes. Do not place the product in any area where it may become wet.
- Place the product on a stable surface.
- If you encounter any technical problems with the product, contact your local distributor

Statement

Revision History

Revision	Date (yyyy/mm/dd)	Changes
Version 1.0	2019/05/23	Initial release

Packing list

- ☐ **AV710 Rugged Fanless System**
- ☐ **CD (Driver + Quick Installation Guide)**

Ordering information

Model Number	Description
AV710	IP65 MIL-STD-810G Rugged Computer with Intel® Core i7-6822EQ, 9V to 36V DC-in, Extended Temp -40 to 70°C

If any of the above items is damaged or missing, please contact your local distributor.

RoHS Compliance

Perfectron RoHS Environmental Policy and Status Update

Perfectron is a global citizen for building the digital infrastructure. We are committed to providing green products and services, which are compliant with

European Union RoHS (Restriction on Use of Hazardous Substance in Electronic Equipment) directive 2011/65/EU, to be your trusted green partner and to protect our environment.

In order to meet the RoHS compliant directives, Perfectron has established an engineering and manufacturing task force to implement the introduction of green products. The task force will ensure that we follow the standard Perfectron development procedure and that all the new RoHS components and new manufacturing processes maintain the highest industry quality levels for which Perfectron are renowned.

The model selection criteria will be based on market demand. Vendors and suppliers will ensure that all designed components will be RoHS compliant

Table Contents

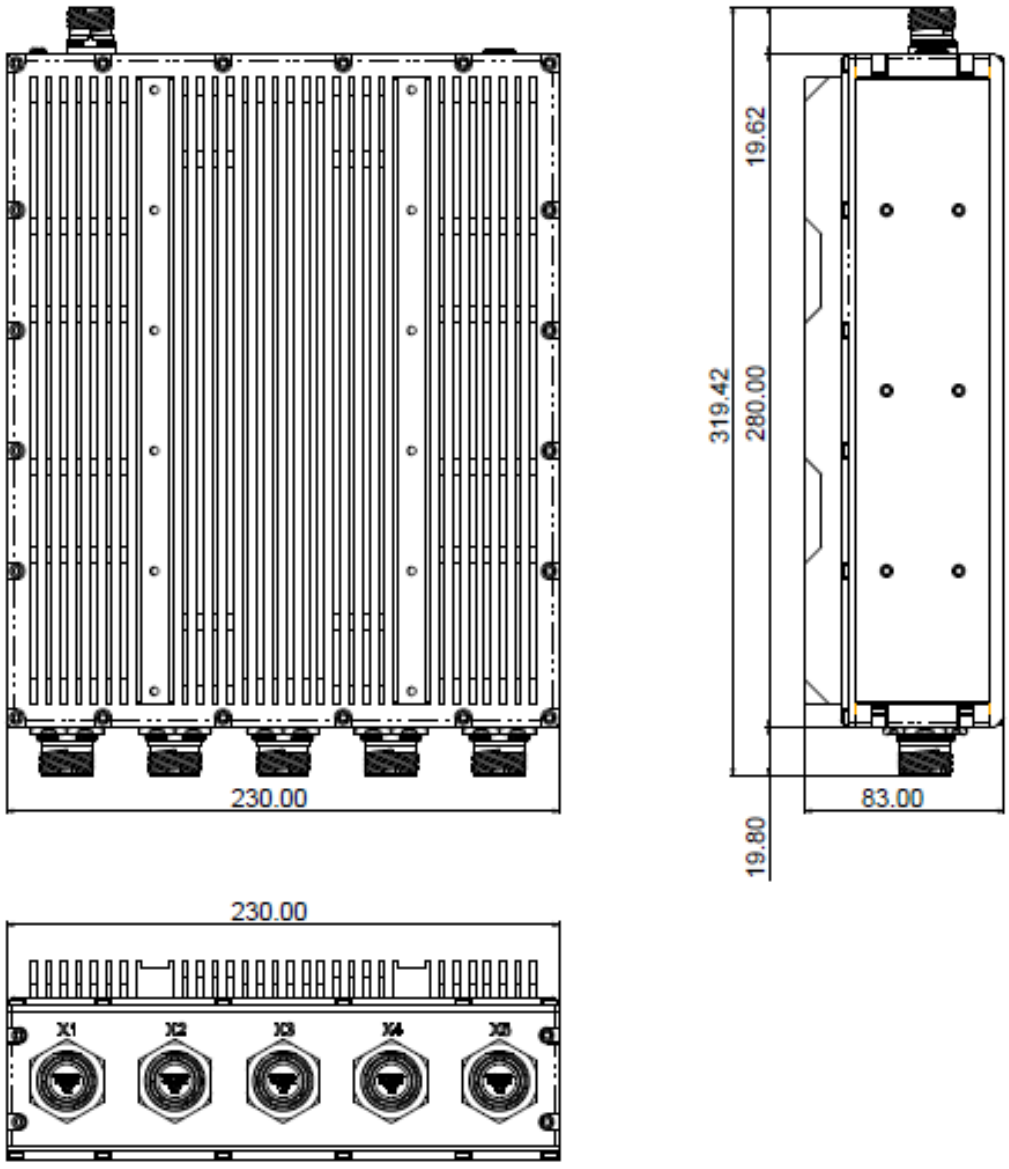
Chapter 1: Product Introduction

1.1 Key Features

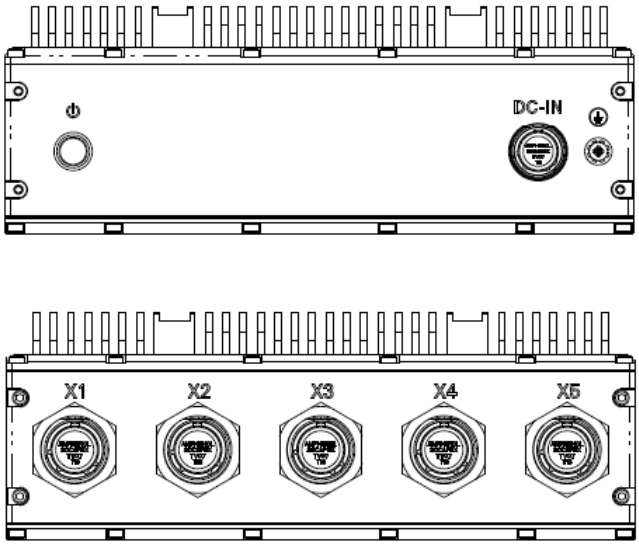
System	
CPU	Intel® Core™ i7-6822EQ Processor (8M Cache, up to 2.80 GHz)
Memory Type	2 x DDR4 SO-DIMM up to 32GB
BIOS	AMI® BIOS
Storage Device	1 x 2.5" SATA SSD
Front I/O	
DC-In	1 (Amphenol TV07RW-11-54P)
Power Button	1 x Power Button with LED backlight
Ground Screw	1 (M4)
Rear I/O	
X1	1 x LAN (Amphenol TV07RW-13-98S)
X2	1 x LAN (Amphenol TV07RW-13-98S)
X3	2 x USB (Amphenol TV07RW-13-98S)
X4	2 x COM (Amphenol TV07RW-13-35S)
X5	1 x VGA (Amphenol TV07RW-13-98S)
Mechanical & Environment	
Construction	Aluminum chassis with fanless design
Power Requirements	9V to 36V DC-in
Dimension (W x H x D)	230 x 83 x 280mm (9.06" x 3.27" x 11.02")
Operating Temp.	-40 to 70°C (ambient with 0.7m/s airflow)
Storage Temp.	-40 to 85°C
Relative Humidity	5% to 95%, non-condensing

