GIGABYTE™

R161-R12

High Efficiency Liquid Cooling System

User Manual

Rev. 1.1

Copyright

Disclaimer

Information in this manual is protected by copyright laws and is the property of GIGABYTE. Changes to the specifications and features in this manual may be made by GIGABYTE without prior notice. No part of this manual may be reproduced, copied, translated, transmitted, or published in any form or by any means without GIGABYTE's prior written permission.

Documentation Classifications

In order to assist in the use of this product, GIGABYTE provides the following types of documentation:

- User Manual: detailed information & steps about the installation, configuration and use this product (e.g. motherboard, server barebones), covering hardware and BIOS.
- User Guide: detailed information about the installation & use of an add-on hardware or software component (e.g. BMC firmware, rail-kit) compatible with this product.
- Quick Installation Guide: a short guide with visual diagrams that you can reference easily for installation purposes of this product (e.g. motherboard, server barebones).

Please see the support section of the online product page to check the current availability of these documents

For More Information

For related product specifications, the latest firmware and software, and other information, please visit our website at: http://www.gigabyte.com.

For GIGABYTE distributors and resellers, additional sales & marketing materials are available from our reseller portal: http://reseller.b2b.gigabyte.com

For further technical assistance, please contact your GIGABYTE representative or visit http://esupport.gigabyte.com/ to create a new support ticket.

For any general sales or marketing enquires, you may message GIGABYTE server directly by email: server.grp@gigabyte.com.

Conventions

The following conventions are used in this user's guide:

✎	**NOTE!** Gives bits and pieces of additional information related to the current topic.
⚠	**CAUTION!** Gives precautionary measures to avoid possible hardware or software problems.
⚠	**WARNING!** Alerts you to any damage that might result from doing or not doing specific actions.

Server Warnings and Cautions

Before installing a server, be sure that you understand the following warnings and cautions.

WARNING!

To reduce the risk of electric shock or damage to the equipment:

- Do not disable the power cord grounding plug. The grounding plug is an important safety feature.
- Plug the power cord into a grounded (earthed) electrical outlet that is easily accessible at all times.
- Unplug the power cord from the power supply to disconnect power to the equipment.
- Do not route the power cord where it can be walked on or pinched by items placed against it. Pay particular attention to the plug, electrical outlet, and the point where the cord extends from the server.

WARNING!

To reduce the risk of personal injury from hot surfaces, allow the drives and the internal system components to cool before touching them.

WARNING!

This server is equipped with high speed fans. Keep away from hazardous moving fan blades during servicing.

CAUTION!

- Do not operate the server for long periods with the access panel open or removed. Operating the server in this manner results in improper airflow and improper cooling that can lead to thermal damage.
- Danger of explosion if battery is incorrectly replaced.
- Replace only with the same or equivalent type recommended by the manufacturer.
- Dispose of used batteries according to the manufacturer’s instructions.

Electrostatic Discharge (ESD)

⚠ **CAUTION!**

ESD CAN DAMAGE DRIVES, BOARDS, AND OTHER PARTS. WE RECOMMEND THAT YOU PERFORM ALL PROCEDURES AT AN ESD WORKSTATION. IF ONE IS NOT AVAILABLE, PROVIDE SOME ESD PROTECTION BY WEARING AN ANTI-STATIC WRIST STRAP ATTACHED TO CHASSIS GROUND -- ANY UNPAINTED METAL SURFACE -- ON YOUR SERVER WHEN HANDLING PARTS.

Always handle boards carefully. They can be extremely sensitive to ESD. Hold boards only by their edges without any component and pin touching. After removing a board from its protective wrapper or from the system, place the board component side up on a grounded, static free surface. Use a conductive foam pad if available but not the board wrapper. Do not slide board over any surface.

System power on/off: To remove power from system, you must remove the system from rack. Make sure the system is removed from the rack before opening the chassis, adding, or removing any non hot-plug components.

Hazardous conditions, devices and cables: Hazardous electrical conditions may be present on power, telephone, and communication cables. Turn off the system and discon-nect the cables attached to the system before servicing it. Otherwise, personal injury or equipment damage can result.

Electrostatic discharge (ESD) and ESD protection: ESD can damage drives, boards, and other parts. We recommend that you perform all procedures in this chapter only at an ESD workstation. If one is not available, provide some ESD protection by wearing an antistatic wrist strap attached to chassis ground (any unpainted metal surface on the server) when handling parts.

ESD and handling boards: Always handle boards carefully. They can be extremely sensi-tive to electrostatic discharge (ESD). Hold boards only by their edges. After removing a board from its protective wrapper or from the system, place the board component side up on a grounded, static free surface. Use a conductive foam pad if available but not the board wrapper. Do not slide board over any surface.

Installing or removing jumpers: A jumper is a small plastic encased conductor that slips over two jumper pins. Some jumpers have a small tab on top that can be gripped with fin-gertips or with a pair of fine needle nosed pliers. If the jumpers do not have such a tab, take care when using needle nosed pliers to remove or install a jumper; grip the narrow sides of the jumper with the pliers, never the wide sides. Gripping the wide sides can dam-age the contacts inside the jumper, causing intermittent problems with the function con-trolled by that jumper. Take care to grip with, but not squeeze, the pliers or other tool used to remove a jumper, or the pins on the board may bend or break.

⚠ **CAUTION!**

Risk of explosion if battery is replaced incorrectly or with an incorrect type. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer’s instructions.

Table of Contents

Chapter 1 Hardware Installation

1-1 Installation Precautions

The motherboard/system contain numerous delicate electronic circuits and components which can become damaged as a result of electrostatic discharge (ESD). Prior to installation, carefully read the service guide and follow these procedures:

- Prior to installation, do not remove or break motherboard S/N (Serial Number) sticker or warranty sticker provided by your dealer. These stickers are required for warranty validation.
- Always remove the AC power by unplugging the power cord from the power outlet before installing or removing the motherboard or other hardware components.
- When connecting hardware components to the internal connectors on the motherboard, make sure they are connected tightly and securely.
- When handling the motherboard, avoid touching any metal leads or connectors.
- It is best to wear an electrostatic discharge (ESD) wrist strap when handling electronic components such as a motherboard, CPU or memory. If you do not have an ESD wrist strap, keep your hands dry and first touch a metal object to eliminate static electricity.
- Prior to installing the motherboard, please have it on top of an antistatic pad or within an electrostatic shielding container.
- Before unplugging the power supply cable from the motherboard, make sure the power supply has been turned off.
- Before turning on the power, make sure the power supply voltage has been set according to the local voltage standard.
- Before using the product, please verify that all cables and power connectors of your hardware components are connected.
- To prevent damage to the motherboard, do not allow screws to come in contact with the motherboard circuit or its components.
- Make sure there are no leftover screws or metal components placed on the motherboard or within the computer casing.
- Do not place the computer system on an uneven surface.
- Do not place the computer system in a high-temperature environment.
- Turning on the computer power during the installation process can lead to damage to system components as well as physical harm to the user.
- If you are uncertain about any installation steps or have a problem related to the use of the product, please consult a certified computer technician.

1-2 Product Specifications

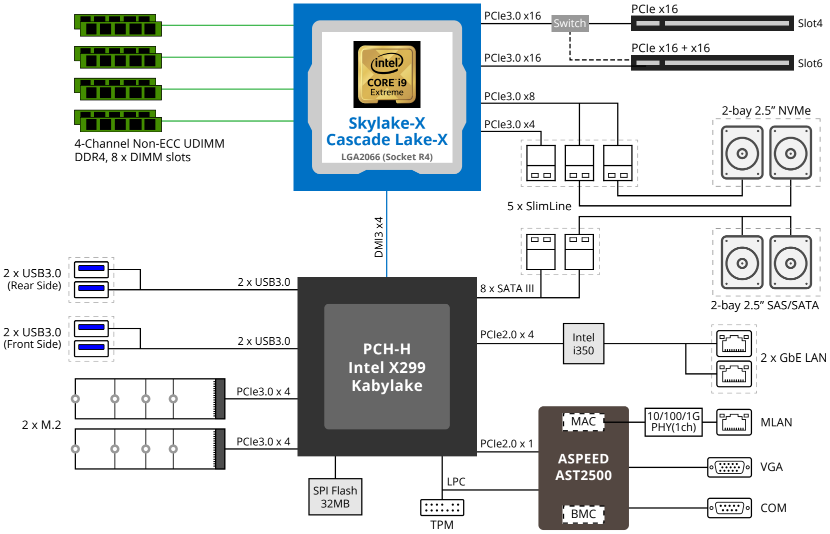
CPU	◆ Intel® Core™ X series 44-lane/28-lane processors
Socket	◆ Intel® Core™ X series 44-lane/28-lane processors
Chipset	◆ System on Chip
Memory	◆ 8 x DIMM slots ◆ DDR4 memory modules supported only ◆ Quad channel memory architecture ◆ Support for non-ECC Un-buffered DIMM ◆ DDR4 modules: 2667/2400/2133 MHz
LAN	◆ 2 x 1Gb/s LAN ports (Intel® I350-AM2) ◆ 1 x 10/100/1000 management LAN
Expansion Slot	◆ 1 x PCIe x16 slots (Gen3 x16), Low profile half-length* ◆ * The PCIe slot is unavailable for system level ◆ * The PCIe slot is shared with riser card 1 x PCIe x16 signal **Riser Card CRS1027:** ◆ 1 x PCIe x16 slots (Gen3 x16), Low profile half-length ◆ -1 x PCIe x16 slots (Gen3 x16), Low profile half-length 2 x M.2 slots: ◆ - M-key ◆ - PCIe Gen3 x4 ◆ - Supports NGFF-2242/2260/2280 cards
Video	◆ Integrated in Aspeed® AST2500 ◆ 2D Video Graphic Adapter with PCIe bus interface ◆ 1920x1200@60Hz 32bpp, DDR4 SDRAM
Storage	◆ 2 x U.2, 2 x SATA/SAS or 4 x SATA/SAS hot-swappable HDD/SSD bays ◆ 2.5" HDD supported only
SATA	◆ Supported
SAS	◆ Supported via add-on SAS Card

Internal Connectors	◆ 3 x Power supply connectors ◆ 5 x SlimSAS connectors ◆ 2 x fan headers ◆ 1 x USB 3.0 header ◆ 1 x TPM header ◆ 1 x VROC connector ◆ 1 x Front panel header ◆ 1 x HDD back plane board header ◆ 1 x IPMB connector ◆ 1 x Clear CMOS jumper ◆ 1 x BIOS recovery jumper
Front Panel LED/Buttons	◆ 2 x USB 3.0 ◆ 1 x Power button with LED ◆ 1 x ID button with LED ◆ 1 x Reset button ◆ 1 x NMI button ◆ 1 x System status LED ◆ 1 x HDD activity LED ◆ 2 x LAN activity LEDs
Rear Panel I/O	◆ 2 x USB 3.0 ◆ 1 x VGA ◆ 1 x COM ◆ 2 x RJ45 ◆ 1 x MLAN
Backplane I/O	◆ Bandwidth: SATAIII 6Gb/s or SAS 12Gb/s or U.2 PCIe Gen3 x4 per port
TPM	◆ 1 x TPM header with LPC interface ◆ Optional TPM2.0 kit: CTM000

System Management	◆ Aspeed® AST2500 management controller ◆ Avocent® MergePoint IPMI 2.0 web interface: ◆ Network settings ◆ Network security settings ◆ Hardware information ◆ Users control ◆ Services settings ◆ IPMI settings ◆ Sessions control ◆ LDAP settings ◆ Power control ◆ Fan profiles ◆ Voltages, fans and temperatures monitoring ◆ System event log ◆ Events management (platform events, trap settings, email settings) ◆ Serial Over LAN ◆ vKVM & vMedia (HTML5)
Power Supply	◆ 2 x 1100W redundant PSUs ◆ 80 PLUS Platinum ◆ AC Input: ◆ - 100-240V~/ 12-6A, 50-60Hz ◆ DC Input: ◆ - 190-310Vdc/ 7A ◆ DC Output: ◆ - Max 850W/ 100-240Vac~ ◆ +12V/ 70A ◆ +5Vsb/ 3A ◆ - Max 1100W/ 200-240Vac ◆ +12V/ 90.5A ◆ +5Vsb/ 3A
Environment Ambient Temperature Relative Humidity	◆ Operating temperature: 10°C to 35°C ◆ Non-operating temperature: -40°C to 60°C ◆ Operating humidity: 8-80% (non-condensing) ◆ Non-operating humidity: 20%-95% (non-condensing)
System Dimension	◆ 1U ◆ 438mm (W) x 43.5mm (H) x 730mm (D)

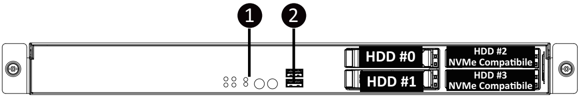
* We reserves the right to make any changes to the product specifications and product-related information without prior notice.

1-3 System Block Diagram



Chapter 2 System Appearance

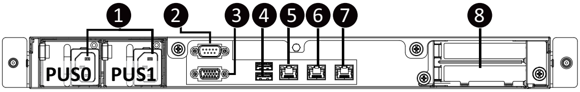
2-1 Front View



No.	Description
1.	Front Panel LEDs and buttons
2.	Front USB 3.0 ports
	Orange HDD Latches Support NVMe

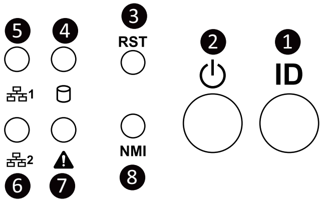
- Please Go to Chapter **2-3 Front Panel LED** and Buttons for detail description of function LEDs.

2-2 Rear View



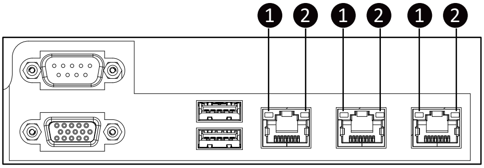
No.	Description
1.	Power Supply Module Cord Socket
2.	Serial Port
3.	VGA Port
4.	USB 3.0 Port x 2
5.	10/100/1000 Server management LAN port
6.	GbE LAN Port #1
7.	GbE LAN Port #2
8.	PCIe Card bay x 2

2-3 Front Panel LED and Buttons



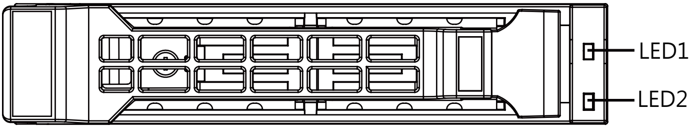
No.	Name	Color	Status	Description
1.	ID Button			Press the button to activate system identification
2.	Power button with LED	Green	On	System is powered on
		Green	Blink	System is in ACPI S1 state (sleep mode)
		N/A	Off	• System is not powered on or in ACPI S5 state (power off) • System is in ACPI S4 state (hibernate mode)
3.	Reset Button			Press the button to reset the system.
4.	HDD Status LED	Green	On	HDD locate
			Blink	HDD access
		Amber	On	HDD fault
		Green/ Amber	Blink	HDD rebuilding
		N/A	Off	No HDD access or no HDD fault.
5/6	LAN 1/2 Active/Link LEDs	Green	Solid On	Link between system and network or no access.
		Green	Blink	Data trasmission or receiving is occuring
		N/A	Off	No data transmission or receiving is occuring
7.	System Status LED	Green	Solid On	System is operating normally.
		Amber	Solid On	Critical condition, may indicate: System fan failure System temperature
			Blink	Non-critical condition, may indicate: Redundant power module failure Temperature and voltage issue Chassis intrusion
		N/A	Off	System is not ready, may indicate: POST error NMI error Processor or terminator missing
8.	NMI button			Press the button server generates a NMI to the processor if the multiple-bit ECC errors occur, which effectively halt the server.

2-4 Rear System LAN LEDs



No.	Name	Color	Status	Description
1.	1GbE Speed LED	Yellow	On	1 Gbps data rate
		Green	On	100 Mbps data rate
		N/A	Off	10 Mbps data rate
2.	1GbE Link/ Activity LED	Green	On	Link between system and network or no access
			Blink	Data transmission or receiving is occurring
		N/A	Off	No data transmission or receiving is occurring

2-5 Hard Disk Drive LEDs



RAID SKU	LED1	Locate	HDD Fault	Rebuilding	HDD Access	HDD Present (No Access)
No RAID configuration (via HBA, ICH)	Disk LED (LED on Back Panel)	Green	ON(*1)	OFF	Green	OFF
		Amber	OFF	OFF	Amber	OFF
	Removed HDD Slot (LED on Back Panel)	Green	ON(*1)	OFF	Green	--
		Amber	OFF	OFF	Amber	--
RAID configuration (via HW RAID Card or SW RAID Card)	Disk LED	Green	ON	OFF	Alternately	OFF
		Amber	OFF	ON	(Low Speed: 2 Hz)	OFF
	Removed HDD Slot	Green	ON(*1)	OFF	(*3)	--
		Amber	OFF	ON	(*3)	--

LED 2	HDD Present	No HDD
Green	ON	OFF

NOTE:

*1: Depends on HBA/Utility Spec.

*2: Blink cycle depends on HDD's activity signal.

*3: If HDD is pulled out during rebuilding, the disk status of this HDD is regarded as faulty.

Chapter 3 System Hardware Installation

Pre-installation Instructions

Computer components and electronic circuit boards can be damaged by discharges of static electricity. Working on computers that are still connected to a power supply can be extremely dangerous. Follow the simple guidelines below to avoid damage to your computer or injury to yourself.

- Always disconnect the computer from the power outlet whenever you are working inside the computer case.
- If possible, wear a grounded wrist strap when you are working inside the computer case. Alternatively, discharge any static electricity by touching the bare metal system of the computer case, or the bare metal body of any other grounded appliance.
- Hold electronic circuit boards by the edges only. Do not touch the components on the board unless it is necessary to do so. Do not flex or stress the circuit board.
- Leave all components inside the static-proof packaging until you are ready to use the component for the installation.

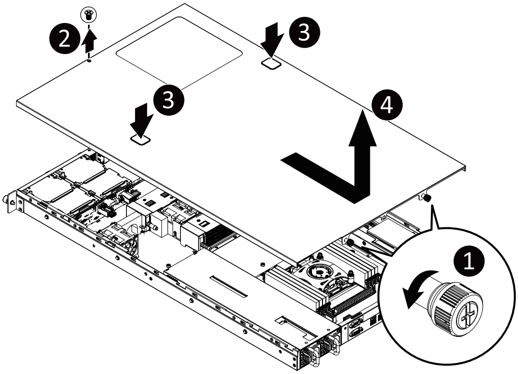
3-1 Removing Chassis Cover

Before you remove or install the system cover

- Make sure the system is not turned on or connected to AC power.

Follow these instructions to remove the system cover:

1. Loosen and the two thumbscrew at the rear of the system.
2. Remove the single secrew at the front of the system.
3. Push down the indentation located at the side of the back chassis
4. Using the grip areas on the top cover and slide the cover horizontally in the direction of the arrow.



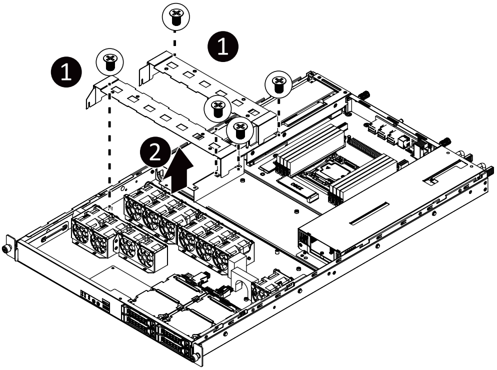
3-2 Installing the Liquid Cooling Module

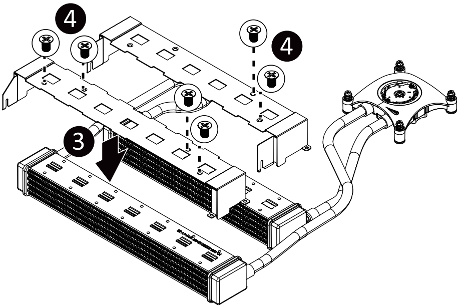
Before you remove or install the liquid cooling module:

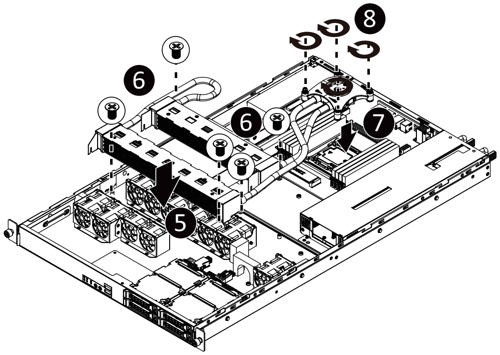
- Make sure the system is not turned on or connected to AC power.

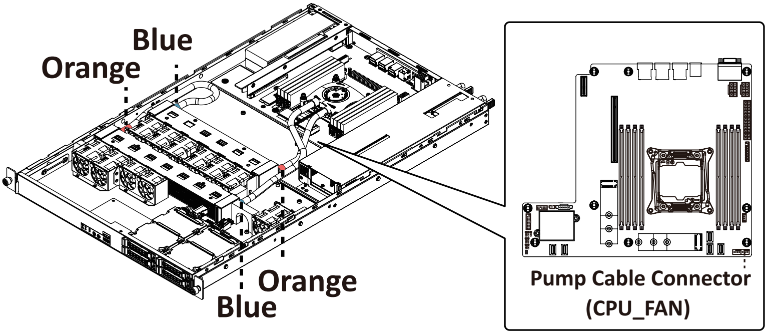
Follow these instructions to install the liquid cooling module:

1. Remove the screws securing brackets .
2. Remove the brackets from the system.
3. Engage the brackets and radiators.
4. Secure the brackets and radiators with 6 screws.
5. Lock the four spring screws.
   NOTE! Remove the pump grease protection cover before installing the pump.
6. Install the fan duct and secure with 2 screws.
7. Connect pump cable to motherboard.






8
6
6
7
5


Blue
Orange
Orange
Blue
Pump Cable Connector
(CPU_FAN)

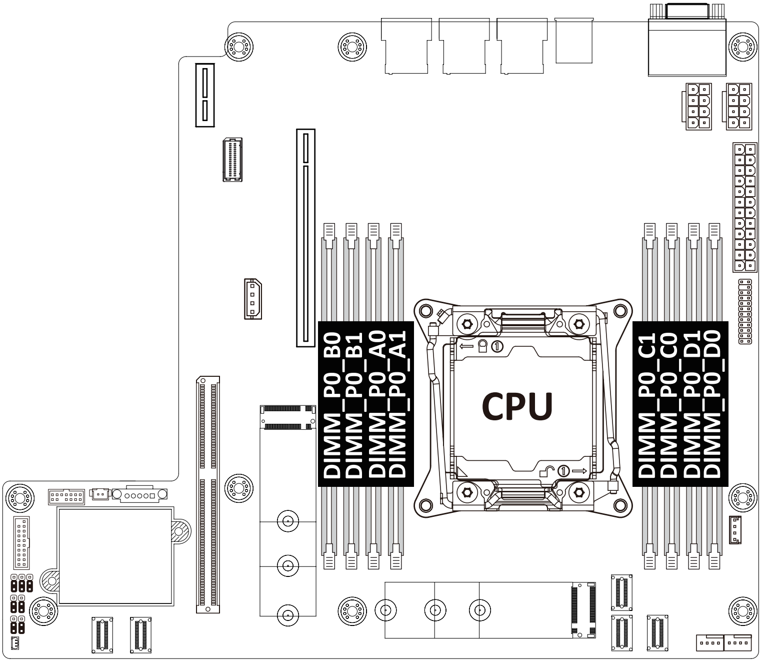
3-3 Installing the Memory

Read the following guidelines before you begin to install the memory:

- Make sure that the motherboard supports the memory. It is recommended that memory of the same capacity, brand, speed, and chips be used.
- Always turn off the computer and unplug the power cord from the power outlet before installing the memory to prevent hardware damage.
- Memory modules have a foolproof design. A memory module can be installed in only one direction. If you are unable to insert the memory, switch the direction.

3-3-1 Four Channel Memory Configuration

This motherboard provides 8 DDR4 memory sockets and supports Four Channel Technology. After the memory is installed, the BIOS will automatically detect the specifications and capacity of the memory. Enabling Four Channel memory mode will be four times of the original memory bandwidth.



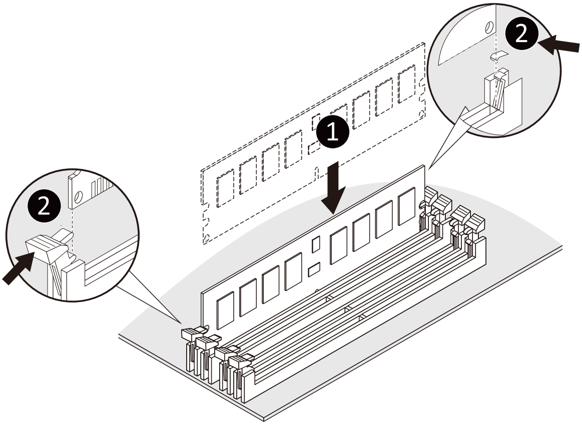
3-3-2 Installing a Memory

Before installing a memory module, make sure to turn off the computer and unplug the power cord from the power outlet to prevent damage to the memory module.

Be sure to install DDR4 DIMMs on this motherboard.

Follow these instructions to install the Memory:

1. Insert the DIMM memory module vertically into the DIMM slot, and push it down.
2. Close the plastic clip at both edges of the DIMM slots to lock the DIMM module.
3. Reverse the installation steps when you want to remove the DIMM module.



3-3-3 DIMM Population Table

Type	Ranks Per DIMM and Data Width	DIMM Capacity (GB)		Speed (MT/s); Voltage (V) Slot Per Channel (SPC) DIMM Per Channel (DPC)		
				1 Slot per Channel	2 Slot per Channel	
		DIMM Density		1DPC	1DPC	2DPC
		4Gb	8Gb	1.2V	1.2V	1.2V
UDIMM	SRx4	4GB	8GB	2666	2666	2666
UDIMM	SRx8	8GB	16GB			
UDIMM	DRx8	8GB	16GB			
UDIMM	DRx8	16GB	32GB			

3-4 Installing the PCI Expansion Card

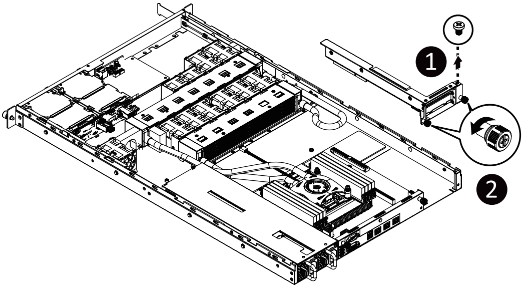
- Voltages can be present within the server whenever an AC power source is connected. This voltage is present even when the main power switch is in the off position. Ensure that the system is powered-down and all power sources have been disconnected from the server prior to installing a PCI card.

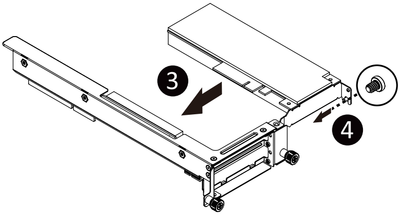
Failure to observe these warnings could result in personal injury or damage to equipment.

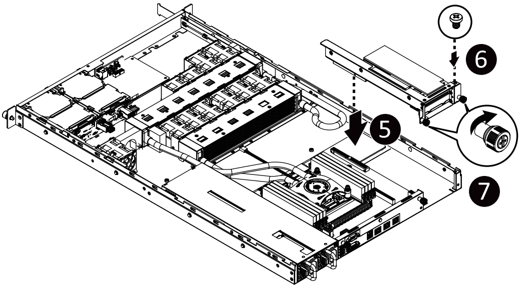
- The PCI riser assembly does not include a riser card or any cabling as standard. To install a PCI card, a riser card must be installed.

Follow these instructions to PCI Expansion card:

1. Remove the securing special screw on the riser bracket.
2. Loosen the thumbscrew on the riser bracket
3. Lift up the riser bracket out of system.
4. Remove the slot covers from the riser bracket.
5. Orient the PCI-E card with the riser guide slot and push in the direction of the arrow until the PCI-E card sits in the PCI card connector.
6. Secure the PCI-E card with the screw.
7. Reverse the steps 3 - 1 to install the riser bracket.







