



# AV710-X3



IP65 MXM-GPU Server with Intel Xeon D-1577 processor, MIL-STD-461 EMI 18-36V DC-In

## **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**

- ▶ All rights reserved. No part of this publication may be reproduced in any form or by any means, without prior written permission from the publisher.
- ▶ All trademarks are the properties of the respective owners.
- ▶ All product specifications are subject to change without prior notice

## Revision History

Revision	Date (yyyy/mm/dd)	Changes
Version 1.0	2022/03/15	Initial release

## Packing list

- ▶ AV710-X3 IP65 MXM-GPU Server System
- ▶ CD (Driver + Quick Installation Guide)

## Ordering information

Model Number	[Scription]
<b>AV710-X3</b>	Military MXM-GPU Server with Intel Xeon D-1577 Processor, IP65 rating, MIL-STD-D38999 Connectors, 18~36V DC-in, Extreme Rugged Operating Temperature -40 to 60°C



---

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

---

## Table Contents

<b>SAFETY INFORMATION</b> .....	<b>2</b>
ELECTRICAL SAFETY .....	2
OPERATION SAFETY .....	2
<b>STATEMENT</b> .....	<b>2</b>
<b>REVISION HISTORY</b> .....	<b>3</b>
<b>PACKING LIST</b> .....	<b>3</b>
<b>ORDERING INFORMATION</b> .....	<b>3</b>
<b>TABLE CONTENTS</b> .....	<b>4</b>
<b>CHAPTER 1: PRODUCT INTRODUCTION</b> .....	<b>5</b>
• KEY FEATURES .....	5
• DIMENSIONS .....	6
<b>CHAPTER 2: JUMPERS AND CONNECTORS LOCATIONS</b> .....	<b>7</b>
► CONNECTOR PIN DEFINITIONS .....	7
Connector X1, X2, X3 .....	8
Connector X4, X5, X6 .....	9
<b>CHAPTER 3: BIOS SETUP</b> .....	<b>10-50</b>

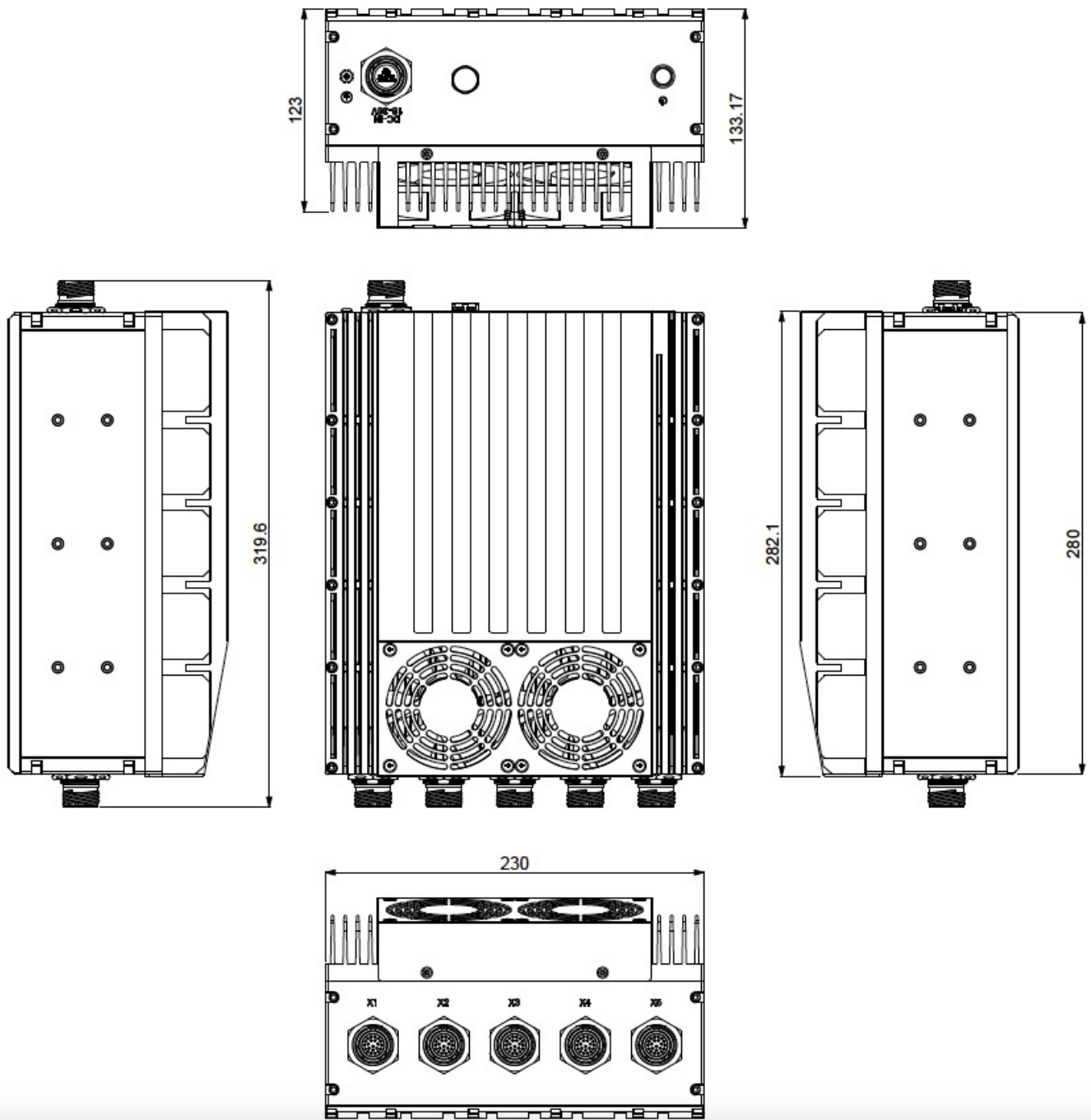
## Chapter 1: Product Introduction

### • Key Features

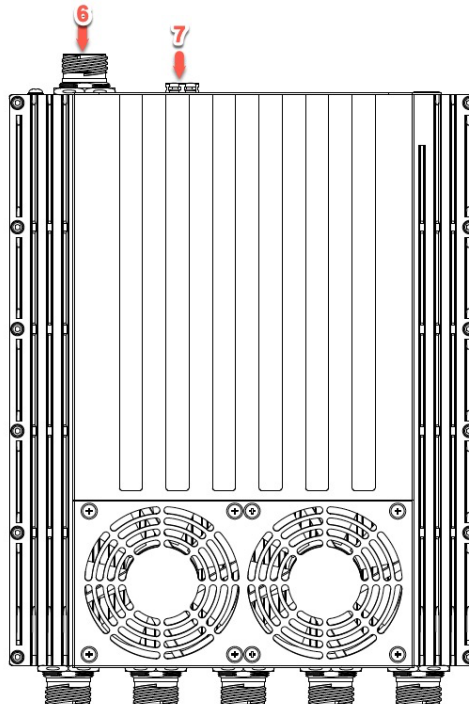
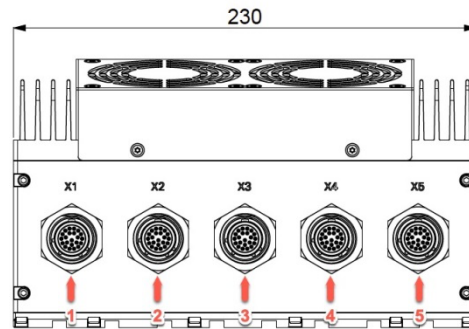
System	
CPU	Intel® Xeon® Processor D-1577 Processor (24M Smart Cache, 16 Cores/ 32 Threads, Base Frequency 1.3GHz; Max Turbo Frequency 2.1 GHz)
Memory Type	Supports up to 256GB DDR4 ECC RDIMM
Graphics Card	Nvidia Quadro RTX5000 MXM (16GB DDR6, 3072 CUDA Cores)
BIOS	AMI® BIOS
Storage Device	SATA1: 2.5" SATAIII SSD
Front I/O	
DC-In	1 x Amphenol TV07RW-11-54P
Power Button	1 x Power Button with LED backlight
Waterproof valve	1
Rear I/O	
DVI-D	1 x DVI-D Amphenol TV07RW-13-35S
1Gb Ethernet	1 x GbE LAN Amphenol TV07RW-13-98S
10Gb Ethernet	1 x 10GbE Copper LAN Amphenol TV07RW-13-98S
10Gb Ethernet	1 x 10GbE Copper LAN Amphenol TV07RW-13-98S
COM	1 x COM Amphenol TV07RW-13-98S
Applications	
Applications	Military Platforms Requiring Compliance to MIL-STD-810G Embedded Computing and applications subject to Harsh Temperature, Shock, Vibration, Altitude, Dust and EMI Conditions.
Operation System	
OS	Windows 10 64bit, Linux by request.
Mechanical & Environment	
Chassis	Aluminum Alloy, Corrosion design
Finish	Anodic aluminum oxide (Color Iron gray)
Cooling	Natural Passive Convection/Conduction. No Moving Parts
Power Requirements	MIL-STD-461 EMI Power Supply, 18-36V DC In 300W
Dimension (W x D x H)	280 x 230 x 122mm (11.02" x 9.05" x 4.8")
Operating Temp.	-40 to 60°C (ambient with air flow)
Storage Temp.	-40 to 85°C
Relative Humidity	5% to 95%, non-condensing

\* Specifications are subject to change without notice\*

- Dimensions



- Panel Component




1	GbE LAN label (X1)
2	10GbE Copper LAN, label (X2)
3	10GbE Copper LAN, label (X3)
4	DVI-D, label (X4)
5	COM, label (X5)
6	DC In, Label (X6)
7	Waterproof valve, label (X7)
8	Power Button with LED backlight

## Chapter 2: Jumpers and Connectors Locations

- D38999 Connector Pin Definitions


(X1): GbE LAN

**X1:GbE LAN** Amphenol TV06RW-13-98p

I/O	Pin define	D38999(B1)	RJ45-F(B2)
	D0+	A	1
	D0-	H	2
	D1+	F	3
	D1-	F	6
	D2+	C	4
	D2-	B	5
	D3+	K	7
	D3-	J	8
	NC	G	G
	NC	D	G


(X2): 10GbE LAN

**X2:10GbE LAN** Amphenol TV06RW-13-98p

I/O	Pin define	D38999(B1)	RJ45 F (B2)
	D0+	A	1
	D0-	H	2
	G	G	G
	D1+	F	3
	D1-	E	6
	G	D	G
	D2+	C	4
	D2-	B	5
	D3+	K	7
	D3-	J	8