* Specifications are subject to change without notice*

1.2 Dimensions



1.3 Panel Component

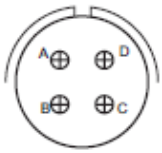


DC-IN	DC-IN 9-36V
X1	1 x Gigabit Ethernet Port
X2	1 x Gigabit Ethernet Port
X3	2 x USB2.0 Ports
X4	2 x RS232 Ports
X5	1 x VGA Port

Chapter 2: Connector pin definition

2.1 DC-IN

Pin	Definition
A	V+
B	V+
C	V-
F	V-



2.2 LAN (X1, X2)

Pin	Signal
A	D0+
B	D0-
C	D1+
D	D1-
E	D2+
F	D2-
G	D3+
H	D3-
J	NC
K	NC

2.3 USB (X3)

Pin	Signal
A	VCC
B	Data -
C	Data +
D	GND
E	VCC
F	Data -
G	Data +
H	GND
J	NC
K	NC

2.4 COM (X4)

Pin	Signal	Pin	Signal
1	DCD	11	DCD
2	RXD	12	RXD
3	TXD	13	TXD
4	DTR	14	DTR
5	GND	15	GND
6	DSR	16	DSR
7	RTS	17	RTS
8	CTS	18	CTS
9	RI	19	RI
10	GND	20	GND
21	GND		
22	GND		

2.5 VGA (X5)

Pin	Signal
A	RED
B	GREEN
C	BLUE
D	Ground
E	V-Sync
F	H-Sync
G	SCL
H	SDA
J	+5Vcc
K	Ground

Chapter 3: AMI BIOS UTILITY

This chapter provides users with detailed descriptions on how to set up a basic system configuration through the AMI BIOS setup utility.

3.1 Menu Structure

This section presents the six primary menus of the BIOS Setup Utility. Use the following table as a quick reference for the contents of the BIOS Setup Utility. The subsections in this section describe the submenus and setting options for each menu item. The default setting options are presented in bold, and the function of each setting is described in the right hand column of the respective table.

Main	Advanced	Security	Boot	Save & Exit
- BIOS Information	- CPU ▶	- Password Description ▶	- Boot Configuration ▶	- Reset Options ▶
- Processor Information	- Memory ▶	- Secure Boot Menu ▶	- CSM Configuration ▶	- Save Options ▶
- PCH Information	- Graphics ▶			
- System Management ▶	- SATA ▶			
- System Date	- USB ▶			
- System Time	- Network ▶			
	- PCI and PCIe ▶			
	- Super IO ▶			
	- ACPI and Power Management ▶			
	- Sound ▶			
	- Serial Port Console ▶			
	- ICC ▶			
	- Thermal ▶			
	- Miscellaneous ▶			
	- AMI Graphic Output Protocol Policy ▶			

3.2 Main

The Main Menu provides read-only information about your system and also allows you to set the System Date and Time. Refer to the tables below the screen shot of this menu for details of the submenus and settings.

3.2.1 BIOS Information

Feature	Options	Description
BIOS Vendor	Info only	BIOS Vendor
Core Version	Info only	.Kernal code version
Compliancy	Info only	UEFI code support
Project version	Info only	ADLINK BIOS version
Build Date and Time	Info only	ADLINK date the BIOS was build
Access Level	Info only	Access Level

3.2.2 Processor Information

Feature	Options	Description
CPU Brand String	Info only	Display CPU Brand Name.
Frequency	Info only	Display CPU Frequency.
Processor ID	Info only	Display CPU ID.
Stepping	Info only	Display CPU Stepping.
Number of Processors	Info only	Display number of Processors.
GT Info	Info only	Display GT info of Intel Graphics.
IGFX VBIOS Version	Info only	Display VBIOS Version.
Total Memory	Info only	Display installed memory size.

3.2.3 PCH Information

Feature	Options	Description
PCH Name	Info only	Display PCH name.
PCH SKU	Info only	Display PCH SKU.
Stepping	Info only	Display PCH stepping.
ME FW Version	Info only	Display version of ME.
ME Firmware SKU	Info only	Display ME Firmware Kit SKU number.
System Management	Submenu	

3.2.3.1 PCH Information System Management

Feature	Options	Description
System Management	Info only	
Version	Info only	Display version.

3.2.4 System Management

3.2.4.1 System Management > Board Information

Board Information	Info only	Description
SMC Firmware	Read only	Display SMC Firmware.
Build Date	Read only	Display SMC firmware build date.
SMC Boot loader	Read only	Display SMC boot loader.
Build Date	Read only	Display SMC boot loader build date.
Hardware Version	Read only	Display SMC hardware Version.
Serial Number	Read only	Display SMC serial Number.
Manufacturing Date	Read only	Display SMC manufacturing date.
Last Repair Date	Read only	Display SMC last repair date.
MAC ID	Read only	Display SMC MAC ID

3.2.4.2 System Management > Temperatures and Fan Speed

Feature	Options	Description
Temperatures and Fan	Info only	
CPU Temperature	Info only	
Current	Read only	Display CPU current temperature.
Startup	Read only	Display CPU startup temperature.
Min	Read only	Display CPU min temperature.
Max	Read only	Display CPU max temperature.
Board Temperatures	Info only	
Current	Read only	Display board current temperature.
Startup	Read only	Display board startup temperature.
Min	Read only	Display board min temperature.
Max	Read only	Display board max temperature.
CPU Fan Speed	Read only	Display CPU fan speed.
System Fan Speed	Read only	Display system fan speed.

