Alderamin Femto Mk5 Series

Version:
v1.0.0

Date:
25.11.2025

Contents

1 Copyright

2 Regulatory Compliances

2.1 Complies with the following EU directives

No	Short Name
2014/35/EU	Low Voltage Directive (LVD)
2014/30/EU	Electromagnetic Compatibility (EMC)
2011/65/EU	Restriction of the use of certain hazardous substances in electrical and electronic equipment Directive (RoHS2)
2015/863/EU	Amendment to Annex II in Directive 2011/65/EU regards the list of restricted substances (RoHS3)

2.2 References of standards applied

Standard	Reference	Issue
EN IEC 62368-1	Safety requirements: Audio/video, information and communication technology	2018 2020+A11:2020
IEC 61000-4-2	Electromagnetic compatibility (EMC) - Part 4-2: Testing and measurement techniques - Electrostatic discharge immunity test	2008
IEC 61000-4-4	Electromagnetic compatibility (EMC) - Part 4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test	2012
IEC 61000-4-3	Electromagnetic compatibility (EMC) - Part 4-3 : Testing and measurement techniques - Radiated, radio-frequency, electromagnetic field immunity test	2020
IEC 61000-4-6	Electromagnetic compatibility (EMC) - Part 4-6: Testing and measurement techniques - Immunity to conducted disturbances, induced by radio-frequency fields	2023 2008
IEC 61000-4-8	Electromagnetic compatibility (EMC) - Part 4-8: Testing and measurement techniques - Power frequency magnetic field immunity test	2009
EN 55032	Electromagnetic compatibility (EMC) of multimedia equipment: Emission Requirements	2015+A1:2020
EN 55035	Electromagnetic compatibility (EMC) of multimedia equipment: Immunity requirements	2017 2017+A11:2020
IEC 61000-4-5	Electromagnetic compatibility (EMC) - Part 4-5: Testing and measurement techniques - Surge immunity test	2014 + AMD1:2017
IEC 61000-4-11	Electromagnetic compatibility (EMC) - Part 4-11: Testing and measurement techniques - Voltage dips, short interruptions and voltage variations immunity tests	2020
EN 61000-3-2	Electromagnetic compatibility (EMC) - Part 3-2: Limits - Limits for harmonic current emissions	2019+A1:2021 Class A
EN 61000-3-3	Electromagnetic compatibility (EMC) - Part 3-3: Limits - Limitation of voltage changes, voltage fluctuations and flicker in public low-voltage supply systems	2013+A1:2019

3 Safety Instructions

Please read these instructions carefully and retain them for future reference.

1. Disconnect this equipment from the power outlet before cleaning. Do not use liquid or sprayed detergent for cleaning. Use a moist cloth or sheet.
2. Keep this equipment away from humidity.
3. Ensure the power cord is positioned to prevent tripping hazards and do not place anything on top of it.
4. Pay attention to all cautions and warnings on the equipment.
5. If the equipment is not used for an extended period, disconnect it from the main power to avoid damage from transient over-voltage.
6. **Prolonged usage with less than 8V may damage the PSU or destroy the mainboard.**
7. Never pour any liquid into openings as this could cause fire or electrical shock.
8. Have the equipment checked by service personnel if:
    - The power cord or plug is damaged.
    - Liquid has penetrated the equipment.
    - The equipment has been exposed to moisture in a condensation environment.
    - The equipment does not function properly, or you cannot get it to work by following the user manual.
    - The equipment has been dropped and damaged.
9. Do not leave this equipment in an unconditioned environment, with storage temperatures below -20 degrees or above 60 degrees Celsius for extended periods, as this may damage the equipment.
10. Unplug the power cord when performing any service or adding optional kits.
11. Lithium Battery Caution:
    - Risk of explosion if the battery is replaced incorrectly. Replace only with the original or an equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.
    - Do not remove the cover, and ensure no user-serviceable components are inside. Take the unit to a service center for service and repair.

⚠ Warning!
Always completely disconnect the power cord from your chassis whenever you work with the hardware. Do not make connections while the power is on. Sensitive electronic components can be damaged by sudden power surges. Only experienced electronics personnel should open the PC chassis.

⚠ Caution!
Always ground yourself to remove any static charge before touching the CPU card. Modern electronic devices are very sensitive to static electric charges. As a safety precaution, use a grounding wrist strap at all times. Place all electronic components in a static-dissipative surface or static-shielded bag when they are not in the chassis.

4 Product Specifications

Alderamin Femto Mk5 Embedded System offers the following features:

- Intel® Alder Lake-N N97 (4C) / i3-N305 (8C8T) Processor
- 1 x DDR5 SO-DIMM and support up to 16GB
- Support Triple display for LVDS (optional eDP), HDMI, and DisplayPort
- 2 x Intel® i226 2.5Gigabit Ethernet
- 1 x M.2 B Key, 1 x M.2 M Key, 1 x M.2 E Key slot
- 2 x USB 2.0, 3 x USB 3.2 Gen2, and 1 x USB Type C
- 8V~26V wide voltage power input
- Support Hailo-8™ AI Accelerator

4.1 Technical Details

Feature	Specification	Details
Processor	CPU	Intel® Alder Lake-N N97 (4C) / i3-N305 (8C8T), 10nm
Memory	System Memory	DDR5 4800 MHz, 1 x 262-pin SO-DIMM, Max. 16GB (Non-ECC)
Graphics	GPU	Intel® UHD Graphics
Storage	Storage Slots	- 2 x SATA III* - 1 x SATA power header - 1 x M.2 2242/3042/3052 B Key (USB2.0 / PCIe x1 / SATA III) - 1 x M.2 2280 M Key (PCIe x1 / SATA III) *Note: 1 SATA port multiplexed with M.2 B Key
Networking	Ethernet	2 x Intel® I226-V 2.5 Gigabit LAN
Audio	Audio	Realtek® ALC256
Security	I/O Chipset	Nuvoton NCT6126D
	TPM	Nuvoton NPCT760AABYX, TPM 2.0
I/O Ports	Internal I/O	1 x AT/ATX Mode Select Jumper 1 x CMOS Jumper 1 x Buzzer
	Front I/O	i3-N305 SKU: 3 x RS232 + 1 x RS232/422/485 N97 SKU: 1 x RS232 + 1 x RS232/422/485 2 x USB 2.0 1 x Line-out
	Side I/O	8-bit GPIO via 10-pin Terminal Block (i3-N305 SKU only) 2 x SMA Antenna hole with rubber caps
	Rear I/O	1 x DisplayPort 1.4 1 x HDMI 1.4 2 x RJ-45 3 x USB 3.2 Gen 2 (10Gbps) 1 x USB Type-C (PD15W, 5V/3A, DP Alt Mode, USB 3.2 Gen1) 1 x 2-pin Terminal Block (Remote Power On/Off) 1 x 2-pin Terminal Block (Power Input) 2 x SMA Antenna hole with rubber caps
Power	Power Input	8~26V Wide Range DC Input with Terminal Block Connectivity
Cooling	Thermal Design	Fanless
Mechanical	Dimensions	6.7” x 5.2” x 2.2” (171 mm x 133 mm x 57 mm)
Environmental	Operating Temperature	-25°C to 60°C (with 0.7 m/s airflow and extended-temp SSD/mSATA/RAM)
	Storage Temperature	-40°C to 85°C
	Operating Humidity	10%~95% R/H (Non-condensing)
	Vibration	5Hz~500Hz, 2Grms, 3 Axes (w/ SSD, IEC60068-2-64)

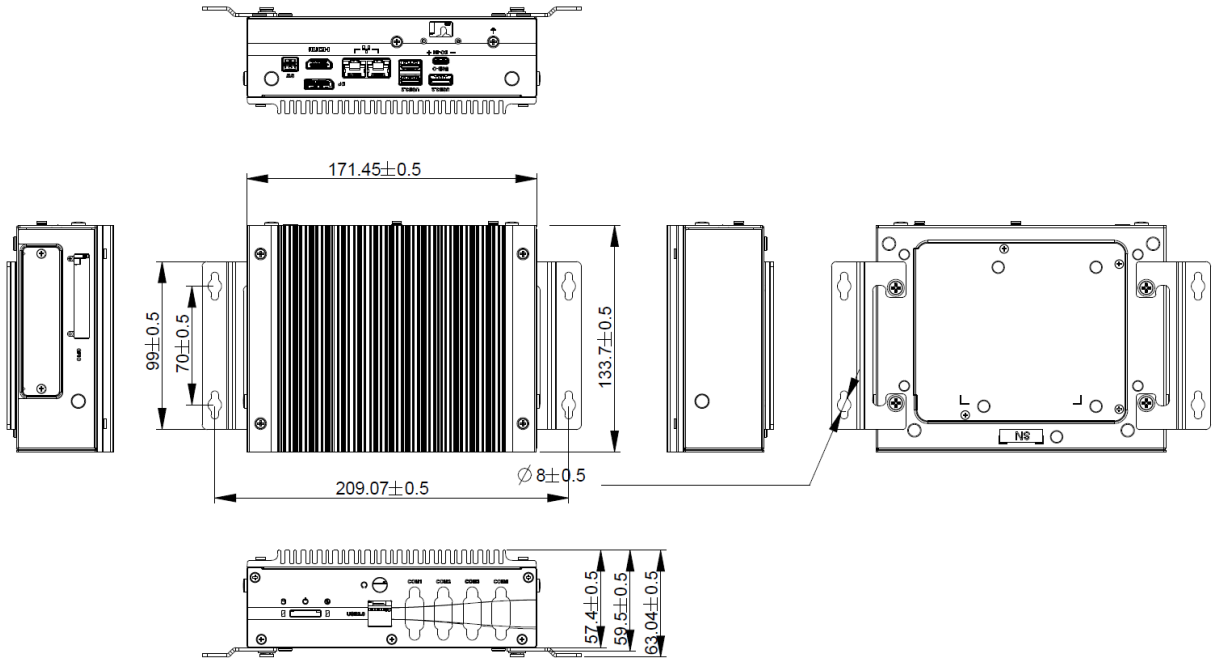
Note

This embedded system includes a lithium battery. Do not puncture, mutilate, or dispose of the battery in fire. There is a risk of explosion if the battery is replaced incorrectly. Replace only with the same or an equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions and local regulations.

The audio jack supports OMTP TRS & TRRS, and CTIA TRS. For CTIA TRRS, the jack may need to be pulled out slightly to ensure proper connection.

