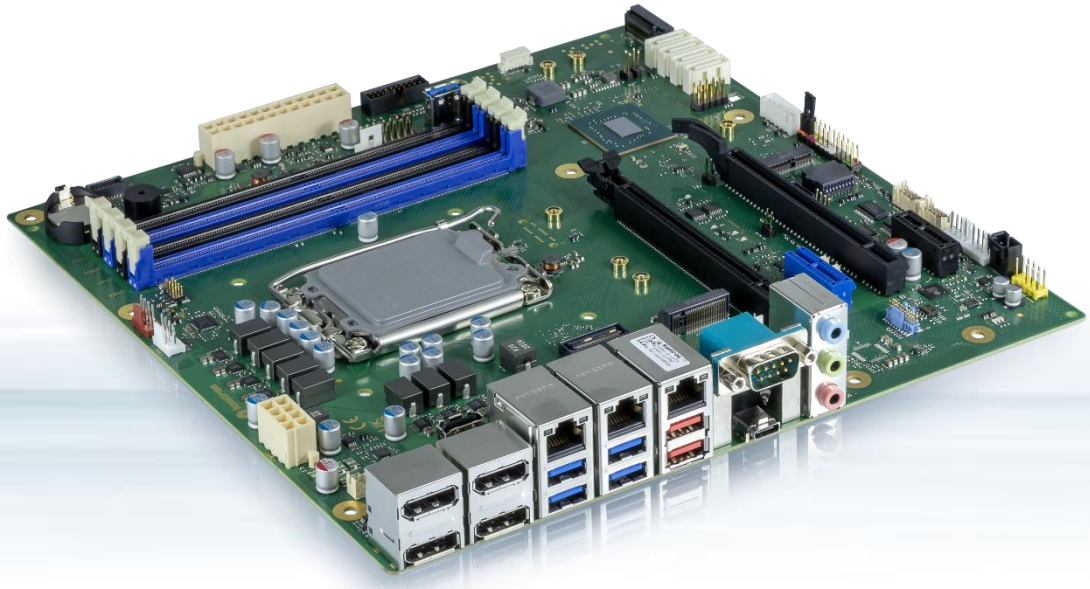
USER GUIDE



BIOS for Intel 600 Series Motherboards

User Guide Rev. 0.9

BIOS FOR INTEL 600 SERIES MOTHERBOARDS - 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
0.8	First released (preliminary) version	06/2022
0.9	BIOS Menu updates added	07/2022

NOTICE

Menus and functions shown here are generally not available for all motherboard versions.

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 https://ftp.kontron.com/

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
- MEBx
- 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.

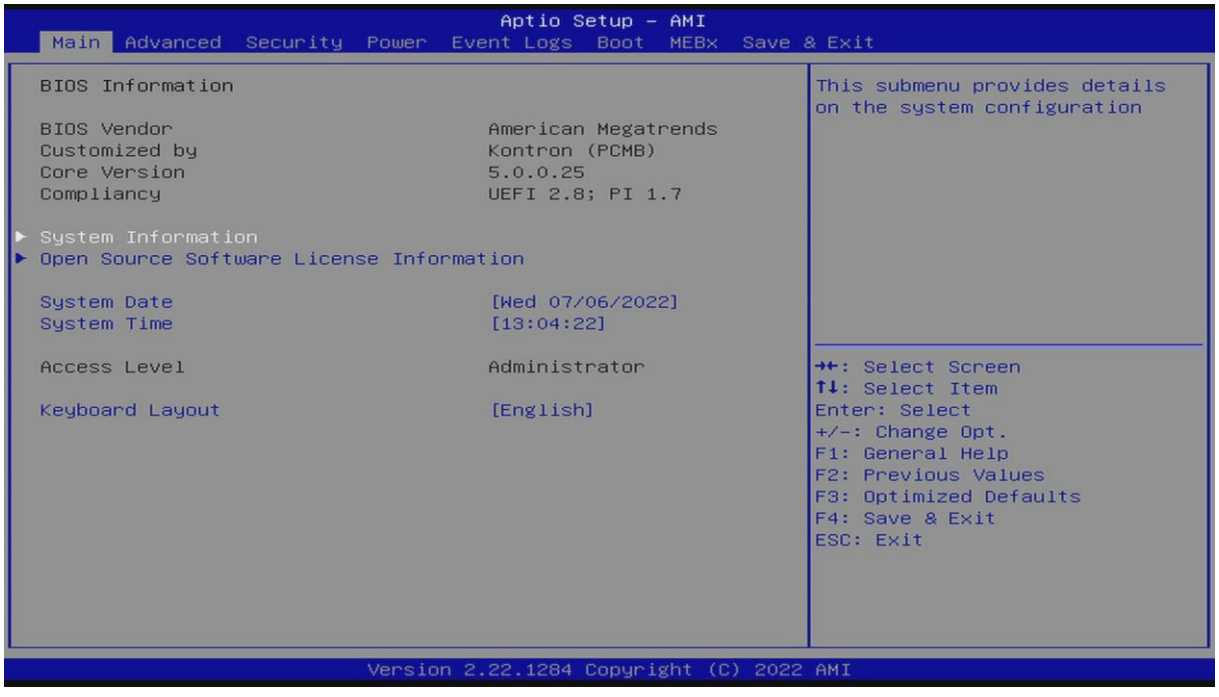


Figure 1: Main Setup Menu Information Initial Screens

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, Customized by Kontron (PCMB), Core version, Compliancy
System Information	Read only field *Displays System Information* The System Information window displays an overview about the system configuration. This includes CPU, memory and LAN configuration data.
Open Source Software Licence Information	Open Source Software License Information This submenu provides licenses information for open source software, used in this system board.
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.
Keyboard Layout	[**English**] (Default) Defines the language used in BIOS setup utility.