3.2.4.3 System Management > Power Consumption

Feature	Options	Description
Power Consumption	Info only	
Current Input Current	Read only	Display input current.
Current Input Power	Read only	Display input power.
VCC_CORE	Read only	Display actual voltage of the VCC_CORE
VGFX	Read only	Display actual voltage of the VGFX
VMEM	Read only	Display actual voltage of the VMEM
5VSB	Read only	Display actual voltage of the 5VSB
VIN	Read only	Display actual voltage of the VIN
5V	Read only	Display actual voltage of the 5V
3,3V	Read only	Display actual voltage of the 3.3V
3.3VSB	Read only	Display actual voltage of the 3.3VSB

3.2.4.4 System Management > Runtime Statistics

Feature	Options	Description
Runtime Statistics	Info only	
Total Runtime	Read only	The returned value specifies the total time in minutes the system is running in S0 state.
Current Runtime	Read 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.
Power Cycles	Read only	The returned value specifies the number of times the external power supply has been shut down
Boot Cycles	Read only	The Bootcounter is increased after a HW- or SW-Reset or after a successful power-up.
Boot Reason	Read only	The boot reason is the event which causes the reboot of the system.

3.2.4.5 System Management > Flags

Feature	Options	Description
Flags	Info only	
BMC Flags	Read only	
BIOS Select	Read only	Display the selection of current BIOS ROM.
ATX/AT-Mode	Read only	Display ATX/AT-Mode.
Exception Code	Read only	System exception reason.

3.2.4.6 System Management > Power Up

Feature	Options	Description
Power Up	Info only	
Power Up watchdog Attention: F12 disables the Power Up Watchdog.	Enabled **Disabled**	The Power-Up Watchdog resets the system after a certain amount of time after power-up.
ECO Mode	**Disabled** Enable	Reduces the power consumption of the system.
Power-up Mode Attention: The Power-Up Mode only has effect, if the module is in ATX-Mode.	**Turn on** Remain off Last State	Turn On: The machine starts automatically when the power supply is turned on. Remain Off: To start the machine the power button has to be pressed. Last State: when powered on during a power failure the system will automatically power on when power is restored

3.2.4.7 System Management > LVDS Backlight

Feature	Options	Description
LVDS Backlight	Info only	
LVDS Backlight Bright	255	The value range starts by 0 and ends by 255.

3.2.4.8 System Management > Smart Fan

Feature	Options	Description
Smart Fan	Info only	
CPU Smart FanTemperature Source	**CPU Sensor** Board Sensor	Select CPU smart fan source.
CPU Fan Mode	AUTO (Smart Fan) Fan Off **Fan On**	Select CPU Fan Mode.
PWM Level	100	**Note:** This option is hidden unless the user selects CPU FAN Mode as "Fan On"
CPU Trigger Point 1	Read only	
Trigger Temperature	15	Specifies the temperature threshold at which the BMC turns on CPU fan with specific PWM level.
PWM Level	30	Select PWM level.
CPU Trigger Point 2	Read only	
Trigger Temperature	60	Specifies the temperature threshold at which the BMC turns on CPU fan with specific PWM level.
PWM Level	40	Select PWM level.
CPU Trigger Point 3	Read only	
Trigger Temperature	70	Specifies the temperature threshold at which the BMC turns on CPU fan with specific PWM level.
PWM Level	63	Select PWM level.
CPU Trigger Point 4	Read only	
Trigger Temperature	80	Specifies the temperature threshold at which the BMC turns on CPU fan with specific PWM level.
PWM Level	100	Select PWM level.

3.2.5 System Date and Time

Feature	Options	Description
System Date	Weekday, MM/DD/YYYY	Requires the alpha-numeric entry of the day of the week, day of the month, calendar month, and all 4 digits of the year, indicating the century and year (Fri XX/XX/20XX)
System Time	HH/MM/SS	Presented as a 24-hour clock setting in hours, minutes, and seconds

3.3 Advanced

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

3.3.1 CPU

Feature	Options	Description
CPU	Info only	Manufacturer, model, speed
CPU Signature	Info only	Display CPU Signature.
Microcode Patch	Info only	Display Microcode Patch.
Max CPU speed	Info only	Display Max CPU speed.
Min CPU speed	Info only	Display Min CPU speed.
CPU Speed	Info only	Display CPU Speed.
Processor Cores	Info only	Display Processor Cores.
Hyper Threading Technology	Info only	Display Hyper Threading Technology support or not.
Intel VT-x Technology	Info only	Display Intel VT-x Technology support or not.
Intel SMX Technology	Info only	Display Intel SMX Technology support or not
64 bit	Info only	Display 64 bit support or not
EIST Technology	Info only	Display EIST Technology support or not
CPU C3 state	Info only	Display CPU C3 state support or not
CPU C6 state	Info only	Display CPU C6 state support or not
CPU C7 state	Info only	Display CPU C7 state support or not
L1 Data Cache	Info only	Display cache info.
L1 Code Cache	Info only	Display cache info.
L2 Cache	Info only	Display cache info.
L3 Cache	Inf o only	Display cache info.
L4 Cache	Inf o only	Display cache info.
Hyper-threading	Disabled **Enabled**	Enabled for Windows XP and Linux (OS optimized for Hyper-Threading Technology) and Disabled for other OS (OS not optimized for Hyper-Threading Technology). When Disabled only one thread per enabled core is enabled.
VT-d	Disabled **Enabled**	Check to enable VT-d function on MCH.
Intel Virtualization Technology	Disabled **Enabled**	Enable/Disable support for the Intel virtualization technology.
Intel(R) SpeedStep(TM)	Disabled **Enabled**	Allows more than two frequency ranges to be supported.
Turbo Mode	Disabled **Enabled**	Turbo mode.
Configurable TDP Boot Mode	**Nominal** Down Deactivate	Configure TDP Mode as Nominal/Down/Deactivate. Disabled option will set MSR to Nominal and MMIO to Zero.

Feature	Options	Description
Config TDP Lock	**Disabled** Enabled	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.
Custom Configurable TDP	**Disabled** Enabled	Custom Configurable TDP settings
Power Limit 1	15W 20W 25W 30W **35W** 40W	XE SKU: Any value can be programmed. 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 Limit."
Power Limit 1 Window	0 **1** 2 3 4 5 6 7 8 10 12 14 16 20 24 28 32 40 48 56 64 80 96 112 128	Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. If the value is 0, default values will be programmed (28 sec for Mobile and 1 sec for Desktop). Indicates the time window over which TDP value should be maintained.
CPU C state	Disabled **Enabled**	Enable or disable CPU C states
C-State Auto Demotion	Disabled C1 C3 **C1 and C3**	Configure C-State Auto Demotion
Package C State limit	C0/C1 C2 C3 C6 C7 **Auto**	Package C State limit
Intel TXT(LT) support	**Disabled** Enabled	Enables or Disables Intel(R) TXT(LT) support.

Feature	Options	Description
CPU DTS	Disabled **Enabled**	Enable/Disable CPU DTS.
ACPI 3.0 T-state	**Disabled** Enabled	Enable/Disable ACPI 3.0 T-States.

