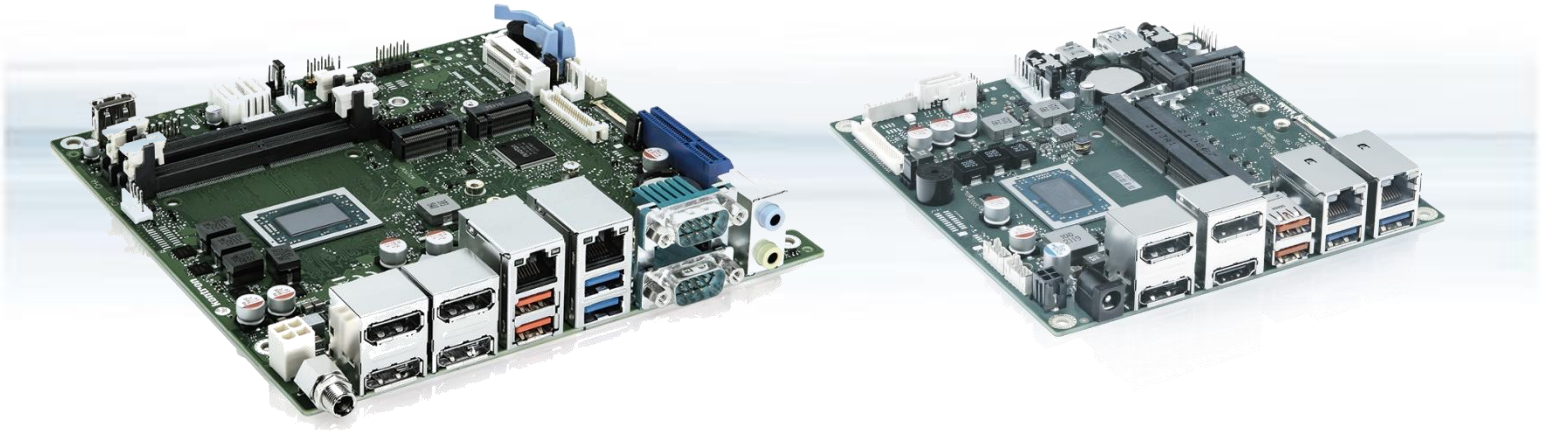
USER GUIDE



BIOS FOR RYZEN EMBEDDED

User Guide Rev. 1.3

POSSIBILITIES START HERE kontron S&T Group

www.kontron.com

BIOS FOR RYZEN EMBEDDED - USER GUIDE

Disclaimer

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

Kontron Europe GmbH

Gutenbergstraße 2
85737 Ismaning
Germany
www.kontron.com

Intended Use

THIS DEVICE AND ASSOCIATED SOFTWARE ARE NOT DESIGNED, MANUFACTURED OR INTENDED FOR USE OR RESALE FOR THE OPERATION OF NUCLEAR FACILITIES, THE NAVIGATION, CONTROL OR COMMUNICATION SYSTEMS FOR AIRCRAFT OR OTHER TRANSPORTATION, AIR TRAFFIC CONTROL, LIFE SUPPORT OR LIFE SUSTAINING APPLICATIONS, WEAPONS SYSTEMS, OR ANY OTHER APPLICATION IN A HAZARDOUS ENVIRONMENT, OR REQUIRING FAIL-SAFE PERFORMANCE, OR IN WHICH THE FAILURE OF PRODUCTS COULD LEAD DIRECTLY TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE (COLLECTIVELY, "HIGH RISK APPLICATIONS").

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

Revision History

Revision	Brief Description of Changes	Date of Issue
1.0	First released version	12/2020
1.1	COM settings updated Power failure recovery settings updated eDP brightness setting removed	03/2021
1.2	Word 2016 issues	03/2021
1.3	Version updated for D3713-V/R, D3714-V/R	06/22

Symbols

The following symbols may be used in this user guide

DANGER	DANGER indicates a hazardous situation which, if not avoided, will result in death or serious injury.
WARNING	WARNING indicates a hazardous situation which, if not avoided, could result in death or serious injury.
NOTICE	NOTICE indicates a property damage message.
CAUTION	CAUTION indicates a hazardous situation which, if not avoided, may result in minor or moderate injury.
	Electric Shock! This symbol and title warn of hazards due to electrical shocks (> 60 V) when touching products or parts of products. Failure to observe the precautions indicated and/or prescribed by the law may endanger your life/health and/or result in damage to your material.
	ESD Sensitive Device! This symbol and title inform that the electronic boards and their components are sensitive to static electricity. Care must therefore be taken during all handling operations and inspections of this product in order to ensure product integrity at all times.
	HOT Surface! Do NOT touch! Allow to cool before servicing.
	Laser! This symbol inform of the risk of exposure to laser beam and light emitting devices (LEDs) from an electrical device. Eye protection per manufacturer notice shall review before servicing.
	This symbol indicates general information about the product and the user guide. This symbol also indicates detail information about the specific product configuration.
	This symbol precedes helpful hints and tips for daily use.

Table of Contents

List of Tables

List of Figures

1 / UEFI BIOS

1.1. Starting the UEFI BIOS

The mainboard uses a Kontron-customized, pre-installed and configured version of Aptio ® V UEFI BIOS based on the Unified Extensible Firmware Interface (UEFI) specification.

The BIOS version covered in this document might not be the latest version. The latest version might have certain differences to the BIOS options and features described in this chapter.

Latest BIOS versions are available for download on the Kontron FTP Server ftp://ftp.kontron.com/Products/Motherboards/Industrial/

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

To start the UEFI BIOS Setup program, follow the steps below:

1. Power on the board.
2. Wait until the first characters appear on the screen (POST messages or splash screen).
3. Press the <F2> key.
4. If the UEFI BIOS is password-protected, a request for password will appear. Enter either the User Password or Supervisor Password.
5. Press <RETURN>.
6. A Setup menu appears.

The UEFI BIOS Setup program uses a hot key navigation system. The hot key legend bar is located at the bottom of the Setup screens. The following table provides a list of navigation hot keys available in the legend bar.

