EM[®] PRO rack – Revision 3 – Device Reference Manual – P –



Please note that some systems may differ from the picture shown above



Copyright © 2024 E.E.P.D. GmbH. All rights reserved.



Manufacturer

E.E.P.D. Electronic Equipment Produktion & Distribution GmbH Gewerbering 3 85258 Weichs

Phone: +49 8136 2282 – 0 Web: https://www.eepd.de E-Mail: sales@eepd.de

Device Reference Manual – P – Revision 3

General Notes

This user manual is for your information.

The information contained herein has been checked carefully and is believed to be reliable. However, E.E.P.D. GmbH gives no guarantee or warranty concerning the accuracy of spoken information and shall not be responsible for any loss or damage of any nature resulting from the usage of or from reliance upon it.

We are thankful for all suggestions or improvements at any time.

E.E.P.D. GmbH reserves the right to make changes in the products or specifications, or both, at any time without notice.

Copyright Notice

Copyright[©] 2024 E.E.P.D. GmbH. ALL RIGHTS RESERVED!

E.E.P.D. GmbH copyrights this document. You may not reproduce, transmit, transcribe, store in a retrieval system, or translate into any language, in any form or by any means, or otherwise, any part of this publication without the express written permission of E.E.P.D. GmbH.

Trademark Acknowledgement

E.E.P.D.® and EMTRUST® are registered trademarks of E.E.P.D. GmbH. All rights reserved. All other mentioned trademarks are registered trademarks of their owners.



11/2024 Version 3.0



Disclaimer

This document is provided for the general information of the customer. It describes the general functionality of the board and is not considered as assured characteristics. The written declarations in this manual are not constituent part of any contract.

E.E.P.D. GmbH reserves the right to modify the information contained in this manual as necessary and the customer should ensure that he has the most recent revision of this document.

E.E.P.D. GmbH makes no warranty for the use of its products and bears no responsibility for any errors, which may appear in this document. The customer should be on notice that the field of personal computers is the subject of many patents held by different parties. Customer must ensure that they take appropriate action so that their use of the products does not infringe upon any patents. It is the policy of E.E.P.D. GmbH to respect the valid patent rights of third parties and not to infringe upon or assist others to infringe upon such rights.

E.E.P.D. GmbH assumes no responsibility for circuits, descriptions and tables within this document as far as patents or other rights of third parties are concerned.

Life Support Applications

E.E.P.D. GmbH products are not intended for being used as critical components in life support appliances, devices or systems in which the failing of an E.E.P.D. GmbH product could be expected to result in personal injury.

FCC and CE Disclaimer

E.E.P.D. GmbH gives no warranty at all that their products will meet the FCC and CE standards when used in combination with other third-party products or when used in any other way than specified.

Warranty

The warranty and/or guarantee conditions according to the current terms and conditions of E.E.P.D. GmbH apply.

Reshipment

If you return the EM[®] PRO system to E.E.P.D. GmbH please remove all connections and peripheral equipment.

Protect the unit with a suitable packaging, preferably use the original packaging.

Packaging

The $\mathsf{EM}^{\texttt{®}}$ PRO system is in a protective package to avoid damage during transport.

This protective package should be recycled in an environmentally friendly way after use.





Disposal of Device



At the end of the lifetime please dispose and/or recycle the components of the device accordingly.

Technical Support

For technical information about hardware and software please contact: support@eepd.de



EM TRUST

Table of Contents

General Notes1			
Revis	ion History6		
Symb	ols7		
Safety	/ Instructions8		
1	Quick-start guide9		
1.1	Switching on the device / Operation9		
2	System Information9		
2.1	Intended Use9		
2.2	Required Tools9		
2.3	Software9		
2.4	Options10		
2.5	Accessories10		
2.6	Scope of Delivery11		
2.7	System Dimensions11		
3	Technical Data13		
4	Interfaces14		
4.1	Connection Overview14		
4.2	Power Button15		
4.3	SFP+ Modules15		
4.4	2.5 Gigabit Ethernet Ports15		
4.5	Dual DisplayPort16		
4.6	USB-C ports16		

E.E.P.D. GmbH | Gewerbering 3 | 85258 Weichs

Device Reference Manual – P – Revision 3

4.7	Service Interface	16
4.8	Auxiliary Power Button HDD/SSD-LEDs	16
5	Opening the system	17
5.1	Inside the system	18
5.2	Installing M.2 modules	18
5.3	Installing SSD	19
6	AMI BIOS – V1000/R1000 variants	20
6.1	Entering Setup	20
6.2	Most Common Settings	20
6.3	Main Menu	21
6.4	Advanced Menu	22
6.5	Security Menu	38
6.6	Boot Menu	42
6.7	Save & Exit Menu	43
7	Insyde BIOS – R2000 variants	44
7.1	Entering Setup	44
7.2	Most Common Settings	44
7.4	Main Menu	45
7.5	Advanced Menu	46
7.6	AMD CBS	52
7.7	AMD PBS Option	58
7.8	Boot Menu	59
7.9	Power Menu	60



EM TRUST

EM[®] PRO rack

7.10	Exit Menu	61
7.11	Security Menu	62
Index of Figures64		
Index of Tables		
List of Abbreviations67		





Revision History

Date	Version	Changes
22.11.2024	3.0	First release





Symbols



The red danger sign warns you when a wrong or missing action dramatically endangers your life or health. The used components as well as the peripheral components could be destroyed.



The yellow ESD sign draws your attention that static sensitive parts of the component could be destroyed. Unpack shielded components only with ESD protections like an ESD wrist strap.



The orange warning sign warns you when a wrong or missing action could seriously harm your health or destroy the used components.



The information sign gives you more information and advice for optimal use of this product. For example, it helps you to purchase necessary or optional accessories.



The yellow caution sign warns you when a wrong or missing action could damage the component.





Safety Instructions

Safety of People



The product generates considerable heat. The housing transports this heat to the environment and thus becomes hot. Take care if you touch the housing as this may cause burns!



Please follow all safety instructions at the installation site. Make sure that no or only necessary cables are connected to the EM[®] PRO system during installation.



If access to the EM[®] PRO system interfaces is not available after installation, all necessary connections must be made before.

Device Safety



The EM[®] PRO system operates exclusively within the specified AC (optional DC) voltage range. Repair work should only be made by an authorized and certified specialty retailer or by the manufacturer's customer service. Do not open the device to avoid damage.

Modifications that have not been approved by the manufacturer void the warranty. Dust, dirt, moisture, and extreme temperatures may significantly impair proper operation.



The device may only be opened by a qualified person.

Cooling System



The EM[®] PRO system consists of a compact, robust metal housing with ventilation holes. It is equipped with an automated fan. To ensure sufficient heat dissipation, never cover the ventilation holes of the case. Do not place any objects onto the device.





Device Reference Manual – P – Revision 3

1 Quick-start guide



If connections are no longer accessible after system installation, connect all cables before final mounting.

Before switching on for the first time, we recommend connecting or inserting:

- Monitor + power cable
- USB keyboard and mouse
- Network cable (optional)

Other plug & play devices can be connected after power-up.

If you don't use a monitor or keyboard, you can access the console via a service interface (Mini USB-B, see chapter *4.7*).

1.1 Switching on the device / Operation

After all preparations have been made, the system is ready to be connected to the power supply.

Press the power button (*Fig. 16/Fig. 10*) to switch on the system. When the system is powered, the Power-LED will be on.

If an operating system is installed, it will load now. An operating system installation can be performed with all common installation media such as USB stick, USB DVD drive or remote network start. The BIOS boot order has to be adjusted accordingly. To enter the BIOS setup, press the [DEL] (AMI BIOS) or [ESC] (Insyde BIOS) key immediately after switching on.

Please refer to the operating system manual for switching off / shutting down.

2 System Information

2.1 Intended Use

The EM[®] PRO Rack is a personal computer to be used with Windows 11, Windows 10, Windows 10 IoT Enterprise or Ubuntu Linux 24.04 LTS. It has been designed for office, workshop and rack mounting environments.

2.2 Required Tools

For the installation of the EM[®] PRO rack the following standard tool is recommended:

Torx screwdriver T10

Other required tools are depending on the installation place and method.

2.3 Software

Supported operating systems are:

- AMD V1000/R1000 processors: Microsoft® Windows® 10 Microsoft® Windows® 10 IoT Enterprise Linux Ubuntu 24.04 LTS
- AMD R2000 processors series: Microsoft® Windows® 11 Microsoft® Windows® 10 Microsoft® Windows® 10 IoT Enterprise Linux Ubuntu 24.04 LTS





Device Reference Manual – P – Revision 3

2.4 Options

Options	Description	
	V1000/R1000: up to 2x 16 GB dual channel up to DDR4-2400 SO-DIMM memory	
	R2000: up to 2 x 32 GB (R2000) dual	
Memory*	DDR4-2667 (R2314 R2514) /	
	DDR4-3200 (R2544) SO-DIMM memory	
	depending on CPU variant	
	ECC support	
SSD*	64 GB – 2 TB	
	Windows® 11* ² , Windows® 10, Windows®	
Operating System*	10 IoT Enterprise* ² , Linux Ubuntu 24.04	
	LTS	
*factory-assembled on request		
*2only available with AMD Ryzen™ Embedded R2000 processor series		
Tab. 1: Options		

2.5 Accessories

For accessories, please contact our sales department.

Accessories	Description		
Mounting brackets	Rack mounting for 19-inch cabinets		
Rubber foots	For standalone purposes		
	MGPI	GPIO Adapter	
	MREL	Relay USB module	
Lin to 2 expansion slate	MADC	Analogue to digital converter	
Op to 3 expansion slots	M232/M485	RS-232/RS-485 Adapter	
Ior interface modules	METH	Gbit Ethernet Adapter	
	MCAN	CAN Adapter	
	MMC	Mini PCIe Adapter	
Display cable	Cable DP to DP, 2 m		
Display cable	Cable DP to HDMI, 2 m		
USB-C adapter cable	USB-C to USB-A adapter cable for HID-devices		
Power button	Power button with LED		
Tab. 2: Accessories			



*For further information about the interface modules, please visit our website <u>USB I/O modules for industrial use</u> or contact our sales department.





2.6 Scope of Delivery

Before you begin installation, please check that your shipment is complete and contains the items listed on the delivery note.



- 1 Manufacturer
- $\boldsymbol{2}-\text{Product name}$
- 3 Voltage input range and DC/AC type
- 4 Serial number with barcode
- ${\bf 5}-Certification\ information$

2.7 System Dimensions

all values [mm] approx.

