RS720Q-E10-RS8U

2U Rackmount Server
User Guide

E18483
First Edition
July 2021

Contents

Contents

Contents

Contents

Safety information

Electrical Safety

- Before installing or removing signal cables, ensure that the power cables for the system unit and all attached devices are unplugged.
- To prevent electrical shock hazard, disconnect the power cable from the electrical outlet before relocating the system.
- When adding or removing any additional 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.
- If the power supply is broken, do not try to fix it by yourself. Contact a qualified service technician or your dealer.

Operation Safety

- Any mechanical operation on this server must be conducted by certified or experienced engineers.
- Before operating the server, carefully read all the manuals included with the server package.
- Before using the server, ensure all cables are correctly connected and the power cables are not damaged. If any damage is detected, contact your dealer as soon as possible.
- To avoid short circuits, keep paper clips, screws, and staples away from connectors, slots, sockets and circuitry.
- Avoid dust, humidity, and temperature extremes. Place the server on a stable surface.

This product is equipped with a three-wire power cable and plug for the user's safety. Use the power cable with a properly grounded electrical outlet to avoid electrical shock.

Restricted Access Location

This product is intended for installation only in a Computer Room where:

- Access can only be gained by SERVICE PERSONS or by USERS who have been instructed about the reasons for the restrictions applied to the location and about any precautions that shall be taken.
- Access is through the use of a TOOL, or other means of security, and is controlled by the authority responsible for the location.

Heavy System

CAUTION! This server system is heavy. Ask for assistance when moving or carrying the system.

Lithium-Ion Battery Warning

CAUTION: Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Avertissement sur les batteries Lithium-Ion

ATTENTION : Danger d'explosion si la batterie n'est pas correctement remplacée. Remplacer uniquement avec une batterie de type semblable ou équivalent, recommandée par le fabricant. Jeter les batteries usagées conformément aux instructions du fabricant.

About this guide

Audience

This user guide is intended for system integrators, and experienced users with at least basic knowledge of configuring a server.

Contents

This guide contains the following parts:

1. **Chapter 1: Product Introduction**

   This chapter describes the general features of the server, including sections on front panel and rear panel specifications.

2. **Chapter 2: Hardware Information**

   This chapter lists the hardware setup procedures that you have to perform when installing or removing system components.

3. **Chapter 3: Installation Options**

   This chapter describes how to install optional components into the barebone server.

4. **Chapter 4: Motherboard Information**

   This chapter gives information about the motherboard that comes with the server. This chapter includes the motherboard layout, jumper settings, and connector locations.

5. **Chapter 5: BIOS Information**

   This chapter tells how to change system settings through the BIOS Setup menus and describes the BIOS parameters.

6. **Chapter 6: Driver Installation**

   This chapter provides instructions for installing the necessary drivers for different system components.

Conventions

To ensure that you perform certain tasks properly, take note of the following symbols used throughout this manual.

DANGER/WARNING: Information to prevent injury to yourself when trying to complete a task.

CAUTION: Information to prevent damage to the components when trying to complete a task.

IMPORTANT: Instructions that you MUST follow to complete a task.

NOTE: Tips and additional information to help you complete a task.

Typography

Bold text	Indicates a menu or an item to select.
Italics	Used to emphasize a word or a phrase.
<Key>	Keys enclosed in the less-than and greater-than sign means that you must press the enclosed key. Example: <Enter> means that you must press the Enter or Return key.
<Key1>+<Key2>+<Key3>	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: <Ctrl>+<Alt>+<Del>
`Command`	Means that you must type the command exactly as shown, then supply the required item or value enclosed in brackets. Example: At the DOS prompt, type the command line: **`format A:/S`**

References

Refer to the following sources for additional information, and for product and software updates.

1. **ASUS Control Center (ACC) user guide**

   This manual tells how to set up and use the proprietary ASUS server management utility.

2. **ASUS websites**

   The ASUS websites provide updated information for all ASUS hardware and software products. Visit https://www.asus.com for more information.

1 Product Introduction

This chapter describes the general features of the chassis kit. It includes sections on front panel and rear panel specifications.

1.1 System package contents

Check your system package for the following items.

Model Name	RS720Q-E10-RS8U
Chassis	ASUS 2U Rackmount Chassis
Motherboard	ASUS Z12PH-16 Server Board
Component	2 x 3000W Power Supply
	2 x Front Panel Board (FPB-R2H-A)
	2 x Power Supply Distribution Board (PDB-R2H-B-3200)
	1 x Power Connection Board (PSB-R2H-A)
	1 x Backplane Board (BP8LE12G-25-R2H-B)
	2 x Midplane Board (MP4LE-D-R2H-D)
	4 x Converter Board (CB8LX12G-R2H-B)
	4 x PCIe Riser Card (RG16R-R2H-D)
	4 x M.2 PCIe Riser Card (RG4RG4L-M2X2-R2HC)
	2 x Backplane Fans (40mm x 28mm)
	4 x System Fans (80mm x 38mm)
	8 x Tool-less Hot-swap 2.5” Storage Bays
Accessories	1 x ASUS RS720Q-E10-RS8U Series Support DVD (includes User Guide)
	8 x CPU Standard Heatsinks
	4 x CPU Liquid Cooling Kits (optional)
	1 x Bag of Screws
	2 x AC Power Cables
	1 x Friction Rail Kit
	8 x LGA4189 CPU Carrier (Barebone)

If any of the above items is damaged or missing, contact your retailer.

1.2 Serial number label

Please take note of the product's serial number. The Serial number contains 12 characters such as xxSxxxxxxxxx similar to the figure shown below.

You need to provide the correct serial number to the ASUS Technical Support team member if you need assistance or, when requesting support.

1.3 System specifications

The ASUS RS720Q-E10-RS8U is a 2U server system featuring the ASUS Z12PH-D16 Server Board. The server supports 3rd Gen Intel® Xeon® Processor Scalable family plus other latest technologies through the chipsets onboard.

Model Name		RS720Q-E10-RS8U
Processor Support / System Bus		2 x Socket P+ (LGA4189) per Node 3rd Gen Intel® Xeon® Processor Scalable Family (Up to 205W for air cooling / Up to 270W for liquid cooling) UPI 11.2 GT/s
Core Logic		Intel® PCH C621A
Memory	Total Slots	16 (8-channel per CPU, 8 DIMM per CPU)
	Capacity	Maximum up to 3TB (Per Node)
	Memory Type	DDR4 3200/2933 RDIMM, LRDIMM, LR-DIMM 3DS (2DIMM per Channel) Intel® Optane™ DC persistent memory 200 Series (DCPMM) * **Refer to ASUS server AVL for the latest update**
	Memory Size	128GB, 64GB, 32GB, 16GB RDIMM 256GB, 128GB, 64GB RDIMM 3DS 128GB, 64GB, 32GB LR-DIMM 3DS 512GB, 256GB, 128GB Intel Optane™ DC persistent memory 200 Series (DCPMM) * **Refer to ASUS server AVL for the latest update**
Expansion Slots	Total PCI/ PCI-E Slots	1+1 per Node
	Slot Type	Per Node: 1 x PCI-E x16 (Gen4 x16 link), LP, HL (CPU1) 1 x OCP 3.0 Mezzanine (Gen4 x16 link) (CPU1)
	M.2	Per Node: 2 x M.2 (Up to 2280, PCIe 4.0 or SATA mode)
Storage Controller	SATA Controller	Per Node: Broadcom SAS3008 (Supports RAID 0, 1) - 2 x SAS 12Gb/s ports **or** - 2 x SATA 6Gb/s ports
	SAS Controller	Same as SATA controller
Storage	Storage Bay	Per System: - 8 x 2.5" Hot-swap Storage Bays (8 x SATA/SAS/NVMe) Per Node: - 2 x 2.5" Hot-swap Storage Bays (2 x SATA/SAS/NVMe)
Networking		Per Node: 1 x LAN Port Intel® I210-AT Gigabit LAN controller 1 x Management Port Optional OCP 3.0 Adapter: Up to 200Gb/s Ethernet / InfiniBand Adapter

(continued on the next page)

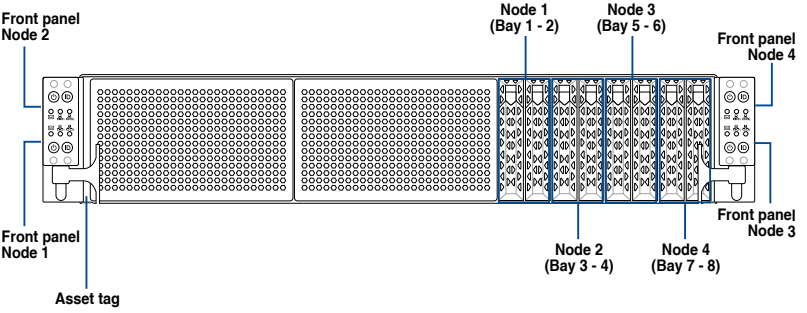
Model Name		RS720Q-E10-RS8U
VGA		Aspeed AST2600 64MB
Rear I/O Connectors		Per Node: 2 x USB 3.2 Gen 1 ports 1 x VGA port 1 x RJ-45 GbE LAN ports 1 x RJ-45 Mgmt LAN port
Switch/LED		Per Node: **Front:** - 1 x Power Switch/LED - 1 x Location Switch/LED - 1 x Message LED - 2 x LAN LED **Rear:** - 1 x Power Switch/LED - 1 x Q-Code/Port 80 LED
Management Solution	Software	ASUS Control Center (Classic)
	Out of Band Remote Management	On-Board ASMB10-iKVM for KVM-over-IP
OS support		Windows® Server 2019 Linux VMware VMMs
Regulatory Compliance		BSMI, CE, CB, FCC (ClassA)
Dimension		800mm x 444mm x 88mm(2U) 31.5” x 17.48” x 3.46”
Gross Weight Kg		41.5 kg
Net Weight Kg (CPU, DRAM, and HDD not included)		32.5 kg
Power Supply (following different configuration by region)		1+1 Redundant 3000W 80 PLUS Titanium Power Supply Rating: 220-240 Vac, 15.5A (x2), 50-60Hz, Class I, (3000W) (240Vdc Only for China)
Environment		Operation temperature: 10°C ~ 35°C (for <205W CPU, with air cooling) Operation temperature: 10°C ~ 30°C (for 205W CPU, with air cooling) Operation temperature: 10°C ~ 35°C (for >205W CPU, with liquid cooling) Non operation temperature: -40°C ~ 60°C Non operation humidity: 20% ~ 90% (Non condensing)

Specifications are subject to change without notice.

1.4 Front panel features

The barebone server displays easily accessible features such as the power and reset buttons, LED indicators, and optical drive.

Refer to the **Front panel LEDs** section for the LED descriptions.



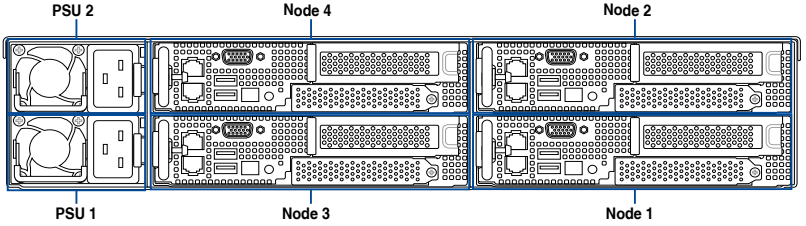
Turn off the system power and detach the power supply before removing or replacing any system component.

Asset tag

The Asset tag is a small polyester film located on the right side of the server's front panel. It provides information about the server such as asset barcode or serial number and is useful in asset tracking and inventory management.

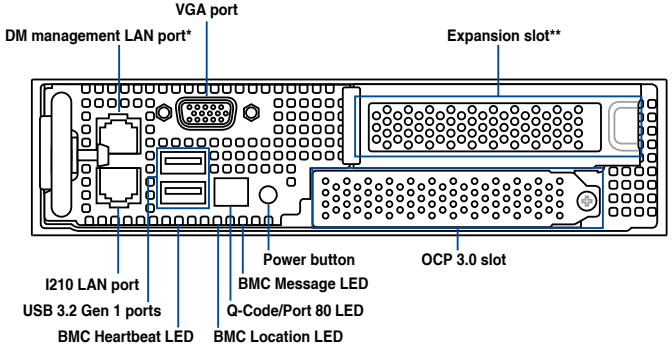
1.5 Rear panel features

RS720Q-E10-RS8U



When installing only two nodes, install the nodes to node slot number 1 and 3 or number 2 and 4.

Z12PH-D16 (Node)

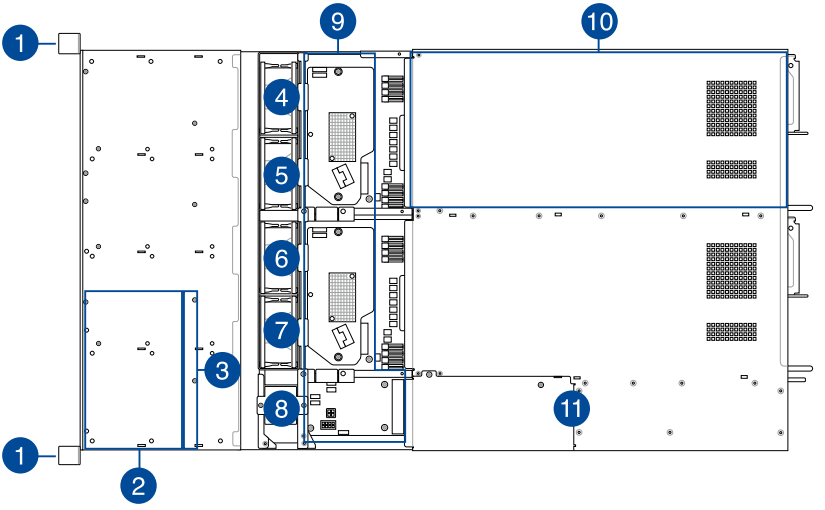


* This port is for ASUS ASMB10-iKVM controller and for technicians only.

** The expansion slot will be reserved for the liquid cooling module if your model comes with a liquid cooling module.

1.6 Internal features

The barebone server includes the basic components as shown.



1. Front LED Boards
2. Hot-swap storage device trays
3. Backplane
4. System fan (SYS_FAN1)
5. System fan (SYS_FAN2)
6. System fan (SYS_FAN3)
7. System fan (SYS_FAN4)
8. BP_FAN1 (top) and BP_FAN2 (bottom)
9. SATA/SAS/NVMe Mid-plane
10. ASUS Z12PH-16 Server Board
11. Power supply and power fan

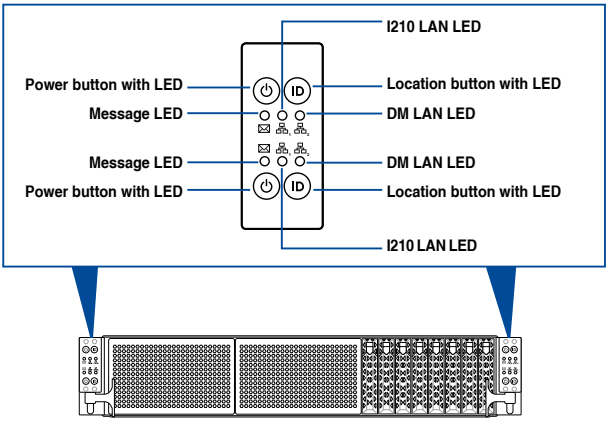
Ensure that the air duct is positioned on the gaps between the memory slots.

Turn off the system power and detach the power supply before removing or replacing any system component.

*WARNING
HAZARDOUS MOVING PARTS
KEEP FINGERS AND OTHER BODY PARTS AWAY

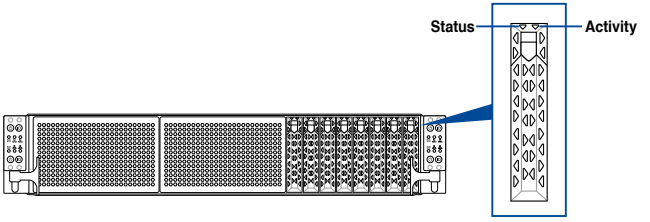
1.7 LED information

1.7.1 Front panel LEDs



LED	Icon	Display status	Description
Power LED		ON	System power ON
Message LED		OFF	System is normal; no incoming event
		ON	A hardware monitor event is indicated
LAN LEDs		OFF	No LAN connection
		Blinking	LAN is transmitting or receiving data
		ON	LAN connection is present
Location LED	ID	ON	Location switched is pressed
		OFF	Normal status (Press the location switch again to turn off.)

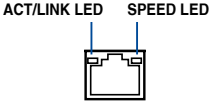
1.7.2 HDD status LEDs



Storage Device LED Description		
Status (RED)	ON	Storage device has failed
	Blinking	RAID rebuilding or locating
Activity (GREEN)	ON	Storage device power ON
	Blinking	Read/write data from/into the SATA/SAS storage device
	OFF	Storage device not found

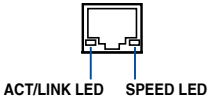
1.7.3 LAN (RJ-45) LEDs

Dedicated Management LAN port (DM_LAN1) LED indications



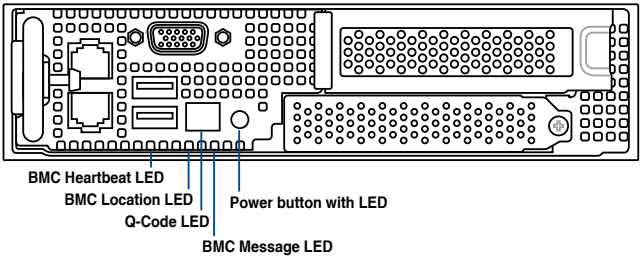
ACT/LINK LED		SPEED LED	
Status	Description	Status	Description
OFF	No link	OFF	10 Mbps connection
GREEN	Linked	ORANGE	100 Mbps connection
BLINKING	Data activity	GREEN	1 Gbps connection

Intel® I210-AT 1G LAN port LEDs



ACT/LINK LED		SPEED LED	
Status	Description	Status	Description
OFF	No link	OFF	10 Mbps connection
GREEN	Linked	ORANGE	100 Mbps connection
BLINKING	Data activity	GREEN	1 Gbps connection

1.7.4 Rear panel LEDs



LED	Display status	Description
Power LED	ON	System power ON
BMC Heartbeat LED	Blinking	BMC is operating normally
BMC Location LED	OFF	System is normal; no incoming event
	ON	A hardware monitor event is indicated
BMC Message LED	OFF	System is normal; no incoming event
	ON	A hardware monitor event is indicated

1.7.5 Q-Code table

Action	PHASE	POST CODE	TYPE	DESCRIPTION
Normal boot	Security Phase	01	Progress	First post code(POWER_ON_POST_CODE)
		02	Progress	Load BSP microcode(MICROCODE_POST_CODE)
		03	Progress	Set cache as ram for PEI phase(CACHE_ENABLED_POST_CODE)
		06	Progress	CPU Early init.(CPU_EARLY_INIT_POST_CODE)
		04	Progress	initializes South bridge for PEI preparation
	PEI(Pre-EFI initialization) phase	10	Progress	PEI Core Entry
		15	Progress	NB initialize before installed memory
		19	Progress	SB initialize before installed memory
		78~00	Progress	Wait BMC ready(duration: 120 seconds).
		A1	MRC Progress	QPI initialization
		A3	MRC Progress	QPI initialization
		A7	MRC Progress	QPI initialization
		A8	MRC Progress	QPI initialization
		A9	MRC Progress	QPI initialization
		AA	MRC Progress	QPI initialization
		AB	MRC Progress	QPI initialization
		AC	MRC Progress	QPI initialization
		AD	MRC Progress	QPI initialization
		AE	MRC Progress	QPI initialization
		AF	MRC Progress	QPI initialization Complete
		2F	Progress	Memory Init.
		B0	MRC Progress	Memory Init.
		B1	MRC Progress	Memory Init.
		AF	MRC Progress	RC Reset if require
		B4	MRC Progress	Memory Init.
		B2	MRC Progress	Memory Init.
		B3	MRC Progress	Memory Init.
		B5	MRC Progress	Memory Init.
		B6	MRC Progress	Memory Init.
		B7	MRC Progress	Memory Init.
		B8	MRC Progress	Memory Init.
		B9	MRC Progress	Memory Init.
		BA	MRC Progress	Memory Init.

(continued on the next page)

Action	PHASE	POST CODE	TYPE	DESCRIPTION
Normal boot	PEI(Pre-EFI initialization) phase	BB	MRC Progress	Memory Init.
		BC	MRC Progress	Memory Init.
		BF	MRC Progress	Memory Init. Done
		5A	MRC Progress	Other config. After RC end
		31	Progress	Memory already installed.
		32	Progress	CPU Init.
		34	Progress	CPU Init.
		36	Progress	CPU Init.
		4F	Progress	DXE Initial Program Load(IPL)
	DXE(Driver Execution Environment) phase	60	Progress	DXE Core Started
		61	Progress	DXE NVRAM Init.
		62	Progress	SB run-time init.
		63	Progress	DXE CPU Init
		68	Progress	NB Init.
		69	Progress	NB Init.
		6A	Progress	NB Init.
		70	Progress	SB Init.
		71	Progress	SB Init.
		72	Progress	SB Init.
		78	Progress	ACPI Init.
		79	Progress	CSM Init.
	BDS(Boot Device Selection) phase	90	Progress	BDS started
		91	Progress	Connect device event
		92	Progress	PCI Bus Enumeration.
		93	Progress	PCI Bus Enumeration.
		94	Progress	PCI Bus Enumeration.
		95	Progress	PCI Bus Enumeration.
		96	Progress	PCI Bus Enumeration.
		97	Progress	Console outout connect event
		98	Progress	Console input connect event
		99	Progress	AMI Super IO start
		9A	Progress	AMI USB Driver Init.
		9B	Progress	AMI USB Driver Init.
		9C	Progress	AMI USB Driver Init.
		9D	Progress	AMI USB Driver Init.
		b2	Progress	Legacy Option ROM Init.
		b3	Progress	Reset system
		b4	Progress	USB hotplug
		b6	Progress	NVRAM clean up
		b7	Progress	NVRAM configuration reset
		A0	Progress	IDE, AHCI Init.
		A1	Progress	IDE, AHCI Init.
		A2	Progress	IDE, AHCI Init.
		A3	Progress	IDE, AHCI Init.
		A8	Progress	BIOS Setup Utility password verify
		A9	Progress	BIOS Setup Utility start
		AB	Progress	BIOS Setup Utility input wait
		AD	Progress	Ready to boot event
		AE	Progress	Legacy boot event
	Operating system phase	AA	Progress	APIC mode
		AC	Progress	PIC mode

Hardware Information

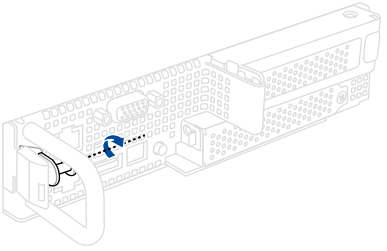
2

This chapter lists the hardware setup procedures that you have to perform when installing or removing system components.

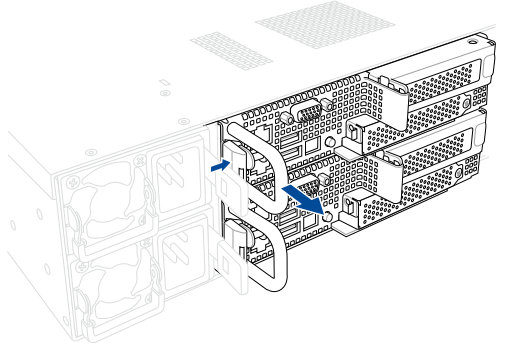
2.1 Server node

2.1.1 Removing a server node

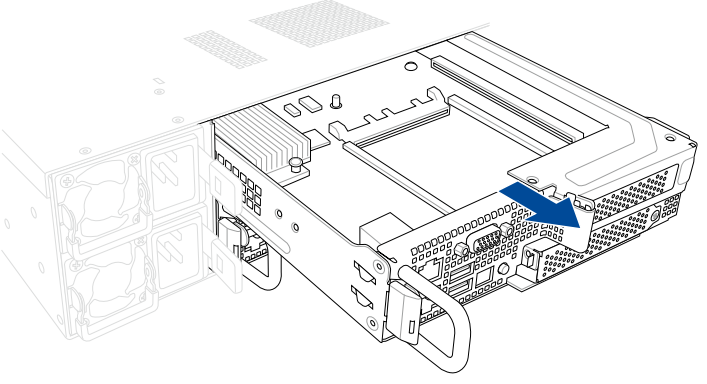
1. Remove the screw located on the node latch.



2. Hold the server node lever and press the green node latch.



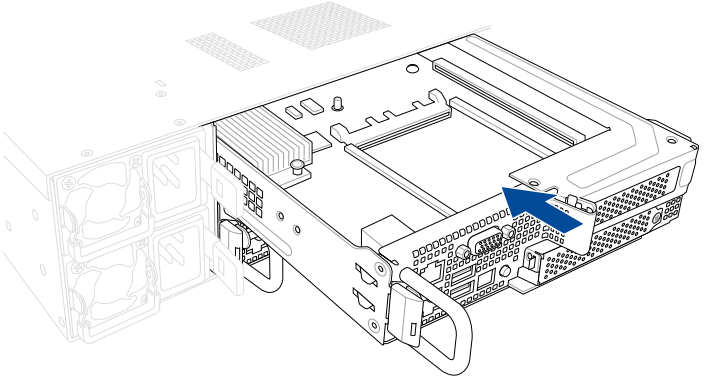
3. Firmly pull the server node out of the server chassis.



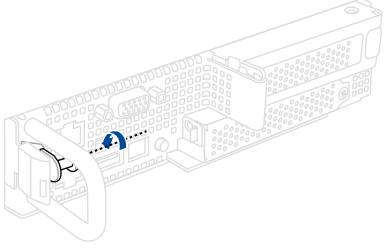
2.1.2 Installing a server node

When installing only two nodes, install the nodes to node slot number 1 and 3 or number 2 and 4. Refer to section **1.5 Rear panel features** for details.

1. Align the node with the node slot on the chassis, then push the node all the way into the node slot.



2. Secure the node latch using the screw previously removed.

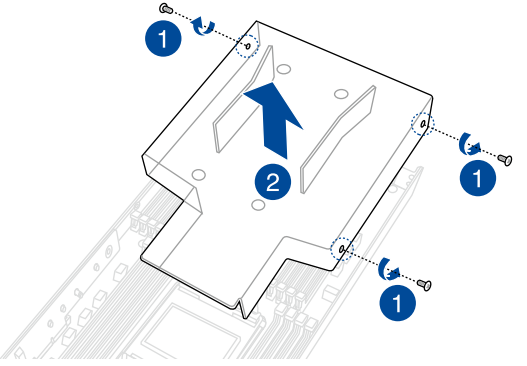


2.2 Air Duct

The RS720Q-E10-RS8U server system comes with a motherboard fan air duct to enable better air flow inside the motherboard while the system is running.

2.2.1 Removing the air duct

1. Remove the three (3) screws securing the air duct on the left and right of the node chassis.
2. Carefully lift the air duct out of the chassis.



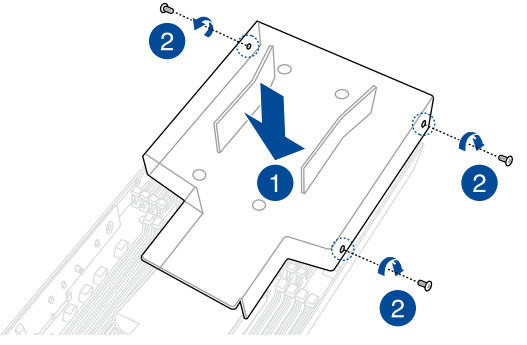
2.2.2 Installing the air duct

1. Position the air duct on top of the motherboard then carefully fit it on top of the motherboard. Refer to the following illustration for the correct orientation of the air duct.

Insert the air duct on the gaps between the memory slots.

Ensure that the air duct is firmly fitted to the motherboard.

2. Secure the air duct using the three (3) screws removed previously.



2.3 Central Processing Unit (CPU)

The motherboard comes with a surface mount LGA 4189 socket designed for the 3rd Gen Intel® Xeon® Processor Scalable Family processors.

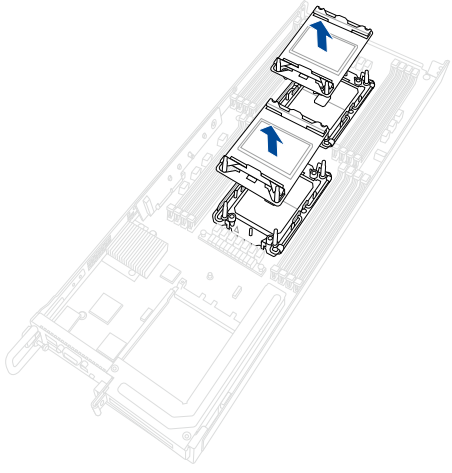
- Upon purchase of the motherboard, ensure that the PnP cap is on the socket and the socket contacts are not bent. Contact your retailer immediately if the PnP cap is missing, or if you see any damage to the PnP cap/socket contacts/motherboard components. ASUS will shoulder the cost of repair only if the damage is shipment/transit-related.
- Keep the cap after installing the motherboard. ASUS will process Return Merchandise Authorization (RMA) requests only if the motherboard comes with the cap on the LGA 4189 socket.
- The product warranty does not cover damage to the socket contacts resulting from incorrect CPU installation/removal, or misplacement/loss/incorrect removal of the PnP cap.

2.3.1 Installing the CPU and heatsink

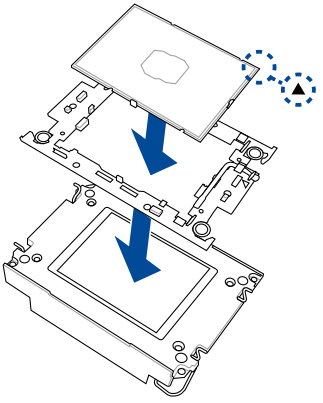
To install a CPU:

1. Remove the server node. For more information, see the section **Removing a server node**.
2. Remove the air duct. For more information, see the section **Removing the air duct**.
3. Remove the PnP caps from the CPU sockets.

Keep the PnP cap. ASUS will process Return Merchandise Authorization (RMA) requests only if the motherboard comes with the PnP cap on the LGA 3647 socket.



4. Attach the CPU to the carrier bracket, ensure the triangle mark is on the same side as the bracket lever, then attach the CPU and carrier bracket to the heatsink.

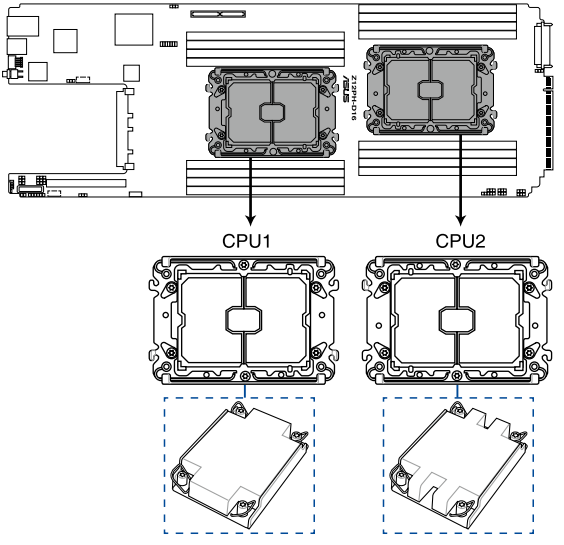


5. Align the CPU and heatsink assembly in the correct orientation so that the triangle marks on both the CPU and socket are aligned in the same direction, then place the heatsinks on top of the CPU sockets.

The CPU and CPU Carrier fits in only one correct orientation. DO NOT force the CPU and CPU Carrier into the socket to prevent damaging the CPU pins on the socket.

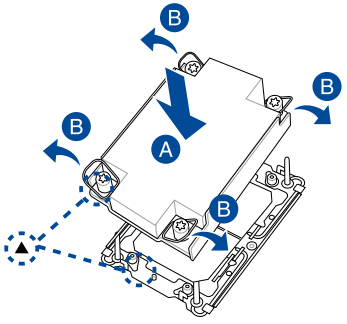
The heatsink for RS720Q-E10-RS8U differs between CPU1 and CPU2, please refer to the illustration below for more information on the heatsink and the corresponding CPU socket.

Z12PH-D16 CPU LGA 4189 Socket



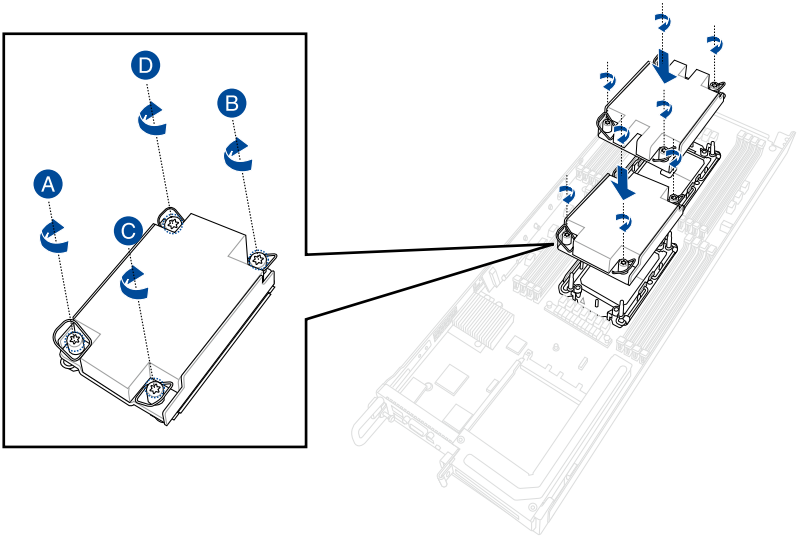
6. Once the heatsink is placed on top of the CPU socket (A). Push the lock latches outwards on all four corners of the heatsink so that the heatsink and CPU assembly is secured to the CPU socket (B).

