

TGU9A2

COM Express Mini Module User's Manual

Copyright

This publication contains information that is protected by copyright. No part of it may be reproduced in any form or by any means or used to make any transformation/adaptation without the prior written permission from the copyright holders.

This publication is provided for informational purposes only. The manufacturer makes no representations or warranties with respect to the contents or use of this manual and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The user will assume the entire risk of the use or the results of the use of this document. Further, the manufacturer reserves the right to revise this publication and make changes to its contents at any time, without obligation to notify any person or entity of such revisions or changes.

Changes after the publication's first release will be based on the product's revision. The website will always provide the most updated information.

© 2021. All Rights Reserved.

Trademarks

Product names or trademarks appearing in this manual are for identification purpose only and are the properties of the respective owners.

COM Express Specification Reference

PICMG® COM Express® Module Base Specification.

<http://www.picmg.org/>

FCC and DOC Statement on Class B

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio TV technician for help.

Notice:

1. The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
2. Shielded interface cables must be used in order to comply with the emission limits.

Index

COM Express Specification Reference	2
FCC and DOC Statement on Class B	2
Static Electricity Precautions	4
Safety Measures	4
About the Package	5
Optional Items	5
Before Using the System Board	5

Chapter 1 - Introduction

Specifications	6
----------------------	---

Chapter 2 - Concept

COM Express Module Standards	7
TGU9A2 is a COM Express Mini. The dimension is 84mm x 55mm. ...	7

Chapter 3 - Hardware Installation

Board Layout	8
Block Diagram	9
System Memory	10
Connectors	11
COM Express Connector	11
COM Express Connector Signal Description	14
Cooling Option	20
Heat Sink	20
Installing TGU9A2 onto a Carrier Board	20
Installing the COM Express Debug Card	21
COMe-DEBUG	22

Chapter 4 - BIOS Setup

Overview	24
Default Configuration	24
Entering the BIOS Setup Utility	24
Legends	24
Scroll Bar	24
Submenu	24
AMI BIOS Setup Utility	25
Main	25
System Time	25
System Date	25
Advanced	25
CPU Configuration	26
Intel (VMX) Virtualization Technology	26
AVX	26
AVX3	26
Active Processor Cores	26

AES	26
Power & Performance	26
CPU - Power Management Control	26
GT - Power Management Control	26
PCIe Configuration	29
PCH-FW Configuration	29
Trusted Computing	30
IT8528 Super IO Configuration	31
Serial Port Console Redirection	31
ACPI Settings	33
Network Stack Configuration	35
CSM Configuration	35
NVMe Configuration	36
DFI EC HW Monitor	37
DFI WDT Configuration	38
Tls Auth Configuration	38
RAM Disk Configuration	39
System Agent (SA) Configuration	40
Memory Configuration	41
Graphics Configuration	41
VMD setup menu	42
PCI Express Configuration	43
PCI Express Root Port	43
PCIe Speed	43
SATA and RST Configuration	44
SATA Controller	44
SATA Speed	44
SATA Mode Selection	44
SATA Port 0 and 1/Hot Plug	44
Software Feature Mask Configuration	44
HDD Unlock	44
LED Locate	44
HD Audio Configuration	45
Audio Controller	45
Disable	45
Enable	45
Hybrid Storage Detection and Configuration Mode	45
Security	46
Boot	47
Setup Prompt Timeout	47
NumLock	47
Quiet Boot	47
Network Stack	47
Ipv4 PXE Support	47
Ipv6 PXE Support	47
Boot Option Priorities	47
Save & Exit	48
Exit Saving Changes	48
Updating the BIOS	49
Notice: BIOS SPI ROM	49

Warranty

1. Warranty does not cover damages or failures that arised from misuse of the product, inability to use the product, unauthorized replacement or alteration of components and product specifications.
2. The warranty is void if the product has been subjected to physical abuse, improper installation, modification, accidents or unauthorized repair of the product.
3. Unless otherwise instructed in this user's manual, the user may not, under any circumstances, attempt to perform service, adjustments or repairs on the product, whether in or out of warranty. It must be returned to the purchase point, factory or authorized service agency for all such work.
4. We will not be liable for any indirect, special, incidental or consequential damages to the product that has been modified or altered.

Static Electricity Precautions

It is quite easy to inadvertently damage your PC, system board, components or devices even before installing them in your system unit. Static electrical discharge can damage computer components without causing any signs of physical damage. You must take extra care in handling them to ensure against electrostatic build-up.

1. To prevent electrostatic build-up, leave the system board in its anti-static bag until you are ready to install it.
2. Wear an antistatic wrist strap.
3. Do all preparation work on a static-free surface.
4. Hold the device only by its edges. Be careful not to touch any of the components, contacts or connections.
5. Avoid touching the pins or contacts on all modules and connectors. Hold modules or connectors by their ends.



Important:

Electrostatic discharge (ESD) can damage your processor, disk drive and other components. Perform the upgrade instruction procedures described at an ESD workstation only. If such a station is not available, you can provide some ESD protection by wearing an antistatic wrist strap and attaching it to a metal part of the system chassis. If a wrist strap is unavailable, establish and maintain contact with the system chassis throughout any procedures requiring ESD protection.

Safety Measures

To avoid damage to the system:

- Use the correct AC input voltage range.

To reduce the risk of electric shock:

- Unplug the power cord before removing the system chassis cover for installation or servicing. After installation or servicing, cover the system chassis before plugging the power cord.

About the Package

The package contains the following items. If any of these items are missing or damaged, please contact your dealer or sales representative for assistance.

- 1 TGU9A2 board

Optional Items

The board and accessories in the package may not come similar to the information listed above. This may differ in accordance with the sales region or models in which it was sold. For more information about the standard package in your region, please contact your dealer or sales representative.

Before Using the System Board

Before using the system board, prepare basic system components.

If you are installing the system board in a new system, you will need at least the following internal components.

- Storage devices such as hard disk drive, etc.

You will also need external system peripherals you intend to use which will normally include at least a keyboard, a mouse and a video display monitor.

Chapter 1 - Introduction

Specifications

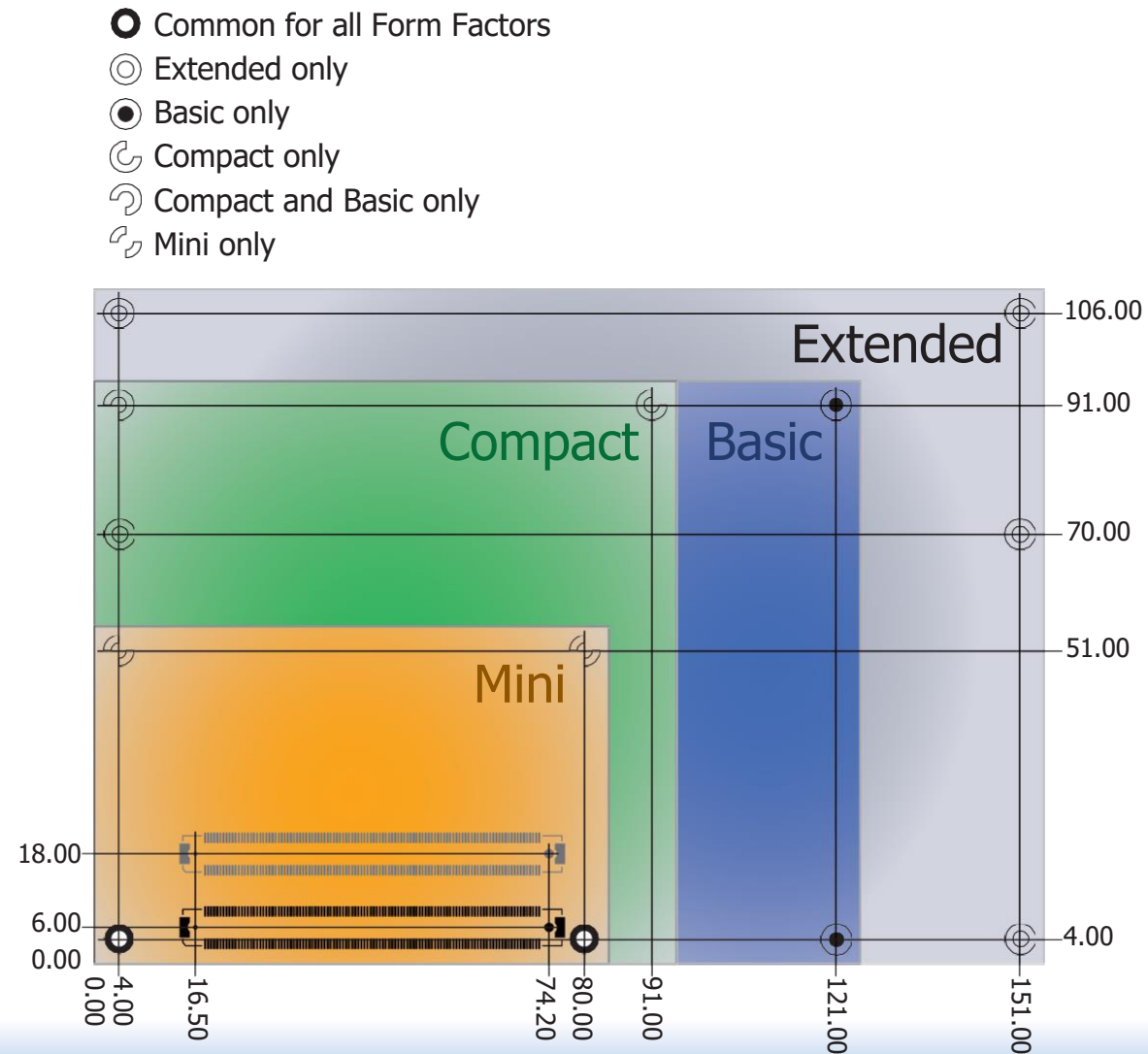
SYSTEM	Processor	Intel® Core™ i7-1185G7E Processor (Core 4; Max speed 2.8 GHz; TDP 15- 28W) Intel® Core™ i7-1185GRE Processor (Core 4; Max speed 2.8 GHz; TDP 15- 28W) Intel® Core™ i5-1145G7E Processor (Core 4; Max speed 2.6 GHz; TDP 15- 28W) Intel® Core™ i5-1145GRE Processor (Core 4; Max speed 2.6 GHz; TDP 15- 28W) Intel® Core™ i3-1115G4E Processor (Core 2; Max speed 3.0 GHz; TDP 15- 28W) Intel® Core™ i3-1115GRE Processor (Core 2; Max speed 3.0 GHz; TDP 15- 28W) Intel® Celeron® 6305RE Processor (Core 2; Max speed 1.8 GHz; TDP 15W)
	Memory	Memory Down up to 16GB Single Channel LPDDR4X 4266MHz
	BIOS	AMI SPI 256Mbit
GRAPHICS	Controller	Intel® Iris® Xe graphics
	Feature	OpenGL 5.0, DirectX 12, OpenCL 2.1 HW Decode: WMV9, AVC/H264, JPEG/MJPEG, HEVC/H265, VP9, AV1 HW Encode: AVC/H264, JPEG, HEVC/H265, VP9
	Display	1 x DDI (HDMI/DVI/DP++) 1 x eDP eDP: resolution up to 3840x2160@60Hz HDMI: resolution up to 3840x2160@30Hz DP++: resolution up to 4096x2160 @ 60Hz
	Dual Display	DDI + eDP
EXPANSION	Interface	1 x PCIe x4 (Gen 3) 1 x I2C 1 x SMBus 2 x SPI 2 x UART (TX/RX)
AUDIO	Interface	HD Audio
ETHERNET	Controller	1 x Intel® Ethernet I225IT (10/100/1000Mbps/2.5GbE)
I/O	USB	2 x USB 3.2 Gen.2 8 x USB 2.0
	NVMe SSD	1 x 128GB/256GB/512GB/1024GB on board SSD (available upon request)
	SATA	2 x SATA 3.0 (up to 6Gb/s)
	DIO	1 x 8-bit DIO
WATCHDOG TIMER	Output & Interval	System Reset, Programmable via Software from 1 to 255 Seconds
SECURITY	TPM	BIOS default support FTPM, TPM2.0 by request.
POWER	Type	4.75V~20V, 5VSB, VCC_RTC (ATX mode) / 4.75V~20V, VCC_RTC (AT mode)
OS SUPPORT (UEFI ONLY)		Windows: Windows 10 IoT Enterprise 64-bit Linux
ENVIRONMENT	Temperature	Operating: -5 to 65°C, -40 to 85°C / Storage: -40 to 85°C
	Humidity	Operating: 10 to 90% RH / Storage: 10 to 90% RH
CERTIFICATIONS	Certification	CE, FCC, RoHS
MECHANICAL	Dimensions	COM Express® Mini 84mm (3.30") x 55mm (2.16")
	Compliance	PICMG COM Express® R2.1, Type 10

Chapter 2 - Concept

COM Express Module Standards

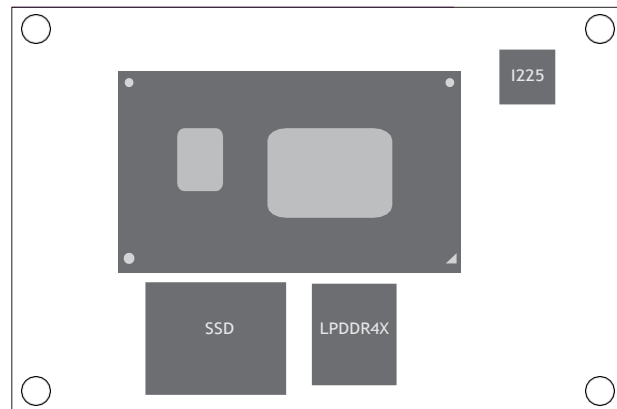
The figure below shows the dimensions of the different types of COM Express modules.

TGU9A2 is a COM Express Mini. The dimension is 84mm x 55mm.

