Alderamin Pico Mk4 Series

Version:
v1.1.0

Date:
25.11.2025

Contents

1 Copyright

2 Regulatory Compliances

2.1 CE and UKCA Notice

This device complies with the requirements of the CE directive and UKCA regulations.

Low Voltage Directive 2014/35/EU + Electrical Equipment Safety Regulations 2016 (SI 2016 No 1101)

- EN IEC 62368-1:2020+A11:2020
- BS EN IEC 62368-1:2020+A11:2020

EMC Directive 2014/30/EU + Electromagnetic Compatibility Regulations 2016

- EN 55032:2015+A11:2020
- BS EN 55032:2015+A11:2020
- EN 55032:2015+A11:2020
- BS EN 55032:2015+A11:2020
- EN IEC 61000-3-2:2019
- BS EN IEC 61000-3-2:2019+A1:2021
- EN 61000-3-3:2013+A1:2019
- BS EN 61000-3-3:2013+A1:2019+A2:2021
- EN 55035:2017+A11:2020
- BS EN 55035:2017+A11:2020
- EN 61000-4-2:2009
- BS EN 61000-4-2:2009
- EN 55035:2017+A11:2020
- BS EN 55035:2017+A11:2020
- EN 61000-4-3:2009
- BS EN 61000-4-3:2009
- EN 61000-4-3:2006+A1:2008+A2:2010
- BS EN IEC 61000-4-3:2020
- EN 61000-4-4:2012
- BS EN 61000-4-4:2012
- EN 61000-4-5:2014+A1:2017
- BS EN 61000-4-5:2014+A1:2017
- EN 61000-4-6:2014
- BS EN 61000-4-6:2014
- EN 61000-4-8:2010
- BS EN 61000-4-8:2010
- EN 61000-4-11:2004

- BS EN 61000-4-11:2004

RoHS 2 Directive 2011/65/EU & 2015/863/EU + RoHS 2 Directive 2020 No. 1647

- Exemption(s) used:
- 6c,7a,7c-I

2.2 FCC PART 15 VERIFICATION STATEMENT

WARNING

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Notice: The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

2.3 ICED-003 ISSUE 7 VERIFICATION STATEMENT

CAN ICES3(B)/NMB3(B)

This device complies with CAN ICES-003 Issue 7 Class B. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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 and 2	
COM 1 and 4	
USB 1 … 6	
HDMI 1 and 2	
DP 1 and 2	
Audio Jack	
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 Product Specifications

5.1 Features

The **Alderamin Pico Mk4 Embedded System** delivers robust performance and versatile connectivity with the following key features:

- **Powerful Processing**: Supports **11th Generation Intel® Tiger Lake-UP3 Core™ i7 / i5 / i3 / Celeron** processors.
- **Integrated Graphics**: Equipped with the **Intel® Iris Xe Graphics Engine**.
- **Enhanced Display Support**: Enables **quad display** connectivity via **HDMI** and **DisplayPort** interfaces.
- **Efficient Cooling**: Fanless chassis design with an expandable module layout.
- **Wide Voltage Range**: Operates on **8–24V** for Pico Mk4 and **12–36V** for Pico Mk4-D.
- **Thermal Performance Options**:
  - **15W TDP**: Operating range of **–40°C to 70°C**
  - **28W TDP**: Operating range of **–40°C to 60°C**

Operating conditions assume 0.7 m/s airflow with extended temperature SSD/mSATA/RAM configurations.

5.2 Packing List

Item	Description	Q'ty
1	Alderamin Pico Mk4 Embedded System	1
2	Wall Mount Brackets (2 pcs in 1 set)	2
3	Screw Pack (For HDD and Wall Mount Bracket)	1
4	3-pin Terminal Block Power Connector (DC Input)	1
5	2-pin Terminal Block Power Connector (Remote Power)	1

5.3 Technical Details

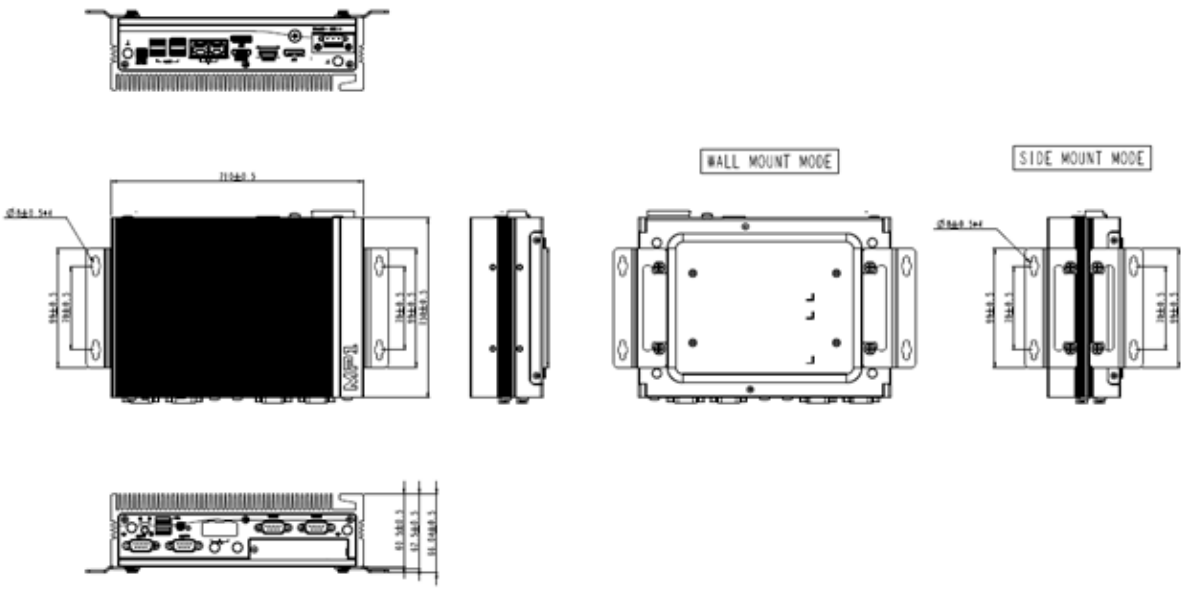
Feature	Specification	Details
Processor	CPU	11th Gen Intel® Tiger Lake-UP3 Core™ i ULV Processor:• **i3-1115G4E** – Dual Core, 6MB Cache, up to 3.90 GHz• **i5-1145G7E** – Quad Core, 8MB Cache, up to 4.10 GHz• **i7-1185G7E** – Quad Core, 12MB Cache, up to 4.40 GHz
Security	I/O Chipset	Nuvoton NCT6126D
	TPM	Nuvoton NPCT750AABYX TPM 2.0
Memory	System Memory	DDR4 3200 MHz, 1 × 260-pin SO-DIMM, up to 32GB (Non-ECC)
Graphics	GPU	Intel® Iris Xe Graphics
Display	Display Interfaces	HDMI, DisplayPort
Storage	Storage Slots	1 × Hot Swappable 2.5″ HDD/SSD (max 9.5 mm height); 1 × M.2 B Key (2280/2260/2242)
Networking	Ethernet	Intel® I225-LM 2.5GbE LAN, Intel® I219-LM Giga LAN*(Optional: 2 × Intel® I210-IT Giga LAN)*
Audio	Audio	Realtek® ALC256
Expansion	Expansion Slots	Wireless: M.2 2230 E Key (PCIe, USB)Storage/LTE/5G: M.2 B Key (USB 2.0 / PCIe x1 / SATA III)*Note: Does not support M.2 M Key NVMe SSD. 5G card support available as a BOM option.*
Indicators	LED Indicators	Power LED, HDD LED
I/O Ports	Front I/O	3 × RS2321 × RS232/422/4851 × Audio Combo Jack (Mic-in/Line-out)1 × Hot Swappable 2.5″ HDD/SSD slot2 × USB 2.02 × SMA Antenna *(Optional)*
	Rear I/O	2 × DisplayPort 1.22 × HDMI 1.42 × RJ-454 × USB 3.1 Gen 2 (10 Gbps)1 × 3-pin Terminal Block Power Input1 × 2-pin Terminal Block Remote Power On/Off2 × SMA Antenna *(Optional)*
Watchdog Timer	Software Programmable	1–255 Steps
Power	Power Input	Alderamin Pico Mk4: 8–24V DC Input with Terminal Block Connectivity*Note: Power Ignition Expansion Module is optional for Pico Mk4-D.*
Cooling	Thermal Design	Fanless
Mechanical	Mounting	Wall Mount / Side Mount; Optional VESA Holes (75 mm × 75 mm) & DIN Rail Mount Kit
	Dimensions	8.3″ × 5.9″ × 2.5″ (210 mm × 150 mm × 63 mm)
	Material	Top Cover: Aluminum Alloy; Bezel & Chassis: Steel
Environmental	Operating Temperature	15W TDP: –40°C to 70°C; 28W TDP: –40°C to 60°C *(0.7 m/s airflow assumed)*
	Operating	10% to 95% R/H (Non-condensing)

5.4 ☒ Important Notes

- **PXE Application**: Ensure the i219-LM driver is pre-installed in the OS image prior to PXE-based OS installation.
- **Lithium Battery Warning**: This system contains a lithium battery. **Do NOT** puncture, mutilate, or dispose of it in fire. Replace only with the manufacturer-recommended type and dispose of used batteries in accordance with local regulations.

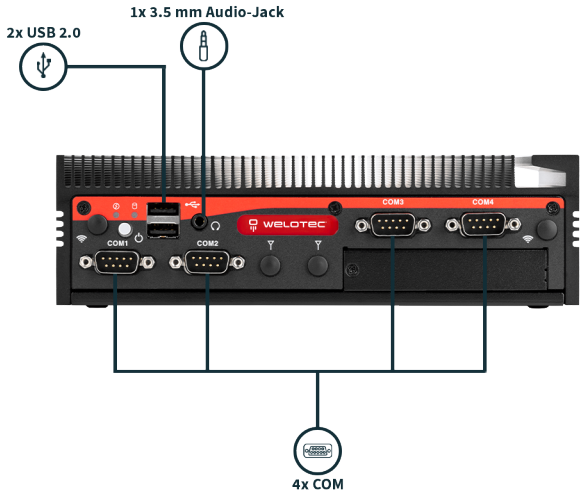
5.5 Mechanical Specification

Mechanical Dimension: 210 mm x 150 mm x 63 mm

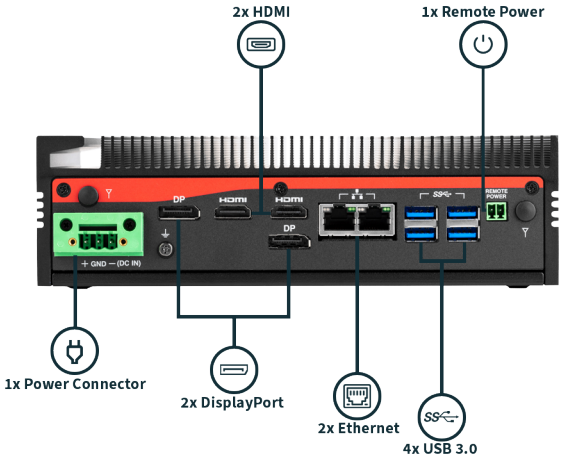


6 Interfaces and Connections

6.1 Front I/O



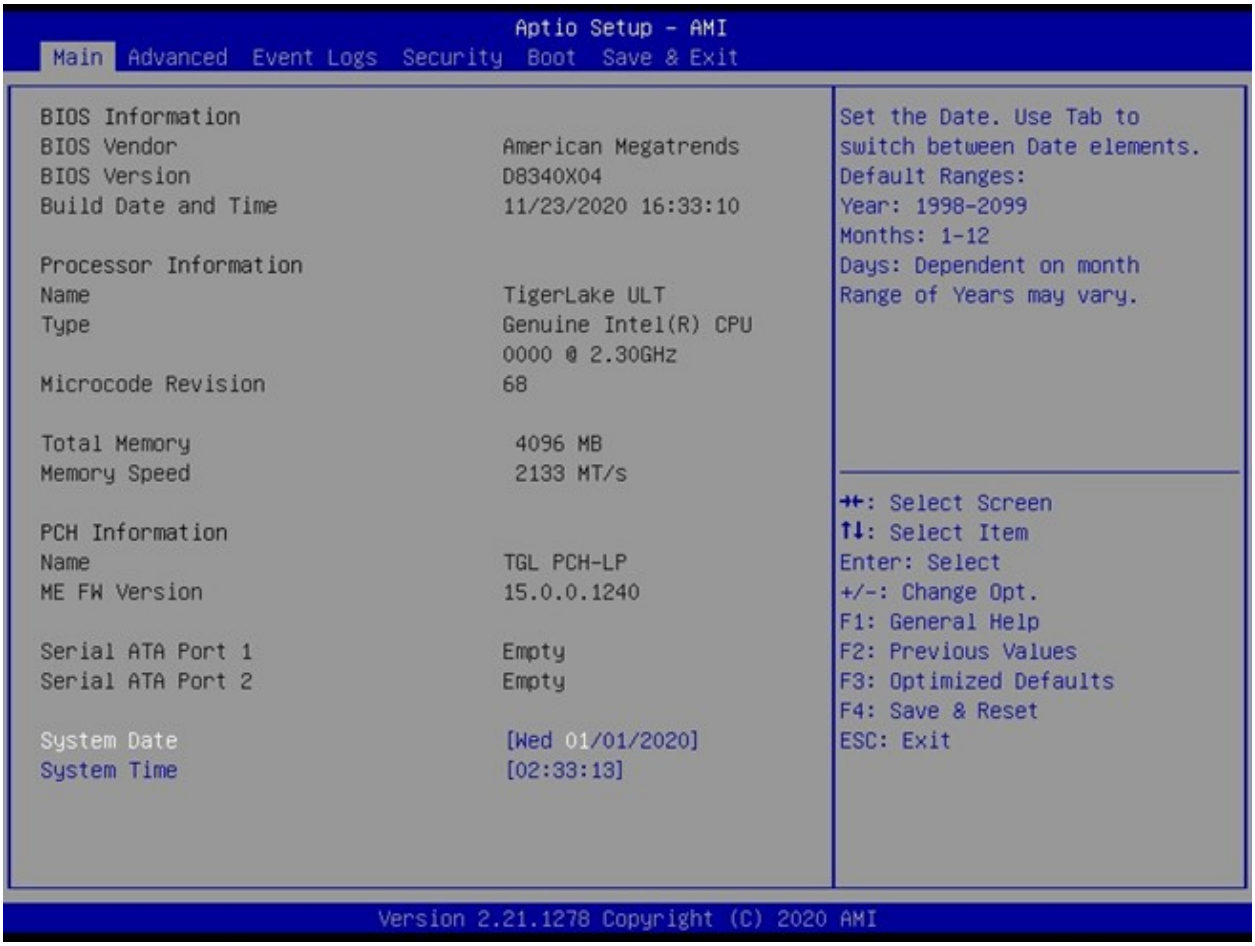
6.2 Rear I/O



7 BIOS

This chapter provides information on setting up the BIOS and using its menu items to adjust basic function settings.