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.

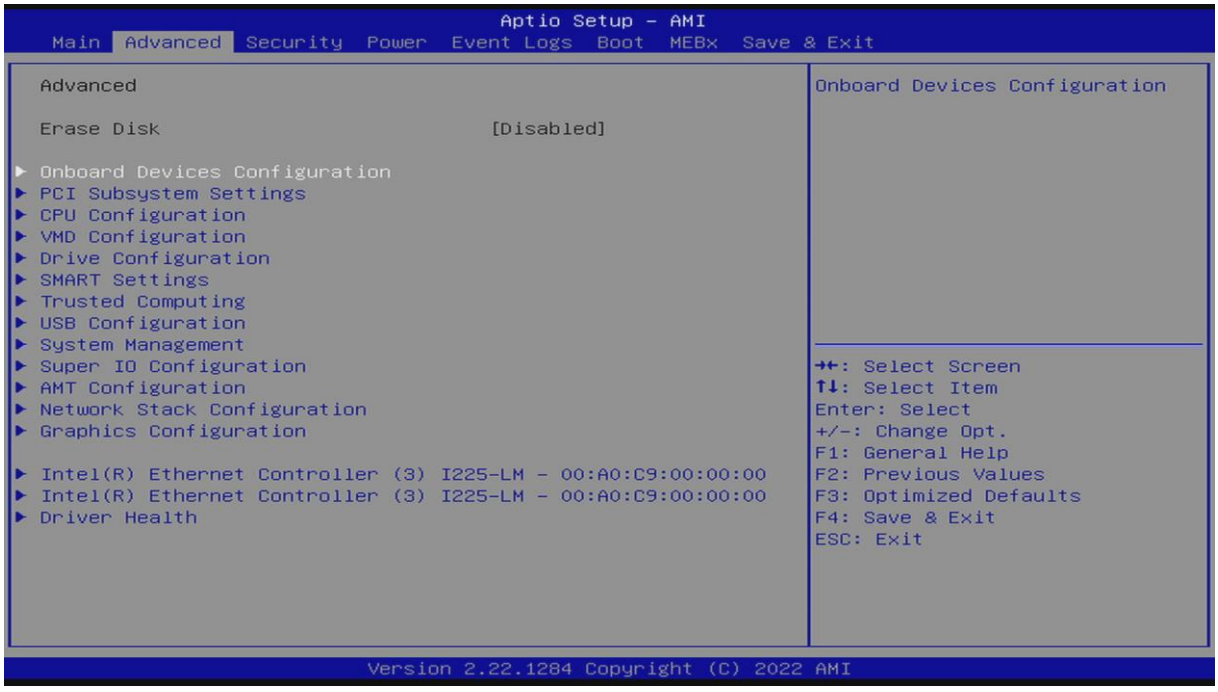


Figure 2: Advanced Setup Menu Initial Screen

Table 3: Advanced Setup Menu Sub-Screens and Functions

Sub-Screen	Function	Second level Sub-Screen / Description	
Erase Disk	[Start after Reboot, **Disabled**]		Erase Disk is a Kontron feature embedded in the system firmware (UEFI: Unified Extensible Firmware Interface) to erase all data from SATA or NVMe drives. The main purpose of this feature is to irretrievably delete all data from built in SATA hard disk(s) or external SATA hard disk(s) using the eSATA port before disk(s) will be discarded or the complete computer system will be sold. It also can be used whenever hard disk(s) should be deleted completely, e.g. before a new operating system will be installed.
Onboard Devices Configuration	LAN 1 Controller	[**Enabled**, Disabled]	LAN controllers can be used as boot devices if a suitable Option ROM is started during BIOS POST. This parameter specifies whether an Option ROM should be started and if so which type of Option ROM. It is only valid for legacy, i.e. non-UEFI Option ROMs.

Sub-Screen	Function	Second level Sub-Screen / Description	
	LAN 2 Controller	[**Enabled**, Disabled]	
	Azalia HD Audio	[**Enabled**, Disabled]	Allows the onboard Azalia HD (High Definition) Audio controller to be activated.
	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.
PCI Subsystems Settings	PERR# Generation	[Enabled, **Disabled**]	Specifies whether PERR# (PCI parity errors) are created.
	SERR# Generation	[Enabled, **Disabled**]	Specifies whether SERR# (PCI system errors) will be created.
	PCI Express Slot 1 .. 4 … x	[**Enabled**, Disabled]	
	Slot 1 .. 4 .. x Link Speed	[**Auto**, Gen1 .. Gen5]	
	Above 4G Decoding	[**Enabled**, Disabled]	
CPU Configuration	Hyper-Threading	[**Enabled**, Disabled]	Hyper-threading technology allows a single physical processor core to appear as several logical processors. With this technology the operating system can better utilize the internal processor resources, which in turn leads to increased performance. The advantages of this technology can only be used by an operating system which supports ACPI. This setting has no effect on operating systems which do not support ACPI.
	Active Processor Cores	[**All**, 1,2,3, …]	For processors that contain multiple processor cores, the number of active processor cores can be limited. Inactive processor cores will not be used and hidden from the operating system.
	Active Efficient-Cores	[**All**, 1,2,3, …]	On processors which contain also multiple efficient processor cores, the number of active processor cores can be limited. Inactive processor cores will not be used and are hidden from the operating system.
	Intel Virtualization Technology	[Enabled, **Disabled**]	Supports the virtualization of platform hardware and several software environments, based on VMX (Virtual

