RSAVP

Version:
v1.0.0

Date:
12.03.2026

Contents

1 Copyright

2 Regulatory Compliances

This documentation is preliminary and subject to change

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)

- applicable standards are pending

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

- applicable standards are pending

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

- Exemptions pending

2.2 FCC PART 15 VERIFICATION STATEMENT

WARNING

This equipment has been tested and found to comply with the limits for a Class (pending) 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 ICES-003 ISSUE 7 VERIFICATION STATEMENT

CAN ICES3(A)/NMB3(A)

This device complies with CAN ICES-003 Issue 7 Class (pending). 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 security information and recommendations to help you configure your Welotec Substation Computer for optimal security in your deployment.

3.1 Intended Use

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

The Computer is designed for being used as a platform for deploying industry-specific applications including but not limited to HMI, Engineering Workstations, Substation Gateways and SCADA systems. Its primary function is to act as a bare-metal server or virtualization host system to provide the infrastructure application deplyoment.

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

3.1.1 Physical Security and Installation Environment

- Enclosure: The Computer must be permanently installed within a secure and controlled enclosure such as a 19” rack which protects against external damage and unauthorized access.
- Controlled Access: Access the installation location must be restricted to authorized personnel only. Physical security measures (e.g., key locks, access control systems) are mandatory.
- Environmental Conditions:
  - Temperature: The Computer must operate within the specified ambient temperature and humidity range as outlined in the technical specifications. Adequate ventilation or active cooling within the enclosure must ensure these limits are not exceeded.
  - Vibration and Shock: The Computer must be mounted securely within the enclosure to minimize exposure to excessive vibrations and mechanical shock, adhering to the manufacturer’s specifications.
  - Cleanliness: The inside of the enclosure 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 relevant 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 Computer must be connected to a dedicated stable and filtered power supply within the specified voltage range. To ensure operational reliability and meet relevant EMC requirements, the power source must provide adequate filtering against surges, transients, electrical fast transients (EFTs), and conducted RF noise common in rolling stock environments. An Uninterruptible Power Supply (UPS) is highly recommended to protect further against power fluctuations and outages.
- Wiring: All wiring connecting to the Computer must comply with applicable 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.

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 Computer 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 Computer 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 Computer'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.

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

- Network Isolation: The Computer and the OT network must be logically and, where feasible, physically separated from the IT network and the internet. This typically involves dedicated industrial network switches, firewalls, and separate cabling.
- Defense in Depth: A multi-layered security approach ("Defense in Depth") must be implemented for the entire system. 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 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 Computer (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 Computer 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 Computer that deviates from the conditions described including but not limited to:

- Operation outside the specified environmental limits.
- Operation outside of a secure enclosure and controlled environment
- Installation or maintenance by unqualified personnel.
- 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). is considered non-intended use and may result in:
- Damage to the Computer or the system.
- 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
LAN1 … n	Depending on configuration and SFP-type
LOM	Lights-Out-Management
USB1 … 5	
Console	Console Redirect
VGA	

Available services highly depend on Operating System type and version.

3.4 Security Reccomentations

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 to enalbe Secure Boot - please refer to "BIOS" section of the manual 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.

Standard Linux OS (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.

Other Operating Systems

Please refer to te documentation of the OS for further details

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 reccomended to:

- Change factory default passwords 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

3.5 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

4.1 General

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

1. This equipment is to be installed for operation in an environment with maximum ambient temperature below 40°C.
2. The openings on the enclosure are for air convection to protect the equipment from overheating. DO NOT COVER THE OPENINGS.
3. Carefully mount the equipment into the rack, in such manner, that it won't be hazardous due to uneven mechanical loading. Place this equipment on a stable surface when install. A drop or fall could cause injury.
4. Make sure the voltage of the power source is within the specification on the label when connecting the equipment to the power outlet. The current load and output power of loads shall be within the specification.
5. This equipment must be connected to reliable grounding before using. Pay special attention to power supplied other than direct connections, e.g. using of power strips.

4.2 Safety Guidelines

Follow these guidelines to ensure general safety:

1. Keep the chassis area clear and dust-free during and after installation.
2. Do not wear loose clothing or jewelry that could get caught in the chassis. Fasten your tie or scarf and roll up your sleeves.
3. Wear safety glasses if you are working under any conditions that might be hazardous to your eyes.
4. Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
5. Disconnect all power by turning off the power and unplugging the power cord before installing or removing a chassis or working near power supplies
6. Do not work alone if potentially hazardous conditions exist.
7. Never assume that power is disconnected from a circuit; always check the circuit.
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.

4.3 Lithium Battery Caution

1. **There is risk of explosion** if the battery is replaced by an incorrect type.
2. Dispose of used batteries according to the instructions.
3. Installation should be conducted only by a trained electrician or only by an electrically trained person who knows all installation procedures and device specifications which are to be applied.
4. Do not carry the handle of power supplies when moving to another place.
5. Please conform to your local laws and regulations regarding safe disposal of lithium battery.
6. Disposal of a battery into fire or a hot oven, or mechanically crushing or cutting of a battery can result in an explosion.
7. Leaving a battery in an extremely high temperature environment can result in an explosion or the leakage of flammable liquid or gas.
8. A battery subjected to extremely low air pressure may result in an explosion or the leakage of flammable liquid or gas.

4.4 Operating Safety

1. Electrical equipment generates heat. Ambient air temperature may not be adequate to cool equipment to acceptable operating temperatures without adequate circulation. Be sure that the room in which you choose to operate your system has adequate air circulation.
2. Ensure that the chassis cover is secure. The chassis design allows cooling air to circulate effectively. An open chassis permits air leaks, which may interrupt and redirect the flow of cooling air from internal components.
3. **Electrostatic discharge (ESD) can damage equipment** and impair electrical circuitry. ESD damage occurs when electronic components are improperly handled and can result in complete or intermittent failures. Be sure to follow ESD-prevention procedures when removing and replacing components to avoid these problems.
4. **Wear an ESD-preventive wrist strap**, ensuring that it makes good skin contact. If no wrist strap is available, ground yourself by touching the metal part of the chassis.
5. Periodically check the resistance value of the antistatic strap, which should be between 1 and 10 megohms (MΩ).

4.5 Mounting Installation Precautions

The following should be put into consideration for rack-mount or similar mounting installations:

1. **Do not install and/or operate this unit in any place that flammable objects are stored or used in.**
2. The installation of this product must be performed by trained specialists; otherwise, a non-specialist might create the risk of the system's falling to the ground or other damages.
3. Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.
4. Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of airflow required for safe operation of the equipment is not compromised.
5. Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
6. Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

7. Reliable Grounding - Reliable grounding of rack mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).
8. Suitable for installation in Information Technology Rooms in accordance with Article 645 of the National Electrical Code and NFPA 75.
9. Equipment is intended for installation in Restricted Access Location / Les matériels sont destinés à être installés dans des EMPLACEMENTS À ACCÈS RESTREINT.

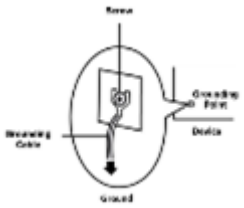
CAUTION: **Stability hazard** - The rack may tip over causing serious personal injury Before extending the rack to the installation position, read the installation instructions. Do not put any load on the slide-rail mounted equipment in the installation position. Do not leave the slide-rail mounted equipment in the installation position.

DANDER: **d'instabilité** - Le rack peut basculer et provoquer des blessures corporelles graves Avant d'étendre le rack en position d'installation, lire les instructions d'installation. Ne pas charger l'équipement monté sur rail de glissière en position d'installation. Ne pas laisser l'équipement monté sur rail de glissière en position d'installation.

4.6 Electrical Safety Instructions

Before turning on the device, ground the grounding cable of the equipment. Proper grounding (grounding) is very important to protect the equipment against the harmful effects of external noise and to reduce the risk of electrocution in the event of a lightning strike. To uninstall the equipment, disconnect the ground wire after turning off the power. A ground wire is required and the part connecting **the conductor must be greater than 4 mm2 or 10 AWG.**

1. **This equipment must be grounded.** The power cord for product should be connected to a socket-outlet with earthing connection.
2. Suitable for installation in Information Technology Rooms in accordance with Article 645 of the National Electrical Code and NFPA 75.
3. The machine can only be used in a restricted access location and has installation instructions by a skilled person.



5 Product Specifications

5.1 Overview

This high-performance server platform is designed for demanding enterprise and industrial applications. Featuring the latest Intel® Xeon®6 Processor with advanced security acceleration and robust networking capabilities, it ensures reliability, scalability, and efficiency. The system supports up to 512GB DDR5 ECC memory, multiple PCIe Gen5 expansion slots, and flexible storage options including NVMe and M.2. Built for harsh environments, it offers wide temperature tolerance, redundant power supplies, and compliance with stringent safety and EMC standards.

5.2 Key Highlights

- Processor: Intel® Xeon®6 6710E, 64 cores / 64 threads, 2.4GHz
- Memory: DDR5 ECC, up to 512GB across 8 DIMM slots
- Networking: Dual 1GbE and dual 10GbE ports with SR-IOV support
- Storage: 4x U.2 NVMe hot-swappable bays + 1x M.2 PCIe Gen5 slot
- Expansion: PCIe Gen5 slots for high-speed add-on cards
- Environmental: Operates from -40°C to 55°C, IP30-rated chassis
- Certifications: CE/UKCA, FCC Class A, RoHS, EN50121-4, IEC-61850-3

5.3 Technical Details

Feature	Specification	Details
Processor	CPU	Intel® Xeon®6 Processor 6710E 64C/64T, 2,4GHz Single Socket
	BIOS	AMI SPI Flash BIOS
	Security Acceleration	Intel® QuickAssist Technology
Memory	System Memory	DDR5, ECC, up to 512GB
	Socket	8x 288-Pin DIMM
Networking	Ethernet	2x 1GbE RJ45, 2x 10GbE RJ45 w/SRIOV
	LOM/OOB	1x RJ45 IPMI LOM Port
Storage	HDD/SSD	4x 2.5” U.2 NVMe Hot-Swappable Drive Bays
	M.2 Storage	1x M.2 2280/22110 M-Key for NVMe (PCIe Gen5)
Expansion	PCIe	2x FHFL (Double-Width) PCIe Gen5*16
		1x FHHL (Single-Width) PCIe Gen5*8
		1x FHHL (Single-Width) PCIe Gen5*4
I/O Interfaces	Button	1x Reset Button
	LED Indicators	Power/Status/HDD/LAN/LOM LED Indicator
	USB	4x USB 3.1 Ports & 1x USB 3.1 Port with Key Lock
	Console Port	1x 1GbE RJ45 Console Port
	Display	1x VGA Port

continues on next page

Table 1 – continued from previous page

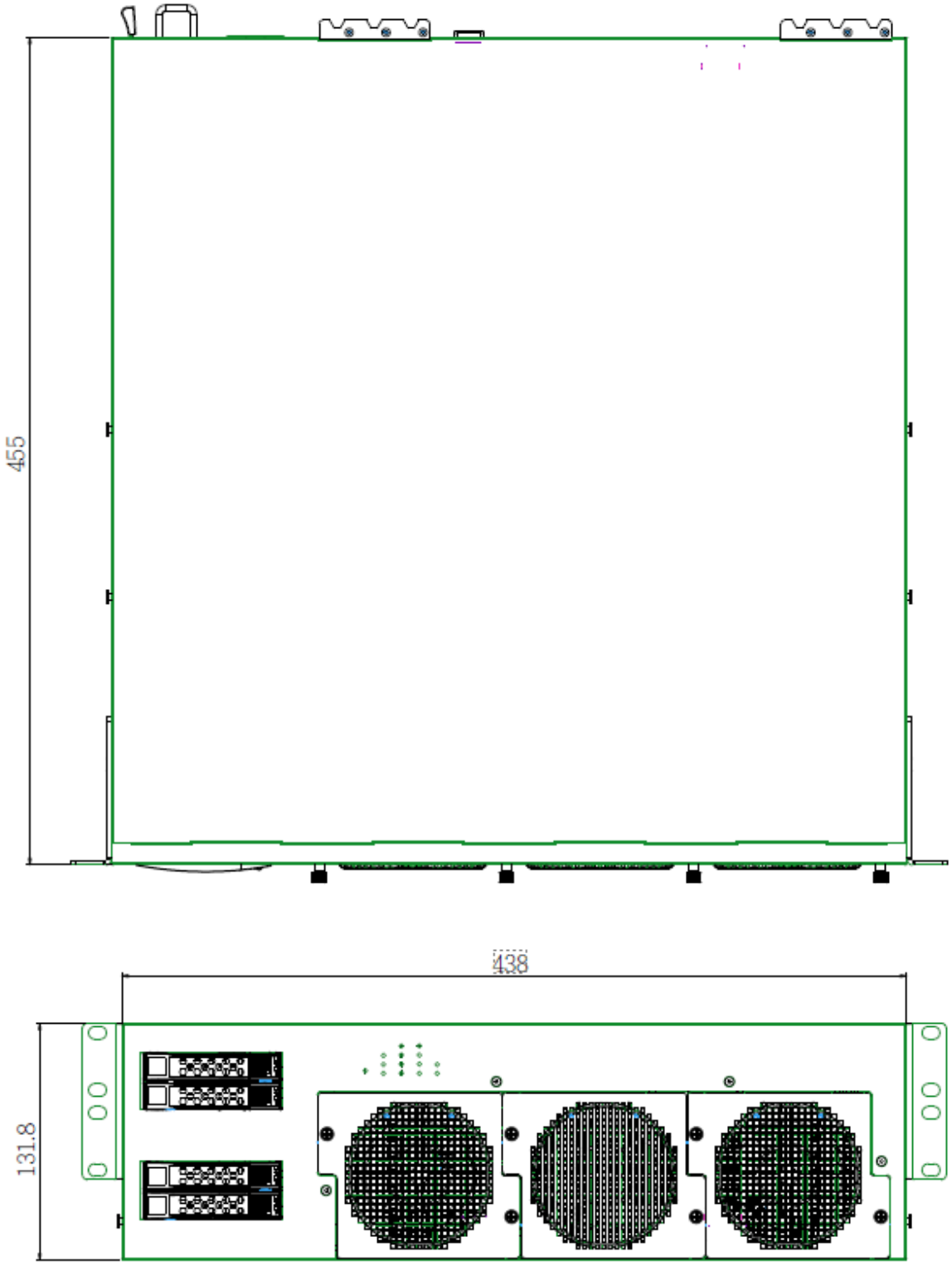
Feature	Specification	Details
Miscellaneous	Watchdog	Yes
	Internal RTC	Yes, with Li Battery
	TPM	TPM 2.0 Onboard
Power	Type/Watts	Dual power Input Up to 750W each
	Input	100~240VAC / 110~240VDC
Cooling	Processor	Passive CPU Heatsink
	System	3x Smart Cooling Fans
Enviromental	Temperature	-40°C ~ 55°C
	Humidity (RH)	Operating: 5% ~ 90%
		Non-Operating: 5%~95%
Mechanical	Dimension	438 x 131.8 x 455 mm
	Weight	TBD
	Form Factor	3U 19” Rackmount, IP30
Certifications	EMC	CE/UKCA, FCC Class A, RoHS, MTBF
	Safety	EN50121-4, UL+CB, IEC-61850-3, IEEE 1613
Driver Support	OS	Linux

5.4 Important Notes

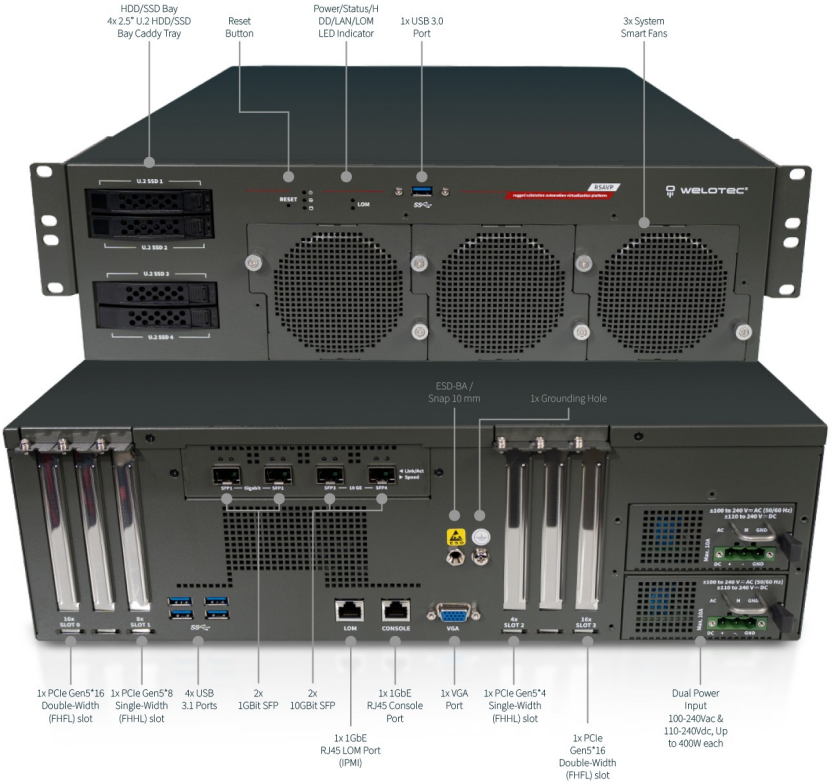
- Operating Conditions: Ensure proper airflow and cooling in rack environments to maintain optimal performance within specified temperature and humidity ranges.
- Power Redundancy: Dual power inputs are recommended for high-availability deployments.
- Firmware Updates: Regular BIOS and firmware updates are essential for security and stability.
- Storage Configuration: NVMe drives should be installed according to manufacturer guidelines for hot-swapping.
- Compliance: Verify local regulatory requirements for EMC and safety certifications before deployment.
- Maintenance: Replace Li battery for RTC as per recommended lifecycle to avoid timekeeping issues.

5.5 Dimension Drawings

- Lenght-455 cm
- Height-131.8 cm
- Width-438 cm

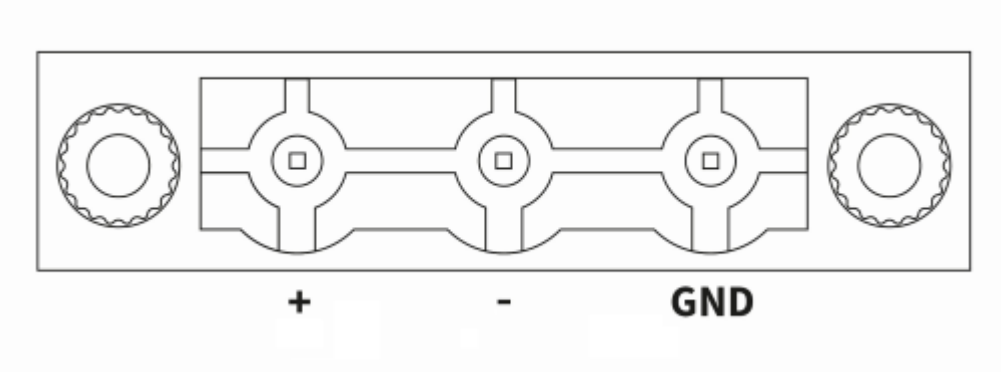


6 Interfaces and Connections



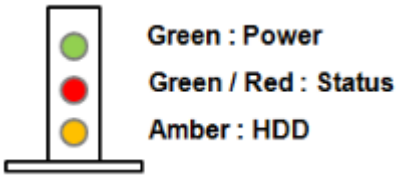
6.1 PSU Connection

- The terminal block consists of three main connection points labeled “+”, “-”, and “GND”. These are used for power and grounding:
  - “+” (Positive): Connect the positive voltage supply.
  - “-” (Negative): Connect the negative voltage or return line.
  - “GND” (Ground): Provides a grounding point for safety and signal reference.



6.2 LED Indicator Explanations

6.2.1 System Power / Status / Storage Activity

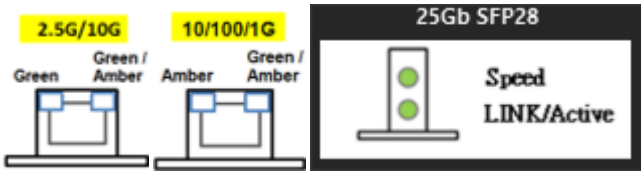


LED	Color on Board	LED Action	Description
POWER	Green	Steady	System Power ON
	Off	N/A	Power OFF
STATUS	Green	Steady	Controlled by GPIO
	Red	Steady	Controlled by GPIO
	Off	N/A	Controlled by GPIO (Default) or Power OFF
Storage	Amber	Blinking	Blinking indicates HDD activity, Include SATA/NVME
	Off	N/A	No data access or No power on

6.2.2 HDD Tray LED

LED	Color	LED Action	Description
POWER	Green	Steady	HDD/SSD Power ON
	Off	N/A	Power OFF
STATUS	Yellow	Blinking	Blinking indicates HDD activity, Include SATA / NVME Storage
	Off	N/A	No data access or Power OFF

6.2.3 RJ-45 LAN LED



6.2.4 1Gb RJ-45 Define:

Speed	Amber (Link/Active)	style=”color:orange”>Amber (Speed)
10M	Blinking / Data access	OFF
100M	Blinking / Data access	ON (Green)
1G	Blinking / Data access	On (Amber)

1. When cable is plug-in and network is linked. Both LED lights will be bright. The behavior is as defined.
2. Without the Cable plug-in, the LED should be off
3. If LAN Driver controls the LED, the behavior will follow the driver

6.2.5 2.5Gb RJ-45 Define:

Speed	Green (Link/Active)	Green/Amber (Speed)
10/100M	Blinking / Data access	OFF
1G	Blinking / Data access	ON (Amber)
2.5G	Blinking / Data access	ON (Green)

1. When cable is plug-in and network is linked. Both LED lights will be bright. The behavior is as defined.
2. Without the Cable plug-in, the LED should be off
3. If LAN Driver controls the LED, the behavior will follow the driver

6.2.6 10Gb RJ-45 Define:

Speed	Green (Link/Active)	Green/Amber (Speed)
100M	Blinking / Data access	OFF
1/2.5/5G	Blinking / Data access	ON (Amber)
10G	Blinking / Data access	ON (Green)

1. When cable is plug-in and network is linked. Both LED lights will be bright. The behavior is as defined.
2. Without the Cable plug-in, the LED should be off
3. If LAN Driver controls the LED, the behavior will follow the driver

6.2.7 25Gb SFP28 Define:

Speed	Green (Link/Active)	Amber/Green (Speed)
10G	Blinking / Data access	ON (Green)
25G	Blinking / Data access	ON (Amber)
Non-Link	OFF	OFF

1. When cable is plug-in and network is linked. Both LED lights will be bright. The behavior is as defined.
2. Without the Cable plug-in, the LED should be off
3. If LAN Driver controls the LED, the behavior will follow the driver

7 Hardware Installation

7.1 Safety Notice

To reduce the risk of **personal injury, electric shock, or damage to the system**, please remove all power connections to shut down the device completely.