Table 1: Navigation Hot Keys Available in the Legend Bar

Sub-screen	Description
<F1>	<F1> key invokes the General Help window
<->	<Minus> key selects the next lower value within a field
<+>	<Plus> key selects the next higher value within a field
<F2>	<F2> key loads previous values
<F3>	<F3> key loads optimized defaults
<F4>	<F4> key Saves and Exits
<→> or <←>	<Left/Right> arrows selects major Setup menus on menu bar, for example, Main or Advanced
<↑> or <↓>	<Up/Down> arrows select fields in the current menu, for example, Setup function or sub-screen
<ESC>	<ESC> key exits a major Setup menu and enters the Exit Setup menu Pressing the <ESC> key in a sub-menu displays the next higher menu level
<RETURN>	<RETURN> key executes a command or selects a submenu

1.2. Setup Menus

The Setup utility features menus listed in the selection bar at the top of the screen are:

- Main
- Advanced
- Security
- Power
- Event Logs
- Boot
- Save & Exit

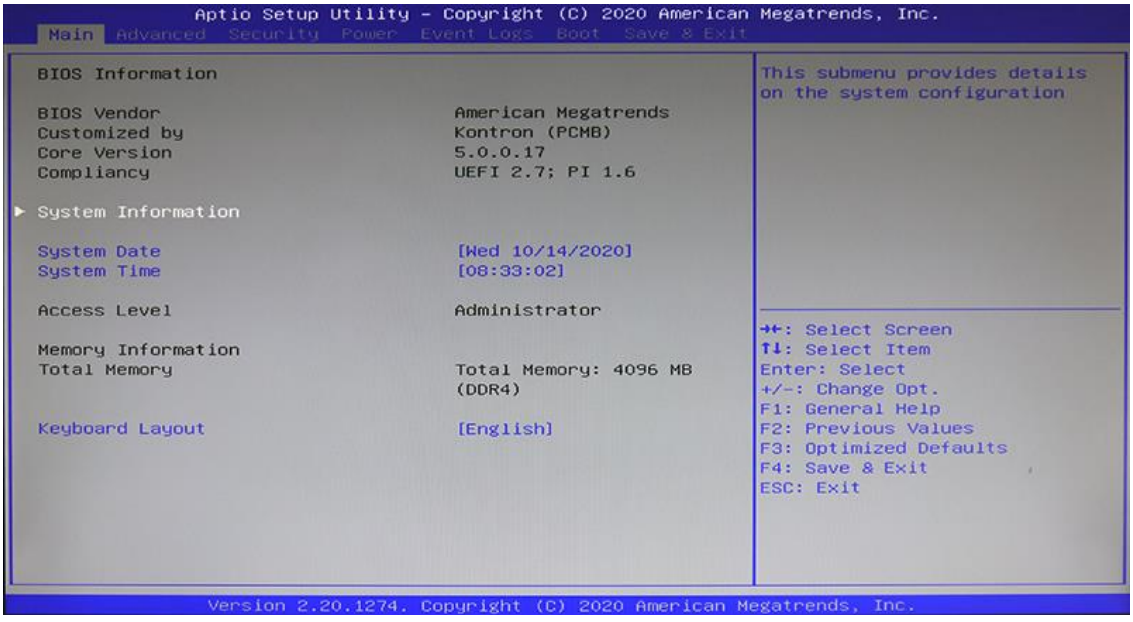
The currently active menu and the currently active UEFI BIOS Setup item are highlighted in white. Use the left and right arrow keys to navigate to the required Setup menu and select the Setup menu by pressing <RETURN>.

Each Setup menu provides two main frames. The left frame displays all available functions. Configurable functions are displayed in blue. Functions displayed in grey provide information about the status or the operational configuration. The right frame displays a Help window providing an explanation of the respective function.

1.2.1. Main Setup Menu

On entering the UEFI BIOS the Setup program displays the Main Setup menu. This screen lists the Main Setup menu sub-screens and provides basic system information as well as functions for setting the system language, time and date.

Figure 1: Main Setup Menu Information Initial Screens



The following table shows the Main Menu sub-screens and functions and describes the content. Default options are displayed **bold**. Some functions include additional information.

Table 2: Main Setup Menu Sub-screens

Sub-Screen	Description
BIOS Information	Read only field *Displays BIOS Information:* BIOS vendor, Core version, Kontron BIOS Version and Compliancy
System Information	Read only field *Displays System Information* This includes CPU, memory and LAN configuration data.
System Date	Displays the system date [Day mm/dd/yyyy]
System Time	Displays the system time [hh:mm:ss]
Access Level	Administrator / User Shows the current access level in BIOS Setup. If the system is not password protected, the access level is Administrator. If only the ADMINISTRATOR password was set, the user has administrator rights. If administrator and user passwords are set, the access level depends on the password entered.
Total Memory	4096 MB (DDR4) Shows the amount of installed system memory
Keyboard Layout	[**English**] (Default) This item is only selectable if a password is not configured to avoid problems while entering the password.

1.2.2. Advanced Setup Menu

The Advanced Setup menu provides sub-screens and second level sub-screens with functions for advanced configuration.

NOTICE Setting items on this screen to incorrect values may cause system malfunctions.

NOTICE Certain menu items may not be available for a specific motherboard model.

NOTICE CPU-TDP setting: The possible selection values depend on the respective board variant, so they are only exemplary.

