



# ESC4000-E10S

## 2U Rackmount Server User Guide



**Copyright © 2023 ASUSTeK COMPUTER INC. All Rights Reserved.**

No part of this manual, including the products and software described in it, may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means, except documentation kept by the purchaser for backup purposes, without the express written permission of ASUSTeK COMPUTER INC. ("ASUS").

ASUS provides this manual "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties or conditions of merchantability or fitness for a particular purpose. In no event shall ASUS, its directors, officers, employees, or agents be liable for any indirect, special, incidental, or consequential damages (including damages for loss of profits, loss of business, loss of use or data, interruption of business and the like), even if ASUS has been advised of the possibility of such damages arising from any defect or error in this manual or product.

Specifications and information contained in this manual are furnished for informational use only, and are subject to change at any time without notice, and should not be construed as a commitment by ASUS. ASUS assumes no responsibility or liability for any errors or inaccuracies that may appear in this manual, including the products and software described in it.

Product warranty or service will not be extended if: (1) the product is repaired, modified or altered, unless such repair, modification or alteration is authorized in writing by ASUS; or (2) the serial number of the product is defaced or missing.

Products and corporate names appearing in this manual may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation and to the owners' benefit, without intent to infringe.

# Contents

Safety information.....	vii
About this guide.....	ix

## Chapter 1: Product Introduction

1.1	System package contents.....	1-2
1.2	Serial number label.....	1-2
1.3	System specifications .....	1-3
1.4	Front panel features.....	1-5
1.5	Rear panel features.....	1-5
1.6	Internal features .....	1-6
1.7	LED information .....	1-7
1.7.1	Front panel LEDs .....	1-7
1.7.2	LAN (RJ-45) LEDs .....	1-8
1.7.3	HDD status LEDs.....	1-9
1.7.4	Q-Code/Port 80 status LEDs.....	1-10

## Chapter 2: Hardware Setup

2.1	Chassis cover.....	2-2
2.1.1	Air duct.....	2-4
2.2	Central Processing Unit (CPU) .....	2-5
2.2.1	Installing the CPU and heatsink .....	2-5
2.3	System memory .....	2-9
2.3.1	Overview .....	2-9
2.3.2	Memory Configurations.....	2-9
2.3.3	Installing a DIMM on a single clip DIMM socket.....	2-11
2.3.4	Removing a DIMM .....	2-12
2.4	Storage devices.....	2-13
2.4.1	To install a 2.5" hot-swap SATA/SAS/NVMe storage device....	2-13
2.5	Expansion slots.....	2-15
2.5.1	The PCI Express riser card.....	2-15
2.5.2	Installing an ASUS PIKE II card.....	2-18
2.5.3	Reconnecting the cable to the M.2 expansion board (only for SKU-3) .....	2-21
2.5.4	Installing an M.2 (NGFF) card.....	2-23
2.5.5	Reconnecting the cable to the OCP 3.0 slot baseboard (only for SKU-2) .....	2-24
2.5.6	(optional) Installing the PFR module .....	2-26
2.5.7	Configuring an expansion card .....	2-27

# Contents

- 2.6 Cable connections ..... 2-28
- 2.7 SATA/SAS backplane cabling ..... 2-29
  - 2.7.1 Reconnecting the cable for 4 NVMe configuration ..... 2-30
- 2.8 Removable/optional components ..... 2-32
  - 2.8.1 Cable organizer metal cover ..... 2-32
  - 2.8.2 System fans ..... 2-33
  - 2.8.3 Redundant power supply units ..... 2-34
  - 2.8.4 GPU cards ..... 2-36
- 2.9 Rail Kit Options ..... 2-40

## Chapter 3: Motherboard Information

- 3.1 ASUS Z12PG-D16 Motherboard layout ..... 3-2
- 3.2 Jumpers ..... 3-4
- 3.3 Internal connectors ..... 3-9
- 3.4 Onboard LEDs ..... 3-17

## Chapter 4: BIOS Setup

- 4.1 Managing and updating your BIOS ..... 4-2
  - 4.1.1 ASUS CrashFree BIOS 3 utility ..... 4-2
  - 4.1.2 ASUS EZ Flash Utility ..... 4-3
  - 4.1.3 BUPDATER utility ..... 4-4
- 4.2 BIOS setup program ..... 4-6
  - 4.2.1 BIOS menu screen ..... 4-7
  - 4.2.2 Menu bar ..... 4-7
- 4.3 Main menu ..... 4-9
- 4.4 Advanced menu ..... 4-10
  - 4.4.1 OffBoard SATA Controller Configuration ..... 4-10
  - 4.4.2 Trusted Computing ..... 4-11
  - 4.4.3 ACPI Settings ..... 4-11
  - 4.4.4 Redfish Host Interface Settings ..... 4-11
  - 4.4.5 Onboard LAN Configuration ..... 4-12

# Contents

4.4.6	Serial Port Console Redirection .....	4-13
4.4.7	SIO Common Setting .....	4-15
4.4.8	SIO Configuration.....	4-16
4.4.9	PCI Subsystem Settings .....	4-17
4.4.10	USB Configuration .....	4-18
4.4.11	Network Stack Configuration.....	4-19
4.4.12	CSM (Compatibility Support Module).....	4-20
4.4.13	NVMe Configuration.....	4-21
4.4.14	APM Configuration .....	4-22
4.4.15	Third-party UEFI driver configurations .....	4-23
<b>4.5</b>	<b>Platform Configuration menu .....</b>	<b>4-24</b>
4.5.1	PCH Configuration .....	4-24
4.5.2	Miscellaneous Configuration .....	4-25
4.5.3	Server ME Configuration.....	4-26
4.5.4	Runtime Error Logging Support .....	4-27
<b>4.6</b>	<b>Socket Configuration menu .....</b>	<b>4-30</b>
4.6.1	Processor Configuration.....	4-31
4.6.2	Common RefCode Configuration.....	4-34
4.6.3	Memory Configuration.....	4-35
4.6.4	IIO Configuration .....	4-36
4.6.5	Advanced Power Management Configuration.....	4-51
<b>4.7</b>	<b>Event Logs menu .....</b>	<b>4-56</b>
4.7.1	Change Smbios Event Log Settings .....	4-57
4.7.2	View Smbios Event Log .....	4-58
<b>4.8</b>	<b>Server Mgmt menu .....</b>	<b>4-59</b>
4.8.1	System Event Log .....	4-60
4.8.2	BMC self test log .....	4-60
4.8.3	BMC network configuration .....	4-61
4.8.4	View System Event Log .....	4-63

# Contents

- 4.9 Security menu ..... 4-64
  - 4.9.1 Secure Boot ..... 4-65
- 4.10 Boot menu ..... 4-68
  - 4.10.1 Boot Configuration ..... 4-69
- 4.11 Tool menu ..... 4-70
- 4.12 Save & Exit menu ..... 4-71

## Chapter 5: Driver Installation

- 5.1 Running the Support DVD ..... 5-2

## Appendix

- Z12PG-D16 block diagram ..... A-2
- Notices ..... A-3
- Service and Support ..... A-5

# 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 Setup**

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

**3. Chapter 3: 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.

**4. Chapter 4: BIOS Setup**

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

**5. Chapter 5: 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.

# Product Introduction

# 1

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

# 1.1 System package contents

Check your system package for the following items.

ESC4000-E10S	
Chassis	ASUS 2U Rackmount Chassis
Motherboard	ASUS Z12PG-D16 Server Board
Accessory box	1 x MB Support DVD 1 x ACC instruction card 1 x Bag of Screws 2 x AC Power Cables 8 x 6+2-pin VGA Power cables 4 x ASUS GPU 8-pin Power cables 4 x GPU air ducts (for Nvidia/AMD cards) 2 x CPU heatsink 1 x Rail Kit (optional)



- If any of the above items is damaged or missing, contact your retailer.
- Optional items come bundled if you selected them when purchasing the system and cannot be bought separately.

# 1.2 Serial number label

Before requesting support from the ASUS Technical Support team, you must take note of the product's serial number containing 12 characters such as xxSxxxxxxx. See the figure below.

With the correct serial number of the product, ASUS Technical Support team members can then offer a quicker and satisfying solution to your problems.



The serial number is printed on the Asset tag.

## 1.3 System specifications

The ASUS ESC4000-E10S Series servers features the ASUS Z12PG-D16 server board that supports Intel® 3<sup>rd</sup> Gen Xeon® Scalable Processors.

Model Name		ESC4000-E10S
<b>Processor / System Bus</b>		Intel® 3 <sup>rd</sup> Gen Xeon® Scalable Processors (up to 235W)
<b>Memory</b>	<b>Total Slots</b>	16 (8 channel per CPU, 8 DIMM per CPU)
	<b>Capacity</b>	Maximum up to 4,096GB
	<b>Memory Type</b>	DDR4 3200/2933 RDIMM/LR-DIMM/LR-DIMM 3DS Intel® Optane Persistent Memory * Please refer to <a href="http://www.asus.com">www.asus.com</a> for latest memory AVL update
	<b>Memory Size</b>	32GB, 16GB (RDIMM) 64GB, 32GB (LRDIMM) 128GB, 64GB (LRDIMM 3DS) * Please refer to <a href="http://www.asus.com">www.asus.com</a> for latest memory AVL update
<b>Expansion Slots</b>	<b>Total PCI/PCI-X/PCI-E/PIKE Slots</b>	11
	<b>Slot Type</b>	<b>Rear:</b> - 4 x PCIe x16 slots (Gen4 x16 link, FH, FL) for dual-slot GPU cards or 8 x PCIe x16 slots (Gen4 x8 link, FH, FL) for single-slot GPU cards - 2 x PCIe x16 slots (Gen4 x16 link, LP, HL) <b>Front:</b> <u>SKU-1 (default)</u> - 1 x PCIe x8 slot (Gen4 x8 link, LP, HL) <u>SKU-2 (per request)</u> - 1 x PCIe x8 slot (Gen4 x8 link, LP, HL) or - 1 x OCP3.0 slot (Gen4 x8 link) by reconnecting the cables <u>SKU-3 (per request)</u> - 1 x PCIe x8 slot (Gen4 x8 link, LP,HL) or - 2 x M.2 sockets (Gen4 x4 link, up to 2280 module) by reconnecting the cables
<b>Disk Controller</b>	<b>SATA Controller</b>	Intel® PCH integrated - 8 x SATA 6Gb/s ports
	<b>SAS Controller</b>	Optional Kits: (One PCIe slot will be occupied) - ASUS PIKE II 3008 8-port SAS HBA Card - ASUS PIKE II 3108 8-port SAS HW RAID Card Support SAS 12Gbps
	<b>NVMe Controller</b>	Intel® CPU integrated Supports Intel® VROC Feature with VROC H/W Key
<b>Storage Bays</b>		8 x 2.5" Hot-swap Storage Bays (backplane supports 4 x SATA/SAS + 4 x SATA/SAS/NVME) 1 x M.2 socket onboard (Gen3 x4 link or SATA mode, up to 2280 module)
<b>Networking</b>	<b>LAN</b>	1 x Dual Port Intel® I350 Gigabit LAN Controller
<b>Graphic</b>	<b>VGA</b>	BMC Integrated (Aspeed AST2600 64MB)
<b>Front I/O ports</b>		4 x USB 3.2 Gen 1 ports

(continued on the next page)

## System specifications

Model Name		ESC4000-E10S
Rear I/O ports		2 x USB 3.2 Gen 1 ports 2 x Gigabit LAN ports (RJ45) 1 x Management port (RJ45) 1 x VGA port
Switch/LED		<b>Front :</b> 1 x Power Switch/LED 1 x Location Switch/LED 1 x HDD LED 1 x Message LED 1 x Q-Code/Port 80 LED 2 x LAN LED <b>Rear :</b> 1 x Power switch/LED 1 x Location LED 1 x Message LED 1 x HDD Access LED
OS Support		Windows® Server 2019 Windows® Server 2022 RedHat® SuSE® Ubuntu Vmware * Please find the latest OS support from <a href="https://www.asus.com/event/Server/OS_support_list/OS.html">https://www.asus.com/event/Server/OS_support_list/OS.html</a>
Management Solution	Out of Band Remote Hardware	ASMB10-iKVM (on-board)
	Software	ASUS Control Center
Dimension		800mm x 440mm x 88mm (2U) 31.50" x 17.22" x 3.46"
Net Weight Kg		34 kg (excluding CPU, DRAM, and HDD)
Gross Weight Kg		44 kg (including packaging, excluding CPU, DRAM, and HDD)
Power Supply (following different configuration by region)		1+1 Redundant 1600W 80 PLUS Platinum Power Supply 1+1 Redundant 2200W 80 PLUS Platinum Power Supply
Environment		Operation temperature: 10° ~ 35° Non operation temperature: -40° ~ 70° Non operation humidity: 20% ~ 90% ( Non condensing)



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.



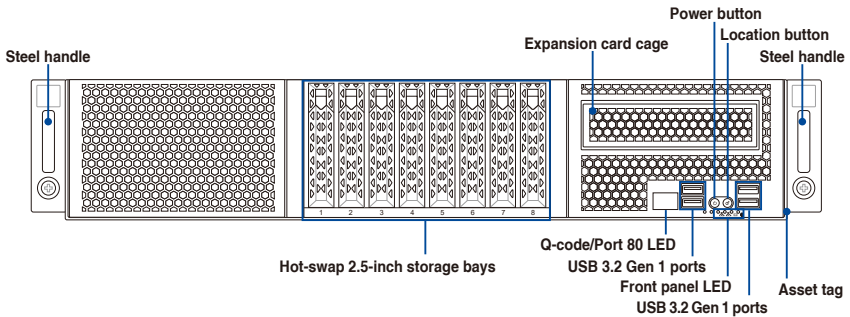
Specifications are subject to change without notice.

## 1.4 Front panel features

The barebone server features a simple yet stylish front panel. The power and location buttons, LED indicators, and USB ports are located and easily accessible on the front panel.

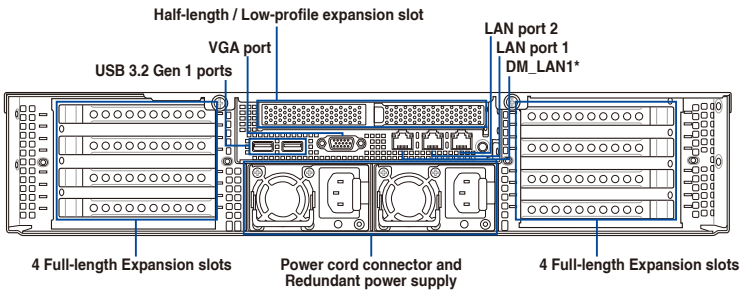


Refer to the **Front panel LEDs** section for the LED descriptions.



## 1.5 Rear panel features

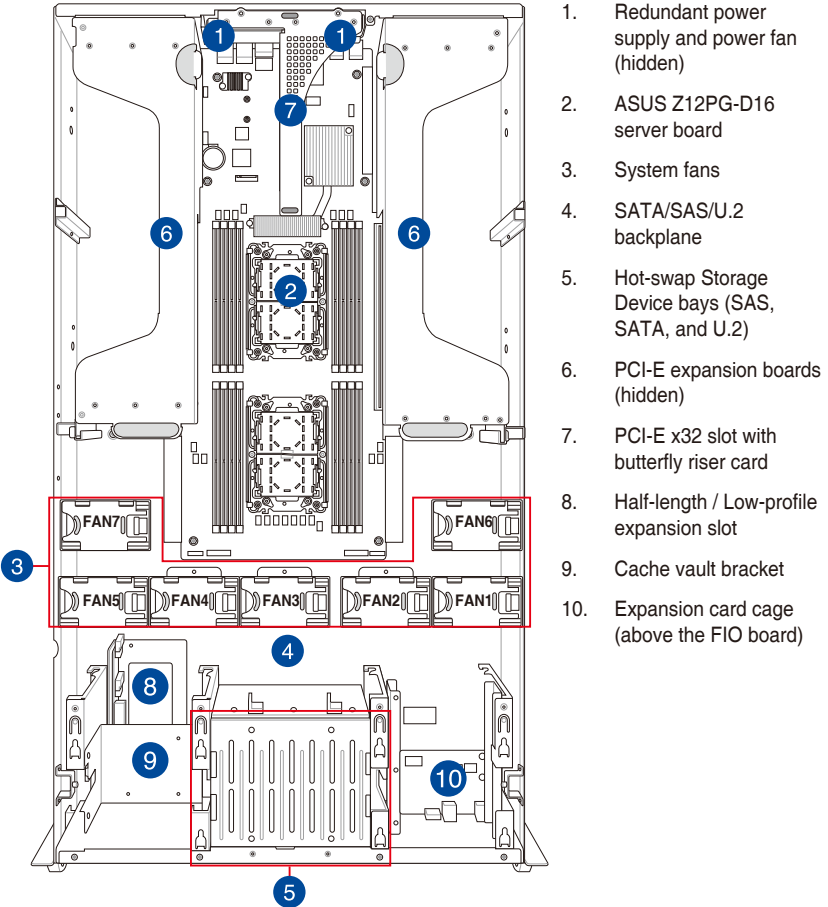
The expansion slots and system power socket is located on the rear panel of the server. The middle part includes the I/O shield with openings for the rear panel connectors on the motherboard.



- The rear I/O ports do not appear on the rear panel if motherboard is not present.
- \*The DM\_LAN1 port is for ASUS ASMB10-iKVM controller only.

## 1.6 Internal features

The barebone server includes the basic components as shown.



1. Redundant power supply and power fan (hidden)
2. ASUS Z12PG-D16 server board
3. System fans
4. SATA/SAS/U.2 backplane
5. Hot-swap Storage Device bays (SAS, SATA, and U.2)
6. PCI-E expansion boards (hidden)
7. PCI-E x32 slot with butterfly riser card
8. Half-length / Low-profile expansion slot
9. Cache vault bracket
10. Expansion card cage (above the FIO board)



A protection film is pre-attached to the front cover before shipping. Please remove the protection film before turning on the system for proper heat dissipation.

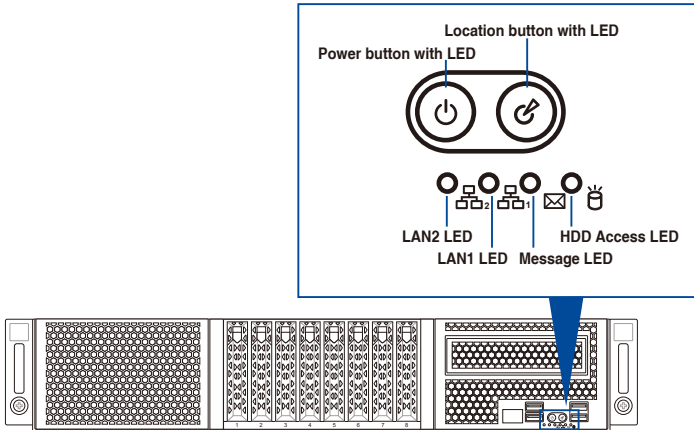
### WARNING

HAZARDOUS MOVING PARTS  
KEEP FINGERS AND OTHER BODY PARTS AWAY



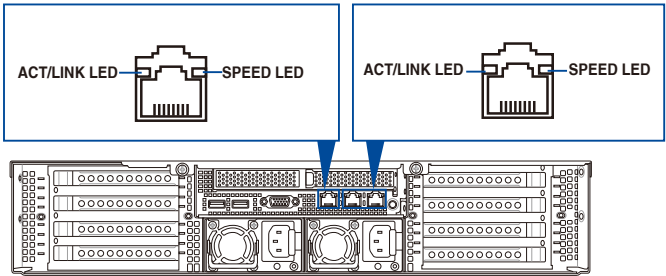
## 1.7 LED information

### 1.7.1 Front panel LEDs



LED	Icon	Display status	Description
Power button with LED		ON	System power on
HDD access LED		OFF	No activity
		Blinking	Data activity
Message LED		OFF	System is normal; no incoming event
		ON	A hardware monitor event is indicated
Location button with LED		OFF	Function off
		ON	Location switch is pressed (Press the location switch again to turn off)
LAN LEDs		OFF	No LAN connection
		Blinking	LAN is transmitting or receiving data
		ON	LAN connection is present

## 1.7.2 LAN (RJ-45) LEDs



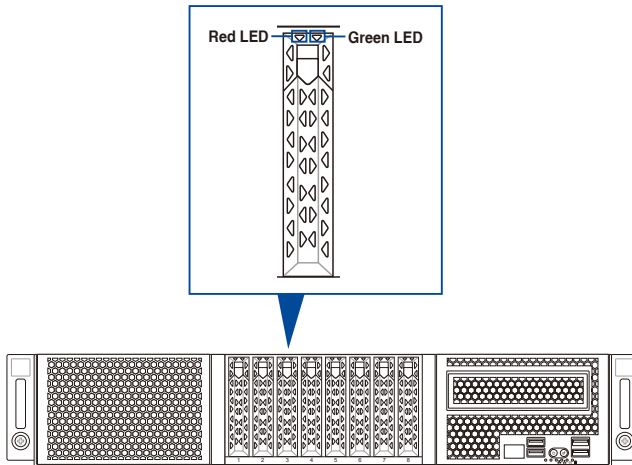
### LAN1/LAN2 LEDs

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

### Dedicated Management LAN (for ASMB10 and DM\_LAN1)

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

### 1.7.3 HDD status LEDs



SATA/SAS HDD LED Description		
GREEN	ON	SATA/SAS HDD power ON
RED	ON	HDD has failed and should be swapped immediately
GREEN/RED	Blinking	RAID rebuilding
GREEN/RED	Blinking	Locate
GREEN/RED	OFF	HDD not found
GREEN	Blinking	Read/write data from/into the SATA/SAS HDD

## 1.7.4 Q-Code/Port 80 status LEDs

The Q-Code LED provides a 2-digit display that shows the status of your system. Refer to the **Q-Code** table of this user guide for more information about the 2-digit codes.