7.2 Opening the Chassis

1. Power off the system. Loosen the two screws on the rear panel and one screw on each side.

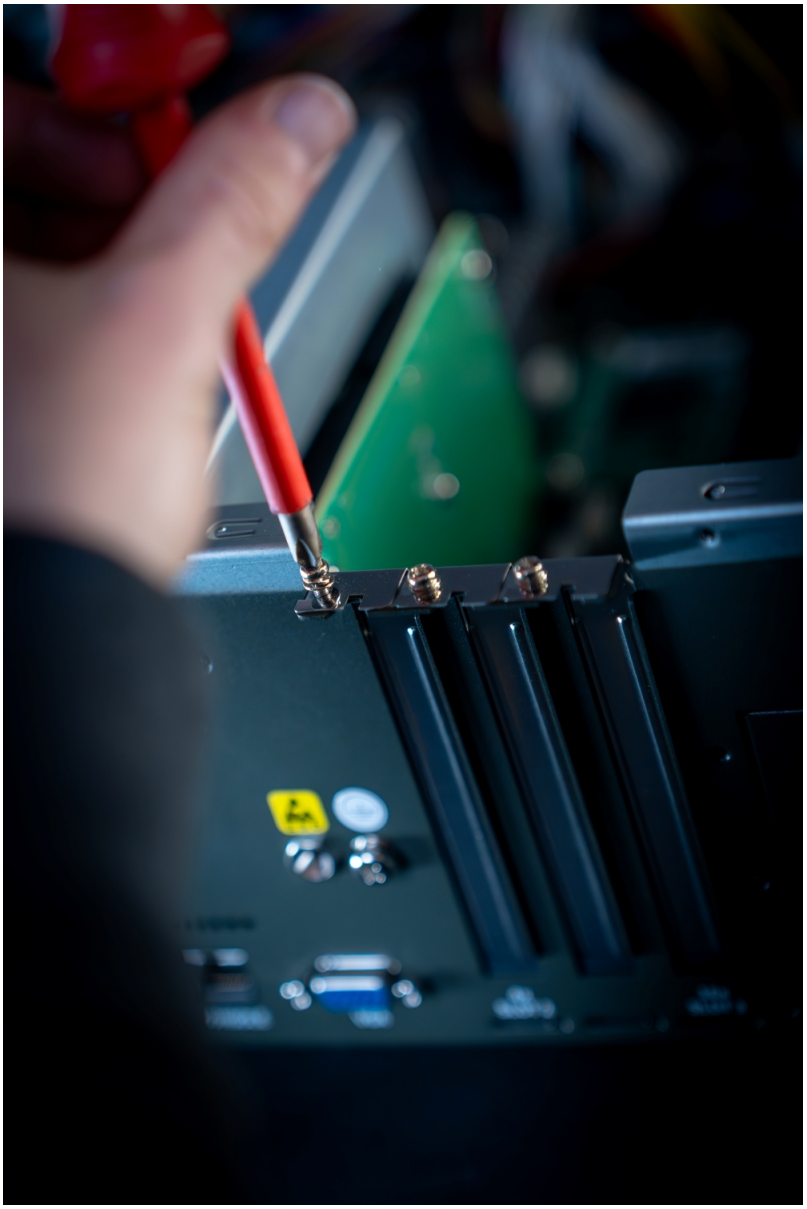
2. Lift the cover up to remove.

3. Gently release the latch by pulling it.
4. Ensure the latch is fully disengaged before lifting or removing the cover to avoid damage.

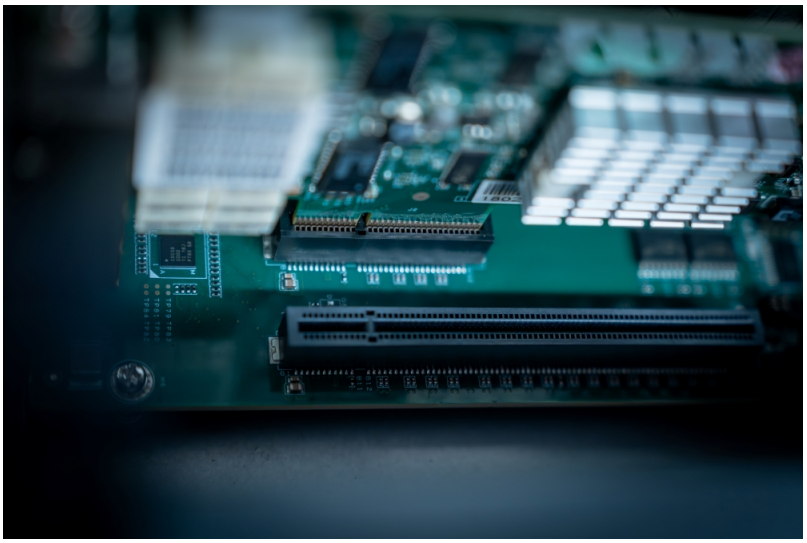
7.3 Install a Graphics Card or Expansion Card

1. **Power Off and Prepare**
   - Shut down the system and disconnect the power cable.
   - Ground yourself to prevent electrostatic discharge (ESD). Use an ESD strap if available.
   - Gather a screwdriver and the card you want to install.
2. **Open the Chassis**
   - Remove the screws or release the latch securing the chassis cover.
   - Carefully remove the cover to access the internal components.
3. **Locate the PCIe Slots**
   - Identify the appropriate PCIe slot for your card (e.g., x16 for graphics cards, x4 for smaller expansion cards).
4. **Remove the Slot Cover**

- Unscrew and remove the metal bracket covering the slot on the rear panel
- Keep the screws for later use.

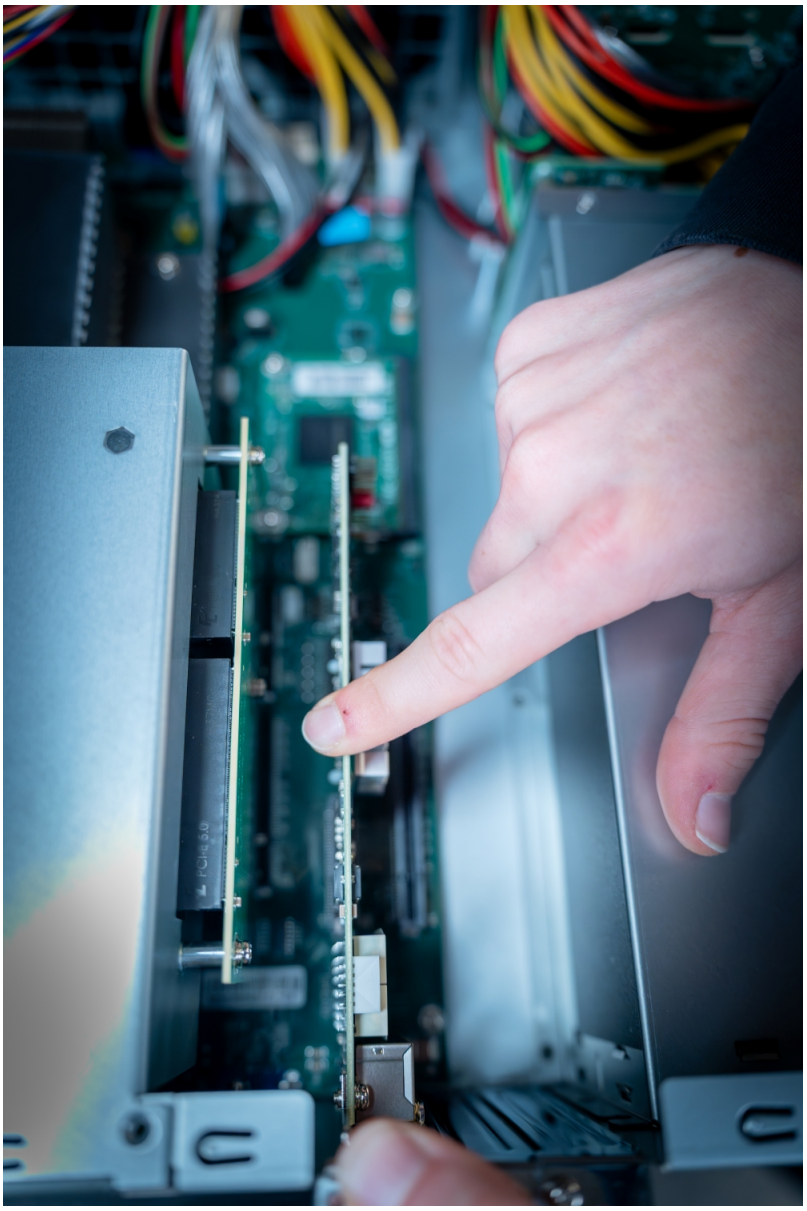


5. **Insert the Card**
    - Align the card’s connector with the PCIe slot.



- Ensure the card’s bracket fits into the rear panel opening.

- Press down firmly until the card is fully seated in the slot.



6. **Secure the Card**

- Use the screws you removed earlier to fasten the card’s bracket to the chassis (see fourth and fifth images).

- Make sure the card is stable and does not move.

7.4 Replacing the Smart Cooling Fans

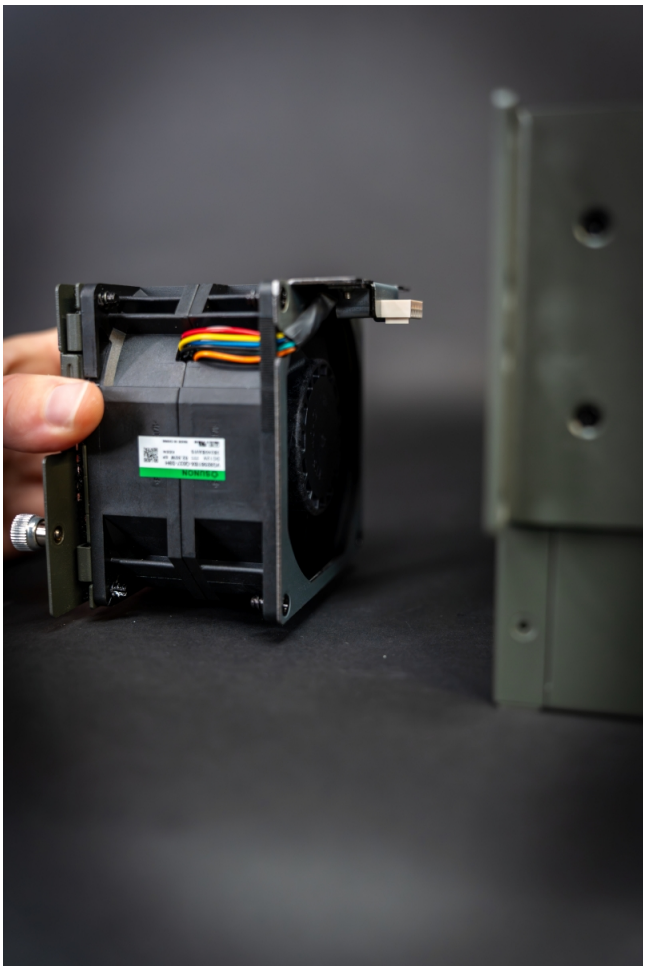
Cooling Fans may wear down eventually, please refer to the steps below for replacing smart cooling fans.

1. Power off the system and locate the cooling fans on the front panel.

2. Using a screwdriver, loosen the two lock-screws of the fan you would like to replace

3. Hold onto the lock screw and gently pull out the cooling fan

4. Insert a new fan into the fan bracket and push until it clicks into place and screw in the two lock-screws.

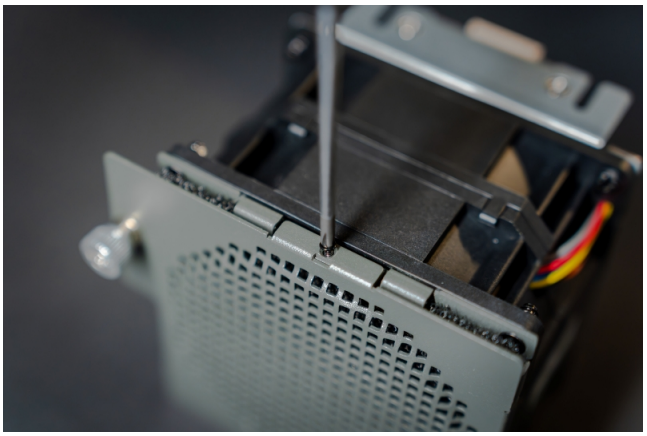


7.5 Changing the filter of the Smart Cooling Fans

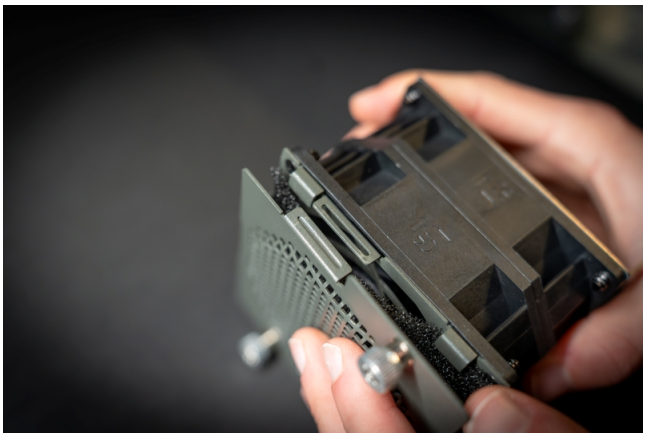
Follow these steps to replace the filter:

1. Remove the Smart Cooling Fan by loosening the two mounting screws by hand or with a screwdriver.
2. Carefully pull the Smart Cooling Fan out of the device.

3. Remove the screws on the top and bottom of the Smart Cooling Fan housing.

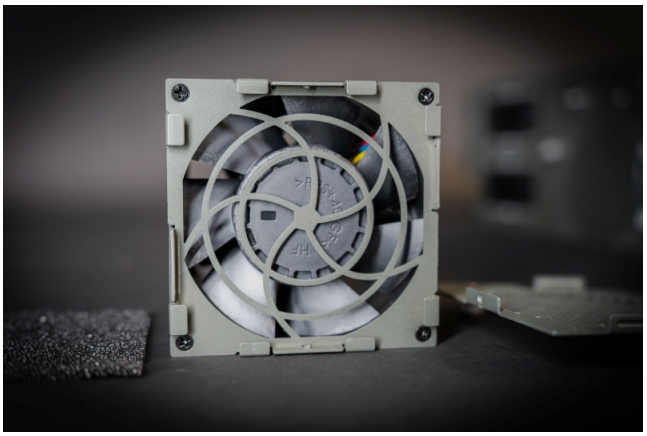


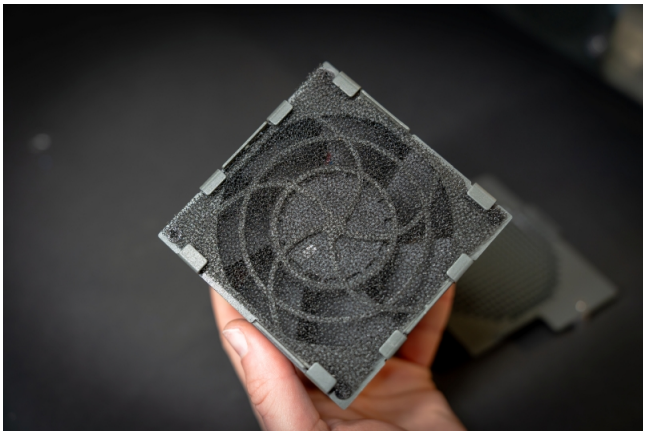
4. Release the cover by gently unclipping it.



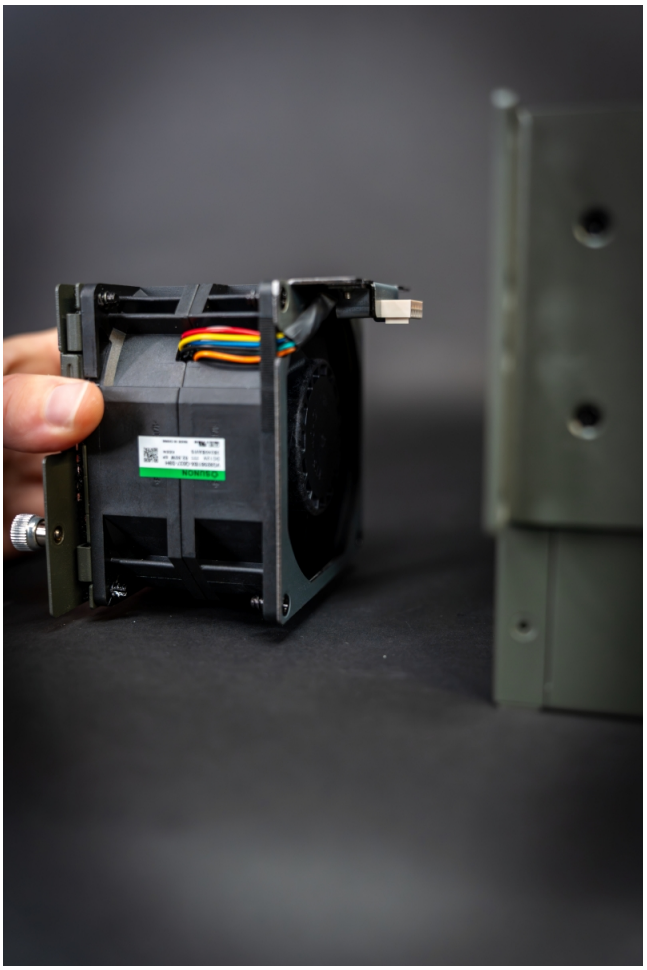
5. Take out the filter mat.

6. Insert a new filter mat and ensure it is properly seated in the corners.
7. Align the cover with the clips and snap it back into place.
8. Reinstall all previously removed screws.





9. Align the plug of the Smart Cooling Fan with the connector inside the device.



10. Slide the Smart Cooling Fan back into the device.

11. Secure the Smart Cooling Fan by tightening the mounting screws.

7.6 Replacing the Power Supply Untis

Power supply units can wear down over time. The RSAVP is compatible with dual power input up to 750W each, based on your chosen configuration. Ensure to use power supply units that align with these capacities.

1. Power off the system and locate the power supply untis on the rear panel.
2. Grip the handle and press the lever inward to pull out the power supply unit.


±100 to 240 V≂ AC (50/60 Hz)
±110 to 240 V⎓ DC
AC
N
Max. 10A
DC

3. Insert a new power supply unit and push until it clicks into place.

7.7 SSD Installation

1. Press the latch to release the handle.

2. Pull the handle to release the cover.

3. Use screws to fasten the SSD to the tray.

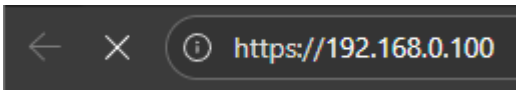
4. Ensure the SSD is firmly attached and does not move.
5. Align the tray with the bay slot
6. Push the tray gently until it clicks into place


U.2 SSD 2

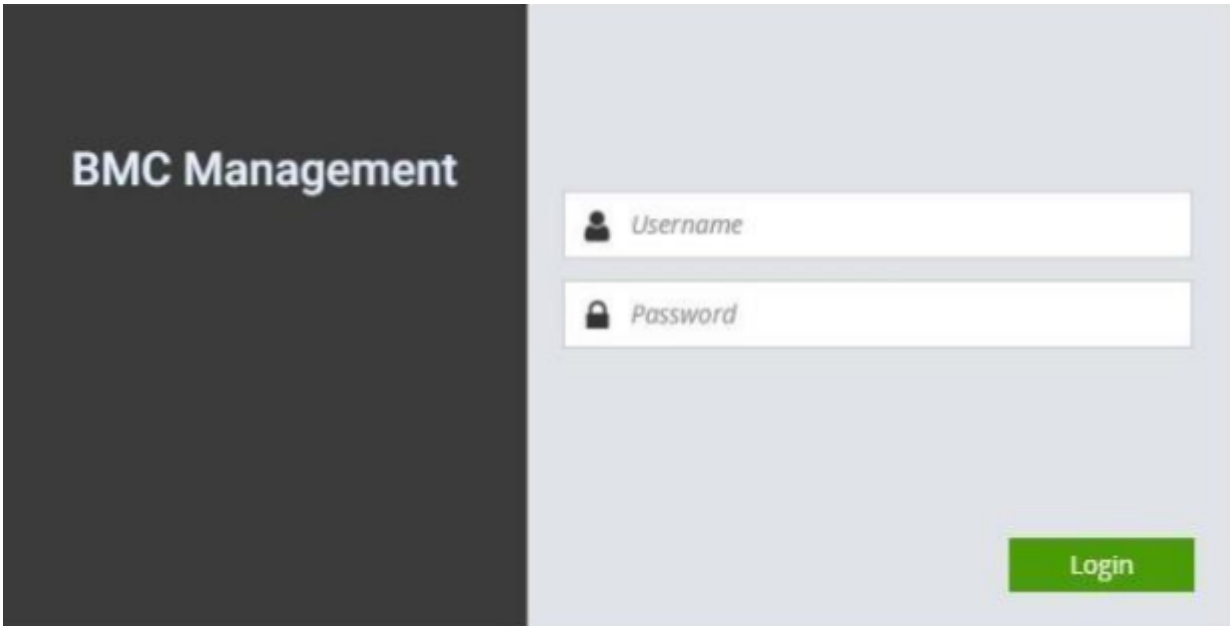
8 Web Configuration

8.1 Using BMC Web UI

In the address bar of your Internet browser, input the IP address of the remote server to access the BMC interface of that server.



Initial access of BMC prompts you to enter the User Name and Password. A screenshot of the login screen is given below:



- Username: Enter your username in this field.
- Password: Enter your password in this field.
- Sign me in: After entering the required credentials, click the Sign me in to log in to Web UI.

