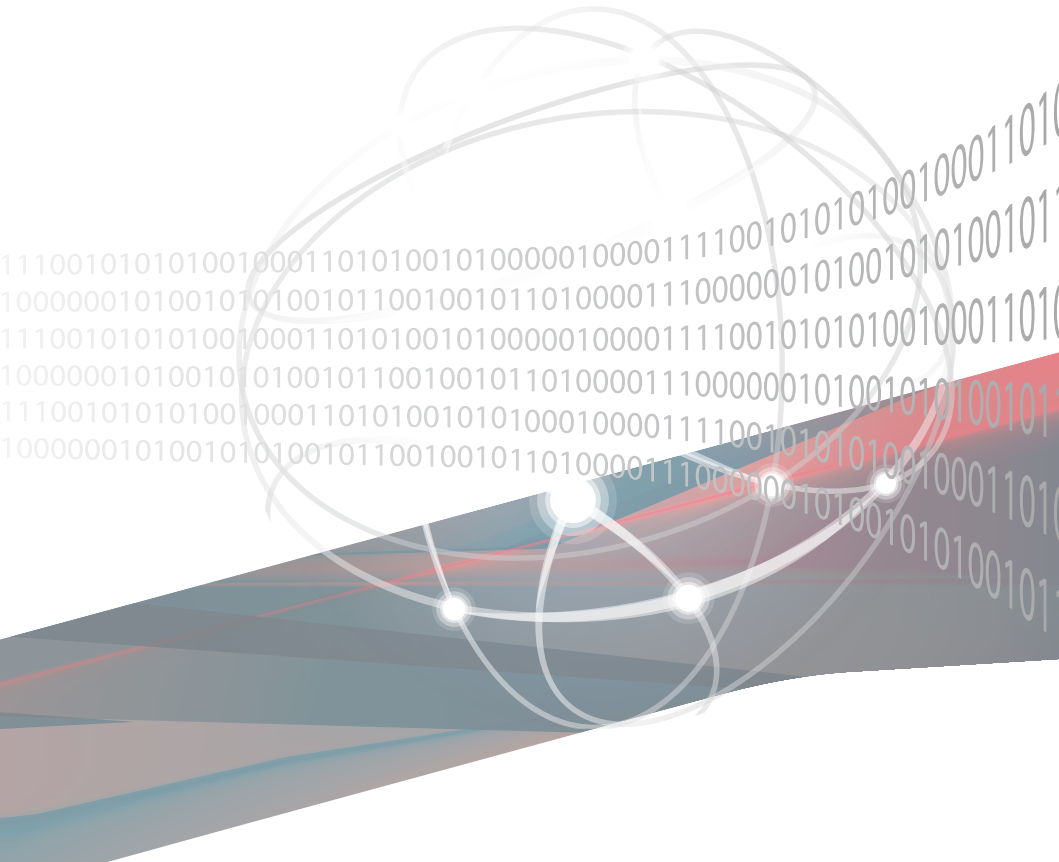




# RS720-E10-RS24U

## 2U Rackmount Server User Guide



E23368  
Revised Edition V2  
July 2023

**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.....	viii

## 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.....	1-7
1.5	Rear panel features.....	1-7
1.6	Internal features .....	1-8
1.7	LED information .....	1-9
1.7.1	Front panel LEDs .....	1-9
1.7.2	Storage device status LED.....	1-10
1.7.3	LAN (RJ-45) LEDs .....	1-11
1.7.4	Rear panel LEDs.....	1-12
1.7.5	Q-Code table.....	1-13

## Chapter 2: Hardware Information

2.1	Chassis cover.....	2-2
2.2	Air ducts.....	2-4
2.3	Central Processing Unit (CPU) .....	2-5
2.3.1	Removing the CPU and heatsink (for Standard model).....	2-5
2.3.2	Removing the CPU and heatsink (for GPU model).....	2-8
2.3.3	Installing the CPU and heatsink.....	2-11
2.4	System memory .....	2-14
2.4.1	Overview .....	2-14
2.4.2	Memory Configurations.....	2-14
2.4.3	Installing a DIMM on a single clip DIMM socket.....	2-17
2.4.4	Removing a DIMM .....	2-17
2.5	Storage devices.....	2-18

# Contents

- 2.6 Expansion slot.....2-22**
  - 2.6.1 Installing an expansion card to riser card bracket 1.....2-24
  - 2.6.2 Installing an expansion card to riser card bracket 2.....2-27
  - 2.6.3 Installing an expansion card to riser card bracket 3.....2-30
  - 2.6.4 Installing an expansion card to riser card bracket 4.....2-33
  - 2.6.5 Installing an OCP 3.0 slot baseboard and OCP 3.0 card to the riser card bracket .....2-36
  - 2.6.6 Installing an ethernet expansion card to the riser card bracket .....2-41
  - 2.6.7 Installing an ASUS PIKE II card.....2-42
  - 2.6.8 Installing M.2 (NGFF) cards.....2-46
  - 2.6.9 Configuring an expansion card .....2-49
- 2.7 Cable connections .....2-50**
- 2.8 SATA/SAS backplane cabling.....2-52**
- 2.9 Removable/optional components.....2-54**
  - 2.9.1 System fans .....2-54
  - 2.9.2 Redundant power supply module.....2-58

## Chapter 3: Installation Options

- 3.1 Tool-less Friction Rail Kit.....3-2**
- 3.2 Installing the tool-less rack rail .....3-3**
- 3.3 Rail kit dimensions .....3-5**
- 3.4 Ball bearing Rail Kit.....3-6**
  - 3.4.1 Selecting rack rail cabinets .....3-6
  - 3.4.2 Attaching the rack rails.....3-7
- 3.5 Cable management arm (optional for 1200 mm rack rails).....3-11**
  - 3.5.1 Attaching the cable management arm .....3-11

## Chapter 4: Motherboard Information

- 4.1 Motherboard layout.....4-2**
- 4.2 Jumpers .....4-5**
- 4.3 Internal LEDs.....4-10**
- 4.4 Internal connectors.....4-13**

# Contents

## Chapter 5: BIOS Setup

<b>5.1</b>	<b>Managing and updating your BIOS</b> .....	<b>5-2</b>
5.1.1	ASUS CrashFree BIOS 3 utility.....	5-2
5.1.2	ASUS EZ Flash Utility .....	5-3
5.1.3	BUPDATER utility .....	5-4
<b>5.2</b>	<b>BIOS setup program</b> .....	<b>5-6</b>
5.2.1	BIOS menu screen.....	5-7
5.2.2	Menu bar .....	5-7
5.2.3	Menu items.....	5-8
5.2.4	Submenu items .....	5-8
5.2.5	Navigation keys.....	5-8
5.2.6	General help.....	5-8
5.2.7	Configuration fields .....	5-8
5.2.8	Pop-up window.....	5-8
5.2.9	Scroll bar.....	5-8
<b>5.3</b>	<b>Main menu</b> .....	<b>5-9</b>
5.3.1	System Language [English] .....	5-9
5.3.2	System Date [Day xx/xx/xxxx].....	5-9
5.3.3	System Time [xx:xx:xx] .....	5-9
<b>5.4</b>	<b>Ai Tweaker menu</b> .....	<b>5-10</b>
<b>5.5</b>	<b>Advanced menu</b> .....	<b>5-11</b>
5.5.1	OffBoard SATA Controller Configuration .....	5-11
5.5.2	Trusted Computing.....	5-12
5.5.3	ACPI Settings.....	5-12
5.5.4	Redfish Host Interface Settings.....	5-12
5.5.5	Onboard LAN Configuration.....	5-13
5.5.6	Serial Port Console Redirection .....	5-15
5.5.7	SIO Common Setting .....	5-18
5.5.8	SIO Configuration.....	5-18
5.5.9	PCI Subsystem Settings .....	5-19
5.5.10	USB Configuration .....	5-20
5.5.11	Network Stack Configuration.....	5-21
5.5.12	CSM (Compatibility Support Module).....	5-22
5.5.13	NVMe Configuration.....	5-23
5.5.14	APM Configuration .....	5-24
5.5.15	Third-party UEFI driver configurations .....	5-25

# Contents

- 5.6 Platform Configuration menu .....5-26**
  - 5.6.1 PCH Configuration ..... 5-26
  - 5.6.2 Miscellaneous Configuration ..... 5-28
  - 5.6.3 Server ME Configuration ..... 5-29
  - 5.6.4 Runtime Error Logging Support ..... 5-30
- 5.7 Socket Configuration menu ..... 5-33**
  - 5.7.1 Processor Configuration ..... 5-34
  - 5.7.2 Common RefCode Configuration ..... 5-36
  - 5.7.3 Memory Configuration ..... 5-37
  - 5.7.4 IIO Configuration ..... 5-38
  - 5.7.5 Advanced Power Management Configuration ..... 5-51
- 5.8 Event Logs menu ..... 5-56**
  - 5.8.1 Change Smbios Event Log Settings ..... 5-57
  - 5.8.2 View Smbios Event Log ..... 5-58
- 5.9 Server Mgmt menu ..... 5-59**
  - 5.9.1 System Event Log ..... 5-60
  - 5.9.2 BMC self test log ..... 5-60
  - 5.9.3 BMC network configuration ..... 5-61
  - 5.9.4 View System Event Log ..... 5-63
- 5.10 Security menu ..... 5-64**
  - 5.10.1 Secure Boot ..... 5-65
- 5.11 Boot menu ..... 5-68**
  - 5.11.1 Boot Configuration ..... 5-69
- 5.12 Tool menu ..... 5-70**
- 5.13 Save & Exit menu ..... 5-71**

## Chapter 6: Driver Installation

- 6.1 Running the Support DVD ..... 6-2**

## Appendix

- Z12PP-D32 block diagram ..... A-2**
- Notices ..... A-3**
- Service and Support ..... A-6**

# 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.
- If you encounter technical problems with the product, contact a qualified service technician or your retailer.



---

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.

---

### 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.

### Heavy System

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

# About this guide

## Audience

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

## Contents

This guide contains the following parts:

**1. Chapter 1: Product Introduction**

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

**2. Chapter 2: Hardware Information**

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

**3. Chapter 3: Installation Options**

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

**4. Chapter 4: Motherboard Information**

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

**5. Chapter 5: BIOS Setup**

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

**6. Chapter 6: Driver Installation**

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



## Conventions

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



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



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



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



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

## Typography

**Bold text**

Indicates a menu or an item to select.

*Italics*

Used to emphasize a word or a phrase.

<Key>

Keys enclosed in the less-than and greater-than sign means that you must press the enclosed key.

Example: <Enter> means that you must press the Enter or Return key.

<Key1>+<Key2>+<Key3>

If you must press two or more keys simultaneously, the key names are linked with a plus sign (+).

Example: <Ctrl>+<Alt>+<Del>

Command

Means that you must type the command exactly as shown, then supply the required item or value enclosed in brackets.

Example: At the DOS prompt, type the command line:  
`format A: /S`

## References

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

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

This manual tells how to set up and use the proprietary ASUS server management utility. Visit [asuscontrolcenter.asus.com](https://www.asus.com/asuscontrolcenter) for more information.

### 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 chassis kit. It includes sections on front panel and rear panel specifications.

# 1.1 System package contents

Check your system package for the following items.

Model Name	RS720-E10-RS24U
Chassis	ASUS R2P-A-R22475 2U Rackmount Chassis
Motherboard	ASUS Z12PP-D32 Server Board
Component	1 x 80PLUS Power Supply
	24 x Hot-swap 2.5-inch Storage Device Trays or Dummy Trays
	1 x 2.5-inch Storage Device Backplane
	1 x Front Panel Board
	1 x Front USB3 Board
	4 x Riser Cards
Accessories	4 x System Fans
	1 x Support DVD
	1 x Bag of Screws
	2 x CPU Heatsink
	2 x AC Power Cable
	1 x External Fan Module (Optional)
Optional Items	1 x OCP3.0 Adapter Card (Optional)
	1 x LAN Module (Optional)
	1 x 80PLUS Power Supply (Second PSU)
	1 x Friction Rail Kit
	1 x Ball Bearing Rail Kit (1000mm)
	1 x Ball Bearing Rail Kit (1200mm)
	1 x Cable Management Arm (only for Ball Bearing Rail Kit 1200mm)

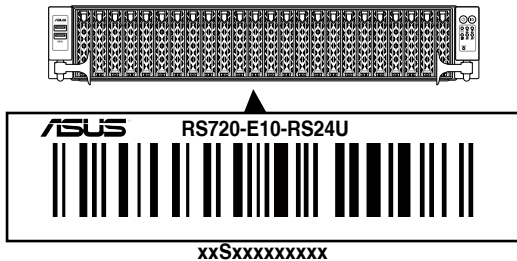


If any of the above items is damaged or missing, contact your retailer.

# 1.2 Serial number label

The product's serial number contains 12 characters such as xxSxxxxxxxxx and printed on the sticker at the server's front cover.

The correct serial number of the product is required if you need to request for support from the ASUS Technical Support team.



## 1.3 System specifications

The ASUS RS720-E10-RS24U features the ASUS Z12PP-D32 server board. The server supports 3<sup>rd</sup> Generation Intel® Xeon® Scalable Processors plus other latest technologies through the chipsets onboard.

Model Name		RS720-E10-RS24U
Motherboard		Z12PP-D32
Processor Support		2 x Socket P+ (LGA 4189) 3 <sup>rd</sup> Generation Intel® Xeon® Scalable Processors
Core Logic		Intel® C621A Chipset
Memory	Total Slots	32 (8-channel per CPU, 16 DIMM per CPU)
	Capacity	Maximum up to 6TB
	Memory Type	DDR4 3200/2933 RDIMM/RDIMM 3DS/LRDIMM/LRDIMM 3DS (2 DIMM per channel) Intel® Optane™ DC persistent memory 200 Series (DCPMM) * Please refer to <a href="http://www.asus.com">www.asus.com</a> for latest memory AVL update
	Memory Size	64GB, 32GB, 16GB, 8GB RDIMM 256GB, 128GB, 64GB RDIMM 3DS 128GB, 64GB LRDIMM 128GB LR-DIMM 3DS 512GB, 256GB, 128GB Intel® Optane™ DC persistent memory 200 Series (PMem) * Refer to <a href="http://www.asus.com/support">www.asus.com/support</a> for more information
Expansion Slots	Total PCIe/PIKE Slots	9
	Slot Type	<b>Slot 1/2:</b> 2 x PCIe x16 (Gen4 x8 link) or 1 x PCIe x16 (Gen4 x16 link), FH, HL (CPU1) <b>Slot 3:</b> 1 x PCIe x16 (Gen4 x16 link), FH, HL (CPU1) * Can be converted to OCP3.0 slot <b>Slot 4:</b> 1 x PCIe x8 (Gen4/Gen3 x8 link) FH, HL (CPU1) * Optional for PIKE II <b>Slot 5/6:</b> 2 x PCIe x16 (Gen4 x8 link) or 1 x PCIe x16 (Gen4 x16 link), FH, HL (CPU2) <b>Slot 7/8:</b> 2 x PCIe x16 (Gen4 x8 link) or 1 x PCIe x16 (Gen4 x16 link), FH, HL (CPU2) <b>Slot 9:</b> 1 x PCIe x16 (Gen4 x16 link), LP, HL (CPU2) * Optional for COM cable ** If PCIe M.2 is in use, it will operate at x8 link

(continued on the next page)

Model Name		RS720-E10-RS24U
Expansion Slots	M.2	2 x M.2 (Support PCIe mode 2260 or 2280 from CPU2)
	Micro SD Card Slot	1
Storage Controller	SATA Controller	Intel® PCH C621A 12 x SATA 6Gb/s ports
	SAS Controller	<b>Optional:</b> ASUS PIKE II 3008 8-port SAS 12Gb/s HBA card ASUS PIKE II 3108 8-port SAS HW 12Gb/s RAID card
Storage Bays	Storage Bay	<b>Front bays</b> 24 x 2.5" Hot-Swap Drive Bays: 12 x NVMe + 12 x NVMe/SATA (2 switch boards) 12 x NVMe + 12 x SATA (1 switch board)
	Motherboard on-board connectors	2 x M.2 connectors 3 x miniSAS HD connectors
	NVMe upgrade option	Additional 12 NVMe (1 x PCIe switch board + 2 x cables)
Networking		4 x 1GbE (Intel® I350-AM4) RJ45 port* or 2 x 10GbE (Intel® X710-AT2) RJ45 port 1 x Management Port
		<b>Optional OCP 3.0 Adapter:</b> Up to 200Gb/s Ethernet / InfiniBand Adapter

(continued on the next page)

<b>Model Name</b>	<b>RS720-E10-RS24U</b>
<b>VGA</b>	Aspeed AST2600 64MB
<b>Front I/O Ports</b>	2 x USB 3.2 Gen 1 ports
<b>Rear I/O Ports</b>	2 x USB 3.2 Gen 1 ports 1 x VGA port 1 x RJ-45 Mgmt LAN port 4/2 x NIC ports* 1 x OCP 3.0 port (Optional) * <b>The number of NIC ports available depends on the LAN Controller card installed</b>
<b>Switch/LED</b>	<b>Front Switch/LED:</b> 1 x Power Switch (w/ LED) 1 x Reset Switch 1 x Location Switch (w/ LED) 1 x Storage Device Access LED* 1 x Message LED LAN 1-4 LED** * <b>The Storage Device Access LED is only functional when an ASUS PIKE II card is installed and connected</b> ** <b>The number of LAN LEDs available depends on the LAN Controller card installed</b>  <b>Rear Switch/LED:</b> 1 x Port 80 LED (Q-Code) 1 x Power Switch (w/ LED) 1 x Location Switch (w/ LED)

*(continued on the next page)*

<b>Model Name</b>		<b>RS720-E10-RS24U</b>
<b>Security Options</b>		TPM-SPI PFR
<b>OS Support</b>		Windows® Server RedHat® Enterprise Linux SuSE® Linux Enterprise Server CentOS Ubuntu * Please find the latest OS support from <a href="http://www.asus.com">http://www.asus.com</a>
<b>Management Solution</b>	<b>Software</b>	ASUS Control Center
	<b>Out of Band Remote Hardware</b>	On-Board ASMB10-iKVM for KVM-over-IP
<b>Regulatory Compliance</b>		BSMI, CE, CB, FCC(Class A)
<b>Dimension</b>		840 mm x 449 mm x 88 mm (2U)
<b>Net Weight Kg (CPU, DRAM &amp; storage device not included)</b>		25.64 Kg
<b>Gross Weight Kg (CPU, DRAM &amp; storage device not included, packing included)</b>		36 Kg
<b>Power Supply (different configuration by region)</b>		1+1 Redundant 1600W 80 PLUS Platinum Power Supply Rating: 100-127Vac/200-240Vac, 13A/9.5A (for each inlet), 50-60Hz, Class I Rating: 100-127Vac/200-240Vac, 12A/10A (for each inlet), 50/60Hz, Class I or 2400W 80 PLUS Titanium Power Supply Rating: 100-127Vac/200-240Vac, 13.8A/15A (for each inlet), 50/60Hz, Class I
<b>Environment</b>		Operating temperature: 10°C ~ 35°C Non operating temperature: -40°C ~ 60°C Non operating humidity: 20% ~ 90% (Non condensing)

\* Specifications are subject to change without notice.

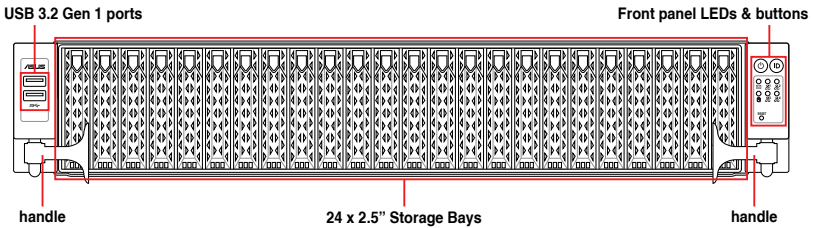


## 1.4 Front panel features

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

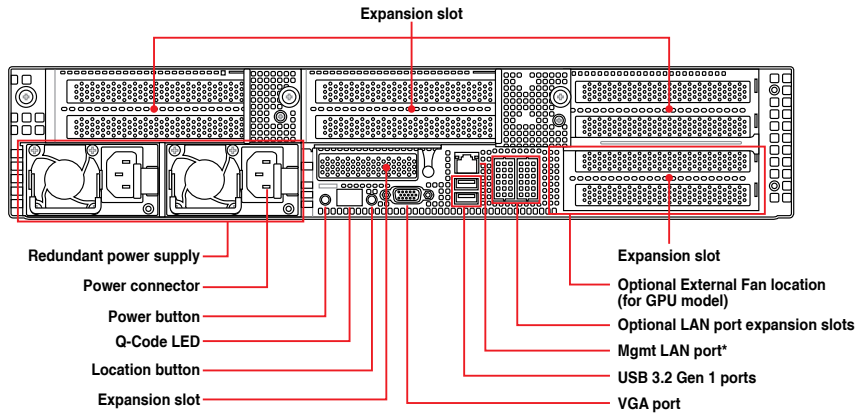


Refer to section 1.7 LED information for the LED descriptions.



## 1.5 Rear panel features

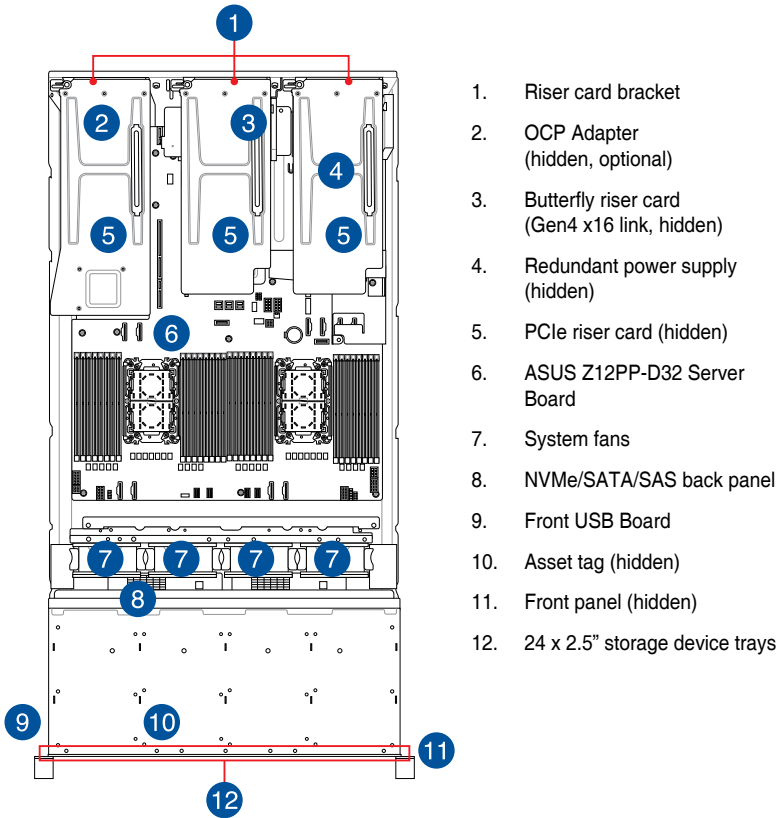
The rear panel includes the expansion slots, system power sockets, and rear fans. The middle part includes the I/O shield with openings for the rear panel connectors on the motherboard.



- Mgmt LAN port is for ASUS ASMB10-iKVM only.
- The Q-Code LED provides the most probable cause of an error code as a starting point for troubleshooting. The actual cause may vary from case to case.
- Refer to the Q-Code table for details.

## 1.6 Internal features

The barebone server includes the basic components as shown.



- 1. Riser card bracket
- 2. OCP Adapter (hidden, optional)
- 3. Butterfly riser card (Gen4 x16 link, hidden)
- 4. Redundant power supply (hidden)
- 5. PCIe riser card (hidden)
- 6. ASUS Z12PP-D32 Server Board
- 7. System fans
- 8. NVMe/SATA/SAS back panel
- 9. Front USB Board
- 10. Asset tag (hidden)
- 11. Front panel (hidden)
- 12. 24 x 2.5" storage device trays



The barebone server does not include a floppy disk drive. Connect a USB floppy disk drive to any of the USB ports on the front or rear panel if you need to use a floppy disk.

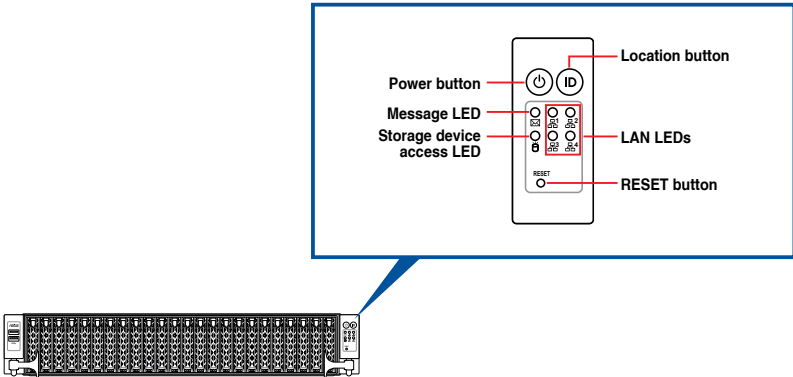


A protection film is pre-attached to the front cover before shipping. Please remove the protection film before turning on the system for proper heat dissipation.

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

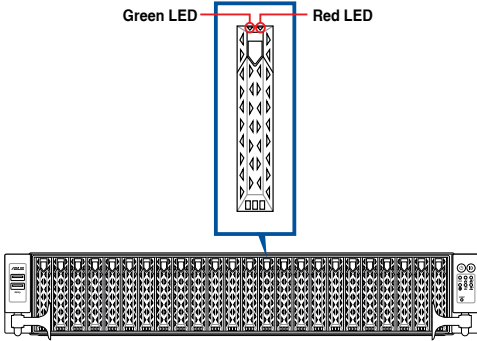
## 1.7 LED information

### 1.7.1 Front panel LEDs



LED	Icon	Display status	Description
Power LED		ON	System power ON
Storage device access LED		OFF	No activity
		Blinking	Read/write data into the storage device
Message LED		OFF	System is normal; no incoming event
		ON	With the onboard ASMB10-iKVM: a hardware monitor event is indicated
LAN LEDs		OFF	No LAN connection
		Blinking	LAN is transmitting or receiving data
		ON	LAN connection is present
Location LED	ID	ON	Location switch is pressed
		OFF	Normal status (Press the location switch again to turn off)

## 1.7.2 Storage device status LED



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

### 1.7.3 LAN (RJ-45) LEDs

#### Intel® I350-AM4 1G LAN port LEDs

ACT/LINK LED    SPEED LED



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

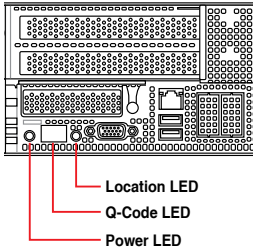
#### Intel® X710-AT2 Gigabit 10G LAN port LEDs

ACT/LINK LED    SPEED LED



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

## 1.7.4 Rear panel LEDs



LED	Display status	Description
Power LED	ON	System power ON
Location LED	OFF ON	Normal status Location switch is pressed (Press the location switch again to turn off)

## 1.7.5 Q-Code table

Action	PHASE	POST CODE	TYPE	DESCRIPTION
SEC Start up	Security Phase	0x01	Progress	Power on post code
		0x02	Progress	Load BSP microcode
		0x03	Progress	Perform early platform cache Initialization
		0x04	Progress	Set cache as ram for PEI phase
		0x05	Progress	Establish Stack
		0x06	Progress	CPU Early Initialization
Quick VGA	PEI(Pre-EFI initialization) phase	0x10	Progress	PEI Core Entry
		0x11		PEI cache as ram CPU initial
		0x15		NB Initialization before installed memory
		0x19		SB Initialization before installed memory
	VR initialization	0xC8	Progress	Infineon Address
		0xCC		
		0xD4		TI Address
		0xDC		
		0xE0		
		0xE4		
		0xE8		
	0xEC			
	OCMR initialization	0x11	Progress	Enter OCMR Procedures
		0x12		Enter OCMR On S3
		0x13		Check New CPU
		0x14		Check Cmos Fail
		0x16		Check Overclock Fail
		0x18		Prepare Parameters
		0x21		Build Voltage Table
		0x22		Patch Voltage Table
		0x23		Adjust Voltage Table
		0x24		Before Set Voltages
		0x25		Set Voltages
		0x31		Before Set Spread Spectrum
0x32		SetBoltStrapAndFrequencyPei		
0x33		Set Spread Spectrum		
0x34	After Set Frequency			

(continued on the next page)

Action	PHASE	POST CODE	TYPE	DESCRIPTION
Quick VGA	KTI initialization	0xA0	Progress	Initialize KTI input structure
		0xA1		Collect info such as SBSP, Boot Mode, Reset type
		0xA3		Setup up minimum path between SBSP & other sockets
		0xA6		Sync up with PBSPs
		0xA7		Topology discovery and route calculation
		0xA8		Program final route
		0xA9		Program final IO SAD setting
		0xAA		Protocol layer and other Uncore settings
		0xAB		Transition links to full speed operation
		0xAE		Coherency Settings
		0xAF		KTI Complete
	IIO Early initialization	0xE0	Progress	IIO early init
		0xE1		Early Pre-link training setting
		0xE2		IIO Gen3 EQ programming
		0xE3		IIO Link training
		0xE4		IIO Gen3 override
		0xE5		IIO early init exit
		0xE6		IIO late init
		0xE7		PCIe port init
		0xE8		IOAPIC init
		0xE9		VTD init
		0xEA		IOAT init
		0xEB		IIO DFX init
		0xEC		NTB init
		0xED		Security init
		0xEE		IIO late init exit
		0xEF		IIO On ready to boot

(continued on the next page)



Action	PHASE	POST CODE	TYPE	DESCRIPTION
Quick VGA	MRC Memory initialization	0x70	Progress	High Bandwidth Memory
		0x7E		Pipe Sync AP Boot Mode
		0xB0		Detect DIMM Configuration
		0xB1		Initialize clocks for all MemSs
		0xB2		Gather SPD Data
		0xB3		Early Configuration
		0xB4		Check DIMM Ranks
		0xB5		Parallel Mode Dispatch
		0xB6		DDRIO Initialization
		0xB7		DDR Training
		0xB8		Initialize Throttling
		0xB9		Memory Test
		0xBA		Memory Init
		0xBB		Initialize Memory Map
		0xBC		Set RAS Configuration
		0xBD		Get Margin
		0xBE		BIOS SSA Initialization
		0xBF		MRC Done
		0xC1		Check POR Compatibility
		0xC2		Unlock Memory
		0xC3		Check Status
		0xC4		Check XMP
		0xC5		Initialize Memory
		0xC6		Socket DIMM Information
		0xC7		Prep NVDIMM for Training
		0xC9		Setup SVL and Scrambling
		0xCA		Init CMI Credit Programming
		0xCB		Check Ras Support After MemInit
		0xCC		Initialize ADR
		0xCD		Init Structures Late
0xCE	Memory Late			
0xCF	Select Boot Mode			

(continued on the next page)