(X3): 10GbE LAN


**X3:10GbE LAN** Amphenol TV06RW-13-98p

I/O	Pin define	D38999(B1)	RJ45 F (B2)
	D0+	A	1
	D0-	H	2
	G	G	G
	D1+	F	3
	D1-	E	6
	G	D	G
	D2+	C	4
	D2-	B	5
	D3+	K	7
	D3-	J	8




(X4): DVI-D

X4: DVI-D Amphenol TV06RW-13-35P

I/O	Pin define	D38999(B1)	DVI-M(B2)
	DPA_TN0	1	1
	DPA_TP0	2	2
	GND	3	3
	DPA_AUXP_CLK(p)	4	6
	DPA_AUXP_CLK(n)	5	7
	GND	6	8
	DPA_TN1	7	9
	DPA_TP1	8	10
	GND	9	11
	DPA_PWR	10	14
	ReturnGND	11	15
	DPA_DET	12	16
	DPA_TN2	13	17
	DPA_TP2	14	18
	GND	15	19
	CLOCK Shield	16	22
	DPA_TP3	17	23
	DPA_TN3	18	24
	GND	19	shell
		20	
		21	
		22	

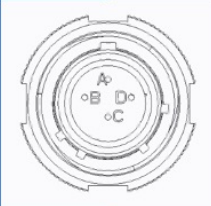
(X5): COM

X5:COM Amphenol TV07RW-13-98P

	Pin define	D38999(B1)	D-SUB-M(B2)
	GND	E	5
	RI	K	9
	DTR	F	4
	CTS	B	8
	TXD	G	3
	RTS	C	7
	RXD	H	2
	DSR	D	6
	DCD	A	1

(X6): DC-In

X6: DC IN Amphenol TV06RW-13-04S

I/O	Pin define	B1	B2
	V+(yellow)	A	+
	V+(yellow)	D	+
	V-(black)	B	-
	V-(black)	C	-

### 3. BIOS Setup

#### • 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	Chipset	Security	Boot	Save & Exit
BIOS Information	Power Management ►	Processor ►	Setup	Boot ►	Save Change and Exit ►
System Information	System Management ►	Configuration ►	Administrator Password ►	Configuration	Discard Changes and Exit ►
Board Information	Thermal Management ►	Advanced Power ►	User Password	FIXED BOOT ORDER ►	Save Changes and Reset ►
System Date and Time	Watchdog Timer ►	Management Configuration ►	Secure Boot ►	Priorities	Discard Changes and Reset ►
Access Level	CSM Configuration ►	Memory Configuration ►		UEFI USB Key Drive BBS Priorities ►	Save Options
	Super IO Configuration ►	I/O Configuration ►			Boot Override ►
	Serial Console Redirection ►	PCH Configuration ►			
	USB Configuration ►				
	Network Stack Configuration ►				
	Miscellaneous ►				
	Driver Health ►				
	Trusted Computing ►				

#### Notes:

- indicates a submenu
- Gray text indicates info only

#### • 3.1.1 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 for details of the settings.

#### • 3.1.2 Main > BIOS Information

Feature	Options	Description
BIOS Vendor	Info only	American Megatrends
BIOS Version	Info only	ADLINK BIOS version
Build Date	Info only	ADLINK BIOS Build Date
SPS Firmware Version	Info only	Display SPS Firmware Version
BIOS Boot Source	Info only	Display BIOS Boot Source

#### • 3.1.3 Main > System Information

Feature	Options	Description
Project Name	Info only	Display Project Name.
CPU Board version	Info only	Display CPU Board Version.
CPU Board String	Info only	Display CPU Board String.
CPU Frequency	Info only	Display CPU Frequency.
Total Memory	Info only	Display Installed Memory Size.

- 3.1.4 Main > Board Information

Feature	Options	Description
Board Information	Submenu	
Board Information	Info only	
Serial Number	Info only	Display SEMA serial Number.
Manufacturing Date	Info only	Display SEMA manufacturing date.
Last Repair Date	Info only	Display SEMA last repair date.
MAC ID	Info only	Display SEMA MAC ID.
Runtime Statistics	Info only	
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.
Power Cycles	Info only	The returned value specifies the number of times the external power supply has been shut down
Boot Cycles	Info only	The Boot counter is increased after a HW- or SW-Reset or after a successful power-up.
Feature	Options	Description
Boot Reason	Info only	The boot reason is the event which causes the reboot of the system.

- 3.1.5 Main >System Date/Time

Feature	Options	Description
System Date	Info only	
System Time	Info only	

- 3.1.6 Main >Access Level

Feature	Options	Description
Access Level	Info only	

## 3.2 Advanced

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

- 3.2.1 Advanced > Power Management

Feature	Options	Description
Power Management	Info only	
Enable ACPI Auto Configuration	Disabled <b>Enabled</b>	Enable or Disables BIOS ACPI Auto Configuration.
Enable Hibernation	Disabled <b>Enabled</b>	Enables or Disables System ability to Hibernate (OS/S4 Sleep State). This option may be not effective with some OS.

Emulation AT/ATX	Emulation AT <b>ATX</b>	Select Emulation AT or ATX function. If this option is set to [Emulation AT], BIOS will report no suspend functions to ACPI OS. In windows XP, it will make OS show shutdown
LID Function	<b>Disabled</b> Enabled	Enable/Disable LID Function
Lock Legacy Resource	<b>Disabled</b> Enabled	Enables or Disables Lock of Legacy Resources
I21x Lan Power Ctrl	<b>PC2</b> PC1 C0	
ECO Mode	<b>Disabled</b> Enabled	
Power-up Mode	<b>Turn On</b> Remain Off Last State	
Power Consumption	Submenu	Power Consumption information.

- 3.2.2 Advanced > Power Management->Power Consumption

Feature	Options	Description
Power Consumption	Info Only	
Current Input Current	Info Only	Display Current Input Current
Current Input Power	Info Only	Display Current Input Power
VCORE	Info Only	Display VCORE Voltage
VMEM	Info Only	Display VMEM Voltage
5VSB	Info Only	Display 5VSB Voltage
VIN	Info Only	Display VIN Voltage
3.3VSB	Info Only	Display 3.3VSB Voltage
5V	Info Only	Display 5V Voltage

- 3.2.3 Advanced > System Management

Feature	Options	Description
System Management	Info Only	
Version	Info Only	Display SEMA Module Version.
SEMA Firmware	Info Only	Display SEMA Firmware Version.
Build Date	Info Only	Display SEMA Firmware Build Date.
SEMA Bootloader	Info Only	Display SEMA Bootloader Version.
Build Date	Info Only	Display SEMA Bootloader Build Date.
SEMA Features	Submenu	Display SEMA Supported Features
SEMA Supported Features	Info only	Display SEMA Supported Features
Flags	Submenu	Flag
Flags	Info only	
BMC Flags	Info Only	

BIOS Select	Info Only	
ATX/AT-Mode	Info Only	
Exception Code	Info Only	

- 3.2.4 Advanced > Thermal Management

Feature	Options	Description
Thermal Configuration Parameters	Info Only	
Thermal and Fan Speed	Submenu	
Smart Fan	Submenu	
Critical Trip Point	<b>Disabled</b> 65 C 75 C 85 C	The value is the temperature threshold of the Critical Trip Point.
Passive Cooling Trip Point	<b>Disabled</b> 80 C 90 C	The value is the temperature threshold of the Passive Cooling Trip Point.
Watchdog ACPI Event Shutdown	<b>Disabled</b> Enabled	Watchdog ACPI Event Shutdown Enabled/Disabled

- 3.2.4.1 Advanced > Thermal Management > Thermal and Fan Speed

Feature	Options	Description
Temperatures and Fan Speed	Info Only	
CPU Temperature	Info Only	
Current	Info Only	Display Current CPU Temperature
Startup	Info Only	Display Startup CPU Temperature
Min	Info Only	Display Min CPU Temperature
Max	Info Only	Display Max CPU Temperature

Feature	Options	Description
Board Temperature	Info Only	
Current	Info Only	Display Current Board Temperature
Startup	Info Only	Display Startup Board Temperature
Min	Info Only	Display Min Board Temperature
Max	Info Only	Display Max Board Temperature
CPU Fan Speed	Info Only	Display CPU Fan Speed

• 3.2.4.2 Advanced > Thermal Management > Smart Fan

Feature	Options	Description
Smart Fan	Info Only	
CPU Smart Fan Temperature Source	<b>CPU Sensor</b> Board Sensor	CPU Smart Fan Temperature Source
CPU Fan Mode	<b>AUTO (Smart Fan)</b> Fan Off Fan On	CPU Fan Mode
Trigger Point 1 to 4	Info Only	Display Trigger Point 1 to 4 information
Trigger Temperature	0-100	Select Trigger Temperature
PWM Level	0-100	Select Trigger Temperature

• 3.2.5 Advanced > Watchdog Timer

Feature	Options	Description
Watchdog Timer	Info only	
Power-Up Watchdog	<b>Disabled</b> Enabled	The Power Up Watchdog resets the system after a certain amount of time after power up.

• 3.2.6 Advanced > CSM Configuration

Feature	Options	Description
Compatibility Support Module Configuration	Info only	
CSM Support	Disabled <b>Enabled</b>	Enabled / Disabled CSM Support.
CSM16 Module Version	Info only	Display CSM16 Module Version
GateA20 Active	<b>Upon Request</b> 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	<b>Force BIOS</b> Keep Current	Set display mode for Option ROM
INT19 Trap Response	Immediate <b>Postponed</b>	BIOS reaction on INT19 trapping by Option ROM:IMMEDIATE – execute the trap right away; POSTPONED – execute the trap during legacy boot.

Feature	Options	Description
Boot option filter	<b>UEFI and Legacy</b> Legacy only UEFI only	This option controls Legacy/UEFI ROMs priority
Option ROM execution	Info only	
Network	<b>Do not launch</b> UEFI Legacy	Controls the execution of UEFI and Legacy PXE OpROM
Storage	Do not launch UEFI <b>Legacy</b>	Controls the execution of UEFI and Legacy Storage OpROM
Video	Do not launch UEFI <b>Legacy</b>	Controls the execution of UEFI and Legacy Video OpROM
Other PCI devices	Do not launch <b>UEFI</b> Legacy	Determines OpROM execution policy for devices other than Network, Storage, or Video

• 3.2.7 Advanced > Super IO Configuration

Feature	Options	Description
Super IO Configuration	Info only	
Super IO Chip NCT5104D	Info only	
Serial Port 1 Configuration	Submenu	Set Parameters of Serial Port 1 (COMA).
Serial Port 2 Configuration	Submenu	Set Parameters of Serial Port 2 (COMB).
Super IO Chip W83627DHG	Info Only	
Serial Port 1 Configuration	Submenu	Set Parameters of Serial Port 1 (COMA).
Serial Port 2 Configuration	Submenu	Set Parameters of Serial Port 2 (COMB).