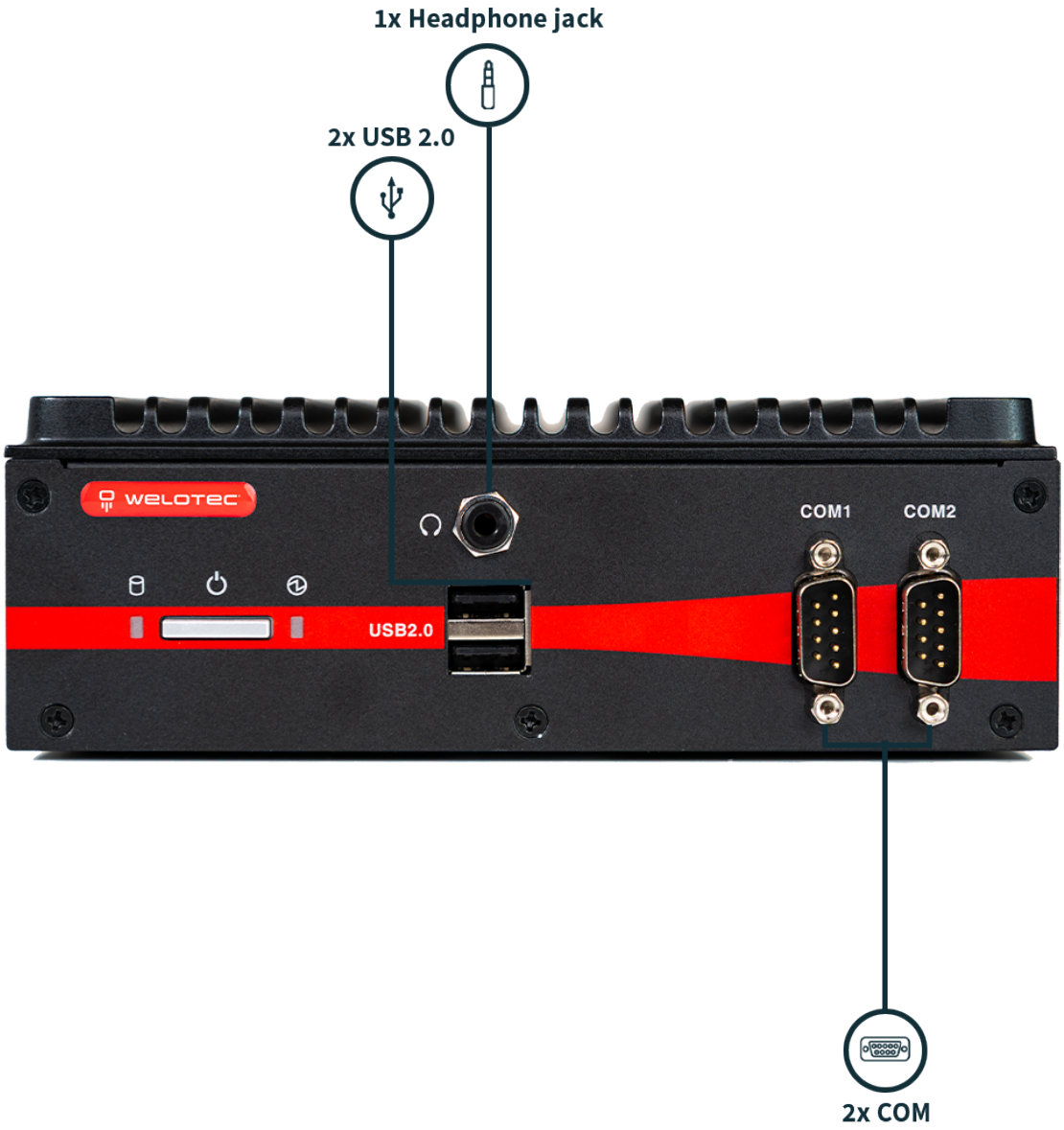
4.2 Mechanical Dimensions

Dimensions: 171 mm x 133 mm x 57 mm

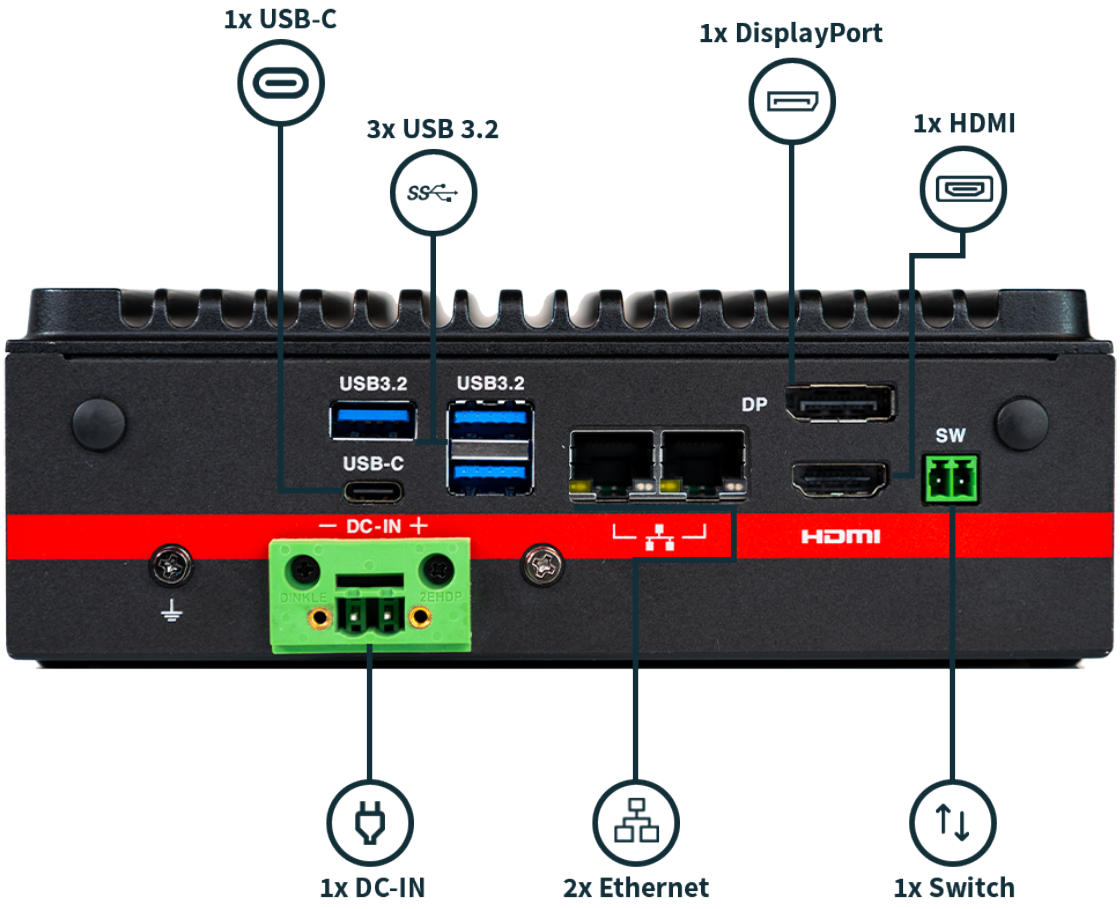


5 Interfaces and Connections

5.1 Front I/O

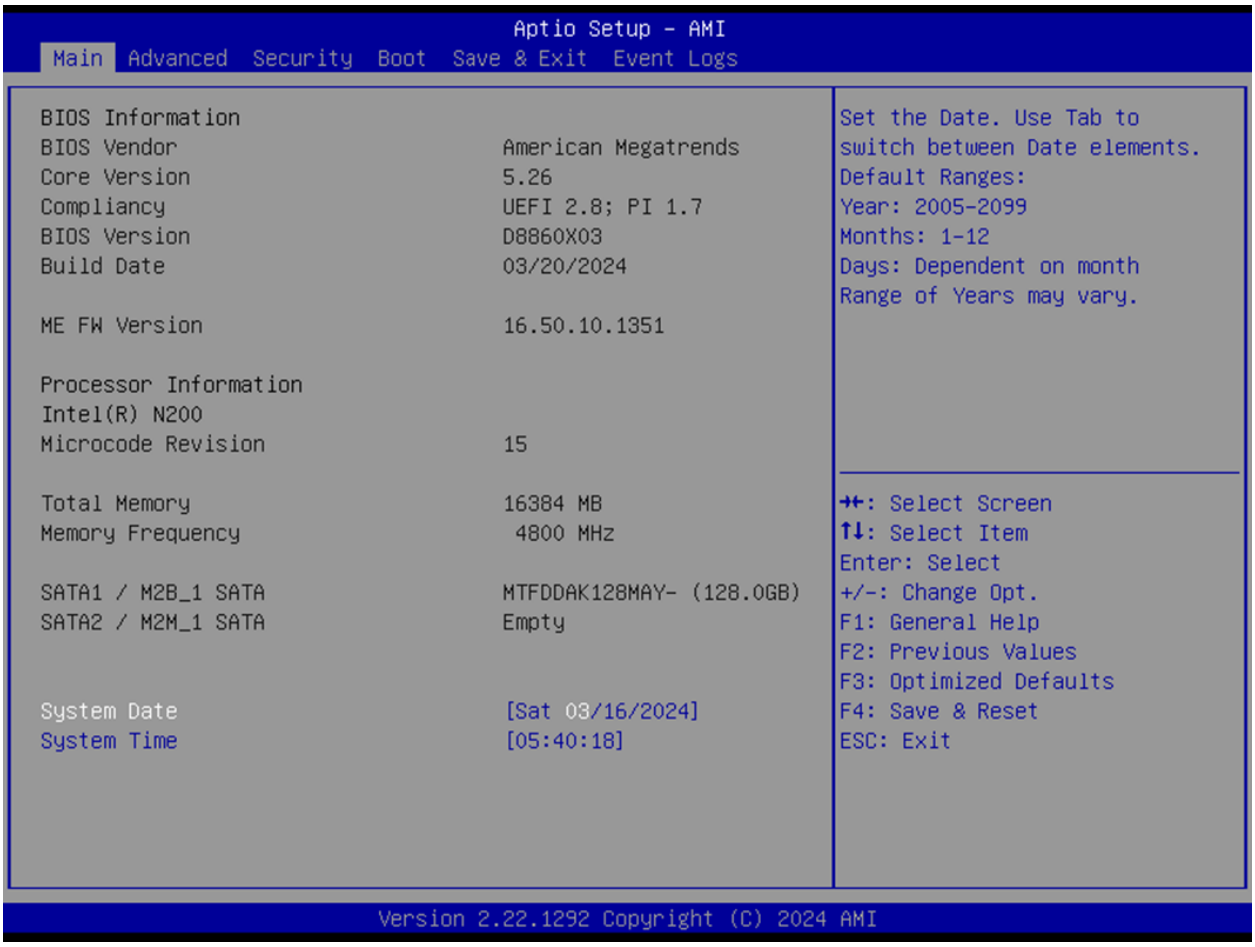


5.2 Rear I/O


1x USB-C
3x USB 3.2
1x DisplayPort
1x HDMI
USB3.2
USB3.2
USB-C
DP
SW
– DC-IN +
HDMI
1x DC-IN
2x Ethernet
1x Switch

6 BIOS

6.1 Main Page



The **Main Page** provides an overview of system-level information. All fields are display-only and cannot be modified:

- **BIOS Vendor:** American Megatrends
- **Core Version:** 5.26
- **Compliancy:** UEFI 2.8 ; PI 1.7
- **BIOS Version:** Displays the version of the BIOS
- **Build Date:** Shows the BIOS build date
- **ME FW Version:** Displays the Management Engine firmware version
- **Processor Information:** Displays the installed CPU brand
- **Microcode Revision:** Displays the CPU microcode revision
- **Total Memory:** Shows the installed memory size
- **Memory Frequency:** Displays the memory frequency

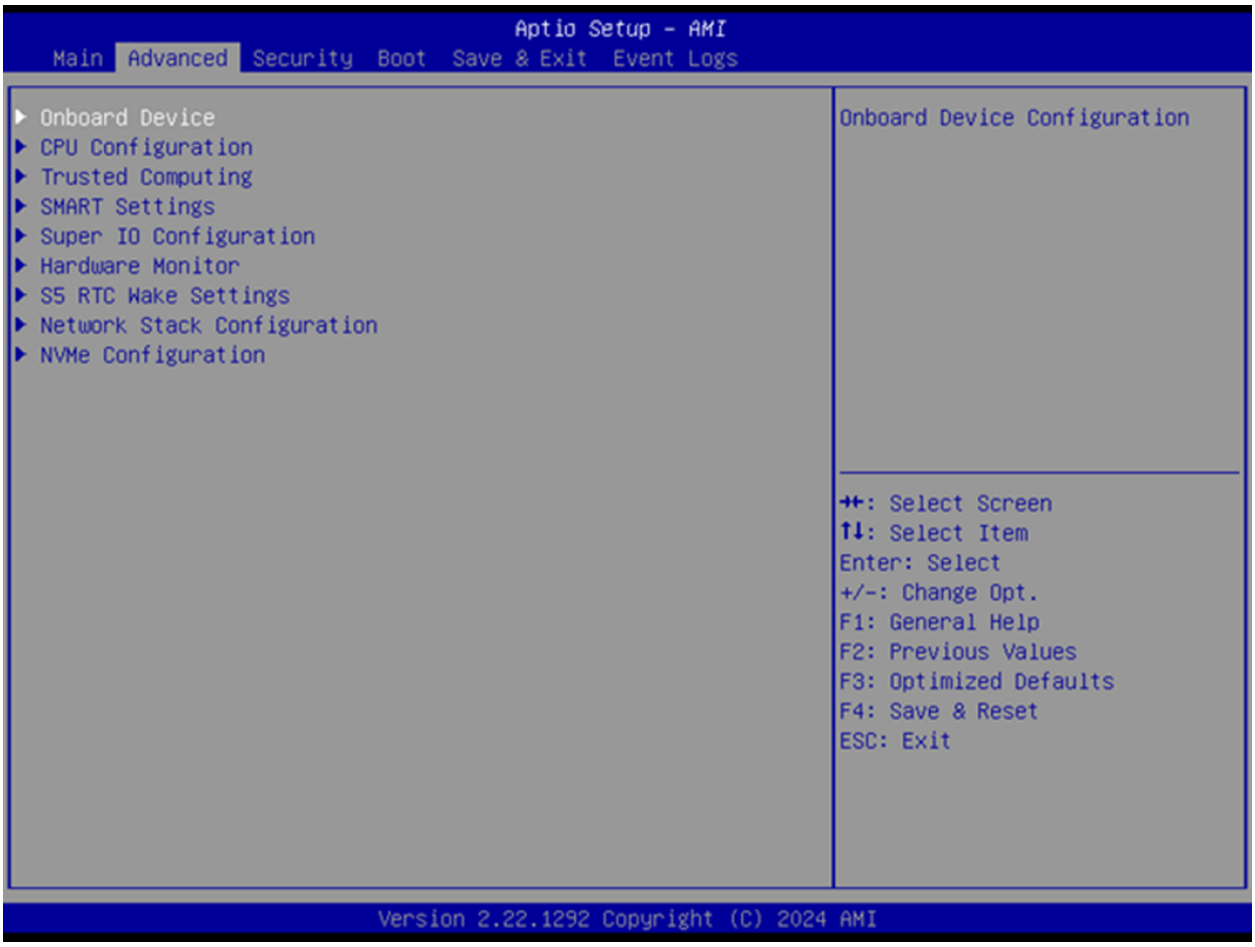
- **SATA1 / M2B_1 SATA:** Lists the installed SATA device model and size
- **SATA2 / M2M_1 SATA:** Lists the installed SATA device model and size

6.1.1 System Date & Time

The **System Date & Time** fields allow configuring the system's real-time clock:

- **System Date**
  - Format: `[Www mm/dd/yyyy]`
  - `Www`: Day of the week (Mon–Sun)
  - `mm`: Month (1–12)
  - `dd`: Day (1–31)
  - `yyyy`: Year (2005–2099)
  - Use Tab to switch between elements
- **System Time**
  - Format: `[hh:mm:ss]`
  - `hh`: Hours (0–23)
  - `mm`: Minutes (0–59)
  - `ss`: Seconds (0–59)
  - Use Tab to switch between elements

6.2 Advanced Page

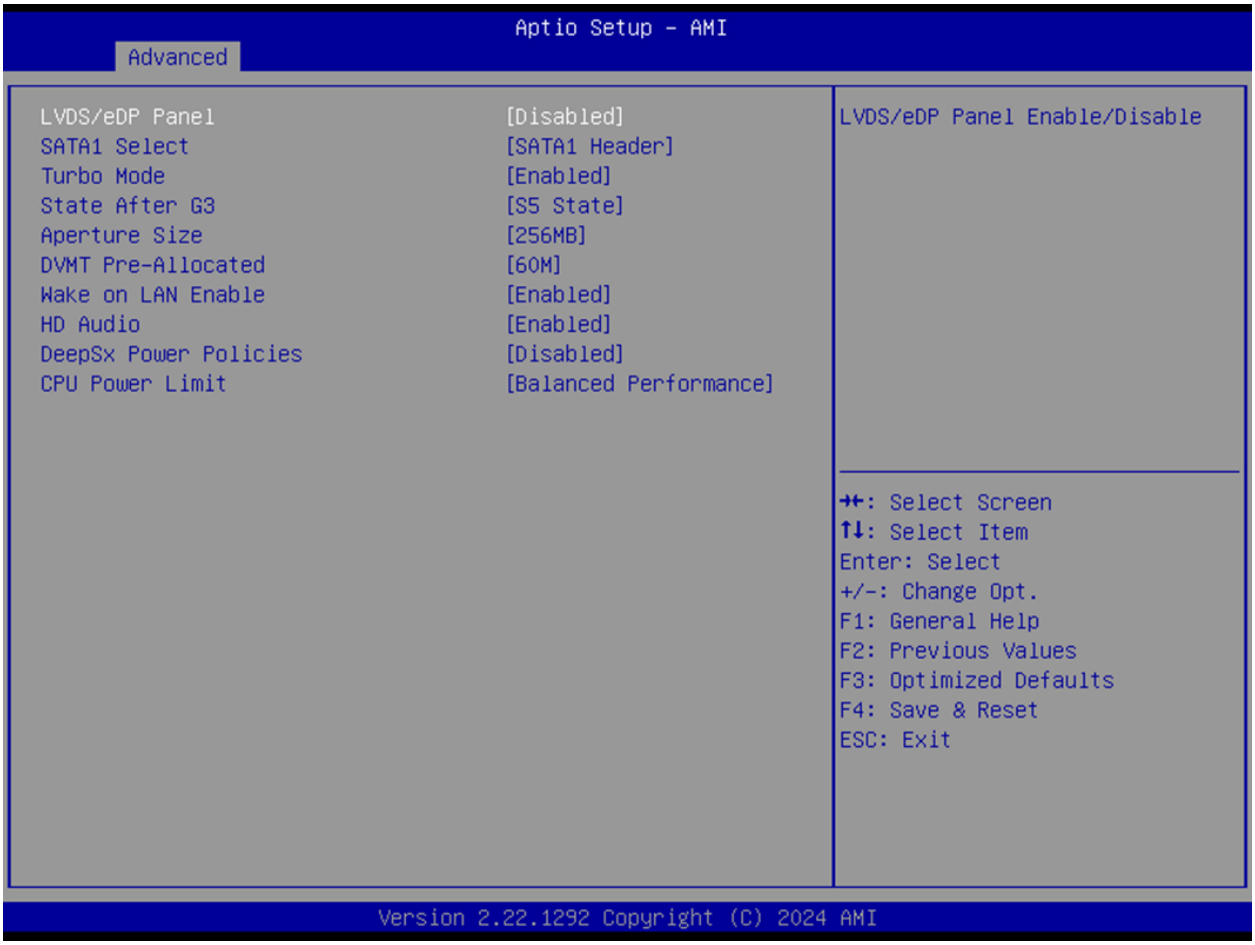


The **Advanced Page** gives you access to configuration menus for detailed system tuning and hardware settings.

