ESC8000A-E13P

4U Rackmount Server

User Guide

E25098
First Edition
December 2024

Contents

Contents

Contents

Chapter 4: BIOS Setup

Contents

Appendix

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.

CAUTION: 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 Area

This equipment should only be installed in a Restricted Access Area where both these conditions apply:

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

Heavy System

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

Shock Hazard

CAUTION! Risk of electric shock.
Disconnect all power supply input plugs before servicing.

About this guide

Audience

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

Contents

This guide contains the following parts:

1. **Chapter 1: Product Introduction**

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

2. **Chapter 2: Hardware Setup**

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

3. **Chapter 3: Motherboard Information**

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

4. **Chapter 4: BIOS Setup**

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

Conventions

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

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

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

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

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

Typography

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

References

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

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

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

2. **ASUS websites**

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

1 Product Introduction

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

1.1 System package contents

Check your system package for the following items.

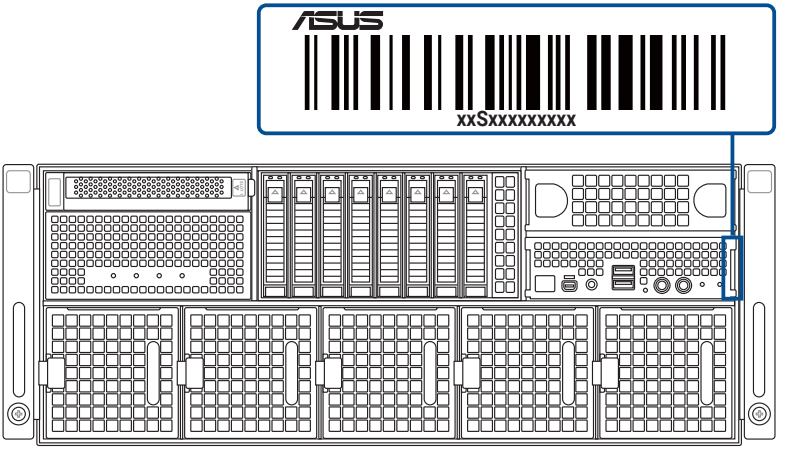
	ESC8000A-E13P
Chassis	ASUS 4U rackmount chassis
Motherboard	ASUS K15PG-D24 server board
Accessories	1 x ASMB12 instruction card 1 x ASUS Control Center instruction card 4 x AC power cables 2 x CPU heatsinks 1 x Foam padding for NVIDIA® H200 GPUs 8 x GPU brackets 1 x Set of GPU screws
Optional items	1 x Rail kit 1 x Broadcom HBA card cable kit 1 x Cable arm

NOTE:

- 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

When requesting support from the ASUS Technical Support Team, provide the product's serial number. The serial number has 12 characters, such as xxSxxxxxxxxx, and is printed on the asset tag. Refer to the below illustration for the location of the asset tag.



1.3 System specifications

The ASUS ESC8000A-E13P server features the ASUS K15PG-D24 server board designed for AMD EPYC™ 9005 series processors.

Model name		ESC8000A-E13P
Motherboard		K15PG-D24
Processor support		2 x Socket SP5 (LGA 6096) for AMD EPYC™ 9005 series processors* * **Up to 500W TDP at an operating temperature of 25°C**
Core logic		System on Chip (SoC)
Memory	Total slots	24 (12 channels per CPU, 12 DIMMs per CPU)
	Capacity	Maximum up to 3TB per CPU socket
	Memory type	DDR5 6400**/6000/5600 RDIMM * **Refer to ASUS server AVL for the latest update** ** **DDR5 6400 support expected in Q1 2025**
	Memory size	128GB, 64GB, 32GB * **Refer to ASUS server AVL for the latest update**
Expansion slots	Total PCIe slots	Up to 14 slots
	PCIe slot type	**Rear:** - 8 x PCIe x16 for dual-slot GPU cards (Gen5 x16 link, FH/FL) - 5 x PCIe x16 for NIC/BlueField-3 cards (Gen5 x16 link, FH/HL) **Front:** - 1 x PCIe x8 (Gen5 x8 link, FH/HL)
	M.2	2 x M.2 socket (Gen5 x4 link, up to 22110) for 2x NVMe devices
Storage	NVMe controller	CPU integrated to support up to 8 NVMe devices
	Storage bays	8 x 2.5" front hot-swap storage bays for 8x NMVe devices
	Connectors	**Backplane:** - 4 x MCIO connectors (x8 link) for NVMe devices - 2 x SLIMSAS connectors (x4 link) for HBA cards only **PCIe switch:** - 4 x MCIO connectors (x8 link) for NVMe devices
	Default cables	4 x Backplane MCIO cables
Networking		1 x Dual Port Intel® X710-AT2 10GbE LAN controller 1 x Management port
Onboard graphics		Aspeed AST2600 64MB (Mini DisplayPort)
Graphics card support		Up to 8 dual-slot GPU cards * **Supports 12VHPWR power connectors by default**
Front I/O ports		1 x Mini DisplayPort 2 x USB 5Gbps ports
Rear I/O ports		1 x USB 5Gbps port 2 x RJ-45 LAN ports 1 x RJ-45 management LAN port

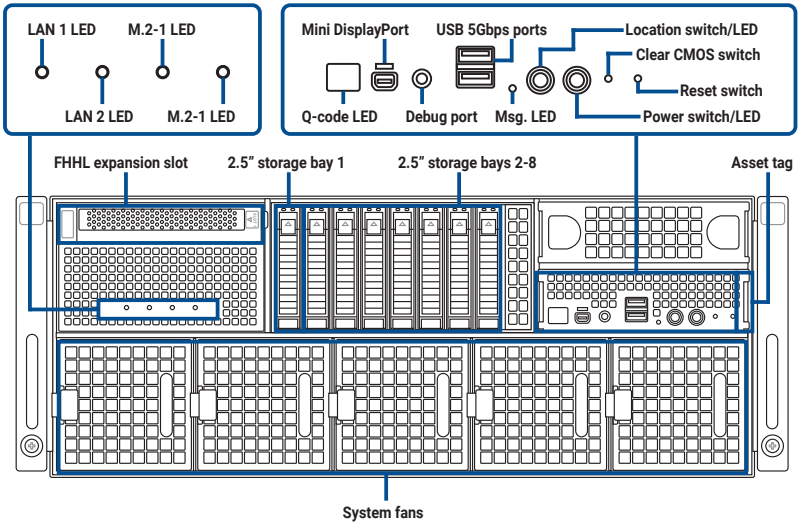
(continued on the next page)

Model name	ESC8000A-E13P	
Switch/LEDs	**Front:** 1 x Power switch/LED 1 x Location switch/LED 1 x Message LED 1 x Clear CMOS switch 1 x Reset switch 2 x M.2 LEDs 2 x LAN LEDs 1 x Q-Code/Port 80 LED	**Rear:** 1 x Power switch/LED 1 x Location switch/LED 1 x Message LED
OS support	Windows® Server, RedHat® Enterprise Linux, SuSE® Linux Enterprise Server, CentOS, Ubuntu, VMware * **Refer to https://servers.asus.com/support/os for the latest supported OS list**	
Management solutions	**Hardware (Out-of-band remote management):** Onboard ASMB12-iKVM **Software:** ASUS Control Center	
Regulatory compliance	BSMI, CB, CE, FCC (Class A), RCM	
Dimensions (HH x WW x DD)	800mm x 439.5mm x 175mm / 31.5” x 17.3” x 6.9” (4U)	
Net weight	42kg	
Gross weight	44.23kg	
Power supply and rating	3+1 redundant 3200W 80 PLUS Titanium power supply 220-240 Vac, 16A (x4) 50/60Hz	
Environment	Operating temperature: 10°C ~ 35°C Non-operating temperature: -40°C ~ 60°C Non-operating humidity: 20% ~ 95% (Non-condensing)	

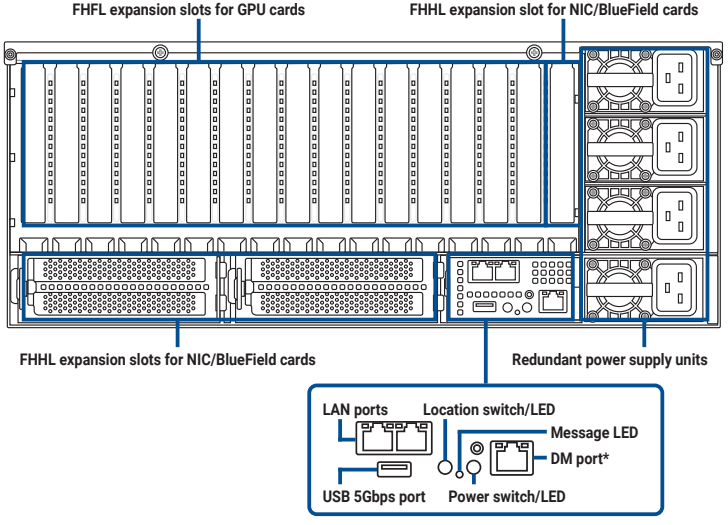
NOTE:

- Specifications are subject to change without notice.
- Refer to www.asus.com for the latest OS AVL update.

1.4 Front panel features

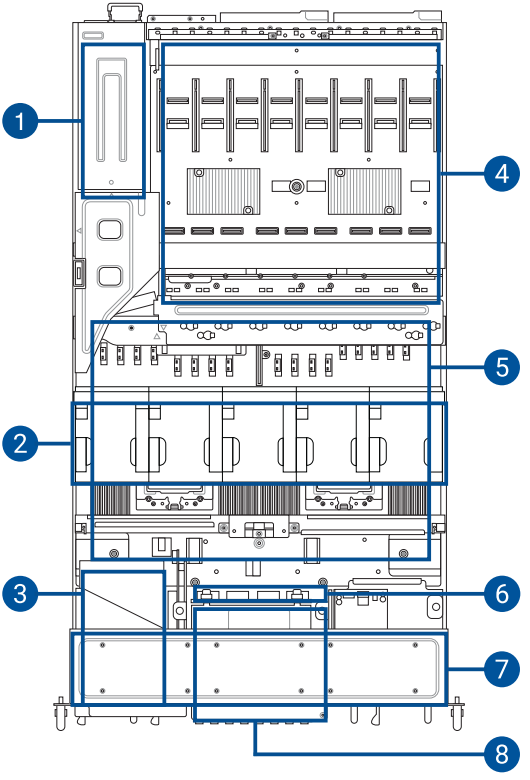


1.5 Rear panel features



NOTE: The DM (Dedicated Management) port is for ASUS ASMB12-iKVM only.

1.6 Internal features



1. Redundant power supply units
2. GPU fans
3. FHHL expansion slot
4. FHFL expansion slots for GPU cards
5. Motherboard
6. Storage device backplane
7. System fans
8. 2.5” storage bays

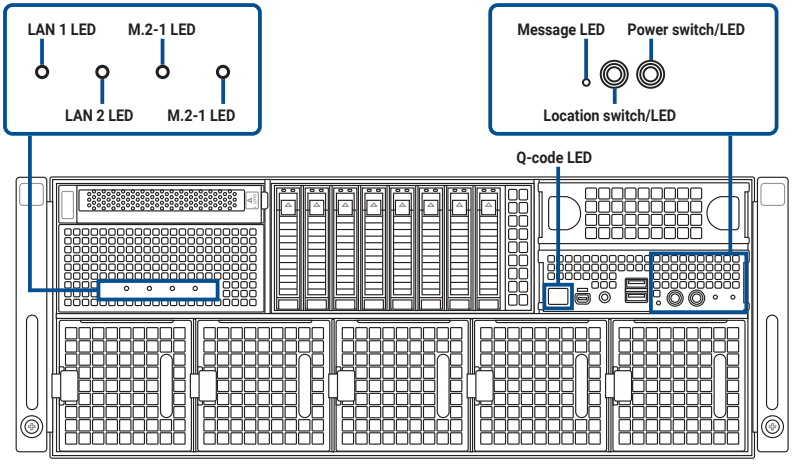
NOTE:

- A protective film is pre-attached to the front cover before shipping. Remove the protective film before turning on the system for sufficient heat dissipation.
- The barebone server does not include a floppy disk drive or an optical drive. Connect a USB floppy disk drive to any of the USB ports on the front or rear panel if you need to use a floppy disk.

WARNING
HAZARDOUS MOVING PARTS
KEEP FINGERS AND OTHER BODY PARTS AWAY

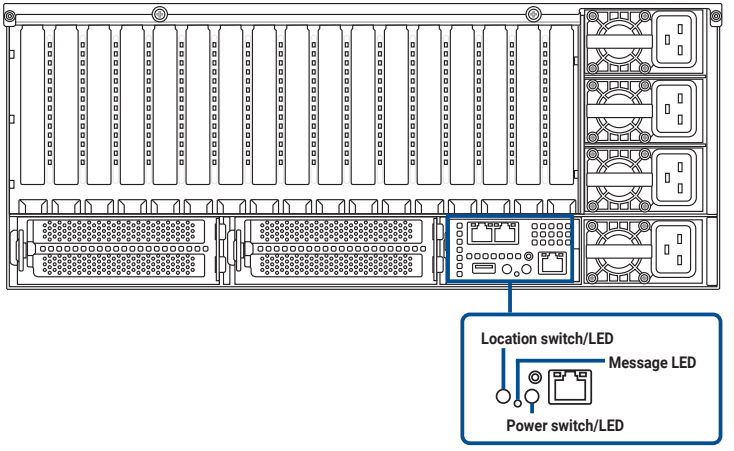
1.7 LED information

1.7.1 Front panel LEDs



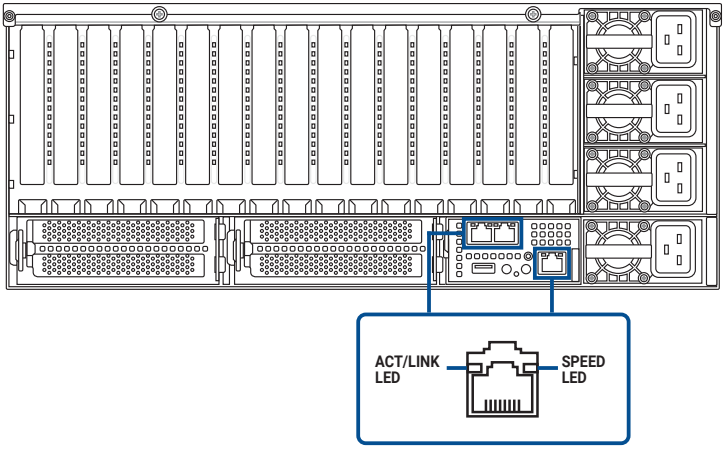
LED	Status	Description
Power switch/LED	ON	System power on
Location switch/LED	ON	Received user command to locate the system
	OFF	Function off
LAN LEDs	Blinking	LAN is transmitting or receiving data
	OFF	No LAN connection
Message LED	ON	A hardware monitor event is indicated
	OFF	System is normal; no incoming event
M.2 LEDs	Blinking	M.2 storage device reading or writing data

1.7.2 Rear panel LEDs



LED	Status	Description
Power switch/LED	ON	System power on
Location switch/LED	ON	Received user command to locate the system
	OFF	Function off
Message LED	ON	A hardware monitor event is indicated
	OFF	System is normal; no incoming event

1.7.3 LAN (RJ-45) LEDs



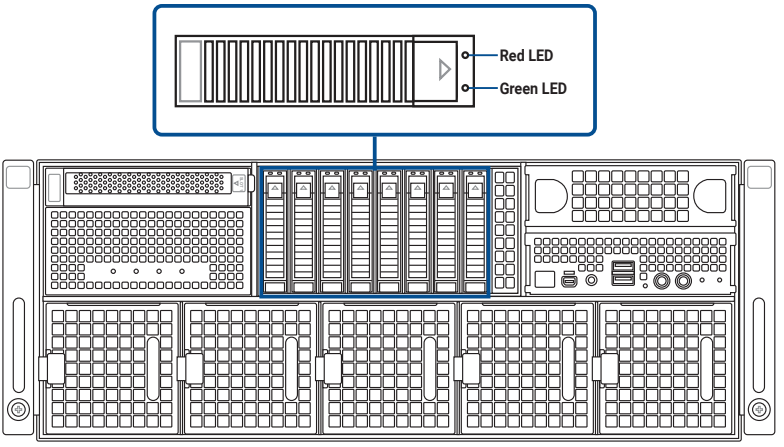
Intel® X710-AT2 10GbE LAN port LEDs

SPEED LED		ACT/LINK LED	
Status	Description	Status	Description
OFF	100 Mbps connection	OFF	No link
ORANGE	1-5 Gbps connection	GREEN	Linked
GREEN	10 Gbps connection	BLINKING	Data activity

Dedicated Management LAN port (DM_LAN1) LEDs

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

1.7.4 Storage device status LEDs



Storage Device LED Description		
Status (RED)	ON	Storage device has failed
	Blinking	RAID rebuilding or locating
Activity (GREEN)	ON	Storage device power ON
	Blinking	Storage device reading or writing data
	OFF	Storage device not found

Hardware Setup

2

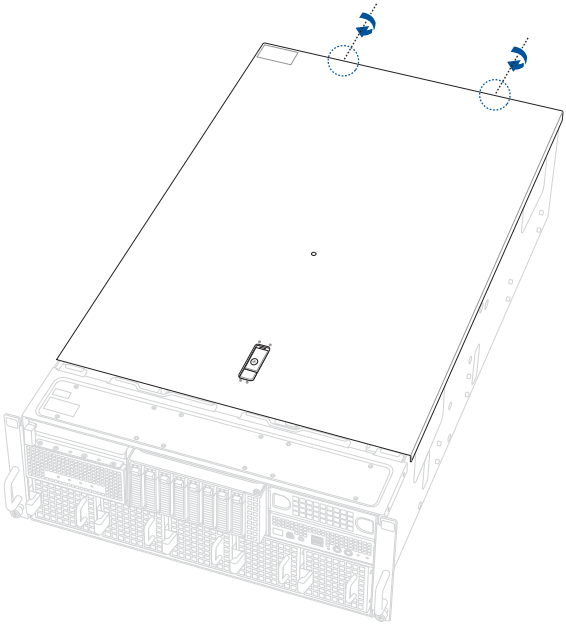
This chapter lists the hardware setup procedures that you have to perform when installing or removing system components.