• 3.2.7.1 Advanced > Super IO Configuration > Serial Port 1 Configuration (NCT5104D)

Feature	Options	Description
Serial Port 1 Configuration	Submenu	Set Parameters of Serial Port 1 (COMA).
Serial Port 1 Configuration	Info only	
Serial Port	Disabled <b>Enabled</b>	Enable or Disable Serial Port (COM).
Device Settings	Info Only	Display IO / IRQ information of COM Port.
Change Settings	<b>Auto</b> IO=240h; IRQ=10; 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.

• 3.2.7.2 Advanced > Super IO Configuration > Serial Port 2 Configuration (NCT5104D)

Feature	Options	Description
Serial Port 2 Configuration	Submenu	Set Parameters of Serial Port 2 (COMB).
Serial Port 2 Configuration	Info only	
Serial Port	Disabled <b>Enabled</b>	Enable or Disable Serial Port (COM).
Device Settings	Info Only	Display IO / IRQ information of COM Port.
Change Settings	<b>Auto</b> IO=248h; IRQ=11; 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.

• 3.2.7.3 Advanced > Super IO Configuration > Serial Port 1 Configuration (W83627DHG)

Feature	Options	Description
Serial Port 1 Configuration	Submenu	Set Parameters of Serial Port 1 (COMA).
Serial Port 1 Configuration	Info only	
Serial Port	Disabled <b>Enabled</b>	Enable or Disable Serial Port (COM).
Device Settings	Info Only	Display IO / IRQ information of COM Port.
Change Settings	<b>Auto</b> IO=3F8h; IRQ=4; IO=3F8h; IRQ=3,4,5,6,7,10,11,12 IO=2F8h; IRQ=3,4,5,6,7,10,11,12 IO=3E8h; IRQ=3,4,5,6,7,10,11,12 IO=2E8h; IRQ=3,4,5,6,7,10,11,12	Select an optimal setting for Super IO Device.

• 3.2.7.4 Advanced > Super IO Configuration > Serial Port 2 Configuration (W83627DHG)

Feature	Options	Description
Serial Port 2 Configuration	Submenu	Set Parameters of Serial Port 2 (COMB).
Serial Port 2 Configuration	Info only	
Serial Port	Disabled <b>Enabled</b>	Enable or Disable Serial Port (COM).
Device Settings	Info Only	Display IO / IRQ information of COM Port.
Change Settings	<b>Auto</b> IO=2F8h; IRQ=3; IO=3F8h; IRQ=3,4,5,6,7,10,11,12 IO=2F8h; IRQ=3,4,5,6,7,10,11,12 IO=3E8h; IRQ=3,4,5,6,7,10,11,12 IO=2E8h; IRQ=3,4,5,6,7,10,11,12	Select an optimal setting for Super IO Device.



• 3.2.8 Advanced > Serial Console Redirection

Feature	Options	Description
COM1	Info only	
Console Redirection	<b>Enabled</b> Disabled	Console Redirection Enable or Disable.
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. The item will be lunched before enable Console Redirection.
COM2	Info only	
Console Redirection	<b>Enabled</b> Disabled	Console Redirection Enable or Disable.
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. The item will be lunched before enable Console Redirection.
COM3	Info only	
Console Redirection	Enabled <b>Disabled</b>	Console Redirection Enable or Disable.
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. The item will be lunched before enable Console Redirection.
COM4	Info only	
Console Redirection	Enabled <b>Disabled</b>	Console Redirection Enable or Disable.
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. The item will be lunched before enable Console Redirection.
Serial Port for Out-of-Band Management Windows Emergency Management Services (EMS)	Info only	
Console Redirection	Disabled <b>Enabled</b>	Console Redirection Enable or Disable.
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.

• 3.2.8.1 Advanced > Serial Console Redirection > Console Redirection Settings (If COM1 Enable)

Feature	Options	Description
COM1	Info only	
Console Redirection Settings	Info only	
Terminal Type	VT100 VT100+ VT-UTF8 <b>ANSI</b>	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 <u>Unicode</u> chars onto 1 or more bytes.
Bits per second	9600 19200 38400 57600 <b>115200</b>	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	7 <b>8</b>	Data Bits
Parity	<b>None</b> Even Odd Mark Space	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the <u>num</u> of 1's in the data bits is even. Odd: parity bit is 0 if <u>num</u> of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection. They can be used as an additional data bit.
Stop Bits	1 2	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.
Flow Control	<b>None</b> Hardware RTS/CTS	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.
VT-UTF8 Combo Key Support	<b>Enabled</b> Disabled	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals
Recorder Mode	<b>Disabled</b> Enabled	With this mode enabled only text will be sent. This is to capture terminal data.
Resolution 100x31	Enabled <b>Disabled</b>	On Legacy OS, the Number of Rows and Columns supported redirection
Legacy OS Redirection Resolution	<b>80x24</b> 80x25	On Legacy OS, the Number of Rows and Columns supported redirection
Putty KeyPad	<b>VT100</b> Intel Linux XTERMR6 SCO ESCN VT400	Select FunctionKey and KeyPad on <u>Putty</u> .

Feature	Options	Description
Redirection After BIOS POST	<b>Always Enable</b> BootLoader	When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS. Default setting for this option is set to Always Enable.

• 3.2..2 Advanced > Serial Console Redirection > Console Redirection Settings (If COM2 Enable)

Feature	Options	Description
COM2	Info only	
Console Redirection Settings	Info only	
Terminal Type	VT100 VT100+ VT-UTF8 <b>ANSI</b>	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 <u>Unicode</u> chars onto 1 or more bytes.
Bits per second	9600 19200 38400 57600 <b>115200</b>	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	7 <b>8</b>	Data Bits
Parity	<b>None</b> Even Odd Mark Space	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the <u>num</u> of 1's in the data bits is even. Odd: parity bit is 0 if <u>num</u> of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection. They can be used as an additional data bit.
Stop Bits	1 2	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.
Flow Control	<b>None</b> Hardware RTS/CTS	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.
VT-UTF8 Combo Key Support	<b>Enabled</b> Disabled	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals
Recorder Mode	<b>Disabled</b> Enabled	With this mode enabled only text will be sent. This is to capture Terminal data.
Resolution 100x31	Enabled <b>Disabled</b>	On Legacy OS, the Number of Rows and Columns supported redirection
Legacy OS Redirection Resolution	<b>80x24</b> 80x25	On Legacy OS, the Number of Rows and Columns supported redirection

Feature	Options	Description
Putty KeyPad	<b>VT100</b> Intel Linux XTERMR6 SCO ESCN VT400	Select FunctionKey and KeyPad on <u>Putty</u> .
Redirection After BIOS POST	<b>Always Enable</b> BootLoader	When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS. Default setting for this option is set to Always Enable.

• 3.2.8.3 Advanced > Serial Console Redirection > Console Redirection Settings (If COM3 Enable)

Feature	Options	Description
COM3	Info only	
Console Redirection Settings	Info only	
Teriminal Type	VT100 VT100+ VT-UTF8 <b>ANSI</b>	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 <u>Unicode</u> chars onto 1 or more bytes.
Bits per second	9600 19200 38400 57600 <b>115200</b>	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	7 <b>8</b>	Data Bits
Parity	<b>None</b> Even Odd Mark Space	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the <u>num</u> of 1's in the data bits is even. Odd: parity bit is 0 if <u>num</u> of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection. They can be used as an additional data bit.
Stop Bits	1 2	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.
Flow Control	<b>None</b> Hardware RTS/CTS	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.
VT-UTF8 Combo Key Support	<b>Enabled</b> Disabled	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals
Recorder Mode	<b>Disabled</b> Enabled	With this mode enabled only text will be sent. This is to capture Terminal data.

Feature	Options	Description
Resolution 100x31	Enabled <b>Disabled</b>	On Legacy OS, the Number of Rows and Columns supported redirection
Legacy OS Redirection Resolution	<b>80x24</b> 80x25	On Legacy OS, the Number of Rows and Columns supported redirection
Putty KeyPad	<b>VT100</b> Intel Linux XTERMR6 SCO ESCN VT400	Select FunctionKey and KeyPad on <u>Putty</u> .
Redirection After BIOS POST	<b>Always Enable</b> BootLoader	When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS. Default setting for this option is set to Always Enable.

• 3.2.8.4 Advanced > Serial Console Redirection > Console Redirection Settings (If COM4 Enable)

Feature	Options	Description
COM4	Info only	
Console Redirection Settings	Info only	
Teriminal Type	VT100 VT100+ VT-UTF8 <b>ANSI</b>	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 <u>Unicode</u> chars onto 1 or more bytes.
Bits per second	9600 19200 38400 57600 <b>115200</b>	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	7 <b>8</b>	Data Bits
Parity	<b>None</b> Even Odd Mark Space	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the <u>num</u> of 1's in the data bits is even. Odd: parity bit is 0 if <u>num</u> of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection.They can be used as an additional data bit.
Stop Bits	1 2	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.
Flow Control	<b>None</b> Hardware RTS/CTS	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.

Feature	Options	Description
VT-UTF8 Combo Key Support	<b>Enabled</b> Disabled	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals
Recorder Mode	<b>Disabled</b> Enabled	With this mode enabled only text will be sent. This is to capture Terminal data.
Resolution 100x31	Enabled <b>Disabled</b>	On Legacy OS, the Number of Rows and Columns supported redirection
Legacy OS Redirection Resolution	<b>80x24</b> 80x25	On Legacy OS, the Number of Rows and Columns supported redirection
Putty KeyPad	<b>VT100</b> Intel Linux XTERMR6 SCO ESCN VT400	Select FunctionKey and KeyPad on <u>Putty</u> .
Redirection After BIOS POST	<b>Always Enable</b> BootLoader	When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS. Default setting for this option is set to Always Enable.

• 3.2.8.5 Advanced > Serial Console Redirection > Legacy Console Redirection Settings

Feature	Options	Description
Legacy Serial Redirection Port	<b>COM1</b> COM2 COM3 COM4	Select a COM port to display redirection of Legacy OS and Legacy OPRM Messages

• 3.2.9 Advanced > USB Configuration

Feature	Options	Description
USB Configuration	Info Only	
USB Module Version	Info Only	Display USB Module Version
USB Controllers:	Info Only	Display USB Controllers is XHCI or EHCI.
USB Devices:	Info Only	Display attachment USB devices.
Legacy USB Support	<b>Enabled</b> 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.
XHCI Hand-off	<b>Enabled</b> Disabled	This is a workaround for Oses without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
EHCI Hand-off	<b>Disabled</b> Enabled	This is a workaround for Oses without EHCI hand-off support. The EHCI ownership change should be claimed by EHCI driver.
USB Mass Storage Driver Support	Disabled <b>Enabled</b>	Enable / Disable USB Mass Storage Driver Support.