6.2.1 Advanced Configuration Options

- **Onboard Device Configuration** – Press Enter to access onboard device settings
- **CPU Configuration** – Press Enter to configure CPU-related features
- **Trusted Computing** – Press Enter to access TPM settings
- **SMART Settings** – Press Enter to configure system SMART behavior
- **Super IO Configuration** – Press Enter to configure Super IO chip parameters
- **Hardware Monitor** – Press Enter to view hardware monitoring status
- **S5 RTC Wake Settings** – Press Enter to enable or disable RTC wake from S5 state
- **Network Stack Configuration** – Press Enter to manage network stack settings
- **NVMe Configuration** – Press Enter to view NVMe device options

6.3 Onboard Device Configuration



The **Onboard Device Configuration** menu allows you to enable or disable onboard components and adjust device-specific behavior.

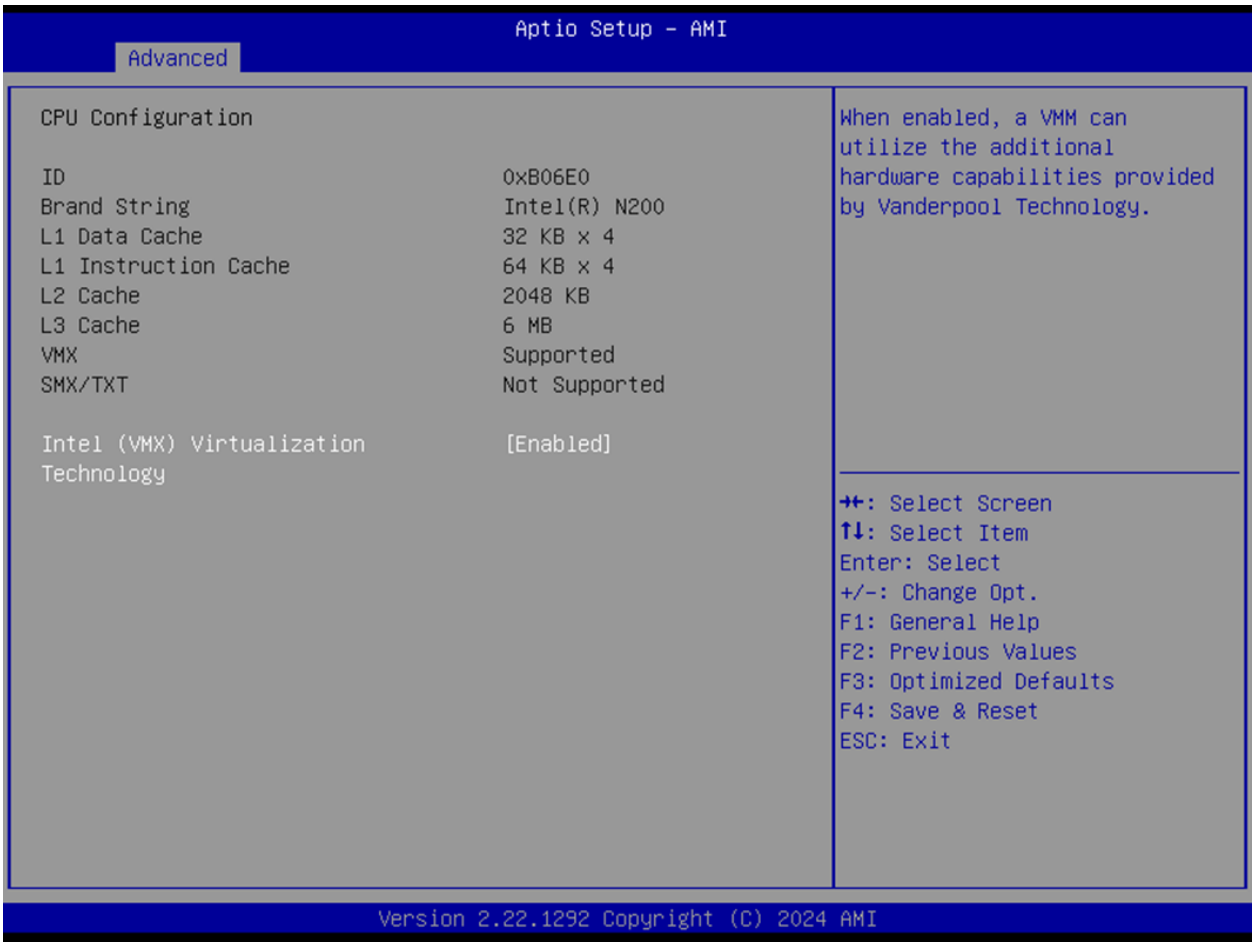
6.3.1 Device Settings

- **LVDS/eDP Panel**
  - Default: `Disabled`
  - Options: `Enabled`, `Disabled`
  - Enables or disables the LVDS/eDP panel output.
- **SATA1 Select**
  - Default: `SATA1 Header`
  - Options: `M2B SATA_PCIE Slot`, `SATA1 Header`
  - Selects the SATA1 device source.
- **Turbo Mode**
  - Default: `Enabled`
  - Options: `Enabled`, `Disabled`
  - Enables or disables the CPU's Turbo Boost feature.
- **State After G3**

  - Default: `S5 State`
  - Options: `S0 State`, `S5 State`
  - Determines the system power state after power is restored following a G3 (mechanical off) state.
- **Aperture Size**
  - Default: `256MB`
  - Options: `128MB`, `256MB`, `512MB`, `1024MB`
  - Sets the graphics aperture size.

    Note: Selecting aperture sizes above 2048MB enables automatic MMIO BIOS assignment. To use this feature, disable CSM Support.
- **DVMT Pre-Allocated**
  - Default: `60M`
  - Options: `32M`, `36M`, `40M`, `44M`, `48M`, `52M`, `56M`, `60M`, `64M`, `96M`, `128M`, `160M`, `32M/F7`
  - Sets fixed graphics memory size (DVMT 5.0) used by the internal graphics device.
- **Wake on LAN Enable**
  - Default: `Enabled`
  - Options: `Enabled`, `Disabled`
  - Allows the system to be powered on remotely via the LAN.
- **HD Audio**
  - Default: `Enabled`
  - Options: `Enabled`, `Disabled`
  - Controls detection of the HD-Audio device.
    Enabled: HDA always on
    Disabled: HDA always off
- **DeepSx Power Policies**
  - Default: `Disabled`
  - Options: `Disabled`, `Enabled in S4-S5`
  - Configures DeepSx low-power mode behavior in specific sleep states.
- **CPU Power Limit**
  - Default: `Balanced Performance`
  - Options: `Maximum Performance`, `Balanced Performance`, `Power Saver`
  - Sets CPU TDP configuration:
    * *Maximum Performance*: Uses max CPU TDP based on SKU
    * *Balanced Performance*: Limits TDP to 10W
    * *Power Saver*: Limits TDP to 6W (N97 only)

6.4 CPU Configuration



The **CPU Configuration** page displays processor-related information and supports virtualization settings. Most fields are read-only and cannot be modified.

6.4.1 CPU Details

- **ID**
  - Displays the CPU signature
  - *Not selectable*
- **Brand String**
  - Displays the CPU brand/model
  - *Not selectable*
- **L1 Data Cache**
  - Shows L1 data cache information
  - *Not selectable*
- **L1 Instruction Cache**
  - Shows L1 instruction cache information
  - *Not selectable*
- **L2 Cache**

  - Shows L2 cache information
  - *Not selectable*
- **L3 Cache**
  - Shows L3 cache information
  - *Not selectable*
- **VMX**
  - Displays whether Virtual Machine Extensions are supported
  - *Not selectable*
- **SMX/TXT**
  - Displays whether Safer Mode Extensions / Trusted Execution Technology is supported
  - *Not selectable*

6.4.2 Virtualization Setting

- **Intel® Virtualization Technology (VMX)**
  - Default: `Enabled`
  - Options: `Enabled`, `Disabled`
  - When enabled, virtualization-based software (VMM) can utilize additional hardware features provided by Intel® VT-x (Vanderpool Technology).

6.5 Trusted Computing

The **Trusted Computing** menu manages settings related to TPM (Trusted Platform Module) and BIOS-level hardware security.

6.5.1 TPM Information

- **Firmware Version**
  - Displays the installed TPM module firmware version
  - *Not selectable*
- **Vendor**
  - Shows the TPM vendor name
  - *Not selectable*

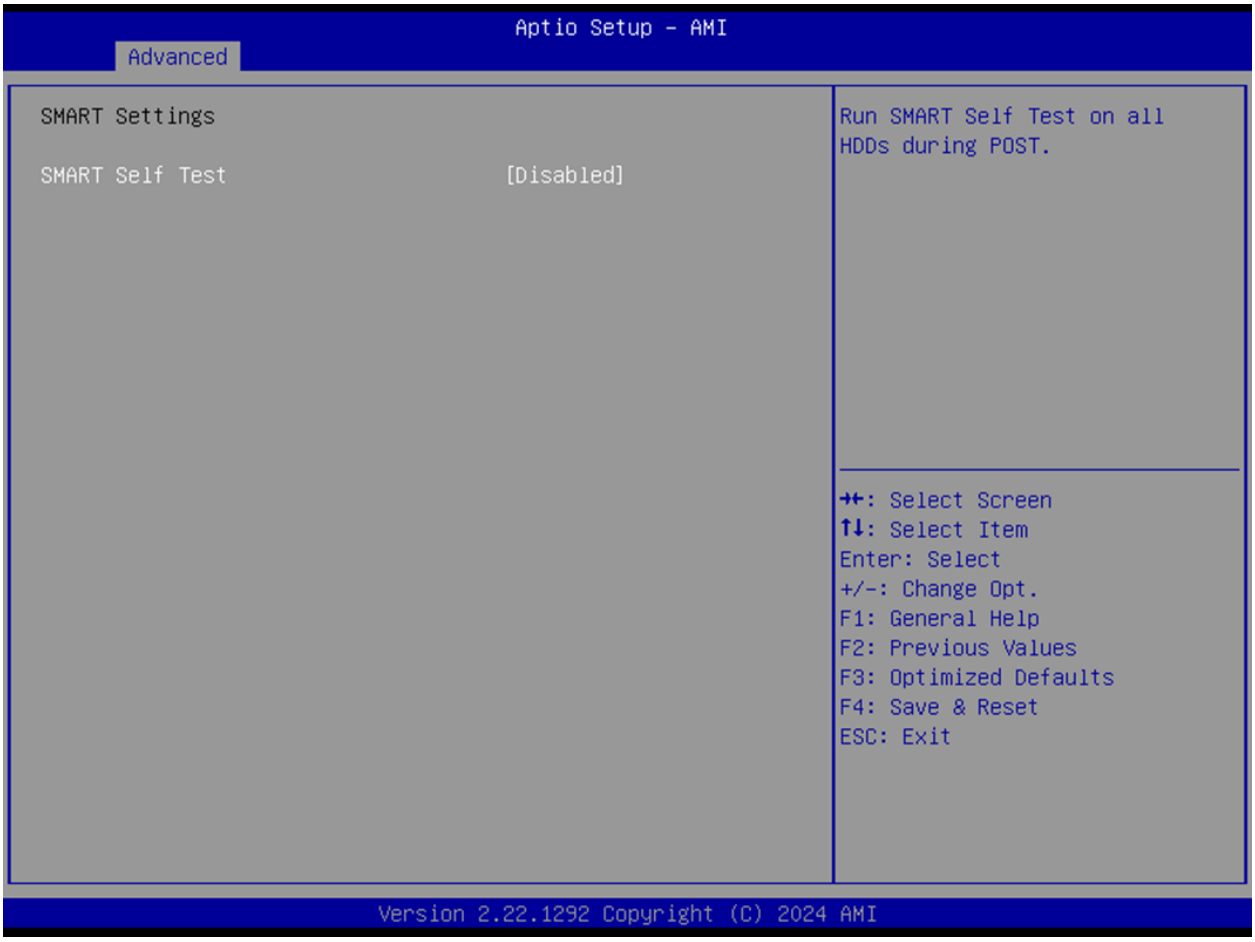
6.5.2 TPM Configuration

- **Security Device Support**
  - Default: `Enabled`
  - Options: `Enabled`, `Disabled`
  - Enables or disables BIOS-level support for the TPM device.

    Note: If disabled, TCG EFI protocol and INT1A interface will not be available, and the OS will not detect the security device.
- **Pending Operation**
  - Default: `None`
  - Options: `None`, `TPM Clear`
  - Schedules a TPM operation.

    Note: The system will reboot during restart to apply the change.

6.6 SMART Settings

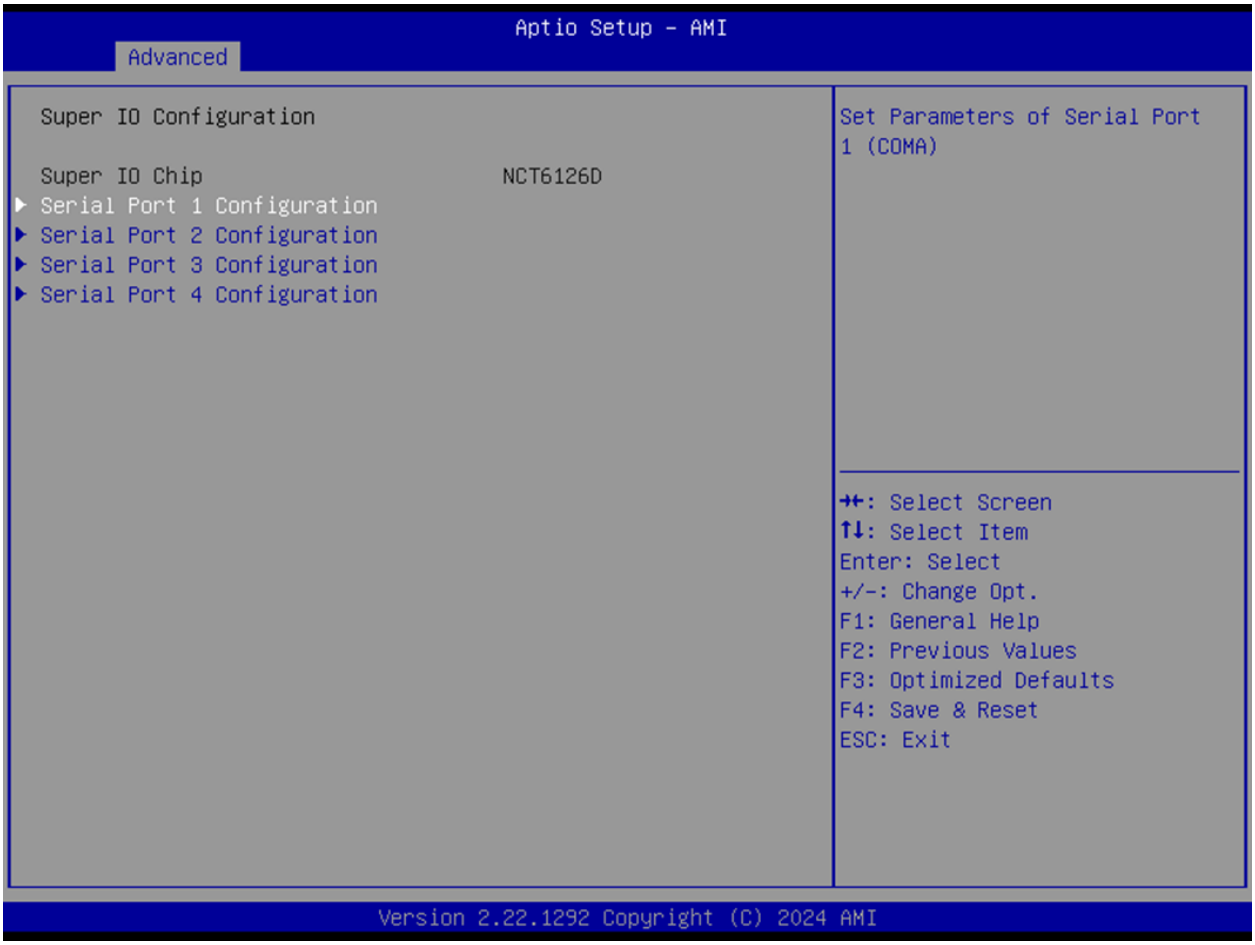


The **SMART Settings** menu allows configuration of SMART (Self-Monitoring, Analysis, and Reporting Technology) for storage health monitoring.

