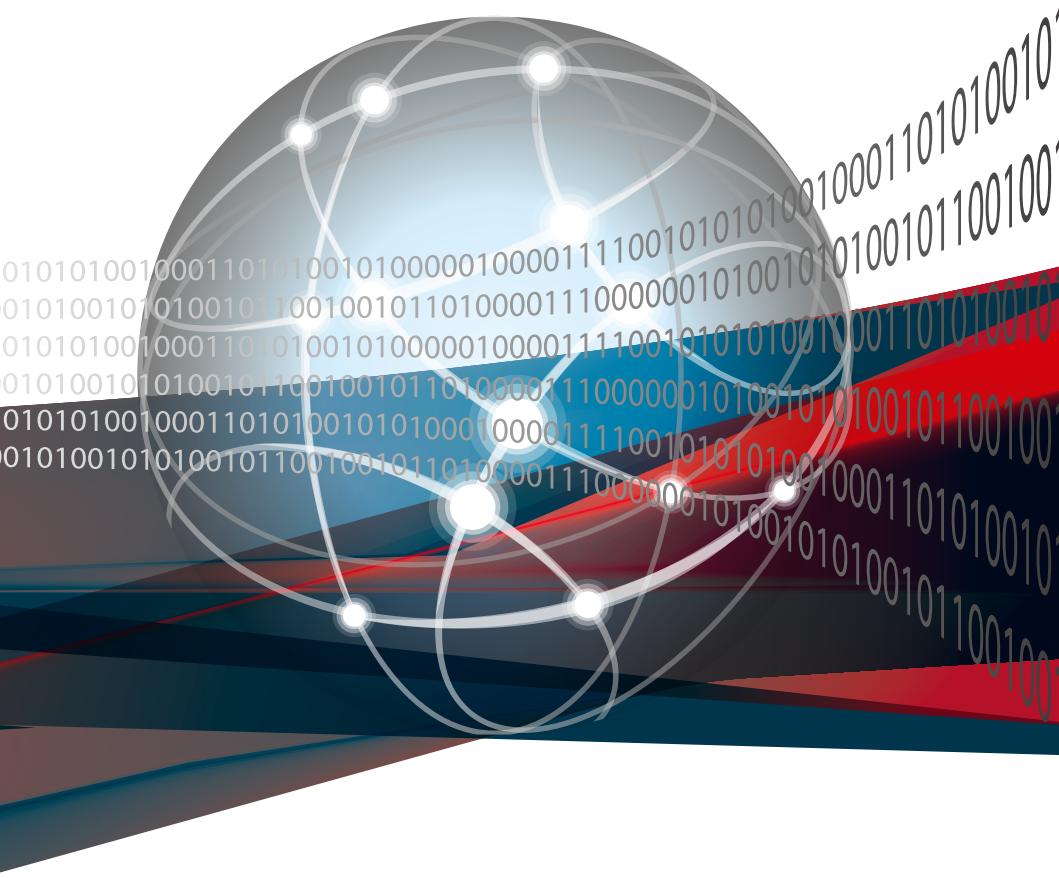




# **ESC N4A-E11**

## **3U Rackmount Server User Guide**



E18522  
First Edition  
September 2021

**Copyright © 2021 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

<b>Safety information</b> .....	vi
<b>About this guide</b> .....	viii

## Chapter 1: Product Introduction

<b>1.1 System package contents</b> .....	1-2
<b>1.2 Serial number label</b> .....	1-2
<b>1.3 System specifications</b> .....	1-3
<b>1.4 Front panel features</b> .....	1-5
<b>1.5 Rear panel features</b> .....	1-6
<b>1.6 Internal features</b> .....	1-7
<b>1.7 LED information</b> .....	1-9
1.7.1    Front panel LEDs .....	1-9
1.7.2    LAN (RJ-45) LEDs .....	1-10
1.7.3    Storage device status LEDs.....	1-11
1.7.4    Rear panel LEDs.....	1-11
1.7.4    Q-Code/Port 80 status LEDs.....	1-12

## Chapter 2: Hardware Setup

<b>2.1 Chassis cover</b> .....	2-2
2.1.1    Removing the rear cover.....	2-2
<b>2.2 Storage devices</b> .....	2-3
2.2.1    Installing a 3.5-inch storage device.....	2-3
2.2.2    Installing a 2.5-inch storage device.....	2-4
<b>2.3 Expansion slots</b> .....	2-5
2.3.1    Installing an expansion card to the right riser card bracket.....	2-5
2.3.2    Installing an expansion card to the left riser card bracket.....	2-9
2.3.3    Installing an OCP 3.0 slot baseboard and OCP 3.0 card to the PCIe riser card bracket .....	2-12

## Chapter 3: Installation Options

<b>3.1 Rail Kit</b> .....	3-2
3.1.1    Selecting rack rail cabinets .....	3-2
3.1.2    Attaching the rack rails .....	3-3
<b>3.2 Cable management arm (optional for 1200 mm rack rails)</b> .....	3-8
3.2.1    Attaching the cable management arm .....	3-8

# Contents

## Chapter 4: BIOS Setup

<b>4.1</b>	<b>Managing and updating your BIOS .....</b>	<b>4-2</b>
4.1.1	ASUS CrashFree BIOS 3 utility.....	4-2
4.1.2	ASUS EzFlash Utility.....	4-3
4.1.3	BUPDATER utility .....	4-4
<b>4.2</b>	<b>BIOS setup program .....</b>	<b>4-6</b>
4.2.1	BIOS menu screen.....	4-7
4.2.2	Menu bar.....	4-7
4.2.3	Menu items.....	4-8
4.2.4	Submenu items .....	4-8
4.2.5	Navigation keys.....	4-8
4.2.6	General help.....	4-8
4.2.7	Configuration fields .....	4-8
4.2.8	Pop-up window.....	4-8
4.2.9	Scroll bar .....	4-8
<b>4.3</b>	<b>Main menu .....</b>	<b>4-9</b>
4.3.1	System Language [English] .....	4-9
4.3.2	System Date [Day xx/xx/xxxx] .....	4-9
4.3.3	System Time [xx:xx:xx] .....	4-9
<b>4.4</b>	<b>Performance Tuning menu.....</b>	<b>4-10</b>
<b>4.5</b>	<b>Advanced menu .....</b>	<b>4-11</b>
4.5.2	Trusted Computing.....	4-11
4.5.2	PSP Firmware Versions.....	4-12
4.5.3	Redfish Host Interface Settings.....	4-12
4.5.4	AMD CBS.....	4-12
4.5.5	APM Configuration.....	4-45
5.5.6	Onboard LAN Configuration.....	4-45
4.5.7	Serial Port Console Redirection.....	4-46
4.5.8	CPU Configuration .....	4-49
4.5.9	PCI Subsystem Settings .....	4-49
4.5.10	USB Configuration .....	4-50
4.5.11	Network Stack Configuration.....	4-51
4.5.12	CSM Configuration.....	4-52
4.5.13	NVMe Configuration.....	4-53
4.5.14	AMD Mem Configuration Status.....	4-54
4.5.15	Third-party UEFI driver configurations .....	4-54
<b>4.6</b>	<b>Chipset menu .....</b>	<b>4-55</b>

## Contents

<b>4.7</b>	<b>Security menu .....</b>	<b>4-57</b>
<b>4.8</b>	<b>Boot menu .....</b>	<b>4-60</b>
<b>4.9</b>	<b>Tool menu .....</b>	<b>4-62</b>
<b>4.10</b>	<b>Event Logs menu .....</b>	<b>4-63</b>
4.10.1	Change Smbios Event Log Settings .....	4-63
4.10.2	View Smbios Event Log .....	4-64
<b>4.11</b>	<b>Server Mgmt menu.....</b>	<b>4-65</b>
4.11.1	System Event Log.....	4-66
4.11.2	BMC network configuration.....	4-66
4.11.3	View System Event Log .....	4-69
<b>4.12</b>	<b>Exit menu.....</b>	<b>4-70</b>

## Chapter 5: Driver Installation

<b>5.1</b>	<b>Running the Support DVD.....</b>	<b>5-2</b>
------------	-------------------------------------	------------

## Appendix

<b>KMPN-U16 block diagram .....</b>	<b>A-2</b>
<b>Notices .....</b>	<b>A-3</b>
<b>Service and Support .....</b>	<b>A-5</b>

# Safety information

## Electrical Safety

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

## Operation Safety

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



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

## Restricted Access Location

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

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

### Heavy System

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

## Lithium-Ion Battery Warning

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

## Avertissement sur les batteries Lithium-Ion

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

# About this guide

## Audience

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

## Contents

This guide contains the following parts:

### 1. Chapter 1: Product Introduction

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

### 2. Chapter 2: Hardware Setup

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

### 3. Chapter 3: Installation Options

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

### 4. Chapter 4: BIOS Setup

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

### 5. Chapter 5: Driver Installation

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

## Conventions

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



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



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



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



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

## Typography

<b>Bold text</b>	Indicates a menu or an item to select.
<i>Italics</i>	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>
<b>Command</b>	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: <b>format A:/s</b>

## References

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

### ASUS websites

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



# 1

## **Product Introduction**

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

## 1.1 System package contents

Check your system package for the following items.

ESC N4A-E11	
Chassis	ASUS 3U Rackmount Chassis
Motherboard	ASUS KMPN-U16 Server Board
Accessory box	1 x MB Support DVD 1 x ACC instruction card 1 x Bag of Screws 2 x AC Power Cables 1 x CPU heatsink 1 x Rail Kit (optional)



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

## 1.2 Serial number label

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

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



The serial number is printed on the Asset tag.

## 1.3 System specifications

The ASUS ESC N4A-E11 Series servers features the ASUS KMPN-U16 server board that supports AMD EPYC™ 7003 series processors.

Model Name		ESC N4A-E11
<b>Processor</b>		AMD EPYC™ 7003 series processors (min. 32 cores/up to 280W)
<b>GPU</b>		<ul style="list-style-type: none"> <li>- SKU 1: HGX A100 4-GPU 40GB(160GB total) 400W</li> <li>- SKU 2: HGX A100 4-GPU 80GB(320GB total) 500W</li> </ul> <p>(Optional Asetek Liquid Cooling solution for 500W support)</p>
<b>Memory</b>	Total Slots	16
	Capacity	Maximum up to 4,096GB
	Memory Type	DDR4 3200/2933 RDIMM/LRDIMM/LRDIMM 3DS * Please refer to <a href="http://www.asus.com">www.asus.com</a> for latest memory AVL update
	Memory Size	<ul style="list-style-type: none"> <li>64GB, 32GB, 16GB (RDIMM)</li> <li>128GB, 64GB (LRDIMM)</li> <li>256GB, 128GB, 64GB (LRDIMM 3DS / 3DS RDIMM)</li> </ul> <p>* Please refer to <a href="http://www.asus.com">www.asus.com</a> for latest memory AVL update</p>
	Total PCI/PCI-X/ PCI-E/PIKE Slots	3
<b>Expansion Slots</b>	Slot Type	PCIe Gen4 x16 (1 x OCP support)
	SATA/SAS Controller	<p>Optional Kits:</p> <ul style="list-style-type: none"> <li>- ASUS PIKE II 3008 8-port SAS 12Gb/s HBA Card</li> <li>- ASUS PIKE II 3108 8-port SAS HW 12Gb/s RAID Card</li> </ul> <p>Support SATA 6Gbps / SAS 12Gbps</p>
	NVMe Controller	<p>Optional Kits:</p> <ul style="list-style-type: none"> <li>- Broadcom MegaRAID 9560-16i card</li> <li>Default supports 2 x NVMe</li> </ul>
<b>Disk Controller</b>	M.2	1 x M.2 socket Gen 4 x4 link, up to 2280
	LAN	<p>2 x RJ45 10G LAN ports (Intel® X710 10GbE LAN controller)</p> <p>1 x RJ45 1GbE IPMI</p>
<b>Networking</b>	VGA	Aspeed AST2600
<b>Front I/O ports</b>		1 x USB 3.2 Gen 1 port
<b>Rear I/O ports</b>		<p>2 x USB 3.2 Gen 1 ports</p> <p>1 x VGA port</p> <p>1 x COM port</p> <p>2 x RJ45 10G LAN ports</p> <p>1 x RJ45 1G Mgmt LAN ports</p>
<b>Switch/LED</b>		<p><b>Front:</b></p> <ul style="list-style-type: none"> <li>1 x Power switch/LED</li> <li>1 x Location switch/LED</li> <li>1 x Storage device access LED</li> <li>1 x Message LED</li> <li>2 x LAN LED</li> </ul>

(continued on the next page)

## System specifications

Model Name		ESC N4A-E11
Switch/LED		<b>Rear:</b> 1 x Power switch/LED 1 x Location switch LED 1 x Q-code/Port 80 LED
OS Support		Windows® Server 2019 RedHat® SuSE® Ubuntu Vmware * Please find the latest OS support from <a href="https://www.asus.com/event/Server/OS_support_list/OS.html">https://www.asus.com/event/Server/OS_support_list/OS.html</a>
Management Solution	Out of Band Remote Hardware Software	ASMB10-iKVM (on-board)  ASUS Control Center
Dimension		823mm x 439.5mm x 130.6mm (3U) 31.50" x 17.22" x 3.46"
Net Weight Kg (CPU, DRAM & HDD not included)		34 kg
Gross Weight Kg (CPU, DRAM & HDD not included, Packing include)		44 kg
Power Supply (following different configuration by region)		1+1 Redundant 3000W 80 PLUS Titanium Power Supply
Environment		Operation temperature: 10° ~ 35° Non operation temperature: -40° ~ 70° Non operation humidity: 20% ~ 90% ( Non condensing)



Always use PSUs with the same watt and power rating. Combining PSUs with different wattage (e.g. 1 x 1600 W + 1 x 2200 W) may yield unstable results and potential damage to your system.



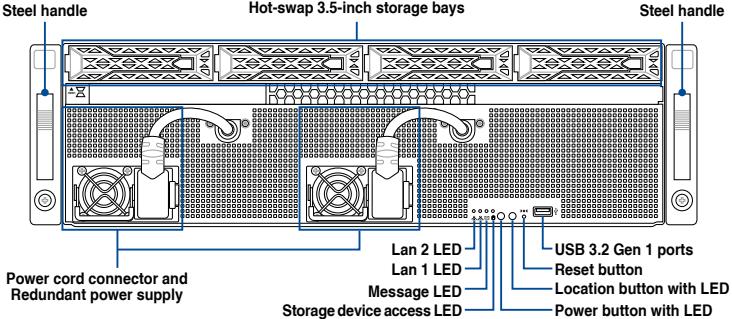
Specifications are subject to change without notice.

## 1.4 Front panel features

The server system features a simple yet stylish front panel. The power and location buttons, LED indicators, and USB port are located on the front panel.



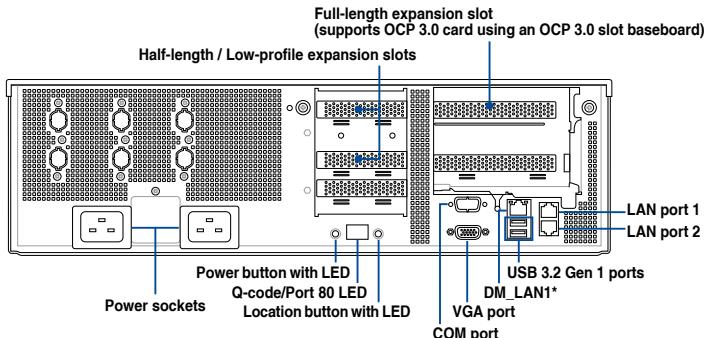
Refer to the 1.7.1 Front panel LEDs section for the LED descriptions.



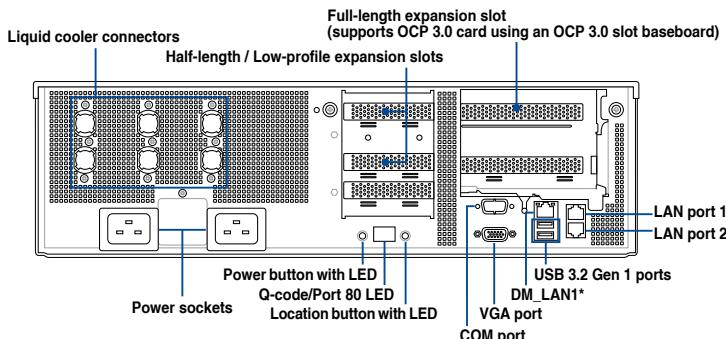
## 1.5 Rear panel features

The expansion slots, system power socket, liquid cooler connectors (on selected models) are located on the rear panel of the server. The right part includes the I/O shield with openings for the rear panel connectors on the motherboard.

### Air cooling solution



### Liquid cooling solution

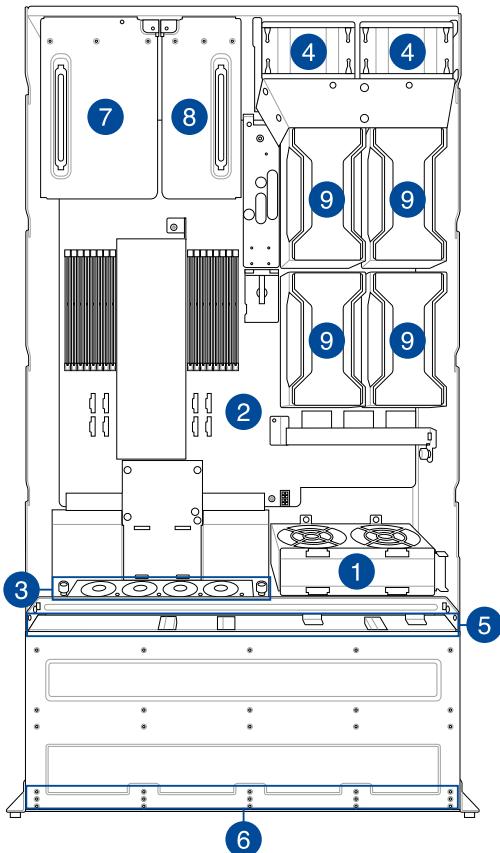


- The rear I/O ports do not appear on the rear panel if motherboard is not present.
- \*The DM\_LAN1 port is for ASUS ASMB10-iKVM controller only.

## 1.6 Internal features

The server system includes the basic components which may differ between different models, as shown below:

### Air cooling solution



1. Front GPU fans
2. ASUS KMPN-U16 server board
3. System fans
4. Rear GPU fans
5. SATA/SAS/NVMe backplane
6. 4 x 3.5" storage device bays
7. PCIe riser card (1 x Gen4 x16 link, supports OCP 3.0 card using a OCP 3.0 slot baseboard)
8. PCIe riser card (2 x Gen4 x16 link)
9. GPU with air cooling modules



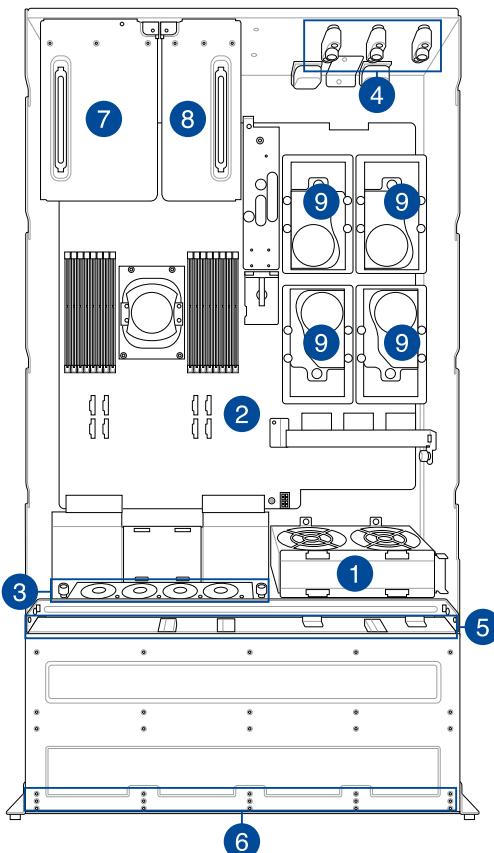
A protection film is pre-attached to the front cover before shipping. Please remove the protection film before turning on the system for proper heat dissipation.

### WARNING

HAZARDOUS MOVING PARTS

KEEP FINGERS AND OTHER BODY PARTS AWAY

## Liquid cooling solution



1. Front GPU fans
2. ASUS KMPN-U16 server board
3. System fans
4. Liquid cooler connectors
5. SATA/SAS/NVMe backplane
6. 4 x 3.5" storage device bays
7. PCIe riser card (1 x Gen4 x16 link, supports OCP 3.0 card using a OCP 3.0 slot baseboard)
8. PCIe riser card (2 x Gen4 x16 link)
9. GPU with water cooling modules



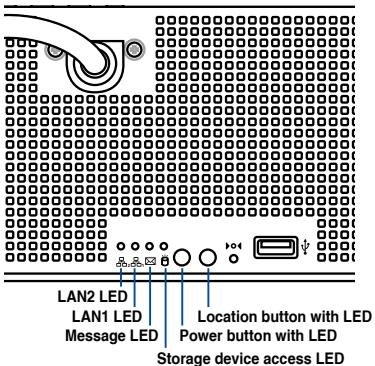
A protection film is pre-attached to the front cover before shipping. Please remove the protection film before turning on the system for proper heat dissipation.

### **WARNING**

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

## 1.7 LED information

### 1.7.1 Front panel LEDs

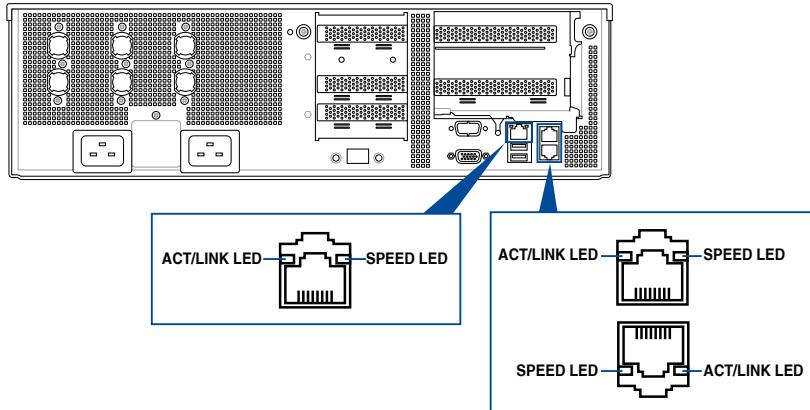


LED	Icon	Display status	Description
Power button with LED		ON	System power on
Storage device access LED		OFF	No activity
		Blinking	Data activity
Message LED		OFF	System is normal; no incoming event
		ON	A hardware monitor event is indicated
Location button with LED		OFF	Function off
		ON	Location switch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

## 1.7.2 LAN (RJ-45) LEDs



The illustration for the system is for reference only, the LAN ports are the same for all models.



