Alderamin Pico Mk5 Series

Version:
v1.1.0

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 62368-1	Safety requirements: Audio/video, information and communication technology	2014+A11:2017+AC2015
ETSI EN 301 489-1	Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements	V1.9.2 V2.2.3
ETSI EN 301 489-17	Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for Broadband Data Transmission Systems	V3.3.1
EN 55032	Electromagnetic compatibility (EMC) of multimedia equipment: Emission Requirements	2015+A11:2020 2015+A1:2020
EN 55035	Electromagnetic compatibility (EMC) of multimedia equipment: Immunity requirements	2017 2017+A11:2020
EN 61000-3-2	Electromagnetic compatibility (EMC) - Part 3-2: Limits - Limits for harmonic current emissions	2014
EN IEC 61000-3-2	Electromagnetic compatibility (EMC) - Part 3-2: Limits - Limits for harmonic current emissions	2019+A1:2021
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 2013+A1:2019

3 Intended Use and IT Security Instructions

This section provides crucial safety and security information and recommendations to help you configure your Welotec Industrial Computer (IPC) for optimal security in your deployment.

3.1 Intended Use

This section specifies the intended use and essential operating conditions for your Welotec Industrial Computer (hereinafter referred to as “IPC”).

The IPC is designed for use as a dedicated control, monitoring, and data acquisition unit within the enclosed control cabinet of a machine. Its primary function is to execute specific machine-control software, process operational data, provide human-machine interface (HMI) functionalities, and/or facilitate communication within the industrial automation environment. The IPC is exclusively intended for continuous operation within a controlled industrial setting.

The intended use of the IPC is strictly defined by the following conditions and requirements:

3.1.1 Physical Security and Installation Environment

- Enclosure: The IPC must be permanently installed within a secure, locked control cabinet (e.g., meeting IP54 or higher protection class) that provides adequate protection against dust, moisture, mechanical impact and unauthorized access.
- Controlled Access: Access to the control cabinet and its wiring must be restricted to authorized personnel only. Physical security measures (e.g., key locks, access control systems) are mandatory.
- Environmental Conditions:
  - Temperature: The IPC must operate within the specified ambient temperature and humidity range as outlined in the technical specifications. Adequate ventilation or active cooling within the cabinet must ensure these limits are not exceeded. This includes accounting for the unit’s own thermal dissipation and that of all other components in the cabinet.
  - Vibration and Shock: The IPC must be mounted securely within the cabinet to minimize exposure to excessive vibrations and mechanical shock, adhering to the manufacturer’s specifications.
  - Cleanliness: The inside of the cabinet must be kept free of dust, debris, and contaminants that could impair cooling or lead to electrical shorts.

3.1.2 EMC compliant electrical Installation and Power Supply

This product is designed to meet EMC standards when installed according to the following instructions. Failure to adhere to these instructions may result in the equipment failing to meet compliance standards and can cause interference with other devices. The installer is responsible for ensuring the EMC conformity of the final system.

- Power Supply: The IPC must be connected to a dedicated stable and filtered power supply within the specified voltage range. To ensure operational reliability and meet EMC requirements, the power source must provide adequate filtering against surges, transients, electrical fast transients (EFTs), and conducted RF noise common in industrial environments. An Uninterruptible Power Supply (UPS) is highly recommended to protect further against power fluctuations and outages.

- Wiring: All wiring connecting to the IPC must comply with applicable industrial wiring standards, be properly insulated, strain-relieved, and protected against mechanical damage.
- Grounding: The unit must be properly grounded according to the installation manual, typically via a low-impedance connection to the control cabinet's central grounding point.

3.1.3 Functional Safety

This unit is not certified as a standalone component for functional safety applications (e.g., SIL, PL).

Intended Use: The unit is intended for standard control and monitoring. It must not be used as the sole or primary controller for safety-critical functions (e.g., emergency stops, safety interlocks, light curtains, burner controls).

System Integration: Safety-related control logic must be executed by dedicated, certified safety controllers (e.g., Safety PLC, safety relays). This unit may be used to supervise or monitor a safety system (e.g., for HMI visualization or data logging) via a non-safety-rated communication channel, but it must not be part of the safety-critical control loop. The failure of this unit must not lead to a loss of the primary safety function.

3.1.4 Qualified and Trained Personnel

- Installation, Configuration, and Maintenance: All installation, configuration, maintenance, troubleshooting, and repair activities on the IPC and its connections within the control cabinet must be performed exclusively by qualified, trained, and authorized technical personnel. This personnel must possess proven expertise in electrical systems, IT hardware, and cybersecurity best practices.
- Security Awareness: All personnel interacting with the IPC or the network it is connected to must receive regular training on IT security awareness including password policies and reporting suspicious activities.

3.1.5 Software and Configuration

- Operating System: Only the pre-installed or manufacturer-approved operating system (OS) version may be used. The OS must be regularly updated with security patches provided by the manufacturer or OS vendor, after thorough testing in a non-production environment.
- Secure Configuration: The IPC's operating system, firmware, and installed applications must be configured according to secure hardening guidelines, including disabling unused services, ports, and protocols, and enforcing strong password policies.
- Secure Boot: Where supported Secure Boot must be enabled to prevent the loading of unsigned or malicious bootloaders.

Please refer to the section "Cyber Security" for further details.

3.1.6 Network Segmentation and "Defense in Depth" IT Security Principles

- Network Segmentation: The unit and its control network must be isolated from all other networks (e.g., corporate, guest, public internet) using industrial firewalls and network segmentation. Direct connection to the internet is considered misuse unless done via a secure, managed gateway.
- Defense in Depth: A multi-layered security approach ("Defense in Depth") must be implemented for the entire machine. This includes:
  - Network Security: Industrial Firewalls (e.g., Next-Generation Firewalls) at network boundaries, strict firewall rules (whitelist approach – only allow explicitly required traffic), VLANs for segmentation.
  - System Security: Operating system hardening (minimum services, disabled unnecessary ports), regular security updates, robust antivirus/anti-malware solutions specifically designed for industrial environments, and strong password policies.

  - Application Security: Secure configuration of all industrial applications, disabling default credentials, and ensuring application-level security features are enabled.
  - Data Integrity: Measures to ensure data integrity and availability (e.g., backups, redundant systems where appropriate).
  - Physical Security: see above

- Access Control: Remote access to the IPC (if required) must be strictly controlled, using secure connections, multi-factor authentication, and granular user permissions. Unnecessary remote access functionalities must be disabled.
- Logging and Monitoring: The IPC and connected network devices should implement logging of security-relevant events. Centralized monitoring and alerting systems are recommended for timely detection of anomalies.

3.2 Non-Intended Use

Any use of the IPC that deviates from the conditions described including but not limited to:

- Operation outside the specified environmental limits.
- Operation without a secure, enclosed control cabinet.
- Operation in hazardous locations (e.g., explosive atmospheres) for which the unit is not explicitly certified.
- Installation or maintenance by unqualified personnel.
- Connection to an unfiltered, unstable, or non-grounded power source.
- Direct connection to unsecured corporate networks or the internet without adequate protective measures.
- Installation of unauthorized software or operating systems.
- Bypassing or disabling of security features (e.g., firewall, antivirus, Secure Boot).
- Failure to implement a cyber security management plan (patching, hardening, access control).

is considered non-intended use and may result in:

- Damage to the IPC or the machine.
- Compromised data security and integrity.
- Serious personal injury or death.
- Failure to comply with regulatory requirements.

3.3 Exposed Interfaces and Services

The following interfaces are exposed:

Interface	Comment
LAN 1 … 4	
COM 1 … 4	
USB 1 … 8	
HDMI	
DP	
Remote Power	Power Switch

Available services highly depend on Operating System type and version.

3.4 Cyber Security

The flexibility to run common operating systems like Windows and Linux places the full responsibility of cyber security implementation on the system integrator and end-user. The unit is a component that must be integrated into a comprehensive, defense-in-depth security architecture.

The intended use requires the integrator/user to implement, at a minimum, the following:

3.4.1 Use Secure Boot

Secure Boot is a crucial security feature that helps protect your system from malware and unauthorized operating systems during the boot process. It's a component of the Unified Extensible Firmware Interface (UEFI) that ensures only trustworthy software, signed with a digital certificate, loads when your system starts. Without Secure Boot, malicious programs or unsigned operating systems could load unnoticed before the actual operating system, compromising your system's integrity and security.

We highly recommend enabling Secure Boot - please refer to "BIOS" section for further details

3.4.2 Enable Storage Encryption

Storage encryption is a critical security measure that protects your sensitive data by rendering it unreadable to unauthorized parties, even if they gain physical access to your storage device. In today's interconnected world, where devices can be lost, stolen, or compromised, ensuring the confidentiality of your information is paramount.

Windows (using BitLocker with TPM)

Windows' built-in BitLocker encryption leverages the TPM to securely store the encryption key, making the process largely automatic and secure.

- Check TPM Status: Ensure that the TPM chip is enabled in the UEFI/BIOS settings
- Open BitLocker Drive Encryption: Search for "BitLocker" in the Windows search bar and select "Manage BitLocker."
- Turn on BitLocker: Select the drive you wish to encrypt (typically your C: drive) and click "Turn on BitLocker."
- Follow the Wizard: Windows will guide you through the process. Since a TPM is present, it will typically automatically use the TPM to store the encryption key. You will be prompted to save a recovery key (e.g., to a Microsoft account, a USB drive, or print it) – this is crucial in case you ever need to access your data if the TPM is reset or unavailable.

- Start Encryption: The encryption process will begin in the background. You can continue using your computer during this time.

Linux (using LUKS with TPM consideration):

Linux uses LUKS (Linux Unified Key Setup) for full disk encryption. Integrating it with a TPM for automatic unlocking at boot can be more involved than BitLocker but offers similar benefits. This typically involves tools like clevis or systemd-cryptenroll.

- Install Necessary Tools: You'll need cryptsetup for LUKS and potentially tpm2-tools and clevis (or similar TPM integration tools) if you want to bind your LUKS key to the TPM for automatic decryption.
- Encrypt the Drive (during OS Installation or manually):
  - During Installation: Most Linux distributions (e.g., Ubuntu, Fedora) offer an option to "Encrypt the disk" during the installation process. This is the simplest way to set up LUKS.
  - Manually (Post-Installation): If encrypting an existing drive or a secondary drive, you would use cryptsetup luksFormat /dev/sdXy to format the partition for LUKS, followed by cryptsetup luksOpen /dev/sdXy my_encrypted_drive and then creating a filesystem on the opened device.
- Bind LUKS Key to TPM (Optional, for automatic unlock):
  - This is the step that utilizes the TPM. Tools like clevis can be used to "bind" a LUKS passphrase (or a key slot) to the TPM. This allows the system to automatically unlock the encrypted volume at boot if the TPM verifies the system's integrity.
  - The exact commands vary, but it generally involves generating a new LUKS key slot and then using a TPM-binding tool to store the key in the TPM and configure the system to use it for unlocking.
- Update Boot Configuration: Ensure your bootloader (e.g., GRUB) is configured correctly to handle the encrypted root partition and, if used, to leverage the TPM for unlocking.

For both operating systems, it's essential to:

- Backup your recovery keys/passphrases: Without them, your data can be permanently lost if there's a hardware failure or you forget your primary password.
- Understand the implications: While encryption provides strong security, proper handling of keys and adherence to security best practices are still crucial.

3.4.3 Use Strong Passwords

Strong passwords are the first line of defense against unauthorized access. If you want to use password based access it is recommended to:

- Change the factory default password on first login
- Use passwords with a minimum length of 12 characters or more
- Use a combination of uppercase and lowercase letters, numbers, and special characters (e.g., !@#$%^&*)
- Do not use easily guessable patterns, such as sequences (e.g., "123456", "abcdef"), repeated characters (e.g., "aaaaaa"), or dictionary words

3.4.4 System Hardening:

The operating system (Windows or Linux) must be hardened. This includes:

- Disabling all unused services, applications, and network ports.
- Enforcing strong, unique passwords for all accounts.
- Implementing a least-privilege access model for users and applications.
- Configuring OS-level firewalls (e.g., ufw, Windows Defender Firewall).

3.4.5 Patch Management

A robust process must be in place for testing and deploying security patches for the operating system and all installed third-party applications. This process must be compatible with the operational constraints of the industrial environment.

3.4.6 Endpoint Protection

Where appropriate for the application, industrial-compatible endpoint protection (e.g., anti-malware, application whitelisting, host-based intrusion detection) must be installed, maintained, and kept up-to-date.

3.4.7 Physical Security

Use of the locked control cabinet (see Section 3) to prevent unauthorized physical access and tampering (e.g., via USB ports) is a critical part of the security model.

3.5 Vulnerability Handling

Welotec has implemented a Coordinated Vulnerability Disclosure Policy - please visit the following site for further details: https://welotec.com/pages/coordinated-vulnerability-disclosure-policy

4 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.