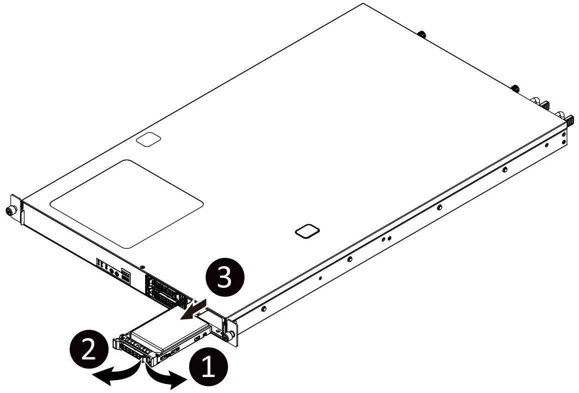
3-5 Installing the Hard Disk Drive

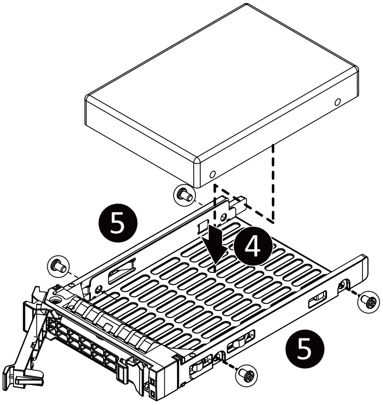
Read the following guidelines before you begin to install the Hard disk drive:

- Take note of the drive tray orientation before sliding it out.
- The tray will not fit back into the bay if inserted incorrectly.
- Make sure that the HDD is connected to the HDD connector on the backplane.

Follow these instructions to install a hard disk drive:

1. Press the release button.
2. Extend the locking lever and pull the locking lever to remove the HDD tray.
3. Place the hard disk drive into the HDD tray.
4. Secure the hard disk drive to the HDD tray with four screws.

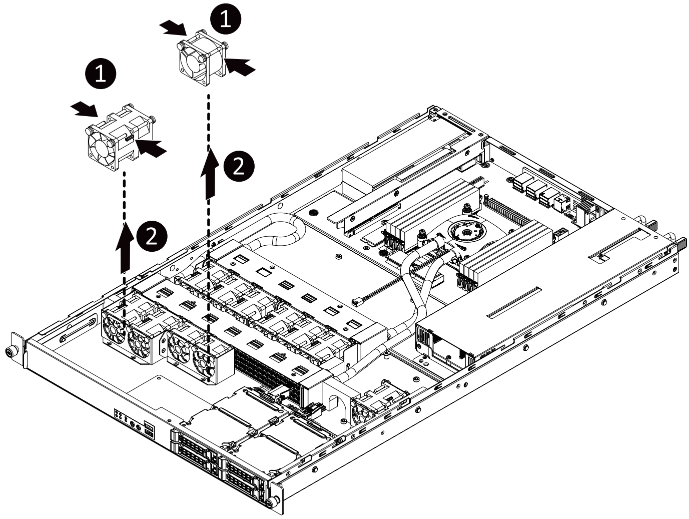




3-6 Replacing the FAN Assemblly

Follow these instructions to replace the fan assembly:

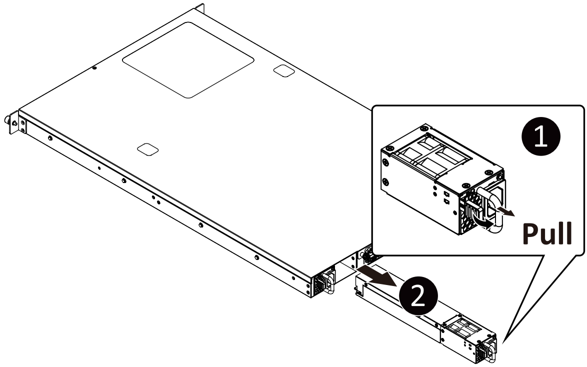
1. Lift up the fan assembly from the chassis.
2. Reverse the previous steps to install the replacement fan assembly.



3-7 Replacing the Power Supply

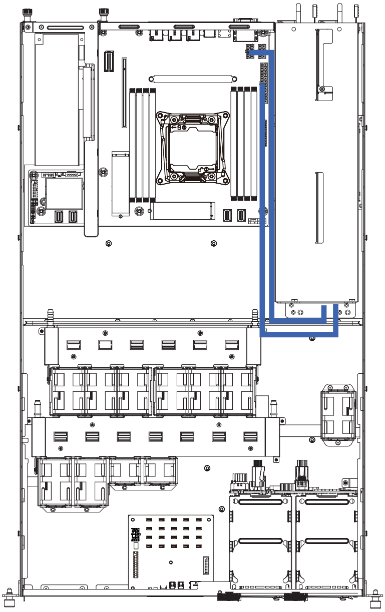
Follow these instructions to replace the power supply:

1. Press the retaining clip on the right side of the power supply along the direction of the arrow.
2. Pull up the power supply handle at the same time and pull out the power supply.
3. Insert the replacement power supply firmly into the chassis. Connect the AC power cord to the replacement power supply.

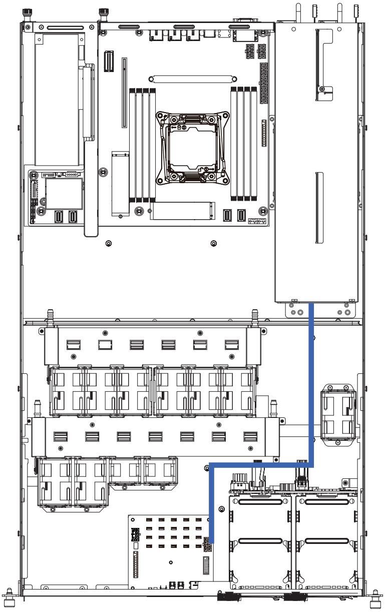


3-8 Cable Routing

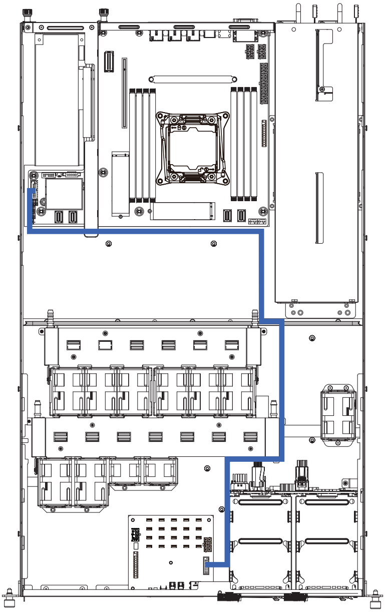
System Power Cable



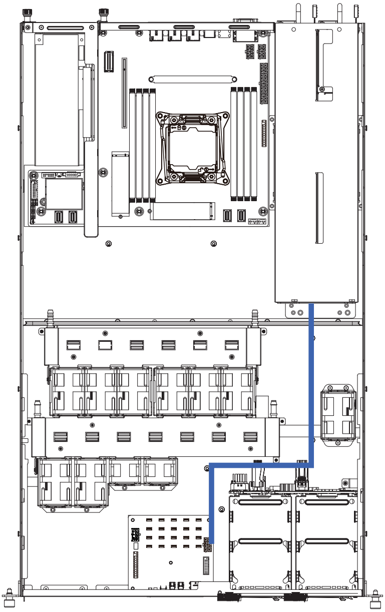
Front IO Board Power Cable



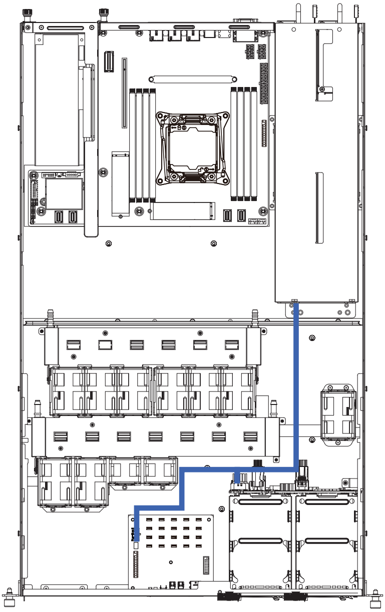
Front Panel USB 3.0 Cable



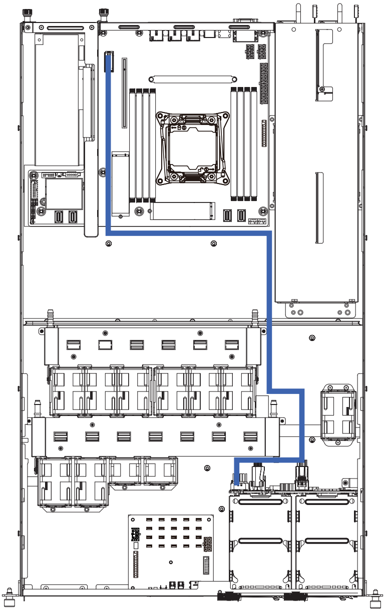
Front IO Board Power Cable



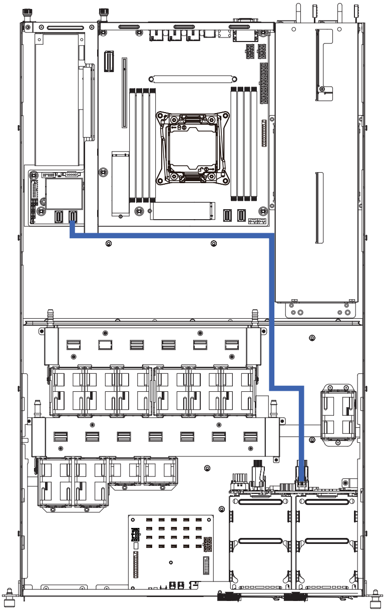
HDD Back Plane Board Power Cable



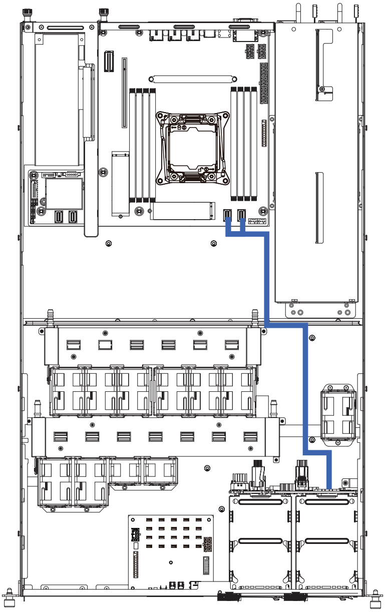
HDD Back Plane Board Signal Cable



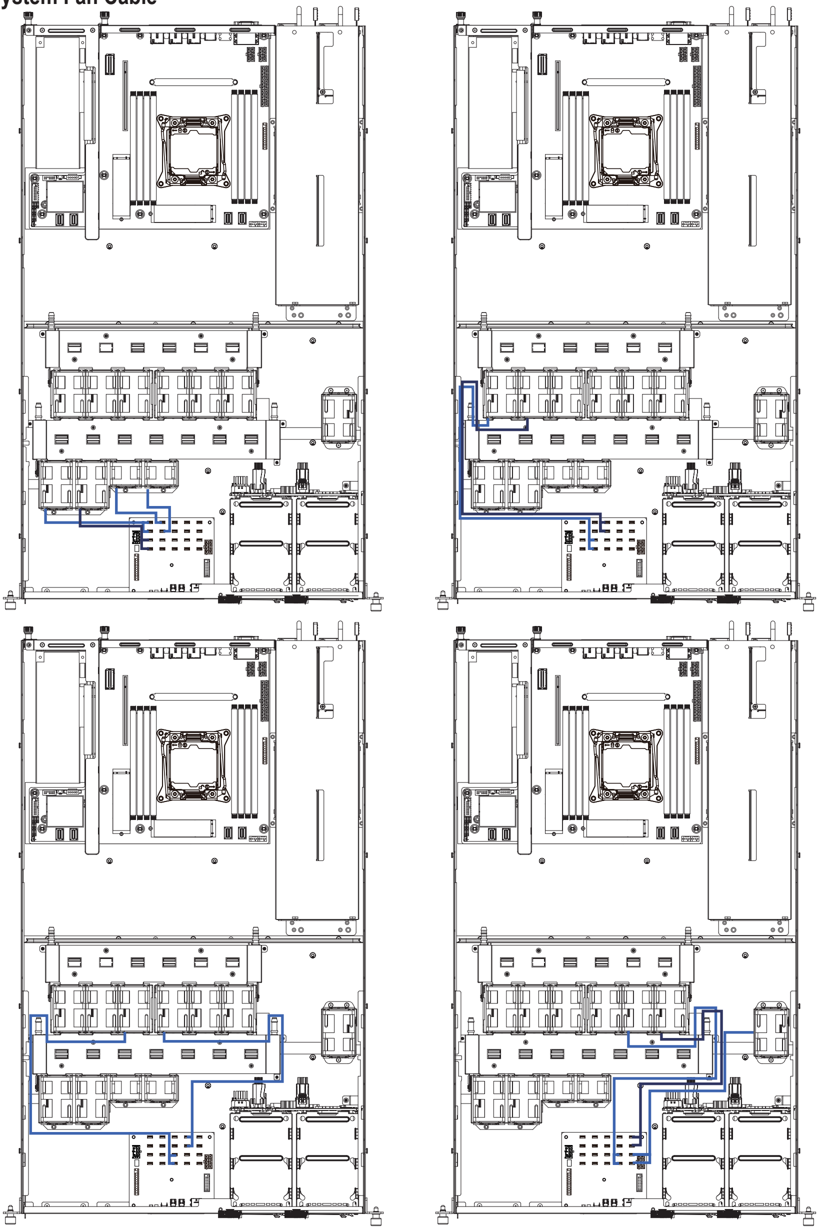
On-Board SATA to HDD Back Plane Board Cable



NVMe Cable



System Fan Cable

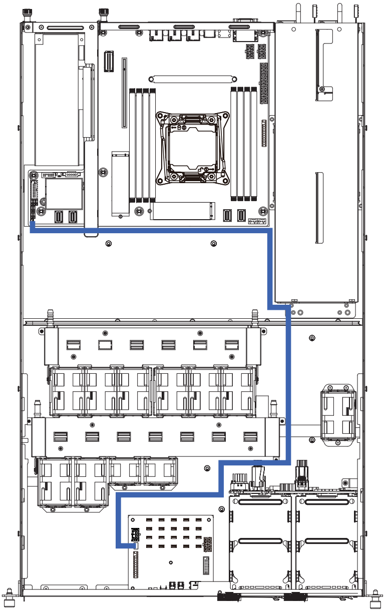


CAUTION!

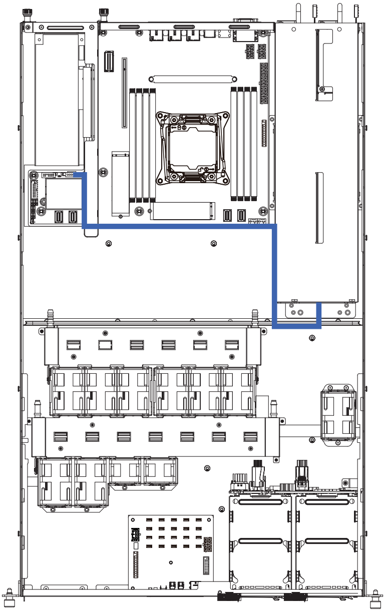
To connect system fan connector, follow the instruction:

- Black/Red cable connect to odd numbered connector.
- White/Amber cable connect to even numbered connector.

SMBus Cable

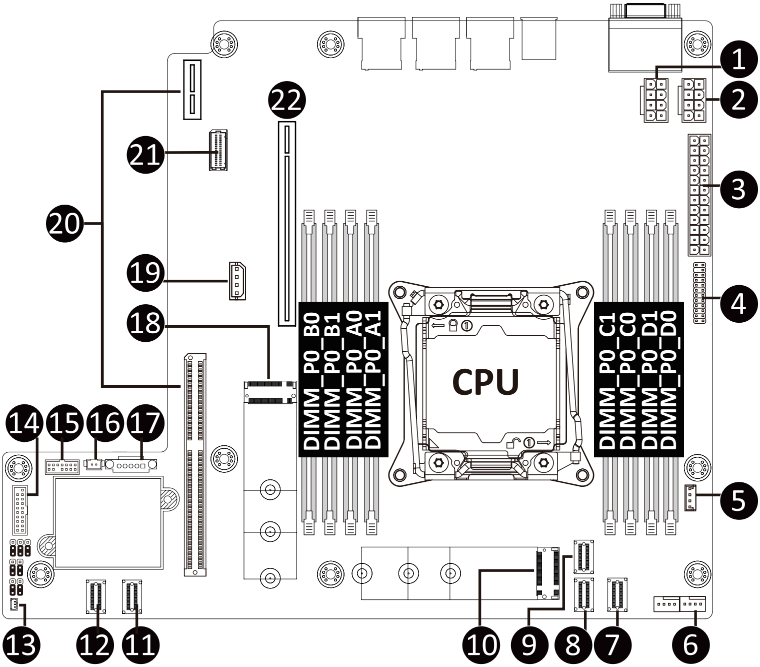


PMBus Cable



Chapter 4 Motherboard Components

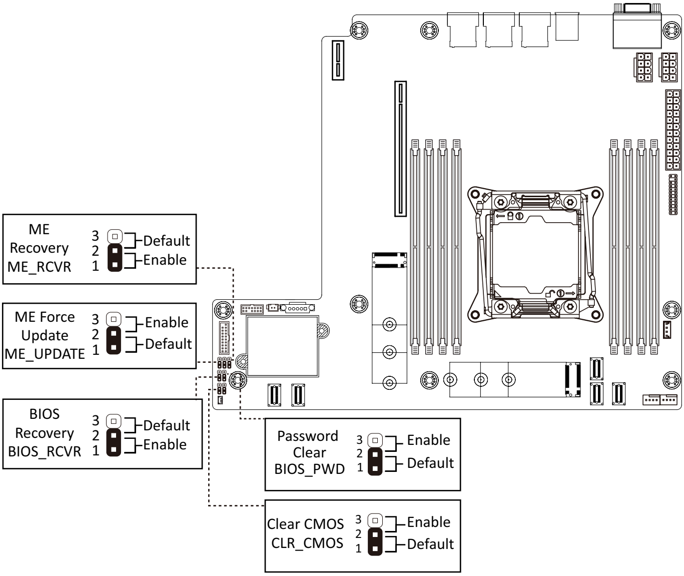
4-1 Motherboard Components



Item	Description
1	2 x 4 Pin CPU Power Connector
2	Auxiliary Power Connector for Overclocking
3	2 x 12 Pin System Power Connector
4	Front Panel Header
5	VROC Upgrade Module
6	CPU Fan Connector (for Liquid Cooling Pump)
7	SlimLine 4i Connector (PCIe Signal)
8	SlimLine 4i Connector (PCIe Signal)
9	SlimLine 4i Connector (PCIe Signal)
10	M.2 slot (PCIe Gen3 x4, Support NGFF-2280, M-Key)
11	SlimLine 4i Connector (SATA Signal)
12	SlimLine 4i Connector (SATA Signal)
13	Front Panel Board Power Connector

14	USB 3.0 Connector
15	TPM Connector
16	System Battery Cable Connector
17	PMBus Connector
18	M.2 slot (PCIe Gen3 x4, Support NGFF-2280, M-Key)
19	IPMB Connector
20	Proprietary Riser Slot
21	2 x 15 Pin HDD Back Plane Board Connector
22	PCIe x16 Slot

4-2 Jumper Setting



Chapter 5 BIOS Setup

BIOS (Basic Input and Output System) records hardware parameters of the system in the EFI on the motherboard. Its major functions include conducting the Power-On Self-Test (POST) during system startup, saving system parameters and loading operating system, etc. BIOS includes a BIOS Setup program that allows the user to modify basic system configuration settings or to activate certain system features. When the power is turned off, the battery on the motherboard supplies the necessary power to the CMOS to keep the configuration values in the CMOS.

To access the BIOS Setup program, press the <DEL> key during the POST when the power is turned on.

- BIOS flashing is potentially risky, if you do not encounter problems of using the current BIOS version, it is recommended that you don't flash the BIOS. To flash the BIOS, do it with caution. Inadequate BIOS flashing may result in system malfunction.
- It is recommended that you not alter the default settings (unless you need to) to prevent system instability or other unexpected results. Inadequately altering the settings may result in system's failure to boot. If this occurs, try to clear the CMOS values and reset the board to default values. (Refer to the **Exit** section in this chapter or introductions of the battery/clearing CMOS jumper in Chapter 1 for how to clear the CMOS values.)

BIOS Setup Program Function Keys

<←><→>	Move the selection bar to select the screen
<↑><↓>	Move the selection bar to select an item
<+>	Increase the numeric value or make changes
<->	Decrease the numeric value or make changes
<Enter>	Execute command or enter the submenu
<Esc>	Main Menu: Exit the BIOS Setup program Submenus: Exit current submenu
<F1>	Show descriptions of general help
<F3>	Restore the previous BIOS settings for the current submenus
<F9>	Load the Optimized BIOS default settings for the current submenus
<F10>	Save all the changes and exit the BIOS Setup program

- **Main**

  This setup page includes all the items in standard compatible BIOS.

- **Advanced**

  This setup page includes all the items of AMI BIOS special enhanced features.

  (ex: Auto detect fan and temperature status, automatically configure hard disk parameters.)

- **Chipset**

  This setup page includes all the submenu options for configuring the functions of the Platform Controller Hub.

- **OC Config**

  This setup page provides items for overclocking configuration.

- **Server Mgmt**

  Server additional features enabled/disabled setup menus.

- **Security**

  Change, set, or disable supervisor and user password. Configuration supervisor password allows you to restrict access to the system and BIOS Setup.

  A supervisor password allows you to make changes in BIOS Setup.

  A user password only allows you to view the BIOS settings but not to make changes.

- **Boot**

  This setup page provides items for configuration of boot sequence.

- **Save & Exit**

  Save all the changes made in the BIOS Setup program to the CMOS and exit BIOS Setup. (Pressing <F10> can also carry out this task.)

  Abandon all changes and the previous settings remain in effect. Pressing <Y> to the confirmation message will exit BIOS Setup. (Pressing <Esc> can also carry out this task.)

5-1 The Main Menu

Once you enter the BIOS Setup program, the Main Menu (as shown below) appears on the screen. Use arrow keys to move among the items and press <Enter> to accept or enter other sub-menu.

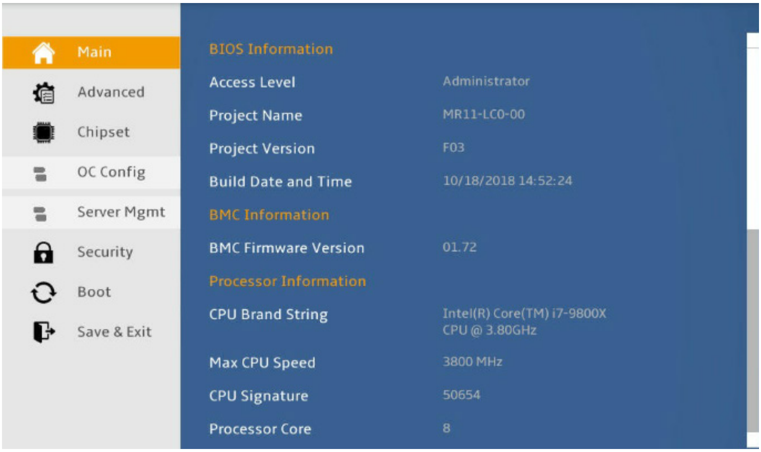
Main Menu Help

The on-screen description of a highlighted setup option is displayed on the bottom line of the Main Menu.

Submenu Help

While in a submenu, press <F1> to display a help screen (General Help) of function keys available for the menu. Press <Esc> to exit the help screen. Help for each item is in the Item Help block on the right side of the submenu.

- When the system is not stable as usual, select the **Restore Defaults** item to set your system to its defaults.
- The BIOS Setup menus described in this chapter are for reference only and may differ by BIOS version.



BIOS Information

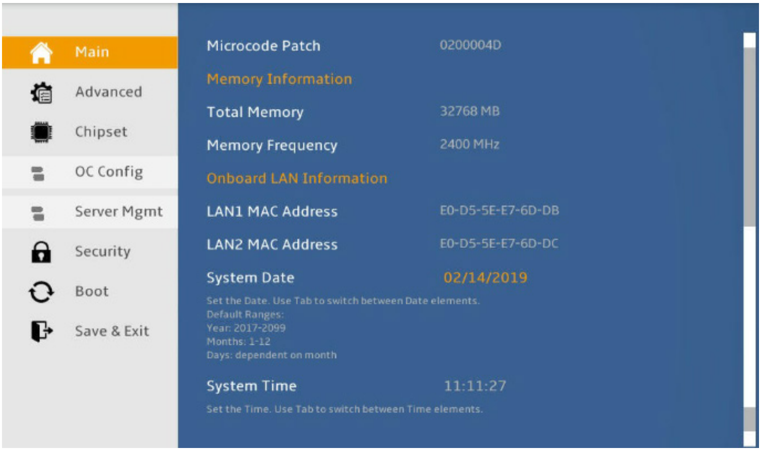
Access Level	Administrator
Project Name	MR11-LC0-00
Project Version	F03
Build Date and Time	10/18/2018 14:52:24

BMC Information

BMC Firmware Version	01.72

Processor Information

CPU Brand String	Intel(R) Core(TM) i7-9800X CPU @ 3.80GHz
Max CPU Speed	3800 MHz
CPU Signature	50654
Processor Core	8



Microcode Patch	0200004D

Memory Information

Total Memory	32768 MB
Memory Frequency	2400 MHz

Onboard LAN Information

LAN1 MAC Address	E0-D5-5E-E7-6D-DB
LAN2 MAC Address	E0-D5-5E-E7-6D-DC
System Date	02/14/2019

Set the Date. Use Tab to switch between Date elements.
Default Ranges:
Year: 2017-2099
Months: 1-12
Days: dependent on month

System Time	11:11:27

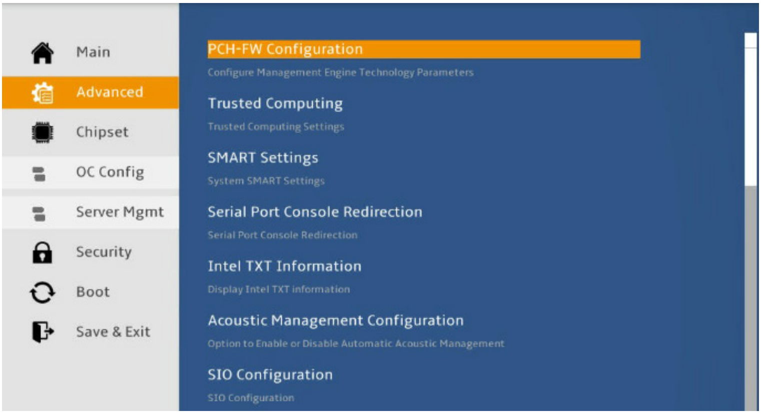
Set the Time. Use Tab to switch between Time elements.

Parameter	Description
BIOS Information	
Access Level	Display the privileges level information.
Project Name	Displays the project name information.
Project Version	Displays version number of the BIOS setup utility.
Build Date and Time	Displays the date and time when the BIOS setup utility was created.
BMC Information(Note)	
BMC Firmware Version(Note)	Displays BMC firmware version information.
Processor Information	
CPU Brand String / Max CPU Speed / CPU Signature / Processor Core / Microcode Patch	Displays the technical specifications for the installed processor(s).
Memory Information	
Total Memory(Note)	Displays the total memory size of the installed memory.
Memory Frequency(Note)	Displays the frequency information of the installed memory.
Onboard LAN Information	
LAN1 MAC Address(Note)	Displays LAN MAC address information.
LAN2 MAC Address (Note)	Displays LAN MAC address information.
System Date	Sets the date following the weekday-month-day-year format.
System Time	Sets the system time following the hour-minute-second format.

(Note) Functions available on selected models.

5-2 Advanced Menu

The Advanced menu display submenu options for configuring the function of various hardware components. Select a submenu item, then press <Enter> to access the related submenu screen.