2.1 Chassis cover

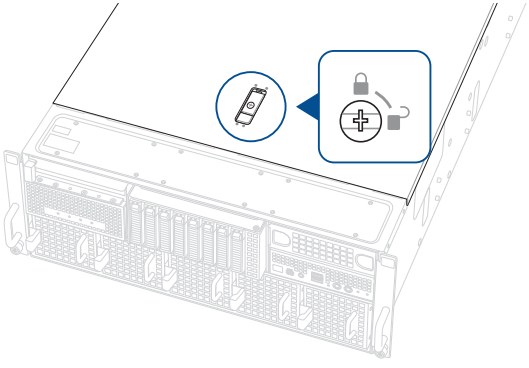
NOTE: A protective film is pre-attached to the system cover before shipping. Remove the protective film before turning on the system for proper heat dissipation.

2.1.1 Removing the rear cover

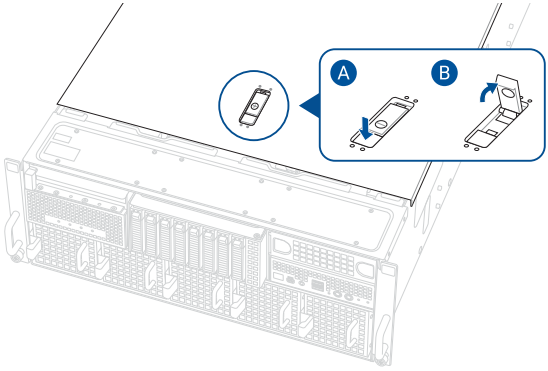
1. Loosen the thumbscrews.



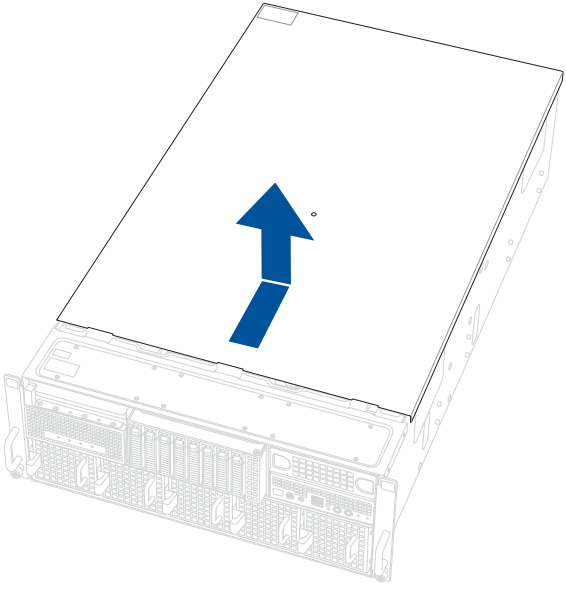
2. Turn the screw clockwise to unlock the latch.



3. Press the spring lock to release the latch, then pull the latch upwards to disengage the chassis cover from the chassis.

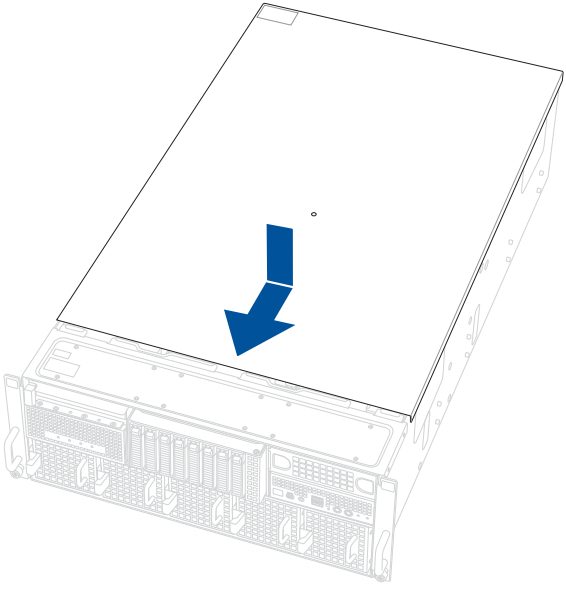


4. Slide the chassis cover towards the rear of the chassis, then lift and remove it from the chassis.

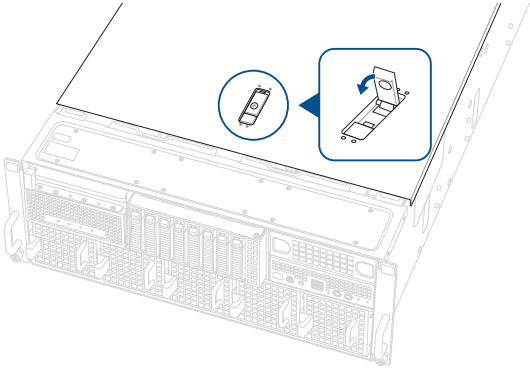


2.1.2 Installing the chassis cover

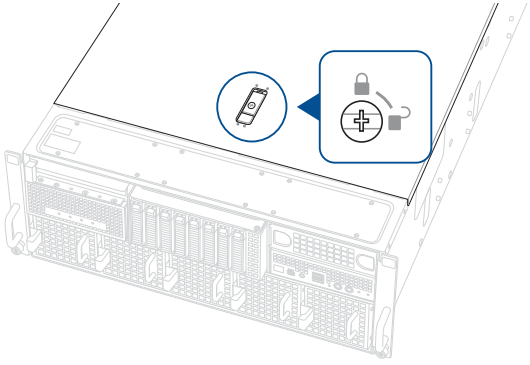
1. Place the chassis cover onto the chassis, then slide the chassis cover towards the front of the chassis.



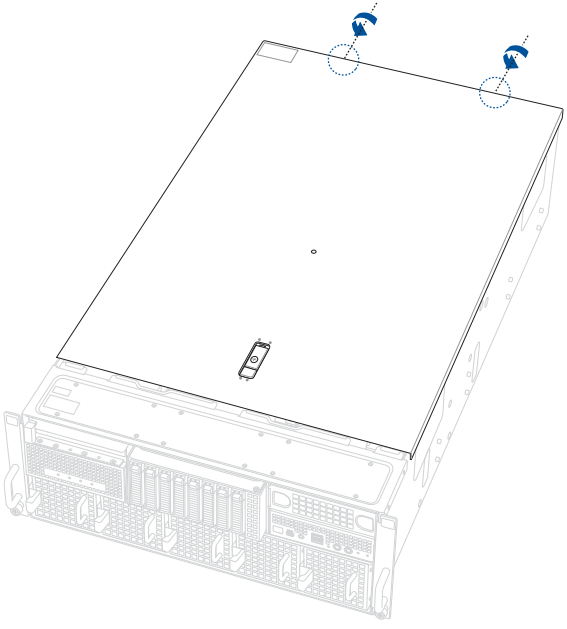
2. Push the latch downwards to lock the chassis cover into place.



3. Turn the screw counter-clockwise to lock the latch.



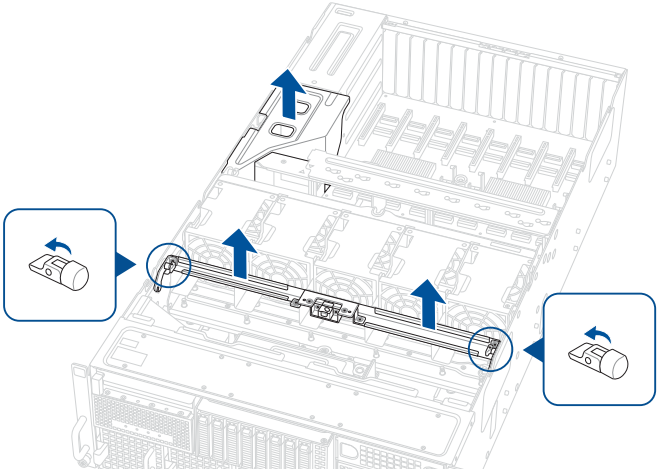
4. Tighten the thumbscrews.



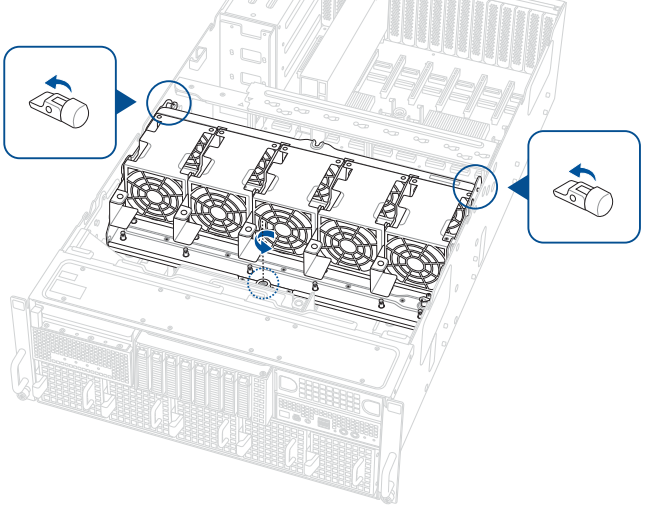
2.2 Air duct

2.2.1 Removing the air duct

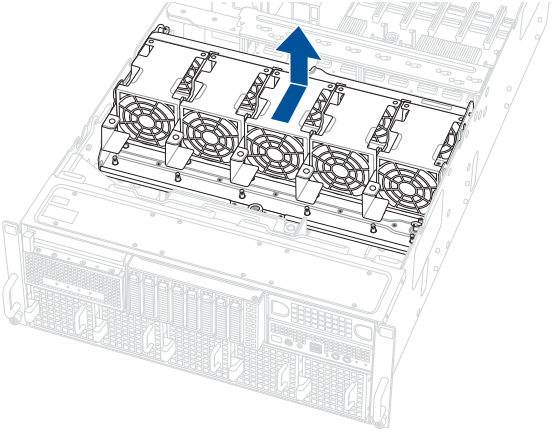
1. Disengage the latches, then remove the metal brackets.



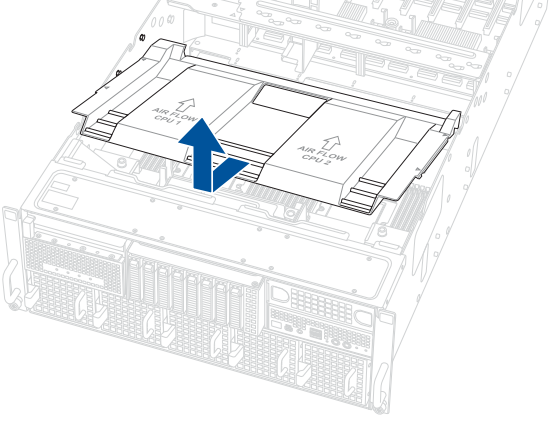
2. Disconnect the cables connected to the GPU fan cage.
3. Disengage the latch and loosen the thumbscrew.



4. Push the GPU fan cage towards the rear of the chassis, then lift and remove the GPU fan cage.



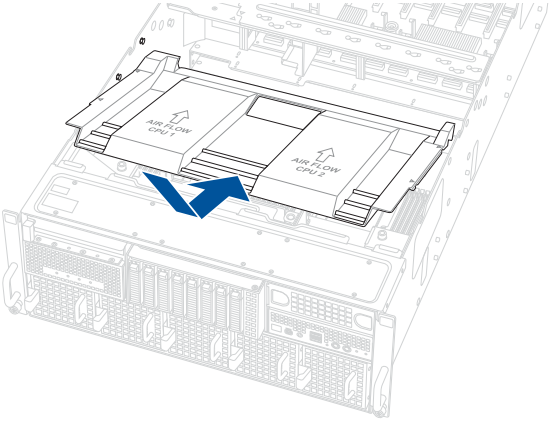
5. Lift and remove the air duct.



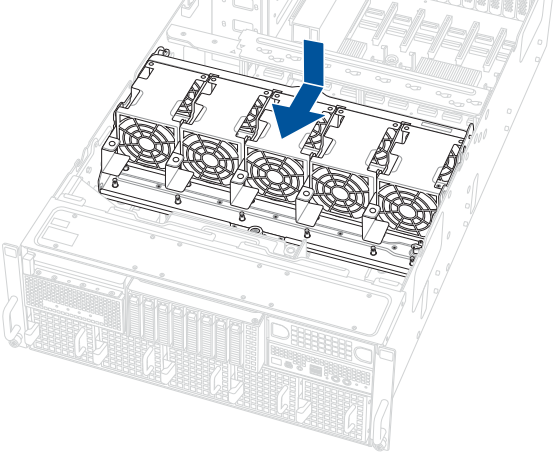
2.2.2 Installing the air duct

1. Align and install the air duct.

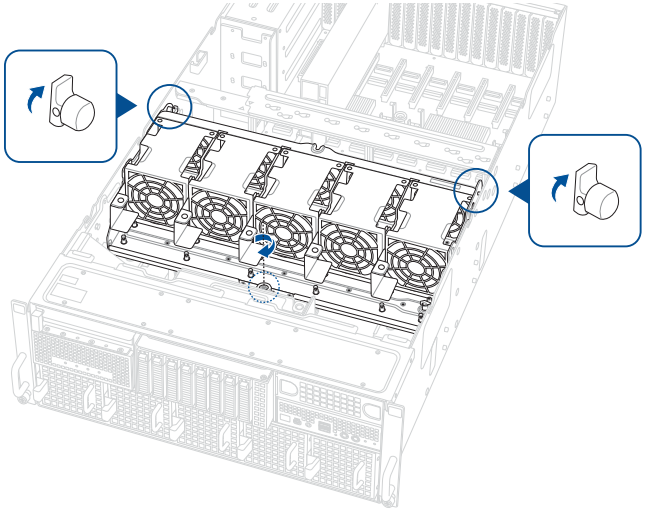
NOTE: Ensure that the triangle marks on the air duct are aligned with the triangle marks on the chassis.



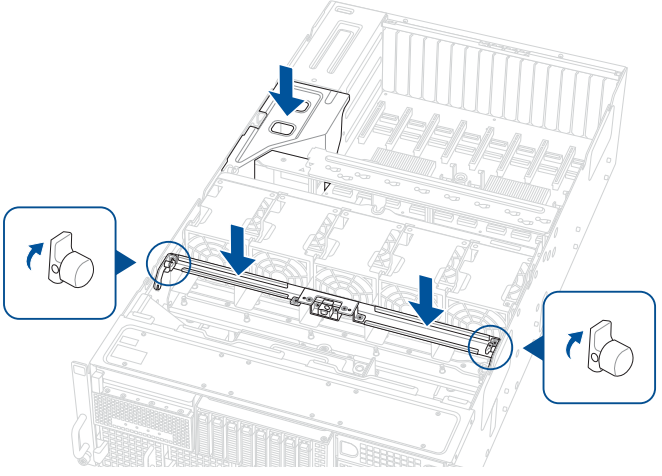
2. Install the GPU fan cage.



3. Return the latch to the locked position and tighten the thumbscrew.
4. Reconnect the cables to the GPU fan cage.



5. Install the metal brackets, then return the latches to the locked position.

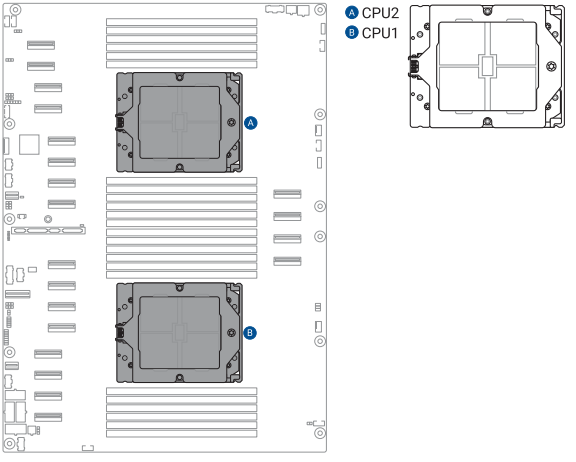


2.3 Central Processing Unit (CPU)

The motherboard comes with two surface mount Socket SP5 sockets designed for AMD EPYC™ 9005 series processors.