7.1 Main Page



7.1.1 System Information

The Main Page displays essential system information. None of these fields are user-configurable:

- **BIOS Vendor:** American Megatrends
- **BIOS Version:** Displays the current BIOS version
- **Build Date and Time:** Shows the BIOS build date
- **Processor Information:** Displays the installed CPU brand
- **Microcode Version:** Displays the CPU microcode revision
- **Total Memory:** Shows the installed memory size
- **Memory Speed:** Displays the installed memory frequency

- **PCH Information:** Shows the PCH family
- **ME FW Version:** Displays the ME Firmware version
- **Serial ATA Port 1 & 2:** Show the installed SATA device models and sizes

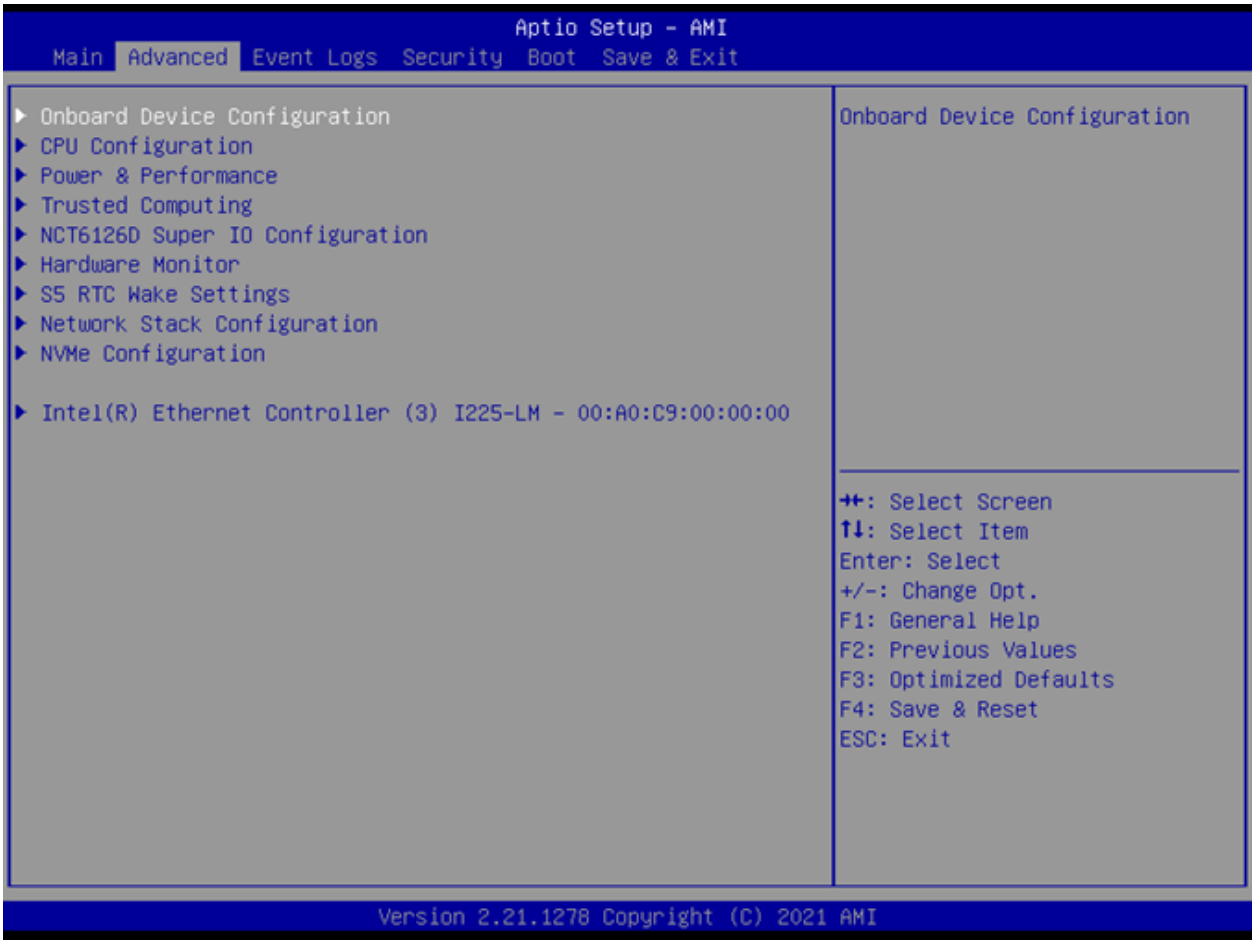
7.1.2 System Date & Time

Set the system's real-time clock using the following formats:

- **System Date:** `[Www mm/dd/yyyy]`
  - *Www:* Day of the week (Mon–Sun)
  - *mm:* Month (1–12)
  - *dd:* Day (1–31)
  - *yyyy:* Year (1998–2099)
- **System Time:** `[hh:mm:ss]`
  - *hh:* Hours (0–23)
  - *mm:* Minutes (0–59)
  - *ss:* Seconds (0–59)

Use the **Tab** key to navigate between date and time fields.

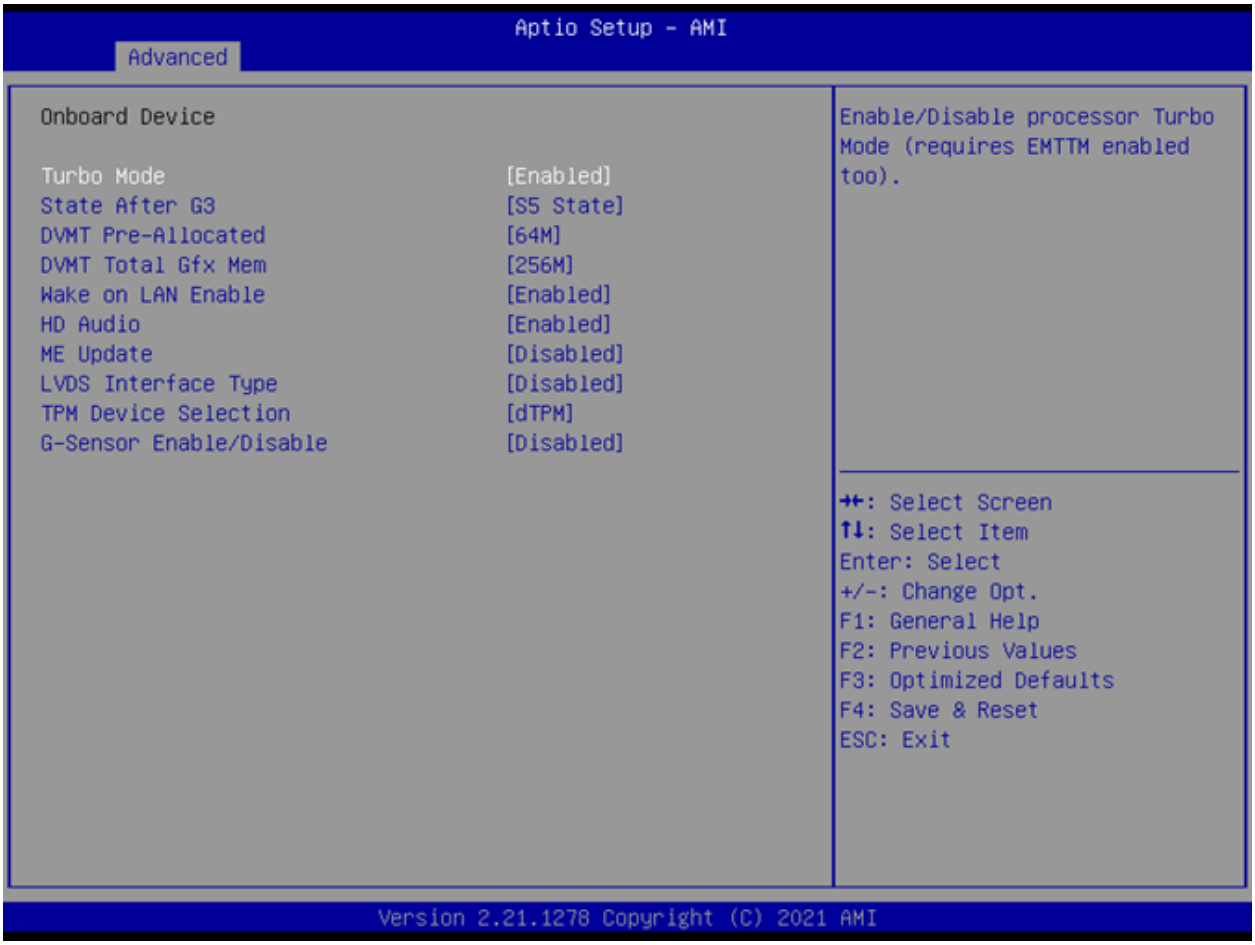
7.2 Advanced Page



The Advanced Page provides additional configuration options to fine-tune system behavior:

- **Onboard Device:** Configure integrated device settings (Press Enter to access the sub-menu).
- **CPU Configuration:** View and adjust processor parameters (Press Enter for details).
- **Power & Performance:** Modify power options and performance tuning (Press Enter to enter its sub-menu).
- **Trusted Computing:** Manage TPM and security features (Press Enter to access its sub-menu).
- **NCT6126D Super IO Configuration:** Set Super IO chip parameters (Press Enter for the sub-menu).
- **HW Monitor:** Monitor hardware status such as temperature and voltage (Press Enter for details).
- **S5 RTC Wake Settings:** Enable wake-up from S5 via RTC alarm (Press Enter to configure).
- **Network Stack Configuration:** Enable or disable UEFI network boot (Press Enter to access the sub-menu).
- **NVMe Configuration:** Configure NVMe device options (Press Enter to access further settings).

7.2.1 Onboard Service



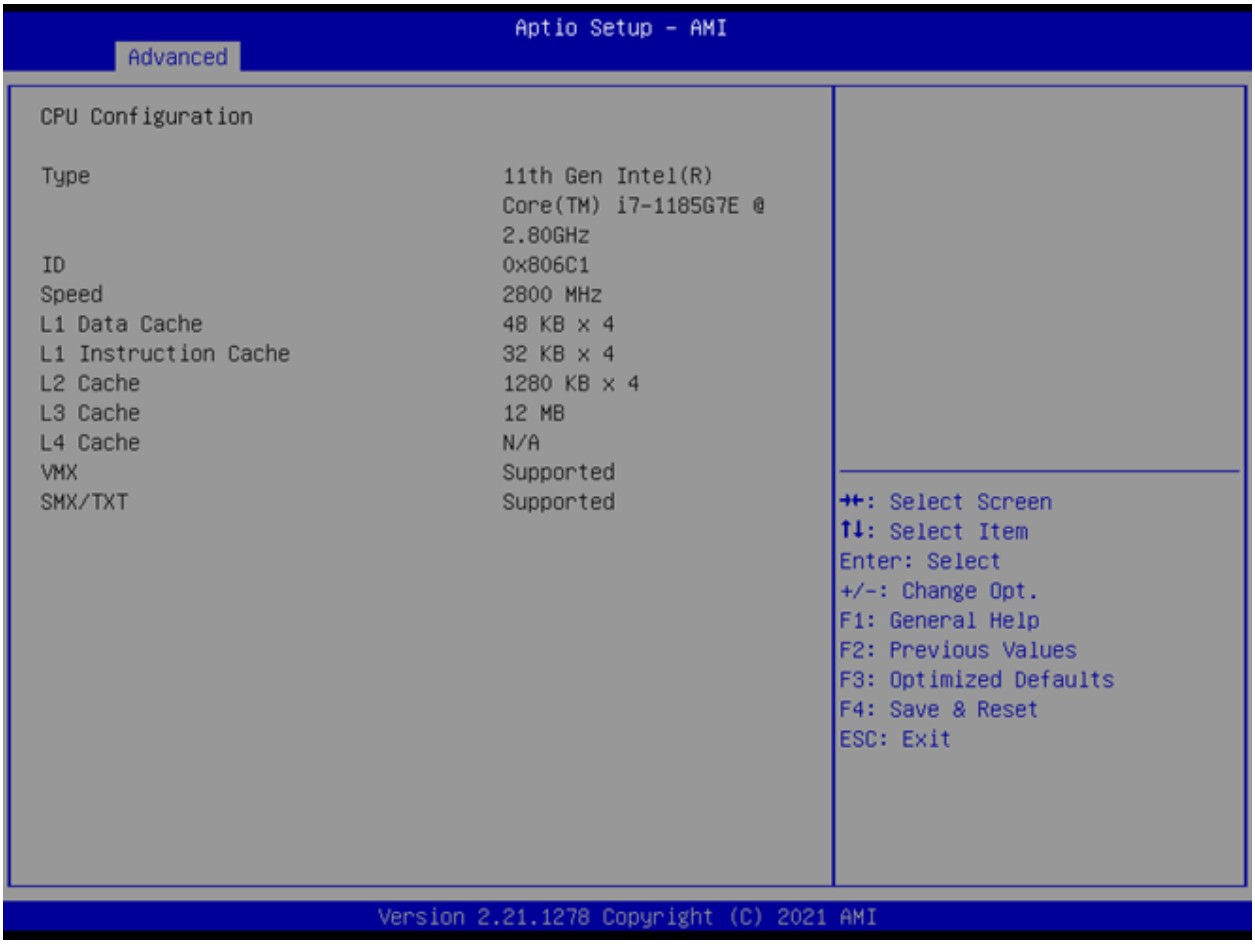
Onboard Service settings include:

- **Turbo Mode:**
  - *Default:* Enabled
  - *Options:* Enabled, Disabled
  - *Function:* Enables/disables processor Turbo Mode (requires EMTTM enabled).
- **State After G3:**

  - *Default:* S5 State
  - *Options:* S0 State, S5 State
  - *Function:* Determines the state when power is re-applied after a power failure.
- **DVMT Pre-Allocated:**
  - *Default:* 64M
  - *Options:* 64M, 32M/F7, 36M, 40M, etc.
  - *Function:* Sets the fixed graphics memory size for the internal graphics device.
- **DVMT Total Gfx Mem:**
  - *Default:* 256M
  - *Options:* 128M, 256M, MAX
  - *Function:* Sets the total graphics memory allocation.
- **Wake on LAN Enable:**
  - *Default:* Enabled
  - *Options:* Enabled, Disabled
  - *Function:* Enables/disables LAN wake-up.
- **HD Audio:**
  - *Default:* Enabled
  - *Options:* Enabled, Disabled
  - *Function:* Controls detection of the HD-Audio device.
- **Intel CSME Temporary Disable:**
  - *Default:* Disabled
  - *Options:* Enabled, Disabled
  - *Function:* Temporarily disables Intel CSME for ME firmware updates (disabled after the first reboot).
- **LVDS Interface Type:**
  - *Default:* Disabled
  - *Options:* 8 bit–VESA Single Channel, Dual Channel, etc.
  - *Function:* Sets the LVDS connectivity type.
- **LVDS Panel Type:**
  - *Default:* 1920x1080 LVDS
  - *Options:* 1024x768 LVDS, 1366x768 LVDS, etc.
  - *Function:* Selects the LVDS panel for the internal graphics device.
- **TPM Device Selection:**
  - *Default:* dTPM
  - *Options:* PTT, dTPM
  - *Function:* Selects the TPM device (switching will clear existing data).
- **G-Sensor Enable/Disable:**
  - *Default:* Disabled
  - *Options:* Enabled, Disabled

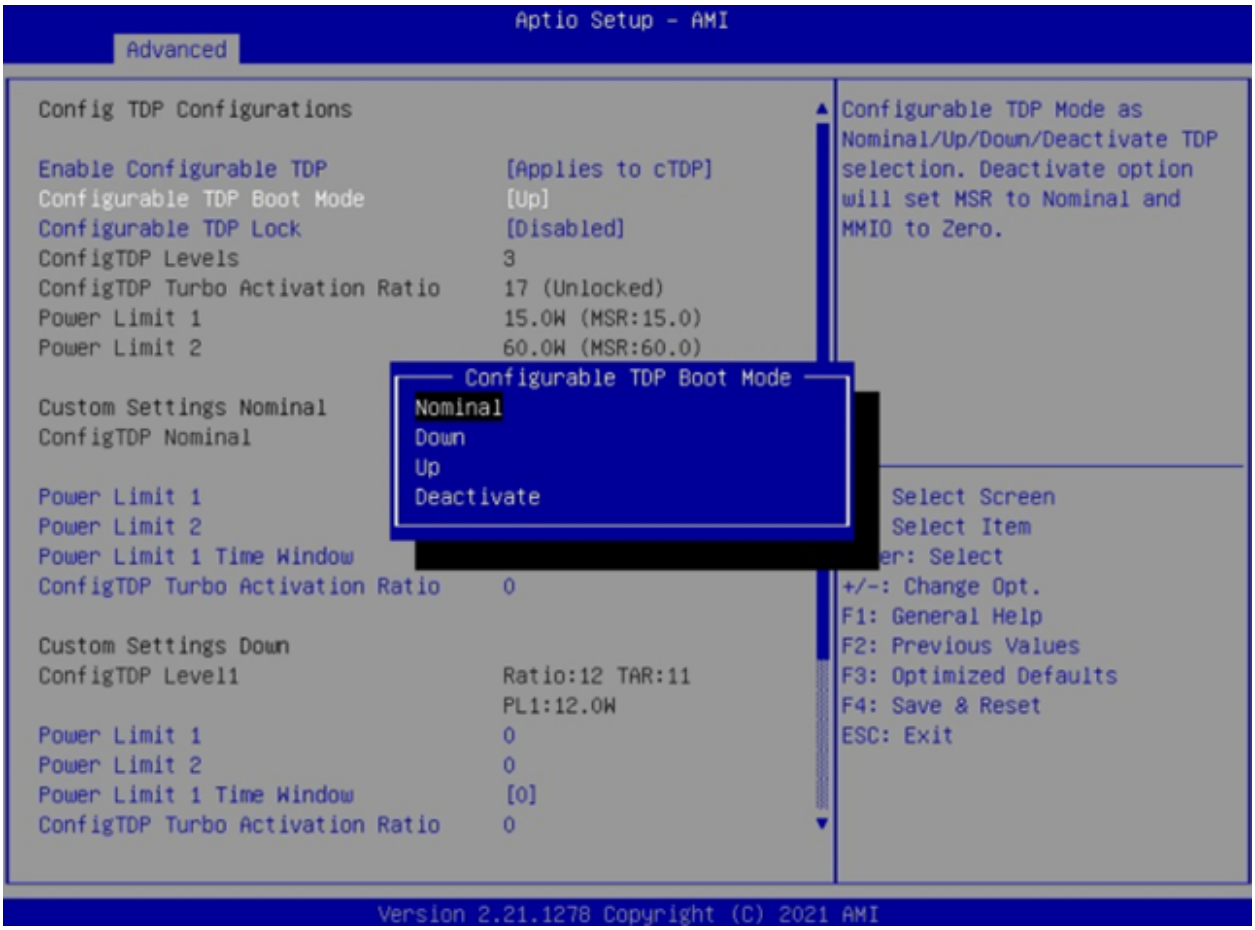
– *Function:* Controls the MS-26CAD-T10 G-Sensor (enabling reserves 2 DIO pins).

7.3 CPU Configuration



This section displays processor details and settings:

- **Processor Type:** Displays the installed CPU brand string.
- **Processor ID:** Shows the CPU signature.
- **Clock Speed:** Indicates the current CPU speed.
- **L1 Data Cache:** Displays L1 data cache size.
- **L1 Instruction Cache:** Displays L1 instruction cache size.
- **L2 Cache:** Displays L2 cache size.
- **L3 Cache:** Displays L3 cache size.
- **L4 Cache:** Displays L4 cache size.
- **VMX:** Indicates if Virtual Machine Extensions are supported.
- **SMX/TXT:** Indicates if SMX/TXT is supported.



7.4 Power & Performance

Adjust power settings:

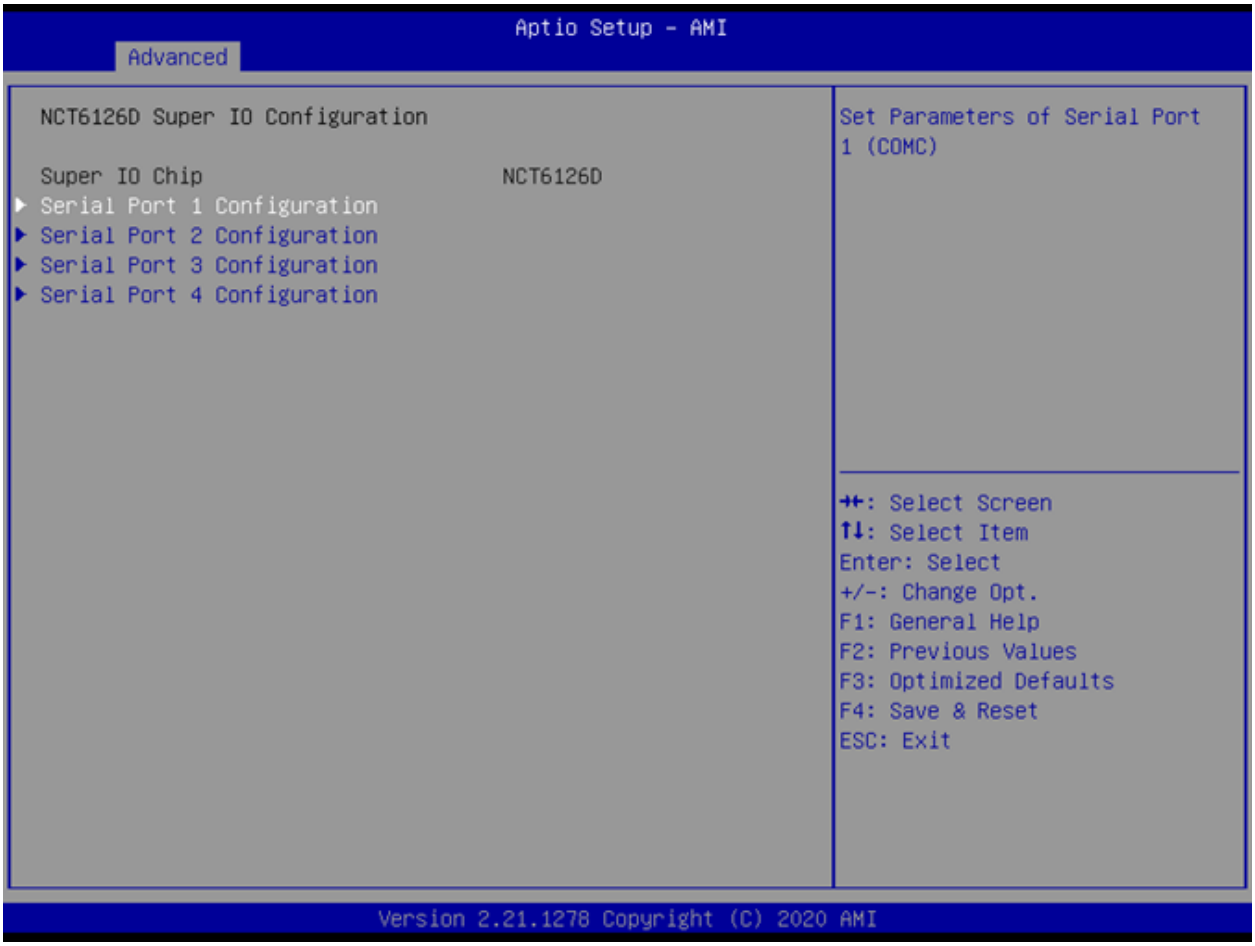
- **Configurable TDP Boot Mode:**
  - *Default:* Nominal
  - *Options:* Nominal, Down, Up, Deactive
  - *Function:*
    - **Nominal:** Sets TDP to 28W
    - **Down:** Sets TDP to 12W
    - **Up:** Sets TDP to 15W

7.5 Trusted Computing

Manage security features:

- **Firmware Version:** Displays the TPM module version.
- **Vendor:** Displays the TPM module vendor name.
- **Security Device Support:**
  - *Default:* Enabled
  - *Options:* Enabled, Disabled
  - *Function:* Enables/disables BIOS support for the security device.
- **Pending Operation:**
  - *Default:* None
  - *Options:* None, TPM Clear
  - *Function:* Schedules an operation for the security device (system will reboot to apply changes).

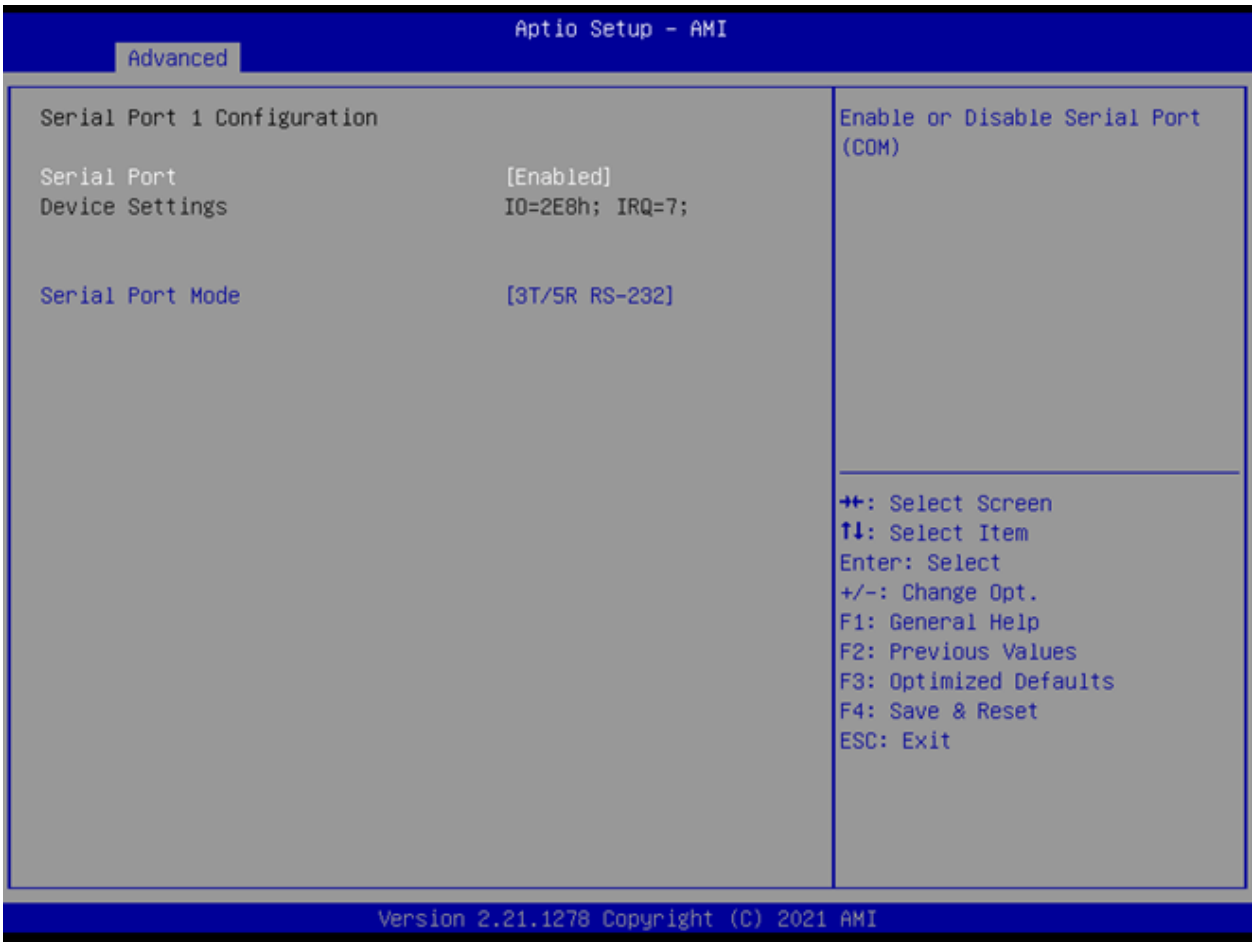
7.6 NCT6126D Super IO Configuration



Access configuration for system I/O controllers via the following sub-menus:

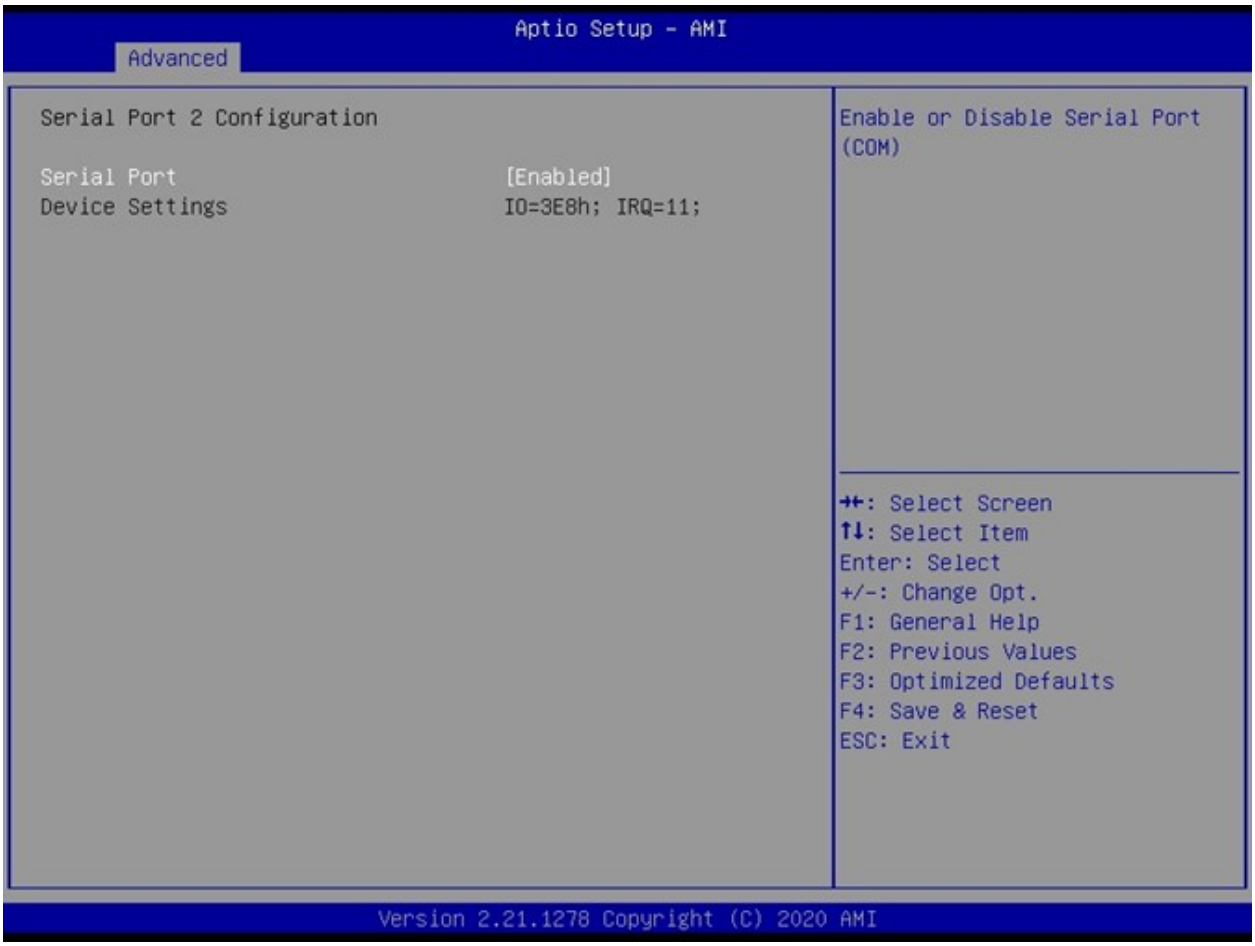
- **Serial Port 1 Configuration (COMC)**
- **Serial Port 2 Configuration (COMD)**
- **Serial Port 3 Configuration (COME)**
- **Serial Port 4 Configuration (COMA)**

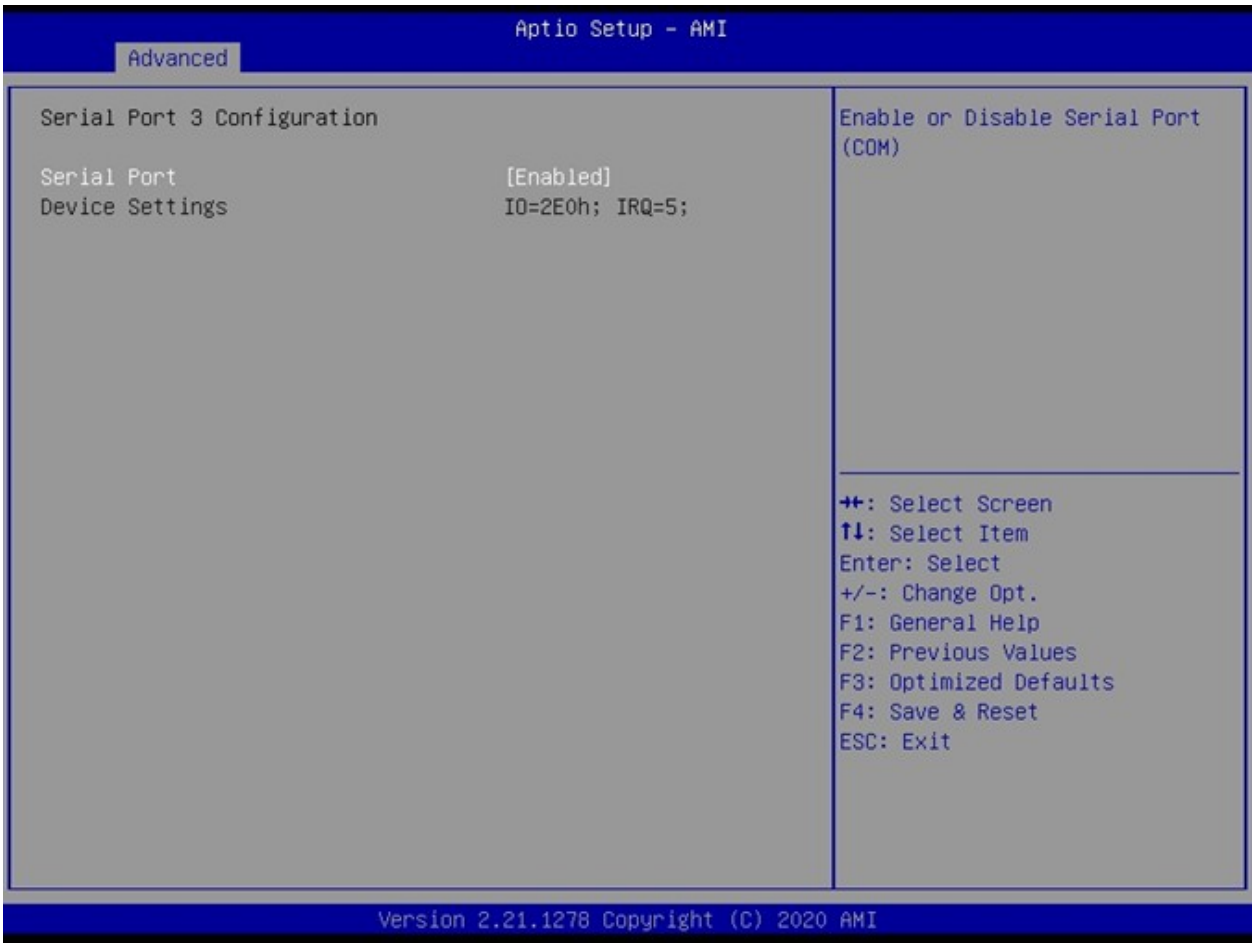
7.6.1 Serial Port 1 Configuration

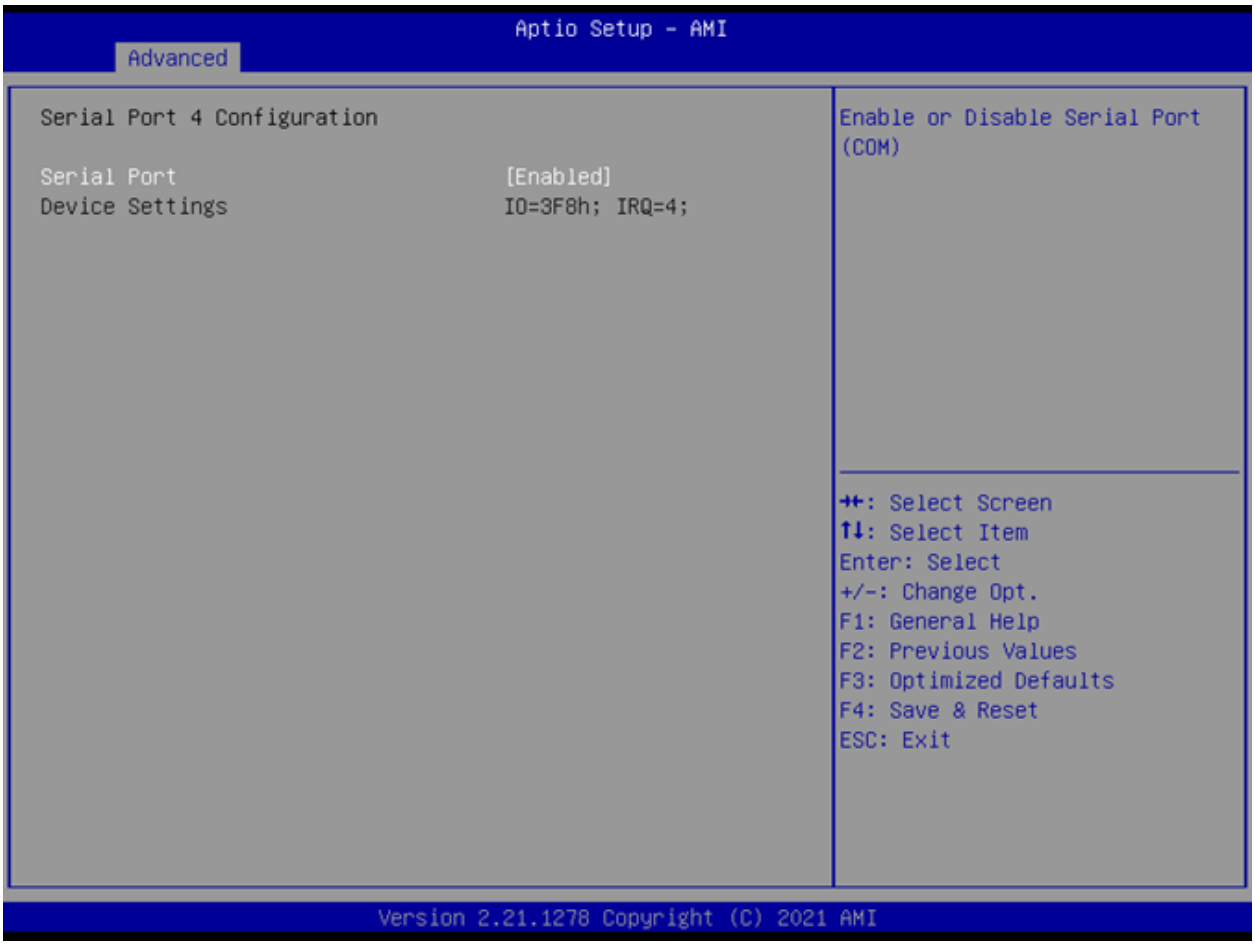


- **Serial Port:**
  - *Default:* Enabled
  - *Options:* Enabled, Disabled
  - *Function:* Enables/disables Serial Port (COM1).
- **Device Settings:** Displays the Super IO COM1 address and IRQ (non-selectable).
- **Mode Configuration:**
  - *Default:* 3T/5R RS232
  - *Options:* 1T/1R RS422; 3T/5R RS232; 1T/1R RS485 TX ENABLE Low Active; 1T/1R RS422 with termination resistor; 1T/1R RS485 with termination resistor TX ENABLE Low Active; Disabled