Figure 2: Advanced Setup Menu Initial Screen

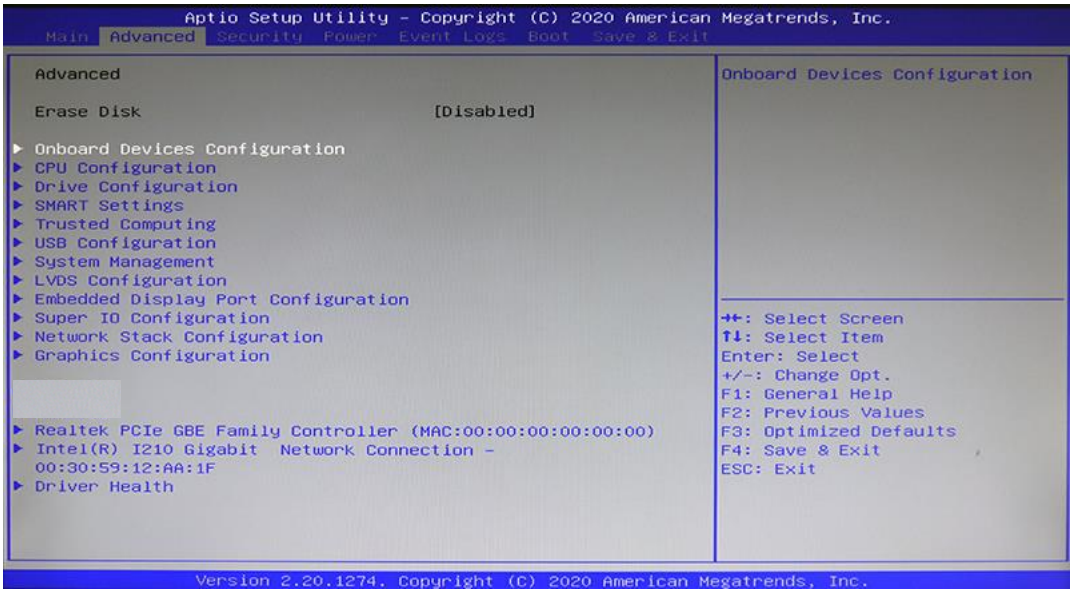


Table 3: Advanced Setup Menu Sub-Screens and Functions

Sub-Screen	Function	Second level Sub-Screen / Description	
Erase Disk	[Start after Reboot, **Disabled**]		The application will only be selectable and executable if an administrator / a supervisor password is assigned (BIOS Setup -> Security Menu). To delete hard disks of a RAID array the RAID controller mode has to be changed to AHCI Mode within SATA Configuration Submenu of Advanced Menu first.
Onboard Devices Configuration	LAN 1 Controller	[**Enabled**, Disabled]	
	LAN 2 Controller	[**Enabled**, Disabled]	
	Azalia HD Audio	[**Enabled**, Disabled]	

Sub-Screen	Function	Second level Sub-Screen / Description	
	M.2 Key-B SATA	[Enabled, **Disabled**]	Selects the routing of the SATA signals between the M.2 Key-B socket or the SATA1 connector. [Disabled] The M.2 Key-B socket does not support SATA. SATA is available on the SATA1 connector. [Enabled] The M.2 Key-B socket supports SATA. The SATA1 connector is no longer usable in this case.
	M.2 Key-M	[**Enabled**, Disabled]	Selects the routing of the PCIe signals, between the M.2 Key-M socket or the PCIe slot. [Disabled] The M.2 Key-M socket is disabled. The PCIe slot is usable. [Enabled] The M.2 Key-M socket is enabled. The PCIe slot is no longer usable in this case.
	WLAN+Bluetooth	[**Enabled**, Disabled]	Specifies whether a populated M.2/PCIe WLAN + Bluetooth Combi-Module is usable. [Disabled] WLAN + Bluetooth Combi-Module is disabled. [Enabled] WLAN + Bluetooth Combi-Module is enabled.
CPU Configuration	Simultaneous Multithreading	[**Auto**, Disabled]	Enables 2 logical processor threads per processor core. [Disabled] Only 1 processor thread is usable by a processor core. [Auto] Up to 2 processor threads are usable by a processor core, if supported by the processor model.
	Active Processor Cores	[**Auto**, 1,2,3]	[1..3] Number of cores to be supported.

Sub-Screen	Function	Second level Sub-Screen / Description	
			[Auto] All available cores are supported."
	Core Performance Boost	[**Enabled**, Disabled]	Allows processor cores to execute at a higher frequency, as long as the package power limits are not exceeded. [Disabled] The nominal frequency will not be exceeded. [Enabled] The nominal frequency can be exceeded.
	Global C-state Control	[Enabled, **Disabled**]	Allows the processor to enter C-states (power saving modes) when it is not fully utilized. [Disabled] No C-states will be entered in order to achieve maximum performance. [Enabled] The processor may enter C-states in order to save energy.
	PSS Support	[**Enabled**, Disabled]	The ACPI Processor Power Management tables are used to notify the possible power and speed modes of the CPU to an ACPI OS. [Disabled] No ACPI Processor Power Management tables are generated. The power and speed modes of the CPU cannot be changed by the ACPI OS. [Enabled] An ACPI OS can change the power and speed modes of the CPU as they are described in the ACPI Processor Power Management tables.
	PPC Adjustment	[**Pstate0**, Pstate1/2]	Specifies the maximum power and speed mode of the processor for the operating system. Lower numbers indicate a higher performance, but also higher power consumption. [PState 0] The operating system is allowed to run in the highest CPU power and speed mode.

Sub-Screen	Function	Second level Sub-Screen / Description	
	NX Mode	[**Enabled**, Disabled]	Defines the protection for executable memory areas (anti-virus protection). The function is only effective if it is also supported by the operating system. The eXecute Disable bit (XD bit) is also known as NX (No eXecute) bit. [Disabled] Prevents the operating system from being able to switch on the function Execute Disable. [Enabled] Enables the operating system to switch on the function eXecute Disable.
	SVM Mode	[**Enabled**, Disabled]	Secure Virtual Machine (SVM) is used to support the visualisation of platform hardware and multiple software environments. Based on Virtual Machine Extensions (VMX), to support the application of multiple software environments under the use of virtual computers. In active mode, a Virtual Machine Monitor (VMM) can use the additional performance features of the Secure Virtual Machine (SVM). [Disabled] A Virtual Machine Monitor (VMM) cannot use the additional performance features of the hardware. [Enabled] A VMM can use the additional performance features of the hardware.
	CPU TDP	[**25W**, 12W, 15W]	TDP limits for specific processor model. Default setting is always the maximum supported TDP. For passive (fanless) cooling, the appropriate TDP setting must be considered. After changing BIOS Setup to "default settings" a reboot is required in order to show this menu.
	Passive Cooling	[Enabled, **Disabled**]	Provides the option to limit the maximum processor temperature; recommended for passive (fanless) cooling solutions. If set to Disabled, the max. processor temperature is 100°C (Default value, defined by AMD)

