

3.5"-SBC-AML/ADN/AMH/ADH

User Guide Template Rev. 2.5

This page has been intentionally left blank

3.5"-SBC-AML/ADN/AMH/ADH – User Guide

Disclaimer

Kontron would like to point out that the information contained in this user guide may be subject to alteration, particularly as a result of the constant upgrading of Kontron products. This document does not entail any guarantee on the part of Kontron with respect to technical processes described in the user guide or any product characteristics set out in the user guide. Kontron assumes no responsibility or liability for the use of the described product(s), conveys no license or title under any patent, copyright or mask work rights to these products and makes no representations or warranties that these products are free from patent, copyright or mask work right infringement unless otherwise specified. Applications that are described in this user guide are for illustration purposes only. Kontron makes no representation or warranty that such application will be suitable for the specified use without further testing or modification. Kontron expressly informs the user that this user guide only contains a general description of processes and instructions which may not be applicable in every individual case. In cases of doubt, please contact Kontron.

This user guide is protected by copyright. All rights are reserved by Kontron. No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the express written permission of Kontron. Kontron points out that the information contained in this user guide is constantly being updated in line with the technical alterations and improvements made by Kontron to the products and thus this user guide only reflects the technical status of the products by Kontron at the time of publishing.

Brand and product names are trademarks or registered trademarks of their respective owners.

©2026 by Kontron Europe GmbH

Kontron Europe GmbH
Gutenbergstraße 2
85737 Ismaning
Germany
www.kontron.com

Intended Use

This device and associated software are not designed, manufactured or intended for use or resale for the operation of nuclear facilities, the navigation, control or communication systems for aircraft or other transportation, air traffic control, life support or life sustaining applications, weapons systems, or any other application in a hazardous environment, or requiring fail-safe performance, or in which the failure of products could lead directly to death, personal injury, or severe physical or environmental damage (collectively, “high risk applications”).

You understand and agree that your use of Kontron devices as a component in High Risk Applications is entirely at your risk. To minimize the risks associated with your products and applications, you should provide adequate design and operating safeguards. You are solely responsible for compliance with all legal, regulatory, safety, and security related requirements concerning your products. You are responsible to ensure that your systems (and any Kontron hardware or software components incorporated in your systems) meet all applicable requirements. Unless otherwise stated in the product documentation, the Kontron device is not provided with error-tolerance capabilities and cannot therefore be deemed as being engineered, manufactured or setup to be compliant for implementation or for resale as device in High Risk Applications. All application and safety related information in this document (including application descriptions, suggested safety measures, suggested Kontron products, and other materials) is provided for reference only.

NOTICE

You find the most recent version of the “General Safety Instructions” online in the download area of this product.

NOTICE

This product is not intended for use or suited for storage or operation in corrosive environments, in particular under exposure to sulfur and chlorine and their compounds. For information on how to harden electronics and mechanics against these stress conditions, contact Kontron Support.

Revision History

| Revision | Brief Description of Changes | Date of Issue | Author |
|----------|---|---------------|--------|
| 1.0 | Initial Issue | 2024-Dec-25 | YS |
| 1.1 | Update CN17 mating connector | 2025-Feb-03 | YS |
| 1.2 | Add EMC compliance standards | 2025-Mar-21 | YS |
| 1.3 | Update COM1 & COM2 pin definition | 2025-May-28 | YS |
| 1.4 | Add UR / CSA compliance standards | 2025-Jun-11 | YS |
| 2.0 | Add 3.5"-SBC-AMH/ADH | 2025-Jun-26 | YS |
| 2.1 | Modify power consumption | 2025-Aug-05 | YS |
| 2.2 | Revise power consumption table | 2025-Aug-15 | YS |
| 2.3 | New user Guide template. New chapters- Technical Support, Storage and Transportation, Warranty, Disposal and Cyber security. Included the statement of memory volatility. | 2025-Nov-14 | YS/CW |
| 2.4 | Correct typo of B2B connector pin description (pin 31 & 32) | 2026-Feb-25 | YS |
| 2.5 | Simplify LAN port pin signal description | 2026-Mar-10 | YS |

Terms and Conditions

Kontron warrants products in accordance with defined regional warranty periods. For more information about warranty compliance and conformity, and the warranty period in your region, visit www.kontron.com/terms-and-conditions.

Kontron sells products worldwide and declares regional General Terms & Conditions of Sale, and Purchase Order Terms & Conditions. Visit www.kontron.com/terms-and-conditions.

For contact information, refer to the corporate offices contact information on the last page of this user guide or visit our website [CONTACT US](#).

Customer Support

Find Kontron contacts by visiting www.kontron.com/support-and-services.

Customer Service

As a trusted technology innovator and global solutions provider, Kontron extends its embedded market strengths into a services portfolio allowing companies to break the barriers of traditional product lifecycles. Proven product expertise coupled with collaborative and highly-experienced support enables Kontron to provide exceptional peace of mind to build and maintain successful products.

For more details on Kontron's service offerings such as: enhanced repair services, extended warranty, Kontron training academy, and more visit www.kontron.com/support-and-services.

Customer Comments

If you have any difficulties using this user guide, discover an error, or just want to provide some feedback, contact [Kontron support](#). Detail any errors you find. We will correct the errors or problems as soon as possible and post the revised user guide on our website.

Symbols

The following symbols may be used in this user guide



DANGER indicates a hazardous situation which, if not avoided, will result in death or serious injury.



WARNING indicates a hazardous situation which, if not avoided, could result in death or serious injury.



CAUTION indicates a hazardous situation which, if not avoided, may result in minor or moderate injury

ATTENTION indique une situation dangereuse qui, si elle n'est pas évitée, peut entraîner des blessures mineures ou modérées.



NOTICE indicates a property damage message.



Electric Shock!

This symbol and title indicate hazards due to electrical shocks (> 60 V) when touching products or parts of products. Failure to observe the precautions indicated and/or prescribed by the law may endanger your life/health and/or result in damage to your material.



ESD Sensitive Device!

This symbol and title indicate that the electronic boards and their components are sensitive to static electricity. Care must be taken during all handling operations and inspections of this product to always ensure product integrity.



Caution: HOT Surface!

This symbol and title indicate a hot surface that must not be touched until cool.

Attention : Surface CHAUDE !

Ce symbole et ce titre indiquent une surface chaude qui ne doit pas être touchée avant d'avoir refroidi.



Caution: Laser!

This symbol and title indicate the risk of exposure to laser beam and light emitting devices (LEDs) from an electrical device. Eye protection per manufacturer notice shall review before servicing.



Caution: High Sound Pressure!

This symbol and title indicate that high sound pressure is possible with headphones. There is a risk of hearing damage. Do not listen at high volume levels for long periods of time.



Security

This symbol and title indicate general information and guidelines regarding the product's cyber security to ensure secure installation, operation, maintenance and disposal of the product within the user's end environment.



This symbol indicates information about the product and the user guide.



This symbol precedes helpful hints and tips for daily use.

For Your Safety

Your new Kontron product was developed and tested carefully to provide all the features necessary to ensure its compliance with electrical safety requirements. It was also designed for a long fault-free life. However, the life expectancy of your product can be drastically reduced by improper treatment during unpacking and installation. Therefore, in the interest of your own safety and of the correct operation of your new Kontron product, you are requested to conform with the following guidelines.

High Voltage Safety Instructions

As a precaution and in case of danger, the power connector must be easily accessible. The power connector is the product's main disconnect device.

⚠ CAUTION

Warning

All operations on this product must be carried out by sufficiently skilled personnel only.

⚠ CAUTION



Electric Shock!

Before installing a non hot-swappable Kontron product into a system always ensure that your mains power is switched off. This also applies to the installation of piggybacks. Serious electrical shock hazards can exist during all installation, repair, and maintenance operations on this product. Therefore, always unplug the power cable and any other cables which provide external voltages before performing any work on this product.

Earth ground connection to vehicle's chassis or a central grounding point shall remain connected. The earth ground cable shall be the last cable to be disconnected or the first cable to be connected when performing installation or removal procedures on this product.

Special Handling and Unpacking Instruction

NOTICE



ESD Sensitive Device!

Electronic boards and their components are sensitive to static electricity. Therefore, care must be taken during all handling operations and inspections of this product, in order to ensure product integrity at all times.

⚠ CAUTION

Handling and operation of the product is permitted only for skilled personnel within a workplace that is access controlled. Follow the "General Safety Instructions" supplied with the product.

Do not handle this product out of the product's protective enclosure while the product is not used for operational purposes unless the product is otherwise protected.

Whenever possible, unpack or pack this product only at an EOS/ESD safe workplace. Where a safe workplace is not guaranteed, it is important for the user to be electrically discharged before touching the product with his/her hands or tools. This is most easily done by touching a metal part of your system housing.

It is particularly important to observe standard anti-static precautions when changing piggybacks, ROM devices, jumper settings etc. If the product contains batteries for RTC or memory backup, ensure that the product is not placed on conductive surfaces, including anti-static plastics or sponges. They can cause short circuits and damage the batteries or conductive circuits on the product.

Lithium Battery Precautions

If your product is equipped with a lithium battery, take the following precautions when replacing the lithium battery.

⚠ CAUTION

Risk of Explosion if the lithium Battery is replaced by an incorrect Type. Dispose of used lithium batteries according to the instructions.

Risque d'explosion si la pile au lithium est remplacée par une pile de type incorrect.

Éliminez les piles au lithium usagées conformément aux instructions.

General Instructions on Usage

In order to maintain Kontron's product warranty, this product must not be altered or modified in any way. Changes or modifications to the product, that are not explicitly approved by Kontron and described in this user guide or received from Kontron Support as a special handling instruction, will void your warranty.

This product should only be installed in or connected to systems that fulfill all necessary technical and specific environmental requirements. This also applies to the operational temperature range of the specific board version that must not be exceeded. If batteries are present, their temperature restrictions must be considered.

In performing all necessary installation and application operations, only follow the instructions supplied by the present user guide.

Keep all the original packaging material for future storage or warranty shipments. If it is necessary to store or ship the product then re-pack the product as delivered.

Special care is necessary when handling or unpacking the product. See Special Handling and Unpacking Instruction.

Quality and Environmental Management

Kontron aims to deliver reliable high-end products designed and built for quality, and aims to comply with environmental laws, regulations, and other environmentally oriented requirements. For more information regarding Kontron's quality and environmental responsibilities, visit [Quality | Kontron](#) and [Material Compliance | Kontron](#).

Table of Contents

| | |
|--|----|
| Revision History..... | 5 |
| Symbols | 6 |
| For Your Safety..... | 8 |
| High Voltage Safety Instructions | 8 |
| Special Handling and Unpacking Instruction | 8 |
| Lithium Battery Precautions | 9 |
| General Instructions on Usage | 9 |
| Quality and Environmental Management | 9 |
| Table of Contents | 10 |
| List of Tables..... | 12 |
| List of Figures | 13 |
| 1/ Introduction..... | 18 |
| 2/ Installation Procedures..... | 19 |
| 2.1. Chassis Safety Standards | 20 |
| 2.2. Lithium Battery Replacement..... | 20 |
| 3/ System Specification..... | 21 |
| 3.1. System Block Diagram | 21 |
| 3.2. Component Main Data | 23 |
| 3.3. Environmental Conditions | 25 |
| 3.4. Compliance | 25 |
| 3.5. Processor Support | 26 |
| 3.6. System Memory Support..... | 26 |
| 3.7. Memory Operating Frequencies | 27 |
| 3.8. On-board Graphics Subsystem | 27 |
| 3.9. Power Input Voltage..... | 28 |
| 3.10. Power Consumption | 28 |
| 4/ Connector Locations..... | 30 |
| 4.1. Top Side | 30 |
| 4.2. Rear Side..... | 32 |
| 4.3. Connector Panel Side | 33 |
| 5/ Connector Definitions | 34 |
| 6/ I/O-Area Connectors | 35 |
| 6.1. Ethernet Connectors (CN15 & CN16) | 35 |
| 6.2. HDMI Connector (CN20)..... | 36 |
| 6.3. DP Connector (CN20 & CN21) | 37 |
| 6.4. DP over USB Type C Connector (CN22) | 38 |
| 6.5. USB Connectors (I/O Area) | 39 |
| 6.6. Power Button (SW1)..... | 40 |
| 6.7. LED Indicators (LED2 & LED3)..... | 40 |
| 7/ Internal Connectors..... | 41 |
| 7.1. Power Connector..... | 41 |
| 7.1.1. Power Input Wafer (CN9) | 41 |
| 7.1.2. RTC Power Input Wafer (CN14) | 42 |
| 7.2. Fan Wafer (CN5) | 42 |
| 7.3. SATA (Serial ATA) Connector (CN10) | 43 |
| 7.4. SATA Power Output Wafer (CN8)..... | 44 |
| 7.5. USB Connectors (Internal) (CN17) | 45 |
| 7.6. Audio AMP Output Wafer (CN1 & CN6) | 45 |
| 7.7. Audio Input / Output Header (CN7) | 46 |
| 7.8. S/PDIF Output Wafer (CN2)..... | 47 |
| 7.9. Front Panel Header (FP1 & FP2) | 47 |
| 7.10. Serial COM1, COM2, COM3 & COM4 Ports (CN25, CN24, CN28 & CN29) | 49 |
| 7.11. LVDS / eDP Combo Connector (CN26)..... | 51 |
| 7.12. LVDS / eDP Backlight Power Wafer (CN23) | 52 |
| 7.13. LVDS / eDP Backlight Brightness Wafer (CN32)..... | 53 |

| | |
|--|-----|
| 7.14. Digital Input / Output Header (CN27) | 54 |
| 7.15. SPI 10-Pins Header (CN11) | 55 |
| 7.16. M.2 Key B 2242 / 3042 / 3052 / 2280 Slot (M2B1)..... | 56 |
| 7.17. M.2 Key E 2230 Slot (M2E1) | 59 |
| 7.18. M.2 Key M 2280 Slot (M2M1) | 62 |
| 7.19. SIM Card Wafer for M.2 Key B (CN3)..... | 65 |
| 7.20. 2.5 GbE LAN LED Header (CN30 & CN31) | 65 |
| 7.21. Board-to-board Connector (CN13) | 66 |
| 7.22. Switches and Jumpers | 70 |
| 7.22.1. LVDS / eDP Backlight Enable Selection (JP2) | 70 |
| 7.22.2. AT / ATX Power Mode Selection (JP3) | 71 |
| 7.22.3. LVDS / eDP Backlight & Panel Power Selection (JP4) | 71 |
| 7.22.4. Onboard DC-DC 12 V Selection (JP5) | 72 |
| 7.22.5. USB Power Selection (JP6)..... | 72 |
| 7.22.6. Flash Descriptor Security Override Selection (JP7)..... | 73 |
| 7.22.7. Clear CMOS Selection (JP8)..... | 73 |
| 8/ BIOS | 74 |
| 8.1. Starting the uEFI BIOS..... | 74 |
| 8.2. Starting the uEFI BIOS..... | 75 |
| 8.2.1. Main Setup Menu | 75 |
| 8.2.2. Advanced Setup Menu | 79 |
| 8.2.3. Chipset Setup Menu | 203 |
| 8.2.4. Security Setup Menu | 276 |
| 8.2.5. Boot Setup Menu..... | 280 |
| 8.2.6. Save & Exit Setup Menu | 282 |
| 9/ Technical Support..... | 283 |
| 9.1. Returning Defective Merchandise..... | 283 |
| 10/ Storage and Transportation | 284 |
| 10.1. Storage | 284 |
| 10.2. Transportation..... | 284 |
| 11/ Warranty | 285 |
| 12/ Disposal | 286 |
| 12.1. Disposal | 286 |
| 12.2. WEEE Compliance..... | 286 |
| 12.3. Data Sanitization | 286 |
| 12.4. Statement of Memory Volatility..... | 288 |
| 13/ Cyber Security | 290 |
| 13.1. Security Defense Strategy | 290 |
| Appendix: List of Acronyms..... | 291 |

List of Tables

| | |
|--|----|
| Table 1: Component Main Data | 23 |
| Table 2: Environmental Conditions | 25 |
| Table 3: Standards and Certifications | 25 |
| Table 4: Processor Support | 26 |
| Table 5: Memory Operating Frequencies..... | 27 |
| Table 6: Triple-displays Configurations 3.5"-SBC-AML/ADN | 27 |
| Table 7: Triple-displays Configurations 3.5"-SBC-AMH/ADH | 28 |
| Table 8: Power Input Voltages | 28 |
| Table 9: Power Consumption | 28 |
| Table 10: Jumper List..... | 30 |
| Table 11: Top Side Internal Connector Pin Assignment | 31 |
| Table 12: Rear Side Internal Connector Pin Assignment..... | 32 |
| Table 13: Connector Panel Side Connector List | 33 |
| Table 14: Pin Assignment Ethernet Connectors CN15, CN16..... | 35 |
| Table 15: Pin Assignment HDMI Connector CN20..... | 36 |
| Table 16: Pin Assignment DP Connector CN20, CN21 | 37 |
| Table 17: Pin Assignment DP over USB Type C Connector CN22 | 38 |
| Table 18: Pin Assignment USB 3.2 Gen 2 Connectors CN18 - Top & Bottom..... | 39 |
| Table 19: Pin Assignment USB 2.0 Connectors CN19..... | 39 |
| Table 20: LED Indicators LED2, LED3 | 40 |
| Table 21: Pin Assignment CN9 | 41 |
| Table 22: Pin Assignment CN14 | 42 |
| Table 23: Pin Assignment CN5 | 42 |
| Table 24: Pin Assignment CN10 | 43 |
| Table 25: Pin Assignment CN8 | 44 |
| Table 26: Pin Assignment CN17 | 45 |
| Table 27: Pin Assignment CN1, CN6..... | 46 |
| Table 28: Pin Assignment CN7 | 46 |
| Table 29: Pin Assignment CN2 | 47 |
| Table 30: Pin Assignment FP1 | 47 |
| Table 31: Pin Assignment FP2 | 48 |
| Table 32: Pin Assignment COM1 CN25, COM2 CN24..... | 49 |
| Table 33: Pin Assignment COM3 CN28, COM4 CN29..... | 49 |
| Table 34: Signal Description | 50 |
| Table 35: Pin Assignment CN26 | 51 |
| Table 36: Pin Assignment CN23 | 52 |
| Table 37: Pin Assignment CN32 | 53 |
| Table 38: Pin Assignment CN27 | 54 |
| Table 39: Pin Assignment CN11 | 55 |
| Table 40: Pin Assignment M2B1..... | 56 |
| Table 41: Pin Assignment M2E1..... | 59 |
| Table 42: Pin Assignment M2M1 | 62 |
| Table 43: Pin Assignment CN3 | 65 |
| Table 44: Pin Assignment CN30, CN31..... | 65 |
| Table 45: Pin Assignment CN13 | 66 |
| Table 46: Pin Assignment JP2..... | 70 |
| Table 47: Pin Assignment JP3..... | 71 |
| Table 48: Pin Assignment JP4..... | 71 |
| Table 49: Pin Assignment JP5..... | 72 |
| Table 50: Pin Assignment JP6..... | 72 |

| | |
|---|-----|
| Table 51: Pin Assignment JP7 | 73 |
| Table 52: Pin Assignment JP8 | 73 |
| Table 53: Hotkeys Table | 74 |
| Table 54: Main Setup Menu Sub-Screens and Functions | 75 |
| Table 54: 3.5"-SBC-AML/ADN/AMH/ADH Statement of Memory Volatility | 288 |

List of Figures

| | |
|---|----|
| Figure 1: System Block Diagram 3.5"-SBC-AML/ADN | 21 |
| Figure 2: System Block Diagram 3.5"-SBC-AMH/ADH | 22 |
| Figure 3: Top Side | 30 |
| Figure 4: Rear Side | 32 |
| Figure 5: Connector Panel Side – 3.5"-SBC-AML/ADN | 33 |
| Figure 6: Connector Panel Side – 3.5"-SBC-AMH/ADH | 33 |
| Figure 7: Ethernet Connector CN15, CN16 | 35 |
| Figure 8: HDMI Connector CN20 | 36 |
| Figure 9: DP Connector CN20, CN21 | 37 |
| Figure 10: DP over USB Type C Connector CN22 | 38 |
| Figure 11: USB 3.2 Gen 2 Connectors CN18 - Top & Bottom | 39 |
| Figure 12: USB 2.0 Connectors CN19 | 39 |
| Figure 13: USB 2.0 High Speed Cable | 40 |
| Figure 14: USB 3.2 High Speed Cable | 40 |
| Figure 15: Power Input Wafer CN9 | 41 |
| Figure 16: RTC Power Input Wafer CN14 | 42 |
| Figure 17: Fan Wafer CN5 | 42 |
| Figure 18: SATA Connector CN10 | 43 |
| Figure 19: SATA Power Output Wafer CN8 | 44 |
| Figure 20: USB 2.0 Port 5, 6 Pin Header CN17 | 45 |
| Figure 21: Audio AMP Output Wafer CN1 (Left Channel), CN6 (Right Channel) | 45 |
| Figure 22: Audio Input / Output Header CN7 | 46 |
| Figure 23: S/PDIF Output Wafer CN2 | 47 |
| Figure 24: Front Panel Header 1 FP1 | 47 |
| Figure 25: Front Panel Header 2 FP2 | 48 |
| Figure 26: Serial COM CN24, CN25, CN28, CN29 | 49 |
| Figure 27: LVDS / eDP Combo Connector CN26 | 51 |
| Figure 28: LVDS / eDP Backlight Power Wafer CN23 | 52 |
| Figure 29: LVDS / eDP Backlight Brightness Wafer CN32 | 53 |
| Figure 30: Digital Input / Output Header CN27 | 54 |
| Figure 31: SPI 10-Pins Header CN11 | 55 |
| Figure 32: M.2 Key B 2242 / 3042 / 3052 / 2280 Slot M2B1 | 56 |
| Figure 33: M.2 Key E 2230 Slot M2E1 | 59 |
| Figure 34: M.2 Key M 2280 Slot M2M1 | 62 |
| Figure 35: SIM Card Wafer CN3 | 65 |
| Figure 36: 2.5 GbE LAN LED Header CN30, CN31 | 65 |
| Figure 37: Board-to-board Connector CN13 | 66 |
| Figure 38: Jumper Connector | 70 |
| Figure 39: LVDS / eDP Backlight Enable Selection JP2 | 70 |
| Figure 40: AT / ATX Power Mode Selection JP3 | 71 |
| Figure 41: LVDS / eDP Backlight & Panel Power Selection JP4 | 71 |
| Figure 42: Onboard DC-DC 12 V Selection JP5 | 72 |

| | |
|--|-----|
| Figure 43: USB Power Selection JP6..... | 72 |
| Figure 44: Flash Descriptor Security Override Selection JP7..... | 73 |
| Figure 45: Clear CMOS Selection JP8..... | 73 |
| Figure 46: BIOS Main Menu Screen System Data and Time..... | 76 |
| Figure 47: BIOS Main Menu Screen – Platform Information..... | 78 |
| Figure 48: BIOS Advanced Menu..... | 80 |
| Figure 49: BIOS Advanced Menu – RC ACPI Settings..... | 82 |
| Figure 50: BIOS Advanced Menu – RC ACPI Settings – PEP Constraints Configuration..... | 84 |
| Figure 51: BIOS Advanced Menu – Connectivity Configuration..... | 87 |
| Figure 52: BIOS Advanced Menu – Connectivity Configuration – WWAN Configuration..... | 99 |
| Figure 53: BIOS Advanced Menu - CPU Configuration..... | 100 |
| Figure 54: BIOS Advanced Menu - CPU Configuration – Efficient-core Information..... | 102 |
| Figure 55: BIOS Advanced Menu - CPU Configuration – CPU SMM Enhancement..... | 103 |
| Figure 56: BIOS Advanced Menu – Power & Performance..... | 104 |
| Figure 57: BIOS Advanced Menu – Power & Performance – CPU – Power Management Control..... | 104 |
| Figure 58: BIOS Advanced Menu – Power & Performance – CPU – Power Management Control – View/Configure Turbo Options..... | 109 |
| Figure 59: BIOS Advanced Menu – Power & Performance – CPU – Power Management Control – View/Configure Turbo Options – Turbo Ratio Limit Options..... | 110 |
| Figure 60: BIOS Advanced Menu – Power & Performance – CPU – Power Management Control – CPU VR Settings..... | 112 |
| Figure 61: BIOS Advanced Menu – Power & Performance – CPU – Power Management Control – CPU VR Settings – Acoustic Noise Settings..... | 115 |
| Figure 62: BIOS Advanced Menu – Power & Performance – CPU – Power Management Control – CPU VR Settings – Core/IA VR Settings..... | 116 |
| Figure 63: BIOS Advanced Menu – Power & Performance – CPU – Power Management Control – CPU VR Settings – GT VR Settings..... | 119 |
| Figure 64: BIOS Advanced Menu – Power & Performance – CPU – Power Management Control – CPU VR Settings – RFI Settings..... | 121 |
| Figure 65: BIOS Advanced Menu – Power & Performance – CPU – Power Management Control – Custom P-state Table..... | 122 |
| Figure 66: BIOS Advanced Menu – Power & Performance – CPU – Power Management Control – Power Limit 3 Settings..... | 123 |
| Figure 67: BIOS Advanced Menu – Power & Performance – CPU – Power Management Control – CPU Lock Configuration..... | 123 |
| Figure 68: BIOS Advanced Menu – Power & Performance – GT – Power Management Control..... | 124 |
| Figure 69: BIOS Advanced Menu - Display Configuration..... | 126 |
| Figure 70: BIOS Advanced Menu – PCH-FW Configuration..... | 127 |
| Figure 71: BIOS Advanced Menu – PCH-FW Configuration – Firmware Update Configuration..... | 128 |
| Figure 72: BIOS Advanced Menu – PCH-FW Configuration – PTT Configuration..... | 128 |
| Figure 73: BIOS Advanced Menu – PCH-FW Configuration – FIPS Configuration..... | 129 |
| Figure 74: BIOS Advanced Menu – PCH-FW Configuration – ME Debug Configuration..... | 129 |
| Figure 75: BIOS Advanced Menu – PCH-FW Configuration – Anti-Rollback SVN Configuration..... | 130 |
| Figure 76: BIOS Advanced Menu – PCH-FW Configuration – OEM Key Revocation Configuration..... | 131 |
| Figure 77: BIOS Advanced Menu – Thermal Configuration..... | 132 |
| Figure 78: BIOS Advanced Menu – Thermal Configuration – CPU Thermal Configuration..... | 132 |
| Figure 79: BIOS Advanced Menu – Thermal Configuration – Platform Thermal Configuration..... | 134 |
| Figure 80: BIOS Advanced Menu – Thermal Configuration – Intel® Dynamic Tuning Technology Configuration..... | 136 |
| Figure 81: BIOS Advanced Menu – Thermal Configuration – Intel® Dynamic Tuning Technology Configuration – OEM variable and Object..... | 137 |
| Figure 82: BIOS Advanced Menu – Platform Settings..... | 139 |
| Figure 83: BIOS Advanced Menu – Platform Settings - VTIO..... | 142 |
| Figure 84: BIOS Advanced Menu – Platform Settings – TCSS Platform Setting..... | 145 |

| | |
|---|-----|
| Figure 85: BIOS Advanced Menu – ACPI D3Cold settings | 147 |
| Figure 86: BIOS Advanced Menu – BCLK Configuration | 149 |
| Figure 87: BIOS Advanced Menu – Intel® Time Coordinated Computing | 150 |
| Figure 88: BIOS Advanced Menu – Intel® Time Coordinated Computing – Intel® TCC Authentication Menu..... | 151 |
| Figure 89: BIOS Advanced Menu – Intel® Time Coordinated Computing – CPU PCI Express Configuration..... | 152 |
| Figure 90: BIOS Advanced Menu – Intel® Time Coordinated Computing – PCH PCI Express Configuration..... | 152 |
| Figure 91: BIOS Advanced Menu – Intel® Time Coordinated Computing – PCH PCI Express Configuration – ASPM / L1 Substates / PTM | 153 |
| Figure 92: BIOS Advanced Menu – Functional Safety Configuration | 157 |
| Figure 93: BIOS Advanced Menu – Debug Settings | 159 |
| Figure 94: BIOS Advanced Menu – Debug Settings – VT-d Debug Settings | 160 |
| Figure 95: BIOS Advanced Menu – Debug Settings – Advanced Debug Settings | 160 |
| Figure 96: BIOS Advanced Menu – Debug Configuration..... | 163 |
| Figure 97: BIOS Advanced Menu - Trusted Computing..... | 165 |
| Figure 98: BIOS Advanced Menu – ACPI Settings..... | 167 |
| Figure 99: BIOS Advanced Menu – Miscellaneous | 168 |
| Figure 100: BIOS Advanced Menu – Miscellaneous – Preset DIO in BIOS..... | 169 |
| Figure 101: BIOS Advanced Menu – Miscellaneous – Control KSC firmware..... | 170 |
| Figure 102: BIOS Advanced Menu – Miscellaneous – Control KSC firmware – KSC OTP area control..... | 170 |
| Figure 103: BIOS Advanced Menu – Miscellaneous – Update KSC firmware..... | 171 |
| Figure 104: BIOS Advanced Menu – Miscellaneous – Generic eSPI Decode Ranges | 171 |
| Figure 105: BIOS Advanced Menu – Miscellaneous – Watchdog..... | 172 |
| Figure 106: BIOS Advanced Menu – SMART Settings..... | 174 |
| Figure 107: BIOS Advanced Menu – H/W Monitor | 175 |
| Figure 108: BIOS Advanced Menu – H/W Monitor – Fan #1 Trip Point Table..... | 176 |
| Figure 109: BIOS Advanced Menu – S5 RTC Wake Settings | 177 |
| Figure 110: BIOS Advanced Menu – UEFI Variables Protection | 178 |
| Figure 111: BIOS Advanced Menu – Serial Port Console Redirection | 179 |
| Figure 112: BIOS Advanced Menu – Serial Port Console Redirection – COM0/1/2/3 Console Redirection Settings | 180 |
| Figure 113: BIOS Advanced Menu – Serial Port Console Redirection – Legacy Console Redirection Settings | 181 |
| Figure 114: BIOS Advanced Menu – Serial Port Console Redirection – Console Redirection EMS Settings | 182 |
| Figure 115: BIOS Advanced Menu – AMI Graphic Output Protocol Policy..... | 183 |
| Figure 116: BIOS Advanced Menu – SIO Common Setting..... | 183 |
| Figure 117: BIOS Advanced Menu – SIO Configuration..... | 184 |
| Figure 118: BIOS Advanced Menu – SIO Configuration – [*Active*] Serial Port 0 | 184 |
| Figure 119: BIOS Advanced Menu – SIO Configuration – [*Active*] Serial Port 1 | 185 |
| Figure 120: BIOS Advanced Menu – SIO Configuration – [*Active*] Serial Port 2 | 185 |
| Figure 121: BIOS Advanced Menu – SIO Configuration – [*Active*] Serial Port 3 | 186 |
| Figure 122: BIOS Advanced Menu – PCI Subsystem Settings..... | 187 |
| Figure 123: BIOS Advanced Menu – USB Configuration | 188 |
| Figure 124: BIOS Advanced Menu – Network Stack Configuration..... | 190 |
| Figure 125: BIOS Advanced Menu – CSM Configuration..... | 191 |
| Figure 126: BIOS Advanced Menu – NVMe Configuration | 193 |
| Figure 127: BIOS Advanced Menu – SDIO Configuration | 194 |
| Figure 128: BIOS Advanced Menu – CH7513A Configurations..... | 195 |
| Figure 129: BIOS Advanced Menu – F81435 Configurations..... | 196 |
| Figure 130: BIOS Advanced Menu – Tls Auth Configuration | 198 |
| Figure 131: BIOS Advanced Menu – Tls Auth Configuration – Server CA Configuration..... | 198 |
| Figure 132: BIOS Advanced Menu – Tls Auth Configuration – Server CA Configuration – Enroll Cert..... | 199 |
| Figure 133: BIOS Advanced Menu – RAM Disk Configuration..... | 200 |
| Figure 134: BIOS Advanced Menu – RAM Disk Configuration – Create raw | 200 |
| Figure 135: BIOS Advanced Menu – Intel® Ethernet Controller I226-IT – C0:EA:C3:D1:D1:0E/0F..... | 201 |

| | |
|--|-----|
| Figure 136: BIOS Advanced Menu – Driver Health..... | 202 |
| Figure 137: BIOS Advanced Menu – Driver Health – Intel® 2.5G Ethernet Controller 0.10.06..... | 202 |
| Figure 138: BIOS Chipset Setup Menu | 203 |
| Figure 139: BIOS Chipset Setup Menu – System Agent (SA) Configuration | 204 |
| Figure 140: BIOS Chipset Setup Menu – System Agent (SA) Configuration – Memory Configuration..... | 205 |
| Figure 141: BIOS Chipset Setup Menu – System Agent (SA) Configuration – Memory Configuration – Memory Thermal Configuration | 212 |
| Figure 142: BIOS Chipset Setup Menu – System Agent (SA) Configuration – Memory Configuration – Memory Thermal Configuration – Memory Power and Thermal Throttling..... | 213 |
| Figure 143: BIOS Chipset Setup Menu – System Agent (SA) Configuration – Memory Configuration – Memory Training Algorithms..... | 214 |
| Figure 144: BIOS Chipset Setup Menu – System Agent (SA) Configuration – Graphics Configuration | 218 |
| Figure 145: BIOS Chipset Setup Menu – System Agent (SA) Configuration – Graphics Configuration – External Gfx Card Primary Display Configuration | 220 |
| Figure 146: BIOS Chipset Setup Menu – System Agent (SA) Configuration – Graphics Configuration – LCD Control..... | 220 |
| Figure 147: BIOS Chipset Setup Menu – System Agent (SA) Configuration – Graphics Configuration – Intel® Ultrabook Event Support..... | 221 |
| Figure 148: BIOS Chipset Setup Menu – System Agent (SA) Configuration – DMI/OPI Configuration | 222 |
| Figure 149: BIOS Chipset Setup Menu – System Agent (SA) Configuration – DMI/OPI Configuration – DMI Advanced Menu | 223 |
| Figure 150: BIOS Chipset Setup Menu – System Agent (SA) Configuration – TCSS setup menu..... | 224 |
| Figure 151: BIOS Chipset Setup Menu – System Agent (SA) Configuration – Display setup menu..... | 226 |
| Figure 152: BIOS Chipset Setup Menu – System Agent (SA) Configuration – PCI Express Configuration | 226 |
| Figure 153: BIOS Chipset Setup Menu – System Agent (SA) Configuration – PCI Express Configuration – PCI Express Root Port 1/2/3 | 227 |
| Figure 154: BIOS Chipset Setup Menu – System Agent (SA) Configuration – MIPI Camera Configuration..... | 231 |
| Figure 155: BIOS Chipset Setup Menu – System Agent (SA) Configuration – MIPI Camera Configuration – Control Logic options | 232 |
| Figure 156: BIOS Chipset Setup Menu – System Agent (SA) Configuration – MIPI Camera Configuration – Link options | 234 |
| Figure 157: BIOS Chipset Setup Menu – System Agent (SA) Configuration – MIPI Camera Configuration – Flash options | 237 |
| Figure 158: BIOS Chipset Setup Menu – PCH-IO Configuration | 238 |
| Figure 159: BIOS Chipset Setup Menu – PCH-IO Configuration – PCI Express Configuration | 242 |
| Figure 160: BIOS Chipset Setup Menu – PCH-IO Configuration – PCI Express Configuration – PCIe EQ settings | 243 |
| Figure 161: BIOS Chipset Setup Menu – PCH-IO Configuration – PCI Express Configuration – PCI Express Root Port 3 / 4 / 7 / 9 / 10 | 245 |
| Figure 162: BIOS Chipset Setup Menu – PCH-IO Configuration – PCI Express Configuration – PCIe clocks..... | 248 |
| Figure 163: BIOS Chipset Setup Menu – PCH-IO Configuration – SATA Configuration | 249 |
| Figure 164: BIOS Chipset Setup Menu – PCH-IO Configuration – USB Configuration | 251 |
| Figure 165: BIOS Chipset Setup Menu – PCH-IO Configuration – Security Configuration | 253 |
| Figure 166: BIOS Chipset Setup Menu – PCH-IO Configuration – HD Audio Configuration | 254 |
| Figure 167: BIOS Chipset Setup Menu – PCH-IO Configuration – HD Audio Configuration – HD Audio Advanced Configuration | 256 |
| Figure 168: BIOS Chipset Setup Menu – PCH-IO Configuration – HD Audio Configuration – HD Audio DSP Features Configuration | 257 |
| Figure 169: BIOS Chipset Setup Menu – PCH-IO Configuration – THC Configuration | 260 |
| Figure 170: BIOS Chipset Setup Menu – PCH-IO Configuration – SerialIO Configuration | 262 |
| Figure 171: BIOS Chipset Setup Menu – PCH-IO Configuration – SerialIO Configuration – Serial IO I2C0 Settings .. | 265 |
| Figure 172: BIOS Chipset Setup Menu – PCH-IO Configuration – SerialIO Configuration – Serial IO I2C0 Settings – Serial IO Touch Pad Settings..... | 265 |

| | |
|---|-----|
| Figure 173: BIOS Chipset Setup Menu – PCH-IO Configuration – SerialIO Configuration – Serial IO I2C0 Settings – Serial IO Touch Panel Settings..... | 266 |
| Figure 174: BIOS Chipset Setup Menu – PCH-IO Configuration – SerialIO Configuration – Serial IO I2C1/2/3/4/5/6/7 Settings..... | 267 |
| Figure 175: BIOS Chipset Setup Menu – PCH-IO Configuration – SerialIO Configuration – Serial IO SPI0/1/2 Settings | 267 |
| Figure 176: BIOS Chipset Setup Menu – PCH-IO Configuration – SerialIO Configuration – Serial IO UART0/1 Settings | 268 |
| Figure 177: BIOS Chipset Setup Menu – PCH-IO Configuration – SCS Configuration..... | 269 |
| Figure 178: BIOS Chipset Setup Menu – PCH-IO Configuration – ISH Configuration | 270 |
| Figure 179: BIOS Chipset Setup Menu – PCH-IO Configuration – Pch Thermal Throttling Control..... | 270 |
| Figure 180: BIOS Chipset Setup Menu – PCH-IO Configuration – FIVR Configuration | 272 |
| Figure 181: BIOS Chipset Setup Menu – PCH-IO Configuration – PMC Configuration..... | 274 |
| Figure 182: BIOS Chipset Setup Menu – PCH-IO Configuration – PMC Configuration – PMC ADR Configuration.... | 274 |
| Figure 183: BIOS Security Setup Menu | 276 |
| Figure 185: BIOS Security Setup Menu – Secure Boot – Key Management | 277 |
| Figure 184: BIOS Security Setup Menu – Secure Boot | 278 |
| Figure 186: BIOS Boot Setup Menu..... | 280 |
| Figure 187: BIOS Save & Exit Setup Menu..... | 282 |

1/Introduction

This user guide describes the 3.5"-SBC-AML/ADN/AMH/ADH board made by Kontron. This board will also be denoted 3.5"-SBC-AML/ADN/AMH/ADH within this user guide.

Use of this user guide implies a basic knowledge of PC-AT hardware and software. This user guide focuses on describing the 3.5"-SBC-AML/ADN/AMH/ADH board's special features and is not intended to be a standard PC-AT textbook.

New users are recommended to study the short installation procedure stated in the following chapter before switching on the power.

All configuration and setup of the CPU board is either carried out automatically or manually by the user via the BIOS setup menus.

Latest revision of this user guide, datasheet, thermal simulations, BIOS, drivers, BSP's (Board Support Packages), mechanical drawings (2D and 3D) can be downloaded from Kontron's Web Page.

2/Installation Procedures

NOTICE



ESD Sensitive Device!

Electrostatic discharge (ESD) can damage equipment and impair electrical circuitry.

- › Wear ESD-protective clothing and shoes
- › Wear an ESD-preventive wrist strap attached to a good earth ground
- › Check the resistance value of the wrist strap periodically (1 MΩ to 10 MΩ)
- › Transport and store the board in its antistatic bag
- › Handle the board at an approved ESD workstation
- › Handle the board only by the edges

NOTICE

Turn off PSU (Power Supply Unit) completely (no mains power connected to the PSU) or leave the Power Connectors unconnected while configuring the board. Otherwise, components (RAM, LAN cards etc.) might get damaged. Make sure the DC single supply used is within the range between 9 V and 36 V with suitable cable kit and PS-ON# active.

NOTICE

The power supply unit shall comply with the requirements as defined in IEC 62368-1 according to Clause 6.2.2 to power source category PS2 "Limited Power Source".

To get the board running follow these steps. If the board shipped from KONTRON already has components like RAM and CPU cooler mounted, then skip the relevant steps below.

1. Turn off the PSU (Power Supply Unit)
2. Insert the DDR5 4800 module
Be careful to push the memory module in the slot before locking the tabs.
3. Connecting interfaces
Insert all external cables for hard disk, keyboard etc. A monitor must be connected in order to change BIOS settings.
4. Connect and turn on PSU
Connect PSU to the board by the 3.0 mm pitch 1x4-pin wafer connector.
5. BIOS setup
Enter the BIOS setup by pressing the key during boot up.
Enter "Exit Menu" and Load Setup Defaults.



To clear all BIOS settings, including Password protection, activate "Clear CMOS Jumper" for 10 sec (without power connected).

6. Mounting the board in chassis

When fixing the board on a chassis, it is recommended to use screws with an integrated washer and a diameter of > 7 mm. Do not use washers with teeth, as they can damage the PCB and cause short circuits.

NOTICE

When mounting the board to chassis etc. Note that the board contains components on both sides of the PCB that can easily be damaged if board is handled without reasonable care. A damaged component can result in malfunction or no function at all.

2.1. Chassis Safety Standards

Before installing the 3.5"-SBC-AML/ADN/AMH/ADH in the chassis, users must evaluate the end product to ensure compliance with the requirements of the IEC 62368-1 safety standard:

- › The board must be installed in a suitable mechanical, electrical and fire enclosure.
- › The system, in its enclosure, must be evaluated for temperature and airflow considerations.
- › The board must be powered by a CSA or UL approved power supply that limits the maximum input current.
- › For interfaces having a power pin such as external power or fan, ensure that the connectors and wires are suitably rated. All connections from and to the product shall be with SELV circuits only.
- › Wires have suitable rating to withstand the maximum available power.
- › The peripheral device enclosure fulfils the IEC 62368-1 fire protecting requirements.

2.2. Lithium Battery Replacement

If replacing the lithium battery follow the replacement precautions stated in the notification below:

⚠ CAUTION

Danger of explosion if the lithium 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

VORSICHT! Explosionsgefahr bei unsachgemäßem Austausch der Batterie.

- › Ersatz nur durch denselben oder einen vom Hersteller empfohlenen gleichwertigen Typ
- › Entsorgung gebrauchter Batterien nach Angaben des Herstellers

ATTENTION! Risque d'explosion avec l'échange inadéquat de la batterie.

- › Remplacement seulement par le même ou un type équivalent recommandé par le producteur
- › L'évacuation des batteries usagées conformément à des indications du fabricant

PRECAUCION! Peligro de explosión si la batería se sustituye incorrectamente.

- › Sustituya solamente por el mismo o tipo equivalente recomendado por el fabricante
- › Disponga las baterías usadas según las instrucciones del fabricante

ADVARSEL! Lithiumbatteri – Eksplosionsfare ved fejlagtig håndtering.

- › Udsiftning må kun ske med batteri af samme fabrikat og type
- › Levér det brugte batteri tilbage til leverandøren

ADVARSEL! Eksplosjonsfare ved feilaktig skifte av batteri.

- › Benytt samme batteritype eller en tilsvarende type anbefalt av apparatfabrikanten
- › Brukte batterier kasseres i henhold til fabrikantens instruksjoner

VARNING! Explosionsfara vid felaktigt batteribyte.

- › Använd samma batterityp eller en ekvivalent typ som rekommenderas av apparattillverkaren
- › Kassera använt batteri enligt fabrikantens instruktion

VAROITUS! Paristo voi räjähtää, jos se on virheellisesti asennettu.

- › Vaihda paristo ainoastaan lalteval- mistajan suosittelemaan tyyppiln
- › Hävitä käytetty paristo valmistajan ohjeiden mukaisesti

3/System Specification

3.1. System Block Diagram

Figure 1: System Block Diagram 3.5"-SBC-AML/ADN

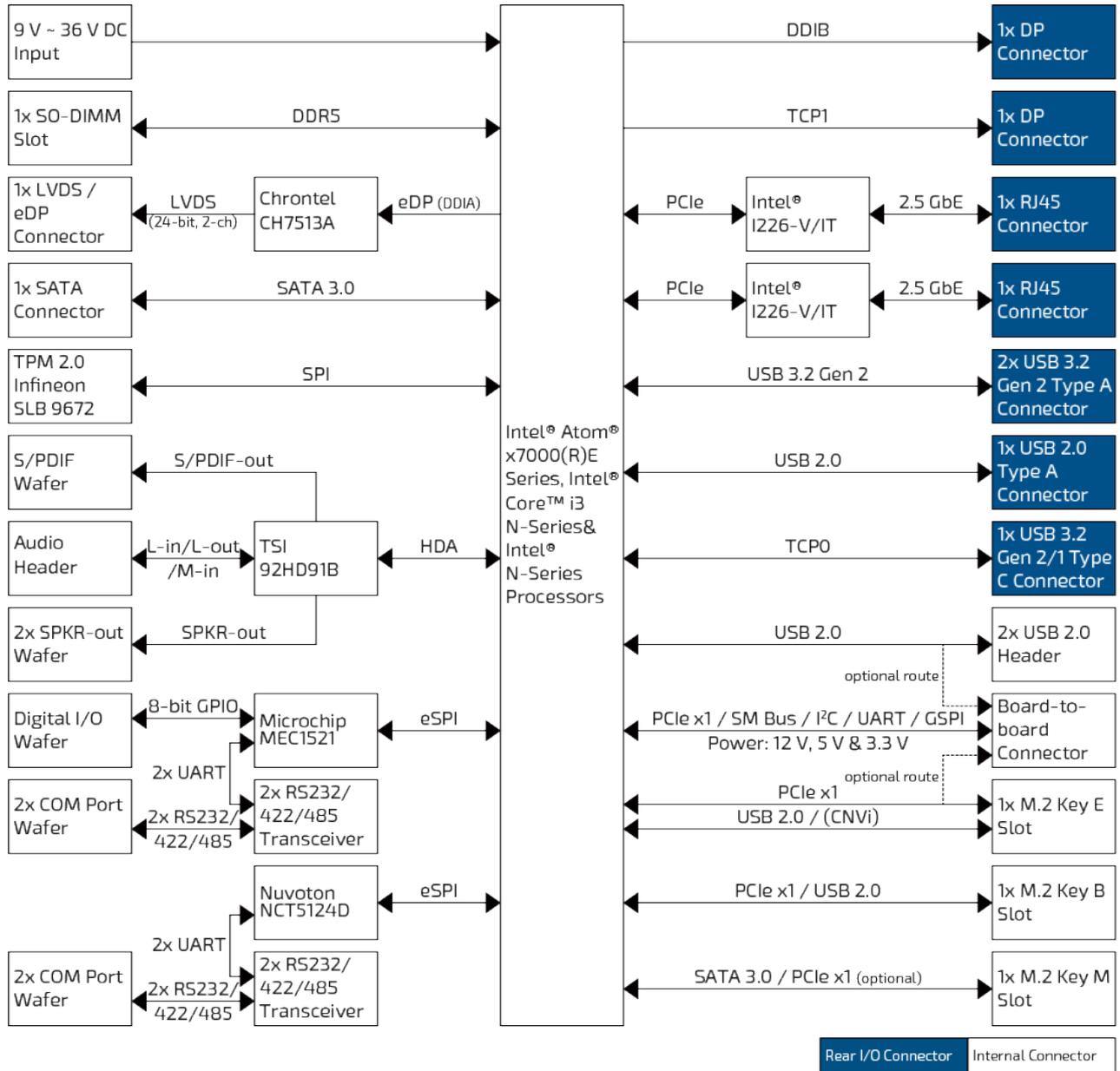
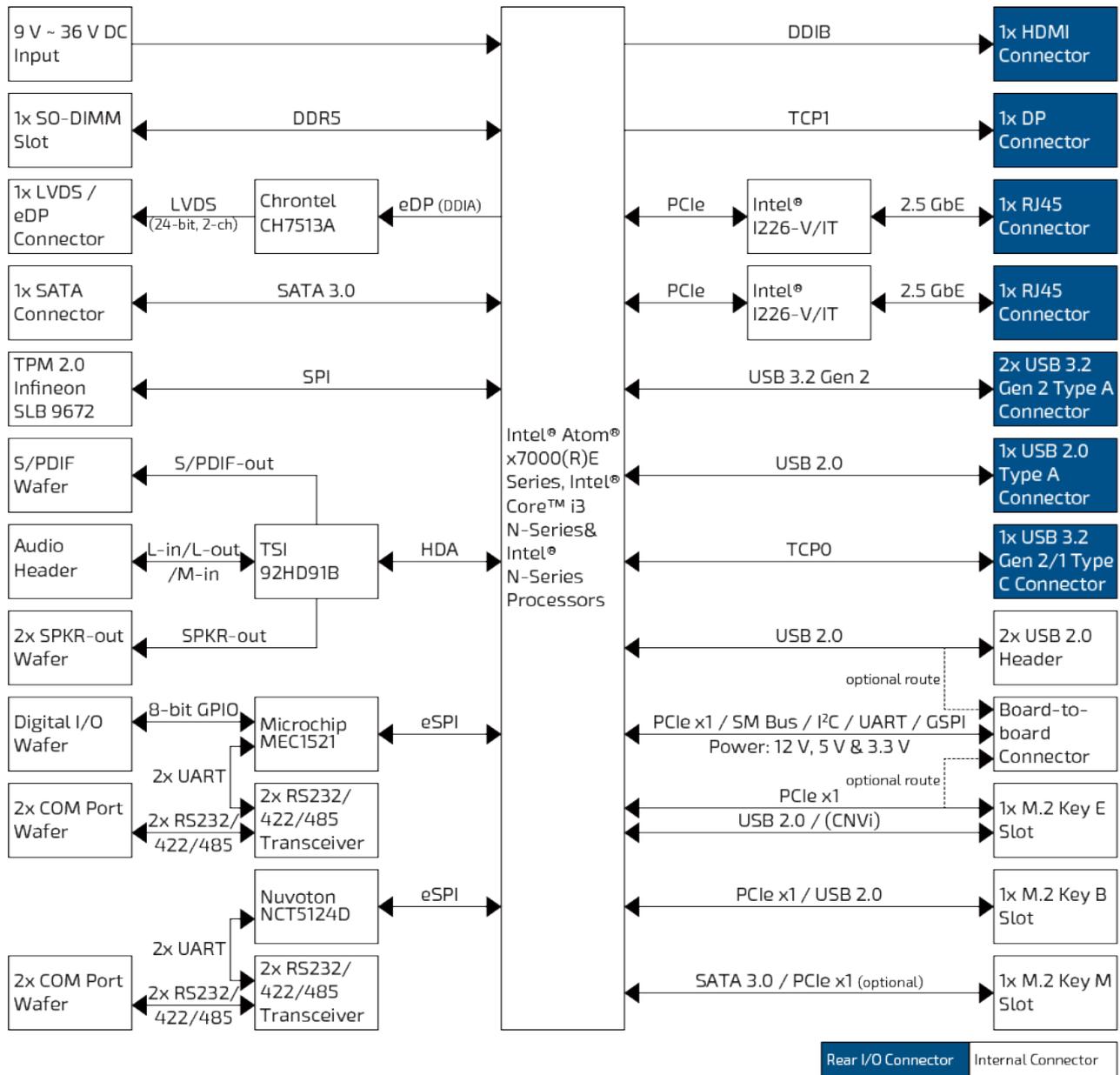


Figure 2: System Block Diagram 3.5"-SBC-AMH/ADH



3.2. Component Main Data

The table below summarizes the features of the 3.5"-SBC-AML/ADN/AMH/ADH single board computer.

Table 1: Component Main Data

| | 3.5"-SBC-AML/ADN | 3.5"-SBC-AMH/ADH |
|--------------------------------|--|--|
| System | | |
| Processor | Intel® Atom® x7000RE Series Processors Intel® Atom® x7000E Series Processors Intel® Core™ i3 N-Series Processors Intel® N-Series Processors | |
| Memory | 1x DDR5 SO-DIMM | |
| Video | | |
| Display Interface | 1x LVDS / eDP (24-bit, 2-ch, 1920 x 1200 @ 60 Hz / 4096 x 2160 @ 60 Hz) 3x DP (4096 x 2160 @ 60 Hz, 2x Full-size DP on rear, 1x DP USB-C on rear) | 1x LVDS / eDP (24-bit, 2-ch, 1920 x 1200 @ 60 Hz / 4096 x 2160 @ 60 Hz) 2x DP (4096 x 2160 @ 60 Hz, 1x Full-size DP on rear, 1x DP USB-C on rear) 1x HDMI 2.0 (4096 x 2160 @ 60 Hz, on rear) |
| Multiple Display | Triple | |
| Audio | | |
| Audio Codec | TSI 92HD91B | |
| Audio Display | 1x Speaker-out (Stereo, 3 W, by header) 1x Line-in (by header) 1x Line-out (by header) 1x Mic-in (by header) 1x S/PDIF Out (by header) | |
| Network Connection | | |
| Ethernet | 2x 2.5 GbE LAN (RJ45 on rear, Intel® I226-V/IT, with TSN for models with Atom® CPUs) | |
| Peripheral Connection | | |
| USB | 2x USB 3.2 Gen 2 Type A (on rear) 1x USB 3.2 Gen 2 Type C (on rear, w/ DP & PD 5 V / 3 A, except Atom® x7000RE) 1x USB 3.2 Gen 1 Type C (on rear, w/ DP & PD 5 V / 3 A, only Atom® x7000RE) 3x USB 2.0 (1x Type A on rear, 2x by header (optl. routed to board-to-board connector)) | |
| Serial Port | 4x RS232/422/485 (2x Tx/Rx only in RS232 signal, by header) | |
| Other I/Os | 4x DI (by wafer) 4x DO (by wafer) | |
| Storage & Expansion | | |
| SATA | 1x SATA 3.0 | |
| M.2 | 1x M.2 Key B (Type 2242 / 3042 / 3052 / 2280, w/ PCIe x1 / USB 2.0 / UIM) 1x M.2 Key E (Type 2230, w/ PCIe x1 (optl. routed to B2B) / USB 2.0 / UART / PCM / CNVi (Atom® x7000RE does not support CNVi)) 1x M.2 Key M (Type 2280, w/ SATA 3.0 (default) / PCIe x1 (optional)) | |
| SIM Card Holder | 1x SIM Card Holder (by header) | |

| | |
|--|---|
| Extended Board-to-board Connector | 1x PCIe x1 (default) / 2x PCIe x1 (optional, 1x replacing PCIe in M.2 Key E) 1x SM Bus 1x I ² C 1x UART 1x GSPI 2x USB 2.0 (optional, replacing the route to 2x internal USB 2.0) |
| Power | |
| Input Voltage | DC 9 V ~ 36 V |
| Connector | 1x4-pin pitch 3.0 mm Wafer |
| Firmware | |
| BIOS | AMI uEFI BIOS w/ 256 Mb SPI Flash |
| Watchdog | Programmable WDT to generate system reset event |
| H/W Monitor | Voltages Temperatures |
| Real Time Clock | Processor integrated RTC |
| Security | TPM 2.0 (Infineon SLB 9672) |
| System Control & Monitoring | |
| Button, Switch & Indicator | 1x Power Button (on rear) 1x Power LED (Green, on rear) 1x Standby LED (Yellow, on rear) 1x Internal Buzzer |
| Front Panel Header | 1x Header Reset Button, M.2 Key M LED & External Buzzer 1x Header for Power Button, Power LED & SM bus 2x Header for 2.5 GbE LAN LED |
| Cooling | |
| FAN | 1x Wafer for Smart Fan |
| Software | |
| OS Support | Windows 11 Windows 10 Linux |
| Mechanical | |
| Dimension (L x W) | ECX (146 mm x 105 mm / 5.75" x 4.13") |

3.3. Environmental Conditions

The 3.5"-SBC-AML/ADN/AMH/ADH is compliant with the following environmental conditions. It is the customer's responsibility to provide sufficient airflow around each of the components to keep them within the allowed temperature range.

Table 2: Environmental Conditions

| Environmental | Description |
|-----------------------|--|
| Operating Temperature | 0 °C ~ 60 °C / 32 °F ~ 140 °F (Standard) -40 °C ~ 85 °C / -40 °F ~ 185 °F (Extreme) |
| Storage Temperature | -20 °C ~ 80 °C / -4 °F ~ 176 °F (Standard) -55 °C ~ 85 °C / -67 °F ~ 185 °F (Extreme) |
| Humidity | 0 % ~ 95 % |

3.4. Compliance

The 3.5"-SBC-AML/ADN/AMH/ADH meets the following standards and certification tests.



If the product is modified, the prerequisites for specific approvals may no longer apply.

Table 3: Standards and Certifications

| Compliance | Description |
|--------------------|---|
| CE Class B UKCA | EN 55032: 2015 + A11: 2020, Class B BS EN 55032: 2015 + A11: 2020 CISPR 32: 2015 + COR1: 2016 EN 55032: 2015 + A1: 2020, Class B BS EN 55032: 2015 + A1: 2020 CISPR 32: 2015 + A1: 2019 EN 61000-3-2: 2014 EN IEC 61000-3-2: 2019 + A1: 2021 EN 61000-3-3: 2013 + A2: 2021 BS EN 61000-3-2:2014 BS EN IEC 61000-3-2: 2019 + A1: 2021 BS EN 61000-3-3: 2013 + A2: 2021 EN 55035: 2017 + A11: 2020 BS EN 55035: 2017 + A11: 2020 IEC 61000-4-2: 2008 IEC 61000-4-3: 2020 IEC 61000-4-4: 2012 IEC 61000-4-5: 2014 + A1: 2017 IEC 61000-4-6: 2023 IEC 61000-4-8: 2009 IEC 61000-4-11: 2020 + COR2: 2022 EN IEC 61000-6-2: 2019 EN IEC 61000-6-4: 2019 |

| Compliance | Description |
|---|--|
| FCC Class B ICES Class B | FCC CFR Title 47 Part 15 Subpart B, Class B ICES-003 Issue 7: 2020 Class B ANSI C63.4: 2014 ANSI C63.4a: 2017 |
| UR (UL Recognized) CSA | UL 62368-1, 3rd Ed. CSA C22.2 No. 62368-1:19, 3rd Ed. |

3.5. Processor Support

The 3.5"-SBC-AML/ADN/AMH/ADH is designed to support Intel® Atom® x7000RE Series, Intel® Atom® x7000E Series, Intel® Core™ i3 N-Series and Intel® N-Series Processors. The BGA CPU is remounted from factory. Kontron has defined the CPU SKUs as listed in the following table for either standard or project-based board versions, so far all based on Embedded CPUs. Other CPU SKUs are expected at a later date.

Table 4: Processor Support

| Name | Core # | Speed (GHz) | Turbo (GHz) | Embedd. | Cache | Socket | TDP (W) | TDP-down (W) | Tj (°C) |
|----------------------|--------|-------------|-------------|---------|-------|-----------|---------|--------------|---------|
| Intel® Atom® x7211RE | 2 | 1.0 | 3.2 | Yes | 6M | FCBGA1264 | 6 | - | 105 |
| Intel® Atom® x7213RE | 2 | 2.0 | 3.4 | Yes | 6M | FCBGA1264 | 9 | - | 105 |
| Intel® Atom® x7433RE | 4 | 1.5 | 3.4 | Yes | 6M | FCBGA1264 | 9 | - | 105 |
| Intel® Atom® x7835RE | 8 | 1.3 | 3.6 | Yes | 6M | FCBGA1264 | 12 | - | 105 |
| Intel® Atom® x7211E | 2 | 1.0 | 3.2 | Yes | 6M | FCBGA1264 | 6 | - | 105 |
| Intel® Atom® x7213E | 2 | 1.7 | 3.2 | Yes | 6M | FCBGA1264 | 10 | - | 105 |
| Intel® Atom® x7425E | 4 | 1.5 | 3.4 | Yes | 6M | FCBGA1264 | 12 | - | 105 |
| Intel® Core™ i3-N305 | 8 | 1.8 | 3.8 | Yes | 6M | FCBGA1264 | 15 | 9 | 105 |
| Intel® N50 | 2 | 1.0 | 3.4 | Yes | 6M | FCBGA1264 | 6 | - | 105 |
| Intel® N97 | 4 | 2.0 | 3.6 | Yes | 6M | FCBGA1264 | 12 | - | 105 |
| Intel® N200 | 4 | 1.0 | 3.7 | Yes | 6M | FCBGA1264 | 6 | - | 105 |

Sufficient cooling must be applied to the CPU in order to remove the effect as listed as TDP (Thermal Design Power) in above table. The sufficient cooling is also depending on the worst case maximum ambient operating temperature and the actual worst case load of processor.

3.6. System Memory Support

The 3.5"-SBC-AML/ADN/AMH/ADH has one DDR5 SO-DIMM sockets.

The socket supports the following memory features:

- › 1x DDR5 SO-DIMM 262-pin
- › Single-channel with 1x SO-DIMM per channel
- › Up to 16 GB
- › SPD timing supported
- › In-band ECC supported

The installed DDR5 SO-DIMM should support the Serial Presence Detect (SPD) data structure. This allows the BIOS to read and configure the memory controller for optimal performance. If non-SPD memory is used, the BIOS will attempt to configure the memory settings, but performance and reliability may be impacted, or the board may not be able to boot totally.

3.7. Memory Operating Frequencies

In all modes, the frequency of system memory is the lowest frequency of the memory module placed in the system. The memory module's frequency can be determined through the SPD register on the memory module. The table below lists the resulting operating memory frequencies based on the combination of SO-DIMM and processor.

Table 5: Memory Operating Frequencies

| SO-DIMM Type | Module Name | Memory Data Transfer (MT/s) | Processor System Bus Frequency (MHz) | Resulting Memory Clock Frequency (MHz) | Peak Transfer Rate (MB/s) |
|--------------|-------------|-----------------------------|--------------------------------------|--|---------------------------|
| DDR5 4800 | PC5-38400 | 4800 | 2400 | 300 | 38400 |

The memory module has in general a much lower longevity than the embedded motherboard, and therefore EOL of the module can be expected several times during lifetime of the motherboard.

As a minimum it is recommend using Kontron memory module for prototype system(s) in order to prove stability of the system and as for reference.

For volume production you might request to test and qualify other types of RAM. In order to qualify RAM it is recommend configuring 3 systems running RAM Stress Test program in heat chamber at 60° C for a minimum of 24 hours.

3.8. On-board Graphics Subsystem

The 3.5"-SBC-AML/ADN/AMH/ADH supports Intel® UHD Graphics Gen12 technology for high quality graphics capabilities. All 3.5"-SBC-AML/ADN/AMH/ADH versions support triple displays pipes.

Triple displays can be used simultaneously and be used to implement independent or cloned display configuration.

The 3.5"-SBC-AML/ADN/AMH/ADH itself provides one internal LVDS / eDP combo interface. The 3.5"-SBC-AML/ADN has two external full-size DisplayPort connectors and one external DisplayPort over USB Type C connector, while the 3.5"-SBC-AMH/ADH has one external HDMI 2.0 connector, one external full-size DisplayPort connector and one external DisplayPort over USB Type C connector.

Table 6: Triple-displays Configurations 3.5"-SBC-AML/ADN

| Display 1 | Display 2 | Display 3 | Max. Resolution (Px) at 60 Hz | | |
|-----------|-----------|-----------|-------------------------------|-------------|-------------|
| | | | Display 1 | Display 2 | Display 3 |
| LVDS | DP | DP | 1920 x 1200 | 4096 x 2160 | 4096 x 2160 |
| eDP | DP | DP | 4096 x 2160 | 4096 x 2160 | 4096 x 2160 |
| LVDS | DP | DP USB-C | 1920 x 1200 | 4096 x 2160 | 4096 x 2160 |
| eDP | DP | DP USB-C | 4096 x 2160 | 4096 x 2160 | 4096 x 2160 |
| DP | DP | DP USB-C | 4096 x 2160 | 4096 x 2160 | 4096 x 2160 |

Table 7: Triple-displays Configurations 3.5"-SBC-AMH/ADH

| Display 1 | Display 2 | Display 3 | Max. Resolution (Px) at 60 Hz | | |
|-----------|-----------|-----------|-------------------------------|-------------|-------------|
| | | | Display 1 | Display 2 | Display 3 |
| LVDS | HDMI | DP | 1920 x 1200 | 4096 x 2160 | 4096 x 2160 |
| eDP | HDMI | DP | 4096 x 2160 | 4096 x 2160 | 4096 x 2160 |
| LVDS | DP | DP USB-C | 1920 x 1200 | 4096 x 2160 | 4096 x 2160 |
| eDP | DP | DP USB-C | 4096 x 2160 | 4096 x 2160 | 4096 x 2160 |
| LVDS | HDMI | DP USB-C | 1920 x 1200 | 4096 x 2160 | 4096 x 2160 |
| eDP | HDMI | DP USB-C | 4096 x 2160 | 4096 x 2160 | 4096 x 2160 |
| HDMI | DP | DP USB-C | 4096 x 2160 | 4096 x 2160 | 4096 x 2160 |

3.9. Power Input Voltage

In order to ensure safe operation of the board, the input power must monitor the input voltage and shut down if the voltage is out of range – refer to the actual input power specification. Please note, in order to keep the power consumption to a minimal level, boards do not implement a guaranteed minimum load. The 3.5"-SBC-AML/ADN/AMH/ADH board must be powered by a single DC input power within the range between 9 V and 36 V applied through the 3.0 mm pitch 1x4-pin wafer connector CN9 (see Chapter 7.1.1).