CAUTION:

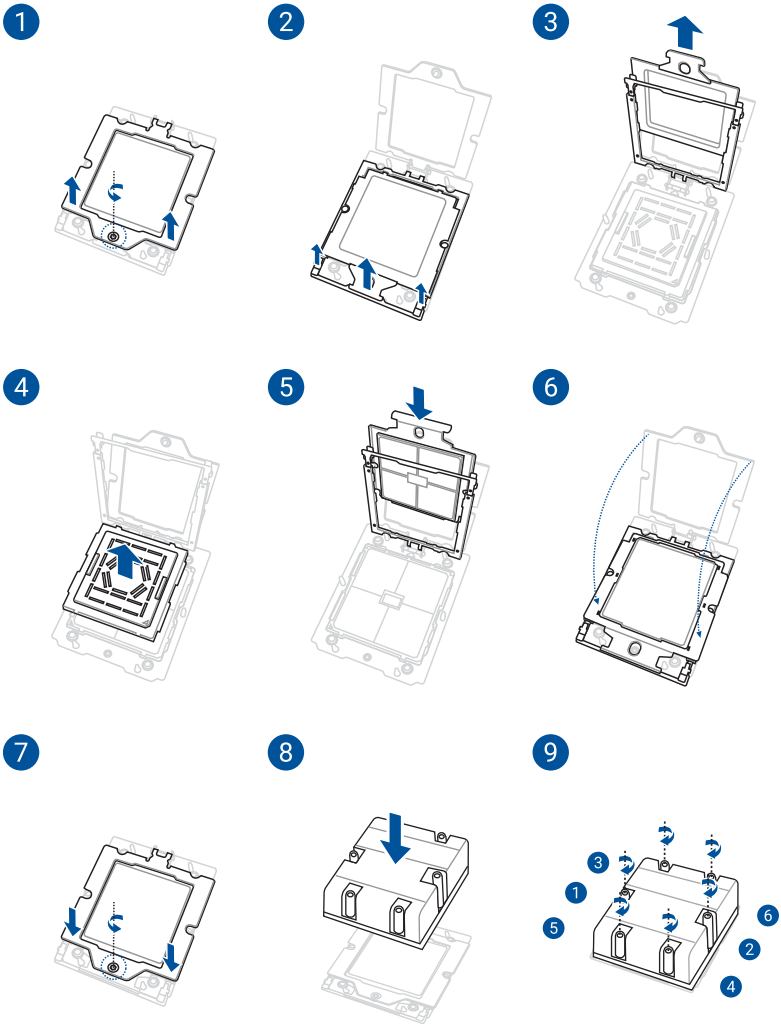
- Upon purchase of the motherboard, ensure that the PnP cap is on the socket and the socket contacts are not bent. Contact your retailer immediately if the PnP cap is missing, or if you see any damage to the PnP cap/socket contacts/motherboard components. ASUS will shoulder the cost of repair only if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



2.3.1 Installing the CPU and heatsink

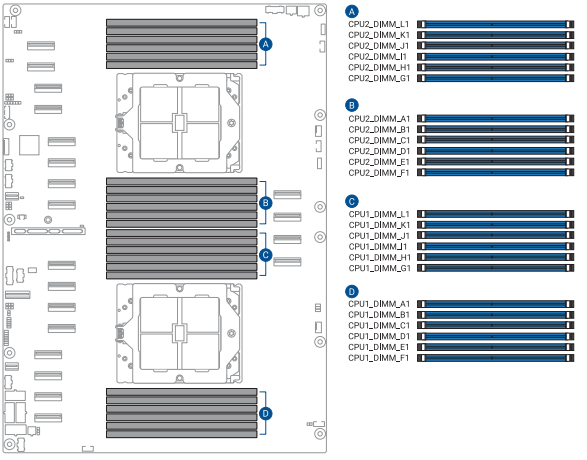
NOTE:

- A T20 screwdriver with a torque value of 13.5±1.0 kgf-cm is recommended.
- When securing the heatsink, partially tighten each of the six screws just enough to attach the heatsink to the motherboard. After all six screws are partially tightened, fully tighten each screw one by one.
- To remove this component, follow the instructions in reverse order.



2.4 System memory

The motherboard comes with twenty four (24) Double Data Rate 5 (DDR5) Dual Inline Memory Modules (DIMM) sockets.



2.4.1 Memory configurations

NOTE:

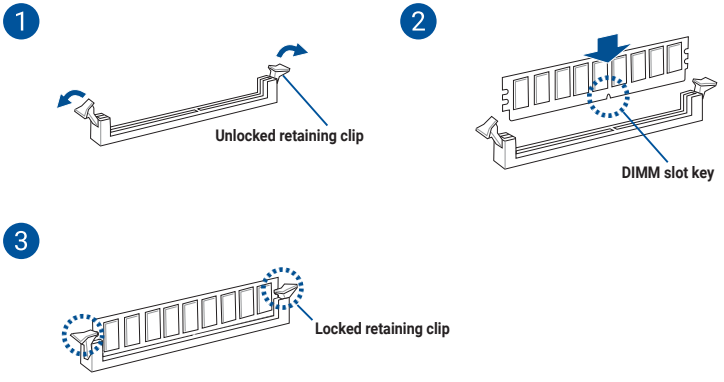
- Refer to ASUS Server AVL for the updated list of compatible DIMMs.
- Always install DIMMs with the same CAS latency. For optimum compatibility, it is recommended that you obtain memory modules from the same vendor.

Recommended dual CPU configuration							
	2 DIMMs	4 DIMMs	8 DIMMs	12 DIMMs	16 DIMMs	20 DIMMs	24 DIMMs
CPU1/CPU2 A1	●	●	●	●	●	●	●
CPU1/CPU2 B1				●	●	●	●
CPU1/CPU2 C1			●	●	●	●	●
CPU1/CPU2 D1						●	●
CPU1/CPU2 E1					●	●	●
CPU1/CPU2 F1							●
CPU1/CPU2 G1		●	●	●	●	●	●
CPU1/CPU2 H1				●	●	●	●
CPU1/CPU2 I1			●	●	●	●	●
CPU1/CPU2 J1						●	●
CPU1/CPU2 K1					●	●	●
CPU1/CPU2 L1							●

2.4.2 Installing a DIMM

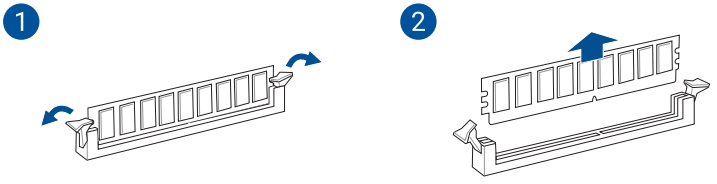
NOTE: A DIMM is keyed with a notch so that it fits in only one direction. DO NOT force a DIMM into a socket in the wrong direction to avoid damaging the DIMM.

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



2.4.3 Removing a DIMM

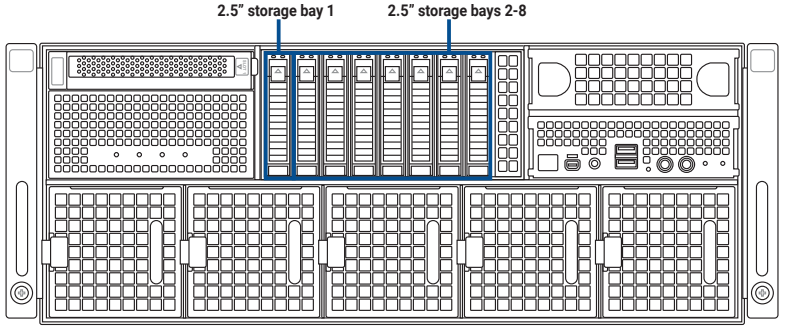
NOTE: Support the DIMM lightly with your fingers when pressing the retaining clips. The DIMM might get damaged when it springs out with extra force.

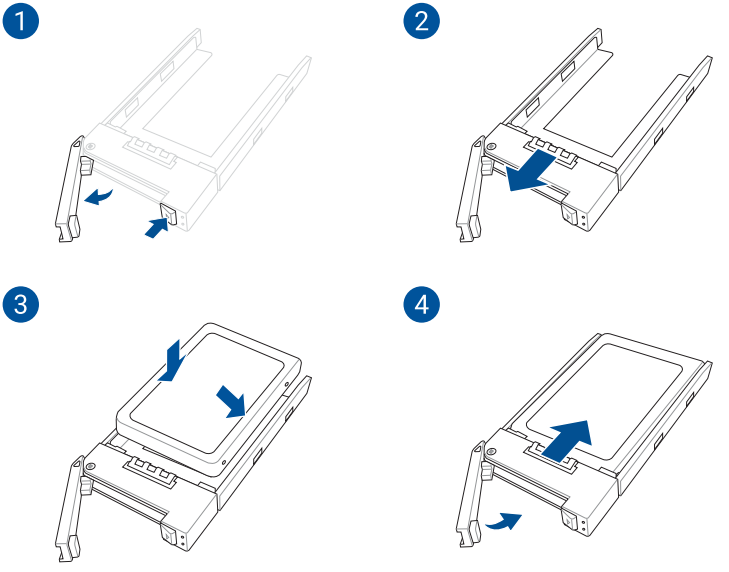


2.5 Storage devices

2.5.1 Installing a 2.5” storage device

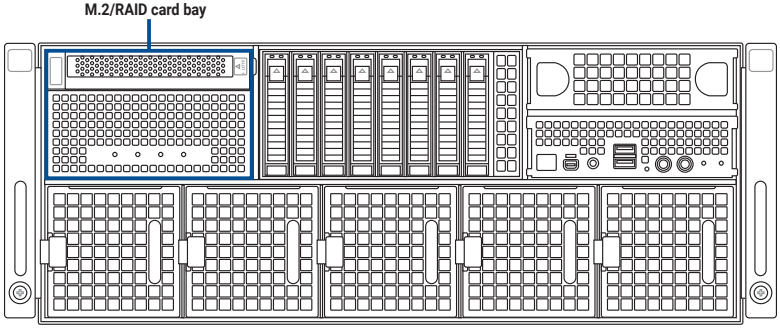
NOTE: To remove this component, follow the instructions in reverse order.



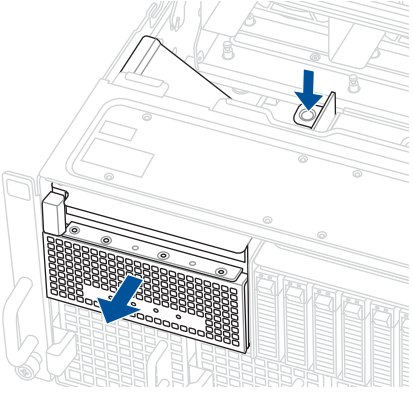


2.5.2 Installing an M.2 SSD module

NOTE: To remove this component, follow the instructions in reverse order.

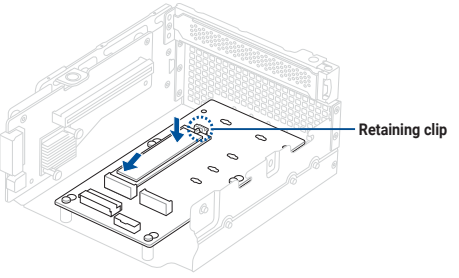


1. Disconnect the cables from the M.2/RAID card bay.
2. Press down on the latch and pull the M.2/RAID card bay out of the chassis.

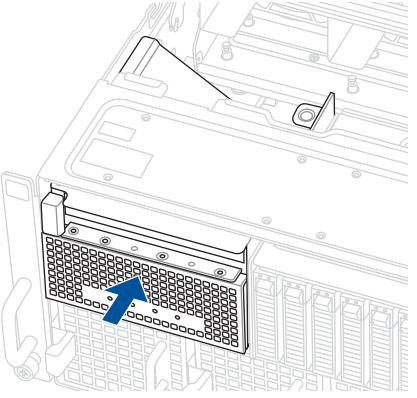


3. Insert the M.2 SSD module into the M.2 slot and push down until the retaining clip locks the M.2 SSD module into place.

NOTE: To install M.2 SSD modules of different lengths, rotate the retaining clip 90 degrees, then remove and install it in a different position. The arrow on the retaining clip should be pointing away from the M.2 slot.



4. Push the M.2/RAID card bay all the way into the chassis.
5. Reconnect the cables to the M.2/RAID card bay.

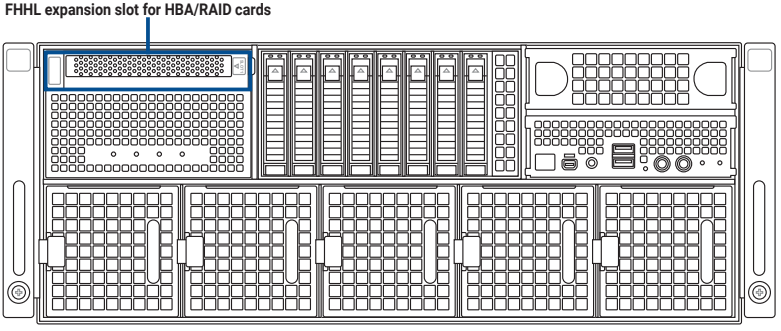


2.6 Expansion slots

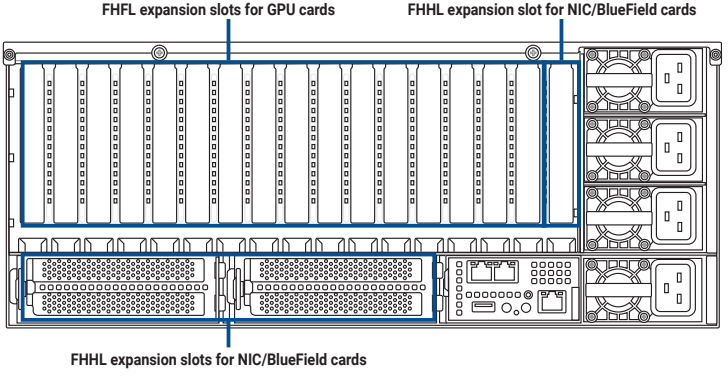
WARNING: Unplug the power cord before adding or removing expansion cards. Failure to do so may cause you physical injury and damage motherboard components.

NOTE: To remove this component, follow the instructions in reverse order.

Front panel



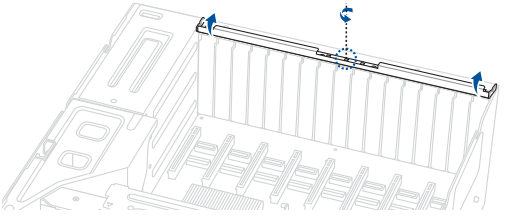
Rear panel



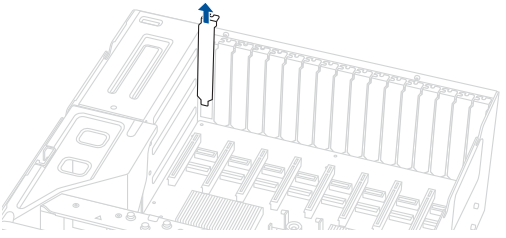
2.6.1 Installing a PCIe expansion card

Upper expansion card slots on the rear panel

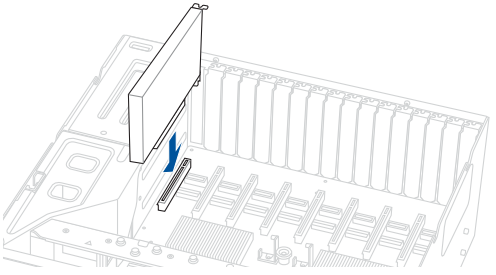
1. Loosen the thumbscrew, then lift the slot cover lock.



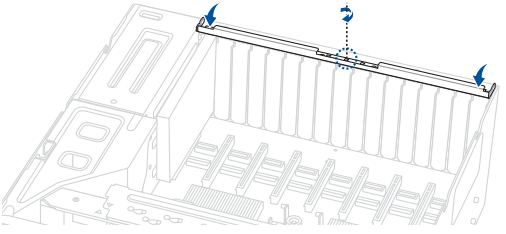
2. Remove the slot cover(s).



3. Install the expansion card.

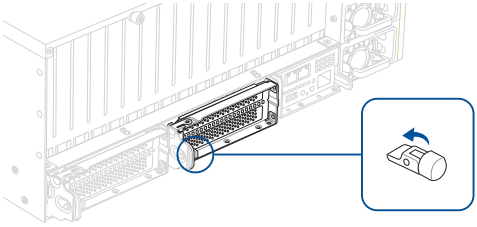


4. Lower the slot cover lock, then tighten the thumbscrew.

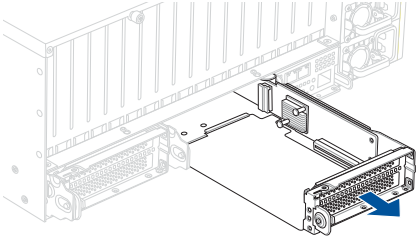


Lower expansion card slots on the rear panel

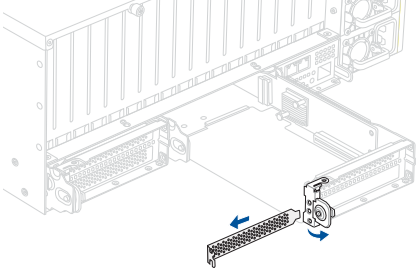
1. Disengage the latch.



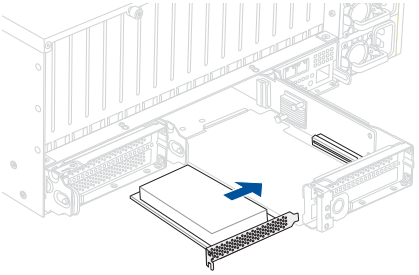
2. Pull the expansion card bay out of the chassis without removing it completely.



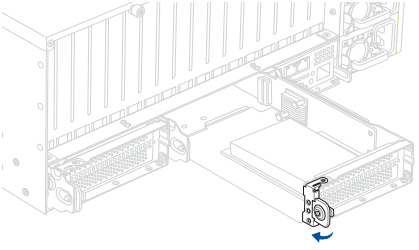
3. Flip the slot cover lock outwards, then remove the slot cover(s).



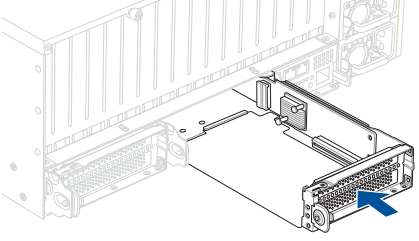
4. Install the expansion card.



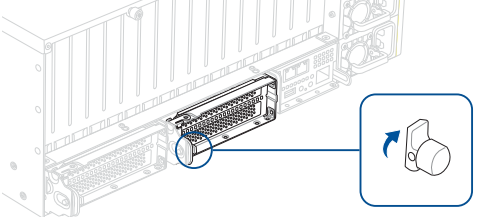
5. Return the slot cover lock to the locked position.