3.3.2 Memory

Feature	Options	Description
Memory RC Version	Info only	Display Memory Reference Code Version.
Memory Frequency	Info only	Display Memory Frequency.
Total Memory	Info only	Display Total Memory.
VDD	Info only	Display Memory Voltage.
DIMM#0/1	Info only	Display DIMM#0/1.
Memory Timings	Info only	Display Memory timings
XMP Profile 1	Info only	Display XMP Profile 1 support or not.
XMP Profile 2	Info only	Display XMP Profile 2 support or not.
I2C Write Protect Control	Active **Write Protect**	I2C write protect control
SPD Write Protect	**Enabled** Disabled	Enable:Writes to SMBus slave addresses A0h - AEh are disabled.
Maximum Memory Frequency	**Auto** 1067 1200 1333 1400 1600 1800 1867 2000 2133 2200 2400 2600 2800 2933 3000 3200	Maximun Memory Frequency Selections in MHz
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.

3.3.3 Graphics

Feature	Options	Description
Graphics Configuration	Info only	
IGFX VBIOS Version	Info only	Display VBIOS Version.
Graphics Turbo IMON Current	31	Graphics turbo IMON current values supported (14-31).
Primary Display	**Auto** IGFX PEG PCIE	Select which of IGFX/PEG/PCI Graphics device should be Primary Display Or select SG for Switchable Gfx.
Primary PEG	**Auto** PEG1 PEG2	Select PEG0/PEG1/PEG2/PEG3 Graphics device should be Primary PEG.
Internal Graphics	**Auto** Disabled Enabled	Keep IGD enabled based on the setup options.
Aperture Size	128MB **256MB** 512MB 1024MB 2048MB 4096MB	Select the Aperture Size.
DVMT Pre-Allocated	**32M** 64M 96M 128M 160M 192M 224M 256M 288M 320M 352M 384M 416M 448M 480M 512M 1024M 1536M 2048M 4M 8M 12M 16M 20M 24M 28M 32M/F7 36M 40M 44M	Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.

Feature	Options	Description
DVMT Pre-Allocated (cont'd)	48M 52M 56M 60M	
DVMT Total Gfx Mem	128M **256M** MAX	Select DVMT5.0 Total Graphic Memory size used by the Internal Graphics Device.
Gfx Low Power Mode	**Enabled** Disabled	This option is applicable for SFF only.
EDP to LVDS Bridge Configuration	**Info only**	
Data Format and Color Depth	VESA 24 bpp JEIDA 24 bpp **JEIDA/VESA 18 bpp**	Data format and color depth select
LVDS Output Mode	**Single LVDS bus** Dual LVDS bus	Single/Dual mode select
DE Polarity	**Active High** Active Low	DE Polarity select
Vsync Polarity	**Active High** Active Low	Vsync Polarity select
Hsync Polarity	**Active High** Active Low	Hsync Polarity select
LVDS/eDP Backlight Mode	**BMC Mode** GTT Mode	Select LVDS Backlight control function.
GTT LVDS/eDP Backlight Control	0% 20% 40% 60% 80% **100%**	Actual backlight value in percent of the maximum setting.
DDI function choose	**Display Port** HDMI	Select DDI function choose to display port or HDMI.
Primary IGFX Boot Display	**VBIOS Default** EFP LFP EFP3 EFP2	Select the Video Device which will be activated during POS.
Select Secondary Display	**Disabled**	Select Secondary Display Device.
LCD Panel Type	**VBIOS Default** 640X480 800X600 1024X768 1280X1024 1400X1050 1600X1200 1366X768 1680X1050 1920X1200 1440X900 1600X900	Select LCD panel used by Internal Graphics Device by selecting the appropriate setup item.

Feature	Options	Description
LCD Panel Type (cont'd)	1024X768 LVDS2 1280X800 1920X1080 2048X1536	
Active LFP	No LVDS **eDP Port-A**	Select the Active LFP Configuration.
Panel Scaling	**Auto** Off Force Scaling	Select the LCD panel scaling option used by the Internal Graphics Device.
RC6(Render Standby)	Enabled **Disabled**	Check to enable render standby support

7.3.4 SATA

Feature	Options	Description
SATA Controller(s)	**Enabled** Disabled	Enable/Disable SATA Device.
SATA Mode Selection	**AHCI** RAID	Determines how SATA controller(s) operate.
SATA Speed Selection	Default Gen1 **Gen2** Gen3	Indicates the maximum speed the SATA controller can support.
SATA Test Mode	Enabled **Disabled**	Test Mode Enable/Disable (Loop Back)
SATA Port Configuration	Submenu	
Software Feature Mask Configuration	Info only	
RAID0	**Enabled** Disabled	Enable/Disable RAID0 feature.
RAID1	**Enabled** Disabled	Enable/Disable RAID1 feature.
RAID10	**Enabled** Disabled	Enable/Disable RAID10 feature.
RAID5	**Enabled** Disabled	Enable/Disable RAID5 feature.
Intel Rapid Recovery Technology	**Enabled** Disabled	Enable/Disable Intel Rapid Recovery Technology.
OROM UI and BANNER	**Enabled** Disabled	If enabled, then the OROM UI is shown. Otherwise, no OROM banner or information will be displayed if all disks and RAID volumes are Normal.
HDD Unlock	**Enabled** Disabled	If enabled, indicates that the HDD password unlock in the OS is enabled.
LED Locate	**Enabled** Disabled	If enabled, indicates that the LED/SGPIO hardware is attached and ping to locate feature is enabled on the OS.
IRRT Only on ESATA	**Enabled** Disabled	If enabled, then only IRRT volumes can span internal and eSATA drives. If disabled, then any RAID volume can span internal and eSATA drives.
Smart Response Technology	**Enabled** Disabled	Enable/Disable Smart Response Technology.
OROM UI Delay	**2 Seconds** 4 Seconds 6 Seconds 8 Seconds	Select the delay time of the OROM UI Splash Screen in a normal status.
RST Force Form	Enabled **Disabled**	Enable/Disable Form for Intel Rapid Storage Technology.
Aggressive LPM Support	**Enabled** Disabled	Enable PCH to aggressively enter link power state.

3.3.4.1 SATA > SATA Port Configuration

Feature	Options	Description
SATA Port Configuration	Info only	
Port X	Disabled **Enabled**	Enable/Disable SATA Port.
Hot Plug	**Disabled** Enabled	Designates this port as Hot Pluggable.
External SATA	**Disabled** Enabled	External SATA Support.
Spin up Device	**Disabled** Enabled	On an edge detect from 0 to 1, the PCH starts a COMRESET initialization sequence to the device.
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, ISATA, Flex, DirectConnect or M2.
Device Sleep	**Disabled** Enabled	mSATA for RTD3
SATA DEVSLEP Idle Timeout Configuration	**Disabled** Enabled	Enable/Disable SATA DTIO Configuration

7.3.5 USB

Feature	Options	Description
USB Configuration	Submenu	
USB Module Version	Info only	
USB Devices	Info only	X Drive, X Keyboards, X Mouse, X Hubs
Legacy USB Support	**Enabled** Disabled Auto	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 and setup.
XHCI Hand-off	**Enabled** Disabled	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by the XHCI OS driver.
USB Mass Storage Driver Support	**Enabled** Disabled	Enable/Disable USB Mass Storage Driver Support.
Port 60/64 Emulation	Enabled **Disabled**	Enables I/O port 60h/64h emulation support. This should be enabled for the complete USB keyboard legacy support for non-USB aware OSes.
USB hardware delays and time-outs:	Info only	
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.
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.
Mass Storage Devices	Info only	List current USB max stroge device.