Ensure the triangle mark on the CPU is located in the same corner as the CPU socket.



7. Do two (2) clockwise turns on each of the heatsink screws in the cross order pattern shown on the illustration until the heatsink screws are tightened and the heatsink is secured onto the motherboard.

Intel® recommends a using a torque driver with a T-30 bit and a torque value of 8 lbf-in to prolong the longetivity of all PEEK nuts after the quality of the load post is corrected.



8. Reinstall the air duct. For more information, see the section **Installing the air duct**.
9. Reinstall the server node. For more information, see the section **Installing a server node**.

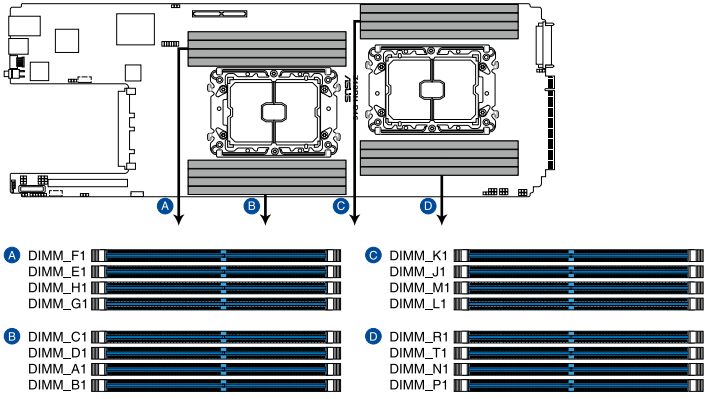
2.4 System memory

2.4.1 Overview

The motherboard comes with twelve (12) Double Data Rate 4 (DDR4) Dual Inline Memory Modules (DIMM) sockets.

The figure illustrates the location of the DDR4 DIMM sockets:

Z12PH-D16 288-pin DDR4 DIMM sockets



2.4.2 Memory Configurations

You may install 16GB, 32GB, 64GB, 128GB RDIMMs; 64GB, 128GB, 256GB RDIMM 3DS; 32GB, 64GB, 128GB LR-DIMM 3DS; or 128GB, 256GB, 258GB Intel® Optane™ DC persistent memory 200 Series (DCPMM) into the DIMM sockets using the memory configurations in this section.

- Refer to ASUS Server AVL for the updated list of compatible DIMMs.
- Always install DIMMs with the same CAS latency. For optimum compatibility, it is recommended that you obtain memory modules from the same vendor.

Dual CPU configuration

You can refer to the following recommended memory population for a dual CPU configuration.

Dual CPU configuration																
	A1	B1	C1	D1	E1	F1	G1	H1	J1	K1	L1	M1	N1	P1	R1	T1
2 DIMMs	✓				✓											
4 DIMMs	✓				✓				✓				✓			
8 DIMMs	✓		✓		✓		✓		✓		✓		✓		✓	
12 DIMMs	✓	✓	✓		✓	✓	✓		✓	✓	✓		✓	✓	✓	
16 DIMMs	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

If you wish to install PMem as well, please refer to the following tables for configurations

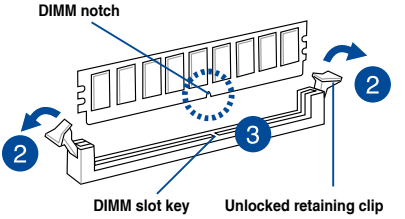
Channel	F	E	H	G	CPU	C	D	A	B
DDR4+BPS	DIMM_F1	DIMM_E1	DIMM_H1	DIMM_G1		DIMM_C1	DIMM_D1	DIMM_A1	DIMM_B1
4+4 (POR/Validated)	BPS	DDR4	BPS	DDR4		DDR4	BPS	DDR4	BPS
	DDR4	BPS	DDR4	BPS		BPS	DDR4	BPS	DDR4
6+1 (POR/Validated)	DDR4	DDR4		DDR4		DDR4	BPS	DDR4	DDR4
		DDR4	DDR4	DDR4		DDR4	DDR4	DDR4	BPS
	DDR4	DDR4	BPS	DDR4		DDR4		DDR4	DDR4
	BPS	DDR4	DDR4	DDR4		DDR4	DDR4	DDR4	
6+1 (POR*)	DDR4	DDR4	DDR4			BPS	DDR4	DDR4	DDR4
	DDR4		DDR4	DDR4		DDR4	DDR4	BPS	DDR4
	DDR4	DDR4	DDR4	BPS			DDR4	DDR4	BPS
	DDR4	BPS	DDR4	DDR4		DDR4	DDR4		DDR4

* **These configurations are POR (allowed by BIOS).**

2.4.3 Installing a DIMM

Ensure to unplug the power supply before adding or removing DIMMs or other system components. Failure to do so may cause severe damage to both the motherboard and the components.

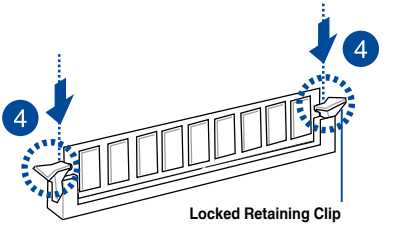
1. Unlock a DIMM socket by pressing the retaining clips outward.
2. Align a DIMM on the socket such that the notch on the DIMM matches the DIMM slot key on the socket.



A DIMM is keyed with a notch so that it fits in only one direction. DO NOT force a DIMM into a socket in the wrong direction to avoid damaging the DIMM.

3. Hold the DIMM by both of its ends then insert the DIMM vertically into the socket. Apply force to both ends of the DIMM simultaneously until the retaining clips snaps back into place.

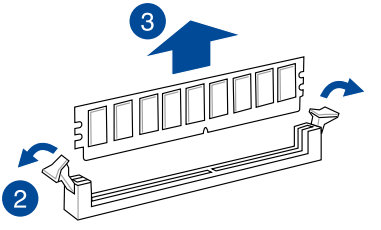
   Ensure that the DIMM is sitting firmly on the DIMM slot.



Always insert the DIMM into the socket VERTICALLY to prevent DIMM notch damage.

2.4.4 Removing a DIMM

1. Remove the chassis cover. For more information, see the section **Chassis cover**.
2. Simultaneously press the retaining clips outward to unlock the DIMM.
3. Remove the DIMM from the socket.



Support the DIMM lightly with your fingers when pressing the retaining clips. The DIMM might get damaged when it flips out with extra force.

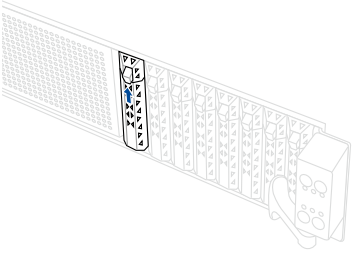
2.5 Storage devices

The system supports two (2) hot-swap storage devices per node. The storage device installed on the drive tray connects to the Midplane via the backplane.

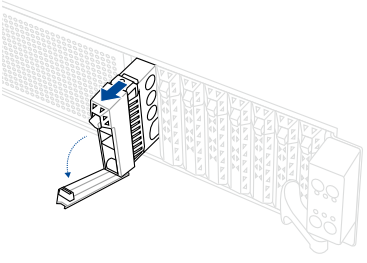
2.5.1 Installing a 2.5” hot-swap SATA/SAS/NVMe storage device

Ensure that the storage devices installed correspond to the correct node. For more information on the nodes and the storage bays, please refer to **1.4 Front panel features** and **1.5 Rear panel features**.

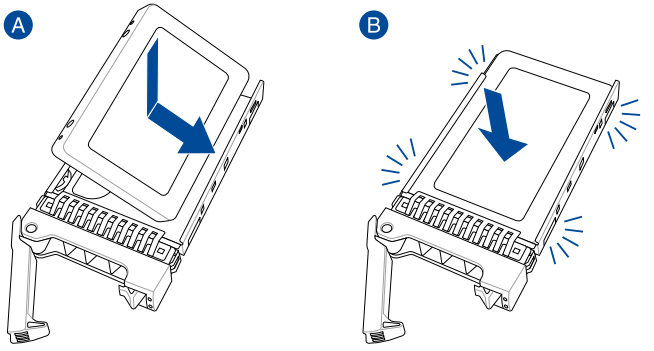
1. Press the spring lock to release the tray lever and to partially eject the tray from the bay.



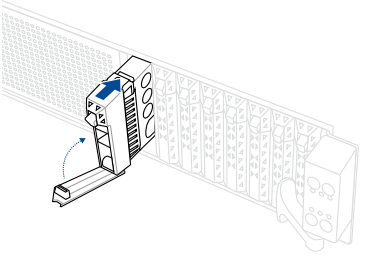
2. Firmly hold the tray lever and carefully pull the drive tray out of the bay.



3. Place the 2.5” storage device into the tray until it clicks into place.



4. Align and insert the 2.5-inch storage device and drive tray assembly into the drive bay.

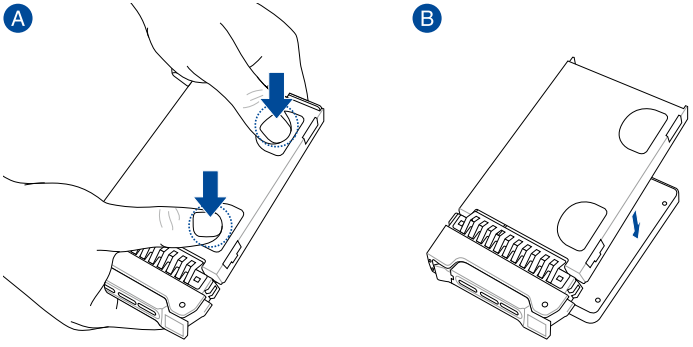


5. Repeat steps 1-4 to install the other 2.5-inch storage devices.

2.5.2 Removing a 2.5” hot-swap SATA/SAS/NVMe storage device

1. Follow steps 1 and 2 of the **Installing a 2.5” hot-swap SATA/SAS/NVMe storage device** section to remove the drive tray.
2. Push the 2.5” storage device through the openings on the bottom of the tray until the 2.5” storage device pops out of the tray.

DO NOT touch the circuit board on the 2.5” storage device. Ensure to push the 2.5” storage device through the opening on the bottom of the tray.



3. Follow step 4 of the **Installing a 2.5” hot-swap SATA/SAS/NVMe storage device** section to install the storage device and drive tray assembly into the drive bay.

2.6 Expansion slots

The following subsections describe the slots and expansion cards that they support.

Ensure to unplug the power cord before adding or removing expansion cards. Failure to do so may cause you physical injury and damage motherboard components.

2.6.1 The PCI Express riser card

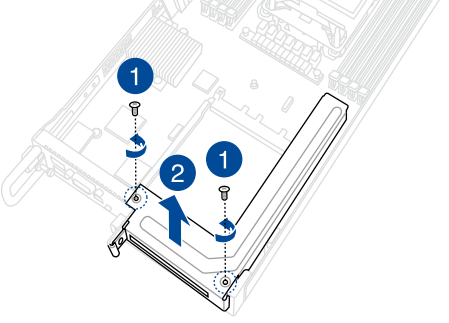
The onboard PCI Express slot on the motherboard comes pre-installed with a riser card that supports one x16 slot (Gen3 x16 link) for installing PCI-E x16 low profile cards.

You can only install a PCIe expansion card with the air cooling configuration. The liquid cooling module will occupy this slot if your model comes with the liquid cooling module.

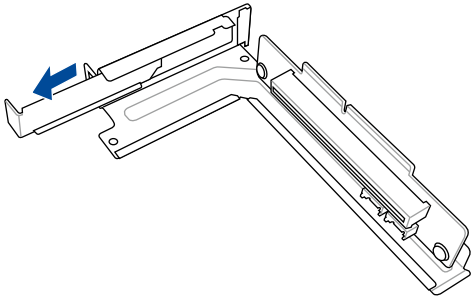
To install PCI-E expansion cards to the riser card:

1. Remove the two (2) screws securing the riser card to the chassis.
2. Firmly hold the riser card then pull it up to detach it from the PCIe x16 slot on the motherboard.

Ensure to remove the air duct before removing the riser card. Please refer to **Removing the air duct** section for more information.



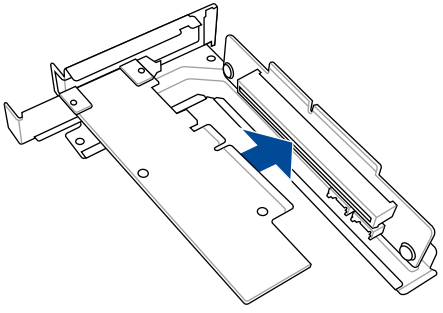
3. Remove the metal bracket from the riser card.



4. Prepare the expansion card.

Before installing an expansion card, read the documentation that came with it and ensure to make the necessary hardware settings.

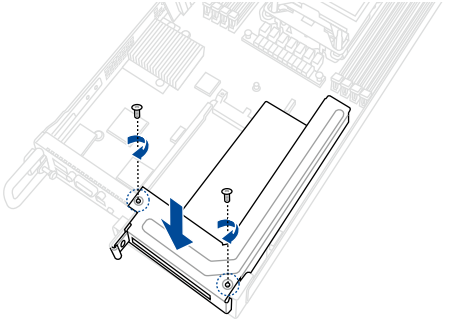
5. Align and insert the golden finger connectors of the expansion card to the PCIe slot connector on the riser card as shown.



6. Align and insert the riser card and expansion card assembly into the PCIe slot on the motherboard.

The expansion card fits in one orientation only. If it does not fit, try reversing it.

7. Secure the riser card with the screws that you removed earlier in step 1.

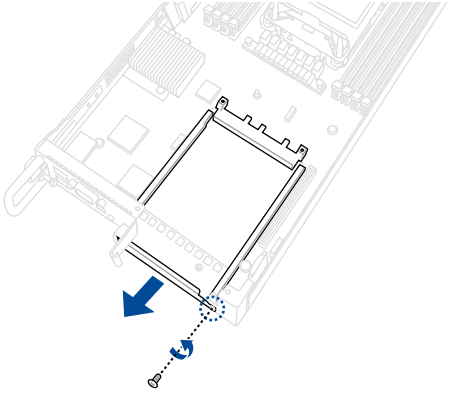


2.6.2 Installing OCP 3.0 card

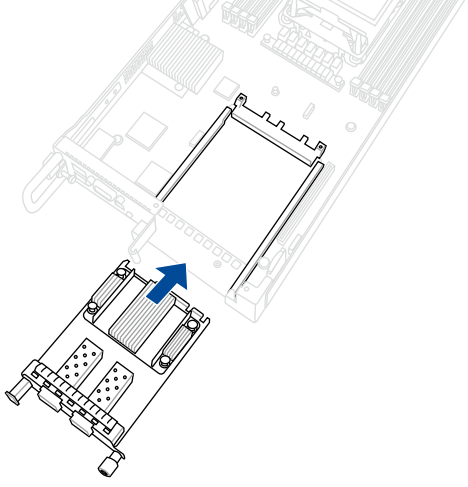
The illustrations in this section are for reference only. The OCP 3.0 card may differ depending on the OCP 3.0 you purchased.

The OCP 3.0 slot does not support hot-plug, if you wish to install or remove the OCP 3.0 card, ensure to power off the system before installing or removing the OCP 3.0 card.

1. Remove the screw on the metal bracket, then remove the metal bracket.



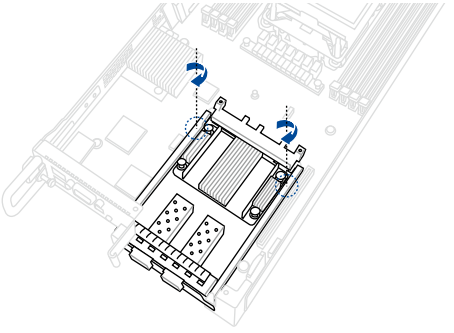
2. Prepare OCP 3.0 card.
3. Align the OCP 3.0 card to the rails on the OCP 3.0 slot, then slide the OCP 3.0 card all the way into the OCP 3.0 slot.



4. Secure the OCP 3.0 card to the OCP 3.0 slot. This may differ depending on the OCP 3.0 card installed, please refer to the following:

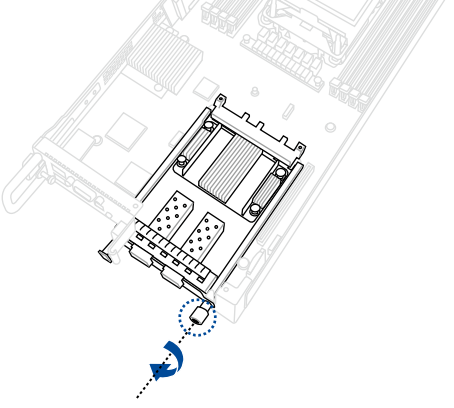
Internal lock OCP 3.0 card

Secure the OCP 3.0 card to the OCP 3.0 slot using the bundled two (2) screws.



External lock OCP 3.0 card

Secure the OCP 3.0 card using the thumbscrew.



2.6.3 Configuring an expansion card

After installing the expansion card, configure it by adjusting the software settings.

1. Turn on the system and change the necessary BIOS settings, if any. See Chapter 5 for information on BIOS setup.
2. Assign an IRQ to the card. Refer to the **Standard Interrupt assignments** table for more information.
3. Install the software drivers for the expansion card.

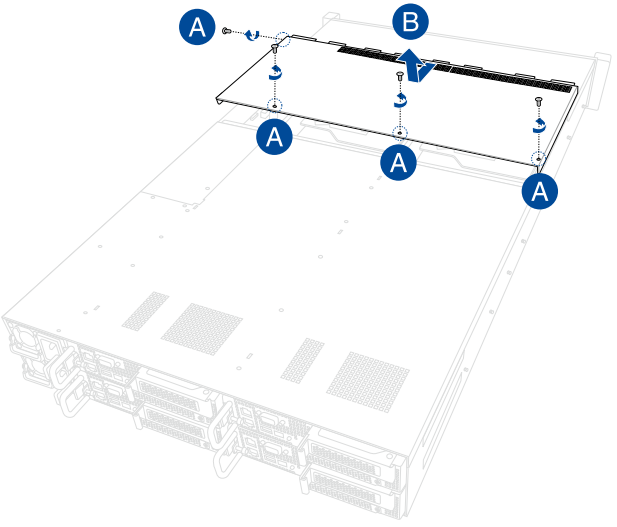
Standard Interrupt assignments

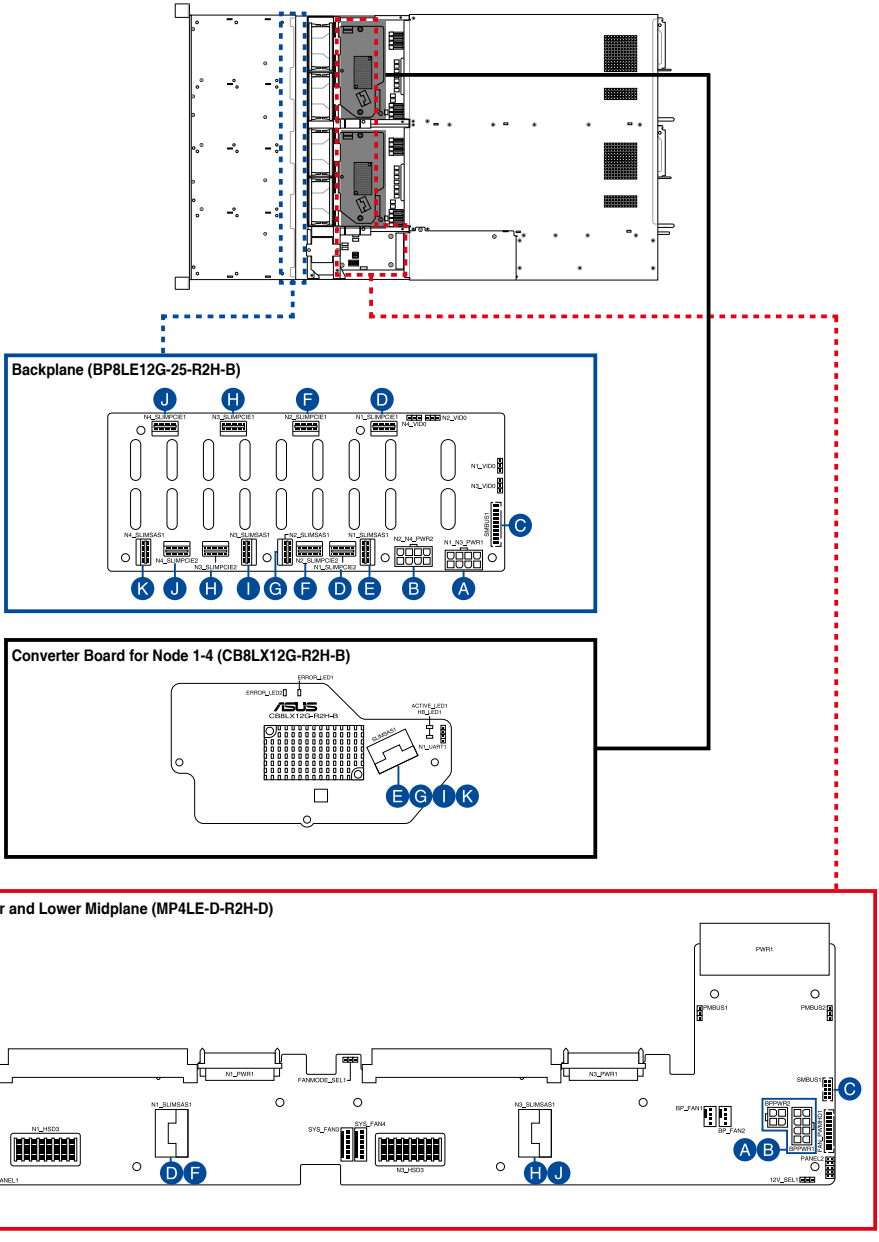
IRQ	Priority	Standard function
0	1	System Timer
1	2	Keyboard Controller
2	-	Programmable Interrupt
3*	11	Communications Port (COM2)
4*	12	Communications Port (COM1)
5*	13	--
6	14	Floppy Disk Controller
7*	15	--
8	3	System CMOS/Real Time Clock
9*	4	ACPI Mode when used
10*	5	IRQ Holder for PCI Steering
11*	6	IRQ Holder for PCI Steering
12*	7	PS/2 Compatible Mouse Port
13	8	Numeric Data Processor
14*	9	Primary IDE Channel
15*	10	Secondary IDE Channel

*** These IRQs are usually available for ISA or PCI devices.**

2.7 Backplane and Midplane cabling

Remove the top cover before configuring the backplane and midplane cabling, by removing the four (4) screws securing the top cover (A), then push the top cover towards the rear of the system and remove the top cover (B).




Backplane (BP8LE12G-25-R2H-B)
J
H
F
D
C
K
J
H
I
G
F
D
E
B
A
Converter Board for Node 1-4 (CB8LX12G-R2H-B)
E
G
I
K
Upper and Lower Midplane (MP4LE-D-R2H-D)
PWR1
C
A
B
D
F
H
J

A	Connect **N1_N3_PWR1** on the Backplane to **BPPWR1** on the Lower Midplane
B	Connect **N2_N4_PWR1** on the Backplane to **BPPWR1** on the Upper Midplane
C	Connect **SMBUS1** on the Backplane to **SMBUS1** on the Upper and Lower Midplane
D	Connect **N1_SLIMPCIE1** and **N1_SLIMPCIE2** on the Backplane to **N1_SLIMSAS1** on the Lower Midplane
E	Connect **N1_SLIMSAS1** on the Backplane to **SLIMSAS1** on the Converter Board for Node 1
F	Connect **N2_SLIMPCIE1** and **N2_SLIMPCIE2** on the Backplane to **N1_SLIMSAS1** on the Upper Midplane
G	Connect **N2_SLIMSAS1** on the Backplane to **SLIMSAS1** on the Converter Board for Node 2
H	Connect **N3_SLIMPCIE1** and **N3_SLIMPCIE2** on the Backplane to **N3_SLIMSAS1** on the Lower Midplane
I	Connect **N3_SLIMSAS1** on the Backplane to **SLIMSAS1** on the Converter Board for Node 3
J	Connect **N4_SLIMPCIE1** and **N4_SLIMPCIE2** on the Backplane to **N3_SLIMSAS1** on the Upper Midplane
K	Connect **N4_SLIMSAS1** on the Backplane to **SLIMSAS1** on the Converter Board for Node 4

2.8 Removable/optional components

You may need to remove previously installed system components when installing or removing system devices. Or you may need to install the optional components into the system. This section tells how to remove/install the following components:

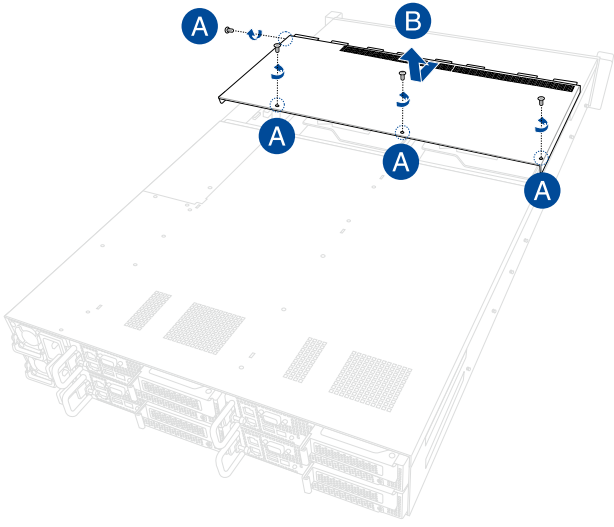
1. System fans
2. Power supply module

Ensure that the system is turned off before removing any components.

2.8.1 System fan

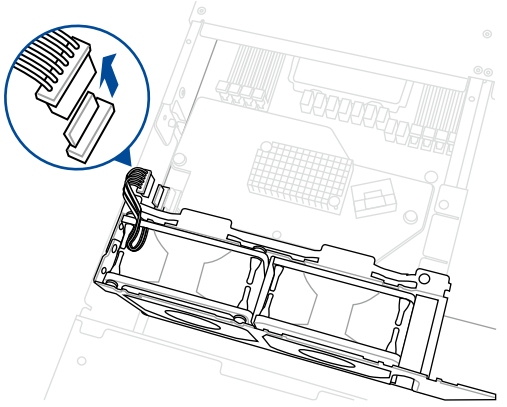
To replace a system fan:

1. Remove the four (4) screws securing the top cover (A), then push the top cover towards the rear of the system and remove the top cover. (B).

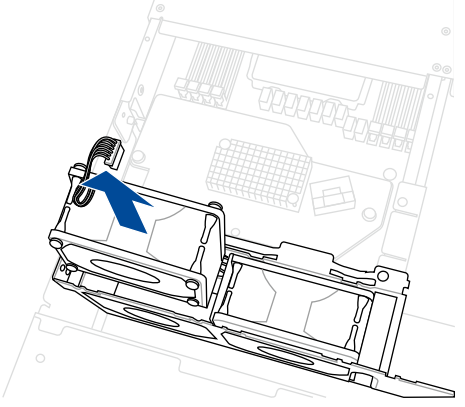


2. Prepare a replacement fan of the same type and size.

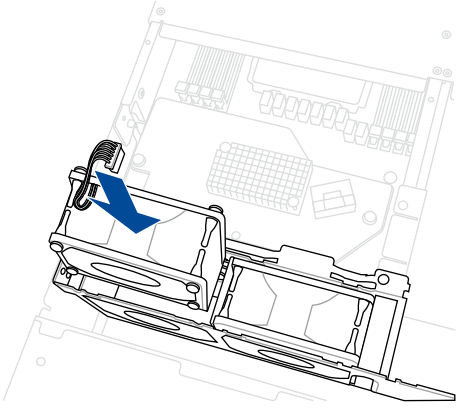
3. Disconnect the system fan cable from the fan connector on the Midplane.



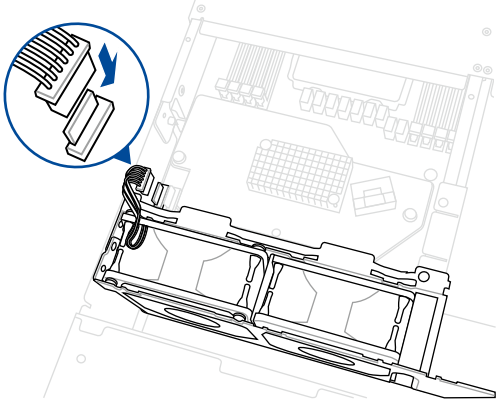
4. Lift the fan then set it aside.



5. Insert the replacement fan into the fan compartment.



6. Connect the system fan cable to the fan connector on the midplane.

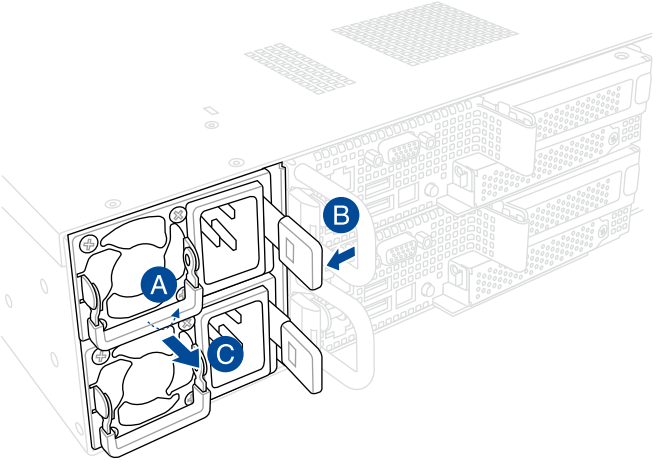


7. Repeat steps 3 to 6 to replace the other system fans.

2.8.2 Power supply module

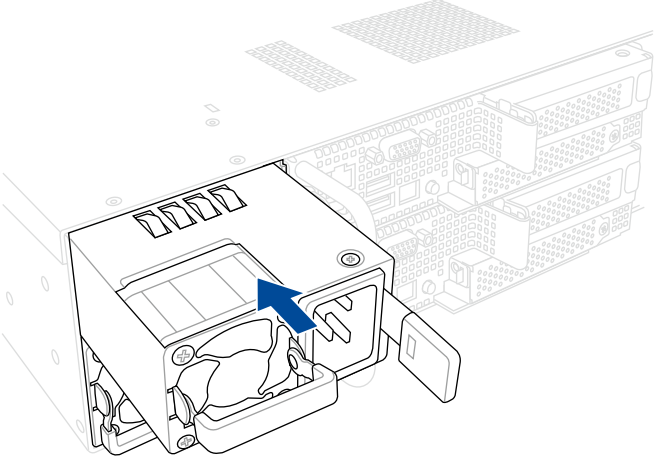
To replace a power supply unit (PSU):

1. Lift up the PSU lever (A) then press the PSU latch (B) and carefully pull the PSU out of the system chassis using the PSU lever (C) while the PSU latch is still pressed down.



2. Prepare the replacement PSU.

3. Align and insert the replacement PSU into the empty PSU bay until it clicks in place.



- The system automatically combines the two power supply modules as a single one. The combined output power varies with input voltages. Refer to the table below for details.

3000W

Input Voltage	Max. Output Power (Watt) per PSU
220V-240Vac, 15.5A (x2), 50-60Hz	3000W

- To enable the hot-swap feature (redundant mode), keep the total power consumption of the system under the maximum output power of an individual power supply module.

- Always use PSUs with the same watt and power rating. Combining PSUs with different wattage (e.g. 1 x 1600 W + 1 x 2200 W) may yield unstable results and potential damage to your system.
- For a steady power input, use only the power cables that come with the server system package.

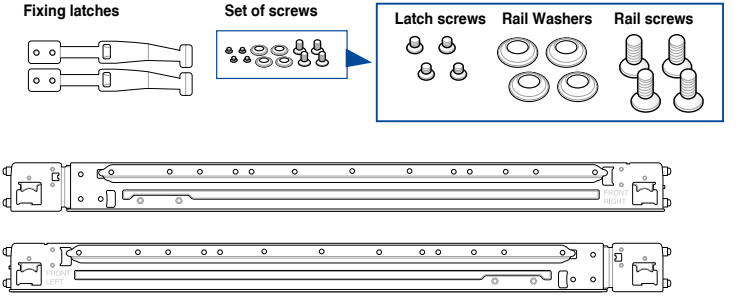
3 Installation Options

This chapter describes how to install the optional components and devices into the barebone server.

3.1 Tool-less Friction Rail Kit

The tool less design of the rail kit allows you to easily install the rack rails into the server rack without the need for additional tools. The kit also comes with a metal stopping bracket that can be installed to provide additional support and stability to the server.