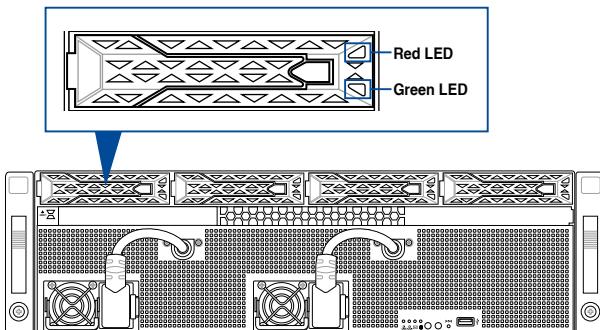
### LAN1/LAN2 LEDs

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

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

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

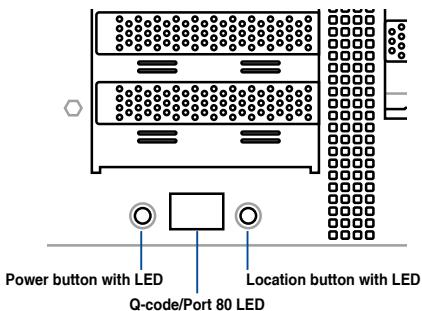
## 1.7.3 Storage device status LEDs



**SATA/SAS HDD LED Description**

GREEN	ON	SATA/SAS/NVMe storage device power ON
RED	ON	Storage device has failed and should be swapped immediately (for HBA/RAID card)
GREEN/RED	Blinking	RAID rebuilding (for HBA/RAID card)
GREEN/RED	Blinking	Locate (for HBA/RAID card)
GREEN/RED	OFF	Storage device not found
GREEN	Blinking	Read/write data from/into the SATA/SAS/NVMe HDD

## 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)

## 1.7.4 Q-Code/Port 80 status LEDs

The Q-Code LED provides a 2-digit display that shows the status of your system.

ACTION	PHASE	POST CODE	TYPE	DESCRIPTION
SEC Start up	Security Phase	0x01	Progress	First post code
		0x02	Progress	Load BSP microcode
		0x03	Progress	Perform early platform Initialization
		0x04	Progress	Set cache as ram for PEI phase
		0x05	Progress	Establish Stack
		0x06	Progress	CPU Early Initialization
PSP Boot	PSP Boot Loader phase (Error Post Codes)	0x00	error	General - Success
		0x01	error	Generic Error Code
		0x02	error	Generic Memory Error
		0x03	error	Buffer Overflow
		0x04	error	Invalid Parameter(s)
		0x05	error	Invalid Data Length
		0x06	error	Data Alignment Error
		0x07	error	Null Pointer Error
		0x08	error	Unsupported Function
		0x09	error	Invalid Service ID
		0x0A	error	Invalid Address
		0x0B	error	Out of Resource Error
		0x0C	error	Timeout
		0x0D	error	data abort exception
		0x0E	error	prefetch abort exception
		0x0F	error	Out of Boundary Condition Reached
		0x10	error	Data corruption
		0x11	error	Invalid command
		0x12	error	The package type provided by BR is incorrect
		0x13	error	Failed to retrieve FW header during FW validation
		0x14	error	Key size not supported
		0x15	error	Agesa0 verification error
		0x16	error	SMU FW verification error
		0x17	error	OEM SINGING KEY verification error
		0x18	error	Generic FW Validation error
		0x19	error	RSA operation fail - bootloader
		0x1A	error	CCP Passthrough operation failed - internal status
		0x1B	error	AES operation fail
		0x1C	error	CCP state save failed
		0x1D	error	CCP state restore failed
		0x1E	error	SHA256/384 operation fail - internal status
		0x1F	error	ZLib Decompression operation fail
		0x20	error	HMAC-SHA256/384 operation fail - internal status
		0x21	error	Booted from boot source not recognized by PSP
		0x22	error	PSP directory entry not found
		0x23	error	PSP failed to set the write enable latch
		0x24	error	PSP timed out because spiron took too long
		0x25	error	Cannot find BIOS directory
		0x26	error	SpiRom is not valid
		0x27	error	slave die has different security state from master
		0x28	error	SMI interface init failure
		0x29	error	SMI interface generic error
		0x2A	error	invalid die ID executes MCM related function
		0x2B	error	invalid MCM configuration table read from bootrom
		0x2C	error	Valid boot mode wasn't detected
		0x2D	error	NVStorage init failure
		0x2E	error	NVStorage generic error
		0x2F	error	MCM 'error' to indicate slave has more data to send
		0x30	error	MCM error if data size exceeds 32B
		0x31	error	Invalid client id for SVC MCM call
		0x32	error	MCM slave status register contains bad bits

(continued on the next page)

ACTION	PHASE	POST CODE	TYPE	DESCRIPTION
PSP Boot	PSP Boot Loader phase (Error Post Codes)	0x33	error	MCM call was made in a single die environment
		0x34	error	PSP secure mapped to invalid segment (should be 0x400_0000)
		0x35	error	No physical x86 cores were found on die
		0x36	error	Insufficient space for secure OS (range of free SRAM to SVC stack base)
		0x37	error	SYSHUB mapping memory target type is not supported
		0x38	error	Attempt to unmap permanently mapped TLB to PSP secure region
		0x39	error	Unable to map an SMN address to AXI space
		0x3A	error	Unable to map a SYSHUB address to AXI space
		0x3B	error	The count of CCXs or cores provided by bootrom is not consistent
		0x3C	error	Uncompressed image size doesn't match value in compressed header
		0x3D	error	Compressed option used in case where not supported
		0x3E	error	Fuse info on all dies don't match
		0x3F	error	PSP sent message to SMU; SMU reported an error
		0x40	error	Function RunPostX86ReleaseUnitTests failed in memcmp()
		0x41	error	Interface between PSP to SMU not available.
		0x42	error	Timer wait parameter too large
		0x43	error	Test harness module reported an error
		0x44	error	x86 wrote C2PMMSG_0 interrupting PSP, but the command has an invalid format
		0x45	error	Failed to read from SPI the Bios Directory or Bios Combo Directory
		0x46	error	Mini-BL, validation of the PSP SRAM image failed on HMAC compare
		0x47	error	Failed to read the combo bios header
		0x48	error	Potential stack corruption in jump to Mini BL
		0x49	error	Error in Validate and Loading AGESA APOB SVC call
		0x4A	error	Correct fuse bits for DIAG_BL loading not set
		0x4B	error	The UmcProgramKeys() function was not called by AGESA
		0x4C	error	Unconditional Unlock based on serial numbers failure
		0x4D	error	Syshub register programming mismatch during readback
		0x4E	error	Family ID in MP0_SFUSE_SEC[7:3] not correct
		0x4F	error	An operation was invoked that can only be performed by the GM
		0x50	error	Failed to acquire host controller semaphore to claim ownership of SMB
		0x51	error	Timed out waiting for host to complete pending transactions
		0x52	error	Timed out waiting for slave to complete pending transactions
		0x53	error	Unable to kill current transaction on host, to force idle
		0x54	error	One of: illegal command, Unclaimed cycle, or Host time out
		0x55	error	An smbus transaction collision detected, operation restarted
		0x56	error	Transaction failed to be started or processed by host, or not completed
		0x57	error	An unsolicited smbus interrupt was received
		0x58	error	An attempt to send an unsupported PSP-SMU message was made
		0x59	error	An error/data corruption detected on response from SMU for sent msg
		0x5A	error	MCM Steady-state unit test failed
		0x5B	error	S3 Enter failed
		0x5C	error	AGESA BL did not set PSP SMU reserved addresses via SVC call
		0x5E	error	CcxSecBisEn not set in fuse RAM
		0x5F	error	Received an unexpected result
		0x60	error	VMG Storage Init failed
		0x61	error	failure in mbedtls user app
		0x62	error	An error occurred whilst attempting to SMN map a fuse register
		0x63	error	Fuse burn sequence/operation failed due to internal SOC error
		0x64	error	Fuse sense operation timed out
		0x65	error	Fuse burn sequence/operation timed out waiting for burn done
		0x66	error	The PMU FW Public key certificate loading or authentication fails
		0x67	error	This PSP FW was revoked
		0x68	error	The platform model/vendor id fuse is not matching the BIOS public key token
		0x69	error	The BIOS OEM public key of the BIOS was revoked for this platform
		0x6A	error	PSP level 2 directory not match expected value.
		0x6B	error	BIOS level 2 directory not match expected value.
		0x6C	error	Reset image not found
		0x6D	error	Generic error indicating the CCP HAL initialization failed
		0x6E	error	failure to copy NVRAM to DRAM.
		0x6F	error	Invalid key usage flag

(continued on the next page)

Action	Phase	Post Code	Type	Description
PSP Boot	PSP Boot Loader phase (Error Post Codes)	0x71	error	RSMU signaled a security violation
		0x72	error	Error programming the WAFL PCS registers
		0x73	error	Error setting waf1 PCS threshold value
		0x74	error	Error loading OEM trustlets
		0x75	error	Recovery mode across all dies is not sync'd
		0x76	error	Uncorrectable WAFL error detected
		0x77	error	Fatal MP1 error detected
		0x78	error	Bootloader failed to find OEM signature
		0x79	error	Error copying BIOS to DRAM
		0x7A	error	Error validating BIOS image signature
		0x7B	error	
		0x7C	error	Platform Vendor ID and/or Model ID binding violation
		0x7D	error	Bootloader detects BIOS request boot from SPI-ROM, which is unsupported for PSB.
		0x7E	error	Requested fuse is already blown, reblow will cause ASIC malfunction
		0x7F	error	Error with actual fusing operation
		0x80	error	(Local Master PSP on P1 socket) Error reading fuse info
		0x81	error	(Local Master PSP on P1 socket) Platform Vendor ID and/or Model ID binding violation
		0x82	error	(Local Master PSP on P1 socket) Requested fuse is already blown, reblow will cause ASIC malfunction
		0x83	error	(Local Master PSP on P1 socket) Error with actual fusing operation
		0x84	error	SEV FW Rollback attempt is detected
		0x85	error	/ SEV download FW command fail to broadcast and clear the lslnSRAM field on slave dies
		0x86	error	Agesa error injection failure
		0x87	error	Uncorrectable TWIX error detected
		0x88	error	Error programming the TWIX PCS registers
		0x89	error	Error setting TWIX PCS threshold value
		0x8A	error	SW CCP queue is full, cannot add more entries
		0x8B	error	CCP command description syntax error detected from input
		0x8C	error	Return value stating that the command has not yet be scheduled
		0x8D	error	The command is scheduled and being worked on
		0x8E	error	The DIXO PHY SRAM Public key certificate loading or authentication fails
		0x8F	error	ITPM binary size exceeds limit allocated in Private DRAM, need to increase the limit
		0x90	error	The TWIX link for a particular CCD is not trained Fatal error
		0x91	error	Security check failed (not all dies are in same security state)
		0x92	error	FW type mismatch between the requested FW type and the FW type embedded in the FW binary header
		0x93	error	SVC call input parameter address violation
		0x94	error	Knoll failed to idle correctly after being reset
		0x95	error	Bad status returned by I2CKnollCheck
		0x96	error	NACK to general call (no device on Knoll I2C bus)
		0x97	error	Null pointer passed to I2CKnollCheck
		0x98	error	Invalid device-ID found during Knoll authentication
		0x99	error	Error during Knoll/Prom key derivation
		0x9A	error	Null pointer passed to Crypto function
		0x9B	error	Error in checksum from wrapped Knoll/Prom keys
		0x9C	error	Knoll returned an invalid response to a command
		0x9D	error	Bootloader failed in Knoll Send Command function
		0x9E	error	No Knoll device found by verifying MAC
		0x9F	error	The maximum allowable error post code
Quick VGA	PEI(Pre-EFI Initialization) phase	0x10	Progress	PEI Core Entry
		0x11	Progress	PEI cache as ram CPU initial
		0x15	Progress	NB Initialization before installed memory
		0x19	Progress	SB Initialization before installed memory
	DXE(Driver Execution Environment) phase	0x32	Progress	CPU POST-Memory Initialization
		0x33	Progress	CPU Cache Initialization
		0x34	Progress	Application Processor(s) (AP) Initialization
		0x35	Progress	BSP Selection
		0x36	Progress	CPU Initialization
		0x37	Progress	Pre-memory NB Initialization
		0x3B	Progress	Pre-memory SB Initialization

(continued on the next page)

ACTION	PHASE	POST CODE	TYPE	DESCRIPTION
Quick VGA	DXE(Driver Execution Environment) phase	0x4F	Progress	DXE Initial Program Load(IPL)
		0x60	Progress	DXE Core Started
		0x61	Progress	DXE NVRAM Initialization
		0x62	Progress	SB run-time Initialization
		0x63	Progress	CPU DXE Initialization
		0x68	Progress	PCI HB Initialization
		0x69	Progress	NB DXE Initialization
		0x6A	Progress	NB DXE SMM Initialization
		0x70	Progress	SB DXE Initialization
		0x71	Progress	SB DXE SMM Initialization
		0x72	Progress	SB DEVICES Initialization
		0x78	Progress	ACPI Module Initialization
		0x79	Progress	CSM Initialization
		0xD0	Progress	CPU PM Structure Initialization
Normal boot	BDS(Boot Device Selection) phase	0x90	Progress	BDS started
		0x91	Progress	Connect device event
		0x92	Progress	PCI Bus Enumeration
		0x93	Progress	PCI Bus Enumeration
		0x94	Progress	PCI Bus Enumeration
		0x95	Progress	PCI Bus Enumeration
		0x96	Progress	PCI Bus Enumeration
		0x97	Progress	Console outout connect event
		0x98	Progress	Console input connect event
		0x99	Progress	AMI Super IO start
		0x9A	Progress	AMI USB Driver Initialization
		0x9B	Progress	AMI USB Driver Initialization
		0x9C	Progress	AMI USB Driver Initialization
		0x9D	Progress	AMI USB Driver Initialization
		0xb2	Progress	Legacy Option ROM Initialization
		0xb3	Progress	Reset system
		0xb4	Progress	USB hotplug
		0xb6	Progress	NVRAM clean up
		0xb7	Progress	NVRAM configuration reset
		0xA0	Progress	IDE, AHCI Initialization
		0xA1	Progress	IDE, AHCI Initialization
		0xA2	Progress	IDE, AHCI Initialization
		0xA3	Progress	IDE, AHCI Initialization
		0x00-0xFF	Progress	Wait BMC ready
		0xA8	Progress	BIOS Setup Utility password verify
		0xA9	Progress	BIOS Setup Utility start
		0xAB	Progress	BIOS Setup Utility input wait
		0xAD	Progress	Ready to boot event
		0xAE	Progress	Legacy boot event
Operating system phase	Operating system phase	0xAA	Progress	APIC mode
		0xAC	Progress	PIC mode



# Hardware Setup

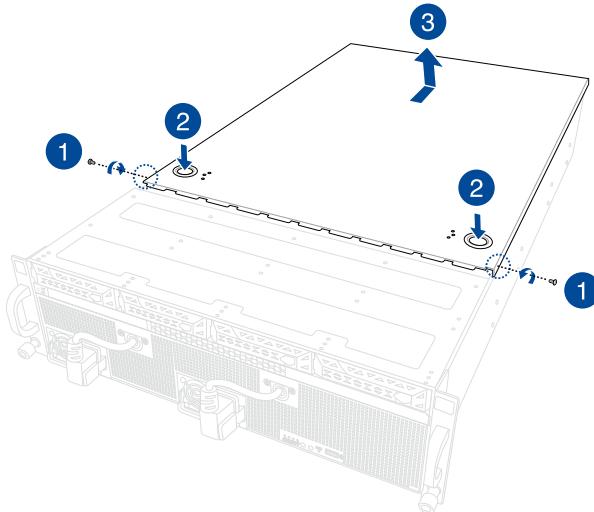
2

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

## 2.1 Chassis cover

### 2.1.1 Removing the rear cover

1. Release the two (2) screws on both sides of the cover with a Phillips screwdriver.
2. Push and hold the cover buttons down, then slide the chassis cover towards the rear to disengage it from the chassis.
3. Lift the chassis cover to completely remove it from the chassis.



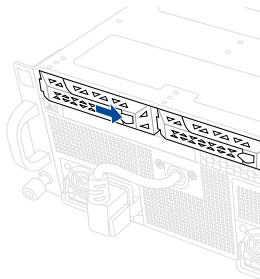
A protection film is pre-attached to the system cover before shipping. Please remove the protection film before turning on the system for proper heat dissipation.

## 2.2 Storage devices

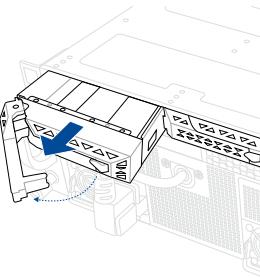
The ASUS ESC N4A-E11 system supports 4 x 3.5-inch or 2.5-inch SATA/SAS/NVMe storage devices.

### 2.2.1 Installing a 3.5-inch storage device

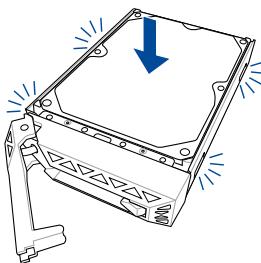
1. Press the spring lock.



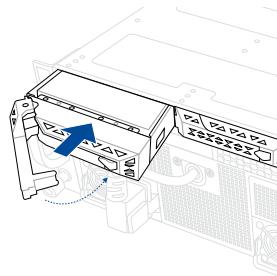
2. Pull the tray lever outwards to remove the drive tray.



3. Prepare the 3.5-inch storage device then place the 3.5" storage device into the tray until it clicks into place.



4. Push the drive 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 drive tray in place.



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

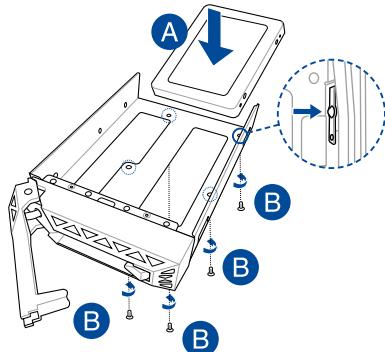
5. Repeat steps 1 to 4 to install the other 3.5-inch storage devices.

## 2.2.2 Installing a 2.5-inch storage device

1. Please follow steps 1 and 2 of the **Installing a 3.5-inch storage device** section to remove the drive tray.
2. Place the 2.5-inch storage device into the tray (A) then secure it with four screws (B).



Ensure to take note of the tool-less notch as it may interfere when trying to align the screw holes. Press the storage device down on the notch if you are experiencing issues trying to align the screw holes.



3. Please follow step 4 of the **Installing a 3.5-inch storage device** section to Replace the drive tray.
4. Repeat steps 1 to 3 to install the other 2.5-inch storage devices.

## 2.3 Expansion slots

The onboard PCIe slots on the motherboard come pre-installed with riser cards that support up to three (3) x16 slot (x16 Gen4 link) for installing PCIe expansion cards and supports an OCP 3.0 card using an OCP 3.0 slot baseboard.



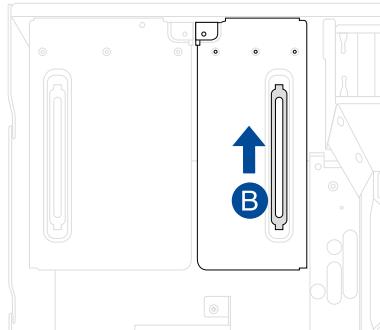
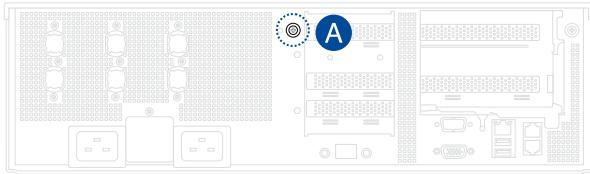
Ensure to unplug the power cord before adding or removing expansion cards. Failure to do so may cause you physical injury and damage motherboard components.



The most bottom PCIe slot on both riser cards are disabled. Please do not install expansion cards to those PCIe slots.

### 2.3.1 Installing an expansion card to the right riser card bracket

1. Loosen the thumbscrew on the rear of the system for the right riser card (A), then pull and lift the riser card bracket out of the system chassis using the plastic tab (B).

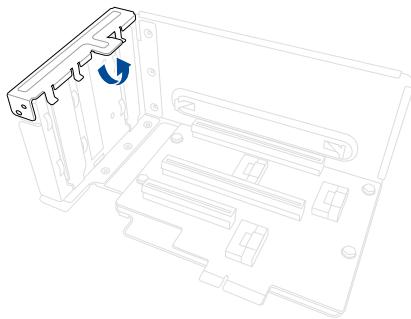


2. Flip the riser card bracket over.



You may disconnect all the cables connected to the riser card if you are having difficulty flipping the riser card bracket over.

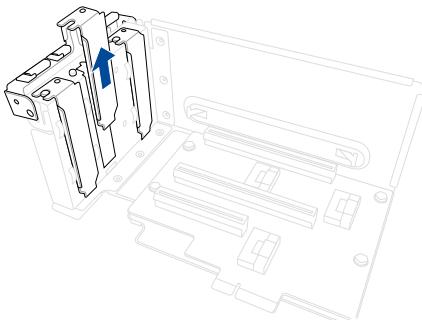
3. Flip the metal bracket lock open.



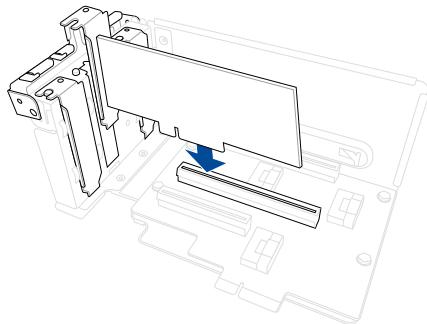
4. Remove the metal bracket for the PCIe slot you wish to install an expansion card to.