3.3.5.1 USB > USB Configuration

Feature	Options	Description
USB Precondition	**Disabled** Enabled	Precondition work on USB host controller and root ports for faster enumeration.
XHCI Disable Compliance Mode	**FALSE** TRUE	Options to disable Compliance Mode. Default is FALSE to not disable Compliance Mode. Set TRUE to disable Compliance Mode.
XDCI Support	**Disabled** Enabled	Enable/Disable XDCI (USB OTG Device)
USB Port Disable Override	**Disabled** Select Per-Pin	Selectively Enable/Disable the corresponding USB port from reporting a Device Connection to the controller.

3.3.6 Network

Feature	Options	Description
Network Stack	Info only	
Network Stack	Enabled **Disabled**	Enable/Disable UEFI network stack.
PCH LAN Controller	**Enabled** Disabled	Enable/Disable onboard NIC.
Wake on LAN	**Enabled** Disabled	Enable/Disable integrated LAN to wake the system. (The Wake On LAN cannot be disabled if ME is on at Sx state.
AMT Configuration	Info only	
Intel AMT	Enabled **Disabled**	Enable/Disable Intel (R) Active Management Technology BIOS Extension.
BIOS Hotkey Pressed	Enabled **Disabled**	Enable/Disable BIOS hotkey press.
MEBx Selection Screen	Enabled **Disabled**	Enable/Disable MEBx selection screen.
Hide Un-Configure ME Confirmation	Enabled **Disabled**	Hide Un-Configure ME without password Confirmation Prompt.
MEBx Debug Message Output	Enabled **Disabled**	Enable MEBx debug message output.
Un-Configure ME	Enabled **Disabled**	Un-Configure ME without password.
Amt Wait Timer	0	Set timer to wait before sending ASF_GET_BOOT_OPTIONS.
Disable ME	Enabled **Disabled**	Set ME to Soft Temporary Disabled.
ASF	**Enabled** Disabled	Enable/Disable Alert Specification Format.
Activate Remote Assistance Process	Enabled **Disabled**	Trigger CIRA boot.
USB Configure	**Enabled** Disabled	Enable/Disable USB Configure function.
PET Progress	**Enabled** Disabled	User can Enable/Disable PET Events progress to recieve PET events or not.
AMT CIRA Timeout	0	OEM defined timeout for MPS connection to be established. 0 - use the default timeout value of 60 seconds. 255 - MEBX waits until the connection succeeds.
Watchdog	Enabled **Disabled**	Enable/Disable WatchDog Timer.
OS Timer		Set OS watchdog timer.
BIOS Timer		Set BIOS watchdog timer.

3.3.7 PCI and PCIe

Feature	Options	Description
PCI Common Settings	Info only	
PCIE Ports 1-4 Configuration	**4x1 Port** 1x2 2x1 Port 2x2 Port 1x4 Port	Configures PCI-E Port 1-4 of PCH. [4X1]: Port 1-4 (x1) and Port 8 (x1) [1x2 2x1]: Port 1 (x2), Port 2 (disabled), Ports 3 and Port 4 (x1) [2x2]: Port 1-2 (x2) and Port 3-4 (x2) [1x4]: Port 1 (x4), Ports 2-4 (disabled)
PCIE Ports 5-8 Configuration	**4x1 Port** 1x2 2x1 Port	Configures PCI-E Port 5-8 of PCH. [4X1]:Port 5-8 (x1) and Port 8 (x1) [1x2 2x1]: Port 5 (x2), Port 6 (disabled), Ports 7 and Port 8 (x1)
PCI Latency Timer	**32 PCI Bus Clocks** 64 PCI Bus Clocks 96 PCI Bus Clocks 128 PCI Bus Clocks 160 PCI Bus Clocks 192 PCI Bus Clocks 224 PCI Bus Clocks 248 PCI Bus Clocks	Value to be programmed into PCI Latency Timer Register.
PCI-X Latency Timer	32 PCI Bus Clocks **64 PCI Bus Clocks** 96 PCI Bus Clocks 128 PCI Bus Clocks 160 PCI Bus Clocks 192 PCI Bus Clocks 224 PCI Bus Clocks 248 PCI Bus Clocks	Value to be programmed into PCI Latency Timer Register.
VGA Palette Snoop	**Disabled** Enabled	Allow PCI cards that do not contain their own VGA color palette to access the video core's palette
PERR# Generation	**Disabled** Enabled	Enables or Disables PCI Device to Generate PERR#.
SERR# Generation	**Disabled** Enabled	Enables/Disables PCI Device to Generate SERR#.
PCI Express Configuration	Submenu	
PEG Configuration	Submenu	

3.3.7.1 PCI and PCIe > PCI Express Configuration

Feature	Options	Description
PCI Express Configuration	Info only	
PCI Express Clock Gating	Disabled **Enabled**	Enable/Disable PCI Express Clock Gating for each root port.
DMI Link ASPM Control	**Disabled** Enabled	Enable/Disable control of Active State Power Management on both NB side and SB side of the DMI Link.
Port8xh Decode	**Disabled** Enabled	Port8xh Decode
Compliance Test Mode	**Disabled** Enabled	Compliance Test Mode
PCI Express Gen3 EQ Lanes	Submenu	
PCI Express Root Port X	Submenu	

PCI and PCIe > PCI Express Configuration > PCI Express Gen3 EQ Lanes

Feature	Options	Description
Override SW EQ settings	**Disabled** Enabled	Override SW EQ settings