The tool-less rail kit package includes:

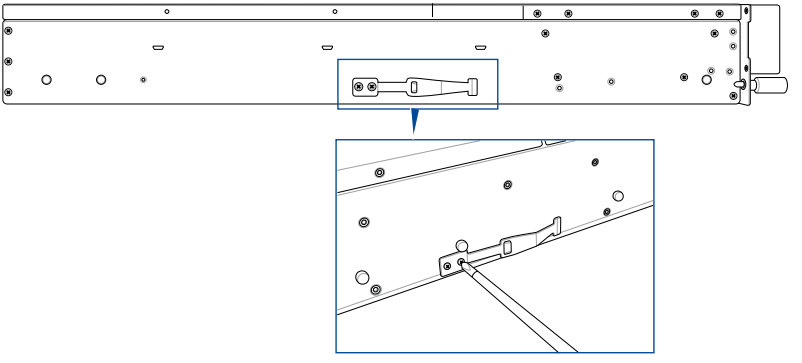


Installing the tool-less rack rail

To install the tool-less rack rails into the rack:

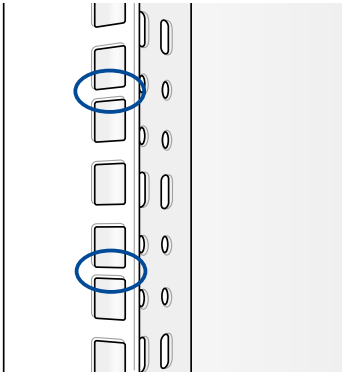
1. Secure the two fixing latches to the two sides of the server using the set of latch screws.

The locations of the screw holes vary with different server models. Refer to your server user manual for details.



2. Select a desired space and place the appropriate rack rail (left and right) on opposite positions on the rack.

A 1U space is consists of three square mounting holes with two thin lips on the top and the bottom.

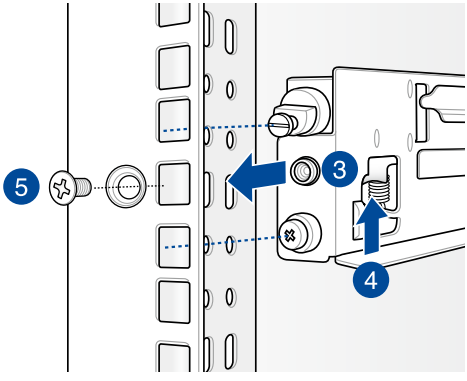


3. Press the spring lock then insert the studs into the selected square mounting holes on the rack post.
4. Press the spring lock on the other end of rail then insert the stud into the mounting hole on the rack post. Extend the rack rail, if necessary.
5. (Optional) Use the rail screw and rail washer that comes with the kit to secure the rack rail to the rack post.

A torque value of 14 kgf.cm is recommended for the rail screw.

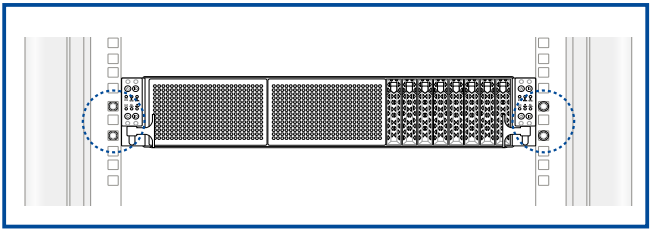
6. Perform steps 3 to 5 for the other rack rail.

Ensure that the installed rack rails (left and right) are aligned, secured, and stable in place.



7. Lift the server chassis and insert into the rack rail.

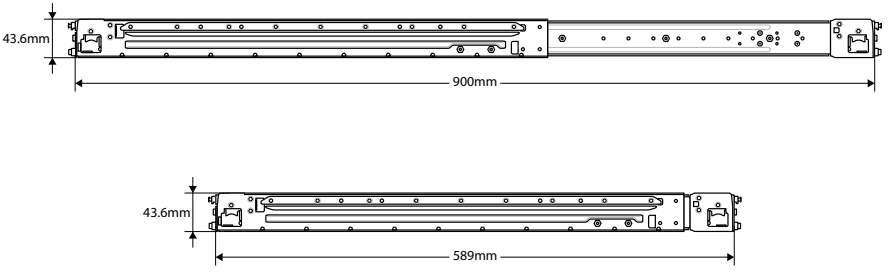
- Ensure that the rack rail cabinet and the rack posts are stable and standing firmly on a level surface.
- We strongly recommend that at least two able-bodied persons perform the steps described in this guide.
- We recommend the use an appropriate lifting tool or device, if necessary.



Ensure to include the side knots on the two sides of the server in the rack rail holders.

The illustrations shown above are for reference only.

3.2 Rail kit dimensions

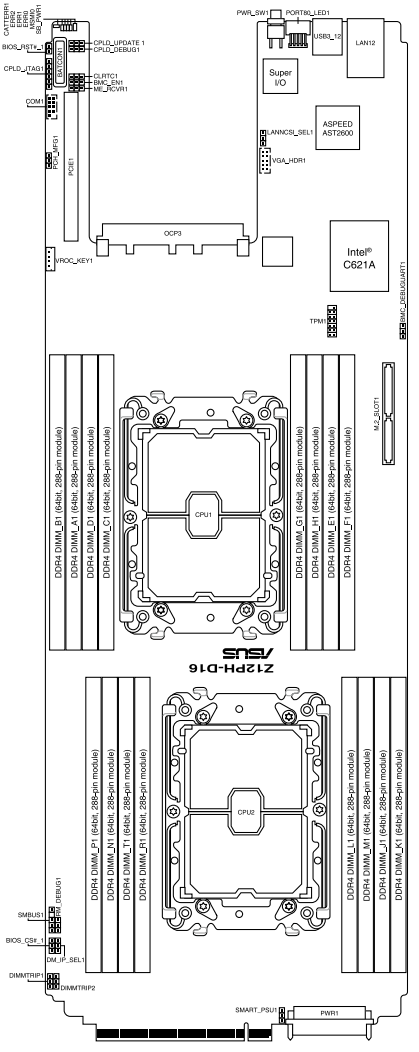


4 Motherboard Information

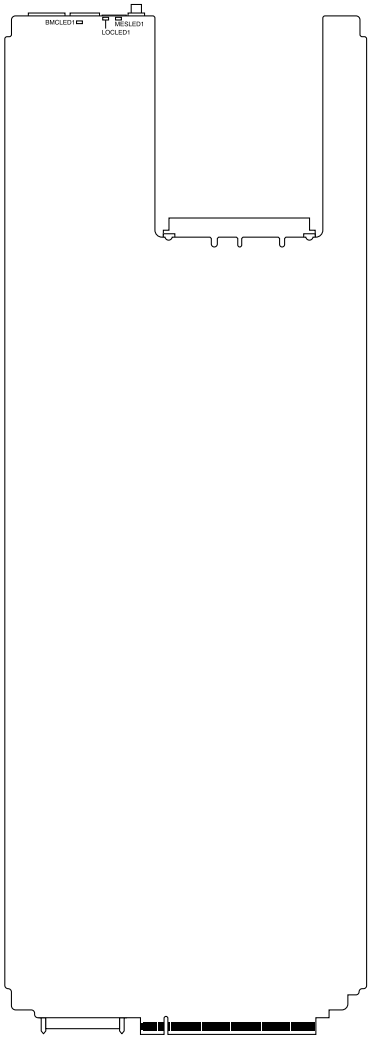
This chapter includes the motherboard layout and brief descriptions of the jumpers and internal connectors.

4.1 Motherboard layout

Top side



Bottom side



4.2 Jumpers

1. Clear RTC RAM (CLRTC1)

This jumper allows you to clear the Real Time Clock (RTC) RAM in CMOS. You can clear the CMOS memory of date, time, and system setup parameters by erasing the CMOS RTC RAM data. The onboard button cell battery powers the RAM data in CMOS, which include system setup information such as system passwords.

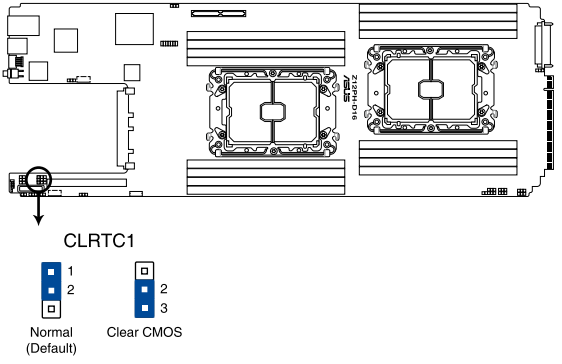
To erase the RTC RAM:

1. Turn OFF the computer and unplug the power cord.
2. Move the jumper cap from pins 1–2 (default) to pins 2–3. Keep the cap on pins 2–3 for about 5–10 seconds, then move the cap back to pins 1–2.
3. Plug the power cord and turn ON the computer.
4. Hold down the <Del> key during the boot process and enter BIOS setup to re-enter data.

Except when clearing the RTC RAM, never remove the cap on CLRTC jumper default position. Removing the cap will cause system boot failure!

If the steps above do not help, remove the onboard battery and move the jumper again to clear the CMOS RTC RAM data. After the CMOS clearance, reinstall the battery.

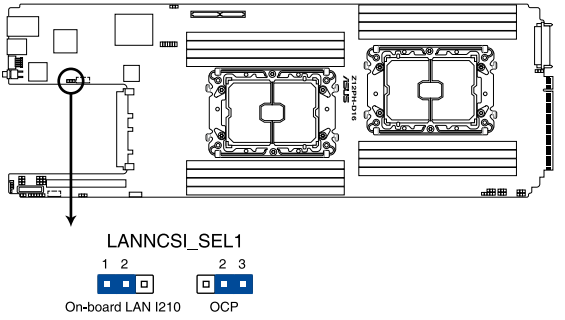
Z12PH-D16 Clear RTC RAM



2. LANNCSI setting (3-pin LANNCSI_SEL1)

This jumper allows you to select which LAN NCSI function to use.

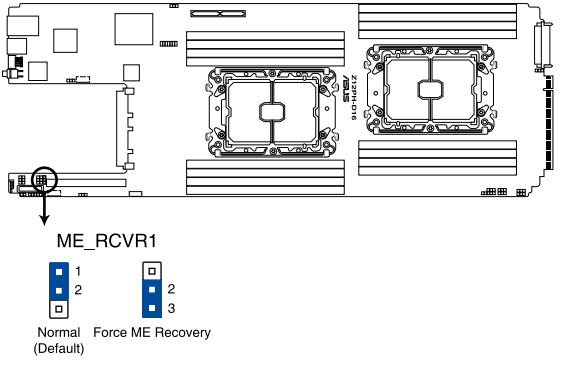
Z12PH-D16 LANNCSI_SEL1 setting



3. ME firmware force recovery setting (3-pin ME_RCVR1)

This jumper allows you to quickly recover the Intel Management Engine (ME) firmware when it becomes corrupted.

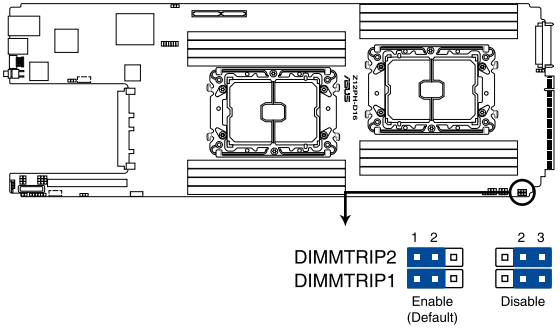
Z12PH-D16 ME recovery setting



4. DDR4 thermal event setting (3-pin DIMMTRIP1-2)

These jumpers allow you to enable or disable DDR4 DIMM thermal sensing event pin.

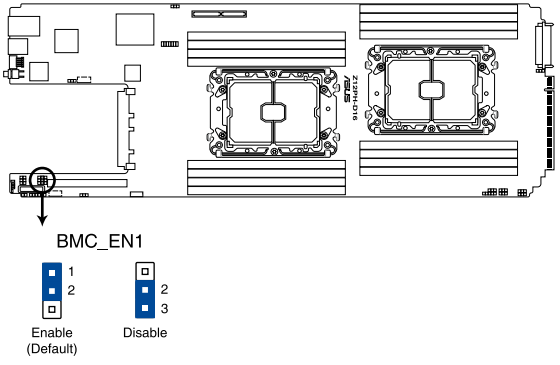
Z12PH-D16 Thermaltrip setting



5. BMC Setting (3-pin BMC_EN1)

This jumper allows you to enable or disable the ASMB10.

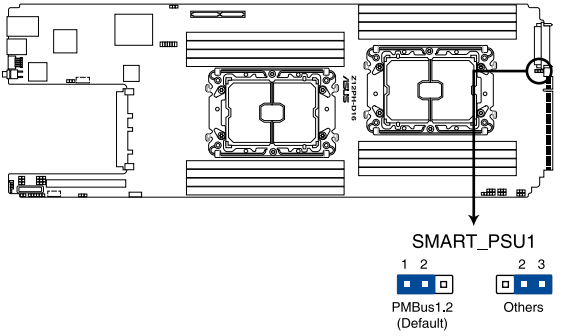
Z12PH-D16 BMC setting



6. PMBus 1.2 PSU select jumper (3-pin SMART_PSU1)

This jumper allows you to select PSU PMBus version.

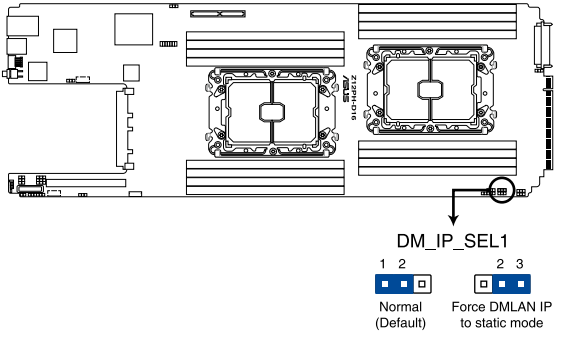
Z12PH-D16 PMBus 1.2 PSU setting



7. DMLAN setting (3-pin DM_IP_SEL1)

This jumper allows you to select the DMLAN setting. Set to pins 2-3 to force the DMLAN IP to static mode (IP=10.10.10.10, submask=255.255.255.0).

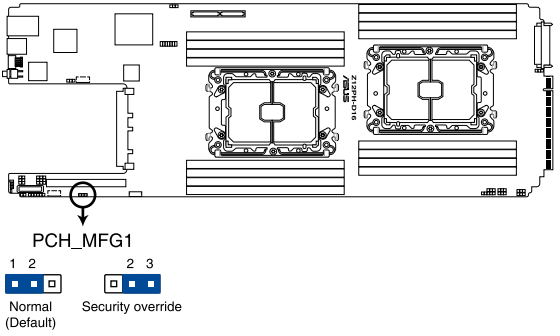
Z12PH-D16 DM_IP_SEL1 setting



8. PCH_MFG setting (3-pin PCH_MFG1)

This jumper allows you to update the BIOS ME block.

Z12PH-D16 PCH_MFG setting

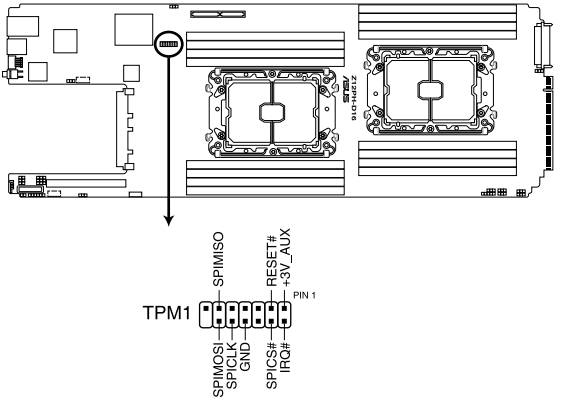


4.3 Internal connectors

1. Trusted Platform Module connector (14-1 pin TPM1)

This connector supports a Trusted Platform Module (TPM) system, which can securely store keys, digital certificates, passwords, and data. A TPM system also helps enhance network security, protects digital identities, and ensures platform integrity.

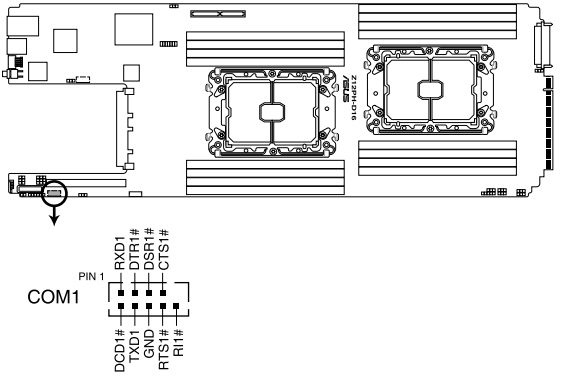
Z12PH-D16 TPM connector



2. Serial port connector (10-1 pin COM1)

This connector is for a serial (COM) port. Connect the serial port module cable to this connector, then install the module to a slot opening at the back of the system chassis.

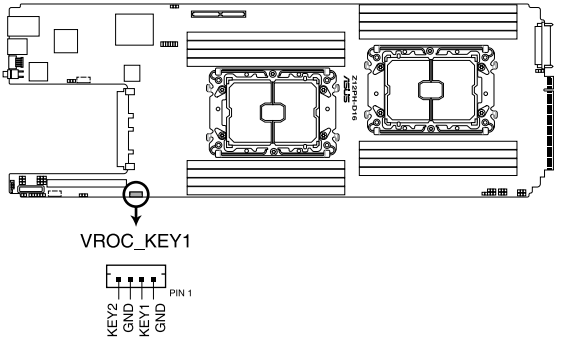
Z12PH-D16 Serial port connector



3. VROC_KEY connector (4-pin VROC_KEY1)

This connector allows you to connect a KEY module to enable CPU RAID functions with Intel® CPU RSTe.

Z12PH-D16 VROC_KEY1

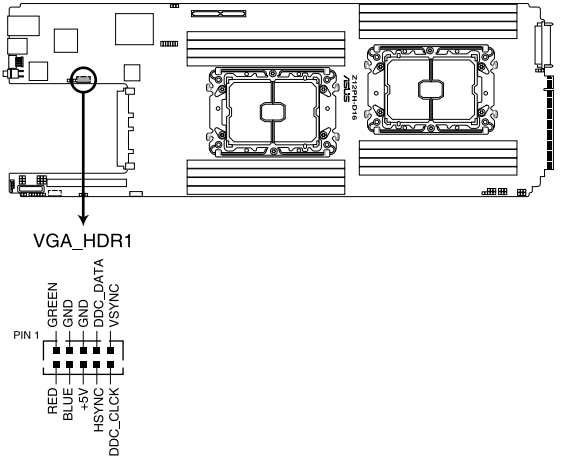


The KEY module is purchased separately.

4. VGA connector (16-1 pin VGA_HDR1)

This connector supports the VGA High Dynamic-Range interface.

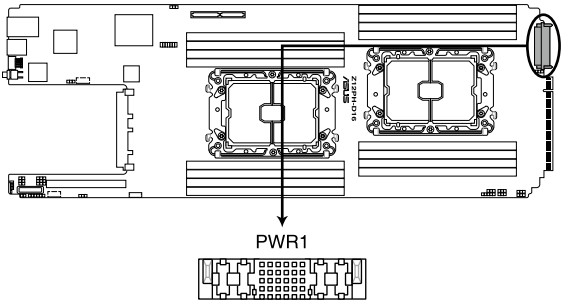
Z12PH-D16 Internal VGA connector



5. Power connector

This power connector connects to the Midplane.

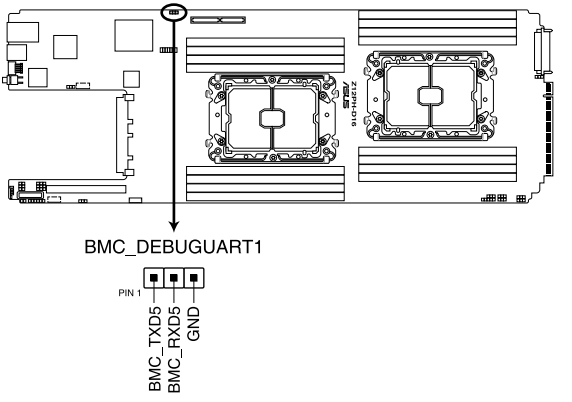
Z12PH-D16 ATX power connectors



6. BMC Debug UART connector (3-pin BMC_DEBUGUART1)

This connector is used for reading the BMC UART Debug log.

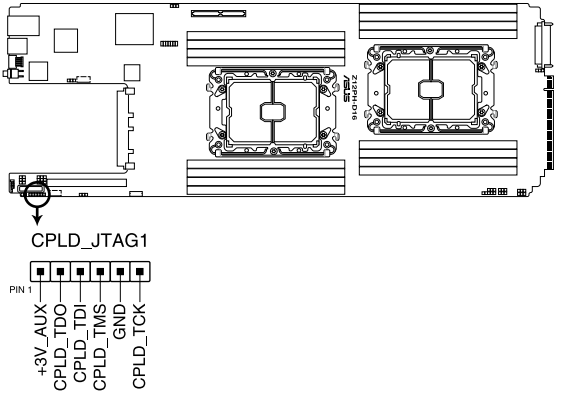
Z12PH-D16 BMC_DEBUGUART1 connector



7. CPLD JTAG connector (6-pin CPLD_JTAG1)

This connector is used for burning the CPLD JTAG.

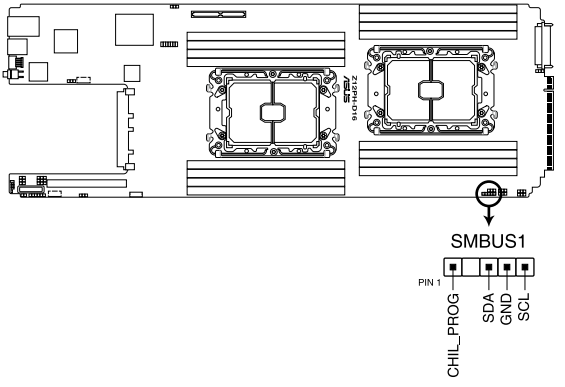
Z12PH-D16 CPLD_JTAG connector



8. System Management Bus (SMBUS) connector (5-1 pin SMBUS1)

This connector controls the system and power management-related tasks. This connector processes the messages to and from devices rather than tripping the individual control lines.

Z12PH-D16 SMBUS connector

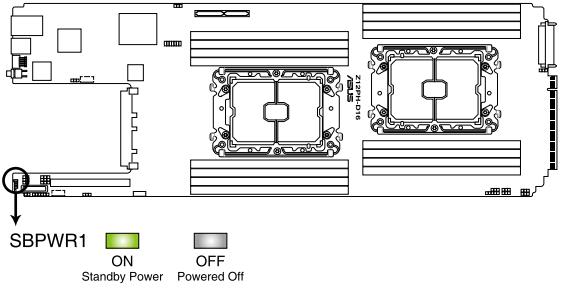


4.4 Internal LEDs

1. Standby Power LED (SBPWR1)

The motherboard comes with a standby power LED. The green LED lights up to indicate that the system is ON, in sleep mode, or in soft-off mode. This is a reminder that you should shut down the system and unplug the power cable before removing or plugging in any motherboard component. The illustration below shows the location of the onboard LED.

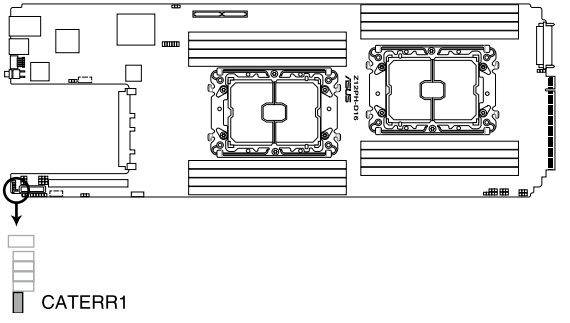
Z12PH-D16 Standby Power LED



2. CAT ERR LED (CATERR1)

The CAT ERR LED indicates that the system has experienced a fatal or catastrophic error and cannot continue to operate.

Z12PH-D16 CATERR1 LED



3. BMC Heartbeat LED (BMCLED1)

The BMC Heartbeat will blink continuously when BMC is operating nomrally.

Z12PH-D16 BMC LED

4. BMC Location LED (LOCLED1)

The BMC Location LED will light up when the locator button is pressed, both the front and rear Location LEDs of the system will light up.

Z12PH-D16 Location LED

5. BMC Message LED (MESLED1)

The BMC Message LED will light up when an error has occurred, both the front and rear Message LEDs of the system will light up.

Z12PH-D16 MESLED

BIOS Setup

5

This chapter tells how to change the system settings through the BIOS Setup menus. Detailed descriptions of the BIOS parameters are also provided.

5.1 Managing and updating your BIOS

The following utilities allow you to manage and update the motherboard Basic Input/Output System (BIOS) setup:

1. **ASUS CrashFree BIOS 3**

   To recover the BIOS using a bootable USB flash disk drive when the BIOS file fails or gets corrupted.

2. **ASUS EzFlash**

   Updates the BIOS using a USB flash disk.

3. **BUPDATER**

   Updates the BIOS in DOS mode using a bootable USB flash disk drive.

Refer to the corresponding sections for details on these utilities.

Save a copy of the original motherboard BIOS file to a bootable USB flash disk drive in case you need to restore the BIOS in the future. Copy the original motherboard BIOS using the BUPDATER utility.

5.1.1 ASUS CrashFree BIOS 3 utility

The ASUS CrashFree BIOS 3 is an auto recovery tool that allows you to restore the BIOS file when it fails or gets corrupted during the updating process. You can update a corrupted BIOS file using a USB flash drive that contains the updated BIOS file.

Prepare a USB flash drive containing the updated motherboard BIOS before using this utility.

Recovering the BIOS from a USB flash drive

To recover the BIOS from a USB flash drive:

1. Insert the USB flash drive with the original or updated BIOS file to one USB port on the system.
2. The utility will automatically recover the BIOS. It resets the system when the BIOS recovery finished.

DO NOT shut down or reset the system while recovering the BIOS! Doing so would cause system boot failure!

The recovered BIOS may not be the latest BIOS version for this motherboard. Visit the ASUS website at www.asus.com to download the latest BIOS file.

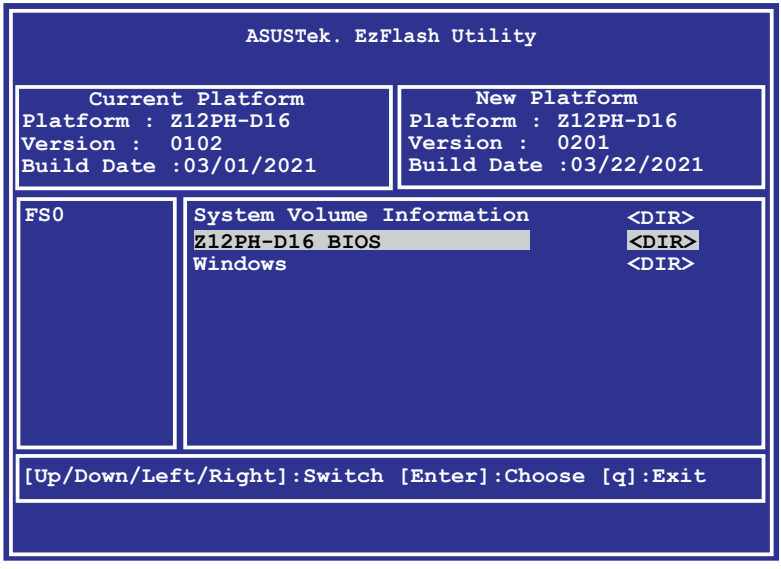
5.1.2 ASUS EZ Flash Utility

The ASUS EZ Flash Utility feature allows you to update the BIOS without having to use a DOS-based utility.

Before you start using this utility, download the latest BIOS from the ASUS website at www.asus.com.

To update the BIOS using EZ Flash Utility:

1. Insert the USB flash disk that contains the latest BIOS file into the USB port.
2. Enter the BIOS setup program. Go to the **Tool** menu then select **ASUS EZ Flash Utility**. Press <Enter>.



3. Press <Tab> to switch to the **Drive** field.
4. Press the Up/Down arrow keys to find the USB flash disk that contains the latest BIOS, then press <Enter>.
5. Press <Tab> to switch to the **Folder Info** field.
6. Press the Up/Down arrow keys to find the BIOS file, and then press <Enter> to perform the BIOS update process. Reboot the system when the update process is done.

- This function can support devices such as a USB flash disk with FAT 32/16 format and single partition only.
- DO NOT shut down or reset the system while updating the BIOS to prevent system boot failure!

Ensure to load the BIOS default settings to ensure system compatibility and stability. Press <F5> and select **Yes** to load the BIOS default settings.

5.1.3 BUPDATER utility

The succeeding BIOS screens are for reference only. The actual BIOS screen displays may not be the same as shown.

The BUPDATER utility allows you to update the BIOS file in the DOS environment using a bootable USB flash disk drive with the updated BIOS file.

Updating the BIOS file

To update the BIOS file using the BUPDATER utility:

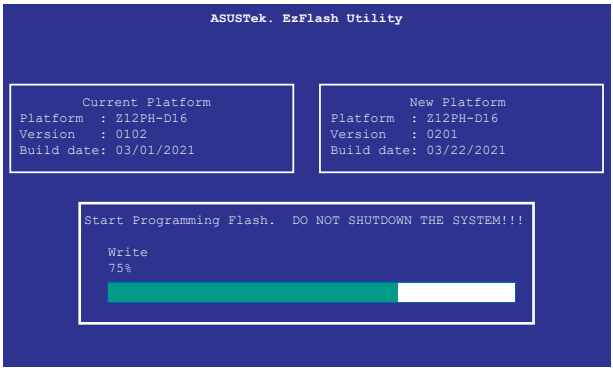
1. Visit the ASUS website at www.asus.com and download the latest BIOS file for the motherboard. Save the BIOS file to a bootable USB flash disk drive.
2. Copy the BUPDATER utility (BUPDATER.exe) from the ASUS support website at support.asus.com to the bootable USB flash disk drive you created earlier.
3. Boot the system in DOS mode, then at the prompt, type:

   `BUPDATER /i[filename].CAP`

   where [filename] is the latest or the original BIOS file on the bootable USB flash disk drive, then press <Enter>.

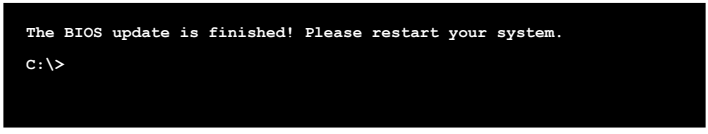
```
A:\>BUPDATER /i[file name].CAP
```

4. The utility verifies the file, then starts updating the BIOS file.



DO NOT shut down or reset the system while updating the BIOS to prevent system boot failure!

5. The utility returns to the DOS prompt after the BIOS update process is completed. Reboot the system from the hard disk drive.



5.2 BIOS setup program

This motherboard supports a programmable firmware chip that you can update using the provided utility described in section **5.1 Managing and updating your BIOS**.

Use the BIOS Setup program when you are installing a motherboard, reconfiguring your system, or prompted to "Run Setup." This section explains how to configure your system using this utility.

Even if you are not prompted to use the Setup program, you can change the configuration of your computer in the future. For example, you can enable the security password feature or change the power management settings. This requires you to reconfigure your system using the BIOS Setup program so that the computer can recognize these changes and record them in the CMOS RAM of the firmware chip.

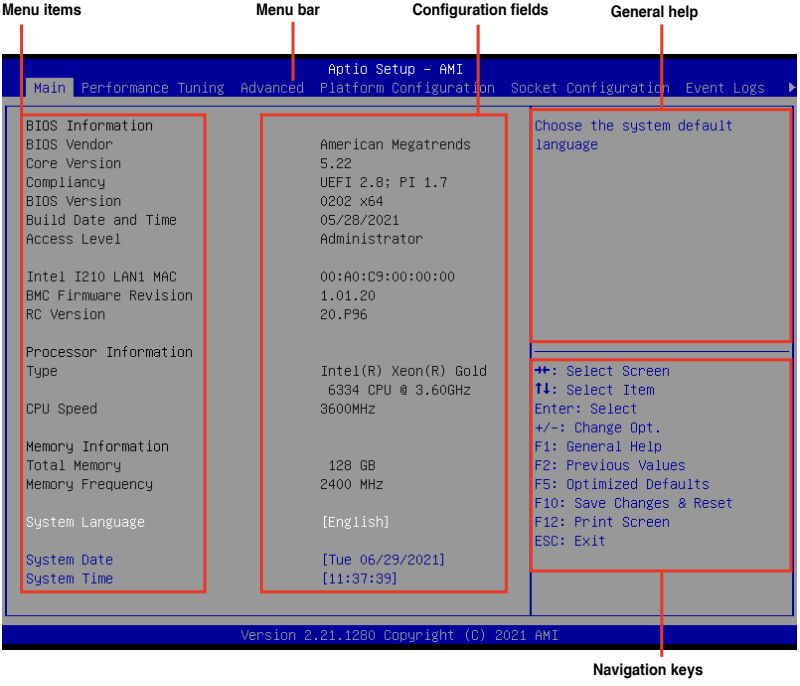
The firmware chip on the motherboard stores the Setup utility. When you start up the computer, the system provides you with the opportunity to run this program. Press <Del> during the Power-On Self-Test (POST) to enter the Setup utility; otherwise, POST continues with its test routines.

If you wish to enter Setup after POST, restart the system by pressing <Ctrl>+<Alt>+<Delete>, or by pressing the reset button on the system chassis. You can also restart by turning the system off and then back on. Do this last option only if the first two failed.

The Setup program is designed to make it as easy to use as possible. Being a menu-driven program, it lets you scroll through the various sub-menus and make your selections from the available options using the navigation keys.

- The default BIOS settings for this motherboard apply for most conditions to ensure optimum performance. If the system becomes unstable after changing any BIOS settings, load the default settings to ensure system compatibility and stability. Press <F5> and select **Yes** to load the BIOS default settings.
- The BIOS setup screens shown in this section are for reference purposes only, and may not exactly match what you see on your screen.
- Visit the ASUS website (www.asus.com) to download the latest BIOS file for this motherboard.

