EM BOX® PC NUCR – Device Reference Manual

Picture shows EM BOX® PC NUCR with custom options

E.E.P.D.
...just embedded!

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

08/2025 Version 5.0

General Notes

This user manual is for your information only.
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

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.

Disclaimer

This document is provided for the general information of the customer. It describes the general functionality of the system and is not considered as assured characteristics. The written declarations in this specification 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. Customers 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.

Limited Warranty

This product will be free from defects in workmanship and material under normal and proper use for the period of time defined in our General Terms of Business, effective the date of the original shipment from E.E.P.D. GmbH.
In the event of a warranty claim for defects, which appear within the warranty period, customer shall deliver the product along with proof of purchase to the original place of purchase, shipping prepaid. Repair, replacement or refund of the purchase price of the defective product will be at the sole option of the manufacturer. All transportation risks and costs in connection with warranty service are the responsibility of the customer.

THIS WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TO ANY CUSTOMER, CONSUMER, END USER, PURCHASER, OR OTHERWISE. IN NO EVENT SHALL MANUFACTURER BE LIABLE FOR LOSS OF PROFITS, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY BREACH OF CONTRACT OR WARRANTY, NEGLIGENCE, STRICT LIABILITY OR OTHERWISE.

The remedies for defects in this product are limited to those set forth above. If this limitation of remedies is held by any court to be void or unenforceable, or if no warranty is made, manufacturers liability shall in no event exceed the purchase price of the product giving rise to the claim, regardless of whether such claim is brought in breach of contract or warranty, negligence, strict liability or otherwise.

Product Returns

Before shipping any equipment back, please contact our customer service team at **rma@eepd.de**.

If you return the Box PC 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 Box PC 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.

Customer Support

Please contact:
https://www.eepd.de/support/

Technical Support

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

Table of Contents

Revision History

Date	Version	Changes	Proofed
18.08.2025	5.0	First release for HW Rev.5	

Symbols

The red danger sign warns you if incorrect operation puts your life or health at great risk. Both the components and the peripherals could be destroyed.

The orange warning sign warns you that an incorrect or missing operation could seriously endanger your health or destroy the used components.

The yellow caution sign indicates that an incorrect or missing action could damage the components.

The yellow ESD symbol indicates that electrostatic sensitive components could be destroyed. Unpack shielded components only with ESD protection such as an ESD wristband or on an ESD protected area.

The information sign gives you further information and advice for optimal use of this product.
For example, it draws your attention to necessary or optional accessories.

Safety Instructions

Safety of People

DANGER

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!

WARNING

Please follow all safety instructions at the installation site. Make sure that no or only necessary cables are connected to the Box PC during installation.

If access to the Box PC interfaces is not available after installation, all necessary connections must be made before.

Device Safety

WARNING

The Box PC operates exclusively within the specified 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.

Cooling System

CAUTION

The Box PC 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.

1 System Information

1.1 Required Tools

For the installation of the Box PC system the following standard tools are recommended:

- Torx screwdriver T10
- Slot screwdriver

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

1.2 OS Support

Microsoft® Windows® 10
Microsoft® Windows® 10 IoT Enterprise
Linux Ubuntu 24.04 LTS.

1.3 Intended Use

The Box PC is the perfect industrial grade communicator for secure and reliable IoT communication. Many interfaces provide a wide range of applications. The simultaneous use of 4G (ODM only) and WLAN (ODM only) allows extended router applications.
The Box PC is intended for indoor use only.

1.4 Options

Please contact our sales department for ordering information of optional product features.

Options	Description
Memory modules*	Max. 2x 16 GB dual-channel up to DDR4-2400 SO-DIMM memory with ECC support
SSD*	64 GB – 2 TB
LTE/modem module*#	M.2 LTE card with three SMA connectors
WLAN/BT module kit*#	M.2 WLAN/BT card with two SMA connectors
Operating System*	Windows® 10 IoT Enterprise LTSC 2021, Linux Ubuntu 24.04 LTS
RS232 interface*	9-pin D-SUB connector
RS485 interface*	9-pin D-SUB connector
Power switch*	Power switch with LED
Sound*	Audio connector 3.5 mm MIC IN / headphone OUT
*factory-assembled on request #ODM option	

Tab. 1: Options

1.5 Accessories

Please contact our sales department for ordering information.

Accessories	Description
4-pin power cable	Power cable with open ends
Power supply (90 W / 24 V)	Power supply incl. cable with EU plug
Display cable	Cable MiniDP to HDMI, 2 m, with interlock
WLAN/BT antenna	SMA antenna
LTE/GPS antenna	SMA antenna with or without cable
DIN rail clip	DIN rail clip with screws for „TS35“ hat-rails
VESA mounting	Allows installation behind a monitor
Universal holder	Allows further mounting options
M.2 module cooler	SSD and modem m.2 slot cooling

Tab. 2: Accessories

1.6 Scope of Delivery

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

1.6.1 Type Label

Fig. 1: Type label

1 – Manufacturer

2 – Product name

3 – Power input voltage range (absolute voltage values)

4 – Serial number with barcode

5 – Certification information

1.7 System Dimensions

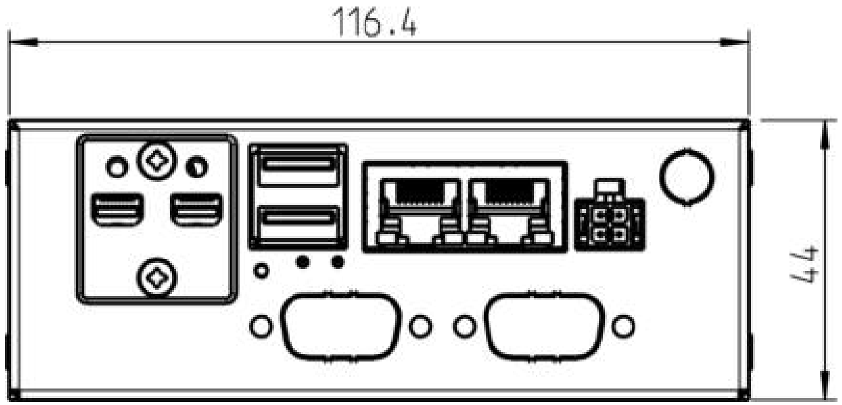


Fig. 2: Dimensions frontside, all values approx. in mm

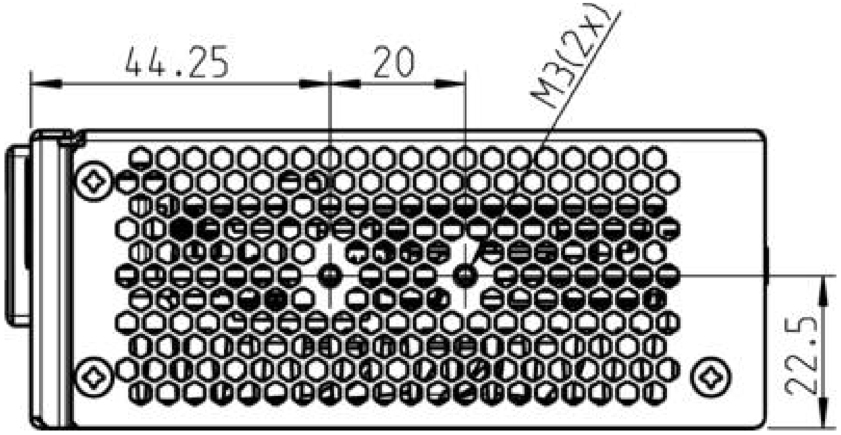


Fig. 4: Dimensions right side, all values approx. in mm

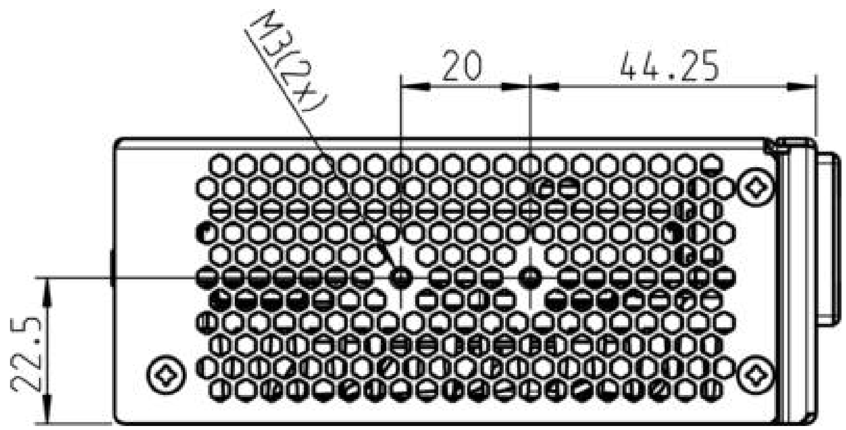


Fig. 3: Dimensions left side, all values approx. in mm

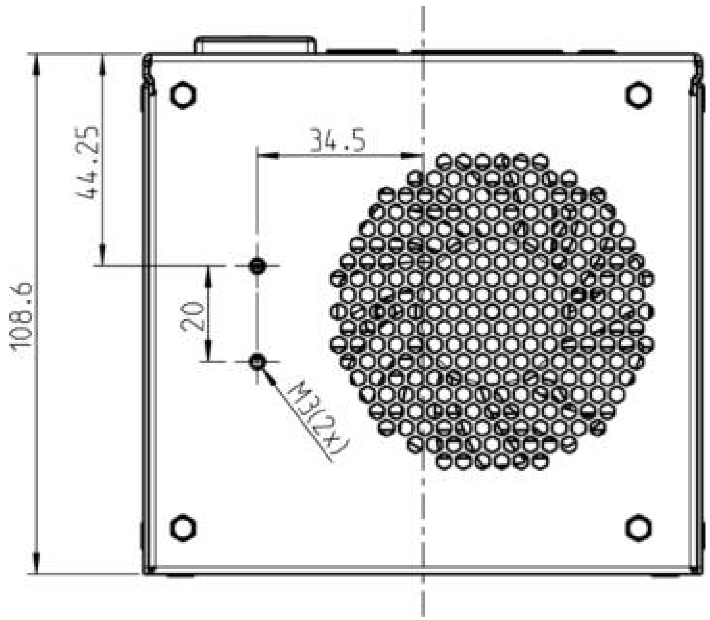


Fig. 5: Dimensions bottom side, all values approx. in mm

1.8 System Mounting

1.8.1 Stand-alone

For use as a desktop computer, apply the self-adhesive rubber feet to the bottom of the housing.

Before attaching the rubber feet, please clean / degrease the bonding areas with a suitable solvent, e.g. alcohol.

Fig. 6: EM BOX® PC NUCD with rubber feet

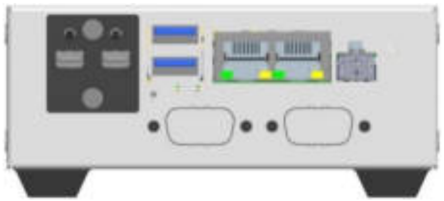


Fig. 7: Front view with rubber feet

1.8.2 VESA mounting (optional)

The EM BOX® PC is also designed for VESA mounting. There is an optional VESA mount available as shown in *Fig. 8*.

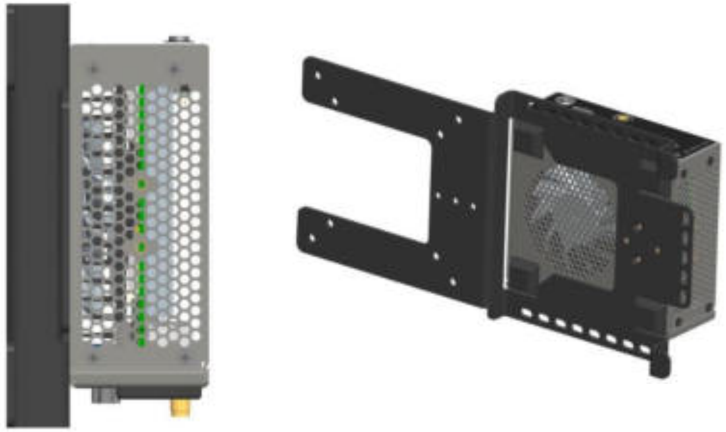


Fig. 8: VESA mounting

1.8.3 Universal Holder (optional)

The EM BOX® PC is also designed for other mounting options. There is an universal holder available as shown in *Fig. 9*.