**Q-Code table**

Action	PHASE	POST CODE	TYPE	DESCRIPTION
SEC Start up	Security Phase	0x1	Progress	First post code
		0x2	Progress	Load BSP microcode
		0x3	Progress	Perform early platform Initialization
		0x4	Progress	Set cache as ram for PEI phase
		0x5	Progress	Establish Stack
		0x6	Progress	CPU Early Initialization
	PEI(Pre-EFI Initialization) phase	0x10	Progress	PEI Core Entry
		0x11	Progress	PEI cache as ram CPU initial
		0x15	Progress	NB Initialization before installed memory
		0x19	Progress	SB Initialization before installed memory
		0x20	Progress	SB Initialization after installed memory
	MRC Progress phase	0xB0	MRC Progress	DIMM detect
		0xB1	MRC Progress	DIMM clock Initialization
		0xB2	MRC Progress	DIMM SPD data Initialization
		0xB3	MRC Progress	DIMM global early
		0xB4	MRC Progress	DIMM rank detect
		0xB5	MRC Progress	DIMM channel early
		0xB6	MRC Progress	DIMM DDRI0 Initialization
		0xB7	MRC Progress	DIMM channel training
		0xB8	MRC Progress	DIMM Initialization throttling
		0xB9	MRC Progress	memory BIST
		0xBA	MRC Progress	MEM memory Initialization
		0xBB	MRC Progress	DIMM DDR memory map
		0xBC	MRC Progress	RAS configuration
		0xBD	MRC Progress	Get Margins
0xBE	MRC Progress	Memory SSA api Initialization		
0xBF	MRC Progress	MRC done		
Quick VGA		0x32	Progress	CPU POST-Memory Initialization
		0x33	Progress	CPU Cache Initialization
		0x34	Progress	Application Processor(s) (AP) Initialization
		0x35	Progress	BSP Selection
		0x36	Progress	CPU Initialization
		0x37	Progress	Pre-memory NB Initialization
		0x3B	Progress	Pre-memory SB Initialization
		0x4F	Progress	DXE Initial Program Load(IPL)
		0x60	Progress	DXE Core Started
		0x61	Progress	DXE NVRAM Initialization
		0x62	Progress	SB run-time Initialization
		0x63	Progress	CPU DXE Initialization
		0x68	Progress	PCI HB Initialization
		0x69	Progress	NB DXE Initialization
	DXE(Driver Execution Environment) phase	0x6A	Progress	NB DXE SMM Initialization
		0x70	Progress	SB DXE Initialization
		0x71	Progress	SB DXE SMM Initialization
		0x72	Progress	SB DEVICES Initialization
		0x78	Progress	ACPI Module Initialization
		0x79	Progress	CSM Initialization
		0xD0	Progress	CPU PM Structure Initialization
		0xD1	Progress	CPU PM CSR programming
		0xD2	Progress	CPU PM MSR programming
		0xD3	Progress	CPU PM PSTATE transition
		0xD4	Progress	CPU PM driver exit
0xD5	Progress	CPU PM On ready to boot event		

(continued on the next page)

## Q-Code table

Action	PHASE	POST CODE	TYPE	DESCRIPTION
Normal boot	BDS(Boot Device Selection) phase	0x90	Progress	BDS started
		0x91	Progress	Connect device event
		0x92	Progress	PCI Bus Enumeration
		0x93	Progress	PCI Bus Enumeration
		0x94	Progress	PCI Bus Enumeration
		0x95	Progress	PCI Bus Enumeration
		0x96	Progress	PCI Bus Enumeration
		0x97	Progress	Console outout connect event
		0x98	Progress	Console input connect event
		0x99	Progress	AMI Super IO start
		0x9A	Progress	AMI USB Driver Initialization
		0x9B	Progress	AMI USB Driver Initialization
		0x9C	Progress	AMI USB Driver Initialization
		0x9D	Progress	AMI USB Driver Initialization
		0xb2	Progress	Legacy Option ROM Initialization
		0xb3	Progress	Reset system
		0xb4	Progress	USB hotplug
		0xb6	Progress	NVRAM clean up
		0xb7	Progress	NVRAM configuration reset
		0xA0	Progress	IDE, AHCI Initialization
		0xA1	Progress	IDE, AHCI Initialization
		0xA2	Progress	IDE, AHCI Initialization
		0xA3	Progress	IDE, AHCI Initialization
		0x00-0xFF	Progress	Wait BMC ready
	0xA8	Progress	BIOS Setup Utility password verify	
	0xA9	Progress	BIOS Setup Utility start	
	0xAB	Progress	BIOS Setup Utility input wait	
	0xAD	Progress	Ready to boot event	
	0xAE	Progress	Legacy boot event	
	Operating system phase	0xAA	Progress	APIC mode
		0xAC	Progress	PIC mode



# Hardware Setup

# 2

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

# 2.1 Chassis cover

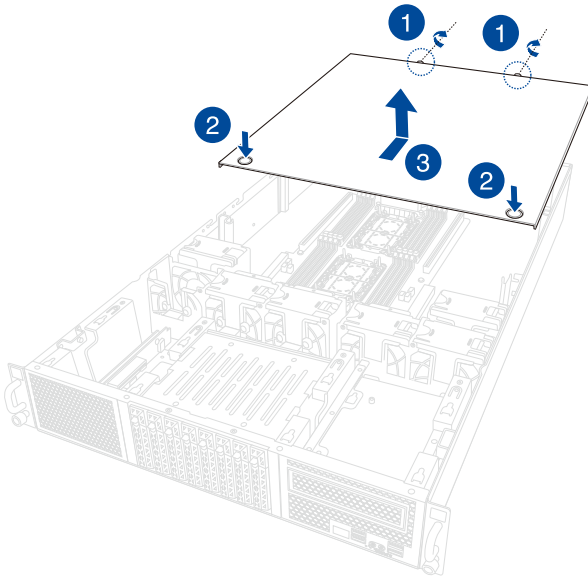
There are three parts of the chassis cover you may remove.



The diagrams in this section are for reference only. The system layout may vary with models, but the installation steps are the same for all models.

To remove the rear chassis cover:

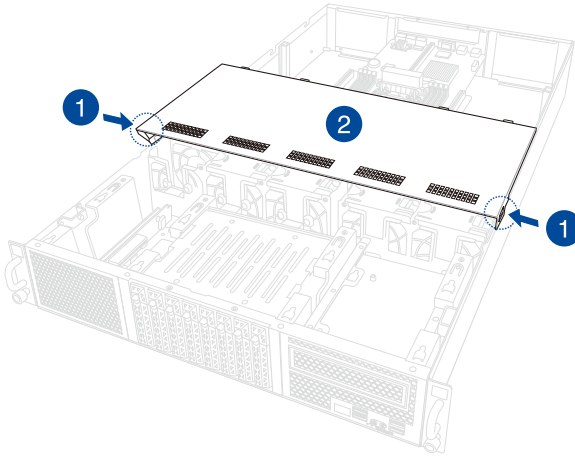
1. Release the two (2) thumbscrews on the rear of the chassis.
2. Push and hold the cover buttons down, then slide the chassis cover towards the rear to disengage it from the chassis.
3. Lift the chassis cover to completely remove it from the chassis.





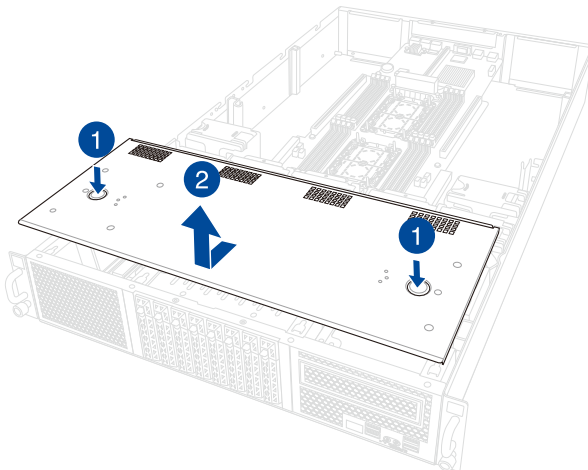
To remove the middle chassis cover:

1. Press the cover latches down on both sides of the middle chassis cover.
2. Lift the chassis cover to completely remove it from the chassis.



To remove the front chassis cover:

1. Push and hold the cover buttons down, then slide the chassis cover towards the front to disengage it from the chassis.
2. Lift the chassis cover to completely remove it from the chassis.



A protection film is pre-attached to the system cover before shipping. Please remove the protection film before turning on the system for proper heat dissipation.

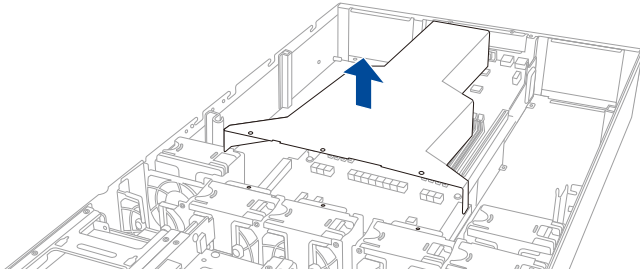
## 2.1.1 Air duct



The diagrams in this section are for reference only. The system layout may vary with models, but the installation steps are the same for all models.

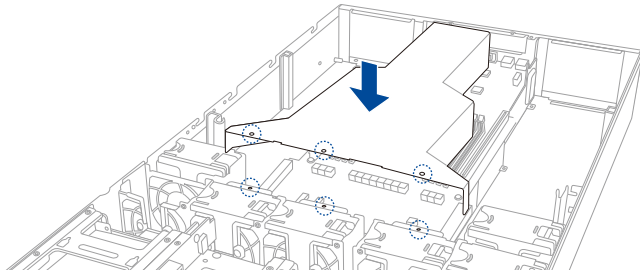
To remove the air duct:

Lift the air duct to remove it from the chassis.



To reinstall the air duct:

Align and replace the air duct to the chassis ensuring that the guide pins on the air duct match the positioning holes on the chassis.



## 2.2 Central Processing Unit (CPU)

The motherboard comes with a surface mount Socket P+ designed for 3<sup>rd</sup> Generation Intel® Xeon® Scalable processors.

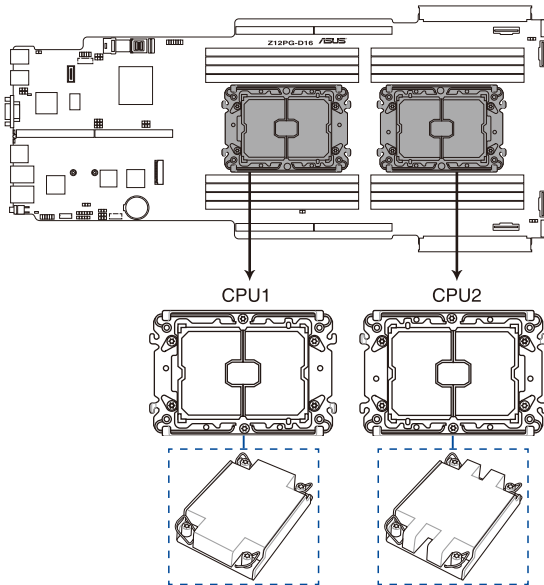


- Upon purchase of the motherboard, ensure that the PnP cap is on the socket and the socket contacts are not bent. Contact your retailer immediately if the PnP cap is missing, or if you see any damage to the PnP cap/socket contacts/motherboard components. ASUS will shoulder the cost of repair only if 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 CPU 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.

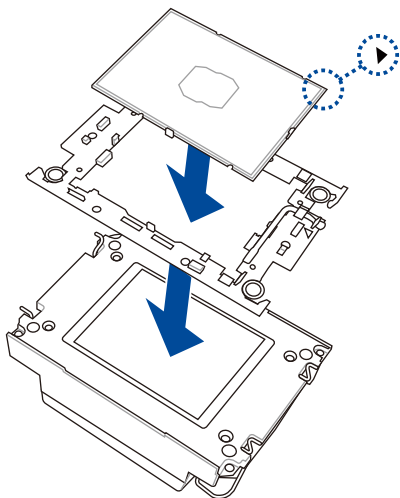
### 2.2.1 Installing the CPU and heatsink

1. Remove the rear chassis cover. For more information, see the **Chassis cover** section.
2. Remove the air duct. For more information, see the **Air Duct** section.
3. Locate the CPU sockets on the motherboard.

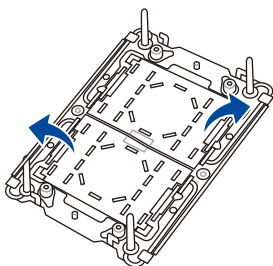
#### Z12PG-D16 CPU LGA 4189 Socket



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



5. Remove the PNP cap from the CPU socket.



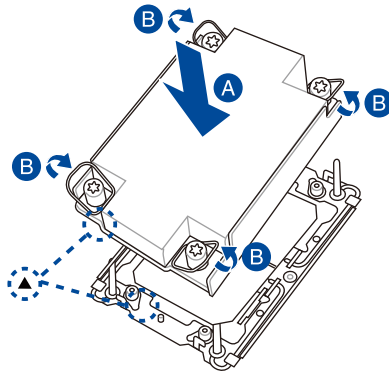
- Align the CPU and heatsink assembly in the correct orientation so that the triangle marks on both the CPU and socket are aligned in the same direction, then place the heatsinks on top of the CPU sockets (A). Push the lock latches inwards on all four corners of the heatsink so that the heatsink and CPU assembly is secured to the CPU socket (B).



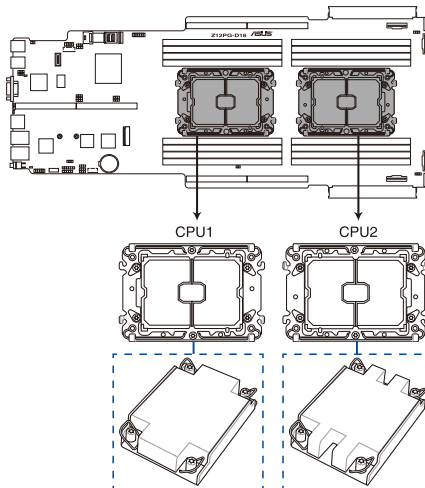
The CPU and CPU Carrier fits in only one correct orientation. DO NOT force the CPU and CPU Carrier into the socket to prevent damaging the CPU pins on the socket.



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



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



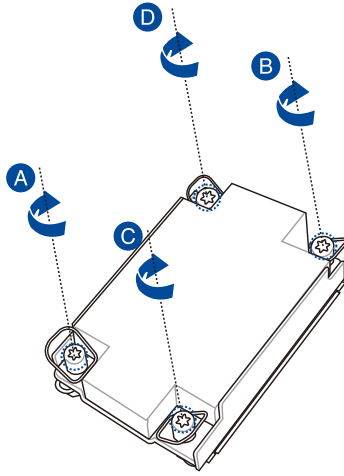
- Do two (2) clockwise turns on each of the heatsink screws in the cross order pattern shown on the illustration until the heatsink screws are tightened and the heatsink is secured onto the motherboard.



---

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

---



- Reinstall the air duct. For more information, see the section **Air Duct**.

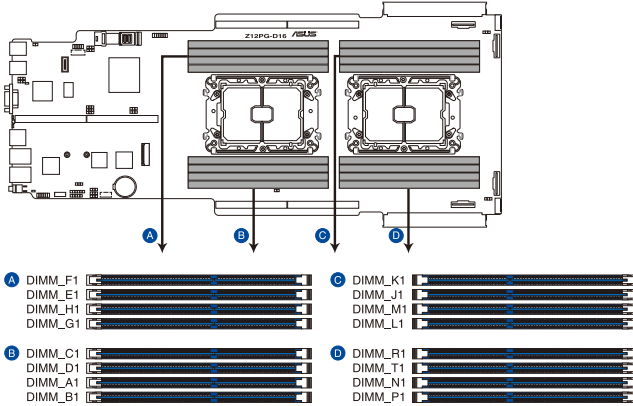
## 2.3 System memory

### 2.3.1 Overview

The motherboard comes with sixteen (16) Double Data Rate 4 (DDR4) Dual Inline Memory Modules (DIMM) sockets.

The figure illustrates the location of the DDR4 DIMM sockets:

#### Z12PG-D16 288-pin DDR4 DIMM sockets



### 2.3.2 Memory Configurations

You may install 16GB, 32GB DDR4 RDIMMs; 32GB, 64GB LRDIMMs; or 64GB, 128GB LRDIMM 3DS 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.

#### Recommended memory configuration for 1 CPU Configuration

1 CPU Configuration	A1	B1	C1	D1	E1	F1	G1	H1
1 DIMM	•							
2 DIMMs	•				•			
4 DIMMs	•		•		•		•	
6 DIMMs	•	•	•		•	•	•	
8 DIMMs	•	•	•	•	•	•	•	•

## Recommended memory configuration for 2 CPU Configuration

2 CPU Configuration								
	A1	B1	C1	D1	E1	F1	G1	H1
2 DIMMs	•							
4 DIMMs	•				•			
8 DIMMs	•		•		•		•	
12 DIMMs	•	•	•	•	•	•	•	
16 DIMMs	•	•	•	•	•	•	•	•

2 CPU Configuration								
	J1	K1	L1	M1	N1	P1	R1	T1
2 DIMMs	•							
4 DIMMs	•				•			
8 DIMMs	•		•		•		•	
12 DIMMs	•	•	•		•	•	•	
16 DIMMs	•	•	•	•	•	•	•	•

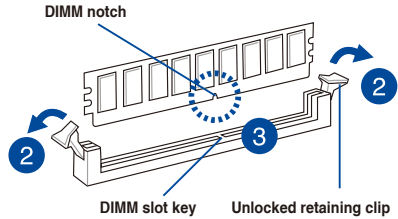


### 2.3.3 Installing a DIMM on a single clip DIMM socket



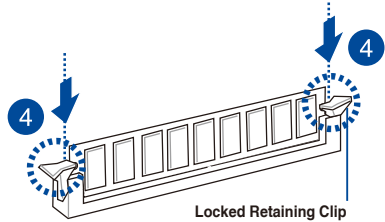
Ensure to unplug the power supply before adding or removing DIMMs or other system components. Failure to do so may cause severe damage to both the motherboard and the components.

1. Remove the rear chassis cover. For more information, refer to the **Chassis cover** section.
2. Unlock a DIMM socket by pressing the retaining clips outward.
3. 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.

4. 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.

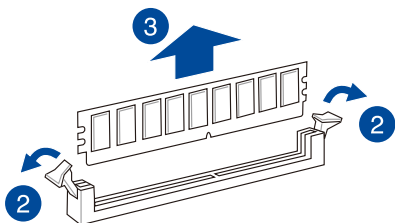


Always insert the DIMM into the socket **VERTICALLY** to prevent DIMM notch damage.

5. Replace the rear chassis cover. For more information, refer to the **Chassis cover** section.

## 2.3.4 Removing a DIMM

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



---

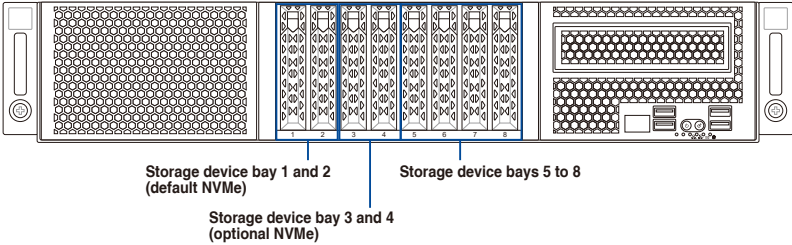
Support the DIMM lightly with your fingers when pressing the retaining clips. The DIMM might get damaged when it flips out with extra force.

---

4. Replace the rear chassis cover. For more information, refer to the **Chassis cover** section.

## 2.4 Storage devices

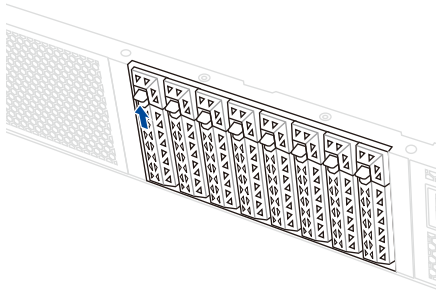
The system supports eight (8) 2.5" hot-swap SATA/SAS/NVMe storage devices (up to 4 x NVMe/SAS/SATA + 4 x SAS/SATA). The storage device installed on the storage device tray connects to the motherboard SATA/SAS/NVMe ports via the SATA/SAS/NVMe backplane.



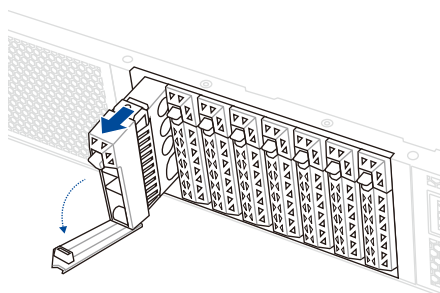
- The default storage device bays to install NVMe drives are storage device bays 1 and 2.
- Support for NVMe drives for storage device bays 3 and 4 is optional, please refer to the **Reconnecting the cable for 4 NVMe configuration** section before installing a NVMe drive to storage device bays 3 and 4.

### 2.4.1 To install a 2.5" hot-swap SATA/SAS/NVMe storage device

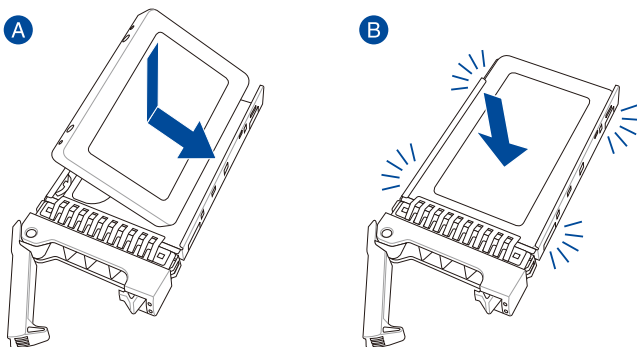
1. Press the spring lock to release the tray lever and to partially eject the tray from the bay.



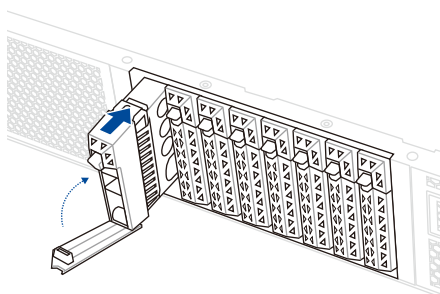
2. Firmly hold the tray lever and carefully pull the drive tray out of the bay.