5.2.1 BIOS menu screen



5.2.2 Menu bar

The menu bar on top of the screen has the following main items:

Main	For changing the basic system configuration
Performance Tuning	For changing the performance settings
Advanced	For changing the advanced system settings
Platform Configuration	For changing the platform settings
Socket Configuration	For changing the socket settings
Event Logs	For changing the event log settings
Server Mgmt	For changing the Server Mgmt settings
Security	For changing the security settings
Boot	For changing the system boot configuration
Tool	For configuring options for special functions
Save & Exit	For selecting the exit options

To select an item on the menu bar, press the right or left arrow key on the keyboard until the desired item is highlighted.

5.2.3 Menu items

The highlighted item on the menu bar displays the specific items for that menu. For example, selecting Main shows the Main menu items.

The other items (Advanced, Platform Configuration, Socket Configuration, Event Logs, Server Mgmt, Security, Boot, Tool, and Save & Exit) on the menu bar have their respective menu items.

5.2.4 Submenu items

A solid triangle before each item on any menu screen means that the item has a submenu. To display the submenu, select the item then press <Enter>.

5.2.5 Navigation keys

At the bottom right corner of a menu screen are the navigation keys for the BIOS setup program. Use the navigation keys to select items in the menu and change the settings.

5.2.6 General help

At the top right corner of the menu screen is a brief description of the selected item.

5.2.7 Configuration fields

These fields show the values for the menu items. If an item is user-configurable, you can change the value of the field opposite the item. You cannot select an item that is not user-configurable.

A configurable field is enclosed in brackets, and is highlighted when selected. To change the value of a field, select it and press <Enter> to display a list of options.

5.2.8 Pop-up window

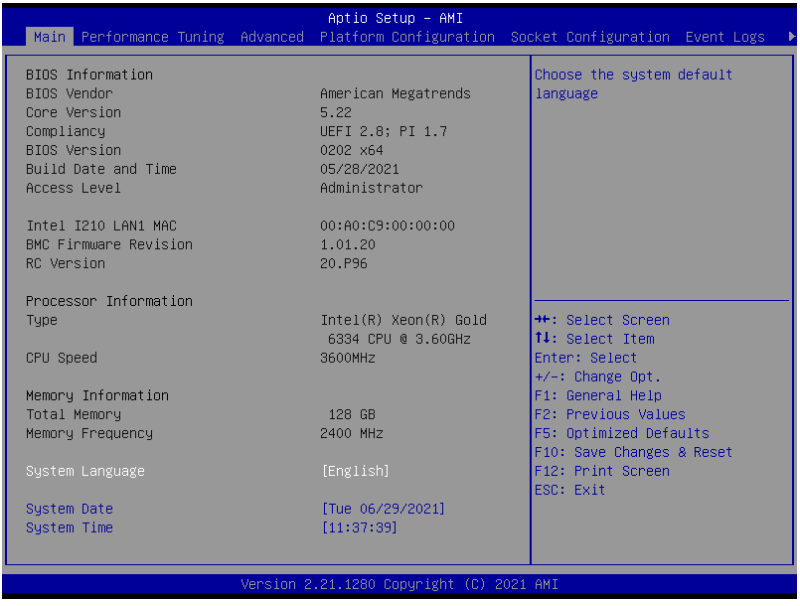
Select a menu item and press <Enter> to display a pop-up window with the configuration options for that item.

5.2.9 Scroll bar

A scroll bar appears on the right side of a menu screen when there are items that do not fit on the screen. Press the Up/Down arrow keys or <Page Up> /<Page Down> keys to display the other items on the screen.

5.3 Main menu

When you enter the BIOS Setup program, the Main menu screen appears. The Main menu provides you an overview of the basic system information, and allows you to set the system date, time, language, and security settings.



5.3.1 System Language [English]

Allows you to select the system default language.

5.3.2 System Date [Day xx/xx/xxxx]

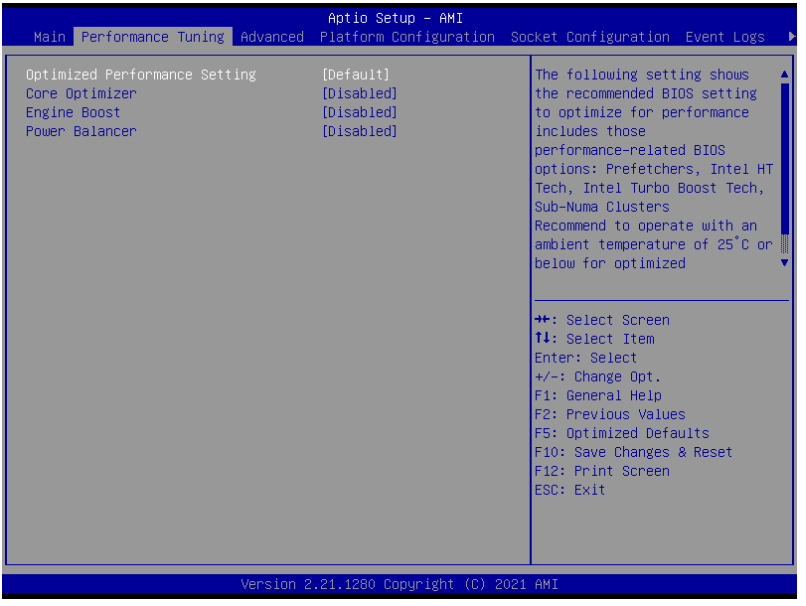
Allows you to set the system date.

5.3.3 System Time [xx:xx:xx]

Allows you to set the system time.

5.4 Performance Tuning menu

The Performance Tuning menu items allow you to change performance related settings for different scenarios.



Optimized Performance Setting [Default]

Allows you to select performance settings for different scenarios.

[Default] Default settings.

[By Benchmark] Optimize for different kinds of benchmarks. Select this option, then select a benchmark type from the >> list.

[By Workload] Optimize for different kinds of workloads. Select this option, then select a workload type from the >> list.

Configuration options:

[Peak Frequency Optimized] - Applies settings with performance and power consumption balance. Recommended for users that need higher performance.

[Latency Optimized] - Applies settings with low latency results. Recommended for latency-sensitive users.

[Power Efficient Optimized] - Applies settings with power efficiency. Recommended for general users.

[HPC] - Applies settings with optimized compute capability. Recommend for traditional HPC applications.

The following item appears only when you set **Power Balancer** to **[Disabled]**.

Core Optimizer [Disabled]

Enable this item to keep the processor operating at the turbo frequency.
Configuration options: [Disabled] [Enable Auto] [Enable Manual]

The following item appears only when you set **Core Optimizer** to **[Enable Manual]**.

CPU Max Frequency [36]

Configuration options: [36]

The following item appears only when you set **Optimized Performance Setting** to **[Default]**.

Engine Boost [Disabled]

Enable this item to boost the CPU's frequency.
Configuration options: [Disabled] [Normal] [Aggressive]

- Operate with an ambient temperature of 25°C or lower for optimized performance.
- We recommend setting Fan Policy to run at Full Speed mode when selecting **[Aggressive]**.

The following item appears only when you set **Core Optimizer** to **[Disabled]**.

Power Balancer [Disabled]

This item dynamically adjusts the frequency of all CPU cores based on their current utilization, delivering better performance per watt for improved system energy efficiency.
Configuration options: [Disabled] [Enable Auto] [Enable Manual]

The following item appears only when you set **Power Balancer** to **[Enable Manual]**.

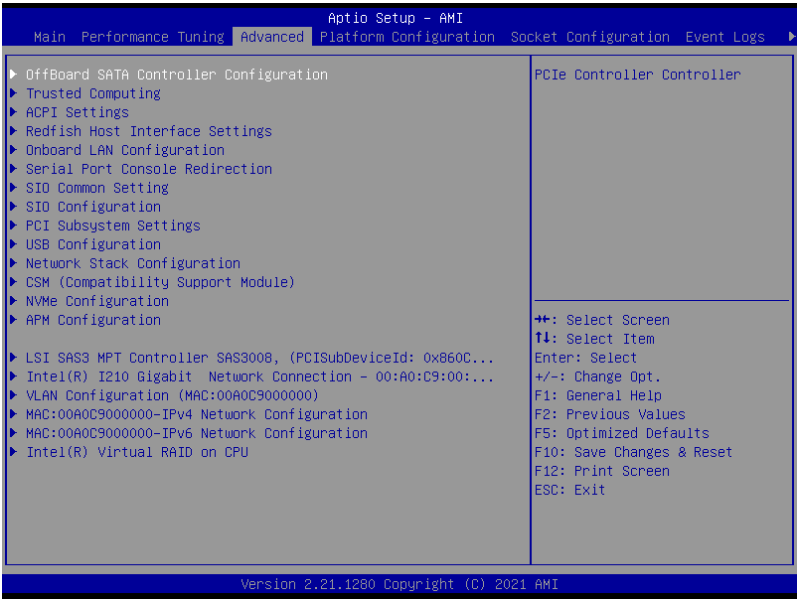
CPU Max Frequency [36]

Configuration options: [36]

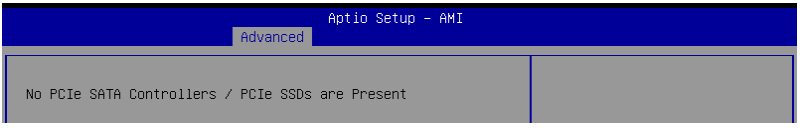
5.5 Advanced menu

The Advanced menu items allow you to change the settings for the CPU and other system devices.

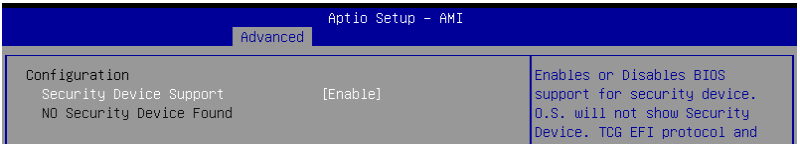
Take caution when changing the settings of the Advanced menu items. Incorrect field values can cause the system to malfunction.



5.5.1 OffBoard SATA Controller Configuration



5.5.2 Trusted Computing

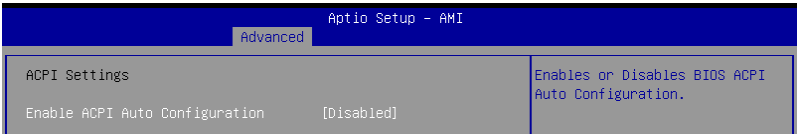


Configuration

Security Device Support [Enabled]

Allows you to enable or disable the BIOS support for security device.
Configuration options: [Disabled] [Enabled]

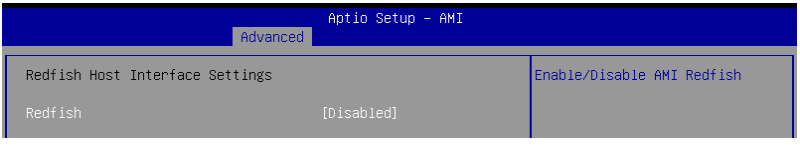
5.5.3 ACPI Settings



Enable ACPI Auto Configuration [Disabled]

Allows you to enable or disable the BIOS ACPI Auto Configuration.
Configuration options: [Disabled] [Enabled]

5.5.4 Redfish Host Interface Settings



Redfish [Disabled]

Allows you to enable or disable Redfish.
Configuration options: [Disabled] [Enabled]

The following items appear only when **Redfish** is set to **[Enabled]**.

Authentication mode [Basic Authentication]

Allows you to select the authentication mode.
Configuration options: [Basic Authentication] [Session Authentication]

Redfish BMC Settings

IP address

Allows you to enter the IP address.

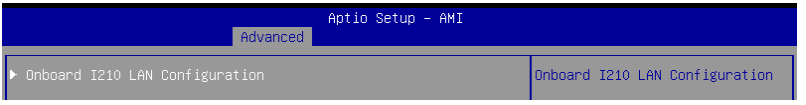
IP Mask address

Allows you to enter the IP Mask address.

IP Port

Allows you to enter the IP Port.

5.5.5 Onboard LAN Configuration



Onboard I210 LAN Configuration

Intel I210 LAN1

LAN Enable [JumperState]

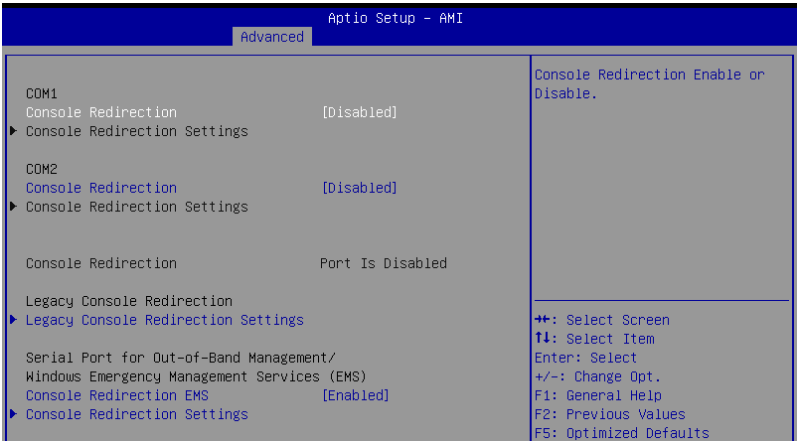
Allows you to enable or disable the Intel LAN.
Configuration options: [Disabled] [Enabled]

The following item appears only when **LAN Enable** is set to **[Enabled]**.

ROM Type [PXE]

Allows you to select the Intel LAN ROM type.
Configuration options: [Disabled] [PXE]

5.5.6 Serial Port Console Redirection



COM1/COM2

Console Redirection [Disabled]

Allows you to enable or disable the console redirection feature.
Configuration options: [Disabled] [Enabled]

The following item appears only when **Console Redirection** for **COM1** or **COM2** is set to **[Enabled]**.

Console Redirection Settings

These items become configurable only when you enable the **Console Redirection** item. 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.

Terminal Type [ANSI]

Allows you to set the terminal type.

[VT100]	ASCII char set.
[VT100+]	Extends VT100 to support color, function keys, etc.
[VT-UTF8]	Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
[ANSI]	Extended ASCII char set.

Bits per second [115200]

Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Configuration options: [9600] [19200] [38400] [57600] [115200]

Data Bits [8]

Configuration options: [7] [8]

Parity [None]

A parity bit can be sent with the data bits to detect some transmission errors. [Mark] and [Space] parity do not allow for error detection.

[None]	None
[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.

Stop Bits [1]

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.
Configuration options: [1] [2]

Flow Control [None]

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.
Configuration options: [None] [Hardware RTS/CTS]

VT -UTF8 Combo Key Support [Enabled]

This allows you to enable the VT -UTF8 Combination Key Support for ANSI/VT100 terminals.
Configuration options: [Disabled] [Enabled]

Recorder Mode [Disabled]

With this mode enabled only text will be sent. This is to capture Terminal data.
Configuration options: [Disabled] [Enabled]

Resolution 100x31 [Enabled]

This allows you enable or disable extended terminal solution.
Configuration options: [Disabled] [Enabled]

Putty Keypad [VT100]

This allows you to select the FunctionKey and Keypad on Putty.
Configuration options: [VT100] [LINUX] [XTERMR6] [SCO] [ESCN] [VT400]

Legacy Console Redirection Settings

Redirection COM Port [COM1]

Allows you to select a COM port to display redirection of Legacy OS and Legacy OPROM Messages.
Configuration options: [COM1] [COM2]

Resolution [80x24]

This allows you to set the number of rows and columns supported on the Legacy OS.
Configuration options: [80x24] [80x25]

Redirection After POST [Always Enable]

The default setting for this option is set to **[Always Enable]**.

[Bootloader] The legacy Console Redirection is disabled before booting to legacy OS.

[Always Enable] Legacy Console Redirection is enabled for legacy OS.

Serial Port for Out-of-Band Management/ Windows Emergency Management Services (EMS)

Console Redirection EMS [Enabled]

Allows you to enable or disable the console redirection feature.
Configuration options: [Disabled] [Enabled]

The following item appears only when **Console Redirection EMS** is set to **[Enabled]**.

Console Redirection Settings

Out-of-Band Mgmt Port [COM1]

Microsoft Windows Emergency Management Services (EMS) allow for remote management of a Windows Server OS through a serial port.
Configuration options: [COM1] [COM2]

Terminal Type EMS [VT-UTF8]

VT-UTF8 is the preferred terminal type for out0of-band management. The next best choice is VT100+, and then VT100. See above, in Console Redirection Settings page for more help with Terminal Type/Emulation.
Configuration options: [VT100] [VT100+] [VT-UTF8] [ANSI]

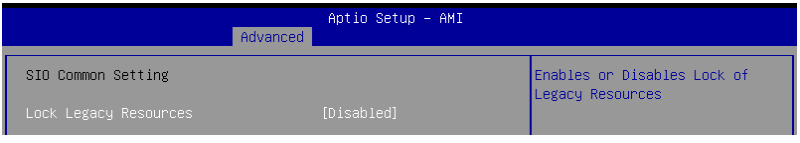
Bits per second EMS [115200]

Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Configuration options: [9600] [19200] [57600] [115200]

Flow Control EMS [None]

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.
Configuration options: [None] [Hardware RTS/CTS] [Software Xon/Xoff]

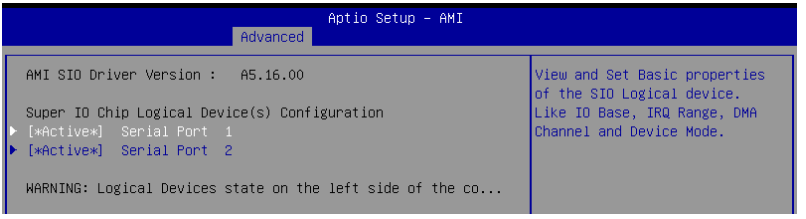
5.5.7 SIO Common Setting



Lock Legacy Resources [Disabled]

Allows you to enable or disable locking of Legacy Resources.
Configuration options: [Disabled] [Enabled]

5.5.8 SIO Configuration



Logical Devices state on the left side of the control, reflects the current Logical Device state. Changes made during Setup Session will be shown after you restart the system.

[*Active*] Serial Port 1 / [*Active*] Serial Port 2

Allows you to view and set basic properties of the SIO Logical device. Like IO Base, IRQ Range, DMA Channel, and Device Mode.

Use This Device [Enabled]

Allows you to enable or disable this Logical Device.
Configuration options: [Disabled] [Enabled]

The following item appears only when **Use This Device** is set to **[Enabled]**.

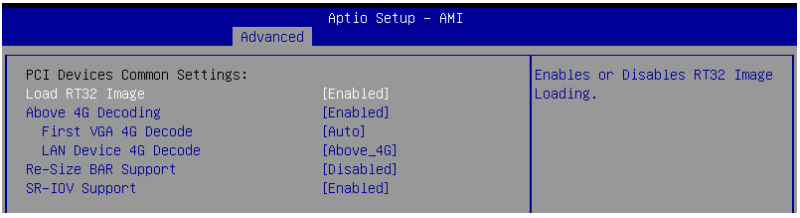
Disabling SIO Logical Devices may have unwanted side effects. PROCEED WITH CAUTION.

Possible: [Use Automatic Settings]

Allows the user to change the device resource settings. New settings will be reflected no this setup page after system restarts.
Configuration options: [Use Automatic Settings] [IO=3F8h; IRQ=4; DMA;] [IO=3F8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA;] [IO=2F8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA;] [IO=3E8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA;] [IO=2E8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA;]

5.5.9 PCI Subsystem Settings

Allows you to configure PCI, PCI-X, and PCI Express Settings.



Load RT32 Image [Enabled]

Allows you to enable or disable RT32 Image Loading.
Configuration options: [Disabled] [Enabled]

Above 4G Decoding [Enabled]

Allows you to enable or disable 64-bit capable devices to be decoded in above 4G address space. It only works if the system supports 64-bit PCI decoding.
Configuration options: [Disabled] [Enabled]

The following items appear only when **Above 4G Decoding** is set to **[Enabled]**.

First VGA 4G Decode [Auto]

[Auto] Auto
[Above_4G] Force First VGA to above 4G.

LAN Device 4G Decode [Above_4G]

Configuration options: [Auto] [Above_4G]

Re-Size BAR Support [Disabled]

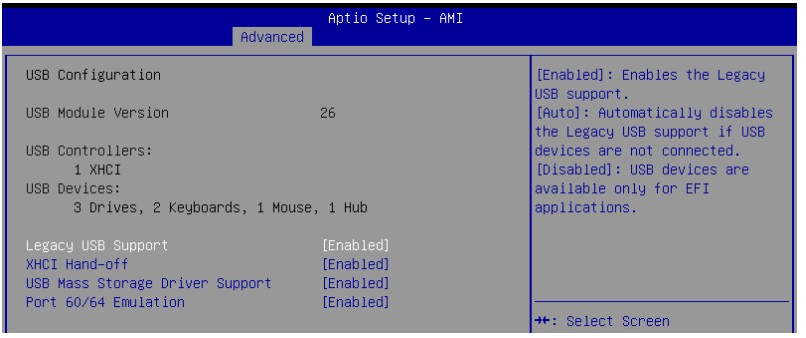
If system has Resizable BAR capable PCIe Devices, this option enables or disables Resizable BAR Support. (Only if system supports 64-bit PCI Decoding).
Configuration options: [Disabled] [Auto]

To enable Re-Size BAR Support for harnessing full GPU memory, please set **CSM (Compatibility Support Module)** to **[Disabled]**.

SR-IOV Support [Enabled]

Allows you to enable or disable Single Root IO Virtualization Support if the system has SR-IOV capable PCIe devices.
Configuration options: [Disabled] [Enabled]

5.5.10 USB Configuration



Legacy USB Support [Enabled]

Allows you to enable or disable Legacy USB device support.

[Enabled] Enables legacy USB support.

[Disabled] Keep USB devices available only for EFI applications.

[Auto] Disables legacy support if no USB devices are connected.

XHCI Hand-off [Enabled]

Allows you to enable or disable workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
Configuration options: [Enabled] [Disabled]

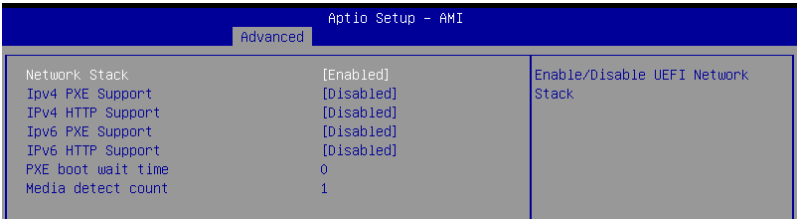
USB Mass Storage Driver Support [Enabled]

Allows you to enable or disable the USB Mass Storage driver support.
Configuration options: [Disabled] [Enabled]

Port 60/64 Emulation [Enabled]

Allows you to enable or disable I/O port 60h/64h emulation support. This should be enabled for the complete keyboard legacy support for non-USB aware OSes.
Configuration options: [Disabled] [Enabled]

5.5.11 Network Stack Configuration



Network Stack [Enabled]

Enables or disables the UEFI network stack.
Configuration options: [Disabled] [Enabled]

The following items appear only when **Network Stack** is set to **[Enabled]**.

Ipv4 PXE Support [Disabled]

Enables or disables the Ipv4 PXE Boot Support. If disabled, Ipv4 PXE boot support will not be available.
Configuration options: [Disabled] [Enabled]

Ipv4 HTTP Support [Disabled]

Enables or disables the Ipv4 HTTP Boot Support. If disabled, Ipv4 HTTP boot support will not be available.
Configuration options: [Disabled] [Enabled]

Ipv6 PXE Support [Disabled]

Enables or disables the Ipv6 PXE Boot Support. If disabled, Ipv6 PXE boot support will not be available.
Configuration options: [Disabled] [Enabled]

Ipv6 HTTP Support [Disabled]

Enables or disables the Ipv6 HTTP Boot Support. If disabled, Ipv6 HTTP boot support will not be available.
Configuration options: [Disabled] [Enabled]

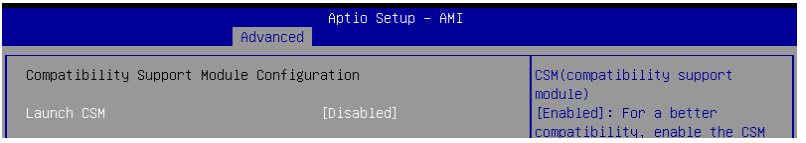
PXE boot wait time [0]

Set the wait time to press ESC key to abort the PXE boot. Use the <+> or <-> to adjust the value. The values range from 0 to 5.

Media detect count [1]

Set the number of times presence of media will be checked. Use the <+> or <-> to adjust the value. The values range from 1 to 50.

5.5.12 CSM (Compatibility Support Module)



Launch CSM [Disabled]

Allows you to enable or disable CSM (Compatibility Support Module) Support.

[Enabled] For a better compatibility, enable the CSM to fully support the non-UEFI driver add-on devices or the Windows UEFI mode.

[Disabled] Disable the CSM to fully support the Windows secure update and secure boot.

The following items appear only when **Launch CSM** is set to **[Enabled]**.

GateA20 Active [Upon Request]

Allows you to set the GA20 option.

[Upon Request] GA20 can be disabled using BIOS services.

[Always] Do not allow GA20 disabling; this option is useful when any RT code is executed above 1MB.

Option ROM Messages [Force BIOS]

This allows you to set the display mode for option ROM.
Configuration options: [Force BIOS] [Keep Current]

Interrupt 19 Capture [Immediate]

Allows you to select the BIOS reaction on INT19 trapping by Option ROM.

[Immediate] Execute the trap right away.

[Postponed] Execute the trap during legacy boot.

[Auto] Auto

HDD Connection Order [Adjust]

Allows you to select the HDD Connection Order. Some OS require HDD handles to be adjusted, i.e. OS is installed on drive 80h.
Configuration options: [Adjust] [Keep]

Boot Device Control [UEFI and Legacy]

Allows you to select the devices boot-up mode according to the devices specification. Devices with the selected mode will in the boot priority list.
Configuration options: [UEFI and Legacy] [Legacy only] [UEFI only]

Option ROM execution

Boot from Network Devices [UEFI only]

Allows you to select the type of onboard LAN controller and installed LAN cards. Network devices will run the selected type during the system boot. Selecting **[Ignore]** will accelerate the boot up time without running network devices during POST (Power-On Self-Test).
Configuration options: [Ignore] [UEFI only] [Legacy only]

Boot from Storage Devices [UEFI only]

Allows you to select the type of storage devices to run first during the system boot. It is recommended to select either **[Legacy only]** or **[UEFI only]** according to devices specification for better stability. Selecting **[Ignore]** will accelerate the boot up time without running network devices during POST (Power-On Self-Test).
Configuration options: [Ignore] [UEFI only] [Legacy only]

Launch Video OPROM policy [UEFI only]

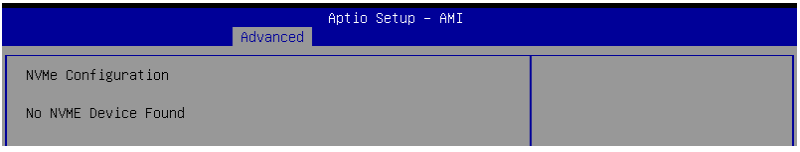
This option controls the execution of UEFI and Legacy Video OPROM.
Configuration options: [Ignore] [UEFI only] [Legacy only]

Boot from PCI-E/PCI Expansion Devices [UEFI only]

Allows you to select the type of PCI-E/PCI Expansion devices to run first during the system boot.
Configuration options: [Ignore] [UEFI only] [Legacy only]

5.5.13 NVMe Configuration

This page will display the NVMe controller and drive information.



Device

The devices and names shown in the NVMe configuration list depends on the connected devices. If no devices are connected, **No NVMe Device Found** will be displayed.

Self Test Option [Short]

This option allows you to select either Short or Extended Self Test. Short option will take couple of minutes, and the extended option will take several minutes to complete.
Configuration options: [Short] [Extended]

Self Test Action [Controller Only Test]

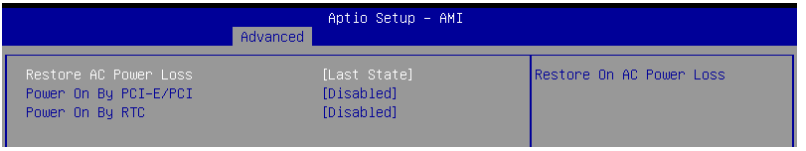
This item allows you to select either to test Controller alone or Controller and NameSpace. Selecting Controller and Namespace option will take a lot longer to complete the test.
Configuration options: [Controller Only Test] [Controller and NameSpace Test]

Run Device Self Test

Press <Enter> to perform device self test for the corresponding Option and Action selected by the user. Pressing the <ESC> key will abort the test. The results shown below is the most recent result logged in the device.

5.5.14 APM Configuration

This page will allow you to configure the Advance Power Management (APM) settings.



Restore AC Power Loss [Last State]

When set to **[Power Off]**, the system goes into off state after an AC power loss. When set to **[Power On]**, the system will reboot after an AC power loss. When set to **[Last State]**, the system goes into either off or on state, whatever the system state was before the AC power loss.
Configuration options: [Power Off] [Power On] [Last State]

Power On By PCI-E/PCI [Disabled]

[Disabled] Disables the PCI/PCIe devices to generate a wake event.

[Enabled] Enables the PCI/PCIe devices to generate a wake event.

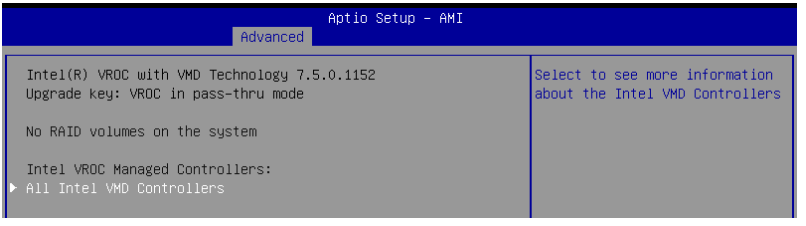
Power On By RTC [Disabled]

[Disabled] Disables RTC to generate a wake event.

[Enabled] When set to [Enabled], the items **RTC Alarm Date (Days)** and **Hour/Minute/Second** will become user-configurable with set values.

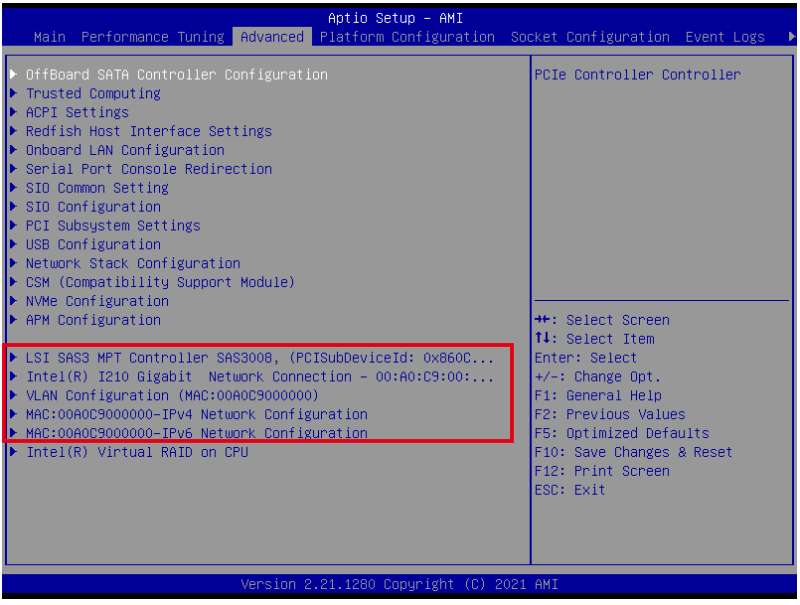
5.5.15 Intel(R) Virtual RAID on CPU

Allows you to manage Intel(R) Virtual RAID on CPU.



5.5.16 Third-party UEFI driver configurations

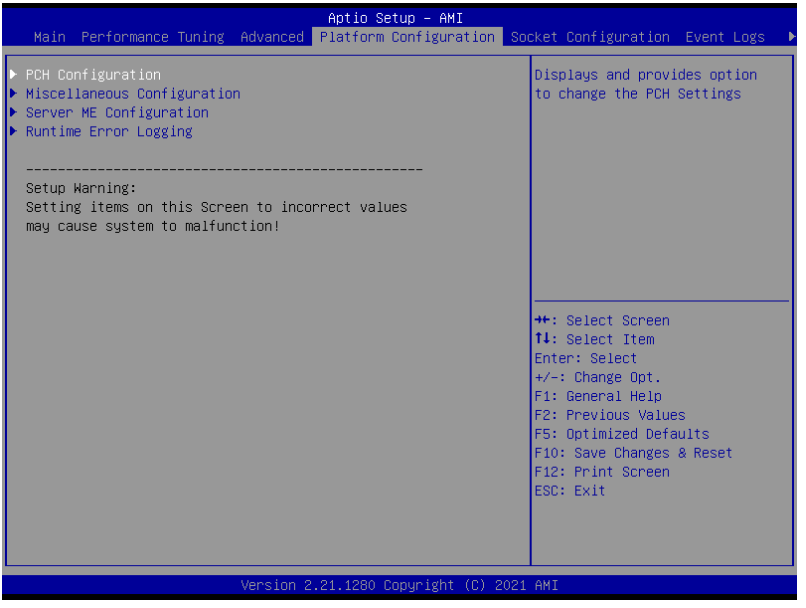
Additonal configuration options for third-party UEFI drivers installed to the system will appear in the section marked in red in the screenshot below.