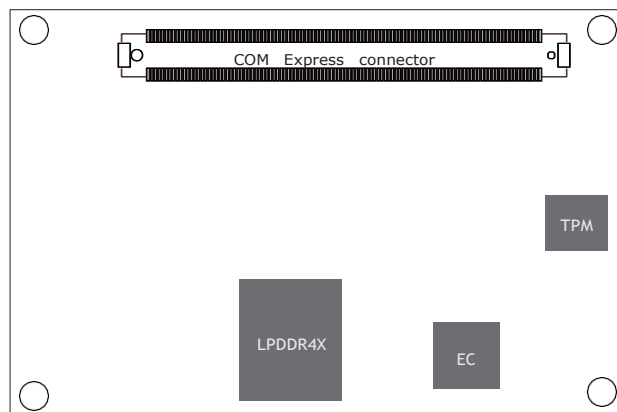


Chapter 3 - Hardware Installation

Board Layout

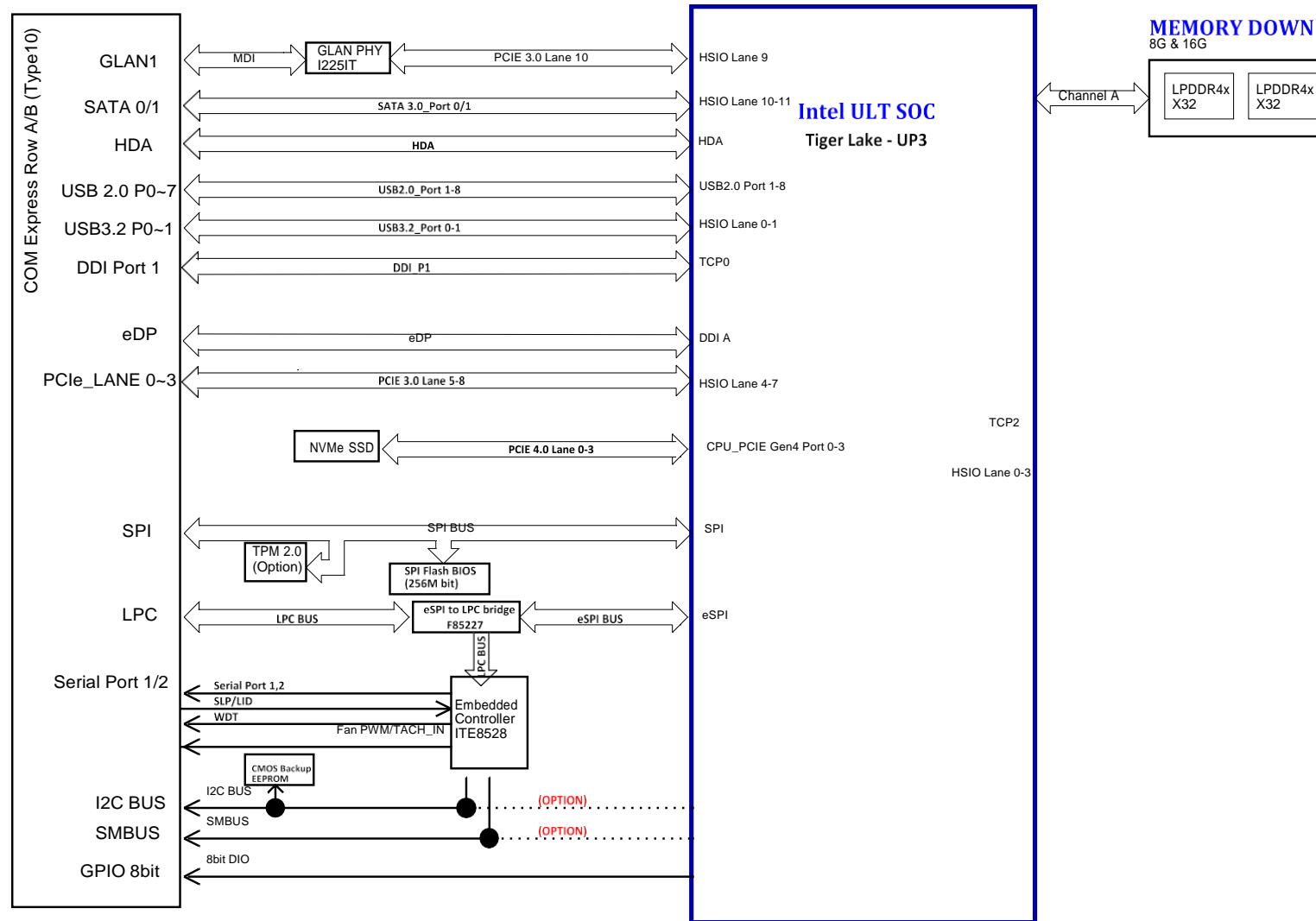


TOP



BOTTOM

Block Diagram

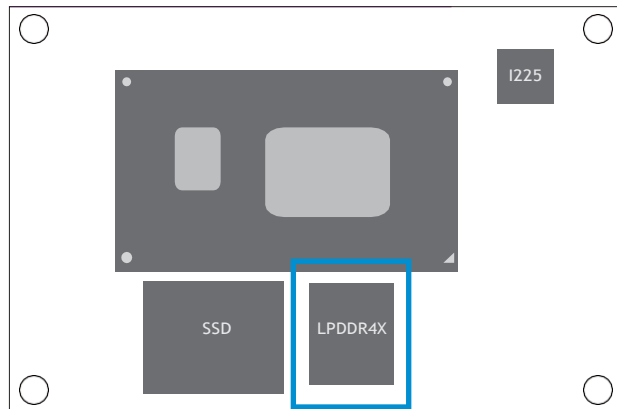




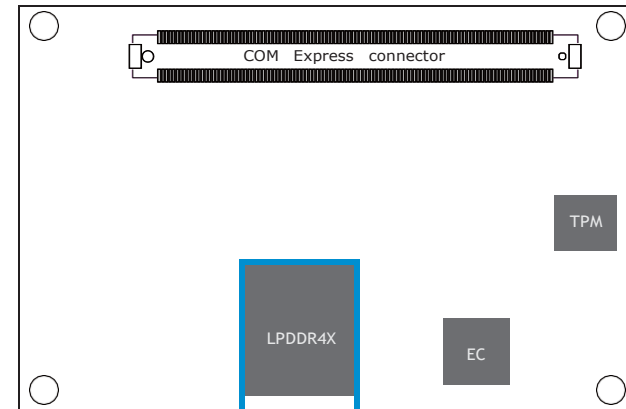
Electrostatic discharge (ESD) can damage your board, processor, disk drives, add-in boards, and other components. Perform installation procedures at an ESD workstation only. If such a station is not available, you can provide some ESD protection by wearing an antistatic wrist strap and attaching it to a metal part of the system chassis. If a wrist strap is unavailable, establish and maintain contact with the system chassis throughout any procedures requiring ESD protection.

System Memory

The system board is equipped with 2 LPDDR4X memory chips onboard.



Top View

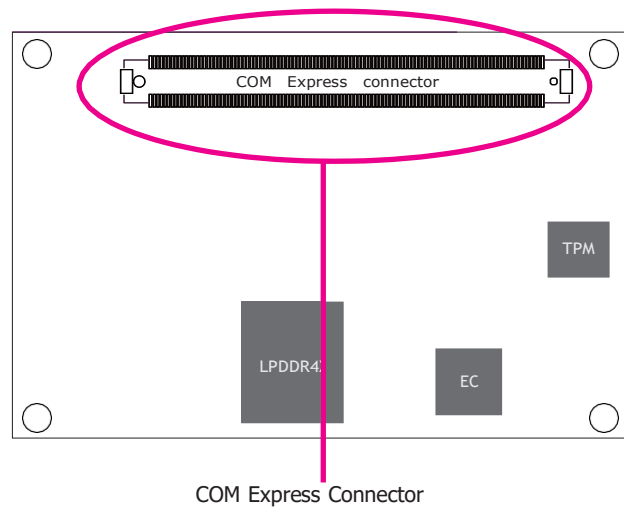


Bottom View

Connectors

COM Express Connector

The COM Express connector is used to interface the TGU9A2 COM Express board to a carrier board. Connect the COM Express connector (located on the solder side of the board) to the COM Express connector on the carrier board.



Refer to the following pages for the pin functions of the connector.

COM Express Connector

Row A		Row B	
A1	GND	B1	GND
A2	GBE_MDI3-	B2	GBE_ACT# / 3.3V Suspend
A3	GBE_MDI3+	B3	LPC_FRAME#
A4	Note*GBE_LED_100- / 3.3V Suspend	B4	LPC_AD0
A5	Note**GBE_LED_1000- / 3.3V Suspend	B5	LPC_AD1
A6	GBE_MDI2-	B6	LPC_AD2
A7	GBE_MDI2+	B7	LPC_AD3
A8	GBE_LED_LINK- / 3.3V Suspend	B8	LPC_DRQ0#
A9	GBE_MDI1-	B9	LPC_DRQ1#
A10	GBE_MDI1+	B10	LPC_CLK
A11	GND	B11	GND
A12	GBE_MDI0-	B12	PWRBTN# / 3.3V Suspend
A13	GBE_MDI0+	B13	SMB_CK / 3.3V Suspend
A14	NA	B14	SMB_DAT / 3.3V Suspend
A15	SUS_S3#	B15	SMB_ALERT# / 3.3V Suspend
A16	SATA0_TX+	B16	SATA1_TX+
A17	SATA0_TX-	B17	SATA1_TX-
A18	SUS_S4#	B18	SUS_STAT#
A19	SATA0_RX+	B19	SATA1_RX+
A20	SATA0_RX-	B20	SATA1_RX-
A21	GND	B21	GND
A22	USB_SSRX0-	B22	USB_SSTX0-
A23	USB_SSRX0+	B23	USB_SSTX0+
A24	SUS_S5#	B24	PWR_OK
A25	USB_SSRX1-	B25	USB_SSTX1-
A26	USB_SSRX1+	B26	USB_SSTX1+
A27	BATLOW# / Pull up 4.7kohm to 3.3V Suspend	B27	WDT / Pull up 10k ohm to 3.3V
A28	ATA_ACT# / Pull up 10kohm to 3.3V Suspend	B28	NA
A29	AC/HDA_SYNC / 3.3V Suspend	B29	NA
A30	AC/HDA_RST# / 3.3V Suspend	B30	AC/HDA_SDIN0

Row A		Row B	
A31	GND	B31	GND
A32	AC/HDA_BITCLK / 3.3V Suspend	B32	SPKR
A33	AC/HDA_SDOUT / 3.3V Suspend	B33	I2C_CK / 3.3V Suspend
A34	BIOS_DIS0#	B34	I2C_DAT / 3.3V Suspend
A35	THRMTRIP# / 3.3V Suspend	B35	THRM#
A36	USB6-	B36	USB7-
A37	USB6+	B37	USB7+
A38	USB_6_7_OC# / 3.3V Suspend	B38	USB_4_5_OC# / 3.3V Suspend
A39	USB4-	B39	USB5-
A40	USB4+	B40	USB5+
A41	GND	B41	GND
A42	USB2-	B42	USB3-
A43	USB2+	B43	USB3+
A44	USB_2_3_OC# / 3.3V Suspend	B44	USB_0_1_OC# / 3.3V Suspend
A45	USB0-	B45	USB1-
A46	USB0+	B46	USB1+
A47	VCC_RTC	B47	EXCD1_PERST#
A48	EXCD0_PERST#	B48	EXCD1_CPPE#
A49	EXCD0_CPPE#	B49	SYS_RESET# / Pull up to 3.3V Suspend
A50	LPC_SERIRQ	B50	CB_RESET# / Pull up to 3.3V Suspend
A51	GND	B51	GND
A52	NC (Option I2C_CLK_EC)	B52	NC (Option COMe_GPI5)
A53	NC (Option I2C_DATA_EC)	B53	NC (Option COMe_GPO5)
A54	GPI0	B54	GPO1
A55	NC (Option COMe_GPI4)	B55	NC (Option COMe_GPI6)
A56	NC (Option COMe_GPO4)	B56	NC (Option COMe_GPO6)
A57	GND	B57	GPO2
A58	PCIE_TX3+	B58	PCIE_RX3+
A59	PCIE_TX3-	B59	PCIE_RX3-
A60	GND	B60	GND

Row A		Row B	
A61	PCIE_TX2+	B61	PCIE_RX2+
A62	PCIE_TX2-	B62	PCIE_RX2-
A63	GPI1	B63	GPO3
A64	PCIE_TX1+	B64	PCIE_RX1+
A65	PCIE_TX1-	B65	PCIE_RX1-
A66	GND	B66	WAKE0#
A67	GPI2	B67	WAKE1#
A68	PCIE_TX0+	B68	PCIE_RX0+
A69	PCIE_TX0-	B69	PCIE_RX0-
A70	GND	B70	GND
A71	eDP_TX2+	B71	DDIO_PAIR0+
A72	eDP_TX2-	B72	DDIO_PAIR0-
A73	eDP_TX1+	B73	DDIO_PAIR1+
A74	eDP_TX1-	B74	DDIO_PAIR1-
A75	eDP_TX0+	B75	DDIO_PAIR2+
A76	eDP_TX0-	B76	DDIO_PAIR2-
A77	eDP_VDD_EN	B77	NA
A78	NC	B78	NA
A79	NC	B79	eDP_BKLT_EN
A80	GND	B80	GND
A81	eDP_TX3+	B81	DDIO_PAIR3+
A82	eDP_TX3-	B82	DDIO_PAIR3-
A83	eDP_AUX+	B83	eDP_BKLT_CTRL
A84	eDP_AUX-	B84	VCC_5V_SBY
A85	GPI3	B85	VCC_5V_SBY
A86	NA	B86	VCC_5V_SBY
A87	eDP_HPD	B87	VCC_5V_SBY
A88	PCIE0_CLK_REF+	B88	BIOS_DIS1#
A89	PCIE0_CLK_REF-	B89	DD0_HPD
A90	GND	B90	GND

Row A		Row B	
A91	SPI_POWER / 3.3V Suspend	B91	NA
A92	SPI_MISO / 3.3V Suspend	B92	NA
A93	GPO0	B93	NA
A94	SPI_CLK / 3.3V Suspend	B94	NA
A95	SPI_MOSI / 3.3V Suspend	B95	DDIO_DDC_AUX_SEL
A96	NA	B96	NC / USB_HOST_PRSNT 3.3V (option)
A97	TYPE10# / Pull down 47k ohm to GND	B97	SPI_CS# / 3.3V Suspend
A98	SER0_TX	B98	DDIO_CTRLCLK_AUX+
A99	SER0_RX	B99	DDIO_CTRLDATA_AUX-
A100	GND	B100	GND
A101	SER1_TX	B101	FAN_PWMOUT
A102	SER1_RX	B102	FAN_TACHIN
A103	LID#	B103	SLEEP#
A104	VCC	B104	VCC
A105	VCC	B105	VCC
A106	VCC	B106	VCC
A107	VCC	B107	VCC
A108	VCC	B108	VCC
A109	VCC	B109	VCC
A110	GND	B110	GND

Note:



1. *GBE_LED_100# is active during a 1Gb connection.
2. **GBE_LED_1000# is active during a 2.5Gb connection.

COM Express Connector Signal Description

Pin Types
 I Input to the Module
 O Output from the Module
 I/O Bi-directional input / output signal
 OD Open drain output

AC97/HDA Signals Descriptions

Signal	Pin#	Pin Type	Pwr Rail /Tolerance	TGU9A2	Carrier Board	Description
AC/HDA_RST#	A30	O CMOS	3.3V Suspend/3.3V		Connect to CODEC pin 11 RESET#	Reset output to CODEC, active low.
AC/HDA_SYNC	A29	O CMOS	3.3V/3.3V		Connect to CODEC pin 10 SYNC	Sample-synchronization signal to the CODEC(s).
AC/HDA_BITCLK	A32	I/O CMOS	3.3V/3.3V		Connect to CODEC pin 6 BIT_CLK	Serial data clock generated by the external CODEC(s).
AC/HDA_SDOUT	A33	O CMOS	3.3V/3.3V		Connect to CODEC pin 5 SDATA_OUT	Serial TDM data output to the CODEC.
AC/HDA_SDIN2	B28	I/O CMOS	3.3V Suspend/3.3V		Connect 33 Ω in series to CODEC2 pin 8 SDATA_IN	Serial TDM data inputs from up to 3 CODECs.
AC/HDA_SDIN1	B29	I/O CMOS	3.3V Suspend/3.3V		Connect 33 Ω in series to CODEC1 pin 8 SDATA_IN	
AC/HDA_SDIN0	B30	I/O CMOS	3.3V Suspend/3.3V		Connect 33 Ω in series to CODEC0 pin 8 SDATA_IN	

Gigabit Ethernet Signals Descriptions

Signal	Pin#	Pin Type	Pwr Rail /Tolerance	TGU9A2	Carrier Board	Description
GBE0_MDI0+	A13	I/O Analog	3.3V max Suspend		Connect to Magnetics Module MDI0+/-	Gigabit Ethernet Controller 0: Media Dependent Interface Differential Pairs 0,1,2,3. The MDI can operate in 1000, 100 and 10 Mbit / sec modes. Some pairs are unused in some modes, per the following: 1000BASE-T 100BASE-TX 10BASE-T MDI[0]+/- B1_DA+/- TX+/- TX+/- MDI[1]+/- B1_DB+/- RX+/- RX+/- MDI[2]+/- B1_DC+/- MDI[3]+/- B1_DD+/-
GBE0_MDI0-	A12	I/O Analog	3.3V max Suspend		Connect to Magnetics Module MDI1+/-	
GBE0_MDI1+	A10	I/O Analog	3.3V max Suspend			
GBE0_MDI1-	A9	I/O Analog	3.3V max Suspend		Connect to Magnetics Module MDI2+/-	
GBE0_MDI2+	A7	I/O Analog	3.3V max Suspend			
GBE0_MDI2-	A6	I/O Analog	3.3V max Suspend		Connect to Magnetics Module MDI3+/-	
GBE0_MDI3+	A3	I/O Analog	3.3V max Suspend			
GBE0_MDI3-	A2	I/O Analog	3.3V max Suspend			
GBE0_ACT#	B2	OD CMOS	3.3V Suspend/3.3V		Connect to LED and recommend current limit resistor 150Ω to 3.3VSB	Gigabit Ethernet Controller 0 activity indicator, active low.
GBE0_LINK#	A8	OD CMOS	3.3V Suspend/3.3V		NC	Gigabit Ethernet Controller 0 link indicator, active low.
GBE0_LINK100#	A4	OD CMOS	3.3V Suspend/3.3V	LED for link speed with 1Gbps	Connect to LED and recommend current limit resistor 150Ω to 3.3VSB	Gigabit Ethernet Controller 0 100 Mbit / sec link indicator, active low.
GBE0_LINK1000#	A5	OD CMOS	3.3V Suspend/3.3V	LED for link speed with 2.5Gbps	Connect to LED and recommend current limit resistor 150Ω to 3.3VSB	Gigabit Ethernet Controller 0 1000 Mbit / sec link indicator, active low.