- **SMART Self Test**
  - Default: `Disabled`

- Options: `Enabled`, `Disabled`
- Enables SMART self-tests on all connected hard disk drives (HDDs) during POST (Power-On Self-Test).

6.7 Super IO Configuration



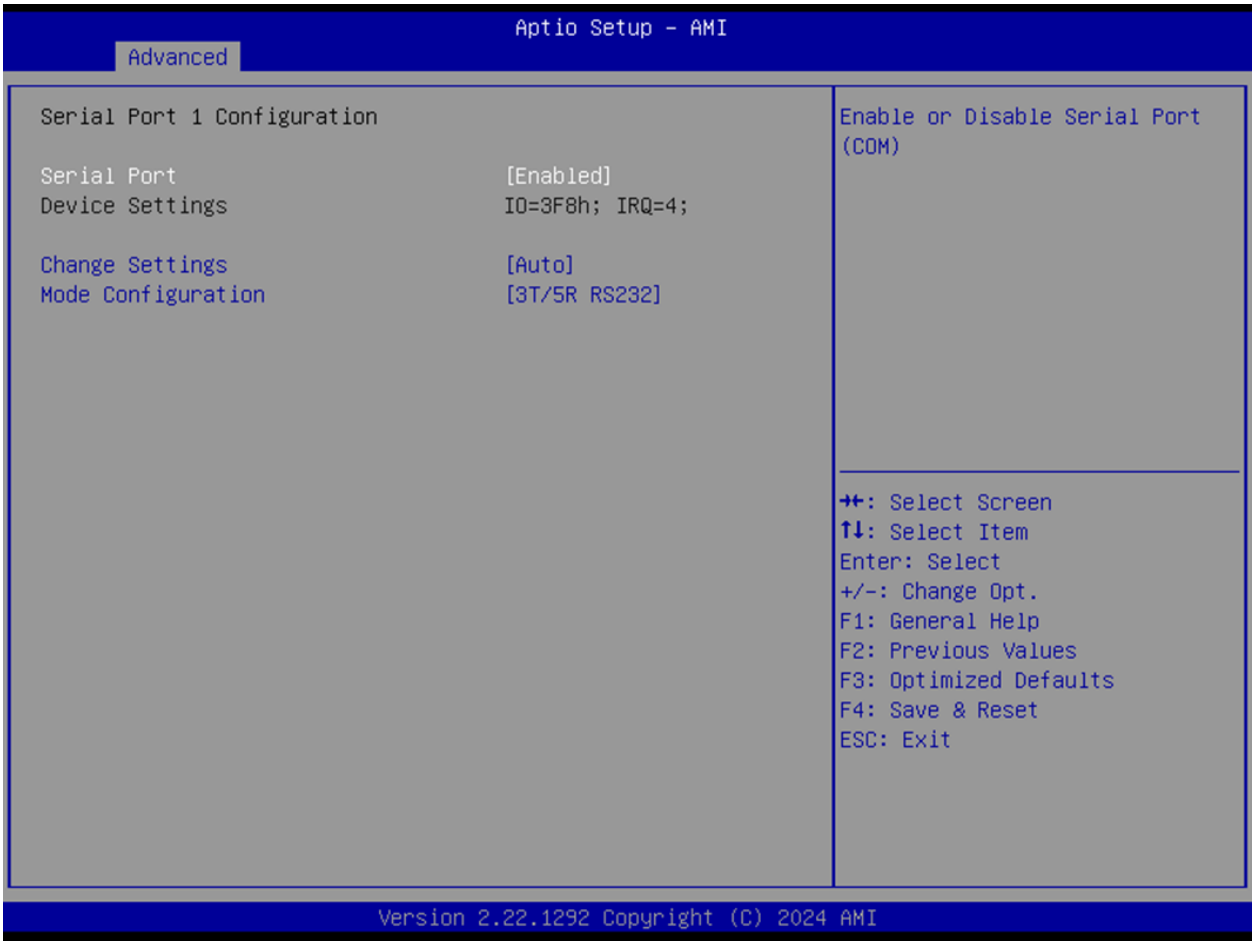
The **Super IO Configuration** menu provides access to settings for the system's serial ports.

6.7.1 Serial Port Configuration

- **Serial Port 1 Configuration**
  - Interface: COMA
  - Press Enter to access configuration submenu for Serial Port 1
- **Serial Port 2 Configuration**
  - Interface: COMB
  - Press Enter to access configuration submenu for Serial Port 2
- **Serial Port 3 Configuration**
  - Interface: COMC
  - Press Enter to access configuration submenu for Serial Port 3
- **Serial Port 4 Configuration**
  - Interface: COMD

- Press Enter to access configuration submenu for Serial Port 4

6.7.2 Serial Port 1 Configuration

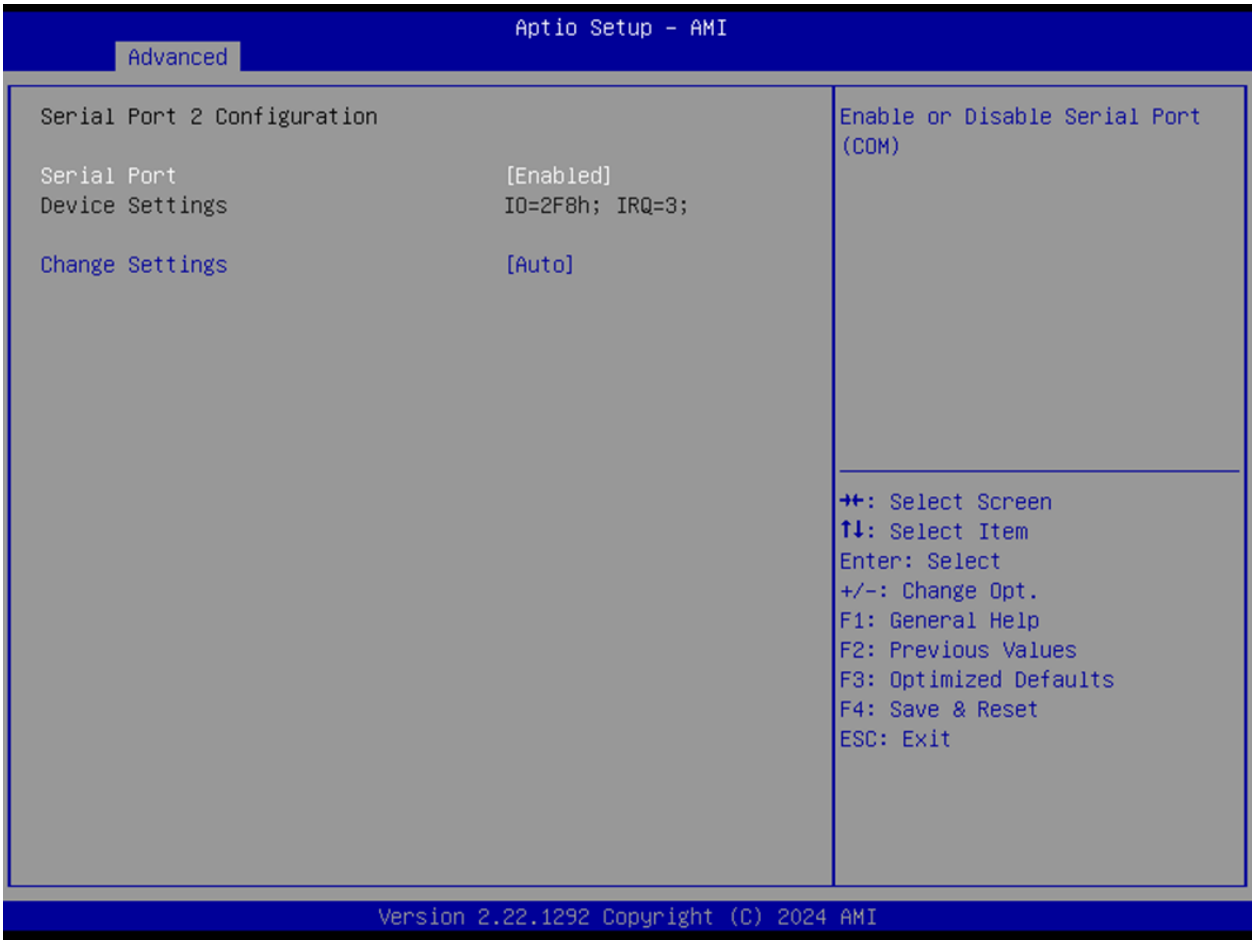


This section configures **Serial Port 1 (COMA)**, including enabling/disabling the port, assigning address/IRQ, and setting the operating mode.

- **Serial Port**
  - Default: `Enabled`
  - Options: `Enabled`, `Disabled`
  - Enables or disables the serial port (COMA).
- **Device Settings**
  - Displays Super IO COM1 address and IRQ
  - *Not selectable*
- **Change Settings**
  - Default: `Auto`
  - Options:
    * `Auto`
    * `IO=3F8h; IRQ=4`
    * `IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12`

    * IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12
    * IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12
    * IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12
  - Allows selecting optimal COM1 settings manually or automatically.
- **Mode Configuration**
  - Default: 3T/5R RS232
  - Options:
    * 1T/1R RS422
    * 3T/5R RS232
    * 1T/1R RS485 TX ENABLE Low Active
    * 1T/1R RS422 with termination resistor
    * 1T/1R RS485 with termination resistor TX ENABLE Low Active
  - Configures the serial port communication mode (RS232/RS422/RS485).

6.7.3 Serial Port 2 Configuration

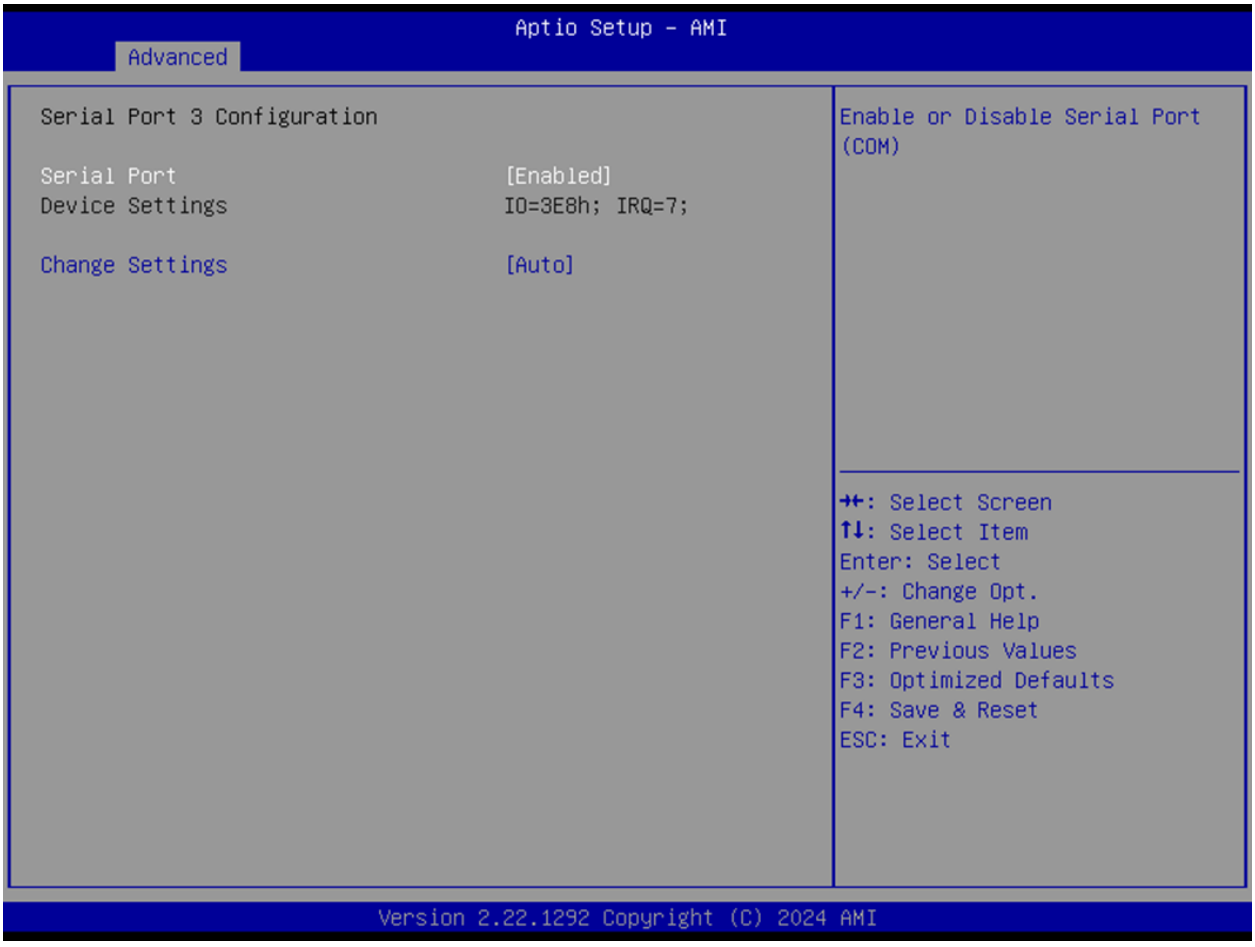


This section configures **Serial Port 2 (COMB)**.

