M10JNP2SB

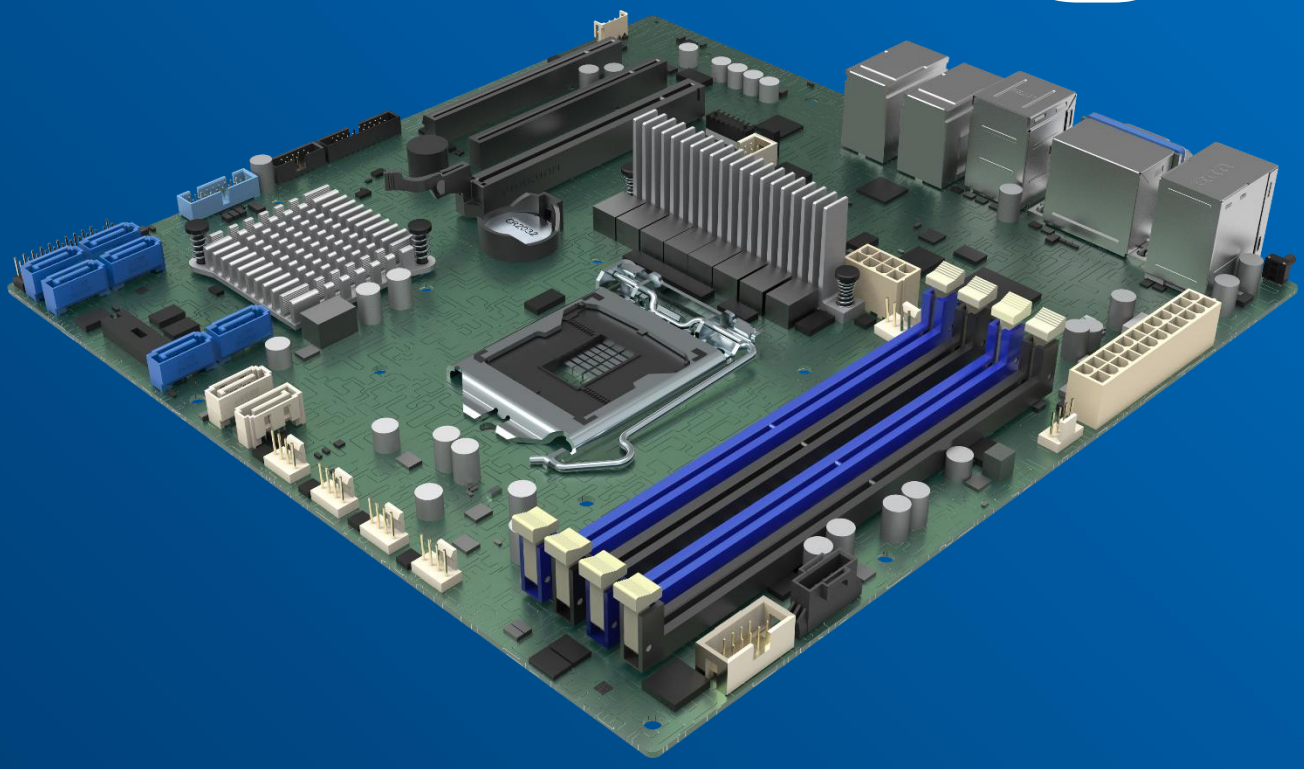
# Intel® Server Board M10JNP2SB

## *BIOS Setup Guide*

An overview of the setup, layout, and organization of BIOS menus.

**Rev. 1.2**

**January 2022**



<Blank page>

# *Document Revision History*

| Date | Revision | Changes |
|---|---|---|
| **October 2019** | 1.0 | Initial release. |
| **January 2020** | 1.1 | Updated Figure 2. BIOS main menu. |
| **January 2022** | 1.2 | Updated Section 3.3.6 ACPI Settings.<br>Updated Section 3.3.8 PCIe* Subsystem Settings.<br>Minor changes throughout the document to improve style and clarity. |

# Disclaimers

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

The products described may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Copies of documents that have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.

Intel and the Intel logo are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

# Table of Contents

# List of Figures

# List of Tables

<Blank Page>

# 1. Introduction

The *Intel® Server Board M10JNP2SB BIOS Setup Guide* describes the layout and organization of the BIOS menus. This document consists of an image-first format followed by a corresponding table filled with definitions and values.

## 1.1 Audience

The BIOS setup design specification is written for people involved in design, validation, integration, production, and support of Intel® server boards and systems in which they are installed. For the reader to better understand this setup guide, they must be familiar with Intel® processors and the standards that define the server architecture.

## 1.2 Purpose

This document contains a description of the BIOS setup implementation for the Intel® server board family. The purpose of this setup guide is specifying how the BIOS setup should function and what interfaces and functions it provides to other system components.

# 2. BIOS Setup Operation

The BIOS setup utility is a text-based utility that allows the user to configure the system and view current settings and environment information for the platform devices. The setup utility controls the platform's built-in devices, the boot manager, and error manager.

The BIOS setup interface consists of a number of pages or menus. Each page contains information or links to other pages. The advanced tab in Setup displays a list of general categories as links. These links lead to menus containing a specific category's configuration.

The BIOS Setup may be protected from unauthorized changes by setting an Administrative Password in the Security screen. When an Administrative Password has been set, all selection and data entry fields in setup (except System Time and Date) are grayed out and cannot be changed unless the Administrative Password has been entered.

**Note**: If an Administrative Password has not been set, anyone who boots the system to Setup has access to all selection and data entry fields in Setup and can change any of them.

## 2.1 Setup Page Layout

The setup page layout is sectioned into functional areas. Each occupies a specific area of the screen and has dedicated functionality. The following table lists and describes each functional area.

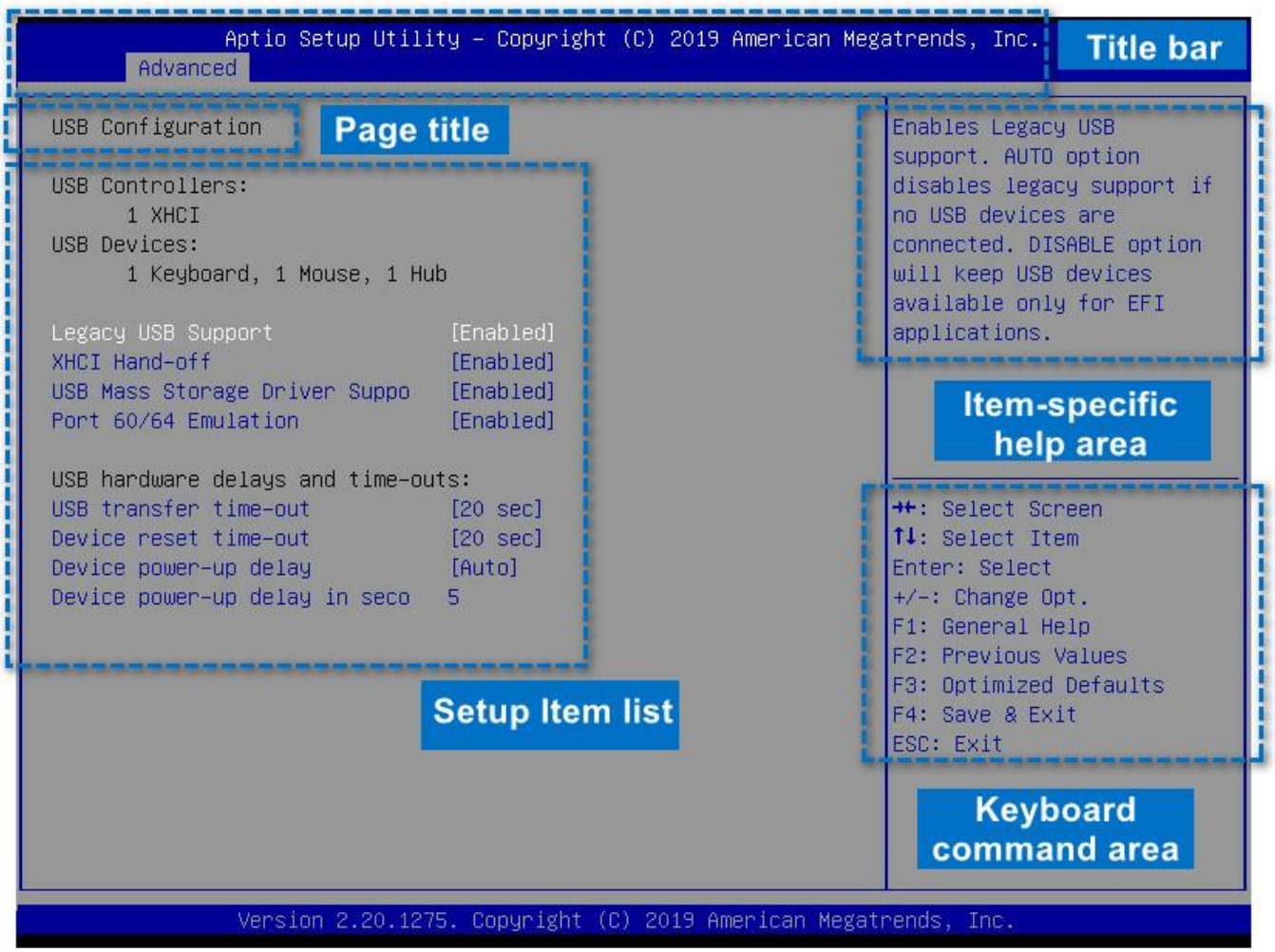



**Figure 1. BIOS setup screen layout**

**Table 1. BIOS setup page layout**

| Functional Area | Description |
|---|---|
| **Title Bar** | The Title Bar is at the top of the screen and displays "tabs" with the titles of the top-level pages or screens that can be selected. Using the left and right arrow keys moves from page to page through the tabs.<br>When there are more tabs than can be displayed on the Title Bar, they will scroll off to the left or right of the screen and temporarily disappear from the visible Title Bar. Using the arrow keys will scroll them back onto the visible Title Bar. When the arrow keys reach either end of the Title Bar, they will "wrap around" to the other end of the Title Bar.<br>For multi-level hierarchies, this shows only the top-level page above the page that the user is currently viewing. The Page Title gives further information. |
| **Page Title** | In a multi-level hierarchy of pages beneath one of the top-level Tabs, the Page Title identifying the specific page that the user is viewing is in the upper left corner of the page. Using the **<ESC>** key will return the user to the higher level in the hierarchy, until the top-level page is reached. |
| **Setup Item List** | The setup item list is a set of control entries and informational items. The list is displayed in two columns. For each item in the list:<br>The left column of the list contains Prompt String (or Label String), a character string that identifies the item. The Prompt String may be up to 34 characters long in the 80 x 24 page format.<br>The right column contains a data field that may be an informational data display, a data input field, or a multiple choice field. Data input or multiple-choice fields are demarcated by square brackets "[….]".<br>This field may be up to 90 characters long but only the first 22 characters can be displayed on the 80 x 24 page (24 characters for an informational display-only field).<br>The operator navigates up and down the right hand column through the available input or choice fields. A Setup Item may also represent a selection to open a new screen with a further group of options for specific functionality. In this case, the operator navigates to the desired selection and presses <Enter> to go to the new screen. |
| **Item-Specific Help Area** | The item-specific help area is on the right side of the screen and contains help text specific to the highlighted Setup Item. Help information may include the meaning and usage of the item, allowable values, effects of the options, etc.<br>The help area is a 29 character by 11 line section of the 80 x 24 page. The help text may have explicit line-breaks within it. When the text is longer than 29 characters, it is also broken to a new line, dividing the text at the last space (blank) character before the 29th character. An unbroken string of more than 29 characters will be arbitrarily wrapped to a new line after the 29th character. Text that extends beyond the end of the 11th line will not be displayed. |
| **Keyboard Command Area** | The keyboard command area is at the bottom right of the screen and continuously displays help for keyboard special keys and navigation keys. |

## 2.2 Entering BIOS Setup

To enter the BIOS setup using a keyboard (or emulated keyboard), press the **<F2>** function key during boot time when the OEM, Intel logo screen, or the POST diagnostic screen is displayed.

The following instructional message is displayed on the diagnostic screen:

```
Press <DEL> or <F2> to enter setup
Press <F11> for BBS POPUP
Press <F12> if you want to boot from the network
```

**Note**: With a USB keyboard, wait until the BIOS "discovers" the keyboard and beeps. Until the USB controller has been initialized and the USB keyboard activated, key pressing will not be read by the system.

The Main menu is initially displayed once the setup utility has been entered.

## 2.3 Exit BIOS Setup

Three ways to exit the BIOS setup are supported:

1. By pressing **<Esc>**
2. By selecting **Save & Exit** >> **Save changes and exit**
3. By selecting **Save & Exit** >> **Discard Changes and Exit**

No matter whether the changes are made or not, the system will do a cold reset after the above methods applied. For more information on the Save & Exit screen, see Section 8.

## 2.4 Setup Navigation Keyboard Commands

The bottom right portion of the setup screen provides a list of commands that are used to navigate through the Setup utility. These commands are displayed at all times.

Each setup menu contains a number of features. Each feature is associated with a value field, except those used for informative purposes. Each value field contains configurable parameters. Depending on the security option chosen and in effect by the password, a menu feature's value may or may not be changed. If a value cannot be changed, its field is made inaccessible and appears grayed out.

**Table 2. BIOS setup keyboard command bar**

| Key | Option | Description |
|---|---|---|
| **<Enter>** | Execute Command | The **<Enter>** key is used to activate submenus when the selected feature is a submenu, or to display a pick list if a selected option has a value field, or to select a subfield for multi-valued features like time and date. If a pick list is displayed, the <Enter> key selects the currently highlighted item, undoes the pick list, and returns the focus to the parent menu. |
| **<Esc>** | Exit | The **<Esc>** key provides a mechanism for backing out of any field. When the **<Esc>** key is pressed while editing any field or selecting features of a menu, the parent menu is re-entered.<br>When the **<Esc>** key is pressed in any submenu, the parent menu is re-entered. |
| **<↑>** | Select Item | The up arrow is used to select the previous value in a pick list, or the previous option in a menu item's option list. The selected item must then be activated by pressing the <Enter> key. |
| **<↓>** | Select Item | The down arrow is used to select the next value in a menu item's option list, or a value field's pick list. The selected item must then be activated by pressing the <Enter> key. |
| **<Tab>** | Select Field | The **<Tab>** key is used to move between fields. For example, <Tab> can be used to move from hours to minutes in the time item in the main menu. |
| **<->** | Change Value | The minus key on the keypad is used to change the value of the current item to the previous value. This key scrolls through the values in the associated pick list without displaying the full list. |
| **<+>** | Change Value | The plus key on the keypad is used to change the value of the current menu item to the next value. This key scrolls through the values in the associated pick list without displaying the full list. On 106-key Japanese keyboards, the plus key has a different scan code than the plus key on the other keyboards but will have the same effect. |
| **<F3>** | Reset to Defaults | Pressing the **<F3>** key causes the following to display:<br>`Load Optimized defaults?`<br>`'Yes' 'No'`<br>If 'Yes' is selected, all setup fields are set to their default values. If 'No' is selected, or if the **<Esc>** key is pressed, the user is returned to where they were before **<F3>** was pressed without affecting any existing field values. |
| **<F4>** | Save Changes and Exit | Pressing the **<F4>** key causes the following message to display:<br>`Save configuration and exit?`<br>`'Yes' 'No'`<br>If 'Yes' is selected, all changes are saved and the setup is exited. If 'No' is selected, or the **<Esc>** key is pressed, the user is returned to where they were before **<F4>** was pressed without affecting any existing values. |

# 3. Setup Menus

The following sections describe the menus available within the BIOS setup utility for the configuration of the server platform.

For each of these menus, there is an image of the menu followed by a table of descriptions detailing the configurable options on the screen.

These tables have the following guidelines:

- The text heading for each field description is the actual text displayed on the BIOS setup screen. The screen text in each figure is a hyperlink to its corresponding field description.
- The help text entry is the actual text that appears on the BIOS setup screen when the item is in focus (active on the screen).
- When information is changed (except date and time), the system requires a save and reboot for the changes to take effect. Alternatively, pressing **<ESC>** discards the changes and resumes power on self-test (POST) to continue to boot the system according to the boot order set from the last boot.

## 3.1 Title Bar

The title bar contains the entire BIOS setup collection and organizes them into major categories. Each category has a hierarchy with a top-level screen from which lower-level screens may be selected.

Each top-level screen appears listed from left to right. To access a top-level screen from the front page or other top-level screen, press the left or right arrow keys to traverse the tabs until the desired menu is selected.

## 3.2 Main Menu

The Main menu is the first screen that appears when entering the BIOS setup configuration utility.

**Note:** The options listed below are for options that can directly be changed within the Main Setup screen.


**Figure 2. BIOS main menu**

**Table 3. BIOS main menu options**

| Menu Item | Description |
|---|---|
| **BIOS Information** | Displays BIOS related information. |
| **Memory Information** | Displays the total memory size. |
| **System Date** | Set the date. Use Tab to switch between date elements. Default Ranges:<br>• Year: 2010–2079<br>• Months: 1–12<br>• Days: dependent on month |
| **System Time** | Set the time.<br>Use **Tab** to switch between time elements. |
| **Access Level** | Read only. |

## 3.3 Advanced Menu

The Advanced menu provides an access point to configure several groups of advanced options. On this menu, select the option group to be configured. Configuration actions are performed on the selected screen and not directly on the Advanced screen.

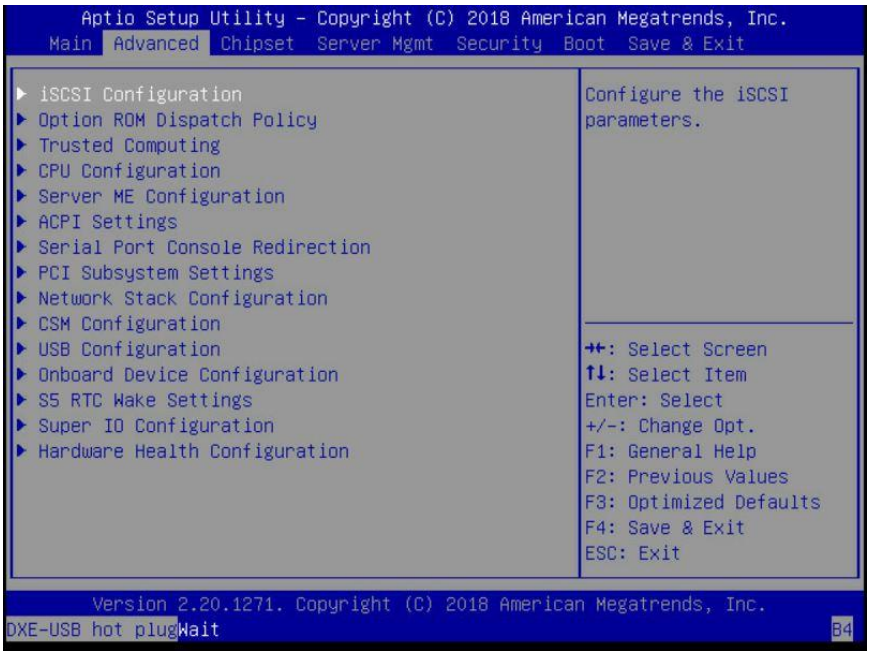



**Figure 3. Advanced menu**

**Table 4. Advanced menu options**

| Menu Item | Description |
|---|---|
| **iSCSI Configuration** | Configure the iSCSI parameters. |
| **Option ROM Dispatch Policy** | Option ROM Dispatch Policy submenu. |
| **Trusted Computing** | Trusted Computing settings submenu. |
| **CPU Configuration** | CPU Configuration parameters submenu. |
| **Server ME Configuration** | Server ME Configuration submenu. |
| **ACPI Settings** | System ACPI parameters submenu. |
| **Serial Port Console Redirection** | Serial Port Console Redirection submenu. |
| **PCI Subsystem Settings** | PCI, PCI-X and PCI Express* Settings submenu. |
| **Network Stack Configuration** | Network Stack Settings submenu. |
| **CSM Configuration** | CSM configuration: Enable/Disable, Option ROM execution settings, etc. |
| **USB Configuration** | USB Configuration Parameters submenu. |
| **Onboard Device Configuration** | Onboard Device Configuration submenu. |
| **S5 RTC Wake Settings** | Enable system to wake from S5 using the RTC alarm. |
| **Super IO Configuration** | System Super IO chip parameters submenu. |
| **Hardware Health Configuration** | Hardware Health Configuration parameters submenu. |

### 3.3.1 iSCSI Configuration

The iSCSI Configuration menu allows the user to configure a connection for booting from an iSCSI target.