Front view



Fig. 2: Dimensions front view

Rear view



Fig. 3: Dimensions rear view





Device Reference Manual – P – Revision 3

Side view



Fig. 4: Dimensions side view

Top view with mounting brackets



Fig. 5: Dimensions top view with optional mounting brackets



Fig. 6: Dimensions top view

Bottom view



Fig. 7: Dimension bottom view



E.E.P.D. GmbH | Gewerbering 3 | 85258 Weichs

Copyright © 2024 by E.E.P.D. GmbH. All rights reserved. | Rev. 3.0



3 Technical Data

- AMD V1000 processor series: V1605B / 4C / 8T / 2.0 GHz – 3.6 GHz / 15 W (12 – 25 W)
- AMD R1000 processor series OEM/ODM only, upon request
- AMD R2000 processor series: R2312 / 2C / 4T / 2.7 GHz – 3.5 GHz / 15 W (12 – 25 W) R2314 / 4C / 4T / 2.1 GHz - 3.5 GHz / 15 W (12 - 35 W) R2514 / 4C / 8T / 2.1 GHz - 3.7 GHz / 15 W (12 - 35 W) R2544 / 4C / 8T / 3.35 GHz – 3.7 GHz / 35 W
- Memory:

Up to 2x 16 GB (V1000/R1000) / 2 x 32 GB (R2000) dual channel up to DDR4-2400 (R2312) / DDR4-2667 (R2314, R2514) / DDR4-3200 (R2544) SO-DIMM memory depending on CPU variant, with ECC support

• Ethernet ports:

Up to 3 Intel i225-LM with IEEE1588:

1 Dual RJ45 at the front side,

support for 10/100/1000/2500 Mbit Ethernet (Base-T)

1 Single RJ45 at the front side,

support for 10/100/1000/2500 Mbit Ethernet (Base-T)

Support for Wake-on-LAN on port 3 only

AMD V1000 and R1000 processors series: Up to 2x 10 Gbit/s SFP+ modules

- WiFi/BT (ODM option only)
 - SSD (optional): 1x M.2 Key M (2280) NVMe/PCIe Gen3 x4, PCIe only 1x M.2 Key M (2280) NVMe/PCIe Gen3 x2, PCIe only 64 GB – 2 TB each slot
- E.E.P.D. GmbH | Gewerbering 3 | 85258 Weichs

Copyright © 2024 by E.E.P.D. GmbH. All rights reserved. | Rev. 3.0

USB ports:

2x USB-C 3.2 Gen2 (10Gb/s, OCP = 3000 mA) or USB-C Alt Mode (limited support) at front side 1x Mini USB-B (4-pin) service interface (console), UART-to-USB 2x USB 3.2 Gen2 (10Gb/s, OCP = 900 mA each) internal 1x USB 2.0 (480 Mb/s, OCP = 900 mA) internal

Display output:

Up to 2x DisplayPort++, v1.4, up to 3840 x 2160 @ 60 Hz Up to 2x USB-C Alt Mode, up to 3840 x 2160 @ 60 Hz (only as secondary monitor)

- Up to 2 controlled FAN (PWM + Tacho) and hardware monitoring
- Power and status LEDs
- Power supply: 100 V 240 V AC 50/60Hz, 120 W / 200 W depending on CPU
- Operating temperature: min. 0 °C to max. +50 °C ambient commercial grade
 Adequate cooling provided, depending on variant and cooling

system, CPU throttling may occur at higher ambient temperatures

- Storage temperature: -40 °C to +85 °C, non-condensing
- Relative humidity: 95% @ 40°C, non-condensing while stored, 89% while working
- Housing: Sturdy metal case
- Mounting: Rack, stand alone
- Dimensions approx.: 226 x 210 x 45 mm
- Weight: approx. 1680 g + options





4 Interfaces

4.1 Connection Overview

The EM[®] PRO rack is equipped with the following standard interfaces:

- 1 Power button
- 2 Up to 2x 10 Gbit/s SFP+ modules (V1000/R1000)
- 3 Up to 3x Ethernet, Port 3 supports WoL
- 4 2x DP++ connector
- 5 2x USB-C port
- 6 1x Mini USB-B (4-pin) service interface (console), UART-to-USB
- 7 Auxiliary power button (Fig. 16)
- $\boldsymbol{8}-\text{Power-LED}$
- 9 HDD/SSD-LED
- 10 Optional DC power in
- 11 Kensington lock
- 12 Slots for EM® USB-I/O-modules
- 13 Optional SMA connectors for WWAN, BT, WiFi antennas
- 14 Protective Earth (optional)
- 15-AC power in, 230 V IEC 60320 C6









Device Reference Manual – P – Revision 3

4.2 Power Button

The power button has an integrated LED that lights up a green ring around the power button when the system is turned on.

Press the power button (Fig. 10) once to switch the computer on and off. Press and hold the power button (>4 Sec.) to hard power off the system. Hard power off may result in data loss.



Fig. 10: power button with LED ring

4.3 SFP+ Modules



Fig. 11: SFP+ modules Detail

4.4 2.5 Gigabit Ethernet Ports

Standard pin assignment



Fig. 12: Ethernet Ports Detail

Yellow LED

Speed-LED is on during 2.5 or 1 Gbit transmission and switched off during 10/100 Mbit transmission.

Green LED

Link-/Activity-LED is permanently on to indicate an active connection on the Ethernet port. LED blinks during communication with the Ethernet network.





Device Reference Manual – P – Revision 3

4.5 Dual DisplayPort

Standard pin assignment



Fig. 13: Dual DisplayPort Detail

4.6 USB-C ports

Standard pin assignment



Fig. 14: USB-C Ports Detail

4.7 Service Interface

Service interface (console) with UART-to-USB interface. Data speed rate is configurable in the operating system. Standard USB pin assignment



Fig. 15: Mini USB-B Detail

4.8 Auxiliary Power Button | HDD/SSD-LEDs

Press the auxiliary power button (Fig. 16) once to switch the computer on and off. Press and hold the auxiliary power button (>4 Sec.) to hard power off the system. Hard power off may result in data loss.



Fig. 16: Auxiliary power button and HDD/SSD-LEDs position





5 Opening the system



EM TRUST

Incorrect installation of the RAM modules may void the warranty. The configuration of the RAM modules must be specified when ordering and will be installed by EEPD. Please contact our sales department for more information.

- 1. Turn off the system and disconnect from the electrical outlet.
- 2. Remove the 12 screws (M3X6) on the right, left and rear side of the system (4 screws each side, see Fig. 17, Fig. 18 and Fig. 19).
- 3. Lift the cover away from the system.
- 4. The assembly is carried out in reverse order.



Do not remove any screws other than those specified, otherwise the warranty will be void and you may damage the system.



Fig. 17: screws on the left side



Fig. 18: screws on the right side



Fig. 19: screws on the rear side





5.1 Inside the system

Top view



Fig. 20: top view of the system without cover

- 1 safety label
- **2** space for interface modules (see chapter 2.5)
- 3 slots for M.2 Key E / Key B modules (WiFi / BT)
- 4 power supply



Do not remove any screws, otherwise the warranty will be void and you may damage the system.

5.2 Installing M.2 modules

Insert the M.2 module into the corresponding slot at an angle. Press it down on the side that protrudes and secure it with the screw provided.



Fig. 21: M.2 Key B module assembly





5.3 Installing SSD

- 1. In order to open the SSD installation slot on the bottom, the top system case cover must be completely removed (see chapter 5).
- 2. Then the long screw (M3X30) near the fan, marked with a lock symbol, must be removed.
- 3. Now remove the screw on the SSD installation slot and carefully open it. Please use the installed flat head screws to mount the SSDs.
- 4. The assembly is carried out in the reverse order.



Fig. 22: opening of SSD installation slot



Fig. 23: M3X30 screw

E.E.P.D. GmbH | Gewerbering 3 | 85258 Weichs

Copyright © 2024 by E.E.P.D. GmbH. All rights reserved. | Rev. 3.0



Note:

Key M 1 = M.2 (2280) NVMe/PCIe Gen3 **x4**, PCIe only Key M 2 = M.2 (2280) NVMe/PCIe Gen3 **x2**, PCIe only



Fig. 24: SSD slots





6 AMI BIOS – V1000/R1000 variants

The following description shows a snapshot of the BIOS setup. Later BIOS updates may change the content slightly.

Asterisk (*) indicates default setting.

6.1 Entering Setup

Power on the board and press and hold [DEL] immediately to enter Setup.

6.2 Most Common Settings

- 1. Firmware / BIOS Version: Main (chapter *6.3*)
- 2. Boot / PXE Boot:
 Boot Priorities (chapter 6.6)
 Advanced → Network Stack Configuration (chapter 6.4.7)
- 3. TDP, fan control, boost mode: TDP setting: Advanced → AMD CBS → NBIO Common Options → System Configuration (chapter 6.4.9.2)
 - Fan control:

Advanced \rightarrow AMD CBS \rightarrow NBIO Common Options \rightarrow Fan Control (chapter 6.4.9.2.4)

Boost mode:

Advanced \rightarrow AMD CBS \rightarrow Zen Common Options \rightarrow Core Performance Boost (chapter *6.4.9.1*)

E.E.P.D. GmbH | Gewerbering 3 | 85258 Weichs

Copyright © 2024 by E.E.P.D. GmbH. All rights reserved. | Rev. 3.0

Device Reference Manual – P – Revision 3

4. Change shared graphics memory

Advanced \rightarrow AMD CBS \rightarrow NBIO Common Options \rightarrow GFX Configurations \rightarrow UMA Frame Buffer Size (chapter *6.4.9.2.1*)

5. USB power

Advanced \rightarrow AMD CBS \rightarrow FCH Common Options \rightarrow USB Configuration Options (chapter 6.4.9.3.1)





6.3 Main Menu

Aptio Setup Utility – Copyright © 2024 American Megatrends, Inc. Main Advanced Security Boot Save & Exit				
Board Information		Set the Date. Use Tab to		
Board	GS2MB	switch between Date elements.		
Board Version	Rev 3	Default Ranges:		
		Year: 1998-9999		
uC Information		Months: 1-12		
uC Firmware Version	0.4.5	Days: Dependent on month		
		Range of Years may vary.		
BIOS Information				
BIOS Vendor	AMI / E.E.P.D. GmbH			
BIOS Version	GS2xx 1.7			
Build Date and Time	03/17/2024 11:59:54			
Memory Information				
Total Memory	8192 MB (DDR4)	→ -: Select Screen		
		†↓: Select Item		
	[Fri 09/06/2024]	Enter: Select		
System Time	[12:04:39]	+/-: Change Opt.		
		F1: General Help		
		F2: Previous Values		
		F3: Optimized Defaults		
		F4: Save & Exit		
		ESC: Exit		

BIOS Settings	Options	Description
System Date		Set the Date. Use Tab to switch between
		Date elements.
		Default Ranges:
		Year: 1998-9999
		Months: 1-12
		Days: Dependent on month
		Range of Years may vary.
System Time		Set the Time. Use Tab to switch between
		Time elements.