`Note: (1) If not specified, the default IP to access BMC is https://192.168.0.100.`

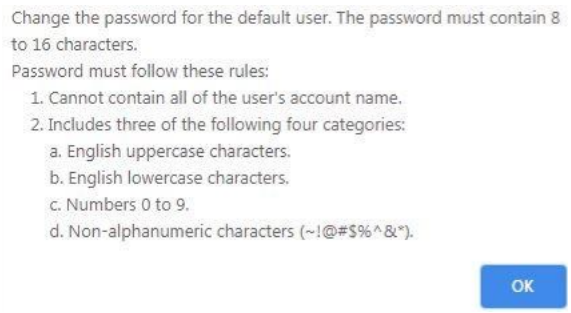
`(2) Please use https to access Web UI.`

8.2 Default User Name and Password

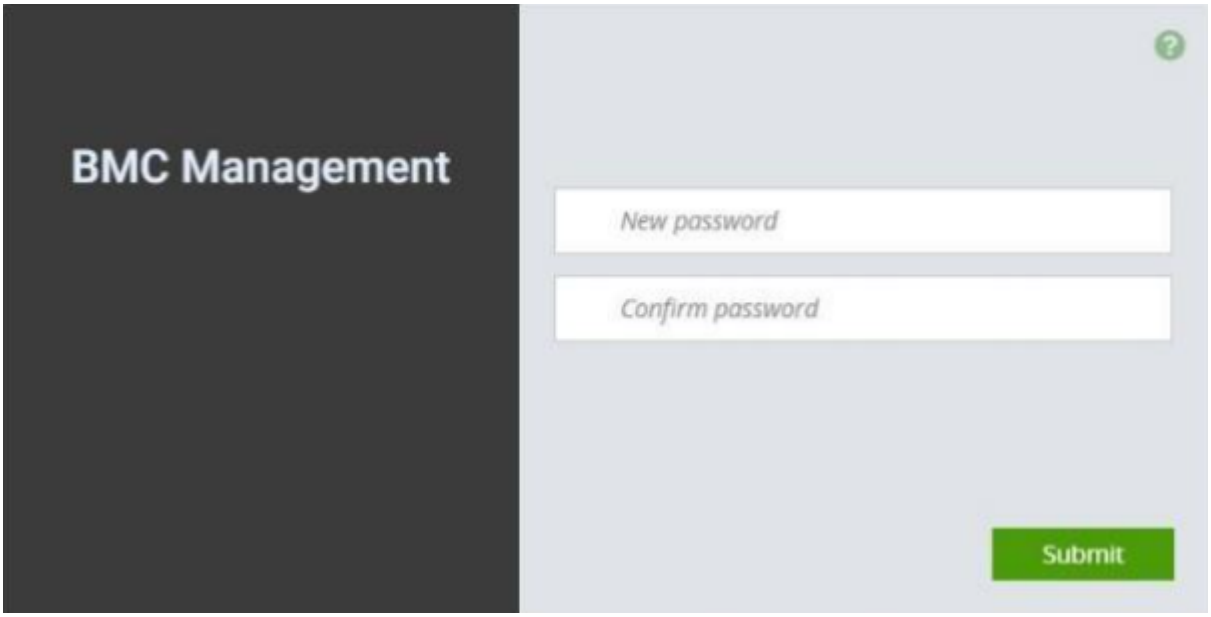
Username: admin

Password: admin

The default username and password are in lower-case characters. When you log in using the default username and password, you will get full administrative rights, and it will ask you to change the default password once you log in. The dialog is shown below:



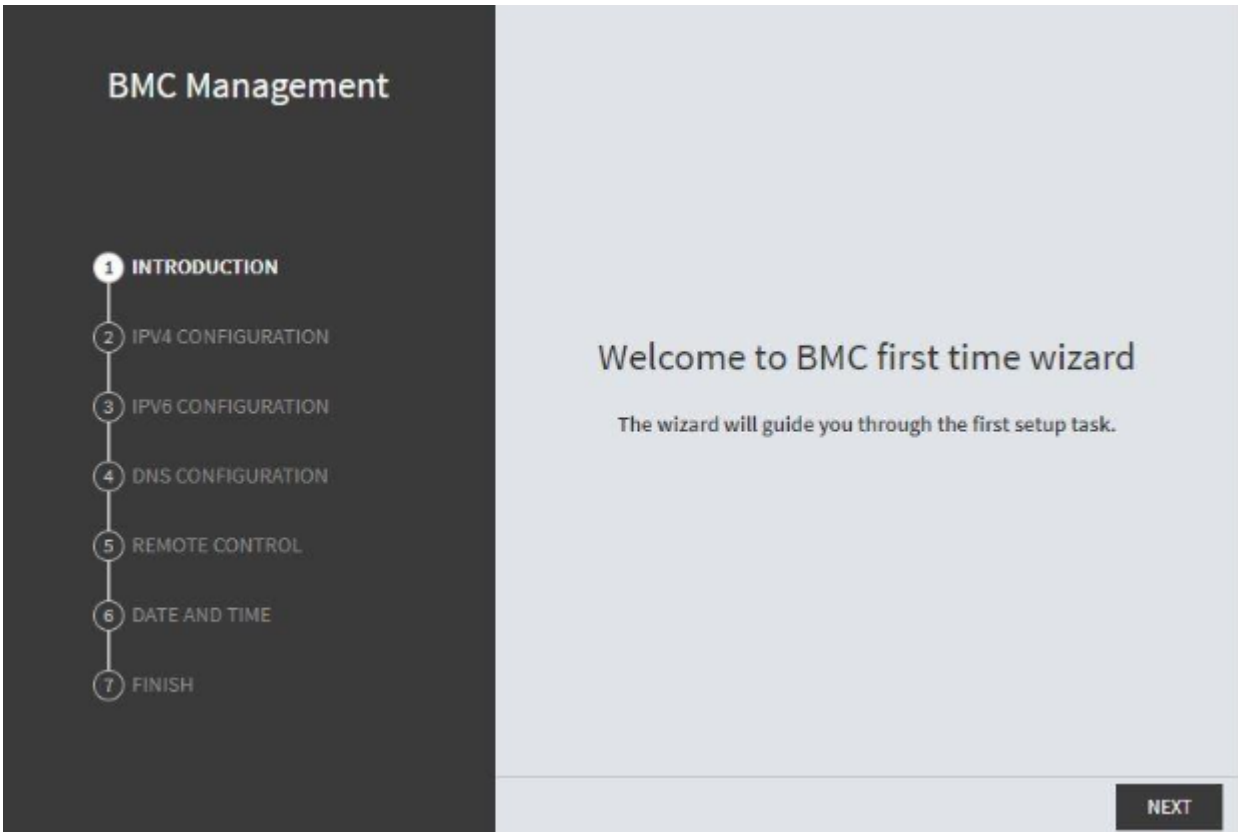
Clicking on OK will take you to set a password.



Change the default password – Set password

8.3 First Time Wizard Page Introduction

1. After the first-time login, you will see first time wizard welcome page as the following picture. Please press the “Next” button and configure your BMC step by step.
2. On the “IPv4”, “IPv6” and “DNS” pages, you could specify the hostname and network settings of BMC.
3. On the “Remote Control” page, you could specify allowed IP region which could access KVM and Remote media web pages.
4. On the “Date and Time” page, you could specify the NTP and time settings.



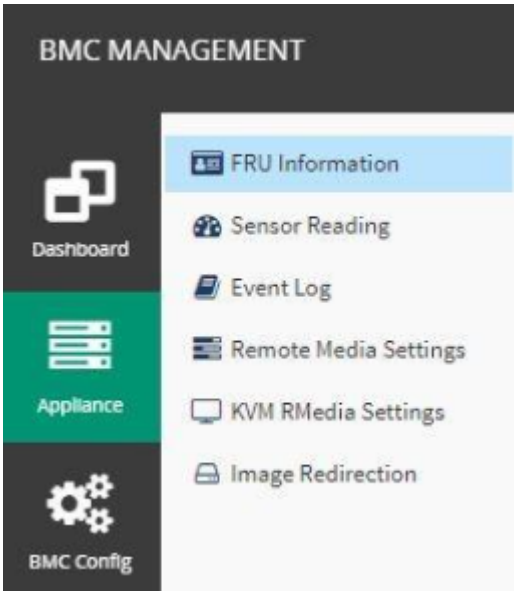
5. In the final page, please press “Finish” button to complete the first-time wizard. BMC will be rebooted and apply new settings. You could reconnect to the WebUI after a few minutes.

8.4 Web UI Layout Introduction

The BMC Web UI consists of various menu items:

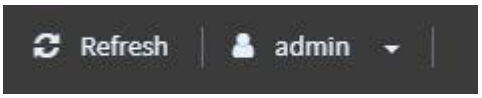
8.4.1 Menu Bar

A screenshot of the menu bar is shown below, please select the page you would like to navigate.



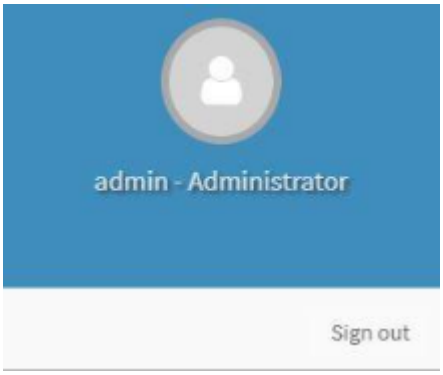
8.4.2 Quick Button and Logged-in User

The user information and quick buttons are located at the top right of the Web UI.



Logged-in user information: Click the User to view the logged-in user information.

A screenshot of the logged-in user information is shown below:



The logged-in user information shows the logged-in user's username, user privilege, with the quick buttons allowing you to perform the following functions:

- Refresh: reload the current page.
- Sign out: log out of the Web UI.

8.4.3 Logged-in User and its Privilege Level

This option shows the logged-in username and privilege. There are four kinds of privileges:

- User: Only valid commands are allowed.

Operator: All BMC commands are allowed except for the configuration commands that can change the behavior of the out-of-hand interfaces.

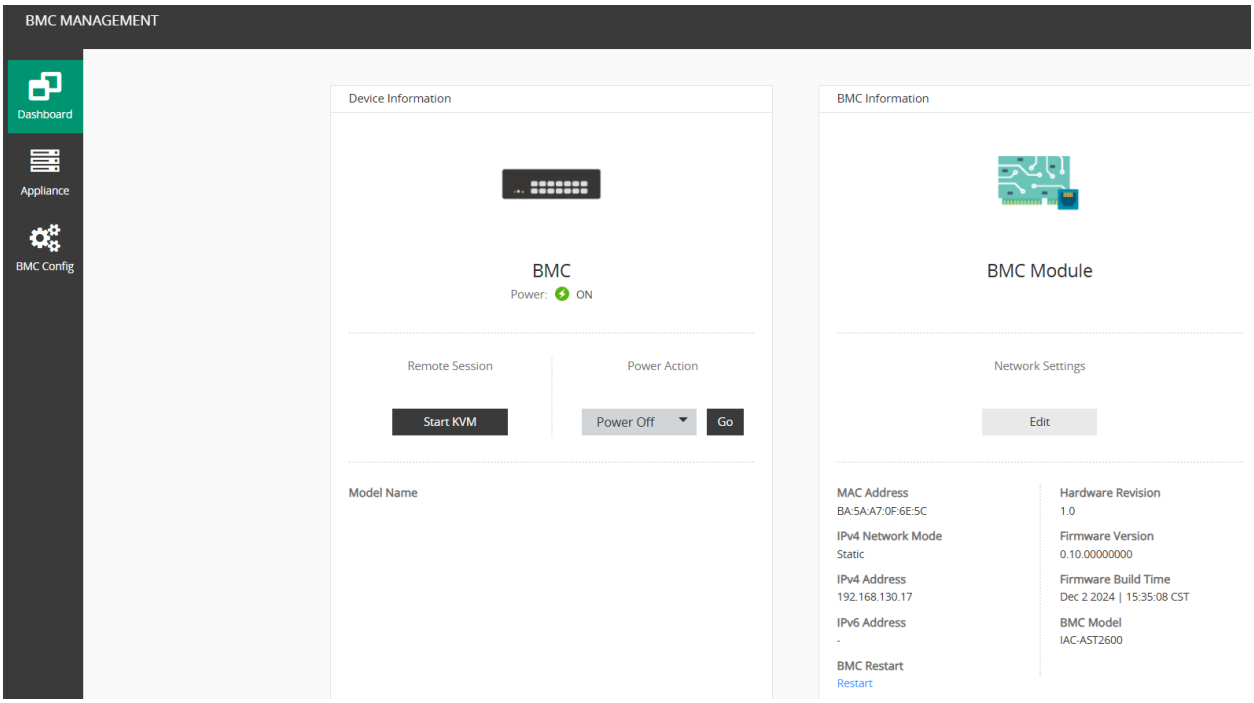
- Administrator: All BMC commands are allowed.
- No Access: Login access denied.

8.4.4 Help

Help: The Help icon is located at the top right of each page in Web UI. Click this help icon to view more detailed field descriptions.

8.5 Dashboard

The dashboard page gives the overall information about the status of a device. To open the Dashboard page, click Dashboard from the menu bar. A sample screenshot of the Dashboard page is shown below:



A brief description of the Dashboard page is given below:

- **Device Information** This indicates the system information such as power status, model name and serial number. You could also execute power action and remote KVM here.
- **BMC Information**
  This indicates the BMC module information such as network settings, firmware info, and model name.

9 BIOS Setup

9.1 Introduction

The system has AMI BIOS built-in, with a SETUP utility that allows users to configure required settings or to ativate certain system features. Pressing Tab or Del key immediately allows you to enter the Setup Utility.

9.2 Enter BIOS Setup

To enter the BIOS setup utility, simply follow the steps below:

1. Boot up the system
2. Press Del during the boot-up if you connect a keyboard to this unit. But if you connect a PC to this unit through console USB/Serial connection, then press Tab. Your system should be running POST (Power-On-Self-Test) upon booting up.
3. Then you will be directed to the BIOS main screen.
4. Instructions of BIOS navigations.

Control Keys	Description
→←	select a setup screen, for example, [Main],[Advanced] and [Platform]
↑↓	select an item/option on a setup screen
Enter	select an item/option or enter a sub-menu
+/-	to adjust values for the selected setup item/option
F1	to display General Help screen
F2	to retrieve previous values
F3	to load optimized default values
F4	to save configurations and exit BIOS
Esc	exit the current screen

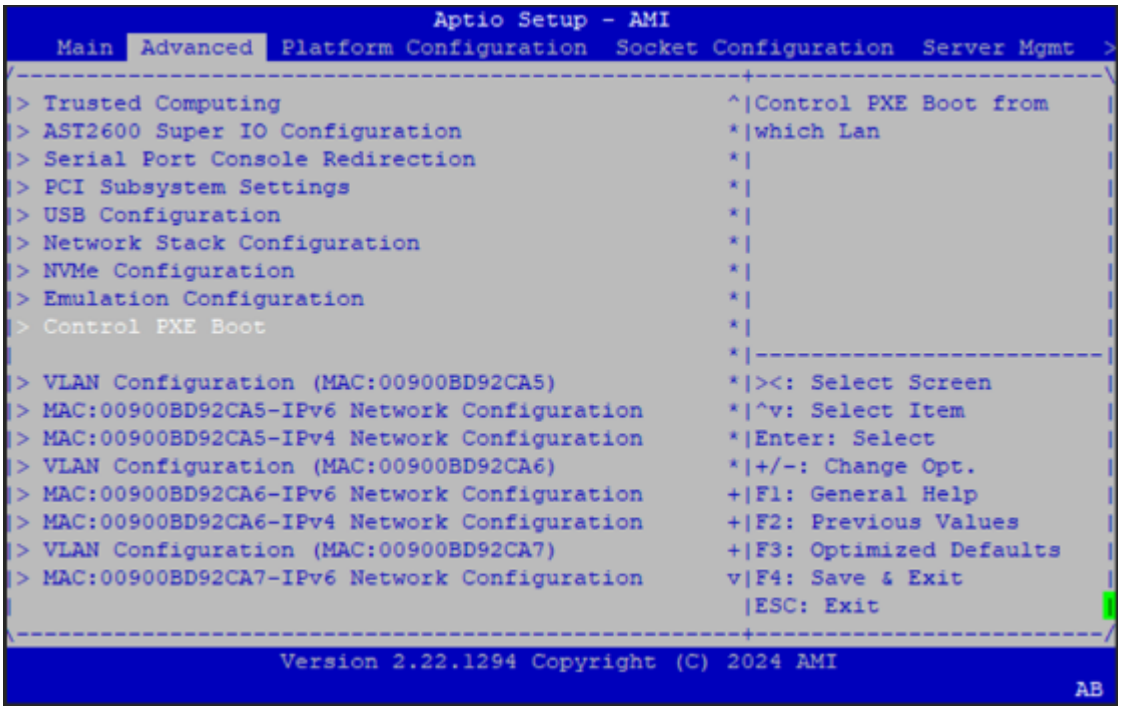
9.3 Main Page

Setup Main Page contains BIOS information and project version information.

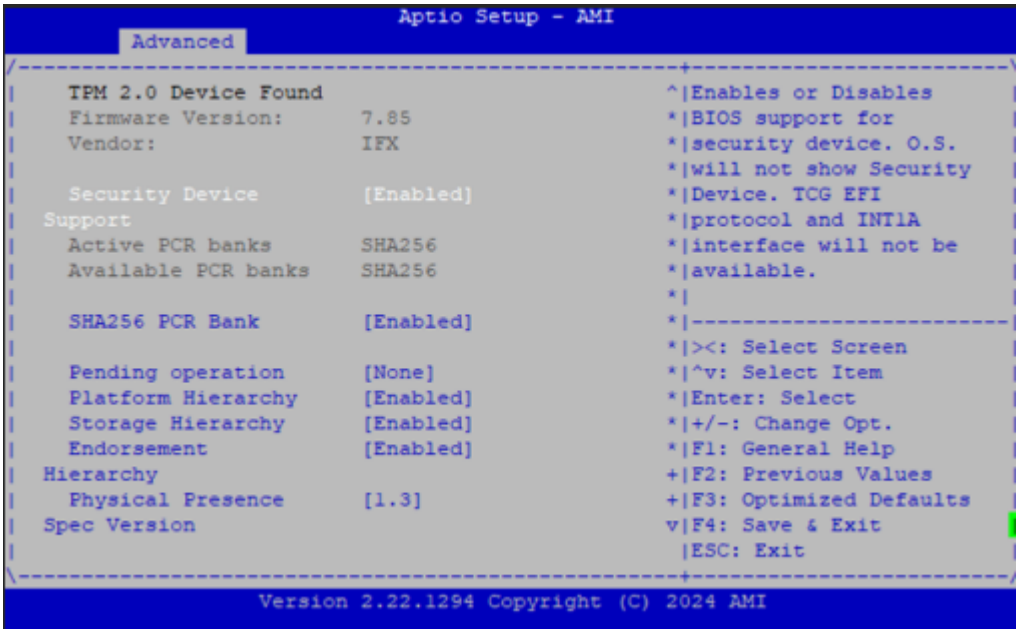
Item	Description
BIOS Information	BIOS Vendor: American Megatrends Core Version: AMI Kernel version, CRB code base, X64 Compliancy: UEFI version, PI version BIOS Version: BIOS release version Build Date and Time: MM/DD/YYYY CPLD Version(M): MB CPLD release version CPLD Version(S): BMC Card CPLD release version Access Level: Administrator / User
Memory Information	Total Memory: by case
System Date	To set the Date, use Tab to switch between Date elements. Default range of Year: 2005-2099 Default range of Month: 1-12 Days: dependent on Month.
System Time	To set the Date, use Tab to switch between Date elements.

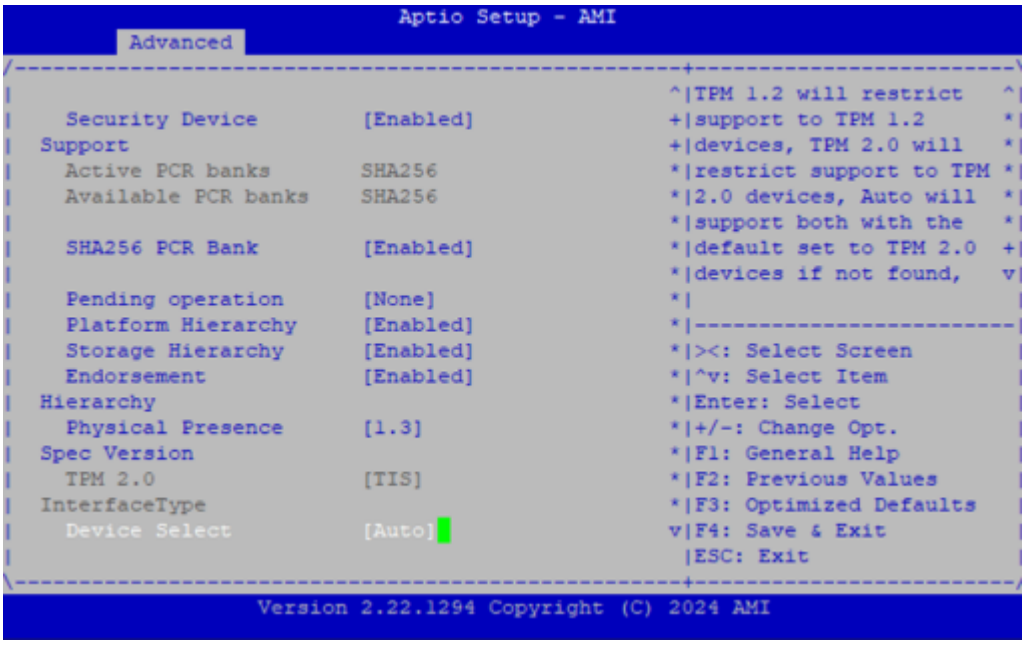
9.4 Advanced Page

Select the Advanced menu tab from the BIOS setup screen to enter the “Advanced” setup screen. Users can slect any of the items in the left frame of the screen