PCH-FW Configuration
Configure Management Engine Technology Parameters

Trusted Computing
Trusted Computing Settings

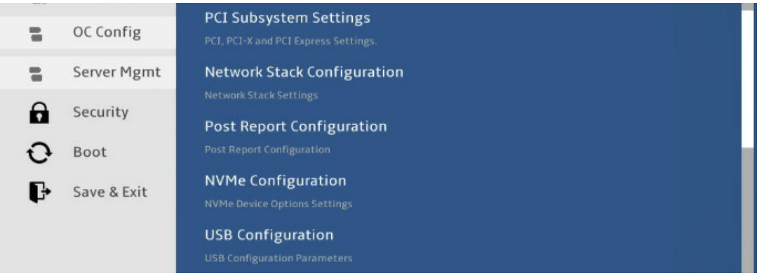
SMART Settings
System SMART Settings

Serial Port Console Redirection
Serial Port Console Redirection

Intel TXT Information
Display Intel TXT information

Acoustic Management Configuration
Option to Enable or Disable Automatic Acoustic Management

SIO Configuration
SIO Configuration



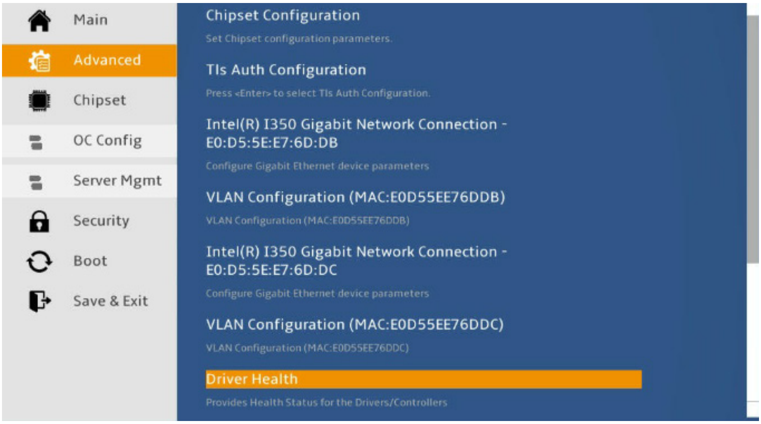
PCI Subsystem Settings
PCI, PCI-X and PCI Express Settings.

Network Stack Configuration
Network Stack Settings

Post Report Configuration
Post Report Configuration

NVMe Configuration
NVMe Device Options Settings

USB Configuration
USB Configuration Parameters



Chipset Configuration
Set Chipset configuration parameters.

Tls Auth Configuration
Press <Enter> to select Tls Auth Configuration.

Intel(R) I350 Gigabit Network Connection - E0:D5:5E:E7:6D:DB
Configure Gigabit Ethernet device parameters

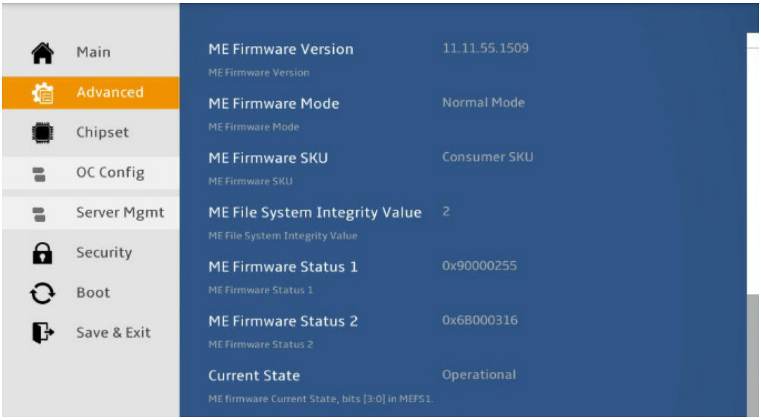
VLAN Configuration (MAC:E0D55EE76DDB)
VLAN Configuration (MAC:E0D55EE76DDB)

Intel(R) I350 Gigabit Network Connection - E0:D5:5E:E7:6D:DC
Configure Gigabit Ethernet device parameters

VLAN Configuration (MAC:E0D55EE76DDC)
VLAN Configuration (MAC:E0D55EE76DDC)

Driver Health
Provides Health Status for the Drivers/Controllers

5-2-1 PCH-FW Configuration



ME Firmware Version 11.11.55.1509
ME Firmware Version

ME Firmware Mode Normal Mode
ME Firmware Mode

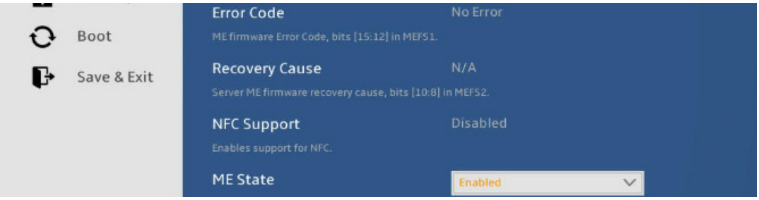
ME Firmware SKU Consumer SKU
ME Firmware SKU

ME File System Integrity Value 2
ME File System Integrity Value

ME Firmware Status 1 0x90000255
ME Firmware Status 1

ME Firmware Status 2 0x6B000316
ME Firmware Status 2

Current State Operational
ME firmware Current State, bits [3:0] in MEFS1.



Error Code No Error
ME firmware Error Code, bits [15:12] in MEFS1.

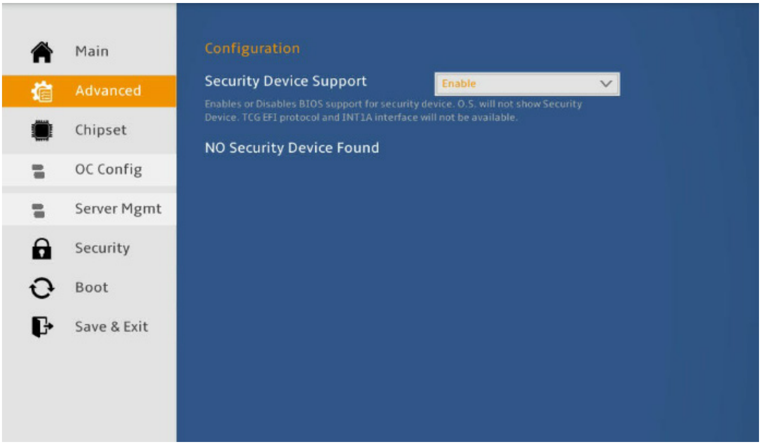
Recovery Cause N/A
Server ME firmware recovery cause, bits [10:8] in MEFS2.

NFC Support Disabled
Enables support for NFC.

ME State Enabled

Parameter	Description
ME Firmware Version	Displays the ME firmware version information.
ME Firmware Mode	Displays the ME firmware mode.
ME Firmware SKU	Displays the ME firmware SKU information.
ME File System Integrity Value	Displays the ME file system integrity value information.
ME Firmware Status 1/2	Displays the ME firmware status 1/2 information.
Current State	Displays the current state of ME firmware.
Error Code	Displays the ME firmware error code information.
Recovery Cause	Displays the cause of ME firmware recovery.
NFC Support	Displays the NFC status.
ME State	Enable/Disable ME state. Options available: Enabled/Disabled. Default setting is **Enabled**.

5-2-2 Trusted Computing



Configuration

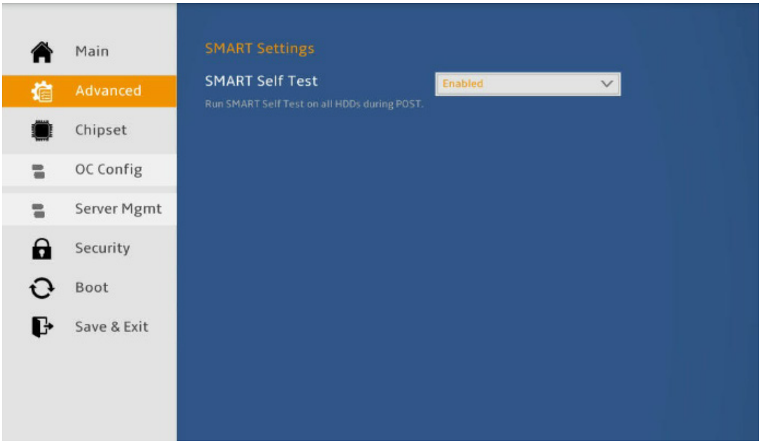
Security Device Support: Enable

Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.

NO Security Device Found

Parameter	Description
Configuration	
Security Device Support	Enable/Disable the TPM support feature. Options available: Enable/Disable. Default setting is **Enable**.

5-2-3 SMART Settings



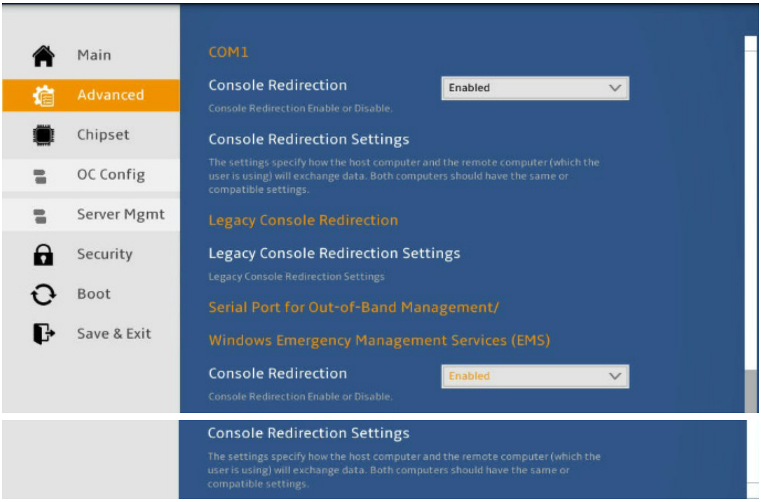
SMART Settings

SMART Self Test — Enabled

Run SMART Self Test on all HDDs during POST.

Parameter	Description
SMART Settings	
SMART Self Test	Enable/Disable SMART Self Test on all HDDs during POST. Options available: Enabled/Disabled. Default setting is **Enabled**.

5-2-4 Serial Port Console Redirection



COM1

Console Redirection: Enabled

Console Redirection Enable or Disable.

Console Redirection Settings

The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings.

Legacy Console Redirection

Legacy Console Redirection Settings

Legacy Console Redirection Settings

Serial Port for Out-of-Band Management/

Windows Emergency Management Services (EMS)

Console Redirection: Enabled

Console Redirection Enable or Disable.

Console Redirection Settings

The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings.

Parameter	Description
COM1 Console Redirection(Note))	Console redirection enables the users to manage the system from a remote location. Options available: Enabled/Disabled. Default setting is **Disabled**.
COM1 Console Redirection Settings	Press [Enter] to configure advanced items. **Please note that this item is configurable when COM1 Console Redirection is set to Enabled.** ◆ Terminal Type – Selects a terminal type to be used for console redirection. – Options available: VT100, VT100+, ANSI, VT-UTF8. Default setting is **VT100+**. ◆ Bits per second – Selects the transfer rate for console redirection. – Options available: 9600, 19200, 38400, 57600, 115200. Default setting is **115200**. ◆ Data Bits – Selects the number of data bits used for console redirection. – Options available: 7/8. Default setting is **8**.

(Note) Advanced items prompt when this item is defined.

Parameter	Description
COM1 Console Redirection Settings (continued)	◆ Parity – A parity bit can be sent with the data bits to detect some transmission errors. – 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. – Mark and Space Parity do not allow for error detection. – Options available: None, Even, Odd, Mark, Space. Default setting is **None**. ◆ Stop Bits – 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. – Options available: 1/2. Default setting is **1**. ◆ Flow Control – 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. – Options available: None, Hardware RTS/CTS. Default setting is **None**. ◆ VT-UTF8 Combo Key Support – Enable/Disable the VT-UTF8 Combo Key Support. – Options available: Enabled/Disabled. Default setting is **Enabled**. ◆ Recorder Mode(Note) – When this mode enabled, only texts will be send. This is to capture Terminal data. – Options available: Enabled/Disabled. Default setting is **Disabled**. ◆ Resolution 100x31(Note) – Enable/Disable extended terminal resolution. – Options available: Enabled/Disabled. Default setting is **Enabled**. ◆ Putty KeyPad(Note) – Selects FunctionKey and LeyPad on Putty. – Options available: VT100, LINUX, XTERMR6, SC0, ESCN, VT400. Default setting is **VT100**.

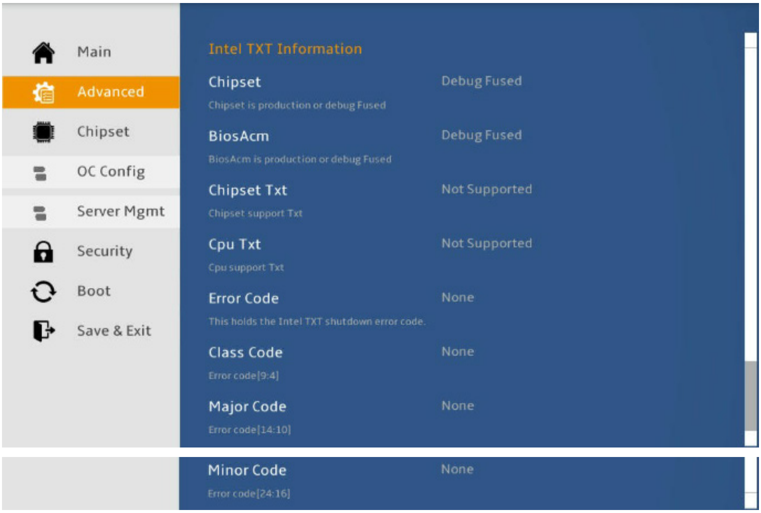
(Note) Advanced items prompt when this item is defined.

Parameter	Description
Legacy Console Redirection	
Legacy Console Redirection Settings	Press [Enter] to configure advanced items. ◆ Redirection COM Port – Selects a COM port for Legacy serial redirection. – Default setting is **COM1**. ◆ Resolution – Selects the number of rows and columns used in Console Redirection for legacy OS support. – Options available: 80x24, 80x25. Default setting is **80x24**. ◆ Redirect After POST – When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS. – Options available: Always Enable, BootLoader. Default setting is **Always Enable**.
Serial Port for Out-of-Band Management / Windows Emergency Management Services (EMS) Console Redirection(Note)	EMS console redirection allows the user to configure Console Redirection Settings to support Out-of-Band Serial Port management. Options available: Enabled/Disabled. Default setting is **Disabled**.
Serial Port for Out-of-Band EMS Console Redirection Settings	Press [Enter] to configure advanced items. **Please note that this item is configurable when Serial Port for Out-of-Band Management EMS Console Redirection is set to Enabled.** ◆ Out-of-Band Mgmt Port – Microsoft Windows Emerency Management Service (EMS) allows for remote management of a Windows Server OS through a serial port. – Default setting is **COM1**. ◆ Terminal Type – Selects a terminal type to be used for console redirection. – Options available: VT100, VT100+, ANSI, VT-UTF8. Default setting is **VT100+**. ◆ Bits per second – Selects the transfer rate for console redirection. – Options available: 9600, 19200, 38400, 57600, 115200. Default setting is **115200**.

(Note) Advanced items prompt when this item is defined.

Parameter	Description
Serial Port for Out-of-Band EMS Console Redirection Settings(continued)	◆ Flow Control – 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. – Options available: None, Hardware RTS/CTS, Software Xon/Xoff. Default setting is **None**.

5-2-5 Intel TXT Information



Intel TXT Information

Chipset — Debug Fused
Chipset is production or debug Fused

BiosAcm — Debug Fused
BiosAcm is production or debug Fused

Chipset Txt — Not Supported
Chipset support Txt

Cpu Txt — Not Supported
Cpu support Txt

Error Code — None
This holds the Intel TXT shutdown error code.

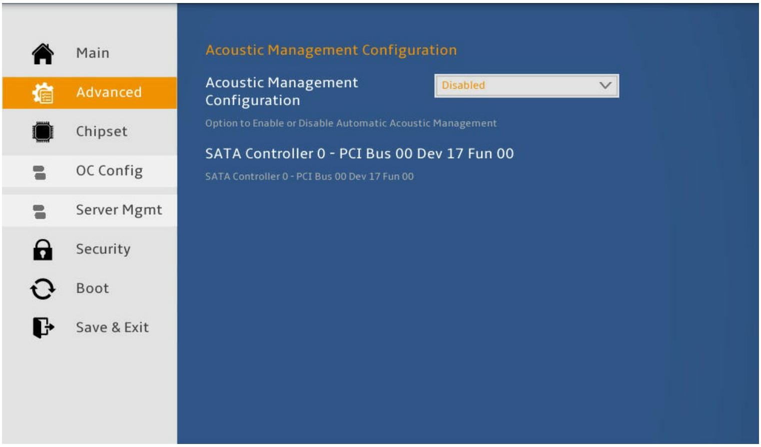
Class Code — None
Error code[9:4]

Major Code — None
Error code[14:10]

Minor Code — None
Error code[24:16]

Parameter	Description
Intel TXT Information	
Chipset	Displays the chipset is production or debug fused.
BiosAcm	Displays the Bios Acm is production or debug fused.
Chipset Txt	Displays the chipset status of TXT support.
Cpu Txt	Displays the CPU status of TXT support.
Error Code	Displays the Intel TXT shut down error code.
Class Code	Displays the class code information.
Major Code	Displays the major code information.
Minor Code	Displays the minor code information.

5-2-6 Acoustic Management Configuration



Acoustic Management Configuration

Acoustic Management Configuration: Disabled

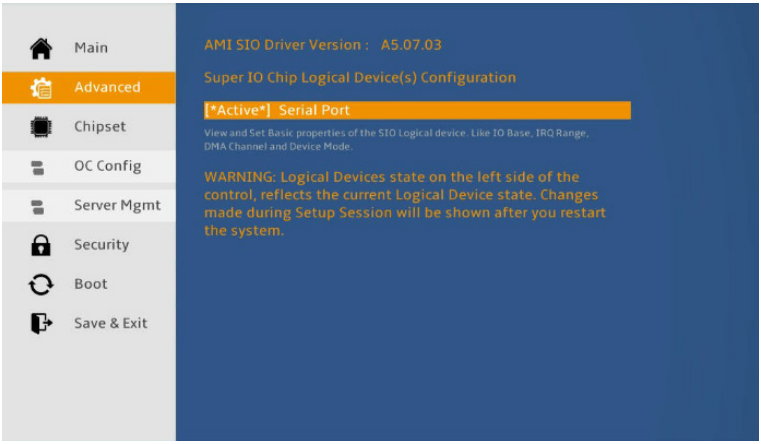
Option to Enable or Disable Automatic Acoustic Management

SATA Controller 0 - PCI Bus 00 Dev 17 Fun 00

SATA Controller 0 - PCI Bus 00 Dev 17 Fun 00

Parameter	Description
Acoustic Management Configuration	Enable/Disable the automatic acoustic management function. Options available: Enabled/Disabled. Default setting is **Disabled**.

5-2-7 SIO Configuration



AMI SIO Driver Version : A5.07.03

Super IO Chip Logical Device(s) Configuration

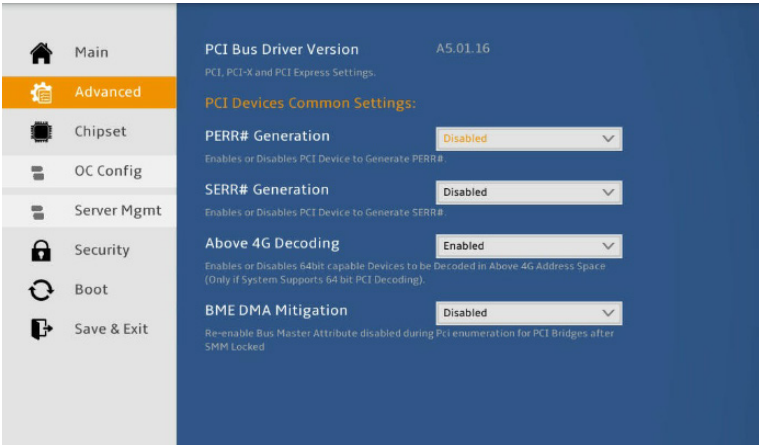
[*Active*] Serial Port

View and Set Basic properties of the SIO Logical device. Like IO Base, IRQ Range, DMA Channel and Device Mode.

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

Parameter	Description
AMI SIO Driver Version	Displays the AMI SIO driver version information.
Super IO Chip Logical Device(s) Configuration	
[*Active*] Serial Port	Press [Enter] to configure advanced items. ◆ Use This Device – When set to Enabled allows you to configure the serial port settings. When set to Disabled, displays no configuration for the serial port. – Options available: Enabled/Disabled. Default setting is **Enabled**. ◆ Current: – Displays the serial port base I/O address and IRQ. ◆ Possible: – Configures the serial port base I/O address and IRQ. Use Automatic Settings IO=3F8h; IRQ=4; DMA; IO=3F8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA; IO=2F8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA; IO=3E8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA; IO=2E8h; IRQ=3, 4, 5, 7, 9, 10, 11, 12; DMA; Default setting is **Use Automatic Settings**.

5-2-8 PCI Subsystem Settings



PCI Bus Driver Version A5.01.16

PCI, PCI-X and PCI Express Settings.

PCI Devices Common Settings:

PERR# Generation: Disabled

Enables or Disables PCI Device to Generate PERR#.

SERR# Generation: Disabled

Enables or Disables PCI Device to Generate SERR#.

Above 4G Decoding: Enabled

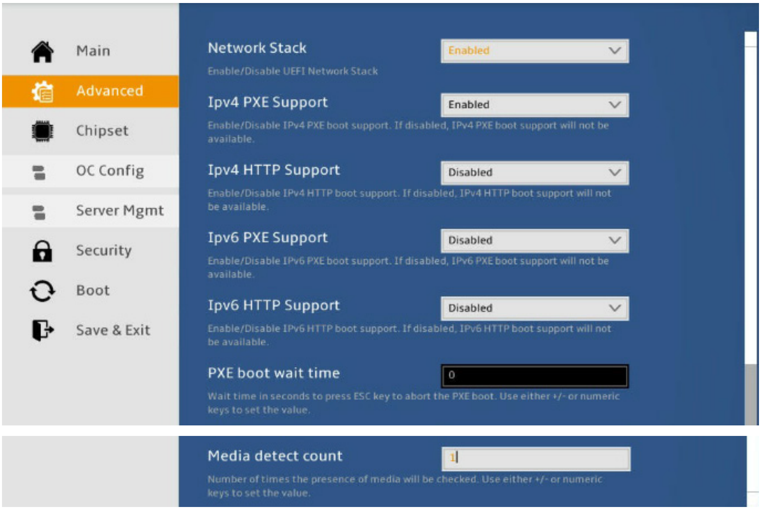
Enables or Disables 64bit capable Devices to be Decoded in Above 4G Address Space (Only if System Supports 64 bit PCI Decoding).

BME DMA Mitigation: Disabled

Re-enable Bus Master Attribute disabled during Pci enumeration for PCI Bridges after SMM Locked

Parameter	Description
PCI Bus Driver Version	Displays the PCI Bus Driver version information.
PCI Devices Common Settings	
PERR# Generation	Enable/Disable PCI device to generate PERR#. Options available: Enabled/Disabled. Default setting is **Disabled**.
SERR# Generation	Enable/Disable PCI device to generate SERR#. Options available: Enabled/Disabled. Default setting is **Disabled**.
Above 4G Decoding	Enable/Disable 64bit capable Devices to be decoded in Above 4G Address Space (only if the system supports 64 bit PCI Decoding). Options available: Enabled/Disabled. Default setting is **Enabled**.
BME DMA Mitigation	Re-enable bus master attribute disabled during PCI enumeration for PCI bridges after SMM is locked. Options available: Enabled/Disabled. Default setting is **Enabled**.

5-2-9 Network Stack Configuration



Network Stack: Enabled
Enable/Disable UEFI Network Stack

Ipv4 PXE Support: Enabled
Enable/Disable IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available.

Ipv4 HTTP Support: Disabled
Enable/Disable IPv4 HTTP boot support. If disabled, IPv4 HTTP boot support will not be available.

Ipv6 PXE Support: Disabled
Enable/Disable IPv6 PXE boot support. If disabled, IPv6 PXE boot support will not be available.

Ipv6 HTTP Support: Disabled
Enable/Disable IPv6 HTTP boot support. If disabled, IPv6 HTTP boot support will not be available.

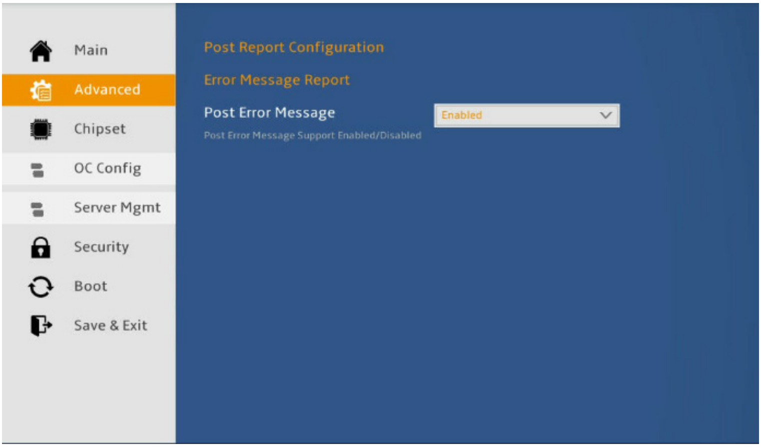
PXE boot wait time: 0
Wait time in seconds to press ESC key to abort the PXE boot. Use either +/- or numeric keys to set the value.

Media detect count: 1
Number of times the presence of media will be checked. Use either +/- or numeric keys to set the value.

Parameter	Description
Network Stack	Enable/Disable the UEFI network stack. Options available: Enabled/Disabled. Default setting is **Enabled**.
Ipv4 PXE Support(Note)	Enable/Disable the Ipv4 PXE feature. Options available: Enabled/Disabled. Default setting is **Enabled**.
Ipv4 HTTP Support(Note)	Enable/Disable the Ipv4 HTTP feature. Options available: Enabled/Disabled. Default setting is **Disabled**.
Ipv6 PXE Support(Note)	Enable/Disable the Ipv6 PXE feature. Options available: Enabled/Disabled. Default setting is **Enabled**.
Ipv6 HTTP Support(Note)	Enable/Disable the Ipv6 HTTP feature. Options available: Enabled/Disabled. Default setting is **Disabled**.
PXE boot wait time(Note)	Wait time in seconds to press ESC key to abort the PXE boot. Press the <+> / <-> keys to increase or decrease the desired values.
Media detect count(Note)	Number of times the presence of media will be checked. Press the <+> / <-> keys to increase or decrease the desired values.

(Note) This item appears when **Network Stack** is set to **Enabled**.

5-2-10 Post Report Configuration



Post Report Configuration

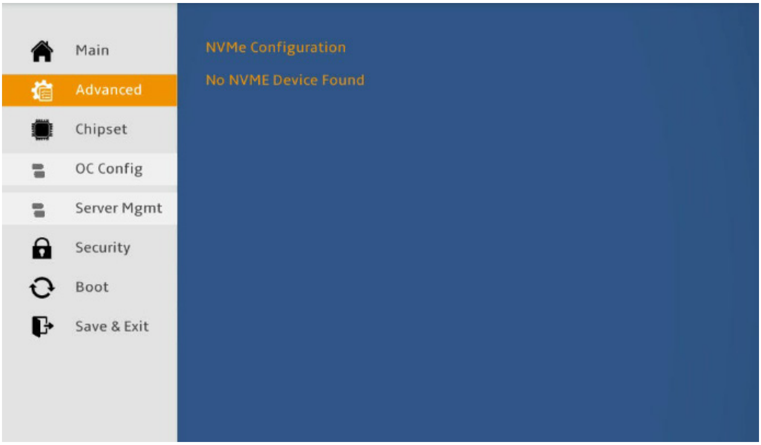
Error Message Report

Post Error Message — Enabled

Post Error Message Support Enabled/Disabled

Parameter	Description
Post Report Configuration	
Error Message Report	
Post Error Message	Enable/Disable the POST Error Message support. Options available: Enabled/Disabled. Default setting is **Enabled**.

5-2-11 NVMe Configuration

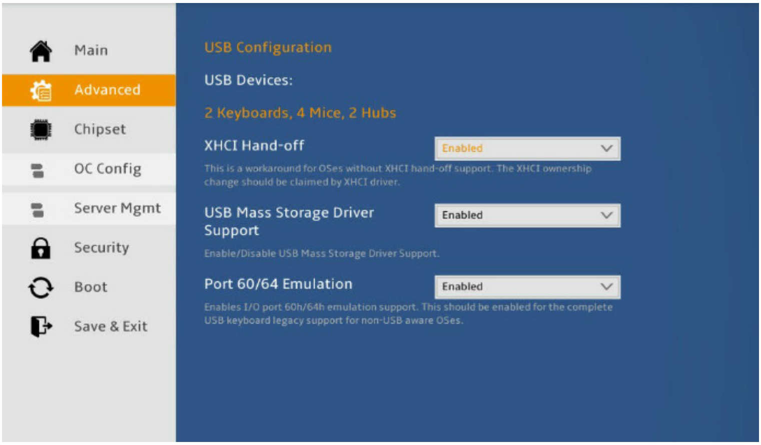


NVMe Configuration

No NVME Device Found

Parameter	Description
NVMe Configuration	Displays the NVMe devices connected to the system

5-2-12 USB Configuration



USB Configuration

USB Devices:

2 Keyboards, 4 Mice, 2 Hubs

XHCI Hand-off: Enabled

This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.