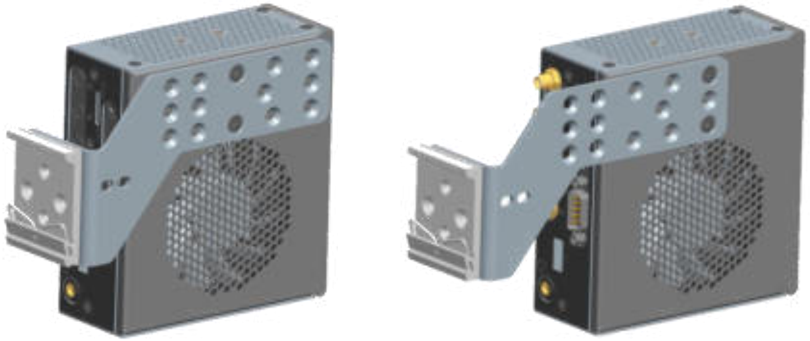


Fig. 9: Universal holder for mounting

1.8.4 DIN Rail Mounting (optional)

The EM BOX® PC is also designed for DIN rail mounting. There are drilled holes for mounting the optional DIN rail holder in various positions (*Fig. 10*).

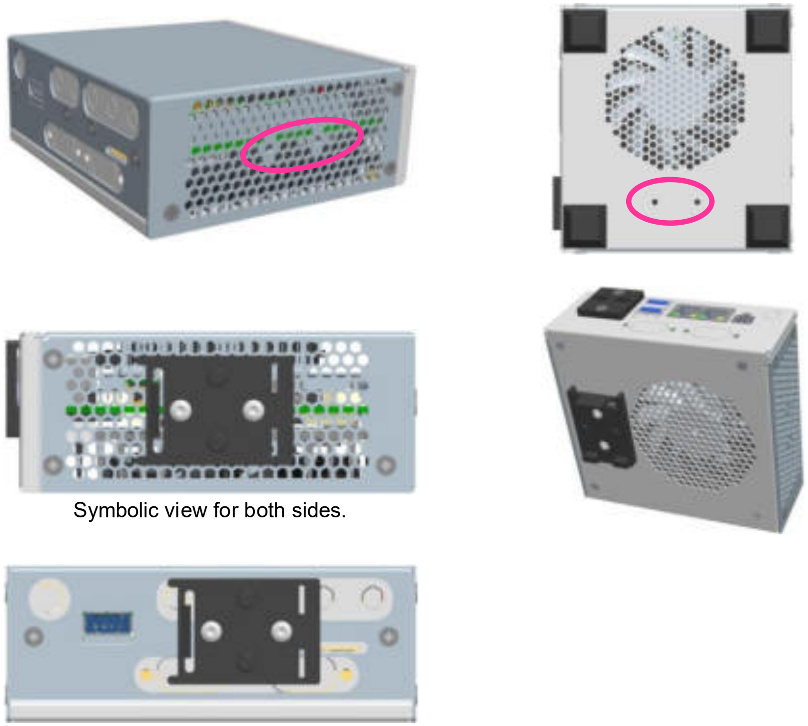


Fig. 10: DIN rail holder positions

Please follow the instructions below:

- Mount the top-hat rail holder with two screws M3x6mm as shown in *Fig. 11* and *Fig. 12*. The top-hat rail holder is suitable for "TS35" DIN rails.
- Place the EM BOX® PC on the DIN rail. Swivel it inwards until it snaps securely into place.
- To detach the system, push it from bottom to top. Swivel it outwards and remove it.

Fig. 11: DIN rail holder mounting

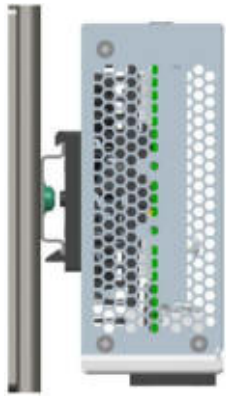


Fig. 12: Side view DIN rail mounted system

2 Technical Data

- AMD Ryzen™ Embedded R1000 processor series:
  R1102G / 2C / 2T / 1.2 GHz - 2.6 GHz / 6 W
  R1305G / 2C / 4T / 1.5 GHz - 2.8 GHz / 10 W (8 - 10 W)
  R1505G / 2C / 4T / 2.4 GHz - 3.3 GHz / 15 W (12 - 25 W)
- Memory: max. 2x 16 GB dual-channel up to DDR4-2400 SO-DIMM memory with ECC support
- Ethernet: 2x Intel® i225-LM with 2.5 Gbit/s with IEEE1588, TSN-support, ETH1 supports Wake-on-LAN
- LTE/4G (ODM option): 300 Mbps max. / EMEA, APAC / Diversity / GNSS
- WiFi/BT (ODM option): 802.11 AC with diversity / Bluetooth version 5
- SSD (optional): M.2 SATA or NVMe / 64 GB – 2 TB
- SD card: µSD XC card slot, supports A1 Application Performance Class, UHS-Class 1
- USB ports:
  2x USB 3.2 Gen2 (10Gb/s, OCP = 1500 mA each) at front side
  1x USB 3.2 Gen2 (10 Gb/s, OCP = 1500 mA) at rear side
- Serial ports (optional):
  1x RS-232 on D-Sub DE-9
  1x RS-232/485 (FDX/HDX) on D-Sub DE-9
- 2x Mini-DP++, v1.4, up to 3840 x 2160 @ 60 Hz
- Sound (optional): 3.5 mm MIC in / HP out on 3.5 mm Audio Jack
- Cooling: CPU fan (5V DC, max. 250 mA, not fused), optional auxiliary fan (5V DC, max. 250 mA, not fused)
- Controlled FAN (PWM + Tacho), temperature sensor, power supply voltage monitoring and watchdog
- Power and status LED
- Power supply: Min. 8.0 V / Max. 32.0 V (DC) / max. 7.5 A, automotive grade | KL15 (ignition), min. 90 W, 8 A fused

CAUTION

Current rating of the power supply has to exceed the expected current draw depending on the system configuration, CPU variant and its TDP settings, and peripheral devices used with the system. Power supplies might derate due to lower efficiency at higher operating temperature. Insufficient power supply might lead to the system instability, shutdown and data loss.

- Power connector:
  4-pin power connector with ignition input.
  Molex 43045 series or compatible, 3.00 mm Micro MF connector with lock, max. 8.5 A
- Power limit:
  Internal and external 3.3 V power max. 20 W; internal and external 5 V power max. 30 W; internal and external power is related to m.2 connectors, USB, FAN, SATA power and display
- AMD® firmware Trusted Platform Module
  TPM 2.0 support (Infineon SLB 9670) (R2312 variants OEM only)
- Operating temperature: 0 °C to +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: stand alone, optional VESA, optional hat rail
- Dimensions approx.: 117 x 51 x 115 mm
- Weight approx.: 700g + options

3 Interfaces

3.1 Connection Overview

The EM BOX® PC is equipped with the following standard interfaces:

1 – 2x Mini-DP++ connector

2 – Dual-USB 3.2 Gen2 port, type A

3 – 2x Ethernet 10/100/1000/2500 Mbit/s (RJ45), port 1 supports WoL

4 – Power supply

5 – Auxiliary power button (accessible with i. e. a paperclip)

5a – Power button (optional)

6 – Up to 2x Serial port RS-232/485 and RS232 (optional)

7 – Sound 3.5 mm MIC in / headphone out (optional)

8 – USB 3.2 Gen2 port, type A

9 – MicroSD card slot

10 – Up to 5x SMA connector (optional, OEM/ODM only)

11 – Internal microSIM card slot

The following illustrations show all interfaces available in EM BOX® PC. Depending on the variant and its configuration, the number of interfaces might be different.

Front View

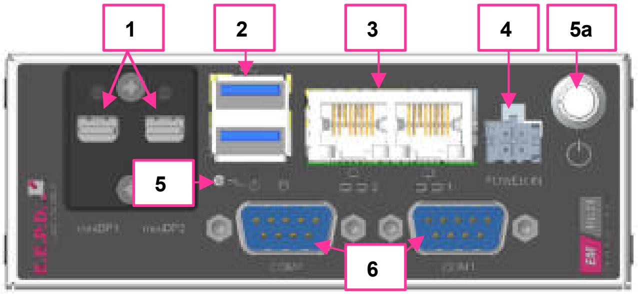


Fig. 13: EM BOX® PC NUCR front view

Rear View

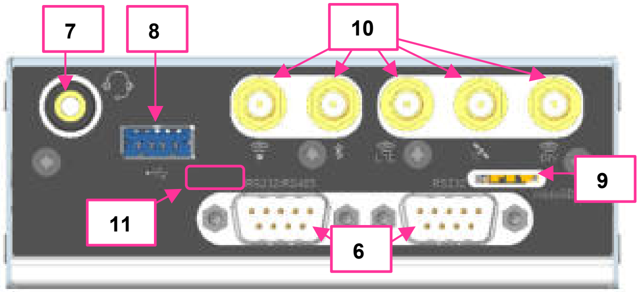


Fig. 14: EM BOX® PC NUCR rear view

3.2 Mini Display Ports

Standard pin assignment

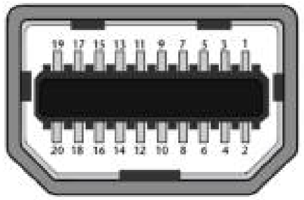


Fig. 15: Mini DisplayPort schematic

Important Note:

There are two types of DisplayPort cables available:

If you connect the display directly to the Mini DP, please use cable with Pin 20 not connected.

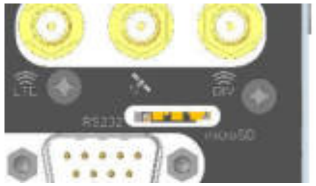
If you use active cables/adapters (e. g. Mini DP to DP, Mini DP to HDMI), please use cable with Pin 20 (supply voltage) on both ends that are connected.

Possible effects if wrong cable is used:

- System might not start up properly.
- Dongle doesn't work properly (e. g. black display).

3.3 MicroSD Slot

Standard pin assignment



To lock the card, slide it completely into the slot until you hear a click. To remove it, first push the card inwards.

Fig. 16: MicroSD slot

3.4 USB 3.2 Gen2 Ports

Standard pin assignment

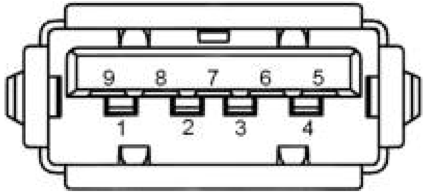


Fig. 17: USB 3.2 schematic

3.5 2.5 Gigabit Ethernet Dual-Port

Standard pin assignment

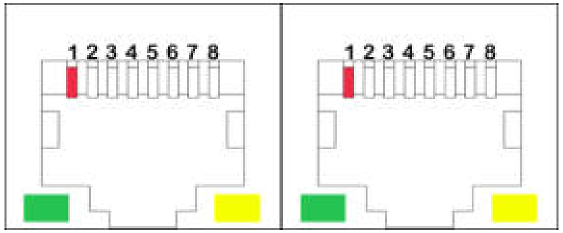


Fig. 18: Dual-Ethernet schematic

Yellow LED
Speed-LED is on during 1 or 2.5 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.

3.6 Power Connector (DC)

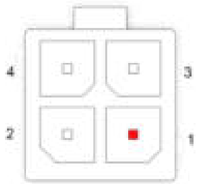


Fig. 19: Power connector schematic

Counterpart - plug:

Molex 43045 series or compatible
3.00 mm micro MF connector with lock, max. 8.5 A

Pin	Signal	Description
1	GND_IN, max. 7.5 A	Ground
2	GND_IN, max. 7.5 A	Ground
3	PVIN, max. 7.5 A	DC+ (min. 8 V to max. 32 V)
4	KL_15*, max. 7.5 A	Ignition

Tab. 3: Pin assignment power connector

* KL_15: ignition enable pin for automotive applications.
The KL_15 pin serves as the ignition enable signal, commonly used in automotive environments.
By default, KL_15 is disabled in the BIOS setup (see chapter *6.4.4*)

When enabled:

- Automatic system startup when ignition is switched on
- Controlled shutdown when the ignition is turned off, using two adjustable timers:
  - Timer 1 – normal shutdown;
  - Timer 2 – forces a hard power-off, if normal shutdown fails

Both timers can be set via the „ignition signal“-setting in the BIOS-Setup.
The Countdown range is 1 to 65535 seconds. Default is 180 seconds – meaning the system will shut down 180 seconds after the ignition is turned off.

