EPS-CFS2

Intel® 8th/9th Coffee Lake Rugged w/Fan Embedded System

Quick Reference Guide

2nd Ed – 17 November 2020

Part No. E2017DAK1A1R

FCC Statement

THIS DEVICE COMPLIES WITH PART 15 FCC RULES. OPERATION IS SUBJECT TO THE FOLLOWING TWO CONDITIONS:

(1) THIS DEVICE MAY NOT CAUSE HARMFUL INTERFERENCE.

(2) THIS DEVICE MUST ACCEPT ANY INTERFERENCE RECEIVED INCLUDING INTERFERENCE THAT MAY CAUSE UNDESIRED OPERATION.

THIS EQUIPMENT HAS BEEN TESTED AND FOUND TO COMPLY WITH THE LIMITS FOR A CLASS "A" DIGITAL DEVICE, PURSUANT TO PART 15 OF THE FCC RULES.

THESE LIMITS ARE DESIGNED TO PROVIDE REASONABLE PROTECTION AGAINST HARMFUL INTERFERENCE WHEN THE EQUIPMENT IS OPERATED IN A COMMERCIAL ENVIRONMENT. THIS EQUIPMENT GENERATES, USES, AND CAN RADIATE RADIO FREQUENCY ENERGY AND, IF NOT INSTATLLED AND USED IN ACCORDANCE WITH THE INSTRUCTION MANUAL, MAY CAUSE HARMFUL INTERFERENCE TO RADIO COMMUNICATIONS.

OPERATION OF THIS EQUIPMENT IN A RESIDENTIAL AREA IS LIKELY TO CAUSE HARMFUL INTERFERENCE IN WHICH CASE THE USER WILL BE REQUIRED TO CORRECT THE INTERFERENCE AT HIS OWN EXPENSE.

A Message to the Customer

Avalue Customer Services

Each and every Avalue's product is built to the most exacting specifications to ensure reliable performance in the harsh and demanding conditions typical of industrial environments. Whether your new Avalue device is destined for the laboratory or the factory floor, you can be assured that your product will provide the reliability and ease of operation for which the name Avalue has come to be known.

Your satisfaction is our primary concern. Here is a guide to Avalue's customer services. To ensure you get the full benefit of our services, please follow the instructions below carefully.

Technical Support

We want you to get the maximum performance from your products. So if you run into technical difficulties, we are here to help. For the most frequently asked questions, you can easily find answers in your product documentation. These answers are normally a lot more detailed than the ones we can give over the phone. So please consult the user's manual first.

To receive the latest version of the user's manual; please visit our Web site at:

http://www.avalue.com.tw/

Content

1. Getting Started

1.1 Safety Precautions

Warning!

Always completely disconnect the power cord from your chassis whenever you work with the hardware. Do not make connections while the power is on. Sensitive electronic components can be damaged by sudden power surges. Only experienced electronics personnel should open the PC chassis.

Caution!

Always ground yourself to remove any static charge before touching the CPU card. Modern electronic devices are very sensitive to static electric charges. As a safety precaution, use a grounding wrist strap at all times. Place all electronic components in a static-dissipative surface or static-shielded bag when they are not in the chassis.

1.2 EPS-CFS2 Packing List

- 1 x EPS-CFS2 Intel® 8th/9th Coffee Lake Rugged w/Fan Embedded System
- Other major components include the followings:
  - Screw kit
  - 120W AC-DC Adapter
  - Power Cord
  - Wall Mount Kit

If any of the above items is damaged or missing, contact your retailer.