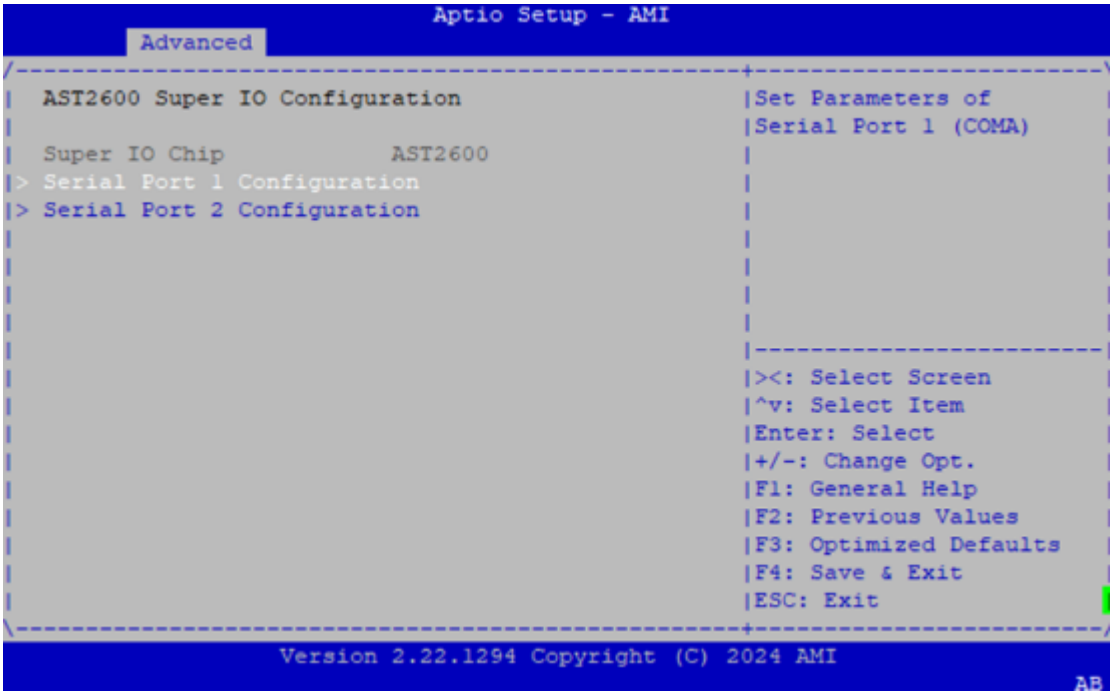
9.5 Trusted Computing



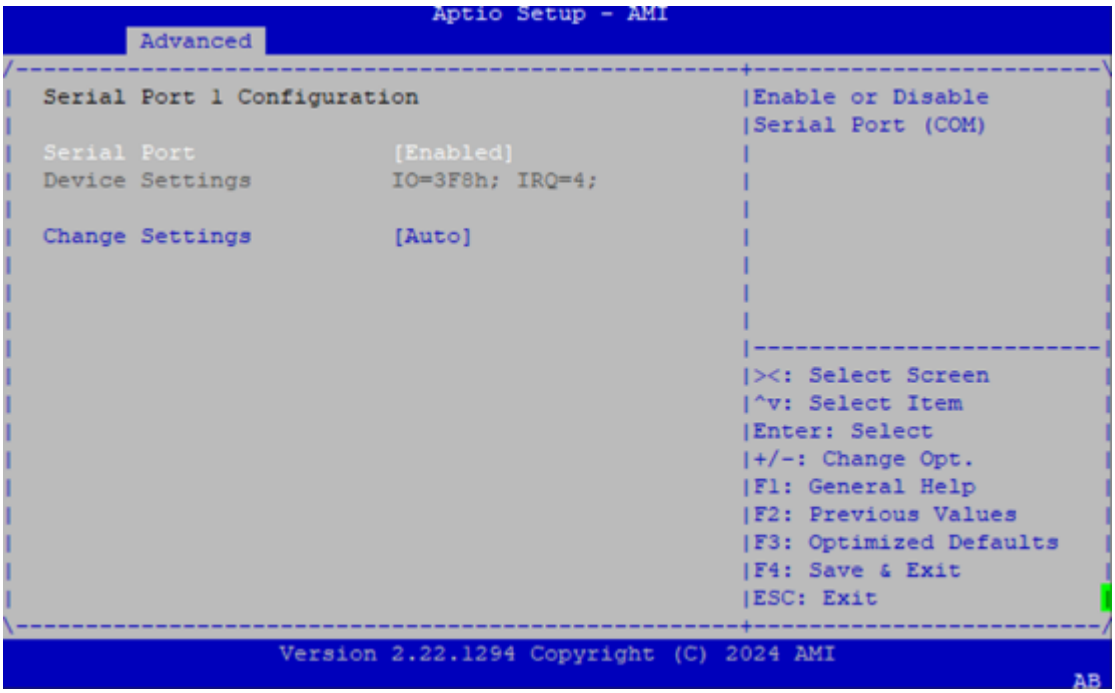


Feature	Options	Description
Security Device Support	Enabled Disabled	Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.
SHA256 PCR Bank	Enabled Disabled	Enable or Disable SHA256 PCR Bank
Pending operation	None TPM Clear	Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change State of Security Device.
Platform Hierarchy	Enabled Disabled	Enable or Disable Platform Hierarchy
Storage Hierarchy	Enabled Disabled	Enable or Disable Storage Hierarchy
Endorsement Hierarchy	Enabled Disabled	Enable or Disable Endorsement Hierarchy
Physical Presence Spec Version	1.2 1.3	Select to Tell O.S. to support PPI Spec Version 1.2 or 1.3. NOTE: Some HCK tests might not support 1.3
TPM 2.0 InterfaceType	TIS	Select the Communication Interface to TPM 2.0 Device
Device Select	TPM 1.2 TPM 2.0 Auto	TPM 1.2 will restrict support to TPM 1.2 devices, TPM 2.0 will restrict support to TPM 2.0 devices, Auto will support both with the default set to TPM 2.0 devices if not found, TPM 1.2 devices will be enumerated

9.6 Super IO Configuration

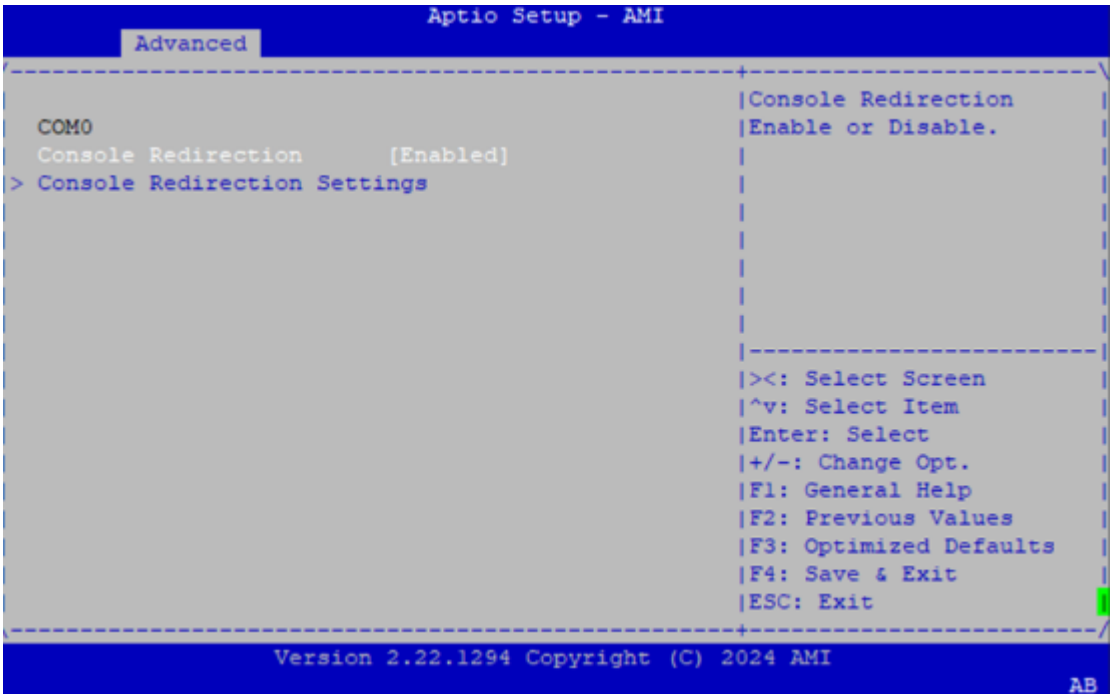


9.6.1 Serial Port 1 Configuration



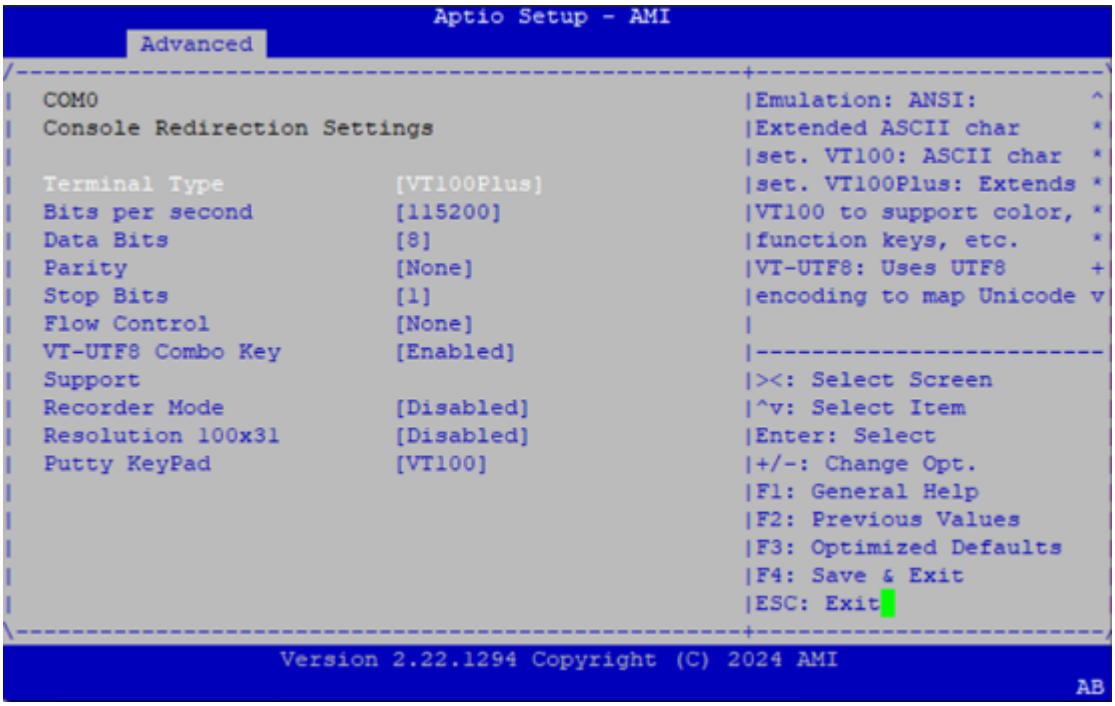
Feature	Options	Description
Serial Port	Enabled Disabled	Enable or Disable Serial Port (COM)
Device Settings	IO=3F8h; IRQ = 4	N/A
Change Settings	Auto IO=3F8h; IRQ=4;IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12;IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12;IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12;IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;	Select an optimal setting for Super IO Device

9.7 Serial Port Console Redirection



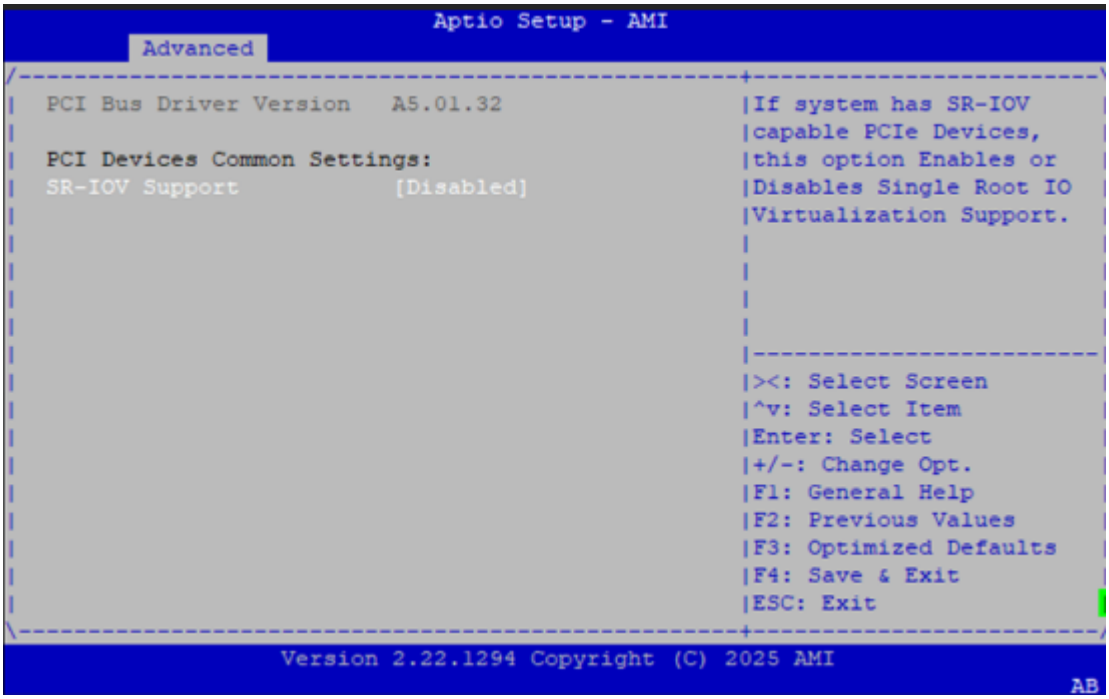
Feature	Options	Description
Console Redirection	Enabled Disabled	Console Redirection Enable or Disable

9.7.1 Console Redirection Settings



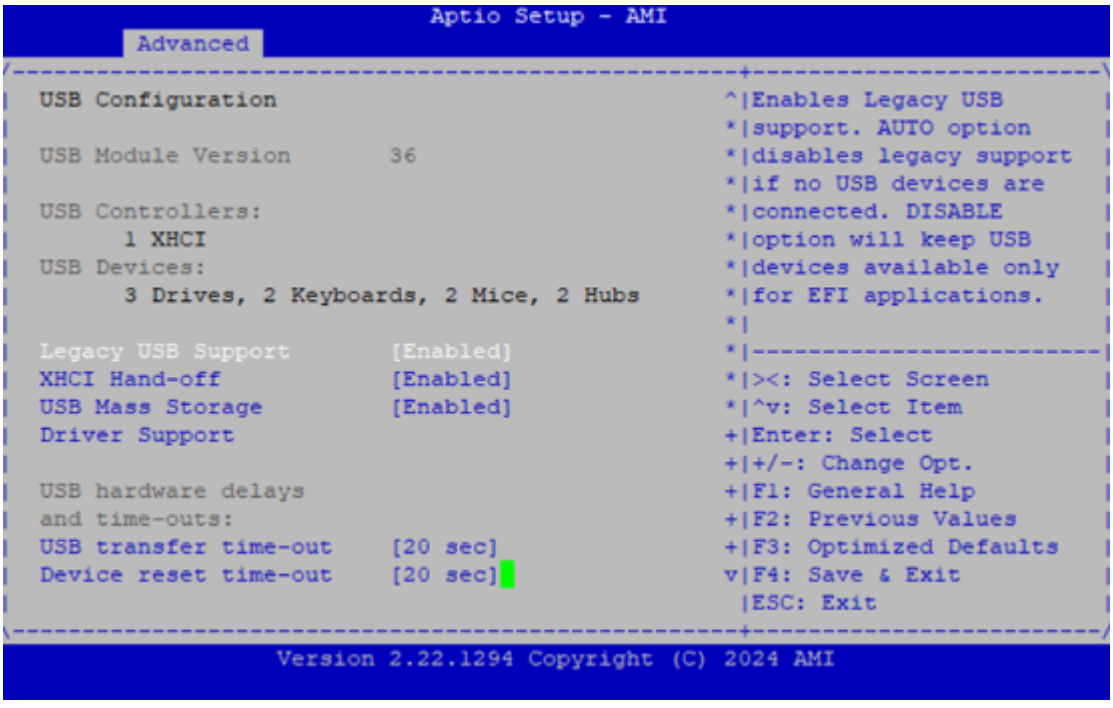
Feature	Options	Description
Terminal Type	VT100 Enabled VT-UTF8 ANSI	Emulation:ANSI: Extended ASCII char set. VT100: ASCII char set. VT100Plus: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytesm.
Bits per Second	9600 19200 38400 57600 115200	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	7 8	Data Bits
Parity	None Even Odd Mark Space	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bit is always 0. Mark and Space Parity do not allow for error detection. They can be used as an additional data bit.
Stop Bits	1 2	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.
Flow Control	None Hardware RTS/CTS	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.
VT-UTF8 Combo Key Support	Disabled Enabled	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals.
Recorder Mode	Disabled Enabled	With this mode enabled only text will be sent. This is to capture Terminal data.
Resolution 100x31	Disabled Enabled	Enables or disables extended terminal resolution
Putty Keypad	VT100 LINUX XTERM86 SCO ESCN VT400	Selects Function Key and Keypad on Putty.

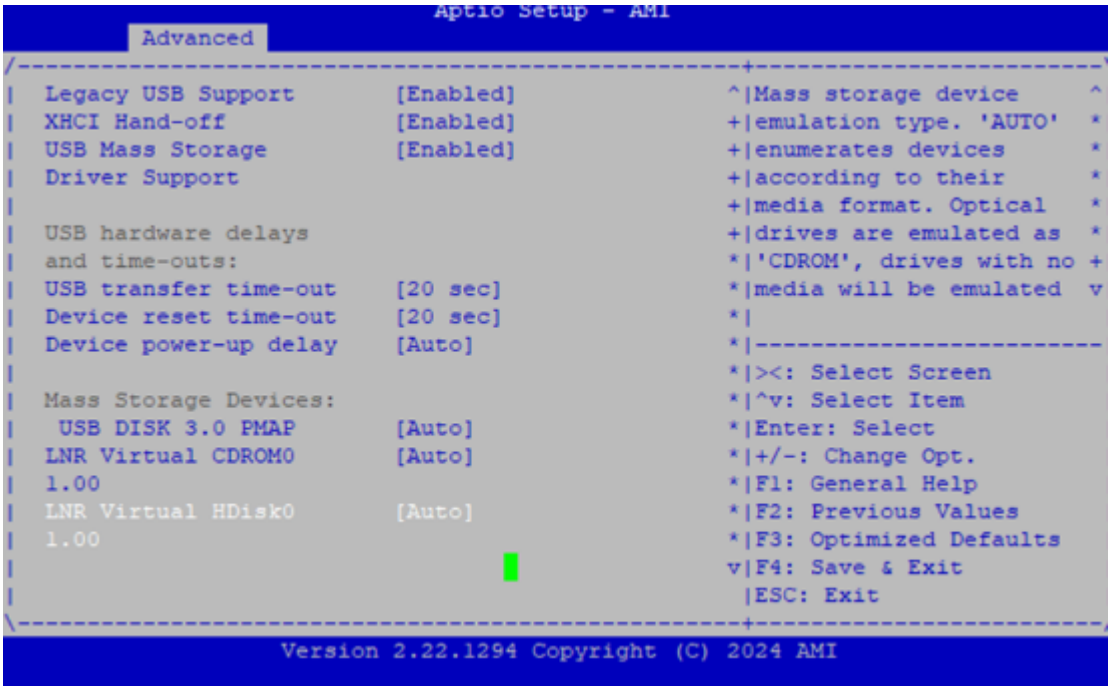
9.8 PCI Subsystem Settings



Feature	Options	Description
SR-IOV Support	Disabled Enabled	If system has SR-IOV capable PCIe Devices, this option Enables or Disables Single Root IO Virtualization Support.

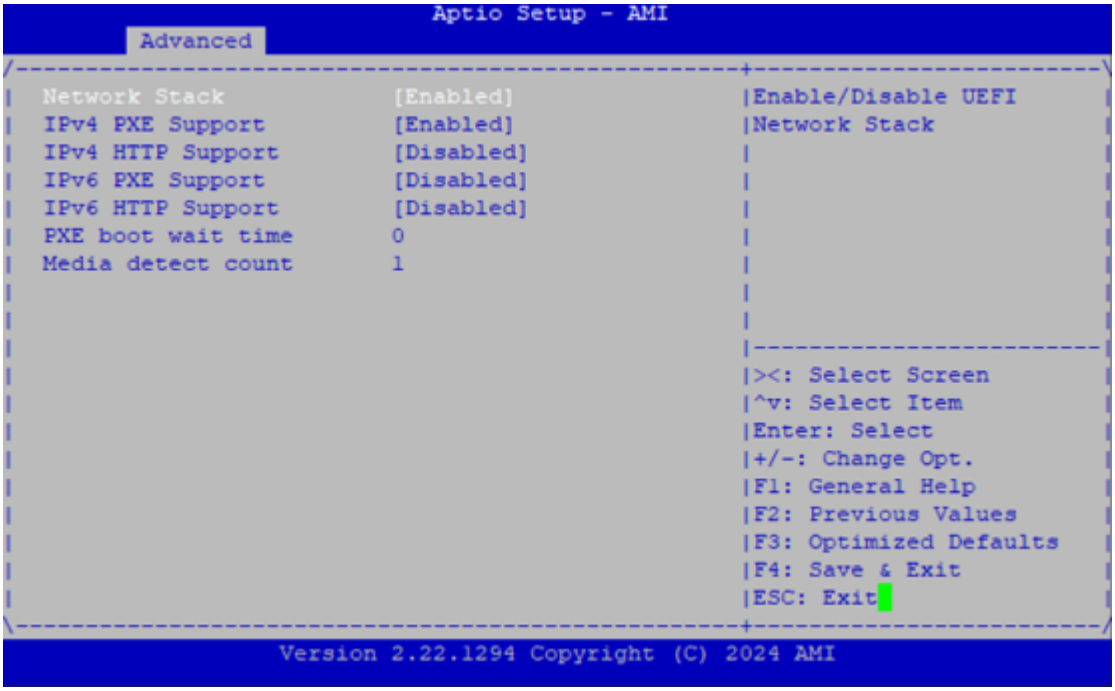
9.9 USB Configuration





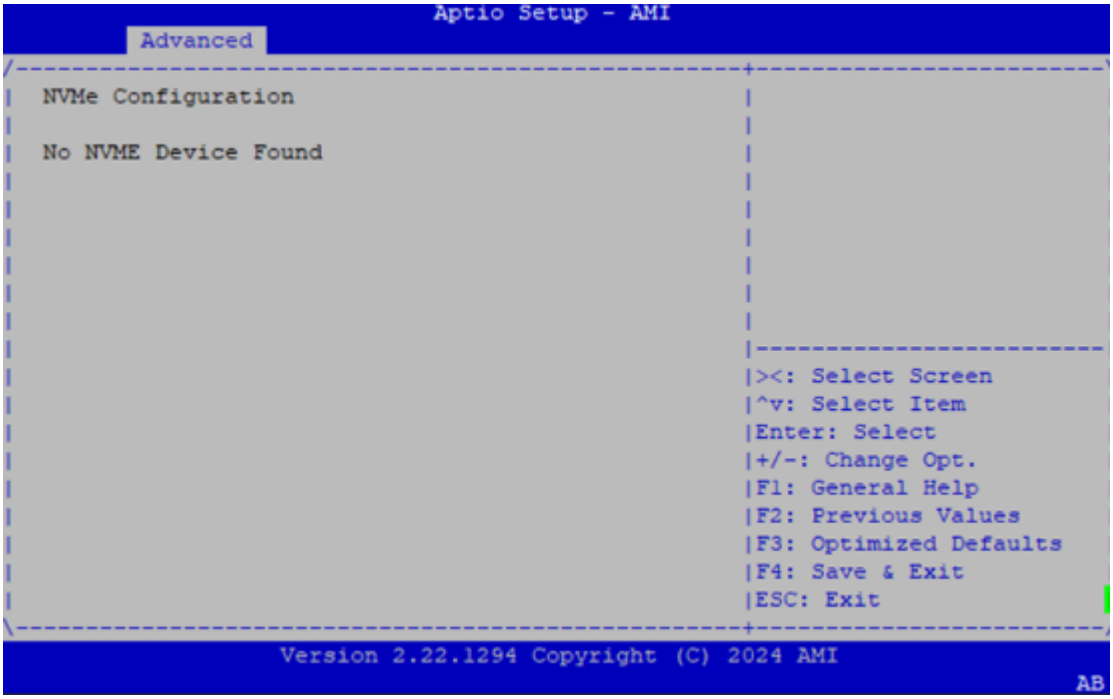
Feature	Options	Description
Legacy USB Support	Enabled Disabled	
XHCI Hand-off	Enabled Disabled	
USB Mass Storage	Enabled	
Driver Support	Disabled	
USB transfer time-out	1 sec 5 sec 10 sec 20 sec	
Device power-up delay	Auto Manual	