7.6.2 Serial Port 2, 3, & 4 Configuration



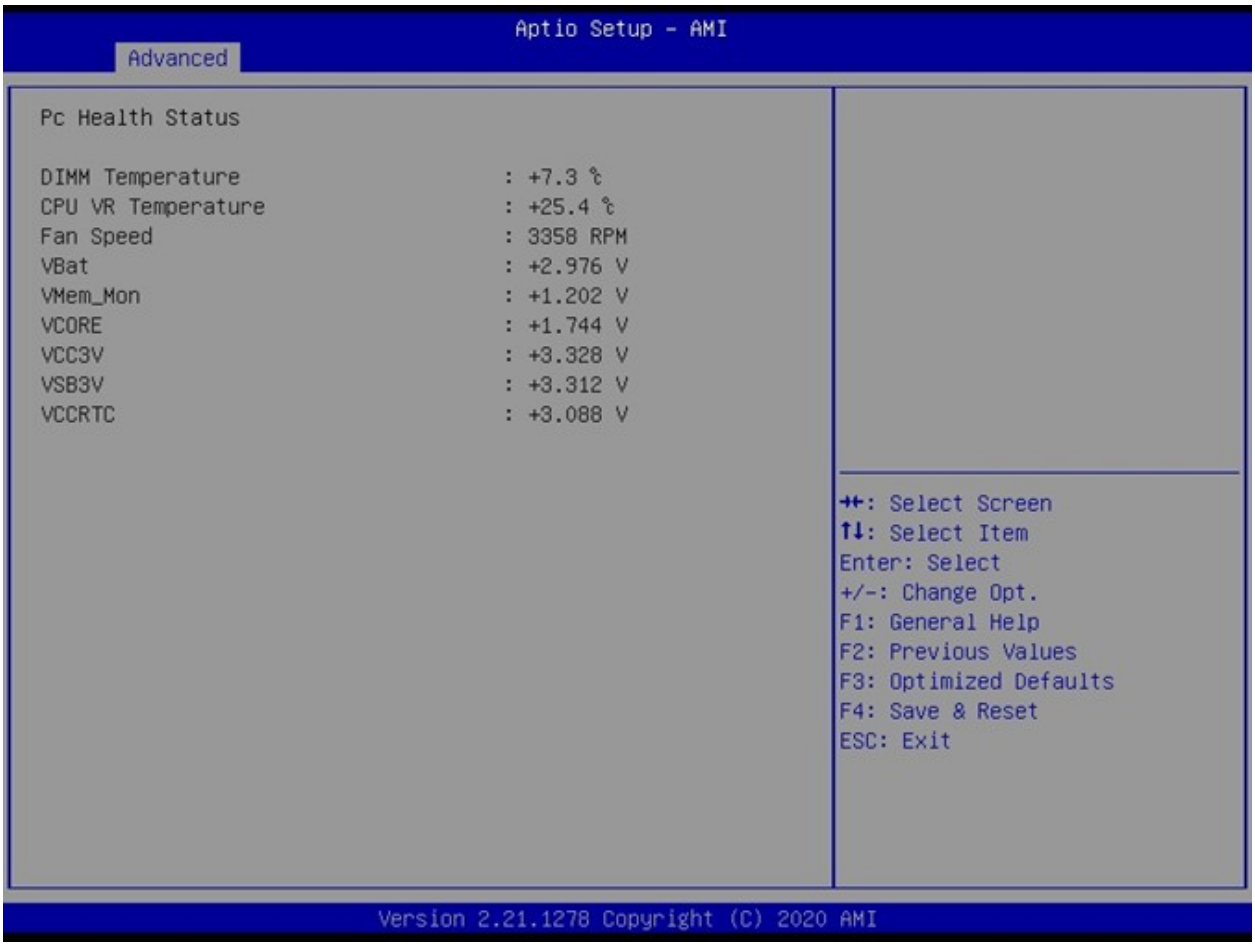

Aptio Setup – AMI
Advanced
Serial Port 3 Configuration
Serial Port [Enabled]
Device Settings IO=2E0h; IRQ=5;
Enable or Disable Serial Port (COM)
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Reset
ESC: Exit
Version 2.21.1278 Copyright (C) 2020 AMI



For each Serial Port (COM2, COM3, COM4):

- **Serial Port:**
  - *Default:* Enabled
  - *Options:* Enabled, Disabled
  - *Function:* Enables/disables the respective Serial Port.
- **Device Settings:** Displays the Super IO address and IRQ (non-selectable).

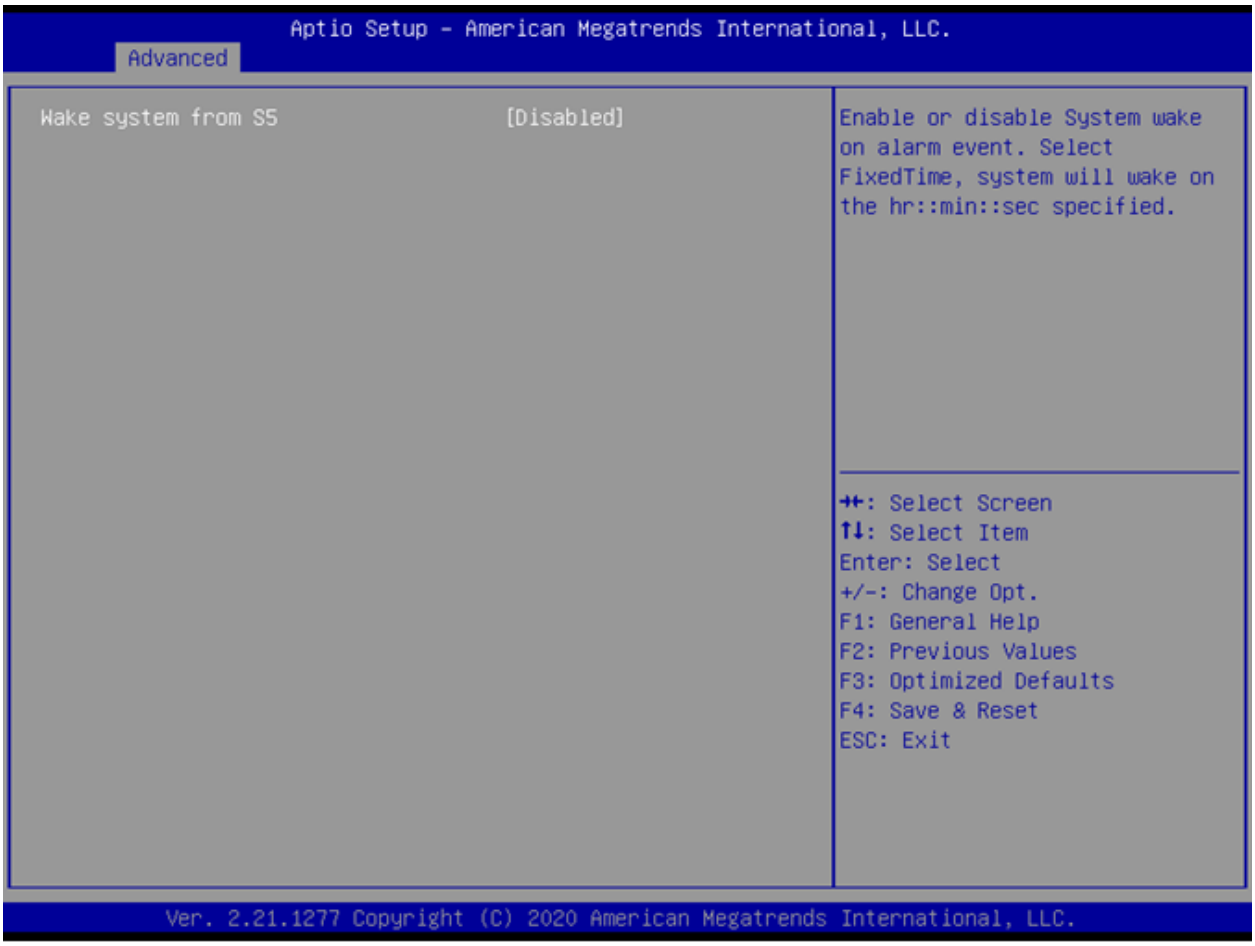
7.7 Hardware Monitor



Monitor system parameters:

- **DIMM Temperature:** 70 to –40
- **CPU VR Temperature:** 70 to –40
- **Fan Speed:** Variable; failed fan speed = 0 RPM (no high RPM limit)
- **VBat:** 2.0 to 3.65V
- **VMem_Mon:** 1.15 to 1.25V
- **VCORE:** 0 to 2V
- **VCC3V:** 3.13 to 3.65V
- **VSB3V:** 3.13 to 3.65V
- **VCCRTC:** 2.0 to 3.2V

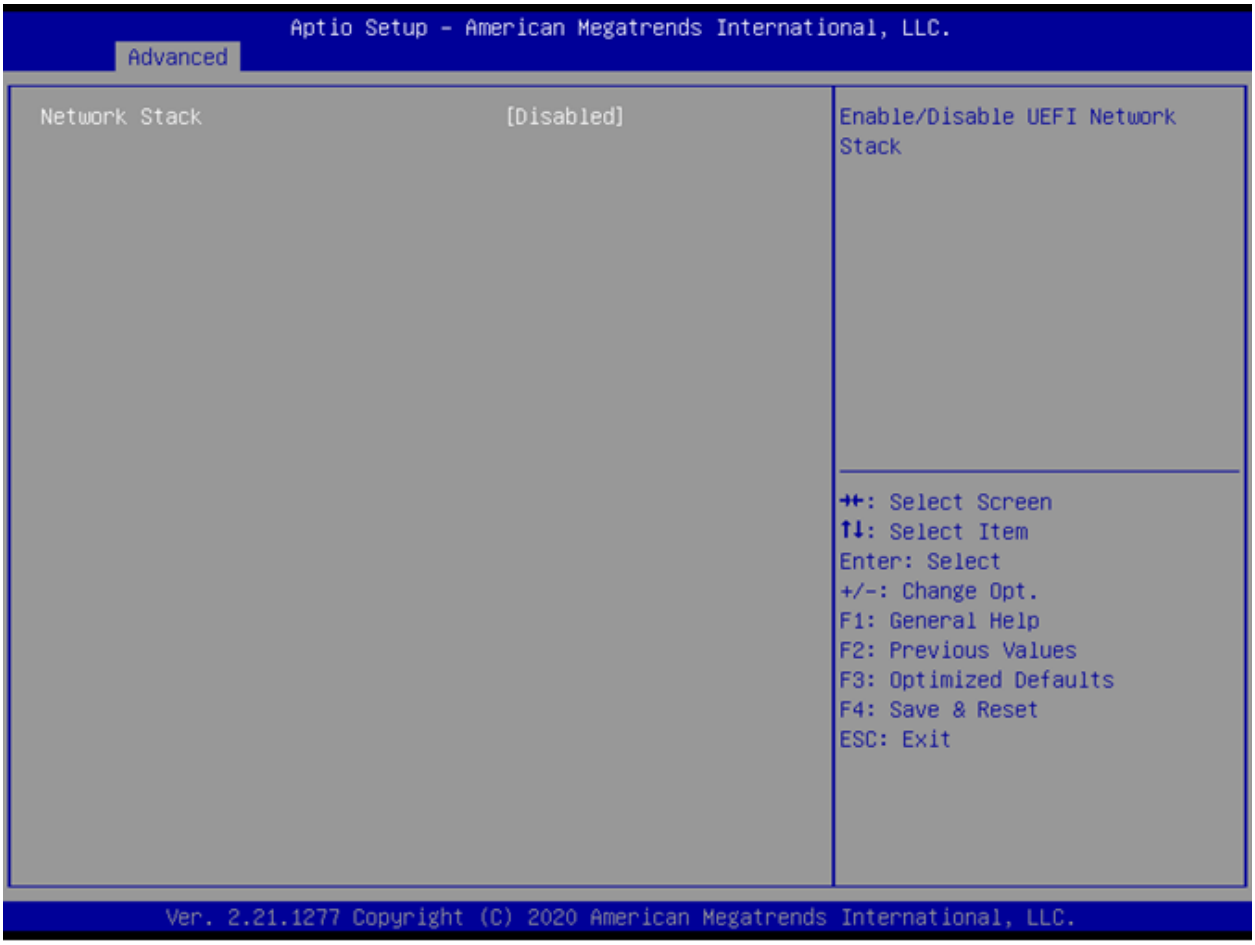
7.8 RTC Wake Settings



Configure the RTC wake-up feature:

- **Wake system from S5:**
  - *Default:* Disabled
  - *Options:* Disabled, Fixed Time
  - *Function:* Enables system wake-up via RTC alarm; select Fixed Time to schedule wake-up.
- **Wake up Hour:**
  - *Default:* 0
  - *Range:* 0–23 (e.g., 3 for 3 AM, 15 for 3 PM)
- **Wake up Minute:**
  - *Default:* 0
  - *Range:* 0–59
- **Wake up Second:**
  - *Default:* 0
  - *Range:* 0–59