- **Serial Port**
  - Default: Enabled

  - Options: `Enabled`, `Disabled`
  - Enables or disables the serial port (COMB).
- **Device Settings**
  - Displays Super IO COM2 address and IRQ
  - *Not selectable*
- **Change Settings**
  - Default: `Auto`
  - Options:
    * `Auto`
    * `IO=2F8h; IRQ=3`
    * `IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12`
    * `IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12`
    * `IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12`
    * `IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12`
  - Allows selecting optimal COM2 settings manually or automatically.

6.7.4 Serial Port 3 Configuration



This section configures **Serial Port 3 (COMC)**.

- **Serial Port**
  - Default: `Enabled`
  - Options: `Enabled`, `Disabled`
  - Enables or disables the serial port (COMC).
- **Device Settings**
  - Displays Super IO COM3 address and IRQ
  - *Not selectable*
- **Change Settings**
  - Default: `Auto`
  - Options:
    * `Auto`
    * `IO=3E8h; IRQ=7`
    * `IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12`
    * `IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12`
    * `IO=220h; IRQ=3,4,5,6,7,9,10,11,12`
    * `IO=228h; IRQ=3,4,5,6,7,9,10,11,12`
  - Allows selecting optimal COM3 settings manually or automatically.

6.7.5 Serial Port 4 Configuration

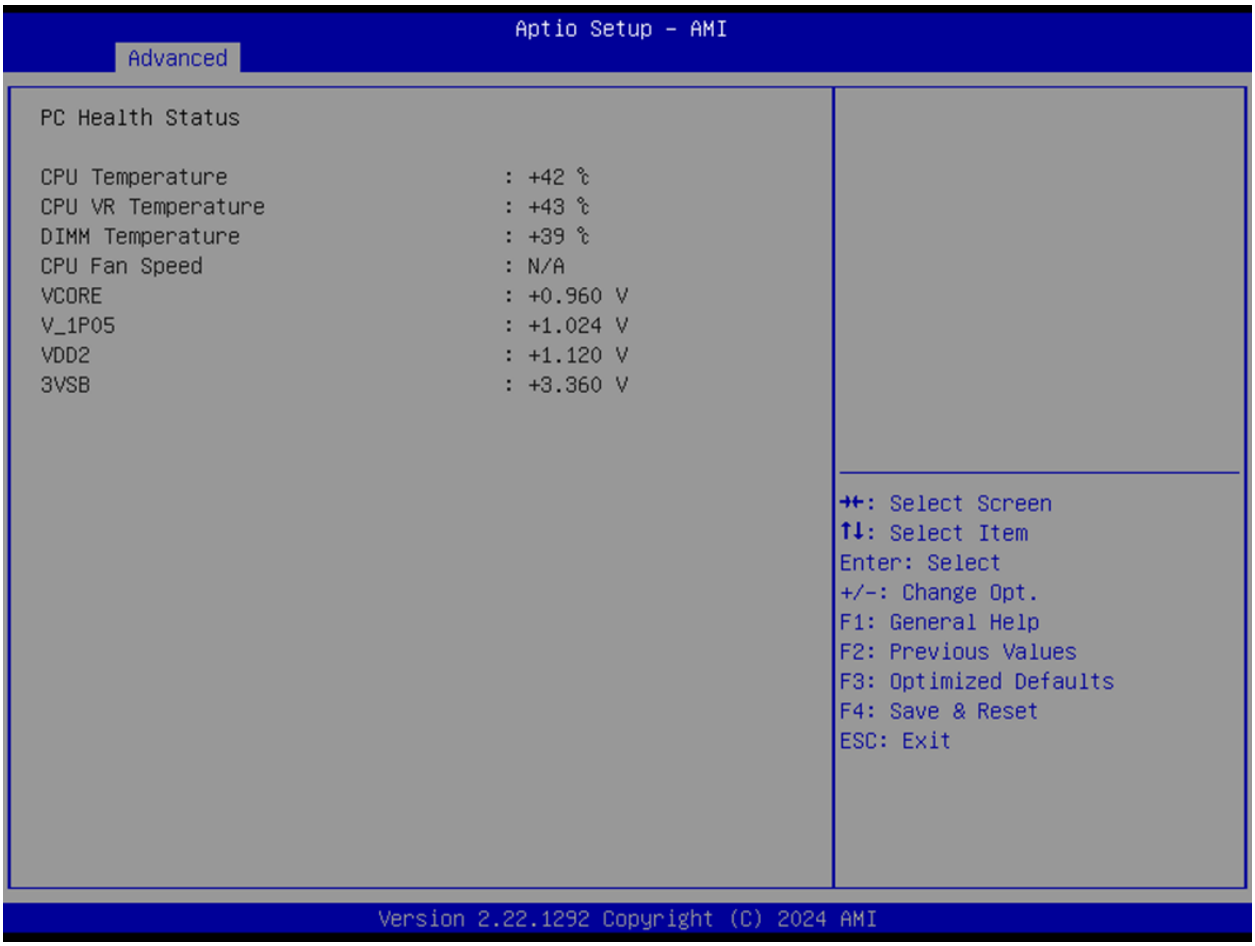
This section configures **Serial Port 4 (COMD)**.

- **Serial Port**
  - Default: `Enabled`
  - Options: `Enabled`, `Disabled`
  - Enables or disables the serial port (COMD).
- **Device Settings**
  - Displays Super IO COM4 address and IRQ
  - *Not selectable*
- **Change Settings**
  - Default: `Auto`
  - Options:
    - `Auto`
    - `IO=2E8h; IRQ=7`
    - `IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12`
    - `IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12`
    - `IO=220h; IRQ=3,4,5,6,7,9,10,11,12`

* IO=228h; IRQ=3,4,5,6,7,9,10,11,12

– Allows selecting optimal COM4 settings manually or automatically.

6.8 Hardware Monitor



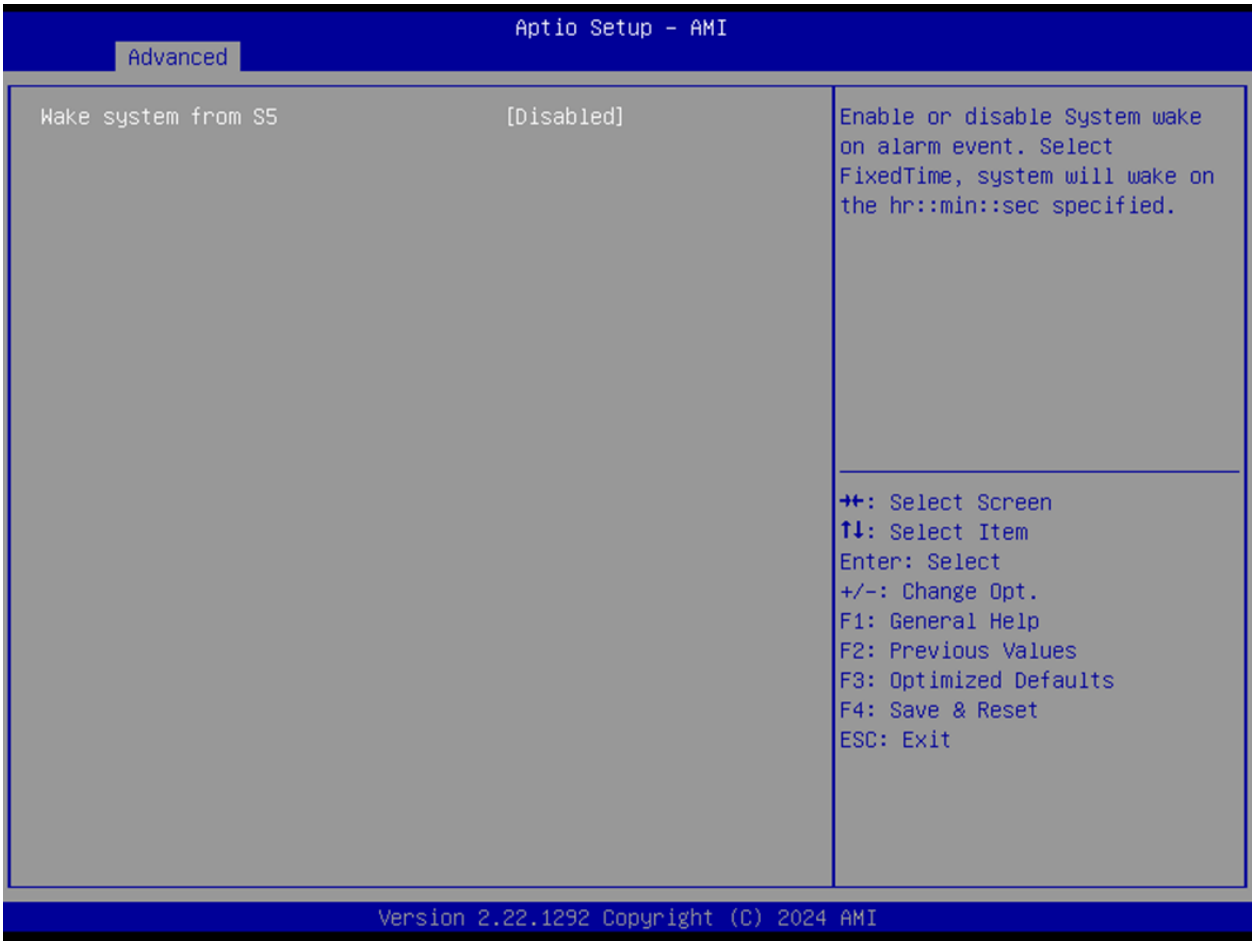
The **Hardware Monitor** page displays real-time system temperature, fan, and voltage information. All fields are read-only and intended for system diagnostics.

6.8.1 Sensor Readings

Type	Range
CPU Temperature	-20°C to Processor TjMax
CPU VR Temperature	-20°C to 120°C
DIMM Temperature	-20°C to 120°C
CPU Fan Speed	0 RPM (minimum failure threshold) – No upper RPM limit
VCORE	0 V to 1.72 V
V_1P05	0.9975 V to 1.1025 V
VDD2	1.045 V to 1.155 V
3VSB	3.135 V to 3.465 V

Note: Fan speed and voltage thresholds are system- and sensor-dependent. RPM reading of 0 indicates a fan failure condition.

6.9 S5 RTC Wake Settings

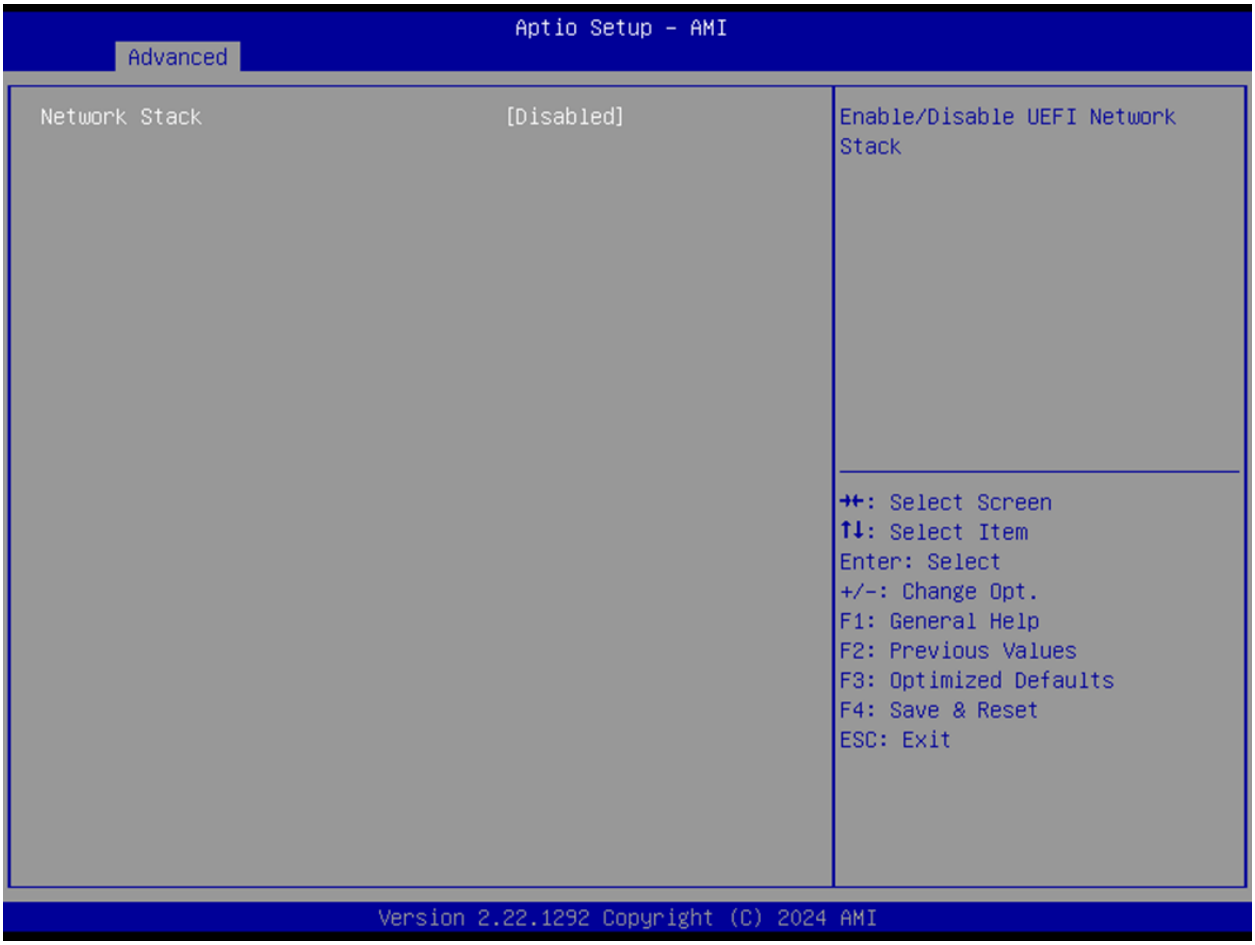


The **S5 RTC Wake Settings** menu configures automatic system wake-up behavior from the S5 (Soft Off) state.

- **Wake System from S5**
  - Default: `Disabled`
  - Options: `Disabled`, `Fixed Time`
  - Enables the system to wake at a defined time from S5 state.
- **Wake Up Hour** *(Visible when Fixed Time is selected)*
  - Default: `0`
  - Range: `0–23`
  - Sets the hour of wake-up. (e.g., 3 = 3 AM, 15 = 3 PM)
- **Wake Up Minute** *(Visible when Fixed Time is selected)*
  - Default: `0`
  - Range: `0–59`
  - Sets the minute of wake-up.
- **Wake Up Second** *(Visible when Fixed Time is selected)*

- Default: 0
- Range: 0–59
- Sets the second of wake-up.