5 Technical Details

Feature	Specification	Details
Processor	CPU	Intel® Meteor Lake-U Core™ Ultra 7 155U / Ultra 5 125U Processor
Memory	System Memory	DDR5 4800 MHz, 1 x 262-pin SO-DIMM, Max. 48GB (Non-ECC)
Graphics	GPU	Intel® Iris Xe Graphics
Display	Display Interface	DisplayPort 1.2, HDMI 1.4
Storage	Storage Slots	1 x 2.5” HDD/SSD Bracket 1 x M.2 B Key 2242 SATA SSD Slot 1 x M.2 M Key 2280 NVMe/SATA SSD Slot
Networking	Ethernet	4 x Intel® I226-LM 2.5G LAN (optional PoE module) Additional 2 x Intel® I210-IT Giga LAN (optional)
Audio	Audio	Realtek® ALC888S
Security	I/O Chipset	Nuvoton NCT6126D
	TPM	Nuvoton NPCT760AABYX TPM 2.0
Expansion	Expansion Slots	1 x M.2 2242/3042/3052 B Key (USB2.0/PCIe X1/SATAIII) 1 x M.2 2280 M Key (PCIe 4.0 X4, SATAIII) 1 x M.2 2230 E Key (PCIe X1, USB2.0)
Indicators	Indicators	Power LED, HDD LED
I/O Ports	Front I/O	3 x RS232 1 x RS232/422/485 8-bit GPIO in DB9 Type 2 x USB 2.0 1 x Line-out HDD LED & Power LED Power Button 4 x SMA holes
	Rear I/O	4 x RJ-45 1 x USB Type C (PD15W, 5V/3A, DP Alt mode, USB3.2 Gen1) 4 x USB 3.2 Gen 2 (10 Gbps) 1 x USB 2.0 (blue type connector) 1 x HDMI 1.4 1 x DisplayPort 1.2 1 x 3-pin Terminal Block Power Input 1 x 2-pin Terminal Block Remote Power on/off 1 x Nano SIM Slot with Cover 2 x SMA holes
Watchdog Timer	Watchdog	1~255 steps programmable by software
Power	Power Input	8~26V Wide Range DC Input with Terminal Block Connectivity
Cooling	Thermal Design	Fanless
Mechanical	Mounting	Wall Mount / Side Mount 75 mm x 75 mm VESA Holes & DIN Rail Mount Combo Kit (optional)
	Dimensions	8.3” x 5.9” x 2.5” (210 x 150 x 63 mm)
	Material	Top Cover: Aluminum Alloy Bezel and Chassis: Steel
Environ	Oper	-40°C to 60°C (with 0.7 m/s airflow and extended-temp SSD/mSATA/RAM)

5.1 ⊠ Important Notes

Restricted Access Location (RAL) A Restricted Access Location is an area with extreme temperatures where only authorized personnel may enter for specific purposes.

1. Access is limited to trained personnel aware of location restrictions and necessary precautions.
2. Entry requires security measures such as tools, lock-and-key, or controlled access by the responsible authority.

Power Consumption Considerations Ensure power consumption is within the power supply's specifications.

- Recommended AC Adapters:
  - **AC/DC 24V/5A, 120W** (3-PIN Terminal Block Power Adaptor, PN 6913SDR12024)
  - **AC/DC 24V/9.58A, 230W** (3-PIN Terminal Block Power Adaptor, PN WIPC05000360)

Ambient Temperature Precaution

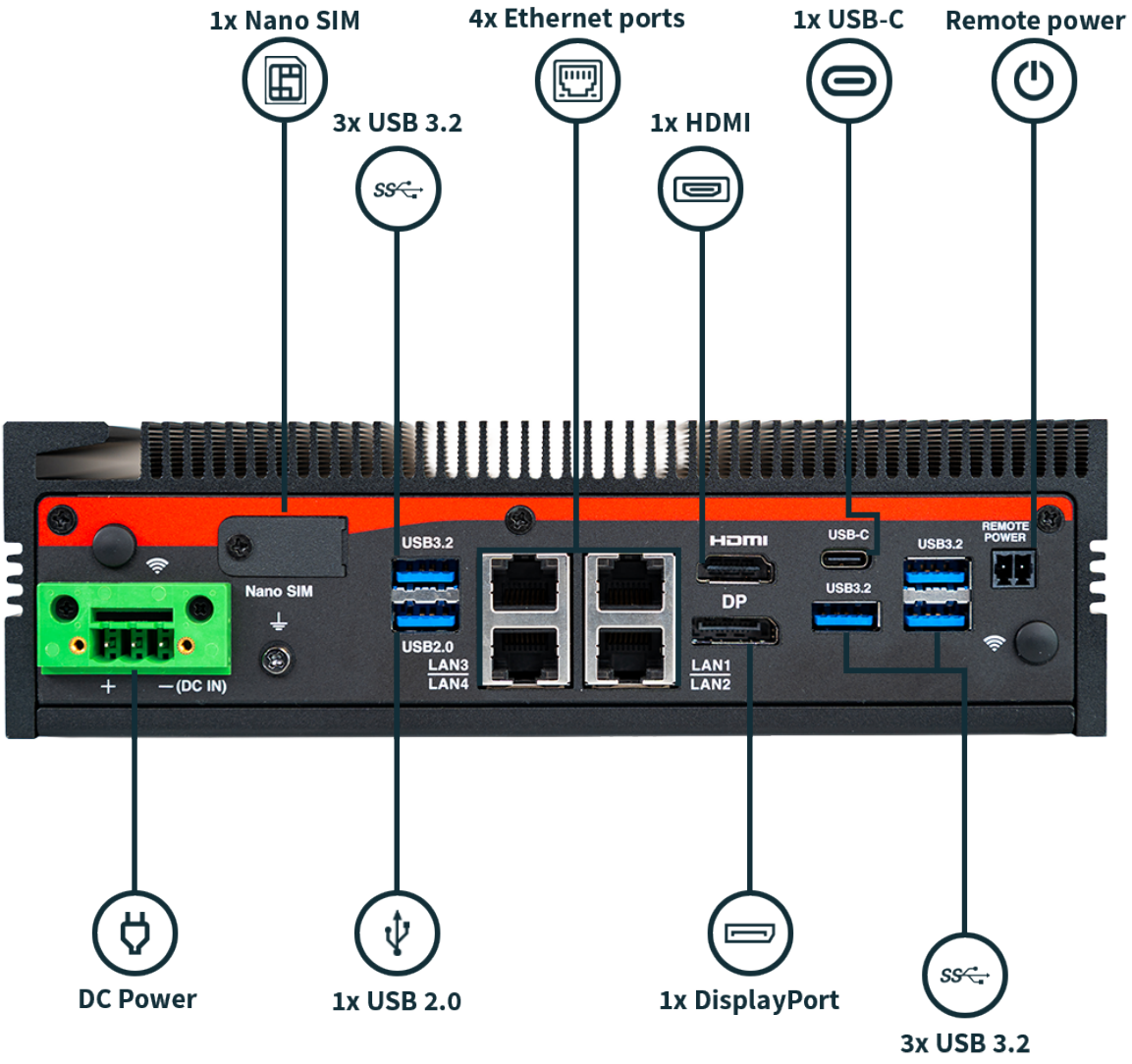
- The maximum safe operating temperature is **70°C** if the external AC adapter model power draw is limited to 90W for **6913SDR12024** or 125W for **WIPC05000360** if it is placed in the same high-temperature area as the embedded system.

Lithium Battery Safety Warning

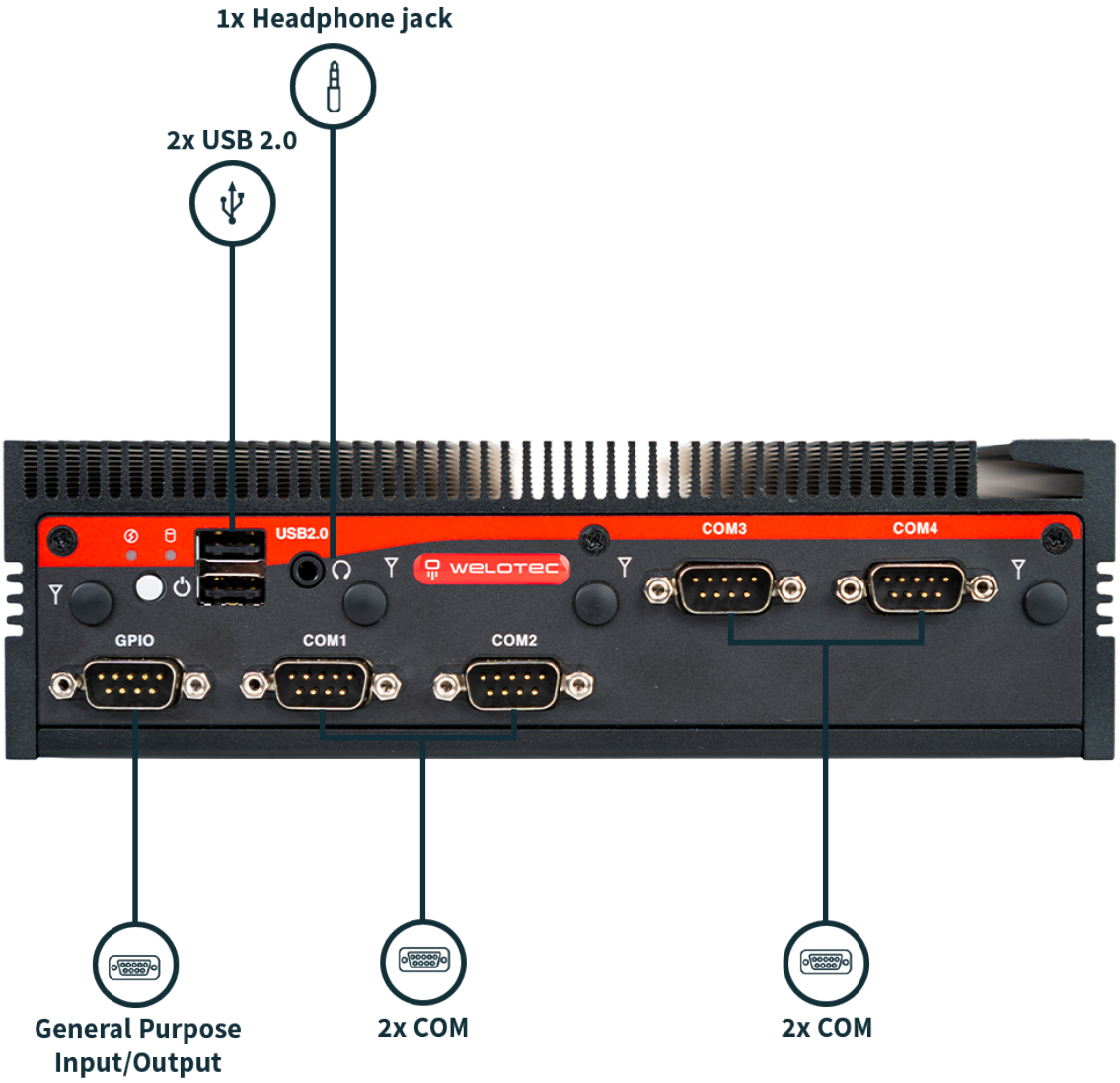
- **Caution:** This system contains a **lithium battery**.
- Do **NOT** puncture, mutilate, or dispose of it in fire.
- Risk of **explosion** if replaced incorrectly — use only manufacturer-recommended replacements.
- Dispose of batteries as per manufacturer instructions and local regulations.

6 Interfaces and Connections

6.1 Front I/O

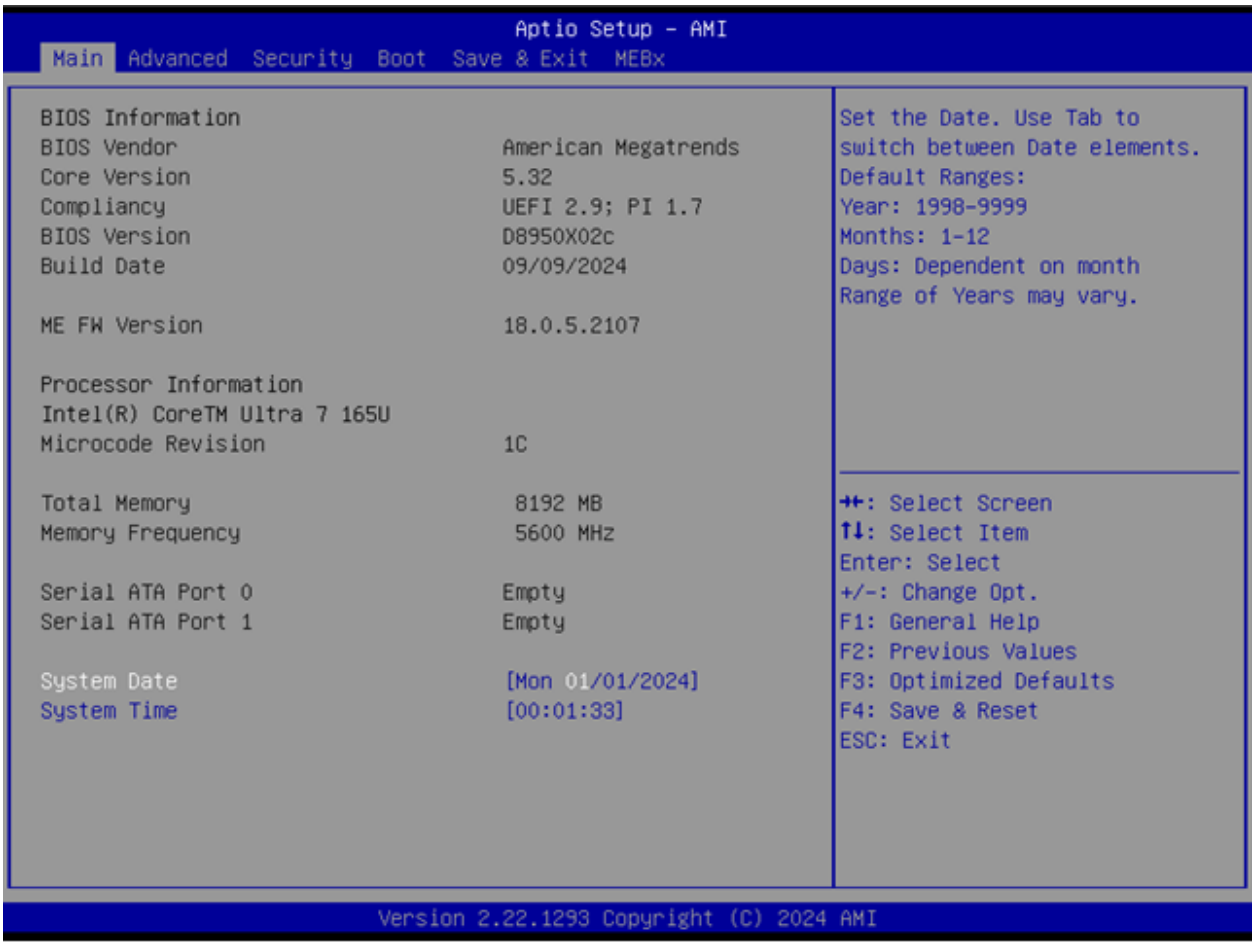


6.2 Rear I/O


1x Headphone jack
2x USB 2.0
USB2.0
COM3
COM4
GPIO
COM1
COM2
General Purpose Input/Output
2x COM
2x COM