Sub-Screen	Function	Second level Sub-Screen / Description	
			Machine Extensions) to support the use of several software environments using virtual computers. Virtualization technology extends the processor support for virtualization purposes with the 16 Bit and 32 Bit protected modes and with the EM64T (Intel® Extended Memory 64 Technology) mode. [Disabled] A VMM (Virtual Machine Monitor) cannot use the additional hardware capabilities. [Enabled] A VMM can use the additional hardware capabilities.
	VT-d	[**Enabled**, Disabled]	VT-d ((Intel Virtualization Technology for Directed I/O) provides hardware support for sharing I/O devices between multiple virtual machines. VMMs (Virtual Machine Monitors) can use VT-d for managing multiple virtual machines accessing the same physical I/O device. [Disabled] VT-d is disabled and not available for VMMs. [Enabled] VT-d for VMMs is enabled.
	Enhanced SpeedStep	[**Enabled**, Disabled]	Defines the processor voltage and frequency. EIST (Enhanced Intel SpeedStep® Technology) is an energy saving function. The processor voltage is adapted to the respective system requirements. A reduction in the clock frequency causes less power to be required by the system. [Disabled] Enhanced SpeedStep functionality is disabled. [Enabled] Enhanced SpeedStep functionality is enabled.
	Intel® Speed Shift Technology	[**Enabled**, Disabled]	Enable or disable Intel® Speed Shift Technology support. Activation makes the CPPC v2 interface visible to enable hardware-controlled P states. [Disabled] Deactived Speed Shift Technology

Sub-Screen	Function	Second level Sub-Screen / Description	
			[Enabled] Actived Speed Shift Technology
	Turbo Mode	[**Enabled**, Disabled]	The processor may work faster than the specified frequency when the operating system requires the maximum performance state (P0). This function is also known as Intel® Turbo Boost Technology. [Disabled] Turbo Mode is disabled. [Enabled] Turbo Mode is enabled.
	C States	[**Enabled**, Disabled]	Enables or disables the CPU Power Management. Allows the CPU to go to C states when it is not 100% utilized. [Disabled] C States is disabled. [Enabled] C States is enabled.
	Package C State Limit	[**Enabled**, Disabled]	Allows to configure processor C State limit. [C0] C0 is the C state limit. [C2] C2 is the C state limit. [C6] C6 is the C state limit. [C6 Retention] C6 Retention is the C state limit. || [C0] C0 is the C state limit. [C2] C2 is the C state limit. [C6] C6 is the C state limit. [C6 Retention] C6 Retention is the C state limit. [No Limit] C7 is the C state limit. [Auto] C6 is set as C state limit.
	Configurable TDP	Power Limit 1 Overwrite	[**Enabled**, Disabled]
		Power Limit 1	0 ... max. TDP

Sub-Screen	Function	Second level Sub-Screen / Description	
		Power Limit 1 Time Window	[0 ... 128]
		Power Limit 2 Overwrite	[**Enabled**, Disabled]
		Power Limit 2	0 ... 409
VMD Configuration	Enable VMD Controller	[Enabled, **Disabled**]	Specifies whether feature VMD (Volume Management Device) should be active or not. Intel Volume Management Device (VMD) technology provides a means to provide volume management across separate PCI Express HBAs and SSDs without requiring operating system support or communication between drivers. For example, the OS will see a single RAID volume instead of multiple storage volumes, when Volume Management Device is used. [Disabled] The VMD Controller is disabled. No RAID support for PCIe storage devices or SATA devices. [Enabled] The VMD Controller is enabled. RAID is supported for PCIe storage devices and SATA devices. The RAID has to be configured within the UEFI VMD driver.
Drive Configuration	SATA Port 0 .. 3	[**Not Installed**]	
	Port 0	[**Enabled**, Disabled]	
	External SATA	[Enabled, **Disabled**]	
	Hot Plug	[Enabled, **Disabled**]	
SMART Settings	SMART Self Test	[**Enabled**, Disabled]	Specifies whether the SMART (Self Monitoring, Analysis and Reporting Technology) self test is enabled for all hard disks during the POST. [Enabled] The SMART self test is enabled during the POST. [Disabled] The SMART self test is disabled during the POST.
Trusted Computing	TPM Support	[**Enabled**, Disabled]	Opens the submenu for enabling TPM and changing the TPM settings. 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