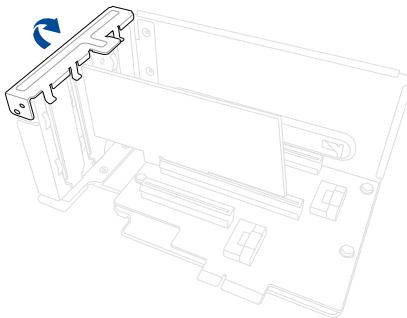
The most bottom PCIe slot is disabled. Please do not install expansion cards to that PCIe slot.



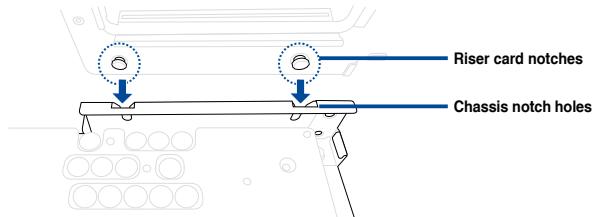
5. Align and insert the golden finger connectors of the expansion cards to the PCIe slot connectors on the riser card as shown.



6. Once your expansion card is installed, flip the metal bracket lock back to secure the expansion card to the PCIe riser card bracket.



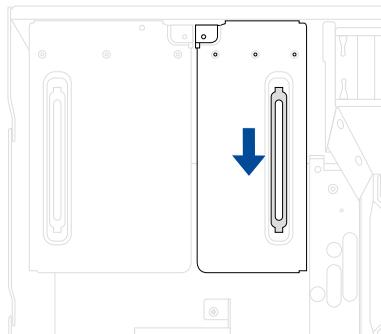
7. Align the notches on the riser card bracket to the notch holes in the system chassis.



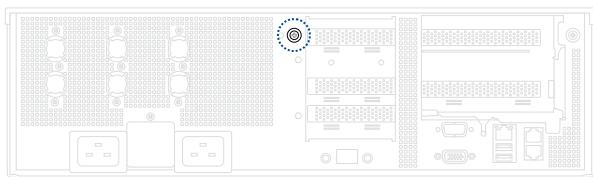
8. Insert the riser card bracket into the PCIe slot on the motherboard.



Reconnect the cables if you removed them earlier.

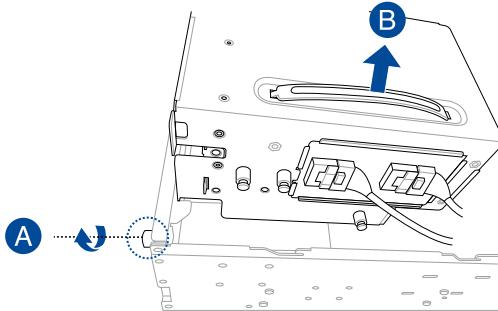


9. Secure the riser card bracket using the thumbscrew on the rear of the system.



### 2.3.2 Installing an expansion card to the left riser card bracket

1. Loosen the thumbscrew on the rear of the system for the left riser card (A), then pull and lift the riser card bracket out of the system chassis using the plastic tab (B).

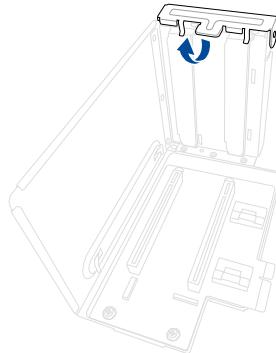


2. Flip the riser card bracket over.



You may disconnect all the cables connected to the riser card if you are having difficulty flipping the riser card bracket over.

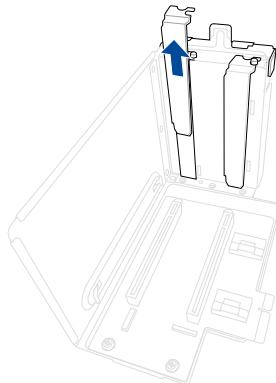
3. Flip the metal bracket lock open.



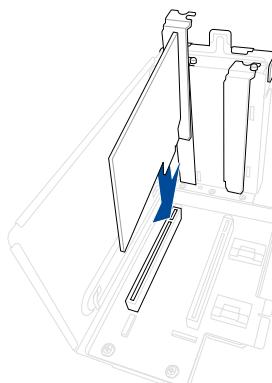
4. Remove the metal bracket for the PCIe slot you wish to install an expansion card to.



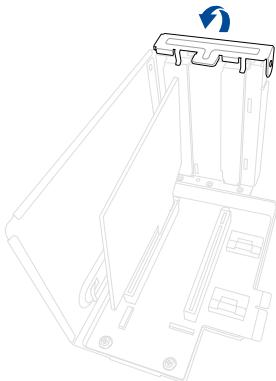
The most bottom PCIe slot is disabled. Please do not install expansion cards to that PCIe slot.



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



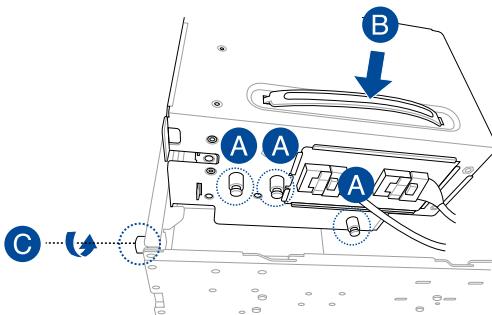
- Once your expansion card is installed, flip the metal bracket lock back to secure the expansion card to the PCIe riser card bracket.



- Align the notches on the riser card bracket to the notch holes in the system chassis (A), then insert the riser card bracket into the PCIe slot on the motherboard (B). Secure the riser card bracket using the thumbscrew on the rear of the system (C).



Reconnect the cables if you removed them earlier.

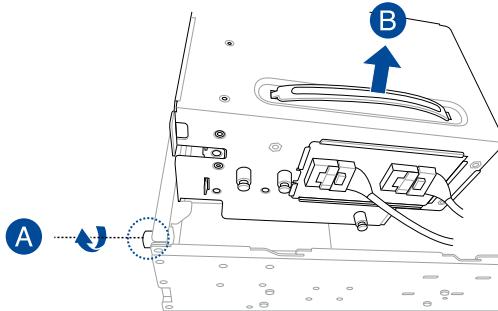


### 2.3.3 Installing an OCP 3.0 slot baseboard and OCP 3.0 card to the PCIe riser card bracket



Install the OCP 3.0 slot baseboard to the **PCIE1** slot on the left PCIe riser card bracket.

1. Loosen the thumbscrew on the rear of the system for the left riser card (A), then pull and lift the riser card bracket out of the system chassis using the plastic tab (B).

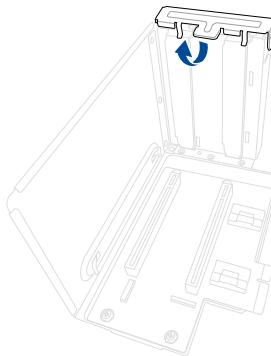


2. Flip the riser card bracket over.

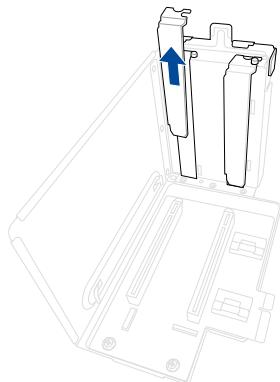


You may disconnect all the cables connected to the riser card if you are having difficulty flipping the riser card bracket over.

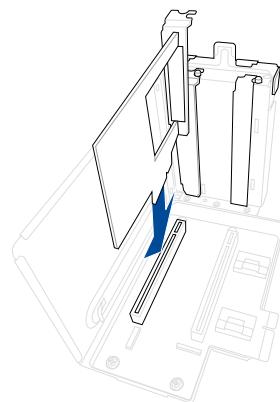
3. Flip the metal bracket lock open.



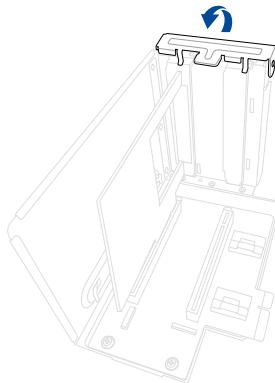
4. Remove the metal bracket for the **PCIE1** slot.



5. Install the OCP 3.0 slot baseboard to the **PCIE1** slot on the PCIe riser card bracket.



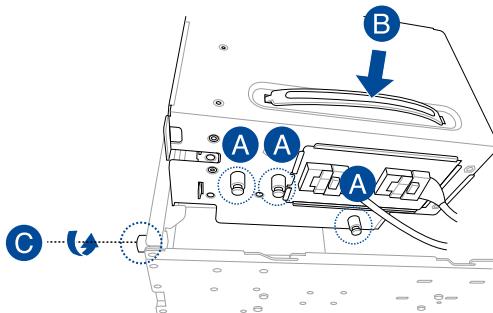
- Once your OCP 3.0 slot baseboard is installed, flip the metal bracket lock back to secure the OCP 3.0 slot baseboard to the PCIe riser card bracket.



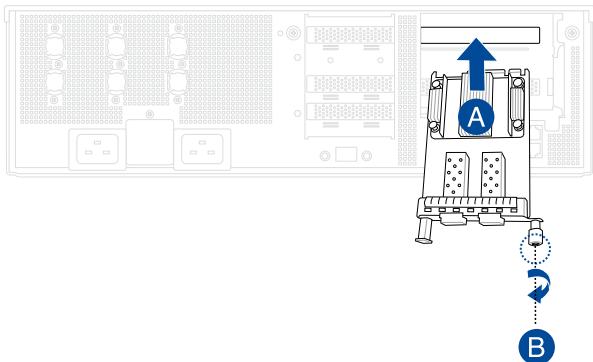
- Align the notches on the riser card bracket to the notch holes in the system chassis (A), then insert the riser card bracket into the PCIe slot on the motherboard (B). Secure the riser card bracket using the thumbscrew on the rear of the system (C).



Reconnect the cables if you removed them earlier.



8. 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).





# 3

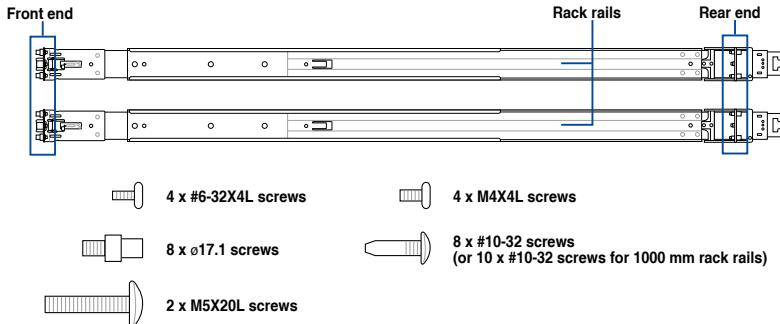
## **Installation Options**

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

### 3.1 Rail Kit

The rail kit package includes:

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



- 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.

### 3.1.1 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

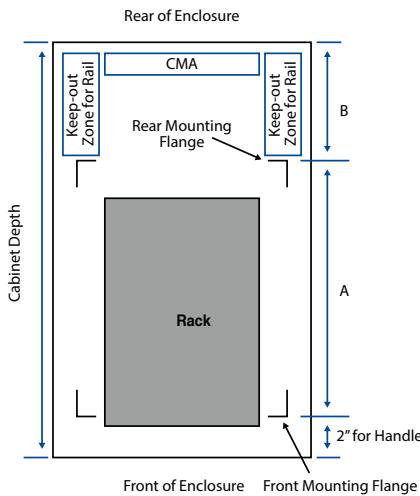
A = 700.3 mm (27.6") ~ 965.5 mm (38")

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.

### 3.1.2 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.

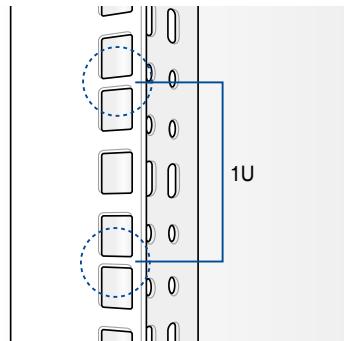
#### Installing the rack rail

To install the rack rails into the rack:

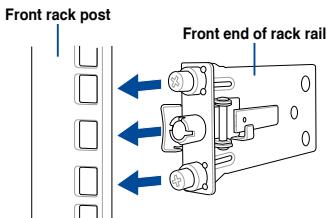
1. Select a desired space on the rack.



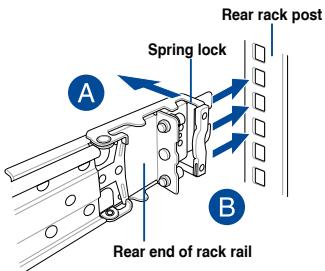
A 1U space consists of three square mounting holes with two thin lips on the top and the bottom.



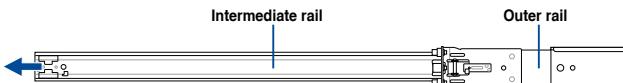
2. Align and insert the front end of the appropriate rack rail (left and right) into the front rack post.



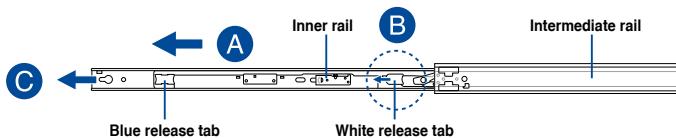
3. Press the spring lock on the rear end of the rack rail and insert the studs into the selected mounting holes on the rear rack post.



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.



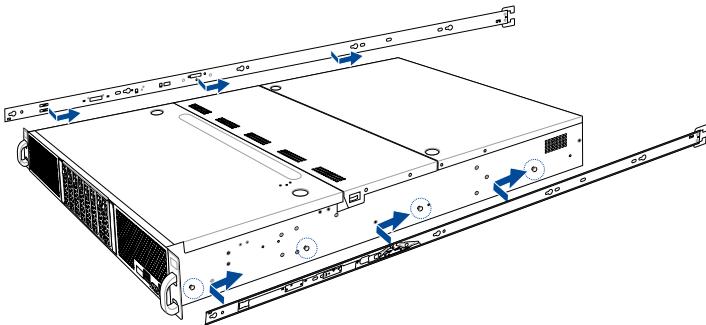
 The blue release tab is available on 1200 mm rack rails. This blue release tab is used to further extend or retract the inner rail.

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

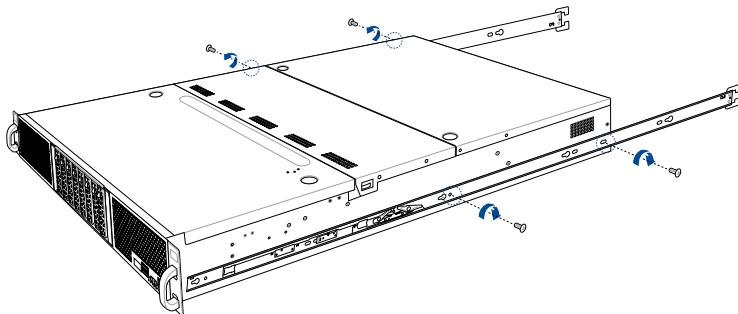


Ensure that the installed rack rails (left and right) are aligned, secured, and stable in place.

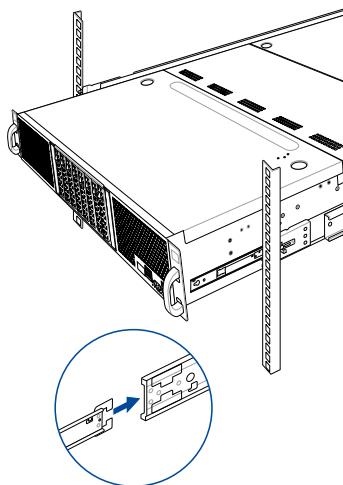
7. Align the inner rails with the studs on both sides of the server system, install the inner rails to the server system, then slide the inner rails toward the rear of the server system until it locks in place.



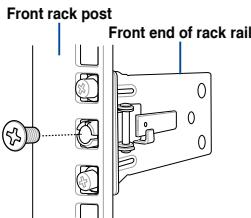
8. Secure the inner rails on both sides of the server system using the #6-32X4L screws.



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

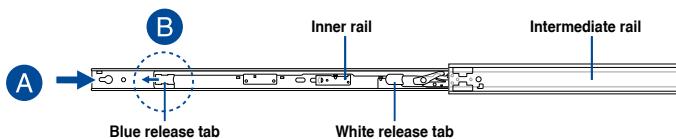


10. (optional) Use the M5X20L screws to secure the rack rails to the rack post.

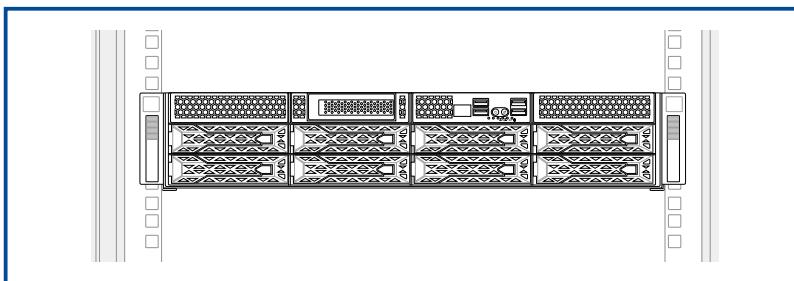


11. Gently push the server system until it is completely installed into the rack rail.

(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.

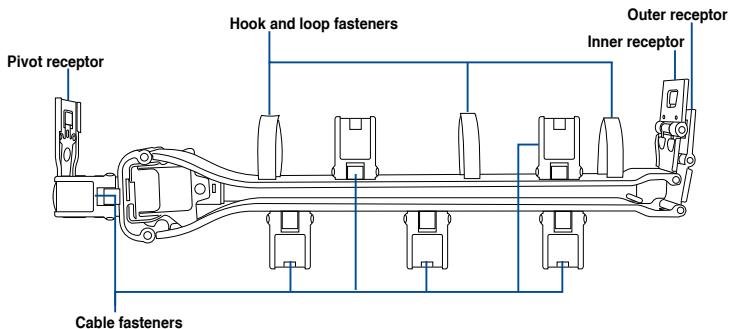


The blue release tab is available on 1200 mm rack rails. This blue release tab is used to further extend or retract the inner rail.



## 3.2 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.



### 3.2.1 Attaching the cable management arm

#### Installing the cable management arm

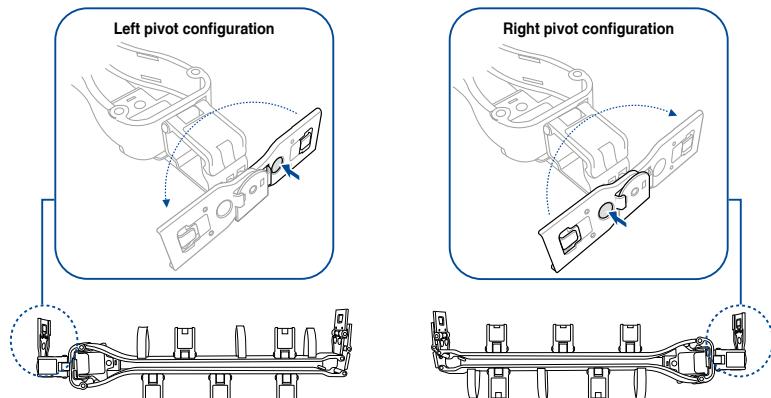
To install the cable management arm:

1. Install the rack rails into the rack.

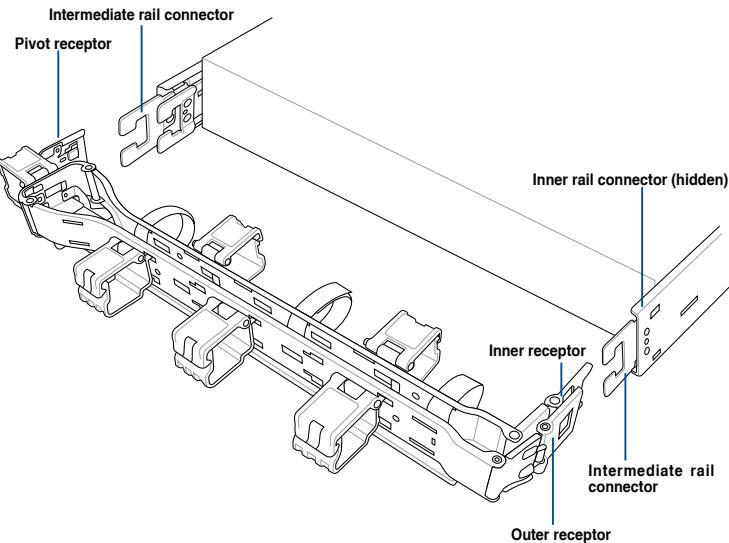


Refer to section 3.1 Rail Kit for the steps on installing the rack rails into the rack.

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.

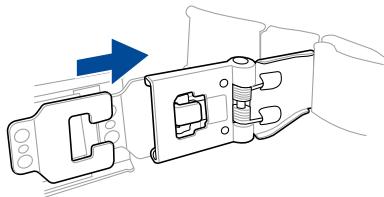


3. Align the three receptors on the CMA with the connectors on the rack rails.

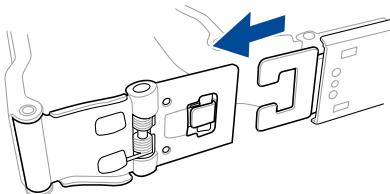


The installation steps in this section uses a **Left pivot configuration** as an example, the installation steps for a **Right pivot configuration** is similar.

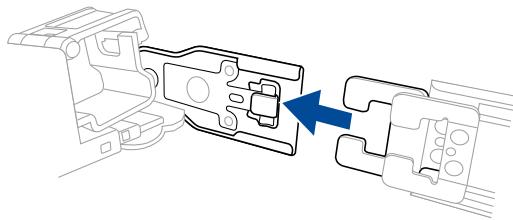
4. Align and connect the inner receptor on the CMA with the connector on the inner rail.