SATA Signals Descriptions

Signal	Pin#	Pin Type	Pwr Rail /Tolerance	TGU9A2	Carrier Board	Description
SATA0_TX+	A16	O SATA	AC coupled on Module	AC Coupling capacitor	Connect to SATA0 Conn TX pin	Serial ATA or SAS Channel 0 transmit differential pair.
SATA0_TX-	A17	O SATA	AC coupled on Module	AC Coupling capacitor		
SATA0_RX+	A19	I SATA	AC coupled on Module	AC Coupling capacitor	Connect to SATA0 Conn RX pin	Serial ATA or SAS Channel 0 receive differential pair.
SATA0_RX-	A20	I SATA	AC coupled on Module	AC Coupling capacitor		
SATA1_TX+	B16	O SATA	AC coupled on Module	AC Coupling capacitor	Connect to SATA1 Conn TX pin	Serial ATA or SAS Channel 1 transmit differential pair.
SATA1_TX-	B17	O SATA	AC coupled on Module	AC Coupling capacitor		
SATA1_RX+	B19	I SATA	AC coupled on Module	AC Coupling capacitor	Connect to SATA1 Conn RX pin	Serial ATA or SAS Channel 1 receive differential pair.
SATA1_RX-	B20	I SATA	AC coupled on Module	AC Coupling capacitor		
ATA_ACT#	A28	I/O CMOS	3.3V / 3.3V	PU 4.7K to 3.3V Suspend	Connect to LED and recommend current limit resistor 220 Ω to 3.3V	ATA (parallel and serial) or SAS activity indicator, active low.

PCI Express Lanes Signals Descriptions

Signal	Pin#	Pin Type	Pwr Rail /Tolerance	TGU9A2	Carrier Board	Description
PCIE_TX0+	A68	O PCIE	AC coupled on Module	AC Coupling capacitor	Connect to PCIE device or slot	PCI Express Differential Transmit Pairs 0
PCIE_TX0-	A69			AC Coupling capacitor		
PCIE_RX0+	B68	I PCIE	AC coupled off Module		Device - Connect AC Coupling cap 0.1uF Slot - Connect to PCIE Conn pin	PCI Express Differential Receive Pairs 0
PCIE_RX0-	B69					
PCIE_TX1+	A64	O PCIE	AC coupled on Module	AC Coupling capacitor	Connect to PCIE device or slot	PCI Express Differential Transmit Pairs 1
PCIE_TX1-	A65			AC Coupling capacitor		
PCIE_RX1+	B64	I PCIE	AC coupled off Module		Device - Connect AC Coupling cap 0.1uF Slot - Connect to PCIE Conn pin	PCI Express Differential Receive Pairs 1
PCIE_RX1-	B65					
PCIE_TX2+	A61	O PCIE	AC coupled on Module	AC Coupling capacitor	Connect to PCIE device or slot	PCI Express Differential Transmit Pairs 2
PCIE_TX2-	A62			AC Coupling capacitor		
PCIE_RX2+	B61	I PCIE	AC coupled off Module		Device - Connect AC Coupling cap 0.1uF Slot - Connect to PCIE Conn pin	PCI Express Differential Receive Pairs 2
PCIE_RX2-	B62					
PCIE_TX3+	A58	O PCIE	AC coupled on Module	AC Coupling capacitor	Connect to PCIE device or slot	PCI Express Differential Transmit Pairs 3
PCIE_TX3-	A59			AC Coupling capacitor		
PCIE_RX3+	B58	I PCIE	AC coupled off Module		Device - Connect AC Coupling cap 0.1uF Slot - Connect to PCIE Conn pin	PCI Express Differential Receive Pairs 3
PCIE_RX3-	B59					
PCIE_CLK_REF+	A88	O PCIE	PCIE		Connect to PCIE device, PCIE CLK Buffer or slot	Reference clock output for all PCI Express and PCI Express Graphics lanes.
PCIE_CLK_REF-	A89					

ExpressCard Signals Descriptions

Signal	Pin#	Pin Type	Pwr Rail /Tolerance	TGU9A2	Carrier Board	Description
EXCD0_CPPE#	A49	I CMOS	3.3V /3.3V			PCI ExpressCard: PCI Express capable card request, active low, one per card
EXCD1_CPPE#	B48					
EXCD0_PERST#	A48	O CMOS	3.3V /3.3V			PCI ExpressCard: reset, active low, one per card
EXCD1_PERST#	B47					

DDI Signals Descriptions

Signal	Pin#	Pin Type	Pwr Rail /Tolerance	TGU9A2	Carrier Board	Description
DDIO_PAIR0+/DP0_LANE0+	B71	O PCIE	AC coupled off Module		Connect AC Coupling Capacitors 0.1uF to Device	DDI 0 Pair 0 differential pairs/Serial Digital Video B red output differential pair
DDIO_PAIR0-/DP0_LANE0-	B72				Connect AC Coupling Capacitors 0.1uF to Device	
DDIO_PAIR1+/DP0_LANE1+	B73	O PCIE	AC coupled off Module		Connect AC Coupling Capacitors 0.1uF to Device	DDI 0 Pair 1 differential pairs/Serial Digital Video B green output differential pair
DDIO_PAIR1-/DP0_LANE1-	B74				Connect AC Coupling Capacitors 0.1uF to Device	
DDIO_PAIR2+/DP0_LANE2+	B75	O PCIE	AC coupled off Module		Connect AC Coupling Capacitors 0.1uF to Device	DDI 0 Pair 2 differential pairs/Serial Digital Video B blue output differential pair
DDIO_PAIR2-/DP0_LANE2-	B76				Connect AC Coupling Capacitors 0.1uF to Device	
DDIO_PAIR3+/DP0_LANE3+	B81	O PCIE	AC coupled off Module		Connect AC Coupling Capacitors 0.1uF to Device	DDI 0 Pair 3 differential pairs/Serial Digital Video B clock output differential pair.
DDIO_PAIR3-/DP0_LANE3-	B82				Connect AC Coupling Capacitors 0.1uF to Device	
DDIO_PAIR4+	B77			NA	NA	NA for TGU9A2
DDIO_PAIR4-	B78			NA	NA	
DDIO_PAIR5+	B91			NA	NA	
DDIO_PAIR5-	B92			NA	NA	
DDIO_PAIR6+	B93			NA	NA	NA for TGU9A2
DDIO_PAIR6-	B94			NA	NA	
DDIO_CTRLCLK_AUX+/DP0_AUX+	B98	I/O PCIE	AC coupled on Module	PD 100K to GND (S/W IC between Rpu/PCH)	Connect to DP AUX+	DP AUX+ function if DDIO_DDC_AUX_SEL is no connect
		I/O OD CMOS	3.3V / 3.3V	PU 10K to 3.3V, PD 100K to GND (S/W IC between Rpu/Rpd)	Connect to HDMI/DVI I2C CTRLCLK	HDMI/DVI I2C CTRLCLK if DDIO_DDC_AUX_SEL is pulled high
DDIO_CTRLDATA_AUX-/DP0_AUX-	B99	I/O PCIE	AC coupled on Module	PU 100K to 3.3V	Connect to DP AUX-	DP AUX- function if DDIO_DDC_AUX_SEL is no connect
DDIO_HPD/DP0_HPD	B89	I/O OD CMOS	3.3V / 3.3V	PU 2.2K to 3.3V/PU 100K to 3.3V	Connect to HDMI/DVI I2C CTRLDATA	HDMI/DVI I2C CTRLDATA if DDIO_DDC_AUX_SEL is pulled high
		I CMOS	3.3V / 3.3V	PD 100K to GND	PD 1M and Connect to device Hot Plug Detect	DDI Hot-Plug Detect

DDI0_DDC_AUX_SEL	B95	I CMOS	3.3V / 3.3V	PD 1M to GND	PU 100K to 3.3V for DDC(HDMI/DVI)	<p>Selects the function of DDI0_CTRLCLK_AUX+ and DDI0_CTRLDATA_AUX-.</p> <p>This pin shall have a 1M pull-down to logic ground on the Module. If this input is floating the AUX pair is used for the DP AUX+/- signals. If pulled-high the AUX pair contains the CTRLCLK and CTRLDATA signals</p> <p>*****</p> <p>DDI[n]_DDC_AUX_SEL shall be pulled to 3.3V on the Carrier with a 100K Ohm resistor to configure the DDI[n]_AUX pair as the DDC channel.</p> <p>Carrier DDI[n]_DDC_AUX_SEL should be connected to pin 13 of the DisplayPort</p>
------------------	-----	--------	-------------	--------------	-----------------------------------	--

USB Signals Descriptions

Signal	Pin#	Pin Type	Pwr Rail /Tolerance	TGU9A2	Carrier Board	Description
USB0+	A46	I/O USB	3.3V Suspend/3.3V		Connect 90Ω @100MHz Common Choke in series and ESD suppressors to GND to USB connector	USB differential pairs 0
USB0-	A45					
USB1+	B46	I/O USB	3.3V Suspend/3.3V		Connect 90Ω @100MHz Common Choke in series and ESD suppressors to GND to USB connector	USB differential pairs 1
USB1-	B45					
USB2+	A43	I/O USB	3.3V Suspend/3.3V		Connect 90Ω @100MHz Common Choke in series and ESD suppressors to GND to USB connector	USB differential pairs 2
USB2-	A42					
USB3+	B43	I/O USB	3.3V Suspend/3.3V		Connect 90Ω @100MHz Common Choke in series and ESD suppressors to GND to USB connector	USB differential pairs 3
USB3-	B42					
USB4+	A40	I/O USB	3.3V Suspend/3.3V		Connect 90Ω @100MHz Common Choke in series and ESD suppressors to GND to USB connector	USB differential pairs 4
USB4-	A39					
USB5+	B40	I/O USB	3.3V Suspend/3.3V		Connect 90Ω @100MHz Common Choke in series and ESD suppressors to GND to USB connector	USB differential pairs 5
USB5-	B39					
USB6+	A37	I/O USB	3.3V Suspend/3.3V		Connect 90Ω @100MHz Common Choke in series and ESD suppressors to GND to USB connector	USB differential pairs 6
USB6-	A36					
USB7+	B37	I/O USB	3.3V Suspend/3.3V		Connect 90Ω @100MHz Common Choke in series and ESD suppressors to GND to USB connector	USB differential pairs 7
USB7-	B36					
USB_0_1_OC#	B44	I CMOS	3.3V Suspend/3.3V	PU 10k to 3.3VSB	Connect to Overcurrent of USB Power Switch	USB over-current sense, USB channels 0 and 1. A pull-up for this line shall be present on the Module. An open drain driver from a USB current monitor on the Carrier Board may drive this line low. Do not pull this line high on the Carrier Board.
USB_2_3_OC#	A44	I CMOS	3.3V Suspend/3.3V	PU 10k to 3.3VSB	Connect to Overcurrent of USB Power Switch	USB over-current sense, USB channels 2 and 3. A pull-up for this line shall be present on the Module. An open drain driver from a USB current monitor on the Carrier Board may drive this line low. Do not pull this line high on the Carrier Board.
USB_4_5_OC#	B38	I CMOS	3.3V Suspend/3.3V	PU 10k to 3.3VSB	Connect to Overcurrent of USB Power Switch	USB over-current sense, USB channels 4 and 5. A pull-up for this line shall be present on the Module. An open drain driver from a USB current monitor on the Carrier Board may drive this line low. Do not pull this line high on the Carrier Board.
USB_6_7_OC#	A38	I CMOS	3.3V Suspend/3.3V	PU 10k to 3.3VSB	Connect to Overcurrent of USB Power Switch	USB over-current sense, USB channels 6 and 7. A pull-up for this line shall be present on the Module. An open drain driver from a USB current monitor on the Carrier Board may drive this line low. Do not pull this line high on the Carrier Board.

USB_SSTX0+	B23	O PCIE	AC coupled on Module	AC Coupling capacitor	Connect 90Ω @100MHz Common Choke in series and ESD suppressors to GND to USB connector	Additional transmit signal differential pairs for the SuperSpeed USB data path.
USB_SSTX0-	B22			AC Coupling capacitor		
USB_SSRX0+	A23	I PCIE	AC coupled off Modul		Connect 90Ω @100MHz Common Choke in series and ESD suppressors to GND to USB connector	Additional receive signal differential pairs for the SuperSpeed USB data path.
USB_SSRX0-	A22					
USB_SSTX1+	B26	O PCIE	AC coupled on Module	AC Coupling capacitor	Connect 90Ω @100MHz Common Choke in series and ESD suppressors to GND to USB connector	Additional transmit signal differential pairs for the SuperSpeed USB data path.
USB_SSTX1-	B25			AC Coupling capacitor		
USB_SSRX1+	A26	I PCIE	AC coupled off Modul		Connect 90Ω @100MHz Common Choke in series and ESD suppressors to GND to USB connector	Additional receive signal differential pairs for the SuperSpeed USB data path.
USB_SSRX1-	A25					
USB_HOST_PRSENT	B96	I CMOS	3.3V Suspend/3.3V	NA	NA	Module USB client may detect the presence of a USB host. A high value (NA for TGU9A2) indicates that a host is present.

eDP Signals Descriptions

Signal	Pin#	Pin Type	Pwr Rail /Tolerance	TGU9A2	Carrier Board	Description
eDP_TX2+	A71	O eDP	eDP		Connect to eDP connector	eDP Channel A differential pairs
eDP_TX2-	A72					
eDP_TX1+	A73	O eDP	eDP		Connect to eDP connector	
eDP_TX1-	A74					
eDP_TX0+	A75	O eDP	eDP		Connect to eDP connector	
eDP_TX0-	A76					
NC	A78	O eDP	eDP		Connect to eDP connector	
NC	A79					
eDP_TX3+	A81	O eDP	eDP		Connect to eDP connector	eDP Channel A differential clock
eDP_TX3-	A82					
eDP_VDD_EN	A77	O CMOS	3.3V / 3.3V		Connect to enable control of eDP panel power circuit	eDP panel power enable
eDP_BKLT_EN	B79	O CMOS	3.3V / 3.3V		Connect to enable control of eDP panel backlight power circuit.	eDP panel backlight enable
eDP_BKLT_CTRL	B83	O CMOS	3.3V / 3.3V		Connect to brightness control of eDP panel backlight power circuit.	eDP panel backlight brightness control
eDP_AUX+	A83	I/O OD CMOS	3.3V / 3.3V	PU 4.7K to 3.3V	Connect to DDC clock of eDP panel	I2C clock output for eDP display use
eDP_AUX-	A84	I/O OD CMOS	3.3V / 3.3V	PU 4.7K to 3.3V	Connect to DDC data of eDP panel	I2C data line for eDP display use