Action	PHASE	POST CODE	TYPE	DESCRIPTION
Quick VGA	DXE(Driver Execution Environment) phase	0x32	Progress	CPU POST-Memory Initialization
		0x33		CPU Cache Initialization
		0x34		Application Processor(s) (AP) Initialization
		0x35		BSP Selection
		0x36		CPU Initialization
		0x37		Pre-memory NB Initialization
		0x3B		Pre-memory SB Initialization
		0x4F		DXE Initial Program Load(IPL)
		0x60		DXE Core Started
		0x61		DXE NVRAM Initialization
		0x62		SB run-time Initialization
		0x63		CPU DXE Initialization
		0x68		PCI HB Initialization
		0x69		NB DXE Initialization
		0x6A		NB DXE SMM Initialization
		0x70		SB DXE Initialization
		0x71		SB DXE SMM Initialization
		0x72		SB DEVICES Initialization
		0x78		ACPI Module Initialization
0x79	CSM Initialization			
Normal boot	BDS(Boot Device Selection) phase	0x90	Progress	BDS started
		0x91		Connect device event
		0x92		PCI Bus Enumeration
		0x93		PCI Bus Enumeration
		0x94		PCI Bus Enumeration
		0x95		PCI Bus Enumeration
		0x96		PCI Bus Enumeration
		0x97		Console output connect event
		0x98		Console input connect event
		0x99		AMI Super IO start
		0x9A		AMI USB Driver Initialization

(continued on the next page)

Action	PHASE	POST CODE	TYPE	DESCRIPTION
Normal boot	BDS(Boot Device Selection) phase	0x9B	Progress	AMI USB Driver Initialization
		0x9C		AMI USB Driver Initialization
		0x9D		AMI USB Driver Initialization
		0xA0		AHCI Initialization
		0xA1		AHCI Initialization
		0xA2		AHCI Initialization
		0xA3		AHCI Initialization
		0xA8		BIOS Setup password verify
		0xA9		BIOS Setup start
		0xAB		BIOS Setup input wait
		0xAD		Ready to Boot event
		0xAE		Legacy Boot event
		0xAF		Exit Boot Services
		0xB2		Legacy Option ROM Initialization
		0xB3		Reset system
		0xB4		USB Hotplug
		0xB5		PCI Bus Hotplug
0xB6	NVRAM clean up			
0xB7	NVRAM configuration reset			



# Hardware Information

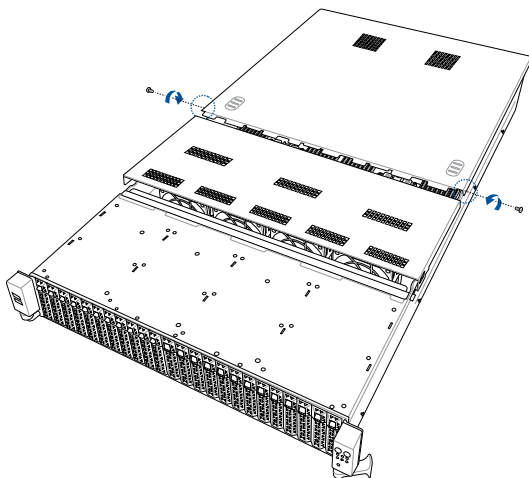
# 2

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

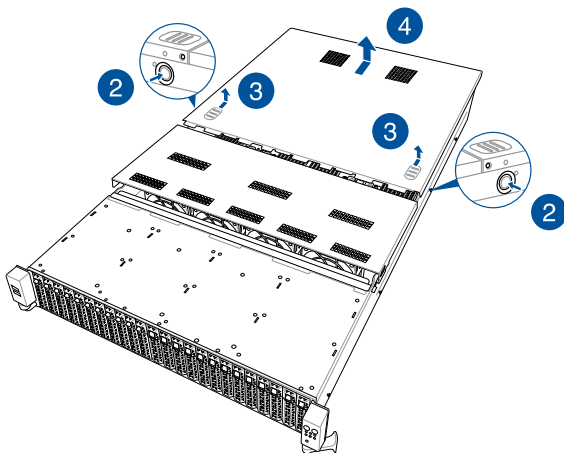
## 2.1 Chassis cover

### Removing the rear cover

1. Remove the two (2) screws on both sides of the rear cover with a Phillips screwdriver.

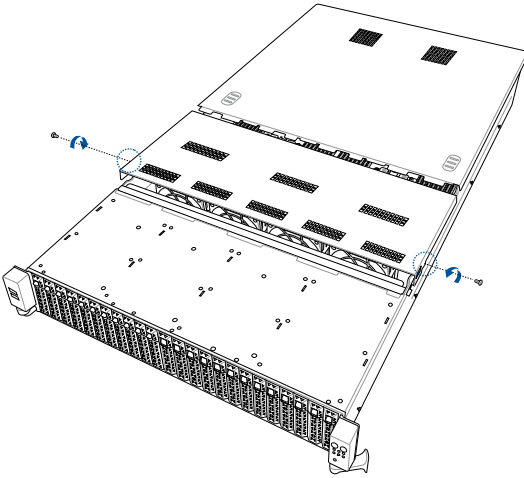


2. Push the buttons on both sides to release the rear cover from the chassis.
3. Slide the rear cover towards the rear panel to disengage it from the chassis.
4. Lift the rear cover from the chassis.

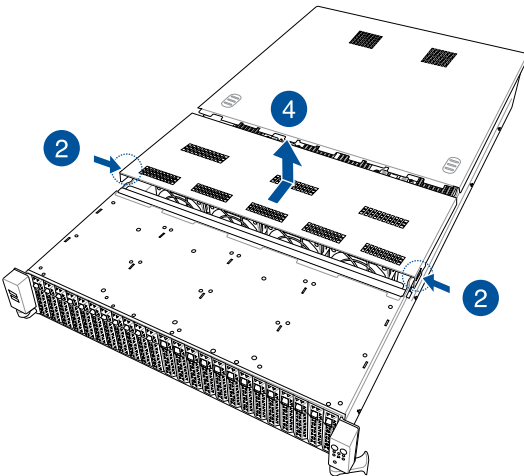


## Removing the mid cover

1. Remove the two (2) screws on both sides of the mid cover with a Phillips screwdriver.



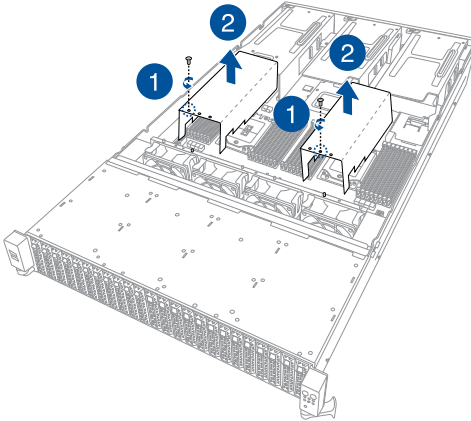
2. Push the buttons on both sides to release the mid cover from the chassis.
3. Slide the mid cover towards the rear panel to disengage it from the chassis.
4. Lift the mid cover from the chassis.



## 2.2 Air ducts

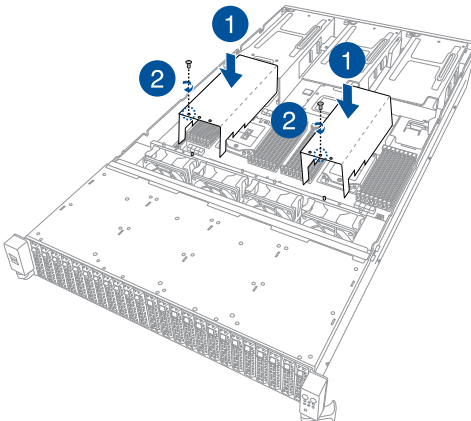
To remove the air ducts:

1. Remove the two (2) screws from the chassis.
2. Gently lift the air ducts vertically out of the chassis.



To install the air ducts:

1. Align the air ducts along the edges of the DIMM slots, then place the air ducts in the chassis, and ensure they are fitted firmly into the chassis.
2. Secure the air ducts to the chassis with the two (2) screws.





## 2.3 Central Processing Unit (CPU)

The motherboard comes with a surface mount Socket P+ designed for the 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 Socket P+.
- The product warranty does not cover damage to the socket contacts resulting from incorrect CPU installation/removal, or misplacement/loss/incorrect removal of the PnP cap.

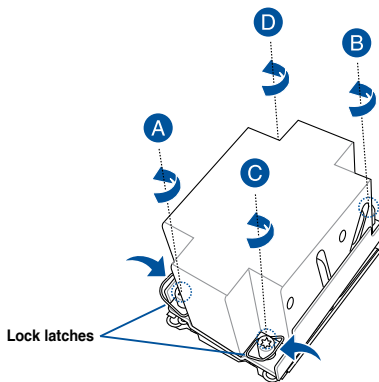
### 2.3.1 Removing the CPU and heatsink (for Standard model)

To install the CPU and heatsink:

1. Remove the rear cover. For more information, refer to **Chassis cover**.
2. Remove the air ducts. For more information, refer to **Air ducts**.
3. Push the lock latches inwards on all four corners of the heatsink, then slightly twist each of the heatsink screws counterclockwise in the order shown on the illustration to loosen the heatsink.



Intel® recommends a torque value of 8 lbf-in to prolong the longevity of all PEEK nuts after the quality of the load post is corrected.



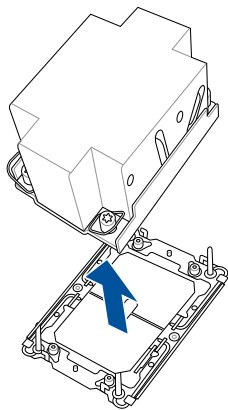
4. Completely loosen all the screws on the heatsink, then lift and remove it from the motherboard.



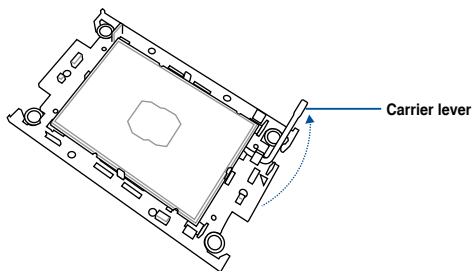
---

Intel® recommends a torque value of 8 lbf-in to prolong the longevity of all PEEK nuts after the quality of the load post is corrected.

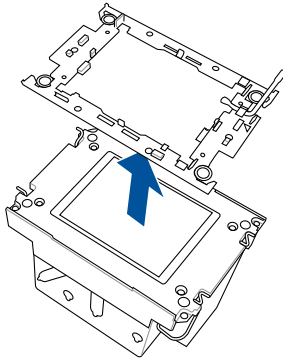
---



5. Flip the heatsink over to reveal the CPU and carrier bracket. Flip the carrier lever over to release the CPU, then remove the CPU from the heatsink and carrier assembly.



6. Remove the carrier bracket from the heatsink.



## 2.3.2 Removing the CPU and heatsink (for GPU model)

To install the CPU and heatsink:

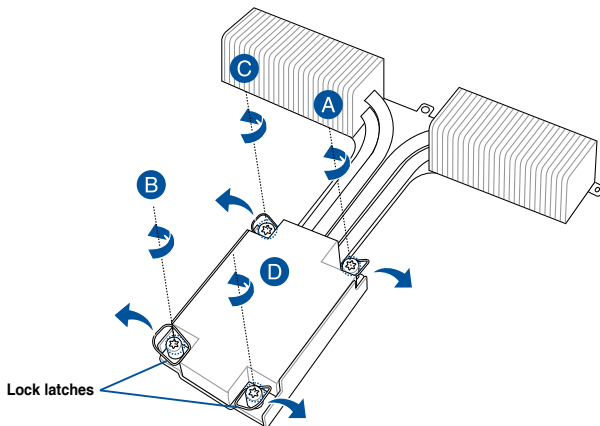
1. Remove the rear cover. For more information, refer to **Chassis cover**.
2. Remove the air ducts. For more information, refer to **Air ducts**.
3. Push the lock latches inwards on all four corners of the heatsink, then slightly twist each of the heatsink screws counterclockwise in the order shown on the illustration to loosen the heatsink.



---

Intel® recommends a torque value of 8 lbf-in to prolong the longevity of all PEEK nuts after the quality of the load post is corrected.

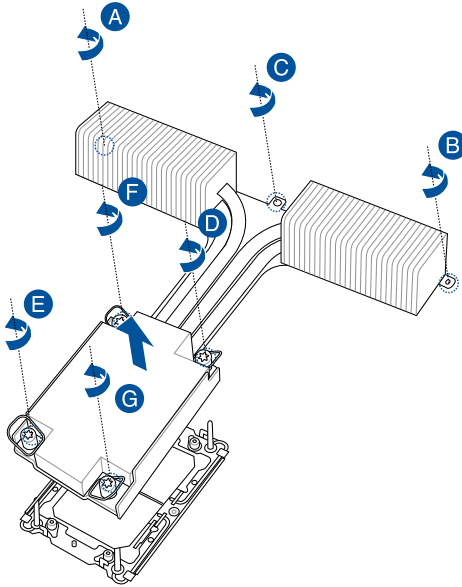
---



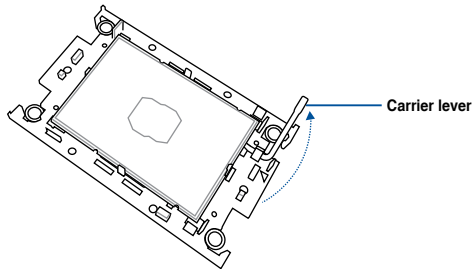
4. Completely loosen all the screws on the heatsink, then lift and remove it from the motherboard.



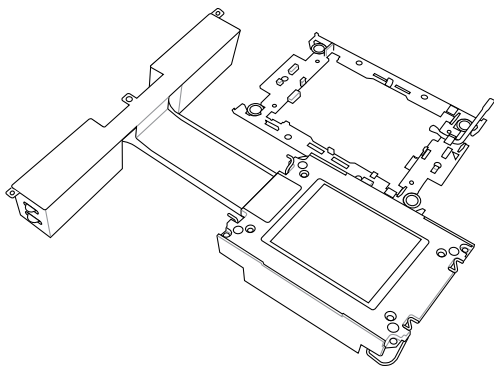
Intel® recommends a torque value of 8 lbf-in to prolong the longevity of all PEEK nuts after the quality of the load post is corrected.



5. Flip the heatsink over to reveal the CPU and carrier bracket. Flip the carrier lever over to release the CPU, then remove the CPU from the heatsink and carrier assembly.

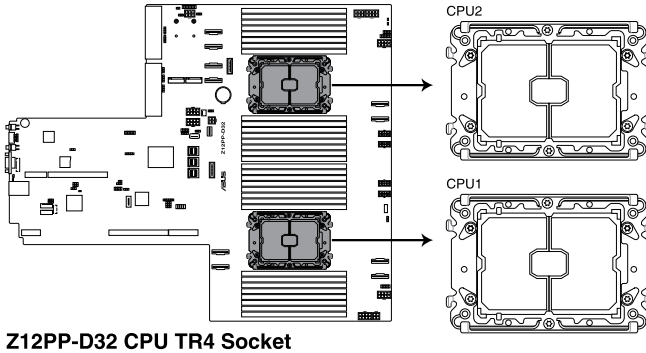


6. Remove the carrier bracket from the heatsink.

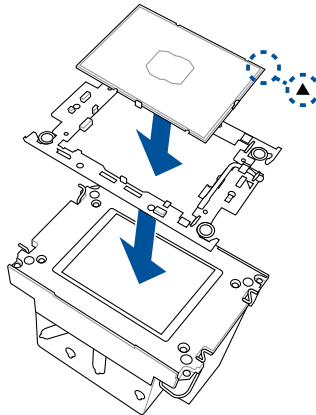


### 2.3.3 Installing the CPU and heatsink

1. Remove the air duct. For more information, refer to the **Air ducts** section.
2. Locate the CPU sockets on your motherboard.



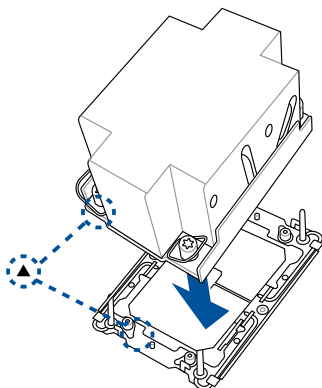
3. Attach the CPU to the carrier bracket, ensure the triangle mark is on the same side as the bracket lever, then attach the CPU and carrier to the heatsink.



4. Remove the PNP cap from the CPU socket.
5. Align the heatsink and CPU assembly to the CPU socket, then place the heatsink on top of the CPU socket.



- 
- Ensure the triangle mark on the CPU is located in the same corner as the CPU socket.
  - The heatsink is symmetrical.
- 





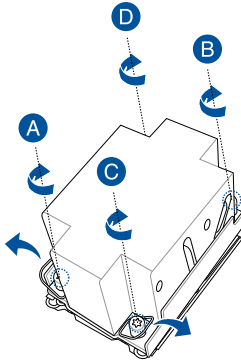
6. Push the lock latches outwards on all four corners of the heatsink, then do two (2) clockwise turns on each of the heatsink screws in the cross order pattern shown on the illustration until the heatsink screws are tightened and the heatsink is secured onto the motherboard.



---

Intel® recommends a torque value of 8 lbf-in to prolong the longevity of all PEEK nuts after the quality of the load post is corrected.

---



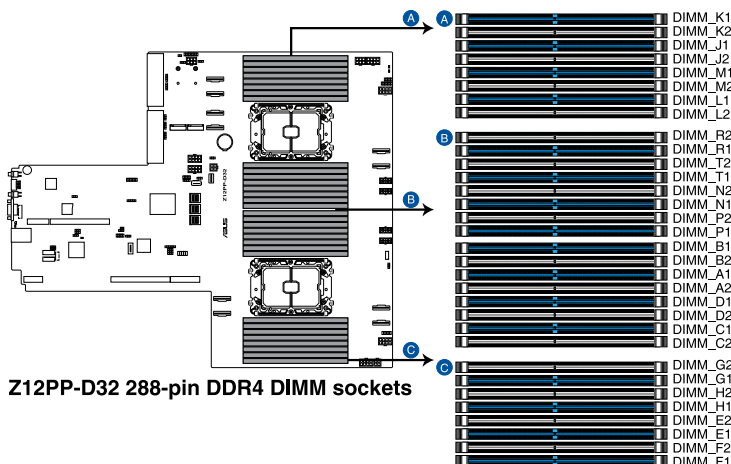
7. Replace the air duct. For more information, refer to the **Air ducts** section.

## 2.4 System memory

### 2.4.1 Overview

The motherboard comes with 32 Double Data Rate 4 (DDR4) Dual Inline Memory Modules (DIMM) sockets.

The figure illustrates the location of the DDR4 DIMM sockets:



### 2.4.2 Memory Configurations

You may install 16GB, 32GB, and 64GB RDIMMs; 64GB and 128GB LRDIMM; or 64GB, 128GB, 256GB LRDIMM 3DS / 3DS RDIMM into the DIMM sockets. If you are not sure on which slots to install the DIMMS, you can use the recommended memory configuration in this section for reference.



- 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.
- Start installing the DIMMs into the second slots (such as DIMM\_A2 , DIMM\_B2, etc.)

Recommended dual CPU configuration						
	DIMMs					
	2	4	8	12	16	32
DIMM_F1				•	•	•
DIMM_F2						•
DIMM_E1			•	•	•	•
DIMM_E2						•
DIMM_H1					•	•
DIMM_H2						•
DIMM_G1			•	•	•	•
DIMM_G2						•
DIMM_C2						•
DIMM_C1		•	•	•	•	•
DIMM_D2						•
DIMM_D1					•	•
DIMM_A2						•
DIMM_A1	•	•	•	•	•	•
DIMM_B2						•
DIMM_B1				•	•	•
DIMM_P1				•	•	•
DIMM_P2						•
DIMM_N1			•	•	•	•
DIMM_N2						•
DIMM_T1					•	•
DIMM_T2						•
DIMM_R1			•	•	•	•
DIMM_R2						•
DIMM_L2						•
DIMM_L1		•	•	•	•	•
DIMM_M2						•
DIMM_M1					•	•
DIMM_J2						•
DIMM_J1	•	•	•	•	•	•
DIMM_K2						•
DIMM_K1				•	•	•

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

Channel	F		E		H		G	
DDR4+BPS	DIMM_F1	DIMM_F2	DIMM_E1	DIMM_E2	DIMM_H1	DIMM_H2	DIMM_G1	DIMM_G2
4+4	BPS		DDR4		BPS		DDR4	
	DDR4		BPS		DDR4		BPS	
6+1	DDR4		DDR4		DDR4		DDR4	
	DDR4		DDR4		BPS		DDR4	
	BPS		DDR4		DDR4		DDR4	
8+1	DDR4		DDR4		DDR4		DDR4	
	DDR4		DDR4		DDR4		DDR4	
	DDR4		DDR4	BPS	DDR4		DDR4	
	DDR4		DDR4		DDR4		DDR4	BPS
8+4	DDR4		DDR4	BPS	DDR4		DDR4	BPS
8+8	DDR4	BPS	DDR4	BPS	DDR4	BPS	DDR4	BPS
12+2	BPS		DDR4	DDR4	DDR4	DDR4	DDR4	DDR4
	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	BPS	

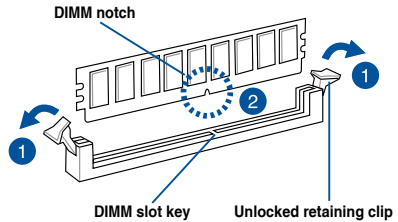
Channel	C		D		A		B	
DDR4+BPS	DIMM_C2	DIMM_C1	DIMM_D2	DIMM_D1	DIMM_A2	DIMM_A1	DIMM_B2	DIMM_B1
4+4		DDR4		BPS		DDR4		BPS
		BPS		DDR4		BPS		DDR4
6+1		DDR4		BPS		DDR4		DDR4
		DDR4		DDR4		DDR4		BPS
		DDR4				DDR4		DDR4
		DDR4		DDR4		DDR4		
8+1		DDR4		DDR4	BPS	DDR4		DDR4
	BPS	DDR4		DDR4		DDR4		DDR4
		DDR4		DDR4		DDR4		DDR4
		DDR4		DDR4		DDR4		DDR4
8+4	BPS	DDR4		DDR4	BPS	DDR4		DDR4
8+8	BPS	DDR4	BPS	DDR4	BPS	DDR4	BPS	DDR4
12+2	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4		BPS
		BPS	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4

## 2.4.3 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.

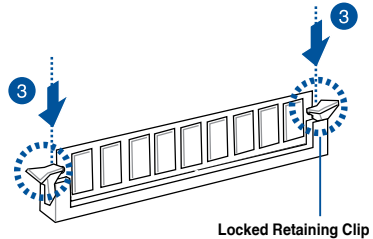
1. Unlock a DIMM socket by pressing the retaining clip outward.
2. Align a DIMM on the socket such that the notch on the DIMM matches the DIMM slot key on the socket.



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

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

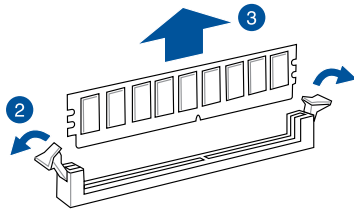
Ensure that the DIMM is sitting firmly on the DIMM slot.



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

## 2.4.4 Removing a DIMM

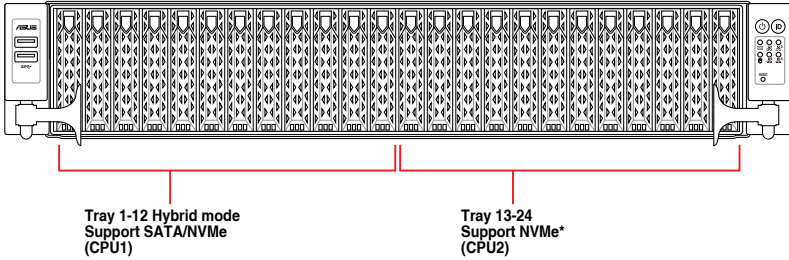
1. Remove the top cover. For more information, see the section 2.1 **Chassis cover**.
2. Simultaneously press the retaining clips outward to unlock the DIMM.
3. Remove the DIMM from the socket.



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

## 2.5 Storage devices

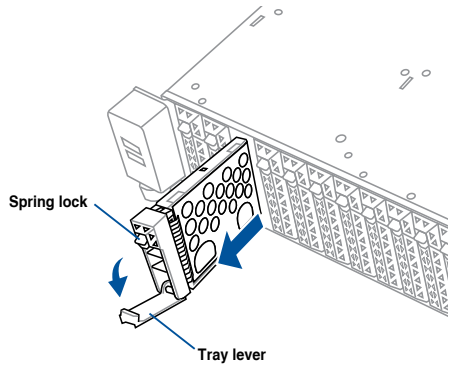
The system supports twenty-four (24) 2.5" hot-swap SATA/SAS/NVMe storage devices (up to 12 x NVMe/SATA + 12 x NVMe). The storage device installed on the storage tray connects to the motherboard SATA/SAS/NVMe ports via the SATA/SAS/NVMe backplane.



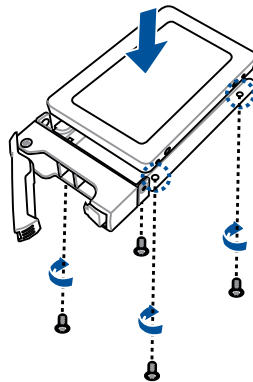
- Select Pike/Storage card for additional SATA/SAS support on Tray 9-24.
- **CPU 1 Support:** 12 x NVMe (Tray1-12).
- **CPU 2 Support:** 12 x NVMe (Tray13-24) with 2 CB boards (on selected models).

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

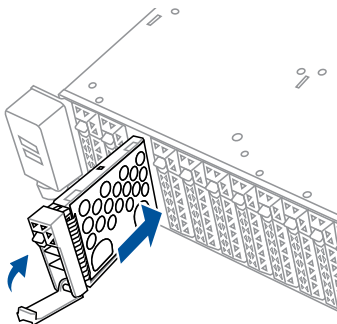
1. Press the spring lock then pull the tray lever outward to release the storage device tray. The storage device tray ejects slightly after you pull out the lever.
2. Firmly hold the tray lever and pull the storage device tray out of the bay.



3. Prepare the 2.5" storage device and the bundled set of screws.
4. Place the 2.5" storage device into the storage device tray then secure it with four screws.



5. Push the storage device tray and storage device assembly all the way into the depth of the bay until the tray lever and spring lock clicks and secures the storage device tray in place.

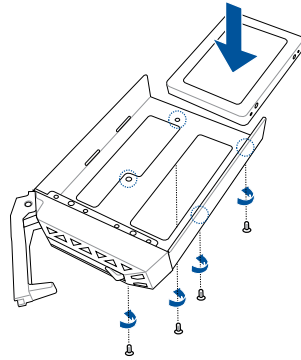


- 
- When installed, the SATA/SAS/NVMe connector on the storage device connects to the SATA/SAS/NVMe interface on the backplane.
  - The storage device tray is correctly placed when its front edge aligns with the bay edge.
- 

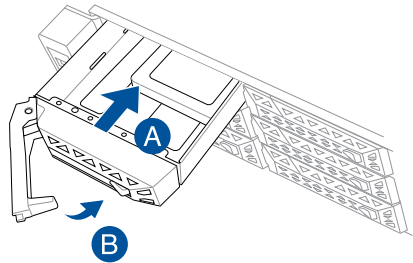
6. Repeat steps 1 to 5 to install the other SATA/SAS/NVMe storage devices.



3. Place the storage device tray on a flat and stable surface.
4. Prepare the 2.5" storage device and the bundled set of screws.
5. Place the 2.5" storage device into the tray then secure it with four screws.

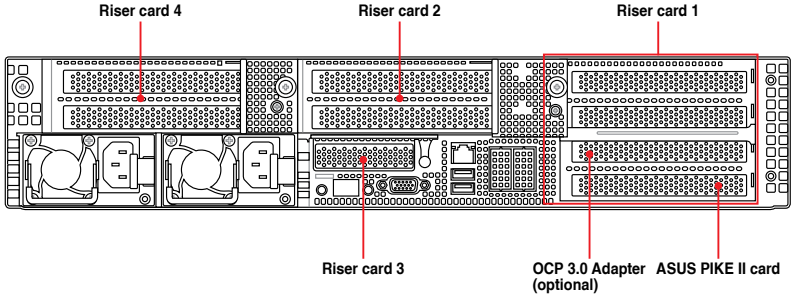


6. Carefully insert the tray and push it all the way to the depth of the bay (A). Lock the secure tab to secure the drive tray in place (B).
7. Repeat steps 1 to 6 to install the other 2.5" storage devices.



## 2.6 Expansion slot

The barebone server comes with four pre-installed riser cards to support nine PCIe slots.



### Riser card bracket 1

Riser card bracket 1 supports PCIe Gen4 slots 1-4 top to bottom.

PCIe slot	Operation mode	
Slot 1	x8	x16
Slot 2	x8	N/A
Slot 3	x16	OCP 3.0
Slot 4	x8 (ASUS PIKE II card)	x8 (ASUS PIKE II card)

### Riser card bracket 2

Riser card bracket 2 supports PCIe Gen4 slots 5-6 top to bottom. Slot 5 can be auto-switch to x16 mode when x16 card is populated whereas slot 6 will be disabled.

PCIe slot	Operation mode	
Slot 5	x8	x16
Slot 6	x8	N/A

### Riser card bracket 3

Riser card bracket 3 supports PCIe Gen4 slots 9. If M.2 is in use, Slot 9 will operate at x8 mode.

PCIe slot	Operation mode	
Slot 9	x16/x8	

### Riser card bracket 4

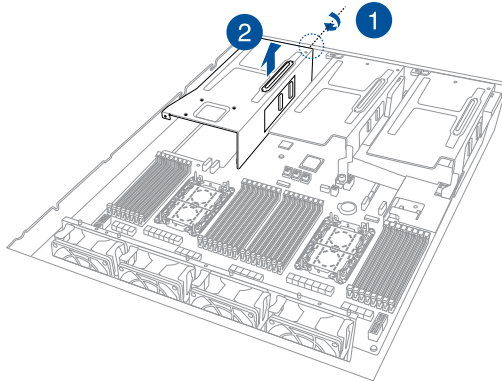
Riser card bracket 4 supports PCIe Gen4 slots 7-8 top to bottom. Slot 7 can be auto-switch to x16 mode when x16 card is populated whereas slot 8 will be disabled.