Sub-Screen	Function	Second level Sub-Screen / Description	
			specified by the Trusted Computing Group (TCG).
	TPM Device	[**Auto**, Integrated TPM]	Selects the TPM device. [Integrated TPM] The integrated Firmware TPM is used. [Auto] An external TPM module will be used, if populated. If not available, the integrated Firmware TPM will be used.
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.
	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 the POST or under the operating system. [Enable all ports] All USB ports are enabled. [Disable all ports] All USB ports are disabled. [Enable front and internal ports] All USB ports on the rear of the device are disabled. [Enable rear and internal ports] All USB ports on the front of the device are disabled. [Enable internal ports only] All external USB ports are disabled. [Enable used ports] All unused USB ports are disabled.
		USB Device Control	
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 fan. The preset mode can be changed depending on the

Sub-Screen	Function	Second level Sub-Screen / Description	
			system configuration and the applications used. If the system is fully configured with all available expansions/upgrades, then silent mode is not recommended. [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.
Super IO Configuration	Serial Port x Configuration	[**Enabled**, Disabled]	Specifies whether the serial port is available or not.
	Device Settings	[IO=xxxh; IRQ=x]	IO- and IRQ-settings are fixed by the BIOS and cannot be changed
	PS2 Controller Configuration	[**Enabled**, Disabled]	Specifies whether the PS2 controller is available or not.
AMT Configuration	Intel® AMT	[**Enabled**, Disabled]	Enables/disables Intel (R) Active Management Technology BIOS Extension (MEBx). iAMT H/W is always enabled. This option simply controls the execution of the BIOS Extension. [Disabled] Intel® AMT BIOS Extension (MEBx) is disabled. [Enabled] Intel® AMT BIOS Extension (MEBx) is enabled.
	USB Provisioning of AMT	[Enabled, **Disabled**]	If this option is enabled, the settings of the AMT/ME configuration can be

Sub-Screen	Function	Second level Sub-Screen / Description	
			changed using a USB stick without starting the Intel® Active Management Technology BIOS Extension (MEBx). [Disabled] USB Provisioning from USB stick is disabled. [Enabled] USB Provisioning from USB stick is enabled.
	Unconfigure AMT/ME	[Enabled, **Disabled**]	If this option is enabled, an MBEx (Management Engine BIOS eXtension) query occurs at the next reboot to establish whether the AMT/ME configuration should be reset to the default values. [Disabled] Do not change the AMT/ME configuration. [Enabled] Start the reset of the AMT/ME configuration. The option is then automatically reset to Disabled.
Network Stack Configuration	Network Stack	[Enabled, **Disabled**]	Configures whether the UEFI Network Stack is available for network access under UEFI. E.g.: is the UEFI Network Stack not available there is no UEFI installation possible via PXE. [Disabled] The UEFI Network Stack is not available. [Enabled] The UEFI Network Stack is available.
Graphics Configuration	Primary Display	[**Auto**, Internal Graphics, PCI Express for Graphics (PEG), PCI Express (PCIE)]	Configures which graphics controller is connected to the primary display. The primary display is used during POST. [Auto] External graphics controller are preferred but if no external device is detected the internal graphics controller is used. [Internal Graphics] The internal graphics controller is used. (This option is available for specific CPUs only) [PCI Express for Graphics (PEG)] The graphics controller which is plugged into the PCI express slot for graphics is used. [PCI Express (PCIE)]

Sub-Screen	Function	Second level Sub-Screen / Description	
			The graphics controller which is plugged into a PCI express slot is used.
	Internal Graphics	[Enabled, Disabled, **Auto**]	Allows to force the internal graphics controller to be enabled or disabled. When Auto is set the BIOS will detect the configuration automatically. [Auto] The BIOS detects the configuration automatically and enables or disables the internal graphics controller. [Disabled] The graphics controller is forced to be disabled. [Enabled] The graphics controller is forced to be enabled.
	DVMT Shared Memory Size	[**32 MB,** 64 MB, 128 MB, 256 MB, 512 MB, 1024 MB, 1536 MB]	Configures the fixed shared memory size for the internal graphics controller.
	DVMT Total Graphics Memory Size	[128 MB, **256 MB**, MAX]	Configures the total shared memory size for the internal graphics controller. [128 MB] 128 MB of the system memory used by the graphics controller. [256 MB] 256 MB of the system memory used by the graphics controller. [MAX] The size of the system memory which is used by the graphics controller will be allocated dynamically.
RAM Disk Configuration	Disk Memory Type	[**Boot Service Data**, Reserved]	
	Create raw	Create raw RAM disk	
	Create from file	Create raw RAM disk from a given file	
	Remove selected RAM disks	Remove selected RAM disks	
Intel® Ethernet Controller (3) I225-LM	UEFI Driver, Device Name, PCI Device ID, Link Status, MAC Adress		
Driver Health	Intel® Gigabit 0.10.01 Healthy	Controller Child 0 Healthy Intel® Ethernet Controller Healthy	

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.