6.10 Network Stack Configuration

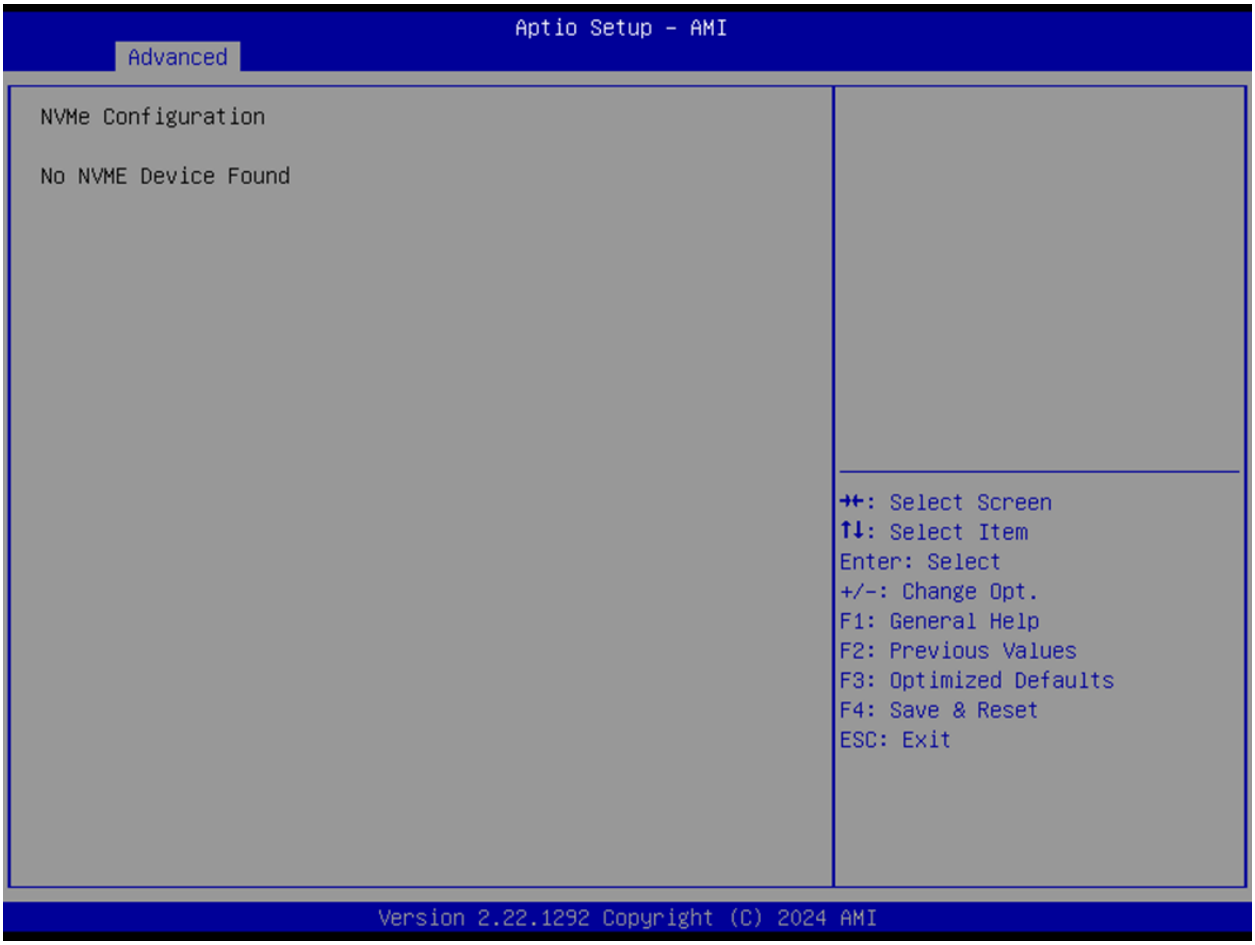


This section allows configuring the UEFI network stack and related PXE boot options.

- **Network Stack**
  - Default: `Disabled`
  - Options: `Enabled`, `Disabled`
  - Enables or disables the UEFI network stack.
- **IPv4 PXE Support** *(Available when Network Stack is Enabled)*
  - Default: `Disabled`
  - Options: `Enabled`, `Disabled`
  - Enables IPv4 PXE boot support.
- **IPv6 PXE Support** *(Available when Network Stack is Enabled)*
  - Default: `Disabled`
  - Options: `Enabled`, `Disabled`

- Enables IPv6 PXE boot support.

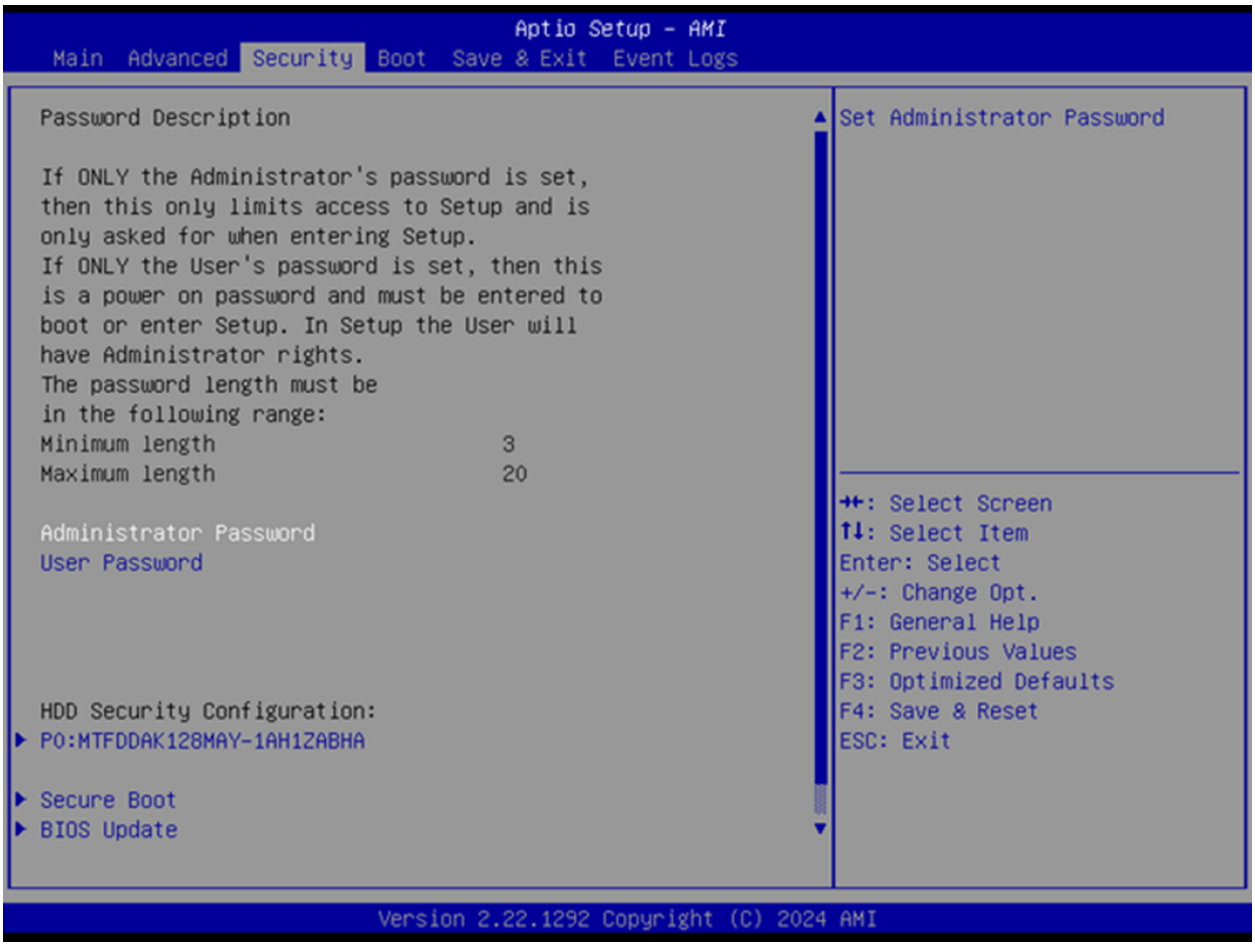
6.11 NVMe Configuration



The **NVMe Configuration** page provides access to settings and information related to connected NVMe devices.

- **(Device)**
  - Press Enter to view device details and configuration sub-menu.

6.12 Security Page

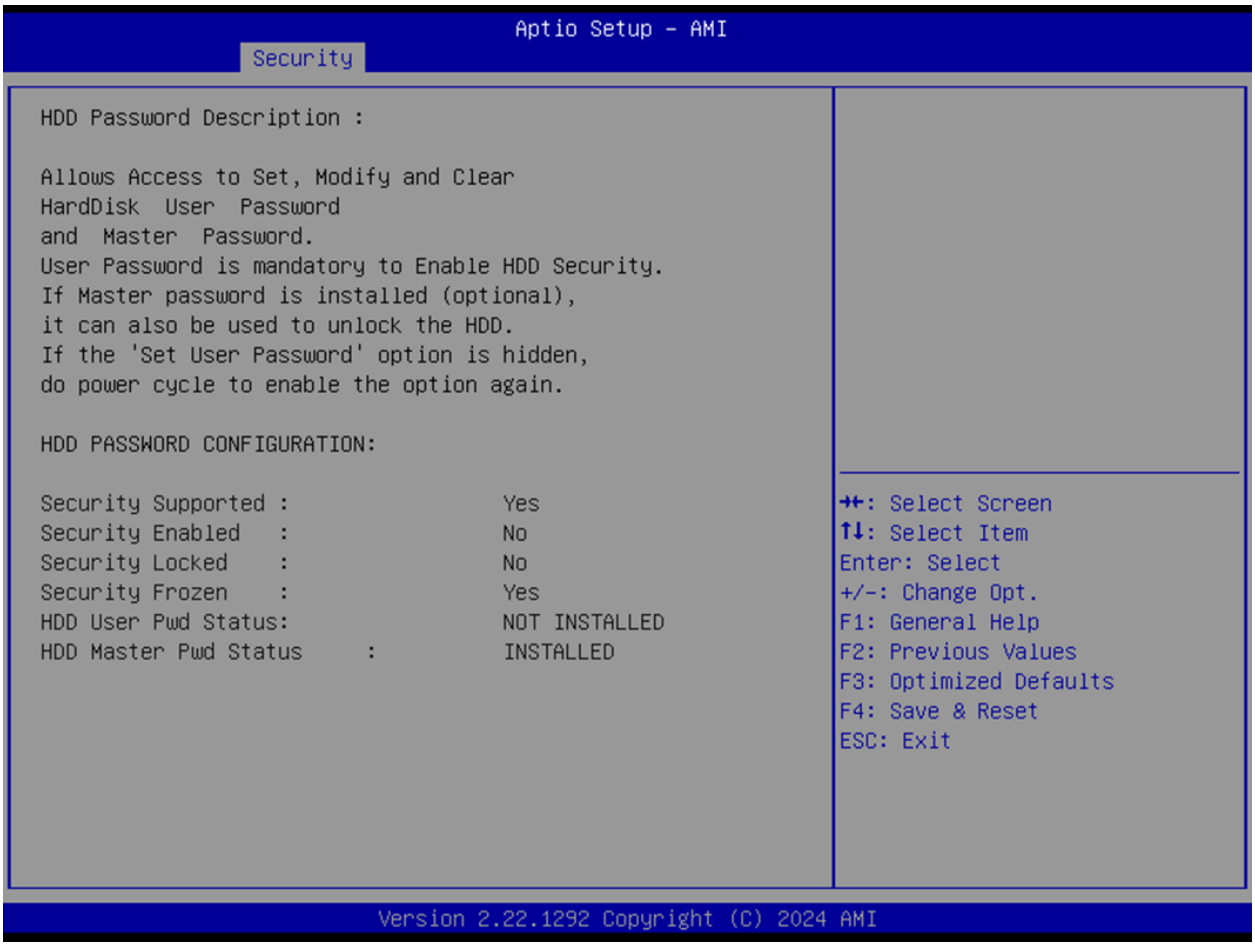


The **Security Page** allows users to configure BIOS access protection, disk security, secure boot, and firmware update options.

6.12.1 Security Options

- **Administrator Password**
  - Set or modify the administrator password to control access to BIOS settings.
- **User Password**
  - Set or modify a user-level password for limited access.
- **HDD Security Drive**
  - Opens the HDD security configuration menu for password protection on specific drives.
  - *Press Enter to access submenu.*
- **Secure Boot**
  - Opens the Secure Boot configuration menu for key and policy management.
  - *Press Enter to access submenu.*
- **BIOS Update**
  - Launches the BIOS update utility.
  - *Press Enter to access submenu.*

6.13 HDD Security



This submenu configures password protection for hard disk drives.

- **Set User Password**
  - Sets a user password for the selected HDD.

    After setting or removing HDD passwords, a full power cycle is recommended. Changes made here are independent of BIOS save/discard actions. If this field becomes hidden, perform a power cycle to restore visibility.

6.14 Secure Boot

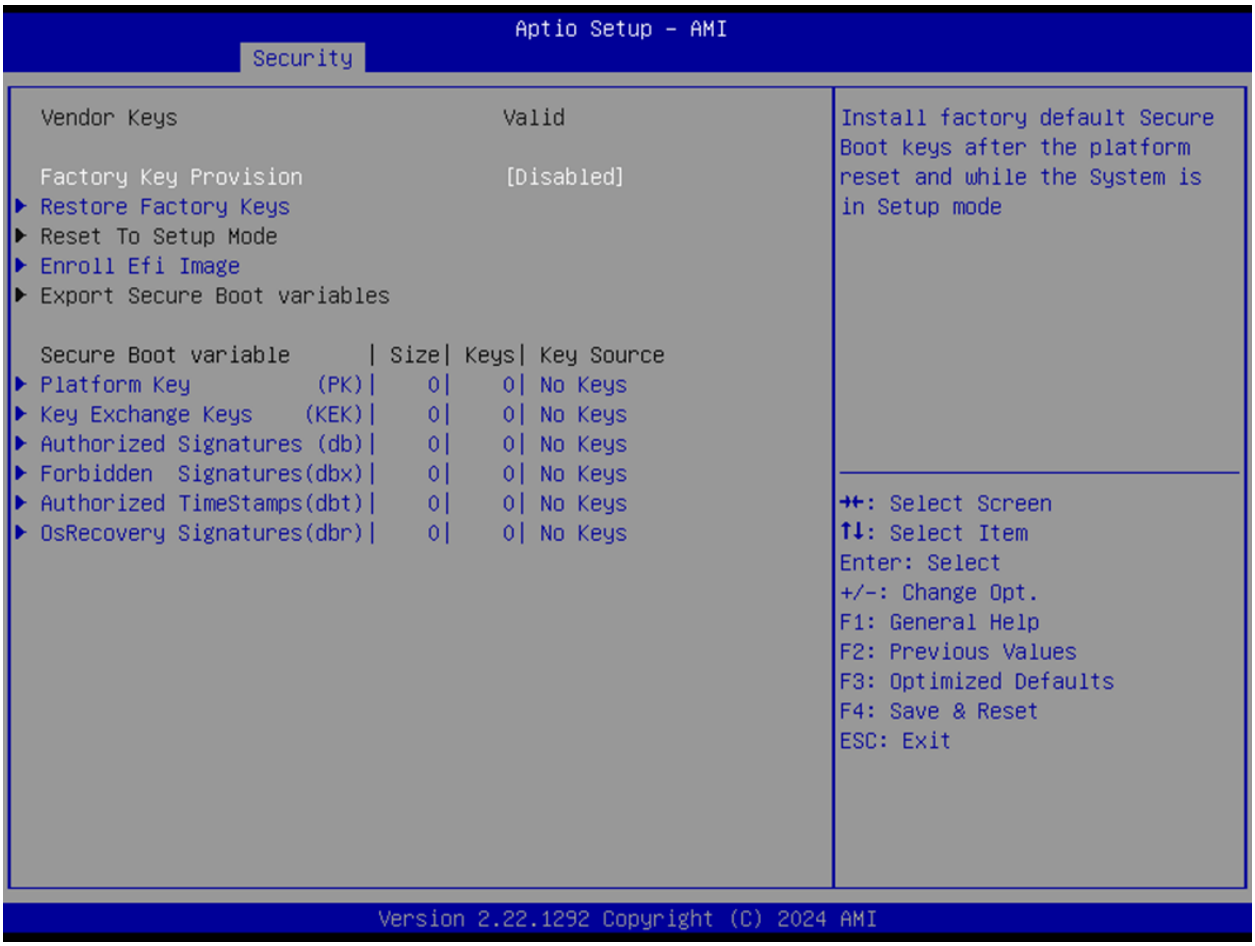
The **Secure Boot** feature ensures that only trusted operating systems and software are loaded during startup.