To access this screen from the front page, select **Advanced** > **iSCSI Configuration**. Press the **<Esc>** key to return to the **Advanced** menu.

---

**Note**: Only LAN1 supports booting from an iSCSI target.

---

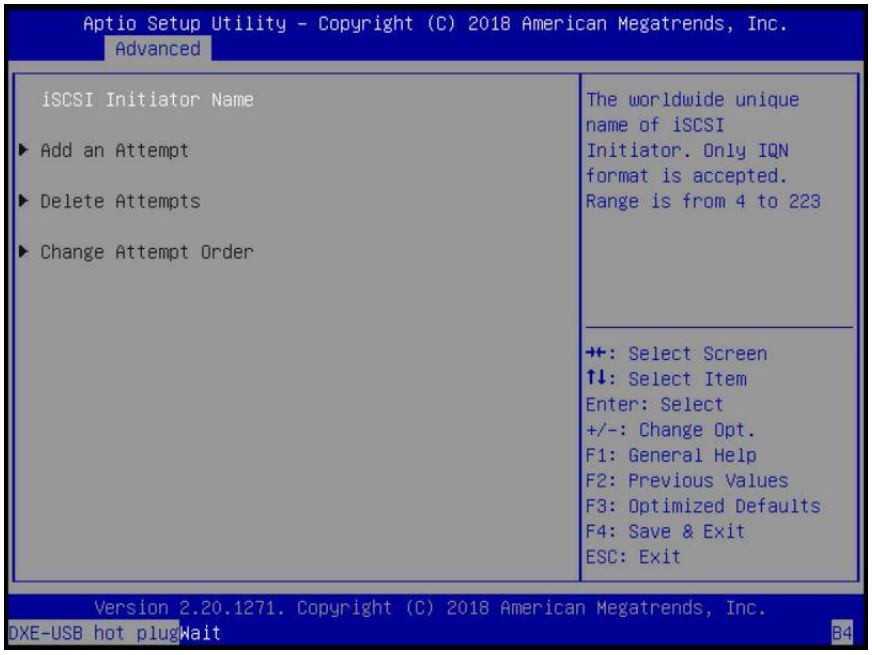



**Figure 4. iSCSI configuration menu**

Follow these instructions to initiate UEFI iSCSI functionality:

1. Connect to iSCSI Server.
2. Option ROM Dispatch Policy Settings:
    a. Advanced > Option ROM Dispatch Policy >> Onboard Lan1 (I210) [Enabled]
3. Advanced > Option ROM Dispatch Policy >> Onboard Lan1 Option ROM type [iSCSI]
4. Network Stack Configuration Settings:
    a. Advanced > Network Stack Configuration >> Network Stack [Enabled]
5. CSM Configuration Settings:
    a. Advanced > CSM Configuration >> CSM Support [Disabled]
    OR
    b. Advanced > CSM Configuration >> CSM Support [Enabled]
    c. Advanced > CSM Configuration >> Network [UEFI]
6. Save changes and reboot.
7. Enter to SCSI Configuration.
8. Set iSCSI Initiator Name (Ex: iqn.xxx)
9. Enter to “Add an Attempt”.
10. Enter to a Device (Ex: MAC A0:42:3F:3A:E4:B4)
11. Set Configuration items.

#### 3.3.1.1 Add an Attempt

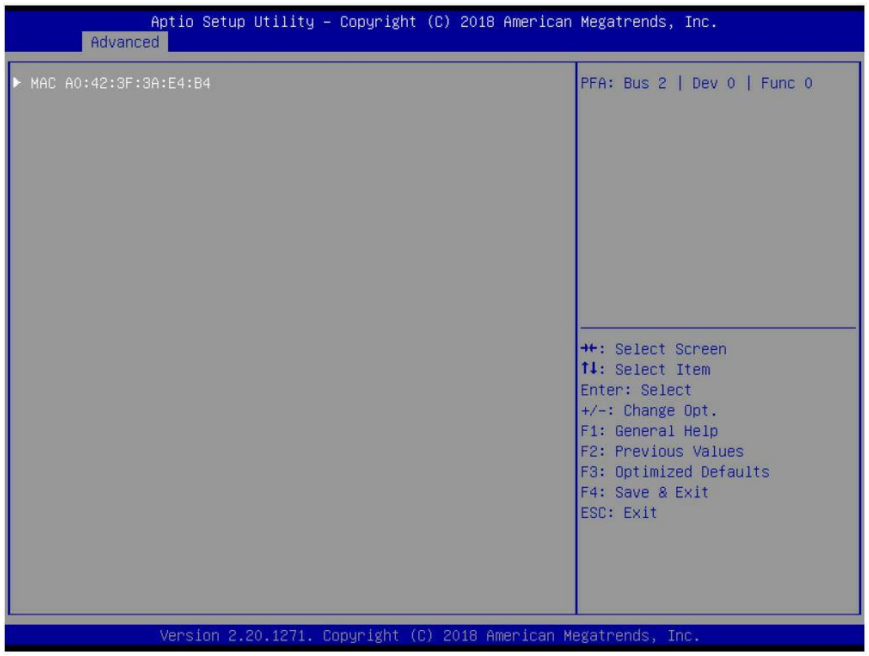



**Figure 5. Adding an attempt menu**

Read only. This MAC address is for iSCSI and subject to change.

### 3.3.1.2 MAC Address

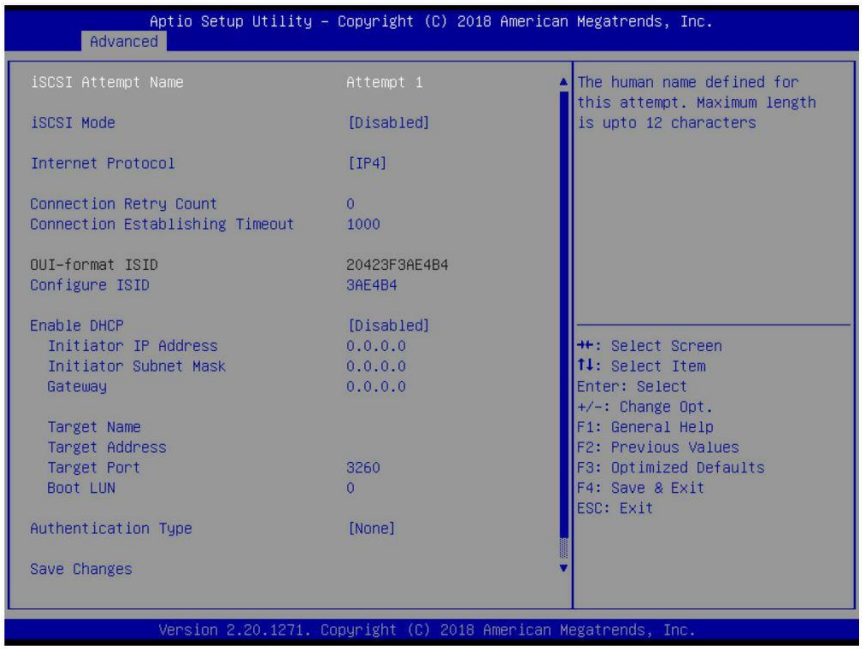



**Figure 6. MAC address menu**

**Note:** The MAC address is for iSCSI and subject to change.

**Table 5. MAC address menu options**

| Menu Item | Description | Values |
|---|---|---|
| **iSCSI Mode** | Choose from Disabled, Enabled, or Enabled for MPIO. | • **Disabled**<br>• Enabled<br>• Enabled for MPIO |
| **Internet Protocol** | The initiator IP address is system assigned in IP6 mode. In Autoconfigure mode, the iSCSI driver attempts to connect to the iSCSI target via the IPv4 stack.<br>If the attempt fails, the system will then attempt to connect via the IPv6 stack. | • **IP4**<br>• IP6<br>• Autoconfigure |
| **Connection Retry Count** | The minimum value is 0, the maximum is 16. 0 means the connection will not retry. | |
| **Connection Establishing Timeout** | The timeout value in milliseconds. The minimum value is 100 milliseconds and the maximum is 20 seconds. | |
| **Configure ISID** | Configures the OUI-format ISID in 6 bytes, and the default value is derived from the MAC address. Only the last 3 bytes are configurable.<br>Example: Update 0ABBCCDDEEFF to OABBCCF07901 by input F07901. | |
| **Enable DHCP** | Enable DHCP | • **Disabled**<br>• Enabled |
| **Initiator IP Address** | Enter an IP address in dotted-decimal notation. | |
| **Initiator Subnet Mask** | Enter an IP address in dotted-decimal notation. | |
| **Gateway** | Enter an IP address in dotted-decimal notation. | |
| **Target Name** | The worldwide unique name of the target. Only iqn. format is accepted. | |
| **Target Port** | Target port. | |
| **Target IP Address** | Enter an IP address in dotted-decimal notation. | |
| **Boot LUN** | Hexadecimal representation of the LU number.<br>Examples are: 4752-3A4F-6b7e-3F99, 6734-9-156f-127, 4186-9. | |
| **Authentication Type** | Choose the authentication method: CHAP, Kerberos, or None. | • **None**<br>• CHAP |
| **Save Changes** | Must reboot system manually for changes to take place. | |

### 3.3.1.3 Delete Attempts

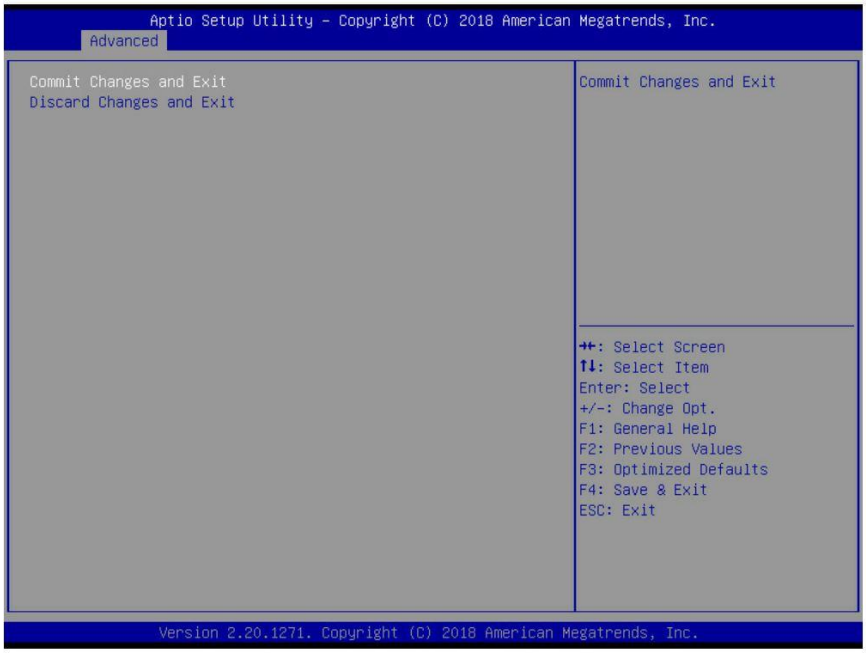



**Figure 7. Deleting an attempt**

**Table 6. Delete attempts submenu options**

| Menu Item | Description |
|---|---|
| **Commit Changes and Exit** | Commit Changes and Exit |
| **Discard Changes and Exit** | Discard Changes and Exit |

#### 3.3.1.4 Change Attempt Order

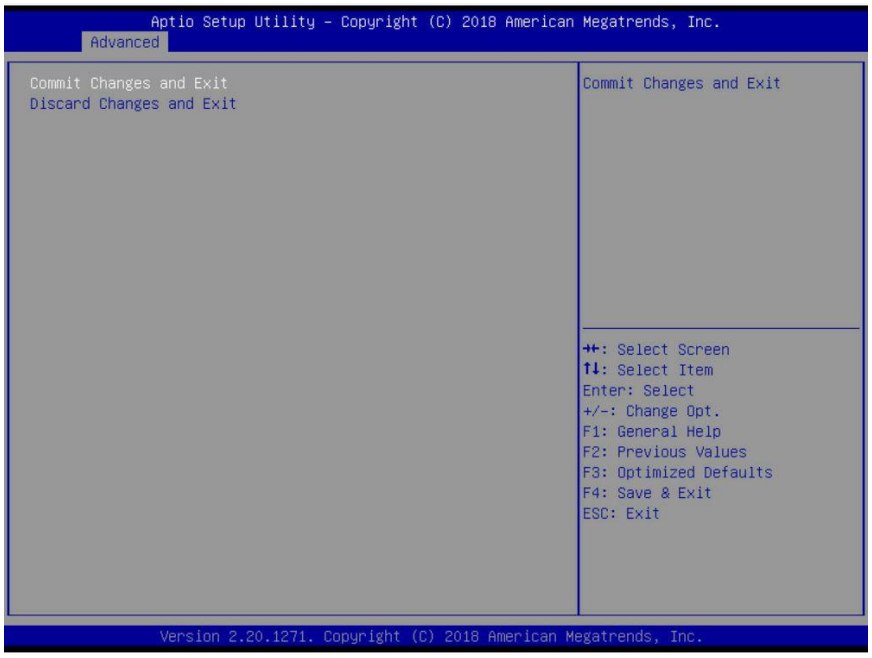



**Figure 8. Changing the attempt order**

**Table 7. Change attempt order submenu options**

| Menu Item | Description |
|---|---|
| **Commit Changes and Exit** | Commit Changes and Exit |
| **Discard Changes and Exit** | Discard Changes and Exit |

### 3.3.2 Option ROM Dispatch Policy

The Option ROM Dispatch Policy menu allows the user to configure different available option ROMs that the BIOS can execute.

To access this screen from the front page, select **Advanced > Option ROM Dispatch Policy**. Press the **<Esc>** key to return to the Advanced menu.

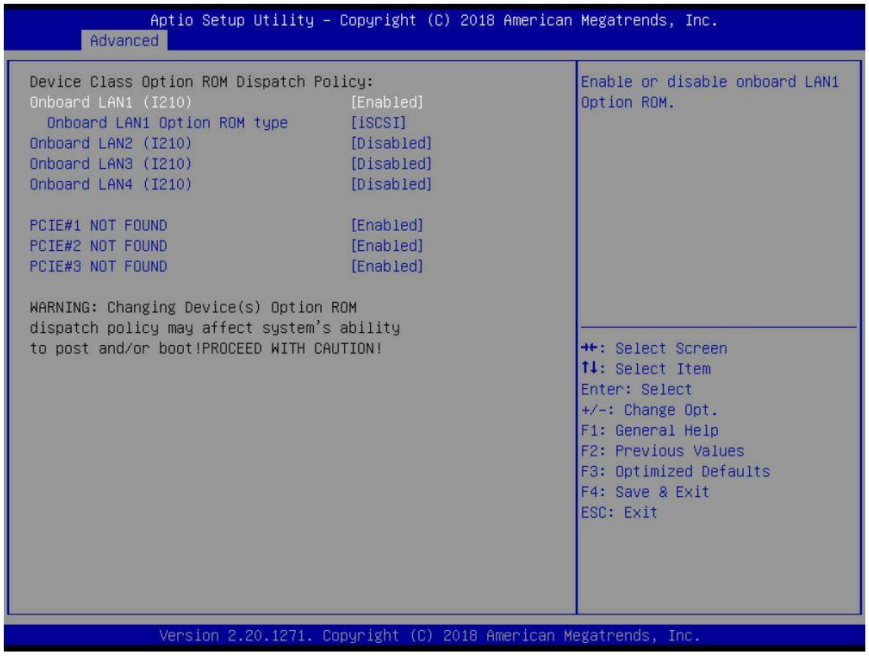



**Figure 9. Option ROM dispatch policy menu**

**Table 8. Option ROM dispatch policy menu options**

| Menu Item | Description | Values |
|---|---|---|
| **Onboard LAN (I210)** | Enable or disable onboard the LAN1 Option ROM. | • **Enabled**<br>• Disabled |
| **Onboard LAN1 Option ROM type** | Select the onboard LAN1 Option ROM type. | • **iSCSI**<br>• PXE |
| **Onboard LAN2 (I210)** | Enable or disable onboard LAN2 Option ROM. | • **Disabled**<br>• Enabled |
| **Onboard LAN3 (I210)** | Enable or disable onboard LAN3 Option ROM. | • **Disabled**<br>• Enabled |
| **Onboard LAN4 (I210)** | Enable or disable onboard LAN4 Option ROM. | • **Disabled**<br>• Enabled |
| **PCIE#1 Not Found ~ PCIE#3 Not Found** | Enable or Disable Option ROM execution for selected Slot. | • **Enabled**<br>• Disabled |

### 3.3.3 Trusted Computing

The Trusted Computing menu allows the user to configure visibility of the TPM device (whether it is installed or not) to the installed OS.

To access this screen from the front page, select **Advanced > Trusted Computing**. Press the **<Esc>** key to return to the Advanced menu.

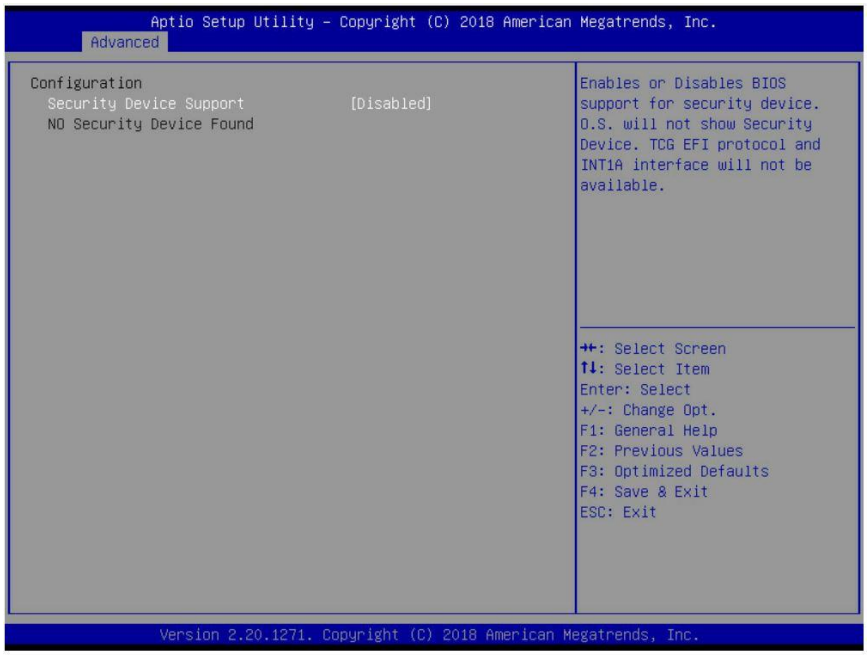



**Figure 10. Trusted computing submenu**

**Table 9. Trusted computing submenu options**

| Menu Item | Description | Values |
|---|---|---|
| **Security Device Support** | Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available. | • **Disabled**<br>• Enabled |

When **Security Device Support** is set to **Enabled**:

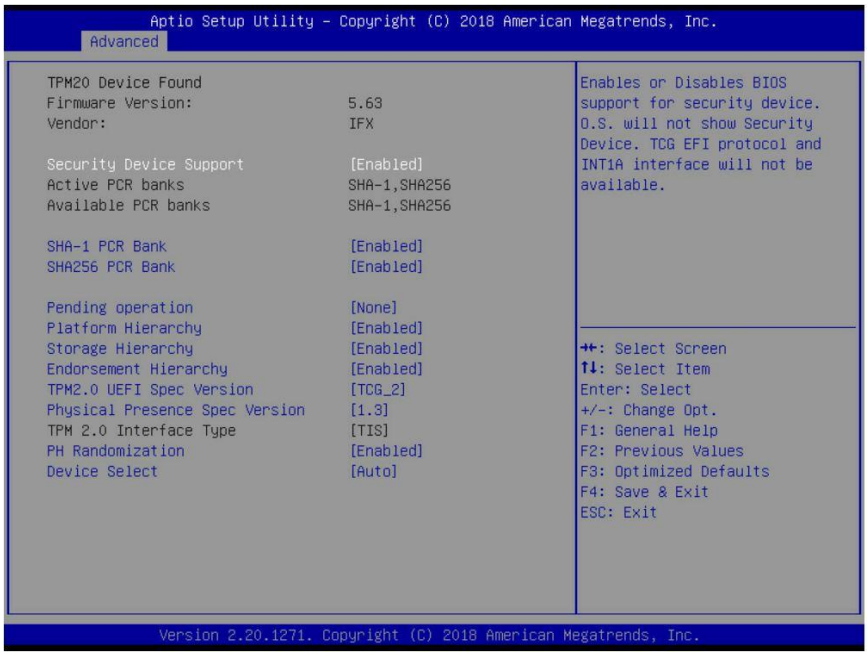



**Figure 11. Security device support submenu**

**Table 10. Security device support submenu options**

| Menu Item | Description | Values |
|---|---|---|
| **SHA-1 PCR Bank** | Enables or Disables SHA-1 PCR Bank. | • **Enabled**<br>• Disabled |
| **SHA256 PCR Bank** | Enables or Disables SHA256 PCR Bank. | • **Enabled**<br>• Disabled |
| **Pending operation** | Schedule an operation for the Security Device The system will reboot during restart in order to change the state of the Security Device. | • **None**<br>• TPM Clear |
| **Platform Hierarchy** | Enable or Disable Platform Hierarchy. | • **Enabled**<br>• Disabled |
| **Storage Hierarchy** | Enable or Disable Storage Hierarchy. | • **Enabled**<br>• Disabled |
| **Endorsement Hierarchy** | Enable or Disable Endorsement Hierarchy. | • **Enabled**<br>• Disabled |
| **TPM2.0 UEFI Spec Version** | Select the TCG2 Spec Version:<br>• TCG_1_2: Compatible mode for Windows* 8/Windows 10<br>• TCG_2: New TCG2 protocol and event format for Windows 10 or later. | • **TCG_2**<br>• TCG_1_2 |
| **Physical Presence Spec Version** | Select to enable PPI Spec version 1.2 or 1.3 in the OS. Some GCJ tests might not support vesrion 1.3. | • **1.3**<br>• 1.2 |
| **TPM 2.0 Interface Type** | Read only. | |
| **PM Randomization** | Enable or Disable Platform Hierarchy randomization. | • **Enabled**<br>• Disabled |
| **Device Select** | TPM 1.2 restricts support to TPM 1.2 devices. TPM 2.0 restricts support to TPM 2.0 devices. Auto supports both with the default set to TPM 2.0 devices if not found. | • **Auto**<br>• TPM 1.2<br>• TPM 2.0 |

### 3.3.4 CPU Configuration

The CPU Configuration menu displays the processor identification and microcode level, core frequency, cache sizes, and supported features. It also allows the user to enable or disable a number of processor options.