3.7 Power Button (optional)

Press the power button (*Fig. 20*) 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.

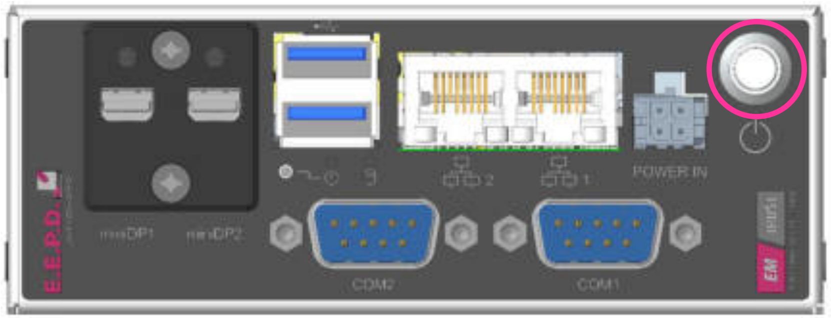


Fig. 20: Power button

3.8 Auxiliary Power Button | Power and HDD/SSD LED

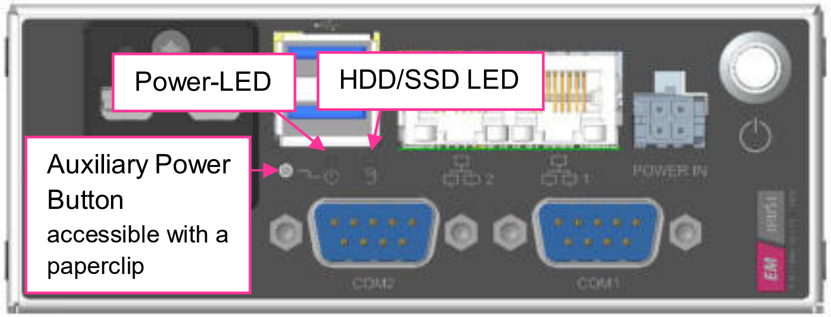


Fig. 21: Auxiliary power button | power and HDD/SSD-LED

3.9 Serial Ports (optional)

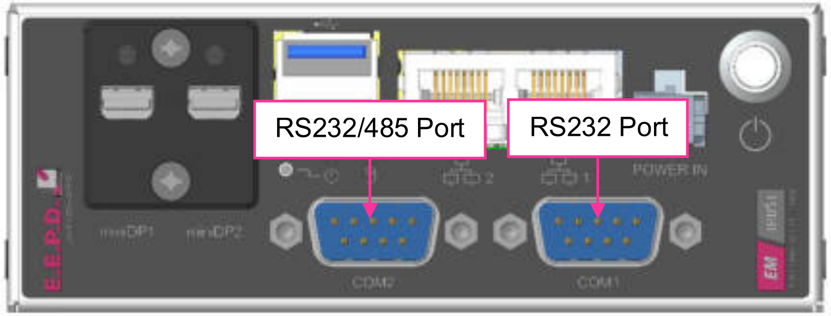


Fig. 22: Serial ports front side option

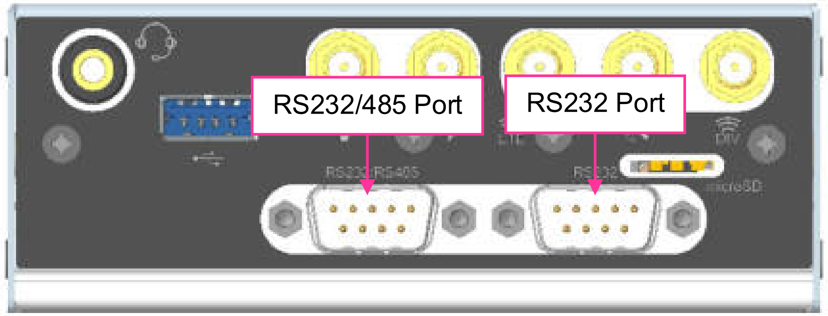


Fig. 23: Serial ports rear side option

This option must be enabled in the BIOS → *UART Configuration Options*
The serial RS232/RS485 interface is provided by a multiprotocol transceiver. The RS485 mode is available as a full duplex configuration only. The RS232 mode is connected to four wires. The connector is a standard 9-pin D-Sub connector (*Fig. 24*).

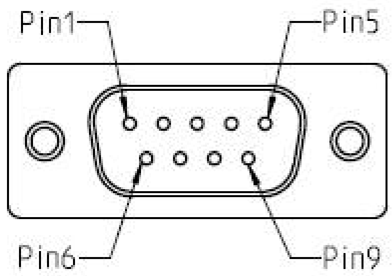


Fig. 24: 9-pin D-SUB connector

9-Pin D-Sub	Signal RS-232	Signal RS-485 FDX only	Signal RS-485/HDX For Win 10/11 only
1	-	RS485-TX_N	RS485-RX/TX_N
2	-	-	
3	RXD	RS485-TX_P	RS485-RX/TX_P
4	RTS	-	
5	TXD	RS485-RX_P	
6	CTS	-	
7	-	RS485-RX_N	
8	-	-	
9	VCC 5 V +/-5%, max. 500 mA not fused	VCC 5 V +/-5%, max. 500 mA not fused	VCC 5 V +/-5%, max. 500 mA not fused

Tab. 4: Pin assignment RS232/RS485

4 Opening the System

All internal installations may only be performed at an ESD-protected workstation.

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

1. Turn off the system and disconnect from the electrical outlet.
2. Remove the 10 screws (M3X4) (3 each side, 4 on the back, see *Fig. 25*).
3. Lift the cover away from the system (*Fig. 26*).
4. The assembly is carried out in reverse order.

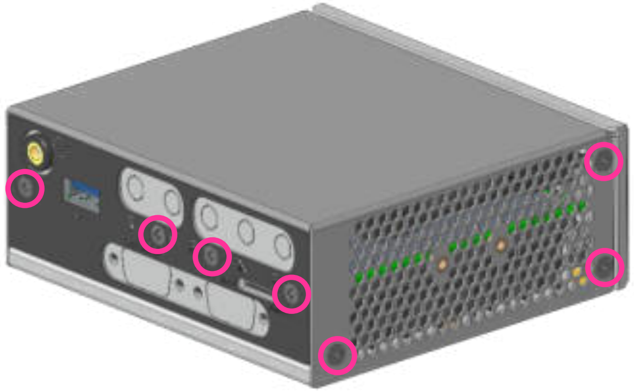


Fig. 25: Remove screws

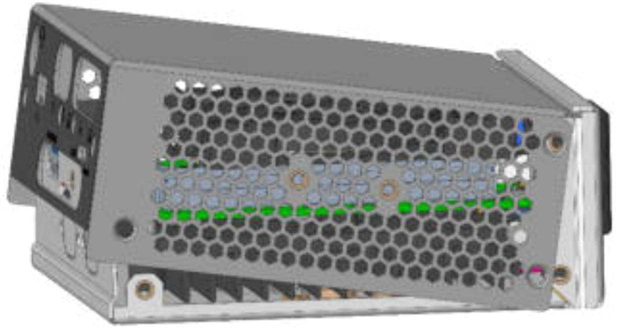


Fig. 26: Cover lifting

4.1 Installing MicroSIM Card

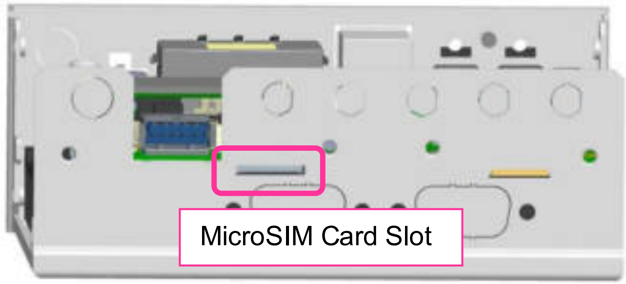


Fig. 27: Open housing | MicroSIM card slot

To lock the card, fully insert it into the slot (*Fig. 27*). Make sure the golden contacts are facing downwards.
To remove the card, first push it inwards.

4.2 Installing M.2 Modules/SSD

Insert the module into the corresponding slot (*Fig. 29*) at an angle. Press it down on the side that protrudes and secure it with the screw provided.

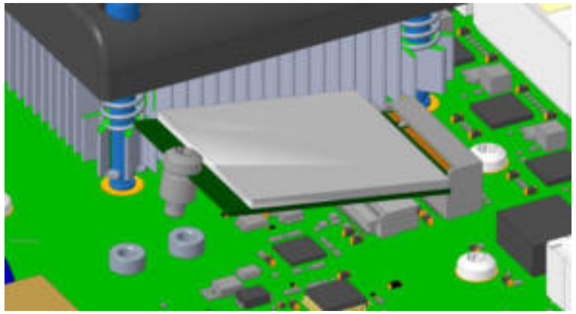


Fig. 28: M.2 module assembly example

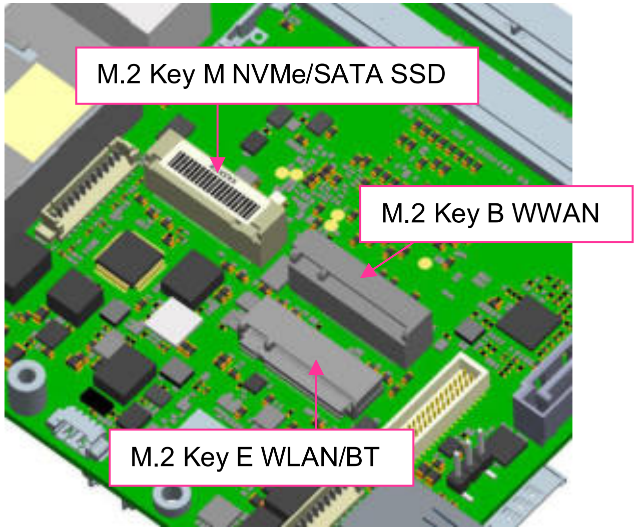


Fig. 29: M.2 module positions

4.3 Installing RAM Modules

To install the memory modules, the battery holder must be loosened by the marked screw:

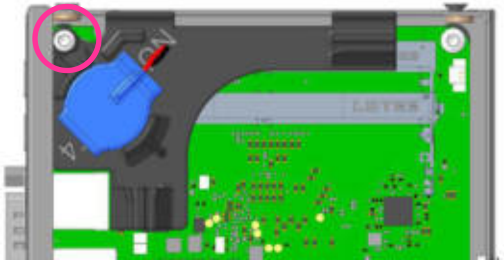


Fig. 30: Installing SO-DIMM modules

Use only 1.2 V DDR SO-DIMM modules compliant with the DDR4 standard.
Dual channel DDR4 SO-DIMM memory, max. 2x 32 GB, up to 3200 MT/s, with ECC support.

Assembly:
First slide RAM module into the RAM socket.
Then press the module in direction to the board till you hear it snap.

Disassembly:
First press both clamps outwards.
Then the RAM module will set upright automatically.
Remove the module from the socket.

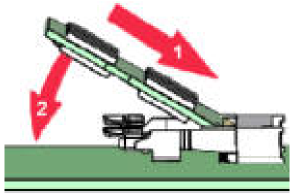


Fig. 31: RAM assembly

E.E.P.D. ...just embedded!

5 Start-up Guide

If connections are no longer accessible after system installation, connect all cables before final mounting. If necessary, also insert the microSD card and the microSIM card in advance.

WARNING

Only connect the power cable when the power supply is switched off.

CAUTION

Only insert the microSIM card when the system is switched off.
Only remove the microSIM card when the system is switched off.

Before commissioning, we recommend connecting or inserting:

- Monitor
- USB keyboard and mouse
- Network cable (optional)
- MicroSD card and microSIM card (optional)
- DC power supply

Other plug & play devices can be connected after commissioning.

5.1 Switching on the Device / Operation

After all preparations have been made, the Box PC system is ready to be connected to the power supply.
Press the power button to switch on the PC. When the system is powered, the Power LED on the optional power button will be on. When the system boots, the Status LED on the housing lights up to indicate that all internal voltages are at normal levels.
If an operating system is installed, it will start now. An operating system installation can be performed with installation media such as USB stick, USB DVD drive or PXE remote network start. The BIOS boot order has to be adjusted accordingly. To enter the BIOS setup, press the [ESC] key immediately after switching on.
Please refer to the operating system manual for switching off / shutting down.