Feature	Options	Description
USB hardware delays and time-outs:	Info Only	
USB transfer time-out	1 sec 5sec 10sec <b>20 sec</b>	The time-out value for Control, Bulk, and Interrupt transfers.
Device reset time-out	10 sec <b>20 sec</b> 30 sec 40 sec	USB mass storage device Start Unit command time-out.
Device power-up delay	<b>Auto</b> Manual	Maximum time the device will take before it properly reports itself to the Hot Controller. 'Auto' uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub descriptor.

• 3.2.10 Advanced > Network Stack Configuration

Feature	Options	Description
Network Stack	<b>Disable</b> Enable	Enable / Disable UEFI Network Stack.

• 3.2.11 Advanced > Miscellaneous

Feature	Options	Description
Miscellaneous	Info Only	Control the PCI Express Root Port.
Smart Battery Function	<b>Disable</b> Enable	Enable / Disable Battery Function
I2C write protect control	Active <b>Write protect</b>	I2C write protect control
Above 4G Decoding	<b>Disabled</b> Enabled	Enables or Disables 64bit capable Devices to be Decode in Above 4G Address Space (Only if System supports 64 bit PCI Decoding).

• 3.2.12 Advanced > Driver Health

Feature	Options	Description
Driver Name	Info only	Provides Health Status for the Drivers / Controllers.

• 3.2.13 Advanced > Trusted Computing

Feature	Options	Description
TPM20 Device Found	Info Only	
Security Device Support	Disable <b>Enable</b>	Enables or Disable BIOS support for security device. OS will not show Security Device. TCG EFI protocol and available.
Active PCR banks	Info Only	
Feature	Options	Description
Available PCR banks	Info Only	
SHA-1 PCR Bank	Disabled <b>Enabled</b>	Enable or Disable SHA-1 PCR Bank
SHA256 PCR Bank	<b>Disabled</b> Enabled	Enable or Disable SHA256 PCR Bank
Pending operation	<b>None</b> TPM Clear	Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart inorder to change State of Security Device.
Platform hierarchy	Disable <b>Enable</b>	Enable or Disable Platform Hierarchy
Storage Hierarchy	Disable <b>Enable</b>	Enable or Disable Storage Hierarchy
Endorsement Hierarchy	Disable <b>Enable</b>	Enable or Disable Endorsement Hierarchy
TPM2.0 UEFI Spec Version	TCG_1_2 <b>TCG_2</b>	Select the TCG2 <u>Spec</u> Version Support, TCG_1_2: the Compatible mode for Win8/Win10, TCG_2: Support new TCG2 protocol and event format for Win10 or later
Physical Presence Spec Version	<b>1.2</b> 1.3	Select to Tell O.S. to support PPI Spec Version 1.2 or 1.3.  Note some HCK tests might not support 1.3.
TPM 20 Interface Type	Info only	
Device Select	TPM 1.2 TPM 2.0 <b>Auto</b>	PM 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 Chipset

#### • 3.3.1 Chipset > Processor Configuration

Feature	Options	Description
Processor Configuration	Info only	
Processor Socket	Info only	Display Processor Socket information
Processor ID	Info only	Display Processor Socket information
Processor Frequency	Info only	Display Processor Frequency information
Processor Max Ratio	Info only	Display Processor Max Ratio information
Processor Min Ratio	Info only	Display Processor Min Ratio information
Microcode Revision	Info only	Display Microcode Revision information
L1 Cache RAM	Info only	Display L1 Cache RAM information
L2 Cache RAM	Info only	Display L2 Cache RAM information
L3 Cache RAM	Info only	Display L3 Cache RAM information
Processor 0 Version	Info only	Display Processor 0 Version information
Hyper-Threading [ALL]	Disable <b>Enable</b>	Enable Hyper Threading (Software Method to Enable/Disable Logical Processor threads.)
Execute Disable Bit	Disable <b>Enable</b>	When disabled, forces the XD feature flag to always return 0.
Enable Intel TXT Support	<b>Disable</b> Enable	Enables Intel Trusted Execution Technology Configuration. Please disable "EV DFX Features" when TXT is enabled.
VMX	Disable <b>Enable</b>	Enables the Vanderpool Technology, takes effect after reboot.
Enable SMX	<b>Disable</b> Enable	Enable Safer Mode Extensions
Hardware Prefetcher	<b>Enable</b> Disable	= MLC Spatial Prefetcher (MSR 1A4h Bit[0])
Adjacent Cache Prefect	<b>Enable</b> Disable	= MLC Spatial Prefetcher (MSR 1A4h Bit[1])
X2APIC	<b>Disable</b> Enable	Enable/disable extended APIC support

#### • 3.3.2 Chipset > Advanced Power Management Configuration

Feature	Options	Description
Advanced Power Management Configuration	Info only	
EIST (P-states)	Disable <b>Enable</b>	When enabled, OS sets CPU frequency according load. When disabled, CPU frequency is set at max non-turbo.
Config TDP	<b>Disable</b> Enable	Option to disable/enable Config TDP

Feature	Options	Description
CPU P State Control	Submenu	Controls CPU frequency.
CPU C State Control	Submenu	Control CPU idle states
Long Pwr Limit Ovrd	<b>Disable</b>	Enable/Disable Long Term Power Limit override. If this option is disabled, BIOS will program the default values for Long Term Power Limit and Long Term Power Limit Time Window.
Long Dur Pwr Limit	<b>0</b>	Turbo Mode Long Duration Power Limit (aka Power Limit 1) in Watts. The value may vary from 0 to Fused Value. If the value is 0, the fused value will be programed. A value greater than fused TDP value will not be programed.
Long Dur Time Window	<b>1</b>	Long Duration Time Window (aka Power Limit 1 Time) value in seconds. The value may vary from 0 to 56. Indicates the time window over which TDP value should be maintained. If the value is 0, the fused value will be programed.

• 3.3.2.1 Chipset > Advanced Power Management Configuration > CPU P State Control

Feature	Options	Description
CPU P State Control	Info only	
P State Domain	<b>ALL</b> <b>ONE</b>	Per Logical: indicates the P-state domain for each logical proc in the system. Per Package: all procs indicate the same domain in the same package.
P-state coordination	<b>HW_ALL</b> <b>SW_ALL</b> <b>SW_ANY</b>	HW_ALL (hardware) coordination is recommended over SW_ALL and SW_ANY (software coordination).
Energy efficient P-state	Disable <b>Enable</b>	Enable/Disable Energy efficient P-state feature. When set to 0, will disable access to ENERGY_PERFORMANCE_BIAS MSR and CPUID Function6 EAX[3] will read 0 indicating nosupport
Boot performance mode	<b>Max Performance</b> Max Efficient	Select the performance state that the BIOS will set before OS handoff.
Turbo mode	Disable <b>Enable</b>	Turbo mode allows a CPU logical processor to execute a higher frequency when enough power is available not exceed CPU defined limits.

• 3.3.2.2 Chipset > Advanced Power Management Configuration > CPU C State Control

Feature	Options	Description
CPU C State Control	Info only	
C2C3TT	Info only	Display PCIE Port assigned to LAN Information.
CPU C State	Disable <b>Enable</b>	Enable the Enhanced Cx state of the CPU, takes effect after reboot.
Package C State limit	C0/C1 state C2 state C6(non Retention) state <b>C6(Retention) state</b> No Limit	Package C State limit

Feature	Options	Description
CPU C3 report	<b>Disable</b> Enable	Enable/Disable CPU C3(ACPI C2) report to OS. Recommended to be disabled.
CPU C6 report	Disable <b>Enable</b>	Enable/Disable CPU C6(ACPI C2) report to OS. Recommended to be enabled.
Enhanced Halt State (C1E)	Disable <b>Enable</b>	Enables the Enhanced C1E state of the CPU, takes effect after reboot.
OS ACPI Cx	<b>ACPI C2</b> ACPI C3	Report CC3/CC6 to OS ACPI C2 or ACPI C3

- 3.3.3 Chipset > Memory Configuration

Feature	Options	Description
Integrated Memory Controller (iMC)	Info only	
Memory Frequency	<b>Auto</b> 1333 1400 1600 1800 1867 2000 2133 2200 2400 2600 2667 2800 2933 3000 3200 Reserved	Maximum Memory Frequency Selections in Mhz. Do not select Reserved
Memory Topology	Submenu	Display memory information

- 3.3.4 Chipset > IIO Configuration

Feature	Options	Description
IIO Configuration	Info only	
PCIe Hot Plug	<b>Disable</b> Enable Auto MANUAL	Enable/Disable PCIe Hot Plug globally
PCIe ACPI Hot Plug	<b>Disable</b> Enable Per-port	Enable/Disable ACPI Hot Plug globally, or allow per-port control. When Disabled, MSI is generated on HP event. When Enabled, _HPGPE message is generated.
IIO0 Configuration	Submenu	
Intel VT for Directed I/O (VT-d)	Submenu	Press <Enter> to bring up the Intel VT for Directed I/O (VT-d) Configuration menu.

• 3.3.4.1 Chipset > IIO Configuration > IIO0 Configuration

Feature	Options	Description
IOU2 (IIO PCIe Port 1)	x4x4 x8 <b>Auto</b>	Select PCIe port Bifurcation for selected slot(s)
IOU1 (IIO PCIe Port 3)	x4x4x4x4 x4x4x8 x8x4x4 x8x8 x16 <b>Auto</b>	Select PCIe port Bifurcation for selected slot(s)
Socket 0 PcieD02F0 – Port 2A	Submenu	Settings related to PCI Express Ports (0/1A/1B/2A/2B/2C/2D/3A/3B/3C/3D)
Socket 0 PcieD02F2 – Port 2C	Submenu	Settings related to PCI Express Ports (0/1A/1B/2A/2B/2C/2D/3A/3B/3C/3D)
Socket 0 PcieD03F0 – Port 3A	Submenu	Settings related to PCI Express Ports (0/1A/1B/2A/2B/2C/2D/3A/3B/3C/3D)

Chipset > IIO Configuration > IIO0 Configuration > Socket 0 PcieD02F0 – Port 2A

Feature	Options	Description
Socket 0 PcieD02F0 – Port2A	Info only	
PCI-E Port	<b>Auto</b> Enable Disable	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Disable is used to disable the port and hide its CFG space.
Hot Plug Capable	<b>Disable</b> Enable	This option specifies if the link is considered Hot Plug capable.
PCI-E Port Link	<b>Enable</b> Disable	This option disables the link so that the no training occurs but the CFG space is still active.
Link Speed	<b>Auto</b> Gen1 (2.5 GT/s) Gen2 (5 GT/s) Gen3 (8 GT/s)	
Override Max Link Wid	<b>Auto</b> x1 x2 x4 x8 x16	Override the max link width that was set by bifurcation
PCI-E Port DeEmphasis	<b>-6.0 dB</b> -3.5 dB	De-Emphasis control (LNKCON2[6]) for this PCIe port.
PCI-E Port Link Status	Info only	
PCI-E Port Link Max	Info only	
PCI-E Port Link Speed	Info only	
PCI-E ASPM Support	Auto <b>Disable</b> L1 Only	This option enables / disables the ASPM (L1) support for the downstream devices.