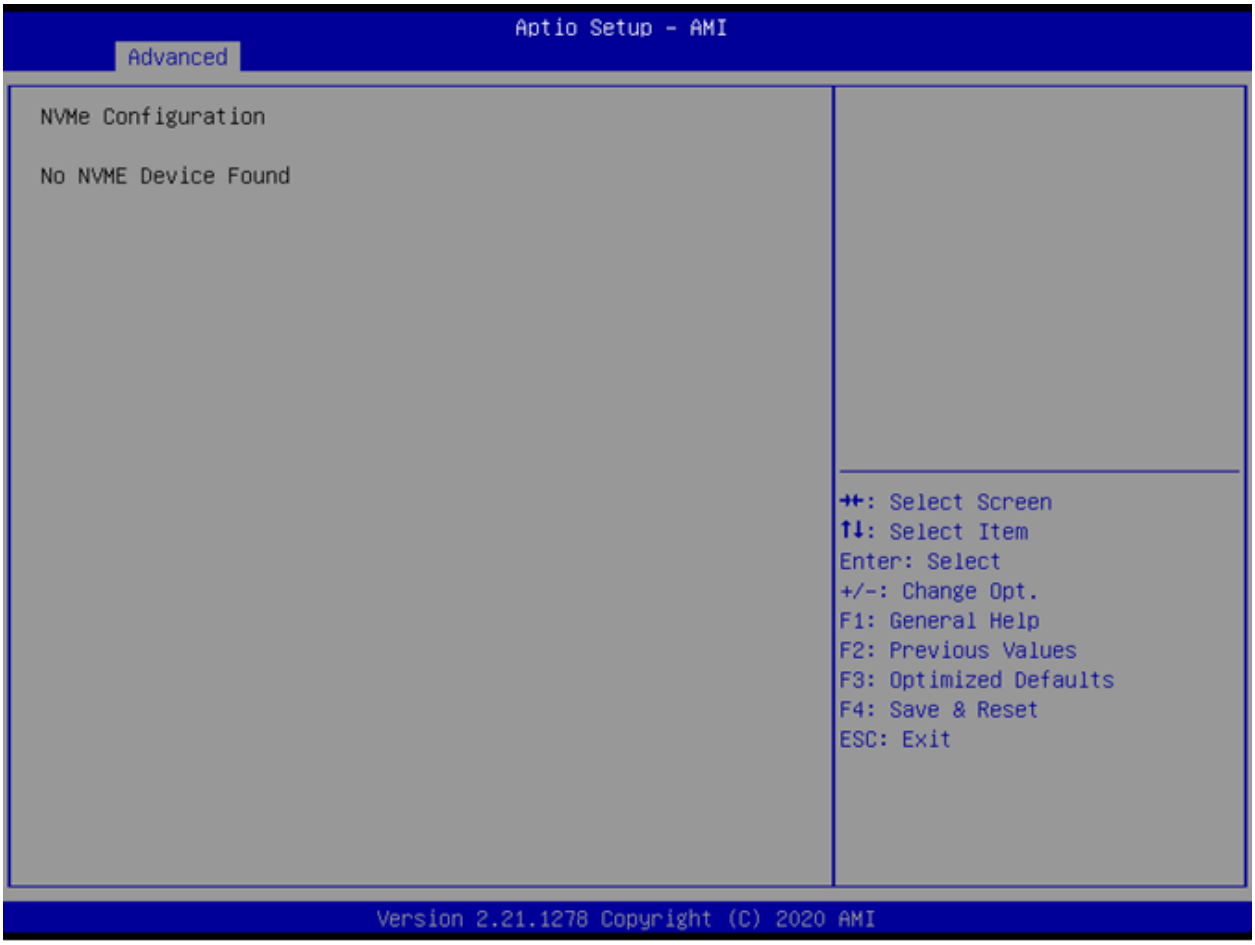
7.9 Network Stack Configuration



Configure network boot settings:

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

7.10 NVMe Configuration



Press Enter to access NVMe device options and configure settings.

7.11 Event Logs

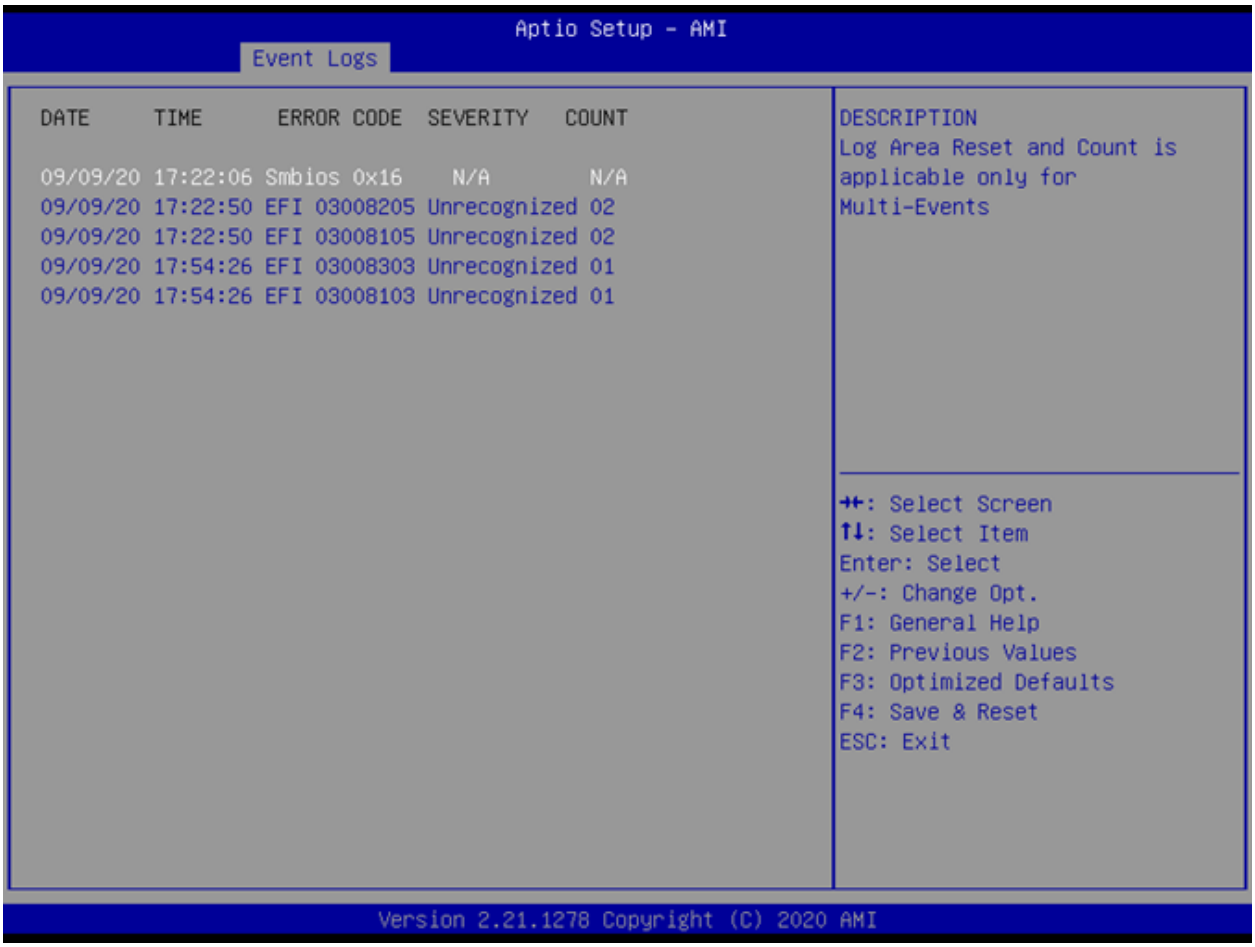
Manage SMBIOS event logs:

- **Change SMBIOS Event Log Settings:** Press Enter to modify settings.
- **View SMBIOS Event Log:** Press Enter to view log entries.

7.11.1 Enabling/Disabling Options

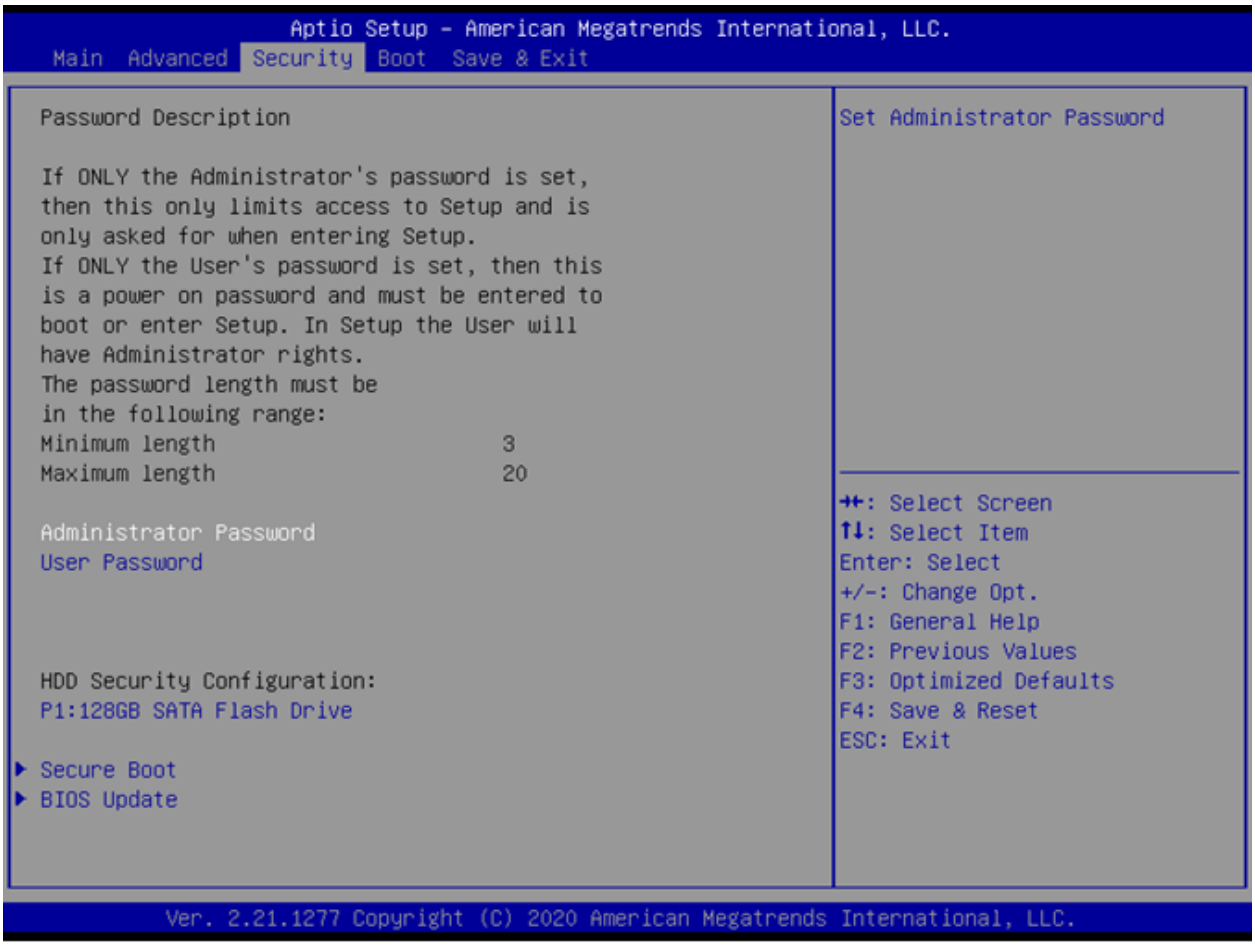
- **SMBIOS Event Log:**
  - *Default:* Enabled
  - *Options:* Enabled, Disabled
- **Erase Event Log:**
  - *Default:* No
  - *Options:* No, Yes (Next Reset), Yes (Every Reset)
- **When Log is Full:**
  - *Default:* Do Nothing
  - *Options:* Do Nothing, Erase Immediately

7.11.2 View SMBIOS Event Log



Displays entries with Date, Time, Error Code, Severity, and Count (formatted as MM/DD/YY HH:MM:SS).

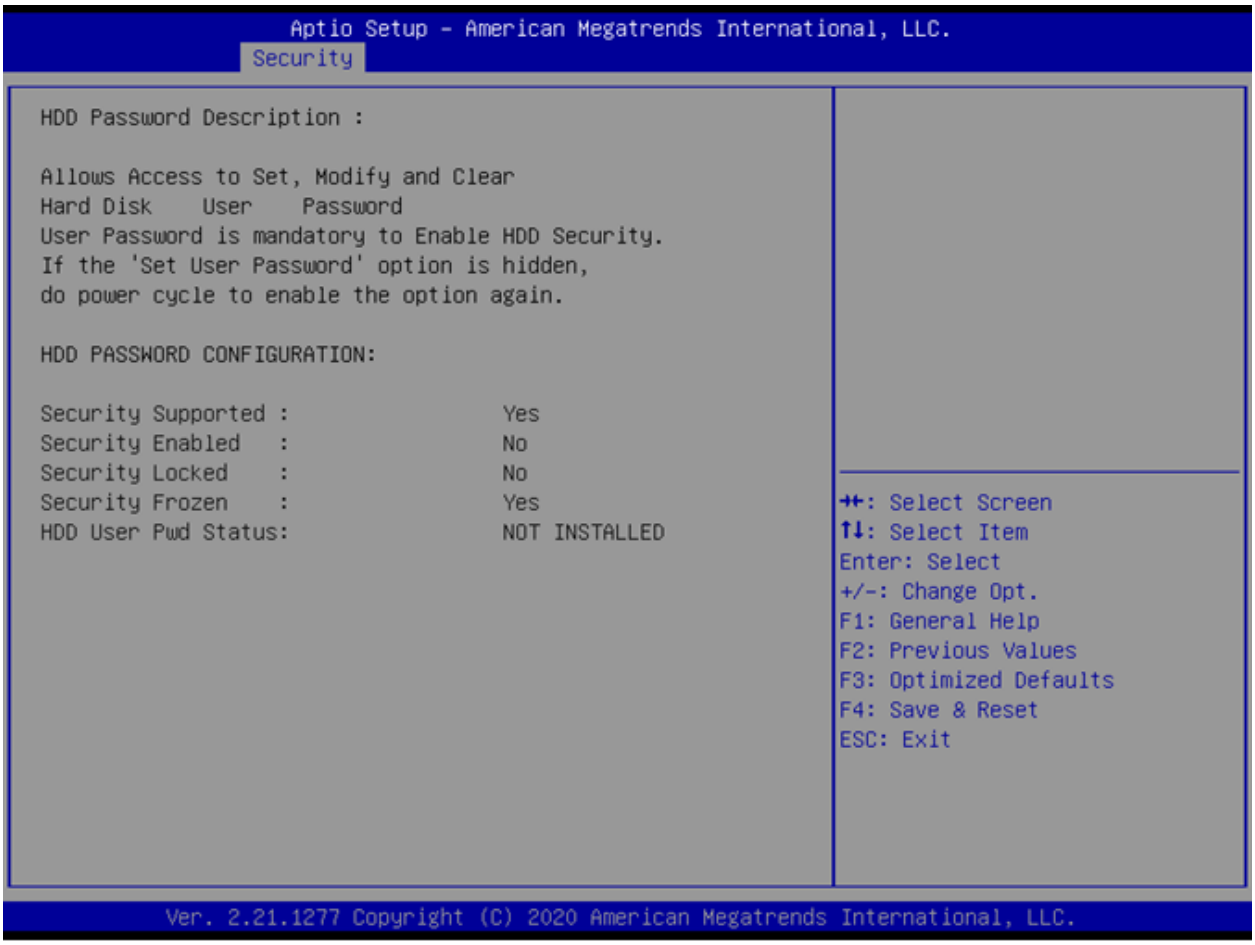
7.12 Security Page



The Security Page allows you to configure password protection and other security features:

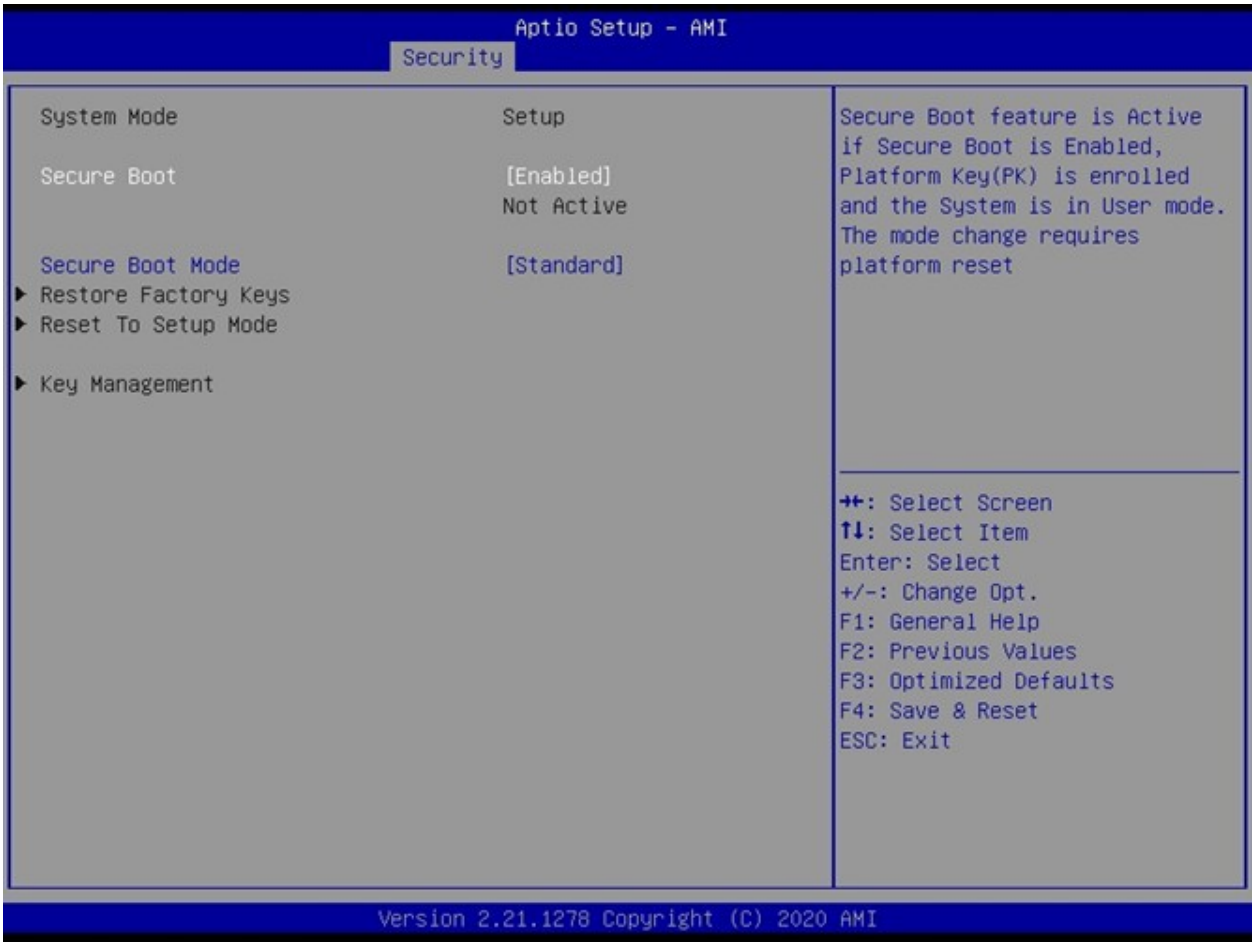
- **Administrator Password:** Set or modify the administrator password.
- **User Password:** Set or modify the user password.
- **HDD Security Drive:** Configure security settings for the selected hard drive.
- **Secure Boot:** Configure Secure Boot options.
- **BIOS Update:** Enable BIOS update support.

7.12.1 HDD Security



- **Set User Password:** Set the HDD user password.
  Note: It is advisable to power cycle the system after setting or removing HDD passwords.

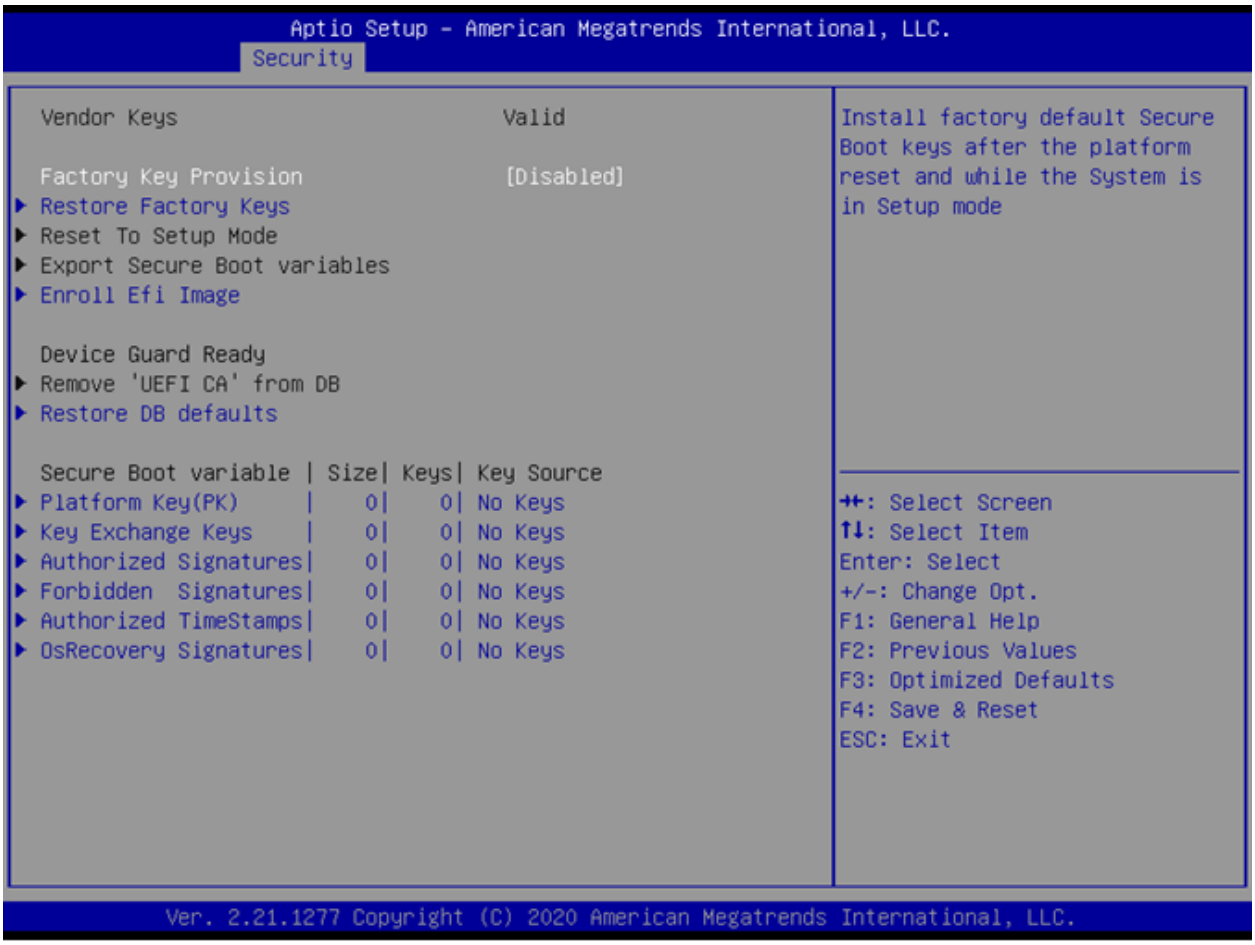
7.12.2 Secure Boot



Secure Boot options include:

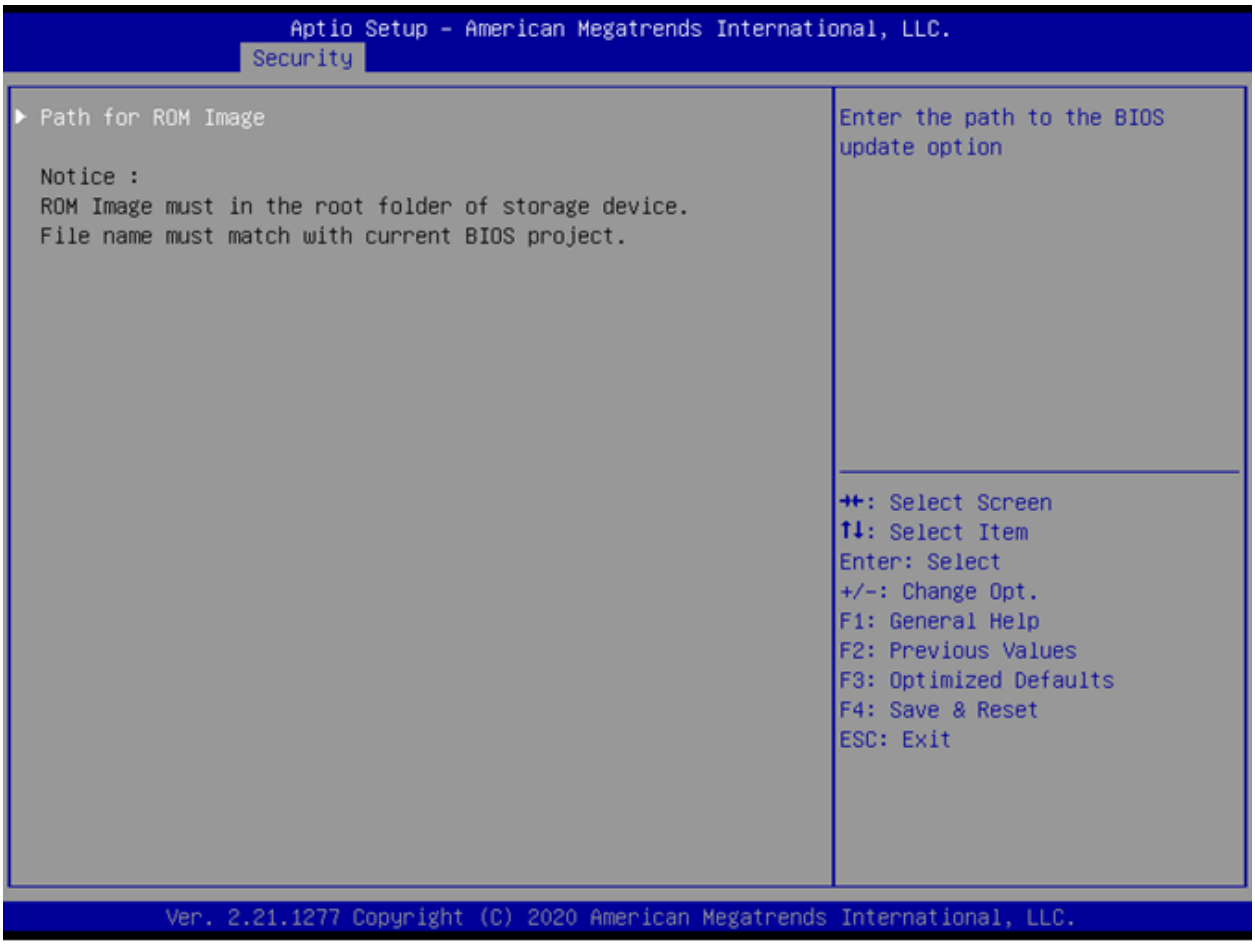
- **Secure Boot:**
  - *Default:* Enabled
  - *Options:* Enabled, Disabled
  - *Function:* Activates Secure Boot when enabled, provided the platform key is enrolled.
- **Secure Boot Mode:**
  - *Default:* Standard
  - *Options:* Standard, Custom
  - *Function:* In Custom mode, Secure Boot variables can be configured manually.
- **Restore Factory Keys:** Restores default Secure Boot keys.
- **Reset to Setup Mode:** Deletes all Secure Boot key databases from NVRAM.
- **Key Management:** Allows expert users to modify Secure Boot policy variables.