NOTICE

Hot Plugging power supply is not supported. Hot plugging might damage the board.

The input voltages applied at the power input connector are required as follows:

Table 8: Power Input Voltages

| Power Input | Min. | Max. | Note |
|-------------|--------|--------|-------------------------------|
| 9 V ~ 36 V | 8.55 V | 37.8 V | Should be $\pm 5\%$ tolerance |

3.10. Power Consumption

The power consumption is measured under the following software and hardware test condition:

- 3.5"-SBC-AML/ADN/AMH/ADH with Intel® Atom® x7835RE processor (Octa Core @ 3.6 GHz)
- Memory: 1x 8 GByte TEAMGROUP DDR5 5600 RAM
- Storage: 128 GByte Phison M.2 SATA SSD
- Operating System: Windows 11 IoT LTSC 24H2

The power consumption in different modes is as follows:

Table 9: Power Consumption

| Power Status | Input Voltage | Power Consumption |
|---------------|---------------|-------------------|
| Boot (Peak) | +36 V | 68.76 W |
| | +9 V | 42.21 W |
| Idle (S0) | +36 V | 7.06 W |
| | +9 V | 8.66 W |
| Full Run (S0) | +36 V | 19.84 W |
| | +9 V | 17.82 W |

| Power Status | Input Voltage | Power Consumption |
|--------------------|---------------|-------------------|
| Sleep (S3) | +36 V | 2.09 W |
| | +9 V | 2.04 W |
| Shutdown (S4 / S5) | +36 V | 2.02 W |
| | +9 V | 2.02 W |
| Shutdown (PSM) | +36 V | 108 mW |
| | +9 V | 36 mW |

4/Connector Locations

4.1. Top Side

Figure 3: Top Side

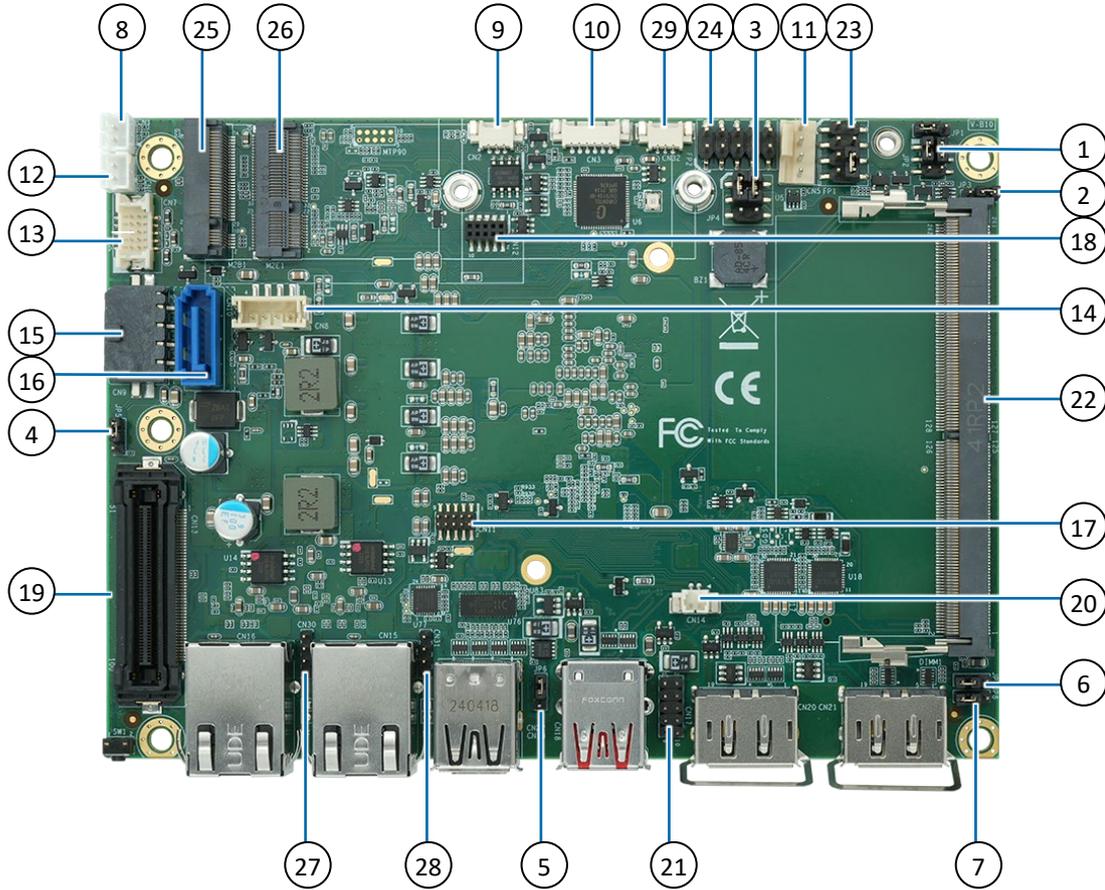


Table 10: Jumper List

| Item | Designation | Description | See Chapter |
|------|-------------|--|-------------|
| 1 | JP2 | LVDS / eDP Backlight Enable Selection | 7.22.1 |
| 2 | JP3 | AT / ATX Power Mode Selection | 7.22.2 |
| 3 | JP4 | LVDS / eDP Backlight Power & Panel Power Selection | 7.22.3 |
| 4 | JP5 | Onboard DC-DC 12 V Selection | 7.22.4 |
| 5 | JP6 | USB Power Selection | 7.22.5 |
| 6 | JP7 | Flash Descriptor Security Override Selection | 7.22.6 |
| 7 | JP8 | Clear CMOS Selection | 7.22.7 |

Table 11: Top Side Internal Connector Pin Assignment

| Item | Designation | Description | See Chapter |
|------|-------------|--|-------------|
| 8 | CN1 | Left Channel Audio AMP Output Wafer | 7.6 |
| 9 | CN2 | S/PDIF Output Wafer | 7.8 |
| 10 | CN3 | SIM Card Wafer for M.2 Key B | 7.19 |
| 11 | CN5 | FAN Wafer | 7.2 |
| 12 | CN6 | Right Channel Audio AMP Output Wafer | 7.6 |
| 13 | CN7 | Audio Input / Output Header | 7.7 |
| 14 | CN8 | SATA Power Output Wafer | 7.4 |
| 15 | CN9 | DC Power Input Wafer | 7.1.1 |
| 16 | CN10 | SATA Connector | 7.3 |
| 17 | CN11 | SPI 10-Pins Header | 7.15 |
| 18 | CN12 | P80 Holder | - |
| 19 | CN13 | Board-to-board Connector | 7.21 |
| 20 | CN14 | RTC Power Input Wafer | 7.1.2 |
| 21 | CN17 | USB 2.0 Port 3 & 4 Header | 7.5 |
| 22 | DIMM1 | DDR5 Channel 1 SO-DIMM Slot | 3.6 |
| 23 | FP1 | Front Panel Header 1 | 7.9 |
| 24 | FP2 | Front Panel Header 2 | 7.9 |
| 25 | M2B1 | M.2 Key B 2242 / 3042 / 3052 / 2280 Slot | 7.16 |
| 26 | M2E1 | M.2 Key E 2230 Slot | 7.17 |
| 27 | CN30 | 2.5 GbE LAN1 LED Header | 7.20 |
| 28 | CN31 | 2.5 GbE LAN2 LED Header | 7.20 |
| 29 | CN32 | LVDS / eDP Backlight Brightness Wafer | 7.13 |

4.2. Rear Side

Figure 4: Rear Side

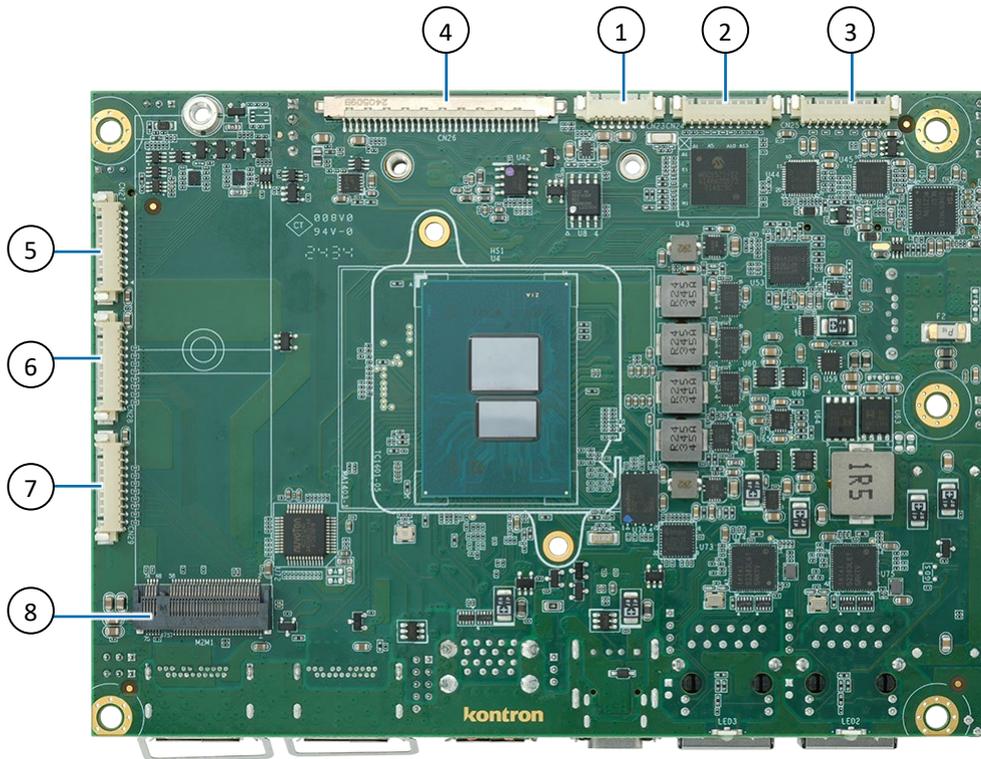


Table 12: Rear Side Internal Connector Pin Assignment

| Item | Designation | Description | See Chapter |
|------|-------------|----------------------------------|-------------|
| 1 | CN23 | LVDS / eDP Backlight Power Wafer | 7.12 |
| 2 | CN24 | RS232/422/485 COM2 Wafer | 7.10 |
| 3 | CN25 | RS232/422/485 COM1 Wafer | 7.10 |
| 4 | CN26 | LVDS / eDP Combo Connector | 7.11 |
| 5 | CN27 | DIO Wafer | 7.14 |
| 6 | CN28 | RS232/422/485 COM3 Wafer | 7.10 |
| 7 | CN29 | RS232/422/485 COM4 Wafer | 7.10 |
| 8 | M2M1 | M.2 Key M 2280 Slot | 7.18 |

4.3. Connector Panel Side

Figure 5: Connector Panel Side – 3.5"-SBC-AML/ADN

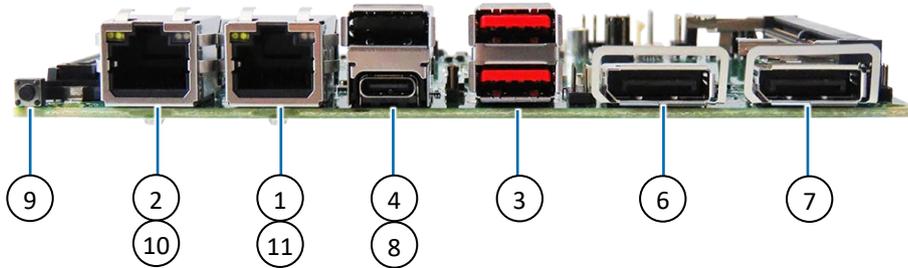


Figure 6: Connector Panel Side – 3.5"-SBC-AMH/ADH

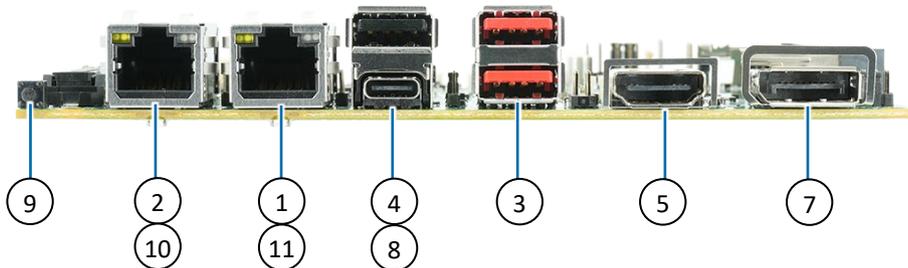


Table 13: Connector Panel Side Connector List

| Item | Designation | Description | See Chapter |
|------|-------------|--|-------------|
| 1 | CN15 | 2.5 GbE LAN2 RJ45 Connector | 6.1 |
| 2 | CN16 | 2.5 GbE LAN1 RJ45 Connector | 6.1 |
| 3 | CN18 | USB 3.2 Gen 2 Port 1, 2 Type A Connector | 6.5 |
| 4 | CN19 | USB 2.0 Port 5 Type A Connector | 6.5 |
| 5 | CN20 | HDMI 2.0 Connector (3.5"-SBC-AMH/ADH only) | 6.2 |
| 6 | CN20 | DP Port 1 Connector (3.5"-SBC-AML/ADN only) | 6.3 |
| 7 | CN21 | DP Port 2 Connector | 6.3 |
| 8 | CN22 | DP over USB 3.2 Gen 2 / Gen 1 Type C Connector | 6.4 |
| 9 | SW1 | Power Button | 6.6 |
| 10 | LED2 | Power LED | 6.7 |
| 11 | LED3 | Standby LED | 6.7 |

5/Connector Definitions

The following defined terms are used within this user guide to give more information concerning the pin assignment and to describe the connector's signals.

| Defined Term | Description |
|--------------------|---|
| Pin | Shows the pin numbers in the connector |
| Signal | The abbreviated name of the signal at the current pin The notation "XX#" states that the signal "XX" is active low |
| Note | Special remarks concerning the signal |
| Designation | Type and number of item described |
| See Chapter | Number of the chapter within this user guide containing a detailed description |

The abbreviation TBD is used for specifications that are not available yet or which are not sufficiently specified by the component vendors.

6/I/O-Area Connectors

6.1. Ethernet Connectors (CN15 & CN16)

The 3.5"-SBC-AML/ADN/AMH/ADH supports two channels of 10/100/1000/2500 Mbit Ethernet, which are based Intel® I226-V/IT controllers.

In order to achieve the specified performance of the Ethernet port, Category 5 twisted pair cables must be used with 10/100 MByte and Category 5E, 6 or 6E with 1 Gbit/2.5 Gbit LAN networks.

The signals for the Ethernet ports are as follows:

Figure 7: Ethernet Connector CN15, CN16

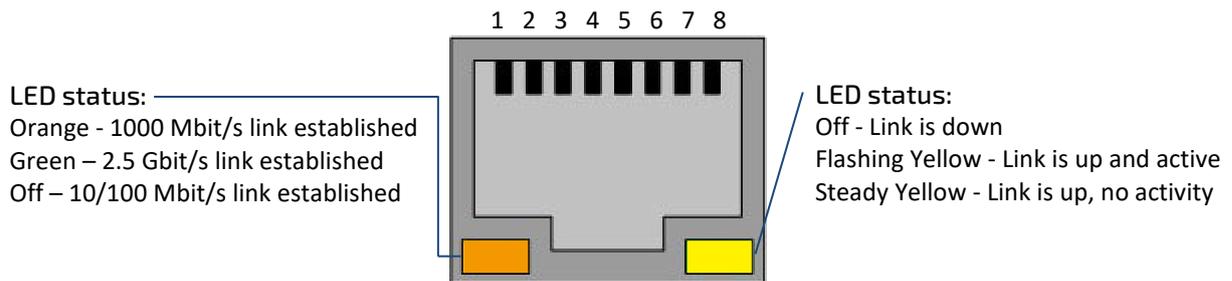


Table 14: Pin Assignment Ethernet Connectors CN15, CN16

| Pin | Signal | Note |
|-----|--------|------|
| 1 | TX1+ | |
| 2 | TX1- | |
| 3 | TX2+ | |
| 4 | TX3+ | |
| 5 | TX3- | |
| 6 | TX2- | |
| 7 | TX4+ | |
| 8 | TX4- | |

Signal Description

| Signal | Description |
|--------------------|--|
| TX1+ / TX1- | In MDI mode, this is the first pair in 2.5GBase-T and 1000Base-T, and is the transmit pair in 10Base-T and 100Base-TX. In MDI crossover mode, this pair is the receive pair in 10Base-T and 100Base-TX. |
| TX2+ / TX2- | In MDI mode, this is the second pair in 2.5GBase-T and 1000Base-T, and is the receive pair in 10Base-T and 100Base-TX. In MDI crossover mode, this pair is the transmit pair in 10Base-T and 100Base-TX. |
| TX3+ / TX3- | In MDI mode, this is the third pair in 2.5GBase-T and 1000Base-T. |
| TX4+ / TX4- | In MDI mode, this is the fourth pair in 2.5GBase-T and 1000Base-T. |

'MDI' – media dependent Interface

6.2. HDMI Connector (CN20)

The 3.5"-SBC-AMH/ADH supports one HDMI connector on the external I/O connector panel. The HDMI connector is based on standard HDMI type A and compliant with HDMI 2.0.

Figure 8: HDMI Connector CN20

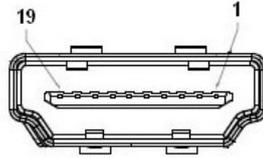


Table 15: Pin Assignment HDMI Connector CN20

| Pin | Signal | Description | Note |
|-----|-----------------|---|------|
| 1 | TMDS Data2+ | HDMI Lane 2 transmitter differential pair (+) | |
| 2 | GND | Ground | |
| 3 | TMDS Data2- | HDMI Lane 2 transmitter differential pair (-) | |
| 4 | TMDS Data1+ | HDMI Lane 1 transmitter differential pair (+) | |
| 5 | GND | Ground | |
| 6 | TMDS Data1- | HDMI Lane 1 transmitter differential pair (-) | |
| 7 | TMDS Data0+ | HDMI Lane 0 transmitter differential pair (+) | |
| 8 | GND | Ground | |
| 9 | TMDS Data0- | HDMI Lane 0 transmitter differential pair (-) | |
| 10 | TMDS Clock+ | HDMI Clock differential pair (+) | |
| 11 | GND | Ground | |
| 12 | TMDS Clock- | HDMI Clock differential pair (-) | |
| 13 | Reserved | No connection on device pin | |
| 14 | Reserved | No connection on device pin | |
| 15 | DDC_CLK | DDC based control signal (clock) | |
| 16 | DDC_DATA | DDC based control signal (data) | |
| 17 | GND | Ground | |
| 18 | +5 V Power | +5 V power supply | |
| 19 | Hot Plug Detect | HDMI hot plug detect | |

6.3. DP Connector (CN20 & CN21)

The 3.5"-SBC-AML/ADN supports two DP (DisplayPort) connectors (CN20 & CN21) on the external I/O connector panel while the 3.5"-SBC-AMH/ADH supports only one (CN21). The DP connectors are based on standard DP female port.

Figure 9: DP Connector CN20, CN21

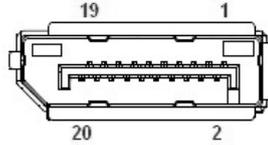


Table 16: Pin Assignment DP Connector CN20, CN21

| Pin | Signal | Description | Note |
|-----|-----------|---|------|
| 1 | ML_Lane0p | DisplayPort Lane 0 transmitter differential pair (+) | |
| 2 | GND | Ground | |
| 3 | ML_Lane0n | DisplayPort Lane 0 transmitter differential pair (-) | |
| 4 | ML_Lane1p | DisplayPort Lane 1 transmitter differential pair (+) | |
| 5 | GND | Ground | |
| 6 | ML_Lane1n | DisplayPort Lane 1 transmitter differential pair (-) | |
| 7 | ML_Lane2p | DisplayPort Lane 2 transmitter differential pair (+) | |
| 8 | GND | Ground | |
| 9 | ML_Lane2n | DisplayPort Lane 2 transmitter differential pair (-) | |
| 10 | ML_Lane3p | DisplayPort Lane 3 transmitter differential pair (+) | |
| 11 | GND | Ground | |
| 12 | ML_Lane3n | DisplayPort Lane 3 transmitter differential pair (-) | |
| 13 | Config1 | Connected to ground, either directly or through a pulldown device | |
| 14 | Config2 | Connected to ground, either directly or through a pulldown device | |
| 15 | AUX_CHp | DisplayPort Auxiliary channel differential pair (+) | |
| 16 | GND | Ground | |
| 17 | AUX_CHn | DisplayPort Auxiliary channel differential pair (-) | |
| 18 | Hot_Plug | DisplayPort hot plug detect | |
| 19 | GND | Ground | |
| 20 | DP_PWR | Power for connector | |

6.4. DP over USB Type C Connector (CN22)

The DP (DisplayPort) over USB Type C connector supports DisplayPort Alternate Mode, USB 3.2 Gen 2 (variants with Intel® Atom® x7000E Series, Intel® Core™ i3 N-Series & Intel® N-Series processors) / Gen 1 (variants with Intel® Atom® x7000RE Series processors) and power delivery of up to 15 W (5 V at 3 A).

Figure 10: DP over USB Type C Connector CN22

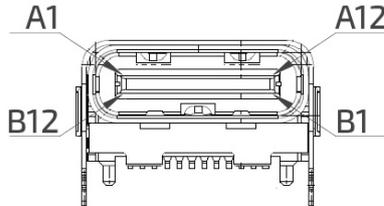


Table 17: Pin Assignment DP over USB Type C Connector CN22

| Pin | Signal | Description | Note |
|-----|------------|---|------|
| A1 | GND | Ground | |
| A2 | CON_TX1P_C | USB 3.2 Tx differential pair (+) / DP Lane 2 Tx differential pair (+) | |
| A3 | CON_TX1N_C | USB 3.2 Tx differential pair (-) / DP Lane 2 Tx differential pair (-) | |
| A4 | +5V_VBUS* | +5 V bus power | |
| A5 | CC1 | Configuration channel signal 1 | |
| A6 | USB2_P | USB 2.0 differential pair (+), position 1 | |
| A7 | USB2_N | USB 2.0 differential pair (-), position 2 | |
| A8 | SBU1 | Sideband use signal 1: DP Auxiliary channel differential pair (+) | |
| A9 | +5V_VBUS* | +5 V bus power | |
| A10 | CON_RX2N_C | DP Lane 0 Tx differential pair (-) | |
| A11 | CON_RX2P_C | DP Lane 0 Tx differential pair (+) | |
| A12 | GND | Ground | |
| B1 | GND | Ground | |
| B2 | CON_TX2P_C | DP Lane 1 Tx differential pair (+) | |
| B3 | CON_TX2N_C | DP Lane 1 Tx differential pair (-) | |
| B4 | +5V_VBUS* | +5 V bus power | |
| B5 | CC2 | Configuration channel signal 2 | |
| B6 | USB2_P | USB 2.0 differential pair (+), position 2 | |
| B7 | USB2_N | USB 2.0 differential pair (-), position 2 | |
| B8 | SUB2 | Sideband use signal 2: DP Auxiliary channel differential pair (-) | |
| B9 | +5V_VBUS* | +5 V bus power | |
| B10 | CON_RX1N_C | USB 3.2 Rx differential pair (-) / DP Lane 3 Tx differential pair (-) | |
| B11 | CON_RX1P_C | USB 3.2 Rx differential pair (+) / DP Lane 3 Tx differential pair (+) | |
| B12 | GND | Ground | |



* The power source of VBUX can be selected through JP6.

6.5. USB Connectors (I/O Area)

The external I/O connector panel supports one dual USB 3.2 Gen 2 connector (CN18) and one USB 2.0 connector (CN19).



USB 3.2 Gen 2 ports are backward compatible with USB 3.2 Gen 1 and USB 2.0.

Figure 11: USB 3.2 Gen 2 Connectors CN18 - Top & Bottom

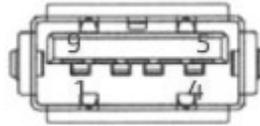


Table 18: Pin Assignment USB 3.2 Gen 2 Connectors CN18 - Top & Bottom

| Pin | Signal | Description | Note |
|-----|-----------|---|------|
| 1 | +USB_VCC* | +5 V power supply for USB device | |
| 2 | USB_D- | USB 2.0 differential pair (-) | |
| 3 | USB_D+ | USB 2.0 differential pair (+) | |
| 4 | GND | Ground | |
| 5 | USB_RX- | USB 3.2 receiver differential pair (-) | |
| 6 | USB_RX+ | USB 3.2 receiver differential pair (+) | |
| 7 | GND | Ground | |
| 8 | USB_TX- | USB 3.2 transmitter differential pair (-) | |
| 9 | USB_TX+ | USB 3.2 transmitter differential pair (+) | |



* The power source of +USB_VCC can be selected through JP6.

Figure 12: USB 2.0 Connectors CN19

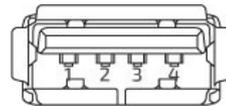


Table 19: Pin Assignment USB 2.0 Connectors CN19

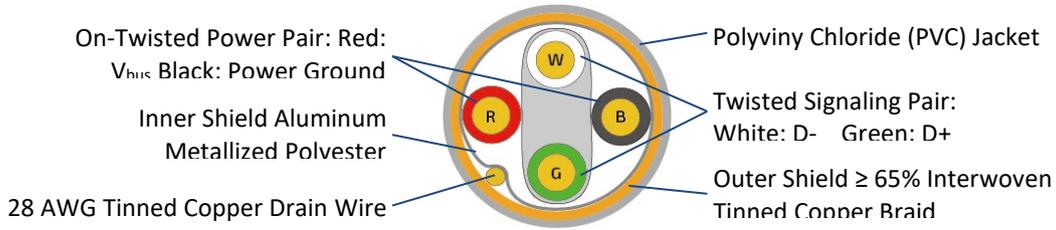
| Pin | Signal | Description | Note |
|-----|-----------|----------------------------------|------|
| 1 | +USB_VCC* | +5 V power supply for USB device | |
| 2 | USB_D- | USB 2.0 differential pair (-) | |
| 3 | USB_D+ | USB 2.0 differential pair (+) | |
| 4 | GND | Ground | |



* The power source of +USB_VCC can be selected through JP6.

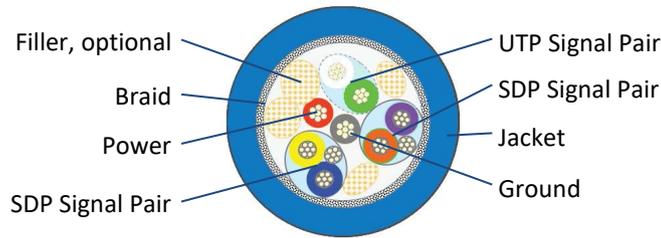
For HiSpeed rates it is required to use a USB cable, which is specified in USB 2.0 standard:

Figure 13: USB 2.0 High Speed Cable



For USB 3.2 Gen 2 cabling it is required to use only HiSpeed USB cable, specified in USB 3.2 standard:

Figure 14: USB 3.2 High Speed Cable



6.6. Power Button (SW1)

The external I/O connector panel supports a power button (SW1) for turning on and off the board.

6.7. LED Indicators (LED2 & LED3)

The external I/O connector panel supports one power LED indicator (LED2) and one standby LED indicator (LED3) for power and standby status indication.

Table 20: LED Indicators LED2, LED3

| LED Status | | Description |
|------------------|--------------------|---------------------------------------|
| Power LED (LED2) | Standby LED (LED3) | |
| Green LED On | Yellow LED On | S0 (Full On) |
| Green LED Blink | Yellow LED On | S3 (Suspend-To-RAM) |
| LED Off | Yellow LED On | S4 (Suspend-To-Disk) or S5 (Soft Off) |
| LED Off | LED Off | EUP Mode or G3 (Mechanical Off) |

7/Internal Connectors

7.1. Power Connector

Power connector must be used to supply the board with a single DC power within the range between 9 V and 36 V ($\pm 5\%$).

NOTICE

Hot plugging any of the power connectors is not allowed.

Hot plugging might damage the board. In other words, turn off main supply etc. to make sure all the power lines are turned off when connecting to the motherboard.

7.1.1. Power Input Wafer (CN9)

The 1x4-pin 3.0 mm pitch power input wafer CN9 provides a single DC power within the range between 9 V and 36 V to the board.

Figure 15: Power Input Wafer CN9

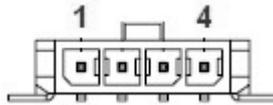


Table 21: Pin Assignment CN9

| Pin | Signal | Description | Note |
|----------------------------|---------------|-------------|------|
| 1 | +Vin* | Power input | |
| 2 | GND | Ground | |
| 3 | GND | Ground | |
| 4 | +Vin* | Power input | |
| Connector Type | | | |
| B2W, 1x4-pin, 3.0 mm pitch | | | |
| Mating Connector | | | |
| Vendor | Pinrex | | |
| Housing Model No. | 733-75-M104B6 | | |
| Terminal Model No. | 733-70-FT0006 | | |

In case of:

- using 12 V supply for LVDS / eDP backlight (refer to Chapter 7.12, CN23);
- using 12 V supply for SATA HDD / SSD (refer to Chapter 7.4, CN8);
- connecting a cooling fan (refer to Chapter 7.2, CN5); and / or
- connecting a daughter board via the board-to-board connector (refer to Chapter 7.21, CN13),



It is recommended that +Vin be above 16 V in order to have a stable 12 V supply for LVDS / eDP backlight, SATA HDD / SSD, smart fan and / or daughter board.

7.1.2. RTC Power Input Wafer (CN14)

The 1x2-pin 1.25 mm pitch RTC power input wafer CN14 is intended to be connected to the battery. The battery provides power to the system clock to retain the time when power is turn off.

Figure 16: RTC Power Input Wafer CN14



Table 22: Pin Assignment CN14

| Pin | Signal | Description | Note |
|-----------------------------|---------------|--------------------------------------|------|
| 1 | +VRTC | Real-time clock backup battery input | |
| 2 | GND | Ground | |
| Connector Type | | | |
| B2W, 1x2-pin, 1.25 mm pitch | | | |
| Mating Connector | | | |
| Vendor | Pinrex | | |
| Housing Model No. | 712-75-02W001 | | |
| Terminal Model No. | 712-70-T00001 | | |

7.2. Fan Wafer (CN5)

The 1x4-pin 2.54 mm pitch fan wafer CN5 is used for the connection of the fan for the processor or system.

Figure 17: Fan Wafer CN5

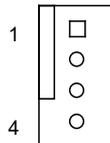


Table 23: Pin Assignment CN5

| Pin | Signal | Description | Note |
|-----------------------------|------------------|--|----------|
| 1 | GND | Power supply ground signal | |
| 2 | V _{FAN} | Power supply for fan ▶ V _{FAN} = +12 V in case of V _{in} between 15 V and 36 V ▶ V _{FAN} = V _{in} – V _{DROP} (≤ +12 V) in case of V _{in} between 9 V and 15 V Depending on the SBC load, V _{DROP} (Voltage Drop) is approximately 1 V ~ 3 V. | 1 A max. |
| 3 | SENSE | Sense input signal from the fan, for rotation speed supervision RPM (Rotations Per Minute). | |
| 4 | PWM | PWM output signal for FAN speed control | |
| Connector Type | | | |
| B2W, 1x4-pin, 2.54 mm pitch | | | |

7.3. SATA (Serial ATA) Connector (CN10)

The SATA connector CN10 supplies the data connection for the SATA hard disk and is SATA 3.0 compatible.

Figure 18: SATA Connector CN10

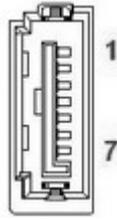


Table 24: Pin Assignment CN10

| Pin | Signal | Description | Note |
|-----------------------------|---------------|---|------|
| 1 | GND | Ground | |
| 2 | TX+ | Host transmitter differential signal pair (+) | |
| 3 | TX- | Host transmitter differential signal pair (-) | |
| 4 | GND | Ground | |
| 5 | RX- | Host receiver differential signal pair (-) | |
| 6 | RX+ | Host receiver differential signal pair (+) | |
| 7 | GND | Ground | |
| Connector Type | | | |
| B2W, 1x7-pin, 1.27 mm pitch | | | |
| Mating Connector | | | |
| Vendor | WINWIN | | |
| Model No. | WATC-07DLPO2U | | |

7.4. SATA Power Output Wafer (CN8)

The 1x4-pin 2.0 mm pitch SATA power output wafer CN8 provides power to the SATA hard disk.

Figure 19: SATA Power Output Wafer CN8

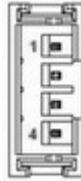


Table 25: Pin Assignment CN8

| Pin | Signal | Description | Note |
|----------------------------|------------------|--|----------|
| 1 | V _{HDD} | Power supply for HDD / SSD ▶ V _{HDD} = +12 V in case of V _{in} between 15 V and 36 V ▶ V _{HDD} = V _{in} - V _{DROP} (≤ +12 V) in case of V _{in} between 9 V and 15 V Depending on the SBC load, V _{DROP} (Voltage Drop) is approximately 1 V ~ 3 V. | 1 A max. |
| 2 | GND | Ground | |
| 3 | GND | Ground | |
| 4 | +5V | +5 V power supply for HDD / SSD | 1 A max. |
| Connector Type | | | |
| B2W, 1x4-pin, 2.0 mm pitch | | | |
| Mating Connector | | | |
| Vendor | Pinrex | | |
| Housing Model No. | 721-75-04W009 | | |
| Terminal Model No. | 721-70-T00009 | | |

7.5. USB Connectors (Internal) (CN17)

The 10-pin 2.0 mm pitch USB port pin header CN17 supports two USB 2.0 ports.

Figure 20: USB 2.0 Port 5, 6 Pin Header CN17

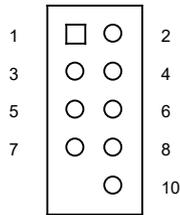


Table 26: Pin Assignment CN17

| Pin | Signal | Description | Note |
|----------------------------|---------------------|---|----------|
| 1 | +USBVCC* | 5 V supply. SB5V is supplied during power down to allow wakeup. | 1 A max. |
| 2 | +USBVCC* | 5 V supply. SB5V is supplied during power down to allow wakeup. | 1 A max. |
| 3 | USB_DA- | USB 2.0 differential pair (-) for channel A | |
| 4 | USB_DB- | USB 2.0 differential pair (-) for channel B | |
| 5 | USB_DA+ | USB 2.0 differential pair (+) for channel A | |
| 6 | USB_DB+ | USB 2.0 differential pair (+) for channel B | |
| 7 | GND | Ground | |
| 8 | GND | Ground | |
| 9 | KEY | | |
| 10 | GND | Ground | |
| Connector Type | | | |
| B2W, 2x5-pin, 2.0 mm pitch | | | |
| Mating Connector | | | |
| Vendor | Dupont | | |
| Housing Model No. | WL2004H-2*5P(DP2.0) | | |
| Terminal Model No. | KB931-21T1A | | |



* The power source of +USBVCC can be selected through JP6.

7.6. Audio AMP Output Wafer (CN1 & CN6)

The Speaker audio-out interface is available through the 2-pin 2.0 mm pitch wafers CN1 for left channel and CN6 for right channel. These outputs are shared with the audio output (Line-out) signals of the audio pin header CN7.

Figure 21: Audio AMP Output Wafer CN1 (Left Channel), CN6 (Right Channel)

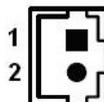
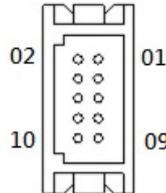


Table 27: Pin Assignment CN1, CN6

| Pin | Signal | Description | Note |
|----------------------------|---------------|--------------------|------|
| 1 | Speaker+ | Speaker output (+) | |
| 2 | Speaker- | Speaker output (-) | |
| Connector Type | | | |
| B2W, 1x2-pin, 2.0 mm pitch | | | |
| Mating Connector | | | |
| Vendor | Pinrex | | |
| Housing Model No. | 721-75-02W009 | | |
| Terminal Model No. | 721-70-T00009 | | |

7.7. Audio Input / Output Header (CN7)

The 10-pin 1.25 mm pitch audio input / output header CN7 provides audio output (Line-Out), audio input (Line-In) and microphone (Mic-In) signals. The audio output signals are shared with those of the speaker connectors CN1 & CN6.

Figure 22: Audio Input / Output Header CN7**Table 28: Pin Assignment CN7**

| Pin | Signal | Description | Note |
|-----------------------------|-----------------|---------------------------------------|------|
| 1 | MIC-In_L | Microphone input left channel signal | |
| 2 | MIC-In_R | Microphone input right channel signal | |
| 3 | MIC-In_JD# | Microphone jack detection | |
| 4 | Line-In_JD# | Audio input jack detection | |
| 5 | Line-In_L | Audio input left channel signal | |
| 6 | Line-In_R | Audio input right channel signal | |
| 7 | Line-Out_L | Audio output left channel signal | |
| 8 | Line-Out_R | Audio output right channel signal | |
| 9 | Line-Out_JD# | Audio output jack detection | |
| 10 | GND | Ground | |
| Connector Type | | | |
| B2W, 2x5-pin, 1.25 mm pitch | | | |
| Mating Connector | | | |
| Vendor | HRS | | |
| Housing Model No. | DF13-10DS-1.25C | | |
| Terminal Model No. | WL1255-T-T-S | | |

7.8. S/PDIF Output Wafer (CN2)

The 3-pin 1.25 mm pitch S/PDIF output wafer CN2 is used to enable a S/PDIF audio output port to carry multi-channel compressed surround sound.

Figure 23: S/PDIF Output Wafer CN2

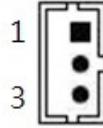


Table 29: Pin Assignment CN2

| Pin | Signal | Description | Note |
|-----------------------------|---------------|---------------|------|
| 1 | SPDIF-O | S/PDIF output | |
| 2 | +5V | 5 V supply | |
| 3 | GND | Ground | |
| Connector Type | | | |
| B2W, 1x3-pin, 1.25 mm pitch | | | |
| Mating Connector | | | |
| Vendor | Pinrex | | |
| Housing Model No. | 712-75-03W001 | | |
| Terminal Model No. | 712-70-T00001 | | |

7.9. Front Panel Header (FP1 & FP2)

The 8-pin 2.54 mm pitch front panel header FP1 supplies signals for the reset button, M.2 Key B SSD LED and system warning speaker.

The 10-pin 2.54 mm pitch front panel header FP2 supplies signals for the power button, power LED, and SM Bus.

Figure 24: Front Panel Header 1 FP1

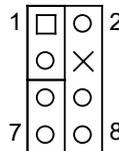


Table 30: Pin Assignment FP1

| Pin | Signal | Description | Note |
|-----|--------------------|---|------|
| 1 | Reset Button + | System reset button (+) | |
| 2 | Speaker + | External system warning speaker (+) | |
| 3 | Reset Button - | System reset button (-) | |
| 4 | - | No connection | |
| 5 | M2M_LED + | M.2 Key B SSD activity LED (+). The LED lights up or flashes when data is ready from or written to the SSD. | |
| 6 | Internal Speaker - | Internal system warning speaker (-) | |
| 7 | M2M_LED - | M.2 Key B SSD activity LED (-). | |
| 8 | Speaker - | External system warning speaker (-) | |

| Pin | Signal | Description | Note |
|-----------------------------|---------------|-------------|------|
| Connector Type | | | |
| B2W, 2x4-pin, 2.54 mm pitch | | | |
| Mating Connector | | | |
| Vendor | Pinrex | | |
| Housing Model No. | 741-75-204B01 | | |
| Terminal Model No. | 741-70-FT0001 | | |



Internal Buzzer is enabled when Pin 6-8 is shorted.

Figure 25: Front Panel Header 2 FP2

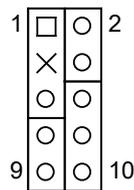


Table 31: Pin Assignment FP2

| Pin | Signal | Description | Note |
|-----------------------------|----------------|---|------|
| 1 | Power LED + | System Power LED (+). The LED lights up when users turn on the system power, and blinks when the system is in sleep mode. | |
| 2 | Power Button + | System power button (+). Pressing the power button turns the system on or puts the system in sleep or soft-off mode depending on the operating system settings. Pressing the power switch for more than four seconds while the system turns from ON to OFF. | |
| 3 | - | No connection | |
| 4 | Power Button - | System power button (-). | |
| 5 | Power LED - | System Power LED (-). | |
| 6 | SM_ALERT# | System Management Bus Alert | |
| 7 | BAT_LOW# | Battery low input. This signal may be driven low by external circuitry to signal that the system battery is low. It also can be used to signal some other external power management event. | |
| 8 | SMBus Data | System management bus bidirectional data line | |
| 9 | GND | Ground | |
| 10 | SMBus Clock | System management bus bidirectional clock line | |
| Connector Type | | | |
| B2W, 2x5-pin, 2.54 mm pitch | | | |
| Mating Connector | | | |
| Vendor | Pinrex | | |
| Housing Model No. | 741-75-205B01 | | |
| Terminal Model No. | 741-70-FT0001 | | |

7.10. Serial COM1, COM2, COM3 & COM4 Ports (CN25, CN24, CN28 & CN29)

The 10-pin 1.25 mm pitch serial COM wafers CN24, CN25, CN28 and CN29 provide RS232/422/485 connections. All wafers support single communication mode on RS485 with only half-duplex configuration. The wafers CN24 (COM2) and CN25 (COM1) support RS232 without hardware flow control.

Figure 26: Serial COM CN24, CN25, CN28, CN29

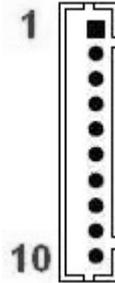


Table 32: Pin Assignment COM1 CN25, COM2 CN24

| Pin | RS232 Signal | RS422 Signal | RS485 Signal | Note |
|------------------------------|---------------|--------------|--------------|-------------|
| 1 | - | TX- | DATA- | |
| 2 | - | - | - | |
| 3 | RXD | TX+ | DATA+ | |
| 4 | - | - | - | |
| 5 | TXD | RX+ | - | |
| 6 | - | - | - | |
| 7 | - | RX- | - | |
| 8 | - | - | - | |
| 9 | GND | GND | GND | |
| 10 | +5V | +5V | +5V | 500 mA max. |
| Connector Type | | | | |
| B2W, 1x10-pin, 1.25 mm pitch | | | | |
| Mating Connector | | | | |
| Vendor | Pinrex | | | |
| Housing Model No. | 712-75-10W001 | | | |
| Terminal Model No. | 712-70-T00001 | | | |

Table 33: Pin Assignment COM3 CN28, COM4 CN29

| Pin | RS232 Signal | RS422 Signal | RS485 Signal | Note |
|-----|--------------|--------------|--------------|------|
| 1 | DCD | TX- | DATA- | |
| 2 | DSR | - | - | |
| 3 | RXD | TX+ | DATA+ | |
| 4 | RTS | - | - | |
| 5 | TXD | RX+ | - | |
| 6 | CTS | - | - | |
| 7 | DTR | RX- | - | |

| Pin | RS232 Signal | RS422 Signal | RS485 Signal | Note |
|------------------------------|---------------|--------------|--------------|-------------|
| 8 | RI | - | - | |
| 9 | GND | GND | GND | |
| 10 | +5V | +5V | +5V | 500 mA max. |
| Connector Type | | | | |
| B2W, 1x10-pin, 1.25 mm pitch | | | | |
| Mating Connector | | | | |
| Vendor | Pinrex | | | |
| Housing Model No. | 712-75-10W001 | | | |
| Terminal Model No. | 712-70-T00001 | | | |

Table 34: Signal Description

| Signal | Description |
|--------------|---|
| TXD | Transmitted Data, sends data to the communications link. The signal is set to the marking state (-12 V) on hardware reset when the transmitter is empty or when loop mode operation is initiated. |
| RXD | Received Data, receives data from the communications link. |
| DTR | Data Terminal Ready, indicates to the modem etc. that the on-board UART is ready to establish communication link. |
| DSR | Data Set Ready, indicates that the modem etc. is ready to establish a communications link. |
| RTS | Request To Send, indicates to the modem etc. that the on-board UART is ready to exchange data. |
| CTS | Clear To Send, indicates that the modem or data set is ready to exchange data. |
| DCD | Data Carrier Detect, indicates that the modem or data set has detected the data carrier. |
| RI | Ring Indicator, indicates that the modem has received a ringing signal from the telephone line. |
| TX+/- | Transmitted Data differential pair sends data to the communications link. |
| RX+/- | Received Data differential pair receives data from the communications link. |
| GND | Power Supply GND signal |

7.11. LVDS / eDP Combo Connector (CN26)

The 30-pole 1.0 mm pitch connector CN26 provides either 24-bit, 2-channel LVDS or eDP panel connection. The switch between LVDS mode and eDP mode can be configured in the BIOS settings.

Figure 27: LVDS / eDP Combo Connector CN26

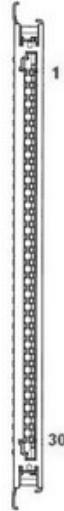


Table 35: Pin Assignment CN26

| Pin | Signal | | Description | | Note |
|-----|-------------|----------|----------------------------------|-----------------------------|------|
| | LVDS Mode | eDP Mode | LVDS Mode | eDP Mode | |
| 1 | LVDSA_TX0- | - | LVDS Ch. A Data 0 diff. pair (-) | - | |
| 2 | LVDSA_TX0+ | - | LVDS Ch. A Data 0 diff. pair (+) | - | |
| 3 | LVDSA_TX1- | eDP_TX1- | LVDS Ch. A Data 1 diff. pair (-) | eDP Lane 1 diff. pair (-) | |
| 4 | LVDSA_TX1+ | eDP_TX1+ | LVDS Ch. A Data 1 diff. pair (+) | eDP Lane 1 diff. pair (+) | |
| 5 | LVDSA_TX2- | eDP_TX0- | LVDS Ch. A Data 2 diff. pair (-) | eDP Lane 0 diff. pair (-) | |
| 6 | LVDSA_TX2+ | eDP_TX0+ | LVDS Ch. A Data 2 diff. pair (+) | eDP Lane 0 diff. pair (+) | |
| 7 | GND | | Ground | | |
| 8 | LVDSA_BCLK- | eDP_AUX- | LVDS Ch. A clock diff. pair (-) | eDP aux. ch. diff. pair (-) | |
| 9 | LVDSA_BCLK+ | eDP_AUX+ | LVDS Ch. A clock diff. pair (+) | eDP aux. ch. diff. pair (+) | |
| 10 | LVDSA_TX3- | - | LVDS Ch. A Data 3 diff. pair (-) | - | |
| 11 | LVDSA_TX3+ | - | LVDS Ch. A Data 3 diff. pair (+) | - | |
| 12 | LVDSB_TX0- | - | LVDS Ch. B Data 0 diff. pair (-) | - | |
| 13 | LVDSB_TX0+ | - | LVDS Ch. B Data 0 diff. pair (+) | - | |
| 14 | GND | | Ground | | |
| 15 | LVDSB_TX1- | - | LVDS Ch. B Data 1 diff. pair (-) | - | |
| 16 | LVDSB_TX1+ | - | LVDS Ch. B Data 1 diff. pair (+) | - | |
| 17 | GND | | Ground | | |
| 18 | LVDSB_TX2- | - | LVDS Ch. B Data 2 diff. pair (-) | - | |
| 19 | LVDSB_TX2+ | - | LVDS Ch. B Data 2 diff. pair (+) | - | |
| 20 | LVDSB_BCLK- | - | LVDS Ch. B clock diff. pair (-) | - | |
| 21 | LVDSB_BCLK+ | - | LVDS Ch. B clock diff. pair (+) | - | |

| Pin | Signal | | Description | | Note |
|-----------------------------|------------|----------|----------------------------------|-----------------------|-------------|
| | LVDS Mode | eDP Mode | LVDS Mode | eDP Mode | |
| 22 | LVDSB_TX3- | - | LVDS Ch. B Data 3 diff. pair (-) | - | |
| 23 | LVDSB_TX3+ | - | LVDS Ch. B Data 3 diff. pair (+) | - | |
| 24 | GND | | Ground | | |
| 25 | - | eDP_HPD | - | eDP hot plug detect | |
| 26 | VDDEN | VDDEN | Output display enable | Output display enable | |
| 27 | - | - | - | - | |
| 28 | +VPNL * | | +3.3 V / +5 V panel power supply | | 500 mA max. |
| 29 | +VPNL * | | +3.3 V / +5 V panel power supply | | 500 mA max. |
| 30 | +VPNL * | | +3.3 V / +5 V panel power supply | | 500 mA max. |
| Connector Type | | | | | |
| B2W, 1x30-pin, 1.0 mm pitch | | | | | |
| Mating Connector | | | | | |
| Vendor | JAE | | | | |
| Model No. | FI-X30HL | | | | |



* Panel Power can be selected through JP4.

7.12. LVDS / eDP Backlight Power Wafer (CN23)

The 7-pin 1.25 mm pitch wafer CN23 provides power supply for flat panel and its backlight inverter.

Figure 28: LVDS / eDP Backlight Power Wafer CN23

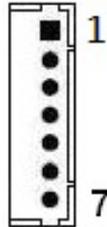


Table 36: Pin Assignment CN23

| Pin | Signal | Description | Note |
|-----|----------|--|-------------|
| 1 | BL_EN* | Backlight Enable signal | |
| 2 | GND | Ground | |
| 3 | +VBKLT** | Backlight power supply | 750 mA max. |
| 4 | +VBKLT** | <ul style="list-style-type: none"> ➤ +VBKLT = +5 V in case of backlight power selected as +5 V through JP2 ➤ +VBKLT = +12 V in case of backing power selected as +12 V / $V_{in} - V_{DROP}$ and V_{in} between 15 V and 36 V ➤ +VBKLT = $V_{in} - V_{DROP}$ ($\leq +12$ V) in case of backlight power selected as +12 V / $V_{in} - V_{DROP}$ and V_{in} between 9 V and 15 V Depending on the SBC load, V_{DROP} (Voltage Drop) is approximately 1 V ~ 3 V. | 750 mA max. |

| Pin | Signal | Description | Note |
|-----------------------------|---------------|--|------|
| 5 | GND | Ground | |
| 6 | NC | Non connection | |
| 7 | BL_ADJ_PWM | Backlight Adjustment PWM (Pulse Width Modulation) signal | |
| Connector Type | | | |
| B2W, 1x7-pin, 1.25 mm pitch | | | |
| Mating Connector | | | |
| Vendor | Pinrex | | |
| Housing Model No. | 712-75-07W001 | | |
| Terminal Model No. | 712-70-T00001 | | |



* BL_EN can be selected through JP2.



** Backlight Power can be selected through JP4.

7.13. LVDS / eDP Backlight Brightness Wafer (CN32)

The 3-pin 1.25 mm pitch wafer CN32 provides signals for backlight brightness level adjustment.

Figure 29: LVDS / eDP Backlight Brightness Wafer CN32

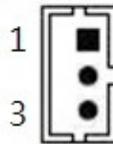


Table 37: Pin Assignment CN32

| Pin | Signal | Description | Note |
|-----------------------------|---------------|--|------|
| 1 | LVDS_BL_UP | Increase LVDS / eDP backlight brightness level | |
| 2 | LVDS_BL_DN | Decrease LVDS / eDP backlight brightness level | |
| 3 | GND | Ground | |
| Connector Type | | | |
| B2W, 1x3-pin, 1.25 mm pitch | | | |
| Mating Connector | | | |
| Vendor | Pinrex | | |
| Housing Model No. | 712-75-03W001 | | |
| Terminal Model No. | 712-70-T00001 | | |

7.14. Digital Input / Output Header (CN27)

The 10-pin 1.25 mm pitch header CN27 supports 8-bit digital input / output signals to provide powering-on function of the connected devices.

Figure 30: Digital Input / Output Header CN27

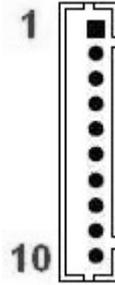


Table 38: Pin Assignment CN27

| Pin | Signal | Description | Note |
|------------------------------|---------------|----------------------------------|-------------|
| 1 | +5V | +5 V power supply | 500 mA max. |
| 2 | DIO_0 | Digital input / output channel 0 | |
| 3 | DIO_1 | Digital input / output channel 1 | |
| 4 | DIO_2 | Digital input / output channel 2 | |
| 5 | DIO_3 | Digital input / output channel 3 | |
| 6 | DIO_4 | Digital input / output channel 4 | |
| 7 | DIO_5 | Digital input / output channel 5 | |
| 8 | DIO_6 | Digital input / output channel 6 | |
| 9 | DIO_7 | Digital input / output channel 7 | |
| 10 | GND | Ground | |
| Connector Type | | | |
| B2W, 1x10-pin, 1.25 mm pitch | | | |
| Mating Connector | | | |
| Vendor | Pinrex | | |
| Housing Model No. | 712-75-10W001 | | |
| Terminal Model No. | 712-70-T00001 | | |

7.15. SPI 10-Pins Header (CN11)

The 10-pin 1.27 mm pitch header CN11 allows connection with a MCU (MicroController Unit) module for a particular application.

Figure 31: SPI 10-Pins Header CN11

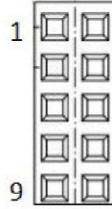


Table 39: Pin Assignment CN11

| Pin | Signal | Description | Note |
|-----------------------------|--------|------------------------------|------|
| 1 | VDD | Primary supply input | |
| 2 | GND | Ground | |
| 3 | CS1# | SPI slave chip select bit 1 | |
| 4 | CS0# | SPI slave chip select bit 0 | |
| 5 | HOLD# | SPI HOLD | |
| 6 | SO | SPI slave serial data output | |
| 7 | SCK | SPI clock input | |
| 8 | WP# | Write-protect pin | |
| 9 | SI | SPI slave serial data input | |
| 10 | EN | Enable pin | |
| Connector Type | | | |
| B2B, 2x5-pin, 1.27 mm pitch | | | |

7.16. M.2 Key B 2242 / 3042 / 3052 / 2280 Slot (M2B1)

The 3.5"-SBC-AML/ADN/AMH/ADH supports a M.2 module in format 2242 / 3042 / 3052 / 2280 with Key B. The M.2 specification supports PCIe x1 and USB 2.0 signals as well as UIM signals connected to SIM card wafer CN3. The slot can be used to integrate WWAN communication or other possible functions to the mainboard.

Figure 32: M.2 Key B 2242 / 3042 / 3052 / 2280 Slot M2B1

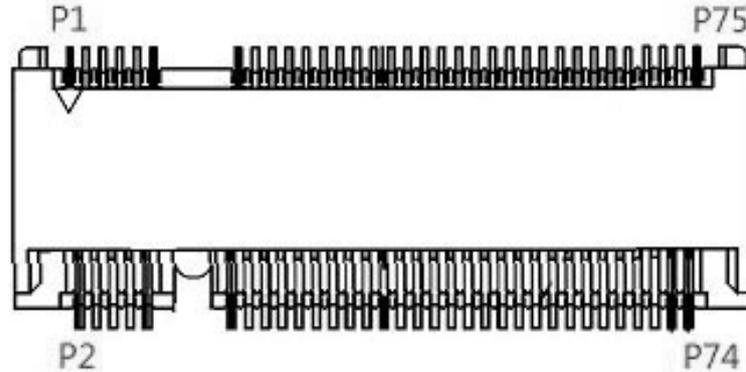


Table 40: Pin Assignment M2B1

| Pin | Signal | Description | Note |
|-----|----------|------------------------------------|------|
| 1 | - | | |
| 2 | +3.3V | 3.3 V power supply | |
| 3 | GND | Ground | |
| 4 | +3.3V | 3.3 V power supply | |
| 5 | GND | Ground | |
| 6 | PWROFF# | M.2 module power enable | |
| 7 | USB_D+ | USB 2.0 data differential pair (+) | |
| 8 | DISABLE# | Wireless disable | |
| 9 | USB_D- | USB 2.0 data differential pair (-) | |
| 10 | - | | |
| 11 | GND | Ground | |
| 12 | KEY | | |
| 13 | KEY | | |
| 14 | KEY | | |
| 15 | KEY | | |
| 16 | KEY | | |
| 17 | KEY | | |
| 18 | KEY | | |
| 19 | KEY | | |
| 20 | - | | |
| 21 | - | | |
| 22 | - | | |
| 23 | - | | |
| 24 | - | | |

| Pin | Signal | Description | Note |
|-----|------------|----------------------------------|------|
| 25 | - | | |
| 26 | - | | |
| 27 | GND | Ground | |
| 28 | - | | |
| 29 | - | | |
| 30 | UIM_RESET* | SIM card reset | |
| 31 | - | | |
| 32 | UIM_CLK* | SIM card clock | |
| 33 | GND | Ground | |
| 34 | UIM_DATA* | SIM card data | |
| 35 | - | | |
| 36 | UIM_PWR* | SIM card power | |
| 37 | - | | |
| 38 | - | | |
| 39 | GND | Ground | |
| 40 | - | | |
| 41 | PERn0 | PCIe Lane 0 receiver pair (-) | |
| 42 | - | | |
| 43 | PERp0 | PCIe Lane 0 receiver pair (+) | |
| 44 | - | | |
| 45 | GND | Ground | |
| 46 | - | | |
| 47 | PETn0 | PCIe Lane 0 transmitter pair (-) | |
| 48 | - | | |
| 49 | PETp0 | PCIe Lane 0 transmitter pair (+) | |
| 50 | PERST# | PCIe reset | |
| 51 | GND | Ground | |
| 52 | CLKREQ# | Reference clock request signal | |
| 53 | - | | |
| 54 | WAKE# | PCIe wake | |
| 55 | - | | |
| 56 | - | | |
| 57 | GND | Ground | |
| 58 | - | | |
| 59 | - | | |
| 60 | - | | |
| 61 | - | | |
| 62 | - | | |
| 63 | - | | |
| 64 | - | | |

| Pin | Signal | Description | Note |
|-----|------------|-------------------------------|------|
| 65 | - | | |
| 66 | SIM_DETECT | SIM card detect | |
| 67 | - | | |
| 68 | SUSCLK | 32.768 kHz clock supply input | |
| 69 | - | | |
| 70 | +3.3V | 3.3 V power supply | |
| 71 | GND | Ground | |
| 72 | +3.3V | 3.3 V power supply | |
| 73 | GND | Ground | |
| 74 | +3.3V | 3.3 V power supply | |
| 75 | - | | |



* These pins are connected to CN3 SIM card wafer directly.

7.17. M.2 Key E 2230 Slot (M2E1)

The 3.5"-SBC-AML/ADN/AMH/ADH supports a M.2 module in format 2230 with Key E. The M.2 specification supports PCIe x1, USB 2.0, UART, PCM and / or CNVi signals (variants with Intel® Atom® x7000RE Series processors do not support CNVi). The slot can be used to integrate WLAN (Wi-Fi or CNVi Wi-Fi) and / or Bluetooth communication or other possible function to the mainboard.

Figure 33: M.2 Key E 2230 Slot M2E1

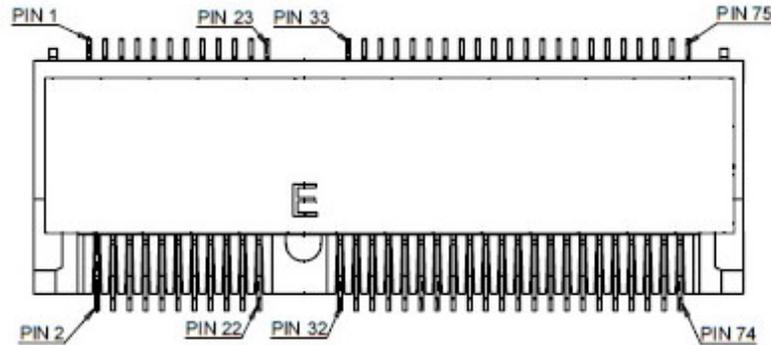


Table 41: Pin Assignment M2E1

| Pin | Key E* | | CNVi* | | Note |
|-----|------------|-----------------------------|----------|----------------------------|------|
| | Signal | Description | Signal | Description | |
| 1 | GND | Ground | GND | Ground | |
| 2 | +3.3V_SB | 3.3 V standby power supply | +3.3V_SB | 3.3 V standby power supply | |
| 3 | USB_D+ | USB 2.0 data diff. pair (+) | - | | |
| 4 | +3.3V_SB | 3.3 V standby power supply | +3.3V_SB | 3.3 V standby power supply | |
| 5 | USB_D- | USB 2.0 data diff. pair (-) | - | | |
| 6 | LED1# | Device active signal 1 | - | | |
| 7 | GND | Ground | GND | Ground | |
| 8 | PCM_CLK | PCM synchronous data clock | - | | |
| 9 | - | | WGR_D1N | CNVio bus Rx Lane 1 (-) | |
| 10 | PCM_SYNC | PCM synchronous data sync | LCP_RSTN | RF companion (CRF) reset | |
| 11 | - | | WGR_D1P | CNVio bus Rx Lane 1 (+) | |
| 12 | PCM_IN | PCM synchronous data input | - | | |
| 13 | GND | Ground | GND | Ground | |
| 14 | PCM_OUT | PCM synchronous data output | CLKREQ0 | Clock request | |
| 15 | - | | WGR_D0N | CNVio bus Rx Lane 0 (-) | |
| 16 | LED2# | Device active signal 2 | - | | |
| 17 | - | | WGR_D0P | CNVio bus Rx Lane 0 (+) | |
| 18 | GND | Ground | GND | Ground | |
| 19 | GND | Ground | GND | Ground | |
| 20 | UART_WAKE# | UART wake-up | - | | |
| 21 | - | | WGR_CLKN | CNVio bus Rx clock (-) | |
| 22 | UART_RX | UART data input | BRI_RSP | BRI bus Rx | |
| 23 | - | | WGR_CLKP | CNVio bus Rx clock (+) | |

| Pin | Key E* | | CNVi* | | Note |
|-----|-------------|--------------------------------|-------------|-------------------------------|------|
| | Signal | Description | Signal | Description | |
| 24 | Key | | Key | | |
| 25 | Key | | Key | | |
| 26 | Key | | Key | | |
| 27 | Key | | Key | | |
| 28 | Key | | Key | | |
| 29 | Key | | Key | | |
| 30 | Key | | Key | | |
| 31 | Key | | Key | | |
| 32 | UART_TX | UART data output | RGI_DT | RGI bus Tx | |
| 33 | GND | Ground | GND | Ground | |
| 34 | UART_CTS | UART clear to send | RGI_RSP | RGI bus Rx | |
| 35 | PET0+ | PCIe Lane 0 Tx pair (+) | - | | |
| 36 | UART_RTS | UART request to send | BRI_DT | BRI bus Tx | |
| 37 | PET0- | PCIe Lane 0 Tx pair (-) | - | | |
| 38 | Clink_RST | Wi-Fi CLINK host bus reset | - | | |
| 39 | GND | Ground | GND | Ground | |
| 40 | Clink_DATA | Wi-Fi CLINK host bus data | - | | |
| 41 | PER0+ | PCIe Lane 0 Rx pair (+) | - | | |
| 42 | Clink_CLK | Wi-Fi CLINK host bus clock | - | | |
| 43 | PER0- | PCIe Lane 0 Rx pair (-) | - | | |
| 44 | - | | - | | |
| 45 | GND | Ground | GND | Ground | |
| 46 | - | | - | | |
| 47 | REFCLK0+ | PCIe reference clock pair (+) | - | | |
| 48 | - | | - | | |
| 49 | REFCLK0- | PCIe reference clock pair (-) | - | | |
| 50 | SUSCLK | 32.768 kHz clock supply input | SUSCLK | 32.768 kHz clock supply input | |
| 51 | GND | Ground | GND | Ground | |
| 52 | PERST0# | PCIe reset | - | | |
| 53 | CLKREQ0# | Reference clock request signal | - | | |
| 54 | W_DISABLE2# | Wireless disable 2 | W_DISABLE2# | Wireless disable 2 | |
| 55 | PEWAKE0# | PCIe wake | - | | |
| 56 | W_DISABLE1# | Wireless disable 1 | W_DISABLE1# | Wireless disable 1 | |
| 57 | GND | Ground | GND | Ground | |
| 58 | - | | - | | |
| 59 | - | | WT_D1N | CNVio bus Tx Lane 1 (-) | |
| 60 | - | | - | | |
| 61 | - | | WT_D1P | CNVio bus Tx Lane 1 (+) | |
| 62 | - | | - | | |

| Pin | Key E* | | CNVi* | | Note |
|-----|----------|----------------------------|----------|----------------------------|------|
| | Signal | Description | Signal | Description | |
| 63 | GND | Ground | GND | Ground | |
| 64 | - | | - | | |
| 65 | - | | WT_D0N | CNVio bus Tx Lane 0 (-) | |
| 66 | PERSTO# | PCIe reset | - | | |
| 67 | - | | WT_D0P | CNVio bus Tx Lane 0 (+) | |
| 68 | - | | - | | |
| 69 | GND | Ground | GND | Ground | |
| 70 | - | | - | | |
| 71 | - | | WT_CLKN | CNVio bus Tx clock (-) | |
| 72 | +3.3V_SB | 3.3 V standby power supply | +3.3V_SB | 3.3 V standby power supply | |
| 73 | - | | WT_CLKP | CNVio bus Tx clock (+) | |
| 74 | +3.3V_SB | 3.3 V standby power supply | +3.3V_SB | 3.3 V standby power supply | |
| 75 | GND | Ground | GND | Ground | |



* The board will auto-detect the module type and re-configure itself to an appropriate mode.

7.18. M.2 Key M 2280 Slot (M2M1)

The 3.5"-SBC-AML/ADN/AMH/ADH supports a M.2 module in format 2280 with Key M. The M.2 specification supports either SATA 3.0 or PCIe x1 signal. The slot can be used to integrate either a M.2 SATA SSD or a M.2 PCIe SSD to the mainboard.

The default configuration is set to support SATA 3.0 signal. In case of the PCIe x1 signal required, it must be stipulated when ordering, as appropriate signal routing must be applied at the factory.