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.

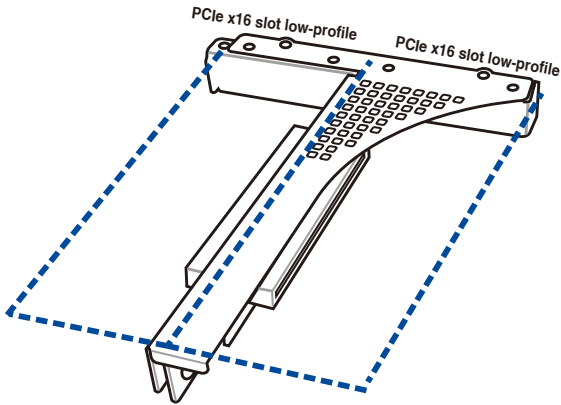
## 2.5 Expansion slots



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.

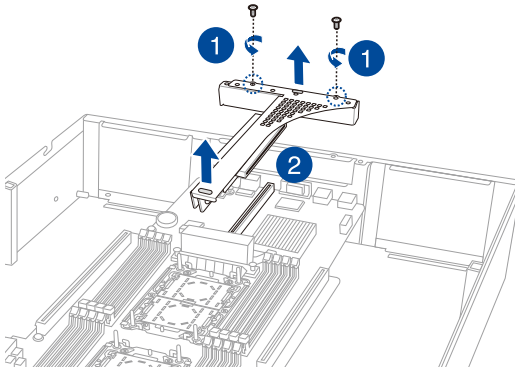
### 2.5.1 The PCI Express riser card

The onboard PCI Express slot on the motherboard comes pre-installed with a riser card that supports two x16 slot (x16 Gen4 link) for installing PCIe x16 low profile cards.

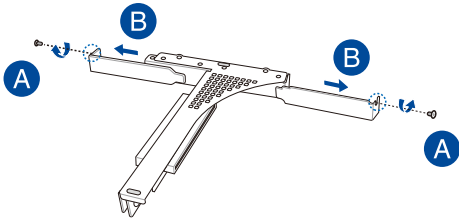


To install PCIe expansion cards to the riser card:

1. Remove the two (2) screws that secure the riser card to the chassis.
2. Firmly hold the riser card then pull it up to detach it from the PCI Express x32 slot on the motherboard.



3. Remove the two (2) screws from the metal brackets on the riser card (A), then remove the metal brackets from the riser card (B).

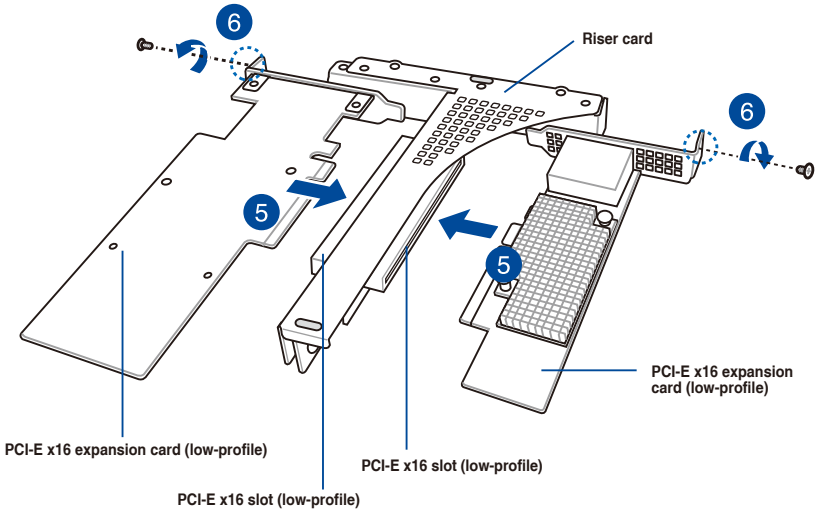


4. Prepare the expansion cards.



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 cards to the PCIe slot connectors on the riser card as shown.
6. Secure the expansion cards with the screws removed earlier.



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

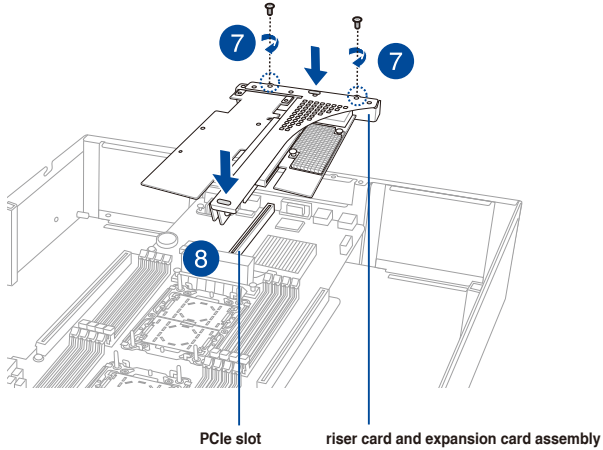


---

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

---

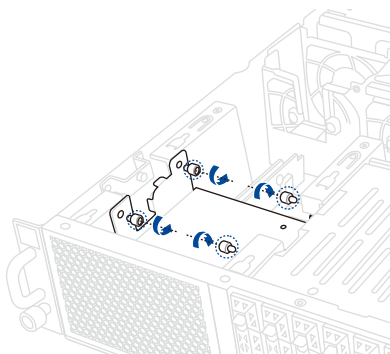
8. Secure the riser card with the two (2) screws that you removed earlier in step 1.



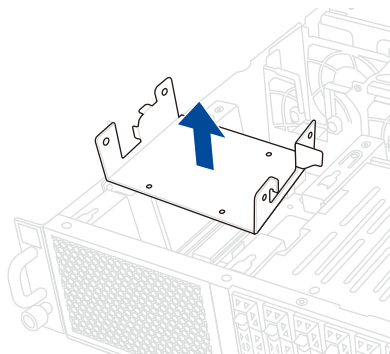
## 2.5.2 Installing an ASUS PIKE II card

You may install an ASUS PIKE II card to the internal SAS/HBA/Storage bracket located in the front of the system.

1. Remove the four (4) thumbscrews from the Cache Vault Power Module clip holder located on the left of the front side of the chassis.

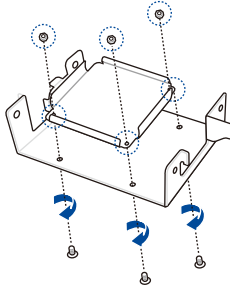


2. Lift and remove the Cache Vault Power Module clip holder from the chassis.

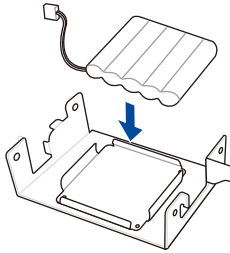




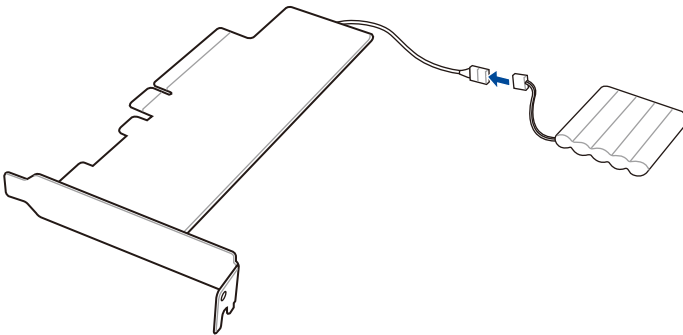
- Align the three screw holes on the Cache Vault Power Module clip to the three screw holes on the Cache Vault Power Module clip holder, then secure the clip with the bundled three (3) screws and three (3) bundled nuts.



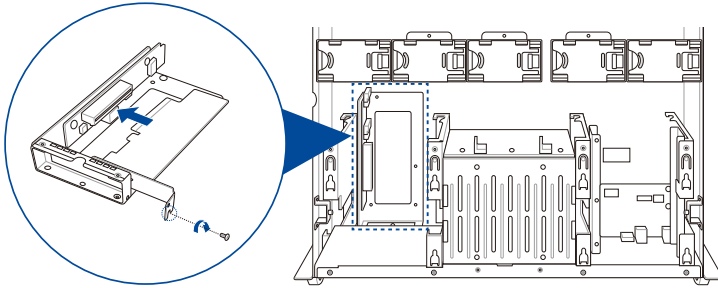
- Align and install the Cache Vault Power Module into the Cache Vault Power Module clip.



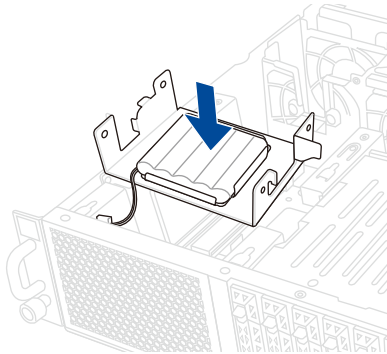
- Connect the cable from the Cache Vault Power Module to the cable from the Cache Vault Flash Module on the ASUS PIKE II card.



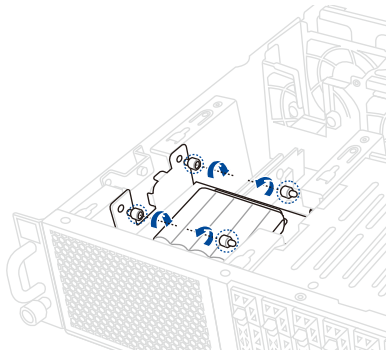
6. Insert the ASUS PIKE II card into the internal SAS/HBA/Storage bracket, then secure it with a screw.



7. Align the Cache Vault Power Module clip holder to the screw holes in the chassis, then replace the Cache Vault Power Module clip holder into the chassis.



8. Secure the Cache Vault Power Module clip holder using the four (4) thumbscrews removed previously.



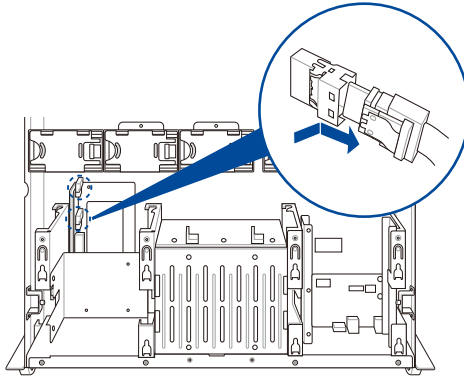
### 2.5.3 Reconnecting the cable to the M.2 expansion board (only for SKU-3)

You may reconnect the cables to enable the M.2 expansion board located in the front of the system.

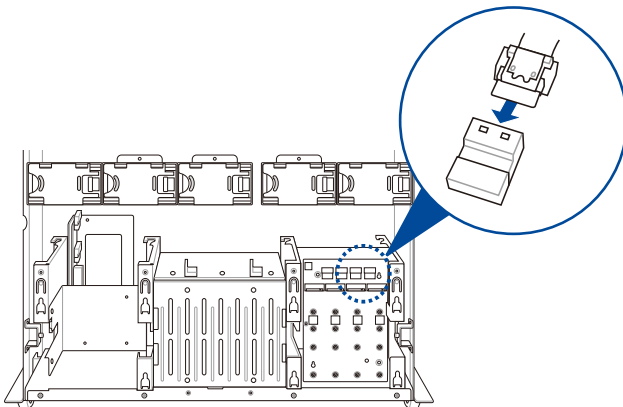


The cables are connected by default if your system package comes with the M.2 expansion board pre-installed.

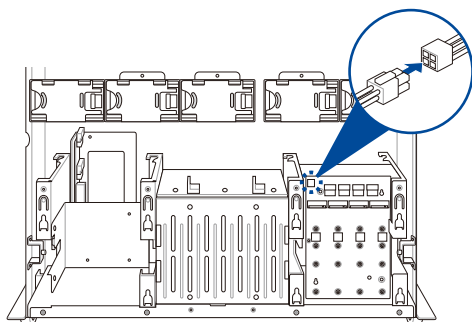
1. (optional) Remove the two (2) slimline SAS cables from the internal riser board for PCIe slot, if your system comes with the slimline SAS cables connected.



2. Connect the two (2) slimline SAS cables removed from the internal riser board for PCIe slot to your M.2 expansion board.



3. Connect the black 4-pin power connector to the 4-pin power connector on the M.2 expansion board.

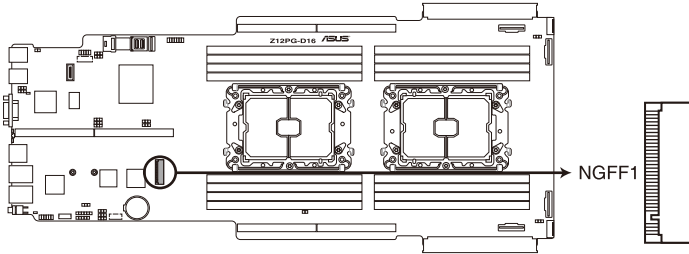


## 2.5.4 Installing an M.2 (NGFF) card

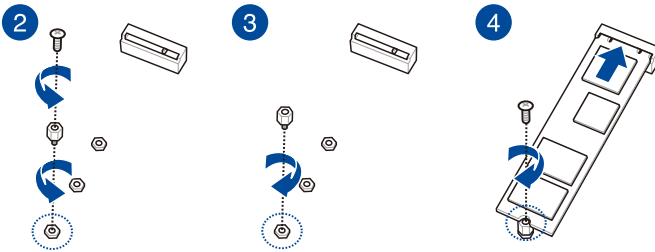
You may install an M.2 card (supports up to 2280) to the onboard M.2 (NGFF) slot on the motherboard.

1. Locate the M.2 connector (NGFF1) on the motherboard.

### Z12PG-D16 Serial port connector



2. Remove the screw on the stand screw.
3. Prepare the M.2 card, then align and insert the M.2 card into the M.2 connector (NGFF1).
4. Secure the M.2 card with the screw you removed in step 2.



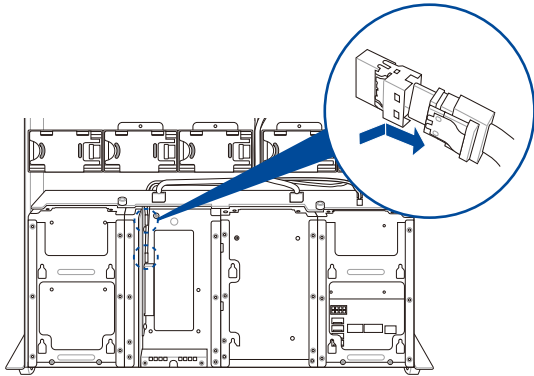
## 2.5.5 Reconnecting the cable to the OCP 3.0 slot baseboard (only for SKU-2)

You may reconnect the cables to enable the OCP3.0 slot baseboard located in the front of the system.

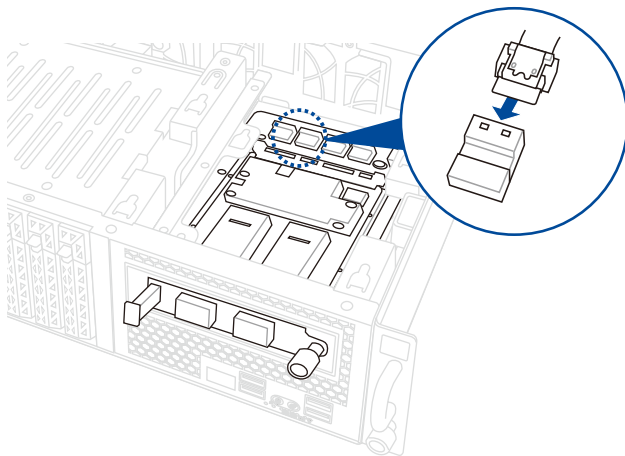


The cables are connected by default if your system package comes with the OCP3.0 slot baseboard pre-installed.

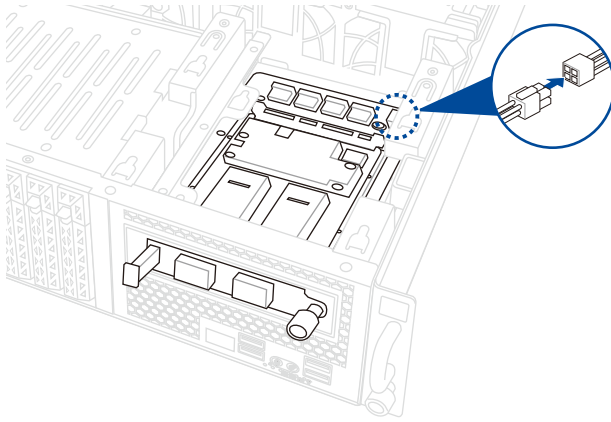
1. (optional) Remove the two (2) slimline SAS cables from the internal riser board for PCIe slot, if your system comes with the slimline SAS cables connected.



2. Connect two (2) slimline SAS cables to the two connectors to the left on your OCP3.0 slot baseboard.



3. Connect the white 4-pin power connector to the 4-pin power connector on the OCP3.0 slot baseboard.



## 2.5.6 (optional) Installing the PFR module

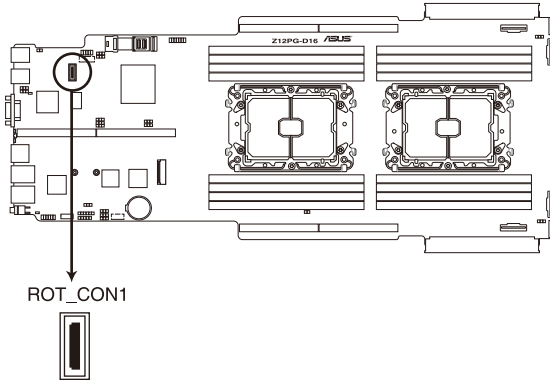
The optional PFR module will come pre-installed on your system and is connected to the PFR module connector on your motherboard.



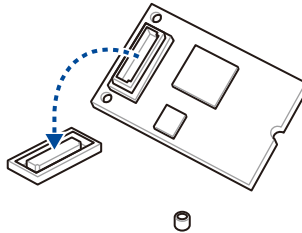
- The illustration below is for reference only.
- For more information or assistance, please refer to [www.asus.com](http://www.asus.com).

1. Locate the PFR module connector on your motherboard.

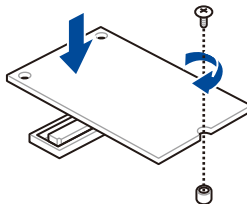
### Z12PG-D16 ROT\_CON1 connector



2. Align and connect the PFR module to the PFR module connector.



3. Push the PFR module down so that it is seated securely on the PFR module connector, then secure it using a screw.





## 2.5.7 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 the **BIOS Setup** chapter 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

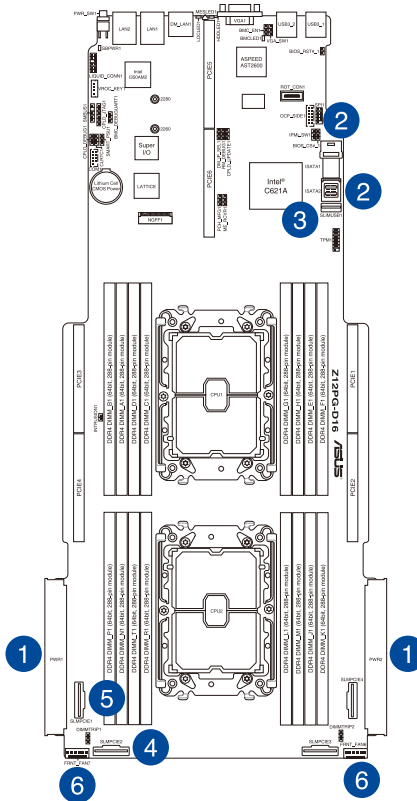
IRQ	Priority	Standard function
0	1	System Timer
1	2	Keyboard Controller
2	-	Programmable Interrupt
3*	11	Communications Port (COM2)
4*	12	Communications Port (COM1)
5*	13	--
6	14	Floppy Disk Controller
7*	15	--
8	3	System CMOS/Real Time Clock
9*	4	ACPI Mode when used
10*	5	IRQ Holder for PCI Steering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

## 2.6 Cable connections



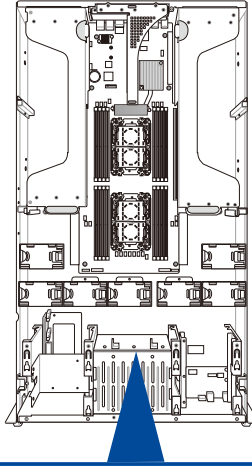
- The bundled system cables are pre-connected before shipment. You do not need to disconnect these cables unless you remove the pre-installed components to install additional devices.
- If you need to remove pre-connected system cables please ensure to remove the cable organizer metal cover beforehand.
- Refer to the **Motherboard Information** chapter for information on the connectors.



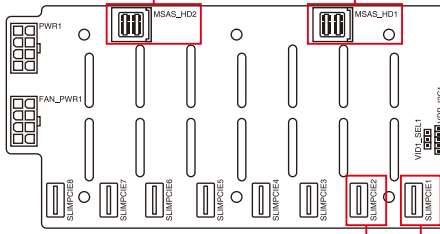
### Pre-connected system cables

1. Power connector (from the power distribution board to the motherboard)
2. ISATA connectors (from motherboard to SATA/SAS/U.2 backplane board)
3. Slim USB connector (from the motherboard to front I/O board)
4. SLIMPICIE2 connector (from motherboard to SATA/SAS/U.2 backplane board)
5. SLIMPICIE1 connector (from motherboard to internal riser board for PCIe slot)
6. System fan connectors (from motherboard FRNT\_FAN6, and FRNT\_FAN7 to system fans)

## 2.7 SATA/SAS backplane cabling



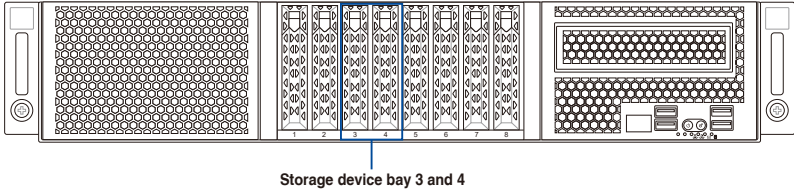
connect to ISATA1 and ISATA2 on the motherboard. With two mini-SAS HD cables connected, a total number of 8 SAS/SATA HDDs can be supported



connect to SLIMPCE2 on the motherboard to support 2 NVMe devices.