USB Mass Storage Driver Support: Enabled

Enable/Disable USB Mass Storage Driver Support.

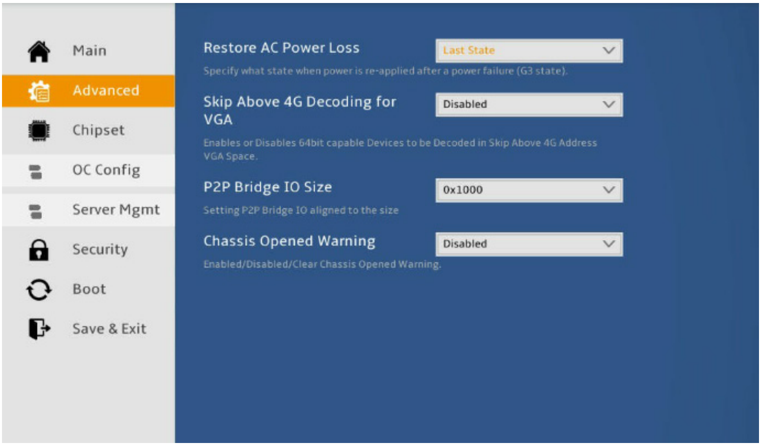
Port 60/64 Emulation: Enabled

Enables I/O port 60h/64h emulation support. This should be enabled for the complete USB keyboard legacy support for non-USB aware OSes.

Parameter	Description
USB Configuration	
USB Devices:	Displays the USB devices connected to the system.
XHCI Hand-off	Enable/Disable the XHCI (USB 3.0) Hand-off support. Options available: Enabled/Disabled. Default setting is **Enabled**.
USB Mass Storage Driver Support(Note)	Enable/Disable the USB Mass Storage Driver Support. Options available: Enabled/Disabled. Default setting is **Enabled**.
Port 60/64 Emulation	Enables the I/O port 60h/64h emulation support. This should be enabled for the complete USB Keyboard Legacy support for non-USB aware OS. Options available: Enabled/Disabled. Default setting is **Enabled**.

(Note) This item is present only if you attach USB devices.

5-2-13 Chipset Configuration



Restore AC Power Loss: Last State

Specify what state when power is re-applied after a power failure (G3 state).

Skip Above 4G Decoding for VGA: Disabled

Enables or Disables 64bit capable Devices to be Decoded in Skip Above 4G Address VGA Space.

P2P Bridge IO Size: 0x1000

Setting P2P Bridge IO aligned to the size

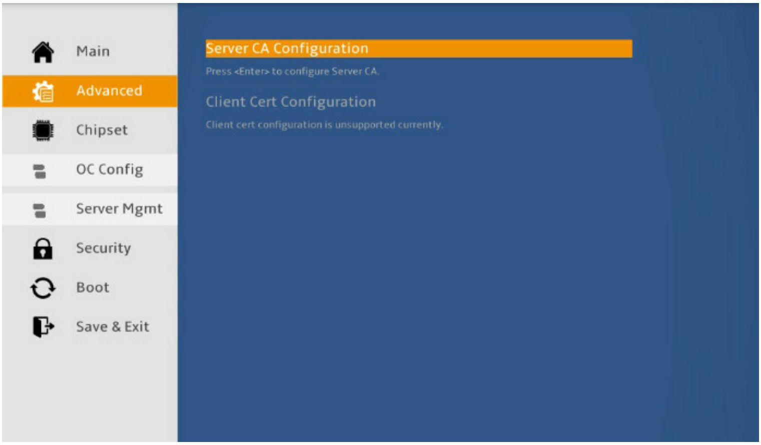
Chassis Opened Warning: Disabled

Enabled/Disabled/Clear Chassis Opened Warning.

Parameter	Description
Restore on AC Power Loss(Note)	Defines the power state to resume to after a system shutdown that is due to an interruption in AC power. When set to Last State, the system will return to the active power state prior to shutdown. When set to Power Off, the system remains off after power shutdown. Options available: Last State, Power Off, Power On, Unspecified. The default setting depends on the BMC setting.
Skip Above 4G Decoding for VGA	Enable/Disable 64bit capable devices to be decoded in Skip Above 4G Address VGA Space. Options available: Enabled/Disabled. Default setting is **Disabled**.
P2P Bridge IO Size	Sets P2P Bridge IO aligned to the size. Options available: 0x100, 0x150, 0x1000. Default setting is **0x1000**.
Chassis Opened Warning	Enable/Disable the chassis intrusion alert function. Options available: Enabled, Disabled, Clear. Default setting is **Disabled**.

(Note) When the power policy is controlled by BMC, please wait for 15-20 seconds for BMC to save the last power state.

5-2-14 Tls Auth Configuration



Server CA Configuration

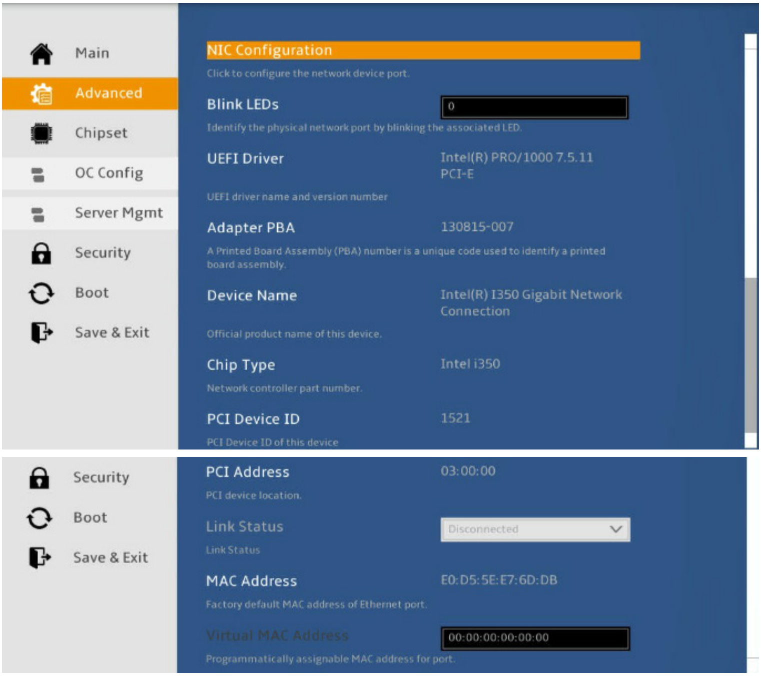
Press <Enter> to configure Server CA.

Client Cert Configuration

Client cert configuration is unsupported currently.

Parameter	Description
Server CA Configuration	Press [Enter] for configuration of advanced items. ◆ Enroll Cert – Press [Enter] to enroll a certificate • Enroll Cert Using File • Cert GUID Input digit character in 1111111-2222-3333-4444-1234567890ab format. – Commit Changes and Exit – Discard Changes and Exit ◆ Delete Cert
Client Cert Configuration	Press [Enter] for configuration of advanced items.

5-2-15 Intel(R) I350 Gigabit Network Connection



NIC Configuration
Click to configure the network device port.

Blink LEDs 0
Identify the physical network port by blinking the associated LED.

UEFI Driver Intel(R) PRO/1000 7.5.11 PCI-E
UEFI driver name and version number

Adapter PBA 130815-007
A Printed Board Assembly (PBA) number is a unique code used to identify a printed board assembly.

Device Name Intel(R) I350 Gigabit Network Connection
Official product name of this device.

Chip Type Intel i350
Network controller part number.

PCI Device ID 1521
PCI Device ID of this device

PCI Address 03:00:00
PCI device location.

Link Status Disconnected
Link Status

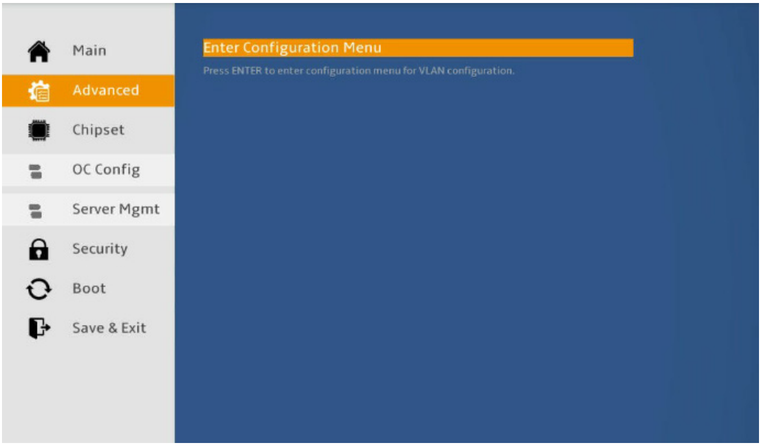
MAC Address E0:D5:5E:E7:6D:DB
Factory default MAC address of Ethernet port.

Virtual MAC Address 00:00:00:00:00:00
Programmatically assignable MAC address for port.

Parameter	Description
NIC Configuration	Press [Enter] to configure advanced items. ◆ Link Speed – Allows for automatic link speed adjustment. – Options available: Auto Negotiated, 10 Mbps Half, 10 Mbps Full, 100 Mbps Half, 100 Mbps Full. Default setting is **Auto Negotiated**. ◆ Wake On LAN – Enables power on of the system via LAN. Note that configuring Wake on LAN in the operating system does not change the value of this setting, but does override the behavior of Wake on LAN in OS controlled power states. – Options available: Enabled/Disabled. Default setting is **Enabled**.
Blink LEDs	Identifies the physical network port by blinking the associated LED. Press the numeric keys to adjust desired values.
UEFI Driver	Displays the technical specifications for the Network Interface Controller.
Adapter PBA	Displays the technical specifications for the Network Interface Controller.
Device Name	Displays the technical specifications for the Network Interface Controller.

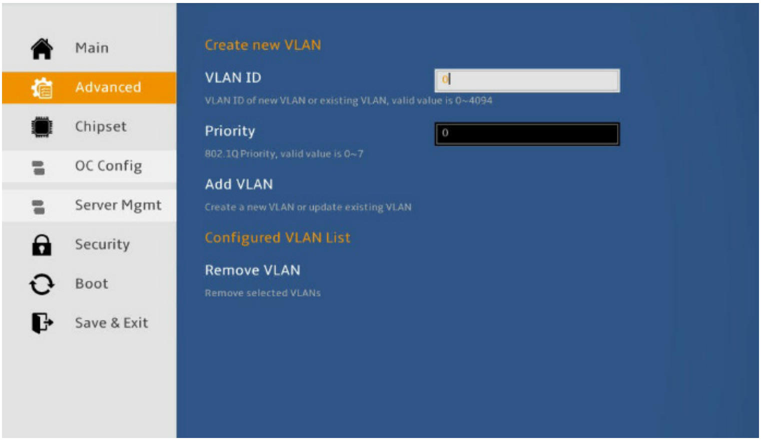
Parameter	Description
Chip Type	Displays the technical specifications for the Network Interface Controller.
PCI Device ID	Displays the technical specifications for the Network Interface Controller.
PCI Address	Displays the technical specifications for the Network Interface Controller.
Link Status	Displays the technical specifications for the Network Interface Controller.
MAC Address	Displays the technical specifications for the Network Interface Controller.
Virtual MAC Address	Displays the technical specifications for the Network Interface Controller.

5-2-16 VLAN Configuration



Enter Configuration Menu

Press ENTER to enter configuration menu for VLAN configuration.



Create new VLAN

VLAN ID 0

VLAN ID of new VLAN or existing VLAN, valid value is 0~4094

Priority 0

802.1Q Priority, valid value is 0~7

Add VLAN

Create a new VLAN or update existing VLAN

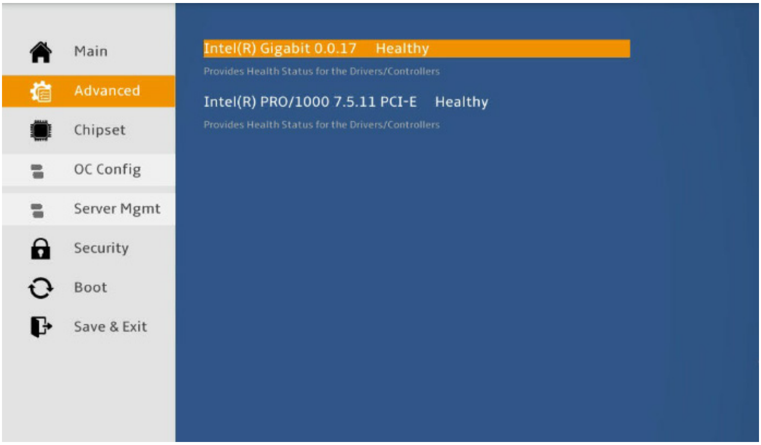
Configured VLAN List

Remove VLAN

Remove selected VLANs

Parameter	Description
Enter Configuration Menu	Press [Enter] to configure advanced items. ◆ Create new VLAN ◆ VLAN ID – Sets VLAN ID for a new VLAN or an existing VLAN. – Press the <+> / <-> keys to increase or decrease the desired values. – The valid range is from 0 to 4094. ◆ Priority – Sets 802.1Q Priority for a new VLAN or an existing VLAN. – Press the <+> / <-> keys to increase or decrease the desired values. – The valid range is from 0 to 7. ◆ Add VLAN – Press [Enter] to create a new VLAN or update an existing VLAN. ◆ Configured VLAN List ◆ Remove VLAN – Press [Enter] to remove an existing VLAN.

5-2-17 Driver Health



Intel(R) Gigabit 0.0.17 Healthy

Provides Health Status for the Drivers/Controllers

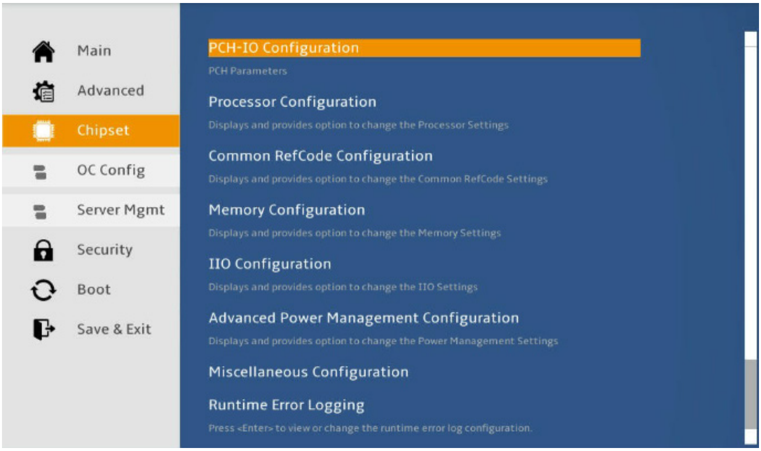
Intel(R) PRO/1000 7.5.11 PCI-E Healthy

Provides Health Status for the Drivers/Controllers

Parameter	Description
Driver Health	Displays driver health status of the devices/controllers if installed

5-3 Chipset Setup Menu

Chipset Setup menu displays submenu options for configuring the function of Platform Controller Hub(PCH). Select a submenu item, then press <Enter> to access the related submenu screen.



PCH-IO Configuration

PCH Parameters

Processor Configuration

Displays and provides option to change the Processor Settings

Common RefCode Configuration

Displays and provides option to change the Common RefCode Settings

Memory Configuration

Displays and provides option to change the Memory Settings

IIO Configuration

Displays and provides option to change the IIO Settings

Advanced Power Management Configuration

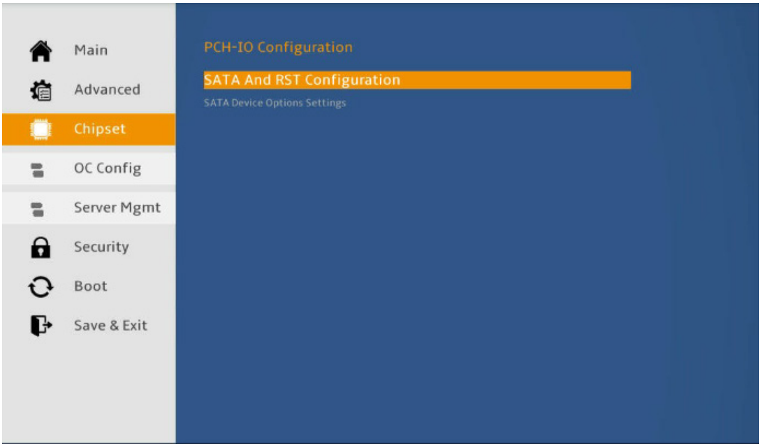
Displays and provides option to change the Power Management Settings

Miscellaneous Configuration

Runtime Error Logging

Press <Enter> to view or change the runtime error log configuration.

5-3-1 PCH-IO Configuration



PCH-IO Configuration

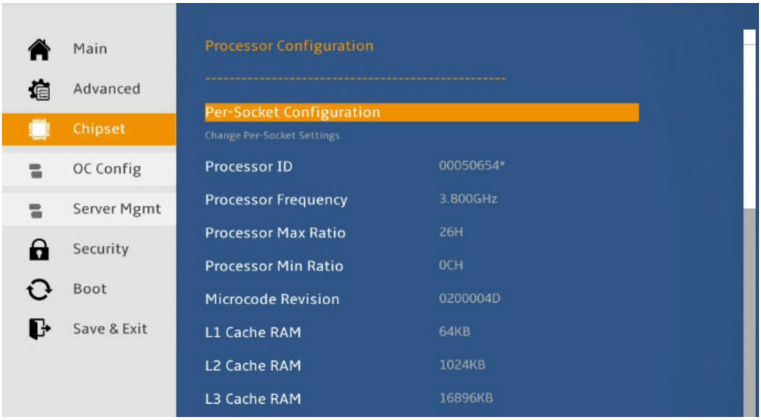
SATA And RST Configuration

SATA Device Options Settings

Parameter	Description
PCH-IO Configuration	
SATA And RST Configuration	Press [Enter] to configure advanced items. ◆ SATA Controller – Enable/Disable SATA device. – Options available: Enabled/Disabled. Default setting is **Enabled**. ◆ SATA Mode Selection – Configures on chip SATA type. – AHCI Mode: the SATA controller enables its AHCI functionality. Then the RAID function is disabled and cannot be access the RAID setup utility at boot time. – Intel RST Premium: the SATA controller enables both its RAID and AHCI functions. You will be allowed to access the RAID setup utility at boot time. – Options available: AHCI/Intel RST Premium. Default setting is **AHCI**. ◆ SATA Port 0/1/2/3/4/5/6/7 – The category identifies SATA hard drives that are installed in the computer. System will automatically detect HDD type. ◆ Port 0/1/2/3/4/5/6/7 – Enable/Disable Port 0/1/2/3/4/5/6/7 device. – Options available: Enabled/Disabled. Default setting is **Enabled**. ◆ Hot Plug (for Port 0/1/2/3/4/5/6/7) – Enable/Disable SATA ports Hot Plug support. – Options available: Enabled/Disabled. Default setting is **Enabled**

Parameter	Description
SATA And RST Configuration (continued)	◆ Spin Up Device – Enable/Disable the SATA ports straggerred spin up function. – Options available: Enabled/Disabled. Default setting is **Disabled**

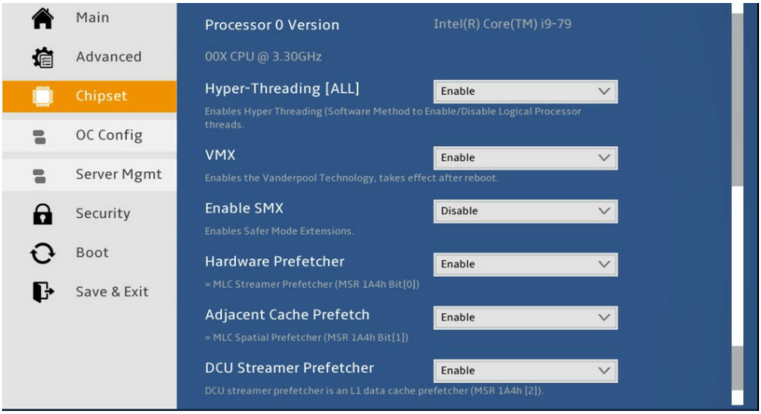
5-3-2 Processor Configuration



Processor Configuration

Per-Socket Configuration
Change Per-Socket Settings

Processor ID	00050654*
Processor Frequency	3.800GHz
Processor Max Ratio	26H
Processor Min Ratio	0CH
Microcode Revision	0200004D
L1 Cache RAM	64KB
L2 Cache RAM	1024KB
L3 Cache RAM	16896KB



Processor 0 Version Intel(R) Core(TM) i9-79
00X CPU @ 3.30GHz

Hyper-Threading [ALL] Enable
Enables Hyper Threading (Software Method to Enable/Disable Logical Processor threads.

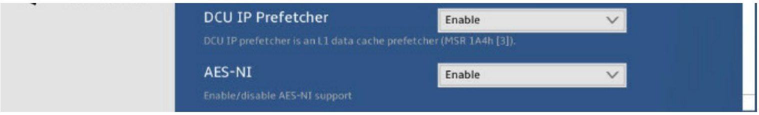
VMX Enable
Enables the Vanderpool Technology, takes effect after reboot.

Enable SMX Disable
Enables Safer Mode Extensions.

Hardware Prefetcher Enable
= MLC Streamer Prefetcher (MSR 1A4h Bit[0])

Adjacent Cache Prefetch Enable
= MLC Spatial Prefetcher (MSR 1A4h Bit[1])

DCU Streamer Prefetcher Enable
DCU streamer prefetcher is an L1 data cache prefetcher (MSR 1A4h [2]).

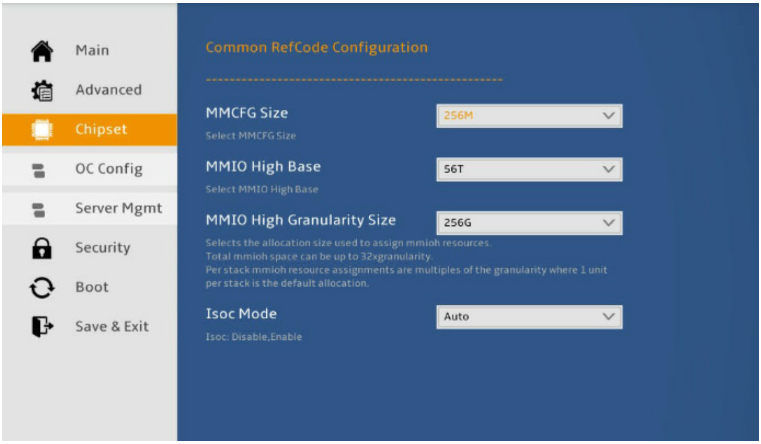


DCU IP Prefetcher Enable
DCU IP prefetcher is an L1 data cache prefetcher (MSR 1A4h [3]).

AES-NI Enable
Enable/disable AES-NI support

Parameter	Description
Processor Configuration	
Per-Socket Configuration	Press [Enter] to configure advanced items. ◆ CPU Socket 0 Configuration – Press [Enter] to configure advanced items. ◆ Core Disable Bitmap(Hex) (for CPU socket 0/1) – Number of Cores to enable. 0 means all cores. FFFFFFF means to disable all cores. The maximum value depends on the number of CPUs available. Press the numeric keys to adjust desired values.
Processor ID / Processor Frequency / Processor Max Ratio / Processor Min Ratio / Microcode Revision / L1 Cache RAM / L2 Cache RAM / L3 Cache RAM / Processor 0 Version	Displays the technical specifications for the installed processor(s).
Hyper-Threading [All]	The Hyper Threading Technology allows a single processor to execute two or more separate threads concurrently. When hyper-threading is enabled, multi-threaded software applications can execute their threads, thereby improving performance. Options available: Enable/Disable. Default setting is **Enable**.
VMX (Vanderpool Technology)	Enable/Disable the Vanderpool Technology. This will take effect after rebooting the system. Options available: Enable/Disable. Default setting is Enable.
Enable SMX	Enable/Disable the Secure Mode Extensions (SMX) support function. Options available: Enable/Disable. Default setting is **Disable**.
Hardware Prefetcher	Select whether to enable the speculative prefetch unit of the processor. Options available: Enable/Disable. Default setting is **Disable**.
Adjacent Cache Prefetch	When enabled, cache lines are fetched in pairs. When disabled, only the required cache line is fetched. Options available: Enable/Disable. Default setting is **Enable**.
DCU Streamer Prefetcher	Prefetches the next L1 data line based upon multiple loads in same cache line. Options available: Enable/Disable. Default setting is **Enable**.
DCU IP Prefetcher	Prefetches the next L1 Data line based upon sequential load history. Options available: Enable/Disable. Default setting is **Enable**.
AES-NI	Enable/Disable the AES-NI (Intel Advanced Encryption Standard New Instructions) support function. Options available: Enable/Disable. Default setting is **Enable**.

5-3-3 Common RefCode Configuration



Common RefCode Configuration

MMCFG Size: 256M
Select MMCFG Size

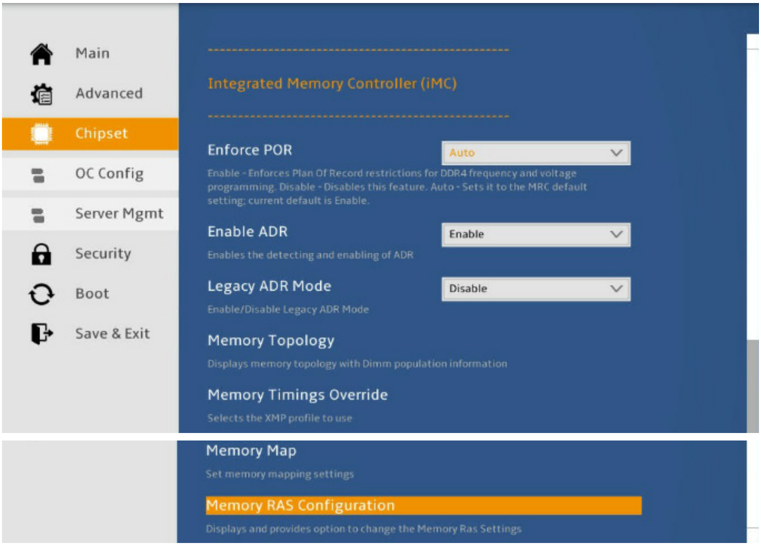
MMIO High Base: 56T
Select MMIO High Base

MMIO High Granularity Size: 256G
Selects the allocation size used to assign mmioh resources.
Total mmioh space can be up to 32xgranularity.
Per stack mmioh resource assignments are multiples of the granularity where 1 unit per stack is the default allocation.

Isoc Mode: Auto
Isoc: Disable,Enable

Parameter	Description
Common RefCode Configuration	
MMCFG Size	Selects MMCFG size. Options available: 64M, 128M, 256M, 512M, 1G, 2G. Default setting is **256M**.
MMIO High Base	Selects the MMIO High Base setting. Options available: 56T, 40T, 24T, 16T, 4T, 1T. Default setting is **56T**.
MMIO High Granularity Size	Selects the allocation size used to assign mmioh resources. Total mmioh space can be up to 32xgranularity. Per stack mmioh resource assignments are multiples of the granularity where 1 unit per stack is the default allocation. Options available: 1G, 4G, 16G, 64G, 256G, 1024G. Default setting is **256G**.
Isoc Mode	Enable/Disable the Isochronous support in order to meet the QoS requirements (Quality of Service). Options available: Auto, Enable, Disable. Default setting is **Auto**.

5-3-4 Memory Configuration



Integrated Memory Controller (iMC)

Enforce POR: Auto

Enable - Enforces Plan Of Record restrictions for DDR4 frequency and voltage programming. Disable - Disables this feature. Auto - Sets it to the MRC default setting; current default is Enable.

