

P/Q-Motherboards

User Manual

01750345464A



Table of Contents

1	Symbols	1-1
2	Important notes	2-1
3	Warranty	3-1
4	ESD (Electrostatic Sensitive Devices)	4-1
5	Motherboard Variants	5-1
5.1	Px Motherboard	5-1
5.1.1	Front view	5-1
5.1.2	Back view	5-2
5.1.3	Specification	5-3
5.2	Qx Motherboard	5-5
5.2.1	Front view	5-5
5.2.2	Back view	5-6
5.2.3	Specification	5-7
6	Block Diagram	6-1
6.1	Px-Motherboard	6-1
6.2	Qx-Motherboard	6-2
7	Apollo Lake	7-1
7.1	Default BIOS Settings	7-1
7.1.1	Information	7-1
7.1.2	Main	7-2
7.1.3	Advanced	7-4
7.1.4	Chipset	7-15
7.1.5	PC Health	7-24
7.1.6	Power	7-25
7.1.7	Security	7-26
7.1.8	Boot	7-29
7.1.9	Save & Exit	7-34
8	Kaby Lake	8-1
8.1	Default BIOS Settings	8-1
8.1.1	Information	8-1
8.1.2	Main	8-2
8.1.3	Advanced	8-4
8.1.4	Chipset	8-27
8.1.5	PC Health	8-35
8.1.6	Power	8-36
8.1.7	Security	8-38
8.1.8	Boot	8-41
8.1.9	Save & Exit	8-44
9	Recycling	9-1

1 Symbols



DANGER

This warning note describes a hazard with a high degree of risk, which, if not avoided, will result in death or grave bodily injury.



WARNING

This warning note describes a hazard with a medium degree of risk, which, if not avoided, will result in death or grave bodily injury.



CAUTION

This warning note describes a hazard with a low degree of risk, which, if not avoided, will result in death or grave bodily injury.



NOTE

This note provides application tips and information that help prevent errors and material damage.

2 Important notes

Take note of the following precautions before you install motherboard components or change any motherboard settings.

Unplug the power cord from the wall socket before touching any component.

Before handling components, use a grounded wrist strap or touch a safely grounded object or a metal object, such as the power supply case, to avoid damaging them due to static electricity.

Hold components by the edges to avoid touching the ICs on them.

Whenever you uninstall any component, place it on a grounded antistatic pad or in the bag that came with the component.

Before you install or remove any component, always remove the AC power by unplugging the power cord from the power outlet. Failure to do so may cause severe damage to the motherboard, peripherals, or components.

3 Warranty

Generally Diebold Nixdorf guarantees a warranty engagement for 12 months beginning with the date of delivery. This warranty engagement covers all damages which occur despite a normal use of the product.

Damages because of improper or insufficient maintenance, improper use of the product or unauthorized modifications of the product, inadequate location or surroundings will not be covered by the warranty.

For further information on the stipulation consult your contract.

All parts of the product which are subject to wear and tear are not included in the warranty engagement. For detailed warranty arrangements please consult your contract documents.



NOTE

Please contact your local service provider for all questions concerning your service contract.

4 ESD (Electrostatic Sensitive Devices)



NOTE

Electrostatic sensitive devices (ESD) may be marked with this sticker.

When you handle components fitted with ESDs, you must observe the following points under all circumstances:

Make sure that the device is de-energized before connecting, removing or installing components with ESD.

Always use the antistatic equipment.

Unplug the power before inserting or removing components containing ESDs.

While working with ESDs you must discharge yourself by using an ESD wrist strap or grounding cable to connect yourself at all times to the earth connector of power socket or a grounded object.

Place all components containing ESDs on a static-safe base.

The equipment and tools you use must be free of static charges.

Always hold boards with ESDs by their edges. Do not touch the components.

Never touch pins or conductors on boards fitted with ESDs.

5 Motherboard Variants

5.1 Px Motherboard

5.1.1 Front view

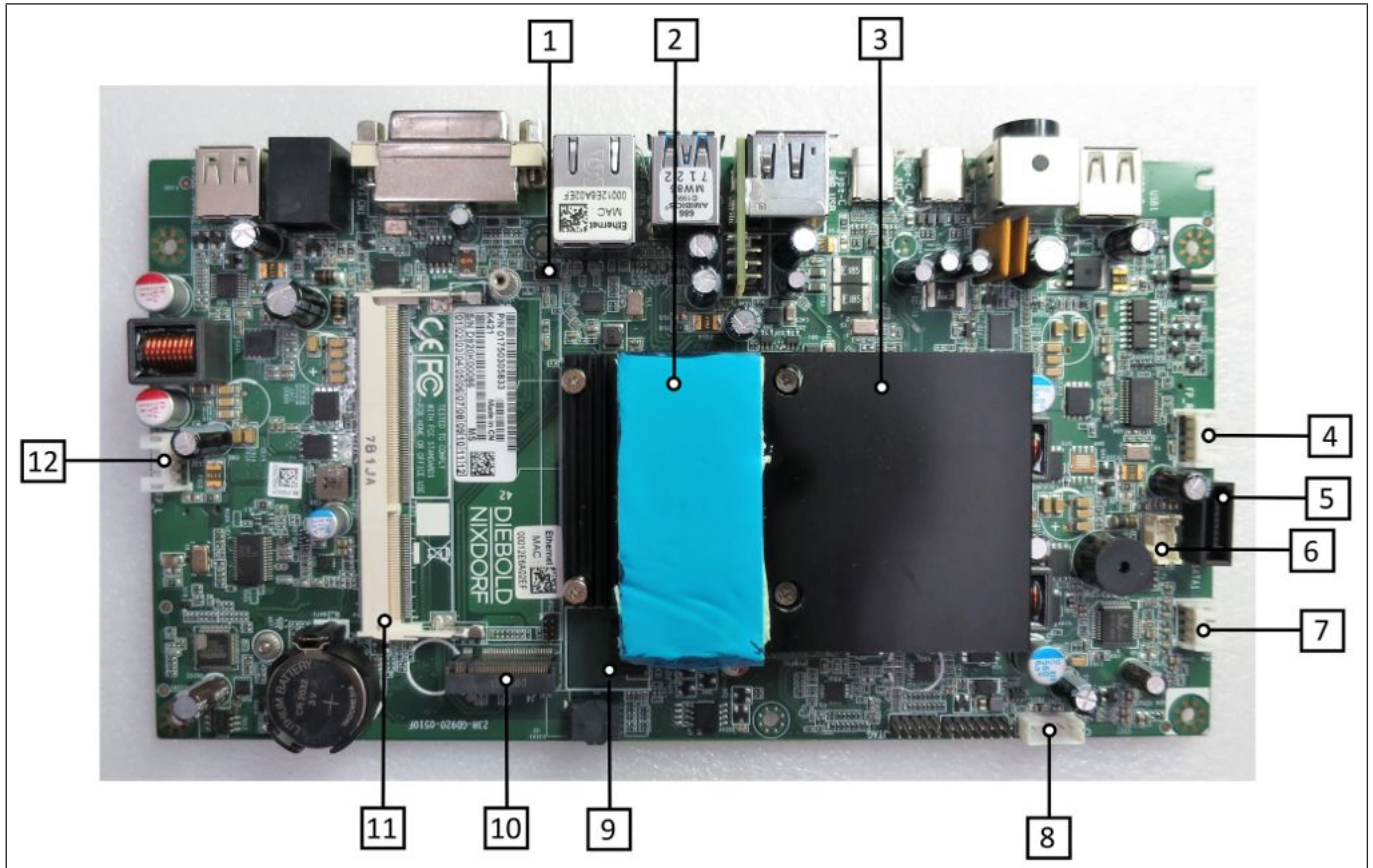


Figure 5-1: Px motherboard, front view, (Apollo Lake)

1	CMOS clear	2	Thermal pad
3	Heat sink	4	USB-R
5	SATA	6	SATA power
7	Speaker	8	Audio line-out
9	TPM option	10	M.2 2280 socket
11	SODIMM socket	12	USB-L

5.1.2 Back view

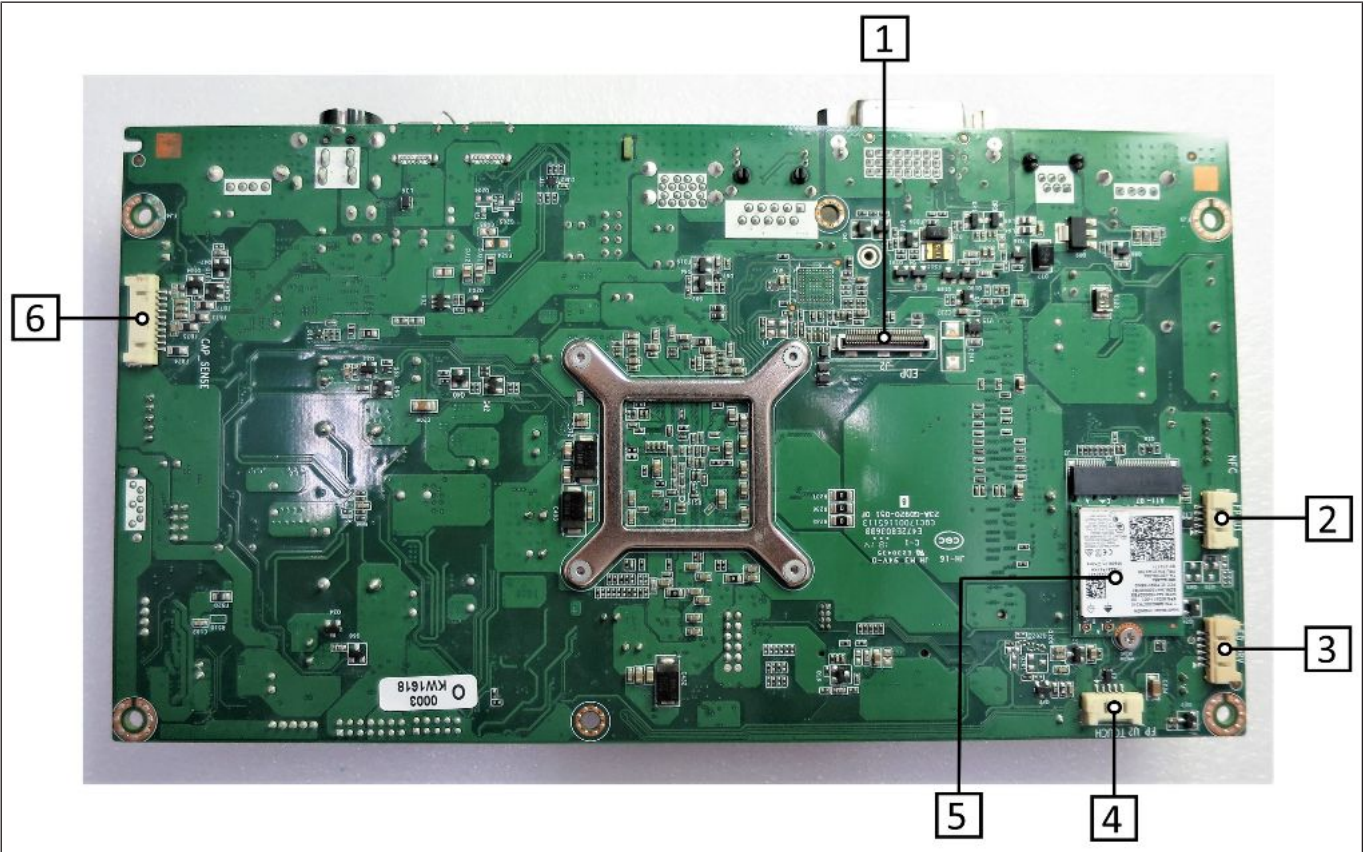


Figure 5-2: Px motherboard, back view, (Apollo Lake)

1	EDP port	2	NFC
3	Backlight	4	Touch
5	WLAN module	6	Front panel

5.1.3 Specification

Model Name	P1.0-APL-AIO
Processor (Apollo Lake)	Pentium N4200
Number of Cores	4
Number of Threads	4
Base Frequency	1.10GHz
Burst Frequency	2.50GHz
Integrated Graphics	Intel HD Graphics 505
TDP	6W
Memory socket	SODIMM, DDR3L 1600/1687, Max 8GB
Audio	Realtek ALC662, Stereo 2x2W Class D
Network	
Wired	Realtek RTL8111F
Wireless/Bluetooth	Intel Wireless-AC 3168 (M.2 2230 E-Key)
Super IO	ITE IT8613
Primary Display	14" TFT, 1920x1080, 6-bit+FRC
M.2 2280 Socket M-Key	SATA SSD
User I/O Ports	1x USB-C Alt DP (PD2.0: 5V, 12V) 1x USB-C (5V) 2x USB3.0, 2x USB2.0 1x 24V-PUSB DVI/PL2 (secondary display)

Motherboard Variants

	RJ12 (Cashdrawer) RJ45 (wired-LAN)
TPM 2.0 Support	TPM Daughter board interface

5.2 Qx Motherboard

5.2.1 Front view

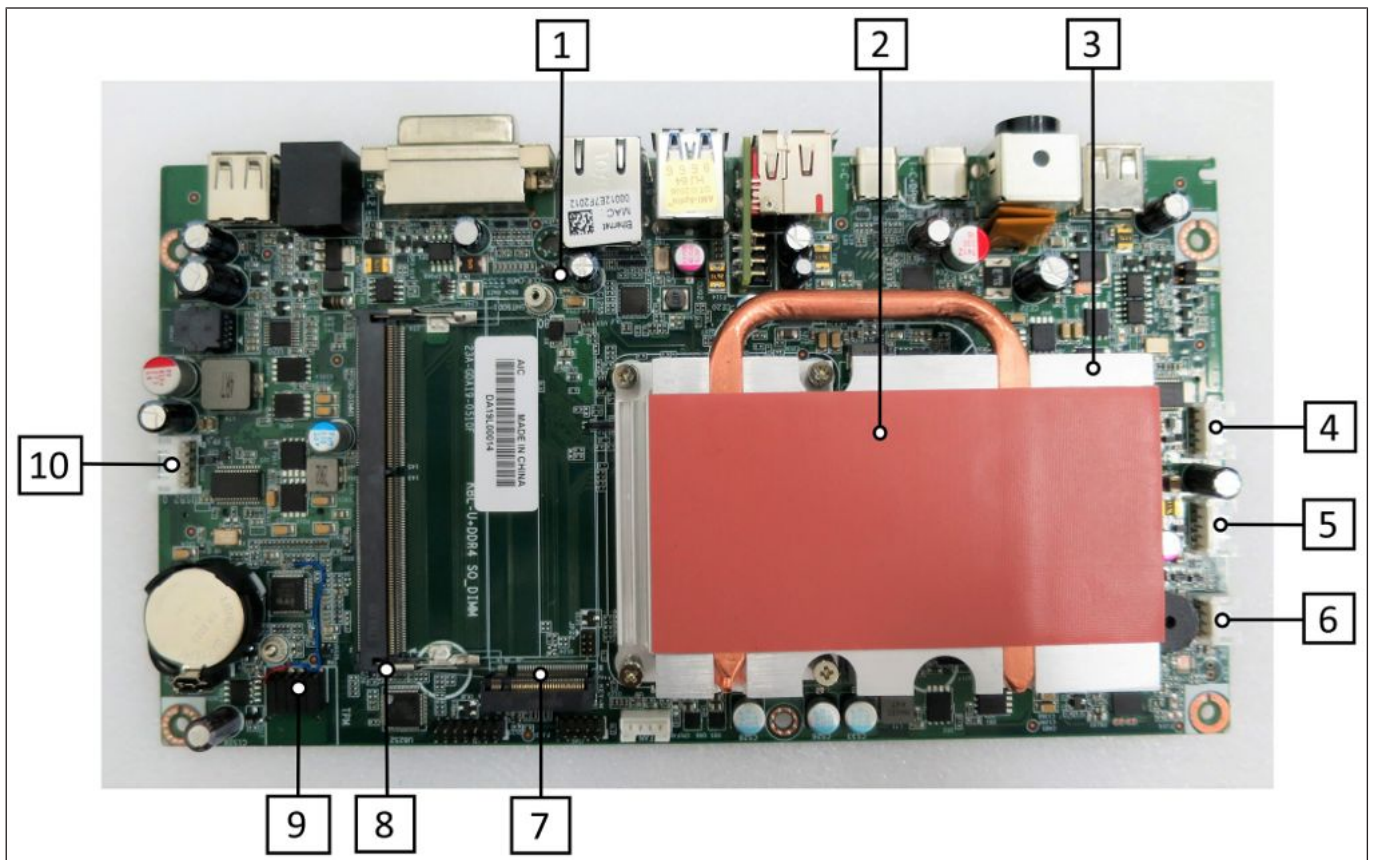


Figure 5-3: Qx motherboard, front view, (Kaby Lake)

1	CMOS clear	2	Thermal pad
3	Heat sink	4	USB-R
5	MF module	6	Speaker
7	M.2 2280 socket	8	SODIMM socket
9	TPM option	10	USB-L

5.2.2 Back view

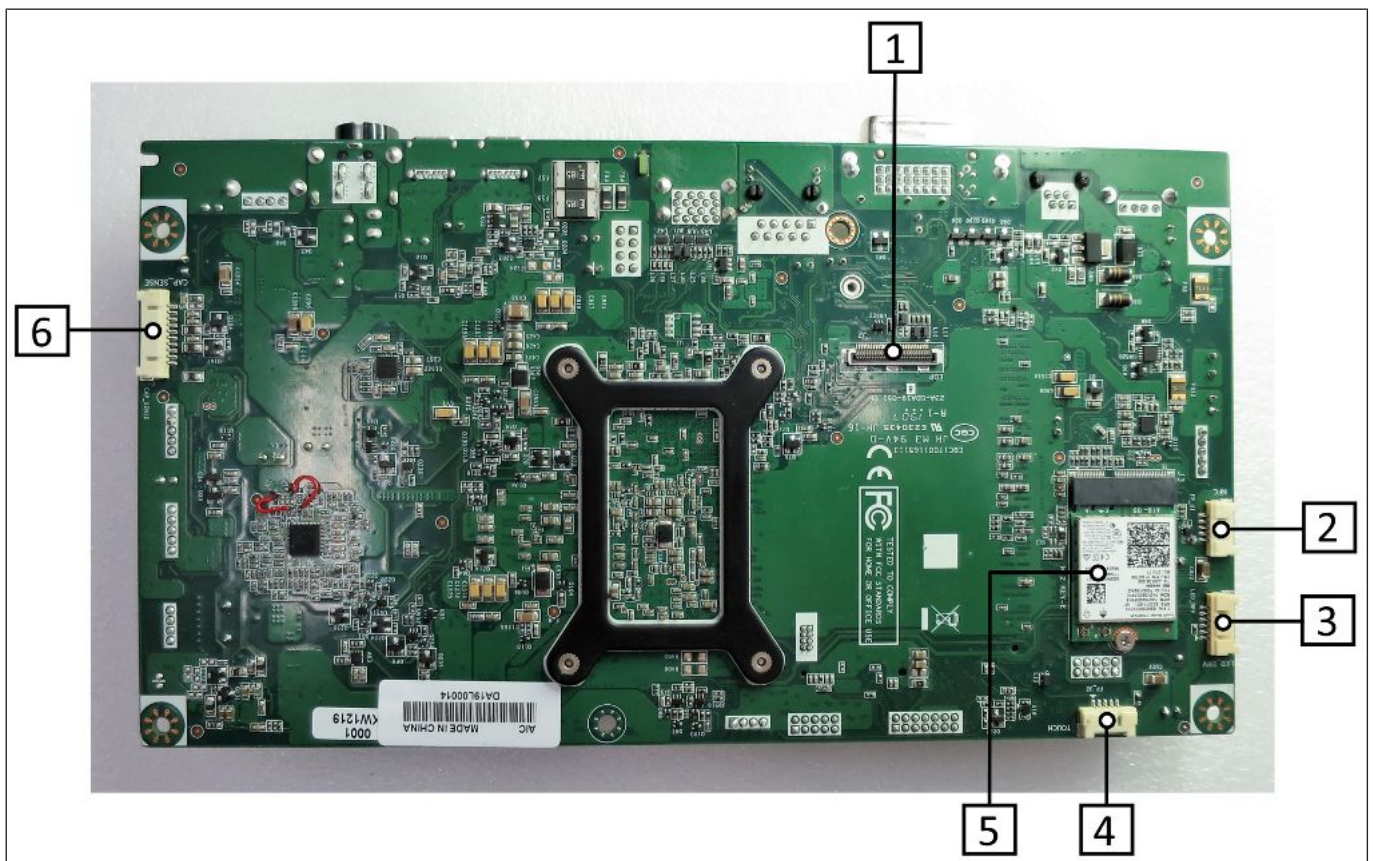


Figure 5-4: Qx motherboard, back view, (Kaby Lake)

1	EDP port	2	NFC
3	Backlight	4	Touch
5	WLAN module	6	Front panel

5.2.3 Specification

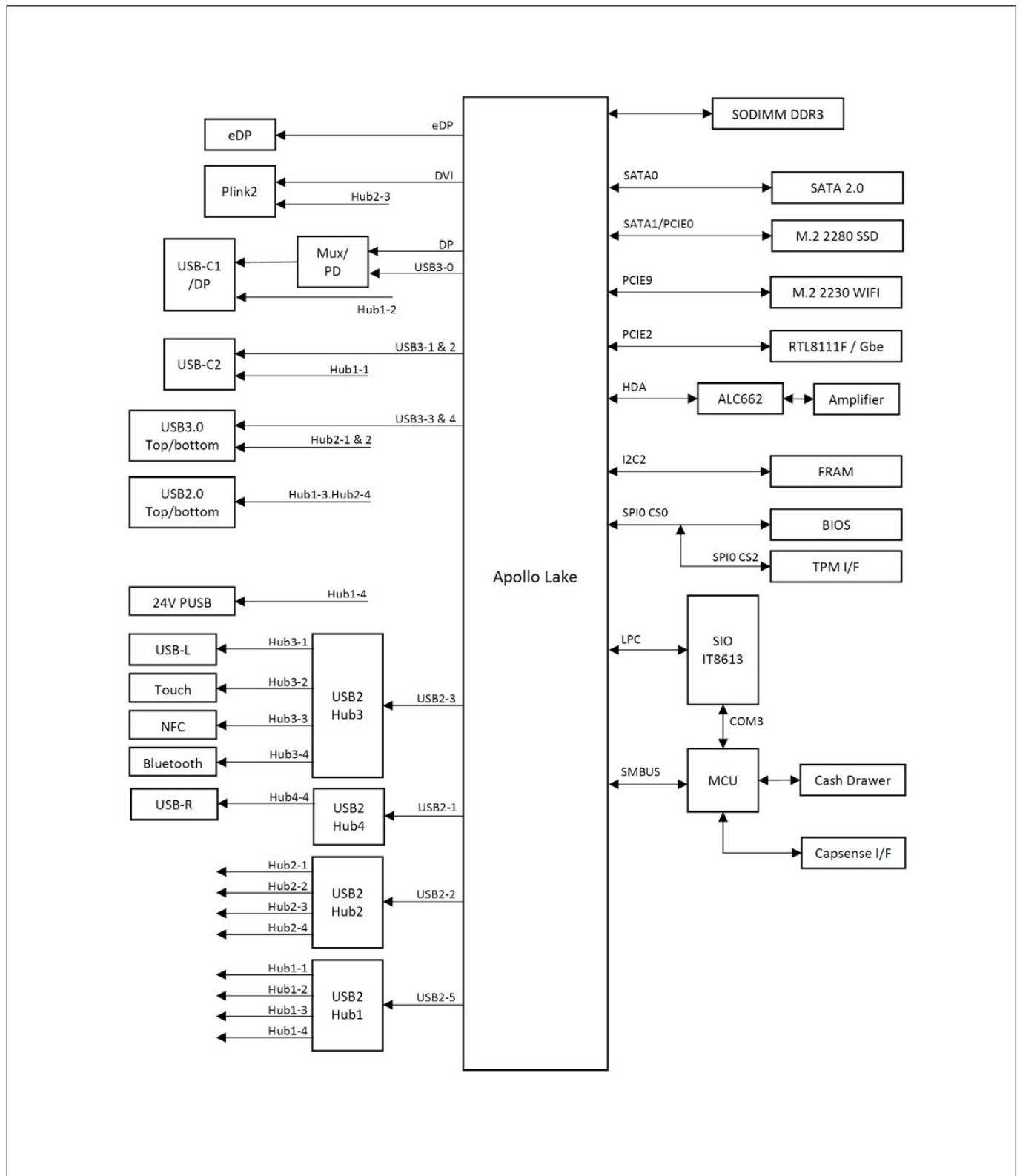
Model Name	Q1.0-KBL-AIO	Q2.0-KBL-AIO	Q3.0-KBL-AIO
Processor (Kaby Lake U)	Celeron 3965U	i3-7100U	i5-7300U
Number of Cores	2	2	2
Number of Threads	2	4	4
Base Frequency	2.20GHz	2.4GHz	2.4GHz
Max Turbo Frequency	-	-	3.5GHz
Integrated Graphics	Intel HD 610	Intel HD 620	Intel HD 620
TDP	15W		
Memory socket	SODIMM, DDR4-2133, Max 8GB		
Audio	Realtek ALC256, Stereo 2x2W Class D		
Network	GbE		
Wired	Intel i219V	Intel i219V	Intel i219LM
Wireless/Bluetooth	Intel Wireless-AC 3168 (M.2 2230 E-Key)		
Super IO	ITE IT8613		
Primary Display	14” TFT, 1920x1080, 6-bit+FRC		
M.2 2280 socket, M-Key	SATA	SATA & 4-Lane PCIe	SATA & 4-Lane PCIe
User I/O Ports	1x USB-C Alt DP (PD2.0: 5V, 12V) 1x USB-C (5V) 2x USB3.0, 2x USB2.0 1x 24V-PUSB DVI/PL2 (secondary display)		

Motherboard Variants

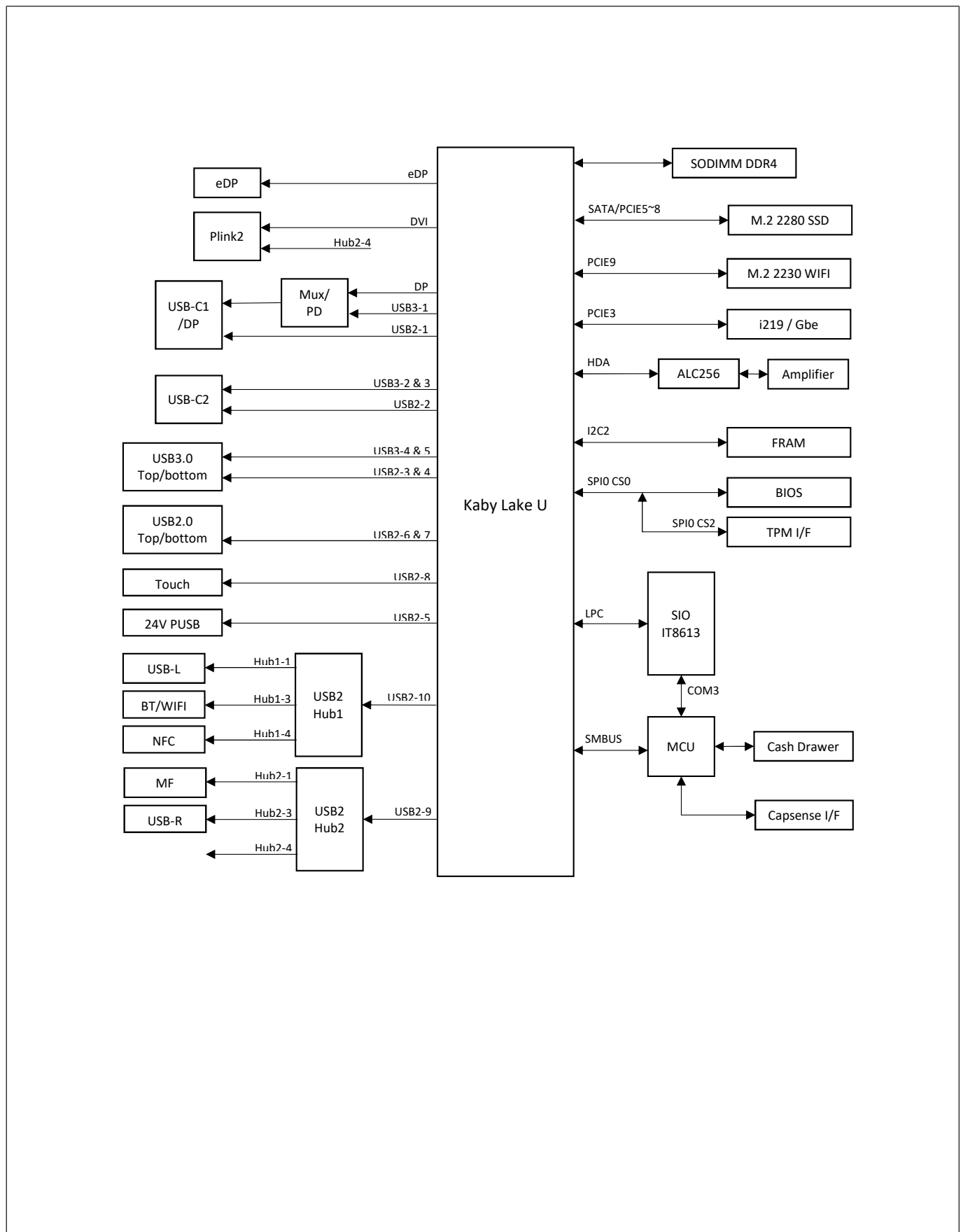
	RJ12 (Cashdrawer) RJ45 (wired-LAN)
TPM 2.0 Support	TPM Daughter board interface

6 Block Diagram

6.1 Px-Motherboard



6.2 Qx-Motherboard



7 Apollo Lake

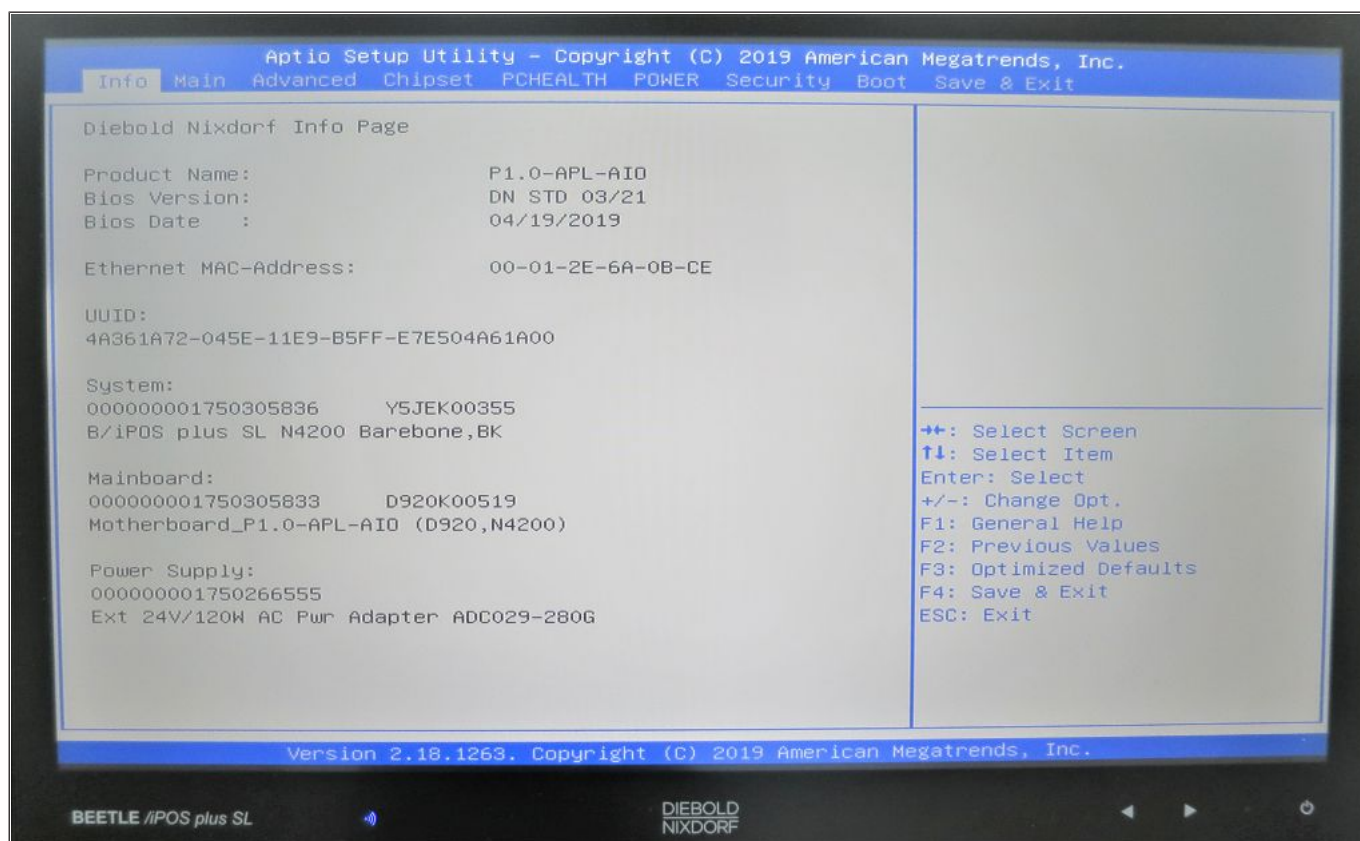
7.1 Default BIOS Settings

The tables below indicate the BIOS default setting for reference purpose. Upon power ON, enter BIOS setup by pressing 'Delete' or pressing 'F2'..



WARNING
Please take note of any special BIOS setting according to your customer's usage before resuming the BIOS setting to its default.

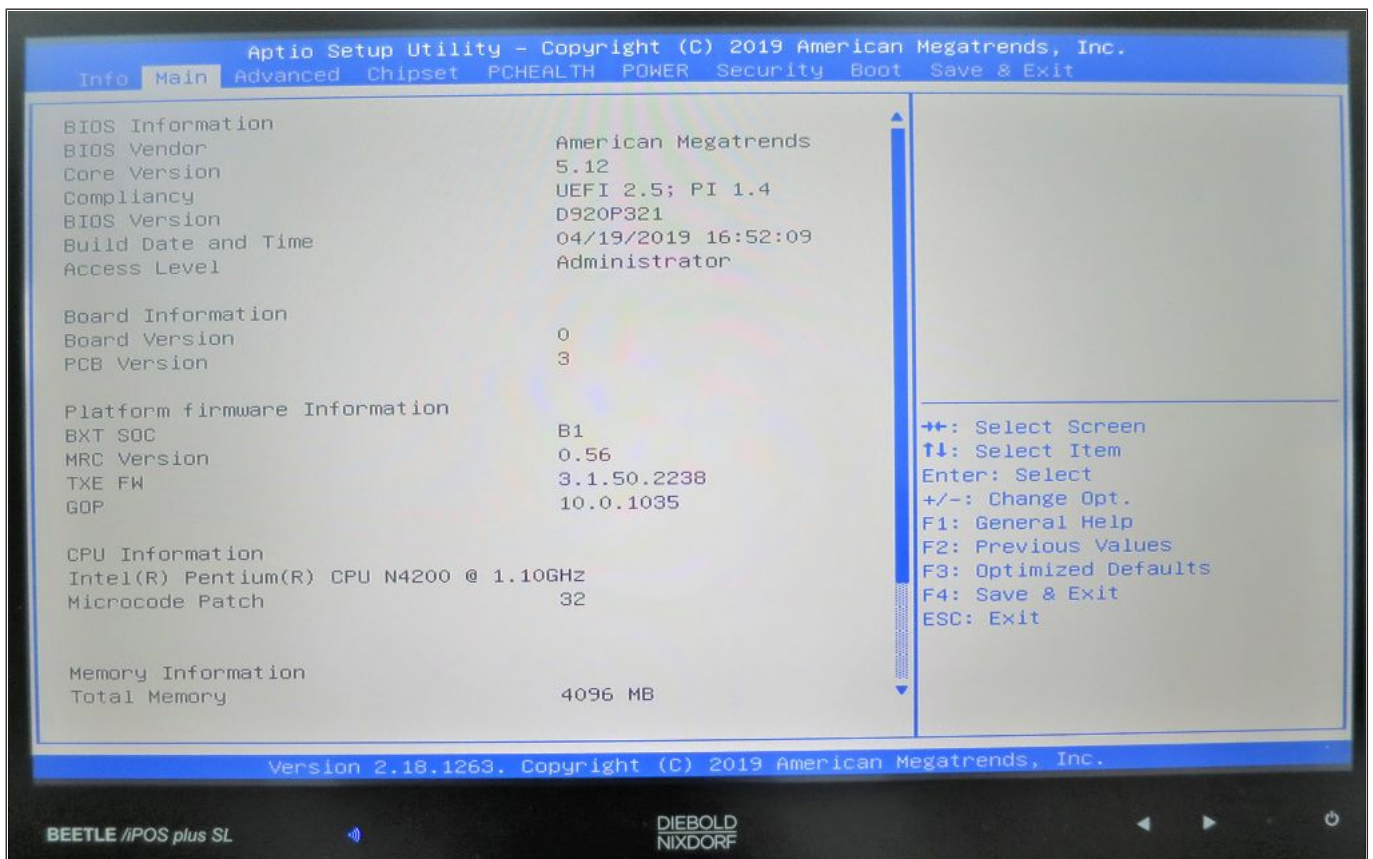
7.1.1 Information



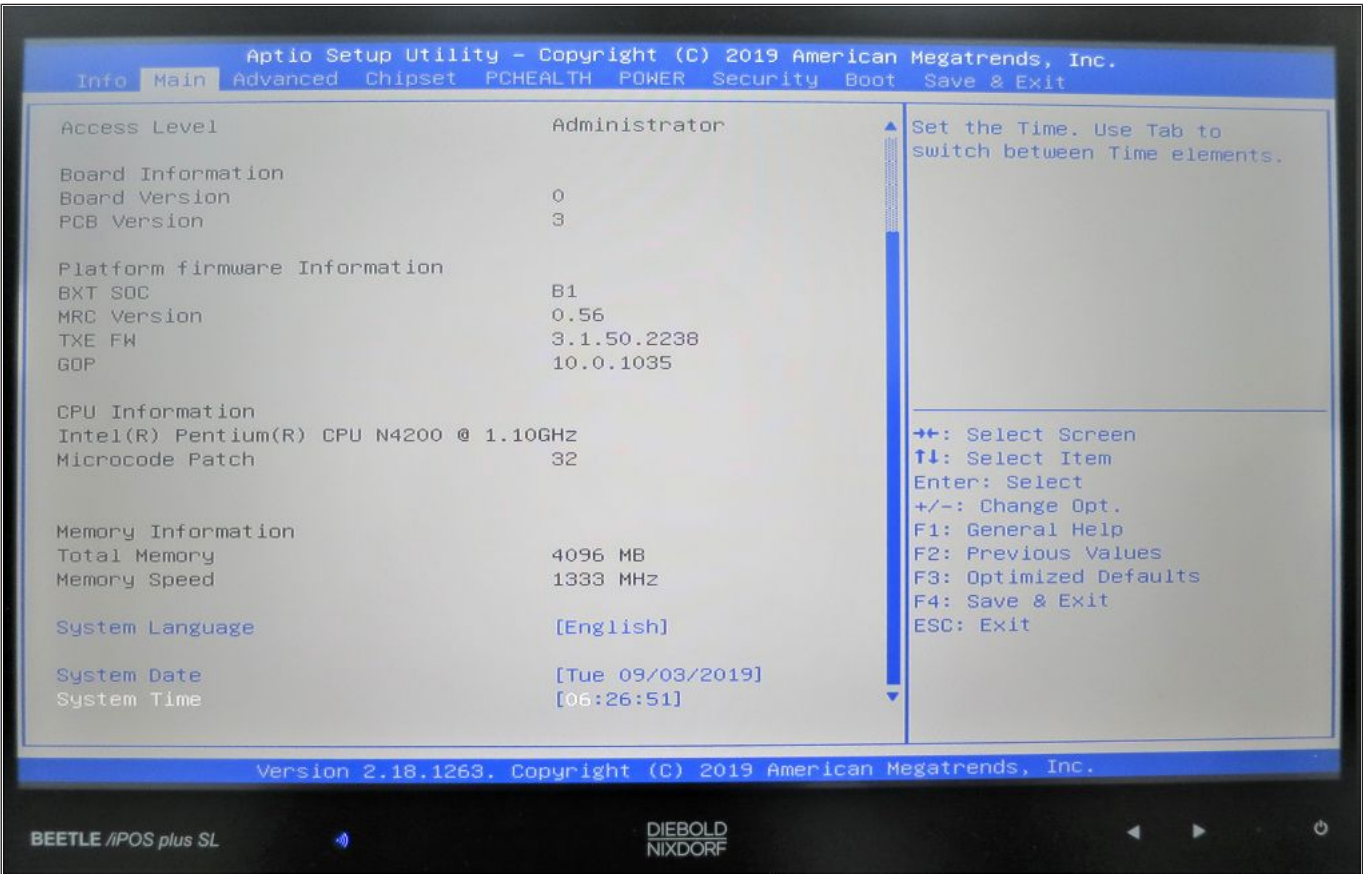
This page displays some system-related information to facilitate the support of your system.