Sub-Screen	Function	Second level Sub-Screen / Description	
	CPU Temperature Limit	[min. value –max. value]	Visible if "Passive Cooling" is set to 'Enabled'. Setting can be changed in the range from min. value –max. value (°C), depending on the motherboard model, processor TDP, cooling solution, chassis type, and environmental temperature.
Drive Configuration	SATA Controller	[**Enabled**, Disabled]	
	SATA Port 0/1	(not present)	Provides information about the device connected to the associated SATA PORT.
SMART Settings	SMART Self Test	[**Enabled**, Disabled]	Specifies whether the SMART (Self Monitoring, Analysis and Reporting Technology, S.M.A.R.T.) self test is enabled for all drives during BIOS POST.
Trusted Computing	TPM Support	[**Enabled**, Disabled]	If this setup menu is available, the system board contains a security and encryption chip (TPM - Trusted Platform Module) which complies with TCG specification 2.0. This chip allows security-related data (passwords etc.) to be stored securely. The use of TPM is standardized and is specified by the Trusted Computing Group (TCG).
	TPM Device	[**Auto**, Integrated TPM]	Selects the TPM device. [Integrated TPM] The integrated AMD Firmware TPM is used. [Auto] An external TPM module will be used, if populated. If not available, the integrated AMD Firmware TPM will be used.
	Pending TPM Operation	[**None**, Enable Take Ownership, Disable Take Ownership, TPM Clear]	Specifies a TPM operation which will be performed during the next boot process. [None] No TPM operation will be performed. [Enable Take Ownership] The operating system can assign ownership of the TPM. [Disable Take Ownership] The operating system cannot assigne ownership of the TPM. [TPM Clear] TPM is reset to the factory setting. All keys in the TPM will be deleted.

Sub-Screen	Function	Second level Sub-Screen / Description	
	Current TPM Status Information		Shows the current TPM (Trusted Platform Module) status.
USB Configuration	USB Devices	n Drive(s), n Keyboard(s), n Mice(s), n Hub(s)	Shows the number of available USB devices, USB keyboards, USB mice and USB hubs.
	Mass Storage Devices	[**Auto,** Floppy, Forced FDD, Hard Disk, CD-ROM]	List of USB Mass Storage Device(s) Allows the user to force a particular device emulation. When set to Auto, the devices are emulated according to their media format. Optical drives are emulated as "CD ROM" and drives without data media according to the drive type. [Auto] Emulation is choosen depending on the USB device. [Floppy] Force USB floppy emulation. [Forced FDD] Force HDD emulated drives to boot as FDD [Hard Disk] Force USB hard disk emulation. [CD-ROM] Force USB CD ROM emulation."
	USB Port Security	USB Port Control: [**Enable all ports**, Disable all ports, Enable front and internal ports, Enable rear and internal ports, Enable internal ports only, Enable all ports]	Configures the use of the USB ports. Disabled USB ports are neither available during BIOS POST nor under the operating system.
		USB Device Control: [**Enable all devices,** Disabled, Enable Keyboard and Mouse only, Enable all devices except mass storage devices/Hubs] visible if 'USB Port Disable' is set to one of the list: Disable all rear ports Disable all front ports	

Sub-Screen	Function	Second level Sub-Screen / Description	
		Disable unused ports	
System Management	Fan startup check	[Enabled, **Disabled**]	Allows to check the startup of fans during system boot. This can prolong the duration of the system boot time by a few seconds. [Disabled] The system does not wait for the fans to start up. A fan startup check is not executed. [Enabled] The system waits for the fans to start up. The fan startup check is executed.
	Fan Control	[Enhanced, **Auto**, Full]	Controls the speed of the fans. The preset mode can be changed depending on the system configuration and the applications used. [Enhanced] The fan speed will be increased automatically so that the maximum CPU performance is achieved. [Auto] The fan speed is adjusted automatically. A compromise between system temperature and CPU performance. [Full] All fans are operated at maximum speed."
	Watchdog Timeout	[**0** ...255]	Determines the time after which a restart of the system takes place. The permitted values are: 0 to 255 [0] The Watchdog is deactivated. This setting is recommended to prevent an unintended restart of the system. [1...255] After expiry of the time set (in minutes), a restart of the system takes place if the Watchdog was not stopped in this timeframe by a tool in the OS or was continuously reset.
LVDS Configuration	LVDS Support	[Enabled, **Disabled**]	Note: LVDS is shared with one rear graphics port [Enabled]

Sub-Screen	Function	Second level Sub-Screen / Description	
			LVDS support is active; shared rear port can no longer be used [Disabled] Shared rear port is useable
	Non-EDID Support	[Enabled, **Disabled**]	"Enabled" must be set for standard LVDS panel without EDID support. For installation of a Linux operating system, despite a connected LVDS panel without DDC support, it may be necessary to select Non-EDID Support = Disabled first. After the Linux and driver installation has been completed, Non-EDID Support = Enabled can then be set again. [Disabled] The LVDS panel supports EDID [Enabled] The LVDS panel does not support EDID
	LVDS Panel Config Select	[**800x600**, 1024x768, 1280x720, 1280x800, 1280x1024, 1366x768, 1440x900, 1600x900, 1920x1080, LVDS adjusted Parameters]	Select a pre-defined LVDS screen resolution Note: Option 10 [LVDS adjusted Parameters] becomes visible after running the "LVDS Tool" for implementing customized LVDS timings once.
	LVDS Mode	**FPDI 8-Bit**, FPDI 6-Bit, LDI 8-Bit, LDI 6-Bit]	The correct mode must be set according to the specification of the attached LVDS panel. This setting is also required if customized LVDS timings are implemented.
	LVDS Channel Swap	[Enabled, **Disabled**]	Depending on the LVDS panel connected, the channels of the LVDS interface can be swapped.
	LVDS Backlight-Enable Polarity	[**Active High**, Active Low]	The polarity for switching on the backlight can be set depending on the LVDS panel connected.
	LVDS Brightness Control	[**BIOS controlled**, OS controlled]	[BIOS controlled] Use LVDS brightness level defined by BIOS Setup [OS controlled] MS Windows: LVDS Brightness Tool respectively API can be used to adjust LVDS brightness
	LVDS Brightness	[0…**8**…15]	Used for „BIOS controlled" brightness level. [0] = minimum brightness