LPC Signals Descriptions

Signal	Pin#	Pin Type	Pwr Rail /Tolerance	TGU9A2	Carrier Board	Description	
LPC_AD0	B4	I/O CMOS	3.3V / 3.3V		Connect to LPC device	LPC multiplexed address, command and data bus	
LPC_AD1	B5						
LPC_AD2	B6						
LPC_AD3	B7						
LPC_FRAME#	B3	O CMOS	3.3V / 3.3V			LPC frame indicates the start of an LPC cycle	
LPC_DRQ0#	B8	I CMOS	3.3V / 3.3V			LPC serial DMA request	
LPC_DRQ1#	B9						
LPC_SERIRQ	A50	I/O CMOS	3.3V / 3.3V			LPC serial interrupt	
LPC_CLK	B10	O CMOS	3.3V / 3.3V			LPC clock output - 33MHz nominal	

SPI Signals Descriptions

Signal	Pin#	Pin Type	Pwr Rail /Tolerance	TGU9A2	Carrier Board	Description
SPI_CS#	B97	O CMOS	3.3V Suspend/3.3V	Connect a series resistor 33Ω	Connect a series resistor 33Ω to Carrier Board SPI Device CS# pin	Chip select for Carrier Board SPI - may be sourced from chipset SP10 or SP11
SPI_MISO	A92	I CMOS	3.3V Suspend/3.3V	Connect a series resistor 33Ω	Connect a series resistor 33Ω to Carrier Board SPI Device SO pin	Data in to Module from Carrier SPI
SPI_MOSI	A95	O CMOS	3.3V Suspend/3.3V	Connect a series resistor 33Ω	Connect a series resistor 33Ω to Carrier Board SPI Device SI pin	Data out from Module to Carrier SPI
SPI_CLK	A94	O CMOS	3.3V Suspend/3.3V	Connect a series resistor 33Ω	Connect a series resistor 33Ω to Carrier Board SPI Device SCK pin	Clock from Module to Carrier SPI
SPI_POWER	A91	O	3.3V Suspend/3.3V			Power supply for Carrier Board SPI – sourced from Module – nominally 3.3V. The Module shall provide a minimum of 100mA on SPI_POWER. Carriers shall use less than 100mA of SPI_POWER. SPI_POWER shall only be used to power SPI devices on the Carrier
BIOS_DIS0#	A34	I CMOS	NA	PU 10K to 3.3V		Selection straps to determine the BIOS boot device.
BIOS_DIS1#	B88					The Carrier should only float these or pull them low, please refer to COM Express Module Base Specification Revision 2.1 for strapping options of BIOS disable signals.

Serial Interface Signals Descriptions

Signal	Pin#	Pin Type	Pwr Rail /Tolerance	TGU9A2	Carrier Board	Description
SER0_TX	A98	O CMOS	5V / 12V(design 3.3v~5V tolerant)		PD 4.7K	General purpose serial port 0 transmitter
SER0_RX	A99	I CMOS	5V / 12V(design 3.3v~5V tolerant)			General purpose serial port 0 receiver
SER1_TX	A101	O CMOS	5V / 12V(design 3.3v~5V tolerant)		PD 4.7K	General purpose serial port 1 transmitter
SER1_RX	A102	I CMOS	5V / 12V(design 3.3v~5V tolerant)			General purpose serial port 1 receiver

Miscellaneous Signal Descriptions

Signal	Pin#	Pin Type	Pwr Rail /Tolerance	TGU9A2	Carrier Board	Description
I2C_CK	B33	I/O OD CMOS	3.3V Suspend/3.3V	PU 2.2K to 3V3SB		General purpose I2C port clock output
I2C_DAT	B34	I/O OD CMOS	3.3V Suspend/3.3V	PU 2.2K to 3V3SB		General purpose I2C port data I/O line
SPKR	B32	O CMOS	3.3V / 3.3V	PU 10K to 3V3SB		Output for audio enunciator - the "speaker" in PC-AT systems. This port provides the PC beep signal and is mostly intended for debugging purposes.
WDT	B27	O CMOS	3.3V / 3.3V			Output indicating that a watchdog time-out event has occurred.
FAN_PWMOUT	B101	O OD CMOS	3.3V / 12V			Fan speed control. Uses the Pulse Width Modulation (PWM) technique to control the fan's RPM.
FAN_TACHIN	B102	I OD CMOS	3.3V / 12V			Fan tachometer input for a fan with a two pulse output.
TPM_PP	A96	I CMOS	3.3V / 3.3V	NC		Trusted Platform Module (TPM) Physical Presence pin. Active high. TPM chip has an internal pull down. This signal is used to indicate Physical Presence to the TPM. (NC for TGU9A2)

Power and System Management Signals Descriptions

Signal	Pin#	Pin Type	Pwr Rail /Tolerance	TGU9A2	Carrier Board	Description
PWRBTN#	B12	I CMOS	3.3V Suspend/3.3V	PU 10K to 3V3SB		A falling edge creates a power button event. Power button events can be used to bring a system out of S5 soft off and other suspend states, as well as powering the system down.
SYS_RESET#	B49	I CMOS	3.3V Suspend/3.3V	PU 4.7K to 3V3SB		Reset button input. Active low request for Module to reset and reboot. May be falling edge sensitive. For situations when SYS_RESET# is not able to reestablish control of the system, PWR_OK or a power cycle may be used.
CB_RESET#	B50	O CMOS	3.3V Suspend/3.3V			Reset output from Module to Carrier Board. Active low. Issued by Module chipset and may result from a low SYS_RESET# input, a low PWR_OK input, a VCC_12V power input that falls below the minimum specification, a watchdog timeout, or may be initiated by the Module software.
PWR_OK	B24	I CMOS	3.3V / 3.3V	PU 10K to 3.3VSB		Power OK from main power supply. A high value indicates that the power is good. This signal can be used to hold off Module startup to allow Carrier based FPGAs or other configurable devices time to be programmed.
SUS_STAT#	B18	O CMOS	3.3V Suspend/3.3V			Indicates imminent suspend operation; used to notify LPC devices.
SUS_S3#	A15	O CMOS	3.3V Suspend/3.3V			Indicates system is in Suspend to RAM state. Active low output. An inverted copy of SUS_S3# on the Carrier Board may be used to enable the non-standby power on a typical ATX supply.
SUS_S4#	A18	O CMOS	3.3V Suspend/3.3V			Indicates system is in Suspend to Disk state. Active low output.
SUS_S5#	A24	O CMOS	3.3V Suspend/3.3V			Indicates system is in Soft Off state.
WAKE0#	B66	I CMOS	3.3V Suspend/3.3V	PU 1K to 3.3VSB		PCI Express wake up signal.
WAKE1#	B67	I CMOS	3.3V Suspend/3.3V	PU 1K to 3.3VSB		General purpose wake up signal. May be used to implement wake-up on PS2 keyboard or mouse activity.
BATLOW#	A27	I CMOS	3.3V Suspend/ 3.3V	PU 4.7K to 3.3VSB		Indicates that external battery is low. This port provides a battery-low signal to the Module for orderly transitioning to power saving or power cut-off ACPI modes.

LID#	A103	I/O CMOS	3.3V Suspend/12V	PU 47K to 3.3VSB	LID switch. Low active signal used by the ACPI operating system for a LID switch.
SLEEP#	B103	I/O CMOS	3.3V Suspend/12V	PU 10K to 3.3VSB	Sleep button. Low active signal used by the ACPI operating system to bring the system to sleep state or to wake it up again.
THRM#	B35	I CMOS	3.3V / 3.3V	PU 10K to 3.3VSB	Input from off-Module temp sensor indicating an over-temp situation.
THRMTRIP#	A35	O CMOS	3.3V / 3.3V	PU 10K to 3.3VSB	Active low output indicating that the CPU has entered thermal shutdown.
SMB_CLK	B13	I/O OD CMOS	3.3V Suspend/3.3V	PU 2.2K to 3.3VSB	System Management Bus bidirectional clock line.
SMB_DAT	B14	I/O OD CMOS	3.3V Suspend/3.3V	PU 2.2K to 3.3VSB	System Management Bus bidirectional data line.
SMB_ALERT#	B15	I CMOS	3.3V Suspend/3.3V	PU 10K to 3.3VSB	System Management Bus Alert – active low input can be used to generate an SMI# (System Management Interrupt) or to wake the system.

GPIO Signals Descriptions

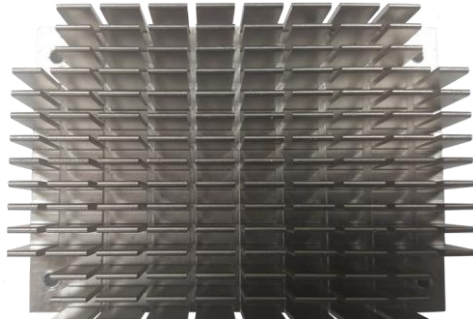
Signal	Pin#	Pin Type	Pwr Rail /Tolerance	TGU9A2	Carrier Board	Description
GPO0	A93	O CMOS	3.3V / 3.3V			General purpose output pins.
GPO1	B54					
GPO2	B57					
GPO3	B63					
GPI0	A54	I CMOS	PU 100K to 3V3	PU 47K to 3.3V		General purpose input pins.
GPI1	A63			PU 47K to 3.3V		
GPI2	A67			PU 47K to 3.3V		
GPI3	A85			PU 47K to 3.3V		

Power and GND Signal Descriptions

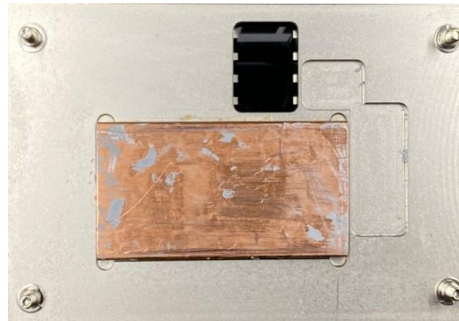
Signal	Pin#	Pin Type	Pwr Rail /Tolerance	TGU9A2	Carrier Board	Description
VCC_12V	A104~A109 B104~B109	Power	4.75V – 20.0V	4.75V – 20.0V		Primary power input: +12V nominal. All available VCC_12V pins on the connector(s) shall be used. The module supplies a wide range of power from 4.75V to 20.0V.
VCC_5V_SBY	B84~B87	Power	4.75V - 5.25V	4.75V - 5.25V		Standby power input: +5.0V nominal. If VCC5_SBY is used, all available VCC_5V_SBY pins on the connector(s) shall be used. Only used for standby and suspend functions. May be left unconnected if these functions are not used in the system design.
VCC_RTC	A47	Power	2.0V - 3.3V	2.0V - 3.3V		Real-time clock circuit-power input. Nominally +3.0V.
GND	A1, A11, A21, A31, A41, A51, A57, A60, A66, A70, A80, A90, A100, A110, B1, B11, B21, B31, B41, B51, B60, B70, B80, B90, B100, B110	Power				Ground - DC power and signal and AC signal return path. All available GND connector pins shall be used and tied to Carrier Board GND plane.

Cooling Option

Heat Sink



Top View of the Heat Sink



Bottom View of the Heat Sink



Important:

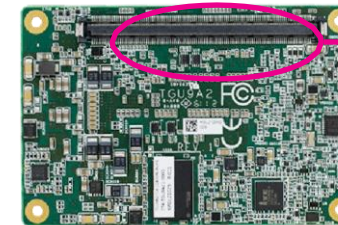
Remove the plastic covering from the thermal pads prior to mounting the heat sink onto board.

Installing TGU9A2 onto a Carrier Board

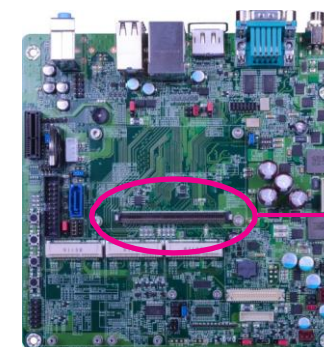
Important:

The carrier board (COM100-B) used in this section is for reference purpose only and may not resemble your carrier board. These illustrations are mainly to guide you on how to install TGU9A2 onto the carrier board of your choice.

1. Grasp TGU9A2 by its edges and position it on top of the carrier board with its COM Express connector aligned with the COM Express connector on the carrier board. This will also help align the mountings holes of TGU9A2 with the standoffs on the carrier board.

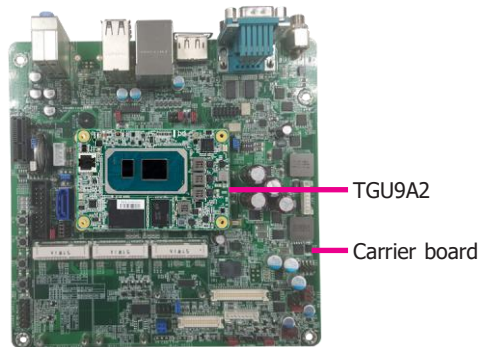


COM Express connector on TGU9A2

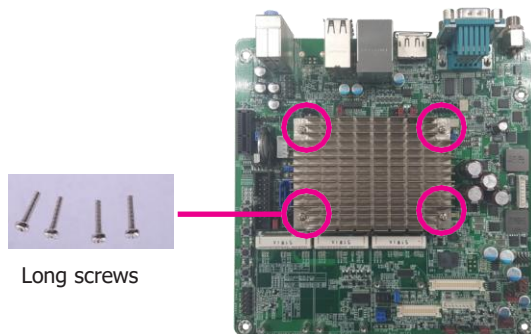


COM Express connector on the carrier board

2. Apply firm even pressure to the side with the COM Express connector first and push down the entire module. Be careful when pressing the module to avoid damaging it. You will hear a distinctive “click”, indicating the module is correctly locked into position.



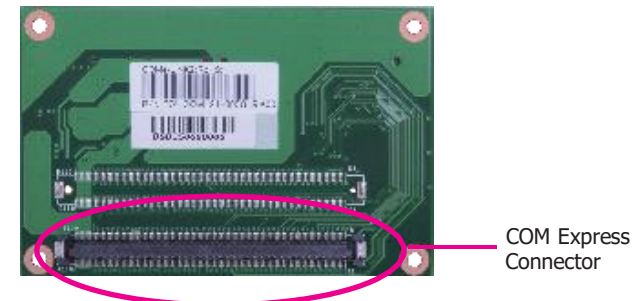
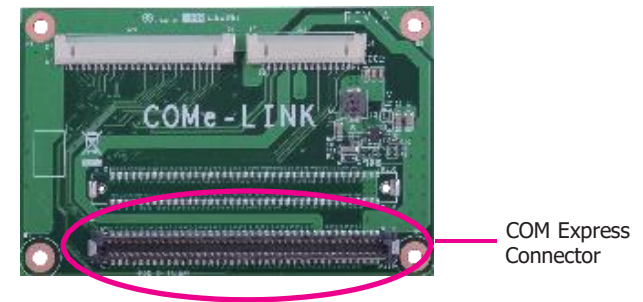
3. Align the mounting holes of the heatsink with the mounting holes of the module. Use the provided mounting screws to install the heat sink onto the module.



Installing the COM Express Debug Card

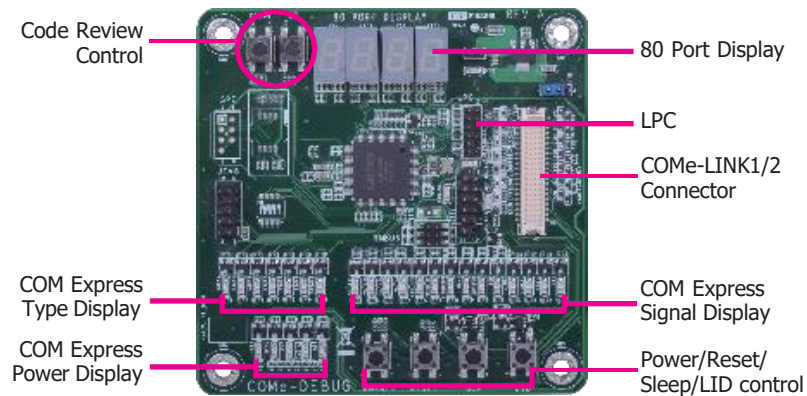
Note:
The system board used in the following illustrations may not resemble the actual board. These illustrations are for reference only.

