Ampere® Altra® 64-Bit Multi-Core Processor

Aptio® V UEFI User's Manual

June 29, 2021

Document Issue 0.92

Contents

Contents (continued)

Contents (continued)

Figures

Figures (continued)

Tables

1. Overview

This manual describes the functions and usage of the Ampere® Altra® Aptio® V Unified Extensible Firmware Interface (UEFI) firmware.

This manual contains advance information. Screen captures of the Aptio® V UEFI firmware user interface are examples from previously released Ampere Computing products.

For information about porting UEFI to various platforms, refer to *Ampere® Altra® Aptio® V UEFI BIOS Porting Guide*.

2. Power-On Self-Test (POST) Screen

The first page displayed when the system starts before booting is the POST screen. There are two kinds of POST screens:

- Normal POST screen: The screen which contains the Logo and copyright messages
- Quiet POST screen

The normal POST screen contains the AMI logo, copyright, and version and product information.

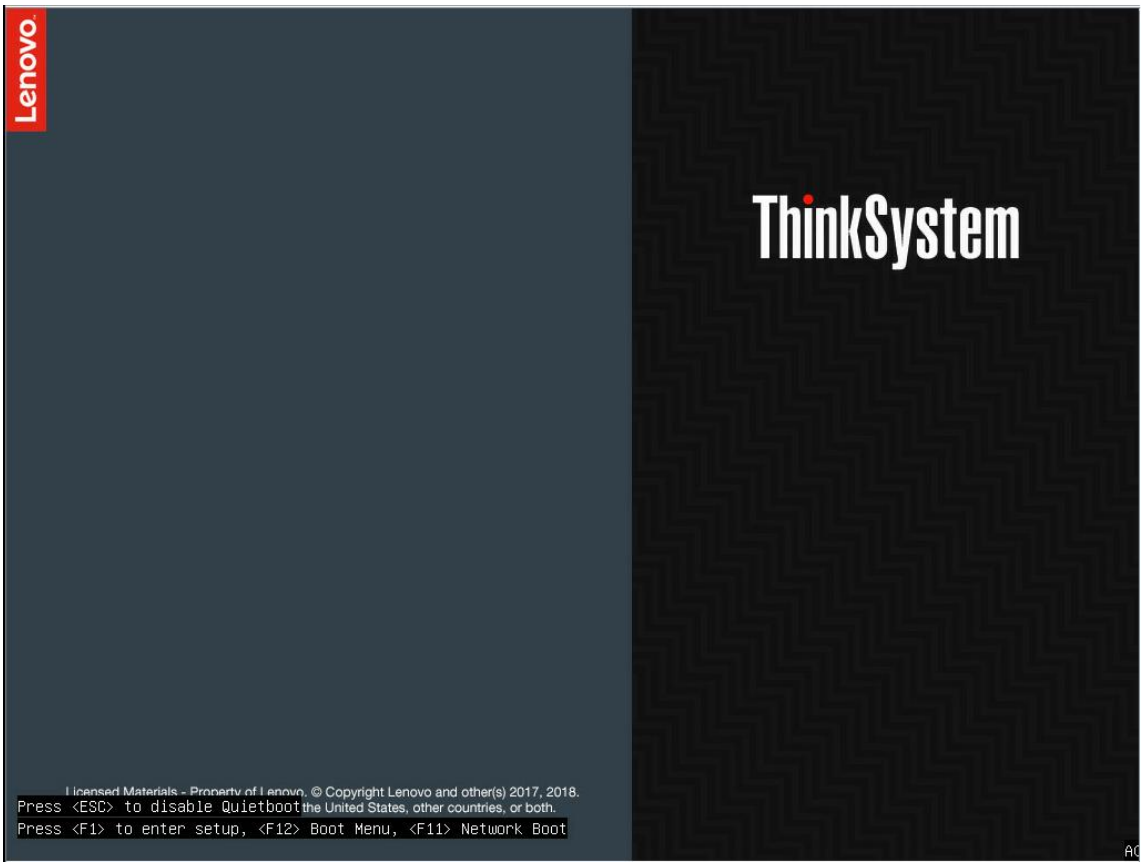
Figure 1: Normal POST Screen

The normal POST screen shows this information:

- Firmware and BIOS versions
- BIOS date

The Quiet POST screen, shown in *Figure 2*, contains only the system logo. By default, the quiet POST screen is enabled. Users can press the ESC key to disable quiet boot and display the normal POST screen.

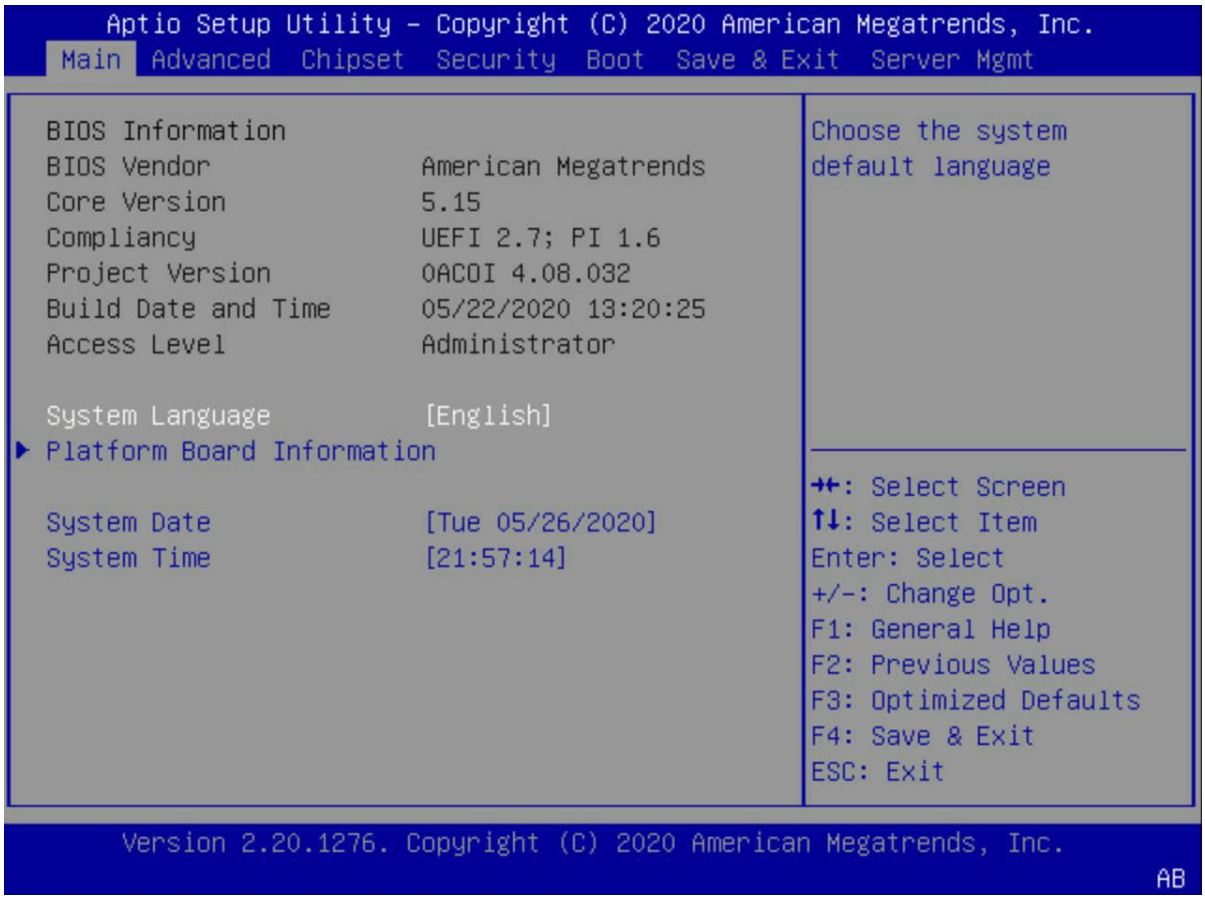
Figure 2: Quiet POST Screen



3. Main Tab

The Main tab provides additional UEFI and system information. On this and other Aptio V screens, UEFI is often called BIOS.

Figure 3: Main Tab



3.1 BIOS Information

The Main tab provides the following information:

- **BIOS Vendor:** American Megatrends
- **Core Version:** Aptio V version. The current version is 5.15.
- **Compliance:** UEFI 2.7; PI 1.6
- **BIOS Build ID:** The BIOS Build ID defined in the document titled *Ampere® Altra® UEFI Functional Specification*
- **BIOS Version:** BIOS release version
- **Build Date and Time:** BIOS build date and time
- **Access Level:** User access level

3.2 System Language

The Main tab enables users to change the displayed language. Currently, only English is supported.

3.3 System Date and Time

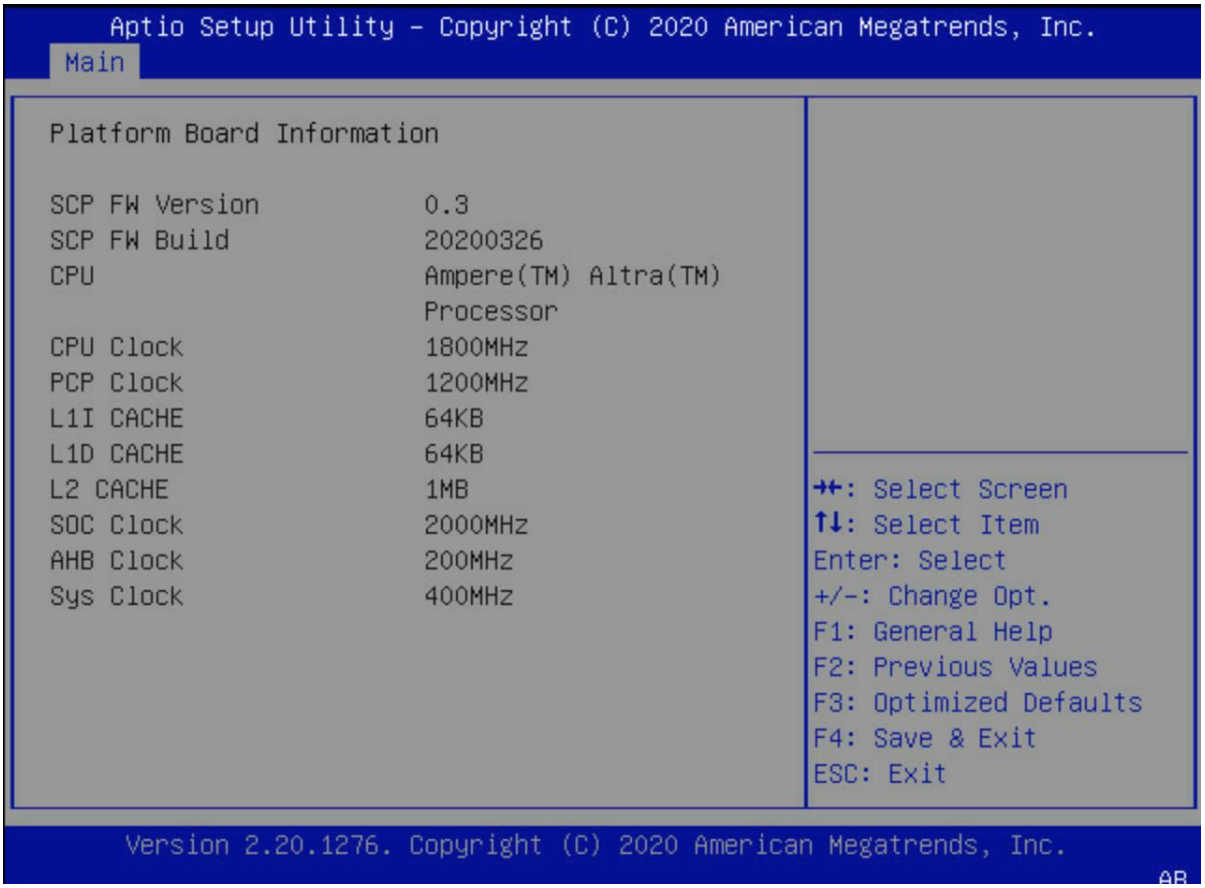
The Main tab enables users to change the system date and time and date using the following steps:

1. Highlight System Time or System Date using the up and down arrow keys.
2. Enter new values using the keyboard.
3. Use the Tab key or the arrow keys to move between fields.
4. The date must be entered in Date MM/DD/YYYY format.
5. The time is entered in HH:MM:SS format.

3.4 Platform Board Information

This screen displays general information about the platform, including SCP firmware information, processor, clocks, and caches.

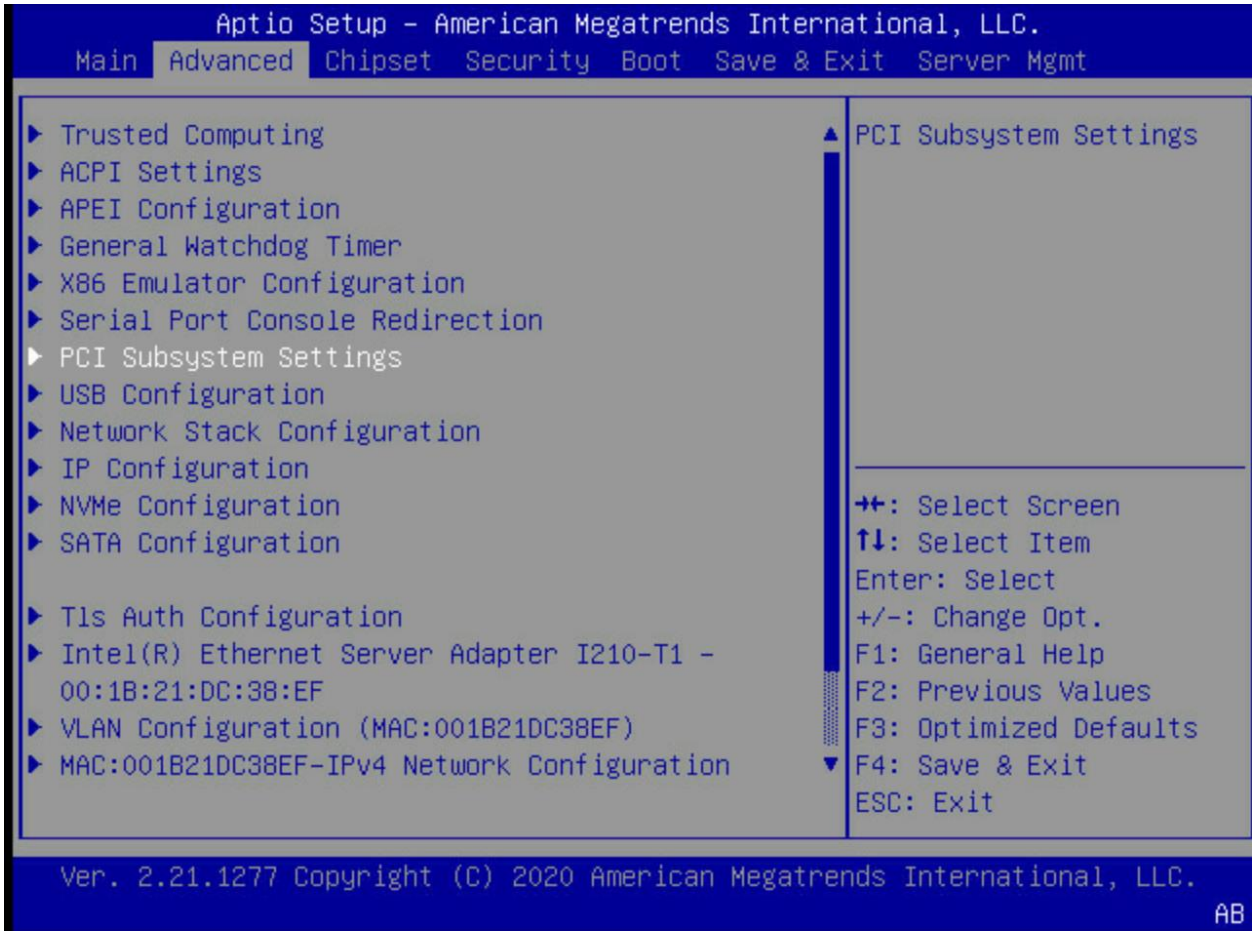
Figure 4: Platform Board Information



4. Advanced Tab

Use the left or right arrow keys to select the Advanced tab. Use the up or down arrow keys to select items in the left pane of the tab. Use the Enter key to display available submenus for a selected item.

Figure 5: Advanced Tab Screen



If the system is unstable after changing any settings in advanced configuration, revert to the default settings on the Save & Exit tab.

4.1 Trusted Computing Settings

This screen displays the details of Trusted Platform Module (TPM) device and displays options to enable and disable TPM features.

Figure 6: Trusted Computing Settings Screen (1 of 2)

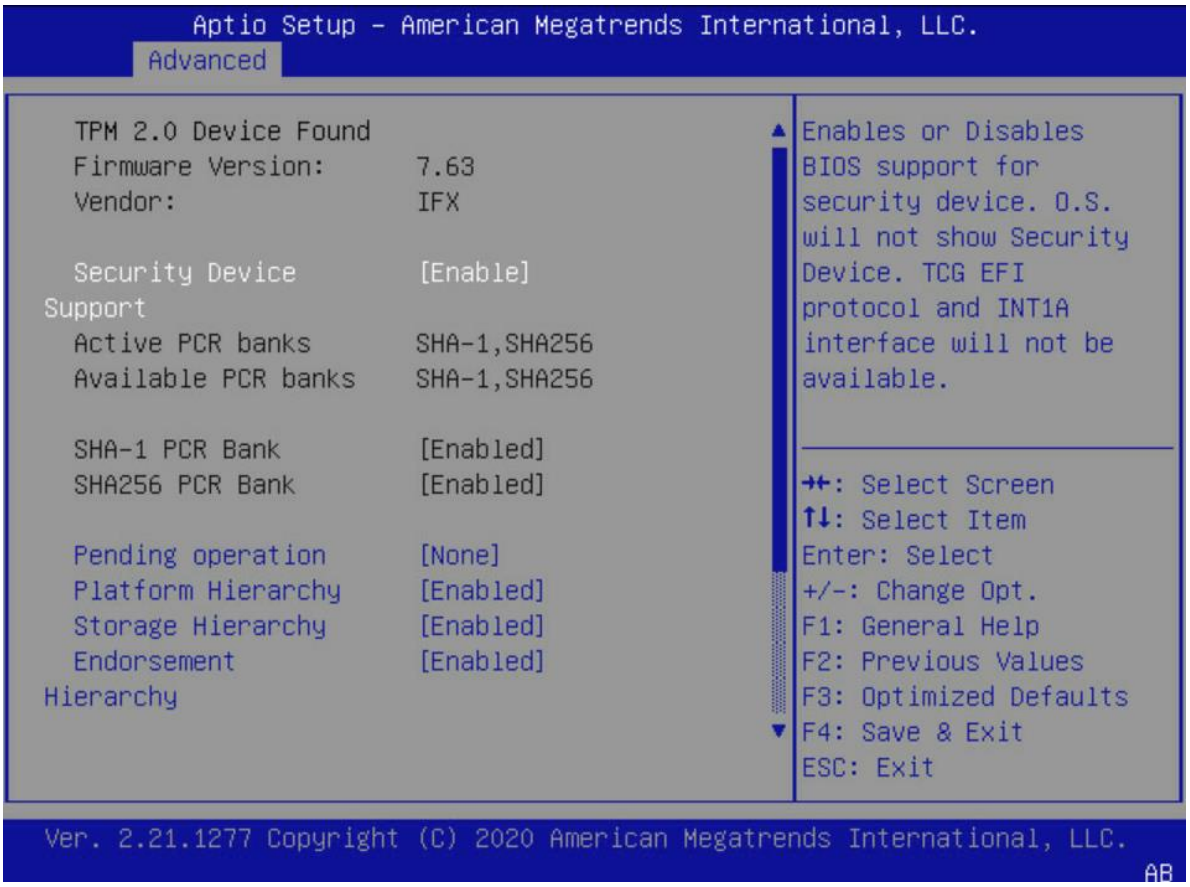


Figure 7: Trusted Computing Settings Screen (2 of 2)

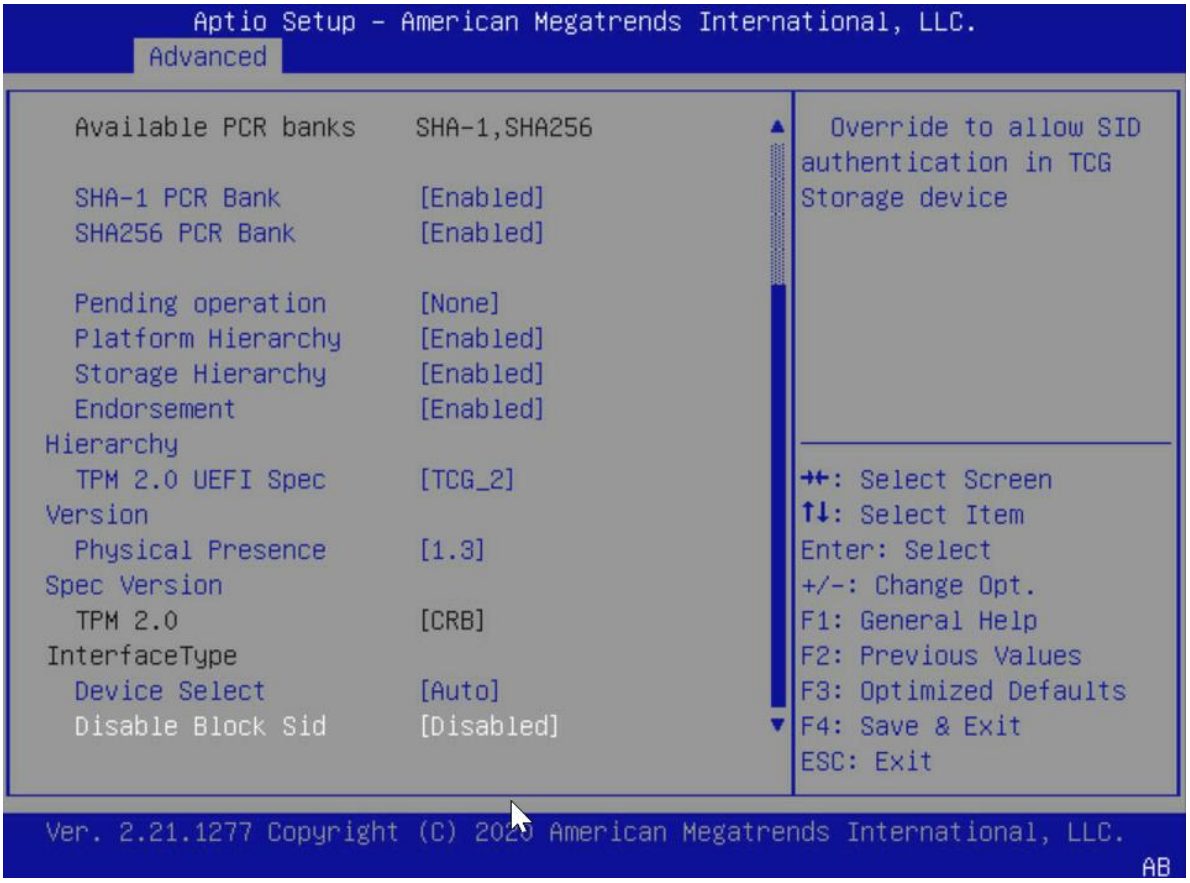


Table 1: Trusted Computing Settings

TRUSTED COMPUTING SETTINGS	DESCRIPTION
Security Device Support	Select **Enable** or Disable to enable or disable the Security TPM Device Support.
SHA-1 Platform Configuration Register (PCR) Bank	Select **Enabled** or Disabled to enable or disable the SHA-1 PCR Bank.
SHA256 PCR Bank	Select **Enabled** or Disabled to enable or disable the SHA256 PCR Bank.
Pending Operation	Schedule an operation for security Device. Selecting **None** does nothing. Selecting TPM Clear clears the TPM and causes a reboot.
Platform Hierarchy	Select **Enabled** or Disabled to enable or disable the Platform Hierarchy.
Storage Hierarchy	Select **Enabled** or Disabled to enable or disable the Storage Hierarchy.
Endorsement Hierarchy	Select **Enabled** or Disabled to enable or disable the Endorsement Hierarchy.
TPM 2.0 UEFI Spec Version	Select **TCG_2** to support the Trusted Computing Group TCG2 protocol and event. Select TCG_1_2 to support the TCG1.2 protocol and event.
Physical Presence Spec Version	Select whether the OS supports TCG PC Client Physical Presence Interface (PPI) Specification 1.2 or **1.3**.
Device Select	Select TPM 1.2 to restrict support to TPM 1.2 devices. Select TPM 2.0 to restrict support to TPM 2.0 device.

TRUSTED COMPUTING SETTINGS	DESCRIPTION
	Select **Auto** to select both with default set to TPM 2.0 if no TPM 1.2 device is found.
Disable Block Sid	Select Enabled or **Disabled** to enable or disable override to allow Secure ID (SID) authentication in the TCG storage device.

4.2 Advanced Configuration and Power Interface (ACPI) Settings

Figure 8: ACPI Settings Screen

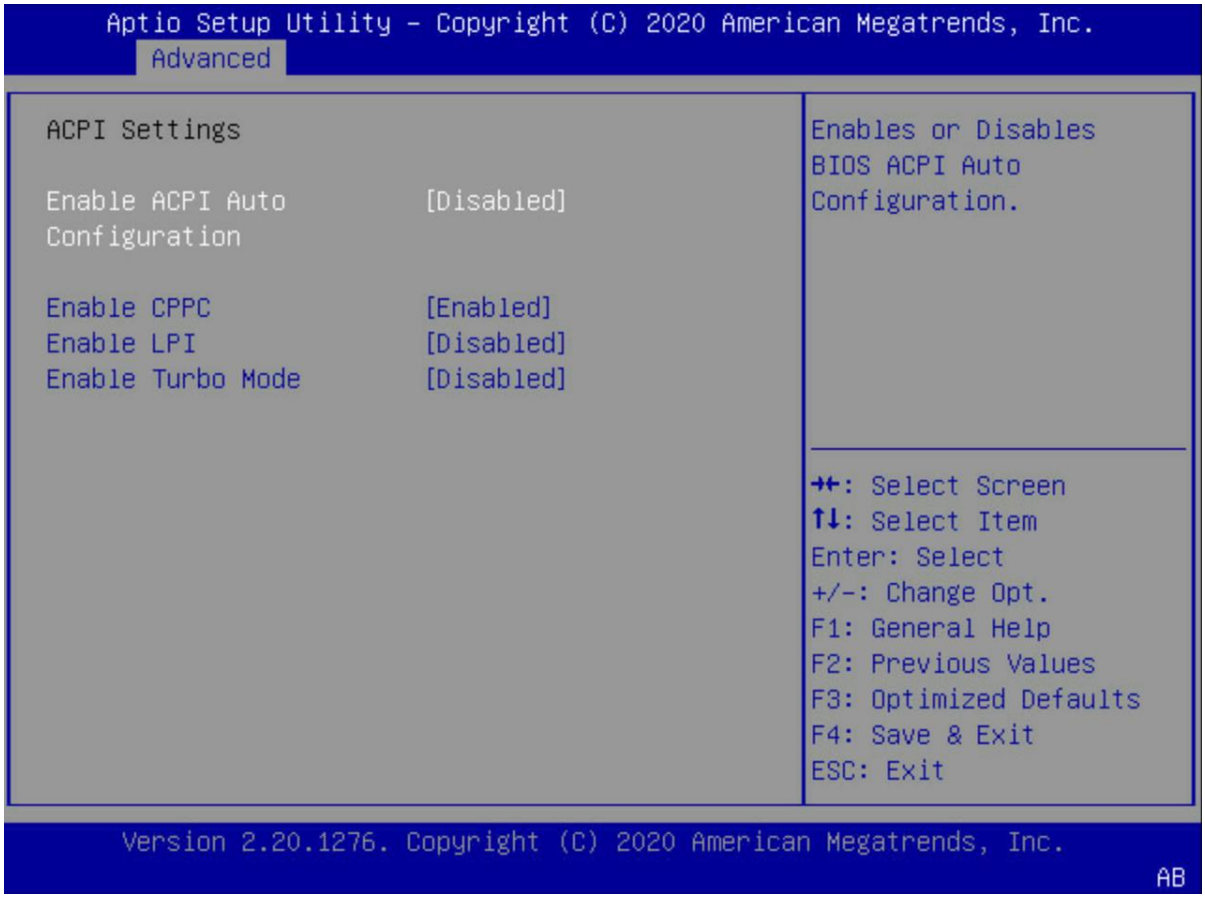


Table 2: ACPI Settings

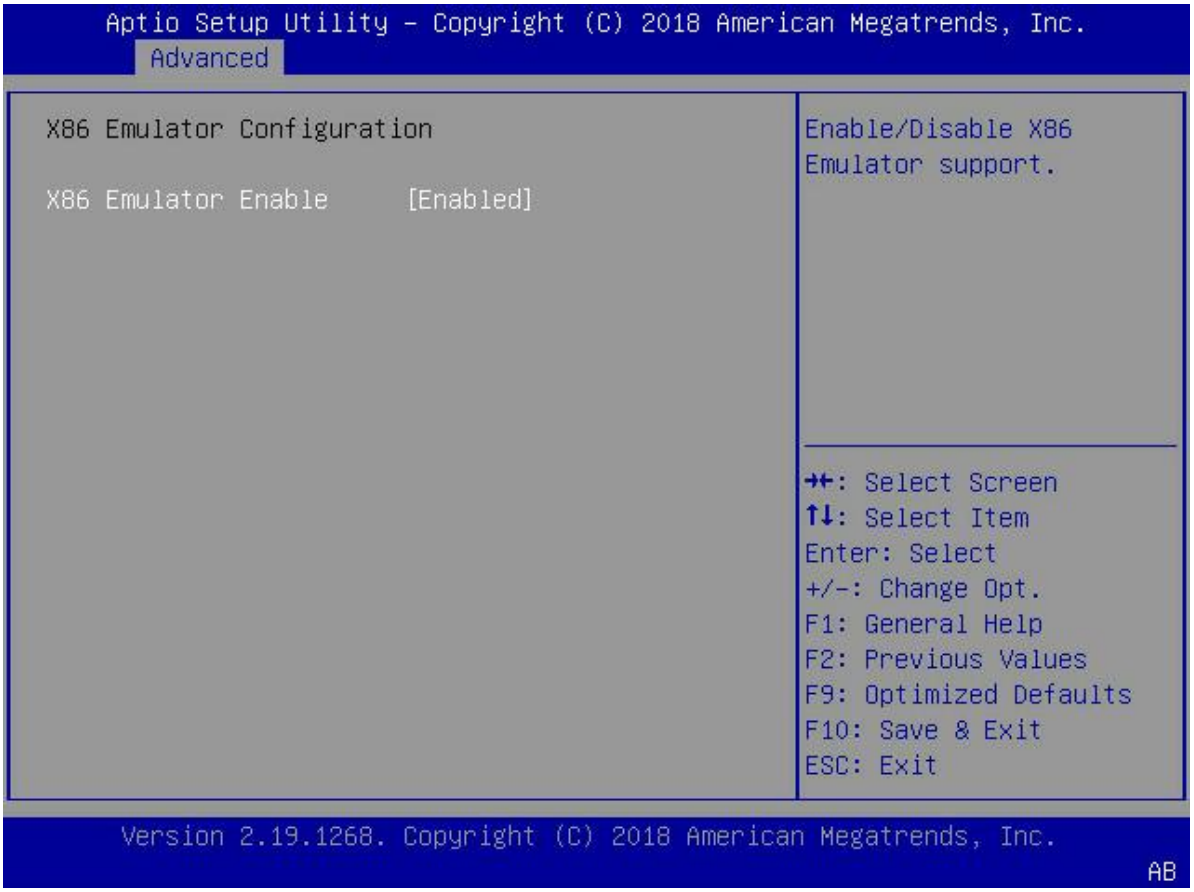
ACPI SETTING	DESCRIPTION
Enable ACPI Auto Configuration	Select Enabled to enable UEFI to select ACPI system options with the following options: • CPPC is enabled • LPI is enabled • Turbo is enabled Select **Disabled** to manually change ACPI following settings.
Enable CPPC	Enable firmware to communicate with the OS using Collaborative Processor Performance Control (CPPC). The options are **Enabled** and Disabled.

ACPI SETTING	DESCRIPTION
Enable LPI	Enable the system to enter LPI (Lower Power Idle) mode. The options are **Enabled** and Disabled.
Enable Turbo mode	Enable Turbo mode, in which the SoC can run at the highest clock frequency (3.3 GHz). The options are Enabled and **Disabled**. **Note:** This mode can be changed only when supported by the SoC.

4.3 X86 Emulator Configuration

This screen enables and disables X86 Emulator support. The options are **Enabled** and Disabled.

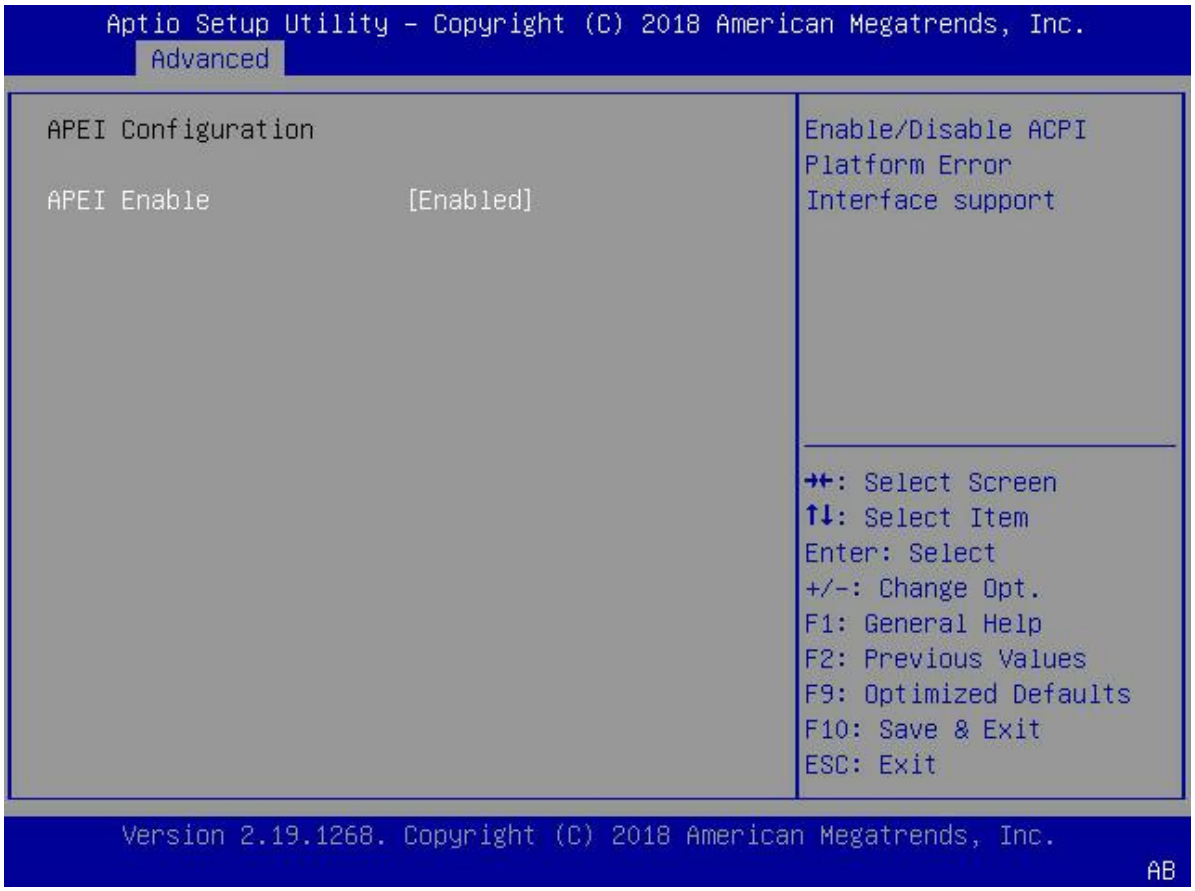
Figure 9: X86 Emulator Support



4.4 ACPI Platform Error Interface (APEI) Configuration

When **APEI Enable** is enabled, the system supports APEI. Enabling this feature causes the system to report hardware errors to the OS. The options are **Enabled** and Disabled.