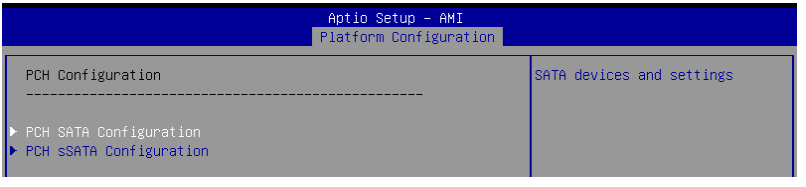
5.6 Platform Configuration menu

The IntelRCSetup menu items allow you to change the platform settings.

Settings items in this menu to incorrect values may cause the system to malfunction!



5.6.1 PCH Configuration



PCH SATA Configuration

SATA Controller [Enable]

Allows you to enable or disable the SATA Controller.
Configuration options: [Disable] [Enable]

The following item appears only when **SATA Controller** is set to **[Enable]**.

Configure SATA as [AHCI]

Allows you to identify the SATA port connected to Solid State Drive or Hard Disk Drive.
Configuration options: [AHCI] [RAID]

SATA Mode options

SATA HDD Unlock [Enable]

When this item is set to **[Enable]** the HDD password unlock will be enabled in the OS.
Configuration options: [Disable] [Enable]

SATA Led locate [Enable]

If this item is enabled, LED/SGPIO is attached.
Configuration options: [Disable] [Enable]

Support Aggressive Link Power Management [Enable]

Allows you to enable or disable SALP.
Configuration options: [Disable] [Enable]

SATA Port 0-7

Hot Plug [Disable]

Allows you to designate SATA port 0-7 as hot pluggable.
Configuration options: [Disable] [Enable]

PCH sSATA Configuration

sSATA Controller [Enable]

Allows you to enable or disable the sSATA Controller.
Configuration options: [Disable] [Enable]

The following item appears only when **sSATA Controller** is set to **[Enable]**.

Configure sSATA as [AHCI]

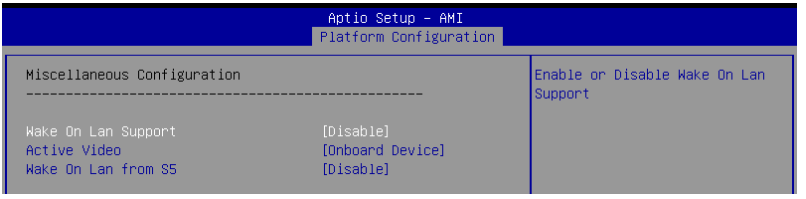
Allows you to identify the SATA port connected to Solid State Drive or Hard Disk Drive.
Configuration options: [AHCI] [RAID]

sSATA Port 0-5

Hot Plug [Disable]

Allows you to designate sSATA port 0-5 as hot pluggable.
Configuration options: [Disable] [Enable]

5.6.2 Miscellaneous Configuration



Wake on LAN Support [Disable]

Allows you to enable or disable Wake On Lan Support.
Configuration options: [Disable] [Enable]

Active Video [Onboard Device]

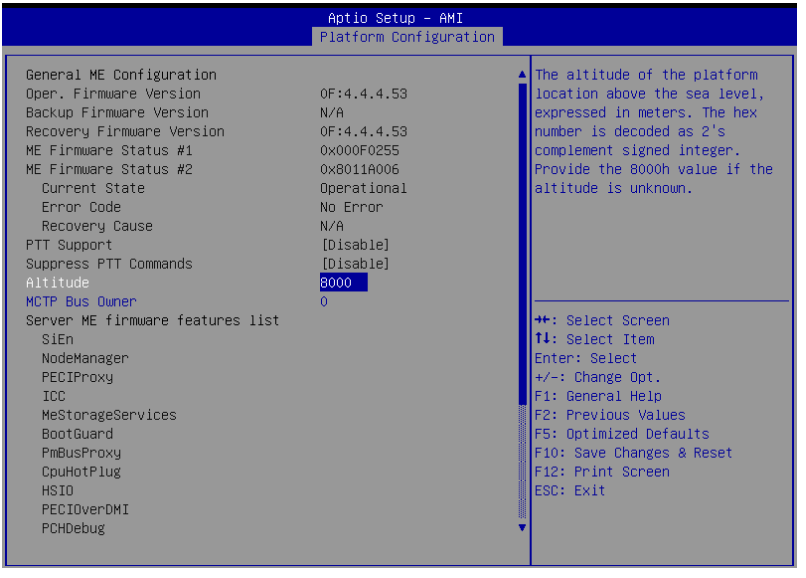
Allows you to select the active video type.
Configuration options: [Auto] [Onboard Device] [PCIE Device]

Wake on LAN from S5 [Disable]

Allows you to enable or disable wake on LAN from S5.
Configuration options: [Disable] [Enable]

5.6.3 Server ME Configuration

Displays the Server ME Technology parameters on your system. Scroll using <Page Up> / <Page Down> keys to see more items.



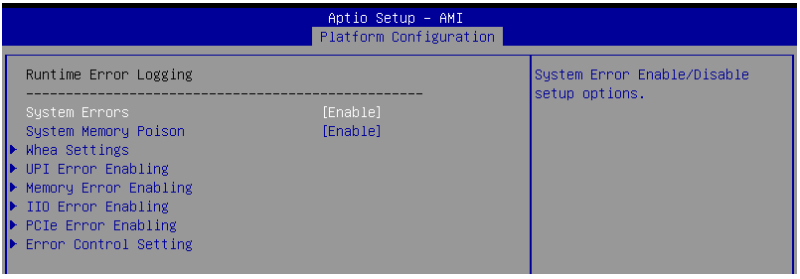
Altitude [8000]

Allows you to set the altitude of the platform location above the sea level, expressed in meters. The hex number is decoded as 2's complement signed integer. Provide the 8000h value if the altitude is unknown.

MCTP Bus Owner [0]

Allows you to enter the MCTP bus owner location on PCIe: [15:8] bus, [7:3] device, [2:0] function. If all zeros sending bus owner will be disabled.

5.6.4 Runtime Error Logging Support



System Errors [Enable]

Allows you to enable or disable System Errors setup options.
Configuration options: [Disable] [Enable]

The following items are only available when **System Errors** is set to **[Enable]**.

System Memory Poison [Enable]

Allows you to enable or disable System Memory Poison.
Configuration options: [Disable] [Enable]

Whea Settings

Whea Support [Enable]

Allows you to enable or disable Whea support.
Configuration options: [Disable] [Enable]

The following items appear only when **Whea Support** is set to **[Enable]**.

Whea Log Memory Error [Enable]

Allows you to enable or disable Whea Log Memory Error.
Configuration options: [Disable] [Enable]

Whea Log Processor Error [Enable]

Allows you to enable or disable Whea Log Processor Error.
Configuration options: [Disable] [Enable]

Whea Log PCI Error [Enable]

Allows you to enable or disable Whea Log PCI Error.
Configuration options: [Disable] [Enable]

UPI Error Enabling

Memory Error Enabling

Memory Error [Enable]

Allows you to enable or disable Memory Error.
Configuration options: [Disable] [Enable]

The following items appear only when **Memory Error** is set to **[Enable]**.

Memory Corrected Error [Enable]

Allows you to enable or disable Memory Corrected Error.
Configuration options: [Disable] [Enable]

The following item appears only when **Memory Corrected Error** is set to **[Enable]**.

Spare Interrupt [SMI]

Allows you to select Spare Interrupt.
Configuration options: [Disable] [SMI] [Error Pin] [CMCI]

PMem CTLR Errors [Enable]

Allows you to enable or disable PMem CTLR Error Reporting & Logging.
Configuration options: [Disable] [Enable]

PMem CTLR Low Priority Error Signaling [SMI]

Allows you to set the signaling for errors bucketed as Low Priority.
Configuration options: [Disable] [SMI] [ERR0# Pin]

PMem CTLR High Priority Error Signaling [SMI]

Allows you to set the signaling for errors bucketed as High Priority.
Configuration options: [Disable] [SMI] [ERR0# Pin]

Set PMem Address Range Scrub [Disable]

Allows you to enable or disable PMem DIMM Physical Address Range Scrub.
Configuration options: [Disable] [Enable]

Set PMem Host Alert Policy for Pat [Enable]

Allows you to enable or disable signaling DDRT interrupt upon receiving Uncorrectable Error for PMem Patrol Scrub.
Configuration options: [Disable] [Enable]

Enable Reporting SPA to OS [Enable]

Allows you to enable or disable reporting SPA to OS. Only set to **[Disable]** for MCE recovery validation.
Configuration options: [Disable] [Enable]

PMem UNC Poison [Enable]

Allows you to enable or disable PMem UNC Poison.
Configuration options: [Disable] [Enable]

Set PMem Host Alert Policy for DPA Error [Poison]

Allows you to configure to signal Poison or Viral upon receiving DIMM Physical Address Error.
Configuration options: [Poison] [Viral]

IIO Error Enabling

IIO/PCH Global Error Support [Enable]

Allows you to enable or disable IIO/PCH Global Error Support.
Configuration options: [Disable] [Enable]

The following item appears only when **IIO/PCH Global Error Support** is set to **[Enable]**.

Os Native AER Support [Disable]

Select FFM or OS native for AER error handling. If OS native is selected, BIOS also intialize FFM first until handshake, which depends on OS capability.
Configuration options: [Disable] [Enable]

IIO Error Registers Clear [Enable]

Allows you to enable or disable Clear IIO Error Registers.
Configuration options: [Disable] [Enable]

PCIe Error Enabling

Corrected Error [Enable]

Enable & escalate Correctable Errors to error pins.
Configuration options: [Disable] [Enable]

Uncorrected Error [Enable]

Enable & escalate Uncorrectable/Recoverable to error pins.
Configuration options: [Disable] [Enable]

Fatal Error Enable [Enable]

Enable & escalate fatal errors to error pins.
Configuration options: [Disable] [Enable]

Error Control Setting

Patrol Scrub Error Reporting [UCNA]

Allows you to select the Patrol Scrub Error type selection.
Configuration options: [UCNA]

2LM Correctable Error Logging in m2mem [Enable]

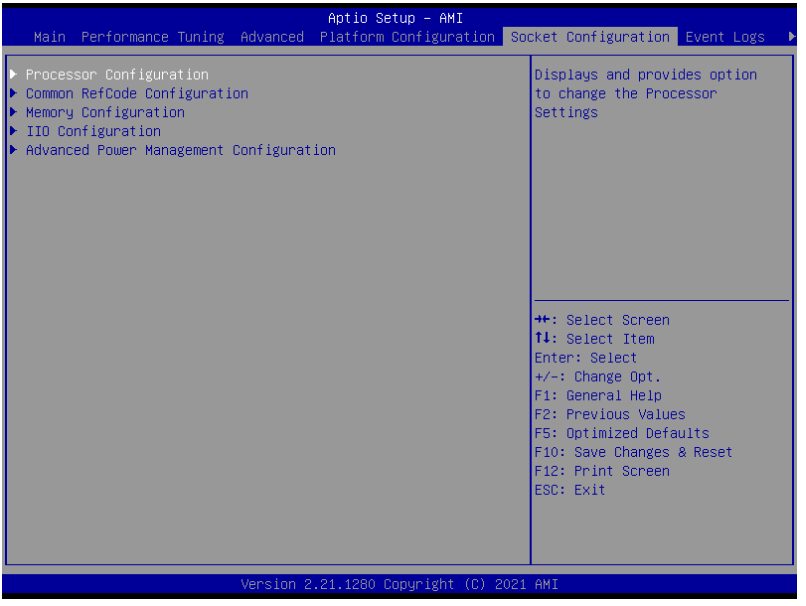
Allows you to enable or disable 2LM correctable error logging in m2mem.
Configuration options: [Disable] [Enable]

Latch First Corrected Error in KTI [Disable]

Allows you to enable or disable latch first corrected error in KTI.
Configuration options: [Disable] [Enable]

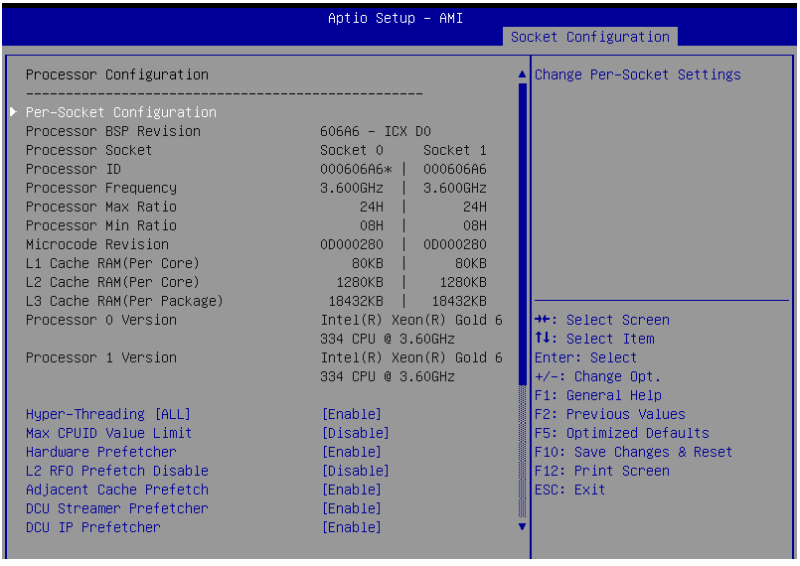
5.7 Socket Configuration menu

The IntelRCSetup menu items allow you to change the socket settings.



5.7.1 Processor Configuration

Scroll using the <Page Up> / <Page Down> keys to view more items.



Per-Socket Configuration

Allows you to change Per-Socket Settings.

CPU Socket 0/1 Configuration

Core Disable Bitmap(Hex) [0]

Allows you to set the Core Disable Bitmap. Set this item to [0] to enable all cores. Set this item to [FFFFFFFFFF] to disable all cores.

At least one core per CPU must be enabled. Disabling all cores is an invalid configuration.

Hyper Threading [ALL] [Enable]

Allows you to enable or disable the Hyper-Threading Technology function. When disabled, only one thread per activated core is enabled. This is the software method to enable or disable Logical Processor threads.
Configuration options: [Disable] [Enable]

Max CPUID Value Limit [Disable]

This item should be enabled in order to boot legacy OSes that cannot support CPUs with extended CPUID functions.
Configuration options: [Disable] [Enable]

Hardware Prefetcher [Enable]

Allows you to enable or disable the mid level cache(L2) streamer prefetcher.
Configuration options: [Disable] [Enable]

L2 RFO Prefetch Disable [Disable]

Allows you to turn enable or disable L2 RFO prefetcher.
Configuration options: [Disable] [Enable]

Adjacent Cache Prefetch [Enable]

Allows you to enable or disable prefetching of adjacent cache lines.
Configuration options: [Disable] [Enable]

DCU Streamer Prefetcher [Enable]

Allows you to enable or disable prefetcher of next L1 data line.
Configuration options: [Disable] [Enable]

DCU IP Prefetcher [Enable]

Allows you to enable or disable prefetch of next L1 line based upon sequential load history.
Configuration options: [Disable] [Enable]

LLC Prefetch [Enable]

Allows you to enable or disable LLC Prefetch on all threads.
Configuration options: [Disable] [Enable]

DCU Mode [Normal]

[Normal] The whole DCU is used for caching.

[Mirror-Mode] DCU is organized as 2x16KB mirrored copies.

Extended APIC [Disable]

Allows you to enable or disable the extended APIC support.
Configuration options: [Disable] [Enable]

This will enable VT-d automatically if x2APIC is enabled.

Enable Intel(R) TXT [Disable]

Allows you to enable or disable Intel(R) TXT.
Configuration options: [Disable] [Enable]

AES-NI [Enable]

Allows you to enable or disable the AES-NI support.
Configuration options: [Disable] [Enable]

TME, TME-MT, TDX

Total Memory Encryption (TME) [Disabled]

Allows you to enable or disable Total Memory Encryption (TME).
Configuration options: [Disabled] [Enabled]

Limit CPU PA to 46 bits [Enable]

Limits CPU physical address to 46 bits to support older Hyper-v. If enabled, automatically disables TME-MT.
Configuration options: [Disable] [Enable]

PSMI Configuration

Global PSMI Enable [Enable]

Configuration options: [Disable] [Enable] [Force setup]

The following item appears only when **Global PSMI Enable** is set to **[Enable]** or **[Force setup]**.

Socket 0/1 Configuration

PSMI Enable [Disable]

Configuration options: [Disable] [Enable]

The following items appear only when **PSMI Enable** is set to **[Enable]**.

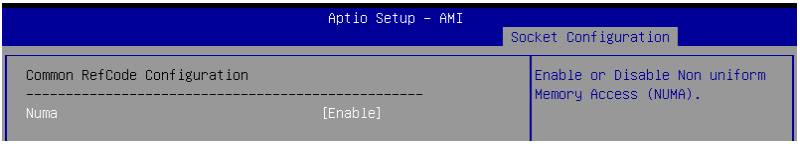
PSMI Handler Size [256K]

Configuration options: [256K] [512K] [1M]

PSMI Trace Region 0-4 [Disable]

Configuration options: [Disable] [Enable]

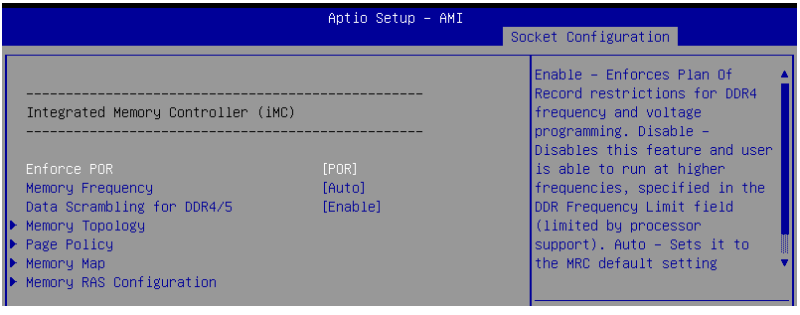
5.7.2 Common RefCode Configuration



Numa [Enable]

This item enables or disables the Non uniform Memory Access (NUMA).
Configuration options: [Disable] [Enable]

5.7.3 Memory Configuration



Enforce POR [POR]

Allows you to enforce POR restrictions for DDR4 frequency and voltage programming. If this item is set to **[Disable]**, user will be able to run at higher frequencies, specified in the DDR Frequency Limit field (limited by processor support).
Configuration options: [POR] [Disable]

Memory Frequency [Auto]

Allows you to select the maximum memory frequency setting in Mhz. If Enforce POR is set to **[Disable]**, user will be able to run at higher frequencies than the memory support (limited by processor support). Do not select Reserved.
Configuration options: [Auto] [1200] - [4800-OvrClk]

Data Scrambling for DDR4/5 [Enable]

[Disable] Disables this feature.

[Enable] Enables data scrambling for DDR4 and DDR5.

Memory Topology

Displays memory topology with DIMM population information.

Page Policy

Allows you to set memory page policy parameters.

Page Policy [Adaptive]

Configuration options: [Closed] [Adaptive]

Memory Map

Allows you to set memory mapping settings.

Volatile Memory Mode [2LM]

Selects 1LM or 2LM mode for volatile memory. For 2LM memory mode, BIOS will try to configure 2LM, but if BIOS is unable to configure 2LM, volatile memory mode will fall beck to 1LM.
Configuration options: [1LM] [2LM]

The following item appears only when **Volatile Memory Mode** is set to **[2LM]**.

AppDirect cache [Disabled]

Allows you to enable or disable caching for the memory region.
Configuration options: [Disabled] [Enabled]

eADR Support [Disable]

Allows you to enable or disable eADR capability in th platform, Pmem/AppDirect caching knob takes precedence.
Configuration options: [Disable] [Enable] [Auto]

The following item appears only when **eADR Support** is set to **[Enable]** or **[Auto]**.

CPU Cache Flush Mode [Parallel]

Allows you to set CPU cache flush execution mode.
Configuration options: [Serial] [Parallel]

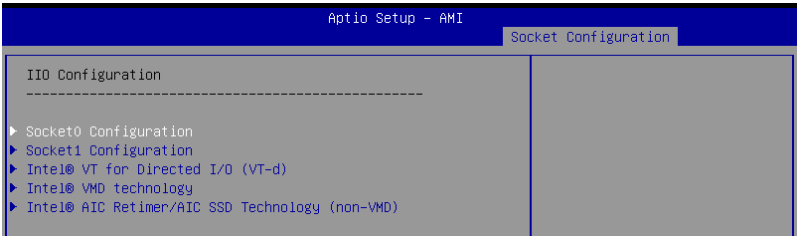
Memory RAS Configuration

Displays and provides options to change the memory RAS Settings.

Correctable Error Threshold [7FFF]

Allows you to set the Correctable Error Threshold (0x01 - 0x7fff) used for sparing, and leaky bucket.

5.7.4 IIO Configuration



Socket0 Configuration

IOU0 (IIO PCie Port 1) [x8x8]

Allows you to select PCIe port Bifurcation for selected slot(s).
Configuration options: [Auto] [x4x4x4x4] [x4x4x8] [x8x4x4] [x8x8] [x16]

IOU1 (IIO PCie Port 2) [x4x4x4x4]

Allows you to select PCIe port Bifurcation for selected slot(s).
Configuration options: [Auto] [x4x4x4x4] [x4x4x8] [x8x4x4] [x8x8] [x16]

IOU2 (IIO PCie Port 3) [x16]

Allows you to select PCIe port Bifurcation for selected slot(s).
Configuration options: [Auto] [x4x4x4x4] [x4x4x8] [x8x4x4] [x8x8] [x16]

IOU3 (IIO PCie Port 4) [x16]

Allows you to select PCIe port Bifurcation for selected slot(s).
Configuration options: [Auto] [x4x4x4x4] [x4x4x8] [x8x4x4] [x8x8] [x16]

IOU4 (IIO PCie Port 5) [x16]

Allows you to select PCIe port Bifurcation for selected slot(s).
Configuration options: [Auto] [x4x4x4x4] [x4x4x8] [x8x4x4] [x8x8] [x16]

Enable PCI-E Completion Timeout (Per-Port) [No]

Allows you enable or disable the PCIe Completion Timeout in Device Control2 register.
Configuration options: [Yes] [No]

The following item appear only when **Enable PCI-E Completion Timeout (Per-Port)** is set to **[Yes]**.

PCI-E Completion Timeout Value [260ms to 900ms]

Allows you to set the PCIe Completion Timeout to program in Device Control2 register.
Configuration options: [50us to 50ms] [50us to 100us] [1ms to 10ms] [16ms to 55ms] [65ms to 210ms] [260ms to 900ms] [1s to 3.5s]

Sck0 RP Correctable Err [No]

Applies to root ports only. Allows you to enable or disable interrupt on correctable errors.
Configuration options: [Yes] [No]

Sck0 RP NonFatal Uncorrectable Err [No]

Applies to root ports only. Allows you to enable or disable interrupt on a non-fatal error.
Configuration options: [Yes] [No]

Sck0 RP Fatal Uncorrectable Err [No]

Applies to root ports only. Allows you to enable or disable MSI/INTx interrupt on fatal errors.
Configuration options: [Yes] [No]

TraceHub Configuration Menu

North Trace Hub Enable Mode [Disabled]
Select **[Host Debugger]** if Trace Hub is used with host debugger tool, or select **[Target Debugger]** if Trace Hub is used by target debugger software.
Configuration options: [Disabled] [Host Debugger] [Target Debugger]

The following items appear only when **North Trace Hub Enable Mode** is set to **[Host Debugger]** or **[Target Debugger]**.

North TH Mem Buffer Size 0 [None/OS]
Select size of memory region 0 buffer. Choose **[None/OS]** if OS-supported memory or trace fowarding is desired.
Configuration options: [None/OS] [1MB] [8MB] [64MB] [128MB] [256MB] [512MB]

Limitation of total buffer size (PCH + CPU) is 512MB.

North TH Mem Buffer Size 1 [None/OS]
Select size of memory region 1 buffer. Choose **[None/OS]** if OS-supported memory or trace fowarding is desired.
Configuration options: [None/OS] [1MB] [8MB] [64MB] [128MB] [256MB] [512MB]

Limitation of total buffer size (PCH + CPU) is 512MB.

Sierra Peak Memory Region Buffer Size [None]
Select size of memory buffer for each single Sierra Peak instance.
Configuration options: [None] [1MB] [8MB] [64MB] [128MB] [256MB] [512MB] [1GB]

Port 0/DMI

Settings related to PCI Express Ports (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A4B/4C/4D/5A/5B/5C/5D)

Link Speed [Auto]

Choose the Link Speed for this PCIe port.
Configuration options: [Auto] [Gen 1 (2.5 GT/s)] [Gen 2 (5 GT/s)] [Gen 3 (8 GT/s)]

The following item appears only when **Link Speed** is set to **[Auto]**, **[Gen 2 (5 GT/s)]**, or **[Gen 3 (8 GT/s)]**.

PCI-E Port DeEmphasis [-6.0 dB]

De-Emphasis control (LNKCON2 [6]) for this PCIe port.
Configuration options: [-6.0 dB] [-3.5 dB]

PCI-E Port Clocking [Common]

Configure port clocking via LNKCON [6]. This refers to this component and the down stream component.
Configuration options: [Distinct] [Common]

PCI-E Port Clock Gating [Enable]

Allows you to enable or disable Clock Gating for this PCIe port.
Configuration options: [Disable] [Enable]

Data Link Feature Exchange [Enable]

Allows you to enable or disable data link feature negotiation in the Data Link Feature Capabilities (DLFCAP) register.
Configuration options: [Disable] [Enable]

DMI Port MPSS [Auto]

Configure Max Payload Size Supported in PCIe Device Capabilities register. If default value is not used make sure MPSS in PCH root ports is updated to the same or smaller value.
Configuration options: [128B] [256B] [Auto]

PCI-E Port D-state [D0]

Set to D0 for normal operation, D3Hot to bi in low-power state.
Configuration options: [D0] [D3Hot]

PCI-E ASPM Support [Disable]

Allows you to enable or disable ASPM (L1) support for the downstream devices.
Configuration options: [Auto] [L1 Only] [Disable]

The following item appears only when **PCI-E ASPM Support** is set to **[Auto]** or **[L1 Only]**.

PCI-E Port L1 Exit Latency [8uS - 16uS]

The length of time this port requires to complete transition from L1 to L0.
Configuration options: [<1uS] [1uS - 2uS] [2uS - 4uS] [4uS - 8uS] [8uS - 16uS] [16uS - 32uS] [32uS - 64uS] [>64uS]

MSI [Disable]

Configuration options: [Disable] [Enable]

PCI-E Extended Sync [No]

Allows you to enable or disable the Extended Sync Mode (D:x F:0 0:7Ch B:7) where x is 0-9.
Configuration options: [No] [Yes]

Compliance Mode [No]
Allows you to enable or disable Compliance Mode for this PCIe port.
Configuration options: [No] [Yes]

EOI [Enable]
Configuration options: [Disable] [Enable]

Fatal Err Over [No]
Allows you to enable or disable forcing fatal error propagation to the IIO core error logic for this port.
Configuration options: [No] [Yes]

Non-Fatal Err Over [No]
Allows you to enable or disable forcing non-fatal error propagation to the IIO core error logic for this port.
Configuration options: [No] [Yes]

Corr Err Over [No]
Allows you to enable or disable forcing correctable error propagation to the IIO core error logic for this port.
Configuration options: [No] [Yes]

ACPI PME Interrupt [No]
Allows you to enable or disable ACPI PME Interrupts generation from this port.
Configuration options: [No] [Yes]

P2P Memory Read [Enable]
Controls Peer2Peer Memory Read Decoding.
Configuration options: [Disable] [Enable]

PME to ACK [Enable]
Controls timeout usage for IIO waiting on PME_TO_ACK after a PME_TURN_OFF message.
Configuration options: [Disable] [Enable]

Unsupported Request [Disable]
Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port.
Configuration options: [Disable] [Enable]

Alternate TxEq [Disable]
Allows you to enable or disable TxEq.
Configuration options: [Disable] [Enable]

SRIS [Disable]
Allows you to enable or disable SRIS.
Configuration options: [Disable] [Enable]

ECRC Generation [Disable]
Allows you to enable or disable ECRC Generation (Error Capabilities and Control Register).
Configuration options: [Disable] [Enable]

ECRC Check [Disable]
Allows you to enable or disable ECRC Check (Error Capabilities and Control Register).
Configuration options: [Disable] [Enable]

SERRE [Disable]
Allows you to enable or disable SERRE (SERR Reporting Enable).
Configuration options: [Disable] [Enable]

IODC Configuration [KTI Option]
Allows you to enable or disable IODC (IO Direct Cache): Generate snoops instead of memory lookups, for remote InvItoM (IIO) and/or WCiLF (cores). Configuration options: [KTI Option] [Auto] [Enable for Remote InvItoM Hybrid Push] [InvItoM AllocFlow] [Enable for Remote InvItoM Hybrid AllocNonAlloc] [Enable for Remote InvItoM and Remove WViLF]

MCTP [Yes]
Allows you to enable or disable MCTP.
Configuration options: [No] [Yes]

Port 1A/2A/4A/5A

Settings related to PCI Express Ports (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A4 B/4C/4D/5A/5B/5C/5D)

PCI-E Port [Auto]
Allows you to enable or disable the port and expose/hide its CFG space. In auto mode, the BIOS will remove the EXP port if there is no device or errors on that device and that device is not HP capable.
Configuration options: [Auto] [Disable] [Enable]

The following items appear only when **PCI-E Port** is set to **[Auto]** or **[Enable]**.

PCI-E Port Link Disable [No]
This option disabled the link so that the no training occurs but the CFG space is still active.
Configuration options: [No] [Yes]

Link Speed [Auto]
Choose the Link Speed for this PCIe port.
Configuration options: [Auto] [Gen 1 (2.5 GT/s)] [Gen 2 (5 GT/s)] [Gen 3 (8 GT/s)]

Override Max Link Width [Auto]
Override the max link width that was set by bifurcation.
Configuration options: [Auto] [x1] [x2] [x4] [x8] [x16]

The following item appears only when **Link Speed** is set to **[Auto]**, **[Gen 2 (5 GT/s)]**, or **[Gen 3 (8 GT/s)]**.

PCI-E Port DeEmphasis [-3.5 dB]
De-Emphasis control (LNKCON2 [6]) for this PCIe port.
Configuration options: [-6.0 dB] [-3.5 dB]

PCI-E Port Clocking [Common]
Configure port clocking via LNKCON [6]. This refers to this component and the down stream component.
Configuration options: [Distinct] [Common]

PCI-E Port Clock Gating [Enable]
Allows you to enable or disable Clock Gating for this PCIe port.
Configuration options: [Disable] [Enable]

Data Link Feature Exchange [Enable]
Allows you to enable or disable data link feature negotiation in the Data Link Feature Capabilities (DLFCAP) register.
Configuration options: [Disable] [Enable]

PCI-E Port MPSS [Auto]
Configure Max Payload Size Supported in PCIe Device Capabilities register.
Configuration options: [128B] [256B] [512B] [Auto]

PCI-E Port D-state [D0]
Set to D0 for normal operation, D3Hot to bi in low-power state.
Configuration options: [D0] [D3Hot]

PCI-E ASPM Support [Disable]
Allows you to enable or disable ASPM (L1) support for the downstream devices.
Configuration options: [Auto] [L1 Only] [Disable]

The following item appears only when **PCI-E ASPM Support** is set to **[Auto]** or **[L1 Only]**.

PCI-E Port L1 Exit Latency [8uS - 16uS]
The length of time this port requires to complete transition from L1 to L0.
Configuration options: [<1uS] [1uS - 2uS] [2uS - 4uS] [4uS - 8uS] [8uS - 16uS] [16uS - 32uS] [32uS - 64uS] [>64uS]

MSI [Disable]
Configuration options: [Disable] [Enable]

PCI-E Extended Sync [No]
Allows you to enable or disable the Extended Sync Mode (D:x F:0 0:7Ch B:7) where x is 0-9.
Configuration options: [No] [Yes]

PCI-E Detect Wait Time [Auto]
Set PCIe port TxRx detect polling.
Configuration options: [Disable] [500ms] [Auto]

Compliance Mode [No]
Allows you to enable or disable Compliance Mode for this PCIe port.
Configuration options: [No] [Yes]

EOI [Disable]
Configuration options: [Disable] [Enable]

Fatal Err Over [No]
Allows you to enable or disable forcing fatal error propagation to the IIO core error logic for this port.
Configuration options: [No] [Yes]

Non-Fatal Err Over [No]
Allows you to enable or disable forcing non-fatal error propagation to the IIO core error logic for this port.
Configuration options: [No] [Yes]

Corr Err Over [No]
Allows you to enable or disable forcing correctable error propagation to the IIO core error logic for this port.
Configuration options: [No] [Yes]

ACPI PME Interrupt [No]
Allows you to enable or disable ACPI PME Interrupts generation from this port.
Configuration options: [No] [Yes]

P2P Memory Read [Enable]
Controls Peer2Peer Memory Read Decoding.
Configuration options: [Disable] [Enable]

PME to ACK [Enable]
Controls timeout usage for IIO waiting on PME_TO_ACK after a PME_ TURN_OFF message.
Configuration options: [Disable] [Enable]

PM ACPI Mode [No]
When enabled, _HPGPE message is generated, otherwise MSI is generated on PM event.
Configuration options: [No] [Yes]

Unsupported Request [Disable]
Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port.
Configuration options: [Disable] [Enable]

Alternate TxEq [Disable]
Allows you to enable or disable TxEq.
Configuration options: [Disable] [Enable]

SRIS [Disable]
Allows you to enable or disable SRIS.
Configuration options: [Disable] [Enable]

ECRC Generation [Disable]
Allows you to enable or disable ECRC Generation (Error Capabilities and Control Register).
Configuration options: [Disable] [Enable]

ECRC Check [Disable]
Allows you to enable or disable ECRC Check (Error Capabilities and Control Register).
Configuration options: [Disable] [Enable]

SERRE [Disable]
Allows you to enable or disable SERRE (SERR Reporting Enable).
Configuration options: [Disable] [Enable]

IODC Configuration [KTI Option]
Allows you to enable or disable IODC (IO Direct Cache): Generate snoops instead of memory lookups, for remote InvItoM (IIO) and/or WCiLF (cores).
Configuration options: [KTI Option] [Auto] [Enable for Remote InvItoM Hybrid Push] [InvItoM AllocFlow] [Enable for Remote InvItoM Hybrid AllocNonAlloc] [Enable for Remote InvItoM and Remove WViLF]

Non-Transparent Bridge PCIe Port Definition [Transparent Bridge]
Configures port as TB, NB-NTB, or NTB-RP (DON'T SELECT NTB-RP for legacy IIO on AO Si!)
Configuration options: [Transparent Bridge] [NTB to NTB]

Imbar2 Size [22]
Used to set the prefetchable Imbar2 size on primary side of NTB. Value range <12...51> representing BAR sizes <4KB...128PB>.