Product Name:	This identification string identifies the motherboard in the system.
BIOS Version:	Display in the format DN STD xx/yy where xx is the BIOS version number and yy is the build number.
MAC Address:	Ethernet MAC Address of the on-board LAN controller.
UUID:	A UUID is an identifier standard used in software construction, standardized by the Open Software Foundation. The intent of the UUIDs is to enable distributed systems to uniquely identify information without significant central coordination.

7.1.2 Main

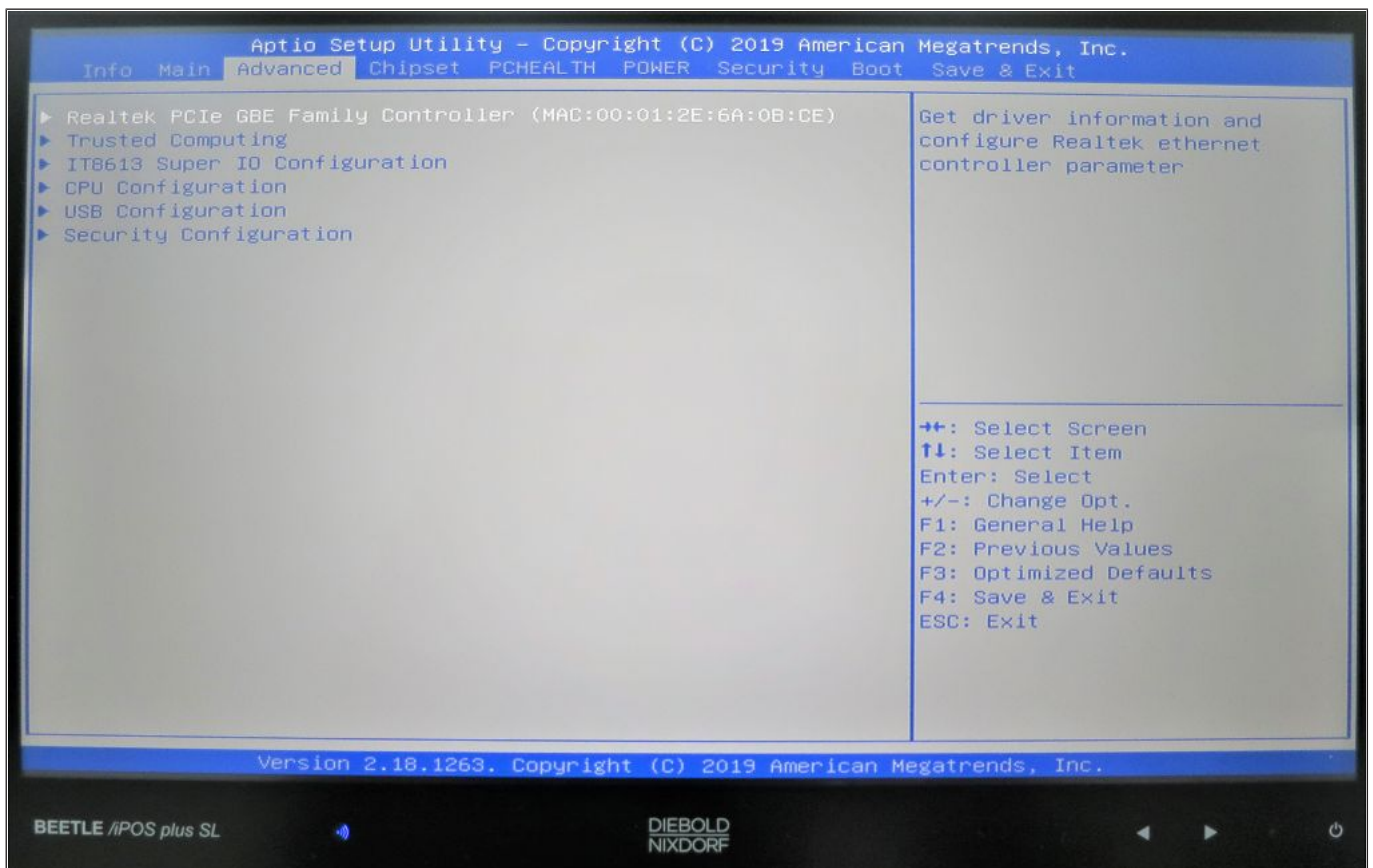


The Main page provides the key information about the system hardware configuration.



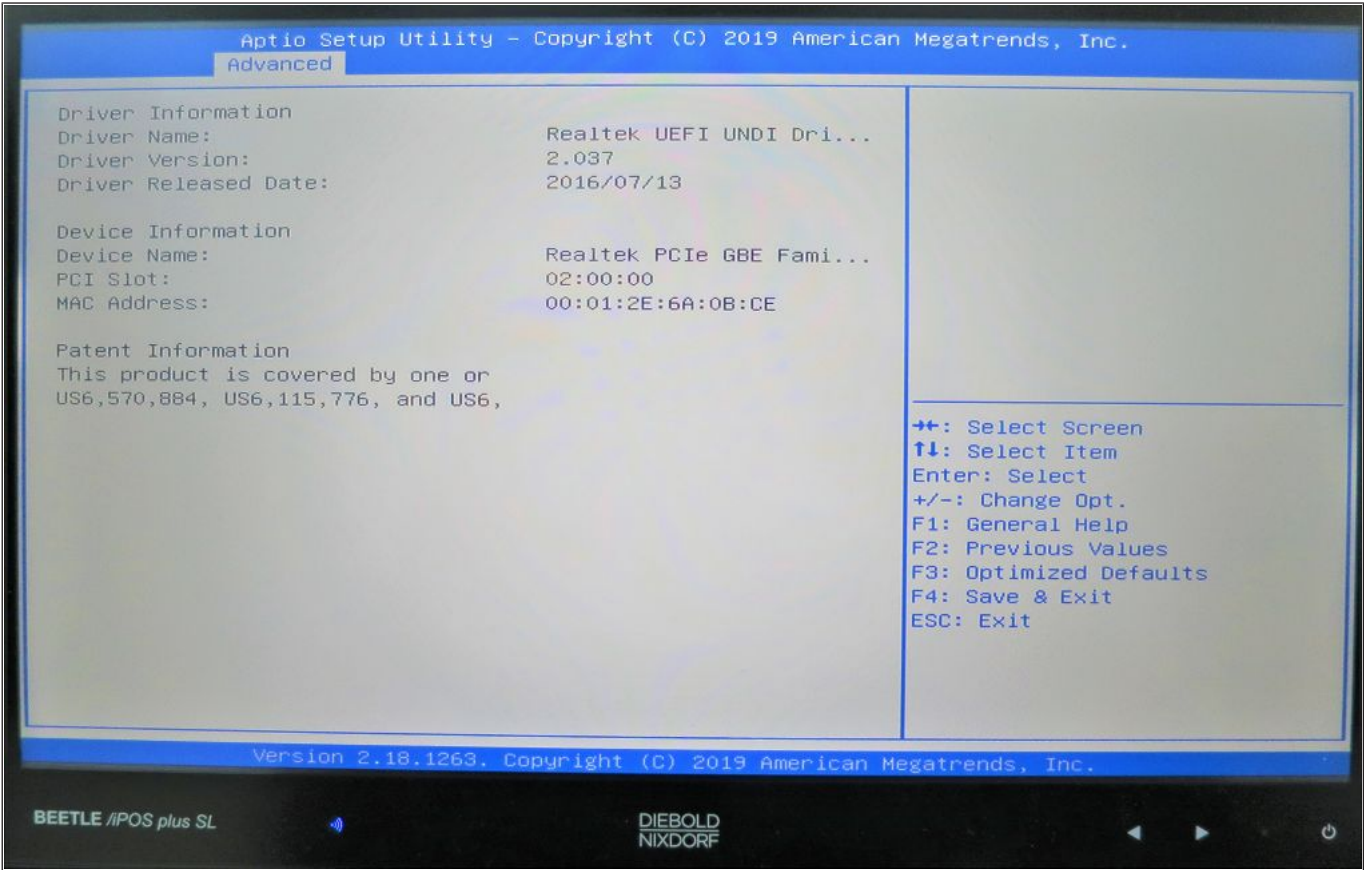
System Date:	To set the date, use tab switch between date elements. Press numeric keys to enter.
System Time:	To set the time, use tab switch between time elements. Press numeric keys to enter.

7.1.3 Advanced

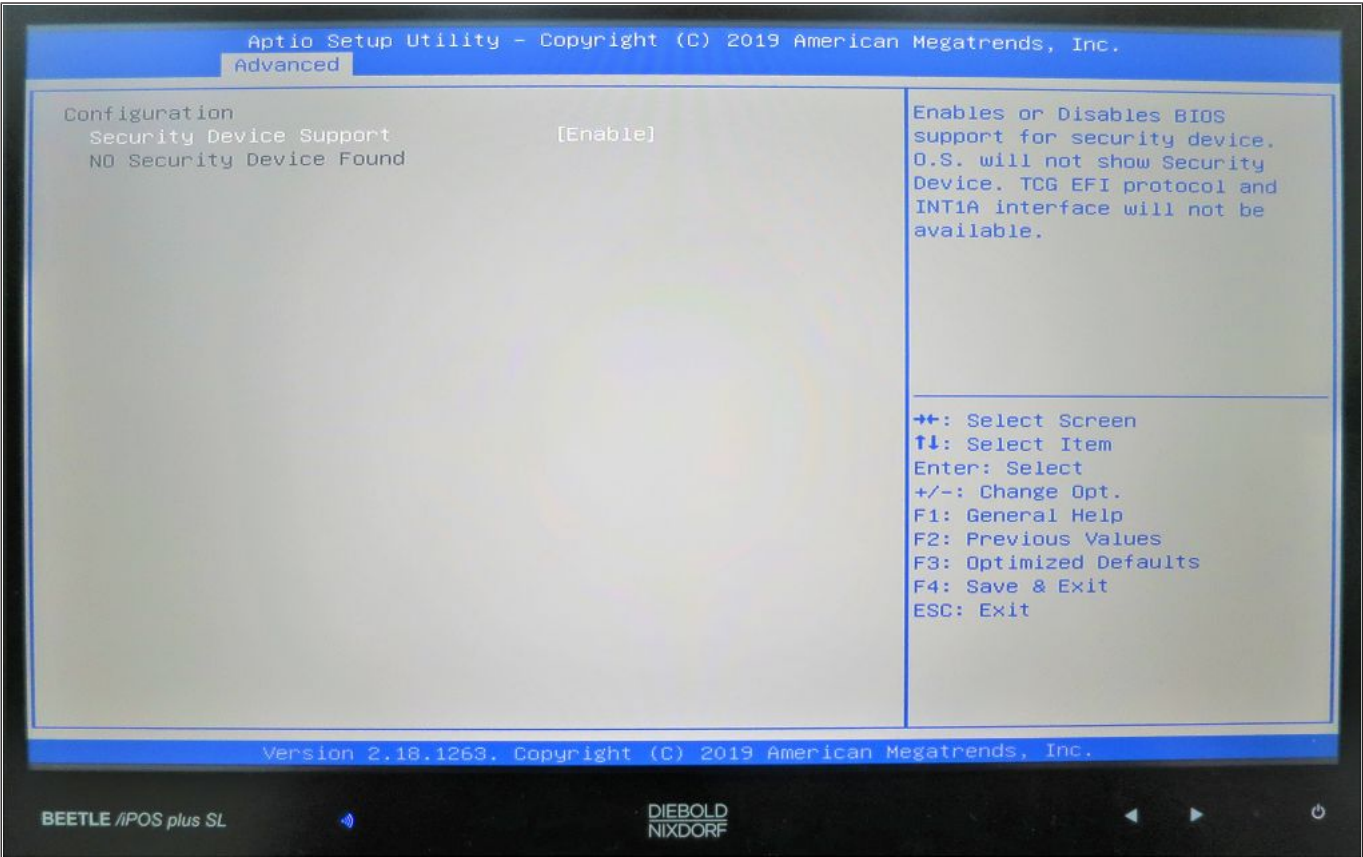


The Advanced function in the system can be configured in this menu for advanced system configuration. Only change the default settings if required for a special purpose. Incorrect settings can cause malfunction.

7.1.3.1 Realtek PCIe GBE Family Controller

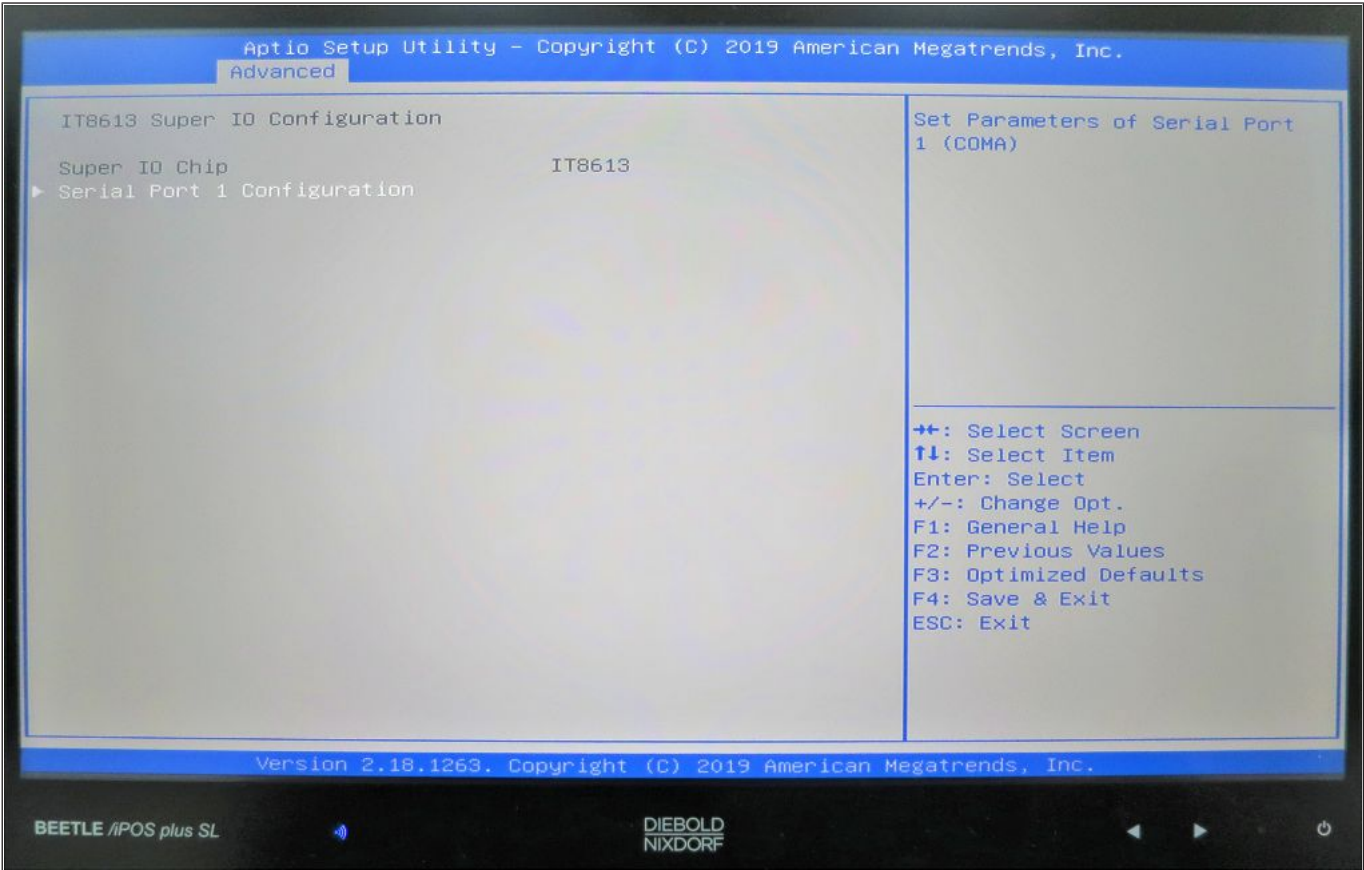


7.1.3.2 Trusted Computing

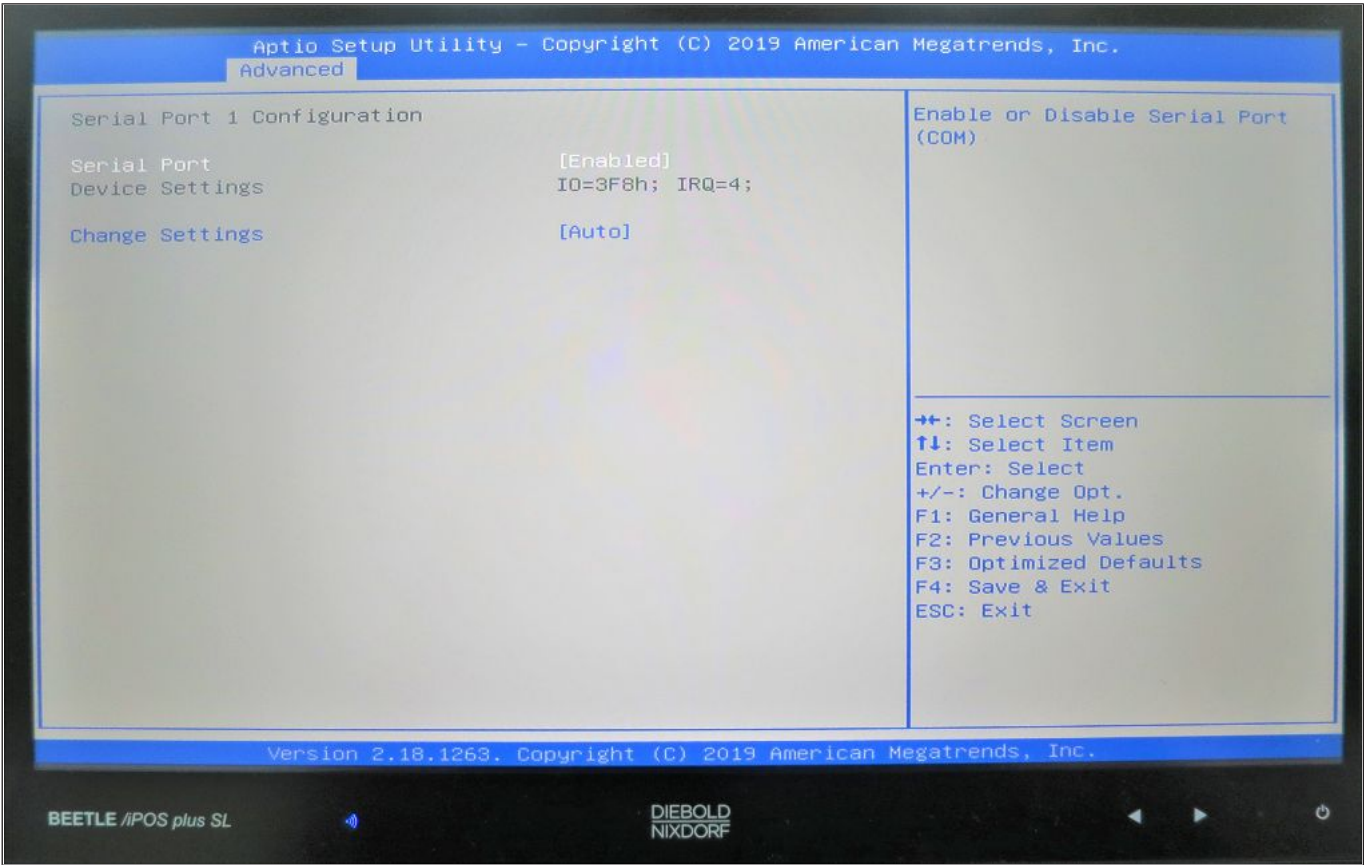


Secure Device Support:	Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.
------------------------	---

7.1.3.3 IT8613 Super IO Configuration

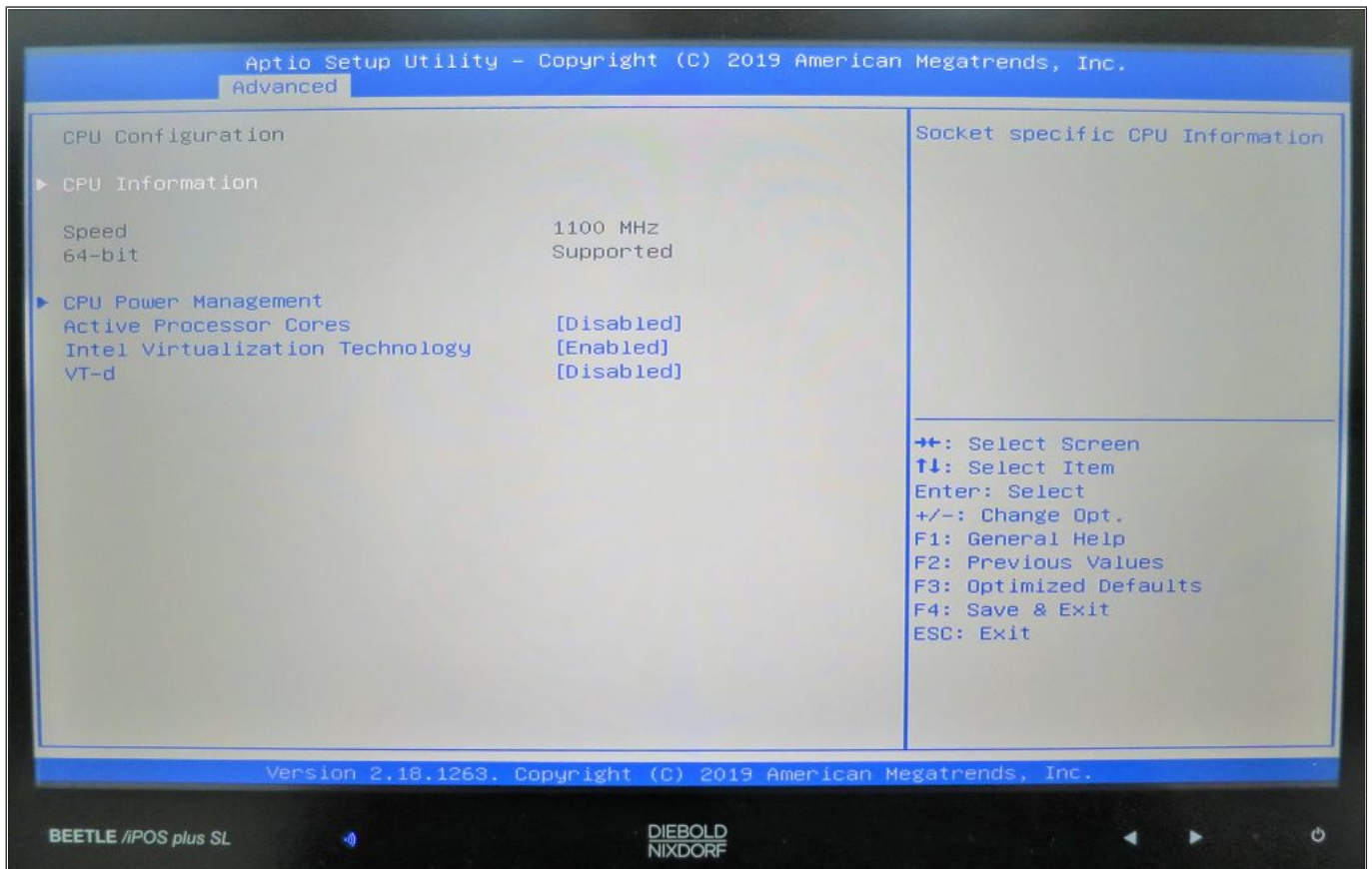


IT8613 Super IO Configuration -> Serial Port 1 Configuration:



Serial Port:	Enable or Disable Serial Port (COM).
--------------	--------------------------------------

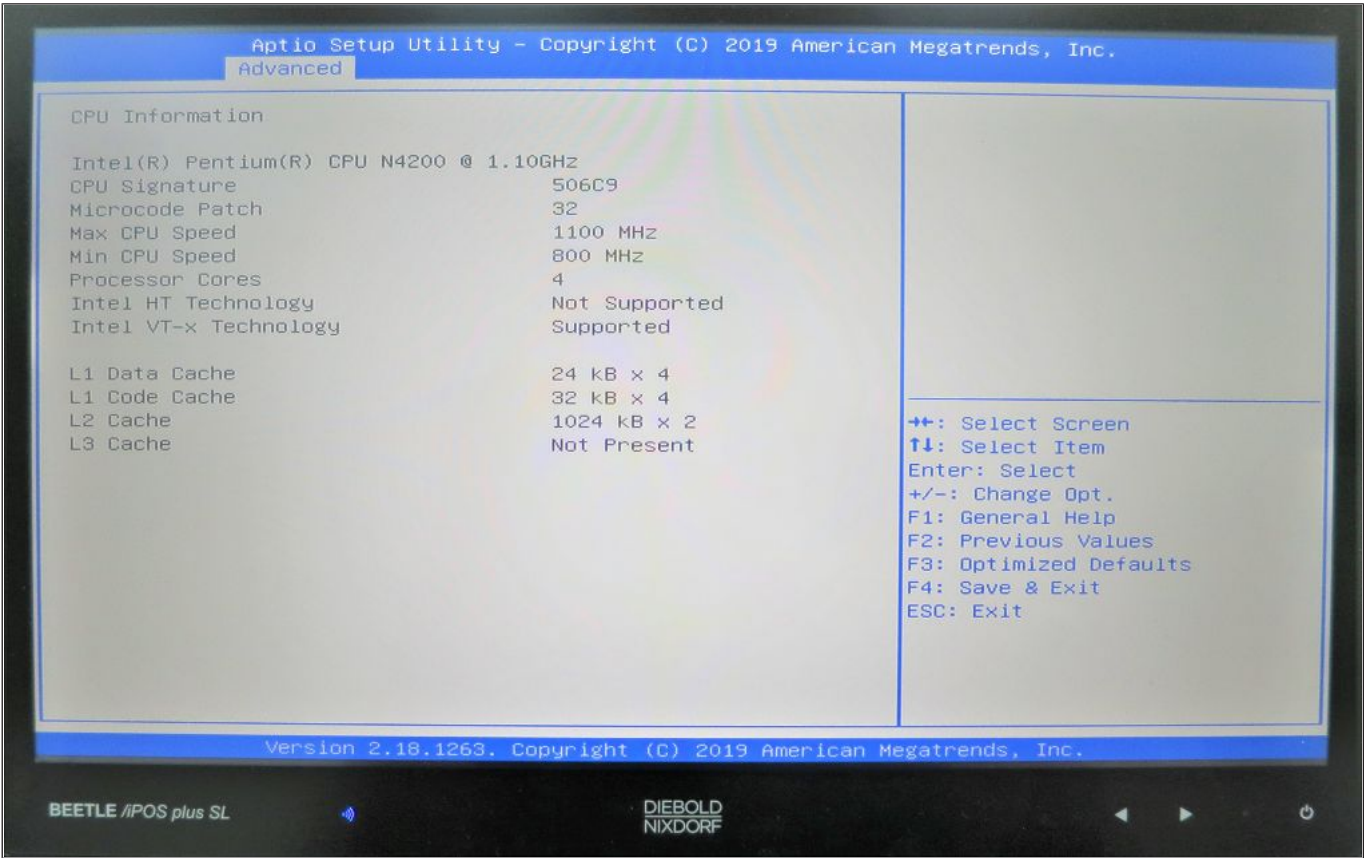
7.1.3.4 CPU Configuration



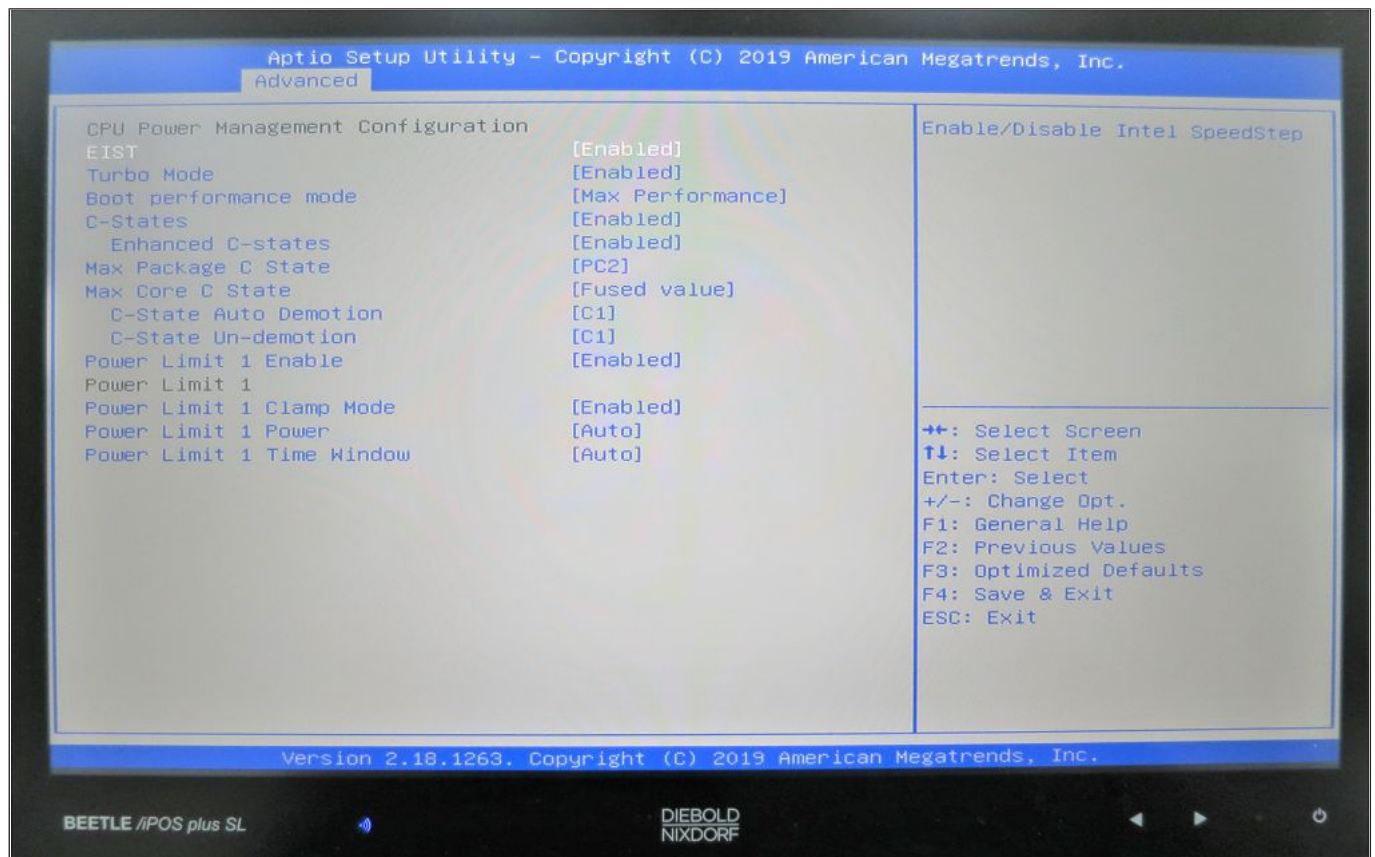
Some of the parameters in the CPU Configuration submenu are only available under certain conditions.

Active Processor Cores:	Enable/Disable Active Processor Cores
Intel Virtualization Technology	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.
VT-d:	Intel® Virtualization Technology for Directed I/O (VT-d) continues from the existing support for IA-32 (VT-x) and Itanium® processor (VT-i) virtualization adding new support for I/O-device virtualization. Intel VT-d can help end users improve security and reliability of the systems and also improve performance of I/O devices in virtualized environments.

CPU Configuration -> CPU Information



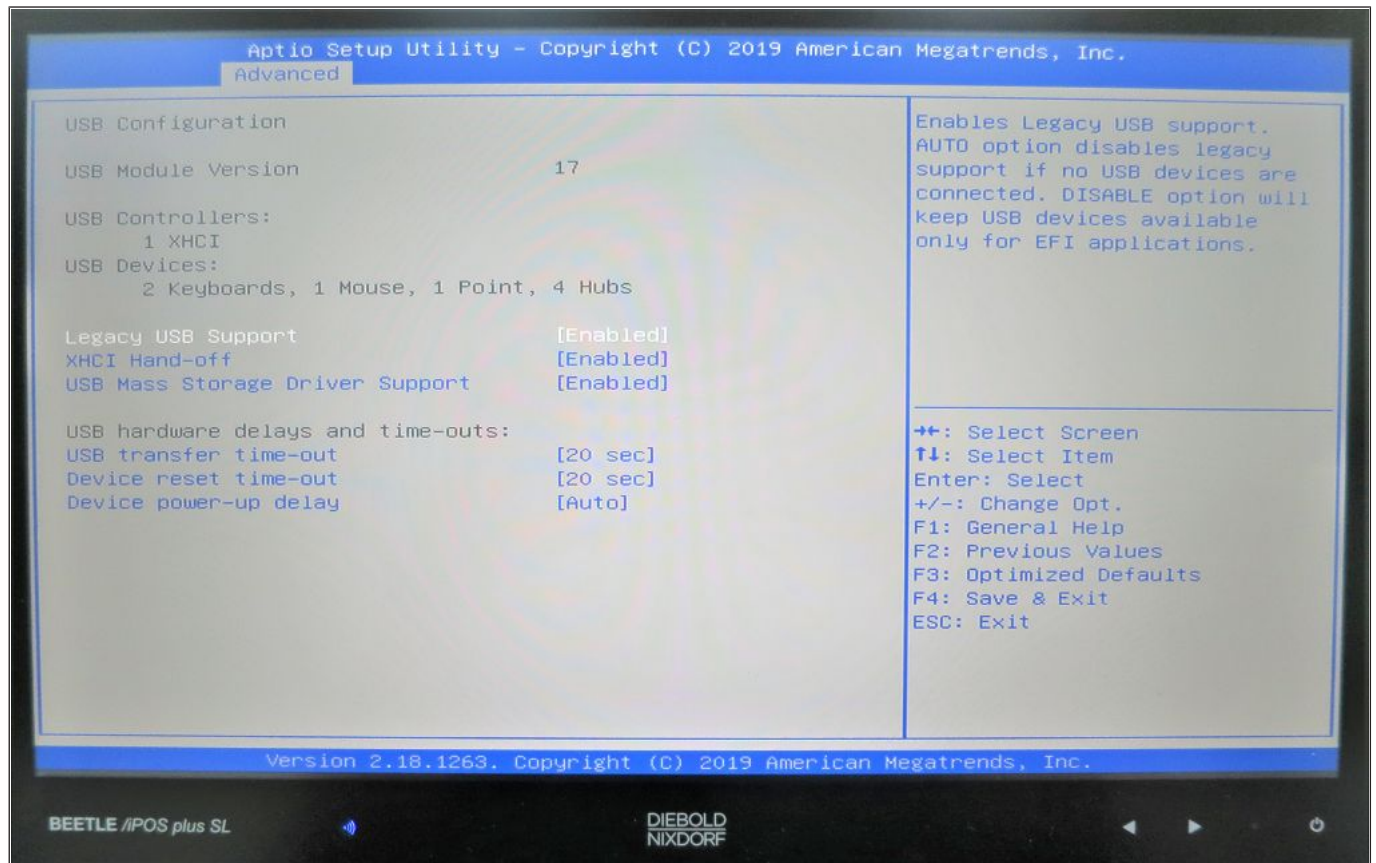
CPU Configuration -> CPU Power Management Configuration



EIST:	Enhanced Intel SpeedStep® Technology for enabling high performance while meeting the power-conservation.
Turbo Mode:	Enable/Disable processor Turbo Mode (also requires EMTTM enabled.) AUTO means enabled, unless max. turbo ratio is bigger than 16 – SKL AO W/A.
Boot Performance Mode:	Selects the performance state that the BIOS will set starting from reset vector.
C-States: Enhanced C-States:	When the processor is idle, low-power idle states (C-States) are used to save power. More power savings actions are taken for numerically higher C-states.
Max Package C State:	The processor supports C0, C2, C3, C6, C7, C8, C9 and C10 package states. A package C-state request is determined by the lowest numerical processor IA core C-state amongst all processor IA cores.
Max Core C State: C-State Auto Demotion: C-State Un-demotion:	Deeper C-states, such as C6 and C7, have long latencies and have higher energy entry/exit costs. To increase residency and improve idle power in deeper C-states, the processor supports C-state auto-demotion.
Power Limit 1 Enable:	Enable/Disable Power Limit 1 programming. If this option is enabled, it activates the PL1 value to be used by the processor to limit the average power of given time window.