Tab. 3: Main Menu – AMI BIOS

Fig. 25: Main Menu – AMI BIOS





6.4 Advanced Menu

Aptio Setup Utility – Copyright © 2024 Ame	erican Megatrends, Inc.	BIOS S	ettings	Options	Description
Trusted Computing	Trusted Computed Settings	Trusted Co	omputing	See submenu	Trusted Computing Settings
► TPM Configuration		TPM Conf	iguration	See submenu	AMD fTPM Settings
 GS2x Advanced Options CPU Configuration AMI Graphic Output Protocol Policy 		GS2x Ad Optic	lvanced ons	See submenu	Show more setup options and debug information
 USB Configuration Network Stack Configuration NVMe Configuration 		CPU Conf	iguration	See submenu	CPU Configuration Parameters
 AMD CBS AMD PBS Intel® Ethernet Controller (3) 1225-LM – 00:E0:33: 		AMI Graph Protocol	ic Output Policy	See submenu	In Dual Screen Operation, select the pre-OS boot graphic output Interface.
 Intel® Ethernet Controller (3) 1225-LM – 00:E0:33: Intel® Ethernet Controller (3) 1225-LM – 00:E0:33: 	E0:33: E0:33: ↑↓: Select Screen ↑↓: Select Item Enter: Select +/- Change Opt	USB Conf	iguration	See submenu	USB Configuration Parameters
		Network Configu	Stack Iration	See submenu	Network Stack Settings
	F1: General Help F2: Previous Values	NVMe Con	figuration	See submenu	NVMe Device Options Settings
	F3: Optimized Defaults	AMD	CBS	See submenu	AMD CBS Setup Page
	ESC: Exit	AMD	PBS	See submenu	AMD PBS Setup Page
		Intel® Et Controller (3	thernet 3) I225-LM	See submenu	Configure Gigabit Ethernet device parameters
Version 2.20.1274. Copyright © 2024 Ameri	can Megatrends, Inc.	Tab. 4: Advanced	Menu – AMI BI	ÖS	•

Fig. 26: Advanced Menu – AMI BIOS





6.4.1 Trusted Computing

Aptio Setup Utility Advanced	y – Copyright © 2024 Americ	can Megatrends, Inc.
TPM 2.0 Device Found Firmware Version:	7.85	Enables or Disables BIOS support for security device. Q.S. will not show Security
Security Device Support Active PCR banks Available PCR banks	[Enable] SHA-1, SHA256 SHA-1, SHA256	Device. TCG EFI protocol and INT1A interface will not be available.
SHA-1 PCR Bank SHA256 PCR Bank	[Enabled] [Enabled]	
Pending operation Platform Hierarchy Storage Hierarchy Endorsement Hierarchy TPM 2.0 UEFI Spec Version Physical Presence Spec Version TPM 2.0 InterfaceType Device Select	[None] [Enabled] [Enabled] [TCG_2] [1.3] [TIS] [Auto]	→ -: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit
Version 2.20.1274.	Copyright © 2024 American	Megatrends, Inc.

Fig. 27: Trusted Computing – AMI BIOS

BIOS Settings	Options	Description
Security Device Support	<enabled>* <disabled></disabled></enabled>	Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.
SHA-1 PCR Bank	<enabled>* <disabled></disabled></enabled>	Enable or Disable SHA-1 PCR Bank.

E.E.P.D. GmbH | Gewerbering 3 | 85258 Weichs

Device Reference Manual – P – Revision 3

SHA256 PCR Bank	<enabled>* <disabled></disabled></enabled>	Enable or Disable SHA256 PCR Bank
Pending operation	<none>* <tpm clear=""></tpm></none>	Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change state of Security Device.
Platform Hierarchy	<enabled>* <disabled></disabled></enabled>	Enable or Disable Platform Hierarchy
Storage Hierarchy	<enabled>* <disabled></disabled></enabled>	Enable or Disable Storage Hierarchy
Endorsement Hierarchy	<enabled>* <disabled></disabled></enabled>	Enable or Disable Endorsement Hierarchy
TPM 2.0 UEFI Spec Version	<tcg_1_2> <tcg_2>*</tcg_2></tcg_1_2>	Select the TCG2 Spec Version Support. TCG_1_2: the Compatible mode for Win8/Win10 TCG_2: Support new TCG2 protocol and event format for Win10 or later
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
Device Select	<tpm 1.2=""> <tpm 2.0=""> <auto>*</auto></tpm></tpm>	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 the default set to TPM 2.0 devices if not found, TPM 1.2 devices will be enumerated

Tab. 5: Trusted Computing – AMI BIOS





6.4.2 TPM Configuration

Aptio Setup Utility – Copyright © 2024 American Megatrends, Inc. Advanced		
TPM Switch Erase fTPM NV for factory reset	[discrete TPM] [Enabled]	AMD CPU fTPM
		 →-: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

BIOS Settings	Options	Description
TPM Switch	<amd firmware="" tpm=""> <disable tpm=""> <discrete tpm="">*</discrete></disable></amd>	AMD CPU fTPM
Erase fTPM NV for factory reset	<enabled>* <disabled></disabled></enabled>	When New CPU is installed, select "Enabled" to reset fTPM, if you have BitLocker or encryption- enabled system, the system will not boot without a recovery key. Select "Disabled" to keep previous fTPM record and continue system boot, fTPM will NOT be enabled with new CPU unless fTPM is reset (reinitialized)

Tab. 6: TPM Configuration – AMI BIOS

Fig. 28: TPM Configuration – AMI BIOS





6.4.3 GS2x Advanced Options

Aptio Setu Advanced	p Utility – Copyright © 2024 A	merican Megatrends, Inc.
Watchdog Timeout KL15 Support	<mark>0</mark> [Disabled]	Seconds before watchdog times out. Set to 0 to disable watchdog
WoL Power LED	[Enabled] [Enabled]	Values between 1 and 30 seconds are set to 30. Range 30-240 seconds
WWAN Power	[Enabled]	
BT Radio Operation	[Enabled]	
		→ =: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

BIOS Settings	Options	Description
Watchdog Timeout		Seconds before watchdog times out. Set to 0 to disable watchdog. Values between 1 and 30 seconds are set to 30. Range 30-240 seconds.
KL15 Support	<enabled> <disabled>*</disabled></enabled>	Enable/Disable KL15 support
WoL	<enabled>* <disabled></disabled></enabled>	Enable/Disable the WoL
Power LED	<enabled>* <disabled></disabled></enabled>	Power LED
WWAN Power	<enabled>* <disabled></disabled></enabled>	Enable/Disable the WWAN PWR
WLAN Radio Operation	<enabled>*</enabled>	Enable/Disable the WLAN
(variant specific)	<disabled></disabled>	radio operation
BT Radio Operation	<enabled>* <disabled></disabled></enabled>	Enable/Disable the BT radio operation

Tab. 7: GS2x Advanced Options – AMI BIOS

Fig. 29: GS2x Advanced Options – AMI BIOS





Device Reference Manual – P – Revision 3

6.4.4 CPU Configuration

Aptio Setup Utility Advanced	– Copyright © 2024 American M	legatrends, Inc.
CPU Configuration Module Version: PiccasoCpu 10 AGESA Version: PiccasoPI 100A		View Memory Information related to Node 0
PSS Support PPC Adjustment NX Mode SVM Mode Node 0 Information	[Enabled] [PState 0] [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 2.20.1274. (Copyright © 2024 American Mec	atrends. Inc.

Fig. 30: CPU Configuration – AMI BIOS

BIOS Settings	Options	Description
Node 0 Information	See submenu	View Memory Information related to Node 0

Tab. 8: CPU Configuration – AMI BIOS

6.4.4.1 Node 0 Information

Aptio Setup Utility – Copyright © 2024 American Megatrends, Inc. Advanced		
Socket0: AMD Ryzen Embedded V1605B with Radeon Vega Gfx 4 Core(s) Running @ 2034 MHz 1218 mV Processor Family: 17h Processor Model: 10h-1Fh CPUID: 00810F10 Max Speed:2000 MHZ Min Speed:1600 MHZ Microcode Patch Level: 8101016 Cache per core L1 Instruction Cache: 64 KB/4-way L1 Data Cache: 32 KB/8-way L2 Cache: 512 KB/8-way Total L3 Cache per Socket: 4 MB/16-way	→ -: Select Screen 1↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2 20 1274, Copyright © 2024 American Me	astronde. Inc	

Fig. 31: Node 0 Information – AMI BIOS





Device Reference Manual – P – Revision 3

6.4.5 AMI Graphic Output Protocol Policy

Aptio Setup Utility – Copyright © 2024 American Megatrends, Inc. Advanced		
RAVEN AMD GOP x64 Release Driver Rev.2.8.0.0.0.Jul 26 2019.11:24:53 Output Select [DFP1_DP]	Select pre-OS graphic output interface when using dual screen	
	→: Select Screen 1: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit	

Fig. 32: AMI Graphic Output Protocol Policy – AMI BIOS

BIOS Settings	Options	Description
Output Select	<dfp1_dp>*</dfp1_dp>	Select pre-OS graphic output interface when using dual screen

Tab. 9: AMI Graphic Output Protocol Policy - AMI BIOS





6.4.6 USB Configuration

Aptio Setup Utility – Copyright © 2023 American Megatrends, Inc. Advanced		
USB Configuration		Enables Legacy USB support. AUTO option disables legacy
USB Module Version	24	support if no USB devices are Connected, DISABLE option will
USB Controllers:		keep USB devices available
3 XHCIs USB Devices:		only for EFI applications.
1 Keyboard, 1 Hub		
Legacy USB Support		
XHCI Hand-off	[Enabled]	
USB Mass Storage Driver Support	[Enabled]	
Port 00/04 Emulation		: Select Screen
USB hardware delays and time-out	s:	tu: Select Item
USB transfer time-out	[20 sec]	Enter: Select
Device reset time-out	[20 sec]	+/-: Change Opt.
Device power-up delay	[Auto]	F1: General Help
		F2: Previous Values
		F3: Optimized Defaults
		F4. Save & EXIL FSC: Evit
		LOO. EXIL
Version 2.20.1274. Copyright © 2023 American Megatrends, Inc.		

Fig. 33: USB Configuration – AMI BIOS

BIOS Settings	Options	Description
Legacy USB Support	<enabled>* <disabled> <auto></auto></disabled></enabled>	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.

E.E.P.D. GmbH | Gewerbering 3 | 85258 Weichs

Device Reference Manual – P – Revision 3

XHCI Hand-off	<enabled>* <disabled></disabled></enabled>	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support	<enabled>* <disabled></disabled></enabled>	Enable/Disable USB Mass Storage Driver Support
Port 60/64 Emulation	<enabled>* <disabled></disabled></enabled>	Enables I/O port 60h/64h emulation support. This should be enabled for the complete USB keyboard legacy support for non-USB aware OSes.
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.
Device power-up delay	<auto>* <manual></manual></auto>	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.