## 2.7.1 Reconnecting the cable for 4 NVMe configuration

Additional NVMe storage devices may be installed in storage device bays 3 and 4 as shown in the illustration below:



To reconnect the cable to support storage device bay 3 and 4:

1. Install the NVMe storage device to storage device bay 3 or 4.

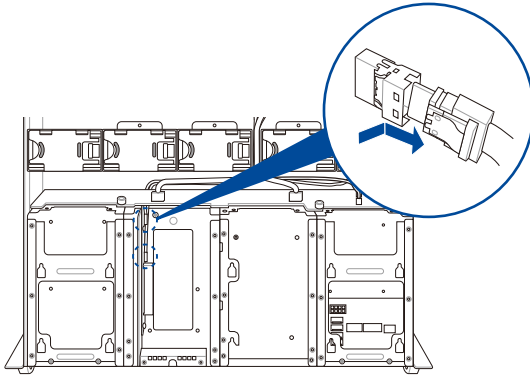


---

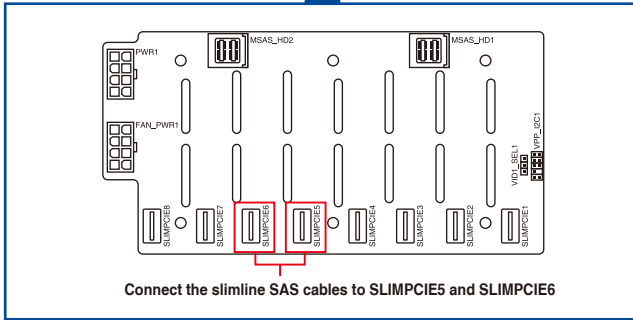
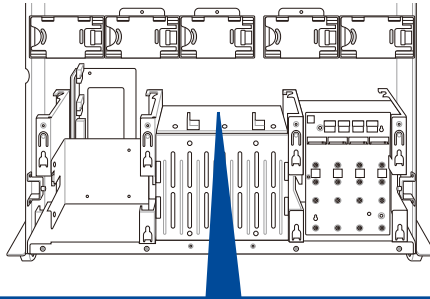
Refer to the **To install a 2.5" hot-swap SATA/SAS/NVMe storage device** section for the steps on installing a 2.5-inch drive to the storage device bay.

---

2. (optional) Remove the two (2) slimline SAS cables from the internal riser board for PCIe slot, if your system comes with the slimline SAS cables connected.



3. Connect two (2) slimline SAS cables to the SLIMPCIE5 and SLIMPCIE6 slots located on the backplane.



## 2.8 Removable/optional components

The following sections describe installation or removal instructions for the following removable/optional components:

1. Cable organizer metal cover
2. System fans
3. Redundant power supply units
4. GPU cards



---

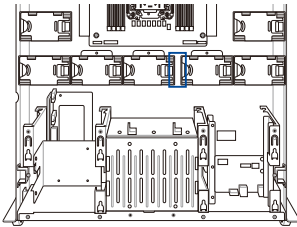
Ensure that the system is turned off before removing any components.

---

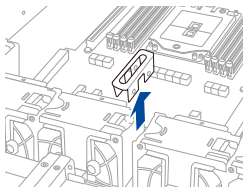
### 2.8.1 Cable organizer metal cover

When you need to organize the cables connecting from the rear to the front of the system, you may need to remove the cable organizer metal cover beforehand.

1. Locate the cable organizer metal cover in between the system fans.



2. Pull the cable organizer metal cover upwards to remove it from the system.

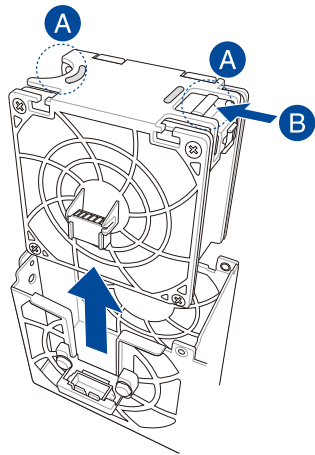


3. Once you have finished organizing the cables, ensure to replace the cable organizer metal cover.

## 2.8.2 System fans

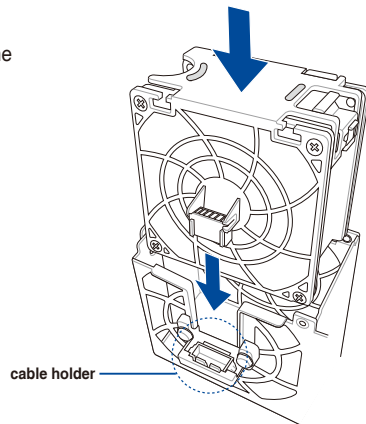
To uninstall the system fans:

1. Hold the system fan by the notches (A), then press the latch inwards (B) to release the system fan from the fan cage.
2. Lift the fan then set it aside.
3. Repeat steps 1 to 2 to uninstall the other system fans.



To reinstall the system fans:

1. Insert the fan into the fan cage. Ensure the fan connector is seated firmly within the cable holder.



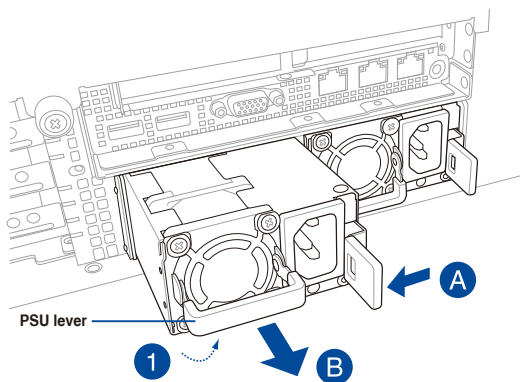
## 2.8.3 Redundant power supply units



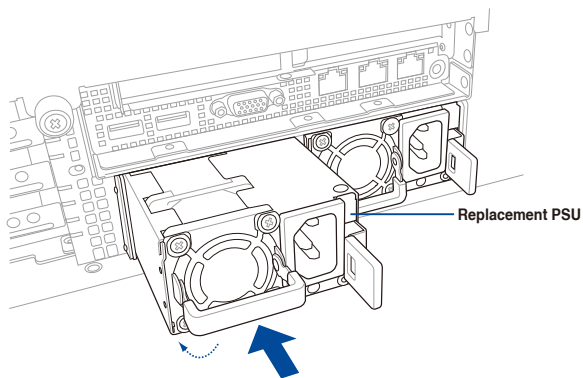
We recommend that you use both of your hands in performing the following steps.

To replace a power supply unit (PSU):

1. Lift up the PSU lever.
2. Hold the PSU lever, press the PSU latch (A) then carefully pull the PSU out of the system chassis (B).



3. Prepare the replacement PSU.
4. 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.

#### **1600W**

<b>Input Voltage</b>	<b>Max. Output Power (Watt) per PSU</b>
100V-127Vac, 13A, 50-60Hz	1000W
100V-127Vac, 12.9A, 47-63Hz	
200V-240Vac, 10A, 50-60Hz	1600W
200V-240Vac, 9.5A, 50-60Hz	
200V-240Vac, 9.5A, 47-63Hz	

#### **2200W**

<b>Input Voltage</b>	<b>Max. Output Power (Watt) per PSU</b>
100V-127Vac, 14A, 47-63Hz	1200W
200V-240Vac, 12.6A, 47-63Hz	2200W

- 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.

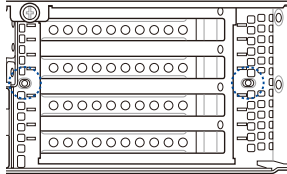


- Always use PSUs with the same watt and power rating. Combining PSUs with different wattage (e.g. 1 x 1620 W + 1 x 2000 W) may yield unstable results and potential damage to your system.
- For a steady power input, use only the power cables that come with the server system package.

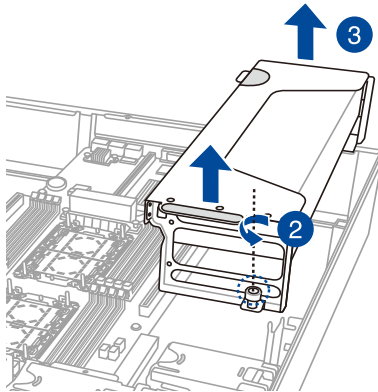
## 2.8.4 GPU cards

Follow the steps below to install a GPU card to the system.

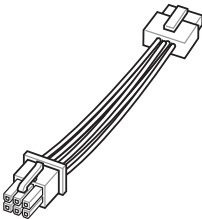
1. Locate and remove the two screws at the rear of the chassis.



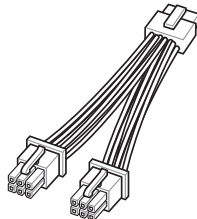
2. Locate and loosen the thumbscrew at the front of the GPU bracket.
3. Firmly hold and pull the GPU bracket upwards to detach it from the motherboard.



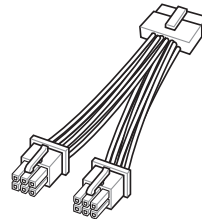
4. Prepare the appropriate GPU power cable depending on the type of GPU card.



**Tesla/AMD**  
8pin to 6pin power cable



**Quadro**  
8pin to 2x6pin power cable



**12VHPWR**  
12+4pin to 2x6pin power cable

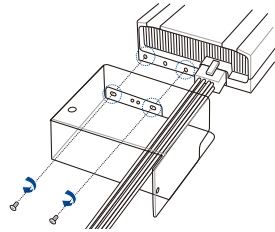
5. Install the air duct, if supported by the GPU card, and connect the GPU power cable.



The GPU air duct is designed and recommended for dual-slot GPU cards with a length of 10.5 inches.

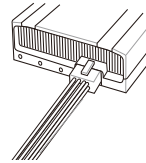
#### For GPU card installation with an air duct

Pass the power cable through the air duct and connect it to the GPU card, then secure the air duct to the GPU card with two screws.

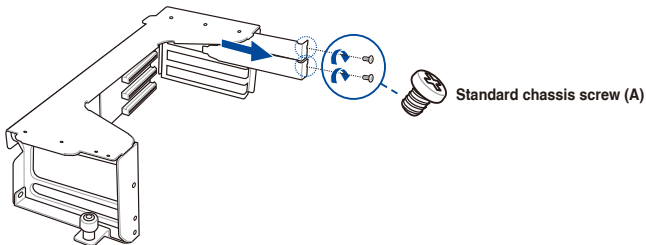


#### For GPU card installation without an air duct

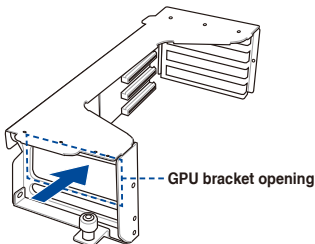
Connect the power cable to the GPU.





6. Place the GPU bracket on a flat and stable surface.
7. Remove the screws on the metal covers, then remove the metal covers.



8. Insert the GPU cables into the opening on the GPU bracket.



9. Align and insert the golden fingers of the GPU card into the card slot on the bracket and ensure that it is securely seated in the slot.
10. Secure the GPU card and air duct assembly to the GPU bracket.

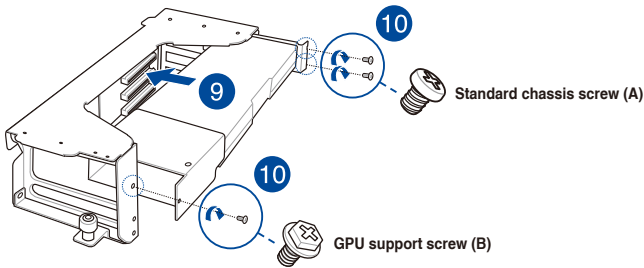
	Standard chassis screw (A)	#6-32 X L 4.2 OD 6mm	6.0±0.5 kgf-cm
	GPU support screw (B)	#6-32 X L 4.76 OD 8mm	6.0±0.5 kgf-cm



The GPU support screws are bundled in the accessory bag. Contact your retailer if any screws are missing.

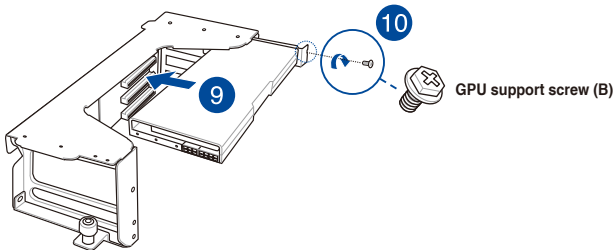
### For GPU card installation with an air duct

Secure the GPU card to the GPU bracket with two standard chassis screws, then secure the air duct using one GPU support screw.



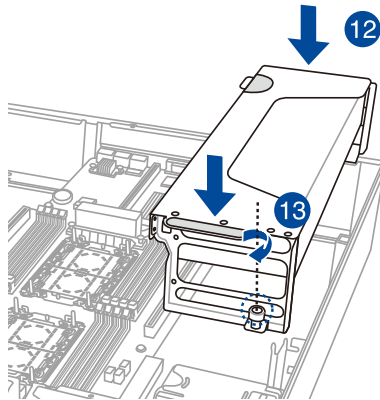
### For GPU card installation without an air duct

Secure the GPU card to the GPU bracket with one or two GPU support screws depending on the type of GPU card.

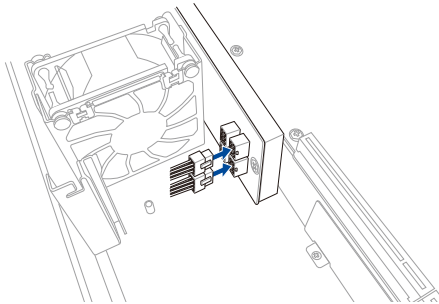


11. Repeat steps 4 to 10 if you need to install an additional GPU card to the bracket.

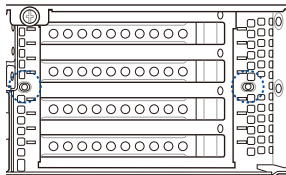
- Align and insert the golden fingers of the GPU bracket into the card slot on the motherboard and ensure that it is securely seated in the slot.
- Secure the thumbscrew at the front of the GPU bracket.



- Connect the other end of the GPU power cable to an available 6-pin power connector in front of the GPU bracket.



- Secure the GPU bracket to the server chassis with two screws.



## 2.9 Rail Kit Options

This server system supports the rail kit options listed below. For more information on rail kit installation, refer to corresponding documentation on the ASUS support site or on the official product site for this server system.



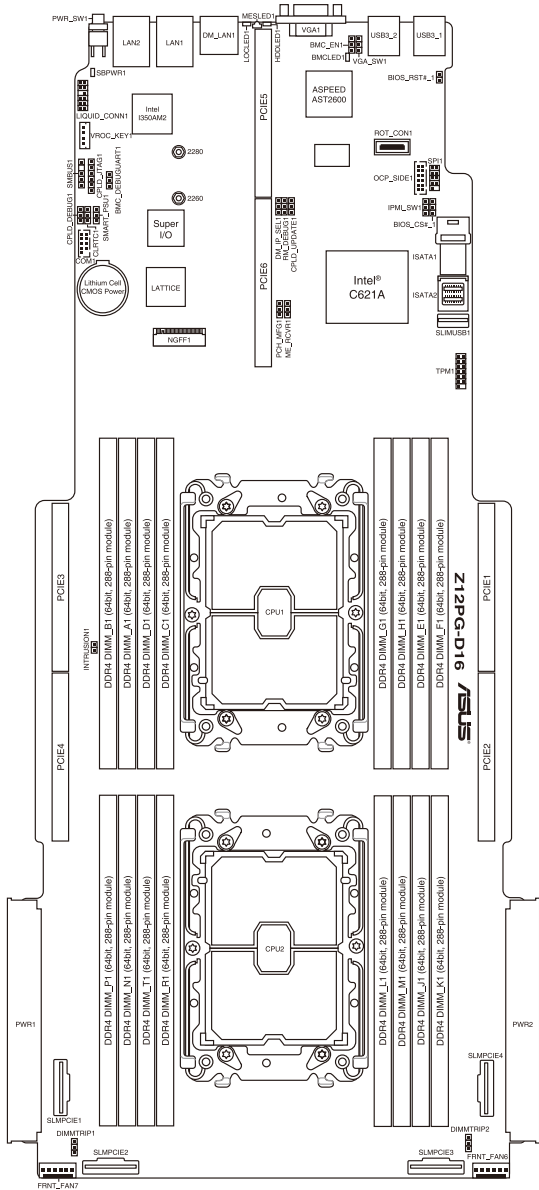
- 
- We strongly recommend that at least two able-bodied persons perform the installation of the rail kit.
  - We recommend the use of an appropriate lifting tool or device, if necessary.
- 
- 1m half extension ball bearing rail kit
  - 1.2m half extension ball bearing rail kit

# 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.

# 3

# 3.1 ASUS Z12PG-D16 Motherboard layout





## Layout contents

Jumpers	Page
1. Clear RTC RAM (3-pin CLRTC1)	3-4
2. VGA controller setting (3-pin VGA_SW1)	3-5
3. Baseboard Management Controller setting (3-pin BMC_EN1)	3-5
4. DMLAN setting (3-pin DM_IP_SEL1)	3-6
5. IPMI SW setting (3-pin IPMI_SW1)	3-6
6. Smart Ride Through jumper (3-pin SMART_PSU1)	3-7
7. DDR4 Thermal Event jumper (3-pin DIMMTRIP1-2)	3-7
8. ME Firmware Force Recovery jumper (3-pin ME_RCVR1)	3-8
9. PCH_MFG1 jumper (3-pin ME_RCVR1)	3-8

Internal connectors	Page
1. Mini-SAS HD connector (ISATA1-2)	3-9
2. Slim PCIe connectors (SLIMPCIE1-4)	3-9
3. USB 3.2 Gen 1 connectors (SLIMUSB1)	3-10
4. Chassis Intrusion (2-pin INTRUSION1)	3-10
5. Front fan connectors (6-pin FRNT_FAN6-7)	3-11
6. Serial port connector (10-1 pin COM1)	3-12
7. TPM connector (13-1 pin TPM1)	3-12
8. M.2 connector (NGFF1)	3-13
9. Power connectors (PWR1-2)	3-13
10. OCP3.0 Sideband Signal connector (12-pin OCP_SIDE1)	3-14
11. BMC Debug UART connector (3-pin BMC_DEBUGUART1)	3-14
12. CPLD JTAG connector (6-pin CPLD_JTAG1)	3-15
13. Liquid connector (12-1 pin LIQUID_CONN1)	3-15
14. System Management Bus connector (5-1 pin SMBUS1)	3-16
15. VROC Key connector (5-pin VROC_KEY1)	3-16

Onboard LEDs	Page
1. Standby Power LED (SBPWR1)	3-17
2. Baseboard Management Controller LED (BMCLED1)	3-17
3. Hard disk activity LED (HDDLED1)	3-18
4. Message LED (MESLED1)	3-18
5. Location LED (LOCLED1)	3-19

## 3.2 Jumpers

### 1. Clear RTC RAM (CLRRTC1)

This jumper allows you to clear the CMOS memory system setup parameters by erasing the CMOS Real Time Clock (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.

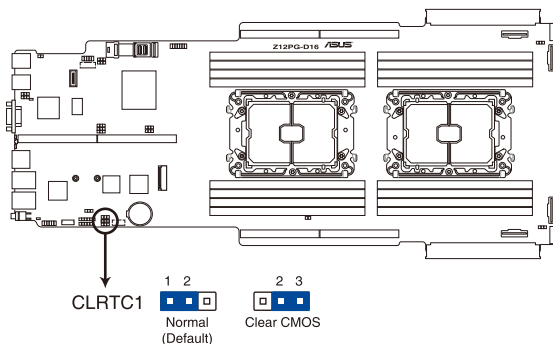


Except when clearing the RTC RAM, never remove the cap on CLRRTC jumper default position. Removing the cap will cause system boot failure!



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.

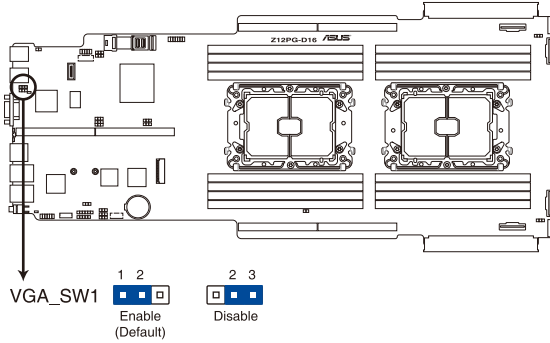
### Z12PG-D16 Clear RTC RAM



## 2. VGA controller setting (3-pin VGA\_SW1)

This jumper allows you to enable or disable the onboard VGA controller. Set to pins 1–2 to activate the VGA feature.

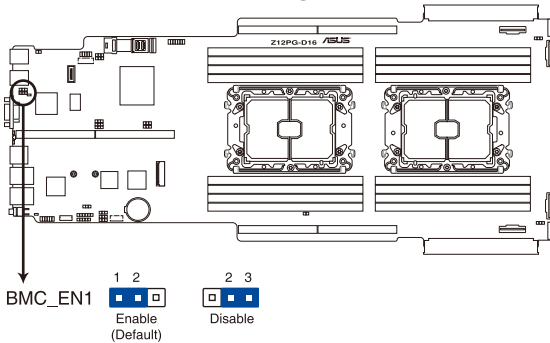
### Z12PG-D16 VGA controller setting



## 3. Baseboard Management Controller setting (3-pin BMC\_EN1)

This jumper allows you to enable (default) or disable on-board BMC. Ensure to set this BMC jumper to enabled to avoid system fan control and hardware monitor error.