6. Push the expansion card bay all the way into the chassis.



7. Return the latch to the locked position.



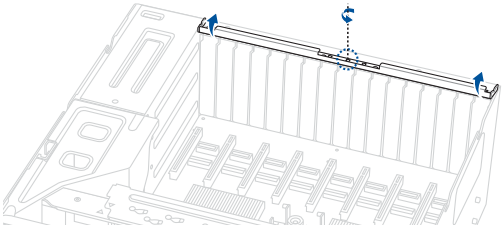
2.6.2 Installing a GPU card

NOTE:

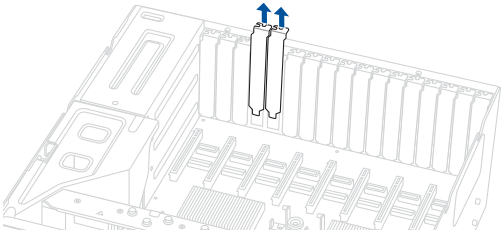
- Use both of your hands in performing the following steps.
- Read the documentation that comes with your GPU card before installing them.
- When installing more than one GPU card, it is recommended to install the cards in the following order: GPU1 > GPU2 > GPU3 > ... > GPU8. Refer to the **GPU SKU board** section for location of the PCIe slots.

Upper expansion card slots on the rear panel

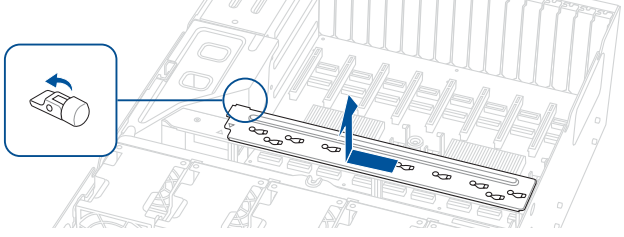
1. Loosen the thumbscrew, then lift the slot cover lock.



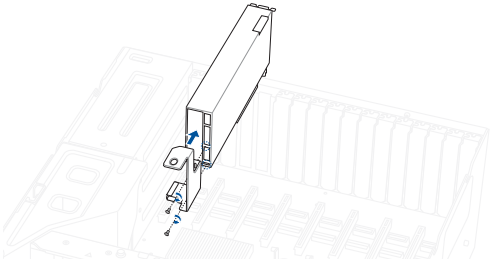
2. Remove the slot cover(s).



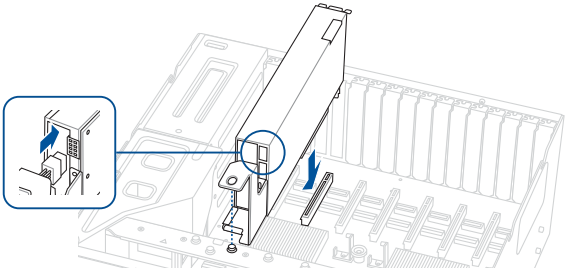
3. Disengage the latch, then remove the GPU bracket.



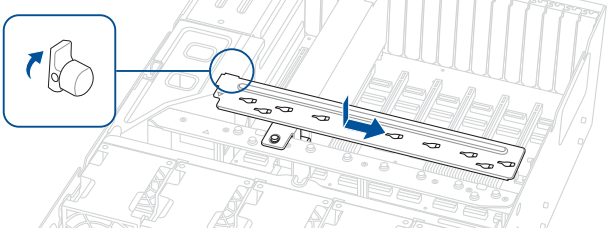
4. Secure the air duct to the GPU card with two screws.



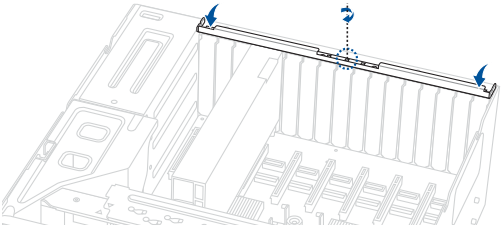
5. Install the GPU card, then connect the GPU power cable to the GPU card.



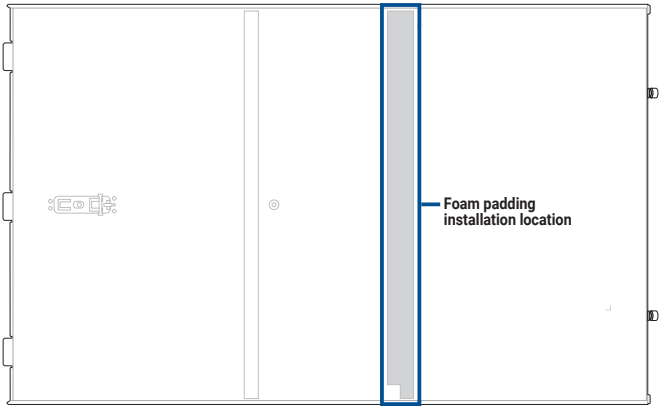
6. Install the GPU bracket, then return the latch to the locked position.



7. Lower the slot cover lock, then tighten the thumbscrew.



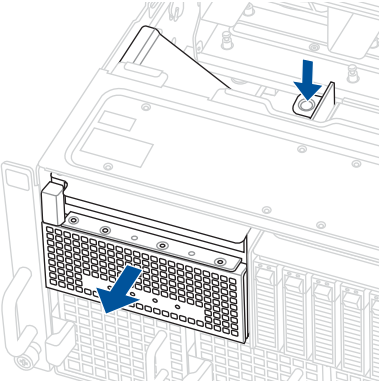
8. If NVIDIA® H200 GPUs are installed, attach the bundled foam padding to the underside of the chassis cover.



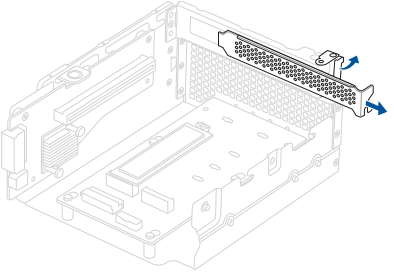
2.6.3 Installing an HBA/RAID card

Upper expansion card slot on the front panel

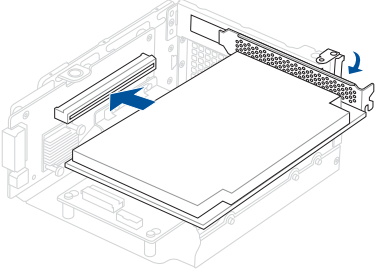
1. Refer to the **Installing a cache vault power module** section to install and connect the cache vault power module (optional).
2. Disconnect the cables from the M.2/RAID card bay.
3. Press down on the latch and pull the M.2/RAID card bay out of the chassis.



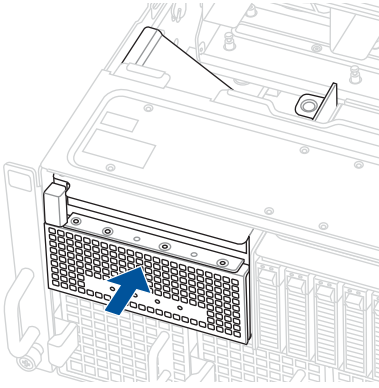
4. Flip the slot cover lock outwards, then remove the slot cover(s).



5. Install the HBA/RAID card, then return the slot cover lock to the locked position.



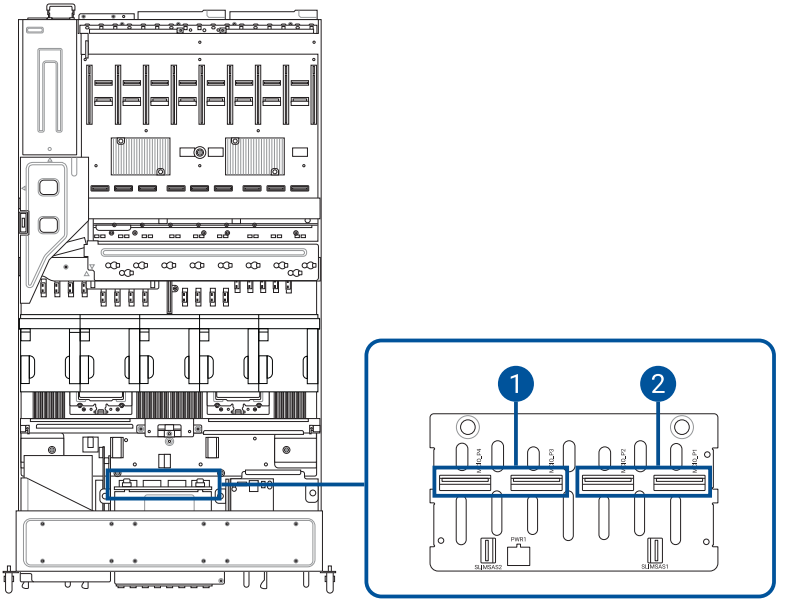
6. Push the M.2/RAID card bay all the way into the chassis.
7. Reconnect the cables to the M.2/RAID card bay.



2.7 Cable connections

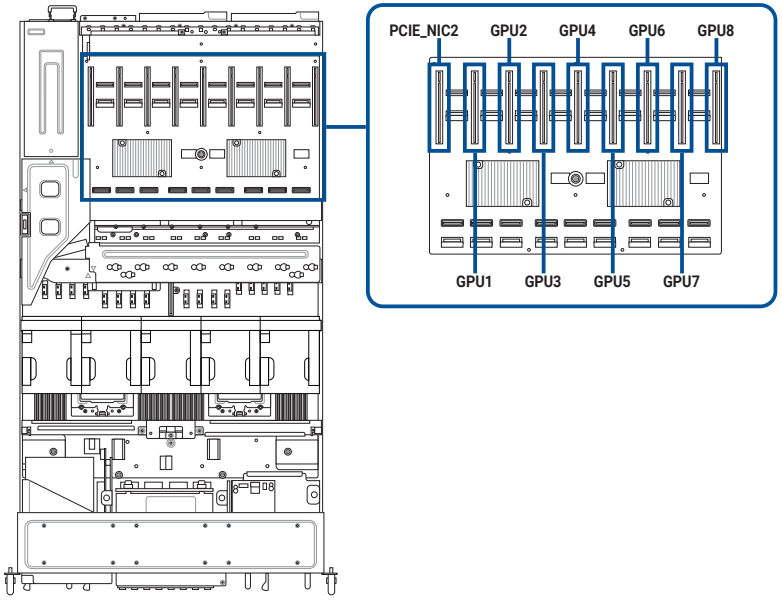
NOTE: The bundled system cables are pre-connected before shipment. You do not need to disconnect these cables unless you remove the pre-installed components to install additional devices.

2.7.1 Storage device backplane

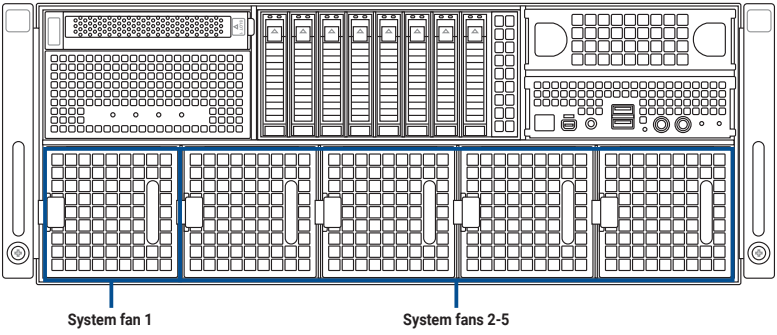


1. Connect to a RAID card for NVMe support on storage bays 5 to 8.
2. Connect to a RAID card for NVMe support on storage bays 1 to 4.

2.7.2 GPU SKU board

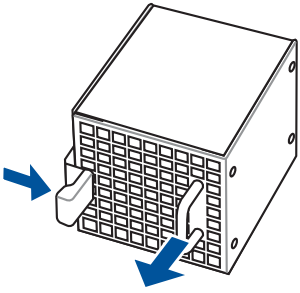


2.8 System fans



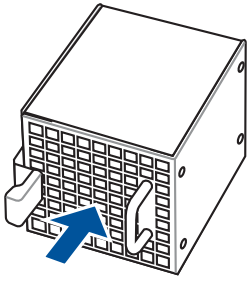
2.8.1 Removing a system fan

Press the latch inwards, then pull and remove the fan from the fan cage.

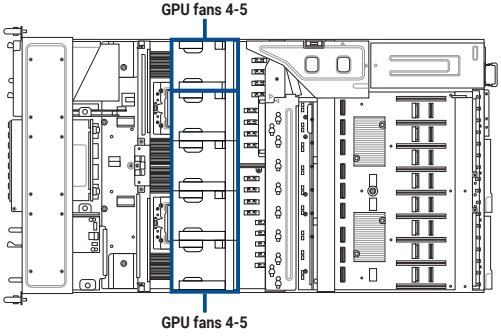


2.8.2 Installing a system fan

Install the fan into the fan cage and ensure it is securely seated.

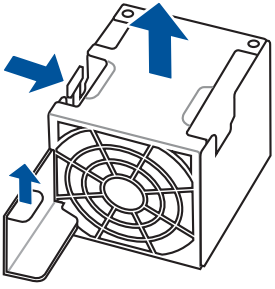


2.9 GPU fans



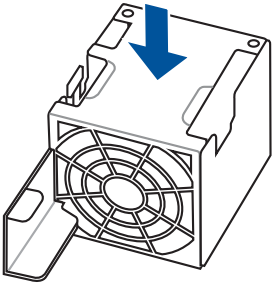
2.9.1 Removing a GPU fan

Press the latch inwards, then pull and remove the fan from the fan cage.



2.9.2 Installing a GPU fan

Install the fan into the fan cage and ensure it is securely seated.



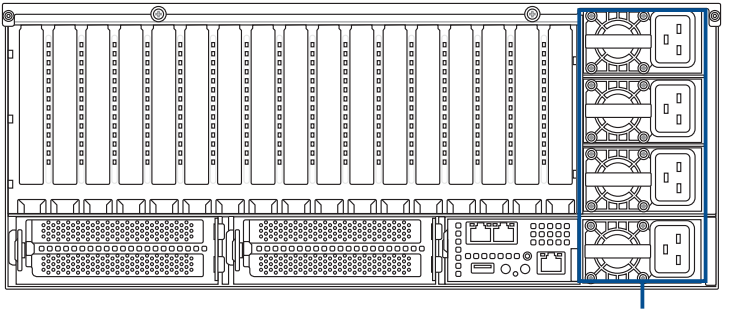
2.10 Redundant power supply units

NOTE:

- The system automatically combines the redundant power supply units. The combined output power varies with input voltages.
- To enable the hot-swap feature (redundant mode), keep the total power consumption of the system under the maximum output power of an individual power supply module.

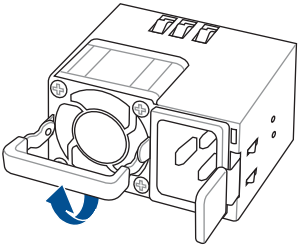
WARNING:

- Always use PSUs with the same watt and power rating. Combining PSUs with different wattages may yield unstable results and potential damage to your system.
- At least three working power supply units are required in order for the system to boot normally.
- For a steady power input, use only the power cables that come with the server system package.

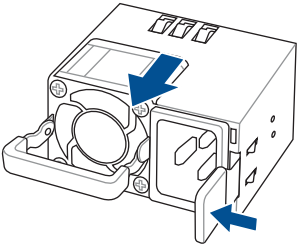


2.10.1 Removing a power supply unit

1. Lift up the PSU lever.

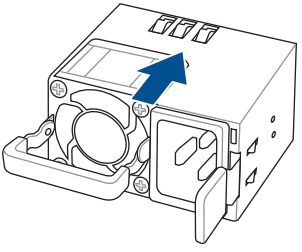


2. Hold the PSU lever and press the PSU latch inwards, then carefully pull the PSU out of the system chassis.



2.10.2 Installing a power supply unit

Align and install the PSU into the server chassis until it clicks into place.



2.11 Motherboard

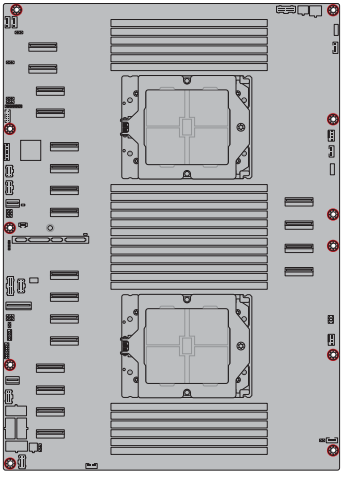
2.11.1 Removing the motherboard

To remove the system motherboard:

1. Disconnect the cables from the motherboard and remove any installed components on the motherboard.

   NOTE: Take a photo or make a note of which components are removed, which cables are disconnected, and which connectors the cables were connected to.

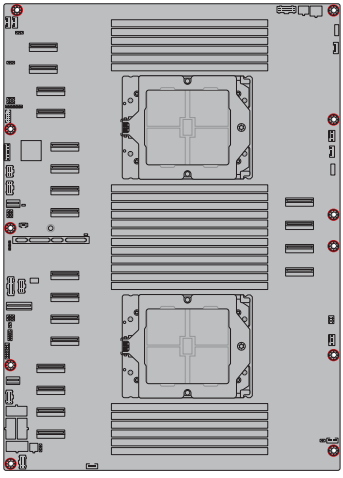
2. Remove the screws, then remove the motherboard.



2.11.2 Installing the motherboard

To install the system motherboard:

1. Place the motherboard into the chassis and ensure the screw holes on the motherboard are aligned with the screw holes in the chassis, then secure the motherboard to the chassis using the screws removed previously.