To access this screen from the main menu, select **Advanced > CPU Configuration**. Press the **<Esc>** key to return to the Advanced menu.

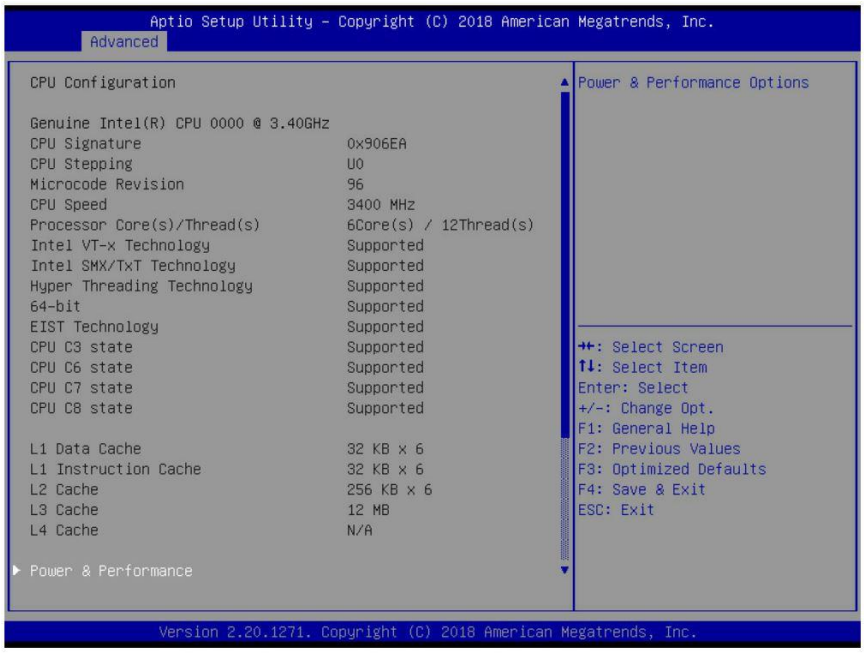



**Figure 12. CPU configuration menu**

**Table 11. CPU configuration menu options**

| Menu Item | Description | Values |
|---|---|---|
| **CPU Configuration** | Read only. | |
| **Power & Performance** | Power & Performance Options. | |
| **Hyper-threading** | **Enabled** for Windows XP and Linux (OS optimized for Intel® Hyper-Threading Technology).<br>**Disabled** for other OS (OS not optimized for Intel® Hyper-Threading Technology).<br>**Note:** If Intel® Hyper-threading Technology is unsupported, this item is hidden. | • **Supported**<br>• Disabled |
| **Active Processor Cores** | Number of cores to enable in each processor package. | • **All**<br>• 1<br>• 2<br>• 3<br>• 4<br>• 5 |
| **Intel (VT-x) Virtualization Technology** | When enabled, a VMM can use the additional hardware capabilities provided by Vanderpool* Technology. | • **Supported**<br>• Disabled |
| **Intel Trusted Execution Technology** | Enables utilization of additional hardware capabilities provided by Intel® Trusted Execution Technology. Changes require a full power cycle to take effect. | • **Supported**<br>• Disabled |

### 3.3.4.1 Power and Performance

The Power & Performance menu allows the user to specify a profile that is optimized in the direction of either reduced power consumption or increased performance.

To access this screen from the front page, select **Advanced Menu > CPU Configuration > Power & Performance**. Press the **<Esc>** key to return to the **CPU Configuration** screen.

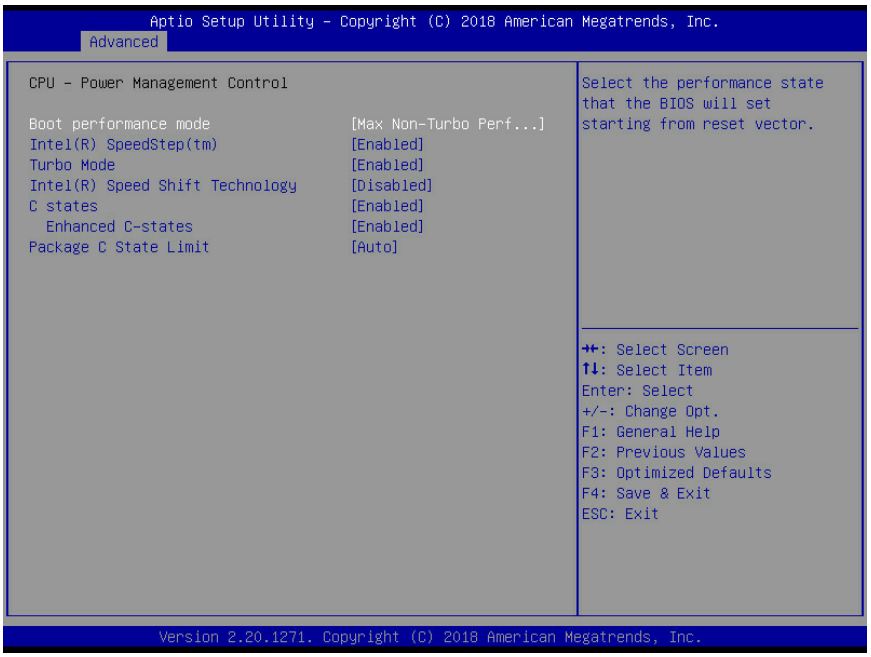



**Figure 13. Power and performance submenu**

**Table 12. Power and performance submenu options**

| Menu Item | Description | Values |
|---|---|---|
| **Boot performance Mode** | Select the performance state that the BIOS will set starting from the reset vector. | • **Max Non-Turbo Performance**<br>• Turbo Performance<br>• Max Battery |
| **Intel® SpeedStep** | Allows more than two frequency ranges to be supported.<br>Enhanced Intel SpeedStep® Technology allows the system to dynamically adjust processor voltage and core frequency, which can result in decreased average power consumption and decreased average heat production. | • **Enabled**<br>• Disabled |
| **Turbo Mode** | Enable/Disable processor Turbo Mode (requires Intel® SpeedStep or Intel® Speed Shift to be available and enabled).<br>Intel® Turbo Boost Technology allows the processor to automatically increase its frequency if it is running below power, temperature, and current specifications. | • **Enabled**<br>• Disabled |
| **Intel® Speed Shift Technology** | Enable/ Disable Intel® Speed Shift Technology support. Enabling will expose the OPPC v2 interface to allow for hardware controlled P-states. | • **Disabled**<br>• Enabled |
| **C states** | Enable/Disable CPU Power Management. Allows the CPU to go into C states when it's not 100% used. When enabled, CPU switches to minimum speed when all cores enter C state. | • **Enabled**<br>• Disabled |
| **Enhanced C-states** | Enable/Disable C1E. When enabled, CPU switches to minimum speed when all cores enter C state. | • **Enabled**<br>• Disabled |
| **Package C State Limit** | Maximum package C State Limit settings.<br>CPU Default: Factory default values.<br>Auto: Automatically selects the deepest available Package C State Limit. | • **Auto**<br>• C0<br>• C1<br>• C2<br>• C3<br>• C6<br>• C7<br>• C8<br>• CPU Default |

### 3.3.5 Server ME Configuration

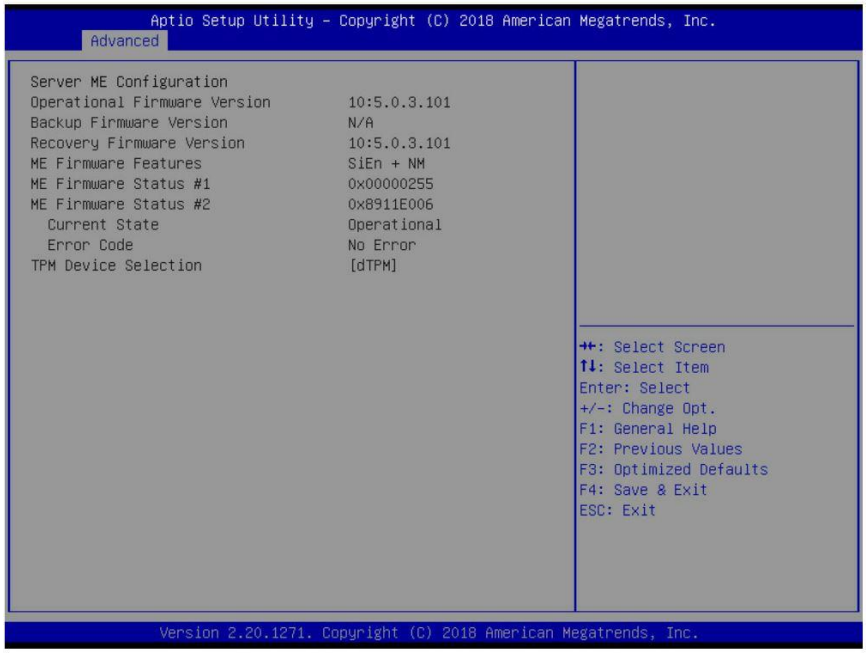



**Figure 14. Server ME configuration menu**

**Table 13. Server ME configuration menu options**

| Menu Item | Description |
|---|---|
| **Server ME Configuration** | Read only. |

### 3.3.6 ACPI Settings

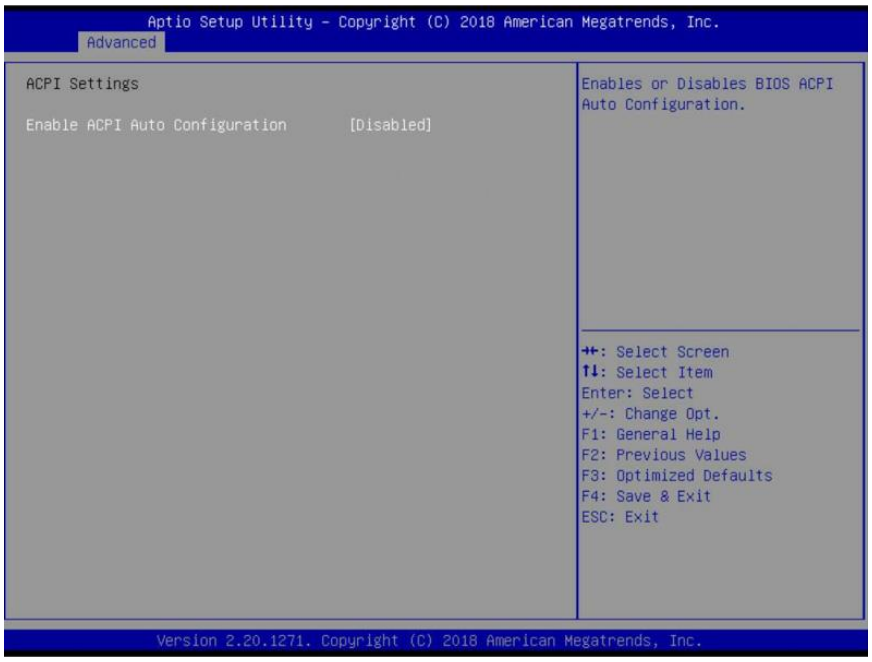



**Figure 15. ACPI settings menu**

**Table 14. ACPI settings menu options**

| Menu Item | Description | Values |
|---|---|---|
| **Enable ACPI Auto Configuration** | Enables or disables BIOS ACPI Auto Configuration. | • **Disabled**<br>• Enabled |

### 3.3.7 Serial Port Console Redirection

The Console Redirection menu allows the user to enable or disable console redirection for remote system management, and to configure the connection options for this feature.

To access this screen from the front page, select **Advanced Menu** > **Console Redirection**. Press the **<Esc>** key to return to the Server Management screen.

When console redirection is active, all POST and setup displays are in text mode. The text mode POST diagnostic screen is displayed regardless of the Quiet Boot setting. This is due to the limitations of console redirection, which is based on data terminal emulation using a serial data interface to transfer character data.

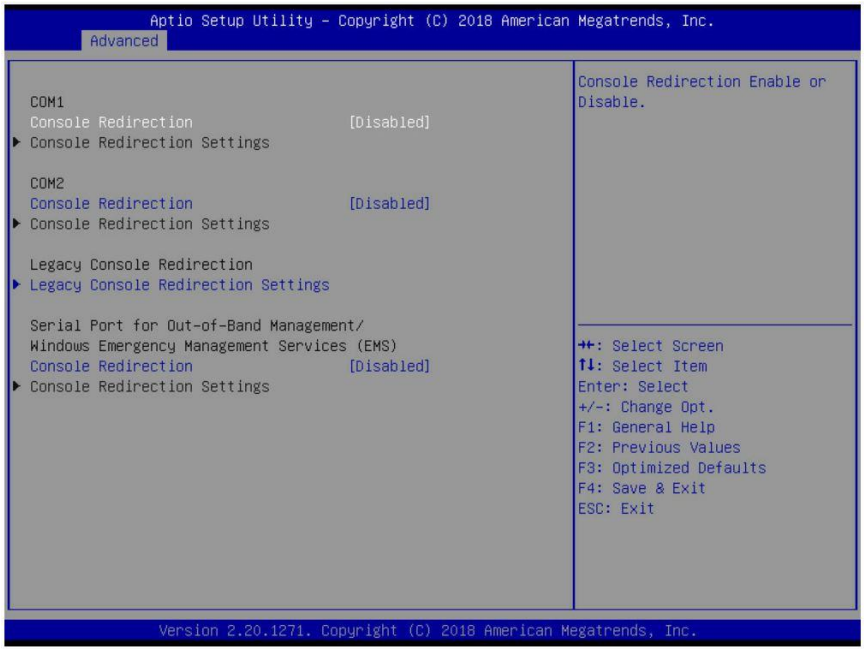



**Figure 16. Serial port console redirection menu**

**Table 15. Serial port console redirection menu options**

| Menu Item | Description | Values |
|---|---|---|
| **COM1 / COM2 / Serial Port for Out-of-Band Management/Windows Emergency Services (EMS) Console Redirection** | Enable or disable console redirection. | • **Disabled**<br>• Enabled |
| **Legacy Console Redirection Settings** | Legacy Console redirection settings. | Submenu |
| **Console Redirection Settings** | The Console Redirection Settings specify how the host computer (that the user is using) exchanges data. Both computers should have the same or compatible settings. | Submenu |

### 3.3.7.1 COM1 / COM2 Console Redirection Settings

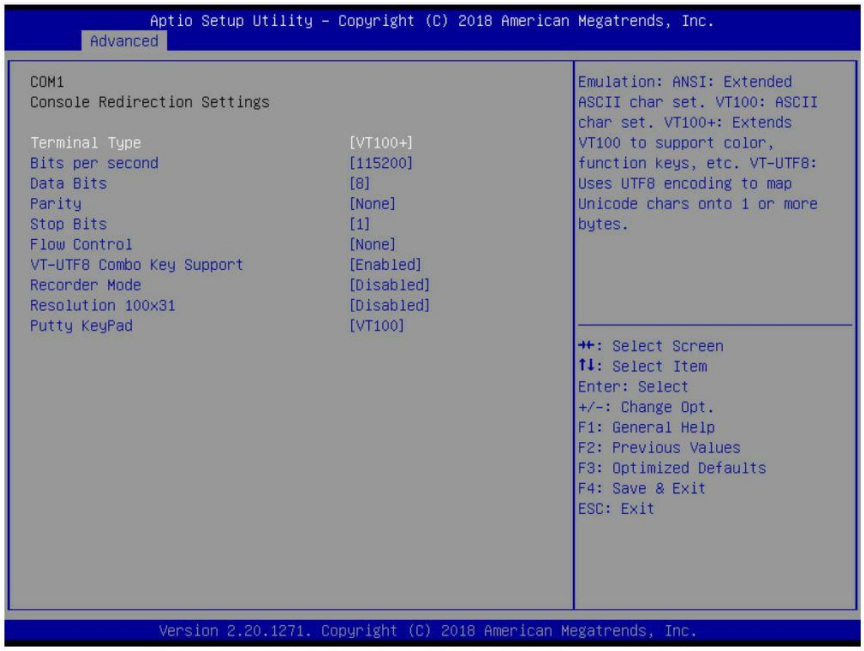



**Figure 17. COM1/COM2 console redirection settings submenu**

**Table 16. COM1/COM2 console redirection settings submenu options**

| Menu Item | Description | Values |
|---|---|---|
| **Terminal Type** | • Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set.<br>• VT100+: Extends VT100 to support color, function keys, etc.<br>• VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.<br>The VT100 and VT100+ terminal emulations are essentially the same. VT-UTF8 is a UTF8 encoding of VT100+. | • **VT100+**<br>• VT100<br>• VT-UTF8<br>• ANSI |
| **Bits per Second** | Select serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds. | • **115200**<br>• 9600<br>• 19200<br>• 38400<br>• 57600 |
| **Data Bits** | | • **8**<br>• 7 |
| **Parity** | A parity bit can be sent with the data bits to detect some transmission errors.<br>• Even: parity bit is 0 if the num of 1's in the data bits is even.<br>• Odd: parity bit is 0 if the num of 1's in the data bits is odd.<br>• Mark: parity bit is always 1.<br>• Space: parity bit is always 0. Mark and Space parity do not allow for error detection. | • **None**<br>• Even<br>• Odd<br>• Mark<br>• Space |
| **Stop Bits** | Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit. | • **1**<br>• 2 |
| **Flow Control** | Flow Control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to restart the flow. Hardware flow control uses two wires to send start/stop signal.<br>Flow control is necessary only when there is a possibility of data overrun. In that case, the Request to Send/Clear to Send (RTS/CTS) hardware handshake is a relatively conservative protocol that can usually be configured at both ends. | • **None**<br>• Hardware RTS<br>• CTS |

| Menu Item | Description | Values |
|---|---|---|
| **VT-UTF8 Combo Key Support** | Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals. | • **Enabled**<br>• Disabled |
| **Recorder Mode** | On this mode enabled only text will be sent. This is to capture Terminal data. | • **Disabled**<br>• Enabled |
| **Resolution 100x31** | Enable or disable extended terminal resolution. | • **Disabled**<br>• Enabled |
| **Putty KeyPad** | Select FunctionKey and KeyPad on Putty. | • **VT100**<br>• LINUX<br>• XTERMR6<br>• SCO<br>• ESCN<br>• VT400 |