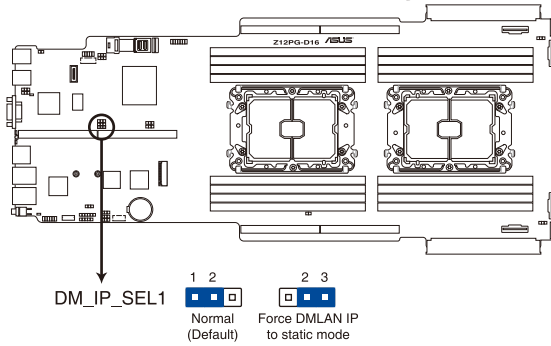
### Z12PG-D16 BMC setting



**4. DMLAN setting (3-pin DM\_IP\_SEL1)**

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

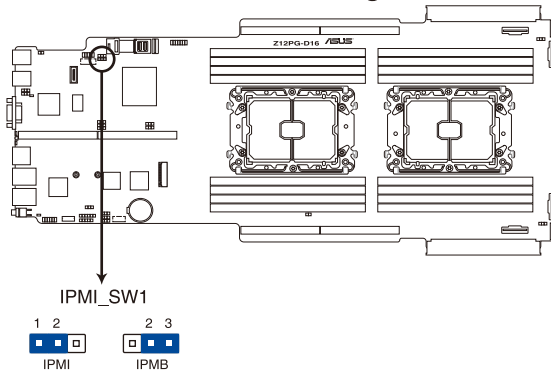
**Z12PG-D16 DM\_IP\_SEL1 setting**



**5. IPMI SW setting (3-pin IPMI\_SW1)**

This jumper allows you to select which protocol in the GPU sensor to function.

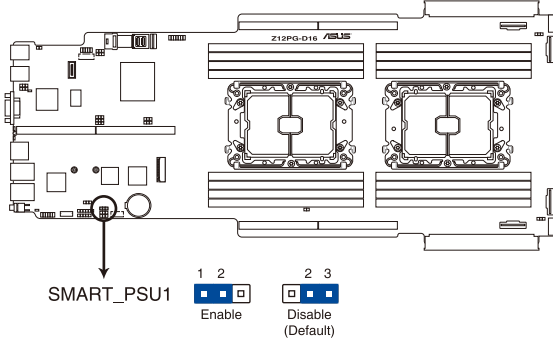
**Z12PG-D16 IPMI\_SW1 setting**



6. **Smart Ride Through jumper (3-pin SMART\_PSU1)**

Set to pins 1-2 to enable the Smart Ride Through (SmaRT) feature to allow uninterrupted operation of the system during an AC loss event.

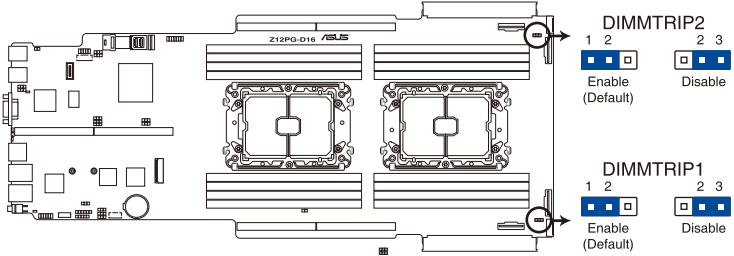
**Z12PG-D16 PMBus 1.2 PSU setting**



7. **DDR4 Thermal Event jumper (3-pin DIMMTRIP1-2)**

Set to pins 1-2 to enable DDR4 DIMM thermal sensing event.

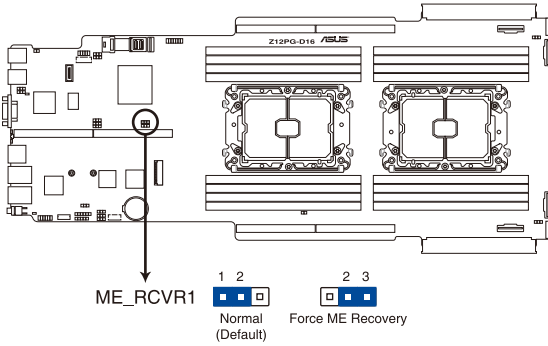
**Z12PG-D16 Thermaltrip setting**



**8. ME Firmware Force Recovery jumper (3-pin ME\_RCVR1)**

Set to pins 2-3 to force Intel® Management Engine (ME) boot from recovery mode when the ME becomes corrupted.

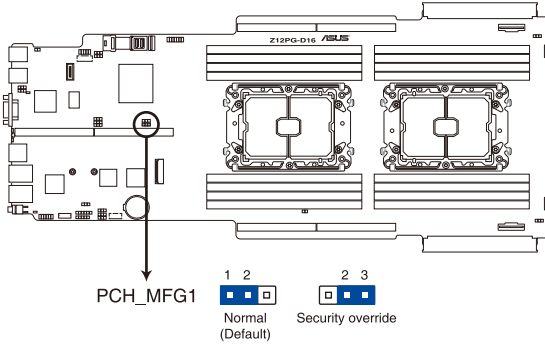
**Z12PG-D16 ME recovery setting**



**9. PCH\_MFG1 jumper (3-pin ME\_RCVR1)**

The PCH\_MFG1 jumper allows you to update the BIOS ME block.

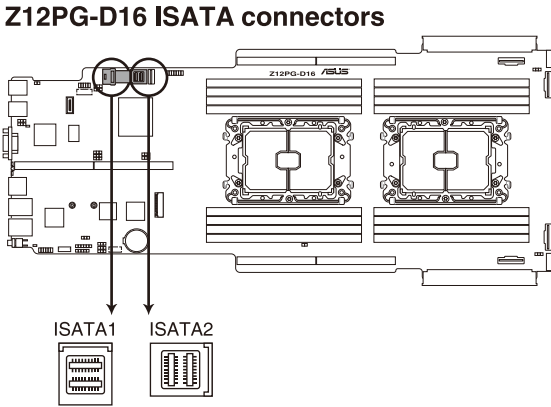
**Z12PG-D16 PCH\_MFG1 setting**



### 3.3 Internal connectors

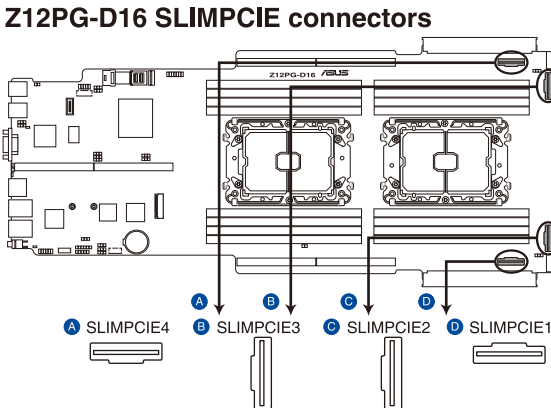
#### 1. Mini-SAS HD connector (ISATA1-2)

This motherboard comes with mini Serial Attached SCSI (SAS) HD connectors, the storage technology that supports Serial ATA. Each connector supports up to four devices.



#### 2. Slim PCIe connectors (SLIMPCIE1-4)

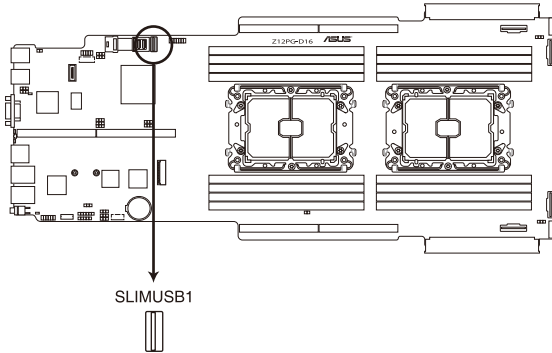
Connects the PCIe signal to the front riser card or NVMe port on the backplane.



**3. USB 3.2 Gen 1 connectors (SLIMUSB1)**

Connect a compatible USB module cable to the SLIMUSB1 connector, and then install the module to a slot opening at the back or front of the system chassis. You can enjoy all the benefits of USB 3.2 Gen 1 including faster data transfer speeds of up to 5 Gbps, faster charging time for USB-chargeable devices, optimized power efficiency, and backward compatibility with USB 2.0. (SLIMUSB1 connector is used for the front USB panel by default).

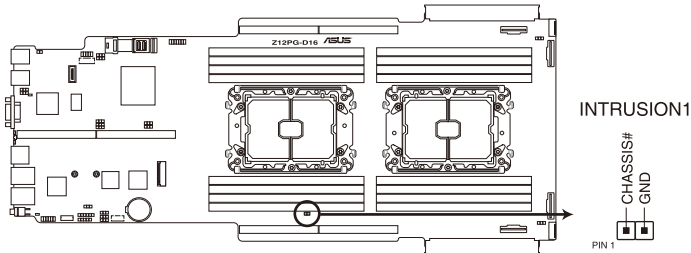
**Z12PG-D16 SLIMUSB connector**



**4. Chassis Intrusion (2-pin INTRUSION1)**

These leads are for the intrusion detection feature for chassis with intrusion sensor or microswitch. When you remove any chassis component, the sensor triggers and sends a high level signal to these leads to record a chassis intrusion event. The default setting is to short the CHASSIS# and the GND pin by a jumper cap to disable the function.

**Z12PG-D16 Chassis Intrusion connector**





## 5. Front fan connectors (6-pin FRNT\_FAN6-7)

The fan connectors support cooling fans of 3.30 A – 3.95 A (47.4 W max.) Connect the fan cables to the fan connectors on the motherboard, ensuring that the black wire of each cable matches the ground pin of the connector.

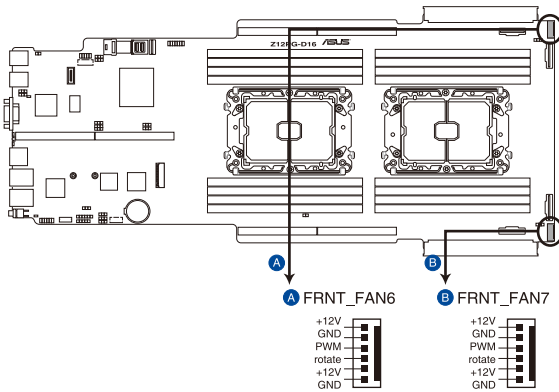


- DO NOT forget to connect the fan cables to the fan connectors. Insufficient air flow inside the system may damage the motherboard components.
- These are not jumpers! DO NOT place jumper caps on the fan connectors!



All fans feature the ASUS Smart Fan technology.

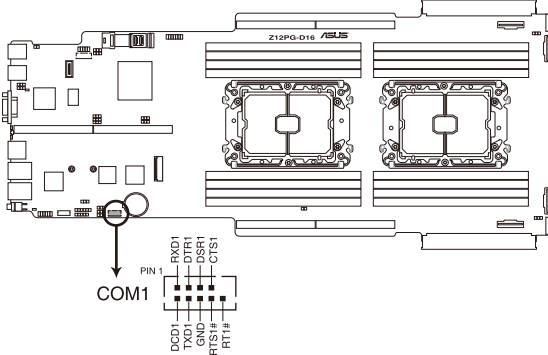
### Z12PG-D16 FAN connectors



**6. Serial port connector (10-1 pin COM1)**

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

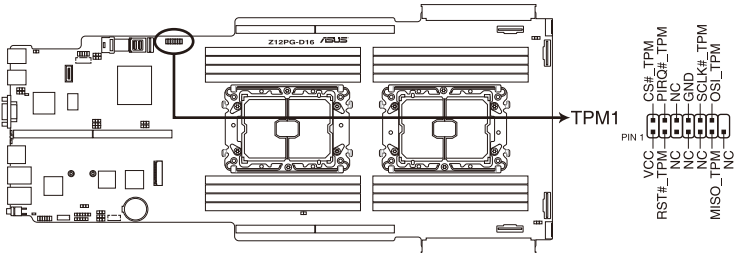
**Z12PG-D16 Serial port connector**



**7. TPM 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.

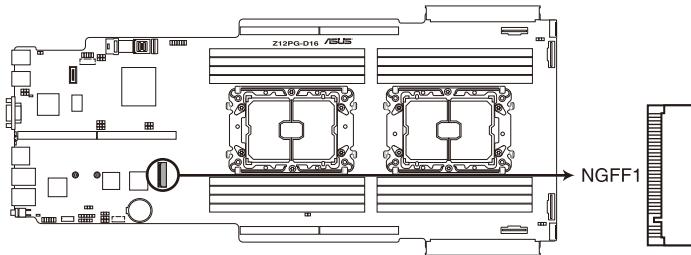
**Z12PG-D16 TPM connector**



## 8. M.2 connector (NGFF1)

This slot allows you to install M.2 devices.

### Z12PG-D16 M.2 connector



This connector supports type 2260 / 2280 devices.



The M.2 (NGFF) device is purchased separately

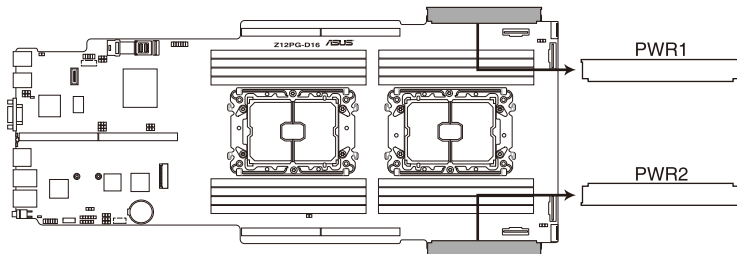
## 9. Power connectors (PWR1-2)

These connectors are for the power sharing boards. The power sharing boards are designed to fit these connectors in only one orientation. Find the proper orientation and push down firmly until the connectors completely fit.



- Use of a PSU with a higher power output is recommended when configuring a system with more power-consuming devices. The system may become unstable or may not boot up if the power is inadequate.
- Ensure that your power supply unit (PSU) can provide at least the minimum power required by your system.

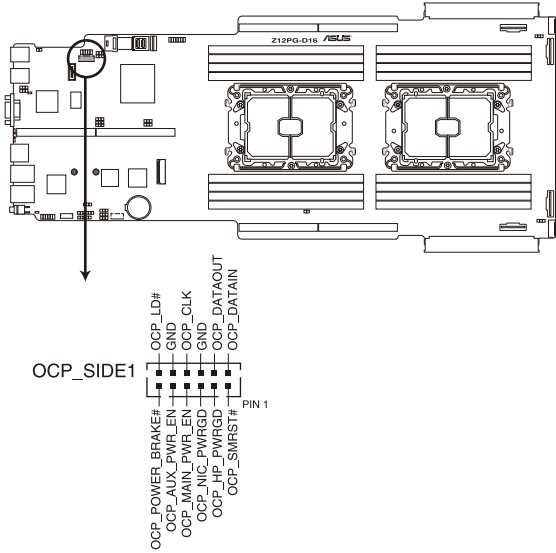
### Z12PG-D16 Power connectors



**10. OCP3.0 Sideband Signal connector (12-pin OCP\_SIDE1)**

This connector is for OCP3.0 sideband signal and allows you to connect an external OCP3.0 card to support additional features such as power brake and scan chain.

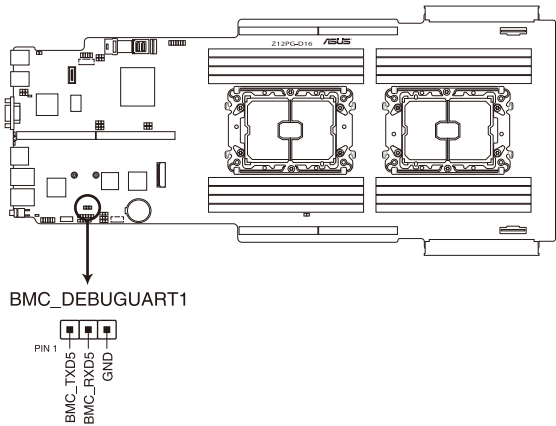
**Z12PG-D16 OCP\_SIDE connector**



**11. BMC Debug UART connector (3-pin BMC\_DEBUGUART1)**

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

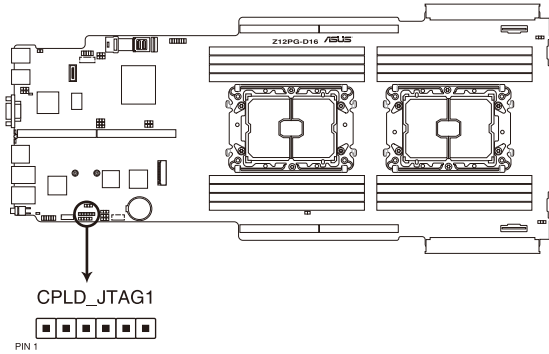
**Z12PG-D16 BMC\_DEBUGUART1 connector**



## 12. CPLD JTAG connector (6-pin CPLD\_JTAG1)

This connector is used for burning the CPLD JTAG.

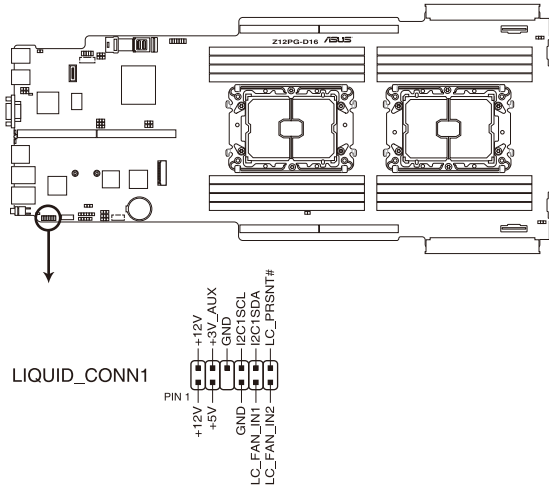
### Z12PG-D16 CPLD\_JTAG connector



## 13. Liquid connector (12-1 pin LIQUID\_CONN1)

This connector is used for detecting the pump speed of the water cooling system.

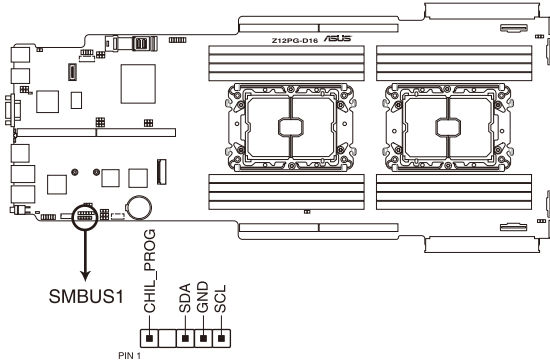
### Z12PG-D16 Liquid connector



**14. System Management Bus connector (5-1 pin SMBUS1)**

The System Management Bus (SMBus) connector allows you to connect SMBus devices. This connector is generally used for communication with the system and power management-related tasks.

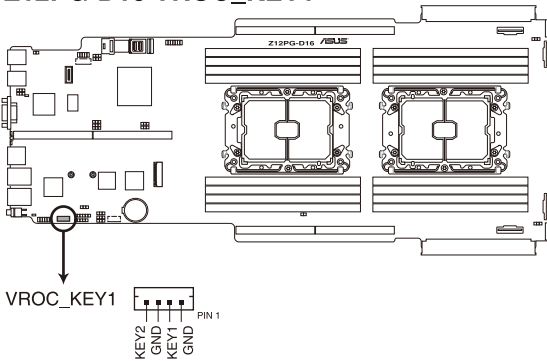
**Z12PG-D16 SMBUS connector**



**15. VROC Key connector (5-pin VROC\_KEY1)**

The VROC (Virtual RAID on CPU) Key connector allows you to connect a VROC hardware key to enable additional CPU RAID functions with Intel® CPU RSTe.

**Z12PG-D16 VROC\_KEY1**

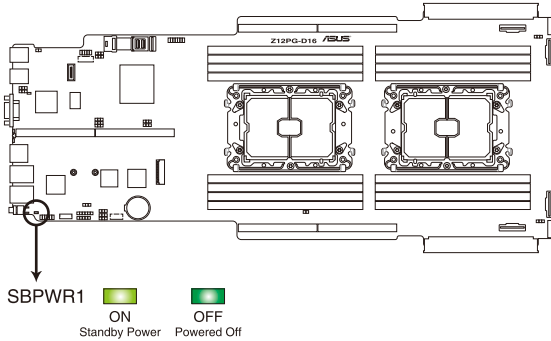


## 3.4 Onboard LEDs

### 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.

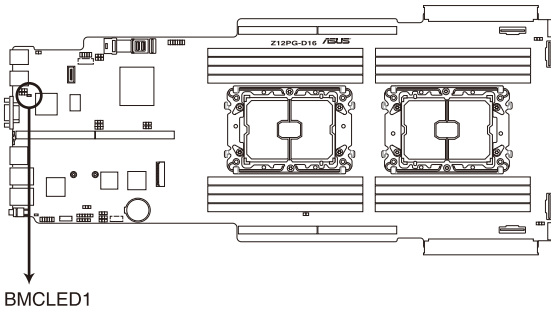
#### Z12PG-D16 Standby Power LED



### 2. Baseboard Management Controller LED (BMCLED1)

The BMC LED lights up to indicate that the on-board BMC is functional.

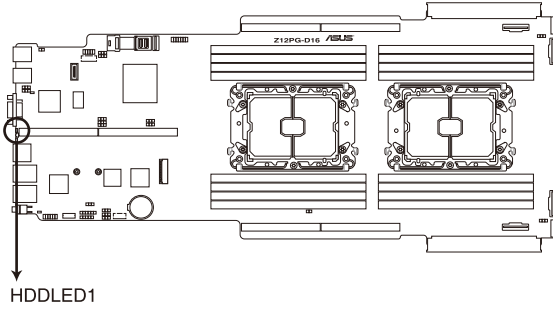
#### Z12PG-D16 BMC LED



**3. Hard disk activity LED (HDDLED1)**

This LED is for the storage devices connected to the onboard SATA, or SATA/SAS add-on card. The read or write activities of any device connected to the onboard SATA, or SATA/SAS add-on card causes the rear panel LED to light up.