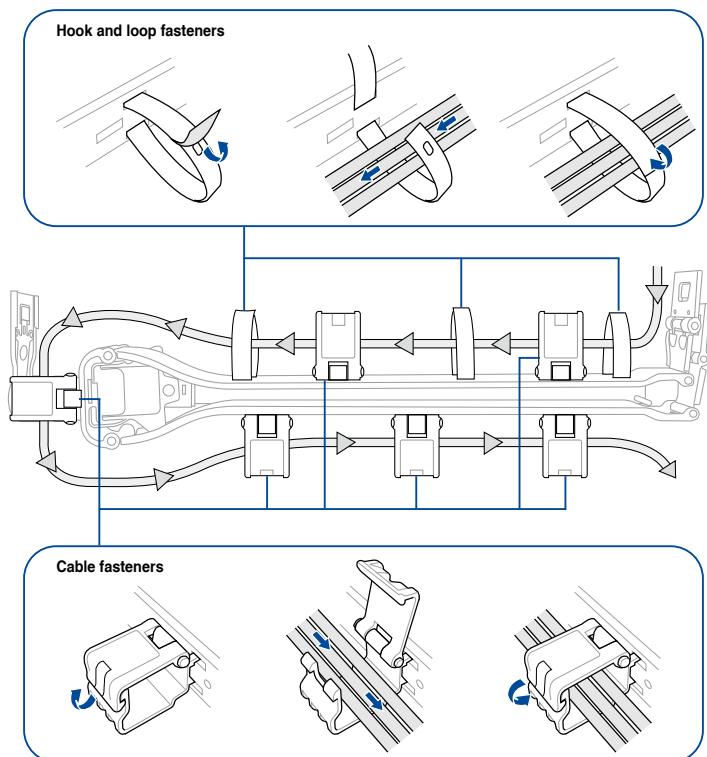
5. Align and connect the outer receptor on the CMA with the connector on the intermediate rail.



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.



# **BIOS Setup**

4

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

## 4.1 Managing and updating your BIOS

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

### 1. ASUS CrashFree BIOS 3

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

### 2. ASUS EzFlash

Updates the BIOS using a USB flash disk.

### 3. BUPDATER

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

Refer to the corresponding sections for details on these utilities.



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

### 4.1.1 ASUS CrashFree BIOS 3 utility

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



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

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

To recover the BIOS from a USB flash drive:

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



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



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

## 4.1.2 ASUS EzFlash Utility

The ASUS EzFlash Utility feature allows you to update the BIOS using a USB flash disk without having to use a DOS-based utility.



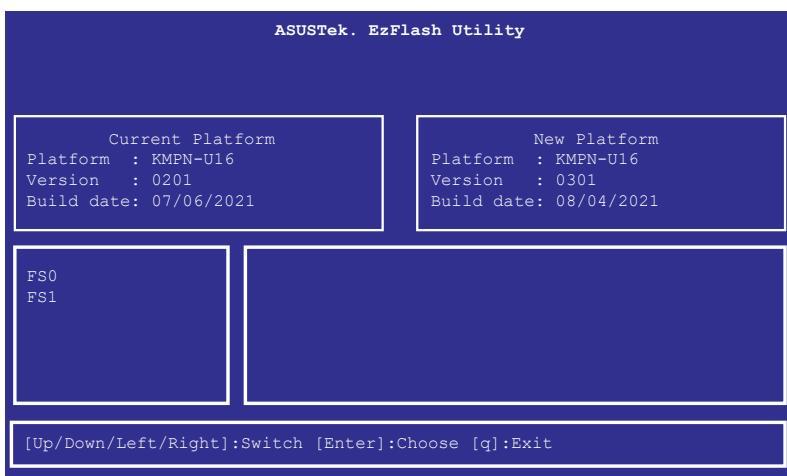
Download the latest BIOS from the ASUS website at [www.asus.com](http://www.asus.com) before using this utility.



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

To update the BIOS using EzFlash Utility:

1. Insert the USB flash disk that contains the latest BIOS file to the USB port.
2. Enter the BIOS setup program. Go to the **Tool** menu to select **Start ASUS EzFlash** and press <Enter> to enable it.



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



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



Ensure to load the BIOS default settings to ensure system compatibility and stability. Press <F2> and select **Yes** to load the BIOS default settings.

### 4.1.3 BUPDATER utility



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

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

#### Updating the BIOS file

To update the BIOS file using the BUPDATER utility:

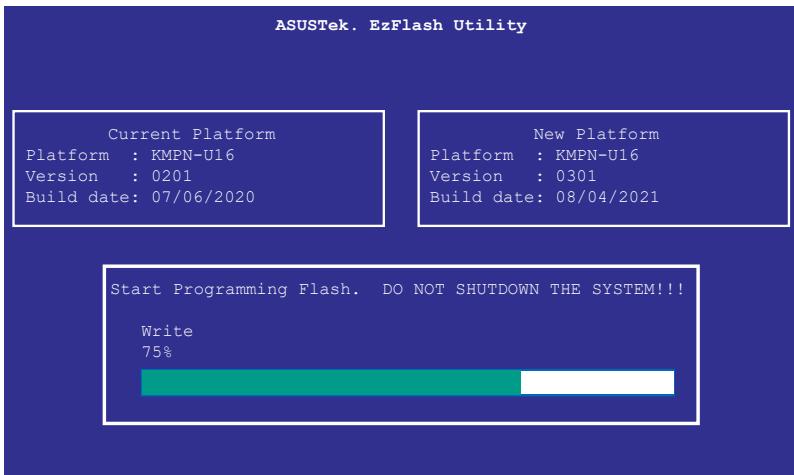
1. Visit the ASUS website at [www.asus.com](http://www.asus.com) and download the latest BIOS file for the motherboard. Save the BIOS file to a bootable USB flash disk drive.
2. Copy the BUPDATER utility (BUPDATER.exe) from the ASUS support website at [www.asus.com/support](http://www.asus.com/support)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

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

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

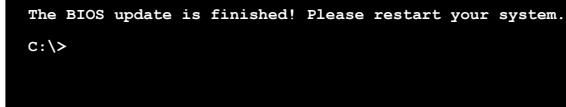
```
A:>BUPDATER /i[file name].CAP
```

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



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

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



## 4.2 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.

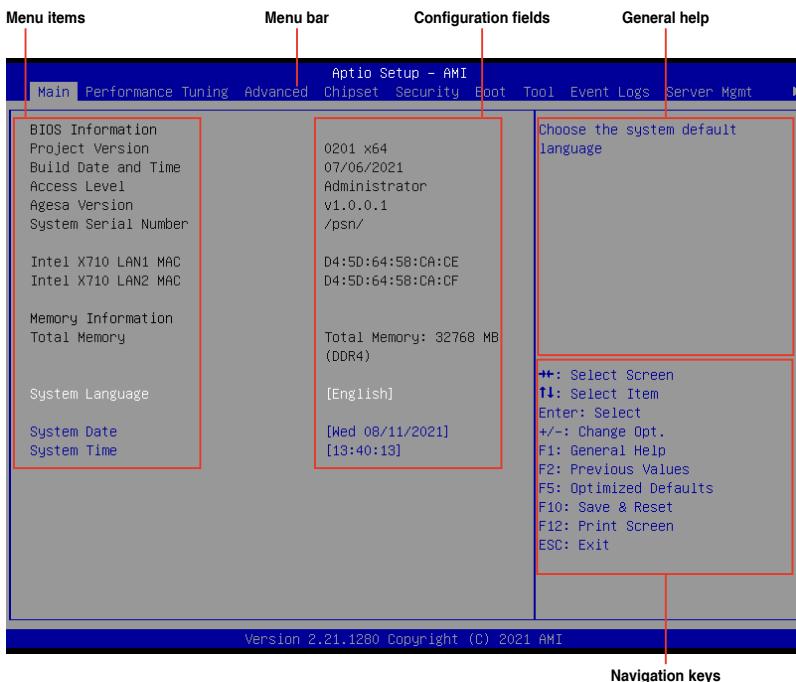
If you wish to enter Setup after POST, restart the system by pressing **<Ctrl>+<Alt>+<Delete>**, or by pressing the reset button on the system chassis. You can also restart by turning the system off and then back on. Do this last option only if the first two failed.

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.

## 4.2.1 BIOS menu screen



## 4.2.2 Menu bar

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

<b>Main</b>	For changing the basic system configuration
<b>Performance Tuning</b>	For changing the performance settings
<b>Advanced</b>	For changing the advanced system settings
<b>Chipset</b>	For changing the chipset settings
<b>Security</b>	For changing the security settings
<b>Boot</b>	For changing the system boot configuration
<b>Tool</b>	For configuring options for special functions
<b>Event Logs</b>	For changing the event log settings
<b>Server Mgmt</b>	For changing the Server Mgmt settings
<b>Exit</b>	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.

## 4.2.3 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.

## 4.2.4 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>.

## 4.2.5 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.

## 4.2.6 General help

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

## 4.2.7 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.

## 4.2.8 Pop-up window

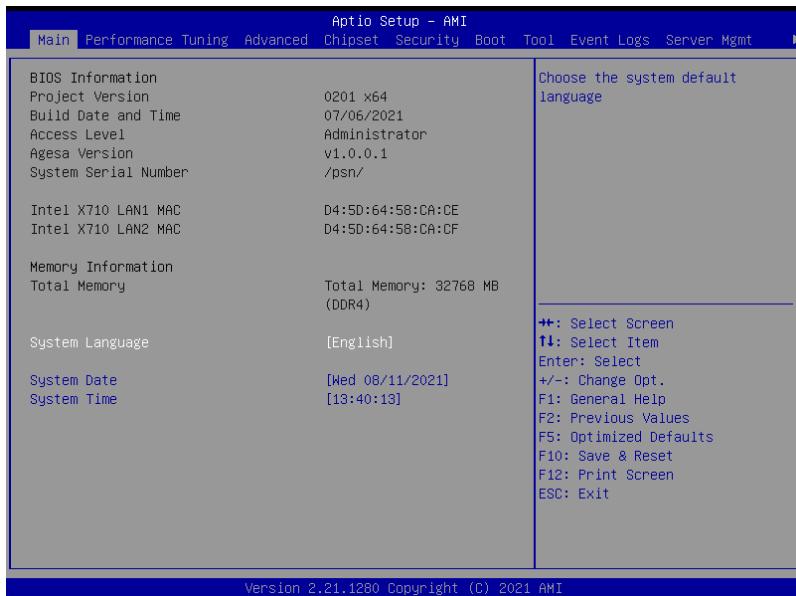
Select a menu item and press <Enter> to display a pop-up window with the configuration options for that item.

## 4.2.9 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.

## 4.3 Main menu

When you enter the BIOS Setup program, the Main menu screen appears. The Main menu provides you an overview of the basic system information, and allows you to set the system date, time, language, and security settings. Scroll using <Page Up> / <Page Down> keys to see more items.



### 4.3.1 System Language [English]

Allows you to select the system default language.

### 4.3.2 System Date [Day xx/xx/yyyy]

Allows you to set the system date.

### 4.3.3 System Time [xx:xx:xx]

Allows you to set the system time.

## 4.4 Performance Tuning menu

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



### Optimized Performance Setting [Default]

Allows you to select performance settings for different scenarios.

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



---

**Core Optimizer and Engine Boost** appear only when you set **Optimized Performance Setting** to [Default] or [By Benchmark].

---

### Core Optimizer [Disabled]

Allows you to keep the processor operating at the turbo highest frequency for the maximum performance. For Windows Server 2019, please set `Powercfg /setacvalueindex scheme_current sub_processor perfautonomous 1 & Powercfg /setactive scheme_current` to enable this feature. For Linux, please set `cpupower frequency-set -g performance`.

Configuration options: [Disabled] [Enabled]



---

Linux support may vary by version of the OS.

---

### Engine Boost [Disabled]

Enable this item to boost the CPU's frequency.

Configuration options: [Disabled] [Enabled]



---

Operate with an ambient temperature of 25°C or lower for optimized performance.

---

### Overclocking [Disabled]

Enable this item to increase the CPU's clock. Please use an external PCIe storage controller for your hard drives when enabling this feature.

Configuration options: [Disabled] [Enabled]



---

Please note that overclocking might cause component damage or system crashes, which may reduce the lifespan of the system and the CPU. Use this tool at your own risk.

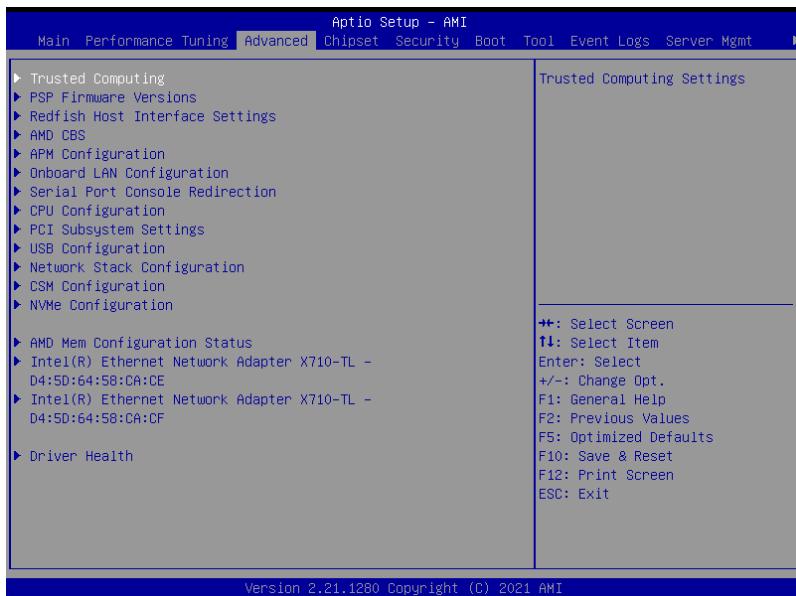
---

## 4.5 Advanced menu

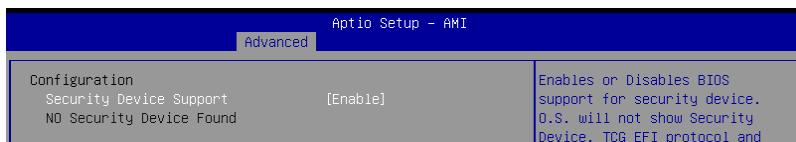
The Advanced menu items allow you to change the settings for the CPU and other system devices.



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



### 4.5.2 Trusted Computing



#### Security Device Support [Enable]

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

## 4.5.2 PSP Firmware Versions

This page displays the PSP firmware versions.

PSP Firmware Versions	
PSP Directory Level 1 (Fixed)	
PSP Recovery BL Ver	FF.13.0.50
SMU FW Version	0.45.63.0
ABL Version	10015012
PSP Directory Level 2 (Updateable)	
PSP BootLoader Version	0.13.0.50
SMU FW Version	0.45.63.0
ABL Version	10015012

## 4.5.3 Redfish Host Interface Settings

Redfish Host Interface Settings	
Redfish	[Disabled]

### Redfish [Disabled]

Allows you to enable or disable Redfish.

Configuration options: [Disabled] [Enabled]

## 4.5.4 AMD CBS

The items in this menu shows the AMD Common BIOS Specifications.



The **AMD CBS** menu will appear in the top menu for AMD EPIC™ 7002 Series processors.

AMD CBS	
▶ CPU Common Options	CPU Common Options
▶ DF Common Options	
▶ UMC Common Options	
▶ NBIO Common Options	
▶ FCH Common Options	
▶ NTB Common Options	
▶ Soc Miscellaneous Control	
▶ Workload Tuning	

## CPU Common Options

### Performance

#### OC Mode [Normal Operation]

Configuration options: [Normal Operation] [Customized]



The following items appear only when **OC Mode** is set to **[Customized]**.

#### Custom Core Pstates

Allows you to enable Core Pstates. Read the disclaimer and select I Accept to continue.



Damage caused by use of your AMD processor outside of specification or in excess of factory settings are not covered by your system manufacturers warranty.



The following items appear only when **[Accept]** is selected for **Custom Core Pstates**.

#### Custom Pstate0 [Auto]

Configuration options: [Auto] [Custom]



The following items appear only when **Custom Pstate0** is set to **[Custom]**.

#### Pstate0 Freq (MHz) [0]

Allows you to specify core frequency (MHz).

#### CCD/Core/Thread Enablement

This option allows you to enable CCD/Core/Thread Enablement.



S3 is not supported on systems where cores/threads have been removed/disabled.

#### CCD Control [Auto]

Sets the number of CCDs to be used. Once this option has been used to remove any CCDs, a POWER CYCLE is required in order for future selections to take effect.

Configuration options: [Auto] [2 CCDs] [3 CCDs] [4 CCDs] [6 CCDs]

#### Core Control [Auto]

Sets the number of cores to be used. Once this option has been used to remove any cores, a POWER CYCLE is required in order for future selections to take effect.

Configuration options: [Auto] [ONE (1 + 0)] [TWO (2 + 0)] [THREE (3 + 0)] [FOUR (4 + 0)] [FIVE (5 + 0)] [SIX (6 + 0)] [SEVEN (7 + 0)]

#### SMT Control [Auto]

Can be used to disable symmetric multithreading. To re-enable SMT, a POWER CYCLE is needed after selecting the [Enable] option. Select [Auto] based on BIOS PCD (PcdAmdSmtMode) defatul setting.

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



S3 is not supported on systems where cores/threads have been removed/disabled.

## Prefetcher settings

### L1 Stream HW Prefetcher [Auto]

Allows you to enable or disable L1 Stream HW Prefetcher.

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

### L1 Stride Prefetcher [Auto]

Uses memory access history of individual instructions to fetch additional lines when each access is a constant distance from the previous.

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

### L1 Region Prefetcher [Auto]

Uses memory access history to fetch additional lines when the data access for a given instruction tends to be followed by other data accesses.

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

### L2 Stream HW Prefetcher [Auto]

Allows you to enable or disable L2 Stream HW Prefetcher.

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

### L2 Up/Down Prefetcher [Auto]

Uses memory access history to determine whether to fetch the next or previous line for all memory access.

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

## Core Watchdog

### Core Watchdog Timer Enable [Auto]

Allows you to enable or disable CPU Watchdog Timer.

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



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

### Core Watchdog Timer Interval [Auto]

Configuration options: [21.461s] [10.730s] [5.364s] [2.681s] [1.340s] [669.41ms] [334.05ms] [166.37ms] [82.53ms] [40.61ms] [20.970ms] [10.484ms] [5.241ms] [2.620ms] [1.309ms] [654.08us] [326.4us] [162.56us] [80.64us] [39.68us] [Auto]

### Core Watchdog Timer Severity [Auto]

Allows you to specify the CPU watch dog timer severity.

Configuration options: [No Error] [Transparent] [Corrected] [Deferred] [Uncorrected] [Fatal] [Auto]

### RedirectForReturnDis [Auto]

This option is from a workaround for GCC/C000005 issue for XV Core on CZ A0, setting MSRC001\_1029 Decode Configuration (DE\_CFG) bit 14 [DecfgNoRdrctForReturns] to 1.

Configuration options: [Auto] [1] [0]

### **Platform First Error Handling [Auto]**

Allows you to enable or disable PFEH, cloak individual banks, and mask deferred error interrupts from each bank.

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

### **Core Performance Boost [Auto]**

Allows you to enable or disable CPB.

Configuration options: [Disabled] [Auto]

### **Global C-state Control [Auto]**

Allows you to control IO based C-state generation and DF C-states.

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

### **Power Supply Idle Control [Auto]**

Configuration options: [Low Current Idle] [Typical Current Idle] [Auto]

### **SEV ASID Count [Auto]**

This field specifies the maximum valid ASID, which affects the maximum system physical address space. 16TB of physical address space is available for systems that support 253 ASIDs, while 8TB of physical address space is available for systems that support 509 ASIDs.

Configuration options: [253 ASIDs] [509 ASIDs] [Auto]

### **SEV-ES ASID Space Limit Control [Auto]**

Configuration options: [Auto] [Manual]



The following item appears only when **SEV-ES ASID Space Limit Control** is set to **[Manual]**.

---

### **SEV-ES ASID Space Limit [Auto]**

SEV Vms using ASIDs below the SEV-ES ASID Space Limit must enable the SEV-ES feature. ASIDs from SEV-ES ASID Space Limit to (SEV ASID Count + 1) can only be used with SEV VMs. If this field is set to (SEV ASID Count + 1), all ASIDs are forced to be SEV-ES ASIDs. Hence, the valid values for this field is 1 - (SEV ASID Count + 1). Configuration options: [1] - [520]

### **Streaming Stores Control [Auto]**

Allows you to enable or disable the streaming stores functionality.

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

### **Local APIC Mode [Auto]**

Configuration options: [Compatibility] [XAPIC] [X2APIC] [Auto]

### **ACPI \_CST C1 Operation [Auto]**

Determines whether or not to declare the C1 state to the OS.

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

### **MCA error thresh enable [Auto]**

Allows you to enable or disable MCA error thresholding.

Configuration options: [False] [True] [Auto]



---

The following item appears only when **MCA error thresh enable** is set to **[True]**.

---

#### **MCA error thresh count [FF5]**

Allows you to set the effective error threshold count = 4095(0xFFFF) - <this value> (e.g. the default value of 0xFF5 results in a threshold of 10).

#### **SMU and PSP Debug Mode [Auto]**

When this option is set to [Enabled], specific uncorrected errors detected by the PSP FW or SMU FW will hang and not reset the system.

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

#### **Xtrig7 Workaround [Auto]**

This workaround is only applicable for Rev A.

[Auto]	The bronze workaround is applied.
[No Workaround]	Applied for Rev B, and changing the selection for this option will not result in any changes.
[Bronze Workaround]	DbReq and PDM function as expected, breakpoint redirect capability compromised.
[Silver Workaround]	DbReq, PDM, and breakpoint redirect function as expected, SCAN capability compromised.

#### **PPIN Opt-in [Auto]**

Allows you to enable or disable the PPIN feature.

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

#### **SNP Memory (RMP Table) Coverage [Auto]**

Setting this option to [Enabled] will cover the entire system's memory.

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

---



The following item appears only when **SNP Memory (RMP Table) Coverage** is set to **[Custom]**.

---

#### **Amount of Memory to Cover [0]**

Allows you to specify MB of System Memory to be covered in Hex.

#### **SMEE [Auto]**

Allows you to enable or disable secure memory encryption control.

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

#### **Action on BIST Failure [Auto]**

Allows you to set action to take when a CCD BIST failure is detected.