1. COMe-LINK2 is the COM Express debug platform installed into COM Express Mini modules for the application of debugging and displaying signals and codes.

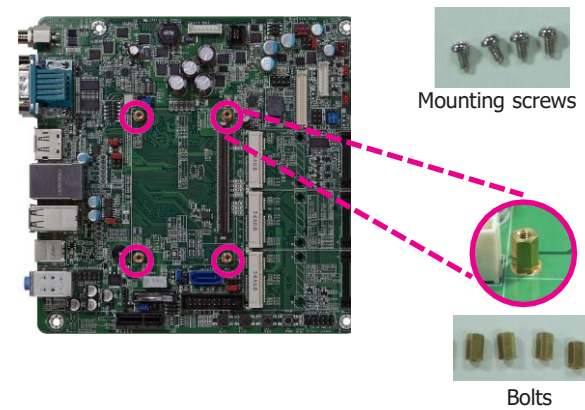


2. Connect the COMe-DEBUG card to COMe-LINK2 via a cable.

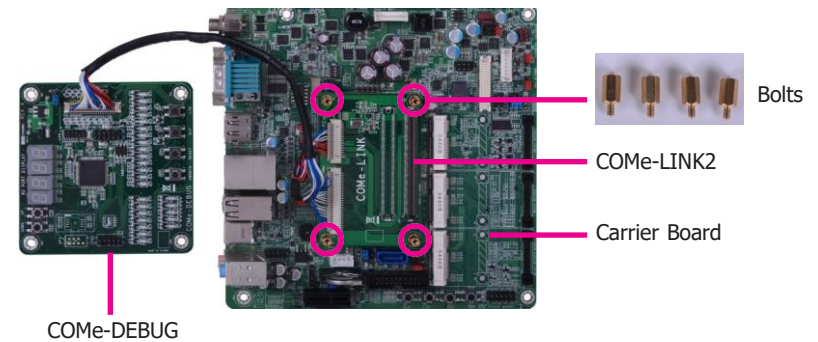
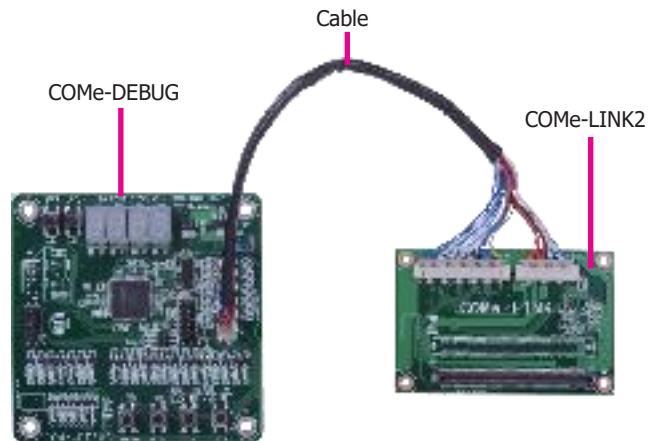
COMe-DEBUG



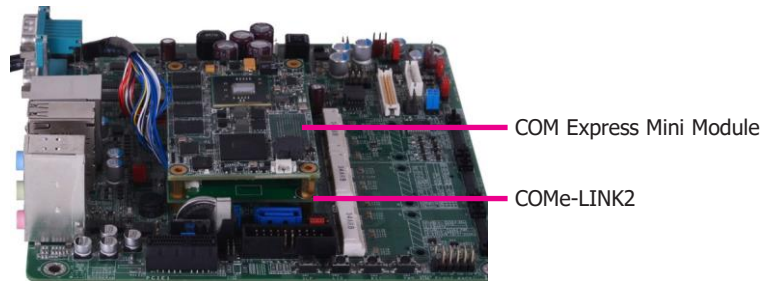
3. Fasten bolts with mounting screws through mounting holes to be fixed in place.



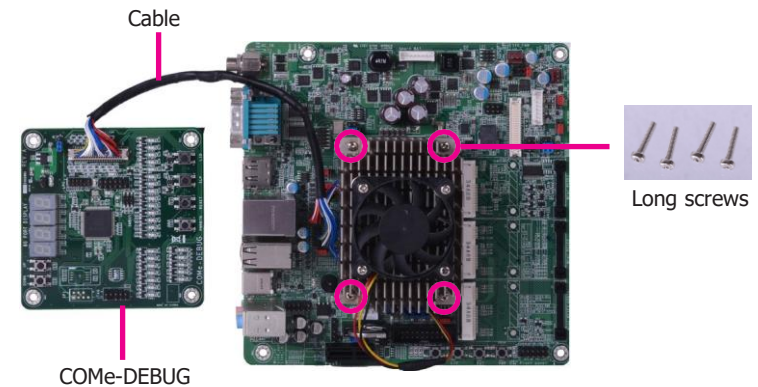
4. Use the provided bolts to fix the COMe-LINK2 debug card onto the carrier board.



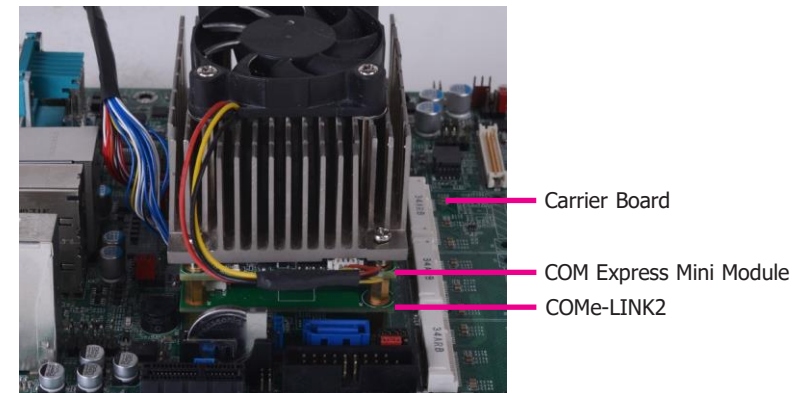
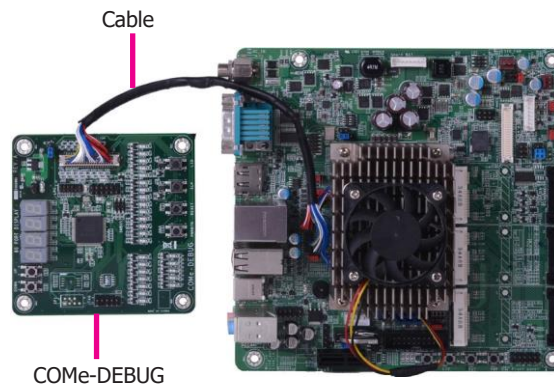
5. Grasp the COM Express Mini module by its edges to press it down on the top of the COMe-LINK2 debug card.



7. Use the long mounting screws to secure the heat sink on the top of the COM Express Mini module and the COMe-LINK2 debug card and connect the cooling fan's cable to the fan connector on the COM Express Mini module. The photo below shows the locations of long mounting screws.



6. Then, grasp the heat sink by its edges and position it down firmly on the top of the COM Express Mini module.



Side View of the Module, Debug Card and Carrier Board

Chapter 4 - BIOS Setup

Overview

The BIOS is a program that takes care of the basic level of communication between the CPU and peripherals. It contains codes for various advanced features found in this system board. The BIOS allows you to configure the system and save the configuration in a battery-backed CMOS so that the data retains even when the power is off. In general, the information stored in the CMOS RAM of the EEPROM will stay unchanged unless a configuration change has been made such as a hard drive replaced or a device added.

It is possible that the CMOS battery will fail causing CMOS data loss. If this happens, you need to install a new CMOS battery and reconfigure the BIOS settings.

**Note:**

The BIOS is constantly updated to improve the performance of the system board; therefore the BIOS screens in this chapter may not appear the same as the actual one. These screens are for reference purpose only.

Default Configuration

Most of the configuration settings are either predefined according to the Load Optimal Defaults settings which are stored in the BIOS or are automatically detected and configured without requiring any actions. There are a few settings that you may need to change depending on your system configuration.

Entering the BIOS Setup Utility

The BIOS Setup Utility can only be operated from the keyboard and all commands are keyboard commands. The commands are available at the right side of each setup screen.

The BIOS Setup Utility does not require an operating system to run. After you power up the system, the BIOS message appears on the screen and the memory count begins. After the memory test, the message "Press DEL to run setup" will appear on the screen. If the message disappears before you respond, restart the system or press the "Reset" button. You may also restart the system by pressing the <Ctrl> <Alt> and keys simultaneously.

Legends

KEYs	Function
Right and Left Arrows	Moves the highlight left or right to select a menu.
Up and Down Arrows	Moves the highlight up or down between submenus or fields.
<Esc>	Exits to the BIOS setup utility
+ (plus key)	Scrolls forward through the values or options of the highlighted field.
- (minus key)	Scrolls backward through the values or options of the highlighted field.
<F1>	Displays general help
<F2>	Displays previous values
<F9>	Optimized defaults
<F10>	Saves and reset the setup program.
<Enter>	Press <Enter> to enter the highlighted submenu

Scroll Bar

When a scroll bar appears to the right of the setup screen, it indicates that there are more available fields not shown on the screen. Use the up and down arrow keys to scroll through all the available fields.

Submenu

When "►" appears on the left of a particular field, it indicates that a submenu which contains additional options are available for that field. To display the submenu, move the highlight to that field and press <Enter>.

AMI BIOS Setup Utility

Main

The Main menu is the first screen that you will see when you enter the BIOS Setup Utility.

Aptio Setup - AMI		
Main	Advanced	Chipset
Project Name TGU9A2		
BIOS Version B217.02A		
EC Version E213.18A		
FSP version 0A.00.45.33		
RC version 0A.E0.45.33		
11th Gen Intel(R) Core(TM) i7-1185GRE @ 2.80GHz		
ID 0x806C1		
Stepping B0		
L1 Data Cache 48 kB x 4		
L1 Instruction Cache 32 kB x 4		
L2 Cache 1080 kB x 4		
L3 Cache 12 MB		
Number of Processors 4Core(s)/8Thread(s)		
BXT SOC B1		
Microcode Revision 78		
Memory RC Version 1.0.18.1		
Total Memory 7396 MB		
Memory Speed 4267 MT/s		
PCH SKU TGL PCH-LP LP IOT SKU		
ME FW Version 15.0.10.1447		
ME Firmware SKU Corporate SKU		
PMC FW Version 150.1.20.1028		
→←: Select Screen		
↑↓: Select Item		
Enter: Select		
+/-: Change Opt.		
F1: General Help		
F2: Previous Values		
F9: Optimized Defaults		
F10: Save & Exit		
ESC: Exit		
Version 2.21.1278. Copyright (C) 2021 American Megatrends, Inc.		

System Time


The time format is <hour>, <minute>, <second>. The time is based on the 24-hour military-time clock. For example, 1 p.m. is 13:00:00. Hour displays hours from 00 to 23. Minute displays minutes from 00 to 59. Second displays seconds from 00 to 59.

System Date

The date format is <day>, <month>, <date>, <year>. Day displays a day, from Sunday to Saturday. Month displays the month, from 01 to 12. Date displays the date, from 01 to 31. Year displays the year, from 2005 to 2099.

Advanced

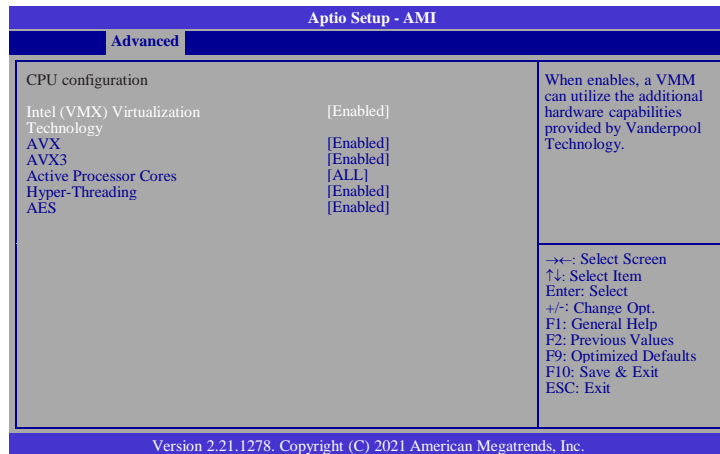
The Advanced menu allows you to configure your system for basic operation. Some entries are defaults required by the system board, while others, if enabled, will improve the performance of your system or let you set some features according to your preference.

**Important:**
Setting incorrect field values may cause the system to malfunction.

Aptio Setup - AMI		
Main	Advanced	Chipset
▶ CPU Configuration		
▶ Power & Performance		
▶ PCIE Configuration		
▶ PCH-FW Configuration		
▶ Trusted Computing		
▶ IT8528 Super IO Configuration		
▶ Serial Port Console Redirection		
▶ ACPI Settings		
▶ AMI Graphic Output Protocol Policy		
▶ USB Configuration		
▶ Network Stack Configuration		
▶ CSM Configuration		
▶ NVMe Configuration		
▶ DFI EC HW Monitor		
▶ DFI WDT Configuration		
▶ Tls Auth Configuration		
▶ RAM Disk Configuration		
CPU Configuration Parameters		
→←: Select Screen		
↑↓: Select Item		
Enter: Select		
+/-: Change Opt.		
F1: General Help		
F2: Previous Values		
F9: Optimized Defaults		
F10: Save & Exit		
ESC: Exit		
Version 2.21.1278. Copyright (C) 2021 American Megatrends, Inc.		

CPU Configuration

This section is used to configure the CPU.



Intel (VMX) Virtualization Technology

When enables, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.

AVX

Enable/ Disable the AVX 2/3 Instructions.

AVX3

Enable/ Disable the AVX 3 Instructions.

Active Processor Cores

Choose how many cores of processor will be activated.

Hyper-Threading

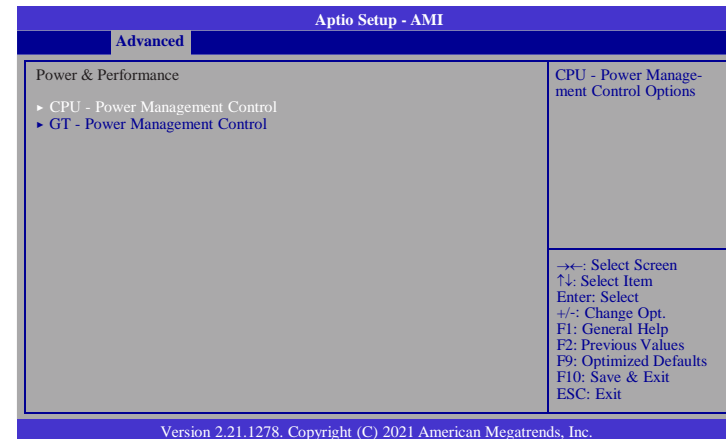
Enable/ Disable the Intel HT technology.

AES

Enable/ Disable Advanced Encryption Standard.

Power & Performance

This section configures power and performance.



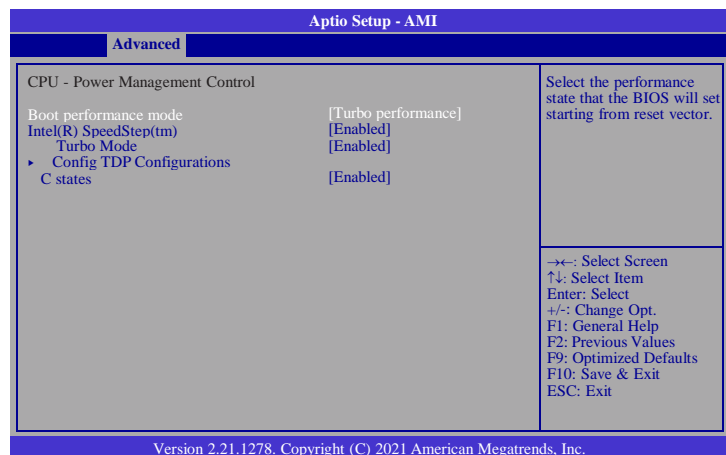
CPU - Power Management Control

CPU Power Management Control options.