Embar1 Size [22]
Used to set the prefetchable Embar1 size on primary side of NTB. Value range <12...51> representing BAR sizes <4KB...128PB>.

Embar2 Size [22]
Used to set the prefetchable Embar2 size on primary side of NTB. Value range <12...51> representing BAR sizes <4KB...128PB>.

Hide Port? [No]
User can force to hide this root port from OS.
Configuration options: [No] [Yes]

MCTP [Yes]
Allows you to enable or disable MCTP.
Configuration options: [No] [Yes]

Port 1C/2B/2C/2D

Settings related to PCI Express Ports (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A4B/4C/4D/5A/5B/5C/5D)

PCI-E Port [Auto]
Allows you to enable or disable the port and expose/hide its CFG space. In auto mode, the BIOS will remove the EXP port if there is no device or errors on that device and that device is not HP capable.
Configuration options: [Auto] [Disable] [Enable]

The following items appear only when **PCI-E Port** is set to **[Auto]** or **[Enable]**.

PCI-E Port Link Disable [No]
This option disabled the link so that the no training occurs but the CFG space is still active.
Configuration options: [No] [Yes]

Link Speed [Auto]
Choose the Link Speed for this PCIe port.
Configuration options: [Auto] [Gen 1 (2.5 GT/s)] [Gen 2 (5 GT/s)] [Gen 3 (8 GT/s)]

Override Max Link Width [Auto]
Override the max link width that was set by bifurcation.
Configuration options: [Auto] [x1] [x2] [x4] [x8] [x16]

The following item appears only when **Link Speed** is set to **[Auto]**, **[Gen 2 (5 GT/s)]**, or **[Gen 3 (8 GT/s)]**.

PCI-E Port DeEmphasis [-3.5 dB]
De-Emphasis control (LNKCON2 [6]) for this PCIe port.
Configuration options: [-6.0 dB] [-3.5 dB]

PCI-E Port Clocking [Common]
Configure port clocking via LNKCON [6]. This refers to this component and the down stream component.
Configuration options: [Distinct] [Common]

PCI-E Port Clock Gating [Enable]
Allows you to enable or disable Clock Gating for this PCIe port.
Configuration options: [Disable] [Enable]

Data Link Feature Exchange [Enable]
Allows you to enable or disable data link feature negotiation in the Data Link Feature Capabilities (DLFCAP) register.
Configuration options: [Disable] [Enable]

PCI-E Port MPSS [Auto]
Configure Max Payload Size Supported in PCIe Device Capabilities register.
Configuration options: [128B] [256B] [512B] [Auto]

PCI-E Port D-state [D0]
Set to D0 for normal operation, D3Hot to bi in low-power state.
Configuration options: [D0] [D3Hot]

PCI-E ASPM Support [Disable]
Allows you to enable or disable ASPM (L1) support for the downstream devices.
Configuration options: [Auto] [L1 Only] [Disable]

The following item appears only when **PCI-E ASPM Support** is set to **[Auto]** or **[L1 Only]**.

PCI-E Port L1 Exit Latency [8uS - 16uS]
The length of time this port requires to complete transition from L1 to L0.
Configuration options: [<1uS] [1uS - 2uS] [2uS - 4uS] [4uS - 8uS] [8uS - 16uS] [16uS - 32uS] [32uS - 64uS] [>64uS]

MSI [Disable]
Configuration options: [Disable] [Enable]

PCI-E Extended Sync [No]
Allows you to enable or disable the Extended Sync Mode (D:x F:0 0:7Ch B:7) where x is 0-9.
Configuration options: [No] [Yes]

PCI-E Detect Wait Time [Auto]
Set PCIe port TxRx detect polling.
Configuration options: [Disable] [500ms] [Auto]

Compliance Mode [No]
Allows you to enable or disable Compliance Mode for this PCIe port.
Configuration options: [No] [Yes]

EOI [Disable]
Configuration options: [Disable] [Enable]

Fatal Err Over [No]
Allows you to enable or disable forcing fatal error propagation to the IIO core error logic for this port.
Configuration options: [No] [Yes]

Non-Fatal Err Over [No]
Allows you to enable or disable forcing non-fatal error propagation to the IIO core error logic for this port.
Configuration options: [No] [Yes]

Corr Err Over [No]
Allows you to enable or disable forcing correctable error propagation to the IIO core error logic for this port.
Configuration options: [No] [Yes]

ACPI PME Interrupt [No]
Allows you to enable or disable ACPI PME Interrupts generation from this port.
Configuration options: [No] [Yes]

P2P Memory Read [Enable]
Controls Peer2Peer Memory Read Decoding.
Configuration options: [Disable] [Enable]

PME to ACK [Enable]
Controls timeout usage for IIO waiting on PME_TO_ACK after a PME_ TURN_OFF message.
Configuration options: [Disable] [Enable]

PM ACPI Mode [No]
When enabled, _HPGPE message is generated, otherwise MSI is generated on PM event.
Configuration options: [No] [Yes]

Unsupported Request [Disable]
Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port.
Configuration options: [Disable] [Enable]

Alternate TxEq [Disable]
Allows you to enable or disable TxEq.
Configuration options: [Disable] [Enable]

SRIS [Disable]
Allows you to enable or disable SRIS.
Configuration options: [Disable] [Enable]

ECRC Generation [Disable]
Allows you to enable or disable ECRC Generation (Error Capabilities and Control Register).
Configuration options: [Disable] [Enable]

ECRC Check [Disable]
Allows you to enable or disable ECRC Check (Error Capabilities and Control Register).
Configuration options: [Disable] [Enable]

SERRE [Disable]
Allows you to enable or disable SERRE (SERR Reporting Enable).
Configuration options: [Disable] [Enable]

IODC Configuration [KTI Option]
Allows you to enable or disable IODC (IO Direct Cache): Generate snoops instead of memory lookups, for remote InvItoM (IIO) and/or WCiLF (cores).
Configuration options: [KTI Option] [Auto] [Enable for Remote InvItoM Hybrid Push] [InvItoM AllocFlow] [Enable for Remote InvItoM Hybrid AllocNonAlloc] [Enable for Remote InvItoM and Remove WViLF]

Hide Port? [No]
User can force to hide this root port from OS.
Configuration options: [No] [Yes]

MCTP [Yes]
Allows you to enable or disable MCTP.
Configuration options: [No] [Yes]

Socket1 Configuration

IOU0 (IIO PCie Port 1) [x16]

Allows you to select PCIe port Bifurcation for selected slot(s).
Configuration options: [Auto] [x4x4x4x4] [x4x4x8] [x8x4x4] [x8x8] [x16]

IOU1 (IIO PCie Port 2) [x16]

Allows you to select PCIe port Bifurcation for selected slot(s).
Configuration options: [Auto] [x4x4x4x4] [x4x4x8] [x8x4x4] [x8x8] [x16]

IOU2 (IIO PCie Port 3) [x16]

Allows you to select PCIe port Bifurcation for selected slot(s).
Configuration options: [Auto] [x4x4x4x4] [x4x4x8] [x8x4x4] [x8x8] [x16]

IOU3 (IIO PCie Port 4) [x16]

Allows you to select PCIe port Bifurcation for selected slot(s).
Configuration options: [Auto] [x4x4x4x4] [x4x4x8] [x8x4x4] [x8x8] [x16]

IOU4 (IIO PCie Port 5) [x8x4x4]

Allows you to select PCIe port Bifurcation for selected slot(s).
Configuration options: [Auto] [x4x4x4x4] [x4x4x8] [x8x4x4] [x8x8] [x16]

Enable PCI-E Completion Timeout (Per-Port) [Yes]

Allows you enable or disable the PCIe Completion Timeout in Device Control2 register.
Configuration options: [Yes] [No]

The following item appear only when **Enable PCI-E Completion Timeout (Per-Port)** is set to **[Yes]**.

PCI-E Completion Timeout Value [260ms to 900ms]

Allows you to set the PCIe Completion Timeout to program in Device Control2 register.
Configuration options: [50us to 50ms] [50us to 100us] [1ms to 10ms] [16ms to 55ms] [65ms to 210ms] [260ms to 900ms] [1s to 3.5s]

Sck1 RP Correctable Err [No]

Applies to root ports only. Allows you to enable or disable interrupt on correctable errors.
Configuration options: [Yes] [No]

Sck1 RP NonFatal Uncorrectable Err [No]

Applies to root ports only. Allows you to enable or disable interrupt on a non-fatal error.
Configuration options: [Yes] [No]

Sck1 RP Fatal Uncorrectable Err [No]

Applies to root ports only. Allows you to enable or disable MSI/INTx interrupt on fatal errors.
Configuration options: [Yes] [No]

TraceHub Configuration Menu

North Trace Hub Enable Mode [Disabled]

Select **[Host Debugger]** if Trace Hub is used with host debugger tool, or select **[Target Debugger]** if Trace Hub is used by target debugger software.
Configuration options: [Disabled] [Host Debugger] [Target Debugger]

The following items appear only when **North Trace Hub Enable Mode** is set to **[Host Debugger]** or **[Target Debugger]**.

North TH Mem Buffer Size 0 [None/OS]

Select size of memory region 0 buffer. Choose **[None/OS]** if OS-supported memory or trace fowarding is desired.
Configuration options: [None/OS] [1MB] [8MB] [64MB] [128MB] [256MB] [512MB]

Limitation of total buffer size (PCH + CPU) is 512MB.

North TH Mem Buffer Size 1 [None/OS]
Select size of memory region 1 buffer. Choose **[None/OS]** if OS-supported memory or trace fowarding is desired.
Configuration options: [None/OS] [1MB] [8MB] [64MB] [128MB] [256MB] [512MB]

Limitation of total buffer size (PCH + CPU) is 512MB.

Sierra Peak Memory Region Buffer Size [None]
Select size of memory buffer for each single Sierra Peak instance.
Configuration options: [None] [1MB] [8MB] [64MB] [128MB] [256MB] [512MB] [1GB]

Port 1A/2A/4A/5A

Settings related to PCI Express Ports (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A4B/4C/4D/5A/5B/5C/5D)

PCI-E Port [Auto]
Allows you to enable or disable the port and expose/hide its CFG space. In auto mode, the BIOS will remove the EXP port if there is no device or errors on that device and that device is not HP capable.
Configuration options: [Auto] [Disable] [Enable]

The following items appear only when **PCI-E Port** is set to **[Auto]** or **[Enable]**.

PCI-E Port Link Disable [No]
This option disabled the link so that the no training occurs but the CFG space is still active.
Configuration options: [No] [Yes]

Link Speed [Auto]
Choose the Link Speed for this PCIe port.
Configuration options: [Auto] [Gen 1 (2.5 GT/s)] [Gen 2 (5 GT/s)] [Gen 3 (8 GT/s)]

Override Max Link Width [Auto]
Override the max link width that was set by bifurcation.
Configuration options: [Auto] [x1] [x2] [x4] [x8] [x16]

The following item appears only when **Link Speed** is set to **[Auto]**, **[Gen 2 (5 GT/s)]**, or **[Gen 3 (8 GT/s)]**.

PCI-E Port DeEmphasis [-3.5 dB]
De-Emphasis control (LNKCON2 [6]) for this PCIe port.
Configuration options: [-6.0 dB] [-3.5 dB]

PCI-E Port Clocking [Common]
Configure port clocking via LNKCON [6]. This refers to this component and the down stream component.
Configuration options: [Distinct] [Common]

PCI-E Port Clock Gating [Enable]
Allows you to enable or disable Clock Gating for this PCIe port.
Configuration options: [Disable] [Enable]

Data Link Feature Exchange [Enable]
Allows you to enable or disable data link feature negotiation in the Data Link Feature Capabilities (DLFCAP) register.
Configuration options: [Disable] [Enable]

PCI-E Port MPSS [Auto]
Configure Max Payload Size Supported in PCIe Device Capabilities register.
Configuration options: [128B] [256B] [512B] [Auto]

PCI-E Port D-state [D0]
Set to D0 for normal operation, D3Hot to bi in low-power state.
Configuration options: [D0] [D3Hot]

PCI-E ASPM Support [Disable]
Allows you to enable or disable ASPM (L1) support for the downstream devices.
Configuration options: [Auto] [L1 Only] [Disable]

The following item appears only when **PCI-E ASPM Support** is set to **[Auto]** or **[L1 Only]**.

PCI-E Port L1 Exit Latency [8uS - 16uS]
The length of time this port requires to complete transition from L1 to L0.
Configuration options: [<1uS] [1uS - 2uS] [2uS - 4uS] [4uS - 8uS] [8uS - 16uS] [16uS - 32uS] [32uS - 64uS] [>64uS]

MSI [Disable]
Configuration options: [Disable] [Enable]

PCI-E Extended Sync [No]
Allows you to enable or disable the Extended Sync Mode (D:x F:0 0:7Ch B:7) where x is 0-9.
Configuration options: [No] [Yes]

PCI-E Detect Wait Time [Auto]
Set PCIe port TxRx detect polling.
Configuration options: [Disable] [500ms] [Auto]

Compliance Mode [No]
Allows you to enable or disable Compliance Mode for this PCIe port.
Configuration options: [No] [Yes]

EOI [Disable]
Configuration options: [Disable] [Enable]

Fatal Err Over [No]
Allows you to enable or disable forcing fatal error propagation to the IIO core error logic for this port.
Configuration options: [No] [Yes]

Non-Fatal Err Over [No]
Allows you to enable or disable forcing non-fatal error propagation to the IIO core error logic for this port.
Configuration options: [No] [Yes]

Corr Err Over [No]
Allows you to enable or disable forcing correctable error propagation to the IIO core error logic for this port.
Configuration options: [No] [Yes]

ACPI PME Interrupt [No]
Allows you to enable or disable ACPI PME Interrupts generation from this port.
Configuration options: [No] [Yes]

P2P Memory Read [Enable]
Controls Peer2Peer Memory Read Decoding.
Configuration options: [Disable] [Enable]

PME to ACK [Enable]
Controls timeout usage for IIO waiting on PME_TO_ACK after a PME_ TURN_OFF message.
Configuration options: [Disable] [Enable]

PM ACPI Mode [No]
When enabled, _HPGPE message is generated, otherwise MSI is generated on PM event.
Configuration options: [No] [Yes]

Unsupported Request [Disable]
Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port.
Configuration options: [Disable] [Enable]

Alternate TxEq [Disable]
Allows you to enable or disable TxEq.
Configuration options: [Disable] [Enable]

SRIS [Disable]
Allows you to enable or disable SRIS.
Configuration options: [Disable] [Enable]

ECRC Generation [Disable]
Allows you to enable or disable ECRC Generation (Error Capabilities and Control Register).
Configuration options: [Disable] [Enable]

ECRC Check [Disable]
Allows you to enable or disable ECRC Check (Error Capabilities and Control Register).
Configuration options: [Disable] [Enable]

SERRE [Disable]
Allows you to enable or disable SERRE (SERR Reporting Enable).
Configuration options: [Disable] [Enable]

IODC Configuration [KTI Option]
Allows you to enable or disable IODC (IO Direct Cache): Generate snoops instead of memory lookups, for remote InvItoM (IIO) and/or WCiLF (cores).
Configuration options: [KTI Option] [Auto] [Enable for Remote InvItoM Hybrid Push] [InvItoM AllocFlow] [Enable for Remote InvItoM Hybrid AllocNonAlloc] [Enable for Remote InvItoM and Remove WViLF]

Non-Transparent Bridge PCIe Port Definition [Transparent Bridge]
Configures port as TB, NB-NTB, or NTB-RP (DON'T SELECT NTB-RP for legacy IIO on AO Si!)
Configuration options: [Transparent Bridge] [NTB to NTB]

Imbar2 Size [22]
Used to set the prefetchable Imbar2 size on primary side of NTB. Value range <12...51> representing BAR sizes <4KB...128PB>.

Embar1 Size [22]
Used to set the prefetchable Embar1 size on primary side of NTB. Value range <12...51> representing BAR sizes <4KB...128PB>.

Embar2 Size [22]
Used to set the prefetchable Embar2 size on primary side of NTB. Value range <12...51> representing BAR sizes <4KB...128PB>.

Hide Port? [No]
User can force to hide this root port from OS.
Configuration options: [No] [Yes]

MCTP [Yes]
Allows you to enable or disable MCTP.
Configuration options: [No] [Yes]

Port 5B/5C

Settings related to PCI Express Ports (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A4B/4C/4D/5A/5B/5C/5D)

PCI-E Port [Auto]
Allows you to enable or disable the port and expose/hide its CFG space. In auto mode, the BIOS will remove the EXP port if there is no device or errors on that device and that device is not HP capable.
Configuration options: [Auto] [Disable] [Enable]

The following items appear only when **PCI-E Port** is set to **[Auto]** or **[Enable]**.

PCI-E Port Link Disable [No]
This option disabled the link so that the no training occurs but the CFG space is still active.
Configuration options: [No] [Yes]

Link Speed [Auto]
Choose the Link Speed for this PCIe port.
Configuration options: [Auto] [Gen 1 (2.5 GT/s)] [Gen 2 (5 GT/s)] [Gen 3 (8 GT/s)]

Override Max Link Width [Auto]
Override the max link width that was set by bifurcation.
Configuration options: [Auto] [x1] [x2] [x4] [x8] [x16]

The following item appears only when **Link Speed** is set to **[Auto]**, **[Gen 2 (5 GT/s)]**, or **[Gen 3 (8 GT/s)]**.

PCI-E Port DeEmphasis [-3.5 dB]
De-Emphasis control (LNKCON2 [6]) for this PCIe port.
Configuration options: [-6.0 dB] [-3.5 dB]

PCI-E Port Clocking [Common]
Configure port clocking via LNKCON [6]. This refers to this component and the down stream component.
Configuration options: [Distinct] [Common]

PCI-E Port Clock Gating [Enable]
Allows you to enable or disable Clock Gating for this PCIe port.
Configuration options: [Disable] [Enable]

Data Link Feature Exchange [Enable]
Allows you to enable or disable data link feature negotiation in the Data Link Feature Capabilities (DLFCAP) register.
Configuration options: [Disable] [Enable]

PCI-E Port MPSS [Auto]
Configure Max Payload Size Supported in PCIe Device Capabilities register.
Configuration options: [128B] [256B] [512B] [Auto]

PCI-E Port D-state [D0]
Set to D0 for normal operation, D3Hot to bi in low-power state.
Configuration options: [D0] [D3Hot]

PCI-E ASPM Support [Disable]
Allows you to enable or disable ASPM (L1) support for the downstream devices.
Configuration options: [Auto] [L1 Only] [Disable]

The following item appears only when **PCI-E ASPM Support** is set to **[Auto]** or **[L1 Only]**.

PCI-E Port L1 Exit Latency [8uS - 16uS]
The length of time this port requires to complete transition from L1 to L0.
Configuration options: [<1uS] [1uS - 2uS] [2uS - 4uS] [4uS - 8uS] [8uS - 16uS] [16uS - 32uS] [32uS - 64uS] [>64uS]

MSI [Disable]
Configuration options: [Disable] [Enable]

PCI-E Extended Sync [No]
Allows you to enable or disable the Extended Sync Mode (D:x F:0 0:7Ch B:7) where x is 0-9.
Configuration options: [No] [Yes]

PCI-E Detect Wait Time [Auto]
Set PCIe port TxRx detect polling.
Configuration options: [Disable] [500ms] [Auto]

Compliance Mode [No]
Allows you to enable or disable Compliance Mode for this PCIe port.
Configuration options: [No] [Yes]

EOI [Disable]
Configuration options: [Disable] [Enable]

Fatal Err Over [No]
Allows you to enable or disable forcing fatal error propagation to the IIO core error logic for this port.
Configuration options: [No] [Yes]

Non-Fatal Err Over [No]
Allows you to enable or disable forcing non-fatal error propagation to the IIO core error logic for this port.
Configuration options: [No] [Yes]

Corr Err Over [No]
Allows you to enable or disable forcing correctable error propagation to the IIO core error logic for this port.
Configuration options: [No] [Yes]

ACPI PME Interrupt [No]
Allows you to enable or disable ACPI PME Interrupts generation from this port.
Configuration options: [No] [Yes]

P2P Memory Read [Enable]
Controls Peer2Peer Memory Read Decoding.
Configuration options: [Disable] [Enable]

PME to ACK [Enable]
Controls timeout usage for IIO waiting on PME_TO_ACK after a PME_ TURN_OFF message.
Configuration options: [Disable] [Enable]

Unsupported Request [Disable]
Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port.
Configuration options: [Disable] [Enable]

Alternate TxEq [Disable]
Allows you to enable or disable TxEq.
Configuration options: [Disable] [Enable]

SRIS [Disable]
Allows you to enable or disable SRIS.
Configuration options: [Disable] [Enable]

ECRC Generation [Disable]
Allows you to enable or disable ECRC Generation (Error Capabilities and Control Register).
Configuration options: [Disable] [Enable]

ECRC Check [Disable]
Allows you to enable or disable ECRC Check (Error Capabilities and Control Register).
Configuration options: [Disable] [Enable]

SERRE [Disable]
Allows you to enable or disable SERRE (SERR Reporting Enable).
Configuration options: [Disable] [Enable]

IODC Configuration [KTI Option]
Allows you to enable or disable IODC (IO Direct Cache): Generate snoops instead of memory lookups, for remote InvItoM (IIO) and/or WCiLF (cores).
Configuration options: [KTI Option] [Auto] [Enable for Remote InvItoM Hybrid Push] [InvItoM AllocFlow] [Enable for Remote InvItoM Hybrid AllocNonAlloc] [Enable for Remote InvItoM and Remove WViLF]

Hide Port? [No]
User can force to hide this root port from OS.
Configuration options: [No] [Yes]

MCTP [Yes]
Allows you to enable or disable MCTP.
Configuration options: [No] [Yes]

Intel® VT for Directed I/O (VT-d)

Intel(R) VT for Directed I/O (VT-d) [Enable]

Allows you to enable or disable the Intel Virtualization Technology for Directed I/O (VT-d) by reporting the I/O device assignment to VMM through DMAR ACPI Tables.
Configuration options: [Disable] [Enable]

Intel® VMD technology

Intel® VMD for Volume Management Device on Socket 0

VMD Config for PCH ports

Enable/Disable VMD [Disable]

Allows you to enable or disable VMD in this Stack.
Configuration options: [Disable] [Enable]

The following items appear only when **Enable/Disable VMD** is set to **[Enable]**.

PCH Root Port 0-19 [Disable]

Allows you to configure PCH root port. Setting this item to **[Enable]** will set to VMD ownership root port.
Configuration options: [Disable] [Enable]

Hot Plug Capable [Disable]

Allows you to enable or disable Hot Plug for PCIe Root Ports.
Configuration options: [Disable] [Enable]

CfgBar size [25]

Allows you to setup VMD Config BAR size (in bits Min=20, Max=27), e.g. 20bits=1MB, 27bits=128MB.
Configuration options: [20] - [27]

CfgBar attribute [64-bit prefetchable]

Allows you to setup VMD Config BAR attribute, like 64-bit or prefetchable.
Configuration options: [32-bit non-prefetchable] [64-bit non-prefetchable] [64-bit prefetchable]

MemBar1 size [25]

Allows you to setup VMD Memory BAR1 size (in bits Min=20), e.g. 20bits=1MB, 22bits=4MB, 26bits=64MB.
Configuration options: [20] - [39]

MemBar1 attribute [32-bit non-prefetchable]

Allows you to setup VMD Memory BAR1 attribute, like 64-bit or prefetchable.
Configuration options: [32-bit non-prefetchable] [64-bit non-prefetchable] [64-bit prefetchable]

MemBar2 size [20]

Allows you to setup VMD Memory BAR2 size (in bits Min=20), e.g. 20bits=1MB, 22bits=4MB, 26bits=64MB.
Configuration options: [20] - [39]

MemBar2 attribute [64-bit non-prefetchable]

Allows you to setup VMD Memory BAR2 attribute, like 64-bit or prefetchable.
Configuration options: [32-bit non-prefetchable] [64-bit non-prefetchable] [64-bit prefetchable]

VMD for Direct Assign [Disable]
Allows you to enable or disable VMD for Direct Assign.
Configuration options: [Disable] [Enable]

VMD Config for IOU 0/2/3/4
Enable/Disable VMD [Disable]
Allows you to enable or disable VMD in this Stack.
Configuration options: [Disable] [Enable]

The following items appear only when **Enable/Disable VMD** is set to **[Enable]**.

VMD Port A-D [Disable]
Allows you to enable or disable Intel® Volume Management Device Technology on specific root port.
Configuration options: [Disable] [Enable]

Hot Plug Capable [Disable]
Allows you to enable or disable Hot Plug for PCIe Root Ports.
Configuration options: [Disable] [Enable]

CfgBar size [25]
Allows you to setup VMD Config BAR size (in bits Min=20, Max=27), e.g. 20bits=1MB, 27bits=128MB.
Configuration options: [20] - [27]

CfgBar attribute [64-bit prefetchable]
Allows you to setup VMD Config BAR attribute, like 64-bit or prefetchable.
Configuration options: [32-bit non-prefetchable] [64-bit non-prefetchable] [64-bit prefetchable]

MemBar1 size [25]
Allows you to setup VMD Memory BAR1 size (in bits Min=20), e.g. 20bits=1MB, 22bits=4MB, 26bits=64MB.
Configuration options: [20] - [39]

MemBar1 attribute [32-bit non-prefetchable]
Allows you to setup VMD Memory BAR1 attribute, like 64-bit or prefetchable.
Configuration options: [32-bit non-prefetchable] [64-bit non-prefetchable] [64-bit prefetchable]

MemBar2 size [20]
Allows you to setup VMD Memory BAR2 size (in bits Min=20), e.g. 20bits=1MB, 22bits=4MB, 26bits=64MB.
Configuration options: [20] - [39]

MemBar2 attribute [64-bit non-prefetchable]
Allows you to setup VMD Memory BAR2 attribute, like 64-bit or prefetchable.
Configuration options: [32-bit non-prefetchable] [64-bit non-prefetchable] [64-bit prefetchable]

VMD for Direct Assign [Disable]
Allows you to enable or disable VMD for Direct Assign.
Configuration options: [Disable] [Enable]

VMD Config for IOU 1
Enable/Disable VMD [Enable]
Allows you to enable or disable VMD in this Stack.
Configuration options: [Disable] [Enable]

The following items appear only when **Enable/Disable VMD** is set to **[Enable]**.

VMD Port A [Enable]
Allows you to enable or disable Intel® Volume Management Device Technology on specific root port.
Configuration options: [Disable] [Enable]

VMD Port B [Enable]
Allows you to enable or disable Intel® Volume Management Device Technology on specific root port.
Configuration options: [Disable] [Enable]

VMD Port C [Disable]
Allows you to enable or disable Intel® Volume Management Device Technology on specific root port.
Configuration options: [Disable] [Enable]

VMD Port D [Disable]
Allows you to enable or disable Intel® Volume Management Device Technology on specific root port.
Configuration options: [Disable] [Enable]

Hot Plug Capable [Enable]
Allows you to enable or disable Hot Plug for PCIe Root Ports.
Configuration options: [Disable] [Enable]

CfgBar size [25]
Allows you to setup VMD Config BAR size (in bits Min=20, Max=27), e.g. 20bits=1MB, 27bits=128MB.
Configuration options: [20] - [27]

CfgBar attribute [64-bit prefetchable]
Allows you to setup VMD Config BAR attribute, like 64-bit or prefetchable.
Configuration options: [32-bit non-prefetchable] [64-bit non-prefetchable] [64-bit prefetchable]

MemBar1 size [25]
Allows you to setup VMD Memory BAR1 size (in bits Min=20), e.g. 20bits=1MB, 22bits=4MB, 26bits=64MB.
Configuration options: [20] - [39]

MemBar1 attribute [32-bit non-prefetchable]
Allows you to setup VMD Memory BAR1 attribute, like 64-bit or prefetchable.
Configuration options: [32-bit non-prefetchable] [64-bit non-prefetchable] [64-bit prefetchable]

MemBar2 size [20]
Allows you to setup VMD Memory BAR2 size (in bits Min=20), e.g. 20bits=1MB, 22bits=4MB, 26bits=64MB.
Configuration options: [20] - [39]

MemBar2 attribute [64-bit non-prefetchable]
Allows you to setup VMD Memory BAR2 attribute, like 64-bit or prefetchable.
Configuration options: [32-bit non-prefetchable] [64-bit non-prefetchable] [64-bit prefetchable]

VMD for Direct Assign [Disable]
Allows you to enable or disable VMD for Direct Assign.
Configuration options: [Disable] [Enable]

Intel® VMD for Volume Management Device on Socket 1

VMD Config for IOU 0-3

Enable/Disable VMD [Disable]

Allows you to enable or disable VMD in this Stack.

The following items appear only when **Enable/Disable VMD** is set to **[Enable]**.

VMD Port A-D [Disable]

Allows you to enable or disable Intel® Volume Management Device Technology on specific root port.
Configuration options: [Disable] [Enable]

Hot Plug Capable [Disable]

Allows you to enable or disable Hot Plug for PCIe Root Ports.
Configuration options: [Disable] [Enable]

CfgBar size [25]

Allows you to setup VMD Config BAR size (in bits Min=20, Max=27), e.g. 20bits=1MB, 27bits=128MB.
Configuration options: [20] - [27]

CfgBar attribute [64-bit prefetchable]

Allows you to setup VMD Config BAR attribute, like 64-bit or prefetchable.
Configuration options: [32-bit non-prefetchable] [64-bit non-prefetchable] [64-bit prefetchable]

MemBar1 size [25]

Allows you to setup VMD Memory BAR1 size (in bits Min=20), e.g. 20bits=1MB, 22bits=4MB, 26bits=64MB.
Configuration options: [20] - [39]

MemBar1 attribute [32-bit non-prefetchable]

Allows you to setup VMD Memory BAR1 attribute, like 64-bit or prefetchable.
Configuration options: [32-bit non-prefetchable] [64-bit non-prefetchable] [64-bit prefetchable]

MemBar2 size [20]

Allows you to setup VMD Memory BAR2 size (in bits Min=20), e.g. 20bits=1MB, 22bits=4MB, 26bits=64MB.
Configuration options: [20] - [39]

MemBar2 attribute [64-bit non-prefetchable]

Allows you to setup VMD Memory BAR2 attribute, like 64-bit or prefetchable.
Configuration options: [32-bit non-prefetchable] [64-bit non-prefetchable] [64-bit prefetchable]

VMD for Direct Assign [Disable]

Allows you to enable or disable VMD for Direct Assign.
Configuration options: [Disable] [Enable]

VMD Config for IOU 4

Enable/Disable VMD [Enable]

Allows you to enable or disable VMD in this Stack.

The following items appear only when **Enable/Disable VMD** is set to **[Enable]**.

VMD Port A [Enable]
Allows you to enable or disable Intel® Volume Management Device Technology on specific root port.
Configuration options: [Disable] [Enable]

VMD Port B [Enable]
Allows you to enable or disable Intel® Volume Management Device Technology on specific root port.
Configuration options: [Disable] [Enable]

VMD Port C [Disable]
Allows you to enable or disable Intel® Volume Management Device Technology on specific root port.
Configuration options: [Disable] [Enable]

VMD Port D [Disable]
Allows you to enable or disable Intel® Volume Management Device Technology on specific root port.
Configuration options: [Disable] [Enable]

Hot Plug Capable [Enable]
Allows you to enable or disable Hot Plug for PCIe Root Ports.
Configuration options: [Disable] [Enable]

CfgBar size [25]
Allows you to setup VMD Config BAR size (in bits Min=20, Max=27), e.g. 20bits=1MB, 27bits=128MB.
Configuration options: [20] - [27]

CfgBar attribute [64-bit prefetchable]
Allows you to setup VMD Config BAR attribute, like 64-bit or prefetchable.
Configuration options: [32-bit non-prefetchable] [64-bit non-prefetchable] [64-bit prefetchable]

MemBar1 size [25]
Allows you to setup VMD Memory BAR1 size (in bits Min=20), e.g. 20bits=1MB, 22bits=4MB, 26bits=64MB.
Configuration options: [20] - [39]

MemBar1 attribute [32-bit non-prefetchable]
Allows you to setup VMD Memory BAR1 attribute, like 64-bit or prefetchable.
Configuration options: [32-bit non-prefetchable] [64-bit non-prefetchable] [64-bit prefetchable]

MemBar2 size [20]
Allows you to setup VMD Memory BAR2 size (in bits Min=20), e.g. 20bits=1MB, 22bits=4MB, 26bits=64MB.
Configuration options: [20] - [39]

MemBar2 attribute [64-bit non-prefetchable]
Allows you to setup VMD Memory BAR2 attribute, like 64-bit or prefetchable.
Configuration options: [32-bit non-prefetchable] [64-bit non-prefetchable] [64-bit prefetchable]

VMD for Direct Assign [Disable]
Allows you to enable or disable VMD for Direct Assign.
Configuration options: [Disable] [Enable]

Intel® AIC Retimer/AIC SSD Technology (non-VMD)

Intel® AIC Retimer/AIC SSD on Socket 0/1

Intel® AIC Retimer/AIC SSD HW at Stack1 [Disable]
Announce Intel® AIC Retimer/AIC SSD HW at Stack1 (Port1A-1D).
Override IOU0 bifurcation if required.
Configuration options: [Enable] [Disable]

The following items appear only when **Intel® AIC Retimer/AIC SSD HW at Stack1** is set to **[Enable]**.