7 BIOS

7.1 Main Page



The **Main Page** provides an overview of essential system information. These fields are read-only and cannot be modified:

- **BIOS Vendor:** American Megatrends
- **Core Version:** 5.32
- **Compliancy:** UEFI 2.9 ; PI 1.7
- **BIOS Version:** Displays the current BIOS version
- **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 CPU microcode revision
- **Total Memory:** Shows the installed memory size
- **Memory Frequency:** Displays the memory frequency

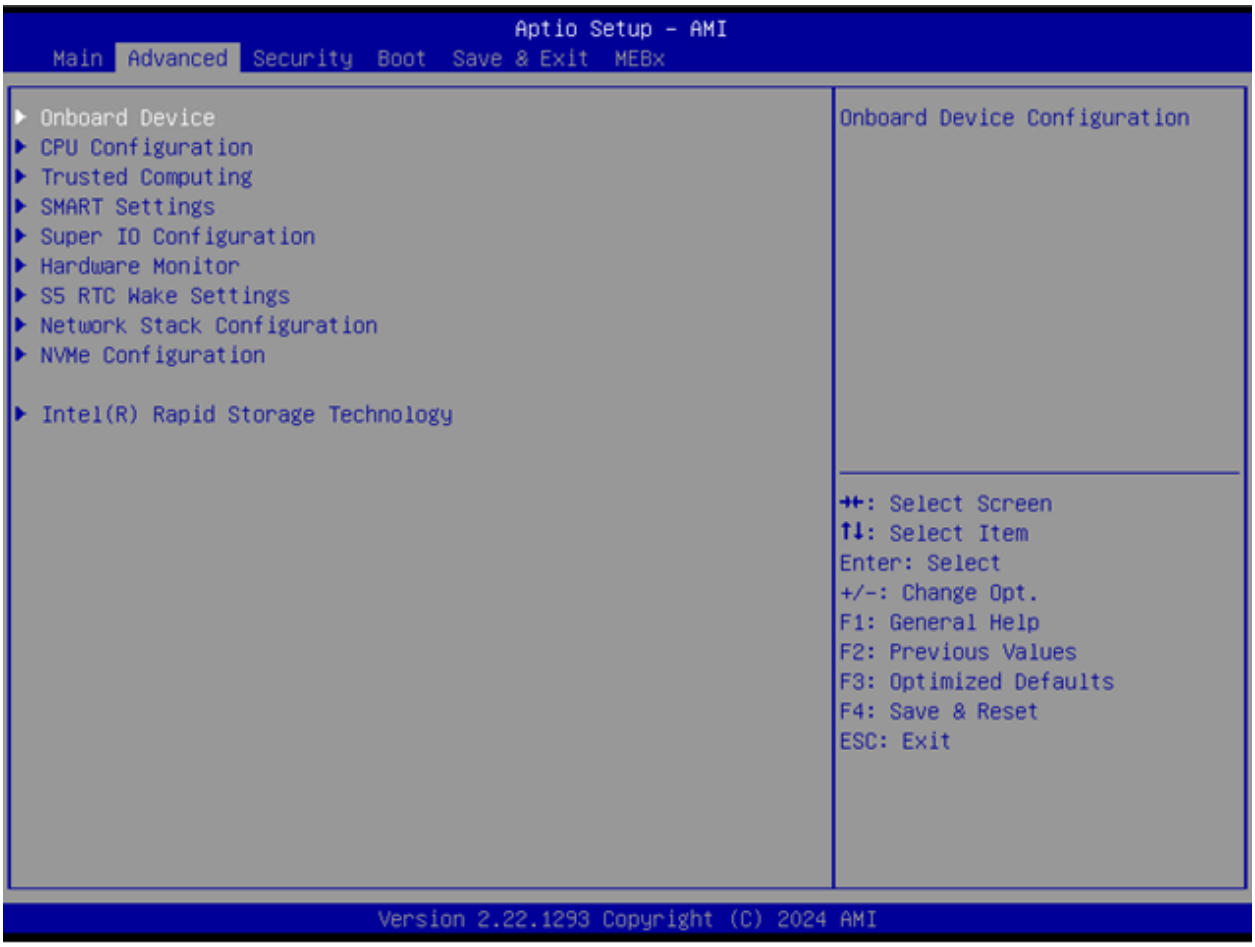
- **Serial ATA Port 0 / Port 1:** Lists the connected SATA device model and size

7.1.1 System Date & Time

The **System Date & Time** settings 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 (1998–9999)
  - Use Tab to move between elements
- **System Time**
  - Format: `[hh:mm:ss]`
  - `hh`: Hours (0–23)
  - `mm`: Minutes (0–59)
  - `ss`: Seconds (0–59)
  - Use Tab to move between elements

7.2 Advanced Page

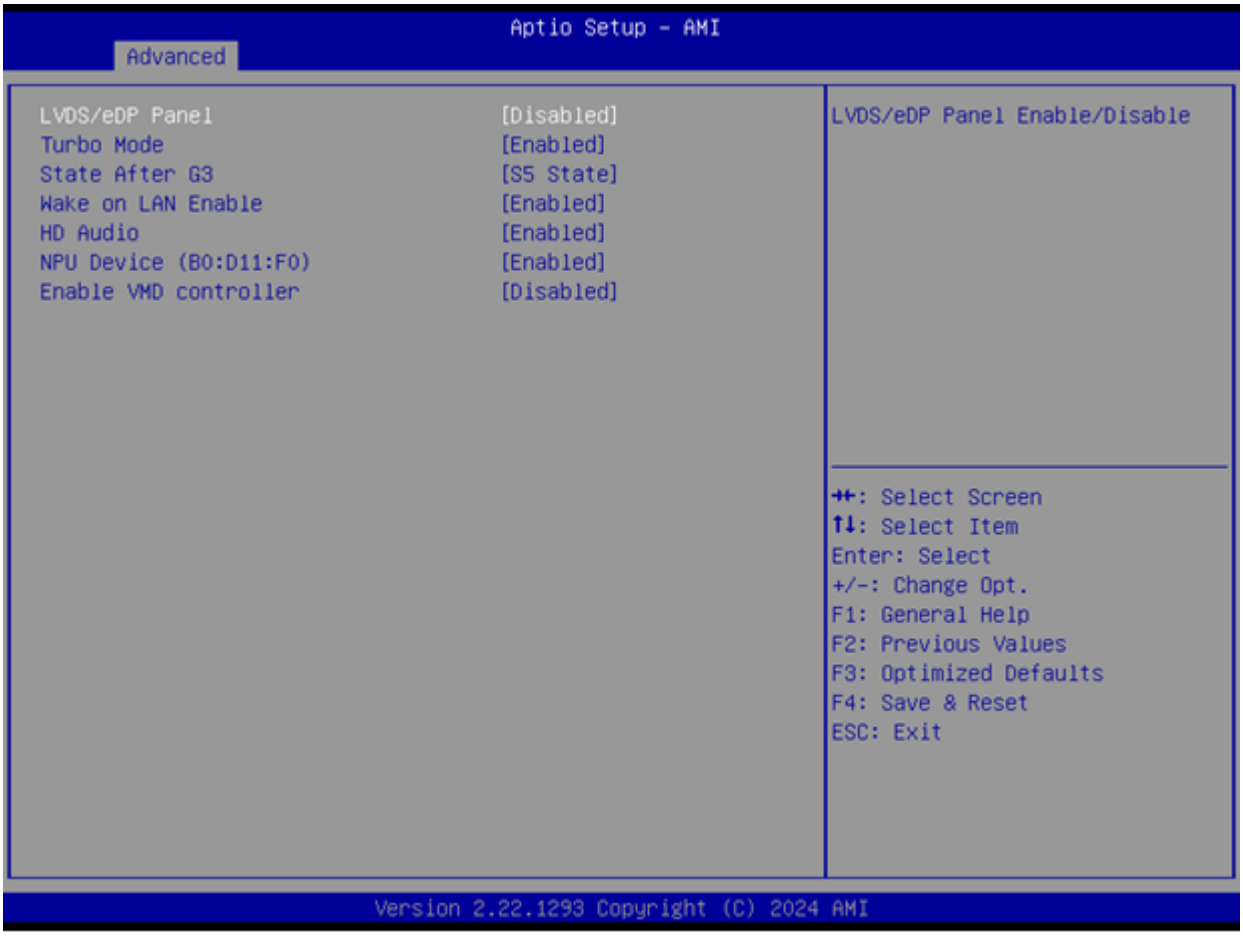


The **Advanced Page** gives you access to detailed configuration menus for advanced users.

7.2.1 Advanced Configuration Options

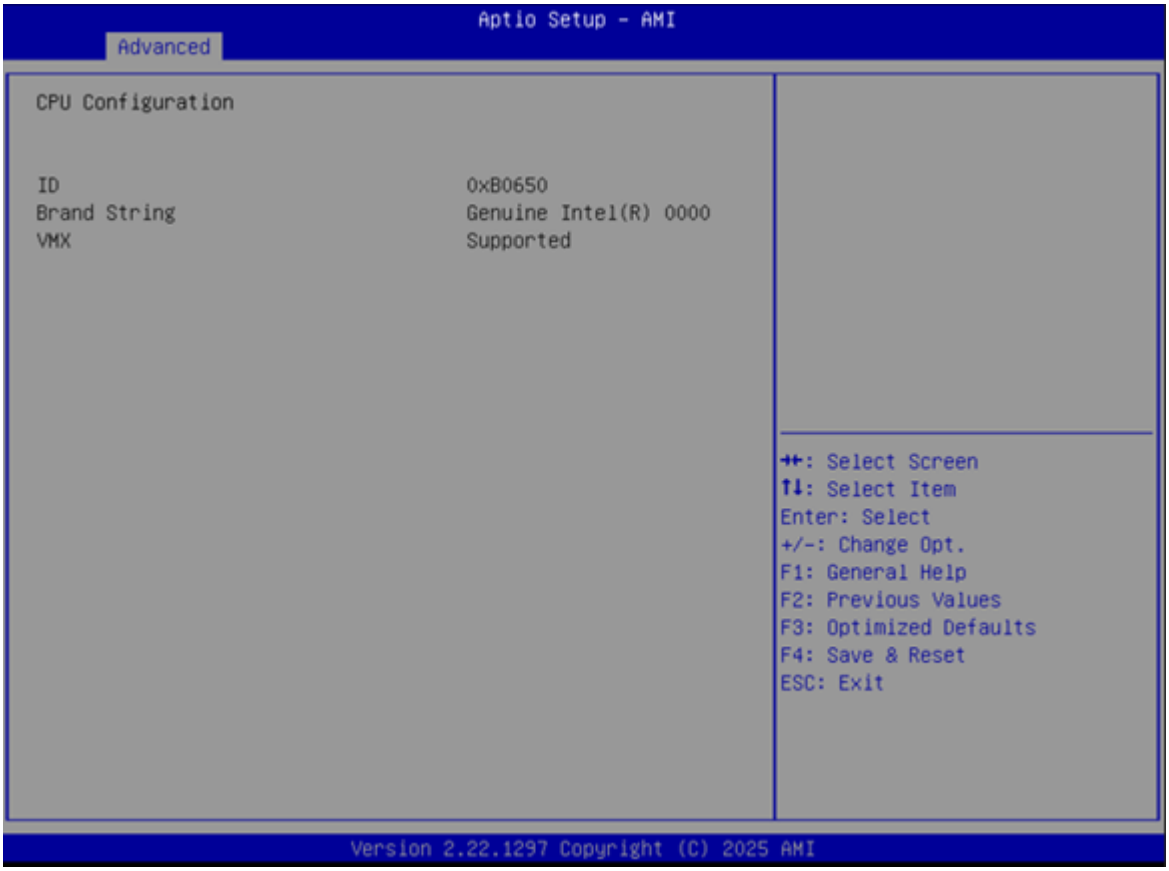
- **Onboard Device Configuration**
- **CPU Configuration**
- **Trusted Computing**
- **SMART Settings**
- **Super IO Configuration**
- **Hardware Monitor**
- **S5 RTC Wake Settings**
- **Network Stack Configuration**
- **NVMe Configuration**
- **Intel® Rapid Storage Technology**

7.3 Onboard Device Configuration



- **LVDS/eDP Panel:** Enable or disable panel output
  - Default: Disabled
- **Turbo Mode:** Enable or disable CPU Turbo Boost
  - Default: Enabled
- **State After G3:** Defines system state after power loss
  - Options: S0 State, S5 State
  - Default: S5 State
- **Wake on LAN Enable:** Allow wake-up from LAN
  - Default: Enabled
- **HD Audio:** Control detection of HD-Audio
  - Default: Enabled
  - Enabled = HDA always on, Disabled = HDA always off
- **NPU Device (B0:D11:F0):** Enable or disable Neural Processing Unit
  - Default: Enabled
- **Enable VMD Controller:** Enable or disable the VMD controller
  - Default: Disabled

7.4 CPU Configuration



The **CPU Configuration** page shows processor details:

- **ID:** Displays CPU Signature
  - Not selectable
- **Brand String:** Displays CPU model name
  - Not selectable
- **VMX:** Shows if Virtual Machine Extensions are supported
  - Not selectable