Figure 10: APEI Configuration Screen



4.5 General Watchdog Timer

When **OS Watchdog Timeout** is enabled, the system reboots and times out if the OS fails to boot. Use this feature if your OS supports the Arm general Watchdog Timer. Select Disabled if unsure. The options are **Enabled** and Disabled.

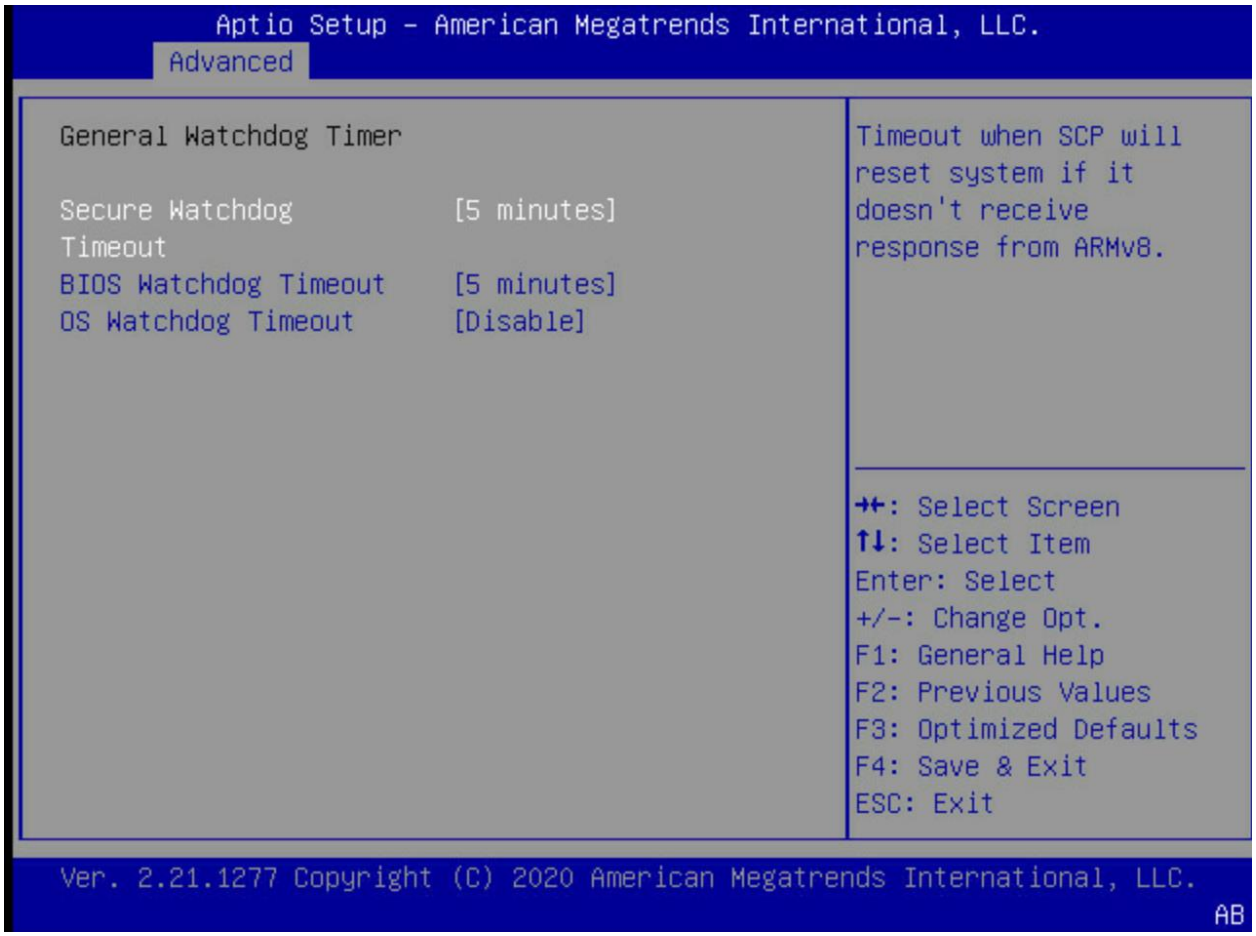
BIOS Watchdog Timeout is the duration after which the system will reboot if the BIOS fails to boot.

Secure Watchdog Timeout is the duration after which the system will reboot if any cores hang for no reason.

This is the behavior of the Watchdog (or failsafe feature):

1. On the first successful boot, UEFI saves a copy of Normal Setting to Last Known Setting in persistent storage.
2. On the first failure boot, the system resets and boots with Last Known Setting. If this boot is successful, UEFI saves a copy of Last Known Setting to Normal Setting.
3. If booting with Last Known Setting fails three times, UEFI boots with the factory default setting.
4. On the first successful boot with factory default settings, UEFI saves a copy of the default setting to the Normal Setting. Subsequent successful boots follow the preceding step.

Figure 11: General Watchdog Timer Screen

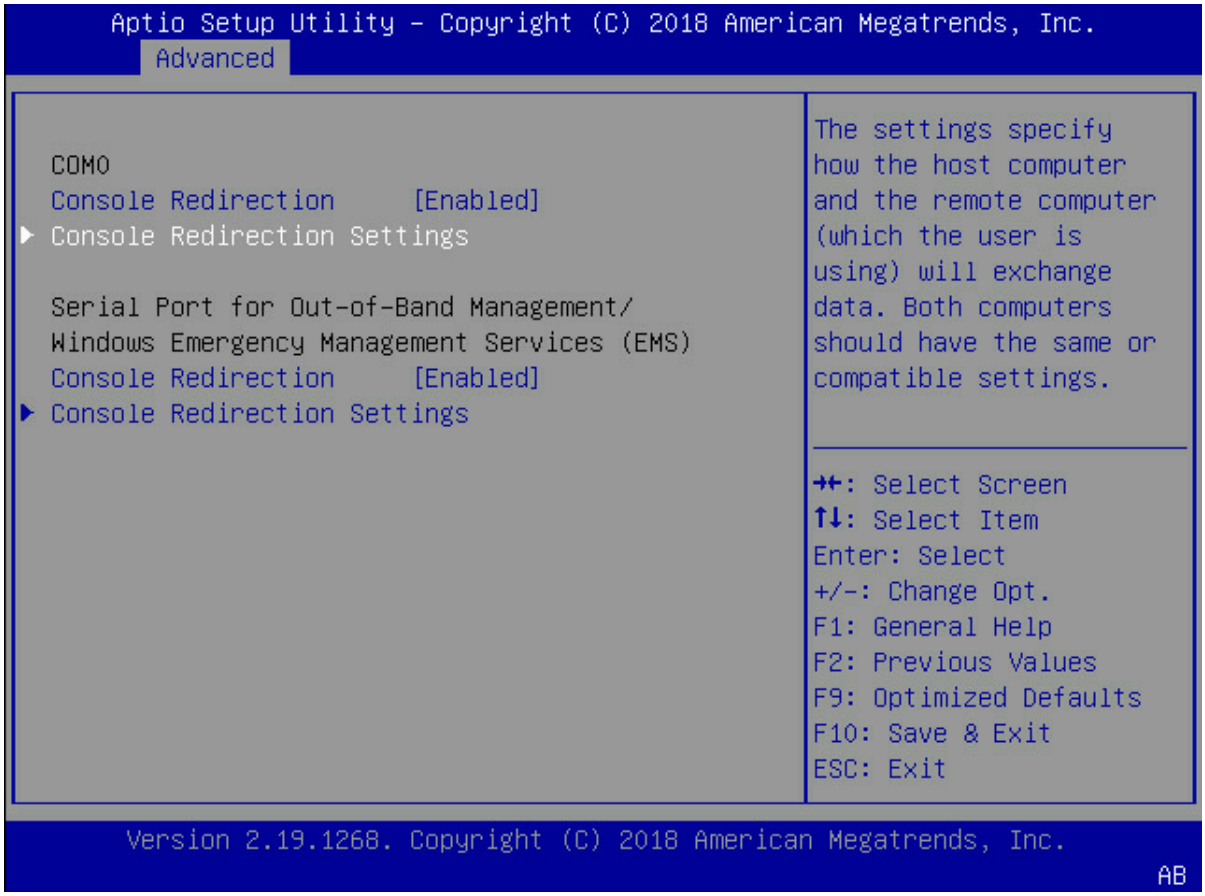


4.6 Serial Port Console Redirection

This screen enables users to configure serial ports for COM0 and the Out-of-Band (OOB) Management port. Subsequent sections provide more detail.

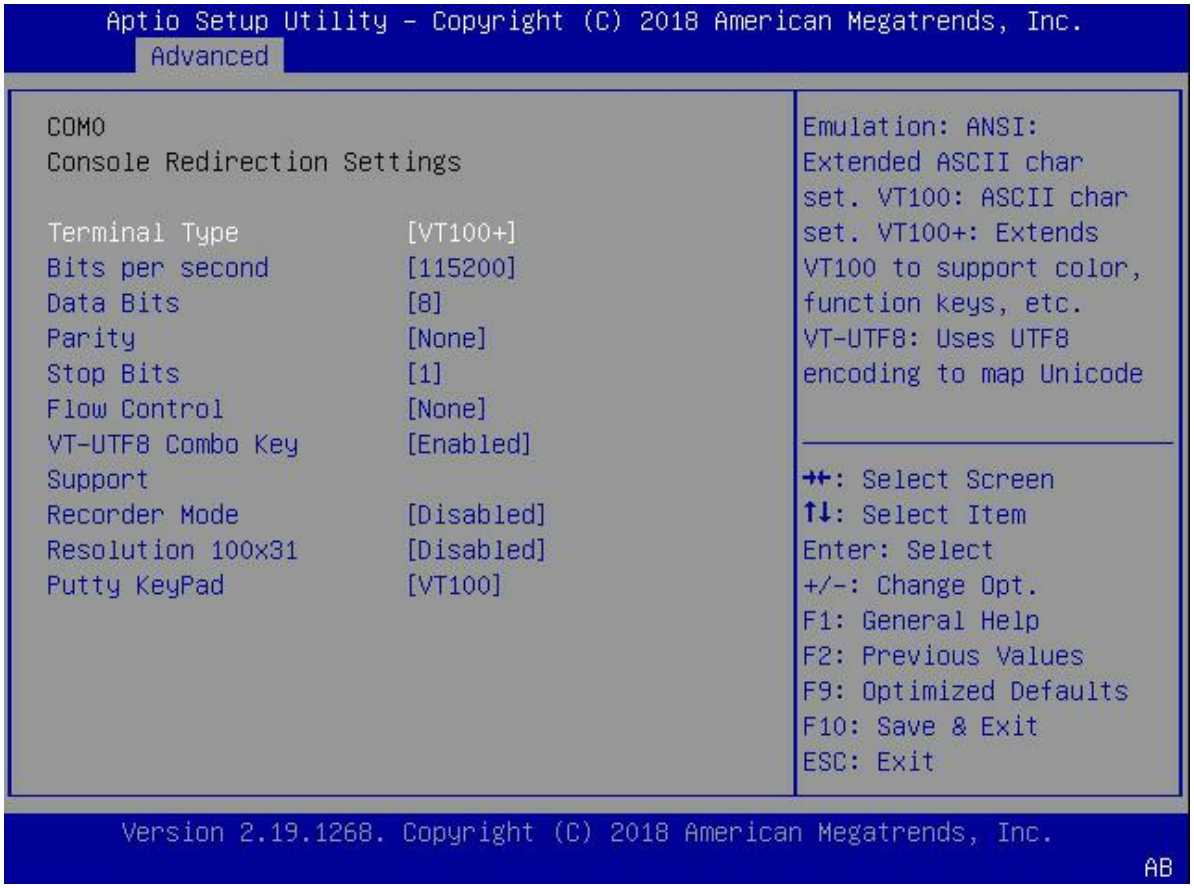
Enable **Console Redirection** to support console redirection for a specific serial port. The options are **Enabled** and Disabled.

Figure 12: Console Redirection Screen



4.6.1 COM0 Settings

Figure 13: COM0 Settings Screen



If console redirection is **Enabled**, the following items are available for user configuration.

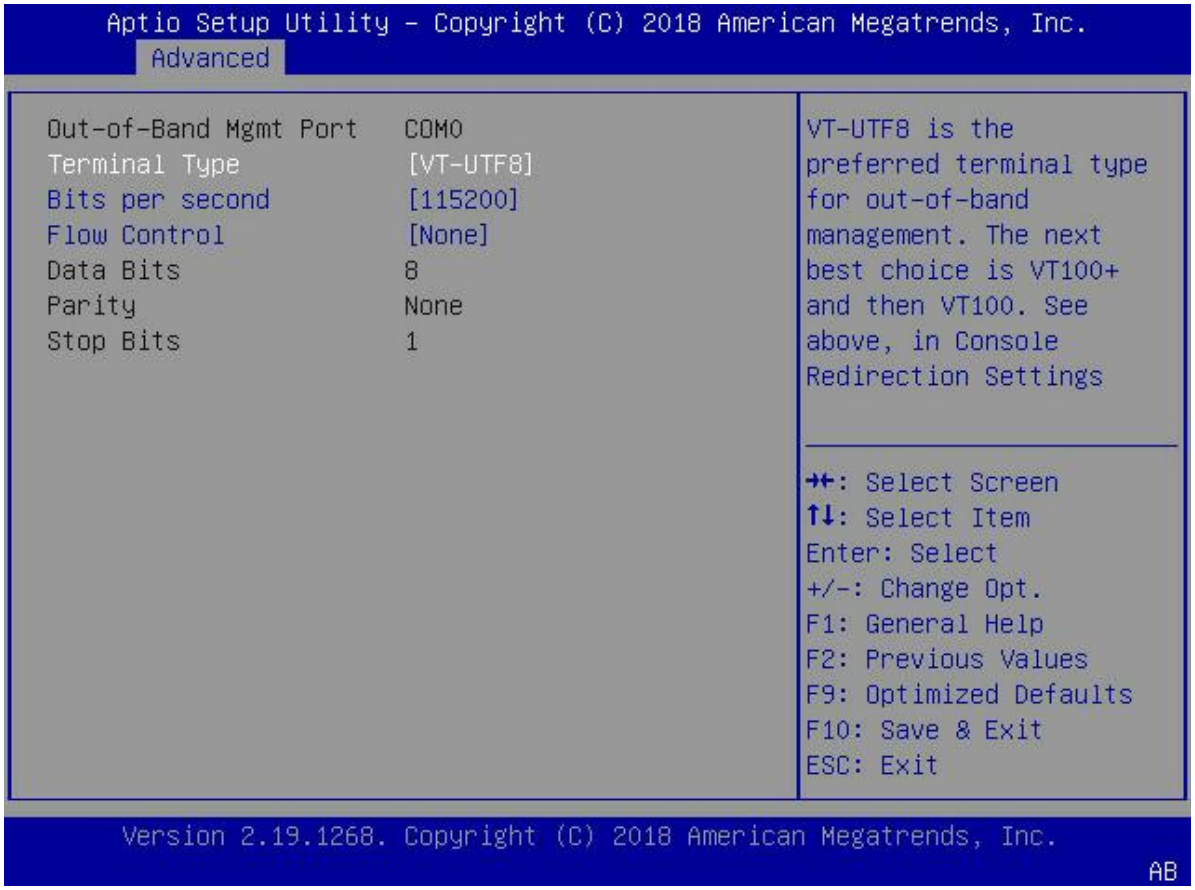
Table 3: Console Redirection Settings

CONSOLE REDIRECTION SETTINGS	DESCRIPTION
Terminal Type	Selects the target terminal emulation type for console redirection: • Select VT100 to use the ASCII Character set. • Select VT100+ to add color and function key support. • Select ANSI to use the Extended ASCII Character Set. • Select VT-UTF8 to use UTF8 encoding to map Unicode characters into one or more bytes. The options are VT100, VT100+, VT-UTF8, and **ANSI**.
Bits per second	Sets the transmission speed, in bits per second, for a serial port used in console redirection. The same speed must be used in the host computer and the client computer. A slower transmission speed may be required for long or busy lines. The options are 9600, 19200, 38400, 57600, and **115200**.
Date Bits	Sets the data transmission size for console redirection. The options are 7 and **8**.

CONSOLE REDIRECTION SETTINGS	DESCRIPTION
Parity	A parity bit can be sent with regular data bits to detect data transmission errors. • Select Even if the parity bit is set to 0, and the number of 1s in data bits is even. • Select Odd if the parity bit is set to 0, and the number of 1s in data bits is odd. • Select None to not send a parity bit with the data bits. • Select Mark to add a mark as a parity bit to be sent with the data bits. • Select Space to add a Space as a parity bit to be sent with the data bits. The options are **None**, Even, Odd, Mark, and Space.
Stop Bits	A stop bit indicates the end of a serial data packet. Select 1 Stop Bit for standard serial data communication. Select 2 Stop Bits if slower devices are used. The options are **1** and 2.
Flow Control	Sets flow control for console redirection to prevent data loss caused by buffer overflow. When set to Hardware RTS/CTS, send a Stop signal to stop sending data when the receiving buffer is full. Send a Start signal to start sending data when the receiving buffer is empty. The options are **None** and Hardware RTS/CTS.
VT-UTF8 Combo Key	Select Enabled to enable VT-UTF8 Combination Key support for ANSI/VT100 terminals. The options are Disabled and **Enabled**.
Recorder Mode	Select Enabled to capture the data displayed on a terminal and send it as text messages to a remote server. The options are **Disabled** and Enabled.
Resolution 100x31	Select Enabled to capture the data displayed on a terminal and send it as text messages to a remote server. The options are **Disabled** and Enabled.
Putty KeyPad	Selects the settings for the Function Keys and KeyPad used for Putty, a terminal emulator for Windows. The options are **VT100**, LINUX, XTERMR6, SCO, ESCN, and VT400.

4.6.2 Serial Port for OOB Management/Windows Emergency Management Services (EMS)

Figure 14: Out-of-Band Management Screen



Select Enabled to enable SOL console redirection support for a specific serial port. The options are **Enabled** and Disabled.

If OOB management is **Enabled**, the following items can be configured.

Table 4: OOB Console Redirection Settings

CONSOLE REDIRECTION SETTINGS	DESCRIPTION
Terminal Type	Selects the target terminal emulation type for console redirection. • Select VT100 to use the ASCII Character set. • Select VT100+ to add color and function key support. • Select ANSI to use the Extended ASCII Character Set. • Select VT-UTF8 to use UTF8 encoding to map Unicode characters into one or more bytes. The options are VT100, VT100+, **VT-UTF8**, and ANSI.
Bits per second	Sets the transmission speed, in bits per second, for a serial port used in out-of-band console redirection. The same speed must be used for the host computer and the client computer. A lower transmission speed may be required for long or busy lines. The options are 9600, 19200, 38400, 57600, and **115200**.

CONSOLE REDIRECTION SETTINGS	DESCRIPTION
Flow Control	Sets flow control for console redirection to prevent data loss caused by buffer overflow. When set to Hardware RTS/CTS, send a Stop signal to stop sending data when the receiving buffer is full. Send a Start signal to start sending data when the receiving buffer is empty. The options are **None** and Hardware RTS/CTS.
Data Bits	Sets the data transmission size for console redirection. The options are 7 and **8.**
Parity	A parity bit can be sent along with regular data bits to detect data transmission errors. • Select Even if the parity bit is set to 0, and the number of 1s in data bits is even. • Select Odd if the parity bit is set to 0, and the number of 1s in data bits is odd. • Select None if you do not want to send a parity bit with your data bits in transmission. • Select Mark to add a mark as a parity bit to be sent along with the data bits. • Select Space to add a Space as a parity bit to be sent with your data bits. The options are **None**, Even, Odd, Mark, and Space.
Stop Bits	A stop bit indicates the end of a serial data packet. • Select 1 stop bits for standard serial data communication. • Select 2 stop bits when slower devices are used. The options are **1** and 2.

4.7 PCI Subsystem Settings

Figure 15 provides standard PCIe configuration settings and information about available PCIe slots.

Figure 15: PCI Settings Screen

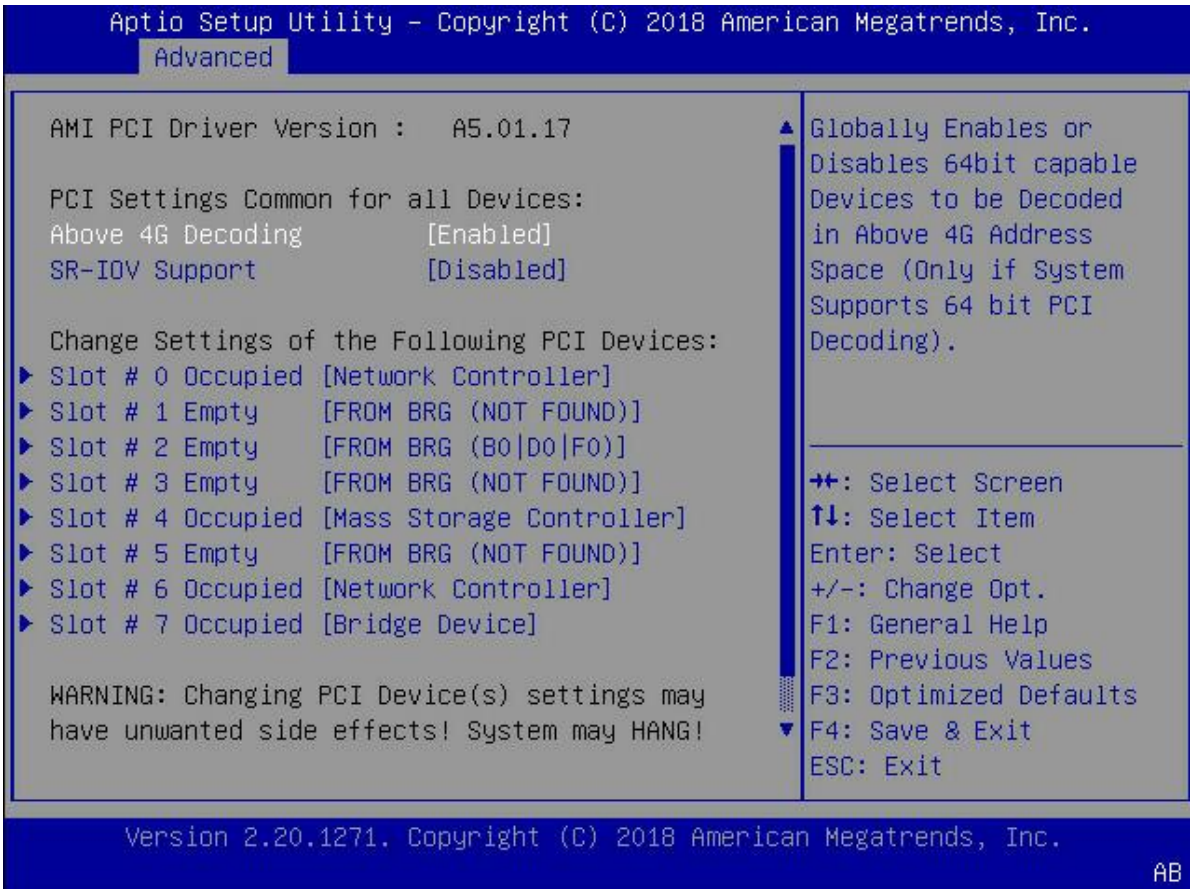


Table 5: PCIe Device Common Settings

PCIE DEVICE COMMON SETTINGS	DESCRIPTION
Above 4G Decoding	**Enable** or Disable 64-bit capable devices to be decoded in the address space above 4 GB.
SR-IOV Support	If the system has SR-IOV capable PCIe devices, Enable or **Disable** SR-IOV support for the system.

4.7.1 PCIe Slot Mapping Table

Table 6 provides the UEFI PCIe slot number to Altra SoC Root Complex (RC) mapping.

Table 6: PCIe Slot Mapping table

SLOT NUMBER TO ROOT COMPLEX MAPPING				BIFURCATION
SLOT NUMBERS	SOCKET NUMBER	ROOT COMPLEX (RC)	DEFAULT	MAXIMUM
0–3	0	RCA3	x16	x4 x4x4x4
4–7	0	RCA2	x16	x4 x4x4x4
8 9	0	RCB0A	x4 x4	x4x4
10 11	0	RCB0B	x4 x4	x4 x4
16 17	0	RCB1A	x4 x4	x4 x4
18 19	0	RCB1B	x4 x4	x4 x4
24 25	0	RCB2A	x4 x4	x4 x4
26–29	0	RCB2B	x8	x2 x2x2x2
32–35	0	RCB3A	x8	x2 x2x2x2
36 37	0	RCB3B	x4 x4	x4 x4
40 41	1	RCA2	x8 x8	x8x8
44 45	1	RCA3	x8 x8	x8x8
48–51	1	RCB0A	x8	x2 x2x2x2
52 53	1	RCB0B	x4 x4	x4 x4
56 57	1	RCB1A	x4 x4	x4 x4
58–61	1	RCB1B	x8	x2 x2x2x2
64 65	1	RCB2A	x4 x4	x4 x4
66 67	1	RCB2B	x4 x4	x4 x4
72 73	1	RCB3A	x4 x4	x4 x4
74 75	1	RCB3B	x4 x4	x4 x4

4.7.1.1 Changing Settings for PCI Devices

Figure 16 shows the settings that can be configured and that are common to all devices.

Figure 16: PCIe Slot Settings Screen

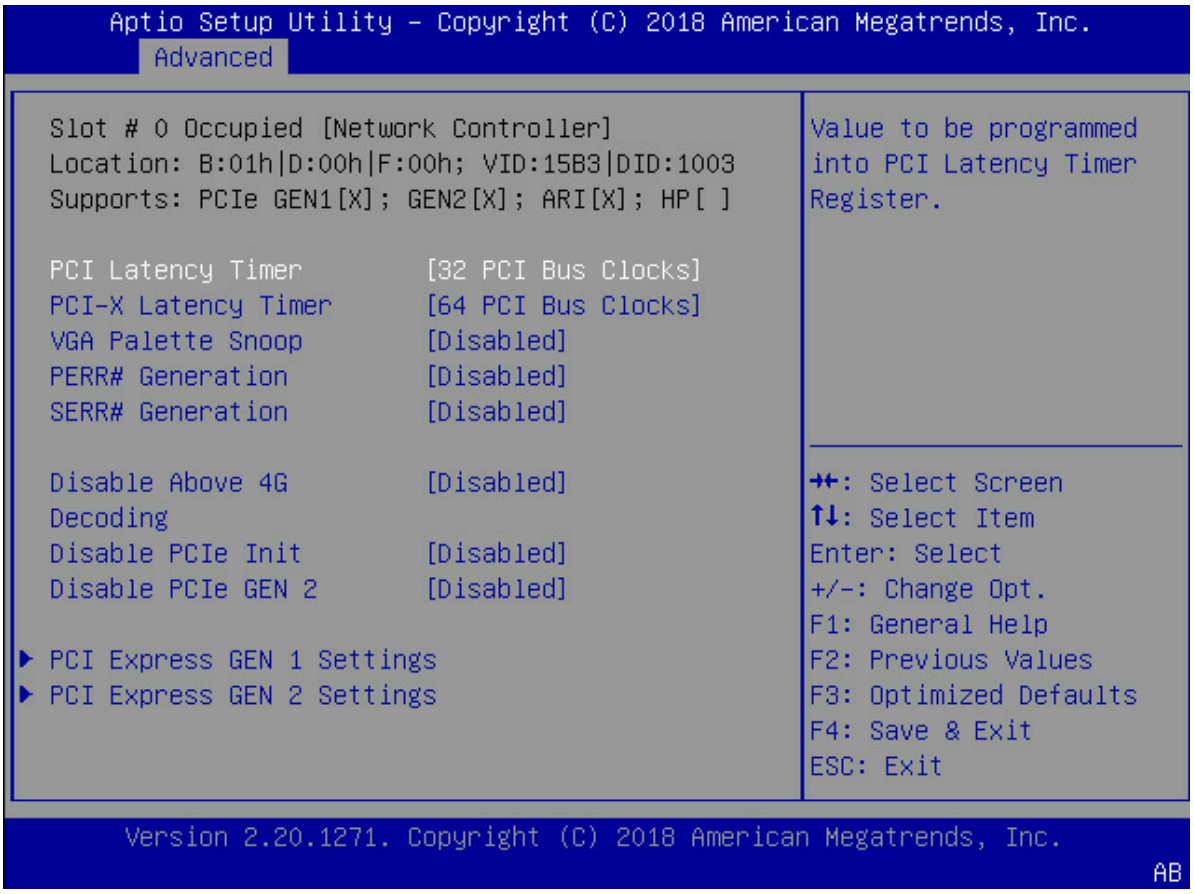
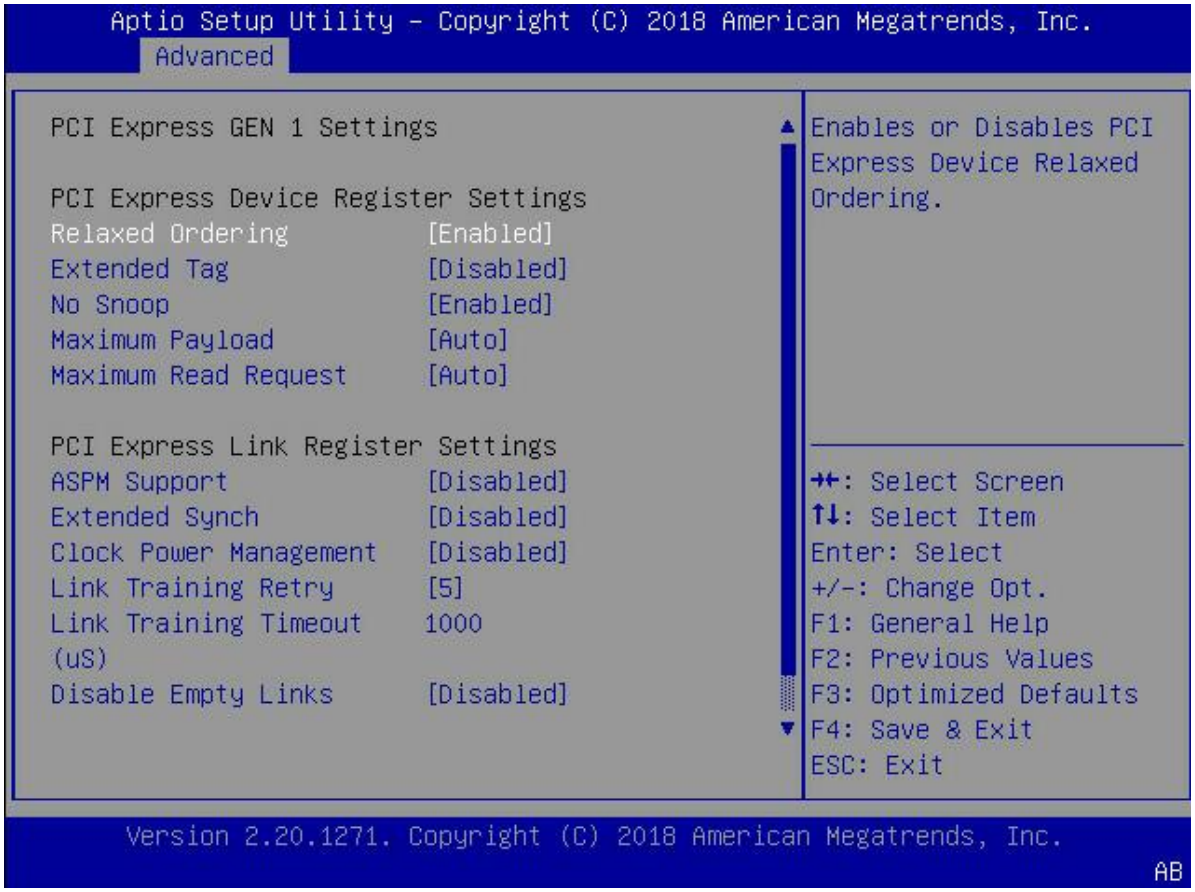


Table 7: PCIe Device Common Settings

PCIE DEVICE COMMON SETTINGS	DESCRIPTION
PCI Latency Timer	The value for the PCI Latency Timer Register.
PCI-X Latency Timer	The value for the PCI Latency Timer Register.
VGA Palette Snoop	Enable or **Disable** VGA Palette Registers Snooping.
PERR# Generation	Enable or **Disable** PCI Device to Generate PERR#.
SERR# Generation	Enable or **Disable** PCI Device to Generate SERR#.
Disable Above 4G Decoding	Enable or **Disable** 64-bit capable devices to be decoded above the 4 GB address space for selected and downstream PCI devices.
Disable PCIe Init	Enable or **Disable** UEFI built-in PCIe initialization for selected and downstream PCI Device(s).
Disable PCIe GEN 2	Enable or **Disable** UEFI built-in PCIe GEN2 initialization for selected and downstream PCI Device(s).

4.7.2 PCIe GEN 1 Settings

Figure 17: PCIe GEN 1 Settings Screen



Warning: Enabling Active State Power Management (ASPM) can cause some PCIe devices to fail.

Note: Some settings may not be fully supported due to hardware limitations.

Table 8: PCIe GEN 1 Settings

SETTING	DESCRIPTION
PCIe Device Register Settings	
Relaxed Ordering	**Enable** and Disable PCIe Device Relaxed Ordering.
Extended Tag	If **Enabled**, enables a Device to use 8-bit Tag field as a requester.
Maximum Payload	Set the Maximum Payload of the PCIe Device or enable UEFI to select the value. The available options are **Auto**, 128 Bytes, 256 Bytes, 512 Bytes, 1024 Bytes, 2048 Bytes, and 4096 Bytes.
Maximum Read Request	Set Maximum Payload Request Size of the PCIe Device or allow System BIOS to select the value. The available options are **Auto**, 128 Bytes, 256 Bytes, 512 Bytes, 1024 Bytes, 2048 Bytes, and 4096 Bytes.

SETTING	DESCRIPTION
PCIe Link Register Settings	
ASPM Support	Set the ASPM Level: • Force L0s: Force all links to L0s State • AUTO: UEFI autoconfigure • **DISABLE:** Disables ASPM.
Extended Synch	If Enabled, allows generation of Extended Synchronization patterns.
Clock Power Management	If supported by hardware and set to Enabled, the device is permitted to use CLKREQ# signal for power management of Link lock according to protocol.
Link Training Retry	Defines number of Retry Attempts software takes to retrain the link if previous training attempt was unsuccessful.
Link Training Timeout	The number of microseconds that software waits before polling the Link Training bit in the Link Status register. Values range from 10 to 10,000 µs.
Disable Empty Links	To save power, software disables unpopulated PCIe links, if this option is set to **Disable**.