PCIe slot	Operation mode	
Slot 7	x8	x16
Slot 8	x8	N/A

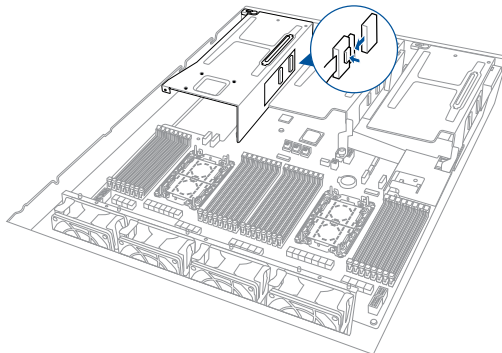
## 2.6.1 Installing an expansion card to riser card bracket 1

To install an expansion card to the riser card bracket 1:

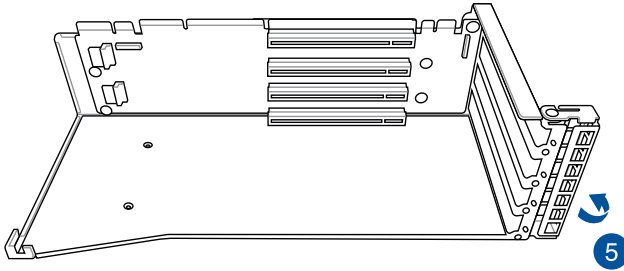
1. Loosen the thumbscrew securing the riser card bracket to the chassis.
2. Lift the riser card out of the chassis by firmly holding it by the tab and pulling it upwards to detach it from the PCIe slot on the motherboard.



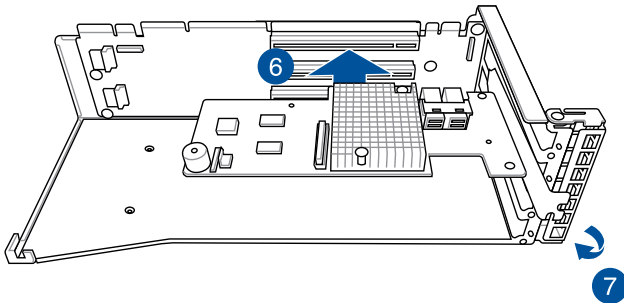
3. Remove the cable from the riser card bracket.



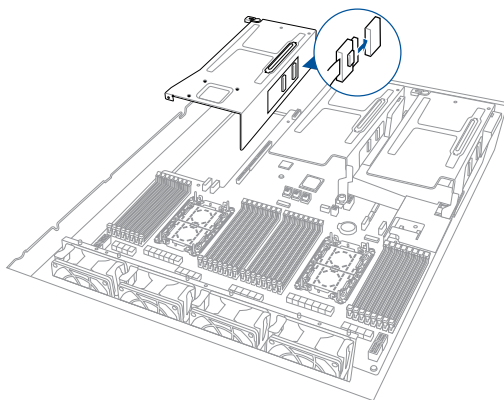
4. Place the riser card bracket on a flat and stable surface in the orientation as shown.
5. Flip the metal bracket lock open.



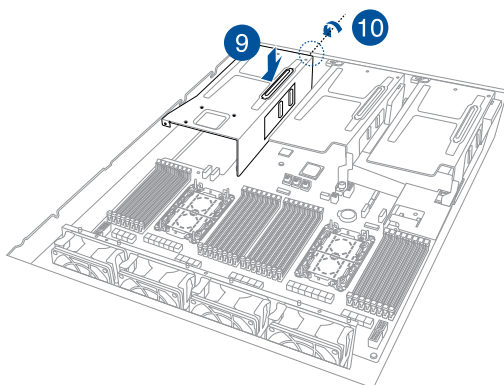
6. Install the PCIe expansion card into the riser card bracket.
7. Flip the metal bracket lock back to secure the PCIe expansion card to the riser card bracket.



8. Reconnect the cable to the riser card bracket.



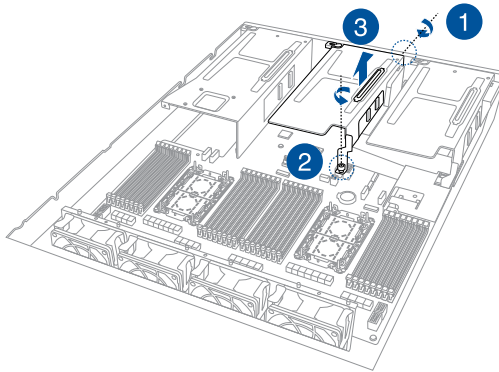
9. Reinstall the riser card to the motherboard.
10. Secure the riser card bracket to the chassis with the thumbscrew.



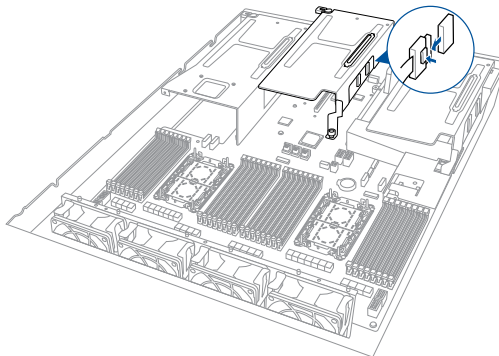
## 2.6.2 Installing an expansion card to riser card bracket 2

To install an expansion card on the riser card bracket 2:

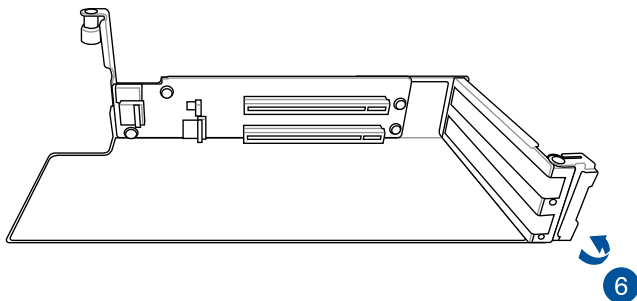
1. Loosen the thumbscrew securing the riser card bracket to the chassis.
2. Loosen the thumbscrew securing the riser card to the motherboard.
3. Lift the riser card out of the chassis by firmly holding it by the tab and pulling it upwards to detach it from the PCIe slot on the motherboard.



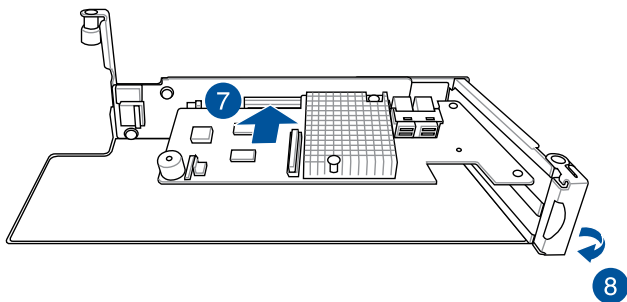
4. Remove the cable from the riser card bracket.



5. Place the riser card bracket on a flat and stable surface in the orientation as shown.
6. Flip the metal bracket lock open.

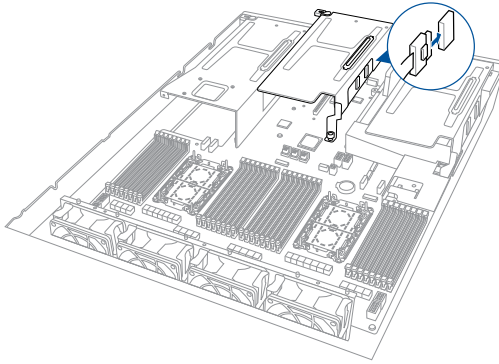


7. Install the PCIE expansion card into the riser card bracket.
8. Flip the metal bracket lock back to secure the PCIE expansion card to the riser card bracket.

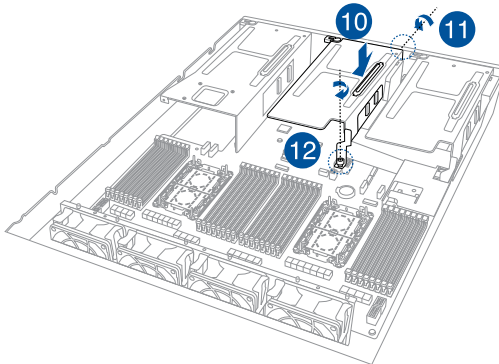




9. Reconnect the cable to the riser card bracket.



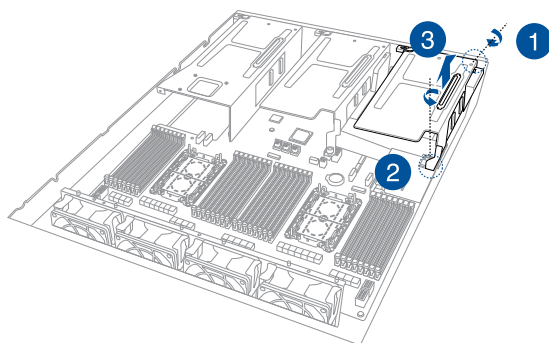
10. Reinstall the riser card to the motherboard.
11. Secure the riser card bracket to the chassis with the thumbscrew.
12. Secure the riser card to the motherboard with the thumbscrew.



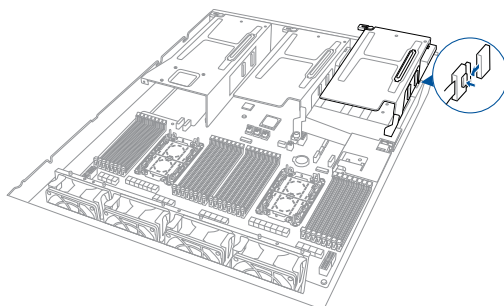
## 2.6.3 Installing an expansion card to riser card bracket 3

To install an expansion card on the riser card bracket 3:

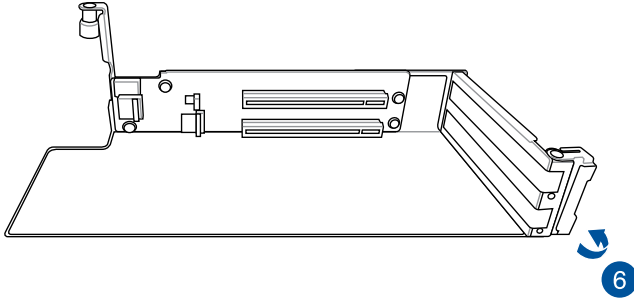
1. Loosen the thumbscrew securing the riser card bracket to the chassis.
2. Loosen the thumbscrew securing the riser card to the motherboard.
3. Lift the riser card out of the chassis by firmly holding it by the tab and pulling it upwards to detach it from the PCIe slot on the motherboard.



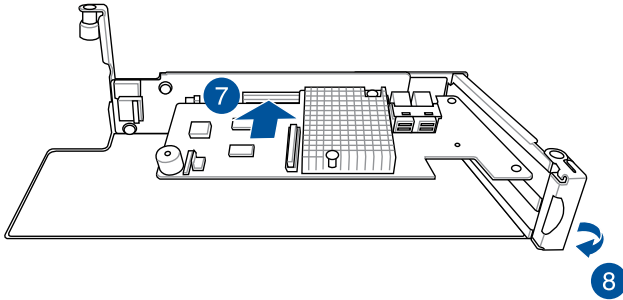
4. Remove the cable from the riser card bracket.



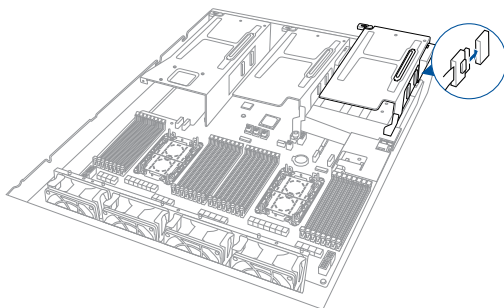
5. Place the riser card bracket on a flat and stable surface in the orientation as shown.
6. Flip the metal bracket lock open.



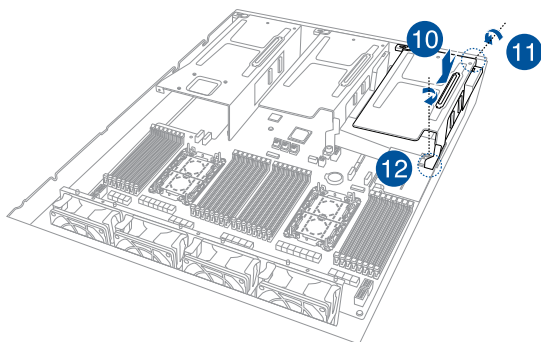
7. Install the PCIe expansion card into the riser card bracket.
8. Flip the metal bracket lock back to secure the PCIe expansion card to the riser card bracket.



9. Reconnect the cable to the riser card bracket.



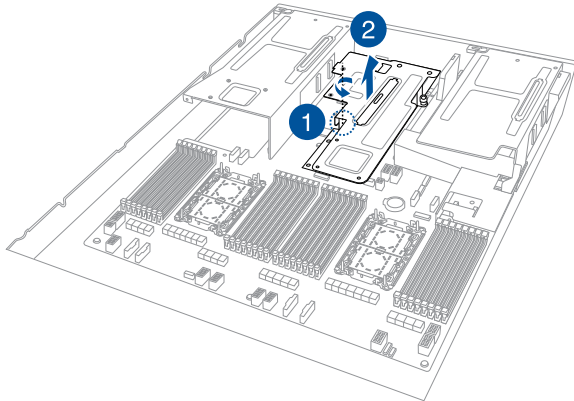
10. Reinstall the riser card to the motherboard.
11. Secure the riser card bracket to the chassis with the thumbscrew.
12. Secure the riser card to the motherboard with the thumbscrew.



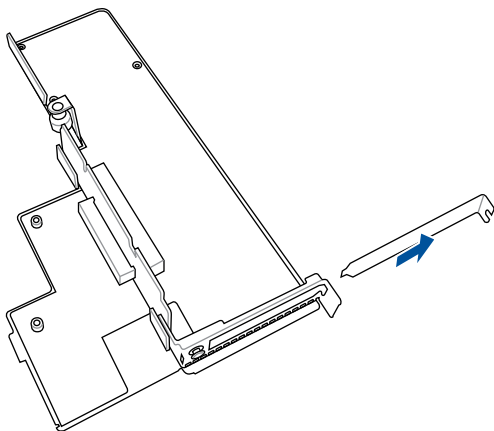
## 2.6.4 Installing an expansion card to riser card bracket 4

To install an expansion card to the riser card bracket 4:

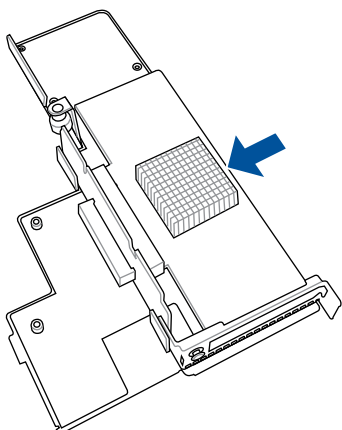
1. Loosen the thumbscrew securing the riser card bracket to the chassis.
2. Lift the riser card out of the chassis by firmly holding it by the tab and pulling it upwards to detach it from the PCIe slot on the motherboard.



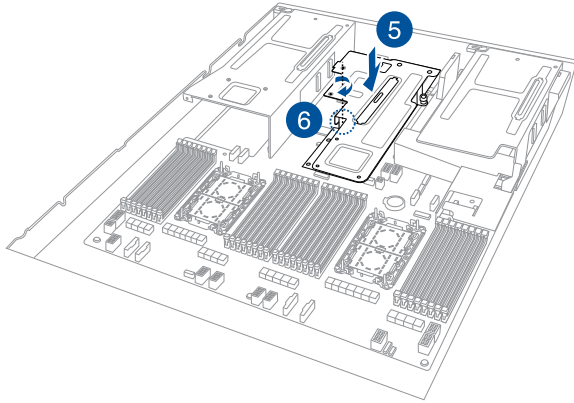
3. Flip the riser card bracket over and remove metal bracket.



4. Install the expansion card to your riser card bracket.



5. Reinstall the riser card to the motherboard.
6. Secure the riser card bracket to the chassis with the thumbscrew.



## 2.6.5 Installing an OCP 3.0 slot baseboard and OCP 3.0 card to the riser card bracket

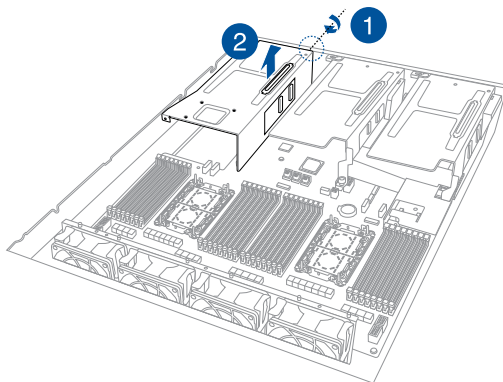


---

We recommend you install the OCP 3.0 slot baseboard to the PCIe2 slot on the riser card bracket 1.

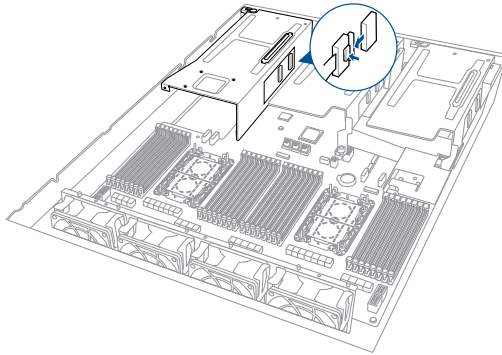
---

1. Loosen the thumbscrew securing the riser card bracket to the chassis.
2. Lift the riser card out of the chassis by firmly holding it by the tab and pulling it upwards to detach it from the PCIe slot on the motherboard.

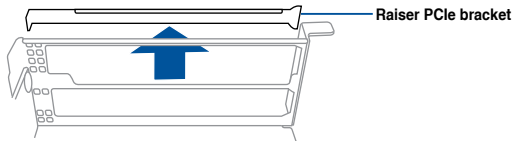




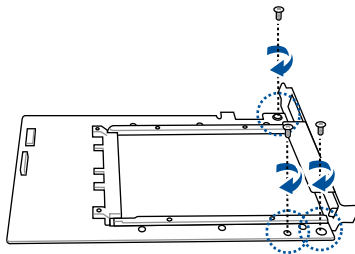
3. Remove the cable from the riser card bracket.



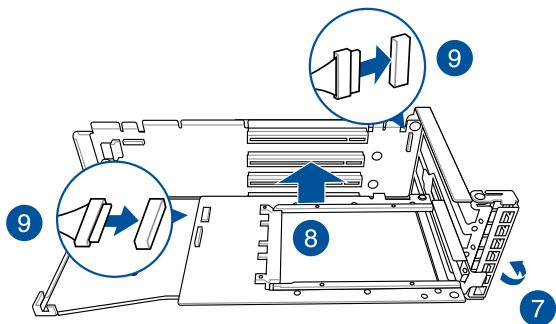
4. Remove the Raiser PCIe bracket.



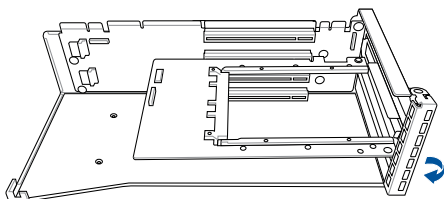
5. Install the bundled OCP 3.0 bracket to the OCP 3.0 slot baseboard using the three (3) bundled screws.



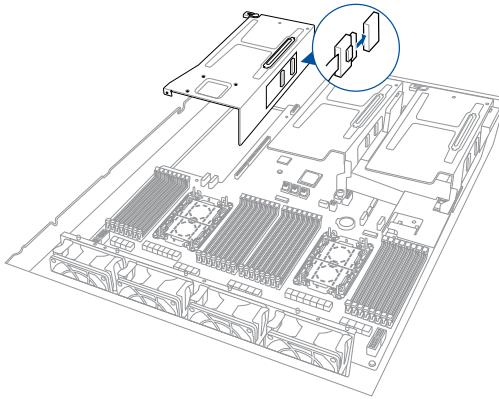
6. Place the riser card bracket on a flat and stable surface in the orientation as shown.
7. Flip the metal bracket lock open.
8. Install the OCP 3.0 slot baseboard to the **PCIE2** slot on the riser card bracket.
9. Connect the cables.



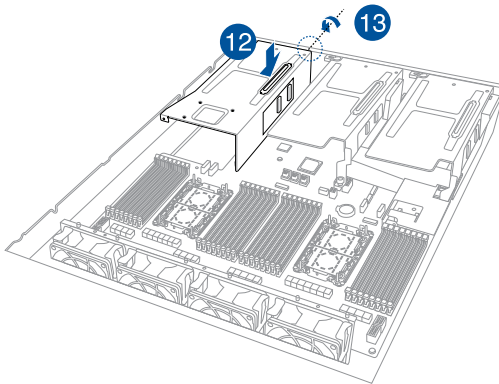
10. Once your OCP 3.0 card is installed, flip the metal bracket lock back to secure the OCP 3.0 slot baseboard to the riser card bracket.



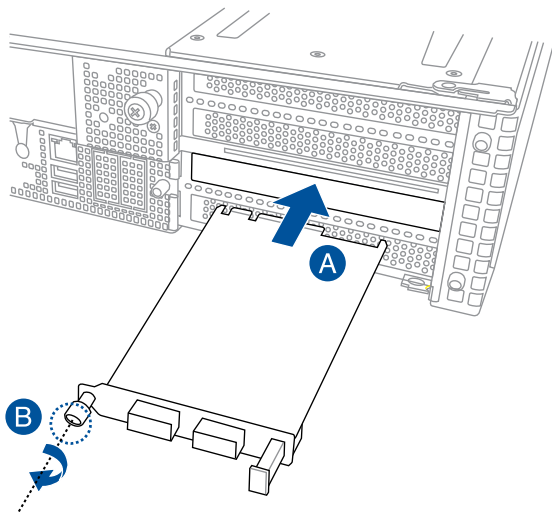
11. Reconnect the cable to the riser card bracket.



12. Reinstall the riser card to the motherboard.
13. Secure the riser card bracket to the chassis with the thumbscrew.



14. Insert the OCP 3.0 card to the OCP 3.0 slot from the rear of the system (A), and make sure the OCP 3.0 card is seated securely in the OCP 3.0 slot, then secure it using the thumbscrew (B).



## 2.6.6 Installing an ethernet expansion card to the riser card bracket

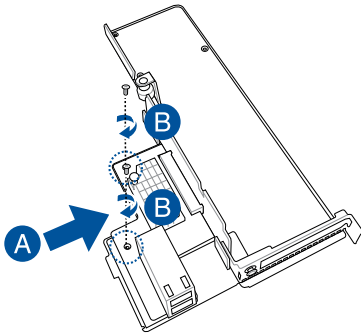
The pre-installed riser card bracket can support a 4-port or 2-port ethernet expansion card.



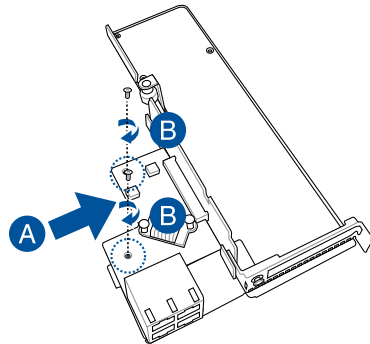
Do not install the 4-port ethernet expansion card if you wish to install the external rear fan.

To install a 4-port or 2-port ethernet expansion card on the riser card bracket:

1. Follow steps 1-2 of **Installing an expansion card to the riser card bracket 4** to remove the riser card bracket from the chassis.
2. Flip the riser card bracket over and insert the 4-port or 2-port ethernet expansion card to the **PCI\_E\_LAN1** slot (A) on the riser card bracket, then secure it using two (2) screws (B).



2-port Ethernet expansion card



4-port Ethernet expansion card

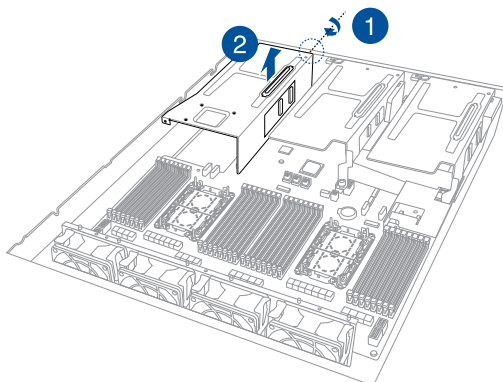
3. Follow steps 5-6 of **Installing an expansion card to the riser card bracket 4** to install the riser card bracket to the chassis.

## 2.6.7 Installing an ASUS PIKE II card

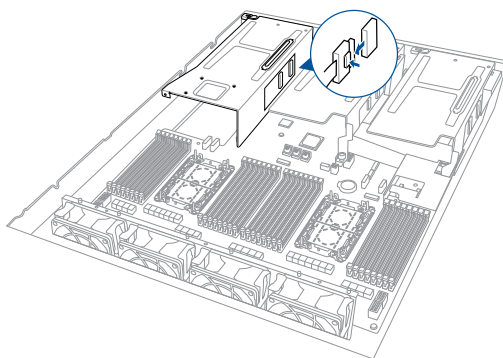
You can replace the pre-installed ASUS PIKE II card to support SAS storage devices in your server system.

To remove the pre-installed ASUS PIKE II card:

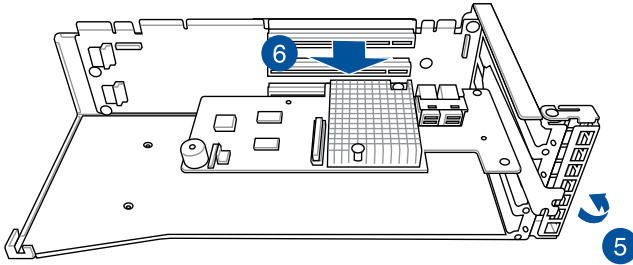
1. Loosen the thumbscrew securing the riser card bracket to the chassis.
2. Lift the riser card out of the chassis by firmly holding it by the tab and pulling it upwards to detach it from the PCIe slot on the motherboard.



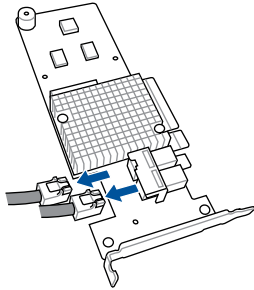
3. Remove the cable from the riser card bracket.



4. Place the riser card bracket on a flat and stable surface in the orientation as shown.
5. Flip the metal bracket lock open.
6. Remove the ASUS PIKE II card from the riser card bracket.

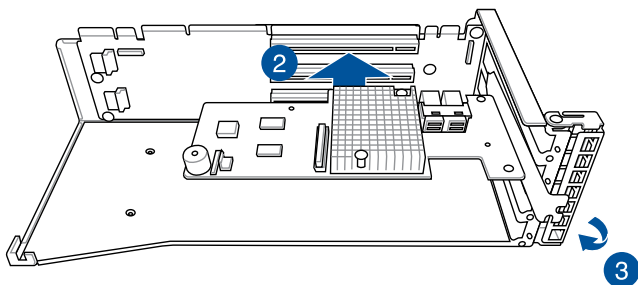


7. Remove the mini SAS HD cables from the ASUS PIKE II card.

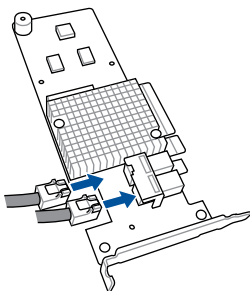


To install an ASUS PIKE II card:

1. Prepare the new ASUS PIKE II card.
2. Insert the ASUS PIKE II card to the PCIe slot on the riser card bracket.
3. Flip the metal bracket lock back to secure the ASUS PIKE II card to the riser card bracket.

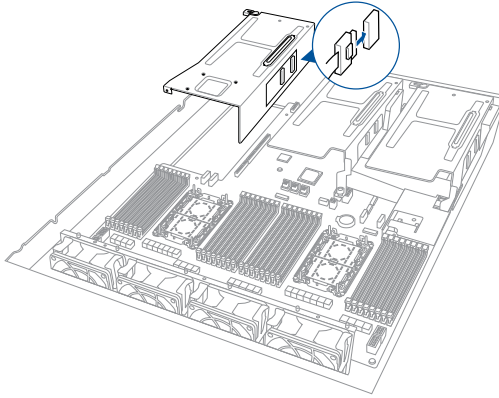


4. Connect the mini SAS HD cables to the ASUS PIKE II card.

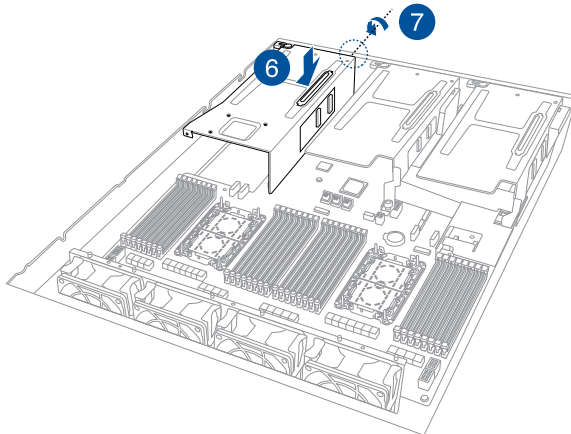




5. Reconnect the cable to the riser card bracket.



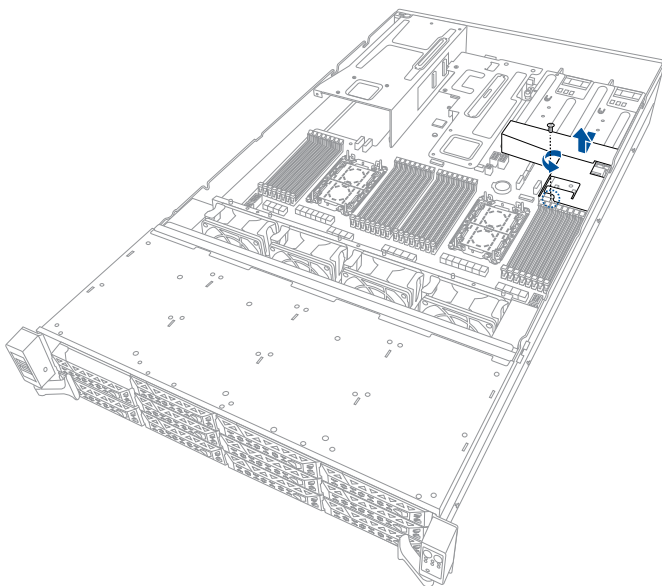
6. Reinstall the riser card to the motherboard.
7. Secure the riser card bracket to the chassis with the thumbscrew.



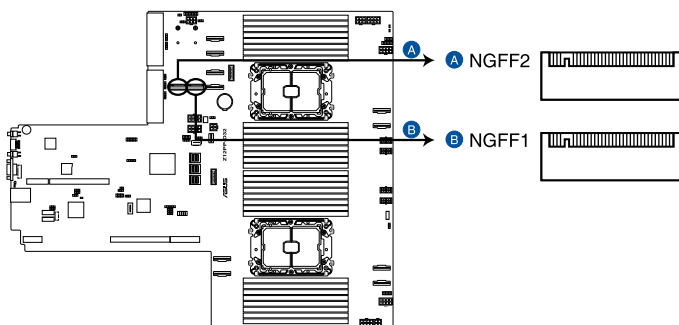
## 2.6.8 Installing M.2 (NGFF) cards

You may install an M.2 card (supports 2260, 2280) to the onboard M.2 (NGFF) slot on the motherboard. To install an M.2 (NGFF) card:

1. Remove the riser card bracket. Please refer to **Installing an expansion card to riser card bracket 3** for more information.
2. Remove the screw securing the PSU air duct then remove the air duct.