6 BIOS

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 [ESC] immediately to enter Setup.

6.2 Most Common Settings

1. Firmware / BIOS Version: *Main Menu* (chapter 6.3)

2. Boot / PXE Boot: *Boot Menu* (chapter 6.6)

3. Fan control, boost mode:
   Fan control (chapter 6.4.10.2.2):
      Setup Utility → AMD CBS → NBIO Common Options → *Fan Control*

   Boost mode (chapter 6.4.10.1):
      Advanced Menu → AMD CBS → *Zen Common Options* → Core Performance Boost

4. Change shared graphics memory (chapter 6.4.10.2.1):
   Advanced Menu → NBIO Common Options → *GFX Configuration* → UMA Frame Buffer Size

5. USB power off in S5 / VCC control (chapter 6.4.4):
   Advanced Menu → *NUCX Advanced Options*

6.3 Main Menu

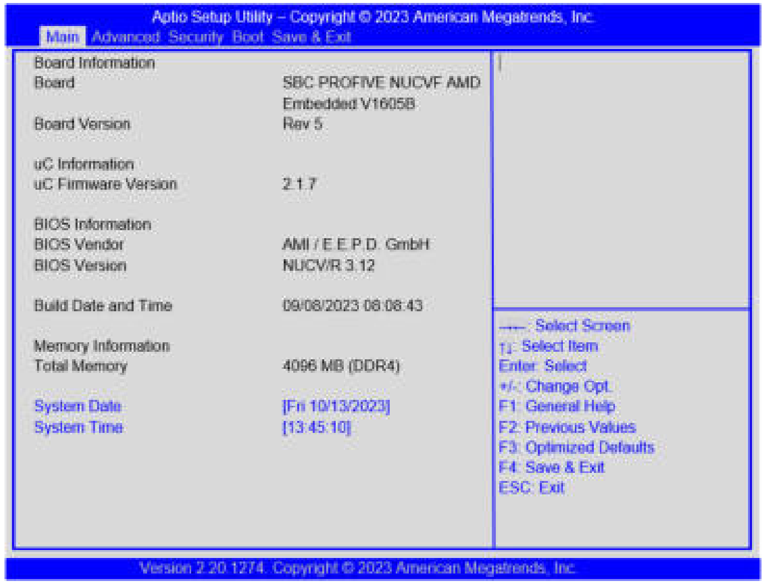


Fig. 32: Main Menu

This setup menu shows an overview of board configuration, CPU type, memory and firmware revisions.

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. 5: Main Menu

E.E.P.D. ...just embedded!

6.4 Advanced Menu

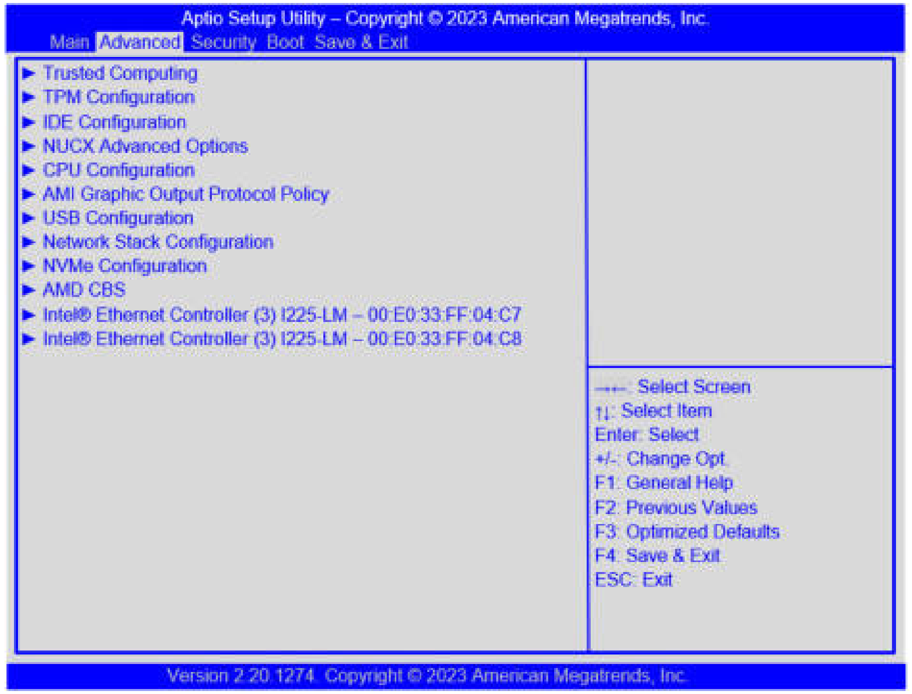


Fig. 33: Advanced Menu

BIOS Settings	Options	Description
Trusted Computing	See submenu	Configure trusted computing options
TPM Configuration	See submenu	TPM configuration menu
IDE Configuration	See submenu	Provides information about SATA configuration
NUCX Advanced Options	See submenu	Configure: PIC watchdog, KL15 support, Wake on LAN, Power LED mode, WWAN Radio Operation and Power
CPU Configuration	See submenu	CPU information
AMI Graphic Output Protocol Policy	See submenu	Graphics information
USB Configuration	See submenu	Configure the USB support
Network Stack Configuration	See submenu	Network Stack configuration menu
NVME Configuration	See submenu	This function shows the connected NVMe devices
AMD CBS	See submenu	AMD Custom BIOS Settings menu

Tab. 6: Advanced Menu

6.4.1 Trusted Computing

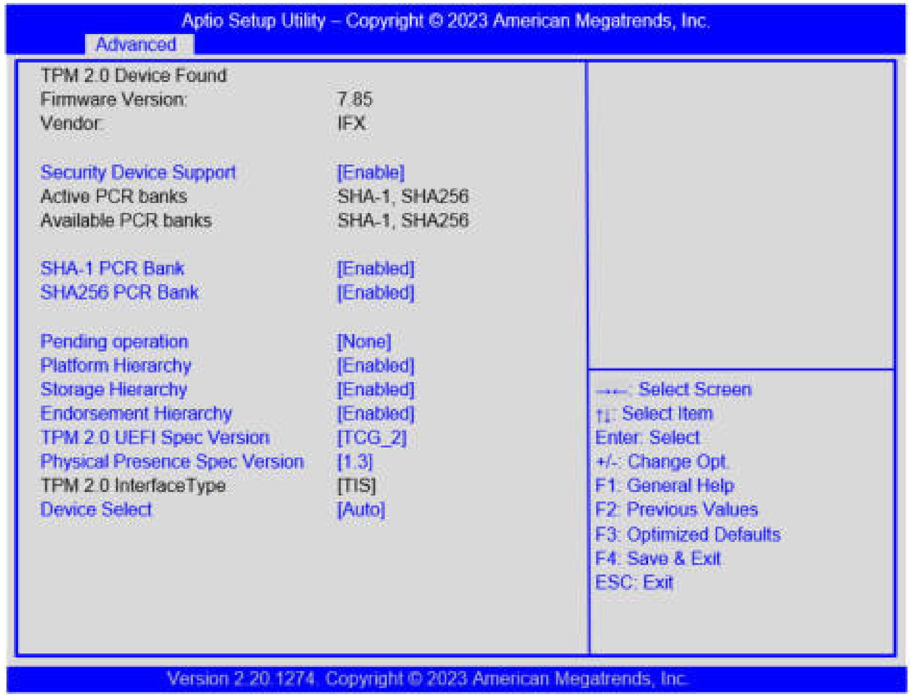


Fig. 34: Trusted Computing

BIOS Settings	Options	Description
Security Device Support	<Enable>* <Disable>	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	<Enable>* <Disable>	Enable or Disable SHA-1 PCR Bank.
SHA256 PCR Bank	<Enable>* <Disable>	Enable or Disable SHA256 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	<Enable>* <Disable>	Enable or Disable Platform Hierarchy
Storage Hierarchy	<Enable>* <Disable>	Enable or Disable Storage Hierarchy
Endorsement Hierarchy	<Enable>* <Disable>	Enable or Disable Endorsement Hierarchy
TPM 2.0 UEFI Spec Version	<TCG_1_2> <TCG_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	<Auto>* <TPM 1.2> <TPM 2.0>	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. 7: Trusted Computing

6.4.2 TPM Configuration

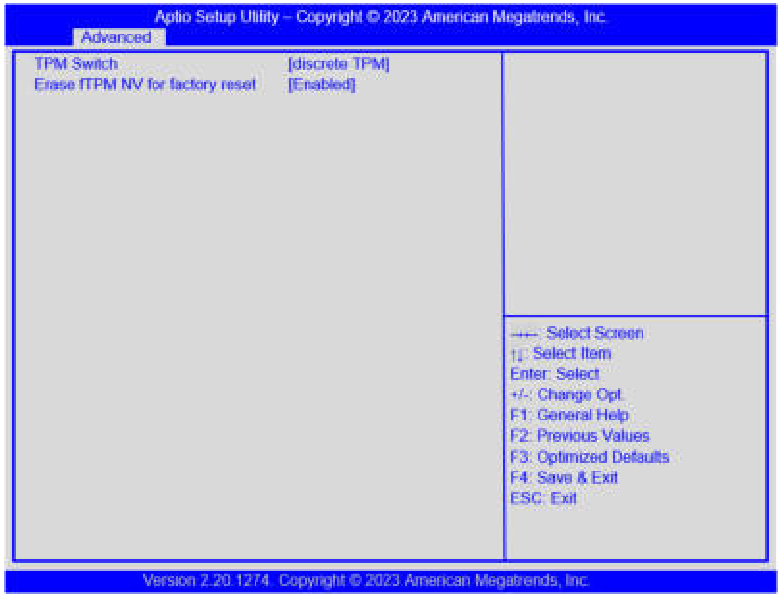


Fig. 35: AMD TPM Configuration Menu

BIOS Settings	Options	Description
TPM Switch	<AMD firmware TPM> <disable TPM> <discrete TPM>*	
Erase fTPM NV for factory reset	<Enable>* <Disable>	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. 8: TPM Configuration Menu

6.4.3 IDE Configuration

This page provides information about SATA configuration.