1.3 EPS-CFS2 System Specifications

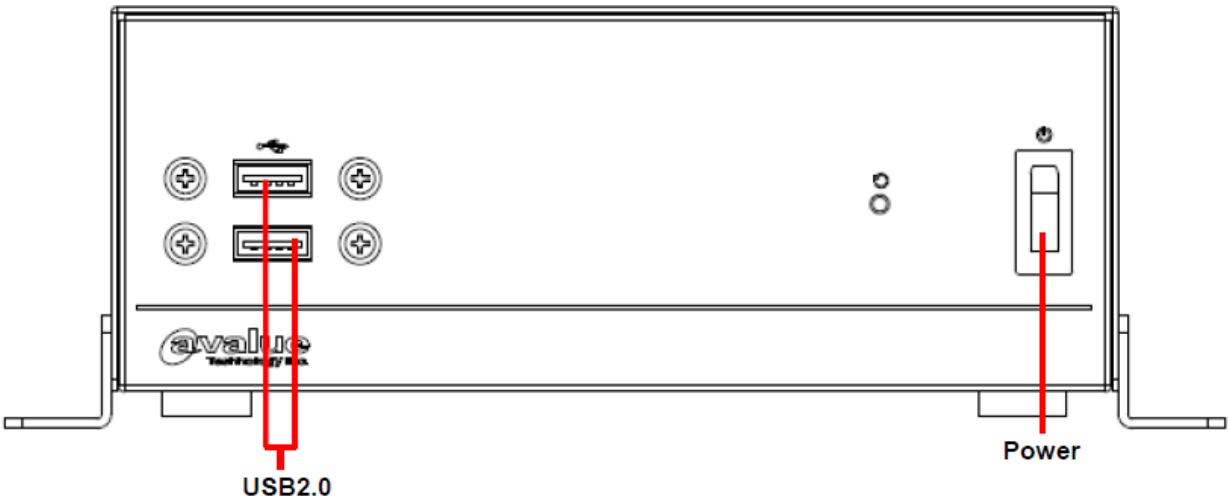
System	
CPU	Intel® Core™ i7-8700T Processor (12M Cache, up to 4.00 GHz) Intel® Core™ i5-8500T Processor (9M Cache, up to 3.50 GHz) Intel® Core™ i3-8100T Processor (6M Cache, 3.10 GHz) Intel® Pentium® Gold G5400T Processor (4M Cache, 3.10 GHz) Intel® Celeron® G4900T Processor (2M Cache, 2.90 GHz
SBC	ECM-CFS
BIOS	AMI uEFO BIOS,256 Mbit SPI Flash ROM iAMT supported
System Chipset	Intel® Q370/H310 Express Chipset
System Memory	1 x 260-Pin SO-DIMM Socket Up to 32GB DDR4 2400/2666MHz
Watchdog Timer	H/W Reset, 1sec. – 65535sec./min. 1sec. step
H/W Status Monitor	Monitoring System Temperature, Voltage and FAN Status with Auto Throttling Control
Expansion	
Expansion	1 x Mini PCIe Socket (Q370 PCIe/SATA/USB 2.0) (H310 SATA/USB2.0)
Storage	
Combination	1 x mSATA 2 x 2.5” Drive Bay (Internal)
Front I/O	
USB Port	2 x USB 2.0
Button	1 x Power On/Off, 1 x Reset button
Rear I/O	
USB Port	4 x USB 3.1 (w/Q370 Gen2; w/H310 Gen1)
Serial Port	2 x RS-232
LED	2 x LED for PWR and HDD LED
LAN	2 x Giga LAN w/LED
Audio	1 x Mic-In, 1 x Line-Out
GPIO	1 x 8-bit GPIO
Others	2 x Antenna with Dust Cover
Display	
Chipset	Processor Graphics Intel® UHD Graphics 630 (i7-8700T, i5-8500T, i3-8100T) Intel® UHD Graphics 610 (Pentium G5400T, Celeron G4900T)

Display Interface	2 x HDMI
Resolution	HDMI: Max. resolution 4096 x 2304 @ 30Hz
Multiple Display	Dual Display
Ethernet	
Chipset	1 x Intel I211AT GbE controller 1 x Intel I219LM Gigabit Ethernet PHY
Ethernet Speed	10/100/1000 Base-Tx compatible
Ethernet Interface	2 x RJ45 w/LED
Audio	
Chipset	Realtek ALC892 Codec
Audio Interface	1 x Mic-In 1 x Line-Out
Mechanical & Environmental	
Power Connector	Lockable DC Jack
Power Requirement	12 Vdc
Power Type	AT/ATX (ATX is default setting)
ACPI	Single power ATX Support S0,S3, S4, S5 ACPI 5.0 Compliant
Dimension (W x L x H)	170mm x 195mm x 65mm 206mm x 195mm x 71mm (w/wall mount)
Weight	2.3kg (w/ package) 1.8kg (system)
Color	Black & Blue
Mounting Kit	Wall mount (standard)
Reliability	
Vibration Test	With SSD: 1.5 Grms, IEC 60068-2-64, Random, 5 ~ 500Hz, 30min/axis
Package vibration test	Without SSD: 2.16 Grms, IEC 60068-2-64, Random, 5 ~ 500Hz, 30min/axis
Shock	With SSD: 10g, IEC 60068-2-27, 11ms
Drop Test	ISTA 2A, IEC-60068-2-32 Test : Ed
Operating Temperature	With extended temperature peripherals: -10°C ~ 45°C (14°F ~ 113°F) with 0.5m/air flow With extended temperature peripherals: -10°C ~ 40°C (14°F ~ 104°F) with 0.2m/air flow
Operating Humidity	40°C @ 95% Relative Humidity, Non-condensing
Storage Temperature	-40°C ~ 75°C (-40°F ~ 167°F)
Certification	CE, FCC Class B
OS Supported	Win 10/ Linux