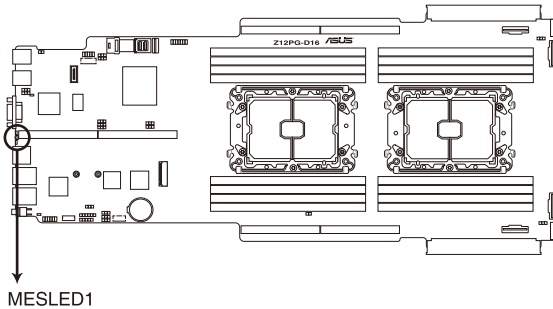
**Z12PG-D16 HDDLED1**



**4. Message LED (MESLED1)**

This onboard LED lights up to red when there is temperature warning or a BMC event log is generated.

**Z12PG-D16 MESLED1**

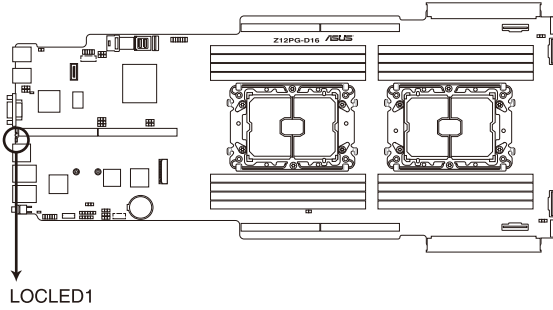




**5. Location LED (LOCLED1)**

This onboard LED lights up when the Location button on the server is pressed or when triggered by a system management software. The Location LED helps visually locate and quickly identify the server in error on a server rack.

**Z12PG-D16 Location LED**





# **BIOS Setup**

# 4

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

## 4.1 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.

---

### 4.1.1 **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](http://www.asus.com) to download the latest BIOS file.

---

## 4.1.2 ASUS EZ Flash Utility

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

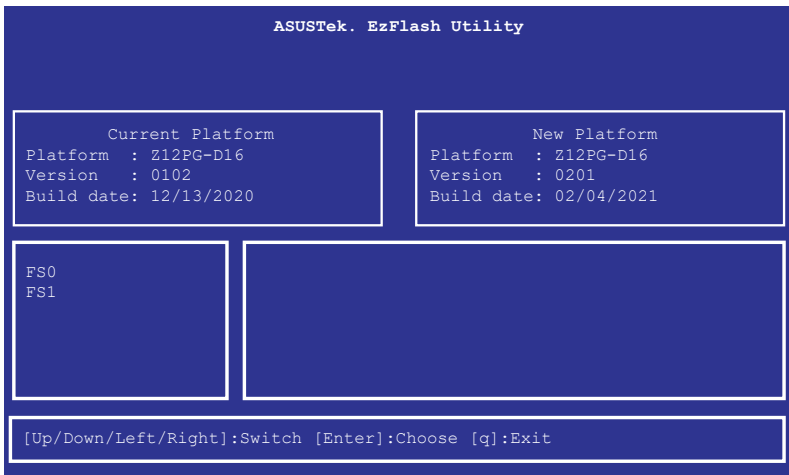
---

Before you start using this utility, download the latest BIOS from the ASUS website at [www.asus.com](http://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 **Start ASUS EzFlash**. Press <Enter>.



3. Press Left arrow key 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 Right arrow key 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 <F2> and select **Yes** to load the BIOS default settings.

### 4.1.3 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:

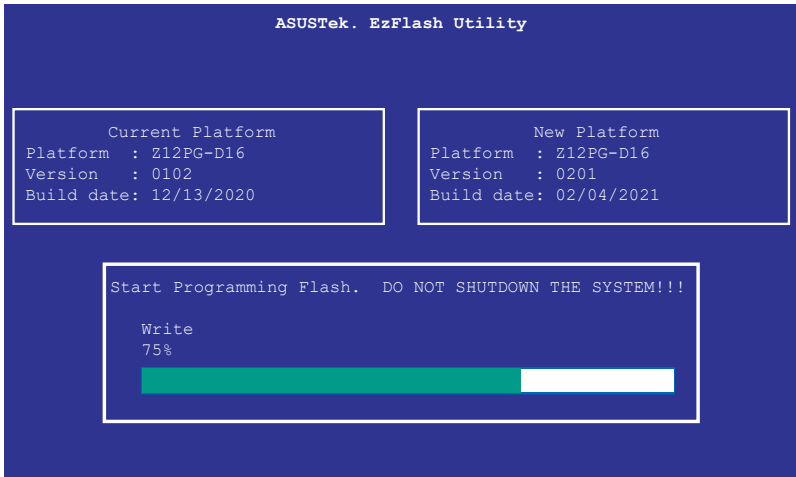
1. Visit the ASUS website at [www.asus.com](http://www.asus.com) and download the latest BIOS file for the motherboard. Save the BIOS file to a bootable USB flash disk drive.
2. Copy the BUPDATER utility (BUPDATER.exe) from the ASUS support website at [www.asus.com/support](http://www.asus.com/support) 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>.

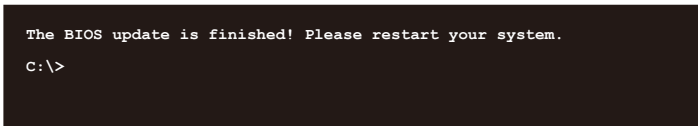
```
A:\>BUPDATER /i[file name].CAP
```

- 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!

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



## 4.2 BIOS setup program

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

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.

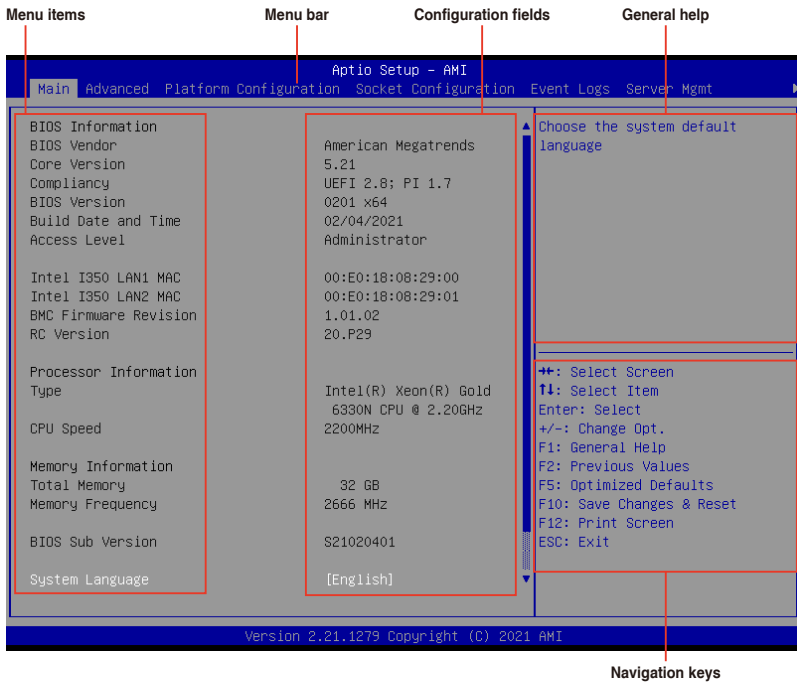
The Setup program is designed to make it as easy to use as possible. Being a menu-driven program, it lets you scroll through the various sub-menus and make your selections from the available options using the navigation keys.



- 
- 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](http://www.asus.com)) to download the latest BIOS file for this motherboard.
-



## 4.2.1 BIOS menu screen



## 4.2.2 Menu bar

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

- Main** For changing the basic system configuration
- Advanced** For changing the advanced system settings
- Platform Configuration** For configuring the platform settings
- Socket Configuration** For configuring 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.

## 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 (such as **Advanced**) on the menu bar have their respective menu items.

## 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>.

## 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.

## General help

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

## 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.

## Pop-up window

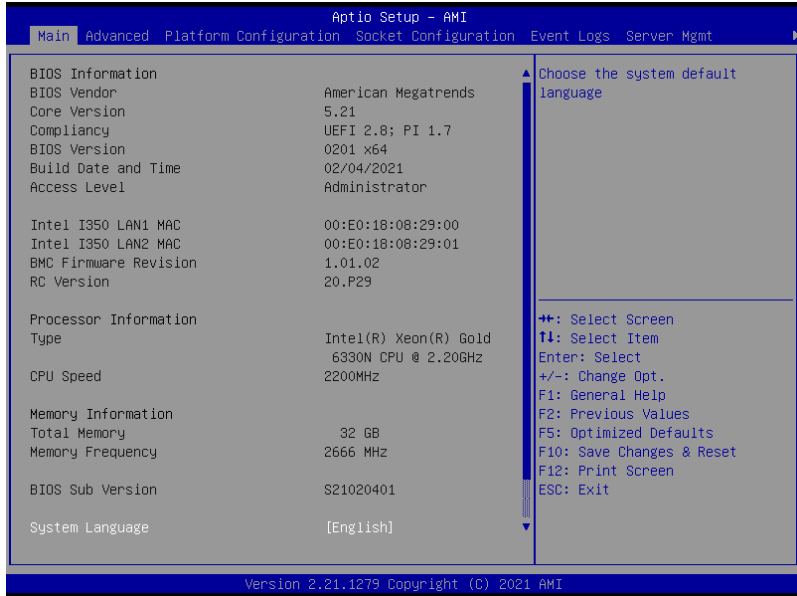
Select a menu item and press <Enter> to display a pop-up window with the configuration options for that item.

## 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.

## 4.3 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. Scroll using <Page Up> / <Page Down> keys to see more items.



### System Language

Allows you to set the system language.

### System Date [MM/DD/YYYY]

Allows you to set the system date.

### System Time [HH:MM:SS]

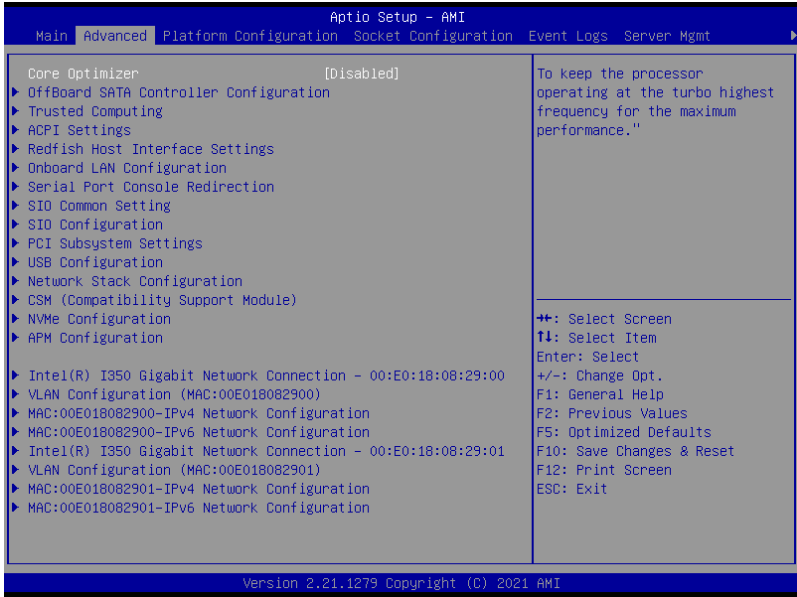
Allows you to set the system time.

## 4.4 Advanced menu

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



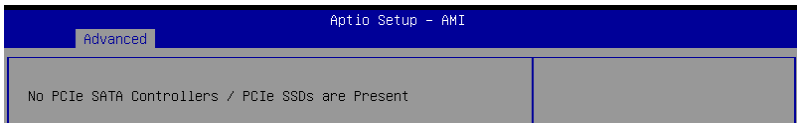
Take caution when changing the settings of the Advanced menu items. Incorrect field values can cause the system to malfunction.



### Core Optimizer [Disabled]

Allows you to enable or disable whether to keep the processor operating at the turbo highest frequency for maximum performance or not.  
Configuration options: [Disabled] [Enabled]

### 4.4.1 OffBoard SATA Controller Configuration



## 4.4.2 Trusted Computing

Advanced		Aptio Setup - AMI
Configuration		
Security Device Support	[Enable]	Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and
NO Security Device Found		Device. TCG EFI protocol and

### Security Device Support [Enable]

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

Configuration options: [Disable] [Enable]

## 4.4.3 ACPI Settings

Advanced		Aptio Setup - AMI
ACPI Settings		
Enable ACPI Auto Configuration	[Disabled]	Enables or Disables BIOS ACPI Auto Configuration.

### Enable ACPI Auto Configuration [Disabled]

Allows you to enable or disable the BIOS ACPI Auto Configuration.

Configuration options: [Disabled] [Enabled]

## 4.4.4 Redfish Host Interface Settings

Advanced		Aptio Setup - AMI
Redfish Host Interface Settings		
Redfish	[Disabled]	Enable/Disable AMI Redfish

### 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.

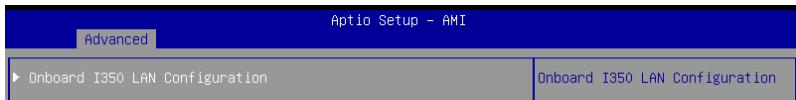
### IP Mask address

Allows you to enter the IP Mask address.

### IP Port

Allows you to enter the IP Port.

## 4.4.5 Onboard LAN Configuration



### Onboard I350 LAN Configuration

#### Intel I350 LAN1

##### LAN Enable [JumperState]

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



---

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

---

##### ROM Type [PXE]

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

#### Intel I350 LAN2

##### LAN Enable [JumperState]

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



---

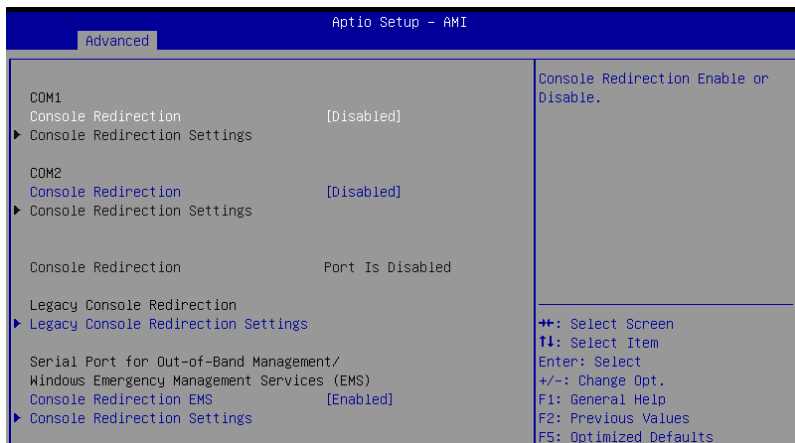
The following item appears only when **LAN Enable** is set to **[JumperState]**.

---

##### ROM Type [Disabled]

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

## 4.4.6 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 out-of-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.

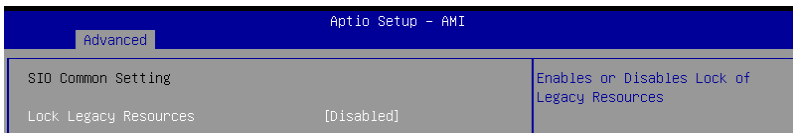
Configuration options: [9600] [19200] [57600] [115200]

#### 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]

## 4.4.7 SIO Common Setting

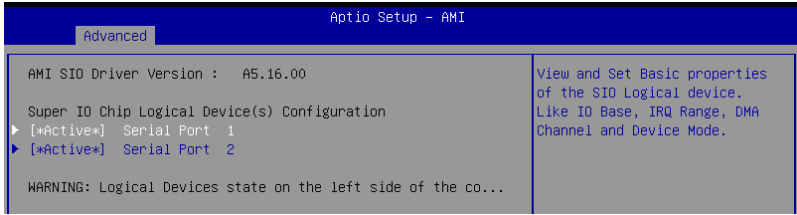


### Lock Legacy Resources [Disabled]

Allows you to enable or disable locking of Legacy Resources.

Configuration options: [Disabled] [Enabled]

## 4.4.8 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;]

## 4.4.9 PCI Subsystem Settings

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

Advanced		Aptio Setup - AMI
PCI Devices Common Settings:		Enables or Disables RT32 Image Loading.
Load RT32 Image	[Enabled]	
Above 4G Decoding	[Enabled]	
First VGA 4G Decode	[Auto]	
LAN Device 4G Decode	[Above_4G]	
Re-Size BAR Support	[Disabled]	
SR-IOV Support	[Enabled]	

### 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]

## 4.4.10 USB Configuration

Advanced		Aptio Setup - AMI	
USB Configuration		[Enabled]: Enables the Legacy USB support.	
USB Module Version	26	[Auto]: Automatically disables the Legacy USB support if USB devices are not connected.	
USB Controllers:		[Disabled]: USB devices are available only for EFI applications.	
1 XHCI			
USB Devices:			
1 Drive, 1 Keyboard, 1 Hub			
Legacy USB Support	[Enabled]		
XHCI Hand-off	[Enabled]		
USB Mass Storage Driver Support	[Enabled]		
Port 60/64 Emulation	[Enabled]		
Mass Storage Devices:		++: Select Screen	
JetFlashTranscend 4GB 8.07	[Auto]	! : Select Item	
		Enter: Select	

### 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]

### Mass Storage Devices:

Allows you to select the mass storage device emulation type for devices connected. **[Auto]** enumerates devices according to their media format. Optical drives are emulated as **[CD-ROM]**, drives with no media will be emulated according to a drive type.

Configuration options: [Auto] [Floppy] [Forced FDD] [Hard Disk] [CD-ROM]

## 4.4.11 Network Stack Configuration

Aptio Setup - AMI		
Advanced		
Network Stack	[Enabled]	Enable/Disable UEFI Network Stack
Ipv4 PXE Support	[Disabled]	
IPv4 HTTP Support	[Disabled]	
Ipv6 PXE Support	[Disabled]	
IPv6 HTTP Support	[Disabled]	
PXE boot wait time	0	
Media detect count	1	

### 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.

## 4.4.12 CSM (Compatibility Support Module)

Advanced		Aptio Setup - AMI
Compatibility Support Module Configuration		CSM(compatibility support module)
Launch CSM	[Disabled]	[Enabled]: For a better compatibility, enable the CSM

### 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.

#### 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]

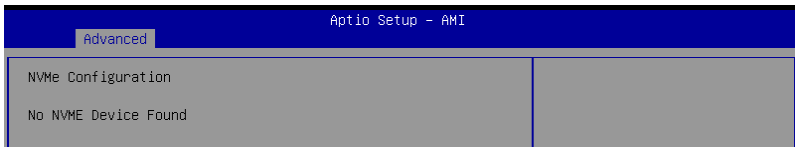
### Boot from PCI-E/PCI Expansion Devices [UEFI only]

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]

## 4.4.13 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.

## 4.4.14 APM Configuration

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

Aptio Setup - AMI		
Advanced		
Restore AC Power Loss	[Last State]	Restore On AC Power Loss
Power On By PCI-E/PCI	[Disabled]	
Power On By RTC	[Disabled]	

### 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]

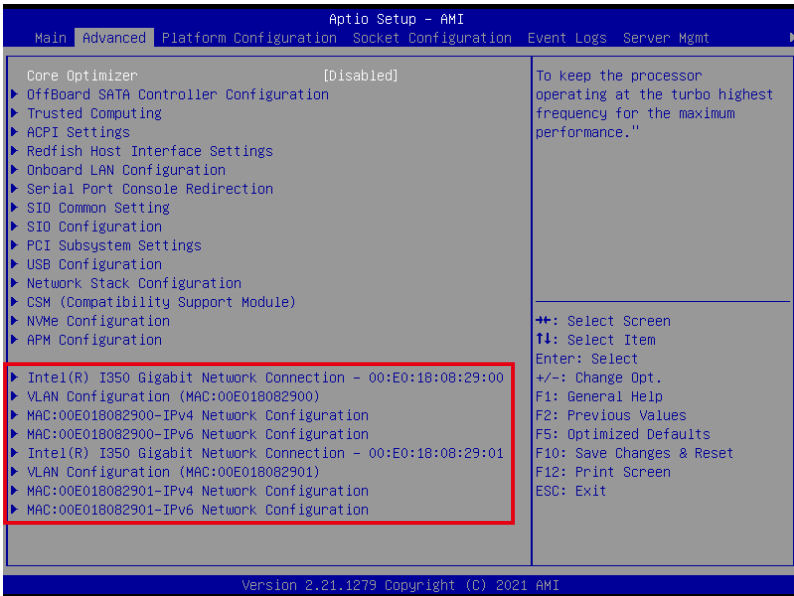
[Disabled] Disables RTC to generate a wake event.

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



## 4.4.15 Third-party UEFI driver configurations

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

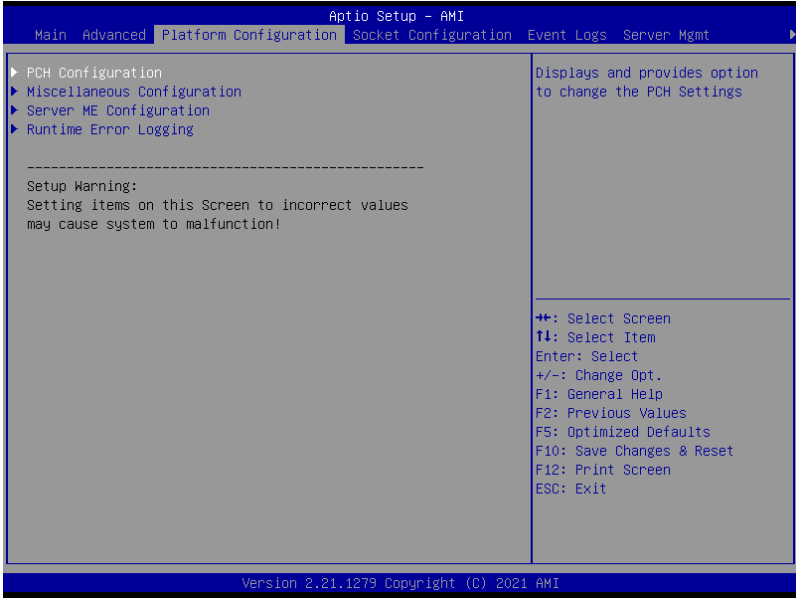


## 4.5 Platform Configuration menu

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!