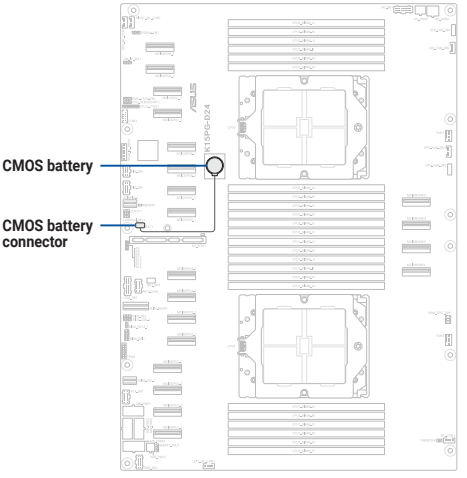


2. Reinstall any removed components and reconnect the cables to the motherboard.

2.12 CMOS battery

2.12.1 Replacing the CMOS battery

1. Disconnect and remove the CMOS battery.



2. Install the replacement CMOS battery and reconnect it to the motherboard.

2.13 Rail kit options

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

NOTE:

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

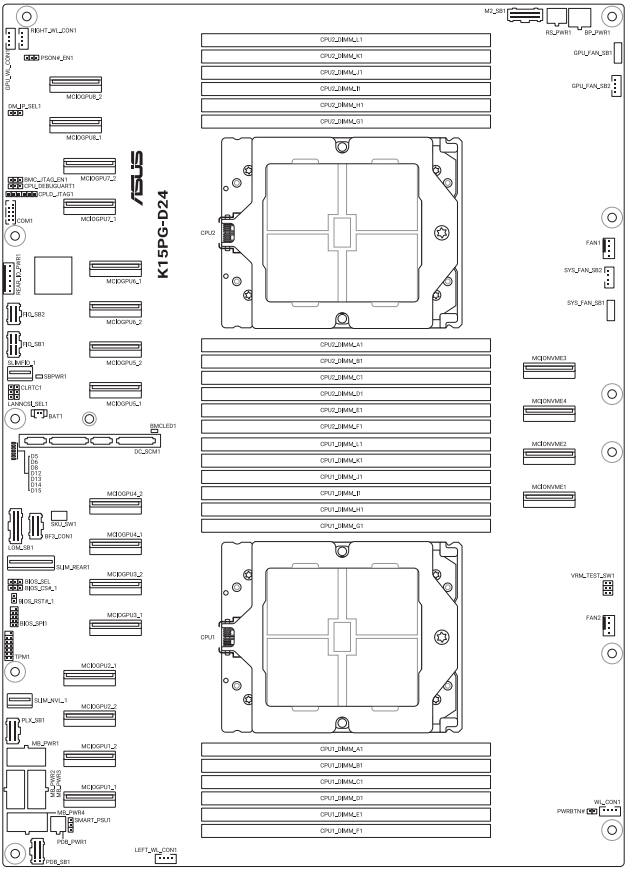
- 2U full extension ball bearing rail kit

Motherboard Information

3

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

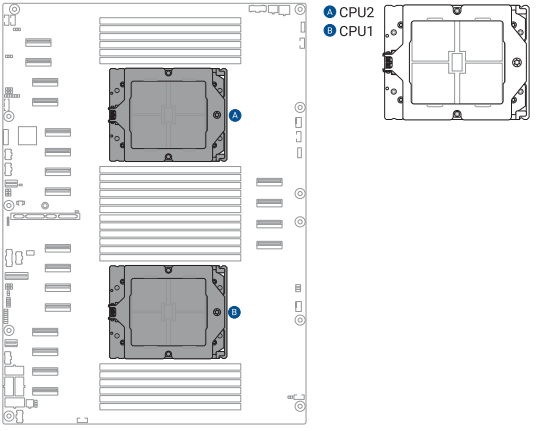
3.1 Motherboard layout



Layout contents

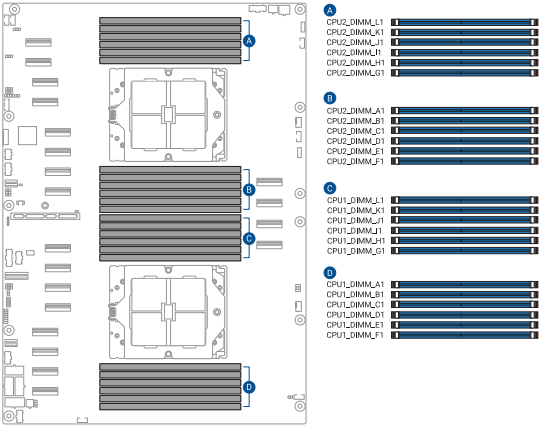
3.2 Central Processing Unit (CPU)

The motherboard comes with two surface mount Socket SP5 sockets designed for AMD EPYC™ 9005 series processors.



3.3 Dual Inline Memory Module (DIMM)

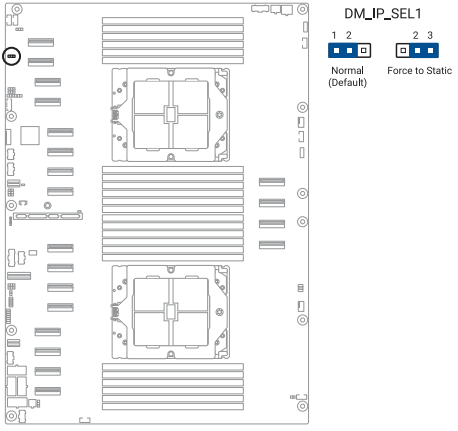
The motherboard comes with twenty four (24) Double Data Rate 5 (DDR5) Dual Inline Memory Modules (DIMM) sockets.



3.4 Jumpers

1. DMLAN setting (3-pin DM_IP_SEL1)

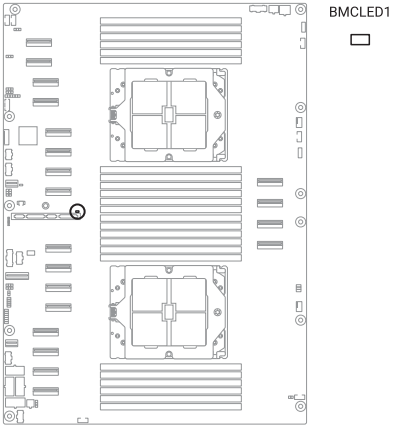
This jumper allows you to select the DMLAN setting. Set to pins 2-3 to force the DMLAN IP to static mode (IP=10.10.10.10, submask=255.255.255.0).



3.5 Onboard LEDs

1. Baseboard Management Controller LED (BMCLED1)

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



BIOS Setup

4

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

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 if the BIOS file fails or gets corrupted.

2. **ASUS EzFlash**

   Updates the BIOS using a USB flash disk.

Refer to the corresponding sections for details on these utilities.

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 if 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.

NOTE: 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.

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

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

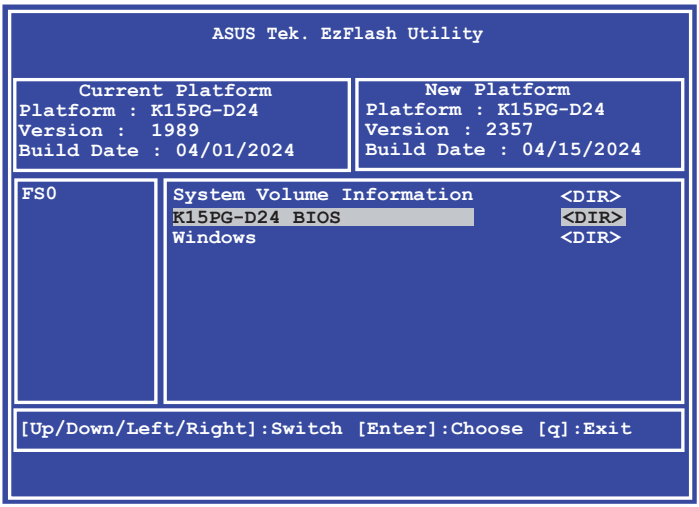
4.1.2 ASUS EZ Flash Utility

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

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

To update the BIOS using EZ Flash Utility:

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



3. Press the Left/Right arrow keys 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 Left/Right arrow keys to switch to the **Folder Info** field.
6. Press the Up/Down arrow keys to find the BIOS file, then press <Enter> to perform the BIOS update process. Reboot the system when the update process is done.

CAUTION:

- 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!

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

4.2 BIOS setup program

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

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

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

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

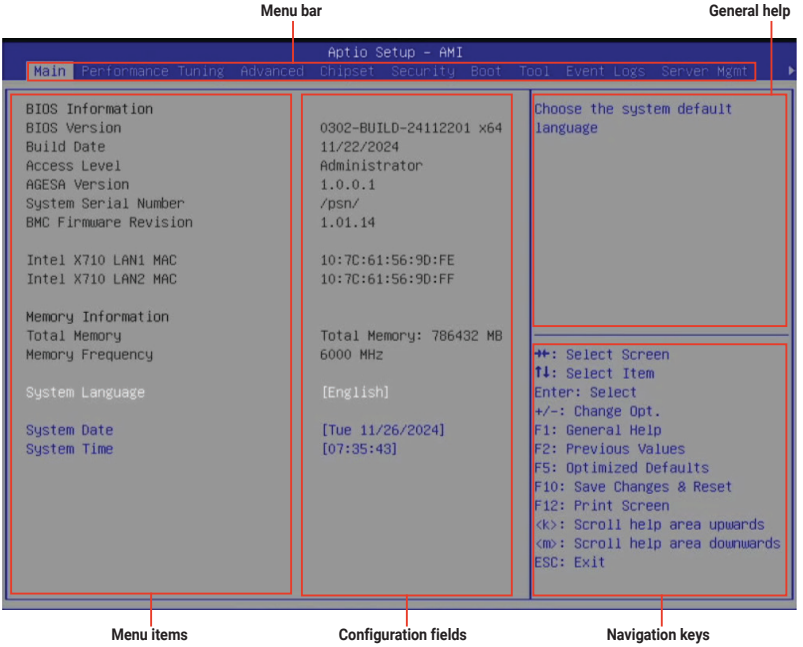
If you wish to enter Setup after POST, restart the system by pressing <Ctrl>+<Alt>+<Delete>, or by pressing the reset button on the system chassis. You can also restart by turning the system off and then back on. Do this last option only if the first two failed.

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

NOTE:

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

4.2.1 BIOS menu screen



4.2.2 Menu bar

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

Main	For changing the basic system configuration
Advanced	For changing the advanced system settings
Chipset	For changing the chipset settings
Security	For changing the security settings
Boot	For changing the system boot configuration
Tool	For configuring options for special functions
Event Logs	For changing the event log settings
Server Mgmt	For changing the Server Mgmt settings
Exit	For selecting the exit options

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

Menu items

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

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

Submenu items

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

Navigation keys

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

General help

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

Configuration fields

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

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

Pop-up window

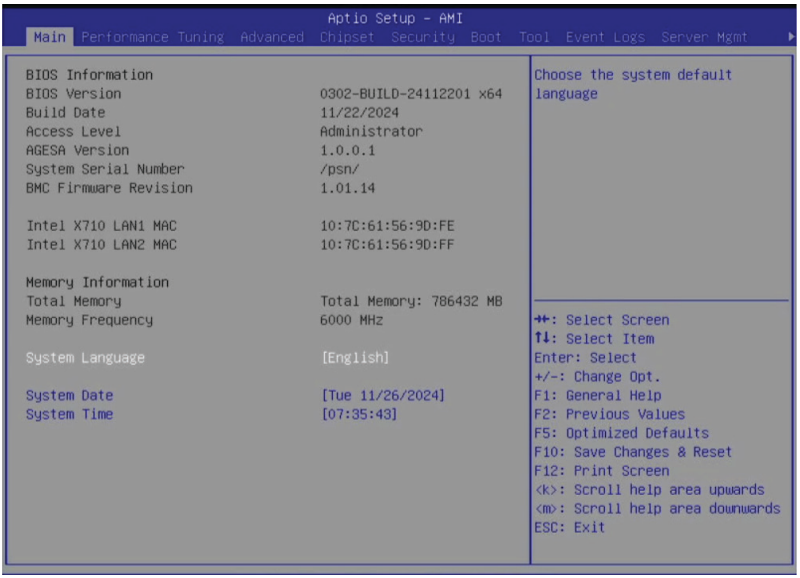
Select a menu item and press <Enter> to display a pop-up window with the configuration options for that item.

Scroll bar

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

4.3 Main menu

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



System Language

Allows you to set the system language.

System Date [MM/DD/YYYY]

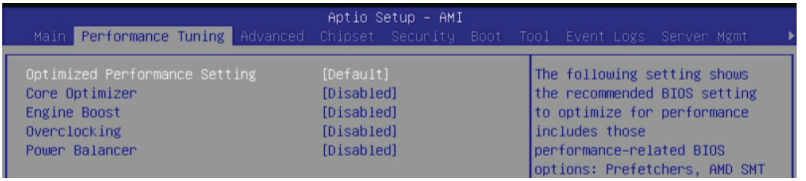
Allows you to set the system date.

System Time [HH:MM:SS]

Allows you to set the system time.

4.4 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.

CAUTION: This function will reset some BIOS settings that you have changed back to their default values. Please check your BIOS settings again.

NOTE: The following item appears only when **Power Balancer** is set to **[Disabled]**, or if Optimized Performance Setting is set to **[Default]** or **[By Benchmark]**.

Core Optimizer [Disabled]

Allows you to keep the processor operating at the turbo highest frequency for the maximum performance.
Configuration options: [Disabled] [Auto] [Manual]

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

CPU Max frequency [XXXX]
The default value for this option will be the maximum supported frequency of the CPU installed and may vary between different CPUs.

NOTE: The following item appears only when **Optimized Performance Setting** is set to **[Default] or [By Benchmark]**.

Engine Boost [Disabled]

Enable this item to boost the CPU's frequency. Recommended operation at an ambient temperature of 25°C or below for optimized performance.
Configuration options: [Disabled] [Normal] [Aggressive]

NOTE: 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]

CAUTION: 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.

NOTE: The following item appears only when **Core Optimizer** is set to **[Disabled]**, or if **Optimized Performance Setting** is set to **[Default]** or **[By Benchmark]**.

Power Balancer [Disabled]

Allows you to dynamically adjust the frequency of all CPU cores based on their current utilization, delivering better performance per watt for improved system energy efficiency.
Configuration options: [Disabled] [Enabled by ACC]

CAUTION: When setting **Power Balancer** to **[Enabled by ACC]**, make sure that you have the latest ASUS Control Center software installed to support Power Balancer. Please see below for recommended software versions:
- ACC: 1.4.3.5 version or above.

NOTE: The following item appears only when **Power Balancer** is set to **[Enabled by ACC]**.

Policy [Auto]
Configuration options: [Auto] [Manual]

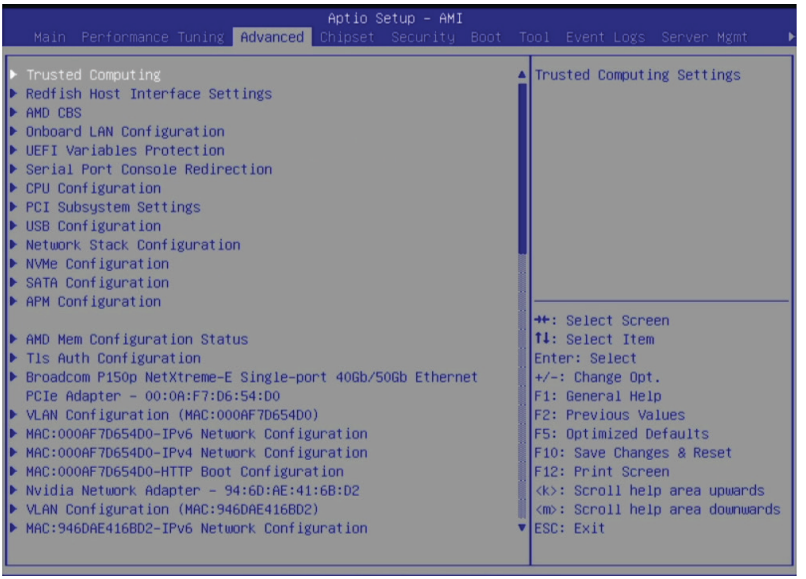
NOTE: The following item appears only when set **Policy** is set to **[Manual]**.

CPU Max frequency [XXXX]
The default value for this option will be the maximum supported frequency of the CPU installed and may vary between different CPUs.

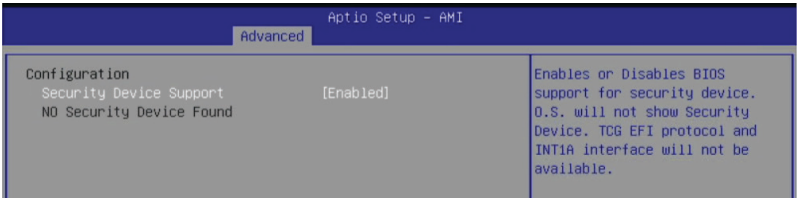
4.5 Advanced menu

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

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



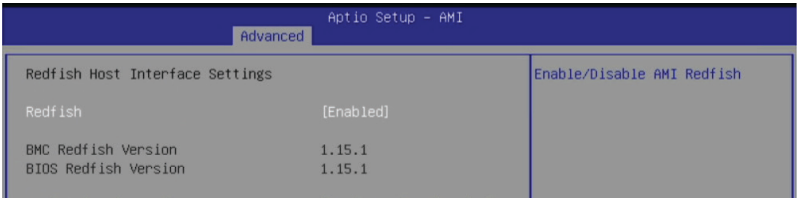
4.5.1 Trusted Computing



Security Device Support [Enabled]

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

4.5.2 Redfish Host Interface Settings



Redfish [Enabled]

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

NOTE: The following item appears only when **Redfish** is set to **[Enabled]**.