Feature	Options	Description
Fatal Err Over	<b>Disable</b> Enable	Enables forcing fatal error propagation to the IIO core error logic for this port
Non-Fatal Err Over	<b>Disable</b> Enable	Enables forcing non-fatal error propagation to the IIO core error logic for this port
Corr Err Over	<b>Disable</b> Enable	Enables forcing correctable error propagation to the IIO core error logic for this port
L0s Support	<b>Disable</b>	When disabled, IIO never puts its transmitter in L0s state
PM ACPI Mode	<b>Disable</b> Enable	When Disabled, MSI is generated on PM event. When Enabled, _HPGPE message is generated
Gen3 Eq Mode	<b>Auto</b> Enable Phase 0,1,2,3 Disable Phase 0,1,2,3 Enable Phase 1 Only Enable Phase 0,1 Only Advanced Enable MMM Offset West Alt Short Channel	PCIe Gen3 Adaptive Equalization Mode
Gen3 Spec Mode	<b>Auto</b> 0.70 July • Sept • Sept	PCIe Gen3 Spec Mode
Gen3 Phase2 Mode	<b>Hardware Adaptive</b> Manual	
Gen3 DN Tx Present	<b>Auto</b> P0 (-6.0/0.0 dB) P1 (-3.5/0.0 dB) P2 (-4.5/0.0 dB) P3 (-2.5/0.0 dB) P4 (0.0/0.0 dB) P5 (0.0/2.0 dB) P6 (0.0/2.5 dB) P7 (-6.0/3.5 dB) P8 (-3.5/3.5 dB) P9 (0.0/3.5 dB)	PCIe Gen3 Downstream Tx Present
Gen3 DN Rx Preset Hint	<b>Auto</b> P0 ( -6.0 dB) P1 ( -7.0 dB) P2 ( -8.0 dB) P3 ( -9.0 dB) P4 ( -10.0 dB) P5 ( -11.0 dB) P6 ( -12.0 dB)	PCIe Gen3 Downstream Rx Present Hint
Gen3 UP Tx Preset	<b>Auto</b> P0 (-6.0/0.0 dB) P1 (-3.5/0.0 dB) P2 (-4.5/0.0 dB) P3 (-2.5/0.0 dB) P4 (0.0/0.0 dB) P5 (0.0/2.0 dB) P6 (0.0/2.5 dB)	PCIe Gen3 Upstream Tx Preset

Feature	Options	Description
	P7 (-6.0/3.5 dB) P8 (-3.5/3.5 dB) P9 (0.0/3.5 dB)	
Hide Port?	<b>no</b> yes	User can force to hide this root port from OS
Pcie Ecrc	Disable Enable <b>Auto</b>	Enable/Disable Pcie Ecrc Support for this port.

Chipset > IIO Configuration > IIO0 Configuration > Socket 0 PcieD02F2 – Port 2C

Feature	Options	Description
Socket 0 PcieD02F2 – Port 2C	Info only	
PCI-E Port	<b>Auto</b> Enable Disable	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Disable is used to disable the port and hide its CFG space.
Hot Plug Capable	<b>Disable</b> Enable	This option specifies if the link is considered Hot Plug capable.
PCI-E Port Link	<b>Enable</b> Disable	This option disables the link so that the no training occurs but the CFG space is still active.
Link Speed	<b>Auto</b> Gen1 (2.5 GT/s) Gen2 (5 GT/s) Gen3 (8 GT/s)	
Override Max Link Wid	<b>Auto</b> x1 x2 x4 x8 x16	Override the max link width that was set by bifurcation
PCI-E Port DeEmphasis	<b>-6.0 dB</b> -3.5 dB	De-Emphasis control (LNKCON2[6]) for this PCIe port.
PCI-E Port Link Status	Info only	
PCI-E Port Link Max	Info only	
PCI-E Port Link Speed	Info only	
PCI-E ASPM Support	Auto <b>Disable</b> L1 Only	This option enables / disables the ASPM (L1) support for the downstream devices.
Fatal Err Over	<b>Disable</b> Enable	Enables forcing fatal error propagation to the IIO core error logic for this port
Non-Fatal Err Over	<b>Disable</b> Enable	Enables forcing non-fatal error propagation to the IIO core error logic for this port
Corr Err Over	<b>Disable</b> Enable	Enables forcing correctable error propagation to the IIO core error logic for this port
L0s Support	<b>Disable</b>	When disabled, IIO never puts its transmitter in L0s state

Feature	Options	Description
PM ACPI Mode	<b>Disable</b> Enable	When Disabled, MSI is generated on PM event. When Enabled, _HPGPE message is generated
Gen3 Eq Mode	<b>Auto</b> Enable Phase 0,1,2,3 Disable Phase 0,1,2,3 Enable Phase 1 Only Enable Phase 0,1 Only Advanced Enable MMM Offset West Alt Short Channel	PCIe Gen3 Adaptive Equilization Mode
Gen3 Spec Mode	<b>Auto</b> 0.70 July <ul style="list-style-type: none"> <li>• Sept</li> <li>• Sept</li> </ul>	PCIe Gen3 Spec Mode
Gen3 Phase2 Mode	<b>Hardware Adaptive</b> Manual	
Gen3 DN Tx Present	<b>Auto</b> P0 (-6.0/0.0 dB) P1 (-3.5/0.0 dB) P2 (-4.5/0.0 dB) P3 (-2.5/0.0 dB) P4 (0.0/0.0 dB) P5 (0.0/2.0 dB) P6 (0.0/2.5 dB) P7 (-6.0/3.5 dB) P8 (-3.5/3.5 dB) P9 (0.0/3.5 dB)	PCIe Gen3 Downstream Tx Present
Gen3 DN Rx Preset Hint	<b>Auto</b> P0 ( -6.0 dB) P1 ( -7.0 dB) P2 ( -8.0 dB) P3 ( -9.0 dB) P4 ( -10.0 dB) P5 ( -11.0 dB) P6 ( -12.0 dB)	PCIe Gen3 Downstream Rx Present Hint
Gen3 UP Tx Preset	<b>Auto</b> P0 (-6.0/0.0 dB) P1 (-3.5/0.0 dB) P2 (-4.5/0.0 dB) P3 (-2.5/0.0 dB) P4 (0.0/0.0 dB) P5 (0.0/2.0 dB) P6 (0.0/2.5 dB) P7 (-6.0/3.5 dB) P8 (-3.5/3.5 dB) P9 (0.0/3.5 dB)	PCIe Gen3 Upstream Tx Preset
Hide Port?	<b>no</b> yes	User can force to hide this root port from OS
Pcie Ecrc	Disable Enable <b>Auto</b>	Enable/Disable Pcie Ecrc Support for this port.

Feature	Options	Description
Socket 0 PcieD03F0 – Port 3A	Info only	
PCI-E Port	<b>Auto</b> Enable Disable	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Disable is used to disable the port and hide its CFG space.
Hot Plug Capable	<b>Disable</b> Enable	This option specifies if the link is considered Hot Plug capable.
PCI-E Port Link	<b>Enable</b> Disable	This option disables the link so that the no training occurs but the CFG space is still active.
Link Speed	<b>Auto</b> Gen1 (2.5 GT/s) Gen2 (5 GT/s) Gen3 (8 GT/s)	
Override Max Link Wid	<b>Auto</b> x1 x2 x4 x8 x16	Override the max link width that was set by bifurcation
PCI-E Port DeEmphasis	<b>-6.0 dB</b> -3.5 dB	De-Emphasis control (LNKCON2[6]) for this PCIe port.
PCI-E Port Link Status	Info only	
PCI-E Port Link Max	Info only	
PCI-E Port Link Speed	Info only	
PCI-E ASPM Support	Auto <b>Disable</b> L1 Only	This option enables / disables the ASPM (L1) support for the downstream devices.
Fatal Err Over	<b>Disable</b> Enable	Enables forcing fatal error propagation to the IIO core error logic for this port
Non-Fatal Err Over	<b>Disable</b> Enable	Enables forcing non-fatal error propagation to the IIO core error logic for this port
Corr Err Over	<b>Disable</b> Enable	Enables forcing correctable error propagation to the IIO core error logic for this port
L0s Support	<b>Disable</b>	When disabled, IIO never puts its transmitter in L0s state
PM ACPI Mode	<b>Disable</b> Enable	When Disabled, MSI is generated on PM event. When Enabled, _HPGPE message is generated
Gen3 Eq Mode	<b>Auto</b> Enable Phase 0,1,2,3 Disable Phase 0,1,2,3 Enable Phase 1 Only Enable Phase 0,1 Only Advanced Enable MMM Offset West Alt Short Channel	PCIe Gen3 Adaptive Equalization Mode



Feature	Options	Description
Gen3 Spec Mode	<b>Auto</b> 0.70 July <ul style="list-style-type: none"> <li>• Sept</li> <li>• Sept</li> </ul>	PCIe Gen3 Spec Mode
Gen3 Phase2 Mode	<b>Hardware Adaptive</b> Manual	
Gen3 DN Tx Present	<b>Auto</b> P0 (-6.0/0.0 dB) P1 (-3.5/0.0 dB) P2 (-4.5/0.0 dB) P3 (-2.5/0.0 dB) P4 (0.0/0.0 dB) P5 (0.0/2.0 dB) P6 (0.0/2.5 dB) P7 (-6.0/3.5 dB) P8 (-3.5/3.5 dB) P9 (0.0/3.5 dB)	PCIe Gen3 Downstream Tx Present
Gen3 DN Rx Preset Hint	<b>Auto</b> P0 ( -6.0 dB) P1 ( -7.0 dB) P2 ( -8.0 dB) P3 ( -9.0 dB) P4 ( -10.0 dB) P5 ( -11.0 dB) P6 ( -12.0 dB)	PCIe Gen3 Downstream Rx Present Hint
Gen3 UP Tx Preset	<b>Auto</b> P0 (-6.0/0.0 dB) P1 (-3.5/0.0 dB) P2 (-4.5/0.0 dB) P3 (-2.5/0.0 dB) P4 (0.0/0.0 dB) P5 (0.0/2.0 dB) P6 (0.0/2.5 dB) P7 (-6.0/3.5 dB) P8 (-3.5/3.5 dB) P9 (0.0/3.5 dB)	PCIe Gen3 Upstream Tx Preset
Hide Port?	<b>no</b> yes	User can force to hide this root port from OS
Pcie Ecrc	Disable Enable <b>Auto</b>	Enable/Disable Pcie Ecrc Support for this port.