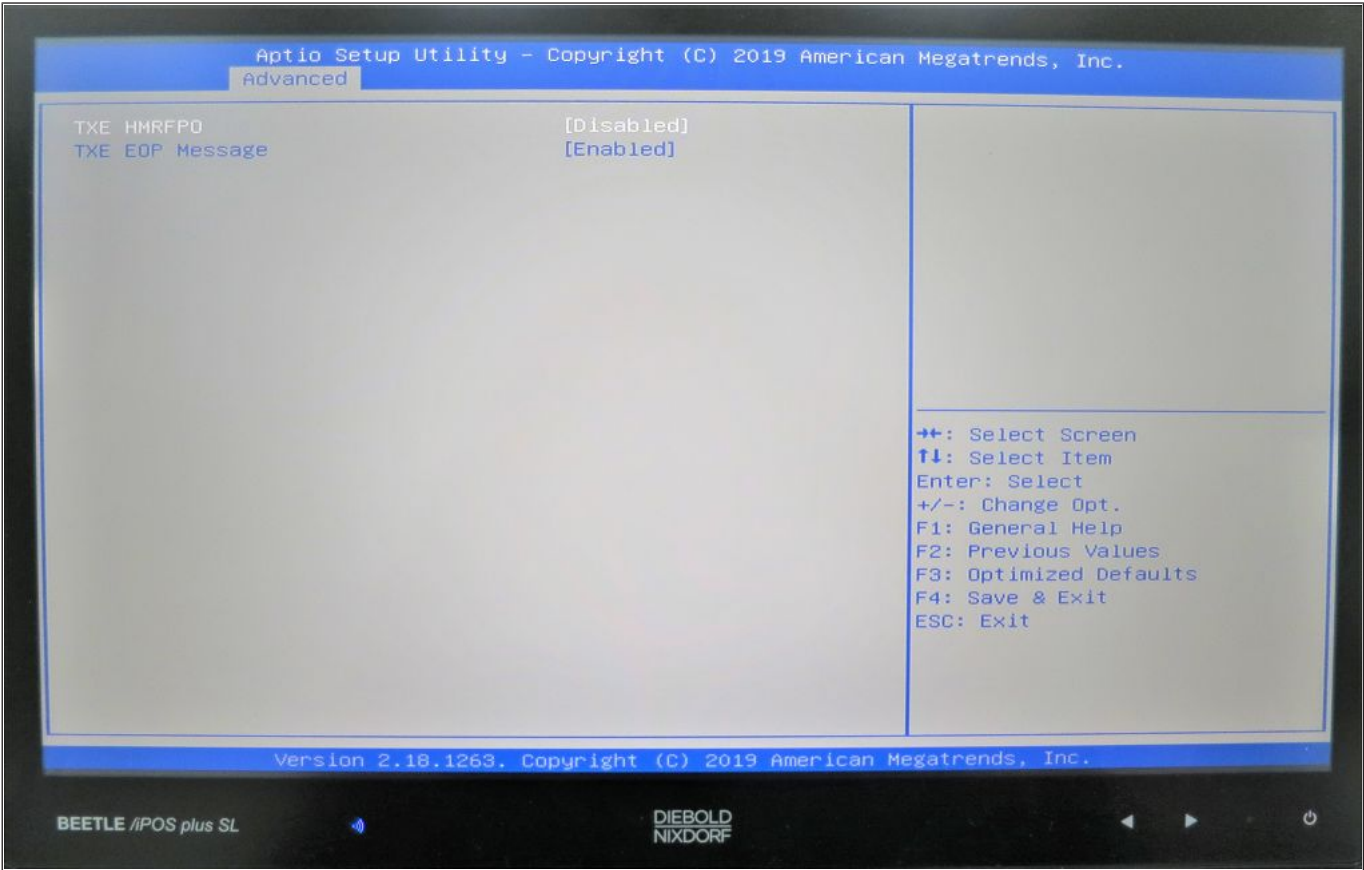
Power Limit 1 Clamp Mode:	Enable/Disable Power Limit 1 Clamp Mode
Power Limit 1 Power:	A threshold for average platform power that will not be exceeded.
Power Limit 1 Time Window:	An averaging constant used for PL1 exponential weighted moving average (EWMA) power calculation.

7.1.3.5 USB Configuration



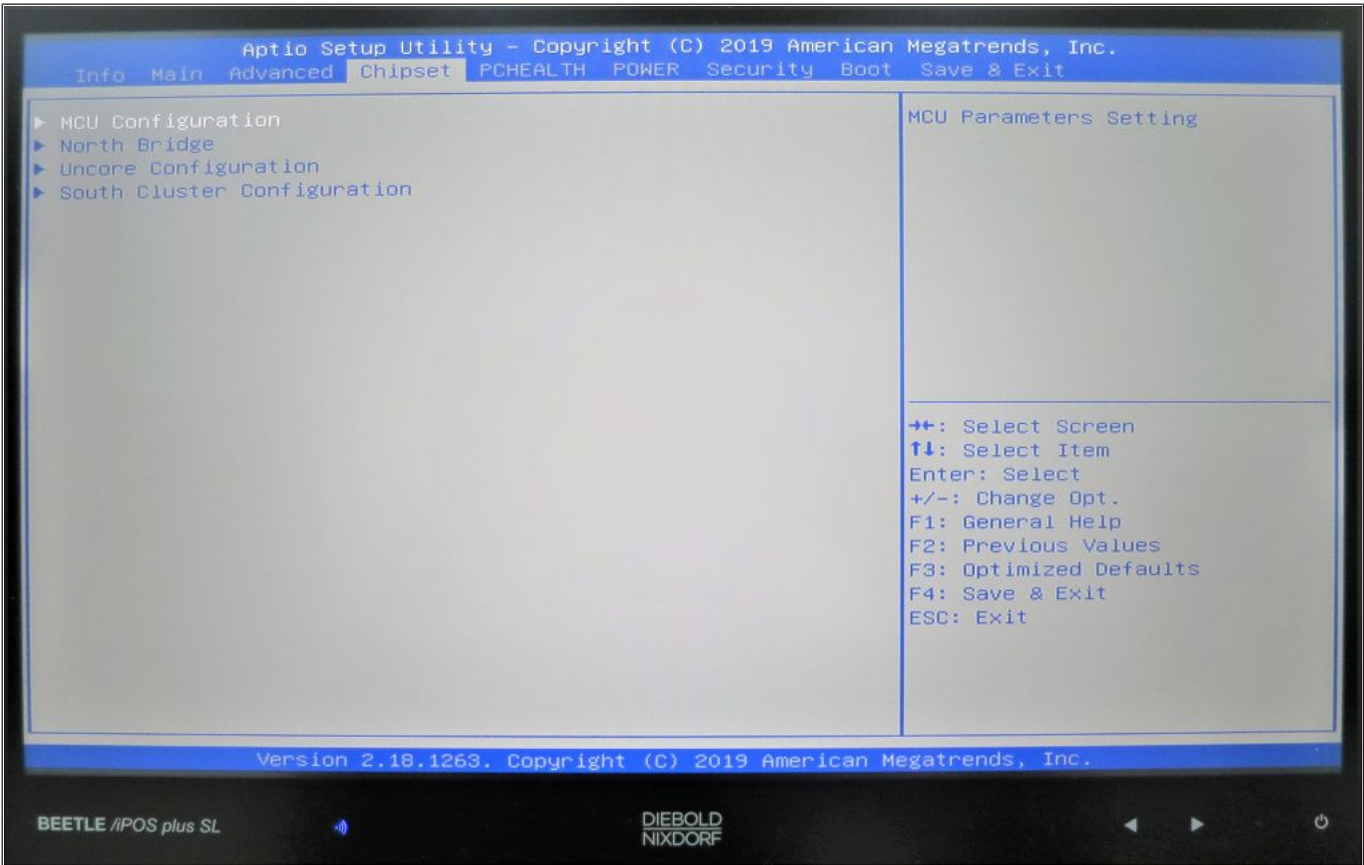
Legacy USB Support:	Enables Legacy USB Support. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications.
XHCI Hand-off:	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be 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:	USB mass storage device Start Unit command time-out.
Device power-up delay	Maximum time the device will take before it properly reports itself to the Host Controller. AUTO uses default value: for a Root port, it is 100 ms. For a Hub port, the delay is taken from Hub descriptor.

7.1.3.6 Security Configuration

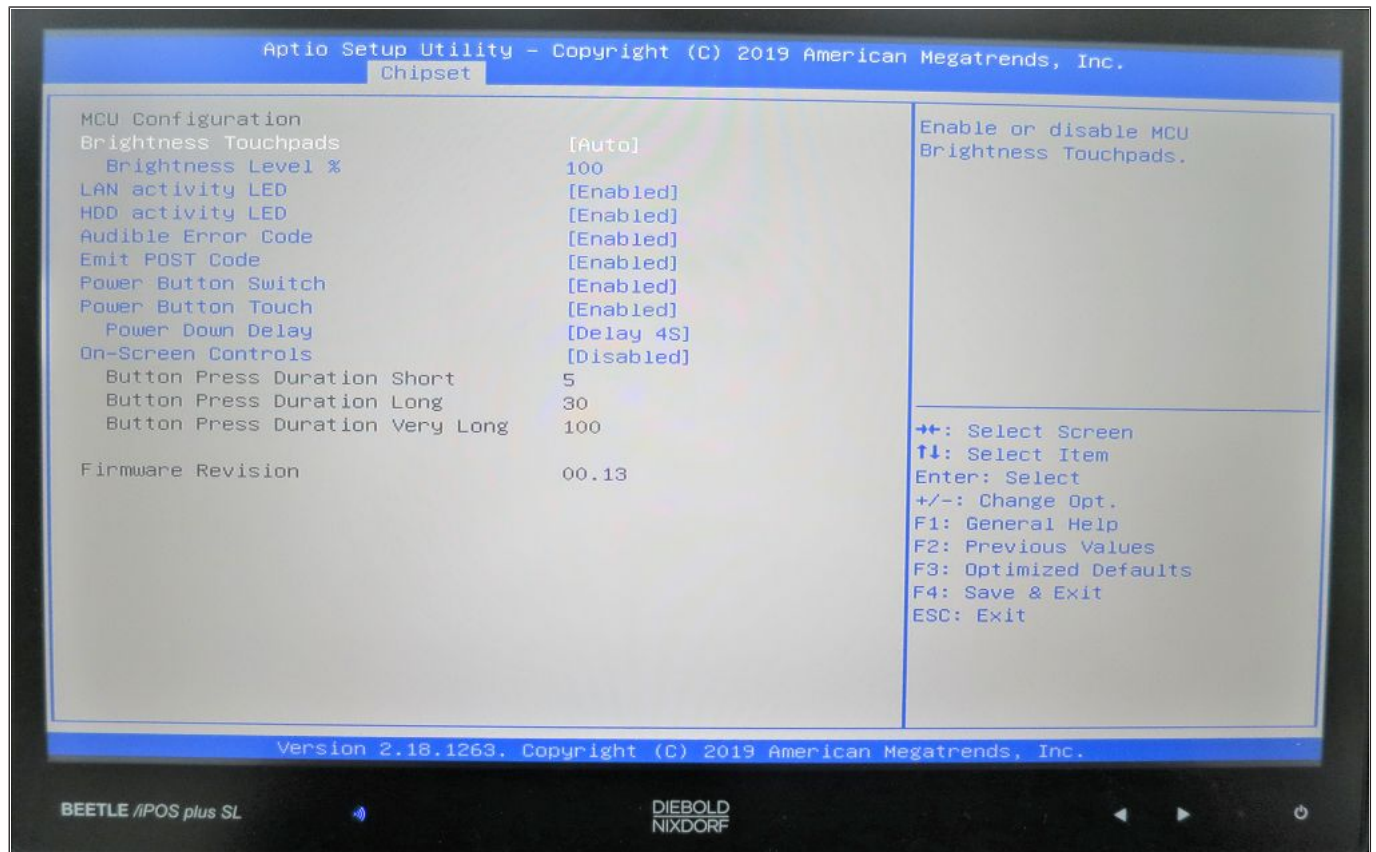


TXE MMRFPD:	Intel Trusted Execution Engine Host ME Region Flash Protection Override.
TXE EOP Message:	Intel Trusted Execution Engine - for testing EOP (End of Post).

7.1.4 Chipset

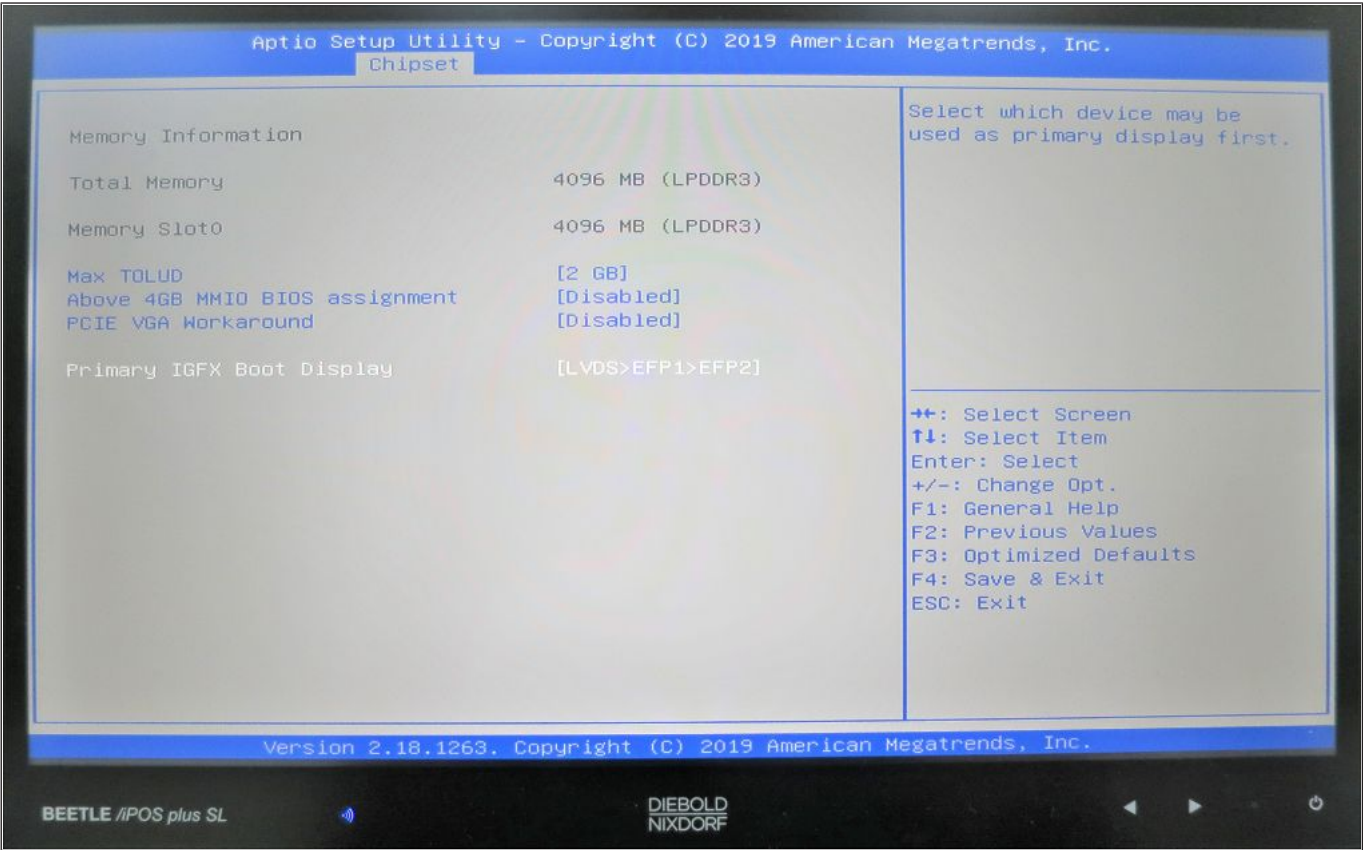


7.1.4.1 MCU Configuration



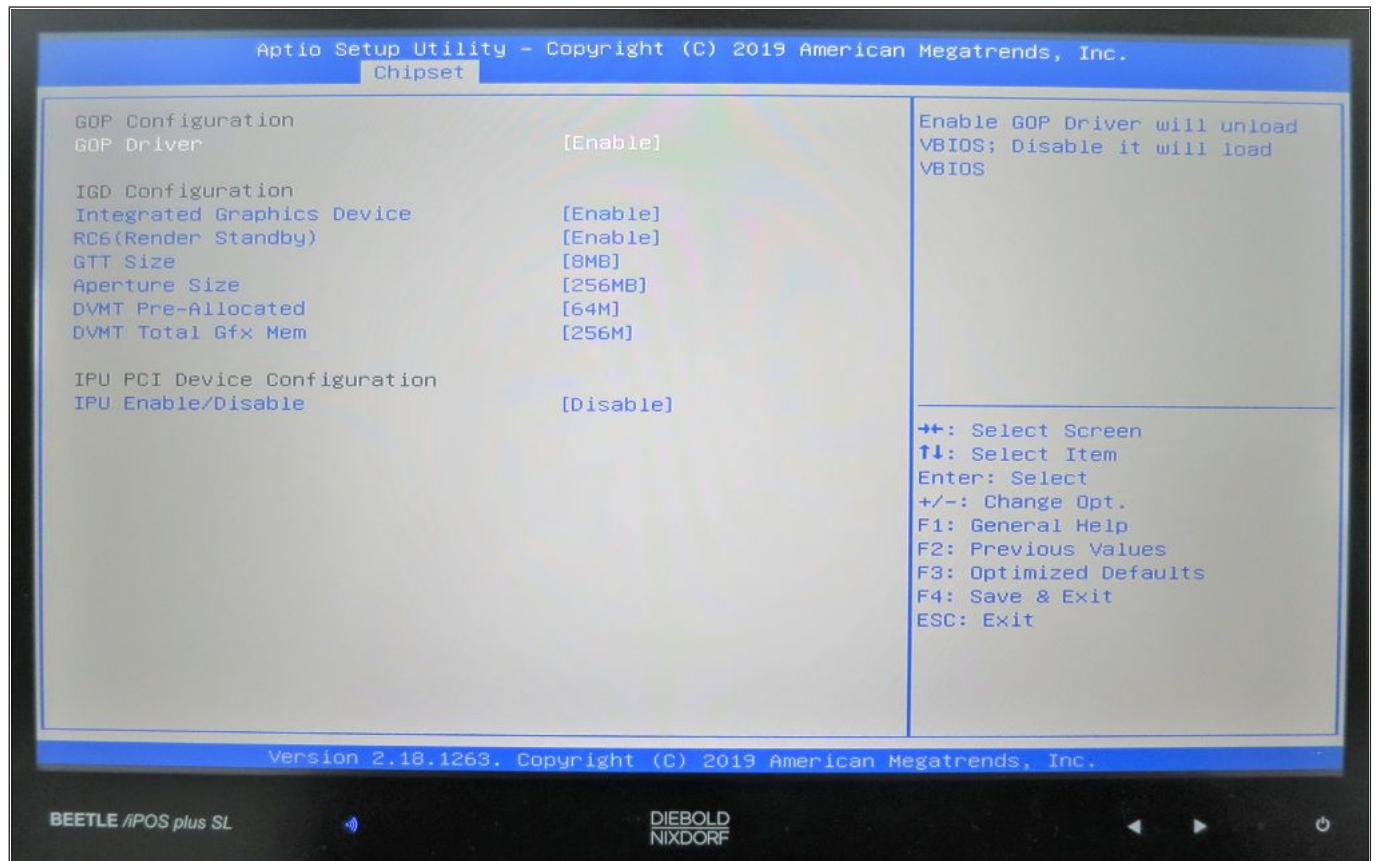
Brightness Touchpads:	Enable or Disable MCU Brightness Touchpads.
Brightness Level %:	Brightness Level Control, Value 10-100.
LAN activity LED:	Enable or Disable MCU LAN activity LED.
HDD activity LED:	Enable or Disable HDD activity LED.
Audible Error Code:	Emit error code using the system beeper/speaker
Emit POST Code:	Emit 8-bit BIOS POST code starting from MSB. Long blink/beep represent "1", short blink/beep represent "0"
Power Button Switch:	Enable or Disable the Power Button Switch.
Power Button Touch:	Enable or Disable the Power Button Touch.
Power Down Delay:	Power Button Power Down mode.
On-screen Controls:	To enable On-screen control.

7.1.4.2 North Bridge



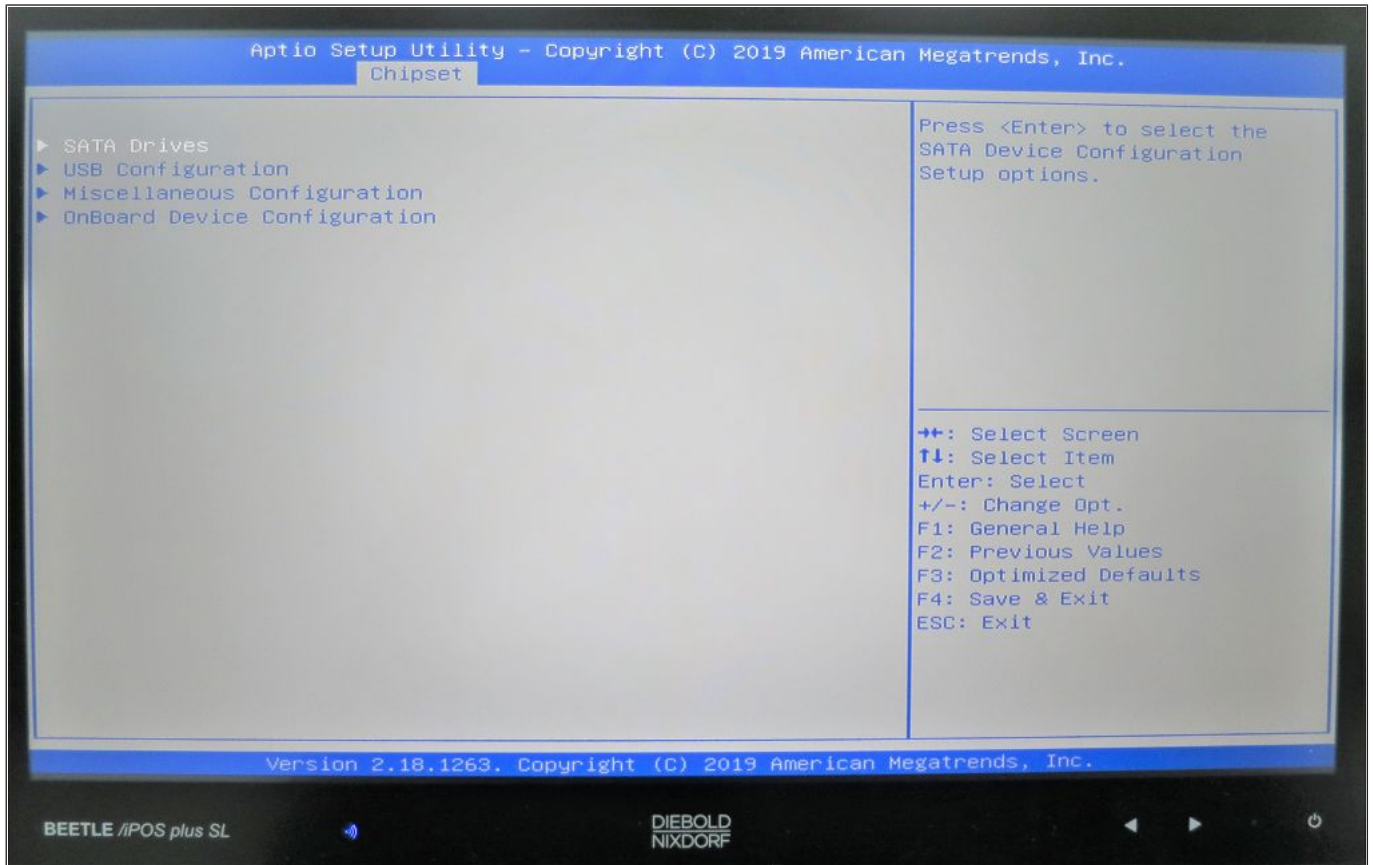
Max TOLUD:	Sets the Top Of Lower Usable DRAM.
Above 4GB MMIO BIOS assignment:	Enable high MMIO (above 4GB).
PCIE VGA Workaround:	Enable/Disable PCIE VGA Workaround.
Primary IGFX Boot Display:	Select which device may be used as primary display first.

7.1.4.3 Uncore Configuration

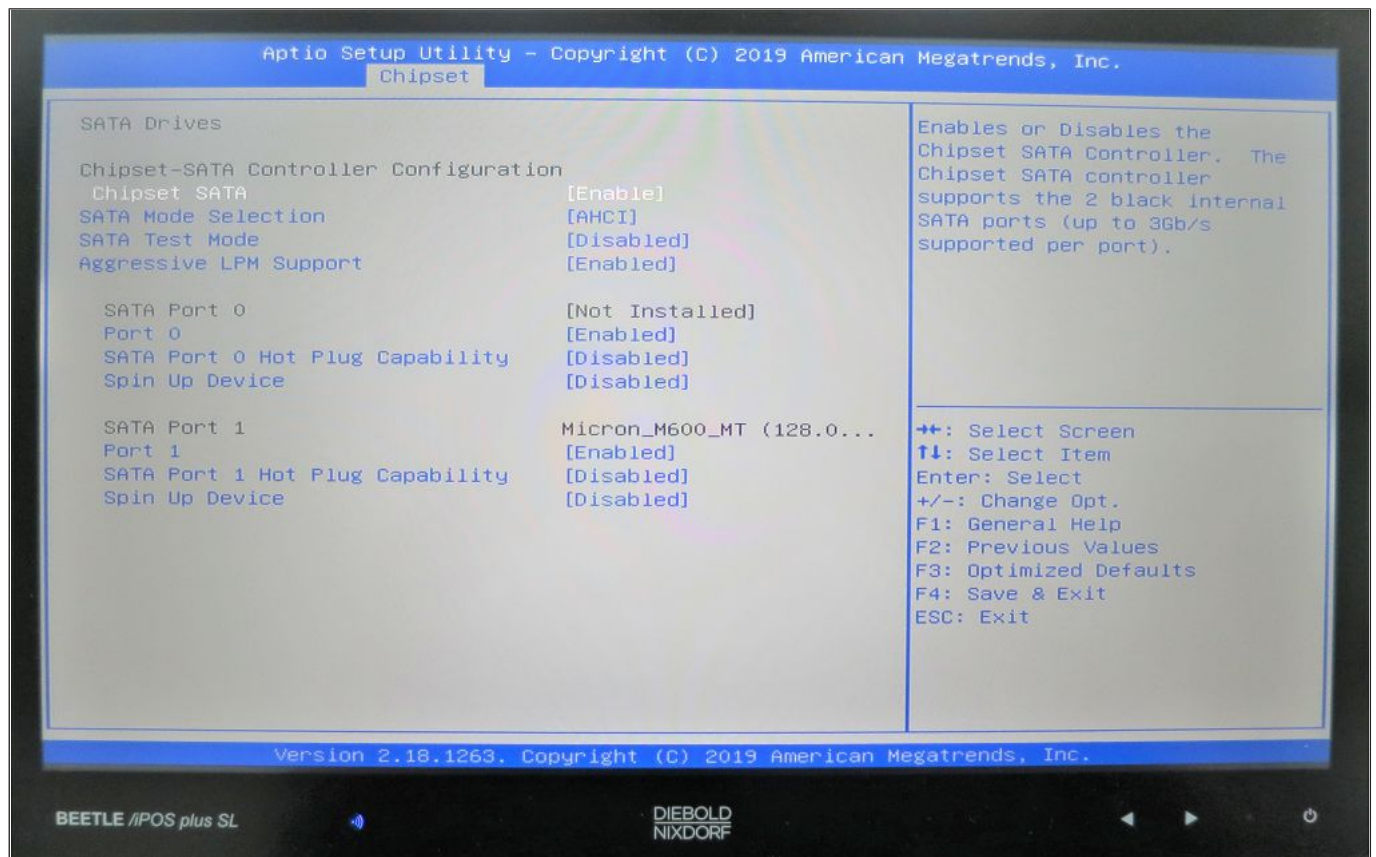


GOP Driver:	Enable/Disable GOP Driver.
Integrated Graphics Device:	Enable/Disable Integrated Graphics Device.
RC6 (Render Standby):	Enable/Disable RC6 (Render Standby).
GTT Size:	Select GTT Size.
Aperture Size:	Select the Aperture Size. Note: Above 4GB MMIO BIOS assignment is automatically enabled when selecting 2048MB aperture. To use this feature, please disable CSM Support.
DVMT Pre-Allocated:	Select DVMT Pre-Allocated size..
DVMT Total Gfx Mem:	Select DVMT5.0 Total Graphic Memory size used by the Internal Graphics Device.
IPU Enable/Disable:	Enable/Disable IPU.

7.1.4.4 South Cluster Configuration

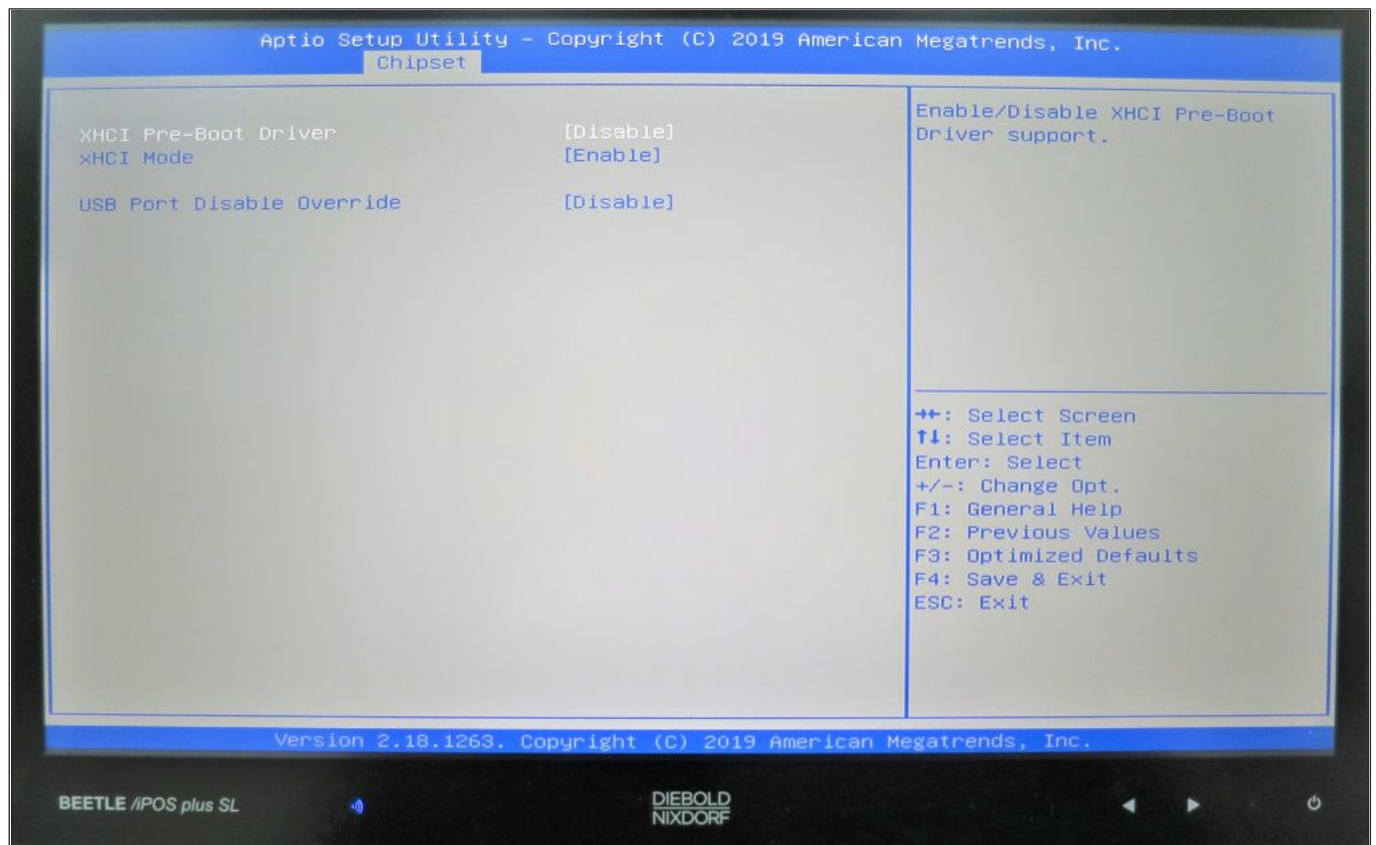


South Cluster Configuration -> SATA Drives



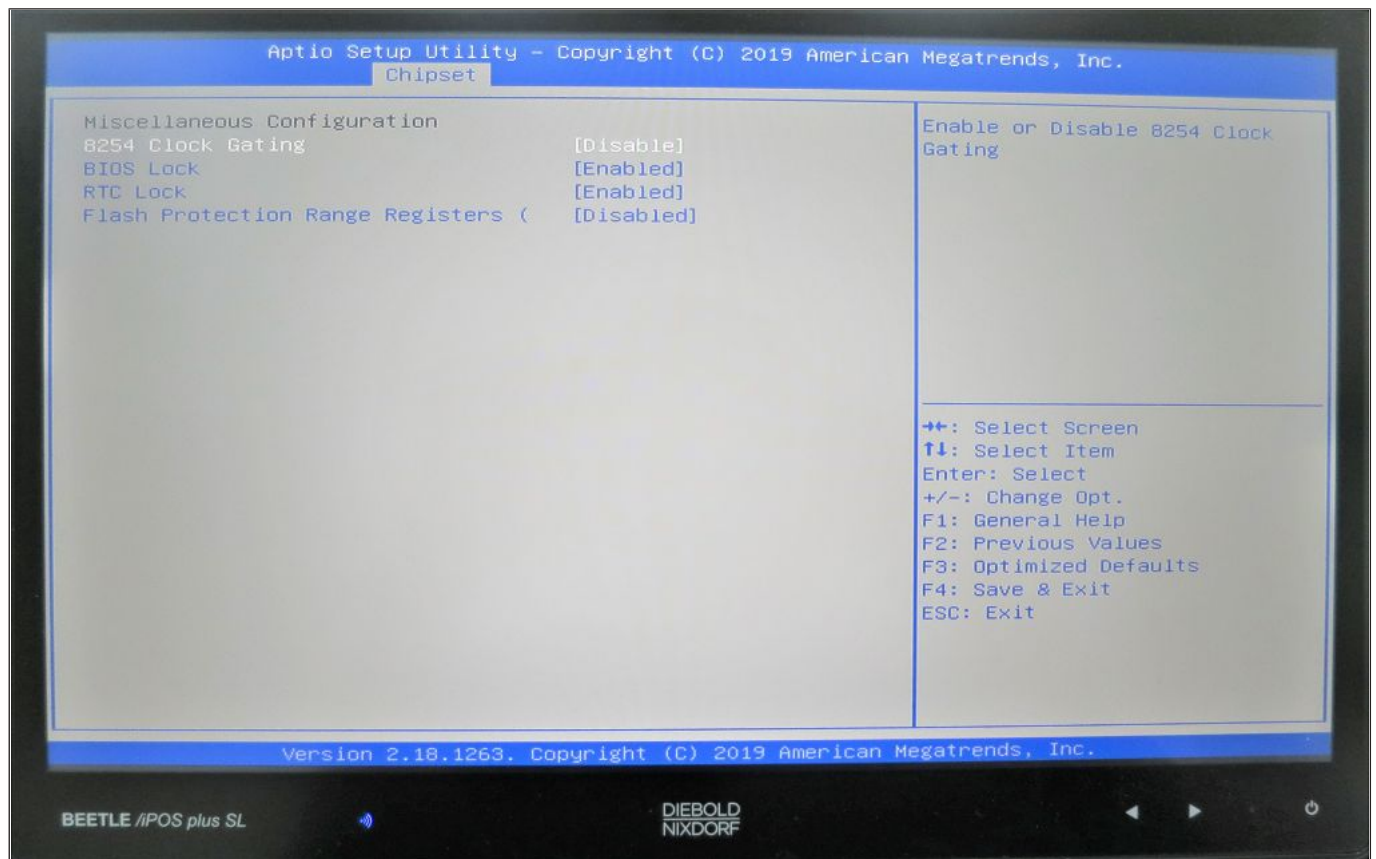
Chipset SATA:	Enable/Disable Chipset SATA.
SATA Mode Selection:	Determines how SATA controller operates.
SATA Test Mode:	Enable/Disable SATA Test Mode.
Aggressive LPM Support:	Enable/Disable Aggressive LPM Support.
Port 0:	Enable/Disable Port 0.
SATA Port 0 Hot Plug Capability:	Enable/Disable SATA Port 0 Hot Plug Capability.
Spin Up Device:	If enabled for any of ports Staggered Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
Port 1:	Enable/Disable Port 1.
SATA Port 1 Hot Plug Capability:	Enable/Disable SATA Port 1 Hot Plug Capability.