Tab. 10: USB Configuration – AMI BIOS



Copyright © 2024 by E.E.P.D. GmbH. All rights reserved. | Rev. 3.0



6.4.7 Network Stack Configuration

Aptio Setup Utility – Copyright © 2024 American Megatrends, Inc. Advanced		
Network Stack	[Disabled]	Enable/Disable UEFI Network Stack
IPv4 PXE Support IPv4 HTTP Support IPv6 PXE Support IPv6 HTTP Support PXE boot wait time Media detect count	[Enabled] [Disabled] [Disabled] [Disabled] 0 1	
		 →←: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.2	0.1274. Copyright © 2024 Ame	erican Megatrends, Inc.

Fig. 34: Network Stack Configuration – AMI BIOS

BIOS Settings	Options	Description
Network Stack	<enable> <disable>*</disable></enable>	Enable/Disable UEFI Network Stack
IPv4 PXE Support	<enable>* <disable></disable></enable>	Enable/Disable IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available
IPv4 HTTP Support	<enable> <disable>*</disable></enable>	Enable/Disable IPv4 HTTP boot support. If disabled, IPv4 HTTP boot support will not be available
IPv6 PXE Support	<enable> <disable>*</disable></enable>	Enable/Disable IPv6 PXE boot support. If disabled, IPv6 PXE boot support will not be available
IPv6 HTTP Support	<enable> <disable>*</disable></enable>	Enable/Disable IPv6 HTTP boot support. If disabled, IPv6 HTTP boot support will not be available
PXE boot wait time	<0 - 5>	Wait seconds to press ESC key to abort the PXE boot. Use either +/- or numeric key to set the value
Media detect count	<1 - 50>	Number of times the presence of media will be checked. Use either +/- or numeric key to set the value.

Tab. 11: Network Stack Configuration – AMI BIOS





Device Reference Manual – P – Revision 3

6.4.8 NVMe Configuration

This function shows the connected NVMe devices.

ID CBS Zen C	Common Optio
n Common Options BIO Common Options CH Common Options The Second	Select Screen Select Item r: Select Change Opt. Seneral Help Previous Value: Optimized Defa Save & Exit
	Common Options IO Common Options H Common Options T1: S Ente +/-: (F1: F3: (F3: (F4: 1) ESC

Fig. 35: NVMe Configuration – AMI BIOS

Fig. 36: AMD CBS – AMI BIOS

6.4.9 AMD CBS

BIOS Settings	Options	Description
Zen Common Options	See submenu	Zen Common Options
NBIO Common Options	See submenu	NBIO Common Options
FCH Common Options	See submenu	FCH Common Options
Tab 12 AMD CDS AMI DIOS		

Tab. 12: AMD CBS – AMI BIOS





Device Reference Manual – P – Revision 3

6.4.9.1 Zen Common Options

Aptio Setup Utility – Copyright © 2024 American Megatrends, Inc. Advanced		
Zen Common Options		Disable CPB
Core Performance Boost		
		→: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.20.4	274 .0	marian Mantania Jac

Fig. 37: Zen Common Options – AMI BIOS

BIOS Settings	Options	Description
Core Performance Boost	<disabled>* <auto></auto></disabled>	This allows the processor to dynamically adjust and control the processor operating frequency to enable performance improvement, provided the processor has sufficient power and is within temperature specifications.

Tab. 13: Zen Common Options – AMI BIOS

6.4.9.2 NBIO Common Options

Aptio Setup Utility – Copyright © 2024 American Megatrends, Inc. Advanced		
NBIO Common Options GFX Configuration NB Configuration PCIe Configuration 		GFX Configuration
System Configuration ► Fan Control	[Auto]	
		→: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Fig. 38: NBIO Common Options – AMI BIOS

BIOS Settings	Options	Description
GFX Configuration	See submenu	GFX Configuration options
NB Configuration	See submenu	NB Configuration options
PCIe Configuration	See submenu	PCIe Configuration options
System Configuration	<minimum> <nominal> <maximum> <auto>*</auto></maximum></nominal></minimum>	Set the TDP settings with minimum, nominal and maximum TPD values for each variant. Auto sets default value
Fan Control	See submenu	Fan Control options

Tab. 14: NBIO Common Options – AMI BIOS





6.4.9.2.1 GFX Configuration

Aptio Setup Utility – Copyright © 2024 American Megatrends, Inc. Advanced		
GFX Configuration		Set UMA FB size
UMA Frame buffer Size UMA Above 4G NB Azalia	[2G] [Auto] [Auto]	
		→ Select Screen 1↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
		I

BIOS Settings	Options	Description
UMA Frame buffer Size	<auto>*, <64M>, <128M>, <256M>, <384M>, <512M>, <80M>, <96M>, <768M>, <1G>, <2G>, <3G>, <4G>, <6G>, <8G>, <16G></auto>	Set UMA Frame Buffer Size. This allows the system to manage the amount of shared memory for graphics. For systems equipped with 8GB of RAM or more, set the UMA buffer size to 1GB or 2GB.
UMA Above 4G	<disabled> <enabled> <auto>*</auto></enabled></disabled>	If requested UMA frame buffer size can't be fit under 4GB or the system has enough available memory above 4GB, this option may be set to TRUE to allow UMA frame buffer size to be allocated successfully.
NB Azalia	<disabled> <enabled> <auto>*</auto></enabled></disabled>	Enable Integrate HD Audio controller

Tab. 15: GFX Configuration – AMI BIOS

Version 2.20.1274. Copyright © 2024 American Megatrends, Inc

Fig. 39: GFX Configuration - AMI BIOS





EM[®] PRO rack

Device Reference Manual – P – Revision 3

6.4.9.2.2 NB Configuration

Aptio Setup Utility – Copyright © 2024 American Megatrends, Inc. Advanced		
NB Configuration		Enable/Disable IOMMU
		→—: Select Screen †↓: Select Item
		+/-: Change Opt.
		F1: General Help
		F3: Optimized Defaults
		F4: Save & Exit
		LOC. EAR
Version 2.2	20.1274. Copyright © 2024 Ame	rican Megatrends, Inc.

Fig. 40: NB Configuration – AMI BIOS

BIOS Settings	Options	Description
IOMMU	<disabled>* <enabled></enabled></disabled>	Enable/Disable IOMMU

Tab. 16: NB Configuration – AMI BIOS

	6.4.9.2.3	PCIe Configuration
--	-----------	--------------------

Aptio Setup Utility – Copyright © 2024 An Advanced	nerican Megatrends, Inc.
PCIe Configuration	No help string
	→: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Fig. 41: PCIe Configuration – AMI BIOS

BIOS Settings	Options	Description
PSPP Policy	<disabled> <performance> <balanced> <power saving=""> <auto>*</auto></power></balanced></performance></disabled>	PSPP Policy. This item allows you to set PCIe speed power policy

Tab. 17: PCIe Configuration – AMI BIOS





Device Reference Manual – P – Revision 3

6.4.9.2.4 Fan Control

Aptio S Advanced	etup Utility – Copyright © 2024 Americ	an Megatrends, Inc.
Fan Control Fan Control	[Optimized Cooling]	Optimized Cooling = Use the Default fan controller settings Silent Mode = Use the Silent Fan controller settings Max Cooling = Use the Max Cooling fan controller settings
		→: Select Screen †↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.20.1274. Copyright © 2024 American Megatrends, Inc.		

Fig. 42: Fan Control – AMI BIOS

BIOS Settings	Options	Description
Fan Control	<optimized cooling="">* <silent mode=""> <max cooling=""></max></silent></optimized>	Optimized Cooling = Use the default fan controller settings Silent Mode = Use the Silent fan controller settings Max Cooling = Use the Max Cooling fan controller settings

Tab. 18: Fan Control – AMI BIOS

E.E.P.D. GmbH | Gewerbering 3 | 85258 Weichs

6.4.9.3 FCH Common Options

Aptio Setup Utility – Copyright © 2 Advanced	2024 American Megatrends, Inc.	
FCH Common Options > USB Configuration Options > Ac Power Loss Options > Uart Configuration Options	USB Configuration Options	
	→: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.20.1274. Copyright © 2024 American Megatrends, Inc.		

Fig. 43: FCH Common Options – AMI BIOS

BIOS Settings	Options	Description
USB Configuration Options	See submenu	USB Configuration Options
Ac Power Loss Options	See submenu	Ac Power Loss Options
Uart Configuration Options	See submenu	Uart Configuration Options

Tab. 19: FCH Common Options - AMI BIOS





6.4.9.3.1 USB Configuration Options

Aptio Setup Utili Advanced	ty — Copyright © 2024 Ar	merican Megatrends, Inc.
USB Configuration Options USBSS 1 Rear USBSS 2 Rear USBSS Power Off in S5	[Enabled] [Enabled] [Disabled]	Enable/Disable the USB Connector VCC
		→ →-: Select Screen †↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Version 2.20.1274. Copyright © 2024 American Megatrends, Inc.

Fig. 44: USB Configuration Options – AMI BIOS

BIOS Settings	Options	Description
USBSS 1 Rear	<disabled> <enabled>*</enabled></disabled>	Enable/Disable the USB connector VCC
USBSS 2 Rear	<disabled> <enabled>*</enabled></disabled>	
USBSS Power Off in S5	<disabled>* <enabled></enabled></disabled>	Enable/Disable the USB connector VCC only in S5 (System Power Off)!

Tab. 20: USB Configuration Options – AMI BIOS

Device Reference Manual – P – Revision 3

6.4.9.3.2 Ac Power Loss Options

Ac Power Loss Options	Select Ac Loss Control Method
	→ : Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

Fig. 45: Ac Power Loss Options – AMI BIOS

BIOS Settings	Options	Description
Ac Loss Control	<always off=""> <always on=""> <previous>*</previous></always></always>	This function allows you to set the power status after a power failure. Select [Always Off] to keep the system power off after a power failure. Select [Always On] to turn the system power after a power failure. Select [Previous] to allow the System to resume its last power state before a power failure.

Tab. 21: Ac Power Loss Options – AMI BIOS





6.4.9.3.3 Uart Configuration Options

Aptio Setup Uti Advanced	lity – Copyright © 2024 Ame	rican Megatrends, Inc.
Uart Configuration Options Uart 0 Enable Uart 0 Legacy Options Uart 1 Enable Uart 1 Legacy Options	[Enabled] [COM1 0x3F8] [Enabled] [COM2 0x2F8]	Enable/Disable UART 0 device
		 →→-: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

BIOS Settings	Options	Description
Uart 0 Enable	<disabled> <enabled>* <auto></auto></enabled></disabled>	Enable/Disable UART 0 device
Uart 0 Legacy Options	<disabled> <com1 0x3f8="">* <com2 0x2f8=""> <com3 0x3e8=""> <com4 0x2e8=""> <auto></auto></com4></com3></com2></com1></disabled>	This function specifies the base I/O port address of a user-specified serial port. Select Auto to allow the BIOS to automatically assign the base I/O address.
Uart 1 Enable	<disabled> <enabled>* <auto></auto></enabled></disabled>	Enable/Disable UART 1 device
Uart 1 Legacy Options	<disabled> <com1 0x3f8=""> <com2 0x2f8="">* <com3 0x3e8=""> <com4 0x2e8=""> <auto></auto></com4></com3></com2></com1></disabled>	This function specifies the base I/O port address of a user-specified serial port. Select Auto to allow the BIOS to automatically assign the base I/O address.