7.5 Trusted Computing

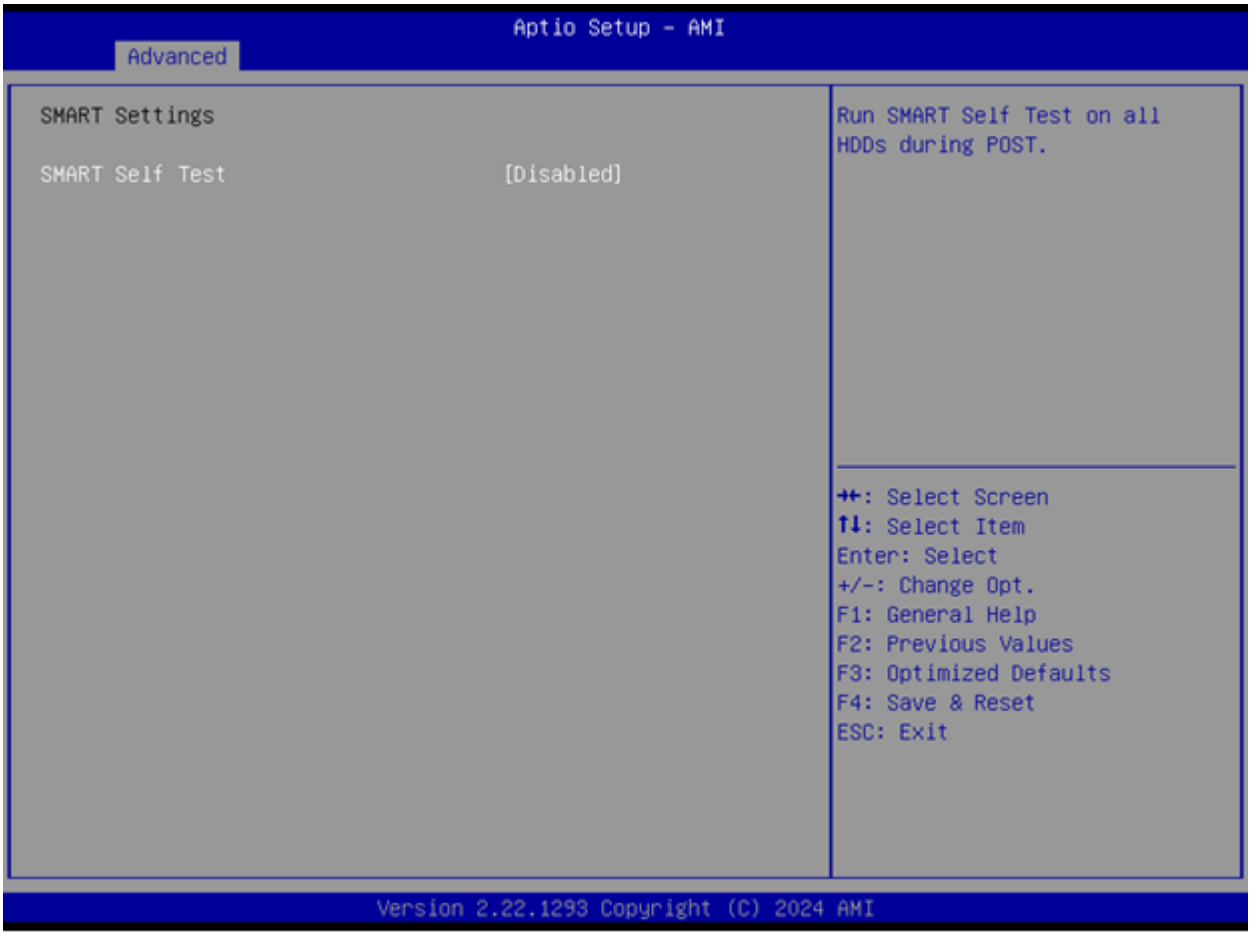
The **Trusted Computing** menu provides TPM configuration:

- **Firmware Version:** Shows TPM firmware version
  - Not selectable
- **Vendor:** Displays TPM manufacturer
  - Not selectable
- **Security Device Support:** Enable or disable TPM security
  - Default: Enabled
  - If disabled, TCG EFI protocol and INT1A interface will not be available
- **Pending Operation:** Schedule a TPM clear
  - Default: None
  - Options: None, TPM Clear
  - *Note*: System will reboot to change state

7.6 SMART Settings

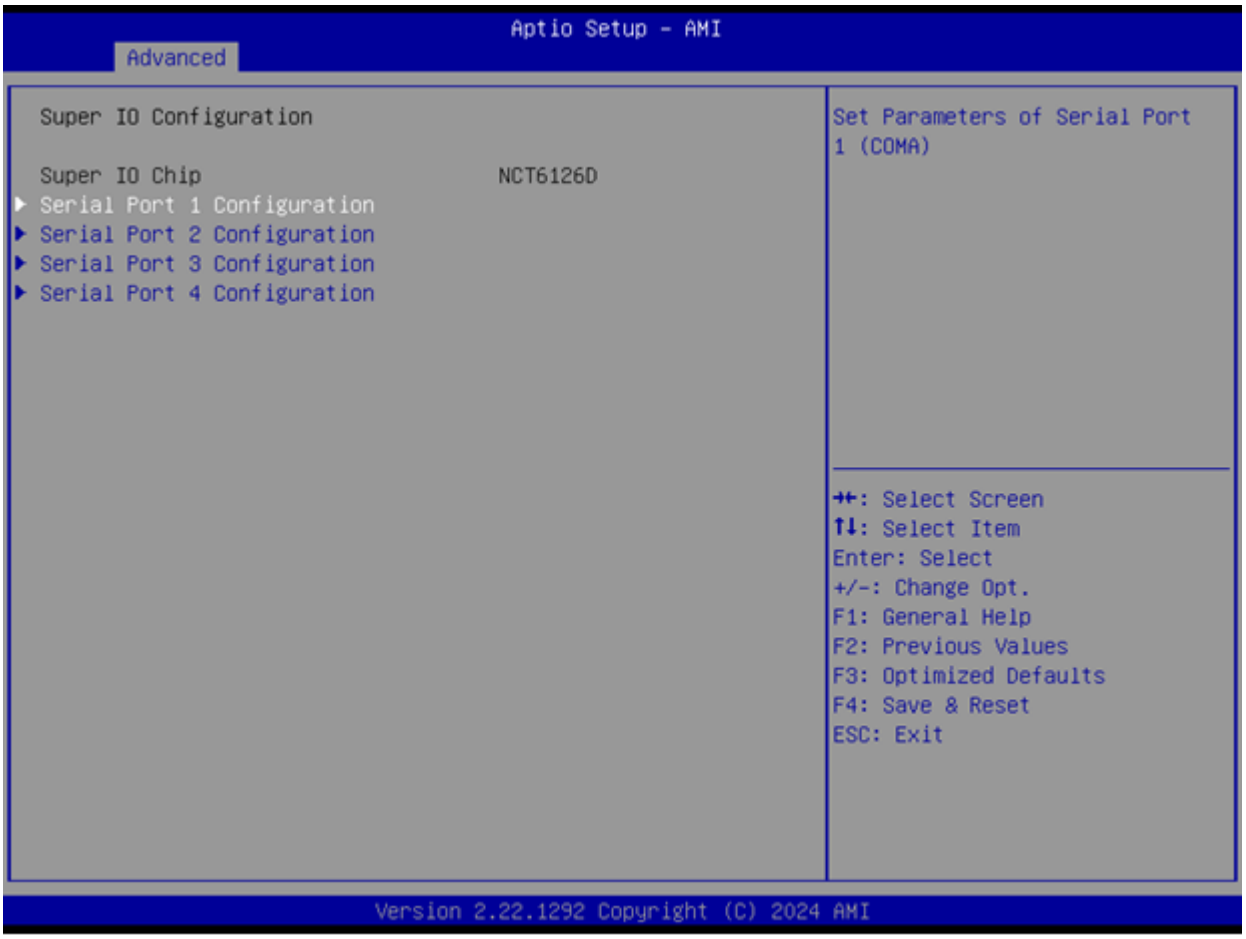
- **SMART Self Test:** Enable SMART self-test on all HDDs during POST
  - Default: Disabled
  - Options: Enabled, Disabled

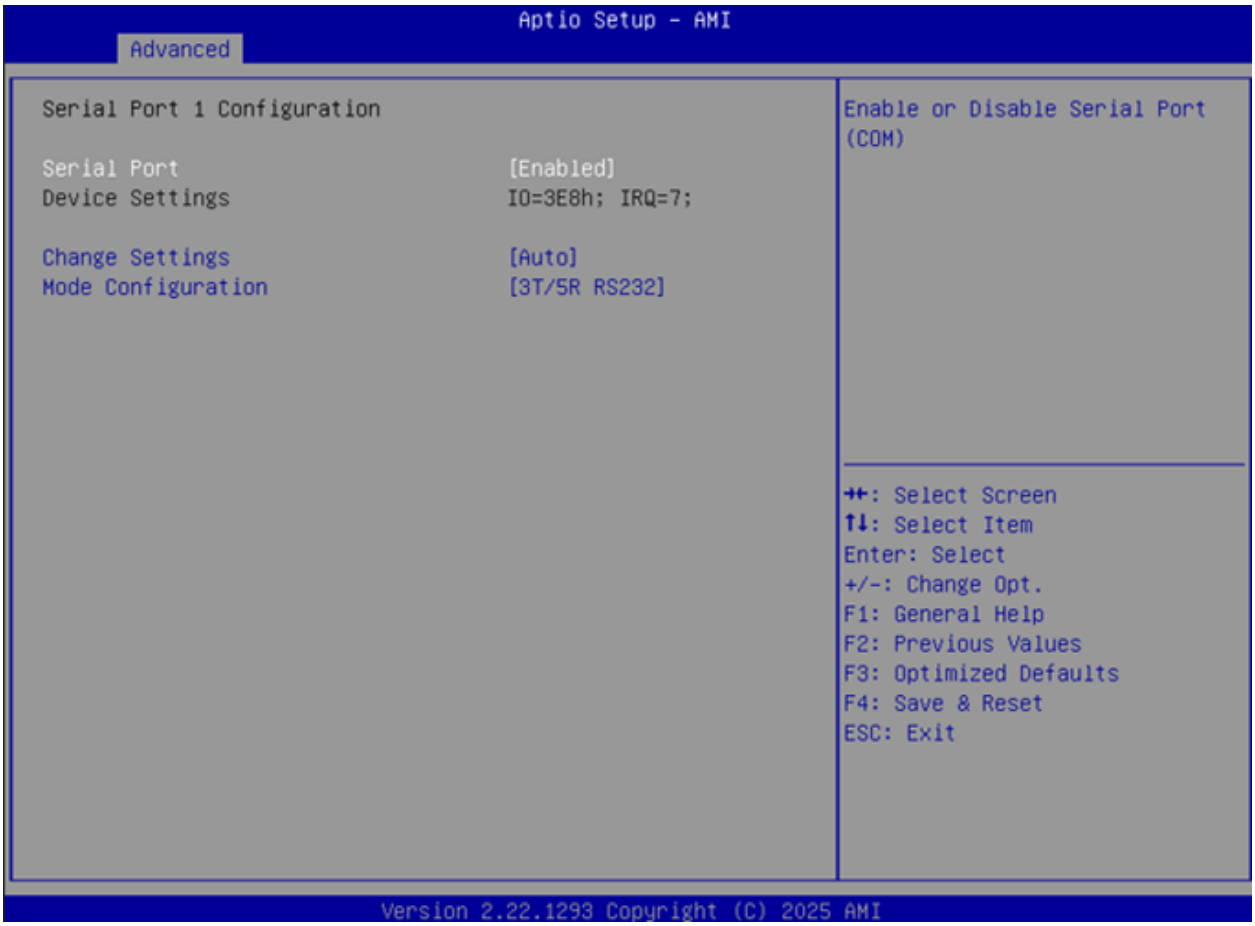
7.7 Super IO Configuration



This section allows configuring serial port parameters.