4.7.3 PCIe GEN 2 Settings

Figure 18: PCIe GEN 2 Settings Screen

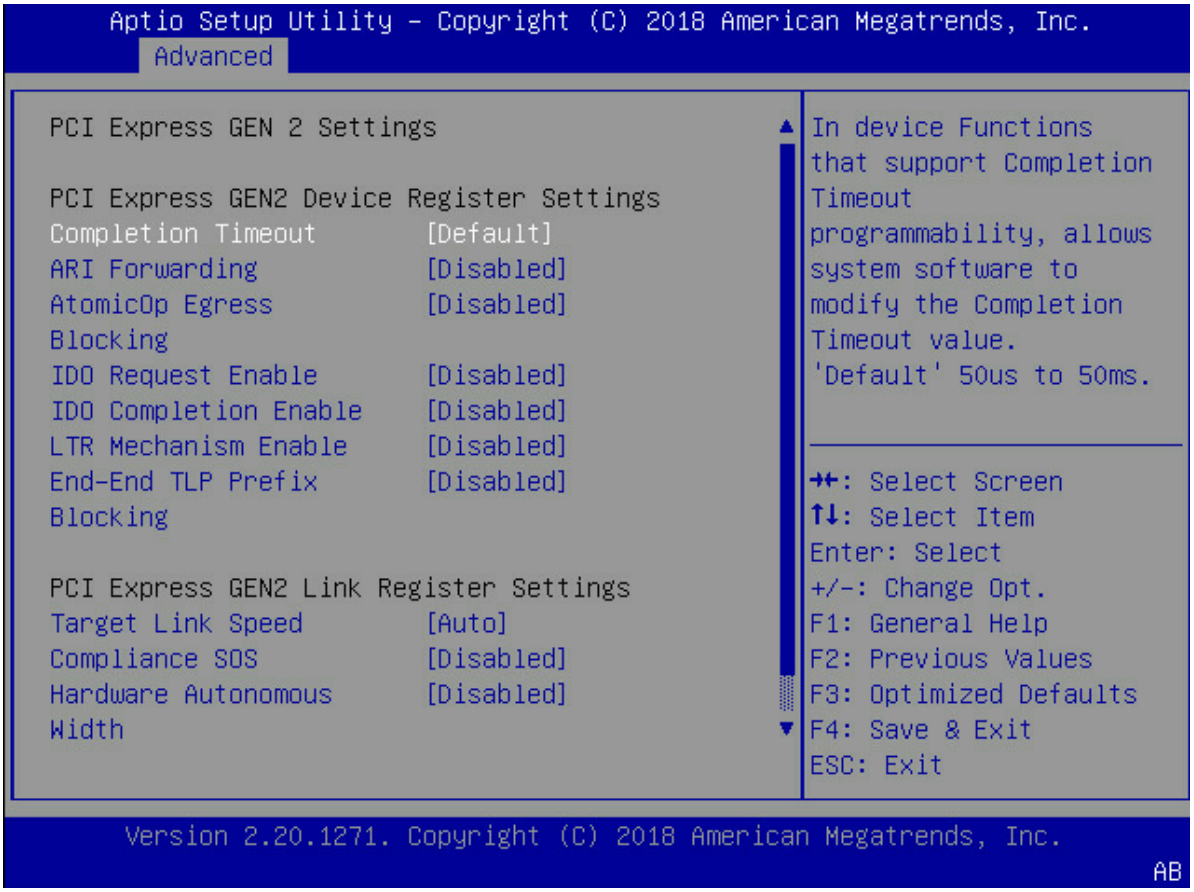


Table 9: PCIe GEN 2 Settings

SETTING	DESCRIPTION
PCIe GEN2 Device Register Settings	
Completion Timeout	Enables system software to modify the Completion Timeout value in devices that support Completion Timeout programming. The default is 50 µs to 50 ms. If Shorter is selected, software uses shorter timeout ranges if supported by hardware. If Longer is selected, software uses longer timeout ranges.
Alternative Routing Interpretation (ARI) Forwarding	If supported by hardware and Enabled, the Downstream Port disables its traditional Device Number filed being 0 enforcement when turning a Type1 Configuration Request into a Type0 Configuration Request, supporting access to Extended Functions in an ARI Device immediately below the port. The default is **Disabled**.
AtomicOp Egress Blocking	If supported by hardware and set to Enable, outbound AtomicOp requests via egress ports are blocked. The default is **Disabled**.
IDO Request Enable	If supported by hardware and set to Enable, this setting enables the number of ID-Based Ordering (IDO) bit (Attribute[2]) requests to be initiated. The default is **Disabled**.
IDO Completion Enable	If supported by hardware and set to Enable, this setting enables the number of ID-Based Ordering (IDO) bit (Attribute[2]) to be completed. The default is **Disabled**.
LTR Mechanism Enable	If supported by hardware and set to Enable, this setting enables the Latency Tolerance Reporting (LTR) Mechanism. The default is **Disabled**.
End-End TLP Prefix Enable	If supported by hardware and set to Enable, this setting blocks the forwarding of TLPs containing End-End TLP Prefixes. The default is **Disabled**.
PCIe GEN2 Link Register Settings	
Target Link Speed	If supported by hardware and set to Force to X.X GT/s for Downstream Ports, this setting restricts the values advertised by the Upstream component in its training sequences to set an upper limit on Link operational speed. When **Auto** is selected, hardware initialized data is used. The options are: **Auto**, Force to 2.5 GT/s, Force to 5.0 GT/s, Force to 8.0 GT/s, and Force to 16.0 GT/s.
Compliance SOS	If supported by hardware and set to Enable, this setting forces LTSSM to send SKP Ordered Sets between sequences when sending Compliance Pattern or Modified Compliance Pattern. The default is **Disabled**.
Hardware Autonomous Width	If supported by hardware and set to **Disabled**, this setting disables the hardware ability to change link width, except to correct unstable link operations.
Hardware Autonomous Speed	If supported by hardware and set to **Disabled**, this setting disables the hardware ability to change link speed, except for speed rate reductions to correct unstable link operations.

4.8 Network Configuration

Figure 19: Network Configuration Screen

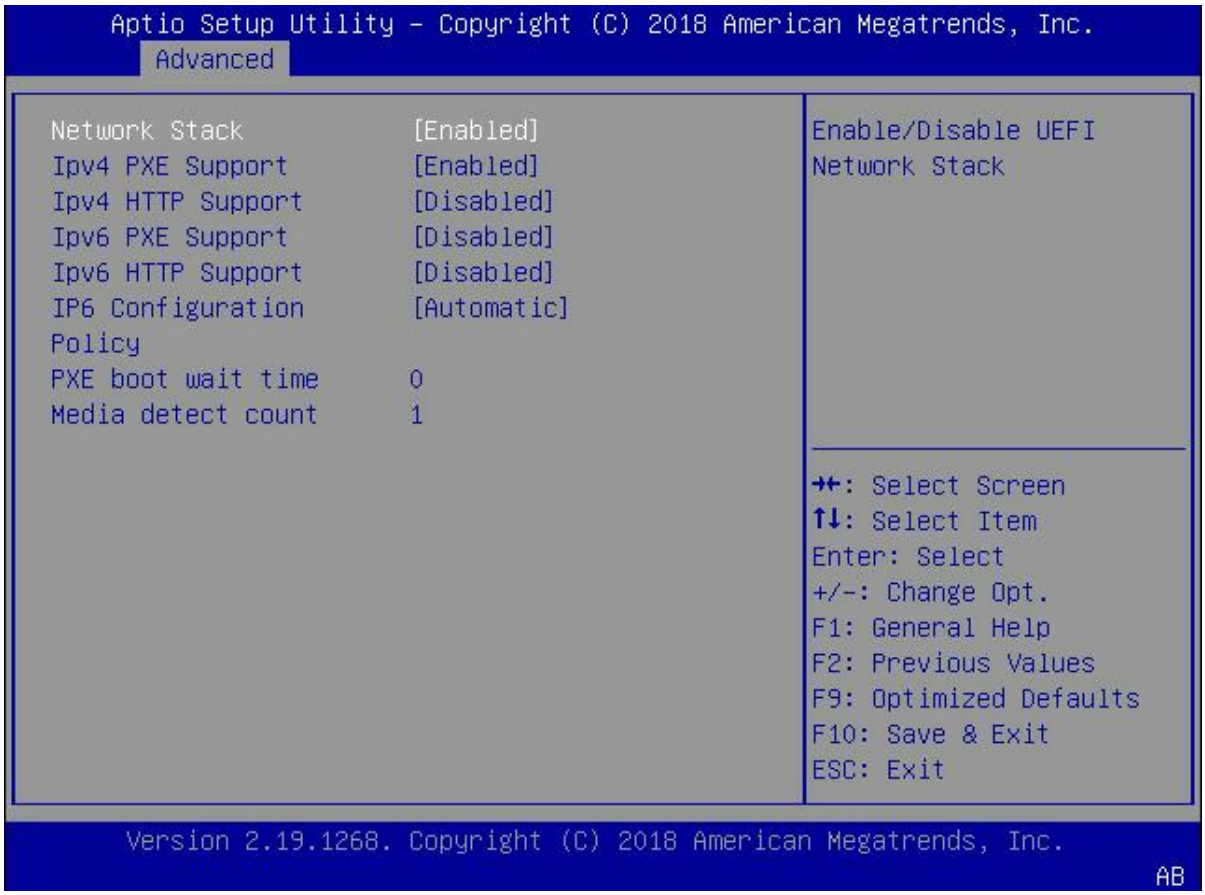
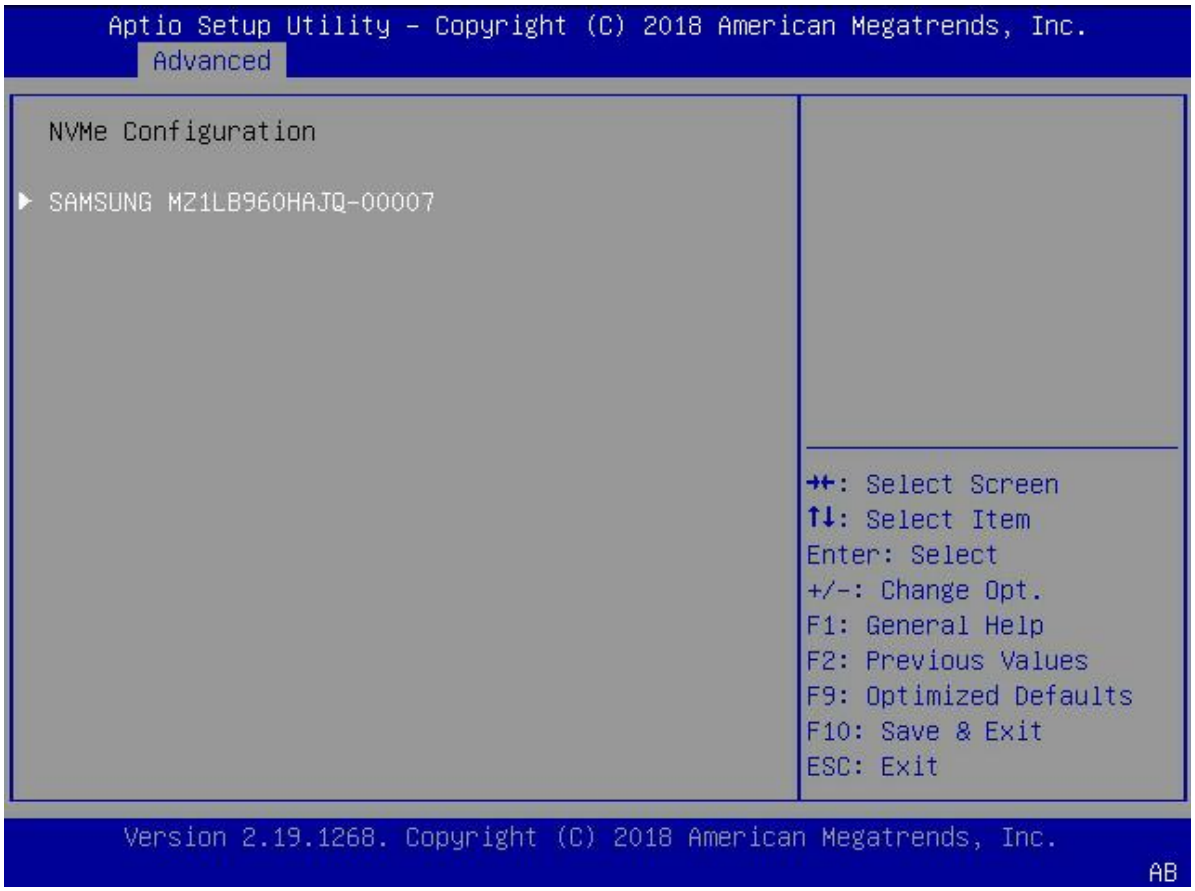


Table 10: Network Configuration Settings

SETTING	DESCRIPTION
Network Stack	**Enable** and Disable the UEFI network stack.
Ipv4 PXE Support	**Enable** and Disable IPv4 PXE boot support. If disabled, IPv4 PXE boot support is unavailable.
Ipv4 HTTP Support	Enable and **Disable** IPv4 HTTP boot support. If disabled, IPv4 HTTP boot support is unavailable.
Ipv6 PXE Support	Enable and **Disable** IPv6 PXE boot support. If disabled, IPv6 PXE boot support is unavailable.
Ipv6 HTTP Support	Enable and **Disable** IPv6 HTTP boot support. If disabled, IPv6 HTTP boot support is unavailable.
PXE boot wait time	Wait time in seconds to press ESC to abort the PXE boot. Use the +/- or numeric keys to set the value. The default is **0**.
Media detect count	Number of times the presence of media is checked. Use the +/- or numeric keys to set the value. The default is **1**.

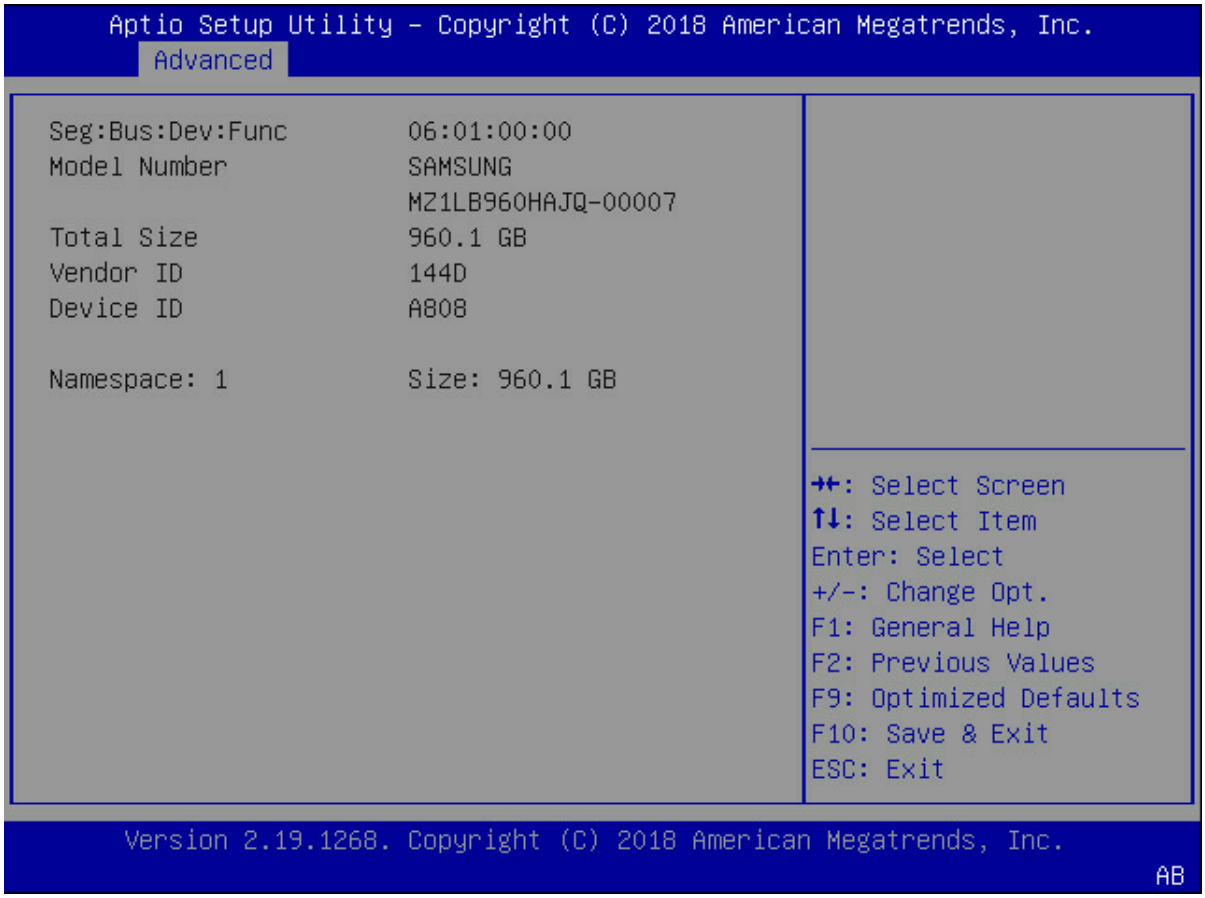
4.9 NVMe Configuration

Figure 20: NVMe Configuration Screen



Selecting a device name displays more information, as shown in *Figure 21*.

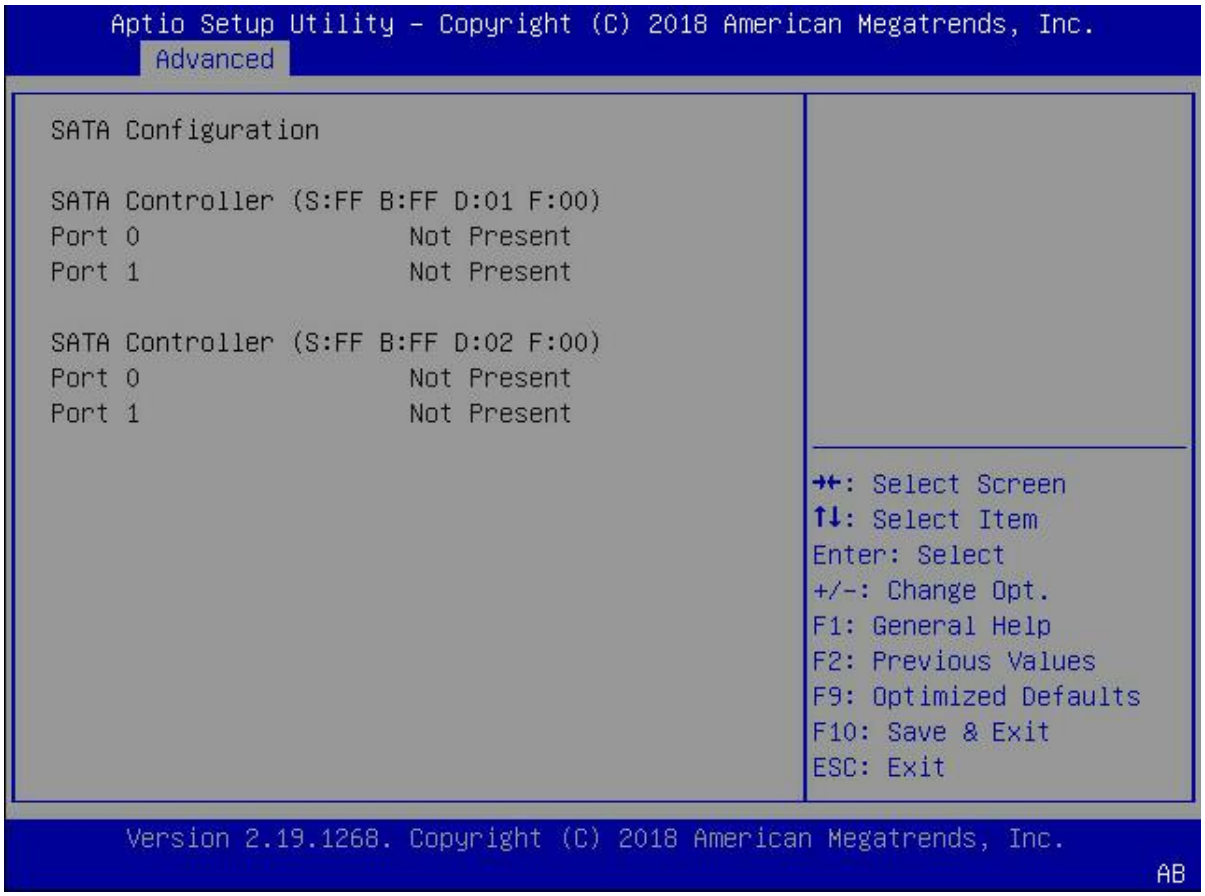
Figure 21: Additional NVMe Information



4.10 SATA Configuration

SATA Controller (S:X B:X D:X F:X) displays information for a SATA controller on a PCIe downstream device.

Figure 22: SATA Configuration Screen



4.11 USB Configuration

Figure 23: USB Configuration Screen (1 of 2)

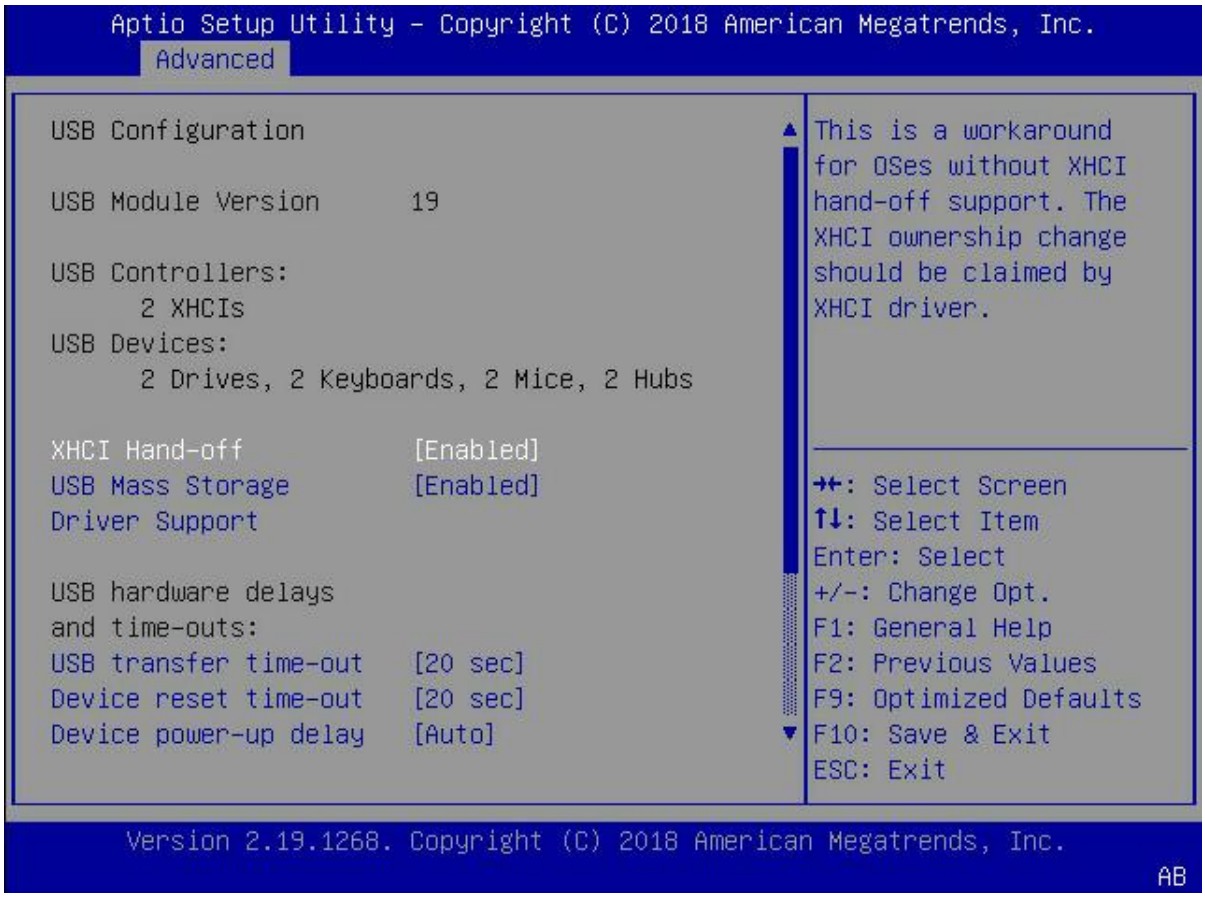
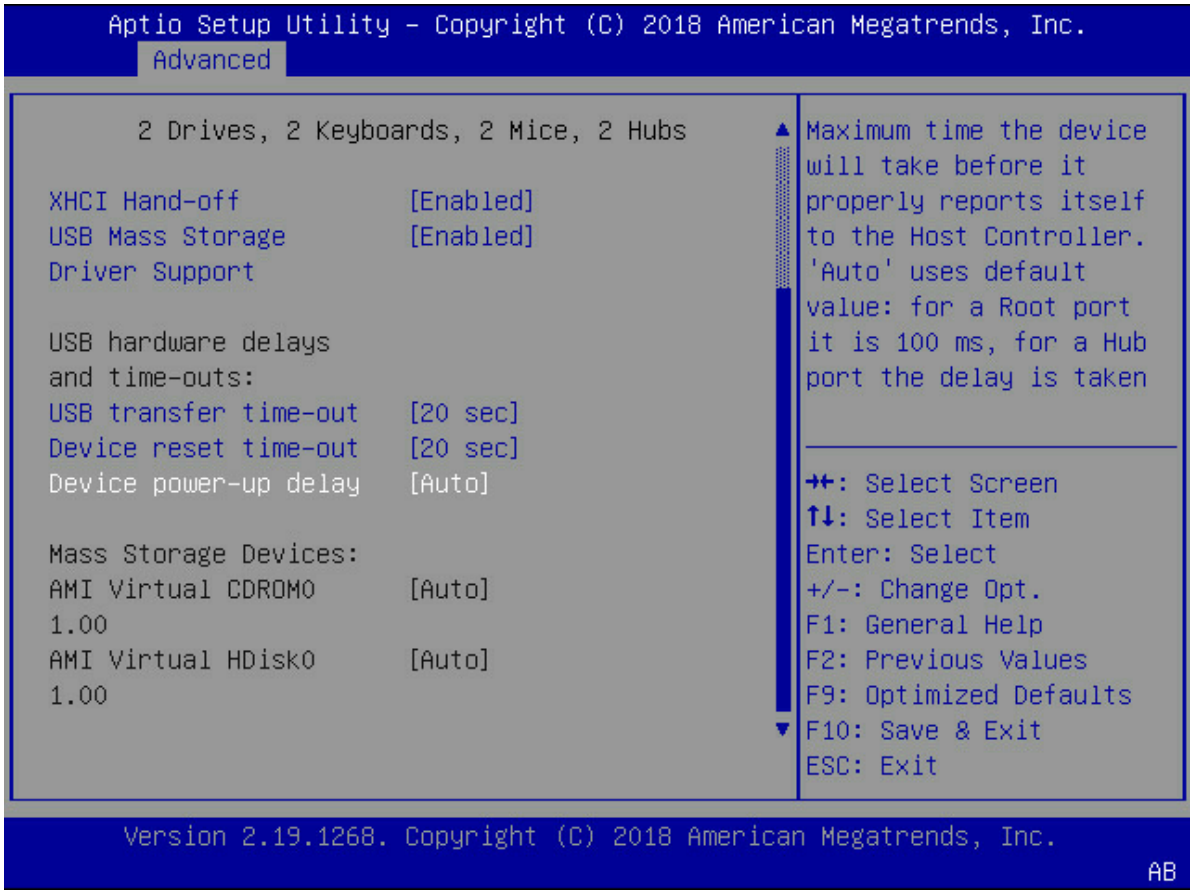


Table 11: USB Configuration Settings

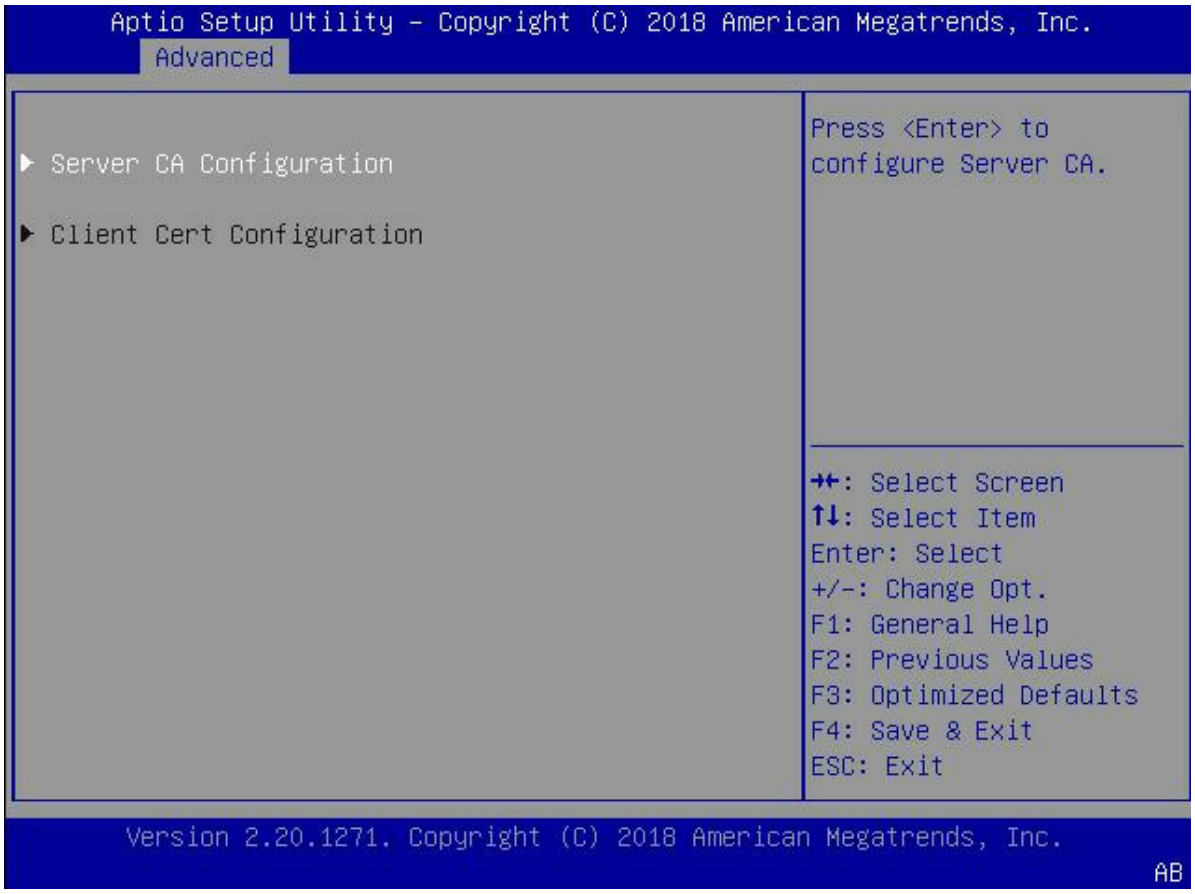
SETTING	DESCRIPTION
USB Controllers	The number of USB controllers installed in the system.
USB Devices	Lists the categories of detected USB devices.
xHCI Hand-off	If **Enabled**, a workaround for OSes without eXtensible Host Controller Interface (xHCI) hand-off support. Ownership changes must be claimed by xHCI driver.
USB Mass Storage Driver Support	**Enable**/Disable USB Mass Storage Driver Support.
USB transfer time-out	The time-out value for Control, Bulk, and Interrupt transfers.
Device reset time-out	The time-out value for the USB mass storage device Start Unit.
Device power-up delay	The maximum time the device takes before it reports itself to the Host Controller. **Auto** uses a default value; for a Root Port, it is 100 ms, and for a Hub Port the delay is taken from the hub description.
Mass Storage Devices	Lists the detected mass storage devices.

Figure 24: USB Configuration Screen (2 of 2)



4.12 Transport Layer Security (TLS) Auth Configuration

Figure 25: TLS Auth Configuration Screen



This screen can be used to add the Server Certificate Authority (CA) certification and Client Cert to use for secure communication between UEFI and an external server.

Note: Client Cert configuration is currently unsupported.

Figure 26: Certificate Management Screen

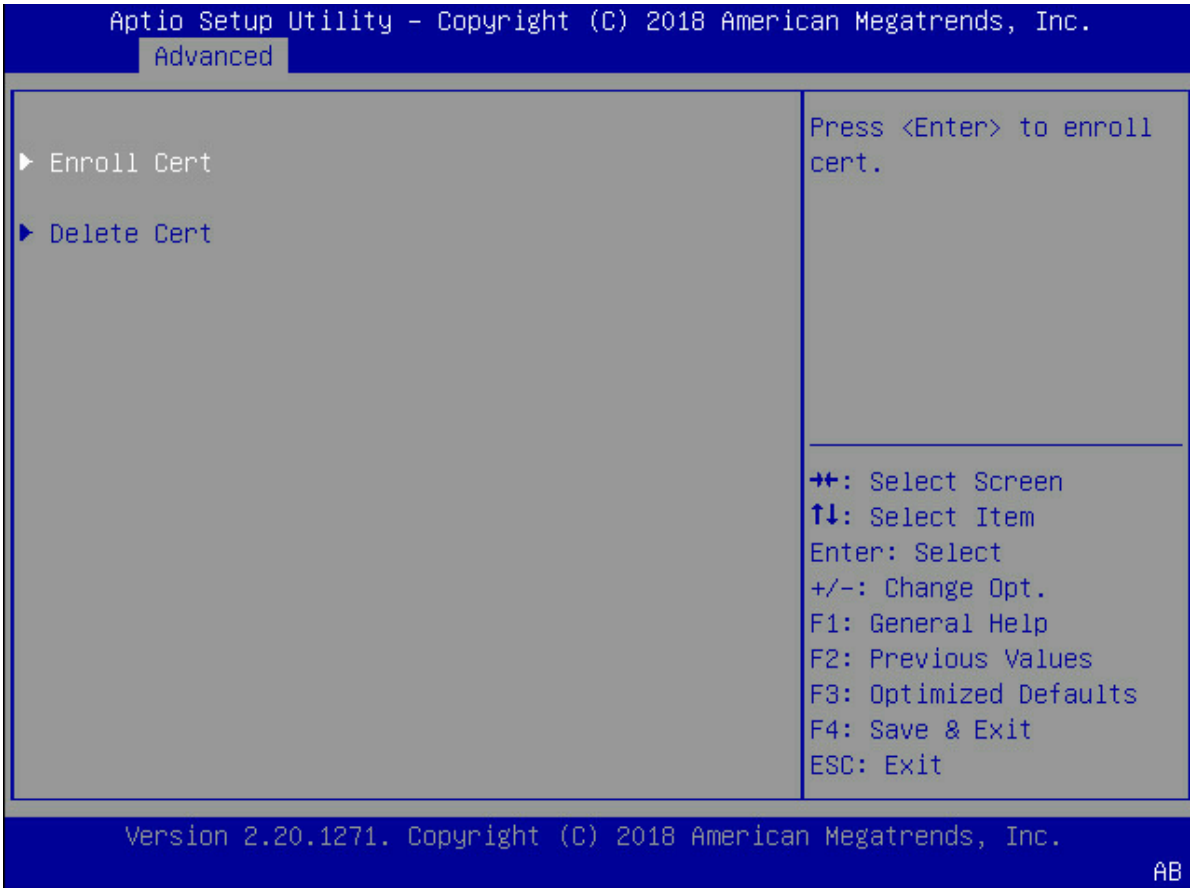


Table 12: Certificate Management Settings

SETTING	DESCRIPTION
Enroll Cert	Enables enrolling a CA Cert from the file system or using GUID <format: 11111111-2222-3333-4444-1234567890ab>
Delete Cert	Enable/Disable an enrolled CA Cert from the system.

4.13 MAC:XXXXXXXXXXXX-IPv4 Network Configuration

When **Network Stack** is enabled on the **Network Configuration** screen, this screen enables IPv4 network configuration for the device having MAC address XXXXXXXXXXXX.

Figure 27: IPv4 Network Configuration Screen

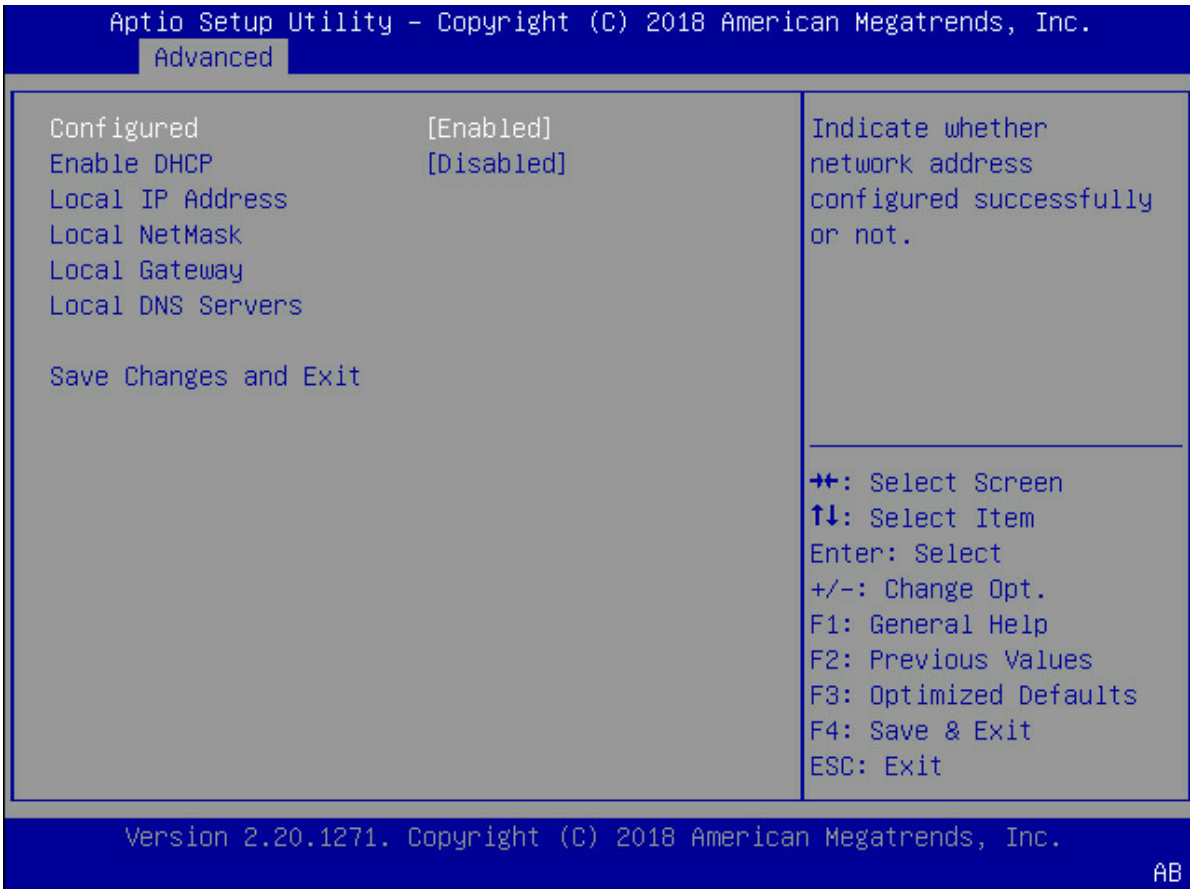


Table 13: IPv4 Network Configuration Settings

SETTING	DESCRIPTION
Configured	**Enable** and Disable IPv4 configuration for this device. When **Enabled**, settings described in this table are available.
Enable DHCP	Enable DHCP mode. The default is **Enabled**.
Local IP Address	When Enable DHCP mode is disabled, enter an IP address in dotted decimal notation for this device, for example, 192.168.1.2.
Local NetMask	When Enable DHCP mode is disabled, enter a NetMask in dotted decimal notation for this device, for example, 255.255.255.0.
Local Gateway	When Enable DHCP mode is disabled, enter the Gateway address in dotted decimal notation for this device, for example, 192.168.1.1.
Local DNS	When Enable DHCP mode is disabled, enter DNS server addresses in dotted-decimal notation for this device, for example, 192.166.1.100 192.168.1 200.
Save Changes and Exit	Press Enter to save changes and exit.