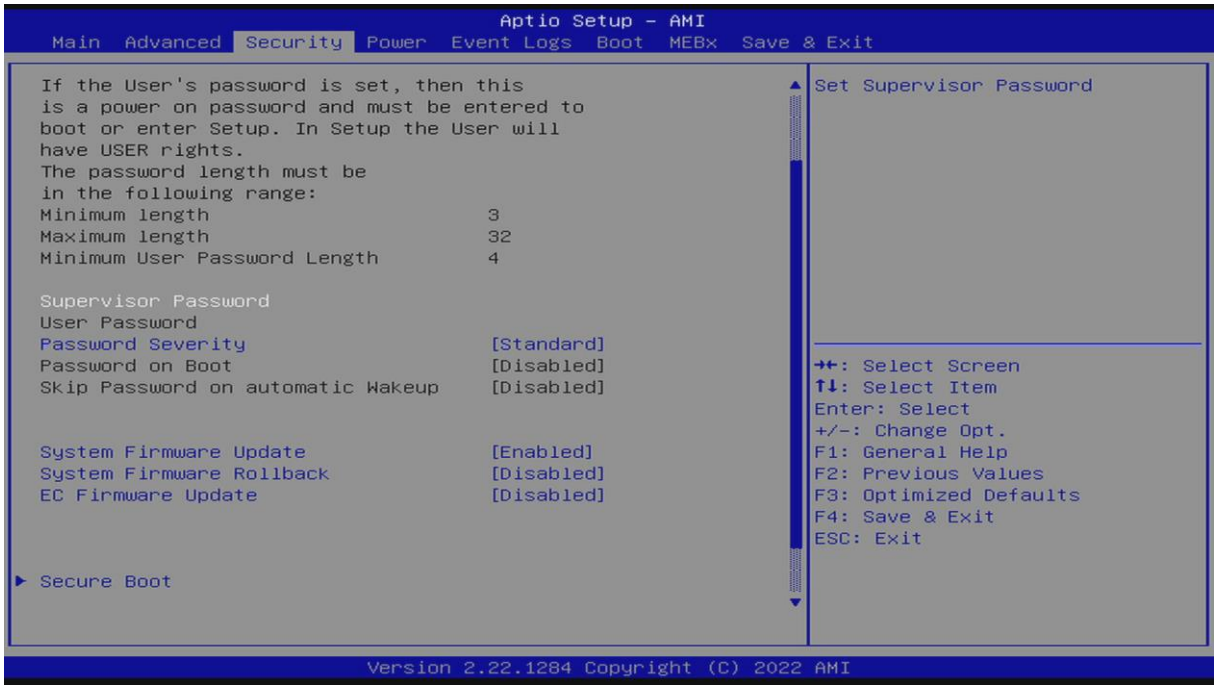


Figure 3: Security Setup Menu Initial Screen

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

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

Table 4: Security Setup Menu Functions

Function	Description
Supervisor Password User Password	Sets Supervisor 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. To call up the complete BIOS Setup, you need the administrator level of access. If an administrator password is allocated, the user password only allows very limited access to the BIOS Setup. User Password Enter a character string to define the password. With the user password, you can prevent unauthorised access to your system. In order to be able to assign a user password, an administrator password must already have been assigned.
Password Severity	Defines ways to access the system if the password has been forgotten. [Standard] A forgotten password can be reset on site. [Strong] It is not possible to reset the password on site. If a password has been forgotten, only the certified, technical support team can enable it. [Stringent] It is not possible to reset the password. If a password has been forgotten, the system remains permanently unusable.
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
System Firmware Update	[**Enabled**, Disabled] Defines how the system firmware (BIOS) update is carried out. [Disabled]

Function	Description	
	The System Firmware (Bios) cannot be written. A Flash BIOS update is not possible. [Restricted] The system firmware (BIOS) can only be updated via specific tools, automatic update via Windows Update (WU) is prevented. [Enabled] The System Firmware (Bios) update is possible both via FUJITSU tools and automatically via Windows Update (WU).	
System Firmware Rollback	[Enabled, **Disabled**] Specifies whether a Flash BIOS update to an older version of the system firmware (BIOS) is possible. [Disabled] The system firmware (BIOS) cannot be flashed back to an older version. [Enabled] The system firmware (BIOS) can be flashed back to an older version.	
EC Firmware Update	[**Disabled**, Enabled]	Enables the AMI Flash Utility to update the System Management Controller Firmware ("EC" = Embedded Controller). This only applies to the next boot, as the feature is disabled automatically during the following boot.

Function	Description	
Secure Boot Opens the submenu for configuring Secure Boot. Secure Boot Configuration defines a firmware execution authentication process. 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.	Secure Boot	[Enabled, **Disabled**] Specifies whether booting of unsigned boot loaders/UEFI OpROMs is permitted. 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.
	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.

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.