South Cluster Configuration -> USB Configuration



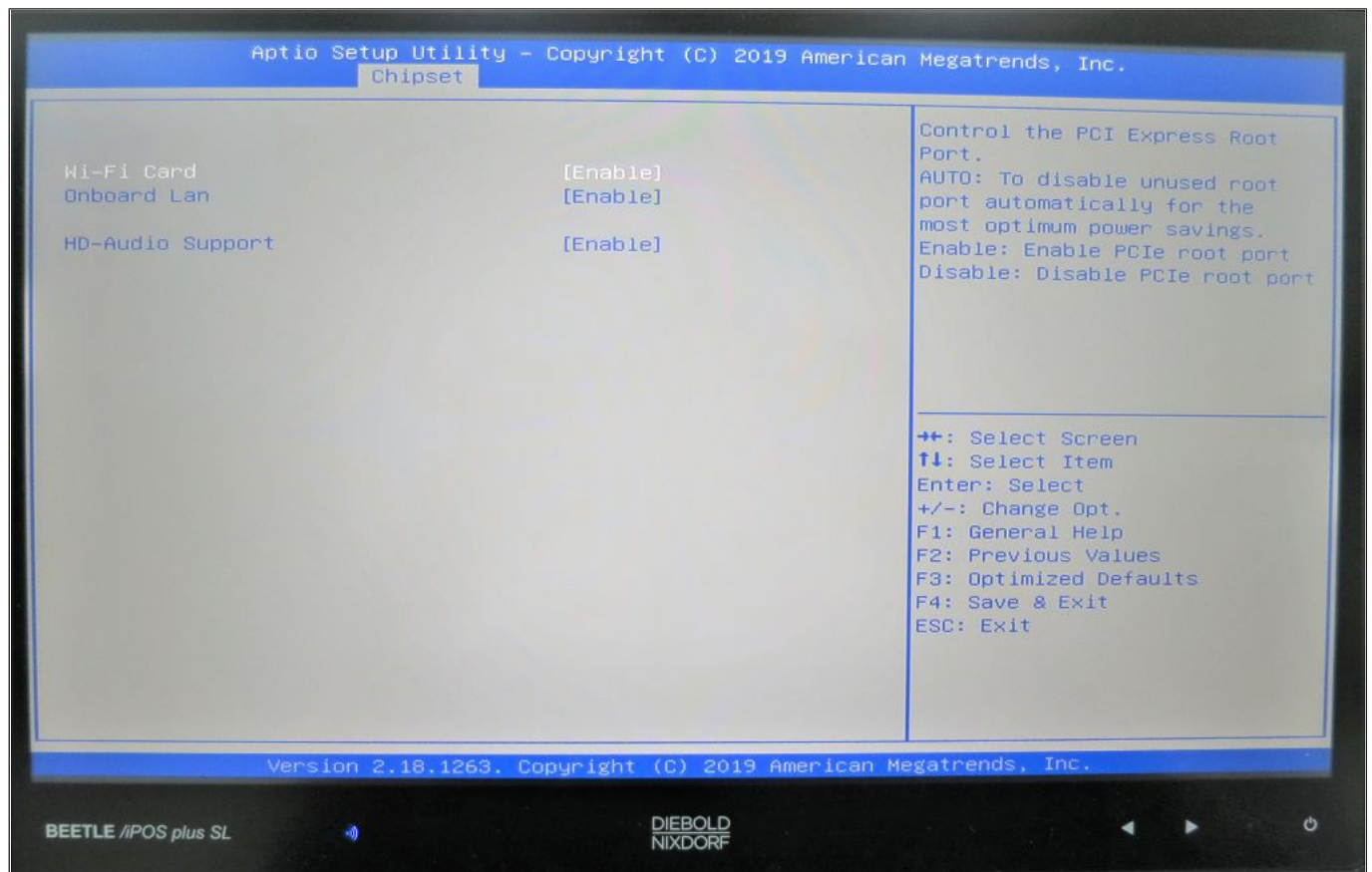
XHCI Pre-Boot Driver:	Enable/Disable XHCI Pre-Boot Driver .
xHCI Mode:	Enable/Disable xHCI Mode
USB Port Disable Override:	Enable/Disable USB Port Disable Override.

South Cluster Configuration -> Miscellaneous Configuration



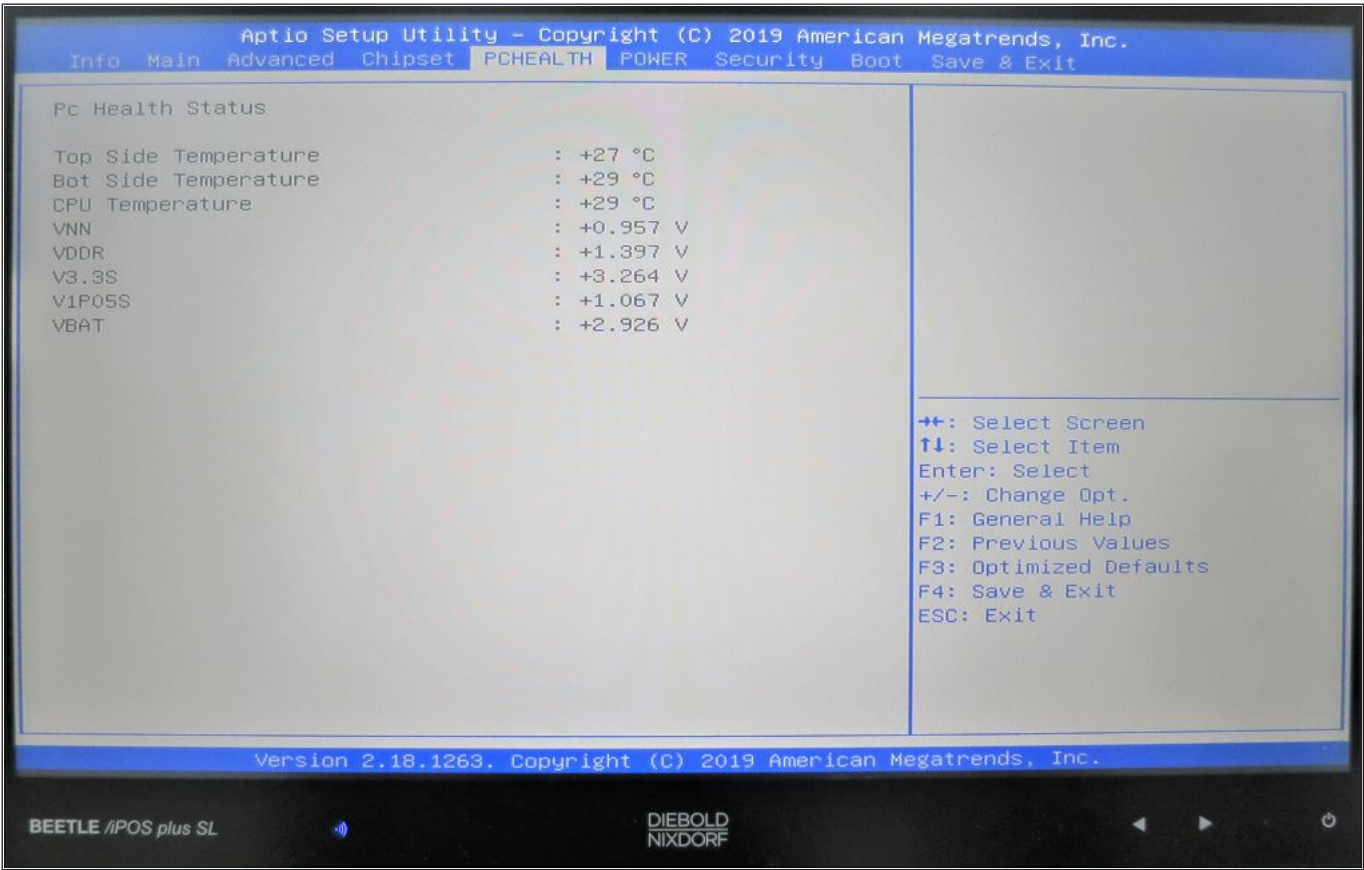
8254 Clock Gating:	Enable/Disable 8254 Clock Gating.
BIOS Lock:	Enable/Disable the PCH BIOS Lock Enable feature. Required to be enabled to ensure SMM protection of flash.
RTC Lock:	Enable will lock bytes 38h-3Fh in the lower/upper 128-byte bank of RTC RAM.
Flash Protection Range Registers:	Enable/Disable Flash Protection Range Registers.

South Cluster Configuration -> OnBoard Device Configuration

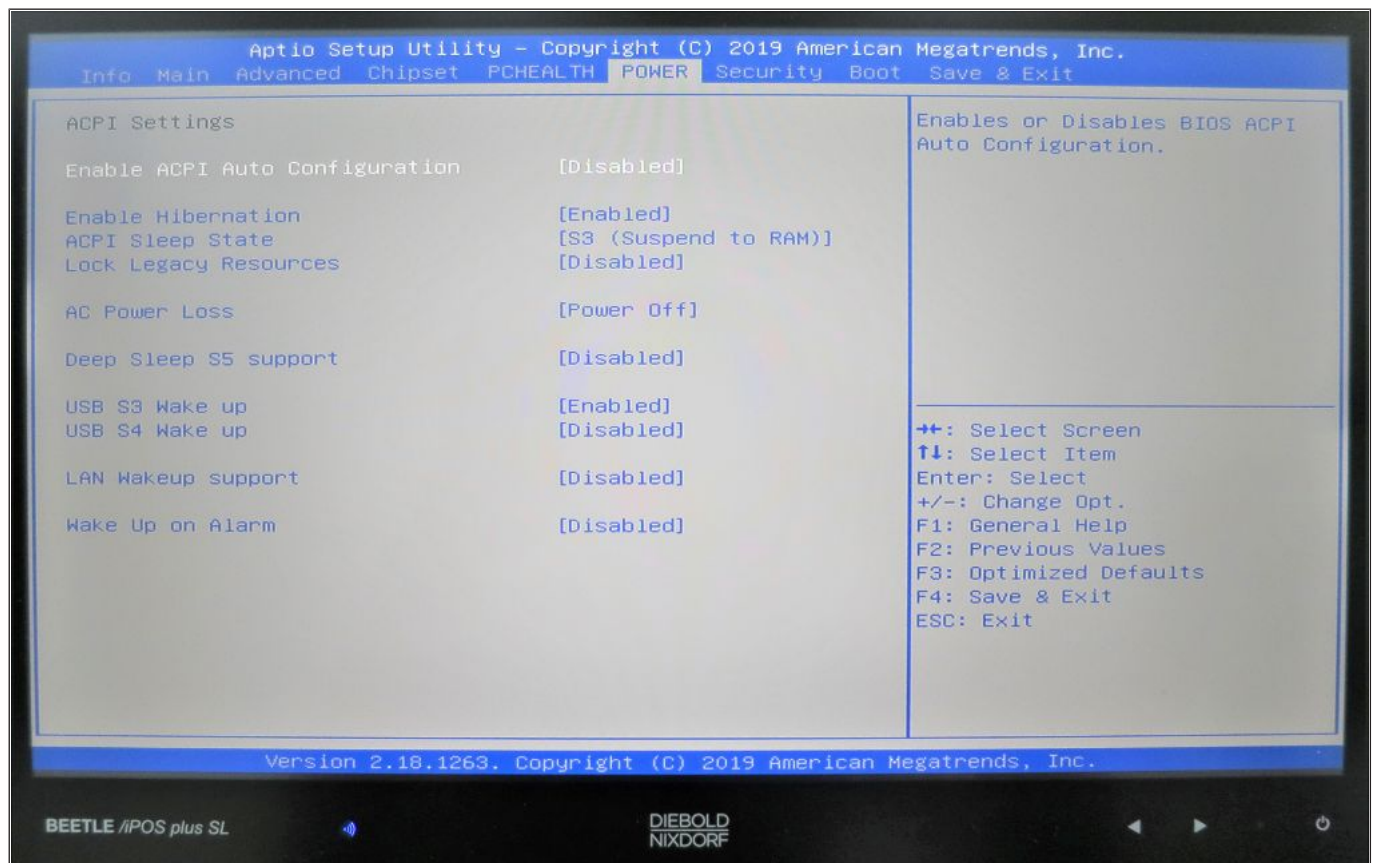


Wi-Fi Card:	Enable/Disable Wi-Fi Card.
Onboard Lan:	Enable/Disable Onboard Lan.
HD-Audio Support:	Enable/Disable HD-Audio Support.

7.1.5 PC Health

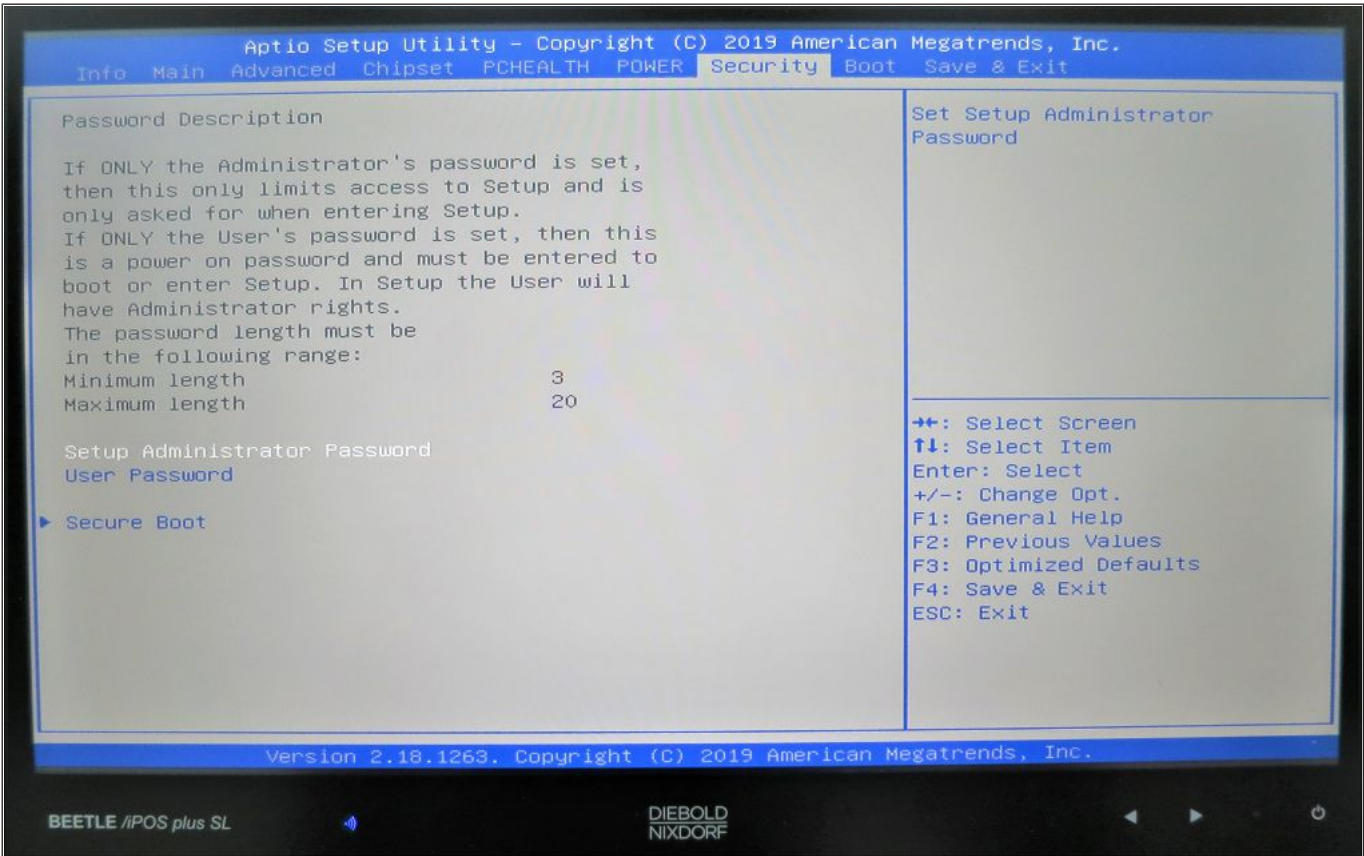


7.1.6 Power



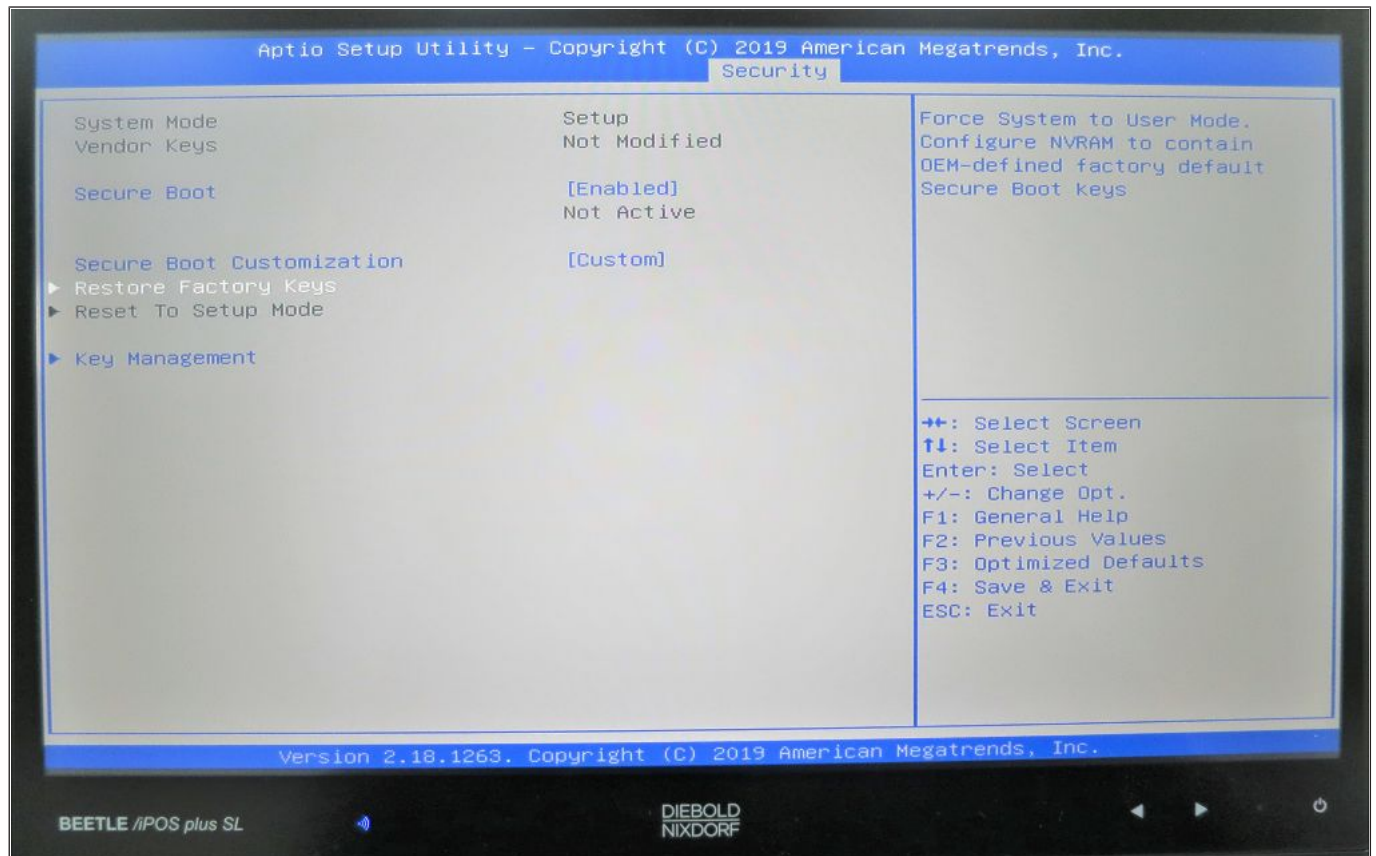
Enable ACPI Auto Configuration:	Enables or Disables BIOS ACPI Auto Configuration.
Enable Hibernation:	Enables or Disables System ability to hibernate (OS/S4 Sleep State). This option may not be effective with some OS.
ACPI Sleep State:	Select the highest ACPI Sleep State the System will enter when the SUSPEND button is pressed.
Lock Legacy Resources:	Enables or Disables Lock or Legacy Resources.
AC Power Loss:	AC Power Loss.
Deep Sleep S5 Support:	Enable/Disable Deep Sleep S5 Support.
USB S3 Wake up:	Enable/Disable USB S3 Wake up.
USD S4 Wake up:	Enable/Disable USB S4 Wake up.
LAN Wakeup support:	Enable/Disable LAN Wakeup support.
Wake Up on Alarm:	Enables or Disables System wake up on alarm event. When enabled, system will wake on the hr::min::sec specified.

7.1.7 Security



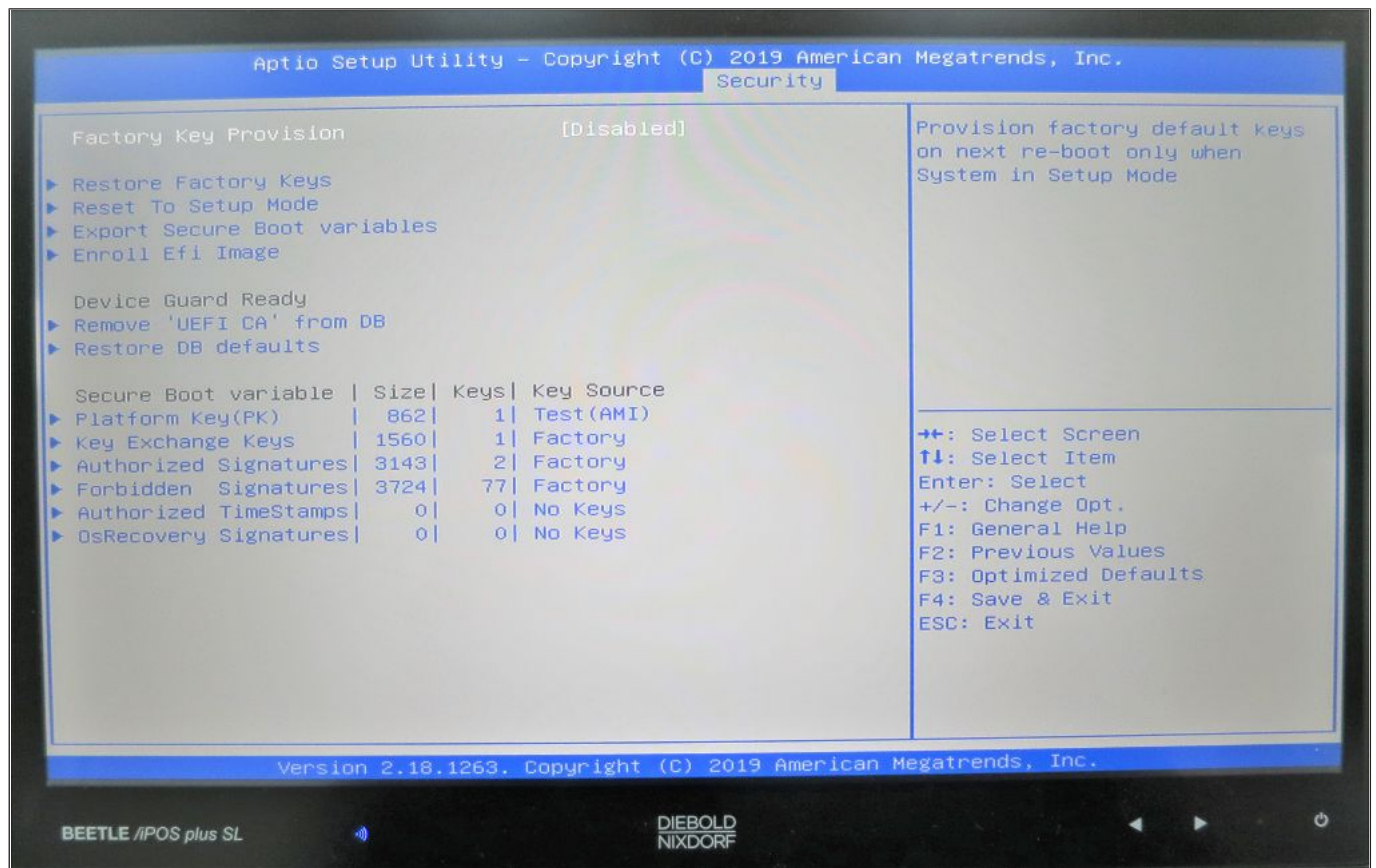
Setup Administrator Password:	Set Administrator Password.
User Password:	Set User Password.

7.1.7.1 Secure Boot



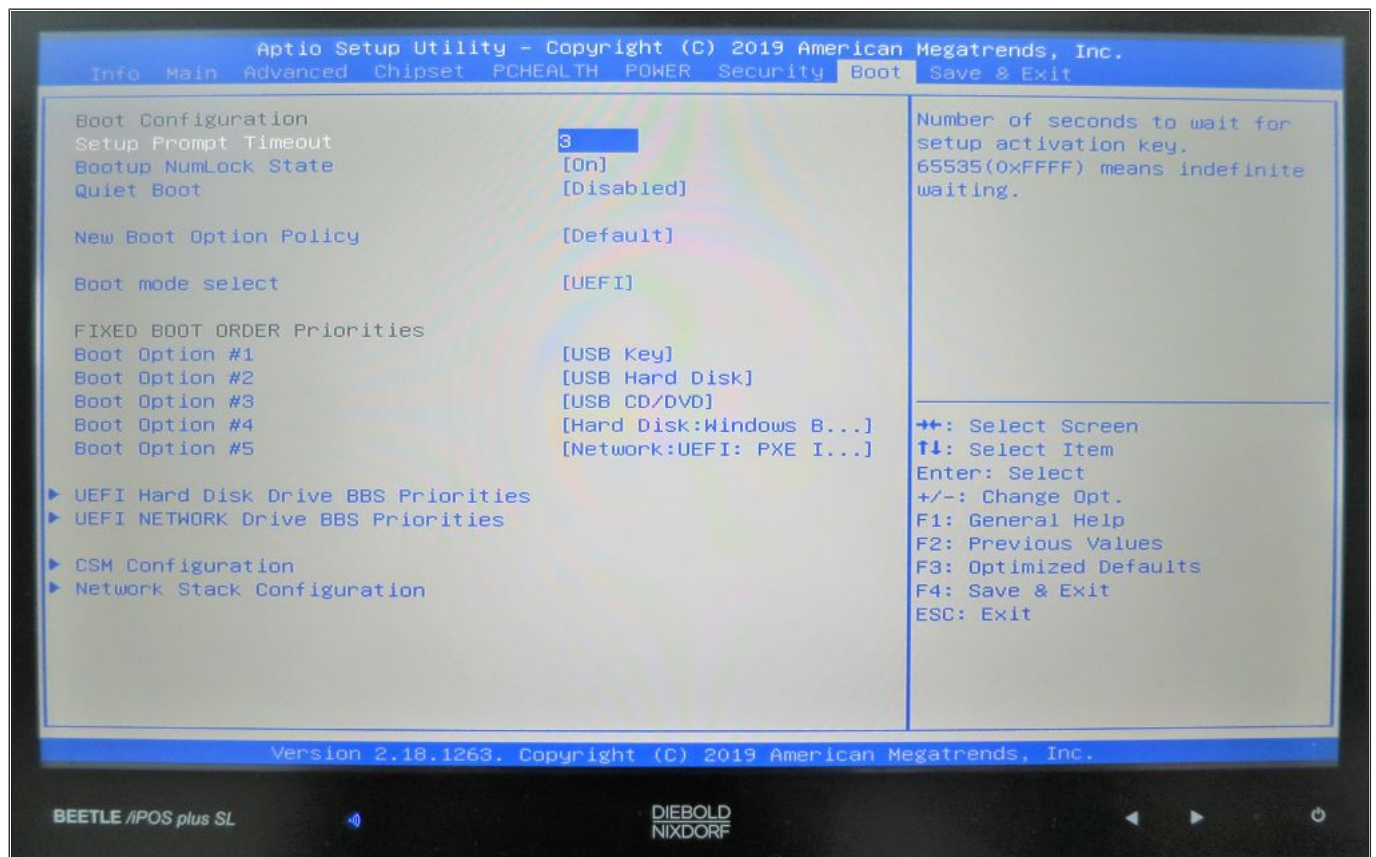
Secure Boot:	Secure Boot is activated when Platform Key (PK) is enrolled, System mode is User/Deployed, and CSM function is disabled.
Secure Boot Customization:	Customizable Secure Boot mode: In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication.
Restore Factory Keys:	Force System to User Mode. Configure NVRAM to contain OEM-defined factory default Secure Boot Keys.
Reset to Setup Mode:	Reset to Setup Mode.
Key Management:	Enables expert users to modify Secure Boot Policy variables without full authentication.

Secure Boot -> Key Management



Factory Key Provision:	Provision factory default keys on next reboot only when System is in Setup Mode.
Restore Factory Keys:	Force System to User Mode. Configure NVRAM to contain OEM-defined factory default Secure Boot Keys.
Reset to Setup Mode:	Reset to Setup Mode.
Export Secure Boot variables:	Export Secure Boot Variables.
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).
Remove 'UEFI CA' from DB:	Remove 'UEFI CA' from DB.
Restore DB defaults:	Restore DB variable to factory defaults.
Secure Boot Variables:	Enroll Factory Defaults or load certificates from a file: 1. Public Key Certificate in: a) EFI_SIGNATURE_LIST, b) EFI_CERT_X509 (DER encoded), c) EFI_CERT_RSA2048 (bin).

7.1.8 Boot



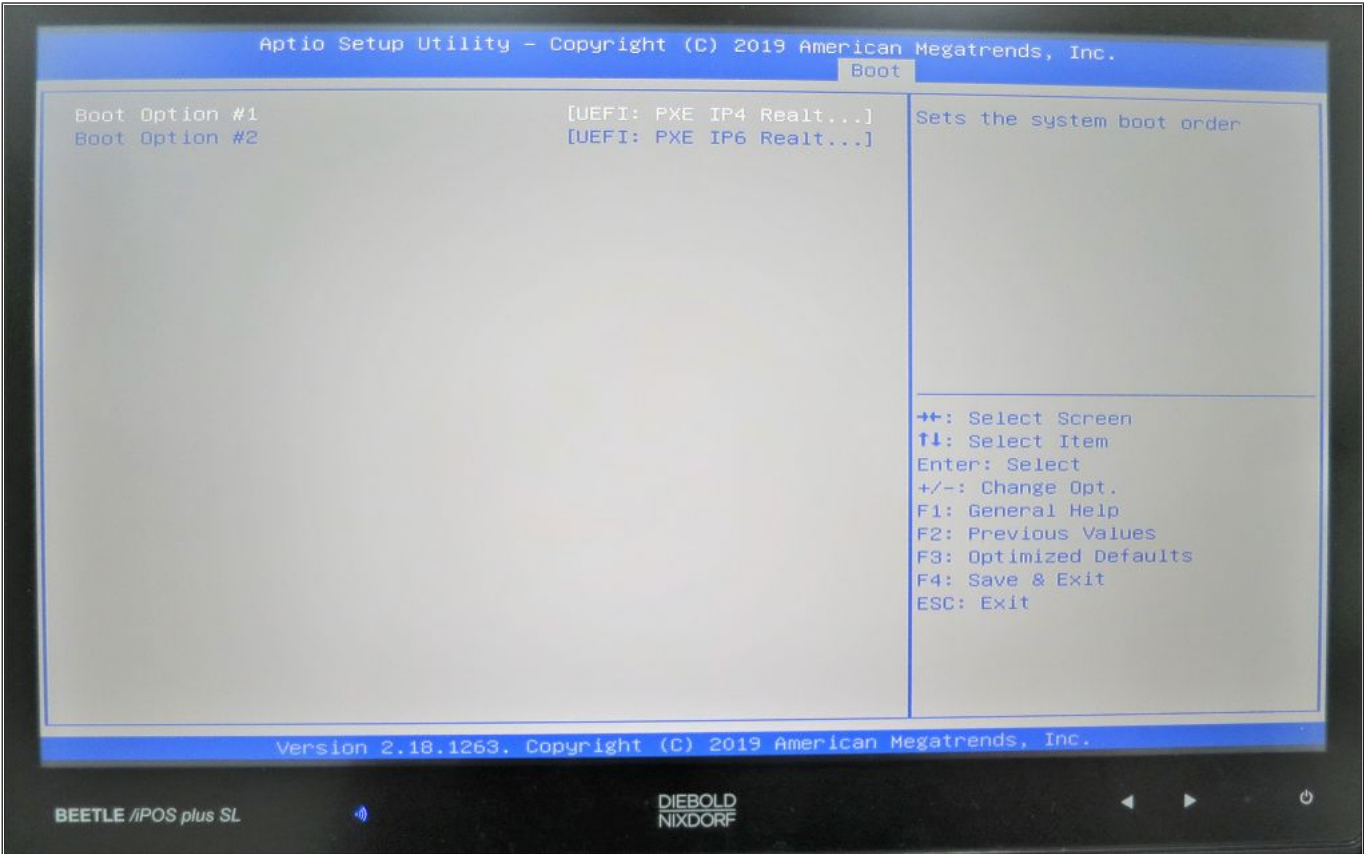
Setup Prompt Timeout:	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.
Bootup NumLock State:	Select the keyboard NumLock State.
Quiet Boot:	Enables or disables Quiet Boot option.
New Boot Option Policy:	Controls the placement of newly detected UEFI boot options.
Boot mode select:	Select boot mode LEGACY/UEFI.
FIXED BOOT ORDER Priorities:	Sets the system boot order.