Tab. 22: Uart Configuration Options - AMI BIOS

Fig. 46: Uart Configuration Options – AMI BIOS





Device Reference Manual – P – Revision 3

6.4.10 AMD PBS

Aptio Setup Utility – Copyright © 2024 American Megatrends, Inc. Advanced			
AMD Firmware Version		4	
AGESA Version	EmbeddedPI-FP5_1.2.0.4RC 4		
PSP Bootloader Version	0.8.0.74		
PSP SecureOS Version	0.8.0.74		
ABL Version	20061500	н	
APCB Version	0029		
AP0B Version	0013		
Ucode Patch Version	8101016	н	
SMU FW Version	0.30.92.0		
SMU RV2 FW Version	0.37.39.0		→: Select Screen
DXIO FW Version	001E.0121	1	t: Select Item
		E	Enter: Select
MP2 I2C FW Version	1.0.24.3	•	⊦/-: Change Opt.
MP2 I2C RV2 FW Version	1.2.2.3	F	F1: General Help
XHCLEW Version	FF FF FF FF		-2. Previous values -3: Optimized Defaults
VBIOS FW Version	113-RAVEN-116	Ē	-4: Save & Exit
GOP Driver Version	AMD GOP X64 Release	E	ESC: Exit
	Driver		
	Rev.2.8.0.0.0.Jul 26		
	2019.11:24:53	•	

Fig. 47: AMD PBS – AMI BIOS





6.5 Security Menu

Aptio Setu Main Advanced Security	ip Utility – Copyright © 2024 A Boot Save & Exit	merican Megatrends, Inc.
Password Description		Set Administrator Password
If ONLY the Administrator's Then this only limits access only asked for when enterin If ONLY the User's passwor is a power on password and boot or enter Setup. In Setu have Administrator rights. The password length must in the following range: Minimum length Maximum length	password is set, to Setup and is g Setup. rd is set, then this d must be entered to p the User will be	
maximum tengui	20	→: Select Screen
Administrator Password		11: Select Item
User Password		Enter: Select
STIBP Status	[Disabled]	+/-: Change Opt. F1: General Help F2: Previous Values
► Secure Boot		F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.2	0.1274. Copyright © 2024 Am	erican Megatrends, Inc.

BIOS Settings	Options	Description
Administrator Password		Set Administrator Password
User Password		Set User Password
STIBP Status	<disabled>* <enabled></enabled></disabled>	Single Thread Indirect Branch Predictor (STIBP) is a method to mitigate indirect branch target injection attacks on AMD products.
Secure Boot	See submenu	Secure Boot configuration

Tab. 23: Security Menu – AMI BIOS

Fig. 48: Security Menu – AMI BIOS





6.5.1 Secure Boot

Aptio Setur Security) Utility – Copyright © 2024 A	merican Megatrends, Inc.
System Mode	Setup	Secure Boot feature is Active If Secure Boot is Enabled.
Secure Boot		Platform Key(PK) is enrolled
	Not Active	and the System is in User mode. The mode change requires
Secure Boot Mode Restore Factory Keys 	[Custom]	platform reset
Reset To Setup Mode		
 Key Management 		
		→: Select Screen ↑↓: Select Item
		Enter: Select
		F1: General Help
		F2: Previous Values
		F4: Save & Exit
		ESC: Exit
Version 2.20	1274 Copyright @ 2024 Am	arican Magatrands. Inc

BIOS Settings	Options	Description
Secure Boot	<disabled>* <enabled></enabled></disabled>	Secure Boot feature is Active if Secure Boot is Enabled, Platform Key (PK) is enrolled and the System is in User mode. The mode change requires platform reset.
Secure Boot Mode	<standard> <custom>*</custom></standard>	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		Force System to User Mode. Install factory default Secure Boot key databases.
Key Management	See submenu	Enables expert users to modify Secure Boot Policy variables without full authentication.

Tab. 24: Secure Boot – AMI BIOS

Fig. 49: Secure Boot – AMI BIOS





6.5.1.1 Key Management

Aptio Setup L Security	Jtility – Copyright © 2024 Ameri	ican Megatrends, Inc.
Vendor Keys	Valid	Install factory default Secure Boot keys after the platform
 Factory Key Provision Restore Factory Keys Reset To Setup Mode Export Secure Boot variables Enroll Efi Image Device Guard Ready Remove 'UEFI CA' from DB Restore DB defaults 		reset and while the System is in Setup mode
Secure Boot variable Si Platform Key(PK) Key Exchange Keys Authorized Signatures Forbidden Signatures Authorized TimeStamps OsRecovery Signatures	ize Keys Key Source 0 0 No Keys 0 0 No Keys	→ -: Select Screen 1↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.20.12	274. Copyright © 2024 America	n Megatrends, Inc.
Fig. 50: Key Management – A	MI BIOS	

BIOS Settings	Options	Description
Factory Key Provision	<disabled>* <enabled></enabled></disabled>	Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode.
Restore Factory Keys		Force System to User Mode. Install factory default Secure Boot key databases.

E.E.P.D. GmbH | Gewerbering 3 | 85258 Weichs

Device Reference Manual – P – Revision 3

Enroll Efi Image	Allow the image to run in Secure Boot mode. Enroll SHA256 Hash certificate of a PE image into Authorized Signature Database (db).
Restore DB defaults	Restore DB variable to factory defaults.
Platform Key (PK)	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_RSA2048 (bin) d) EFI_CERT_SHAXXX 2. Authenticated UEFI Variable 3. EFI PE/COFF Image (SHA256) Key Source: Factory, External, Mixed
Key Exchange Keys	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_RSA2048 (bin) d) EFI_CERT_SHAXXX 2. Authenticated UEFI Variable 3. EFI PE/COFF Image (SHA256) Key Source: Factory, External, Mixed
Authorized Signatures	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 2. Authenticated UEFI Variable





	3. EFI PE/COFF Image (SHA256) Key Source: Factory, External, Mixed
Forbidden Signatures	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 2. Authenticated UEFI Variable 3. EFI PE/COFF Image (SHA256) Key Source: Factory, External, Mixed
Authorized TimeStamps	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 2. Authenticated UEFI Variable 3. EFI PE/COFF Image (SHA256) Key Source: Factory, External, Mixed
OsRecovery Signatures	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 2. Authenticated UEFI Variable 3. EFI PE/COFF Image (SHA256) Key Source: Factory, External, Mixed

Tab. 25: Key Management – AMI BIOS

E.E.P.D. GmbH | Gewerbering 3 | 85258 Weichs

Copyright © 2024 by E.E.P.D. GmbH. All rights reserved. | Rev. 3.0



6.6 Boot Menu

Aptio Setup Main Advanced Security	Utility – Copyright © 2024 A Boot Save & Exit	merican Megatrends, Inc.
Boot Configuration Setup Prompt Timeout Bootup NumLock State Quiet Boot	1 [On] [Enabled]	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.
Boot Option Priorities Fast Boot Driver Option Priorities	[Disabled]	
		→ ←: Select Screen 1↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2 20 1	274 Copyright © 2024 Am	erican Megatrends, Inc.

Fig. 51: Boot Menu – AMI BIOS

BIOS Settings	Options	Description
Setup Prompt Timeout		Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.
Bootup NumLock State	<on>* <off></off></on>	Select the keyboard NumLock state
Quiet Boot	<disabled> <enabled>*</enabled></disabled>	Enables or disables Quiet Boot option.
Fast Boot	<disabled>* <enabled></enabled></disabled>	Enables or disables boot with initialization of a minimal set of devices required to launch active boot option. Has no effect or BBS boot options.

Tab. 26: Boot Menu – AMI BIOS





6.7 Save & Exit Menu

Aptio Setup Utility – Copyright © 2024 / Main Advanced Security Boot Save & Exit	American Megatrends, Inc.
Save Options	Exit system setup after saving
Save Changes and Exit	the changes.
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	→ ←: Select Screen
	tu: Select Item
Boot Override	Enter: Select
Launch EFI Shell from filesystem device	+/-: Change Opt.
	F1: General Help
	F2: Previous Values
	F3: Optimized Defaults
	F4: Save & Exit
	ESC: EXIL
Version 2.20.1274. Copyright © 2024 Am	nerican Megatrends, Inc.

Fig. 52: Save & Exit Menu – AMI BIOS

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

Tab. 27: Save & Exit Menu – AMI BIOS





7 Insyde BIOS – R2000 variants

The following description shows a snapshot of the BIOS setup. Later BIOS updates may change the content slightly.

Asterisk (*) indicates default setting.

7.1 Entering Setup

Power on the board and press and hold [ESC] immediately to enter Setup.

7.2 Most Common Settings

- 1. Firmware / BIOS Version: Main (chapter 7.4)
- Boot / PXE Boot: Boot → Network Stack Configuration (chapter 7.8)
- TDP, fan control, boost mode: TDP setting: AMD CBS → NBIO Common Options → System Configuration (chapter 7.6.2)

Fan control: AMD CBS \rightarrow NBIO Common Options \rightarrow Fan Control (chapter 7.6.2.2) Boost mode: Advanced \rightarrow AMD CBS \rightarrow Zen Common Options \rightarrow Core

Performance Boost (chapter 7.6.1)

- Change shared graphics memory AMD CBS → NBIO Common Options → GFX Configurations → UMA Frame Buffer Size (chapter 7.6.2.1)
- E.E.P.D. GmbH | Gewerbering 3 | 85258 Weichs

Device Reference Manual – P – Revision 3

5. USB power

Advanced \rightarrow USB Configuration Options \rightarrow Enable/Disable – VCC of USB Jacks (chapter 7.5.4.1)





7.4 Main Menu



Fig.	53:	Main	Menu –	InsydeH2O
------	-----	------	--------	-----------

BIOS Settings	Options	Description
Language	<english>*</english>	
System Time	No options	Set the time. Use tab to switch between time elements. Valid range is from 0 to 23, 0 to 59, 0 to 59. INCREASE/REDUCE: +/-
System Date	No options	Set the date. Use tab to switch between date elements. Valid range is from 1 to 12, 1 to 31, 2000 to 2099. (Error checking will be done against month/day/year combinations that are not supported.) INCREASE/REDUCE: +/-
About this software		
Tab 28: Main Menu - Insvd	eH2O	

Tab. 28: Main Menu – InsydeH2O





7.5 Advanced Menu



BIOS Settings	Options	Description
Boot Configuration	See submenu	Configures Boot Settings
Peripheral Configuration	See submenu	Configures the peripheral devices.
NVMe Configurations	See submenu	This functions shows the connected NVMe devices
USB Configuration	See submenu	Configure the USB support
ACPI Table/Features Control	See submenu	Configures ACPI Tables/Features setting
CPU related setting	See submenu	CPU Related settings
Above 4GB MMIO	<disabled> <enabled>*</enabled></disabled>	Enable/Disable above 4GB MemoryMappedIO BIOS assignment. It's only available with Uefi Boot mode.
GS2XX options	See submenu	GS2XX options: Configure PIC watchdog!