Sub-Screen	Function	Second level Sub-Screen / Description	
	POST Screen Mode	[**Graphic Mode** Text Mode]	Default setting = Graphic Mode (800 x 600 screen resolution). For panels < 800 x 600 resolution the mode can be changed to <Text Mode> in order to enable full BIOS POST screen respectively full BIOS Setup screen (otherwise some portion of the screen may be cut off)
	LVDS Dual Channel Mode	[Enabled, **Disabled**]	Allows to enable dual channel mode also for LVDS devices with horizontal resolution ≤ 1366 and vertical resolution ≤ 800. Most such low resolution devices need single channel mode, so normally leave this option on "Disabled". Only for special LVDS devices that need dual channel data regardless of low resolutions this option should be set to "Enabled". [Disabled] LVDS mode is set based on the panel resolution. If the horizontal resolution is > 1366 or the vertical resolution is > 800 then dual channel mode is set; otherwise single channel mode is set. [Enabled] LVDS is always set to dual channel mode.
Embedded Display Port Configuration	eDP	[Enabled, **Disabled**]	eDP is shared with one rear graphics port [Enabled] eDP support is active; shared rear port can no longer be used [Disabled] Shared rear port is useable
Super IO Configuration	Serial Port 1/2/3/4	[**Enabled**, Disabled]	Specifies whether the selected serial port is available or not. Specific device settings are shown.
	Serial Port Mode	[**Auto**, RS-232, RS-485/422 Full Duplex, RS-485 Half Duplex]	Selects the serial communication protocol for the serial port, if supported. [Auto] The serial communication protocol is choosen automatically. [RS-232] The serial communication protocol is set to RS-232. [RS-485/422 Full Duplex]

Sub-Screen	Function	Second level Sub-Screen / Description	
			The serial communication protocol is set to RS-485/422 Full Duplex. [RS-485 Half Duplex] The serial communication protocol is set to RS-485 Half Duplex.
	Termination	[Enabled, **Disabled**]	(For COM ports supporting RS4xx) Configure the line termination for RS-422 or RS-485 mode. [Disabled] The line termination for RS422/485 mode is disabled. [Enabled] The line termination for RS422/485 mode is enabled.
	Fast Slew Rate	[Enabled, **Disabled**]	(For COM ports supporting RS4xx) Configure the fast slew rate for RS-422 or RS-485 mode. Note: Fast slew rate should be enabled for data rates above 250kbps.
Network Stack Configuration	Network Stack	[**Enabled**, Disabled]	Configures whether the UEFI Network Stack is available for network access under UEFI. If the UEFI Network Stack is not available there is no UEFI installation possible via PXE.
	Ipv4 PXE Support	[**Enabled**, Disabled]	Specifies whether the PXE UEFI Boot via Ipv4 for installation of operating systems is available in UEFI mode.
	Ipv6 PXE Support	[**Enabled**, Disabled]	Specifies whether the PXE UEFI Boot via Ipv6 for installation of operating systems is available in UEFI mode.
Graphics Configuration	Primary Video Device	[**Integrated Graphics**, External Graphics]	Select Primary Video Device that BIOS will use for output. [Integrated Graphics] The onboard graphics is used. [External Graphics] The external graphics adapter card is used for graphics output, if populated.
	Integrated Graphics	[Enabled, Disabled, **Auto**]	Specifies whether the graphics controller integrated on the system board is available. [Auto]

Sub-Screen	Function	Second level Sub-Screen / Description	
			The integrated graphics controller is not available if a PCIe graphics card is installed. [Enabled] The integrated graphics controller is always available.
	UMA Frame Buffer Size	[**Auto,** 64 MB, 128 MB, 256 MB, 384 MB, 512 MB, 768 MB, 1 GB, 2 GB, 3 GB, 4 GB, 6 GB, 8 GB, 16 GB]	Specifies the dedicated size of the graphics frame buffer. The main memory available for the operating system is reduced by the selected amount.
Realtec PCI GBE Family Controller	Driver Information	Name/Version/ Release	
Intel® I219 Gigabit Network Connection	NIC Configuration	Link Speed	[**Auto Negotiated**, 10 Mbps Half, 10 Mbps Full, 100 Mbps Half, 100 Mbps Full]
		Wake On LAN	[**Enabled**, Disabled]
Driver Health	Intel® PRO/1000 8.9.05 PCI-E Healthy	Controller Child 0 Healthy Intel® I210 Gigabit Network Connection Healthy	If a UEFI driver of a PCI express device supports the Driver Health protocol, the UEFI firmware can query the status of the devices with the UEFI drivers which they manage. The status of the UEFI drivers supporting Driver Health are shown in this menu.

1.2.3. Security Setup Menu

The Security Setup menu provides information about the passwords and functions for specifying the security settings. Passwords are case-sensitive.

NOTICE

Under "Security" there is an item "Housing Monitoring" (= Intrusion). This is only visible if the intrusion switch (with the corresponding short circuit cable) is plugged in. The entry can only be changed if an admin password is assigned.

Housing monitoring is supported by Ryzen motherboards D3713/D3723 only

Figure 3: Security Setup Menu Initial Screen

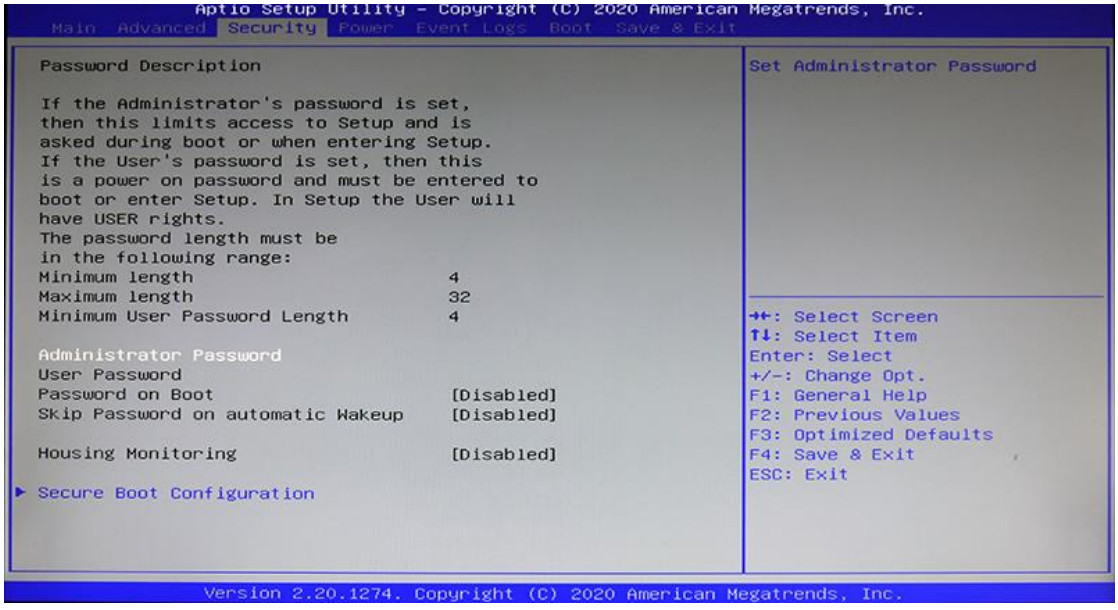


Table 4: Security Setup Menu Functions

If only the administrator's password is set, then only access to setup is limited and requested when entering the setup.