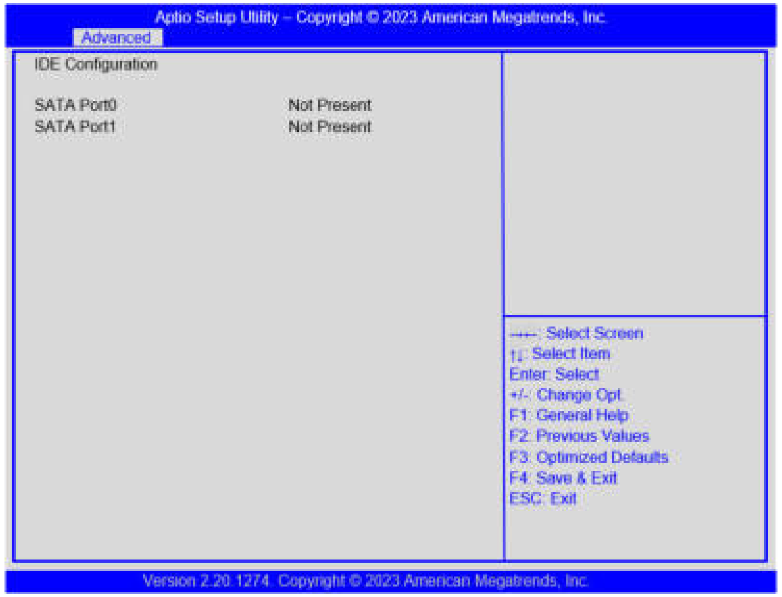


Fig. 36: IDE Configuration

6.4.4 NUCX Advanced Options

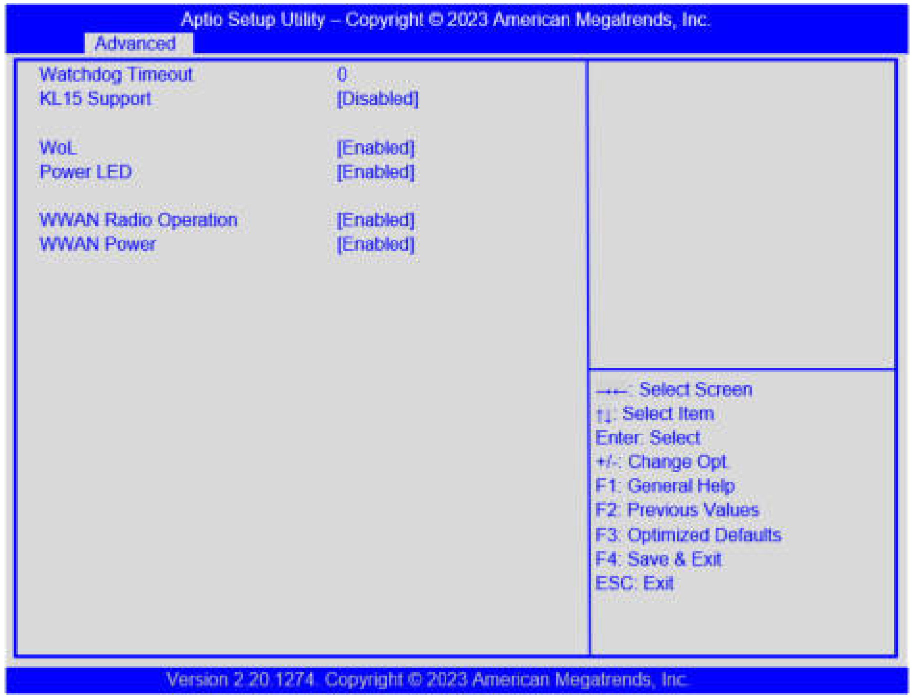


Fig. 37: NUCX Advanced Options

BIOS Settings	Options	Description
Watchdog Timeout		Seconds before watchdog times out. Set to 0 to disable watchdog. Values between 1 and 30 are set to 30. Range: 30-240 seconds.
KL15 Support	<Enabled> <Disabled>*	Enable/Disable KL15 Support (see chapter 3.6)
WoL	<Enabled>* <Disabled>	Enable/Disable Wake on LAN
Power LED	<Enabled>* <Disabled>	Enable/Disable Power LED
WWAN Radio Operation	<Enabled>* <Disabled>	Enable/Disable WWAN Radio Operation
WWAN Power	<Enabled>* <Disabled>	Enable/Disable WWAN Power

Tab. 9: NUCX Advanced Options

Enabling watchdog leads to the reset of the board after time out. Please contact EEPD for further instructions.

6.4.5 CPU Configuration

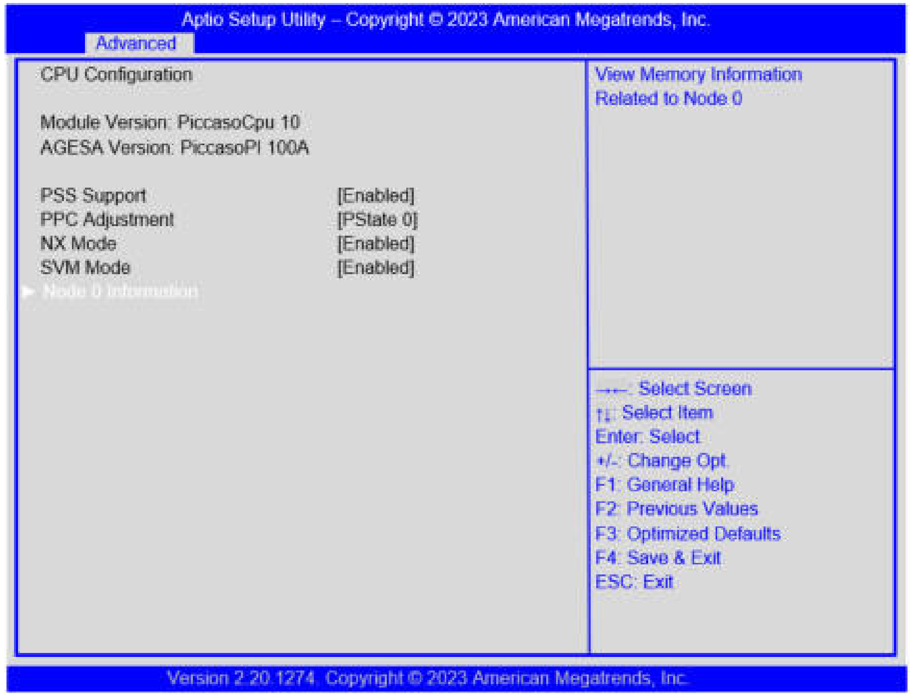


Fig. 38: CPU Configuration

BIOS Settings	Options	Description
Node 0 Information	see submenu	Detailed Information on CPU. Processor Family | Processor Model | CPU ID | Max./Min. Speed (Frequency) | Cache

Tab. 10: CPU Configuration

6.4.6 AMI Graphic Output Protocol Policy

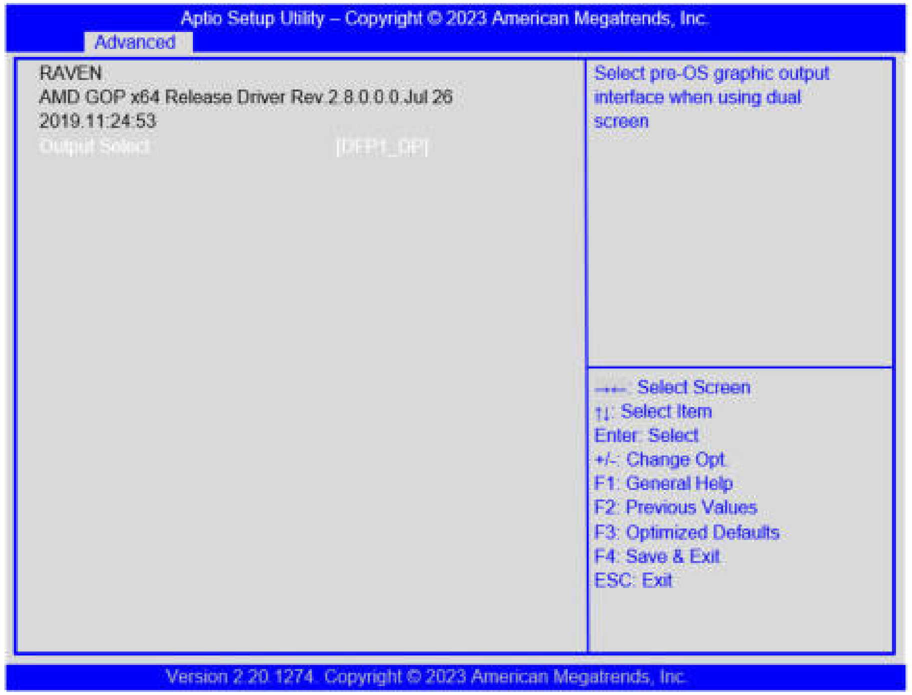


Fig. 39: AMI Graphic Output Protocol Policy

6.4.7 USB Configuration

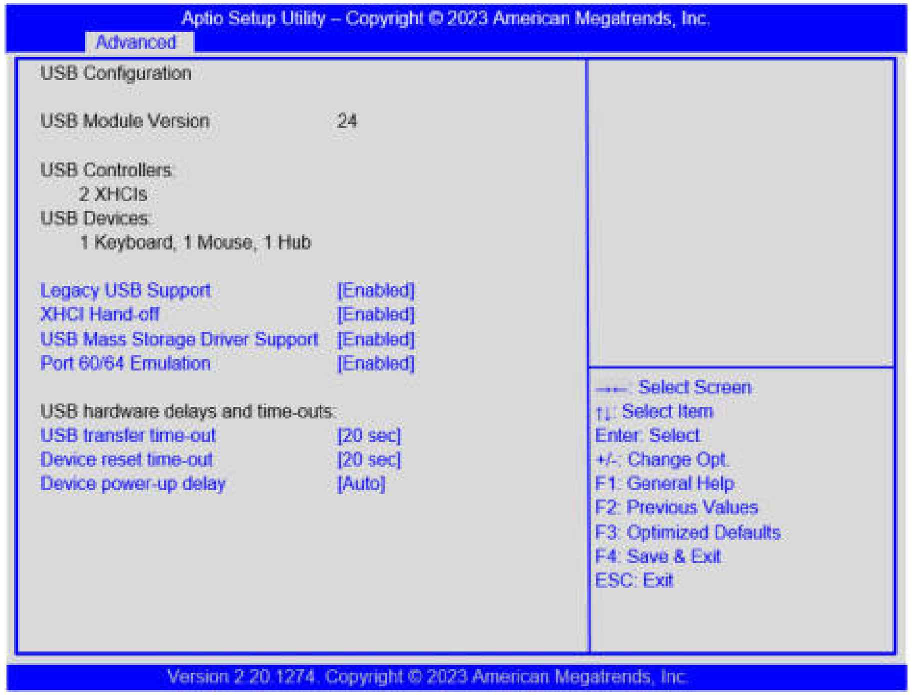


Fig. 40: USB Configuration

BIOS Settings	Options	Description
USB Module Version		Shows the USB module version used by the UEFI firmware
USB Controllers		Shows the number of XHCI controllers that are available.
USB Devices		Shows the connected USB devices
Legacy USB Support	<Enabled>* <Disabled> <Auto>	Select Enabled to support legacy onboard USB devices. Select Auto to disable support for legacy USB devices if no legacy USB devices are present. Select Disabled to have all USB devices available for EFI applications only.
XHCI Hand-off	<Enabled>* <Disabled>	This is a workaround for operating systems without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support	<Enabled>* <Disabled>	Enable/Disable USB Mass Storage Driver Support
Port 60/64 Emulation	<Enabled>* <Disabled>	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>*	Select time-out section. The time-out value for control, mass 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>	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. 11: USB Configuration

6.4.8 Network Stack Configuration

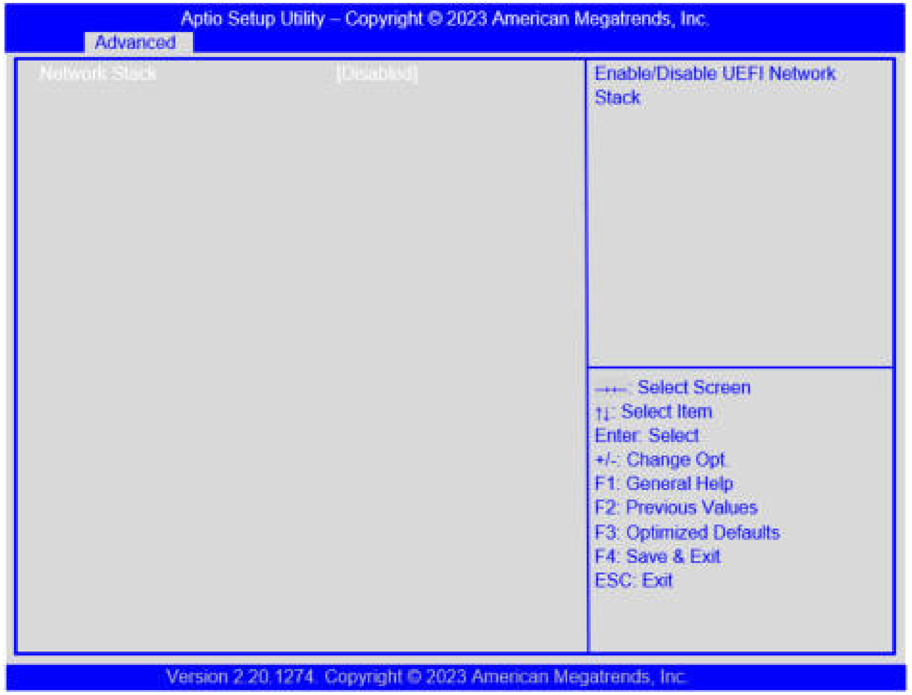


Fig. 41: Network Stack Configuration

BIOS Settings	Options	Description
Network Stack	<Enable> <Disable>*	Enable/Disable UEFI Network Stack
When the above function is set to Enabled, the following functions are available for configuration:		
Ipv4 PXE Support	<Enabled>* <Disabled>	Select Enabled to enable IPv4 PXE boot support.
Ipv4 HTTP Support	<Enabled> <Disabled>*	Select Enabled to enable IPv4 HTTP boot support.
Ipv6 PXE Support	<Enabled>* <Disabled>	Select Enabled to enable IPv6 PXE boot support.
Ipv6 HTTP Support	<Enabled> <Disabled>*	Select Enabled to enable IPv6 HTTP boot support.
PXE boot wait time		This function allows you to set the waiting time for pressing the ESC key to cancel the PXE boot process. Press “+” or “-“ on your keyboard to change the value. The default setting is 0.
Media detect count		This function allows you to specify how often media should be checked. Press “+” or “-2 on your keyboard to change the value. The default setting is 1.