Enable ADR: Enable

Enables the detecting and enabling of ADR

Legacy ADR Mode: Disable

Enable/Disable Legacy ADR Mode

Memory Topology

Displays memory topology with Dimm population information

Memory Timings Override

Selects the XMP profile to use

Memory Map

Set memory mapping settings

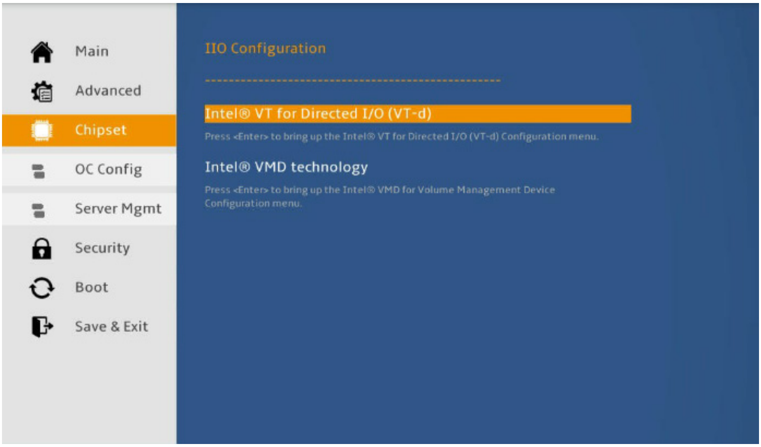
Memory RAS Configuration

Displays and provides option to change the Memory Ras Settings

Parameter	Description
Integrated Memory Controller (iMC)	
Enforce POR	When set to Enable, the system enforces Plan Of Record restrictions for DDR4 frequency and voltage programming. When set to Auto, the system sets it to the MRC default settings. Options available: Auto, POR, Disable. Default setting is **Auto**.
Enable ADR	Enables the detecting and enabling of ADR (Asynchronous DRAM Refresh) function. Options available: Enable/Disable. Default setting is **Enable**.
Legacy ADR Mode	Enable/Disable the Legacy ADR Mode. Options available: Enable/Disable. Default setting is **Disable**.
Memory Topology	Press [Enter] to view memory topology with DIMM population information.
Memory Map	Press [Enter] to configure advanced items. ◆ IMC Interleaving – controls the interleaving between the Integrated Memory Controllers (IMCs). – Options available: Auto, 1-way Interleave, 2-way Interleave. Default setting is **Auto**.

Parameter	Description
Memory RAS Configuration	Press [Enter] to configure advanced items. ◆ Static Virtual Lockstep Mode – Enable/Disable the Static Virtual Lockstep mode. – Options available: Disable/Enable. Default setting is **Disable**. ◆ Mirror Mode – Mirror Mode will set entire 1LM/2LM memory in system to be mirrored, consequently reducing the memory capacity by half. Enables the Mirror Mode will disable the XPT Prefetch. – Options available: Disable, Mirror Mode 1LM, Mirror Mode 2LM. Default setting is **Disable**. ◆ Correctable Error Threshold – Correctable Error Threshold (1-32767) used for sparing, tagging, and leaky bucket. – Press the <+> / <-> keys to increase or decrease the desired values.

5-3-5 IIO Configuration



IIO Configuration

Intel® VT for Directed I/O (VT-d)

Press <Enter> to bring up the Intel® VT for Directed I/O (VT-d) Configuration menu.

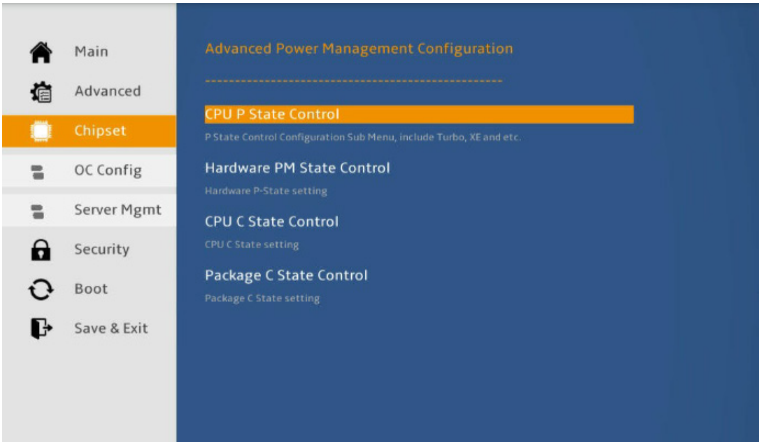
Intel® VMD technology

Press <Enter> to bring up the Intel® VMD for Volume Management Device Configuration menu.

Parameter	Description
IIO Configuration	
Intel® VT for Directed I/O (VT-d)	Press [Enter] to configure advanced items. ◆ Intel® VT for Directed I/O (VT-d) – Enable/Disable the Intel VT for Directed I/O (VT-d) support function by reporting the I/O device assignment to VMM through DMAR ACPI Tables. – Options available: Enable/Disable. Default setting is **Enable**. ◆ Interrupt Remapping – Enable/Disable the interrupt remapping support function. – Options available: Enable/Disable. Default setting is **Enable**. ◆ PassThrough DMA – Enable/Disable the Non-Isoch VT_D Engine PassThrough DMA support function. – Options available: Enable/Disable. Default setting is **Enable**. ◆ ATS – Enable/Disable Non-Isoch VT_D Engine ATS support. – Options available: Enable/Disable. Default setting is **Enable**. ◆ Posted Interrupt – Enable/Disable VT_D posted interrupt. – Options available: Enable/Disable. Default setting is **Enable**. ◆ Coherency Support (Non-Isoch) – Enable/Disable Non-Isoch VT_D Engine Coherency support. – Options available: Enable/Disable. Default setting is **Enable**.

Parameter	Description
Intel® VMD technology	Press [Enter] to configure advanced items. ◆ Intel® VMD technology ◆ Intel® VMD Configuration – Enable/Disable the Intel VMD support function. – Options available: Enable/Disable. Default setting is **Disable**.

5-3-6 Advanced Power Management Configuraiton



Advanced Power Management Configuration

CPU P State Control
P State Control Configuration Sub Menu, include Turbo, XE and etc.

Hardware PM State Control
Hardware P-State setting

CPU C State Control
CPU C State setting

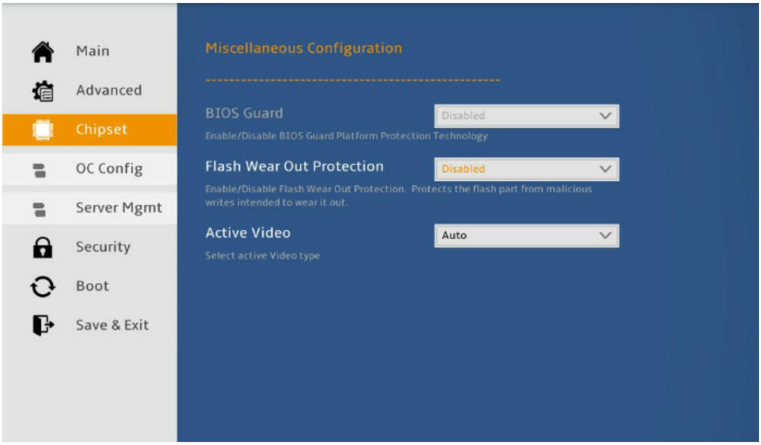
Package C State Control
Package C State setting

Parameter	Description
Advanced Power Management Configuration	
CPU P State Control	Press [Enter] to configure advanced items. ◆ SpeedStep (Pstates) – Conventional Intel SpeedStep Technology switches both voltage and frequency in tandem between high and low levels in response to processor load. – Options available: Enable/Disable. Default setting is **Enable**. ◆ Turbo Mode – When this item is enabled, the processor will automatically ramp up the clock speed of 1-2 of its processing cores to improve its performance. When this item is disabled, the processor will not overclock any of its core. – Options available: Enable/Disable. Default setting is **Enable**.
Hardware PM State Control	Press [Enter] to configure advanced items. ◆ Hardware P-States – When this item is disabled, the processor hardware chooses a P-state based on OS Request (Legacy P-States). – In Native mode, the processor hardware chooses a P-state based on OS guidance. – In Out of Band mode, the processor hardware autonomously chooses a P-state (with no OS guidance). – Options available: Disable, Native Mode, Out of Band Mode, Native Mode with No Legacy Support. Default setting is **Native Mode**.

Parameter	Description
CPU C State Control	Press [Enter] to configure advanced items. ◆ Autonomous Core C-State – Enable/Disable the Autonomous Core C-State Control. – Options available: Enable/Disable. Default setting is **Disable**. ◆ CPU C6 Report – Allows you to determine whether to let the CPU enter C6 mode in system halt state. When enabled, the CPU core frequency and voltage will be reduced during system halt state to decrease power consumption. The C6 state is a more enhanced power-saving state than C1. – Options available: Disable/Enable/Auto. Default setting is **Auto**. ◆ Enhanced Halt State (C1E)(Note) – Core C1E auto promotion control. Takes effect after reboot. – Options available: Enable/Disable. Default setting is **Enable**.
Package C State Control	Configures the state for the C-State package limit. Options available: C0/C1 state, C2 state, C6(non Retention) state, C6(Retention) state, No Limit, Auto. Default setting is **Auto**.

(Note) Advanced items prompt when this item is defined.

5-3-7 Miscellaneous Configuration



Miscellaneous Configuration

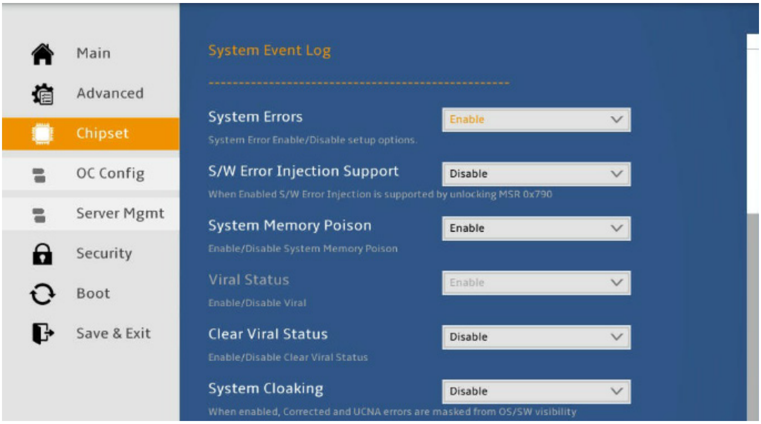
BIOS Guard: Disabled
Enable/Disable BIOS Guard Platform Protection Technology

Flash Wear Out Protection: Disabled
Enable/Disable Flash Wear Out Protection. Protects the flash part from malicious writes intended to wear it out.

Active Video: Auto
Select active Video type

Parameter	Description
Miscellaneous Configuration	
BIOS Guard	Enable/Disable BIOS Guard Platform Protection Technology. Options available: Enabled/Disabled. Default setting is **Disabled**.
Flash Wear Out Protection	Enable/Disable the function to protect the flash part from malicious writes intended to wear it out. Options available: Enabled/Disabled. Default setting is **Disabled**.
Active Video	Selects active video type. Options available: Auto, Onboard Device, PCIE Device. Default setting is **Auto**.

5-3-8 Runtime Error Logging



System Event Log

System Errors — Enable
System Error Enable/Disable setup options.

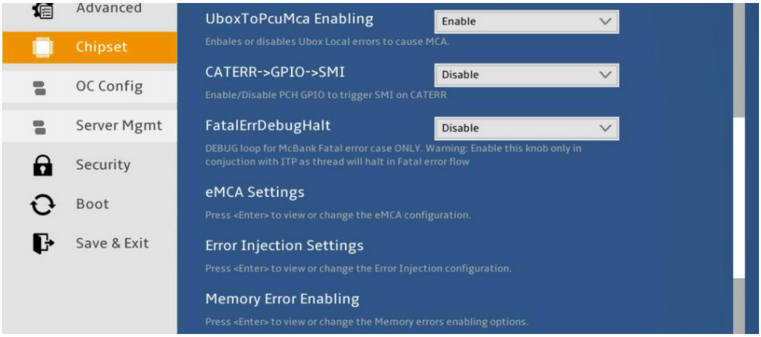
S/W Error Injection Support — Disable
When Enabled S/W Error Injection is supported by unlocking MSR 0x790

System Memory Poison — Enable
Enable/Disable System Memory Poison

Viral Status — Enable
Enable/Disable Viral

Clear Viral Status — Disable
Enable/Disable Clear Viral Status

System Cloaking — Disable
When enabled, Corrected and UCNA errors are masked from OS/SW visibility



UboxToPcuMca Enabling — Enable
Enbales or disables Ubox Local errors to cause MCA.

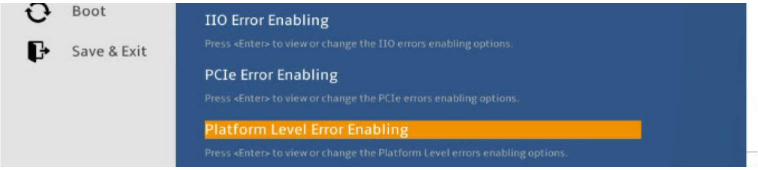
CATERR->GPIO->SMI — Disable
Enable/Disable PCH GPIO to trigger SMI on CATERR

FatalErrDebugHalt — Disable
DEBUG loop for McBank Fatal error case ONLY. Warning: Enable this knob only in conjuction with ITP as thread will halt in Fatal error flow

eMCA Settings
Press <Enter> to view or change the eMCA configuration.

Error Injection Settings
Press <Enter> to view or change the Error Injection configuration.

Memory Error Enabling
Press <Enter> to view or change the Memory errors enabling options.



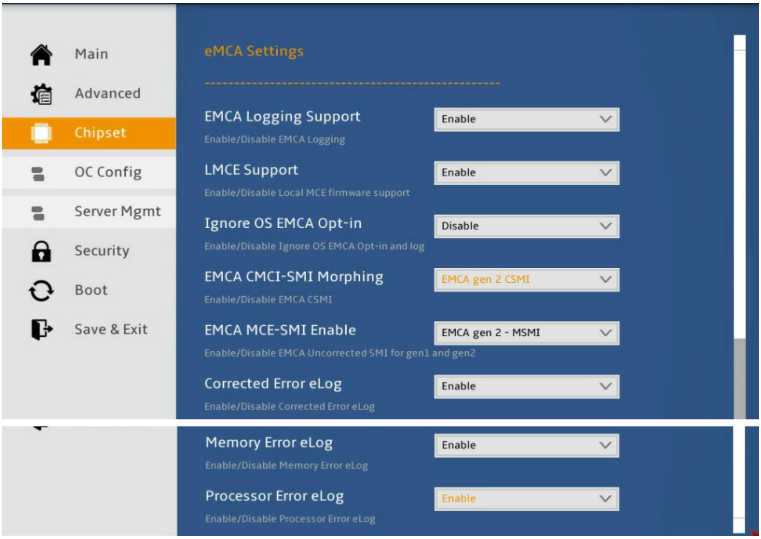
IIO Error Enabling
Press <Enter> to view or change the IIO errors enabling options.

PCIe Error Enabling
Press <Enter> to view or change the PCIe errors enabling options.

Platform Level Error Enabling
Press <Enter> to view or change the Platform Level errors enabling options.

Parameter	Description
System Event Log	
System Errors	Enable/Disable system error logging function. Options available: Enable/Disable. Default setting is **Enable**.
S/W Error Injection Support	When enabled, software error injection is supported by unlocking MSR 0x790. Options available: Enable/Disable. Default setting is **Disable**.
System Memory Poison	Enable/Disable system memory poison function. Options available: Enable/Disable. Default setting is **Enable**.
Viral Status	Enable/Disable viral function. Options available: Enable/Disable. Default setting is **Enable**.
Clear Viral Status	Enable/Disable clear viral function. Options available: Enable/Disable. Default setting is **Disable**.
System Cloaking	When Enabled system cloaking function, corrected and UCNA errors are masked from OS/SW visibility. Options available: Enable/Disable. Default setting is **Disable**.
UboxToPcuMca Enabling	Enable/Disable system to report Ubox local errors to MCA. Options available: Enable/Disable. Default setting is **Enable**.
CATERR->GPIO->SMI	Enable/Disable PCH GPIO to trigger SMI on CATERR. Options available: Enable/Disable. Default setting is **Disable**.
FatalErrDebugHalt	Debug loop for McBank Fatal error case ONLY. **Warning:** Enable this knob only in conjuction with ITP as thread will halt in Fatal error flow. Options available: Enable/Disable. Default setting is **Disable**.
eMCA Settings	Press [Enter] to view or configure advanced items.
Error Injection Settings	Press [Enter] to view or configure advanced items.
Memory Error Enabling	Press [Enter] to view or configure advanced items.
IIO Error Enabling	Press [Enter] to view or configure advanced items.
PCIe Error Enabling	Press [Enter] to view or configure advanced items.
Platform Level Error Enabling	Press [Enter] to view or configure advanced items.

5-3-8-1 eMCA Settings



eMCA Settings

EMCA Logging Support: Enable
Enable/Disable EMCA Logging

LMCE Support: Enable
Enable/Disable Local MCE firmware support

Ignore OS EMCA Opt-in: Disable
Enable/Disable Ignore OS EMCA Opt-in and log

EMCA CMCI-SMI Morphing: EMCA gen 2 CSMI
Enable/Disable EMCA CSMI

EMCA MCE-SMI Enable: EMCA gen 2 - MSMI
Enable/Disable EMCA Uncorrected SMI for gen1 and gen2

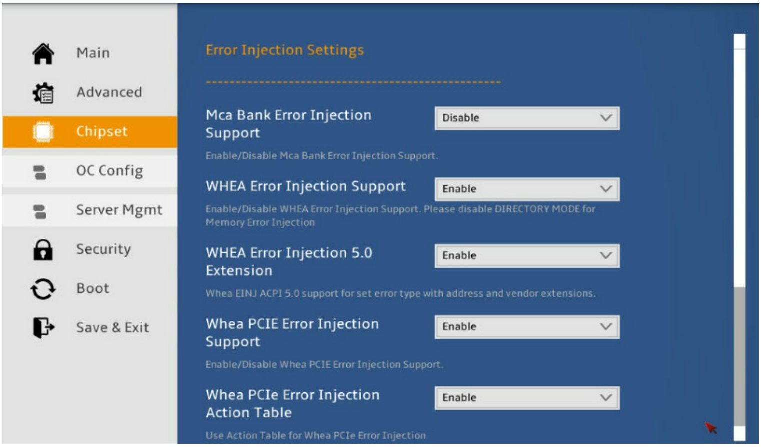
Corrected Error eLog: Enable
Enable/Disable Corrected Error eLog

Memory Error eLog: Enable
Enable/Disable Memory Error eLog

Processor Error eLog: Enable
Enable/Disable Processor Error eLog

Parameter	Description
eMCA Settings	
EMCA Logging Support	Enable/Disable EMCA logging function. Options available: Enable/Disable. Default setting is **Enable**.
LMCE Support	Enable/Disable Local MCE firmware support. Options available: Enable/Disable. Default setting is **Enable**.
Ignore OS EMCA Opt-in	Enable/Disable Ignore OS EMCA Opt-in and log feature. Options available: Enable/Disable. Default setting is **Disable**.
EMCA CMCI-SMI Morphing	Enable/Disable EMCA CSMI support. Options available: Disable, EMCA gen1 Lite, EMCA gen2 CSMI. Default setting is **EMCA gen2 CSMI**.
EMCA MCE-SMI Enable	Enable/Disable EMCA Uncorrected SMI for gen1 and gen2. Options available: Disable, EMCA gen1 Dual Mode, EMCA gen2-MSMI. Default setting is **EMCA gen2-MSMI**.
Corrected Error eLog	Enable/Disable corrected error eLog feature. Options available: Enable/Disable. Default setting is **Enable**.
Processor Error eLog	Enable/Disable processor error eLog feature. Options available: Enable/Disable. Default setting is **Enable**.

5-3-8-2 Error Injection Settings



Error Injection Settings

Mca Bank Error Injection Support — Disable

Enable/Disable Mca Bank Error Injection Support.

WHEA Error Injection Support — Enable

Enable/Disable WHEA Error Injection Support. Please disable DIRECTORY MODE for Memory Error Injection

WHEA Error Injection 5.0 Extension — Enable

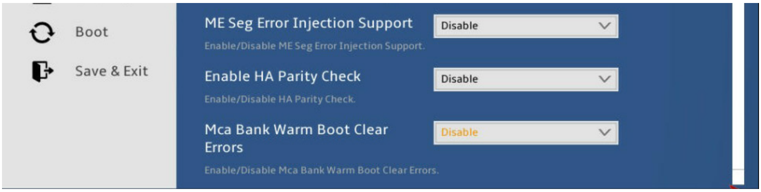
Whea EINJ ACPI 5.0 support for set error type with address and vendor extensions.

Whea PCIE Error Injection Support — Enable

Enable/Disable Whea PCIE Error Injection Support.

Whea PCIe Error Injection Action Table — Enable

Use Action Table for Whea PCIe Error Injection



ME Seg Error Injection Support — Disable

Enable/Disable ME Seg Error Injection Support.

Enable HA Parity Check — Disable

Enable/Disable HA Parity Check.

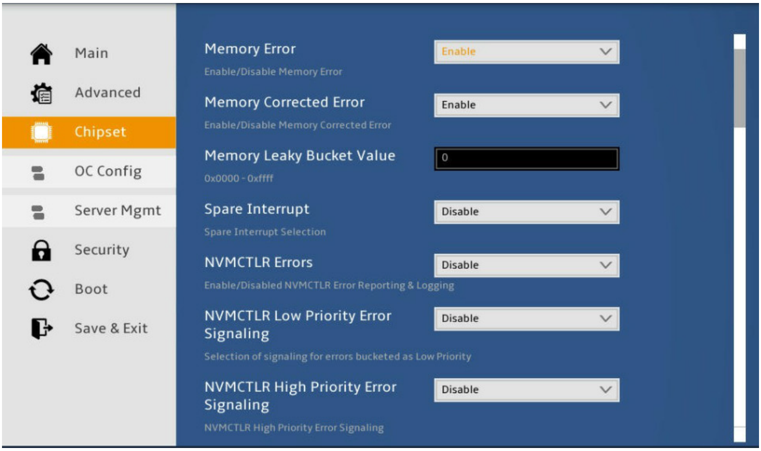
Mca Bank Warm Boot Clear Errors — Disable

Enable/Disable Mca Bank Warm Boot Clear Errors.

Parameter	Description
Error Injection Settings	
Mca Bank Error Injection Support	Enable/Disable Mca Bank Error Injection Support. Options available: Enable/Disable. Default setting is **Disable**.
WHEA Error Injection Support	Enable/Disable WHEA Error Injection support. Please disable DIRECTORY MODE for memory error injection. Options available: Enable/Disable. Default setting is **Enable**.
EHEA Error Injection 5.0 Extension	Enable/Disable Whea EINJ ACPI 5.0 support for set error type with address and vendor extensions. Options available: Enable/Disable. Default setting is **Enable**.
Whea PCIE Error Injection support	Enable/Disable Whea PCIE Error Injection support. Options available: Enable/Disable. Default setting is **Enable**.
Whea PCIe Error Injection Action Table	Enable/Disable Whea PCIe Error Injection Action Table. Options available: Enable/Disable. Default setting is **Enable**.

Parameter	Description
ME Seg Error Injection Support	Enable/Disable ME Seg Error Injection Support. Options available: Enable/Disable. Default setting is **Disable**.
Enable HA Parity Check	Enable/Disable HA Parity Check feature. Options available: Enable/Disable. Default setting is **Disable**.
Mca Bank Warm Boot Clear Errors	Enable/Disable Mca Bank Warm Boot Clear Errors feature. Options available: Enable/Disable. Default setting is **Disable**.

5-3-8-3 Memory Error Enabling



Memory Error — Enable
Enable/Disable Memory Error

Memory Corrected Error — Enable
Enable/Disable Memory Corrected Error

Memory Leaky Bucket Value — 0
0x0000 - 0xffff

Spare Interrupt — Disable
Spare Interrupt Selection

NVMCTLR Errors — Disable
Enable/Disabled NVMCTLR Error Reporting & Logging

NVMCTLR Low Priority Error Signaling — Disable
Selection of signaling for errors bucketed as Low Priority

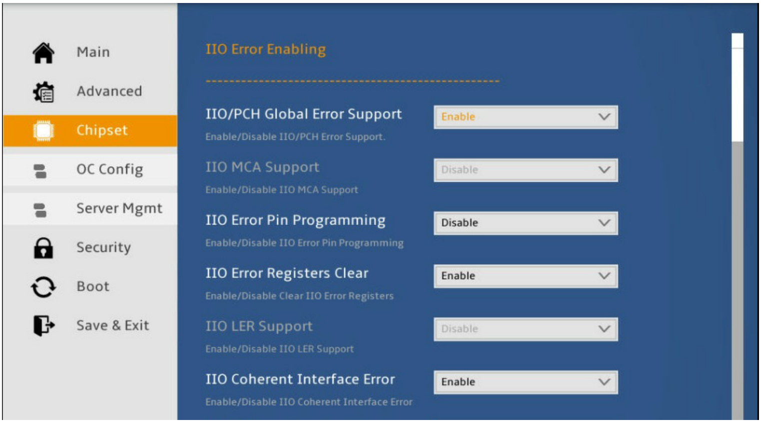
NVMCTLR High Priority Error Signaling — Disable
NVMCTLR High Priority Error Signaling

Parameter	Description
Memory Error Enabling	
Memory Error	Enable/Disable Memory Error. Options available: Enable/Disable. Default setting is **Enable**.
Memory Corrected Error	Enable/Disable Memory Corrected Error. Options available: Enable/Disable. Default setting is **Enable**.
Memory Leaky Bucket Value	Sets Memory Leaky Bucket Value. (0x0000 - 0xffff)
Spare Interrupt	Selects Spare Interrupt type. Options available: Disable, SMI, Error Pin, CMCI. Default setting is **Disable**.
NVMCTLR Errors	Enable/Disable NVMCTLR Errors Reporting and Logging. Options available: Enable/Disable. Default setting is **Disable**.
NVMCTLR Low Priority Error Signaling	Specifies the NVMCTLR low priority signaling. Options available: Disable, SMI, ERRO# Pin. Default setting is **Disable**.
NVMCTLR High Priority Error Signaling	Specifies the NVMCTLR high priority signaling. Options available: Disable, SMI, ERRO# Pin. Default setting is **Disable**.

Parameter	Description
CLR/Ring[(Note)]	Press [Enter] to configure advanced items. ◆ CLR Max OC Ratio – Sets the maximum OC Ratio for the CLR Domain. ◆ CLR Min Ratio – Sets the minimum ratio for the CLR Domain. ◆ CLR Voltage Mode – In Override mode, the voltage selected will be applied over all operating frequencies. – In Adaptive mode, the voltage is interpolated only in turbo mode. – Options available: Adaptive/Override. Default setting is **Adaptive**. ◆ CLR Extra Turbo Voltage – Specifies the extra turbo voltage applied while GT is operating in millivolts. Range 0-2000 mV. ◆ CLR Voltage Offset – Specifies the Offset voltage applied to GT domain. This voltage is specified in millivolts. Range -1000 to 1000 mV. ◆ Offset Prefix – Sets the offset value as positive or negative.
Uncore[(Note)]	Press [Enter] to configure advanced items. ◆ Uncore Voltage Offset – Specifies the Offset voltage applied to the Uncore domain. This voltage is specified in millivolts. Range -1000 to 1000 mV. ◆ Offset Prefix – Sets the offset value as positive or negative.
SVID/FIVR[(Note)]	Press [Enter] to configure advanced items. ◆ VCCIN – Enable/Disable VCCIN through external VR. – Options available: Enable/Disable. Default setting is **Disable**. ◆ FIVR Faults – Enable/Disable FIVR faults. When this function are disabled, OVP and OCP protection mechanisms will be masked. This is a dangerous configuration and the risk of using it is assumed by the user. – Options available: Enable/Disable. Default setting is **Enable**. ◆ FIVR Efficiency Management – FIVR efficiency management is good for power delivery efficiency, but it may be an impediment to proper power delivery control under overclocking, particularly BCLK overclocking. – Options available: Enable/Disable. Default setting is **Enable**.
TJ-Max offset[(Note)]	Changes the TJ-Max offset (125°C - fuse value).

(Note) This item appears when **OverClocking Feature** is set to **Enabled**.

5-3-8-4 IIO Error Enabling



IIO Error Enabling

IIO/PCH Global Error Support — Enable
Enable/Disable IIO/PCH Error Support.