7.7.1 Serial Port 1 Configuration





- **Serial Port:** Enable or disable COM1
  - Default: Enabled
  - Options: Enabled, Disabled
- **Device Settings:** Shows COM1 address/IRQ
  - Not selectable
- **Change Settings:**
  - Default: Auto
  - Possible values:
    - 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
- **Mode Configuration:**
  - Default: 3T/5R RS232
  - Possible values:
    - 1T/1R RS422

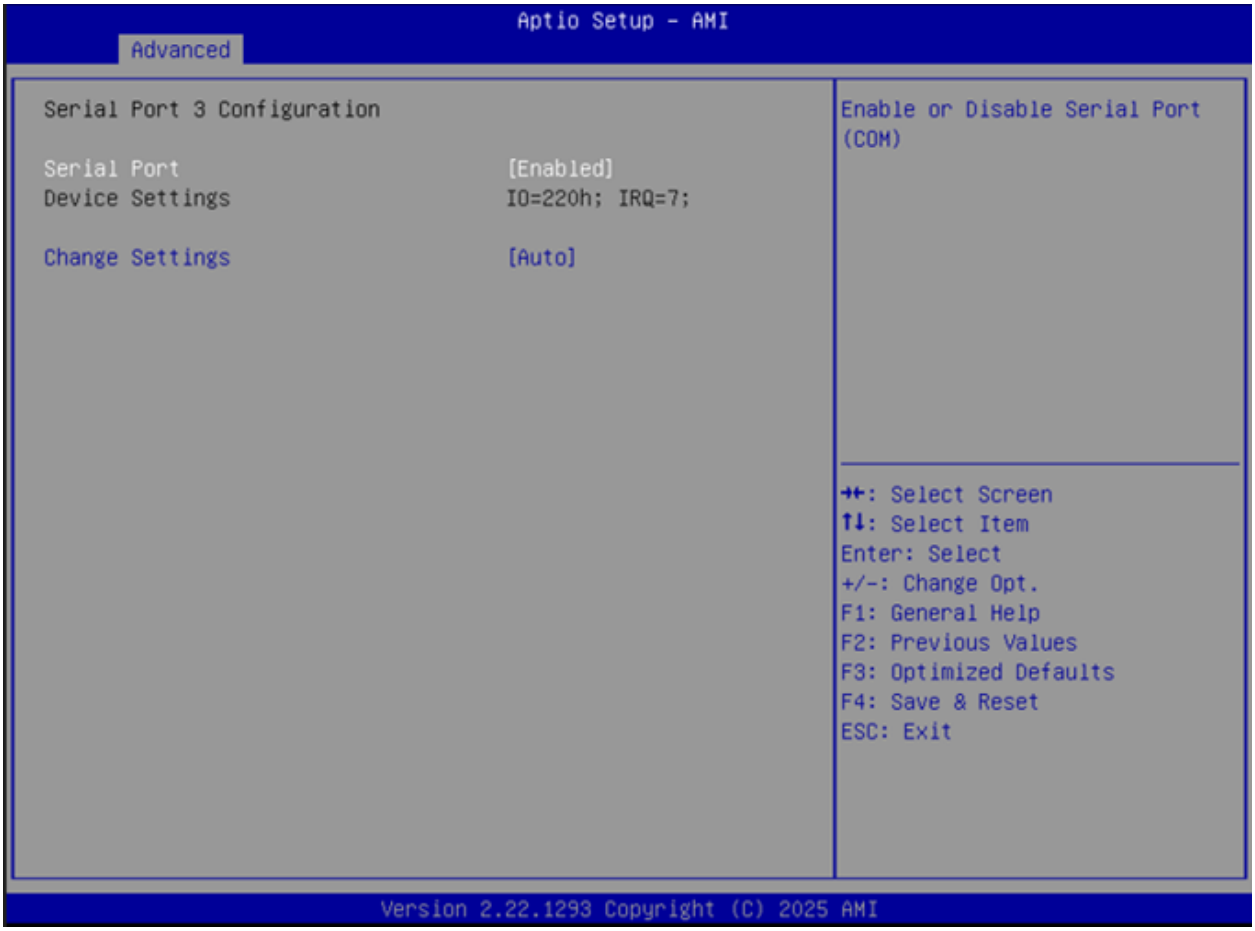
* 3T/5R RS232
* 1T/1R RS485 TX ENABLE Low Active
* 1T/1R RS422 with termination resistor
* 1T/1R RS485 with termination resistor TX ENABLE Low Active
* Disabled

7.7.2 Serial Port 2 Configuration

- **Serial Port:** Enable or disable COM2
  - Default: Enabled
  - Options: Enabled, Disabled
- **Device Settings:** Shows COM2 address/IRQ
  - Not selectable
- **Change Settings:**
  - Default: Auto
  - Possible values:
    * Auto
    * IO=2E8h;IRQ=7
    * IO=3E8h;IRQ=3,4,5,6,7,9,10,11,12

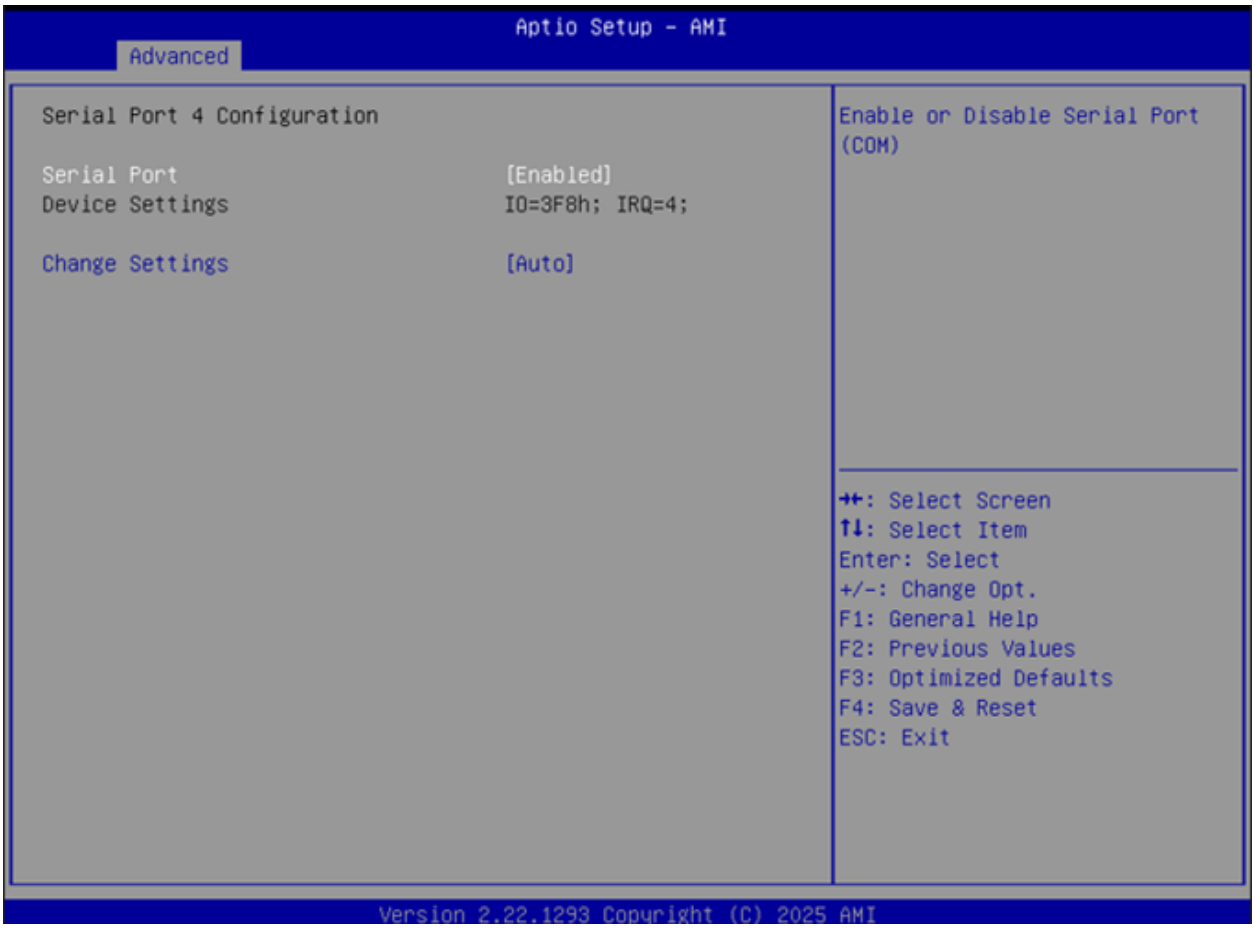
* IO=2E8h;IRQ=3,4,5,6,7,9,10,11,12
* IO=220h;IRQ=3,4,5,6,7,9,10,11,12
* IO=228h;IRQ=3,4,5,6,7,9,10,11,12

7.7.3 Serial Port 3 Configuration



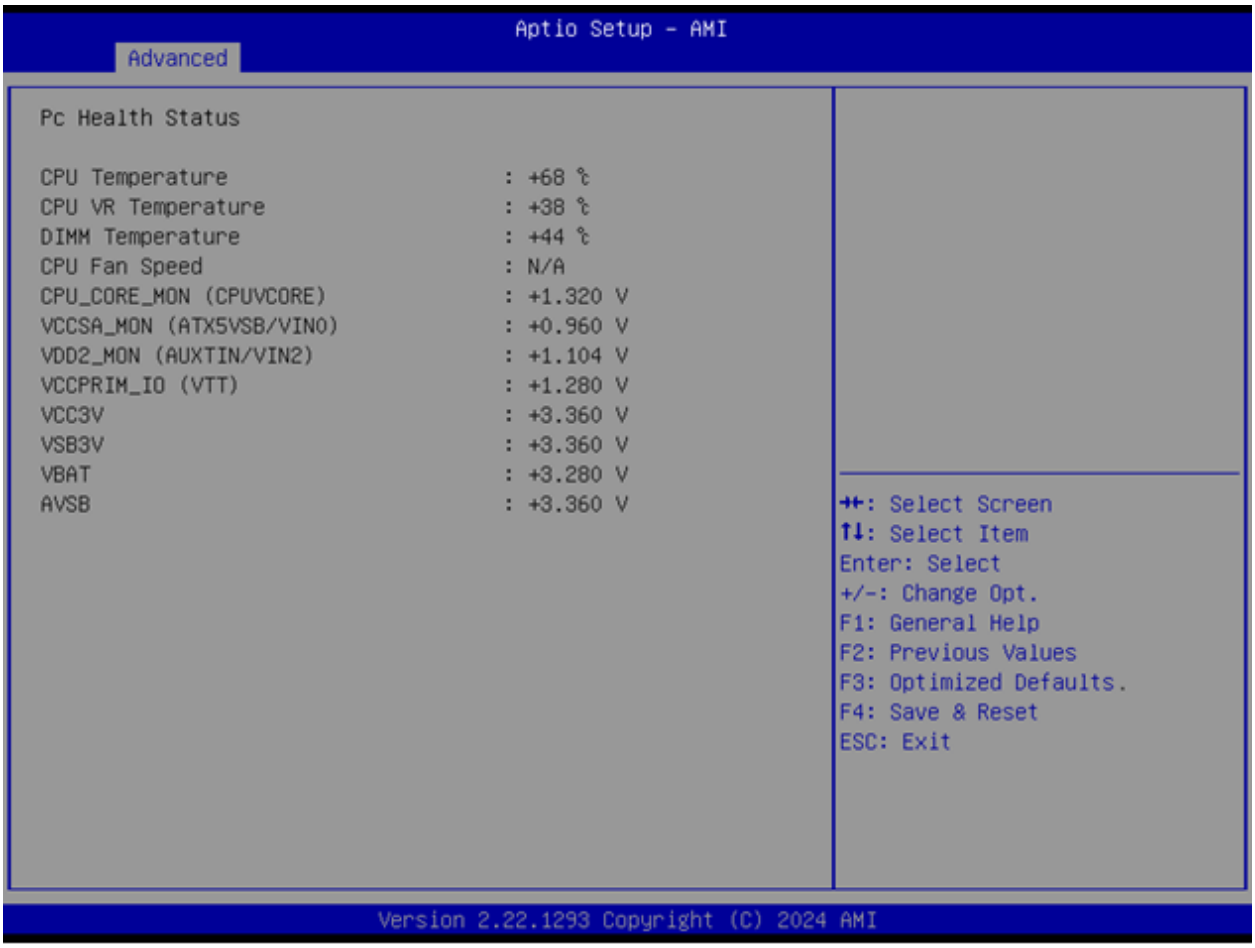
- **Serial Port:** Enable or disable COM3
  - Default: Enabled
  - Options: Enabled, Disabled
- **Device Settings:** Shows COM3 address/IRQ
  - Not selectable
- **Change Settings:**
  - Default: Auto
  - Possible values:
    * Auto
    * IO=3E8h;IRQ=3,4,5,6,7,9,10,11,12
    * IO=2E8h;IRQ=3,4,5,6,7,9,10,11,12
    * IO=220h;IRQ=3,4,5,6,7,9,10,11,12
    * IO=228h;IRQ=3,4,5,6,7,9,10,11,12

7.7.4 Serial Port 4 Configuration



- **Serial Port:** Enable or disable COM4
  - Default: Enabled
  - Options: Enabled, Disabled
- **Device Settings:** Shows COM4 address/IRQ
  - Not selectable
- **Change Settings:**
  - Default: Auto
  - Possible values:
    - 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

7.8 Hardware Monitoring

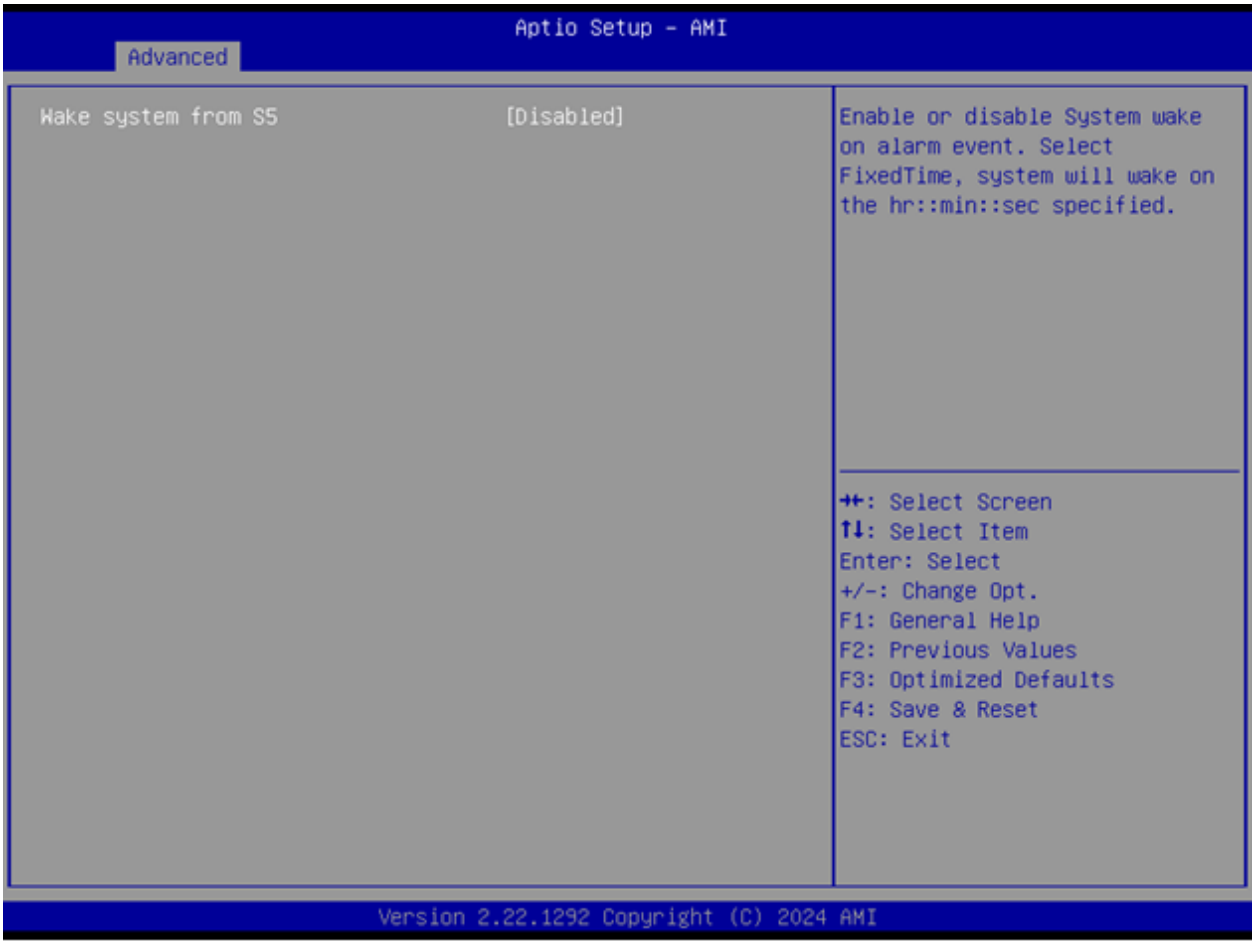


This section shows real-time hardware status:

- **CPU Temperature**
- **CPU VR Temperature**
- **DIMM Temperature**
- **CPU Fan Speed**
- **CPU_CORE_MON (CPUVCORE) Voltage**
- **VCCSA_MON (ATX5VSB/VIN0) Voltage**
- **VDD2_MON (AUXTIN/VIN2) Voltage**
- **VCCPRIM_IO (VTT) Voltage**
- **VCC3V**
- **VSB3V**
- **VBAT**
- **AVSB**

All fields above are display-only and cannot be modified.