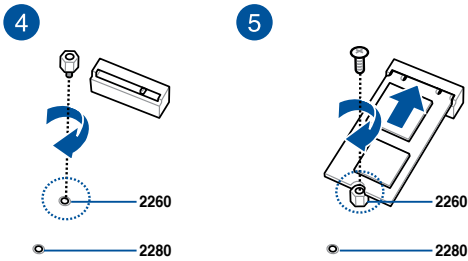


3. Locate the M.2 connectors (NGFF1 or NGFF2) on the motherboard.

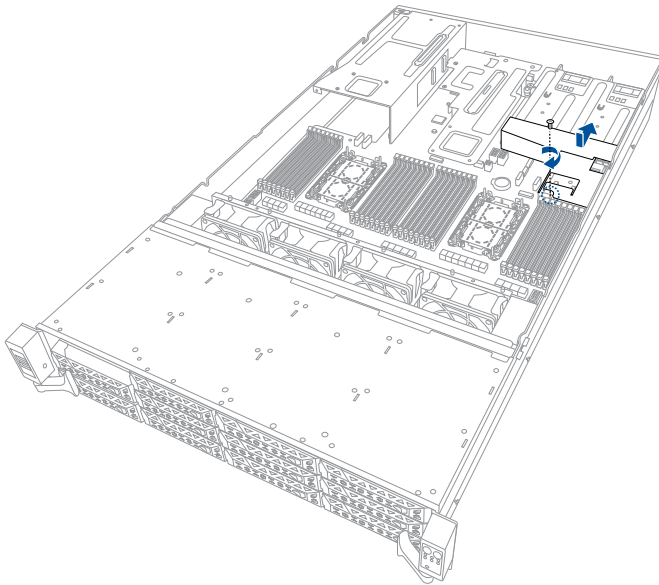


**Z12PP-D32 NGFF connectors**

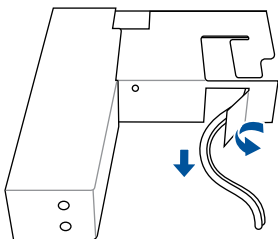
4. Select an appropriate screw hole on the motherboard for your M.2 card, then secure the stand to the motherboard.
5. Insert the M.2 into the M.2 (NGFF) slot, then secure it using the bundled screw.



6. Replace the PSU air duct, then secure it using the screw removed previously.



7. Ensure the cabling is organized so that the cables are directed out of the PSU air duct.



## 2.6.9 Configuring an expansion card

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

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

### Standard Interrupt assignments

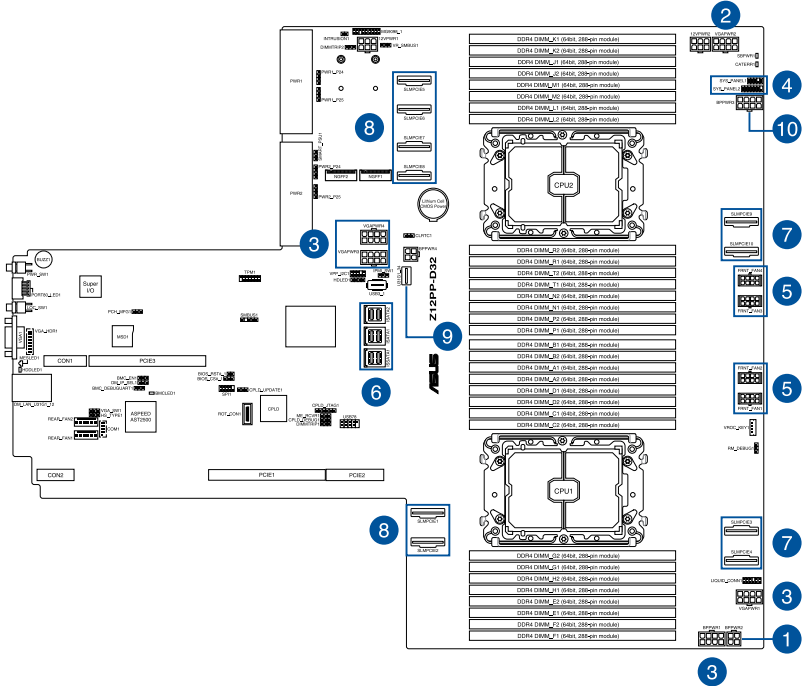
IRQ	Priority	Standard function
0	1	System Timer
1	2	Keyboard Controller
2	-	Programmable Interrupt
3*	11	Communications Port (COM2)
4*	12	Communications Port (COM1)
5*	13	--
6	14	Floppy Disk Controller
7*	15	--
8	3	System CMOS/Real Time Clock
9*	4	ACPI Mode when used
10*	5	IRQ Holder for PCI Steering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

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

## 2.7 Cable connections



- The bundled system cables are pre-connected before shipment. You do not need to disconnect these cables unless you are going to remove pre-installed components to install additional devices.
- Refer to Chapter 4 for detailed information on the connectors.

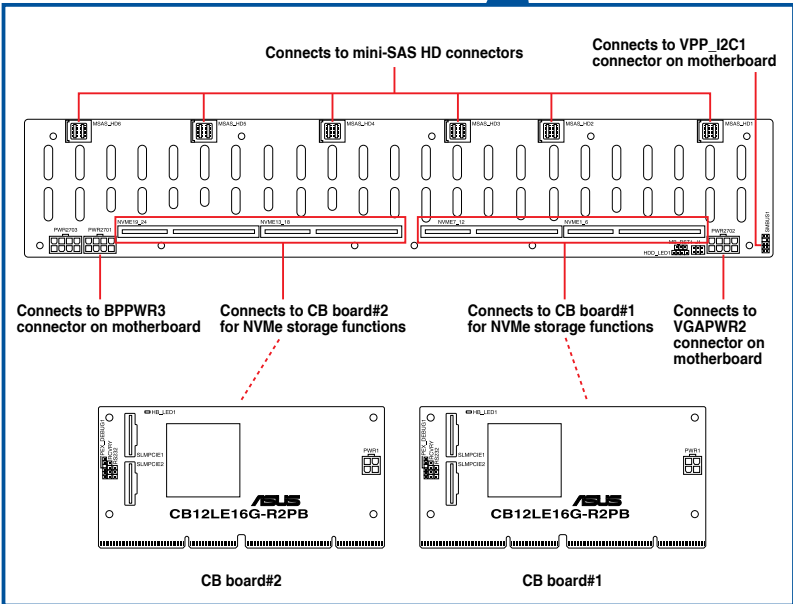
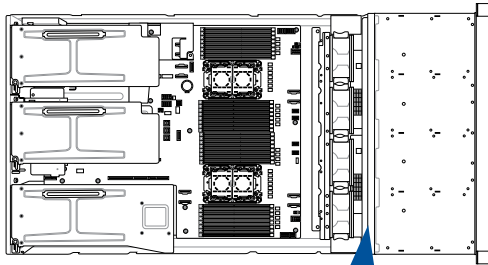


## **Pre-connected system cables**

1. 4-pin BPPWR2 power connector (connected to CB board)
2. 8-pin VGAPWR2 power connector (connected to backplane)
3. 8-pin VGA power connectors (connected to Graphics card, on selected models)
4. Panel connector (connected to CB board)
5. System fan connectors (from motherboard FAN1-4 to Fan board)
6. Mini SAS connectors
7. SLMPCIE3, SLMPCIE4, SLMPCIE9, SLMPCIE10 Slim PCIe connectors (connected to CB board)
8. SLMPCIE1, SLMPCIE2, SLMPCIE5, SLMPCIE6, SLMPCIE7, SLMPCIE8 Slim PCIe connectors (connected to PCIe riser card)
9. USB 3.2 Gen 1 connector (connected to front I/O board)
10. 8-pin BPPWR3 power connector (connected to backplane)

## 2.8 SATA/SAS backplane cabling

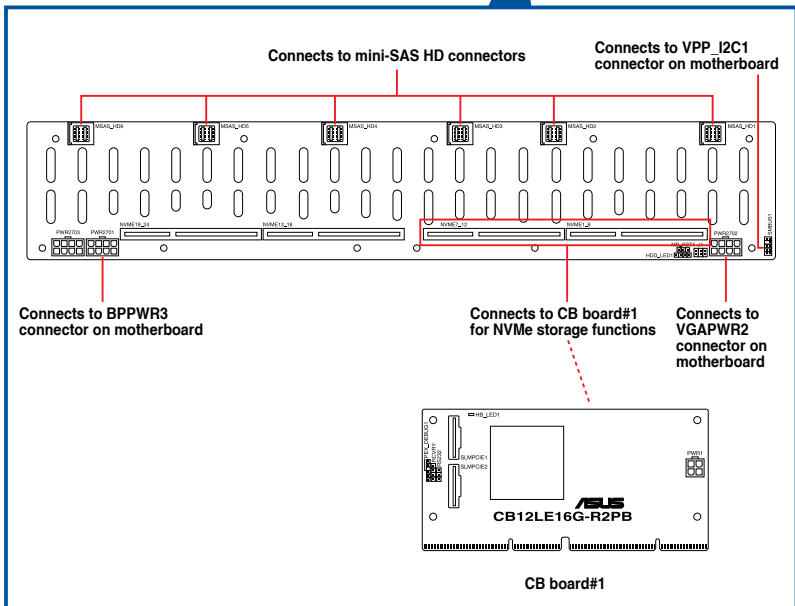
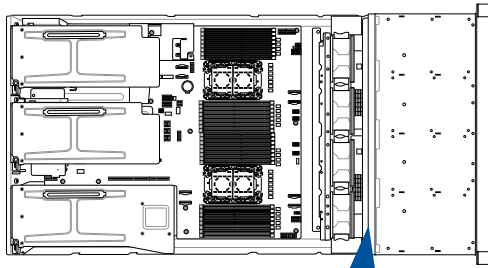
### 24 x NVMe (on selected models)



Backplane connector	Cable	Connect to
SLMPCIE1 (CB Board#1)	Slimline PCIe to Slimline PCIe	SLMPCIE3 on motherboard
SLMPCIE2 (CB Board#1)	Slimline PCIe to Slimline PCIe	SLMPCIE4 on motherboard
SLMPCIE1 (CB Board#2)	Slimline PCIe to Slimline PCIe	SLMPCIE9 on motherboard
SLMPCIE2 (CB Board#2)	Slimline PCIe to Slimline PCIe	SLMPCIE10 on motherboard
MSAS_HD1	Mini-SAS HD to Mini-SAS HD	ISSATA1 on motherboard
MSAS_HD2	Mini-SAS HD to Mini-SAS HD	ISATA1 on motherboard
MSAS_HD3	Mini-SAS HD to Mini-SAS HD	ISATA2 on motherboard



**12 x NVMe (on selected models)**



Backplane connector	Cable	Connect to
SLMPCIE1 (CB Board#1)	Slimline PCIe to Slimline PCIe	SLMPCIE3 on motherboard
SLMPCIE2 (CB Board#1)	Slimline PCIe to Slimline PCIe	SLMPCIE4 on motherboard
MSAS_HD1	Mini-SAS HD to Mini-SAS HD	ISSATA1 on motherboard
MSAS_HD2	Mini-SAS HD to Mini-SAS HD	ISATA1 on motherboard
MSAS_HD3	Mini-SAS HD to Mini-SAS HD	ISATA2 on motherboard

## 2.9 Removable/optional components

This section explains how to install optional components into the system and covers the following components:

1. System fans
2. Redundant power supply module



---

Ensure that the system is turned off before removing the system fans.

---

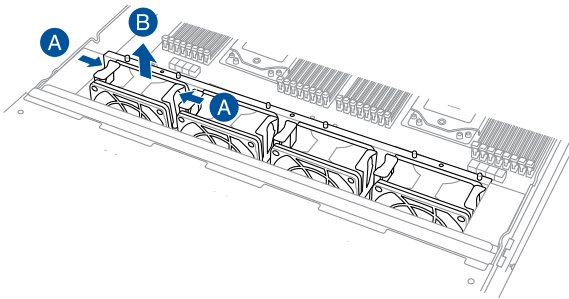


- The redundant power supply module is hot pluggable.
  - You may need to remove previously installed component or factory shipped components when installing optional components.
- 

### 2.9.1 System fans

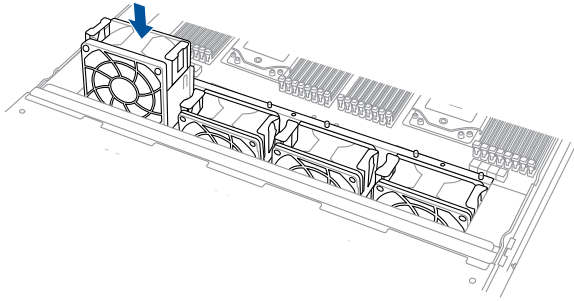
To remove the system fans:

1. Locate the fan you want to replace.
2. Press the retaining clip (A) and lift upward (B) to remove the fan.



To reinstall the system fans:

1. Prepare the fan with the same model and size.
2. Install the fan to the fan cage.



---

The fan can only be installed in one direction. If the fan cannot be installed, turn it around and try again.

---

To install the external rear fan:

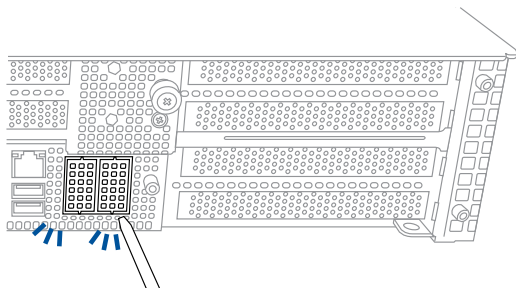
1. Use a screwdriver to pry open the slot.



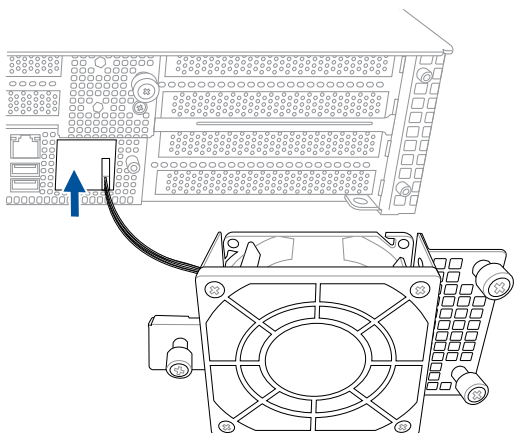
---

Do not install the 4-port ethernet expansion card if you wish to install the external rear fan.

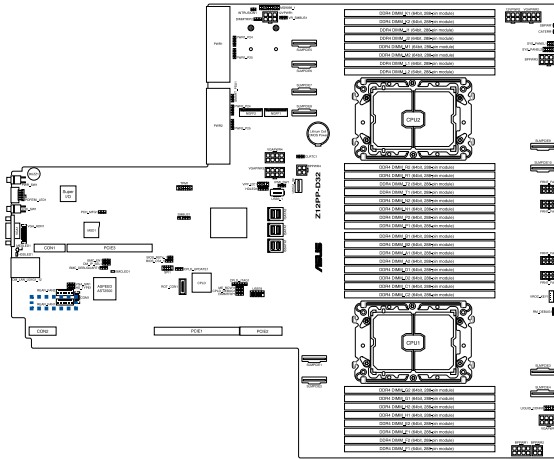
---



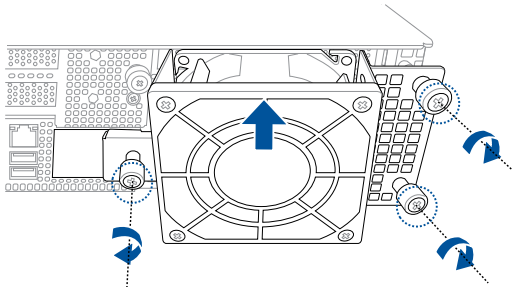
2. Prepare the rear external fan.
3. Pass the cable of the rear external fan through the open slot. Ensure the cabling is organized so that the cables are directed around the 2-port Ethernet expansion card.



4. Connect the cable of the rear external fan to the **REAR\_FAN1** connector on the motherboard.



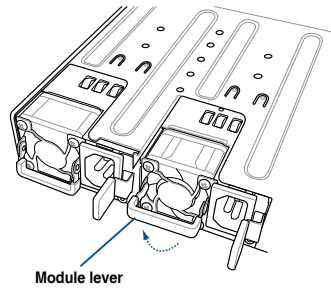
5. Align and place the rear external fan on the chassis.
6. Secure the rear external fan to the chassis with the thumbscrews.



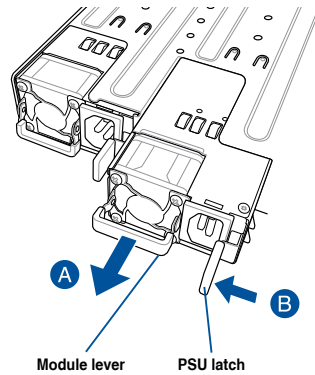
## 2.9.2 Redundant power supply module

To replace a failed redundant power supply module:

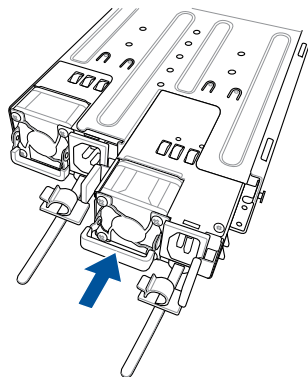
1. Lift up the power supply module lever.



2. Hold the power supply module lever and press the PSU latch, then pull the power supply module out of the system chassis.



3. Prepare the replacement power supply module.
4. Insert the replacement power supply module into the chassis then push it inwards until the latch locks into place.



# Installation Options

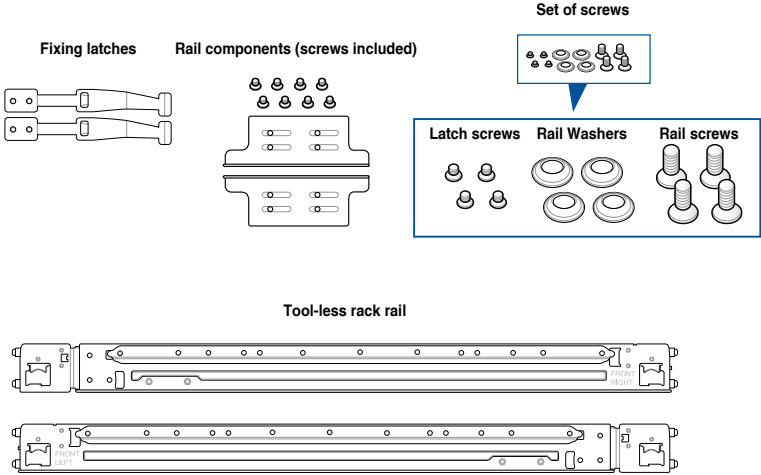
# 3

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

### 3.1 Tool-less Friction Rail Kit

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

The tool-less rail kit package includes:





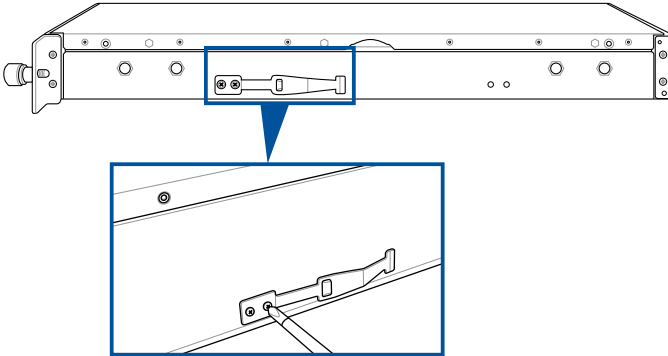
## 3.2 Installing the tool-less rack rail

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

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



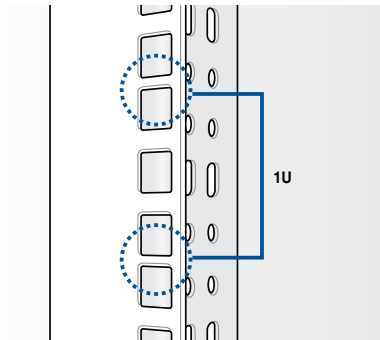
The locations of the screw holes vary with different server models. Refer to your server user manual for details.



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



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



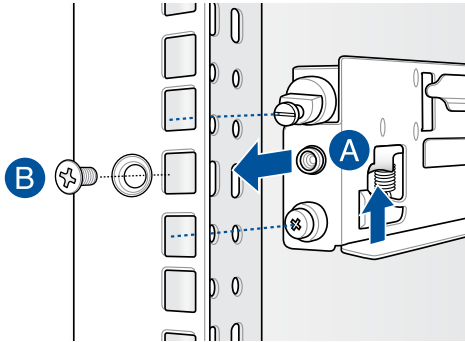
3. Secure the rail components to the rail using the bundled screws.
4. Press the spring lock (A) then insert the studs into the selected square mounting holes on the rack post.
5. Press the spring lock on the other end of rail then insert the stud into the mounting hole on the rack post. Extend the rack rail, if necessary.
6. (Optional) Use the rail screw and rail washer (B) that comes with the kit to secure the rack rail to the rack post.
7. Perform steps 3 to 5 for the other rack rail.



---

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

---



8. Lift the server chassis and insert it into the rack rail.

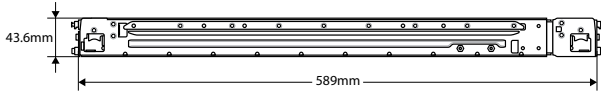
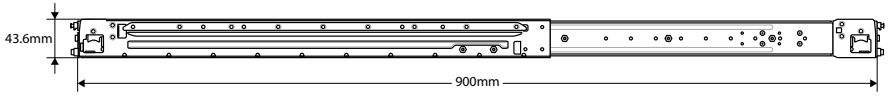


---

Ensure that the rack rail cabinet and the rack posts are stable and standing firmly on a level surface.

---

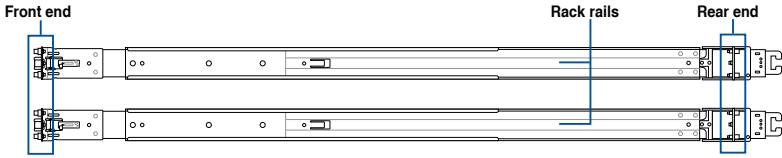
### 3.3 Rail kit dimensions








### 3.4 Ball bearing Rail Kit

The rail kit package includes:

2 x 1200 mm rack rails (or 2 x 1000 mm rack rails)



-  4 x #6-32X4L screws
-  4 x M4X4L screws
-  8 x ø17.1 screws
-  8 x #10-32 screws  
(or 10 x #10-32 screws for 1000 mm rack rails)
-  2 x M5X20L screws



- The bundled screw package includes different types of screws for you to choose from, not all screws are required for the installation.
- Package content and specifications are subject to change without notice.

#### 3.4.1 Selecting rack rail cabinets

Refer to the guide below for more information on selecting a rack rail cabinet and rack rail for your server system.

##### 1200 mm rack rail with CMA

A = 700.3 mm (27.6") ~ 965.5 mm (38")

A + B > 1125 mm (44.3")

##### 1200 mm rack rail without CMA

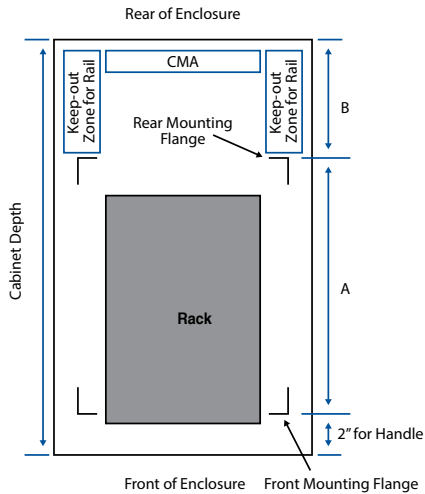
A = 700.3 mm (27.6") ~ 965.5 mm (38")

A + B > 1025 mm (40.4")

##### 1000 mm rack rail without CMA

A = 685.7 mm (27") ~ 916.5 mm (36")

A + B > 835 mm (32.9")



Even without a CMA, another 9" (for 1200 mm rack rails) or 2" (for 1000 mm rack rails) of additional keep-out zone should be reserved behind the inner rail. No obstructions such as power cables or sockets should be present in this keep-out zone.

## 3.4.2 Attaching the rack rails



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



- The installation steps in this section uses a **1200 mm rack rail** as an example, the installation steps for a **1000 mm rack rail** is exactly the same.
- The illustrations in this section are for reference only.

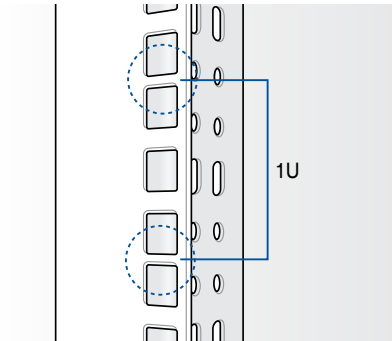
### Installing the rack rail

To install the rack rails into the rack:

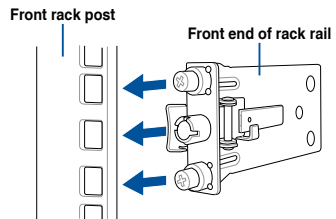
1. Select a desired space on the rack.



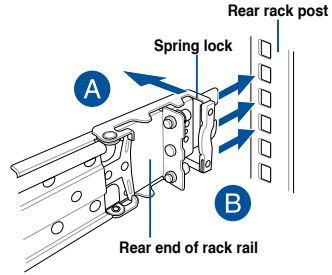
A 1U space consists of three square mounting holes with two thin lips on the top and the bottom.



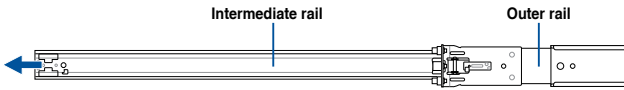
2. Align and insert the front end of the appropriate rack rail (left and right) into the front rack post.



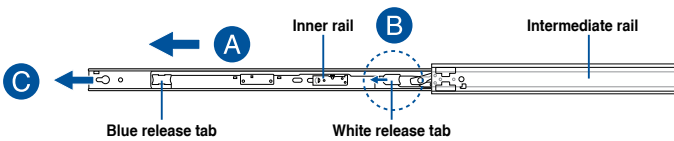
3. Press the spring lock on the rear end of the rack rail and insert the studs into the selected mounting holes on the rear rack post.



4. Slide the intermediate rail out of the outer rail until it clicks to a stop.



5. Slide the inner rail out of the intermediate rail until it clicks to a stop. Slide the white release tab outwards and remove the inner rail completely from the intermediate rail.




---

The blue release tab is available on 1200 mm rack rails. This blue release tab is used to further extend or retract the inner rail.

---

6. Repeat steps 2 to 5 for the other rack rail.




---

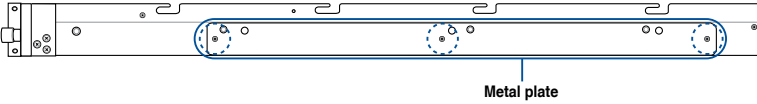
Ensure that the installed rack rails (left and right) are aligned, secured, and stable in place.

---

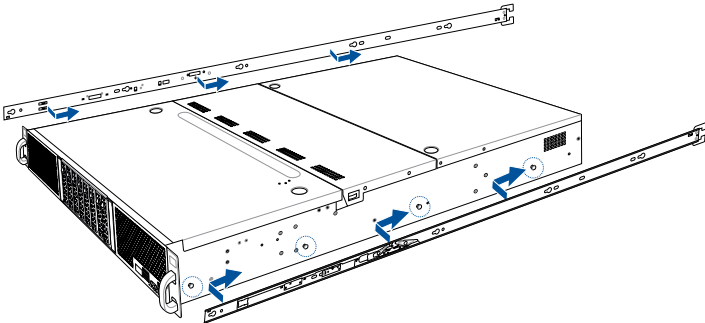
7. Remove the three (3) screws from both left and right sides of the server system chassis, then remove the metal plate.



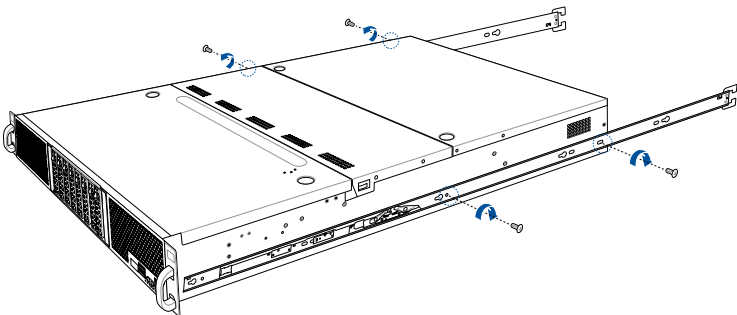
The illustration below only shows one side of the server system chassis, but the screws on the other side should be at the same place.



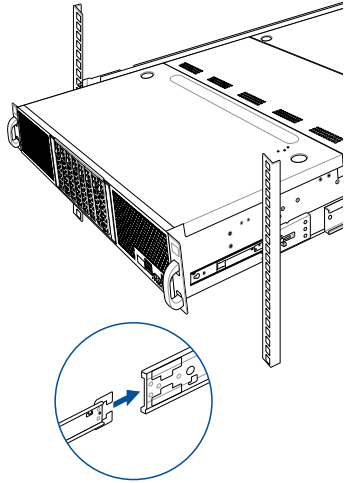
8. Align the inner rails with the studs on both sides of the server system, install the inner rails to the server system, then slide the inner rails toward the rear of the server system until it locks in place.



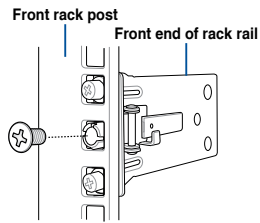
9. Secure the inner rails on both sides of the server system using the #6-32X4L screws.



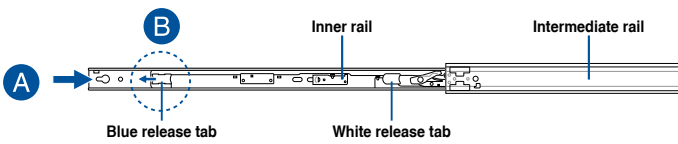
- Align the server system and gently insert it into the rack rails.



- (optional) Use the M5X20L screws to secure the rack rails to the rack post.



- Gently push the server system until it is completely installed into the rack rail.  
 (optional) For 1200 mm rack rails, if the inner rail clicks to a stop while you are installing the server system into the rack rails, slide the blue release tab outwards and gently push the server system until it is completely installed into the rack rail.