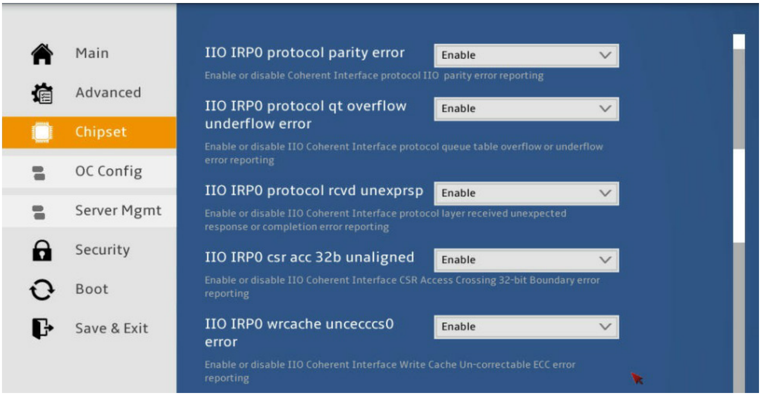
IIO MCA Support — Disable
Enable/Disable IIO MCA Support

IIO Error Pin Programming — Disable
Enable/Disable IIO Error Pin Programming

IIO Error Registers Clear — Enable
Enable/Disable Clear IIO Error Registers

IIO LER Support — Disable
Enable/Disable IIO LER Support

IIO Coherent Interface Error — Enable
Enable/Disable IIO Coherent Interface Error



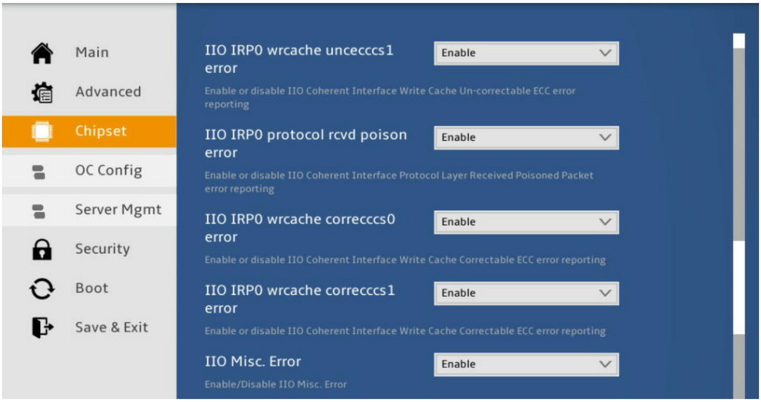
IIO IRP0 protocol parity error — Enable
Enable or disable Coherent Interface protocol IIO parity error reporting

IIO IRP0 protocol qt overflow underflow error — Enable
Enable or disable IIO Coherent Interface protocol queue table overflow or underflow error reporting

IIO IRP0 protocol rcvd unexprsp — Enable
Enable or disable IIO Coherent Interface protocol layer received unexpected response or completion error reporting

IIO IRP0 csr acc 32b unaligned — Enable
Enable or disable IIO Coherent Interface CSR Access Crossing 32-bit Boundary error reporting

IIO IRP0 wrcache uncecccs0 error — Enable
Enable or disable IIO Coherent Interface Write Cache Un-correctable ECC error reporting



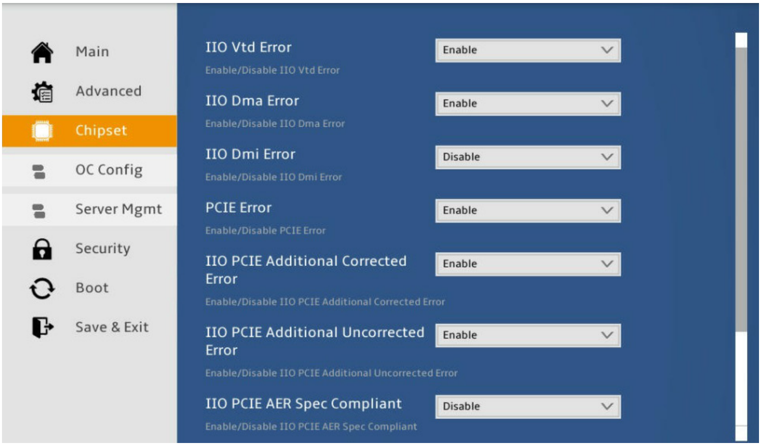
IIO IRP0 wrcache uncecccs1 error — Enable
Enable or disable IIO Coherent Interface Write Cache Un-correctable ECC error reporting

IIO IRP0 protocol rcvd poison error — Enable
Enable or disable IIO Coherent Interface Protocol Layer Received Poisoned Packet error reporting

IIO IRP0 wrcache correcccs0 error — Enable
Enable or disable IIO Coherent Interface Write Cache Correctable ECC error reporting

IIO IRP0 wrcache correcccs1 error — Enable
Enable or disable IIO Coherent Interface Write Cache Correctable ECC error reporting

IIO Misc. Error — Enable
Enable/Disable IIO Misc. Error



IIO Vtd Error: Enable

Enable/Disable IIO Vtd Error

IIO Dma Error: Enable

Enable/Disable IIO Dma Error

IIO Dmi Error: Disable

Enable/Disable IIO Dmi Error

PCIE Error: Enable

Enable/Disable PCIE Error

IIO PCIE Additional Corrected Error: Enable

Enable/Disable IIO PCIE Additional Corrected Error

IIO PCIE Additional Uncorrected Error: Enable

Enable/Disable IIO PCIE Additional Uncorrected Error

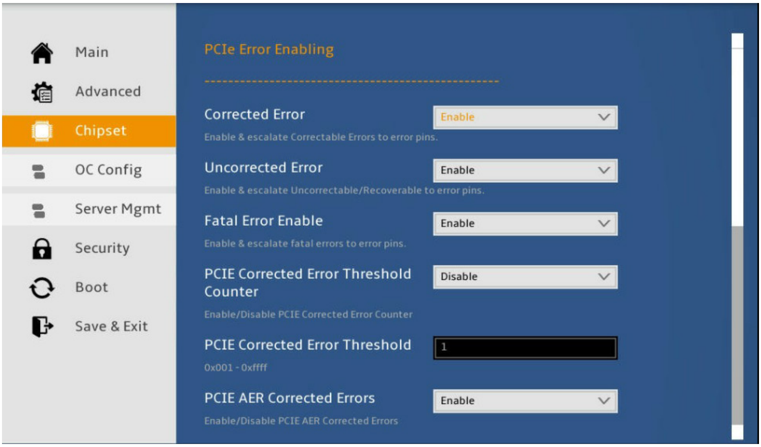
IIO PCIE AER Spec Compliant: Disable

Enable/Disable IIO PCIE AER Spec Compliant

Parameter	Description
IIO Error Enabling	
IIO/PCH Global Error Support	Enable/Disable IIO/PCH Error Support. Options available: Enable/Disable. Default setting is **Enable**.
IIO MCA Support	Enable/Disable IIO MCA Support. Options available: Enable/Disable. Default setting is **Disable**.
IIO Error Pin Programming	Enable/Disable IIO Error Pin Programming. Options available: Enable/Disable. Default setting is **Disable**.
IIO Error Registers Clear	Enable/Disable clearing IIO Error registers. Options available: Enable/Disable. Default setting is **Enable**.
IIO LER Support	Enable/Disable IIO LER Support. Options available: Enable/Disable. Default setting is **Disable**.
IIO Coherent Interface Error	Enable/Disable IIO Coherent Interface Error. Options available: Enable/Disable. Default setting is **Enable**.
IIO IRP0 protocol parity error	Enable/Disable Coherent Interface protocol IIO parity error reporting. Options available: Enable/Disable. Default setting is **Enable**.
IIO IRP0 protocol qt overflow underflow error	Enable/Disable IIO Coherent Interface protocol queue table overflow or underflow error reporting. Options available: Enable/Disable. Default setting is **Enable**.
IIO IRP0 protocol rcvd unexprsp	Enable/Disable IIO Coherent Interface protocol layer received unexpected response or completion error reporting. Options available: Enable/Disable. Default setting is **Enable**.
IIO IRP0 csr acc 32b unaligned	Enable/Disable IIO Coherent Interface CSR Access Crossing 32-bit Boundary error reporting. Options available: Enable/Disable. Default setting is **Enable**.

Parameter	Description
IIO IRP0 wrcache uncecccs0 error	Enable/Disable IIO Coherent Interface Write Cache Un-correctable ECC error reporting. Options available: Enable/Disable. Default setting is **Enable**.
IIO IRP0 wrcache uncecccs1 error	Enable/Disable IIO Coherent Interface Write Cache Un-correctable ECC error reporting. Options available: Enable/Disable. Default setting is **Enable**.
IIO IRP0 protocol rcvd poison error	Enable/Disable IIO Coherent Interface protocol layer received poisoned packet error reporting. Options available: Enable/Disable. Default setting is **Enable**.
IIO IRP0 wrcache correcccs0 error	Enable/Disable IIO Coherent Interface Write Cache Correctable ECC error reporting. Options available: Enable/Disable. Default setting is **Enable**.
IIO IRP0 wrcache correcccs1 error	Enable/Disable IIO Coherent Interface Write Cache Correctable ECC error reporting. Options available: Enable/Disable. Default setting is **Enable**.
IIO Misc. Error	Enable/Disable IIO Misc. Error. Options available: Enable/Disable. Default setting is **Enable**.
IIO Vtd Error	Enable/Disable IIO Vtd Error. Options available: Enable/Disable. Default setting is **Enable**.
IIO Dma Error	Enable/Disable IIO DMA Error. Options available: Enable/Disable. Default setting is **Enable**.
IIO Dmi Error	Enable/Disable IIO DMI Error. Options available: Enable/Disable. Default setting is **Disable**.
PCIE Error	Enable/Disable PCIe Error. Options available: Enable/Disable. Default setting is **Enable**.
IIO PCIE Additional Corrected Error	Enable/Disable IIO PCIe additional corrected error. Options available: Enable/Disable. Default setting is **Enable**.
IIO PCIE Additional Uncorrected Error	Enable/Disable IIO PCIe additional uncorrected error. Options available: Enable/Disable. Default setting is **Enable**.
IIO PCIE AER Spec Compliant	Enable/Disable IIO PCIe AER(Advanced Error Reporting) Spec compliant. Options available: Enable/Disable. Default setting is **Disable**.

5-3-8-5 PCIe Error Enabling



PCIe Error Enabling

Corrected Error — Enable
Enable & escalate Correctable Errors to error pins.

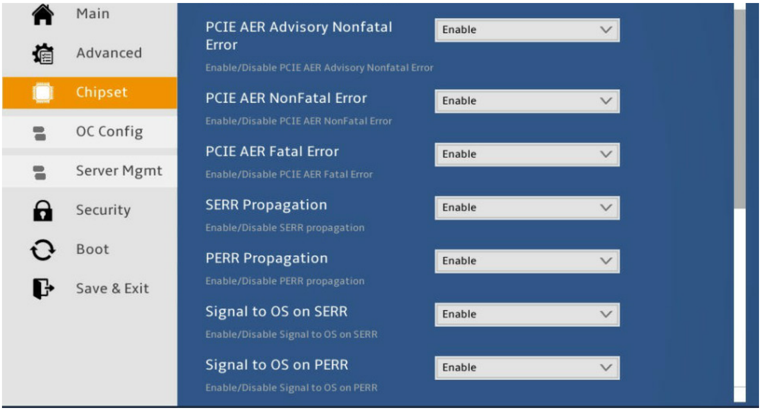
Uncorrected Error — Enable
Enable & escalate Uncorrectable/Recoverable to error pins.

Fatal Error Enable — Enable
Enable & escalate fatal errors to error pins.

PCIE Corrected Error Threshold Counter — Disable
Enable/Disable PCIE Corrected Error Counter

PCIE Corrected Error Threshold — 1
0x001 - 0xffff

PCIE AER Corrected Errors — Enable
Enable/Disable PCIE AER Corrected Errors



PCIE AER Advisory Nonfatal Error — Enable
Enable/Disable PCIE AER Advisory Nonfatal Error

PCIE AER NonFatal Error — Enable
Enable/Disable PCIE AER NonFatal Error

PCIE AER Fatal Error — Enable
Enable/Disable PCIE AER Fatal Error

SERR Propagation — Enable
Enable/Disable SERR propagation

PERR Propagation — Enable
Enable/Disable PERR propagation

Signal to OS on SERR — Enable
Enable/Disable Signal to OS on SERR

Signal to OS on PERR — Enable
Enable/Disable Signal to OS on PERR

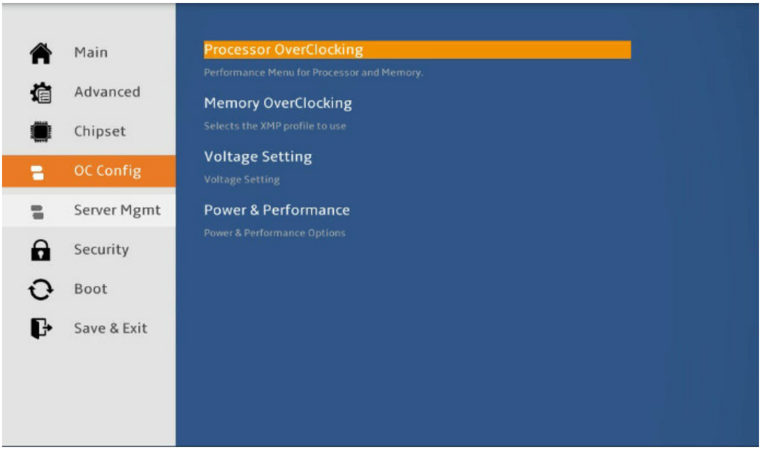
Parameter	Description
PCIe Error Enabling	
Corrected Error	Enables and escalates Correctable Errors to error pins. Options available: Enable/Disable. Default setting is **Enable**.
Uncorrected Error	Enables and escalates Uncorrectable/Recoverable Errors to error pins. Options available: Enable/Disable. Default setting is **Enable**.
Fatal Error Enable	Enables and escalates Fatal Errors to error pins. Options available: Enable/Disable. Default setting is **Enable**.
PCIE Corrected Error Threshold Counter	Enable/Disable PCIe corrected error counter. Options available: Enable/Disable. Default setting is **Disable**.

Parameter	Description
PCIE Corrected Error Threshold	Configures PCIe corrected error threshold. (0x001 - 0xfff)
PCIE AER Corrected Errors	Enable/Disable PCIe AER corrected error. Options available: Enable/Disable. Default setting is **Enable**.
PCIE AER Advisory Nonfatal Error	Enable/Disable PCIe AER nonfatal error. Options available: Enable/Disable. Default setting is **Enable**.
PCIE AER Fatal Error	Enable/Disable PCIe AER fatal error. Options available: Enable/Disable. Default setting is **Enable**.
SERR Propagation	Enable/Disable SERR propagation. Options available: Enable/Disable. Default setting is **Enable**.
PERR Propagation	Enable/Disable PERR propagation. Options available: Enable/Disable. Default setting is **Enable**.
Signal to OS on SERR	Enable/Disable Signal to OS on SERR. Options available: Enable/Disable. Default setting is **Enable**.
Signal to OS on PERR	Enable/Disable Signal to OS on PERR. Options available: Enable/Disable. Default setting is **Enable**.

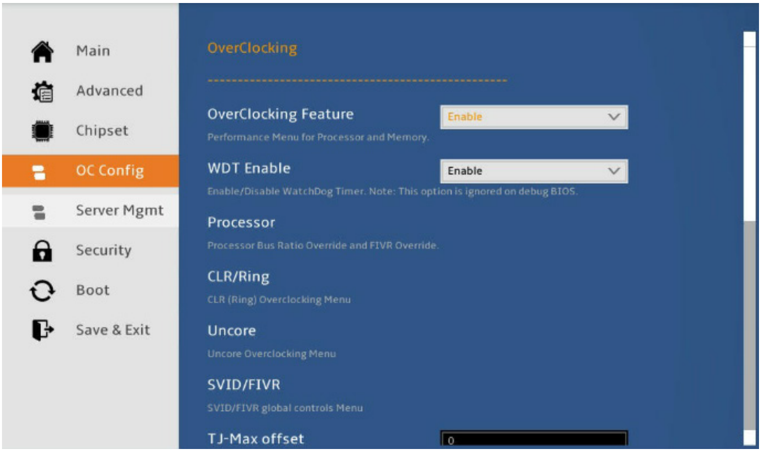
5-4 OC Configuration Menu

OC Configuration menu displays submenu options for configuring the function of Processor OverClocking, Memory OverClocking, Voltage Setting and Power & Performace.

Select a submenu item, then press <Enter> to access the related submenu screen.



5-4-1 Processor OverClocking



OverClocking

OverClocking Feature — Enable

Performance Menu for Processor and Memory.

WDT Enable — Enable

Enable/Disable WatchDog Timer. Note: This option is ignored on debug BIOS.

Processor

Processor Bus Ratio Override and FIVR Override.

CLR/Ring

CLR (Ring) Overclocking Menu

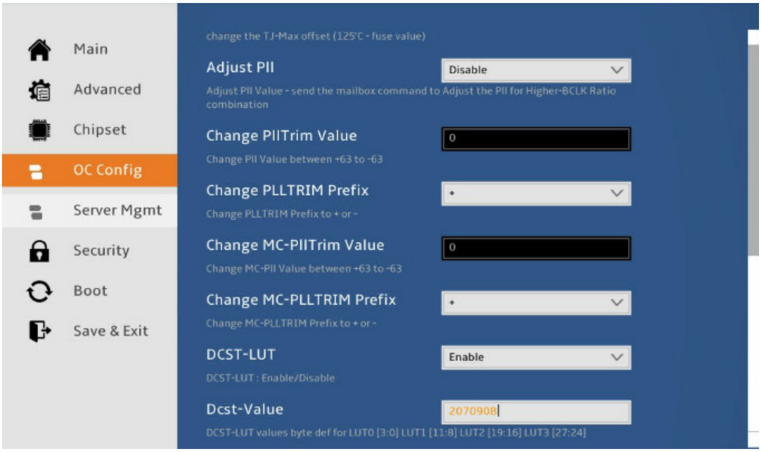
Uncore

Uncore Overclocking Menu

SVID/FIVR

SVID/FIVR global controls Menu

TJ-Max offset — 0



change the TJ-Max offset (125'C - fuse value)

Adjust Pll — Disable

Adjust Pll Value - send the mailbox command to Adjust the Pll for Higher-BCLK Ratio combination

Change PllTrim Value — 0

Change Pll Value between +63 to -63

Change PLLTRIM Prefix — +

Change PLLTRIM Prefix to + or -

Change MC-PllTrim Value — 0

Change MC-Pll Value between +63 to -63

Change MC-PLLTRIM Prefix — +

Change MC-PLLTRIM Prefix to + or -

DCST-LUT — Enable

DCST-LUT : Enable/Disable

Dcst-Value — 207090B

DCST-LUT values byte def for LUT0 [3:0] LUT1 [11:8] LUT2 [19:16] LUT3 [27:24]

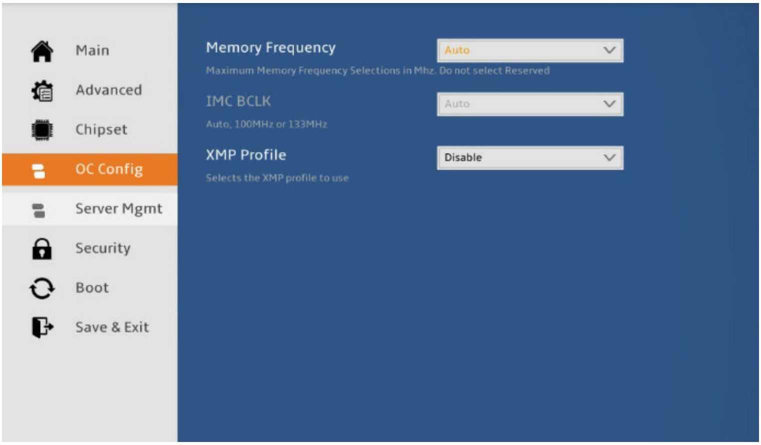
Parameter	Description
OverClocking	
OverClocking Feature	Enable/Disable OverClocking feature. Options available: Enable/Disable. Default setting is **Disable**.
WDT Enable	Enable/Disable WatchDog Timer. Note: This option is ignored on debug BIOS. Options available: Enable/Disable. Default setting is **Enable**.
Processor[(Note)]	Press [Enter] to configure advanced items. ◆ CPU Mode – Options available: All core/Per core. Default setting is **All core**. ◆ Core Max OC Ratio – Sets the maximum OC Ratio for the CPU core. Range 0-80. ◆ Core Voltage Mode – In Override mode, the voltage selected will be applied over all operating frequencies. – In Adaptive mode, the voltage is interpolated only in turbo mode. – Options available: Adaptive/Override. Default setting is **Adaptive**. ◆ Core Extra Turbo Voltage – Specifies the extra turbo voltage applied while IA core is operating in turbo mode. Range 0-2000 mV. ◆ Core Voltage Offset – Specifies the Offset voltage applied to IA core domain. This voltage is specified in millivolts. Range -500 to 500 mV. ◆ Offset Prefix – Sets the offset value as positive or negative. ◆ AVX2 Negative Offset – AVX2 Negative Offset applied by Pcode OC mailbox read(0x1A)/Write(0x1B). ◆ AVX3 Negative Offset – AVX3 Negative Offset applied by Pcode OC mailbox read(0x1A)/Write(0x1B). ◆ BCLK Setting – Options available: 1, 2, 3, 4, 5, 6, 7. Default setting is **7**.

(Note) This item appears when **OverClocking Feature** is set to **Enabled**.

Parameter	Description
Adjust Pll(Note)	Enable/Disable Adjust Pll Value - send the mailbox command to adjust the Pll for Higher-BCLK Ratio combination. Options available: Enable/Disable. Default setting is **Disable**.
Change PllTrim Value(Note)	Changes Pll Value between +63 to -63.
Change PLLTRIM Prefix(Note)	Changes PLLTRIM Prefix to + or -.
Change MC-PllTrim Value(Note)	Changes MC-Pll Value between +63 to -63.
Change MC-PllTrim Prefix(Note)	Changes MC-PLLTRIM Prefix to + or -.
DCST-LUT(Note)	Enable/Disable DCST-LUT feature. Options available: Enable/Disable. Default setting is **Enable**.
Dcst-Value(Note)	Configues the DCST-LUT values byte def for LUT0 [3:0] LUT1 [11:8] LUT2 [19:16] LUT3 [27:24].

(Note) This item appears when **OverClocking Feature** is set to **Enabled**.

5-4-2 Memory OverClocking



Memory Frequency: Auto

Maximum Memory Frequency Selections in Mhz. Do not select Reserved

IMC BCLK: Auto

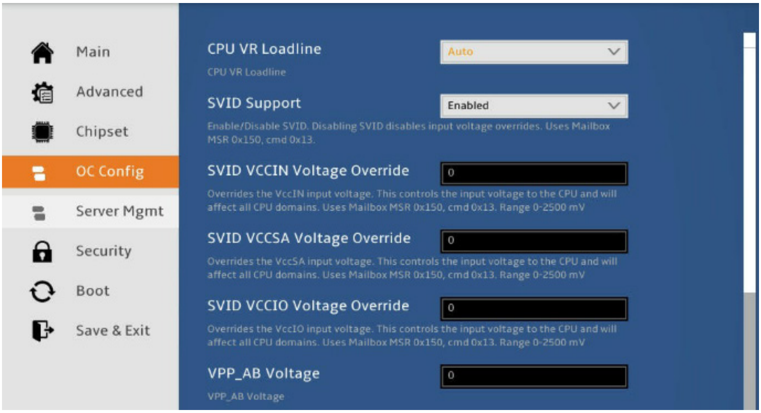
Auto, 100MHz or 133MHz

XMP Profile: Disable

Selects the XMP profile to use

Parameter	Description
Memory Frequency	Configures the maximum memory frequency. Default setting is **Auto**.
IMC BCLK	Configures IMC BCLK. Default setting is **Auto**.
XMP Profile	Selects the XMP profile to use. Options available: Disable, Manual, Profile1. Default setting is **Disable**.

5-4-3 Voltage Setting



CPU VR Loadline: Auto
CPU VR Loadline

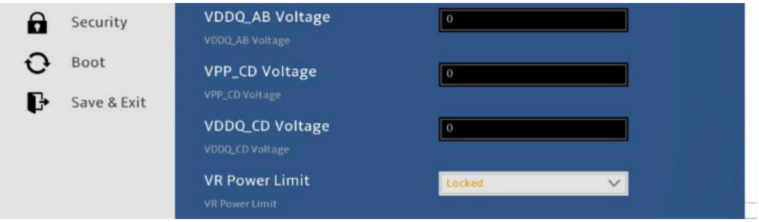
SVID Support: Enabled
Enable/Disable SVID. Disabling SVID disables input voltage overrides. Uses Mailbox MSR 0x150, cmd 0x13.

SVID VCCIN Voltage Override: 0
Overrides the VccIN input voltage. This controls the input voltage to the CPU and will affect all CPU domains. Uses Mailbox MSR 0x150, cmd 0x13. Range 0-2500 mV

SVID VCCSA Voltage Override: 0
Overrides the VccSA input voltage. This controls the input voltage to the CPU and will affect all CPU domains. Uses Mailbox MSR 0x150, cmd 0x13. Range 0-2500 mV

SVID VCCIO Voltage Override: 0
Overrides the VccIO input voltage. This controls the input voltage to the CPU and will affect all CPU domains. Uses Mailbox MSR 0x150, cmd 0x13. Range 0-2500 mV

VPP_AB Voltage: 0
VPP_AB Voltage



VDDQ_AB Voltage: 0
VDDQ_AB Voltage

VPP_CD Voltage: 0
VPP_CD Voltage

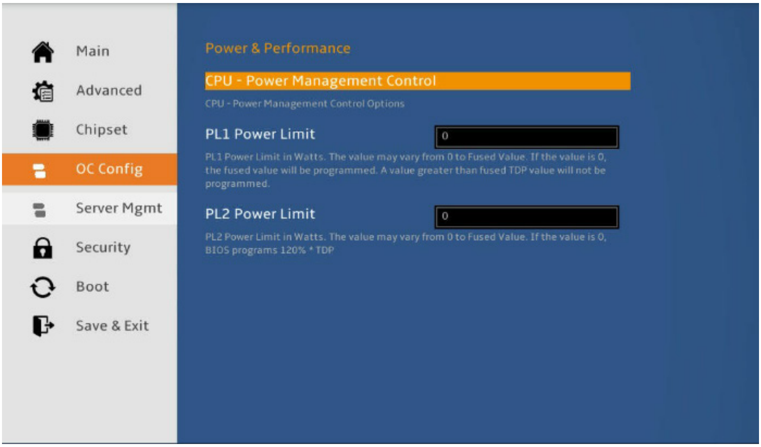
VDDQ_CD Voltage: 0
VDDQ_CD Voltage

VR Power Limit: Locked
VR Power Limit

Parameter	Description
CPU VR Loadline	Configures CPU VR Loadline. Options available: Auto, Level 1, Level 2, Level 3. Default setting is **Auto**.
SVID Support	Enable/Disable SVID support to input voltage overrides. Options available: Enabled/Disabled. Default setting is **Enabled**.
SVID VCCIN Voltage Override	Sets a value (0~2500 mV) for overriding the VccIN input voltage. This controls the input voltage to the CPU and will affect all CPU domains. Default setting is **0**.
SVID VCCSA Voltage Override	Sets a value (0~2500 mV) for overriding the VccSA input voltage. This controls the input voltage to the CPU and will affect all CPU domains. Default setting is **0**.
SVID VCCIO Voltage Override	Sets a value (0~2500 mV) for overriding the VccIO input voltage. This controls the input voltage to the CPU and will affect all CPU domains. Default setting is **0**.
VPP_AB Voltage	Configures the settings of VPP_AB Voltage.
VDDQ_AB Voltage	Configures the settings of VDDQ_AB Voltage.
VPP_CD Voltage	Configures the settings of VPP_CD Voltage.

Parameter	Description
VDDQ_CD Voltage	Configures the settings of VDDQ_CD Voltage.
VR Power Limit	Configures VR Power Limit. Options available: Locked/Unclocked. Default setting is **Locked**.