Tab. 12: Network Stack Configuration

E.E.P.D. ...just embedded!

6.4.9 NVME Configuration

Fig. 42: NVME Configuration

BIOS Settings	Options	Description
NVME Configuration		This function shows the connected NVME devices.

Tab. 13: NVME Configuration

6.4.10 AMD CBS

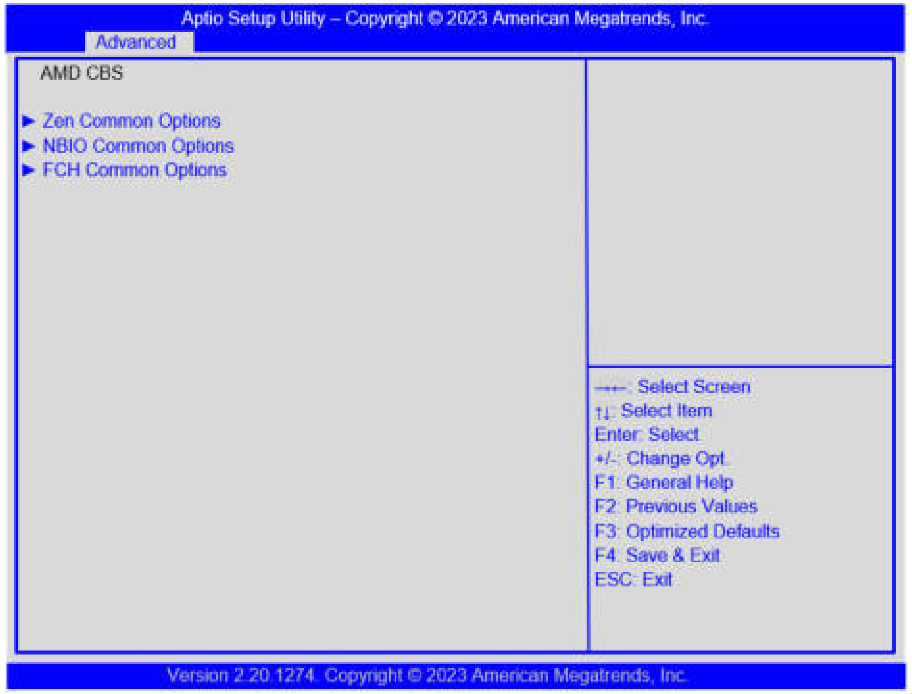


Fig. 43: AMD CBS Menu

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. 14: AMD CBS Menu

6.4.10.1 Zen Common Options

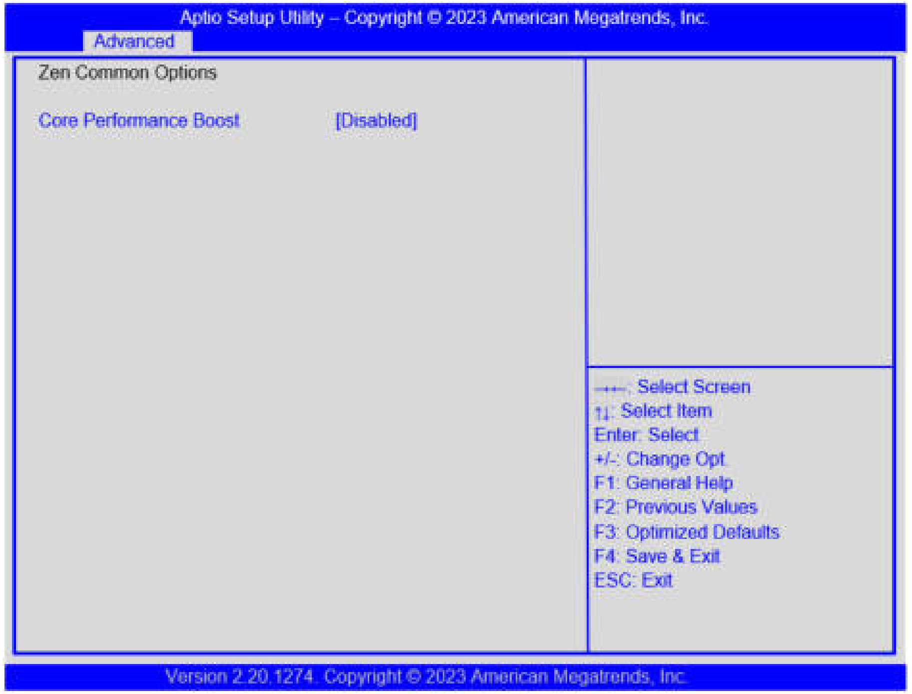


Fig. 44: Zen Common Options

BIOS Settings	Options	Description
Core Performance Boost	<Disabled>* <Auto>	Set Core Performance Boost to Disabled or Auto.

Tab. 15: Zen Common Options

6.4.10.2 NBIO Common Options

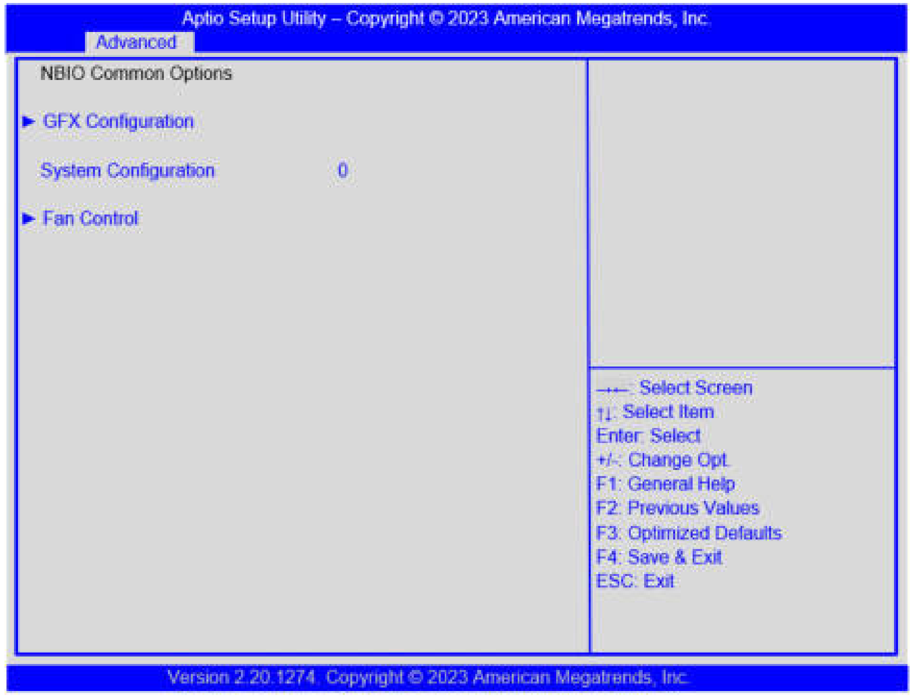


Fig. 45: NBIO Common Options

BIOS Settings	Options	Description
GFX Configuration	See submenu	GFX Configuration options
System Configuration		With this function the max. system performance can be set. 0 = default, value is read from the corresponding register of the CPU.
Fan Control	See submenu	Fan Control options

Tab. 16: NBIO Common Options

6.4.10.2.1 GFX Configuration

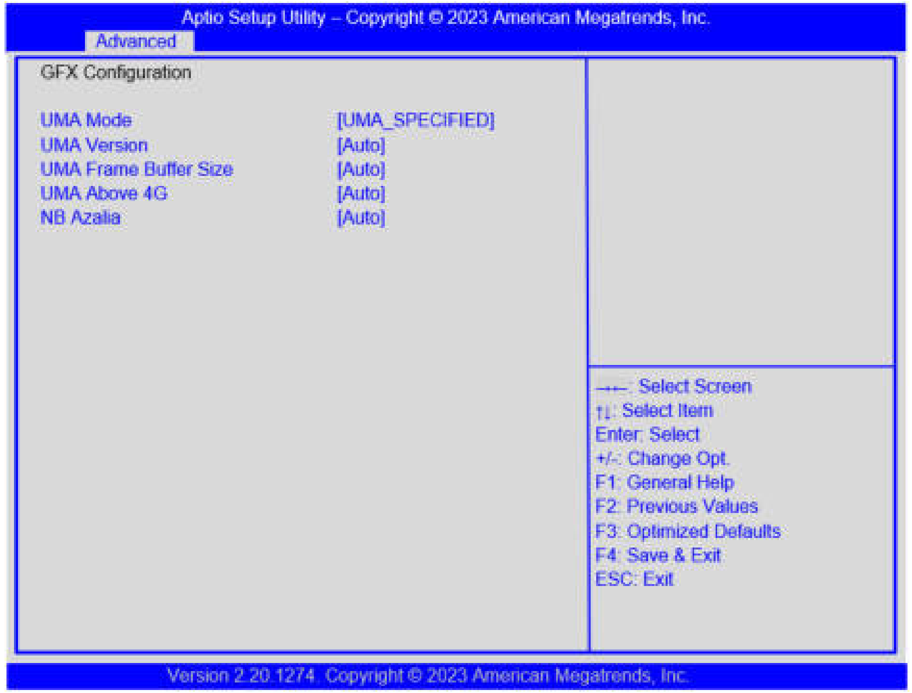


Fig. 46: GFX Configuration

BIOS Settings	Options	Description
UMA Mode	<Auto> <UMA_SPECIFIED>* <UMA_AUTO>	Select UMA Mode.
UMA Version	<Legacy> <Non-Legacy> <Hybrid Secure> <Auto>*	UMA Legacy Version, UMA non-legacy version or Hybrid Secure
UMA Frame Buffer Size	<Auto>* <64M> <128M> <256M> <384M> <512M> <80M> <96M> <768M> <1G> <2G> <3G> <4G> <6G> <8G> <16G>	Set UMA FB size. This allows the system to manage the amount of shared memory for graphics.
UMA Above 4G	<Disabled> <Enabled> <Auto>*	This option enables or disables 64-bit capable devices to be decoded in above 4G address space. It only works if the system supports 64-bit PCI decoding.
NB Azalia	<Disabled> <Enabled> <Auto>*	Select Enabled to enable the Azalia High Definition Audio feature.

Tab. 17: GFX Configuration

6.4.10.2.2 Fan Control

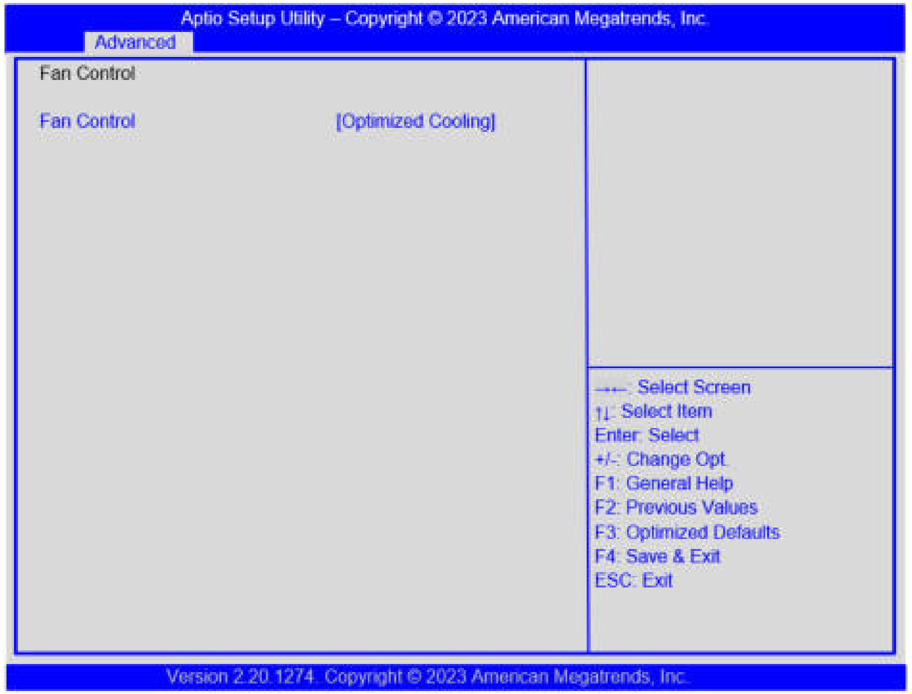


Fig. 47: Fan Control

BIOS Settings	Options	Description
Fan Control	<Optimized Cooling>* <Silent Mode> <Max Cooling>	Optimized Cooling → automatic PWM control Silent mode → less noise (30%) Maximum Cooling → always on (100%)