### 3.3.7.2 Legacy Console Redirection Settings

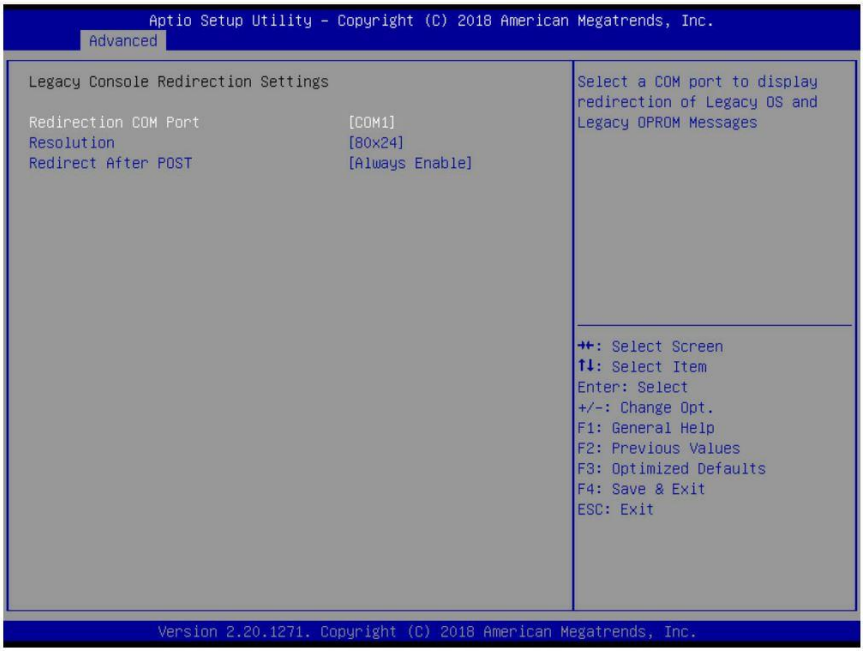



**Figure 18. Legacy console redirection settings submenu**

**Table 17. Legacy console redirection settings submenu options**

| Menu Item | Description | Values |
|---|---|---|
| **Redirection COM Port** | Select a COM port to display redirection of the legacy OS and legacy OPROM Messages. | • **COM1**<br>• COM2 |
| **Resolution** | On the legacy OS, the Number of Rows and Columns supported in redirection. | • **80x24**<br>• 80x25 |
| **Redirect After POST** | When Bootloader is selected, legacy Console Redirection is disabled before booting to the legacy OS. When Always Enable is selected, then legacy Console Redirection is enabled for the legacy OS. The default setting for this option is set to Always Enable. | • **Always Enable**<br>• BootLoader |

### 3.3.7.3 Serial Port for Out-of-Band Management Console Redirection Settings

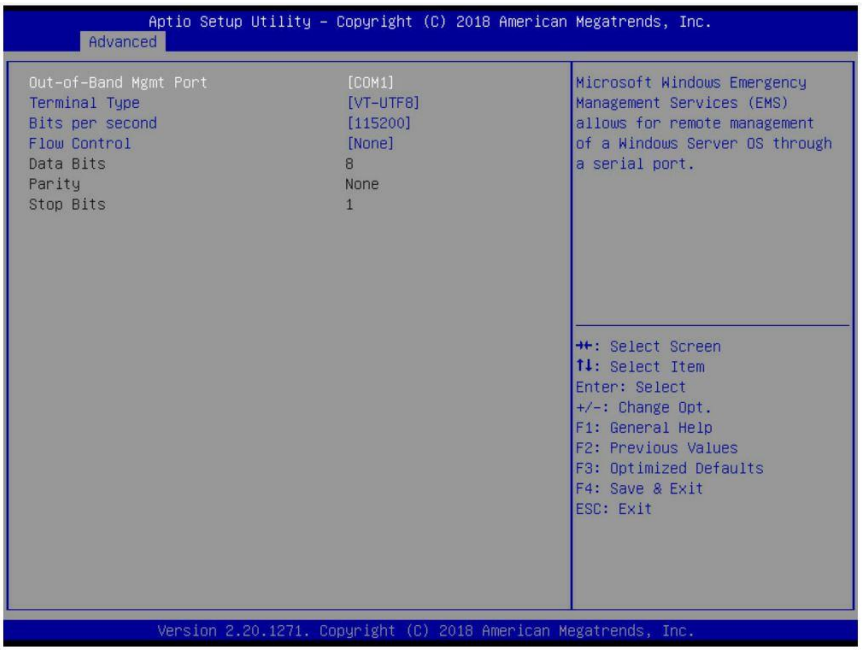



**Figure 19. Serial port for out-of-band management console redirection settings submenu**

**Table 18. Serial port for out-of-band management console redirection settings submenu options**

| Menu Item | Description | Values |
|---|---|---|
| **Out-of-Band Mgmt Port** | Microsoft* Windows Emergency Management Services (EMS) allows for remote management of a Windows Server OS through a serial port. | • **COM1**<br>• COM2 |
| **Terminal Type** | VT-UTF8 is the preferred terminal type for out-of-band management. The next best choice is VT100+ and then VT100. See above, in Console Redirection Settings page, for more Help with Terminal Type/Emulation. | • **VT-UTF8**<br>• VT100<br>• VT100+<br>• ANSI |
| **Bits per Second** | Select serial port transmission speed. The speed must be matched on the other device. Long or noisy lines may require lower speeds. | • **115200**<br>• 9600<br>• 19200<br>• 57600 |
| **Flow Control** | Flow Control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a stop signal can be sent to stop the data flow. Once the buffers are empty, a start signal can be sent to restart the flow. Hardware flow control uses two wires to send start/stop a signal. | • **None**<br>• Hardware RTS<br>• CTS<br>• Software Xon/Xoff |
| **Data Bits / Parity / Stop Bits** | Read only. | |

### 3.3.8 PCIe* Subsystem Settings

The PCIe* Subsystem Settings menu allows the user to configure the available USB controller options.

To access this screen from the front page, select **Advanced > PCI Devices Common Settings**. Press the **<Esc>** key to return to the **Advanced** menu.

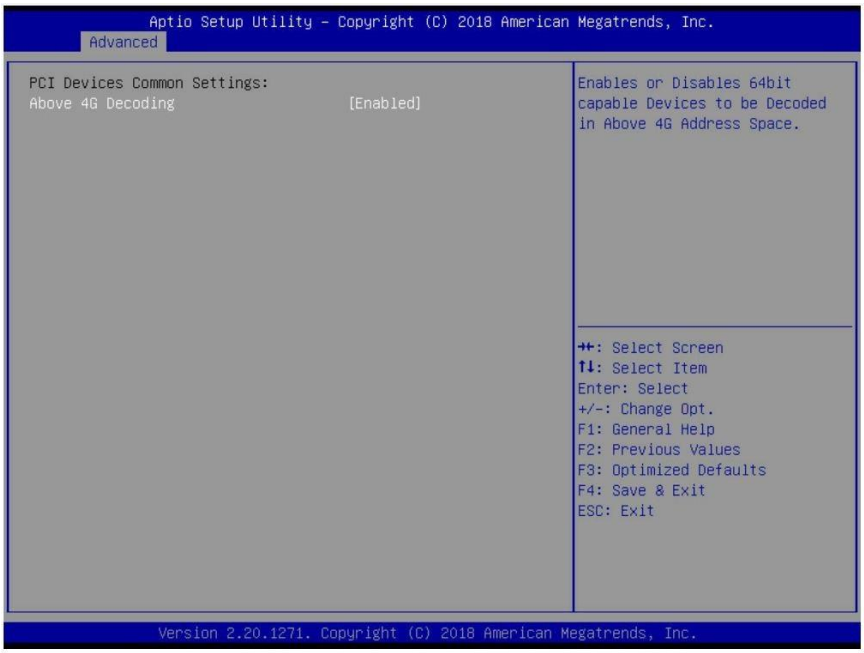



**Figure 20. PCIe* subsystem settings menu**

**Table 19. PCIe* subsystem settings menu options**

| Menu Item | Description | Values |
|---|---|---|
| **Above 4G Decoding** | Enables or Disables 64-bit capable Devices to be Decoded in Above 4G Address Space. | • **Enabled**<br>• Disabled |

### 3.3.9 Network Stack Configuration

The Network Stack menu configures the network interface card (NIC) controller options for BIOS POST. This menu handles the built-in network controllers on the server board. It does not configure or report anything related to network adapter cards.

To access this screen from the front page, select **Advanced Menu > Network Stack Configuration**. Press the **<Esc>** key to return to the **Advanced** menu.

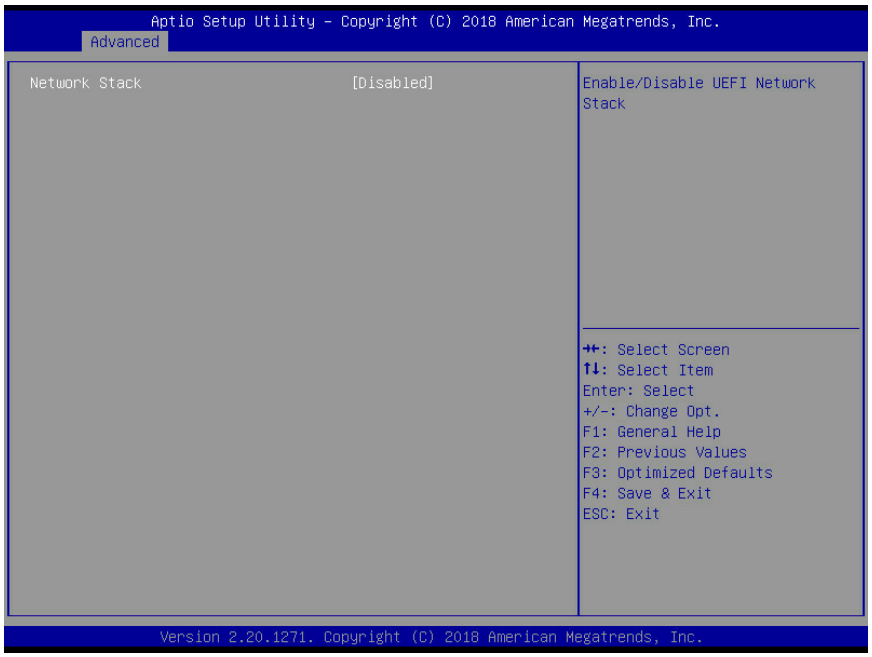



**Figure 21. Network stack configuration menu**

**Note:** The BIOS will automatically read the onboard LAN controller.

**Table 20. Network stack configuration menu options**

| Menu Item | Description | Values |
|---|---|---|
| **Network Stack** | Enable/Disable UEFI Network Stack. | • **Disabled**<br>• Enabled |
| **If Network Stack is set to Enabled** | | |
| **Ipv4 PXE Support** | Enable Ipv4 PXE Boot Support. If disabled the IPV4 PXE boot option is not created. | • **Disabled**<br>• Enabled |
| **Ipv4 HTTP Support** | Enable Ipv4 HTTP Boot Support. If disabled the IPV4 HTTP boot option is not created. | • **Disabled**<br>• Enabled |
| **Ipv6 PXE Support** | Enable Ipv6 PXE Boot Support. If disabled the IPV6 PXE boot option is not created. | • **Disabled**<br>• Enabled |
| **Ipv6 HTTP Support** | Read only. | |
| **PXE boot wait time** | Enable Ipv6 HTTP Boot Support. If disabled the IPV6 HTTP boot option is not created. | • **0** |
| **Media detect count** | The number of times the presence of media is checked. | • **1** |

### 3.3.10 Compatibility Support Mode (CSM) Configuration

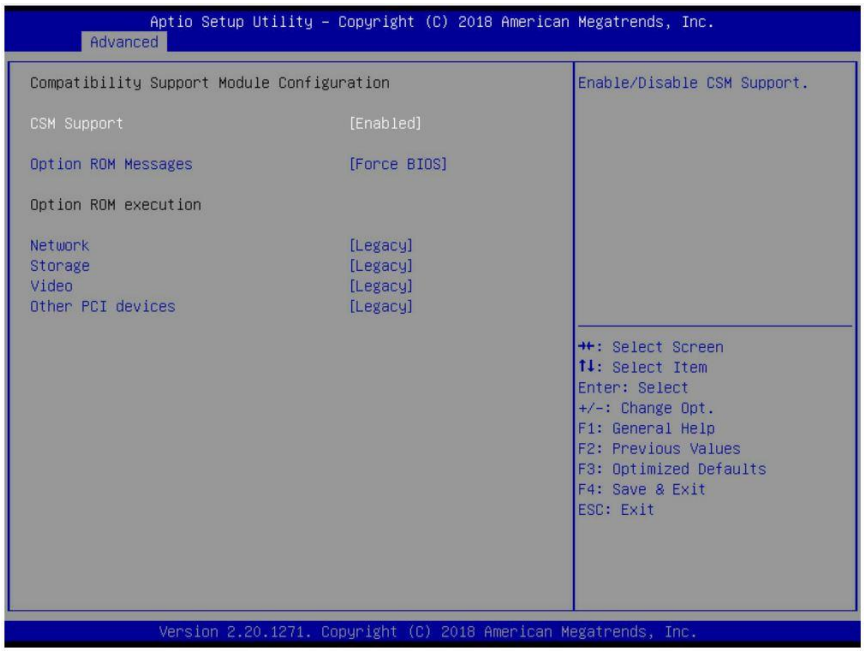



**Figure 22. CSM configuration menu**

**Table 21. CSM configuration menu options**

| Menu Item | Description | Values |
|---|---|---|
| **CSM Support** | Enable/Disable CSM Support. | • **Enabled**<br>• Disabled |
| **Option ROM Messages** | Set the display mode for the Option ROM. | • **Force BIOS**<br>• Keep Current |
| **Network** | Controls the execution of UEFI and Legacy PXE OpROM. | • **Legacy**<br>• UEFI |
| **Storage** | Controls the execution of UEFI and Legacy Storage OpROM. | • **Legacy**<br>• UEFI |
| **Video** | Controls the execution of UEFI and Legacy Video OpROM. | • **Legacy**<br>• UEFI |
| **Other PCI Devices** | Determines OpROM execution policy for devices other than Network, Storage, or Video. | • **Legacy**<br>• UEFI |
| **Media detect count** | The number of times presence of media is checked. | • **Legacy**<br>• UEFI |

### 3.3.11 USB Configuration

The USB Configuration menu allows the user to configure the available USB controller options.

To access this screen from the front page, select **Advanced** > **USB Configuration**. Press the **<Esc>** key to return to the **Advanced** menu.

This screen displays all USB mass storage devices that have been detected in the system. These include USB-attached hard disk drives (HDDs), floppy disk drives (FDDs), CD-ROM and DVD-ROM drives, and USB flash memory devices (such as s USB key or key fob).

**Note**: USB devices can be hot plugged during POST, and are detected, enumerated, and work under OS environment. They are NOT displayed on this screen or enumerated as bootable devices.

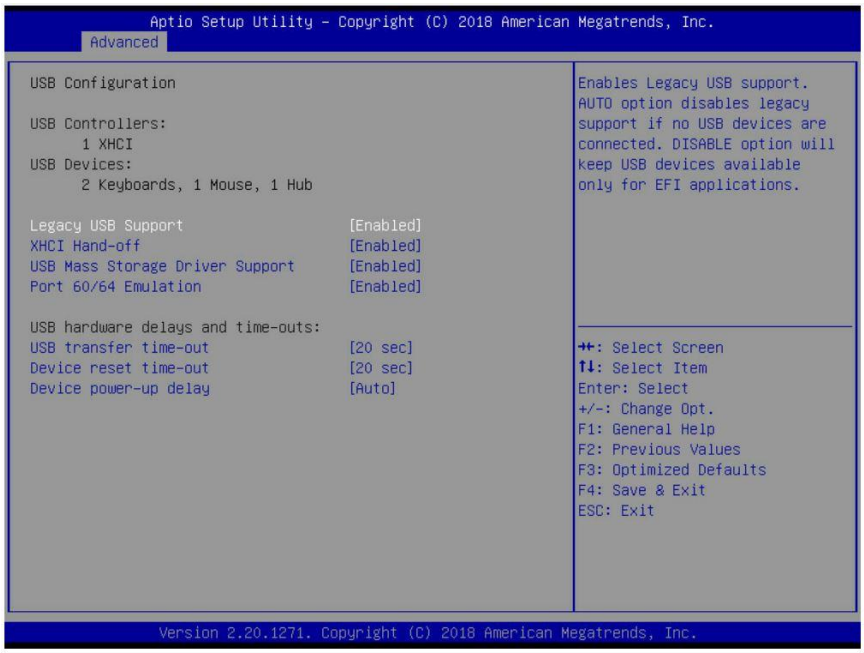



**Figure 23. USB configuration menu**

**Table 22. USB configuration menu options**

| Menu Item | Description | Values |
|---|---|---|
| **USB Controllers / USB Devices** | Read only. | |
| **Legacy USB Support** | Enables Legacy USB support. The **Auto** option disables legacy support if no USB devices are connected, while the **Disable** option only keeps USB Keyboard devices available for EFI applications.<br>If the USB controller setting is disabled, this field is grayed out and inactive. | • **Enabled**<br>• Disabled<br>• Auto |
| **XHCI Hand-off** | This is a workaround for an OS without XHCI hand-off support. The XHCI ownership change should be claimed by the XHCI driver. | • **Enabled**<br>• Disabled |
| **USB Mass Storage Driver Support** | Enable/Disable USB Mass Storage Driver support. | • **Enabled**<br>• Disabled |
| **Port 60/64 Emulation** | Enables I/O Port 60h/64h emulation support. This should be enabled for the complete USB keyboard legacy support for a non-USB aware OS. | • **Enabled**<br>• Disabled |
| **USB transfer time-out** | The time-out value for Control, Bulk and Interrupt transfers. | • **20 sec**<br>• 1 sec<br>• 5 sec<br>• 10 sec |

| Menu Item | Description | Values |
|---|---|---|
| **Device reset time-out** | This option controls the USB mass storage device Start Unit command time-out.<br>Setting the time-out to a larger value provides more time for a mass storage device to be ready, if needed. | • **20 sec**<br>• 10 sec<br>• 30 sec<br>• 40 sec |
| **Device power-up delay** | The maximum time the device will take before it properly reports itself to the Host Controller.<br>**Auto** uses the default value: 100 ms for a root port. For a Hub port, the delay is taken from the Hub descriptor. | • **Auto**<br>• Manual |

### 3.3.12 Onboard Device Configuration

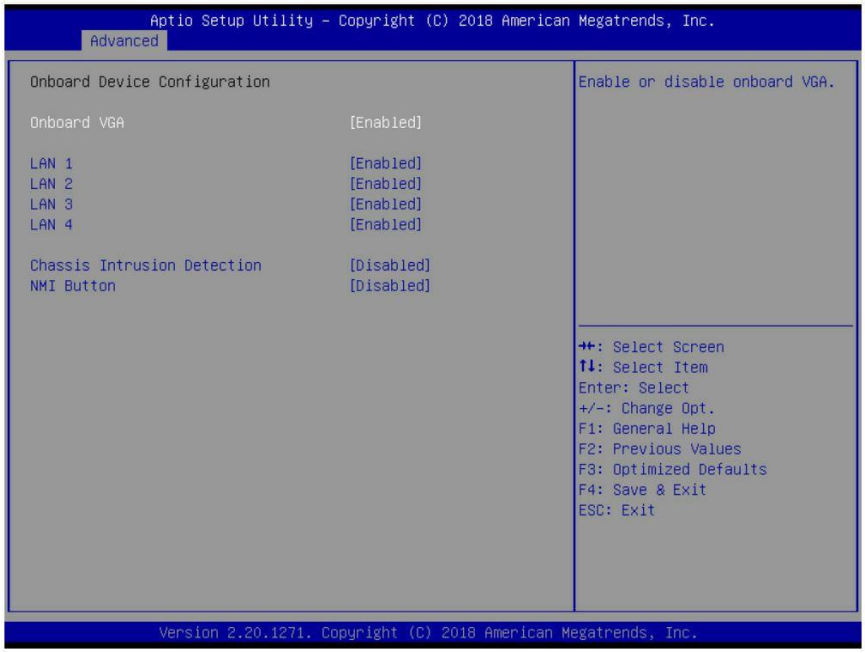



**Figure 24. Onboard device configuration menu**

**Note:** The BIOS automatically reads the onboard LAN controller.

**Table 23. Onboard device configuration menu options**

| Menu Item | Description | Values |
|---|---|---|
| **Onboard VGA** | Enable or disable onboard VGA. | • **Enabled**<br>• Disabled |
| **LAN1 / LAN2** | LAN Enable/Disable control function. | • **Enabled**<br>• Disabled |
| **LAN3 / LAN4** | LAN Enable/Disable control function. | • **Enabled**<br>• Disabled |
| **Chassis Intrusion Detection** | Enabled: when a chassis intrusion event is detected, the BIOS records the event. | • **Disabled**<br>• Enabled |
| **NMI Button** | Enable or Disable NMI button. | • **Disabled**<br>• Enabled |

### 3.3.13 S5 RTC Wake Settings

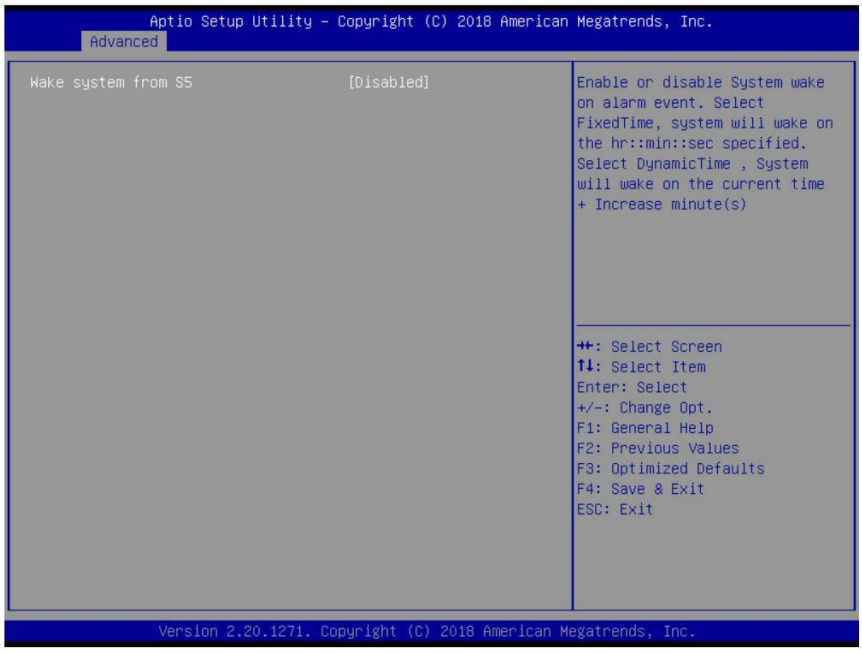



**Figure 25. S5 RTC wake settings menu**

**Table 24. S5 RTC wake settings menu options**

| Menu Item | Description | Values |
|---|---|---|
| **Wake system from S5** | Enable or disable System wake on an alarm event.<br>Fixed Time: the system wakes on the hr:min:sec specified.<br>Dynamic Time: the system wakes on the current time and an increase minute(s). | • **Disabled**<br>• Fixed Time<br>• Dynamic Time |
| **Wake system from S5 (when set to [Fixed time])**<br>**Wake up hour** | Select 0–23.<br>Ex: Enter 3 for 3am and 15 for 3pm. | • **0–23** |
| **Wake up minute** | Select 0–59. | • **0–59** |
| **Wake up second** | Select 0–59. | • **0–59** |
| **Wake system from S5 (when set to [Dynamic time])**<br>**Wake up minute increase** | Select 1–5. | • **1–5** |

### 3.3.14 Super IO Configuration

The Super IO Configuration menu allows the user to configure Serial Port 1 and view the health and sensor readouts of the server board.