GT - Power Management Control

GT Power Management Control options.

- CPU Power Management Control



Boot performance mode

Select the performance state that the BIOS will set starting from reset vector - Max Battery, Max Non-Turbo Performance, Turbo Performance.

Intel(R) SpeedStep(tm)

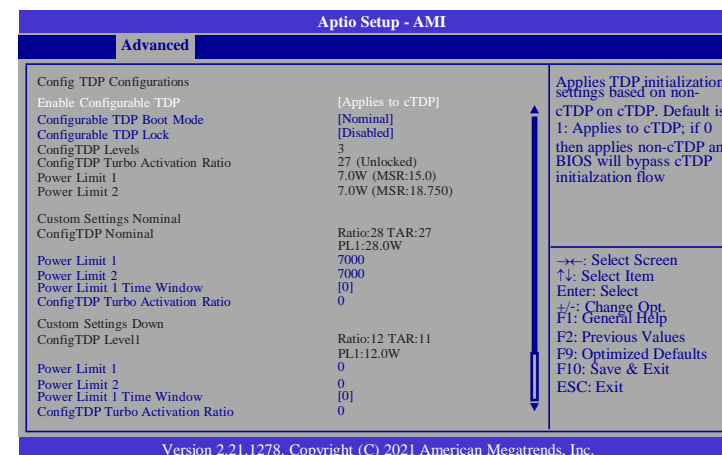
Allows more than two frequency ranges to be supported. - Enabled and disabled.

-Turbo Mode: Enable/Disable processor Turbo Mode (requires EMTTM enabled too). AUTO means enabled.

-Config TDP Configurations: See next page.

C-States

Enable or disable CPU Power Management. It allows CPU to go to C States when it's not 100% utilized.



Enable Configurable TDP

Applies TDP initialization settings based on non-cTDP on cTDP. Default is 1: Applies to cTDP; if 0 then applies non-cTDP and BIOS will bypass cTDP initialization flow

Configurable TDP Boot Mode

Configurable TDP Mode as Nominal/Up/Down/Deactivate selection. Deactivate option will set MSR to Nominal and MMIO to Zero.

Configurable TDP Lock

Configurable TDP Mode Lock sets the Lock bits on TURBO_ACTIVATION_RATIO and CONFIG_TDP_CONTROL. Note: When CTDP Lock is enabled Custom ConfigTDP Cou will be forced to 1 and Cust ConfigTDP Boot Index will be forced to 0.

Power Limit 1

Power Limit 1 in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Overclocking SKU: Value must be between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). Other between Min Power Limit and TDP Limit.

Power Limit 2

Power Limit 2 value in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Processor applies control policies such that the package power does not exceed this limit.

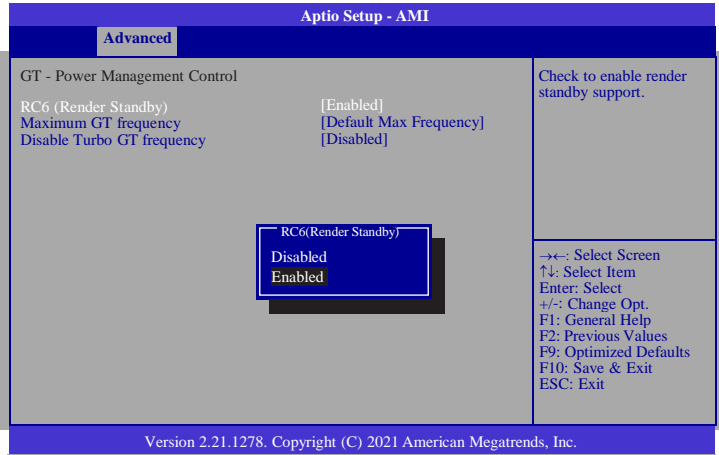
Power Limit 1 Time Window

Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0 = default value (28 sec for Mobile and 8 sec for Desktop). Defines time window which TDP value should be maintained.

ConfigTDP Turbo Activation Ratio

Custom value for Turbo Activation Ratio. Needs to be configured with valid values from LFM to Max Turbo. 0 means don't use custom value.

- GT Power Management Control



RC6 (Render Standby)

Check to enable render standby support.

Maximum GT frequency

Maximum GT frequency limited by the user. Choose between 100MHz (RPN) and 1350MHZ(RPO). Value beyond the range will be clipped to min/max supported by SKU

Disable Turbo GT frequency

Enabled: Disables Turbo GT frequency. Disabled: GT frequency is not limited

PCIE Configuration

Aptio Setup - AMI	
Advanced	
PCIE Configuration ▶ IMR Configuration	IMR Configuration →←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values P9: Optimized Defaults F10: Save & Exit ESC: Exit
Version 2.21.1278. Copyright (C) 2021 American Megatrends, Inc.	

Aptio Setup - AMI	
Advanced	
PCIe IMR [Enabled] PCIe IMR Size 0 PCIe RP Location for IMR [PCH PCIe] RP index for IMR 0	Enable/Disable PCIe IMR →←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values P9: Optimized Defaults F10: Save & Exit ESC: Exit
Version 2.21.1278. Copyright (C) 2021 American Megatrends, Inc.	

IMR Configuration

- **PCIe IMR:** Enable/Disable PCIe IMR.
- **PCIe IMR Size:** PCIe Reserved Memory Size to be requested in MB.
Maximum value of 1024 MB
- **PCIe RP Location for IMR:** Select SA or PCH roor port associated with IMR
- **RP index for IMR:** Selects which root port will be associated with IMR

PCH-FW Configuration

Aptio Setup - AMI	
Advanced	
ME State [Enabled] Manageability Features State [Enabled] AMT BIOS Features [Enabled] ▶ AMT Configuration ME Unconfig on RTC Clear [Enabled] ▶ Firmware Update Configuration	When Disabled ME will be put into ME Temporarily Disabled Mode. →←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values P9: Optimized Defaults F10: Save & Exit ESC: Exit
Version 2.21.1278. Copyright (C) 2021 American Megatrends, Inc.	

ME State

Enable or disable Management Engine. When this field is set to Disabled, ME will be put into ME Temporarily Disabled Mode. The following fields will only appear when ME State is enabled.

Manageability Features State

Enable or disable Intel(R) Manageability features. This option disables/enables Manageability Features support in FW. To disable, support platform must be in an unprovisioned state first.

AMI BIOS Features

When disabled, AMT BIOS features are no longer supported and user is no longer able to access MEBx Setup. This option does not disable manageability features in FW.

▶ AMT Configuration

This section is used to configure Intel(R) Active Management Technology Parameters. Please refer to the following pages.

ME Unconfig on RTC Clear

When disabled, ME will not be unconfigured on RTC Clear.

▶ Firmware Update Configuration

Please refer to the following pages.

► AMT Configuration

USB Provisioning of AMT

Enable or disable AMT USB Provisioning.

► Secure Erase Configuration

Please refer to the following pages.

► OEM Flags Settings

Please refer to the following pages.

► AMT Configuration ► Secure Erase Configuration

This section is used to configure Secure Erase.

Secure Erase Mode

Select Secure Erase module behavior: Simulated or Real.

Force Secure Erase

Enable or disable Force Secure Erase on next boot.

Hide Unconfigure ME Confirmation Prompt

Enable or disable to hide unconfigure ME confirmation prompt when attempting ME unconfiguration.

Unconfigure ME

Enable or disable to unconfigure ME with resetting MEBx password to default.

Me FW Image Re-Flash

This field is used to enable or disable the Me FW Image Re-Flash function.

Trusted Computing

Aptio Setup - AMI		
	Advanced	
TPM 2.0 Device Found	7.85	Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.
Firmware Version:	IFX	
Vendor:		
Security Device Support	[Enable]	
Active PCR banks	SHA256	←→: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
Available PCR banks	SHA-1,SHA256	
SHA-1 PCR Bank	[Disabled]	
SHA256 PCR Bank	[Enabled]	
Pending operation	[None]	
Platform Hierarchy	[Enabled]	
Storage Hierarchy	[Enabled]	
Endorsement Hierarchy	[Enabled]	
Version 2.21.1278. Copyright (C) 2021 American Megatrends, Inc.		

Security Device Support

To enable or disable BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.

SHA-1 PCR Bank

Enable or Disable SHA-1 PCR Bank.

SHA-256 PCR Bank

Enable or Disable SHA256 PCR Bank

Pending operation

Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change State of Security Device.

Platform Hierarchy

Enable or Disable Platform Hierarchy.

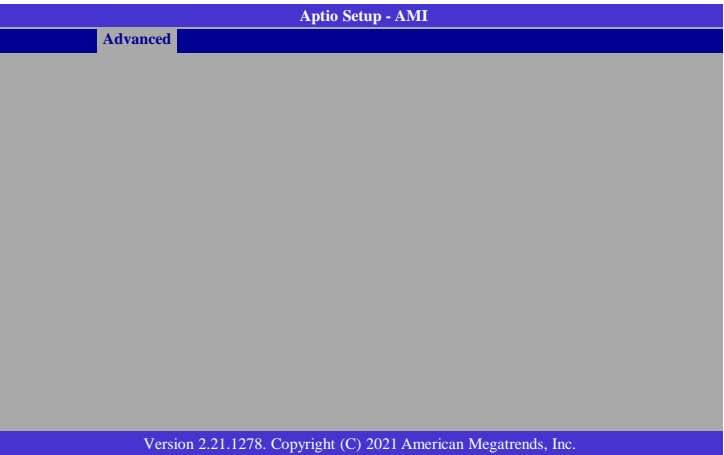
Storage Hierarchy

Enable or Disable Storage Hierarchy

Endorsement Hierarchy

Enable or Disable Endorsement Hierarchy.

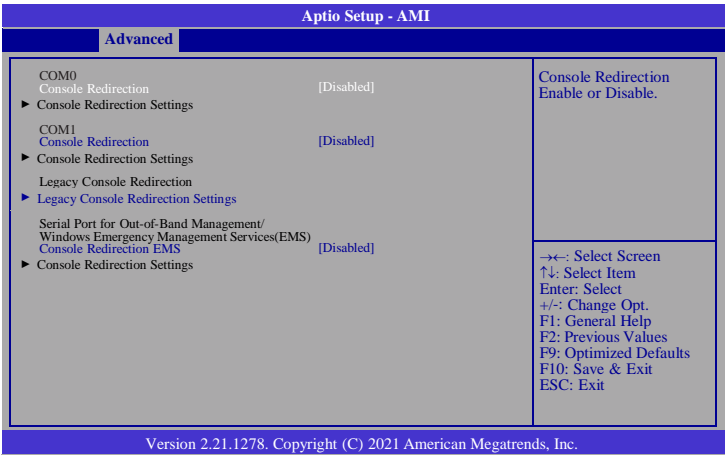
IT8528 Super IO Configuration



Serial Port Configuration

Set Parameters of Serial Ports.

Serial Port Console Redirection



Console Redirection

Console Redirection Enable or Disable.

Console Redirection Settings

See next page.

Legacy Console Redirection Settings

See following pages.

Console Redirection EMS

See following pages.

Aptio Setup - AMI		
Advanced		
COM0 Console Redirection Settings		Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100Plus: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
Terminal Type	[VT100Plus]	
Bits per second	[115200]	
Data Bits	[8]	
Parity	[None]	
Stop Bits	[1]	→←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
Flow Control	[None]	
VT-UTF8 Combo Key Support	[Enabled]	
Recorder Mode	[Disabled]	
Resolution 100x31	[Enabled]	
Putty KeyPad	[VT100]	
Version 2.21.1278. Copyright (C) 2021 American Megatrends, Inc.		

Terminal Type

Emulation:

ANSI: Extended ASCII char set. VT100:

ASCII char set.

VT100Plus: 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

Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.

Data Bits

Determine data bits.

Parity

A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even.

Odd: parity bit is 0 if num 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.

Stop Bits

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

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

Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals.

Recorder Mode

With this mode enabled only text will be sent. This is to capture Terminal data.

Resolution 100x31

Enables or disables extended terminal resolution.

Putty KeyPad

Select Functionkey and KeyPad on Putty.

Aptio Setup - AMI		
Advanced		
Legacy Console Redirection Settings		
Redirection COM Port	[COM0]	Select a COM port to display redirection of Legacy OS and Legacy OPRM Messages
Resolution	[80x24]	
Redirect After POST	[Always Enable]	
		→←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
Version 2.21.1278. Copyright (C) 2021 American Megatrends, Inc.		

Redirection COM Port

Select a COM port to display redirection of Legacy OS and Legacy OPRM Messages.

Resolution

On Legacy OS, the Number of Rows and Columns supported redirection.

Redirect After POST

When Boot loader 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.

ACPI Settings

Aptio Setup - AMI		
Advanced		
ACPI Settings		
Wake System from S5 via RTC State After G3	[Disabled] [S0 State]	Enable or disable System wake on alarm event. When enabled System will wake on the hr:min:sec specified
		→←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
Version 2.21.1278. Copyright (C) 2021 American Megatrends, Inc.		

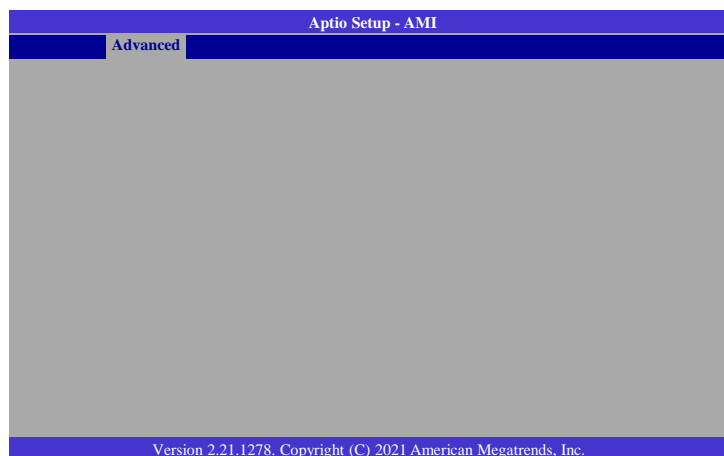
Wake System from S5 via RTC

Enable or disable System wake on alarm event. When enabled System will wake on the hr:min:sec specified.

State After G3

Select between S0 State, Last State, and S5 State. This field is used to specify what state the system is set to return to when power is re-applied after a power failure (G3 state).

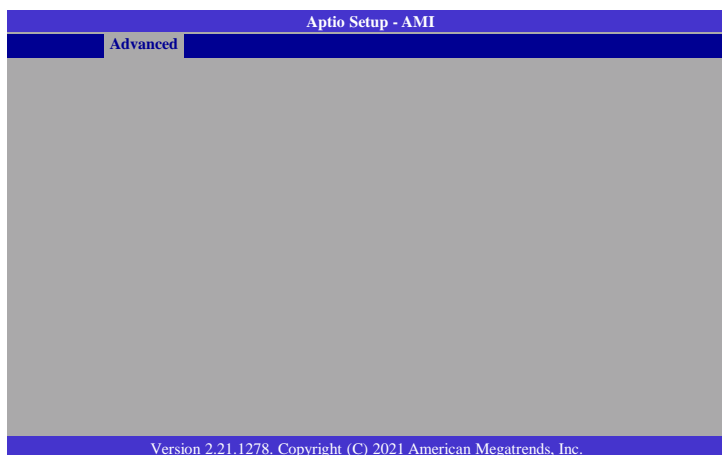
AMI Graphic Output Protocol Policy



Output Select

Select output interface.

USB Configuration



Legacy USB Support

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

Enable or disable XHCI Hand-off.

USB Mass Storage Driver Support

Enable or Disable USB Mass Storage Driver Support.