7.9 S5 RTC Wake Settings

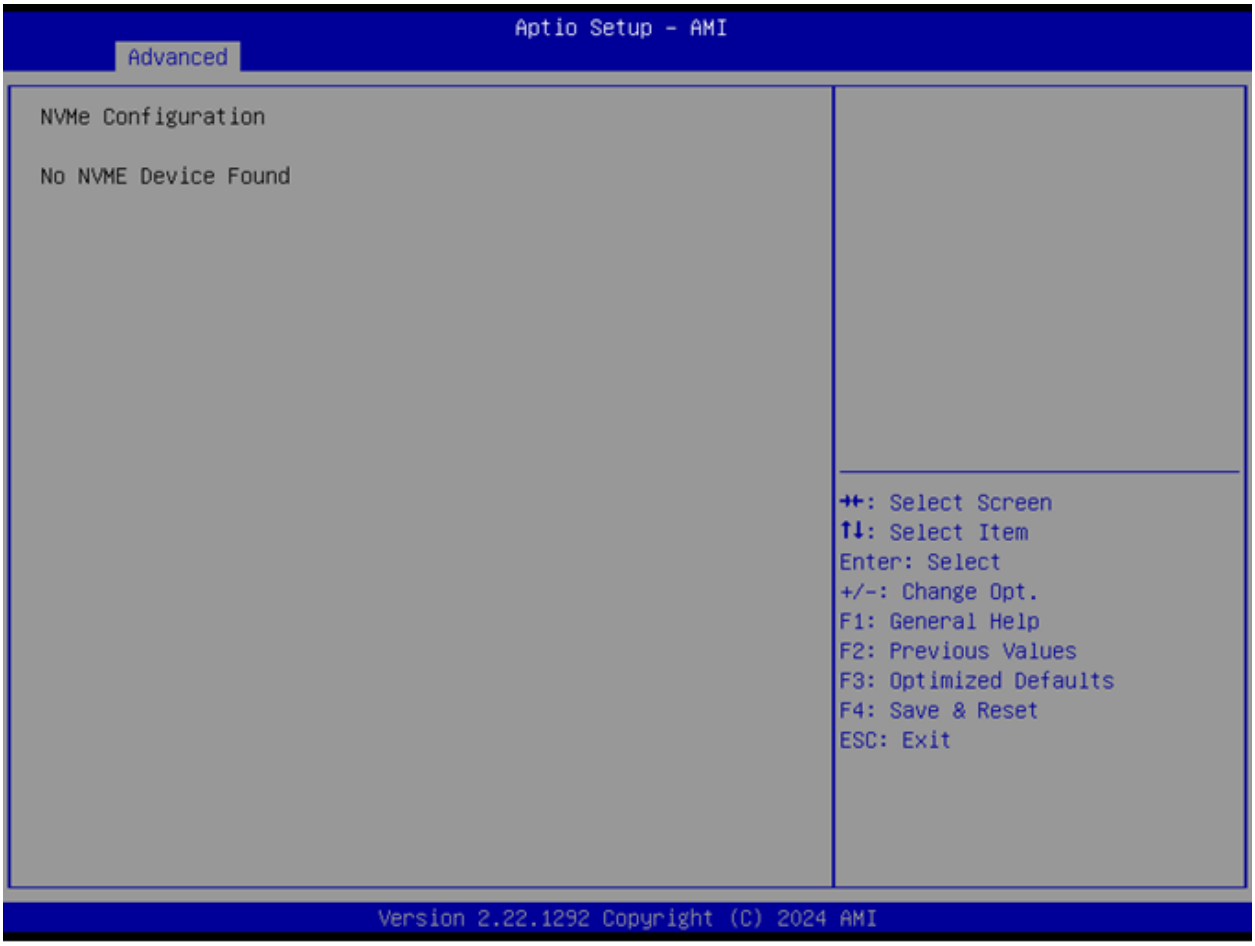


- **Wake system from S5:**
  - Default: Disabled
  - Options: Disabled, Fixed Time
- **Wake up hour:**
  - Default: 0
  - Range: 0–23
- **Wake up minute:**
  - Default: 0
  - Range: 0–59
- **Wake up second:**
  - Default: 0
  - Range: 0–59

7.10 Network Stack Configuration

- **Network Stack:**
  - Default: Disabled
  - Options: Enabled, Disabled
- **IPv4 PXE Support:**
  - Default: Disabled
  - Options: Enabled, Disabled
- **IPv6 PXE Support:**
  - Default: Disabled
  - Options: Enabled, Disabled

7.11 NVMe Configuration

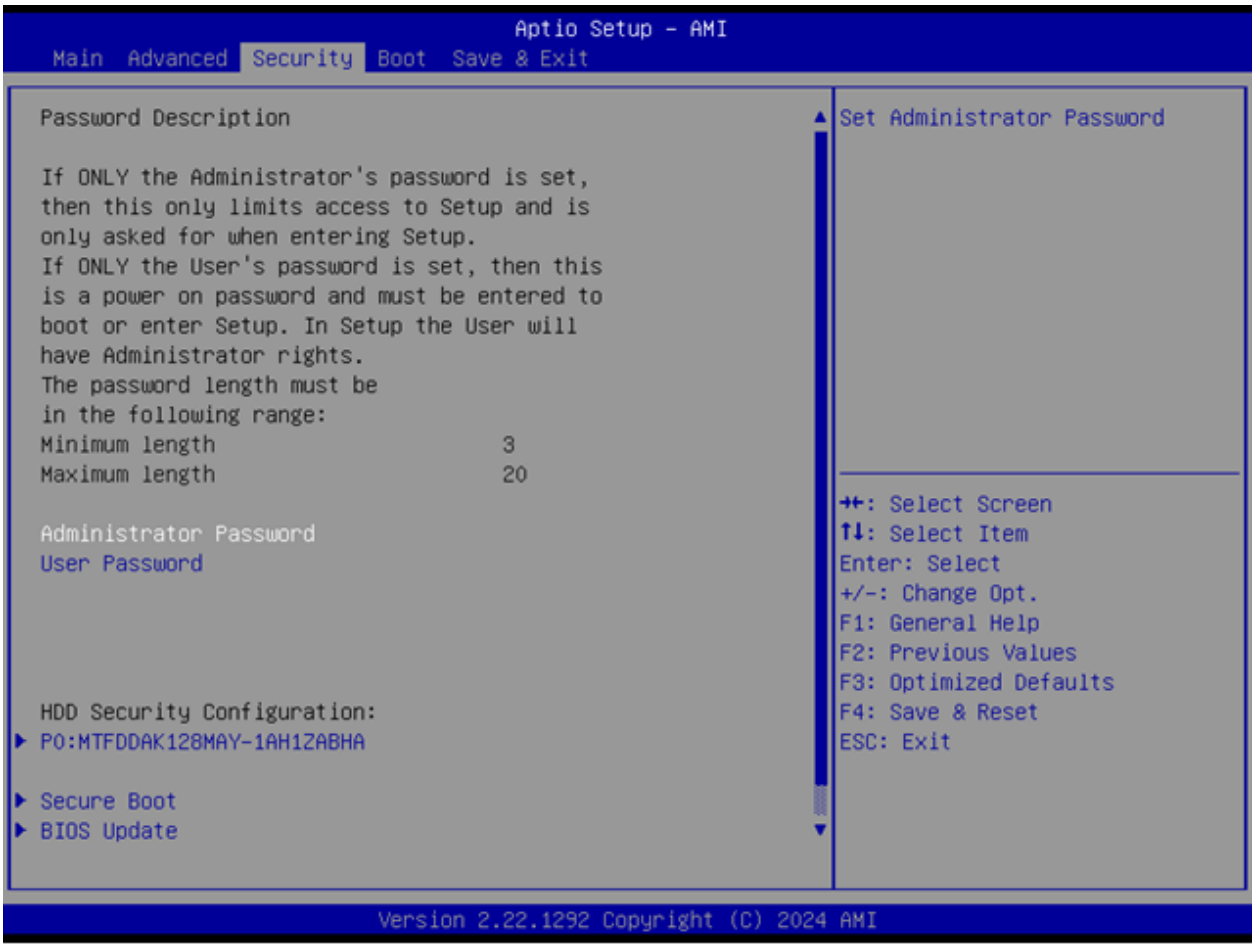


- View and manage connected NVMe devices

7.12 Intel® Rapid Storage Technology

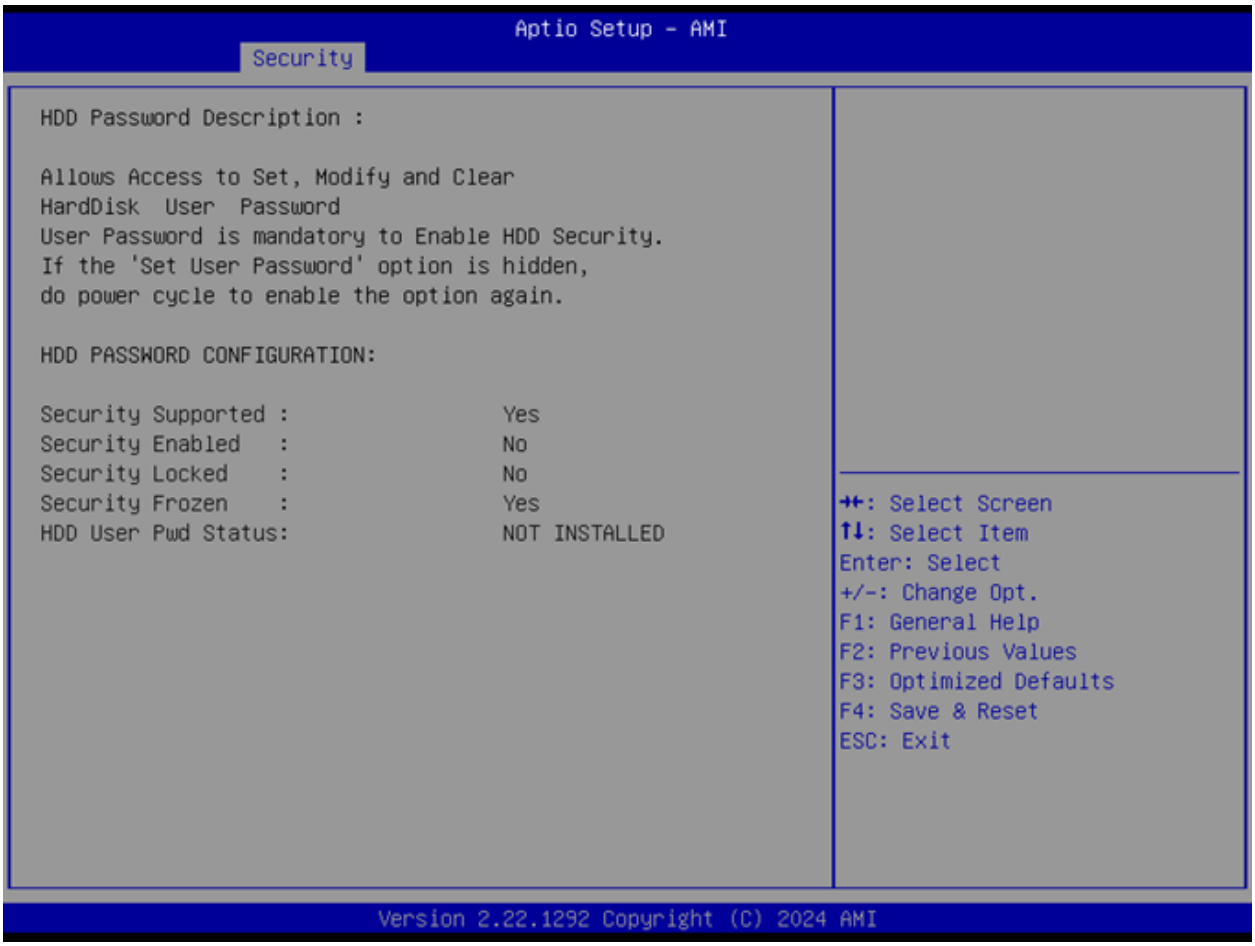
- Configure RAID volumes and manage Intel® RST

7.13 Security Page



The **Security Page** allows you to manage BIOS-level security features, passwords, and secure boot.