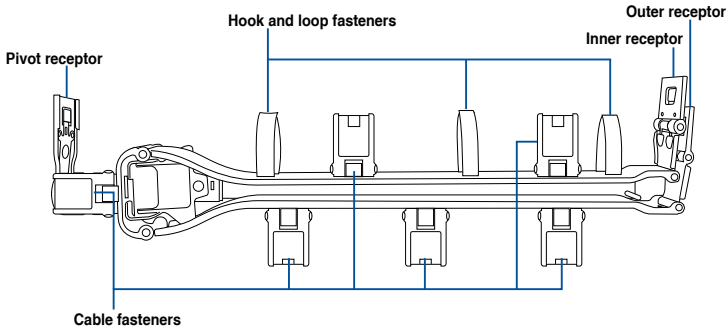


The blue release tab is available on 1200 mm rack rails. This blue release tab is used to further extend or retract the inner rail.



## 3.5 Cable management arm (optional for 1200 mm rack rails)

You can install an additional cable management arm (CMA) to the rack rails to help you manage the cables from your server system. The CMA is designed with movable parts that allow you to move the server system along the rack rail without the need to remove the CMA.



### 3.5.1 Attaching the cable management arm

#### Installing the cable management arm

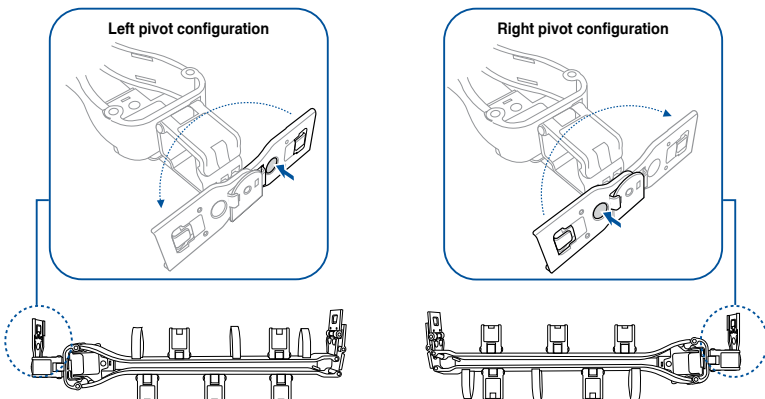
To install the cable management arm:

1. Install the rack rails into the rack.

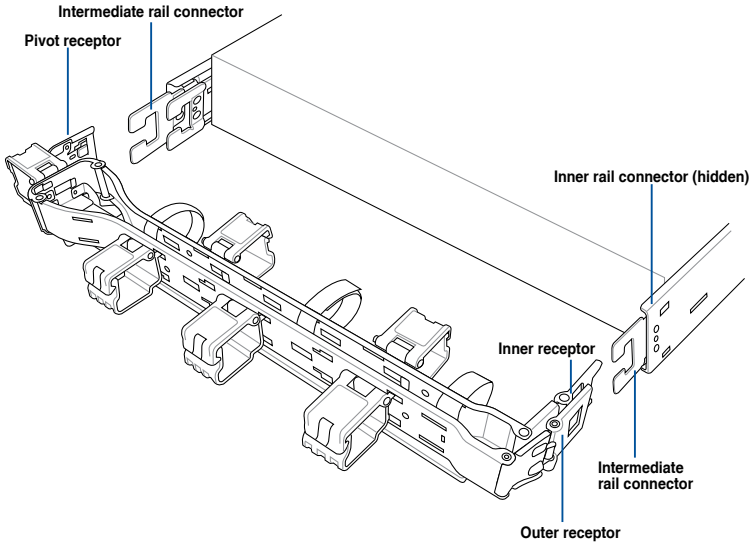


Refer to section 3.1 **Tool-less Friction Rail Kit** for the steps on installing the rack rails into the rack.

2. Press the round button on the pivot receptor, then rotate the pivot receptor to the left or right for a left pivot configuration or right pivot configuration.

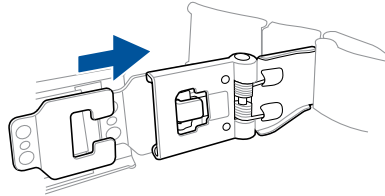


3. Align the three receptors on the CMA with the connectors on the rack rails.

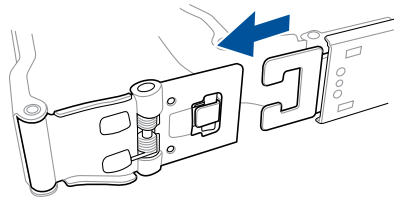


The installation steps in this section uses a **Left pivot configuration** as an example, the installation steps for a **Right pivot configuration** is similar.

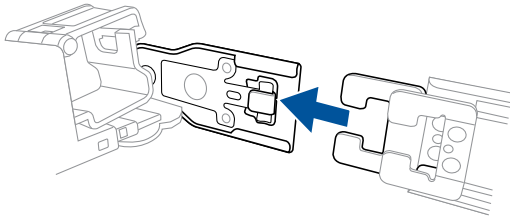
4. Align and connect the inner receptor on the CMA with the connector on the inner rail.



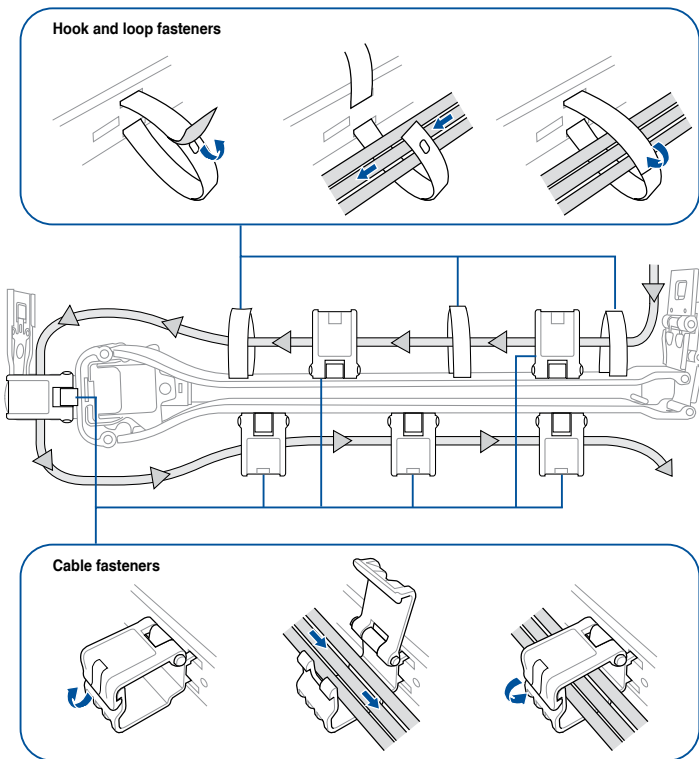
5. Align and connect the outer receptor on the CMA with the connector on the intermediate rail.



6. Align and connect the pivot receptor on the CMA with the connector on the other intermediate rail.



7. Pass the cables from the server system through the hook and loop fasteners and the cable fasteners on the CMA to complete.



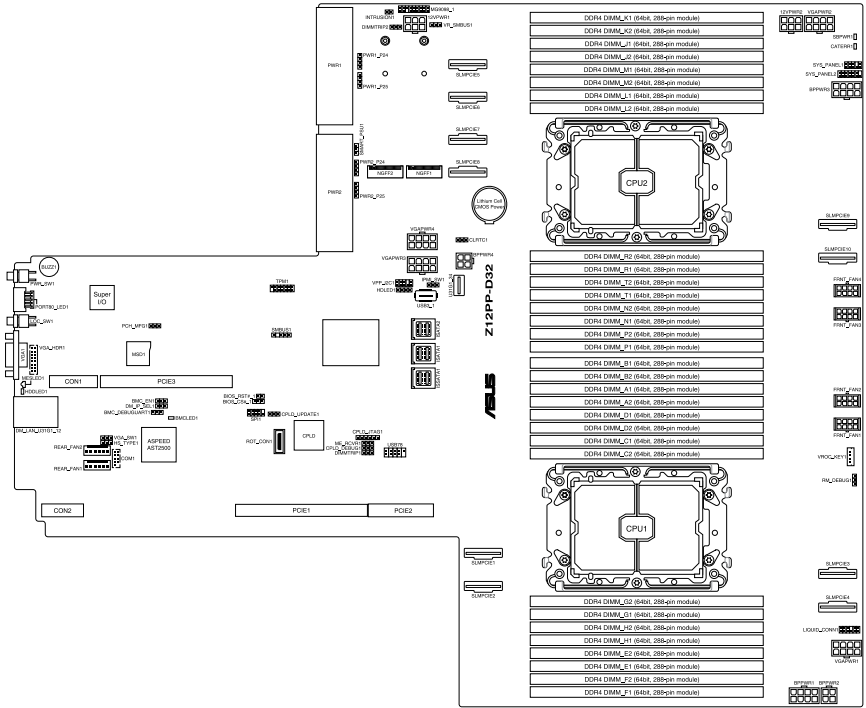


# Motherboard Information

# 4

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

# 4.1 Motherboard layout



## Layout contents

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

Onboard LEDs	Page
1. Standby Power LED (SBPWR1)	4-10
2. Baseboard Management Controller LED (BMCLED1)	4-10
3. Message LED (MESLED1)	4-11
4. Hard disk activity LED (HDDLED1)	4-11
5. CAT ERR LED (CATERR1)	4-12

Internal connectors	Page
1. Mini-SAS HD connector (ISATA1-2; ISSATA1)	4-13
2. Slim PCIe connector (SLIMPCIE1-10)	4-13
3. USB 2.0 connector (10-1 pin USB78)	4-14
4. USB 3.2 Gen 1 connector (U31G1_34; USB3_1)	4-14
5. Chassis Intrusion (2-pin INTRUSION1)	4-15
6. Serial port connector (10-1 pin COM1)	4-15
7. System fan connectors (8-pin FRNT_FAN1-4; 6-pin REAR_FAN1-2)	4-16
8. TPM connector (14-1 pin TPM1)	4-16
9. M.2 (NGFF) card connector (NGFF1-2)	4-17
10. Back panel power connector (4-pin BPPWR2, BPPWR4; 8-pin BPPWR3, VGAPWR2)	4-17
11. VGA power connector (8-pin VGAPWR1, VGAPWR3, VGAPWR4, BPPWR1)	4-18
12. VGA connector (16-pin VGA_HDR1)	4-18
13. Micro SD card slot (MSD1)	4-19

*(continued on the next page)*

Internal connectors	Page
14. System panel connector (10-1 pin SYS_PANEL1; 14-1 pin SYS_PANEL2)	4-20
15. Hard disk activity LED connector (4-pin HDLED1)	4-21
16. VPP_I2C connector (10-1 pin VPP_I2C1)	4-22
17. BMC Debug UART connector (3-pin BMC_DEBUGUART1)	4-22
18. CPLD JTAG1 connector (6-pin CPLD_JTAG1)	4-23
19. Liquid connector (12-1 pin LIQUID_CONN1)	4-23
20. System Management Bus (SMBUS) connector (5-1 pin SMBUS1)	4-24
21. VROC Key connector (4-pin VROC_KEY1)	4-24



## 4.2 Jumpers

### 1. Clear RTC RAM (3-pin CLRTC1)

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

To erase the RTC RAM:

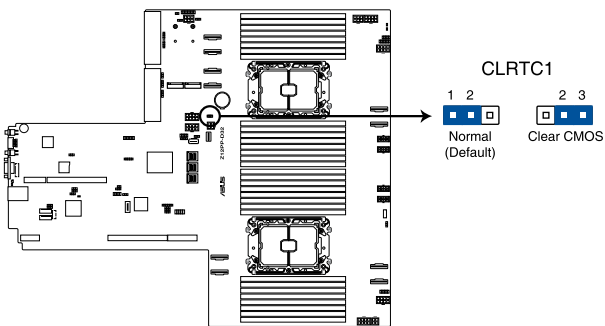
1. Turn OFF the computer and unplug the power cord.
2. Move the jumper cap from pins 1–2 (default) to pins 2–3. Keep the cap on pins 2–3 for about 5–10 seconds, then move the cap back to pins 1–2.
3. Plug the power cord and turn ON the computer.
4. Hold down the <Del> key during the boot process and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



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



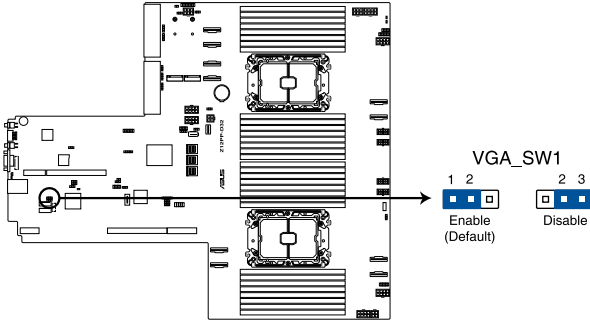
If the steps above do not help, remove the onboard battery and move the jumper again to clear the CMOS RTC RAM data. After the CMOS clearance, reinstall the battery.



**Z12PP-D32 Clear RTC RAM**

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

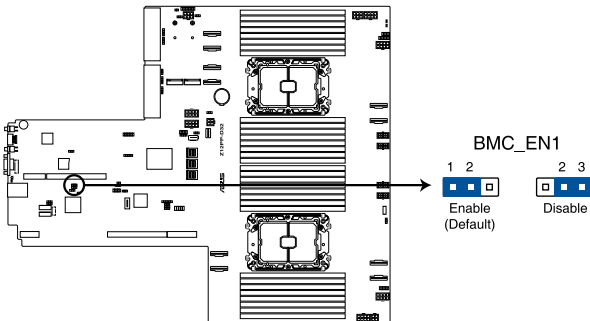
This jumper allows you to enable or disable the onboard VGA controller. Set to pins 1–2 to activate the VGA feature.



**Z12PP-D32 VGA setting**

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

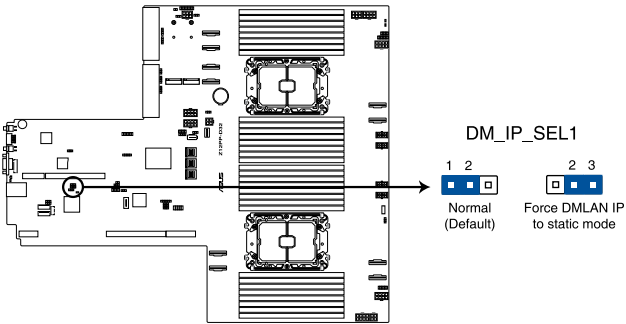
This jumper allows you to enable (default) or disable on-board BMC. Ensure to set this BMC jumper to enabled to avoid system fan control and hardware monitor error.



**Z12PP-D32 BMC setting**

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

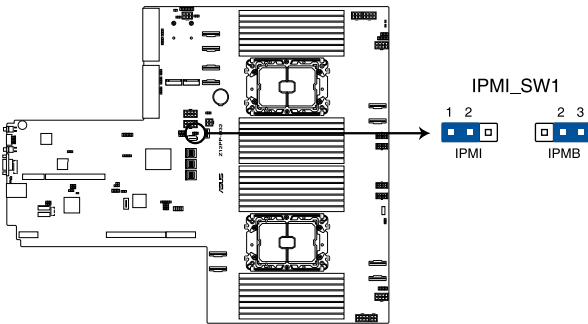
This jumper allows you to select the DMLAN setting. Set to pins 2-3 to force the DMLAN IP to static mode (IP=10.10.10.10, submask=255.255.255.0).



**Z12PP-D32 DM\_IP\_SEL1 setting**

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

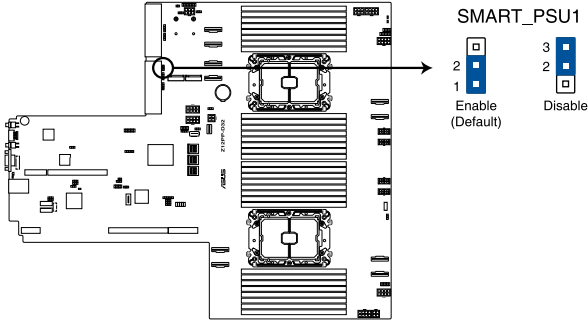
This jumper allows you to select which protocol in the GPU sensor to function.



**Z12PP-D32 IPMI\_SW1 setting**

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

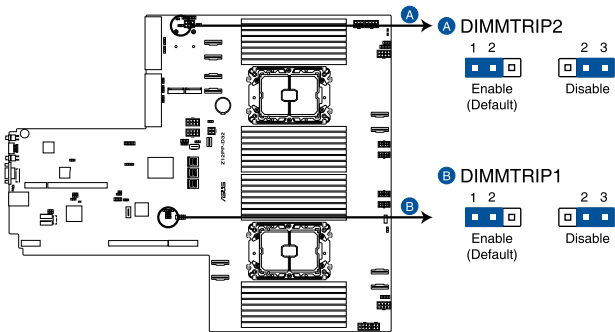
This jumper allows you to enable or disable the Smart Ride Through (SmaRT) function. This feature is enabled by default. Set to pins 2-3 to disable it. When enabled, SmaRT allows uninterrupted operation of the system during an AC loss event.



**Z12PP-D32 Smart Ride Through setting**

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

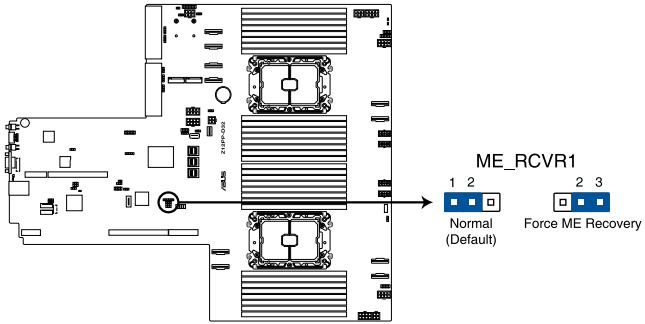
Set to pins 1-2 to enable DDR4 DIMM thermal sensing event.



**Z12PP-D32 Thermaltrip setting**

**8. ME firmware force recovery setting (3-pin ME\_RCVR1)**

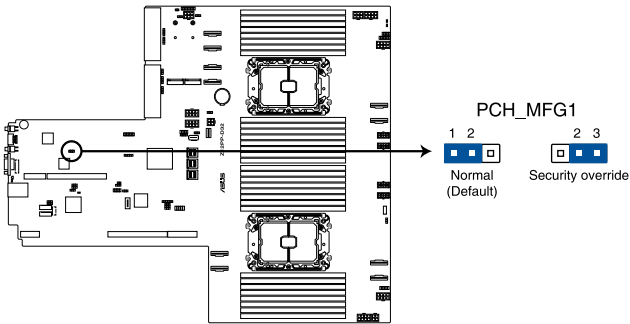
This jumper allows you to force Intel Management Engine (ME) boot from recovery mode when ME become corrupted.



**Z12PP-D32 ME recovery setting**

**9. PCH\_MFG1 setting (3-pin PCH\_MFG1)**

This jumper allows you to update the BIOS ME block select.

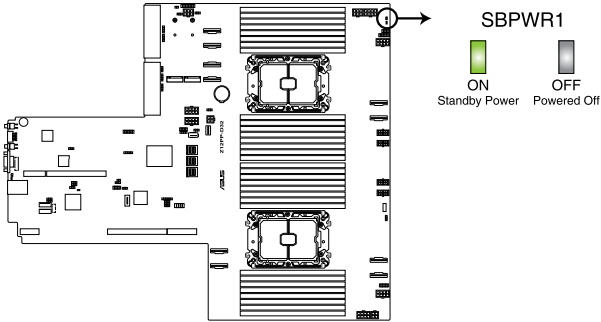


**Z12PP-D32 PCH\_MFG1 setting**

## 4.3 Internal LEDs

### 1. Standby Power LED (SBPWR1)

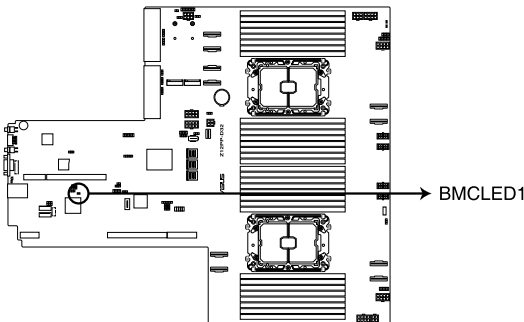
The motherboard comes with a standby power LED. The green LED lights up to indicate that the system is ON, in sleep mode, or in soft-off mode. This is a reminder that you should shut down the system and unplug the power cable before removing or plugging in any motherboard component. The illustration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



**Z12PP-D32 Standby Power LED**

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

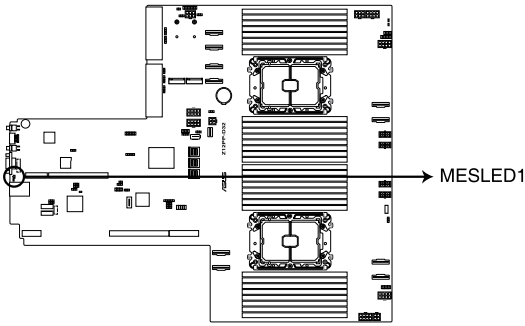
The BMC LED blinks to indicate that the on-board BMC is functional.



**Z12PP-D32 BMC LED**

### 3. Message LED (MESLED1)

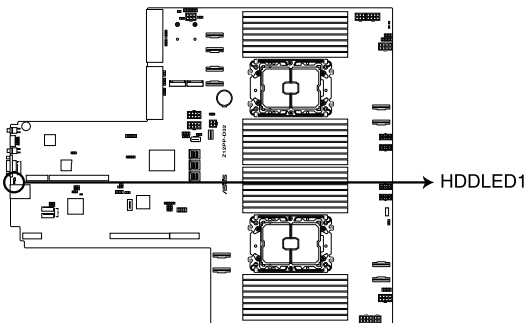
This onboard LED lights up red when there is a BMC event log generated.



**Z12PP-D32 MESLED**

### 4. Hard disk activity LED (HDDLED1)

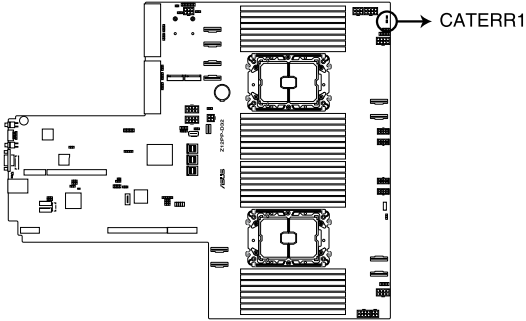
This LED is for the storage devices connected to the onboard SATA, or SATA/SAS add-on card. The read or write activities of any device connected to the onboard SATA, or SATA/SAS add-on card causes the rear panel LED to light up.



**Z12PP-D32 HDDLED1**

**5. CAT ERR LED (CATERR1)**

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



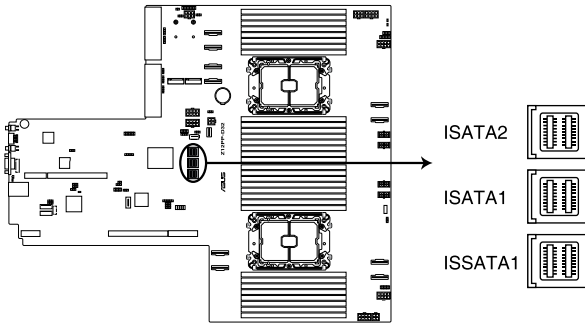
**Z12PP-D32 CATERR1 LED**



## 4.4 Internal connectors

### 1. Mini-SAS HD connector (ISATA1-2; ISSATA1)

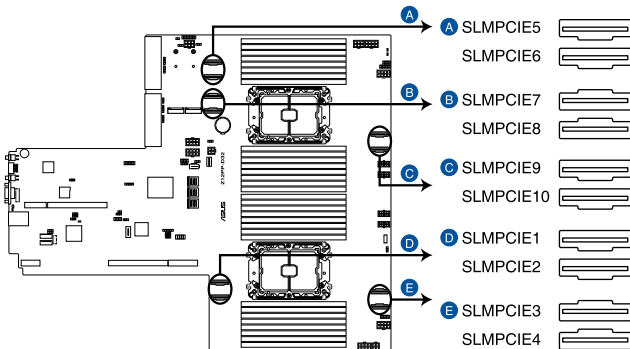
This motherboard comes with mini Serial Attached SCSI (SAS) HD connectors, the storage technology that supports Serial ATA. Each connector supports up to four devices.



**Z12PP-D32 ISATA connectors**

### 2. Slim PCIe connector (SLMPCIE1-10)

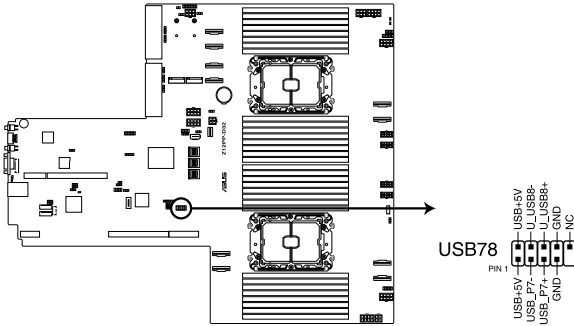
Connects the PCIe signal to the riser card or NVMe port on the backplane.



**Z12PP-D32 SLMPCIE connectors**

**3. USB 2.0 connector (10-1 pin USB78)**

This connector is for USB 2.0 ports. Connect the USB module cable to the connector, and then install the module to a slot opening at the back of the system chassis. The USB connectors comply with USB 2.0 specification that supports up to 480 Mbps connection speed.



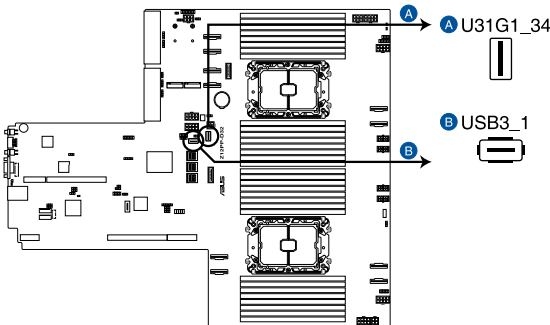
**Z12PP-D32 USB 2.0 connector**



The USB port module is purchased separately.

**4. USB 3.2 Gen 1 connector (U31G1\_34; Type-A USB3\_1)**

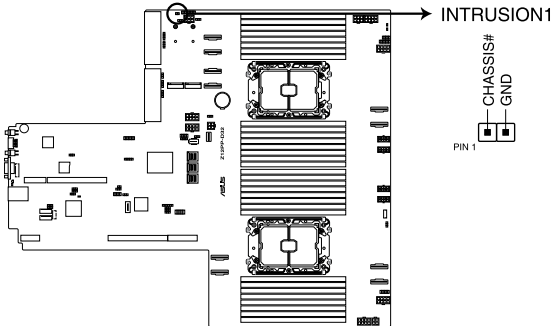
This connector allows you to connect a USB 3.2 Gen 1 module for additional USB 3.2 Gen 1 ports on the front panel. The USB 3.2 Gen 1 connector provides data transfer speeds of up to 10 Gb/s. The Type-A connector allows you to directly connect a USB flash drive.



**Z12PP-D32 USB 3.2 Gen 1 connectors**

## 5. Chassis Intrusion (2-pin INTRUSION1)

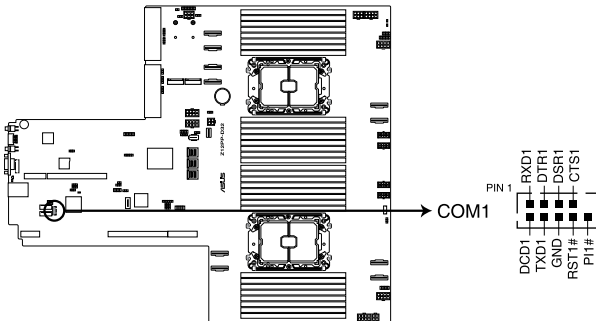
These leads are for the intrusion detection feature for chassis with intrusion sensor or microswitch. When you remove any chassis component, the sensor triggers and sends a high level signal to these leads to record a chassis intrusion event. The default setting is to short the CHASSIS# and the GND pin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



**Z12PP-D32 Chassis Intrusion connector**

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

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



**Z12PP-D32 Serial port connector**



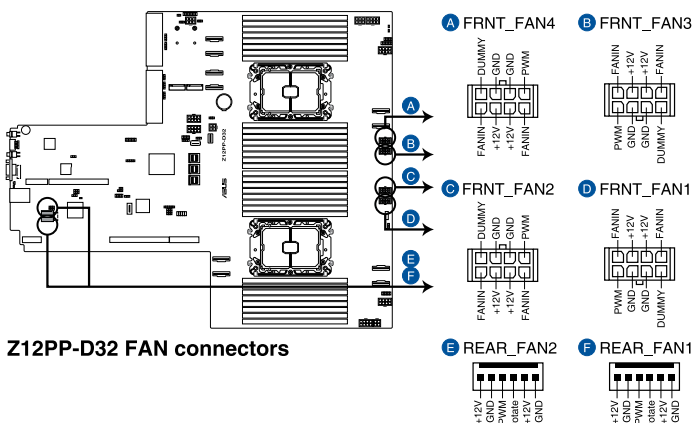
The COM module is purchased separately.

## 7. System fan connectors (8-pin FRNT\_FAN1-4; 6-pin REAR\_FAN1-2)

The 8-pin FRNT\_FAN connectors are connected to the Fan board. The 6-pin REAR\_FAN connectors support cooling fans of 0.8A–1.0A (12 W max.) or a total of 6.4 A–8.0 A (96 W max.) at +12V. Connect the fan cables to the fan connectors on the motherboard, making sure that the black wire of each cable matches the ground pin of the connector.

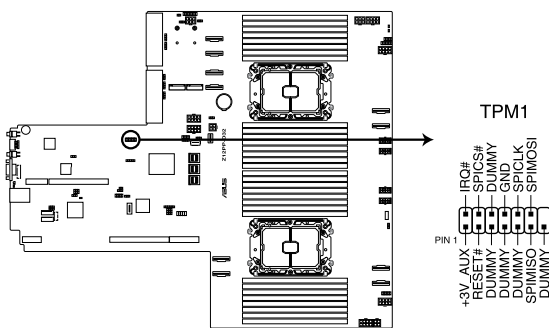


DO NOT forget to connect the fan cables to the fan connectors. Insufficient air flow inside the system may damage the motherboard components. These are not jumpers! DO NOT place jumper caps on the fan connectors!



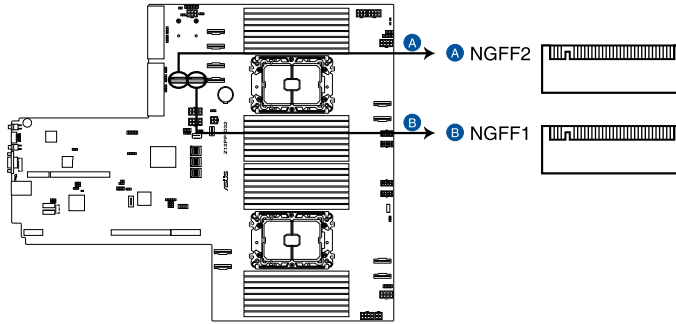
## 8. TPM connector (14-1 pin TPM1)

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.



## 9. M.2 (NGFF) card connector (NGFF1-2)

These connectors allow you to install M.2 devices.