Port 60/64 Emulation

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 transfer time-out

The time-out value for Control, Bulk, and Interrupt transfers.

Device reset time-out

USB mass storage device Start Unit command time-out.

Device power-up delay

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.

Network Stack Configuration

Aptio Setup - AMI		
Advanced		
Network Stack	[Enabled]	Enable/Disable UEFI Network Stack
IPv4 PXE Support	[Disabled]	
IPv4 HTTP Support	[Disabled]	
IPv6 PXE Support	[Disabled]	
IPv6 HTTP Support	[Disabled]	
PXE boot wait time	0	
Media detect count	1	
		→←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
Version 2.21.1278. Copyright (C) 2021 American Megatrends, Inc.		

Network Stack

Enable or disable UEFI network stack. The following fields will appear when this field is enabled.

IPv4 PXE Support

Enable/Disable IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available.

IPv4 HTTP Support

Enable/Disable IPv4 HTTP boot support. If disabled, IPv4 HTTP boot support will not be available.

IPv6 PXE Support

Enable/Disable IPv6 PXE boot support. If disabled, IPV6 PXE boot support will not be available.

IPv6 HTTP Support

Enable/Disable IPv6 HTTP boot support. If disabled, IPv6 HTTP boot support will not be available.

Media detect count

Set the number of times the presence of media will be checked. Use either +/- or numeric keys to set the value.

CSM Configuration

Aptio Setup - AMI		
Advanced		
Compatibility Support Module Configuration		Enable/Disable CSM Support.
CSM Support	[Enabled]	
GateA20 Active	[Upon Request]	
INT19 Trap Response	[Immediate]	
Boot option filter	[UEFI only]	
Option ROM execution		
Network	[Do not launch]	→←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
Storage	[UEFI]	
Video	[UEFI]	
Other PCI devices	[UEFI]	
Version 2.21.1278. Copyright (C) 2021 American Megatrends, Inc.		

CSM Support

Enable/Disable CSM Support.

GateA20 Active

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.

INT19 Trap Response

BIOS reaction on INT19 trapping by Option ROM:
 IMMEDIATE - execute the trap right away;
 POSTPONED - execute the trap during legacy boot.

Boot option filter

This option controls Legacy/UEFI ROMS priority.

Others see next page.

Network

This field controls the execution of UEFI and Legacy Network OpROM.

Storage

This field controls the execution of UEFI and Legacy Storage OpROM.

Video

This field controls the execution of UEFI and Legacy Video OpROM.

Other PCI devices

This field determines OpROM execution policy for devices other than Network, Storage or Video.

NVMe Configuration

Aptio Setup - AMI		
Advanced		
Seg : Bus : Dev : Func	00:01:00:00	Select either Short or Extended Self Test. Short option will take couple of minutes and extended option will take several minutes to complete.
Model Number	MTFDHBL128TDQ	
Total Size	128.0 GB	
Vendor ID	1344	
Device ID	6001	
Namespace: 1	Size: 128.0 GB	← Select Screen ↑↓ Select Item Enter Select +/- Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
Device Self Test:		
Self Test Option	[Short]	
Self Test Action	[Controller Only Test]	
Run Device Self Test		
Short Device Selftest Result	[Not Available]	
Extended Device Selftest Result	[Not Available]	
Version 2.21.1278. Copyright (C) 2021 American Megatrends, Inc.		

Self Test Option

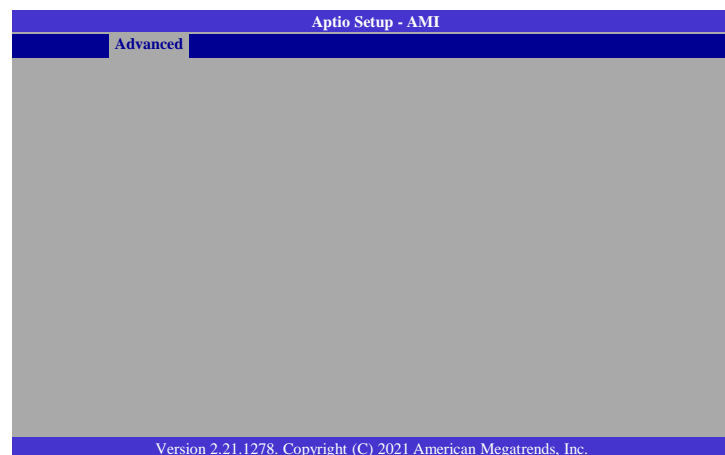
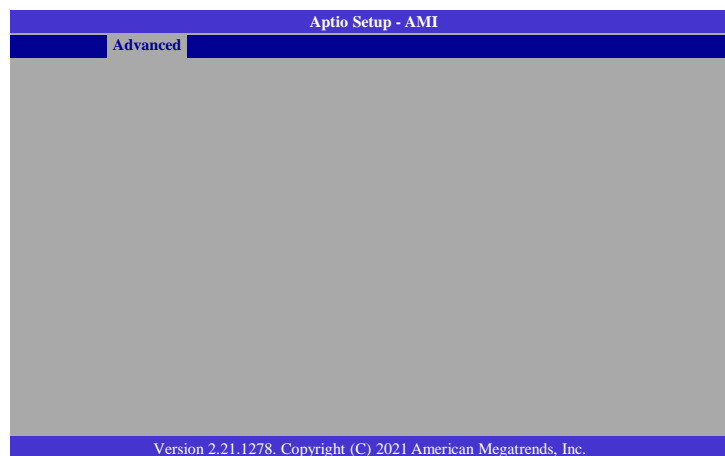
Select either Short or Extended Self Test. Short option will take couple of minutes and extended option will take several minutes to complete.

Self Test Action

Select either to test Controller alone or Controller and NameSpace. Selecting Controller and NameSpace option will take lot longer to complete the test.

Run Device Self Test

Perform device self test for the corresponding Option and Action selected by user. Pressing 'Esc' key will abort the test. Result shown below is the recent result logged in the device.



Smart Fan is a fan speed moderation strategy dependent on the current system temperature. When the system temperature goes higher than the Boundary setting, the fan speed will be turned up to the setting of the Fan Speed Count that bears the same index as the Boundary field.

▼ CPU Smart Fan Mode = [SMART FAN IV]

Boundary 1 to Boundary 4

Set the boundary temperatures that determine the fan speeds accordingly, the value ranging from 0-127. For example, when the system temperature reaches Boundary 1 setting, the fan speed will be turned up to the designated speed of the Fan Speed Count 1 field.

Fan Speed Count 1 to Fan Speed Count 4

Set the fan speed, the value ranging from 1-100%, 100% being full speed. The fans will operate according to the specified boundary temperatures above-mentioned.

▼ CPU Smart Fan Control = [Manual]

Fix Fan Speed Count

Set the fan speed, the value ranging from 1-100%, 100% being full speed. The fans will always operate at the specified speed regardless of gauged temperatures.

DFI WDT Configuration

Aptio Setup - AMI		
Advanced		
DFI WDT Configuration		Enable/Disable Watchdog Timer
Watchdog Timer	[Enabled]	
Output Options	[Mode1]	
Enable Delay	300	
Timeout Delay	150	
		→←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
Version 2.21.1278. Copyright (C) 2021 American Megatrends, Inc.		

Watchdog Timer

Enable/Disable Watchdog Timer.

Output Options

Select the Output Options.

Mode1 = A Watchdog Timeout causes the system to be reset.

Mode2 = WDT pin goes high upon timeout of the watchdog timer.

Mode3 = Generate NMI upon timeout of the watchdog timer.

Enable Delay

The enable delay allows time for the OS to boot and the application to load and initialize. The unit is 1 sec.

Timeout Delay

The Timeout delay allows time for period of the watchdog timer. The unit is 0.1 sec.

Tls Auth Configuration

Aptio Setup - AMI	
Advanced	
► Server CA Configuration	Press <Enter> to configure Server CA.
► Client Cert Configuration	
	→←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
Version 2.21.1278. Copyright (C) 2021 American Megatrends, Inc.	

Server CA Configuration

Press <Enter> to configure Server CA.

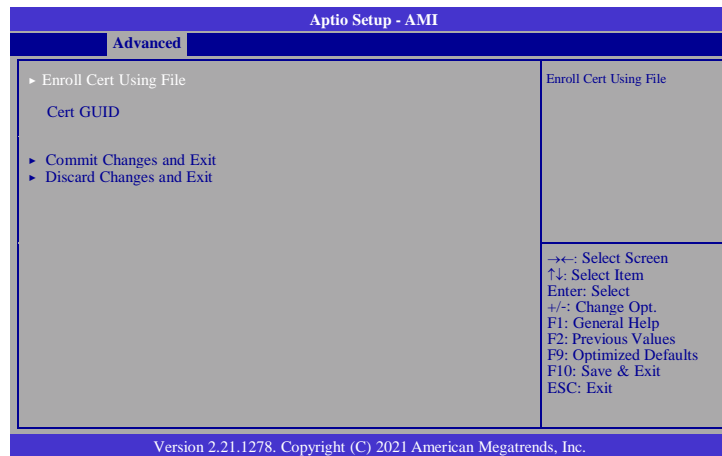
Enroll Cert

See next page.

Delete Cert

To delete cert.

RAM Disk Configuration



Enroll Cert Using File

Choose a cert file to enroll cert.

Cert GUID

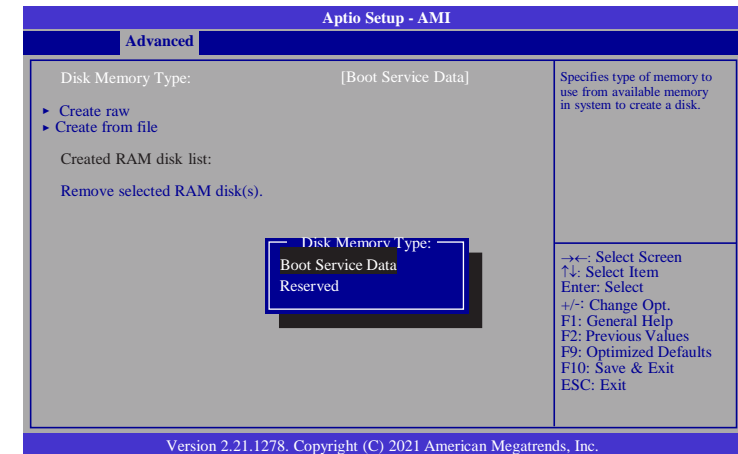
Input digit character in 11111111-2222-3333-4444-1234567 890ab format.

Commit Changes and Exit

Commit Changes and Exit

Discard Changes and Exit

Discard Changes and Exit



Disk Memory Type:

Specifies type of memory to use from available memory in system to create a disk.

Create raw

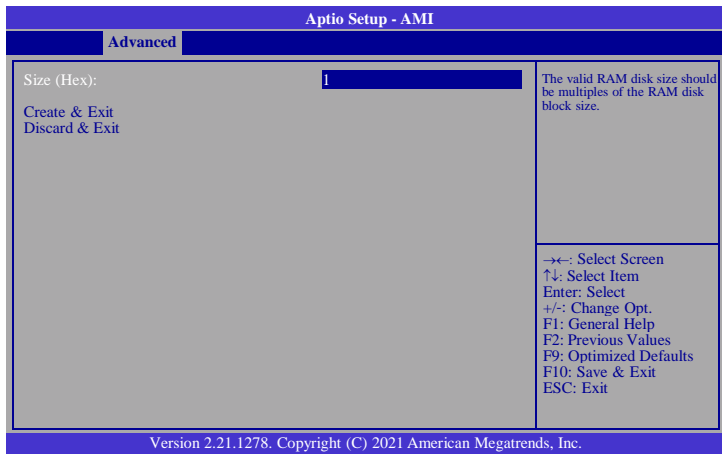
Create a raw RAM Disk. See next page.

Create from file

Create a RAM disk from saved file.

Remove selected RAM disk(s)

Remove RAM disk from system.



Size (Hex):

The valid RAM disk size should be multiples of the RAM disk block size.

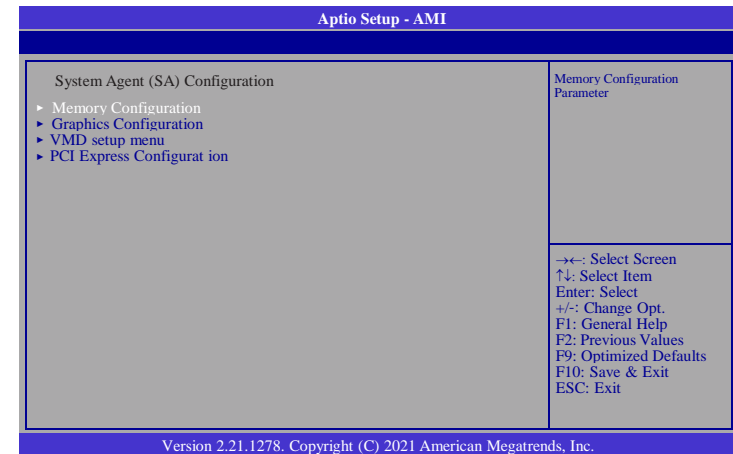
Create & Exit

Create the raw RAM Disk and exit.

Discard & Exit

Discard the change and exit.

System Agent (SA) Configuration



Memory Configuration

Memory Configuration Parameter.

Graphics Configuration

Settings about graphic.

VMD setup menu

VMD Configuration settings.

PCI Express Configuration

PCI Express Configuration settings.

Memory Configuration

Aptio Setup - AMI		
Chipset		
Memory Configuration		Maximum Value of TOLUD. Dynamic assignment would adjust TOLUD automatically based on largest MMIO length of installed graphic controller
Max TOLUD	[Dynamic]	
Enable RH Prevention	[Disabled]	
In-Band ECC Support	[Enabled]	
In-Band ECC Error Injection	[Disabled]	
In-Band ECC Operation Mode	[2]	
Memory Remap	[Enabled]	
		→←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
Version 2.21.1278. Copyright (C) 2021 American Megatrends, Inc.		

Max TOLUD

Maximum Value of TOLUD. Dynamic assignment would adjust TOLUD automatically based on largest MMIO length of installed graphic controller.

Enable RH Prevention

Actively prevent Row Hammer.

In-Band ECC Support

Enable/Disable In-Band ECC. Either the IBECC or the TME can be enabled.

In-Band ECC Error Injection

By enabling this Error Injection feature, the user acknowledges the security risks. Enabling Error Injection allows attackers who have access to the Host Operating System to inject IBECC errors that can cause unintended memory corruption and enable the leak of security data.

In-Band ECC Operation Mode

0: Functional Mode protects requests based on the address range 1:
Makes all requests non protected and ignore range checks
2: Makes all requests protected and ignore range checks

Enable RH Prevention

Enable/Disable Memory Remap above 4GB.

Graphics Configuration

Aptio Setup - AMI		
Chipset		
Graphics Configuration		Select which of IGFX/PEG/PCI Graphics device should be Primary Display Or select HG for Hybrid Gfx.
Primary Display	[Auto]	
Internal Graphics	[Auto]	
GTT Size	[8MB]	
Aperture Size	[256MB]	
DVMT Pre-Allocated	[60M]	
DVMT Total Gfx Mem	[256M]	
		→←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
Version 2.21.1278. Copyright (C) 2021 American Megatrends, Inc.		

Primary Display

Select which of IGFX/PEG/PCI Graphics device should be Primary Display Or select HG for Hybrid Gfx.

Internal Graphics

Keep IGFX enabled based on the setup options.

GTT Size

Select the GTT Size.

Aperture Size

Select the Aperture Size. Note : Above 4GB MMIO BIOS assignment is automatically enabled when selecting 2048MB aperture. To use this feature, please disable CSM Support.