Configuration options: [Do Nothing] [Down-CCD] [Auto]

#### **Fast Short REP MOVSB [Enabled]**

Default set to 1, can be set to zero for analysis purposes as long as OS supports it.

Configuration options: [Disabled] [Enabled]

#### **Enhanced REP MOVSB/STOSB [Enabled]**

Default set to 1, can be set to zero for analysis purposes as long as OS supports it.

Configuration options: [Disabled] [Enabled]

### **REP-MOV/STOS Streaming [Enabled]**

Allows REP-MOVS/STOS to use non-caching streaming stores for large sizes.  
Configuration options: [Disabled] [Enabled]

### **X3D [Auto]**

Allows you to set the override of X3D technology.  
Configuration options: [Auto] [Disable] [1 stack] [2 stacks] [4 stacks]

### **IBS hardware workaround [Auto]**

Set this option if using IBS execution sampling without software workaround for erratum 1,285. May impact performance.  
Configuration options: [Auto] [Enabled]

## **DF Common Options**

### **Scrubber**

#### **DRAM scrub time [Auto]**

Allows you to set a number of hours to scrub memory.  
Configuration options: [Disabled] [1 hour] [4 hours] [8 hours] [16 hours] [24 hours] [48 hours] [Auto]

#### **Poison scrubber control [Auto]**

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

#### **Redirect scrubber control [Auto]**

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

#### **Redirect scrubber limit [Auto]**

Configuration options: [2] [4] [8] [Infinite] [Auto]

#### **Periodic Directory Rinse [Auto]**

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

### **Memory Addressing**

#### **NUMA nodes per socket [Auto]**

Specifies the number of desired NUMA nodes per socket. Zero will attempt to interleave the two sockets together.  
Configuration options: [NPS1] [NPS2] [NPS4] [Auto]

#### **Memory interleaving [Auto]**

This item allows for disabling memory interleaving. Note that NUMA nodes per socket will be honored regardless of this setting.  
Configuration options: [Disabled] [Auto]

#### **Memory interleaving size [Auto]**

This item controls the memory interleaving size. The valid values are AUTO, 256 bytes, 512 bytes, 1 Kbytes, or 2 Kbytes. This also determines the starting address of the interleave (bit 8, 9, 10, or 11).  
Configuration options: [256 Bytes] [512 Bytes] [1 KB] [2 KB] [Auto]

#### **1TB remap [Auto]**

Attempt to remap DRAM out of the space just below the 1TB boundary. The ability to remap depends on DRAM configuration, NPS, and interleaving selection, and may not always be possible.

Configuration options: [Do not remap] [Attempt to remap] [Auto]

### **DRAM map inversion [Auto]**

Inverting the map will cause the highest memory channels to get assigned the lowest addresses in the system.

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

### **Location of private memory regions [Auto]**

Controls whether or not the private memory regions (PSP, SMU, and CC6) are at the top of DRAM or distributed. Note that distributed requires memory on all dies. Note that it will always be at the top of DRAM if some dies don't have memory regardless of this option's setting.

Configuration options: [Distributed] [Consolidated] [Consolidated to 1st DRAM pair] [Auto]

## **ACPI**

### **ACPI SRAT L3 Cache As NUMA Domain [Auto]**

[Disabled]	Memory Addressing \ NUMA nodes per socket will be declared.
[Enabled]	Each CCX in the system will be declared as a separate NUMA Domain.
[Auto]	Auto.

### **ACPI SLIT Distance Control [Auto]**

This option determines how the SLIT distances are declared.

Configuration options: [Manual] [Auto]



---

The following items appear only when **ACPI SLIT Distance Control** is set to **[Auto]**.

---

### **ACPI SLIT remote relative distance [Auto]**

Allows you to set the remote socket distance for 2P systems as near (2.8) or far (3.2).

Configuration options: [Near] [Far] [Auto]



---

The following items appear only when **ACPI SLIT Distance Control** is set to **[Manual]**.

---

### **ACPI SLIT same socket distance [C]**

Specify the distance to other physical domains within the same socket.

### **ACPI SLIT remote socket distance [20]**

Specify the distance to domains the remote socket.

### **ACPI SLIT local SLink distance [32]**

Specify the distance to an SLink domain on the same socket.

### **ACPI SLIT remote SLink distance [3C]**

Specify the distance to an SLink domain on the other socket.

### **ACPI SLIT local inter-SLink distance [FF]**

Specify the distance between two SLink domains on the same socket.

### **ACPI SLIT remote inter-SLink distance [FF]**

Specify the distance between two SLink domains, each on a different socket.

## Link

### **GMI encryption control [Auto]**

Allows you to control the GMI link encryption.

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

### **xGMI encryption control [Auto]**

Allows you to control the xGMI link encryption.

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

### **CAKE CRC perf bounds control [Auto]**

Configuration options: [Auto] [Manual]



---

The following item appears only when **CAKE CRC perf bounds control** is set to **[Manual]**.

---

### **CAKE CRC perf bounds [64]**

This item specifies the amount of performance loss that is acceptable to enable CRC protection. Units are in 0.00001%, RangeL disabled (0) - 10% (1000000).

### **xGMI Link Configuration [Auto]**

Allows you to configure the number of xGMI2 links used on a multi-socket system.

Configuration options: [Auto] [2 xGMI Links] [3 xGMI Links] [4 xGMI Links]

### **4-link xGMI max speed [Auto]**

Configuration options: [6.4Gbps] [7.467Gbps] [8.533Gbps] [9.6Gbps] [10.667Gbps] [11Gbps] [12Gbps] [13Gbps] [14Gbps] [15Gbps] [16Gbps] [17Gbps] [18Gbps] [19Gbps] [20Gbps] [21Gbps] [22Gbps] [23Gbps] [24Gbps] [25Gbps] [Auto]

### **3-link xGMI max speed [Auto]**

Configuration options: [6.4Gbps] [7.467Gbps] [8.533Gbps] [9.6Gbps] [10.667Gbps] [11Gbps] [12Gbps] [13Gbps] [14Gbps] [15Gbps] [16Gbps] [17Gbps] [18Gbps] [19Gbps] [20Gbps] [21Gbps] [22Gbps] [23Gbps] [24Gbps] [25Gbps] [Auto]

### **xGMI TXEQ Mode [Auto]**

Allows you to select the XGMI TXEQ/RX vetting mode.

Configuration options: [TXEQ\_Disabled] [TXEQ\_Lane] [TXEQ\_Link] [TXEQ\_RX\_Vet] [Auto]

### **xGMI 18GACOFC [Auto]**

Allows you to enable or disable the 18GACOFC control.

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

### **Disable DF to external downstream IP SyncFloodPropagation [Auto]**

Allows you to enable or disable Error propagation to UMC or any downstream slaves e.g. FCH. Use this to avoid reset in failure scenario.

Configuration options: [Sync Flood disabled] [Sync Flood enabled] [Auto]

### **Disable DF sync flood propagation [Auto]**

Allows you to enable or disable propagation from PIE to other DF components and eventually to SDP ports.

Configuration options: [Sync Flood disabled] [Sync Flood enabled] [Auto]

### **Freeze DF module queues on error [Auto]**

Allows you to enable or disable freezing of all DF queues on error and also forces a sync flood on HWA even if MCAs are disabled.

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

### **CC6 memory region encryption [Auto]**

Allows you to control whether or not the CC6 save/restore memory is encrypted.

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

### **System probe filter [Auto]**

Allows you to control whether or not the probe filter is enabled. Has no effect on parts where the probe filter is fuse disabled.

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

### **Memory Clear [Auto]**

Allows you to enable or disable memory clear. When this item is set to [Disabled], BIOS does not implement MemClear after memory training (only if non-ECC DIMMs are used).

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

### **PSP error injection support [False]**

Configuration options: [False] [True]

## **UMC Common Option**

### **DDR4 Common Options**

#### **DRAM Timing Configuration**

Allows you to enable DRAM timing configuration.



Damage caused by use of your AMD processor outside of specification or in excess of factory settings are not covered by your system manufacturers warranty.



The following items appear only when **[Accept]** is selected for **DRAM Timing Configuration**.

#### **Overclock [Auto]**

Configuration options: [Auto] [Enabled]



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

#### **Memory Clock Speed [Auto]**

Specifies the memory clock frequency.

Configuration options: [Auto] [667MHz] [800MHz] [933MHz] [1067MHz] [1200MHz] [1333MHz] [1467MHz] [1600MHz] [1633MHz] [1667MHz] [1700MHz] [1733MHz] [1767MHz] [1800MHz] [400MHz]

#### **Tcl [Auto]**

Specifies the CAS latency.

Configuration options: [Auto] [8 Clk] [9 Clk] [0Ah Clk] [0Bh Clk] [0Ch Clk] [0Dh Clk] [0Eh Clk] [0Fh Clk] [10h Clk] [11h Clk] [12h Clk] [13h Clk] [14h Clk] [15h Clk] [16h Clk] [17h Clk] [18h Clk] [19h Clk] [1Ah Clk] [1Bh Clk] [1Ch Clk] [1Dh Clk] [1Eh Clk] [1Fh Clk] [20h Clk] [21h Clk]

**Trcdrd [Auto]**

Specifies the RAS# Active to CAS# Read Delay Time.

Configuration options: [Auto] [8 Clk] [9 Clk] [0Ah Clk] [0Bh Clk] [0Ch Clk] [0Dh Clk] [0Eh Clk] [0Fh Clk] [10h Clk] [11h Clk] [12h Clk] [13h Clk] [14h Clk] [15h Clk] [16h Clk] [17h Clk] [18h Clk] [19h Clk] [1Ah Clk] [1Bh Clk]

**Trcdwr [Auto]**

Specifies the RAS# Active to CAS# Write Delay Time.

Configuration options: [Auto] [8 Clk] [9 Clk] [0Ah Clk] [0Bh Clk] [0Ch Clk] [0Dh Clk] [0Eh Clk] [0Fh Clk] [10h Clk] [11h Clk] [12h Clk] [13h Clk] [14h Clk] [15h Clk] [16h Clk] [17h Clk] [18h Clk] [19h Clk] [1Ah Clk] [1Bh Clk]

**Trp [Auto]**

Specifies the Row Precharge Delay Time.

Configuration options: [Auto] [8 Clk] [9 Clk] [0Ah Clk] [0Bh Clk] [0Ch Clk] [0Dh Clk] [0Eh Clk] [0Fh Clk] [10h Clk] [11h Clk] [12h Clk] [13h Clk] [14h Clk] [15h Clk] [16h Clk] [17h Clk] [18h Clk] [19h Clk] [1Ah Clk] [1Bh Clk]

**Tras [Auto]**

Specifies the Active to Precharge Delay Time.

Configuration options: [Auto] [15h Clk] [16h Clk] [17h Clk] [18h Clk] [19h Clk] [1Ah Clk] [1Bh Clk] [1Ch Clk] [1Dh Clk] [1Eh Clk] [1Fh Clk] [20h Clk] [21h Clk] [22h Clk] [23h Clk] [24h Clk] [25h Clk] [26h Clk] [27h Clk] [28h Clk] [29h Clk] [2Ah Clk] [2Bh Clk] [2Ch Clk] [2Dh Clk] [2Eh Clk] [2Fh Clk] [30h Clk] [31h Clk] [32h Clk] [33h Clk] [34h Clk] [35h Clk] [36h Clk] [37h Clk] [38h Clk] [39h Clk] [3Ah Clk]

**Trc Ctrl [Auto]**

Specifies Trc.

Configuration options: [Auto] [Manual]



---

The following item appears only when **Trc Ctrl** is set to **[Manual]**.

---

**Trc [39]**

Specifies Active to Active/Refresh Delay Time. Valid values 87h-1Dh.

**TrrdS [Auto]**

Specifies the Activate to Activate Delay Time, different back group (tRRD\_S).

Configuration options: [Auto] [4 Clk] [5 Clk] [6 Clk] [7 Clk] [8 Clk] [9 Clk] [0Ah Clk] [0Bh Clk] [0Ch Clk]

**TrrdL [Auto]**

Specifies the Activate to Activate Delay Time, same back group (tRRD\_L).

Configuration options: [Auto] [4 Clk] [5 Clk] [6 Clk] [7 Clk] [8 Clk] [9 Clk] [0Ah Clk] [0Bh Clk] [0Ch Clk]

**Tfaw Ctrl [Auto]**

Specifies Tfaw.

Configuration options: [Auto] [Manual]



---

The following item appears only when **Tfaw Ctrl** is set to **[Manual]**.

---

**Tfaw [1A]**

Specifies the Four Activate Window Time. Valid values 36h-6h.

***TwtrS [Auto]***

Specifies the Minimum Write to Read Time, different bank group.

Configuration options: [Auto] [2 Clk] [3 Clk] [4 Clk] [5 Clk] [6 Clk] [7 Clk] [8 Clk] [9 Clk] [0Ah Clk] [0Bh Clk] [0Ch Clk] [0Dh Clk] [0Eh Clk]

***TwtrL [Auto]***

Specifies the Minimum Write to Read Time, same bank group.

Configuration options: [Auto] [2 Clk] [3 Clk] [4 Clk] [5 Clk] [6 Clk] [7 Clk] [8 Clk] [9 Clk] [0Ah Clk] [0Bh Clk] [0Ch Clk] [0Dh Clk] [0Eh Clk]

***Twr Ctrl [Auto]***

Specifies Twr.

Configuration options: [Auto] [Manual]

---



The following item appears only when **Twr Ctrl** is set to **[Manual]**.

***Twr [12]***

Specifies the Minimum Write Recovery Time. Valid values 51h-Ah.

***Trcpage Ctrl [Auto]***

Specifies Trcpage.

Configuration options: [Auto] [Manual]

---



The following item appears only when **Trcpage Ctrl** is set to **[Manual]**.

***Trcpage [0]***

SDRAM Optional Features (tMAW MAC). Valid values 3FFh-0h.

***TrdrdScL Ctrl [Auto]***

Specifies TrdrdScL.

Configuration options: [Auto] [Manual]

---



The following item appears only when **TrdrdScL Ctrl** is set to **[Manual]**.

***TrdrdScL [3]***

Specifies the CAS to CAS Delay Time, same bank group. Valid values Fh-1h.

***TwrwrScL Ctrl [Auto]***

Specifies TwrwrScL.

Configuration options: [Auto] [Manual]

---



The following item appears only when **TwrwrScL Ctrl** is set to **[Manual]**.

***TwrwrScL [3]***

Specifies the CAS to CAS Delay Time, same bank group. Valid values 3Fh-1h.

***Trfc Ctrl [Auto]***

Specifies Trfc.

Configuration options: [Auto] [Manual]



---

The following item appears only when **Trfc Ctrl** is set to **[Manual]**.

---

**Trfc [138]**

Specifies the Refresh Recovery Delay Time (tRFC1). Valid values 3DEh-3Ch.

**Trfc2 Ctrl [Auto]**

Specifies Trfc2.

Configuration options: [Auto] [Manual]

---



The following item appears only when **Trfc2 Ctrl** is set to **[Manual]**.

---

**Trfc2 [C0]**

Specifies the Refresh Recovery Delay Time (tRFC2). Valid values 3DEh-3Ch.

**Trfc4 Ctrl [Auto]**

Specifies Trfc4.

Configuration options: [Auto] [Manual]

---



The following item appears only when **Trfc4 Ctrl** is set to **[Manual]**.

---

**Trfc4 [84]**

Specifies the Refresh Recovery Delay Time (tRFC4). Valid values 3DEh-3Ch.

**Tcwl [Auto]**

Specifies the CAS Write Latency.

Configuration options: [Auto] [9 Clk] [0Ah Clk] [0Bh Clk] [0Ch Clk] [0Eh Clk] [10h Clk] [12h Clk] [14h Clk]

**Trtp [Auto]**

Specifies the Read CAS# to Precharge Delay Time.

Configuration options: [Auto] [5 Clk] [6 Clk] [7 Clk] [8 Clk] [9 Clk] [0Ah Clk] [0Bh Clk] [0Ch Clk] [0Dh Clk] [0Eh Clk]

**Tcke [Auto]**

Specifies the CKE minimum high and low pulse width in memory clock cycles.

Configuration options: [Auto] [1 Clk] [2 Clk] [3 Clk] [4 Clk] [5 Clk] [6 Clk] [7 Clk] [8 Clk] [9 Clk] [0Ah Clk] [0Bh Clk] [0Ch Clk] [0Dh Clk] [0Eh Clk] [0Fh Clk] [10h Clk] [11h Clk] [12h Clk] [13h Clk] [14h Clk] [15h Clk] [16h Clk] [17h Clk] [18h Clk] [19h Clk] [1Ah Clk] [1Bh Clk] [1Ch Clk] [1Dh Clk] [1Eh Clk] [1Fh Clk]

**Trdwr [Auto]**

Specifies the Read to Write turnaround timing.

Configuration options: [Auto] [1 Clk] [2 Clk] [3 Clk] [4 Clk] [5 Clk] [6 Clk] [7 Clk] [8 Clk] [9 Clk] [0Ah Clk] [0Bh Clk] [0Ch Clk] [0Dh Clk] [0Eh Clk] [0Fh Clk] [10h Clk] [11h Clk] [12h Clk] [13h Clk] [14h Clk] [15h Clk] [16h Clk] [17h Clk] [18h Clk] [19h Clk] [1Ah Clk] [1Bh Clk] [1Ch Clk] [1Dh Clk] [1Eh Clk] [1Fh Clk]

**Twrrd [Auto]**

Specifies the Write to Read turnaround timing.

Configuration options: [Auto] [1 Clk] [2 Clk] [3 Clk] [4 Clk] [5 Clk] [6 Clk] [7 Clk] [8 Clk] [9 Clk] [0Ah Clk] [0Bh Clk] [0Ch Clk] [0Dh Clk] [0Eh Clk] [0Fh Clk]

***TwrwrSc [Auto]***

Specifies the Write to Write turnaround timing in the same chipselect. Configuration options: [Auto] [1 Clk] [2 Clk] [3 Clk] [4 Clk] [5 Clk] [6 Clk] [7 Clk] [8 Clk] [9 Clk] [0Ah Clk] [0Bh Clk] [0Ch Clk] [0Dh Clk] [0Eh Clk] [0Fh Clk]

***TwrwrSd [Auto]***

Specifies the Write to Write turnaround timing in the same DIMM. Configuration options: [Auto] [1 Clk] [2 Clk] [3 Clk] [4 Clk] [5 Clk] [6 Clk] [7 Clk] [8 Clk] [9 Clk] [0Ah Clk] [0Bh Clk] [0Ch Clk] [0Dh Clk] [0Eh Clk] [0Fh Clk]

***TwrwrDd [Auto]***

Specifies the Write to Write turnaround timing in a different DIMM. Configuration options: [Auto] [1 Clk] [2 Clk] [3 Clk] [4 Clk] [5 Clk] [6 Clk] [7 Clk] [8 Clk] [9 Clk] [0Ah Clk] [0Bh Clk] [0Ch Clk] [0Dh Clk] [0Eh Clk] [0Fh Clk]

***TrdrdSc [Auto]***

Specifies the Read to Read turnaround timing in the same chipselect. Configuration options: [Auto] [1 Clk] [2 Clk] [3 Clk] [4 Clk] [5 Clk] [6 Clk] [7 Clk] [8 Clk] [9 Clk] [0Ah Clk] [0Bh Clk] [0Ch Clk] [0Dh Clk] [0Eh Clk] [0Fh Clk]

***TrdrdSd [Auto]***

Specifies the Read to Read turnaround timing in the same DIMM. Configuration options: [Auto] [1 Clk] [2 Clk] [3 Clk] [4 Clk] [5 Clk] [6 Clk] [7 Clk] [8 Clk] [9 Clk] [0Ah Clk] [0Bh Clk] [0Ch Clk] [0Dh Clk] [0Eh Clk] [0Fh Clk]

***TrdrdDd [Auto]***

Specifies the Read to Read turnaround timing in a different DIMM. Configuration options: [Auto] [1 Clk] [2 Clk] [3 Clk] [4 Clk] [5 Clk] [6 Clk] [7 Clk] [8 Clk] [9 Clk] [0Ah Clk] [0Bh Clk] [0Ch Clk] [0Dh Clk] [0Eh Clk] [0Fh Clk]

***ProcODT [Auto]***

Specifies the Processor ODT.

Configuration options: [Auto] [High Impedance] [480 ohm] [240 ohm] [160 ohm] [120 ohm] [96 ohm] [80 ohm] [68.6 ohm] [60 ohm] [53.3 ohm] [48 ohm] [43.6 ohm] [40 ohm] [36.9 ohm] [34.3 ohm] [32 ohm] [30 ohm] [28.2 ohm]

## DRAM Controller Configuration

***DRAM Power Options******Power Down Enable [Auto]***

Allows you to enable or disable power down mode.

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

***Power Down Entry Delay [BB8]***

Allows you to specify value at UMC::CH::DramTiming17 [19:8]  
PwrDownDly.

***SubUrgRefLowerBound [4]***

Specifies the stored refresh limit required to enter sub-urgent refresh mode. Constraint: SubUrgRefLowerBound <= UrgRefLimit. Valid value: 6-1

***UrgRefLimit [6]***

Specifies the stored refresh limit required to enter urgent refresh mode. Constraint: SubUrgRefLowerBound <= UrgRefLimit. Valid value: 6-1

### ***DRAM Maximum Activate Count [Auto]***

Override DIMM SPD Byte 7 [3:0]. Maximum Activate Count (MAC).

When set to [Auto] it will be based on SPD setting.

Configuration options: [Untested MAC] [700 K] [600 K] [500 K] [400 K] [300 K] [200 K] [Unlimited MAC] [Auto]

### ***DRAM Refresh Rate [7.8 usec]***

Configuration options: [7.8 usec] [3.9 usec]

### ***Self-Refresh Exit Staggering [Disabled]***

$Tcksrx += (Trfc/n * (UMC_Number \% 4))$ , here  $n = 3$  or  $4$ .

Configuration options: [Disabled] [Trfc / 3] [Trfc / 4]



---

Does not apply the extra addition if set to [Disabled].

---

### ***Cmd2T***

Select between 1T and 2T mode on ADDR/CMD.

Configuration options: [Auto] [1T] [2T]

### ***Gear Down Mode***

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

## **CAD Bus Configuration**

### ***CAD Bus Timing User Controls [Auto]***

Allows you to set the CAD bus signals to Auto or Manual.