4.14 MAC:XXXXXXXXXXXX-IPv6 Network Configuration

When **Network Stack** is enabled on the **Network Configuration** screen, this screen enables IPv6 network configuration for the device having MAC address XXXXXXXXXXXX.

Figure 28: IPv6 Network Configuration Screen

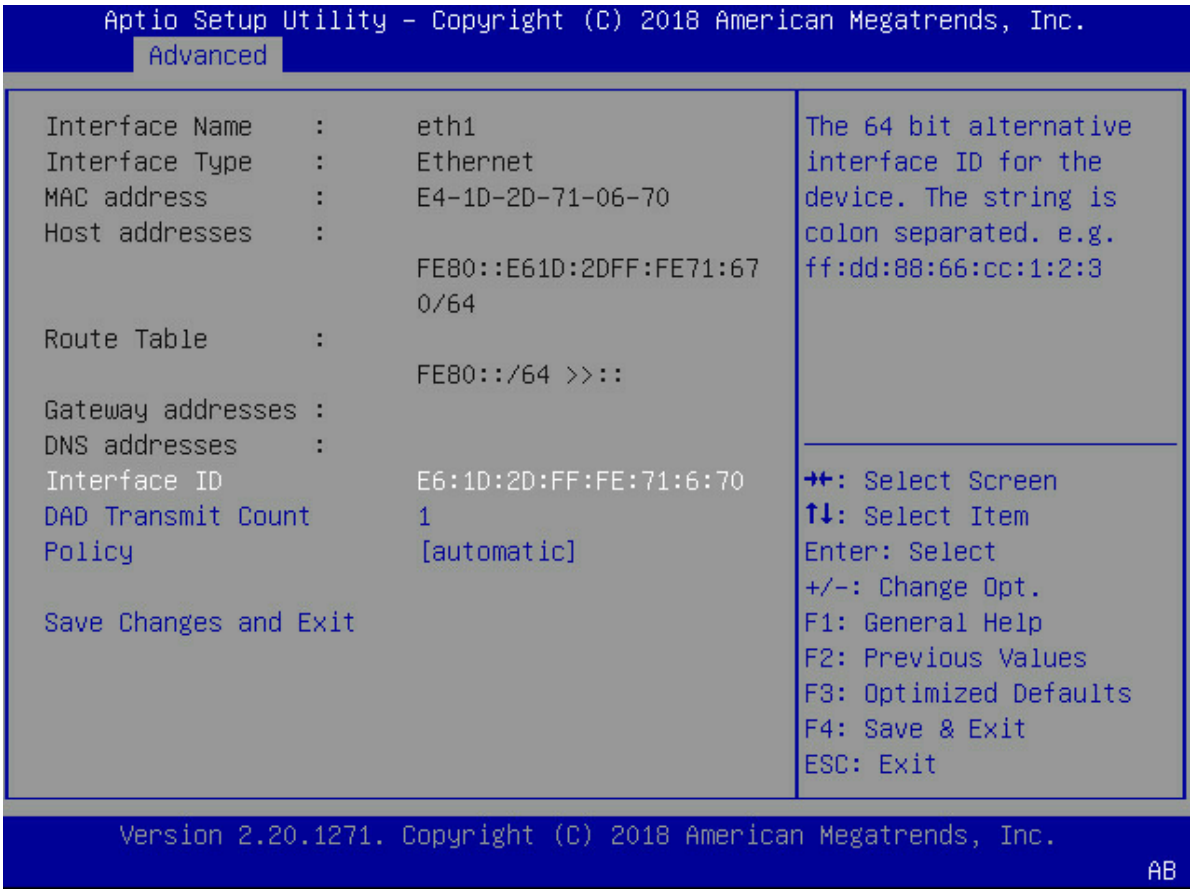


Table 14: IPv6 Network Configuration Settings

SETTING	DESCRIPTION
Interface ID	Enables changing the 64-bit alternative interface ID for the device. The string is colon separated, for example, ff:dd:88:66:cc:1:2:3.
DAD Transmit Count	Enables changing the number of consecutive Neighbor Solicitation messages sent while performing Duplicate Address Detection (DAD) on a tentative address. A value of 0 indicates that DAD is not performed. The default is **1**.
Policy	The options are **Automatic** and **Manual**. Using **Automatic**, IPv6 configuration is set automatically. Using Manual enables manual IPv6 configuration of the IP address, gateway address, and DNS address.

The screen in *Figure 29* is available when Policy is set to Manual and Advanced Configuration is selected. This supports manual network address configuration.

Figure 29: Manual IPv6 Address Configuration Screen

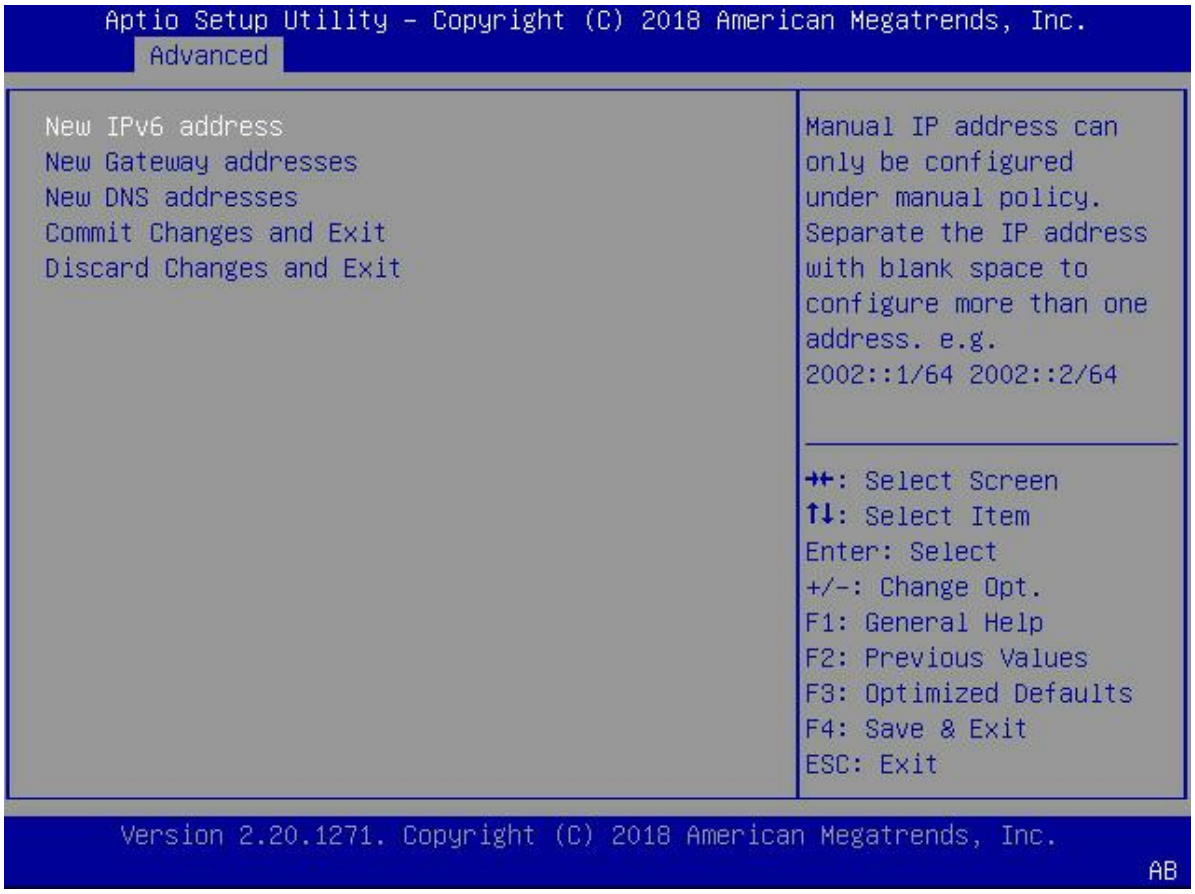


Table 15: Manual IPv6 Address Configuration

SETTING	DESCRIPTION
New IPv6 address	A manual IP address can be configured only under manual policy, for example, 2002::1/64.
New Gateway addresses	A gateway IP address can be configured only under manual policy. Use a space to separate IP addresses to configure more than one gateway address, for example, 2002::2 2002::3.
New DNS addresses	A DNS address can be configured only under manual policy. Use a space to separate IP addresses to configure more than one DNS address, for example, 2002::4/64 2002::5/64.
Commit Changes and Exit	Commit changes and exit.
Discard Changes and Exit	Discard changes and exit.

4.15 MAC:XXXXXXXXXXXX-HTTP Boot Configuration

When the HTTP boot feature is enabled on the **Network Configuration** screen, HTTP parameters can be configured for the device having MAC address XXXXXXXXXXXX.

Figure 30: HTTP Boot Configuration Screen

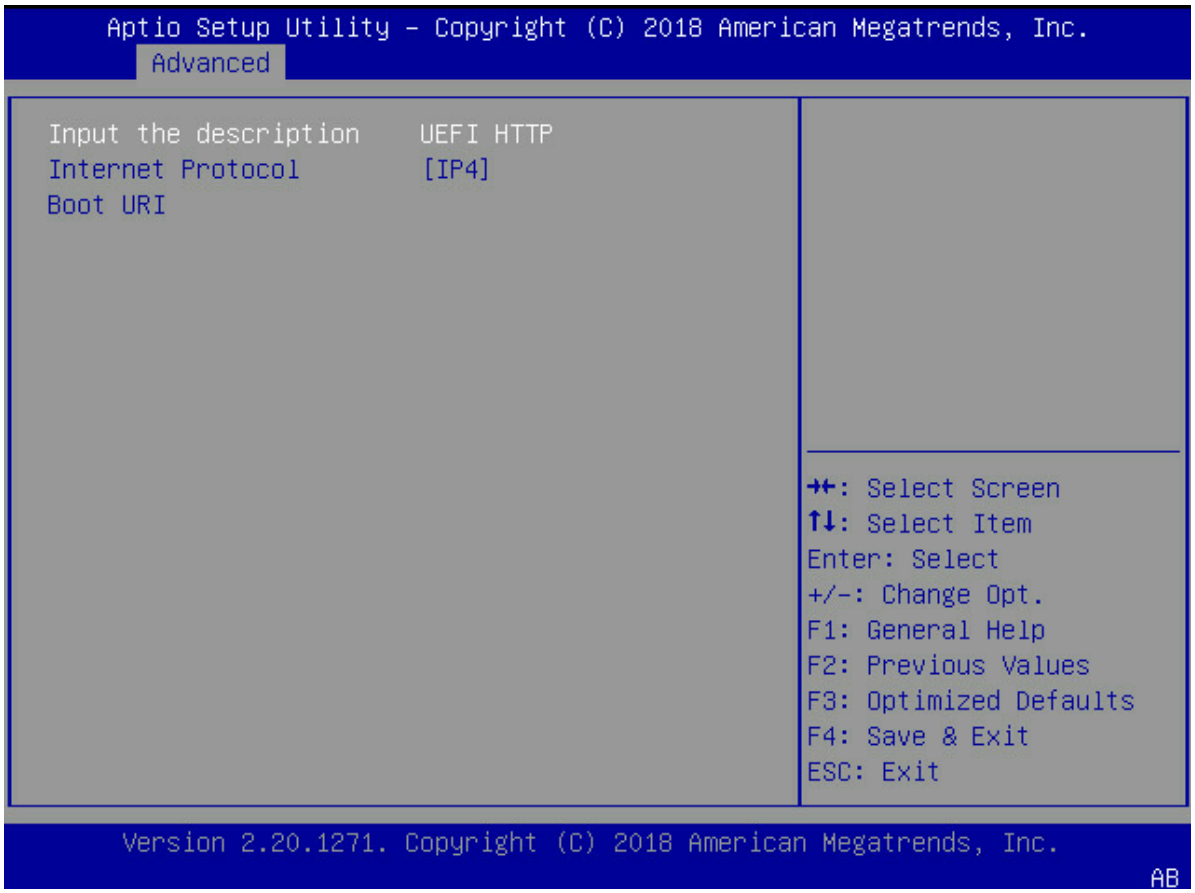


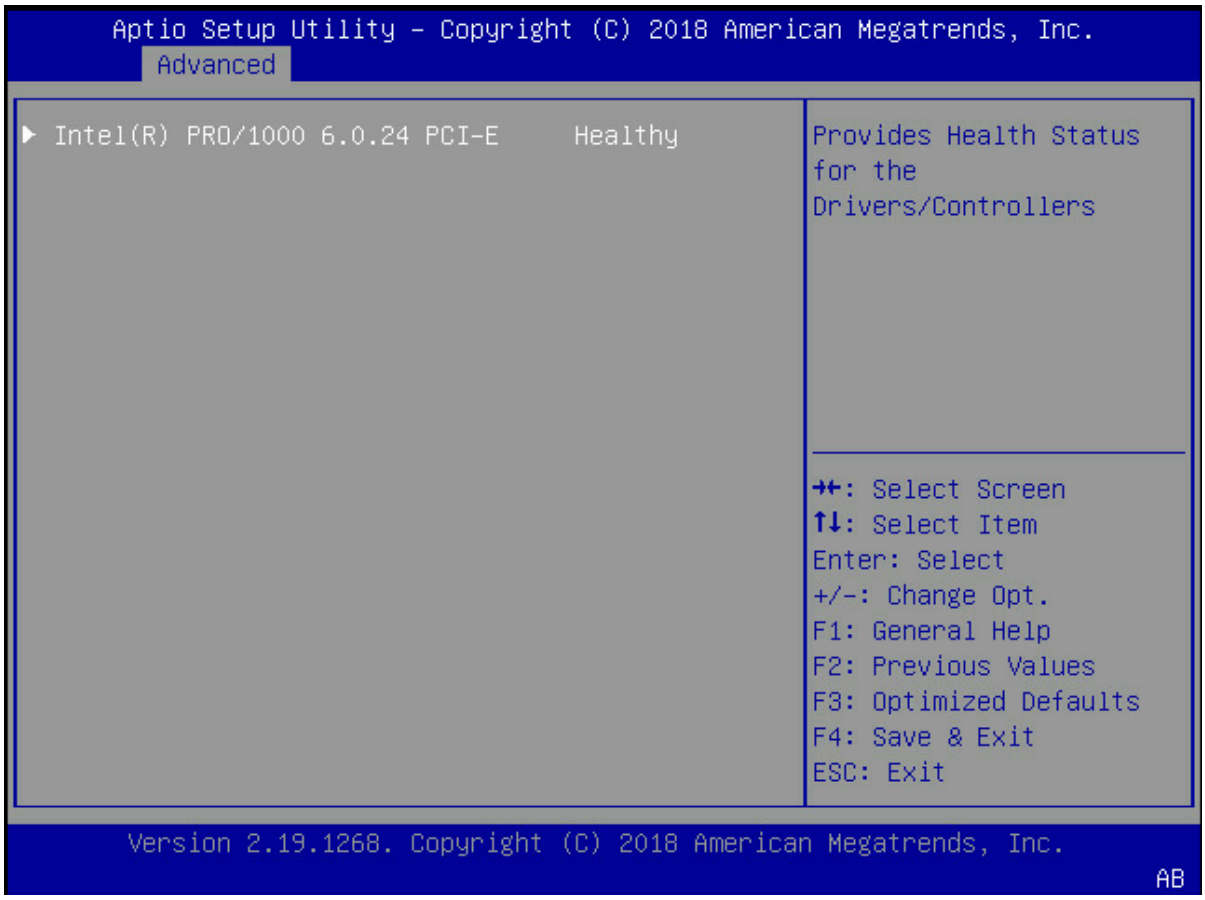
Table 16: HTTP Boot Settings

SETTING	DESCRIPTION
Input the description	Enter the description text for this HTTP boot.
Internet Protocol	Select **IPv4** or IPv6 for this HTTP boot.
Boot URI	A new Boot Option is created based upon this Boot URI.

4.16 Driver Health

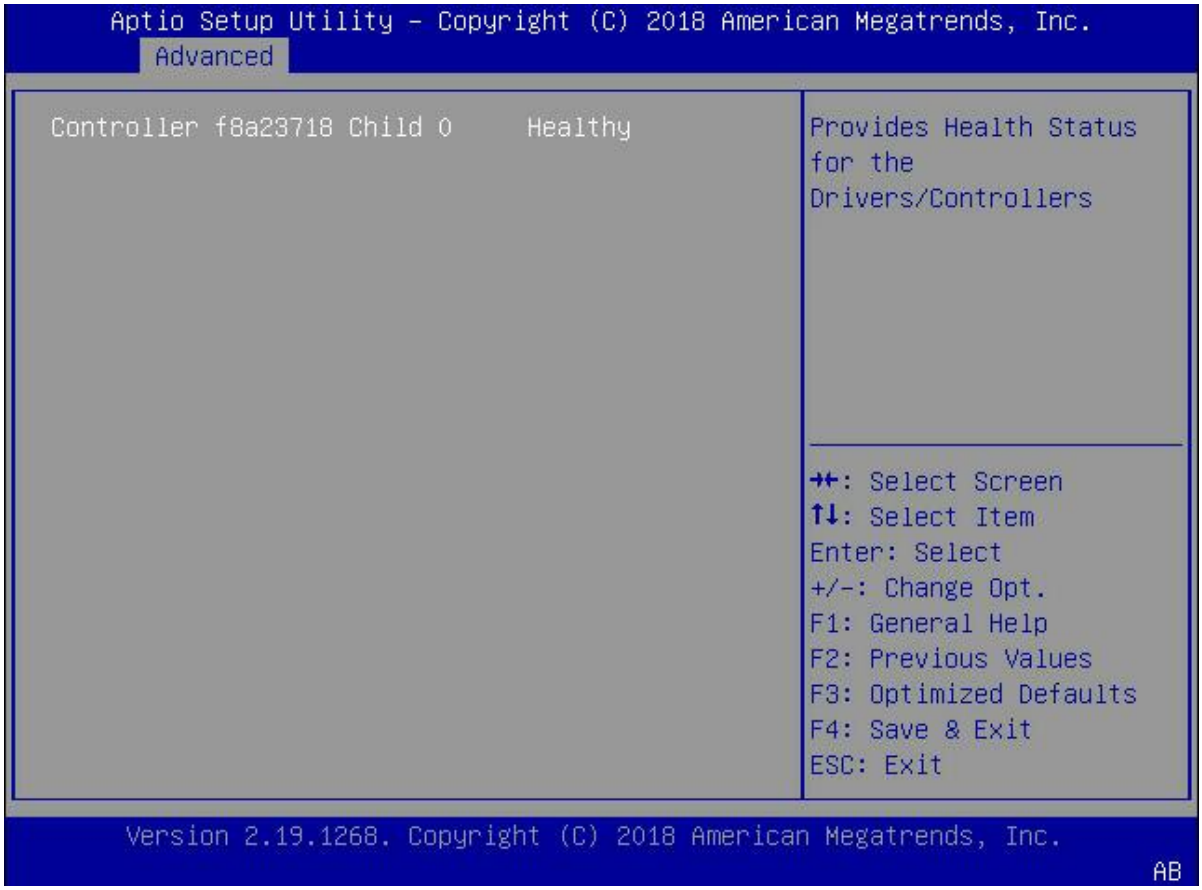
On the Advanced tab, press Enter at **Driver Health** to enter this setup screen, which shows all PCIe devices having drivers that install the driver health protocol.

Figure 31: Driver Health Screen (1 of 2)



Select the item to learn the status of the driver, such as Healthy, Failed, Configuration, and so on. The displayed information depends upon information provided by the driver.

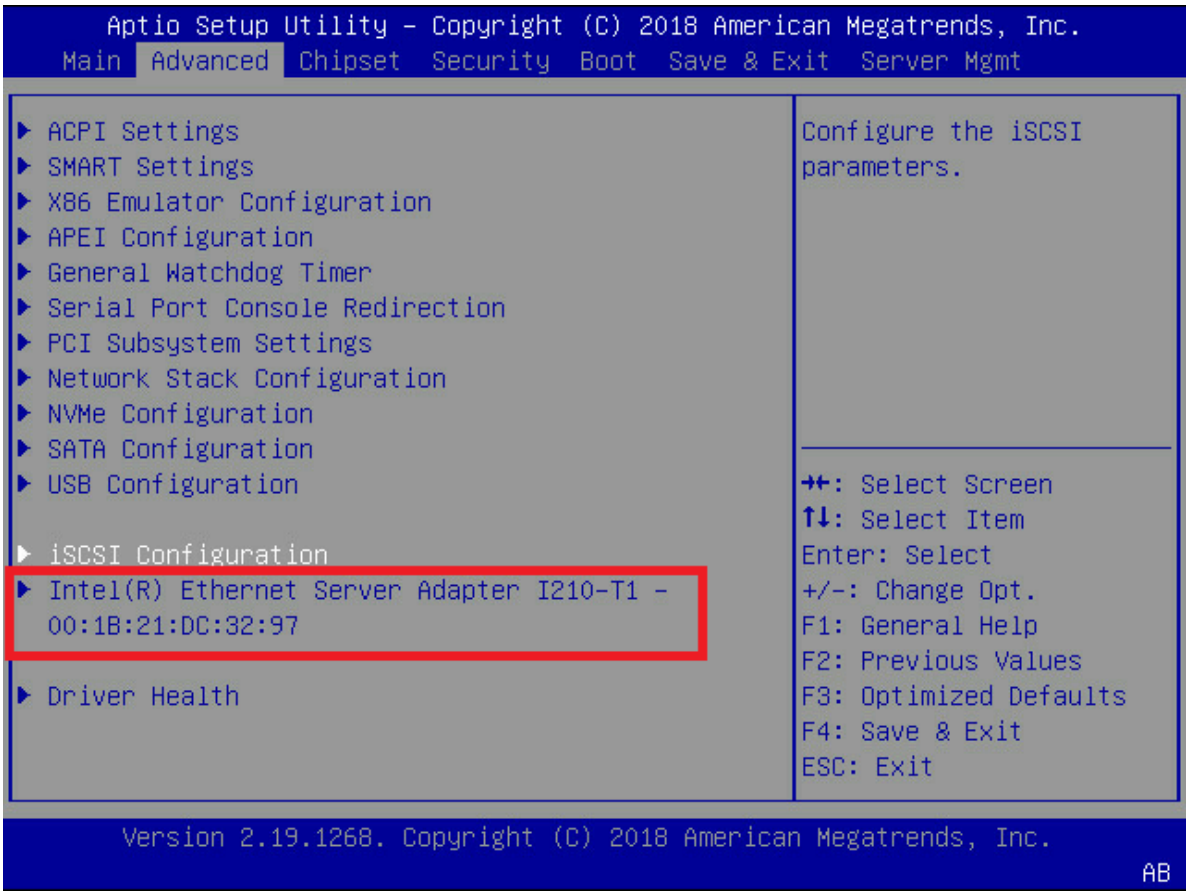
Figure 32: Driver Health Screen (2 of 2)



4.17 Additional Configuration Items

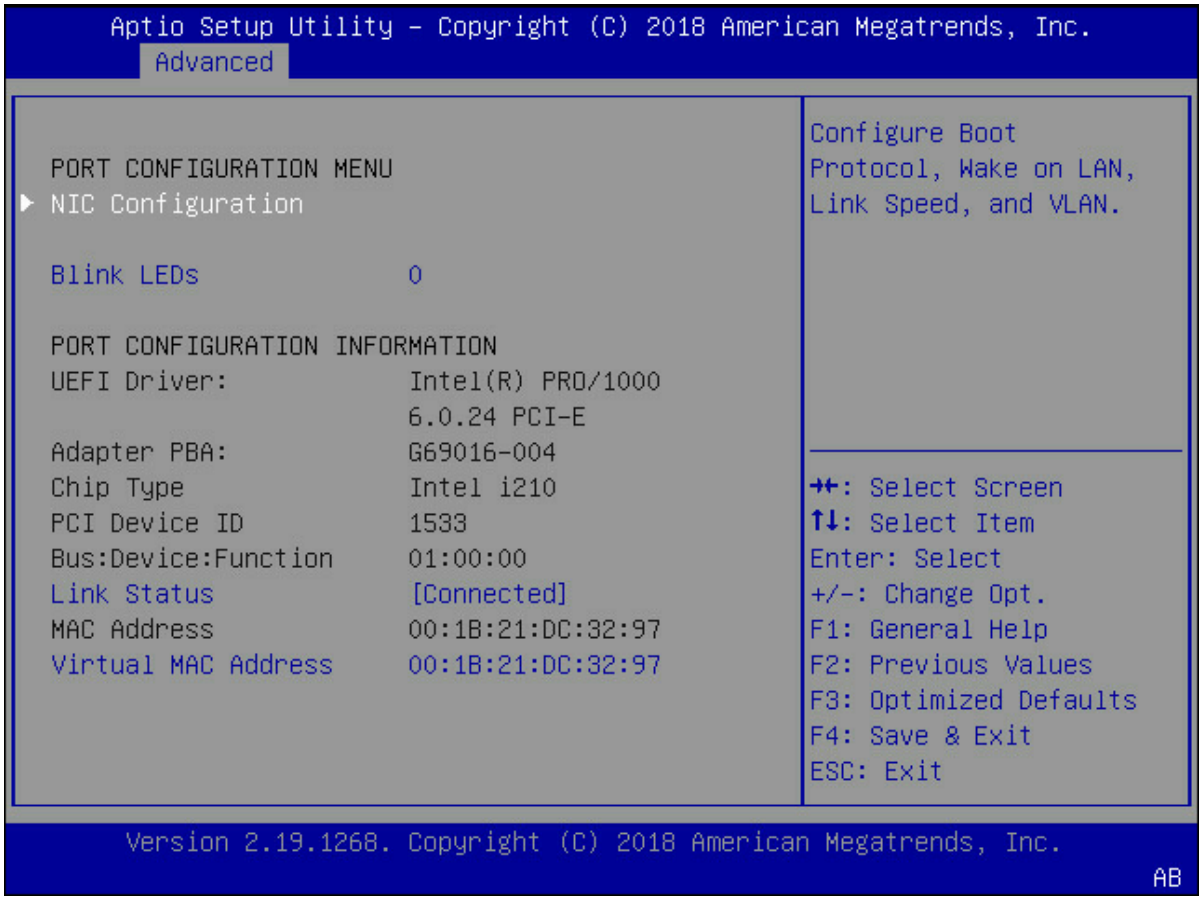
Depending upon the device drivers for installed PCIe devices, additional menu items may appear on the Advanced tab.

Figure 33: Additional Configuration Items



Selecting a menu item, for example, NIC Configuration, enables users to configure device parameters.

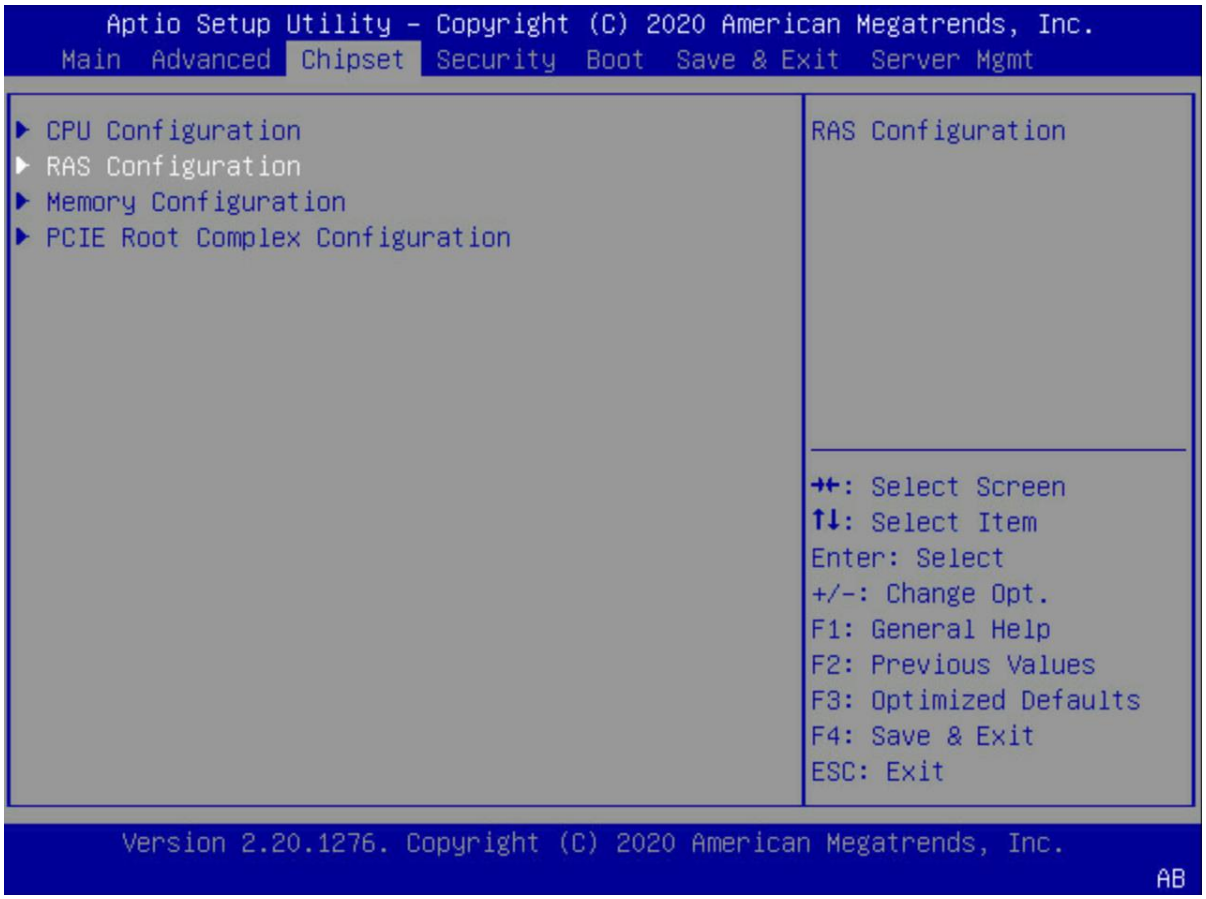
Figure 34: NIC Configuration Screen



5. Chipset Tab

Use the left or right arrow keys to select the Chipset tab. Use the up or down arrow keys to select items on the left pane of the tab. Use the Enter key to display available submenus for a selected item.

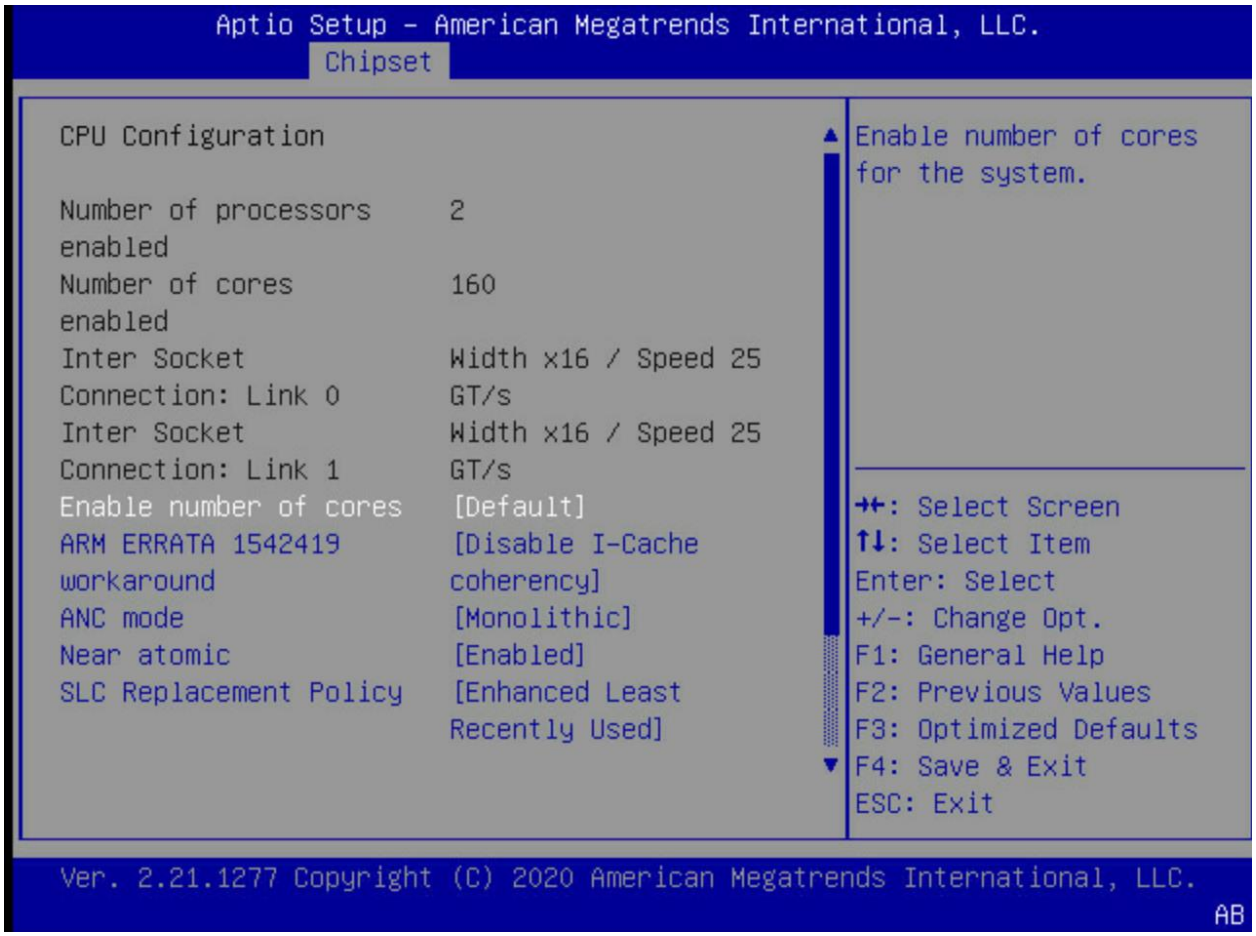
Figure 35: Chipset Tab



If the system is unstable after changing settings, use Save & Exit to revert to the default settings.

5.1 CPU Configuration

Figure 36: CPU Configuration Screen



Display information about all sockets.