Key Management (Secure Boot Mode set to Custom)



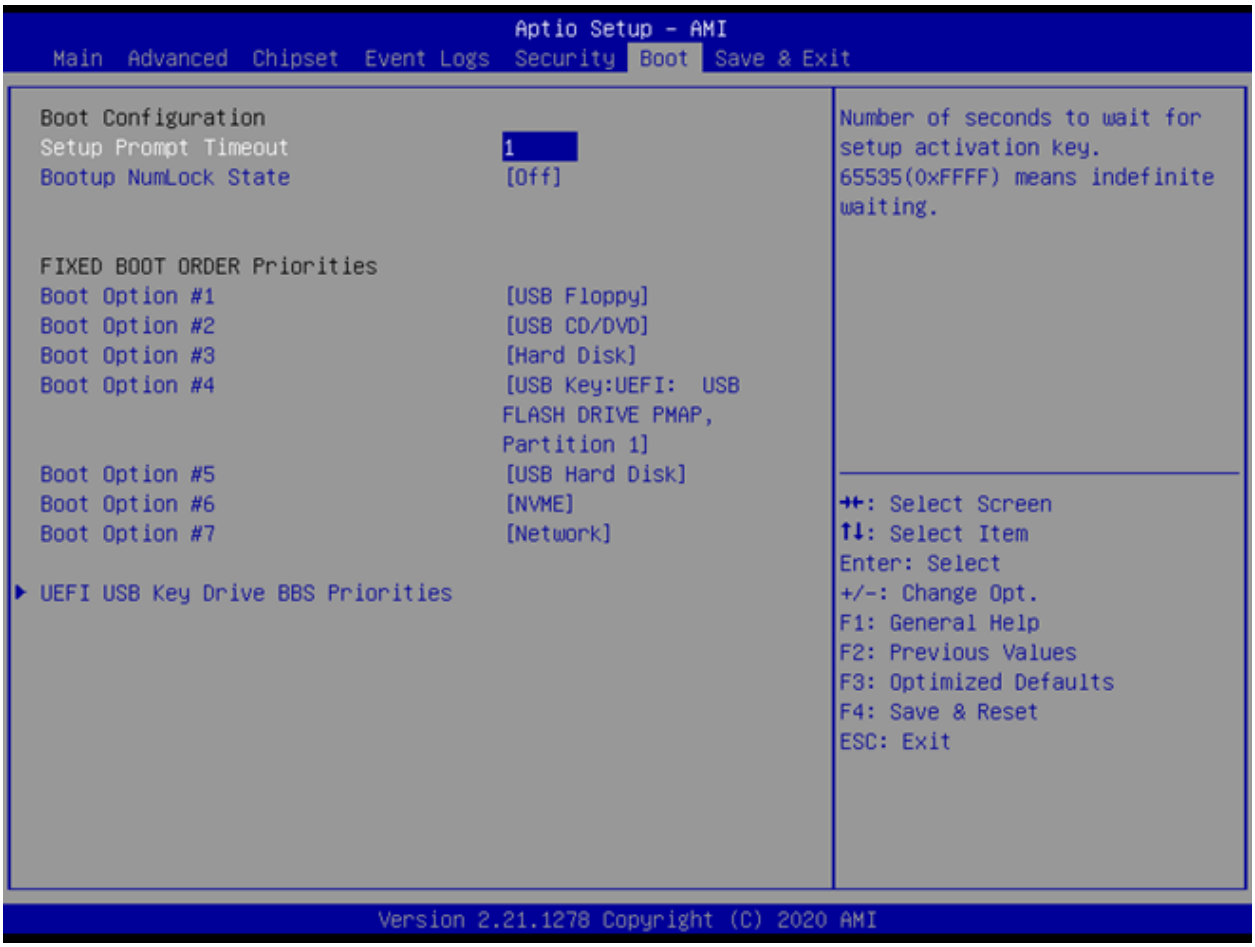
- **Factory Key Provision:**
  - *Default:* Disabled
  - *Options:* Enabled, Disabled
  - *Function:* Installs factory default keys after a platform reset when in Setup mode.
- **Restore Factory Keys:** Forces system into User Mode to install factory keys.
- **Reset to Setup Mode:** Deletes all Secure Boot key databases from NVRAM.
- **Export Secure Boot Variables:** Exports Secure Boot variables to a file.
- **Enroll EFI Image:** Enrolls a PE image's SHA256 hash certificate into the Authorized Signature Database.
- **Remove 'UEFI CA' from DB:** Removes the Microsoft UEFI CA certificate from the Authorized Signature database.
- **Restore DB Defaults:** Restores the Secure Boot database to its factory defaults.
- **Platform Key (PK):** Allows certificate enrollment for the Platform Key.
- **Key Exchange Keys:** Enables certificate enrollment for Key Exchange Keys.
- **Authorized Signatures:** Manage authorized public key certificates.
- **Forbidden Signatures:** Manage forbidden signatures for Secure Boot.
- **Authorized TimeStamps:** Manage timestamps for authorized signatures.
- **OS Recovery Signatures:** Manage recovery signatures for the operating system.

7.12.3 BIOS Update



- **BIOS Update:**
  - *Default:* N/A
  - *Options:* N/A
  - *Function:* Enter the path for the Secure flash option to update BIOS.

7.13 Boot Page



Configure boot settings:

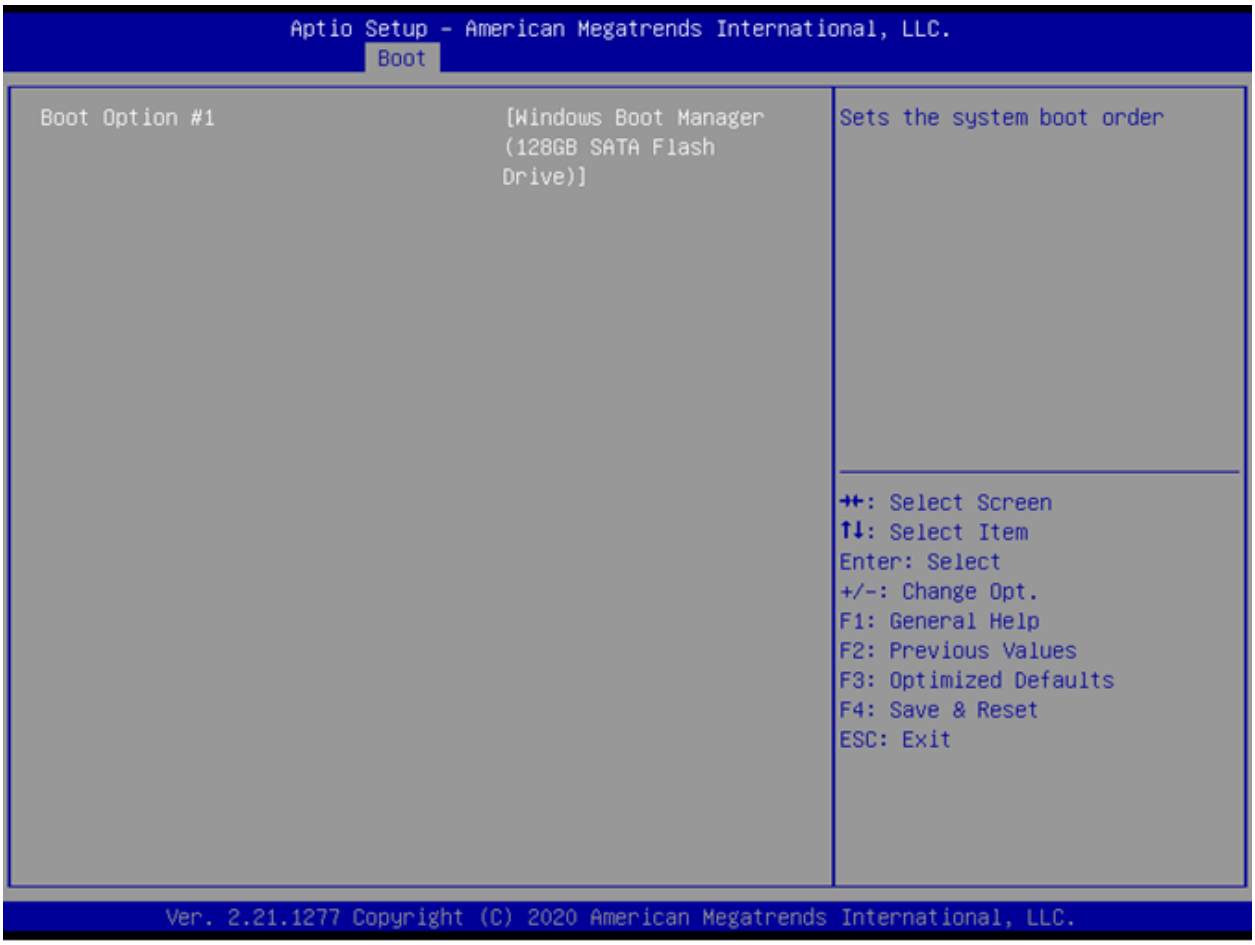
- **Setup Prompt Timeout:**
  - *Default:* 1 second
  - *Range:* 1–65535 (65535 indicates indefinite waiting)
- **Bootup NumLock State:**
  - *Default:* Off
  - *Options:* On, Off
- **Boot Options:**
  - **Boot Option #1:** Default is USB Floppy
  - **Boot Option #2:** Default is USB CD/DVD
  - **Boot Option #3:** Default is Hard Disk
  - **Boot Option #4:** Default is USB Key
  - **Boot Option #5:** Default is USB Hard Disk
  - **Boot Option #6:** Default is NVME
  - **Boot Option #7:** Default is Network

  - *Options for each:* USB Floppy, CD/DVD, USB CD/DVD, Hard Disk, USB Key, USB Hard Disk, NVME, Network, Disabled

For UEFI boot device priorities:

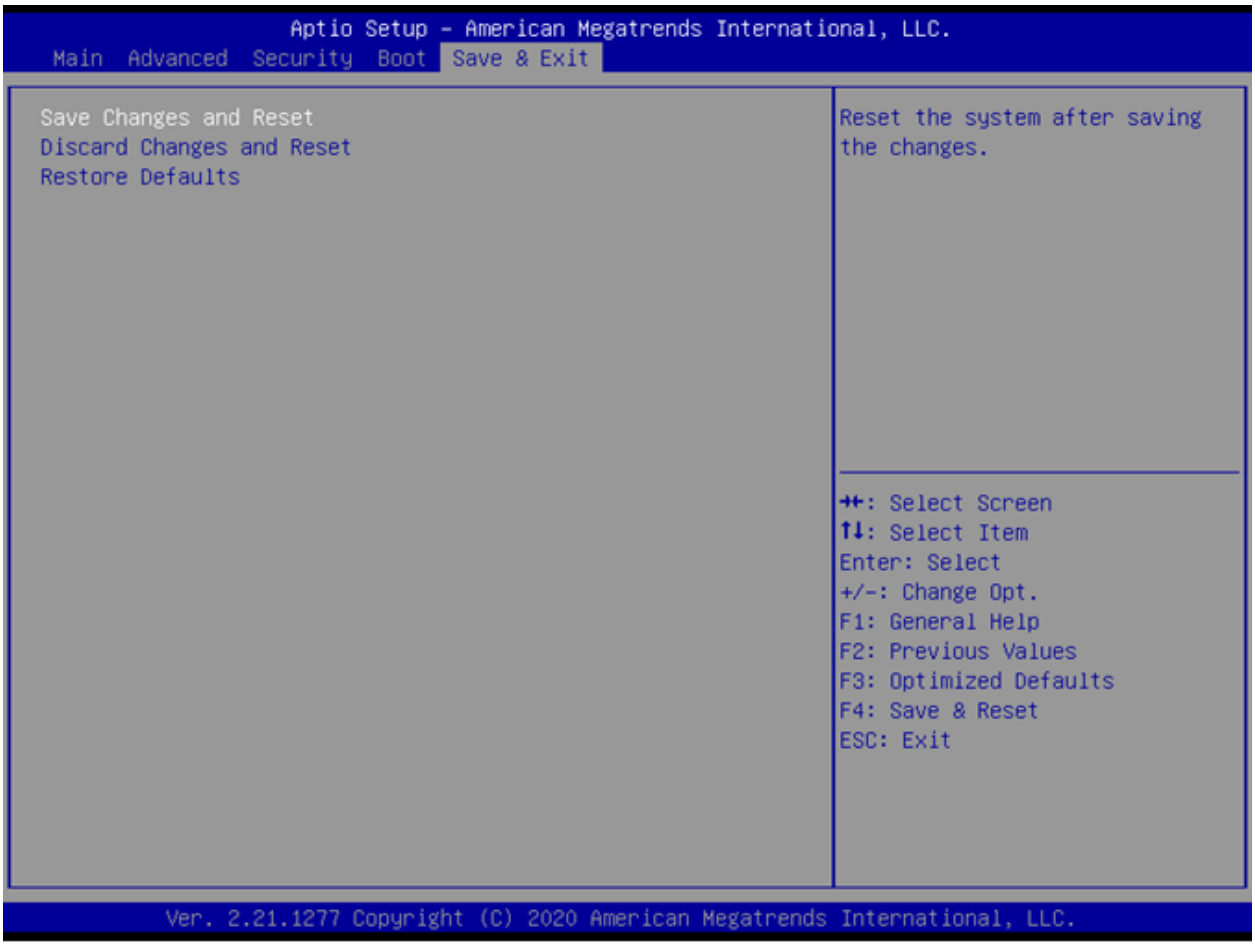
- **(UEFI) USB Floppy Drive BBS Priorities:** Default is N/A
- **(UEFI) USB CDROM/DVD Drive BBS Priorities:** Default is N/A
- **(UEFI) Hard Disk Drive BBS Priorities:** Default is N/A
- **(UEFI) USB KEY Drive BBS Priorities:** Default is N/A
- **(UEFI) USB Hard Disk Drive BBS Priorities:** Default is N/A
- **(UEFI) NVME Drive BBS Priorities:** Default is N/A
- **(UEFI) NETWORK Drive BBS Priorities:** Default is N/A

Additionally, for a specific boot device type:



- **Boot Option #1 (of a listed type):**
  - *Default:* N/A
  - *Options:* Boot Device Name 1 of this type, or Disabled

7.14 Save & Exit Page



Finalize your BIOS configuration:

- **Save Changes and Reset:** Saves changes and restarts the system.
- **Discard Changes and Reset:** Restarts without saving modifications.
- **Restore Defaults:** Loads factory default settings for all BIOS options.