Tab. 29: Advanced Menu – InsydeH2O

Fig. 54: Advanced Menu – InsydeH2O





7.5.1 Boot Configuration



Fig. 55: Boot Configuration – InsydeH2O

BIOS Settings	Options	Description
Numlock	<off> <on>*</on></off>	Configuration of Numlock key at power up.

Tab. 30: Boot Configuration – InsydeH2O

Device Reference Manual – P – Revision 3

7.5.2 Peripheral Configuration



Fig. 56: Peripheral Configuration – InsydeH2O

BIOS Settings	Options	Description
Trust Platform Module	<disabled> <enable discrete="" tpm="">* <enable firmware="" tpm=""></enable></enable></disabled>	Enable/Disable TPM physical presence. Need to reboot when set from disable to enable before selecting TPM Operation.
Erase fTPM NV for factory reset	<disabled> <enabled>*</enabled></disabled>	Control if need to erase the TPM NV when fTPM factory reset flag set.

Tab. 31: Peripheral Configuration – InsydeH2O





7.5.3 NVMe Configurations



Fig. 57: NVMe Configurations - InsydeH2O

BIOS Settings	Options	Description
NVMe Configuration		This function shows the connected NVMe devices

Tab. 32: NVMe Configurations

Device Reference Manual – P – Revision 3

7.5.4 USB Configuration



Fig. 58: USB Configurations – InsydeH2O

BIOS Settings	Options	Description
Enable/Disable – VCC	No options	Enable/Disable – USB VCC
of USB Jacks		of USB3.1 Rear Port 1 and 2
T-L OO LIOD O- Constitute La		

Tab. 33: USB Configuration – InsydeH2O





(1) 2023/10/13 FRI MAINBOARD SYSTEM E.E.P.D. 09:04 31°C 36°C AMD Ryzer Enbedded R2E14 DRAM Frequency 2667 MH Memory Size: 8192 MB Advanced > Enable/Disable - VCC of USB Jacks Main Enable/Disable - USB VCC of USB3.1 Rear Port 1 and 2 USB3.1 Rear Port 2 USB3.1 Rear Port 1 Ð, Advanced Enable/Disable - USB VCC of USB3.1 Rear Port 1 and 2 © Security Power e Boot AMD PBS AMD CBS (F1)(F5)(F6) (ESC) (+)(+) (+)(+)ENTER (F9) (F10) <+ Exit Change Values Select SubMenu Setup Defaults Save and Exit

Fig. 59: Enable/Disable - VCC of USB Jacks - InsydeH2O

7.5.4.1 Enable/Disable – VCC of USB Jacks

BIOS Settings	Options	Description
USB 3.1 Rear Port 1	<disabled> <enabled>*</enabled></disabled>	Enable/Disable – USB VCC of USB 3.1 Rear Port 1
USB 3.1 Rear Port 2	<disabled> <enabled>*</enabled></disabled>	Enable/Disable – USB VCC of USB 3.1 Rear Port 2

Tab. 34: Enable/Disable – VCC of USB Jacks – InsydeH2O

Device Reference Manual – P – Revision 3

7.5.5 ACPI Table/Features Control



Fig. 60: ACPI Table/Features Control – InsydeH2O

BIOS Settings	Options	Description
HPET – HPET Support	<disabled> <enabled>*</enabled></disabled>	High Precision Event Timer is supported in Windows Vista or above. HPET controller should not been seen in Windows XP no matter enable/disable in SCU. If this feature is enabled, the HPET table will be added into ACPI Tables.

Tab. 35: ACPI Table/Features Control – InsydeH2O





Device Reference Manual – P – Revision 3

7.5.6 CPU Related setting



Fig. 61: CPU related setting - InsydeH2O

BIOS Settings	Options	Description
SVM support	<disabled> <enabled>*</enabled></disabled>	Enable/Disable SVM support

Tab. 36: CPU related setting - InsydeH2O





7.5.7 GS2XX options – Watchdog



Fig. 62: GS2XX options – Watchdog – InsydeH2O

BIOS Settings	Options	Description
PIC Watchdog	<disabled>* <enabled></enabled></disabled>	Enable/Disable the PIC watchdog
Watchdog Timeout (s)	Adjust value [30-254] Default value [40]*	Seconds before PIC watchdog times out. Range: 30-254 seconds.
Wake on LAN	<disabled> <enabled>*</enabled></disabled>	Enable/Disable wake on LAN
Power LED Mode	<disabled> <enabled>*</enabled></disabled>	Set Power LED Mode (Enable/Disable)
KL15 support	<disabled>* <enabled></enabled></disabled>	KL15 support (Enable/Disable) If enabled, set AMD CBS > FCH Common Options > AC Power Loss Options -> Always Off To achieve minimum of power consumption when system is Off, set also in GS2XX option -> USB Power Off in S5 to Enabled (for all USB Ports) and Wake on LAN to Disabled In addition set in OS that power button press -> shuts down the system!
USB3.1 Rear Port 1	<disabled>* <enabled></enabled></disabled>	Force VCC Off of USB Jacks in S5. Let VCC of USB Jack unchanged as
USB3.1 Rear Port 2	<disabled>* <enabled></enabled></disabled>	in Advanced > USB Configuration > Enable/Disable - VCC of USB Jacks or Switches it off when in S5 (System Power Off)!

Tab. 37: GS2XX options – Watchdog – InsydeH2O





7.6 AMD CBS



Fig. 63: AMD CBS - InsydeH2O

BIOS Settings	Options	Description
Zen Common Options	See submenu	Zen Common Options
NBIO Common Options	See submenu	NBIO Common Options
FCH Common Options	See submenu	FCH Common Options

Tab. 38: AMD CBS – InsydeH2O

Device Reference Manual – P – Revision 3

7.6.1 Zen Common Options



Fig. 64: Zen Common Options – InsydeH2O

BIOS Settings	Options	Description
Core Performance Boost	<disabled>* <auto></auto></disabled>	Disable CPB
CPU Thermal Throttling Control	<disabled>* <enabled></enabled></disabled>	CPU Thermal Throttling Enable/Disable

Tab. 39: Zen Common Options – InsydeH2O





7.6.2 NBIO Common Options



BIOS Settings Options		Description
GFX Configuration	No options	GFX Configuration
CPU and Auxiliary Fan Control	No options	CPU and Auxiliary Fan Control
System Configuration	<35W POR Configuration>*	Warning: Select System Configuration may cause the system to hang, as some System Configuration may not be supported by your OPN.

Tab. 40: NBIO Common Options – InsydeH2O

Fig. 65: NBIO Common Options – InsydeH2O





7.6.2.1 GFX Configuration



Fig. 66: GFX Configuration – InsydeH2O

BIOS Settings	Options	Description
UMA Mode	<auto> <uma_specified>* <uma_auto></uma_auto></uma_specified></auto>	UMA Mode
UMA Version	<legacy> <non-legacy> <hybrid secure=""> <auto>*</auto></hybrid></non-legacy></legacy>	UMA Legacy Version UMA Non Legacy Version Hybrid Secure
UMA Frame buffer Size	<auto>* <64M> <128M> <256M> <384M> <512M> <80M> <96M> <768M> <1G> <2G> <3G> <4G> <6G> <8G> <16G></auto>	Set UMA FB size
UMA Above 4G	<disabled> <enabled> <auto>*</auto></enabled></disabled>	If requested UMA frame buffer size can't be fit under 4GB or the system has enough available memory above 4GB, this option may be set to TRUE to allow UMA frame buffer size to be allocated successfully.
NB Azalia	<disabled> <enabled> <auto>*</auto></enabled></disabled>	Enable Integrate HD Audio controller
Tab. 41: GFX Configura	tion – InsvdeH2O	

b. 41: GFX Configuration – InsydeH2O





7.6.2.2 CPU and Auxiliary Fan Control

E.E.P.D JUST 6/7. AMD Ryzer Enbodied R2E3 DRAM Frequency 2667 Mi Memory Suri: 8142 MB	Deladeral A with Kadeon Graphu te	09:05	SYSTEM 31°C		PU Emperature 36°C	
Main	AMD(CPU and Auxilia	CBS > CPU an	d Auxiliary Fa	an Contro 	ot	
Advanced	CPU Fan C	ontrol ()ptimized Cooli >	Exte	ernal Fan Control	
Security	External Fi	an Control	No Cooling >	User Opt Siler Max No f	can set: imized Cooling nt Mode> Less noise imum Cooling> Alwa Cooling> Always off	ys on
Power						
Boot						
AMD PBS						
⊲ Exit	F1 Help	ESC Exit Select Item	Select Item)F6 (ge Values Select	SubMenu Setup Defaults	F10 Save and Exit

Fig. 67: CPU and Auxiliary Fan Control - InsydeH2O

BIOS Settings	Options	Description
CPU Fan Control	<optimized cooling="">* <silent mode=""> <maximum cooling=""> <no cooling=""></no></maximum></silent></optimized>	User can set: Optimized Cooling Silent Mode> Less noise Maximum Cooling> Always on No Cooling> Always off
Auxiliary Fan Control	<optimized cooling=""> <silent mode=""> <maximum cooling=""> <no cooling="">*</no></maximum></silent></optimized>	User can set: Optimized Cooling Silent Mode> Less noise Maximum Cooling> Always on No Cooling> Always off
External Fan Control	<optimized cooling=""> <silent mode=""> <maximum cooling=""> <no cooling="">*</no></maximum></silent></optimized>	User can set: Optimized Cooling Silent Mode> Less noise Maximum Cooling> Always on No Cooling> Always off
CPU Fan Control	<optimized cooling="">* <silent mode=""> <maximum cooling=""> <no cooling=""></no></maximum></silent></optimized>	User can set: Optimized Cooling Silent Mode> Less noise Maximum Cooling> Always on No Cooling> Always off
Tab. 42: CPLL and Auviliar	v Ean Control InsvdoH2O	

Tab. 42: CPU and Auxiliary Fan Control – InsydeH2O





7.6.3 FCH Common Options



Fig. 68: FCH Common Options – InsydeH2O

BIOS Settings	Options	Description
Ac Power Loss Options	No options	Ac Power Loss Options
Uart Configuration Options	No options	Uart Configuration Options