- **Secure Boot**
  - Default: `Enabled`
  - Options: `Enabled`, `Disabled`
  - When enabled, Secure Boot is active if a Platform Key (PK) is enrolled and the system is in User Mode.

    Mode changes require a platform reset.
- **Secure Boot Mode**
  - Default: `Standard`
  - Options: `Standard`, `Custom`
  - In **Standard** mode, keys and policies follow default specifications.
    In **Custom** mode, policy variables can be modified by a physically present user without full authentication.
- **Restore Factory Keys**
  - Restores factory default Secure Boot key databases and forces system into User Mode.
- **Reset to Setup Mode**
  - Deletes all Secure Boot key databases from NVRAM.
- **Key Management**

- Opens advanced Secure Boot key management options.
- *Press Enter to access submenu.*

6.15 Key Management



The **Key Management** submenu provides expert-level control over Secure Boot certificates and key databases.

- **Factory Key Provision**
  - Default: `Disabled`
  - Options: `Enabled`, `Disabled`
  - Installs factory default Secure Boot keys after platform reset when in Setup Mode.
- **Restore Factory Keys**
  - Reinstalls all factory Secure Boot keys and switches system to User Mode.
- **Reset to Setup Mode**
  - Clears all Secure Boot key databases from NVRAM.
- **Enroll EFI Image**
  - Allows SHA256 hash of a PE image to be enrolled into the authorized signature database (db) to permit its execution under Secure Boot.
- **Export Secure Boot Variables**
  - Saves the content of current Secure Boot variables from NVRAM to a file.

6.15.1 Key Databases

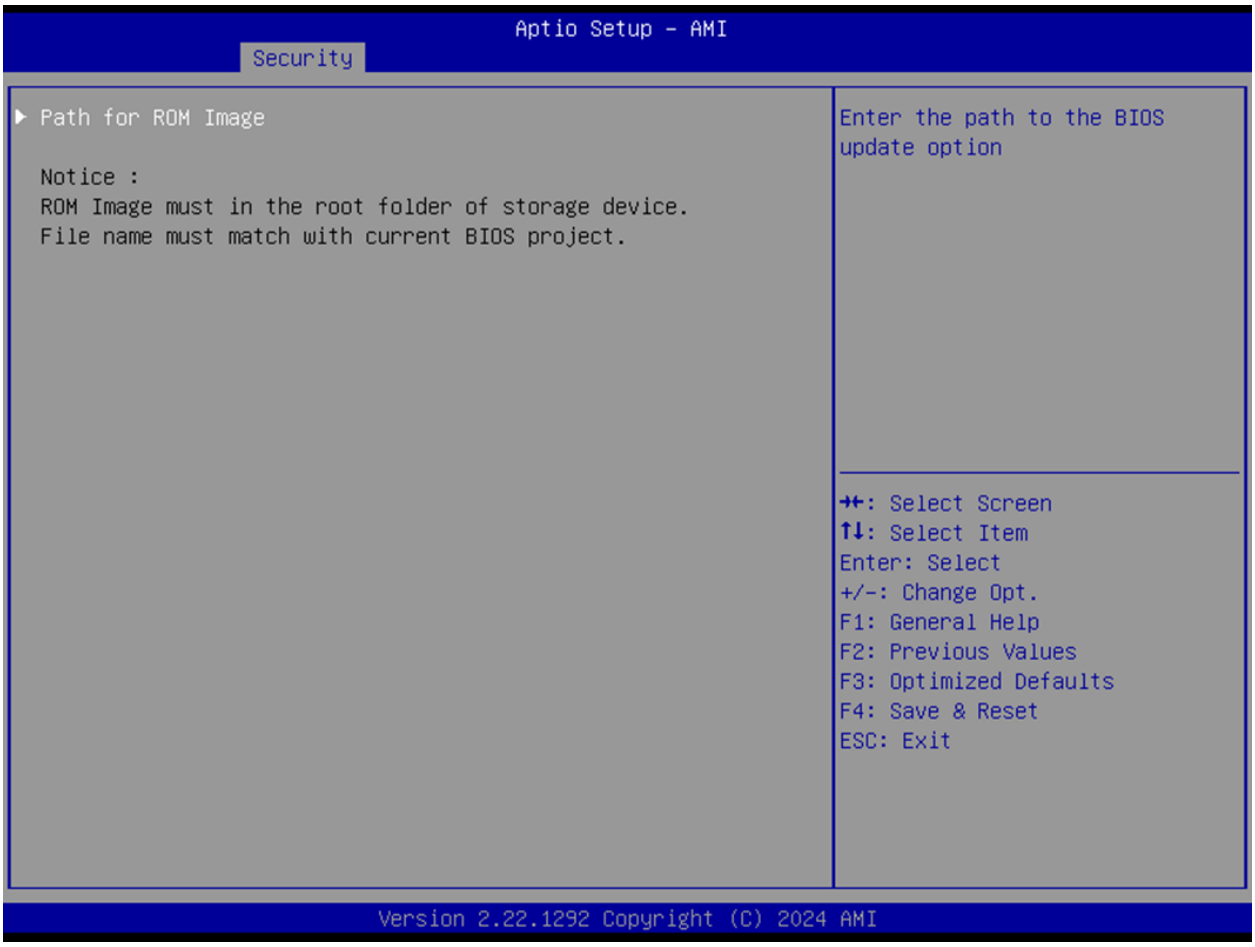
Each item below shows key size, count, and source. All support Factory, Modified, or Mixed key sources. Press Enter to manage entries in their respective sub-menus.

- **Platform Key (PK)**
  - Default: `Size: 0, Keys: 0, Key Source: No Keys`
- **Key Exchange Keys (KEK)**
  - Default: `Size: 0, Keys: 0, Key Source: No Keys`
- **Authorized Signatures (db)**
  - Default: `Size: 0, Keys: 0, Key Source: No Keys`
- **Forbidden Signatures (dbx)**
  - Default: `Size: 0, Keys: 0, Key Source: No Keys`
- **Authorized TimeStamps (dbt)**
  - Default: `Size: 0, Keys: 0, Key Source: No Keys`
- **OS Recovery Signatures (dbr)**
  - Default: `Size: 0, Keys: 0, Key Source: No Keys`

  Each key field accepts:

  1. Public Key Certificates:
     - `EFI_SIGNATURE_LIST`
     - `EFI_CERT_X509 (DER)`
     - `EFI_CERT_RSA2048 (bin)`
     - `EFI_CERT_SHAXXX`
  2. Authenticated UEFI Variable
  3. EFI PE/COFF Image (SHA256)

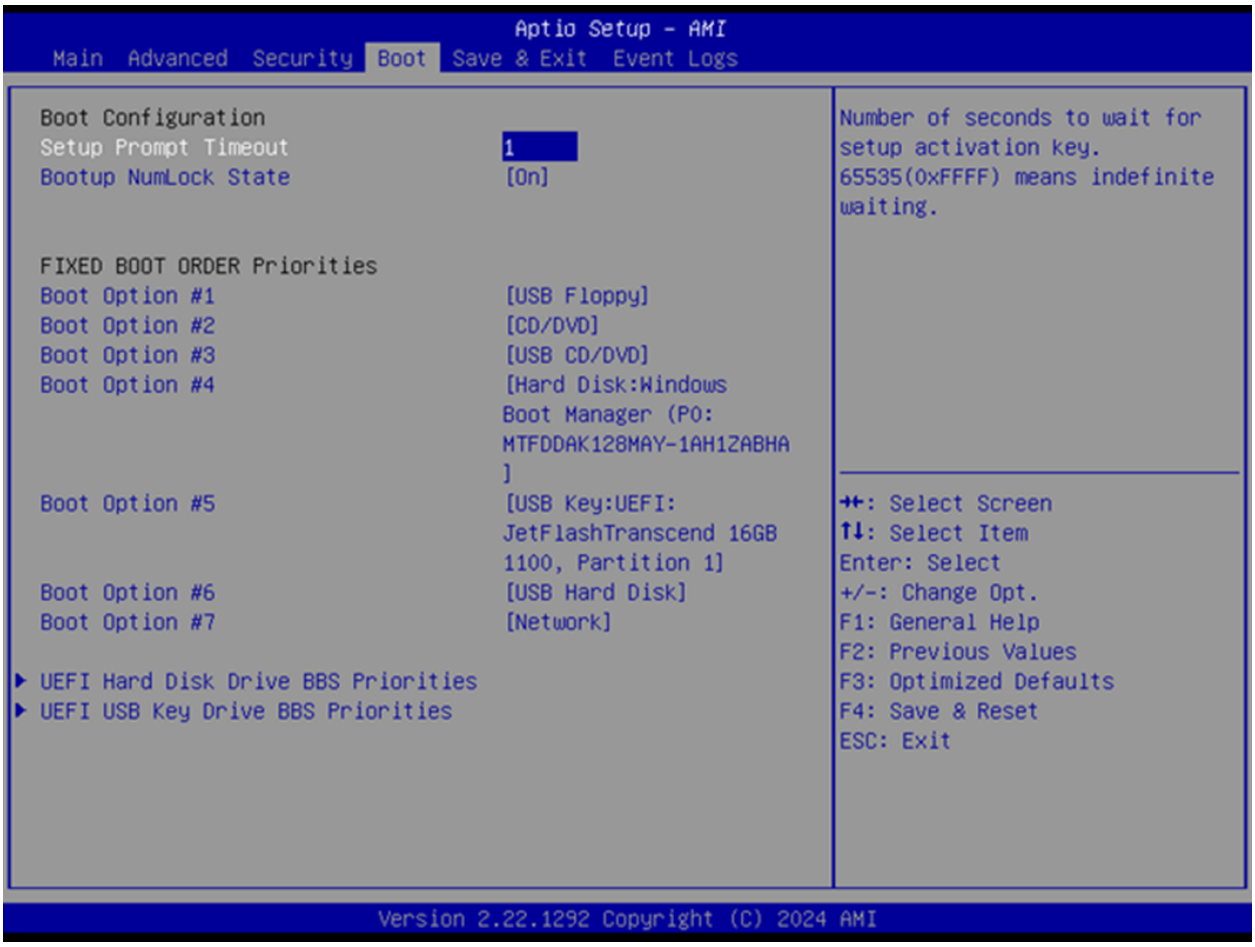
6.16 BIOS Update



The **BIOS Update** submenu allows users to specify the file path to a BIOS ROM image for updating firmware.

- **Path for ROM Image**
  - Enter the location or path of the BIOS update file to initiate the update process.

6.17 Boot Page



The **Boot Page** allows configuring boot behavior, NumLock state, and boot priority order.

6.17.1 Boot Settings

- **Setup Prompt Timeout**
  - Default: `1`
  - Range: `1`–`65535`
  - Sets the number of seconds to wait for setup activation key.

    `65535` (0xFFFF) means indefinite wait.
- **Bootup NumLock State**
  - Default: `On`
  - Options: `On`, `Off`
  - Sets the keyboard NumLock state at boot.

6.17.2 Boot Options

- **Boot Option #1 – #7**
  - Default Values:
    - #1: `USB Floppy`
    - #2: `CD/DVD`
    - #3: `USB CD/DVD`
    - #4: `Hard Disk`
    - #5: `USB Key`
    - #6: `USB Hard Disk`
    - #7: `Network`
  - Options: `USB Floppy`, `CD/DVD`, `USB CD/DVD`, `Hard Disk`, `USB Key`, `USB Hard Disk`, `Network`, `Disabled`
  - Defines the system boot sequence. Lower numbers indicate higher priority.

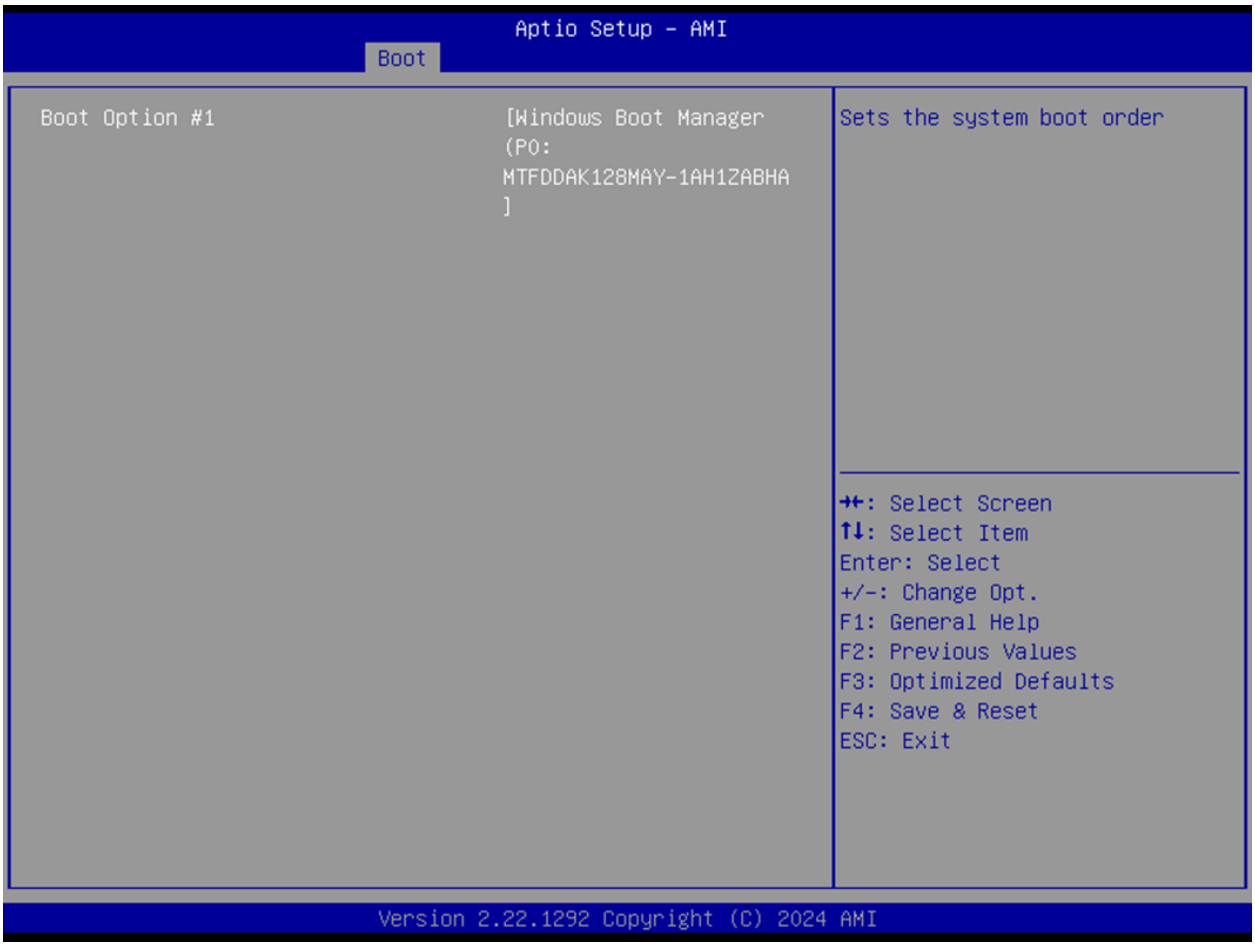
6.17.3 UEFI BBS Priorities

The following submenus allow ordering of UEFI-compatible boot devices within their respective types:

- **(UEFI) USB Floppy Drive BBS Priorities**
- **(UEFI) CDROM/DVD Drive BBS Priorities**
- **(UEFI) USB CDROM/DVD ROM Drive BBS Priorities**
- **(UEFI) Hard Disk Drive BBS Priorities**
- **(UEFI) USB Key Drive BBS Priorities**
- **(UEFI) USB Hard Disk Drive BBS Priorities**
- **(UEFI) Network Drive BBS Priorities**

  Press Enter to access each submenu and define device-specific boot priorities.