### 4.5.1 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 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]**

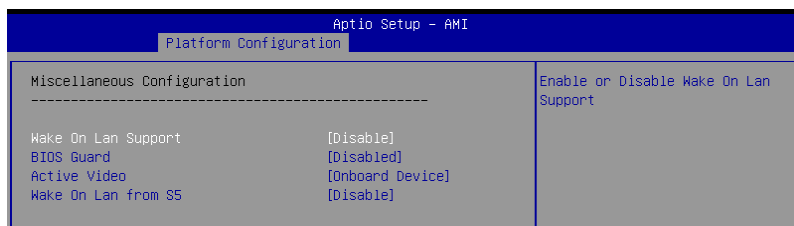
Allows you to identify the SATA port connected to Solid State Drive or Hard Disk Drive.  
Configuration options: [AHCI] [RAID]

### **sSATA Port 0-5**

#### **Hot Plug [Disable]**

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

## **4.5.2 Miscellaneous Configuration**



### **Wake on LAN Support [Disable]**

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

### **BIOS Guard [Disabled]**

Allows you to enable or disable BIOS Guard Platform Protection Technology.  
Configuration options: [Disabled] [Enabled]

### Active Video [Onboard Device]

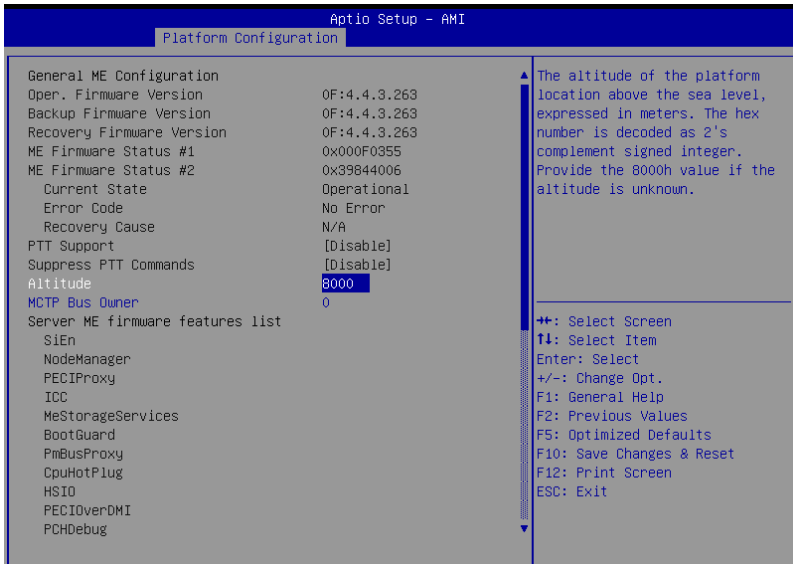
Allows you to select the active video type.  
Configuration options: [Auto] [Onboard Device] [PCIe Device]

### Wake on LAN from S5 [Disable]

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

## 4.5.3 Server ME Configuration

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



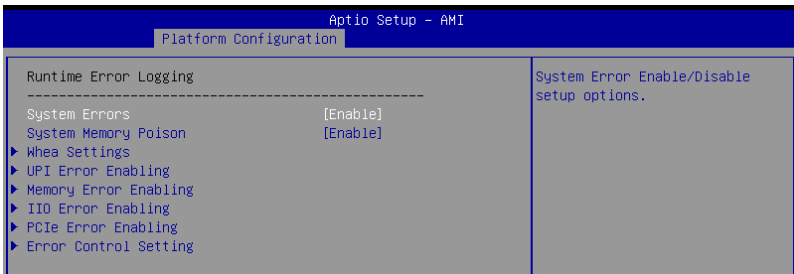
### Altitude [8000]

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.

## 4.5.4 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

#### SMI UPI Lane Failover [Disable]

Allows you to enable or disable SMI when clock/data failover is set.

Configuration options: [Disable] [Enable]

## 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]

## I/O Error Enabling

### I/O/PCH Global Error Support [Enable]

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



---

The following item appears only when **I/O/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 initialize FFM first until handshake, which depends on OS capability.

Configuration options: [Disable] [Enable]

### I/O Error Registers Clear [Enable]

Allows you to enable or disable Clear I/O 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]

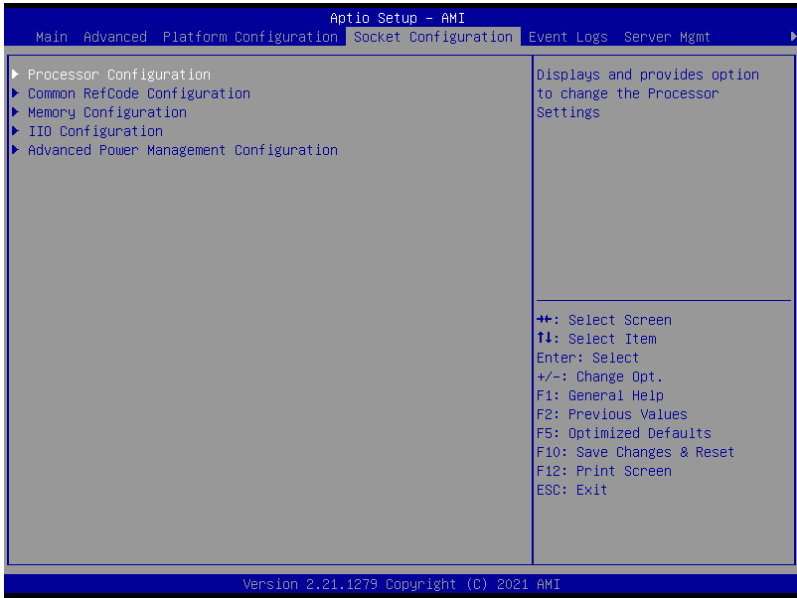
### Latch First Corrected Error in KTI [Enable]

Allows you to enable or disable latch first corrected error in KTI.

Configuration options: [Disable] [Enable]

## 4.6 Socket Configuration menu

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





## 4.6.1 Processor Configuration

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

Aptio Setup - AMI  
Socket Configuration

Processor Configuration

Per-Socket Configuration

Processor	Socket 0	Socket 1
BSP Revision	606A6 - ICX D0	
Socket	Socket 0	Socket 1
ID	000606A6*	N/A
Frequency	2.200GHz	N/A
Max Ratio	16H	N/A
Min Ratio	08H	N/A
Microcode Revision	000001E0	N/A
L1 Cache RAM(Per Core)	80KB	N/A
L2 Cache RAM(Per Core)	1280KB	N/A
L3 Cache RAM(Per Package)	43008KB	N/A
Version	Intel(R) Xeon(R) Gold 6330N CPU @ 2.20GHz	

Hyper-Threading [ALL] [Enable]  
Max CPUID Value Limit [Disable]  
Hardware Prefetcher [Enable]  
L2 RFD Prefetch Disable [Disable]  
Adjacent Cache Prefetch [Enable]  
DCU Streamer Prefetcher [Enable]  
DCU IP Prefetcher [Enable]  
LLC Prefetch [Enable]  
DCU Mode [Normal]

Change Per-Socket Settings

Legend:  
+/-: Select Screen  
F1: Select Item  
Enter: Select  
+/-: Change Opt.  
F1: General Help  
F2: Previous Values  
F5: Optimized Defaults  
F10: Save Changes & Reset  
F12: Print Screen  
ESC: Exit

### Per-Socket Configuration

Allows you to change Per-Socket Settings.

#### CPU Socket 0 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 [FFFFFFFF] 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 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]

## Processor Dfx Configuration

This item displays and provides options to change the Processor Dfx Settings.

### DFX Test Core Sparing [0]

Emulate core BIST failures, input hex digit, 1 in each bit means this core has BIST failure.

### Software Guard Extension (SGX) - DFX

#### SGX Debug Print [Auto]

This item prints info messages.

Configuration options: [Enabled] [Auto]

#### SGX registration server [Auto]

Allows you to choose which server to be used for SGX registration.

Configuration options: [PRX] [SBX] [Auto]

#### MCHECK MSR 0x72 [Auto]

Triggers MCHECK with MSR 0x72, support for Simics.

Configuration options: [Enabled] [Auto]

#### Mock that system HW is not SGX cap [Auto]

Mock that system HW is not SGX capable which allows test suppress in BIOS menu.

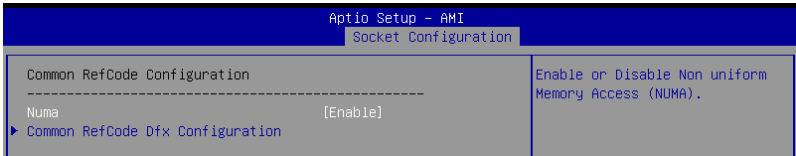
Configuration options: [Enabled] [Auto]

#### SGX APB Support [Auto]

FPE on APB

Configuration options: [Enabled] [Disabled] [Auto]

## 4.6.2 Common RefCode Configuration



### Numa [Enable]

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

### Common RefCode Dfx Configuration

Displays and provides options to change the Common RefCode Dfx Settings.

#### RST\_CPL Bits Programming [F]

Allows you to enable or disable rst\_cpl bits programming. This is a 4-bit bitmask, each bit masks to rst\_cpl1, 2, 3, 4 (bit-0 maps to rst\_cpl1). When the bit is zero, BIOS skips setting the respective cpl bit.

#### B2P Mailbox Commands

Displays and provides options to enable or disable BOIS-to-Pcode mailbox commands.

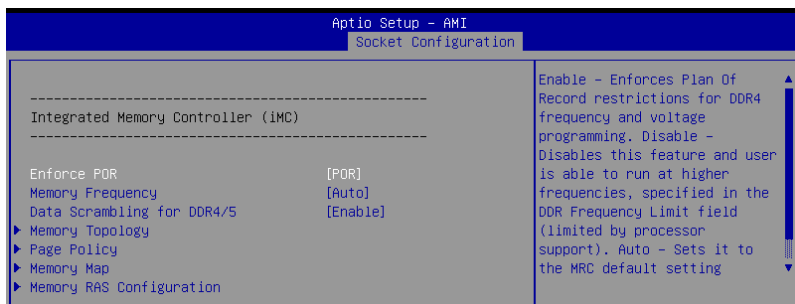
##### B2P Mailbox CMD 0xXX-0xXX [FF]

Enable or disable BIOS-to-Pcode mailbox commands 0xXX-0xXX. This is an 8-bit bitmask, bit-0 maps to CMD 0xXX, ..., bit-7 maps to CMD 0xXX. When the bit is zero, BIOS skips issuing the respective command to Pcode.

##### B2P Error Assert [0]

Enter the command value to assert on if there is an error returned from B2P command. Value 0xFF will assert on all errors.

## 4.6.3 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] - [3800-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 back 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 the 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]

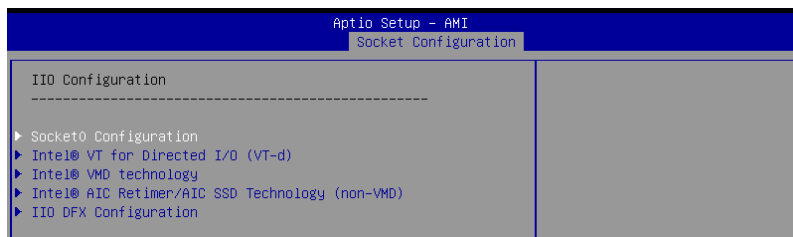
### **Memory RAS Configuration**

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.

## **4.6.4 IIO Configuration**



### **Socket0 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) [Auto]**

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]

### **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 forwarding 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 forwarding 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 Invltom (IIO) and/or WCiLF (cores).

Configuration options: [KTI Option] [Auto] [Enable for Remote Invltom Hybrid Push] [Invltom AllocFlow] [Enable for Remote Invltom Hybrid AllocNonAlloc] [Enable for Remote Invltom and Remove WViLF]

**MCTP [Yes]**

Allows you to enable or disable MCTP.

Configuration options: [No] [Yes]

**Port 1A-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]**.

---

**Hot Plug Capable [Auto]**

This option specifies if the link is considered Hot Plug capable.

Configuration options: [Auto] [Disable] [Enable]

**Surprise Hot Plug Capable [Disable]**

This option specifies if the link is considered Surprise Hot Plug capable.

Configuration options: [Disable] [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 Invltom (IIO) and/or WCiLF (cores).  
Configuration options: [KTI Option] [Auto] [Enable for Remote Invltom Hybrid Push] [Invltom AllocFlow] [Enable for Remote Invltom Hybrid AllocNonAlloc] [Enable for Remote Invltom 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]

## **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(R) 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.



---

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 Config for IOU 0-4****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]

**Intel® AIC Retimer/AIC SSD Technology (non-VMD)****Intel® AIC Retimer/AIC SSD on Socket 0****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]

## IIO DFX Configuration

### Socket0 Configuration

**MMIO Poison Control**

**Enable MMIO read cmp1 poison for STACK\_0-5 [Disabled]**

Configuration options: [Disabled] [Enabled]

**Intel® VT-d Disable Mask [0]**

Bitmap of VT-d engines to disable for debug or diagnostic purpose.

**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)



## Gen3 Override mode [UniPhy]

Set specific TxEq overrides in PCIe features.

Configuration options: [UniPhy] [Manual] [Test Card]



---

The following items appear only when **Gen3 Override mode** is set to **[Manual]**.

---

### PH2 TxEq Precursor [11]

Override Ph2 TXEQ register.

### PH2 TxEq Cursor [41]

Override Ph2 TXEQ register.

### PH2 TxEq Postcursor [11]

Override Ph2 TXEQ register.

### PH3 TxEq Precursor [11]

Override Ph3 TXEQ register.

### PH3 TxEq Cursor [41]

Override Ph3 TXEQ register.

### PH3 TxEq Postcursor [11]

Override Ph3 TXEQ register.



---

The following items appear only when **Gen3 Override mode** is set to **[Test Card]**.

---

## PCIe NTB Test Card [LAGUNA]

Execute TxEq Phase2 for NTB PCIe Test Cards.

Configuration options: [LAGUNA] [NTB]

### Preset Settings

#### DN Tx Preset [Auto]

PCIe Downstream Tx Preset.

Configuration options: [Auto] [P0 (-6.0/0.0 dB)] [P1 (-3.5/0.0 dB)] [P2 (-4.5/0.0 dB)] [P3 (-2.5/0.0 dB)] [P4 (0.0/0.0 dB)] [P5 (0.0/2.0 dB)] [P6 (0.0/2.5 dB)] [P7(-6.0/3.5 dB)] [P8 (-3.5/3.5 dB)] [P9 (0.0/3.5 dB)]

#### DN Tx Preset Hint [Auto]

PCIe Downstream Tx Preset Hint.

Configuration options: [Auto] [P0 (-6.0 dB)] [P1 (-7.0 dB)] [P2 (-8.0 dB)] [P3 (-9.0 dB)] [P4 (-10.0 dB)] [P5 (-11.0 dB)] [P6 (-12.0 dB)]

#### UP Tx Preset [Auto]

PCIe Upstream Tx Preset.

Configuration options: [Auto] [P0 (-6.0/0.0 dB)] [P1 (-3.5/0.0 dB)] [P2 (-4.5/0.0 dB)] [P3 (-2.5/0.0 dB)] [P4 (0.0/0.0 dB)] [P5 (0.0/2.0 dB)] [P6 (0.0/2.5 dB)] [P7(-6.0/3.5 dB)] [P8 (-3.5/3.5 dB)] [P9 (0.0/3.5 dB)]

#### DN Tx Preset Gen4 [Auto]

PCIe Downstream Tx Preset for Gen4.

Configuration options: [Auto] [P0 (-6.0/0.0 dB)] [P1 (-3.5/0.0 dB)] [P2 (-4.5/0.0 dB)] [P3 (-2.5/0.0 dB)] [P4 (0.0/0.0 dB)] [P5 (0.0/2.0 dB)] [P6 (0.0/2.5 dB)] [P7(-6.0/3.5 dB)] [P8 (-3.5/3.5 dB)] [P9 (0.0/3.5 dB)]

#### UP Tx Preset Gen4 [Auto]

PCIe Upstream Tx Preset for Gen4.

Configuration options: [Auto] [P0 (-6.0/0.0 dB)] [P1 (-3.5/0.0 dB)] [P2 (-4.5/0.0 dB)] [P3 (-2.5/0.0 dB)] [P4 (0.0/0.0 dB)] [P5 (0.0/2.0 dB)] [P6 (0.0/2.5 dB)] [P7(-6.0/3.5 dB)] [P8 (-3.5/3.5 dB)] [P9 (0.0/3.5 dB)]

## Miscellaneous Configuration

### Link Re-Train [Disable]

Enable Link Re-Train if connected at degraded speed or width.

Configuration options: [Disable] [Enable]

### Port 1A-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)

### Gen3 Override mode [MgPhy]

Set specific TxEq overrides in PCIe features.

Configuration options: [MgPhy] [Manual] [Manual Ph2] [Manual Ph3] [Test Card]



---

The following items appear only when **Gen3 Override mode** is set to **[Manual]** or **[Manual Ph2]**.

---

### PH2 TxEq Precursor [0]

Override Ph2 TXEQ register.

### PH2 TxEq Cursor [24]

Override Ph2 TXEQ register.

### PH2 TxEq Postcursor [0]

Override Ph2 TXEQ register.



---

The following items appear only when **Gen3 Override mode** is set to **[Manual]** or **[Manual Ph3]**.

---

### PH3 TxEq Precursor [11]

Override Ph3 TXEQ register.

### PH3 TxEq Postcursor [11]

Override Ph3 TXEQ register.



---

The following items appear only when **Gen3 Override mode** is set to **[Test Card]**.

---

### PCIe NTB Test Card [LAGUNA]

Execute TxEq Phase2 for NTB PCIe Test Cards.

Configuration options: [LAGUNA] [NTB]

### Gen4 Override mode [MgPhy]

Set specific TxEq overrides in PCIe features.

Configuration options: [MgPhy] [MgPhyShortCh] [Manual] [Manual Ph2] [Manual Ph3] [Test Card]



---

The following items appear only when **Gen4 Override mode** is set to **[Manual]** or **[Manual Ph2]**.

---

### PH2 TxEq Precursor [0]

Override Ph2 TXEQ register.

### PH2 TxEq Cursor [24]

Override Ph2 TXEQ register.

### PH2 TxEq Postcursor [0]

Override Ph2 TXEQ register.



---

The following items appear only when **Gen3 Override mode** is set to **[Manual]** or **[Manual Ph3]**.

---

**PH3 TxEq Precursor [11]**

Override Ph3 TXEQ register.

**PH3 TxEq Postcursor [11]**

Override Ph3 TXEQ register.

---



The following items appear only when **Gen3 Override mode** is set to **[Test Card]**.

---

**PCIe NTB Test Card [LAGUNA]**

Execute TxEq Phase2 for NTB PCIe Test Cards.

Configuration options: [LAGUNA] [NTB]

**Preset Settings**

**DN Tx Preset [Auto]**

PCIe Downstream Tx Preset.

Configuration options: [Auto] [P0 (-6.0/0.0 dB)] [P1 (-3.5/0.0 dB)] [P2 (-4.5/0.0 dB)] [P3 (-2.5/0.0 dB)] [P4 (0.0/0.0 dB)] [P5 (0.0/2.0 dB)] [P6 (0.0/2.5 dB)] [P7(-6.0/3.5 dB)] [P8 (-3.5/3.5 dB)] [P9 (0.0/3.5 dB)]

**DN Tx Preset Hint [Auto]**

PCIe Downstream Tx Preset Hint.

Configuration options: [Auto] [P0 (-6.0 dB)] [P1 (-7.0 dB)] [P2 (-8.0 dB)] [P3 (-9.0 dB)] [P4 (-10.0 dB)] [P5 (-11.0 dB)] [P6 (-12.0 dB)]

**UP Tx Preset [Auto]**

PCIe Upstream Tx Preset.

Configuration options: [Auto] [P0 (-6.0/0.0 dB)] [P1 (-3.5/0.0 dB)] [P2 (-4.5/0.0 dB)] [P3 (-2.5/0.0 dB)] [P4 (0.0/0.0 dB)] [P5 (0.0/2.0 dB)] [P6 (0.0/2.5 dB)] [P7(-6.0/3.5 dB)] [P8 (-3.5/3.5 dB)] [P9 (0.0/3.5 dB)]

**DN Tx Preset Gen4 [Auto]**

PCIe Downstream Tx Preset for Gen4.

Configuration options: [Auto] [P0 (-6.0/0.0 dB)] [P1 (-3.5/0.0 dB)] [P2 (-4.5/0.0 dB)] [P3 (-2.5/0.0 dB)] [P4 (0.0/0.0 dB)] [P5 (0.0/2.0 dB)] [P6 (0.0/2.5 dB)] [P7(-6.0/3.5 dB)] [P8 (-3.5/3.5 dB)] [P9 (0.0/3.5 dB)]

**UP Tx Preset Gen4 [Auto]**

PCIe Upstream Tx Preset for Gen4.

Configuration options: [Auto] [P0 (-6.0/0.0 dB)] [P1 (-3.5/0.0 dB)] [P2 (-4.5/0.0 dB)] [P3 (-2.5/0.0 dB)] [P4 (0.0/0.0 dB)] [P5 (0.0/2.0 dB)] [P6 (0.0/2.5 dB)] [P7(-6.0/3.5 dB)] [P8 (-3.5/3.5 dB)] [P9 (0.0/3.5 dB)]

**Miscellaneous Configuration**

**Link Re-Train [Disable]**

Enable Link Re-Train if connected at degraded speed or width.

Configuration options: [Disable] [Enable]

**EV DFX Features [Disable]**

Expose IIO DFX devices and other CPU devices like PMON.

Configuration options: [Disable] [Enable]

**Disable BIOS Done [Disabled]**

When set suppresses notifying processor via MSR 151h that boot initialization is finished.

Configuration options: [Disabled] [Enabled]

### **LTSSM Logger [No]**

Allows you to enable or disable LTSSM Logger for PCIe functionality.  
Configuration options: [No] [Yes]



---

The following items appear only when **LTSSM Logger** is set to **[Yes]**.