To access this menu from the front page, select **Advanced** > **Super IO Configuration**. Press the **<Esc>** key to return to the **Advanced** menu.

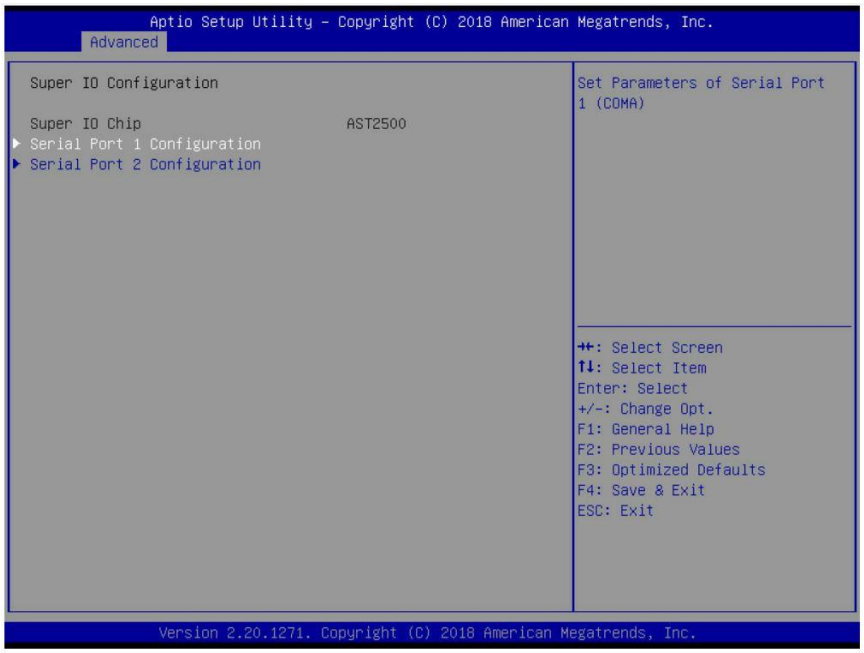



**Figure 26. Super IO configuration menu**

**Table 25. Super IO configuration menu options**

| Menu Item | Description |
|---|---|
| **Super IO Chip** | Read only. |

### 3.3.14.1 Serial Port 1 Configuration

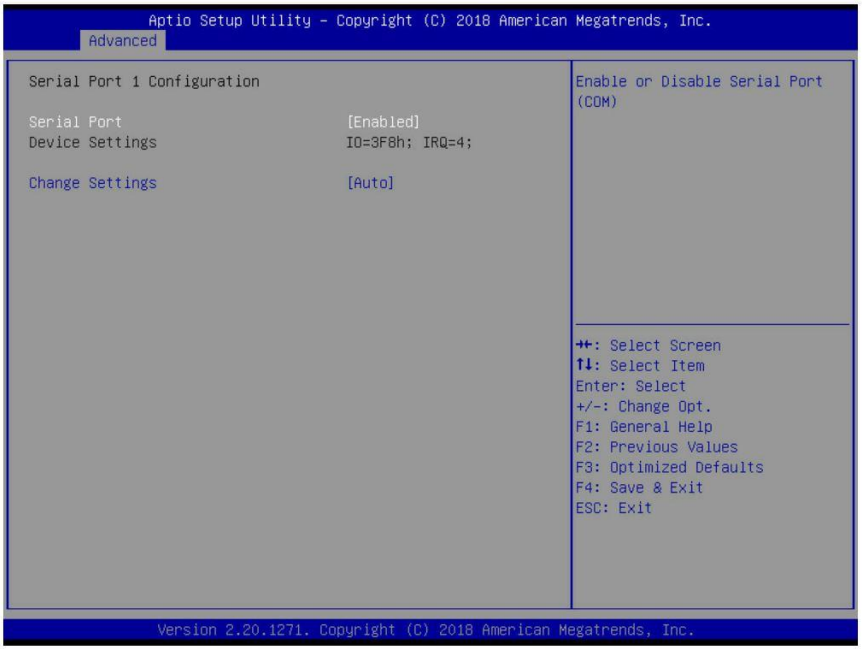



**Figure 27. Serial Port 1 configuration submenu**

**Table 26 Serial port 1 configuration submenu options**

| Menu Item | Description | Values |
|---|---|---|
| **Serial Port** | Enable or Disable Serial Port (COM). | • **Enabled**<br>• Disabled |
| **Device Settings** | Read only. | |
| **Change Settings** | Select an optimal setting for Super IO Device. | • **Auto**<br>• IO=3F8h; IRQ=4;<br>• IO=3F8h, IRQ=3, 4, 5, 6, 7, 10, 11, 12;<br>• IO=2F8h; IRQ=3, 4, 5, 6, 7, 10, 11, 12;<br>• IO=3E8h, IRQ=3, 4, 5, 6, 7, 10, 11, 12;<br>• IO=2E8h, IRQ=3, 4, 5, 6, 7, 10, 11, 12; |

### 3.3.15 Hardware Health Configuration

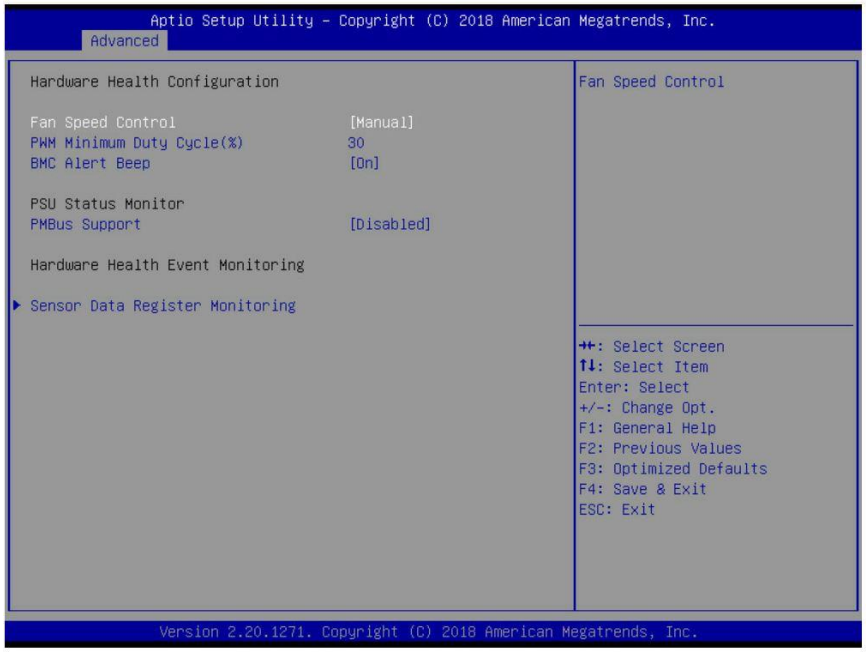



**Figure 28. Hardware health configuration**

**Table 27. Hardware health configuration menu options**

| Menu Item | Description | Values |
|---|---|---|
| **Fan Speed Control** | Fan Speed Control. | • **Manual**<br>• Full Speed |
| **PWM Minimum Duty Cycle (%)** | PWM Minimum Duty Cycle (%) | • **30** |
| **BMC Alert Beep** | Enable/Disable BMC Alert Beep. | • **On**<br>• Off |
| **PMBus Support** | PMBus Support. | • **Disabled**<br>• Enabled |

### 3.3.16 Sensor Data Register Monitoring

This is a read-only menu.

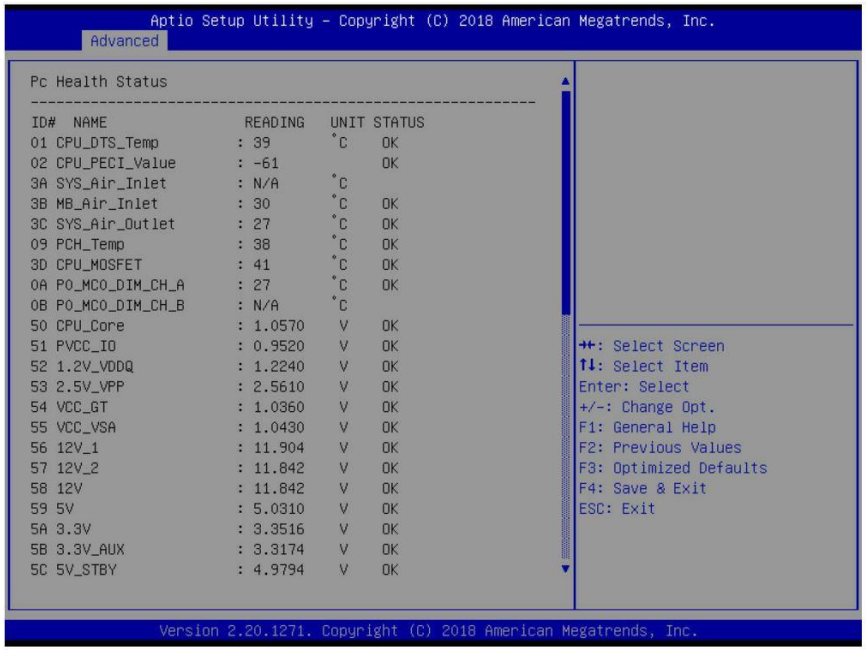



**Figure 29. Sensor data register monitoring menu**

# 4. Chipset Menus

The Chipset Configuration menu allows the user to configure options for memory, graphics, storage, PCIe* and other options, grouped in north bridge and south bridge functions.

To access the configuration screens, select either the North or South Bridge options by pressing **<↑>** or **<↓>** on the keyboard and then pressing the **<Enter>** key.

Configuration actions are performed on the selected menu and not directly on the Chipset menu.

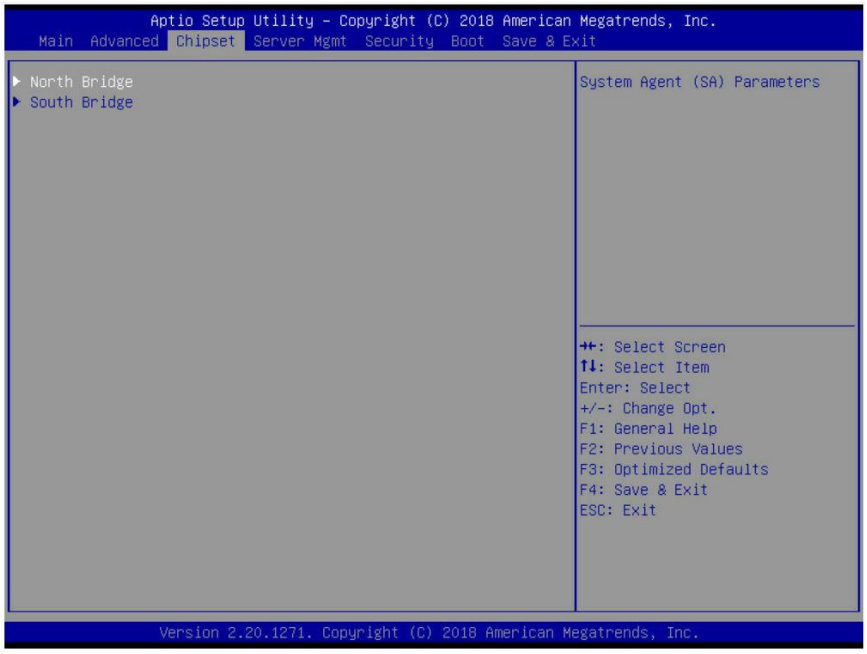



**Figure 30. Chipset menu**

**Table 28. Chipset menu options**

| Menu Item | Description | Values |
|---|---|---|
| **North Bridge** | System Agent (SA) Parameters. | Submenu |
| **South Bridge** | South Bridge Parameters. | Submenu |

## 4.1 North Bridge Configuration

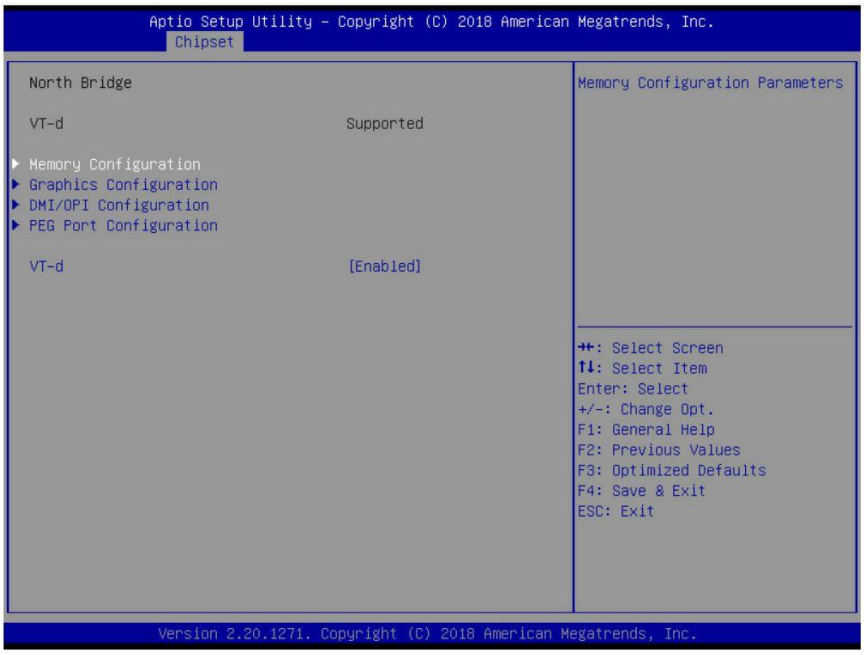



**Figure 31. North bridge configuration menu**

**Table 29. North bridge configuration menu options**

| Menu Item | Description | Values |
|---|---|---|
| **Memory Configuration** | Memory Configuration Parameters. | Submenu |
| **Graphics Configuration** | Graphics Configuration. | |
| **DMI/OPI Configuration** | Control various DMI functions. | |
| **PEG Port Configuration** | PEG Port Options. | |
| **VT-d** | VT-d capability. | • **Enabled**<br>• Disabled |

### 4.1.1 Memory Configuration

The Memory Configuration screen allows the user to view details about the DDR4 DIMMs that are installed as system memory, and configure memory frequency and ECC support. The installed memory information will vary depending on the specific system configuration. Figure 32 shows an example of the installed memory information.

This screen differs somewhat between different boards that have different memory configurations. Some boards have one processor socket and fewer DIMMs, while other boards have two sockets or four sockets, more DIMMs, and the boards may have RAS and performance options if configured for them.

To access this screen from the front page, select **Chipset** > **Memory Configuration**. Press the **<Esc>** key to return to the **Chipset** screen.

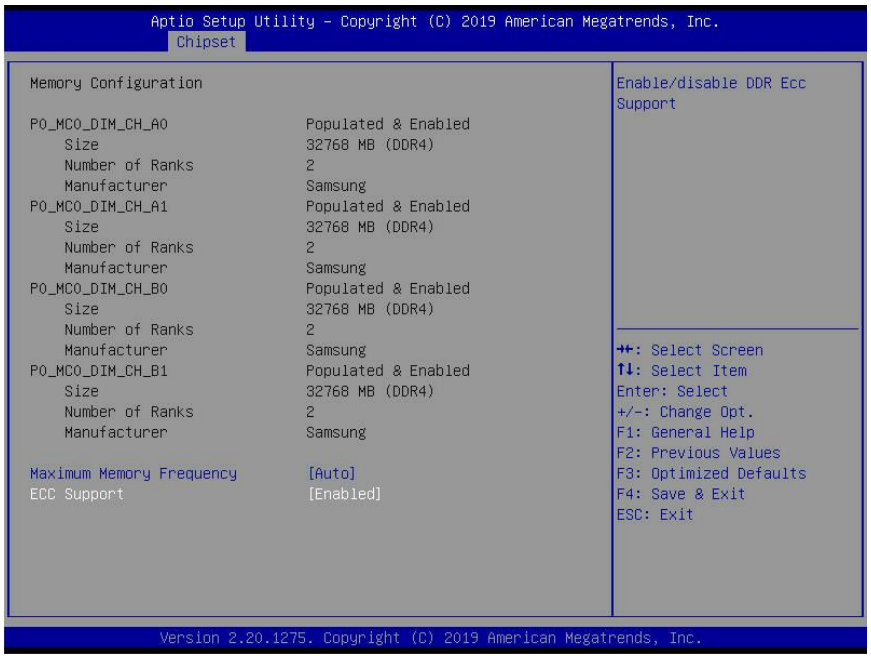



**Figure 32. Memory configuration submenu**

### 4.1.2 Graphics Configuration

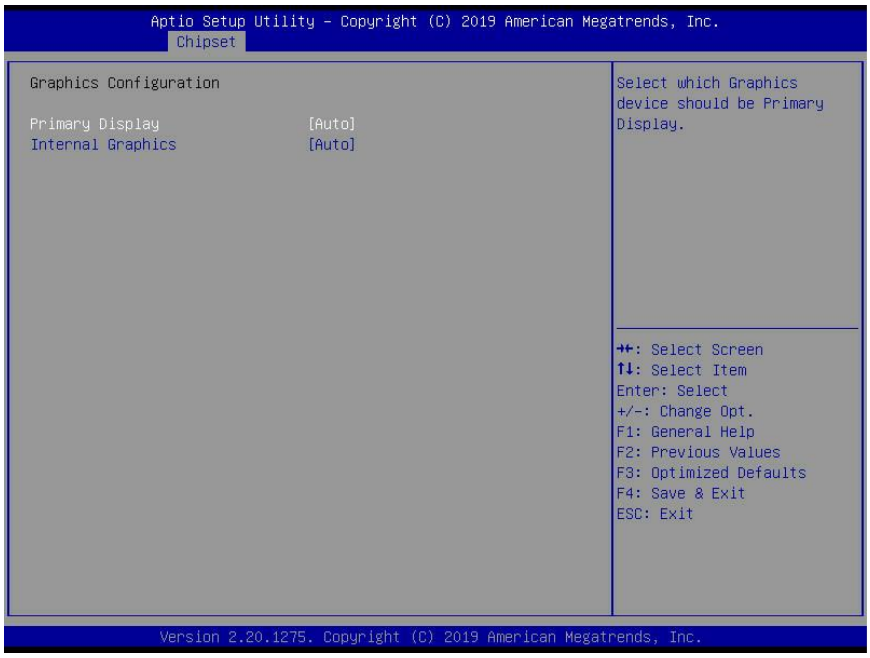



**Figure 33. Graphics configuration submenu**

**Table 30. Graphics configuration submenu options**

| Menu Item | Description | Values |
|---|---|---|
| **Primary Display** | Select which graphics device should be the primary display. | • **Auto**<br>• IGFX<br>• PEG<br>• PCH PCIe |
| **Internal Graphics** | Keep IGFX enabled based on the setup options. | • **Auto**<br>• Disabled<br>• Enabled |