5-4-4 Power & Performance



Power & Performance

CPU - Power Management Control

CPU - Power Management Control Options

PL1 Power Limit 0

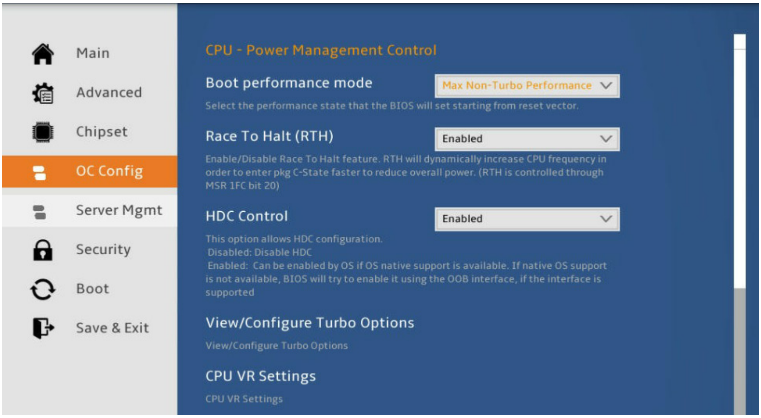
PL1 Power Limit in Watts. The value may vary from 0 to Fused Value. If the value is 0, the fused value will be programmed. A value greater than fused TDP value will not be programmed.

PL2 Power Limit 0

PL2 Power Limit in Watts. The value may vary from 0 to Fused Value. If the value is 0, BIOS programs 120% * TDP

Parameter	Description
Power & Performance	
CPU-Power Management Control	Press [Enter] to configure advanced items.
PL1 Power Limit	Configures PL1 Power Limit in Watts. The value may vary from 0 to fused value. If the value is 0, the fused value will be programmed. A value greater than fused TDP value will not be programmed.
PL2 Power Limit	Configures PL2 Power Limit in Watts. The value may vary from 0 to fused value. If the value is 0, BIOS programs 120% * TDP.

5-4-4-1 CPU-Power Management Control



CPU - Power Management Control

Boot performance mode: Max Non-Turbo Performance

Select the performance state that the BIOS will set starting from reset vector.

Race To Halt (RTH): Enabled

Enable/Disable Race To Halt feature. RTH will dynamically increase CPU frequency in order to enter pkg C-State faster to reduce overall power. (RTH is controlled through MSR 1FC bit 20)

HDC Control: Enabled

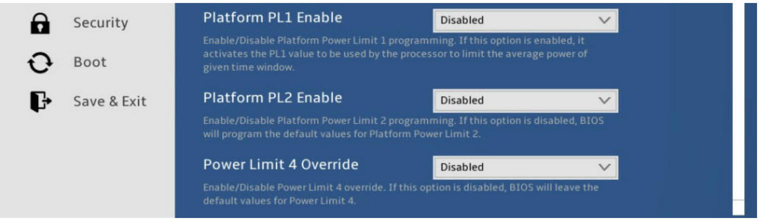
This option allows HDC configuration.
Disabled: Disable HDC
Enabled: Can be enabled by OS if OS native support is available. If native OS support is not available, BIOS will try to enable it using the OOB interface, if the interface is supported

View/Configure Turbo Options

View/Configure Turbo Options

CPU VR Settings

CPU VR Settings



Platform PL1 Enable: Disabled

Enable/Disable Platform Power Limit 1 programming. If this option is enabled, it activates the PL1 value to be used by the processor to limit the average power of given time window.

Platform PL2 Enable: Disabled

Enable/Disable Platform Power Limit 2 programming. If this option is disabled, BIOS will program the default values for Platform Power Limit 2.

Power Limit 4 Override: Disabled

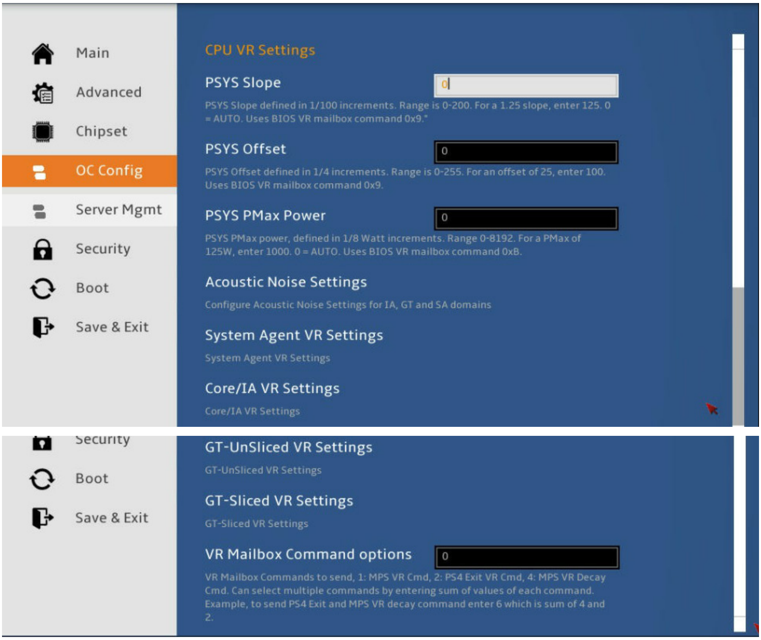
Enable/Disable Power Limit 4 override. If this option is disabled, BIOS will leave the default values for Power Limit 4.

Parameter	Description
CPU-Power Management Control	
Boot performance mode	Selects the performance state that the BIOS will set starting from reset vector. Options available: Max Battery, Max Non-Turbo Performance, Turbo Performance. Default setting is **Max Non-Turbo Performance**.
Race To Halt (RTH)	Enable/Disable Race to Halt feature. RTH will dynamically increase CPU frequency in order to enter pkg C-state faster to reduce overall power. (RTH is controlled through MSR 1FC bit 20) Options available: Enabled/Disabled. Default setting is **Enabled**.
HDC Control	Enable/Disable HDC configuration. Options available: Enabled/Disabled. Default setting is **Enabled**.

Parameter	Description
View/Configure Turbo Options	Press [Enter] to view/configure Turbo Options. ◆ Energy Efficient P-state – Enable/Disable Energy Efficient P-state feature. – Options available: Enabled/Disabled. Default setting is **Enabled**. ◆ Package Power Limit MSR Lock – Enable/Disable locking of package power limit settings. When enabled, PACKAGE_POWER_LIMIT MSR will be locked and a reset will be required to unlock the register. – Options available: Enabled/Disabled. Default setting is **Disabled**. ◆ PL1 Limit – Enable/Disable PL1 limit feature. If this option is disabled, BIOS will program the default values for PL1 Power Limit and PL1 Time Window. – Options available: Enabled/Disabled. Default setting is **Disabled**. ◆ PL1 Power Limit – Configures PL1 power limit in Watts. The value may vary from 0 to fused value. If the value is 0, the fused value will be programmed. A value greater than fused TDP value will not be programmed. ◆ PL1 Time Window – Configures PL1 value in seconds. The value may vary from 0 to 56. Indicated the time window over which TDP value should be maintained. if the value is 0, the fused value will be programmed. ◆ Power Limit 2 Override – Enable/Disable power limit 2 override. If this option is disabled, BIOS will program the default values for Power Limit 2. – Options available: Enabled/Disabled. Default setting is **Enabled**. ◆ Power Limit 2 – Configures PL2 power limit in Watts. The value may vary from 0 to fused value. If the value is 0, BIOS programs 120% * TDP. ◆ #1/2/3/4-Core Ratio Limit Override – Configures #-Core Ratio Limit with range 0 to 83. The minimum rang may vary between processors. – The 1-Core Ratio Limit must be greater than or equal to 2-Core Ratio Limit, 3-Core Ratio Limit, 4-Core Ratio Limit.

Parameter	Description
View/Configure Turbo Options (continued)	◆ Energy Efficient Turbo – Enable/Disable Energy Efficient Turbo feature. This feature will opportunistically lower the turbo frequency to increase efficiency. Recommended only to disable in overclocking situations where turbo frequency must remain constant. Otherwise, leave enabled. – Options available: Enabled/Disabled. Default setting is **Enabled**.
CPU VR Settings	Press [Enter] to configure advanced items.
Platform PL1 Enable	Enable/Disable Platform Power Limit 1 programming. If this item is enabled, it will activate the PL1 value to be used by the processor to limit the average power of given time window. Options available: Enabled/Disabled. Default setting is **Disabled**.
Platform PL2 Enable	Enable/Disable Platform Power Limit 2 programming. If this item is disabled, BIOS will program the default values for Platform Power Limit 2. Options available: Enabled/Disabled. Default setting is **Disabled**.
Power Limit 4 Override	Enable/Disable Power Limit 4 override, If this item is disabled, BIOS will leave the default values for Power Limit 4. Options available: Enabled/Disabled. Default setting is **Disabled**.

5-4-4-1-1 CPU VR Setting



CPU VR Settings

PSYS Slope 0

PSYS Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x9."

PSYS Offset 0

PSYS Offset defined in 1/4 increments. Range is 0-255. For an offset of 25, enter 100. Uses BIOS VR mailbox command 0x9.

PSYS PMax Power 0

PSYS PMax power, defined in 1/8 Watt increments. Range 0-8192. For a PMax of 125W, enter 1000. 0 = AUTO. Uses BIOS VR mailbox command 0xB.

Acoustic Noise Settings

Configure Acoustic Noise Settings for IA, GT and SA domains

System Agent VR Settings

System Agent VR Settings

Core/IA VR Settings

Core/IA VR Settings

GT-UnSliced VR Settings

GT-UnSliced VR Settings

GT-Sliced VR Settings

GT-Sliced VR Settings

VR Mailbox Command options 0

VR Mailbox Commands to send, 1: MPS VR Cmd, 2: PS4 Exit VR Cmd, 4: MPS VR Decay Cmd. Can select multiple commands by entering sum of values of each command. Example, to send PS4 Exit and MPS VR decay command enter 6 which is sum of 4 and 2.

Parameter	Description
CPU VR Settings	
PSYS Slope	Sets a value for PSYS Slope which is defined in 1/100 increments. The Range is 0-200. Default setting is **0**.
PSYS Offset	Sets a value for PSYS Offset which is defined in 1/4 increments. The Range is 0-255. Default setting is **0**.
PSYS PMax Power	Sets a value for PSYS PMax power which is defined in 1/8 Watt increments. The Range is 0-8192. Default setting is **0**.
Acoustic Noise Settings	Press [Enter] to configure advanced items. ◆ Acoustic Noise Mitigation – Enable/Disable this item to help mitigate acoustic noise on certain SKUs when the CPU is in deeper C state. – Options available: Enabled/Disabled. Default setting is **Disabled**. ◆ IA/GT/SA VR Domain(Note) ◆ Disable Fast PKG C State Ramp for IA/GT/SA Domain(Note) – This option needs to be configured to reduce acoustic nosie during deeper C states. – Options available: TRUE/FALSE. Default setting is **FALSE**.

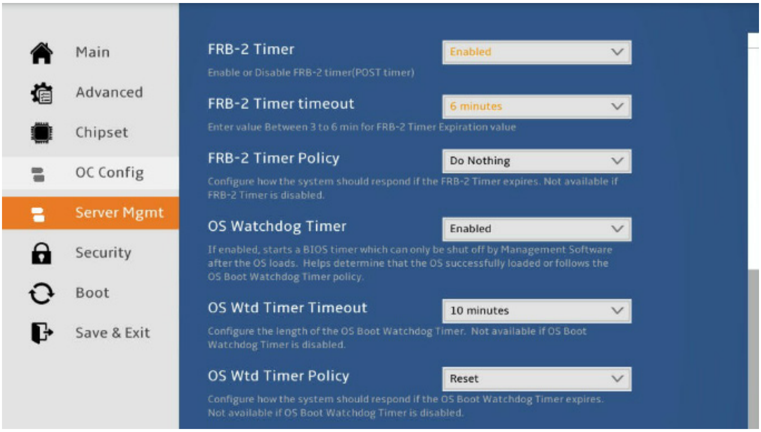
(Note) This item is available when **Acoustic Nosie Mitigation** is set to **Enabled**.

Parameter	Description
Acoustic Noise Settings (continued)	◆ Slow Slew Rate for IA/GT/SA Domain(Note) – Sets VR IA/GT/SA Slow Slew Rate for Deep Package C State ramp time. Slow slew rate equals to Fast devided by number 2, 4, 8, 16. – Options available: Fast/2, Fast/4, Fast/8, Fast/16. Default setting is **Fast/2**.
System Agent VR Settings/ Core/IA VR Settings/ GT-UnSliced VR Settings/ GT-Sliced VR Settings	Press [Enter] to configure advanced items. ◆ VR Config Enable – Enable/Disable VR Configuration. – Options available: Enabled/Disabled. Default setting is **Enabled**. ◆ AC Loadline – Sets a value for AC Loadline which is defined in 1/100 mOhms. A value of 100 equals 1.0 mOhm, and 1255 is 12.55mOhms. The range is 0-6249 (0-62.49 mOhms). Default setting is **0**. ◆ DC Loadline – Sets a value for DC Loadline which is defined in 1/100 mOhms. A value of 100 equals 1.0 mOhm, and 1255 is 12.55mOhms. The range is 0-6249 (0-62.49 mOhms). Default setting is **0**. ◆ PS Current Threshold1 – Sets a value for PS Current Threshold1 which is defined in 1/4A increments. A value of 400 equals 100A. The range is 0-512 which translates to 0-128A. Default setting is **80** for 20A. ◆ PS Current Threshold2 – Sets a value for PS Current Threshold2 which is defined in 1/4A increments. A value of 400 equals 100A. The range is 0-512 which translates to 0-128A. Default setting is **20** for 5A. ◆ PS Current Threshold3 – Sets a value for PS Current Threshold3 which is defined in 1/4A increments. A value of 400 equals 100A. The range is 0-512 which translates to 0-128A. Default setting is **4** for 1A. ◆ PS3 Enable – Enable/Disable PS3. – Options available: Enabled/Disabled. Default setting is **Enabled**.

(Note) This item is available when **Acoustic Nosie Mitigation** is set to **Enabled**.

Parameter	Description
System Agent VR Settings/ Core/IA VR Settings/ GT-UnSliced VR Settings/ GT-Sliced VR Settings (continued)	◆ PS4 Enable – Enable/Disable PS4. – Options available: Enabled/Disabled. Default setting is **Enabled**. ◆ IMON Slope – Sets a value for IMON Slope which is defined in 1/100 increments. The range is 0-200. Default setting is **0**. ◆ IMON Offset – Sets a value for IMON Offset which is defined in 1/1000 increments. The range is 0-63999. Default setting is **0**. ◆ IMON Prefix – Sets the offset value as positive or negative. ◆ VR Current Limit – Sets a value for Voltage Regulator Current Limit. The value represents the maximum instantaneous current allowed at any given time.The value is represented in 1/4A (Ampere) increments. A value of 400 equals 100A. Default setting is **0**. ◆ VR Voltage Limit – Sets a value for VR Voltage Limit which is defined in mV. The range is 0-7999mV, Default setting is **0**. ◆ TDC Enable – Enable/Disable TDC. – Options available: Enabled/Disabled. Default setting is **Enabled**. ◆ TDC Current Limit – Sets a value for TDC current Limit which is defined in 1/8A increments. The range is 0-32767. Default setting is **0**. ◆ TDC Time Window – Options available: 1ms, 2ms, 3ms, 4ms, 5ms, 6ms, 7ms, 8ms, 9ms, 10ms. Default setting is **1ms**. ◆ TDC Lock – Enable/Disable TDC Lock. – Options available: Enabled/Disabled. Default setting is **Disabled**.
VR Mailbox Command options	VR mailbox commands to send, 1:MPS VR cmd, 2:PS4 Exit VR cmd, 4:MPS VR Decay cmd. It can select multiple commands by entering sum of values of each command.

5-5 Server Management Menu



FRB-2 Timer — Enabled
Enable or Disable FRB-2 timer(POST timer)

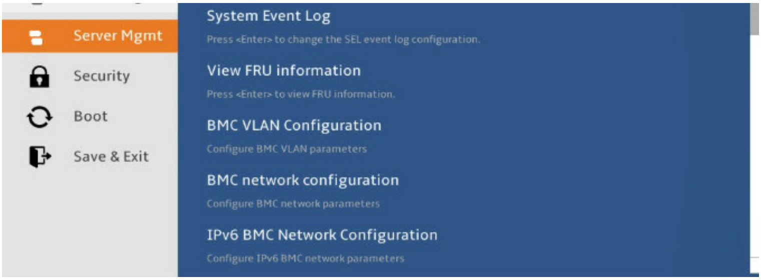
FRB-2 Timer timeout — 6 minutes
Enter value Between 3 to 6 min for FRB-2 Timer Expiration value

FRB-2 Timer Policy — Do Nothing
Configure how the system should respond if the FRB-2 Timer expires. Not available if FRB-2 Timer is disabled.

OS Watchdog Timer — Enabled
If enabled, starts a BIOS timer which can only be shut off by Management Software after the OS loads. Helps determine that the OS successfully loaded or follows the OS Boot Watchdog Timer policy.

OS Wtd Timer Timeout — 10 minutes
Configure the length of the OS Boot Watchdog Timer. Not available if OS Boot Watchdog Timer is disabled.

OS Wtd Timer Policy — Reset
Configure how the system should respond if the OS Boot Watchdog Timer expires. Not available if OS Boot Watchdog Timer is disabled.



System Event Log
Press <Enter> to change the SEL event log configuration.

View FRU information
Press <Enter> to view FRU information.

BMC VLAN Configuration
Configure BMC VLAN parameters

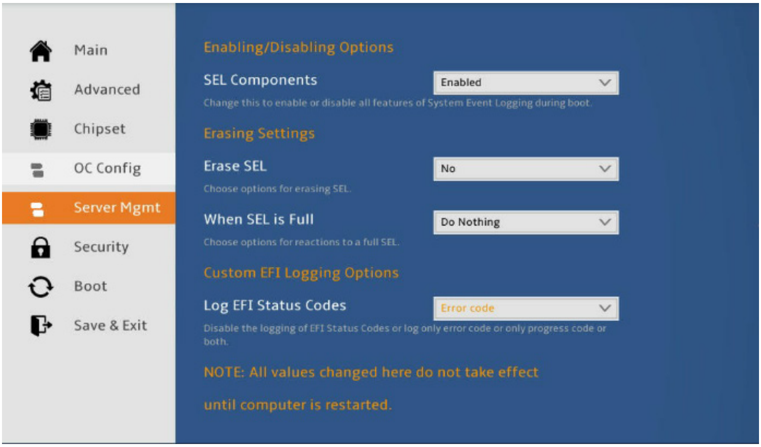
BMC network configuration
Configure BMC network parameters

IPv6 BMC Network Configuration
Configure IPv6 BMC network parameters

Parameter	Description
FRB-2 Timer	Enable/Disable FRB-2 timer (POST timer). Options available: Enabled/Disabled. Default setting is **Disabled**.
FRB-2 Timer timeout	Configure the FRB2 Timer timeout. Options available: 3 minutes/4 minutes/5 minutes/6 minutes. Default setting is **6 minutes**. **Please note that this item is configurable when FRB-2 Timer is set to Enabled.**
FRB-2 Timer Policy	Configure the FRB2 Timer policy. Options available: Do Nothing/Reset/Power Down. Default setting is **Do Nothing**. **Please note that this item is configurable when FRB-2 Timer is set to Enabled.**
OS Watchdog Timer	Enable/Disable OS Watchdog Timer function. Options available: Enabled/Disabled. Default setting is **Disabled**.

Parameter	Description
OS Wtd Timer Timeout	Configure OS Watchdog Timer. Options available: 5 minutes, 10 minutes, 15 minutes, 20 minutes. Default setting is **5 minutes**. **Please note that this item is configurable when OS Watchdog Timer is set to Enabled.**
OS Wtd Timer Policy	Configure OS Watchdog Timer Policy. Options available: Reset/Do Nothing/Power Down. Default setting is **Reset**. **Please note that this item is configurable when OS Watchdog Timer is set to Enabled.**
System Event Log	Press [Enter] to configure advanced items.
View FRU Information	Press [Enter] to view the advanced items.
BMC VLAN Configuration	Press [Enter] to view the advanced items.
BMC network configuration	Press [Enter] to configure advanced items.
IPv6 BMC Network Configuration	Press [Enter] to configure advanced items.

5-5-1 System Event Log



Enabling/Disabling Options

SEL Components: Enabled

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

Erasing Settings

Erase SEL: No

Choose options for erasing SEL.

When SEL is Full: Do Nothing

Choose options for reactions to a full SEL.

Custom EFI Logging Options

Log EFI Status Codes: Error code

Disable the logging of EFI Status Codes or log only error code or only progress code or both.

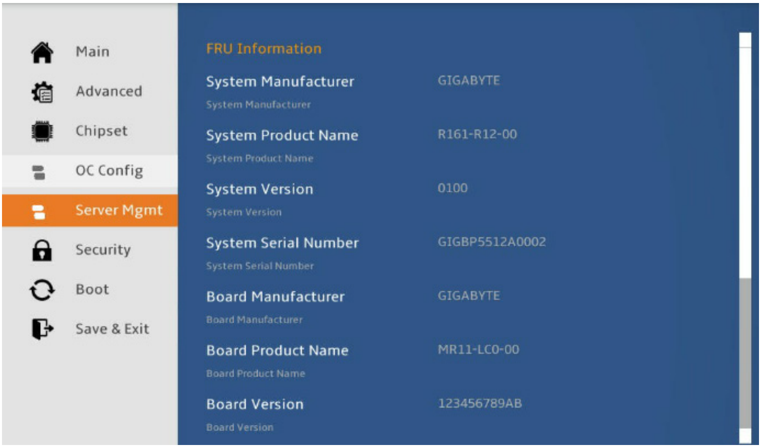
NOTE: All values changed here do not take effect

until computer is restarted.

Parameter	Description
Enabling / Disabling Options	
SEL Components	Change this item to enable or disable all features of System Event Logging during boot. Options available: Enabled/Disabled. Default setting is **Enabled**.
Erasing Settings	
Erase SEL	Choose options for erasing SEL. Options available: No/Yes, On next reset/Yes, On every reset. Default setting is **No**.
When SEL is Full	Choose options for reactions to a full SEL. Options available: Do Nothing, Erase Immediately, Delete Oldest Record. Default setting is **Do Nothing**.
Custom EFI Logging Options	
Log EFI Status Codes	Enable/Disable the logging of EFI Status Codes (if not already converted to legacy). Options available: Disabled, Both, Error code, Progress code. Default setting is **Error code**.

5-5-2 View FRU Information

The FRU page is a simple display page for basic system ID information, as well as System product information. Items on this window are non-configurable.



FRU Information

System Manufacturer GIGABYTE
System Manufacturer

System Product Name R161-R12-00
System Product Name

System Version 0100
System Version

System Serial Number GIGBP5512A0002
System Serial Number

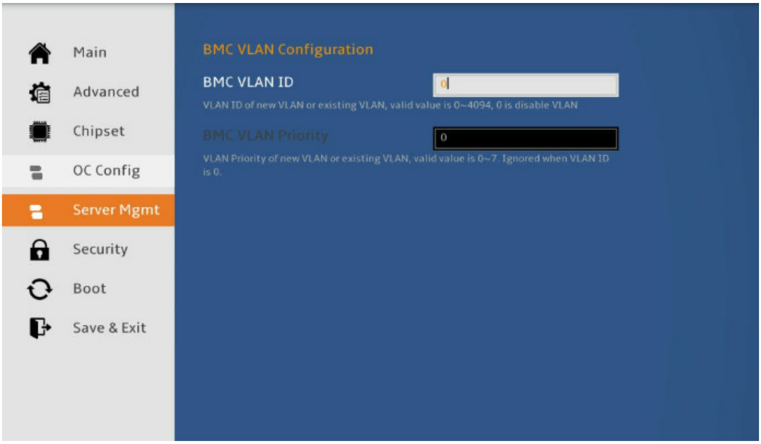
Board Manufacturer GIGABYTE
Board Manufacturer

Board Product Name MR11-LC0-00
Board Product Name

Board Version 123456789AB
Board Version

(Note) The model name will vary depends on the product you purchased

5-5-3 BMC VLAN Configuration



BMC VLAN Configuration

BMC VLAN ID: 0

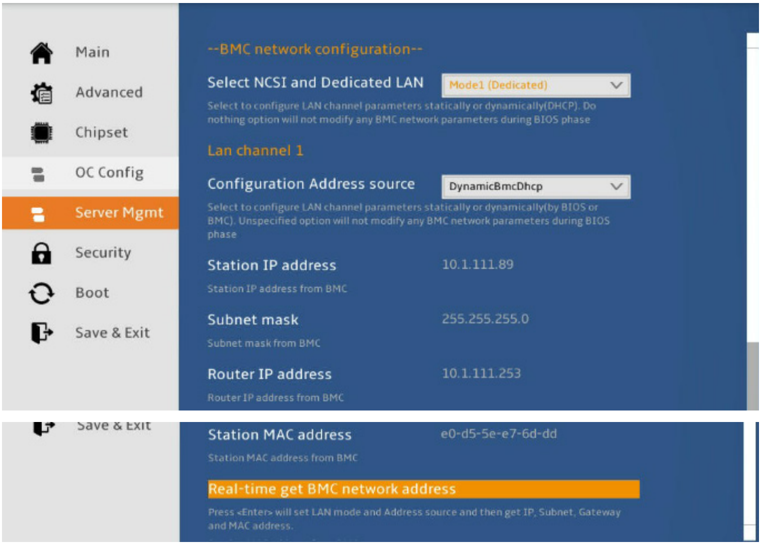
VLAN ID of new VLAN or existing VLAN, valid value is 0~4094, 0 is disable VLAN

BMC VLAN Priority: 0

VLAN Priority of new VLAN or existing VLAN, valid value is 0~7. Ignored when VLAN ID is 0.

Parameter	Description
BMC VLAN Configuration	
BMC VLAN ID	Select to configure BMC VLAN ID. The valid range is from 0 to 4094. When set to 0, BMC VLAN ID will be disabled.
BMC VLAN Priority	Select to configure BMC VLAN Priority. The valid range is from 0 to 7. When BMC VLAN ID is set to 0, BMC VLAN Priority will not be selected.

5-5-4 BMC Network Configuration



--BMC network configuration--

Select NCSI and Dedicated LAN: Mode1 (Dedicated)

Select to configure LAN channel parameters statically or dynamically(DHCP). Do nothing option will not modify any BMC network parameters during BIOS phase

Lan channel 1

Configuration Address source: DynamicBmcDhcp

Select to configure LAN channel parameters statically or dynamically(by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase

Station IP address: 10.1.111.89

Station IP address from BMC

Subnet mask: 255.255.255.0

Subnet mask from BMC

Router IP address: 10.1.111.253

Router IP address from BMC

Station MAC address: e0-d5-5e-e7-6d-dd

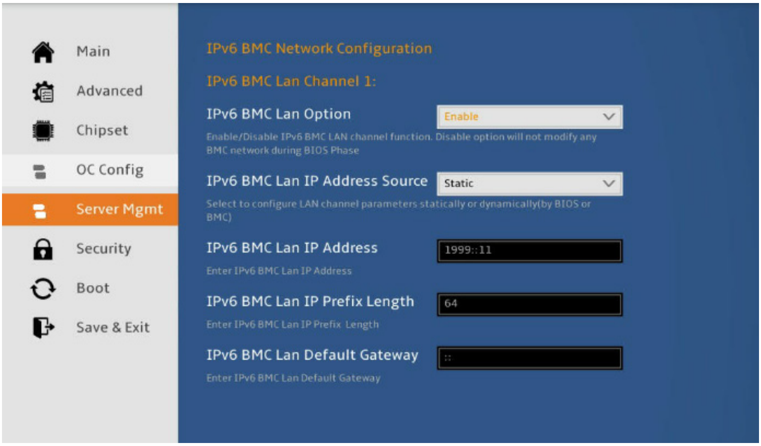
Station MAC address from BMC

Real-time get BMC network address

Press <Enter> will set LAN mode and Address source and then get IP, Subnet, Gateway and MAC address.

Parameter	Description
BMC network configuration	
Select NCSI and Dedicated LAN	Switch NCSI and dedicated LAN and send KCS command. Options available: Do Nothing, Mode1 (Dedicated), Mode2(NSCI), Mode3 (Failover). Default setting is **Mode1 (Dedicated)**.
Lan Channel 1	
Configuration Address source	Select to configure LAN channel parameters statically or dynamically (DHCP). Do nothing option will not modify any BMC network parameters during BIOS phase. Options available: Unspecified, Static, DynamicBmcDhcp. Default setting is **DynamicBmcDhcp**.
Station IP address	Displays IP Address information.
Subnet mask	Displays Subnet Mask information. Please note that the IP address must be in three digitals, for example, 192.168.000.001.
Router IP address	Displays the Router IP Address information.
Station MAC address	Displays the MAC Address information.
Real-time get BMC network address	Press [Enter] will set LAN mode and Address source and then get IP, Subnet, Gateway and MAC address.