Tab. 18: Fan Control

6.4.10.3 FCH Common Options

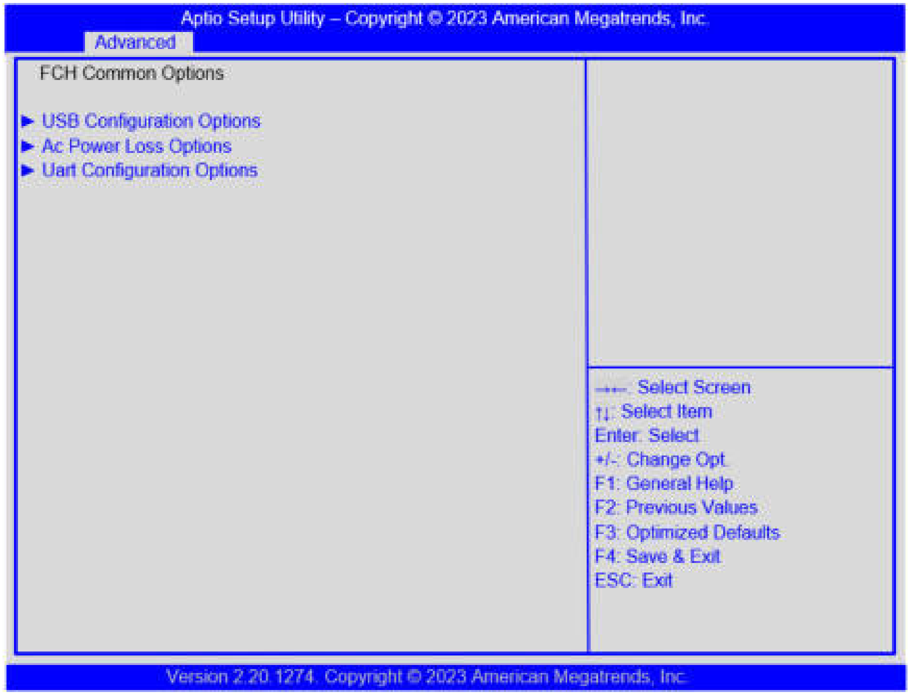


Fig. 48: FCH Common Options

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

6.4.10.3.1 USB Configuration Options

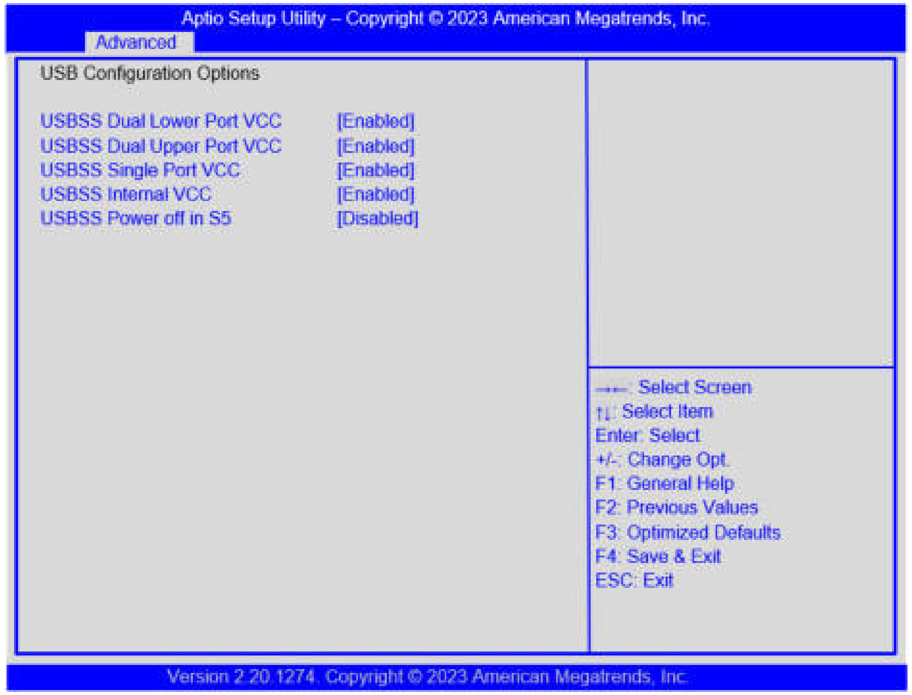


Fig. 49: USB Configuration Options

BIOS Settings	Options	Description
USBSS Dual Lower Port VCC	<Enabled>* <Disabled>	This function allows you to enable or disable the power for the Front Bottom USB port.
USBSS Dual Upper Port VCC	<Enabled>* <Disabled>	This function allows you to enable or disable the power for the Front Top USB port.
USBSS Single Port VCC	<Enabled>* <Disabled>	This function allows you to enable or disable the power for the Rear USB port.
USBSS Internal VCC	<Enabled>* <Disabled>	This function allows you to enable or disable the power for the internal USB header.
USBSS Power Off in S5	<Enabled> <Disabled>*	Enable/Disable the USB connector VCC in S5 Mode

Tab. 20: USB Configuration Options

Note:
In order to not exclude yourself from the BIOS setup, at least one USB port should be enabled at all times. In case you select the “Disabled” option on all ports, the “USBSS Dual Lower Port VCC” port will automatically be enabled by the system.

6.4.10.3.2 Ac Power Loss Options

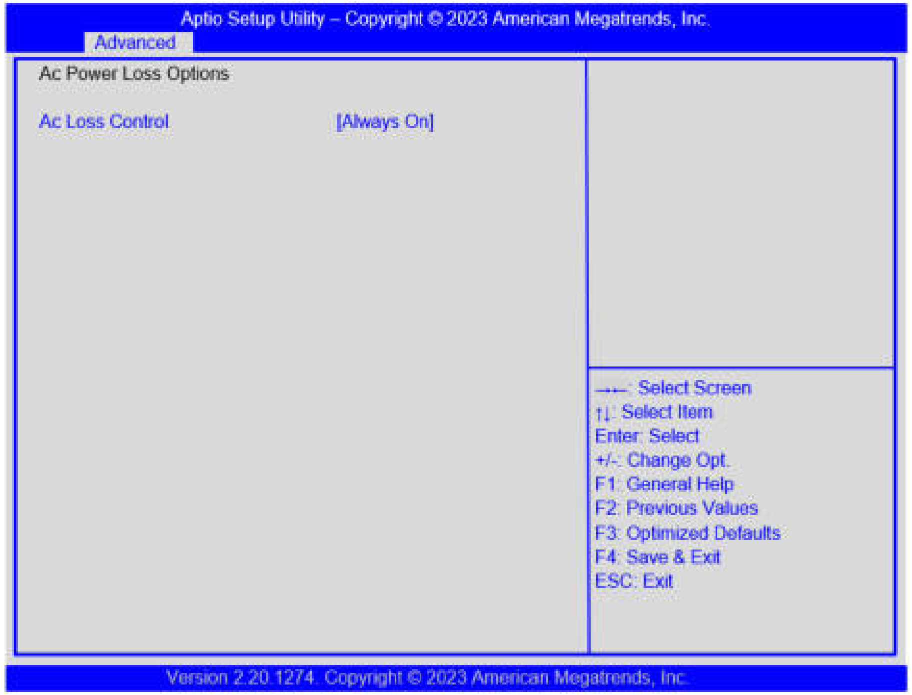


Fig. 50: Ac Power Loss Options

BIOS Settings	Options	Description
Ac Loss Control	<Always Off> <Always On>* <Previous>	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

6.4.10.3.3 UART Configuration Options

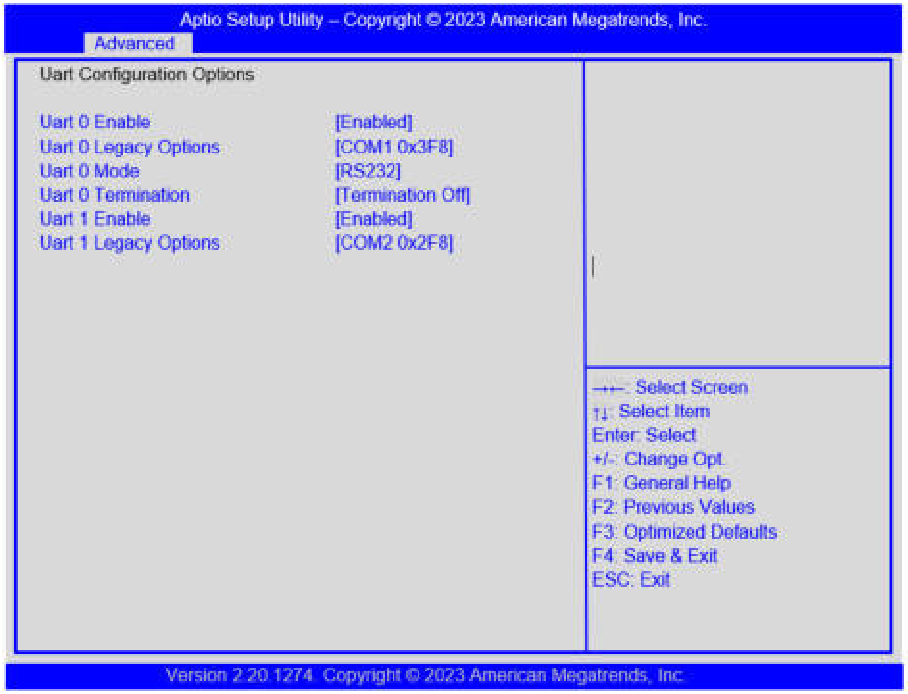


Fig. 51: UART Configuration Options

BIOS Settings	Options	Description
UART 0 Enable	<Enabled>* <Disabled> <Auto>	This function allows you to enable or disable the UART0 port.
UART 0 Legacy Options	<Disabled> <COM1 0x3F8>* <COM2 0x2F8> <COM3 0x3E8> <COM4 0x2E8> <Auto>	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 0 Mode	<RS232>* <RS485 Half-Duplex> <RS485 Full-Duplex>	Shows the UART Modes
UART 0 Termination	<120 Ohm diff> <Termination Off>*	Select UART 0 transceiver termination.
UART 1 Enable	<Enabled>* <Disabled> <Auto>	This function allows you to enable or disable the UART1 port.
UART 1 Legacy Options	<Disabled> <COM1 0x3F8> <COM2 0x2F8>* <COM3 0x3E8> <COM4 0x2E8> <Auto>	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

6.5 Security Menu

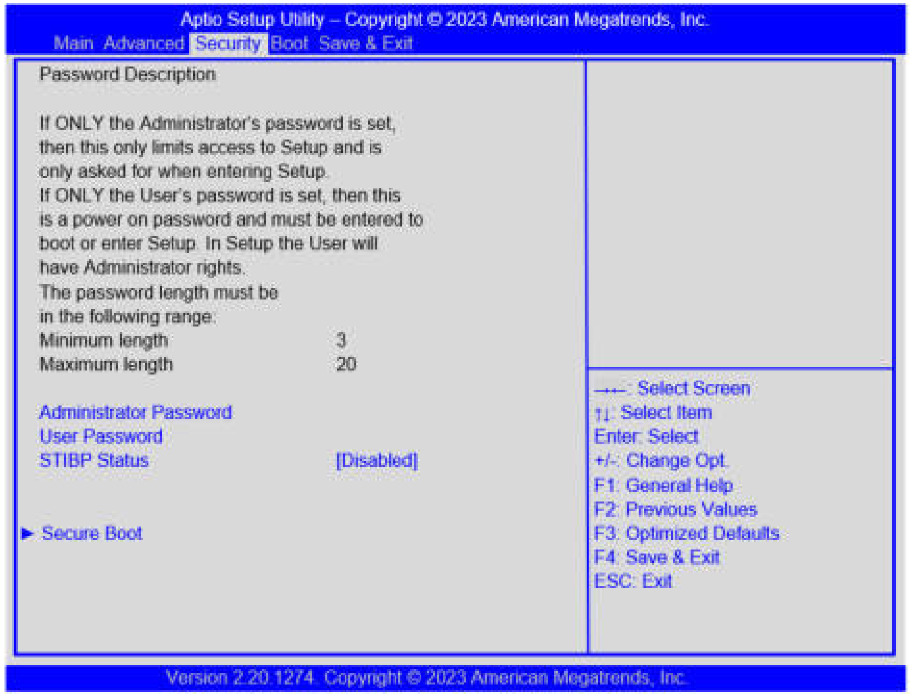


Fig. 52: Security Menu

BIOS Settings	Options	Description
Administrator Password		Use this feature to set the administrator password required to enter the BIOS setup utility. The password should be 3 to 20 characters long. - this controls access to the BIOS setup ONLY
User Password		Press Enter to create a new, or change an existing User password. - this password must be entered at each system start or boot and also has administrator rights in the setup.
STIBP Status	<Disabled>* <Enabled>	The STIBP-BIOS function (Single Thread Indirect Branch Predictor, STIBP) mitigates the Spectre variant 2 vulnerability on systems with AMD processors. Enabling STIBP may have some performance impact depending on system load.
Secure Boot	See submenu	Secure Boot Options