### 4.1.3 DMI/OPI Configuration

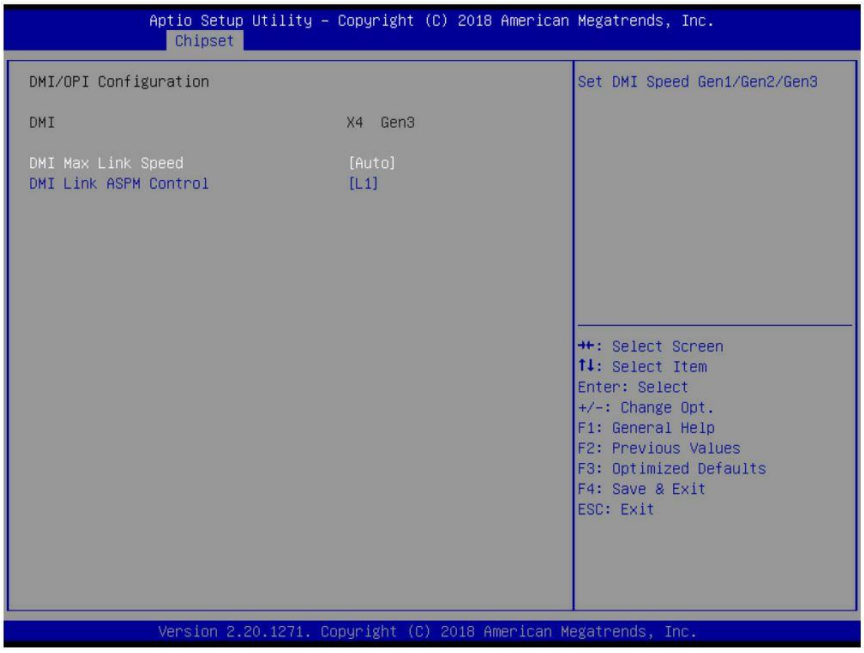



**Figure 34. DMI/OPI configuration submenu**

**Table 31. DMI/OPI configuration submenu options**

| Menu Item | Description | Values |
|---|---|---|
| **DMI Max Link Speed** | Set DMI Speed Gen1/Gen2/Gen3. | • **Auto**<br>• Gen1<br>• Gen2<br>• Gen3 |
| **DMI Link ASPM Control** | Enable/Disable the control of Active State Power Management on the SA side of the DMI Link. | • **L1**<br>• Disabled<br>• L0s<br>• L0sL1 |

### 4.1.4 PEG Port Configuration

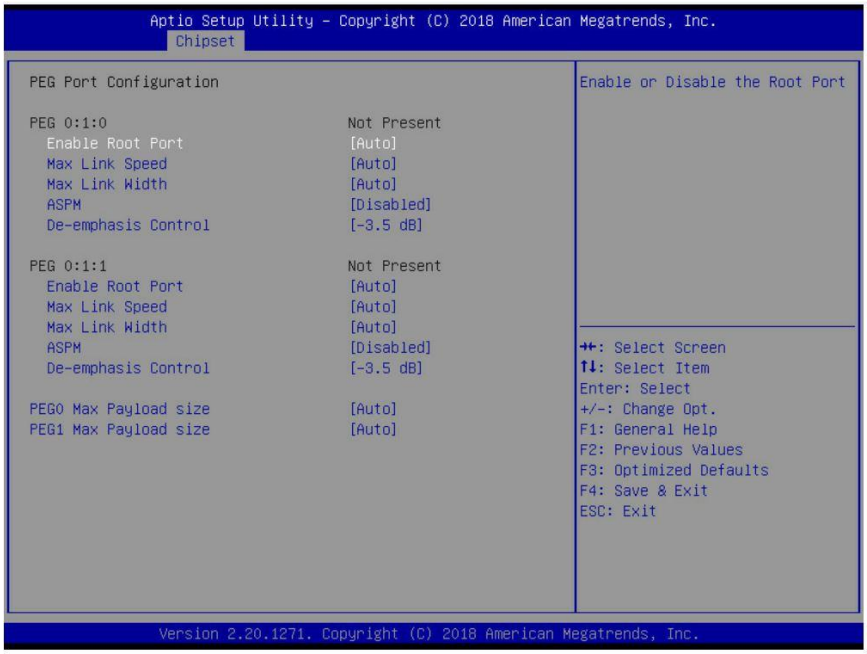



**Figure 35. PEG-port configuration submenu**

**Table 32. PEG-port configuration submenu options**

| Menu Item | Description | Values |
|---|---|---|
| **Enable Root Port** | Enable/Disable the root port. | • **Auto**<br>• Disabled<br>• Enabled |
| **Max Link Speed** | Configure the PEG 0:1:0 or PEG 0:1:1 maximum speed. | • **Auto**<br>• Gen1<br>• Gen2<br>• Gen3 |
| **Max Link Width** | Force the PEG link to retrain to x1/2/4/8. | • **Auto**<br>• Force x1<br>• Force x2<br>• Force x4<br>• Force x8 |
| **ASPM** | Control ASPM support for the PEG 0. This option does not affect the system if PEG is not the current active device. | • **Disabled**<br>• Auto<br>• ASPM L0s<br>• ASPM L1<br>• ASPM L0sL1 |
| **De-emphasis control** | PEG 0 or PEG-1: Configure the De-emphasis control on PEG. | • **-3.5 dB**<br>• -6 dB |
| **PEG0 Max Payload size** | Select PEG0 Max Payload Size; Choose **Auto** (Default Device Capability) or force to **128/256** Bytes. | • **Auto**<br>• 128<br>• 256 TLP |
| **PEG1 Max Payload size** | Select PEG1 Max Payload Size; Choose Auto (Default Device Capability) or force to **128/256** Bytes. | • **Auto**<br>• 128<br>• 256 TLP |

## 4.2 South Bridge Configuration

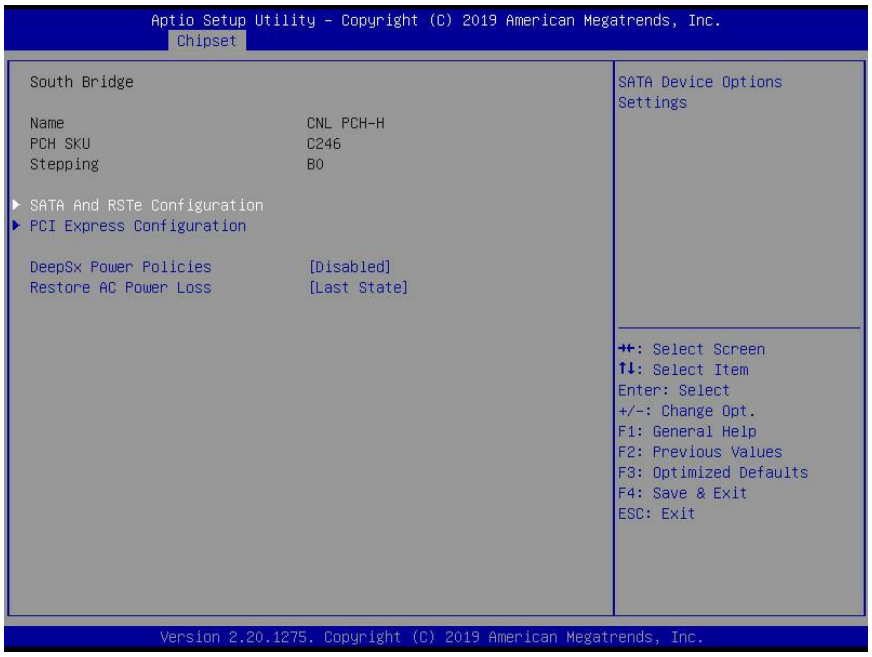



**Figure 36. South bridge configuration menu**

**Table 33. South bridge configuration menu options**

| Menu Item | Description | Values |
|---|---|---|
| **SATA And RSTe Configuration** | SATA Device Options Settings. | Submenu |
| **PCI Express Configuration** | **PCI Express Configuration settings.** | Submenu |
| **DeepSx Power Policies** | Configure DeepSx Mode. | • **Disabled**<br>• Enabled in S4-S5 |
| **Restore AC Power Loss** | Select AC power state when power is re-applied after a power failure. | • **Last State**<br>• Power Off<br>• Power On |

### 4.2.1 SATA and RSTe Configuration

The SATA and RSTe Configuration menu allows the user to configure the AHCI-capable controllers that are integrated into the server board on which the BIOS is executing. There are also informational displays of AHCI controller configuration and SATA drive information when applicable.

To access this screen from the front page, select **Chipset > SATA and RSTe Configuration**. Press the **<Esc>** key to return to the **Chipset** menu.

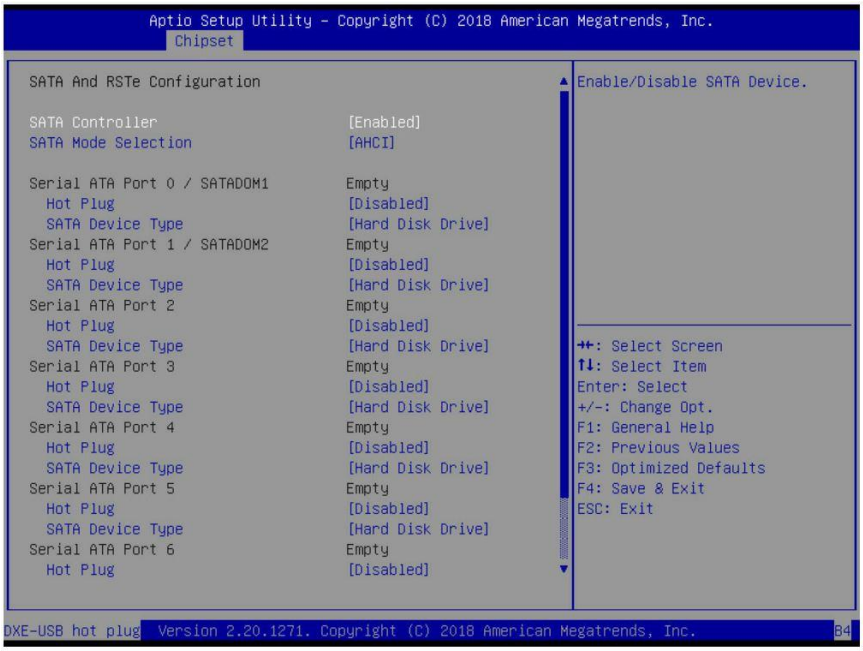



**Figure 37. SATA and RSTe configuration submenu**

**Table 34. SATA and RSTe configuration submenu options**

| Menu Item | Description | Values |
|---|---|---|
| **SATA Controller** | Enable/Disable SATA Device. | • **Enabled**<br>• Disabled |
| **SATA Mode Selection** | Determines how SATA controller(s) operate. | • **AHCI**<br>• RAID |
| Serial ATA Port 0 / SATADOM1 / Serial ATA Port 1 / SATADOM2 / Serial ATA Port 2 / Serial ATA Port 3 / Serial ATA Port 4 / Serial ATA Port 5 | Read only. | |
| Serial ATA Port 6 / Serial ATA Port 7 | Read only. | |
| **Hot Plug** | Designates this port as Hot Pluggable. | • **Disabled**<br>• Enabled |
| **SATA Device Type** | Identify the SATA port is connected to Solid State Drive or Hard Disk Drive. | • **Hard Disk Drive**<br>• Solid State Drive |

### 4.2.2 PCI Express Configuration

The PCI Configuration screen allows the user to configure the PCI memory space used for onboard and add-in adapters for each specific PCIe* port. To access this screen from the front page, select **Chipset** > **South Bridge Configuration -> PCI Configuration**. Press the **<Esc>** key to return to the Advanced screen.

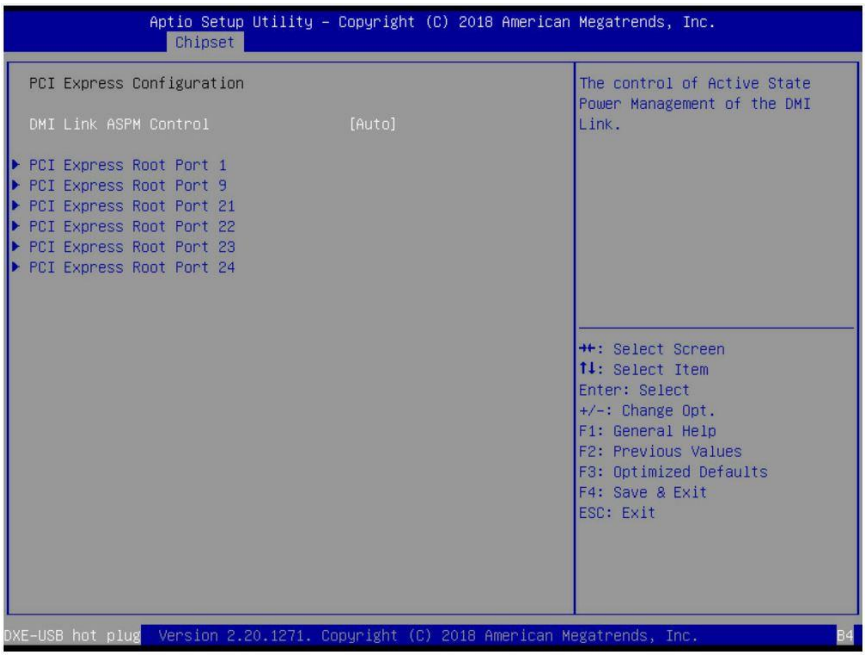



**Figure 38. PCIe* configuration submenu**

**Table 35. PCIe* configuration submenu**

| Menu Item | Description | Values |
|---|---|---|
| **DMI Link ASPM Control** | Control over the Active State Power Management of the DMI link. | • **Auto**<br>• Disabled<br>• L0s<br>• L1<br>• L0sL1 |
| **PCI Express Root Port 1 / 9 / 21 / 22 / 23 / 24** | PCI Express Root Port settings. | Submenu |

#### 4.2.2.1 PCI Express Root Port

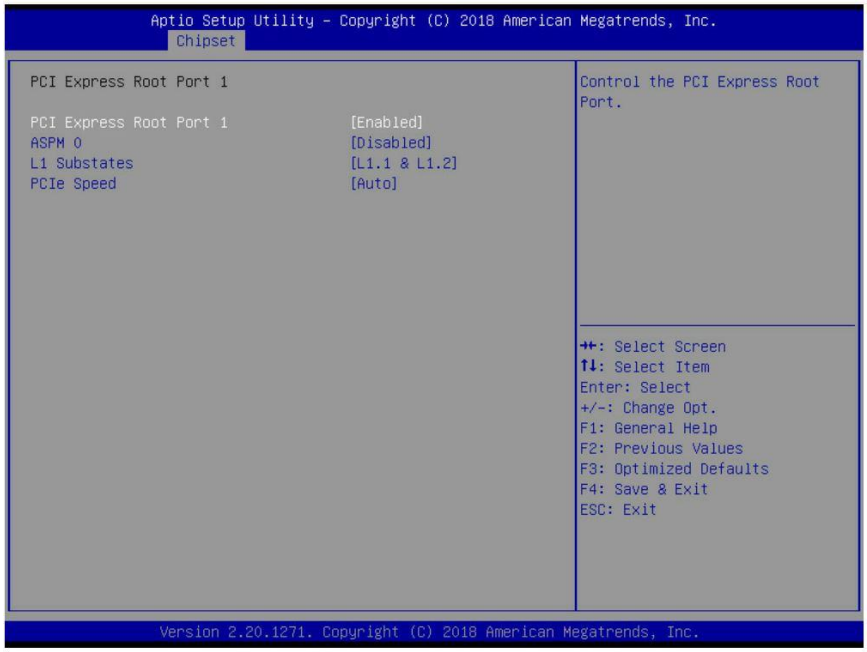



**Figure 39. PCIe* root port submenu**

**Table 36. PCIe* root port submenu options**

| Menu Item | Description | Values |
|---|---|---|
| **PCI Express Root Port 1** | Control the PCI Express Root Port | • **Enabled**<br>• Disabled |
| **ASPM 0** | Set the SPM Level:<br>• Force L0s: Force all links to L0s State<br>• Auto: BIOS auto configuration<br>• Disable: Disables ASPM | • **Disabled**<br>• L0s<br>• L1<br>• L0sL1<br>• Auto |
| **L1 Substates** | PCI Express L1 Substates settings | • **L1.1 & L1.2**<br>• Disabled<br>• L1.1 |
| **PCIe* Speed** | Configure PCIe* Speed. | • **Auto**<br>• Gen1<br>• Gen2<br>• Gen3 |

**Note:** All port submenus have common optons, the only difference being the number of the port listed.

# 5. Server Management

The Server Management menu allows the user to configure several server management features. This screen also provides an access point to the menus for setting FRB and watchdog timers, displaying system information, and controlling the BMC LAN configuration.

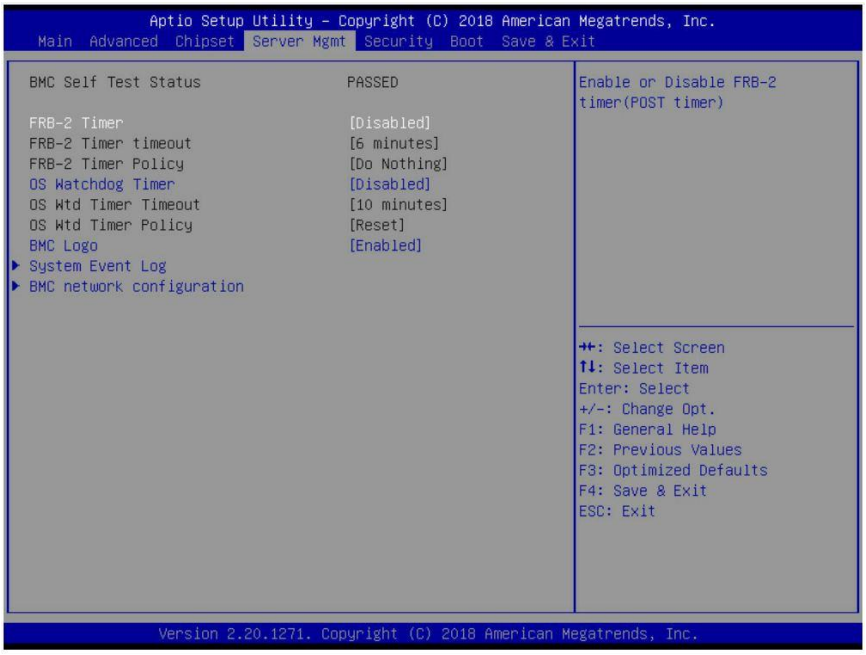



**Figure 40. Server management menu**

**Table 37. Server management menu options**

| Menu Item | Description | Values |
|---|---|---|
| **FRB-2 Timer** | Enable or Disable the FRB-2 timer (POST timer). | • **Enabled**<br>• Disabled |
| **FRB-2 Timer timeout** | Enter a value Between 3–6 min for the FRB-2 Timer Expiration value. | • **6 minutes**<br>• 3 minutes<br>• 4 minutes<br>• 5 minutes |
| **FRB-2 Timer Policy** | Configure how the system should respond if the FRB-2 Timer expires. Not available if FRB-2 Timer is disabled. | • **Do Nothing**<br>• Reset<br>• Power Down<br>• Power Cycle |
| **OS Watchdog Timer** | If enabled, starts a BIOS timer that can only be shut off by Management Software after the OS loads. Helps determine that the OS successfully loaded or follows the OS Boot Watchdog Timer policy. | • **Disabled**<br>• Enabled |
| **OS Wtd Timer timeout** | Configure how the system should respond if the FRB-2 Timer expires. Not available if FRB-2 Timer is disabled. | • **10 minutes**<br>• 5 minutes<br>• 15 minutes<br>• 20 minutes |
| **OS Wtd Timer Policy** | Configure the length of the OS Boot Watchdog Timer. Not available if OS Boot Watchdog timer is disabled. | • **Reset**<br>• Do Nothing<br>• Power Down<br>• Power Cycle |
| **BMC Logo** | Enable or Disable the BMC Logo. | • **Enabled**<br>• Disabled |
| **System Event Log** | Press <Enter> to change the SEL event log configuration. | Submenu |
| **BMC network configuration** | Configure BMC network parameters. | Submenu |

## 5.1 System Event Log

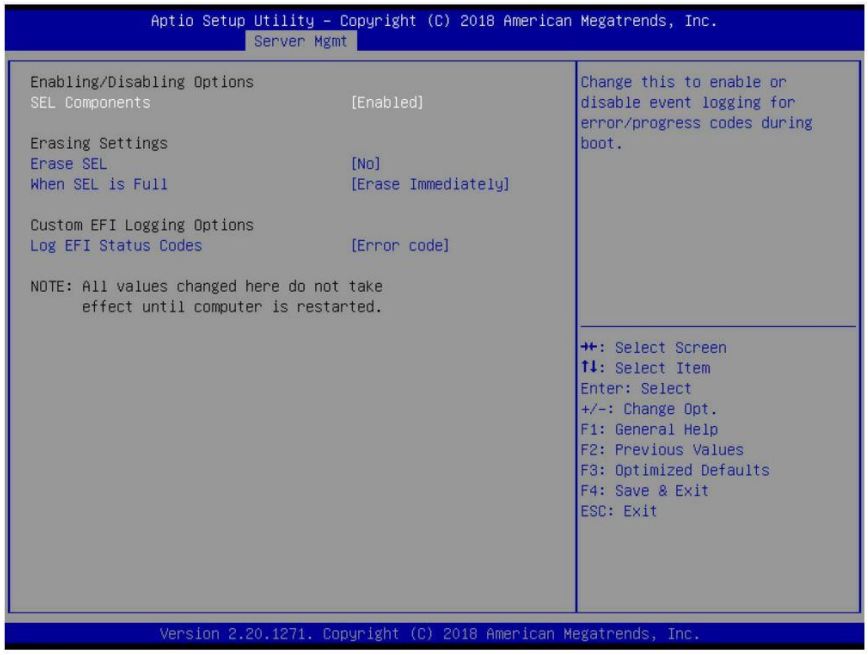



**Figure 41. System event log submenu**

**Note:** When **SEL Components** is set to **Disabled**, the options in this submenu are read only.

**Table 38. System event log submenu options**

| Menu Item | Description | Values |
|---|---|---|
| **SEL Components** | Enable or disable all features of System Event Logging during boot. | • **Enabled**<br>• Disabled |
| **Erase SEL** | Choose options for erasing the SEL. | • **No**<br>• Yes, on next reset<br>• Yes, on every reset |
| **When SEL is Full** | Choose options for reactions to a full SEL. | • **Erase Immediately**<br>• Do nothing |
| **Log EFI Status Codes** | Disable the logging of EFI Status Codes or log only error code or only progress code or both. | • **Error Code**<br>• Disabled<br>• Both<br>• Progress Code |

## 5.2 BMC Network Configuration

The BMC network configuration screen allows the user to configure the BMC baseboard LAN channel and a dedicated management LAN channel.