Figure 34: M.2 Key M 2280 Slot M2M1

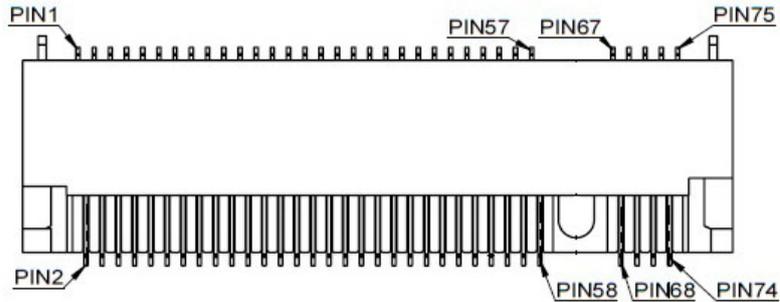


Table 42: Pin Assignment M2M1

| Pin | Signal | Description | Note |
|-----|--------------------|--|------|
| 1 | GND | Ground | |
| 2 | +3.3V | 3.3 V power supply | |
| 3 | GND | Ground | |
| 4 | +3.3V | 3.3 V power supply | |
| 5 | - | | |
| 6 | - | | |
| 7 | - | | |
| 8 | - | | |
| 9 | GND | Ground | |
| 10 | DAS / DSS# / LED1# | Device active signal / disable staggered spin-up / LED | |
| 11 | - | | |
| 12 | +3.3V | 3.3 V power supply | |
| 13 | - | | |
| 14 | +3.3V | 3.3 V power supply | |
| 15 | GND | Ground | |
| 16 | +3.3V | 3.3 V power supply | |
| 17 | - | | |
| 18 | +3.3V | 3.3 V power supply | |
| 19 | - | | |
| 20 | - | | |
| 21 | GND | Ground | |
| 22 | - | | |
| 23 | - | | |
| 24 | - | | |

| Pin | Signal | Description | Note |
|-----|-----------------|--|------|
| 25 | - | | |
| 26 | - | | |
| 27 | GND | Ground | |
| 28 | - | | |
| 29 | - | | |
| 30 | - | | |
| 31 | - | | |
| 32 | - | | |
| 33 | GND | Ground | |
| 34 | - | | |
| 35 | - | | |
| 36 | - | | |
| 37 | - | | |
| 38 | - | | |
| 39 | GND | Ground | |
| 40 | - | | |
| 41 | SATA_B+ / PERn0 | SATA receiver pair (+) / PCIe Lane 0 receiver pair (-) | |
| 42 | - | | |
| 43 | SATA_B- / PERp0 | SATA receiver pair (-) / PCIe Lane 0 receiver pair (+) | |
| 44 | - | | |
| 45 | GND | Ground | |
| 46 | - | | |
| 47 | SATA_A- / PETn0 | SATA transmitter pair (-) / PCIe Lane 0 transmitter pair (-) | |
| 48 | - | | |
| 49 | SATA_A+ / PETp0 | SATA transmitter pair (+) / PCIe Lane 0 transmitter pair (+) | |
| 50 | - / PERST# | Non connection / PCIe reset | |
| 51 | GND | Ground | |
| 52 | - / CLKREQ# | Non connection / Reference clock request signal | |
| 53 | REFCLKn | PCIe reference clock pair (-) | |
| 54 | - / PEWAKE# | - / PCIe wake | |
| 55 | REFCLKp | PCIe reference clock pair (+) | |
| 56 | - | | |
| 57 | GND | Ground | |
| 58 | - | | |
| 59 | Key | | |
| 60 | Key | | |
| 61 | Key | | |
| 62 | Key | | |
| 63 | Key | | |
| 64 | Key | | |

| Pin | Signal | Description | Note |
|-----|--------|-------------------------------|------|
| 65 | Key | | |
| 66 | Key | | |
| 67 | - | | |
| 68 | SUSCLK | 32.768 kHz clock supply input | |
| 69 | PEDET | PCIe detect | |
| 70 | +3.3V | 3.3 V power supply | |
| 71 | GND | Ground | |
| 72 | +3.3V | 3.3 V power supply | |
| 73 | GND | Ground | |
| 74 | +3.3V | 3.3 V power supply | |
| 75 | GND | Ground | |

7.19. SIM Card Wafer for M.2 Key B (CN3)

The SIM card wafer CN3 is intended to enable a SIM card holder to accommodate a SIM card and connected to UIM signals on the M.2 Key B slot M2B1.

Figure 35: SIM Card Wafer CN3



Table 43: Pin Assignment CN3

| Pin | Signal | Description | Note |
|-----|----------|---------------------------------|------|
| 1 | +UIM_PWR | Power +5 V or +3.3 V | |
| 2 | UIM_DATA | Input or output for serial data | |
| 3 | UIM_CLK | Clock signal | |
| 4 | UIM_RST | Reset signal | |
| 5 | UIM_CD | Card detect | |
| 6 | GND | Ground | |

7.20. 2.5 GbE LAN LED Header (CN30 & CN31)

The header CN30 is intended to connect 2.5 GbE LAN1 LED cable.

The header CN31 is intended to connect 2.5 GbE LAN2 LED cable.

Figure 36: 2.5 GbE LAN LED Header CN30, CN31

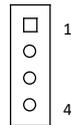


Table 44: Pin Assignment CN30, CN31

| Pin | Signal | Description | Note |
|----------------------------|--------------------------------|----------------------|--|
| 1 | ACT_LED+ | LAN activity LED (+) | Off – Link is down |
| 2 | ACT_LED- | LAN activity LED (-) | Flashing Yellow – Link is up and active Steady Yellow – Link is up, no activity |
| 3 | 2.5G_LINK_LED- / GbE_LINK_LED+ | LAN speed LED (+) | Orange – 1000 Mbit/s link established |
| 4 | 2.5G_LINK_LED+ / GbE_LINK_LED- | LAN speed LED (-) | Green – 2.5 Gbit/s link established Off – 10/100 Mbit/s link established |
| Connector Type | | | |
| B2W, 1x4-pin, 2.0 mm pitch | | | |

7.21. Board-to-board Connector (CN13)

The board-to-board connector CN13 provides connection to a daughter board for additional I/O port and / or feature expansion. The specification of the board-to-board connector supports PCIe x1, SM bus, I²C, UART and GSPI signals. It can an additional PCIe x1 and two USB 2.0 signal optionally by trading off PCIe x1 and USB 2.0 signals on M.2 Key B slot (M2B1) and USB 2.0 Port 3 & 4 Header (CN17) respectively.

Figure 37: Board-to-board Connector CN13

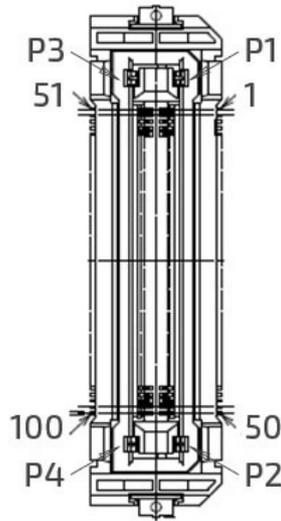


Table 45: Pin Assignment CN13

| Pin | Signal | Description | Note |
|-----|-------------|----------------------------|-------------|
| 1 | VCC_3V3_SBY | 3.3 V standby power output | 400 mA max. |
| 2 | VCC_3V3_SBY | 3.3 V standby power output | 400 mA max. |
| 3 | VCC_3V3_SBY | 3.3 V standby power output | 400 mA max. |
| 4 | VCC_3V3_SBY | 3.3 V standby power output | 400 mA max. |
| 5 | VCC_3V3_SBY | 3.3 V standby power output | 400 mA max. |
| 6 | GND | Ground | |
| 7 | - | - | |
| 8 | - | | |
| 9 | GND | Ground | |
| 10 | - | | |
| 11 | - | | |
| 12 | GND | Ground | |
| 13 | - | | |
| 14 | - | | |
| 15 | GND | Ground | |
| 16 | - | | |
| 17 | - | | |
| 18 | GND | Ground | |
| 19 | - | | |
| 20 | - | | |

| Pin | Signal | Description | Note |
|-----|--------------------|---|------|
| 21 | GND | Ground | |
| 22 | PCIE0_CLK_REF+ | PCIe Lane 0 clock reference pair (+) | |
| 23 | PCIE0_CLK_REF- | PCIe Lane 0 clock reference pair (-) | |
| 24 | GND | Ground | |
| 25 | PCIE0_TX+ | PCIe Lane 0 transmitter pair (+) | |
| 26 | PCIE0_TX- | PCIe Lane 0 transmitter pair (-) | |
| 27 | GND | Ground | |
| 28 | PCIE0_RX+ | PCIe Lane 0 receiver pair (+) | |
| 29 | PCIE0_RX- | PCIe Lane 0 receiver pair (-) | |
| 30 | GND | Ground | |
| 31 | PCIE2_TX+ | PCIe Lane 2 transmitter pair (+) | |
| 32 | PCIE2_TX- | PCIe Lane 2 transmitter pair (-) | |
| 33 | GND | Ground | |
| 34 | PCIE2_RX+ | PCIe Lane 2 receiver pair (+) | |
| 35 | PCIE2_RX- | PCIe Lane 2 receiver pair (-) | |
| 36 | GND | Ground | |
| 37 | USB0_D- (Reserved) | USB 2.0 differential pair (-) for channel 0 | |
| 38 | USB0_D+ (Reserved) | USB 2.0 differential pair (+) for channel 0 | |
| 39 | GND | Ground | |
| 40 | UART_TXD | UART transmitted data | |
| 41 | UART_RXD | UART received data | |
| 42 | UART_CTS# | UART clear to send | |
| 43 | UART_RTS# | UART request to send | |
| 44 | GND | Ground | |
| 45 | - | | |
| 46 | - | | |
| 47 | - | | |
| 48 | - | | |
| 49 | - | | |
| 50 | USB_OC# | Over current detect for USB | |
| 51 | GSPI_CLK | General SPI clock | |
| 52 | GSPI_MOSI | General SPI master output / slave input | |
| 53 | GSPI_MISO | General SPI master input / slave output | |
| 54 | GSPI_CS0# | General SPI chip select bit 0 | |
| 55 | GSPI_CS1# | General SPI chip select bit 1 | |
| 56 | GND | Ground | |
| 57 | - | | |
| 58 | - | | |
| 59 | GND | Ground | |

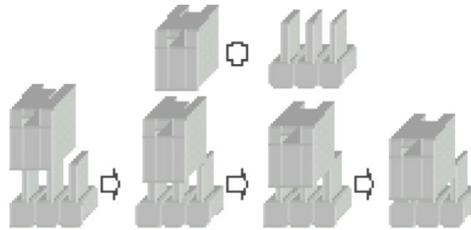
| Pin | Signal | Description | Note |
|-----|--------------------|---|------|
| 60 | - | | |
| 61 | - | | |
| 62 | GND | Ground | |
| 63 | - | | |
| 64 | - | | |
| 65 | GND | Ground | |
| 66 | - | | |
| 67 | - | | |
| 68 | GND | Ground | |
| 69 | - | | |
| 70 | - | | |
| 71 | GND | Ground | |
| 72 | PCIE1_CLK_REF+ | PCIe Lane 1 clock reference pair (+) | |
| 73 | PCIE1_CLK_REF- | PCIe Lane 1 clock reference pair (-) | |
| 74 | GND | Ground | |
| 75 | - | | |
| 76 | - | | |
| 77 | GND | Ground | |
| 78 | - | | |
| 79 | - | | |
| 80 | GND | Ground | |
| 81 | - | | |
| 82 | - | | |
| 83 | GND | Ground | |
| 84 | - | | |
| 85 | - | | |
| 86 | GND | Ground | |
| 87 | USB1_D- (Reserved) | USB 2.0 differential pair (-) for channel 1 | |
| 88 | USB1-D+ (Reserved) | USB 2.0 differential pair (+) for channel 1 | |
| 89 | GND | Ground | |
| 90 | I2C_CK | I2C clock | |
| 91 | I2C_DAT | I2C data | |
| 92 | SMB_CK | SM bus clock | |
| 93 | SMB_DAT | SM bus data | |
| 94 | GND | Ground | |
| 95 | SMB_ALERT# | SM bus alert | |
| 96 | WAKE# | PCIe wake | |
| 97 | PLTRST# | PCIe platform reset | |
| 98 | - | | |
| 99 | - | | |

| Pin | Signal | Description | Note |
|-----------------------------|-------------------|--|----------|
| 100 | PS_ON# | Power supply enable / disable | |
| P1 | VCC_5V_SBY | 5 V standby power output | 2 A max. |
| P2 | VCC_12V_IN_OUT | 12 V input (in case of power supplied from daughter board to SBC.) | 3 A max. |
| P3 | VCC_12V_IN_OUT | V _{B2B} output (in case of power supplied from SBC to daughter board.) | 3 A max. |
| P4 | VCC_12V_IN_OUT | <ul style="list-style-type: none"> ▶ V_{B2B} = +12 V in case of V_{in} between 15 V and 36 V ▶ V_{B2B} = V_{in} – V_{DROP} (≤ +12 V) in case of V_{in} between 9 V and 15 V Depending on the SBC load, V _{DROP} (Voltage Drop) is approximately 1 V ~ 3 V. | 3 A max. |
| Connector Type | | | |
| B2B, 2x50-pin, 0.5 mm pitch | | | |
| Mating Connector | | | |
| Vendor | HRS | | |
| Model No. | FX23-100P-0.5SV20 | | |

7.22. Switches and Jumpers

The product has several jumpers which must be properly configured to ensure correct operation.

Figure 38: Jumper Connector



For a three-pin jumper (see Figure 38), the jumper setting is designated “1-2” when the jumper connects pins 1 and 2. The jumper setting is designated “2-3” when pins 2 and 3 are connected and so on. You will see that one of the lines surrounding a jumper pin is thick, which indicates pin No.1.

To move a jumper from one position to another, use needle-nose pliers or tweezers to pull the pin cap off the pins and move it to the desired position.

7.22.1. LVDS / eDP Backlight Enable Selection (JP2)

The 2.0 mm patch "LVDS / eDP Backlight Enable Selection" jumper JP2 can be used to select the voltage level and the polarity of backlight enable signal.

Figure 39: LVDS / eDP Backlight Enable Selection JP2

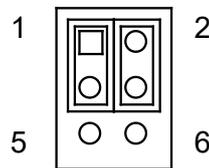


Table 46: Pin Assignment JP2

| Jumper 1 Position | | Description |
|-------------------|---------|------------------|
| Pin 1-3 | Pin 3-5 | |
| X | - | Voltage = +3.3 V |
| - | X | Voltage = +5 V |
| Jumper 2 Position | | Description |
| Pin 2-4 | Pin 4-6 | |
| X | - | High Active |
| - | X | Low Active |

“X” = Jumper set (short) and “-” = jumper not set (open)

7.22.2. AT / ATX Power Mode Selection (JP3)

The 2.0 mm pitch jumper JP3 can be used to select AT power mode or ATX power mode.

Figure 40: AT / ATX Power Mode Selection JP3

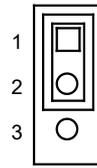


Table 47: Pin Assignment JP3

| Jumper 1 Position | | Description |
|-------------------|---------|--------------------------|
| Pin 1-2 | Pin 2-3 | |
| X | - | ATX Power Mode (Default) |
| - | X | AT Power Mode |

"X" = Jumper set (short) and "-" = jumper not set (open)

7.22.3. LVDS / eDP Backlight & Panel Power Selection (JP4)

The 2.54 mm pitch "LVDS / eDP Backlight & Panel Power Selection" jumper JP4 can be used to select LVDS / eDP backlight and panel power voltage.

The backlight power is +5 V when leaving the Jumper 1 in place on pins 3-5; while the backlight power is either +12 V or $V_{in} - V_{DROP} (\leq +12 V)$ depending on the DC input voltage from the power input wafer CN9 when leaving the Jumper 1 in place on pins 1-3.

Figure 41: LVDS / eDP Backlight & Panel Power Selection JP4

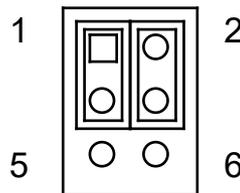


Table 48: Pin Assignment JP4

| Jumper 1 Position | | Description |
|-------------------|---------|--|
| Pin 1-3 | Pin 3-5 | |
| X | - | Backlight Power = +12 V / $V_{in} - V_{DROP} (\leq +12 V)$ (refer to Chapter 7.12, CN23) |
| - | X | Backlight Power = +5 V |
| Jumper 2 Position | | Description |
| Pin 2-4 | Pin 4-6 | |
| X | - | Panel Power = +3.3 V |
| - | X | Panel Power = +5 V |

"X" = Jumper set (short) and "-" = jumper not set (open)

7.22.4. Onboard DC-DC 12 V Selection (JP5)

The 2.0 mm pitch "Onboard DC-DC 12 V Selection" jumper JP5 can be used to enable or disable onboard DC-DC 12 V power supply. When enabled, the board is powered from the DC power input wafer CN9; when disabled, the board is powered from the daughter board via the 12 V power pins in board-to-board connector CN13.

Figure 42: Onboard DC-DC 12 V Selection JP5

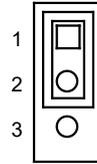


Table 49: Pin Assignment JP5

| Jumper 1 Position | | Description |
|-------------------|---------|--------------------|
| Pin 1-2 | Pin 2-3 | |
| X | - | DC-DC 12 V Enable |
| - | X | DC-DC 12 V Disable |

"X" = Jumper set (short) and "-" = jumper not set (open)

7.22.5. USB Power Selection (JP6)

The 2.0 mm pitch "USB Power Selection" jumper JP6 can be used to determine whether the USB ports are powered in the S4 / S5 state.

Figure 43: USB Power Selection JP6

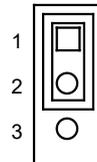


Table 50: Pin Assignment JP6

| Jumper 1 Position | | Description |
|-------------------|---------|-------------|
| Pin 1-2 | Pin 2-3 | |
| X | - | +5 V |
| - | X | +5 VSB |

"X" = Jumper set (short) and "-" = jumper not set (open)

7.22.6. Flash Descriptor Security Override Selection (JP7)

The 2.0 mm pitch "Flash Descriptor Security Override Selection" jumper JP7 can be used to specify whether to override the flash descriptor.

Figure 44: Flash Descriptor Security Override Selection JP7

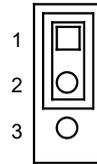


Table 51: Pin Assignment JP7

| Jumper 1 Position | | Description |
|-------------------|---------|--|
| Pin 1-2 | Pin 2-3 | |
| X | - | Controlled by EC (Embedded Controller) |
| - | X | Flash Security Override |

"X" = Jumper set (short) and "-" = jumper not set (open)

7.22.7. Clear CMOS Selection (JP8)

The 2.0 mm pitch "Clear CMOS Selection" jumper JP8 can be used to reset the Real Time Clock (RTC) and drain RTC well.

The jumper has one position: Pin 1-2 mounted (default position) and Pin 2-3 mounted. More information on setting the "Clear CMOS Selection" jumper can be found in the following table.

Figure 45: Clear CMOS Selection JP8

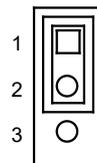


Table 52: Pin Assignment JP8

| Jumper 1 Position | | Description |
|-------------------|---------|---|
| Pin 1-2 | Pin 2-3 | |
| X | - | Normal Operation (default position) |
| - | X | Clear CMOS (board does not boot with the jumper in this position) |

"X" = Jumper set (short) and "-" = jumper not set (open)



Do not leave the jumper in position 2-3, otherwise if the power is disconnected, the battery will fully deplete within a few weeks.

8/BIOS

8.1. Starting the uEFI BIOS

The 3.5"-SBC-AML/ADN/AMH/ADH is provided with a Kontron-customized, pre-installed and configured version of AMI Aptio® V uEFI BIOS. AMI BIOS firmware is based on the Unified Extensible Firmware Interface (UEFI) specification and the Intel® Platform Innovation Framework for EFI. This uEFI BIOS provides a variety of new and enhanced functions specifically tailored to the hardware features of the 3.5"-SBC-AML/ADN/AMH/ADH.

The uEFI BIOS comes with a setup program that provides quick and easy access to the individual function settings for control or modification of the uEFI BIOS configuration. The setup program allows the accessing of various menus that provide functions or access to sub-menus with more specific functions of their own.

To start the uEFI BIOS setup program, follow the steps below:

1. Power on the board.
2. Wait until the first characters appear on the screen (POST messages or splash screen).
3. Press the key.
4. If the uEFI BIOS is password-protected, a request for password will appear. Enter either the User Password or the Supervisor Password (see Security menu), press <ENTER>, and proceed with step 5.
5. A setup menu will appear.

The 3.5"-SBC-AML/ADN/AMH/ADH uEFI BIOS setup program uses a hot key-based navigation system. A hot key legend bar is located on the bottom of the setup screens.

The following table provides information concerning the usage of these hot keys.

Table 53: Hotkeys Table

| Signal | Description |
|-------------|--|
| <F1> | The <F1> key invokes the General Help window. |
| <-> | The <Minus> key selects the next lower value within a field. |
| <+> | The <Plus> key selects the next higher value within a field. |
| <F2> | The <F2> key loads the previous values. |
| <F3> | The <F3> key loads the standard default values. |
| <F4> | The <F4> key saves the current settings and exit the uEFI BIOS setup. |
| <=> or <<=> | The <Left/Right> arrows select major setup menus on the menu bar. For example: Main, Advanced, Security, etc. |
| <↑> or <↓> | The <Up/Down> arrows select fields in the current menu. For example: A setup function or a sub-screen. |
| <ESC> | The <ESC> key exits a major setup menu and enter the Exit setup menu. Pressing the <ESC> key in a sub-menu displays the next higher menu level. |
| <ENTER> | The <ENTER> key executes a command or select a submenu. |

8.2. Starting the uEFI BIOS

The Setup utility feature shows six menus in the selection bar at the top of the screen:

- › Main
- › Advanced
- › Chipset
- › Security
- › Boot
- › Save & Exit

The Setup menus are selected via the left and right arrow keys. The currently active menu and the currently active uEFI BIOS Setup items are highlighted in white. Each Setup menu provides two main frames. The left frame displays all available functions. Functions that can be configured are displayed in blue. Functions displayed in gray provide information about the status or the operational configuration. The right frame displays an Item Specific Help window providing an explanation of the respective function.

8.2.1. Main Setup Menu

Upon entering the uEFI BIOS Setup program, the Main Setup menu is displayed. This screen lists the Main Setup menu sub-screens and provides basic system information. Additionally functions for setting the system time and date are offered.

Table 54: Main Setup Menu Sub-Screens and Functions

| Function | Description |
|-----------------------|---|
| Product Information | Read only field. Displays information about the product name |
| BIOS Information | Read only field. Displays information about the system BIOS |
| FSP Information | Read only field. Display information about the FSP |
| Processor Information | Read only field. Display information about the processor |
| Memory Information | Read only field. Displays information about the memory |
| PCH Information | Read only field. Display information about the PCH |
| ME Information | Read only field. Display information about Intel Management Engine (ME) firmware |
| System Language | Read only field. [English] only |
| Platform Information | Sub-screen to board information. |
| System Date | Set System Date |
| System Time | Set System Time |

Figure 46: BIOS Main Menu Screen System Data and Time

| Aptio Setup – AMI | | | | | |
|------------------------------|-----------------------------------|---------|----------|------|-------------|
| Main | Advanced | Chipset | Security | Boot | Save & Exit |
| Product Information | | | | | |
| Product Name | 3.5-SBC-ADN_AML (3.5-SBC-ADH_AMH) | | | | |
| BIOS Information | | | | | |
| BIOS Vendor | American Megatrends | | | | |
| Core Version | 5.27 | | | | |
| Compliance | UEFI 2.8; PI 1.7 | | | | |
| Kontron BIOS Version | ADNUEXR.100 (x64) | | | | |
| Access Level | Administrator | | | | |
| Hide Default CRB Setup Items | [Disabled] | | | | |
| FSP Information | | | | | |
| FSP Version | 0C.02.89.40 | | | | |
| RC Version | 0C.E0.89.40 | | | | |
| Build Date | | | | | |
| FSP Mode | Dispatch Mode | | | | |
| Board Information | | | | | |
| Board Name | 3.5-SBC-ADN_AML (3.5-SBC-ADH_AMH) | | | | |
| Board ID | N/A | | | | |
| Fab ID | Default string | | | | |
| LAN PHY Revision | N/A | | | | |
| Processor Information | | | | | |
| Name | Alder Lake ULX | | | | |
| Type | Intel® Atom® x7433RE | | | | |
| Speed | 1500 MHz | | | | |
| ID | 0xB06E0 | | | | |
| Stepping | A0 | | | | |
| Package | Not Implemented Yet | | | | |
| Number of Efficient-cores | 4 Core(s) / 4 Thread(s) | | | | |
| Microcode Revision | 17 | | | | |
| GT Info | 0x46D0 | | | | |
| eDRAM Size | N/A | | | | |
| IGFX GOP Version | 21.0.1063 | | | | |
| Memory RC Version | 0.0.4.74 | | | | |
| Total Memory | 16384 MB | | | | |

| Aptio Setup – AMI | | | | | |
|--|----------|---------------------|----------|------|------------------------|
| Main | Advanced | Chipset | Security | Boot | Save & Exit |
| Memory Frequency | | 4800 MHz | | | |
| PCH Information | | | | | |
| Name | | PCH-N | | | |
| PCH SKU | | N ASL IOT INDU SKU | | | |
| Stepping | | A0 | | | |
| Chipset Init Base Revision | | 4 | | | |
| Chipset Init OEM Revision | | 0 | | | |
| Package | | Not Implemented Yet | | | |
| TXT Capability of Platform / PCH | | Unsupported | | | |
| Production Type | | Production | | | |
| Dual Output Fast Read support | | Supported | | | |
| Read ID / Status Clock Freq | | 50 MHz | | | |
| Write and Erase Clock Freq | | 50 MHz | | | |
| Fast Read Clock Freq | | 50 MHz | | | |
| Fast Read support | | Supported | | | |
| Number of Components | | 1 Component | | | |
| SPI Component 0 Density | | 32 MB | | | |
| eSPI Flash Sharing Mode | | G3 | | | |
| EC PECI Mode | | Legacy PECI mode | | | |
| ME FW Version | | 16.50.12.1453 | | | → ←: Select Screen |
| ME Firmware SKU | | Consumer SKU | | | ↑ ↓: Select Item |
| PMC FW Version | | 160.50.0.1010 | | | Enter: Select |
| | | | | | +/-: Change Opt. |
| System Language | | [English] | | | F1: General Help |
| > Platform Information | | | | | F2: Previous Values |
| | | | | | F3: Optimized Defaults |
| System Date | | [Tue 03/25/2025] | | | F4: Save & Exit |
| System Time | | [15:52:06] | | | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | | | | |

| Feature | Option | Description |
|------------------------------|--------------------------|--|
| Hide Default CRB Setup Items | [Disabled], [Enabled] | For RD Test Only!! |
| System Date | [dd/mm/yyyy] | Set the Date. Use Tab to switch between Data elements. |
| System Time | [hh:mm:ss] | Set the Time. Use Tab to switch between Time elements. |

Figure 47: BIOS Main Menu Screen – Platform Information

| Aptio Setup – AMI | | | |
|--|--------------------------------------|--|--|
| Main | | | |
| Product Information | | | |
| Product Name | 3.5-SBC-ADN_AML (3.5-SBC-ADH_AMH) | | |
| Serial # | Default string | | |
| UUID | 00020003-0004-0005-0006-000700080009 | | |
| KSC Information | | | |
| Controller | KSC Main Controller | | |
| Operating Mode | Normal | | |
| Board Name | 3.5-SBC-ADN | | |
| Platform ID | 000A | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit | |
| KSC SW Spec. Version | 1.20 | | |
| BIOS Protocol Version | 2.3.1 | | |
| BIOS SW Spec. Version | 1.18 | | |
| Core Firmware Version | 1.4.0 RC 1 | | |
| Board Firmware Version | 1.0.0 RC 1 | | |
| SCM Info | F2-3A-5A-93 | | |
| Boot Counter | N/A | | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | | |

8.2.2. Advanced Setup Menu

The Advanced setup menu provides sub-screens and functions for advanced configurations.

NOTICE

Setting items on this screen to incorrect values may cause the system to malfunction.

The following sub-screen functions are included in the menu:

- › cTDP, IBCECC, Audio, Compliance Test & Power Configuration
- › RC ACPI Settings
- › Connectivity Configuration
- › CPU Configuration
- › Power & Performance
- › Display Configuration
- › PCH-FW Configuration
- › Thermal Configuration
- › Platform Settings
- › ACPI D3Cold Settings
- › BCLK Configuration
- › Intel® Time Coordinated Computing
- › Functional Safety Configuration
- › Debug Settings
- › Debug Configuration
- › Trusted Computing
- › ACPI Settings
- › Miscellaneous
- › SMART Settings
- › H/W Monitor
- › S5 RTC Wake Settings
- › UEFI Variables Protection
- › Serial Port Console Redirection
- › AMI Graphic Output Protocol Policy
- › SIO Common Settings
- › SIO Configuration
- › PCI Subsystem Settings
- › USB Configuration
- › Network Stack Configuration
- › CSM Configuration
- › NVMe Configuration
- › SDIO Configuration
- › CH7513A Configurations
- › F81435 Configurations
- › Tls Auth Configuration
- › RAM Disk Configuration

- Intel® Ethernet Controller I226-IT – C0:EA:C3:D1:D1:0E
- Intel® Ethernet Controller I226-IT – C0:EA:C3:D1:D1:0E
- Driver Health

Figure 48: BIOS Advanced Menu

| Aptio Setup – AMI | | | | | |
|--------------------------------------|----------|---------|--------------|------|-------------|
| Main | Advanced | Chipset | Security | Boot | Save & Exit |
| Configurable TDP Mode | | | [15W] | | |
| In-Band ECC Support | | | [Disabled] | | |
| Compliance Test Mode | | | [Disabled] | | |
| HD Audio | | | [Enabled] | | |
| Power Mode Selection | | | [ATX Mode] | | |
| Restore AC Power Loss | | | [Last State] | | |
| Power Saving Mode | | | [Enabled] | | |
| > RC ACPI Settings | | | | | |
| > Connectivity Configuration | | | | | |
| > CPU Configuration | | | | | |
| > Power & Performance | | | | | |
| > Display Configuration | | | | | |
| > PCH-FW Configuration | | | | | |
| > Thermal Configuration | | | | | |
| > Platform Settings | | | | | |
| > ACPI D3Cold Settings | | | | | |
| > BCLK Configuration | | | | | |
| > Intel® Time Coordinated Computing | | | | | |
| > Functional Safety Configuration | | | | | |
| > Debug Settings | | | | | |
| > Debug Configuration | | | | | |
| > Trusted Computing | | | | | |
| > ACPI Settings | | | | | |
| > Miscellaneous | | | | | |
| > SMART Settings | | | | | |
| > H/W Monitor | | | | | |
| > S5 RTC Wake Settings | | | | | |
| > UEFI Variables Protection | | | | | |
| > Serial Port Console Redirection | | | | | |
| > AMI Graphic Output Protocol Policy | | | | | |
| > SIO Common Setting | | | | | |
| > SIO Configuration | | | | | |
| > PCI Subsystem Settings | | | | | |
| > USB Configuration | | | | | |
| > Network Stack Configuration | | | | | |

| Aptio Setup – AMI | | | | | |
|---|----------|---------|----------|---|-------------|
| Main | Advanced | Chipset | Security | Boot | Save & Exit |
| > CSM Configuration > NVMe Configuration > SDIO Configuration > CH7513A Configurations > F81435 Configurations > TIs Auth Configuration > RAM Disk Configuration > Intel® Ethernet Controller I226-IT – C0:EA:C3:D1:D1:0E > Intel® Ethernet Controller I226-IT – C0:EA:C3:D1:D1:0E > Driver Health | | | | → ←: Select Screen ↑ ↓ : Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | | | | |

| Feature | Option | Description |
|-----------------------|------------------------------|--|
| Configurable TDP Mode | [15W], [Deactivate] | Configurable Processor Base Power (cTDP) Mode as 15W (Nominal) / 9W (Level 1) / Deactivate TDP selection. Deactivate option will set MSR to Nominal and MMIO to Zero. This option is only available for CPU i3 SKUs. |
| In-Band ECC Support | [Disabled], [Enabled] | Enable / Disable In-Band ECC. Will be enabled if memory has symmetric configuration |
| Compliance Test Mode | [Disabled], [Enabled] | Enable when using Compliance Load Board |
| HD Audio | [Disabled], [Enabled] | Control Detection of the HD-Audio device. [Disabled] = HDA will be unconditionally disabled. [Enabled] = HDA will be unconditionally enabled. |
| Power Mode Selection | [ATX mode] | Read only item. |
| Restore AC Power Loss | [Power Off], [Last State] | Choose options for restoring AC power loss |
| Power Saving Mode | [Disabled], [Enabled] | Enable / Disable power saving mode |

Figure 49: BIOS Advanced Menu – RC ACPI Settings

| Aptio Setup – AMI | | |
|--|--------------|--|
| Advanced | | |
| RC ACPI Settings | | |
| PTID Support | [Enabled] | |
| PECI Access Method | [Direct I/O] | |
| Native PCIE Enable | [Enabled] | |
| Native ASPM | [Auto] | |
| BDAT ACPI Table Support | [Disabled] | |
| ACPI Debug | [Disabled] | |
| D3 Setting for Storage | [D3Hot] | |
| Low Power S0 Idle Capability | [Enabled] | |
| PUIS Enable | [Disabled] | |
| EC Notification | [Enabled] | |
| EC CS Debug Light | [Disabled] | |
| EC Low Power Mode | [Enabled] | |
| Sensor Standby | [Disabled] | |
| CS PL1 Limit | [Disabled] | |
| > PEP Constraints Configuration | | |
| LPIT Residency Counter | [SLP S0] | |
| PCI Delay Optimization | [Disabled] | |
| MSI enabled | [Enabled] | |
| | | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|--------------------|-------------------------------------|---|
| PTID Support | [Disabled], [Enabled] | PTID Support will be loaded if enabled. |
| PECI Access Method | [Direct I/O], [ACPI] | PECI Access Method is Direct I/O or ACPI. |
| Native PCIE Enable | [Disabled], [Enabled] | Bit – PCIe Native * control 0 - ~ Hot Plug 1 – SHPC Native Hot Plug control 2 - ~ Power Management Events 3 – PCIe Advanced Error Reporting control 4 – PCIe Capability Structure control 5 – Latency Tolerance Reporting control |
| Native ASPM | [Auto], [Enabled], [Disabled] | [Enabled]: OS Controlled ASPM [Disabled]: BIOS Controlled ASPM |

| Feature | Option | Description |
|------------------------------|--------------------------|--|
| BDAT ACPI Table Support | [Disabled], [Enabled] | Enables support for the BDAT ACPI table. |
| ACPI Debug | [Disabled], [Enabled] | Open a memory buffer for storing debug strings. Reenter SETUP after enabling to see the buffer address. Use method ADBG to write strings to buffer. |
| D3 Setting for Storage | [Disabled], [D3Hot] | RTD3 support for storage. PCIE storage PEP constraint needs to be set as D0/F1 (Intel Advanced → ACPI Settings → PEP PCle Storage) when this setup is disabled / D3Hot. |
| Low Power S0 Idle Capability | [Disabled], [Enabled] | This variable determines if we enable ACPI Lower Power S0 Idle Capability (Mutually exclusive with Smart connect). While this is enabled, it also disables 8254 timer for SLP_S0 support. |
| PUIS Enable | [Enabled], [Disabled] | Enable / Disable Power-Up In Standby (PUIS) feature set allows devices to be powered-up into the Standby power management state to minimize inrush current at power-up and to allow the host to sequence the spin-up of devices. |
| EC Notification | [Disabled], [Enabled] | Sends EC notification of Low Power S0 Idle State |
| EC CS Debug Light | [Disabled], [Enabled] | When EC enters Low Power S0 Idle State, the CAPS LOCK light will be turned on |
| EC Low Power Mode | [Disabled], [Enabled] | This option controls whether EC will go to low power mode during Low Power S0 Idle State |
| Sensor Standby | [Disabled], [Enabled] | Enable / Disable Sensor standby mode |
| CS PL1 Limit | [Disabled], [Enabled] | Limit PL1 (Power Limit 1) while in Connected Standby |
| LPIT Residency Counter | [C10], [SLP S0] | Select Residency Counter |
| PCI Delay Optimization | [Disabled], [Enabled] | Experimental ACPI additions for FW latency optimizations |
| MSI enabled | [Disabled], [Enabled] | When disabled, MSI support is disabled in FADT |

Figure 50: BIOS Advanced Menu – RC ACPI Settings – PEP Constraints Configuration

| Aptio Setup – AMI | | |
|--|-----------------|--|
| Advanced | | |
| PEP Constraints Configuration | | |
| PEP CPU | [Enabled] | |
| PEP Graphics | [Enabled] | |
| PEP IPU | [Enabled] | |
| PEP GNA | [Enabled] | |
| PEP SATA | [Adapter D3] | |
| PEP enumerated SATA ports | [Disabled] | |
| PEP PCIe Storage | [D0/F1] | |
| PEP PCIe LAN | [D0/F1] | |
| PEP PCIe WLAN | [D0/F1] | |
| PEP PCIe GFX | [D0/F1] | |
| PEP PCIe Other | [No Constraint] | |
| PEP UART | [Enabled] | |
| PEP I2C0 | [Enabled] | |
| PEP I2C1 | [Enabled] | |
| PEP I2C2 | [Enabled] | |
| PEP I2C3 | [Enabled] | |
| PEP I2C4 | [Enabled] | |
| PEP I2C5 | [Enabled] | |
| PEP I2C6 | [Enabled] | |
| PEP I2C7 | [Enabled] | |
| PEP SPI | [Enabled] | |
| PEP XHCI | [Enabled] | |
| PEP Audio | [D0/F1] | |
| PEP CSME | [Enabled] | |
| PEP HECI3 | [Enabled] | |
| PEP THC0 | [Enabled] | |
| PEP THC1 | [Enabled] | |
| PEP UPS0 | [Enabled] | |
| PEP UFS1 | [Enabled] | |
| PEP TCSS | [Enabled] | |
| | | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|--------------|--------------------------|--------------------------------|
| PEP CPU | [Disabled], [Enabled] | Add CPU in PEP mitigation list |
| PEP Graphics | [Disabled], [Enabled] | Add Gfx in PEP mitigation list |

| Feature | Option | Description |
|---------------------------|--|--|
| PEP IPU | [Disabled], [Enabled] | Add IPU in PEP mitigation list |
| PEP GNA | [Disabled], [Enabled] | Add GNA in PEP mitigation list |
| PEP SATA | [No Constraint], [Adapter D0/F1], [Raid Volume 0], [Adapter D3] | Add Storage device in PEP mitigation list |
| PEP enumerated SATA ports | [Disabled], [Enabled] | Add enumerated SATA ports in PEP Constraint list |
| PEP PCIe Storage | [No Constraint], [D0/F1], [D3] | Add PCIe root ports (storage) in PEP mitigation list |
| PEP PCIe LAN | [No Constraint], [D0/F1], [D3] | Add PCIe root ports (LAN) in PEP mitigation list |
| PEP PCIe WLAN | [No Constraint], [D0/F1], [D3] | Add PCIe root ports (WLAN) in PEP mitigation list |
| PEP PCIe GFX | [No Constraint], [D0/F1], [D3] | Add PCIe root ports (GFX) in PEP mitigation list |
| PEP PCIe Other | [No Constraint], [D0/F1], [D3] | Add PCIe root ports (Other) in PEP mitigation list |
| PEP UART | [Disabled], [Enabled] | Add UART in PEP mitigation list |
| PEP I2CO..7 | [Enabled] | Read only item |
| PEP SPI | [Disabled], [Enabled] | Add SPI in PEP mitigation list |
| PEP XHCI | [Disabled], [Enabled] | Add XHCI in PEP mitigation list |
| PEP Audio | [No Constraint], [D0/F1], [D3] | Add Audio in PEP mitigation list |
| PEP CSME | [Disabled], [Enabled] | Add CSME in PEP mitigation list |
| PEP HECI3 | [Disabled], [Enabled] | Add HECI3 in PEP mitigation list |
| PEP THC0/1 | [Disabled], [Enabled] | Add THC in PEP mitigation list. Applies only if THCx has assigned port. |
| PEP UFS0/1 | [Disabled], [Enabled] | Add UFSx IPs in PEP mitigation list |

| Feature | Option | Description |
|----------|--------------------------|-------------------------------------|
| PEP TCSS | [Disabled], [Enabled] | Add TCSS IPs in PEP mitigation list |

Figure 51: BIOS Advanced Menu – Connectivity Configuration

| Aptio Setup – AMI | |
|---------------------------------------|------------------|
| Advanced | |
| CNVi CRF Present | |
| CNVi Configuration | |
| CNVi Mode | [Auto Detection] |
| Wi-Fi Core* | [Enabled] |
| BT Core* | [Enabled] |
| BT Audio Offload* | [Enabled] |
| BT RF-Kill Delay Time* | 0 |
| RFI Mitigation | [Enabled] |
| CoExistence Manager | [Disabled] |
| Discrete Bluetooth Interface | [USB] |
| BT Interrupt Mode** | [GPIO Interrupt] |
| BT Tile Mode | [Disabled] |
| Advanced settings | [Disabled] |
| Switched Antenna Diversity Selection# | [Diversity] |
| SPLC# | |
| Domain Type SPLC 1# | 7 |
| Default Power Limit# | 65535 |
| Default Time Window# | 30000 |
| WAND# | |
| TRxDelay_A# | 50 |
| TRxCableLength_A# | 50 |
| TRxDelay_B# | 50 |
| TRxCableLength_B# | 50 |
| WRDD Package 1# | |
| Domain Type# | 7 |
| Country Identifier# | 16720 |
| 11Ax Control# | |
| 11Ax Setting for Ukraine# | [Disabled] |
| 11Ax Mode for Ukraine# | [Disabled] |
| 11Ax Setting for Russia# | [Disabled] |
| 11Ax Mode for Russia# | [Disabled] |
| WRDS Package# | |
| WiFi SAR# | [Disabled] |
| SAR 2400 MHz Set1 Chain A# | 0 |
| SAR 5150-5350 MHz Set1 Chain A# | 0 |
| SAR 5350-5470 MHz Set1 Chain A# | 0 |

| Aptio Setup – AMI | | |
|-------------------------------------|---|--|
| Advanced | | |
| SAR 5470-5725 MHz Set1 Chain A# | 0 | |
| SAR 5725-5925 MHz Set1 Chain A# | 0 | |
| SAR 5945-6165 MHz Set1 Chain A# | 0 | |
| SAR 6165-6405 MHz Set1 Chain A# | 0 | |
| SAR 6405-6525 MHz Set1 Chain A# | 0 | |
| SAR 6525-6705 MHz Set1 Chain A# | 0 | |
| SAR 6705-6865 MHz Set1 Chain A# | 0 | |
| SAR 6865-7105 MHz Set1 Chain A# | 0 | |
| SAR 2400 MHz Set1 Chain B# | 0 | |
| SAR 5150-5350 MHz Set1 Chain B# | 0 | |
| SAR 5350-5470 MHz Set1 Chain B# | 0 | |
| SAR 5470-5725 MHz Set1 Chain B# | 0 | |
| SAR 5725-5925 MHz Set1 Chain B# | 0 | |
| SAR 5945-6165 MHz Set1 Chain B# | 0 | |
| SAR 6165-6405 MHz Set1 Chain B# | 0 | |
| SAR 6405-6525 MHz Set1 Chain B# | 0 | |
| SAR 6525-6705 MHz Set1 Chain B# | 0 | |
| SAR 6705-6865 MHz Set1 Chain B# | 0 | |
| SAR 6865-7105 MHz Set1 Chain B# | 0 | |
| SAR CDB 2400 MHz Set1 Chain A# | 0 | |
| SAR CDB 5150-5350 MHz Set1 Chain A# | 0 | |
| SAR CDB 5350-5470 MHz Set1 Chain A# | 0 | |
| SAR CDB 5470-5725 MHz Set1 Chain A# | 0 | |
| SAR CDB 5725-5925 MHz Set1 Chain A# | 0 | |
| SAR CDB 5945-6165 MHz Set1 Chain A# | 0 | |
| SAR CDB 6165-6405 MHz Set1 Chain A# | 0 | |
| SAR CDB 6405-6525 MHz Set1 Chain A# | 0 | |
| SAR CDB 6525-6705 MHz Set1 Chain A# | 0 | |
| SAR CDB 6705-6865 MHz Set1 Chain A# | 0 | |
| SAR CDB 6865-7105 MHz Set1 Chain A# | 0 | |
| SAR CDB 2400 MHz Set1 Chain B# | 0 | |
| SAR CDB 5150-5350 MHz Set1 Chain B# | 0 | |
| SAR CDB 5350-5470 MHz Set1 Chain B# | 0 | |
| SAR CDB 5470-5725 MHz Set1 Chain B# | 0 | |
| SAR CDB 5725-5925 MHz Set1 Chain B# | 0 | |
| SAR CDB 5945-6165 MHz Set1 Chain B# | 0 | |
| SAR CDB 6165-6405 MHz Set1 Chain B# | 0 | |
| SAR CDB 6405-6525 MHz Set1 Chain B# | 0 | |
| SAR CDB 6525-6705 MHz Set1 Chain B# | 0 | |
| SAR CDB 6705-6865 MHz Set1 Chain B# | 0 | |

| Aptio Setup – AMI | |
|---|----------------------|
| Advanced | |
| SAR CDB 6865-7105 MHz Set1 Chain B [#] | 0 |
| EWRD Package [#] | |
| WiFi Dynamic SAR [#] | [Disabled] |
| Extended SAR Range Sets [#] | [No Additional sets] |
| SAR 2400 MHz Set2 Chain A [#] | 0 |
| SAR 5150-5350 MHz Set2 Chain A [#] | 0 |
| SAR 5350-5470 MHz Set2 Chain A [#] | 0 |
| SAR 5470-5725 MHz Set2 Chain A [#] | 0 |
| SAR 5725-5925 MHz Set2 Chain A [#] | 0 |
| SAR 5945-6165 MHz Set2 Chain A [#] | 0 |
| SAR 6165-6405 MHz Set2 Chain A [#] | 0 |
| SAR 6405-6525 MHz Set2 Chain A [#] | 0 |
| SAR 6525-6705 MHz Set2 Chain A [#] | 0 |
| SAR 6705-6865 MHz Set2 Chain A [#] | 0 |
| SAR 6865-7105 MHz Set2 Chain A [#] | 0 |
| SAR 2400 MHz Set2 Chain B [#] | 0 |
| SAR 5150-5350 MHz Set2 Chain B [#] | 0 |
| SAR 5350-5470 MHz Set2 Chain B [#] | 0 |
| SAR 5470-5725 MHz Set2 Chain B [#] | 0 |
| SAR 5725-5925 MHz Set2 Chain B [#] | 0 |
| SAR 5945-6165 MHz Set2 Chain B [#] | 0 |
| SAR 6165-6405 MHz Set2 Chain B [#] | 0 |
| SAR 6405-6525 MHz Set2 Chain B [#] | 0 |
| SAR 6525-6705 MHz Set2 Chain B [#] | 0 |
| SAR 6705-6865 MHz Set2 Chain B [#] | 0 |
| SAR 6865-7105 MHz Set2 Chain B [#] | 0 |
| SAR 2400 MHz Set3 Chain A [#] | 0 |
| SAR 5150-5350 MHz Set3 Chain A [#] | 0 |
| SAR 5350-5470 MHz Set3 Chain A [#] | 0 |
| SAR 5470-5725 MHz Set3 Chain A [#] | 0 |
| SAR 5725-5925 MHz Set3 Chain A [#] | 0 |
| SAR 5945-6165 MHz Set3 Chain A [#] | 0 |
| SAR 6165-6405 MHz Set3 Chain A [#] | 0 |
| SAR 6405-6525 MHz Set3 Chain A [#] | 0 |
| SAR 6525-6705 MHz Set3 Chain A [#] | 0 |
| SAR 6705-6865 MHz Set3 Chain A [#] | 0 |
| SAR 6865-7105 MHz Set3 Chain A [#] | 0 |
| SAR 2400 MHz Set3 Chain B [#] | 0 |
| SAR 5150-5350 MHz Set3 Chain B [#] | 0 |
| SAR 5350-5470 MHz Set3 Chain B [#] | 0 |

| Aptio Setup – AMI | | |
|-------------------------------------|---|--|
| Advanced | | |
| SAR 5470-5725 MHz Set3 Chain B# | 0 | |
| SAR 5725-5925 MHz Set3 Chain B# | 0 | |
| SAR 5945-6165 MHz Set3 Chain B# | 0 | |
| SAR 6165-6405 MHz Set3 Chain B# | 0 | |
| SAR 6405-6525 MHz Set3 Chain B# | 0 | |
| SAR 6525-6705 MHz Set3 Chain B# | 0 | |
| SAR 6705-6865 MHz Set3 Chain B# | 0 | |
| SAR 6865-7105 MHz Set3 Chain B# | 0 | |
| SAR 2400 MHz Set4 Chain A# | 0 | |
| SAR 5150-5350 MHz Set4 Chain A# | 0 | |
| SAR 5350-5470 MHz Set4 Chain A# | 0 | |
| SAR 5470-5725 MHz Set4 Chain A# | 0 | |
| SAR 5725-5925 MHz Set4 Chain A# | 0 | |
| SAR 5945-6165 MHz Set4 Chain A# | 0 | |
| SAR 6165-6405 MHz Set4 Chain A# | 0 | |
| SAR 6405-6525 MHz Set4 Chain A# | 0 | |
| SAR 6525-6705 MHz Set4 Chain A# | 0 | |
| SAR 6705-6865 MHz Set4 Chain A# | 0 | |
| SAR 6865-7105 MHz Set4 Chain A# | 0 | |
| SAR 2400 MHz Set4 Chain B# | 0 | |
| SAR 5150-5350 MHz Set4 Chain B# | 0 | |
| SAR 5350-5470 MHz Set4 Chain B# | 0 | |
| SAR 5470-5725 MHz Set4 Chain B# | 0 | |
| SAR 5725-5925 MHz Set4 Chain B# | 0 | |
| SAR 5945-6165 MHz Set4 Chain B# | 0 | |
| SAR 6165-6405 MHz Set4 Chain B# | 0 | |
| SAR 6405-6525 MHz Set4 Chain B# | 0 | |
| SAR 6525-6705 MHz Set4 Chain B# | 0 | |
| SAR 6705-6865 MHz Set4 Chain B# | 0 | |
| SAR 6865-7105 MHz Set4 Chain B# | 0 | |
| SAR CDB 2400 MHz Set2 Chain A# | 0 | |
| SAR CDB 5150-5350 MHz Set2 Chain A# | 0 | |
| SAR CDB 5350-5470 MHz Set2 Chain A# | 0 | |
| SAR CDB 5470-5725 MHz Set2 Chain A# | 0 | |
| SAR CDB 5725-5925 MHz Set2 Chain A# | 0 | |
| SAR CDB 5945-6165 MHz Set2 Chain A# | 0 | |
| SAR CDB 6165-6405 MHz Set2 Chain A# | 0 | |
| SAR CDB 6405-6525 MHz Set2 Chain A# | 0 | |
| SAR CDB 6525-6705 MHz Set2 Chain A# | 0 | |
| SAR CDB 6705-6865 MHz Set2 Chain A# | 0 | |

| Aptio Setup – AMI | |
|---|---|
| Advanced | |
| SAR CDB 6865-7105 MHz Set2 Chain A [#] | 0 |
| SAR CDB 2400 MHz Set2 Chain B [#] | 0 |
| SAR CDB 5150-5350 MHz Set2 Chain B [#] | 0 |
| SAR CDB 5350-5470 MHz Set2 Chain B [#] | 0 |
| SAR CDB 5470-5725 MHz Set2 Chain B [#] | 0 |
| SAR CDB 5725-5925 MHz Set2 Chain B [#] | 0 |
| SAR CDB 5945-6165 MHz Set2 Chain B [#] | 0 |
| SAR CDB 6165-6405 MHz Set2 Chain B [#] | 0 |
| SAR CDB 6405-6525 MHz Set2 Chain B [#] | 0 |
| SAR CDB 6525-6705 MHz Set2 Chain B [#] | 0 |
| SAR CDB 6705-6865 MHz Set2 Chain B [#] | 0 |
| SAR CDB 6865-7105 MHz Set2 Chain B [#] | 0 |
| SAR CDB 2400 MHz Set3 Chain A [#] | 0 |
| SAR CDB 5150-5350 MHz Set3 Chain A [#] | 0 |
| SAR CDB 5350-5470 MHz Set3 Chain A [#] | 0 |
| SAR CDB 5470-5725 MHz Set3 Chain A [#] | 0 |
| SAR CDB 5725-5925 MHz Set3 Chain A [#] | 0 |
| SAR CDB 5945-6165 MHz Set3 Chain A [#] | 0 |
| SAR CDB 6165-6405 MHz Set3 Chain A [#] | 0 |
| SAR CDB 6405-6525 MHz Set3 Chain A [#] | 0 |
| SAR CDB 6525-6705 MHz Set3 Chain A [#] | 0 |
| SAR CDB 6705-6865 MHz Set3 Chain A [#] | 0 |
| SAR CDB 6865-7105 MHz Set3 Chain A [#] | 0 |
| SAR CDB 2400 MHz Set3 Chain B [#] | 0 |
| SAR CDB 5150-5350 MHz Set3 Chain B [#] | 0 |
| SAR CDB 5350-5470 MHz Set3 Chain B [#] | 0 |
| SAR CDB 5470-5725 MHz Set3 Chain B [#] | 0 |
| SAR CDB 5725-5925 MHz Set3 Chain B [#] | 0 |
| SAR CDB 5945-6165 MHz Set3 Chain B [#] | 0 |
| SAR CDB 6165-6405 MHz Set3 Chain B [#] | 0 |
| SAR CDB 6405-6525 MHz Set3 Chain B [#] | 0 |
| SAR CDB 6525-6705 MHz Set3 Chain B [#] | 0 |
| SAR CDB 6705-6865 MHz Set3 Chain B [#] | 0 |
| SAR CDB 6865-7105 MHz Set3 Chain B [#] | 0 |
| SAR CDB 2400 MHz Set4 Chain A [#] | 0 |
| SAR CDB 5150-5350 MHz Set4 Chain A [#] | 0 |
| SAR CDB 5350-5470 MHz Set4 Chain A [#] | 0 |
| SAR CDB 5470-5725 MHz Set4 Chain A [#] | 0 |
| SAR CDB 5725-5925 MHz Set4 Chain A [#] | 0 |
| SAR CDB 5945-6165 MHz Set4 Chain A [#] | 0 |

| Aptio Setup – AMI | |
|---|-----|
| Advanced | |
| SAR CDB 6165-6405 MHz Set4 Chain A [#] | 0 |
| SAR CDB 6405-6525 MHz Set4 Chain A [#] | 0 |
| SAR CDB 6525-6705 MHz Set4 Chain A [#] | 0 |
| SAR CDB 6705-6865 MHz Set4 Chain A [#] | 0 |
| SAR CDB 6865-7105 MHz Set4 Chain A [#] | 0 |
| SAR CDB 2400 MHz Set4 Chain B [#] | 0 |
| SAR CDB 5150-5350 MHz Set4 Chain B [#] | 0 |
| SAR CDB 5350-5470 MHz Set4 Chain B [#] | 0 |
| SAR CDB 5470-5725 MHz Set4 Chain B [#] | 0 |
| SAR CDB 5725-5925 MHz Set4 Chain B [#] | 0 |
| SAR CDB 5945-6165 MHz Set4 Chain B [#] | 0 |
| SAR CDB 6165-6405 MHz Set4 Chain B [#] | 0 |
| SAR CDB 6405-6525 MHz Set4 Chain B [#] | 0 |
| SAR CDB 6525-6705 MHz Set4 Chain B [#] | 0 |
| SAR CDB 6705-6865 MHz Set4 Chain B [#] | 0 |
| SAR CDB 6865-7105 MHz Set4 Chain B [#] | 0 |
| WGDS Package [#] | |
| SAR 2400 MHz Max Allowed for Group 1 (FCC) [#] | 255 |
| SAR 2400 MHz Chain A Offset for Group 1 (FCC) [#] | 0 |
| SAR 2400 MHz Chain B Offset for Group 1 (FCC) [#] | 0 |
| SAR 5200 MHz Max Allowed for Group 1 (FCC) [#] | 255 |
| SAR 5200 MHz Chain A Offset for Group 1 (FCC) [#] | 0 |
| SAR 5200 MHz Chain B Offset for Group 1 (FCC) [#] | 0 |
| SAR 6000-7000 MHz Max Allowed for Group 1 (FCC) [#] | 255 |
| SAR 6000-7000 MHz Chain A Offset for Group 1 (FCC) [#] | 0 |
| SAR 6000-7000 MHz Chain B Offset for Group 1 (FCC) [#] | 0 |
| SAR 2400 MHz Max Allowed for Group 2 (EU Japan) [#] | 255 |
| SAR 2400 MHz Chain A Offset for Group 2 (EU Japan) [#] | 0 |
| SAR 2400 MHz Chain B Offset for Group 2 (EU Japan) [#] | 0 |
| SAR 5200 MHz Max Allowed for Group 2 (EU Japan) [#] | 255 |
| SAR 5200 MHz Chain A Offset for Group 2 (EU Japan) [#] | 0 |
| SAR 5200 MHz Chain B Offset for Group 2 (EU Japan) [#] | 0 |

| Aptio Setup – AMI | |
|---|-------------|
| Advanced | |
| SAR 6000-7000 MHz Max Allowed for Group 2 (EU Japan) # | 255 |
| SAR 6000-7000 MHz Chain A Offset for Group 2 (EU Japan) # | 0 |
| SAR 6000-7000 MHz Chain B Offset for Group 2 (EU Japan) # | 0 |
| SAR 2400 MHz Max Allowed for Group 3 (ROW) # | 255 |
| SAR 2400 MHz Chain A Offset for Group 3 (ROW) # | 0 |
| SAR 2400 MHz Chain B Offset for Group 3 (ROW) # | 0 |
| SAR 5200 MHz Max Allowed for Group 3 (ROW) # | 255 |
| SAR 5200 MHz Chain A Offset for Group 3 (ROW) # | 0 |
| SAR 5200 MHz Chain B Offset for Group 3 (ROW) # | 0 |
| SAR 6000-7000 MHz Max Allowed for Group 3 (ROW) # | 255 |
| SAR 6000-7000 MHz Chain A Offset for Group 3 (ROW) # | 0 |
| SAR 6000-7000 MHz Chain B Offset for Group 3 (ROW) # | 0 |
| External 32KHz Clock# | [Not Valid] |
| PPAG Package# | |
| WiFi ANT Gain control# | [Disabled] |
| Ant Gain 2400 MHz Chain A# | 24 |
| Ant Gain 5150-5350 MHz Chain A# | 40 |
| Ant Gain 5350-5470 MHz Chain A# | 40 |
| Ant Gain 5470-5725 MHz Chain A# | 40 |
| Ant Gain 5725-5945 MHz Chain A# | 40 |
| Ant Gain 5945-6165 MHz Chain A# | 40 |
| Ant Gain 6165-6405 MHz Chain A# | 40 |
| Ant Gain 6405-6525 MHz Chain A# | 40 |
| Ant Gain 6525-6705 MHz Chain A# | 40 |
| Ant Gain 6705-6865 MHz Chain A# | 40 |
| Ant Gain 6865-7105 MHz Chain A# | 40 |
| Ant Gain 2400 MHz Chain B# | 24 |
| Ant Gain 5150-5350 MHz Chain B# | 40 |
| Ant Gain 5350-5470 MHz Chain B# | 40 |
| Ant Gain 5470-5725 MHz Chain B# | 40 |
| Ant Gain 5725-5945 MHz Chain B# | 40 |
| Ant Gain 5945-6165 MHz Chain B# | 40 |

| Aptio Setup – AMI | | |
|---|----------------------------------|--|
| Advanced | | |
| Ant Gain 6165-6405 MHz Chain B [#] | 40 | |
| Ant Gain 6405-6525 MHz Chain B [#] | 40 | |
| Ant Gain 6525-6705 MHz Chain B [#] | 40 | |
| Ant Gain 6705-6865 MHz Chain B [#] | 40 | |
| Ant Gain 6865-7105 MHz Chain B [#] | 40 | |
| Bluetooth SAR [#] | [Disabled] | |
| Bluetooth SAR BR [#] | 0 | |
| Bluetooth SAR EDR2 [#] | 0 | |
| Bluetooth SAR EDR3 [#] | 0 | |
| Bluetooth SAR LE [#] | 0 | |
| Bluetooth SAR LE 2Mhz [#] | 0 | |
| Bluetooth SAR LE LR [#] | 0 | |
| Disable SRD Active Channels [#] | 0 | |
| Supported Indonesia 5.15-5.35 GHz Band [#] | 0 | |
| Ultra High Band Support [#] | 0 | |
| Regulatory Configurations [#] | [Disable DRS for China Location] | |
| UART Configurations [#] | [Default] | |
| UNII-4 [#] | 0 | |
| Indoor Control [#] | 0 | |
| Wi-Fi Time Average SAR – WTAS [#] | | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| WTAS Selection [#] | [Disabled] | |
| WTAS List Entries [#] | 0 | |
| ISO country code to block [#] | 0 | |
| : | | |
| : | | |
| ISO country code to block [#] | 0 | |
| > WWAN Configuration | | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when selecting [Auto Detection] for CNVi Mode.