**Z12PP-D32 NGFF connectors**



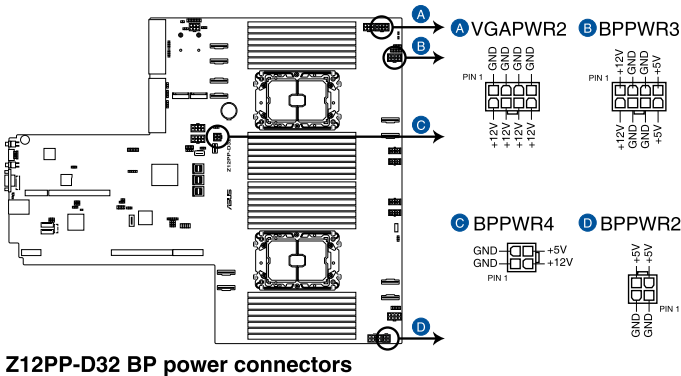
This connector supports type 2260 / 2280 devices on PCIe interface.



The M.2 (NGFF) device is purchased separately.

## 10. Back panel power connector (4-pin BPPWR2, BPPWR4; 8-pin BPPWR3, VGAPWR2)

These connectors are for the power supply plugs that connects to the back panel. The power supply plugs are designed to fit these connectors in only one orientation. Find the proper orientation and push down firmly until the connectors completely fit.



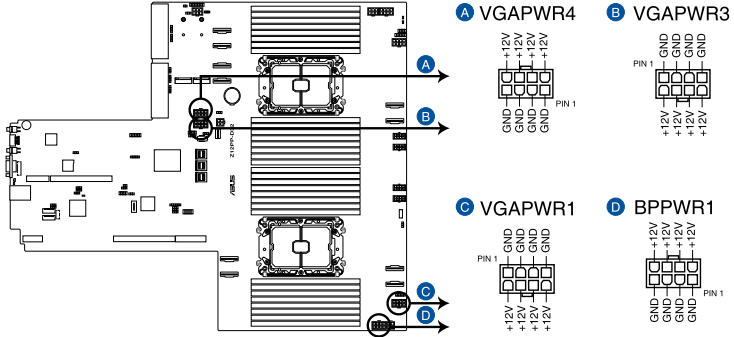
**Z12PP-D32 BP power connectors**



**DO NOT** connect VGA cards to these connectors. Doing so may cause system boot errors and permanent damage to your motherboard or device.

**11. VGA power connectors (8-pin VGAPWR1, VGAPWR3, VGAPWR4, BPPWR1)**

These connectors are for the power supply plugs that connects to the VGA card. The power supply plugs are designed to fit these connectors in only one orientation. Find the proper orientation and push down firmly until the connectors completely fit.



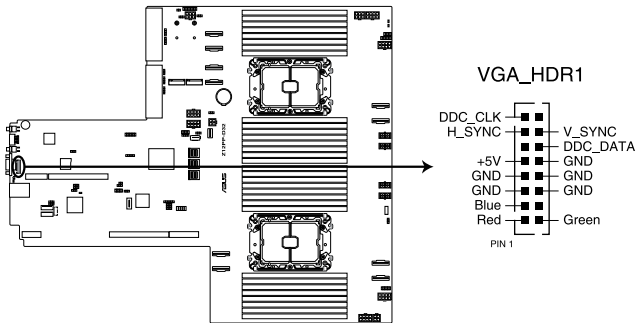
**Z12PP-D32 VGA power connectors**



DO NOT connect the back panel to these connectors. Doing so may cause system boot errors and permanent damage to your motherboard or device.

**12. VGA connector (16-pin VGA\_HDR1)**

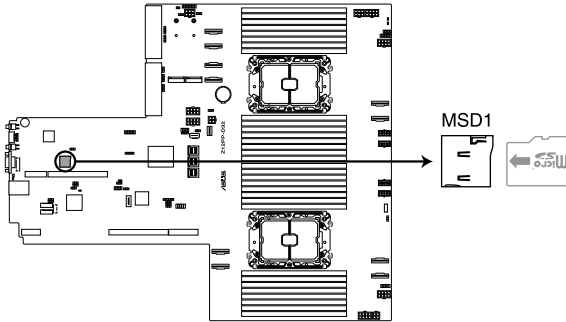
This connector supports the VGA High Dynamic-Range interface.



**Z12PP-D32 Internal VGA connector**

### 13. Micro SD card slot (MSD1)

Your motherboard supports SD Memory Card v2.00 (SDHC) / v3.00 (SDXC).



**Z12PP-D32 MSD1**



---

Disconnect all power (including redundant PSUs) from the existing system before you add or remove a Memory Card, then reboot the system to access the Memory Card.

---



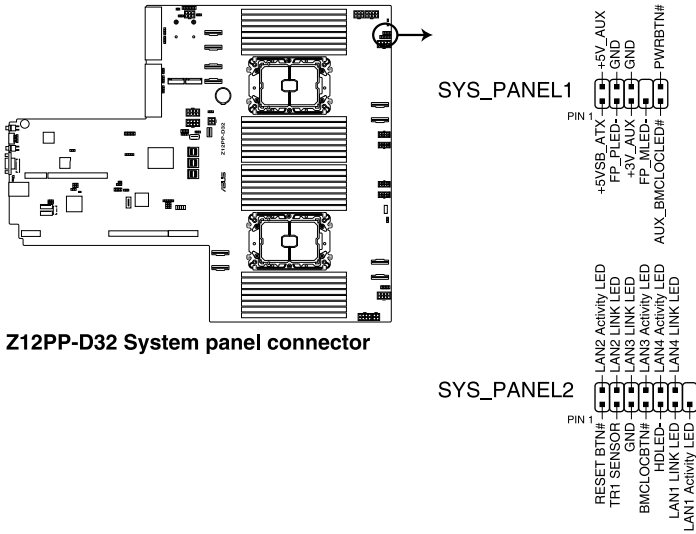
---

Some memory cards may not be compatible with your motherboard. Ensure that you use only compatible memory cards to prevent loss of data, damage to your device, or memory card, or both.

---

#### 14. System panel connector (10-1 pin SYS\_PANEL1; 14-1 pin SYS\_PANEL2)

This connector supports several chassis-mounted functions.



- System power LED (FP\_PLED)**

This 2-pin connector is for the system power LED. Connect the chassis power LED cable to this connector. The system power LED lights up when you turn on the system power, and blinks when the system is in sleep mode.
- Message LED (2-pin FP\_MLED)**

This 2-pin connector is for the message LED cable that connects to the front message LED. The message LED is controlled by the BMC to indicate an abnormal event occurrence.
- Locator LED connector (AUX\_BMCLOCKED)**

This connector allows you to connect the Locator LED. The Location LED helps visually locate and identify the server in error on a server rack.
- Power Button/Soft-off Button connector (PWRBTN)**

The 3-1 pin connector allows you to connect the system power button. Press the power button to power up the system, or put the system into sleep or soft-off mode (depending on the operating system settings).
- LAN activity LED connector (LAN1\_LED, LAN2\_LED, LAN3\_LED, LAN4\_LED)**

This 2-pin connector allows you to connect the Gigabit LAN Activity LED.



- **Reset button connector (RESET)**

This connector allows you to connect the chassis-mounted reset button. Press the reset button to reboot the system.

- **TR1 Sensor connector (TR1 SENSOR)**

This connector allows detection of the environmental temperature of the front panel.

- **Locator button connector (BMCLOCBTN#)**

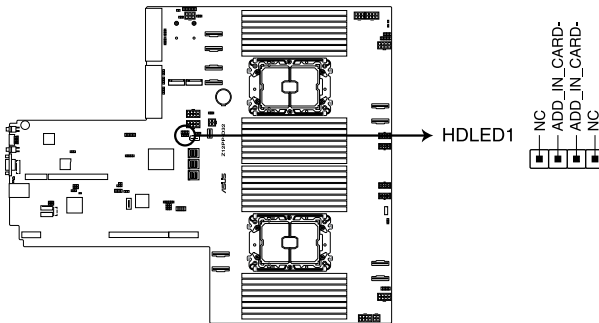
This connector allows you to connect the Locator button. Press the button to light up the Locator LED.

- **Storage Device Activity LED connector (HDLED)**

This connector allows you to connect the Storage Device Activity LED. The Storage Device Activity LED lights up or blinks when data is read from or written to the storage device or storage device add-on card.

**15. Storage device activity LED connector (4-pin HDLED1)**

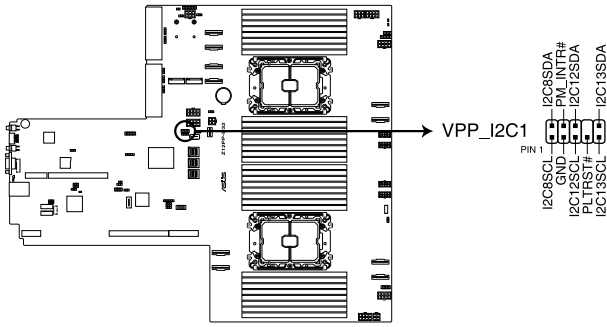
This LED connector is for the storage add-on card cable connected to the SATA or SAS add-on card. The read or write activities of any device connected to the SATA or SAS add-on card causes the front panel LED to light up.



**Z12PP-D32 Storage device activity LED connector**

**16. VPP\_I2C connector (10-1 pin VPP\_I2C1)**

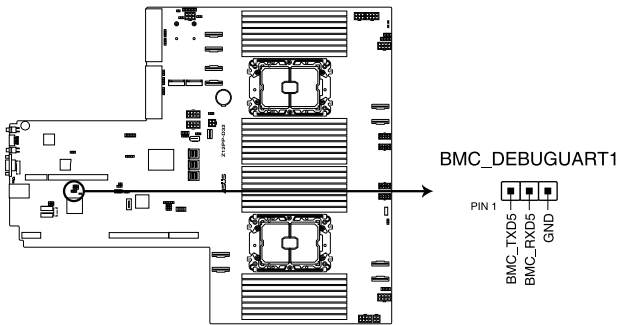
The VPP\_I2C connector is used for the storage backplane with sensor readings.



**Z12PP-D32 VPP\_I2C1 connector**

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

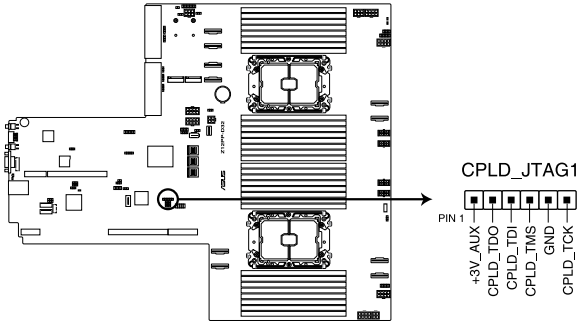
This connector is used for reading the BMC UART Debug log.



**Z12PP-D32 BMC\_DEBUGUART1 connector**

**18. CPLD JTAG connector (6-pin CPLD\_JTAG1)**

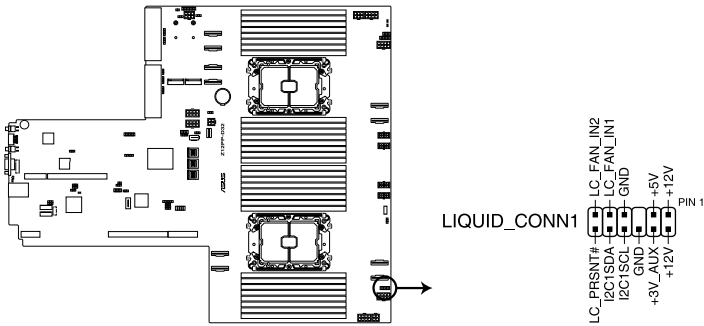
This connector is used for burning the CPLD JTAG.



**Z12PP-D32 CPLD\_JTAG1 connector**

**19. Liquid connector (12-pin LIQUID\_CONN1)**

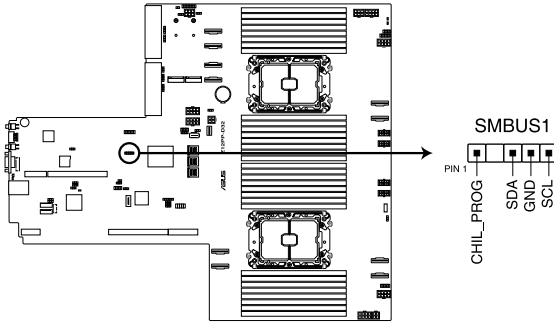
This connector is used for detecting the pump speed of the water cooling system.



**Z12PP-D32 LIQUID\_CONN1 connector**

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

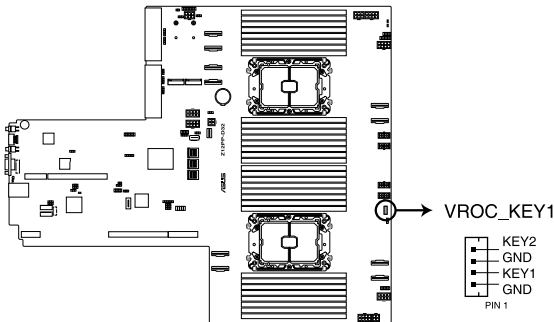
This connector controls the system and power management-related tasks. This connector processes the messages to and from devices rather than tripping the individual control lines.



**Z12PP-D32 SMBUS connector**

**21. VROC Key connector (4-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.



**Z12PP-D32 VROC\_KEY1**



- The VROC hardware key is purchased separately.
- Supports RAID 0/1/10 with Intel® VROC Standard Upgrade key.
- Supports RAID 0/1/5/10 with Intel® VROC Premium Upgrade key.
- Supports RAID 0/1/5/10 for Intel® NVMe SSDs with Intel® VROC Intel-SSD-Only Upgrade key (Non-Intel NVMe SSDs supported in Pass-thru).

# **BIOS Setup**

# 5

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

## 5.1 Managing and updating your BIOS

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

### 1. **ASUS CrashFree BIOS 3**

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

### 2. **ASUS EzFlash**

Updates the BIOS using a USB flash disk.

### 3. **BUPDATER**

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

Refer to the corresponding sections for details on these utilities.



---

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

---

### 5.1.1 **ASUS CrashFree BIOS 3 utility**

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



---

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

---

### **Recovering the BIOS from a USB flash drive**

To recover the BIOS from a USB flash drive:

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



---

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

---



---

The recovered BIOS may not be the latest BIOS version for this motherboard. Visit the ASUS website at [www.asus.com](http://www.asus.com) to download the latest BIOS file.

---

## 5.1.2 ASUS EZ Flash Utility

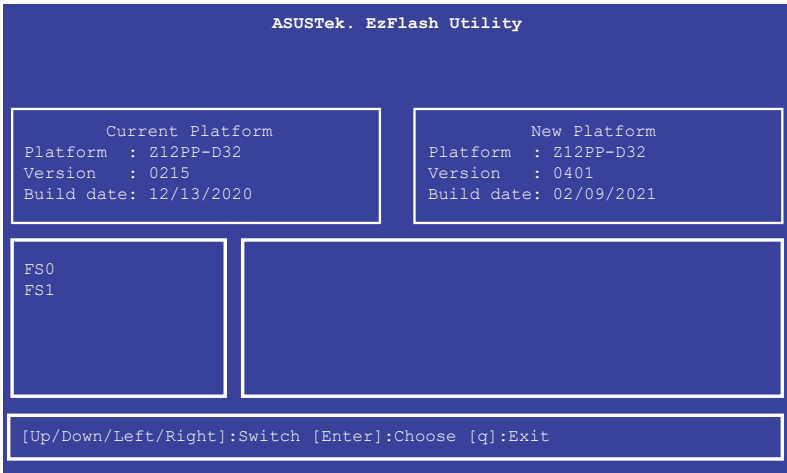
The ASUS EZ Flash Utility feature allows you to update the BIOS without having to use a DOS-based utility.



Before you start using this utility, download the latest BIOS from the ASUS website at [www.asus.com](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 <F5> and select **Yes** to load the BIOS default settings.

## 5.1.3 BUPDATER utility



---

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

---

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

### Updating the BIOS file

To update the BIOS file using the BUPDATER utility:

1. Visit the ASUS website at [www.asus.com](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:

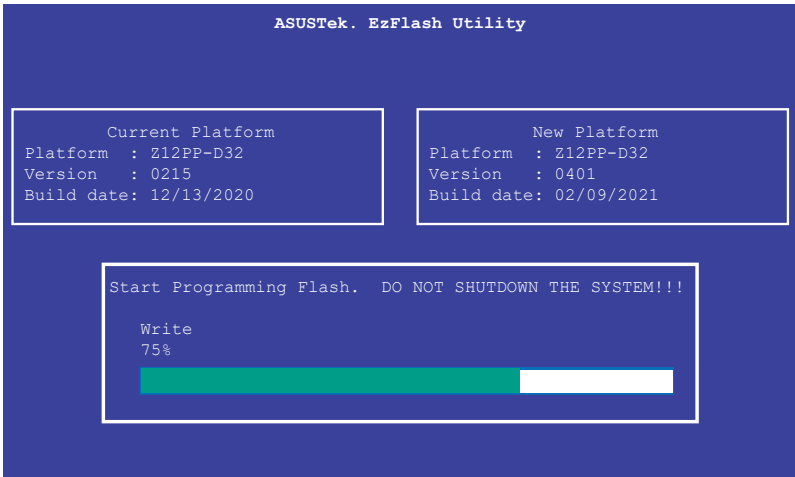
```
BUPDATER /i[filename].CAP
```

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.



## 5.2 BIOS setup program

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

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

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

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

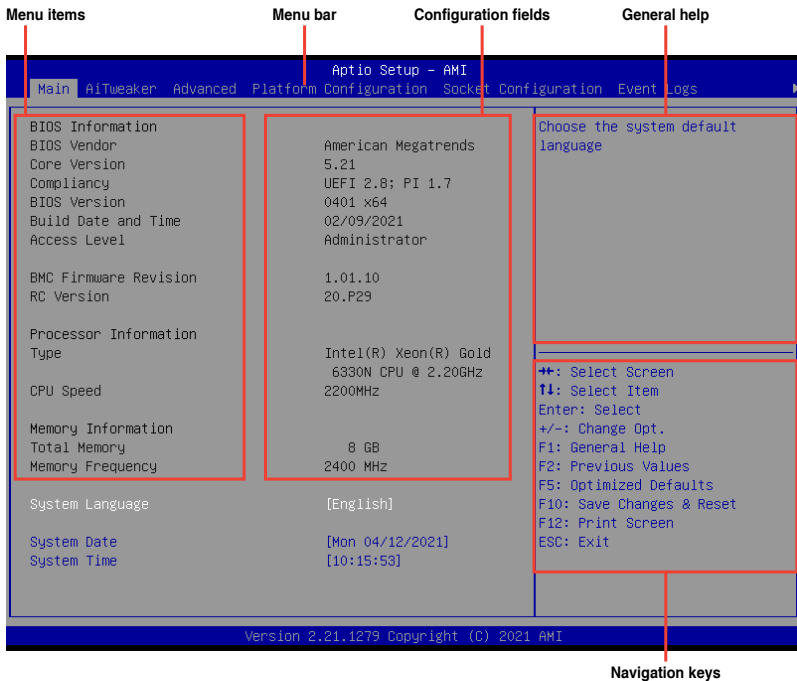
If you wish to enter Setup after POST, restart the system by pressing <Ctrl>+<Alt>+<Delete>, or by pressing the reset button on the system chassis. You can also restart by turning the system off and then back on. Do this last option only if the first two failed.

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



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

## 5.2.1 BIOS menu screen



## 5.2.2 Menu bar

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

- Main** For changing the basic system configuration
- Ai Tweaker** For changing the overclocking settings
- 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.

### **5.2.3 Menu items**

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

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

### **5.2.4 Submenu items**

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

### **5.2.5 Navigation keys**

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

### **5.2.6 General help**

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

### **5.2.7 Configuration fields**

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

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

### **5.2.8 Pop-up window**

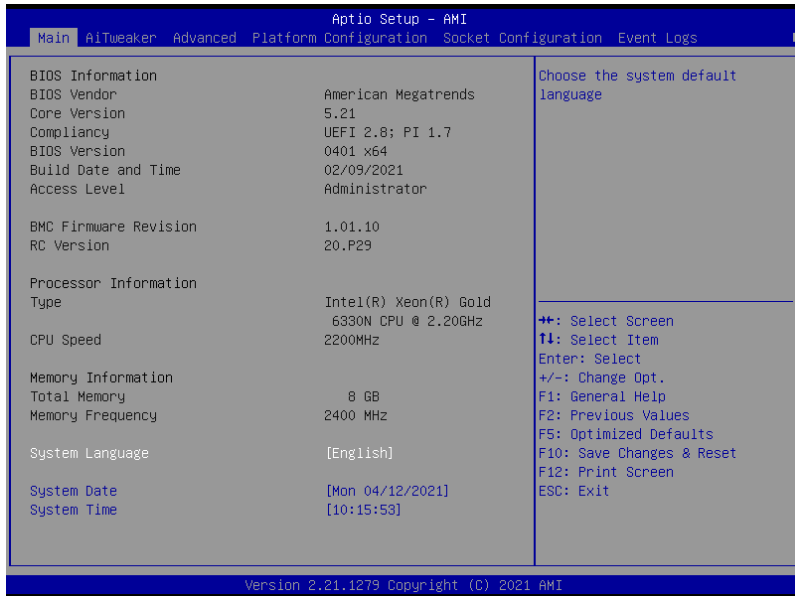
Select a menu item and press <Enter> to display a pop-up window with the configuration options for that item.

### **5.2.9 Scroll bar**

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

## 5.3 Main menu

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



### 5.3.1 System Language [English]

Allows you to select the system default language.

### 5.3.2 System Date [Day xx/xx/xxxx]

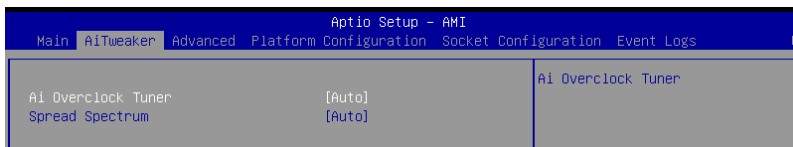
Allows you to set the system date.

### 5.3.3 System Time [xx:xx:xx]

Allows you to set the system time.

## 5.4 Ai Tweaker menu

The Ai Tweaker menu items allow you to configure overclocking-related items.



### Ai Overclock Tuner [Auto]

Configuration options: [Auto] [Manual] [OC Tune]



---

The following item appears only when **Ai Overclock Tuner** is set to **[Manual]**.

---

### BCLK Frequency [100.0]

Use the <+> or <-> to adjust the value. The values range from 80.0MHz to 300.0MHz.



---

The following item appears only when **Ai Overclock Tuner** is set to **[OC Tune]**.

---

### OC Tune Level [Level 1]

Configuration options: [Level1] [Level2] [Level3]

### Spread Spectrum [Auto]

Setting this item to **[Disabled]** may enhance the BCLK overclocking ability.

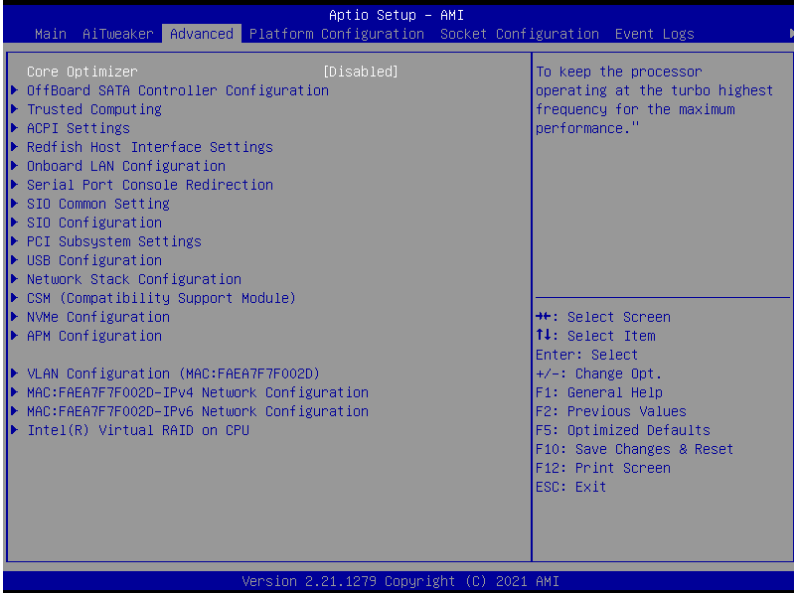
Configuration options: [Auto] [Disabled] [Enabled]

## 5.5 Advanced menu

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



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

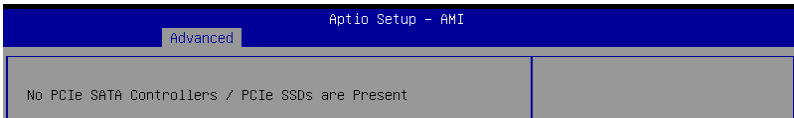


### Core Optimizer [Disabled]

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]

### 5.5.1 OffBoard SATA Controller Configuration



## 5.5.2 Trusted Computing

Aptio Setup - AMI		
Advanced		
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		

### 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]

## 5.5.3 ACPI Settings

Aptio Setup - AMI		
Advanced		
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]

## 5.5.4 Redfish Host Interface Settings

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

### Redfish [Enabled]

Allows you to enable or disable Redfish.

Configuration options: [Disabled] [Enabled]



---

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

---

### Authentication mode [Basic Authentication]

Allows you to select the authentication mode.

Configuration options: [Basic Authentication] [Session Authentication]

### Redfish BMC Settings

#### IP address

Allows you to enter the IP address.



## IP Mask address

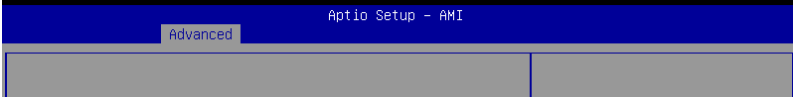
Allows you to enter the IP Mask address.

## IP Port

Allows you to enter the IP Port.

## 5.5.5 Onboard LAN Configuration

The items in this submenu will differ depending on the Lan controller installed on the system.



The following item appears only when an Intel® X710-AT2 LAN controller is installed on the system.

### Onboard X710 LAN Configuration

#### Intel X710 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].

##### Enable OPROM

Allows you to enable or disable X710 option ROM.  
Configuration options: [Disabled] [Enabled]

#### Intel X710 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].

##### Enable OPROM

Allows you to enable or disable X710 option ROM.  
Configuration options: [Disabled] [Enabled]



---

The following item appears only when an Intel® I350-AM4 LAN controller is installed on the system.

---

## 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]

### Intel I350 LAN3

#### 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]

### Intel I350 LAN4

#### LAN Enable [JumperState]

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



---

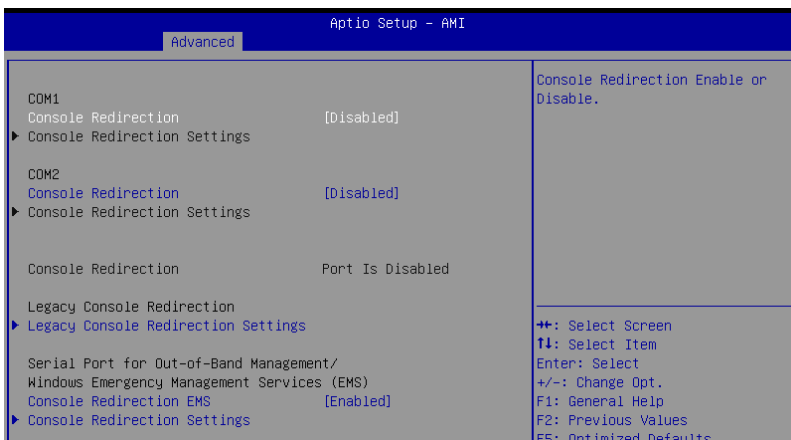
The following item appears only when **LAN Enable** is set to **[JumperState]**.

---

### ROM Type [Disabled]

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

## 5.5.6 Serial Port Console Redirection



### COM1/COM2

#### Console Redirection [Disabled]

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



---

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

---

#### Console Redirection Settings

These items become configurable only when you enable the **Console Redirection** item. The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings.

**Terminal Type [ANSI]**

Allows you to set the terminal type.

[VT100] ASCII char set.

[VT100+] Extends VT100 to support color, function keys, etc.

[VT-UTF8] Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.

[ANSI] Extended ASCII char set.

**Bits per second [115200]**

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

Configuration options: [9600] [19200] [38400] [57600] [115200]

**Data Bits [8]**

Configuration options: [7] [8]

**Parity [None]**

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

[None] None

[Even] Parity bit is 0 if the num of 1's in the data bits is even.

[Odd] Parity bit is 0 if num of 1's in the data bits is odd.

[Mark] Parity bit is always 1.

[Space] Parity bit is always 0.

**Stop Bits [1]**

Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning.)

The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.

Configuration options: [1] [2]

**Flow Control [None]**

Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a "stop" signal can be sent to stop the data flow. Once the buffers are empty, a "start" signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.

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

**VT -UTF8 Combo Key Support [Enabled]**

This allows you to enable the VT -UTF8 Combination Key Support for ANSI/VT100 terminals.

Configuration options: [Disabled] [Enabled]

**Recorder Mode [Disabled]**

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

Configuration options: [Disabled] [Enabled]

**Resolution 100x31 [Enabled]**

This allows you enable or disable extended terminal solution.

Configuration options: [Disabled] [Enabled]

### Putty Keypad [VT100]

This allows you to select the FunctionKey and Keypad on Putty.

Configuration options: [VT100] [LINUX] [XTERMR6] [SCO] [ESCN] [VT400]

## Legacy Console Redirection Settings

### Redirection COM Port [COM1]

Allows you to select a COM port to display redirection of Legacy OS and Legacy OPROM Messages.

Configuration options: [COM1] [COM2]

### Resolution [80x24]

This allows you to set the number of rows and columns supported on the Legacy OS.

Configuration options: [80x24] [80x25]

### Redirection After POST [Always Enable]

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

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

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

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

### Console Redirection EMS [Enabled]

Allows you to enable or disable the console redirection feature.

Configuration options: [Disabled] [Enabled]



---

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

---

### Console Redirection Settings

#### Out-of-Band Mgmt Port [COM1]

Microsoft Windows Emergency Management Services (EMS) allow for remote management of a Windows Server OS through a serial port.

Configuration options: [COM1] [COM2]

#### Terminal Type EMS [VT-UTF8]

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

Configuration options: [VT100] [VT100+] [VT-UTF8] [ANSI]

#### Bits per second EMS [115200]

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

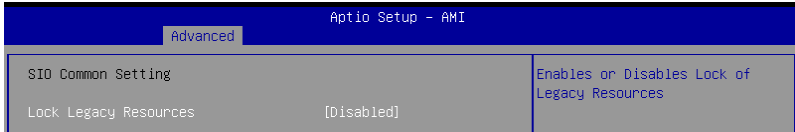
Configuration options: [9600] [19200] [57600] [115200]

### Flow Control EMS [None]

Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a “stop” signal can be sent to stop the data flow. Once the buffers are empty, a “start” signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.