To access this screen from the front page, select **Server Management** > **BMC LAN Configuration**. Press the **<Esc>** key to return to the Server Management screen.

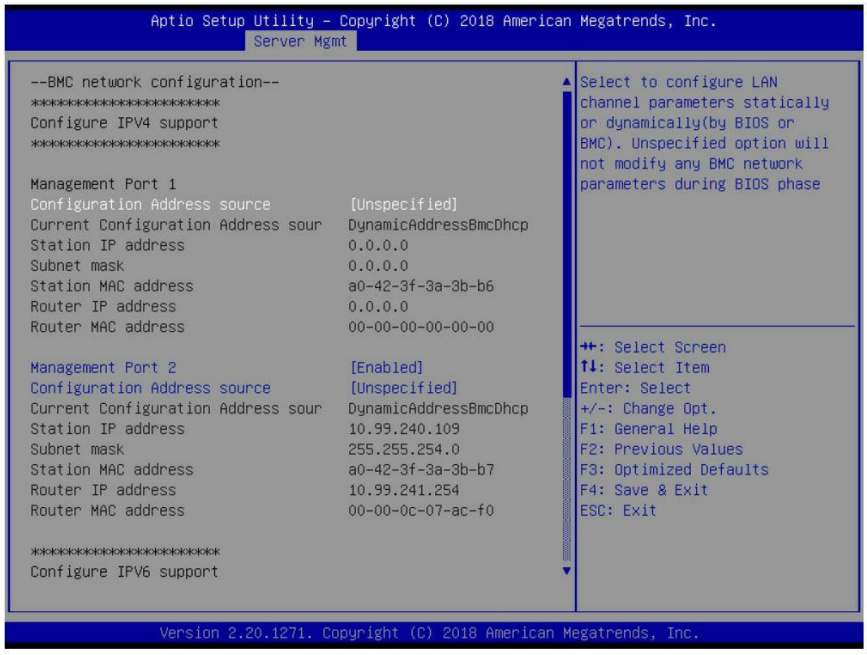



**Figure 42. BMC network configuration submenu**

**Table 39. BMC network configuration submenu options**

| Menu Item | Description | Values |
|---|---|---|
| **Configuration Address Source** | Select the configure LAN channel parameters statically or dynamically (by BIOS or BMC). The unspecified option will not modify any BMC network parameters during BIOS phase. | • **Unspecified**<br>• Static<br>• DynamicBmcDhcp<br>• DynamicBmcNonDhcp |
| **Server Management Port 2** | Enable/Disable BMC Share Nic. | • **Enabled**<br>• Disabled |
| **IPV6 Support** | Enable or Disable LAN1 IPV6 Support.<br>Option to Enable/Disable IPv6 addressing and any IPv6 network traffic on these channels.<br>If this option is set to Disabled, all other IPv6 fields are not visible. | • **Unspecified**<br>• Static<br>• DynamicBmcDhcp<br>• DynamicBmcNonDhcp |

# 6. Security

The Security screen allows the user to enable and set the administrator and user passwords. This BIOS supports (but does not require) strong passwords for security. The strong password criteria for both administrator and user passwords require that passwords be from 3 through 20 characters in length, and a password must contain at least one case-sensitive alphabetical character, one numeric character, and one special character.

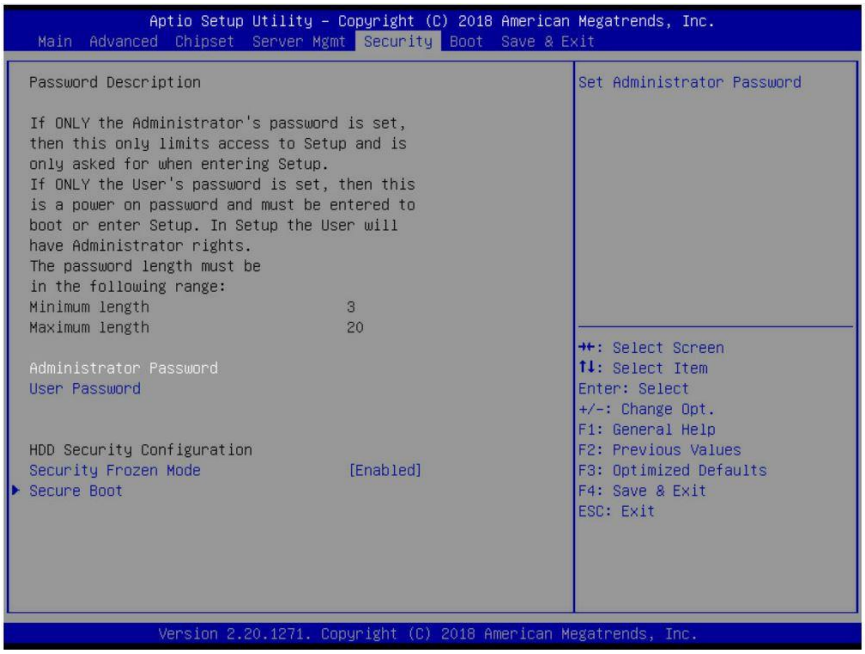



**Figure 43. Security menu**

**Table 40. Security menu options**

| Menu Item | Description | Values |
|---|---|---|
| **Administrator Password** | Set an administrator password in the **Create New Password** window.<br>After keying in the password, the **Confirm New Password** window will pop up to ask for confirmation | Set password |
| **User Password** | Set a user password in the **Create New Password** window.<br>After keying in the password, the **Confirm New Password** window will pop up to ask for confirmation | Set password |
| **Security Frozen Mode** | Enable or disable the HDD security freeze lock. Disable to support the secure erase function. | • **Enabled**<br>• Disabled |
| **Secure Boot** | Customizable Secure Boot settings. | Submenu |

## 6.1 Secure Boot

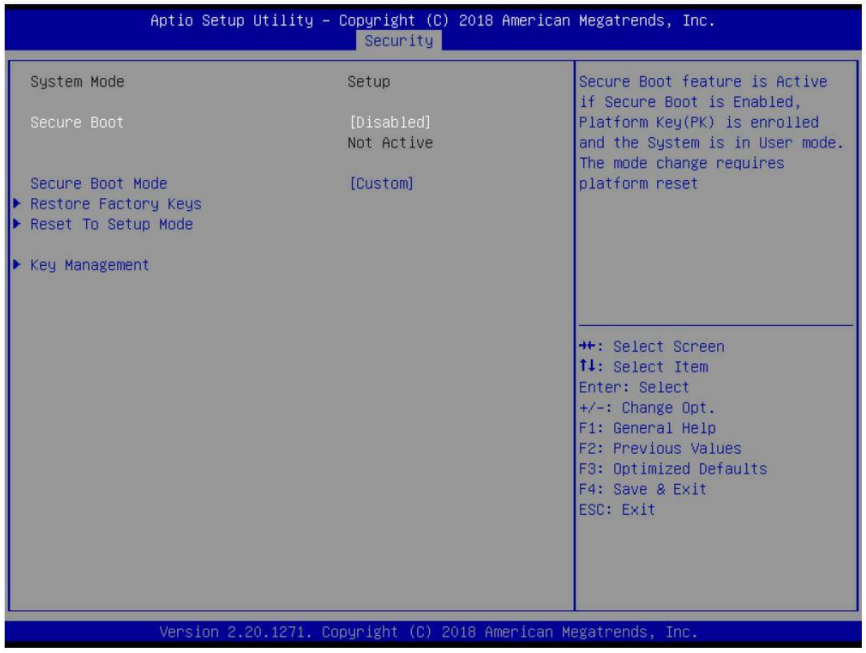



**Figure 44. Secure boot submenu**

**Table 41. Secure boot submenu options**

| Menu Item | Description | Values |
|---|---|---|
| **Secure Boot** | The Secure Boot feature is Active if Secure Boot is Enabled.<br>The Platform Key (PK) is enrolled and the System is in User mode. A mode change requires a system reset. | • **Disabled**<br>• Enabled |
| **Secure Boot Mode** | Secure Boot mode options: Standard or Custom.<br>In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication. | • **Custom**<br>• Standard |
| **Restore Factory Keys** | Force the system into User Mode. Install factory default Secure Boot key databases. | See description |
| **Reset to Setup Mode** | Delete all Secure Boot key databases from NVRAM. | See description |
| **Key Management** | Enables expert users to modify Secure Boot Policy variables without full authentication. | Submenu |

### 6.1.1 Restore Factory Keys

Upon selecting **Restore Factory Keys** a confirmation popup will appear. Press **Yes** to proceed and **No** to cancel.

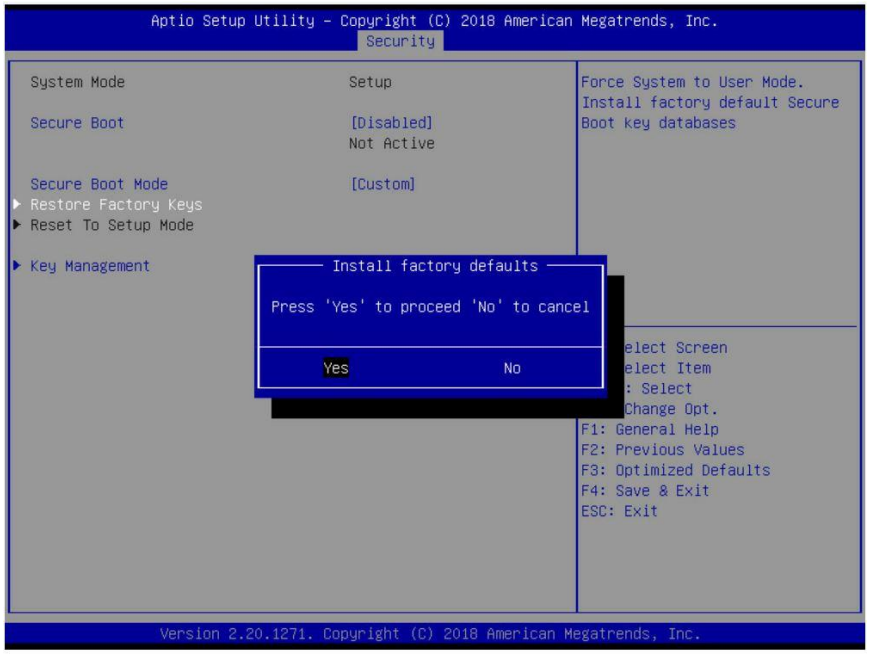



**Figure 45. Restore factory keys submenu**

### 6.1.2 Reset to Setup Mode

Upon selecting **Reset to Setup Mode** a confirmation popup will appear. Press **Yes** to proceed and **No** to cancel.

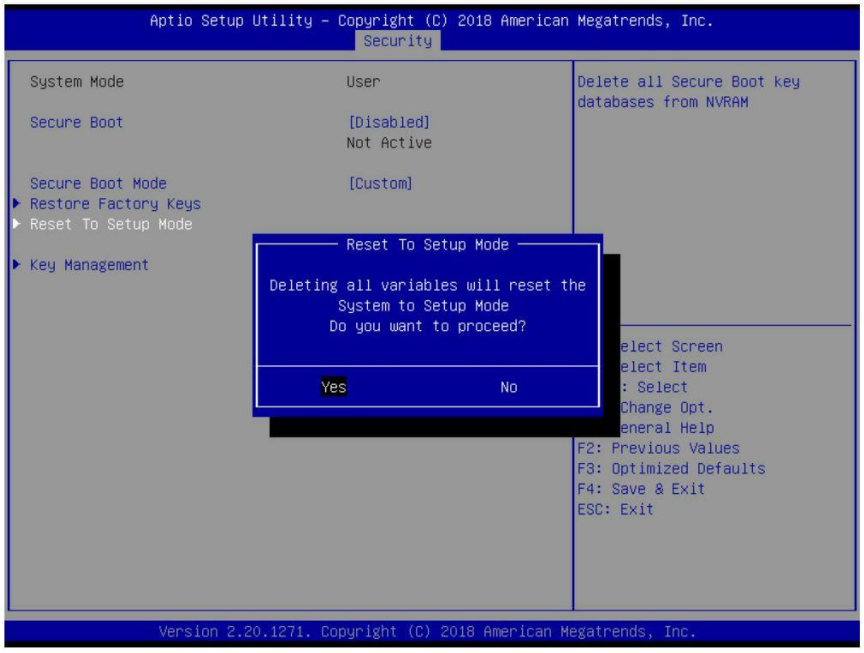



**Figure 46. Reset to setup mode submenu**

### 6.1.3 Key Management

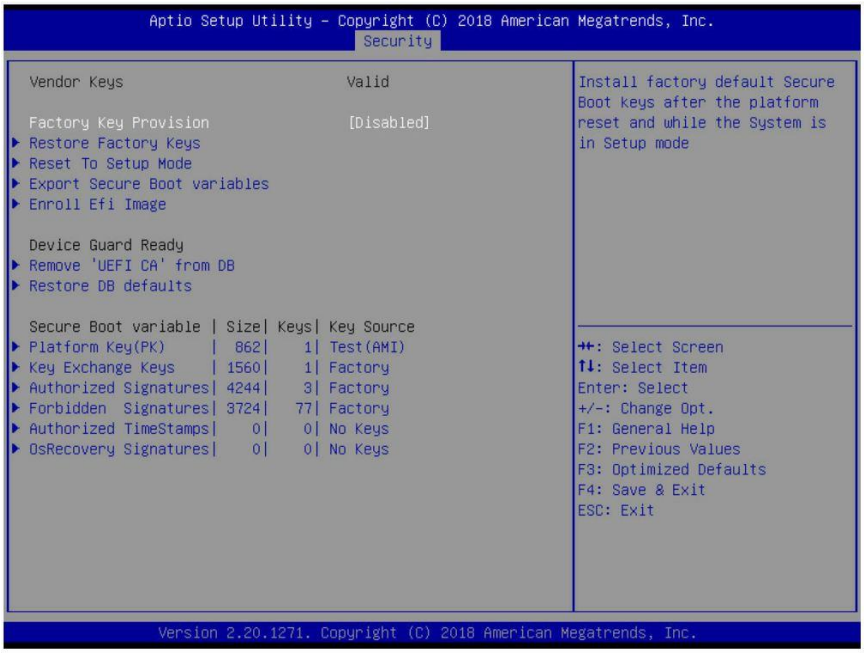



**Figure 47. Key management submenu**

**Table 42. Key management submenu options**

| Menu Item | Description | Values |
|---|---|---|
| **Factory Key Provision** | Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode. | • **Disabled**<br>• Enabled |
| **Restore Factory Keys** | Upon selecting **Restore Factory Keys** a confirmation popup will appear. Press **Yes** to proceed **No** to cancel. | See description |
| **Reset to Setup Mode** | Upon selecting **Reset to Setup Mode** a confirmation popup will appear. Press **Yes** to proceed **No** to cancel. This will reset the system to factory conditions. | See description |
| **Export Secure Boot variables** | Copy NVRAM content of Secure Boot variables to files in a root folder on a file system device. | See description |
| **Enroll Efi Image** | Allow the image to run in Secure Boot mode. Enroll SHA256 Hash certificate of a PE image into Authorized Signature Database (db) | See description |
| **Remove 'UEFI CA' DB** | Device Guard ready system must not list 'Microsoft UEFI CA' Certificate in Authorized Signature (db).<br>Press **Yes** to proceed **No** to cancel. | • **Yes**<br>• No |
| **Restore DB defaults** | Upon selecting **Restore DB Defaults** a confirmation popup will appear. Press **Yes** to proceed **No** to cancel. | • **Yes**<br>• No |
| **Platform Key (PK)** | Enroll Factory Defaults or load certificates from a file:<br>• Public Key Certificate:<br>  ○ EFI_SIGNATURE_LIST<br>  ○ EFI_CERT_X509 (DER)<br>  ○ EFI_CERT_RSA2048 (bin)<br>  ○ EFI_CERT_SHAXXX<br>• Authenticated UEFI Variable<br>• EFI EFI/COFF Image (SHA256)<br>Key source: Factory, External, Mixed. | • **Update**<br>• Append |

| Menu Item | Description | Values |
|---|---|---|
| **Key Exchange Keys** | Enroll Factory Defaults or load certificates from a file:<br>• Public Key Certificate:<br>  ○ EFI_SIGNATURE_LIST<br>  ○ EFI_CERT_X509 (DER)<br>  ○ EFI_CERT_RSA2048 (bin)<br>  ○ EFI_CERT_SHAXXX<br>• Authenticated UEFI Variable<br>• EFI EFI/COFF Image (SHA256)<br>Key source: Factory, External, Mixed | • **Update**<br>• Append |
| **Authorized Signatures** | Enroll Factory Defaults or load certificates from a file:<br>• Public Key Certificate:<br>  ○ EFI_SIGNATURE_LIST<br>  ○ EFI_CERT_X509 (DER)<br>  ○ EFI_CERT_RSA2048 (bin)<br>  ○ EFI_CERT_SHAXXX<br>• Authenticated UEFI Variable<br>• EFI EFI/COFF Image (SHA256)<br>Key source: Factory, External, Mixed | • **Update**<br>• Append |
| **Forbidden Signatures** | Enroll Factory Defaults or load certificates from a file:<br>• Public Key Certificate:<br>  ○ EFI_SIGNATURE_LIST<br>  ○ EFI_CERT_X509 (DER)<br>  ○ EFI_CERT_RSA2048 (bin)<br>  ○ EFI_CERT_SHAXXX<br>• Authenticated UEFI Variable<br>• EFI EFI/COFF Image (SHA256)<br>Key source: Factory, External, Mixed | • **Update**<br>• Append |
| **Authorized TimeStamps** | Enroll Factory Defaults or load certificates from a file:<br>• Public Key Certificate:<br>  ○ EFI_SIGNATURE_LIST<br>  ○ EFI_CERT_X509 (DER)<br>  ○ EFI_CERT_RSA2048 (bin)<br>  ○ EFI_CERT_SHAXXX<br>• Authenticated UEFI Variable<br>• EFI EFI/COFF Image (SHA256)<br>Key source: Factory, External, Mixed | • **Update**<br>• Append |
| **OsRecovery Signatures** | Enroll Factory Defaults or load certificates from a file:<br>• Public Key Certificate:<br>  ○ EFI_SIGNATURE_LIST<br>  ○ EFI_CERT_X509 (DER)<br>  ○ EFI_CERT_RSA2048 (bin)<br>  ○ EFI_CERT_SHAXXX<br>• Authenticated UEFI Variable<br>• EFI EFI/COFF Image (SHA256)<br>Key source: Factory, External, Mixed | • **Update**<br>• Append |

# 7. Boot Manager

The Boot Manager menu allows the user to view a list of devices available for booting and to select a boot device for immediately booting the system. There is no predetermined order for listing bootable devices, and are simply listed in order of discovery.