Global settings are displayed:

- **Number of processors enabled:** Display the number of processors enabled in the system.
- **Number of cores enabled:** Display the number of cores enabled in the system for all processors.
- **Inter Socket Connection:** Link x: The information of inter socket connection. Only available if the system boots on 2P mode.
- **Enable number of cores:** Select the number of cores to be enabled in the system. This option requires a reboot to take effect.
- **ARM ERRATA 1542419:** Enable/Disable the ARM 1542419 workaround. Provides three options: Disable workaround, **Disable I-Cache coherency**, Trap each IC IVAU to EL3.
- **ANC mode:** Select the mode for Ampere Non-Uniform Memory Access (NUMA) control. This provides three modes: **Monolithic**, Hemisphere, and Quadrant. Systems with Monolithic mode have one NUMA partition per socket. Systems with Hemisphere mode have two NUMA partitions per socket. Systems with Quadrant mode have four NUMA partitions per socket.
- **Near atomic: Enable** or disable cacheable atomic instruction execution.
- **SLC Replacement Policy: Select replacement policy.** Change this feature *only if you know what you are doing*.

For each populated socket, these settings are displayed:

- **L1 Cache Size:** Display the CPU L1 Instruction Cache and Data Cache sizes, in KB, in each core.
- **L2 Cache Size:** Display the CPU L2 Cache size, in MB, in each Cluster Processor Module (CPM); each CPM contains two cores.
- **SLC:** Display the System Level Cache (SLC) size, in MB, for each processor.
- **Warranty:** Display warranty information for each processor.

5.2 Reliability, Availability, and Serviceability (RAS) Configuration

Figure 37: RAS Configuration Screen

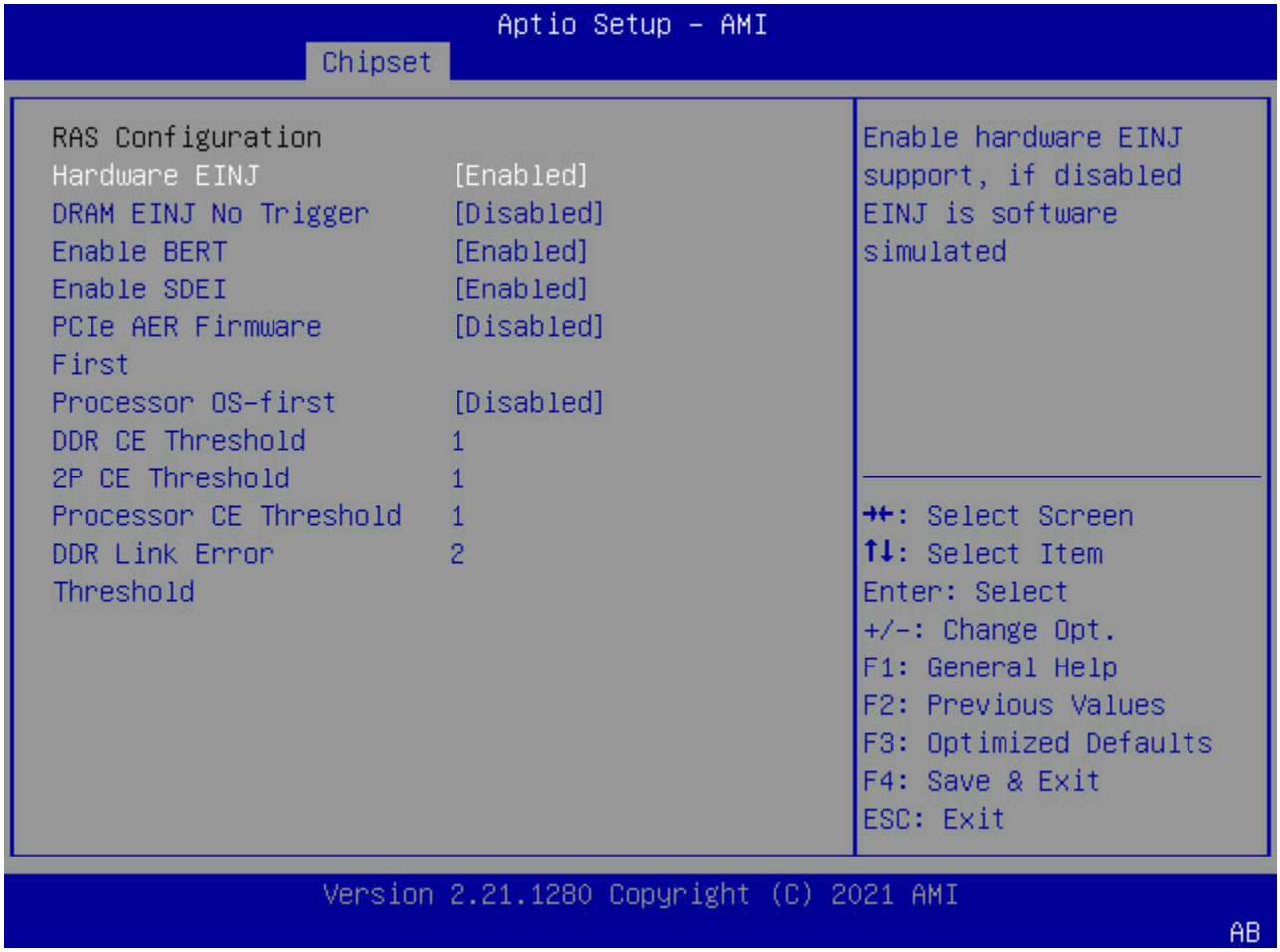


Table 17: RAS Configuration Parameters

SETTING	DESCRIPTION
Hardware EINJ	Enable Hardware Error Injection (EINJ) support. If supported and disabled, EINJ requests are software simulated. Hardware EINJ is supported only on non-warranty parts. The IRQ is 72 (external IRQ 0 – GPIO 0).
Enable BERT	Enable Boot Error Record Table (BERT). If disabled, BERT will not be populated when a catastrophic error occurs.
Enable SDEI	Enable Software Delegated Exception Interface (SDEI) for NMI support.
PCIe AER Firmware First	Enable firmware to detect PCIe AER. If disabled, OS detects PCIe AER.

SETTING	DESCRIPTION
Processor OS-First	Enable OS-first handling of processor errors through the AEST ACPI table.
DDR CE Threshold	Set the DDR CE Threshold. If a DDR CE occurs and the threshold is not met, the OS will only be notified through polled APEI HEST buffers. If the threshold is met, the OS will be notified through an SCI based APEI HEST buffer for immediate reporting/handling. **Note:** When the board "DRAM CE Threshold Windows Filter" feature is enabled, this UEFI RAS configuration feature will be hidden and disabled.
2P CE Threshold	Set the 2P Link CE Threshold. If a 2P Link CE occurs and the threshold is not met, the OS will only be notified through polled APEI HEST buffers. If the threshold is met, the OS will be notified through an SCI based APEI HEST buffer for immediate reporting/handling.
Processor CE Threshold	Set the Processor CE Threshold. If a Processor CE occurs and the threshold is not met, the OS will only be notified through polled APEI HEST buffers. If the threshold is met, the OS will be notified through an SCI based APEI HEST buffer for immediate reporting/handling.
DDR Link Error Threshold	Set the DDR Link Error Threshold. If DDR Link Errors occur and the threshold is not met, then they will be considered corrected by the hardware. If DDR Link Errors occur and the threshold is met, they will be considered as a persistent error and reported to the OS as a fatal severity.

5.3 Memory Configuration

Figure 38: Memory Configuration Screen

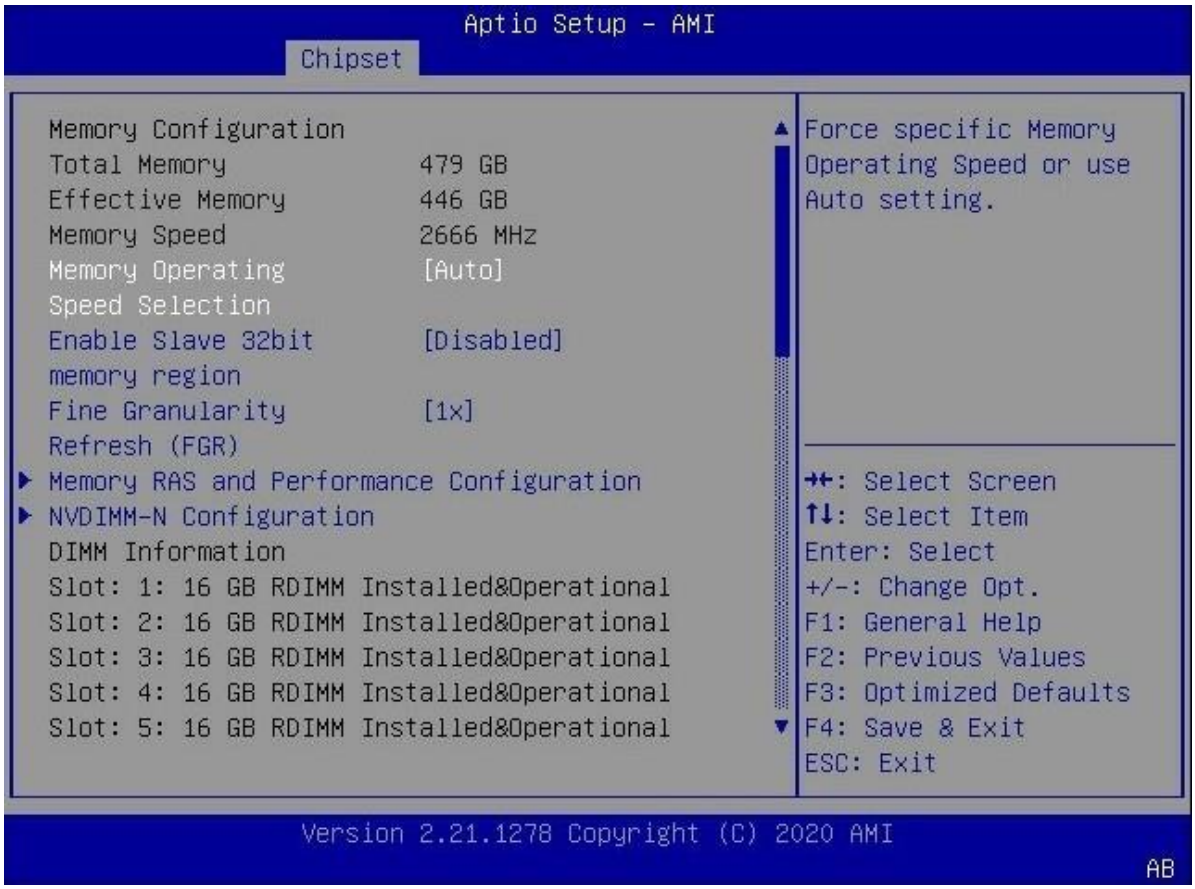


Table 18: Memory Configuration Parameters

SETTING	DESCRIPTION
Total memory	The total memory installed in the system.
Effective Memory	The memory available for UEFI and OSes. Some memory is reserved for lower-level firmware and is not otherwise available.
Memory Speed	The current speed, in MHz, at which the DDR controller runs.
Memory Operating Speed Selection	Sets the speed of DDR controller. The options are: **Auto**, 2133, 2400, 2666, 2933, and 3200. Changing this option can make the system unstable. The system recovers to the previous value if booting fails.
Enable Slave 32-bit memory region	When a processor is populated in the slave socket, this option Enables/**Disables** a 32-bit memory region (1 GB) of that processor. This option supports recapping all memory regions as much as possible. Enabling this option can slow OS boot.
Memory RAS and Performance Configuration	Displays and provides options to change memory Reliability, Availability, and Serviceability (RAS) and performance settings.
NVDIMM-N Configuration	Displays and provides options to change NVDIMM-N settings.
DIMM Information	Displays DDR information for the memory slots in the system.

Figure 39: Memory RAS and Performance Configuration Screen

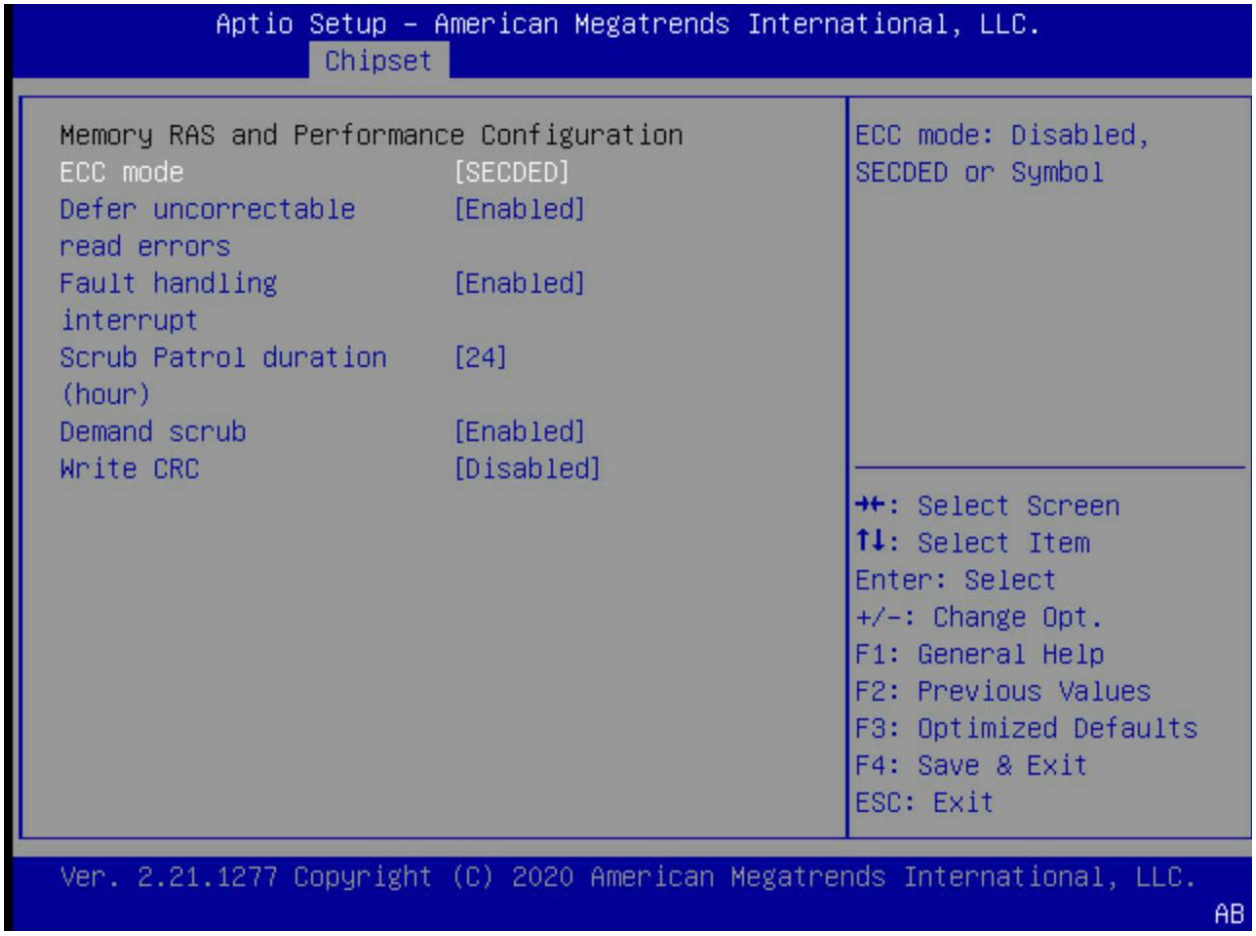


Table 19: Memory Performance Parameters

SETTING	DESCRIPTION
ECC mode	Provides 3 ECC modes: Disabled, Single Error Correction and Double Error Detection (**SECDED**), or Symbol for all memory controllers.
Defer uncorrectable read errors	When **Enabled**, the DMC defers uncorrectable read errors to the consumer by sending an OK response and setting the TXDAT poison flag on the CHI-B interconnect. If this bit is clear, the DMC defaults to non-deferred behavior when encountering an unrecoverable error.
Fault handling interrupt	The fault handling interrupt is **Enabled**. This interrupt is raised to notify that an ECC fault is recorded.
Scrub Patrol duration	Select duration (hour) for Scrub patrol.
Demand scrub	**Enable**/Disable the ability to write corrected data back to the memory once a correctable error is detected.
Write CRC	Enable/**Disable** Cyclic Redundancy Check (CRC) functionality on write data. Note that enabling CRC will degrade Write bandwidth.

If a DIMM fails, the system reconfigures to the next-best channel configuration to ensure that the system can still boot at the same DDR speed.

Table 20: Supported Memory Channel Configurations

CONFIG	CHANNELS	MC7	MC6	MC5	MC4	MC3	MC2	MC1	MC0	COMMENT
1	8	Y	Y	Y	Y	Y	Y	Y	Y	All channels work
2	6	–	Y	Y	Y	–	Y	Y	Y	Channel 3 or 7 failed
3	6	Y	–	Y	Y	Y	–	Y	Y	Channel 2 or 6 failed
4	6	Y	Y	–	Y	Y	Y	–	Y	Channel 1 or 5 failed
5	6	Y	Y	Y		Y	Y	Y		Channel 0 or 4 failed
6	4	–	–	Y	Y	–	–	Y	Y	Channel 2,3 or 6,7 failed
7	4	–	Y	–	Y		Y	–	Y	Channel 1,3 or 5,7 failed
8	4	Y	–	–	Y	Y	–	–	Y	Channel 1,2 or 5,6 failed
9	4	–	Y	Y			X	Y	–	Channel 0,3 or 4,7 failed
10	4	Y	–	Y	–	Y	–	Y	–	Channel 0,2 or 4,6 failed
11	4	Y	Y	–	–	Y	X		–	Channel 0,1 or 4,5 failed
12	2	–	–	–	X	–	–	–	Y	Channel 1,2,3 or 5,6,7 failed
13	1	–	–	–	–	–	–	–	Y	Only Channel 0 works
14	1	–	–	–	–	–	–	Y	–	Only Channel 1 works
15	1	–	–	–	–	–	Y	–	–	Only Channel 2 works
16	1	–	–	–	–	Y	–	–	–	Only Channel 3 works
17	1	–	–	–	Y	–	–	–	–	Only Channel 4 works
18	1	–	–	Y	–	–	–	–	–	Only Channel 5 works
19	1	–	Y	–	–	–	–	–	–	Only Channel 6 works
20	1	Y	–	–	–	–	–	–	–	Only Channel 7 works

Figure 40: NVDIMM-N Configuration

Table 21: NVDIMM-N Configuration Settings

SETTING	DESCRIPTION
Socket0 Configured Mode	Current configured NVDIMM-N mode of Socket0.
Socket1 Configured Mode	Current configured NVDIMM-N mode of Socket1.
Mode Selection	Select NVDIMM-N mode: **Non-NVDIMM**: Configure NVDIMM-N to work like normal DIMM. **Non-Hashed**: Configure NVDIMM-N to work in non-hashed mode. **Hashed**: Configure NVDIMM-N to work in hashed mode. **Auto**: NVDIMM-N works in default Hashed mode if NVDIMM-N are plugged at both Channel 3 (Slot 6) and Channel 7 (Slot 14). Otherwise, NVDIMM-N will work in Non-Hashed mode if there is only one NVDIMM-N plugged at Channel 3 or Channel 7. **Note**: A switch between Hashed and Non-Hashed mode will make previous stored data unusable.

5.4 PCIe Root Complex (RC) Configuration

Note: UEFI automatically configures PCIe based on the detected riser card. Users must not change RC settings.

Figure 41: PCIe RC Configuration Screen

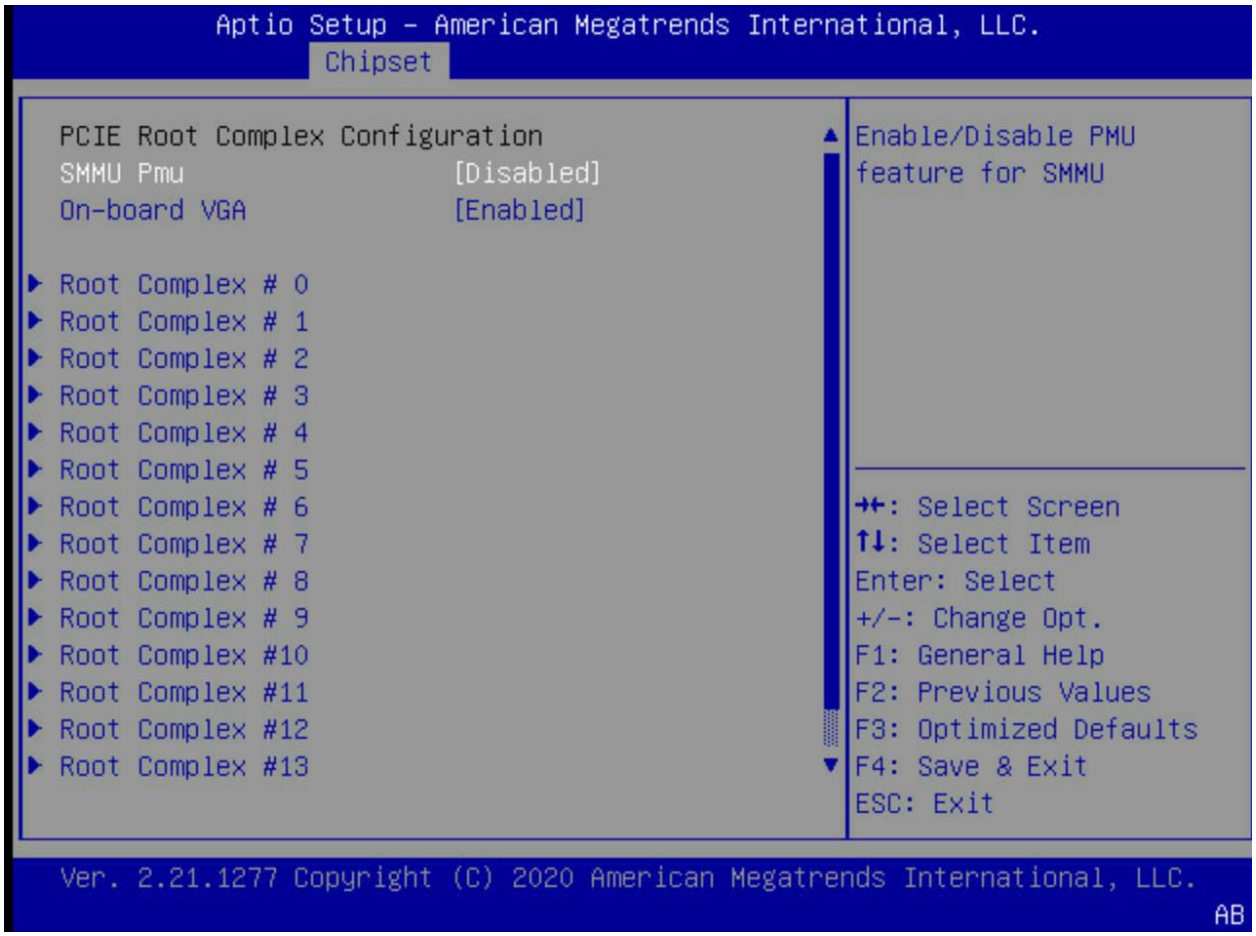


Table 22: PCIe RC Configuration Settings

SETTING	DESCRIPTION
SMMU Pmu	Enable PMU feature for SMMU. Ensure you use the above Linux 5.8; otherwise, the system may crash during booting.
On-board VGA	**Enable**/disable on-board VGA.

When selecting each entry, the following screen is displayed.

Figure 42: Selected RC Screen

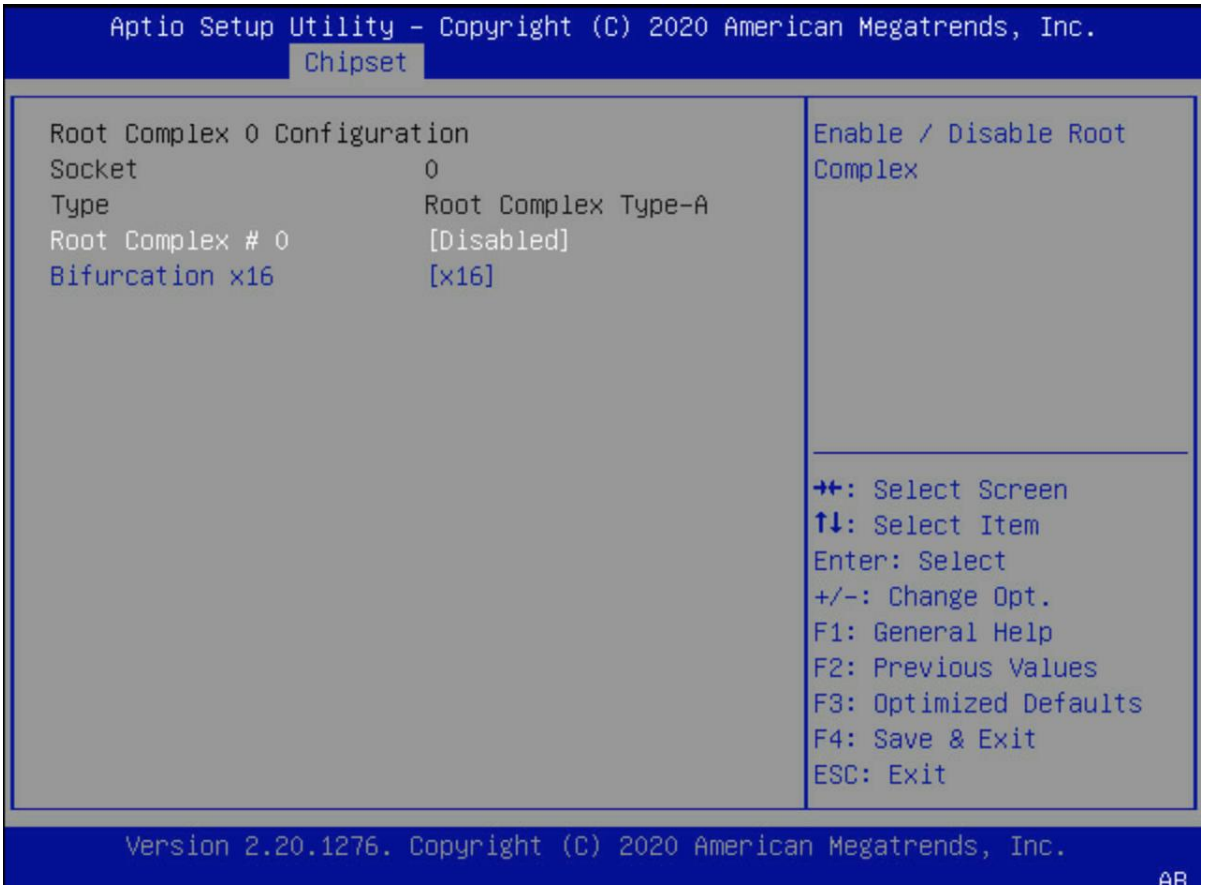


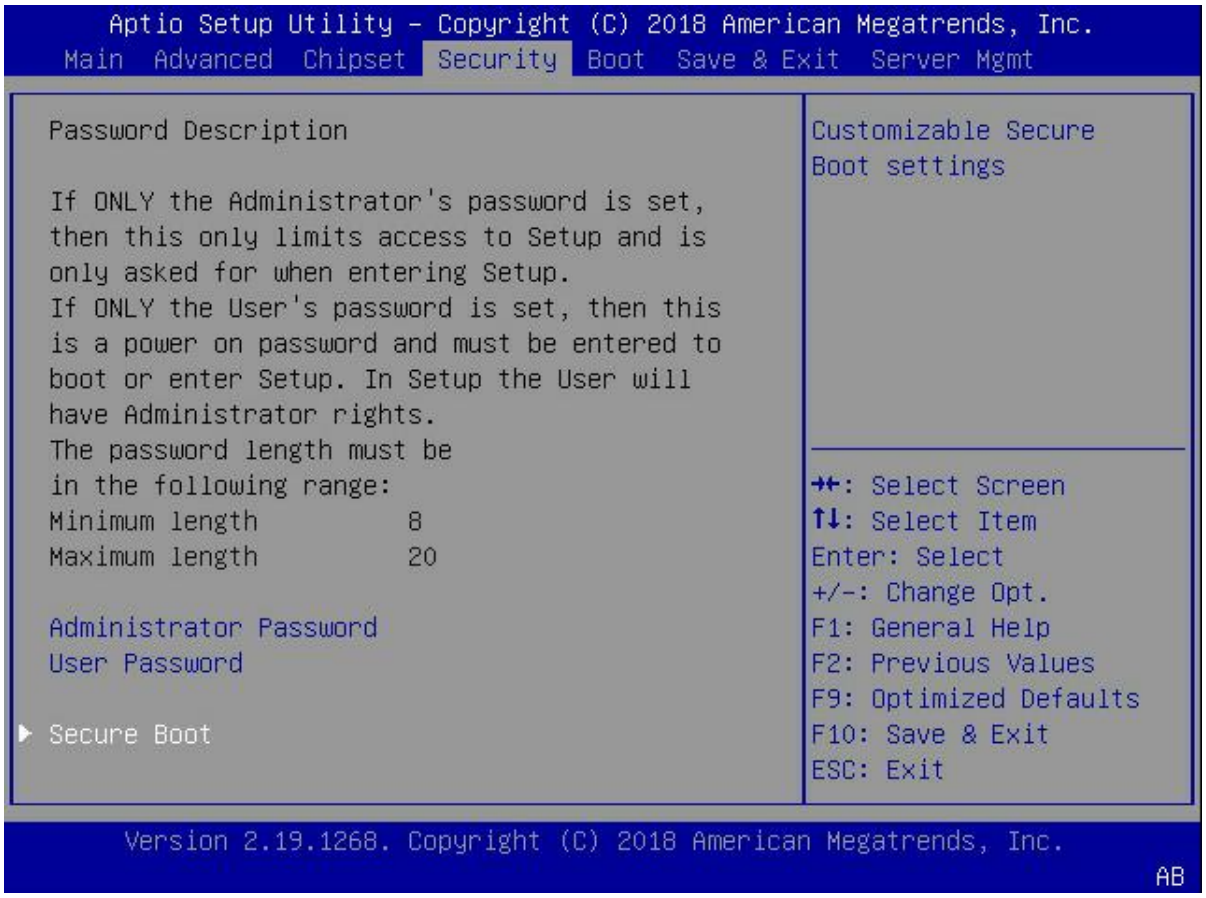
Table 23: Root Complex Configuration

SETTING	DESCRIPTION
Socket	The socket associated with the RC.
Type	The RC type: Type-A or Type-B.
RC #	Enable or disable this RC. The default setting is dependent upon board settings.
Bifurcation	Enable changing the RC bifurcation setting.

6. Security Tab

Use the left or right arrow keys to select the Security tab. Use the up or down arrow keys to select items on the left pane of the tab. Use the Enter key to display available submenus for a selected item.

Figure 43: Security Tab

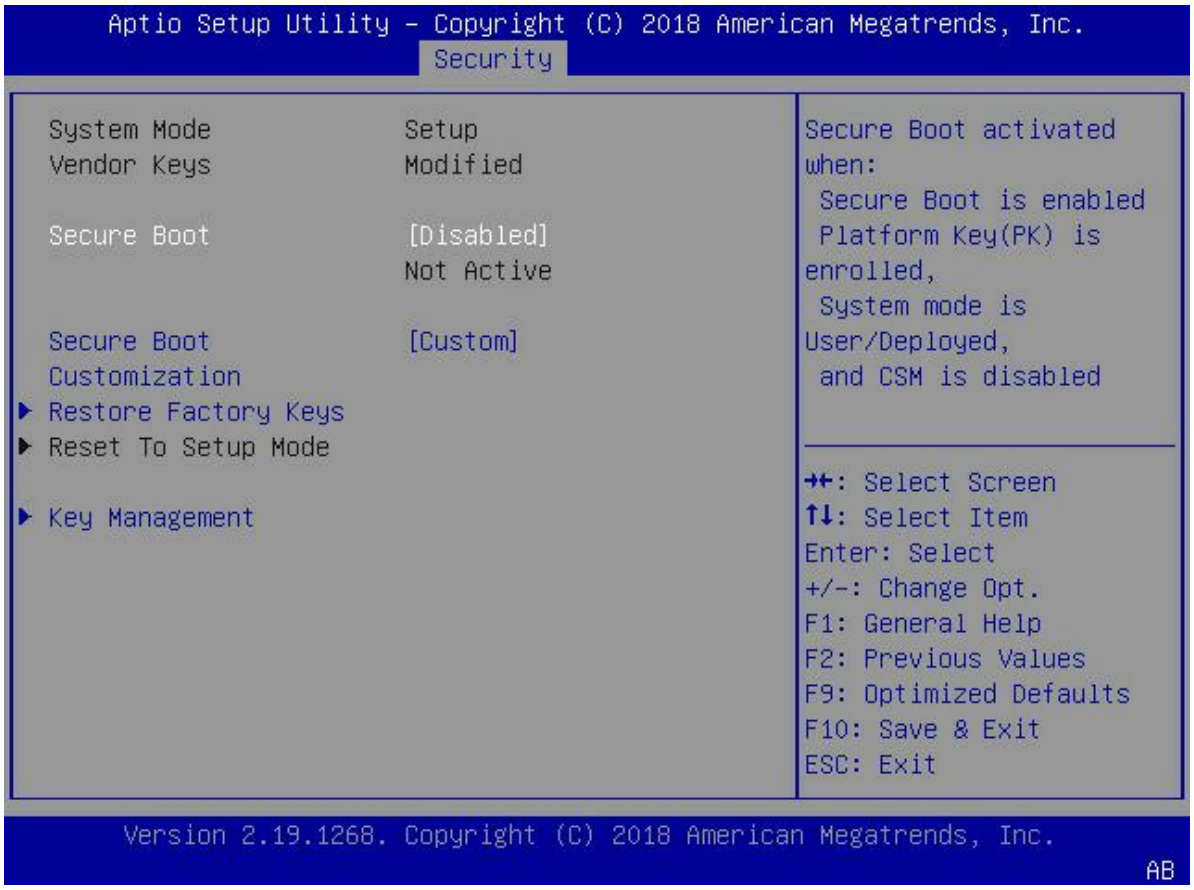


- **Administrator Password:** Selecting this option enables users to set the Administrator password.
- **User Password:** Selecting this option enables users to set the User password.

6.1 Secure Boot

Select **Secure Boot** to configure boot mode and manage keys.

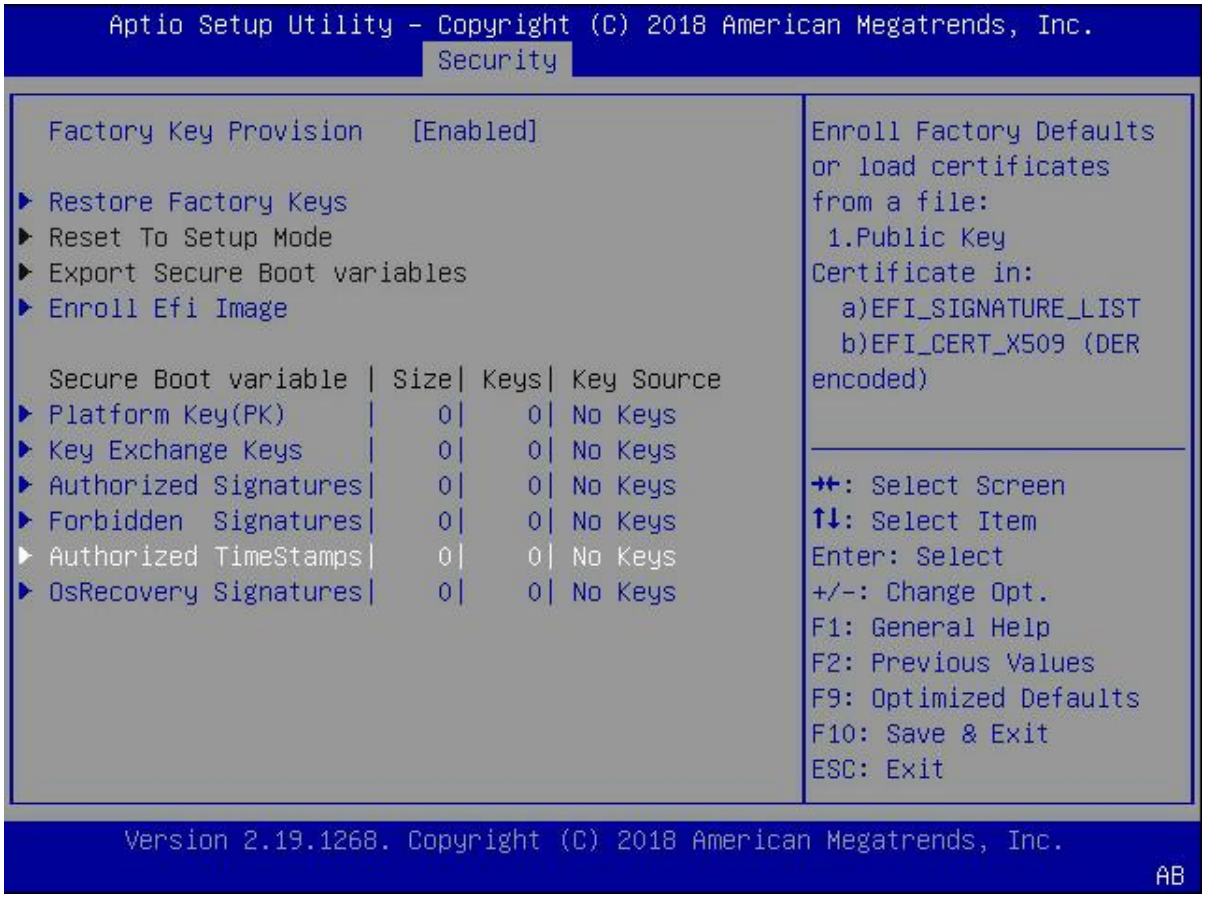
Figure 44: Secure Boot Screen



- **Secure Boot**: Allows users to enable and disable the secure boot feature. The default is **Disabled**.
  The secure boot feature is active when secure boot is enabled, Platform Key (PK) is enrolled, and the system is in User mode. A mode change requires a platform reset.
- **Secure Boot Customization**: The secure boot mode options are Standard and Custom. In Custom mode, a physically present user can configure secure boot policy variables without full authentication.
- **Restore Factory Keys:** Forces the system to User mode and installs factory-default secure boot key databases.
- **Reset To Setup Mode:** Delete the NVRAM content of all UEFI secure boot keys.
- **Key Management**: Enables a user to configure key management settings.