7.13.1 Security Options



- **Administrator Password:** Set or modify the administrator password to control BIOS access
- **User Password:** Set or modify a user-level password
- **HDD Security Drive:** Configure HDD password security for data protection
  - *Press Enter* to open the HDD Security sub-menu
- **Secure Boot:** Configure the secure boot feature to enforce trusted OS loaders
  - *Press Enter* to open the Secure Boot sub-menu
- **BIOS Update:** Launch the BIOS update utility
  - *Press Enter* to open the BIOS Update menu

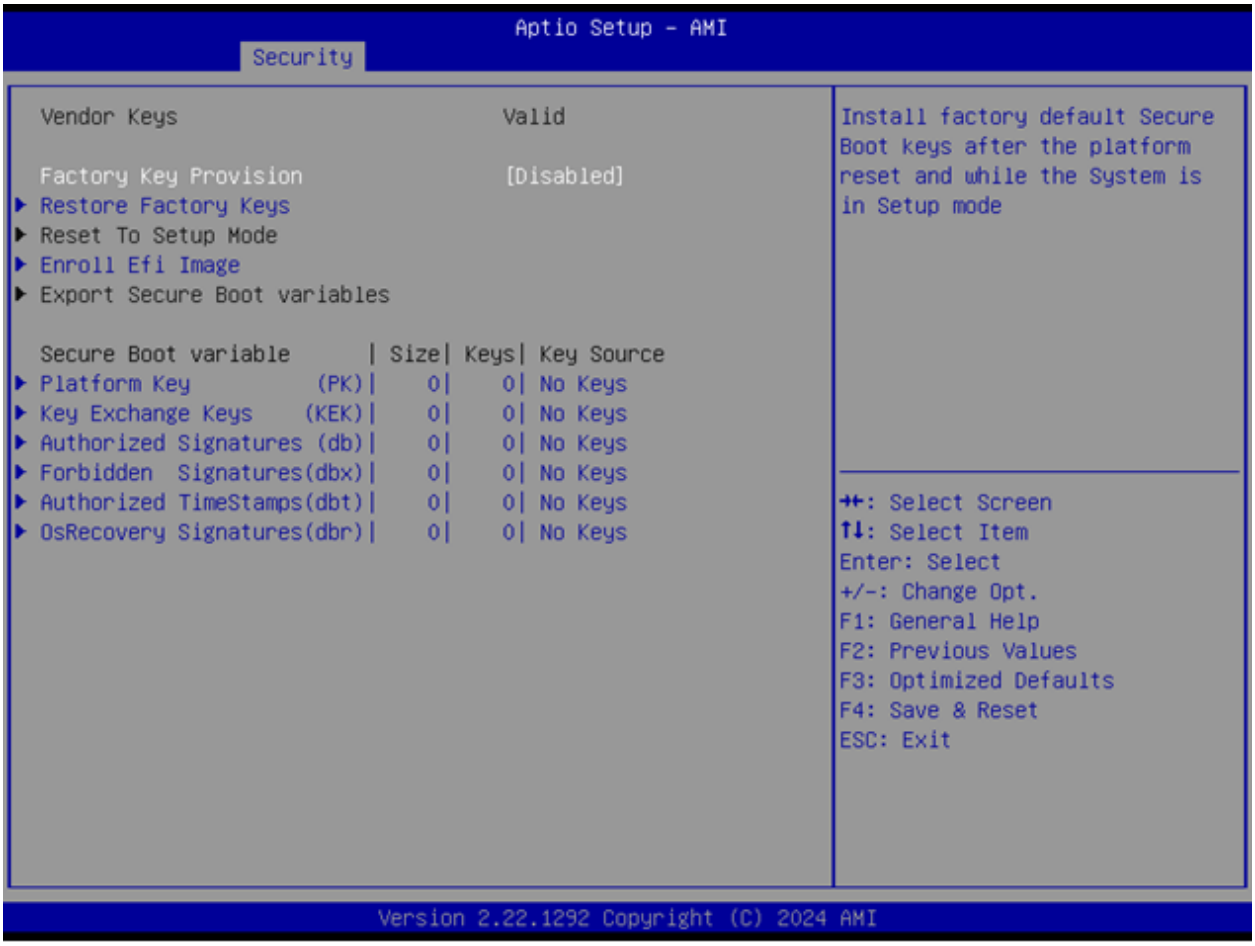
7.14 Secure Boot

The **Secure Boot** menu allows fine-grained security configuration of boot keys and policies:

- **Secure Boot:**
  - Default: Enabled
  - Options: Enabled, Disabled
  - When enabled, the platform key (PK) must be enrolled and system is in User mode
  - Mode change requires a platform reset
- **Secure Boot Mode:**
  - Default: Standard
  - Options: Standard, Custom
  - In Custom mode, you can configure Secure Boot Policy variables manually
- **Restore Factory Keys:**
  - Force system to User Mode and reinstall factory default Secure Boot key databases
- **Reset to Setup Mode:**
  - Deletes all Secure Boot keys from NVRAM
- **Key Management:**
  - Advanced certificate management for Secure Boot

- *Press Enter* to open Key Management

7.14.1 Key Management



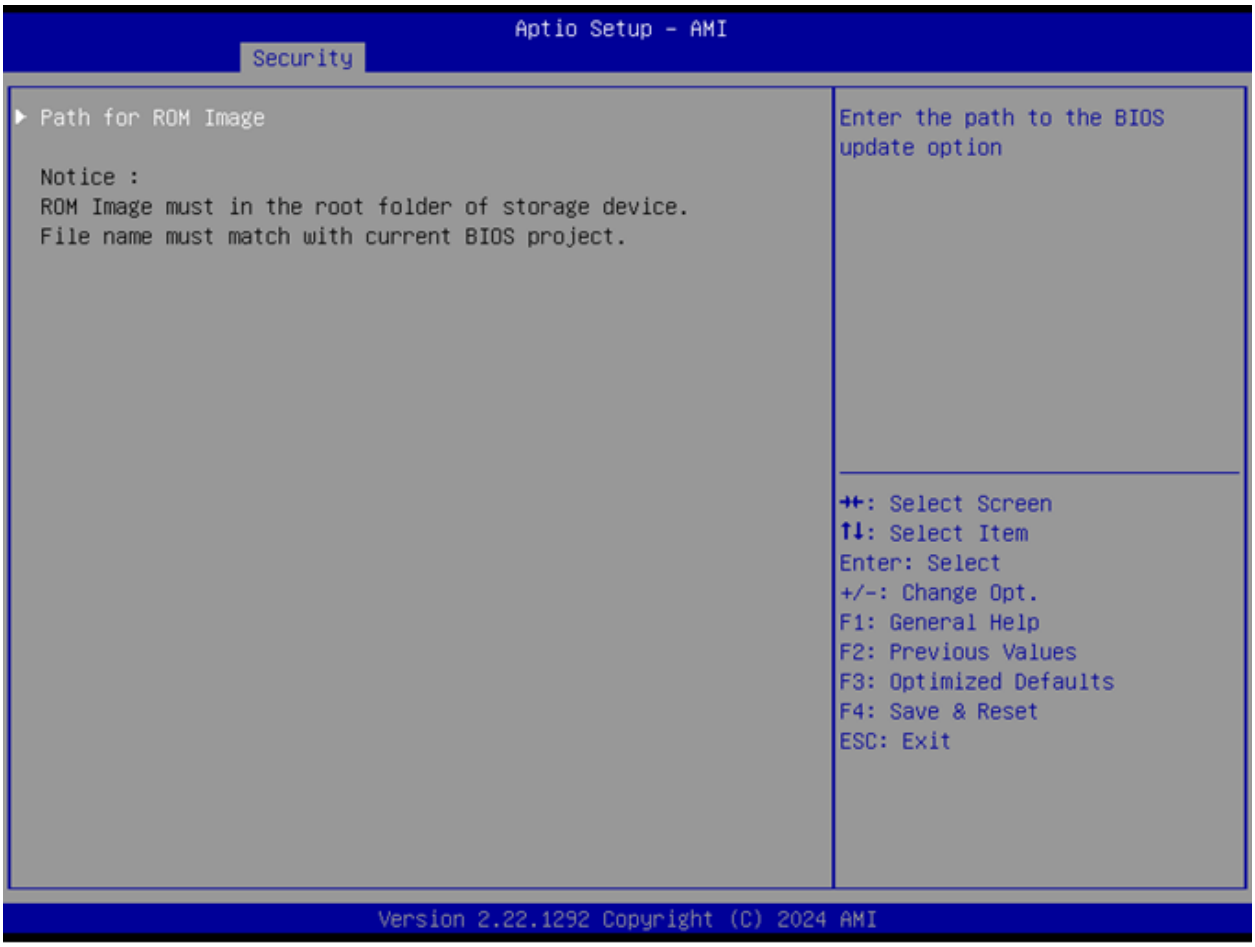
This sub-menu provides advanced options to manage Secure Boot certificates:

- **Factory Key Provision:**
  - Default: Disabled
  - Options: Enabled, Disabled
  - Installs factory default Secure Boot keys after a platform reset in Setup mode
- **Restore Factory Keys:**
  - Reinstalls factory default Secure Boot key databases
- **Reset to Setup Mode:**
  - Deletes all Secure Boot key databases from NVRAM
- **Enroll EFI Image:**
  - Allows specific EFI images to run in Secure Boot mode
  - Enrolls the SHA256 certificate of a PE image into the authorized signature database (db)
- **Export Secure Boot Variables:**
  - Save the NVRAM content of Secure Boot variables to a file
- **Platform Key (PK):**

  - Displays size, count, and source of keys
  - Allows enrollment from factory or custom
- **Key Exchange Keys (KEK):**
  - Same functionality as PK, but for key exchange
- **Authorized Signatures (db):**
  - Shows enrolled signatures
- **Forbidden Signatures (dbx):**
  - Shows blocked signatures
- **Authorized TimeStamps (dbt):**
  - Manages time-based keys
- **OsRecovery Signatures (dbr):**
  - Handles signatures for OS recovery images

All key items above support factory, modified, and mixed key sources.

7.15 BIOS Update

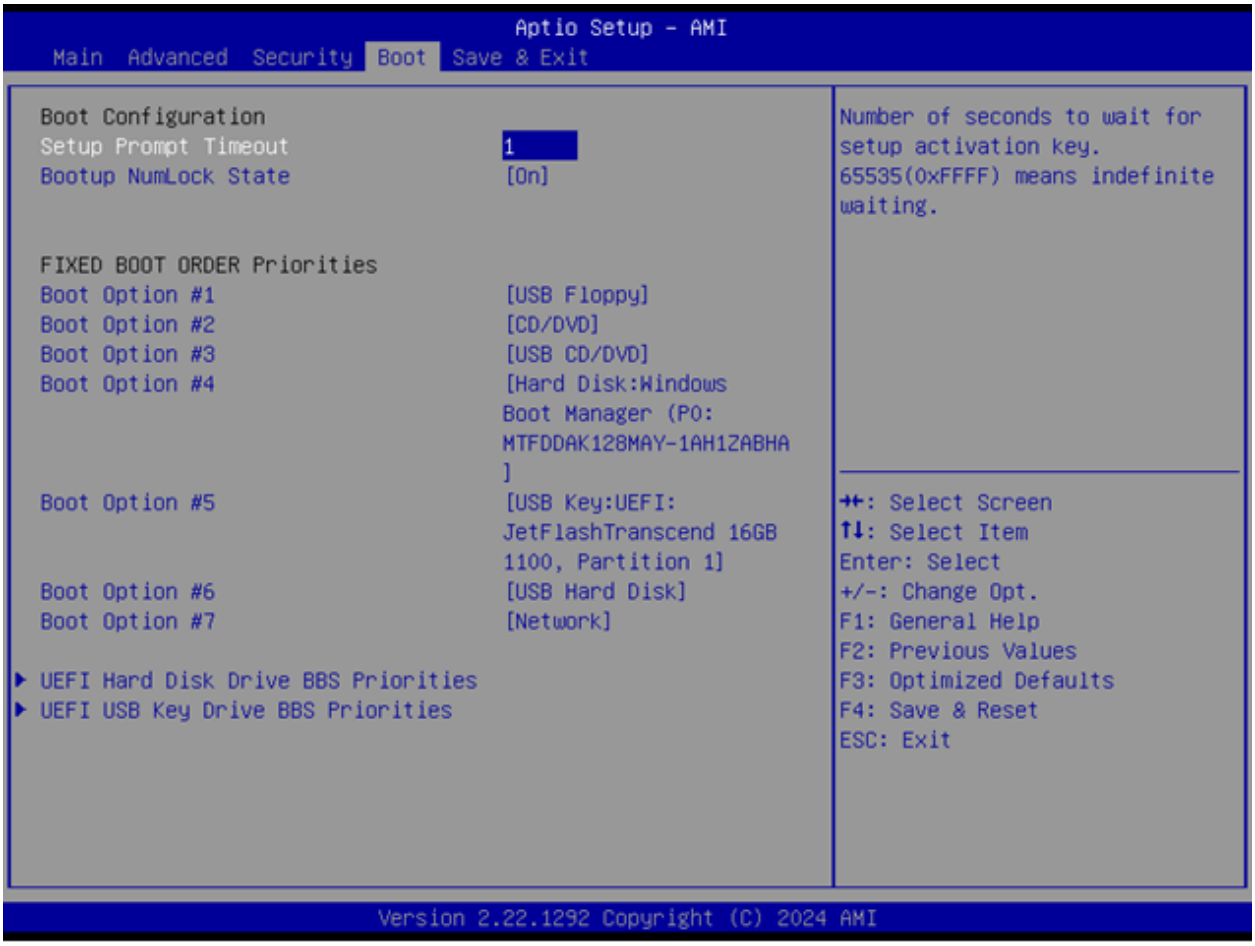


The **BIOS Update** sub-menu lets you specify a file path to a BIOS ROM image:

- **Path for ROM Image:**

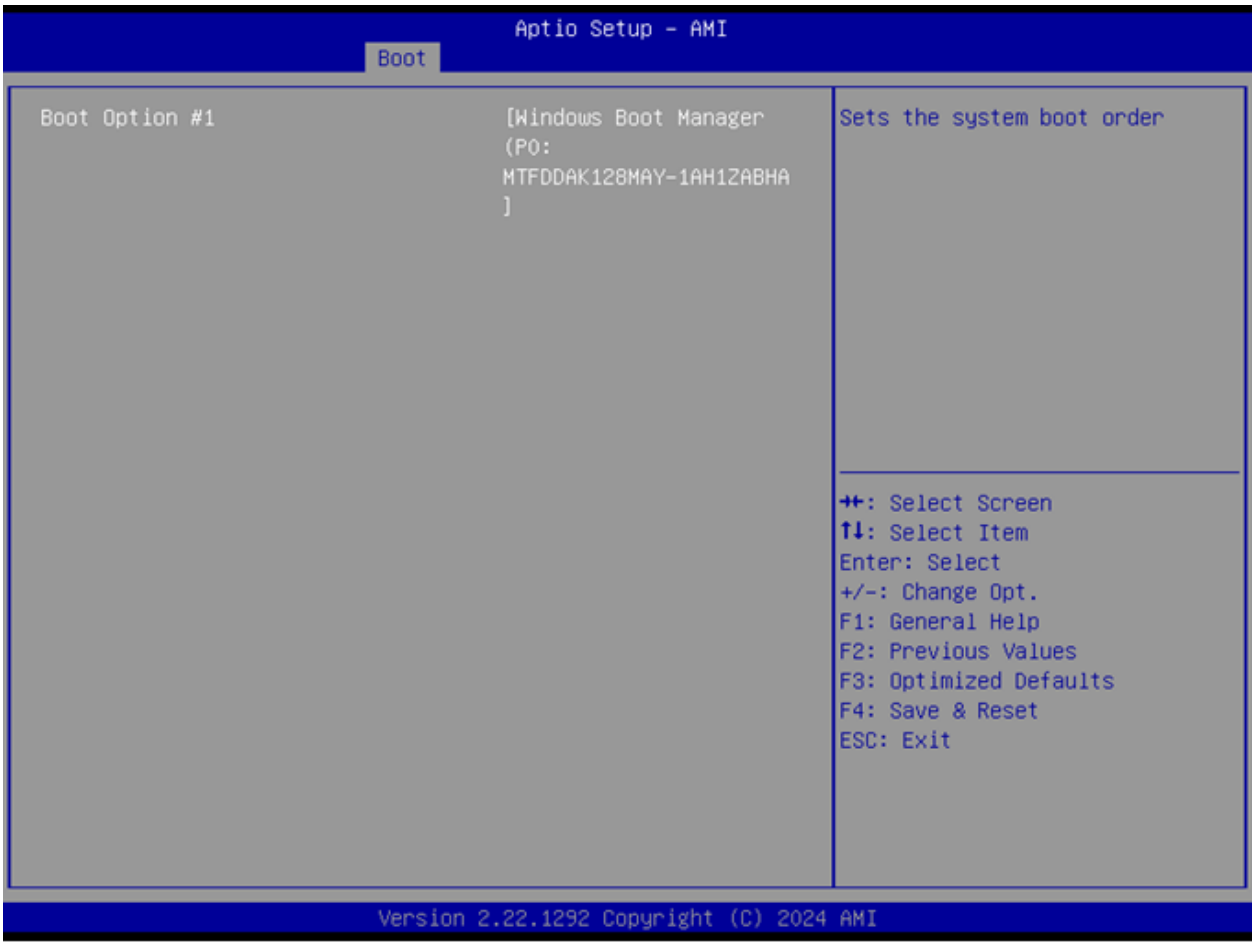
- Enter the location of the BIOS update image

7.16 Boot Page



The **Boot Page** allows configuring boot priorities and timeouts:

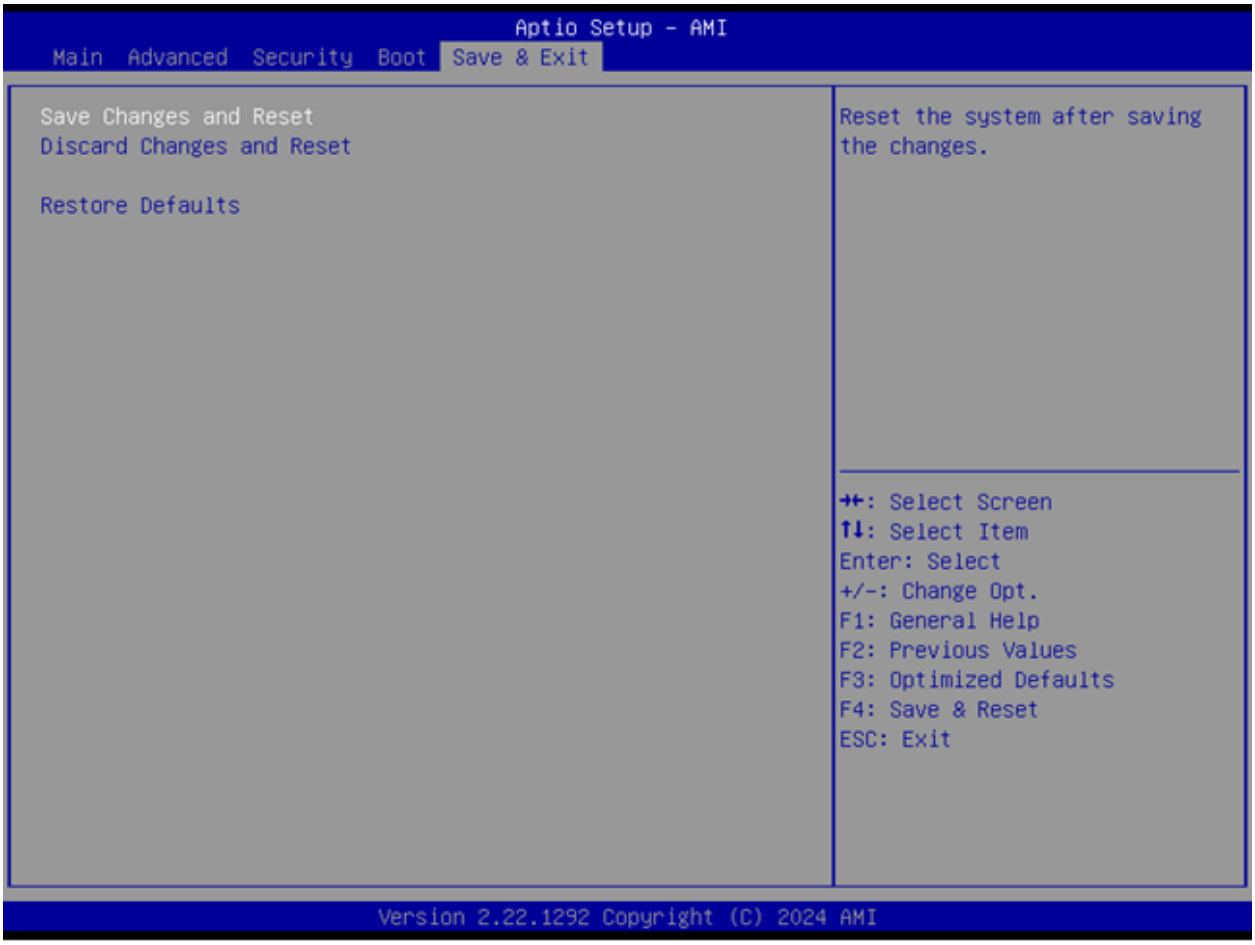
- **Setup Prompt Timeout:**
  - Default: 1 second
  - Range: 1–65535 (0xFFFF means indefinite)
  - Sets how long the BIOS waits for user input
- **Bootup NumLock State:**
  - Default: On
  - Options: On, Off
  - Controls keyboard NumLock



- **Boot Option #1–#7:**
  - Define priority among USB, CD/DVD, hard disk, network, and disabled
  - Examples:
    - USB Floppy
    - CD/DVD
    - USB Hard Disk
    - Network
    - Disabled
- **(UEFI) USB Floppy Drive BBS Priorities:**
  - Configure boot device order for UEFI USB floppy devices
- **(UEFI) CDROM/DVD Drive BBS Priorities:**
  - Configure boot device order for UEFI CD/DVD devices
- **(UEFI) USB CDROM/DVD ROM Drive BBS Priorities:**
  - Configure boot device order for UEFI USB CD/DVD devices
- **(UEFI) Hard Disk Drive BBS Priorities:**
  - Configure boot device order for UEFI hard disks
- **(UEFI) USB Key Drive BBS Priorities:**
  - Configure boot device order for UEFI USB key drives

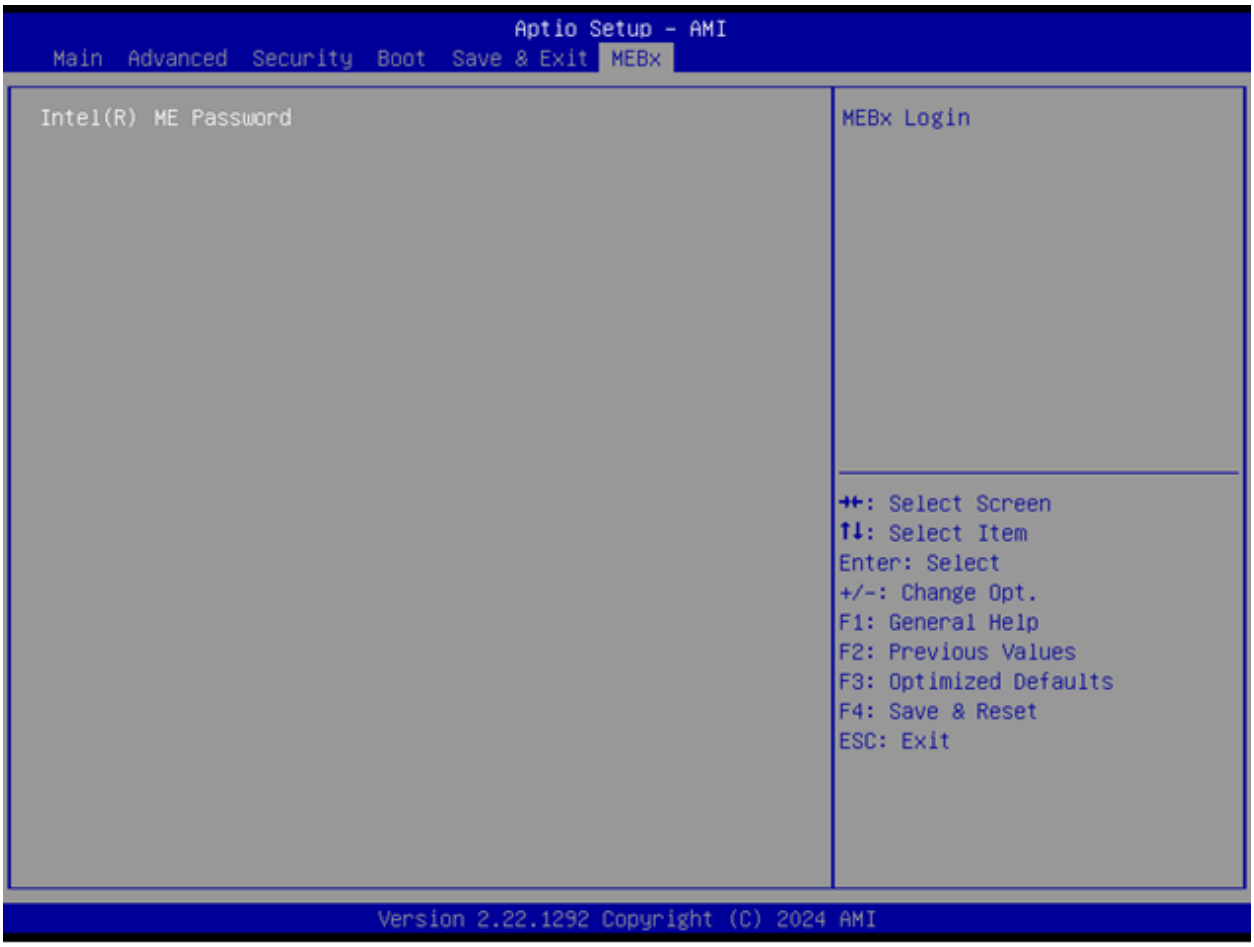
- **(UEFI) USB Hard Disk Drive BBS Priorities:**
  - Configure boot device order for UEFI USB hard disks
- **(UEFI) Network Drive BBS Priorities:**
  - Configure boot device order for UEFI network devices

7.17 Save & Exit



- **Save Changes and Reset:** Save configuration and restart
- **Discard Changes and Reset:** Restart without saving
- **Restore Defaults:** Reset all BIOS settings to factory defaults

7.18 MEBx



If the platform supports Intel AMT, the **MEBx** page allows secure remote management:

- **Intel® ME Password:** Default: `admin`
  - Requires immediate password change on first login
  - **Password Policy:**
    1. Minimum 8, maximum 32 characters
    2. Must include:
       * at least one digit (0–9)
       * at least one ASCII special character (excluding `:`, `,`, `"`)
       * at least one upper-case and one lower-case letter

This page will not appear if Intel AMT is not supported.