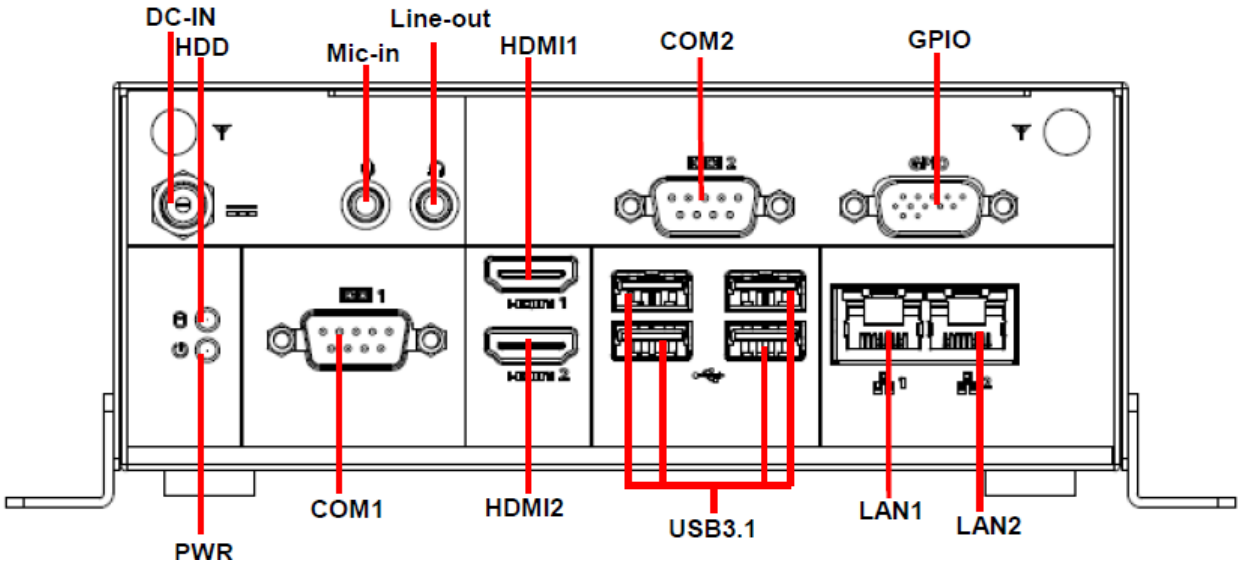
Note: Specifications are subject to change without notice.