** This item appears only when selecting [UART] for Discrete Bluetooth Interface.

These items appear only when enabling Advanced Settings.

| Feature | Option | Description |
|-----------|---|---|
| CNVi Mode | [Disable Integrated], [Auto Detection] | This option configures Connectivity. [Auto Detection] means that if Discrete solution is discovered it will be enabled by default. Otherwise Integrated solution (CNVi) will be enabled; [Disable Integrated] disables Integrated Solution. |

| Feature | Option | Description |
|--------------------------------------|---|---|
| | | Note: When CNVi is present, the GPIO pins that are used for radio interface cannot be assigned to the other native function. |
| Wi-Fi Core | [Enabled] | Read only item |
| BT Core | [Enabled] | Read only item |
| BT Audio Offload | [Enabled] | Read only item |
| BT RF-Kill Delay Time | 0 | Read only item |
| RFI Mitigation | [Enabled], [Disabled] | This is an option intended to Enable / Disable DDR-RFIM feature for Connectivity. This RFI mitigation feature may result in temporary slowdown of the DDR speed. |
| CoExistence Manager | [Disabled] | Read only item |
| Discrete Bluetooth Interface | [Disabled], [USB], [UART] | Serial IO UART0 needs to be enabled to select BT interface |
| BT Interrupt Mode | [GPIO Interrupt], [APIC Interrupt] | Selects routing of interrupt from BT Module |
| BT Tile Mode | [Disabled], [Enabled] | Enable / Disable Tile |
| Advanced settings | [Disabled], [Enabled] | Configure ACPI objects for wireless devices |
| Switched Antenna Diversity Selection | [Antenna1], [Antenna2], [Diversity], [Diversity Antenna1], [Diversity Antenna2] | This allows WiFi modules which have only one antenna to use one of the 2 possible antennas with the options: 0 – Antenna1 1 – Antenna2 2 – Diversity 3 – Diversity Antenna1 4 – Diversity Antenna2 |
| Domain Type SPLC 1 | Value input | 09h: Module (M.2); 07h: WiFi / WLAN; 0Fh: WWAN; 10h: WiGig; 14h: RFEM |
| Default Power Limit | Value input | Power Limit in milli watts |
| Default Time Window | Value input | Time Window in milli seconds |
| TRxDelay_A / B | Value input | Antenna A / B delay possible values: 1-100 in 10ths of nano seconds resolution |
| TrxCableLength_A / B | Value input | Antenna A / B cable length possible values: 1-100 cm in 1 cm resolution |
| 11Ax Setting for Ukraine | [Disabled], [Enabled] | 11Ax Setting for Ukraine Bit 2 – Apply changes to country Ukraine. 11Ax Setting within module certification 00 – None. Work with Wi-Fi FW/OTP definitions [Default] 01 – Apply changes |
| 11Ax Mode for Ukraine | [Disabled], | 11Ax Mode for Ukraine |

| Feature | Option | Description |
|---|--|---|
| | [Enabled] | Bit 1 – 11Ax Mode. Effective only if Bit 0 set to 1 00 – Disable 11Ax on country Ukraine [Default] 01 – Enable 11Ax on country Ukraine |
| 11Ax Setting for Russia | [Disabled], [Enabled] | 11Ax Setting for Russia Bit 2 – Apply changes to country Russia. 11Ax Setting within module certification 00 – None. Work with Wi-Fi FW/OTP definitions [Default] 01 – Apply changes |
| 11Ax Mode for Russia | [Disabled], [Enabled] | 11Ax Mode for Russia Bit 3 – 11Ax Mode. Effective only if Bit 2 set to 1 00 – Disable 11Ax on country Russia [Default] 01 – Enable 11Ax on country Russia |
| WiFi SAR | [Disabled], [Enabled] | Enable / Disable WiFi SAR Tx Power Limit; [Disabled]: Device ignores WiFi SAR Configuration Table; [Enabled]; Device uses WiFi SAR Configuration Table. |
| SAR 2400 / 5150-5350 / .. / 6865-7105 MHz Set 1 Chain A / B | Value input | Defines the WiFi SAR Tx Power Limit – 8bit unsigned with 5bit integer and 3bit fractional. 0x00 = 0b00000000 = 0.125dB; 0xFF = 0b11111111 = 31.875dB. Each step is equivalent to 0.125dB |
| SAR CDB 2400 / 5150-5350 / .. / 6865-7105 MHz Set 1 Chain A / B | Value input | Defines the WiFi CDB SAR Tx Power Limit – 8bit unsigned with 5bit integer and 3bit fractional. 0x00 = 0b00000000 = 0.125dB; 0xFF = 0b11111111 = 31.875dB. Each step is equivalent to 0.125dB |
| WiFi Dynamic SAR | [Disabled], [Enabled] | Enable / Disable WiFi Dynamic SAR Tx Power Limit which shall be set dynamically according to the Proximity Sensor |
| Extended SAR Range Sets | [No Additional sets], [Set 2], [Set 3], [Set 4] | Defines the WiFi SAR Sets that can be used to set the power limits dynamically based on the Proximity Sensor, Set 1 is always present if WiFi SAR enabled and Set 2-3 are additional sets. |
| SAR 2400 / 5150-5350 / .. / 6865-7105 MHz Set 2 / 3 / 4 Chain A / B | Value input | Defines the WiFi SAR Tx Power Limit – 8bit unsigned with 5bit integer and 3bit fractional. 0x00 = 0b00000000 = 0.125dB; 0xFF = 0b11111111 = 31.875dB. Each step is equivalent to 0.125dB |
| SAR CDB 2400 / 5150-5350 / .. / 6865-7105 MHz Set 2 / 3 / 4 Chain A / B | Value input | Defines the WiFi CDB SAR Tx Power Limit – 8bit unsigned with 5bit integer and 3bit fractional. 0x00 = 0b00000000 = 0.125dB; 0xFF = 0b11111111 = 31.875dB. Each step is equivalent to 0.125dB |
| SAR 2400 / 5200 / 6000-7000 MHz Max Allowed for Group 1 / 2 / 3 (FCC / EU Japan / ROW) | Value input | Defines the WiFi SAR Delta Value to be applied – 8bit unsigned with 5bit integer and 3bit fractional. 0x00 = 0b00000000 = 0.125dB; 0xFF = 0b11111111 = 31.875dB. Each step is equivalent to 0.125dB |
| SAR 2400 / 5200 / 6000-7000 MHz Chain A Offset for Group 1 / 2 / 3 (FCC / EU Japan / ROW) | Value input | Defines the WiFi SAR Delta Value to be applied – 8bit unsigned with 5bit integer and 3bit fractional. 0x00 = 0b00000000 = 0.125dB; 0xFF = 0b11111111 = 31.875dB. Each step is equivalent to 0.125dB |

| Feature | Option | Description |
|--|--|--|
| SAR 2400 / 5200 / 6000-7000 MHz Chain B Offset for Group 1 / 2 / 3 (FCC / EU Japan / ROW) | Value input | Defines the WiFi SAR Tx Power Limit – 8bit unsigned with 5bit integer and 3bit fractional. 0x00 = 0b00000000 = 0.125dB; 0xFF = 0b11111111 = 31.875dB. Each step is equivalent to 0.125dB |
| External 32KHz Clock | [Not Valid], [Valid] | This will be used to specify that platform does have valid External 32KHz clock or not. |
| ANT Gain 2400 / 5150-5350 / .. / 6865-7105 MHz Chain A / B | Value input | Defines the WiFi ANT gain Delta Value to be supplied – 8bit signed Two's complement 0.125dB. 0x80 = 0b10000000 = -16dB; 0x7F = 0b01111111 = 15.875dB. Each step is equivalent to 0.125dB |
| Bluetooth SAR | [Disabled], [Enabled] | Define the mode of SAR control to be used. [Disabled]: Tx power shall be mandated by device NVM [Enabled]: Tx power shall be the minimum between BIOS SAR table and BT Device NVM (either Module or Platform) |
| Bluetooth SAR BR / EDR2 / EDR3 / LE / LE 2Mhz / LE LR | Value input | Defines the SAR power restriction for BR / EDR2 / EDR3 / LE / LE 2Mhz / LE LR Modulation |
| Disable SRD Active Channels | Value input | Enable / Disable SRD Active Channels 00 – ETSI 5.8 GHz SRD Active Scan Enable 01 – ETSI 5.8 GHz SRD Passive Scan Enable 02 – ETSI 5.8 GHz SRD Disabled |
| Supported Indonesia 5.15-5.35 GHz Band | Value input | Enable / Disable Indonesia 5.15-5.35 GHz 00 – Set 5.15-5.35 GHz to Disable in Indonesia 01 – Set 5.15-5.35 GHz to Enable (Passive) in Indonesia 02 – Reserved |
| Ultra High Band Support | Value input | Please input HEX value. Bit0 '0' No override [Default] '1' Only allow countries enabled in the following bits Bit1 – USA '0' USA 6GHz disable '1' 6GHz allowed in USA Bit2 – Rest of World Bit3 – EU countries Bit4 – South Korea Bit5 – Brazil Bit6 – Chile Bit7 – Japan Bit8 – Canada Bit31:9 – Reserved |
| Regulatory Configurations | [Disable DRS for China Location], [Enable DRS for China Location] | Enabling DRS for China Location |

| Feature | Option | Description |
|---------------------------|--------------------------|---|
| UART Configurations | [Default] | TBD |
| UNII-4 | Value input | Control Enablement UNII-4 over certificate modules Please input HEX value. FCC Bit0 – Apply changes over FCC, UNII-4 setting within module certification (Default Intel module definitions) '0' Work with WiFi FW/OTP definitions '1' Apply changes Bit1 – UNII-4 mode on FCC '0' Disable UNII-4 '1' Enable UNII-4 ETSI Bit2 – Apply changes over ETSI, UNII-4 setting within module certification (Default Intel module definition) Bit3 – UNII-4 mode on ETSI Bit31:4 – Reserved shall set to Zeros |
| Indoor Control | Value input | Device for Indoor Use Only (Solar Family onwards) Please input HEX value. Bit0 – EU Bit1 – Japan Bit2 – China, applied only in case of China BIOS or DRS in China Enabled Bit3 – USA Bit31:4 – Reserved shall set to Zeros |
| WTAS Selection | [Disabled], [Enabled] | Enable / Disable WTAS |
| WTAS List Entries | Value input | No. of blocked countries not approved by OEM to support this feature. |
| ISO country code to block | Country code input | The decimal equivalent of country code (a two-ASCII-character) as specified in ISO_3166-1. Ex. For JP – 19024 |

Figure 52: BIOS Advanced Menu – Connectivity Configuration – WWAN Configuration

| Aptio Setup – AMI | | |
|---|------------|--|
| Advanced | | |
| WWAN Device | [Disabled] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Firmware Flash Device ^{(1) (2)} | [Disabled] | |
| Wireless CNV Config Device ^{(1) (2)} | [Enabled] | |
| WWAN Reset Workaround ^{(1) (2)} | [Enabled] | |
| WA – WWAN OEM SVID ⁽²⁾ | 1CF8 | |
| WA – WWAN SVID Detect Timeout ⁽²⁾ | 0 | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

⁽¹⁾ These items appear only when selecting [4G – 7360/7560] for WWAN Device.

⁽²⁾ This item appears only when selecting [5G – M80] for WWAN Device.

| Feature | Option | Description |
|-------------------------------|--|---|
| WWAN Device | [Disabled], [4G – 7360/7560], [5G – M80] | Select the M.2 WWAN Device options to enable 4G – 7360/7560 (Intel), 5G – M80 (MediaTek) Modems |
| Firmware Flash Device | [Disabled], [Enabled] | Enable or Disable WWAN Firmware Flash Device |
| Wireless CNV Config Device | [Disabled], [Enabled] | Enable or Disable WCCD ACPI device node |
| WWAN Reset Workaround | [Disabled], [Enabled] | Enabling this workaround will result in BIOS asserting FULL_CARD_POWER_OFF#, PERST# and RESET# WWAN signals before the WWAN Device Power-On Sequence is executed. Disabling it has no impact. |
| WA – WWAN OEM SVID | ID input | WWAN OEM Sub-Vendor ID |
| WA – WWAN SVID Detect Timeout | Value input | The timeout value (ms) for detecting WWAN OEM SVID. Please notice it is a workaround for OEM only. |

Figure 53: BIOS Advanced Menu - CPU Configuration

| Aptio Setup – AMI | | | | | |
|--|----------|---------|----------|--|-------------|
| Main | Advanced | Chipset | Security | Boot | Save & Exit |
| CPU Configuration > Efficient-core Information > Performance-core Information ID Brand String VMX SMX/TXT TXT Crash Code TXT SPAD Boot Guard State Boot Guard ACM Policy Status Boot Guard SACM Information C6DRAM [Enabled] CPU Flex Ratio Override [Disabled] CPU Flex Ratio Settings* 15 Hardware Prefetcher [Enabled] Adjacent Cache Line Prefetch [Enabled] Intel (VMX) Virtualization Technology [Enabled] PECC [Enabled] AVX [Enabled] Active Efficient-cores [All] BIST [Disabled] AP threads Idle Manner [MWAIT Loop] AES [Enabled] MachineCheck [Enabled] MonitorMWait [Enabled] > CPU SMM Enhancement | | | | | |
| | | | | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | | | | |

*This item is activated only when enabling CPU Flex Ratio Override.

| Feature | Option | Description |
|-------------------------|--------------------------|---|
| C6DRAM | [Disabled], [Enabled] | Enable / Disable moving of DRAM contents to PRM memory when CPU is in C6 state |
| CPU Flex Ratio Override | [Disabled], [Enabled] | Enable / Disable CPU Flex Ratio Programming |
| CPU Flex Ratio Settings | Value input | This value must between Max Efficiency Ratio (LFM) and Maximum non-turbo ratio set by Hardware (HFM). |

| Feature | Option | Description |
|---------------------------------------|---|---|
| Hardware Prefetcher | [Disabled], [Enabled] | To turn on / off the MLC streamer prefetcher. |
| Adjacent Cache Line Prefetch | [Disabled], [Enabled] | To turn on / off prefetching of adjacent cache lines. |
| Intel (VMX) Virtualization Technology | [Disabled], [Enabled] | When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology. |
| PECI | [Disabled], [Enabled] | Enable / Disable Peci |
| AVX | [Enabled], [Disabled] | Enable / Disable the AVX 2 Instructions. This is applicable for Performance-core only |
| Active Efficient-cores | [All], [3], [2], [1], [0] | Number of E-cores to enable in each processor packages. Note: Number of Cores and E-cores are looked at together. When both are {0,0}, Pcode will enable all cores. |
| BIST | [Disabled], [Enabled] | Enable / Disable BIST (Built-In Self Test) on reset |
| AP threads Idle Manner | [HALF Loop], [MWAIT Loop], [RUN Loop] | AP threads Idle Manner for waiting signal to run |
| AES | [Disabled], [Enabled] | Enable / Disable AES (Advanced Encryption Standard) |
| MachineCheck | [Disabled], [Enabled] | Enable / Disable Machine Check |
| MonitorMWait | [Disabled], [Enabled] | Enable / Disable MonitorMWait, if Disable MonitorMWait, the AP threads Idle Manner should not set in MWAIT Loop. |

Figure 54: BIOS Advanced Menu - CPU Configuration – Efficient-core Information

| Aptio Setup – AMI | | |
|--|-----------|--|
| Advanced | | |
| Efficient-core Information | | |
| L1 Data Cache | 32 KB x 4 | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| L1 Instruction Cache | 64 KB x 4 | |
| L2 Cache | 2048 KB | |
| L3 Cache | 6 MB | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

Figure 55: BIOS Advanced Menu - CPU Configuration – CPU SMM Enhancement

| Aptio Setup – AMI | | |
|--|-----------|--|
| Advanced | | |
| CPU SMM Enhancement | | |
| SMM Use Delay Indication | [Enabled] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| SMM Use Block Indication | [Enabled] | |
| SMM Use SMM en-US Indication | [Enabled] | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|------------------------------|--------------------------|--|
| SMM Use Delay Indication | [Disabled], [Enabled] | Enable / Disable usage of SMM_DELAYED MSR for MP sync in SMI |
| SMM Use Block Indication | [Disabled], [Enabled] | Enable / Disable usage of SMM_BLOCKED MSR for MP sync in SMI |
| SMM Use SMM en-US Indication | [Disabled], [Enabled] | Enable / Disable usage of SMM_ENABLE MSR for MP sync in SMI |

Figure 56: BIOS Advanced Menu – Power & Performance

| Aptio Setup – AMI | | | | | |
|---|----------|---------|----------|--|-------------|
| Main | Advanced | Chipset | Security | Boot | Save & Exit |
| Power & Performance | | | | | |
| > CPU – Power Management Control > GT – Power Management Control | | | | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | | | | |

Figure 57: BIOS Advanced Menu – Power & Performance – CPU – Power Management Control

| Aptio Setup – AMI | |
|---|---------------------|
| Advanced | |
| CPU – Power Management Control | |
| Boot performance mode | [Turbo Performance] |
| Intel® SpeedStep™ | [Enabled] |
| Race To Halt (RTH) | [Enabled] |
| Intel® Speed Shift Technology | [Enabled] |
| Per Core P State OS control mode | [Enabled] |
| HwP Autonomous Per Core P State | [Enabled] |
| HwP Autonomous EPP Grouping | [Enabled] |
| EPB override over PECL | [Disabled] |
| HwP Lock | [Enabled] |
| HDC Control | [Enabled] |
| Turbo Mode | [Enabled] |
| > View/Configure Turbo Options | |
| > CPU VR Settings | |
| Platform PL1 Enable | [Disabled] |
| Platform PL1 Power ⁽¹⁾ | 0 |
| Platform PL1 Time Window ⁽¹⁾ | [0] |
| Platform PL2 Enable | [Disabled] |
| Platform PL2 Power ⁽²⁾ | 0 |
| Power Limit 4 Override | [Disabled] |

| Aptio Setup – AMI | | |
|--|------------------|------------------------|
| Advanced | | |
| Power Limit 4 ⁽³⁾ | 0 | |
| Power Limit 4 Lock ⁽³⁾ | [Disabled] | |
| C states | [Disabled] | |
| Enhanced C-states ⁽⁴⁾ | [Disabled] | |
| C-State Auto Demotion ⁽⁴⁾ | [C1] | |
| C-State Un-demotion ⁽⁴⁾ | [C1] | |
| Package C-State Demotion ⁽⁴⁾ | [Enabled] | |
| Package C-State Un-demotion ⁽⁴⁾ | [Enabled] | |
| CState Pre-Wake ⁽⁴⁾ | [Enabled] | |
| IO MWAIT Redirection ⁽⁴⁾ | [Disabled] | |
| Package C State Limit ⁽⁴⁾ | [Auto] | |
| C6/C7 Short Latency Control (MSR 0x60B) ⁽⁴⁾ | | |
| Time Unit ⁽⁴⁾ | [1024 ns] | |
| Latency ⁽⁴⁾ | 0 | |
| C6/C7 Long Latency Control (MSR 0x60C) ⁽⁴⁾ | | |
| Time Unit ⁽⁴⁾ | [1024 ns] | |
| Latency ⁽⁴⁾ | 0 | |
| C8 Latency Control (MSR 0x633) ⁽⁴⁾ | | |
| Time Unit ⁽⁴⁾ | [1024 ns] | |
| Latency ⁽⁴⁾ | 0 | |
| C9 Latency Control (MSR 0x634) ⁽⁴⁾ | | |
| Time Unit ⁽⁴⁾ | [1024 ns] | |
| Latency ⁽⁴⁾ | 0 | |
| C10 Latency Control (MSR 0x635) ⁽⁴⁾ | | |
| Time Unit ⁽⁴⁾ | [1024 ns] | |
| Latency ⁽⁴⁾ | 0 | |
| Thermal Monitor | [Enabled] | |
| Interrupt Redirection Mode Selection | [Fixed Priority] | |
| Time MWAIT | [Disabled] | |
| > Custom P-state Table | | |
| EC Turbo Control Mode | [Disabled] | |
| AC brick Capacity ⁽⁵⁾ | [90W AC Brick] | → ←: Select Screen |
| EC Polling Period ⁽⁵⁾ | 1 | ↑ ↓: Select Item |
| EC Guard Band Value ⁽⁵⁾ | 0 | Enter: Select |
| EC Algorithm Selection ⁽⁵⁾ | 1 | +/-: Change Opt. |
| Energy Performance Gain | [Disabled] | F1: General Help |
| EPG DIMM Idd3N ⁽⁶⁾ | 26 | F2: Previous Values |
| EPG DIMM Idd3P ⁽⁶⁾ | 11 | F3: Optimized Defaults |
| > Power Limit 3 Settings | | F4: Save & Exit |

| Aptio Setup – AMI | |
|--|-----------|
| Advanced | |
| > CPU Lock Configuration | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

- ⁽¹⁾ These items appear only when enabling Platform PL1 Enable.
⁽²⁾ This item appears only when enabling Platform PL2 Enable.
⁽³⁾ These items appear only when enabling Power Limit 4 Override.
⁽⁴⁾ These items appear only when enabling C states.
⁽⁵⁾ These items appear only when enabling EC Turbo Control Mode.
⁽⁶⁾ These items are activated only when enabling Energy Performance Gain.

| Feature | Option | Description |
|----------------------------------|---|--|
| Boot performance mode | [Max Battery], [Max Non-Turbo Performance], [Turbo Performance] | Select the performance state that the BIOS will set starting from reset vector. |
| Intel® SpeedStep™ | [Disabled], [Enabled] | Allows more than two frequency ranges to be supported. |
| Race To Halt (RTH) | [Disabled], [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) |
| Intel® Speed Shift Technology | [Disabled], [Enabled] | Enable / Disable Intel® Speed Shift Technology support. Enabling will expose the CPPC v2 interface to allow for hardware controlled P-states. |
| Per Core P State OS control mode | [Disabled], [Enabled] | Enable / Disable Per Core P state OS control mode. Disabling will set Bit 31 = 1 command 0x06. When set, the highest core request is used for all other core requests. |
| HwP Autonomous Per Core P State | [Disabled], [Enabled] | Disable Autonomous PCPS (Bit 30 = 1, command 0x11) Autonomous will request the same value for all cores all the time. Enable PCPS (default Bit 30 = 0, command 0x11) |
| HwP Autonomous EPP Grouping | [Disabled], [Enabled] | Enable EPP grouping (default Bit 29 = 0, command 0x11) Autonomous will request the same values for all cores with same EPP. Disable EPP grouping (Bit 29 = 1, command 0x11) autonomous will not necessarily request same values for all cores with same EPP. |
| EPB override over PECI | [Disabled], [Enabled] | Enable / Disable EPB override over PECI. Enable by sending pcode command 0x2b, subcommand 0x3 to 1. This will allow OOB EPB PECI override control. |
| HwP Lock | [Disabled], [Enabled] | Enable / Disable HWP Lock support in Misc Power Management MSR. |
| HDC Control | [Disabled], [Enabled] | This option allows HDC configuration. [Disabled]: Disable HDC. |

| Feature | Option | Description |
|--------------------------|--|---|
| | | [Enabled]: Can be enabled by OS if OS native support is available. |
| Turbo Mode | [Disabled], [Enabled] | Enable / Disable processor Turbo Mode (requires EMTTM enabled too). AUTO means enabled. |
| Platform PL1 Enable | [Disabled], [Enabled] | Enable / Disable Platform Power Limit 1 programming. If this option is disabled, it activates the PL1 value to be used by the processor to limit the average power of given time window. |
| Platform PL1 Power | Value input | Platform Power Limit 1 Power in Milli Watts/Percent. BIOS will round to the nearest 1/8W when programming. Any value can be programmed between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). For example, if 12.50W, enter 12500; if 12%, enter 12000; if 50%, enter 50000. This setting will act as the new PL1 value for the Package RAPL algorithm. |
| Platform PL1 Time Window | [0], [1], [2], [3], [4], [5], [6], [7], [8], [10], [12], [14], [16], [20], [24], [28], [32], [40], [48], [56], [64], [80], [96], [112], [128] | Platform Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0 = default values. Indicates the time window over which Platform Processor Base Power (TDP) value should be maintained. |
| Platform PL2 Enable | [Disabled], [Enabled] | Enable / Disable Platform Power Limit 2 programming. If this option is disabled, BIOS will program the default values for Platform Power Limit 2. |
| Platform PL2 Power | Value input | Platform Power Limit 2 Power in Milli Watts/Percent. BIOS will round to the nearest 1/8W when programming. Any value can be programmed between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). For example, if 12.50W, enter 12500; if 12%, enter 12000; if 50%, enter 50000. This setting will act as the new PL2 value for the Package RAPL algorithm. |
| Power Limit 4 Override | [Disabled], [Enabled] | Enable / Disable Power Limit 4 override. If this option is disabled, BIOS will leave the default value for Power Limit 4. |
| Power Limit 4 | Value input | Power Limit 4 in Milli Watts. BIOS will round to the nearest 1/8W when programming. For 12.50W, enter 12500. If the value is 0, BIOS leaves default value. |
| Power Limit 4 Lock | [Disabled], [Enabled] | Power Limit 4 MSR 601h Lock. When enabled PL4 configurations are locked during OS. When disabled PL4 configuration can be changed during OS. |
| C states | [Disabled], [Enabled] | Enable / Disable CPU Power Management. Allow CPU to go to C states when it's not 100% utilized. |
| Enhanced C-states | [Disabled], [Enabled] | Enable / Disable C1E. When enabled, CPU will switch to minimum speed when all cores enter C-State. |
| C-State Auto Demotion | [Disabled], [C1] | Configure C-State Auto Demotion |
| C-State Un-demotion | [Disabled], [C1] | Configure C-State Un-demotion |

| Feature | Option | Description |
|--------------------------------------|--|--|
| Package C-State Demotion | [Disabled], [Enabled] | Package C-State Demotion |
| Package C-State Un-demotion | [Disabled], [Enabled] | Package C-State Un-demotion |
| CState Pre-Wake | [Disabled], [Enabled] | [Disabled]: Sets bit 30 of POWER_CTL MSR (0x1FC) to 1 to disable the CState Pre-Wake |
| IO MWAIT Redirection | [Disabled], [Enabled] | When set, will map IO_read instructions sent to IO registers PMG_IO_BASE_ADDRBASE+offset to MWAIT (offset) |
| Package C State Limit | [C0/C1], [C2], [C3], [C6], [C7], [C7S], [C8], [C9], [C10], [CPU Default], [Auto] | Maximum Package C State Limit Setting. [CPU Default]: Leaves to Factory default value. [Auto]: Initializes to deepest available Package C State Limit. |
| Time Unit | [1 ns], [32 ns], [1024 ns], [32768 ns], [1048576 ns], [33554432 ns] | Unit of measurement for IRTL value – bits [12:10] |
| Latency | Value input | Interrupt Response Time Limit value – bits [9:0], Enter 0-1023 |
| Thermal Monitor | [Disabled], [Enabled] | Enable / Disable Thermal Monitor |
| Interrupt Redirection Mode Selection | [Fixed Priority], [Round Robin], [Hash Vector], [No Change] | Interrupt Redirection Mode Select for Logical Interrupts |
| Timed MWAIT | [Disabled], [Enabled] | Enable / Disable Timed MWAIT Support |
| EC Turbo Control Mode | [Disabled], [Enabled] | Enable / Disable EC Turbo Control mode |
| Energy Performance Gain | [Disabled], [Enabled] | Enable / Disable Energy Performance Gain. |
| EPG DIMM Idd3N | Value input | Active standby current (Idd3N) in milliamps from datasheet. Must be calculated on a per DIMM basis. |
| EPG DIMM Idd3P | Value input | Active power-down current (Idd3P) in milliamps from datasheet. Must be calculated on a per DIMM basis. |

Figure 58: BIOS Advanced Menu – Power & Performance – CPU – Power Management Control – View/Configure Turbo Options

| Aptio Setup – AMI | | |
|--|------------|------------------------|
| Advanced | | |
| Current Turbo Settings | | |
| Max Turbo Power Limit | 4095.875 | |
| Min Turbo Power Limit | 0.0 | |
| Package TDP Limit | 9.0 | |
| Power Limit 1 | 9.0 | |
| Power Limit 2 | 25.0 | |
| > Turbo Ratio Limit Options | | → ←: Select Screen |
| Energy Efficient P-state | [Enabled] | ↑ ↓: Select Item |
| Package Power Limit MSR Lock | [Disabled] | Enter: Select |
| Power Limit 1 Override | [Disabled] | +/-: Change Opt. |
| Power Limit 1* | 0 | F1: General Help |
| Power Limit 1 Time Window* | [0] | F2: Previous Values |
| Power Limit 2 Override | [Disabled] | F3: Optimized Defaults |
| Power Limit 2** | 0 | F4: Save & Exit |
| Energy Efficient Turbo | [Enabled] | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

*Appear only when enabling Power Limit 1 Override / ** Appears only when enabling Power Limit 2 Override.

| Feature | Option | Description |
|------------------------------|--------------------------|--|
| Energy Efficient P-state | [Disabled], [Enabled] | Enable / Disable Energy Efficient P-state feature. When set to 0, will disable access to ENERGY_PERFORMANCE_BIAS MSR and CPUID Function 6 ECX[3] will read 0 indicating no support for Energy Efficient policy setting. When set to 1, will enable access to ENERGY_PERFORMANCE_BIAS MSR 1B0h and CPUID Function 6 ECX[3] will read 1 indicating Energy Efficient policy setting is supported. |
| Package Power Limit MSR Lock | [Disabled], [Enabled] | 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. |
| Power Limit 1 Override | [Disabled], [Enabled] | Enable / Disable Power Limit 1 override. If this option is disabled, BIOS will program the default values for Power Limit 1 and Power Limit 1 Time Window. |
| Power Limit 1 | Value input | Power Limit 1 in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Overclocking SKU: Value must be between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). |

| Feature | Option | Description |
|---------------------------|---|---|
| | | Other SKUs: This value must be between Min Power Limit and Processor Base Power (TDP) Limit. If value is 0, BIOS will program Processor Base Power (TDP) value. |
| Power Limit 1 Time Window | [0], [1], [2], [3], [4], [5], [6], [7], [8], [10], [12], [14], [16], [20], [24], [28], [32], [40], [48], [56], [64], [80], [96], [112], [128] | Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0 = default values (28 sec for Mobile and 8 sec for Desktop). Defines time window which Processor Base Power (TDP) value should be maintained. |
| Power Limit 2 Override | [Disabled], [Enabled] | Enable / Disable Power Limit 2 override. If this option is disabled, BIOS will program the default values for Power Limit 2. |
| Power Limit 2 | Value input | Power Limit 2 value in Milli Watts. BIOS will round to the nearest 1/8W when programming. If the value is 0, BIOS will program this value as 1.25 * Processor Base Power (TDP). For 12.50W, enter 12500. Processor applies control policies such that the package power does not exceed this limit. |
| Energy Efficient Turbo | [Disabled], [Enabled] | 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. |

Figure 59: BIOS Advanced Menu – Power & Performance – CPU – Power Management Control – View/Configure Turbo Options – Turbo Ratio Limit Options

| Aptio Setup – AMI | |
|------------------------------------|----|
| Advanced | |
| Current Turbo Ratio Limit Settings | |
| E-core Turbo Ratio Limit Numcore0 | 1 |
| E-core Turbo Ratio Limit Numcore1 | 2 |
| E-core Turbo Ratio Limit Numcore2 | 3 |
| E-core Turbo Ratio Limit Numcore3 | 4 |
| E-core Turbo Ratio Limit Numcore4 | 5 |
| E-core Turbo Ratio Limit Numcore5 | 6 |
| E-core Turbo Ratio Limit Numcore6 | 7 |
| E-core Turbo Ratio Limit Numcore7 | 8 |
| E-core Turbo Ratio Limit Ratio0 | 34 |
| E-core Turbo Ratio Limit Ratio1 | 33 |
| E-core Turbo Ratio Limit Ratio2 | 27 |
| E-core Turbo Ratio Limit Ratio3 | 27 |
| E-core Turbo Ratio Limit Ratio4 | 27 |

| Aptio Setup – AMI | | | |
|--|----|--|--|
| Advanced | | | |
| E-core Turbo Ratio Limit Ratio5 | 27 | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit | |
| E-core Turbo Ratio Limit Ratio6 | 27 | | |
| E-core Turbo Ratio Limit Ratio7 | 27 | | |
| E-core Turbo Ratio Limit Numcore0 | 1 | | |
| E-core Turbo Ratio Limit Numcore1 | 2 | | |
| E-core Turbo Ratio Limit Numcore2 | 3 | | |
| E-core Turbo Ratio Limit Numcore3 | 4 | | |
| E-core Turbo Ratio Limit Numcore4 | 5 | | |
| E-core Turbo Ratio Limit Numcore5 | 6 | | |
| E-core Turbo Ratio Limit Numcore6 | 7 | | |
| E-core Turbo Ratio Limit Numcore7 | 8 | | |
| E-core Turbo Ratio Limit Ratio0 | 34 | | |
| E-core Turbo Ratio Limit Ratio1 | 33 | | |
| E-core Turbo Ratio Limit Ratio2 | 27 | | |
| E-core Turbo Ratio Limit Ratio3 | 27 | | |
| E-core Turbo Ratio Limit Ratio4 | 27 | | |
| E-core Turbo Ratio Limit Ratio5 | 27 | | |
| E-core Turbo Ratio Limit Ratio6 | 27 | | |
| E-core Turbo Ratio Limit Ratio7 | 27 | | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | | |

| Feature | Option | Description |
|---|-------------|--|
| E-core Turbo Ratio Limit Numcore0/1/2/3/4/5/6/7 | Value input | Efficient-core Turbo Ratio Limit Numcore0/1/2/3/4/5/6/7 defines the core range, the turbo ratio is defined in E-core Turbo Ratio Limit Ratio0/1/2/3/4/5/6/7. If value is zero, this entry is ignored. |
| E-core Turbo Ratio Limit Ratio0/1/2/3/4/5/6/7 | Value input | Efficient-core Turbo Ratio Limit Ratio0/1/2/3/4/5/6/7 defines the turbo ratio (max is 85 irrespective of the core extension mode), the core range is defined in E-core Turbo Ratio Limit Numcore0/1/2/3/4/5/6/7. |

Figure 60: BIOS Advanced Menu – Power & Performance – CPU – Power Management Control – CPU VR Settings

| Aptio Setup – AMI | | |
|--|------------|------------------------|
| Advanced | | |
| CPU VR Settings | | |
| Current Vccln Aux Icc Max | 108 | |
| PSYS Slope | 0 | |
| PSYS Offset | 0 | |
| PSYS Prefix | [+] | |
| PSYS Pmax Power | 0 | |
| Min Voltage Override | [Disabled] | |
| Min Voltage Runtime* | 0 | |
| Min Voltage C8* | 0 | |
| Vccln Aux Icc Max | 0 | |
| Vccln Aux IMON Slope | 111 | |
| Vccln Aux IMON Offset | 0 | |
| Vccln Aux IMON Prefix | [+] | |
| Vsys/Psys Critical | [Disabled] | |
| Vsys/Psys Full Scale** | 200000 | |
| Vsys/Psys Critical Threshold** | 130000 | |
| Assertion Deglitch Mantissa | 1 | → ←: Select Screen |
| Assertion Deglitch Exponent | 0 | ↑ ↓: Select Item |
| De assertion Deglitch Mantissa | 13 | Enter: Select |
| De assertion Deglitch Exponent | 2 | +/-: Change Opt. |
| VR Power Delivery Design | [AUTO] | F1: General Help |
| > Acoustic Noise Settings | | F2: Previous Values |
| > Core/IA VR Settings | | F3: Optimized Defaults |
| > GT VR Settings | | F4: Save & Exit |
| > RFI Settings | | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

*These items appear only when enabling Power Min Voltage Override.

** These items appear only when enabling Vsys/Psys Critical.

| Feature | Option | Description |
|-------------|-------------|--|
| PSYS Slope | Value input | 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 | Value input | PSYS Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. PSYS Uses BIOS VR mailbox command 0x4. |
| PSYS Prefix | [+], [-] | Set the offset value as positive or negative. |

| Feature | Option | Description |
|---|---|---|
| PSYS Pmax Power | Value input | PSYS Pmax power, defined in 1/8 Watt or Percent increments. For Watts, Range is 0-8191 (ex. For 125W, enter 1000). For ATX12VO (ex. For 200%, enter 1600). Uses BIOS VR mailbox command 0xB. |
| Min Voltage Override | [Disabled], [Enabled] | Min Voltage Override. Enable to override minimum voltage for runtime and for C8. |
| Min Voltage Runtime / C8 | Value input | Min Voltage for Runtime / Package C8. Range is 0 – 1999mV in 1/128 volt increments. Input is in mVolts. |
| VccIn Aux Icc Max | Value input | Sets the Max Icc VccIn Aux value defined in 1/4A increments. Range is 0 – 512. For an IccMax 32A, enter 128 (32*4). |
| VccIn Aux IMON Slope | Value input | VccIn Aux IMON Slope defined in 1/100 increments. Range is 0 - 200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x18. |
| VccIn Aux IMON Offset | Value input | VccIn Aux IMON Offset defined in 1/1000 increments. Range is 0 - 63999. For an offset of 25.348, enter 25348. IMON Uses BIOS VR mailbox command 0x18. |
| VccIn Aux IMON Prefix | [+], [-] | Set the offset value as positive or negative. |
| Vsys/Psys Critical | [Disabled], [Psys Critical], [Vsys Critical] | Vsys/Psys Critical Enable or disable |
| Vsys/Psys Full Scale / Critical Threshold | Value input | Input Vsys/Psys Full Scale & Critical Threshold. Vsys/Psys Critical = (Critical Threshold / Full Scale). Vsys input is in mVolts. Psys input is in mW or in m% (for ATX12VO) |
| Assertion Deglitch Mantissa | Value input | Assertion Deglitch Mantissa 0x4F [7-3]. Assertion Deglitch = $2\mu\text{s} * \text{Mantissa} * 2^{(\text{Exponent})}$ |
| Assertion Deglitch Exponent | Value input | Assertion Deglitch Exponent 0x4F [3-0]. Assertion Deglitch = $2\mu\text{s} * \text{Mantissa} * 2^{(\text{Exponent})}$ |
| De assertion Deglitch Mantissa | Value input | De Assertion Deglitch Mantissa 0x49 [7-3]. Assertion Deglitch = $2\mu\text{s} * \text{Mantissa} * 2^{(\text{Exponent})}$ |
| De assertion Deglitch Exponent | Value input | De Assertion Deglitch Exponent 0x49 [3-0]. Assertion Deglitch = $2\mu\text{s} * \text{Mantissa} * 2^{(\text{Exponent})}$ |
| VR Power Delivery Design | [AUTO], [ADL P 282 15W], [ADL P 482 28W], [ADL P 682 28W], [ADL P 682 45W], [ADL P 142 15W], [ADL P 242 15W], [ADL P 482 45W], [ADL P 442 45W], [ADL P 442 28W], [ADL P 282 28W], [ADL P 242 28W], | Specifies the ADL Desktop board design used for the VR settings override values. By default, BIOS will override the default Desktop VR settings based on the board design. A value of AUTO (0) will use the board ID to determine the board design. Any other value will override the board ID logic to provide a custom VR Power Delivery Design value. This is intended primarily for validation. |

| Feature | Option | Description |
|---------|---|-------------|
| | [ADL P 142 28W], [ADL P 242 45W], [ADL P 182 28W], [ADL P 662 28W], [ADL P 642 28W], [ADL P 642 45W] | |

Figure 61: BIOS Advanced Menu – Power & Performance – CPU – Power Management Control – CPU VR Settings – Acoustic Noise Settings

| Aptio Setup – AMI | | | |
|--|------------|--|--|
| Advanced | | | |
| Acoustic Noise Settings | | | |
| Acoustic Noise Mitigation | [Disabled] | | |
| Pre Wake Time* | 0 | | |
| Ramp Up Time* | 0 | | |
| Ramp Down Time* | 0 | | |
| IA VR Domain | | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit | |
| Disable Fast PKG C State Ramp for IA Domain* | [FALSE] | | |
| Slow Slew Rate for IA Domain* | [Fast/2] | | |
| GT VR Domain | | | |
| Disable Fast PKG C State Ramp for GT Domain* | [FALSE] | | |
| Slow Slew Rate for GT Domain* | [Fast/2] | | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | | |

*These items are activated only when enabling Acoustic Noise Mitigation.

| Feature | Option | Description |
|---|--|---|
| Acoustic Noise Mitigation | [Disabled], [Enabled] | Enabling this option will help mitigate acoustic noise on certain SKUs when the CPU is in deeper C state. |
| Pre Wake / Ramp Up / Ramp Down Time | Value input | Set the maximum Pre Wake / Ramp Up / Ramp Down randomization time in micro ticks. Range is 0 – 255. This is for acoustic noise mitigation Dynamic Periodicity Alteration (DPA) tuning. |
| Disable Fast PKG C State Ramp for IA Domain | [FALSE], [TRUE] | This option needs to be configured to reduce acoustic noise during deeper C states. [False]: Don't disable Fast ramp during deeper C states; [True]: Disable Fast ramp during deeper C state. |
| Slow Slew Rate for IA Domain | [Fast/2], [Fast/4], [Fast/8], [Fast/16] | Set VR IA Slow Slew Rate for Deep Package C State ramp time; Slow slew rate equals to Fast divided by number, the number is 2, 4, 8, 16 to slow down the slew rate to help minimize acoustic noise. |
| Disable Fast PKG C State Ramp for GT Domain | [FALSE], [TRUE] | This option needs to be configured to reduce acoustic noise during deeper C states. [False]: Don't disable Fast ramp during deeper C states; [True]: Disable Fast ramp during deeper C state. |
| Slow Slew Rate for GT Domain | [Fast/2], [Fast/4], [Fast/8] | Set VR GT Slow Slew Rate for Deep Package C State ramp time; Slow slew rate equals to Fast divided by number, the number is |

| Feature | Option | Description |
|---------|--------|---|
| | | 2, 4, 8 to slow down the slew rate to help minimize acoustic noise; divide by 16 is disabled. |

Figure 62: BIOS Advanced Menu – Power & Performance – CPU – Power Management Control – CPU VR Settings – Core/IA VR Settings

| Aptio Setup – AMI | | |
|--|------------|--|
| Advanced | | |
| Core/IA VR Domain | | |
| VR Config Enable | [Enabled] | |
| Current AC Loadline* | 500 | |
| Current DC Loadline* | 500 | |
| Current Psi1 Threshold* | 16 | |
| Current Psi2 Threshold* | 8 | |
| Current Psi3 Threshold* | 4 | |
| Current Imon Slope* | 0 | |
| Current Imon Offset* | 1 | |
| Current VR Current Limit* | 128 | |
| Current Tdc Current Limit* | 208 | |
| Current Voltage Limit* | 1600 | |
| AC Loadline* | 0 | |
| DC Loadline* | 0 | |
| PS Current Threshold1* | 18 | |
| PS Current Threshold2* | 8 | |
| PS Current Threshold3* | 4 | |
| PS3 Enable* | [Enabled] | |
| PS4 Enable* | [Enabled] | |
| IMON Slope* | 0 | |
| IMON Offset* | 0 | |
| IMON Prefix* | [+] | |
| VR Current Limit* | 0 | |
| VR Voltage Limit* | 0 | |
| TDC Enable* | [Enabled] | |
| TDC Current Limit* | 0 | |
| TDC Time Window* | [1 sec] | |
| TDC Lock* | [Disabled] | |
| IRMS* | [Disabled] | |
| | | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

*These items appear only when enabling VR Config Enable.

| Feature | Option | Description |
|---------------------------|--------------------------|--|
| VR Config Enable | [Disabled], [Enabled] | VR Config Enable |
| AC / DC Loadline | Value input | AC / DC Loadline defined I 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. Range is 0 – 6249 (0 – 62.49 mOhm). 0 = AUTO/HW default. Uses BIOS mailbox command 0x2. |
| PS Current Threshold1/2/3 | Value input | PS Current Threshold1/2/3, defined in 1/4 A increments. A value of 400 = 100 A. Range 0 – 512, which translates to 0 – 128 A. 0 = AUTO. Uses BIOS VR mailbox command 0x3. |
| PS3 / PS4 Enable | [Disabled], [Enabled] | PS3 / PS4 Enable / Disable. 0 – Disabled 1 – Enabled Uses BIOS VR mailbox command 0x3. |
| IMON Slope | Value input | IMON Slope defined in 1/100 increments. Range is 0 – 200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x4. |
| IMON Offset | Value input | IMON Offset defined in 1/1000 increments. Range is 0 – 63999. For an offset of 25.348, enter 25348. IMON Uses BIOS VR mailbox command 0x4. |
| IMON Prefix | [+], [-] | Sets the offset value as positive or negative. |
| VR Current Limit | Value input | Voltage Regulator Current Limit (IccMax). This value represents the Maximum instantaneous current allowed at any given time. The value is represented in 1/4 A increments. 0 means AUTO. Uses BIOS VR mailbox command 0x6. |
| VR Voltage Limit | Value input | Voltage Limit (VMAX). This value represents the Maximum instantaneous voltage allowed at any given time. Range is 0 – 7999 mV. Uses BIOS VR mailbox command 0x8. |
| TDC Enable | [Disabled], [Enabled] | TDC Enable. 0 – Disable 1 - Enable |
| TDC Current Limit | Value input | TDC Current Limit, defined in 1/8 A increments. Range 0 – 32767. For a TDC Current Limit of 125 A, enter 1000. 0 = 0 Amps. Uses BIOS VR mailbox command 0x1A. |

| Feature | Option | Description |
|-----------------|---|---|
| TDC Time Window | [1 sec], [2 sec], [3 sec], [4 sec], [5 sec], [6 sec], [7 sec], [8 sec], [10 sec], [12 sec], [14 sec], [16 sec], [20 sec], [24 sec], [28 sec], [32 sec], [40 sec], [48 sec], [56 sec], [64 sec], [80 sec], [96 sec], [112 sec], [128 sec], [160 sec], [192 sec], [224 sec], [256 sec], [320 sec], [384 sec], [448 sec] | VR TDC Time Window, value in seconds. 1s is default. Range from 1s to 448s. |
| TDC Lock | [Disabled], [Enabled] | TDC Lock |
| IRMS | [Disabled], [Enabled] | Enable / Disable IRMS – Current root mean square |

Figure 63: BIOS Advanced Menu – Power & Performance – CPU – Power Management Control – CPU VR Settings – GT VR Settings

| Aptio Setup – AMI | | |
|--|------------|--|
| Advanced | | |
| GT Domain | | |
| VR Config Enable | [Enabled] | |
| Current AC Loadline* | 650 | |
| Current DC Loadline* | 650 | |
| Current Psi1 Threshold* | 80 | |
| Current Psi2 Threshold* | 20 | |
| Current Psi3 Threshold* | 4 | |
| Current Imon Slope* | 103 | |
| Current Imon Offset* | 1 | |
| Current VR Current Limit* | 116 | |
| Current Tdc Current Limit* | 160 | |
| Current Voltage Limit* | 1519 | |
| AC Loadline* | 0 | |
| DC Loadline* | 0 | |
| PS Current Threshold1* | 80 | |
| PS Current Threshold2* | 20 | |
| PS Current Threshold3* | 4 | |
| PS3 Enable* | [Enabled] | |
| PS4 Enable* | [Enabled] | |
| IMON Slope* | 103 | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| IMON Offset* | 0 | |
| IMON Prefix* | [+] | |
| VR Current Limit* | 0 | |
| VR Voltage Limit* | 0 | |
| TDC Enable* | [Enabled] | |
| TDC Current Limit*# | 0 | |
| TDC Time Window*# | [1 sec] | |
| TDC Lock*# | [Disabled] | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

*These items appear only when enabling VR Config Enable.

These items appear only when enabling TDC Enable.

| Feature | Option | Description |
|------------------|--------------------------|--|
| VR Config Enable | [Disabled], [Enabled] | VR Config Enable |
| AC / DC Loadline | Value input | AC / DC Loadline defined I 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. Range is 0 – 6249 (0 – 62.49 mOhm). |

| Feature | Option | Description |
|---------------------------|---|--|
| | | 0 = AUTO/HW default. Uses BIOS mailbox command 0x2. |
| PS Current Threshold1/2/3 | Value input | PS Current Threshold1/2/3, defined in 1/4 A increments. A value of 400 = 100 A. Range 0 – 512, which translates to 0 – 128 A. 0 = AUTO. Uses BIOS VR mailbox command 0x3. |
| PS3 / PS4 Enable | [Disabled], [Enabled] | PS3 / PS4 Enable / Disable. 0 – Disabled 1 – Enabled Uses BIOS VR mailbox command 0x3. |
| IMON Slope | Value input | IMON Slope defined in 1/100 increments. Range is 0 – 200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x4. |
| IMON Offset | Value input | IMON Offset defined in 1/1000 increments. Range is 0 – 63999. For an offset of 25.348, enter 25348. IMON Uses BIOS VR mailbox command 0x4. |
| IMON Prefix | [+], [-] | Sets the offset value as positive or negative. |
| VR Current Limit | Value input | Voltage Regulator Current Limit (IccMax). This value represents the Maximum instantaneous current allowed at any given time. The value is represented in 1/4 A increments. 0 means AUTO. Uses BIOS VR mailbox command 0x6. |
| VR Voltage Limit | Value input | Voltage Limit (VMAX). This value represents the Maximum instantaneous voltage allowed at any given time. Range is 0 – 7999 mV. Uses BIOS VR mailbox command 0x8. |
| TDC Enable | [Disabled], [Enabled] | TDC Enable. 0 – Disable 1 - Enable |
| TDC Current Limit | Value input | TDC Current Limit, defined in 1/8 A increments. Range 0 – 32767. For a TDC Current Limit of 125 A, enter 1000. 0 = 0 Amps. Uses BIOS VR mailbox command 0x1A. |
| TDC Time Window | [1 sec], [2 sec], [3 sec], [4 sec], [5 sec], [6 sec], [7 sec], [8 sec], [10 sec], [12 sec], [14 sec], [16 sec], [20 sec], [24 | VR TDC Time Window, value in seconds. 1s is default. Range from 1s to 448s. |

| Feature | Option | Description |
|----------|---|-------------|
| | sec], [28 sec], [32 sec], [40 sec], [48 sec], [56 sec], [64 sec], [80 sec], [96 sec], [112 sec], [128 sec], [160 sec], [192 sec], [224 sec], [256 sec], [320 sec], [384 sec], [448 sec] | |
| TDC Lock | [Disabled], [Enabled] | TDC Lock |

Figure 64: BIOS Advanced Menu – Power & Performance – CPU – Power Management Control – CPU VR Settings – RFI Settings

| Aptio Setup – AMI | | |
|--|------------|---|
| Advanced | | |
| RFI Domain | | |
| RFI Current Frequency | 139.200MHz | → ←: Select Screen ↑ ↓ : Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| RFI Frequency | 0 | |
| FIVR Spread Spectrum | [Enabled] | |
| RFI Spread Spectrum* | [1.5%] | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

*This item appears only when enabling FIVR Spread Spectrum.

| Feature | Option | Description |
|----------------------|---|--|
| RFI Frequency | Value input | Set desired RFI frequency, in increments of 100 KHz. (For a frequency of 100.6 MHz, enter 1006.) |
| FIVR Spread Spectrum | [Disabled], [Enabled] | Enable or Disable the FIVR Spread Spectrum |
| RFI Spread Spectrum | [0.5%], [1%], [1.5%], [2%], [3%], [4%], [5%], [6%] | Set the Spread Spectrum |

Figure 65: BIOS Advanced Menu – Power & Performance – CPU – Power Management Control – Custom P-state Table

| Aptio Setup – AMI | | |
|--|---|--|
| Advanced | | |
| Custom P-state Table | | |
| Number of P states | 0 | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|--------------------|-------------|--|
| Number of P states | Value input | Sets the number of custom P-states. At least 2 states must be present. |

Figure 66: BIOS Advanced Menu – Power & Performance – CPU – Power Management Control – Power Limit 3 Settings

| Aptio Setup – AMI | | |
|--|------------|------------------------|
| Advanced | | |
| Power Limit 3 Override | [Disabled] | |
| Power Limit 3* | 0 | |
| Power Limit 3 Time Window* | [0] | → ←: Select Screen |
| Power Limit 3 Duty Cycle* | 0 | ↑ ↓: Select Item |
| Power Limit 3 Lock* | [Disabled] | Enter: Select |
| | | +/-: Change Opt. |
| | | F1: General Help |
| | | F2: Previous Values |
| | | F3: Optimized Defaults |
| | | F4: Save & Exit |
| | | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

*These items appear only when enabling Power Limit 3 Override.

| Feature | Option | Description |
|---------------------------|---|---|
| Power Limit 3 Override | [Disabled], [Enabled] | Enable / Disable Power Limit 3 override. If this option is disabled, BIOS will leave the hardware default values for Power Limit 3 and Power Limit 3 Time Window. |
| Power Limit 3 | Value input | Power Limit 3 in Milli Watts/Percent. BIOS will round to the nearest 1/8W when programming. For example, if 12.50W, enter 12500; if 12%, enter 12000; if 50%, enter 50000. XE SKU: Any value can be programmed. Overclocking SKU: Value must be between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). Other SKUs: This value must be between Min Power Limit and Processor Base Power (TDP) Limit. If the value is 0, BIOS leaves the hardware default value. |
| Power Limit 3 Time Window | [0], [3], [4], [5], [6], [7], [8], [10], [12], [14], [16], [20], [24], [28], [32], [40], [48], [56], [64] | Power Limit 3 Time Window value in Milli seconds. The value may vary from 3 to 64 (max). Indicates the time window over which Power Limit 3 value should be maintained. If the value is 0, BIOS leaves the hardware default value. |
| Power Limit 3 Duty Cycle | Value input | Specify the duty cycle in percentage that the CPU is required to maintain over the configured time window. Range is 0 – 100. |
| Power Limit 3 Lock | [Disabled], [Enabled] | Power Limit 3 MSR 615h Lock. When enabled PL3 configurations are locked during OS. When disabled PL3 configuration can be changed during OS. |

Figure 67: BIOS Advanced Menu – Power & Performance – CPU – Power Management Control – CPU Lock Configuration

| Aptio Setup – AMI | | |
|--|-----------|--|
| Advanced | | |
| CFG Lock | [Enabled] | |
| Overclocking Lock | [Enabled] | |
| | | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|-------------------|--------------------------|--|
| CFG Lock | [Disabled], [Enabled] | Configure MSR 0xE2[15], CGF Lock bit |
| Overclocking Lock | [Disabled], [Enabled] | Enable / Disable Overclocking Lock (BIT 20) in FLEX_RATIO(194) MSR |

Figure 68: BIOS Advanced Menu – Power & Performance – GT – Power Management Control

| Aptio Setup – AMI | | |
|--|-------------------------|--|
| Advanced | | |
| GT – Power Management Control | | |
| RC6(Render Standby) | [Enabled] | |
| Maximum GT frequency | [Default Max Frequency] | |
| Disable Turbo GT frequency | [Disabled] | |
| | | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|----------------------|--------------------------|--|
| RC6(Render Standby) | [Disabled], [Enabled] | Check to enable render standby support. |
| Maximum GT frequency | [Default Max Frequency], | Maximum GT frequency limited by the user. Choose between 200 MHz (RPN) and 1000 MHz (RP0). |

| Feature | Option | Description |
|----------------------------|---|--|
| | [100Mhz], [150Mhz], [200Mhz], [250Mhz], [300Mhz], [350Mhz], [400Mhz], [450Mhz], [500Mhz], [550Mhz], [600Mhz], [650Mhz], [700Mhz], [750Mhz], [800Mhz], [850Mhz], [900Mhz], [950Mhz], [1000Mhz], [1050Mhz], [1100Mhz], [1150Mhz], [1200Mhz] | Value beyond the range will be clipped to min / max supported by SKU. |
| Disable Turbo GT frequency | [Disabled], [Enabled] | [Enabled]: Disable Turbo GT frequency. [Disabled]: GT frequency is not limited. |

Figure 69: BIOS Advanced Menu - Display Configuration

| Aptio Setup – AMI | | |
|--|-----------------|--|
| Advanced | | |
| Display Configuration | | |
| Primary Display | [IGFX] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Internal | [Enabled] | |
| Aperture Size | [256MB] | |
| DVMT Pre-Allocated | [32M] | |
| Primary IGFX Boot Display | [VBIOS Default] | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|---------------------------|--|--|
| Primary Display | [Auto], [IGFX], [PEG Slot], [PCH PCI], [HG] | Select which of IGFX / PEG / PCI Graphics device should be Primary Display or select HG for Hybrid Gfx. |
| Internal Graphics | [Enabled] | Read only item |
| Aperture Size | [128MB], [256MB], [512MB], [1024MB] | Select the Aperture Size. Note: Above 4GB MMIO BIOS assignment is automatically enabled when selecting > 2048MB aperture. To use this feature, please disable CSM Support. |
| DVMT Pre-Allocated | [0M], [32M], [64M], [96M], [128M], [160M], [4M], [8M], [12M], [16M], [20M], [24M], [28M], [32M/F7], [36M], [40M], [44M], [48M], [52M], [56M], [60M] | Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device. |
| Primary IGFX Boot Display | [VBIOS Default], [EFP], [LFP], [EFP3], [EFP2], [EFP4] | Select the Video Device which will be activated during POST. This has no effect if external graphics present. Secondary boot display selection will appear based on your selection. VGA modes will be supported only on primary display. |

Figure 70: BIOS Advanced Menu – PCH-FW Configuration

| Aptio Setup – AMI | | |
|--|---------------|--|
| Advanced | | |
| ME Firmware Version | 16.50.12.1453 | |
| ME Firmware Mode | Normal Mode | |
| ME Firmware SKU | Consumer SKU | |
| ME Firmware Status 1 | 0x90000255 | |
| ME Firmware Status 2 | 0x80100106 | |
| ME Firmware Status 3 | 0x00000020 | |
| ME Firmware Status 4 | 0x00004000 | |
| ME Firmware Status 5 | 0x00000000 | |
| ME Firmware Status 6 | 0x40400002 | |
| ME State | [Enabled] | |
| ME Unconfig on RTC Clear* | [Enabled] | |
| Comms Hub Support* | [Disabled] | |
| JHI Support* | [Disabled] | |
| Core Bios Done Message* | [Enabled] | |
| > Firmware Update Configuration* | | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| > PTT Configuration* | | |
| > FIPS Configuration* | | |
| > ME Debug Configuration* | | |
| > Anti-Rollback SVN Configuration* | | |
| > OEM Key Revocation Configuration* | | |
| Extend CSME Measurement to TPM-PCR | [Disabled] | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when enabling ME State.

| Feature | Option | Description |
|--------------------------|--------------------------|---|
| ME State | [Disabled], [Enabled] | When Disabled ME will be put into ME Temporarily Disabled Mode. |
| ME Unconfig on RTC Clear | [Disabled], [Enabled] | When Disabled ME will not be unconfigured on RTC Clear. |
| Comms Hub Support | [Disabled], [Enabled] | Enables / Disables support for Comms Hub. |
| JHI Support | [Disabled], [Enabled] | Enable / Disable Intel® DAL Host Interface Service (JHI). |
| Core Bios Done Message | [Disabled], [Enabled] | Enable / Disable Core Bios Done message sent to ME. |

| Feature | Option | Description |
|------------------------------------|--------------------------|--|
| Extend CSME Measurement to TPM-PCR | [Disabled], [Enabled] | Enable / Disable Extend CSME Measurement to TPM-PCR[0] and AMT Config to TPM-PCR[1]. |

Figure 71: BIOS Advanced Menu – PCH-FW Configuration – Firmware Update Configuration

| Aptio Setup – AMI | | |
|--|------------|--|
| Advanced | | |
| ME FW Image Re-Flash | [Disabled] | |
| FW Update | [Enabled] | |
| | | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|----------------|--------------------------|---|
| ME FW Re-Flash | [Disabled], [Enabled] | Enable / Disable ME FW Image Re-Flash function. |
| FW Update | [Disabled], [Enabled] | Enable / Disable ME FW Update function. |

Figure 72: BIOS Advanced Menu – PCH-FW Configuration – PTT Configuration

| Aptio Setup – AMI | | |
|--|--------|--|
| Advanced | | |
| PTT Capability / State | 1 / 0 | |
| TPM Device Selection | [dTPM] | |
| | | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|----------------------|------------------|--|
| TPM Device Selection | [dTPM], [PTT] | Selects TPM device: PTT or dTPM. [PTT]: Enables PTT in SkuMgr [dTPM]: Disables PTT in SkuMgr Warning! PTT /dTPM will be disabled and all data saved on it will be lost. |

Figure 73: BIOS Advanced Menu – PCH-FW Configuration – FIPS Configuration

| Aptio Setup – AMI | | |
|--|---------------|--|
| Advanced | | |
| FIPS Mode Select | [Disabled] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Current FIPS mode | Disabled | |
| Crypto driver FIPS version | 16.50.12.1453 | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|------------------|--------------------------|-------------------------|
| FIPS Mode Select | [Disabled], [Enabled] | FIPS Mode configuration |

Figure 74: BIOS Advanced Menu – PCH-FW Configuration – ME Debug Configuration

| Aptio Setup – AMI | | |
|--|---------------|--|
| Advanced | | |
| HECI Timeouts | [Enabled] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Force ME DID Init Status | [Disabled] | |
| CPU Replaced Polling Disable | [Disabled] | |
| HECI Message check Disable | [Disabled] | |
| MBP HOB Skip | [Disabled] | |
| HECI2 Interface Communication | [Disabled] | |
| KT Device | [Enabled] | |
| End Of Post Message | [Send in DXE] | |
| DOI3 Setting for HECI Disable | [Disabled] | |
| MCTP Broadcast Cycle | [Disabled] | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|-------------------------------|--|---|
| HECI Timeouts | [Disabled], [Enabled] | Enable / Disable HECI Send / Receive Timeouts. |
| Force ME DID Init Status | [Disabled], [0 – Success], [1 – No Memory in Channels], [2 – Memory Init Error] | Force the DID Initialization Status value. |
| CPU Replaced Polling Disable | [Disabled], [Enabled] | Setting this option disables CPU replacement polling loop |
| HECI Message check Disable | [Disabled], [Enabled] | Setting this option disables message check for Bios Boot Path when sending |
| MBP HOB Skip | [Disabled], [Enabled] | Setting this option will skip MBP HOB |
| HECI2 Interface Communication | [Disabled], [Enabled] | Adds and Removes HECI2 Device from PCI space. |
| KT Device | [Disabled], [Enabled] | Enable / Disable KT Device |
| End Of Post Message | [Disabled], [Send in DXE] | Enable / Disable End of Post message sent to ME |
| D0I3 Setting for HECI Disable | [Disabled], [Enabled] | Setting this option disables setting D0I3 bit for all HECI devices |
| MCTP Broadcast Cycle | [Disabled], [Enabled] | Enable / Disable Management Component Transport Protocol Broadcast Cycle and Set PMT as Bus Owner |

Figure 75: BIOS Advanced Menu – PCH-FW Configuration – Anti-Rollback SVN Configuration

| Aptio Setup – AMI | | |
|--|------------|--|
| Advanced | | |
| Minimal Allowed Anti-Rollback SVN | 0 | |
| Executing Anti-Rollback SVN | 1 | |
| Automatic HW-Enforced Anti-Rollback SVN | [Disabled] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Set HW-Enforced Anti-Rollback for Current SVN* | [Disabled] | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* This item appears only when disabling Automatic HW-Enforced Anti-Rollback SVN.

| Feature | Option | Description |
|---|--------------------------|--|
| Automatic HW-Enforced Anti-Rollback SVN | [Disabled], [Enabled] | When enabled, hardware-enforced Anti-Rollback mechanism is automatically activated: once ME FW was successfully run on a platform, FW with lower ARB-SVN will be blocked from execution. |
| Set HW-Enforced Anti-Rollback for Current SVN | [Disabled], [Enabled] | Enable hardware-enforced Anti-Rollback mechanism for current ARB-SVN value. FW with lower ARB-SVN will be blocked from execution. The value will be restored to disable after the command is sent. |

Figure 76: BIOS Advanced Menu – PCH-FW Configuration – OEM Key Revocation Configuration

| Aptio Setup – AMI | | |
|--|------------|--|
| Advanced | | |
| Automatic OEM Key Revocation | [Disabled] | |
| Invoke OEM Key Revocation* | [Disabled] | |
| | | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* This item appears only when disabling Automatic OEM Key Revocation.

| Feature | Option | Description |
|------------------------------|--------------------------|---|
| Automatic OEM Key Revocation | [Disabled], [Enabled] | When enabled, BIOS will automatically send HECI command to revoke OEM keys. |
| Invoke OEM Key Revocation | [Disabled], [Enabled] | A HECI command will be send to revoke OEM key. |

Figure 77: BIOS Advanced Menu – Thermal Configuration

| Aptio Setup – AMI | | |
|--|-----------|--|
| Advanced | | |
| Thermal Configuration | | |
| Enable All Thermal Functions | [Enabled] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| > CPU Thermal Configuration | | |
| > Platform Thermal Configuration | | |
| > Intel® Dynamic Tuning Technology Configuration | | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|------------------------------|--------------------------|---|
| Enable All Thermal Functions | [Disabled], [Enabled] | “Enable All Thermal Functions” is Enabled it Enables ‘Memory Thermal Management’, ‘Active Trip Points’, ‘Critical Trip Points’. Set to disabled for Manual Configuration. |

Figure 78: BIOS Advanced Menu – Thermal Configuration – CPU Thermal Configuration

| Aptio Setup – AMI | | |
|--|------------|--|
| Advanced | | |
| CPU Thermal Configuration | | |
| Current Tcc Activation Offset | 0 | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Tcc Activation Offset | 0 | |
| Tcc Offset Time Window | [Disabled] | |
| Tcc Offset Clamp Enable | [Disabled] | |
| Tcc Offset Lock Enable | [Enabled] | |
| Bi-directional PROCHOT# | [Enabled] | |
| Disable PROCHOT# Output | [Enabled] | |
| Disable VR Thermal Alert | [Disabled] | |
| PROCHOT Response | [Enabled] | |
| PROCHOT Lock | [Enabled] | |
| ACPI T-States | [Disabled] | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|-----------------------|-------------|-------------|
| Tcc Activation Offset | Value input | |

| Feature | Option | Description |
|--------------------------|---|---|
| Tcc Offset Time Window | [Disabled], [5 ms], [10 ms], [55 ms], [156 ms], [375 ms], [500 ms], [750 ms], [1 sec], [2 sec], [3 sec], [4 sec], [5 sec], [6 sec], [7 sec], [8 sec], [10 sec], [12 sec], [14 sec], [16 sec], [20 sec], [24 sec], [28 sec], [32 sec], [40 sec], [48 sec], [56 sec], [64 sec], [80 sec], [96 sec], [112 sec], [128 sec], [160 sec], [192 sec], [224 sec], [256 sec], [320 sec], [384 sec], [448 sec] | Tcc Offset Time Window for Running Average Temperature Limit (RATL) feature. The Tcc offset time window can range from 5 ms to 448 s. |
| Tcc Offset Clamp Enable | [Disabled], [Enabled] | Tcc Offset Clamp bit Enable for Running Average Temperature Limit (RATL) feature to allow CPU to throttle below P1. |
| Tcc Offset Lock Enable | [Disabled], [Enabled] | Lock Enable for Running Average Temperature Limit (RATL) feature to lock Temperature Target MSR. |
| Bi-directional PROCHOT# | [Disabled], [Enabled] | When a processor thermal sensor trips (either core), the PROCHOT# will be driven. If bi-direction is enabled, external agents can drive PROCHOT# to throttle the processor. |
| Disable PROCHOT# Output | [Disabled], [Enabled] | Enable / Disable PROCHOT# Output |
| Disable VR Thermal Alert | [Disabled], [Enabled] | Enable / Disable VR Thermal Alert |
| PROCHOT Response | [Disabled], [Enabled] | Enable / Disable PROCHOT Response |
| PROCHOT Lock | [Disabled], [Enabled] | Enable / Disable PROCHOT Lock |
| ACPI T-States | [Disabled], [Enabled] | Enable / Disable ACPI T-States. |

Figure 79: BIOS Advanced Menu – Thermal Configuration – Platform Thermal Configuration

| Aptio Setup – AMI | | |
|--|---------------|------------------------|
| Advanced | | |
| Platform Thermal Configuration | | |
| Critical Trip Point | [119 C (POR)] | |
| Active Trip Point 0 | [71 C] | |
| Active Trip Point 0 Fan Speed | 100 | |
| Active Trip Point 1 | [55 C] | |
| Active Trip Point 1 Fan Speed | 75 | |
| Passive Trip Point | [95 C] | |
| Passive TC1 Value | 1 | |
| Passive TC2 Value | 5 | |
| Passive TSP Value | 10 | |
| Active Trip Points | [Enabled] | |
| Passive Trip Points | [Disabled] | |
| Critical Trip Points | [Enabled] | |
| PCH Temp Read | [Enabled] | |
| CPU Energy Read | [Enabled] | → ←: Select Screen |
| CPU Temp Read | [Enabled] | ↑ ↓: Select Item |
| Alert Enable Lock | [Disabled] | Enter: Select |
| PCH Alert* | [Disabled] | +/-: Change Opt. |
| DIMM Alert* | [Disabled] | F1: General Help |
| CPU Temp | 72 | F2: Previous Values |
| CPU Fan Speed | 65 | F3: Optimized Defaults |
| Boot DTS Read | [Disabled] | F4: Save & Exit |
| | | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when enabling Alert Enable Lock.

| Feature | Option | Description |
|-------------------------|--|---|
| Critical Trip Point | [15 C], [23 C], [31 C], [39 C], [47 C], [55 C], [63 C], [71 C], [79 C], [87 C], [95 C], [100 C], [103 C], [111 C], [119 C (POR)], [127 C], [130 C] | This value controls the temperature of the ACPI Critical Trip Point – the point in which the OS will shut the system off. NOTE: 119 C is the Plan Of Record (POR) for all Intel mobile processors. |
| Active Trip Point 0 / 1 | [Disabled], [15 C], [23 C], [31 C], [39 C], [47 C], [55 C], [63 C], [71 C], [79 C], [87 C], [95 C] | This value controls the temperature of the ACPI Active Trip Point 0 / 1 – the point in which the OS will turn the processor fan on Active Trip Point 0 / 1 Fan Speed. |

| Feature | Option | Description |
|-------------------------------|---|--|
| | C], [103 C], [111 C], [119 C (POR)] | |
| Active Trip Point 0 Fan Speed | Value input | Active Trip Point 0 Fan Speed in percentage. Value must be between 0 (Fan off) – 100 (Max fan speed). This is the speed at which fan will run when Active Trip Point 0 is crossed. |
| Active Trip Point 1 Fan Speed | Value input | Active Trip Point 1 Fan Speed in percentage. Value must be between 0 (Fan off) – 100 (Max fan speed). This value must be less than Active Trip Point 0 Fan Speed. This is the speed at which fan will run when Active Trip 1 is crossed. |
| Passive Trip Point | [Disabled], [15 C], [23 C], [31 C], [39 C], [47 C], [55 C], [63 C], [71 C], [79 C], [87 C], [95 C], [103 C], [111 C], [119 C (POR)] | This value controls the temperature of the ACPI Passive Trip Point – the point in which the OS will begin throttling the processor. |
| Passive TC1/2 Value | Value input | This value sets the TC1/2 value for the ACPI Passive Cooling Formula. Range 1 - 16 |
| Passive TSP Value | Value input | This item sets the TSP value for the ACPI Passive Cooling Formula. It represents in tenths of a second how often the OS will read the temperature when passive cooling is enabled. Range 2 - 32 |
| Active Trip Points | [Disabled], [Enabled] | Disable Active Trip Points |
| Passive Trip Points | [Disabled], [Enabled] | Disable passive Trip Points |
| Critical Trip Points | [Disabled], [Enabled] | Disable Critical Trip Points |
| PCH Temp Read | [Disabled], [Enabled] | PCH Temperature Read Enable |
| CPU Energy Read | [Disabled], [Enabled] | CPU Energy Read Enable |
| CPU Temp Read | [Disabled], [Enabled] | CPU Temperature Read Enable |
| Alert Enable Lock | [Disabled], [Enabled] | Lock all Alert Enable settings |
| PCH Alert | [Disabled], [Enabled] | PCH Alert pin enable |
| DIMM Alert | [Disabled], [Enabled] | DIMM Alert pin enable |
| CPU Temp | Value input | Fail Safe temp that EC will use if OS is hung |
| CPU Fan Speed | Value input | Fan speed that EC will use if OS is hung |
| Boot DTS Read | [Disabled], [Enabled] | Read PCH, CPU DTS Temperature and publish via SMBIOS table |

Figure 80: BIOS Advanced Menu – Thermal Configuration – Intel® Dynamic Tuning Technology Configuration

| Aptio Setup – AMI | | |
|--|---------------------|------------------------|
| Advanced | | |
| Intel® Dynamic Tuning Technology Configuration | | |
| Intel® Dynamic Tuning Technology | [Enabled] | |
| INT3400 Device* | [Enabled] | |
| Processor Thermal Device* | [SA Thermal Device] | |
| PPCC Step Size*(1) | [0.5 Watts] | |
| Intel® Dynamic Tuning Technology Configuration* | 0 | |
| FAN1 Device* | [Enabled] | |
| FAN2 Device* | [Disabled] | |
| FAN3 Device* | [Disabled] | |
| Charger participant* | [Disabled] | |
| Power participant* | [Disabled] | |
| Battery Participant* | [Disabled] | |
| Intel® Dynamic Tuning Technology Battery Sampling Period*(2) | 0 | → ←: Select Screen |
| PCH FIVR Participant* | [Disabled] | ↑ ↓: Select Item |
| | | Enter: Select |
| Sensor Device 1* | [Disabled] | +/-: Change Opt. |
| Sensor Device2* | [Disabled] | F1: General Help |
| Sensor Device 3* | [Disabled] | F2: Previous Values |
| Sensor Device 4* | [Disabled] | F3: Optimized Defaults |
| Sensor Device 5* | [Disabled] | F4: Save & Exit |
| > OEM variable and Object* | | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when enabling Intel® Dynamic Tuning Technology.