Authentication Mode [Basic Authentication]

Configuration options: [Basic Authentication] [Session Authentication] [Authentication None]

IP Address

Allows you to set the IP address

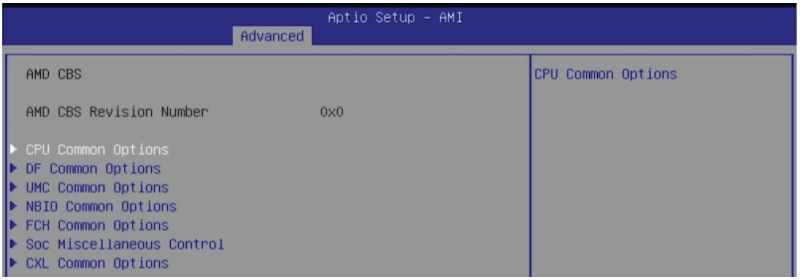
IP Mask Address

Allows you to set the IP mask address

IP Port

Allows you to set the IP port

4.5.3 AMD CBS



CPU Common Options

Performance

Allows you to configure performance options.

REP-MOV/STOS Streaming [Enabled]

Allows you to enable or disable the use of non-caching streaming stores for large sizes.
Configuration options: [Disabled] [Enabled]

Prefetcher Settings

Allows you to configure prefetcher options.

Core Watchdog

Allows you to configure core watchdog options.

RedirectForReturnDis [Auto]

Allows you to set RedirectForReturnDis to 0, 1, or Auto as a workaround for GCC/C000005 issue for XV Core on CZ A0.
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: [Disabled] [Enabled] [Auto]

Core Performance Boost [Auto]

Configuration options: [Disabled] [Auto]

Global C-State Control [Auto]

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

Power Supply Idle Control [Auto]

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

Streaming Stores Control [Auto]

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

Local APIC Mode [Auto]

Configuration options: [Compatibility] [xAPIC] [x2APIC] [Auto]

ACPI _CST C1 Declaration [Auto]

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

ACPI CST C2 Latency [100]

Allows you to set the C2 latency value in microseconds.

MCA Error Threshold Enable [Auto]

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

NOTE: The following item appears only when **MCA Error Threshold Enable** is set to **[True]**.

MCA Error Threshold Count [FF5]
Allows you to set the MCA error threshold count.

MCA FruText [True]

Configuration options: [False] [True]

SMU and PSP Debug Mode [Auto]

If this option is enabled, uncorrected errors detected by the PSP FW or SMU FW will hang and not reset the system instead of causing a cold reset.
Configuration options: [Disabled] [Enabled] [Auto]

PPIN Opt-in [Auto]

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

SMEE [Auto]

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

NOTE: The following item appears only when **SMEE** is set to **[Enabled]**.

SEV Control [Enabled]
Configuration options: [Disabled] [Enabled]

SEV-ES ASID Space Limit [1]
Allows you to set the SEV-ES ASID Space Limit.

SNP Memory (RMP Table) Coverage [Auto]
Configuration options: [Disabled] [Enabled] [Custom] [Auto]

NOTE: The following items appear only when **SNP Memory (RMP Table) Coverage** is set to **[Enabled]** or **[Custom]**.

Split RMP Table [Auto]
Configuration options: [Disabled] [Enabled] [Auto]

Segmented RMP Table [Auto]
Configuration options: [Disabled] [Enabled] [Auto]

RMP Segment Size [Auto]
Configuration options: [Disabled] [Enabled] [Auto]

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

RMP Coverage for 64Bit MMIO Ranges [Auto]
Configuration options: [Disabled] [Enabled] [Auto]

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

Amount of Memory to Cover [0]
Allows you to set the amount of system memory (MB) to be covered in hex.

Action on BIST Failure [Auto]

Allows you to configure what action is taken when a CCD BIST failure is detected.
Configuration options: [Do nothing] [Down-CCD] [Auto]

Enhanced Short REP MOVSB/STOSB (ESRM) [Auto]

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

Log Transparent Errors [Auto]

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

AVX512 [Auto]

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

MONITOR and MWAIT Disable [Auto]

When this option is enabled, MONITOR, MWAIT, MONITORX, and MWAITX opcodes become invalid.
Configuration options: [Disabled] [Enabled] [Auto]

CPU Speculative Store Modes [Auto]

Configuration options: [Balanced] [More Speculative] [Auto]

Fast Short REP MOVSB (FSRM) [Auto]

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

PauseCntSel_1_0 [Auto]

Configuration options: [Auto] [16 cycles] [32 cycles] [64 cycles] [128 cycles]

Prefetch/Request Throttle [Auto]

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

Scan Dump Debug Enable [Disabled]

Configuration options: [Disabled] [Enabled]

MCAX 64 Bank Support [Auto]

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

Adaptive Allocation (AA) [Auto]

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

Latency Under Load (LUL) [Auto]

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

Core Trace Dump Enable [Disabled]

Configuration options: [Disabled] [Enabled]

FP512 [Auto]

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

DF Common Options

Memory Addressing

Allows you to configure memory addressing options.

ACPI

Allows you to configure ACPI options.

Link

Allows you to configure Link options.

SDCI

Allows you to configure SDCI options.

Probe Filter

Allows you to configure Probe Filter options.

DF Watchdog Timer Interval [Auto]

Configuration options: [Auto] [41ms] [166ms] [334ms] [669ms] [1.34 seconds] [2.68 seconds] [5.36 seconds]

Disable DF to external IP Sync Flood Propagation [Auto]

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

Sync Flood Propagation to DF Components [Auto]

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

Freeze DF Module Queues on Error [Auto]

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

CC6 Memory Region Encryption [Auto]

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

CC6 B/W Balance Throttle Level [Auto]

Configuration options: [Auto] [Level 0] [Level 1] [Level 2] [Level 3] [Level 4]

Number of PCI Segments [Auto]

Configuration options: [Auto] [1 Segment] [2 Segments] [4 Segments]

CCM Throttler [Auto]

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

> **NOTE:** The following item appears only when **CCM Throttler** is set to **[Enabled]**.

MemReqBandwidthControl [FineThrotHeavy] [0]
Allows you to set the CCM throttle limit.

MemReqBandwidthControl [FineThrotLight] [0]
Allows you to set the CCM throttle limit.

Clean Victim FTI Cmd Balancing [Auto]

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

> **NOTE:** The following item appears only when **Clean Victim FTI Cmd Balancing** is set to **[Enabled]**.

CCMConfig5 [ReqvReqNDImbThr] [Auto]
Configuration options: [Auto] [1h] [2h] [3h] [4h] [5h] [6h] [7h]

CXL Strongly Ordered Writes [Disabled]

Configuration options: [Disabled] [One at a time]

UMC Common Options

DDR Addressing Options

Allows you to configure DDR addressing options.

DDR Controller Configuration

Allows you to configure DDR controller options.

DDR MBIST Options

Allows you to configure DDR MBIST options.

DDR RAS

Allows you to configure DDR RAS options.

DDR Bus Configuration

Allows you to configure DDR Bus options.

DDR Timing Configuration

Allows you to configure DDR Timing options.

DDR Training Options

Allows you to configure DDR Training options.

DDR Security

Allows you to configure DDR Security options.

DDR PMIC Configuration

Allows you to configure DDR PMIC options.

DDR Thermal Throttling

Allows you to configure DDR Thermal Throttling options.

DDR Miscellaneous

Allows you to configure DDR Miscellaneous options.

NBIO Common Options

SMU Common Options

Allows you to configure SMU Common options.

NBIO RAS Common Options

Allows you to configure NBIO RAS Common options.

PCIE

Allows you to configure PCIE options.

nBif Common Options

Allows you to configure nBif Common options.

IOMMU/Security

Allows you to configure IOMMU/Security options.

Enable Port Bifurcation

Allows you to configure Port Bifurcation options.

Link EQ Preset Options

Allows you to configure Link EQ Preset options.

PCIe Loopback Mode [Auto]

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

Enable 2SPC (Gen 4) [Auto]

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

Enable 2SPC (Gen 5) [Auto]

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

Safe recovery upon a BERExceeded Error [Auto]

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

Periodic Calibration [Auto]

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

FCH Common Options

I3C/I2C Configuration Options

Allows you to configure I3C/I2C options.

SATA Configuration Options

Allows you to configure SATA options.

USB Configuration Options

Allows you to configure USB options.

AC Power Loss Options

Allows you to configure AC power loss options.

UART Configuration Options

Allows you to configure UART options.

FCH RAS Options

Allows you to configure FCH RAS options.

Miscellaneous Options

Allows you to configure miscellaneous FCH options.

SOC Miscellaneous Control

ABL Console Out Control [Auto]

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

NOTE: The following items appear only when **ABL Console Out Control** is set to **[Enabled]**.

ABL Console Out Serial Port [Auto]
Configuration options: [eSPI UART] [SOC UART0] [SOC UART1] [Auto]

ABL Console Out Serial Port IO [Auto]
Configuration options: [0x3F8] [0x2F8] [0x3E8] [0x2E8] [Auto]

ABL Serial Port IO Customized Enabled [Disabled]
Configuration options: [Disabled] [Enabled]

ABL Basic Console Out Control [Auto]
Configuration options: [Disabled] [Enabled] [Auto]

ABL PMU Message Control [Auto]
Allows you to control the number of PMU debug messages.

Configuration options: [Detailed debug messages] [Coarse debug messages] [Stage completion] [Auto]

ABL Memory Population Message Control [Warning Message]

Configuration options: [Warning Message] [Fatal Error]

PSP Error Injection Support [False]

Configuration options: [False] [True]

Firmware Anti-rollback (FAR)

Allows you to configure Firmware Anti-Rollback (FAR) options.

SEC_I2C Voltage Mode [Auto]

Configuration options: [Auto] [1.8V] [1.1V]

CXL Common Options

CXL Control [Auto]

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

CXL Physical Addressing [Auto]

Configuration options: [Normalized address] [System address] [Auto]

CXL Memory Attribute [Auto]

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

CXL Encryption [Disabled]

Configuration options: [Disabled] [Enabled]

CXL DVSEC Lock [Auto]

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

CXL HDM Decoder Lock On Commit [Auto]

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

Temp Gen5 Advertisement [Auto]

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

Sync Header Bypass [Auto]

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

Sync Header Bypass Compatibility Mode [Auto]

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

CXL RAS

Allows you to configure CXL RAS options.

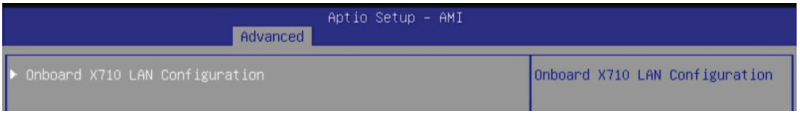
CXL Memory Online/Offline [Disabled]

Configuration options: [Disabled] [Enabled]

Override CXL Memory Size [Auto]

Configuration options: [32GB] [64GB] [128GB] [Auto]

4.5.4 Onboard LAN Configuration



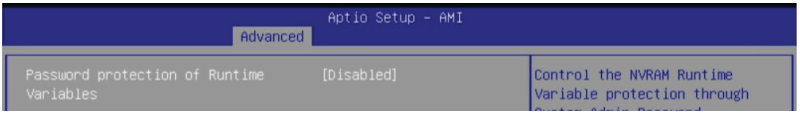
Onboard X710 LAN Configuration

Intel X710 LAN1 and LAN2

LAN Enable [LAN1, LAN2 Enabled]

Configuration options: [Disabled] [LAN1 Enabled Only] [LAN1, LAN2 Enabled]

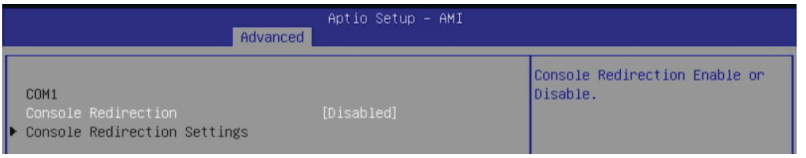
4.5.5 UEFI Variables Protection



Password Protection of Runtime Variables [Disabled]

Configuration options: [Disabled] [Enabled]

4.5.6 Serial Port Console Redirection



COM1/COM2(SOL)

Console Redirection [Disabled]

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

NOTE: The following items appear only when **Console Redirection** is set to **[Enabled]**.

Terminal Type [VT100Plus]

Allows you to set the terminal type.

[VT100]	ASCII char set.
[VT100Plus]	Extends VT100 to support color, function keys, etc.
[VT-UTF8]	Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
[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 [Hardware RTS/CTS]

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 to set the number of rows and columns supported on the Legacy OS.
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]

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

Console Redirection EMS [Disabled]

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

> **NOTE:** The following items appear only when **Console Redirection EMS** is set to **[Enabled]**.

Console Redirection Settings

Out-of-Band Mgmt Port [COM1]

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

Terminal Type EMS [VT-UTF8]

Microsoft Windows Emergency Management Services (EMS) allow for remote management of a Windows Server OS through a serial port.
Configuration options: [VT100] [VT100Plus] [VT-UTF8] [ANSI]

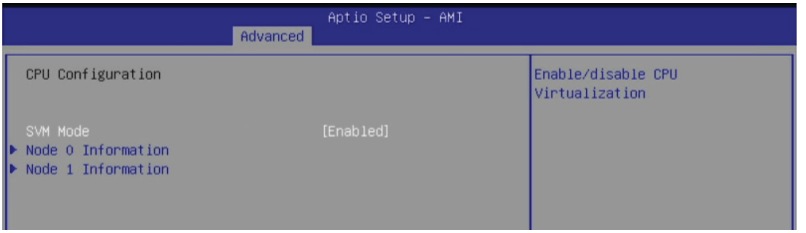
Bits per second EMS [115200]

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 EMS [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]

4.5.7 CPU Configuration



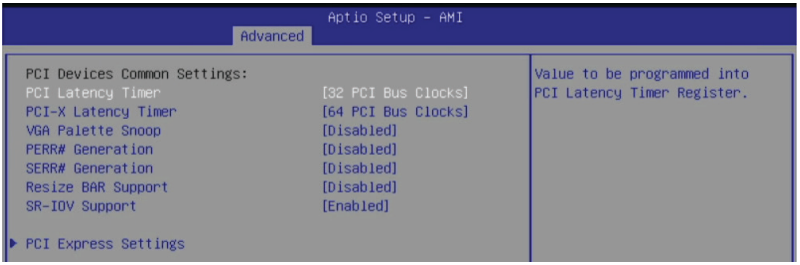
SVM Mode [Enabled]

This item allows you enable or disable CPU Virtualization.
Configuration options: [Disabled] [Enable]

Node Information

This item allows you to view memory information related to the selected node.

4.5.8 PCI Subsystem Settings



PCI Latency Timer [32 PCI Bus Clocks]

Configuration options: [32 PCI Bus Clocks] [64 PCI Bus Clocks] [96 PCI Bus Clocks] [128 PCI Bus Clocks] [160 PCI Bus Clocks] [192 PCI Bus Clocks] [224 PCI Bus Clocks] [248 PCI Bus Clocks]

PCI-X Latency Timer [64 PCI Bus Clocks]

Configuration options: [32 PCI Bus Clocks] [64 PCI Bus Clocks] [96 PCI Bus Clocks] [128 PCI Bus Clocks] [160 PCI Bus Clocks] [192 PCI Bus Clocks] [224 PCI Bus Clocks] [248 PCI Bus Clocks]

VGA Palette Snoop [Disabled]

Configuration options: [Disabled] [Enabled]

PERR# Generation [Disabled]

Configuration options: [Disabled] [Enabled]

SERR# Generation [Disabled]

Configuration options: [Disabled] [Enabled]

Re-Size BAR Support [Disabled]

Configuration options: [Disabled] [Auto]

SR-IOV Support [Enabled]

Configuration options: [Disabled] [Enabled]

PCI Express Settings

Allows you to configure PCI Express options.

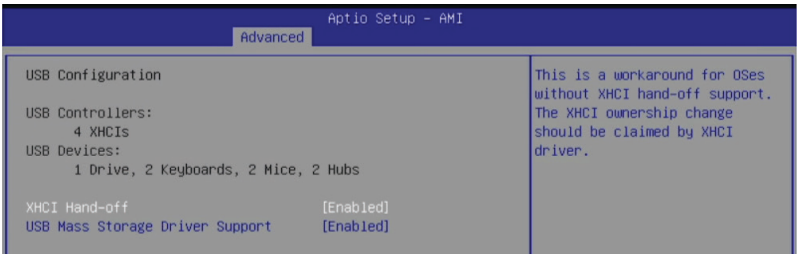
PCI Express GEN 2 Settings

Allows you to configure PCI Express GEN 2 options.

PCI Hot-Plug Settings

Allows you to configure PCI Hot-Plug options.

4.5.9 USB Configuration



XHCI Hand-off [Enabled]

Configuration options: [Enabled] [Disabled]

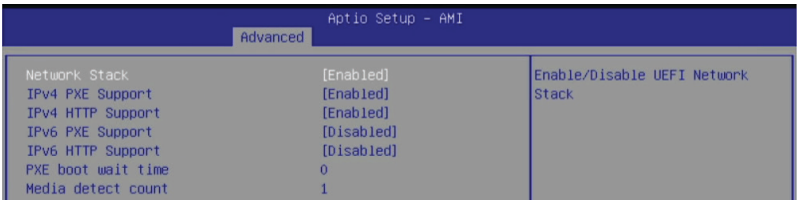
USB Mass Storage Driver Support [Enabled]

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]

4.5.10 Network Stack Configuration



Network Stack [Enabled]

Configuration options: [Disabled] [Enabled]

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

IPv4 PXE Support [Enabled]

Configuration options: [Disabled] [Enabled]

IPv4 HTTP Support [Enabled]

Configuration options: [Disabled] [Enabled]

IPv6 PXE Support [Disabled]

Configuration options: [Disabled] [Enabled]

IPv6 HTTP Support [Disabled]

Configuration options: [Disabled] [Enabled]

PXE boot wait time [0]

Wait time to press ESC key to abort the PXE boot.