1.2.4. Power Menu

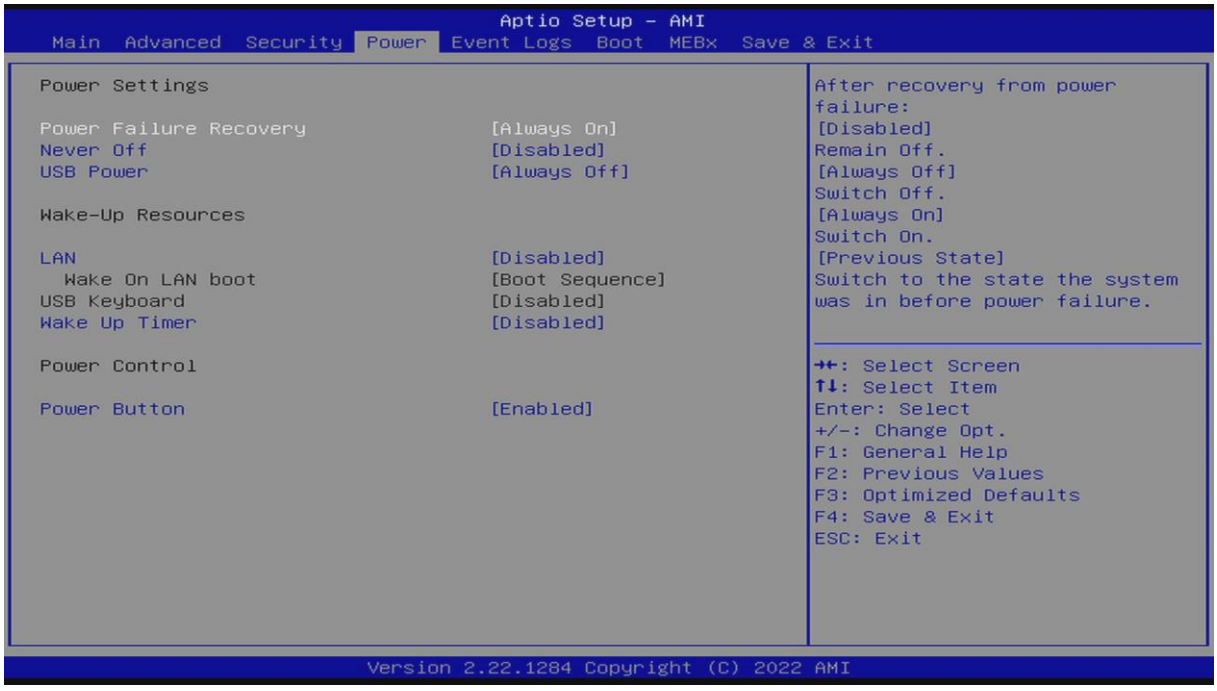


Figure 4: Power Screen

Table 5: Power Menu Functions

Function	Description
Power Failure Recovery	[Disabled, 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). [Disabled] The system does not switch on.
Never Off	[Enabled, **Disabled**] Specifies whether the system can be switched off.

Function	Description
	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. When this feature is enabled, Power Failure Recovery should be set to [Always On]. [Disabled] The Never Off functionality is deactivated. [Enabled] The Never Off functionality is activated.
USB Power	[**Always Off**, Always On] Enables and 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 system-board or expansion card). [Disabled] The system cannot be switched on via a LAN controller. [Enabled] The system can be switched on via a LAN controller.
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.
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.