6.1.1 Key Management

Figure 45: Factory Key Provision Screen



Key management accesses these formats:

- Public Key Certificate: EFI Signature List, EFI CERT X509 (DER Encoded), EFI CERT RSA2048 (Bin), EFI SERT SHAXXX
- Authenticated UEFI Variable
- Authenticated UEFI Variable
- Key Source: Factory, External, Mixed.

Settings for key management:

- Factory Key Provision: If enabled, install factory default Secure Boot keys after platform reset. This applies only when the system is in setup mode.
- Restore Factory Keys: To force the system to user mode, configure NVRAM to contain OEM-defined factory default secure boot keys.
- Reset to Setup Mode: Delete all secure boot key databases from NVRAM.
- Export Secure Boot variables: Copy the NVRAM content of secure boot variables to files in a root folder on a file system device.
- Enroll EFI Image: Enables the image to run in secure boot mode. Enroll the SHA256 Hash certificate of a PE image into Authorized Signature database.

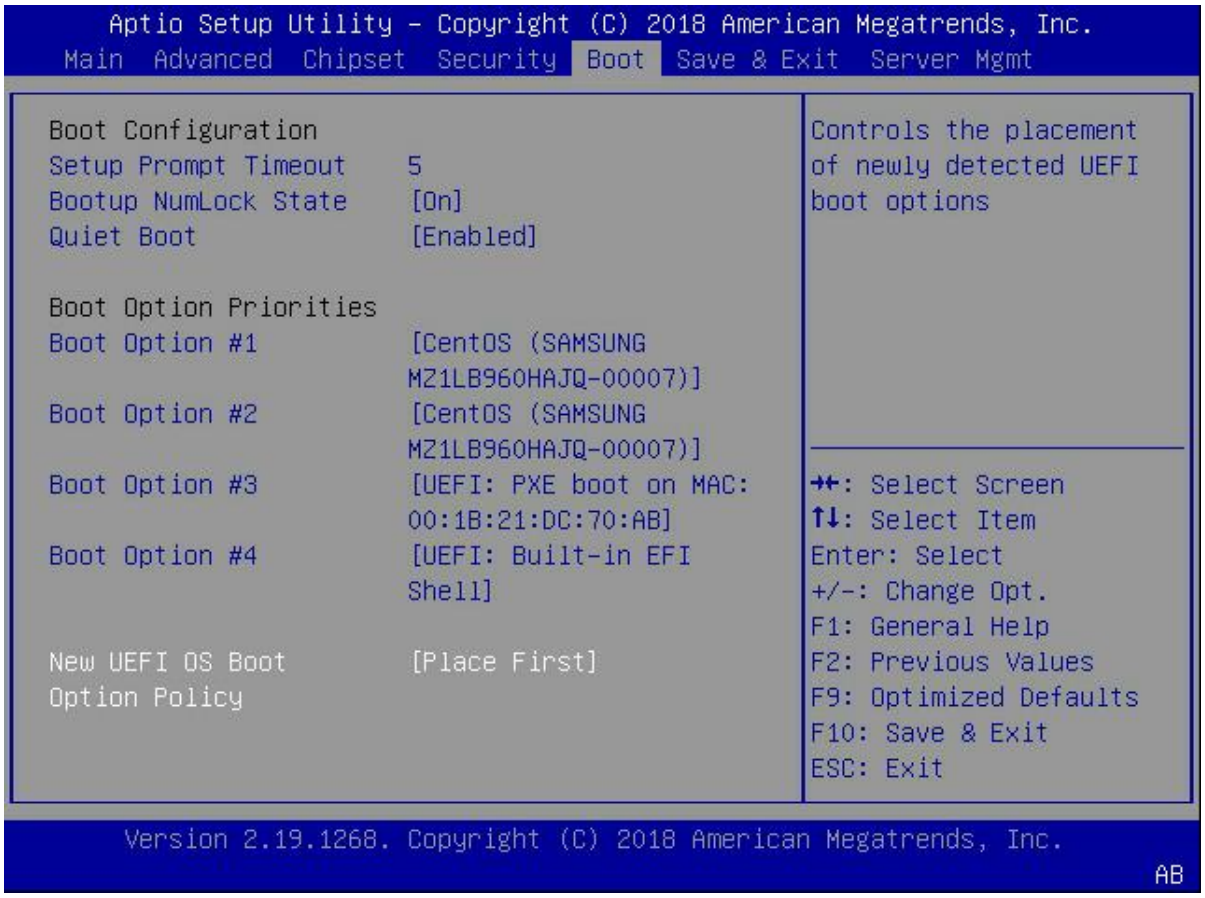
6.1.1.1 Secure Boot Variables

- Platform Key (PK): Enables users to configure PK settings. Users can update the settings using a value from factory defaults or from a file in the file system.
- Key Exchange Key (KEK): Enables users to configure KEK settings. Users can update or append this using a value from factory defaults or from a file in the file system.
- Authorized Signatures: Enables users to configure Authorized Signatures settings. Users can update or append this using a value from factory defaults or from a file in the file system.
- Forbidden Signatures: Enables users to configure Forbidden Signatures settings. Users can update or append this using a value from factory defaults or from a file in the file system.
- Authorized TimeStamps: Enables users to configure the settings of the Authorized TimeStamps. Users can update or append this using a value from factory defaults or from a file in the file system.
- OsRecovery Signatures: Enables users to configure the settings of the OsRecovery Signatures. Users can update or append this using a value from factory defaults or from a file in the file system.

7. Boot Tab

Use the left or right arrow keys to select the Boot tab. Use the up or down arrow keys to select items on the left pane of the tab. Use the Enter key to display available submenus for a selected item.

Figure 46: Boot Tab



7.1 Boot Configuration

- **Setup Prompt Timeout:** Set the number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting. The default is **5** seconds.
- **Bootup NumLock State:** Select the keyboard NumLock state when booting. The options are **On** and Off.
- **Quiet Boot:** Enables or disables the Quiet Boot option. The default value is **Enabled**.

7.2 Boot Option Priorities

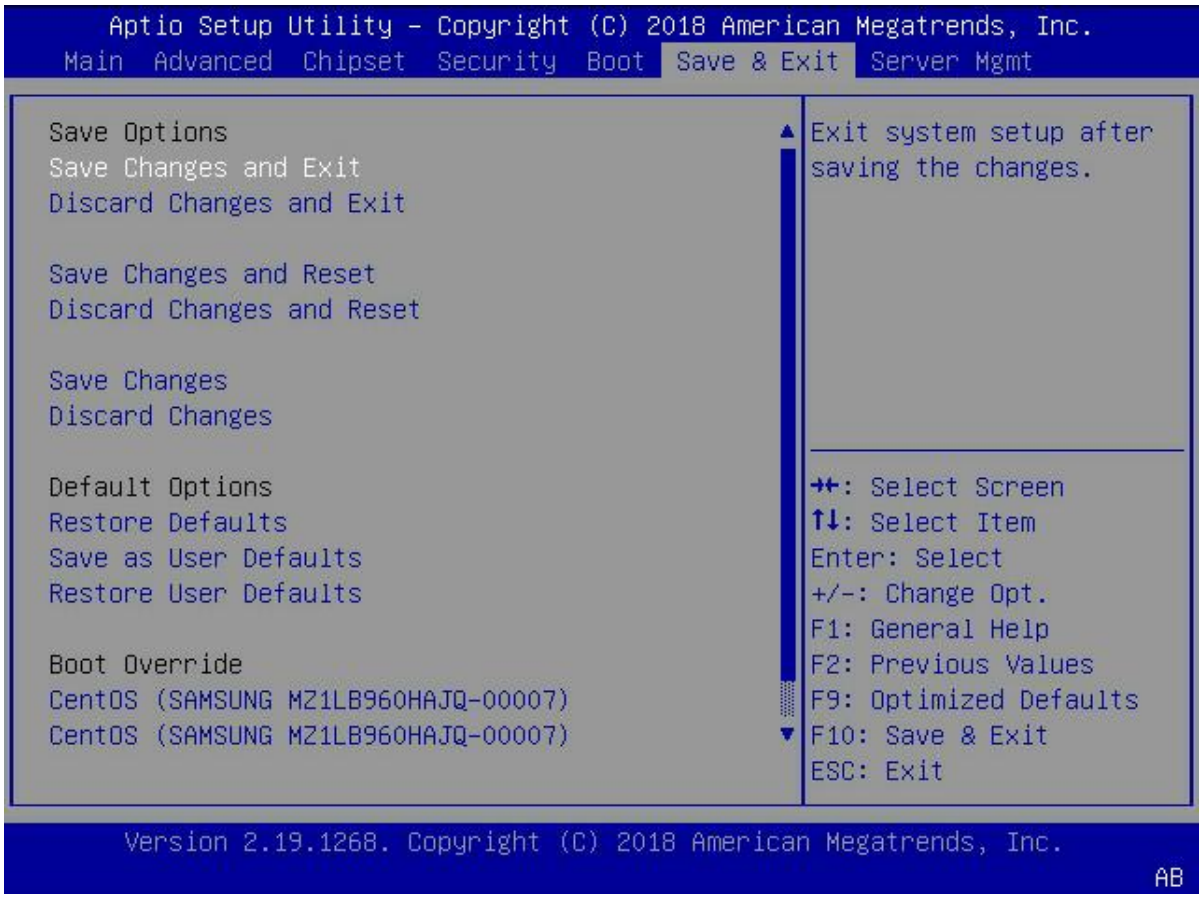
This prioritizes the order of bootable devices from which the system boots. To select devices, press Enter on each entry from top to bottom.

New UEFI OS Boot Option Policy controls the placement of newly detected UEFI boot options. The default is **Place First** so that any newly installed OS has the highest priority. The options are Default, **Place First**, and Place Last.

8. Save & Exit Tab

Use the left or right arrow keys to select the Save & Exit tab. Use the up or down arrow keys to select items on the left pane of the tab. Use the Enter key to display available submenus for a selected item.

Figure 47: Save & Exit Tab



8.1 Save Options

- **Save Changes and Exit:** Set this option to exit system setup after saving the changes.
- **Discard Changes and Exit:** Select this option to quit the BIOS Setup without making any permanent changes to the system configuration.
- **Save Changes and Reset:** Select this option to reset the system after saving the changes.
- **Save Changes:** Save the changes from users and allow users to continue to make changes.
- **Discard Changes:** Revert the system to its previous state.
- **Discard Changes and Reset:** Select this option to reset the system without changing the system configuration.

Note: UEFI is reset after **Save Changes and Exit** is selected and these settings have changed.

- RAS/APEI settings.
- X86 emulation settings.
- CPU settings.
- PCIe settings.
- Memory controller settings.

8.2 Default Options

- **Restore Defaults:** Set this option to restore factory settings, which are designed for maximum system stability rather than maximum performance.
- **Save as User Defaults:** Select this option to enables a user to save changes to the UEFI setup for future use.
- **Restore User Defaults:** Select this option to retrieve previously saved user-defined settings.

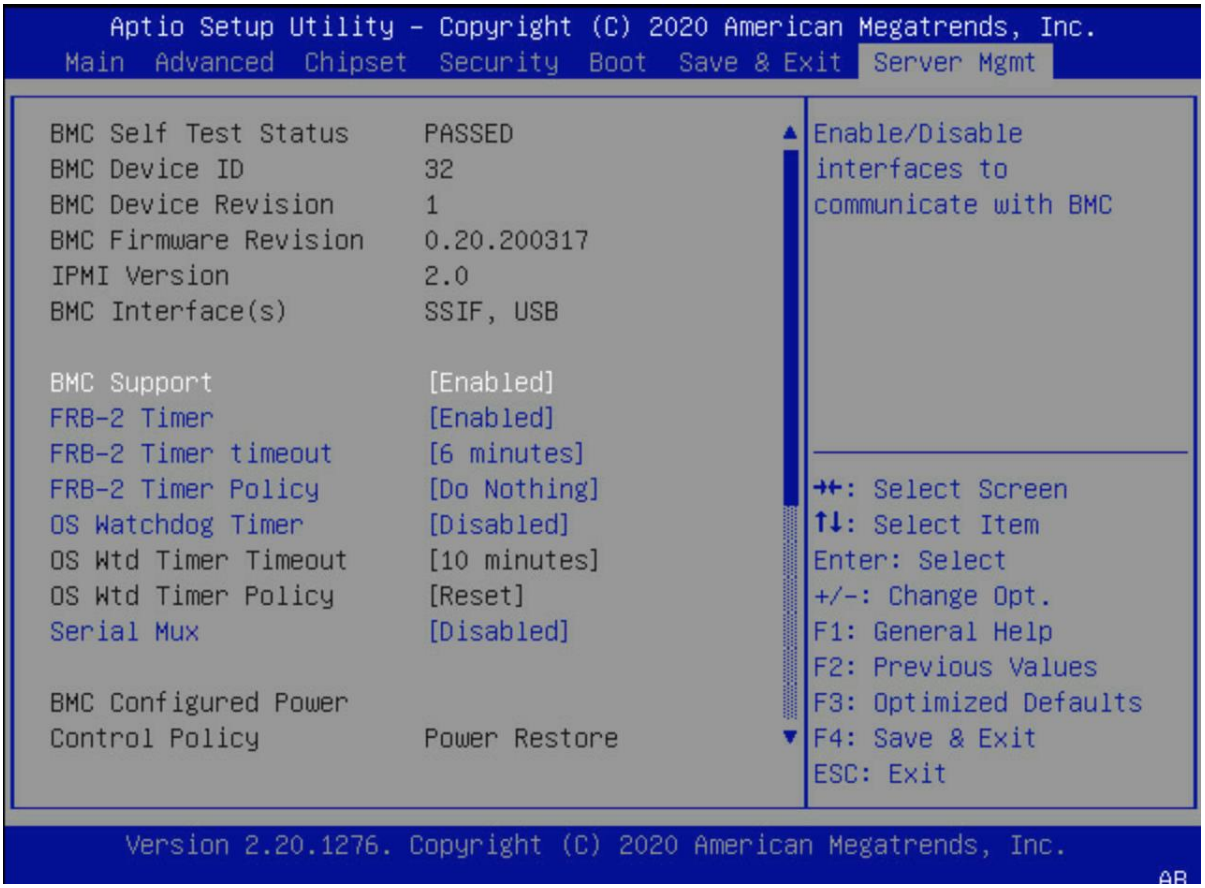
8.3 Boot Override

This section lists the boot options for the system. Select an option, press Enter, and the system boots using the selected boot option.

9. Server Mgmt Tab

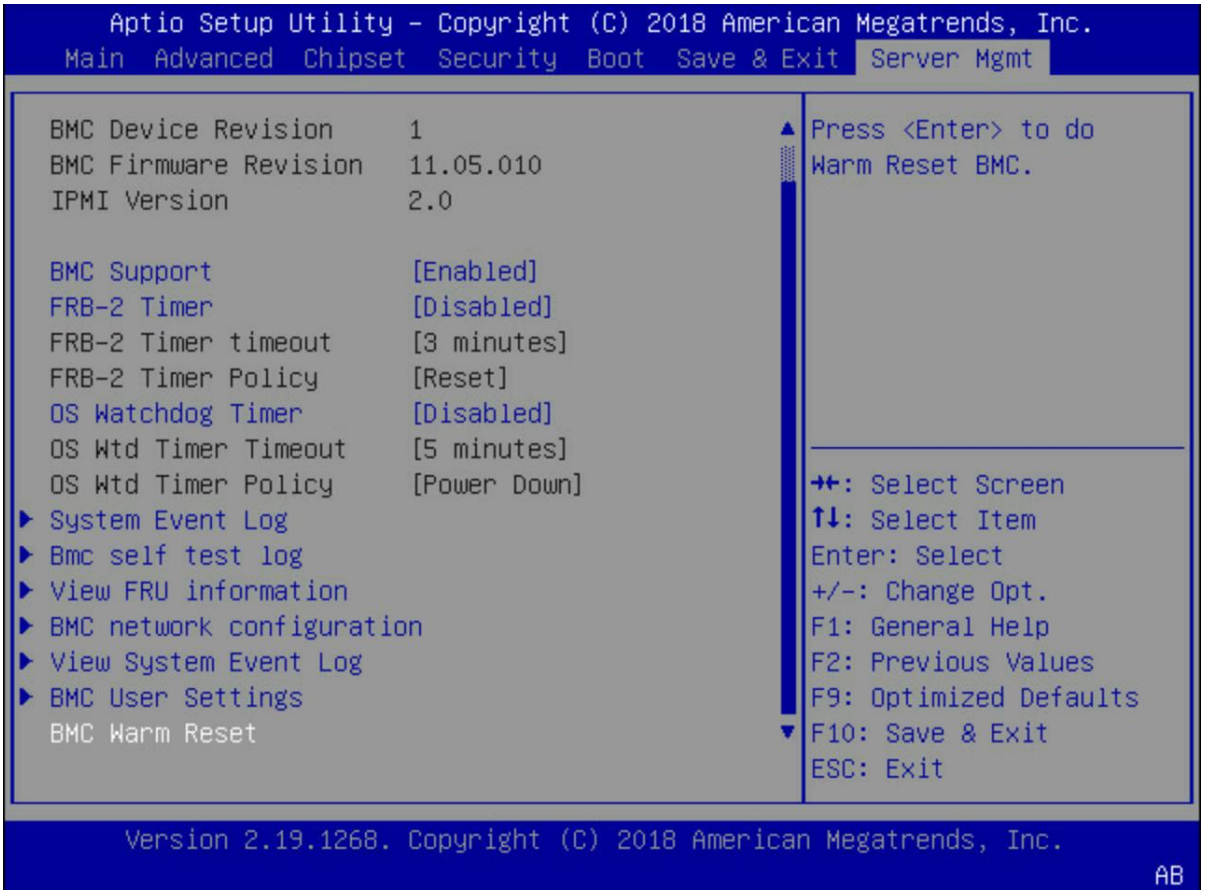
Use the left or right arrow keys to select the Server Mgmt tab. Use the up or down arrow keys to select items on the left pane of the tab. Use the Enter key to display available submenus for a selected item.

Figure 48: Server MGMT Tab (1 of 2)



- **BMC Support: Enable** and Disable interfaces to communicate with the BMC.
- **FRB-2 Timer:** Enable and **Disable** the Fault Resilient Booting (FRB-2) timer (POST Timer). When Enabled, the BMC ensures that the system completes POST.
- **FRB-2 Timer timeout:** Enter a value between 3 and 6 minutes for FRB-2 Timer Expiration value. The default is **6** minutes.
- **FRB-2 Timer Policy:** Select what to do in case the FRB-2 Timer expires. The options are: Do nothing, Reset, Power Down, and Power Cycle.
- **OS Watchdog Timer:** If Enabled, this starts a BIOS timer that only can be shut off by BMC after the OS loads. Helps determine that the OS successfully loaded.
- **OS Wtd Timer Timeout:** Configure the length of the OS Boot Watchdog Timer if the OS Boot Watchdog Timer is Enabled.
- **OS Wtd Timer Policy:** Configure the system response to OS Boot Watchdog Timer expiration if the OS Boot Watchdog Timer is Enabled.
- **View System Event Log**: Press Enter to view the **System Event Log**. It can take some time to retrieve all logs. See the section titled *View System Event Log* in this document for more information.

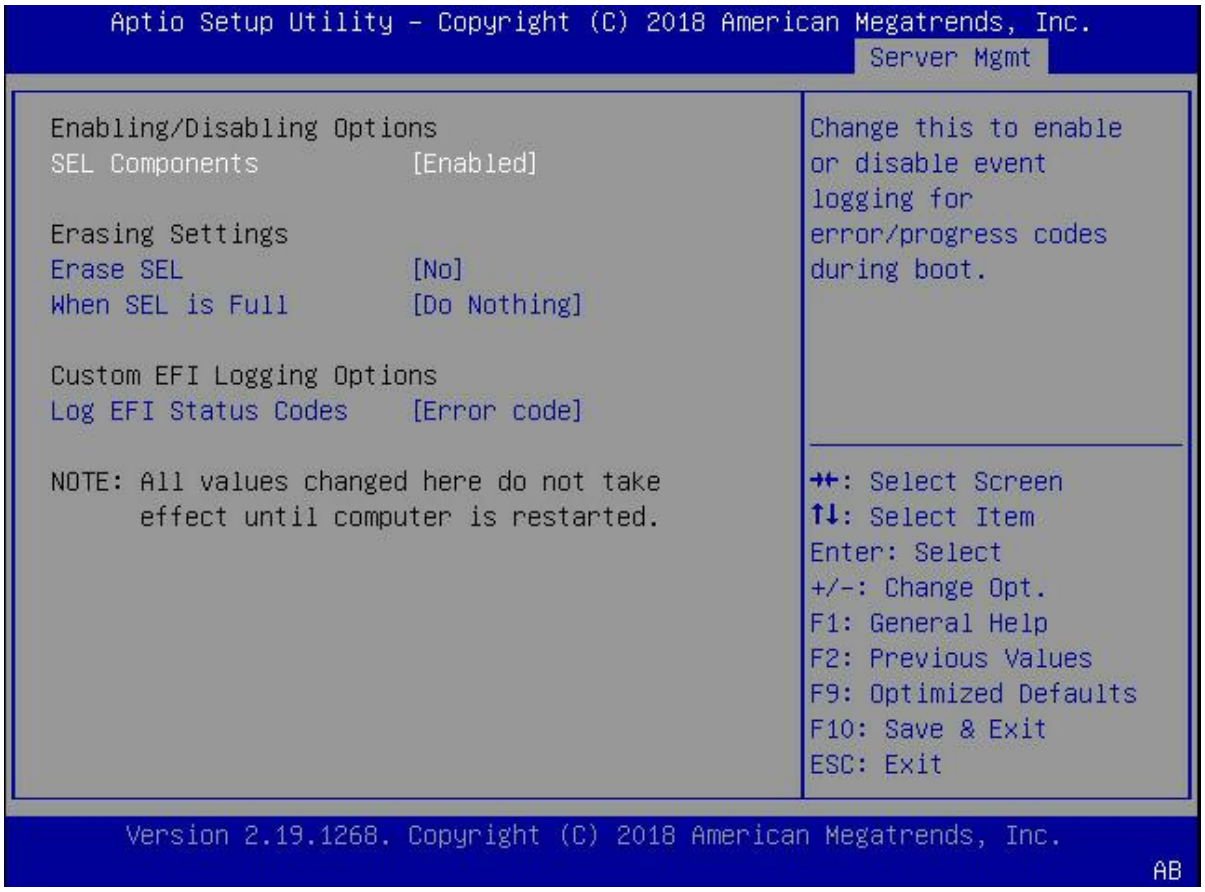
Figure 49: Server MGMT Tab (2 of 2)



- **Bmc self test log**: Press Enter to display the **Bmc self test log** setup screen. See the section titled *BMC Self-Test Log* in this document for more information.
- **View FRU information**: Press Enter to display the **View FRU information** setup screen. See the section titled *View Field Replaceable Unit (FRU) Information* in this document for more information.
- **BMC network configuration**: Press Enter to display the **BMC network configuration** setup screen. See the section titled *View Field Replaceable Unit (FRU) Information* in this document for more information.
- **View FRU information:** View FRU information for the system.
- **BMC User Settings:** Press Enter to display the **BMC User Settings** setup page. See the section titled *BMC User Settings* in this document for more information.
- **BMC Warm Reset:** Press Enter to perform a warm BMC reset.
  Note: The BMC heartbeat LED does not flash quickly during a warm BMC reset.

9.1 System Event Logs

Figure 50: SEL Screen

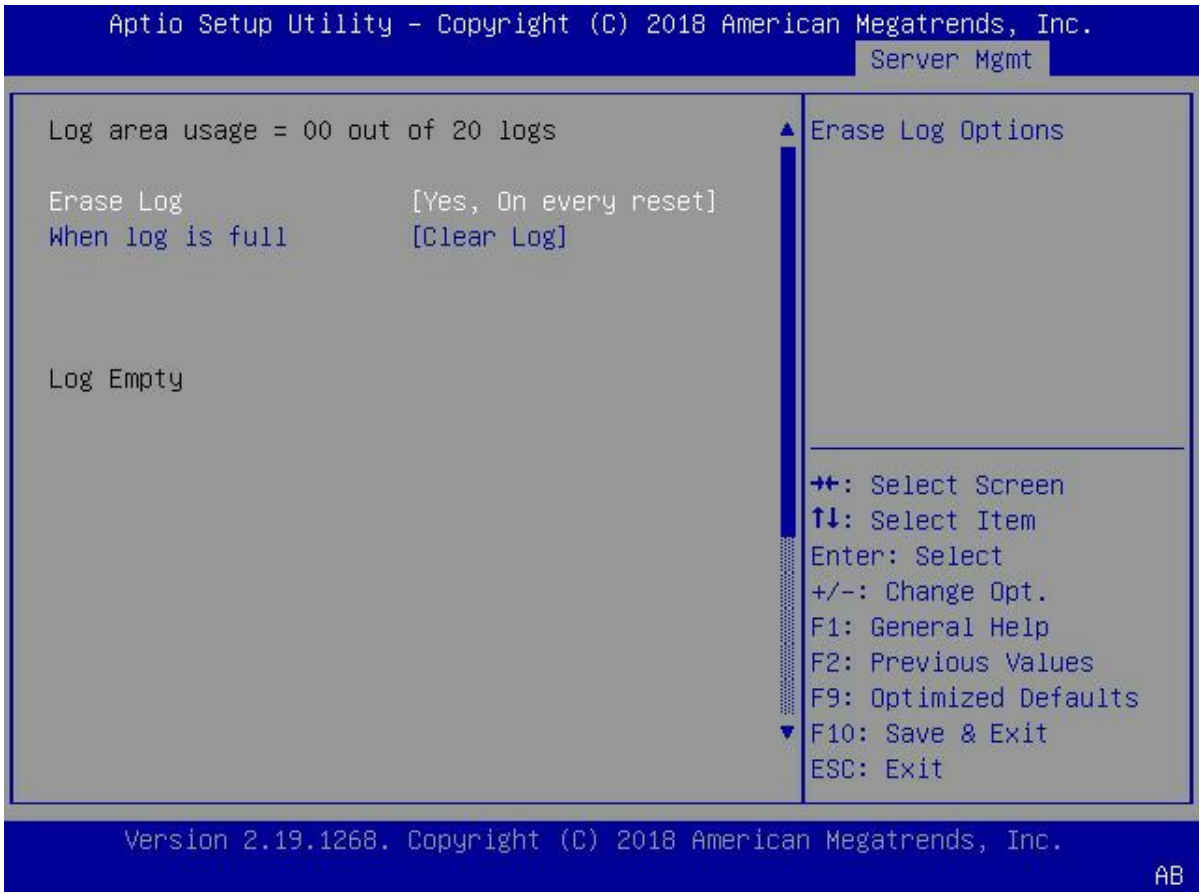


- **SEL Components:** Change this to enable or disable event logging for error/progress codes during boot.
- **Erase SEL:** Select Yes on the next reset to erase system event logs at the next system reboot. Select **No** to keep system event logs after each system reboot.
- **When SEL is Full:** This feature enables users to decide what UEFI must do when the system event log is full. Select Erase Immediately to erase all events in the log when the system event log is full. The options are **Do Nothing** and Erase Immediately.
- **Log EFI Status Codes:** Disable EFI Status Codes logging, or log only error codes, only progress codes, or both. The default is **Error Code** only.
  Note: Changed values for these options do not take effect until the system reboots.

9.2 BMC Self-Test Log

This displays the BMC self-test log during boot progress.

Figure 51: Log Settings Screen

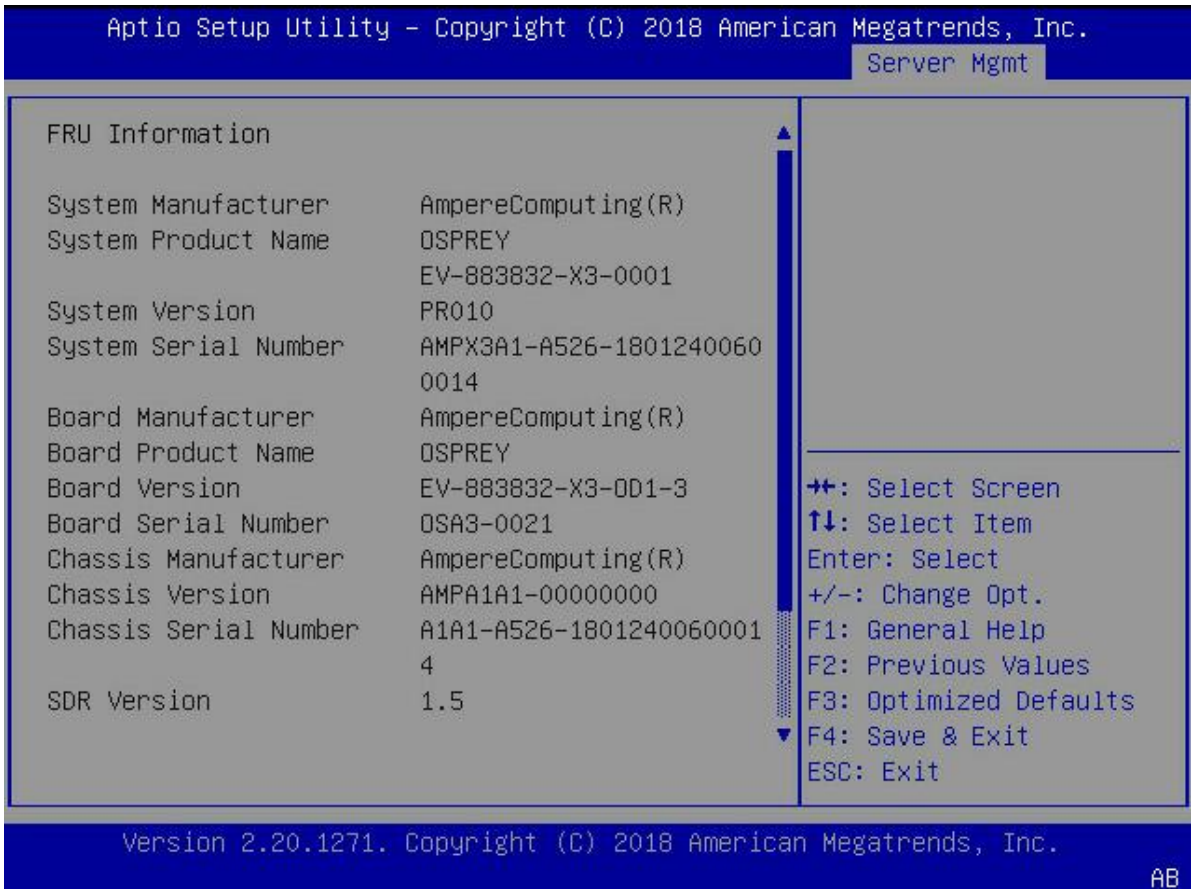


- **Erase Log:** The option to erase log on every reset or keep it. The default is **Yes, On every reset**.
- **When log is full:** Select the action to take when the log is full. The options are **Clear log** and Do not log any more.

9.3 View Field Replaceable Unit (FRU) Information

This feature allows to view the FRU information of system.