Configuration options: [Auto] [Manual]



---

The following items appear only when **CAD Bus Timing User Controls** is set to [Manual].

---

### ***AddrCmdSetup [0]***

Allows you to setup time on CAD bus signals.

Configuration options: [0] - [39]

### ***CsOdtSetup [0]***

Allows you to setup time on CAD bus signals.

Configuration options: [0] - [39]

### ***CkeSetup [0]***

Allows you to setup time on CAD bus signals.

Configuration options: [0] - [39]

### ***CAD Bus Drive Strength User Controls [Auto]***

Allows you to set the CAD bus signals to Auto or Manual.

Configuration options: [Auto] [Manual]



---

The following items appear only when **CAD Bus Drive Strength User Controls** is set to [Manual].

---

### ***ClkDrvStren [Auto]***

Configuration options: [Auto] [120.0 Ohm] [60.0 Ohm] [40.0 Ohm] [30.0 Ohm] [24.0 Ohm] [20.0 Ohm]

### ***AddrCmdDrvStren [Auto]***

Configuration options: [Auto] [120.0 Ohm] [60.0 Ohm] [40.0 Ohm] [30.0 Ohm] [24.0 Ohm] [20.0 Ohm]

### ***Cs0dtDrvStren [Auto]***

Configuration options: [Auto] [120.0 Ohm] [60.0 Ohm] [40.0 Ohm] [30.0 Ohm] [24.0 Ohm] [20.0 Ohm]

### ***CkeDrvStren [Auto]***

Configuration options: [Auto] [120.0 Ohm] [60.0 Ohm] [40.0 Ohm] [30.0 Ohm] [24.0 Ohm] [20.0 Ohm]

## **Data Bus Configuration**

### ***Data Bus Configuration User Controls [Auto]***

Allows you to specify the mode for drive strength.

Configuration options: [Auto] [Manual]



The following items appear only when **Data Bus Configuration User Controls** is set to **[Manual]**.

### ***RttNom [Auto]***

Configuration options: [Rtt\_Nom Disable] [RZQ/4] [RZQ/2] [RZQ/6] [RZQ/1] [RZQ/5] [RZQ/3] [RZQ/7] [Auto]

### ***RttWr [Auto]***

Configuration options: [Dynamic ODT Off] [RZQ/2] [RZQ/1] [Hi-Z] [RZQ/3] [Auto]

### ***RttPark [Auto]***

Configuration options: [Rtt\_PARK Disable] [RZQ/4] [RZQ/2] [RZQ/6] [RZQ/1] [RZQ/5] [RZQ/3] [RZQ/7] [Auto]

## **Common RAS**

### ***Data Poisoning [Auto]***

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

### ***DRAM Post Package Repair [Disable]***

Allows you to enable or disable DRAM POST Package Repair.

Configuration options: [Enable] [Disable]

### ***RCD Parity [Auto]***

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

### ***DRAM Address Command Parity Retry [Auto]***

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



The following item appears only when **DRAM Address Command Parity Retry** is set to **[Enabled]**.

### ***Max Parity Error Replay [8]***

The values in hex, 1, 2, or 3 is invalid.

Configuration options: [0] - [39]

### ***Write CRC Enable [Auto]***

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

### ***DRAM Write CRC Enable and Retry Limit [Auto]***

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



---

The following item appears only when **DRAM Write CRC Enable and Retry Limit** is set to **[Enabled]**.

---

***Max Write CRC Error Replay [8]***

The values in hex, 1, 2, or 3 is invalid.

Configuration options: [0] - [39]

***Disable Memory Error Injection [True]***

Configuration options: [False] [True]

***ECC Configuration***

***DRAM ECC Symbol Size [Auto]***

Configuration options: [x4] [x8] [x16] [Auto]

***DRAM ECC Enable [Auto]***

This option allows you to enable or disable DRAM ECC. Auto will set ECC to enable.

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

***DRAM UECC Retry [Auto]***

This option allows you to enable or disable DRAM UECC Retry.

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

**Security**

***TSME [Auto]***

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

***Data Scramble [Auto]***

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

**Phy Configuration**

***PMU Training***

***DFE Read Training [Auto]***

Perform 2D Read Training with DFE on.

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

***FFE Write Training [Auto]***

Perform 2D Read WriteTraining with FFE on.

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

***PMU Pattern Bits Control [Auto]***

Configuration options: [Auto] [Manual]



---

The following item appears only when **PMU Pattern Bits Control** is set to **[Manual]**.

---

***PMU Pattern Bits [0]***

Configuration options: [0] - [9]

**DRAM Memory Mapping**

***Chipselect Interleaving [Auto]***

Allows you to set interleave memory blocks across the DRAM chip selects for node 0.

Configuration options: [Disabled] [Auto]

***BankGroupSwap [Auto]***

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



### **BankGroupSwapAlt [Auto]**

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

---

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

---

### **Address Hash Bank 2 ColXor [3F8]**

Configuration options: [000] - [FFF]

### **Address Hash Bank [Auto]**

Allows you to enable or disable bank address hashing.  
Configuration options: [Enabled] [Disabled] [Auto]

### **Address Hash CS [Auto]**

Allows you to enable or disable CS address hashing.  
Configuration options: [Enabled] [Disabled] [Auto]

### **Address Hash Rm [Auto]**

Allows you to enable or disable RM address hashing.  
Configuration options: [Enabled] [Disabled] [Auto]

### **SPD Read Optimization [Auto]**

Allows you to enable or disable SPD Read Optimization, if set to [Enabled],  
SPD reads are skipped for Reserved fields and most of upper 256 Bytes. If set  
to [Disabled], read all 512 SPD Bytes.  
Configuration options: [Enabled] [Disabled] [Auto]

## **NVDIMM**

### **Disable NVDIMM-N Feature [No]**

Allows you to disable NVDIMM-N feature for memory margin tool.  
Configuration options: [No] [Yes]

## **Memory MBIST**

### **MBIST Enable [Disabled]**

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

---



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

---

### **MBIST Test Mode [Auto]**

Allows you to select the MBIST Test Mode - Interface Mode (Tests Single and  
Multiple CS transactions and Basic Connectivity) or Data Eye Mode (Measures  
Voltage vs. Timing).  
Configuration options: [Interface Mode] [Data Eye Mode] [Both] [Auto]

### **MBIST Aggressors [Auto]**

Allows you to enable or disable Memory Aggressor test.  
Configuration options: [Enabled] [Disabled] [Auto]

### **MBIST Per Bit Slave Die Reporting [Auto]**

Reports 2D Data Eye Results in ABL Log for each DQ, Chipselect, and  
Channel.  
Configuration options: [Enabled] [Disabled] [Auto]

## Data Eye

### **Pattern Select [PRBS]**

Configuration options: [PRBS] [SS0] [Both]

### **Pattern Length [3]**

This token helps to determine the pattern length. The possible options are N=3...12.

Configuration options: [3] – [9]

### **Aggressor Channel [1 Aggressor Channel]**

This helps read the aggressors channels. If set to [Enabled], you can read from one or more than one aggressor channel. The default is set to [Disabled].

Configuration options: [Disabled] [1 Aggressor Channel] [3 Aggressor Channels] [7 Aggressor Channels]

### **Aggressor Static Lane Control [Disabled]**

Configuration options: [Disabled] [Enabled]



---

The following items appear only when **Aggressor Static Lane Control** is set to **[Enabled]**.

---

### **Aggressor Static Lane Select Upper 32 bits [0]**

Static Lane Select for Upper 32 bits. The bit mask represents the bits to be read.

Configuration options: [0] - [99999999]

### **Aggressor Static Lane Select Lower 32 bits [0]**

Static Lane Select for Lower 32 bits. The bit mask represents the bits to be read.

Configuration options: [0] - [99999999]

### **Aggressor Static Lane Select ECC [0]**

Static Lane Select for ECC Lanes. The bit mask represents the bits to be read.

Configuration options: [0] - [9]

### **Aggressor Static Lane Value [0]**

Configuration options: [0] - [9]

### **Target Static Lane Control [Disabled]**

Configuration options: [Disabled] [Enabled]



---

The following items appear only when **Target Static Lane Control** is set to **[Enabled]**.

---

### **Target Static Lane Select Upper 32 bits [0]**

Static Lane Select for Upper 32 bits. The bit mask represents the bits to be read.

Configuration options: [0] - [99999999]

### **Target Static Lane Select Lower 32 bits [0]**

Static Lane Select for Lower 32 bits. The bit mask represents the bits to be read.

Configuration options: [0] - [99999999]

### **Target Static Lane Select ECC [0]**

Static Lane Select for ECC Lanes. The bit mask represents the bits to be read.

Configuration options: [0] - [9]

**Target Static Lane Value [0]**

Configuration options: [0] - [9]

**Worst Case Margin Granularity [Per Chip Select]**

Configuration options: [Per Chip Select] [Per Nibble]

**Read Voltage Sweep Step Size [1]**

This option determines the step size for Read Data Eye voltage sweep.

Configuration options: [1] [2] [4]

**Read Timing Sweep Step Size [1]**

This option supports step size for Read Data Eye.

Configuration options: [1] [2] [4]

**Write Voltage Sweep Step Size [1]**

This option determines the step size for write Data Eye voltage sweep.

Configuration options: [1] [2] [4]

**Write Timing Sweep Step Size [1]**

This option supports step size for write Data Eye.

Configuration options: [1] [2] [4]

**Memory Healing BIST [Disabled]**

Allows you to enable a full memory test. The testing will increase the boot time. BIOS mem BIST tests the full memory after training. Failing memory will be repaired using soft or hard PPR depending on the PPC configuration. The test will take 3 minutes per 16GN of installed memory. Self-Healing BIST runs the JEDEC DRAM self healing if the device supports the feature. The DRAM will do a hard repair for failing memory. The test will take 10 seconds per memory rank per channel.

Configuration options: [Disabled] [BIOS Mem BIST] [Self-Healing Mem BIST] [BIOS and Self-Healing Mem BIST]



---

The following items appear only when **Memory Healing BIST** is set to **[BIOS Mem BIST]**.

---

**Mem BIST Test Select [Vendor Tests Enabled]**

Select the vendor specific tests to use with BIOS memory healing BIST.

Configuration options: [Vendor Tests Enabled] [Vendor Tests Disabled] [All Tests - All Vendors]

**Mem BIST Post Package Repair Type [Soft Repair]**

For DRAM errors found in the BIOS memory BIST select the repair type, soft, hard, or test only and do not attempt to repair.

Configuration options: [Soft Repair] [Hard Repair] [No Repairs - Test only]

## NBIO Common Options

**IOMMU [Disabled]**

Allows you to enable or disable IOMMU.

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

**DMAR Support [Auto]**

Allows you to enable DMAr system protection during POST.

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



---

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

---

### **ACS Enable [Auto]**

AER must be enabled for ACS enable to work.  
Configuration options: [Disable] [Enable] [Auto]

### **PCIe ARI Support [Auto]**

This item enables Alternative Routing-ID Interpretation.  
Configuration options: [Disable] [Enable] [Auto]

### **PCIe ARI Enumeration [Auto]**

Allows ARI Forwarding for each downstream port.  
Configuration options: [Disable] [Enable] [Auto]

### **PCIe Ten Bit Tag Support [Auto]**

This item enables PCIe ten bit tags for supported devices. [Auto] = [Disabled].  
Configuration options: [Disable] [Enable] [Auto]

### **HD Audio Enable [Auto]**

Configuration options: [Disabled] [Enable] [Auto]

## **SMU Common Options**

### **Determinism Control [Manual]**

[Auto] Use the fused Determinism.  
[Manual] User can set customized Determinism.



---

The following item appears only when **Determinism Control** is set to **[Manual]**.

---

### **Determinism Slider [Power]**

Configuration options: [Auto] [Power] [Performance]

### **Fan Control**

#### ***Fan Table Control [Auto]***

[Auto] Use the default fan table.  
[Manual] User can set customized fan table.



---

The following item appears only when **Fan Table Control** is set to **[Manual]**.

---

#### ***Low Temperature [0]***

Allows you to set the low temperature in °C.

#### ***Medium Temperature [0]***

Allows you to set the medium temperature in °C.

#### ***High Temperature [0]***

Allows you to set the high temperature in °C.

#### ***Critical Temperature [0]***

Allows you to set the critical temperature in °C.

#### ***Low Pwm [0]***

Allows you to set the low Pwm from 0-100.

#### ***Medium Pwm [0]***

Allows you to set the medium Pwm from 0-100.

#### ***High Pwm [0]***

Allows you to set the high Pwm from 0-100.

### **Temperature Hysteresis [0]**

Allows you to set the temperature hysteresis in °C.

### **Pwm Frequency [25kHz]**

Configuration options: [100Hz] [25kHz]

### **Fan Polarity [Negative]**

Configuration options: [Negative] [Positive]

### **cTDP Control [Manual]**

[Auto] Use the fused TDP.

[Manual] User can set customized TDP.



---

The following item appears only when **cTDP Control** is set to **[Manual]**.

---

### **cTDP [280]**

Allows you to customize cTDP.

### **EfficiencyModeEn [Auto]**

[Auto] Use performance optimized CCLK DPM settings.

[Enabled] Use power efficiency optimized CCLK DPM settings.

### **Power Package Limit Control [Manual]**

[Auto] Use the fused PPT.

[Manual] User can set customized PPT.



---

The following item appears only when **Power Package Limit Control** is set to **[Manual]**.

---

### **Power Package Limit [280]**

Allows you to customize PPT.

### **xGMI Link Width Control [Auto]**

[Auto] Use default xGMI link width controller settings.

[Manual] User can set custom xGMI link width controller settings.



---

The following items appear only when **xGMI Link Width Control** is set to **[Manual]**.

---

### **xGMI Force Link Width Control [Unforce]**

[Unforce] Do not force the xGMI to a fixed width.

[Force]Force the xGMI to the user specified width.



---

The following item appears only when **xGMI Force Link Width Control** is set to **[Force]**.

---

### **xGMI Force Link Width [2]**

[0] Force xGMI link width to x2.

[1] Force xGMI link width to x8.

[2] Force xGMI link width to x16.

### **xGMI Max Link Width Control [Auto]**

[Auto] Use default xGMI max supported link width.

[Manual] User can set custom xGMI max link width.



---

The following item appears only when **xGMI Max Link Width Control** is set to **[Manual]**.

---

**xGMI Max Link Width [1]**

- [0] Set max xGMI link width to x8.
- [1] Set max xGMI link width to x16.

**APBDIS [Auto]**

- [0] Not APBDIS (mission mode)
- [1] APBDIS
- [Auto] Auto

**DF Cstates [Auto]**

Allows you to enable or disable DF C-states.  
Configuration options: [Disabled] [Enabled] [Auto]

**CPPC [Auto]**

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

**HSMP Support [Auto]**

This option allows you to enable or disable HSMP support.  
Configuration options: [Disabled] [Enabled] [Auto]

**DLWM Support [Auto]**

This option allows you to enable or disable DLWM support.  
Configuration options: [Disabled] [Enabled] [Auto]

**BoostFmaxEn [Auto]**

[Auto] Use the default Fmax.  
[Manual] User can set the boost Fmax.



---

The following item appears only when **Boost FmaxEn** is set to **[Manual]**.

---

**BoostFmax [0]**

Allows you to specify the boost Fmax frequency limit to apply to all cores (MHz).

**EDC Current Tracking [Disable]**

The generation of a correctable MCE when the telemetry current value is over the set threshold defined by EDC Current Tracking Current Threshold.  
Configuration options: [Disable] [Enable]



---

The following items appears only when **EDC Current Tracking** is set to **[Enable]**.

---

**EDC Tracking Current Threshold [0]**

The current threshold in AMPs for EDC Current Tracking feature.

**EDC Tracking Report Interval [1]**

Reporting interval. Every nth observed excursion results in SMU logging a correctable MCE.

### LCLK Frequency Control

#### *Root Complex 0x00 LCLK Frequency [Auto]*

Set Root Complex LCLK Frequency (Bus range 0x00-0x3F).

[Auto] Dynamic Frequency Control (Enhanced PIO setting will be in effect).

[593MHz] Set LCLK Frequency at 593MHz (Overrides Enhanced PIO setting).

#### *Root Complex 0x40 LCLK Frequency [Auto]*

Set Root Complex LCLK Frequency (Bus range 0x40-0x7F).

[Auto] Dynamic Frequency Control (Enhanced PIO setting will be in effect).

[593MHz] Set LCLK Frequency at 593MHz (Overrides Enhanced PIO setting).

#### *Root Complex 0x80 LCLK Frequency [Auto]*

Set Root Complex LCLK Frequency (Bus range 0x80-0xBF).

[Auto] Dynamic Frequency Control (Enhanced PIO setting will be in effect).

[593MHz] Set LCLK Frequency at 593MHz (Overrides Enhanced PIO setting).

#### *Root Complex 0xC0 LCLK Frequency [Auto]*

Set Root Complex LCLK Frequency (Bus range 0xC0-0xFF).

[Auto] Dynamic Frequency Control (Enhanced PIO setting will be in effect).

[593MHz] Set LCLK Frequency at 593MHz (Overrides Enhanced PIO setting).

### DF PState Mode Select [Auto]

[Normal] Normal

[Limit Highest] FCLK is limited to DF Pstate FCLK Limit, only the highest DF Pstate is used.

[Limit All] FCLK is limited to DF Pstate FCLK limit, all DF Pstates are used.

[Auto] Auto



---

The following item appears only when **DF PState Mode Select** is set to **[Limit Highest]** or **[Limit All]**.

---

### DF PState FClk Limit [Auto]

Allows you to set the fixed PState when DF PState Mode Select is overridden. Configuration options: [1600 MHz] [1467 MHz] [1333 MHz] [1200 MHz] [1067 MHz] [933 MHz] [800 MHz] [Auto]

### EDC Control [Auto]

[Auto] Use the fused VDDCR\_CPU EDC limit.

[Manual] User can set customized VDDCR\_CPU EDC limit.



---

The following items appear only when **EDC Control** is set to **[Manual]**.

---

### **EDC [0]**

Allows you to set the VDDCR\_CPU EDC Limit [A].

### **EDC Platform Limit [0]**

Allows you to set the EDC Platform Limit [W].

## **NBIO RAS Common Options**

### **NBIO RAS Control [Auto]**

Configuration options: [Disabled] [MCA] [Legacy] [Auto]

### **Egress Poison Severity High [30011]**

Each bit set to 1 enables HIGH severity on the associated IOHC egress port. A bit of 0 indicates LOW severity.

### **Egress Poison Severity Low [4]**

Each bit set to 1 enables HIGH severity on the associated IOHC egress port. A bit of 0 indicates LOW severity.

### **NBIO SyncFlood Generation [Auto]**

This value may be used to mask SyncFlood caused by NBIO RAS options. When set to TRUE, SyncFlood from NBIO is masked. When set to FALSE, NBIO is capable of generating SyncFlood.

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

### **NBIO SyncFlood Reporting [Auto]**

This value may be used to enable SyncFlood reporting to APML. When set to TRUE, SyncFlood will be reported to APML. When set to FALSE, the reporting will be disabled.

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

### **Egress Poison Mask High [FFFCFFFF]**

These set the enable mask for masking of errors logged in EGRESS\_POISON\_STATUS. For each bit set to 1, errors are masked. For each bit set to 0, errors trigger response actions.

### **Egress Poison Mask Low [FFFFFFFB]**

These set the enable mask for masking of errors logged in EGRESS\_POISON\_STATUS. For each bit set to 1, errors are masked. For each bit set to 0, errors trigger response actions.

### **Uncorrected Converted to Poison Enable Mask High [30000]**

These set the enable mask for masking of uncorrectable parity errors on internal arrays. For each bit set to 1, a system fatal error event is triggered for UCP errors on arrays associated with that egress port. For each bit set to 0, errors are masked.

### **Uncorrected Converted to Poison Enable Mask Low [4]**

These set the enable mask for masking of uncorrectable parity errors on internal arrays. For each bit set to 1, a system fatal error event is triggered for UCP errors on arrays associated with that egress port. For each bit set to 0, errors are masked.

**System Hub Watchdog Timer [A28]**

This value specifies the timer interval of the SYSHUB Watchdog Timer in milliseconds.

**SLink Read Response OK [Disabled]**

This value specifies whether SLINK read response errors are converted to an Okay response. When this value is set to TRUE, read response errors are converted to Okay responses with data of all FFs. When set to FALSE, read response errors are not converted.

Configuration options: [Disabled] [Enabled]

**SLink Read Response Error Handling [Log Errors in MCA]**

This value specifies whether SLINK write response errors are converted to an Okay response. When this value is set to 0, write response errors will be logged in the MCA. When set to 1, write response errors will trigger an MCOMMIT error. When this value is set to 2, write response errors are converted.

Configuration options: [Enabled] [Trigger MCOMMIT Error] [Log Errors in MCA]

**Log Poison Data from SLINK [Disabled]**

This value specifies whether poison data propagated from SLINK will generate a deferred error. When this value is set to TRUE, deferred errors are enabled. When set to FALSE, errors are not generated.

Configuration options: [Disabled] [Enabled]

**PCIe Aer Reporting Mechanism [Auto]**

This value selects the method of reporting AER errors from PCI Express. A value of 0 indicates that the hardware will report the error through MCA. A value of 1 allows OS First handling of the errors through generation of a system control interrupt (SCI). A value of 2 allows Firmware First handling of the errors through generation of a system control interrupt (SCI).

Configuration options: [Firmware First] [OS First] [Auto]

**Edpc Control [Auto]**

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

**NBIO Poison Consumption [Auto]**

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

**Sync Flood on PCIe Fatal Error [Auto]**

Configuration options: [Auto] [True] [False]

**Enable AER Cap [Auto]**

Allows you to enable or disable Advanced Error Reporting Capability.

Configuration options: [Enable] [Disabled] [Auto]

**Early Link Speed [Auto]**

Allows you to set Early Link Speed.

Configuration options: [Auto] [Gen1] [Gen2]

**Hot Plug Handling mode [Auto]**

Allows you to control the Hot Plug Handling mode.

Configuration options: [OS First] [Firmware First] [Auto]

### **Presence Detect Select mode [Auto]**

Allows you to control the Presence Detect Select mode.