If only the user's password is set, then the password is a power on password and must be entered to boot or enter Setup. In the Setup the user has administrator rights.

The required password length in characters is max. 32 and min. 3.

Function	Description
Administrator Password User Password	Sets administrator/user password If you press the enter key, a window will open in which you can assign the administrator password. Enter a character string to define the password. If you confirm an empty password field, the password will be deleted.

Function	Description	
	To call the complete BIOS Setup, you need administrator access level. If an administrator password is allocated, the user password enables only very limited access to the BIOS Setup. In order to be able to assign a user password, an administrator password must already have been installed.	
Password on Boot>	[On Every Boot, On First Boot, **Disabled**] Specifies whether a Password prompt appears when booting. [On Every Boot] Entering a password is required before each boot. [On First Boot] Entering a password is required before each cold boot. [Disabled] The system boots without entering a password.	
Skip Password on automatic Wakeup	[Enabled, **Disabled**] Specifies whether the request for a password is skipped or is prompted when the system is started automatically	
HDD Password on Boot	[**Enabled**, Disabled] Specifies whether a hard disk user password must be entered during every boot process. [Enabled] Entry of a hard disk user password is required during every boot process.	
Housing Monitoring	[Enabled, **Disabled**] Specifies whether opening of the chassis should be monitored. This menu item is only visible if a switch for cover monitoring is present. This menu item is greyed out if no administrator password has been assigned. [Disabled] The system continues to operate normally, even if the chassis was opened. [Enabled] If the chassis has been opened, then the boot process is suspended until BIOS Setup is called. If the BIOS Setup is protected with a password, then this must be entered. An SMBIOS event log entry will be generated.	
Secure Boot Configuration Provides the submenus for configuring Secure Boot. Secure Boot Configuration defines a firmware execution authentication process.	Secure Boot Control	[Enabled, **Disabled**] Note: The setting is kept even if the battery is dead or removed. Specifies whether booting of unsigned boot loaders/UEFI OpROMs is permitted.

Function	Description	
As an industry standard, Secure Boot defines how platform firmware manages certificates, authenticates firmware, and how the operating system interfaces with this process. Secure Boot Configuration is based on the Public Key Infrastructure (PKI) process to authenticate modules before they are allowed to execute.		The associated signatures are saved in the BIOS or can be reloaded in the Key Management submenu. [Disabled] All boot loaders / OpROMs (Legacy / UEFI) can be executed. [Enabled] Only booting of signed boot loaders/UEFI OpROMs is permitted.
	Platform Mode	[**User**, Setup] Shows whether the system is in user mode or setup mode. [User] In user mode, the Platform Key (PK) is installed. Secure Boot can be enabled or disabled via the Secure Boot Control menu option. [Setup] In setup mode, the Platform Key (PK) is not installed. Secure Boot is disabled and cannot be enabled via the Secure Boot Control menu option.
	Secure Boot Mode	[Custom, **Standard**] Specifies whether the Key Management submenu is available. [Standard] The Key Management submenu is not available. [Custom] The Key Management submenu is available.
	Vendor Keys	[Modified, **Not Modified**] Shows whether the Vendor Keys have been modified.
	Key Management	Submenu for deleting, changing and adding the key and signature databases required for Secure Boot.

Function	Description	
		Without the installed Platform Key (PK), the system is in setup mode (Secure Boot is disabled). As soon as the PK is installed, the system switches to user mode (Secure Boot can be enabled).

1.2.3.1. Remember the Password

It is highly recommended to keep a record of all passwords in a safe place. Forgotten passwords results in the user being locked out of the system.

If the system cannot be booted because the User Password or the Supervisor Password are not known, clear the UEFI BIOS settings, or contact Kontron Support for further assistance.