5-5-5 IPv6 BMC Network Configuration



IPv6 BMC Network Configuration

IPv6 BMC Lan Channel 1:

IPv6 BMC Lan Option: Enable

Enable/Disable IPv6 BMC LAN channel function. Disable option will not modify any BMC network during BIOS Phase

IPv6 BMC Lan IP Address Source: Static

Select to configure LAN channel parameters statically or dynamically(by BIOS or BMC)

IPv6 BMC Lan IP Address: 1999::11

Enter IPv6 BMC Lan IP Address

IPv6 BMC Lan IP Prefix Length: 64

Enter IPv6 BMC Lan IP Prefix Length

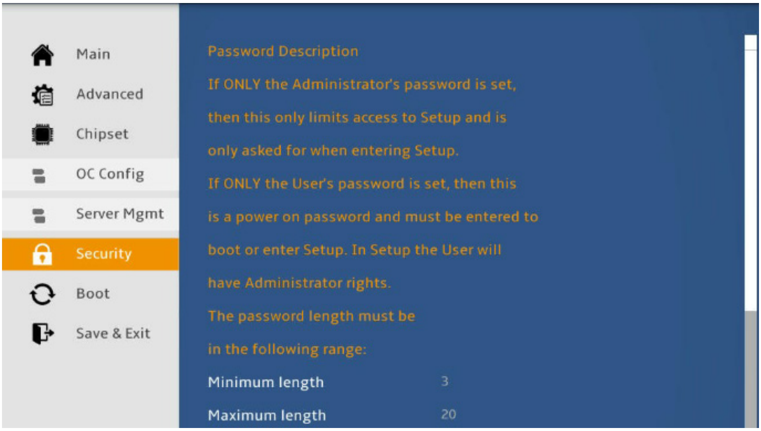
IPv6 BMC Lan Default Gateway: ::

Enter IPv6 BMC Lan Default Gateway

Parameter	Description
IPv6 BMC Network Configuration	
IPv6 BMC Lan Channel 1	
IPv6 BMC Lan Option	Enable/Disable IPv6 BMC LAN channel function. When this item is disabled, the system will not modify any BMC network during BIOS phase. Options available: Unspecified, Enable, Disable. Default setting is **Enable**.
IPv6 BMC Lan IP Address Source	Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Options available: Unspecified, Static, Dynamic-Obtained by BMC running DHCP. Default setting is **Dynamic-Obtained by BMC running DHCP**.
IPv6 BMC Lan IP Address	Configures IPv6 BMC Lan IP Address.
IPv6 BMC Lan IP Prefix Length	Configures IPv6 BMC Lan IP Prefix Length.
IPv6 BMC Lan Default Gateway	Configures IPv6 BMC Lan Default Gateway

5-6 Security Menu

The Security menu allows you to safeguard and protect the system from unauthorized use by setting up access passwords.



Password Description

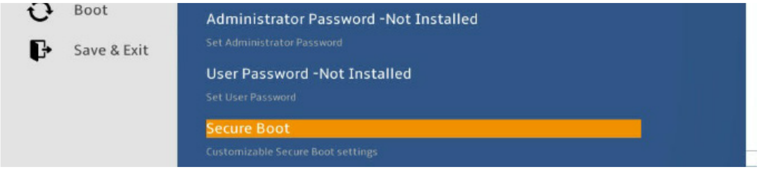
If ONLY the Administrator's password is set, then this only limits access to Setup and is only asked for when entering Setup.

If ONLY the User's password is set, then this is a power on password and must be entered to boot or enter Setup. In Setup the User will have Administrator rights.

The password length must be in the following range:

Minimum length 3

Maximum length 20



Administrator Password -Not Installed

Set Administrator Password

User Password -Not Installed

Set User Password

Secure Boot

Customizable Secure Boot settings

There are two types of passwords that you can set:

- Administrator Password

  Entering this password will allow the user to access and change all settings in the Setup Utility.

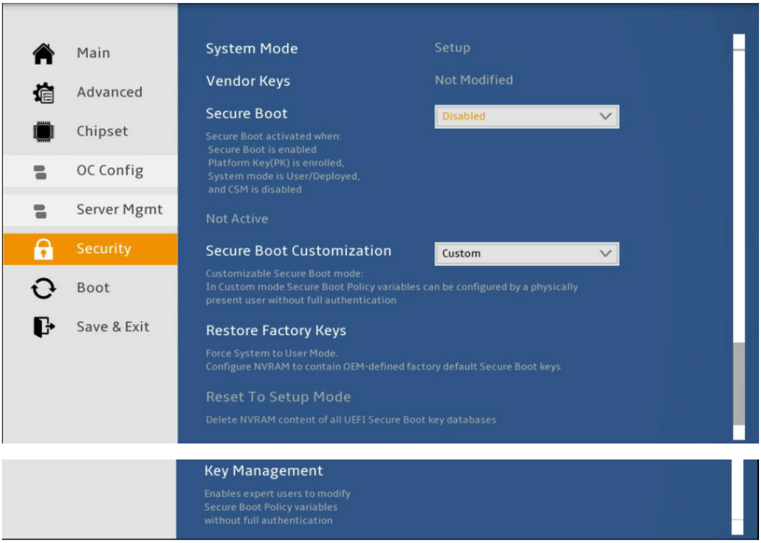
- User Password

  Entering this password will restrict a user's access to the Setup menus. To enable or disable this field, a Administrator Password must first be set. A user can only access and modify the System Time, System Date, and Set User Password fields.

Parameter	Description
Administrator Password	Press [Enter] to configure the administrator password.
User Password	Press [Enter] to configure the user password.
Secure Boot	Press [Enter] to configure advanced items.

5-6-1 Secure Boot

The Secure Boot submenu is applicable when your device is installed the Windows® 8 (or above) operating system.



System Mode — Setup

Vendor Keys — Not Modified

Secure Boot — Disabled

Secure Boot activated when:
Secure Boot is enabled
Platform Key(PK) is enrolled,
System mode is User/Deployed,
and CSM is disabled

Not Active

Secure Boot Customization — Custom

Customizable Secure Boot mode:
In Custom mode Secure Boot Policy variables can be configured by a physically present user without full authentication

Restore Factory Keys

Force System to User Mode.
Configure NVRAM to contain OEM-defined factory default Secure Boot keys

Reset To Setup Mode

Delete NVRAM content of all UEFI Secure Boot key databases

Key Management

Enables expert users to modify
Secure Boot Policy variables
without full authentication

Parameter	Description
System Mode	Displays the system is in User mode or Setup mode.
Vendor Keys	Displays the Vendor Keys function is active or not active.
Secure Boot	Secure Boot activated when Platform Key (PK) is enrolled, System mode is User/Deployed, and CSM function is disabled. Options available: Enabled/Disabled. Default setting is **Disabled**.
Secure Boot Customization(Note)	Secure Boot requires all the applications that are running during the booting process to be pre-signed with valid digital certificates. This way, the system knows all the files being loaded before Windows loads and gets to the login screen have not been tampered with. When set to Standard, it will automatically load the Secure Boot keys form the BIOS databases. When set to Custom, you can customize the Secure Boot settings and manually load its keys from the BIOS database. Options available: Standard/Custom. Default setting is Custom.
Restore Factory Keys	Forces the system to user mode and installs factury default Secure Boot key database.
Reset To Setup Mode	Delete NVRAM content of all UEFI Secure Boot key databases.

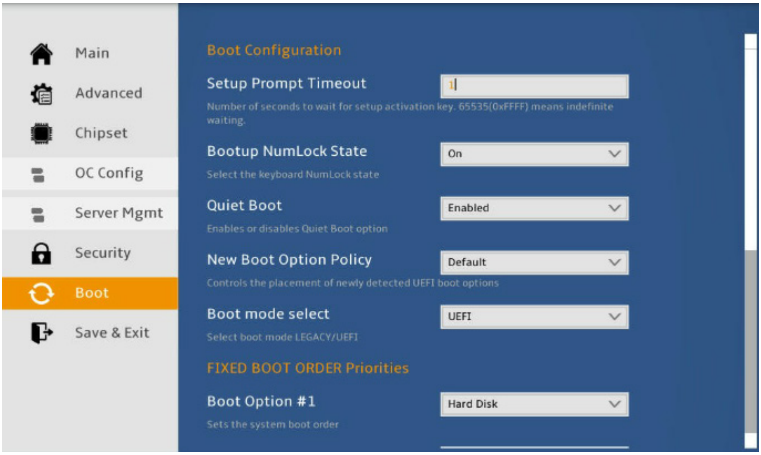
(Note) Advanced items prompt when this item is set to **Custom**.

Parameter	Description
Key Management	Press [Enter] to configure advanced items. **Please note that this item is configurable when Secure Boot Mode is set to Custom.** ◆ Factory Key Provision – Allows to provision factory default Secure Boot keys when system is in Setup Mode. – Options available: Enabled/Disabled. Default setting is **Disabled**. ◆ Restore Factory Keys – Installs all factory default keys. It will force the system in User Mode. – Options available: Yes/No. ◆ Reset To Setup Mode – Delete NVRAM content of all UEFI Secure Boot key databases. ◆ Export Secure Boot variables – Copy NVRAM content of Secure Boot variables to files in a root folder on a file system device. ◆ Enroll Efi Image – Press [Enter] to enroll SHA256 hash of the binary into Authorized Signature Database (db). ◆ Device Guard Ready ◆ Remove 'UEFI CA' from DB – Remove 'Microsoft UEFI CA' certificate from Authorized Signature datatbase. ◆ Restore DB defaults – Restore the DB variable to factory defaults. ◆ Secure Boot variable ◆ Platform Key (PK) – Displays the current status of the Platform Key (PK). – Press [Enter] to configure a new PK. – Options available: Set New. ◆ Key Exchange Keys (KEK) – Displays the current status of the Key Exchange Key Database (KEK). – Press [Enter] to configure a new KEK or load additional KEK from storage devices. – Options available: Set New/Append. ◆ Authorized Signatures (DB) – Displays the current status of the Authorized Signature Database. – Press [Enter] to configure a new DB or load additional DB from storage devices. – Options available: Set New/Append. ◆ Forbidden Signatures (DBX) – Displays the current status of the Forbidden Signature Database. – Press [Enter] to configure a new dbx or load additional dbx from storage devices. – Options available: Set New/Append.

Parameter	Description
Key Management (continued)	◆ Authorized TimeStamps (DBT) – Displays the current status of the Authorized TimeStamps Database. – Press [Enter] to configure a new DBT or load additional DBT from storage devices. – Options available: Set New/Append. ◆ OsRecovery Signatures – Displays the current status of the OsRecovery Signature Database. – Press [Enter] to configure a new OsRecovery Signature or load additional OsRecovery Signature from storage devices. – Options available: Set New/Append.

5-7 Boot Menu

The Boot menu allows you to set the drive priority during system boot-up. BIOS setup will display an error message if the legacy drive(s) specified is not bootable.



Boot Configuration

Setup Prompt Timeout: 1
Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.

Bootup NumLock State: On
Select the keyboard NumLock state

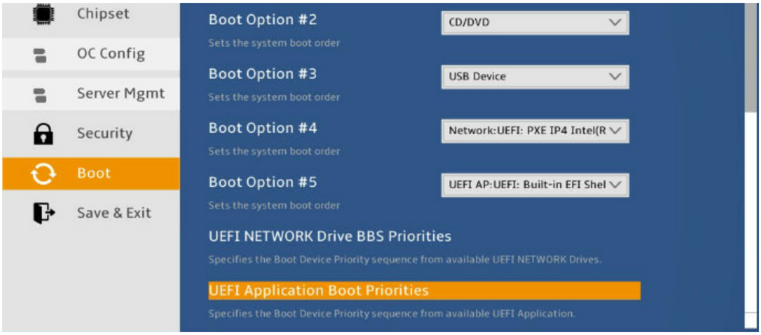
Quiet Boot: Enabled
Enables or disables Quiet Boot option

New Boot Option Policy: Default
Controls the placement of newly detected UEFI boot options

Boot mode select: UEFI
Select boot mode LEGACY/UEFI

FIXED BOOT ORDER Priorities

Boot Option #1: Hard Disk
Sets the system boot order



Boot Option #2: CD/DVD
Sets the system boot order

Boot Option #3: USB Device
Sets the system boot order

Boot Option #4: Network:UEFI: PXE IP4 Intel(R
Sets the system boot order

Boot Option #5: UEFI AP:UEFI: Built-in EFI Shel
Sets the system boot order

UEFI NETWORK Drive BBS Priorities
Specifies the Boot Device Priority sequence from available UEFI NETWORK Drives.

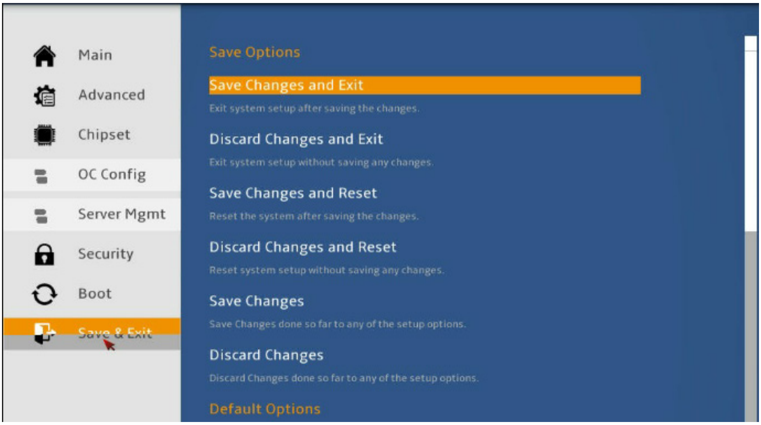
UEFI Application Boot Priorities
Specifies the Boot Device Priority sequence from available UEFI Application.

Parameter	Description
Boot Configuration	
Setup Prompt Timeout	Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting. Press the numeric keys to input the desired values.
Bootup NumLock State	Enable/Disable the Bootup NumLock function. Options available: On/Off. Default setting is **On**.
Quiet Boot	Enable/Disable showing the logo during POST. Options available: Enabled/Disabled. Default setting is **Enabled**.
New Boot Option Policy	Controls the placement of newly detected UEFI boot options. Options available: Default, Place First, Place Last. Default setting is **Default**.

Parameter	Description
Boot mode select	Selects the boot mode. Options available: LEGACY/UEFI. Default setting is **UEFI**.
FIXED BOOT ORDER Priorities	
Boot Option #1 / #2 / #3 / #4 / #5	Press [Enter] to configure the boot priority. By default, the server searches for boot devices in the following sequence: 1. Hard drive. 2. CD-COM/DVD drive. 3. USB device. 4. Network. 5. UEFI.
UEFI Network Drive BBS Priorities	Press [Enter] to configure the boot device priority sequence from available UEFI network drives.
UEFI Application Boot Priorities	Press [Enter] to configure the boot device priority sequence from available UEFI application.

5-8 Save & Exit Menu

The Save & Exit menu displays the various options to quit from the BIOS setup. Highlight any of the exit options then press <Enter>.



Save Options

Save Changes and Exit

Exit system setup after saving the changes.

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.

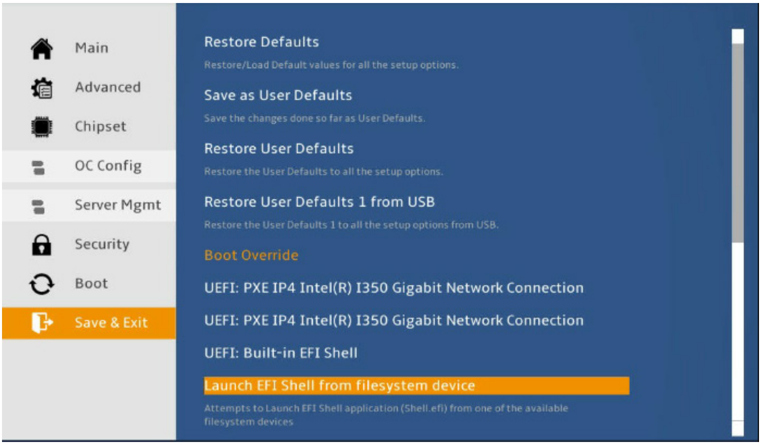
Save Changes

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

Discard Changes

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

Default Options



Restore Defaults

Restore/Load Default values for all the setup options.

Save as User Defaults

Save the changes done so far as User Defaults.

Restore User Defaults

Restore the User Defaults to all the setup options.

Restore User Defaults 1 from USB

Restore the User Defaults 1 to all the setup options from USB.

Boot Override

UEFI: PXE IP4 Intel(R) I350 Gigabit Network Connection

UEFI: PXE IP4 Intel(R) I350 Gigabit Network Connection

UEFI: Built-in EFI Shell

Launch EFI Shell from filesystem device

Attempts to Launch EFI Shell application (Shell.efi) from one of the available filesystem devices

Parameter	Description
Save Options	
Save Changes and Exit	Saves changes made and closes the BIOS setup. Options available: Yes/No.
Discard Changes and Exit	Discards changes made and exits the BIOS setup. Options available: Yes/No.
Save Changes and Reset	Restarts the system after saving the changes made. Options available: Yes/No.

Parameter	Description
Discard Changes and Reset	Restarts the system without saving any changes. Options available: Yes/No.
Save Changes	Saves changes made in the BIOS setup. Options available: Yes/No.
Discard Changes	Discards changes made and closes the BIOS setup. Options available: Yes/No.
Default Options	
Restore Defaults	Loads the default settings for all BIOS setup parameters. Setup Defaults are quite demanding in terms of resources consumption. If you are using low-speed memory chips or other kinds of low-performance components and you choose to load these settings, the system might not function properly. Options available: Yes/No.
Save as User Defaults	Saves the changes made as the user default settings. Options available: Yes/No.
Restore User Defaults	Loads the user default settings for all BIOS setup parameters. Options available: Yes/No.
Restore User Defaults 1 from USB	Restore the user defaults 1 to all the setup options from USB.
Boot Override	Press [Enter] to configure the device as the boot-up drive.

5-9 BIOS POST Codes

5-9-1 AMI Standard - PEI

PEI_CORE_STARTED	0x10
PEI_CAR_CPU_INIT	0x11
PEI_CAR_NB_INIT	0x15
PEI_CAR_SB_INIT	0x19
PEI_MEMORY_SPD_READ	0x2B
PEI_MEMORY_PRESENCE_DETECT	0x2C
PEI_MEMORY_TIMING	0x2D
PEI_MEMORY_CONFIGURING	0x2E
PEI_MEMORY_INIT	0x2F
PEI_MEMORY_INSTALLED	0x31
PEI_CPU_INIT	0x32
PEI_CPU_CACHE_INIT	0x33
PEI_CPU_AP_INIT	0x34
PEI_CPU_BSP_SELECT	0x35
PEI_CPU_SMM_INIT	0x36
PEI_MEM_NB_INIT	0x37
PEI_MEM_SB_INIT	0x3B
PEI_DXE_IPL_STARTED	0x4F
DXE_CORE_STARTED	0x60
//Recovery	
PEI_RECOVERY_AUTO	0xF0
PEI_RECOVERY_USER	0xF1
PEI_RECOVERY_STARTED	0xF2
PEI_RECOVERY_CAPSULE_FOUND	0xF3
PEI_RECOVERY_CAPSULE_LOADED	0xF4
//S3	
PEI_S3_STARTED	0xE0
PEI_S3_BOOT_SCRIPT	0xE1
PEI_S3_VIDEO_REPOST	0xE2
PEI_S3_OS_WAKE	0xE3
DXE_CORE_STARTED	0x60
DXE_NVRAM_INIT	0x61
DXE_SBRUN_INIT	0x62

5-9-2 AMI Standard - DXE

DXE_CPU_INIT	0x63
DXE_NB_HB_INIT	0x68
DXE_NB_INIT	0x69
DXE_NB_SMM_INIT	0x6A
DXE_SB_INIT	0x70
DXE_SB_SMM_INIT	0x71
DXE_SB_DEVICES_INIT	0x72

DXE_ACPI_INIT	0x78
DXE_CSM_INIT	0x79
DXE_BDS_STARTED	0x90
DXE_BDS_CONNECT_DRIVERS	0x91
DXE_PCI_BUS_BEGIN	0x92
DXE_PCI_BUS_HPC_INIT	0x93
DXE_PCI_BUS_ENUM	0x94
DXE_PCI_BUS_REQUEST_RESOURCES	0x95
DXE_PCI_BUS_ASSIGN_RESOURCES	0x96
DXE_CON_OUT_CONNECT	0x97
DXE_CON_IN_CONNECT	0x98
DXE_SIO_INIT	0x99
DXE_USB_BEGIN	0x9A
DXE_USB_RESET	0x9B
DXE_USB_DETECT	0x9C
DXE_USB_ENABLE	0x9D
DXE_IDE_BEGIN	0xA0
DXE_IDE_RESET	0xA1
DXE_IDE_DETECT	0xA2
DXE_IDE_ENABLE	0xA3
DXE_SCSI_BEGIN	0xA4
DXE_SCSI_RESET	0xA5
DXE_SCSI_DETECT	0xA6
DXE_SCSI_ENABLE	0xA7
DXE_SETUP_VERIFYING_PASSWORD	0xA8
DXE_SETUP_START	0xA9
DXE_SETUP_INPUT_WAIT	0xAB
DXE_READY_TO_BOOT	0xAD
DXE_LEGACY_BOOT	0xAE
DXE_EXIT_BOOT_SERVICES	0xAF
RT_SET_VIRTUAL_ADDRESS_MAP_BEGIN	0xB0
RT_SET_VIRTUAL_ADDRESS_MAP_END	0xB1
DXE_LEGACY_OPROM_INIT	0xB2
DXE_RESET_SYSTEM	0xB3
DXE_USB_HOTPLUG	0xB4
DXE_PCI_BUS_HOTPLUG	0xB5
DXE_NVRAM_CLEANUP	0xB6
DXE_CONFIGURATION_RESET	0xB7

5-9-3 AMI Standard - ERROR

PEI_MEMORY_INVALID_TYPE	0x50
PEI_MEMORY_INVALID_SPEED	0x50
PEI_MEMORY_SPD_FAIL	0x51
PEI_MEMORY_INVALID_SIZE	0x52
PEI_MEMORY_MISMATCH	0x52
PEI_MEMORY_NOT_DETECTED	0x53
PEI_MEMORY_NONE_USEFUL	0x53
PEI_MEMORY_ERROR	0x54
PEI_MEMORY_NOT_INSTALLED	0x55
PEI_CPU_INVALID_TYPE	0x56
PEI_CPU_INVALID_SPEED	0x56
PEI_CPU_MISMATCH	0x57
PEI_CPU_SELF_TEST_FAILED	0x58
PEI_CPU_CACHE_ERROR	0x58
PEI_CPU_MICROCODE_UPDATE_FAILED	0x59
PEI_CPU_NO_MICROCODE	0x59
PEI_CPU_INTERNAL_ERROR	0x5A
PEI_CPU_ERROR	0x5A
PEI_RESET_NOT_AVAILABLE	0x5B
//Recovery	
PEI_RECOVERY_PPI_NOT_FOUND	0xF8
PEI_RECOVERY_NO_CAPSULE	0xF9
PEI_RECOVERY_INVALID_CAPSULE	0xFA
//S3 Resume	
PEI_MEMORY_S3_RESUME_FAILED	0xE8
PEI_S3_RESUME_PPI_NOT_FOUND	0xE9
PEI_S3_BOOT_SCRIPT_ERROR	0xEA
PEI_S3_OS_WAKE_ERROR	0xEB
DXE_CPU_ERROR	0xD0
DXE_NB_ERROR	0xD1
DXE_SB_ERROR	0xD2
DXE_ARCH_PROTOCOL_NOT_AVAILABLE	0xD3
DXE_PCI_BUS_OUT_OF_RESOURCES	0xD4
DXE_LEGACY_OPROM_NO_SPACE	0xD5
DXE_NO_CON_OUT	0xD6
DXE_NO_CON_IN	0xD7
DXE_INVALID_PASSWORD	0xD8
DXE_BOOT_OPTION_LOAD_ERROR	0xD9
DXE_BOOT_OPTION_FAILED	0xDA
DXE_FLASH_UPDATE_FAILED	0xDB
DXE_RESET_NOT_AVAILABLE	0xDC

5-9-4 Intel UPI POST Codes

Initialize KTIRC inuput structure default values	0xA0
Collect info such as SBSP, Boot Mode, Reset type etc	0xA1
Setup IO SADs in SBSP to access the config space	0xA2
Setup up minimum path between SBSP & other sockets Add the node to the tree Parse the LEP of the discovered socket Check if the system has the supported topology Setup the boot path for the parent which is not directly connected to Legacy CPU Setup path from SBSP to the new found node	0xA3
Setup IO SADs in PBSP to access the config space	0xA4
System configurations that require some kind of reset	0xA5
Sync up with PBSPs	0xA6
Topology discovery and route calculation	0xA7
Program final route	0xA8
Program final IO SAD setting	0xA9
Protocol layer and other Uncore settings	0xAA
Transition links to full speed operation	0xAB
Phy layer settings	0xAC
Link layer settings	0xAD
Coherency Settings	0xAE
KTIRC is done	0xAF

5-9-5 Intel UPI Error Codes

When system BSP tries to setup path for remote sockets or sends a Boot_Go command to remote socket in SetupSbspPathToAllSockets() or SyncUpPbspForReset(). If the remote socket(s) hasn't checked-in, assert; it is a fatal condition, this error will be logged. No retry. *RC Behavior: System Halt*	0xD8
When SBSP tries to add this remote socket into system topology tree in SetupSbspPathToAllSockets(), there are some errors occur in the data structure. No retry. *RC Behavior: The current Socket is not added to the tree.* When SBSP setups the boot path for the parent which is not directly connected to Legacy CPU in SetupSbspPathToAllSockets(). The Child is not an immediate neighbor of Parent. No retry.	0xDA

SAD setup error *RC Behavior: System Halt*	0xDB
Unsupported topology *RC Behavior: System Halt*	0xDC
SBSP cannot find KPIRC TXEQ Parameters for this link in GetSocketLinkEparams(). No retry. *RC Behavior: System Halt*	0xDD

5-9-6 Intel MRC POST Codes

Detect DIMM population	0xB0
Set DDR frequency	0xB1
Gather remaining SPD data	0xB2
Program registers on the memory controller level	0xB3
Evaluate RAS modes and save rank information	0xB4
Program registers on the channel level	0xB5
DDRIO Initialization	0xB6
Train DDR	0xB7
Initialize CLTT/OLTT	0xB8
Hardware memory test and init	0xB9
Execute memory init	0xBA
Program memory map and interleaving	0xBB
Program RAS configuration	0xBC
Rank margin tool	0xBD
MRC is done	0xBF

5-9-7 Intel MRC Error Codes

No memory was detected	0xE8
Memory test failure	0xEB
Different dimm types are detected installed in the system	0xED
Number of HAs found in system greater than MAX_HA defined in MRC build	0xEE
Indicates a CLTT table structure error	0xEF
Invalid VR mode, unable to set DRAM VDD	0xF0
Failure occurred reserving memory for IOT	0xF1
Reference code assert	0xF2
Unsupported MC frequency set	0xF3
Unable to get current MC frequency	0xF4

5-9-8 Intel PM POST Codes

Start of PPM structure initialization	0xD0
PPM CSR programming	0xD1
PPM MSR programming	0xD2
Start of PState transition init	0xD3
PPM exit	0xD4
PPM On ready to boot event	0xD5

5-9-9 Intel PM POST Codes

Start of IIO early Initialization	0xE0
Pre Link training	0xE1
Start of Gen3 EQ training	0xE2
Start of PState transition init	0xE3
Gen3 parameters override	0xE4
End of IIO Early Initialization	0xE5
Start of IIO Late initialization	0xE6
PCIE port initialization	0xE7
IOAPIC initialization	0xE8
VTD initialization	0xE9
IOAT initialization	0xEA
DFX initialization	0xEB
NTB initialization	0xEC
Security Initialization	0xED
IIO late initialization	0xEE
IIO On ready to boot event	0xEF

5-10 BIOS POST Beep code (AMI standard)

5-10-1 PEI Beep Codes

# of Beeps	Description
1	Memory not Installed.
1	Memory was installed twice (InstallPeiMemory routine in PEI Core called twice)
2	Recovery started
3	DXEIPL was not found
3	DXE Core Firmware Volume was not found
4	Recovery failed
4	S3 Resume failed
7	Reset PPI is not available

5-10-2 DXE Beep Codes

# of Beeps	Description
1	Invalid password
4	Some of the Architectural Protocols are not available
5	No Console Output Devices are found
5	No Console Input Devices are found
6	Flash update is failed
7	Reset protocol is not available
8	Platform PCI resource requirements cannot be met