(1) This item appears only when selecting [SA Thermal Device] for Processor Thermal Device.

(2) This item appears only when enabling Battery Participant.

| Feature | Option | Description |
|----------------------------------|---|---|
| Intel® Dynamic Tuning Technology | [Disabled], [Enabled] | Enable / Disable Intel Dynamic Platform Thermal Framework |
| INT3400 Device | [Disabled], [Enabled] | Enable / Disable the INT3400 Device. |
| Processor Thermal Device | [Disabled], [SA Thermal Device] | Enable / Disable Processor Thermal Device. |
| PPCC Step Size | [0.5 Watts], [1.0 Watts], [1.5 Watts], [2.0 Watts] | Step size for Turbo power limit (RAPL) control |

| Feature | Option | Description |
|--|--------------------------|--|
| Intel® Dynamic Tuning Technology Configuration | Value input | An Integer containing the Intel® Dynamic Tuning Technology Configuration bitmaps: BIT0[Generic UI Access Control] (0 = enable, 1 = disable) BIT1[Restricted UI Access Control] (0 = enable, 1 = disable) BIT2[shell Access Control] (0 = enable, 1 = disable) BIT3[Environment Monitoring Report Control] (0 = report, 1 = silent) BIT4[Thermal Mitigation Report Control] (0 = silent, 1 = report) BIT5[Thermal Policy Report Control] (0 = silent, 1 = report) |
| FAN1 Device | [Enabled] | Read only item |
| FAN2/3 Device | [Disabled] | Read only item |
| Charger participant | [Disabled], [Enabled] | Enable / Disable Charger device |
| Power participant | [Disabled], [Enabled] | Enable / Disable the Power participant. |
| Battery Participant | [Disabled], [Enabled] | Enable / Disable the Battery Participant. |
| Intel® Dynamic Tuning Technology Battery Sampling Period | Value input | This battery sampling period for the Battery Participant Object. |
| PCH FIVR Participant | [Disabled], [Enabled] | Enable / Disable PCH FIVR Participant |
| Sensor Device 1 / 2 / 3 / 4 / 5 | [Disabled] | Read only item |

Figure 81: BIOS Advanced Menu – Thermal Configuration – Intel® Dynamic Tuning Technology Configuration – OEM variable and Object

| Aptio Setup – AMI | | |
|-------------------------|------------|--------------------|
| Advanced | | |
| OEM variable and Object | | |
| Design Variable 0 | 0 | |
| Design Variable 1 | 0 | |
| Design Variable 2 | 0 | |
| Design Variable 3 | 0 | |
| Design Variable 4 | 0 | |
| Design Variable 5 | 0 | |
| PPCC Object | [Enabled] | |
| ARTG Object | [Enabled] | → ←: Select Screen |
| PMAX Object | [Enabled] | ↑ ↓: Select Item |
| PMAX Device | [Disabled] | Enter: Select |

| Aptio Setup – AMI | | |
|--|------------|------------------------|
| Advanced | | |
| PMAX Audio codec* | [Enabled] | +/-: Change Opt. |
| PMAX WF Camera* | [Enabled] | F1: General Help |
| PMAX UF Camera* | [Enabled] | F2: Previous Values |
| PMAX Flash device* | [Enabled] | F3: Optimized Defaults |
| Processor Thermal Device | | F4: Save & Exit |
| _TMP 1 Object | [Disabled] | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when enabling PMAX Device.

| Feature | Option | Description |
|---------------------------------------|--------------------------|--|
| Design Variable 0 / 1 / 2 / 3 / 4 / 5 | Value input | OEM Design Variable: an integer between 0 – 255. This allows OEM's to customize Intel® Dynamic Tuning Technology behavior based on platform changes. |
| PPCC Object | [Disabled], [Enabled] | Enable / Disable PPCC object for validation. |
| ARTG Object | [Disabled], [Enabled] | Enable / Disable ARTG object for validation. |
| PMAX Object | [Disabled], [Enabled] | Enable / Disable PMAX object for validation. |
| PMAX Device | [Enabled], [Disabled] | Enable / Disable PMAX device for validation. |
| PMAX Audio codec | [Disabled], [Enabled] | Enable / Disable PMAX Audio codec for validation. |
| PMAX WF Camera | [Disabled], [Enabled] | Enable / Disable PMAX WF Camera for validation. |
| PMAX UF Camera | [Disabled], [Enabled] | Enable / Disable PMAX UF Camera for validation. |
| PMAX Flash device | [Disabled], [Enabled] | Enable / Disable PMAX Flash device for validation. |
| _TMP 1 Object | [Disabled], [Enabled] | Enable / Disable _TMP 1 object for validation. |

Figure 82: BIOS Advanced Menu – Platform Settings

| Aptio Setup – AMI | |
|--|------------------------------|
| Advanced | |
| Platform Settings | |
| Charging Method | [Normal Charging] |
| Pseudo G3 | [Disabled] |
| Firmware Configuration | [Test] |
| Scan Matrix Keyboard Support | [Enabled] |
| EC PECI Mode | [Legacy PECI mode] |
| Power Loss Notification Feature | [Default] |
| Device password support | [Enabled] |
| Pmic Vcc IO Level | [Disabled] |
| Pmic Vddq Level | [Disabled] |
| HEBC value | 144371 |
| Pmic SlpS0 VM Support | [Disabled] |
| Power Sharing Manager | [Disabled] |
| Domain Type SPLC 1* | 9 |
| Default Power Limit 1 SPLC* | 4000 |
| Default Time Window 1 SPLC* | 30000 |
| Domain Type DPLC 1* | 9 |
| Domain Preference DPLC 1* | 9 |
| Power Limit Index 1 DPLC* | 0 |
| Default Power Limit 1 DPLC* | 1200 |
| Default Time Window 1 DPLC* | 30000 |
| Minimum Power Limit 1 DPLC* | 1200 |
| Maximum Power Limit 1 DPLC* | 1200 |
| Maximum Time Window 1 DPLC* | 1000 |
| Enable FFU Support | [Disabled] |
| HID Event Filter Driver | [Enabled] |
| System Time and Alarm Source | [ACPI Time and Alarm Device] |
| Enable PowerMeter | [Disabled] |
| MPDT Support | [Disabled] |
| Closed Lid WoV LED Lighting Support | [Disabled] |
| > VTIO | |
| > TCSS Platform Setting | |
| → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit | |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

* These items appear only when enabling Power Sharing Manager.

| Feature | Option | Description |
|---------------------------------|--|--|
| Charging Method | [Normal Charging], [Fast Charging] | Select charging method as Normal Charging or Fast Charging. |
| Pseudo G3 | [Enabled], [Disabled] | Enable / Disable Pseudo G3 |
| Firmware Configuration | [Ignore Policy Update], [Production], [Test] | Firmware Configuration options. NOTE: Ignore Policy Update (STR_FW_CONFIG_DEFAULT_VALUE) is to skip policy update and will ONLY WORK ON A PLATFORM. |
| Scan Matrix Keyboard Support | [Enabled], [Disabled] | Enable Scan Matrix Keyboard Support |
| EC PECI Mode | [Legacy PECI mode], [PECI over eSPI mode] | Switch eSPI PECI Mode or Legacy PECI mode |
| Power Loss Notification Feature | [Disabled], [Enabled], [Default] | Enable / Disable Power Loss Notification Feature |
| Device password support | [Disabled], [Enabled] | Support device password feature |
| Pmic Vcc IO Level | [Disabled], [1.05V], [1.071V], [1.023V], [0.997V], [0.850V], [0.900V], [0.950V] | Select the Pmic Vcc IO Voltage Level |
| Pmic Vddq Level | [Disabled], [0], [1], [2], [3], [4], [5], [6], [7] | Select the Pmic Vddq Voltage Level |
| HEBC value | Value input | HEBC value 32bit |
| Pmic SlpS0 VM Support | [Disabled], [Enabled] | Support to auto check Primium PMIC and disable SlpS0 voltage. |
| Power Sharing Manager | [Disabled], [Enabled] | Configure the PSM ACPI objects. |
| Domain Type SPLC 1 | Code input | 09h: Module (M.2); 07h: WiFi / WLAN; 0Fh: WWAN; 10h: WiGig; |

| Feature | Option | Description |
|-------------------------------------|--|---|
| | | 14h: RFEM |
| Default Power Limit 1 SPLC | Value input | Power Limit in milli watts |
| Default Time Window 1 SPLC | Value input | Time Window in milli seconds |
| Domain Type DPLC 1 | Code input | 09h: Module (M.2); 07h: WiFi / WLAN; 0Fh: WWAN; 10h: WiGig; 14h: RFEM |
| Domain Preference DPLC 1 | Code input | 09h: Module (M.2); 07h: WiFi / WLAN; 0Fh: WWAN; 10h: WiGig; 14h: RFEM |
| Power Limit Index 1 DPLC | Value input | Index of the specific power limit range information |
| Default Power Limit 1 DPLC | Value input | Power Limit in milli watts |
| Default Time Window 1 DPLC | Value input | Time Window in milli seconds |
| Minimum Power Limit 1 DPLC | Value input | Power Limit in milli watts |
| Maximum Power Limit 1 DPLC | Value input | Power Limit in milli watts |
| Maximum Time Window 1 DPLC | Value input | Time Window in milli seconds |
| Enable FFU Support | [Disabled], [Enabled] | Enable / Disable FFU Support. |
| HID Event Filter Driver | [Disabled], [Enabled] | Enables / Disables HID Event Filter Driver interface to OS. |
| System Time and Alarm Source | [ACPI Time and Alarm Device], [Legacy RTC] | Select source of system time and alarm functions. ACPI Time and Alarm (default, legacy RTC disabled) or Legacy RTC support only |
| Enable PowerMeter | [Disabled], [Enabled] | Enables / Disables PowerMeter |
| MPDT Support | [Disabled], [Sensor_BOM1], [Sensor_BOM2], [Sensor_BOM1 with Companion Chip] | Enable (Sensor_BOM1, Sensor_BOM2 and Sensor_BOM1 with Companion Chip) / Disable MPDT Support in BIOS |
| Closed Lid WoV LED Lighting Support | [Enabled], [Disabled] | Disables / Enables Closed Lid WoV LED Lighting Support. |

Figure 83: BIOS Advanced Menu – Platform Settings - VTIO

| Aptio Setup – AMI | |
|--|------------|
| Advanced | |
| VTIO | |
| Enable VTIO Support | [Disabled] |
| Expose ISP SDEV Entry* | [Disabled] |
| Number of Sensor Entries* ⁽¹⁾ | 2 |
| Flags* ⁽¹⁾ | 0 |
| Sensor Entry 1* ⁽¹⁾ | 1 |
| Sensor Entry 2* ⁽¹⁾ | 85 |
| Expose HECI SDEV Entry | [Disabled] |
| Number of Sensor Entries* ⁽²⁾ | 0 |
| Expose SPI1 Dev 1E Fun 2 SDEV Entry* | [Disabled] |
| Number of Sensor Entries* ⁽³⁾ | 1 |
| Flags* ⁽³⁾ | 0 |
| Sensor Entry 1* ⁽³⁾ | 1 |
| Expose SPI2 Dev 1E Fun 3 SDEV Entry* | [Disabled] |
| Number of Sensor Entries* ⁽⁴⁾ | 1 |
| Flags* ⁽⁴⁾ | 0 |
| Sensor Entry 1* ⁽⁴⁾ | 1 |
| Expose XHCI SDEV Entry* | [Disabled] |
| Number of USB Devices* ⁽⁵⁾ | 2 |
| Flags* ⁽⁵⁾ | 0 |
| USB Device 1* ⁽⁵⁾ | |
| Attributes* ⁽⁵⁾ | 0 |
| Root Port Number* ⁽⁵⁾ | 0 |
| VID* ⁽⁵⁾ | 0 |
| PID* ⁽⁵⁾ | 0 |
| Revision* ⁽⁵⁾ | 0 |
| Interface Number* ⁽⁵⁾ | 0 |
| Class* ⁽⁵⁾ | E |
| Subclass* ⁽⁵⁾ | 1 |
| Protocol* ⁽⁵⁾ | 1 |
| ACPI Path String Offset* ⁽⁵⁾ | 34 |

| Aptio Setup – AMI | | |
|--|-------------------------------|------------------------|
| Advanced | | |
| ACPI Path String Length ^{*(5)} | 1E | |
| Firmware Hash [255:192] ^{*(5)} | 0 | |
| Firmware Hash [191:128] ^{*(5)} | 0 | |
| Firmware Hash [127:64] ^{*(5)} | 0 | |
| Firmware Hash [63:0] ^{*(5)} | 0 | |
| ACPI Path Name ^{*(5)} | _SB.PC00.XHCI.RHUB.HS00.CRGB | |
| USB Device 2 ^{*(5)} | | |
| Attributes ^{*(5)} | 0 | |
| Root Port Number ^{*(5)} | 1 | |
| VID ^{*(5)} | 0 | |
| PID ^{*(5)} | 0 | |
| Revision ^{*(5)} | 0 | |
| Interface Number ^{*(5)} | 0 | |
| Class ^{*(5)} | E | |
| Subclass ^{*(5)} | 1 | → ←: Select Screen |
| Protocol ^{*(5)} | 1 | ↑ ↓: Select Item |
| ACPI Path String Offset ^{*(5)} | 34 | Enter: Select |
| ACPI Path String Length ^{*(5)} | 1D | +/-: Change Opt. |
| Firmware Hash [255:192] ^{*(5)} | 0 | F1: General Help |
| Firmware Hash [191:128] ^{*(5)} | 0 | F2: Previous Values |
| Firmware Hash [127:64] ^{*(5)} | 0 | F3: Optimized Defaults |
| Firmware Hash [63:0] ^{*(5)} | 0 | F4: Save & Exit |
| ACPI Path Name ^{*(5)} | _SB.PC00.XHCI.RHUB.HS01.CIR | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when enabling Enable VTIO Support.

(1) These items appear only when enabling Expose ISP SDEV Entry.

(2) These item appears only when enabling Expose HECI SDEV Entry.

(3) These items appear only when enabling Expose SPI1 Dev 1E Fun 2 SDEV Entry.

(4) These items appear only when enabling Expose SPI2 Dev 1E Fun 3 SDEV Entry.

(5) These items appear only when enabling Expose XHCI SDEV Entry.

| Feature | Option | Description |
|-------------------------------------|--------------------------|---|
| Enable VTIO Support | [Disabled], [Enabled] | Enable / Disable VTIO Support. |
| Expose ISP SDEV Entry | [Disabled], [Enabled] | ISP Entry in SDEV table will be exposed based on this option |
| Expose HECI SDEV Entry | [Disabled], [Enabled] | HECI Entry in SDEV table will be exposed based on this option |
| Expose SPI1 Dev 1E Fun 2 SDEV Entry | [Disabled], [Enabled] | SPI1 Entry in SDEV table will be exposed based on this option |
| Expose SPI2 Dev 1E Fun 3 SDEV Entry | [Disabled], [Enabled] | SPI2 Entry in SDEV table will be exposed based on this option |

| Feature | Option | Description |
|---|--------------------------|--|
| Expose XHCI SDEV Entry | [Disabled], [Enabled] | XHCI Entry in SDEV table will be exposed based on this option |
| Number of Sensor Entries | Value input | An array of Sensors Entries |
| Flags | Value input | Enter HEX value BIT[0] – Allow handoff to non-secure OS |
| Sensor Entry 1 / 2 | Value input | Enter HEX value BIT[8:7] – Camera type BIT[6] – Plu-N-Play supported BIT[5:2] – Port ID BIT[1] – Privacy Enabled Sensor present BIT[0] – Embedded Sensor present |
| Attributes | Value input | Enter HEX value BIT[7:1] – Reserved BIT[0] – USB Composite Device 0x0 – A single interface USB device 0x1 – A function on a USB composite device |
| Root Port Number | Value input | Root port number on which the secure device is attached to the root hub. |
| VID | ID input | Vendor ID |
| PID | ID input | Product ID |
| Revision | Revision input | Revision |
| Interface Number | Value input | Interface number (0-based) of the interface on the device that this entry corresponds to. This field is considered valid only if the Attributes indicates that the device is a composite device. |
| Class | Number input | Class Number of the secure device |
| Subclass | Number input | Subclass Number of the secure device |
| Protocol | Number input | Protocol Number of the secure device |
| ACPI Path String Offset | Value input | Offset for fully qualified ACPI path name of the secure device from the beginning of this table |
| ACPI Path String Length | Read only | Read only item |
| Firmware Hash [255:192] / [191:128] / [127:64] / [63:0] | Value input | Firmware Hash [255:192] / [191:128] / [127:64] / [63:0] |
| ACPI Path Name | Path name input | ACPI Path Name. The default value is _SB.PC00.XHCI.RHUB.HS00.CGRB / _SB.PC00.XHCI.RHUB.HS01.CIR |

Figure 84: BIOS Advanced Menu – Platform Settings – TCSS Platform Setting

| Aptio Setup – AMI | | |
|---|------------|------------------------|
| Advanced | | |
| TCSS Platform Setting | | |
| Disable TBT PCIE Tree SME | [Enabled] | |
| USBC connector manager selection | [Disabled] | |
| Aux Ori Override | [Disabled] | |
| Type C retimer TX Compliance Mode | [Enabled] | |
| Type C Port 0* | [Enabled] | |
| Type C Port 1* | [Disabled] | |
| Type C Port 2* | [Disabled] | |
| Type C Port 3* | [Disabled] | |
| BIOS-TCSS handshake | [Enabled] | |
| Timeout for EC USB enumeration message | 500 | → ←: Select Screen |
| USBC and USBA Wake Capability | [S4] | ↑ ↓: Select Item |
| USBC DataRole Swap Platform Disable Option | [TURE] | Enter: Select |
| PD Information | | +/-: Change Opt. |
| PD0 Version | N/A | F1: General Help |
| PD1 Version | N/A | F2: Previous Values |
| Type C Port 1 Conv to TypeA | [Disabled] | F3: Optimized Defaults |
| Type C Port 2 Conv to TypeA Name ⁽⁵⁾ | [Disabled] | F4: Save & Exit |
| | | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when enabling Type C retimer TX Compliance Mode.

| Feature | Option | Description |
|-----------------------------------|--|---|
| Disable TBT PCIE Tree BME | [Disabled], [Enabled] | Disable TBT PCIE RP and child device Tree BME to Enable VTD Base Security |
| USBC connector manager selection | [Disabled], [Enable UCSI Device], [Enable UCMC Device] | Select UCSI or UCMC device in ACPI support based on configuration |
| Aux Ori Override | [Disabled], [Enabled] | Aux Ori Override |
| Type C retimer TX Compliance Mode | [Disabled], [Enabled] | Default is disable Compliance Mode. Change to enabled for Type C retimer Tx Compliance Mode testing. |
| Type C Port 0 / 1 / 2 / 3 | [Disabled], [Enabled] | Enable / Disable Compliance Mode Type C Port 0 / 1 / 2 / 3 |
| BIOS-TCSS handshake | [Disabled], [Enabled] | Enable / Disable BIOS TCSS handshake messages. [Disabled]: TCSS handshake disabled [Enabled]: TCSS handshake with either EC or PMC is enabled based on the board ID |

| Feature | Option | Description |
|--|--------------------------|--|
| Timeout for EC USB enumeration message | Value input | BIOS-EC handshake message USBC_GetUSBConnStatus timeout value in milli seconds |
| USBC and USBA Wake Capability | [S3], [S4] | USBC and USBA Wake Capability |
| USBC DataRole Swap Platform Disable Option | [TRUE], [FALSE] | Enable / Disable setting USBC DataRole Swap Platform Disable Option |
| Type C Port 1 / 2 Conv to TypeA | [Disabled], [Enabled] | Enable / Disable Type C Port 1 / 2 Convert to TypeA |

Figure 85: BIOS Advanced Menu – ACPI D3Cold settings

| Aptio Setup – AMI | | |
|--|------------|------------------------|
| Advanced | | |
| ACPI D3Cold settings | | |
| ACPI D3Cold Support | [Disabled] | |
| VR Ramp up delay* | 16 | |
| PCIE Slot 5 Device Power-on delay in ms* | 100 | |
| Audio Delay* | 200 | |
| SensorHub* | 68 | |
| TouchPad* | 68 | |
| TouchPanel* | 68 | |
| P-state Capping* | [Disabled] | |
| USB Port 1* | [Disabled] | |
| USB Port 2* | [Disabled] | |
| ZPODD* | [Disabled] | |
| WWAN* | [D3/L2] | → ←: Select Screen |
| Sata Port 0* | [Disabled] | ↑ ↓: Select Item |
| Sata Port 1* | [Disabled] | Enter: Select |
| Sata Port 2* | [Disabled] | +/-: Change Opt. |
| Sata Port 3* | [Disabled] | F1: General Help |
| Sata Port 4* | [Disabled] | F2: Previous Values |
| Sata Port 5* | [Disabled] | F3: Optimized Defaults |
| Sata Port 6* | [Disabled] | F4: Save & Exit |
| Sata Port 7* | [Disabled] | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when enabling ACPI D3Cold Support.

| Feature | Option | Description |
|---|--------------------------|--|
| ACPI D3Cold Support | [Disabled], [Enabled] | Enable / Disable ACPI D3Cold support to be executed on D3 entry and exit Note: Disable it would affect the Storage D3 setting |
| VR Ramp up delay | Value input | Delay between subsequent VR ramp ups if they are all Turn ON at the same time |
| PCIE Slot 5 Device Power-on delay in ms | Value input | Delay between applying core power and Deasserting PERST# |
| Audio Delay | Value input | Delay after applying power to HD Audio (Realtek) codec device. |
| SensorHub | Value input | Delay after applying power to SensorHub device. |
| TouchPad | Value input | Delay after applying power to TouchPad device. |
| TouchPanel | Value input | Delay in PR_ON after applying power to TouchPanel device. |
| P-state Capping | [Disabled], [Enabled] | Set _PPC and send ACPI notification |

| Feature | Option | Description |
|----------------|--|--|
| USB Port 1 | [High Speed], [Super Speed], [Disabled] | USB RTD3 support. [Super Speed]: USB 3.0 devices will be exposed as RTD3 capable. [High Speed]: USB 2.0 devices will be exposed as RTD3 capable. [Disabled]: USB RTD3 support disabled. For SawtoothPeak USB Port1 (Below) is Superspeed and Port2 (Top) is HighSpeed. Check respective board configuration to know about USB port position. |
| USB Port 2 | [Disabled], [High Speed], [Super Speed], [Super Speed WWAN] | USB RTD3 support. [Super Speed]: USB 3.0 devices will be exposed as RTD3 capable. [High Speed]: USB 2.0 devices will be exposed as RTD3 capable. [Disabled]: USB RTD3 support disabled. For SawtoothPeak USB Port1 (Below) is Superspeed and Port2 (Top) is HighSpeed. Check respective board configuration to know about USB port position. |
| ZPODD | [Disabled], [Enabled] | Zero Power ODD option is applicable only for the board with ZPODD support. |
| WWAN | [D3/L2] | Read only item |
| Sata Port 0..7 | [Disabled], [Enabled] | Setup option to control the SATA port RTD3 functionality |

Figure 86: BIOS Advanced Menu – BCLK Configuration

| Aptio Setup – AMI | | |
|--|------------|------------------------|
| Advanced | | |
| BCLK Source Config | CPU BCLK | |
| CPU – BCLK Clock Settings | | → ←: Select Screen |
| BCLK Frequency | 100.00 MHz | ↑ ↓: Select Item |
| | | Enter: Select |
| | | +/-: Change Opt. |
| | | F1: General Help |
| | | F2: Previous Values |
| | | F3: Optimized Defaults |
| | | F4: Save & Exit |
| | | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

Read only.

Figure 87: BIOS Advanced Menu – Intel® Time Coordinated Computing

| Aptio Setup – AMI | |
|--|--|
| Advanced | |
| Intel® Time Coordinated Computing (Intel® TCC) | |
| #AC Split Lock | [Disabled] |
| #GP Fault UC Lock | [Disabled] |
| > Intel® TCC Authentication Menu | |
| Intel® TCC Mode | [Disabled] |
| Intel TCC Mode Affected Settings | |
| IO Fabric Low Latency | [Disabled] |
| GT CLOS | [Disabled] |
| > C states ⁽¹⁾ | |
| > Intel® Speed Shift Technology ⁽¹⁾ | |
| > Intel® SpeedStep™ ⁽¹⁾ | |
| > ACPI D3Cold Support ⁽²⁾ | |
| > Low Power S0 Idle Capability ⁽³⁾ | |
| > SA GV ⁽⁴⁾ | |
| > Page Close Idle Timeout ⁽⁴⁾ | |
| > Power Down Mode ⁽⁴⁾ | |
| > RC6 (Render Standby) ⁽⁵⁾ | |
| > DMI Link ASPM Control ⁽⁶⁾ | |
| > Legacy IO Low Latency ⁽⁷⁾ | |
| > CPU PCI Express Configuration | |
| > PCH PCI Express Configuration | |
| | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

- ⁽¹⁾ The sub-menu is redirected to CPU – Power Management Control (see Figure 54) when pressing these items.
- ⁽²⁾ The sub-menu is redirected to ACPI D3Cold settings (see Figure 82) when pressing this item.
- ⁽³⁾ The sub-menu is redirected to RC ACPI Settings (see Figure 46) when pressing this item.
- ⁽⁴⁾ The sub-menu is redirected to Memory Configuration (see Figure 137) when pressing this item.
- ⁽⁵⁾ The sub-menu is redirected to GT – Power Management Control (see Figure 65) when pressing this item.
- ⁽⁶⁾ The sub-menu is redirected to PCI Express Configuration (see Figure 156) when pressing this item.
- ⁽⁷⁾ The sub-menu is redirected to PCH-IO Configuration (see Figure 155) when pressing this item.

| Feature | Option | Description |
|-------------------|--------------------------|---|
| #AC Split Lock | [Enabled], [Disabled] | Enable or Disable Alignment Check Exception (#AC). When enabled, this will assert an #AC when any atomic operation has an operand that crosses two cache lines. |
| #GP Fault UC Lock | [Enabled], [Disabled] | Enable or Disable GP Fault Exception (GP#). When enabled, this will assert an GP# when encountering a Lock to un-cacheable memory before the bus is locked. |
| Intel® TCC Mode | [Disabled], [Enabled] | Enable or Disable Intel® TCC Mode. When enabled, this will modify system settings to improve real-time performance. The |

| Feature | Option | Description |
|-----------------------|--------------------------|--|
| | | full list of settings and their current state are displayed below when Intel® TCC mode is enabled. |
| IO Fabric Low Latency | [Disabled], [Enabled] | Enable or Disable IO Fabric Low Latency. This will turn off some power management in the PCH IO fabrics. This option provides the most aggressive IO Fabric performance settings. S3 state is NOT supported. |
| GT CLOS | [Disabled], [Enabled] | Enable or Disable Graphics Technology (GT) Class of Service. Enable will reduce Gfx LLC allocation to minimize impact of Gfx workload on LLC. |

Figure 88: BIOS Advanced Menu – Intel® Time Coordinated Computing – Intel® TCC Authentication Menu

| Aptio Setup – AMI | |
|--|--------------------|
| Advanced | |
| Intel® TCC Authentication | [OEM Enrolled Key] |
| → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit | |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

| Feature | Option | Description |
|---------------------------|--------------------|----------------|
| Intel® TCC Authentication | [OEM Enrolled Key] | Read only item |

Figure 89: BIOS Advanced Menu – Intel® Time Coordinated Computing – CPU PCI Express Configuration

| Aptio Setup – AMI | |
|---|---|
| Advanced | |
| <p>CPU PCI Express Configuration</p> <p>PCI Express Root Port 1</p> <ul style="list-style-type: none"> > ASPM* > L1 Substates* > PTM* > VC* > Multi-VC* > PCI Express Clock Gating* <p>PCI Express Root Port 2</p> <ul style="list-style-type: none"> > ASPM* > L1 Substates* > PTM* > VC* > PCI Express Clock Gating* <p>PCI Express Root Port 3</p> <ul style="list-style-type: none"> > ASPM* > L1 Substates* > PTM* > VC* > PCI Express Clock Gating* | <p>→ ←: Select Screen</p> <p>↑ ↓: Select Item</p> <p>Enter: Select</p> <p>+/-: Change Opt.</p> <p>F1: General Help</p> <p>F2: Previous Values</p> <p>F3: Optimized Defaults</p> <p>F4: Save & Exit</p> <p>ESC: Exit</p> |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

* The sub-menu is redirected to PCI Express Root Port 1/2/3 (see Figure 150) when pressing these items.

Figure 90: BIOS Advanced Menu – Intel® Time Coordinated Computing – PCH PCI Express Configuration

| Aptio Setup – AMI | |
|---|--|
| Advanced | |
| <p>PCH PCI Express Configuration</p> <p>PCI Express Root Port 3</p> <ul style="list-style-type: none"> > ASPM > L1 Substates > PTM <p>PCI Express Root Port 4</p> <ul style="list-style-type: none"> > ASPM | |

| Aptio Setup – AMI | |
|--|--|
| Advanced | |
| > L1 Substates > PTM PCI Express Root Port 7 > ASPM > L1 Substates > PTM PCI Express Root Port 9 > ASPM > L1 Substates > PTM PCI Express Root Port 10 > ASPM > L1 Substates > PTM | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

Figure 91: BIOS Advanced Menu – Intel® Time Coordinated Computing – PCH PCI Express Configuration – ASPM / L1 Substates / PTM

| Aptio Setup – AMI | |
|----------------------------------|---------------|
| Advanced | |
| PCI Express Root Port 3/4/7/9/10 | [Enabled] |
| Connection Type* | [Slot] |
| ASPM* | [Auto] |
| L1 Substates* | [L1.1 & L1.2] |
| L1 Low* | [Enabled] |
| ACS* | [Enabled] |
| PTM* | [Enabled] |
| DPC* | [Disabled] |
| EDPC* | [Enabled] |
| URR* | [Disabled] |
| FER* | [Disabled] |
| NFER* | [Disabled] |
| CER* | [Disabled] |
| SEFE* | [Disabled] |
| SENF* | [Disabled] |
| SECE* | [Disabled] |

| Aptio Setup – AMI | | |
|---|------------|--|
| Advanced | | |
| PME SCI* | [Enabled] | |
| Hot Plug* | [Disabled] | |
| Advanced Error Reporting* | [Enabled] | |
| PCIe Speed* | [Auto] | |
| Transmitter Half Swing* | [Disabled] | |
| Detect Timeout* | 0 | |
| Extra Bus Reserved* | 0 | |
| Reserved Memory* | 10 | |
| Reserved I/O* | 4 | |
| PCH PCIe LTR Configuration* | | |
| LTR* | [Enabled] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Snoop Latency Override** | [Auto] | |
| Snoop Latency Value** ⁽¹⁾ | 60 | |
| Snoop Latency Multiplier** ⁽¹⁾ | [1024 ns] | |
| Non Snoop Latency Override** | [Auto] | |
| Non Snoop Latency Value** ⁽²⁾ | 60 | |
| Non Snoop Latency Multiplier** ⁽²⁾ | [1024 ns] | |
| LTR Lock* | [Disabled] | |
| Peer Memory Write Enable* | [Disabled] | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when enabling PCI Express Root Port 3/4/7/9/10

These items appear only when enabling LTR.

⁽¹⁾ These items appear only when selecting Manual for Snoop Latency Override.

⁽²⁾ These items appear only when selecting Manual for Mon Snoop Latency Override.

| Feature | Option | Description |
|----------------------------------|---|---|
| PCI Express Root Port 3/4/7/9/10 | [Disabled], [Enabled] | Control the PCI Express Root Port. |
| Connection Type | [Bulit-in], [Slot] | [Built-in]: a built-in device is connected to this rootport. SlotImplemented bit will be clear. [Slot]: this rootport connects to user-accessible slot. SlotImplemented bit will be set. |
| ASPM | [Disabled], [L1], [Auto] | Set the ASPM Level: Force L0s – Force all links to L0s State AUTO – BIOS auto configure DISABLE – Disables ASPM |
| L1 Substates | [Disabled], [L1.1], [L1.1 & L1.2] | PCI Express L1 Substates settings. |
| L1 Low | [Disabled], | PCI Express L1 Low Substates Enable / Disable. |

| Feature | Option | Description |
|--------------------------|---|--|
| | [Enabled] | |
| ACS | [Disabled], [Enabled] | Enable / Disable Access Control Services Extended Capability |
| PTM | [Disabled], [Enabled] | Enable / Disable Precision Time Measurement |
| DPC | [Disabled], [Enabled] | Enable / Disable Downstream Port Containment |
| EDPC | [Disabled], [Enabled] | Enable / Disable Rootport extensions for Downstream Port Containment |
| URR | [Disabled], [Enabled] | PCI Express Unsupported Request Reporting Enable / Disable. |
| FER | [Disabled], [Enabled] | PCI Express Device Fatal Error Reporting Enable / Disable. |
| NFER | [Disabled], [Enabled] | PCI Express Device Non-Fatal Error Reporting Enable / Disable. |
| CER | [Disabled], [Enabled] | PCI Express Device Correctable Error Reporting Enable / Disable. |
| SEFE | [Disabled], [Enabled] | Root PCI Express System Error on Fatal Error Enable / Disable. |
| SENF | [Disabled], [Enabled] | Root PCI Express System Error on Non-Fatal Error Enable / Disable. |
| SECE | [Disabled], [Enabled] | Root PCI Express System Error on Correctable Error Enable / Disable. |
| PME SCI | [Disabled], [Enabled] | PCI Express PME SCI Enable / Disable. |
| Hot Plug | [Disabled], [Enabled] | PCI Express Hot Plug Enable / Disable. |
| Advanced Error Reporting | [Disabled], [Enabled] | Advanced Error Reporting Enable / Disable. |
| PCIe Speed | [Auto], [Gen1], [Gen2], [Gen3] | Configure PCIe Speed |
| Transmitter Half Swing | [Disabled], [Enabled] | Transmitter Half Swing Enable / Disable. |
| Detect Timeout | Value input | The number of milliseconds reference code will wait for link to exit Detect state for enabled ports before assuming there is no device and potentially disabling the port. |
| Extra Bus Reserved | Value input | Extra Bus Reserved (0-7) for bridges behind this Root Bridge. |
| Reserved Memory | Value input | Reserved Memory for this Root Bridge (1-20) MB |
| Reserved I/O | Value input | Reserved I/O (4K/8K/12K/16K/20K) Range for this Root Bridge. |
| LTR | [Disabled], [Enabled] | PCH PCIE Latency Reporting Enable / Disable |

| Feature | Option | Description |
|------------------------------|--|---|
| Snoop Latency Override | [Disabled], [Manual], [Auto] | Snoop Latency Override for PCH PCIE. [Disabled]: Disable override. [Manual]: Manually enter override values. [Auto] (default): Maintain default BIOS flow. |
| Snoop Latency Value | Value input | LTR Snoop Latency value of PCH PCIE |
| Snoop Latency Multiplier | [1 ns], [32 ns], [1024 ns], [32768 ns], [1048576 ns], [33554432 ns] | LTR Snoop Latency Multiplier of PCH PCIE |
| Non Snoop Latency Override | [Disabled], [Manual], [Auto] | Non Snoop Latency Override for PCH PCIE. [Disabled]: Disable override. [Manual]: Manually enter override values. [Auto] (default): Maintain default BIOS flow. |
| Non Snoop Latency Value | Value input | LTR Non Snoop Latency value of PCH PCIE |
| Non Snoop Latency Multiplier | [1 ns], [32 ns], [1024 ns], [32768 ns], [1048576 ns], [33554432 ns] | LTR Non Snoop Latency Multiplier of PCH PCIE |
| LTR Lock | [Disabled], [Enabled] | PCIE LTR Configuration Lock |
| Peer Memory Write Enable | [Disabled], [Enabled] | Peer Memory Write Enable / Disable |

Figure 92: BIOS Advanced Menu – Functional Safety Configuration

| Aptio Setup – AMI | | |
|--|--------------------|--|
| Advanced | | |
| Functional Safety Configuration | | |
| Fusa Enable | [Disabled] | |
| Startup Array BIST options | | |
| Enable Startup Array BIST | [Disabled] | |
| Startup Scan BIST options | | |
| Enable Startup Scan BIST | [Disabled] | |
| Periodic Scan BIST options | | |
| Enable Periodic Scan BIST | [Disabled] | |
| Lock Step options for module 0 | | |
| Core Lockstep Configuration | [Disable lockstep] | |
| Lock Step options for module 1 | | |
| Core Lockstep Configuration | [Disable lockstep] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Display Fusa Configuration | [Enabled] | |
| Graphics Fusa Configuration | [Enabled] | |
| Opio Fusa Configuration | [Enabled] | |
| Psf Fusa Configuration | [Disabled] | |
| Iop Fusa Configuration | [Enabled] | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|---------------------------|--------------------------|---|
| Fusa Enable | [Disabled], [Enabled] | Enable / Disable all Functional Safety (FUSA) feature |
| Enable Startup Array BIST | [Disabled], [Enabled] | Enabling this will execute startup array test during boot |
| Enable Startup Scan BIST | [Disabled], [Enabled] | Enabling this will execute startup scan test during boot |

| Feature | Option | Description |
|-----------------------------|--|---|
| Enable Periodic Scan BIST | [Disabled], [Enabled] | Enabling this will execute periodic scan test during boot |
| Core Lockstep Configuration | [Disable lockstep], [Enable lockstep for Core 0 with Core 1, Core 2 with Core 3], [Enable lockstep for Core 0 with Core 1], [Enable lockstep for Core 2 with Core 3] | Enable / Disable Lockstep for Efficient-core module, which has 4 cores each |
| Display Fusa Configuration | [Disabled], [Enabled] | Enable / Disable Functional Safety (FUSA) on Display |
| Graphics Fusa Configuration | [Disabled], [Enabled] | Enable / Disable Functional Safety (FUSA) on Graphics |
| Opio Fusa Configuration | [Disabled], [Enabled] | Enable / Disable Functional Safety (FUSA) on Opio |
| Psf Fusa Configuration | [Disabled], [Enabled] | Enable / Disable Functional Safety (FUSA) on Psf |
| Iop Fusa Configuration | [Disabled], [Enabled] | Enable / Disable Functional Safety (FUSA) on Iop |

Figure 93: BIOS Advanced Menu – Debug Settings

| Aptio Setup – AMI | | |
|--|---------------|--|
| Advanced | | |
| Debug Settings | | |
| Kernel Debug Serial Port | [Legacy UART] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Serial Io Uart Debug Power Gating* | [Disabled] | |
| Kernel Debug Patch | [Disabled] | |
| Debug Token is present | No | |
| Platform Debug Consent | [Disabled] | |
| > VT-d Debug Settings | | |
| > Advanced Debug Settings | | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* This item appears only when selecting SERIALIO UART0 for Kernel Debug Serial Port.

| Feature | Option | Description |
|-----------------------------------|---|--|
| Kernel Debug Serial Port | [Legacy UART], [SERIALIO UART0] | Select Kernel Debug Port and report in ACPI DBG2 table |
| Serial Io Uart Debug Power Gating | [Disabled], [Enabled] | For S0iX support with Kernel Debugger Enabled. BIOS needs to change DBG2 Port Sub Type as value of 0x14 (0x0014 Intel LPSS) Note: Requires OS support |
| Kernel Debug Patch | [Disabled], [Enabled] | Enable / Disable Kernel Debug Patch |
| Platform Debug Consent | [Disabled], [Enabled (All Probes+TraceHub)], [Enabled (Low Power)], [Manual] | Enabled (All Probes+TraceHub) supports all probes with TraceHub enabled and blocks s0ix. Enabled (Low Power) Tracehub is powergated by default, s0ix is viable. Manual: user needs to configure Advanced Debug Settings manually, aimed at advanced users. |

Figure 94: BIOS Advanced Menu – Debug Settings – VT-d Debug Settings

| Aptio Setup – AMI | | |
|--|-----------|--|
| Advanced | | |
| IGD VTD Enable | [Enabled] | |
| IPU VTD Enable | [Enabled] | |
| IOP VTD Enable | [Enabled] | |
| | | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|----------------|--------------------------|--------------------------|
| IGD VTD Enable | [Enabled], [Disabled] | Enable / Disable IGD VTD |
| IPU VTD Enable | [Enabled], [Disabled] | Enable / Disable IPU VTD |
| IOP VTD Enable | [Enabled], [Disabled] | Enable / Disable IOP VTD |

Figure 95: BIOS Advanced Menu – Debug Settings – Advanced Debug Settings

| Aptio Setup – AMI | | |
|---|-----------------------|--|
| Advanced | | |
| USB3 Type-C UFP2DFP Kernel/Platform Debug Support | [No Change] | |
| USB DbC Enable Mode | [No Change] | |
| PCH Trace Hub Enable Mode | [Disabled] | |
| CPU Trace Hub Enable Mode | [Disabled] | |
| CPU Run Control | [No Change] | |
| CPU Run Control Lock ⁽¹⁾ | [Enabled] | |
| USB Overcurrent Override for VISA | [Disabled] | |
| Processor trace memory allocation | [Disabled] | |
| Processor trace ⁽²⁾ | [Disabled] | |
| Processor Trace OutPut Scheme ⁽²⁾ | [Single Range Output] | |
| SMM Processor Trace ⁽²⁾ | [Disabled] | |
| JTAG C10 Power Gate | [Enabled] | |
| Three Strike Counter | [Enabled] | |
| | | → ←: Select Screen ↑ ↓: Select Item |

| Aptio Setup – AMI | | |
|--|------------|------------------------|
| Advanced | | |
| CrashLog Feature | [Enabled] | Enter: Select |
| CrashLog On All Reset ⁽³⁾ | [Disabled] | +/-: Change Opt. |
| CrashLog Rearm Enable ⁽³⁾ | [Enabled] | F1: General Help |
| CrashLog Clear Enable ⁽³⁾ | [Disabled] | F2: Previous Values |
| CrashLog GPRs ⁽³⁾ | [Disabled] | F3: Optimized Defaults |
| PMC Debug Message Enable | [Disabled] | F4: Save & Exit |
| Delayed Authentication Mode | [Disabled] | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

⁽¹⁾ This item appears only when selecting Disabled or Enabled for CPU Run Control.

⁽²⁾ These items appear only when enabling Processor trace memory allocation.

⁽³⁾ These items appear only when enabling CrashLog Feature.

| Feature | Option | Description |
|---|--|---|
| USB3 Type-C UFP2DFP Kernel/Platform Debug Support | [Disabled], [Enabled], [No Change] | This BIOS option enables kernel and platform debug for USB3 interface over a UFP Type-C receptacle, select 'No Change' will do nothing to UFP2DFP setting. |
| USB DbC Enable Mode | [Disabled], [USB2], [USB3], [Both], [No Change] | [Disabled]: Clear both USB2/3DBCEN [USB2]: Set USB2DBCEN [USB3]: Set USB3DBCEN [Both]: Set both USB2/3DBCEN [No Change]: Comply with HW value |
| PCH / CPU Trace Hub Enable Mode | [Disabled] | Read only item |
| CPU Run Control | [Disabled], [Enabled], [No Change] | Enable / Disable CPU Run Control Support [No Change]: Comply with HW value |
| CPU Run Control Lock | [Disabled], [Enabled] | Enable / Disable CPU Run Control Lock |
| USB Overcurrent Override for VISA | [Disabled], [Enabled] | This option overrides USB Over Current enablement state that USB OC will be considered after enabling this option. Enable when VISA pin is muxed with USB OC. |
| Processor trace memory allocation | [Disabled], [4KB], [8KB], [16KB], [32KB], [64KB], [128KB], [256KB], [512KB], [1MB], [2MB], [4MB], [8MB], [32MB], [64MB], [128MB] | Disable or Select Processor trace memory region size: from 4KB ~ 128MB. |
| Processor trace | [Disabled], [Enabled] | Enable / Disable processor trace feature from CPU MSR. Enabling this feature will immediately start trace collection. |
| Processor Trace OutPut Scheme | [Single Range Output], [ToPA Output] | Select Single Range Output scheme or ToPA table Output scheme |

| Feature | Option | Description |
|-----------------------------|--|---|
| SMM Processor Trace | [Disabled], [Enabled] | Enable / Disable usage of Processor Trace in SMM |
| JTAG C10 Power Gate | [Disabled], [Enabled] | When Enabled, JTAG is power gated in C10 state. When Disabled, keeps the JTAG power up during C10 and deeper power states for debug purpose. |
| Three Strike Counter | [Disabled], [Enabled] | Enable / Disable Three Strike Counter |
| CrashLog Feature | [Disabled], [Enabled] | The feature helps collecting crash data from PMC SSRAM |
| CrashLog On All Reset | [Disabled], [Enabled] | Option to invoke CrashLog collection on all reset |
| CrashLog Rearm Enable | [Disabled], [Enabled] | Option to invoke crashlog re-arm |
| CrashLog Clear Enable | [Disabled], [Enabled] | Option to invoke CrashLog clear |
| CrashLog GPRs | [Disabled], [Enabled], [Gprs Enabled, Smm Gprs Disabled] | Helps collecting crash data from PMC SSRAM. Enabling this may expose personal or confidential information that may be held in the GPRs at the time of the Crash trigger. |
| PMC Debug Message Enable | [Disabled], [Enabled] | When Enabled, PMC HW will send debug messages to trace hub; When Disabled, PMC HW will never send debug messages to trace hub. Note: When Enabled, may not enter S0ix. |
| Delayed Authentication Mode | [Disabled], [Enabled] | Enable / Disable Delayed Authentication Mode |

Figure 96: BIOS Advanced Menu – Debug Configuration

| Aptio Setup – AMI | | |
|--|--------------------------------|--|
| Advanced | | |
| Debug Configuration | | |
| RAM | [Disabled] | |
| Legacy UART | [Enabled] | |
| USB3 | [Disabled] | |
| Serial IO UART | [Disabled] | |
| Trace Hub | [Disabled] | |
| MRC Serial Debug Messages | [Disabled] | |
| Serial Debug Messages | [Load, Error, Warnings & Info] | |
| Serial Debug Message Baud Rate | [115200] | |
| Serial IO Debug Controller Configuration | | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Controller Number* | [Serial IO UART 0] | |
| Baud Rate* | [115200] | |
| Stop Bits* | [1] | |
| Parity Bits* | [None] | |
| Flow Control* | [Disabled] | |
| Word Length* | [8 BITS] | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when enabling Serial IO UART.

| Feature | Option | Description |
|---------------------------|--|--|
| RAM | [Disabled], [Enabled] | Debug Messages Interface |
| Legacy UART | [Disabled], [Enabled] | Debug Messages Interface |
| USB3 | [Disabled], [Enabled] | Debug Messages Interface |
| Serial IO UART | [Disabled], [Enabled] | Debug Messages Interface |
| Trace Hub | [Disabled], [Enabled] | Debug Messages Interface |
| MRC Serial Debug Messages | [Disabled], [Error Only], [Error & Warnings], [Load, Error, Warnings & Info], [Load, Error, Warnings, Info & Event], [Load, Error, Warnings, Info & Verbose] | Enable / Disable MRC Serial Debug Messages |

| Feature | Option | Description |
|--------------------------------|--|---|
| Serial Debug Messages | [Disabled], [Error Only], [Error & Warnings], [Load, Error, Warnings & Info], [Load, Error, Warnings, Info & Event], [Load, Error, Warnings, Info & Verbose] | Enable / Disable some Platform Serial Debug Messages |
| Serial Debug Message Baud Rate | [9600], [19200], [57600], [115200] | Baud Rate for Serial Debug Messages |
| Controller Number | [Serial IO UART 0], [Serial IO UART 1], [Serial IO UART 2] | Pch Integrated UART controller number |
| Baud Rate | [9600], [19200], [57600], [115200], [460800], [921600], [1500000], [1843200], [3000000], [3686400], [6000000] | Serial IO transmission speed in baud [Bd] per second |
| Stop Bits | [Default], [1], [1.5], [2] | Number of stop bits. This is used to select the number of stop bits per character that the peripheral transmits and receives. |
| Parity Bits | [Default], [None], [Even], [Odd] | Enable and disable parity generation and detection in transmitted and received serial character. |
| Flow Control | [Disabled], [Enabled] | Auto or None. Used to help for flow control using external IO pins with the pairing device. |
| Word Length | [5 BITS], [6 BITS], [7 BITS], [8 BITS] | Select the number of data bits per character that the peripheral transmits and receives. |

Figure 97: BIOS Advanced Menu - Trusted Computing

| Aptio Setup – AMI | | |
|--|----------------|--|
| Advanced | | |
| TPM 2.0 Device Found | | |
| Firmware Version: | 16.13 | |
| Vendor: | IFX | |
| Security Device Support | [Enabled] | |
| Active PCR banks* | SHA256 | |
| Available PCR banks* | SHA256, SHA384 | |
| SHA256 PCR Bank* | [Enabled] | |
| SHA384 PCR Bank* | [Disabled] | |
| Pending operation* | [None] | |
| Platform Hierarchy* | [Enabled] | |
| Storage Hierarchy* | [Enabled] | |
| Endorsement Hierarchy* | [Enabled] | |
| Physical Presence Spec Version* | [1.3] | |
| TPM 2.0 Interface Type* | [TIS] | |
| Device Select* | [Auto] | |
| | | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when enabling Security Device Support.

| Feature | Option | Description |
|--------------------------------|--------------------------|---|
| Security Device Support | [Disabled], [Enabled] | Enable or Disable BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available. |
| SHA256 PCR Bank | [Disabled], [Enabled] | Enable or Disable SHA256 PCR Bank |
| SHA384 PCR Bank | [Disabled], [Enabled] | Enable or Disable SHA384 PCR Bank |
| Pending operation | [None], [TPM Clear] | Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change State of Security Device. |
| Platform Hierarchy | [Disabled], [Enabled] | Enable or Disable Platform Hierarchy |
| Storage Hierarchy | [Disabled], [Enabled] | Enable or Disable Storage Hierarchy |
| Endorsement Hierarchy | [Disabled], [Enabled] | Enable or Disable Endorsement Hierarchy |
| Physical Presence Spec Version | [1.2], [1.3] | Select to Tell O.S. to support PPI Spec Version 1.2 or 1.3. Note some HCK tests might not support 1.3. |

| Feature | Option | Description |
|------------------------|------------------------------------|--|
| TPM 2.0 Interface Type | [TIS] | Read only item |
| Device Select | [TPM 1.2], [TPM 2.0], [Auto] | TPM 1.2 will restrict support to TPM 1.2 devices, TPM 2.0 will restrict support to TPM 2.0 devices, Auto will support both with default set to TPM 2.0 devices if not found, TPM 1.2 devices will be enumerated. |

Figure 98: BIOS Advanced Menu – ACPI Settings

| Aptio Setup – AMI | | |
|--|-----------------------|--|
| Advanced | | |
| ACPI Settings | | |
| Enable ACPI Auto Configuration | [Disabled] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Enable Hibernation* | [Enabled] | |
| ACPI Sleep State* | [S3 (Suspend to RAM)] | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when disabling Enable ACPI Auto Configuration.

| Feature | Option | Description |
|--------------------------------|--|--|
| Enable ACPI Auto Configuration | [Disabled], [Enabled] | Enables or Disables BIOS ACPI Auto Configuration. |
| Enable Hibernation | [Disabled], [Enabled] | Enables or Disables System ability to Hibernate (OS/S4 Sleep State). This option may not be effective with some operating systems. |
| ACPI Sleep State | [Suspend Disabled], [S3 (Suspend to RAM)] | Select the highest ACPI sleep state the system will enter when the SUSPEND button is pressed. |

Figure 99: BIOS Advanced Menu – Miscellaneous

| Aptio Setup – AMI | | |
|---|------------------|------------------------|
| Advanced | | |
| Miscellaneous Configuration | | |
| > Preset DIO in BIOS > Control KSC firmware > Update KSC firmware > Generic eSPI Decode Ranges > Watchdog | | |
| Reset Button Behavior | [Chipset Reset] | |
| I2C Speed | [100 KHz] | → ←: Select Screen |
| Onboard I2C Mode | [Multimaster] | ↑ ↓: Select Item |
| Manufacturing mode | [Disabled] | Enter: Select |
| BIOS Test Mode | [Disabled] | +/-: Change Opt. |
| Last system reset through | [Power-on reset] | F1: General Help |
| Create GSPI ACPI dev | [Disabled] | F2: Previous Values |
| PCIe Wake | [Disabled] | F3: Optimized Defaults |
| | | F4: Save & Exit |
| Onboard EEPROM Write Protect | [WP Enabled] | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|------------------------------|--|--|
| Reset Button Behavior | [Chipset Reset], [Power Cycle] | Select Reset Button Behavior: Chipset Reset & Power Cycle. |
| I2C Speed | [100 KHz], [400 KHz], [1 MHz] | Select I2C Bus Speed in KHz. For a default system 100 KHz should be an appropriate value. |
| Onboard I2C Mode | [Multimaster], [Busclear] | MultiMaster / BusClear |
| Manufacturing mode | [Disabled] | Read only item |
| BIOS Test Mode | [Disabled] | Read only item |
| Last system reset through | [Power-on reset] | Read only item |
| Create GSPI ACPI dev | [Disabled], [Kontron Linux BSP], [Win10 RhProxy style] | If set to 'Kontron Linux BSP' then a generic GSPI device will be used by Kontron Linux BSP. 'Win10 RhProxy style' supports this driver type under Win10. |
| PCIe Wake | [Disabled], [Enabled] | Set to enable or disable PCIe wake. This would affect features such as Wake 0/1 and Wake from Lan (WOL). |
| Onboard EEPROM Write Protect | [WP Disabled], [WP Enabled] | Set WP enable or disable the Onboard EEPROM Write Protect |

Figure 100: BIOS Advanced Menu – Miscellaneous – Preset DIO in BIOS

| Aptio Setup – AMI | | |
|---|------------|--|
| Advanced | | |
| Allows to preset GPIOs during BIOS startup. | | |
| Control DIO in BIOS | [Disabled] | |
| DIO #0* | [Skip] | |
| Output level ^{*(1)} | [Low] | |
| DIO #1* | [Skip] | |
| Output level ^{*(1)} | [Low] | |
| DIO #2* | [Skip] | |
| Output level ^{*(1)} | [Low] | |
| DIO #3* | [Skip] | |
| Output level ^{*(1)} | [Low] | |
| DIO #4* | [Skip] | |
| Output level ^{*(1)} | [Low] | |
| DIO #5* | [Skip] | |
| Output level ^{*(1)} | [Low] | |
| DIO #6* | [Skip] | |
| Output level ^{*(1)} | [Low] | |
| DIO #7* | [Skip] | |
| Output level ^{*(1)} | [Low] | |
| | | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when enabling Control DIO in BIOS.

⁽¹⁾ This item appears only when selecting Output for DIO #0/1/2/3/4/5/6/7 respectively.

| Feature | Option | Description |
|---------------------|---------------------------------|--|
| Control DIO in BIOS | [Disabled], [Enabled] | Enables or disables DIO GPIO control in BIOS. If set to 'disabled' then the GPIOs are not touched by BIOS. |
| DIO #0..7 | [Input], [Output], [Skip] | Determine the type of the DIO configuration. If this is set to 'Skip' then this GPIO will be left untouched. |
| Output level | [Low], [High] | Set the level of a DIO pin |

Figure 101: BIOS Advanced Menu – Miscellaneous – Control KSC firmware

| Aptio Setup – AMI | |
|---|-----------|
| Advanced | |
| Allows to control KSC firmware related settings. | |
| Lock FW update access | [Enabled] |
| > KSC OTP area control | |
| → ←: Select Screen ↑ ↓ : Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit | |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

| Feature | Option | Description |
|-----------------------|--------------------------|---|
| Lock FW update access | [Disabled], [Enabled] | Locks access to KSC firmware area during runtime. |

Figure 102: BIOS Advanced Menu – Miscellaneous – Control KSC firmware – KSC OTP area control

| Aptio Setup – AMI | |
|---|-----------|
| Advanced | |
| Allows to control KSC OTP area related settings. | |
| KSC OTP access lock | [Enabled] |
| → ←: Select Screen ↑ ↓ : Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit | |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

| Feature | Option | Description |
|---------------------|-----------|----------------|
| KSC OTP access lock | [Enabled] | Read only item |

Figure 103: BIOS Advanced Menu – Miscellaneous – Update KSC firmware

| Aptio Setup – AMI | | |
|--|------------|--|
| Advanced | | |
| Allows to update KSC firmware from BIOS. | | |
| Auto update KSC FW | [Disabled] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|--------------------|--------------------------|--|
| Auto update KSC FW | [Disabled], [Enabled] | Updates KSC firmware to BIOS internal version (best known config) on next system start. To update FW set item to 'Enabled' and exit the setup using 'Save changes and exit'. |

Figure 104: BIOS Advanced Menu – Miscellaneous – Generic eSPI Decode Ranges

| Aptio Setup – AMI | | |
|--|------------|--|
| Advanced | | |
| Generic eSPI Decode Ranges | | |
| Generic LPC via eSPI Decode 1 | [Disabled] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Base Address* | 100 | |
| Length* | 8 | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when enabling Generic LPC via eSPI Decode 1.

| Feature | Option | Description |
|-------------------------------|--------------------------|---|
| Generic LPC via eSPI Decode 1 | [Disabled], [Enabled] | Enable generic LPC via eSPI decode range. |
| Base Address | Value input | Base address of the generic decode range. |

| Feature | Option | Description |
|---------|-------------|--|
| | | Valid between 0100h – FFF0h. Must be 8-byte aligned. Please note that it also has to be length-aligned. |
| Length | Value input | Length of the generic decode range in hexadecimal notation. Valid between 0008h – 0100h. Must be multiple of 8h. |

Figure 105: BIOS Advanced Menu – Miscellaneous – Watchdog

| Aptio Setup – AMI | | |
|--|------------|--|
| Advanced | | |
| Watchdog Configuration. | | |
| Auto-reload | [Disabled] | |
| Global Lock | [Disabled] | |
| WDT Strobe | [Disabled] | |
| Stage 1 Mode | [Disabled] | |
| Assert WDT Signal ⁽¹⁾ | [Disabled] | |
| Stage 1 Timeout ⁽²⁾ | [1m] | → ←: Select Screen ↑ ↓: Select Item |
| Stage 2 Mode ⁽³⁾ | [Delay] | Enter: Select |
| Assert WDT Signal ⁽¹⁾ | [Disabled] | +/-: Change Opt. |
| Stage 2 Timeout ⁽²⁾ | [1m] | F1: General Help |
| Stage 3 Mode ⁽³⁾ | [Delay] | F2: Previous Values |
| Assert WDT Signal ⁽¹⁾ | [Disabled] | F3: Optimized Defaults |
| Stage 3 Timeout ⁽²⁾ | [1m] | F4: Save & Exit |
| | | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

⁽¹⁾ This item appears only when selecting Reset or Delay for Stage 1/2/3 Mode.

⁽²⁾ This item appears only when selecting Reset, Delay or WDT Signal only for Stage 1/2/3 Mode.

⁽³⁾ This item appears only when selecting Delay or WDT Signal only for Stange N-1 Mode.

| Feature | Option | Description |
|------------------|--|---|
| Auto-reload | [Disabled], [Enabled] | Enable automatic reload of watchdog timers on timeout. |
| Global Lock | [Disabled], [Enabled] | If set to enabled, all Watchdog registers (except WD_KICK) become read only until the board is reset. |
| WDT Strobe | [Disabled], [Enabled] | Enable / disable WDT Strobe input. |
| Stage 1/2/3 Mode | [Disabled], [Reset], [Delay], [WDT Signal only] | Select Action for this Watchdog stage |

| Feature | Option | Description |
|---------------------|-----------------------------------|---|
| Assert WDT Signal | [Disabled], [Enabled] | Enable / disable assertion of WDT signal to baseboard on stage timeout. |
| Stage 1/2/3 Timeout | [1m], [3m], [10m], [30m] | Select Timeout value for this Watchdog stage |

Figure 106: BIOS Advanced Menu – SMART Settings

| Aptio Setup – AMI | | |
|--|------------|---|
| Advanced | | |
| SMART Settings | | |
| SMART Self Test | [Disabled] | → ←: Select Screen ↑ ↓ : Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|-----------------|--------------------------|--|
| SMART Self Test | [Disabled], [Enabled] | Run SMART Self Test on all HDDs during POST. |

Figure 107: BIOS Advanced Menu – H/W Monitor

| Aptio Setup – AMI | | |
|--|---|------------------------|
| Advanced | | |
| KSC based H/W Monitor | | |
| Temperature sensors: | | |
| #1: CPU Temp | : | + 38.8 C |
| #2: PCH Temp | : | + 35.0 C |
| #3: SYSTEM Temp | : | + 35.0 C |
| Voltage sensors: | | |
| #1: V_IN | : | 9.1 V |
| #2: 12V_S0 | : | 8.1 V |
| #3: 5V_S0 | : | 5.1 V |
| #4: 3V3_S0 | : | 3.4 V |
| #5: 3V_BAT | : | 2.9 V |
| Fan speed & control: | | |
| #1: CPU Fan | : | 4200 RPM |
| Fan Control | : | [Auto] |
| Signal Filter Control** | : | [Auto] |
| Signal Filter** ⁽¹⁾ | : | Enabled |
| Fan Pulse** | : | [Auto] |
| Fan Pulse** ⁽²⁾ | : | 2 |
| Fan Speed Control** | : | [Auto] |
| Fan Speed Control** ⁽³⁾ | : | Normal |
| Fan Speed [#] | : | 100 |
| Reference Temperature* | : | [All Temperatures] |
| > Fan #1 Trip Point Table* | | |
| | | → ←: Select Screen |
| | | ↑ ↓: Select Item |
| | | Enter: Select |
| | | +/-: Change Opt. |
| | | F1: General Help |
| | | F2: Previous Values |
| | | F3: Optimized Defaults |
| | | F4: Save & Exit |
| | | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear when selecting Auto for Fan Control.

These items appear when selecting Manual for Fan Control.

⁽¹⁾ This item appears only when selecting Auto for Signal Filter Control.

⁽²⁾ This item appears only when selecting Auto for Fan Pulse.