1.2.4. Power Menu

Figure 4: Power Screen

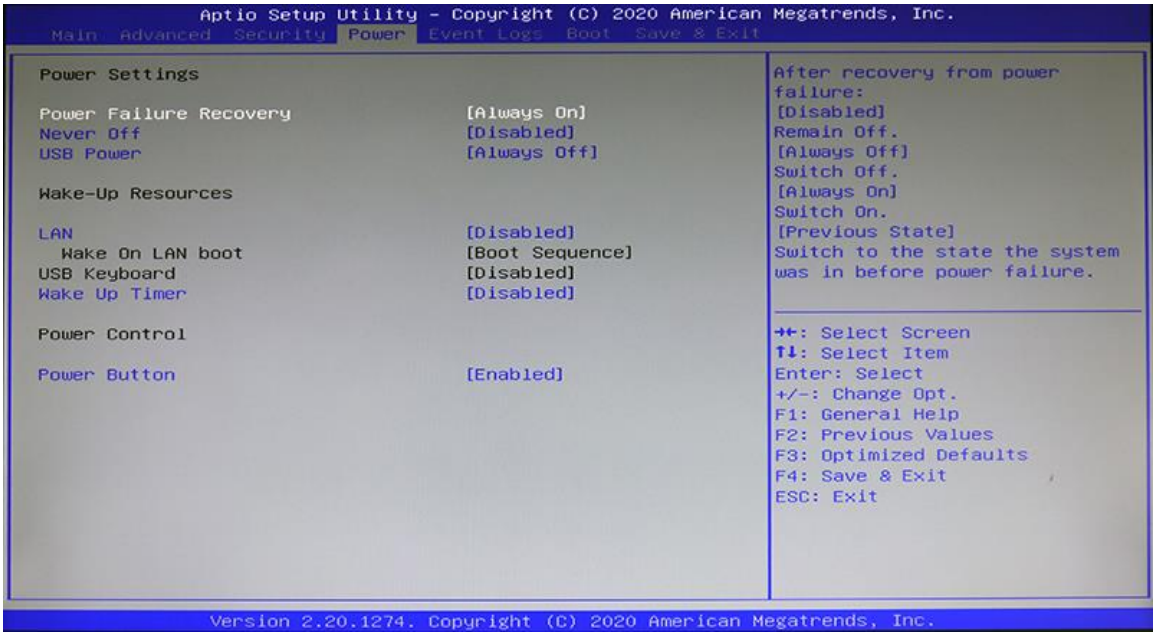


Table 5: Power Menu Functions

Function	Description
Power Failure Recovery	[Always Off, **Always On**, Previous State] Specifies how the system behaves during a reboot following a power failure. [Always Off] The system switches on briefly, performs a status check (initialisation), and then switches off. [Always On] The system switches on. [Previous State] The system switches on briefly, performs a status check, and then returns the mode it was in before the power failure occurred (ON or OFF).
Never Off	[Enabled, **Disabled**] Specifies whether the system can be switched off. If the Never Off function is active, the system switches itself on again immediately when it is shut down via the operating system or the power button. The system can only be switched off, by disconnecting it from the power supply. Note: When this feature is enabled, Power Failure Recovery should be set to [Always On].
USB Power	[**Always Off**, Always On] Enables or disables the power supply to the USB ports when the system is switched off. [Always off] The USB ports are no longer supplied with power after the system is shut down. [Always on] The USB ports continue to be supplied with power after the system is shut down.
LAN	[Enabled, **Disabled**] Determines whether the system can be switched on via a LAN controller (on the systemboard or expansion card).
Wake On LAN Boot	[**Boot Sequence**, Force LAN Boot] Specifies the system behaviour when switched on by means of network signals. [Boot Sequence] The system boots up according to the device sequence specified in the Boot menu when switched on via LAN.

Function	Description
	[Force LAN Boot] The system is booted remotely via LAN when switched on via LAN.
Wake Up Timer	[Enabled, **Disabled**] The time at which the system should be switched on can be specified here. [Disabled] Wake Up Timer is not enabled. [Enabled] Wake Up Timer is enabled. The system is switched on at the time specified. The submenus provide detailed schedule options
Power Button	[**Enabled**, Disabled] When set to "disabled", the system power button (connected via front panel header) can only be used to switch on the mainboard. Switching off the mainboard (incl. power button override) is disabled then.

1.2.5. Event Log´s Menu

The Event Log´s menu provides functions for the monitoring of the setup.

Figure 5: Event Log´s Screen

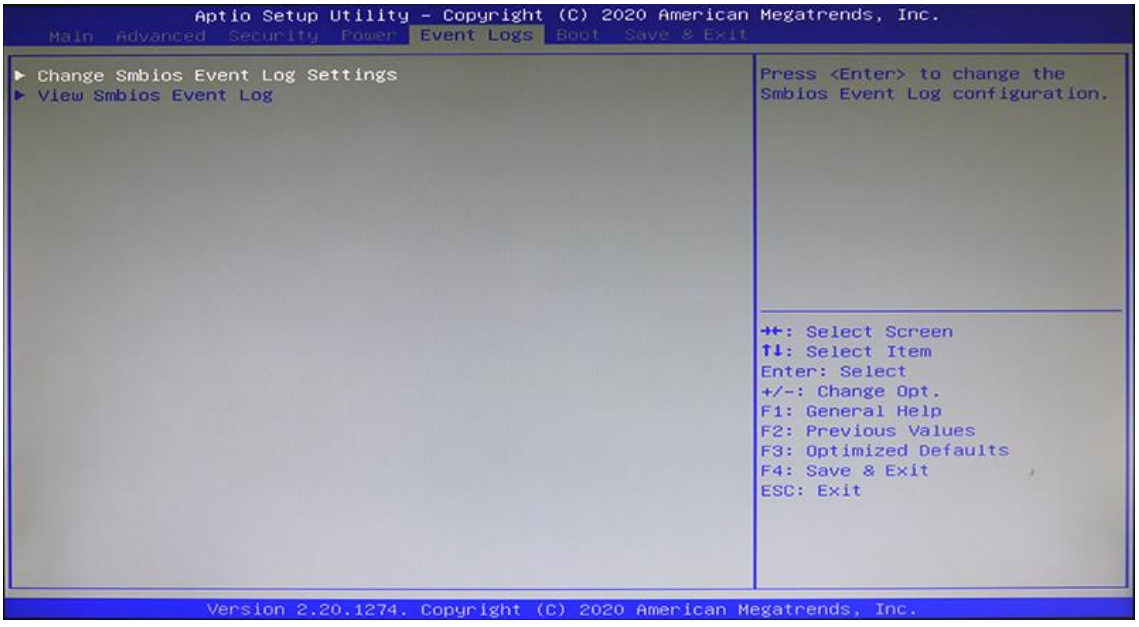


Table 6: Event Log´s Menu Functions

Function	Description	
Change Smbios Event Log Settings	Smbios Event Log	[**Enabled**, Disabled]
	Erase Event Log	[**No**, Yes Next reset, Yes Every reset]
	When Log is Full	[**Do nothing**, Erase Immediately]
View Smbios Event Log	Date/Time/Error Code/Severity	