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

## 5.5.7 SIO Common Setting

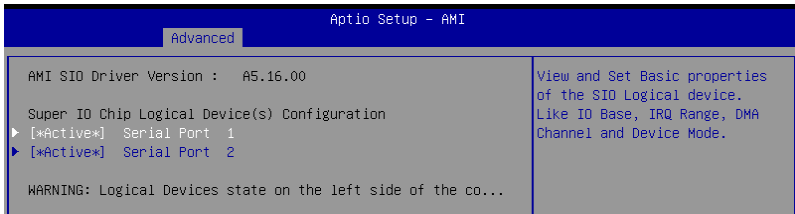


### Lock Legacy Resources [Disabled]

Allows you to enable or disable locking of Legacy Resources.

Configuration options: [Disabled] [Enabled]

## 5.5.8 SIO Configuration



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

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

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

#### Use This Device [Enabled]

Allows you to enable or disable this Logical Device.

Configuration options: [Disabled] [Enabled]



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



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

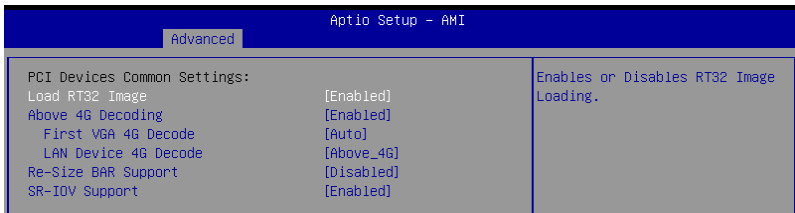
### Possible: [Use Automatic Settings]

Allows the user to change the device resource settings. New settings will be reflected no this setup page after system restarts.

Configuration options: [Use Automatic Settings] [IO=3F8h; IRQ=4; DMA;] [IO=3F8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA;] [IO=2F8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA;] [IO=3E8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA;] [IO=2E8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA;]

## 5.5.9 PCI Subsystem Settings

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



### Load RT32 Image [Enabled]

Allows you to enable or disable RT32 Image Loading.

Configuration options: [Disabled] [Enabled]

### Above 4G Decoding [Enabled]

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

Configuration options: [Disabled] [Enabled]



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

#### First VGA 4G Decode [Auto]

[Auto]          Auto  
[Above\_4G]      Force First VGA to above 4G.

#### LAN Device 4G Decode [Above\_4G]

Configuration options: [Auto] [Above\_4G]

### Re-Size BAR Support [Disabled]

If system has Resizable BAR capable PCIe Devices, this option enables or disables Resizable BAR Support. (Only if system supports 64-bit PCI Decoding).

Configuration options: [Disabled] [Auto]



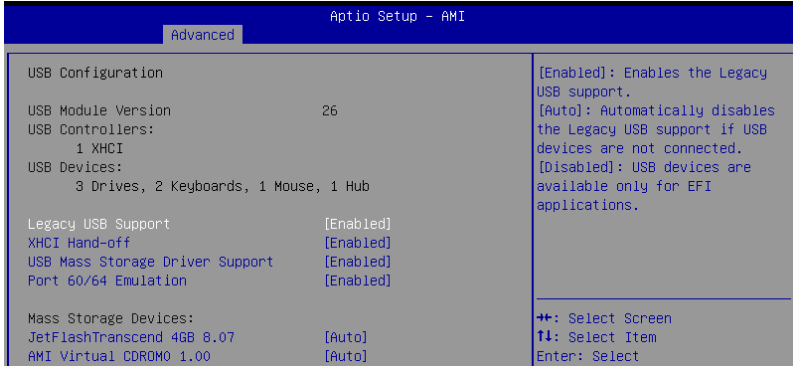
To enable Re-Size BAR Support for harnessing full GPU memory, please set **CSM (Compatibility Support Module)** to **[Disabled]**.

## SR-IOV Support [Enabled]

Allows you to enable or disable Single Root IO Virtualization Support if the system has SR-IOV capable PCIe devices.

Configuration options: [Disabled] [Enabled]

## 5.5.10 USB Configuration



### Legacy USB Support [Enabled]

Allows you to enable or disable Legacy USB device support.

[Enabled] Enables legacy USB support.

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

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

### XHCI Hand-off [Enabled]

Allows you to enable or disable workaround for OSES without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.

Configuration options: [Enabled] [Disabled]

### USB Mass Storage Driver Support [Enabled]

Allows you to enable or disable the USB Mass Storage driver support.

Configuration options: [Disabled] [Enabled]

### Port 60/64 Emulation [Enabled]

Allows you to enable or disable I/O port 60h/64h emulation support. This should be enabled for the complete keyboard legacy support for non-USB aware OSES.

Configuration options: [Disabled] [Enabled]

### 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]



## 5.5.11 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.

## 5.5.12 CSM (Compatibility Support Module)

Aptio Setup - AMI	
Advanced	
Compatibility Support Module Configuration	
Launch CSM	[Disabled]
CSM(compatibility support module) [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]

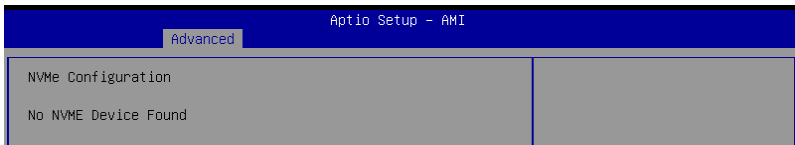
## Boot from PCI-E/PCI Expansion Devices [UEFI only]

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]

## 5.5.13 NVMe Configuration

This page will display the NVMe controller and drive information.



### Device



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

### Self Test Option [Short]

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

Configuration options: [Short] [Extended]

### Self Test Action [Controller Only Test]

This item allows you to select either to test Controller alone or Controller and NameSpace. Selecting Controller and Namespace option will take a lot longer to complete the test.

Configuration options: [Controller Only Test] [Controller and NameSpace Test]

### Run Device Self Test

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

## 5.5.14 APM Configuration

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

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.

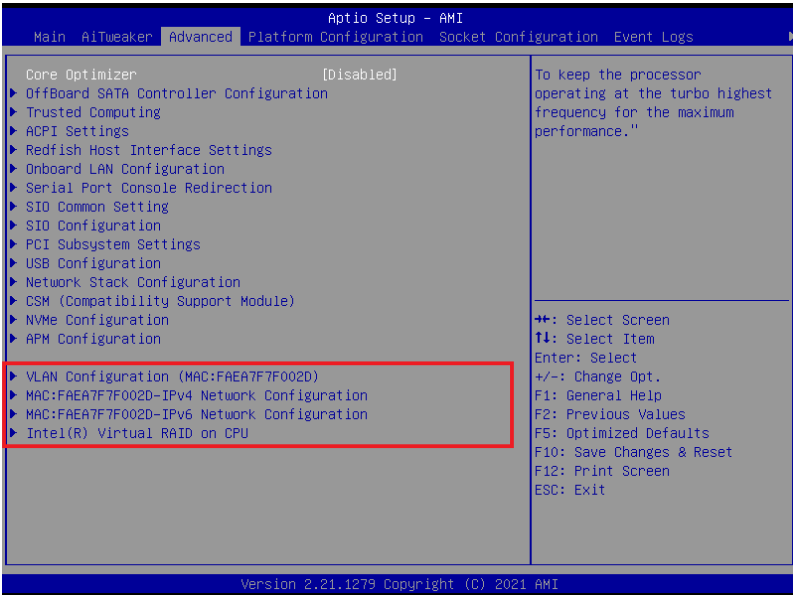
### Power On By RTC [Disabled]

[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.

## 5.5.15 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.

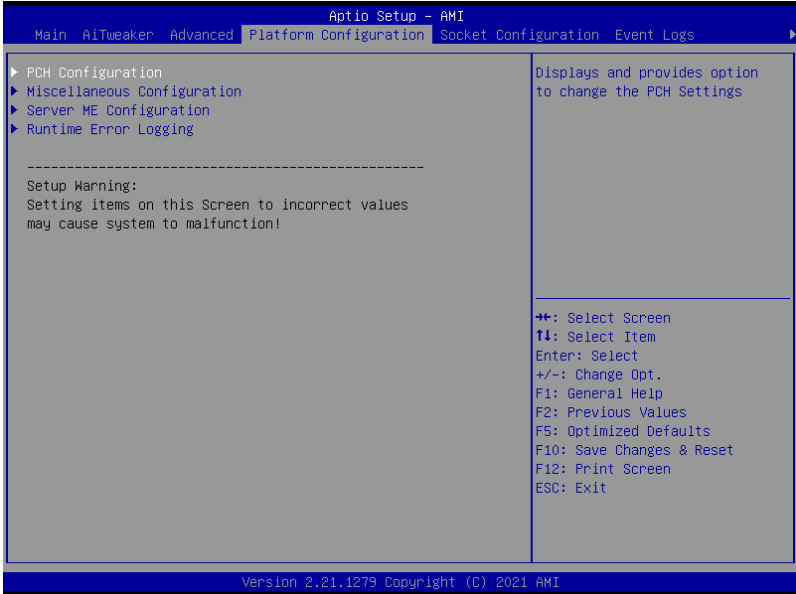


# 5.6 Platform Configuration menu

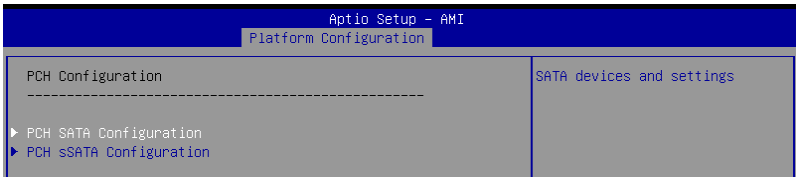
The IntelRCSetup menu items allow you to change the platform settings.



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



## 5.6.1 PCH Configuration



### PCH SATA Configuration

#### SATA Controller [Enable]

Allows you to enable or disable the SATA Controller.

Configuration options: [Disable] [Enable]



---

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

---

### **Configure SATA as [AHCI]**

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

### **SATA Mode options**

This submenu allows you to configure SATA mode related options.

#### ***SATA HDD Unlock [Enable]***

If this item is set to **[Enable]**, HDD password is enabled in the OS.  
Configuration options: [Disable] [Enable]

#### ***SATA Led locate [Enable]***

If this item is set to **[Enable]**, LED/SGPIO hardware is attached.  
Configuration options: [Disable] [Enable]

### **Support Aggressive Link Power Management [Enable]**

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

### **SATA Port 0-7**

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

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

## **PCH sSATA Configuration**

### **sSATA Controller [Enable]**

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



---

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

---

### **Configure sSATA as [AHCI]**

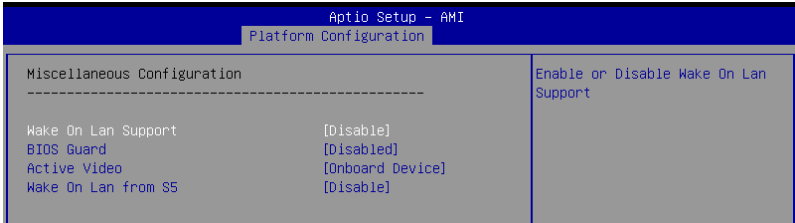
Allows you to identify the SATA port connected to Solid State Drive or Hard Disk Drive.  
Configuration options: [AHCI] [RAID]

### **sSATA Port 0-3**

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

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

## 5.6.2 Miscellaneous Configuration



### Wake on LAN Support [Disable]

Allows you to enable or disable Wake On Lan Support.

Configuration options: [Disable] [Enable]

### 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]

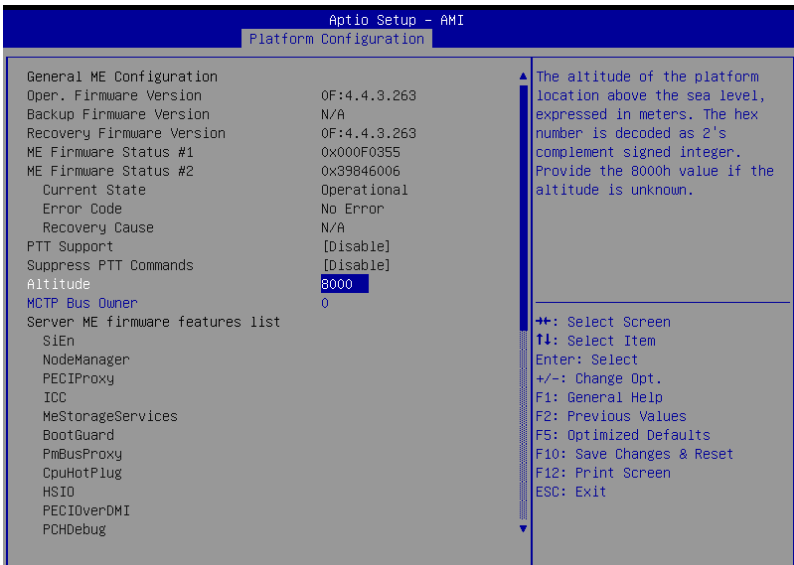
Allows you to enable or disable wake on LAN from S5.

Configuration options: [Disable] [Enable]



### 5.6.3 Server ME Configuration

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



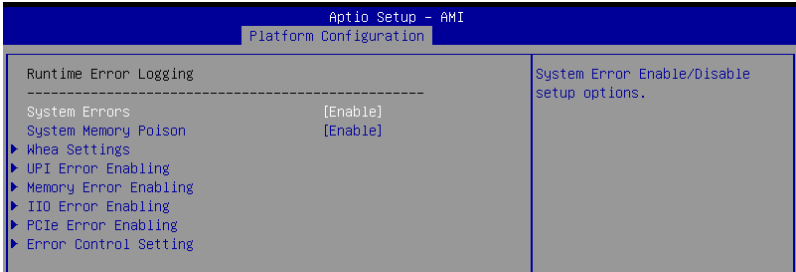
#### Altitude [8000]

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

#### MCTP Bus Owner [0]

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

## 5.6.4 Runtime Error Logging Support



### System Errors [Enable]

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



---

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

---

### System Memory Poison [Enable]

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

### Whea Settings

#### Whea Support [Enable]

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



---

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

---

#### Whea Log Memory Error [Enable]

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

#### Whea Log Processor Error [Enable]

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

#### Whea Log PCI Error [Enable]

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

### UPI Error Enabling

#### 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]

## **IIO Error Enabling**

### **IIO/PCH Global Error Support [Enable]**

Allows you to enable or disable IIO/PCH Global Error Support.

Configuration options: [Disable] [Enable]



---

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

---

### **Os Native AER Support [Disable]**

Select FFM or OS native for AER error handling. If OS native is selected, BIOS also initialize FFM first until handshake, which depends on OS capability.

Configuration options: [Disable] [Enable]

### **IIO Error Registers Clear [Enable]**

Allows you to enable or disable Clear IIO Error Registers.

Configuration options: [Disable] [Enable]

## **PCIe Error Enabling**

### **Corrected Error [Enable]**

Enable & escalate Correctable Errors to error pins.

Configuration options: [Disable] [Enable]

### **Uncorrected Error [Enable]**

Enable & escalate Uncorrectable/Recoverable to error pins.

Configuration options: [Disable] [Enable]

### **Fatal Error Enable [Enable]**

Enable & escalate fatal errors to error pins.

Configuration options: [Disable] [Enable]

## **Error Control Setting**

### **Patrol Scrub Error Reporting [UCNA]**

Allows you to select the Patrol Scrub Error type selection.

Configuration options: [UCNA]

### **2LM Correctable Error Logging in m2mem [Enable]**

Allows you to enable or disable 2LM correctable error logging in m2mem.

Configuration options: [Disable] [Enable]

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

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

Configuration options: [Disable] [Enable]

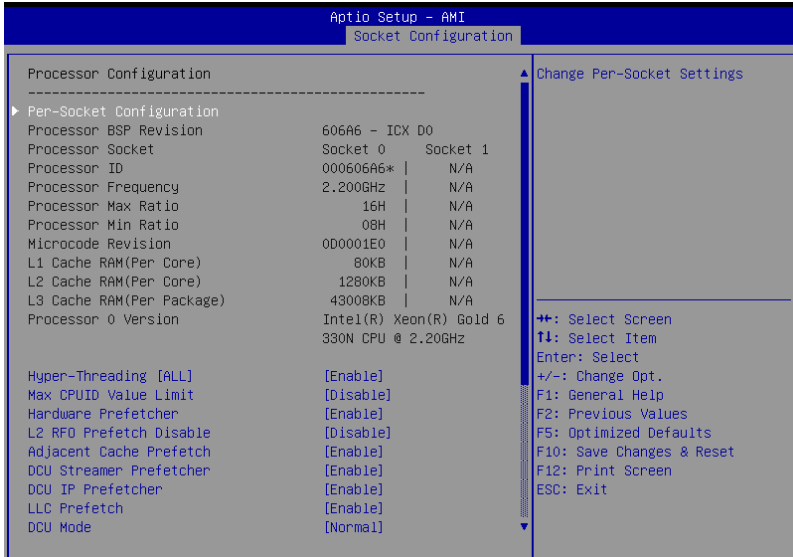
## 5.7 Socket Configuration menu

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



## 5.7.1 Processor Configuration

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



### Per-Socket Configuration

Allows you to change Per-Socket Settings.

#### CPU Socket 0 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 [FFFFFFFFF] 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]

## 5.7.2 Common RefCode Configuration



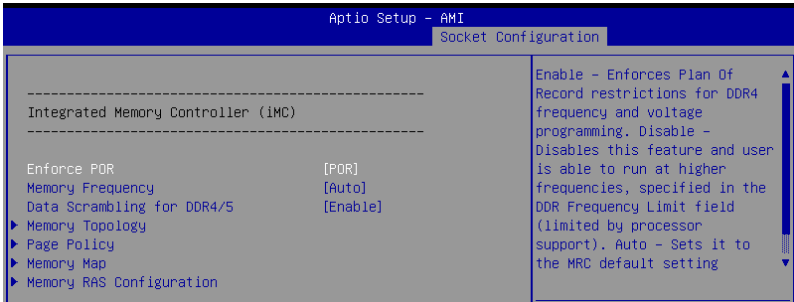
### Numa [Enable]

This item enables or disables the Non uniform Memory Access (NUMA).

Configuration options: [Disable] [Enable]



## 5.7.3 Memory Configuration



### Enforce POR [POR]

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

Configuration options: [POR] [Disable]

### Memory Frequency [Auto]

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

Configuration options: [Auto] [1200] - [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 th platform, Pmem/AppDirect caching knob takes precedence.

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



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

### **CPU Cache Flush Mode [Paralle]**

Allows you to set CPU cache flush execution mode.

Configuration options: [Serial] [Paralle]

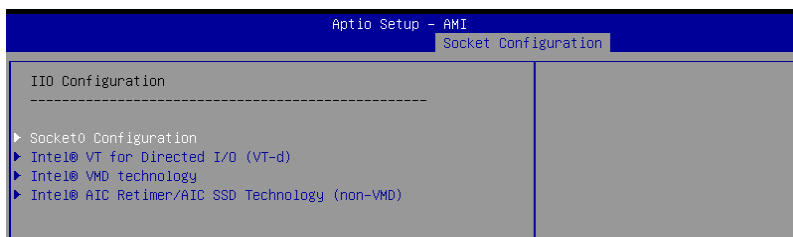
## **Memory RAS Configuration**

Displays and provides options to change the memory RAS Settings.

### **Correctable Error Threshold [7FFF]**

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

## **5.7.4 IIO Configuration**



### **Socket0 Configuration**

#### **IOU0 (IIO PCIe Port 1) [x8x8]**

Allows you to select PCIe port Bifurcation for selected slot(s).

Configuration options: [Auto] [x4x4x4x4] [x4x4x8] [x8x4x4] [x8x8] [x16]

#### **IOU1 (IIO PCIe Port 2) [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) [x4x4x8]**

Allows you to select PCIe port Bifurcation for selected slot(s).

Configuration options: [Auto] [x4x4x4x4] [x4x4x8] [x8x4x4] [x8x8] [x16]

### **IOU4 (IIO PCIe Port 5) [x4x4x4x4]**

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/1C/2A/4A/4C/4D/5A/5B/5C/5D**

Settings related to PCI Express Ports (0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A/4B/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 InvltM (IIO) and/or WCiLF (cores).  
Configuration options: [KTI Option] [Auto] [Enable for Remote InvltM Hybrid Push] [InvltM AllocFlow] [Enable for Remote InvltM Hybrid AllocNonAlloc] [Enable for Remote InvltM 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 0-2****Enable/Disable VMD [Disable]**

Allows you to enable or disable VMD in this Stack.



---

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

---

**VMD Port A-D [Disable]**

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

**Hot Plug Capable [Disable]**

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

**CfgBar size [25]**

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

**CfgBar attribute [64-bit prefetchable]**

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

**MemBar1 size [25]**

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

***MemBar1 attribute [32-bit non-prefetchable]***

Allows you to setup VMD Memory BAR1 attribute, like 64-bit or prefetchable.

Configuration options: [32-bit non-prefetchable] [64-bit non-prefetchable] [64-bit prefetchable]

***MemBar2 size [20]***

Allows you to setup VMD Memory BAR2 size (in bits Min=20), e.g. 20bits=1MB, 22bits=4MB, 26bits=64MB.

Configuration options: [20] - [39]

***MemBar2 attribute [64-bit non-prefetchable]***

Allows you to setup VMD Memory BAR2 attribute, like 64-bit or prefetchable.

Configuration options: [32-bit non-prefetchable] [64-bit non-prefetchable] [64-bit prefetchable]

***VMD Config for IOU 3***

***Enable/Disable VMD [Enable]***

Allows you to enable or disable VMD in this Stack.



---

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

---

***VMD Port A [Disable]***

Allows you to enable or disable Intel® Volume Management Device Technology on specific root port.

Configuration options: [Disable] [Enable]

***VMD Port B [Disable]***

Allows you to enable or disable Intel® Volume Management Device Technology on specific root port.

Configuration options: [Disable] [Enable]

***VMD Port C [Enable]***

Allows you to enable or disable Intel® Volume Management Device Technology on specific root port.

Configuration options: [Disable] [Enable]

***VMD Port D [Enable]***

Allows you to enable or disable Intel® Volume Management Device Technology on specific root port.

Configuration options: [Disable] [Enable]

***Hot Plug Capable [Disable]***

Allows you to enable or disable Hot Plug for PCIe Root Ports.

Configuration options: [Disable] [Enable]

***CfgBar size [25]***

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

Configuration options: [20] - [27]

***CfgBar attribute [64-bit prefetchable]***

Allows you to setup VMD Config BAR attribute, like 64-bit or prefetchable.

Configuration options: [32-bit non-prefetchable] [64-bit non-prefetchable] [64-bit prefetchable]

***MemBar1 size [25]***

Allows you to setup VMD Memory BAR1 size (in bits Min=20), e.g. 20bits=1MB, 22bits=4MB, 26bits=64MB.

Configuration options: [20] - [39]

**MemBar1 attribute [32-bit non-prefetchable]**

Allows you to setup VMD Memory BAR1 attribute, like 64-bit or prefetchable.

Configuration options: [32-bit non-prefetchable] [64-bit non-prefetchable] [64-bit prefetchable]

**MemBar2 size [20]**

Allows you to setup VMD Memory BAR2 size (in bits Min=20), e.g. 20bits=1MB, 22bits=4MB, 26bits=64MB.

Configuration options: [20] - [39]

**MemBar2 attribute [64-bit non-prefetchable]**

Allows you to setup VMD Memory BAR2 attribute, like 64-bit or prefetchable.

Configuration options: [32-bit non-prefetchable] [64-bit non-prefetchable] [64-bit prefetchable]

**VMD Config for IOU 4****Enable/Disable VMD [Enable]**

Allows you to enable or disable VMD in this Stack.



---

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

---

**VMD Port A [Enable]**

Allows you to enable or disable Intel® Volume Management Device Technology on specific root port.

Configuration options: [Disable] [Enable]

**VMD Port B [Enable]**

Allows you to enable or disable Intel® Volume Management Device Technology on specific root port.

Configuration options: [Disable] [Enable]

**VMD Port C [Enable]**

Allows you to enable or disable Intel® Volume Management Device Technology on specific root port.

Configuration options: [Disable] [Enable]

**VMD Port D [Enable]**

Allows you to enable or disable Intel® Volume Management Device Technology on specific root port.

Configuration options: [Disable] [Enable]

**Hot Plug Capable [Enable]**

Allows you to enable or disable Hot Plug for PCIe Root Ports.

Configuration options: [Disable] [Enable]

**CfgBar size [25]**

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

Configuration options: [20] - [27]

**CfgBar attribute [64-bit prefetchable]**

Allows you to setup VMD Config BAR attribute, like 64-bit or prefetchable.

Configuration options: [32-bit non-prefetchable] [64-bit non-prefetchable] [64-bit prefetchable]

**MemBar1 size [25]**

Allows you to setup VMD Memory BAR1 size (in bits Min=20), e.g.

20bits=1MB, 22bits=4MB, 26bits=64MB.

Configuration options: [20] - [39]

### **VMD Config for IOU 3**

#### **Enable/Disable VMD [Enable]**

Allows you to enable or disable VMD in this Stack.



---

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

---

#### **VMD Port A [Disable]**

Allows you to enable or disable Intel® Volume Management Device Technology on specific root port.

Configuration options: [Disable] [Enable]

#### **VMD Port B [Disable]**

Allows you to enable or disable Intel® Volume Management Device Technology on specific root port.

Configuration options: [Disable] [Enable]

#### **VMD Port C [Enable]**

Allows you to enable or disable Intel® Volume Management Device Technology on specific root port.

Configuration options: [Disable] [Enable]

#### **VMD Port D [Enable]**

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]

## **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 Stack3 [Disable]**

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



---

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

---

**Port 3A - 3D [Disable]**

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

**Hot Plug Capable [Disable]**

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

**Intel® AIC Retimer/AIC SSD HW at Stack4 [Disable]**

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



---

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

---

**Port 4A - 4D [Disable]**

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

**Hot Plug Capable [Disable]**

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

**Intel® AIC Retimer/AIC SSD HW at Stack5 [Disable]**

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



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

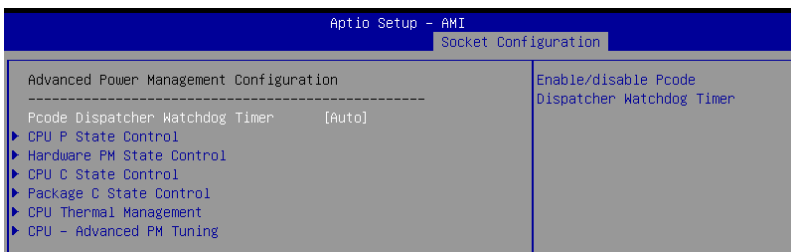
#### **Port 5A - 5D [Disable]**

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

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

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

## 5.7.5 Advanced Power Management Configuration



### **Pcode Dispatcher Watchdog Timer [Auto]**

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

### **CPU P State Control**

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

#### **Uncore Freq Scaling [Enable]**

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



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

#### **Uncore Freq [127]**

Configuration options: [0] - [127]

#### **AVX Licence Pre-Grant Override [Disable]**

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



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

#### **AVX ICCP pre-grant level [128 Heavy]**

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

### **SpeedStep (Pstates) [Enable]**

Allows you to enable or disable EIST (P-States).

Configuration options: [Disable] [Enable]



---

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

---

### **Configure TDP Lock [Enable]**

Allows you to configure TDP CONTROL Lock Bit.

Configuration options: [Disable] [Enable]

### **AVX P1 [Normal]**

AVX P1 level selection.

Configuration options: [Normal] [Level 1] [Level 2]

### **Activate SST-BF [Disable]**

Allows you to enable or disable SST-BF.

Configuration options: [Disable] [Enable]



---

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

---

### **Configure SST-BF [Enable]**

Allows BIOS to configure SST-BF High Priority Cores so that SW does not have to configure.

Configuration options: [Disable] [Enable]

### **EIST PSD Function [HW\_ALL]**

Configuration options: [HW\_ALL] [SW\_ALL]

### **Boot performance mode [Max Performance]**

Allows you to select the performance state that the BIOS will set before OS hand off.

Configuration options: [Max Performance] [Max Efficient] [Set by Intel Node Manager]

### **Energy Efficient Turbo [Enable]**

Allows you to enable or disable Energy Efficient Turbo.

Configuration options: [Disable] [Enable]

### **Turbo Mode [Enabled]**

Allows you to enable or disable processor Turbo Mode (requires EMTTM enabled as well).

Configuration options: [Disable] [Enable]

### **CPU Flex Ratio Override [Disable]**

Allows you to enable or disable CPU Flex Ratio Programming.

Configuration options: [Disable] [Enable]

### **CPU Flex Ratio [23]**

Non-Turbo Mode Processor Core Ratio Multiplier.

Configuration options: [0] - [100]



### GPSS timer [500 us]

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

### Perf P-Limit

#### **Perf P-Limit Differential [1]**

Parameter used to tune how far below local socket frequency remote socket frequency is allowed to be. Also impacts rate at which frequency drops when feature disengages.

#### **Perf P-Limit Clip [1F]**

Maximum value the floor is allowed to be set to for perf P-Limit.

#### **Perf P-Limit Threshold [F]**

Uncore frequency threshold above which this socket will trigger the feature and start trying to raise frequency of other sockets.

#### **Perf P-Limit [Enable]**

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

## Hardware PM State Control

### Hardware P-States [Native Mode]

Allows you to switch between Hardware P-States mode.

[Disable] Hardware chooses a P-state based on OS Request (Legacy P-States).

[Native Mode] Hardware chooses a P-state based on OS guidance.

[Out of Band Mode] Hardware autonomously chooses a P-state (no OS guidance).

[Native Mode with no Legacy Support] Hardware chooses a P-state based on OS guidance (without Legacy support).



---

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

---

### HardwarePM Interrupt [Disable]

Allows you to enable or disable Hardware PM Interrupt.

Configuration options: [Disable] [Enable]



---

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

---

### EPP Enable [Enable]

When disabled, HW masks EPP in CPUID[6].10 and uses EPB for EPP.

Configuration options: [Disable] [Enable]



---

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

---

### EPP profile [Balanced Performance]

Allows you to choose an HWPM Profile (EPP).

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

**APS rocketing [Disable]**

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

Configuration options: [Disable] [Enable]

**Scalability [Disable]**

Allows you to enable or disable Core Performance to Frequency Scalability Based Optimizations in the CPU.

Configuration options: [Disable] [Enable]

**Native ASPM [Disabled]**

[Auto] BIOS Controlled ASPM

[Enabled] OS Controlled ASPM

[Disabled] ASPM Off

**CPU C State Control****Enable Monitor MWAIT [Enable]**

Allows you to enable or disable Monitor and MWAIT instructions.

Configuration options: [Disable] [Enable]

**CPU C1 auto demotion [Enable]**

Allows CPU to automatically demote to C1. Takes effect after reboot.

Configuration options: [Disable] [Enable]

**CPU C1 auto undemotion [Enable]**

Allows CPU to automatically undemote from C1. Takes effect after reboot.