9.10 Network Stack Configuration

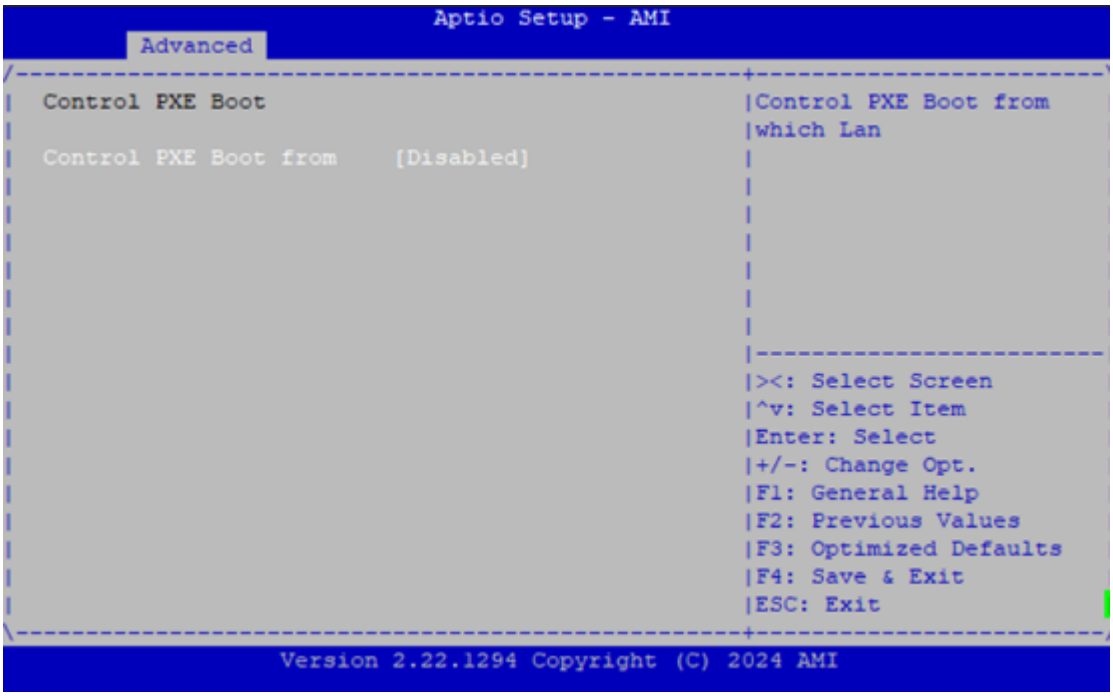


Feature	Options	Description
Network Stack	Disabled Enabled	Enables or disables UEFI Network Stack
IPv4 PXE Support	Disabled Enabled	Enable/Disable IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available.
IPv4 HTTP Support	Disabled Enabled	Enable/Disable IPv4 HTTP boot support. If disabled, IPv4 HTTP boot support will not be available.
IPv6 PXE Support	Disabled Enabled	Enable/Disable IPv6 PXE boot support. If disabled, IPv6 PXE boot support will not be available.
IPv6 HTTP Support	Disabled Enabled	Enable/Disable IPv6 HTTP boot support. If disabled, IPv6 HTTP boot support will not be available.
PXE boot wait time	0	Wait time in seconds to press ESC key to abort the PXE boot. Use either +/- or numeric keys to set the value.
Media detect count	1	Number of times the presence of media will be checked. Use either +/- or numeric keys to set the value.

9.11 NVMe Configuration

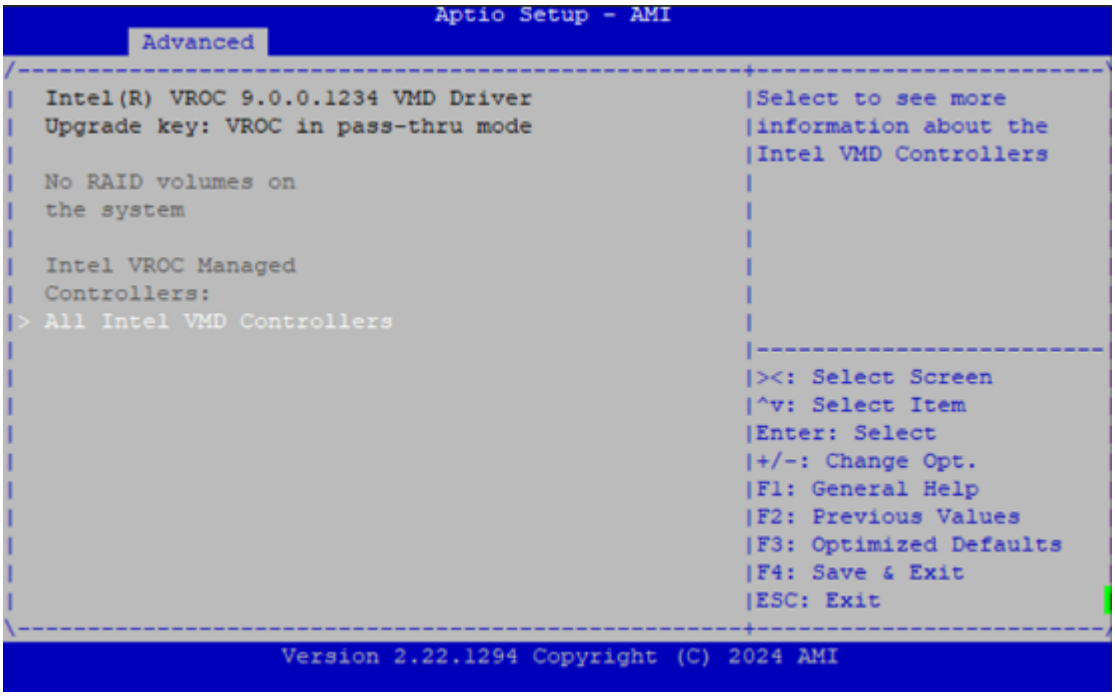


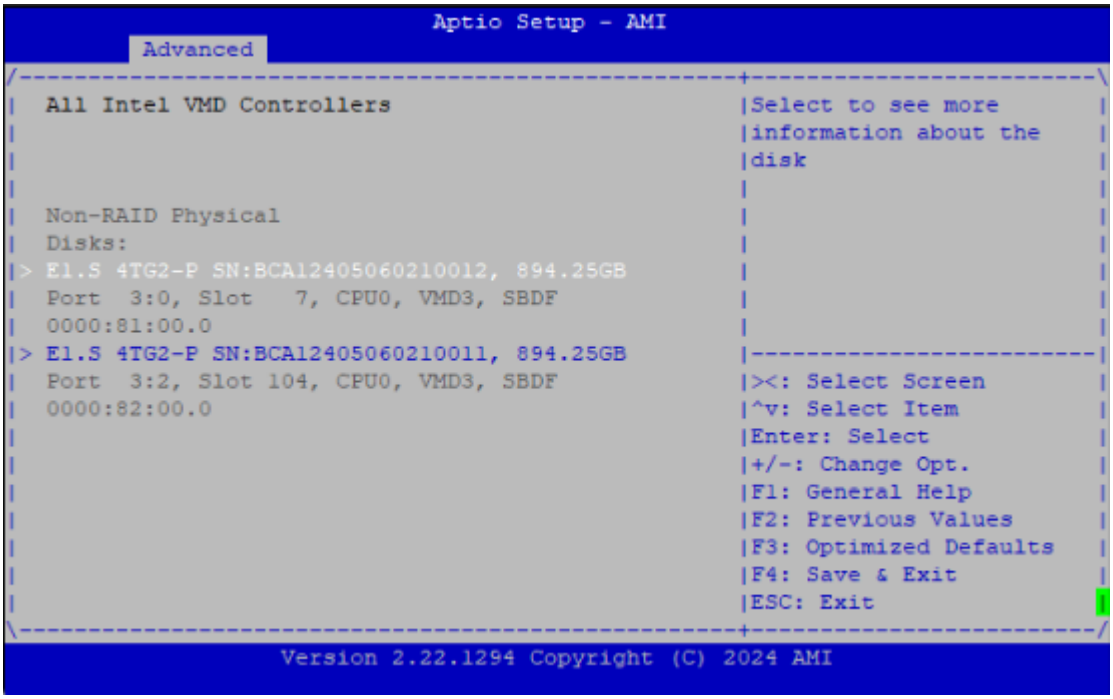
9.12 Control PXE Boot



Feature	Options	Description
Control PXE Boot from	Disabled Enabled	Control PXE Boot from which Lan. Note: LAN port is set with Intel I210, the setup menu item is Enable or Disable PXE Boot function via Intel I210 LAN port.

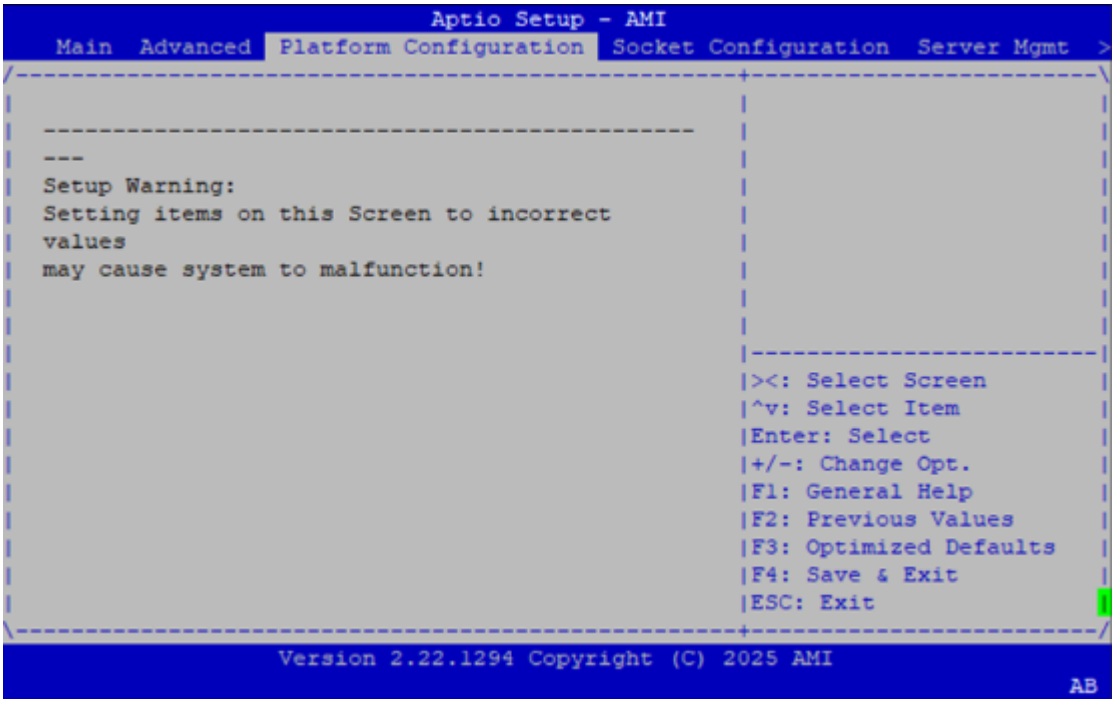
9.13 Intel VROC





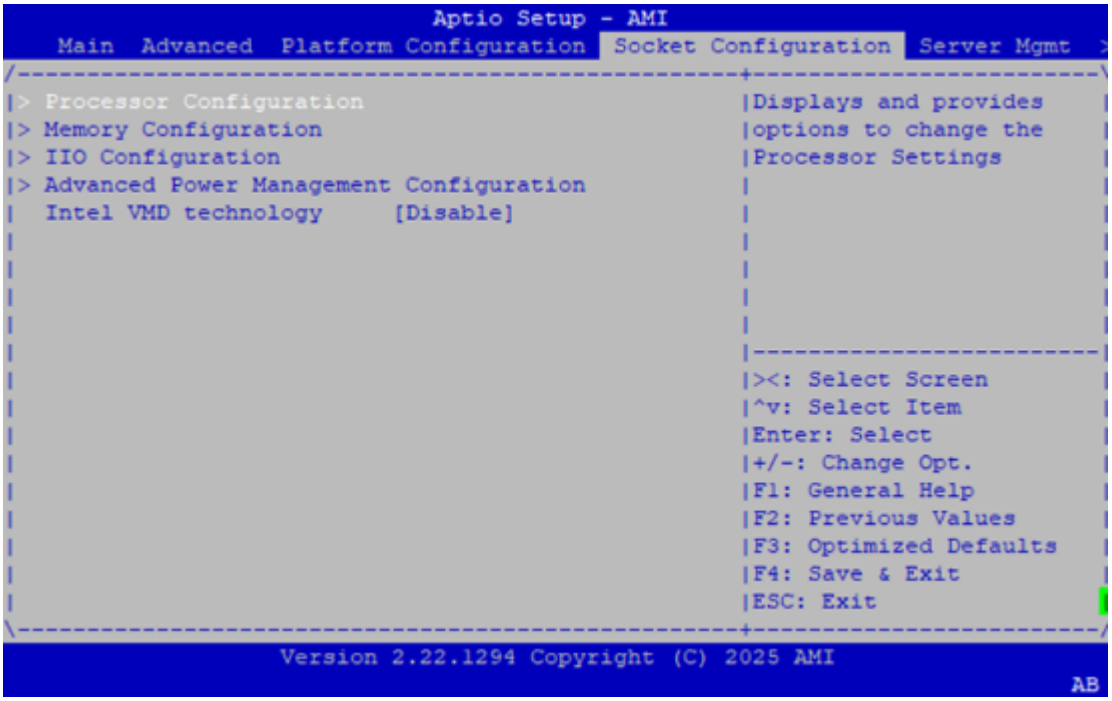
9.14 Platform Configuration

Select the Platform menu item from the BIOS setup screen to enter the Platform Setup screen. Users can select any of the items in the left frame of the screen.



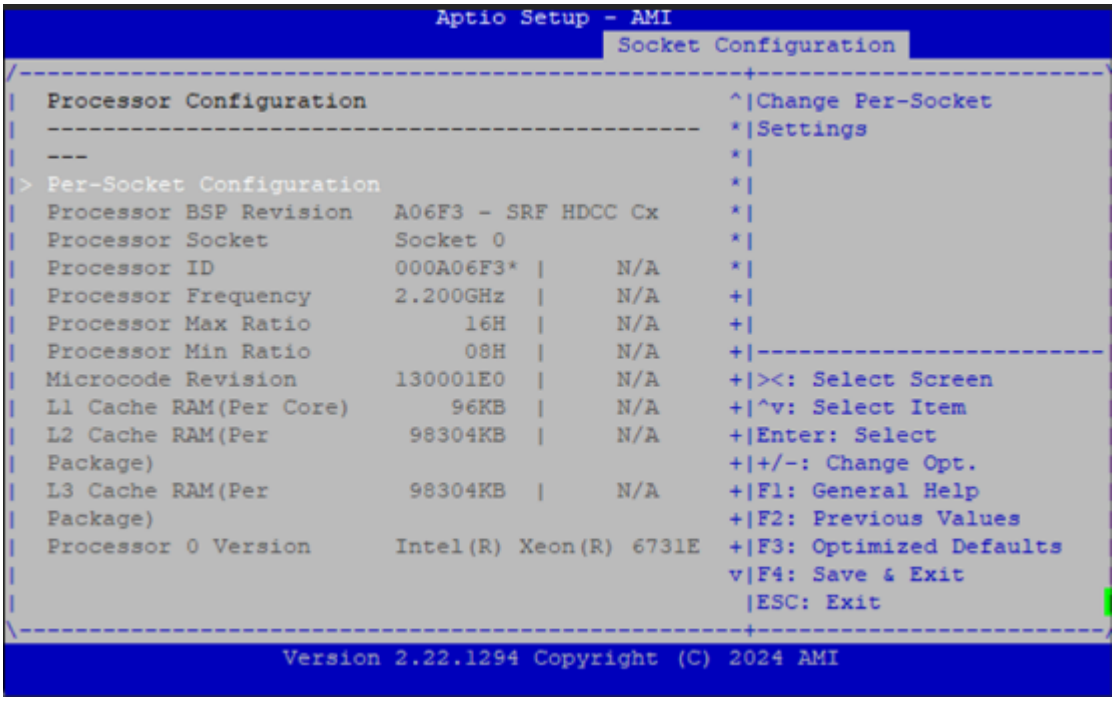
9.15 Socket Configuration

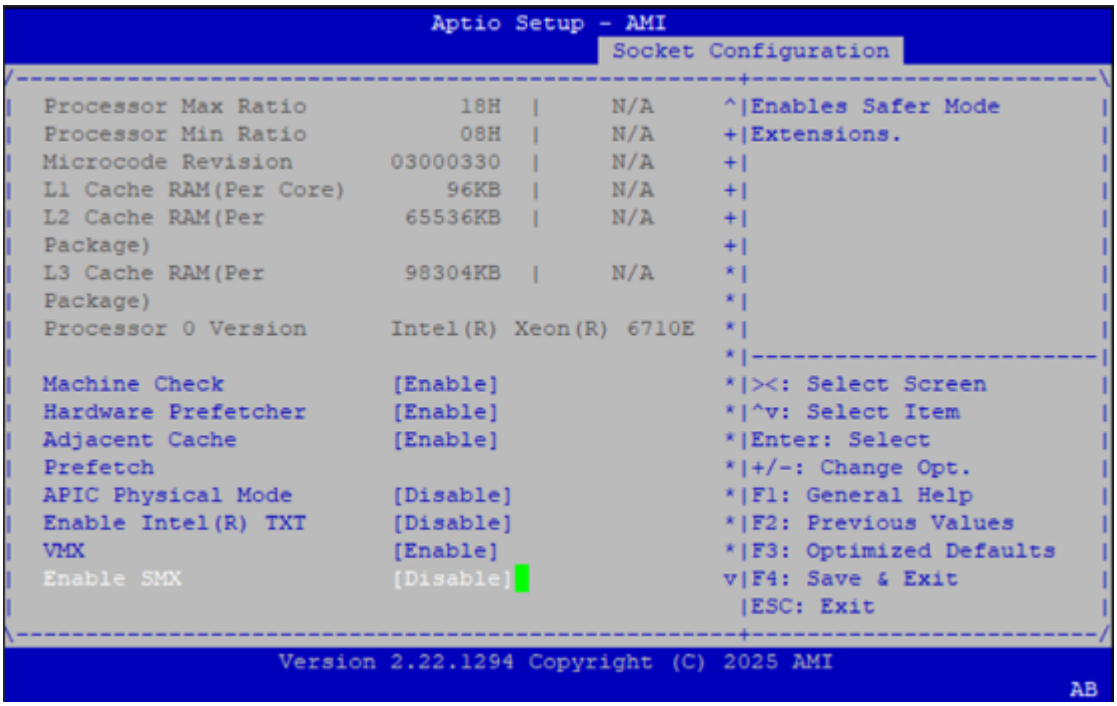
Select the Socket menu item from the BIOS setup screen to enter the Socket Setup screen. Users can select any of the items in the left frame of the screen.



Feature	Options	Description
Processor Configuration	None	Displays and provides option to change the Processor Settings
Memory Configuration	None	Displays and provides option to change the Memory Settings
IIO Configuration	None	Displays and provides option to change the IIO Settings
Advanced Power Management Configuration	None	Displays and provides option to change the Power Management Settings
Intel VMD technology	Disable Enable	Enable/Disable VMD this IIO Domain.