• 3.3.4.2 Chipset > IIO Configuration > Intel VT for Directed I/O (VT-d)

Feature	Options	Description
Intel VT for Directed I/O (VT-d)	Info	
VTd Azalea VCp Optimizations	<b>Disable</b> Enable	Enable/Disable Azalea VCp Optimizations
Intel VT for Directed	<b>Enable</b> Disable	Enable/Disable Intel Virtualization Technology for Directed I/O (VT-d) by reporting the I/O device assignment to VMM through DMAR ACPI Tables.

Feature	Options	Description
ACS Control	<b>Enable</b> Disable	Enable: Programs ACS only to Chipset Pcie Root Ports Bridges; Disable: Programs ACS to all Pcie bridges
Interrupt Remapping	<b>Enable</b> Disable	Enable/Disable VT_D Interrupt Remapping Support
Coherency Support (Non-Isoch)	<b>Enable</b> Disable	Enable/Disable Non-Isoch VT_D Engine Coherency support
Coherency Support (Isoch)	<b>Enable</b> Disable	Enable/Disable Isoch VT_D Engine Coherency support

• 3.3.5 Chipset > IIO Configuration

Feature	Options	Description
IIO Configuration	Info only	
PCIe Hot Plug	<b>Disable</b> Enable Auto MANUAL	Enable/Disable PCIe Hot Plug globally
PCIe ACPI Hot Plug	<b>Disable</b> Enable Per-port	Enable/Disable ACPI Hot Plug globally, or allow per-port control. When Disabled, MSI is generated on HP event. When Enabled, _HPGPE message is generated.
IIO0 Configuration	Submenu	
Intel VT for Directed I/O (VT-d)	Submenu	Press <Enter> to bring up the Intel VT for Directed I/O (VT-d) Configuration menu.

• 3.3.5.1 Chipset > IIO Configuration > IIO0 Configuration

Feature	Options	Description
IOU2 (IIO PCIe Port 1)	x4x4 x8 <b>Auto</b>	Select PCIe port Bifurcation for selected slot(s)
IOU1 (IIO PCIe Port 3)	x4x4x4x4 x4x4x8 x8x4x4 x8x8 x16 <b>Auto</b>	Select PCIe port Bifurcation for selected slot(s)
Socket 0 PcieD02F0 – Port 2A	Submenu	Settings related to PCI Express Ports (0/1A/1B/2A/2B/2C/2D/3A/3B/3C/3D)
Socket 0 PcieD02F2 – Port 2C	Submenu	Settings related to PCI Express Ports (0/1A/1B/2A/2B/2C/2D/3A/3B/3C/3D)
Socket 0 PcieD03F0 – Port 3A	Submenu	Settings related to PCI Express Ports (0/1A/1B/2A/2B/2C/2D/3A/3B/3C/3D)

Chipset > IIO Configuration > IIO0 Configuration > Socket 0 PcieD02F0 – Port 2A

Feature	Options	Description
Socket 0 PcieD02F0 – Port2A	Info only	
PCI-E Port	<b>Auto</b> Enable Disable	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Disable is used to disable the port and hide its CFG space.
Hot Plug Capable	<b>Disable</b> Enable	This option specifies if the link is considered Hot Plug capable.
PCI-E Port Link	<b>Enable</b> Disable	This option disables the link so that the no training occurs but the CFG space is still active.
Link Speed	<b>Auto</b> Gen1 (2.5 GT/s) Gen2 (5 GT/s) Gen3 (8 GT/s)	
Override Max Link Wid	<b>Auto</b> x1 x2 x4 x8 x16	Override the max link width that was set by bifurcation
PCI-E Port DeEmphasis	<b>-6.0 dB</b> -3.5 dB	De-Emphasis control (LNKCON2[6]) for this PCIe port.
PCI-E Port Link Status	Info only	
PCI-E Port Link Max	Info only	
PCI-E Port Link Speed	Info only	
PCI-E ASPM Support	Auto <b>Disable</b> L1 Only	This option enables / disables the ASPM (L1) support for the downstream devices.

Feature	Options	Description
Fatal Err Over	<b>Disable</b> Enable	Enables forcing fatal error propagation to the IIO core error logic for this port
Non-Fatal Err Over	<b>Disable</b> Enable	Enables forcing non-fatal error propagation to the IIO core error logic for this port
Corr Err Over	<b>Disable</b> Enable	Enables forcing correctable error propagation to the IIO core error logic for this port
L0s Support	<b>Disable</b>	When disabled, IIO never puts its transmitter in L0s state
PM ACPI Mode	<b>Disable</b> Enable	When Disabled, MSI is generated on PM event. When Enabled, _HPGPE message is generated
Gen3 Eq Mode	<b>Auto</b> Enable Phase 0,1,2,3 Disable Phase 0,1,2,3 Enable Phase 1 Only Enable Phase 0,1 Only Advanced Enable MMM Offset West Alt Short Channel	PCIe Gen3 Adaptive Equalization Mode
Gen3 Spec Mode	<b>Auto</b> 0.70 July <ul style="list-style-type: none"> <li>• Sept</li> <li>• Sept</li> </ul>	PCIe Gen3 Spec Mode
Gen3 Phase2 Mode	<b>Hardware Adaptive</b> Manual	
Gen3 DN Tx Present	<b>Auto</b> P0 (-6.0/0.0 dB) P1 (-3.5/0.0 dB) P2 (-4.5/0.0 dB) P3 (-2.5/0.0 dB) P4 (0.0/0.0 dB) P5 (0.0/2.0 dB) P6 (0.0/2.5 dB) P7 (-6.0/3.5 dB) P8 (-3.5/3.5 dB) P9 (0.0/3.5 dB)	PCIe Gen3 Downstream Tx Present
Gen3 DN Rx Preset Hint	<b>Auto</b> P0 ( -6.0 dB) P1 ( -7.0 dB) P2 ( -8.0 dB) P3 ( -9.0 dB) P4 ( -10.0 dB) P5 ( -11.0 dB) P6 ( -12.0 dB)	PCIe Gen3 Downstream Rx Present Hint
Gen3 UP Tx Preset	<b>Auto</b> P0 (-6.0/0.0 dB) P1 (-3.5/0.0 dB) P2 (-4.5/0.0 dB) P3 (-2.5/0.0 dB) P4 (0.0/0.0 dB) P5 (0.0/2.0 dB) P6 (0.0/2.5 dB)	PCIe Gen3 Upstream Tx Preset

Feature	Options	Description
	P7 (-6.0/3.5 dB) P8 (-3.5/3.5 dB) P9 (0.0/3.5 dB)	
Hide Port?	<b>no</b> yes	User can force to hide this root port from OS
Pcie Ecrc	Disable Enable <b>Auto</b>	Enable/Disable Pcie Ecrc Support for this port.

Chipset > IIO Configuration > IIO0 Configuration > Socket 0 PcieD02F2 – Port 2C

Feature	Options	Description
Socket 0 PcieD02F2 – Port 2C	Info only	
PCI-E Port	<b>Auto</b> Enable Disable	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Disable is used to disable the port and hide its CFG space.
Hot Plug Capable	<b>Disable</b> Enable	This option specifies if the link is considered Hot Plug capable.
PCI-E Port Link	<b>Enable</b> Disable	This option disables the link so that the no training occurs but the CFG space is still active.
Link Speed	<b>Auto</b> Gen1 (2.5 GT/s) Gen2 (5 GT/s) Gen3 (8 GT/s)	
Override Max Link Wid	<b>Auto</b> x1 x2 x4 x8 x16	Override the max link width that was set by bifurcation
PCI-E Port DeEmphasis	<b>-6.0 dB</b> -3.5 dB	De-Emphasis control (LNKCON2[6]) for this PCIe port.
PCI-E Port Link Status	Info only	
PCI-E Port Link Max	Info only	
PCI-E Port Link Speed	Info only	
PCI-E ASPM Support	Auto <b>Disable</b> L1 Only	This option enables / disables the ASPM (L1) support for the downstream devices.
Fatal Err Over	<b>Disable</b> Enable	Enables forcing fatal error propagation to the IIO core error logic for this port
Non-Fatal Err Over	<b>Disable</b> Enable	Enables forcing non-fatal error propagation to the IIO core error logic for this port
Corr Err Over	<b>Disable</b> Enable	Enables forcing correctable error propagation to the IIO core error logic for this port
L0s Support	<b>Disable</b>	When disabled, IIO never puts its transmitter in L0s state

Feature	Options	Description
PM ACPI Mode	<b>Disable</b> Enable	When Disabled, MSI is generated on PM event. When Enabled, _HPGPE message is generated
Gen3 Eq Mode	<b>Auto</b> Enable Phase 0,1,2,3 Disable Phase 0,1,2,3 Enable Phase 1 Only Enable Phase 0,1 Only Advanced Enable MMM Offset West Alt Short Channel	PCIe Gen3 Adaptive Equilization Mode
Gen3 Spec Mode	<b>Auto</b> 0.70 July <ul style="list-style-type: none"> <li>• Sept</li> <li>• Sept</li> </ul>	PCIe Gen3 Spec Mode
Gen3 Phase2 Mode	<b>Hardware Adaptive</b> Manual	
Gen3 DN Tx Present	<b>Auto</b> P0 (-6.0/0.0 dB) P1 (-3.5/0.0 dB) P2 (-4.5/0.0 dB) P3 (-2.5/0.0 dB) P4 (0.0/0.0 dB) P5 (0.0/2.0 dB) P6 (0.0/2.5 dB) P7 (-6.0/3.5 dB) P8 (-3.5/3.5 dB) P9 (0.0/3.5 dB)	PCIe Gen3 Downstream Tx Present
Gen3 DN Rx Preset Hint	<b>Auto</b> P0 ( -6.0 dB) P1 ( -7.0 dB) P2 ( -8.0 dB) P3 ( -9.0 dB) P4 ( -10.0 dB) P5 ( -11.0 dB) P6 ( -12.0 dB)	PCIe Gen3 Downstream Rx Present Hint
Gen3 UP Tx Preset	<b>Auto</b> P0 (-6.0/0.0 dB) P1 (-3.5/0.0 dB) P2 (-4.5/0.0 dB) P3 (-2.5/0.0 dB) P4 (0.0/0.0 dB) P5 (0.0/2.0 dB) P6 (0.0/2.5 dB) P7 (-6.0/3.5 dB) P8 (-3.5/3.5 dB) P9 (0.0/3.5 dB)	PCIe Gen3 Upstream Tx Preset
Hide Port?	<b>no</b> yes	User can force to hide this root port from OS
Pcie Ecrc	Disable Enable <b>Auto</b>	Enable/Disable Pcie Ecrc Support for this port.