Port 1A - 1D [Disable]
Allows you to enable or disable NVMe Legacy mode on specific root port.
Configuration options: [Disable] [Enable]

Hot Plug Capable [Disable]
Allows you to enable or disable Hot Plug for PCIe Root Ports.
Configuration options: [Disable] [Enable]

Intel® AIC Retimer/AIC SSD HW at Stack2 [Disable]
Announce Intel® AIC Retimer/AIC SSD HW at Stack2 (Port2A-2D).
Override IOU0 bifurcation if required.
Configuration options: [Enable] [Disable]

The following items appear only when **Intel® AIC Retimer/AIC SSD HW at Stack2** is set to **[Enable]**.

Port 2A - 2D [Disable]
Allows you to enable or disable NVMe Legacy mode on specific root port.
Configuration options: [Disable] [Enable]

Hot Plug Capable [Disable]
Allows you to enable or disable Hot Plug for PCIe Root Ports.
Configuration options: [Disable] [Enable]

Intel® AIC Retimer/AIC SSD HW at Stack1 [Disable]
Announce Intel® AIC Retimer/AIC SSD HW at Stack3 (Port3A-3D).
Override IOU0 bifurcation if required.
Configuration options: [Enable] [Disable]

The following items appear only when **Intel® AIC Retimer/AIC SSD HW at Stack3** is set to **[Enable]**.

Port 3A - 3D [Disable]
Allows you to enable or disable NVMe Legacy mode on specific root port.
Configuration options: [Disable] [Enable]

Hot Plug Capable [Disable]
Allows you to enable or disable Hot Plug for PCIe Root Ports.
Configuration options: [Disable] [Enable]

Intel® AIC Retimer/AIC SSD HW at Stack4 [Disable]
Announce Intel® AIC Retimer/AIC SSD HW at Stack4 (Port4A-4D).
Override IOU0 bifurcation if required.
Configuration options: [Enable] [Disable]

The following items appear only when **Intel® AIC Retimer/AIC SSD HW at Stack4** is set to **[Enable]**.

Port 4A - 4D [Disable]
Allows you to enable or disable NVMe Legacy mode on specific root port.
Configuration options: [Disable] [Enable]

Hot Plug Capable [Disable]
Allows you to enable or disable Hot Plug for PCIe Root Ports.
Configuration options: [Disable] [Enable]

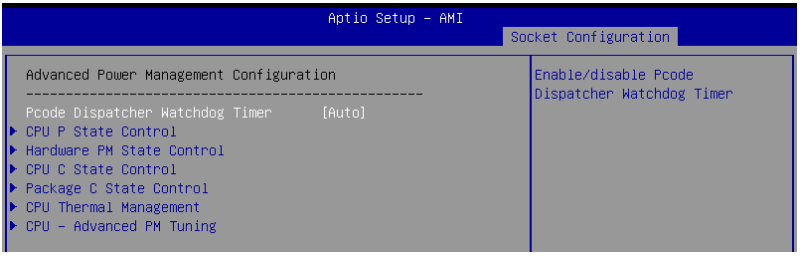
Intel® AIC Retimer/AIC SSD HW at Stack5 [Disable]
Announce Intel® AIC Retimer/AIC SSD HW at Stack5 (Port5A-5D).
Override IOU0 bifurcation if required.
Configuration options: [Enable] [Disable]

The following items appear only when **Intel® AIC Retimer/AIC SSD HW at Stack5** is set to **[Enable]**.

Port 5A - 5D [Disable]
Allows you to enable or disable NVMe Legacy mode on specific root port.
Configuration options: [Disable] [Enable]

Hot Plug Capable [Disable]
Allows you to enable or disable Hot Plug for PCIe Root Ports.
Configuration options: [Disable] [Enable]

5.7.5 Advanced Power Management Configuration



Pcode Dispatcher Watchdog Timer [Auto]

Allows you to enable or disable Pcode Dispatcher Watchdog Timer.
Configuration options: [Disable] [Enable] [Auto]

CPU P State Control

P State Control Configuration Sub Menus, including Turbo, XE, etc.

Uncore Freq Scaling [Enable]

If disable, user can input Uncore Frequency.
Configuration options: [Disable] [Enable]

The following item appears only when **Uncore Freq Scaling** is set to **[Disable]**.

Uncore Freq [127]

Configuration options: [0] - [127]

AVX Licence Pre-Grant Override [Disable]

Enabled AVX ICCP pre-grant level override.
Configuration options: [Disable] [Enable]

The following item appears only when **AVX Licence Pre-Grant Override** is set to **[Enable]**.

AVX ICCP pre-grant level [128 Heavy]

Pre-grants an AVX level to the core. Base frequency is not updated.
Configuration options: [128 Heavy] [256 Light] [256 Heavy] [512 Light] [512 Heavy]

SpeedStep (Pstates) [Enable]

Allows you to enable or disable EIST (P-States).
Configuration options: [Disable] [Enable]

The following items appear only when **SpeedStep (Pstates)** is set to **[Enable]**.

Configure TDP Lock [Enable]

Allows you to configure TDP CONTROL Lock Bit.
Configuration options: [Disable] [Enable]

AVX P1 [Normal]

AVX P1 level selection.
Configuration options: [Normal] [Level 1] [Level 2]

Activate SST-BF [Disable]

Allows you to enable or disable SST-BF.
Configuration options: [Disable] [Enable]

The following item appears only when **Activate SST-BF** is set to **[Enable]**.

Configure SST-BF [Enable]

Allows BIOS to configure SST-BF High Priority Cores so that SW does not have to configure.
Configuration options: [Disable] [Enable]

EIST PSD Function [HW_ALL]

Configuration options: [HW_ALL] [SW_ALL]

Boot performance mode [Max Performance]

Allows you to select the performance state that the BIOS will set before OS hand off.
Configuration options: [Max Performance] [Max Efficient] [Set by Intel Node Manager]

Energy Efficient Turbo [Enable]

Allows you to enable or disable Energy Efficient Turbo.
Configuration options: [Disable] [Enable]

Turbo Mode [Enabled]

Allows you to enable or disable processor Turbo Mode (requires EMTTM enabled as well).
Configuration options: [Disable] [Enable]

CPU Flex Ratio Override [Disable]

Allows you to enable or disable CPU Flex Ratio Programming.
Configuration options: [Disable] [Enable]

The following item appears only when **CPU Flex Ratio Override** is set to **[Enable]**.

CPU Flex Ratio [23]

Non-Turbo Mode Processor Core Ratio Multiplier.
Configuration options: [0] - [100]

GPSS timer [500 us]

P-state changes hysteresis time window.
Configuration options: [0 us] [50 us] [500 us]

Perf P-Limit

Perf P-Limit Differential [1]
Parameter used to tune how far below local socket frequency remote socket frequency is allowed to be. Also impacts rate at which frequency drops when feature disengages.

Perf P-Limit Clip [1F]
Maximum value the floor is allowed to be set to for perf P-Limit.

Perf P-Limit Threshold [F]
Uncore frequency threshold above which this socket will trigger the feature and start trying to raise frequency of other sockets.

Perf P-Limit [Enable]
Allows you to enable or disable Performance P-Limit.
Configuration options: [Disable] [Enable]

Hardware PM State Control

Hardware P-States [Native Mode]

Allows you to switch between Hardware P-States mode.
[Disable] Hardware chooses a P-state based on OS Request (Legacy P-States).
[Native Mode] Hardware chooses a P-state based on OS guidance.
[Out of Band Mode] Hardware autonomously chooses a P-state (no OS guidance).
[Native Mode with no Legacy Support] Hardware chooses a P-state based on OS guidance (without Legacy support).

The following item is available only when **Hardware P-States** is set to **[Native]**.

HardwarePM Interrupt [Disable]

Allows you to enable or disable Hardware PM Interrupt.
Configuration options: [Disable] [Enable]

The following items are available only when **Hardware P-States** is either set to **[Native]**, **[Out of Band Mode]**, or **[Native Mode with no Legacy Support]**.

EPP Enable [Enable]

When disabled, HW masks EPP in CPUID[6].10 and uses EPB for EPP.
Configuration options: [Disable] [Enable]

The following item only appears when **Hardware P-States** is set to **[Out of Band Mode]** and **EPP Enable** is set to **[Enable]**.

EPP profile [Balanced Performance]

Allows you to choose an HWPM Profile (EPP).
Configuration options: [Performance] [Balanced Performance] [Balanced Power] [Power]

APS rocketing [Disable]

Allows you to enable or disable the rocketing mechanism in the HWP p-state selection pcode algorithm. Rocketing enables the core ratio to jump to max turbo instantaneously as opposed to a smooth ramp up.
Configuration options: [Disable] [Enable]

Scalability [Disable]

Allows you to enable or disable Core Performance to Frequency Scalability Based Optimizations in the CPU.
Configuration options: [Disable] [Enable]

Native ASPM [Disabled]

[Auto]	BIOS Controlled ASPM
[Enabled]	OS Controlled ASPM
[Disabled]	ASPM Off

CPU C State Control

Enable Monitor MWAIT [Enable]

Allows you to enable or disable Monitor and MWAIT instructions.
Configuration options: [Disable] [Enable]

CPU C1 auto demotion [Enable]

Allows CPU to automatically demote to C1. Takes effect after reboot.
Configuration options: [Disable] [Enable]

CPU C1 auto undemotion [Enable]

Allows CPU to automatically undemote from C1. Takes effect after reboot.
Configuration options: [Disable] [Enable]

CPU C6 Report [Auto]

Allows you to enable or disable CPU C6 (ACPI C3) report to OS.
Configuration options: [Disable] [Enable] [Auto]

Enhanced Halt State (C1E) [Enable]

Core C1E auto promotion Control. Takes effect after reboot.
Configuration options: [Disable] [Enable]

OS ACPI Cx [ACPI C2]

Allows you to select to report CC3/CC6 to OS ACPI C2 or ACPI C3.
Configuration options: [ACPI C2] [ACPI C3]

Package C State Control

Package C State [Auto]

Allows you to select Package C State limit.
Configuration options: [C0/C1 state] [C2 state] [C6(non Retention state] [Auto]

Register Access Low Latency Mode [Disabled]

Enable low latency mode for register accesses.
Configuration options: [Disabled] [Enabled]

Enabling this mode will prevent PkgC6 as register access fabric is prevented from going to idle.

CPU Thermal Management

CPU T State Control

Software Controlled T-States [Disabled]
Allows you to enable or disable Software Controlled T-States.
Configuration options: [Disabled] [Enabled]

The following item appears only when **Software Controlled T-States** is set to **[Enabled]**.

T-State Throttle Level [Disable]
On-Die Thermal Throttling.
Configuration options: [Disabled] [6.25%] [12.5%][18.75%][25.0%][31.25%] [37.5%][43.75%][50.0%][56.25%][62.5%][68.75%][75.0%] [81.25%][87.5%] [93.75%]

CPU - Advanced PM Tuning

Uncore Freq Scaling [Enable]

If this item is disabled, user can input Uncore Frequency.
Configuration options: [Disable] [Enable]

The following item appears only when **Uncore Freq Scaling** is set to **[Disable]**.

Uncore Freq: [127]

Configuration options: [0] - [127]

Uncore Freq RAPL [Enable]

Configuration options: [Disable] [Enable]

Energy Perf BIAS

Power Performance Tuning [OS Controls EPB]
Configuration options: [OS Controls EPB] [BIOS Controls EPB] [PECI Controls EPB]

The following item appears only when **Power Performance Tuning** is set to **[OS Controls EPB]** or **[PECI Controls EPB]**.

PECI CPS EPB [OS controls EPB]
Controls whether PECI has control over EPB.
Configuration options: [OS Controls EPB] [PECI Controls EPB using PCS]

The following item appears only when **Power Performance Tuning** is set to **[BIOS Controls EPB]**.

ENERGY_PERF_BIAS_CFG mode [Balanced Performance]
Configuration options: [Performance] [Balanced Performance] [Balanced Power] [Power]

Dynamic Loadline Switch [Enable]
Configuration options: [Disable] [Enable]

Workload Configuration [Balanced]
This allows optimization for the workload characterization.
Configuration options: [Balanced] [I/O Sensitive]

Averaging Time Window [1A]
This is used to control the effective window of the average for C0 and P0 time.

P0 TotalTimeThreshold Low [28]
This is used to control the effective window of the average for C0 and P0 time.

P0 TotalTimeThreshold High [3F]
This is used to control the effective window of the average for C0 and P0 time.

SAPM Control [Enable]

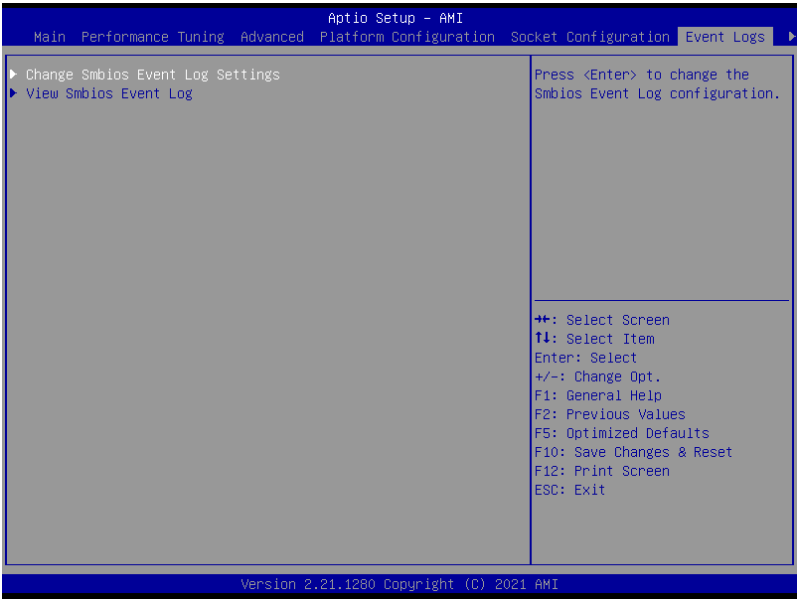
Configuration options: [Enable] [Disable]

EET Mode [Coarse Grained Mode]

[Coarse Grained Mode] Decides whether to grant user request turbo on P1.
[Fine Grained Mode] Decides how much turbo to be granted.

5.8 Event Logs menu

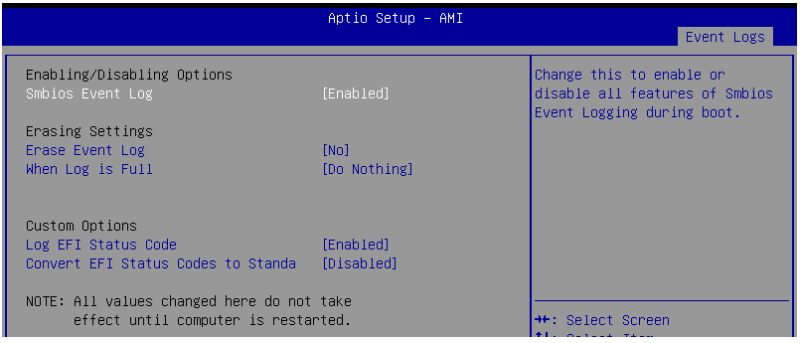
The Event Logs menu items allow you to change the event log settings and view the system event logs.



5.8.1 Change Smbios Event Log Settings

Press <Enter> to change the Smbios Event Log configuration.

All values changed here do not take effect until computer is restarted.



Enabling/Disabling Options

Smbios Event Log [Enabled]

Change this to enable or disable all features of Smbios Event Logging during boot.
Configuration options: [Disabled] [Enabled]

The following items only appear when **Smbios Event Log** is set to **[Enabled]**.

Erasing Settings

Erase Event Log [No]

Choose options for erasing Smbios Event Log. Erasing is done prior to any logging activation during reset.
Configuration options: [No] [Yes, Next reset] [Yes, Every reset]

When Log is Full [Do Nothing]

Choose options for reactions to a full Smbios Event Log.
Configuration options: [Do Nothing] [Erase Immediately]

Custom Options

Log EFI Status Code [Enabled]

Allows you to enable or disable the logging of EFI Status Codes as OEM reserved type E0 (if not already converted to legacy).
Configuration options: [Disabled] [Enabled]

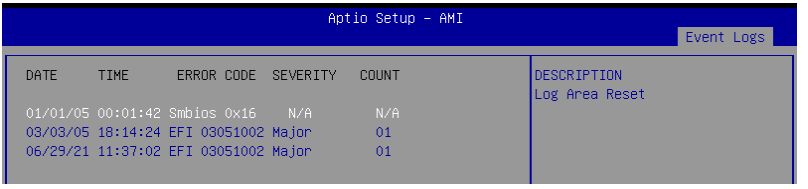
The following item only appears when **Log EFI Status Code** is set to **[Enabled]**.

Convert EFI Status Codes to Standard Smbios Type [Disabled]

Allows you to enable or disable the converting of EFI Status Codes to Standard Smbios Types (not all may be translated).
Configuration options: [Disabled] [Enabled]

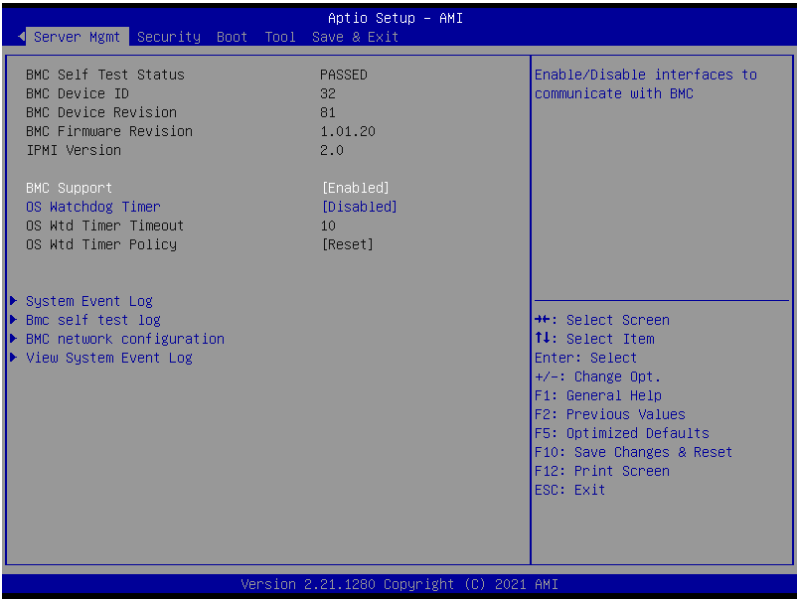
5.8.2 View Smbios Event Log

Press <Enter> to view all smbios event logs.



5.9 Server Mgmt menu

The Server Management menu displays the server management status and allows you to change the settings.



BMC Support [Enabled]

Allows you to enable or disable interfaces to communicate with BMC.
Configuration options: [Disabled] [Enabled]

The following items are available only when **BMC Support** is set to **[Enabled]**.

OS Watchdog Timer [Disabled]

This item allows you to start a BIOS timer which can only be shut off by Management Software after the OS loads. Helps determine if the OS successfully loaded or follows the OS Boot Watchdog Timer policy.
Configuration options: [Disabled] [Enabled]

The following items are available only when **OS Watchdog Timer** is set to **[Enabled]**.

OS Wtd Timer Timeout [10]

Allows you to enter a value between 1 to 30 minutes for OS Boot Watchdog Timer Expiration. Not available if OS Boot Watchdog Timer is disabled.
Configuration options: [1] - [30]

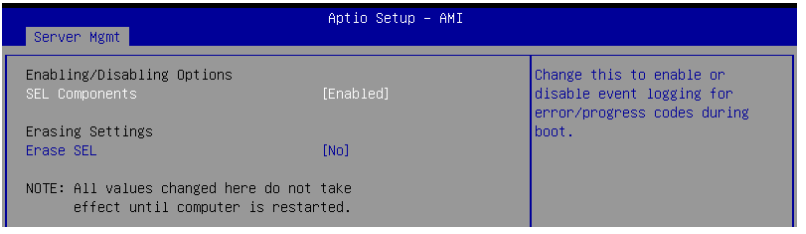
OS Wtd Timer Policy [Reset]

This item allows you to configure the how the system should respond if the OS Boot Watch Timer expires. Not available if OS Boot Watchdog Timer is disabled.
Configuration options: [Do Nothing] [Reset] [Power Down] [Power Cycle]

5.9.1 System Event Log

Allows you to change the SEL event log configuration.

All values changed here do not take effect until computer is restarted.



SEL Components [Enabled]

Allows you to enable or disable event logging for error/progress codes during boot.
Configuration options: [Disabled] [Enabled]

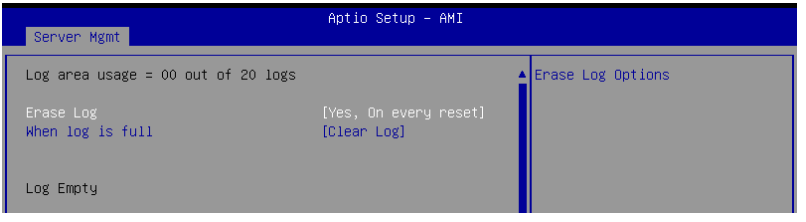
The following item is available only when **SEL Components** is set to **[Enabled]**.

Erase SEL [No]

Allows you to choose options for erasing SEL.
Configuration options: [No] [Yes, On next reset] [Yes, On every reset]

5.9.2 BMC self test log

Logs the report returned by BMC self test command.



Erase Log [Yes, On every reset]

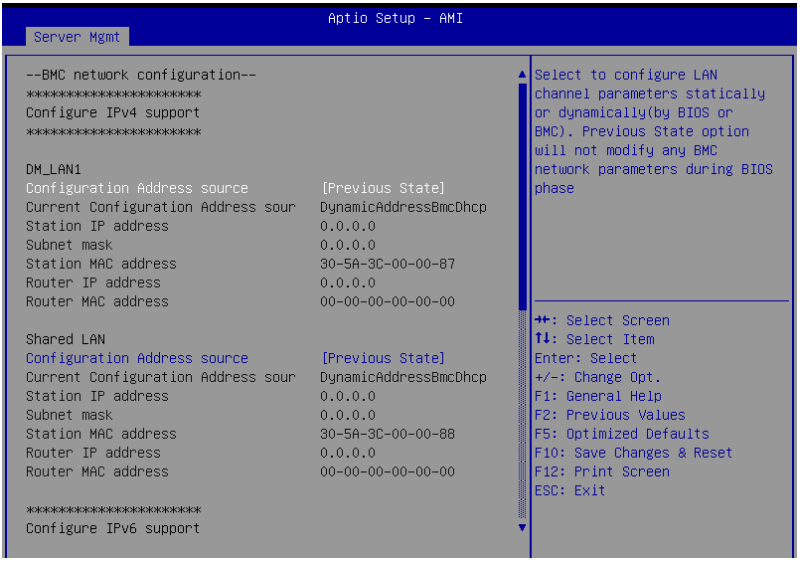
Allows you to choose options for erasing log.
Configuration options: [Yes, On every reset] [No]

When log is full [Clear Log]

Select the action to be taken when log is full.
Configuration options: [Clear Log] [Do not log any more]

5.9.3 BMC network configuration

The sub-items in this configuration allow you to configure the BMC network parameters. Scroll using <Page Up> / <Page Down> keys to see more items.



Configure IPV4 support

DM_LAN1 / Shared LAN

Configuration Address source [Previous State]

Allows you to set the LAN channel parameters statically or dynamically (by BIOS or by BMC). **[Previous State]** option will not modify any BMC network parameters during BIOS phase.
Configuration options: [Previous State] [Static] [DynamicBmcDhcp]

The following items are available only when **Configuration Address source** is set to **[Static]**.

Station IP address

Allows you to set the station IP address.

Subnet mask

Allows you to set the subnet mask. We recommend that you use the same Subnet Mask you have specified on the operating system network for the used network card.

Router IP Address

Allows you to set the router IP address.

Router MAC Address

Allows you to set the router MAC address.

Configure IPV6 support

DM_LAN1 / Shared LAN

IPV6 support [Enabled]

Allows you to enable or disable IPV6 support.
Configuration options: [Enabled] [Disabled]

The following items appear only when **IPV6 support** is set to **[Enabled]**.

Configuration Address source [Previous State]

Allows you to set the LAN channel parameters statically or dynamically (by BIOS or by BMC). **[Previous State]** option will not modify any BMC network parameters during BIOS phase.
Configuration options: [Previous State] [Static] [DynamicBmcDhcp]

The following items are available only when **Configuration Address source** is set to **[Static]**.

Station IPV6 address

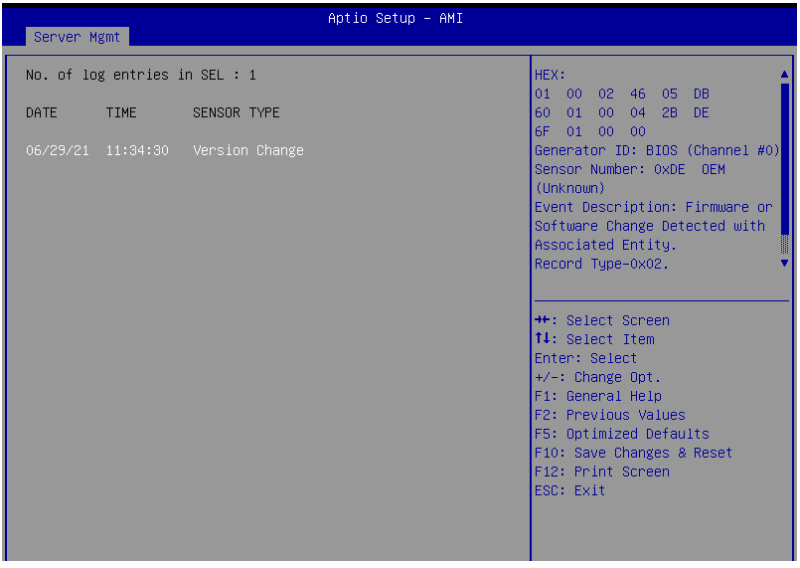
Allows you to set the station IPV6 address.

Prefix Length

Allows you to set the prefix length (maximum of Prefix Length is 128).

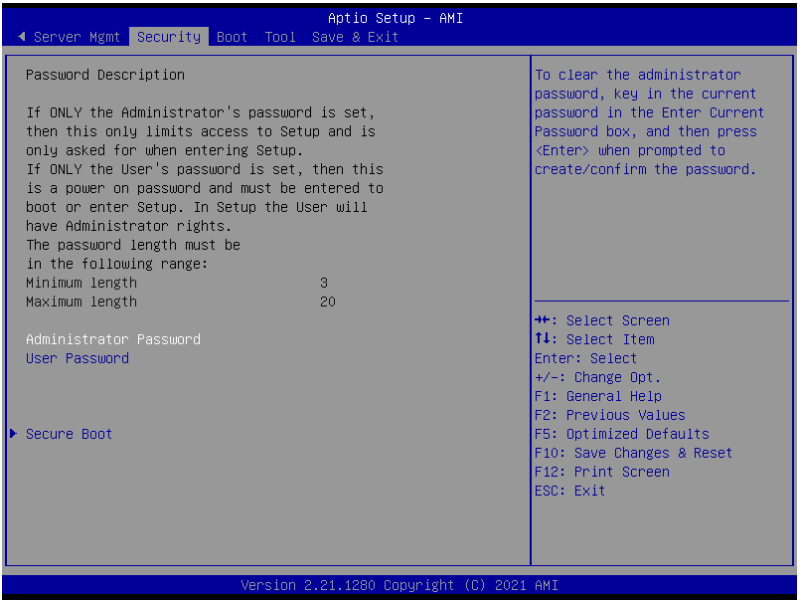
5.9.4 View System Event Log

This item allows you to view the system event log records. Scroll using <Page Up> / <Page Down> keys to see more items.



5.10 Security menu

This menu allows a new password to be created or a current password to be changed. The menu also enables or disables the Secure Boot state and lets the user configure the System Mode state.



Administrator Password

To set an administrator password:

1. Select the Administrator Password item and press <Enter>.
2. From the Create New Password box, key in a password, then press <Enter>.
3. Confirm the password when prompted.

To change an administrator password:

1. Select the Administrator Password item and press <Enter>.
2. From the Enter Current Password box, key in the current password, then press <Enter>.
3. From the Create New Password box, key in a new password, then press <Enter>.
4. Confirm the password when prompted.

To clear the administrator password, follow the same steps as in changing an administrator password, but press <Enter> when prompted to create/confirm the password.

User Password

To set a user password:

1. Select the User Password item and press <Enter>.
2. From the Create New Password box, key in a password, then press <Enter>.
3. Confirm the password when prompted.

To change a user password:

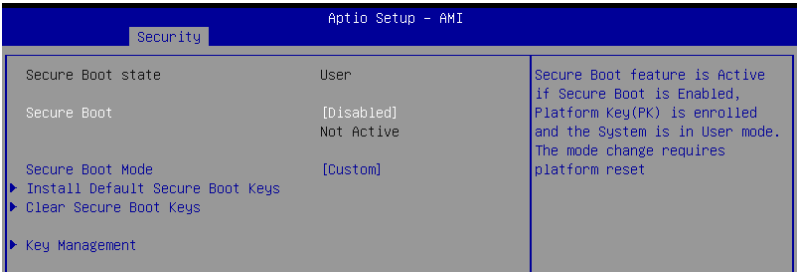
1. Select the User Password item and press <Enter>.
2. From the Enter Current Password box, key in the current password, then press <Enter>.
3. From the Create New Password box, key in a new password, then press <Enter>.
4. Confirm the password when prompted.

To clear a user password:

1. Select the Clear User Password item and press <Enter>.
2. Select **Yes** from the Warning message window then press <Enter>.

5.10.1 Secure Boot

This item allows you to customize the Secure Boot settings.



Secure Boot [Disabled]

Secure Boot feature is active if Secure Boot is Enabled, Platform Key (PK) is enrolled and the system is in User mode. The mode change requires platform reset.
Configuration options: [Disabled] [Enabled]

Secure Boot Mode [Custom]

Allows you to set the Secure Boot selector. In Custom mode, Secure Boot Policy variables can be configured physically by the present user without full authentication.
Configuration options: [Custom] [Standard]

The following items are available only when **Secure Boot Mode** is set to **[Custom]**.

Install Default Secure Boot Keys

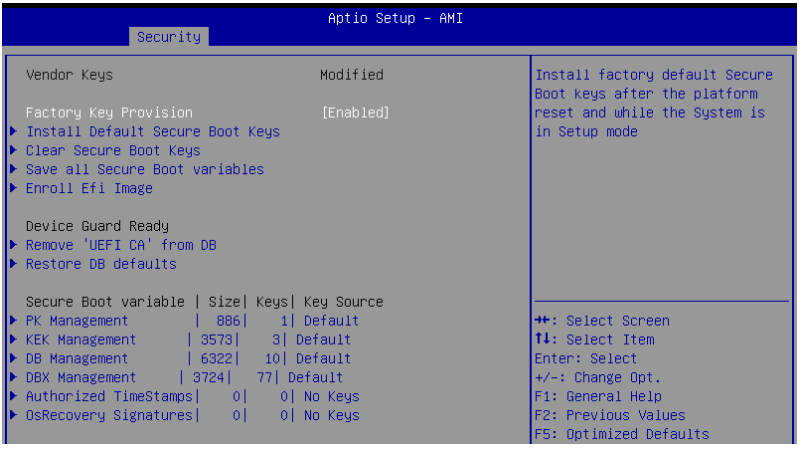
This option will load the default secure boot keys, including the PK (Platform key), KEK (key-exchange key), db (signature database), and dbx (revoked signature database). All the secure boot keys states will change from unloaded to loaded. Save changes and reset the system for the changes to take effect.

Clear Secure Boot Keys

This option will delete all previously applied secure boot keys, including the PK (Platform key), KEK (key-exchange key), db (signature database), and dbx (revoked signature database). All the secure boot keys states will change from unloaded to loaded. Save changes and reset the system for the changes to take effect.

Key Management

This item only appears when the item **Secure Boot Mode** is set to **[Custom]**. The Key Management item allows you to modify Secure Boot variables and set Key Management page.



Factory Key Provision [Enabled]

Allows you to provision factory default Secure Boot keys when the system is in Setup Mode.
Configuration options: [Disabled] [Enabled]

Install Default Secure Boot Keys

This option will load the default secure boot keys, including the PK (Platform key), KEK (key-exchange key), db (signature database), and dbx (revoked signature database). All the secure boot keys states will change from unloaded to loaded. Save changes and reset the system for the changes to take effect.

Clear Secure Boot Keys

This option will delete all previously applied secure boot keys, including the PK (Platform key), KEK (key-exchange key), db (signature database), and dbx (revoked signature database). All the secure boot keys states will change from unloaded to loaded. Save changes and reset the system for the changes to take effect.

Save all Secure Boot Variables

This option will save NVRAM content of Secure Boot policy variables to the file (EFI_ SIGNATURE_LIST data format) in root foler on a target file system device.