⁽³⁾ This item appears only when selecting Auto for Fan Speed Control.

| Feature | Option | Description |
|-----------------------|-------------------------------------|---|
| Fan Control | [Disabled], [Manual], [Auto] | Set fan control mode. 'Disabled' will disable the control circuit and stops the fan. |
| Signal Filter Control | [Disabled], [Enabled], [Auto] | Enable / Disable Fan Tacho Signal Filter. [Auto] = Setting from KSC |

| Feature | Option | Description |
|-----------------------|--|---|
| Fan Pulse | [Auto], [1], [2], [3], [4], [5], [6], [7], [8] | Number of pulses the fan produces during one revolution. Range: 1 - 8 |
| Fan Speed Control | [Normal], [Reverse], [Auto] | Set fan speed control method. [Auto] = Setting from KSC [Normal] = Signal has normal behaviour [Reverse] = Signal has reversed behaviour |
| Fan Speed | Value input | Manual fan speed in % |
| Reference Temperature | [#1: CPU Temp], [#2: PCH Temp], [#3: SYSTEM Temp], [All Temperatures] | Determines the temperature source which is used for automatic fan control |

Figure 108: BIOS Advanced Menu – H/W Monitor – Fan #1 Trip Point Table

| Aptio Setup – AMI | | |
|--|------------------|---|
| Advanced | | |
| Fan #1 Automode | [Internal table] | |
| Fan Trip Point 1* | 50 | |
| Fan Hysteresis 1* | 50 | |
| Fan TP Speed 1* | 54 | |
| Fan Trip Point 2* | 60 | |
| Fan Hysteresis 2* | 55 | |
| Fan TP Speed 2* | 58 | → ←: Select Screen ↑ ↓: Select Item |
| Fan Trip Point 3* | 70 | Enter: Select |
| Fan Hysteresis 3* | 61 | +/-: Change Opt. |
| Fan TP Speed 3* | 82 | F1: General Help F2: Previous Values |
| Fan Trip Point 4* | 80 | F3: Optimized Defaults |
| Fan Hysteresis 4* | 71 | F4: Save & Exit |
| Fan TP Speed 4* | 100 | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when selecting User table for Fan #1 Automode.

| Feature | Option | Description |
|-----------------|-----------------------------------|--|
| Fan #1 Automode | [Internal table], [User table] | Chooses between internal table and user table for automatic fan control. |

Figure 109: BIOS Advanced Menu – S5 RTC Wake Settings

| Aptio Setup – AMI | | |
|--|------------|--|
| Advanced | | |
| Wake system from S5 | [Disabled] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Wake up hour ⁽¹⁾ | 0 | |
| Wake up minute ⁽¹⁾ | 0 | |
| Wake up second ⁽¹⁾ | 0 | |
| Wake up minute increase ⁽²⁾ | 1 | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

⁽¹⁾ These items appear only when selecting Fixed Time for Wake system from S5.

⁽²⁾ This item appears only when selecting Dynamic Time for Wake system from S5.

| Feature | Option | Description |
|-------------------------|--|--|
| Wake system from S5 | [Disabled], [Fixed Time], [Dynamic Time] | Enable or disable System wake on alarm event. Select Fixed Time, system will wake on the hr::min::sec specified. Select Dynamic Time, system will wake on the current time + Increase minute(s). |
| Wake up hour | Value input | Select 0 – 23 For example, enter 3 for 3 am and 15 for 3 pm. |
| Wake up minute | Value input | Select 0 – 59 for Minute |
| Wake up second | Value input | Select 0 – 59 for Second |
| Wake up minute increase | Value input | 1 - 5 |

Figure 110: BIOS Advanced Menu – UEFI Variables Protection

| Aptio Setup – AMI | |
|--|-----------|
| Advanced | |
| Password protection of Runtime Variables | [Enabled] |
| → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit | |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

| Feature | Option | Description |
|--|--------------------------|--|
| Password protection of Runtime Variables | [Enabled], [Disabled] | Control the NVRAM Runtime Variables protection through System Admin Password |

Figure 111: BIOS Advanced Menu – Serial Port Console Redirection

| Aptio Setup – AMI | | |
|--|------------|--|
| Advanced | | |
| COM0 | | |
| Console Redirection | [Disabled] | |
| > Console Redirection Settings* | | |
| COM1 | | |
| Console Redirection | [Disabled] | |
| > Console Redirection Settings* | | |
| COM2 | | |
| Console Redirection | [Disabled] | |
| > Console Redirection Settings* | | |
| COM3 | | |
| Console Redirection | [Disabled] | |
| > Console Redirection Settings* | | |
| Legacy Console Redirection | | |
| > Legacy Console Redirection Settings | | |
| Serial Port for Out-of-Band Management / Windows Emergency Management Services (EMS) | | |
| Console Redirection EMS | [Disabled] | |
| > Console Redirection Settings* | | |
| | | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items activate only when enabling Console Redirection (EMS).

| Feature | Option | Description |
|---------------------------|--------------------------|--|
| Console Redirection (EMS) | [Disabled], [Enabled] | Console Redirection Enable or Disable. |

Figure 112: BIOS Advanced Menu – Serial Port Console Redirection – COM0/1/2/3 Console Redirection Settings

| Aptio Setup – AMI | | |
|--|------------|--|
| Advanced | | |
| COM0/1/2/3 Console Redirection Settings | | |
| Terminal Type | [ANSI] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Bits per second | [115200] | |
| Data Bits | [8] | |
| Parity | [None] | |
| Stop Bits | [1] | |
| Flow Control | [None] | |
| VT-UTF8 Combo Key Support | [Enabled] | |
| Recorder Mode | [Disabled] | |
| Resolution 100x31 | [Disabled] | |
| Putty KeyPad | [VT100] | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|-----------------|---|---|
| Terminal Type | [VT100], [VT100Plus], [VT-UTF8], [ANSI] | Emulation: [ANSI]: Extended ASCII char set. [VT100]: ASCII char set. [VT100Plus]: Extends VT100 to support color, function keys, etc. [VT-UTF8]: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes. |
| Bits per second | [9600], [19200], [38400], [57600], [115200] | Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds. |
| Data Bits | [7], [8] | Data Bits |
| Parity | [None], [Even], [Odd], [Mark], [Space] | 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. They can be used as an additional data bit. |
| Stop Bits | [1], [2] | 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. |

| Feature | Option | Description |
|---------------------------|--|---|
| Flow Control | [None], [Hardware RTS/CTS] | Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start / stop signals. |
| VT-UTF8 Combo Key Support | [Disabled], [Enabled] | Enable VT-UTF8 Combination Key Support for ANSI / VT100 terminals |
| Recorder Mode | [Disabled], [Enabled] | With this mode enabled only text will be sent. This is to capture Terminal data. |
| Resolution 100x31 | [Disabled], [Enabled] | Enables or disables extended terminal resolution |
| Putty KeyPad | [VT100], [LINUX], [XTERMR6], [SCO], [ESCN], [VT400] | Select FunctionKey and KeyPad on Putty. |

Figure 113: BIOS Advanced Menu – Serial Port Console Redirection – Legacy Console Redirection Settings

| Aptio Setup – AMI | | |
|--|-----------------|--|
| Advanced | | |
| Legacy Console Redirection Settings | | |
| Redirection COM Port | [COM2] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Resolution | [80x24] | |
| Redirect After POST | [Always Enable] | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|----------------------|---|---|
| Redirection COM Port | [COM2], [COM3], [COM0], [COM1] | Select a COM port to display redirection of Legacy OS and Legacy OPROM Messages |
| Resolution | [80x24], [80x25] | On Legacy OS, the number of Rows and Columns supported redirection |

| Feature | Option | Description |
|---------------------|----------------------------------|---|
| Redirect After POST | [Always Enable], [BootLoader] | 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. Default setting for this option is set to Always Enable. |

Figure 114: BIOS Advanced Menu – Serial Port Console Redirection – Console Redirection EMS Settings

| Aptio Setup – AMI | | |
|--|-----------|---|
| Advanced | | |
| Out-of-Band Mgmt Port | [COM2] | → ←: Select Screen ↑ ↓ : Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Terminal Type EMS | [VT-UTF8] | |
| Bits per second EMS | [115200] | |
| Flow Control EMS | [None] | |
| Data Bits EMS | 8 | |
| Parity EMS | None | |
| Stop Bits EMS | 1 | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|-----------------------|---|---|
| Out-of-Band Mgmt Port | [COM2], [COM3], [COM0], [COM1] | Microsoft Windows Emergency Management Services (EMS) allows for remote management of a Windows Server OS through a serial port. |
| Terminal Type EMS | [VT100], [VT100Plus], [VT-UTF8], [ANSI] | VT-UTF8 is the preferred terminal type for out-of-band management. The next best choice is VT100+ and then VT100. See above, in Console Redirection Settings page, for more Help with Terminal Type / Emulation. |
| Bits per second EMS | [9600], [19200], [57600], [115200] | Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds. |
| Flow Control EMS | [None], [Hardware RTS/CTS], [Software Xon/Xoff] | 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. |

Figure 115: BIOS Advanced Menu – AMI Graphic Output Protocol Policy

| Aptio Setup – AMI | | |
|---|------------|--|
| Advanced | | |
| Intel® Graphics Controller Intel® GOP Driver [21.0.1063] | | |
| Output Select | [EDP1] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| BIST Enable | [Disabled] | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|---------------|---|---|
| Output Select | [EDP1], [DP1], [EDP1 + DP1 [ACTIVE]] | Output Interface |
| BIST Enable | [Disabled], [Enabled] | Starts or stops the BIST on the integrated display panel. |

Figure 116: BIOS Advanced Menu – SIO Common Setting

| Aptio Setup – AMI | | |
|--|------------|--|
| Advanced | | |
| SIO Common Setting | | |
| Lock Legacy Resources | [Disabled] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| | | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|-----------------------|--------------------------|--|
| Lock Legacy Resources | [Disabled], [Enabled] | Enables or Disables Lock of Legacy Resources |

Figure 117: BIOS Advanced Menu – SIO Configuration

| Aptio Setup – AMI | |
|--|---|
| Advanced | |
| AMI SIO Driver Version: A5.19.00 Super IO Chip Logical Devices(s) Configuration > [*Active*] Serial Port 0 > [*Active*] Serial Port 1 > [*Active*] Serial Port 2 > [*Active*] Serial Port 3 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. | → ←: Select Screen ↑ ↓ : Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

Figure 118: BIOS Advanced Menu – SIO Configuration – [*Active*] Serial Port 0

| Aptio Setup – AMI | |
|--|---|
| Advanced | |
| Serial Port 0 Configuration Use This Device [Enabled] Logical Device Settings:* Current: IO=3F8h; IRQ=4;* Possible:* [Use Automatic Settings] WARNING: Disabling SIO Logical Devices may have unwanted side effects. PROCEED WITH CAUTION. | → ←: Select Screen ↑ ↓ : Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

* These items appear only when enabling Use This Device.

| Feature | Option | Description |
|-----------------|--|--|
| Use This Device | [Disabled], [Enabled] | Enables or Disables this Logical Device. |
| Possible: | [Use Automatic Settings], [IO=3F8h; IRQ=4;], [IO=3F8h; IRQ=4;], [IO=2F8h; IRQ=3;] | Allows the user to change the device resource settings. New settings will be reflected on this setup page after system restarts. |

Figure 119: BIOS Advanced Menu – SIO Configuration – [*Active*] Serial Port 1

| Aptio Setup – AMI | |
|---|--|
| Advanced | |
| Serial Port 1 Configuration | |
| Use This Device [Enabled] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Logical Device Settings: Current: IO=2F8h; IRQ=3;* | |
| Possible:* [Use Automatic Settings] | |
| WARNING: Disabling SIO Logical Devices may have unwanted side effects. PROCEED WITH CAUTION. | |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

* These items appear only when enabling Use This Device.

| Feature | Option | Description |
|-----------------|--|--|
| Use This Device | [Disabled], [Enabled] | Enables or Disables this Logical Device. |
| Possible: | [Use Automatic Settings], [IO=2F8h; IRQ=3;], [IO=2F8h; IRQ=3;], [IO=3F8h; IRQ=4;] | Allows the user to change the device resource settings. New settings will be reflected on this setup page after system restarts. |

Figure 120: BIOS Advanced Menu – SIO Configuration – [*Active*] Serial Port 2

| Aptio Setup – AMI | |
|---|--|
| Advanced | |
| Serial Port 2 Configuration | |
| Use This Device [Enabled] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Logical Device Settings: Current: IO=220h; IRQ=7;* | |
| Possible:* [Use Automatic Settings] | |
| WARNING: Disabling SIO Logical Devices may have unwanted side effects. PROCEED WITH CAUTION. | |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

* These items appear only when enabling Use This Device.

| Feature | Option | Description |
|-----------------|---|--|
| Use This Device | [Disabled], [Enabled] | Enables or Disables this Logical Device. |
| Possible: | [Use Automatic Settings], [IO=220h; IRQ=7; DMA;], [IO=220h; IRQ=5,6,7,10,11,12; DMA;] | Allows the user to change the device resource settings. New settings will be reflected on this setup page after system restarts. |

Figure 121: BIOS Advanced Menu – SIO Configuration – [*Active*] Serial Port 3

| Aptio Setup – AMI | | |
|---|--------------------------|---|
| Advanced | | |
| Serial Port 3 Configuration | | |
| Use This Device | [Enabled] | → ←: Select Screen ↑ ↓ : Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Logical Device Settings:* | | |
| Current: IO=230h; IRQ=10;* | | |
| Possible:* | [Use Automatic Settings] | |
| WARNING: Disabling SIO Logical Devices may have unwanted side effects. PROCEED WITH CAUTION. | | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when enabling Use This Device.

| Feature | Option | Description |
|-----------------|--|--|
| Use This Device | [Disabled], [Enabled] | Enables or Disables this Logical Device. |
| Possible: | [Use Automatic Settings], [IO=230h; IRQ=10; DMA;], [IO=230h; IRQ=5,6,7,10,11,12; DMA;] | Allows the user to change the device resource settings. New settings will be reflected on this setup page after system restarts. |

Figure 122: BIOS Advanced Menu – PCI Subsystem Settings

| Aptio Setup – AMI | |
|--|---|
| Advanced | |
| <p>AMI PCI Driver Version: A5.01.28</p> <p>PCI Settings Common for all Devices:</p> <p>Re-Size BAR Support [Disabled]</p> <p>BME DMA Mitigation [Disabled]</p> <p>Change Settings of the Following PCI Devices:</p> <p>WARNING: Changing PCI Device(s) settings may have unwanted side effects! System may HANG! PROCEED WITH CAUTION.</p> | <p>→ ←: Select Screen</p> <p>↑ ↓: Select Item</p> <p>Enter: Select</p> <p>+/-: Change Opt.</p> <p>F1: General Help</p> <p>F2: Previous Values</p> <p>F3: Optimized Defaults</p> <p>F4: Save & Exit</p> <p>ESC: Exit</p> |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

| Feature | Option | Description |
|---------------------|--------------------------|--|
| Re-Size BAR Support | [Disabled], [Enabled] | If system has Resizable BAR capable PCIe Devices, this option Enables or Disables Resizable BAR Support. |
| BME DMA Mitigation | [Disabled], [Enabled] | Re-enable Bus Master Attribute disabled during Pci enumeration for PCI Bridges after SMM Locked. |

Figure 123: BIOS Advanced Menu – USB Configuration

| Aptio Setup – AMI | | | |
|--|-----------|--|--|
| Advanced | | | |
| USB Configuration | | | |
| USB Module Version | 32 | | |
| USB Controllers: | | | |
| 2 XHCIs | | | |
| USB Devices: | | | |
| 1 Keyboard | | | |
| Legacy USB Support | [Enabled] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit | |
| XHCI Hand-off | [Enabled] | | |
| USB Mass Storage Driver Support | [Enabled] | | |
| USB hardware delays and time-outs: | | | |
| USB transfer time-out | [20 sec] | | |
| Device reset time-out | [20 sec] | | |
| Device power-up delay | [Auto] | | |
| Device power-up delay in seconds* | 5 | | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | | |

* This item appears only when selecting Manual for Device power-up delay in seconds.

| Feature | Option | Description |
|---------------------------------|---|--|
| Legacy USB Support | [Enabled], [Disabled], [Auto] | Enables Legacy USB support. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications. |
| XHCI Hand-off | [Enabled], [Disabled] | 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 | [Disabled], [Enabled] | Enable / Disable USB Mass Storage Driver Support. |
| USB transfer time-out | [1 sec], [5 sec], [10 sec], [20 sec] | The time-out value for Control, Bulk, and Interrupt transfers. |
| Device reset time-out | [10 sec], [20 sec], [30 sec], [40 sec] | USB mass storage device Start Unit command time-out. |

| Feature | Option | Description |
|----------------------------------|---------------------|---|
| Device power-up delay | [Auto], [Manual] | Maximum time the device will take before it properly reports itself to the Host Controller. 'Auto' uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub descriptor. |
| Device power-up delay in seconds | Value input | Delay range is 1..40 seconds, in one second increments |

Figure 124: BIOS Advanced Menu – Network Stack Configuration

| Aptio Setup – AMI | | |
|--|------------|--|
| Advanced | | |
| Network Stack | [Disabled] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| IPv4 PXE Support* | [Disabled] | |
| IPv4 HTTP Support* | [Disabled] | |
| IPv6 PXE Support* | [Disabled] | |
| IPv6 HTTP Support* | [Disabled] | |
| PXE boot wait time* | 0 | |
| Media detect count* | 1 | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when enabling Network Stack.

| Feature | Option | Description |
|--------------------|--------------------------|---|
| Network Stack | [Disabled], [Enabled] | Enable / Disable UEFI Network Stack |
| IPv4 PXE Support | [Disabled], [Enabled] | Enable / Disable IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available. |
| IPv4 HTTP Support | [Disabled], [Enabled] | Enable / Disable IPv4 HTTP boot support. If disabled, IPv4 HTTP boot support will not be available. |
| IPv6 PXE Support | [Disabled], [Enabled] | Enable / Disable IPv6 PXE boot support. If disabled, IPv6 PXE boot support will not be available. |
| IPv6 HTTP Support | [Disabled], [Enabled] | Enable / Disable IPv6 HTTP boot support. If disabled, IPv6 HTTP boot support will not be available. |
| PXE boot wait time | Value input | 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 | Value input | Number of times the presence of media will be checked. Use either +/- or numeric keys to set the value. |

Figure 125: BIOS Advanced Menu – CSM Configuration

| Aptio Setup – AMI | | |
|--|---------------------|--|
| Advanced | | |
| Compatibility Support Module Configuration | | |
| CSM Support | [Disabled] | |
| CSM16 Module Version | N/A, reset required | |
| GateA20 Active* | [Upon Request] | |
| Option ROM Messages ^{*(1)} | [Force BIOS] | |
| INT19 Trap Response* | [Immediate] | |
| HDD Connection Order ^{*(2)} | [Adjust] | |
| Boot option filter* | [UEFI only] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Option ROM execution* | | |
| Network* | [Do not launch] | |
| Storage* | [UEFI] | |
| Video* | [UEFI] | |
| Other PCI devices* | [UEFI] | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when enabling CSM Support.

⁽¹⁾ This item appears only when selecting Legacy for Video.

⁽²⁾ This item appears only when selecting UEFI and Legacy or Legacy only for Boot option filter.

| Feature | Option | Description |
|----------------------|---|--|
| CSM Support | [Disabled], [Enabled] | Enable / Disable CSM Support. |
| GateA20 Active | [Upon Request], [Always] | [Upon Request]: GA20 can be disabled using BIOS services. [Always]: do not allow disabling GA20. This option is useful when any RT code is executed above 1MB. |
| Option ROM Messages | [Force BIOS], [Keep Current] | Set display mode for Option ROM |
| INT19 Trap Response | [Immediate], [Postponed] | BIOS reaction on INT19 trapping by Option ROM: [Immediate]: execute the trap right away; [Postponed]: execute the trap during legacy boot. |
| HDD Connection Order | [Adjust], [Keep] | Some OS require HDD handles to be adjusted, i.e. OS is installed on drive 80h. |
| Boot option filter | [UEFI and Legacy], [Legacy only], [UEFI only] | This option controls Legacy / UEFI ROMs priority |

| Feature | Option | Description |
|-------------------|---|---|
| Network | [Do not launch], [UEFI], [Legacy] | Controls the execution of UEFI and Legacy Network OpROM |
| Storage | [Do not launch], [UEFI], [Legacy] | Controls the execution of UEFI and Legacy Storage OpROM |
| Video | [Do not launch], [UEFI], [Legacy] | Controls the execution of UEFI and Legacy Video OpROM |
| Other PCI devices | [Do not launch], [UEFI], [Legacy] | Determines OpROM execution policy for devices other than Network, Storage, or Video |

Figure 126: BIOS Advanced Menu – NVMe Configuration

| Aptio Setup – AMI | |
|--|--|
| Advanced | |
| NVMe Configuration | |
| No NVME Device Found | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

Figure 127: BIOS Advanced Menu – SDIO Configuration

| Aptio Setup – AMI | |
|--|--|
| Advanced | |
| SDIO Configuration | |
| SDIO Access Mode | [Auto] |
| | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

| Feature | Option | Description |
|------------------|--|--|
| SDIO Access Mode | [Auto], [ADMA], [SDMA], [PIO] | [Auto]: Access SD device in DMA mode if controller supports it, otherwise in PIO mode. [DMA]: Access SD device in DMA mode. [PIO]: Access SD device in PIO mode. |

Figure 128: BIOS Advanced Menu – CH7513A Configurations

| Aptio Setup – AMI | | |
|--|-----------------------|--|
| Advanced | | |
| CH7513A Configurations | | |
| LFP Selection | [LVDS] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| LVDS Panel Type ⁽¹⁾ | [1920x1080 24Bit 2CH] | |
| Backlight Source Selection ⁽¹⁾⁽²⁾ | [Controlled by PCH] | |
| Panel Brightness ⁽¹⁾⁽²⁾ | 254 | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

⁽¹⁾ These items appear when selection LVDS for LFP Selection.

⁽²⁾ These items appear when selecting eDP for LFP Selection.

| Feature | Option | Description |
|----------------------------|--|---|
| LFP Selection | [Disabled], [LVDS], [eDP] | Select the LFP Configuration |
| LVDS Panel Type | [800x600 18Bit 1CH], [1024x768 18Bit 1CH], [1024x768 24Bit 1CH], [1280x768 18Bit 1CH], [1280x800 18Bit 1CH], [1280x960 18Bit 1CH], [1280x1024 24Bit 2CH], [1366x768 18Bit 1CH], [1366x768 24Bit 1CH], [1440x900 24Bit 2CH], [1400x1050 24Bit 2CH], [1600x900 24Bit 2CH], [1680x1050 24Bit 2CH], [1600x1200 24Bit 2CH], [1920x1080 24Bit 2CH], [1920x1200 24Bit 2CH] | LVDS panel by selecting the appropriate setup item. |
| Backlight Source Selection | [Controlled by PCH], [Controlled by Switch] | Set the backlight source Selection |
| Panel brightness | Value input | Set panel brightness |

Figure 129: BIOS Advanced Menu – F81435 Configurations

| Aptio Setup – AMI | | |
|--|--|------------------------|
| Advanced | | |
| F81435 Configurations | | |
| COM0 Mode Selection | [RS-232] | |
| COM0 Slew Rate Control | [RS-232 to 3 Mbps or RS-485/RS-422 to 20 Mbps] | |
| COM0 Transceiver | [Normal mode] | |
| COM0 Internal Terminator Switch Control | [Terminator switch is disabled] | |
| COM0 External Terminator Switch Control | [Terminator switch is disabled] | |
| COM1 Mode Selection | [RS-232] | |
| COM1 Slew Rate Control | [RS-232 to 3 Mbps or RS-485/RS-422 to 20 Mbps] | |
| COM1 Transceiver | [Normal mode] | |
| COM1 Internal Terminator Switch Control | [Terminator switch is disabled] | |
| COM1 External Terminator Switch Control | [Terminator switch is disabled] | |
| COM2 Mode Selection | [RS-232] | |
| COM2 Slew Rate Control | [RS-232 to 3 Mbps or RS-485/RS-422 to 20 Mbps] | |
| COM2 Transceiver | [Normal mode] | |
| COM2 Internal Terminator Switch Control | [Terminator switch is disabled] | |
| COM2 External Terminator Switch Control | [Terminator switch is disabled] | |
| COM3 Mode Selection | [RS-232] | |
| COM3 Slew Rate Control | [RS-232 to 3 Mbps or RS-485/RS-422 to 20 Mbps] | |
| COM3 Transceiver | [Normal mode] | |
| COM3 Internal Terminator Switch Control | [Terminator switch is disabled] | |
| COM3 External Terminator Switch Control | [Terminator switch is disabled] | |
| | | → ←: Select Screen |
| | | ↑ ↓: Select Item |
| | | Enter: Select |
| | | +/-: Change Opt. |
| | | F1: General Help |
| | | F2: Previous Values |
| | | F3: Optimized Defaults |
| | | F4: Save & Exit |
| | | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|---|---|--|
| COM0/1/2/3 Mode Selection | [RS-422 Signal Master], [RS-232], [RS-485 with Auto Flow Control], [RS-422 Multi Master] | Mode selection for COM0/1/2/3 |
| COM0/1/2/3 Slew Rate Control | [Limit driver slew rate to 250Kbps for RS-232 and RS-485/RS-422], [RS-232 to 3 Mbps or RS-485/RS-422 to 20 Mbps] | Slew rate control for COM0/1/2/3 |
| COM0/1/2/3 Transceiver | [Shutdown mode], [Normal mode] | Shutdown the Transceiver of COM0/1/2/3 |
| COM0/1/2/3 Internal Terminator Switch Control | [Terminator switch is disabled], [Terminator switch is enabled] | Internal Terminator switch control for RS-422/RS-485 of COM0/1/2/3 |
| COM0/1/2/3 External Terminator Switch Control | [Terminator switch is disabled], [Terminator switch is enabled] | External Terminator switch control for RS-422/RS-485 of COM0/1/2/3 |

Figure 130: BIOS Advanced Menu – Tls Auth Configuration

| Aptio Setup – AMI | |
|---|--|
| Advanced | |
| > Server CA Configuration > Client Cert Configuration* | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

* Read only item

Figure 131: BIOS Advanced Menu – Tls Auth Configuration – Server CA Configuration

| Aptio Setup – AMI | |
|--|--|
| Advanced | |
| > Enroll Cert > Delete Cert | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

Figure 132: BIOS Advanced Menu – Tls Auth Configuration – Server CA Configuration – Enroll Cert

| Aptio Setup – AMI | |
|--|--|
| Advanced | |
| > Enroll Cert Using File Cert GUID > Commit Changes and Exit > Discard Changes and Exit | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

| Feature | Option | Description |
|-----------|----------|---|
| Cert GUID | ID input | Input digit character in 11111111-2222-3333-4444-1234567890ab format. |

Figure 133: BIOS Advanced Menu – RAM Disk Configuration

| Aptio Setup – AMI | |
|--|--|
| Advanced | |
| Disk Memory Type: | [Boot Service Data] |
| > Create raw | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| > Create from file | |
| Created RAM disk list: | |
| RAM Disk 0: [0x6BF98018, 0x6BF99017]* | |
| Remove selected RAM disk(s). | |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

* This item is available only when creating a RAM disk.

| Feature | Option | Description |
|------------------|------------------------------------|--|
| Disk Memory Type | [Boot Service Data], [Reserved] | Specifies type of memory to use from available memory pool in system to create a disk. |
| RAM Disk 0 | [Disabled], [Enabled] | Select for remove |

Figure 134: BIOS Advanced Menu – RAM Disk Configuration – Create raw

| Aptio Setup – AMI | |
|--|--|
| Advanced | |
| Size (Hex): | 1 |
| Create & Exit | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Discard & Exit | |
| | |
| | |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

| Feature | Option | Description |
|------------|-------------|---|
| Size (Hex) | Value input | The valid RAM disk size should be multiples of the RAM disk block size. |

Figure 135: BIOS Advanced Menu – Intel® Ethernet Controller I226-IT – C0:EA:C3:D1:D1:0E/0F

| Aptio Setup – AMI | | |
|--|--|--|
| Advanced | | |
| UEFI Driver | Intel® 2.5G Ethernet Controller 0.10.06 | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Device Name | Intel® Ethernet Controller I226-IT | |
| Link Status | [Disconnected] | |
| MAC Address | C0:EA:C3:D1:D1:0E/0F | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

Read only

Figure 136: BIOS Advanced Menu – Driver Health

| Aptio Setup – AMI | | |
|---|---------|--|
| Advanced | | |
| > Intel® 2.5G Ethernet Controller 0.10.06 | Healthy | |
| > Intel® 2.5G Ethernet Controller 0.10.06 | Healthy | |
| | | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

Figure 137: BIOS Advanced Menu – Driver Health – Intel® 2.5G Ethernet Controller 0.10.06

| Aptio Setup – AMI | | |
|--|---------|--|
| Advanced | | |
| Intel® Ethernet Controller I226-IT | Healthy | |
| Intel® Ethernet Controller I226-IT | Healthy | |
| | | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

Read only

8.2.3. Chipset Setup Menu

The Chipset setup menu provides functions and a sub-screen for chipset configurations. The following sub-screen functions are included in the menu:

- System Agent (SA) Configuration
- PCH-IO Configuration

Figure 138: BIOS Chipset Setup Menu

| Aptio Setup – AMI | | | | | |
|---|----------|---------|----------|---|-------------|
| Main | Advanced | Chipset | Security | Boot | Save & Exit |
| > System Agent (SA) Configuration > PCH-IO Configuration | | | | | |
| | | | | → ←: Select Screen ↑ ↓ : Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | | | | |

Figure 139: BIOS Chipset Setup Menu – System Agent (SA) Configuration

| Aptio Setup – AMI | |
|--|----------------------------|
| Chipset | |
| System Agent (SA) Configuration | |
| VT-d | Supported |
| > Memory Configuration > Graphics Configuration > DMI/OPI Configuration > TCSS setup menu > Display setup menu > PCI Express Configuration | |
| Stop Grant Configuration | [Auto] |
| Number of Stop Grant Cycles* | 1 |
| VT-d | [Enabled] |
| Control Iommu Pre-boot Behavior | [Enable IOMMU during boot] |
| X2APIC Opt Out | [Disabled] |
| DMA Control Guarantee | [Enabled] |
| Thermal Device (B0:D4:F0) | [Disabled] |
| Cpu CrashLog (Device 10) | [Disabled] |
| GNA Device (B0:D8:F0) | [Enabled] |
| CRID Support | [Disabled] |
| WRC Feature | [Disabled] |
| Above 4GB MMIO BIOS assignment | [Enabled] |
| IPU Device (B0:D5:F0) | [Disabled] |
| IPU 1811 Dash Camera | [Disabled] |
| > MIPI Camera Configuration | |
| → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit | |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

* This item appears only when selecting Manual for Stop Grant Configuration.

| Feature | Option | Description |
|---------------------------------|--|---|
| Stop Grant Configuration | [Auto], [Manual] | Automatic / Manual stop grant configuration |
| Number of Stop Grant Cycles | Value input | Selects number of Stop-Grant cycles. |
| VT-d | [Enabled], [Disabled] | VT-d capability |
| Control Iommu Pre-boot Behavior | [Disable IOMMU], [Enable IOMMU during boot] | Enable IOMMU in Pre-boot environment (If DMAR table is installed in DXE and if VTD_INFO_PPI is installed in PEI.) |

| Feature | Option | Description |
|--------------------------------|--------------------------|--|
| X2APIC Opt Out | [Enabled], [Disabled] | Enable / Disable X2APIC_OPT_OUT bit |
| DMA Control Guarantee | [Enabled], [Disabled] | Enable / Disable DMA_CONTROL_GUARANTEE bit |
| Thermal Device (B0:D4:F0) | [Enabled], [Disabled] | Enable / Disable SA Thermal Device. Always enabled for ICL A0 stepping. |
| Cpu CrashLog (Device 10) | [Enabled], [Disabled] | Enable / Disable Cpu CrashLog Device. |
| GNA Device (B0:D8:F0) | [Enabled], [Disabled] | Enable / Disable SA GNA Device. |
| CRID Support | [Enabled], [Disabled] | Enable / Disable SA CRID and TCSS CRID control for Intel SIPP |
| WRC Feature | [Enabled], [Disabled] | Enable / Disable SA WRC (Write Cache) Feature of IOP. When enabled, supports IO devices allocating onto the ring and into LLC. |
| Above 4GB MMIO BIOS assignment | [Enabled], [Disabled] | Enable / Disable above 4GB MemoryMappedIO BIOS assignment. This is enabled automatically when Aperture Size is set to 2048MB. |
| IPU Device (B0:D5:F0) | [Enabled], [Disabled] | Enable / Disable SA IPU Device. |
| IPU 1181 Dash Camera | [Enabled], [Disabled] | Enable / Disable SA IPU 1181 Dash Camera support. |

Figure 140: BIOS Chipset Setup Menu – System Agent (SA) Configuration – Memory Configuration

| Aptio Setup – AMI | |
|--------------------------------|--------------------------|
| Chipset | |
| > Memory Thermal Configuration | |
| > Memory Training Algorithms | |
| Memory Configuration | |
| Memory RC Version | 0.0.4.74 |
| Memory Frequency | 4800 MHz |
| tCL-tRCD-tRP-tRAS | 40-39-39-77 |
| MC 0 Ch 0 DIMM 0 | Populated & Enabled |
| Size | 16384 MB (DDR5) |
| Number of Ranks | 1 |
| Manufacturer | Unknown |
| MC 0 Ch 0 DIMM 1 | Not Populated / Disabled |
| MC 1 Ch 0 DIMM 0 | Not Populated / Disabled |
| MC 1 Ch 0 DIMM 1 | Not Populated / Disabled |

| Aptio Setup – AMI | |
|---|------------------|
| Chipset | |
| Debug Value | 0 |
| MRC ULT Safe Config | [Disabled] |
| LPDDR DqDqs Re-Training | [Enabled] |
| Safe Mode Support | [Disabled] |
| Memory Test on Warm Boot | [Enabled] |
| Maximum Memory Frequency | [Auto] |
| LP5 Bank Mode | [Auto] |
| Frequency Limit for Mixed 2DPC DDR4 | 0 |
| Frequency Limit for Mixed 2DPC DDR5 1 Rank 8GB and 8GB | 2000 |
| Frequency Limit for Mixed 2DPC DDR5 1 Rank 16GB and 16GB | 2000 |
| Frequency Limit for Mixed 2DPC DDR5 1 Rank 8GB and 16GB | 2000 |
| Frequency Limit for Mixed 2DPC DDR5 2 Rank | 2000 |
| LCT Cmd Eye Width | 96 |
| HOB Buffer Size | [Auto] |
| Max TOLUD | [Dynamic] |
| SA GV | [Enabled] |
| Gear Ratio ⁽¹⁾ | 0 |
| First Point Frequency ⁽²⁾ | 0 |
| First Point Gear ⁽²⁾ | 0 |
| Second Point Frequency ⁽²⁾ | 0 |
| Second Point Gear ⁽²⁾ | 0 |
| Third Point Frequency ⁽²⁾ | 0 |
| Third Point Gear ⁽²⁾ | 0 |
| Fourth Point Frequency ⁽²⁾ | 0 |
| Fourth Point Gear ⁽²⁾ | 0 |
| SAGV Switch Factor IA | 30 |
| SAGV Switch Factor GT | 30 |
| SAGV Switch Factor IO | 30 |
| SAGV Switch Factor Stall | 30 |
| Threshold For Switch Up | 1 |
| Threshold For Switch Down | 1 |
| Retrain on Fast Fail | [Enabled] |
| DDR4_1DPC | [Enabled] |
| Row Hammer Mode | [RFM] |
| RH LFSR0 Mask ⁽³⁾ | [1/2^11] |
| RH LFSR1 Mask ⁽³⁾ | [1/2^11] |
| MC Refresh Rate | [NORMAL Refresh] |
| Refresh Watermarks | [High] |

| Aptio Setup – AMI | | |
|--|-------------------------|------------------------|
| Chipset | | |
| LPDDR ODT RttWr | 0 | |
| LPDDR ODT RttCa | 0 | |
| Exit On Failure (MRC) | [Enabled] | |
| New Features 1 - MRC | [Disabled] | |
| New Features 2 – MRC | [Disabled] | |
| Ch Hash Override | [Disabled] | |
| Ch Hash Support ⁽⁴⁾ | [Enabled] | |
| Ch Hash Mask ⁽⁴⁾ | 2096 | |
| Ch Hash Interleaved Bit ⁽⁴⁾ | [BIT8] | |
| Extended Bank Hashing | [Enabled] | |
| Per Bank Refresh | [Enabled] | |
| VC1 Read Metering | [Enabled] | |
| Strong Weak Leaker | 7 | |
| Power Down Mode | [Auto] | |
| Pwr Down Idle Timer | 0 | |
| Page Close Idle Timeout | [Enabled] | |
| Memory Scrambler | [Enabled] | |
| Force ColdReset | [Disabled] | |
| Controller 0, Channel 0 Control | [Enabled] | |
| Controller 0, Channel 1 Control | [Enabled] | |
| Controller 0, Channel 2 Control | [Enabled] | |
| Controller 0, Channel 3 Control | [Enabled] | |
| Controller 1, Channel 0 Control | [Enabled] | |
| Controller 1, Channel 1 Control | [Enabled] | |
| Controller 1, Channel 2 Control | [Enabled] | |
| Controller 1, Channel 3 Control | [Enabled] | |
| Force Single Rank | [Disabled] | |
| Memory Remap | [Enabled] | |
| Time Measure | [Disabled] | |
| Fast Boot | [Enabled] | |
| Rank Margin Tool Per Task | [Disabled] | |
| Training Tracing | [Disabled] | |
| Lpddr Mem WL Set | [Set B] | → ←: Select Screen |
| BDAT Memory Test Type | [Rank Margin Tool Rank] | ↑ ↓ : Select Item |
| Rank Margin Tool Loop Count | 0 | Enter: Select |
| ECC DFT | [Disabled] | +/-: Change Opt. |
| Write0 | [Disabled] | F1: General Help |
| Periodic DCC | [Disabled] | F2: Previous Values |
| LPMODE | [Auto] | F3: Optimized Defaults |
| PPR Enable | [Disabled] | F4: Save & Exit |

| Aptio Setup – AMI | | |
|--|------------|-----------|
| Chipset | | |
| SAM Overloading | [Disabled] | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

⁽¹⁾ This item appears only when selecting Disabled for SA GV.

⁽²⁾ These items appear only when selecting Enabled or Fixed to 1st / 2nd / 3rd / 4th Point for SA GV.

⁽³⁾ These items appear only when selecting RFM or pTRR for Row Hammer Mode.

⁽⁴⁾ These items activate only when enabling Ch Hash Override.

| Feature | Option | Description |
|--|---|---|
| Debug Value | Value input | Debug Value |
| MRC ULT Safe Config | [Disabled], [Enabled] | MRC ULT Safe Config for PO |
| LPDDR DqDqs Re-Training | [Disabled], [Enabled] | Disable / Enable LPDDR DqDqs Re-Training |
| Safe Mode Support | [Disabled], [Enabled] | Safe Mode enable support. Option will be used for changes/WAs that may affect an stable MRC |
| Memory Test on Warm Boot | [Disabled], [Enabled] | Enable or Disable Base Memory Test Run on Warm Boot |
| Maximum Memory Frequency | [Auto], [1067], [1333], [1400], [1600], [1800], [1867], [2000], [2133], [2200], [2400], [2600], [2667], [2800], [2933], [3000], [3200], [3467], [3600], [3733], [4000], [4200], [4267], [4400], [4600], [4800], [5000], [5200], [5400], [5600], [5800], [6000], [6200], [6400], [10000], [12800] | Maximum Memory Frequency Selection in Mhz. |
| LP5 Bank Mode | [Auto], [LP5 8 Bank Mode], [LP5 16 Bank Mode], [LP5 BG Mode] | LP5 Bank Mode |
| Frequency Limit for Mixed 2DPC DDR4 | Value input | Override the reduced speed in mixed 2DPC config or non-POR 2DPC config. 0 = Auto, otherwise speed in MT/s |
| Frequency Limit for Mixed 2DPC DDR5 1 Rank 8GB/16GB and 8GB/16GB | Value input | Override the reduced speed in mixed 2DPC config or non-POR 2DPC config. 0 = Auto, otherwise speed in MT/s |

| Feature | Option | Description |
|---|--|---|
| Frequency Limit for Mixed 2DPC DDR5 2 Rank | Value input | Override the reduced speed in mixed 2DPC config or non-POR 2DPC config. 0 = Auto, otherwise speed in MT/s |
| LCT Cmd Eye Width | Value input | LCT Cmd Eye Width. 0 = Auto |
| HOB Buffer Size | [Auto], [1B], [1KB], [Max (assuming 63KB total HOB size)] | Size to set HOB Buffer |
| Max TOLUD | [Dynamic], [1 GB], [1.25 GB], [1.5 GB], [1.75 GB], [2 GB], [2.25 GB], [2.5 GB], [2.75 GB], [3 GB], [3.25 GB], [3.5 GB] | Maximum Value of TOLUD. Dynamic assignment would adjust TOLUD automatically based on largest MMIO length of installed graphic controller |
| SA GV | [Disabled], [Enabled], [Fixed to 1st Point], [Fixed to 2nd Point], [Fixed to 3rd Point], [Fixed to 4th Point] | System Agent Geyserville. Can disable, fix to a specific point, or enable frequency switching. |
| Gear Ratio | Value input | Gear ratio when SAGV is disabled. 0 = Auto, 1 = G1, 2 = G2, 4 = G4 |
| First / Second / Third / Fourth Point Frequency | Value input | Specify the frequency for the given point. 0 = MRC auto, Else a specific frequency as an integer: 1333 |
| First / Second / Third / Fourth Point Gear | Value input | Gear ratio for this SAGV point. 0 = Auto, 1 = G1, 2 = G2, 4 = G4 |
| SAGV Switch Factor IA | Value input | SAGV Switch Factor of IA Load Percentage To Trigger Switching Up And Down |
| SAGV Switch Factor GT | Value input | SAGV Switch Factor of GT Load Percentage To Trigger Switching Up And Down |
| SAGV Switch Factor IO | Value input | SAGV Switch Factor of IO Load Percentage To Trigger Switching Up And Down |
| SAGV Switch Factor Stall | Value input | SAGV Switch Factor of IA / GT Stall Percentage To Trigger Switching Up And Down |
| Threshold For Switch Up | Value input | Duration In MS Of High Activity After Which SAGV Will Switch Up |
| Threshold For Switch Down | Value input | Duration In MS Of Low Activity After Which SAGV Will Switch Down |

| Feature | Option | Description |
|--------------------------|--|---|
| Retrain on Fast Fail | [Disabled], [Enabled] | Restart MRC in Cold mode if SW MemTest fails during Fast flow. Default = Enabled |
| DDR4_1DPC | [Disabled], [Enabled on DIMM0 only], [Enabled on DIMM1 only], [Enabled] | DDR4 1DPC performance feature for 2R DIMMs. Can be enabled on DIMM0 or DIMM1 only, or on both |
| Row Hammer Mode | [Disabled], [RFM], [pTRR] | Row Hammer Prevention Mode. RFM will fall back to pTRR if not available. |
| RH LFSR0/1 Mask | [1/2^1], [1/2^2], [1/2^3], [1/2^4], [1/2^5], [1/2^6], [1/2^7], [1/2^8], [1/2^9], [1/2^10], [1/2^11], [1/2^12], [1/2^13], [1/2^14], [1/2^15] | LFSR0/1 mask for RH pTRR |
| MC Refresh Rate | [NORMAL Refresh], [2x Refresh], [4x Refresh] | Select refresh rate on the MC |
| Refresh Watermarks | [Low], [High] | Sets Refresh Panic Watermark and Refresh High-Priority Watermark to HIGH or LOW values |
| LPDDR ODT RttWr / RttCa | Value input | Initial RttWr / RttCa ODT override for LP4/5 in Ohms. Range 0x01 – 0xFF Default 0 = AUTO |
| Exit On Failure (MRC) | [Disabled], [Enabled] | Exit On Failure for MRC training steps |
| New Features 1 / 2 - MRC | [Disabled], [Enabled] | Enabling / Disabling Generic New Features 1 / 2 |
| Ch Hash Override | [Disabled], [Enabled] | Override Channel Hash settings |
| Ch Hash Support | [Disabled], [Enabled] | Enable / Disable Channel Hash Support. Note: ONLY if memory interleaved Mode |
| Ch Hash Mask | Value input | Set the BIT(s) to be included in the XOR function. NOTE BIT mask corresponds to BITS [19:6] |
| Ch Hash Interleaved Bit | [BIT6], [BIT7], [BIT8], [BIT9], [BIT10], [BIT11], [BIT12], [BIT13] | Select the BIT to be used for Channel Interleaved mode. NOTE: BIT7 will interleave the channels at a 2 cacheline granularity, BIT8 at 4 and BIT9 at 8. |
| Extended Bank Hashing | [Disabled], [Enabled] | Enable / disable Extended Bank Hashing. |
| Per Bank Refresh | [Disabled], [Enabled] | Enables and Disables the per bank refresh. This only impacts memory technologies that support PBR: LPDDR4, LPDDR5 and DDR5. |
| VC1 Read Metering | [Disabled], | Enable / Disable VC1 Read Metering Feature (RdMeter) |

| Feature | Option | Description |
|---|---|--|
| | [Enabled] | |
| Strong Weak Leaker | Value input | Value for StrongWKLeaker |
| Power Down Mode | [Auto], [No Power Down], [APD], [PPD-DLLoff] | CKE Power Down Mode Control |
| Pwr Down Idle Timer | Value input | The minimum value should = to the worst case Roundtrip delay + Burst_Length. 0 means AUTO, 64 for ULX/ULT, 128 for DT/Halo |
| Page Close Idle Timeout | [Enabled], [Disabled] | Page Close Idle Timeout Control |
| Memory Scrambler | [Disabled], [Enabled] | Enable / Disable Memory Scrambler support. |
| Force ColdReset | [Enabled], [Disabled] | Force ColdReset OR Choose MrcColdBoot mode, when Coldboot is required during MRC execution. Note: If ME 5.0MB is present, ForceColdReset is required! |
| Controller 0 / 1, Channel 0 / 1 / 2 / 3 Control | [Enabled], [Disabled] | Controller 0 / 1, Channel 0 / 1 / 2 / 3 Control – Enable or Disable Controller 0 / 1, Channel 0 / 1 / 2 / 3. |
| Force Signal Rank | [Disabled], [Enabled] | When enabled, only Rank 0 will be used in each DIMM |
| Memory Remap | [Enabled], [Disabled] | Enable / Disable Memory Remap above 4GB |
| Time Measure | [Disabled], [Enabled] | Enable / Disable printing of the time it takes to execute MRC. |
| Fast Boot | [Disabled], [Enabled] | Enable / Disable fast path thru the MRC |
| Rank Margin Tool Per Task | [Disabled], [Enabled] | Enable / Disable RMT running at every major training step |
| Tarining Tracing | [Disabled], [Enabled] | Enables / Disables printing of the current trained state at every major training step. |
| Lpddr Mem WL Set | [Set A], [Set B] | Only applicable to LPDDR, Memory Write Latency Set selection (A is default, B will be used if memory devices support it) |
| BDAT Memory Test Type | [Rank Margin Tool Rank] | Read only item |
| Rank Margin Tool Loop Count | Value input | Specifies the Loop Count to be used during Rank Margin Tool Testing. 0 = AUTO |
| ECC DFT | [Disabled], [Enabled] | Enable / Disable ECC DFT feature |
| Write0 | [Disabled], [Enabled] | Write0 feature for LP5/DDR5 |
| Periodic DCC | [Disabled], [Enabled] | Enable / Disable Periodic DCC |

| Feature | Option | Description |
|-----------------|-------------------------------------|--|
| LPMode | [Auto], [Enabled], [Disabled] | Control LPMode feature |
| PPR Enable | [Disabled], [Hard PPR] | PPR permanently repairs failed rows (if possible). |
| SAM Overloading | [Disabled], [Enabled] | [Enabled]: copy the sagv frequency point. [Disabled]: not copy. |

Figure 141: BIOS Chipset Setup Menu – System Agent (SA) Configuration – Memory Configuration – Memory Thermal Configuration

| Aptio Setup – AMI | | |
|--|------------|--|
| Chipset | | |
| Memory Thermal Configuration | | |
| > Memory Power and Thermal Throttling | | |
| Memory Thermal Management | [Enabled] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| PECI Injected Temperature* | [Disabled] | |
| EXTTS# via TS-on-Board* | [Disabled] | |
| EXTTS# via TS-on-DIMM* | [Disabled] | |
| Virtual Temperature Sensor (VTS)* | [Disabled] | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when enabling Memory Thermal Management.

| Feature | Option | Description |
|----------------------------------|--------------------------|---|
| Memory Thermal Management | [Disabled], [Enabled] | Enable / Disable Memory Thermal Management. |
| PECI Injected Temperature | [Disabled], [Enabled] | Enable / Disable memory temperatures to be injected to the processor via Peci. |
| EXTTS# via TS-on-Board | [Disabled], [Enabled] | Enable / Disable routing TS-on-Board’s ALERT# and THERM# to EXTTS# pins on the PCH. |
| EXTTS# via TS-on-DIMM | [Disabled], [Enabled] | Enable / Disable routing TS-on-DIMM’s ALERT# to EXTTS# pin on the PCH. |
| Virtual Temperature Sensor (VTS) | [Disabled], [Enabled] | Enable / Disable Virtual Temperature Sensor (VTS). |

Figure 142: BIOS Chipset Setup Menu – System Agent (SA) Configuration – Memory Configuration – Memory Thermal Configuration – Memory Power and Thermal Throttling

| Aptio Setup – AMI | | |
|--|-----------------------|------------------------|
| Chipset | | |
| Memory Power and Thermal Throttling | | |
| DDR PowerDown and idle counter | [BIOS] | |
| For LPDDR Only: DDR PowerDown and idle counter | [BIOS] | |
| REFRESH_2X_MODE | [2- Enabled HOT only] | → ←: Select Screen |
| SelfRefresh Enable | [Enabled] | ↑ ↓ : Select Item |
| SelfRefresh IdleTimer | 512 | Enter: Select |
| Throttler CKEMin Defeature | [Enabled] | +/-: Change Opt. |
| Throttler CKEMin Timer | 0 | F1: General Help |
| Allow Opp Ref Below Write Threshold | [Disabled] | F2: Previous Values |
| Write Threshold | 0 | F3: Optimized Defaults |
| For LPDDR only: Throttler CKEMin Defeature | [Enabled] | F4: Save & Exit |
| For LPDDR only: Throttler CKEMin Timer | 0 | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|--|---|---|
| DDR PowerDown and idle counter | [PCODE], [BIOS] | [BIOS]: BIOS is in control of DDR CKE mode and idle timer value. [PCODE]: pcode will manage the modes. |
| For LPDDR Only: DDR PowerDown and idle counter | [PCODE], [BIOS] | For LPDDR Only [BIOS]: BIOS is in control of DDR CKE mode and idle timer value. [PCODE]: pcode will manage the modes. |
| REFRESH_2X_MODE | [Disabled], [1- Enabled for WARM or HOT], [2- Enabled HOT only] | 0 – Disabled 1 – iMC enables 2xRef when Warm and Hot 2 – iMC enables 2xRef when Hot |
| SelfRefresh Enable | [Disabled], [Enabled] | Enable = Def |
| SelfRefresh IdleTimer | Value input | Range [64K-1;512] in DLCK800s, (512 = Def) |
| Throttler CKEMin Defeature | [Enabled], [Disabled] | Enable or disable Throttler CKEMin Defeature |
| Throttler CKEMin Timer | Value input | Timer value for CKEMin, range [255;0]. Req'd min of SC_ROUND_T + BYTE_LENGTH (4) |
| Allow Opp Ref Below Write Threshold | [Disabled], [Enabled] | Allow opportunistic refreshes while we don't exit power down. |
| Write Threshold | Value input | Number of writes that can be accumulated while CKE is low before CKE is asserted. |
| For LPDDR Only: Throttler CKEMin Defeature | [Enabled], [Disabled] | For LPDDR Only Enable or disable Throttler CKEMin Defeature |

| Feature | Option | Description |
|--|-------------|---|
| For LPDDR Only: Throttler CKEMin Timer | Value input | For LPDDR Only: Timer value for CKEMin, range [255;0]. Req'd min of SC_ROUND_T + BYTE_LENGTH (4) |

Figure 143: BIOS Chipset Setup Menu – System Agent (SA) Configuration – Memory Configuration – Memory Training Algorithms

| Aptio Setup – AMI | |
|---|------------|
| Chipset | |
| Early Command Training | [Enabled] |
| SenseAmp Offset Training | [Disabled] |
| Early ReadMPR Timing Centering 2D | [Enabled] |
| Read MPR Training | [Disabled] |
| Receive Enable Training | [Enabled] |
| Jedec Write Leveling | [Enabled] |
| Early Write Time Centering 2D | [Enabled] |
| Early Read Time Centering 2D | [Enabled] |
| Write Timing Centering 1D | [Enabled] |
| Write Voltage Centering 1D | [Enabled] |
| Read Timing Centering 1D | [Enabled] |
| Dimm ODT Training* | [Enabled] |
| Max RTT_WR ⁽¹⁾ | [ODT Off] |
| DIMM RON Training* | [Disabled] |
| Write Drive Strength / Equalization 2D* | [Disabled] |
| Write Slew Rate Training* | [Enabled] |
| Read ODT Training* | [Enabled] |
| Read Equalization Training* | [Enabled] |
| Read Amplifier Training* | [Enabled] |
| Write Timing Centering 2D | [Enabled] |
| Read Timing Centering 2D | [Enabled] |
| Command Voltage Centering | [Enabled] |
| Write Voltage Centering 2D | [Enabled] |
| Read Voltage Centering 2D | [Enabled] |
| Late Command Training | [Enabled] |
| Round Trip Latency | [Enabled] |
| Turn Around Timing Training | [Disabled] |
| CMD CTL CLK Slew Rate | [Enabled] |
| CMD/CTL DS & E 2D | [Enabled] |
| Read Voltage Centering 1D | [Enabled] |
| TxDqTCO Comp Training* | [Enabled] |
| ClkTCO Comp Training* | [Enabled] |
| TxDqsTCO Comp Training* | [Enabled] |

| Aptio Setup – AMI | | |
|--|------------|------------------------|
| Chipset | | |
| VccDLL Bypass Training | [Enabled] | |
| CMD/CTL Drive Strength Up/Dn 2D | [Enabled] | |
| DIMM CA ODT Training | [Enabled] | |
| PanicVttDnLp Training* | [Enabled] | |
| Read Vref Decap Training* | [Enabled] | |
| Vddq Training | [Disabled] | |
| Duty Cycle Correction Training | [Enabled] | |
| Rank Margin Tool Per Bit | [Disabled] | |
| DIMM DFE Training | [Enabled] | |
| EARLY DIMM DFE Training | [Enabled] | |
| Tx Dqs Dcc Training | [Enabled] | |
| DRAM DCA Training | [Enabled] | |
| Write Driver Strength Training | [Enabled] | |
| Rank Margin Tool | [Disabled] | → ←: Select Screen |
| Memory Test | [Disabled] | ↑ ↓: Select Item |
| DQS OFFSET ADJUST Training | [Enabled] | Enter: Select |
| DIMM SPD Alias Test | [Disabled] | +/-: Change Opt. |
| Receive Enable Centering 1D | [Enabled] | F1: General Help |
| Retrain Margin Check | [Disabled] | F2: Previous Values |
| Write Drive Strength Up/Dn independently | [Enabled] | F3: Optimized Defaults |
| Margin Check Limit | [Disabled] | F4: Save & Exit |
| Maring Limit Check L2 ⁽²⁾ | 100 | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

⁽¹⁾ This item activates only when enabling Read Timing Centering 1D.

⁽²⁾ This item activates only when selecting L2 or Both for Margin Check Limit.

| Feature | Option | Description |
|-----------------------------------|--------------------------|---|
| Early Command Training | [Disabled], [Enabled] | Enable or disable Early Command Training |
| SenseAmp Offset Training | [Disabled], [Enabled] | Enable or disable SenseAmp Offset Training |
| Early ReadMPR Timing Centering 2D | [Disabled], [Enabled] | Enable or disable Early ReadMPR Timing Centering 2D |
| Read MPR Training | [Disabled], [Enabled] | Enable or disable Read MPR Training |
| Receive Enable Training | [Disabled], [Enabled] | Enable or disable Receive Enable Training |
| Jedec Write Leveling | [Disabled], [Enabled] | Enable or disable Jedec Write Leveling |
| Early Write Time Centering 2D | [Disabled], [Enabled] | Enable or disable Early Write Time Centering 2D |

| Feature | Option | Description |
|---|--------------------------|---|
| Early Read Time Centering 2D | [Disabled], [Enabled] | Enable or disable Early Read Time Centering 2D |
| Write Timing Centering 1D | [Disabled], [Enabled] | Enable or disable Write Timing Centering 1D |
| Write Voltage Centering 1D | [Disabled], [Enabled] | Enable or disable Write Voltage Centering 1D |
| Read Timing Centering 1D | [Disabled], [Enabled] | Enable or disable Read Timing Centering 1D |
| Dimm ODT Training* | [Disabled], [Enabled] | Dimm On-Die Termination Training* |
| Max RTT_WR | [ODT Off], [120 Ohms] | Caps the maximum RTT_WR in power training. |
| DIMM RON Training* | [Disabled], [Enabled] | Enable or disable DIMM RON Training* |
| Write Drive Strength / Equalization 2D* | [Disabled], [Enabled] | Enable or disable Write Drive Strength / Equalization 2D* |
| Write Slew Rate Training* | [Disabled], [Enabled] | Enable or disable Write Slew Rate Training* |
| Read ODT Training* | [Disabled], [Enabled] | Read On-Die Termination Training* |
| Read Equalization Training* | [Disabled], [Enabled] | Enable or disable Read Equalization Training* |
| Read Amplifier Training* | [Disabled], [Enabled] | Enable or disable Read Amplifier Training* |
| Write Timing Centering 2D | [Disabled], [Enabled] | Write Dq-Dqs Timing Centering 2D |
| Read Timing Centering 2D | [Disabled], [Enabled] | Read Dq-Dqs Timing Centering 2D |
| Command Voltage Centering | [Disabled], [Enabled] | Enable or disable Command Voltage Centering |
| Write Voltage Centering 2D | [Disabled], [Enabled] | Enable or disable Write Voltage Centering 2D |
| Read Voltage Centering 2D | [Disabled], [Enabled] | Enable or disable Read Voltage Centering 2D |
| Late Command Training | [Disabled], [Enabled] | Enable or disable Late Command Training |
| Round Trip Latency | [Disabled], [Enabled] | Enable or disable Round Trip Latency Training |
| Turn Around Timing Training | [Disabled], [Enabled] | Enable or disable Turn Around Timing Training |
| CMD CTL CLK Slew Rate | [Disabled], [Enabled] | Enable or disable CMD CTL CLK Slew Rate |

| Feature | Option | Description |
|---------------------------------|--------------------------|---|
| CMD/CTL DS & E 2D | [Disabled], [Enabled] | CMD/CTL Drive Strength and Equalization 2D |
| Read Voltage Centering 1D | [Disabled], [Enabled] | Enable or disable Read Voltage Centering 1D |
| TxDqTCO Comp Training* | [Disabled], [Enabled] | Enable or disable TxDqTCO Comp Training* |
| ClkTCO Comp Training* | [Disabled], [Enabled] | Enable or disable ClkTCO Comp Training* |
| TxDqsTCO Comp Training* | [Disabled], [Enabled] | Enable or disable TxDqsTCO Comp Training* |
| VccDLL Bypass Training | [Disabled], [Enabled] | Enable or disable VccDLL Bypass Training |
| CMD/CTL Drive Strength Up/Dn 2D | [Disabled], [Enabled] | Enable or disable CMD/CTL Drive Strength Up/Dn 2D |
| DIMM CA ODT Training | [Disabled], [Enabled] | Enable or disable DIMM CA ODT Training |
| PanicVttDnLP Training* | [Disabled], [Enabled] | Enable or disable PanicVttDnLp Training* |
| Read Vref Decap Training | [Disabled], [Enabled] | Enable or disable Vref Decap Training* |
| Vddq Training | [Disabled], [Enabled] | Enable or disable Vddq Training |
| Duty Cycle Correction Training | [Disabled], [Enabled] | Enable or disable Duty Cycle Correction Training |
| Rank Margin Tool Per Bit | [Disabled], [Enabled] | Enable or disable Rank Margin Tool Per Bit |
| DIMM DFE Training | [Disabled], [Enabled] | Enable or disable DIMM DFE Training |
| EARLY DIMM DFE Training | [Disabled], [Enabled] | Enable or disable EARLY DIMM DFE Training |
| Tx Dqs Dcc Training | [Disabled], [Enabled] | Enable or disable Tx Dqs duty cycle Training |
| DRAM DCA Training | [Disabled], [Enabled] | Enable or disable DRAM DCA Training |
| Write Driver Strength Training | [Disabled], [Enabled] | Enable or disable Write Driver Strength Training |
| Rank Margin Tool | [Disabled], [Enabled] | Enable or disable Rank Margin Tool Training |
| Memory Test | [Disabled], [Enabled] | Enable or disable Memory Test Training |
| DQS OFFSET ADJUST Training | [Disabled], [Enabled] | Enable or disable DQS OFFSET ADJUST Training |

| Feature | Option | Description |
|--|---|---|
| DIMM SPD Alias Test | [Disabled], [Enabled] | Enable or disable DIMM SPD Alias Test |
| Receive Enable Centering 1D | [Disabled], [Enabled] | Enable or disable Receive Enable Centering 1D |
| Retrain Margin Check | [Disabled], [Enabled] | Enable or disable Retrain Margin Check |
| Write Drive Strength Up/Dn independently | [Disabled], [Enabled] | Enable or disable Write Drive Strength Up/Dn independently |
| Margin Check Limit | [Disabled], [L1], [L2], [Both] | Checks Margin to Limit to see if next boot memory needs to be retrain |
| Margin Limit Check L2 | Value input | L2 check threshold is scale of L1 check. Ex. 200 is 2x L1 Check |

Figure 144: BIOS Chipset Setup Menu – System Agent (SA) Configuration – Graphics Configuration

| Aptio Setup – AMI | | |
|---|---|------------------------|
| Chipset | | |
| Graphics Configuration | | |
| Graphics Turbo IMON Current | 31 | |
| Skip Scanning of External Gfx Card | [Disabled] | |
| > External Gfx Card Primary Display Configuration | | |
| GTT Size | [8MB] | |
| PSMI SUPPORT | [Disabled] | |
| PSMI Region Size ⁽¹⁾ | [32MB] | |
| Intel Graphics Pei Display Peim | [Disabled] | |
| VDD Enable | [Enabled] | |
| Configure GT for use | [Enabled] | → ←: Select Screen |
| RC1p Support ⁽²⁾ | [Disabled] | ↑ ↓: Select Item |
| PAVP Enable | [Enabled] | Enter: Select |
| Cdynmax Clamping Enable | [Disabled] | +/-: Change Opt. |
| Cd Clock Frequency | [Max CdClock freq based on Reference Clk] | F1: General Help |
| Enable Display Audio Link in Pre-OS | [Disabled] | F2: Previous Values |
| IUER Button Enable | [Disabled] | F3: Optimized Defaults |
| > LCD Control | | F4: Save & Exit |
| > Intel® Ultrabook Event Support | | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

⁽¹⁾ This item appears only when enabling PSMI SUPPORT.