1.4 System Overview

1.4.1 Front View



1.4.2 Rear View



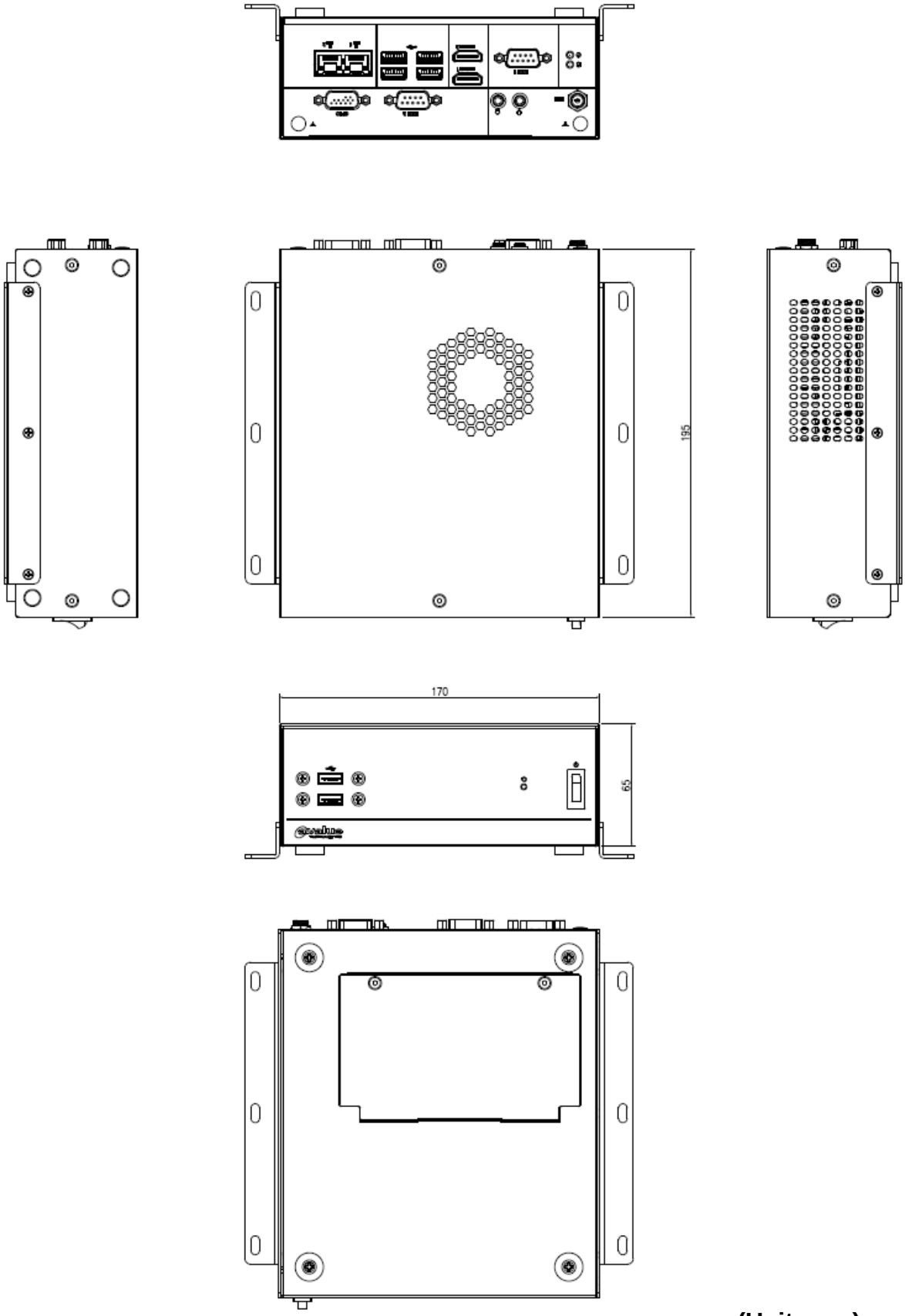
Connectors

Label	Function	Note
Power	Power on button	
USB2.0	USB 2.0 connector x 2	
USB3.1	USB 3.1 connector x 4	
COM1/2	Serial port 1/2 connector	

DC-IN	DC power-in connector
LAN1/2	RJ-45 Ethernet 1/2
HDMI1/2	HDMI connector 1/2
DC-IN	DC Power-in connector
HDD	HDD indicator
PWR	System power indicator
Mic-in	Mic-in audio jack
Line-out	Line-out audio jack
GPIO	General purpose I/O connector

1.5 System Dimensions

1.5.1 Front & Top view



(Unit: mm)

2. Hardware Configuration

Jumper and Connector Setting, BIOS Installing

For advanced information, please refer to:

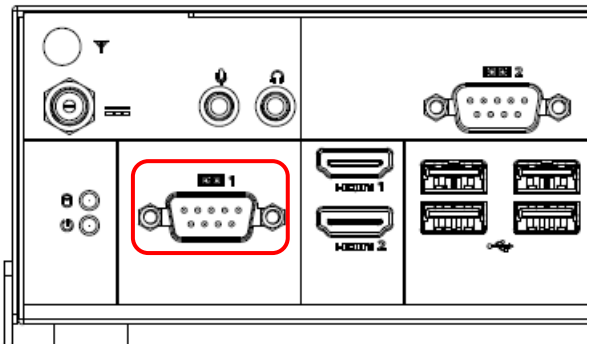
1- ECM-CFS User's Manual.