---

### **Stop [99]**

Allows you to configure the Stop value for LTSSM Logger.  
Configuration options: [0] - [99]

### **Speed [Gen 1 (2.5 GT/s)]**

Allows you to configure the Speed value for LTSSM Logger.  
Configuration options: [Gen 1 (2.5 GT/s)] [Gen 2 (5 GT/s)] [Gen 3 (8 GT/s)]  
[Gen 4 (16 GT/s)]

### **Mask [FF]**

Allows you to configure the Mask value for LTSSM Logger.

### **Jitter Logger [No]**

Allows you to enable or disable Jitter Logger for PCIe functionality.  
Configuration options: [No] [Yes]

### **IIO RC flow [Auto]**

Allows you to enable or disable IIO RC flow execution.  
Configuration options: [Disable] [Enable] [Auto]



---

The following item appears only when **IIO RC flow** is set to **[Enable]** or **[Auto]**.

---

### **IIO PCIE link training [Auto]**

Allows you to enable or disable PCIE link training execution.  
Configuration options: [Disable] [Enable] [Auto]

### **Skip Port Personality Lock [Disable]**

When enabled leaves capability registers of PCI and DMI ports not locked.  
Configuration options: [Disable] [Enable]

### **OTC Pipe Hazard Thresh [4]**

Sets OTC Pipe Hazard Thresh value, 0 cycles as default and used to disable workaround for outbound parity errors.  
Configuration options: [0] - [9]

### **Bad Transaction Type WA [Auto]**

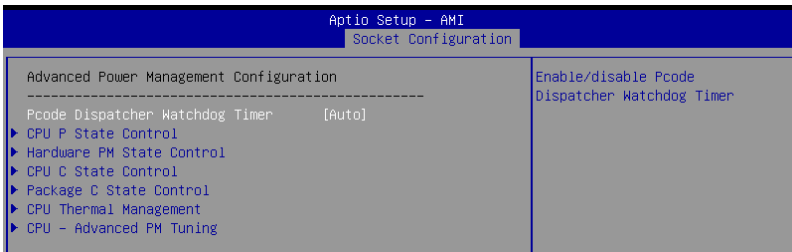
Allows you to enable or disable M2IOSF bad transaction type workaround execution.  
Configuration options: [Disable] [Enable] [Auto]

### **Socket 0, Device Hide Menu**

#### **Uncore Stack0-1 Devhide0-7 [0]**

If entire DEVHIDEx is 0, then register will not be modified. If any byte is non-zero, then the entire DEVHIDE register will be overridden with these values (thus overriding any other HIDE option in setup such as PCIe port hide questions).

## 4.6.5 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]

### **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 [Disable]

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 [Disable]

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

### 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]

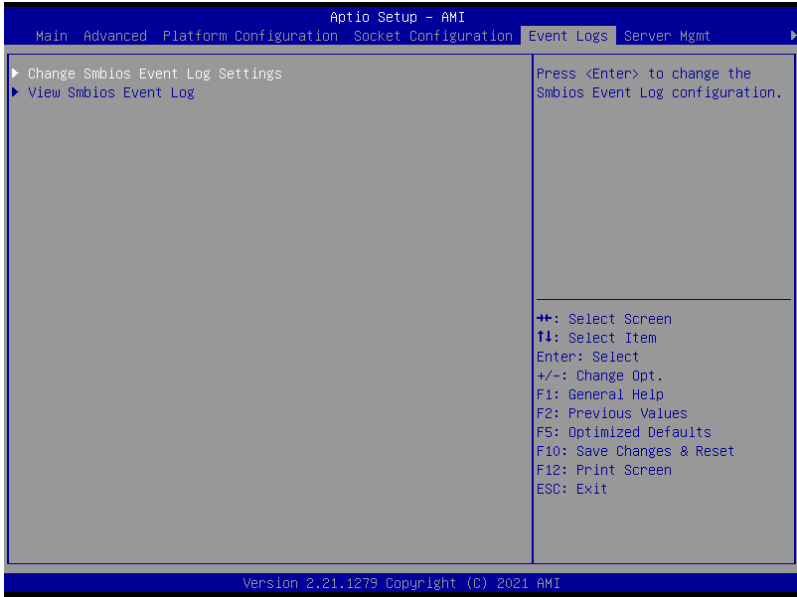
#### EET Mode [Coarse Grained Mode]

[Coarse Grained Mode] Decides whether to grant user request turbo on P1.

[Fine Grained Mode] Decides how much turbo to be granted.

# 4.7 Event Logs menu

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

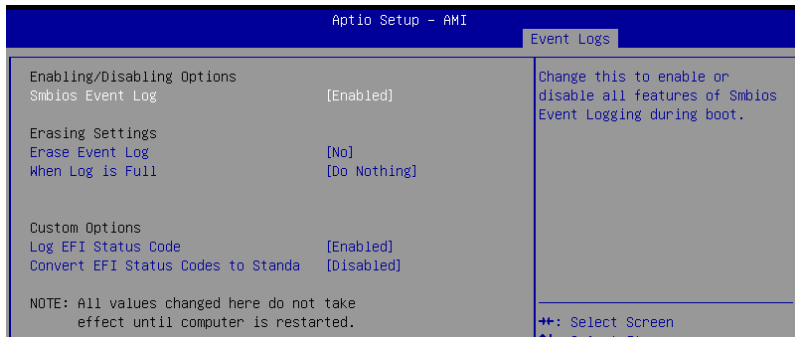


## 4.7.1 Change Smbios Event Log Settings

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]

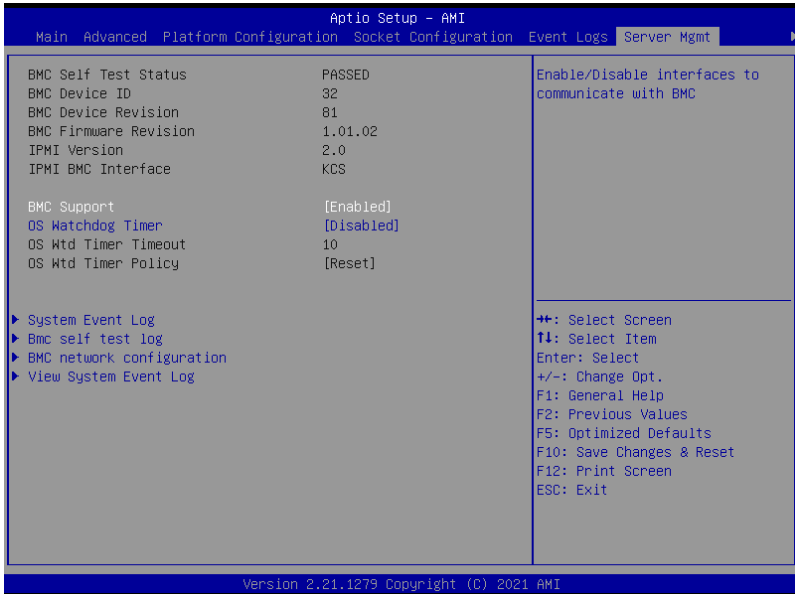
## **4.7.2 View Smbios Event Log**

Press <Enter> to view all smbios event logs.

Aptio Setup - AMI					
					Event Logs
DATE	TIME	ERROR CODE	SEVERITY	COUNT	DESCRIPTION
02/24/21	11:00:42	Smbios 0x16	N/A	N/A	Log Area Reset
02/24/21	16:45:17	EFI 03051002	Major	01	
02/25/21	09:09:22	EFI 03051002	Major	01	

## 4.8 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]

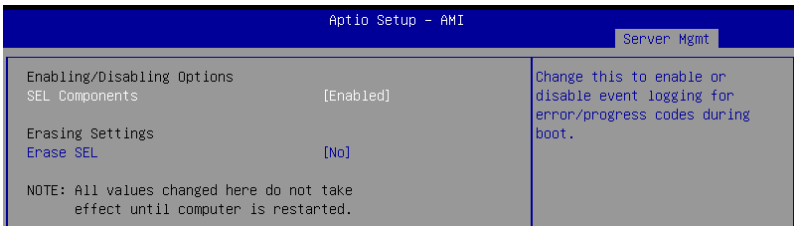
This item allows you to configure the how the system should respond if the OS Boot Watch Timer expires. Not available if OS Boot Watchdog Timer is disabled.  
Configuration options: [Do Nothing] [Reset] [Power Down] [Power Cycle]

## 4.8.1 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]



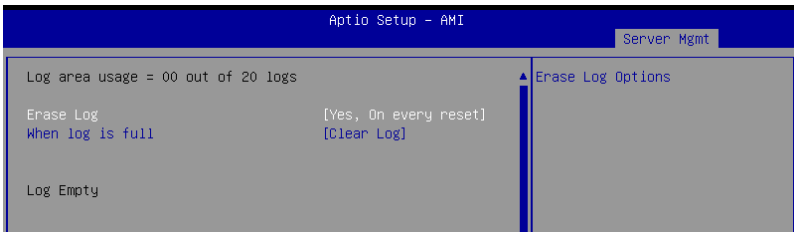
The following item is available only when **SEL Components** is set to **[Enabled]**.

### Erase SEL [No]

Allows you to choose options for erasing SEL.  
Configuration options: [No] [Yes, On next reset] [Yes, On every reset]

## 4.8.2 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]

## 4.8.3 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.

The screenshot shows the Aptio Setup - AMI interface with the Server Mgmt tab selected. The main window displays the BMC network configuration options, which are divided into two sections: DM\_LAN1 and Shared LAN. The DM\_LAN1 section shows the Configuration Address source set to [Previous State], with other parameters like Station IP address, Subnet mask, Station MAC address, Router IP address, and Router MAC address. The Shared LAN section shows the Configuration Address source set to [Previous State], with other parameters like Station IP address, Subnet mask, Station MAC address, Router IP address, and Router MAC address. A right-hand pane provides instructions on how to navigate the menu, including options like Select Screen, Select Item, Enter: Select, +/-: Change Opt., F1: General Help, F2: Previous Values, F5: Optimized Defaults, F10: Save Changes & Reset, F12: Print Screen, and ESC: Exit.

### 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).

#### Configuration Router LAN1/2 Address [Previous State]

Allows you to set the LAN channel parameters statically or dynamically (by BIOS or by BMC). Unspecified 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 Router LAN1/2 Address** is set to **[Static]**.

---

#### IPV6 Router1 IP Address

Allows you to set the IPV6 Router1 IP address.

#### IPV6 Router1 Prefix Length Lan1/2

Allows you to set the IPV6 router prefix length (maximum of IPV6 Router Prefix Length is 128).

#### IPV6 Router1 Prefix Value Lan1/2

Allows you to change the IPV6 router prefix value.



## 4.8.4 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.

Aptio Setup - AMI

Server Mgmt

No. of log entries in SEL : 1978

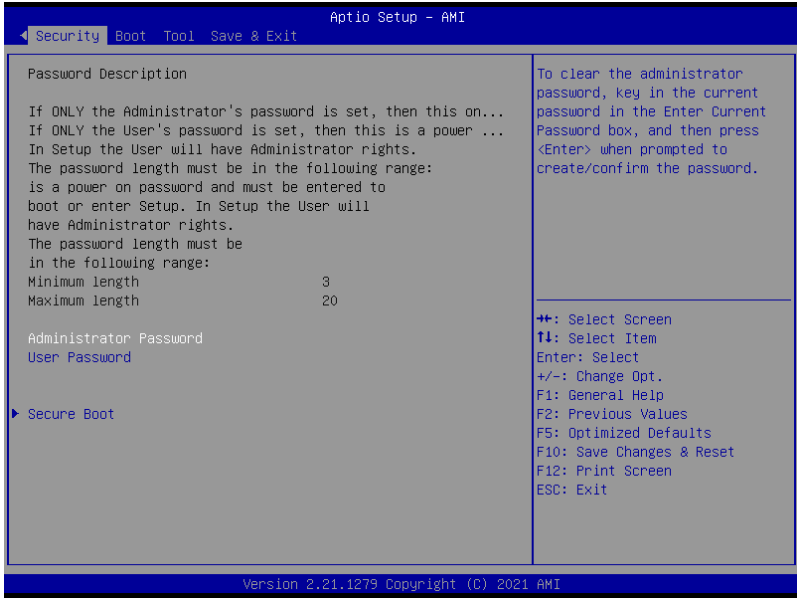
DATE	TIME	SENSOR TYPE
12/24/20	04:33:36	Power Supply
12/24/20	04:33:36	Power Supply
12/24/20	04:33:39	Power Supply
12/24/20	04:33:39	Power Supply
12/24/20	04:34:05	Power Supply
12/24/20	04:34:05	Power Supply
12/24/20	04:34:08	Power Supply
12/24/20	04:34:08	Power Supply
12/24/20	04:34:08	Power Supply
12/24/20	04:39:43	Power Supply
12/24/20	04:39:43	Power Supply
12/24/20	04:42:01	Power Supply
12/24/20	04:42:04	Power Supply
12/24/20	04:42:41	Power Supply
12/24/20	04:42:44	Power Supply
12/24/20	04:45:37	Power Supply
12/24/20	04:45:37	Power Supply
12/24/20	04:45:40	Power Supply
12/24/20	04:45:40	Power Supply
12/24/20	04:46:10	Power Supply
12/24/20	04:46:10	Power Supply
12/24/20	04:46:10	Power Supply

HEX:  
01 00 02 20 1A E4  
5F 20 00 04 08 DF  
01 50 00 00  
Generator ID: BMC - LUN #0  
(Channel #0)  
Sensor Number: 0xDF OEM  
(Unknown)  
Event Description:  
Record Type-0x02.  
Assertion Event.

++: Select Screen  
↑↓: Select Item  
Enter: Select  
+/-: Change Opt.  
F1: General Help  
F2: Previous Values  
F5: Optimized Defaults  
F10: Save Changes & Reset  
F12: Print Screen  
ESC: Exit

## 4.9 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:

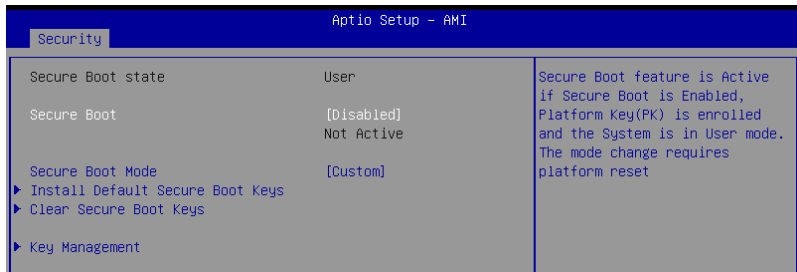
1. Select the User Password item and press <Enter>.
2. From the Enter Current Password box, key in the current password, then press <Enter>.
3. From the Create New Password box, key in a new password, then press <Enter>.
4. Confirm the password when prompted.

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>.

### 4.9.1 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.

Aptio Setup - AMI

Security

Vendor Keys Modified

Factory Key Provision [Enabled]

- ▶ Install Default Secure Boot Keys
- ▶ Clear Secure Boot Keys
- ▶ Save all Secure Boot variables
- ▶ Enroll Efi Image

Device Guard Ready

- ▶ Remove 'UEFI CA' from DB
- ▶ Restore DB defaults

Secure Boot variable	Size	Keys	Key Source
▶ PK Management	886	1	Default
▶ KEK Management	3573	3	Default
▶ DB Management	6322	10	Default
▶ DBX Management	3724	77	Default
▶ Authorized TimeStamps	0	0	No Keys
▶ OsRecovery Signatures	0	0	No Keys

Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode

++: Select Screen  
! : Select Item  
Enter: Select  
+/-: Change Opt.  
F1: General Help  
F2: Previous Values  
F5: Optimized Defaults

### 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 folder 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**

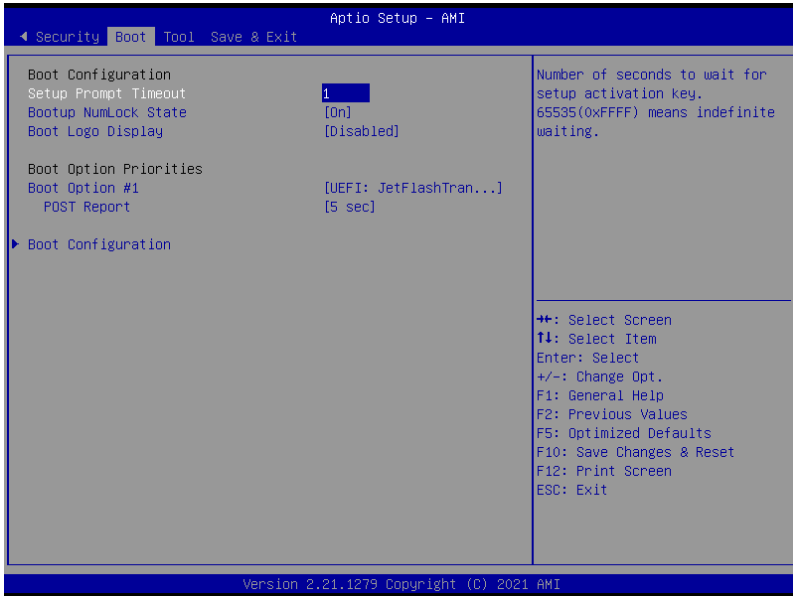
Configuration options: [Details] [Save To File] [Set New Key] [Append Key] [Delete key]

### **Authorized TimeStamps / OsRecovery Signatures**

Configuration options: [Set New Key] [Append Key]

## 4.10 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(0xFFFF) 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]

## 4.10.1 Boot Configuration

Aptio Setup - AMI		
Boot		
Boot Configuration		
Boot Sector (MBR/GPT) Recovery Pol	[Local User Control]	Determines Boot Sector Policy.
Next Boot Recovery Action	[Skip]	Auto Recovery: Follow UEFI Rule. Local User Control: You can

### 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]

## 4.11 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.

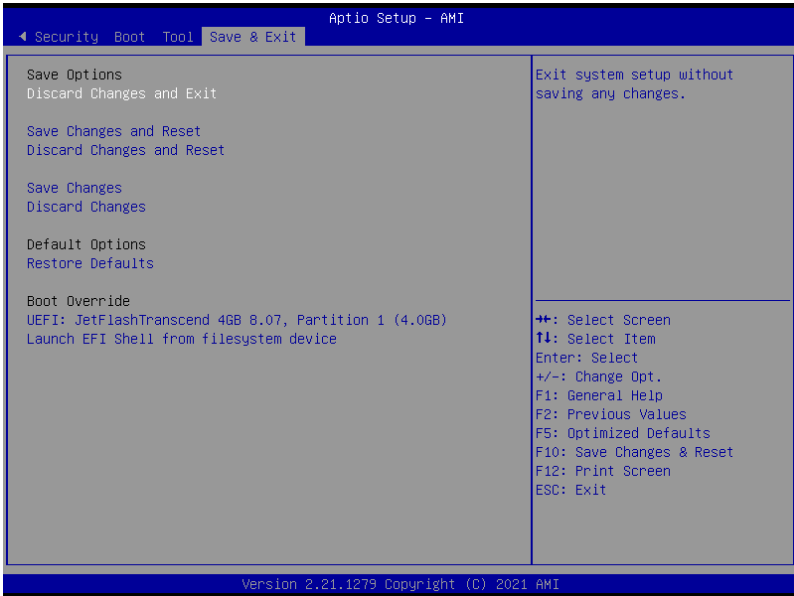
### ASUS SMBIOS Viewer

Allows you to start ASUS SMBIOS Viewer when you press <Enter>.



## 4.12 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.

# Driver Installation

# 5

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

## 5.1 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](http://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.

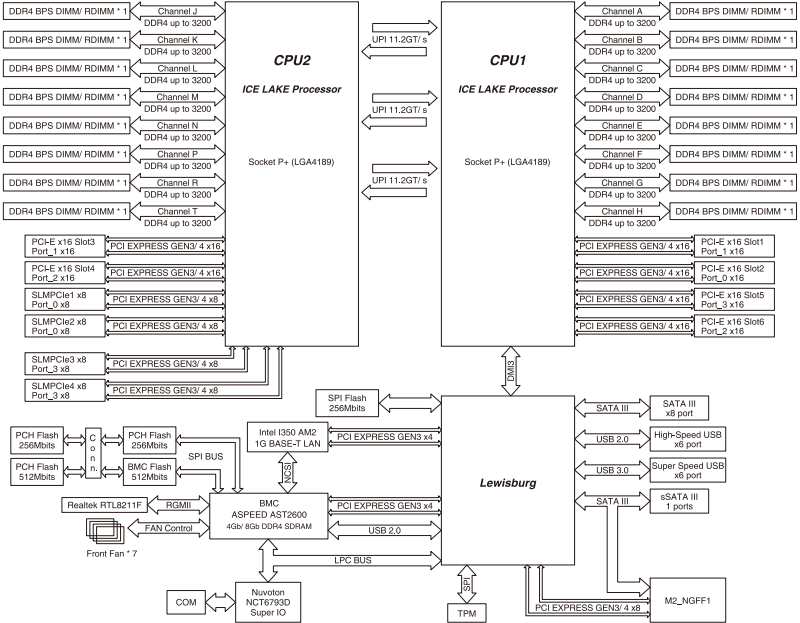
---

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

This appendix includes additional information that you may refer to when configuring the motherboard.

# Z12PG-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)

### 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.

## Japan JATE

本製品は電気通信事業者（移動通信会社、固定通信会社、インターネットプロバイダ等）の通信回線（公衆無線LANを含む）に直接接続することができません。本製品をインターネットに接続する場合は、必ずルーター等を経由し接続してください。

## 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.

## 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 năm 2011 trở về sau, đều phải đáp ứng các yêu cầu của Thông tư 30/2011/TT-BCT của Việt Nam.

## Türkiye 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>.

## KC: Korea Warning Statement



R-R-MSQ-ESC4000-E10S

이 기기는 업무용 환경에서 사용할 목적으로 적합성평가를 받은 기기로서 가정용 환경에서 사용하는 경우 전파간섭의 우려가 있습니다.

## Safety Precautions

Accessories that came with this product have been designed and verified for the use in connection with this product. Never use accessories for other products to prevent the risk of electric shock or fire.

## 安全上のご注意

付属品は当該専用品です。他の機器には使用しないでください。機器の破損もしくは、火災や感電の原因となることがあります。

## Service and Support

Visit our multi-language website at <https://www.asus.com/support/>