1.2.6. Boot Menu

Figure 6: Boot Screen

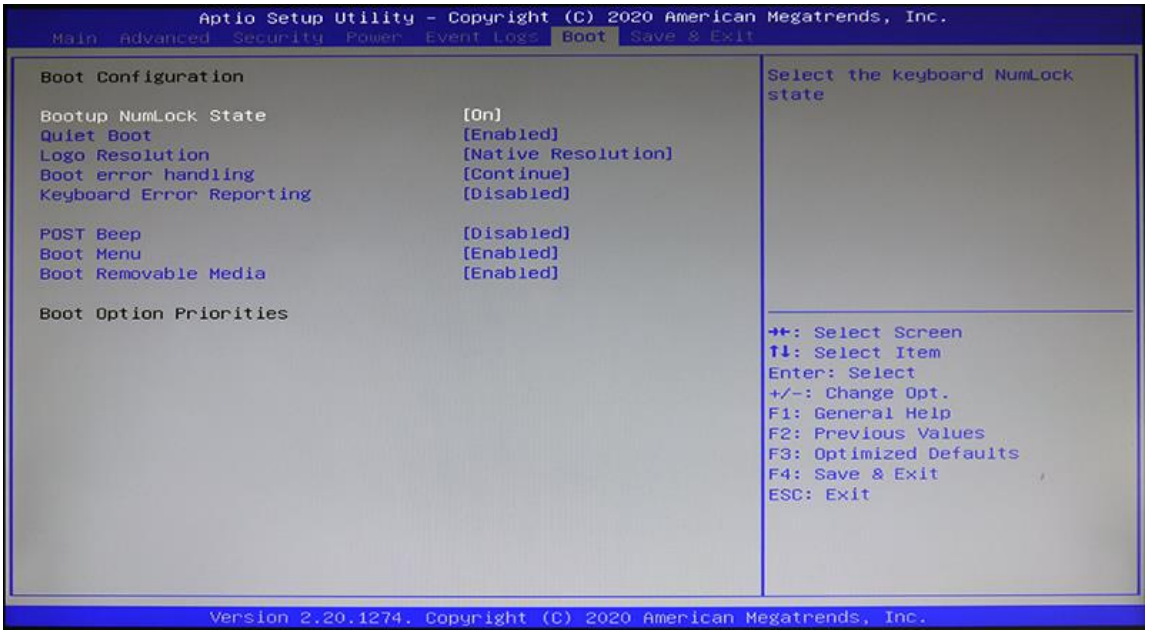


Table 7: Boot Menu Functions

Function	Description
Bootup NumLock State	[**On**, Off]
Quiet Boot	[**Enabled**, Disabled] [Disabled] The BIOS POST information is shown on the screen. [Enabled] The boot logo is shown on the screen instead of the BIOS POST information.
Logo Resolution	[Default Resolution, **Native Resolution,** Static Resolution] Configures the screen resolution. [Default Resolution] Default screen resolution is used. [Native Resolution] Native Display resolution is used. [Static Resolution] Limit screen resolution to 800x600.
Boot error handling	[Continue, Pause and wait for key]

Function	Description
	Specifies whether the system boot process is interrupted and the system stopped when an error is detected. [Continue] The system boot is not paused. The error is ignored as far as possible. [Pause and wait for key] If an error is detected during POST, the boot process is interrupted and the system stopped.
Keyboard Error Reporting	[Enabled, **Disabled**] Specifies whether a keyboard error message is displayed and entered in the event log.
POST Beep	[**Disabled**, At start of POST, At end of POST, At start and end of POST] Configures the signaling via a short beep during POST.
Boot Menu	[**Enabled**, Disabled] Specifies whether the Boot menu can be called by pressing the [F12] key during the POST process.
Boot Removable Media	[**Enabled**, Disabled]
Boot Option Priorities	Displays the current boot order. Press the cursor keys [↑] or [↓] to select the device for which you want to change the boot order. Press the [+] key to increase the priority and the [-] key to decrease the priority for the selected device. Press the [Enter] key and select Disabled to remove the selected device from the boot order.

1.2.7. Save and Exit Setup Menu

The Save and Exit setup menu provides functions for handling changes made to the UEFI BIOS settings and exiting the Setup program.

Figure 7: Save and Exit Setup Menu Initial Screen

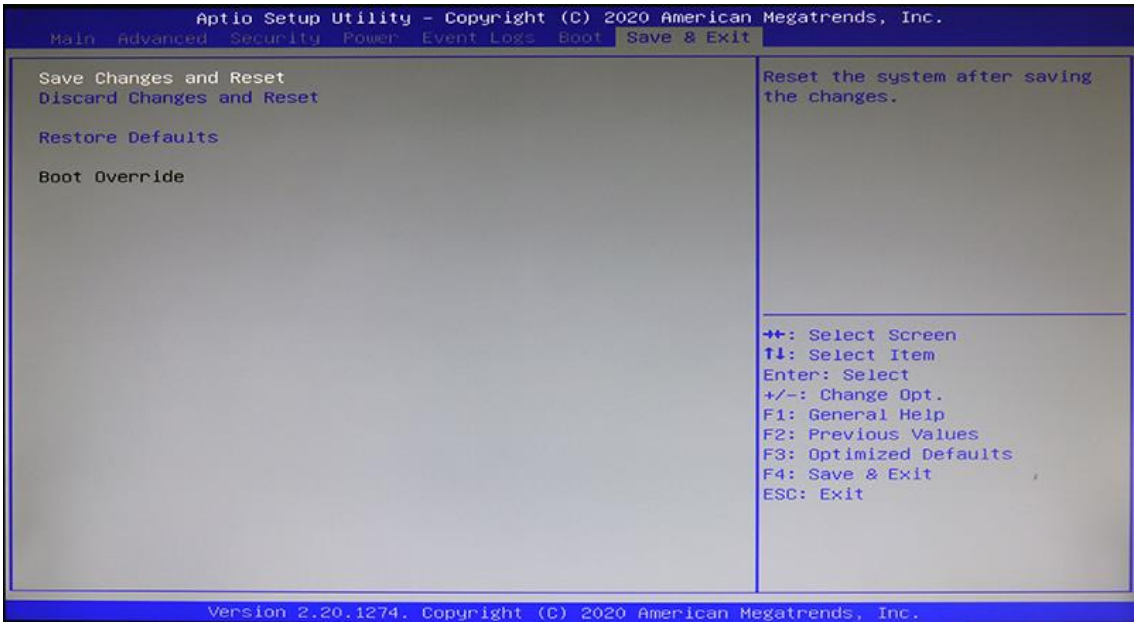


Table 8: Save and Exit Setup Menu Functions

Function	Description
Save Changes and Exit	Exits BIOS Setup after saving changes
Discard Changes and Exit	Exits BIOS Setup without saving changes
Restore Defaults	Restores/loads standard default values for all setup options

About Kontron – Member of the S&T Group

Kontron is a global leader in IoT/Embedded Computing Technology (ECT). As a part of technology group S&T, Kontron, together with its sister company S&T Technologies, offers a combined portfolio of secure hardware, middleware and services for Internet of Things (IoT) and Industry 4.0 applications. With its standard products and tailor-made solutions based on highly reliable state-of-the-art embedded technologies, Kontron provides secure and innovative applications for a variety of industries. As a result, customers benefit from accelerated time-to-market, reduced total cost of ownership, product longevity and the best fully integrated applications overall.

For more information, please visit: **www.kontron.com**

GLOBAL HEADQUARTERS

Kontron Europe GmbH

Gutenbergstraße 2
85737 Ismaning
Germany
Tel.: + 49 821 4086-0
info@kontron.com