7.1.8.1 UEFI Hard Disk Drive BBS Priorities



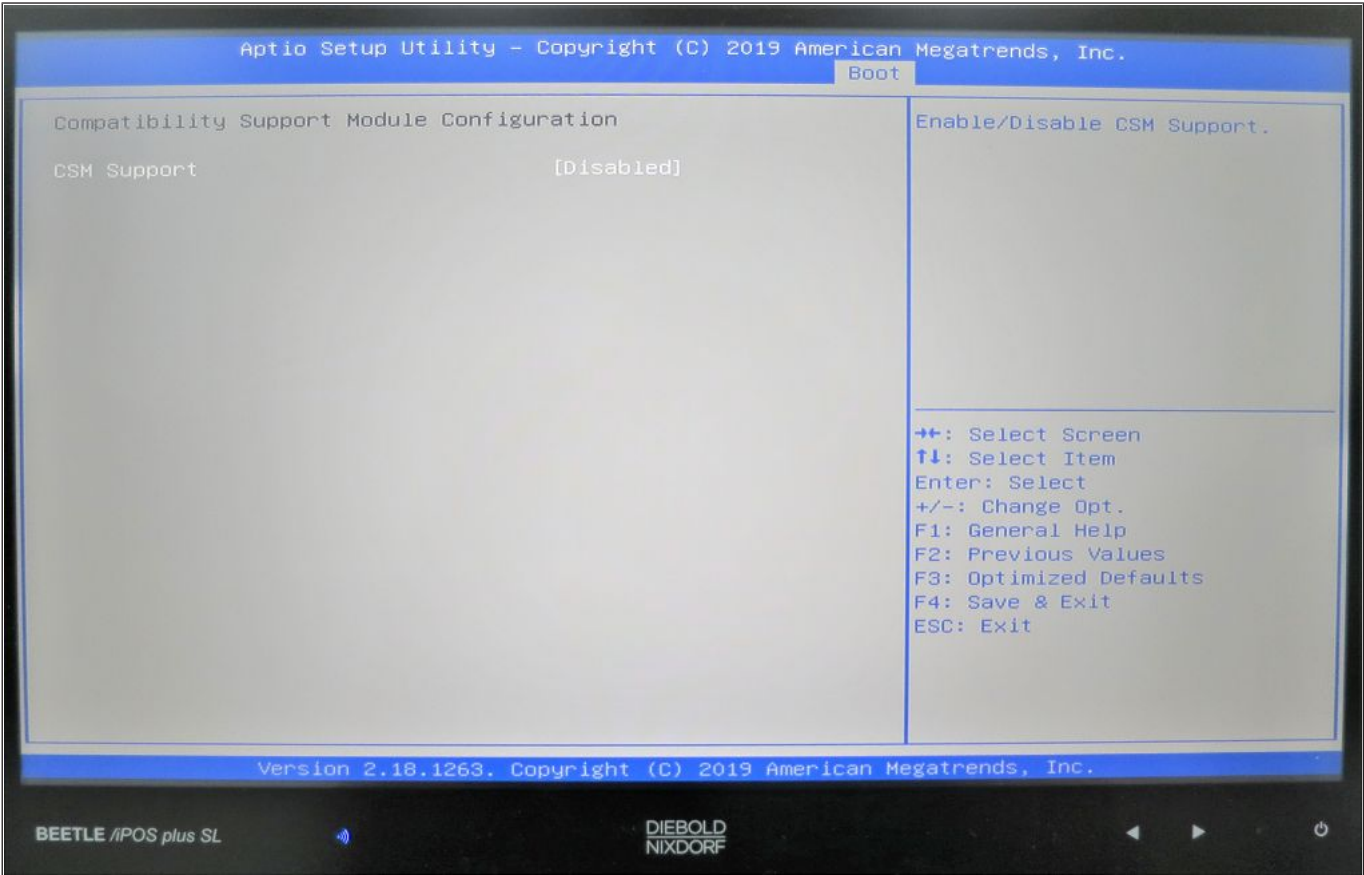
Boot Option #1:	Sets the system boot order.
-----------------	-----------------------------

7.1.8.2 UEFI NETWORK Drive BBS Priorities



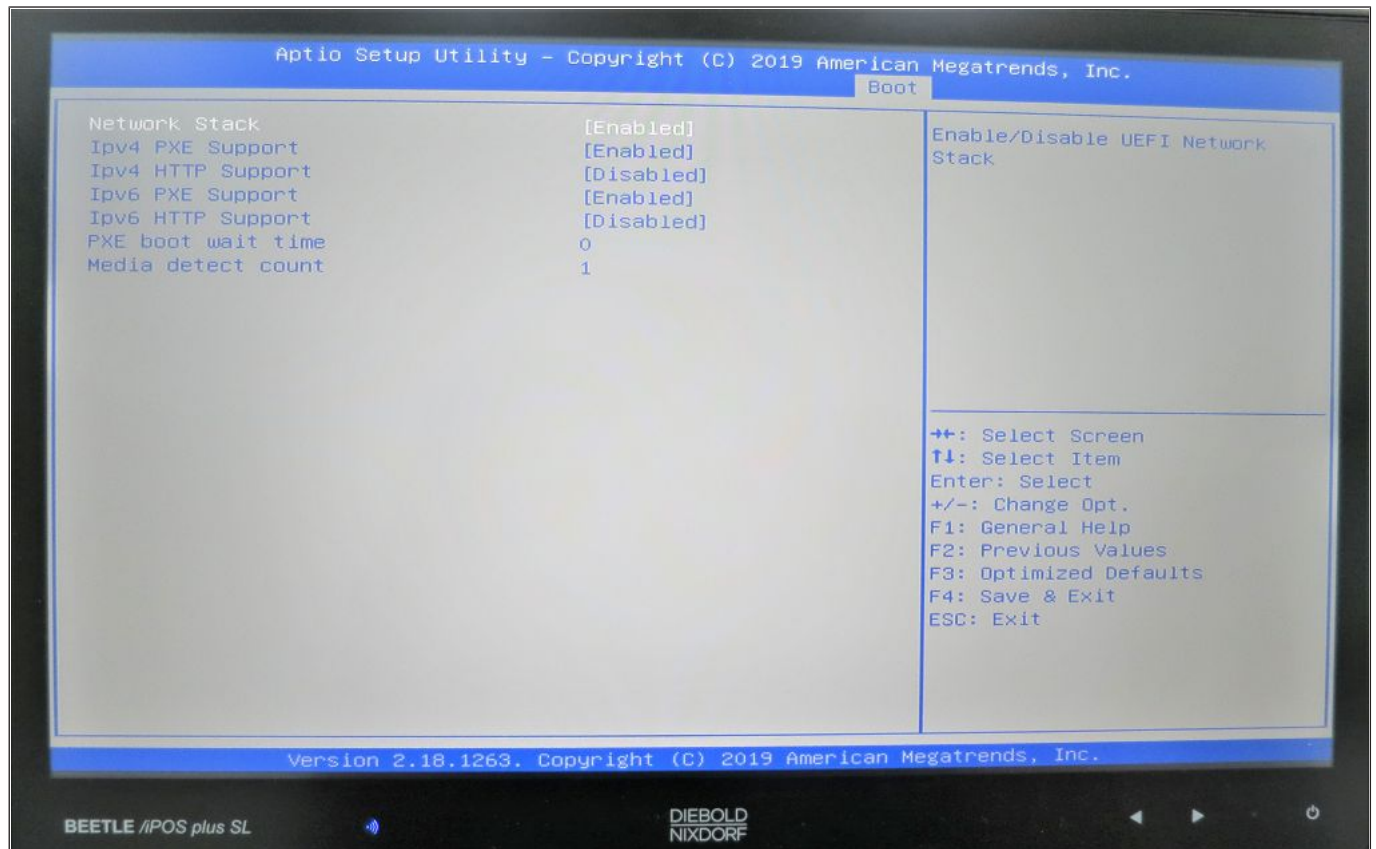
Boot Option #1:	Sets the system boot order.
Boot Option #2:	Sets the system boot order.

7.1.8.3 CSM Configuration



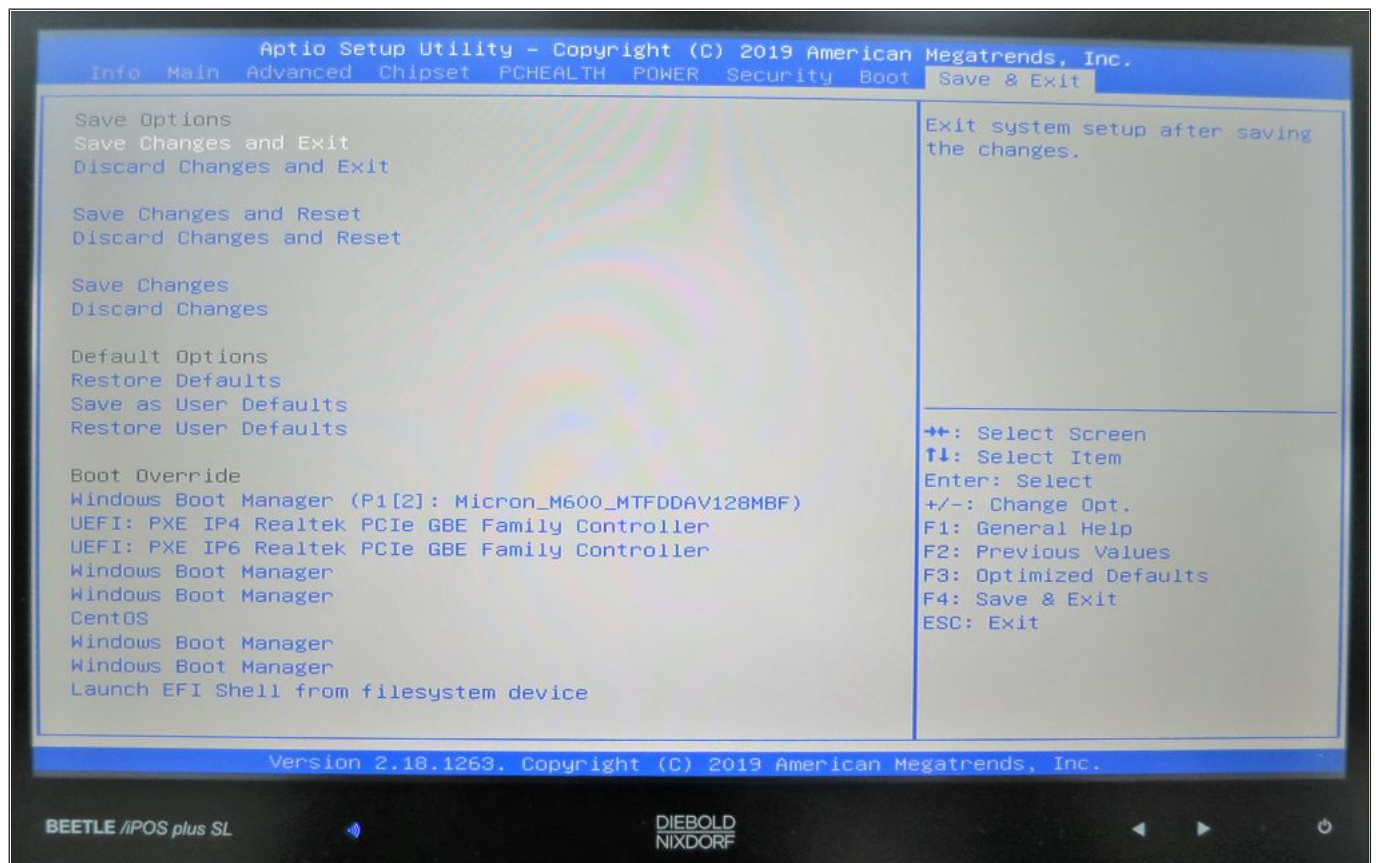
CSM Support	Enable/Disable CSM Support.
-------------	-----------------------------

7.1.8.4 Network Stack Configuration



Network Stack:	Enable/Disable UEFI Network Stack.
Ipv4 PXE Support:	Enable/Disable Ipv4 PXE Support.
Ipv4 HTTP Support:	Enable/Disable Ipv4 HTTP Support:.
Ipv6 PXE Support:	Enable/Disable Ipv6 PXE Support:..
Ipv6 HTTP Support:	Enable/Disable Ipv6 HTTP Support:..
PXE boot wait time:	Select PXE boot wait time.
Media detect count:	Select Media detect count.

7.1.9 Save & Exit



Save Changes and Exit:	Exit system setup after saving the changes.
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.
Boot Overrides:	Detected Boot devices are shown here. If Boot Mode selected is Legacy UEFI boot device will not appear in this list. You may override the fixed boot priority order by selecting from this list the device to boot from. Alternatively, boot override can also be call out with the F10 hotkey.

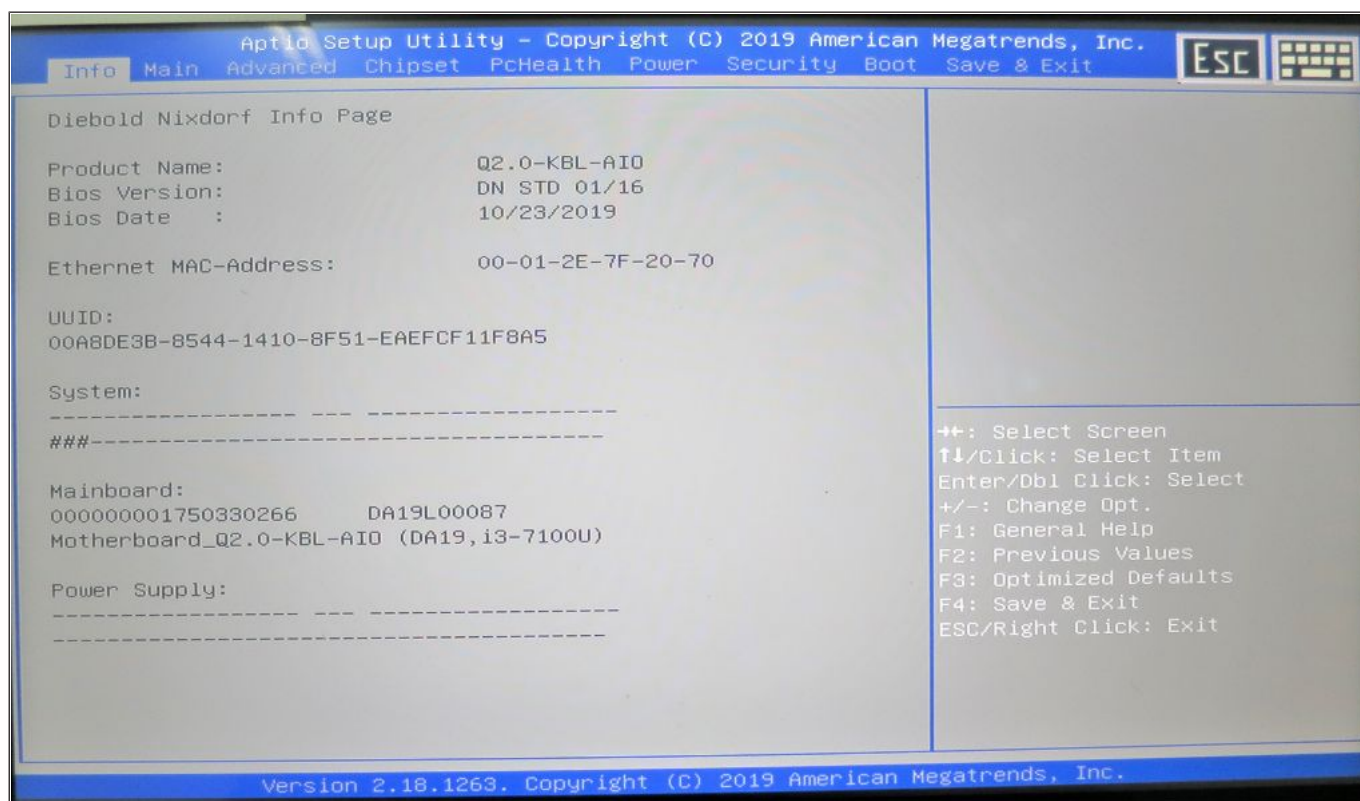
8 Kaby Lake

8.1 Default BIOS Settings

The tables below indicate the BIOS default setting for reference purpose. Upon power ON, enter BIOS setup by pressing 'Delete'.

	 WARNING
	Please take note of any special BIOS setting according to your customer's usage before resuming the BIOS setting to its default.

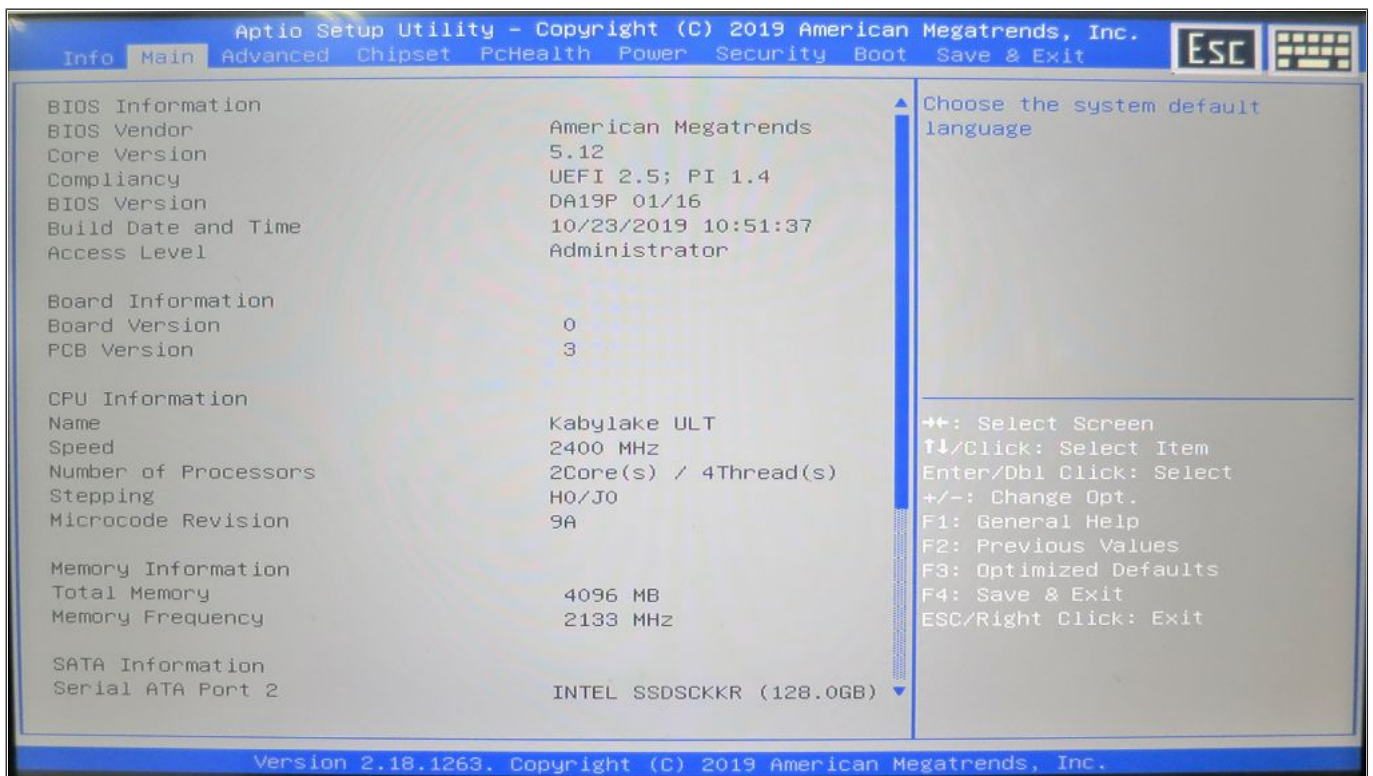
8.1.1 Information



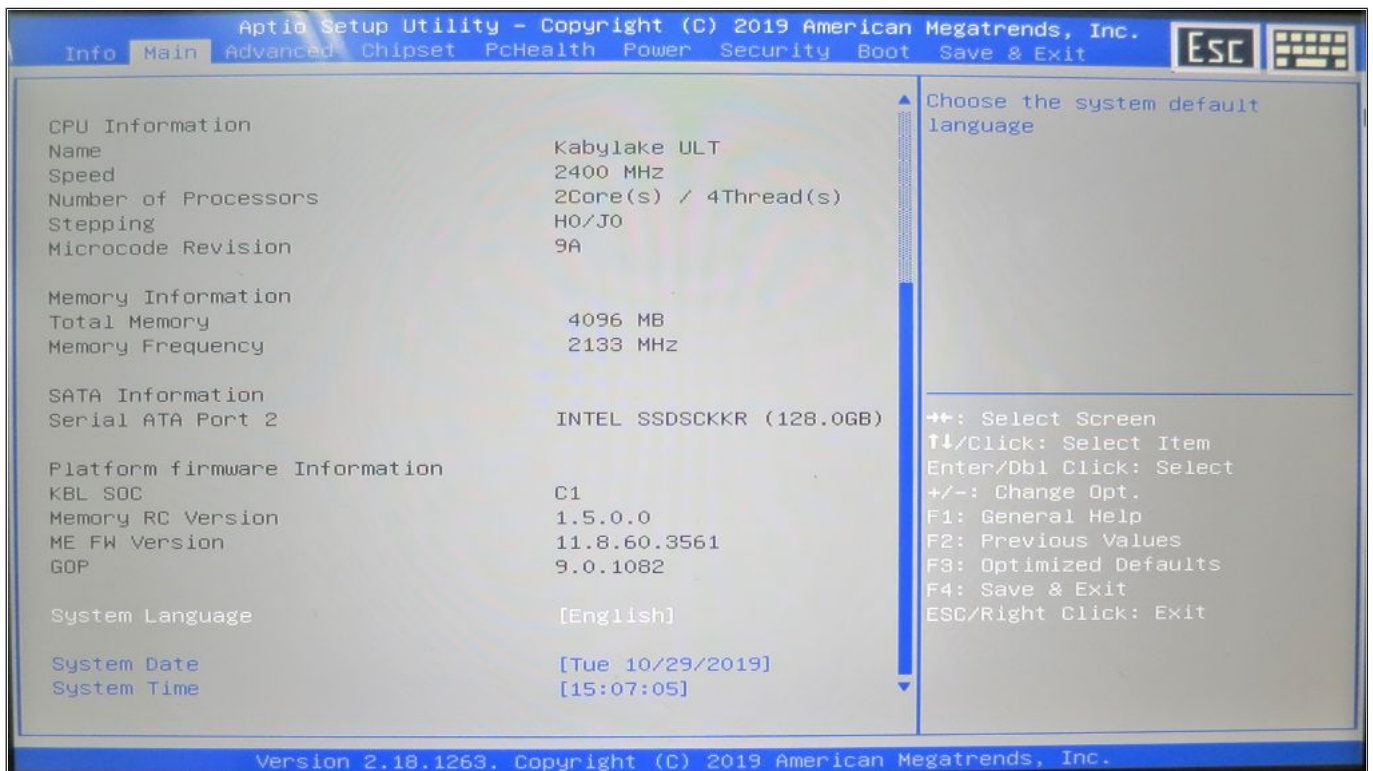
This page displays some system-related information to facilitate the support of your system.

Product Name:	This identification string identifies the motherboard in the system.
BIOS Version:	Display in the format DN STD xx/yy where xx is the BIOS version number and yy is the build number.
Ethernet MAC-Address:	Ethernet MAC Address of the on-board LAN controller.
UUID:	A UUID is an identifier standard used in software construction, standardized by the Open Software Foundation. The intent of the UUIDs is to enable distributed systems to uniquely identify information without significant central coordination.

8.1.2 Main

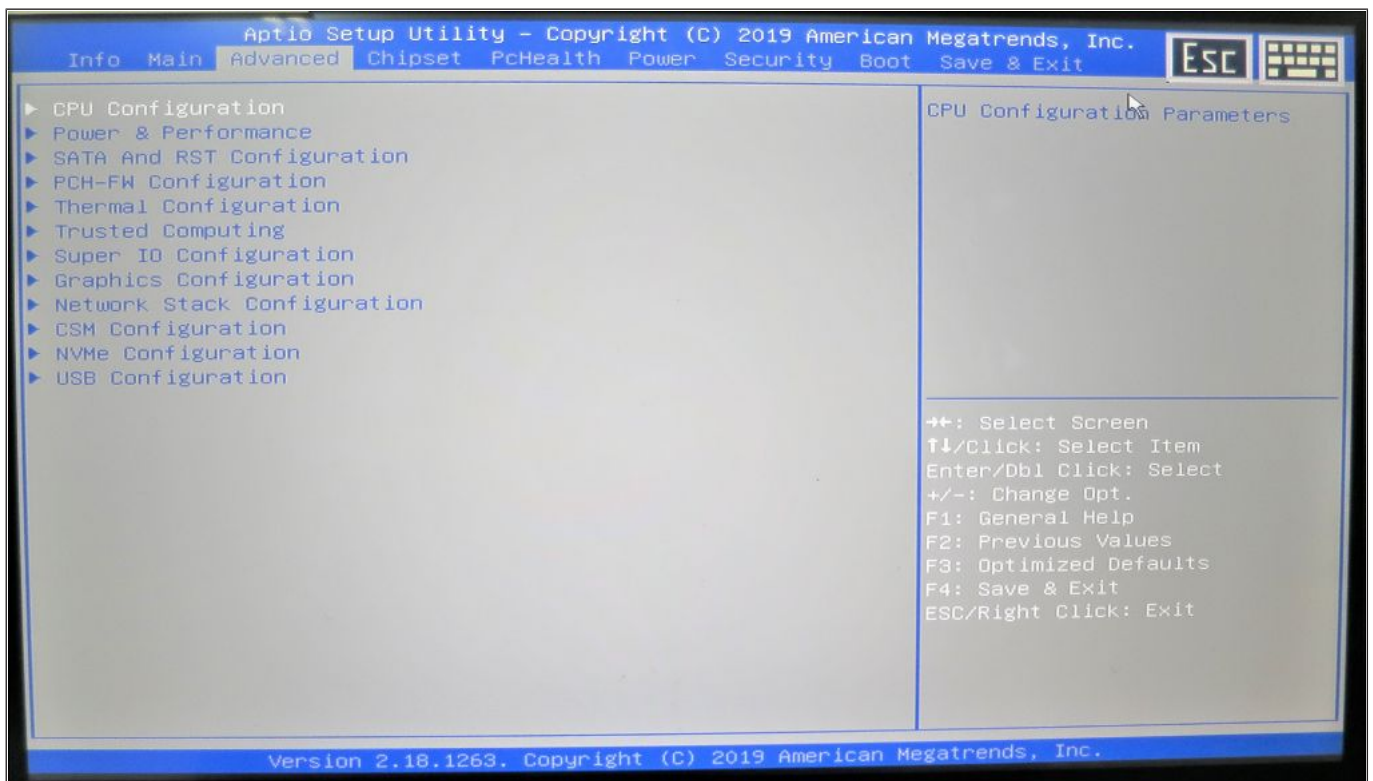


The Main page provides the key information about the system hardware configuration.



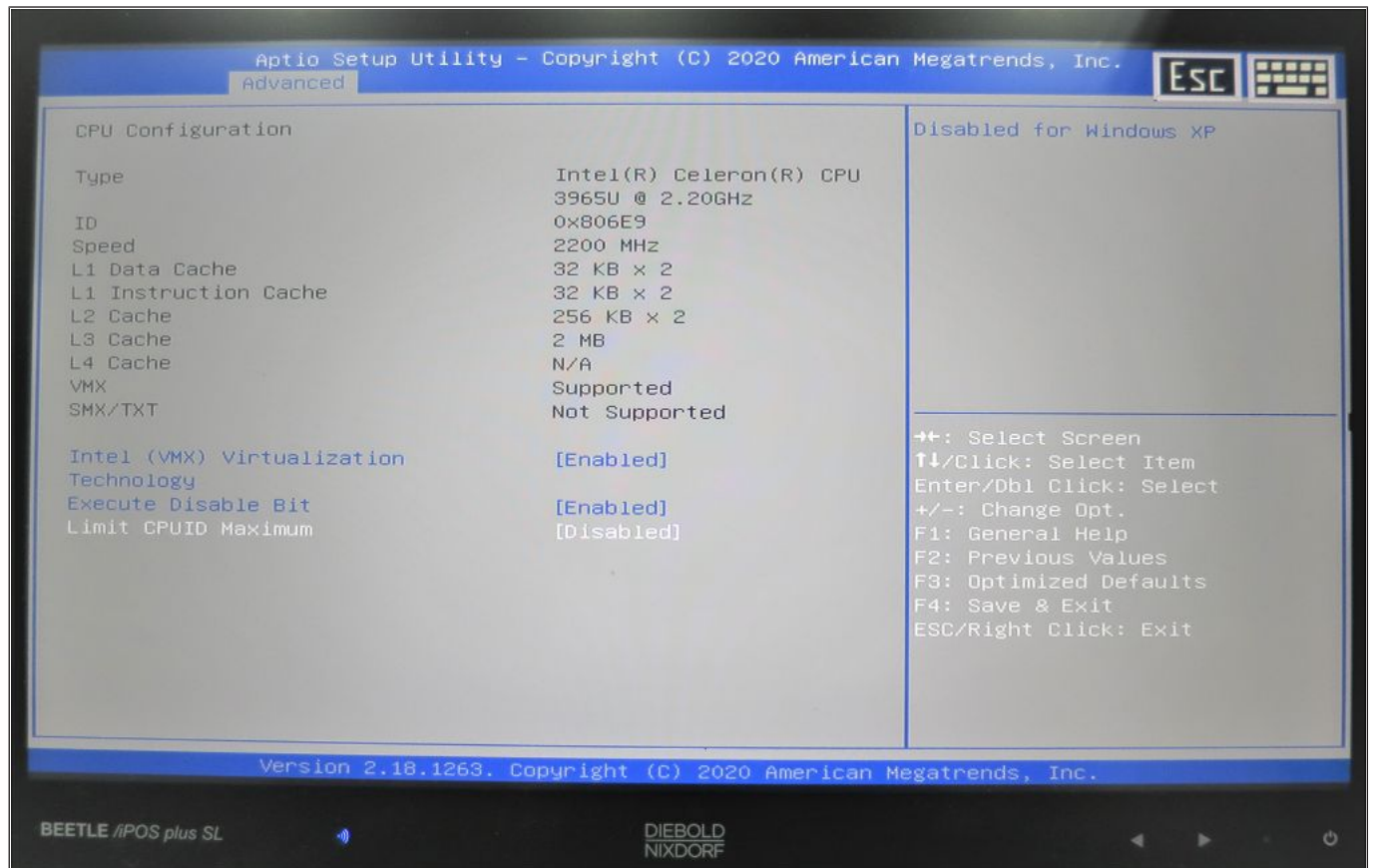
System Date:	To set the date, use tab switch between date elements. Press numeric keys to enter.
System Time:	To set the time, use tab switch between time elements. Press numeric keys to enter.

8.1.3 Advanced



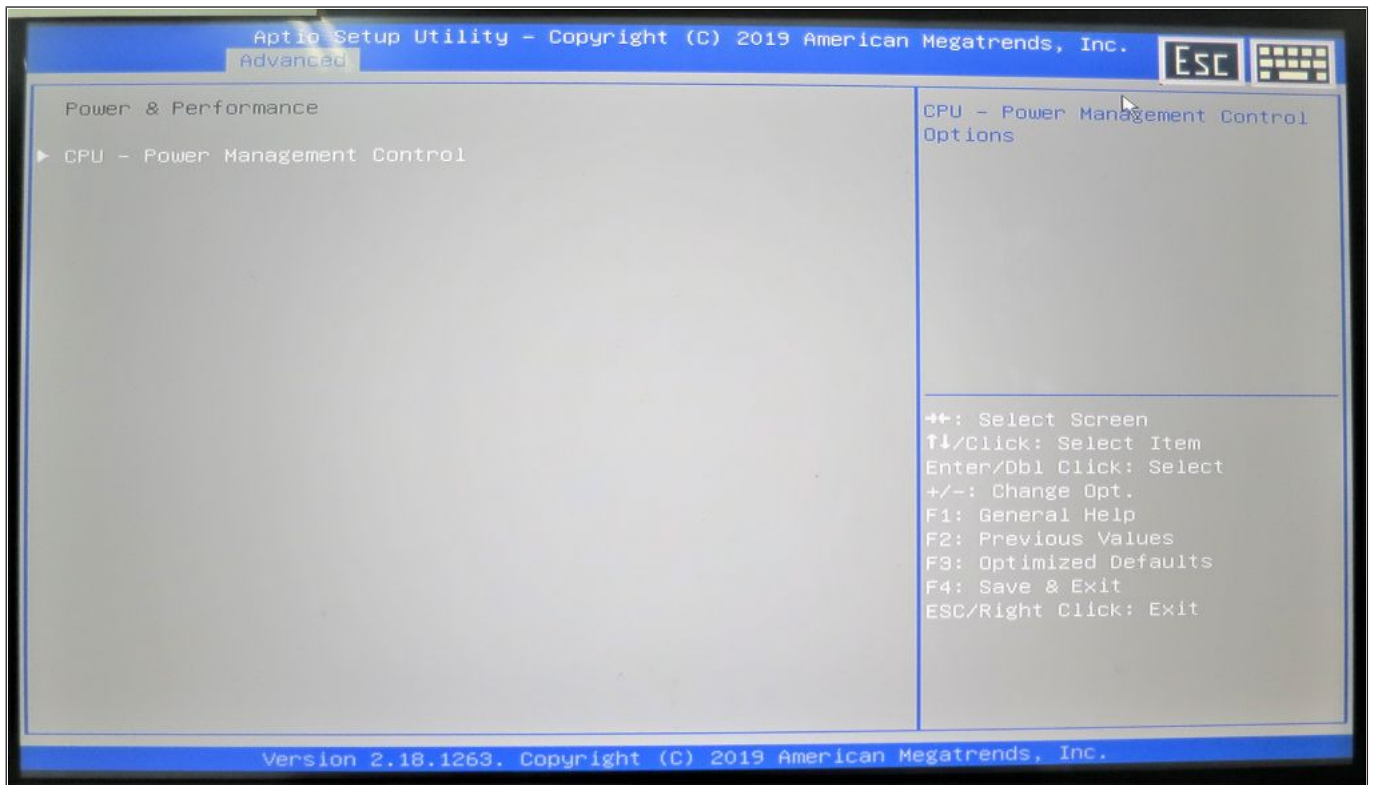
The Advanced function in the system can be configured in this menu for advanced system configuration. Only change the default settings if required for a special purpose. Incorrect settings can cause malfunction.

8.1.3.1 CPU Configuration

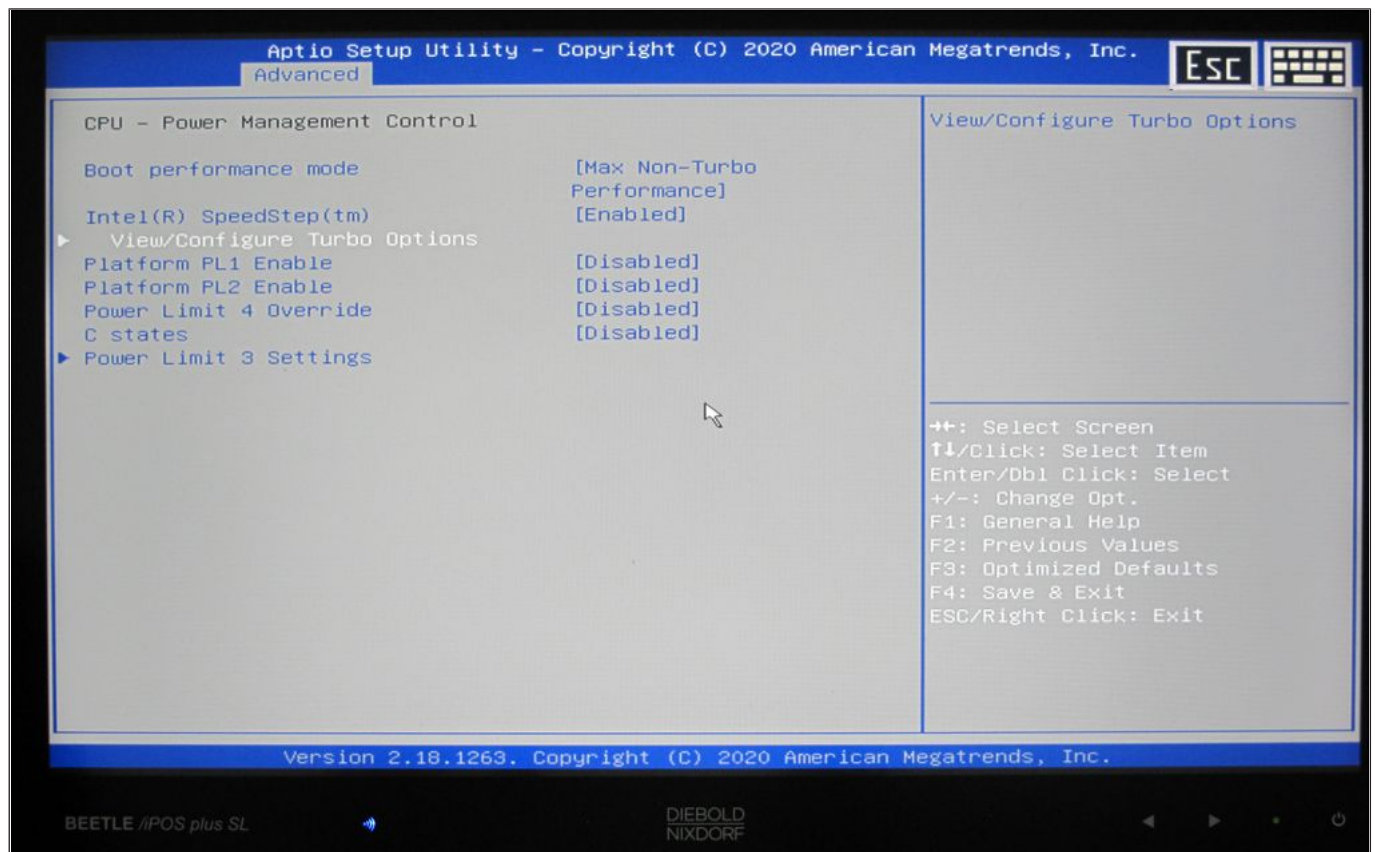


Intel (VMX) Virtualization Technology:	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.
Execute Disable Bit:	Execute Disable Bit is a hardware-based security feature that can reduce exposure to viruses and malicious code attacks and prevent harmful software from executing and propagating on the server or network.
Limit CPUID Maximum:	Disabled for Windows XP

8.1.3.2 Power & Performance

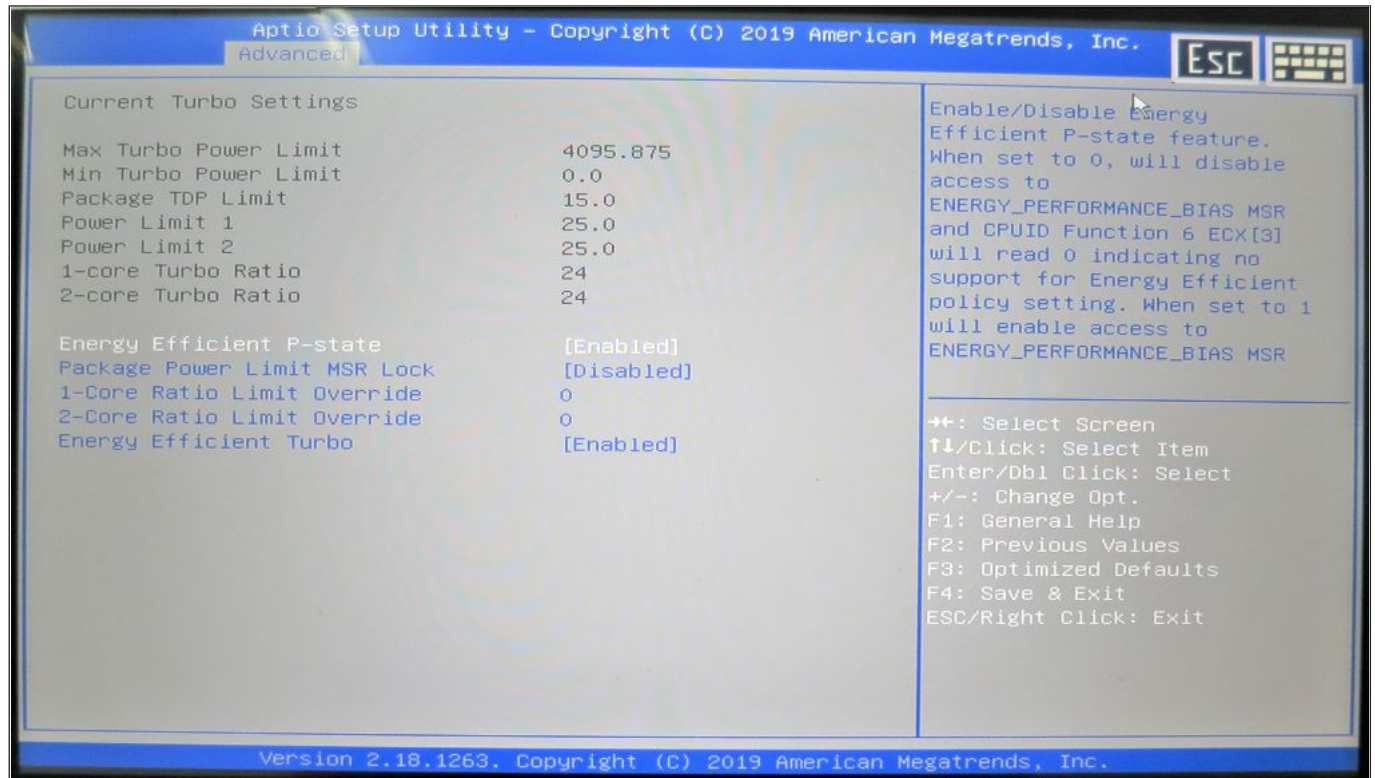


8.1.3.2.1 CPU - Power Management Configuration



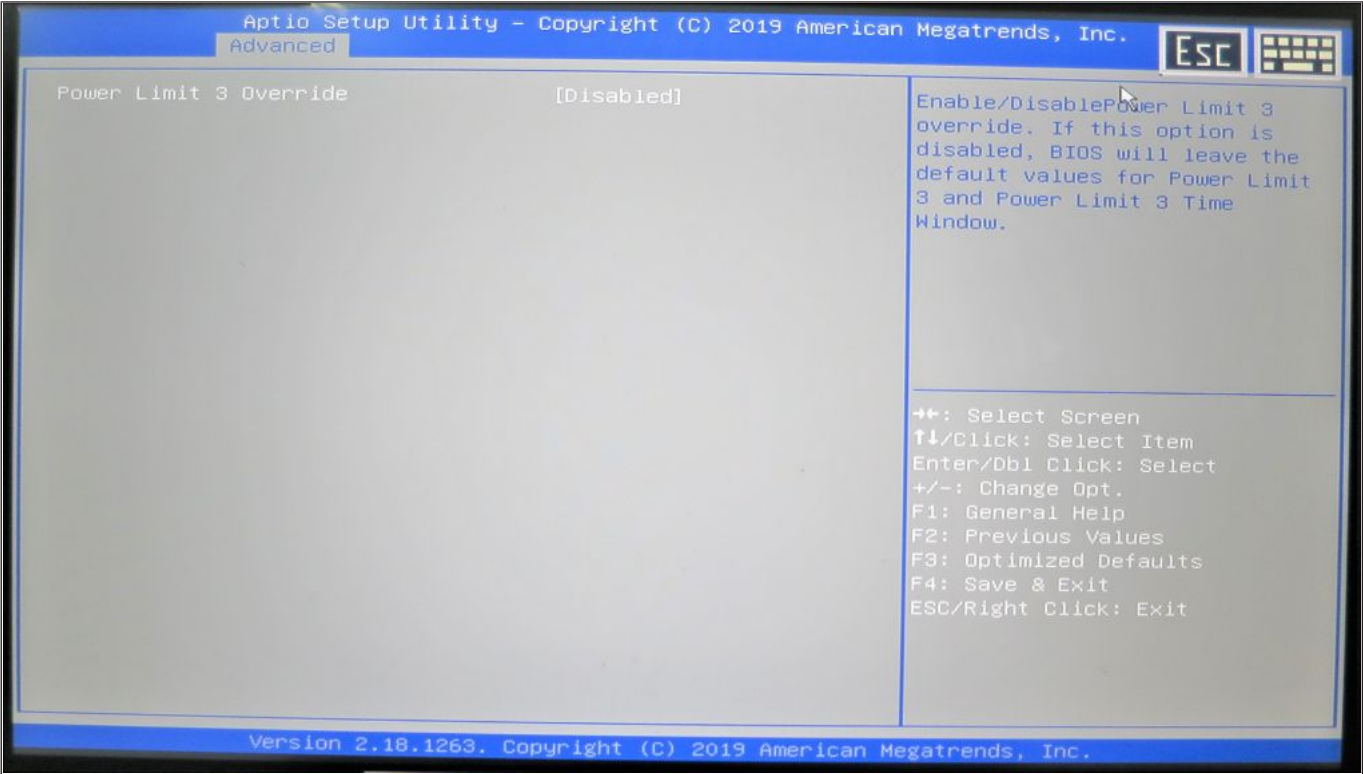
Boot performance mode:	Selects the performance state that the BIOS will set starting from reset vector.
Intel ® SpeedStep™	Enhanced Intel SpeedStep® Technology for enabling high performance while meeting the power-conservation.
View/Configure Turbo Options:	View/Configure Turbo Options
Platform PL1 Enable:	Enable/Disable Platform Power Limit 1 programming. If this option is enabled, it activates the PL1 value to be used by the processor to limit the average power of given time window.
Platform PL2 Enable:	Enable/Disable Platform Power Limit 2 programming. If this option is disabled, BIOS will program the default values for Platform Power Limit 2.
Power Limit 4 Override:	Enable/Disable Power Limit 4 Override. If this option is disabled, BIOS will leave the default values for Power Limit 4.