Enroll Efi Image

This item will allow the image to run in Secure Boot mode. Enroll SHA256 Hash certificate of a PE image into Authorized Signature Database (db).

Device Guard Ready

Remove 'UEFI CA' from DB

Remove Microsoft UEFI CA from Secure Boot DB.

Restore DB defaults

Restore DB variable to factory defaults.

PK Management

Configuration options: [Details] [Save To File] [Set New Key] [Delete key]

KEK Management / DB Management / DBX Management

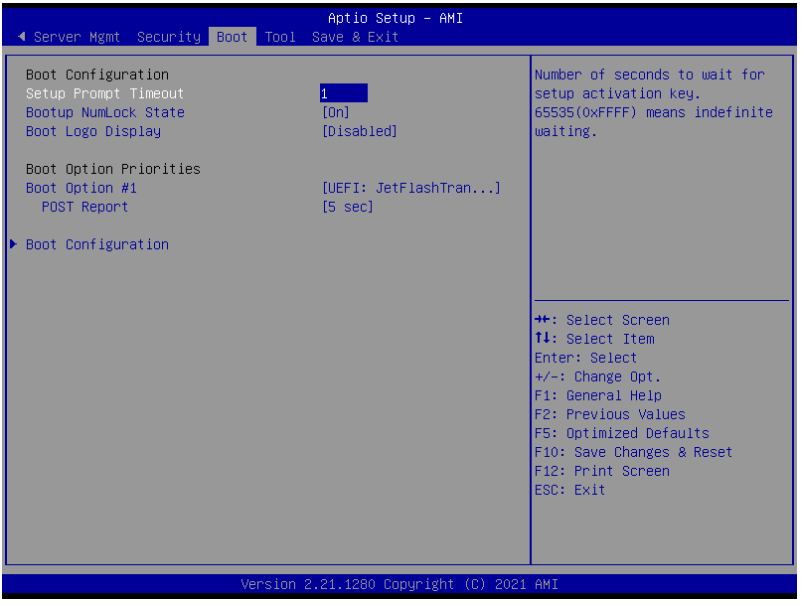
Configuration options: [Details] [Save To File] [Set New Key] [Append Key] [Delete key]

Authorized TimeStamps / OsRecovery Signatures

Configuration options: [Set New Key] [Append Key]

5.11 Boot menu

The Boot menu items allow you to change the system boot options.



Setup Prompt Timeout [1]

Allows you to set the number of seconds that the firmware waits before initiating the original default boot selection. 65535(OxFFFF) means indefinite waiting. Use the <+> or <-> to adjust the value.

Bootup NumLock State [On]

Allows you to select the power-on state for the NumLock.
Configuration options: [Off] [On]

Boot Logo Display [Disabled]

[Disabled] Hide the logo during POST.

[Enabled] Display the logo during POST.

Boot Option Priorities

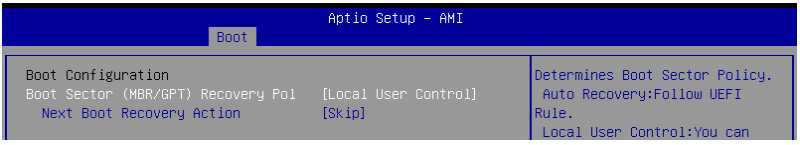
These items specify the boot device priority sequence from the available devices. The number of device items that appears on the screen depends on the number of devices installed in the system.

- To select the boot device during system startup, press <F11> when logo appears.
- To access Windows OS in Safe Mode, please press <F8> after POST.

POST Report [5 sec]

Allows you to set the desired POST Report waiting time from 1 to 10 seconds.
Configuration options: [1 sec] ~ [10 sec] [Until Press ESC]

5.11.1 Boot Configuration



Boot Sector (MBR/GPT) Recovery Policy [Local User Control]

Determines the Boot Sector Recovery Policy.

[Auto Recovery] Follow UEFI Rule.

[Local User Control] You can enter setup page and select Boot Sector (MBR/GPT) Recovery Policy to recover MBR/GPT on the next boot.

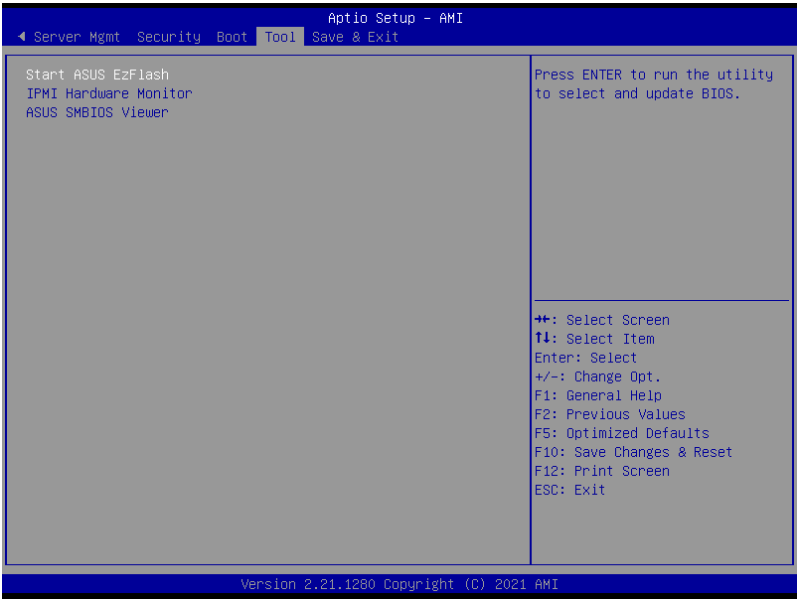
The following item appears only when **Boot Sector (MBR/GPT) Recovery Policy** is set to **[Local User Control]**.

Next Boot Recovery Action [Skip]

Allows you to select the (MBR/GPT) recovery action on the next boot.
Configuration options: [Skip] [Recovery]

5.12 Tool menu

The Tool menu items allow you to configure options for special functions. Select an item then press <Enter> to display the submenu.



Start ASUS EzFlash

Allows you to run ASUS EzFlash BIOS ROM Utility when you press <Enter>. Refer to the ASUS EzFlash Utility section for details.

IPMI Hardware Monitor

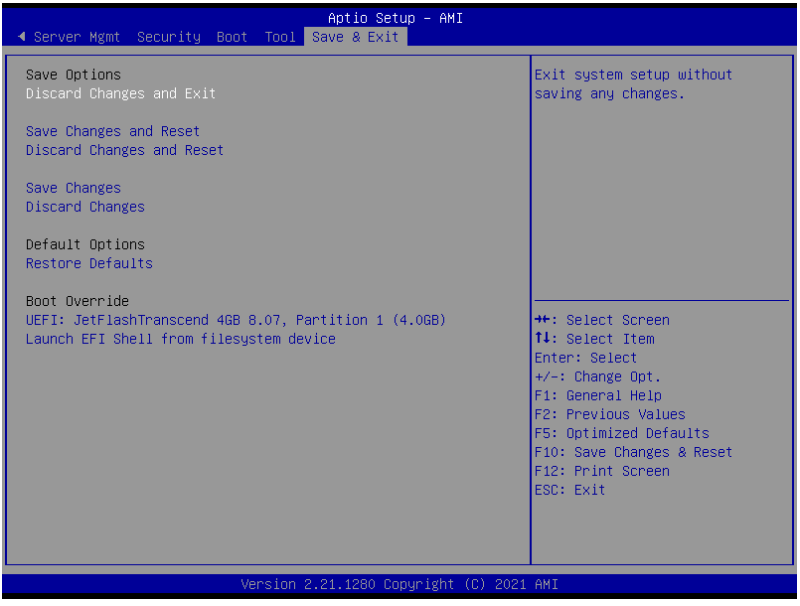
Allows you to run the IPMI hardware monitor.

ASUS SMBIOS Viewer

Allows you to start ASUS SMBIOS Viewer when you press <Enter>.

5.13 Save & Exit menu

The Save & Exit menu items allow you to save or discard your changes to the BIOS items.



Pressing <Esc> does not immediately exit this menu. Select one of the options from this menu or <F10> from the legend bar to exit.

Discard Changes and Exit

Exit system setup without saving any changes.

Save Changes and Reset

Reset system after saving the changes.

Discard Changes and Reset

Reset system setup without saving any changes.

Save Changes

Save changes done so far to any of the setup options.

Discard Changes

Discard changes done so far to any of the setup options.

Restore Defaults

Restore/load default values for all the setup options.

Boot Override

These items displays the available devices. The device items that appears on the screen depends on the number of devices installed in the system. Click an item to start booting from the selected device.

6 RAID Configuration

This chapter provides instructions for setting up, creating, and configuring RAID sets using the available utilities.

6.1 Setting up RAID

The motherboard supports the **Intel® Rapid Storage Technology enterprise Option ROM Utility** with RAID 0, RAID 1, RAID 10, and RAID 5 support (for Windows OS and Linux).

6.1.1 RAID definitions

RAID 0 (Data striping) optimizes two identical hard disk drives to read and write data in parallel, interleaved stacks. Two hard disks perform the same work as a single drive but at a sustained data transfer rate, double that of a single disk alone, thus improving data access and storage. Use of two new identical hard disk drives is required for this setup.

RAID 1 (Data mirroring) copies and maintains an identical image of data from one drive to a second drive. If one drive fails, the disk array management software directs all applications to the surviving drive as it contains a complete copy of the data in the other drive. This RAID configuration provides data protection and increases fault tolerance to the entire system. Use two new drives or use an existing drive and a new drive for this setup. The new drive must be of the same size or larger than the existing drive.

RAID 10 is data striping and data mirroring combined without parity (redundancy data) having to be calculated and written. With the RAID 10 configuration you get all the benefits of both RAID 0 and RAID 1 configurations. Use four new hard disk drives or use an existing drive and three new drives for this setup.

RAID 5 stripes both data and parity information across three or more hard disk drives. Among the advantages of RAID 5 configuration include better HDD performance, fault tolerance, and higher storage capacity. The RAID 5 configuration is best suited for transaction processing, relational database applications, enterprise resource planning, and other business systems. Use a minimum of three identical hard disk drives for this setup.

If you want to boot the system from a hard disk drive included in a created RAID set, copy first the RAID driver from the support DVD to a floppy disk before you install an operating system to the selected hard disk drive.

6.1.2 Installing hard disk drives

The motherboard supports Serial ATA and NVME for RAID set configuration. For optimal performance, install identical drives of the same model and capacity when creating a disk array.

To install the SATA or NVME hard disks for RAID configuration, please refer to **2.5 Storage devices** for more information.

6.1.3 RAID configuration utilities

Depending on the RAID connectors that you use, you can create a RAID set using the utilities embedded in each RAID controller. For example, use the **Intel® Rapid Storage Technology** if you installed Serial ATA hard disk drives on the Serial ATA connectors supported by the Intel® C621A chipset.

Refer to the succeeding section for details on how to use the RAID configuration utility.

6.2 Intel® Virtual Raid on CPU in BIOS

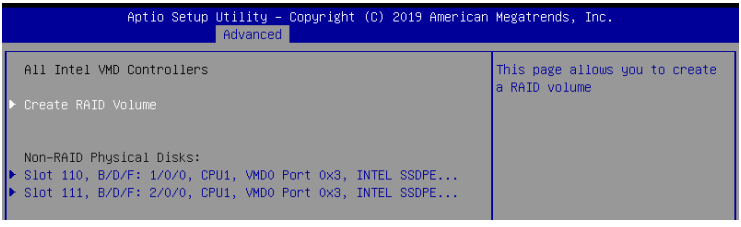
This feature allows you to do CPU RAID functions with Intel® CPU RSTe.

- Due to chipset behavior, enabling the Intel® RSTe CPU RAID functions requires an Intel® VROC hardware key module.
- Refer to section **4.3 Internal connectors** for the location of the VROC_KEY1 connector.
- The KEY module is purchased separately.

To enter the Intel® Virtual Raid on CPU in BIOS:

1. Enter the BIOS Setup during POST.
2. Go to the **Advanced** menu **> Intel(R) Virtual Raid on CPU** > **All Intel VMD Controllers** then press <Enter> to display the Intel® Virtual Raid on CPU menu.

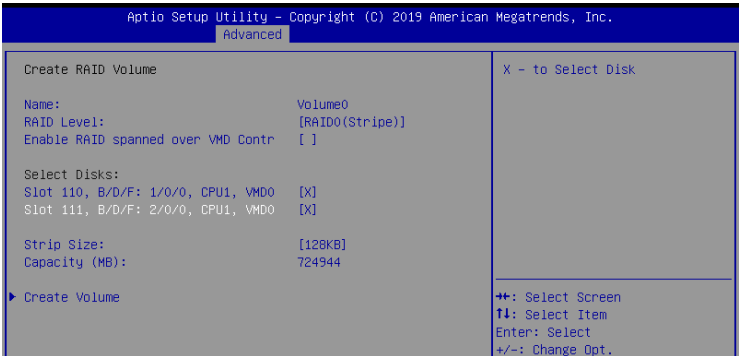
Refer to Chapter 5 for details on entering and navigating through the BIOS Setup.



6.2.1 Creating a RAID set

To create a RAID set:

1. From the Intel® Virtual Raid on CPU menu, select **Create RAID Volume** and press <Enter>. The following screen appears:



2. When the **Name** item is selected, enter a name for the RAID set and press <Enter>.
3. When the **RAID Level** item is selected, press <Enter> to select the RAID level to create, and then press <Enter>.
4. When the **Enable RAID spanned over VMD Controllers** item is selected, press <Enter> and select **X** to enable this function.
5. Under Select Disks, press <Enter> and select **X** for the disks you want to include in the RAID set.
6. When the **Strip Size** item is selected, press <Enter> to select strip size for the RAID array (for RAID 0, 10 and 5 only), and then press <Enter>. The available strip size values range from 4 KB to 128 KB. The following are typical values:
   - RAID 0: 128 KB
   - RAID 10: 64 KB
   - RAID 5: 64 KB

We recommend a lower strip size for server systems, and a higher strip size for multimedia computer systems used mainly for audio and video editing.

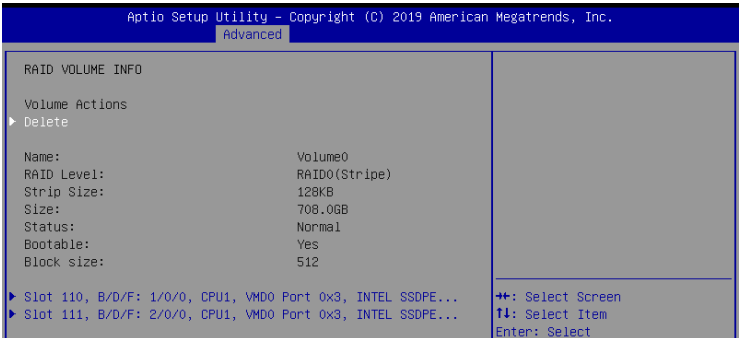
7. When the **Capacity (MB)** item is selected, enter the RAID volume capacity that you want and press <Enter>. The default value indicates the maximum allowed capacity.
8. When the **Create Volume** item is selected, press <Enter> to create the RAID volume and return to the Intel® Rapid Storage Technology menu.

6.2.2 Deleting a RAID set

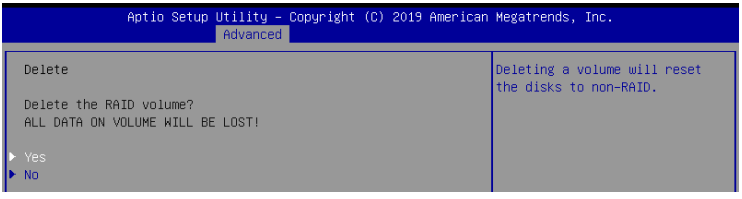
Be cautious when deleting a RAID set. You will lose all data on the hard disk drives when you delete a RAID set.

To delete a RAID set:

1. From the Intel® Virtual Raid on CPU menu, select the RAID volume you want to delete and press <Enter>. The following screen appears:



2. When the **Delete** item is selected, press <Enter>, then select **Yes** to delete the RAID volume and return to the Intel® Virtual Raid on CPU menu, or select **No** to cancel.



6.3 Intel® Rapid Storage Technology enterprise (Windows)

The Intel® Rapid Storage Technology enterprise allows you to create RAID 0, RAID 1, RAID 10 (RAID 1+0), and RAID 5 set(s) from Serial ATA hard disk drives that are connected to the Serial ATA connectors supported by the Southbridge.

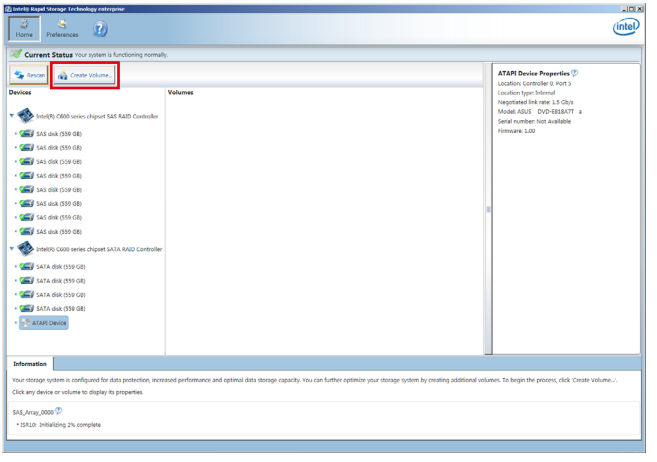
You need to manually install the Intel® Rapid Storage Technology enterprise utility on a Windows® operating system. Please refer to the installation instructions in Chapter 7.

To enter the Intel® Rapid Storage Technology enterprise utility under Windows operating system:

1. Turn on the system and go to the windows desktop.

2. Click the **Intel® Rapid Storage Technology enterprise** icon to display the main menu.

   Your storage system is configured for data protection, increased performance and optimal data storage capacity. You can create additional volumes to further optimize your storage system.

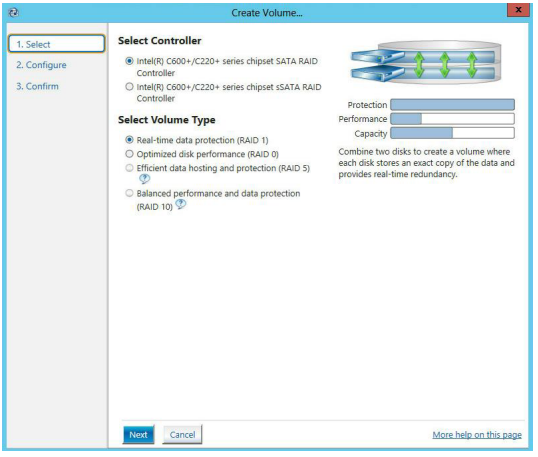


You can click **Rescan** to re-scan any attached hard disks.

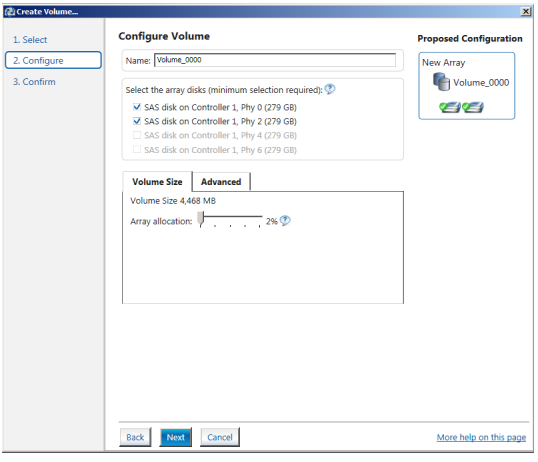
6.3.1 Creating a RAID set

To create a RAID set:

1. From the utility main menu, select **Create Volume** and select volume type.
2. Click **Next**.



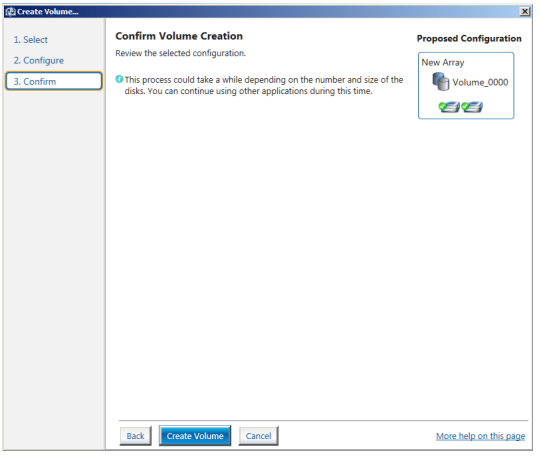
3. Enter a name for the RAID set, then select the array disks.
4. Select **Volume Size** tab, you can drag the bar to decide the volume size.
5. Click **Next**.



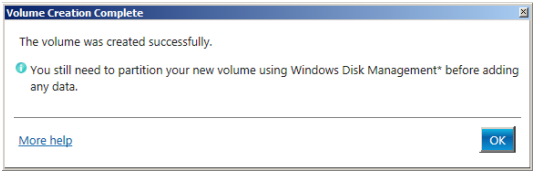
- If you do not want to keep the data on one of the selected disks, select **NO** when prompted.
- If you want to **Enable volume write-back cache** or **Initialize volume**, click **Advanced**.

6. Confirm the volume creation, than click **Create Volume** to continue.

This process could take a while depending on the number and size of the disks. You can continue using other applications during this time.

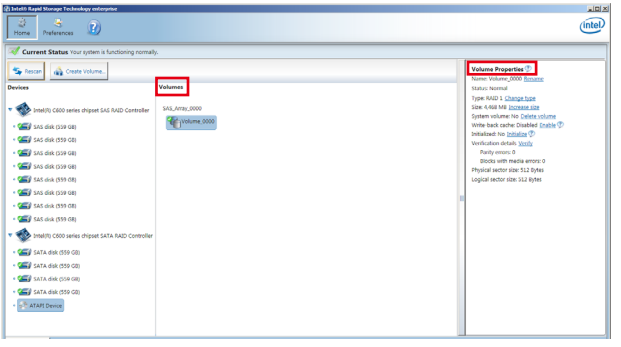


7. Wait until the process is completed, then click **OK** when prompted.



You still need to partition your new volume using Windows Disk Management before adding any data.

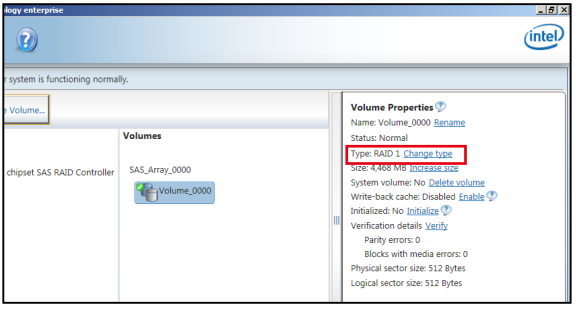
The RAID set is displayed in the **Volumes** list and you can change the settings in **Volume Properties**.



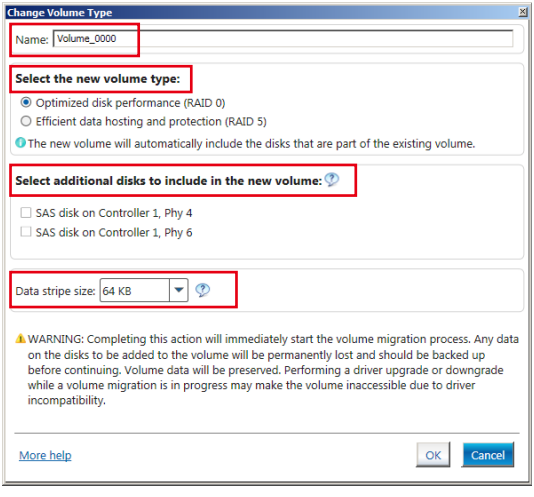
6.3.2 Changing a Volume Type

To change the volume type in **Volume Properties**:

1. Click the SATA array items you want to change in **Volumes** field.
2. From the **Volume Properties** field, select **Type: RAID 1 Change type**.



3. You can change the **Name**, **Select the new volume type**, and **Select additional disks to include in the new volume** if needed.
4. Select the **Data stripe size** for the RAID array (for RAID 0, 10 and 5 only), and click **OK**. The available stripe size values range from 4 KB to 128 KB. The following are typical values:
   RAID 0: 128KB
   RAID 10: 64KB
   RAID 5: 64KB



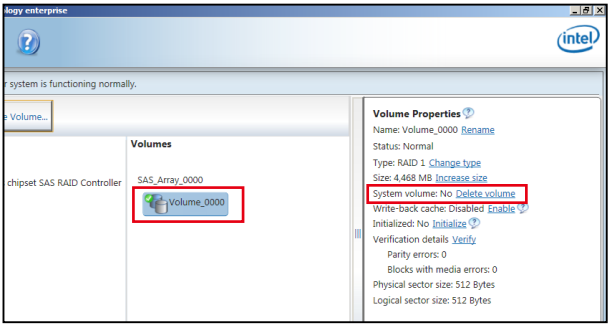
We recommend a lower stripe size for server systems, and a higher stripe size for multimedia computer systems used mainly for audio and video editing.

6.3.3 Deleting a volume

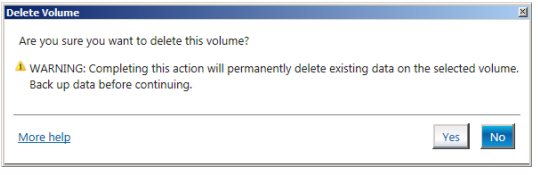
Be cautious when deleting a volume. You will lose all data on the hard disk drives. Before you proceed, ensure that you back up all your important data from your hard drives.

To delete a volume:

1. From the utility main menu, select the volume (ex. Volume_0000) in **Volumes** field you want to delete.



2. Select **Delete volume** in **Volume Properties** field. The following screen appears.

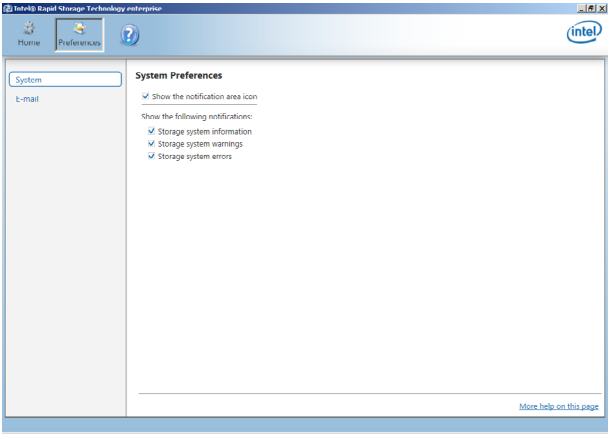


3. Click **Yes** to delete the volume and return to the utility main menu, or click **No** to return to the main menu.

6.3.4 Preferences

System Preferences

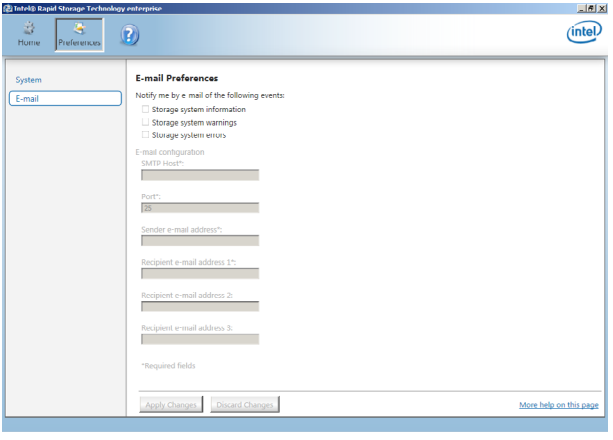
Allow you to set to show the notification area icon and show system information, warning, or errors here.



E-Mail Preferences

Allow you to set to sent e-mail of the following events:

- Storage system information
- Storage system warnings
- Storage system errors



7 Driver Installation

This chapter provides instructions for installing the necessary drivers for different system components.

7.1 Running the Support DVD

The support DVD that is bundled with your motherboard contains drivers, management applications, and utilities that you can install to maximize the features of your motherboard.

The contents of the support DVD are subject to change at any time without notice. Visit the ASUS website (www.asus.com) for the latest updates on software and utilities.

The main screen of the Support DVD contains the following tabs:

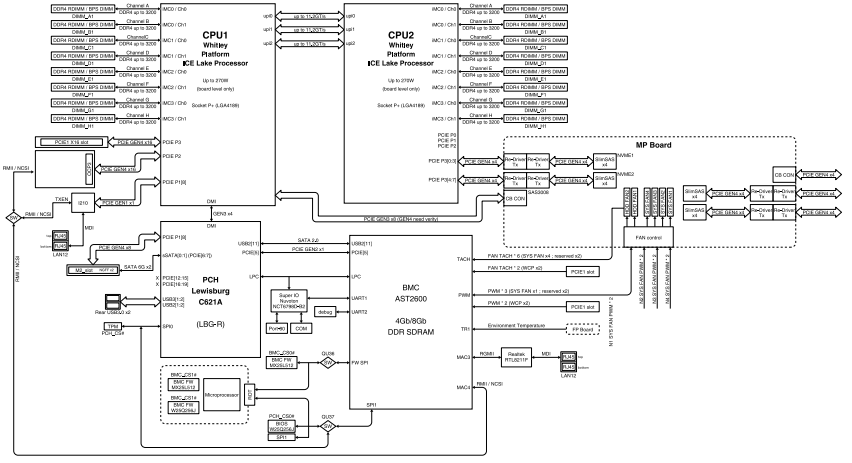
1. Drivers - Shows the available device drivers that the system detects.
2. Utilities - Displays the software applications and utilities that the motherboard supports.
3. Manual - Provides the link to the user guide(s).

You need an internet browser installed in your OS to view the User Guide.

4. Contact - Displays the ASUS contact information, e-mail addresses, and useful links if you need more information or technical support for your motherboard.

Appendix

Z12PH-D16 block diagram



Notices

Federal Communications Commission Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class A 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 commercial environment. 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. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

The use of shielded cables for connection of the monitor to the graphics card is required to assure compliance with FCC regulations. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

Compliance Statement of Innovation, Science and Economic Development Canada (ISED)

This device complies with Innovation, Science and Economic Development Canada licence exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

CAN ICES-003(A)/NMB-003(A)

Déclaration de conformité de Innovation, Sciences et Développement économique Canada (ISED)

Le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

CAN ICES-003(A)/NMB-003(A)

Australia statement notice

From 1 January 2012 updated warranties apply to all ASUS products, consistent with the Australian Consumer Law. For the latest product warranty details please visit https://www.asus.com/support/. Our goods come with guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure.

If you require assistance please call ASUS Customer Service 1300 2787 88 or visit us at https://www.asus.com/support/.

DO NOT throw the motherboard in municipal waste. This product has been designed to enable proper reuse of parts and recycling. This symbol of the crossed out wheeled bin indicates that the product (electrical and electronic equipment) should not be placed in municipal waste. Check local regulations for disposal of electronic products.

DO NOT throw the mercury-containing button cell battery in municipal waste. This symbol of the crossed out wheeled bin indicates that the battery should not be placed in municipal waste.

Japan statement notice

This product cannot be directly connected to the Internet (including public wireless LAN) of a telecom carrier (mobile network companies, landline network companies, Internet providers, etc.). When connecting this product to the Internet, be sure to connect it through a router or switch.

Declaration of compliance for product environmental regulation

ASUS follows the green design concept to design and manufacture our products, and makes sure that each stage of the product life cycle of ASUS product is in line with global environmental regulations. In addition, ASUS disclose the relevant information based on regulation requirements.

Please refer to http://csr.asus.com/Compliance.htm for information disclosure based on regulation requirements ASUS is complied with:

EU REACH and Article 33

Complying with the REACH (Registration, Evaluation, Authorization, and Restriction of Chemicals) regulatory framework, we publish the chemical substances in our products at ASUS REACH website at http://csr.asus.com/english/REACH.htm.

EU RoHS

This product complies with the EU RoHS Directive. For more details, see http://csr.asus.com/english/article.aspx?id=35

Japan JIS-C-0950 Material Declarations

Information on Japan RoHS (JIS-C-0950) chemical disclosures is available on http://csr.asus.com/english/article.aspx?id=19

India RoHS

This product complies with the “India E-Waste (Management) Rules, 2016” and prohibits use of lead, mercury, hexavalent chromium, polybrominated biphenyls (PBBs) and polybrominated diphenyl ethers (PBDEs) in concentrations exceeding 0.1% by weight in homogenous materials and 0.01% by weight in homogenous materials for cadmium, except for the exemptions listed in Schedule II of the Rule.

Vietnam RoHS

ASUS products sold in Vietnam, on or after September 23, 2011,meet the requirements of the Vietnam Circular 30/2011/TT-BCT.

Các sản phẩm ASUS bán tại Việt Nam, vào ngày 23 tháng 9 năm2011 trở về sau, đều phải đáp ứng các yêu cầu của Thông tư 30/2011/TT-BCT của Việt Nam.

Turkey RoHS

AEEE Yönetmeliğine Uygundur

ASUS Recycling/Takeback Services

ASUS recycling and takeback programs come from our commitment to the highest standards for protecting our environment. We believe in providing solutions for you to be able to responsibly recycle our products, batteries, other components as well as the packaging materials. Please go to http://csr.asus.com/english/Takeback.htm for detailed recycling information in different regions.

Ecodesign Directive

European Union announced a framework for the setting of ecodesign requirements for energy-related products (2009/125/EC). Specific Implementing Measures are aimed at improving environmental performance of specific products or across multiple product types. ASUS provides product information on the CSR website. The further information could be found at https://csr.asus.com/english/article.aspx?id=1555.

Service and Support

Visit our multi-language website at https://www.asus.com/support/