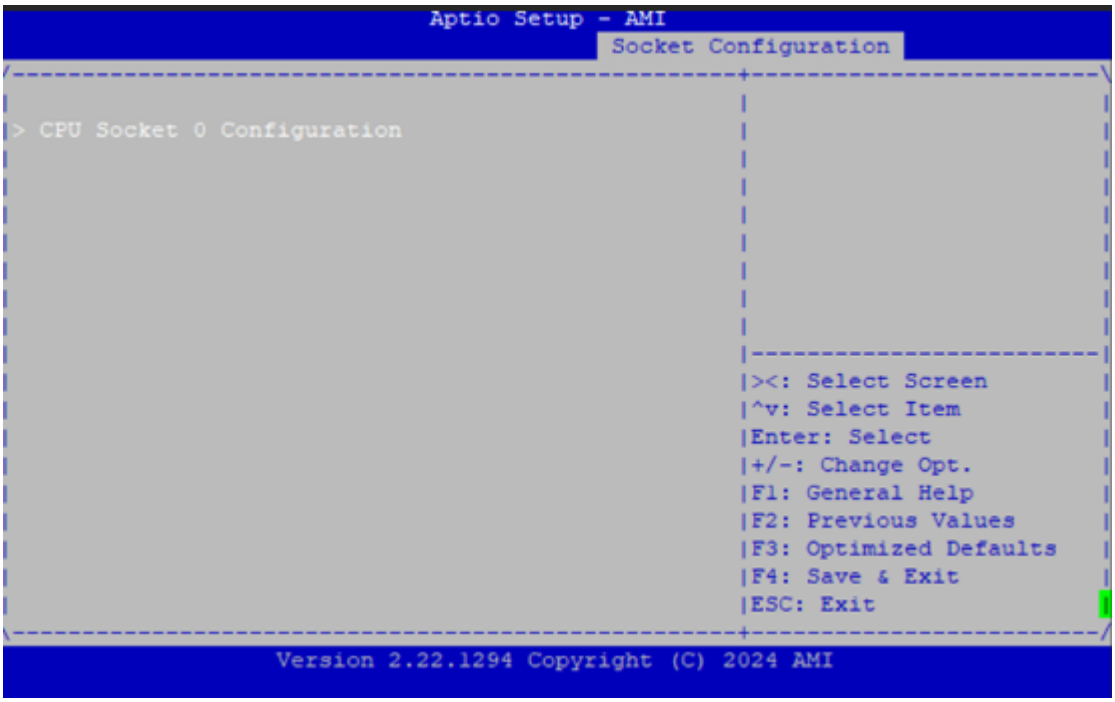
9.15.1 Processor Configuration





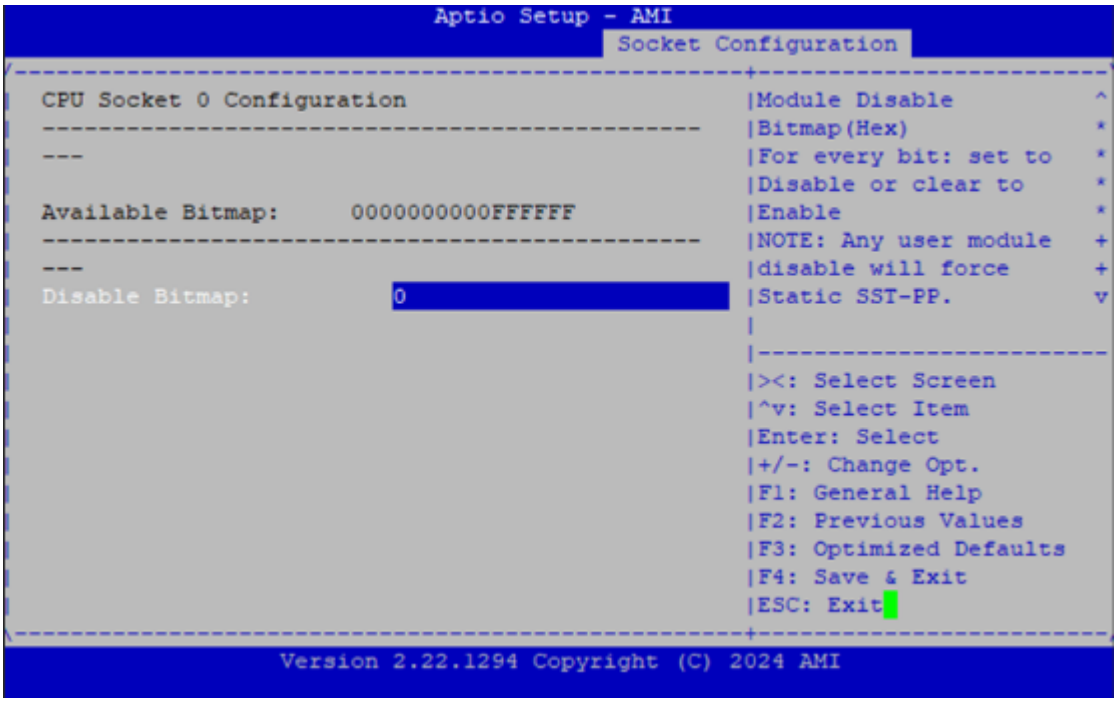
Feature	Options	Description
Machine Check	Disabled Enabled	Enable or Disable the Machine Check
Hardware Prefetcher	Disabled Enabled	MLC Streamer Prefetcher (MSR 1A4h Bit [0])
Adjacent Cache Prefetcher	Disabled Enabled	MLC Spatial Prefetcher (MSR 1A4h Bit [1])
APIC Physical Mode	Disabled Enabled	Enable/Disable the APIC physical destination mode
Enable Intel® TXT	Disabled Enabled	Enables Intel(R) TXT
VMX	Disabled Enabled	Enables the Vanderpool Technology, which takes effect after reboot.
Enable SMX	Disabled Enabled	Enables Safer Mode Extensions

9.15.2 Per-Socket Configuration

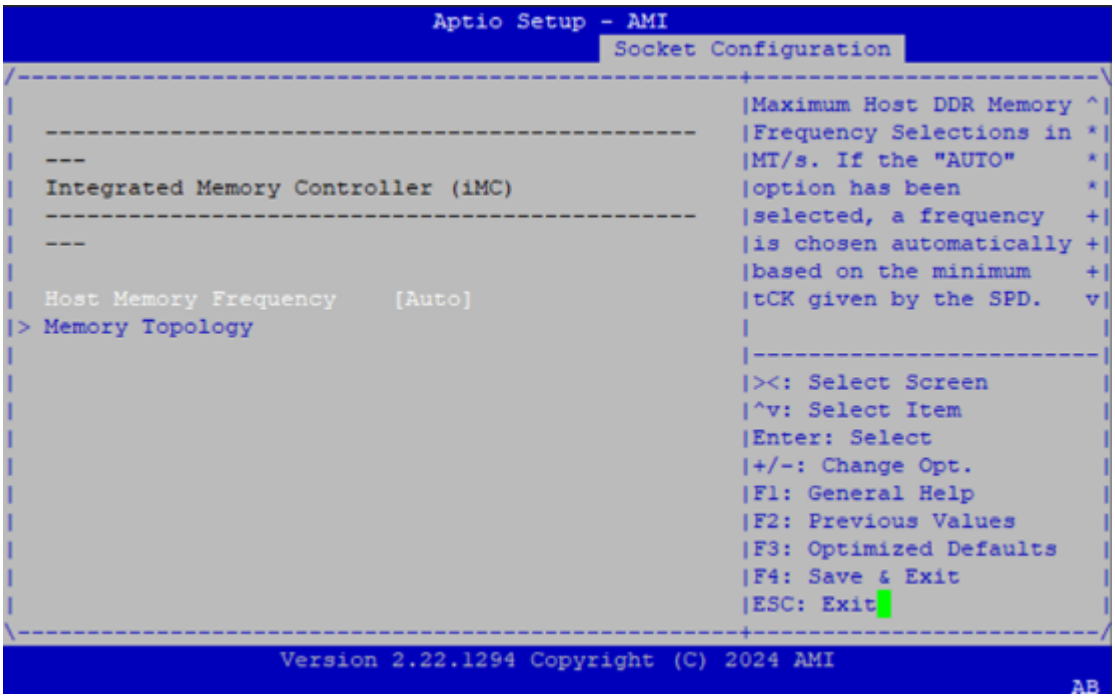


9.15.3 CPU Socket0 Configuration

Feature	Options	Description
Disable Bitmap (Hex)	0	0: Enable all cores. FFFFFFFFFF: Disable all cores least one core per CPU must be enabled. Disabling all cores is an invalid configuration.

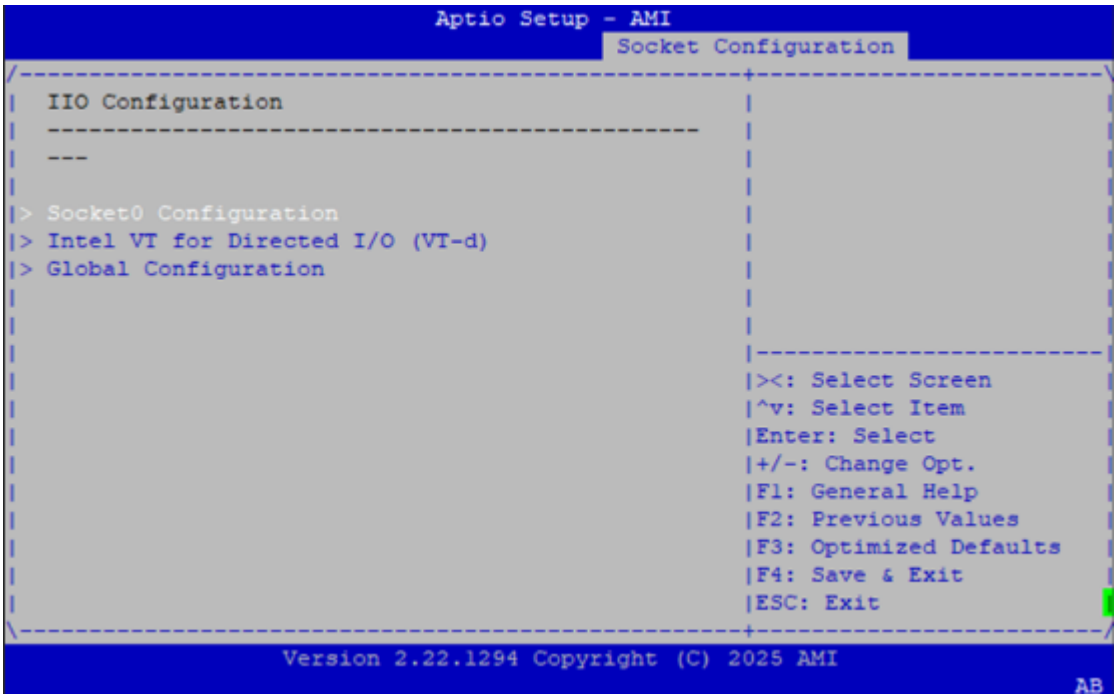


9.15.4 Memory Configuration



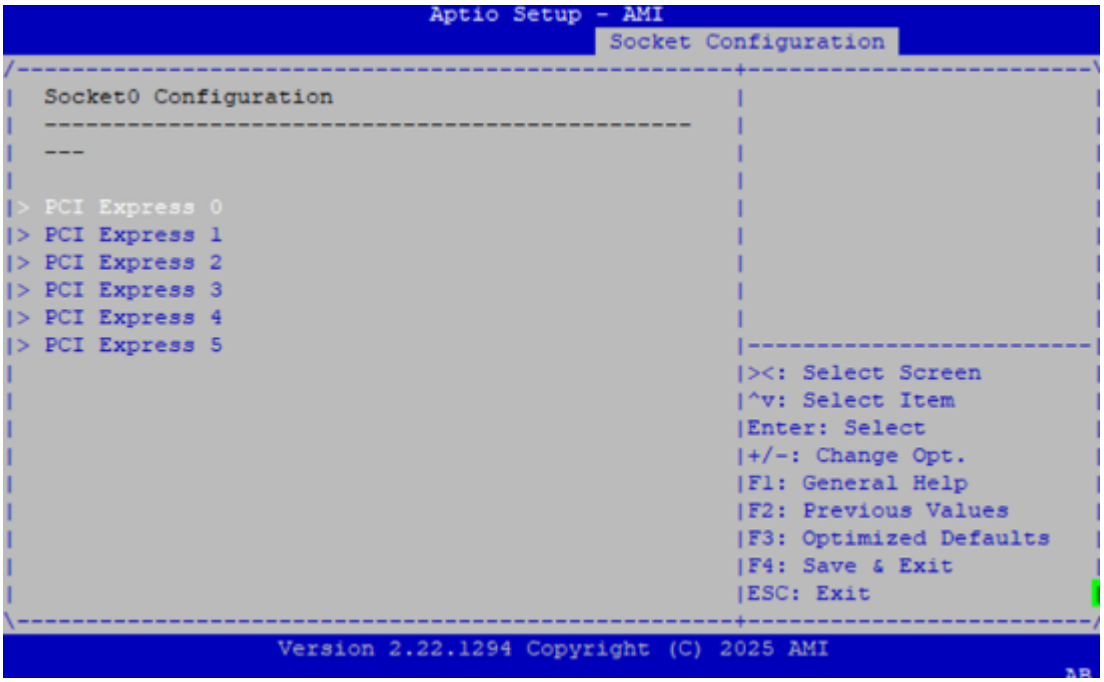
Feature	Options	Description
Host Memory Frequency	Auto 4800 5200 5600 6000 6400	Maximum Memory Frequency Selections in MT/s. If the “AUTO” option has been selected, a frequency is chosen automatically based on the minimum tCK given by the SPD. If Enforce POR is disabled, user will be able to run at higher frequencies than the memory support (limited by processor support)
Memory Topology	None	Displays memory topology with Dimm population information

9.15.5 IIO Configuration



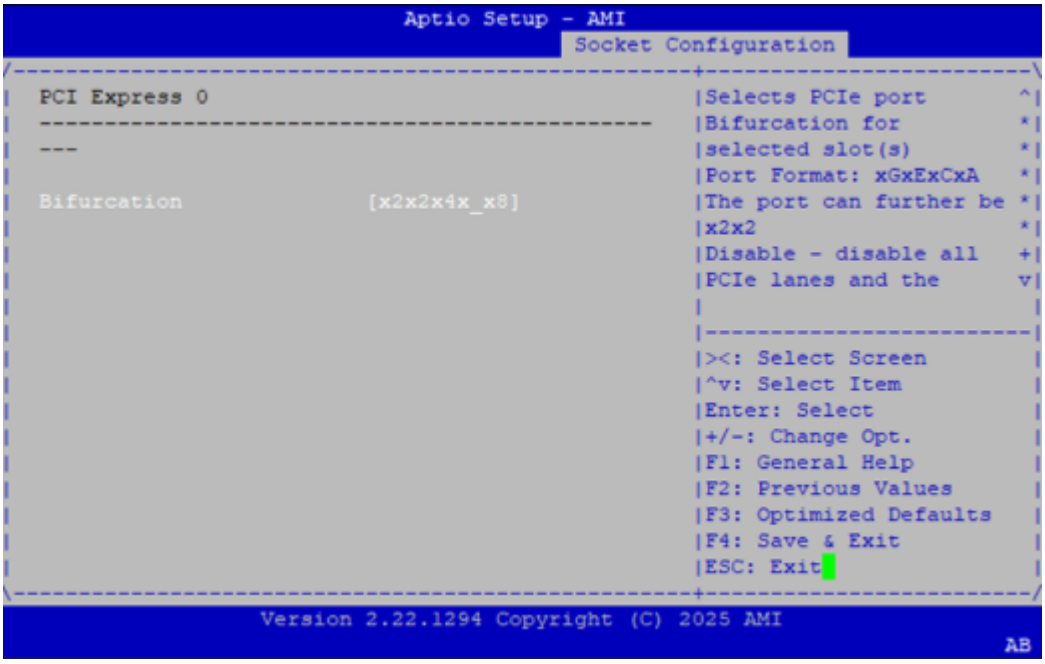
Feature	Options	Description
Socket0 Configuration	None	PCI Express Root Port setting page
Intel VT for Directed I/O (VT-d)	None	Intel VT-d technology setting page. Note: If no understand setting affection, please do not change setting in page
Global Configuration	None	For all PCI Express Root Port setting page

9.15.6 Socket0 Configuration



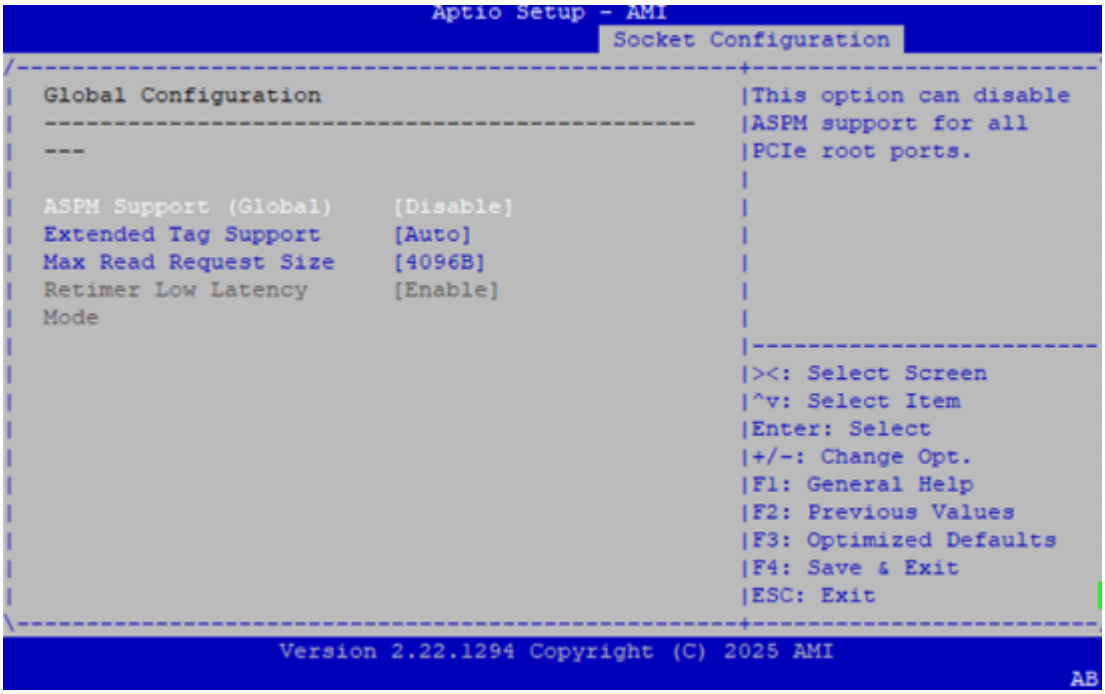
Feature	Options	Description
PCI Express 0~8	None	PCI Express 0~8 can adjust root port setting, such as bifurcation, VMD…etc. Note: Base on HW design, PCI Express 1 will affect BMC and External USB Port

9.15.7 PCI Express 0



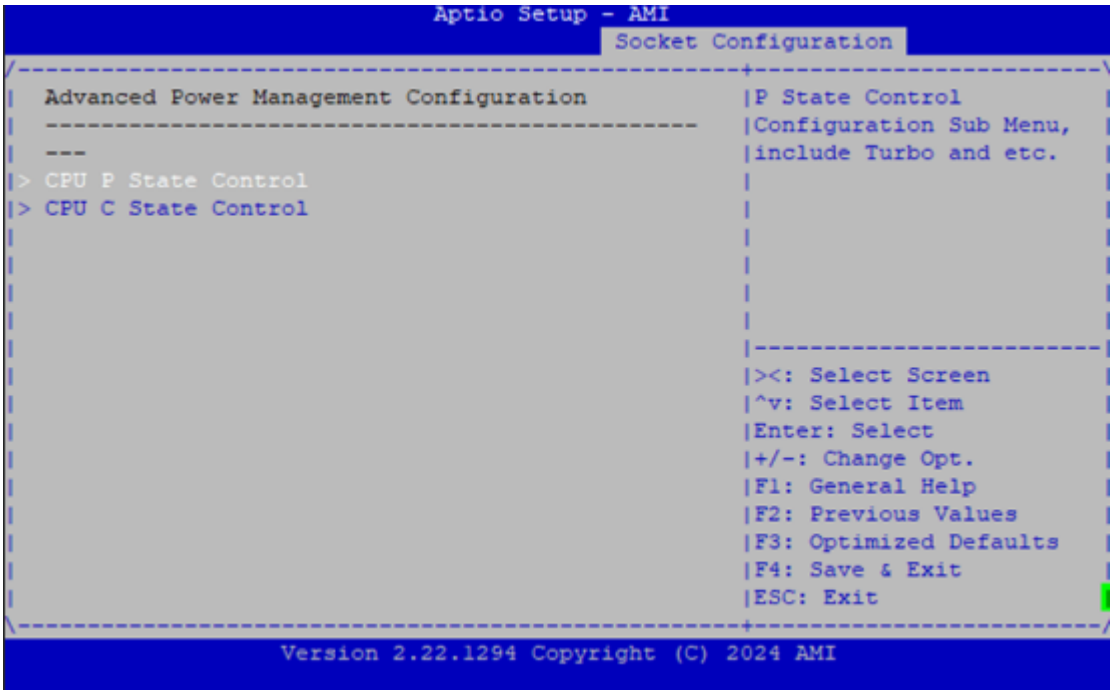
Feature	Options	Description
Bifurcation	Auto x4x4x4x4 x4x4x_x8 x_x8x4x4 x_x8x_x8 x_x_x_x16 x2x2x4x_x8 x4x2x2x_x8 x_x8x2x2x4 x2x2x4x4x4 x4x2x2x4x4 x4x4x2x2x4 x2x2x2x2x_x8 x2x2x2x2x4x4 x2x2x4x2x2x4 x4x2x2x2x2x4 x2x2x2x2x2x2x4 x_x8x4x2x2 x4x4x4x2x2 x_x8x2x2x2x2 x2x2x4x4x2x2 x4x2x2x4x2x2 x4x4x2x2x2x2 x2x2x2x2x4x2x2 x2x2x4x2x2x2x2 x4x2x2x2x2x2x2 x2x2x2x2x2x2x2x2	Selects PCIe port Bifurcation for selected slot(s): “Port Format: xGxExCxA” “The port can further be x2x2” “Disable - disable all PCIe lanes and the controller. Note: if no special device or configuration change, please do not adjust this item

9.15.8 Global Configuration

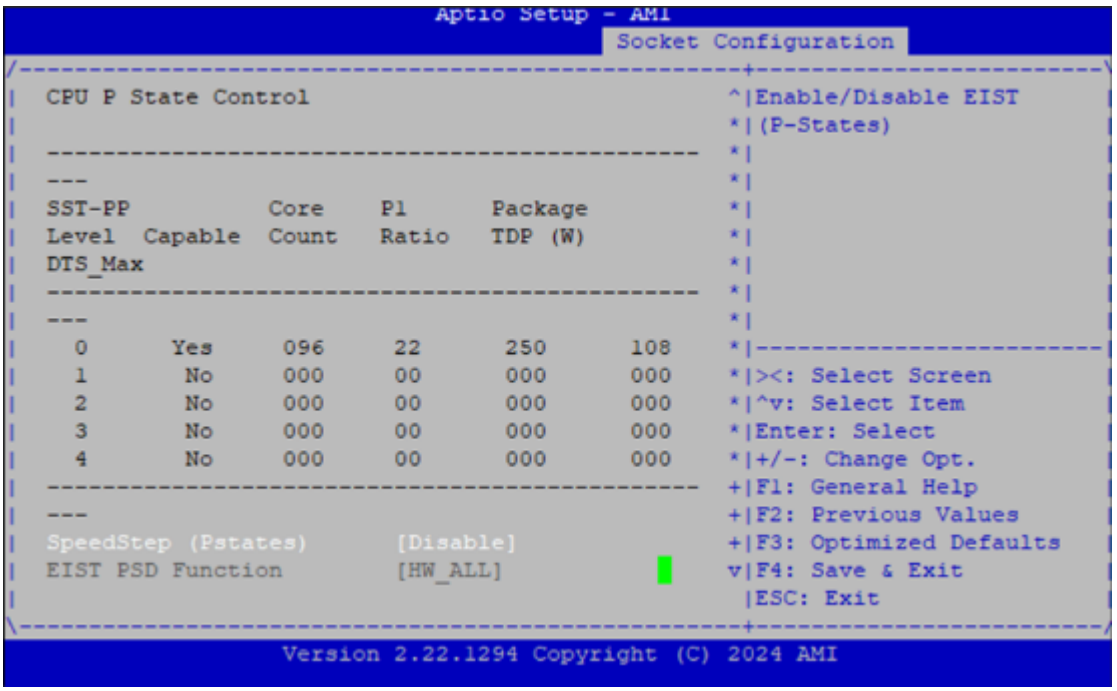


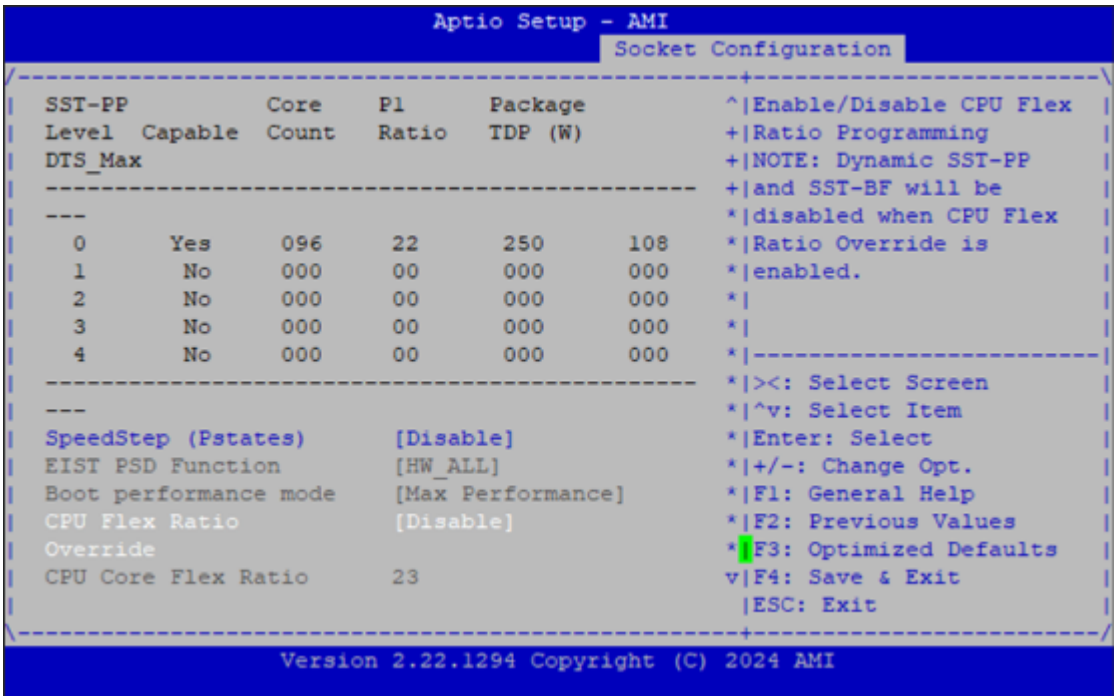
Feature	Options	Description
ASPM Support (Global)	Disable Per-port	This option can disable ASPM support for all PCIe root ports.
Extended Tag Support	Disable Auto	This option can disable 8-bit Tag support in all PCIe root ports. ‘Auto’ keeps hardware default.
Max Read Request Size	Auto 128B 256B 512B 1024B 2048B 4096B	Set Max Read Request Size in End Points