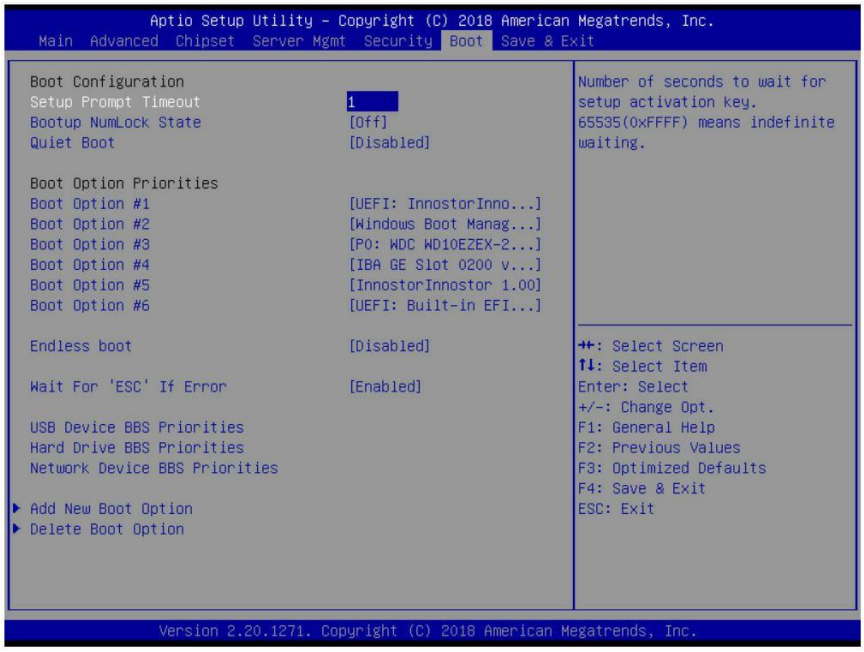



**Figure 48. Boot manager menu**

**Table 43. Boot manager menu options**

| Menu Item | Description | Values |
|---|---|---|
| **Setup Prompt Timeout** | Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting. | • **1** |
| **Bootup NumLock State** | Select the keyboard NumLock state. | • **Off**<br>• On |
| **Quiet Boot** | Enable or disable Quiet Boot option. | • **Disabled**<br>• Enabled |
| **Boot Option #1~#6** | Sets the system boot order. | • **Device Name**<br>• Disabled |
| **Endless Boot** | Restart the INT19 boot process automatically if all IPL devices fail to boot. | • **Disabled**<br>• Enabled |
| **Wait for 'ESC' If Error** | Wait for 'ESC' key to be pressed if error occurs. | • **Enabled**<br>• Disabled |
| **USB Device BBS Priorities** | Set the order of the legacy devices in this group. | Submenu |
| **Hard Drive BBS Priorities** | Set the order of the legacy devices in this group. | Submenu |
| **Network Device BBS Priorities** | Set the order of the legacy devices in this group. | Submenu |
| **Add New Boot Option** | Add a new EFI boot option to the boot order. | Submenu |
| **Delete Boot Option** | Delete an EFI boot option from the boot order. | Submenu |

## 7.1 USB Device BBS Priorities


**Figure 49. USB device BBS priorities submenu**

**Table 44. USB device BBS priorities submenu options**

| Menu Item | Description | Values |
|---|---|---|
| **Boot Option #1** | Sets the system boot order. | • **Device Name**<br>• Disabled |

## 7.2 Hard Drive BBS Priorities

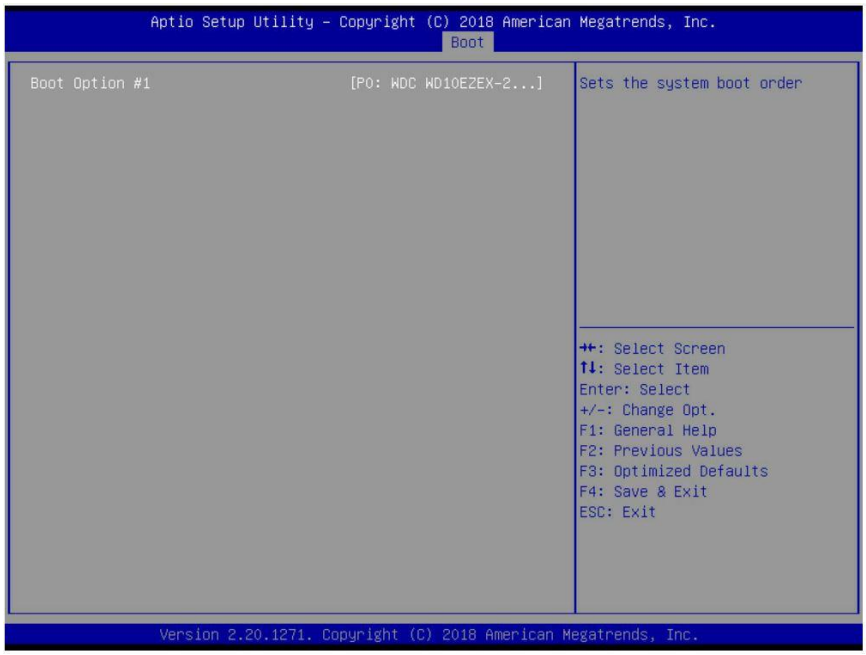



**Figure 50. Hard drive BBS priorities submenu**

**Table 45. Hard drive BBS priorities submenu options**

| Menu Item | Description | Values |
|---|---|---|
| **Boot Option #1** | Sets the system boot order. | • **Device Name**<br>• Disabled |

## 7.3 Network Device BBS Priorities

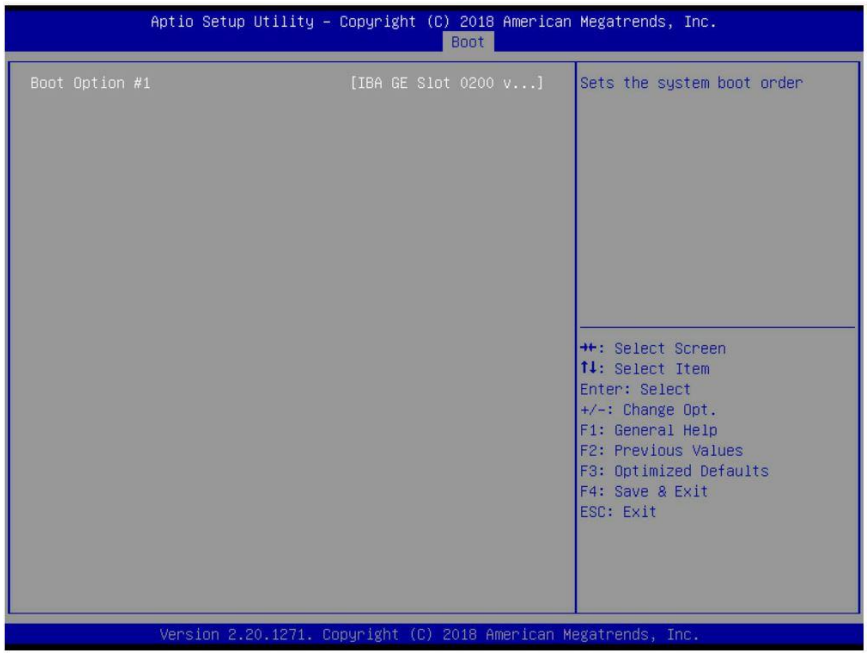



**Figure 51. Network device BBS priorities submenu**

**Table 46. Network device BBS priorities submenu options**

| Menu Item | Description |
|---|---|
| **Boot Option #1** | Sets the system boot order. |

## 7.4 Add New Boot Option

The Add New Boot Option menu allows the user to add a boot option to the boot order. The Internal EFI Shell boot option is permanent and cannot be added or deleted.

To access this screen from the main menu, select **Boot** > **Add New Boot Option**. Press the **<Esc>** key to return to the Boot menu.

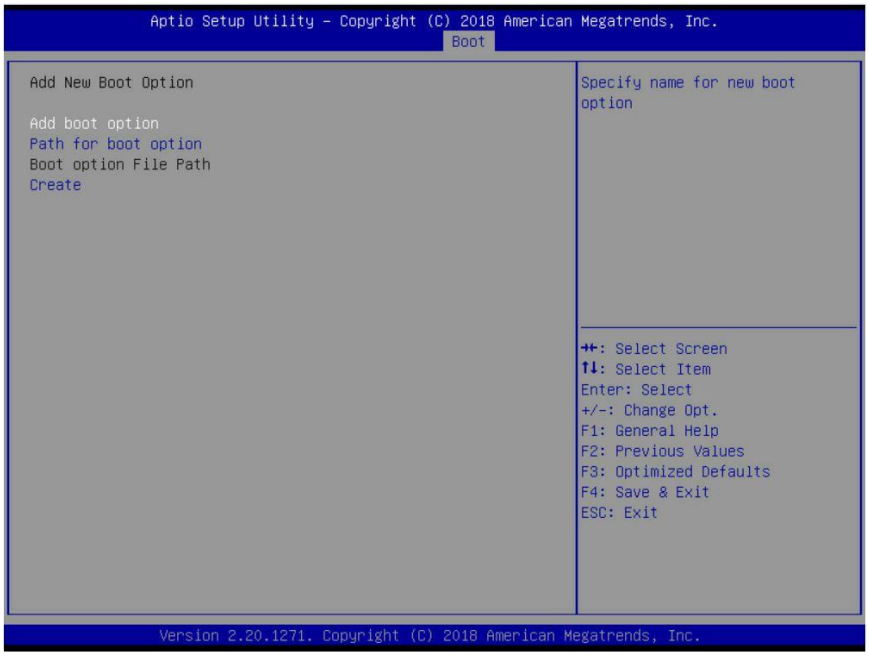



**Figure 52. Add new boot option submenu**

**Table 47. Add new boot option submenu options**

| Menu Item | Description | Values |
|---|---|---|
| **Boot Option #1** | Sets the system boot order. | • **Device Name**<br>• Disabled |

## 7.5 Delete Boot Option


**Figure 53. Delete boot option submenu**

**Table 48. Delete boot option submenu options**

| Menu Item | Description | Values |
|---|---|---|
| Delete Boot Option | Remove an EFI boot option from the boot order. | • **Select one to delete**<br>• UEFI: Built-in EFI Shell |

# 8. Save & Exit

The save and exit menu allows the user to choose whether to save or discard the configuration changes made on other setup screens. It also allows the user to restore the BIOS settings to the factory defaults or to save or restore them to a set of user-defined default values.

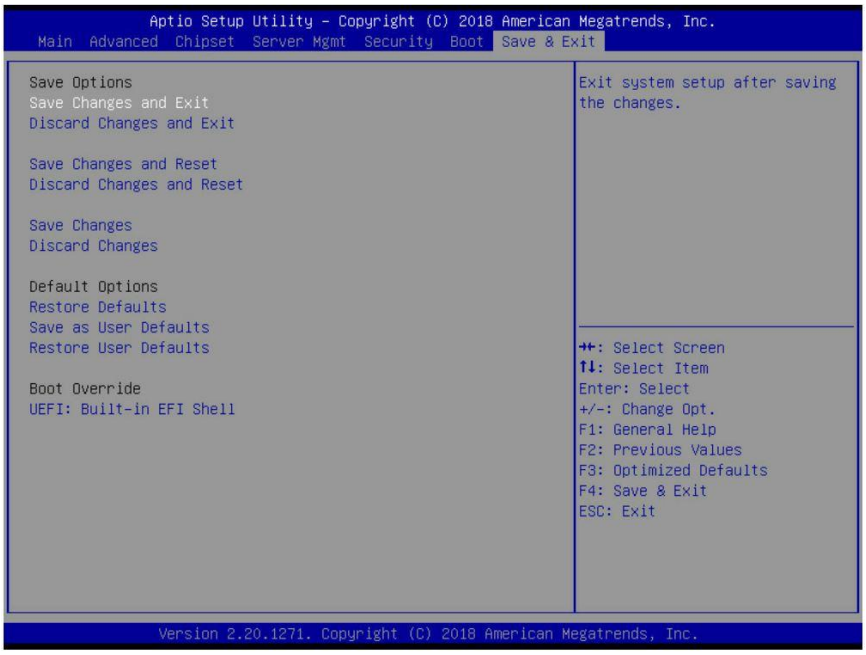



**Figure 54. Save and exit menu**

**Table 49. Save and exit menu options**

| Menu Item | Description | Values |
|---|---|---|
| **Save Changes and Exit** | Exit system setup after saving the changes. | See description. |
| **Discard Changes and Exit** | Exit system setup without saving any changes. | |
| **Save Changes and Reset** | Reset the system after saving the changes. | |
| **Discard Changes and Reset** | Reset system setup without saving any changes. | |
| **Save Changes** | Save changes done so far to any of the setup options. | |
| **Discard Changes** | Discard changes done so far to any of the setup options. | |
| **Restore Defaults** | Restore/Load Default values for all the setup options. | |
| **Save as User Defaults** | Save the changes done so far as User Defaults. | |
| **Restore User Defaults** | Restore the User Defaults to all the setup options. | |

# Appendix A. Glossary

| Term | Definition |
|---|---|
| **16-bit Legacy** | The traditional personal computer environment. Includes legacy Option ROMs and legacy 16-bit code. |
| **ACPI** | Advanced Configuration and Power Interface. ACPI is an open industry specification proposed by Intel, Microsoft and Toshiba. ACPI enables and supports reliable power management through improved hardware and OS coordination. |
| **ADDDC** | Adaptive Double Device Data Correction |
| **AES** | Advanced Encryption Standard – encryption algorithm |
| **AER** | Advanced Error Reporting |
| **AHCI** | Advanced Host Controller Interface, a technical standard that specifies the operation of Serial ATA (SATA) host bus adapters |
| **ANSI** | American National Standards Institute |
| **API** | Application Programming Interface. A software abstraction provided by the BIOS to applications and/or the OS. |
| **ASCII** | American Standard Code for Information Interchange. An 8-level code (7 bits plus parity check) widely used in data processing and data communications systems |
| **ATA** | Advanced Technology Attachment, a disk interface standard |
| **BDS** | Boot Device Selection |
| **Bit** | The smallest unit of binary data, which may have values only of 0 or 1. Bits are typically combined to form larger units of data, e.g., 8 bits form a byte. In combination with a quantifier like “K”, “M”, or “G”, bits is abbreviated to lowercase “b” – e.g., Kb, Mb, or Gb. |
| **BIOS** | Basic Input/Output System – Firmware interface to the system hardware |
| **BMC** | Baseboard Management Controller |
| **Byte** | A data unit made up of 8 bits, which in turn may be combined into larger units of data, e.g., words or doublewords. In the Intel Architecture, a byte is the smallest addressable unit of memory. In combination with a quantifier like “K”, “M”, or “G”, bytes is abbreviated to uppercase “B” – e.g., KB, MB, or GB. |
| **CATERR, CATERR#** | Catastrophic Error signal, triggering an SMI if pulsed or indicating a fatal hardware error when held asserted. |
| **COM1** | Communication Port 1, serial port 1 |
| **COM2** | Communication Port 2, serial port 2 |
| **CSM** | Compatibility Support Module |
| **DDR4** | Double Data Rate 3 is a high bandwidth memory technology. |
| **DHCP** | Dynamic Host Configuration Protocol, for dynamically assigned IIP addresses |
| **DIMM** | Dual In-line Memory Module, a plug-in memory module with signal and power pins on both sides of the internal printed circuit board (front and back). |
| **DMI** | Direct Media Interface – connection from the processor to the PCH |
| **Doubleword** | A data unit composed of 32 bits = 4 bytes = 2 words. |
| **DRAM** | Dynamic Random Access Memory, memory chips from which DIMMs are constructed |
| **DR** | Dual Rank or Double Rank – memory DIMM organization, DRAMs organized in two ranks |
| **DWORD** | Doubleword, a 32-bit quantity |
| **ECC** | Error Correction Code. Refers to a memory system that has extra bit(s) to support limited detection/correction of memory errors. |
| **FRB** | Fault Resilient Booting |
| **FRU** | Field Replaceable Unit |
| **FSB** | Front Side Bus |
| **GUID** | Globally Unique Identifier |
| **Hot key** | A key combination recognized as an unprompted command input. For example, pressing <F2> during POST will take the operator to the Setup Utility. |
| **Intel® Optane™ DC Persistent Memory Module** | Intel® Optane™ Data Center Persistent Memory Module |
| **Intel® HT Technology** | Intel® Hyper-Threading Technology |
| **I/O** | Input/output |
| **IPMI** | Intelligent Platform Management Interface – an industry standard that defines standardized, abstracted interfaces to platform management hardware. |
| **IRQ** | Interrupt Request |

| Term | Definition |
|---|---|
| **IT** | Information Technology |
| **LAN** | Local Area Network |
| **Mb** | "Megabit" – 1024 kilobits, or 1,048,576 bits. Lowercase "b" distinguishes "bits". |
| **MB** | "Megabyte" – 1024 kilobytes, or 1,048,576 bytes. Uppercase "B" distinguishes "bytes". |
| **Intel® ME** | Intel® Management Engine |
| **Mega~** | Mega as a quantifier prefix means 1,048,576 (1024 * 1024), or 1024 * Kilo, e.g., MB means "megabyte" or 1024 KB. Mega is sometimes loosely used as meaning "million". |
| **Intel® NM** | Intel® Node Manager – now Intel® Intelligent Power Node Manager |
| **NMI** | Non-Maskable Interrupt |
| **NUMA** | Non-Uniform Memory Access (secondary usage as Non-Uniform Memory Architecture) |
| **OEM** | Original Equipment Manufacturer |
| **OS** | Operating System |
| **PCH** | Platform Controller Hub |
| **PCI** | Peripheral Component Interconnect, or PCI Local Bus Standard – also called "Conventional PCI" |
| **PCIe*** | PCI Express* -- an updated form of PCI offering better throughput and better error management |
| **PCI-X** | And enhanced version of PCI, offering better throughput, protocol and error handling improvements |
| **PECI** | Platform Environmental Control Interface |
| **PERR** | Parity Error |
| **PMI** | Platform Management Interrupt |
| **POST** | Power On Self-Test – BIOS activity from the time on Power On until Operating System boot begins. |
| **RAID** | Redundant Array of Inexpensive Disks – provides data security by spreading data over multiple disk drives. RAID 0, RAID 1, RAID 10, and RAID 5 are different patterns of data on varying numbers of disks to provide varying degrees of security and performance. |
| **RAS** | Reliability, Availability, and Serviceability |
| **RDIMM** | Registered DIMM (also called buffered) memory modules have an address buffer register between the SDRAM modules and the system's memory controller. |
| **ROM** | Read-Only Memory |
| **RT** | Runtime. Component of Intel® Platform Innovation Framework for EFI architecture |
| **RTC** | Real Time Clock |
| **SAS** | Serial Attached SCSI, a high speed serial data version of SCSI |
| **SATA** | Serial ATA, a high speed serial data version of the disk ATA interface |
| **TDP** | Thermal Design Power |
| **Intel® TXT** | Intel® Trusted Execution Technology |
| **UEFI** | Unified Extensible Firmware Interface – replacement for Legacy BIOS and the Legacy DOS interface |
| **URL** | Uniform Resource Locator, a symbolic Internet address to locate a specific item such as a web page, a file, or an application. A URL is composed of the protocol (e.g., "http") plus the domain (e.g., www.intel.com plus the name of the resource to be accessed. |
| **USB** | Universal Serial Bus, a standard serial expansion bus meant for connecting peripherals. |
| **Intel® VT** | Intel® Virtualization Technology |
| **Intel® VT-c** | Intel® Virtualization Technology for Connectivity |
| **Intel® VT-d** | Intel® Virtualization Technology for Directed I/O |
| **Intel® VT-x** | Intel® Virtualization Technology for IA-32, Intel® 64 and Intel® Architecture |