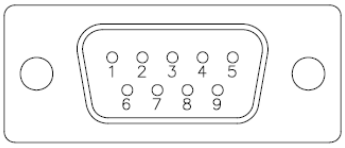
Note: If you need more information, please visit our website:

http://www.avalue.com.tw

2.1 EPS-CFS2 connector mapping

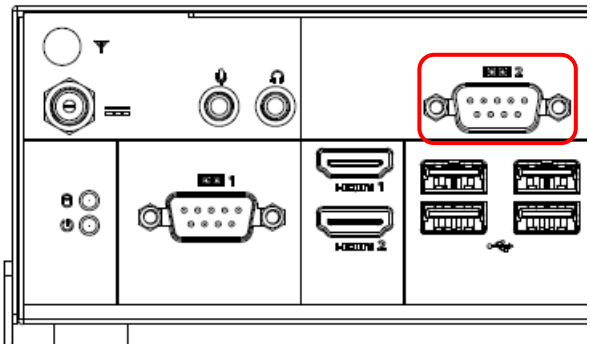
2.1.1 Serial Port 1 connector (COM1)

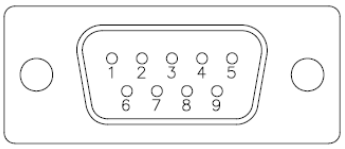




Signal	PIN	PIN	Signal
DCD#	1	6	DSR#
RXD	2	7	RTS#
TXD	3	8	CTS#
DTR#	4	9	RI#
GND	5		

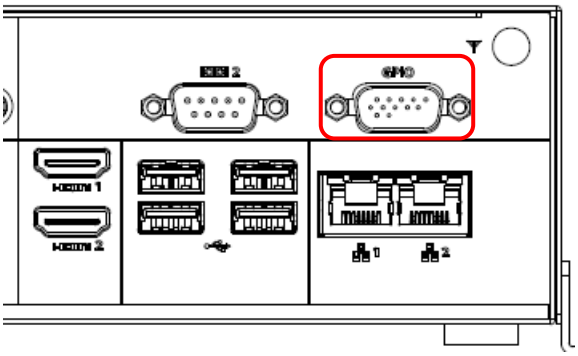
2.1.2 Serial Port 2 connector (COM2)

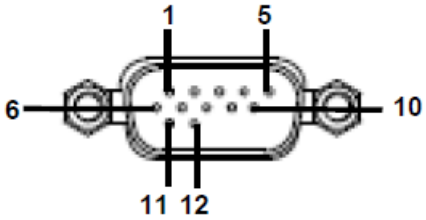




Signal	PIN	PIN	Signal
DCD#	1	6	DSR#
RXD	2	7	RTS#
TXD	3	8	CTS#
DTR#	4	9	RI#
GND	5		

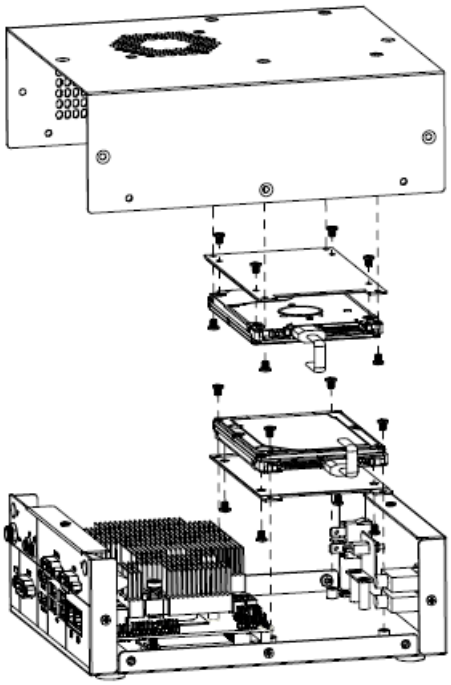
2.1.3 General purpose I/O connector (GPIO)