Tab. 43: FCH Common Options - InsydeH2O

Device Reference Manual – P – Revision 3

7.6.3.1 Ac Power Loss Options



Fig. 69: Ac Power Loss Options – InsydeH2O

BIOS Settings	Options	Description		
Ac Loss Control	<always off=""> <always on=""> <previous>*</previous></always></always>	Select Ac Loss Control Method		
Take 44. As Deversel and Onlines - Jacobillion				

Tab. 44: Ac Power Loss Options – InsydeH2O





7.6.3.2 Uart Configuration Options

E.E.P.D. Jast emb AMD Ryzer Enbodies (2514 DRAM Frequency 2667 MH Memory See: 8102 MB	900 ded With Rakson Graph L.	() 2023/1 FRI 09:	05	MAINBOA SYSTEM 31°(C	J CPU TEMPERATUR 36°C	I <mark>E</mark>	
Main	AMD Uart Configur	CBS > U ation Options	art Confi	guratio	n Optioi	าร		
Advanced	Uart 0 E Uart 0 L	nable egacy Option	s (Enabl	.ed > F8 >	Uart 1 Legacy	Options	
Security	Uart 1 E Uart 1 L	nable egacy Option	s (Enabl GM2 0x2	ed > F8 = 1	ivo netp string		
Power								
AMD PBS								
AMD CBS								
Exit	(F1) Help	ESC Exit	Select Item S	elect Item	(F5)(F6) Change Values	Select SubMenu Se	F9 etup Defaults S	F10 ave and Exit

BIOS Settings	Options	Description
Uart 0 Enable	<disabled></disabled>	No help string
	<enabled>*</enabled>	
Uart 0 Legacy Options	<disabled></disabled>	No help string
	<com1 0x3f8="">*</com1>	
	<com2 0x2f8=""></com2>	
	<com3 0x3e8=""></com3>	
	<com4 0x2e8=""></com4>	
Uart 1 Enable	<disabled></disabled>	No help string
	<enabled>*</enabled>	
Uart 1 Legacy Options	<disabled></disabled>	No help string
	<com1 0x3f8=""></com1>	
	<com2 0x2f8="">*</com2>	
	<com3 0x3e8=""></com3>	
	<com4 0x2e8=""></com4>	

Tab. 45: Uart Configuration Options - InsydeH2O

Fig. 70: Uart Configuration Options – InsydeH2O





7.7 AMD PBS Option



Fig. 71: AMD PBS Option - InsydeH2O

BIOS Settings	Options	Description
AMD Firmware Version	No options	Show all of AMD Firmware Version
WWAN Power	<disabled></disabled>	Enable/disable power of M.2 Key B Slot
Control	<enabled>*</enabled>	
WLAN Radio	<enabled>*</enabled>	Enable/disable WLAN radio operation of
Operation	<disabled></disabled>	M.2 Key E Slot
BT Radio	<enabled>*</enabled>	Enable/disable Bluetooth(BT) radio
Operation	<disabled></disabled>	operation of M.2 Key E Slot

Tab. 46: AMD PBS Option – InsydeH2O

Device Reference Manual – P – Revision 3

7.7.1 AMD Firmware Version

E.E.P.D. Jost emu AMD Rozen Entocodos (2211 DRAM Frequency: 2647 MH Memory Sue: 8192 MB	eadeal A with' Rideon Graph	© 2023/10/13 FRI 09:04	4 MAINBOARD SYSTEM 31°C	/	CPU TEMPERATURE 36°C
		AMD PBS > AMI	D Firmware Version	1	
Main	AMD F	irmware Version			
Advanced	. A(GESA Version	EmbeddedR2KPI-FP5_1.0.0		DXIO FW Version
\odot	💼 ps	SP BootLoader Version	0.8.A3.84		
Security	PS	SP SecureOS Version	0.8.A3.84		
(T T D					
Power	🗖 AE	3L Version	211126EE		
	📕 AF	PCB Version	0029		
~15	I AF	POB Version	0013		
ē.					PIC FW Version
Advanced	Uc	code Patch Version	8108109		
	SN	40 FW Version	4.30.86.0		
Security	D>	KIO FW Version	001F.01C0		
Power	– M	P2 I2C FW Version	1. r. 2.4		
615	📮 XH	HCI FW Version	FC.CE.8B.6A		
Boot	📕 VE	3IOS FW Version	113-PICASSO-117		
AMD PBS	■ G(DP Driver Version	AMD GOP X64 Release Driver Rev.2.8.0.0.0.Jul 26 2019.11:24:53		
AMD CBS	🔹 PI	C FW Version	000403		
	6			2	
exit	Help	Exit Selec	t Item Select Item Change Va	alues S	elect SubMenu Setup Defaults Save and Exit

Fig. 72: AMD Firmware Version - InsydeH2O





7.8 Boot Menu



Fig. 73: Boot Menu – InsydeH2O

BIOS Settings	Options	Description
Quick Boot	<enabled>* <disabled></disabled></enabled>	Allows InsydeH2O to skip certain tests while booting. This will decrease the time needed to boot the system.
Quiet Boot	<enabled>* <disabled></disabled></enabled>	Disables or enables booting in Text Mode.
Network Stack	<disabled>* <enabled></enabled></disabled>	Network Stack Support: Windows 8 BitLocker Unlock

Device Reference Manual – P – Revision 3

		UEFI IPv4/IPv6 PXE Legacy PXE OPROM
PXE Boot capability	<disabled>*</disabled>	Disabled : Support Network Stack UEFI PXE : IPv4/IPv6 Legacy : Legacy PXE OPROM only
Power Up In Standby Support	<enabled> <disabled>*</disabled></enabled>	Disable or enable Power Up In Standby Support. The 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.
Add Boot Options	<first> <last> <auto>*</auto></last></first>	Position in Boot Order for Shell,Network and Removables
USB Boot	<enabled>* <disabled></disabled></enabled>	Disables or enables booting to USB boot devices.
UEFI OS Fast Boot	<enabled>* <disabled></disabled></enabled>	If enabled the system firmware does not initialize keyboard and check for firmware menu key.
USB Hot Key Support	<disabled> <enabled>*</enabled></disabled>	Enable/Disable to support USB hot key while booting. This will decrease the time needed to boot the system.
Timeout	Adjust value [0-10] Default value [5]	The number of seconds that the firmware will wait before booting the original default boot selection.
Automatic Failover	<disabled> <enabled>*</enabled></disabled>	Enable: if boot to default device fail, it will directly try to boot next device. Disable: if boot to default device fail, it will pop warning message then go into firmware UI.
EFI	No options	EFI Boot Order Settings

Tab. 47: Boot Menu – InsydeH2O



EM[®] PRO rack



EM TRUST

E.E.P.D. Just em AMD. Ryzen Enbodder (231) DRAM. Frequency, 2667 Mil Memory Stat: 8162 Mb	Dirdded) L4 with Radson Graphi He	() ²⁰ FR 0	9:04	AAINBO SYSTEM 31°	C	J CPU TEMPERAT	rure 2	
Main	U Boot	t > EFI						
Advanced	EFI USI EFI Inte	3 Device (S ernal Shell	SanDisk)	Enabled		EFI Interna	l Shell	<u>()</u>
Security								
Boot								
AMD PBS								
AMD CBS	F1	ESC Exit		Select Item	(F5)(F6) Change Values	Select SubMenu	(F9) Setup Defaults	F10 Save and Exit

Fig. 74: EFI – InsydeH2O

BIOS Settings	Options	Description
EFI USB Device (SanDisk)	[]* [X]	
EFI Internal Shell	[]* [X]	

Tab. 48: EFI – InsydeH2O

Device Reference Manual – P – Revision 3

7.9 Power Menu



Fig. 75: Power Menu – InsydeH2O

BIOS Settings	Options	Description
Wake on PME	<disabled> <enabled>*</enabled></disabled>	Determines the action taken when the system power is off and a PCI Power Management Enable wake up event occurs.
Auto Wake on S5	<disabled>* <by day="" every=""> <by day="" month="" of=""></by></by></disabled>	Auto wake on S5, By Day of Month or Fixed time of every day

Tab. 49: Power Menu – InsydeH2O





7.10 Exit Menu



BIOS Settings	Options	Description
Exit Saving Changes		Exit system setup and save your changes.
Save Change Without Exit		Save your changes and without exiting system.
Exit Discarding Changes		Exit system setup and without saving your changes.
Load Optimal Defaults		Load Optimal Defaults.
Load Custom Defaults		Load Custom Defaults.
Save Custom Defaults		Save Custom Defaults
Discard Changes		Discard Changes

Tab. 50: Exit Menu – InsydeH2O

Fig. 76: Exit Menu – InsydeH2O





7.11 Security Menu

Device Reference Manual – P – Revision 3

E.E.P.D. 	udded Holason Graph	() 2023/10/13 FRI 09:04	MAINBOARD SYSTEM 31°C		CPU TEMPERATURE 36°C	
Main	Ø	Security		n		
R.	Cu	urrent TPM Device	TPM 2.0 (DTPM)) >	Clear TPM	
Advanced	I TF	PM State	All Hierarchies Enabl Owned	led,		<u> </u>
Security	TP Al	PM Active PCR Hash Igorithm	SHA256		Clear TPM. Removes context associated w Owner.	all TPM th a specific
	TF Ha	PM Hardware Supported ash Algorithm	SHA1, SHA256			
Power	I BI Al	IOS Supported Hash Igorithm	SHA1, SHA256, SHA3 SHA512, SM3_25	384, 6		
<u>ب</u> ه	Tr	rEE Protocol Version		. >		
Boot	TF	PM Availability				
	TF	PM Operation	No Operation	1 >		
പ	CI	lear TPM	Disabled			
Boot	SL	upervisor Password	Not Installed			
AMD PBS	Se	et Supervisor Password				
AMD CBS						
Exit	F1 Help	Esc elect	Item Select Item Ch	F5 F6	Select SubMenu Setup Def	aults Save and Exit

Fig. 77: Security Menu - InsydeH2O

BIOS Settings	Options	Description
Current TPM Device	<not detected=""> <tpm 1.2=""> <tpm (dtpm)="" 2.0="">*</tpm></tpm></not>	Current TPM Device: TPM1.2, or

TrEE Protocol Version	<1.0> <1.1>*	TrEE Protocol Version: 1.0 or 1.1
TPM Availability	<available>* <hidden></hidden></available>	When hidden, don't expose TPM to OS
TPM Operation	<no operation="">* <enable> <setpcrbanks(algorithm)> <logalldigests> <setpprequiredforclear_true> <setpprequiredforclear_false> <setpprequiredforturnon_false> <setpprequiredforturnon_true> <setpprequiredforturnoff_false> <setpprequiredforturnoff_true> <setpprequiredforchangepcrs_false> <setpprequiredforchangepcrs_true> <setpprequiredforchangeeps_false> <setpprequiredforchangeeps_false> <setpprequiredforchangeeps_false> <setpprequiredforchangeeps_false></setpprequiredforchangeeps_false></setpprequiredforchangeeps_false></setpprequiredforchangeeps_false></setpprequiredforchangeeps_false></setpprequiredforchangepcrs_true></setpprequiredforchangepcrs_false></setpprequiredforturnoff_true></setpprequiredforturnoff_false></setpprequiredforturnon_true></setpprequiredforturnon_false></setpprequiredforclear_false></setpprequiredforclear_true></logalldigests></setpcrbanks(algorithm)></enable></no>	Select one of the supported operations to change TPM2 state.
Clear TPM	[] [X]	Clear TPM. Removes all TPM context associated with a specific Owner.
Set Supervisor Password	None	Install or change the password and the length of password must be greater than one character.
Tab. 51: Security Mer	nu – InsydeH2O	

E.E.P.D.