Feature	Options	Description
Socket 0 PcieD03F0 – Port 3A	Info only	
PCI-E Port	<b>Auto</b> Enable Disable	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Disable is used to disable the port and hide its CFG space.
Hot Plug Capable	<b>Disable</b> Enable	This option specifies if the link is considered Hot Plug capable.
PCI-E Port Link	<b>Enable</b> Disable	This option disables the link so that the no training occurs but the CFG space is still active.
Link Speed	<b>Auto</b> Gen1 (2.5 GT/s) Gen2 (5 GT/s) Gen3 (8 GT/s)	
Override Max Link Wid	<b>Auto</b> x1 x2 x4 x8 x16	Override the max link width that was set by bifurcation
PCI-E Port DeEmphasis	<b>-6.0 dB</b> -3.5 dB	De-Emphasis control (LNKCON2[6]) for this PCIe port.
PCI-E Port Link Status	Info only	
PCI-E Port Link Max	Info only	
PCI-E Port Link Speed	Info only	
PCI-E ASPM Support	Auto <b>Disable</b> L1 Only	This option enables / disables the ASPM (L1) support for the downstream devices.
Fatal Err Over	<b>Disable</b> Enable	Enables forcing fatal error propagation to the IIO core error logic for this port
Non-Fatal Err Over	<b>Disable</b> Enable	Enables forcing non-fatal error propagation to the IIO core error logic for this port
Corr Err Over	<b>Disable</b> Enable	Enables forcing correctable error propagation to the IIO core error logic for this port
L0s Support	<b>Disable</b>	When disabled, IIO never puts its transmitter in L0s state
PM ACPI Mode	<b>Disable</b> Enable	When Disabled, MSI is generated on PM event. When Enabled, _HPGPE message is generated
Gen3 Eq Mode	<b>Auto</b> Enable Phase 0,1,2,3 Disable Phase 0,1,2,3 Enable Phase 1 Only Enable Phase 0,1 Only Advanced Enable MMM Offset West Alt Short Channel	PCIe Gen3 Adaptive Equalization Mode

Feature	Options	Description
Gen3 Spec Mode	<b>Auto</b> 0.70 July <ul style="list-style-type: none"> <li>• Sept</li> <li>• Sept</li> </ul>	PCIe Gen3 Spec Mode
Gen3 Phase2 Mode	<b>Hardware Adaptive</b> Manual	
Gen3 DN Tx Present	<b>Auto</b> P0 (-6.0/0.0 dB) P1 (-3.5/0.0 dB) P2 (-4.5/0.0 dB) P3 (-2.5/0.0 dB) P4 (0.0/0.0 dB) P5 (0.0/2.0 dB) P6 (0.0/2.5 dB) P7 (-6.0/3.5 dB) P8 (-3.5/3.5 dB) P9 (0.0/3.5 dB)	PCIe Gen3 Downstream Tx Present
Gen3 DN Rx Preset Hint	<b>Auto</b> P0 ( -6.0 dB) P1 ( -7.0 dB) P2 ( -8.0 dB) P3 ( -9.0 dB) P4 ( -10.0 dB) P5 ( -11.0 dB) P6 ( -12.0 dB)	PCIe Gen3 Downstream Rx Present Hint
Gen3 UP Tx Preset	<b>Auto</b> P0 (-6.0/0.0 dB) P1 (-3.5/0.0 dB) P2 (-4.5/0.0 dB) P3 (-2.5/0.0 dB) P4 (0.0/0.0 dB) P5 (0.0/2.0 dB) P6 (0.0/2.5 dB) P7 (-6.0/3.5 dB) P8 (-3.5/3.5 dB) P9 (0.0/3.5 dB)	PCIe Gen3 Upstream Tx Preset
Hide Port?	<b>no</b> yes	User can force to hide this root port from OS
Pcie Ecrc	Disable Enable <b>Auto</b>	Enable/Disable Pcie Ecrc Support for this port.

• 3.3.5.2 Chipset > IIO Configuration > Intel VT for Directed I/O (VT-d)

Feature	Options	Description
Intel VT for Directed I/O (VT-d)	Info	
VTd Azalea VCp Optimizations	<b>Disable</b> Enable	Enable/Disable Azalea VCp Optimizations
Intel VT for Directed	<b>Enable</b> Disable	Enable/Disable Intel Virtualization Technology for Directed I/O (VT-d) by reporting the I/O device assignment to VMM through DMAR ACPI Tables.



Feature	Options	Description
ACS Control	<b>Enable</b> Disable	Enable: Programs ACS only to Chipset Pcie Root Ports Bridges; Disable: Programs ACS to all Pcie bridges
Interrupt Remapping	<b>Enable</b> Disable	Enable/Disable VT_D Interrupt Remapping Support
Coherency Support (Non-Isoch)	<b>Enable</b> Disable	Enable/Disable Non-Isoch VT_D Engine Coherency support
Coherency Support (Isoch)	<b>Enable</b> Disable	Enable/Disable Isoch VT_D Engine Coherency support

### • 3.4 Security

#### • 3.4.1 Security > Password Description

Feature	Options	Description
Password Description	Info only	
Setup Administrator Password	Enter Password	Set Setup Administrator Password
User Password	Enter Password	Set User Password
Secure Boot	Submenu	Customizable Secure Boot settings.
System Mode	Info only	
Secure Boot	Info only	
Vender Keys	Info only	
Attempt Secure Boot	Disabled <b>Enabled</b>	Secure Boot activated when Platform Key(PK) is enrolled, System mode is User / Deployed, and CSM function is disabled
Secure Boot Mode	<b>Standard</b> Custom	Secure Boot Mode - Custom & Standard, Set UEFI Secure Boot Mode to STANDARD mode or CUSTOM mode, this change is effect after save. And after reset, the mode will return to STANDARD mode

### • 3.5 Boot

Feature	Options	Description
Boot Configuration	Info only	
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 Number state.
Quiet Boot	Disabled <b>Enabled</b>	Select the keyboard NumLock state.
Fast Boot	<b>Disabled</b> Enabled	Enable or Disable FastBoot features. Most probes are skipped to reduce time cost during boot.
New Boot Option Policy	<b>Default</b> Place First Place Last	Controls the placement of newly detected UEFI boot option.

#### • 3.5.1 Boot > FIXED BOOT ORDER Priorities

Feature	Options	Description
Boot Option #1	<b>Hardware</b>	Set the system boot order.
Boot Option #2	<b>CD/DVD</b>	Set the system boot order.
Boot Option #3	<b>USB Hard Disk</b>	Set the system boot order.
Boot Option #4	<b>USB CD/DVD</b>	Set the system boot order.
Boot Option #5	<b>USB Key</b>	Set the system boot order.
Boot Option #6	<b>USB Floppy</b>	Set the system boot order.
Boot Option #7	<b>USB Lan</b>	Set the system boot order.
Boot Option #8	<b>Network</b>	Set the system boot order.

### • 3.6 Save & Exit

Feature	Options	Description
Save Changes and Exit		Exit system setup after saving the changes.
Discard Changes and Exit		Exit system setup without saving any changes.
Save Change and Reset		Reset the system after saving the changes.
Discard Changes and Reset		Reset system setup without saving any changes.
Save Options	Info only	
Save Changes		Save Changes done so far to any of 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.
Boot Override	Info only	

## ►4. BIOS Checkpoints, Beep Codes

This section of this document lists checkpoints and beep codes generated by AMI Aptio BIOS. The checkpoints defined in this document are inherent to the AMIBIOS generic core, and do not include any chipset or board specific checkpoint definitions.

### Checkpoints and Beep Codes Definition

A checkpoint is either a byte or word value output to I/O port 80h. The BIOS outputs checkpoints throughout bootblock and Power-On Self Test (POST) to indicate the task the system is currently executing. Checkpoints are very useful for debugging problems that occur during the preboot process.

Beep codes are used by the BIOS to indicate a serious or fatal error. They are used when an error occurs before the system video has been initialized, and generated by the system board speaker.

### Aptio Boot Flow

While performing the functions of the traditional BIOS, Aptio 5.x core follows the firmware model described by the Intel Platform Innovation Framework for EFI ("the Framework"). The Framework refers the following "boot phases", which may apply to various status code & checkpoint descriptions:

- Security (SEC) – initial low-level initialization
- Pre-EFI Initialization (PEI) – memory initialization<sup>1</sup>
- Driver Execution Environment (DXE) – main hardware initialization<sup>2</sup>
  - Boot Device Selection (BDS) – system setup, pre-OS user interface & selecting a bootable device (CD/DVD, rHDD, USB, Network, Shell, ...)

### Viewing BIOS Checkpoints

Viewing all checkpoints generated by the BIOS requires a checkpoint card, also referred to as a <OST Card or POST Diagnostic Card. These are PCI add-in cards that show the value of I/O port 80h on a LED display.

Some computers display checkpoints in the bottom right corner of the screen during POST. This display method is limited, since it only displays checkpoints that occur after the video card has been activated.

Keep in mind that not all computers using AMI Aptio BIOS enable this feature. In most cases, a checkpoint card is the best tool for viewing AMI Aptio BIOS checkpoints.