Media detect count [1]

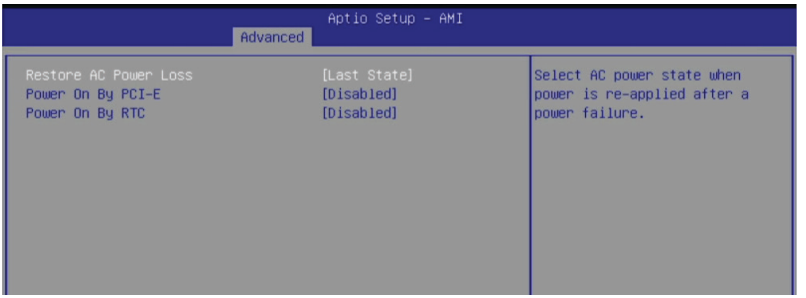
Wait time (in seconds) to detect media.

4.5.11 NVMe Configuration

This page will display the NVMe controller and drive information.

4.5.12 APM Configuration

Allows you to configure the Advance Power Management (APM) settings.



Restore AC Power Loss [Last State]

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

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.

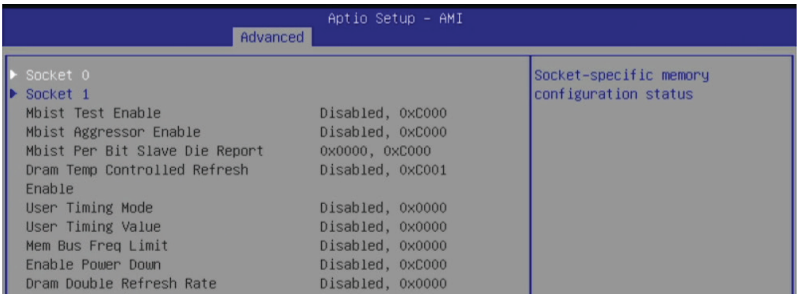
Power On By RTC [Disabled]

[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.

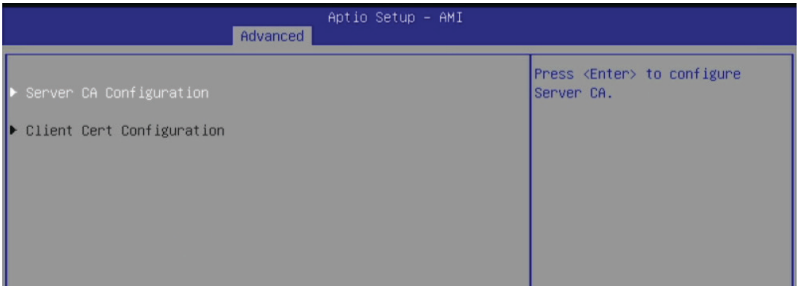
4.5.13 AMD Mem Configuration Status

The items in this menu display the memory configuration (initialized by ABL) status.



4.5.14 T1s Auth

Allows you to configure the Server Certificate Authority (CA).



Server / Client CA Configuration

Enroll Cert

Allows you to enroll a certificate using a certificate file or manually input a certificate GUID.

Enroll Cert Using File
Allows you to enroll a certificate using a certificate file. You will be prompted to select a storage device and navigate to the location of the certificate file.

Cert GUID
Allows you to enroll a certificate by manually inputting the certificate GUID.

Commit Changes and Exit
Exit Server CA configuration after saving the changes.

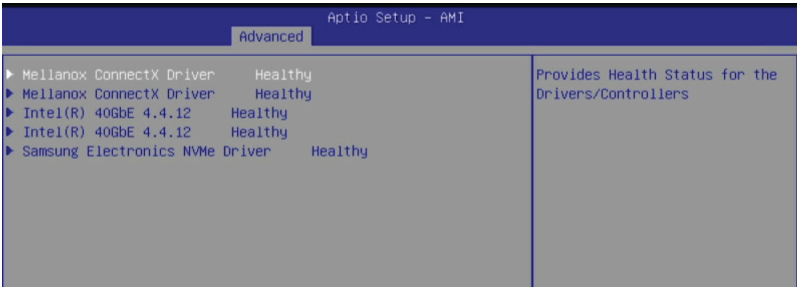
Discard Changes and Exit
Exit Server CA configuration without saving any changes.

Delete Cert

Allows you to delete the certificate.

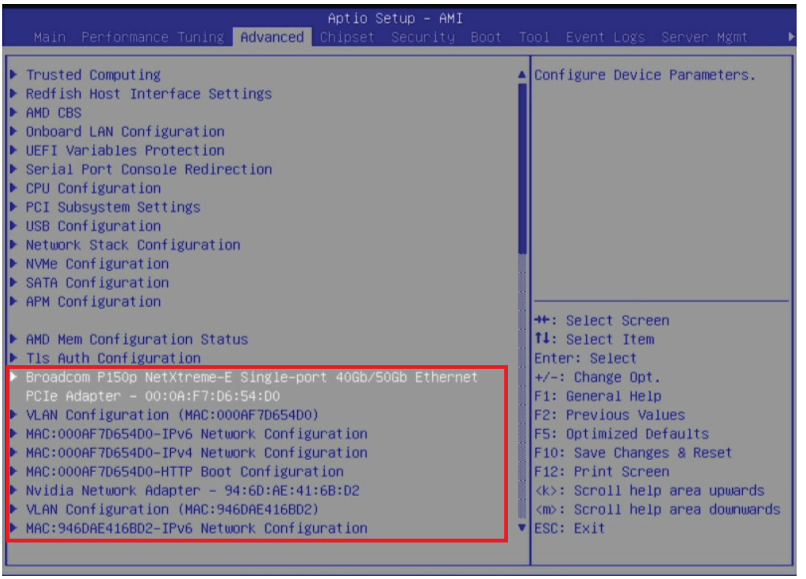
4.5.15 Driver Health

This page will display the driver and controller health status.

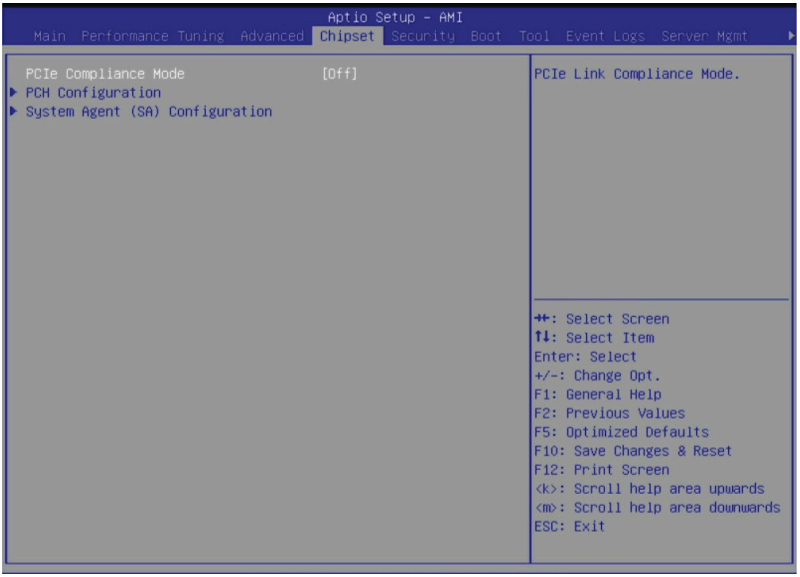


4.5.16 Third-party UEFI driver configurations

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



PCIe Compliance Mode [Off]

This item allows you to turn the PCIe Compliance Mode on or off.
Configuration options: [Off] [On]

PCH Configuration

SB Debug Configuration

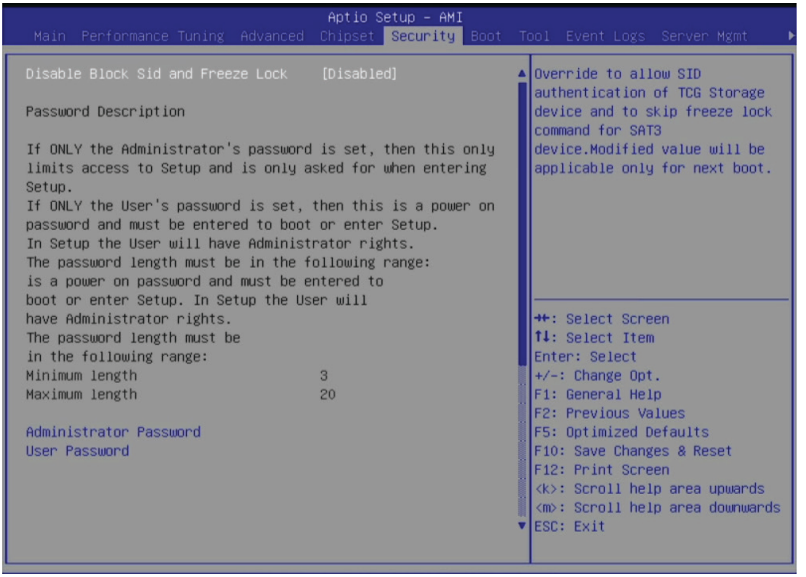
Allows you to configure SB Debug options.

System Agent (SA) Configuration

Socket Information

This item displays the memory information for the selected socket.

4.7 Security menu



Disable Block Sid and Freeze Lock [Disabled]

Configuration options: [Disabled] [Enabled]

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.

NOTE: 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.

NOTE: To clear the user password, follow the same steps as in changing a user password, but press <Enter> when prompted to create/confirm the password.

Media Sanitization

This item allows you to sanitize selected drives. After selecting the drive you wish to sanitize, select the Method Type from between [Clear] or [Purge]. The default method is set to [Clear], and will apply logical techniques to sanitize data in all user-addressable storage locations through standard Read and Write commands to the storage device.

When [Purge] is selected, it will apply physical or logical techniques that render Target Data recovery infeasible using state-of-the-art laboratory techniques.

Secure Boot

Secure Boot [Disabled]

Secure Boot can be enabled if the system is running in User mode with enrolled platform Key (EPK) or if the CSM function is disabled.
Configuration options: [Disabled] [Enabled]

Secure Boot Mode [Custom]

Allows you to set the Secure Boot selector.
Configuration options: [Standard] [Custom]

Restore Factory Keys

Allows you to restore the factory keys.

Reset To Setup Mode

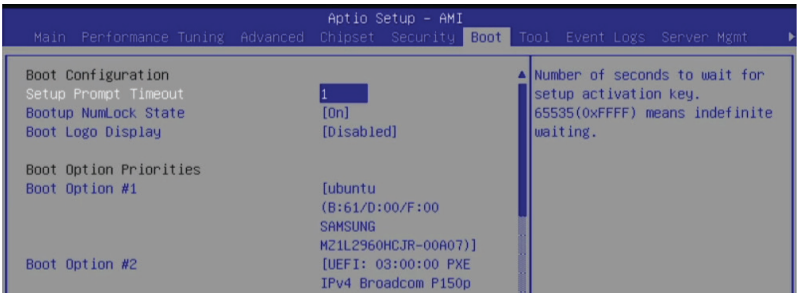
Allows you to reset to setup mode.

Expert Key Management

Allows you to configure Expert Key Management options.

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: [On] [Off]

Boot Logo Display [Disabled]

Allows you to enable or disable Quiet Boot option.
Configuration options: [Disabled] [Enabled]

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.

NOTE: To select the boot device during system startup, press <F8> when ASUS Logo appears.

POST Report [5 sec]

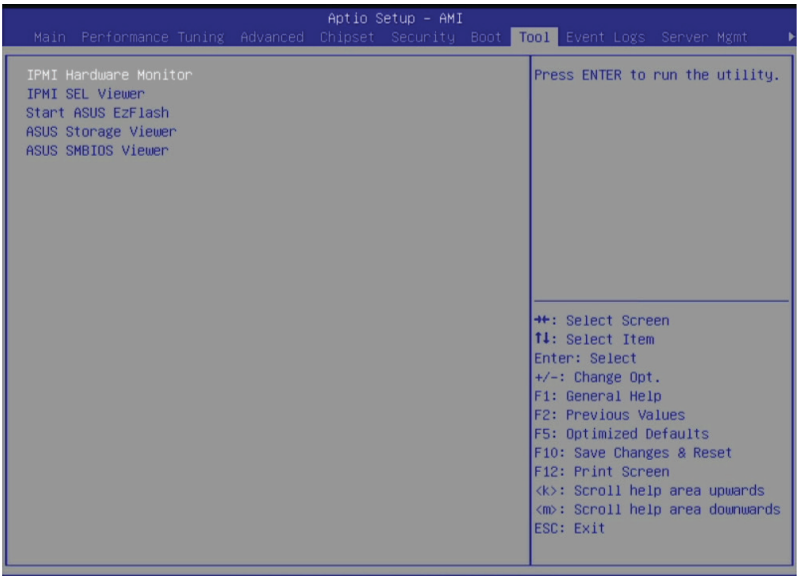
Allows you to set the desired POST Report waiting time from 1 to 10 seconds.
Configuration options: [1 sec] - [10 sec] [Until Press ESC]

Hard Drive BBS Priorities

These items appear only when you connect a network cable or SATA ODD to the SATA port, and allows you to set the booting order of the Network / SATA devices.

4.9 Tool menu

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



IPMI Hardware Monitor

Allows you to run the IPMI hardware monitor.

IPMI SEL Viewer

Allows you to run the IPMI SEL viewer.

Start ASUS EzFlash

Allows you to run ASUS EZ Flash BIOS ROM Utility. Refer to the ASUS EZ Flash Utility section for details.

ASUS Storage Viewer

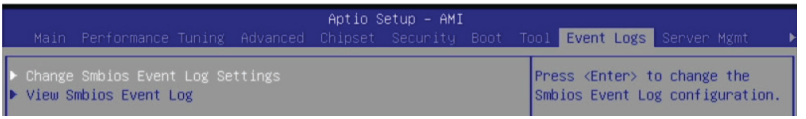
Allows you to run ASUS Storage Viewer.

ASUS SMBIOS Viewer

Allows you to run 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.



4.10.1 Change Smbios Event Log Settings

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

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

Smbios Event Log [Enabled]

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

NOTE: The following item appears only when **Smbios Event Log** is set to **[Enabled]**.

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]

Log EFI Status Code [Enabled]

This option allows you to enable or disable logging of the EFI Status Codes.
Configuration options: [Disabled] [Enabled]

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

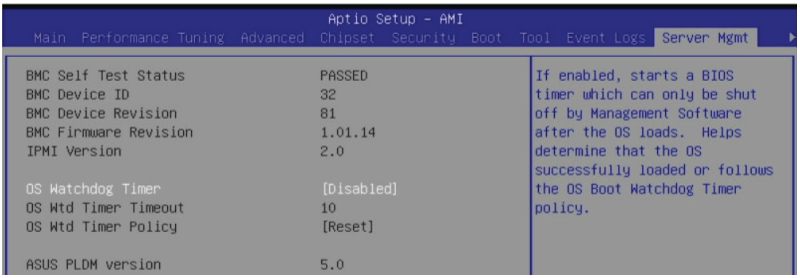
Convert EFI Status Codes to Standard Smbios Type [Disabled]
This option allows you to enable or disable converting of EFI Status Codes to Standard Smbios Type (Not all may be translated).
Configuration options: [Disabled] [Enabled]

4.10.2 View Smbios Event Log

Press <Enter> to view all smbios event logs.

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]

This item allows you to start a BIOS timer which can only be shut off by management software after the OS loads.
Configuration options: [Enabled] [Disabled]

NOTE: The following items appear only when **OS Watchdog Timer** is set to **[Enabled]**.

OS Wtd Timer Timeout [10]

Enter the value between 1 to 30 minutes to configure the length fo the OS Boot Watchdog Timer.

OS Wtd Timer Policy [Reset]

This item allows you to configure the how the system should respond if the OS Boot Watch Timer expires.
Configuration options: [Do Nothing] [Reset] [Power Down] [Power Cycle]

4.11.1 System Event Log

Allows you to change the SEL event log configuration.

Erase SEL [No]

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

4.11.2 BMC network configuration

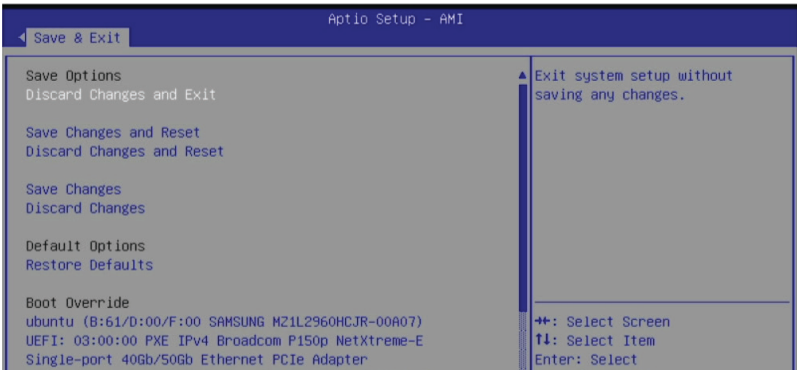
The sub-items in this configuration allow you to configure the BMC network parameters.

4.11.3 View System Event Log

This item allows you to view the system event log records.

4.12 Exit menu

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



Discard Changes and Exit

Exit system setup without saving any changes.

Save Changes and Reset

Reset the 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.

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.