7.11.1 Storage Password Setup Page



BIOS Settings	Options	Description
TCG Storage Action	<no operation="">* <enable_blocksidfunc> <disable_blocksidfunc> <pprequiredforenableblocksid_true> <pprequiredforenableblocksid_false> <pprequiredfordisableblocksid_true> <pprequiredfordisableblocksid_false></pprequiredfordisableblocksid_false></pprequiredfordisableblocksid_true></pprequiredforenableblocksid_false></pprequiredforenableblocksid_true></disable_blocksidfunc></enable_blocksidfunc></no>	Change BlockSID actions, includes enable or disable BlockSID, Require or not require physical presence when remote enable or disable BlockSID

Tab. 52: Storage Password Setup Page – InsydeH2O

Fig. 78: Storage Password Setup Page – InsydeH2O





Index of Figures

Fig. 1: Type label (example)	11
Fig. 2: Dimensions front view	11
Fig. 3: Dimensions rear view	11
Fig. 4: Dimensions side view	12
Fig. 5: Dimensions top view with optional mounting brackets	12
Fig. 6: Dimensions top view	12
Fig. 7: Dimension bottom view	12
Fig. 8: Interfaces front view	14
Fig. 9: Interfaces rear view	14
Fig. 10: power button with LED ring	15
Fig. 11: SFP+ modules Detail	15
Fig. 12: Ethernet Ports Detail	15
Fig. 13: Dual DisplayPort Detail	16
Fig. 14: USB-C Ports Detail	16
Fig. 15: Mini USB-B Detail	16
Fig. 16: Auxiliary power button and HDD/SSD-LEDs position	16
Fig. 17: screws on the left side	17
Fig. 18: screws on the right side	17
Fig. 19: screws on the rear side	17
Fig. 20: top view of the system without cover	18
Fig. 21: M.2 Key B module assembly	18
Fig. 22: opening of SSD installation slot	19
Fig. 23: M3X30 screw	19
Fig. 24: SSD slots	19
Fig. 25: Main Menu – AMI BIOS	21
Fig. 26: Advanced Menu – AMI BIOS	22
Fig. 27: Trusted Computing – AMI BIOS	23
Fig. 28: TPM Configuration – AMI BIOS	24
Fig. 29: GS2x Advanced Options – AMI BIOS	25
Fig. 30: CPU Configuration – AMI BIOS	26

Device Reference Manual – P – Revision 3

Fig.	31: Node 0 Information – AMI BIOS	.26
Fig.	32: AMI Graphic Output Protocol Policy – AMI BIOS	.27
Fig.	33: USB Configuration – AMI BIOS	.28
Fig.	34: Network Stack Configuration – AMI BIOS	.29
Fig.	35: NVMe Configuration – AMI BIOS	.30
Fig.	36: AMD CBS – AMI BIOS	.30
Fig.	37: Zen Common Options – AMI BIOS	.31
Fig.	38: NBIO Common Options – AMI BIOS	.31
Fig.	39: GFX Configuration – AMI BIOS	.32
Fig.	40: NB Configuration – AMI BIOS	.33
Fig.	41: PCIe Configuration – AMI BIOS	.33
Fig.	42: Fan Control – AMI BIOS	.34
Fig.	43: FCH Common Options – AMI BIOS	.34
Fig.	44: USB Configuration Options – AMI BIOS	.35
Fig.	45: Ac Power Loss Options – AMI BIOS	.35
Fig.	46: Uart Configuration Options – AMI BIOS	.36
Fig.	47: AMD PBS – AMI BIOS	.37
Fig.	48: Security Menu – AMI BIOS	.38
Fig.	49: Secure Boot – AMI BIOS	.39
Fig.	50: Key Management – AMI BIOS	.40
Fig.	51: Boot Menu – AMI BIOS	.42
Fig.	52: Save & Exit Menu – AMI BIOS	.43
Fig.	53: Main Menu – InsydeH2O	.45
Fig.	54: Advanced Menu – InsydeH2O	.46
Fig.	55: Boot Configuration – InsydeH2O	.47
Fig.	56: Peripheral Configuration – InsydeH2O	.47
Fig.	57: NVMe Configurations – InsydeH2O	.48
Fig.	58: USB Configurations – InsydeH2O	.48
Fig.	59: Enable/Disable – VCC of USB Jacks – InsydeH2O	.49
Fig.	60: ACPI Table/Features Control – InsydeH2O	.49
Fig.	61: CPU related setting – InsydeH2O	.50
Fig.	62: GS2XX options – Watchdog – InsydeH2O	.51



EM TRUST

EM[®] PRO rack

Device	Reference	Manual –	P –	Revision 3	
--------	-----------	----------	------------	-------------------	--

Fig. 63: AMD CBS – InsydeH2O	52
Fig. 64: Zen Common Options – InsydeH2O	52
Fig. 65: NBIO Common Options – InsydeH2O	53
Fig. 66: GFX Configuration – InsydeH2O	54
Fig. 67: CPU and Auxiliary Fan Control – InsydeH2O	55
Fig. 68: FCH Common Options – InsydeH2O	56
Fig. 69: Ac Power Loss Options – InsydeH2O	56
Fig. 70: Uart Configuration Options – InsydeH2O	57
Fig. 71: AMD PBS Option – InsydeH2O	58
Fig. 72: AMD Firmware Version – InsydeH2O	58
Fig. 73: Boot Menu – InsydeH2O	59
Fig. 74: EFI – InsydeH2O	60
Fig. 75: Power Menu – InsydeH2O	60
Fig. 76: Exit Menu – InsydeH2O	61
Fig. 77: Security Menu – InsydeH2O	62
Fig. 78: Storage Password Setup Page – InsydeH2O	63





Index of Tables

Tab. 1: Options	10
Tab. 2: Accessories	10
Tab. 3: Main Menu – AMI BIOS	21
Tab. 4: Advanced Menu – AMI BIOS	22
Tab. 5: Trusted Computing – AMI BIOS	23
Tab. 6: TPM Configuration – AMI BIOS	24
Tab. 7: GS2x Advanced Options – AMI BIOS	25
Tab. 8: CPU Configuration – AMI BIOS	26
Tab. 9: AMI Graphic Output Protocol Policy – AMI BIOS	27
Tab. 10: USB Configuration – AMI BIOS	28
Tab. 11: Network Stack Configuration – AMI BIOS	29
Tab. 12: AMD CBS – AMI BIOS	30
Tab. 13: Zen Common Options – AMI BIOS	31
Tab. 14: NBIO Common Options – AMI BIOS	31
Tab. 15: GFX Configuration – AMI BIOS	32
Tab. 16: NB Configuration – AMI BIOS	33
Tab. 17: PCIe Configuration – AMI BIOS	33
Tab. 18: Fan Control – AMI BIOS	34
Tab. 19: FCH Common Options – AMI BIOS	34
Tab. 20: USB Configuration Options – AMI BIOS	35
Tab. 21: Ac Power Loss Options – AMI BIOS	35
Tab. 22: Uart Configuration Options – AMI BIOS	36
Tab. 23: Security Menu – AMI BIOS	38
Tab. 24: Secure Boot – AMI BIOS	39
Tab. 25: Key Management – AMI BIOS	41
Tab. 26: Boot Menu – AMI BIOS	42
Tab. 27: Save & Exit Menu – AMI BIOS	43
Tab. 28: Main Menu – InsydeH2O	45
Tab. 29: Advanced Menu – InsydeH2O	46
Tab. 30: Boot Configuration – InsydeH2O	47

E.E.P.D. GmbH | Gewerbering 3 | 85258 Weichs

Device Reference Manual – P – Revision 3

Tab. 31: Peripheral Configuration – InsvdeH2O	47
Tab. 32: NVMe Configurations	48
Tab. 33: USB Configuration – InsvdeH2O	48
Tab. 34: Enable/Disable – VCC of USB Jacks – InsvdeH2O	49
Tab. 35: ACPI Table/Features Control – InsydeH2O	49
Tab. 36: CPU related setting – InsydeH2O	50
Tab. 37: GS2XX options – Watchdog – InsydeH2O	51
Tab. 38: AMD CBS – InsydeH2O	52
Tab. 39: Zen Common Options – InsydeH2O	52
Tab. 40: NBIO Common Options – InsydeH2O	53
Tab. 41: GFX Configuration – InsydeH2O	54
Tab. 42: CPU and Auxiliary Fan Control – InsydeH2O	55
Tab. 43: FCH Common Options - InsydeH2O	56
Tab. 44: Ac Power Loss Options – InsydeH2O	56
Tab. 45: Uart Configuration Options – InsydeH2O	57
Tab. 46: AMD PBS Option – InsydeH2O	58
Tab. 47: Boot Menu – InsydeH2O	59
Tab. 48: EFI – InsydeH2O	60
Tab. 49: Power Menu – InsydeH2O	60
Tab. 50: Exit Menu – InsydeH2O	61
Tab. 51: Security Menu – InsydeH2O	62
Tab. 52: Storage Password Setup Page – InsydeH2O	63





List of Abbreviations

AC	Alternating current
APAC	Asia Pacific and countries
BIOS	Basic input/output system
BT	Bluetooth
DC	Direct current
DDR4	Fourth generation "double data rate" memory technology
DP	Display port
EMEA	Europe, Middle East, Africa
GND	Ground
GNSS	Global Navigation Satellite System
loT	Internet of Things
LTE	Long Term Evolution
MIC	Microphone
M.2	Next generation mSATA
NVME	Non-Volatile Memory Express
OCP	Over Current Protection
PWM	Pulse-width modulation
RAM	Random access memory
RS-232	Serial standard interface
RS-485	Serial standard interface
SD	Secure digital memory card
SIM	Subscriber identity module
SMA	Subminiature version A connector
SO-DIMM	Small outline dual inline memory module
SSD	Solid state drive
UART	Universal Asynchronous Receiver / Transmitter
USB	Universal serial bus

WLAN	Wireless local area network
WWAN	Wireless wide area network