Configuration options: [Disable] [Enable]

**CPU C6 Report [Auto]**

Allows you to enable or disable CPU C6 (ACPI C3) report to OS.

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

**Enhanced Halt State (C1E) [Enable]**

Core C1E auto promotion Control. Takes effect after reboot.

Configuration options: [Disable] [Enable]

**OS ACPI Cx [ACPI C2]**

Allows you to select to report CC3/CC6 to OS ACPI C2 or ACPI C3.

Configuration options: [ACPI C2] [ACPI C3]

**Package C State Control****Package C State [Auto]**

Allows you to select Package C State limit.

Configuration options: [C0/C1 state] [C2 state] [C6(non Retention state) [Auto]

## Register Access Low Latency Mode [Disabled]

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



---

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

---

## CPU Thermal Management

### CPU T State Control

#### **Software Controlled T-States [Disabled]**

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



---

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

---

#### **T-State Throttle Level [Disable]**

On-Die Thermal Throttling.

Configuration options: [Disabled] [6.25%] [12.5%] [18.75%] [25.0%] [31.25%] [37.5%] [43.75%] [50.0%] [56.25%] [62.5%] [68.75%] [75.0%] [81.25%] [87.5%] [93.75%]

## CPU - Advanced PM Tuning

### Energy Perf BIAS

#### **Power Performance Tuning [PECI Controls EPB]**

Configuration options: [OS Controls EPB] [BIOS Controls EPB] [PECI Controls EPB]



---

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

---

#### **PECI CPS EPB [OS controls EPB]**

Controls whether Peci has control over EPB.

Configuration options: [OS Controls EPB] [PECI Controls EPB using PCS]



---

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

---

#### **ENERGY\_PERF\_BIAS\_CFG mode [Balanced Performance]**

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

#### **Dynamic Loadline Switch [Enable]**

Configuration options: [Disable] [Enable]

#### **Workload Configuration [Balanced]**

This allows optimization for the workload characterization.

Configuration options: [Balanced] [I/O Sensitive]

#### **Averaging Time Window [1A]**

This is used to control the effective window of the average for C0 and P0 time.

### ***P0 TotalTimeThreshold Low [28]***

This is used to control the effective window of the average for C0 and P0 time.

### ***P0 TotalTimeThreshold High [3F]***

This is used to control the effective window of the average for C0 and P0 time.

### **SAPM Control [Enable]**

Configuration options: [Enable] [Disable]

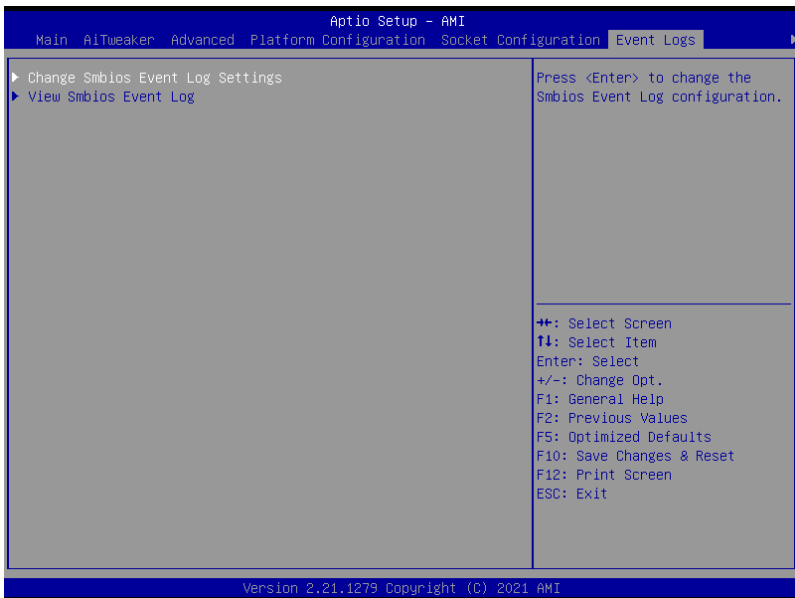
### **EET Mode [Coarse Grained Mode]**

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

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

## **5.8 Event Logs menu**

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

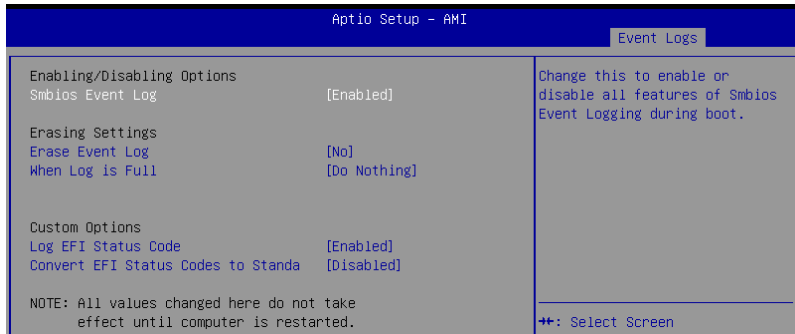


## 5.8.1 Change Smbios Event Log Settings

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



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



### Enabling/Disabling Options

#### Smbios Event Log [Enabled]

Change this to enable or disable all features of Smbios Event Logging during boot.

Configuration options: [Disabled] [Enabled]



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

### Erasing Settings

#### Erase Event Log [No]

Choose options for erasing Smbios Event Log. Erasing is done prior to any logging activation during reset.

Configuration options: [No] [Yes, Next reset] [Yes, Every reset]

#### When Log is Full [Do Nothing]

Choose options for reactions to a full Smbios Event Log.

Configuration options: [Do Nothing] [Erase Immediately]

### Custom Options

#### Log EFI Status Code [Enabled]

Allows you to enable or disable the logging of EFI Status Codes as OEM reserved type E0 (if not already converted to legacy).

Configuration options: [Disabled] [Enabled]



---

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

---

### **Convert EFI Status Codes to Standard Smbios Type [Disabled]**

Allows you to enable or disable the converting of EFI Status Codes to Standard Smbios Types (not all may be translated).

Configuration options: [Disabled] [Enabled]

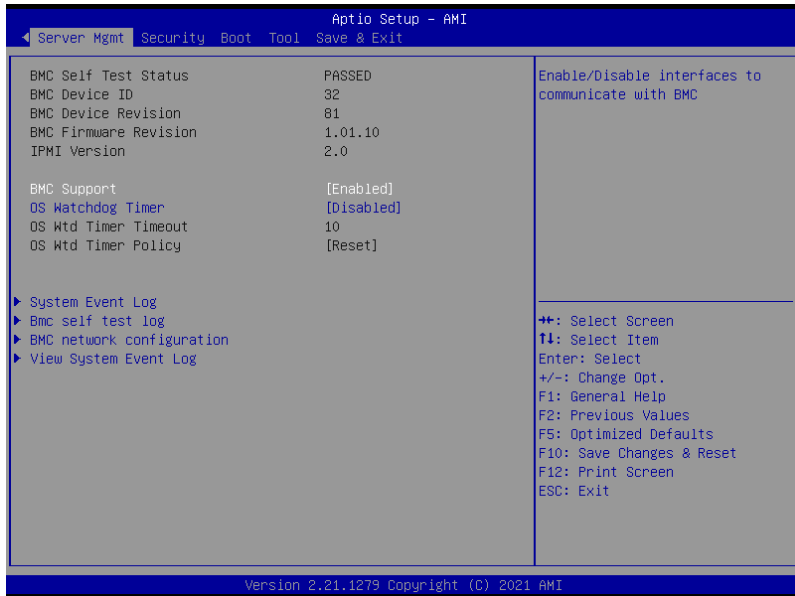
## **5.8.2 View Smbios Event Log**

Press <Enter> to view all smbios event logs.

Aptio Setup - AMI					
					Event Logs
DATE	TIME	ERROR CODE	SEVERITY	COUNT	DESCRIPTION
01/12/05	00:45:51	Smbios 0x16	N/A	N/A	Log Area Reset

## 5.9 Server Mgmt menu

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



### BMC Support [Enabled]

Allows you to enable or disable interfaces to communicate with BMC.

Configuration options: [Disabled] [Enabled]



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

### OS Watchdog Timer [Disabled]

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

Configuration options: [Disabled] [Enabled]



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

### OS Wtd Timer Timeout [10]

Allows you to enter a value between 1 to 30 minutes for OS Boot Watchdog Timer Expiration. Not available if OS Boot Watchdog Timer is disabled.

Configuration options: [1] - [30]

### OS Wtd Timer Policy [Reset]

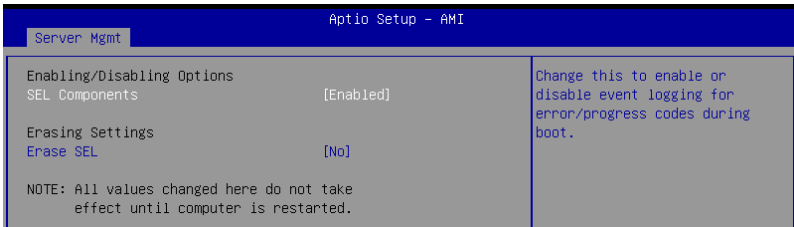
This item allows you to configure the how the system should respond if the OS Boot Watch Timer expires. Not available if OS Boot Watchdog Timer is disabled.  
Configuration options: [Do Nothing] [Reset] [Power Down] [Power Cycle]

## 5.9.1 System Event Log

Allows you to change the SEL event log configuration.



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



### SEL Components [Enabled]

Allows you to enable or disable event logging for error/progress codes during boot.  
Configuration options: [Disabled] [Enabled]



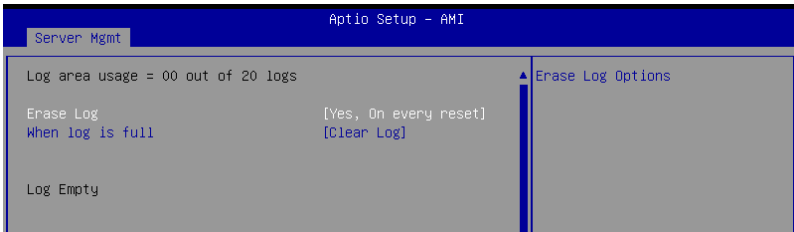
The following item is available only when **SEL Components** is set to **[Enabled]**.

### Erase SEL [No]

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

## 5.9.2 BMC self test log

Logs the report returned by BMC self test command.



### Erase Log [Yes, On every reset]

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



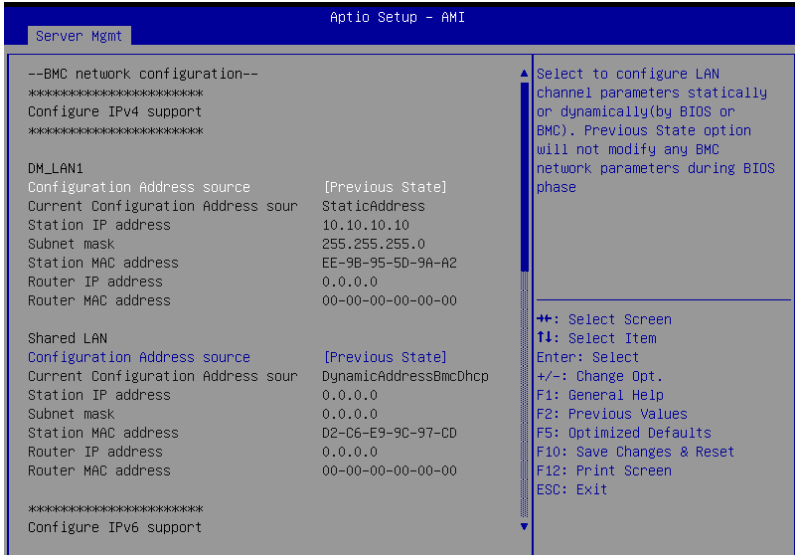
### When log is full [Clear Log]

Select the action to be taken when log is full.

Configuration options: [Clear Log] [Do not log any more]

## 5.9.3 BMC network configuration

The sub-items in this configuration allow you to configure the BMC network parameters. Scroll using <Page Up> / <Page Down> keys to see more items.



### Configure IPv4 support

#### DM\_LAN1 / Shared LAN

#### Configuration Address source [Previous State]

Allows you to set the LAN channel parameters statically or dynamically (by BIOS or by BMC). [Previous State] option will not modify any BMC network parameters during BIOS phase.

Configuration options: [Previous State] [Static] [DynamicBmcDhcp]



The following items are available only when **Configuration Address source** is set to [Static].

#### Station IP address

Allows you to set the station IP address.

#### Subnet mask

Allows you to set the subnet mask. We recommend that you use the same Subnet Mask you have specified on the operating system network for the used network card.

### Router IP Address

Allows you to set the router IP address.

### Router MAC Address

Allows you to set the router MAC address.

## Configure IPV6 support

### DM\_LAN1 / Shared LAN

#### IPV6 support [Enabled]

Allows you to enable or disable IPV6 support.

Configuration options: [Enabled] [Disabled]



---

The following items appear only when **IPV6 support** is set to **[Enabled]**.

---

#### Configuration Address source [Previous State]

Allows you to set the LAN channel parameters statically or dynamically (by BIOS or by BMC). **[Previous State]** option will not modify any BMC network parameters during BIOS phase.

Configuration options: [Previous State] [Static] [DynamicBmcDhcp]



---

The following items are available only when **Configuration Address source** is set to **[Static]**.

---

#### Station IPV6 address

Allows you to set the station IPV6 address.

#### Prefix Length

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

#### 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.

## 5.9.4 View System Event Log

This item allows you to view the system event log records. Scroll using <Page Up> / <Page Down> keys to see more items.

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	04:45:40	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

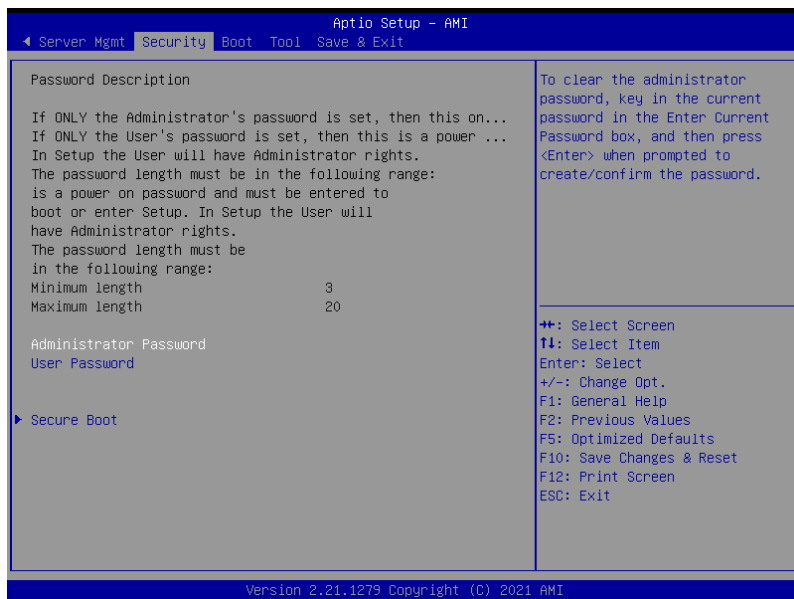
▲ HEX:  
01 00 02 20 1A E4  
5F 20 00 04 08 DF  
01 50 00 00  
Generator ID: BMC - LUN #0  
(Channel #0)  
Sensor Number: 0xDF DEM  
(Unknown)  
Event Description:  
Record Type-0x02.  
Assertion Event.

◆◆: 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

▼

## 5.10 Security menu

This menu allows a new password to be created or a current password to be changed. The menu also enables or disables the Secure Boot state and lets the user configure the System Mode state.



### Administrator Password

To set an administrator password:

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

To change an administrator password:

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



To clear the administrator password, follow the same steps as in changing an administrator password, but press <Enter> when prompted to create/confirm the password.

## User Password

To set a user password:

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

To change a user password:

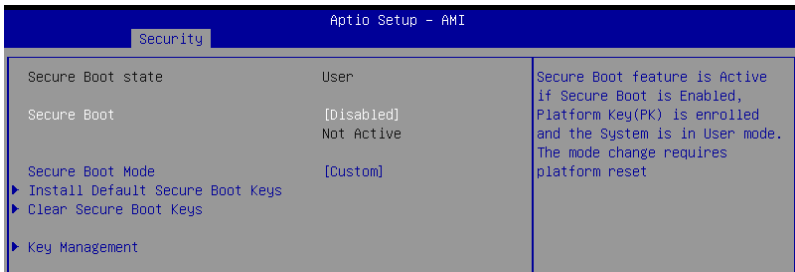
1. Select the User Password item and press <Enter>.
2. From the Enter Current Password box, key in the current password, then press <Enter>.
3. From the Create New Password box, key in a new password, then press <Enter>.
4. Confirm the password when prompted.

To clear a user password:

1. Select the Clear User Password item and press <Enter>.
2. Select **Yes** from the Warning message window then press <Enter>.

## 5.10.1 Secure Boot

This item allows you to customize the Secure Boot settings.



### Secure Boot [Disabled]

Secure Boot feature is active if Secure Boot is Enabled, Platform Key (PK) is enrolled and the system is in User mode. The mode change requires platform reset.

Configuration options: [Disabled] [Enabled]

### Secure Boot Mode [Custom]

Allows you to set the Secure Boot selector. In Custom mode, Secure Boot Policy variables can be configured physically by the present user without full authentication.

Configuration options: [Custom] [Standard]



The following items are available only when **Secure Boot Mode** is set to **[Custom]**.

## Install Default Secure Boot Keys

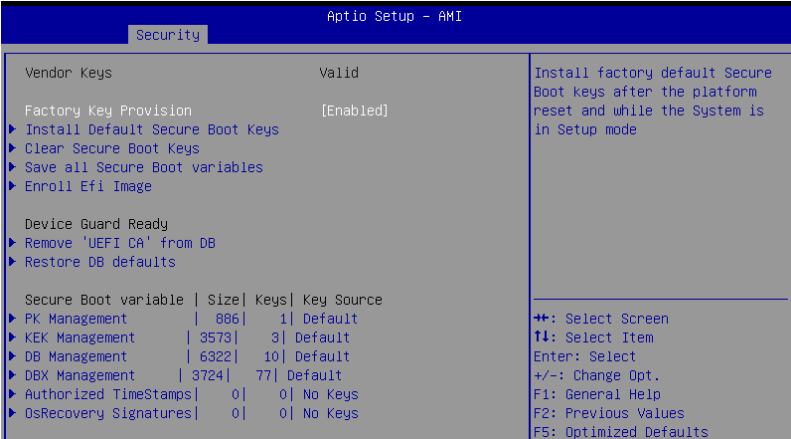
This option will load the default secure boot keys, including the PK (Platform key), KEK (key-exchange key), db (signature database), and dbx (revoked signature database). All the secure boot keys states will change from unloaded to loaded. Save changes and reset the system for the changes to take effect.

## Clear Secure Boot Keys

This option will delete all previously applied secure boot keys, including the PK (Platform key), KEK (key-exchange key), db (signature database), and dbx (revoked signature database). All the secure boot keys states will change from unloaded to loaded. Save changes and reset the system for the changes to take effect.

## Key Management

This item only appears when the item **Secure Boot Mode** is set to **[Custom]**. The Key Management item allows you to modify Secure Boot variables and set Key Management page.



The screenshot shows the 'Security' menu in the Aptio Setup - AMI BIOS. The 'Factory Key Provision' option is set to '[Enabled]'. Below it, there are several options: 'Install Default Secure Boot Keys', 'Clear Secure Boot Keys', 'Save all Secure Boot variables', and 'Enroll Efi Image'. There is also a 'Device Guard Ready' section with options to 'Remove 'UEFI CA' from DB' and 'Restore DB defaults'. A table lists 'Secure Boot variable' with columns for 'Size', 'Keys', and 'Key Source'. The table includes entries for PK Management, KEK Management, DB Management, and DBX Management. At the bottom, there are navigation instructions: '++: Select Screen', '↑: Select Item', '+/-: Change Opt.', 'F1: General Help', 'F2: Previous Values', and 'F5: Optimized 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

### 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**

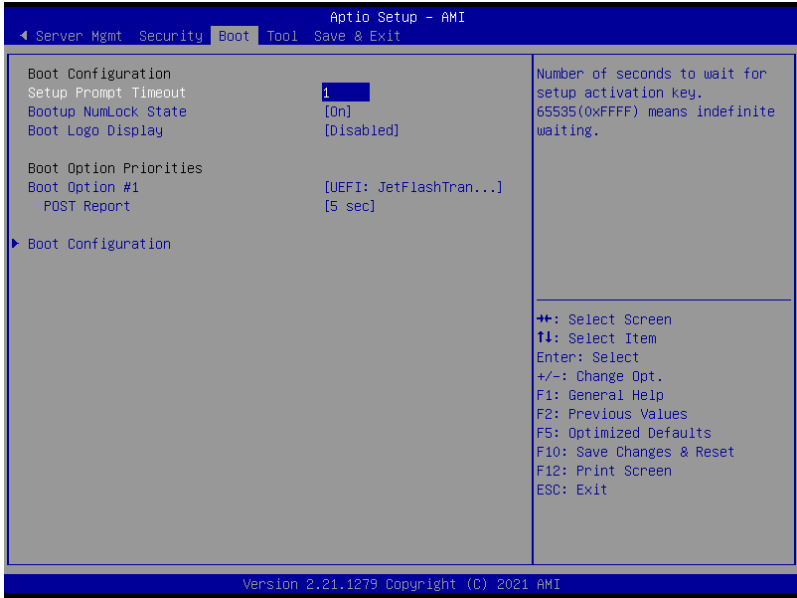
Configuration options: [Details] [Save To File] [Set New Key] [Append Key] [Delete key]

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

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

# 5.11 Boot menu

The Boot menu items allow you to change the system boot options.



## Setup Prompt Timeout [1]

Allows you to set the number of seconds that the firmware waits before initiating the original default boot selection. 65535(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]

## 5.11.1 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]**.

---

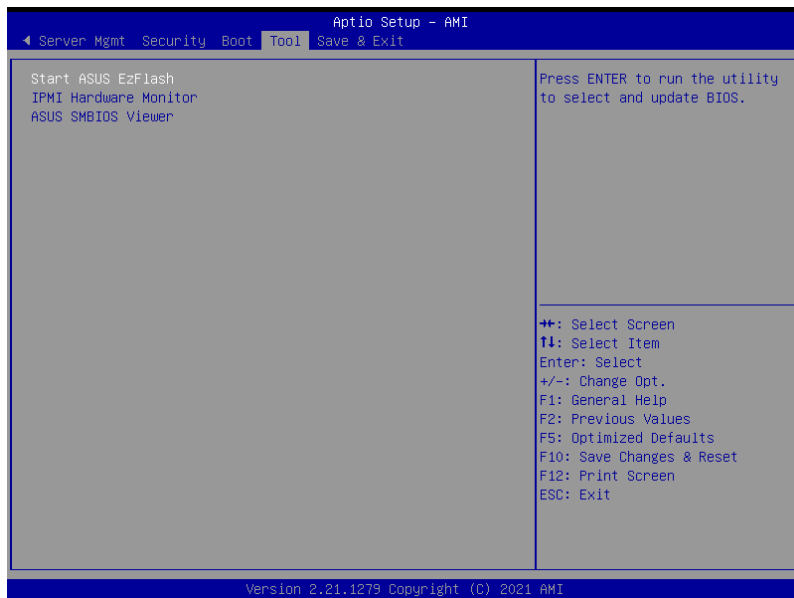
### Next Boot Recovery Action [Skip]

Allows you to select the (MBR/GPT) recovery action on the next boot.

Configuration options: [Skip] [Recovery]

## 5.12 Tool menu

The Tool menu items allow you to configure options for special functions. Select an item then press <Enter> to display the submenu.



### Start ASUS EzFlash

Allows you to run ASUS EzFlash BIOS ROM Utility when you press <Enter>. Refer to the ASUS EzFlash Utility section for details.

### IPMI Hardware Monitor

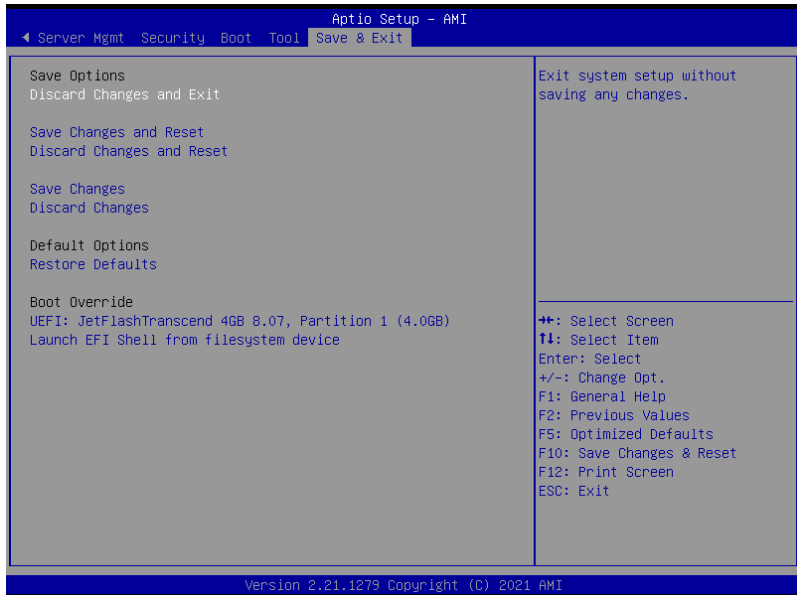
Allows you to run the IPMI hardware monitor.

### ASUS SMBIOS Viewer

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

## 5.13 Save & Exit menu

The Save & Exit menu items allow you to save or discard your changes to the BIOS items.



Pressing <Esc> does not immediately exit this menu. Select one of the options from this menu or <F10> from the legend bar to exit.

### Discard Changes and Exit

Exit system setup without saving any changes.

### Save Changes and Reset

Reset system after saving the changes.

### Discard Changes and Reset

Reset system setup without saving any changes.

### Save Changes

Save changes done so far to any of the setup options.

### Discard Changes

Discard changes done so far to any of the setup options.

### Restore Defaults

Restore/load default values for all the setup options.

## **Boot Override**

These items displays the available devices. The device items that appears on the screen depends on the number of devices installed in the system. Click an item to start booting from the selected device.

# Driver Installation

# 6

This chapter provides the instructions for installing the necessary drivers for different system components in the Windows® Operating System.

## 6.1 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 support DVD is supported on Windows® Server 2016 and Windows® Server 2019.

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).



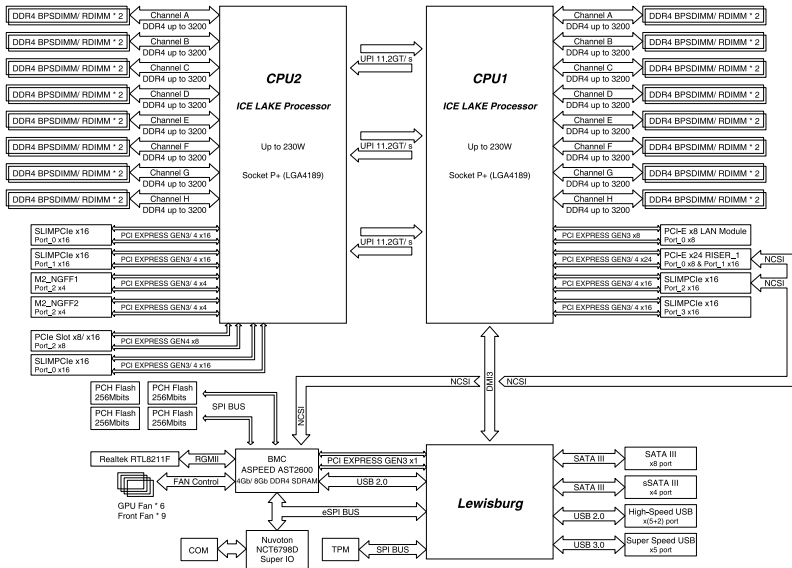
You need an Internet browser installed in your OS to view the User Guide.

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.

# Z12PP-D32 block diagram





## Notices

### Federal Communications Commission Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.



---

The use of shielded cables for connection of the monitor to the graphics card is required to assure compliance with FCC regulations. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

---

### Compliance Statement of Innovation, Science and Economic Development Canada (ISED)

This device complies with Innovation, Science and Economic Development Canada licence exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

CAN ICES-003(A)/NMB-003(A)

### Déclaration de conformité de Innovation, Sciences et Développement économique Canada (ISED)

Le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

CAN ICES-003(A)/NMB-003(A)

## Australia statement notice

From 1 January 2012 updated warranties apply to all ASUS products, consistent with the Australian Consumer Law. For the latest product warranty details please visit <https://www.asus.com/support/>. Our goods come with guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure.

If you require assistance please call ASUS Customer Service 1300 2787 88 or visit us at <https://www.asus.com/support/>.



---

DO NOT throw the motherboard in municipal waste. This product has been designed to enable proper reuse of parts and recycling. This symbol of the crossed out wheeled bin indicates that the product (electrical and electronic equipment) should not be placed in municipal waste. Check local regulations for disposal of electronic products.

---



---

DO NOT throw the mercury-containing button cell battery in municipal waste. This symbol of the crossed out wheeled bin indicates that the battery should not be placed in municipal waste.

---

## Japan statement notice

This product cannot be directly connected to the Internet (including public wireless LAN) of a telecom carrier (mobile network companies, landline network companies, Internet providers, etc.). When connecting this product to the Internet, be sure to connect it through a router or switch.

## **Declaration of compliance for product environmental regulation**

ASUS follows the green design concept to design and manufacture our products, and makes sure that each stage of the product life cycle of ASUS product is in line with global environmental regulations. In addition, ASUS disclose the relevant information based on regulation requirements.

Please refer to <http://csr.asus.com/Compliance.htm> for information disclosure based on regulation requirements ASUS is complied with:

### **EU REACH and Article 33**

Complying with the REACH (Registration, Evaluation, Authorization, and Restriction of Chemicals) regulatory framework, we publish the chemical substances in our products at ASUS REACH website at <http://csr.asus.com/english/REACH.htm>.

### **EU RoHS**

This product complies with the EU RoHS Directive. For more details, see <http://csr.asus.com/english/article.aspx?id=35>

### **Japan JIS-C-0950 Material Declarations**

Information on Japan RoHS (JIS-C-0950) chemical disclosures is available on <http://csr.asus.com/english/article.aspx?id=19>

## India RoHS

This product complies with the “India E-Waste (Management) Rules, 2016” and prohibits use of lead, mercury, hexavalent chromium, polybrominated biphenyls (PBBs) and polybrominated diphenyl ethers (PBDEs) in concentrations exceeding 0.1% by weight in homogenous materials and 0.01% by weight in homogenous materials for cadmium, except for the exemptions listed in Schedule II of the Rule.

## Vietnam RoHS

ASUS products sold in Vietnam, on or after September 23, 2011, meet the requirements of the Vietnam Circular 30/2011/TT-BCT.

Các sản phẩm ASUS bán tại Việt Nam, vào ngày 23 tháng 9 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>.

## Service and Support

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