⁽²⁾ This item appears only when enabling Configure GT for use.

| Feature | Option | Description |
|-------------------------------------|---|--|
| Graphics Turbo IMON Current | Value input | Graphics turbo IMON current values supported (14 - 31) |
| Skip Scanning of External Gfx Card | [Disabled], [Enabled] | If Enable, it will not scan for External Gfx Card on PEG and PCH PCIE Ports |
| GTT Size | [2MB], [4MB], [8MB] | Select the GTT Size |
| PSMI SUPPORT | [Disabled], [Enabled] | PSMI Enable / Disable |
| PSMI Region Size | [32MB], [288MB], [544MB], [800MB], [1024MB] | Select the PSMI Region Size: Range from 32MB to 1024MB |
| Intel Graphics Pei Display Peim | [Enabled], [Disabled] | Enable / Disable Pei (Early) Display |
| VDD Enable | [Disabled], [Enabled] | Enable / Disable forcing of VDD in the BIOS |
| Configure GT for use | [Enabled], [Disabled] | Enable / Disable GT configuration in BIOS |
| RC1p Support | [Enabled], [Disabled] | Enable / Disable RC1p support. If RC1p is enabled, send a RC1p frequency request to PMA based other conditions being met |
| PAVP Enable | [Enabled], [Disabled] | Enable / Disable PAVP |
| Cdynmax Clamping Enable | [Enabled], [Disabled] | Enable / Disable Cdynmax Clamping |
| Cd Clock Frequency | [192 Mhz], [307.2 Mhz], [556.8 Mhz], [652.8 Mhz], [Max CdClock freq based on Reference Clk] | Select the highest Cd Clock frequency supported by the platform |
| Enable Display Audio Link in Pre-OS | [Disabled], [Enabled] | [Enabled]: Display Audio Link will be enabled in Pre-OS. [Disabled]: Display Audio Link will be disabled in Pre-OS. |
| IUER Button Enable | [Disabled], [Enabled] | Enable / Disable IUER Button Functionality |

Figure 145: BIOS Chipset Setup Menu – System Agent (SA) Configuration – Graphics Configuration – External Gfx Card Primary Display Configuration

| Aptio Setup – AMI | |
|---|---|
| Chipset | |
| External Gfx Card Primary Display Configuration | → ←: Select Screen ↑ ↓ : Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

Figure 146: BIOS Chipset Setup Menu – System Agent (SA) Configuration – Graphics Configuration – LCD Control

| Aptio Setup – AMI | |
|--|---|
| Chipset | |
| LCD Control | |
| LCD Panel Type | [VBIOS Default] |
| Panel Scaling | [Auto] |
| Backlight Control | [PWM Normal] |
| Active LFP | [eDP Port-A] |
| Panel Color Depth | [18 Bit] |
| Backlight Brightness | 255 |
| | → ←: Select Screen ↑ ↓ : Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

| Feature | Option | Description |
|----------------|---|--|
| LCD Panel Type | [VBIOS Default], [640x480 LVDS], [800x600 LVDS], [1024x768 LVDS], [1280x1024 LVDS], [1400x1050 LVDS1], [1400x1050 LVDS2], [1600x1200 LVDS], [1280x768 LVDS], [1680x1050 LVDS], | Select LCD panel used by Internal Graphics Device by selecting the appropriate setup item. |

| Feature | Option | Description |
|----------------------|---|---|
| | [1920x1200 LVDS], [1600x900 LVDS], [1280x800 LVDS], [1280x600 LVDS], [2048x1536 LVDS], [1366x768 LVDS] | |
| Panel Scaling | [Auto], [Off], [Force Scaling] | Select the LCD panel scaling option used by the Internal Graphics Device. |
| Backlight Control | [PWM Inverted], [PWM Normal] | Back Light Control Setting |
| Active LFP | [No eDP], [eDP Port-A] | Select the Active LFP Configuration. [No LVDS]: VBIOS does not enable LVDS. [Int-LVDS]: VBIOS enables LVDS driver by Integrated encoder. [SDVO LVDS]: VBIOS enables LVDS driver by SDVO encoder. [eDP Port-A]: LFP Driven by Int-DisplayPort encoder from Port-A. [eDP Port-D]: LFP Driven by Int-DisplayPort encoder from Port-D (through PCH). |
| Panel Color Depth | [18 Bit], [24 Bit] | Select the LFP Panel Color Depth |
| Backlight Brightness | Value input | Set VBIOS Brightness. Range: 0 – 255. |

Figure 147: BIOS Chipset Setup Menu – System Agent (SA) Configuration – Graphics Configuration – Intel® Ultrabook Event Support

| Aptio Setup – AMI | | |
|--|---------------|--|
| Chipset | | |
| Intel® Ultrabook Event Support | | |
| IUER Slate Enable | [Disabled] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Slate Mode boot value ⁽¹⁾ | [Laptop Mode] | |
| Slate Mode on S3 and S4 resume ⁽¹⁾ | [No change] | |
| IUER Dock Enable | [Disabled] | |
| Dock Mode boot value ⁽²⁾ | [Undocked] | |
| Dock Mode upon S3 and S4 resume ⁽²⁾ | [No change] | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

⁽¹⁾ These items appear only when enabling IUER Slate Enable.

⁽²⁾ These items appear only when enabling IUER Dock Enable.

| Feature | Option | Description |
|---------------------------------|--------------------------------|--|
| IUER Slate Enable | [Disabled], [Enabled] | Enable / Disable IUER Slate Functionality |
| Slate Mode boot value | [Slate Mode], [Laptop Mode] | Choose Slate or Laptop as boot mode. |
| Slate Mode on S3 and S4 resume | [No change], [Toggle] | Keep it the same as Sx entry or toggle it. |
| IUER Dock Enable | [Disabled], [Enabled] | Enable / Disable IUER Dock Functionality |
| Dock Mode boot value | [Undocked], [Docked] | Choose Docked or Undocked as boot mode. |
| Dock Mode upon S3 and S4 resume | [No change], [Toggle] | Keep it the same as Sx entry or toggle it. |

Figure 148: BIOS Chipset Setup Menu – System Agent (SA) Configuration – DMI/OPI Configuration

| Aptio Setup – AMI | | |
|--|------------|---|
| Chipset | | |
| DMI/OPI Configuration | | |
| CDR Relock for CPU DMI | [Disabled] | → ←: Select Screen ↑ ↓ : Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| DMI Gen3 Eq Phase 2 | [Auto] | |
| DMI Gen3 Eq Phase 3 Method | [Auto] | |
| DMI Gen3 ASPM | [ASPM L1] | |
| DMI ASPM | [ASPM L1] | |
| DMI Gen3 L1 Exit Latency | 4 | |
| New FOM for CPU DMI | [Disabled] | |
| > DMI Advanced Menu | | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|----------------------------|---|---|
| CDR Relock for CPU DMI | [Disabled], [Enabled] | Keep it the same as Sx entry or toggle it. |
| DMI Gen3 Eq Phase 2 | [Disabled], [Enabled], [Auto] | Perform Gen3 Equalization Phase 2 |
| DMI Gen3 Eq Phase 3 Method | [Auto], [Adaptive Hardware Equalization], [Adaptive Software Equalization], [Static Equalization], [Disabled] | Select Method foe Gen3 Equalization Phase 3 |

| Feature | Option | Description |
|--------------------------|---|--------------------------|
| DMI Gen3 ASPM | [Disabled], [Auto], [ASPM L0s], [ASPM L1], [ASPM L0sL1] | DMI Gen3 ASPM Support |
| DMI ASPM | [Disabled], [Auto], [ASPM L0s], [ASPM L1], [ASPM L0sL1] | DMI ASPM Support |
| DMI Gen3 L1 Exit Latency | Value input | DMI Gen3 L1 Exit Latency |
| New FOM for CPU DMI | [Disabled], [Enabled] | Enable / Disable New FOM |

Figure 149: BIOS Chipset Setup Menu – System Agent (SA) Configuration – DMI/OPI Configuration – DMI Advanced Menu

| Aptio Setup – AMI | |
|---------------------------|---------|
| Chipset | |
| DMI Advanced Menu | |
| DMI Gen4 EQ Mode | [HW EQ] |
| DMI Gen4 RTCO Cpre Lane0 | 0 |
| DMI Gen4 RTCO Cpost Lane0 | 0 |
| DMI Gen4 RTCO Cpre Lane1 | 14 |
| DMI Gen4 RTCO Cpost Lane1 | 7 |
| DMI Gen4 RTCO Cpre Lane2 | 10 |
| DMI Gen4 RTCO Cpost Lane2 | 6 |
| DMI Gen4 RTCO Cpre Lane3 | 7 |
| DMI Gen4 RTCO Cpost Lane3 | 7 |
| DMI Gen4 RTCO Cpre Lane4 | 7 |
| DMI Gen4 RTCO Cpost Lane4 | 7 |
| DMI Gen4 RTCO Cpre Lane5 | 7 |
| DMI Gen4 RTCO Cpost Lane5 | 7 |
| DMI Gen4 RTCO Cpre Lane6 | 7 |
| DMI Gen4 RTCO Cpost Lane6 | 7 |
| DMI Gen4 RTCO Cpost Lane7 | 7 |
| DMI Gen4 RTCO Cpre Lane7 | 7 |
| DMI Gen3 RTCO Cpre Lane0 | 0 |
| DMI Gen3 RTCO Cpost Lane0 | 0 |
| DMI Gen3 RTCO Cpre Lane1 | 0 |
| DMI Gen3 RTCO Cpost Lane1 | 0 |

| Aptio Setup – AMI | | |
|--|---|---|
| Chipset | | |
| DMI Gen3 RTCO Cpre Lane2 | 0 | → ←: Select Screen ↑ ↓ : Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| DMI Gen3 RTCO Cpost Lane2 | 0 | |
| DMI Gen3 RTCO Cpre Lane3 | 0 | |
| DMI Gen3 RTCO Cpost Lane3 | 0 | |
| DMI Gen3 RTCO Cpre Lane4 | 0 | |
| DMI Gen3 RTCO Cpost Lane4 | 0 | |
| DMI Gen3 RTCO Cpre Lane5 | 0 | |
| DMI Gen3 RTCO Cpost Lane5 | 0 | |
| DMI Gen3 RTCO Cpre Lane6 | 0 | |
| DMI Gen3 RTCO Cpost Lane6 | 0 | |
| DMI Gen3 RTCO Cpre Lane7 | 0 | |
| DMI Gen3 RTCO Cpost Lane7 | 0 | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|---|---------------------------------------|---|
| DMI Gen4 EQ Mode | [Disabled], [Fixed EQ], [HW EQ] | DMI Gen4 EQ Mode |
| DMI Gen4 RTCO Cpre Lane0/1/2/3/4/5/6/7 | Value input | DMI Gen4 Lane Transmitter Pre-Cursor Coefficient values. |
| DMI Gen4 RTCO Cpost Lane0/1/2/3/4/5/6/7 | Value input | DMI Gen4 Lane Transmitter Post-Cursor Coefficient values. |
| DMI Gen3 RTCO Cpost Lane0/1/2/3/4/5/6/7 | Value input | DMI Gen3 Lane Transmitter Pre-Cursor Coefficient values. |
| DMI Gen3 RTCO Cpre Lane0/1/2/3/4/5/6/7 | Value input | DMI Gen3 Lane Transmitter Post-Cursor Coefficient values. |

Figure 150: BIOS Chipset Setup Menu – System Agent (SA) Configuration – TCSS setup menu

| Aptio Setup – AMI | |
|-----------------------------|--|
| Chipset | |
| TCSS Configuration | |
| IOM FW version: 23000800 | |
| PHY FW version: 0FA7 | |
| TBT FW IMR Status: 00000000 | |
| TBT FW version: N/A | |

| Aptio Setup – AMI | | |
|--|------------|---|
| Chipset | | |
| Deepest TC state: 0000 | | |
| TCSS xHCI Support | [Enabled] | → ←: Select Screen ↑ ↓ : Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| > TCSS USB Configuration* | | |
| VCCST status of IOM* | [Enabled] | |
| D3 Cold Enable/Disable* | [Disabled] | |
| D3Hot* | [Disabled] | |
| Tc C-State Limit* | [Disabled] | |
| TC Cold Power Saving Factor* | [Disabled] | |
| IOM before entering TC cold ⁽¹⁾ | 10 | |
| IOM stay in TC cold ⁽¹⁾ | 50 | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when enabling TCSS xHCI Support.

⁽¹⁾ These items appear only when enabling TC Cold Power Saving Factor.

| Feature | Option | Description |
|-----------------------------|---|---|
| TCSS xHCI Support | [Disabled], [Enabled] | Enable / Disable TCSS xHCI |
| VCCST status of IOM | [Disabled], [Enabled] | Enables / Disables VCCST. [Enabled]: Sends VCCST ON message to EC or PMC. [Disabled]: Sends VCCST OFF message to EC or PMC. |
| D3 Cold Enable / Disable | [Disabled], [Enabled] | Enables / Disables D3 Cold. [Enabled]: D3 cold support for IOM is enabled. [Disabled]: D3 cold support for IOM is disabled. |
| D3Hot | [Disabled], [Enabled] | Enables / Disables D3 Hot. [Enabled]: D3 Hot support for IOM is enabled. [Disabled]: D3 Hot support for IOM is disabled. |
| Tc C-State Limit | [Disabled], [1], [2], [4], [5], [6], [7], [10] | BIOS mailbox to limit deepest TCx state |
| TC Cold Power Saving Factor | [Disabled], [Enabled] | TC Cold Power Saving Factor Switch |
| IOM before entering TC cold | Value input | Represent Y in seconds for IOM before entering TC cold |
| IOM stay in TC cold | Value input | Represent X in seconds for IOM stays in TC cold |

Figure 151: BIOS Chipset Setup Menu – System Agent (SA) Configuration – Display setup menu

| Aptio Setup – AMI | |
|--|---|
| Chipset | |
| Display Configurations | |
| | → ←: Select Screen ↑ ↓ : Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

Figure 152: BIOS Chipset Setup Menu – System Agent (SA) Configuration – PCI Express Configuration

| Aptio Setup – AMI | |
|---|---|
| Chipset | |
| PCI Express Configuration | |
| Fia Programming [Enabled] Compliance Test Mode [Disabled] CDR Relock [Enabled] Assertion on Link Down GPIOs [Disabled] PCI Express Slot Selection [M2] > PCI Express Root Port 1 > PCI Express Root Port 2 > PCI Express Root Port 3 | → ←: Select Screen ↑ ↓ : Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

| Feature | Option | Description |
|------------------------------|--------------------------|---|
| Fia | [Disabled], [Enabled] | Load Fia Configuration if Enabled for each root port. |
| Compliance Test Mode | [Disabled], [Enabled] | Enable when using Compliance Load Board |
| CDR Relock | [Disabled], [Enabled] | Enable / Disable CDR Relock |
| Assertion on Link Down GPIOs | [Disabled], [Enabled] | GPIO Assertion on Link Down |

| Feature | Option | Description |
|----------------------------|-----------------------|----------------------------------|
| PCI Express Slot Selection | [M2], [CEMx4 slot] | Select the PCIe M2 or CEMx4 slot |

Figure 153: BIOS Chipset Setup Menu – System Agent (SA) Configuration – PCI Express Configuration – PCI Express Root Port 1/2/3

| Aptio Setup – AMI | |
|---|---------------|
| Chipset | |
| PCI Express Root Port 1/2/3 | [Enabled] |
| Connection Type* | [Slot] |
| PCI Express Clock Gating* | [Disabled] |
| PCI Express Power Gating* | [Disabled] |
| ASPM* | [Disabled] |
| L1 Substates* | [L1.1 & L1.2] |
| Gen3 Eq Phase3 Method* | [Hardware] |
| Gen4 Eq Phase3 Method* | [Hardware] |
| ACS* | [Enabled] |
| PTM* | [Enabled] |
| DPC* | [Disabled] |
| FOM Scoreboard Control Policy* | [Auto] |
| Multi-VC* | [Disabled] |
| EDPC* | [Enabled] |
| URR* | [Disabled] |
| FER* | [Disabled] |
| NFER* | [Disabled] |
| CER* | [Disabled] |
| CTO* | [Disabled] |
| SEFE* | [Disabled] |
| SENF* | [Disabled] |
| SECE* | [Disabled] |
| PME SCI* | [Enabled] |
| Hot Plug* ⁽³⁾ | [Disabled] |
| Advanced Error Reporting* | [Enabled] |
| PCIe Speed* | [Auto] |
| Enable ClockReq Messaging* | [Disabled] |
| Transmitter Half Swing* | [Disabled] |
| Detect Timeout* | 0 |
| P2P Support* | [Disabled] |
| CPU PCIe Func0 Link Disable* ⁽³⁾ | [Disabled] |
| SA PCIe LTR Configuration* | |
| LTR* | [Enabled] |

| Aptio Setup – AMI | | | |
|--|------------|--|--|
| Chipset | | | |
| Snoop Latency Override*# | [Auto] | | |
| Snoop Latency Value*#(1) | 60 | | |
| Snoop Latency Multiplier*#(1) | [1024 ns] | | |
| Non Snoop Latency Override*# | [Auto] | | |
| Non Snoop Latency Value*#(2) | 60 | | |
| Non Snoop Latency Multiplier*#(2) | [1024 ns] | | |
| Force LTR Override*# | [Disabled] | | |
| LTR Lock* | [Disabled] | | |
| CPU PCIe Gen3 HWEQ Config | | | |
| UPTP | 5 | | |
| DPTP | 7 | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit | |
| CPU PCIe Gen4 HWEQ Config | | | |
| UPTP | 8 | | |
| DPTP | 9 | | |
| CPU PCIe Gen5 HWEQ Config | | | |
| UPTP ⁽⁵⁾ | 5 | | |
| DPTP ⁽⁵⁾ | 7 | | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | | |

- * These items appear only when enabling PCI Express Root Port 1/2/3.
- # These items appear only when enabling LTR.
- (1) These items appear only when selecting Manual for Snoop Latency Override.
- (2) These items appear only when selecting Manual for Mon Snoop Latency Override.
- (3) This item is available only for PCI Express Root Port 1/3.
- (4) This item is available only for PCI Express Root Port 1.
- (5) These items are available only for PCI Express Root Port 2.

| Feature | Option | Description |
|-----------------------------|--------------------------|---|
| PCI Express Root Port 1/2/3 | [Disabled], [Enabled] | Control the PCI Express Root Port. |
| Connection Type | [Bulit-in], [Slot] | [Built-in]: a built-in device is connected to this rootport. SlotImplemented bit will be clear. [Slot]: this rootport connects to user-accessible slot. SlotImplemented bit will be set. |
| PCI Express Clock Gating | [Disabled], [Enabled] | PCI Express Clock Gating Enable / Disable for each root port. |
| PCI Express Power Gating | [Disabled], [Enabled] | PCI Express Power Gating Enable / Disable for each root port. |
| ASPM | [Disabled], [L0s], | Set the ASPM Level: Force L0s – Force all links to L0s State |

| Feature | Option | Description |
|-------------------------------|---|--|
| | [L1], [L0sL1] | AUTO – BIOS auto configure DISABLE – Disables ASPM |
| L1 Substates | [L1.1 & L1.2] | Read only item |
| Gen3/4 Eq Phase3 Method | [Hardware], [Static Coeff.] | PCIe Gen3/4 Equalization Phase 3 Method |
| ACS | [Disabled], [Enabled] | Enable / Disable Access Control Services Extended Capability |
| PTM | [Disabled], [Enabled] | Enable / Disable Precision Time Measurement |
| DPC | [Disabled], [Enabled] | Enable / Disable Downstream Port Containment |
| FOM Scoreboard Control Policy | [Auto], [Gen3], [Gen4], [Gen3/Gen4], [Gen5] | Select the FOM Scoreboard Control Policy, when set to Auto, speed is based on TLS. |
| Multi-VC | [Disabled], [Enabled] | Enable / Disable Multi Virtual Channel |
| EDPC | [Disabled], [Enabled] | Enable / Disable Rootport extensions for Downstream Port Containment |
| URR | [Disabled], [Enabled] | PCI Express Unsupported Request Reporting Enable / Disable. |
| FER | [Disabled], [Enabled] | PCI Express Device Fatal Error Reporting Enable / Disable. |
| NFER | [Disabled], [Enabled] | PCI Express Device Non-Fatal Error Reporting Enable / Disable. |
| CER | [Disabled], [Enabled] | PCI Express Device Correctable Error Reporting Enable / Disable. |
| CTO | [Disabled], [Enabled] | PCI Express Completion Timer TO Enable / Disable. |
| SEFE | [Disabled], [Enabled] | Root PCI Express System Error on Fatal Error Enable / Disable. |
| SENF | [Disabled], [Enabled] | Root PCI Express System Error on Non-Fatal Error Enable / Disable. |
| SECE | [Disabled], [Enabled] | Root PCI Express System Error on Correctable Error Enable / Disable. |
| PME SCI | [Disabled], [Enabled] | PCI Express PME SCI Enable / Disable. |
| Hot Plug | [Disabled], [Enabled] | PCI Express Hot Plug Enable / Disable. |
| Advanced Error Reporting | [Disabled], [Enabled] | Advanced Error Reporting Enable / Disable. |
| PCIe Speed | [Auto], | Configure PCIe Speed |

| Feature | Option | Description |
|------------------------------|--|--|
| | [Gen1], [Gen2], [Gen3], [Gen4], [Gen5] | Option [Gen5] only for PCI Express Root Port 2/3 |
| Enable ClockReq Messaging | [Enabled], [Disabled] | Enable or Disable ClockReq Messaging |
| Transmitter Half Swing | [Disabled], [Enabled] | Transmitter Half Swing Enable / Disable. |
| Detect Timeout | Value input | The number of milliseconds reference code will wait for link to exit Detect state for enabled ports before assuming there is no device and potentially disabling the port. |
| P2P Support | [Disabled], [Enabled] | Program P2P Support Registers according to setup option |
| CPU PCIE Func0 Link Disable | [Disabled], [Enabled] | CPU PCIE Func0 Link Disable while Device attached into Port having Func0 and FuncN. |
| LTR | [Disabled], [Enabled] | SA PCIE Latency Reporting Enable / Disable |
| Snoop Latency Override | [Disabled], [Manual], [Auto] | Snoop Latency Override for SA PCIE. [Disabled]: Disable override. [Manual]: Manually enter override values. [Auto] (default): Maintain default BIOS flow. |
| Snoop Latency Value | Value input | LTR Snoop Latency value of SA PCIE |
| Snoop Latency Multiplier | [1 ns], [32 ns], [1024 ns], [32768 ns], [1048576 ns], [33554432 ns] | LTR Snoop Latency Multiplier of SA PCIE |
| Non Snoop Latency Override | [Disabled], [Manual], [Auto] | Non Snoop Latency Override for SA PCIE. [Disabled]: Disable override. [Manual]: Manually enter override values. [Auto] (default): Maintain default BIOS flow. |
| Non Snoop Latency Value | Value input | LTR Non Snoop Latency value of PCH PCIE |
| Non Snoop Latency Multiplier | [1 ns], [32 ns], [1024 ns], [32768 ns], [1048576 ns], [33554432 ns] | LTR Non Snoop Latency Multiplier of SA PCIE |
| Force LTR Override | [Disabled], [Enabled] | Force LTR Override for SA PCIE. [Disabled]: LTR override values will not be forced. |

| Feature | Option | Description |
|----------|--------------------------|---|
| | | [Enabled]: LTR override values will be forced and LTR messages from the device will be ignored. |
| LTR Lock | [Disabled], [Enabled] | PCIE LTR Configuration Lock |
| UPTP | Value input | Upstream Port Transmitter Preset |
| DPTP | Value input | Downstream Port Transmitter Preset |

Figure 154: BIOS Chipset Setup Menu – System Agent (SA) Configuration – MIPI Camera Configuration

| Aptio Setup – AMI | | |
|--|------------|--|
| Chipset | | |
| CVF Support | | |
| Control Logic 1 | [Disabled] | |
| > Control Logic options* | | |
| Control Logic 2 | [Disabled] | |
| > Control Logic options* | | |
| Control Logic 3 | [Disabled] | |
| > Control Logic options* | | |
| Control Logic 4 | [Disabled] | |
| > Control Logic options* | | |
| Camera1 | [Disabled] | |
| > Link options# | | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| > Flash options# | | |
| Camera2 | [Disabled] | |
| > Link options# | | |
| > Flash options# | | |
| Camera3 | [Disabled] | |
| > Link options# | | |
| Camera4 | [Disabled] | |
| > Link options# | | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when enabling Control Logic 1/2/3/4 respectively.

These items appear only when enabling Camera1/2/3/4 respectively.

| Feature | Option | Description |
|-----------------------|--|--|
| CVF Support | [Native IOs], [Disabled], [USB Bridge] | Disables / Enables CVF using either Native Ios or USB Ios Expansion. |
| Control Logic 1/2/3/4 | [Disabled], [Enabled] | Disable / Enable Control Logic 1/2/3/4 |
| Camera1/2/3/4 | [Disabled], [Enabled] | Disable / Enable Camera1/2/3/4 |

Figure 155: BIOS Chipset Setup Menu – System Agent (SA) Configuration – MIPI Camera Configuration – Control Logic options

| Aptio Setup – AMI | |
|--|---------------|
| Chipset | |
| Control Logic options | |
| Control Logic Type | [Discrete] |
| CRD Version | [CRD-D] |
| Input Clock ⁽¹⁾⁽²⁾⁽⁴⁾ | [19.2 MHz] |
| PCH Clock Source ⁽¹⁾⁽²⁾⁽⁴⁾ | [IMGCLKOUT_0] |
| PMIC Flash Panel ^{(1)(2)(3)*} | [Back] |
| I2C Channel ⁽²⁾⁽⁴⁾ | [I2C3] |
| I2C Address ⁽²⁾⁽⁴⁾ | 4D |
| WLED1 Type ⁽²⁾ | [White Led] |
| WLED1 Flash Max Current ⁽²⁾ | 0 |
| WLED1 Torch Max Current ⁽²⁾ | 0 |
| WLED2 Type ⁽²⁾ | [IR Led] |
| WLED2 Flash Max Current ⁽²⁾ | 0 |
| WLED2 Torch Max Current ⁽²⁾ | 0 |
| SubPlatformId ⁽²⁾ | 0 |
| Number of GPIO Pins ⁽¹⁾⁽²⁾⁽³⁾ | 3 |
| GPIO 0 ⁽¹⁾⁽²⁾⁽³⁾ | |
| Group Pad Number ⁽¹⁾⁽²⁾⁽³⁾ | 21 |
| Group Number ⁽¹⁾⁽²⁾⁽³⁾ | [A] |
| Function ⁽¹⁾⁽²⁾⁽³⁾ | [Reset] |
| Active Value ⁽¹⁾⁽²⁾⁽³⁾ | 1 |
| Initial Value ⁽¹⁾⁽²⁾⁽³⁾ | 0 |
| GPIO 1 ⁽¹⁾⁽²⁾⁽³⁾ | |
| Group Pad Number ⁽¹⁾⁽²⁾⁽³⁾ | 23 |
| Group Number ⁽¹⁾⁽²⁾⁽³⁾ | [B] |
| Function ⁽¹⁾⁽²⁾⁽³⁾ | [Power_En] |
| Active Value ⁽¹⁾⁽²⁾⁽³⁾ | 1 |
| Initial Value ⁽¹⁾⁽²⁾⁽³⁾ | 0 |
| GPIO 2 ⁽¹⁾⁽²⁾⁽³⁾ | |
| Group Pad Number ⁽¹⁾⁽²⁾⁽³⁾ | 14 |
| Group Number ⁽¹⁾⁽²⁾⁽³⁾ | [B] |
| Function ⁽¹⁾⁽²⁾⁽³⁾ | [pLED_En] |
| Active Value ⁽¹⁾⁽²⁾⁽³⁾ | 1 |
| Initial Value ⁽¹⁾⁽²⁾⁽³⁾ | 0 |
| → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit | |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

⁽¹⁾ These items appear when selecting Discrete for Control Logic Type.⁽²⁾ These items appear when selecting PMIC_TPS68470 or PMIC_UP6641 for Control Logic Type.⁽³⁾ These items appear when selecting PMIC_HDMI2MIPI_LT6911UXC for Control Logic Type.⁽⁴⁾ These items appear when selecting PMIC_USER0/1 for Control Logic Type.

* This item appears when selecting CRD-G or CRD-G2 for CRD Version.

| Feature | Option | Description |
|---------------------------|---|---|
| Control Logic Type | [Discrete], [PMIC_TPS68470], [PMIC_UP6642], [PMIC_HDMI2MIPI_L T6911UXC], [PMIC_USER0], [PMIC_USER1] | Control Logic Type |
| CRD Version | [PTC], [CRD-G], [Kilshon-PPV], [CRD-D], [CRD-G2], [LT6911UXC-V1] | CRD Version |
| Input Clock | [24 MHz], [26 MHz], [20 MHz], [19.2 MHz] | Input Clock |
| PCH Clock Source | [IMGCLKOUT_0], [IMGCLKOUT_1], [IMGCLKOUT_2], [IMGCLKOUT_3], [IMGCLKOUT_4] | This option specifies which IMGCLKOUT is chosen |
| PMIC Flash Panel | [Front], [Back] | PMIC Flash Panel |
| I2C Channel | [I2C0], [I2C1], [I2C2], [I2C3], [I2C4], [I2C5], [I2C6], [I2C7] | I2C Channel |
| I2C Address | Value input | I2C Address |
| WLED1/2 Type | [Disabled], [White Led], [Warm Led], [IR Led], [Xeon Led] | WLED Type |
| WLED1/2 Flash Max Current | Value input | WLED Flash Max Current Valid range is 0x00-0x1F 0x00 for HW default max current |
| WLED1/2 Torch Max Current | Value input | WLED Torch Max Current Valid range is 0x00-0x07 0x00 for HW default max current |
| SubPlatformId | Value input | SubPlatformId |
| Number of GPIO Pins | Value input | Number of GPIO Pins |
| Group Pad Number | Value input | Group Pad Number |

| Feature | Option | Description |
|---------------|--|---------------|
| Group Number | [A], [B], [C], [E], [F], [H], [S], [T], [U], [D], [R] | Group Number |
| Function | [Reset], [Power_En], [Clock_En], [pLED_En], [Strobe_En], [Handshake_En], [READY_STAT], [HDMI_DETECT] | Function |
| Active Value | Value input | Active Value |
| Initial Value | Value inpu | Initial Value |

Figure 156: BIOS Chipset Setup Menu – System Agent (SA) Configuration – MIPI Camera Configuration – Link options

| Aptio Setup – AMI | |
|--------------------------|-------------------|
| Chipset | |
| Camera1/2/3/4 | |
| Sensor Model | [OVTI01AS] |
| Lanes Clock division | [4 4 2 2] |
| CRD Version | [CRD-D] |
| GPIO control | [Control Logic 1] |
| Camera position | [Front] |
| Flash Support | [Enabled] |
| Privacy LED | [Driver default] |
| Rotation | [0] |
| PMIC Position* | [Position 1] |
| Voltage Rail*(1) | [3 voltage rail] |
| PPR Value | 10 |
| PPR Unit | A |
| Camera module name | YHRN |
| MIPI port | 1 |
| LaneUsed | [x1] |
| PortSpeed | [1] |
| MCLK | 19200000 |
| EEPROM Type | [ROM_NONE] |
| VCM Type | [VCM_NONE] |
| Number of I2C Components | 1 |
| I2C Channel | [I2C1] |
| Device 0 | |

→ ←: Select Screen
 ↑ ↓: Select Item
 Enter: Select
 +/-: Change Opt.
 F1: General Help

| Aptio Setup – AMI | | |
|--|------------|------------------------|
| Chipset | | |
| I2C Address | 36 | F2: Previous Values |
| Device Type | [Sensor] | F3: Optimized Defaults |
| Flash Driver Selection | [External] | F4: Save & Exit |
| Flash Driver Selection* | [Flash1] | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* This item appears only when selecting CRD-G2 for CRD Version.

⁽¹⁾ This item appears only when selecting Position 2 for PMIC Position.

| Feature | Option | Description |
|----------------------|--|----------------------|
| Sensor Model | [IMX135], [OV5693], [IMX179], [OV8858], [OV2740-IVCAM], [OV9728], [IMX188], [IMX208], [OV5670], [OV8865], [HM2051], [OV2742], [OV9234], [OV8856], [OV16860], [IMX362], [OVTID858], [IMX488], [OVTI01AS], [OVTI01A0], [OVTI5678], [OVTI9738], [HIMAX11B1], [LONTIUM], [User Custom] | Control Logic Type |
| Lanes Clock division | [4 4 2 2], [4 4 3 1], [4 4 4 0], [8 0 2 2], [8 0 3 1], [8 0 4 0] | Lanes Clock division |
| CRD Version | [PTC], [CRD-G], [Kilshon-PPV], [CRD-D], [CRD-G2] | CRD Version |
| GPIO control | [No Control Logic], [Control Logic 1], [Control Logic 2], [Control Logic 3], [Control Logic 4] | GPIO control |
| Camera position | [Front], [Back] | Camera position |
| Flash Support | [Driver default], [Disabled], [Enabled] | Flash Support |
| Privacy LED | [Driver default], [ILED A, 16mA], [ILED B, 2mA], | Privacy LED |

| Feature | Option | Description |
|--------------------|--|--|
| | [ILEDDB, 4mA], [ILEDDB, 8mA], [ILEDDB, 16mA] | |
| Rotation | [0], [90], [180], [270] | Rotation |
| PMIC Position | [Position 1], [Position 2] | OMIC Position Position 1 indicates the current module is placed on the left side of the CRD-G2 card. Position 2 indicates the current module is placed on the right side of the CRD-G2 card. |
| Voltage Rail | [3 voltage rail], [2 voltage rail] | Voltage Rail |
| PPR Value | Value input | PPR value of sensor |
| PPR Unit | Value input | PPR unit of sensor |
| Camera module name | Name input | Camera module name |
| MIPI port | Value input | LinkUsed |
| LaneUsed | [x1], [x2], [x3], [x4], [x8] | LaneUsed |
| PortSpeed | [0], [1], [2], [3], [4], [5], [6] | PortSpeed: [0]: Sensor default [1]: <416Mbps [2]: <1.5Gbps [3]: <2Gbps [4]: <2.5Gbps [5]: <4Gbps [6]: >4Gbps |
| MCLK | Value input | MCLK |
| EEPROM | [ROM_OPT], [ROM_EEPROM_16K_64], [ROM_EEPROM_16K_16], [ROM_OTP_ACPI_ACPI], [ROM_ACPI], [ROM_EEPROM_BRCA016GWZ], [ROM_EEPROM_24AA32], [ROM_EEPROM_M24C64], [ROM_EEPROM_DW9806B], [ROM_EEPROM_CAT24C16], [ROM_EEPROM_CAT24C64], [ROM_EEPROM_24AA16], [ROM_NONE], [ROM_EEPROM_CAT24C08] | EEPROM Type 0x00: ROM_NONE 0x01: ROM_OTP 0x02: ROM_EEPROM_16K_64 0x03: ROM_EEPROM_16K_16 0x04: ROM_OTP_ACPI_ACPI 0x05: ROM_ACPI 0x06: ROM_EEPROM_BRCA016GWZ 0x07: ROM_EEPROM_24AA32 0x08: ROM_EEPROM_CAT24C08 0x09: ROM_M24C64 0x0A: ROM_DW9806B 0x10: ROM_EEPROM_CAT24C16 0x11: ROM_EEPROM_CAT24C64 0x12: ROM_EEPROM_24AA16 |
| VCM Type | [VCM_NONE], [VCM_AD5823], [VCM_AD5816], | VCM Type 0x00: VCM_NONE 0x01: VCM_AD5823 |

| Feature | Option | Description |
|--------------------------|--|--|
| | [VCM_DW9719], [VCM_DW9718], [VCM_DW9806B], [VCM_WV517S], [VCM_LC898122XA], [VCM_LC898212AXB], [VCM_RESERVED1], [VCM_RESERVED2], [VCM_BU64297GWZ], [VCM_DW9714], [VCM_AK7371] | 0x02: VCM_DW9714 0x03: VCM_AD5816 0x04: VCM_DW9719 0x05: VCM_DW9718 0x06: VCM_DW9806B 0x07: VCM_WV517S 0x08: VCM_LC898122XA 0x09: VCM_LC898212AXB 0x0F: VCM_AK7371 0x10: VCM_BU64297GWZ |
| Number of I2C Components | Value input | Number of I2C Components |
| I2C Channel | [I2C0], [I2C1], [I2C2], [I2C4], [I2C3], [I2C5], [I2C6], [I2C7] | I2C Channel |
| I2C Address | Value input | I2C Address |
| Device Type | [Sensor], [VCM], [EEPROM], [EEPROM_EXT1], [EEPROM_EXT2], [EEPROM_EXT3], [EEPROM_EXT4], [EEPROM_EXT5], [EEPROM_EXT6], [EEPROM_EXT7], [IO Expander], [Flash] | Device Type |
| Flash Driver Selection | [Disabled], [External], [Internal PMIC] | Select the Flash Driver as External or Internal PMIC |
| Flash Driver Selection | [Flash1], [Flash2], [Flash3], [Flash4], [Flash5], [Flash6] | Select the Flash Driver as External or Internal PMIC |

Figure 157: BIOS Chipset Setup Menu – System Agent (SA) Configuration – MIPI Camera Configuration – Flash options

| Aptio Setup – AMI | | |
|--------------------|---------------------|---------------------|
| Chipset | | |
| Flash1/2 | | |
| Flash Model | [External – LM3643] | |
| Flash Mode | [Xeon Led] | → ←: Select Screen |
| Camera module name | YHRN | ↑ ↓: Select Item |
| I2C Channel | [I2C1] | Enter: Select |
| I2C Address | 63 | +/-: Change Opt. |
| Flash Trigger Gpio | | F1: General Help |
| Group Pad Number | 18 | F2: Previous Values |

| Aptio Setup – AMI | | |
|--|-----|------------------------|
| Chipset | | |
| Group Number | [B] | F3: Optimized Defaults |
| Active Value | 1 | F4: Save & Exit |
| Initial Value | 0 | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|--------------------|---|---|
| Flash Model | [External – LM3643], [PMIC - WRC] | Flash Model |
| Flash Mode | [Disabled], [White Led], [Warm Led], [IR Led], [Xeon Led] | Select Flash Mode: White LED / Warm LED / IR LED / Xeon LED |
| Camera module name | Name input | Camera module name |
| I2C Channel | [I2C0], [I2C1], [I2C2], [I2C3], [I2C4], [I2C5], [I2C6], [I2C7] | I2C Channel |
| I2C Address | Value input | I2C Address |
| Group Pad Number | Value input | Group Pad Number |
| Group Number | [A], [C], [E], [F], [H], [R], [S], [T], [U], [B], [D] | Group Number |
| Active Value | Value input | Active Value |
| Initial Value | Value input | Initial Value |

Figure 158: BIOS Chipset Setup Menu – PCH-IO Configuration

| Aptio Setup – AMI | |
|--|--|
| Chipset | |
| PCH-IO Configuration | |
| > PCI Express Configuration ⁽¹⁾ | |
| > SATA Configuration | |
| > USB Configuration | |
| > Security Configuration | |
| > HD Audio Configuration | |
| > THC Configuration | |
| > Seriallo Configuration | |
| > SCS Configuration | |
| > ISH Configuration | |

| Aptio Setup – AMI | |
|--|---|
| Chipset | |
| > Pch Thermal Throttling Control | |
| Skip VCCIN_AUX Configuration | [Disabled] |
| > FIVR Configuration | |
| > PMC Configuration | |
| > TSN GBE Configuration | |
| PCH LAN Controller | No GbE Region |
| Foxville I225 LAN Controller | [Disabled] |
| Foxville I225 Wake on LAN Support ⁽²⁾ | [Disabled] |
| Sensor Hub Type | [I2C Sensor Hub] |
| DeepSX Power Policies | [Disabled] |
| Wale on WLAN and BT Enable | [Disabled] |
| DeepSx Wake on WLAN and BT Enable ⁽³⁾ | [Disabled] |
| Disable DSX ACPRESENT PullDown | [Disabled] |
| Port 80h Redirection | [LPC Bus] |
| Enhance Port 80h LPC Decoding ⁽⁴⁾ | [Enabled] |
| Espi CS1 GIR Address | 0 |
| Espi CS1 GMR Address | 0 |
| Compatible Revision ID | [Disabled] |
| Legacy IO Low Latency | [Enabled] |
| PCH Cross Throttling | [Enabled] |
| PCH Energy Reporting | [Enabled] |
| LPM S0i2.0 | [Disabled] |
| LPM S0i3.0 | [Disabled] |
| C10 Dynamic Threshold adjustment | [Disabled] |
| IEH Mode | [Bypass Mode] |
| Enable TCO Timer | [Disabled] |
| Enable Timed GPIO0 | [Disabled] |
| Enable Timed GPIO1 | [Disabled] |
| Pcie Ref Pll SSC | [Auto] |
| IOAPIC 24-119 Entries | [Enabled] |
| Enable 8254 Clock Gate | [Enabled] |
| Lock PCH Sideband Access | [Enabled] |
| Flash Protection Range Registers (FPRR) | [Disabled] |
| SPD Write Disable | [TRUE] |
| LGMR | [Disabled] |
| HOST_C10 reporting to Target | [Disabled] |
| OS IDLE Mode | [Enabled] |
| S0ix Auto Demotion | [Disabled] |
| | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. |

| Aptio Setup – AMI | | |
|--|------------|------------------------|
| Chipset | | |
| Latch Events C10 Exit | [Disabled] | F1: General Help |
| Hybrid Storage Detection and Configuration Mode | [Disabled] | F2: Previous Values |
| Cpu Root port used for hybrid storage ⁽⁵⁾ | 255 | F3: Optimized Defaults |
| Extended BIOS Range Decode | [Disabled] | F4: Save & Exit |
| ACPI L6D PME Handling | [Disabled] | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

⁽¹⁾ The sub-menu is redirected to CPU – Power Management Control (see Figure 54) when pressing these items.

⁽²⁾ This item appears only when enabling Foxville I225 LAN Controller.

⁽³⁾ This item appears only when enabling Wake on WLAN and BT Enable.

⁽⁴⁾ This item activates only when selecting LPC Bus for Port 80h Redirection.

⁽⁵⁾ This item appears only when selecting Dynamic Configuration for Hybrid Storage Enable for Hybrid Storage Detection and Configuration Mode.

| Feature | Option | Description |
|-----------------------------------|---|--|
| Skip VCCIN_AUX Configuration | [Disabled], [Enabled] | Skips VCCIN_AUX Configuration if enabled |
| Foxville I225 LAN Controller | [Enabled], [Disabled] | Enable / Disable Foxville I225 LAN Controller. |
| Foxville I225 Wake on LAN Support | [Enabled], [Disabled] | Enable / Disable Foxville I225 Wake on LAN Support. |
| Sensor Hub Type | [None], [I2C Sensor Hub], [USB Sensor Hub] | Choose the Sensor Hub Type. 'None' will suppress 'I2C Sensor Hub' setup option. 'I2C' will suppress 'ALS' setup option. 'USB' will suppress both I2C and ALS. |
| DeepSx Power Policies | [Disabled], [Enabled in S4-S5-Battery], [Enabled in S5-Battery], [Enabled in S4-S5], [Enabled in S5] | Configure the DeepSx Mode configuration. |
| Wake on WLAN and BT Enable | [Enabled], [Disabled] | Enable / Disable PCI Express Wireless LAN and Bluetooth to wake the system. |
| DeepSx Wake on WLAN and BT Enable | [Enabled], [Disabled] | Enable / Disable PCI Express Wireless LAN and Bluetooth to wake the system from DeepSx. |
| Disable DSX ACPRESENT PullDown | [Enabled], [Disabled] | Disable PCH internal ACPRESENT PullDown when DeepSx or G3 exit. |
| Port 80h Redirection | [LPC Bus], [PCIe Bus] | Control where the Port 80h cycles are sent. |
| Enhance Port 80h LPC Decoding | [Disabled], [Enabled] | Support the word / dword decoding of port 80h behind LPC |
| Espi CS1 GIR Address | Value input | This is to set 16Bit CS1 GIR Address. |
| Espi CS1 GMR Address | Value input | This is to set 32Bit CS1 GMR Address. |

| Feature | Option | Description |
|---|--|---|
| Compatible Revision ID | [Disabled] | Read only item |
| Legacy IO Low Latency | [Disabled], [Enabled] | Set to enable low latency of legacy IO. Some systems require low IO latency irrespective of power. This is a tradeoff between power and IO latency. |
| PCH Cross Throttling | [Disabled], [Enabled] | Enable / Disable the PCH Cross Throttling feature. Only ULT support this feature. |
| PCH Energy Reporting | [Disabled], [Enabled] | Enable Energy Report. MUST set it as ENABLED. This is only for test purpose. |
| LPM S0i2.0/3.0 | [Disabled], [Enabled] | Enable / Disable S0ix sub-state. This setting is for test purpose. S0ix sub-states should be enabled for production. |
| C10 Dynamic threshold adjustment | [Disabled], [Enabled] | Enable / Disable C10 dynamic threshold adjustment |
| IEH Mode | [Bypass Mode], [Enabled] | Enable / Bypass IEH Mode |
| Enable TCO Timer | [Disabled], [Enabled] | Enable / Disable TCO timer. When disabled, it disables PCH ACPI timer, stops TCO timer, and ACPI WDAT table will not be published. |
| Enable Timed GPIO0/1 | [Disabled], [Enabled] | Enable / Disable Timed GPIO0/1. When disabled, it disables cross time stamp time-synchronization as extension of Hammock Harbor time synchronization. |
| Pcie Ref Pll SSC | [Auto], [0.0%], [0.1%], [0.2%], [0.3%], [0.4%], [0.5%], [Disabled] | Pcie Ref Pll SSC Percentage. [Auto]: Keep hw default, no BIOS override. Range is 0.0% ~ 0.5%. |
| IOAPIC 24-119 Entries | [Disabled], [Enabled] | Enables / Disables IOAPIC 24-119 Entries. IRQ24-119 may be used by PCH devices. Disabling those interrupts may cause certain devices failure. |
| Enable 8254 Clock Gate | [Disabled], [Enabled], [Enabled In Runtime and S3 Resume] | Enables / Disables 8254 clock gate in early phase. Set 8254CGE is necessary for SLP_S0 support. Platform is able disable this policy and set 8254CGE in late phase. |
| Lock PCH Sideband Access | [Disabled], [Enabled] | Lock PCH Sideband access, include SideBand interface lock and SideBand PortID mask for certain end point (e.g. PSFx). The option is invalid if POSTBOOT SAI is set. |
| Flash Protection Range Registers (FPRR) | [Disabled], [Enabled] | Enable Flash Protection Range Registers |
| SPD Write Disable | [TRUE], [FALSE] | Enable / Disable setting SPD Write Disable. For security recommendations, SPD write disable bit must be set. |
| LGMR | [Enabled], [Disabled] | 64KB memory block for LGMR (LPC Memory Range Decode) |
| HOST_C10 reporting to Target | [Disabled], [Enabled] | This option enables HOST_C10 reporting to Target via eSPI Virtual Wire. |

| Feature | Option | Description |
|---|---|--|
| OS IDLE Mode | [Disabled], [Enabled] | Enable / Disable OS Idle Mode Feature |
| S0ix Auto Demotion | [Enabled], [Disabled] | Enable / Disable Host Low Power Mode S0ix Auto-Demotion |
| Latch Events C10 Exit | [Enabled], [Disabled] | Enable / Disable Latch Events on C10 Exit |
| Hybrid Storage Detection and Configuration Mode | [Dynamic Configuration for Hybrid Storage Enable], [Disabled] | Select Hybrid Storage Detection and Configuration Mode |
| Cpu Root port used for hybrid storage | Value input | Select cpu root port used for hybrid storage value between 0 to 2 |
| Extended BIOS Range Decode | [Disabled], [Enabled] | Enabling this will make memory cycles falling in a specific area to be redirected to SPI flash controller |
| ACPI L6D PME Handling | [Enabled], [Disabled] | BIOS through ACPI code can associate specific method to a particular GPE. In this case _L6D for Level-triggered Event, BIOS-ACPI can verify PMEENABLE and PMESTATUS of each device that requires GPE related wake. |

Figure 159: BIOS Chipset Setup Menu – PCH-IO Configuration – PCI Express Configuration

| Aptio Setup – AMI | |
|----------------------------|---|
| Chipset | |
| PCI Express Configuration | |
| DMI Link ASPM Control | [Auto] |
| Port8xh Decode | [Disabled] |
| Port8xh Decode Port#* | 0 |
| PCIe function swap | [Enabled] |
| PCH PCIE Clock Gating | [Disabled] |
| PCH PCIE Power Gating | [Disabled] |
| > PCIe EQ settings | |
| PCI Express Root Port 1 | Lane configured as USB / SATA / UFS |
| PCI Express Root Port 2 | Lane configured as USB / SATA / UFS |
| > PCI Express Root Port 3 | |
| > PCI Express Root Port 4 | |
| PCI Express Root Port 5 | Not present in this SKU |
| PCI Express Root Port 6 | Not present in this SKU |
| > PCI Express Root Port 7 | |
| PCI Express Root Port 8 | Not present in this SKU |
| > PCI Express Root Port 9 | |
| > PCI Express Root Port 10 | |
| | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help |

| Aptio Setup – AMI | | |
|--|-------------------------------------|------------------------------|
| Chipset | | |
| PCI Express Root Port 11 | Lane configured as USB / SATA / UFS | F2: Previous Values |
| PCI Express Root Port 12 | Lane configured as USB / SATA / UFS | F3: Optimized Defaults |
| > PCIE clocks | | F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* This item appears only when enabling Port8xh Decode.

| Feature | Option | Description |
|-----------------------|--|--|
| DMI Link ASPM Control | [Disabled], [L0s], [L1], [L0sL1], [Auto] | The control of Active State Power Management of the DMI Link. |
| Port8xh Decode | [Disabled], [Enabled] | PCI Express Port8xh Decode Enable / Disable. |
| Port8xh Decode Port# | Value input | Select PCI Express Port8xh Decode Root Port. User to ensure port availability |
| PCIe function swap | [Disabled], [Enabled] | When Disabled, prevents PCIe rootport function swap. If any function other than 0 th is enabled, 0 th will become visible. |
| PCH PCIe Clock Gating | [Disabled], [Enabled] | PCH PCI Express Clock Gating Enable / Disable for all port |
| PCH PCIe Power Gating | [Disabled], [Enabled] | PCH PCI Express Power Gating Enable / Disable for all port |

Figure 160: BIOS Chipset Setup Menu – PCH-IO Configuration – PCI Express Configuration – PCIe EQ settings

| Aptio Setup – AMI | | |
|---|-------------------------|--|
| Chipset | | |
| PCIe EQ override | [Disabled] | |
| PCIe EQ method* | [PCIe hardware EQ] | |
| PCIe EQ mode* | [Use presets during EQ] | |
| EQ PH1 downstream port transmitter present* | 0 | |
| EQ PH1 upstream port transmitter present* | 0 | |
| Enable EQ phase 2 local transmitter override* | [Disabled] | |
| Number of presents or coefficients used during phase 3* | 0 | |
| Preset 0 ^{*(1)} | 0 | |
| Preset 1 ^{*(1)} | 0 | |
| Preset 2 ^{*(1)} | 0 | |
| Preset 3 ^{*(1)} | 0 | |
| Preset 4 ^{*(1)} | 0 | |
| Preset 5 ^{*(1)} | 0 | |

| Aptio Setup – AMI | | |
|---|---|------------------------|
| Chipset | | |
| Preset 6 ^{*(1)} | 0 | |
| Preset 7 ^{*(1)} | 0 | |
| Preset 8 ^{*(1)} | 0 | |
| Preset 9 ^{*(1)} | 0 | |
| Preset 10 ^{*(1)} | 0 | |
| Pre-cursor coefficient 0 ^{*(2)} | 0 | |
| Post-cursor coefficient 0 ^{*(2)} | 0 | |
| Pre-cursor coefficient 1 ^{*(2)} | 0 | |
| Post-cursor coefficient 1 ^{*(2)} | 0 | |
| Pre-cursor coefficient 2 ^{*(2)} | 0 | |
| Post-cursor coefficient 2 ^{*(2)} | 0 | |
| Pre-cursor coefficient 3 ^{*(2)} | 0 | |
| Post-cursor coefficient 3 ^{*(2)} | 0 | |
| Pre-cursor coefficient 4 ^{*(2)} | 0 | |
| Post-cursor coefficient 4 ^{*(2)} | 0 | |
| Pre-cursor coefficient 5 ^{*(2)} | 0 | |
| Post-cursor coefficient 5 ^{*(2)} | 0 | → ←: Select Screen |
| Pre-cursor coefficient 6 ^{*(2)} | 0 | ↑ ↓: Select Item |
| Post-cursor coefficient 6 ^{*(2)} | 0 | Enter: Select |
| Pre-cursor coefficient 7 ^{*(2)} | 0 | +/-: Change Opt. |
| Post-cursor coefficient 7 ^{*(2)} | 0 | F1: General Help |
| Pre-cursor coefficient 8 ^{*(2)} | 0 | F2: Previous Values |
| Post-cursor coefficient 8 ^{*(2)} | 0 | F3: Optimized Defaults |
| Pre-cursor coefficient 9 ^{*(2)} | 0 | F4: Save & Exit |
| Post-cursor coefficient 9 ^{*(2)} | 0 | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when enabling PCIe EQ override.

⁽¹⁾ These items appear only when selecting Use presets during EQ for PCIe EQ mode.

⁽²⁾ These items appear only when selecting Use coefficients during EQ for PCIe EQ mode.

| Feature | Option | Description |
|---|---|--|
| PCIe EQ override | [Disabled], [Enabled] | Choose your own PCIe EQ settings, only for users who have a thorough understanding of equalization process |
| PCIe EQ method | [PCIe hardware EQ], [PCIe fixed EQ] | Choose PCIe EQ method |
| PCIe EQ mode | [Use presets during EQ], [Use coefficients during EQ] | Choose EQ mode. Preset mode – root port will use presets during EQ process, Coefficient mode – root port will use coefficients during EQ process |
| EQ PH1 downstream port transmitter preset | Value input | Choose the value of the preset that will be used during phase 1 of the equalization |

| Feature | Option | Description |
|---|--------------------------|--|
| EQ PH1 upstream port transmitter preset | Value input | Choose the value of the preset that will be used during phase 1 of the equalization |
| Enable EQ phase 2 local transmitter override | [Disabled], [Enabled] | EQ Phase 2 local transmitter override can be used to debug issues with PCI devices equalization. |
| Number of presets or coefficients used during phase 3 | Value input | Select how many presets or coefficients will be used during phase 3 of EQ. Please not that you have to set all of the list entries to valid values. The interpretation of this field depends on PCIe EQ mode |
| Preset 0..10 | Value input | Choose the target preset value |
| Pre-cursor coefficient 0..9 | Value input | Choose the target pre-cursor coefficient value |
| Post-cursor coefficient 0..9 | Value input | Choose the target post-cursor coefficient value |

Figure 161: BIOS Chipset Setup Menu – PCH-IO Configuration – PCI Express Configuration – PCI Express Root Port 3 / 4 / 7 / 9 / 10

| Aptio Setup – AMI | |
|--|---------------|
| Chipset | |
| PCI Express Root Port 3 / 4 / 7 / 9 / 10 | [Enabled] |
| Connection Type* | [Slot] |
| ASPM* | [Auto] |
| L1 Substates* | [L1.1 & L1.2] |
| L1 Low* | [Enabled] |
| ACS* | [Enabled] |
| PTM* | [Enabled] |
| DPC* | [Disabled] |
| EDPC* | [Enabled] |
| URR* | [Disabled] |
| FER* | [Disabled] |
| NFER* | [Disabled] |
| CER* | [Disabled] |
| SEFE* | [Disabled] |
| SENF* | [Disabled] |
| SECE* | [Disabled] |
| PME SCI* | [Enabled] |
| Hot Plug* | [Disabled] |
| Advanced Error Reporting* | [Enabled] |
| PCIe Speed* | [Auto] |
| Transmitter Half Swing* | [Disabled] |
| Detect Timeout* | 0 |

| Aptio Setup – AMI | | |
|--|------------|---|
| Chipset | | |
| Extra Bus Reserved* | 0 | → ←: Select Screen ↑ ↓ : Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Reserved Memory* | 10 | |
| Reserved I/O* | 4 | |
| PCH PCIe LTR Configuration* | | |
| LTR* | [Enabled] | |
| Snoop Latency Override*# | [Auto] | |
| Snoop Latency Value*#(1) | 60 | |
| Snoop Latency Multiplier*#(1) | [1024 ns] | |
| Non Snoop Latency Override*# | [Auto] | |
| Non Snoop Latency Value*#(2) | 60 | |
| Non Snoop Latency Multiplier*#(2) | [1024 ns] | |
| LTR Lock* | [Disabled] | |
| Peer Memory Write Enable* | [Disabled] | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when enabling PCI Express Root Port 3 / 4 / 7 / 9 / 10.

These items appear only when enabling LTR.

(1) These items appear only when selecting Manual for Snoop Latency Override.

(2) These items appear only when selecting Manual for Mon Snoop Latency Override.

| Feature | Option | Description |
|--|---|---|
| PCI Express Root Port 3 / 4 / 7 / 9 / 10 | [Disabled], [Enabled] | Control the PCI Express Root Port. |
| Connection Type | [Bulit-in], [Slot] | [Built-in]: a built-in device is connected to this rootport. SlotImplemented bit will be clear. [Slot]: this rootport connects to user-accessible slot. SlotImplemented bit will be set. |
| ASPM | [Disabled], [L1], [Auto] | Set the ASPM Level: Force L0s – Force all links to L0s State AUTO – BIOS auto configure DISABLE – Disables ASPM |
| L1 Substates | [Disabled], [L1.1], [L1.1 & L1.2] | PCI Express L1 Substates settings. |
| L1 Low | [Disabled], [Enabled] | PCI Express L1 Low Substate Enable / Disable. |
| ACS | [Disabled], [Enabled] | Enable / Disable Access Control Services Extended Capability |
| PTM | [Disabled], [Enabled] | Enable / Disable Precision Time Measurement |

| Feature | Option | Description |
|--------------------------|---|--|
| DPC | [Disabled], [Enabled] | Enable / Disable Downstream Port Containment |
| EDPC | [Disabled], [Enabled] | Enable / Disable Rootport extensions for Downstream Port Containment |
| URR | [Disabled], [Enabled] | PCI Express Unsupported Request Reporting Enable / Disable. |
| FER | [Disabled], [Enabled] | PCI Express Device Fatal Error Reporting Enable / Disable. |
| NFER | [Disabled], [Enabled] | PCI Express Device Non-Fatal Error Reporting Enable / Disable. |
| CER | [Disabled], [Enabled] | PCI Express Device Correctable Error Reporting Enable / Disable. |
| SEFE | [Disabled], [Enabled] | Root PCI Express System Error on Fatal Error Enable / Disable. |
| SENF | [Disabled], [Enabled] | Root PCI Express System Error on Non-Fatal Error Enable / Disable. |
| SECE | [Disabled], [Enabled] | Root PCI Express System Error on Correctable Error Enable / Disable. |
| PME SCI | [Disabled], [Enabled] | PCI Express PME SCI Enable / Disable. |
| Hot Plug | [Disabled], [Enabled] | PCI Express Hot Plug Enable / Disable. |
| Advanced Error Reporting | [Disabled], [Enabled] | Advanced Error Reporting Enable / Disable. |
| PCIe Speed | [Auto], [Gen1], [Gen2], [Gen3] | Configure PCIe Speed |
| Transmitter Half Swing | [Disabled], [Enabled] | Transmitter Half Swing Enable / Disable. |
| Detect Timeout | Value input | The number of milliseconds reference code will wait for link to exit Detect state for enabled ports before assuming there is no device and potentially disabling the port. |
| Extra Bus Reserved | Value input | Extra Bus Reserved (0-7) for bridges behind this Root Bridge. |
| Reserved Memory | Value input | Reserved Memory for this Root Bridge (1-20) MB |
| Reserved I/O | Value input | Reserved I/O (4K/8K/12K/16K/20K) Range for this Root Bridge. |
| LTR | [Disabled], [Enabled] | PCH PCIE Latency Reporting Enable / Disable |
| Snoop Latency Override | [Disabled], [Manual], [Auto] | Snoop Latency Override for PCH PCIE. [Disabled]: Disable override. [Manual]: Manually enter override values. [Auto] (default): Maintain default BIOS flow. |
| Snoop Latency Value | Value input | LTR Snoop Latency value of PCH PCIE |

| Feature | Option | Description |
|------------------------------|--|---|
| Snoop Latency Multiplier | [1 ns], [32 ns], [1024 ns], [32768 ns], [1048576 ns], [33554432 ns] | LTR Snoop Latency Multiplier of PCH PCIE |
| Non Snoop Latency Override | [Disabled], [Manual], [Auto] | Non Snoop Latency Override for PCH PCIE. [Disabled]: Disable override. [Manual]: Manually enter override values. [Auto] (default): Maintain default BIOS flow. |
| Non Snoop Latency Value | Value input | LTR Non Snoop Latency value of PCH PCIE |
| Non Snoop Latency Multiplier | [1 ns], [32 ns], [1024 ns], [32768 ns], [1048576 ns], [33554432 ns] | LTR Non Snoop Latency Multiplier of PCH PCIE |
| LTR Lock | [Disabled], [Enabled] | PCIE LTR Configuration Lock |
| Peer Memory Write Enable | [Disabled], [Enabled] | Peer Memory Write Enable / Disable |

Figure 162: BIOS Chipset Setup Menu – PCH-IO Configuration – PCI Express Configuration – PCIE clocks

| Aptio Setup – AMI | | |
|-------------------|----------------|---|
| Chipset | | |
| Clock0 assignment | [Platform-POR] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help |
| ClkReq for Clock0 | [Platform-POR] | |
| Clock1 assignment | [Platform-POR] | |
| ClkReq for Clock1 | [Platform-POR] | |
| Clock2 assignment | [Platform-POR] | |
| ClkReq for Clock2 | [Platform-POR] | |
| Clock3 assignment | [Platform-POR] | |
| ClkReq for Clock3 | [Platform-POR] | |
| Clock4 assignment | [Platform-POR] | |
| ClkReq for Clock4 | [Platform-POR] | |
| Clock5 assignment | [Platform-POR] | |
| ClkReq for Clock5 | [Platform-POR] | |
| Clock6 assignment | [Platform-POR] | |
| ClkReq for Clock6 | [Platform-POR] | |
| Clock7 assignment | [Platform-POR] | |
| ClkReq for Clock7 | [Platform-POR] | |

| Aptio Setup – AMI | | |
|--|----------------|------------------------|
| Chipset | | |
| Clock8 assignment | [Platform-POR] | F2: Previous Values |
| ClkReq for Clock8 | [Platform-POR] | F3: Optimized Defaults |
| Clock9 assignment | [Platform-POR] | F4: Save & Exit |
| ClkReq for Clock9 | [Platform-POR] | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|----------------------|---|---|
| Clock0..9 assignment | [Platform-POR], [Enabled], [Disabled] | [Platform-POR]: clock is assigned to PCIe port or LAN according to board layout. [Enabled]: keep clock enabled even if unused. [Disabled]: Disable clock. |
| ClkReq for Clock0..9 | [Platform-POR], [Disabled] | [Platform-POR]: CLKREQ signal is assigned to CLKSRC according to board layout. [Disabled]: CLKREQ will not be used. |

Figure 163: BIOS Chipset Setup Menu – PCH-IO Configuration – SATA Configuration

| Aptio Setup – AMI | |
|--------------------------------|--------------------|
| Chipset | |
| SATA Configuration | |
| SATA Controller(s) | [Enabled] |
| SATA Mode Selection* | [AHCI] |
| SATA Test Mode* | [Disabled] |
| Aggressive LPM Support*(1) | [Enabled] |
| Serial ATA Port 0* | Empty |
| Software Preserve* | Unknown |
| Port 0* | [Enabled] |
| Hot Plug* | [Disabled] |
| Configured as eSATA*(3) | Hot Plug supported |
| External* | [Disabled] |
| Mechanical Presence Switch*(2) | [Disabled] |
| Spin Up Device* | [Disabled] |
| SATA Device Type* | [Hard Disk Drive] |
| Topology* | [Unknown] |
| SATA Port 0 DevSlp* | [Disabled] |
| DITO Configuration* | [Disabled] |
| DITO Value*(4) | 625 |
| DM Value*(4) | 15 |
| Serial ATA Port 1* | Empty |

| Aptio Setup – AMI | | |
|--|--------------------|--|
| Chipset | | |
| Software Preserve* | Unknown | |
| Port 1* | [Enabled] | |
| Hot Plug* | [Disabled] | |
| Configured as eSATA ^{*(3)} | Hot Plug supported | |
| External* | [Disabled] | |
| Mechanical Presence Switch ^{*(2)} | [Disabled] | |
| Spin Up Device* | [Disabled] | |
| SATA Device Type* | [Hard Disk Drive] | |
| Topology* | [Unknown] | |
| SATA Port 1 DevSlp* | [Disabled] | |
| DITO Configuration* | [Disabled] | |
| DITO Value ^{*(4)} | 625 | |
| DM Value ^{*(4)} | 15 | |
| Serial ATA Port 2* | Empty | |
| Software Preserve* | Unknown | |
| Port 2* | [Enabled] | |
| Hot Plug* | [Disabled] | |
| Configured as eSATA ^{*(3)} | Hot Plug supported | |
| External* | [Disabled] | |
| Mechanical Presence Switch ^{*(2)} | [Disabled] | |
| Spin Up Device* | [Disabled] | |
| SATA Device Type* | [Hard Disk Drive] | |
| Topology* | [Unknown] | |
| SATA Port 2 DevSlp* | [Disabled] | |
| DITO Configuration* | [Disabled] | |
| DITO Value ^{*(4)} | 625 | |
| DM Value ^{*(4)} | 15 | |
| | | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when enabling SATA Controller(s).

(1) This item appears only when disabling SATA Test Mode.

(2) This item appears only when enabling Hot Plug.

(3) This item appears only when disabling External.