8.1.3.2.1.1 View/Configure Turbo Options



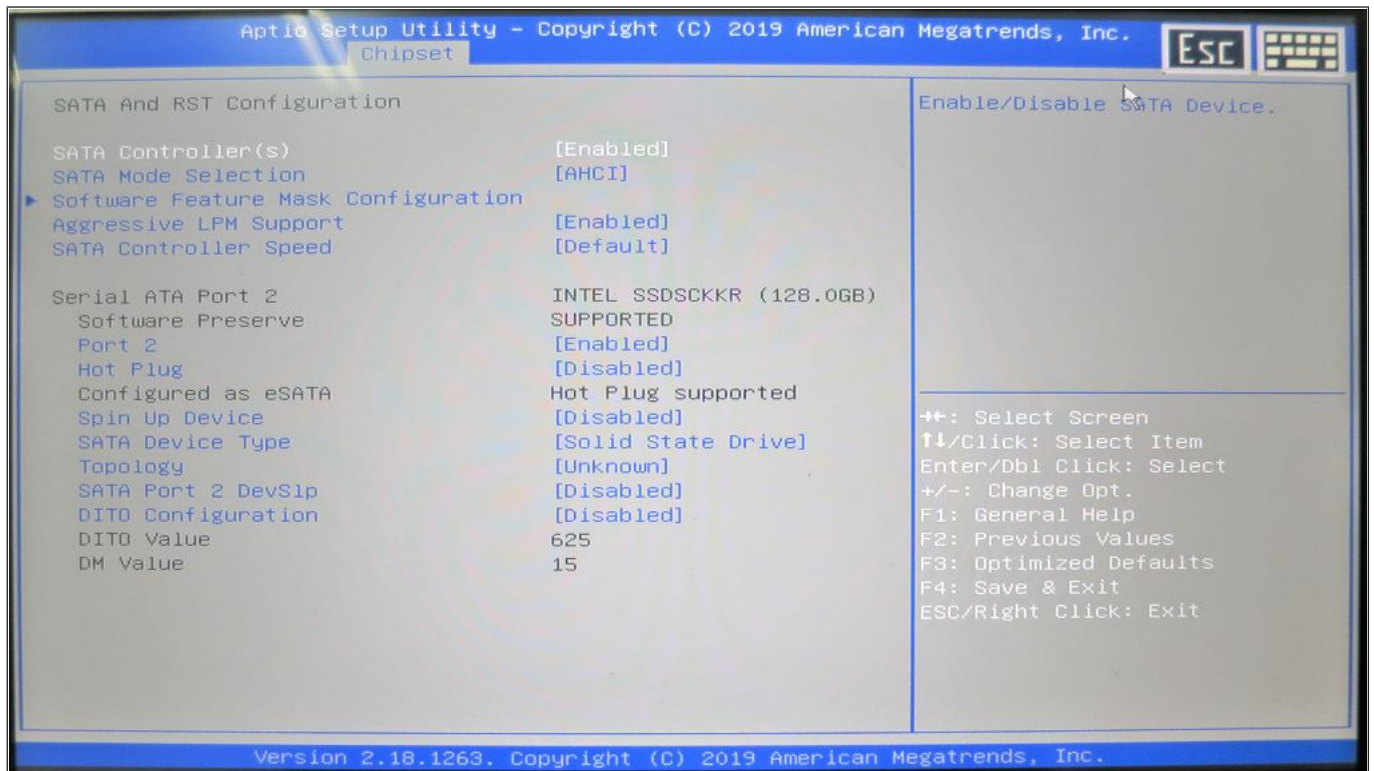
Energy Efficient P-state:	Enable/Disable Energy Efficient P-state feature. When set to 0, will disable access to ENERGY_PERFORMANCE_BIAS MSR and CPUID Function 6 ECX[3] will read 0 indicating no support for Energy Efficient policy setting. When set to 1, will enable access to ENERGY_PERFORMANCE_BIAS MSR:
Package Power Limit MSR Lock:	Enable/Disable locking of Package Power Limit settings. When enabled, PACKAGE_POWER_LIMIT MSR will be locked and a reset will be required to unlock the register.
1-Core Ratio Limit Override:	1-Core Ratio Limit with range 0 to 83. The minimum range may vary between processors. This 1-Core Ratio Limit must be greater than or equal to 2-Core Ratio Limit, 3-Core Ratio Limit, 4-Core Ratio Limit.
2-Core Ratio Limit Override:	2-Core Ratio Limit with range 0 to 83. The minimum range may vary between processors. This 2-Core Ratio Limit must be greater than or equal to 1-Core Ratio Limit.
Energy Efficient Turbo:	Enable/Disable Energy Efficient Turbo feature. This feature will opportunistically lower the turbo frequency to increase efficiency. Recommended only to disable in overclocking.

8.1.3.2.1.2 Power Limit 3 Settings



Power Limit 3 Override:	Enable/Disable Power Limit 3 Override. If this option is disabled, BIOS will leave the default values for Power Limit 3 and Power Limit 3 Time Window.
-------------------------	--

8.1.3.3 SATA & RST Configuration



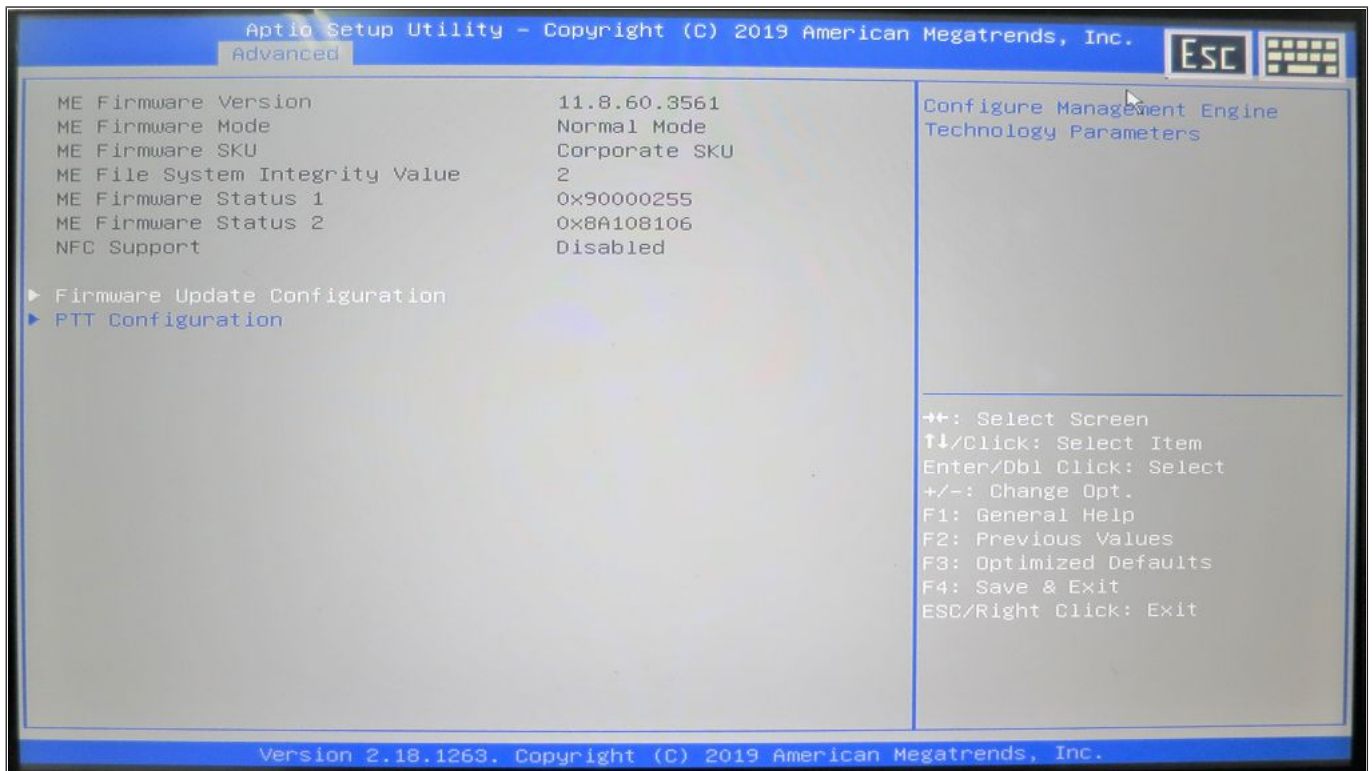
SATA Controller(s):	Enable/Disable SATA Controller(s).
SATA Mode Selection:	Determines how SATA controller operates.
Aggressive LPM Support:	Enable/Disable Aggressive LPM Support.
SATA Controller Speed:	Indicates the maximum speed the SATA controller can support.
Port 2:	Enable/Disable Port 2.
Hot Plug:	Enable/Disable Hot Plug Capability.
Spin Up Device:	If enabled for any of ports Staggered Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type:	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.
Topology:	Identify the SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2.
SATA Port 2 DevSlp:	Enable/Disable SATA Port 2 DevSlp. Board rework for LP needed before enable.
DITO Configuration:	Enable/Disable DITO Configuration.

8.1.3.3.1 Software Feature Mask Configuration

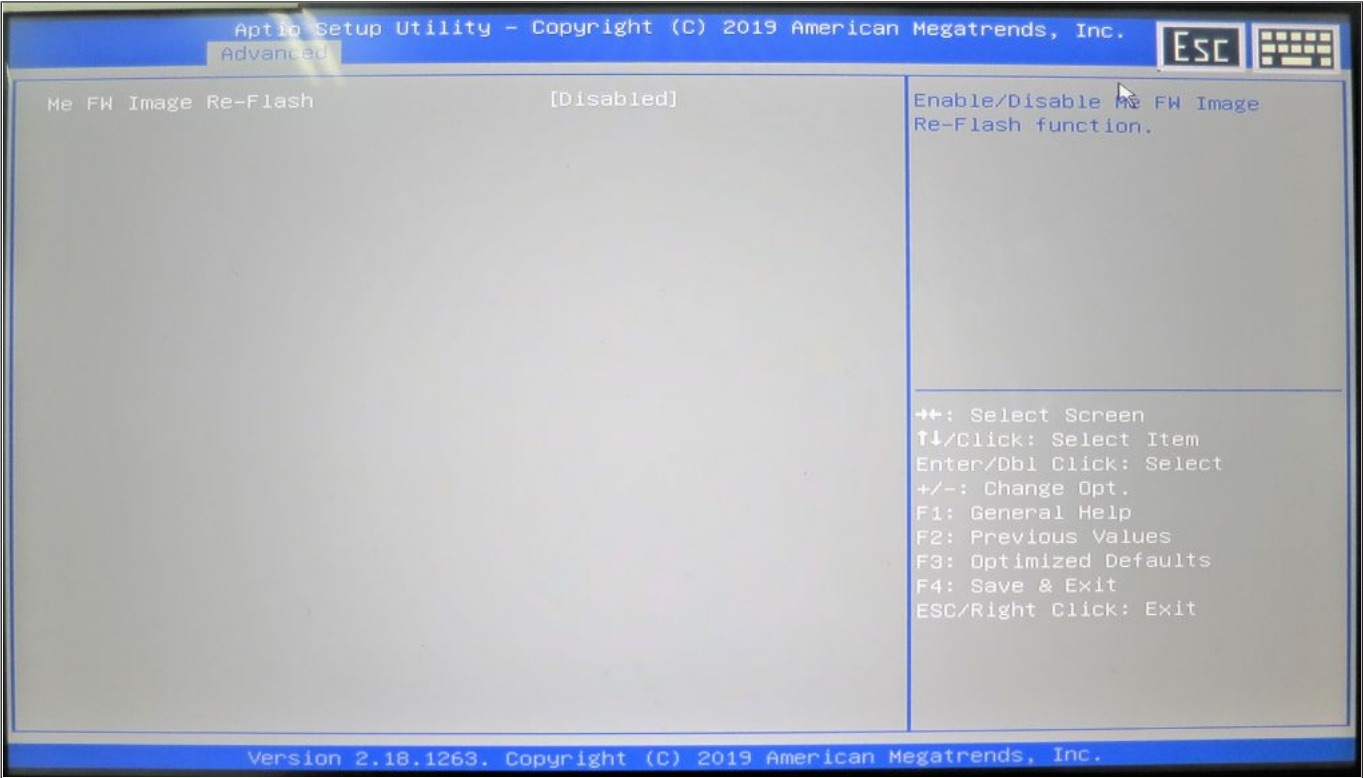


HDD Unlock:	If enabled, indicates that the HDD password un- lock in the OS is enabled.
LED Locate:	If enabled, indicates that the LED/SGPIO hard- ware is attached and ping to locate feature is en- abled on the OS.

8.1.3.4 PCH-FW Configuration

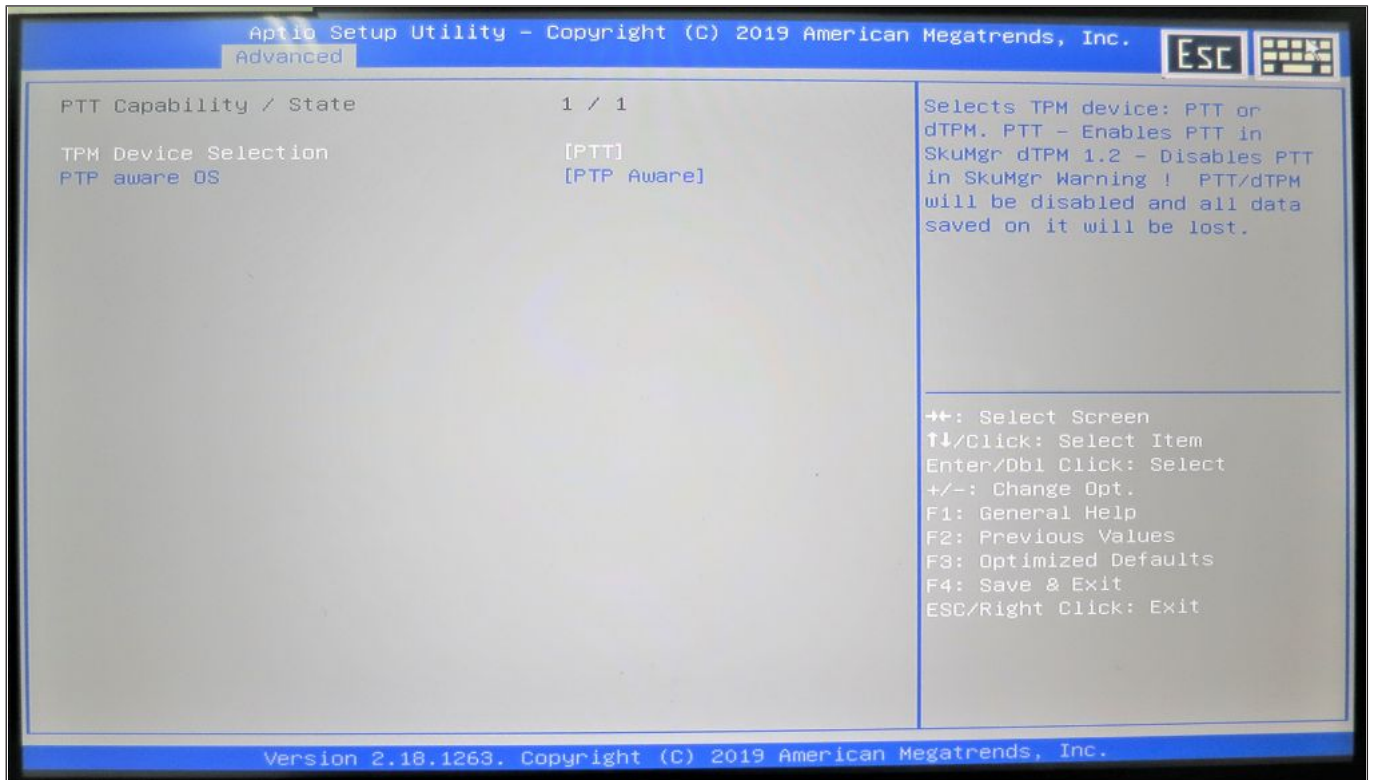


8.1.3.4.1 **Firmware Update Configuration**



Me FW Image Re-Flash:	Enable/Disable Me FW Image Re-Flash function.
-----------------------	---

8.1.3.4.2 PTT Configuration

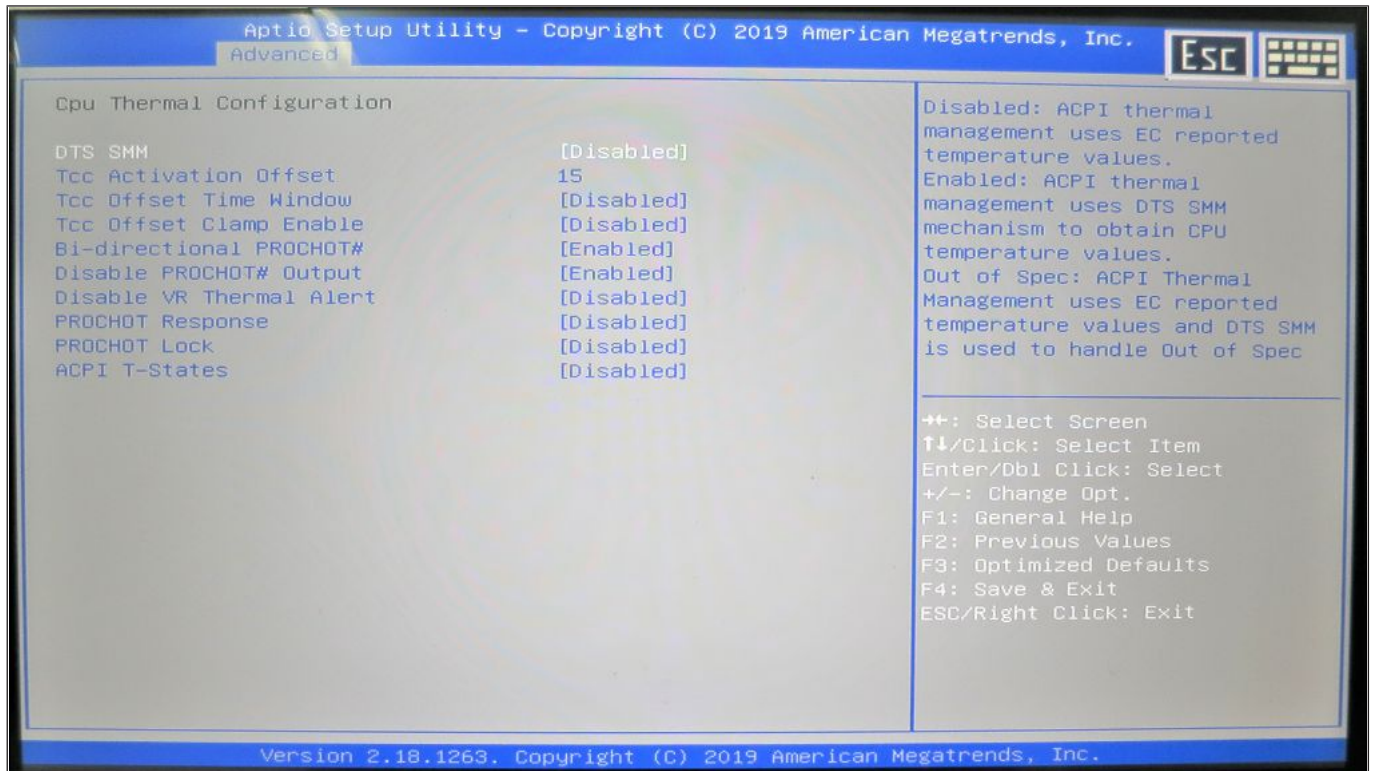


TPM Device Selection:	Select TPM device: PTT or dTPM. PTT – Enables PTT in SkuMgr dTPM 1.2 – Disables PTT in SkuMgr Warning! PTT/dTPM will be disabled and all data saved on it will be lost.
PTP aware OS:	Select whether or not the OS you will boot to will be PTP aware.

8.1.3.5 Thermal Configuration



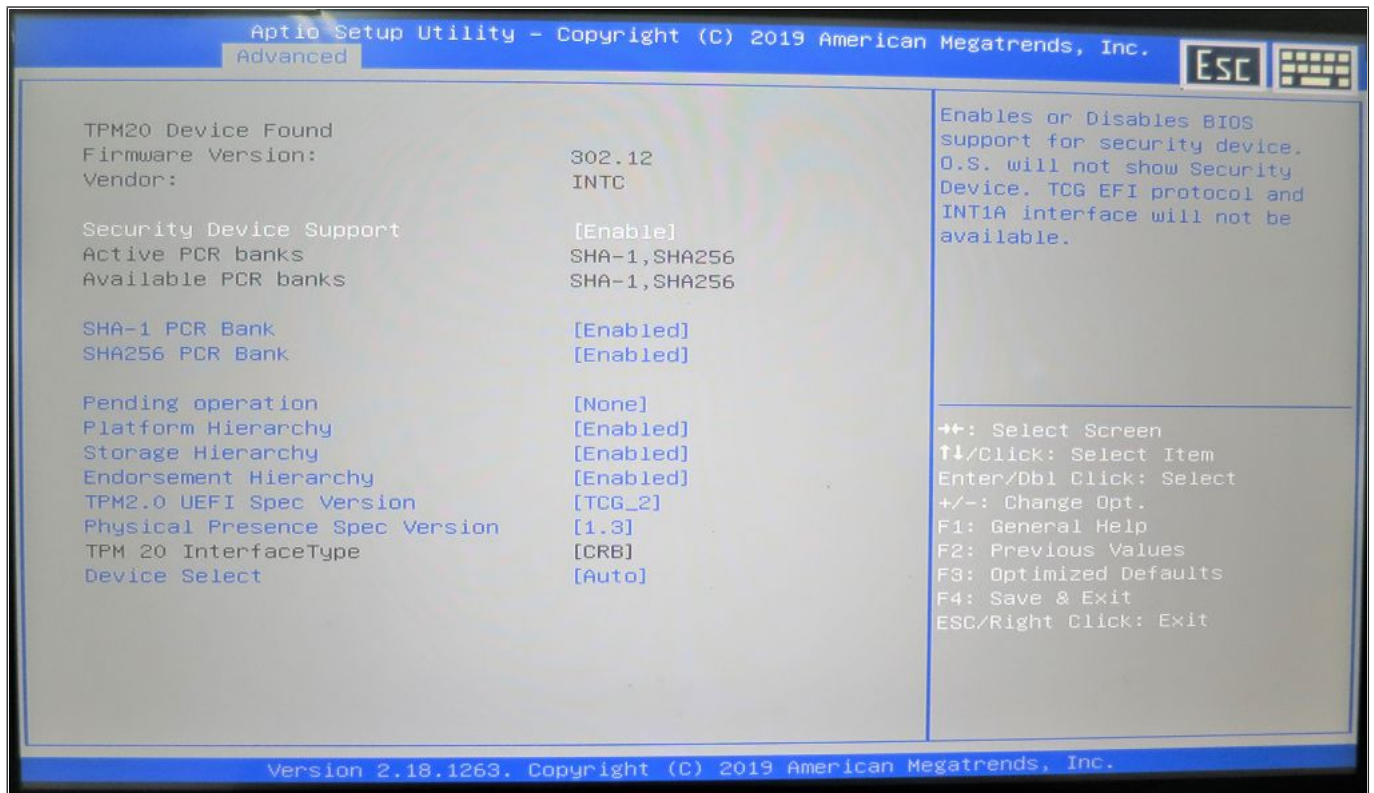
8.1.3.5.1 CPU Thermal Configuration



DTS SMM:	When disabled, ACPI thermal management uses EC reported temperature values. When enabled, ACPI thermal management uses DTS SMM mechanism to obtain CPU temperature values.
Tcc Activation Offset:	Factory default for the TCC Offset depends on the processor. For Celeron and i3, TCC offset is 15. For i5, TCC offset is 25.
Tcc Offset Time Window:	Tcc Offset Time Window for Running Average Temperature Limit (RATL) feature. The Tcc offset time window can range from 5ms to 448s. For SKL Y SKU the recommended default is 5 sec, and all other SKUs the recommended default are disabled.
Tcc Offset Clamp Enable:	Tcc Offset Clamp bit Enable for Running Average Temperature Limit (RATL) feature to allow CPU to throttle below P1.
Bi-directional PROCHOT#:	When a processor thermal sensor trips (either core), the PROCHOT# will be driven. If bi-direction is enabled, external agents can drive PROCHOT# to throttle the processor.
Disable PROCHOT# Output:	Enable/Disable PROCHOT# output.
Disable VR Thermal Alert:	Enable/Disable VR Thermal Alert.

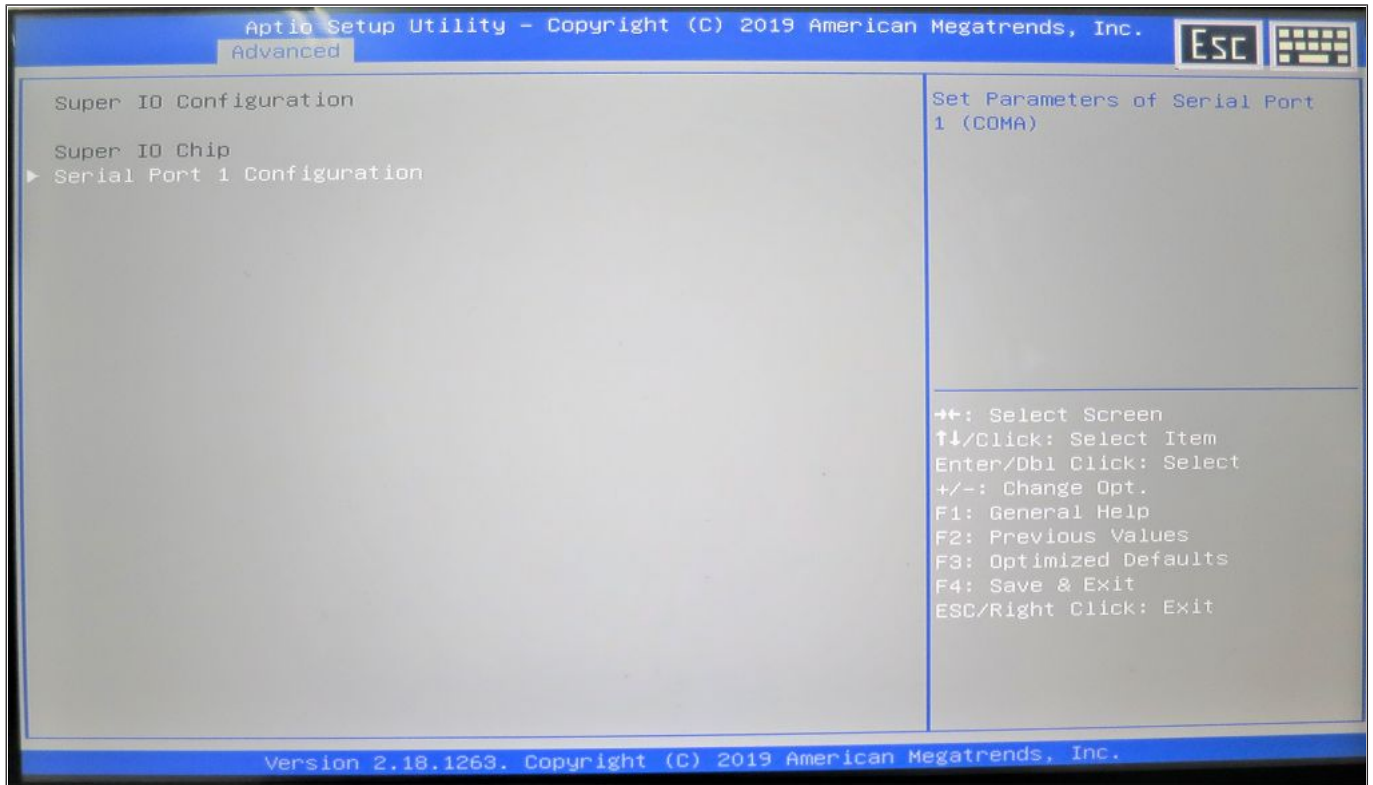
PROCHOT Response:	Enable/Disable PROCHOT Response.
PROCHOT Lock:	Enable/Disable PROCHOT Lock.
ACPI T-States:	Enable/ Disable ACPI T-States.

8.1.3.6 Trusted Computing

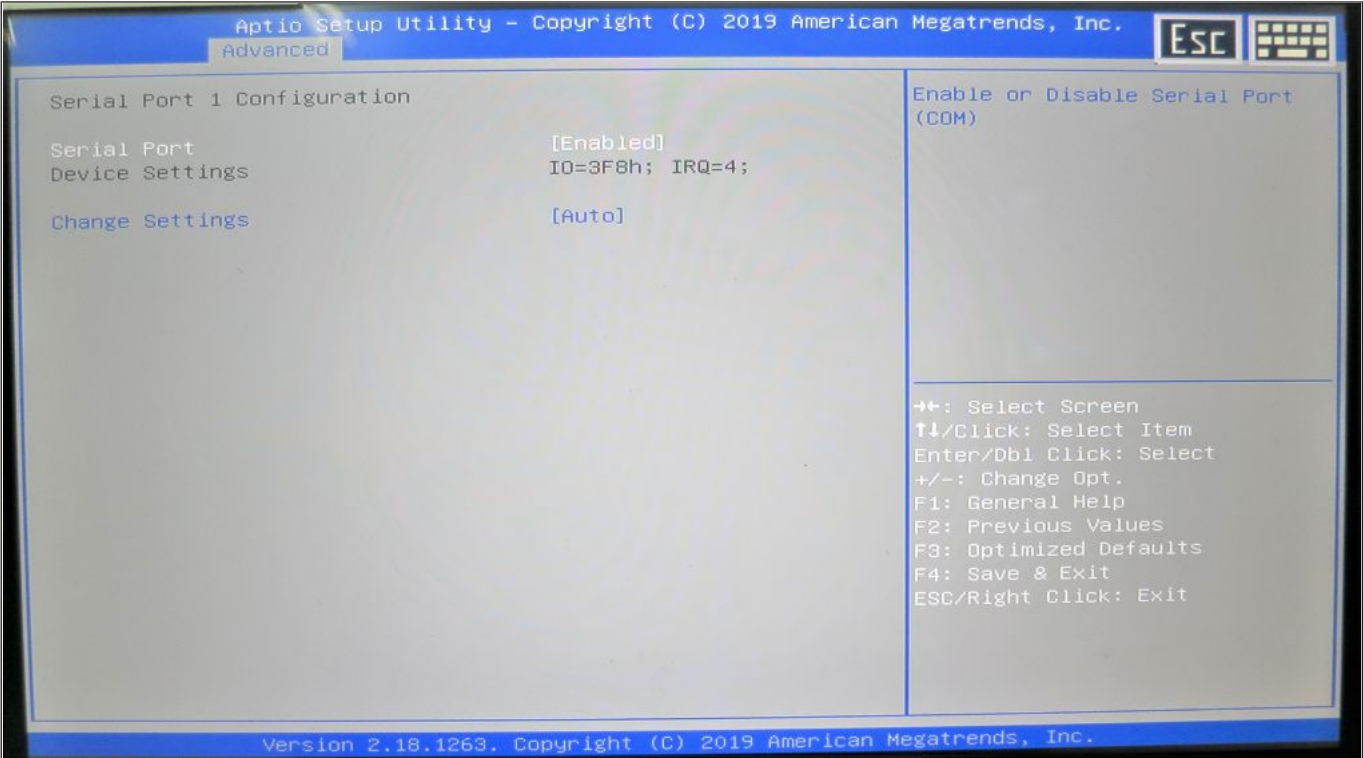


Security Device Support:	Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.
SHA-1 PCR Bank:	Enable or Disable SHA-1 PCR Bank.
SHA 256 PCR Bank:	Enable or Disable SHA256 PCR Bank.
Pending operation:	Schedule an operation for the Security Device. NOTE: your computer will reboot during restart in order to change state of Security Device.
Platform Hierarchy:	Enable or Disable Platform Hierarchy.
Storage Hierarchy:	Enable or Disable Storage Hierarchy.
Endorsement Hierarchy:	Enable or Disable Endorsement Hierarchy.
TPM2.0 UEFI Spec Version:	Select the TCG2 Spec Version Support. TCG_1_2: the compatible mode for Win8/Win10. TCG_2: Support new TCG2 protocol and event format for Win10 or later.
Device Select:	TPM 1.2 will restrict support to TPM 1.2 devices, TPM 2.0 will restrict support to TPM 2.0 devices, Auto will support both with the default set to TPM 2.0 devices if not found, TPM 1.2 devices will be enumerated.