Configuration options: [OR] [AND] [Auto]

### **Preferred IO [Auto]**

Allows you to select the preferred IO select type.

Configuration options: [Bus] [Auto]

### **Data Link Feature Cap [Auto]**

Allows you to set Data Link Feature Capability.

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

### **CV test [Auto]**

Set this to [Enabled] to support running PCIECV tool. Selecting [Auto] will preserve h/w defaults.

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

### **SEV-SNP Support [Disable]**

Configuration options: [Disabled] [Enabled]

### **SRIS [Auto]**

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

## **FCH Common Options**

### **SATA Configuration Optoins**

#### **SATA Enable [Auto]**

Allows you to enable or disable OnChip SATA controller.

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



---

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

---

#### **SATA Mode [AHCI]**

Allows you to select the OnChip SATA Type.

Configuration options: [AHCI] [AHCI as ID 0x7904] [Auto]

#### **Sata RAS Support [Auto]**

Allows you to enable or disable Sata RAS Support.

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

#### **Sata Disabled AHCI Prefetch Function [Auto]**

Allows you to enable or disable Sata Disabled AHCI Prefetch Function.

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

#### **Aggressive SATA Device Sleep Port 0 [Auto]**

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



---

The following item appears only when **Aggressive SATA Device Sleep Port 0** is set to **[Enabled]**.

---

#### **DevSleep0 Port Number [0]**

Allows you to set the DEVSLP port 0.

Configuration options: [0] - [7]



## Aggressive SATA Device Sleep Port 1 [Auto]

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

---

The following item appears only when **Aggressive SATA Device Sleep Port 1** is set to **[Enabled]**.

---

### DevSleep1 Port Number [0]

Allows you to set the DEVSLP port 1.

Configuration options: [0] - [7]

## SATA Controller options

### **SATA Controller Enable**

#### **Sata0 Enable [Auto]**

Allows you to enable or disable Sata0. Each IOD has 4 SATA Controllers.

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

#### **Sata1 Enable [Auto]**

Allows you to enable or disable Sata1. Each IOD has 4 SATA Controllers.

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

#### **Sata2 Enable [Auto]**

Allows you to enable or disable Sata2. Each IOD has 4 SATA Controllers.

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

#### **Sata3 Enable [Auto]**

Allows you to enable or disable Sata3. Each IOD has 4 SATA Controllers.

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

#### **Sata4 (Socket1) Enable [Auto]**

Allows you to enable or disable Sata4 on Socket 1 (IOD1). Each IOD has 4 SATA Controllers.

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

#### **Sata5 (Socket1) Enable [Auto]**

Allows you to enable or disable Sata5 on Socket 1 (IOD1). Each IOD has 4 SATA Controllers.

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

#### **Sata6 (Socket1) Enable [Auto]**

Allows you to enable or disable Sata6 on Socket 1 (IOD1). Each IOD has 4 SATA Controllers.

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

#### **Sata7 (Socket1) Enable [Auto]**

Allows you to enable or disable Sata7 on Socket 1 (IOD1). Each IOD has 4 SATA Controllers.

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

## SATA Controller eSATA



### **SATA Controller DevSlp**

#### **Socket1 DevSlp**

##### **Socket1 DevSlp0 Enable [Auto]**

Only Sata0 on each IOD/socket supports DevSlp.

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

---

The following item appears only when **Socket1 DevSlp0 Enable** is set to [Enabled].

##### **DevSleep0 Port Number [0]**

Allows you to set DEVSLP port 0.

Configuration options: [0] - [7]

##### **Socket1 DevSlp1 Enable [Auto]**

Only Sata0 on each IOD/socket supports DevSlp.

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

---



The following item appears only when **Socket1 DevSlp1 Enable** is set to [Enabled].

##### **DevSleep1 Port Number [1]**

Allows you to set DEVSLP port 1.

Configuration options: [0] - [7]

### **SATA Controller GPIO**

#### **Sata0 GPIO [Auto]**

Allows you to enable or disable SataSgpi on Sata0.

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

#### **Sata1 GPIO [Auto]**

Allows you to enable or disable SataSgpi on Sata1.

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

#### **Sata2 GPIO [Auto]**

Allows you to enable or disable SataSgpi on Sata2.

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

#### **Sata3 GPIO [Auto]**

Allows you to enable or disable SataSgpi on Sata3.

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

#### **Sata4 GPIO [Auto]**

Allows you to enable or disable SataSgpi on Sata4.

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

#### **Sata5 GPIO [Auto]**

Allows you to enable or disable SataSgpi on Sata5.

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

#### **Sata6 GPIO [Auto]**

Allows you to enable or disable SataSgpi on Sata6.

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

#### **Sata7 GPIO [Auto]**

Allows you to enable or disable SataSgpi on Sata7.

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

## USB Configuration Options

### XHCI Controller0 enable [Auto]

Allows you to enable or disable USB3 controller.  
Configuration options: [Enabled] [Disabled] [Auto]

### XHCI Controller1 enable [Auto]

Allows you to enable or disable USB3 controller.  
Configuration options: [Enabled] [Disabled] [Auto]

### USB ecc SMI Enable [Auto]

Configuration options: [Enable] [Off] [Auto]

### MCM USB enable

#### XHCI2 enable (Socket1) [Auto]

Allows you to enable or disable USB3 controller.  
Configuration options: [Disabled] [Enabled] [Auto]

#### XHCI3 enable (Socket1) [Auto]

Allows you to enable or disable USB3 controller.  
Configuration options: [Disabled] [Enabled] [Auto]

## SD Dump Options

### SD Configuration Mode [SD Dump disabled]

Configuration options: [SD Dump disabled] [SD Dump enabled]

## Ac Power Loss Options

### AC Loss Control [Always On]

Allows you to select Ac Loss Control Method.  
Configuration options: [Always Off] [Always On] [Reserved] [Previous] [Auto]

## I2C Configuration Options

### I2C 0 Enable [Auto]

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

### I2C 1 Enable [Auto]

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

### I2C 2 Enable [Auto]

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

### I2C 3 Enable [Auto]

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

### I2C 4 Enable [Auto]

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

### I2C 5 Enable [Auto]

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

## Uart Configuration Options

### Uart 0 Enable [Auto]

Uart 0 has no HW FC is Uart 2 is enabled.

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



---

The following item appears only when **Uart 0 Enable** is set to **[Enabled]**.

---

#### **Uart 0 Legacy Options [Auto]**

Configuration options: [Disabled] [0x2E8] [0x2F8] [0x3E8] [0x3F8] [Auto]

#### **Uart 1 Enable [Auto]**

Uart 1 has no HW FC is Uart 3 is enabled.

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



---

The following item appears only when **Uart 1 Enable** is set to **[Enabled]**.

---

#### **Uart 1 Legacy Options [Auto]**

Configuration options: [Disabled] [0x2E8] [0x2F8] [0x3E8] [0x3F8] [Auto]

#### **Uart 2 Enable (no HW FC) [Auto]**

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



---

The following item appears only when **Uart 2 Enable (no HW FC)** is set to **[Enabled]**.

---

#### **Uart 2 Legacy Options [Auto]**

Configuration options: [Disabled] [0x2E8] [0x2F8] [0x3E8] [0x3F8] [Auto]

#### **Uart 3 Enable (no HW FC) [Auto]**

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



---

The following item appears only when **Uart 3 Enable (no HW FC)** is set to **[Enabled]**.

---

#### **Uart 3 Legacy Options [Auto]**

Configuration options: [Disabled] [0x2E8] [0x2F8] [0x3E8] [0x3F8] [Auto]

### **FCH RAS Options**

#### **ALink RAS Support [Auto]**

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

#### **Reset after sync flood [Auto]**

Enable AB to forward downstream sync-flood message to system controller.

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

### **Miscellaneous Options**

#### **Boot Timer Enable [Auto]**

[Disabled] Force PMx44 bit 27 = 1.

[Enabled] Force PMx44 bit 27 = 0.

[Auto] PMx44 bit 27 = PcdBootTimerEnable.

### **NTB Common Options**

#### **Socket-0 P0 NTB Enable [Auto]**

Allows you to enable NTB on Socket-0 P0 Link.

Configuration options: [Auto] [Enable]



---

The following items appear only when **Socket-0 P0 NTB Enable** is set to **[Enabled]**.

---

#### **Socket-0 P0 Start Lane [0]**

Allows you to set the NTB Start Lane on Socket-0 P0 Link.  
Configuration options: [0] - [15]

#### **Socket-0 P0 End Lane [15]**

Allows you to set the NTB End Lane on Socket-0 P0 Link.  
Configuration options: [0] - [15]

#### **Socket-0 P0 Link Speed [Auto]**

Allows you to select the Link Speed for Socket-0 P0.  
Configuration options: [Max Speed] [Gen 1] [Gen 2] [Gen 3] [Auto] [Gen 4]

#### **Socket-0 P0 NTB Mode [Auto]**

Allows you to select the NTB Mode for Socket-0 P0 Link.  
Configuration options: [Auto] [NTB Disabled] [NTB Primary] [NTB Secondary]

#### **Socket-0 P1 NTB Enable [Auto]**

Allows you to enable NTB on Socket-0 P1 Link.  
Configuration options: [Auto] [Enable]



---

The following items appear only when **Socket-0 P1 NTB Enable** is set to **[Enabled]**.

---

#### **Socket-0 P1 Start Lane [32]**

Allows you to set the NTB Start Lane on Socket-0 P1 Link.  
Configuration options: [32] - [47]

#### **Socket-0 P1 End Lane [47]**

Allows you to set the NTB End Lane on Socket-0 P1 Link.  
Configuration options: [32] - [47]

#### **Socket-0 P1 Link Speed [Auto]**

Allows you to select the Link Speed for Socket-0 P1.  
Configuration options: [Max Speed] [Gen 1] [Gen 2] [Gen 3] [Auto] [Gen 4]

#### **Socket-0 P1 NTB Mode [Auto]**

Allows you to select the NTB Mode for Socket-0 P1 Link.  
Configuration options: [Auto] [NTB Disabled] [NTB Primary] [NTB Secondary]

#### **Socket-0 P2 NTB Enable [Auto]**

Allows you to enable NTB on Socket-0 P2 Link.  
Configuration options: [Auto] [Enable]



---

The following items appear only when **Socket-0 P2 NTB Enable** is set to **[Enabled]**.

---

#### **Socket-0 P2 Start Lane [80]**

Allows you to set the NTB Start Lane on Socket-0 P2 Link.  
Configuration options: [80] - [95]

### **Socket-0 P2 End Lane [95]**

Allows you to set the NTB End Lane on Socket-0 P2 Link.

Configuration options: [80] - [95]

### **Socket-0 P2 Link Speed [Auto]**

Allows you to select the Link Speed for Socket-0 P2.

Configuration options: [Max Speed] [Gen 1] [Gen 2] [Gen 3] [Auto] [Gen 4]

### **Socket-0 P2 NTB Mode [Auto]**

Allows you to select the NTB Mode for Socket-0 P2 Link.

Configuration options: [Auto] [NTB Disabled] [NTB Primary] [NTB Secondary]

### **Socket-0 P3 NTB Enable [Auto]**

Allows you to enable NTB on Socket-0 P3 Link.

Configuration options: [Auto] [Enable]



The following items appear only when **Socket-0 P3 NTB Enable** is set to **[Enabled]**.

---

### **Socket-0 P3 Start Lane [112]**

Allows you to set the NTB Start Lane on Socket-0 P3 Link.

Configuration options: [112] - [127]

### **Socket-0 P3 End Lane [127]**

Allows you to set the NTB End Lane on Socket-0 P3 Link.

Configuration options: [112] - [127]

### **Socket-0 P3 Link Speed [Auto]**

Allows you to select the Link Speed for Socket-0 P3.

Configuration options: [Max Speed] [Gen 1] [Gen 2] [Gen 3] [Auto] [Gen 4]

### **Socket-0 P3 NTB Mode [Auto]**

Allows you to select the NTB Mode for Socket-0 P3 Link.

Configuration options: [Auto] [NTB Disabled] [NTB Primary] [NTB Secondary]

## **Soc Miscellaneous Control**

### **ABL Console Out Control [Auto]**

[Disable] Disable ConsoleOut Function for ABL.

[Enable] Enable ConsoleOut Function for ABL.

[Auto] Keep default behavior.



The following items appear only when **ABL Console Out Control** is set to **[Enable]**.

---

### **ABL Basic Console Out Control [Auto]**

[Disable] Disable Basic ConsoleOut Function for ABL.

[Enable] Enable Basic ConsoleOut Function for ABL.

[Auto] Keep default behavior.

### **ABL PMU message Control [Auto]**

Allows you to control the total number of PMU debug messages. Several major controls are listed below:

1. Detailed debug messages (e.g. Eye delays)
2. Coarse debug messages (e.g. rank information)
3. Stage completion
4. Firmware completion message only

Configuration options: [Detailed debug message] [Coarse debug messages] [Stage completion] [Firmware completion message only] [Auto]

## **Workload Tuning**

### **Workload Profile [Auto]**

Allows you to select the profile for different workloads.

[Disabled]	Don't use any workload profile.
[CPU Intensive]	Tuned for CPU intensive workloads, providing optimal integer and floating point performance.
[Java Throughput]	Tuned for the highest level of throughput with java workloads.
[Java Latency]	Tuned for the latency sensitive java workloads, to meet critical SLA's.
[Power Efficiency]	Tuned for optimal power efficiency.
[Memory Throughput Intensive]	Tuned for the highest memory throughput available.
[Storage IO Intensive]	Tuned for the highest storage IO bandwidth.
[NIC Throughput Intensive]	Tuned for maximum TCP/IP and RDMA network throughput.
[NIC Latency Intensive]	Tuned for network performance where the kernel performs L3 packet forwarding.
[Accelerator Throughput]	Tuned to maximum peer-to-peer PCIe throughput with accelerators such as GPU's.
[VMware vSphere Optimized]	Tuned for general virt+P3+Q4.
[Linux KVM Optimized]	Tuned for general virtualization performance when using Linux KVM.
[Container Optimized]	Optimized for container performance.
[RDBMS Optimized]	Tuned for relational databases.
[Big Data Analytics Optimized]	Tuned for big data analytics.
[IOT Gateway]	Tuned for throughput analytics as observed by IOT gateways.
[HPC Optimized]	Tuned for general HPC performance.
[OpenStack NFV]	Tuned for Openstack based NFV workloads.
[OpenStack for RealTime Kernel]	Tuned for Openstack with RealTime kernel enabled.
[Auto]	Use BIOS default workload profile.

### Performance Tracing [Auto]

Allows you to enable or disable allow capturing performance traces.  
Configuration options: [Disabled] [Enabled] [Auto]

## 4.5.5 APM Configuration

Allows you to configure the Advance Power Management (APM) settings.

Aptio Setup - AMI		
Advanced		
Restore AC Power Loss	[Last State]	Select AC power state when power is re-applied after a power failure.
Power On By PCI-E	[Disabled]	
Power On By RTC	[Disabled]	

### Restore AC Power Loss [Last State]

[Power Off] The system goes into off state after an AC power loss.  
[Power On] The system will reboot after an AC power loss.  
[Last State] The system goes into either off or on state, whatever the system state was before the AC power loss.

### Power On By PCI-E [Disabled]

[Disabled] Disables the PCIE devices to generate a wake event.  
[Enabled] Enables the 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.

## 5.5.6 Onboard LAN Configuration

Aptio Setup - AMI	
Advanced	
► Onboard X710 LAN Configuration	Onboard X710 LAN Enable/Disable

### Onboard X710 LAN Configuration

#### Intel X710 LAN1

##### ROM Type [PXE]

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

#### Intel X710 LAN2

##### LAN Enable [JumperState]

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



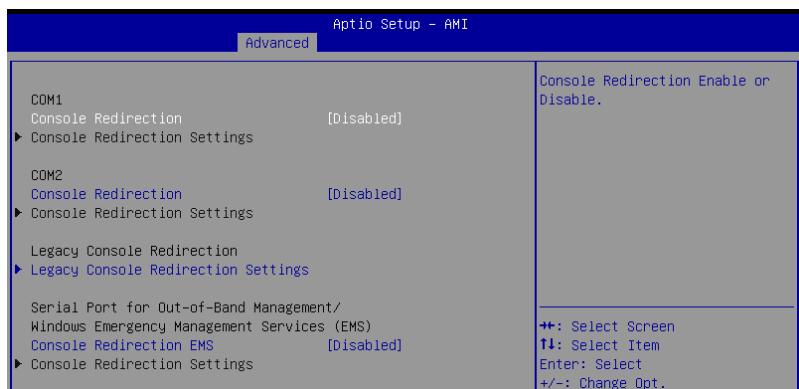
The following item appears only when **LAN Enable** is set to **[JumperState]**.

#### **ROM Type [Disabled]**

Allows you to select the Intel LAN ROM type.

Configuration options: **[Disabled]** **[PXE]**

### **4.5.7 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** 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 resolution.

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

### Legacy Console Redirection Port [COM1]

Allows you to select a COM port to display redirection of Legacy OS and Legacy OROM 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]

This setting allows you to specify if Bootloader is selected than Legacy console redirection.

Configuration options: [Always Enable] [Bootloader]

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

### Console Redirection EMS [Disabled]

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 [VT-UTF8]

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

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

#### Bits per second [115200]

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

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

#### Flow Control [None]

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

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

## 4.5.8 CPU Configuration

This page displays the CPU node information.

Aptio Setup - AMI		
Advanced		
CPU Configuration		Enable/disable CPU Virtualization
SVM Mode	[Enable]	
► Node 0 Information		

### SVM Mode [Enable]

Allows you to enable or disable CPU Virtualization.

Configuration options: [Disabled] [Enabled]

### Node 0 Information

Allows you to view memory information related to Node 0.

## 4.5.9 PCI Subsystem Settings

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

Aptio Setup - AMI		
Advanced		
PCI Devices Common Settings:		
Above 4G Decoding	[Enabled]	Enables or Disables 64bit capable Devices to be Decoded in Above 4G Address Space (Only if System Supports 64 bit PCI Decoding).
First VGA 4G Decode	[Auto]	
LAN Device 4G Decode	[Auto]	
Re-Size BAR Support	[Disabled]	
SR-IOV Support	[Disabled]	

### 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 [Auto]

LAN Device 4G Decode.

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]



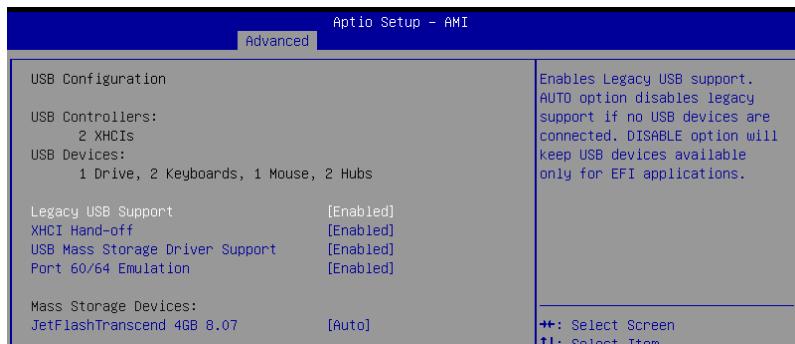
To enable Re-Size BAR Support for harnessing full GPU memory, please set CSM (Compatibility Support Module) to [Disabled].

## SR-IOV Support [Disabled]

This option enables or disables Single Root IO Virtualization Support if the system has SR-IOV capable PCIe devices.

Configuration options: [Disabled] [Enabled]

## 4.5.10 USB Configuration



### Legacy USB Support [Enabled]

Allows you to enable or disable Legacy USB device support.

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

### 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.

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

## 4.5.11 Network Stack Configuration

Aptio Setup - AMI		
Advanced		
Network Stack	[Disabled]	Enable/Disable UEFI Network Stack

### Network stack [Disabled]

Enables or disables the network stack feature.

Configuration options: [Disable] [Enable]



The following item appears 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 option will not be created.

Configuration options: [Disabled] [Enabled]

### Ipv4 HTTP Support [Disabled]

Enables or disables the Ipv4 HTTP Boot Support. If disabled, Ipv4 HTTP boot option will not be created.

Configuration options: [Disabled] [Enabled]

### Ipv6 PXE Support [Disabled]

Enables or disables the Ipv6 PXE Boot Support. If disabled, Ipv6 PXE boot option will not be created.

Configuration options: [Disabled] [Enabled]

### Ipv6 HTTP Support [Disabled]

Enables or disables the Ipv6 HTTP Boot Support. If disabled, Ipv6 HTTP boot option will not be created.

Configuration options: [Disabled] [Enabled]

### PXE boot wait time [0]

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

### Media detect count [1]

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

## 4.5.12 CSM Configuration

Aptio Setup - AMI	
Advanced	
Compatibility Support Module Configuration	Enable/Disable CSM Support.
CSM Support [Disabled]	

### CSM Support [Disabled]

This option allows you to enable or disable CSM Support.

Configuration options: [Disabled] [Enabled]



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

### GateA20 Active [Upon Request]

This allows you to set the GA20 option.

Configuration options: [Upon Request] [Always]

### Option ROM Messages [Force BIOS]

This allows you to set the display mode for option ROM.

Configuration options: [Force BIOS] [Keep Current]

### INT19 Trap Response [Immediate]

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]

This option 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 Option filter [UEFI and Legacy]

This option allows you to control the Legacy/UEFI ROMs priority.

Configuration options: [UEFI and Legacy] [Legacy only] [UEFI only]

### Network [UEFI]

This option allows you to control the execution of UEFI and Legacy Network OpROM.

Configuration options: [Do Not Launch] [UEFI] [Legacy]

### Storage [UEFI]

This option allows you to control the execution of UEFI and Legacy Storage OpROM.

Configuration options: [Do Not Launch] [UEFI] [Legacy]

### Video [Legacy]

This option allows you to control the execution of UEFI and Legacy Video OpROM.