Tab. 23: Security Menu

6.5.1 Secure Boot

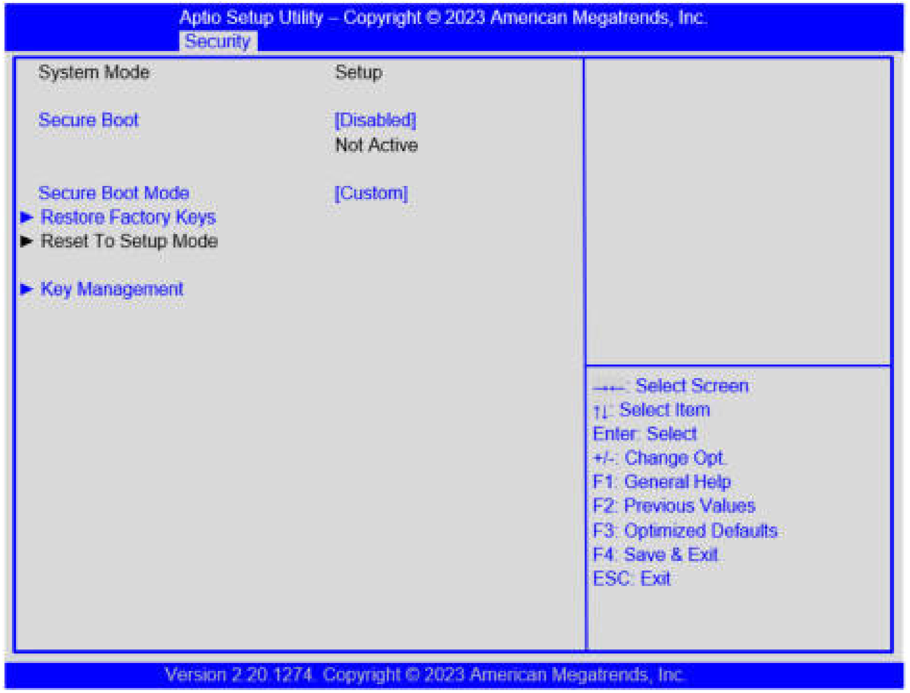


Fig. 53: Secure Boot

BIOS Settings	Options	Description
Secure Boot	<Disabled>* <Enabled>	This function allows you to select the desired secure boot mode for the system. When the secure boot mode is set to custom, key management functions are available for configuration.
Secure Boot Mode	<Standard> <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

6.5.1.1 Key Management

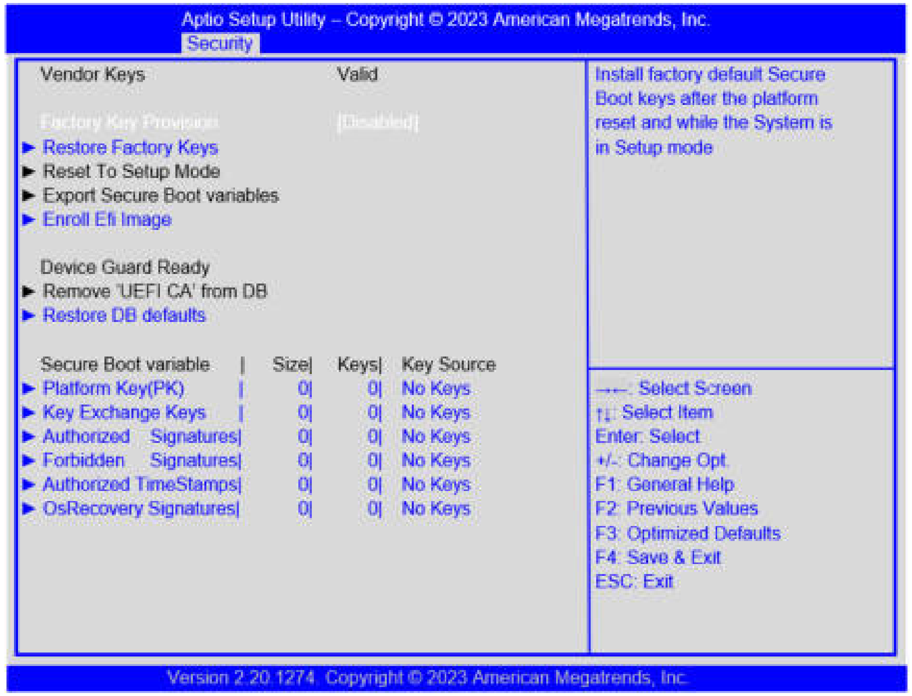


Fig. 54: Key Management

BIOS Settings	Options	Description
Factory Key Provision	<Enabled> <Disabled>*	Select Enabled to install the default secure boot keys set by the manufacturer.
Restore Factory Keys		Force System to User Mode. Install factory default Secure Boot key databases.
Reset to Setup Mode		Delete all secure boot key databases from NVRAM and force the system to setup mode.
Export Secure Boot variables		Use this feature to copy NVRAM content of the secure boot variables to a file in a root folder on a file system device.
Enroll Efi Image		This feature allows the image to run in Secure Boot mode.
Remove 'UEFI CA' from DB		Use this feature to remove the Microsoft UEFI CA certificate from the database.
Restore DB defaults		Restore all DBs to factory defaults settings.
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 2. Authenticated UEFI Variable 3. EFI PE/COFF Image (SHA256) Key Source: Factory, External, Mixed
Key Exchange Keys	<Details> <Export> <Update> <Append>	Enroll Factory Defaults or load certificates from a file: 1. Public Key Certificate: a) EFI_SIGNATURE_LIST

	<Delete>	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 Signatures	<Details> <Export> <Update> <Append> <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 2. Authenticated UEFI Variable 3. EFI PE/COFF Image (SHA256) Key Source: Factory, External, Mixed
Forbidden Signatures	<Details> <Export> <Update> <Append> <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 2. Authenticated UEFI Variable 3. EFI PE/COFF Image (SHA256) Key Source: Factory, External, Mixed
Authorized TimeStamps	<Update> <Append>	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	<Update> <Append>	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

6.6 Boot Menu

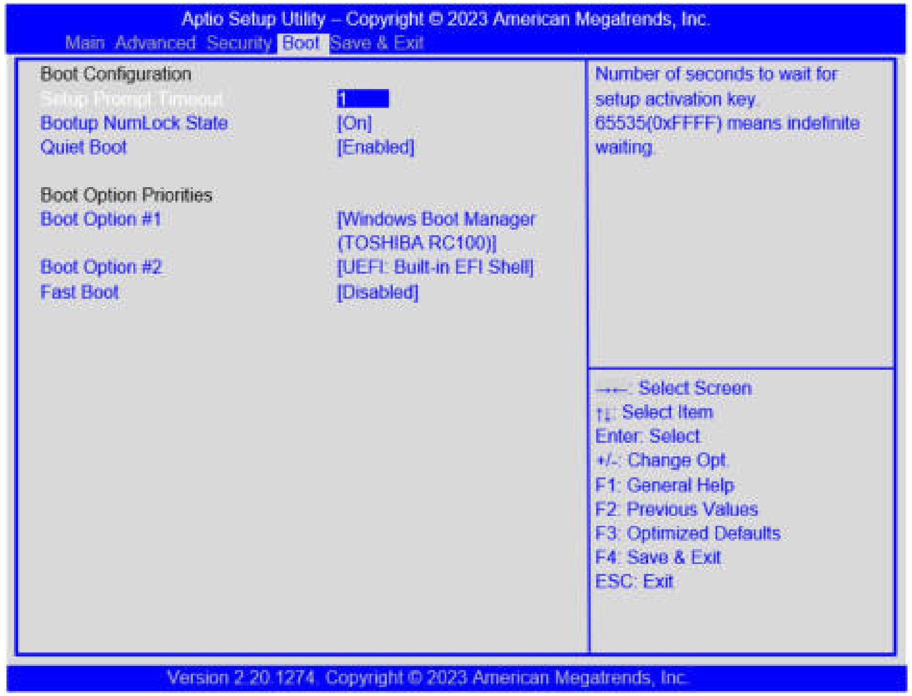


Fig. 55: Boot Menu

If one of the following options is disabled, they will not be available until after OS boot: SATA Support, NVMe Support, Display Support, USB Support, Network Stack Driver Support, Redirection Support.

BIOS Settings	Options	Description
Setup Prompt Timeout		This function allows you to specify the amount of time (in seconds) the BIOS should wait before rebooting the system when the Setup Activation key is pressed. Enter the value 65535 (0xFFFF) that the BIOS should wait indefinitely. The default setting is 1.
Bootup NumLock State	<On>* <Off>	Configuration of Numlock key at power up
Quiet Boot	<Enabled>* <Disabled>	This function allows you to select the screen display between POST messages or the E.E.P.D. logo at startup. Select 'Enabled' to display the E.E.P.D logo instead of the normal POST messages. Select 'Disabled' to display the POST messages.
Boot Option Priorities		This option prioritizes the order of bootable devices from which the system is booted. Press <Enter> on each entry from top to bottom to select devices.
Fast Boot	<Enabled> <Disabled>*	Fast Boot is a BIOS feature that shortens the boot time. The computer will boot with a minimal set of required devices.

Tab. 26: Boot Menu

6.7 Save & Exit Menu

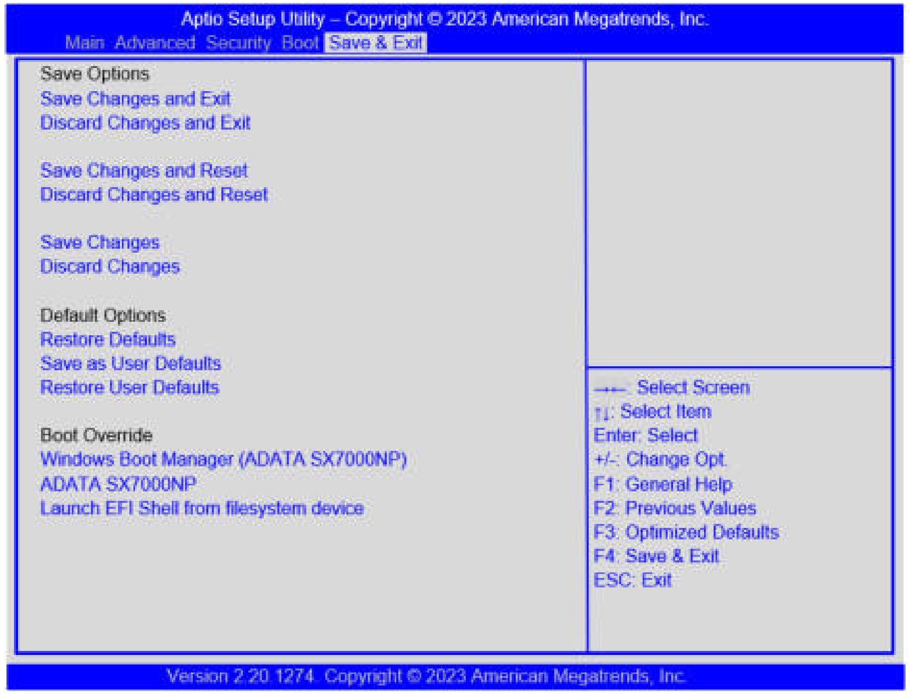


Fig. 56: Save & Exit Menu

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.
Boot Override		Set this feature to override a previously defined boot device.
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

Index of Figures

Index of Tables

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
IoT	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

...just embedded!

systems you can trust

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

...just embedded!