8.1.3.7 Super IO Configuration



8.1.3.7.1 Serial Port 1 Configuration



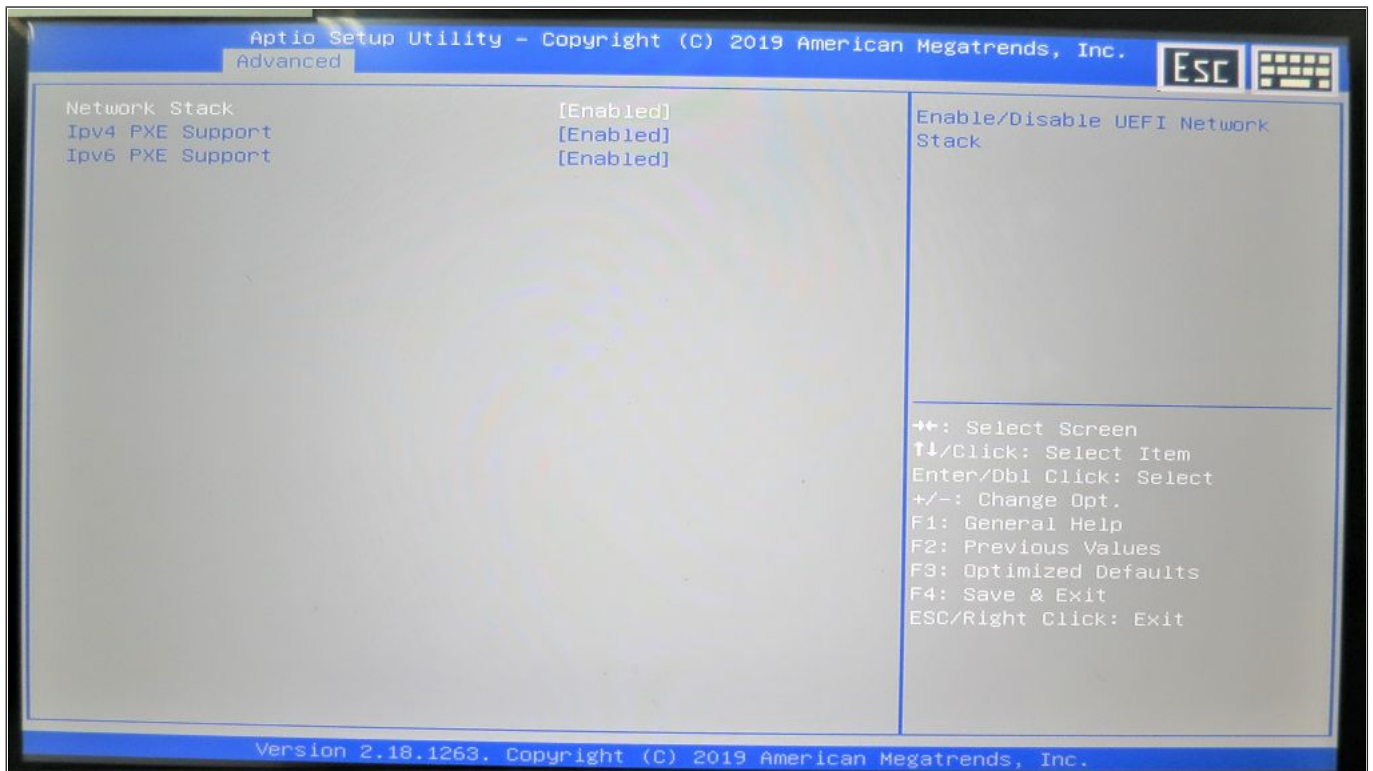
Serial Port:	Enable/Disable Serial Port.
--------------	-----------------------------

8.1.3.8 Graphic Configuration



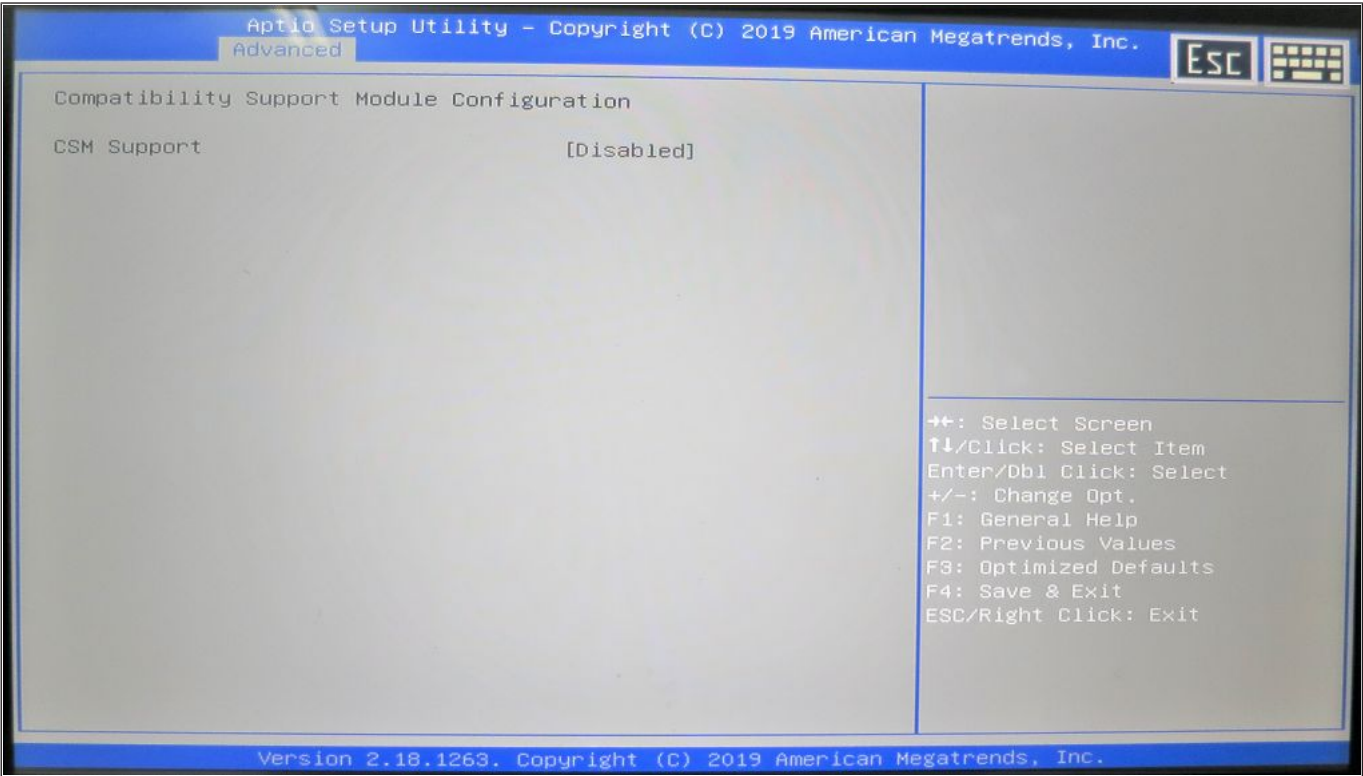
Primary IGFX Boot Display:	Select which device may be used as primary display first.
Aperture Size:	Select the Aperture Size. Note: Above 4GB MMIO BIOS assignment is automatically enabled when selecting 2048MB aperture. To use this feature, please disable CSM Support.
DVMT Total Gfx Mem:	Select DVMT5.0 Total Graphic Memory size used by the Internal Graphics Device.
Gfx Low Power Mode:	This option is applicable for SFF only.

8.1.3.9 Network Stack Configuration



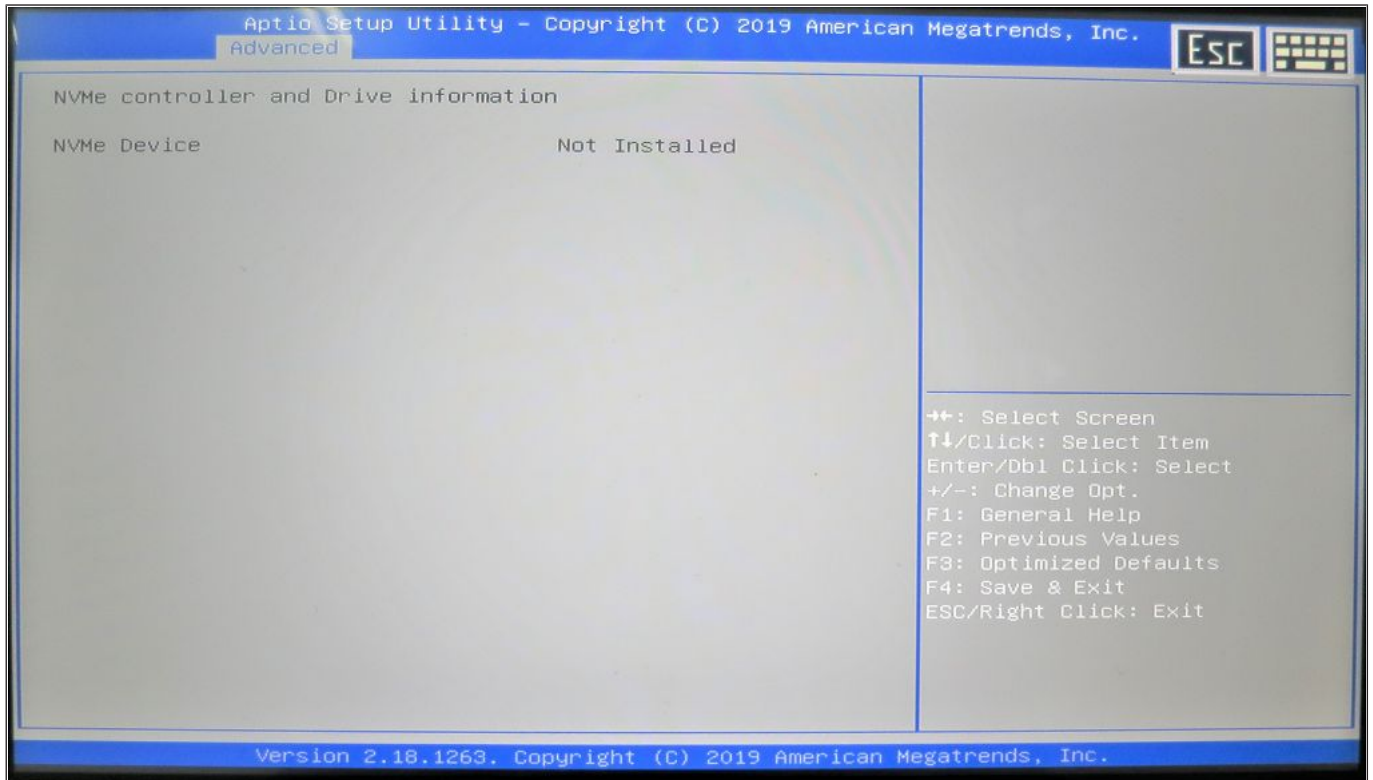
Network Stack:	Enable/Disable UEFI Network Stack.
Ipv4 PXE Support:	Enable/Disable Ipv4 PXE Support.
Ipv6 PXE Support:	Enable/Disable Ipv6 PXE Support..

8.1.3.10 CSM Configuration

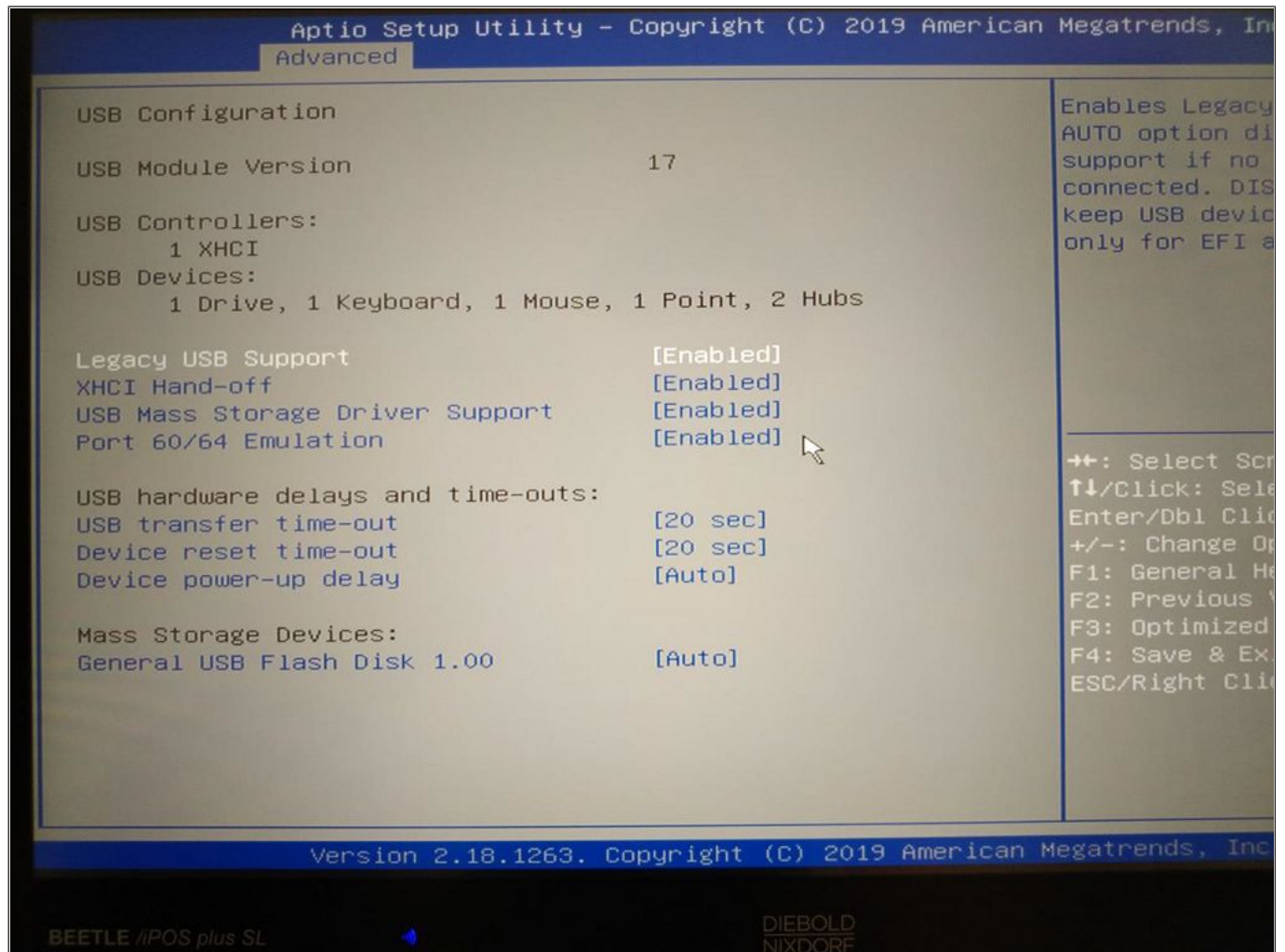


CSM Support:	Enable/Disable CSM Support.
--------------	-----------------------------

8.1.3.11 NVMe Configuration



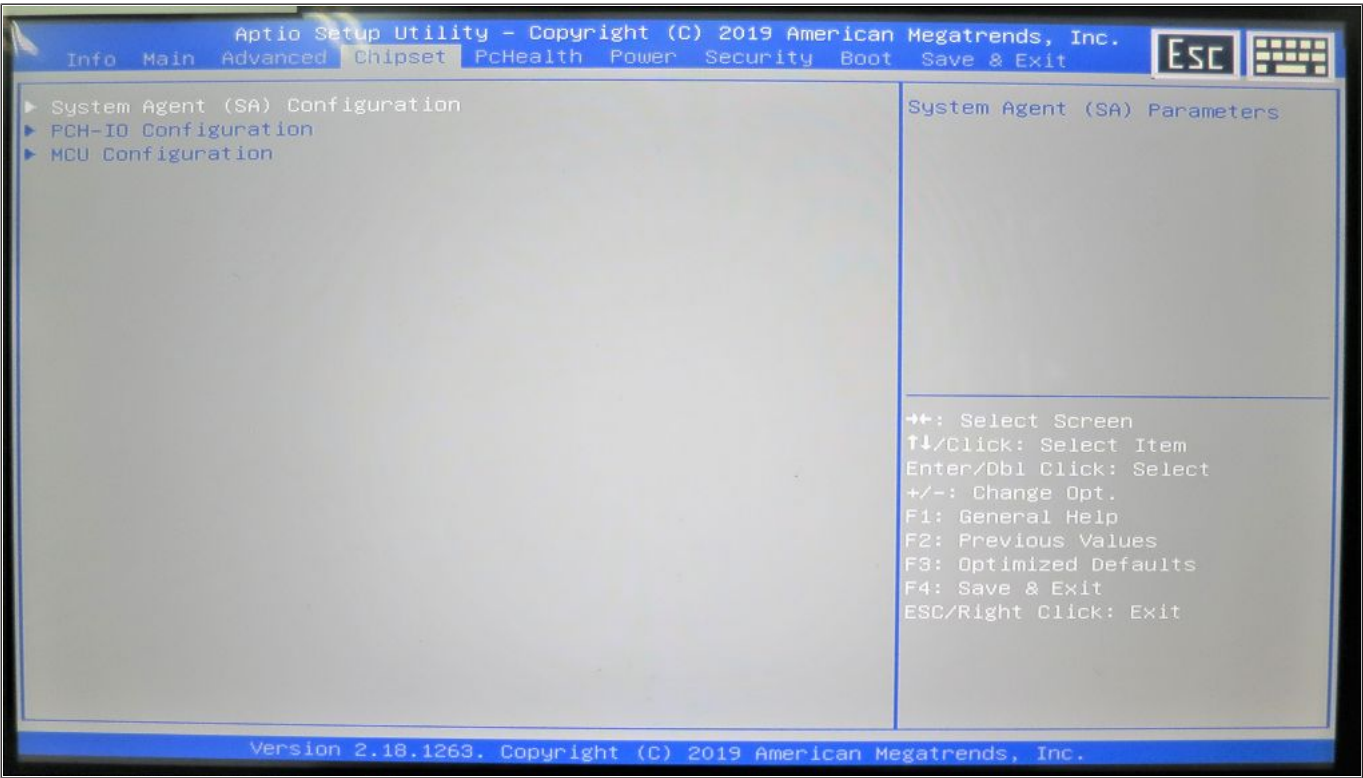
8.1.3.12 USB Configuration



Legacy USB Support:	Enables Legacy USB Support. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications.
XHCI Hand-off:	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support:	Enable/Disable USB Mass Storage Driver Support.
Port 60/64 Emulation:	Enables I/O port 60h/64h emulation support. This should be enabled for the complete USB keyboard legacy support for non-USB aware OSes.
USB transfer time-out:	The time-out value for Control, Bulk, and Interrupt transfers.
Device reset time-out:	USB mass storage device Start Unit command time-out.

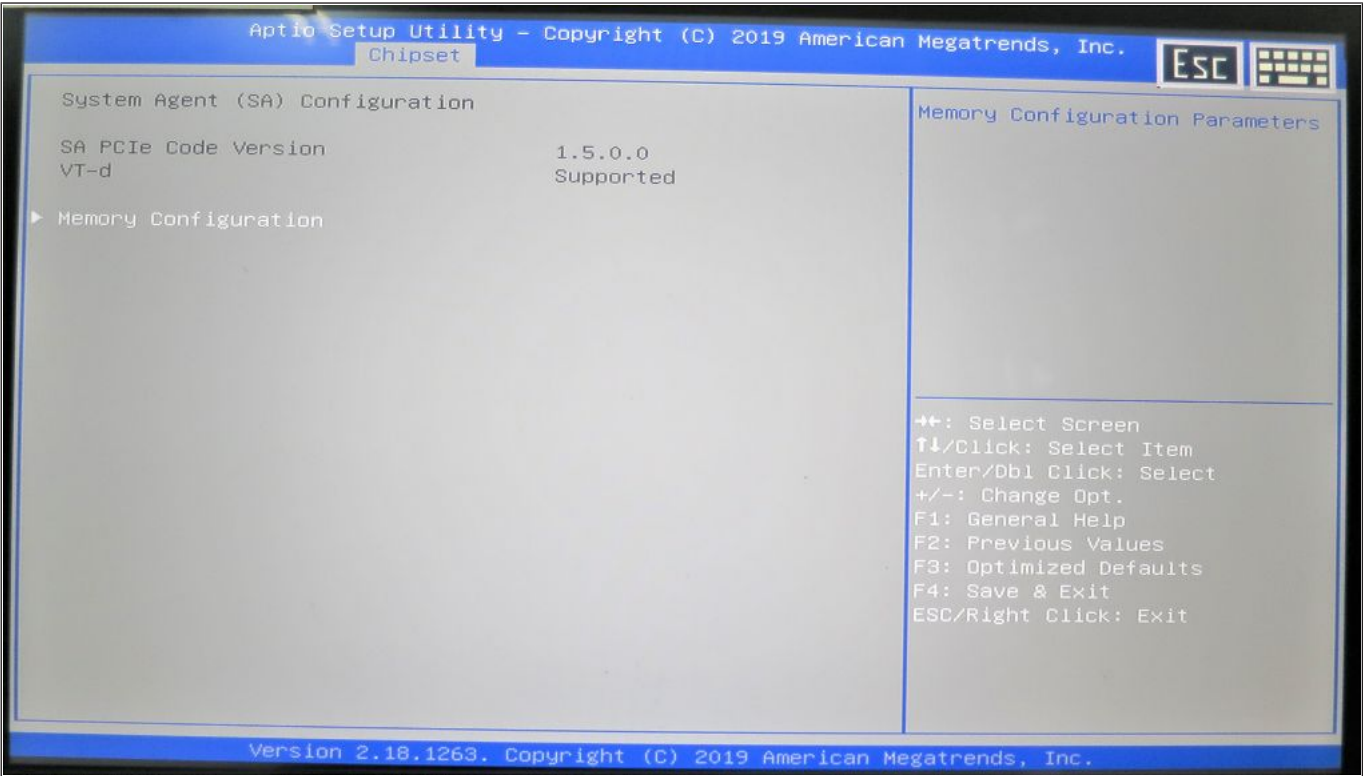
Device power-up delay:	Maximum time the device will take before it properly reports itself to the Host Controller. AUTO uses default value: for a Root port, it is 100 ms. For a Hub port, the delay is taken from Hub descriptor.
Mass Storage Devices:	This setting is visible if there are USB mass storage devices plugged in.

8.1.4 Chipset



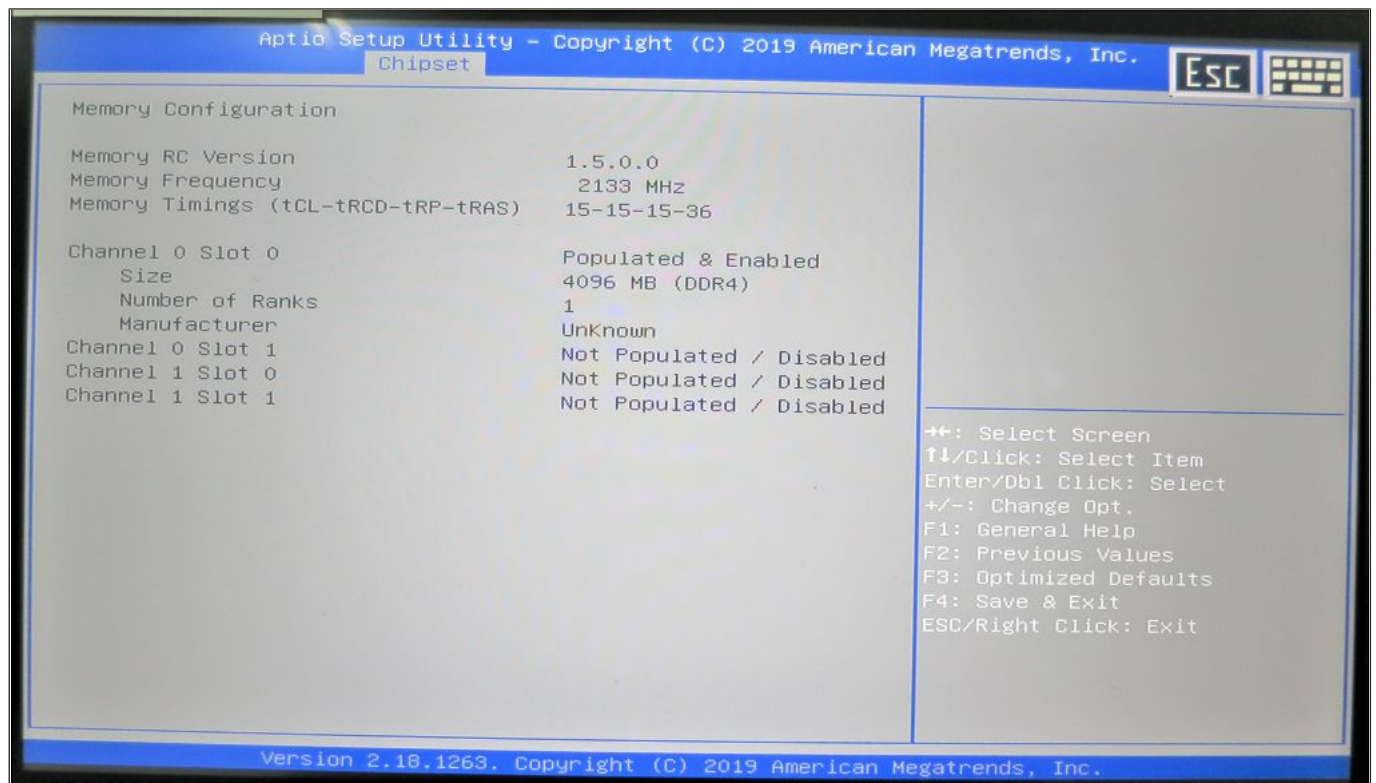
System Agent (SA) Configuration:	System Agent (SA) Parameters
PCH-IO Configuration:	PCH Parameters
MCU Configuration:	MCU Parameters

8.1.4.1 System Agent (SA) Configuration

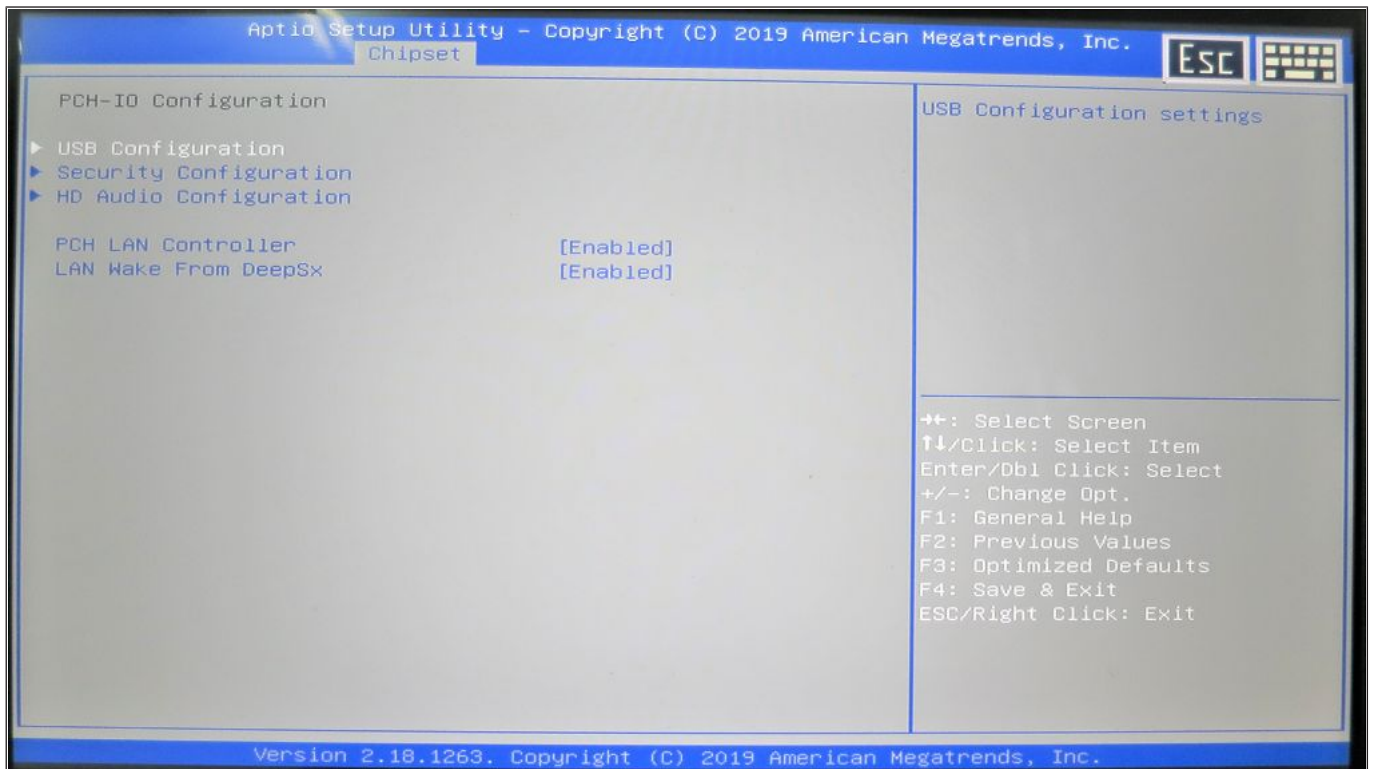


Memory Configuration:	Memory Configuration Parameters
-----------------------	---------------------------------

8.1.4.1.1 Memory Configuration

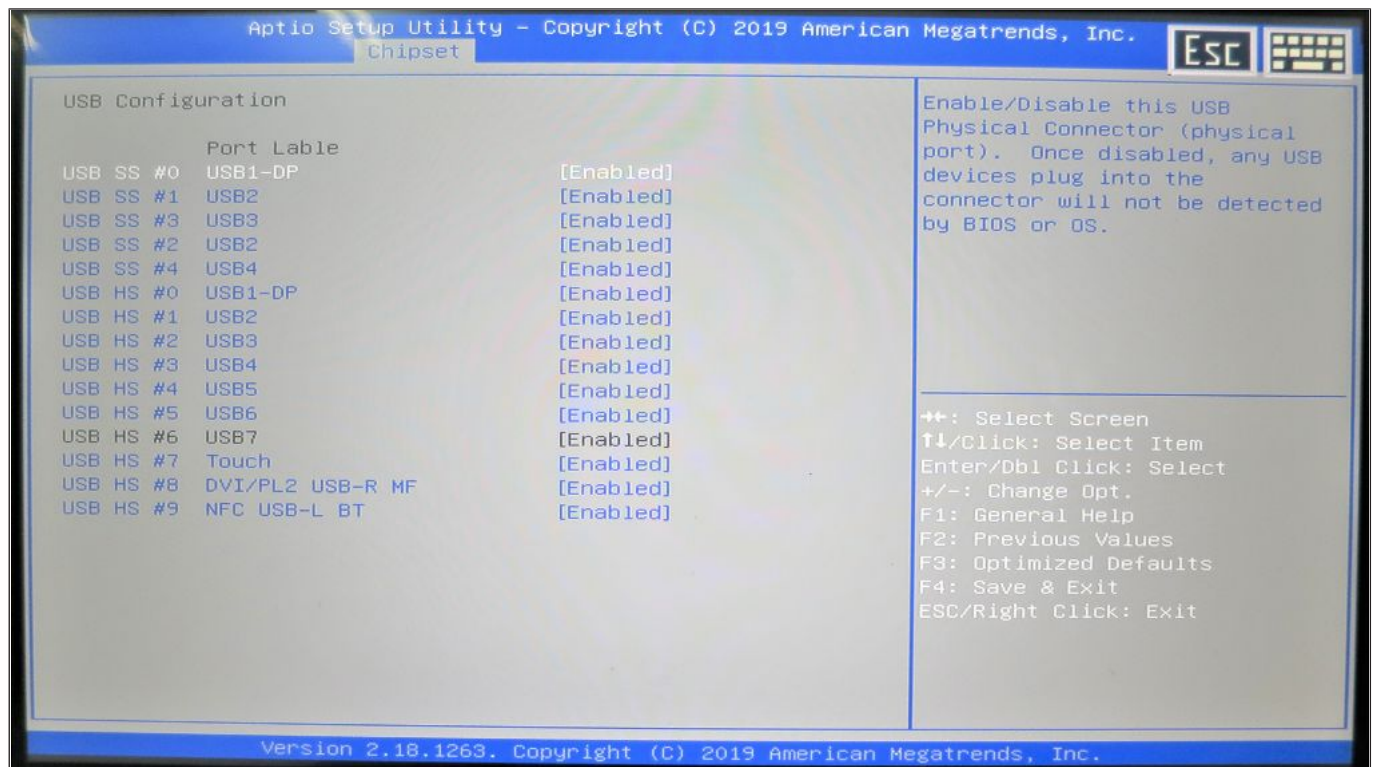


8.1.4.2 PCH-IO Configuration



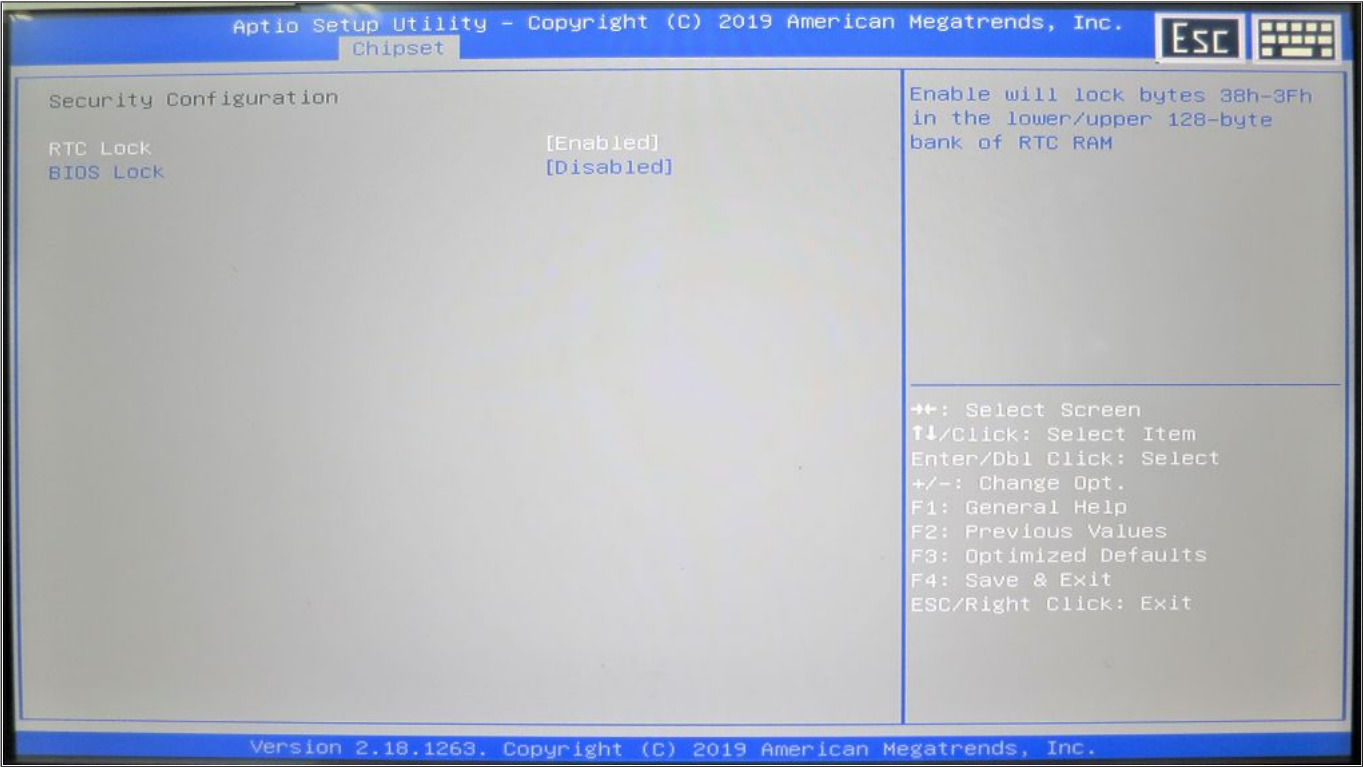
PCH LAN Controller:	Enable/Disable PCH LAN Controller.
LAN Wake From DeepSx:	Enable/Disable LAN Wake From DeepSx.