PCI and PCIe > PCI Express Configuration > PCI Express Root Port X

Feature	Options	Description
PCI Express Root Port	Disabled **Enabled**	Control the PCI Express Root Port.
Topology	**Unknown** x1 x4 Sata Express M2	Identify the SATA Topology: Default, ISATA, Flex, DirectConnect or M2.
ASPM Support	**Disabled** L0s L1 L0sL1 Auto	Set the ASPM Level. Force L0s - Force all links to L0s State Auto - BIOS auto configure; Disabled - Disables ASPM
L1 Substates	Disabled L1.1 L1.2 **L1.1 & L1.2**	PCI Express L1 Substates settings.
Gen3 Eq Phase3 Method	Hardware Static Coeff **Software Search**	PCIe Gen3 Equalization Phase 3 Method
UPTP	5	Upstream Port Transmitter Preset
DPTP	7	Downstream Port Transmitter Preset
ACS	Disabled **Enabled**	Enable/Disable Access Control Service Extend Capability
URR	**Disabled** Enabled	Enable/Disable PCI Express Unsupported Request Reporting.
FER	**Disabled** Enabled	Enable/Disable PCI Express Device Fatal Error Reporting.
NFER	**Disabled** Enabled	Enable/Disable PCI Express Device Non-Fatal Error Reporting.
CER	**Disabled** Enabled	Enable/Disable PCI Express Device Correctable Error Reporting.
CTO	**Disabled** Enabled	Enable/Disable PCI Express Completion Timer TO.
SEFE	**Disabled** Enabled	Enable/Disable Root PCI Express System Error on Fatal Error.
SENFE	**Disabled** Enabled	Enable/Disable Root PCI Express System Error on Non-Fatal Error.

Feature	Options	Description
SECE	**Disabled** Enabled	Enable/Disable Root PCI Express System Error on Correctable Error.
PME SCI	Disabled **Enabled**	Enable/Disable PCI Express PME SCI.
Hot Plug	**Disabled** Enabled	Enable/Disable PCI Express Hot Plug.
Advanced Error Reporting	Disabled **Enabled**	Advanced Error Reporting Enable/Disable
PCIe Speed	**Auto** Gen1 Gen2 Gen3	Select PCI Express port speed.
Transmitter Half Swing	**Disabled** Enabled	Transmitter Half Swing Enable/Disable.
Detect Non-Compiance	**Disabled** Enabled	Detect Non-Compliance PCI Express Device. If enabled, it will take more time at POST time.
Extra Bus Reserved	**0**	Extra Bus Reserved (0-7) for bridges behind this Root Bridge.
Reseved Memory	**10**	Reserved Memory Range for this Root Bridge.
Prefetchable Memory	**10**	Prefetchable Memory Range for this Root Bridge.
Reserved I/O	**4**	Reserved I/O (4K/8K/12K/16K/..../48K) Range for this Root Bridge.
PCIE Cp	**2**	Gen3 Equalization settings for physical PCIe lane
PCIE Cm	**6**	Gen3 Equalization settings for physical PCIe lane
PCIE LTR	Disabled **Enabled**	PCIE Latency Reporting Enable/Disable.
PCIE LTR Lock	**Disabled** Enabled	PCIE LTR Configuration Lock.
PCIE1 CLKREQ Mapping Override	Default **No CLKREQ** Custom number	PCIE CLKREQ Override for default platform mapping
Snoop Latency Ocerrid	Disabled Manual **Auto**	Snoop Latency Ocerride for PCH PCIE.
Non Snoop Latency Ocerrid	Disabled Manual **Auto**	Non Snoop Latency Ocerride for PCH PCIE.

3.3.7.2 PCI and PCIe > PEG Configuration

Feature	Options	Description
PEG Configuration	Info only	
PEG0	**Not Present**	Display PEG0 present or not.
Enable Root Port	Disabled Enabled **Auto**	Enable/Disable the Root Port.
Max Link Speed	**Auto** Gen1 Gen2 Gen3	Configure 0:1:0 Max Speed
PEG0 Slot Power Limit Value	**75**	Sets the upper limit on power supplied by slot. Power limit (in watts) is calculated by multiplying this value by the Slot Power Limit Scale. Values 0-255
PEG0 Slot Power Limit Scale	**1.0x** 0.1x 0.01x 0.001x	Select the scale used for the Slot Power Limit Value.
PEG0 Physical Slot Number	1	Set the physical slot number attached to this Port. The number has to be globally unique within the chassis. Values 0-8191
Detect Non-compliance Device	**Disabled** Enabled	Detect Non-Compliance PCI Express Device in PEG.
Program PCIe ASPM after OpROM	**Disabled** Enabled	Enabled: PCIe ASPM will be programmed after OpROM. Disabled: PCIe ASPM will be programmed before OpROM.
Program Static Phase1 Eq	**Enabled** Disable	Program Phase1 Presets/CTLEp
Gen3 Root Port Preset Value for each lane 0~15	**7**	Root Port preset value per lane for Gen3 Equalization
Gen3 Endpoint Preset value for each Lane 0~15	**7**	Endpoint preset value per lane for Gen3 Equalization
Gen3 Endpoint Hint value for each Lane 0~15	**2**	Endpoint Hint value per lane for Gen3 Equalization
PEG Gen3 RxCTLE Control 0~7	**0**	PEG Gen3 RxCTLE Control per Bundle
Always Attempt SW EQ	**Disabled** Enabled	Always Attempt SW EQ, even it has been done once
Number of Presets to test	7, 3, 5 0 – 9 **Auto**	Choose between 7,3,5 and 0-9. Auto = current default for CPU
Allow PERST# GPIO Usage	**Enabled** Disable	Enable/Disable GPIO-based resets to PEG endpoint(s) during margin search, if needed
SW EQ Enable VOC	Jitter Only Test Mode Jitter & VOC Test Mode **Auto**	Select Jitter & VOC test mode (default) or Jitter only test mode. Auto will current default (Enabled)
Jitter Dwell Time	**3000**	PEG Gen3 Preset Search dwell time [0..65535] in [usec]
Jitter Error Target	**2**	The margin search error target value [1..65535]
VOC Dwell Time	**10000**	The VOC margin search dwell time [0..65535] in [usec]

Feature	Options	Description
VOC Error Target	**2**	The VOC margin search error target value [1..65535]
Generate BDAT PEG Margin Data	**Disabled** Generate Port Jitter Data	Enable to generate BDAT PCIe margin tables
PCIe Rx CEM Test Mode	**Disabled** Enabled	Enable/Disable PEG Rx CEM Loopback Mode
PCIe Spread Spectrum Clocking	**Enabled** Disable	Allows disabling of Spread Spectrum Clocking for compliance testing

3.3.8 Super IO

Feature	Options	Description
Super IO Chip	Info only	
W83627DHG Super IO Configuration	Info only	
Serial Port 1 Configuration		
Serial Port	**Enabled** Disabled	Enable/Disable Serial Port (COM).
Device Settings	IO=3F8h; IRQ=4	Fixed configuration of serial port.
Change Settings	**Auto** IO=3F8h; IRQ=4 IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12 IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12 IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12 IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12	Select an optimal setting for Super IO device.
Serial Port 2 Configuration		
Serial Port	**Enabled** Disabled	Enable/Disable Serial Port (COM).
Device Settings	IO=2F8h; IRQ=3	Fixed configuration of serial port.
Change Settings	**Auto** IO=2F8h; IRQ=3 IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12 IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12 IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12 IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12	Select an optimal setting for Super IO device.
Device Mode	**Standard Serial Port Mode** IrDA Active pulse 1.6 uS IrDA Active pulse 3/16 bit time ASKIR Mode	

Feature	Options	Description
N5104D Super IO Configuration	Info only	
Serial Port 1 Configuration		
Serial Port	**Enabled** Disabled	Enable/Disable Serial Port (COM).
Device Settings	IO=240h; IRQ=7	Fixed configuration of serial port.
Change Settings	**Auto** IO=240h; 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.
Serial Port 2 Configuration		
Serial Port	**Enabled** Disabled	Enable/Disable Serial Port (COM).
Device Settings	IO=248h; IRQ=5	Fixed configuration of serial port.
Change Settings	**Auto** IO=248h; IRQ=5 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.