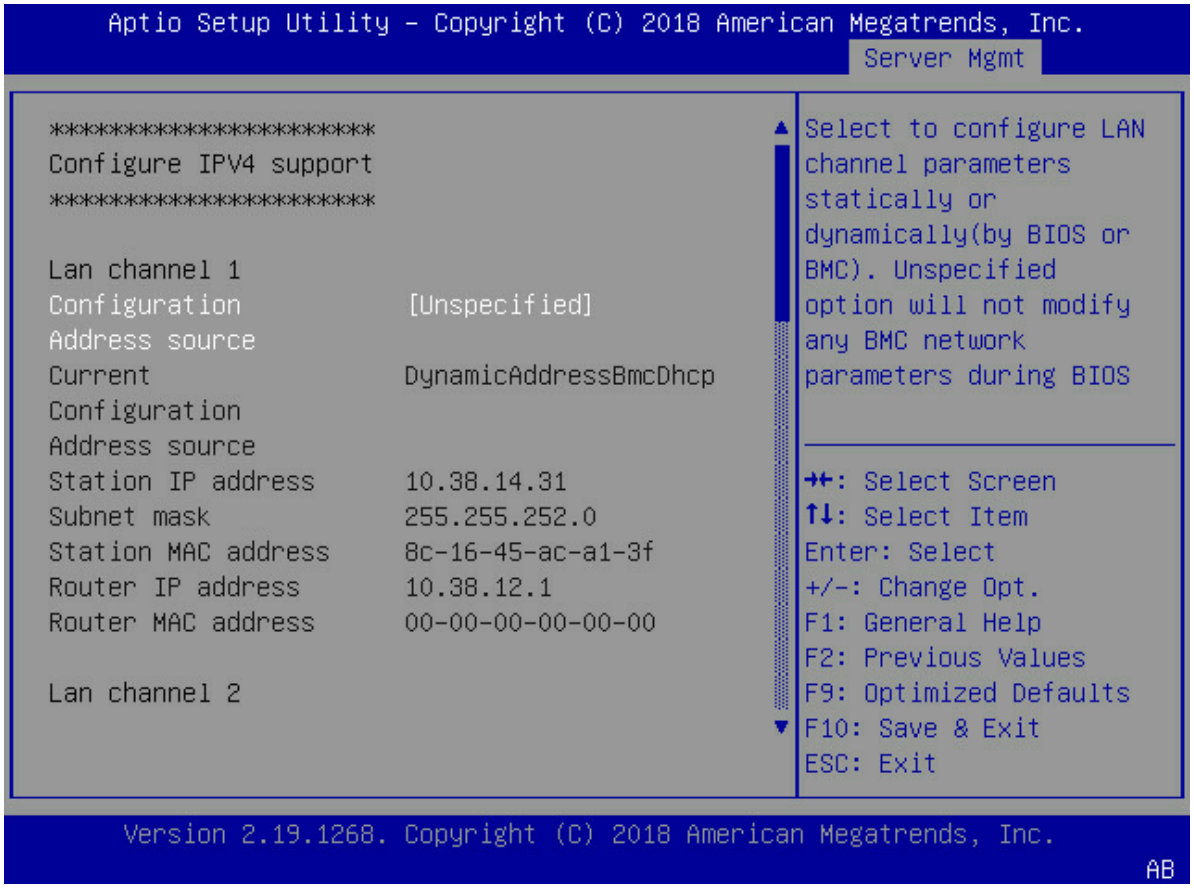
Figure 52: FRU Information Screen



9.4 BMC Network Configuration

9.4.1 Configuring IPv4 Support

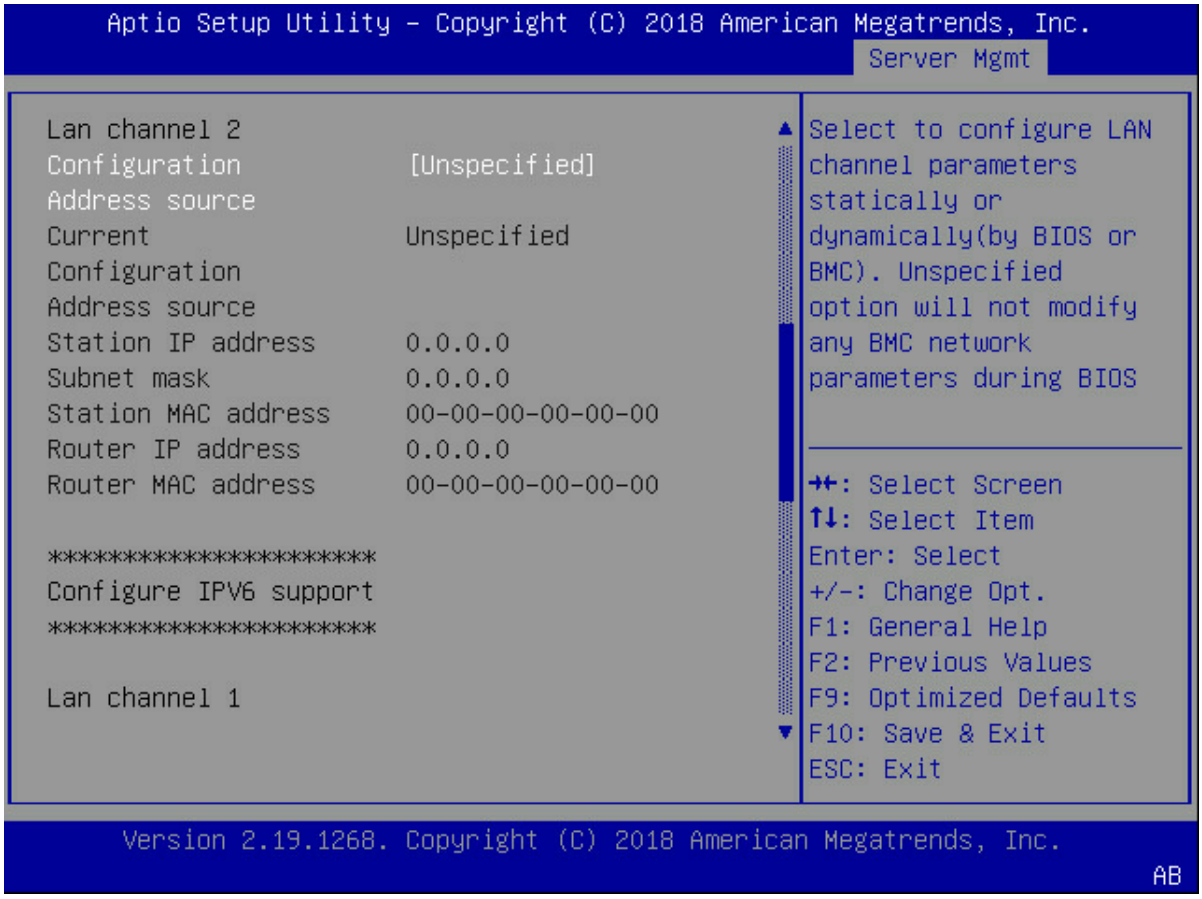
Figure 53: Configure IPv4 Support Screen



- Configuration Address source: This feature enables users to select the source of the IP address for BMC network. If Static is selected, the IP address of the BMC must be manually entered into the system.
  - If DynamicBmcDhcp is selected, the BMC IP address is requested using DHCP from the BMC side.
  - If DynamicBmcNonDhcp is selected, the BMP IP address is requested using the BMC address protocol.
  - The Unspecified option does not modify the BMC network during UEFI booting.

9.4.2 Configuring IPv6 Support

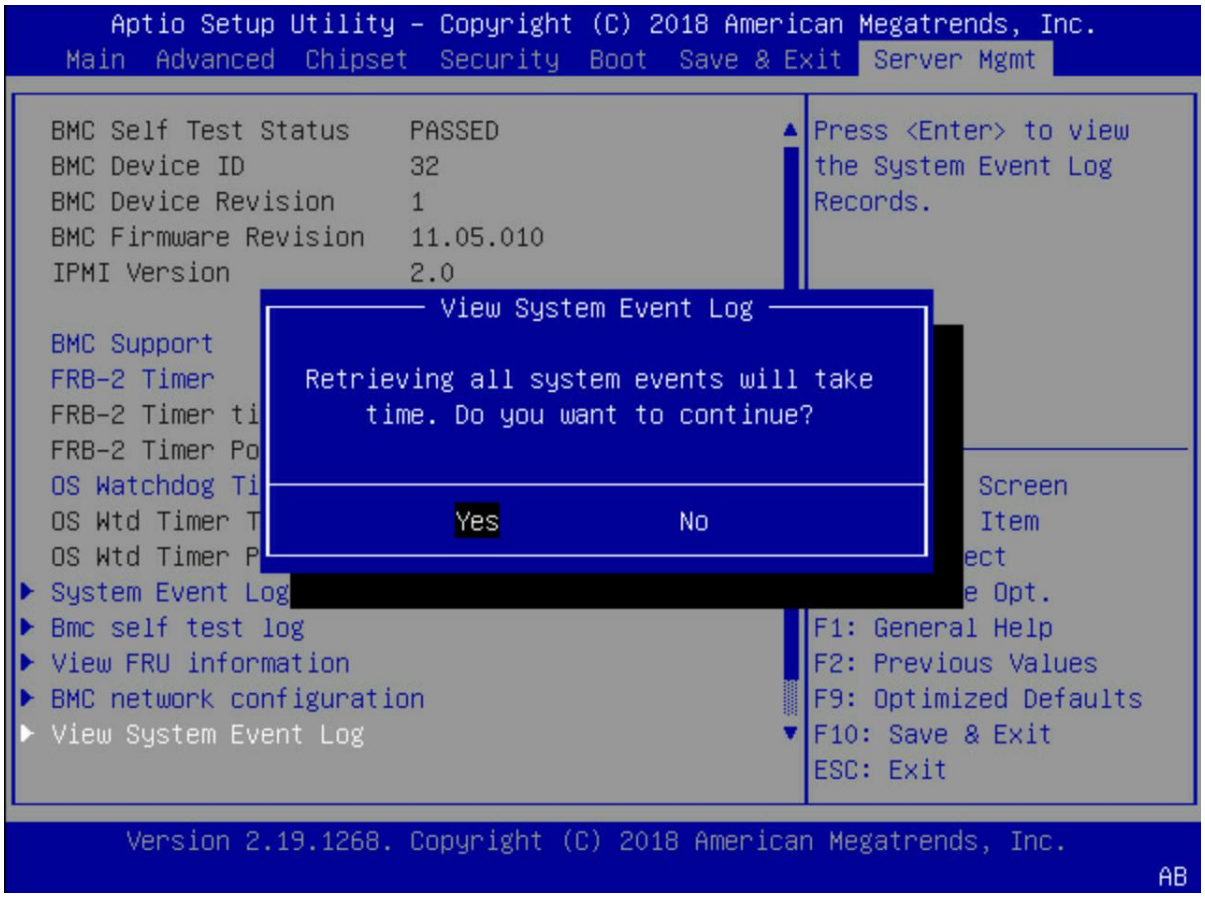
Figure 54: Configure IPv6 Support Screen



- **Configuration Address source:** This feature enables users to select the source of the IP address for BMC network. If Static is selected, the IP address of the BMC must be manually entered into the system.
  - If DynamicBmcDhcp is selected, the BMC IP address is requested using DHCP from the BMC side.
  - If DynamicBmcNonDhcp is selected, the BMP IP address is requested using the BMC address protocol.
  - The Unspecified option does not modify the BMC network during UEFI booting.

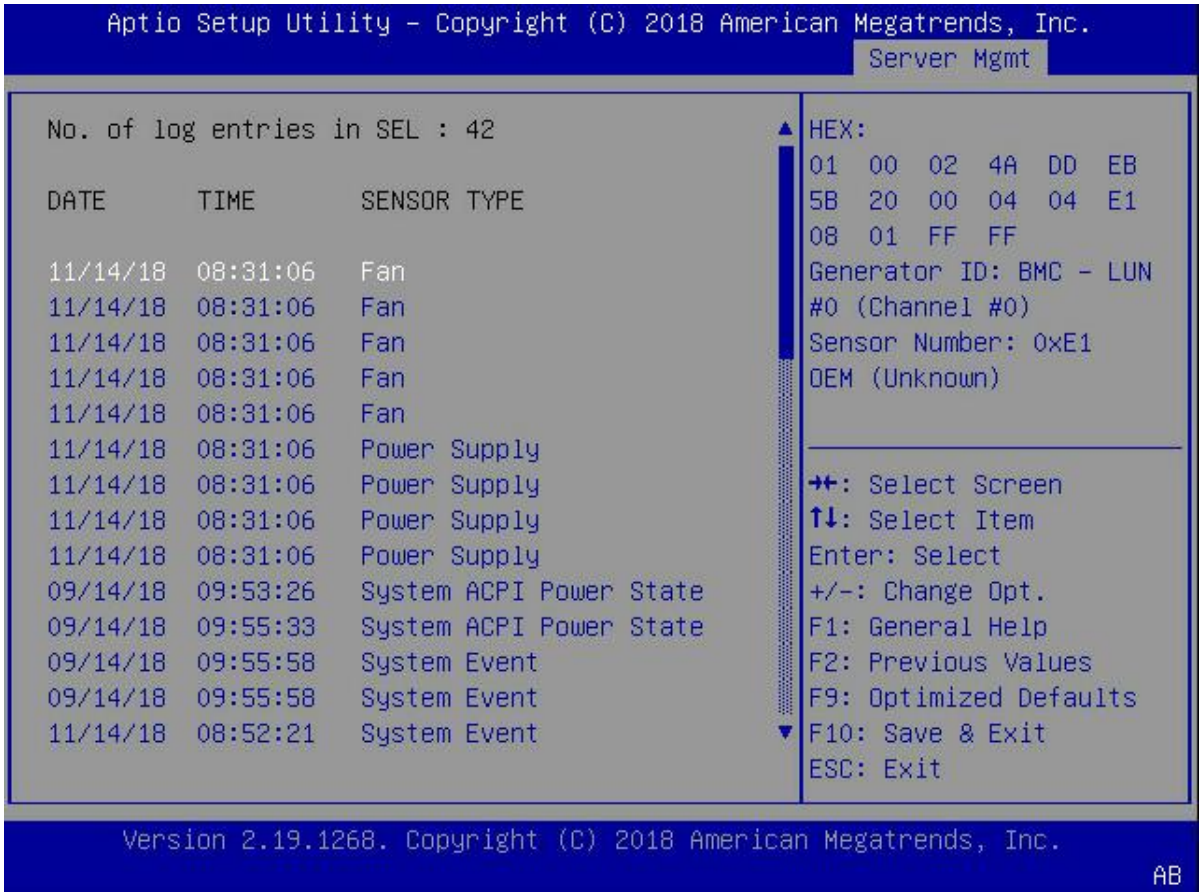
9.5 View System Event Log

Figure 55: View System Event Log Screen



This feature supports viewing all System Event Logs. Retrieving these logs may take time.

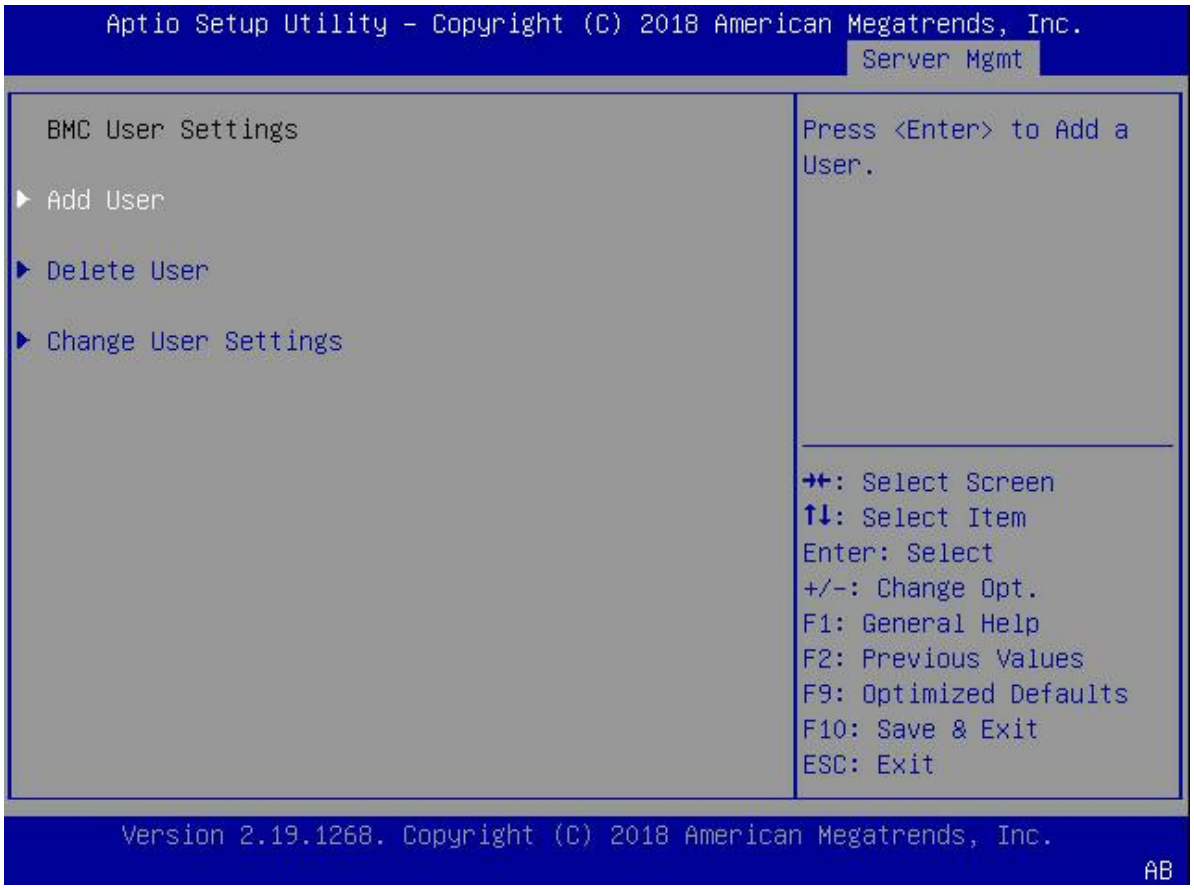
Figure 56: Sample Log View Screen



9.6 BMC User Settings

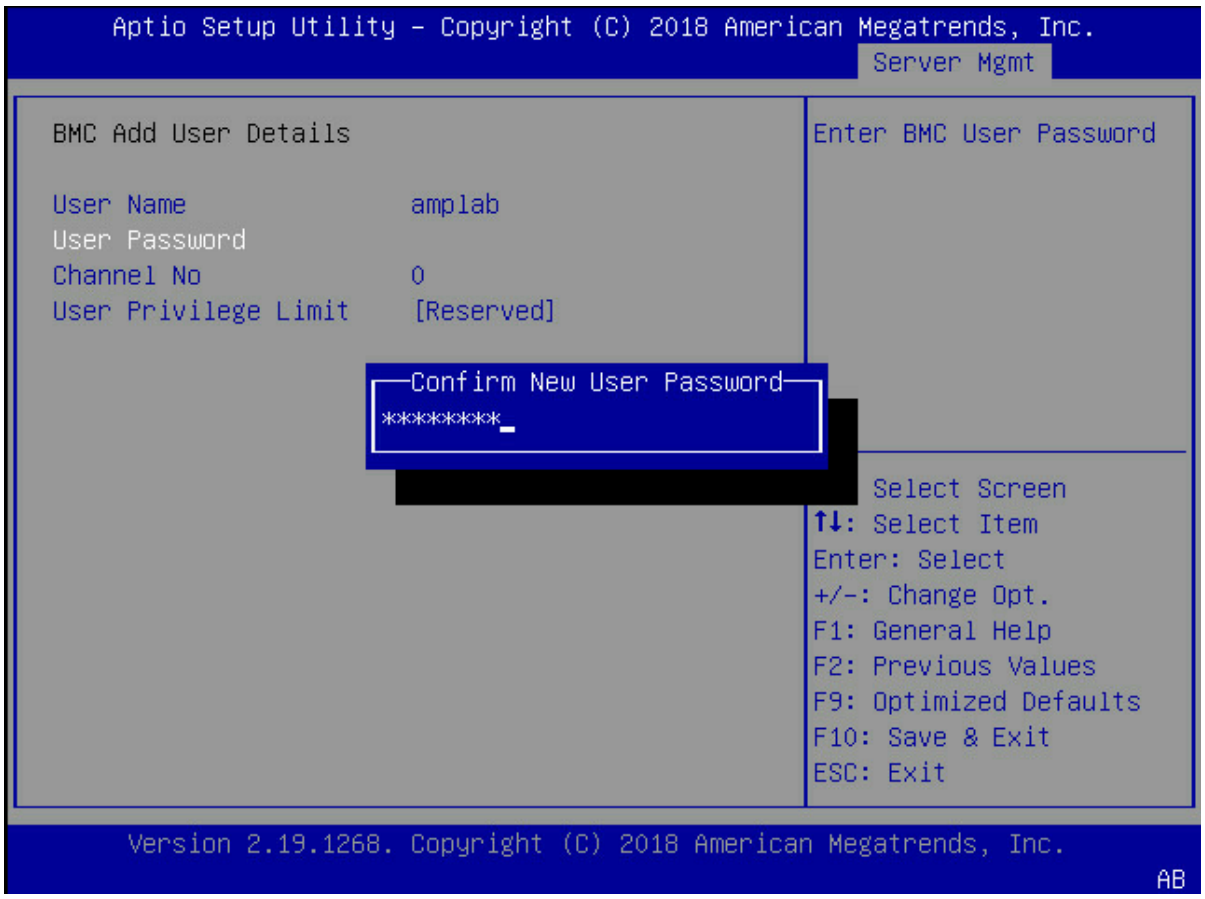
This screen supports adding and deleting BMC users and changing BMC user settings.

Figure 57: BMC View User Settings Screen



9.6.1 BMC Add User Details

Figure 58: BMC Add User Details Screen

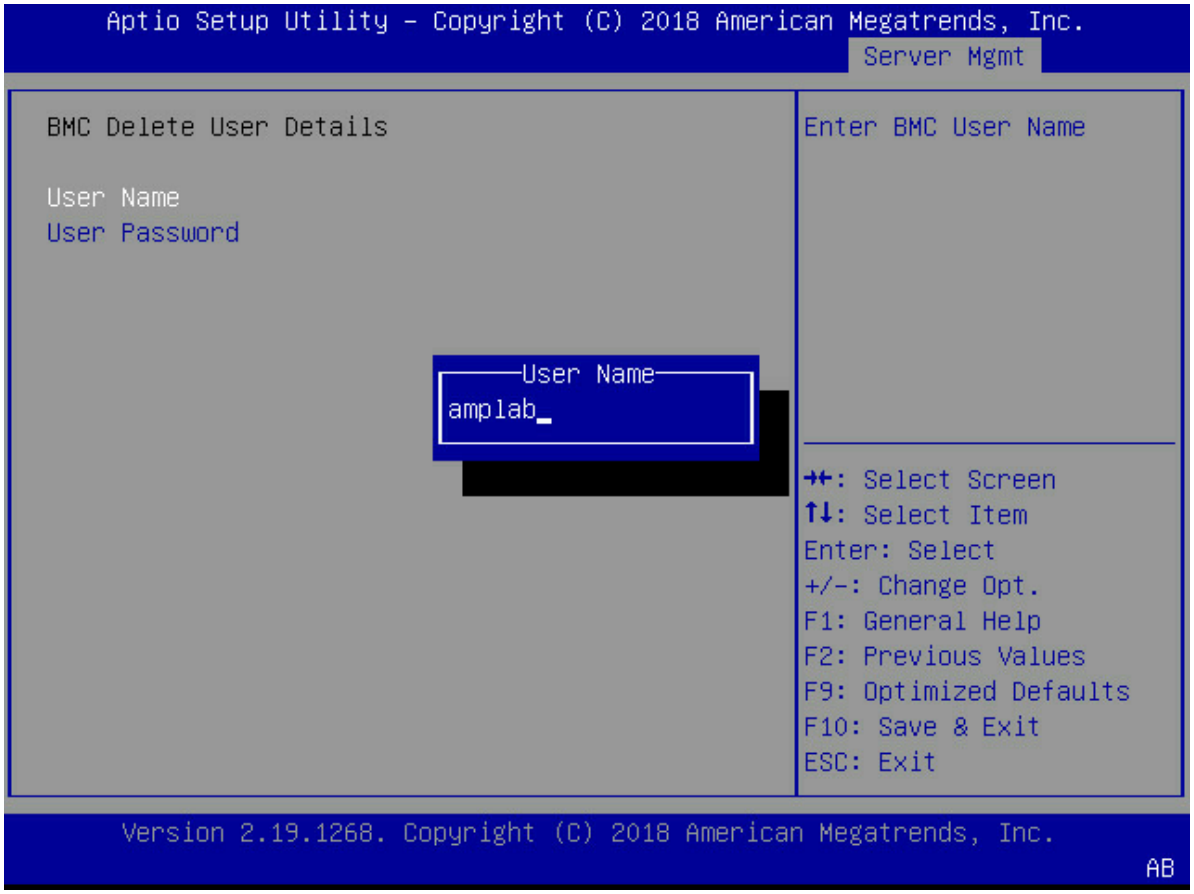


To add a user to the BMC user list, enter this information:

- **User Name:** Enter the username to create.
- **User Password:** Enter and confirm the user password.
- **Channel No**: Enter the LAN channel that the user can have access to if the BMC on this system has more than one LAN port. Otherwise, enter 0.
- **User Privilege Limit**: Choose the Privilege of this user for the selected channel. The options are Reserved, Callback, User, Operator, Administrator, OEM Proprietary, and No Access.
  Note: This option is not available for Channel No 0.

9.6.2 BMC Delete User Details

Figure 59: BMC Delete User Details Screen

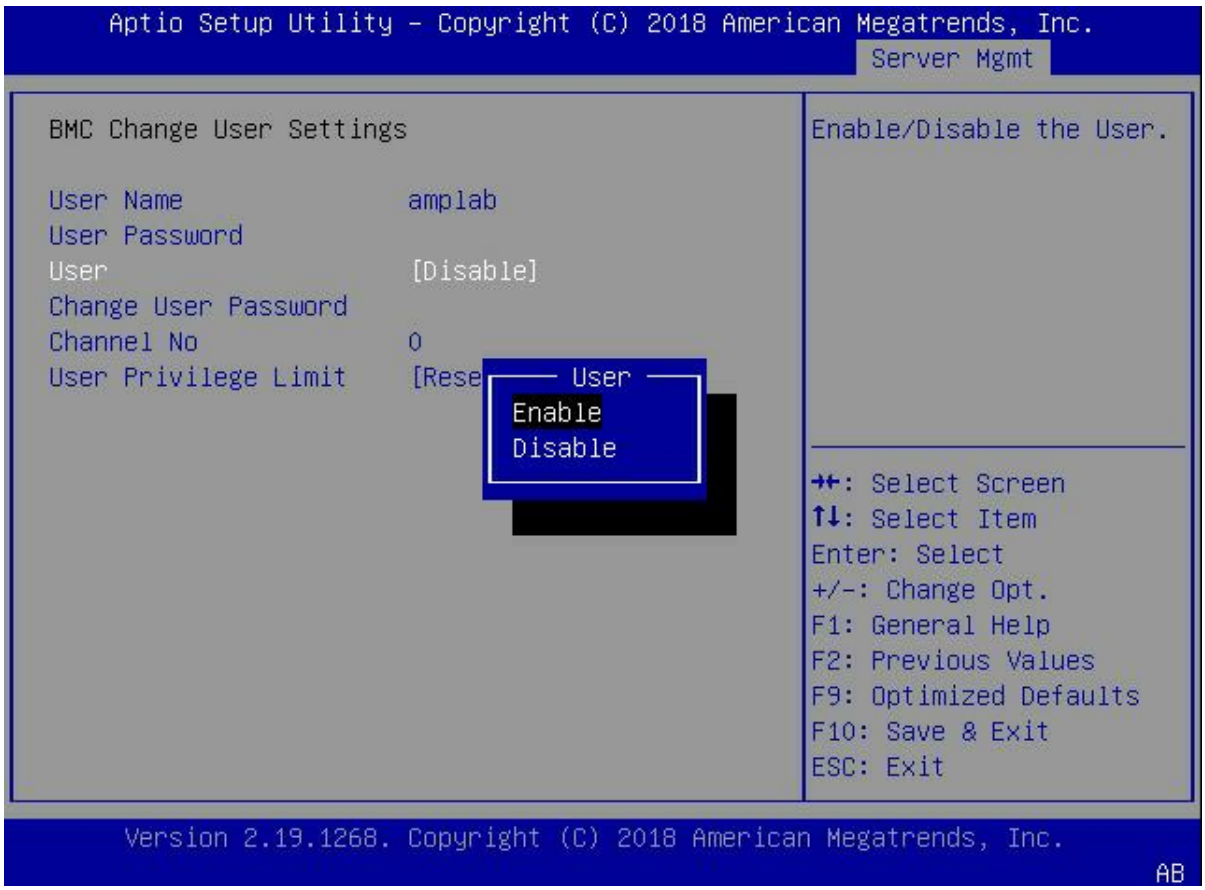


To delete a user from the BMC user list, enter this information. If the information matches, the user is deleted.

- User Name: Enter the username.
- User Password: Enter the user password.

9.6.3 BMC Change User Settings

Figure 60: Change User Settings Screen

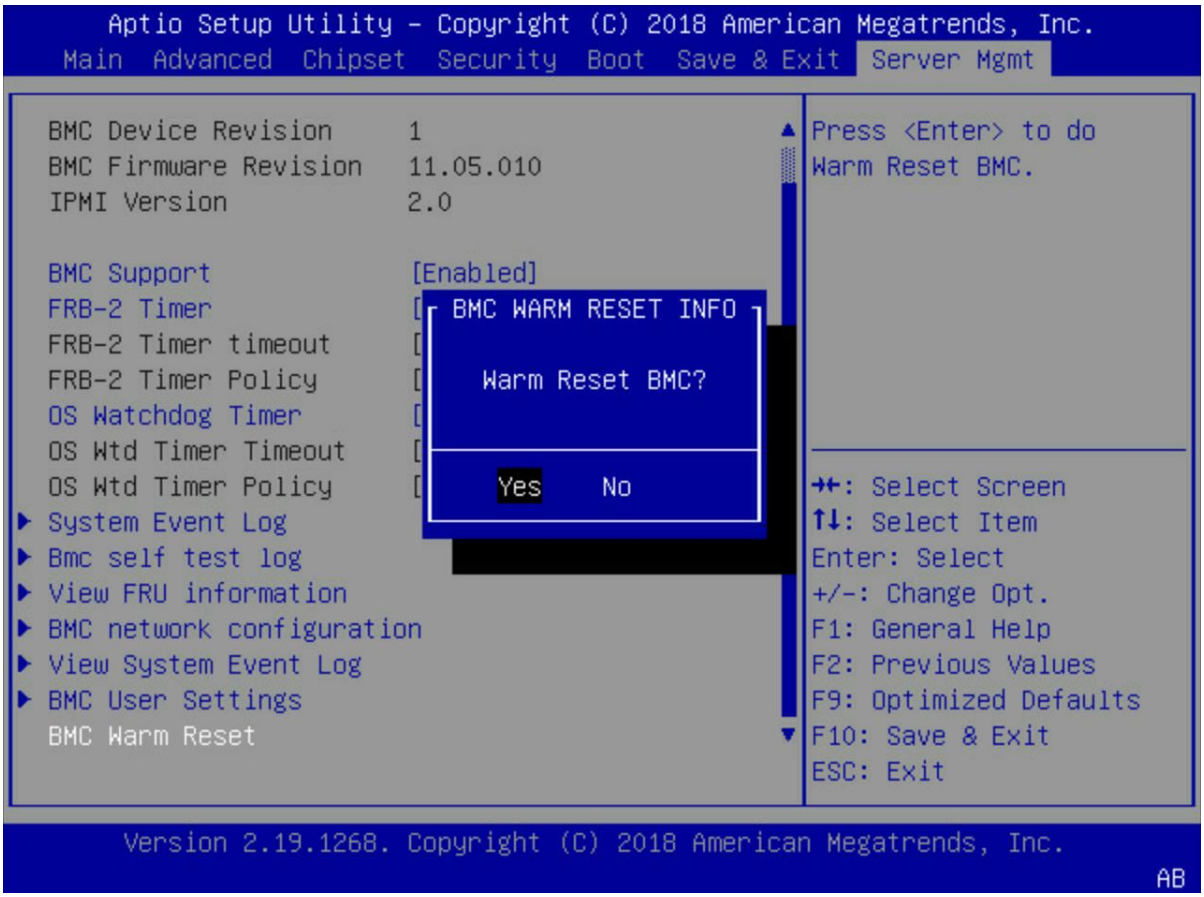


To change a user setting, you must enter the username and user password before changing other settings. The user settings are:

- User Name: Enter the username.
- User Password: Enter the user password.
- User: Enable or Disable access for the user. If Disable is selected, the user does not have BMC access.
- Change User Password: Enter the new user password.
- Channel No: Enter the channel number to change.
- User Privilege Limit: Choose the user privilege for the selected channel. The options are: Reserved, Callback, User, Operator, Administrator, OEM Proprietary, and No Access.
  Note: This option is available for Channel No 0.

9.7 BMC Warm Reset

Figure 61: BMC Warm Reset Screen



Press Enter to perform a warm reset of the BMC. When using **BMC Warm Reset**, a dialog appears to confirm the BMC warm reset request. Select **Yes** to trigger the BMC to reset.

Note: The BMC heartbeat LED does not flash quickly during a BMC warm reset.

10. Programming In-Band Firmware

The Altra UEFI supports two ways to program in-band firmware.

10.1 Programming Firmware Using the UEFI Shell

A new firmware binaries package must contain *.cap files and a CapsuleApp.efi file. The *.cap files contain firmware binaries. CapsuleApp.efi contains an EFI application to program the *.cap files.

Copy the *.cap files and CapsuleApp.efi to a USB or boot partition of the OS (typically mounted under /boot/efi).

When booting to the UEFI shell, follow these steps to upgrade the firmware. Perform the same steps for each *.cap file:

```
Shell>CapsuleApp.efiBIOS.cap
Shell> reset
```

10.2 Programming Firmware Using Linux

A Linux OS that supports capsule updates provides a tool called fwupdate to upgrade the BIOS. If the Linux distribution does not support capsule upgrades, UEFI shell upgrades can be used instead.

Note: If fwupdate does not clear older update firmware variables created during the previous update capsule operation, use this command from the shell to clear them.

```
Shell>dmpstore -d -guid 0ABBA7DC-E516-4167-BBF5-4D9D1C739416
Delete variable '0ABBA7DC-E516-4167-BBF5-4D9D1C739416:fwupdate-c9f52c58-bb02-4bb5-86d2-
eb9af752c2d5-0': Success
```

1. Check whether capsule update is supported:
   ```
   # fwupdate –s
   ```
2. Use the fwupdate utility to see the list of supported firmware updates. This command lists the supported capsule GUIDs:
   ```
   # fwupdate –l
   {6169f638-85ed-11e6-ae22-56b6b6499611} version 0 can be updated to any version above -1
   ```
3. Use the fwupdate utility to apply the ATF/BIOS update capsule:
   BIOS only:
   ```
   # fwupdate -a 6169f638-85ed-11e6-ae22-56b6b6499611 <BIOS cap>
   # reboot
   ```
4. After the update completes, reboot the system. After the reboot, the firmware updates automatically.

Appendix A: UEFI Process Checkpoint Code Mapping Table

This appendix describes UEFI boot process checkpoint code mapping. The listed boot process checkpoint code helps to determine which point the UEFI boot process reaches during the Pre-EFI Initialization (PEI) and Driver eXecution Environment (DXE) phases.

Here is an example of checkpoint code displayed during BIOS booting:

```
DRAM Initialization: [100%] [ ==================== ]
Checkpoint 2F
Checkpoint 2E
Checkpoint 31
Checkpoint 32
```

Table 24 lists all checkpoint codes; an implementation may support all of them.