8.1.4.2.1 USB Configuration



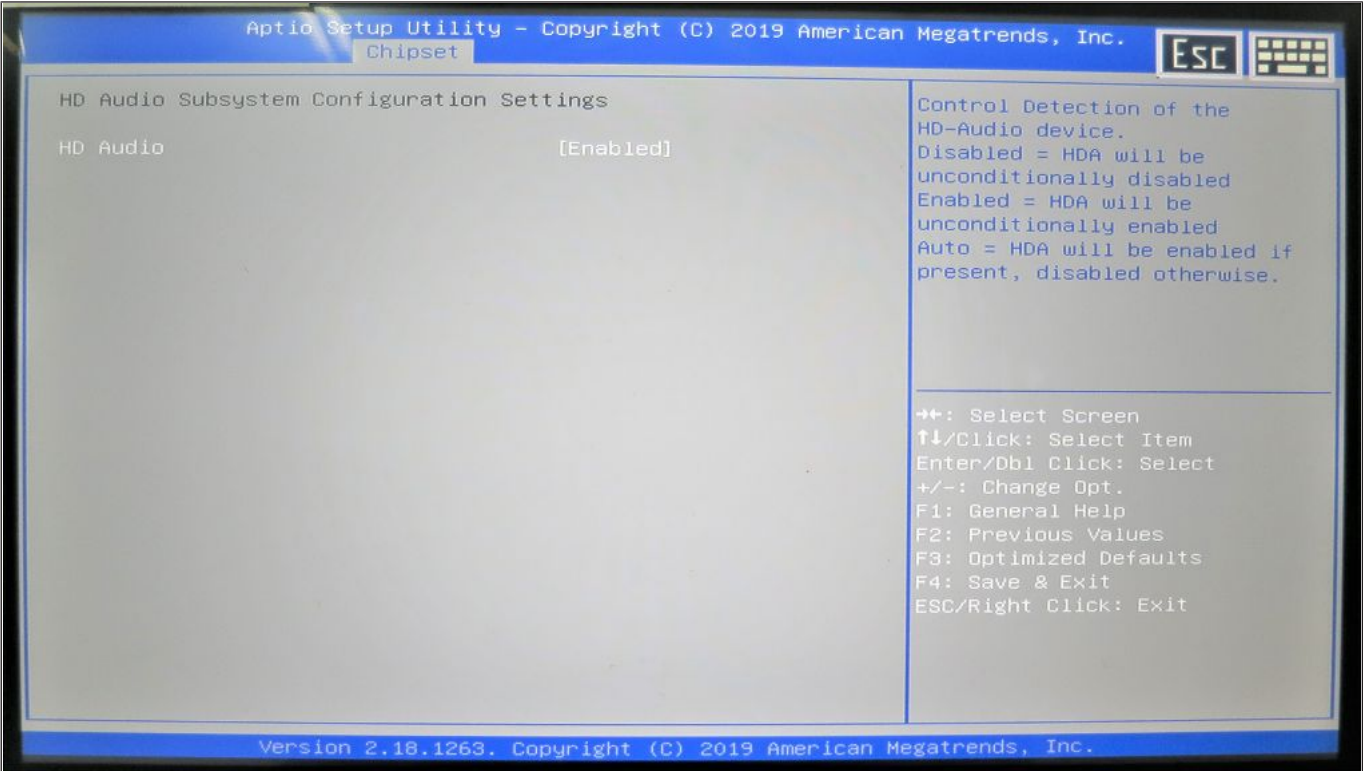
USB SS #0 USB1-DP:	Enable or disable this USB Physical Connector (physical port). Once disabled, any USB devices plugged into the connector will not be detected by BIOS or OS.
USB SS #1 USB2:	
USB SS #3 USB3:	
USB SS #2 USB2:	
USB SS #4 USB4:	
USB HS #0 USB1-DP:	
USB HS #1 USB2:	
USB HS #2 USB3:	
USB HS #3 USB4:	
USB HS #4 USB5:	
USB HS #5 USB6:	
USB HS #6 USB7:	
USB HS #7 Touch:	
USB HS #8 DVI/PL2 USB-R MF:	
USB HS #9 NFC USB-L BT:	

8.1.4.2.2 Security Configuration



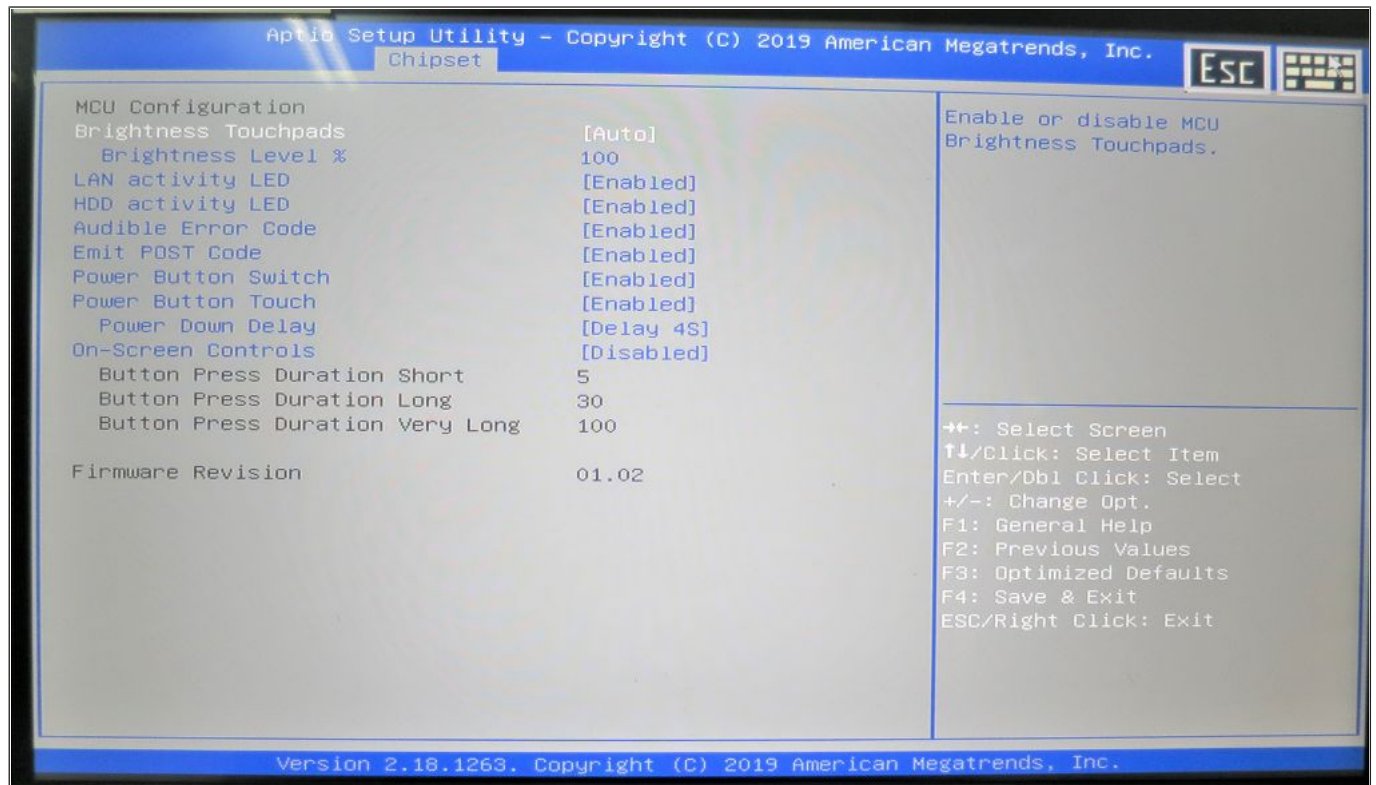
RTC Lock:	Enable will lock bytes 38h-3Fh in the lower/upper 128-byte bank of RTC RAM.
BIOS Lock:	Enable/Disable the PCH BIOS Lock Enable feature. Required to be enabled to ensure SMM protection of flash.

8.1.4.2.3 HD Audio Configuration



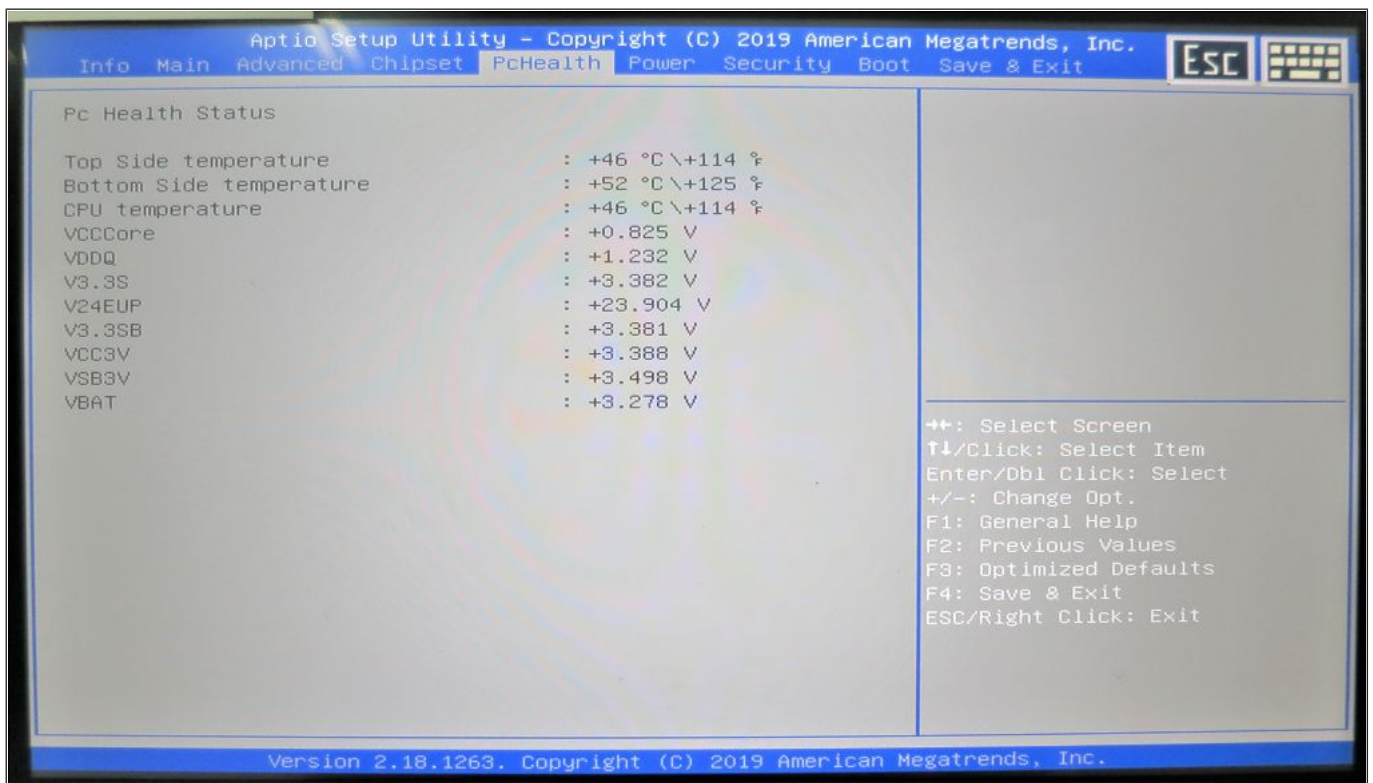
HD Audio:	Enable/Disable HD Audio.
-----------	--------------------------

8.1.4.3 MCU Configuration

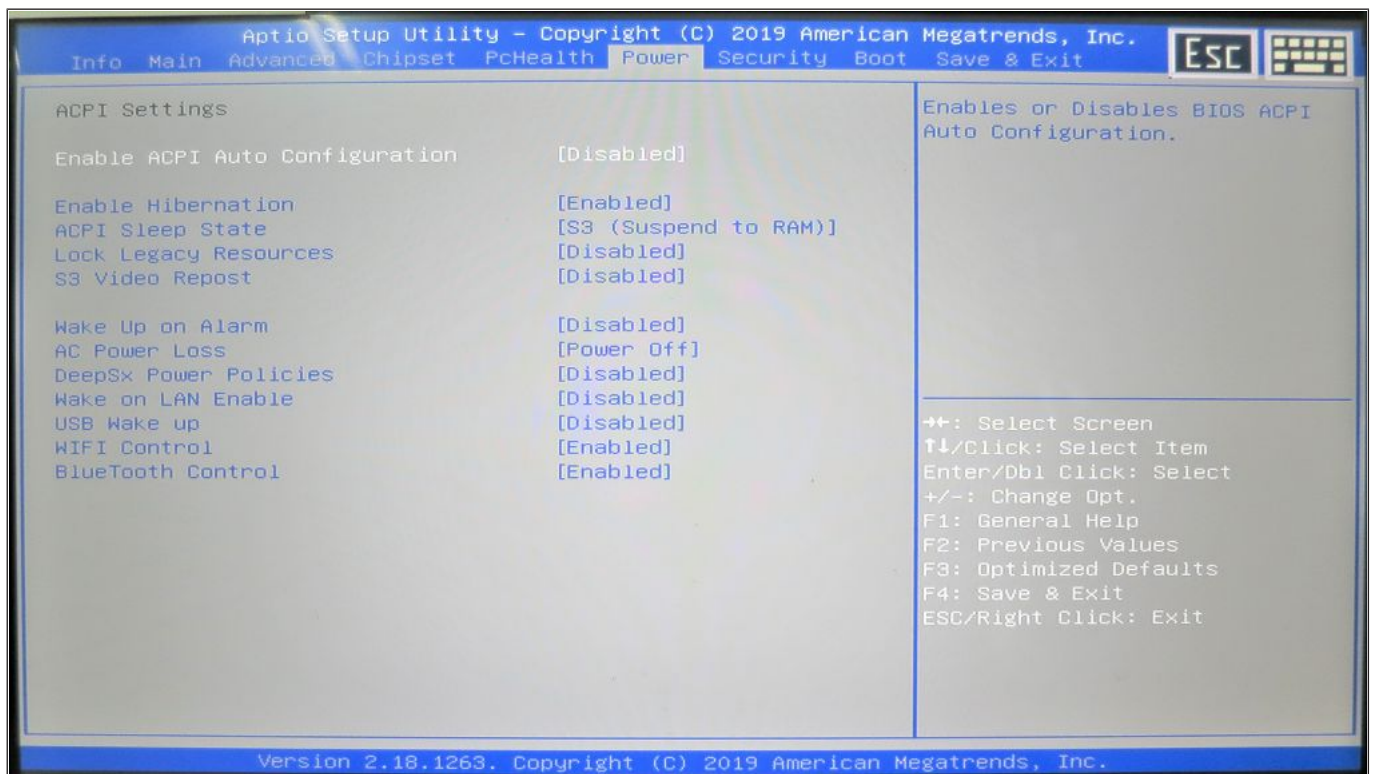


Brightness Touchpads:	Enable or Disable MCU Brightness Touchpads.
Brightness Level %:	Brightness Level Control, Value 10-100.
LAN activity LED:	Enable or Disable MCU LAN activity LED.
HDD activity LED:	Enable or Disable HDD activity LED.
Audible Error Code:	Emit error code using the system beeper/speaker
Emit POST Code:	Emit 8-bit BIOS POST code starting from MSB. Long blink/beep represent "1", short blink/beep represent "0"
Power Button Switch:	Enable or Disable the Power Button Switch.
Power Button Touch:	Enable or Disable the Power Button Touch.
Power Down Delay:	Power Button Power Down mode.
On-screen Controls:	To enable On-screen control.

8.1.5 PC Health



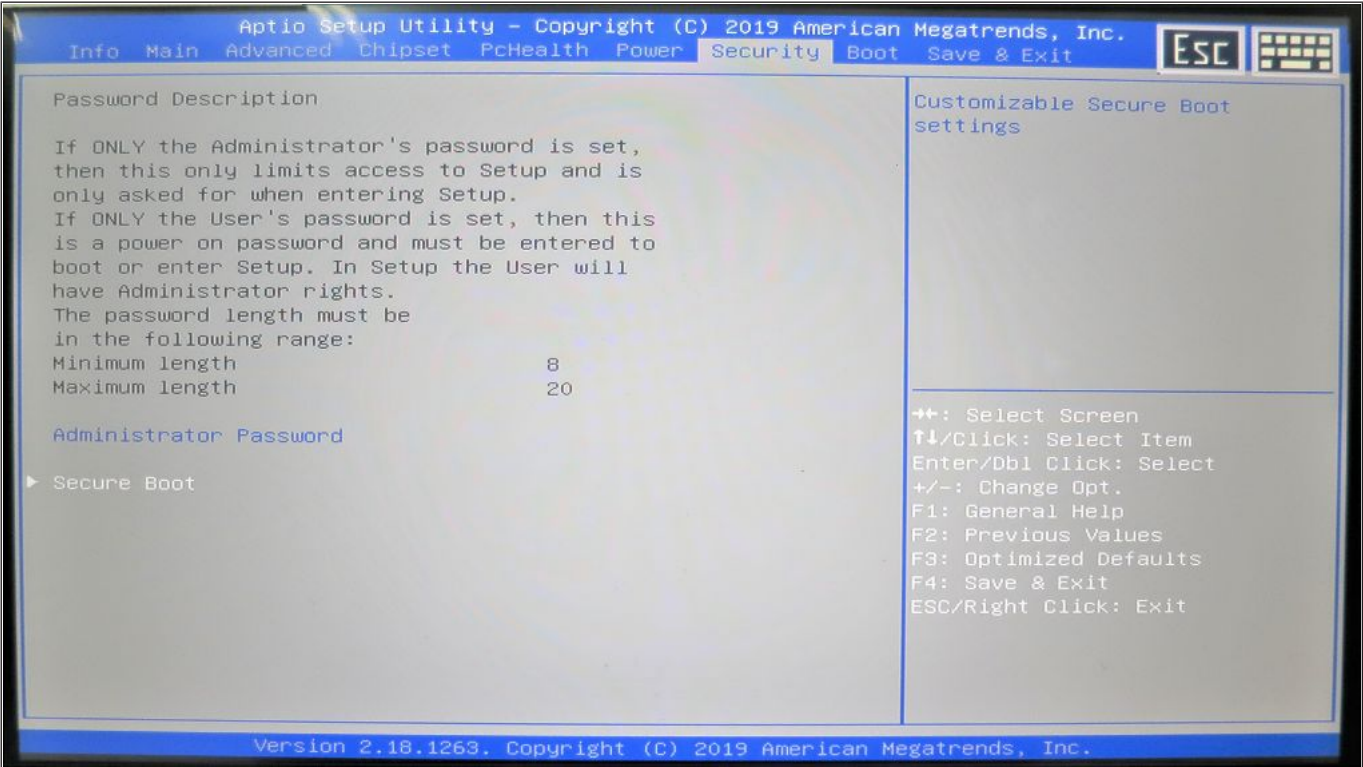
8.1.6 Power



Enable ACPI Auto Configuration:	Enables or Disables BIOS ACPI Auto Configuration.
Enable Hibernation:	Enables or Disables System ability to hibernate (OS/S4 Sleep State). This option may not be effective with some OS.
ACPI Sleep State:	Select the highest ACPI Sleep State the System will enter when the SUSPEND button is pressed.
Lock Legacy Resources:	Enables or Disables Lock or Legacy Resources.
S3 Video Repost:	Enable/Disable S3 Video Repost.
Wake Up on Alarm:	Enables or Disables System wake up on alarm event. When enabled, system will wake on the hr::min::sec specified.
AC Power Loss:	AC Power Loss. Options available: 1) Power Off 2) Follow AC Power 3) Last State
DeepSx Power Policies:	Enable/Disable DeepSx Power Policies.
Wake on LAN Enable:	Enables or Disables System wake up on LAN event.
USB Wake up:	Enable/Disable USB Wake up.
WIFI Control:	WIFI Control, Enabled/Disabled.

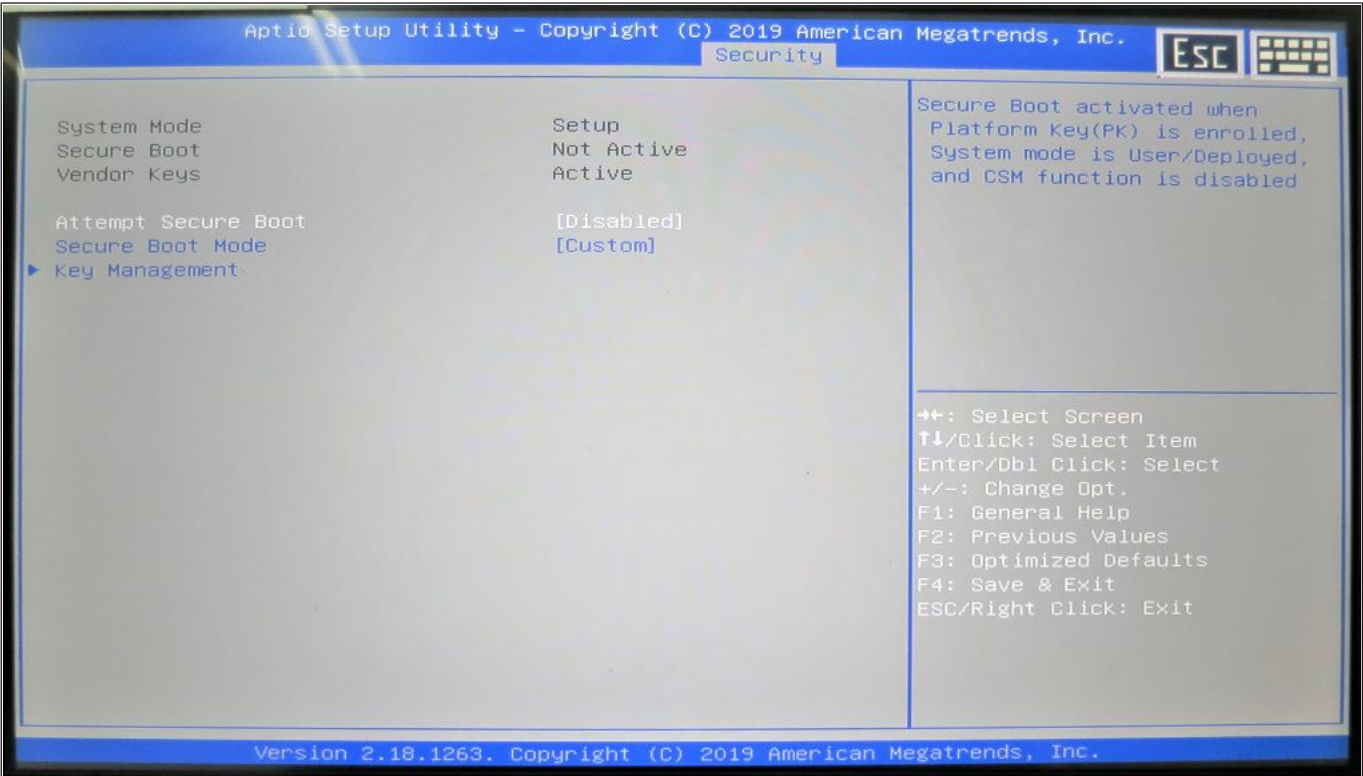
BlueTooth Control:	BlueTooth control, Enabled/Disabled.
--------------------	--------------------------------------

8.1.7 Security



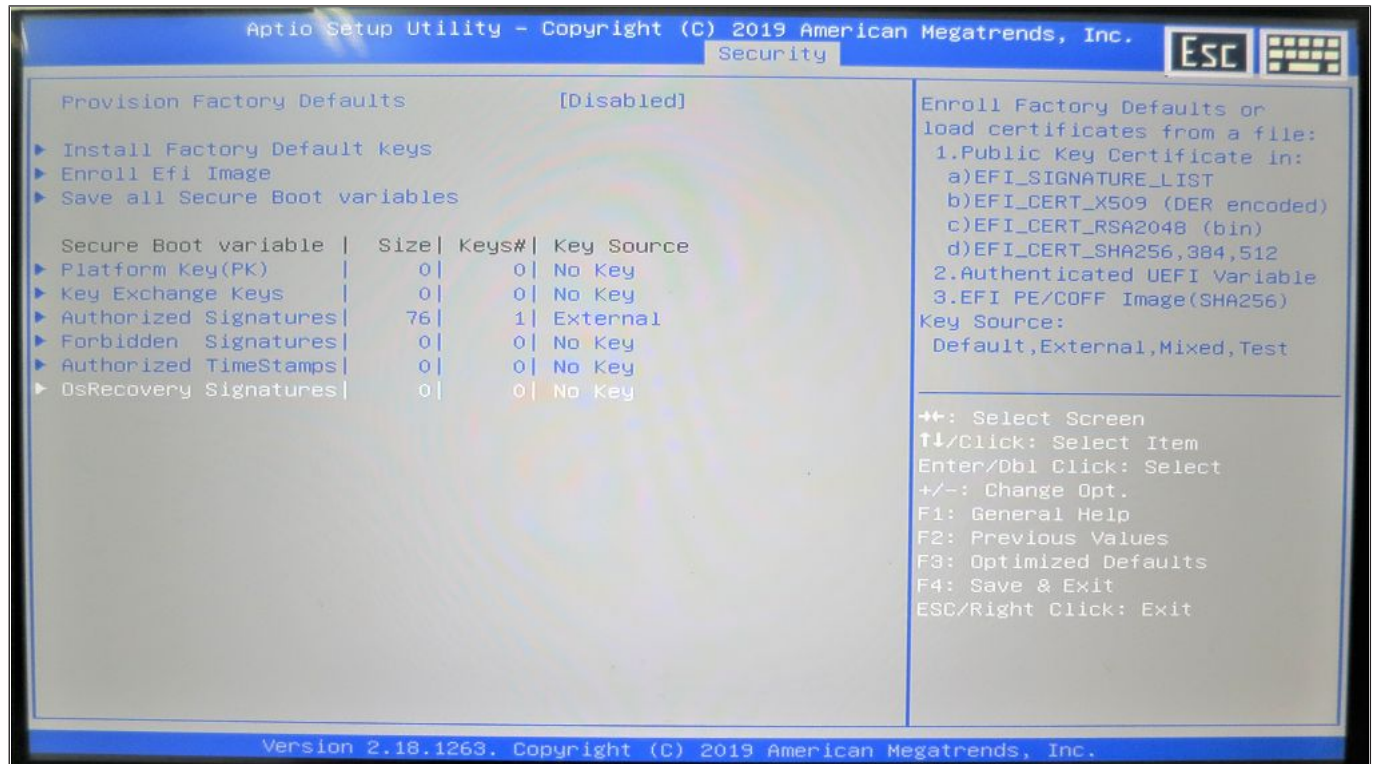
Administrator Password:	Set Administrator Password.
-------------------------	-----------------------------

8.1.7.1 Secure Boot



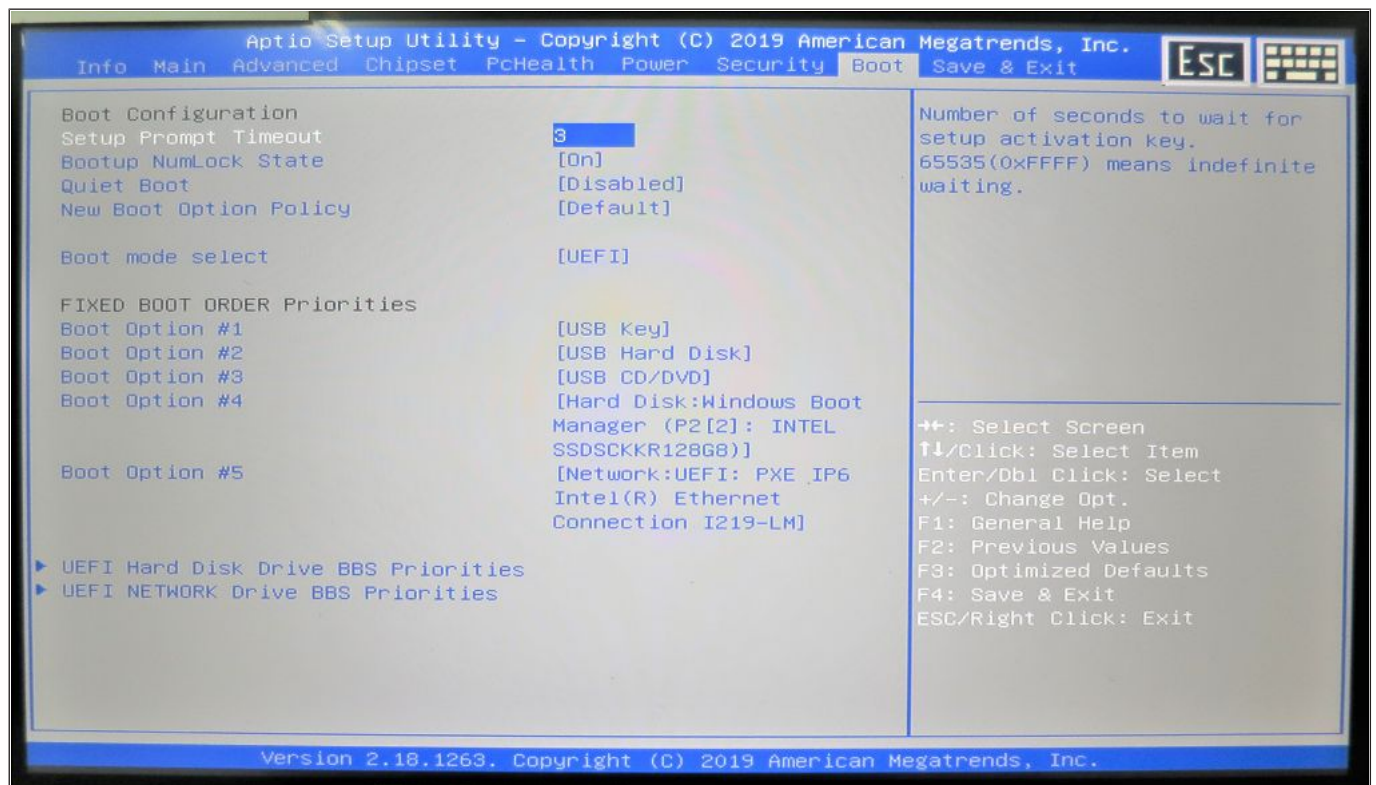
Attempt Secure Boot:	Enable/Disable Attempt Secure Boot.
Secure Boot Mode:	Secure Boot is activated when Platform Key (PK) is enrolled, System mode is User/Deployed, and CSM function is disabled.

8.1.7.1.1 Key Management



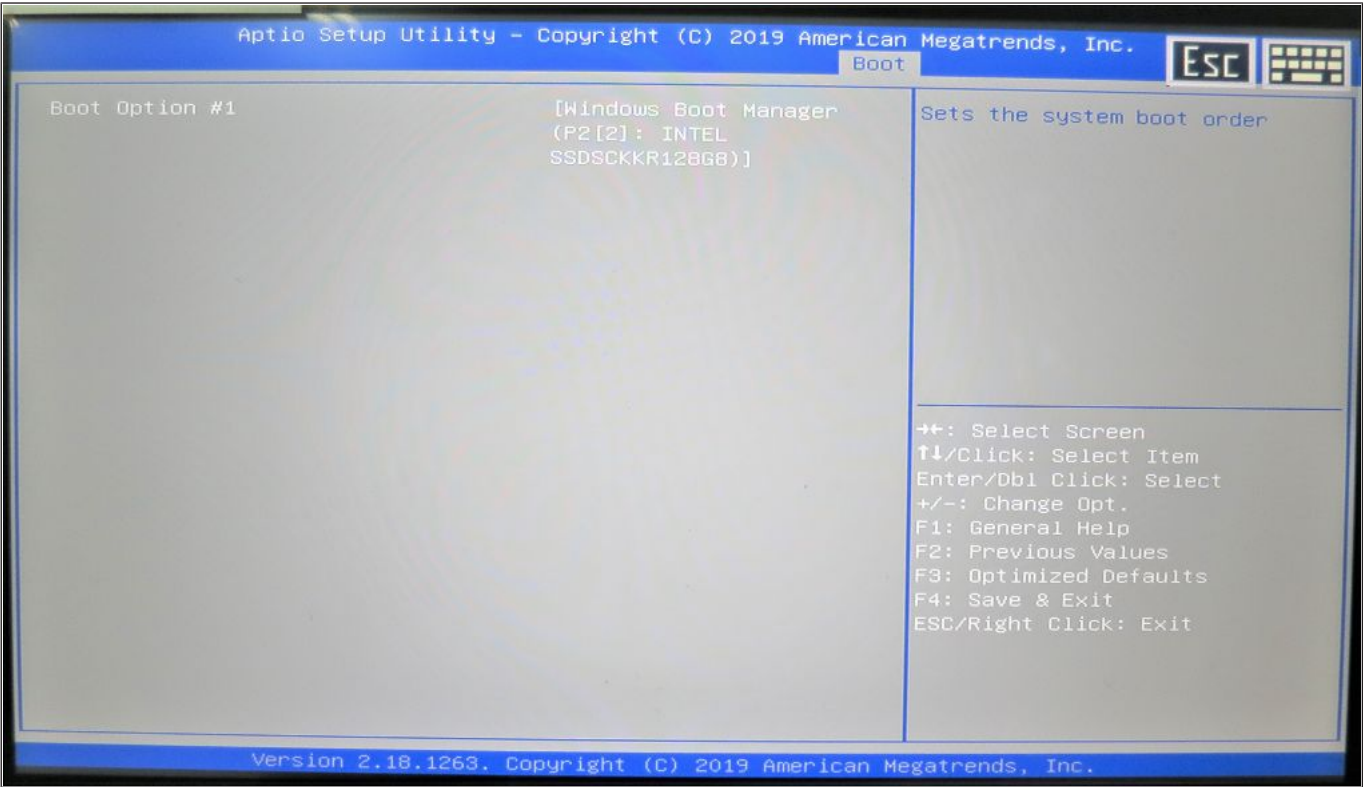
Install Factory Default Keys:	Force system to User Mode – install all Factorz Default keys.
Enroll Efi Image:	Allow the image to run in Secure Boot mode. Enroll SHA256 Hash certificate of a PE image into Authorized Signature Database (DB).
Platform Key (PK):	Enroll Factory Defaults or load certificates from a file: 1. Public Key Certificate in: a) EFI_SIGNATURE_LIST b) EFI_CERT_X509 (DER encoded) c) EFI_CERT_RSA2048 (bin) d) EFI_CERT_SHA256, 384, 512 2. Authenticated UEFI Variable 3. EFI PE/COFF Image (SHA256) Key Source: Default, External, Mixed, Test
Key Exchange Keys:	
Authorized Signatures:	
Forbidden Signatures:	
Authorized TimeStamps:	
OsRecovery Signatures:	

8.1.8 Boot



Setup Prompt Timeout:	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.
Bootup NumLock State:	Select the keyboard NumLock State.
Quiet Boot:	Enables or disables Quiet Boot option.
New Boot Option Policy:	Controls the placement of newly detected UEFI boot options.
Boot mode select:	Select boot mode LEGACY/UEFI.
Boot Option #1:	Sets the system boot order.
Boot Option #2:	
Boot Option #3:	
Boot Option #4:	
Boot Option #5:	

8.1.8.1 UEFI Hard Disk Drive BBS Priorities



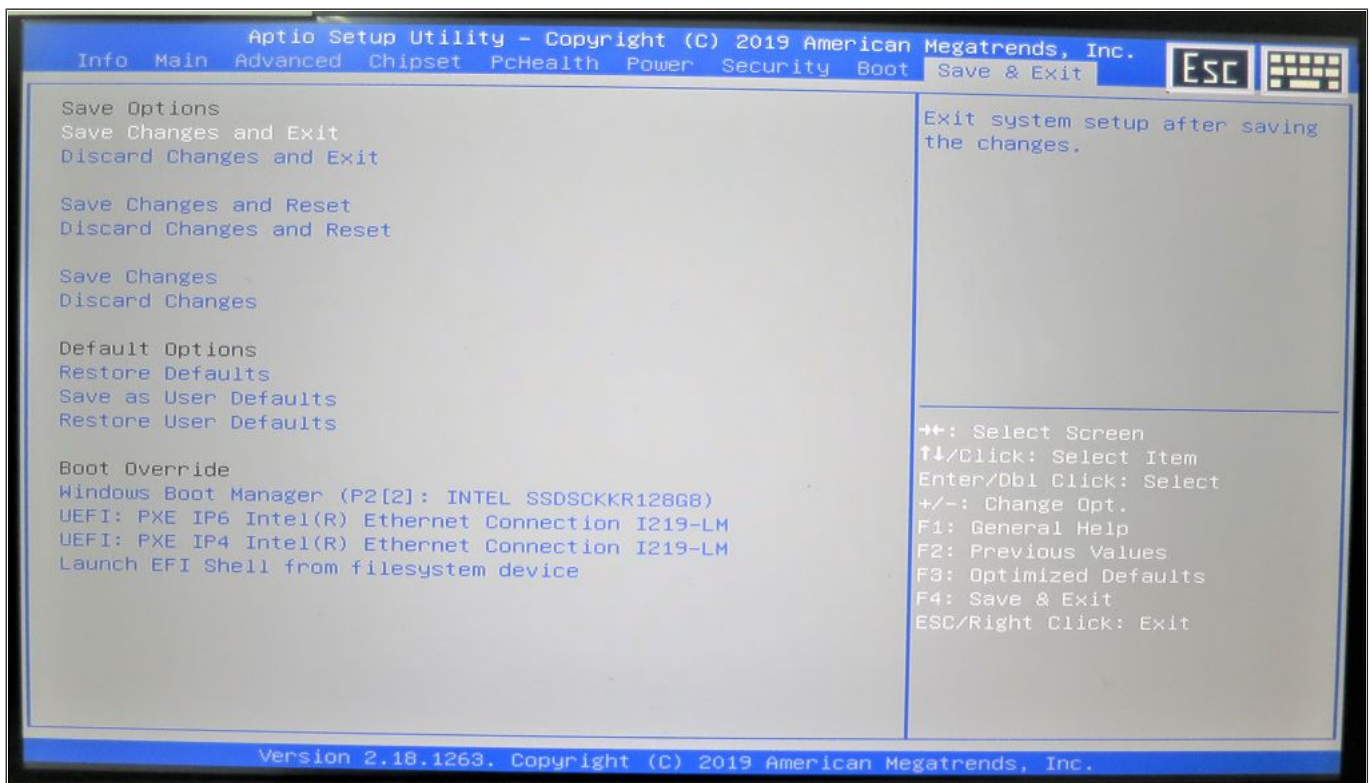
Boot Option #1:	Sets the system boot order.
-----------------	-----------------------------

8.1.8.2 UEFI NETWORK Drive BBS Priorities



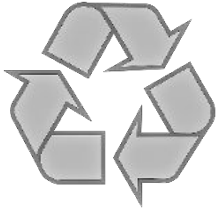
Boot Option #1:	Sets the system boot order.
Boot Option #2:	Sets the system boot order.

8.1.9 Save & Exit



Save Changes and Exit:	Exit system setup after saving the changes.
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.
Launch EFI Shell from filesystem device:	Attempts to Launch EFI Shell application (Shell.efi) from one of the available filesystem devices.

9 Recycling



This product was designed according to our internal norm “Environmental conscious product design and development”.

The system is manufactured without the use of CFC and CHC and is produced mainly from reusable components and materials.

The processed plastics can, for the most part, be recycled. Even the precious metals can be recovered.

Diebold Nixdorf guarantees the environmentally safe disposal of these parts in a Recycling Center, which is certified pursuant to ISO 9001 and ISO 14001.

Please contact your competent branch for information on how to return and reuse devices and disposable materials.

DIEBOLD NIXDORF

5995 Mayfair Road | North Canton, OH 44720 | United States

© 2021 Diebold Nixdorf, Incorporated. All Rights Reserved.