3.3.9 ACPI and Power Management

Feature	Options	Description
ACPI and Power Management	Info only	
Enable ACPI Auto Configuration	Enabled **Disabled**	Enables or Disables BIOS ACPI Auto Configuration.
Enable Hibernation	**Enabled** Disabled	Enables or Disables System ability to Hibernate (OS/S4 Sleep State). This option may be not effective with some OS.
ACPI Sleep State	Suspend Disabled **S3 (Suspend to RAM)**	Select ACPI sleep state the system will enter when the SUSPEND button is pressed.
Lock Legacy Resources	Enabled **Disabled**	Enables or Disables Lock of Legacy Resources
ACPI Low Power S0 Idle	Enabled **Disabled**	Enable or Disable ACPI Low Power S0 Idle Support.
Emulation AT/ATX	Emulation AT **ATX**	Select Emulation AT or ATX function. If this option set to [Emulation AT], BIOS will report no suspend functions to ACPI OS. In windows XP, it will make OS show shutdown message during system shutdown.

3.3.10 Sound

Feature	Options	Description
Sound	Info only	
HD Audio	Disabled Enabled **Auto**	Control Detection of the HD-Audio device. Disabled: HDA will be unconditionally disabled. Enabled: HDA will be unconditionally enabled. Auto: HDA will be enabled if present, disabled other.

3.3.11 Serial Port Console

Feature	Options	Description
Serial Port Console	Info only	
COM1	Info only	
Console Redirection	Enabled **Disabled**	Console Redirection Enable or Disable.
Console Redirection Settings	Submenu	
COM2	Info only	
Console Redirection	Enabled **Disabled**	Console Redirection Enable or Disable.
Console Redirection Settings	Submenu	
COM3	Info only	
Console Redirection	Enabled **Disabled**	Console Redirection Enable or Disable.
Console Redirection Settings	Submenu	
COM4	Info only	
Console Redirection	Enabled **Disabled**	Console Redirection Enable or Disable.
Console Redirection Settings	Submenu	
Legacy Console Redirection	Info only	
Legacy Console Redirection Settings	Submenu	
Serial Port for Out-of-Band Management/ Windows Emergency Management Services (EMS)	Info only	
Console Redirection	**Disabled** Enabled	Console Redirection Enable or Disable.

3.3.11.1 Serial Port Console > Console Redirection Settings

Feature	Options	Description
Console Redirection Settings	Info only	
Terminal Type	VT100 VT100+ VT-UTF8 **ANSI**	Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100+: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
Bits per second	9600 19200 38400 57600 **115200**	Selects serial port transmission speed.
Data Bits	7 **8**	Select Data Bits.
Parity	**None** Even Odd Mark Space	Select Parity.
Stop Bits	**1** 2	Select number of stop bits.
Flow Control	**None** Hardware RTS/CTS	Select flow control.
VT-UTF8 Combo Key Support	Disabled **Enabled**	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals.
Recorder Mode	**Disabled** Enabled	With this mode enabled only text will be sent. This is to capture Terminal data.
Resolution 100x31	**Disabled** Enabled	Enables or disables extended terminal resolution
Legacy OS Redirection	**80x24** 80x25	On Legacy OS, the Number of Rows and Columns supported redirection
Putty KeyPad	**VT100** LINUX XTERMR6 SCO ESCN VT400	Select FunctionKey and KeyPad on Putty.
Redirection After BIOS Post	**Always Enabled** BootLoader	The Settings specify if BootLoader is selected than Legacy console redirection is disabled before booting to Legacy OS. Default value is Always Enable which means Legaacy console Redirection is enabled for Legacy OS.

3.3.11.2 Serial Port Console > Legacy Console Redirection Settings

Feature	Options	Description
Legacy Console Redirection Port	**COM1** COM2+ COM3 COM4	Select a COM port to display redirection of Legacy OS and Legacy OPROM Messages

3.3.11.3 ICC Configuration

Feature	Options	Description
ICC Information	Info only	

Note1: The item is view only in standard BIOS default, the options can be opened by customer request if neccessary.

3.3.12 Thermal

Feature	Options	Description
Thermal	Info only	
Active Trip Point	Disabled 40 C 50 C 60 C 70 C **BMC Default**	This value controls the temperature of the ACPI Active Trip Point - the point in which the OS will turn the processor fan on Active Trip Point Fan Speed.
Passive Trip Point	**Disabled** 80 C 90 C	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
Critical Trip Point	**Disabled** 65 C 75 C 85 C	This value controls the temperature of the ACPI Critical Trip Point - the point in which the OS will shut the system off. NOTE: 100C is the Plan Of Record (POR) for all Intel mobile processors.
Watchdog ACPI Even Shutdown	**Disabled** Enabled	Enable/Disable Watchdog ACPI Even Shutdown.

3.3.13 Miscellaneous

Feature	Options	Description
Smart Battery Function	Enabled **Disabled**	Auto/Disable Smart Battery Function
Trusted Computing	Submenu	
NVME Configuration	Submenu	

3.3.13.1 Miscellaneous > Trusted Computing

Feature	Options	Description
Security Device Support	Enabled **Disabled**	Enables or Disables BIOS support for security device. When disabled OS wil not show Security Device. TCG EFI protocol and INT1A interface will not be available
TPM State	**Enabled** Disabled	Enable/Disable Security Device. NOTE: Your Computer will reboot during restart in order to change State of the Device.
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.
Device Start	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

3.3.13.2 Miscellaneous > NVME Configuration

Feature	Options	Description
NVME controller and Drive information	Info Only	

3.3.14 AMI Graphic Output Protocol Policy

Feature	Options	Description
Intel (R) Graphics Controller Intel (R) GOP Driver [9.0.1042]	Info Only	
Brightness Setting	255	Set GOP Brightness value
BIST Enable	Enabled **Disabled**	Starts or stops the BIST on the integrated display panel.