(4) These items appear only when enabling DITO Configuration.

| Feature | Option | Description |
|------------------------|--------------------------|--|
| SATA Controller(s) | [Enabled], [Disabled] | Enable / Disable SATA Device. |
| SATA Mode Selection | [AHCI] | Read only item |
| SATA Test Mode | [Enabled], [Disabled] | Test Mode Enable / Disable (Loop Back). |
| Aggressive LPM Support | [Disabled], [Enabled] | Enable PCH to aggressively enter link power state. |

| Feature | Option | Description |
|----------------------------|--|---|
| Port 0..2 | [Disabled], [Enabled] | Enable or Disable SATA Port |
| Hot Plug | [Disabled], [Enabled] | Designates this port as Hot Pluggable. |
| External | [Disabled], [Enabled] | Marks this port as external. |
| Mechanical Presence Switch | [Disabled], [Enabled] | Controls reporting if this port has an Mechanical Presence Switch. Note: Requires hardware support. |
| Spin Up Device | [Disabled], [Enabled] | If enabled for any of ports Staggerred Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot. |
| SATA Device Type | [Hard Disk Drive], [Solid State Drive] | Identify the SATA port is connected to Solid State Drive or Hard Disk Drive |
| Topology | [Unknown], [ISATA], [Direct Connect], [Flex], [M2] | Identify the SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2 |
| SATA Port 0..2 DevSlp | [Disabled], [Enabled] | Enable / Disable SATA Port 0..2 DevSlp. For DevSlp to work, both hard drive and SATA port need to support DevSlp function, otherwise an unexpected behavior might happen. Please check board design before enabling it. |
| DITO Configuration | [Disabled], [Enabled] | Enable / Disable DITO Configuration |
| DITO Value | Value input | DITO Value |
| DM Value | Value input | DM Value |

Figure 164: BIOS Chipset Setup Menu – PCH-IO Configuration – USB Configuration

| Aptio Setup – AMI | |
|--------------------------------|------------|
| Chipset | |
| USB Configuration | |
| xDCI Support | [Disabled] |
| USB2 PHY Sus Well Power Gating | [Enabled] |
| USB PDO Programming | [Enabled] |
| USB Overcurrent | [Enabled] |
| USB Overcurrent Lock | [Enabled] |
| USB Audio Offload | [Enabled] |
| Enable HSII on xHCI | [Enabled] |

| Aptio Setup – AMI | | |
|--|------------|------------------------|
| Chipset | | |
| USB3.1 Portx Speed Selection | 0 | |
| USB Port Disable Override | [Disabled] | |
| USB SW Device Mode Port #0* | [Disabled] | |
| USB SW Device Mode Port #1* | [Disabled] | |
| USB SW Device Mode Port #2* | [Disabled] | |
| USB SW Device Mode Port #3* | [Disabled] | |
| USB SW Device Mode Port #4* | [Disabled] | |
| USB SW Device Mode Port #5* | [Disabled] | |
| USB SW Device Mode Port #6* | [Disabled] | |
| USB SW Device Mode Port #7* | [Disabled] | |
| USB SW Device Mode Port #8* | [Disabled] | |
| USB SW Device Mode Port #9* | [Disabled] | |
| USB SS Physical Connector #0* | [Enabled] | |
| USB SS Physical Connector #1* | [Enabled] | |
| USB SS Physical Connector #2* | [Enabled] | |
| USB SS Physical Connector #3* | [Enabled] | |
| USB HS Physical Connector #0* | [Enabled] | |
| USB HS Physical Connector #1* | [Enabled] | → ←: Select Screen |
| USB HS Physical Connector #2* | [Enabled] | ↑ ↓: Select Item |
| USB HS Physical Connector #3* | [Enabled] | Enter: Select |
| USB HS Physical Connector #4* | [Enabled] | +/-: Change Opt. |
| USB HS Physical Connector #5* | [Enabled] | F1: General Help |
| USB HS Physical Connector #6* | [Enabled] | F2: Previous Values |
| USB HS Physical Connector #7* | [Enabled] | F3: Optimized Defaults |
| USB HS Physical Connector #8* | [Disabled] | F4: Save & Exit |
| USB HS Physical Connector #9* | [Enabled] | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when selecting Select Per-Pin for USB Port Disable Override.

| Feature | Option | Description |
|--------------------------------|--------------------------|--|
| xDCI | [Disabled], [Enabled] | Enable / Disable xDCI (USB OTG Device). |
| USB2 PHY Sus Well Power Gating | [Disabled], [Enabled] | Select 'Enabled' to enable SUS Well PG for USB2 PHY. This option has no effect on PCH-H. |
| USB PDO Programming | [Disabled], [Enabled] | Select 'Enabled' if Port Disable Override functionality is used. |
| USB Overcurrent | [Disabled], [Enabled] | Select 'Disabled' for pin-based debug. If pin-based debug is enabled but USB overcurrent is not disabled, USB DbC does not work. |

| Feature | Option | Description |
|---------------------------------|---------------------------------|---|
| USB Overcurrent Lock | [Disabled], [Enabled] | Select 'Disabled' if Overcurrent functionality is used. Enabling this will make xHCI controller consume the Overcurrent mapping data |
| USB Audio Offload | [Disabled], [Enabled] | Enable / Disable USB Audio Offload functionality |
| Enable HSII on xHCI | [Disabled], [Enabled] | Enable / Disable HSII feature. It may lead to increased power consumption. |
| USB3.1 Portx Speed Selection | Value input | Port Selection value in decimal for Gen1; Default – Gen2; Bit 0 corresponds to Port 0 and so on. |
| USB Port Disable Override | [Disabled], [Select Per-Pin] | Selectively Enable / Disable the corresponding USB port from reporting a Device Connection to the controller. |
| USB SW Device Mode Port #0..9 | [Disabled], [Enabled] | Enable Connector Event for device subscription. |
| USB SS Physical Connector #0..3 | [Disabled], [Enabled] | Enable / Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS. |
| USB HS Physical Connector #0..9 | [Disabled], [Enabled] | Enable / Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS. |

Figure 165: BIOS Chipset Setup Menu – PCH-IO Configuration – Security Configuration

| Aptio Setup – AMI | | |
|--|-----------|--|
| Chipset | | |
| Security Configuration | | |
| RTC Memory Lock | [Enabled] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| BIOS Lock | [Enabled] | |
| Force unlock on all GPIO pads | [Enabled] | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|-----------------|--------------------------|--|
| RTC Memory Lock | [Disabled], [Enabled] | Enable will lock bytes 38h-3Fh in the lower / upper 128-byte bank of RTC RAM |
| BIOS Lock | [Disabled], [Enabled] | Enable / Disable the PCH BIOS Lock Enable feature. Required to be enabled to ensure SMM protection of flash. |

| Feature | Option | Description |
|-------------------------------|--------------------------|--|
| Force unlock on all GPIO pads | [Disabled], [Enabled] | If Enabled BIOS will force all GPIO pads to be in unlocked state |

Figure 166: BIOS Chipset Setup Menu – PCH-IO Configuration – HD Audio Configuration

| Aptio Setup – AMI | | |
|---|----------------------|--|
| Chipset | | |
| HD Audio Subsystem Configuration Settings | | |
| Audio DSP | [Disabled] | |
| Audio DSP Compliance Mode* | [Non-UAA (IntelSST)] | |
| HDA Link | [Enabled] | |
| DMIC #0 | [Disabled] | |
| DMIC #1 | [Disabled] | |
| SSP #0 | [Disabled] | |
| SSP #1 | [Disabled] | |
| SSP #2 | [Disabled] | |
| SSP #3 | [Disabled] | |
| SSP #4 | [Disabled] | |
| SSP #5 | [Disabled] | |
| SNDW #0 | [Disabled] | |
| SNDW #1 | [Disabled] | |
| SNDW #2 | [Disabled] | |
| SNDW #3 | [Disabled] | |
| > HD Audio Advanced Configuration | | |
| > HD Audio DSP Features Configuration* | | |
| HD Audio Bus Controller Subsystem Id | [72708086] | |
| Virtual Channel Type | [VC0] | |
| HDA Codec ALC245 Configuration | [No Dmic to codec] | |
| | | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when enabling Audio DSP.

| Feature | Option | Description |
|---------------------------|---|--|
| Audio DSP | [Disabled], [Enabled] | Enable / Disable Audio DSP. |
| Audio DSP Compliance Mode | [Non-UAA (IntelSST)], [UAA (HDA Inbox/IntelSST)] | Specifies DSP enabled system compliance: 1. Non-UAA (IntelSST driver support only – CC_040100) 2. UAA (HD Audio Inbox or IntelSST driver support – CC_040380) Note: NHLT (DMIC/BT/I2S configuration) is published for non-UAA only. |

| Feature | Option | Description |
|--|---|---|
| HDA Link DMIC #0/1 SSP #0..5 SNDW #0..3 | [Disabled], [Enabled] | Muxed interfaces: 1) HDA/SSP0 2) HDA[SDI1]/SSP1 3) DMIC0/SNDW4 4) DMIC1/SNDW3 CNL only: 5) HDA/SNDW1 6) SSP1/SNDW2 |
| HD Audio Bus Controller Subsystem Id | [72708086], [300010EC], [300210EC], [300410EC], [300610EC], [300810EC], [300A10EC], [300C10EC], [300E10EC], [301010EC], [301210EC], [301610EC], [301810EC], [301A10EC], [301C10EC], [301E10EC], [302010EC], [302210EC], [302410EC], [302610EC], [302810EC], [302A10EC], [302C10EC], [302E10EC], [303010EC], [304210EC], [304A10EC], [305410EC], [305610EC], [0A321028] | Select HA Audio Bus Controller Subsystem Id |
| Virtual Channel Type | [VC0], [VC1] | Enable / Disable HD Audio to use VC0 / VC1. Default is VC0. |
| HDA Codec ALC245 Configuration | [No Dmic to codec], [4 Dmic to codec], [2 Dmic to codec] | Option for configuring DMIC connection to ALC245. |

Figure 167: BIOS Chipset Setup Menu – PCH-IO Configuration – HD Audio Configuration – HD Audio Advanced Configuration

| Aptio Setup – AMI | |
|--|--------------------|
| Chipset | |
| HD Audio Subsystem Advanced Configuration Settings | |
| iDisplay Audio Disconnect | [Disabled] |
| Codec Sx Wake Capability | [Disabled] |
| PME Enable | [Disabled] |
| Statically Switchable BCLK Clock Frequency Configuration: | |
| HD Audio Link Frequency | [24 MHz] |
| iDisplay Audio Link Frequency | [96 MHz] |
| iDisplay Audio Link T-Mode | [8T Mode] |
| Autonomous Clock Stop SNDW #0 | [Disabled] |
| Autonomous Clock Stop SNDW #1 | [Disabled] |
| Autonomous Clock Stop SNDW #2 | [Disabled] |
| Autonomous Clock Stop SNDW #3 | [Disabled] |
| Data On Active Interval Select SNDW #0 | [11 clock periods] |
| Data On Active Interval Select SNDW #1 | [11 clock periods] |
| Data On Active Interval Select SNDW #2 | [11 clock periods] |
| Data On Active Interval Select SNDW #3 | [11 clock periods] |
| Data On Delay Select SNDW #0 | [3 clock periods] |
| Data On Delay Select SNDW #1 | [3 clock periods] |
| Data On Delay Select SNDW #2 | [3 clock periods] |
| Data On Delay Select SNDW #3 | [3 clock periods] |
| → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit | |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

| Feature | Option | Description |
|-------------------------------|-----------------------------------|---|
| iDisplay Audio Disconnect | [Disabled], [Enabled] | Disconnects SDI2 signal to hide / disable iDisplay Audio Codec. |
| Codec Sx Wake Capability | [Disabled], [Enabled] | Capability to detect wake initiated by a codec in Sx (eg by modem codec) |
| PME Enable | [Disabled], [Enabled] | Enables PME wake of HD Audio controller during POST. |
| HD Audio Link Frequency | [6 MHz], [12 MHz], [24 MHz] | Selects HD Audio Link frequency. Applicable only if HDA codec supports selected frequency. |
| iDisplay Audio Link Frequency | [48 MHz], [96 MHz] | Selects iDisplay Link frequency. |

| Feature | Option | Description |
|---|--|--|
| iDisplay Audio Link T-Mode | [1T Mode], [2T Mode], [4T Mode], [8T Mode], [16T Mode] | Indicates whether SDI is operating in 1T, 2T (CNL) or 2T, 4T, 8T mode (ICL). |
| Autonomous Clock Stop SNDW #0..3 | [Disabled], [Enabled] | Enable / Disable Autonomous Clock Stop for SoundWire LINK0..3 |
| Data On Active Interval Select SNDW #0..3 | [6 clock periods], [7 clock periods], [8 clock periods], [11 clock periods] | Data On Active Interval Select: 1) 6 clock periods 2) 7 clock periods 3) 8 clock periods 4) 11 clock periods |
| Data On Delay Select SNDW #0..3 | [2 clock periods], [3 clock periods] | Data On Delay Select: 1) 2 clock periods 2) 3 clock periods |

Figure 168: BIOS Chipset Setup Menu – PCH-IO Configuration – HD Audio Configuration – HD Audio DSP Features Configuration

| Aptio Setup – AMI | |
|--|-------------------|
| Chipset | |
| HD Audio Subsystem Features Configuration (ACPI) | |
| Audio DSP NHLT Endpoints Configuration: | |
| Dmic Mono 38.4MHz | [Disabled] |
| Dmic Stereo 38.4MHz | [Disabled] |
| Dmic Quad 38.4MHz | [Disabled] |
| Dmic Mono 24MHz | [Disabled] |
| Dmic Stereo 24MHz | [Disabled] |
| Dmic Quad 24MHz | [Disabled] |
| Bluetooth 38.4MHz | [Enabled] |
| Bluetooth 24MHz | [Disabled] |
| I2S Alc274 38.4MHz | [Disabled] |
| I2S Alc274 24MHz | [Disabled] |
| LONTIUMI2S0 | [Disabled] |
| LONTIUMI2S2 | [Disabled] |
| EVEREST8316 | [Disabled] |
| I2S Codec Select | [Disabled] |
| I2S Codec Bus Number | [I2CO Controller] |
| Audio DSP Feature Support: | |
| WoV (Wake on Voice) | [Enabled] |

| Aptio Setup – AMI | |
|--|-------------------------------|
| Chipset | |
| Bluetooth Sideband | [Enabled] |
| BT Intel HFP | [Enabled] |
| BT Intel A2DP | [Enabled] |
| BT Intel Low Energy | [Disabled] |
| Codec based VAD | [Disabled] |
| DSP based Speech Pre-Processing | [Disabled] |
| Disabled | |
| Voice Activity Detection | [Windows 10 Voice Activation] |
| Audio DSP Pre/Post-Processing Module Support: | |
| Waves Post-process | [Disabled] |
| DTS | [Disabled] |
| IntelSST Speech | [Disabled] |
| Dolby | [Disabled] |
| Waves Pre-process | [Disabled] |
| Audyssey | [Disabled] |
| Maxim Smart AMP | [Disabled] |
| ForteMedia SAMSoft | [Disabled] |
| Sound Research IP | [Disabled] |
| Conexant Pre-Process | [Disabled] |
| Conexant Smart Amp | [Disabled] |
| Realtek Post-Process | [Disabled] |
| Realtek Smart Amp | [Disabled] |
| Icepower IP MFX sub module | [Disabled] |
| Icepower IP EFX sub module | [Disabled] |
| Icepower IP SFX sub module | [Disabled] |
| Voice Preprocessing | [Disabled] |
| Acoustic Context Awareness (ACA) | [Disabled] |
| Custom Module 'Alpha' | [Disabled] |
| 'Alpha' GUID: ⁽¹⁾ | |
| Custom Module 'Beta' | [Disabled] |
| 'Beta' GUID: ⁽²⁾ | |
| Custom Module 'Gamma' | [Disabled] |
| 'Gamma' GUID: ⁽³⁾ | |
| → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit | |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

⁽¹⁾ This item appears only when enabling Custom Module 'Alpha'.

⁽²⁾ This item appears only when enabling Custom Module 'Beta'.

⁽³⁾ This item appears only when enabling Custom Module 'Gamma'.

| Feature | Option | Description |
|--|---|---|
| WoV (Wake on Voice) | [Disabled], | Enables / Disables DSP Feature. |
| Bluetooth Sideband | [Enabled] | Bitmask structure: |
| BT Intel HFP | | [BIT0] – WoV |
| BT Intel A2DP | | [BIT1] – BT Sideband |
| BT Intel Low Energy | | [BIT2] – Codec based VAD |
| Codec based VAD | | [BIT5] – BT Intel HFP |
| Voice Activity Detection | [Intel Wake on Voice], [Windows 10 Voice Activation] | [BIT6] – BT Intel A2DP [BIT7] – DSP based speech pre-processing disabled (for Intel WoV mode) [BIT8] – WoV Mode: Intel WoV / Windows Voice Activation for Cortana |
| DSP based Speech Pre-Processing Disabled | [Disabled] | Read only item |
| Waves Post-process | [Disabled], | Enables / Disables 3rd Party Processing Module Support (identified by GUID). |
| DTS | [Enabled] | WoV must be enabled as a feature first to select relevant WoV IP. |
| IntelSST Speech | | |
| Dolby | | |
| Waves Pre-process | | |
| Audyssey | | |
| Maxim Smart AMP | | |
| ForteMedia SAMSoft | | |
| Sound Research IP | | |
| Conexant Pre-Process | | |
| Conexant Smart Amp | | |
| Realtek Post-Process | | |
| Realtek Smart Amp | | |
| Icepower IP MFX sub module | | |
| Icepower IP EFX sub module | | |
| Icepower IP SFX sub module | | |
| Voice Preprocessing | | |
| Acoustic Context Awareness (ACA) | | |
| Custom Module 'Alpha' | | |
| Custom Module 'Beta' | | |
| Custom Module 'Gamma' | | |
| 'Alpha' GUID | Digit character | Input hex digit character in aabbccdd-eeff-gghh-ijj- |
| 'Beta' GUID | input | kkllmmnnoopp format. |
| 'Gamma' GUID | | |

Figure 169: BIOS Chipset Setup Menu – PCH-IO Configuration – THC Configuration

| Aptio Setup – AMI | |
|--|-------------------|
| Chipset | |
| Touch Host Controller Configuration | |
| THC Port Configuration | [None] |
| Port Clock* | [Functional] |
| Active LTR* | FFFFFFFF |
| Idle LTR* | FFFFFFFF |
| HID Over SPI Limit Packet Size* | 0 |
| Hid Over Spi Performance Limitation* | 0 |
| Wake On Touch* | [Disabled] |
| THC Mode* | [HID over SPI] |
| Connection Speed* | 17000000 |
| Flags* | [Single SPI Mode] |
| Input Report Body Address* | 0 |
| Input Report Header Address* | 0 |
| Output Report Address* | 0 |
| Write Opcode* | 0 |
| Read Opcode* | 0 |
| Reset Pad Trigger* | [Low] |
| THC Port Configuration | [None] |
| Port Clock* | [Functional] |
| Active LTR* | FFFFFFFF |
| Idle LTR* | FFFFFFFF |
| HID Over SPI Limit Packet Size* | 0 |
| Hid Over Spi Performance Limitation* | 0 |
| Wake On Touch* | [Disabled] |
| THC Mode* | [HID over SPI] |
| Connection Speed* | 17000000 |
| Flags* | [Single SPI Mode] |
| Input Report Body Address* | 0 |
| Input Report Header Address* | 0 |
| Output Report Address* | 0 |
| Write Opcode* | 0 |
| Read Opcode* | 0 |
| Reset Pad Trigger* | [Low] |
| → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit | |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

* These items appear only when selecting THC0 / THC1 for THC Port Configuration.

| Feature | Option | Description |
|-------------------------------------|---|---|
| THC Port Configuration | [None], [THC0 / THC1] | Assign Port to THC |
| Port Clock | [Functional], [DFX] | SPI_DFX_CLK_EN BIT set to 0 or 1 |
| Active LTR | Value input | Expose Active LTR data through ACPI _DSM for OS driver to configure |
| Idle LTR | Value input | Expose Idle LTR data through ACPI _DSM for OS driver to configure |
| HID Over SPI Limit Packet Size | Value input | When set, limits SPI read & write packet size to 64B. Otherwise, THC uses Max Soc packet size for SPI Read and Write 0 – Max Soc Packet Size 1 – 64 Bytes |
| Hid Over Spi Performance Limitation | Value input | Minimum amount of delay the driver must wait between end of write operation and begin pf read operation. This value shall be in 10us multiples 0 – Disabled 1 – 65535 (0xFFFF) up to 655350us |
| Wake On Touch | [Disabled], [Enabled] | Based on this setting vGPIO for given THC will be in native mode, and additional _CRS foe wake will be exposed in ACPI. |
| THC Mode | [HID over SPI] | Read only item |
| Connection Speed | Value input | HID Over SPI Connection Speed in Hz |
| Flags | [Single SPI Mode], [Dual SPI Mode], [Quad SPI Mode] | HID Over SPI Flags |
| Input Report Body Address | Value input | HID Over SPI Input Report Body Address |
| Input Report Header Address | Value input | HID Over SPI Input Report Header Address |
| Output Report Address | Value Input | HID Over SPI Output Report Address |
| Write Opcode | Value input | HID Over SPI Write Opcode |
| Read Opcode | Value input | HID Over SPI Read Opcode |
| Reset Pad Trigger | [Low], [High] | HID Over SPI Reset Pad Trigger |

Figure 170: BIOS Chipset Setup Menu – PCH-IO Configuration – SerialIO Configuration

| Aptio Setup – AMI | |
|--|------------|
| Chipset | |
| SerialIO Configuration | |
| I2C0 Controller | [Disabled] |
| I2C1 Controller ⁽¹⁾ | [Disabled] |
| I2C2 Controller ⁽¹⁾ | [Disabled] |
| I2C3 Controller ⁽¹⁾ | [Disabled] |
| I2C4 Controller | [Disabled] |
| I2C5 Controller | [Disabled] |
| I2C6 Controller | [Disabled] |
| I2C7 Controller | [Disabled] |
| SPI0 Controller | [Disabled] |
| SPI1 Controller | [Enabled] |
| SPI2 Controller | [Disabled] |
| SPI3 Controller | [Disabled] |
| SPI4 Controller | [Disabled] |
| SPI5 Controller | [Disabled] |
| SPI6 Controller | [Disabled] |
| UART0 Controller | [Enabled] |
| UART1 Controller | [Disabled] |
| UART2 Controller | [Disabled] |
| UART3 Controller | [Disabled] |
| UART4 Controller | [Disabled] |
| UART5 Controller | [Disabled] |
| UART6 Controller | [Disabled] |
| GPIO IRQ Route | [IRQ14] |
| <ul style="list-style-type: none"> > Serial IO I2C0 Settings ⁽²⁾ > Serial IO I2C1 Setting ⁽²⁾ > Serial IO I2C2 Setting ⁽²⁾ > Serial IO I2C3 Setting ⁽²⁾ > Serial IO I2C4 Settings ⁽²⁾ > Serial IO I2C5 Settings ⁽²⁾ > Serial IO I2C6 Settings ⁽²⁾ > Serial IO I2C7 Settings ⁽²⁾ > Serial IO SPI0 Settings ⁽³⁾ > Serial IO SPI1 Settings ⁽³⁾ > Serial IO SPI2 Settings ⁽³⁾ > Serial IO UART0 Settings ⁽⁴⁾ > Serial IO UART1 Settings ⁽⁴⁾ | |

| Aptio Setup – AMI | | |
|---|------------|--|
| Chipset | | |
| WITT/MITT I2C Test Device | [Disabled] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| WITT/MITT Device selection ⁽⁵⁾ | [MITT] | |
| I2C0 ⁽⁵⁾ | [Disabled] | |
| I2C1 ⁽⁵⁾ | [Disabled] | |
| I2C2 ⁽⁵⁾ | [Disabled] | |
| I2C4 ⁽⁵⁾ | [Disabled] | |
| I2C4 ⁽⁵⁾ | [Disabled] | |
| I2C5 ⁽⁵⁾ | [Disabled] | |
| WITT/MITT SPI Test Device | [Disabled] | |
| SPI0 ⁽⁶⁾ | [Disabled] | |
| SPI1 ⁽⁶⁾ | [Disabled] | |
| SPI2 ⁽⁶⁾ | [Disabled] | |
| UART Test Device | [Disabled] | |
| Additional Serial IO devices | [Disabled] | |
| SerialIO Timing parameters | [Disabled] | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

- ⁽¹⁾ These items activate only when enabling I2C0 Controller.
- ⁽²⁾ These items appear only when enabling I2C0/4/5/6/7 Controllers respectively.
- ⁽³⁾ These items appear only when enabling SPI0/1/2 Controllers respectively.
- ⁽⁴⁾ These items appear only when enabling UART0/1 Controllers respectively.
- ⁽⁵⁾ These items appear only when enabling WITT/MITT I2C Test Device.
- ⁽⁶⁾ These items appear only when enabling WITT/MITT SPI Test Device.

| Feature | Option | Description |
|---------------------------|--------------------------|--|
| I2C0/1/2/3/6/7 Controller | [Disabled], [Enabled] | Enables / Disables Seriallo Controller If given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI CFG Space will still be visible. This is needed to allow PCI enumerator access functions above 0 in a multifunction device. |
| SPI0/1/3/4/5/6 Controller | | The following devices depend on each other: I2C0 and I2C1, 2, 3 UART0 and UART1, SPI0, 1 UART2 and I2C4, 5 |
| UART1/3/4/5/6 Controller | | UART 0 (00:30:00) cannot disabled when: 1. Child device is enabled like CNVi Bluetooth (_SB.PC00>UA00>BTH0) UART 0 (00:30:00) cannot be enabled when: 1. I2S Audio codec is enabled (_SB.PC00.I2C0>HDAC) |
| I2C4 Controller | [Disabled], [Enabled] | Enables / Disables Seriallo Controller For I2C5 and UART2 to work, this device has to be enabled. |

| Feature | Option | Description |
|------------------------------|--|--|
| I2C5 Controller | [Disabled], [Enabled], [Post Code Only] | Enables / Disables SerialIo Controller For This device to work, I2C4 has to be enabled. |
| SPI2 Controller | [Disabled], [Enabled] | Enables / Disables SerialIo SPI2 Controller The following device depends from: Thermal Subsystem in PCI mode Otherwise SPI2 will not appear in this OS |
| UART0 Controller | [Disabled], [Enabled], [Communication port (COM)] | Set UART0 mode - DBG used for BIOS log print and / or Kernel OS Debug - COM – 16550 compatible serial port with Power Gating support |
| UART2 Controller | [Disabled] | Read only item |
| GPIO IRQ Route | [IRQ14], [IRQ15] | Route all GPIOs to one of the IRQ. |
| WITT/MITT I2C Test Device | [Disabled], [Enabled] | Enable SIO I2C WITT Device and select which are all controller used it |
| WITT/MITT Device selection | [WITT], [MITT] | Change WITT Device version |
| I2C0/1/2/4/5 | [Disabled], [Enabled] | Enable SIO I2C WITT Device and select which are all controller used it |
| WITT/MITT SPI Test Device | [Disabled], [Enabled] | Enable SIO SPI WITT Device and select which are all controller used it |
| SPI0/1/2 | [Disabled], [Enabled] | Enable SIO SPI WITT Device and select which are all controller used it |
| UART Test Device | [Disabled], [Enabled – UART0], [Enabled – UART1], [Enabled – UART2] | Choose if UART Test Device is used and with which controller |
| Additional Serial IO devices | [Disabled], [Enabled] | When enabled, ACPI will report additional devices connected to Serial IO. |
| SerialIO Timing parameters | [Disabled], [Enabled] | Enables additional timing parameters for all SerialIO controllers. Defaults can be changed in each controller setting. Platform restart required to apply changes. |

Figure 171: BIOS Chipset Setup Menu – PCH-IO Configuration – SerialIO Configuration – Serial IO I2C0 Settings

| Aptio Setup – AMI | |
|--|---|
| Chipset | |
| Serial IO I2C0 Settings | |
| > Serial IO Touch Pad Settings | → ←: Select Screen ↑ ↓ : Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| > Serial IO Touch Panel Settings | |
| Timing parameters disabled | |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

Figure 172: BIOS Chipset Setup Menu – PCH-IO Configuration – SerialIO Configuration – Serial IO I2C0 Settings – Serial IO Touch Pad Settings

| Aptio Setup – AMI | | |
|--|------------------|---|
| Chipset | | |
| Touch Pad | [Disabled] | |
| Touch Pad Interrupt Mode* | [APIC Interrupt] | |
| Device’s bus address*(1) | 0 | → ←: Select Screen ↑ ↓ : Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Device’s HID address*(1) | 0 | |
| Device’s bus speed*(1) | [100kHz] | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when enabling Touch Pad.

(1) These items appear only when selecting Custom device for Touch Pad.

| Feature | Option | Description |
|-----------|---|---|
| Touch Pad | [Disabled], [Synaptics Precision Touchpad], [Synaptics Forcepad], [ALPS Precision Touchpad ClickPad], [THAT Touchpad], [SenseI Forcepad], | Indicates what type of I2C Touch Pad is connected to this SerialIO controller |

| Feature | Option | Description |
|--------------------------|---------------------------------------|--|
| | [Smart C Cover], [Custom device] | |
| Touch Pad Interrupt Mode | [GPIO Interrupt], [APIC Interrupt] | Select different routing for interrupts from Touch Pad |
| Device's bus address | Value input | Specify parameters of custom I2C device |
| Device's HID address | Value input | Specify parameters of custom I2C device |
| Device's bus speed | [100kHz], [400kHz], [1MHz] | Specify parameters of custom I2C device |

Figure 173: BIOS Chipset Setup Menu – PCH-IO Configuration – SerialIO Configuration – Serial IO I2C0 Settings – Serial IO Touch Panel Settings

| Aptio Setup – AMI | | | |
|--|------------------|--|--|
| Chipset | | | |
| Touch Panel | [Disabled] | | |
| Touch Panel Interrupt Mode* | [APIC Interrupt] | | |
| Device's bus address* ⁽¹⁾ | 0 | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit | |
| Device's HID address* ⁽¹⁾ | 0 | | |
| Device's bus speed* ⁽¹⁾⁽²⁾ | [400kHz] | | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | | |

* These items appear only when enabling Touch Panel.

⁽¹⁾ These items appear when selecting Custom device for Touch Panel.

⁽²⁾ This item appears when selecting WACOM TouchPanel for Touch Panel.

| Feature | Option | Description |
|-------------|---|---|
| Touch Panel | [Disabled], [Atme13432 TouchPanel], [Atme12952 TouchPanel], [Elan9048 TouchPanel], N- Trig/Samsung 13.3"], [N-Trig/Sharp 12.5"], [WACOM TouchPanel], [Custom device] | Indicates what type of I2C Touch Panel is connected to this Seriallo controller |

| Feature | Option | Description |
|----------------------------|---------------------------------------|--|
| Touch Panel Interrupt Mode | [GPIO Interrupt], [APIC Interrupt] | Select different routing for interrupts from Touch Panel |
| Device’s bus address | Value input | Specify parameters of custom I2C device |
| Device’s HID address | Value input | Specify parameters of custom I2C device |
| Device’s bus speed | [100kHz], [400kHz], [1MHz] | Specify parameters of custom I2C device |

Figure 174: BIOS Chipset Setup Menu – PCH-IO Configuration – SerialIO Configuration – Serial IO I2C1/2/3/4/5/6/7 Settings

| Aptio Setup – AMI | |
|--|--|
| Chipset | |
| Serial IO I2C1/2/3/4/5/6/7 Settings | |
| Timing parameters disabled | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

Read only.

Figure 175: BIOS Chipset Setup Menu – PCH-IO Configuration – SerialIO Configuration – Serial IO SPI0/1/2 Settings

| Aptio Setup – AMI | |
|--|--|
| Chipset | |
| Serial IO SPI0/1/2 Settings | |
| ChipSelect 0 polarity | [Active High] |
| Delayed Rx Clock SPI0 | [0] |
| ChipSelect 1 polarity | [Active High] |
| Timing parameters disabled | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

| Feature | Option | Description |
|---------------------------|--------------------------------|---|
| ChipSelect 0/1 polarity | [Active Low], [Active High] | Sets initial polarity for ChipSelect signal. Active low is with initial idle polarity of low and vice versa |
| Delayed Rx Clock SPI0/1/2 | [0], [1], [2], [3] | Configure the SPI Delayed Rx Clock option: Default: 0 [DEC] Minimum: 1 [DEC] Maximum: 10 [DEC] |

Figure 176: BIOS Chipset Setup Menu – PCH-IO Configuration – SerialIO Configuration – Serial IO UART0/1 Settings

| Aptio Setup – AMI | |
|--|---|
| Chipset | |
| Serial IO UART0/1 Settings | |
| Hardware Flow Control | [Disabled] |
| DMA Enable | [Enabled] |
| Power Gating | [Enabled] |
| Timing parameters disabled | |
| | → ←: Select Screen ↑ ↓ : Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

| Feature | Option | Description |
|-----------------------|-------------------------------------|--|
| Hardware Flow Control | [Disabled], [Enabled] | When enabled configurations additional 2 GPIO pads for use as RTS/CTS signals for UART |
| DMA Enable | [Disabled], [Enabled] | [Enabled]: UART OS driver will use DMA when possible. [Disabled]: OS driver will enforce PIO mode |
| Power Gating | [Disabled], [Enabled], [Auto] | [Disabled]: No _PS0 _PS3 support, device is left in D0, after initialization [Enabled]: _PS0 _PS3 that supports getting device out of reset [Auto]: _PS0 and _PS3 detection through ACPI if device was initialized prior to first PG. If it was used (DBG2) PG is disabled |

Figure 177: BIOS Chipset Setup Menu – PCH-IO Configuration – SCS Configuration

| Aptio Setup – AMI | | |
|--|------------|--|
| Chipset | | |
| eMMC 5.1 Controller | [Disabled] | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| eMMC 5.1 HS400 Mode* | [Disabled] | |
| Enable HS400 Software tuning* ⁽¹⁾ | [Disabled] | |
| Driver Strength* | [40 Ohm] | |
| eMMC 5.1 HS200 Mode* ⁽²⁾ | [Enabled] | |
| UFS 2.0 Controller 1 | [Disabled] | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

* These items appear only when enabling eMMC 5.1 Controller.

⁽¹⁾ This item appears only when enabling eMMC 5.1 HS400 Mode.

⁽²⁾ This item appears only when disabling eMMC 5.1 HS400 Mode.

| Feature | Option | Description |
|------------------------------|------------------------------------|---|
| eMMC 5.1 Controller | [Disabled], [Enabled] | Enable or disable SCS eMMC 5.1 Controller |
| eMMC 5.1 HS400 Mode | [Disabled], [Enabled] | Enable or disable SCS eMMC 5.1 HS400 Mode |
| Enable HS400 Software tuning | [Disabled], [Enabled] | Software tuning should improve eMMC HS400 stability at the expense of boot time |
| Diver Strength | [33 Ohm], [40 Ohm], [50 Ohm] | Set I/O driver strength |
| eMMC 5.1 HS200 Mode | [Disabled], [Enabled] | Enable or disable SCS eMMC 5.1 HS200 Mode |
| UFS 2.0 Controller 1 | [Disabled], [Enabled] | Enable or disable UFS 2.0 Controller |

Figure 178: BIOS Chipset Setup Menu – PCH-IO Configuration – ISH Configuration

| Aptio Setup – AMI | |
|--|--|
| Chipset | |
| ISH is not available | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

Read only.

Figure 179: BIOS Chipset Setup Menu – PCH-IO Configuration – Pch Thermal Throttling Control

| Aptio Setup – AMI | |
|--|---------------------|
| Chipset | |
| Thermal Throttling Level | [Suggested Setting] |
| Thermal Throttling ⁽¹⁾ | [Disabled] |
| TT State 13 ⁽¹⁾ | [Disabled] |
| Thermal Throttling Lock ⁽¹⁾ | [Disabled] |
| T0 Level ⁽¹⁾ | 0 |
| T1 Level ⁽¹⁾ | 0 |
| T2 Level ⁽¹⁾ | 0 |
| DMI Thermal Setting | [Suggested Setting] |
| DMI Thermal Sensor Autonomous Width ⁽²⁾ | [Disabled] |
| Thermal Sensor 0 Width ⁽²⁾ | [x8] |
| Thermal Sensor 1 Width ⁽²⁾ | [x4] |
| Thermal Sensor 2 Width ⁽²⁾ | [x2] |
| Thermal Sensor 3 Width ⁽²⁾ | [x1] |
| SATA Thermal Setting | [Suggested Setting] |
| Port 0 ⁽³⁾ | |
| T1 Multiplier ⁽³⁾ | [x1] |
| T2 Multiplier ⁽³⁾ | [x2] |
| T3 Multiplier ⁽³⁾ | [x4] |
| Alternate Fast Init Tdispatch ⁽³⁾ | [Disabled] |
| Tdispatch ⁽³⁾ | [~32ms] |
| Tinactive ⁽³⁾ | [~32ms] |

| Aptio Setup – AMI | | |
|--|------------|------------------------|
| Chipset | | |
| Port 1 ⁽³⁾ | | Enter: Select |
| T1 Multiplier ⁽³⁾ | [x1] | +/-: Change Opt. |
| T2 Multiplier ⁽³⁾ | [x2] | F1: General Help |
| T3 Multiplier ⁽³⁾ | [x4] | F2: Previous Values |
| Alternate Fast Init Tdispatch ⁽³⁾ | [Disabled] | F3: Optimized Defaults |
| Tdispatch ⁽³⁾ | [~32ms] | F4: Save & Exit |
| Tinactive ⁽³⁾ | [~32ms] | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

⁽¹⁾ These items appear only when selecting Manual for Thermal Throttling Level.

⁽²⁾ These items appear only when selecting Manual for DMI Thermal Setting.

⁽³⁾ These items appear only when selecting Manual for SATA Thermal Setting.

| Feature | Option | Description |
|-------------------------------------|---|--|
| Thermal Throttling Level | [Suggested Setting], [Manual] | Determine if use Intel suggested setting |
| Thermal Throttling | [Disabled], [Enabled] | Enable / Disable the thermal throttling status control |
| TT State 13 | [Disabled], [Enabled] | PMSync state 13 will force at least T2 state |
| Thermal Throttling Lock | [Disabled], [Enabled] | Lock the entire TL register |
| T0 Level | Value input | If Trip Point Temperature <= T0Level, the system is in T0 state |
| T1 Level | Value input | If T1Level >= Trip Point Temperature > T0Level, the system is in T1 state |
| T2 Level | Value input | If T2Level >= Trip Point Temperature > T1Level, the system is in T2 state |
| DMI Thermal Setting | [Suggested Setting], [Manual] | Determine if use Intel suggested setting |
| DMI Thermal Sensor Autonomous Width | [Disabled], [Enabled] | Enable / Disable Thermal Sensor initiated Autonomous Width Negotiation |
| Thermal Sensor 0/1/2/3 Width | [x1], [x2], [x4], [x8], [x16] | Determine the DMI Link Width when the output from the Thermal Sensor is T0/1/2/3 |
| SATA Thermal Setting | [Suggested Setting], [Manual] | Determine if use Intel suggested setting |
| T1/2/3 Multiplier | [Disabled], [x1], [x2], [x4] | Determine the value of SATA Port T1/2/3 Multiplier |

| Feature | Option | Description |
|-------------------------------|---------------------------------|--|
| Alternate Fast Init Tdispatch | [Disabled], [Enabled] | Enable / Disable SATA Port Alternate Fast Init Tdispatch |
| Tdispatch | [~32ms], [~128ms], [~8ms] | Determine the value of SATA Port Tdispatch |
| Tinactive | [~32ms], [~128ms], [~8ms] | Determine The value of SATA Port Tinactive |

Figure 180: BIOS Chipset Setup Menu – PCH-IO Configuration – FIVR Configuration

| Aptio Setup – AMI | |
|--|--|
| Chipset | |
| External V1P05 Rail Sx/S0ix Configuration | |
| Enable Rail in S0i1/S0i2 | [Disabled] |
| Enable Rail in S0i3 | [Disabled] |
| Enable Rail in S3 | [Disabled] |
| Enable Rail in S4 | [Disabled] |
| Enable Rail in S5 | [Disabled] |
| Enable Rail in S0 | [Disabled] |
| External Vnn Rail Sx/S0ix Configuration | |
| Enable Rail in S0i1/i2 | [Disabled] |
| Enable Rail in S0i3 | [Disabled] |
| Enable Rail in S3 | [Disabled] |
| Enable Rail in S4 | [Disabled] |
| Enable Rail in S5 | [Disabled] |
| Enable Rail in S0 | [Disabled] |
| External Vnn Rail Voltage Configuration at S0 and S0ix | [0.78V@Bypass – 0.78V@Bypass – 1.05V@Internal] |
| External Rails Voltage and Current settings | |
| External V1P05 Icc Max Value | 500 |
| External Vnn Icc Max Value | 500 |
| VCCIN_AUX voltage rail timing configuration | |
| Retention to Low Current Mode | 43 |
| Retention to High Current Mode | 54 |
| Low to High Current Mode | 12 |
| Off to High Current Mode | 150 |
| → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values | |

| Aptio Setup – AMI | | |
|--|------------|------------------------------|
| Chipset | | |
| FIVR Dynamic PM | [Disabled] | F3: Optimized Defaults |
| VCCST ICCMax Control | [Enabled] | F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

| Feature | Option | Description |
|--|---|--|
| Enable Rail in S0i1/S0i2/S0i3/S3/S4/S5/S0 | [Disabled], [Enabled] | Enables External V1P05 / Vnn Rail in corresponding Sx/S0ix |
| External Vnn Rail Voltage Configuration at S0 and S0ix | [0.78V@Bypass – 0.78V@Bypass – 1.05V@Internal], [1.05V@Bypass – 1.05V@Bypass – 1.05V@Bypass] | Configures TARGET_VOLT_LEVEL for External Rail |
| External V1P05 / Vnn Icc Max Value | Value input | Icc Max Value for external V1p05 / Vnn rail. Expressed in mA. Accepted value are between 0 and 500 mA. |
| Retention to Low Current Mode | Value input | Transition time in microseconds from Off (0V) to High Current Mode Voltage. This field has 1us resolution. |
| Retention to High Current Mode | Value input | Transition time in microseconds from Retention Mode Voltage to High Current Mode Voltage. This field has 1us resolution. |
| Low to High Current Mode | Value input | Transition time in microseconds from Low Current Mode Voltage to High Current Mode Voltage. This field has 1us resolution. |
| Off to High Current Mode | Value input | Transition time in microseconds from Off (0V) to High Current Mode Voltage. This field has 1us resolution. 0 = Transition to 0V is disabled. The value must be greater than or equal to VccST board FET ramp time. |
| FIVR Dynamic PM | [Disabled], [Enabled] | Enable / Disable FIVR Dynamic Power Management |
| VCCST ICCMax Control | [Disabled], [Enabled] | Enable / Disable FIVR VCCST ICCMax Control |

Figure 181: BIOS Chipset Setup Menu – PCH-IO Configuration – PMC Configuration

| Aptio Setup – AMI | |
|--|---|
| Chipset | |
| > PMC ADR Configuration | |
| | → ←: Select Screen ↑ ↓ : Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

Figure 182: BIOS Chipset Setup Menu – PCH-IO Configuration – PMC Configuration – PMC ADR Configuration

| Aptio Setup – AMI | |
|--|---|
| Chipset | |
| ADR Enable | [Platform-POR] |
| Host Partition Reset ADR Enable* | [Enabled] |
| ADR timer 1 expire time* | 32 |
| ADR timer 1 time unit* | [1s] |
| | → ←: Select Screen ↑ ↓ : Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | |

* These items appear only when enabling ADR enable.

| Feature | Option | Description |
|---------------------------------|---|---|
| ADR enable | [Platform-POR], [Enabled], [Disabled] | Enable asynchronous DRAM refresh |
| Host Partition Reset ADR Enable | [Platform-POR], [Enabled], [Disabled] | Enables / Disables ADR on Host Partition Reset |
| ADR timer 1 expire time | Value input | Type desired ADR timer expire time, valid values - <1, 256>. Entered time is scaled by ADR timer time unit. |

| Feature | Option | Description |
|-----------------------|--|-----------------------------|
| ADR timer 1 time unit | [1us], [10us], [100us], [1ms], [10ms], [100ms], [1s], [10s] | Select ADR timer time unit. |

Figure 184: BIOS Security Setup Menu – Secure Boot – Key Management

| Aptio Setup – AMI | | | | |
|--|------------|------|------------|--|
| Security | | | | |
| Vendor Keys | Valid | | | |
| Factory Key Provision | [Disabled] | | | |
| > Restore Factory Keys | | | | |
| > Reset To Setup Mode | | | | |
| > Enroll Efi Image | | | | |
| > Export Secure Boot variables | | | | |
| Secure Boot variable | Size | Keys | Key Source | |
| > Platform Key (PK) | 0 | 0 | No Keys | |
| > Key Exchange Keys (KEK) | 0 | 0 | No Keys | |
| > Authorized Signatures (db) | 0 | 0 | No Keys | |
| > Forbidden Signatures (dbx) | 0 | 0 | No Keys | |
| > Authorized TimeStamps (dbt) | 0 | 0 | No Keys | |
| > OsRecovery Signatures (dbr) | 0 | 0 | No Keys | |
| → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit | | | | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | | | |

| Feature | Option | Description |
|------------------------------|---|---|
| Factory Key Provision | [Disabled], [Enabled] | Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode. |
| Reset Factory Keys | [Yes], [No] | Force System to User Mode. Install factory default Secure Boot key databases. |
| Reset to Setup Mode | [Yes], [No] | Delete all Secure Boot key databases from NVRAM. |
| Enroll Efi Image | Select a File system | Allow the image to run in Secure Boot mode. Enroll SHA256 Hash certificate of a PE image into Authorized Signature Database (db). |
| Export Secure Boot variables | Select a File system | Save NVRAM content of Secure Boot variables to a file |
| Platform Key (PK) | [Details], [Export], [Update], [Delete] | Enroll Factory Defaults or load certificates from a file: 1. Public Key Certificate: (a) EFI_SIGNATURE_LIST (b) EFI_CERT_X509 (DER) (c) EFI_CERT_RSA2048 (bin) (d) EFI_CERT_SHAXXX |
| Key Exchange Keys (KEK) | [Details], [Export], [Update], [Append], [Delete] | 2. Authenticated UEFI Variable 3. EFI PE / COFF Image (SHA256) Key Source: Factory, Modified, Mixed |
| Authorized Signatures (db) | [Details], [Export], | |

| Feature | Option | Description |
|-----------------------------|---|-------------|
| | [Update], [Append], [Delete] | |
| Forbidden Signatures (dbx) | [Details], [Export], [Update], [Append], [Delete] | |
| Authorized TimeStamps (dbt) | [Update], [Append] | |
| OsRecovery Signatures (dbr) | [Update], [Append] | |

Figure 185: BIOS Security Setup Menu – Secure Boot

| Aptio Setup – AMI | | |
|--|--------------------------|--|
| Security | | |
| System Mode | Setup | |
| Secure Boot | [Disabled] Not Active | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit |
| Secure Boot Mode | [Standard] | |
| > Restore Factory Keys* | | |
| > Reset To Setup Mode | | |
| > Key Management* | | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | |

*These items are selectable only when selecting Custom for Secure Boot Mode.

| Feature | Option | Description |
|----------------------|--------------------------|--|
| Secure Boot | [Disabled], [Enabled] | Secure Boot feature is Active if Secure Boot is Enabled, Platform Key (PK) is enrolled and the System is in User mode. The mode change requires platform reset. |
| Secure Boot Mode | [Standard], [Custom] | Secure Boot mode options: Standard or Custom. In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication. |
| Restore Factory Keys | [Yes], [No] | Force System to User Mode. Install factory default Secure Boot key databases. |

8.2.4.1. Remember the Password

It is highly recommended to keep a record of all passwords in a safe place. Forgotten passwords results in being locked out of the system.

If the system cannot be booted because the User Password or the Supervisor Password are not known, contact Kontron Support for further assistance.



HDD security passwords cannot be cleared using the above method.

8.2.5. Boot Setup Menu

The boot setup menu lists the boot device priority order, that is generated dynamically.

Figure 186: BIOS Boot Setup Menu

| Aptio Setup – AMI | | | | | |
|---|----------|-------------------------------|----------|------|------------------------|
| Main | Advanced | Chipset | Security | Boot | Save & Exit |
| Boot Configuration | | | | | |
| Setup Prompt Timeout | | 1 | | | |
| Bootup NumLock State | | [On] | | | |
| Quiet Boot | | [Disabled] | | | |
| Fixed Boot Order Mode | | [Disabled] | | | |
| Boot Option Priorities ⁽¹⁾ | | | | | |
| Boot Option #1 ⁽¹⁾ | | [UEFI: Built-in EFI Shell] | | | |
| Fast Boot | | [Disabled] | | | → ←: Select Screen |
| SATA Support ⁽²⁾ | | [Last Boot SATA Devices Only] | | | ↑ ↓: Select Item |
| NVMe Support ⁽²⁾ | | [Enabled] | | | Enter: Select |
| UFS Support ⁽²⁾ | | [Enabled] | | | +/-: Change Opt. |
| VGA Support ⁽²⁾ | | [EFI Driver] | | | F1: General Help |
| USB Support ⁽²⁾ | | [Full Initial] | | | F2: Previous Values |
| PS2 Devices Support ⁽²⁾ | | [Enabled] | | | F3: Optimized Defaults |
| Network Stack Driver Support ⁽²⁾ | | [Disabled] | | | F4: Save & Exit |
| Redirection Support ⁽²⁾ | | [Disabled] | | | ESC: Exit |
| Version 2.22.1293 Copyright (C) 2024 AMI | | | | | |

⁽¹⁾ These items appear only when disabling Fixed Boot Order Mode.

⁽²⁾ These items appear only when enabling Fast Boot.

| Feature | Option | Description |
|-----------------------|---|--|
| Setup Prompt Timeout | Value Input | Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting. |
| Bootup NumLock State | [On], [Off] | Select the keyboard NumLock state [On]: The keys on the keypad will act as numeric keys. [Off]: The keys on the keypad will act as cursor keys. |
| Quiet Boot | [Disabled], [Enabled] | Enables or disables Quiet Boot option |
| Fixed Boot Order Mode | [Disabled], [Enabled] | If enabled then 'Fixed Order Boot Mode' is used, otherwise 'BCP boot order' (default). NOTE: If you changed this setting please immediately save & exit and re-enter setup to apply further changes on boot settings! |
| Boot Option #1 | [UEFI: Built-in EFI Shell], [Disabled] | Sets the system boot order |

| Feature | Option | Description |
|------------------------------|--|---|
| Fast Boot | [Disabled], [Enabled] | Enables or disables boot with initialization of a minimal set of devices required to launch active boot option. Has no effect for BBS boot options. |
| SATA Support | [Last Boot SATA Devices Only], [All SATA Devices] | If Last Boot SATA Devices Only, Only last boot SATA devices will be available in Post. If All SATA Devices, all SATA devices will be available in OS and Post. |
| NVMe Support | [Disabled], [Enabled] | If Disabled, NVMe device will be skipped. |
| UFS Support | [Disabled], [Enabled] | If Disabled, UFS device will be skipped. |
| VGA Support | [Auto], [EFI Driver] | If Auto, only install Legacy OpRom with Legacy OS and logo would NOT be shown during post. Efi driver will still be installed with EFI OS. |
| USB Support | [Disabled], [Full Initial], [Partial Initial] | If Disabled, all USB devices will NOT be available until after OS boot. If Partial Initial, USB Mass Storage and specific USB port / device will NOT be available before OS boot. If Enabled, all USB devices will be available in OS and Post. |
| PS2 Devices Support | [Disabled], [Enabled] | If Disabled, PS2 devices will be skipped. |
| Network Stack Driver Support | [Disabled], [Enabled] | If Disabled, Network Stack Driver will be skipped. |
| Redirection Support | [Disabled], [Enabled] | If disable, Redirection function will be disabled. |

8.2.6. Save & Exit Setup Menu

The exit setup menu provides functions for handling changes made to the UEFI BIOS settings and the exiting of the setup program.

Figure 187: BIOS Save & Exit Setup Menu

| Aptio Setup – AMI | | | | | |
|---|----------|---------|----------|--|-------------|
| Main | Advanced | Chipset | Security | Boot | Save & Exit |
| Save Options Save Changes and Exit Discard Changes and Exit Save Changes and Reset Discard Changes and Reset Save Changes Discard Changes | | | | | |
| Default Options Restore Defaults Save as User Defaults Restore User Defaults Boot Override UEFI: Built-in EFI Shell | | | | → ←: Select Screen ↑ ↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit | |
| Version 2.22.1293 Copyright (C) 2024 AMI | | | | | |

| Feature | Description |
|---------------------------|--|
| 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. |
| 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. |
| UEFI: Built-in EFI Shell | This group of functions includes a list of tokens, each of them corresponding to one device within the boot order. Select a drive to immediately boot that device regardless of the current boot order. If booting to EFI Shell this way, an exit from the shell returns to Setup. |

9/Technical Support

For technical support contact our Support Department:

- › E-mail: support@kontron.com
- › Phone: +49-821-4086-888

Make sure you have the following information available when you call:

- › Product ID Number (PN)
- › Serial Number (SN)



The serial number can be found on the Type Label, located on the product's rear panel.

Be ready to explain the nature of your problem to the service technician.

9.1. Returning Defective Merchandise

All equipment returned to Kontron must have a Return of Material Authorization (RMA) number assigned exclusively by Kontron. Kontron cannot be held responsible for any loss or damage caused to the equipment received without an RMA number. The buyer accepts responsibility for all freight charges for the return of goods to Kontron's designated facility. Kontron will pay the return freight charges back to the buyer's location in the event that the equipment is repaired or replaced within the stipulated warranty period. Follow these steps before returning any product to Kontron.

1. Visit the RMA Information website: <https://www.kontron.com/en/support/rma-information>.
2. Download the RMA Request sheet for Kontron Europe GmbH and fill out the form. Take care to include a short, detailed description of the observed problem or failure and to include the product identification Information (Name of product, Product number and Serial number). If a delivery includes more than one product, fill out the above information in the RMA Request form for each product.
3. Send the completed RMA-Request form to the fax or email address given below at Kontron Europe GmbH. Kontron will provide an RMA-Number.
4. Kontron Europe GmbH
RMA Support
Phone: +49 (0) 821 4086-0
Fax: +49 (0) 821 4086 111
Email: service@kontron.com
5. The goods for repair must be packed properly for shipping, considering shock and ESD protection.



Goods returned to Kontron Europe GmbH in non-proper packaging will be considered as customer caused faults and cannot be accepted as warranty repairs.

6. Include the RMA-Number with the shipping paperwork and send the product to the delivery address provided in the RMA form or received from Kontron RMA Support.

10/ Storage and Transportation

10.1. Storage

If the product is not in use for an extended period time, disconnect the power plug from the power supply. If it is necessary to store the product then re-pack the product as originally delivered to avoid damage. The storage facility must meet the product's environmental storage requirements as stated within this user guide. Kontron recommends keeping the original packaging material for future storage or warranty shipments.

10.2. Transportation

To ship the product, use the original packaging, designed to withstand impact and adequately protect the product. When packing or unpacking products, always take shock and ESD protection into consideration and use an EOS/ESD safe working area.

11/ Warranty

Due to their limited-service life, parts that by their nature are subject to a particularly high degree of wear (wearing parts) are excluded from the warranty beyond that provided by law. This applies to the lithium battery, for example.

12/ Disposal

12.1. Disposal

Dispose of the product in accordance with country, state, or local regulations and requirements as part of your disposal and decommissioning policies or recycle the product or parts of the product for re-use after performing data sanitization to erase sensitive data stored on the product's memory devices.

When disposing of the product

- › Remove any product labels from the product that could indicate ownership and provide a clue to the type of data stored on the memory device.
- › Comply with your company's environmental requirements and the requirements of Waste Electrical and Electronic Equipment (WEEE) directive.
- › Use data sanitization guidelines to ensure that data sensitive to your business and/or confidential or proprietary data and software is removed from the product using a data sanitization method that stops the data from being retrieved or reconstructed.

12.2. WEEE Compliance

The Waste Electrical and Electronic Equipment (WEEE) Directive aims to:

- › Reduce waste arising from electrical and electronic equipment (EEE).
- › Make producers of EEE responsible for the environmental impact of their products, especially when the product becomes waste.
- › Encourage separate collection and subsequent treatment, reuse, recovery, recycling and sound environmental disposal of EEE.
- › Improve the environmental performance of all those involved during the lifecycle of EEE.



Environmental protection is a high priority with Kontron.
Kontron follows the WEEE directive
You are encouraged to return our products for proper disposal.

12.3. Data Sanitization

Data sanitization is the process of permanently erasing or destroying sensitive data on the product's memory devices to prevent unauthorized access to data sensitive to your business and/or confidential/proprietary data stored on the memory devices.

When designing a system, users must plan for data sanitization and design in memory devices that are easier to sanitize, memory devices from manufacturers that provide an effective data erasure tool or a return to factory default command.

When performing data sanitization, the user must consider if the product's memory devices contain sensitive data and develop a data sanitization plan to erase all sensitive data in accordance with country, state, or local data sanitization regulations and requirements or as part of your disposal and decommissioning policies.



Data Sanitization

Users are responsible for erasing sensitive data on memory devices in accordance with country, state, or local data sanitization regulations and requirements, or as part of your disposal and decommissioning policies.

Kontron recommends performing data sanitization when reusing the product in a different user environment, sending the product in for repair, disposing of the product or decommissioning the product.

General guidelines when performing data sanitization on memory devices containing data sensitive to your business and/or confidential/proprietary data are:

- › Before powering down, consider if power is required to perform data sanitization on the product's memory devices.
- › When disconnected from the power source, dismantle all removable memory devices from the product and erase sensitive data.
- › Volatile memory devices only store data temporarily. Data on volatile memory can be erased easily by disconnecting the power or removing the battery for approximately 24 hours.
- › Non-volatile memory devices store data permanently and retain information when disconnected from power. Data on non-volatile memory, and must be actively erased using one of the following methods:
 - › Use an accredited third-party software tool that provides an audit trail, capable of performing a complete data clean including areas such as hidden data and bad blocks not accessed by general service-based utilities.
 - › Use the manufacturer's data erasure tool or return to factory default command (if provided by the manufacturer). The manufacturer's tools and commands have been designed to fulfil the data sanitization requirement of the manufacturer's specific memory device(s).
 - › Use the physical destruction method on memory devices that cannot be securely erased using software. The aim of the destruction is to break the silicon die within the chips package to prevent reading data from the die. If this service is performed by a third-party, obtain destruction certificates for confirmation.
- › Always verify that all sensitive data has been effectively sanitized.



Dismantle Removable Memory

Dismantle all removable memory devices and erase sensitive data for reuse by using:

- › An accredited third-party software tool.
- › Manufacturer's data erasure tool' or 'return to factory default command'. (if provided)

If the removable memory is not for reuse, physically destruct the memory according to data sanitization guidelines.



Erase Data

To ensure that forensic tools cannot be used to recover sensitive data:

- › Use an accredited third-party software tool, with an audit trail, capable of performing a complete data clean including areas such as hidden data and bad blocks not accessed by general service-based utilities.
- › Use the manufacturer's data erasure tool or return to factory default command designed to fulfil data sanitization requirement of the manufacturer's specific memory device(s).



Physical Destruction

When physically destructing the memory:

- › Follow proper safety protocols.
- › Break the chip packaged silicon die into two or more parts, fragments ≤ 6 mm.
- › Check both sides as memory devices may be positioned on the rear side.
- › Use a third-party destruction company providing certificates for confirmation.

12.4. Statement of Memory Volatility

The 3.5"-SBC-AML/ADN/AMH/ADH statement of memory volatility provides the user with a detailed list of the product's memory devices and their volatility, to enable the user to develop a suitable data sanitization plan.

Note that not all listed memory devices may be part of your delivered product. Some memory devices may be configuration options. Users are responsible for considering the memory devices installed on the product and must take appropriate action to clear the memory if required.

Third-party devices such as M.2 modules installed on the product may include memory devices and should be removed by the user before disposing of the product. It is the responsibility of the user to observe that the third-party devices are removed according to the manufacturer's instructions.



In some cases, special tools and/or software are necessary to access the memory



The statement of memory volatility list, is an overview of all the known possible memory devices and due to configuration options may differ from your delivered product.

Table 55: 3.5"-SBC-AML/ADN/AMH/ADH Statement of Memory Volatility

| Memory Type | Ref. # /Loc. | Memory Size | Volatility | Retain Data when Power Off | Alterable in Field ^[1] | Battery Backed Up | Data Type | Write Protected | Emergency Erase | Process to Clear |
|-------------------------------|--------------|---|---|----------------------------|-----------------------------------|-------------------|----------------------------|-----------------|-----------------|-----------------------|
| DDR | | | | | | | | | | |
| DDR5 SO-DIMM | | Up to 16 GB | Volatile | No | Yes | No | User Data | No | No | NA |
| EC | | | | | | | | | | |
| Embedded Controller MEC1521 | | Code Storage: 480 KB (Code + Data) Data RAM: 32 KB | Non-volatile (Code storage) Volatile (RAM) | Yes | Yes | No | Embedded controller config | Yes | No | Perform EC FW update |
| CMOS-FLASH SPI MX25V16 35FM2I | | 16 Mbit | Non-volatile | Yes | Yes | No | EFI Boot | Yes | Yes | Perform BIOS recovery |
| LAN | | | | | | | | | | |
| FLASH SPI W25Q16J VSSIQ | | 16 Mbit | Non-volatile | Yes | Yes | No | EFI Boot | Yes (SW) | No | Perform BIOS recovery |
| BIOS | | | | | | | | | | |
| FLASH SPI W25Q256J VEIQ | | 256 Mbit | Non-volatile | Yes | Yes | No | EFI Boot | Yes (SW) | No | Perform BIOS recovery |
| EEPROM | | | | | | | | | | |
| EEPROM AT24C32E-SSHM-T | | 32 Kbit | Non-volatile | Yes | Yes | No | Module ID Data | Yes | No | NA |

| Memory Type | Ref. # /Loc. | Memory Size | Volatility | Retain Data when Power Off | Alterable in Field ^[1] | Battery Backed Up | Data Type | Write Protected | Emergency Erase | Process to Clear |
|------------------------------|--------------|---|--------------|----------------------------|-----------------------------------|-------------------|----------------|-----------------|-----------------|---|
| LVDS | | | | | | | | | | |
| EEPROM Chrontel CH9904 | | 64 Kbits | Non-volatile | Yes | Yes | No | Module ID Data | Yes | No | NA |
| PD | | | | | | | | | | |
| F75183I | | uC internal RAM 256 Byte / Flash ROM Size: 16 KByte | Non-volatile | Yes | No | No | PSC Config. | Yes | No | NA (Board will not operate with modified data) |
| VCORE | | | | | | | | | | |
| MP2964R | | 8 Kbit | Non-volatile | Yes | No | No | VR Config. | No | No | NA |
| TPM | | | | | | | | | | |
| SLB 9672XU2.0 | | 51 KByte | Non-volatile | Yes | Yes | No | User Data | Yes | No | Perform clear item under OS |

^[1] In some cases special tools and/or software are necessary to access the memory.

13/ Cyber Security

Cyber security is an important aspect to consider when installing, operating, maintaining and disposing of the product. This chapter provides cyber security guidelines for the user.



Security White Paper

For cyber security guidelines to protect your Kontron product from potential cyber security threats, refer the [Kontron Security Guideline Whitepaper](#).



Security Measures

Kontron is not aware of the final target end user environment in which the product operates. It is not possible for Kontron to provide precise instructions for your cyber security measures. Kontron strives to provide hints for considerations for your threat analysis and to point out particular security mechanisms implemented in Kontron products.

13.1. Security Defense Strategy

When developing your security defense strategy consider implementing the following guidelines to help you effectively secure the product:

- › Policies and procedures developed in association with the product's/end environment's security.
- › Instructions and recommendations for periodic security maintenance activities and reporting product security incidents.
- › Security network controls/setting such as firewall rules.
- › Third-party software tools that further protect the product.
- › Authentication to access the product, limit user privileges and managing user accounts.
- › Data encryption.
- › Reduced number of potential security entry points.
- › BIOS/OS and security updates that do not compromise the product's operation or defense in depth strategy.
- › User accounts with length and complexity requirements.
- › Supplied default passwords are changed.
- › Limited network access (IP address range).
- › Installation of anti-virus and malware software.
- › Network access requirements such as VPN.

Appendix: List of Acronyms

| | |
|-----------------------|---|
| AC | Alternating Current |
| AWG | American Wire Gauge |
| BIOS | Basic Input Output System |
| CAN | Controller Area Network |
| CE | Conformité Européenne |
| COM | Communication port |
| DC | Direct Current |
| DIMM | Dual In-line Memory Module |
| DOC | Declaration of Conformity |
| DDIO | Digital Data Input/Output |
| DDR5 | Double Data Rate 5 |
| DP | Display Port |
| ECC | Error Code Correction |
| eDP | Embedded DisplayPort |
| EMC | ElectroMagnetic compatibility |
| ESD | ElectroStatic Discharge |
| FCC | Federal Communications Commission |
| GB | Ground Benign |
| GbE | Giga Bit Ethernet |
| GSPI | Generic Serial Peripheral Interface |
| HD | High Definition |
| HDMI | High Definition Multimedia Interface |
| IEC | International Electrotechnical Commission |
| I²C | Inter-Intergrated Circuit |
| IOT | Internet of Things |
| LAN | Local Area Network |
| LED | Light Emitting Diode |
| LPC | Limited Power Source |
| LVDS | Low Voltage Differential Signaling |
| MBR | Master Boot Record |
| MDI | Media Dependent Interface |
| MFG mode | Manufacturing mode |
| MTBF | Mean Time Before Failure |
| NVME | Non-Volatile Memory Express |
| PCIe | Peripheral Component Interconnect Express |
| PN | Part Number |
| PS | Power Source |

| | |
|----------------|---|
| PVC | Polyviny Chloride |
| RAM | Random Access Memory |
| RMA | Return of Material Authorization |
| RoHS | Restriction of Hazardous Substances |
| RTC | Real Time Clock |
| RX | Receive |
| SATA | Serial Advanced Technology Attachment, |
| SD card | Secure Digital Card |
| SDP | Standard Data Port |
| SIM | Subscriber Identity Module |
| SM | System Management |
| SN | Serial Number |
| SPI | Serial Peripheral Interface |
| SP/DIF | Sony Philips / Digital Interface |
| SVGA | Super Video Graphics Array |
| TCP | Transmission Code protocol |
| TDP | Thermal Design Power |
| TFT | Thin-Film Transistors |
| TPM | Trusted Platform Module |
| TX | Transmit |
| UART | Universal Asynchronous Receiver Transmitter |
| UEFI | Unified Extensible Firmware Interface |
| UL | Underwriters Laboratories |
| USB | Universal Serial Bus |
| UTP | Unshielded twisted pair |
| UV | Ultra Violet |
| VESA | Video Electronics Standards Association |
| VGA | Video Graphics Array |
| WEEE | Waste Electrical and Electronic Equipment |
| WXGA | Wide Extended Graphics Array |
| XGA | Extended Graphics Array |



About Kontron

Kontron is a global leader in IoT/Embedded Computing Technology (ECT) and offers individual solutions in the areas of Internet of Things (IoT) and Industry 4.0 through a combined portfolio of hardware, software and services. With its standard and customized products based on highly reliable state-of-the-art technologies, Kontron provides secure and innovative applications for a wide variety of industries. As a result, customers benefit from accelerated time-to-market, lower total cost of ownership, extended product lifecycles and the best fully integrated applications.

For more information, please visit: www.kontron.com

Global Headquarters

Kontron Europe GmbH

Gutenbergstraße 2
85737 Ismaning, Germany
Tel.: +49 8214 4086-0
info@kontron.com

www.kontron.de