9.15.9 Advanced Power Management Configuration



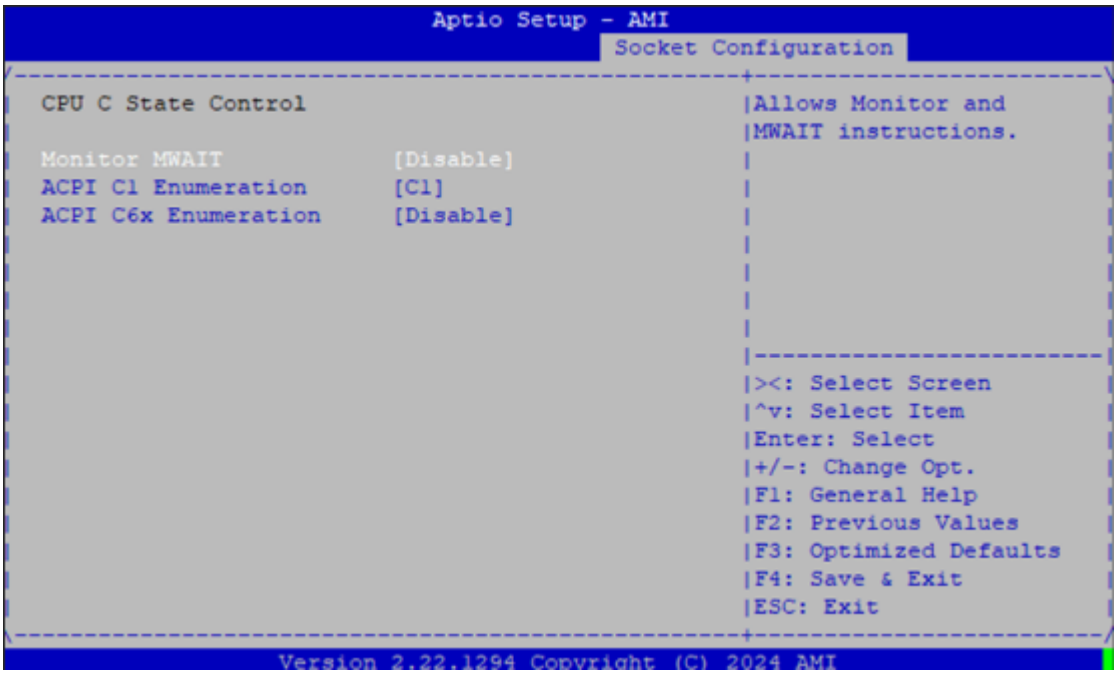
9.15.10 CPU P State Control





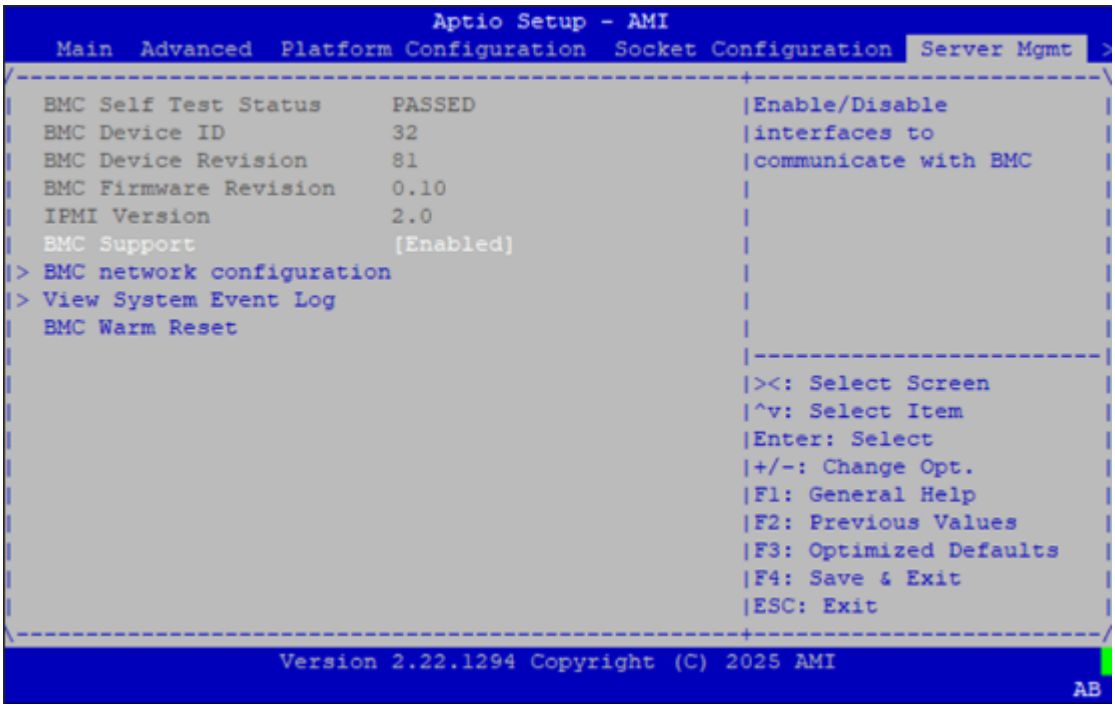
Feature	Options	Description
SpeedStep (Pstates)	Disable Enable	Enables or disables EIST (P-States).
EIST PSD Function	HW_ALL SW_ALL	Choose HW_ALL/SW_ALL in _PSD return.
Boot performance mode	Max Performance Max Efficiency	Select the performance state that the BIOS will set before OS hand off.
Turbo Mode	Disable Enable	Enable/Disable processor Turbo Mode.
Energy Efficient Turbo	Enable Disable	Enable/Disable Energy Efficient Turbo. Enable: MSR 0x1FC Bit[19] = 0 Disable: MSR 0x1FC Bit[19] = 1.
CPU Flex Ratio	Disabled	Enable/Disable CPU Flex Ratio Programming.
Override	Enabled	Note: Dynamic SST-PP and SST-BF will be disabled when CPU Flex Ratio Override is enabled.
CPU Core Flex Ratio	23	Non-Turbo Mode Processor Core Ratio Multiplier.

9.15.11 CPU C State Control



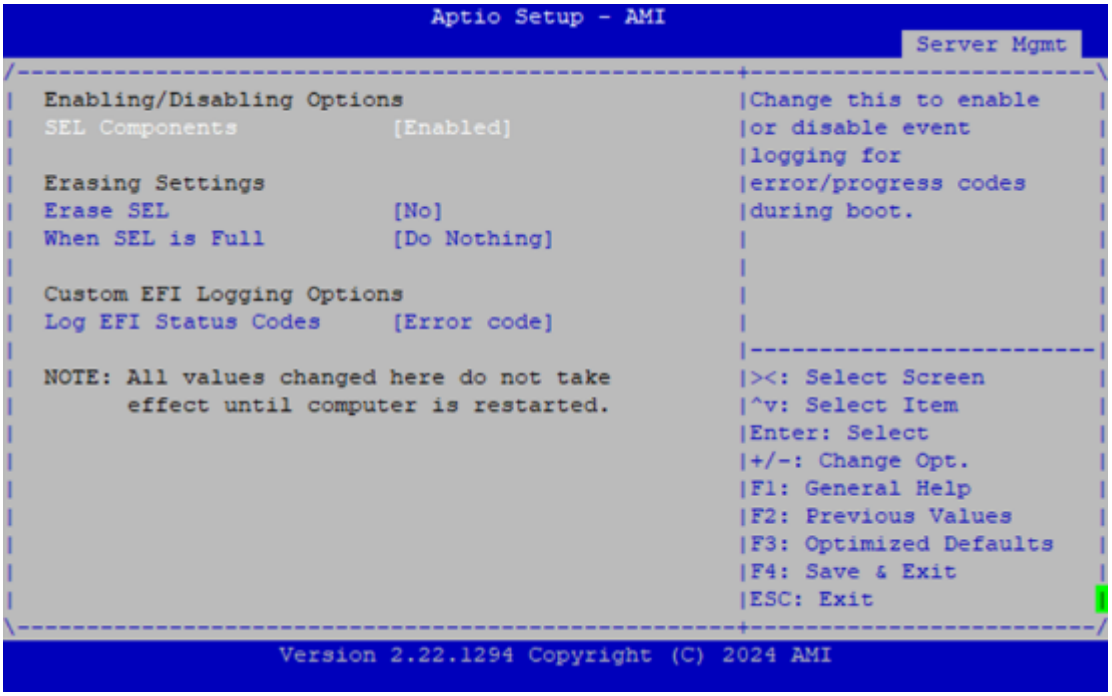
Feature	Options	Description
Monitor MWAIT	Disable Enable	Allows Monitor and MWAIT instructions.
ACPI C1 Enumeration	C1 C1e	Enumerate C1/C1e as ACPI C1.
ACPI C6x Enumeration	Disable C6S as ACPI C2 C6S as ACPI C3 C6S-P as ACPI C2 C6S-P as ACPI C3 Auto	AUTO: Maps to C6S-P as ACPI C2 Disable: Don't enumerate any C6S state in ACPI C6S as ACPI C2/C3: Enumerate C6S as ACPI C2/C3 state. PkgC6 is not allowed C6S-P as ACPI C2/C3: Enumerate C6S-P as ACPI C2/C3 state. PkgC6 is allowed.

9.16 Server Mgmt



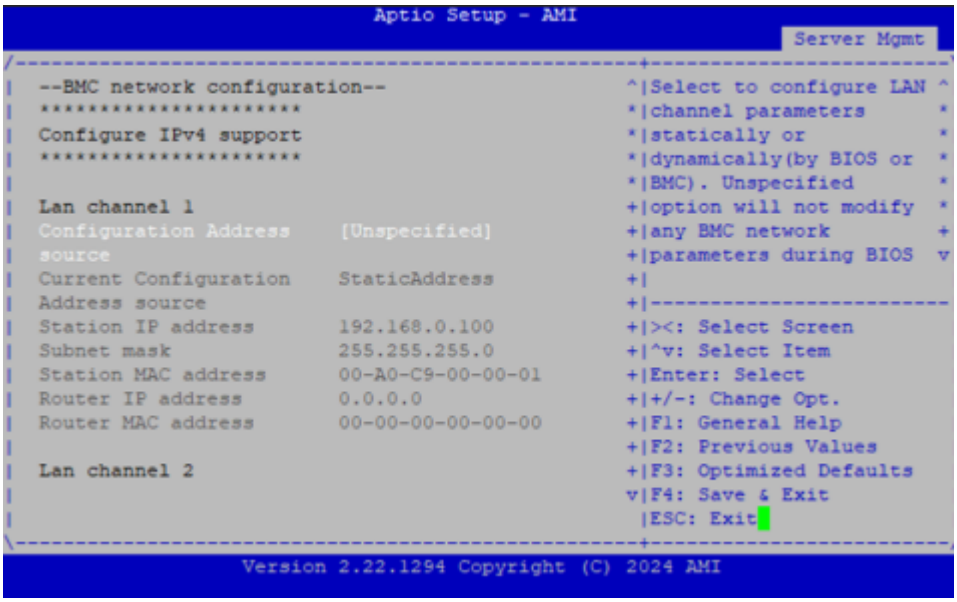
Feature	Options	Description
BMC Support	Enable Disable	Enable or disables interfaces to communicate with BMC.
BMC network configuration	NA	Configure BMC network parameters.
View System Event Log	NA	Press to view the System Event Log Records.
BMC Warm Reset	NA	Press to do Warm Reset BMC.

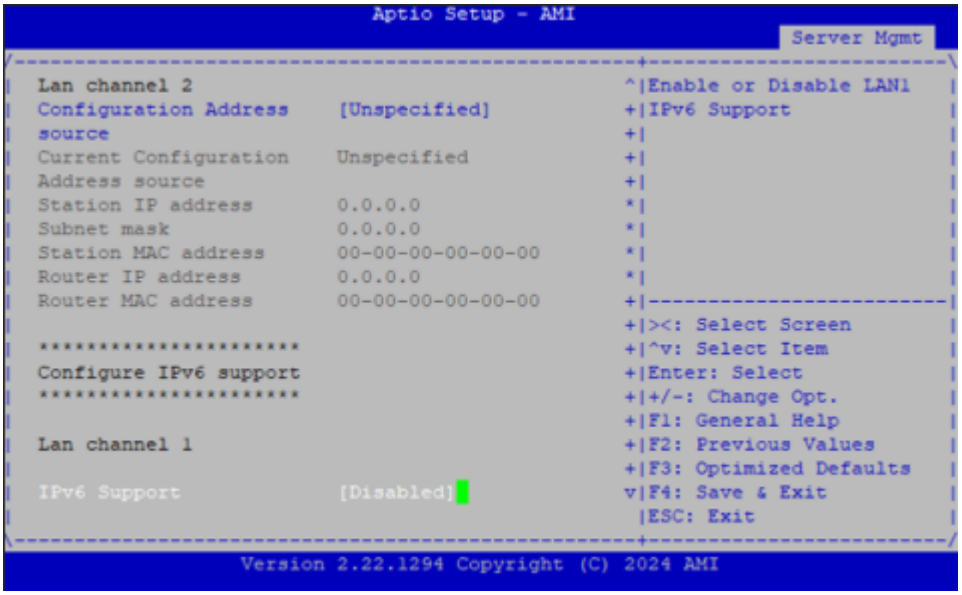
9.16.1 System Event Log

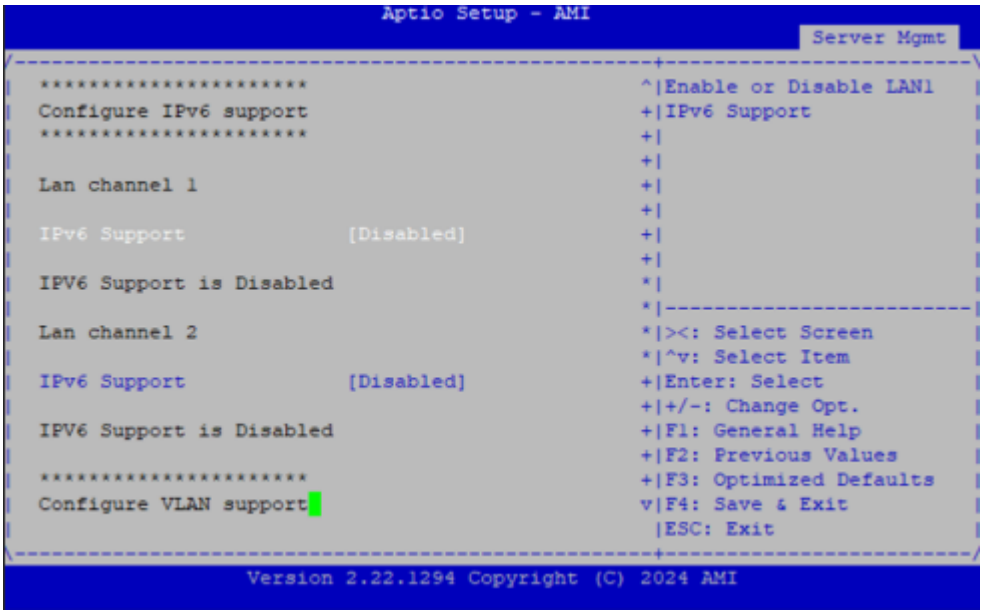


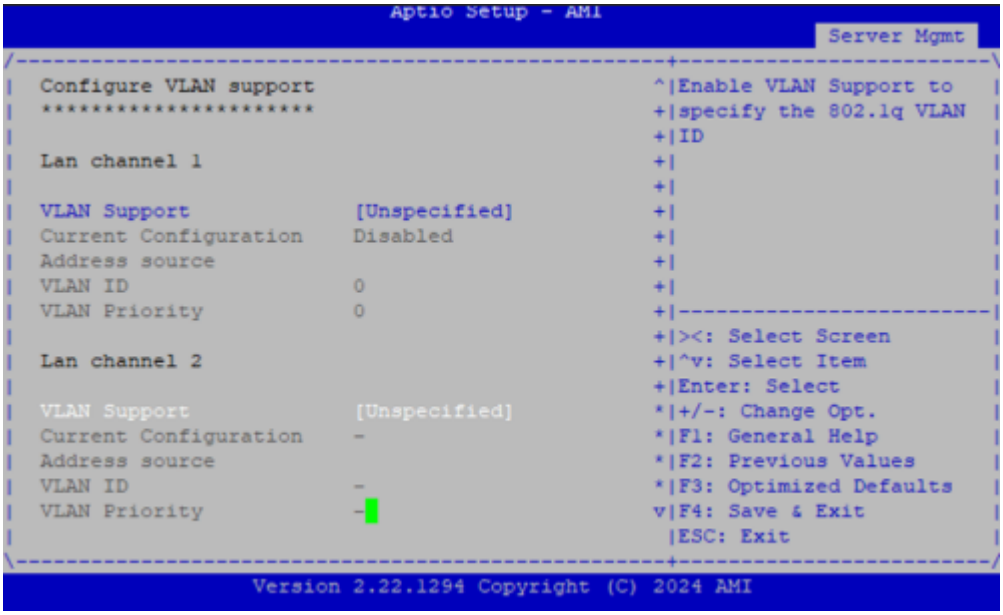
Feature	Options	Description
SEL Components	Enable Disable	Change this to enable or disable event logging for error/progress codes during boot.
Erase SEL	NO Yes, On next reset Yes, On every reset	Choose options for erasing SEL.
When SEL is Full	Do Nothing Erase Immediately Delete Oldest Record	Choose options for reactions to a full SEL.
Log EFI Status Codes	Disabled Both Error code Progress code	Disable the logging of EFI Status Codes or log only error code or only progress code or both.

9.16.2 BMC Network Configuration



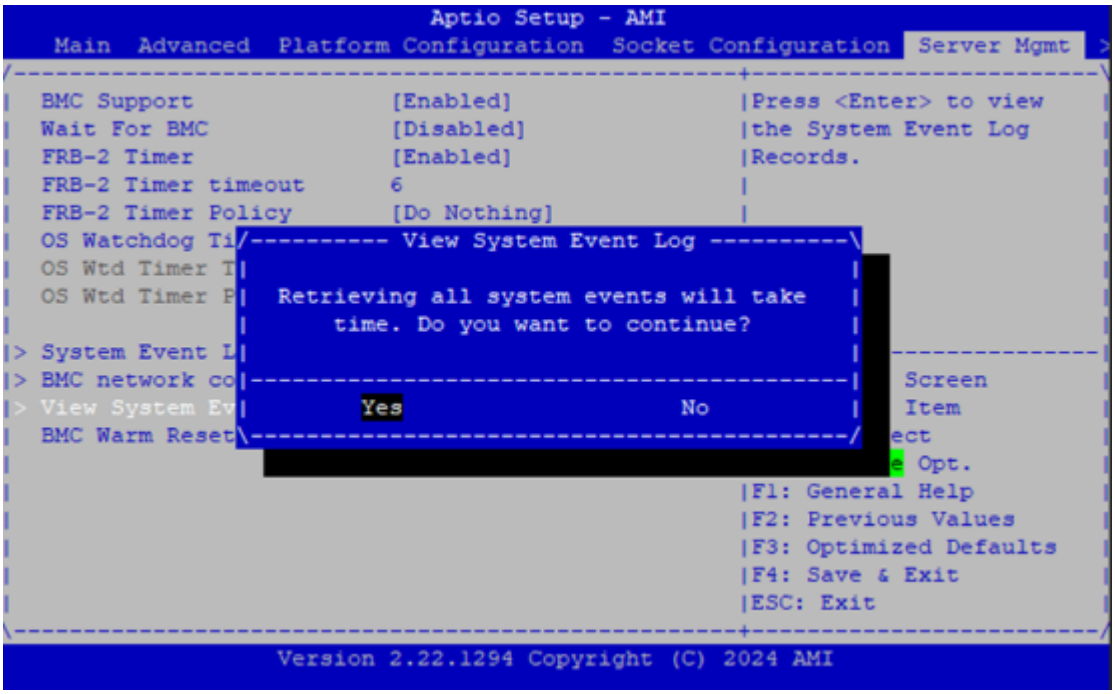






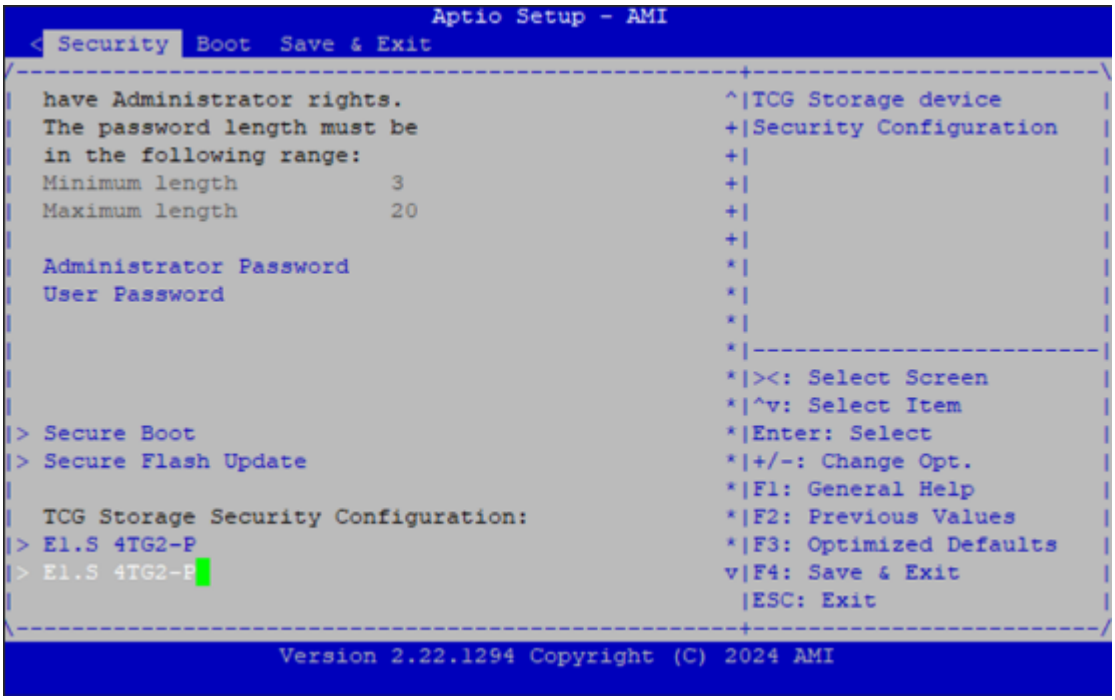
Feature	Options	Description
Configuration Address source	Unspecified Static DynamicBmcDhcp	Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). The unspecified option will not modify any BMC network parameters during BIOS phase.