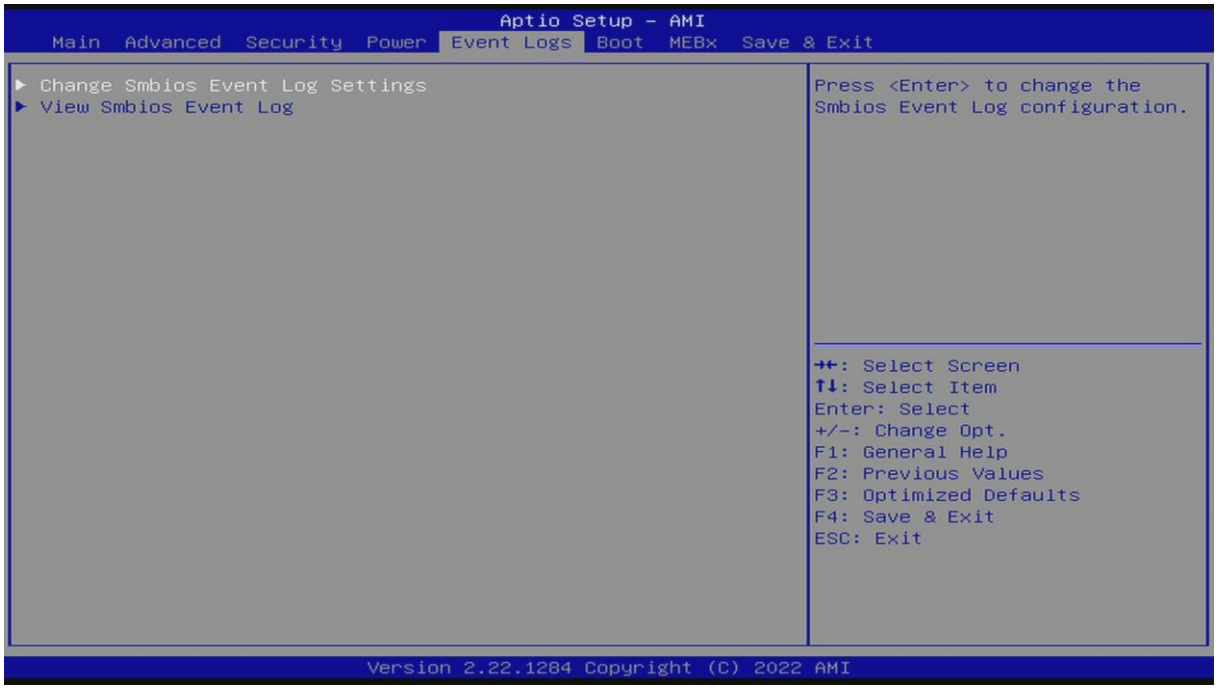


Figure 5: Event Log´s Screen

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

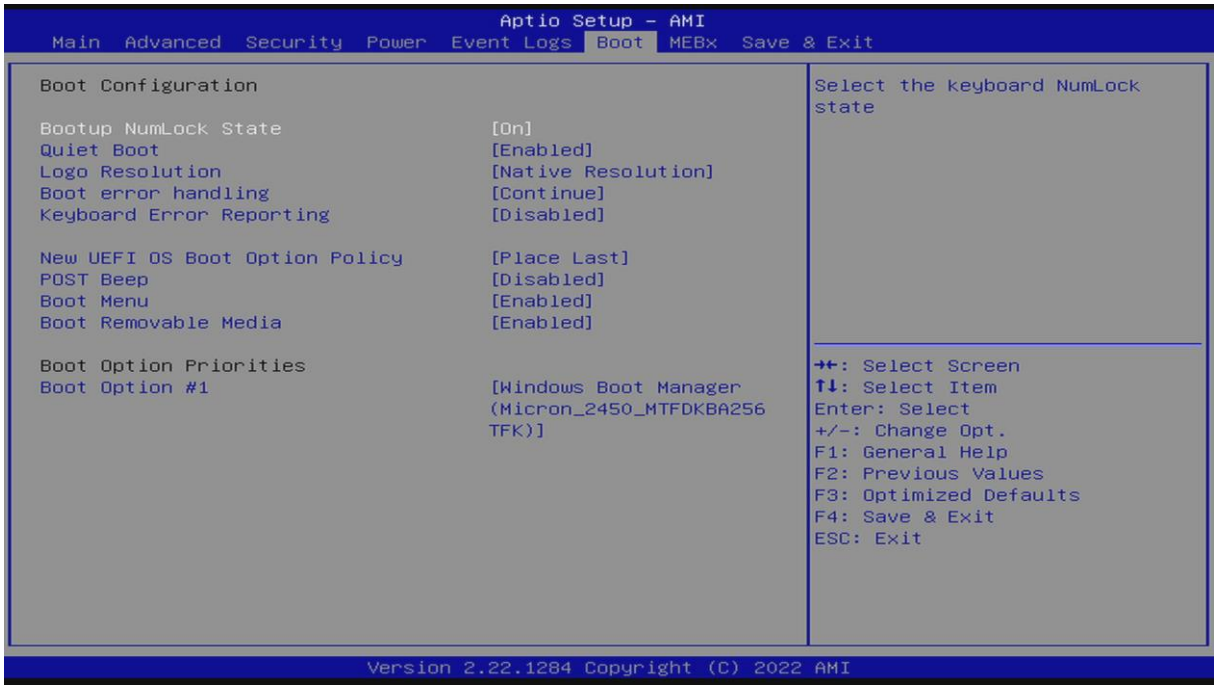


Figure 6: Boot Screen

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.
New UEFI OS Boot Option Policy	Configures the placement rule for new boot options in the boot options priorities list for non removeable media. [Default] No placement rule is applied to new boot options. [Place First] New boot options are placed at the beginning. [Place Last] New boot options are placed at the end.
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 up by pressing the [F12] key during the POST process. [Enabled] The Boot menu can be called up during the POST. [Disabled] The Boot menu cannot be called up during the POST.
Boot Removable Media	[**Enabled**, Disabled] Specifies whether booting via a removable data storage device such as a USB stick is supported. [Disabled] Booting via a removable data storage device is disabled. [Enabled] Booting via a removable data storage device is enabled.
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.

Function	Description
	Press the [Enter] key and select Disabled to remove the selected device from the boot order.
Boot Option #	List of Bootable Devices USB Floppy USB Key USB Hard Disk USB CD/DVD USB Lan Hard Disk CD/DVD Network Disabled

1.2.7. MEBx Setup Menu

The Intel® Management Engine BIOS Extension (MEBx) setup menu provides functions for Menu items depending on MEBx configuration or the Login state.