6.18 Drive BBS Priorities



This submenu appears per device type (USB, CD/DVD, HDD, etc.) and allows granular boot ordering for matching devices.

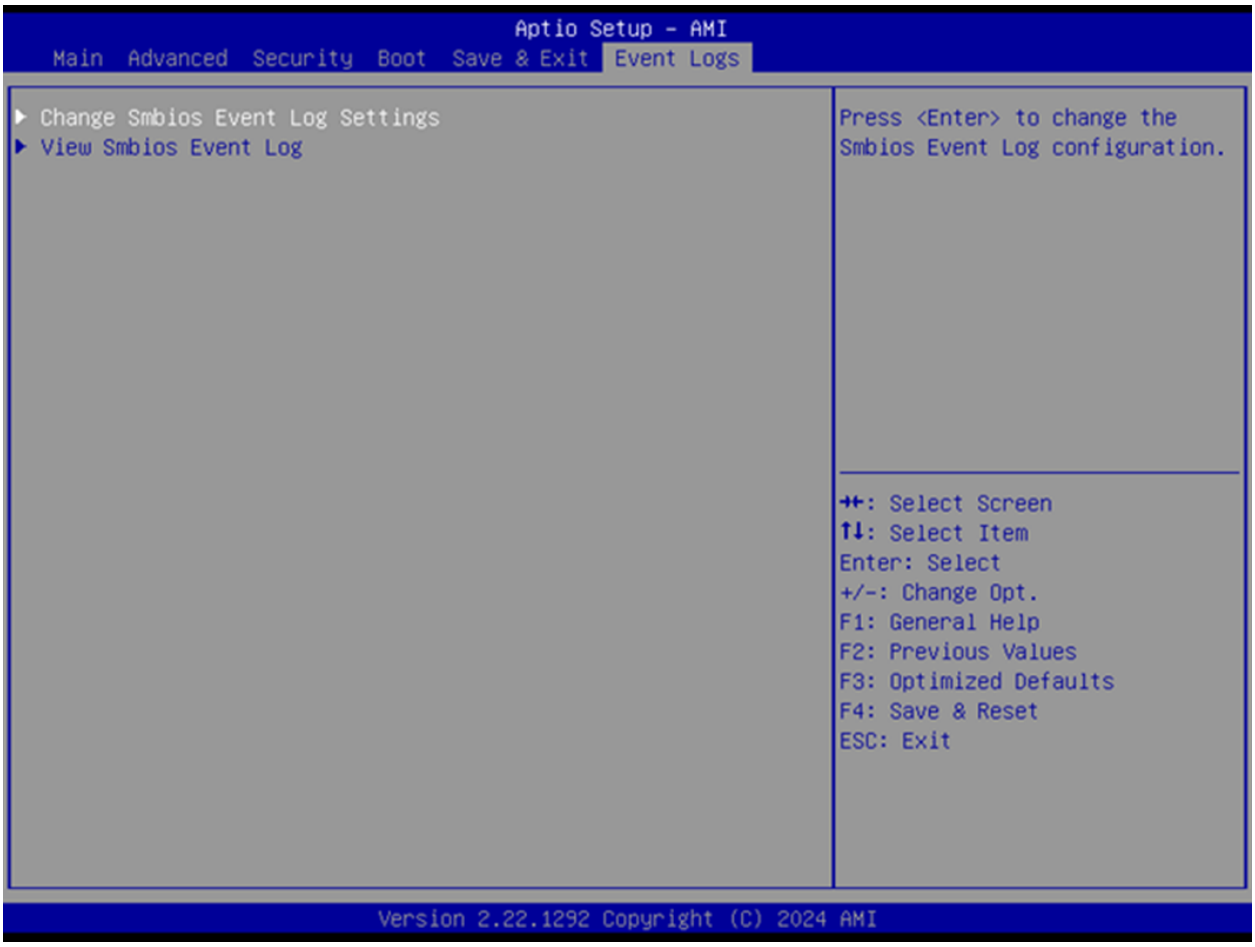
- **Boot Option #1**
  - Options: `<Device Name>` or `Disabled`
  - Sets boot priority for available devices of the selected type.

6.19 Save & Exit Page

The **Save & Exit Page** provides options for applying or discarding changes and restoring factory defaults.

- **Save Changes and Reset**
  - Saves BIOS configuration changes and restarts the system.
- **Discard Changes and Reset**
  - Restarts the system without saving any changes.
- **Restore Defaults**
  - Restores all BIOS settings to their factory default values.

6.20 Event Logs

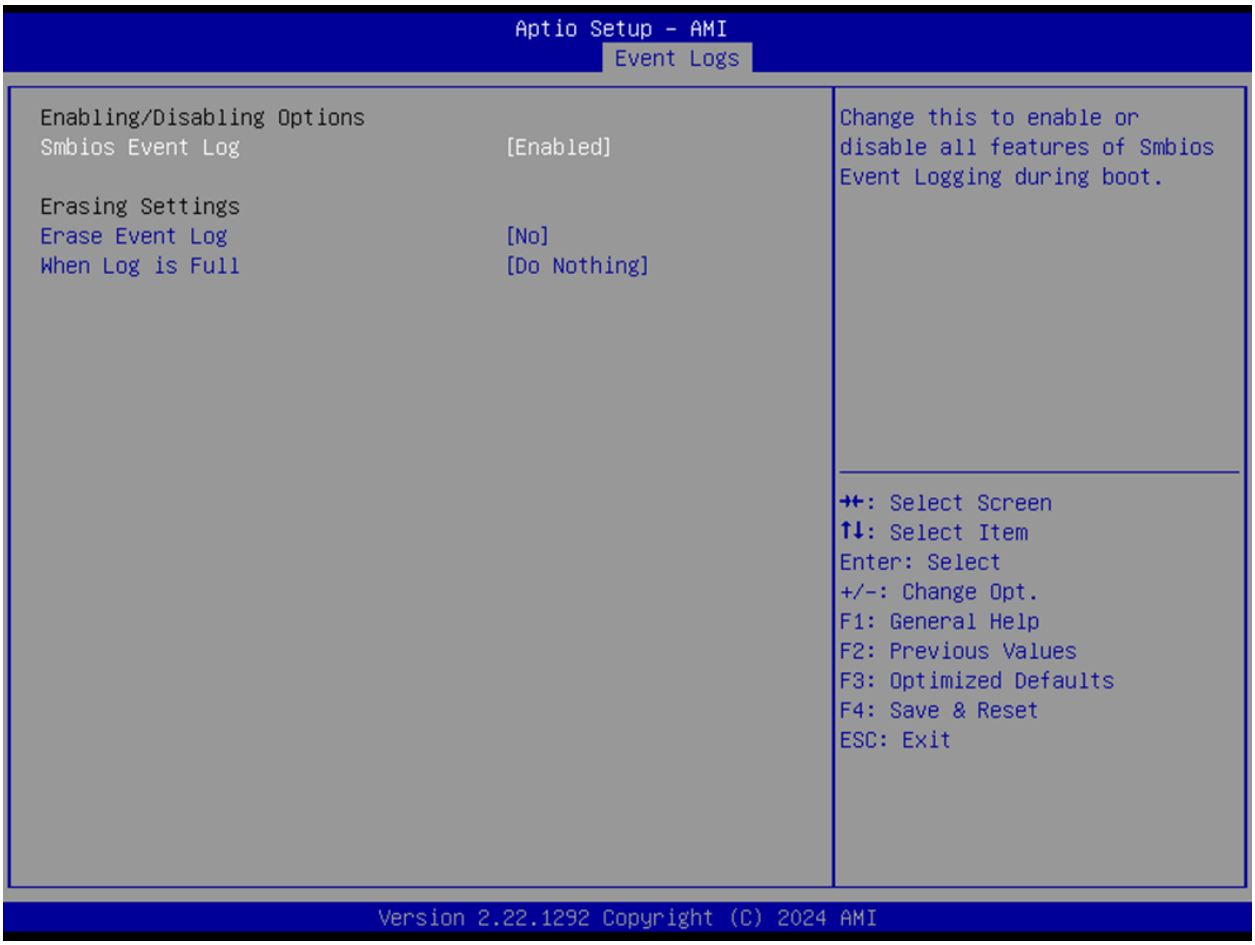


The **Event Logs** section allows you to configure and view SMBIOS event logging activity.

6.20.1 Event Log Options

- **Change SMBIOS Event Log Settings**
  - Press Enter to configure logging behavior.
  - *Opens the associated submenu.*
- **View SMBIOS Event Log**
  - Press Enter to view recorded SMBIOS event entries.
  - *Opens the associated submenu.*

6.20.2 Change SMBIOS Event Log Settings



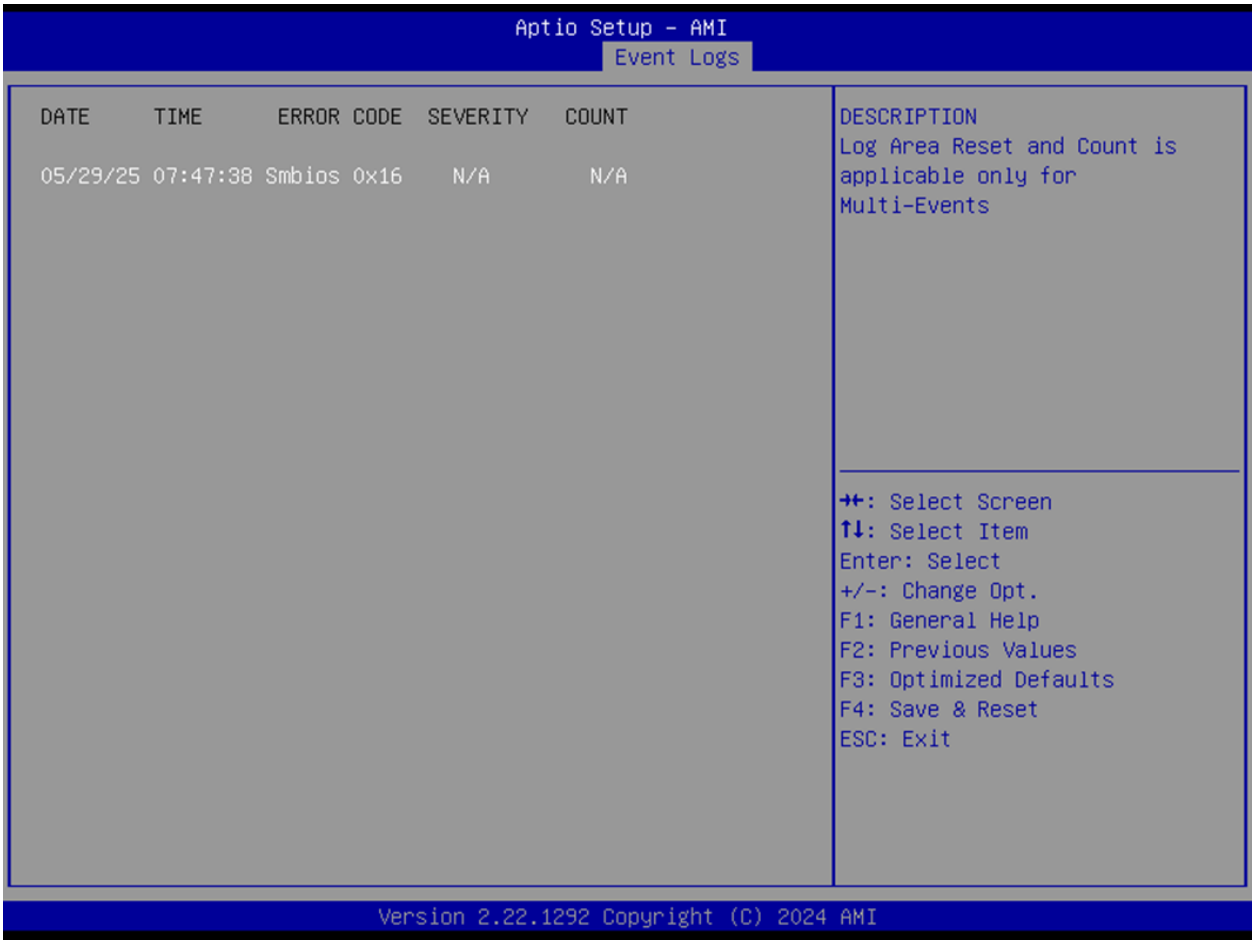
This submenu controls whether SMBIOS events are logged and how logs are handled.

- **SMBIOS Event Log**
  - Default: `Enabled`
  - Options: `Enabled`, `Disabled`
  - Enables or disables event logging during boot.
- **Erase Event Log**
  - Default: `No`
  - Options:
    * `No`
    * `Yes, Next reset`
    * `Yes, Every reset`
  - Determines if/when the event log should be cleared.
- **When Log is Full**
  - Default: `Do Nothing`
  - Options:
    * `Do Nothing`

* Erase Immediately

– Defines the system's behavior when the event log reaches capacity.

6.20.3 View SMBIOS Event Log



Displays recorded SMBIOS events with date, time, error code, severity, and count.

- **DATE / TIME / ERROR CODE / SEVERITY / COUNT**
  - Example Entry: `MM/DD/YY HH:MM:SS Smbios 0x16 N/A N/A`
  - Events are listed in chronological order.