3.4 Boot

3.4.1 Boot Configuration

Feature	Options	Description
Boot Configuration	Info only	
Setup Prompt Timeout	**1**	Enable/Disable the onboard SATA controllers.
Bootup NumLock State	**On** Off	Select SATA controller mode.
Quiet Boot	Disabled **Enabled**	Enable/Disable the PATA port. In fact this enables or disables the SATA channel on which the onboard SATA to PATA converter is attached. When set to enabled the system boot will be delayed for the time specified in PATA Port Detection Timeout if no PATA device is connected. Auto: Scan for PATA device and enable per default.
CSM Configuration	Submenu	
Boot Option Priorities	Info only	
Boot Option #1 / Boot Option #2 ...		Press [Enter] to configure the boot priority. This option allows you to specify the boot device priority from the available UEFI applications during system boot-up. **Note:** Use this item to determine system boot order from available options
Fast Boot	**Disabled** Enabled	Define the maximum time to wait for drive detection on PATA port.
SATA Support	Last Boot HDD Only **All SATA Devices**	
VGA Support	Auto **EFI Driver**	If set to Auto, only install Legacy OpRom with Legacy OS and logo would NOT be shown during post. EFI driver will still be installed with EFI OS.
USB Support	Disabled Full Initial **Partial Initial**	If Disabled, all USB devices will NOT be available until after OS boot. If Partial Initial, USB Mass Storge and specific USB port/device will NOT be available before OS boot. If Enabled, all USB devices will be available in OS and Post.
PS2 Devices Support	Disabled **Enabled**	If Disabled, PS2 devices will be skipped.
NetWork Stack Driver Support	**Disabled** Enabled	If Disabled, NetWork Stack Driver will be skipped.
Redirection Support	**Disabled** Enabled	If disable, Redirection function will be disabled.
New Boot Option Policy	**Default** Place First Place Last	Controls the placement of newly detected UEFI boot options

3.4.1.1 CSM Configuration

Feature	Options	Description
CSM Support	**Enabled** Disable	This option controls if CSM will be launched.
CSM16 Module Version	Info only	

GateA20 Active	**Upon Request** Always	UPON REQUEST - GA20 can be disabled using BIOS services. ALWAYS - do not allow disabling GA20; this option is useful when any RT code is executed above 1MB.
Option ROM Messages	**Force BIOS** Keep Current	Set display mode for Option ROM.
INT19 Trap Response	**Immediate** Postponed	BIOS reaction on INT19 trapping by Option ROM: Immediate: execute the trap right away; Postponed: execute the trap during legacy boot.
Boot Option filter	**UEFI and Legacy** Legacy only UEFI only	This option controls what devices system can to boot.
Option ROM execution	Info only	
Network	**Do not launch** Legacy only UEFI only	Controls the execution of UEFI and Legacy PXE OpROM.
Storage	Do not launch UEFI only **Legacy only**	Controls the execution of UEFI and Legacy Storage OpROM.
Video	Do not launch UEFI only **Legacy only**	Controls the execution of UEFI and Legacy Video OpROM.
Other PCI devices	Do not launch **UEFI** Legacy	For PCI devices other than Network, Mass storage or Video defines which OpROM to launch.

3.5 Security

3.5.1 Password Description

Feature	Options	Description
Administrator Password	Enter password	
User Password	Enter password	
Secure Boot menu	Submenu	

3.5.2 Security > Secure Boot menu

Feature	Options	Description
System Mode	Info only	
Secure Boot	Info only	
Vendor Keys	Info only	
Secure Boot	**Disabled** Enabled	Secure Boot can be enabled if: 1..System running in User mode with enrolled Platform Key(PK) 2..CSM function is disabled
Secure Boot Mode	Standard **Custom**	Secure Boot mode selector. 'Custom' mode allows users to change Image Execution policy and manage Secure Boot Keys
Key Management	**Submenu**	

3.5.3 Security > Secure Boot menu > Key Management

Feature	Options	Description
Provision Factory Default Keys	**Disabled** Enabled	Install factory default Secure Boot Keys when system is in Setup Mode
Enroll all Factory Default Keys		Force System to User Mode: Install all Factory Default Keys (PK,KEK,db,dbt). Change takes effect after reboot.
Save all Secure Boot variables		Save NVRAM content of all Secure Boot variables to the files (EFI_SIGNATURE_LIST data format) in root folder on a target file system device
Platform Key (PK)	Set New Key	Enroll Factory Defaults or load the keys from a file with: 1. Public Key Certificate in: a) EFI_SIGNATURE_LIST b) EFI_CERT_X509 (DER encoded) c) EFI_CERT_RSA2048 (bin) d) EFI_CERT_SHA256 (bin) 2. Authenticated UEFI Variable Key Source: Default , Custom, Mixed
Key Exchange Keys	Set New Key Append Key	Enroll Factory Defaults or load the keys from a file with: 1. Public Key Certificate in: a) EFI_SIGNATURE_LIST b) EFI_CERT_X509 (DER encoded) c) EFI_CERT_RSA2048 (bin) d) EFI_CERT_SHA256 (bin) 2. Authenticated UEFI Variable Key Source: Default , Custom, Mixed
Authorized Signatures	Set New Key Append Key	Enroll Factory Defaults or load the keys from a file with: 1. Public Key Certificate in: a) EFI_SIGNATURE_LIST b) EFI_CERT_X509 (DER encoded) c) EFI_CERT_RSA2048 (bin) d) EFI_CERT_SHA256 (bin) 2. Authenticated UEFI Variable Key Source: Default , Custom, Mixed
Forbidden Signatures	Set New Key Append Key	Enroll Factory Defaults or load the keys from a file with: 1. Public Key Certificate in: a) EFI_SIGNATURE_LIST b) EFI_CERT_X509 (DER encoded) c) EFI_CERT_RSA2048 (bin) d) EFI_CERT_SHA256 (bin) 2. Authenticated UEFI Variable Key Source: Default , Custom, Mixed
Authorized TimeStamps	Set New Key Append Key	Enroll Factory Defaults or load the keys from a file with: 1. Public Key Certificate in: a) EFI_SIGNATURE_LIST b) EFI_CERT_X509 (DER encoded) c) EFI_CERT_RSA2048 (bin) d) EFI_CERT_SHA256 (bin) 2. Authenticated UEFI Variable Key Source: Default , Custom, Mixed

3.6 Save & Exit

3.6.1 Reset Options

Feature	Options	Description
Save Changes and Reset	Save changes and reset the system.	Save Changes and Reset
Discard Changes and Reset	Reset the system without saving any changes.	Discard Changes and Reset

3.6.2 Save Options

Feature	Options	Description
Save Changes		Save Changes done so far to any of the setup options.
Discard Changes		Discard Changes done so far to any of the setup options.
Restore Defaults		Restore/Load Default values for all the setup options.
Save as User Defaults		Save the changes done so far as User Defaults.
Restore User Defaults		Restore the User Defaults to all the setup options.