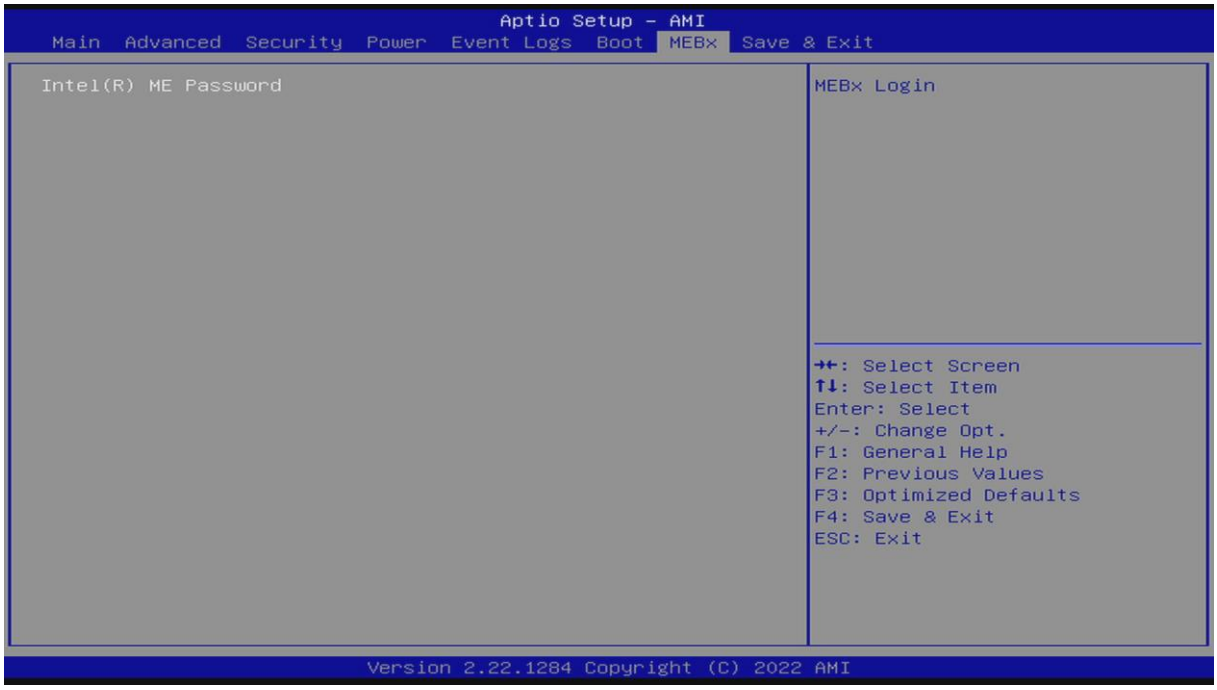


Figure 7: MEBx Setup Menu Initial Screen

Table 8: MEBx Setup Menu Functions

Function	Description
Intel® ME Password	MEBx Login

1.2.8. 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.

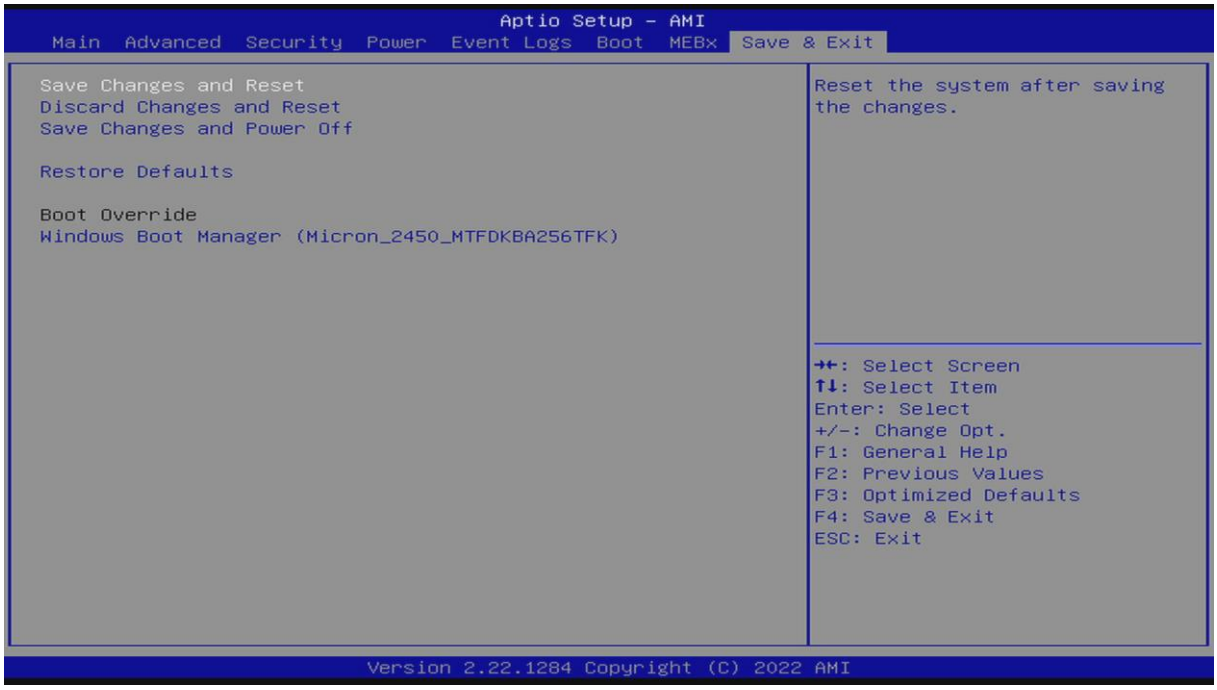


Figure 8: Save and Exit Setup Menu Initial Screen

Table 9: Save and Exit Setup Menu Functions

Function	Description
Save Changes and Exit	To save the current menu entries and exit the BIOS-Setup, select Save Changes and Exit followed by Yes. The new settings will be effective and the POST continues as long as no changed option requires a reset.
Discard Changes and Exit	Select Discard Changes and Exit followed by Yes to discard the changes you have made since entering BIOS-Setup or since invoking 'Save Changes'. The BIOS-Setup will be closed and the POST continues.
Save Changes and Power Off	To save the current entries in the menus and then shut down the system, select Save Changes and Power Off and Yes.
Restore Defaults	To reset all the menus of the BIOS setup to the default values, select Restore Defaults and Yes. If you wish to leave the BIOS Setup with these settings, select Save Changes and Exit and Yes.
Windows Boot Manager	List of Bootable devices

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