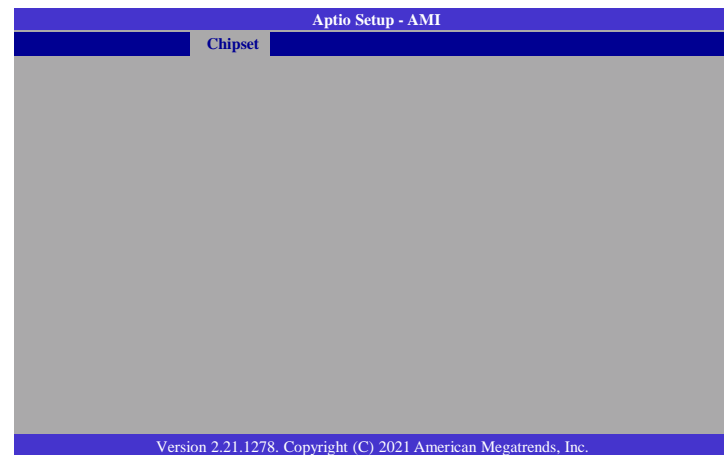
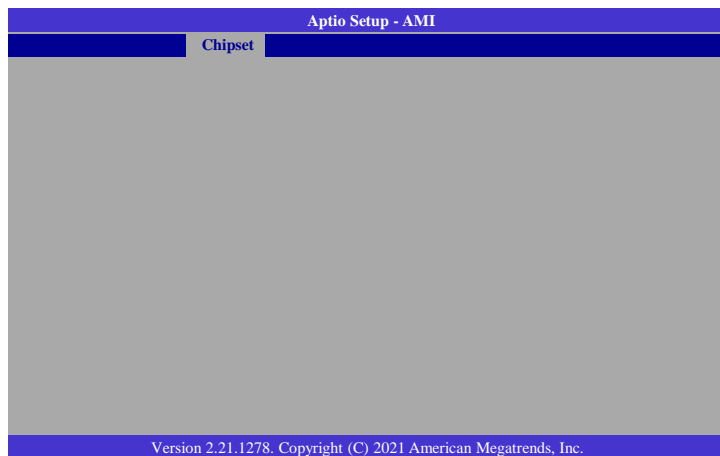
DVMT Pre-Allocated

Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.

DVMT Total Gfx Mem

Select DVMT5.0 Total Graphic Memory size used by the Internal Graphics Device.

VMD setup menu



Enable VMD controller

Enable/Disable to VMD controller.

Enable VMD Global Mapping

Enable/Disable to VMD Global Mapping

Map this Root Port under VMD

Map/UnMap this Root Port to VMD.

RAID0/1/5/10

To disable or enable RAID0/1/5/10.

Intel Rapid Recovery Technology

Enable/Disable Intel Rapid Recovery Technology.

RRT volumes can span internal and eSATA drives

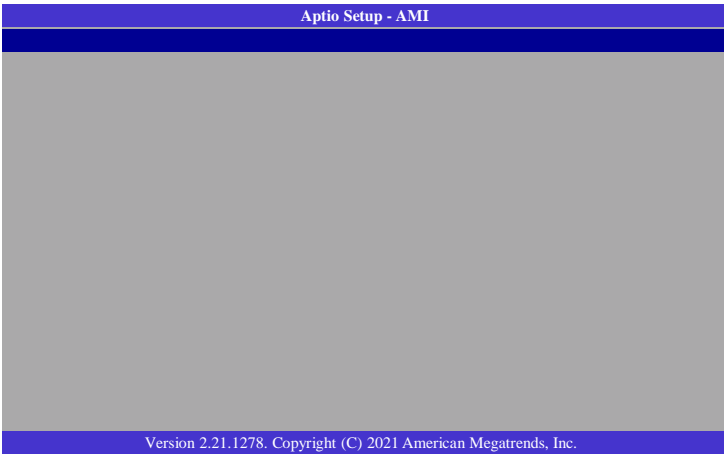
Enable/Disable RRT volumes can span internal and eSATA drives.

Intel(R) Optane(TM) Memory

Enable/Disable System Acceleration with Intel(R) Optane(TM) Memory feature.

PCI Express Configuration

This section configures settings relevant to PCI Express devices.

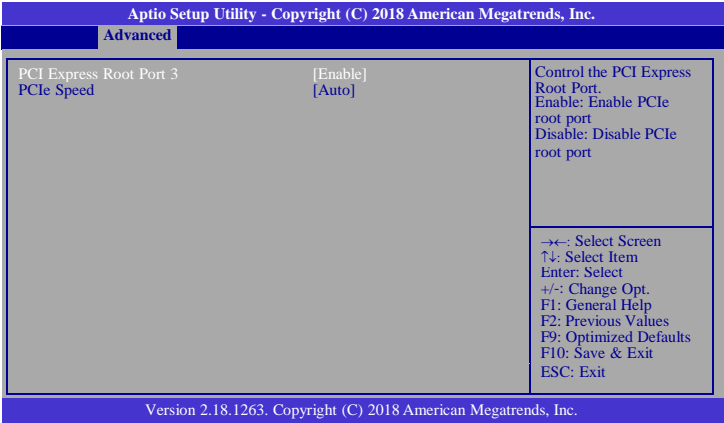


PCI Express Root Port

This field is used to enable or disable the PCI express root port.

PCIe Speed

Select the speed of the PCI Express root port.



SATA and RST Configuration

This section configures the SATA controller.

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.		
Advanced		
SATA and RST Configuration		Enables or Disables the Chipset SATA Controller.
SATA Controller(s)	[Enable]	
SATA Speed	[Auto]	
SATA Mode Selection	[AHCI]	
Software Feature Mask Configuration		
SATA Port 0	[Not Installed]	
Port 0	[Enabled]	
Hot Plug	[Disabled]	
SATA Port 1	[Not Installed]	
Port 1	[Enabled]	
Hot Plug	[Disabled]	
		→←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
Version 2.18.1263. Copyright (C) 2018 American Megatrends, Inc.		

SATA Controller

This field is used to enable or disable the Serial ATA controller.

SATA Speed

Select Serial ATA controller(s) speed.

SATA Mode Selection

The mode selection determines how the SATA controller(s) operates.

AHCI

This option allows the Serial ATA controller(s) to use AHCI (Advanced Host Controller Interface).

SATA Port 0 and 1/Hot Plug

Enable or disable the Serial ATA port and its hot plug function.

Software Feature Mask Configuration

RST Legacy OROM/RST UEFI driver will refer to the SWFM configuration to enable/disable the storage features.

Aptio Setup - AMI		
Software Feature Mask Configuration		
HDD Unlock	[Enabled]	If enabled, indicates that the HDD password unlock in the OS is enabled.
LED Locate	[Disabled]	
		→←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F9: Optimized Defaults F10: Save & Exit ESC: Exit
Version 2.21.1278. Copyright (C) 2021 American Megatrends, Inc.		

HDD Unlock

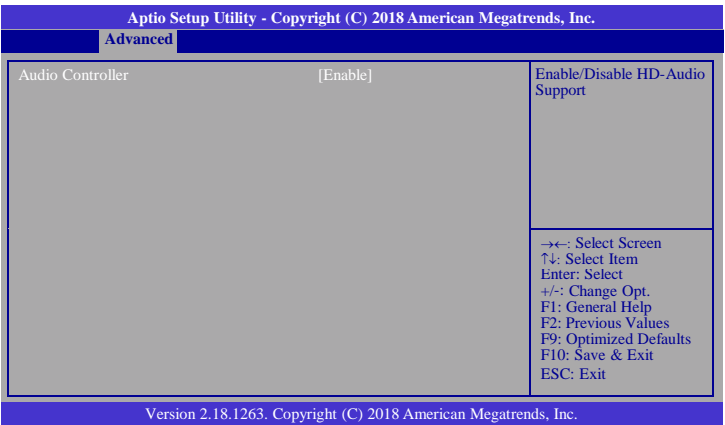
If enabled, indicates that the HDD password unlock in the OS is enabled.

LED Locate

If enabled, indicates that the LED/SGPIO hardware is attached and ping to locate feature is enabled on the OS.

HD Audio Configuration

This section configures the audio settings.



Audio Controller

Control the detection of the high-definition audio device.

Disable

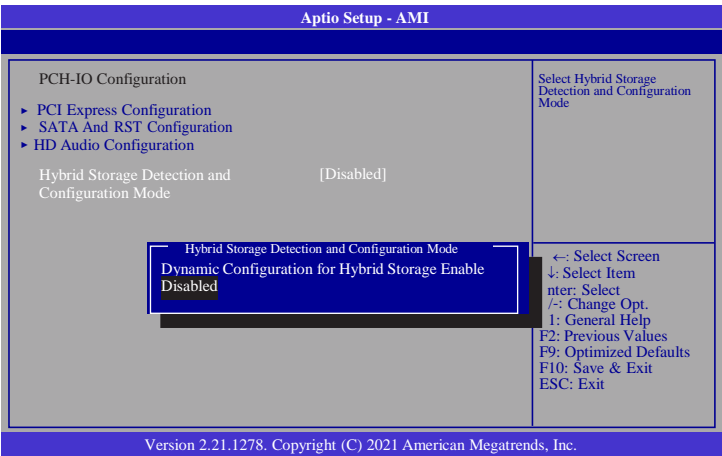
HD Audio will be disabled.

Enable

HD Audio will be enabled.

Hybrid Storage Detection and Configuration Mode

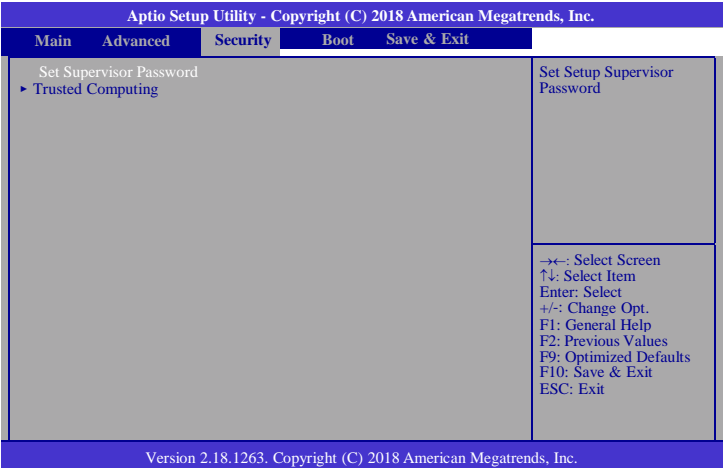
This section configures the Hybrid Storage Detection and Configuration Mode settings.



Hybrid Storage Detection and Configuration Mode

To enable or disable Hybrid Storage Detection and Configuration Mode.

Security

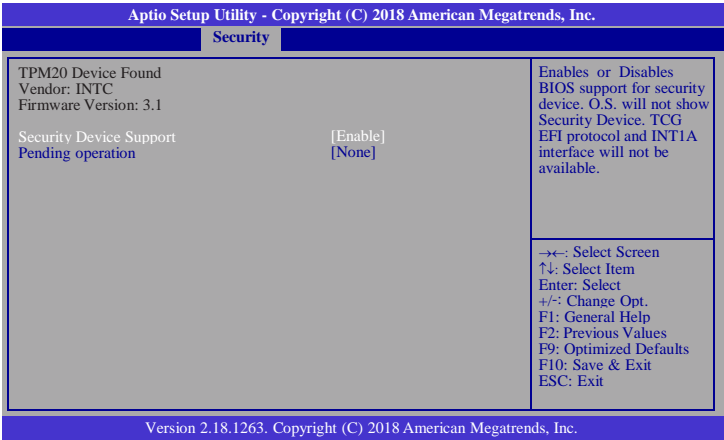


Set Supervisor Password

Set the supervisor password.

Trusted Computing

This section configures settings relevant to Trusted Computing innovations.



Security Device Support

Enables or Disables the BIOS support for the security device. O.S. will not show the security device. TCG EFI protocol and TNT1A interface will not be available.

Pending operation

Schedule an operation for the security device.

Note:
Your computer will reboot during restarting in order to change the security device state.

Boot

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.				
Main	Advanced	Security	Boot	Save & Exit
Setup Prompt Timeout		1		Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.
NumLock		[On]		
Quiet Boot		[Disabled]		
Network Stack		[Disabled]		
Boot Option Priorities				
Driver Option Priorities				

Setup Prompt Timeout

Select the number of seconds to wait for the setup activation key. 65535 (0xFFFF) denotes indefinite waiting.

NumLock

This allows you to determine the default state of the numeric keypad. By default, the system boots up with NumLock on wherein the function of the numeric keypad is the number keys. When set to Off, the function of the numeric keypad is the arrow keys.

Quiet Boot

This section is used to enable or disable quiet boot option.

Network Stack

This section is used to enable or disable UEFI network stack. When Network Stack is set to enabled, it will display Ipv4 PXE Support and Ipv6 PXE Support.

Aptio Setup Utility - Copyright (C) 2018 American Megatrends, Inc.				
Main	Advanced	Security	Boot	Save & Exit
Setup Prompt Timeout		1		Enable/Disable UEFI Ipv4 Ipv6 PXE Boot Support
NumLock		[On]		
Quiet Boot		[Disabled]		
Network Stack		[Enabled]		
Ipv4 PXE Support		[Enabled]		
Ipv6 PXE Support		[Disabled]		
Boot Option Priorities				
Driver Option Priorities				
Version 2.18.1263. Copyright (C) 2018 American Megatrends, Inc.				

Ipv4 PXE Support

When enabled, Ipv4 PXE boot supports. When disabled, Ipv4 PXE boot option will not be created.

Ipv6 PXE Support

When enabled, Ipv6 PXE boot supports. When disabled, Ipv6 PXE boot option will not be created.

Boot Option Priorities

Sets the system boot order.

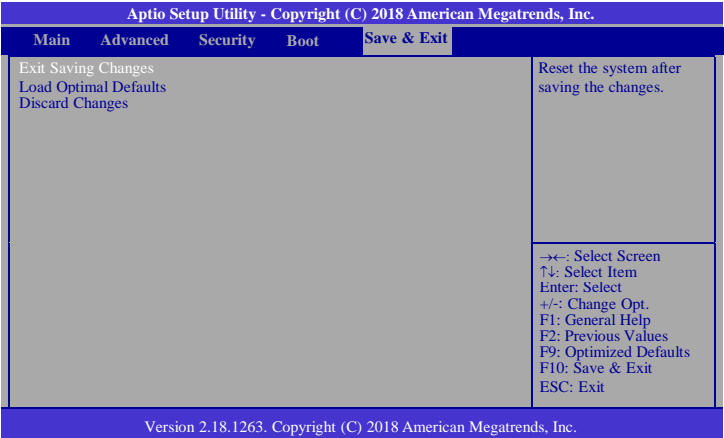
Driver Option Priorities

Sets the driver boot order.



Note:
TGU9A2 only supports UEFI boot, no Legacy boot.

Save & Exit



Exit Saving Changes

Select Yes and then press <Enter> to exit the system setup and save your changes.

Load Optimal Defaults

Select Yes and then press <Enter> to load optimal defaults.

Discard Changes

Select Yes and then press <Enter> to exit the system setup without saving your changes.

Updating the BIOS

To update the BIOS, you will need the new BIOS file and a flash utility. Please contact technical support or your sales representative for the files. For updating AMI BIOS in UEFI mode, you may refer to the how-to-video at <https://www.dfi.com/Knowledge/Video/5>.

Notice: BIOS SPI ROM

1. The Intel® Trusted Execution Engine has already been integrated into this system board. Due to the safety concerns, the BIOS (SPI ROM) chip cannot be removed from this system board and used on another system board of the same model.
2. The BIOS (SPI ROM) on this system board must be the original equipment from the factory and cannot be used to replace one which has been utilized on other system boards.
3. If you do not follow the methods above, the Intel® Trusted Execution Engine will not be updated and will cease to be effective.

Note:



- a. You can take advantage of flash tools to update the default configuration of the BIOS (SPI ROM) to the latest version anytime.
- b. When the BIOS IC needs to be replaced, you have to populate it properly onto the system board after the EEPROM programmer has been burned and follow the technical person's instructions to confirm that the MAC address should be burned or not.