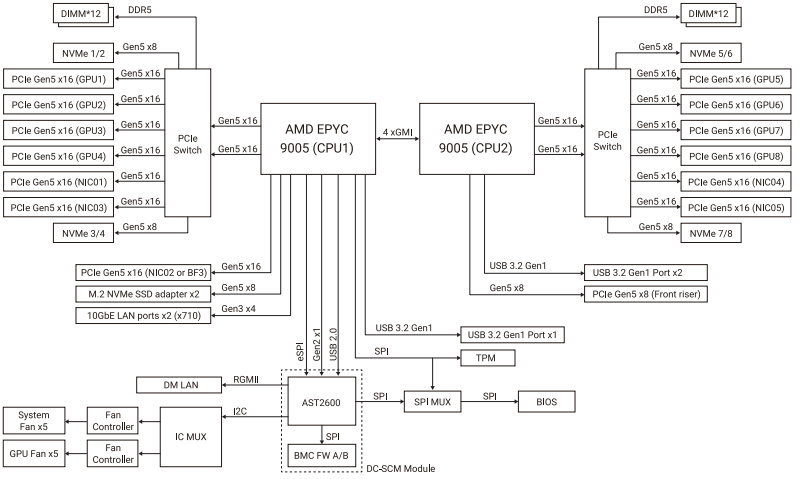
Launch EFI Shell from filesystem device

This item allows you to attempt to launch the EFI Shell application (shellx64.efi) from one of the available filesystem devices.

Appendix

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

Block diagram



Q-Code table

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 spirom 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
		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

(continued on the next page)

ACTION	PHASE	POST CODE	TYPE	DESCRIPTION
PSP Boot	PSP Boot Loader phase (Error Post Codes)	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 C2PMSG_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	Failed to find FW entry in SPL Table
		0x47	error	Failed to read the combo bios header
		0x48	error	SPL version mismatch
		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
		0x5D	error	Reserved PSP/SMU memory region is invalid
		0x5E	error	CcxSecBisiEn 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 occured 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
		0x70	error	Unexpected fuse set
		0x71	error	RSMU signaled a security violation
		0x72	error	Error programming the WAFL PCS registers
		0x73	error	Error setting wafl PCS threshold value
		0x74	error	Error loading OEM trustlets
		0x75	error	Recovery mode accross 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	OEM Key validation failed
		0x7C	error	Platform Vendor ID and/or Model ID binding violation

(continued on the next page)

ACTION	PHASE	POST CODE	TYPE	DESCRIPTION
PSP Boot	PSP Boot Loader phase (Status Post Codes)	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 broadcase and clear the IsInSRAM 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 DXIO PHY SRAM Public key certificate loading or authentication fails
		0x8F	error	fTPM 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	Firmware Compatibility Level mismatch
		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
		0xA0	error	Bootloader successfully entered C Main
		0xA1	error	Master initialized C2P / slave waited for master to init C2P
		0xA2	error	HMAC key successfully derived
		0xA3	error	Master got Boot Mode and sent boot mode to all slaves
		0xA4	error	SpiRom successfully initialized
		0xA5	error	BIOS Directory successfully read from SPI to SRAM
		0xA6	error	Early unlock check
		0xA7	error	Inline Aes key successfully derived
		0xA8	error	Inline-AES key programming is done
		0xA9	error	Inline-AES key wrapper derivation is done
		0xAA	error	Bootloader successfully loaded HW IP configuration values
		0xAB	error	Bootloader successfully programmed MBAT table
		0xAC	error	Bootloader successfully loaded SMU FW
		0xAD	error	Progress code is available
		0xAE	error	User mode test Uapp completed successfully
		0xAF	error	Bootloader loaded Agesa0 from SpiRom
		0xB0	error	AGESA phase has completed
		0xB1	error	RunPostDramTrainingTests() completed successfully
		0xB2	error	SMU FW Successfully loaded to SMU Secure DRAM
		0xB3	error	Sent all required boot time messages to SMU
		0xB4	error	Validated and ran Security Gasket binary
		0xB5	error	UMC Keys generated and programmed
		0xB6	error	Inline AES key wrapper stored in DRAM
		0xB7	error	Completed FW Validation step
		0xB8	error	Completed FW Validation step
		0xB9	error	BIOS copy from SPI to DRAM complete
		0xBA	error	Completed FW Validation step

(continued on the next page)

ACTION	PHASE	POST CODE	TYPE	DESCRIPTION
PSP Boot	PSP Boot Loader phase (Status Post Codes)	0xBB	error	BIOS load process fully complete
		0xBC	error	Bootloader successfully release x86
		0xBD	error	Early Secure Debug completed
		0xBE	error	GetFWVersion command received from BIOS is completed
		0xBF	error	SMIInfo command received from BIOS is completed
		0xC0	error	Successfully entered WarmBootResume()
		0xC1	error	Successfully copied SecureOS image to SRAM
		0xC2	error	Successfully copied trustlets to PSP Secure Memory
		0xC3	error	About to jump to Secure OS (SBL about to copy and jump)
		0xC4	error	Successfully restored CCP and UMC state on S3 resume
		0xC5	error	PSP SRAM HMAC validated by Mini BL
		0xC6	error	About to jump to <t-base in Mini BL
		0xC7	error	VMG ECDH unit test started
		0xC8	error	VMG ECDH unit test passed
		0xC9	error	VMG ECC CDH primitive unit test started
		0xCA	error	VMG ECC CDH primitive unit test passed
		0xCB	error	VMG SP800-108 KDF-CTR HMAC unit test started
		0xCC	error	VMG SP800-108 KDF-CTR HMAC unit test passed
		0xCD	error	VMG LAUNCH_* test started
		0xCE	error	VMG LAUNCH_* test passed
		0xCF	error	MP1 has been taken out of reset, and executing SMUFW
		0xD0	error	PSP and SMU Reserved Addresses correct
		0xD1	error	Reached Naples steady-state WFI loop
		0xD2	error	Knoll device successfully initialized
		0xD3	error	32-byte RandOut successfully returned from Knoll
		0xD4	error	32-byte MAC successfully received from Knoll.
		0xD5	error	Knoll device verified successfully
		0xD6	error	CNLI Keys generated and programmed
		0xD7	error	Enter recovery mode due to trustlet validation fail.
		0xD8	error	Enter recovery mode due to OS validation fail.
		0xD9	error	Enter recovery mode due to OEM public key not found.
		0xDA	error	Enter recovery mode with header corruption
		0xDB	error	We should not treat this error as blocking
		0xDC	error	When same fw image type is already loaded in SRAM
		0xDD	error	0xE2 progress codes are available
		0xE0	error	Unlock return
		0xE2	error	Token expiration reset triggered
		0xE3	error	Completed DXIO PHY SRAM FW key Validation step
		0xE4	error	MP1 firmware load to SRAM success
		0xE5	error	Bootloader read the MP1 SRAM successfully
		0xE6	error	Bootloader successfully reset MP1
		0xE7	error	DF init successfully done (in absence of AGESA)
		0xE8	error	UMC init successfully done (in absence of AGESA)
		0xE9	error	LX6 Boot ROM code ready
		0xEA	error	Bootloader successfully asserted LX6 reset
		0xEB	error	LX6 load to SRAM success
		0xEC	error	Bootloader successfully set LX6 reset vector to SRAM
		0xED	error	Bootloader successfully de-asserted LX6 reset
		0xEE	error	LX6 firmware is running and ready
		0xEF	error	Loading of S3 image done successfully
		0xF0	error	Bootloader successfully verify signed image using 4K/2K key
		0xF1	error	Bootloader identified as running on SP32P or multi-socket boot
		0xF2	error	Security Policy check successful (only in secure boot)
		0xF3	error	Bootloader successfully loaded SS3
		0xF4	error	Bootloader successfully load fTPM Driver
		0xF5	error	Bootloader successfully loaded sys_drv
		0xF6	error	Bootloader successfully loaded secure OS
		0xF7	error	Bootloader about to transfer control to secureOS
		0xFF	error	Bootloader sequence finished
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

(continued on the next page)

ACTION	PHASE	POST CODE	TYPE	DESCRIPTION
Quick VGA	DXE(Driver Execution Environment) phase	0x32	Progress	CPU POST-Memory Initialization
		0x33	Progress	CPU Cache Initialization
		0x34	Progress	Application Processor(s) (AP) Initialization
		0x35	Progress	BSP Selection
		0x36	Progress	CPU Initialization
		0x37	Progress	Pre-memory NB Initialization
		0x3B	Progress	Pre-memory SB Initialization
		0x4F	Progress	DXE Initial Program Load(IPL)
		0x60	Progress	DXE Core Started
		0x61	Progress	DXE NVRAM Initialization
		0x62	Progress	SB run-time Initialization
		0x63	Progress	CPU DXE Initialization
		0x68	Progress	PCI HB Initialization
		0x69	Progress	NB DXE Initialization
		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
		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 output 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
		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
	Operating system phase	0xAA	Progress	APIC mode
		0xAC	Progress	PIC mode

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.

NOTE: 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(A)/NMB(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(A)/NMB(A)

Australia statement notice

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

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

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

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

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 https://esg.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 https://esg.asus.com/Compliance.htm.

EU RoHS

This product complies with the EU RoHS Directive. For more details, see https://esg.asus.com/Compliance.htm

Japan JIS-C-0950 Material Declarations

Information on Japan RoHS (JIS-C-0950) chemical disclosures is available on https://esg.asus.com/Compliance.htm

India RoHS

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

Vietnam RoHS

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

Các sản phẩm ASUS bán tại Việt Nam, vào ngày 23 tháng 9 năm2011 trở về sau, đều phải đáp ứng các yêu cầu của Thông tư 30/2011/TT-BCT của Việt Nam.

Türkiye RoHS

AEEE Yönetmeliğine Uygundur

ASUS Recycling/Takeback Services

ASUS recycling and takeback programs come from our commitment to the highest standards for protecting our environment. We believe in providing solutions for you to be able to responsibly recycle our products, batteries, other components as well as the packaging materials. Please go to https://esg.asus.com/en/Takeback.htm for detailed recycling information in different regions.

Ecodesign Directive

The 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 at https://esg.asus.com/Compliance.htm.

インターネット回線への接続に関するご注意

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。

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.

Safety Precautions

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

安全上のご注意

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

Access Advance Patent Notice

Simplified EU Declaration of Conformity

English ASUSTeK Computer Inc. hereby declares that this device is in compliance with the essential requirements and other relevant provisions of related Directives. Full text of EU declaration of conformity is available at: www.asus.com/support

Français AsusTek Computer Inc. déclare par la présente que cet appareil est conforme aux critères essentiels et autres clauses pertinentes des directives concernées. La déclaration de conformité de l'UE peut être téléchargée à partir du site Internet suivant : www.asus.com/support

Deutsch ASUSTeK Computer Inc. erklärt hiermit, dass dieses Gerät mit den wesentlichen Anforderungen und anderen relevanten Bestimmungen der zugehörigen Richtlinien übereinstimmt. Der gesamte Text der EU-Konformitätserklärung ist verfügbar unter: www.asus.com/support

Italiano ASUSTeK Computer Inc. con la presente dichiara che questo dispositivo è conforme ai requisiti essenziali e alle altre disposizioni pertinenti con le direttive correlate. Il testo completo della dichiarazione di conformità UE è disponibile all'indirizzo: www.asus.com/support

Русский Компания ASUS заявляет, что это устройство соответствует основным требованиям и другим соответствующим условиям соответствующих директив. Подробную информацию, пожалуйста, смотрите на www.asus.com/support

Български С настоящото ASUSTeK Computer Inc. декларира, че това устройство е в съответствие със съществените изисквания и другите приложими постановления на свързаните директиви. Пълният текст на декларацията за съответствие на ЕС е достъпна на адрес: www.asus.com/support

Hrvatski ASUSTeK Computer Inc. ovim izjavljuje da je ovaj uređaj sukladan s bitnim zahtjevima i ostalim odgovarajućim odredbama vezanih direktiva. Cijeli tekst EU izjave o sukladnosti dostupan je na: www.asus.com/support

Čeština Společnost ASUSTeK Computer Inc. tímto prohlašuje, že toto zařízení splňuje základní požadavky a další příslušná ustanovení souvisejících směrnic. Plné znění prohlášení o shodě EU je k dispozici na adrese: www.asus.com/support

Dansk ASUSTeK Computer Inc. erklærer hermed, at denne enhed er i overensstemmelse med hovedkravene og andre relevante bestemmelser i de relaterede direktiver. Hele EU-overensstemmelseserklæringen kan findes på: www.asus.com/support

Nederlands ASUSTeK Computer Inc. verklaart hierbij dat dit apparaat voldoet aan de essentiële vereisten en andere relevante bepalingen van de verwante richtlijnen. De volledige tekst van de EU-verklaring van conformiteit is beschikbaar op: www.asus.com/support

Eesti Käesolevaga kinnitab ASUSTeK Computer Inc, et see seade vastab asjakohaste direktiivide oluliste nõuetele ja teistele asjassepuutuvatele sätetele. EL vastavusdeklaratsiooni täielik tekst on saadaval järgmisel aadressil: www.asus.com/support

Suomi ASUSTeK Computer Inc. ilmoittaa täten, että tämä laite on asiaankuuluvien direktiivien olennaisten vaatimusten ja muiden tätä koskevien säädösten mukainen. EU-yhdenmukaisuusilmoituksen koko teksti on luettavissa osoitteessa: www.asus.com/support

Ελληνικά Με το παρόν, η AsusTek Computer Inc. δηλώνει ότι αυτή η συσκευή συμμορφώνεται με τις θεμελιώδεις απαιτήσεις και άλλες σχετικές διατάξεις των Οδηγιών της ΕΕ. Το πλήρες κείμενο της δήλωσης συμβατότητας είναι διαθέσιμο στη διεύθυνση: www.asus.com/support

Magyar Az ASUSTeK Computer Inc. ezennel kijelenti, hogy ez az eszköz megfelel a kapcsolódó Irányelvek lényeges követelményeinek és egyéb vonatkozó rendelkezéseinek. Az EU megfelelőségi nyilatkozat teljes szövege innen letölthető: www.asus.com/support

Latviski ASUSTeK Computer Inc. ar šo paziņo, ka šī ierīce atbilst saistīto Direktīvu būtiskajām prasībām un citiem citiem saistošajiem nosacījumiem. Pilns ES atbilstības paziņojuma teksts pieejams šeit: www.asus.com/support

Lietuvių „ASUSTeK Computer Inc.“ šiuo tvirtina, kad šis įrenginys atitinka pagrindinius reikalavimus ir kitas svarbias susijusių direktyvų nuostatas. Visą ES atitikties deklaracijos tekstą galima rasti: www.asus.com/support

Norsk ASUSTeK Computer Inc. erklærer herved at denne enheten er i samsvar med hovedsaklige krav og andre relevante forskrifter i relaterte direktiver. Fullstendig tekst for EU-samsvarserklæringen finnes på: www.asus.com/support

Polski Firma ASUSTeK Computer Inc. niniejszym oświadcza, że urządzenie to jest zgodne z zasadniczymi wymogami i innymi właściwymi postanowieniami powiązanych dyrektyw. Pełny tekst deklaracji zgodności UE jest dostępny pod adresem: www.asus.com/support

Português A ASUSTeK Computer Inc. declara que este dispositivo está em conformidade com os requisitos essenciais e outras disposições relevantes das Diretivas relacionadas. Texto integral da declaração da UE disponível em: www.asus.com/support

Română ASUSTeK Computer Inc. declară că acest dispozitiv se conformează cerinţelor esenţiale şi altor prevederi relevante ale directivelor conexe. Textul complet al declaraţiei de conformitate a Uniunii Europene se găseşte la: www.asus.com/support

Srpski ASUSTeK Computer Inc. ovim izjavljuje da je ovaj uređaj u saglasnosti sa osnovnim zahtevima i drugim relevantnim odredbama povezanih Direktiva. Pun tekst EU deklaracije o usaglašenosti je dostupan da adresi: www.asus.com/support

Slovensky Spoločnosť ASUSTeK Computer Inc. týmto vyhlasuje, že toto zariadenie vyhovuje základným požiadavkám a ostatým príslušným ustanoveniam príslušných smerníc. Celý text vyhlásenia o zhode pre štáty EÚ je dostupný na adrese: www.asus.com/support

Slovenščina ASUSTeK Computer Inc. izjavlja, da je ta naprava skladna z bistvenimi zahtevami in drugimi ustreznimi določbami povezanih direktiv. Celotno besedilo EU-izjave o skladnosti je na voljo na spletnem mestu: www.asus.com/support

Español Por la presente, ASUSTeK Computer Inc. declara que este dispositivo cumple los requisitos básicos y otras disposiciones pertinentes de las directivas relacionadas. El texto completo de la declaración de la UE de conformidad está disponible en: www.asus.com/support

Svenska ASUSTeK Computer Inc. förklarar härmed att denna enhet överensstämmer med de grundläggande kraven och andra relevanta föreskrifter i relaterade direktiv. Fulltext av EU-försäkran om överensstämmelse finns på: www.asus.com/support

Українська ASUSTeK Computer Inc. заявляє, що цей пристрій відповідає основним вимогам та іншим відповідним положенням відповідних Директив. Повний текст декларації відповідності стандартам ЄС доступний на: www.asus.com/support

Türkçe AsusTek Computer Inc., bu aygıtın temel gereksinimlerle ve ilişkili Yönergelerin diğer ilgili koşullarıyla uyumlu olduğunu beyan eder. AB uygunluk bildiriminin tam metni şu adreste bulunabilir: www.asus.com/support

Bosanski ASUSTeK Computer Inc. ovim izjavljuje da je ovaj uređaj usklađen sa bitnim zahtjevima i ostalim odgovarajućim odredbama vezanih direktiva. Cijeli tekst EU izjave o usklađenosti dostupan je na: www.asus.com/support

Simplified UKCA Declaration of Conformity

ASUSTeK Computer Inc. hereby declares that this device is in compliance with the essential requirements and other relevant provisions of related Regulations. Full text of UKCA declaration of conformity is available at: www.asus.com/support

Service and Support

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