Configuration options: [Do Not Launch] [UEFI] [Legacy]

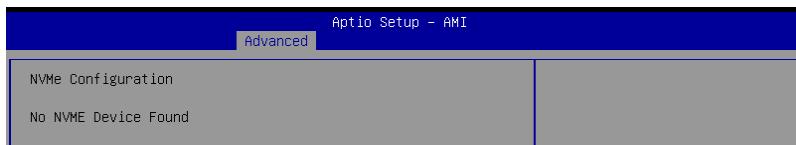
### Other PCI devices [UEFI]

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

Configuration options: [Do Not Launch] [UEFI] [Legacy]

## 4.5.13 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]

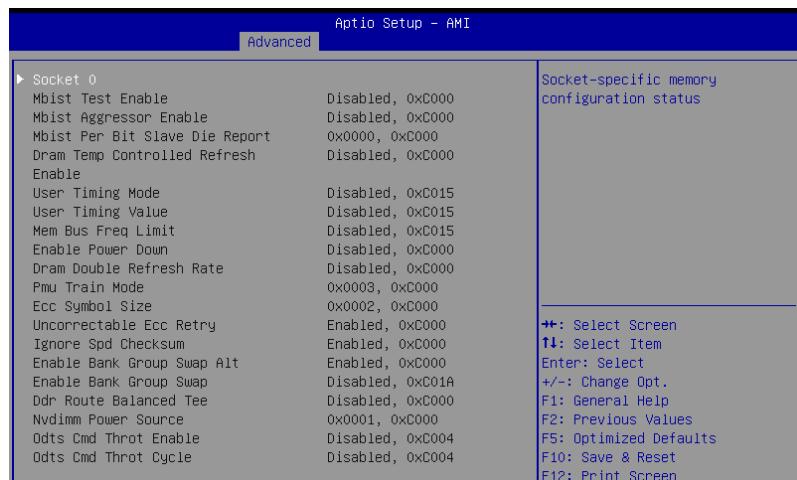
Allows you to select either to test Controller alone or Controller and NameSpace. Selecting Controller and Namespace option will take a lot longer to complete the test. Configuration options: [Controller Only Test] [Controller and NameSpace Test]

### Run Device Self Test

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

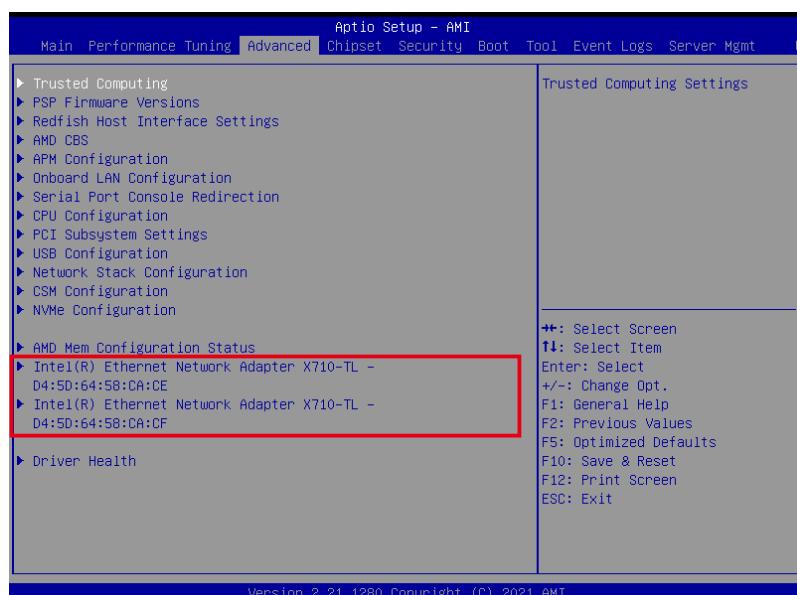
## 4.5.14 AMD Mem Configuration Status

The items in this menu display the memory configuration (initialized by ABL) status.



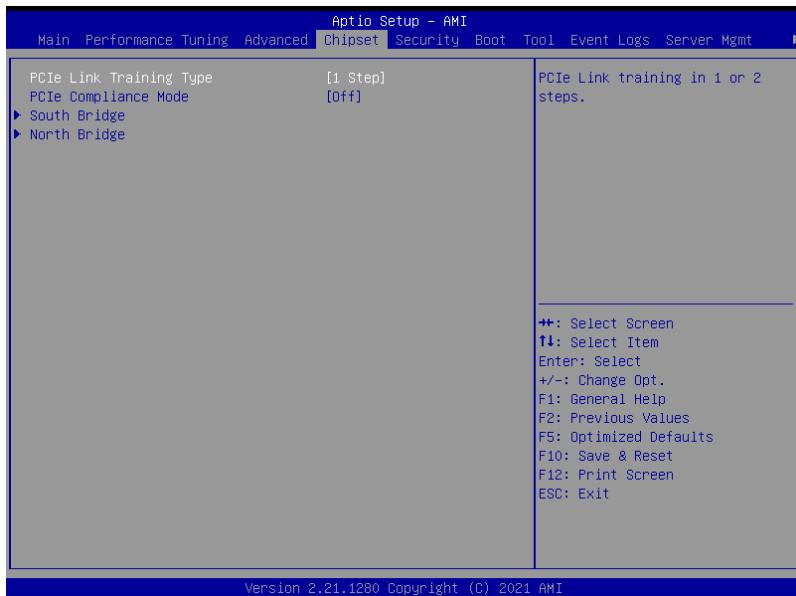
## 4.5.15 Third-party UEFI driver configurations

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



## 4.6 Chipset menu

The Chipset menu items allow you to change the Chipset settings.



### PCIe Link Training Type [1 Step]

Allows you to select PCIe Link Training in 1 or 2 steps.

Configuration options: [1 Step] [2 Step]

### PCIe Compliance Mode [Off]

Allows you to turn the PCIe Compliance Mode on or off.

#### South Bridge

##### SB Debug Configuration

###### SB SATA DEBUG Configuration

The items in this submenu contains options for SATA DEBUG Configuration.

###### **Aggressive Link PM Capability [Enabled]**

Indicates whether Host Bus Adapter (HBA) can support Auto-generating Link Requests to the partial or slumber states when there are no commands to process.

Configuration options: [Disabled] [Enabled]

###### **Port Multiplier Capability [Enabled]**

Indicates whether Host Bus Adapter (HBA) can support a port multiplier.

Configuration options: [Disabled] [Enabled]

###### **SATA Ports Auto Clock Control [Enabled]**

Allows you to enable or disable SATA Ports Auto Clock Control.

Configuration options: [Disabled] [Enabled]

**SATA Partial State Capability [Enabled]**

Indicates whether Host Bus Adapter (HBA) can support transitions to the partial state.

Configuration options: [Disabled] [Enabled]

**SATA FIS Based Switching [Enabled]**

Indicates whether Host Bus Adapter (HBA) can support port multiplier FIS-based switching.

Configuration options: [Disabled] [Enabled]

**SATA Command Completion Coalescing Support [Disabled]**

Indicates whether Host Bus Adapter (HBA) can support command completion coalescing.

Configuration options: [Disabled] [Enabled]

**SATA Slumber State Capability [Enabled]**

Indicates whether Host Bus Adapter (HBA) can support transitions to the slumber state.

Configuration options: [Disabled] [Enabled]

**SATA Target Support 8 Devices [Disabled]**

Indicates whether SATA target support 8 devices function.

Configuration options: [Disabled] [Enabled]

**Generic Mode [Disabled]**

Allows you to SATA disable Generic Mode.

Configuration options: [Disabled] [Enabled]

**SATA AHCI Enclosure [Disabled]**

Allows you to enable or disable SATA AHCI Enclosure Management.

Configuration options: [Disabled] [Enabled]

**SATA SGPIO 0 [Disabled]**

Allows you to enable or disable SATA Serial General Purpose Input/Output (SGPIO) 0.

Configuration options: [Disabled] [Enabled]

**SB FUSION DEBUG Configuration**

The items in this submenu contains options for SB FUSION DEBUG Configuration.

**TimerTick Tracking [Disabled]**

Configuration options: [Disabled] [Enabled]

**Clock Interrupt Tag [Disabled]**

Configuration options: [Disabled] [Enabled]

**SB MISC DEBUG Configuration**

The items in this submenu contains options for SB DEBUG Configuration.

**SB Clock Spread Spectrum [Enabled]**

Allows you to enable or disable CG1\_PLL Spread Spectrum.

Configuration options: [Disabled] [Enabled]

**HPET In SB [Enabled]**

Allows you to enable or disable the HPET Function Switch.

Configuration options: [Disabled] [Enabled]

**MsiDis in HPET [Enabled]**

Expose MSI capability in HPET Capability register.

Configuration options: [Disabled] [Enabled]

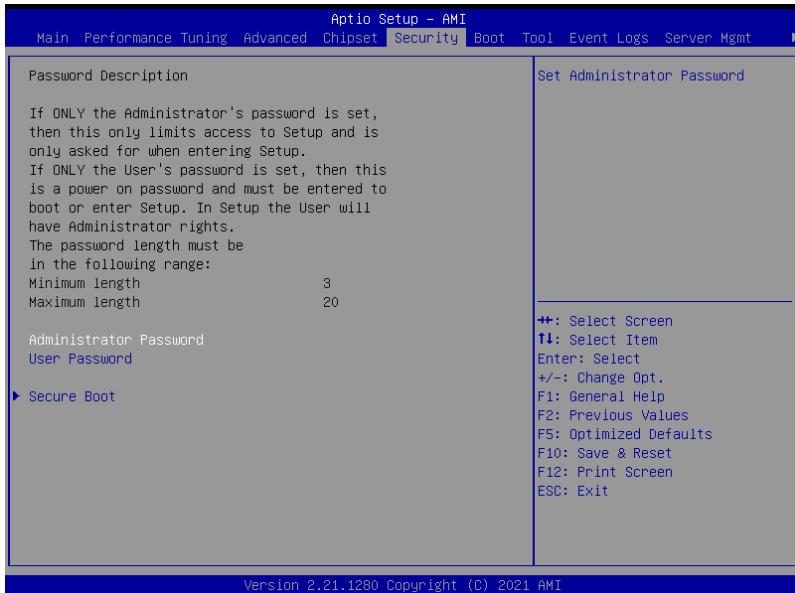
## North Bridge

### Socket 0 Information

This item displays the memory information on Socket 0.

## 4.7 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>.

## Secure Boot

Allows you to customize the Secure Boot settings.

Aptio Setup - AMI		
Security		
System Mode	User	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
Secure Boot	[Disabled] Not Active	
Secure Boot Mode	[Custom]	
▶ Restore Factory Keys		
▶ Reset To Setup Mode		

### Secure Boot [Disabled]

Secure Boot feature is Active if Secure Boot is set to **[Enabled]**, Platform Key(PK) is enrolled, and the system is in User mode. A mode change requires a 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 by a physically present user without fill authentication.

Configuration options: **[Custom]** **[Standard]**



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

## Restore Factory Keys

This option will force the system to User Mode, and install factory default Secure Boot key databases.

## Reset to Setup Mode

This option will delete all Secure Boot key databases from NVRAM.

## Key Management

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

Aptio Setup - AMI			
Security			
Vendor Keys	Valid		Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode
Factory Key Provision	[Enabled]		
▶ Restore Factory Keys			++: Select Screen
▶ Reset To Setup Mode			!1: Select Item
▶ Export Secure Boot variables			Enter: Select
▶ Enroll Efi Image			+/-: Change Opt.
Device Guard Ready			F1: General Help
▶ Remove 'UEFI CA' from DB			F2: Previous Values
▶ Restore DB defaults			F5: Optimized Defaults
Secure Boot variable   Size  Keys  Key Source			
▶ Platform Key(PK)   886  1  Factory			
▶ Key Exchange Keys   3573  3  Factory			
▶ Authorized Signatures  6322  10  Factory			
▶ Forbidden Signatures  3724  77  Factory			
▶ 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]

### Restore Factory Keys

This item will install all Factory Default keys.

### Reset to Setup Mode

This item appears only when you load the default Secure Boot keys. Allows you to clear all default Secure Boot keys.

### Export Secure Boot Variables

This item will ask you if you want to save all secure boot variables. Select Yes if you want to save all secure boot variables, otherwise select No.

### Enroll Efi Image

This item will allow the image to run in Secure Boot mode.

Configuration options: [Set New] [Append]

### 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.

#### Platform Key (PK)

Configuration options: [Details] [Export] [Update] [Delete]

#### Key Exchange Keys (KEK) / Authorized Signatures (DB) / Forbidden Signatures (DBX)

Configuration options: [Details] [Export] [Update] [Append] [Delete]

#### Authorized TimeStamps (DBT) / OsRecovery Signatures

Configuration options: [Update] [Append]

## 4.8 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 <F8> when ASUS Logo appears.
- To access Windows OS in Safe Mode, please press <F8> after POST.

---

## **POST Report [5 sec]**

Allows you to set the desired POST Report waiting time from 1 to 10 seconds.

Configuration options: [1 sec] - [10 sec] [Until Press ESC]

## 4.9 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 run the ASUS SMBIOS Viewer

## 4.10 Event Logs menu

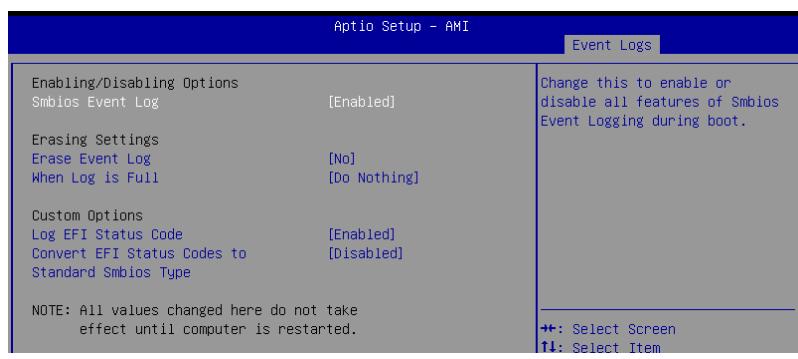
The Event Logs menu items allow you to change the event log settings and view the system event logs.



Version 2.21.1280 Copyright (C) 2021 AMI

### 4.10.1 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 appear only 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]

This option allows you to enable or disable logging of the EFI Status Codes.  
Configuration options: [Disabled] [Enabled]



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

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

This option allows you to enable or disable converting of EFI Status Codes to Standard Smbios Type (Not all may be translated).  
Configuration options: [Disabled] [Enabled]

## 4.10.2 View Smbios Event Log

Press <Enter> to view all smbios event logs.

Aptio Setup - AMI					Event Logs
DATE	TIME	ERROR CODE	SEVERITY	COUNT	DESCRIPTION
07/20/21	15:59:54	Smbios 0x16	N/A	N/A	Log Area Reset and Count is applicable only for Multi-Events
08/05/21	18:29:11	EFI 03051002	Major	01	

## 4.11 Server Mgmt menu

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



### OS Watchdog Timer [Disabled]

Allows you to start a BIOS timer which can only be shut off by Intel Management Software after the OS loads.

Configuration options: [Disabled] [Enabled]



---

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

---

### OS Wtd Timer Timeout [10]

Allows you to set the time in minutes for the OS Boot Watchdog Timer Expiration. Not available if OS Boot Watchdog Timer is disabled.

Configuration options: [1] - [30]

### OS Wtd Timer Policy [Reset]

Allows you to configure the how the system should respond if the OS Boot Watchdog Timer expires. Not available if OS Boot Watchdog Timer is disabled.

Configuration options: [Do Nothing] [Reset] [Power Down]

## 4.11.1 System Event Log

Allows you to change the SEL event log configuration.

Optio Setup - AMI

Server Mgmt

Erasing Settings Erase SEL [No]  NOTE: All values changed here do not take effect until computer is restarted.	Choose options for erasing SEL.
---	---------------------------------

### Erase SEL [No]

Allows you to choose options for erasing SEL.

Configuration options: [No] [Yes, On next reset] [Yes, On every reset]



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

## 4.11.2 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.

Optio Setup - AMI

Server Mgmt

--BMC network configuration-- ***** Configure IPv4 support *****		▲ Select to configure LAN channel parameters statically or dynamically(by BIOS or BMC). Previous State option will not modify any BMC network parameters during BIOS phase
DM_LAN1 Configuration Address source [Previous State] Current Config Address source DHCP Mode Station IP address 0.0.0.0 Subnet mask 0.0.0.0 MAC Address in BMC : 00-E0-E8-05-04-03 Router IP address 0.0.0.0 Router MAC address 00-00-00-00-00-00		▼ ++: Select Screen !!: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F5: Optimized Defaults F10: Save & Reset F12: Print Screen ESC: Exit
Shared LAN Configuration Address source [Previous State] Current Config Address source DHCP Mode Station IP address 0.0.0.0 Subnet mask 0.0.0.0 MAC Address in BMC : 00-E0-E8-05-04-04 Router IP address 0.0.0.0 Router MAC address 00-00-00-00-00-00		
***** Configure IPv6 support		

## Configure IPV4 support

### DM\_LAN1 / Shared LAN

#### Configuration Address source [Previous State]

Allows you to configure LAN channel parameters statistically or dynamically (by BIOS or 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

#### IPV6 Support [Enabled]

Allows you to enable or disable LAN1 IPV6 Support.

Configuration options: [Disabled] [Enabled]



---

The following item appears only when **IPV6 Support** is set to **[Enabled]**.

---

#### Configuration Address source [Previous State]

Allows you to configure LAN channel parameters statistically or dynamically (by BIOS or 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 Address source [Previous State]

Select to configure LAN channel parameters statically or dynamically (by BIOS or by BMC). Unspecified option will not modify any BMC network parameters during BIOS phase.



The following items are available only when Configuration Router Lan1 Address source is set to [Static].

### IPv6 Router1 IP address

Allows you to change the IPv6 Router1 IP Address.

### IPv6 Router1 Prefix Length Lan1

Allows you to change the IPv6 Router Prefix Length.

### IPv6 Router1 Prefix Value Lan1

Allows you to change the IPv6 Router Prefix Value.

## Shared LAN

### IPV6 Support [Enabled]

Allows you to enable or disable LAN1 IPV6 Support.

Configuration options: [Disabled] [Enabled]



The following item appears only when IPV6 Support is set to [Enabled].

## Configuration Address source [Previous State]

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

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

### 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 Lan2 Address source [Previous State]

Select to configure LAN channel parameters statically or dynamically (by BIOS or by BMC). Unspecified option will not modify any BMC network parameters during BIOS phase.



The following items are available only when Configuration Router Lan2 Address source is set to [Static].

### IPv6 Router1 IP address

Allows you to change the IPv6 Router1 IP Address.

### IPv6 Router1 Prefix Length Lan2

Allows you to change the IPv6 Router Prefix Length.

## IPv6 Router1 Prefix Value Lan2

Allows you to change the IPv6 Router Prefix Value.

### 4.11.3 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 : 4				
DATE	TIME	SENSOR	TYPE	HEX:
08/05/21	19:08:18	Temperature		01 00 02 22 37 0C
08/05/21	19:08:59	Temperature		61 20 00 04 01 01
08/05/21	19:11:50	Temperature		01 57 59 59
08/05/21	19:12:11	Temperature		Generator ID: BMC - LUN #0 (Channel #0) Sensor Number: 0x01 CPU1 Temperature Event Description: Record Type-0x02. Assertion Event.

## 4.12 Exit menu

The 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.

## **Launch EFI Shell from USB drives**

Allows you to attempt to launch the EFI Shell application (shellx64.efi) from one of the available filesystem devices.



# 5

## Driver Installation

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

## 5.1 Running the Support DVD

The support DVD that is bundled with your motherboard contains drivers, management applications, and utilities that you can install to maximize the features of your motherboard.



The contents of the support DVD are subject to change at any time without notice. Visit the ASUS website ([www.asus.com](http://www.asus.com)) for the latest updates on software and utilities.

The main screen of the Support DVD contains the following tabs:

1. Drivers - Shows the available device drivers that the system detects.
2. Utilities - Displays the software applications and utilities that the motherboard supports.
3. Manual - Provides the link to the user guide(s).

---

A small, stylized icon of a quill pen, pointing downwards, used as a bullet point or decorative element.

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

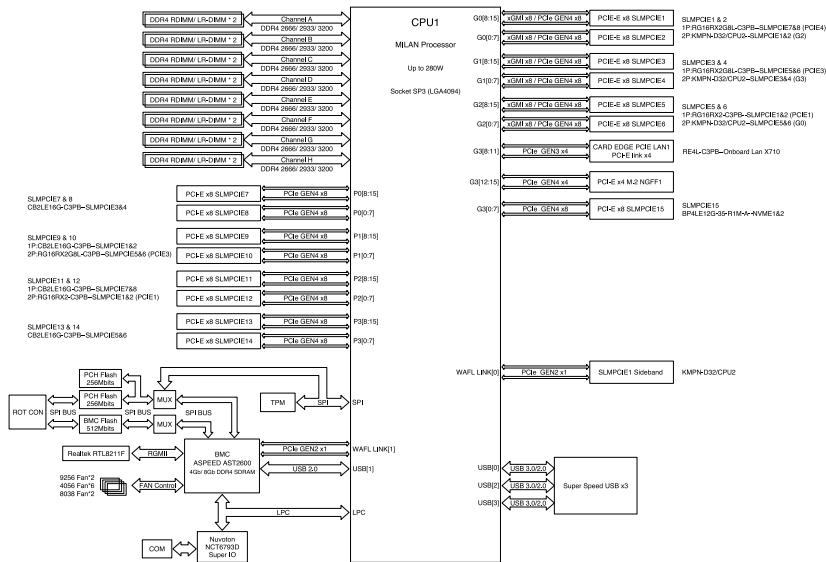
---

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.

# KMPN-U16 block diagram



## Notices

### Federal Communications Commission Statement

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

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

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



---

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

---

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

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

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

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

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

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

### Japan JATE

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

## Australia statement notice

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

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



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



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

## 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.

## **Turkey RoHS**

AEEE Yönetmeliğine Uygundur

## **ASUS Recycling/Takeback Services**

ASUS recycling and takeback programs come from our commitment to the highest standards for protecting our environment. We believe in providing solutions for you to be able to responsibly recycle our products, batteries, other components as well as the packaging materials. Please go to <http://csr.asus.com/english/Takeback.htm> for detailed recycling information in different regions.

## **Ecodesign Directive**

European Union announced a framework for the setting of ecodesign requirements for energy-related products (2009/125/EC). Specific Implementing Measures are aimed at improving environmental performance of specific products or across multiple product types. ASUS provides product information on the CSR website. The further information could be found at <https://csr.asus.com/english/article.aspx?id=1555>.

## **Service and Support**

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