<sup>1</sup>Analogous to "bootblock" functionality of legacy BIOS

<sup>2</sup>Analogous to "POST" functionality in legacy BIOS

#### • 4.1 Status Code Ranges

Status Code Range	Description
0x01 – 0x0B	SEC execution
0x0C – 0x0F	SEC errors
0x10 – 0x2F	PEI execution up to and including memory detection
0x30 – 0x4F	PEI execution after memory detection
0x50 – 0x5F	PEI errors
0x60 – 0x8F	DXE execution up to BDS
0x90 – 0xCF	BDS execution
0xD0 – 0xDF	DXE errors
0xE0 – 0xE8	S3 Resume (PEI)
0xE9 – 0xEF	S3 Resume errors (PEI)
0xF0 – 0xF8	Recovery (PEI)
0xF9 – 0xFF	Recovery errors (PEI)

#### • 4.1 Standard Status Codes

##### • 4.1.1 SEC Phase

Status Code	Description
0x00	Not used
<b>Progress Codes</b>	
0x01	Power on. Reset type detection (soft/hard).
0x02	AP initialization before microcode loading
0x03	North Bridge initialization before microcode loading
0x04	South Bridge initialization before microcode loading
0x05	OEM initialization before microcode loading
0x06	Microcode loading
0x07	AP initialization after microcode loading
0x08	North Bridge initialization after microcode loading
0x09	South Bridge initialization after microcode loading
0x0A	OEM initialization after microcode loading
0x0B	Cache initialization

SEC Error Codes	
0x0C – 0x0D	Reserved for future AMI SEC error codes
0x0E	Microcode not found
0x0F	Microcode not loaded

- 4.1.2 SEC Beep Codes

None

- 4.1.3 PEI Phase

Status Code	Description
<b>Progress Codes</b>	
0x10	PEI Core is started
0x11	Pre-memory CPU initialization is started
0x12	Pre-memory CPU initialization (CPU module specific)
0x13	Pre-memory CPU initialization (CPU module specific)
0x14	Pre-memory CPU initialization (CPU module specific)
0x15	Pre-memory North Bridge initialization is started
0x16	Pre-Memory North Bridge initialization (North Bridge module specific)
0x17	Pre-Memory North Bridge initialization (North Bridge module specific)
0x18	Pre-Memory North Bridge initialization (North Bridge module specific)
0x19	Pre-memory South Bridge initialization is started
0x1A	Pre-memory South Bridge initialization (South Bridge module specific)
0x1B	Pre-memory South Bridge initialization (South Bridge module specific)
0x1C	Pre-memory South Bridge initialization (South Bridge module specific)
0x1D – 0x2A	OEM pre-memory initialization codes
0x2B	Memory initialization. Serial Presence Detect (SPD) data reading
0x2C	Memory initialization. Memory presence detection
0x2D	Memory initialization. Programming memory timing information
0x2E	Memory initialization. Configuring memory
0x2F	Memory initialization (other).
0x30	Reserved for ASL (see ASL Status Codes section below)
0x31	Memory Installed
0x32	CPU post-memory initialization is started
0x33	CPU post-memory initialization. Cache initialization
0x34	CPU post-memory initialization. Application Processor(s) (AP) initialization

Status Code	Description
0x35	CPU post-memory initialization. Boot Strap Processor (BSP) selection
0x36	CPU post-memory initialization. System Management Mode (SMM) initialization
0x37	Post-Memory North Bridge initialization is started
0x38	Post-Memory North Bridge initialization (North Bridge module specific)
0x39	Post-Memory North Bridge initialization (North Bridge module specific)
0x3A	Post-Memory North Bridge initialization (North Bridge module specific)
0x3B	Post-Memory South Bridge initialization is started
0x3C	Post-Memory South Bridge initialization (South Bridge module specific)
0x3D	Post-Memory South Bridge initialization (South Bridge module specific)
0x3E	Post-Memory South Bridge initialization (South Bridge module specific)
0x3F-0x4E	OEM post memory initialization codes
0x4F	DXE IPL is started
<b>PEI Error Codes</b>	
0x50	Memory initialization error. Invalid memory type or incompatible memory speed
0x51	Memory initialization error. SPD reading has failed
0x52	Memory initialization error. Invalid memory size or memory modules do not match.
0x53	Memory initialization error. No usable memory detected
0x54	Unspecified memory initialization error.
0x55	Memory not installed
0x56	Invalid CPU type or Speed
0x57	CPU mismatch
0x58	CPU self test failed or possible CPU cache error
0x59	CPU micro-code is not found or micro-code update is failed
0x5A	Internal CPU error
0x5B	reset PPI is not available
0x5C-0x5F	Reserved for future AML error codes
<b>S3 Resume Progress Codes</b>	
0xE0	S3 Resume is started (S3 Resume PPI is called by the DXE IPL)
0xE1	S3 Boot Script execution
0xE2	Video repost
0xE3	OS S3 wake vector call
0xE4-0xE7	Reserved for future AML progress codes

Status Code	Description
S3 Resume Error Codes	
0xE8	S3 Resume Failed
0xE9	S3 Resume PPI not Found
0xEA	S3 Resume Boot Script Error
0xEB	S3 OS Wake Error
0xEC-0xEF	Reserved for future AML error codes
Recovery Progress Codes	
0xF0	Recovery condition triggered by firmware (Auto recovery)
0xF1	Recovery condition triggered by user (Forced recovery)
0xF2	Recovery process started
0xF3	Recovery firmware image is found
0xF4	Recovery firmware image is loaded
0xF5-0xF7	Reserved for future AML progress codes
Recovery Error Codes	
0xF8	Recovery PPI is not available
0xF9	Recovery capsule is not found
0xFA	Invalid recovery capsule
0xFB – 0xFF	Reserved for future AML error codes

- 4.1.4 PEI Beep Codes

# of Beeps	Description
1	Memory not Installed
1	Memory was installed twice (InstallPeiMemory routine in PEI Core called twice)
2	Recovery started
3	DXE IPL was not found
3	DXE Core Firmware Volume was not found
4	Recovery failed
4	S3 Resume failed
7	Reset PPI is not available

#### 4.1.5 DXE Status Codes

Status Code	Description
0x60	DXE Core is started
0x61	NVRAM initialization
0x62	Installation of the South Bridge Runtime Services
0x63	CPU DXE initialization is started
0x64	CPU DXE initialization (CPU module specific)
0x65	CPU DXE initialization (CPU module specific)
0x66	CPU DXE initialization (CPU module specific)
0x67	CPU DXE initialization (CPU module specific)
0x68	PCI host bridge initialization
0x69	North Bridge DXE initialization is started
0x6A	North Bridge DXE SMM initialization is started
0x6B	North Bridge DXE initialization (North Bridge module specific)
0x6C	North Bridge DXE initialization (North Bridge module specific)
0x6D	North Bridge DXE initialization (North Bridge module specific)
0x6E	North Bridge DXE initialization (North Bridge module specific)
0x6F	North Bridge DXE initialization (North Bridge module specific)
0x70	South Bridge DXE initialization is started
0x71	South Bridge DXE SMM initialization is started
0x72	South Bridge devices initialization
0x73	South Bridge DXE Initialization (South Bridge module specific)
0x74	South Bridge DXE Initialization (South Bridge module specific)
0x75	South Bridge DXE Initialization (South Bridge module specific)
0x76	South Bridge DXE Initialization (South Bridge module specific)
0x77	South Bridge DXE Initialization (South Bridge module specific)
0x78	ACPI module initialization
0x79	CSM initialization
0x7A – 0x7F	Reserved for future AMI DXE codes
0x80 – 0x8F	OEM DXE initialization codes
0x90	Boot Device Selection (BDS) phase is started
0x91	Driver connecting is started
0x92	PCI Bus initialization is started
0x93	PCI Bus Hot Plug Controller Initialization
0x94	PCI Bus Enumeration



Status Code	Description
0x95	PCI Bus Request Resources
0x96	PCI Bus Assign Resources
0x97	Console Output devices connect
0x98	Console input devices connect
0x99	Super IO Initialization
0x9A	USB initialization is started
0x9B	USB Reset
0x9C	USB Detect
0x9D	USB Enable
0x9E – 0x9F	Reserved for future AML codes
0xA0	IDE initialization is started
0xA1	IDE Reset
0xA2	IDE Detect
0xA3	IDE Enable
0xA4	SCSI initialization is started
0xA5	SCSI Reset
0xA6	SCSI Detect
0xA7	SCSI Enable
0xA8	Setup Verifying Password
0xA9	Start of Setup
0xAA	Reserved for ASL (see ASL Status Codes section below)
0xAB	Setup Input Wait
0xAC	Reserved for ASL (see ASL Status Codes section below)
0xAD	Ready To Boot event
0xAE	Legacy Boot event
0xAF	Exit Boot Services event
0xB0	Runtime Set Virtual Address MAP Begin
0xB1	Runtime Set Virtual Address MAP End
0xB2	Legacy Option ROM Initialization
0xB3	System Reset
0xB4	USB hot plug
0xB5	PCI bus hot plug
0xB6	Clean-up of NVRAM
0xB7	Configuration Reset (reset of NVRAM settings)

Status Code	Description
0xB8 – 0xBF	Reserved for future AML codes
0xC0 – 0xCF	OEM BDS initialization codes
<b>DXE Error Codes</b>	
0xD0	CPU initialization error
0xD1	North Bridge initialization error
0xD2	South Bridge initialization error
0xD3	Some of the Architectural Protocols are not available
0xD4	PCI resource allocation error. Out of Resources
0xD5	No Space for Legacy Option ROM
0xD6	No Console Output Devices are found
0xD7	No Console Input Devices are found
0xD8	Invalid password
0xD9	Error loading Boot Option (LoadImage returned error)
0xDA	Boot Option is failed (StartImage returned error)
0xDB	Flash update is failed
0xDC	Reset protocol is not available

- 4.1.6 DXE Beep Codes

# of Beeps	Description
1	Invalid password
4	Some of the Architectural Protocols are not available
5	No Console Output Devices are found
5	No Console Input Devices are found
6	Flash update is failed
7	Reset protocol is not available
8	Platform PCI resource requirements cannot be met

- 4.1.7 ACPI/ASL Checkpoint

Status Code	Description
0x01	System is entering S1 sleep state
0x02	System is entering S2 sleep state
0x03	System is entering S3 sleep state
0x04	System is entering S4 sleep state
0x05	System is entering S5 sleep state

Status Code	Description
0x10	System is waking up from the S1 sleep state
0x20	System is waking up from the S2 sleep state
0x30	System is waking up from the S3 sleep state
0x40	System is waking up from the S4 sleep state
0xAC	System has transitioned into ACPI mode. Interrupt controller is in PIC mode.
0xAA	System has transitioned into ACPI mode. Interrupt controller is in APIC mode.

#### 4.1 OEM-Reserved Checkpoint Ranges

Status Code	Description
0x05	OEM SEC initialization before microcode loading
0x0A	OEM SEC initialization after microcode loading
0x1D – 0x2A	OEM pre-memory initialization codes
0x3F – 0x4E	OEM PEI post memory initialization codes
0x80 – 0x8F	OEM DXE initialization codes
0xC0 – 0xCF	OEM BDS initialization codes

This page intentionally left blank