Table 24: BIOS Checkpoint Code

GROUP	CODE	DESCRIPTION
SEC execution	1 – 0xF	SEC execution
PEI CAR execution	0x10	PEI_CORE_STARTED
	0x11	PEI_CAR_CPU_INIT
	0x12 – 0x14	Reserved for CPU
	0x15	PEI_CAR_NB_INIT
	0x16 – 0x18	Reserved for NB
	0x19	PEI_CAR_SB_INIT
	0x1A – 0x1C	Reserved for SB
	0x1D – 0x2A	Reserved for OEM use
	0x2B	PEI_MEMORY_SPD_READ
	0x2C	PEI_MEMORY_PRESENCE_DETECT
	0x2D	PEI_MEMORY_TIMING
	0x2E	PEI_MEMORY_CONFIGURING
	0x2F	PEI_MEMORY_INIT

GROUP	CODE	DESCRIPTION
PEI execution after memory detection	0x30	Reserved for AMI use
	0x31	PEI_MEMORY_INSTALLED
	0x32	PEI_CPU_INIT
	0x33	PEI_CPU_CACHE_INIT
	0x34	PEI_CPU_AP_INIT
	0x35	PEI_CPU_BSP_SELECT
	0x36	PEI_CPU_SMM_INIT
	0x37	PEI_MEM_NB_INIT
	0x38 – 0x3A	Reserved for NB
	0x3B	PEI_MEM_SB_INIT
	0x3C – 0x3E	Reserved for SB
	0x3F – 0x4E	Reserved for OEM use
	0x4F	PEI_DXE_IPL_STARTED
PEI errors	0x50	PEI_MEMORY_INVALID_TYPE, SPEED
	0x51	PEI_MEMORY_SPD_FAIL
	0x52	PEI_MEMORY_INVALID_SIZE, MISMATCH
	0x53	PEI_MEMORY_NOT_DETECTED, NONE_USEFUL
	0x54	PEI_MEMORY_ERROR
	0x55	PEI_MEMORY_NOT_INSTALLED
	0x56	PEI_CPU_INVALID_TYPE, SPEED
	0x57	PEI_CPU_MISMATCH
	0x58	PEI_CPU_SELF_TEST_FAILED, CACHE_ERROR
	0x59	PEI_CPU_MICROCODE_UPDATE_FAILED
	0x5A	PEI_CPU_INTERNAL_ERROR
	0x5B	PEI_RESET_NOT_AVAILABLE
	0x5C – 0x5F	Reserved for AMI use

GROUP	CODE	DESCRIPTION
DXE execution	0x60	DXE_CORE_STARTED
	0x61	DXE_NVRAM_INIT
	0x62	DXE_SBRUN_INIT
	0x63	DXE_CPU_INIT
	0x64 – 0x67	Reserved for CPU
	0x60	DXE_CORE_STARTED
	0x61	DXE_NVRAM_INIT
	0x62	DXE_SBRUN_INIT
	0x63	DXE_CPU_INIT
	0x64 – 0x67	Reserved for CPU
	0x68	DXE_NB_HB_INIT
	0x69	DXE_NB_INIT
	0x6A	DXE_NB_SMM_INIT
	0x6B – 0x6F	Reserved for NB
	0x70	DXE_SB_INIT
	0x71	DXE_SB_SMM_INIT
	0x72	DXE_SB_DEVICES_INIT
	0x73 – 0x77	Reserved for SB
	0x78	DXE_ACPI_INIT
	0x79	DXE_CSM_INIT
	0x7A – 0x7F	Reserved for AMI use
	0x80 – 0x8F	Reserved for OEM use
	0x90	DXE_BDS_STARTED
	0x91	DXE_BDS_CONNECT_DRIVERS
	0x92	DXE_PCI_BUS_BEGIN
	0x93	DXE_PCI_BUS_HPC_INIT
	0x94	DXE_PCI_BUS_ENUM
	0x95	DXE_PCI_BUS_REQUEST_RESOURCES
	0x96	DXE_PCI_BUS_ASSIGN_RESOURCES
	0x97	DXE_CON_OUT_CONNECT
	0x98	DXE_CON_IN_CONNECT

GROUP	CODE	DESCRIPTION
	0x99	DXE_SIO_INIT
	0x9A	DXE_USB_BEGIN
	0x9B	DXE_USB_RESET
	0x9C	DXE_USB_DETECT
	0x9D	DXE_USB_ENABLE
	0x9E – 0x9F	Reserved for AMI use
	0xA0	DXE_IDE_BEGIN
	0xA1	DXE_IDE_RESET
	0xA2	DXE_IDE_DETECT
	0xA3	DXE_IDE_ENABLE
	0xA4	DXE_SCSI_BEGIN
	0xA5	DXE_SCSI_RESET
	0xA6	DXE_SCSI_DETECT
	0xA7	DXE_SCSI_ENABLE
	0xA8	DXE_SETUP_VERIFYING_PASSWORD
	0xA9	DXE_SETUP_START
	0xAA	Reserved for AMI use
	0xAB	DXE_SETUP_INPUT_WAIT
	0xAC	Reserved for AMI use
	0xAD	DXE_READY_TO_BOOT
	0xAE	DXE_LEGACY_BOOT
	0xAF	DXE_EXIT_BOOT_SERVICES
	0xB0	RT_SET_VIRTUAL_ADDRESS_MAP_BEGIN
	0xB1	RT_SET_VIRTUAL_ADDRESS_MAP_END
	0xB2	DXE_LEGACY_OPROM_INIT
	0xB3	DXE_RESET_SYSTEM
	0xB4	DXE_USB_HOTPLUG
	0xB5	DXE_PCI_BUS_HOTPLUG
	0xB6	DXE_NVRAM_CLEANUP
	0xB7	DXE_CONFIGURATION_RESET
	0xB8 – 0xBF	Reserved for AMI use

GROUP	CODE	DESCRIPTION
	0xC0 – 0xCF	Reserved for OEM use
DXE errors	0xD0	DXE_CPU_ERROR
	0xD1	DXE_NB_ERROR
	0xD2	DXE_SB_ERROR
	0xD3	DXE_ARCH_PROTOCOL_NOT_AVAILABLE
	0xD4	DXE_PCI_BUS_OUT_OF_RESOURCES
	0xD5	DXE_LEGACY_OPROM_NO_SPACE
	0xD6	DXE_NO_CON_OUT
	0xD7	DXE_NO_CON_IN
	0xD8	DXE_INVALID_PASSWORD
	0xD9	DXE_BOOT_OPTION_LOAD_ERROR
	0xDA	DXE_BOOT_OPTION_FAILED
	0xDB	DXE_FLASH_UPDATE_FAILED
	0xDC	DXE_RESET_NOT_AVAILABLE
	0xDE – 0xDF	Reserved for AMI use
S3 Resume	0xE0	PEI_S3_STARTED
	0xE1	PEI_S3_BOOT_SCRIPT
	0xE2	PEI_S3_VIDEO_REPOST
	0xE3	PEI_S3_OS_WAKE PEI_SOFTWARE_PEI_MODULE PEI_SW_PEI_PC_OS_WAKE
	0xE4 – 0xE7	Reserved for AMI use
	0xE8	PEI_MEMORY_S3_RESUME_FAILED

GROUP	CODE	DESCRIPTION
S3 Resume errors	0xE9	PEI_S3_RESUME_PPI_NOT_FOUND
	0xEA	PEI_S3_BOOT_SCRIPT_ERROR
	0xEB	PEI_S3_OS_WAKE_ERROR
	0xEC – 0xEF	Reserved for AMI use
Recovery	0xF0	PEI_RECOVERY_AUTO
	0xF1	PEI_RECOVERY_USER
	0xF2	PEI_RECOVERY_STARTED
	0xF3	PEI_RECOVERY_CAPSULE_FOUND
	0xF4	PEI_RECOVERY_CAPSULE_LOADED
	0xF5 – 0xF7	Reserved for AMI use
	0xF8	PEI_RECOVERY_PPI_NOT_FOUND
Recovery errors	0xF9	PEI_RECOVERY_NO_CAPSULE
	0xFA	PEI_RECOVERY_INVALID_CAPSULE
	0xFB – 0xFF	Reserved for AMI use

Appendix B: Pre-Boot Settings

UEFI settings are configured either using menus, or from the UEFI shell using set variable commands. Low-level firmware uses some variables before UEFI execution. Additionally, UEFI menus or set variable commands do not control all. The xtool command is used to set variables and pre-boot settings that are not controlled using normal UEFI methods.

Table 25 and *Table 26* describe these pre-boot variables.

The xtool syntax is as follows:

```
>xtool<Address><value>
```

where <Address> is listed in *Table 25* and *Table 26*.

Table 25: Manufacturing Pre-Boot Settings

#	NAME	ADDR (ID)	DEFAULT VALUE	DESCRIPTION
0	NV_SI_DDR_VMARGIN	0x4000	0	Manufacturing adjustment for DDR voltage (limited to ±120 mV).
1	NV_SI_SOC_VMARGIN	0x4008	0	Manufacturing adjustment for SoC voltage (limited to ±120 mV).
2	NV_SI_AVS_VMARGIN	0x4010	0	Manufacturing adjustment for AVS voltage (limited to ±120 mV).
3	NV_SI_TPC_TM1_MARGIN	0x4018	0	Manufacturing adjustment for TPC TM1 temperature (limited to ±25 mV).
4	NV_SI_TPC_TM2_MARGIN	0x4020	0	Manufacturing adjustment for TPC TM2 temperature (limited to ±10 mV).
5	NV_SI_TPC_FREQ_THROTTLE	0x4028	0	Manufacturing disable of TPC frequency throttle (set to 1 to disable throttle).
6	NV_SI_T_LTLM_EN	0x4030	0	Manufacturing disable of TLIMIT (set to 0 to disable).
7	NV_SI_T_LTLM_THRSHLD	0x4038	0	Manufacturing local temperature limit threshold for TLIMIT. The default temperature limit for TLIMIT is 95°C. The core frequency divider is throttled based on this limit.
8	NV_SI_T_GTLM_THRSHLD	0x4040	0	Manufacturing global temperature limit threshold for TLIMIT. The default temperature limit for TLIMIT is 95°C. The core PLL is throttled based on the limit.
9	NV_SI_P_LM_EN	0x4048	1	Manufacturing disable of PLIMIT feature (Set to 0 to disable)
10	NV_SI_P_LM_THRSHLD	0x4050	Chip TDP	Manufacturing power limit threshold for PLIMIT. The default power limit is the chip TDP.
11	NV_SI_TPC_OVERTEMP_ISR_DISABLE	0x4058	0	Manufacturing disable of hardware over temperature interrupt.
12	NV_SI_VPP_VMARGIN	0x4060	0	Manufacturing adjustment for RCA voltage (limited to ±120 mV).
13	NV_SI_PMPRO_FAILSAFE	0x4068	0	Manufacturing simulate PMpro boot failure.
14	NV_SI_FAILSAFE_DISABLE	0x4070	0	Manufacturing disable of failsafe feature.

#	NAME	ADDR (ID)	DEFAULT VALUE	DESCRIPTION
15	NV_SI_PLIMIT_APM_DS_PERCENTAGE	0x4078	25	PM1 duty-cycle percentage step size. At each PM1 evaluation period (EP), the burst/break times are adjusted using NV_SI_PLIMIT_APM_DS_PERCENTAGE
16	NV_SI_PLIMIT_APM_EP_MS	0x4080	100	PM1 Evaluation Period (EP), in ms. EP = Burst time + Break time Burst time: Time during which power cap = TDP * (1 + NV_SI_PLIMIT_APM_PM1_PERCENTAGE_TDP /100) Break time: Time during which power cap = TDP
17	NV_SI_PLIMIT_APM_PM1_PERCENTAGE_TDP	0x4088	8	PM1 Short term power expressed as TDP%. Example: With value 8%, PM1 = TDP * 108%
18	NV_SI_CPU_LPI_FREQ_DISABLE	0x4090	1	Disable LPI frequency scale-down feature. With this feature, when the CPU is in WFI/WFE, PMpro scales the CPU clock ratio to the minimum 16/32.
19	NV_SI_CPU_LPI_FREQ_ENERGY_THRSHLD	0x4098	0	Energy threshold to detect if the CPU is in the WFI/WFE states.
20	NV_SI_CCIX_OPT_CONFIG	0x40A0	0	Manufacturing the CCIX optimization config. [0]: Enable Message Packing [1]: Enable Optimized Header [3:2]: Maximum packet size 00: 128B 01: 256B 10: 512B
21	NV_SI_MESH_FREQ_MARGIN	0x40A8	0	Manufacturing the Mesh frequency margin in range [-250, +250] MHz
22	NV_SI_MESH_TURBO_EN	0x40B0	1	Enable mesh turbo frequency • 2.8 GHz part which allows Mesh to run at 1.75 GHz at a turbo frequency of 3.0 GHz • 3.0 GHz part which allows Mesh to run at 1.85 GHz at a turbo frequency of 3.3 GHz
23	NV_SI_PWR_HEADROOM_WATT	0x40B8	25	Turbo Mesh frequency when the (chip power + NV_SI_PWR_HEADROOM_WATT) < PLIMIT threshold.
24	NV_SI_EXTRA_PCP_VOLT_MV	0x40C0	35	Adding extra PCP voltage when turbo Mesh frequency is running (default is 35 mV).
25	NV_SI_CPU_LPI_HYST_CNT	0x40C8	10	Hysteresis counter which waits when the core is idle for a fixed period (100 µs) before starting to reduce the CPU clock ratio in half.
26	NV_SI_DVFS_VOLT_INC_STEP_MV	0x40D0	30	The maximum DVFS voltage increase step
27	NV_SI_DVFS_VOLT_DEC_STEP_MV	0x40D8	30	The maximum DVFS voltage decrease step

#	NAME	ADDR (ID)	DEFAULT VALUE	DESCRIPTION
28	NV_SI_PLIMIT_APM_TEMP_THLD	0x40E0	TM1 - 3	PM1 Temperature threshold. If the temperature exceeds this threshold, the burst/break times are adjusted using NV_SI_PLIMIT_APM_DS_PERCENTAGE
29	NV_SI_PLIMIT_APM_EN	0x40E8	1	PM1 enable
30	NV_SI_VDM_EN	0x40F0	1	VDM, voltage drop mitigation, enable
31	NV_SI_VDM_VMARGIN_MV	0x40F8	0	VDM voltage margin in mV
32	NV_SI_PLT_EN	0x4100	0	Booting Platform Tool rather than normal ATF BL1
33	NV_SI_PLT_SOCKET	0x4108	0	Target Socket mask
34	NV_SI_PLT_MCU_MASK	0x4110	0xFF	Target MCU mask
35	NV_SI_PLT_RANK_MASK	0x4118	0xFF	Target Rank mask on MCU
36	NV_SI_PLT_RSVD	0x4120	–	–
37	NV_SI_PLT_RSVD	0x4128	–	–
38	NV_SI_PLT_X_PARAM	0x4130	1	X Axis Parameters: 0: Invalid 1: RDRISE 2: RDFALL 3: WRDQ 4: WRLVL 5: RDGATE 6: ADCMD
39	NV_SI_PLT_Y_PARAM	0x4138	1	Y axis parameters: 0: Invalid 1: PHY_VREF 2: DIMM_VREF
40	NV_SI_PLT_X_LEFT	0x4140	-80	Left margin leveling value
41	NV_SI_PLT_X_RIGHT	0x4148	80	Right margin leveling value
42	NV_SI_PLT_X_STEP	0x4150	4	Leveling step
43	NV_SI_PLT_Y_BOTTOM	0x4158	-0x20	Bottom margin Vref value
44	NV_SI_PLT_Y_TOP	0x4160	0x20	Top margin Vref value
45	NV_SI_PLT_Y_STEP	0x4168	4	Vref step
46	NV_SI_PLT_RSVD	0x4170	–	–
47	NV_SI_PLT_RSVD	0x4178	–	–
48	NV_SI_PLT_SIZE	0x4180	–	Memory test size (limit to 32-bit size)
49	NV_SI_PLT_RSVD	0x4188	–	–
50	NV_SI_PLT_SCREEN	0x4190	0	Enable Memory Screen Mode
51	NV_SI_PLT_RSVD	0x4198	–	–
52	NV_SI_DVFS_VOLT_CHANGE_BY_STEP_EN	0x41A0	1	DVFS PCPC voltage step size in mV.

#	NAME	ADDR (ID)	DEFAULT VALUE	DESCRIPTION
53	NS_SI_DVFS_TCAL_F_LIMIT	0x41A8	3000	DVFS CPUPLL frequency calibration limit in MHz.
54	NS_SI_DVFS_TCAL_T_LIMIT	0x41B0	95	DVFS temperature calibration limit in °C. When the frequency and temperature exceed the calibration limit threshold, the CPUPLL is reduced by 50 MHz.
55	NV_SI_CCIX_DIAG_CTRL1	0x41B8	0	Reserved.
56	NV_SI_CCIX_DIAG_CTRL2	0x41C0	0	Reserved.
57	NV_SI_DDR_TCAL_EN	0x41C8	1	DDR temperature calibration, "DDR Cal", enable Value: 0: Disable 1: Enable
58	NV_SI_DDR_TCAL_DIMM_LOW_TEMP_THRESHOLD	0x41D0	25	"DDR Cal" DIMM low temperature threshold in °C.
59	NV_SI_DDR_TCAL_DIMM_HIGH_TEMP_THRESHOLD	0x41D8	40	"DDR Cal" DIMM high temperature threshold in °C.
60	NV_SI_DDR_TCAL_MCU_LOW_TEMP_THRESHOLD	0x41E0	25	"DDR Cal" MCU low temperature threshold in °C.
61	NV_SI_DDR_TCAL_MCU_HIGH_TEMP_THRESHOLD	0x41F8	40	"DDR Cal" MCU high temperature threshold in °C.
62	NV_SI_DDR_TCAL_LOW_TEMP_VOLT_OFF_MV	0x4200	50	"DDR Cal" low temperature VRD SOC voltage positive offset in mV.
63	NV_SI_DDR_TCAL_PERIOD_SEC	0x4208	10	"DDR Cal" checking period in seconds.
64	NV_SI_DDR_TCAL_SOC_VOLT_CAP_MV	0x4210	780	"DDR Cal" maximum VRD SOC voltage in mV.

Table 26: User Pre-Boot Settings

#	NAME	ADDR (ID)	DEFAULT VALUE	DESCRIPTION
0	NV_SI_S0_PCP_ACTIVECPM_0_31	0x8000	0xFFFF.FFFF	Master socket user changeable active CPM mask for CPM0 to CPM31 from UEFI. This mask is ORed with the eFuse setting to produce a list of available CPMs.
1	NV_SI_S0_PCP_ACTIVECPM_32_63	0x8008	0xFFFF.FFFF	Master socket user changeable active CPM mask for CPM32 to CPM63 from UEFI. This mask is ORed with the eFuse setting to produce a list of available CPMs.
2	NV_SI_S1_PCP_ACTIVECPM_0_31	0x8010	0xFFFF.FFFF	Slave socket user changeable active CPM mask for CPM0 to CPM31 from UEFI. This mask is ORed with the eFuse setting to produce a list of available CPMs.
3	NV_SI_S1_PCP_ACTIVECPM_32_63	0x8018	0xFFFF.FFFF	Slave socket user changeable active CPM mask for CPM32 to CPM63 from UEFI. This mask is ORed with the chip setting to produce a list of available CPMs.
4	NV_SI_WDT_BIOS_EXP_MINS	0x8020	5	Non-secure watchdog time-out value.

#	NAME	ADDR (ID)	DEFAULT VALUE	DESCRIPTION
5	NV_SI_DDR_CE_RAS_THRESHOLD	0x8028	160	User changeable RAS CE threshold from UEFI. Maximum CE before reporting to BMC per interval windows.
6	NV_SI_DDR_CE_RAS_INTERVAL	0x8030	10	User changeable RAS CE interval window in seconds from UEFI.
7	NV_SI_DRAM_SPEED	0x8038	3200	User changeable DDR speed frequency (MHz) from UEFI. The actual frequency is the minimum of this value and the chip setting. Valid value includes 1600, 1866, 2133, 2400, 2666, 2933, and 3200.
8	NV_SI_DDR_SCRUB_EN	0x8040	1	User changeable DDR background scrubbing.
9	NV_SI_DDR_ECC_MODE	0x8048	1	User changeable ECC Mode. 0: Disabled 1: SECDED 2: Symbol
10	NV_SI_S0_RCA_PCI_DEVMAP	0x8050	0	Reserved.
11	NV_SI_S0_RCB_PCI_DEVMAP	0x8058	0	Reserved.
12	NV_SI_S1_RCA_PCI_DEVMAP	0x8060	0	Reserved.
13	NV_SI_S1_RCB_PCI_DEVMAP	0x8068	0	Reserved.
14	NV_SI_DDR_ERRCTRL	0x8070	0x3	DDR Error Handling Control. Bit 0: err0ctlr0[err0ctrl_de] set to enable defer on read. Bit 1: err0ctlr0[err0ctrl_fi] set to enable FHI (Fault Handling Interrupt). Default is set.
15	NV_SI_DDR_REFRESH_GRANULARITY	0x8078	0x0	Control 2x refresh recovery delay time granularity at high temp. 0: Disabled 1: Enabled
16	NV_SI_SUBNUMA_MODE	0x8080	0x0	Change Sub-NUMA Clustering (SNC) mode. 0: Monolithic 1: Hemisphere 2: Quadrant
17	NV_SI_ERRATUM_1542419_WA	0x8088	0x0	Select workaround for Arm errata 1542419 0: Enable "Disable I-cache coherency" workaround 1: Enable "Software workaround" by trapping to EL3 for each IC IVAU 2: Do not enable the workaround
18	NV_SI_NEAR_ATOMIC_DISABLE	0x8090	0x0	Disable Near-Atomic When disabled, cpuactlr2_el1[2:2] = 0b0
19	NV_SI_DDR_SLAVE_32BIT_MEM_EN	0x8098	0x0	In 2P configuration, when set to 1, hide the slave 1 GB 32-bit PCIe memory region.

#	NAME	ADDR (ID)	DEFAULT VALUE	DESCRIPTION
20	NV_SI_CPUECTLR_EL1_0_31	0x80A0	0x0	Configure CPUECTLR_EL1 register Bit 0-31. **Note**: Pair with the write enable bitmask NV_SI_CPUECTLR_EL1_0_31_WR_EN_MASK.
21	NV_SI_CPUECTLR_EL1_32_63	0x80A8	0x0	Configure CPUECTLR_EL1 register Bit 32-63 . **Note**: Pair with the write enable bitmask NV_SI_CPUECTLR_EL1_32_63_WR_EN_MASK.
22	NV_SI_HARDWARE_EINJ	0x80B0	0x0	Enable Hardware EINJ. When enabled, EINJ requests trigger errors in the hardware for supported IPs. When disabled, EINJ requests generate software simulated errors and do not affect hardware.
23	NV_SI_2P_CE_RAS_THRESHOLD	0x80B8	0x0	Configure the 2P Correctable Error (CE) threshold
24	NV_SI_2P_CE_RAS_INTERVAL	0x80C0	0x0	Configure the 2P CE threshold interval
25	NV_SI_RAS_BERT_ENABLED	0x80C8	0x0	Enable Boot Error Record Table reporting for catastrophic errors
26	NV_SI_HNF_AUX_CTL_0_31	0x80D0	0x0	Configure HNF_AUX_CTL register Bit 0-31. **Note**: Pair with the write enable bitmask NV_SI_HNF_AUX_CTL_0_31_WR_EN_MASK.
27	NV_SI_HNF_AUX_CTL_32_63	0x80D8	0x0	Configure HNF_AUX_CTL register Bit 0-31. **Note:** Pair with the write enable bitmask NV_SI_HNF_AUX_CTL_0_31_WR_EN_MASK.
28	NV_SI_CPM_CE_RAS_THRESHOLD	0x80E0	0x0	Configure the CPM CE threshold
29	NV_SI_CPM_CE_RAS_INTERVAL	0x80E8	0x0	Configure the CPM CE threshold interval
30	NV_SI_HNF_AUX_CTL_0_31_WR_EN_MASK	0x80F0	0x0	Configure write enable bitmask for NV_SI_HNF_AUX_CTL_0_31
31	NV_SI_HNF_AUX_CTL_32_63_WR_EN_MASK	0x80F8	0x0	Configure write enable bitmask for NV_SI_HNF_AUX_CTL_32_63
32	NV_SI_DDR_WR_BACK_EN	0x8100	0x0	–
33	NV_SI_CPUECTLR_EL1_0_31_WR_EN_MASK	0x8108	0x0	Configure write enable bitmask for NV_SI_CPUECTLR_EL1_0_31
34	NV_SI_CPUECTLR_EL1_32_63_WR_EN_MASK	0x8110	0x0	Configure write enable bitmask for NV_SI_CPUECTLR_EL1_32_63
35	NV_SI_LINK_ERR_THRESHOLD	0x8118	0x0	–
36	NV_SI_SEC_WDT_BIOS_EXP_MINS	0x8120	0x5	Configure secure watchdog timeout value. The default timeout value is 5 minutes. Watchdog timer can be disabled by setting this value to '0'.
37	NV_SI_NVDIMM_MODE	0x8128	0x0	Configure NVDIMM-N enabled mode Bits [1:0]: Enabled Mode 0: Disabled 1: Non-Hashed Mode 2: Hashed Mode Bit 31: Valid Check Bit

#	NAME	ADDR (ID)	DEFAULT VALUE	DESCRIPTION
38	NV_SI_RAS_SDEI_ENABLED	0x8130	–	–
39	NV_SI_NVDIMM_PROV_MASK_S0	0x8138	0x0	Indicates whether NVDIMM-N on Socket-0 has been provisioned and will be restored on the next boot. Each bit indicates corresponding populated DIMM: Bit 6: MCU3 Slot0 (0: Not provisioned, 1: Provisioned) Bit 7: MCU3 Slot1 Bit 14: MCU7 Slot0 Bit 15: MCU7 Slot1 Bit 31: Valid Check Bit
40	NV_SI_NVDIMM_PROV_MASK_S1	0x8140	0x0	Indicates whether NVDIMM-N on Socket-1 has been provisioned and will be restored on the next boot. The format is the same with NV_SI_NVDIMM_PROV_MASK_S0.
41	NV_SI_DDR_ZQCS_EN	0x8148	0x0	Configure ZQCS period (in milliseconds) which run in background from SCP. **Note**: Set to 0 to disable ZQCS.
42	NV_SI_DDR_CRC_MODE	0x8150	0x0	Configure DDR Write CRC function (0: Disable, 1: Enable)
43	NV_SI_CXG_RA_AUX_CTL_0_31	0x8158	0x0	Configure CXG_RA_AUX_CTLregister Bit 0-31. **Note**: Pair with the write enable bitmask NV_SI_CXG_RA_AUX_CTL_0_31_WR_EN_MASK.
44	NV_SI_CXG_RA_AUX_CTL_32_63	0x8160	0x0	Configure CXG_RA_AUX_CTL register Bit 32-63. **Note**: Pair with the write enable bitmask NV_SI_CXG_RA_AUX_CTL_32_63_WR_EN_MASK
45	NV_SI_CXG_RA_AUX_CTL_0_31_WR_EN_MASK	0x8168	0x0	–
46	NV_SI_CXG_RA_AUX_CTL_32_63_WR_EN_MASK	0x8170	0x0	–
47	NV_SI_CXLA_AUX_CTL_0_31	0x8178	0x0	Configure CXLA_AUX_CTL register Bit 0-31. **Note**: Pair with the write enable bitmask NV_SI_CXLA_AUX_CTL_0_31_WR_EN_MASK.
48	NV_SI_CXLA_AUX_CTL_32_63	0x8180	0x0	Configure CXLA_AUX_CTL register Bit 32-63. **Note**: Pair with the write enable bitmask NV_SI_CXLA_AUX_CTL_32_63_WR_EN_MASK.
49	NV_SI_CXLA_AUX_CTL_0_31_WR_EN_MASK	0x8188	0x0	–
50	NV_SI_CXLA_AUX_CTL_32_63_WR_EN_MASK	0x8190	0x0	–
51	NV_SI_DDR_LOW_POWER_CFG	0x8198	–	Configure DDR Low Power function. Bit 0: Enable APD (Auto Power-Down). Bit 1: Enable ASR (Auto Self-Refresh). Bit 2: Enable SCP Auto ASR. Bit 8: Enable DMC clock gating. Bit 16: Enable PHY clock gating.

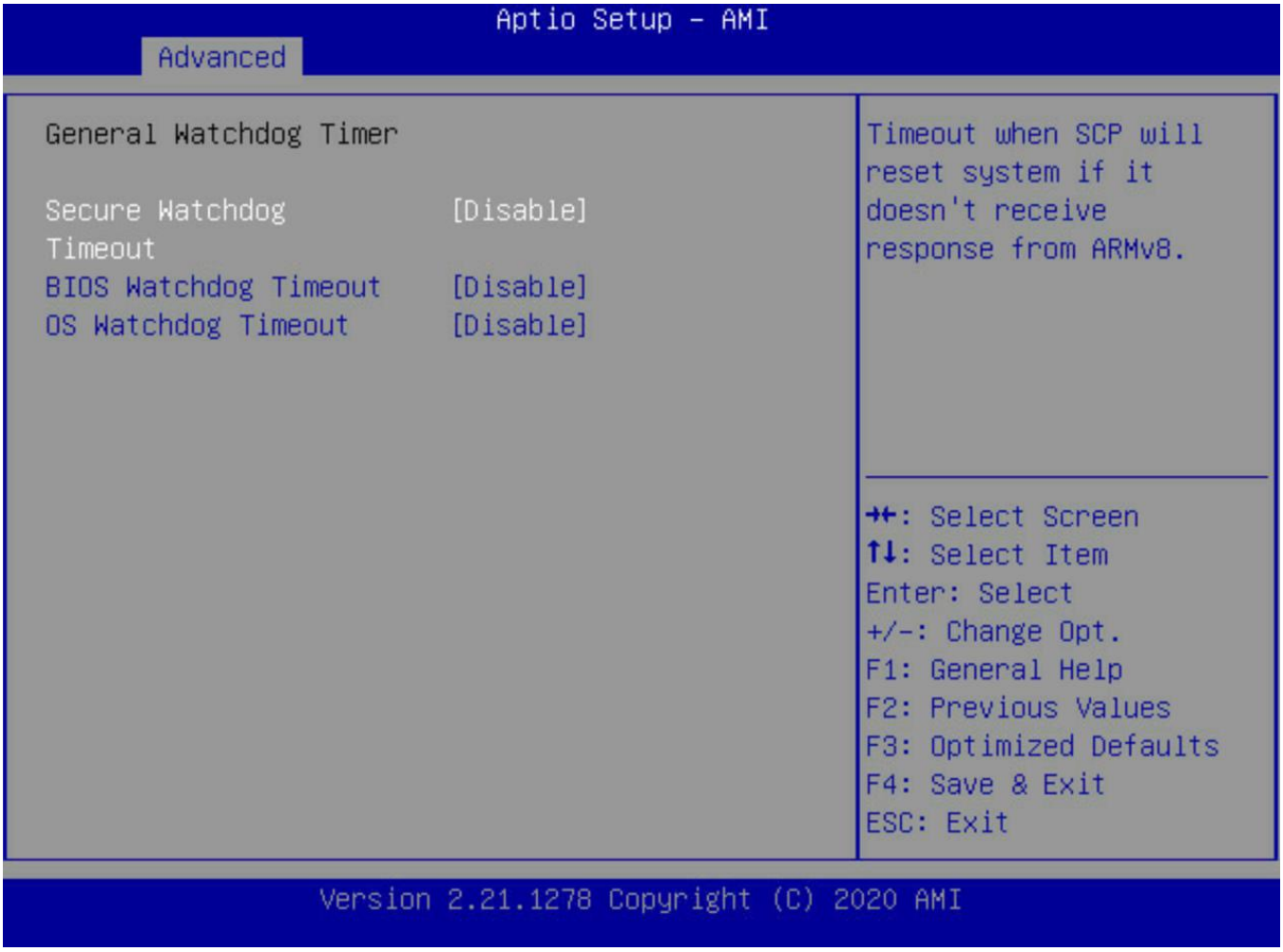
#	NAME	ADDR (ID)	DEFAULT VALUE	DESCRIPTION
52	NV_SI_ALERT_DIMM_SHUTDOWN_EN	0x81A0	–	–
53	NV_SI_DFS_EN	0x81A8	–	DFS, Dynamic Frequency Scale, mode enable. If enabled, DVFS only scales the frequency without changing the voltage.
54	NV_SI_RAS_PCIE_AER_FW_FIRST	0x81B0	–	Override PCIe AER FW-first board setting to enable/disable PCIe AER FW-first. Default: 0x0 – disabled.
55	NV_SI_RAS_DRAM_EINJ_NOTRIGGER	0x81B8	–	Default: 0x0 – disabled.
56	NV_SI_RAS_AEST_PROC_EN	0x81C0	–	Default: 0x0 – disabled.
57	NV_SI_MESH_S0_CXG_RC_STRONG_ORDERING_EN	0x81C8	–	User config to force the PCIe strong-order for S0 (Default is 0x0) Value: 0: Disable, 1: Enable BIT 0: RCA0 BIT 1: RCA1 BIT 2: RCA2 BIT 3: RCA3 BIT 4: RCA4 / RCB0 BIT 5: RCA5 / RCB1 BIT 6: RCA6 / RCB2 BIT 7: RCA7 / RCB3
58	NV_SI_MESH_S1_CXG_RC_STRONG_ORDERING_EN	0x81D0	–	User config to force the PCIe strong-order for S1 (Default is 0x0) Value: 0: Disable, 1: Enable BIT 0: RCA0 BIT 1: RCA1 BIT 2: RCA2 BIT 3: RCA3 BIT 4: RCA4 / RCB0 BIT 5: RCA5 / RCB1 BIT 6: RCA6 / RCB2 BIT 7: RCA7 / RCB3
59	NV_SI_2P_RESERVED0	0x81D8	–	This User value is reserved.
60	NV_SI_2P_RESERVED1	0x81E0	–	This User value is reserved.
61	NV_SI_2P_RESERVED2	0x81E8	–	This User value is reserved.
62	NV_SI_HCR_EL2_CTL_LOW	0x81F0	–	< >
63	NV_SI_HCR_EL2_CTL_HIGH	0x81F8	–	< >

#	NAME	ADDR (ID)	DEFAULT VALUE	DESCRIPTION
64	NV_SI_ESM_SPEED	0x8200	–	This User config value is used to configure 2p Link Speed between sockets (Default is 0x14 – 20 Gbps) Value: 0x10 – 16 Gbps 0x14 – 20 Gbps 0x19 – 25 Gbps

Appendix C: Preventing System Reboot During Core Debugging

While debugging Aptio® V, the system may reboot after a while because of a Watchdog timer timeout. To prevent this scenario, the user must navigate to **Advanced** > **General Watchdog Timer** setup screen and disable both **Secure Watchdog Timeout** and **BIOS Watchdog Timeout** as shown in *Figure 62*.

Figure 62: Disabling BIOS/SCP Watchdog Timeout



Appendix D: Disabling NVMe Freeze Lock

By default, BIOS enables freeze lock feature for all NVMe disks detected. To allow the OS to use low-level commands to erase the disk, this feature must be disabled by setting the NvmeFreezeSkip UEFI variable.

Example commands in Linux to do this are:

```
echo -n $'\x01' > binary01.dat
efivar -w -n ec87d643-eba4-4bb5-a1e5-3f3e36b20da9-NvmeFreezeSkip -f binary01.dat -t 7
efivar -p -n ec87d643-eba4-4bb5-a1e5-3f3e36b20da9-NvmeFreezeSkip
```

Appendix E: Accessing NVPARAM from OS

To read/write an Ampere NVPARAM value in OS:

- GUID for accessing UEFI variable: 0xa12544a4, 0xbcc0, 0x4b12, { 0xaa, 0x56, 0x0a, 0x2a, 0x76, 0xf1, 0x65, 0x63 }

To read an NVPARAM:

+ Write offset (4 bytes) to UEFI variable name "Offset".

+ Read back UEFI variable name "Offset" (4 bytes) to get the value.

To write a NVPARAM:

+ Write offset (4 bytes) to UEFI variable name "Offset"

+ Write 4 bytes value to UEFI variable name "Value".

Document Revision History

ISSUE	DATE	DESCRIPTION
0.92	June 29, 2021	• Updated *Figure 37* (*RAS Configuration Screen*). • Added *PCIe AER Firmware First* and *Processor OS First* settings to *Table 17* (*RAS Configuration Parameters*). • Updated the description for the *DDR CE Threshold* setting in *Table 17* (*RAS Configuration Parameters*).
0.91	April 27, 2021	• Updated the section titled *General Watchdog Timer* to describe watchdog behavior for settings.
0.90	April 21, 2021	• Updated *Table 6* (*PCIe Slot Mapping table*). • Updated *Table 25* (*Manufacturing Pre-Boot Settings*). • Updated *Table 26* (*User Pre-Boot Settings*). • Added *Appendix C: Preventing System Reboot During Core Debugging*. • Added *Appendix D: Disabling NVMe Freeze Lock*. • Added *Appendix E: Accessing NVPARAM from OS*.
0.83	September 25, 2020	• Added NVDIMM-N configuration screen in the section titled *Memory Configuration*. • Added PCIe Settings screen in the section titled *PCI Subsystem Settings*. • Updated RAS Configuration screen in the section titled *Reliability, Availability, and Serviceability (RAS) Configuration*. • Added the description for Hemisphere in the section titled *CPU Configuration*. • Minor technical and editorial revisions.
0.82	September 23, 2020	• Added PCIe Settings screen in the section titled *PCI Subsystem Settings*. • Updated RAS Configuration screen in the section titled *Reliability, Availability, and Serviceability (RAS) Configuration*. • Minor technical and editorial revisions.
0.81	September 11, 2020	Updated the following: • *Advanced Tab*. • *General Watchdog Timer*, including the Secure Watchdog Timeout option. • Updated CPU screen in the section titled *CPU Configuration*, including inter-socket information. • Updated memory performance screen, including new options in the section titled *Memory Configuration*. • Updated chipset PCIe screen, including new options in the section titled *PCIe Root Complex (RC) Configuration*. • Minor technical and editorial revisions.

ISSUE	DATE	DESCRIPTION
0.80	July 26, 2020	Updated the following: • *Power-On Self-Test (POST) Screen* • *Advanced Tab* • *Chipset Tab* • *Table 25* (*Manufacturing Pre-Boot Settings*) • *Table 26* (*User Pre-Boot Settings*) Added the following: • *Trusted Computing Settings* • *Table 19* (*Memory Performance Parameters*) • *Table 20* (*Supported Memory Channel Configurations*) • *Table 23* (*Root Complex Configuration*) Deleted the following: • Section titled *VGA Controller* • Minor technical and editorial revisions.
0.55	April 07, 2020	• Updated the section titled *Trusted Computing Settings*. • Minor technical and editorial revisions.
0.50	December 18, 2019	Initial issue.

June 29, 2021

Ampere Computing reserves the right to change or discontinue this product without notice.

While the information contained herein is believed to be accurate, such information is preliminary, and should not be relied upon for accuracy or completeness, and no representations or warranties of accuracy or completeness are made.

The information contained in this document is subject to change or withdrawal at any time without notice and is being provided on an "AS IS" basis without warranty or indemnity of any kind, whether express or implied, including without limitation, the implied warranties of non-infringement, merchantability, or fitness for a particular purpose.

Any products, services, or programs discussed in this document are sold or licensed under Ampere Computing's standard terms and conditions, copies of which may be obtained from your local Ampere Computing representative. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Ampere Computing or third parties.

Without limiting the generality of the foregoing, any performance data contained in this document was determined in a specific or controlled environment and not submitted to any formal Ampere Computing test. Therefore, the results obtained in other operating environments may vary significantly. Under no circumstances will Ampere Computing be liable for any damages whatsoever arising out of or resulting from any use of the document or the information contained herein.

Ampere Computing
4655 Great America Parkway, Santa Clara, CA 95054
Phone: (669) 770-3700
https://www.amperecomputing.com

Ampere Computing reserves the right to make changes to its products, its datasheets, or related documentation, without notice and warrants its products solely pursuant to its terms and conditions of sale, only to substantially comply with the latest available datasheet.

Ampere, Ampere Computing, the Ampere Computing and 'A' logos, Altra, and eMAG are registered trademarks of Ampere Computing.

Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere. All other trademarks are the property of their respective holders.