9.16.3 View System Event Log



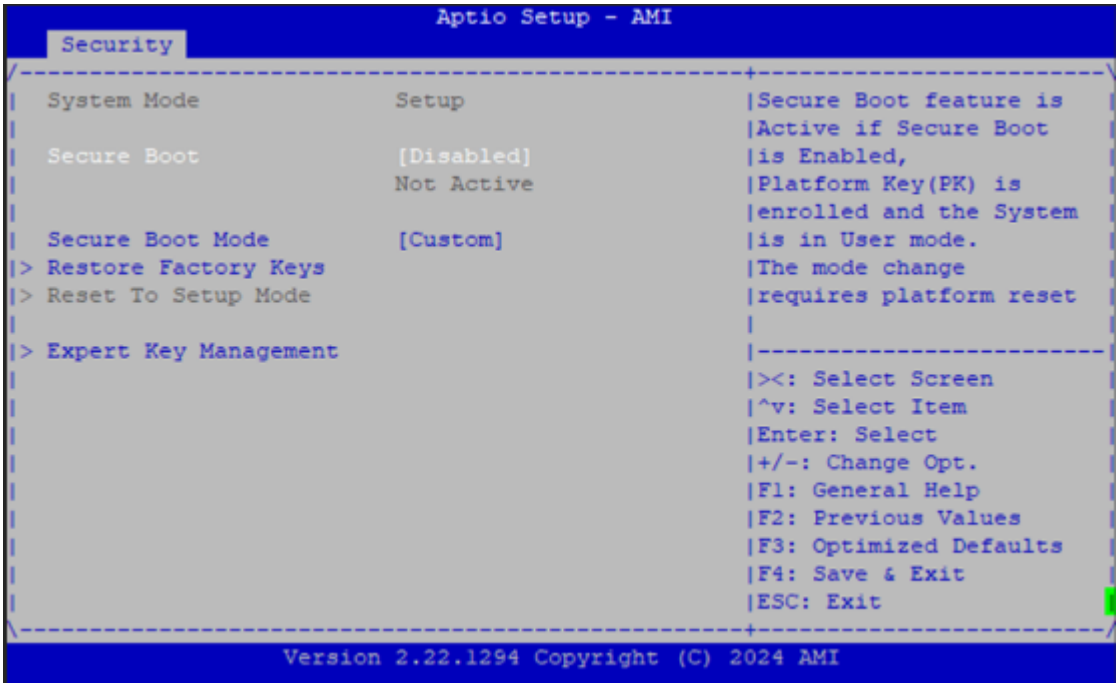
9.17 Security

Select the Security menu item from the BIOS setup screen to enter the Security Setup screen. Users can select any of the items in the left frame of the screen.



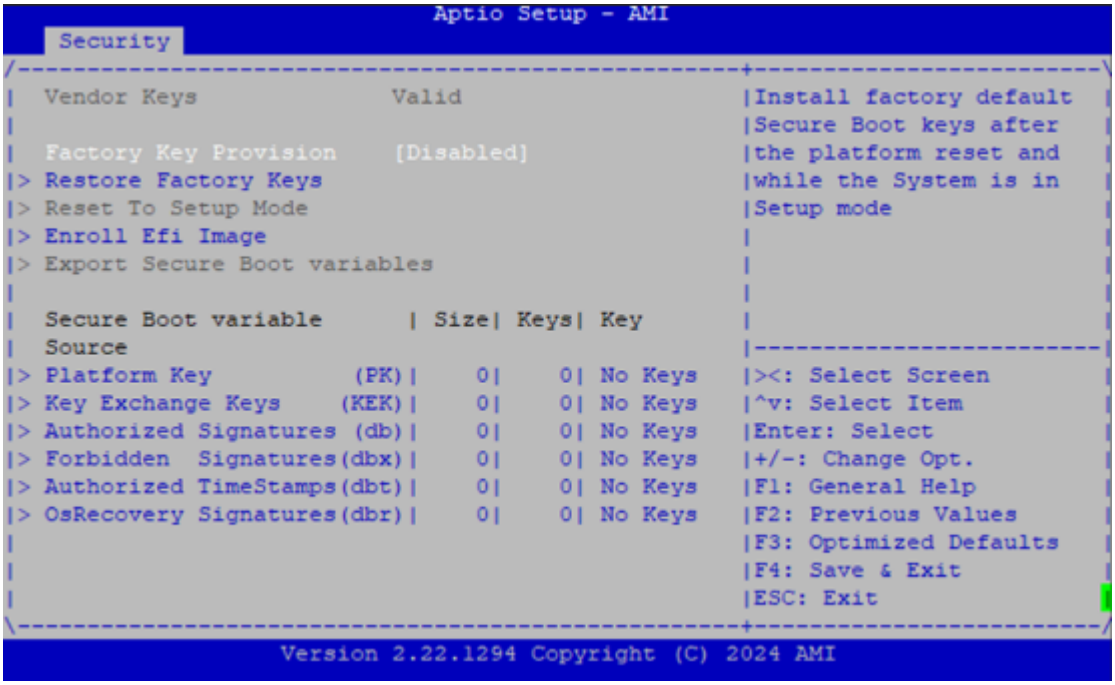
Feature	Description
Administrator Password	If ONLY the Administrator's password is set, it only limits access to Setup and is only asked for when entering Setup.
User Password	If ONLY the User's password is set, it serves as a power-on password and must be entered to boot or enter Setup. In Setup, the User will have Administrator rights.

9.17.1 Secure Boot



Feature	Options	Description
Secure Boot	Disable Enable	Secure Boot feature is Active if Secure Boot is Enabled, Platform Key(PK) is enrolled and the System is in User mode. The mode change requires platform reset.
Secure Boot Mode	Standard Custom	

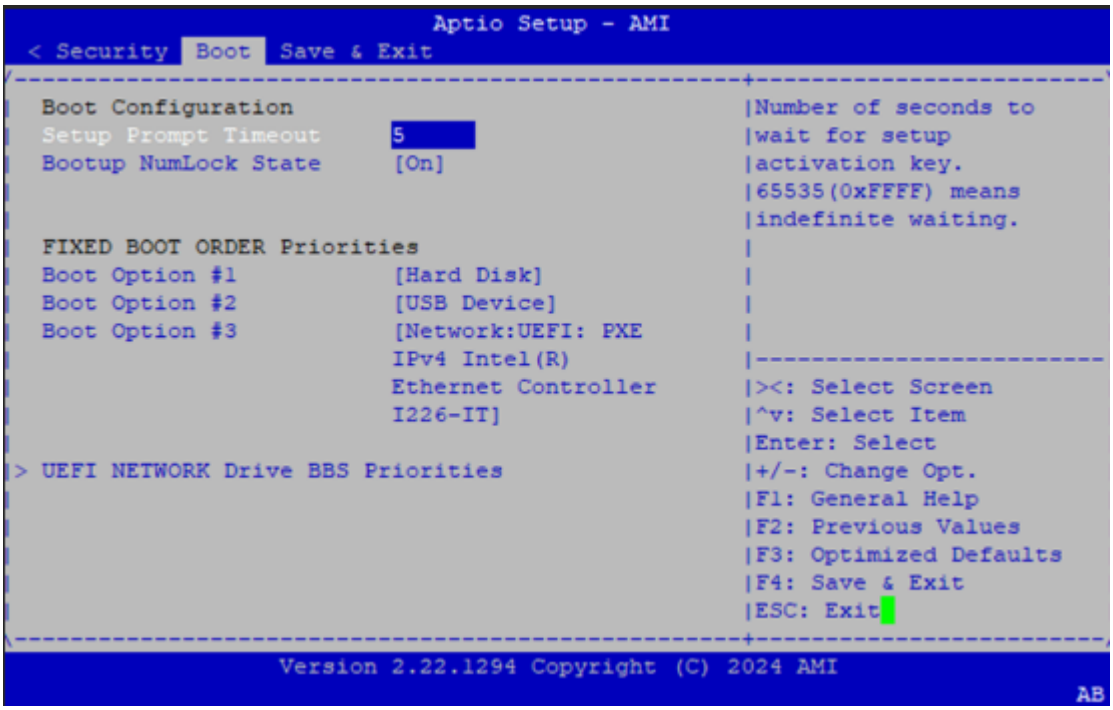
9.17.2 Key Management



Feature	Options	Description
Factory Key Provision	Disable Enable	Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode.
Restore Factory keys	None	Force System to User Mode. Install factory default Secure Boot key databases.
Enroll Efi Image	None	Allow Efi image to run in Secure Boot mode. Enroll SHA256 Hash certificate of a PE image into Authorized Signature Database (db).

9.18 Boot Menu

Select the Boot menu item from the BIOS setup screen to enter the Boot Setup screen. Users can select any of the items in the left frame of the screen.

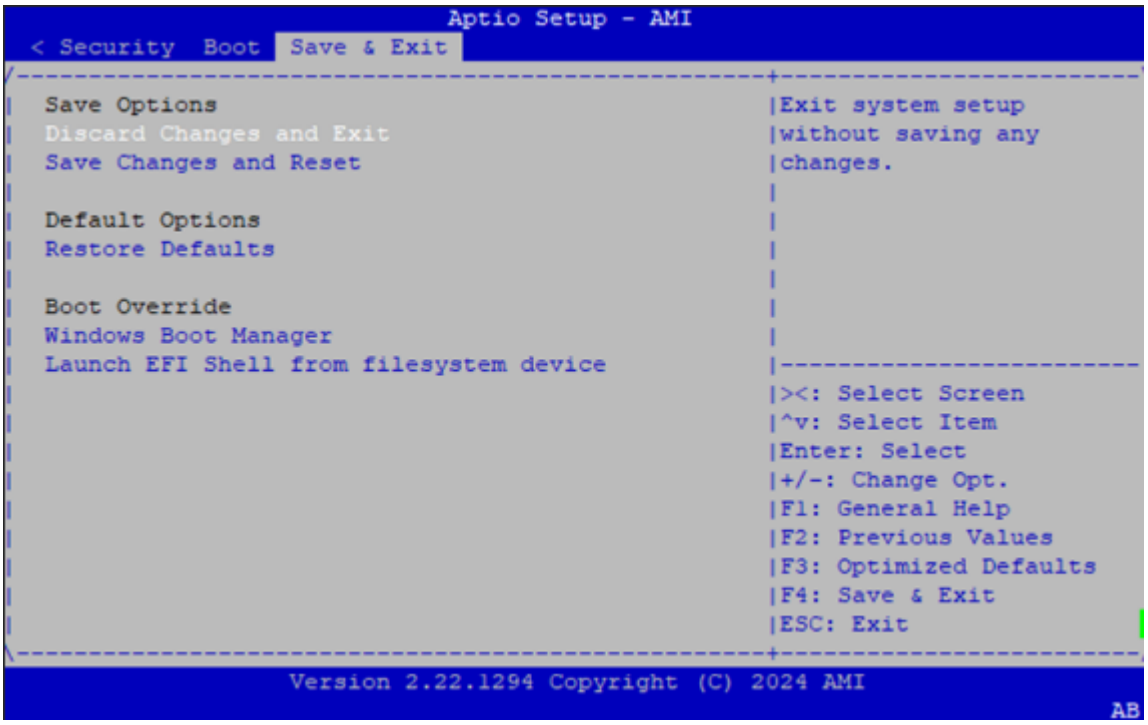


Feature	Options	Description
Setup Prompt Timeout	5	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.
Bootup NumLock State	On Off	Select the keyboard NumLock state

- Choose boot priority from boot option group.
- Choose specific boot device priority sequence from available Group device.

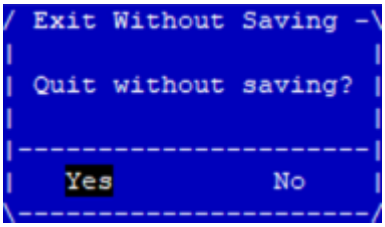
9.19 Save and Exit Menu

Select the Save and Exit menu item from the BIOS setup screen to enter the Save and Exit Setup screen. Users can select any of the items in the left frame of the screen.



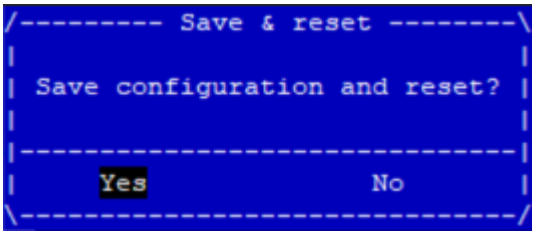
9.19.1 Discard Changes and Exit

- Select this option to quit Setup without saving any modifications to the system configuration. The following window will appear after the “Discard Changes and Exit” option is selected. Select “Yes” to discard changes and Exit Setup.



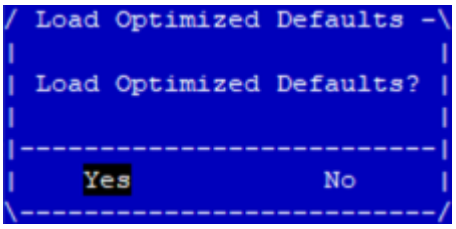
9.19.2 Save Changes and Reset

- When Users have completed the system configuration changes, select this option to save the changes and reset from BIOS Setup in order for the new system configuration parameters to take effect. The following window will appear after selecting the “Save Changes and Reset” option is selected. Select “Yes” to Save Changes and reset.



9.19.3 Restore Defaults

- Restore default values for all setup options. Select “Yes” to load Optimized defaults.



Note: The items under Boot Override may not be the same a the image above, as it should depend on the actual devices connect to the system.

9.20 Intel® RAID Key Configuration

9.20.1 Configuring Intel VMD and Creating a RAID Volume

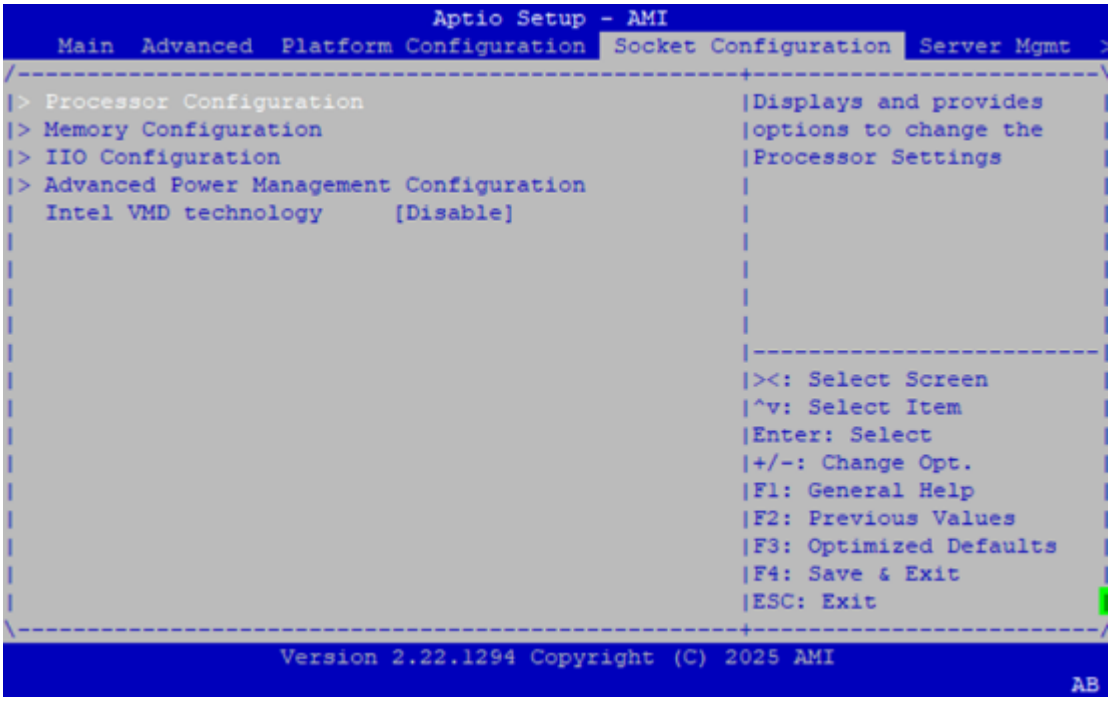
Step 1: Install the VROC Key

1. Connect the VROC key to the motherboard’s JRAID_CON1 header.

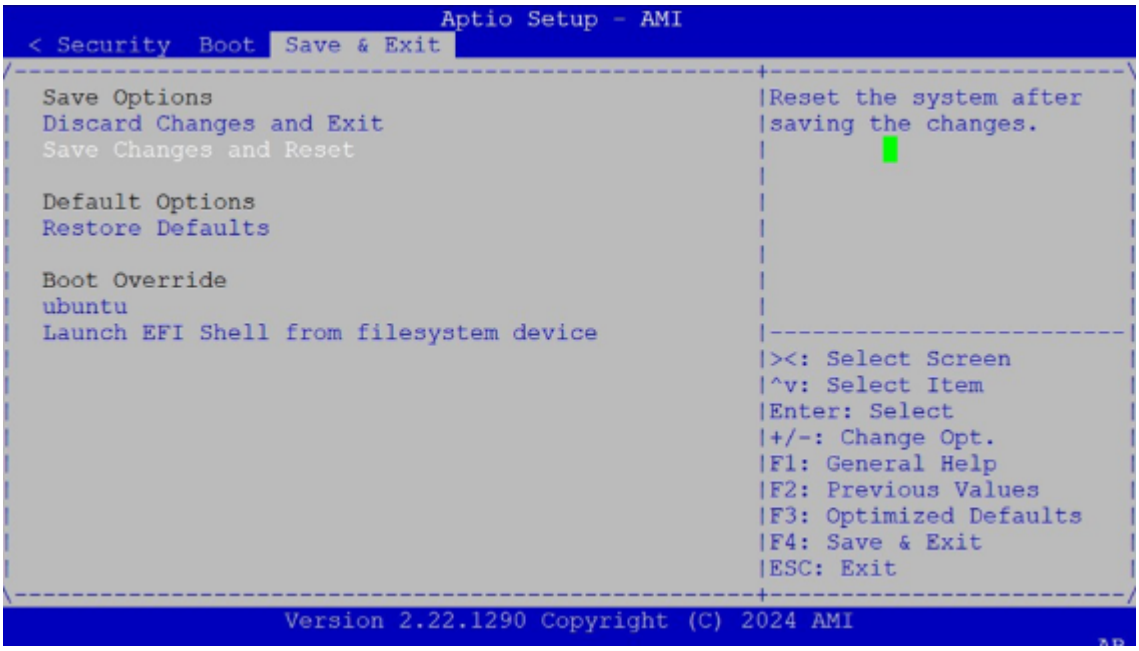
![alt text](Pics/VROC Key.png)

Step 2: Boot into BIOS

1. Boot into BIOS à Navigate to Socket Configuration and set Intel VMD Technology to Enabled

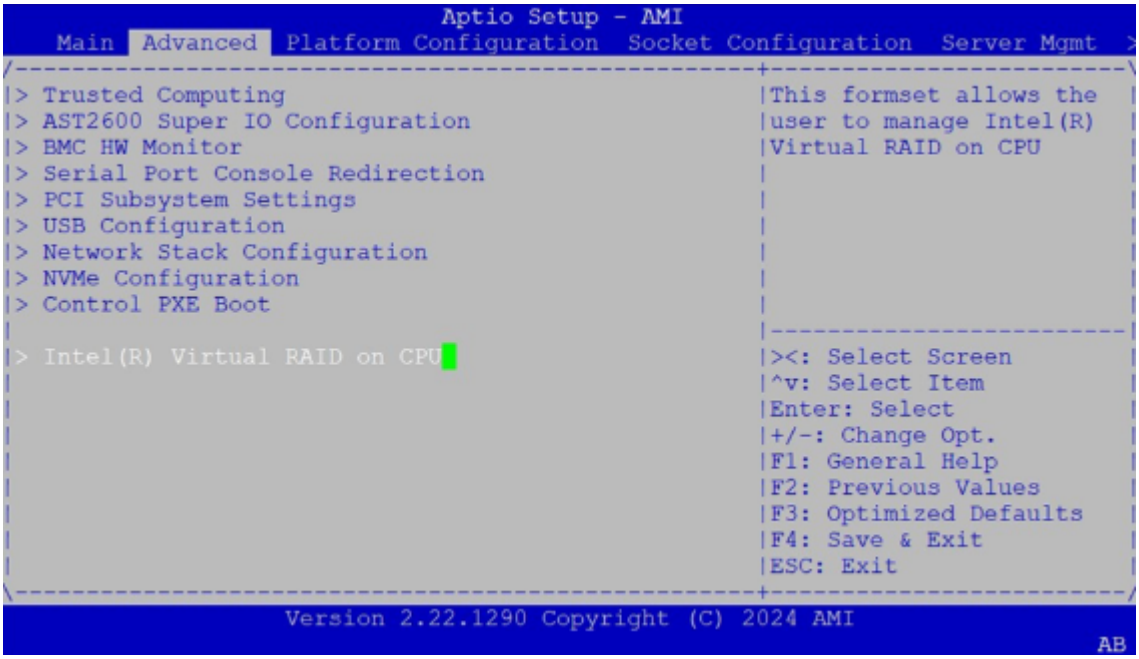


2. Save & Exit: Choose Save Changes and Reset to reboot the system.



Step 3: Re-enter BIOS

1. After reboot, enter BIOS again.
2. Navigate to Advanced > Intel Virtual RAID on CPU > All Intel VMD Controllers.



3. Select Create RAID Volume, then choose the desired RAID Level.
4. Select the storage devices to include in the RAID array.
5. Click Create Volume, then confirm with Yes.
6. Exit BIOS.

Step 4: Boot into the OS

Use the command lsblk to verify the RAID volume. It will appear as /dev/mdxxx