Signal	PIN	PIN	Signal
DIO_GP20	1	7	DIO_GP23
DIO_GP10	2	8	DIO_GP13
DIO_GP21	3	9	SMB_SCL_S0
DIO_GP11	4	10	SMB_SDA_S0
DIO_GP22	5	11	GND
DIO_GP12	6	12	+5V

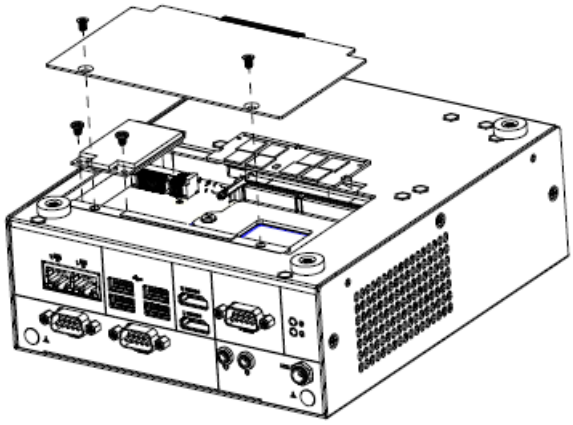
2.2 Installing SSD & Memory, Mini PCIe (EPS-CFS2)



Step1. For SSD installation, please remove the top cover, Fix SSD using the 8 screws in the Accessory Kit.

Note:

Before installing SSD, the FAN cable must be removed first while opening the chassis.



Step2. For Memory and Mini PCIe installation, Unfasten 2 screws to remove the cover.

Step3. Insert Mini PCIe card into designated locations and fasten with 2 screws to complete MPCIE installation.

Step4. Slide the DDR4 SODIMM into the memory socket and press it down until properly seated.

Step5. Re-assemble your system back through previous steps to complete the installation.

3.BIOS Setup

3.1 Introduction

The BIOS setup program allows users to modify the basic system configuration. In this following chapter will describe how to access the BIOS setup program and the configuration options that may be changed.

3.2 Starting Setup

AMI BIOS™ is immediately activated when you first power on the computer. The BIOS reads the system information contained in the NVRAM and begins the process of checking out the system and configuring it. When it finishes, the BIOS will seek an operating system on one of the disks and then launch and turn control over to the operating system.

While the BIOS is in control, the Setup program can be activated in one of two ways:
By pressing <F2> or <Del> immediately after switching the system on, or
By pressing the <F2> or <Del> key when the following message appears briefly at the left-top of the screen during the POST (Power On Self Test).

Press <F2> or <Del> to enter SETUP

If the message disappears before you respond and you still wish to enter Setup, restart the system to try again by turning it OFF then ON or pressing the "RESET" button on the system case. You may also restart by simultaneously pressing <Ctrl>, <Alt>, and <Delete> keys.

3.3 Using Setup

In general, you use the arrow keys to highlight items, press <Enter> to select, use the PageUp and PageDown keys to change entries, press <F1> for help and press <Esc> to quit. The following table provides more detail about how to navigate in the Setup program using the keyboard.

Button	Description
↑	Move to previous item
↓	Move to next item
←	Move to the item in the left hand
→	Move to the item in the right hand
Esc key	Main Menu -- Quit and not save changes into NVRAM Status Page Setup Menu and Option Page Setup Menu -- Exit current page and return to Main Menu
+ key	Increase the numeric value or make changes
- key	Decrease the numeric value or make changes
F1 key	General help, only for Status Page Setup Menu and Option Page Setup Menu
F2 key	Previous Values
F3 key	Optimized defaults
F4 key	Save & Exit Setup

- **Navigating Through The Menu Bar**

  Use the left and right arrow keys to choose the menu you want to be in.

Note: Some of the navigation keys differ from one screen to another.

- **To Display a Sub Menu**

  Use the arrow keys to move the cursor to the sub menu you want. Then press <Enter>. A "➢" pointer marks all sub menus.

3.4 Getting Help

Press F1 to pop up a small help window that describes the appropriate keys to use and the possible selections for the highlighted item. To exit the Help Window press <Esc> or the F1 key again.

3.5 In Case of Problems

If, after making and saving system changes with Setup, you discover that your computer no longer is able to boot, the BIOS supports an override to the NVRAM settings which resets your system to its defaults.

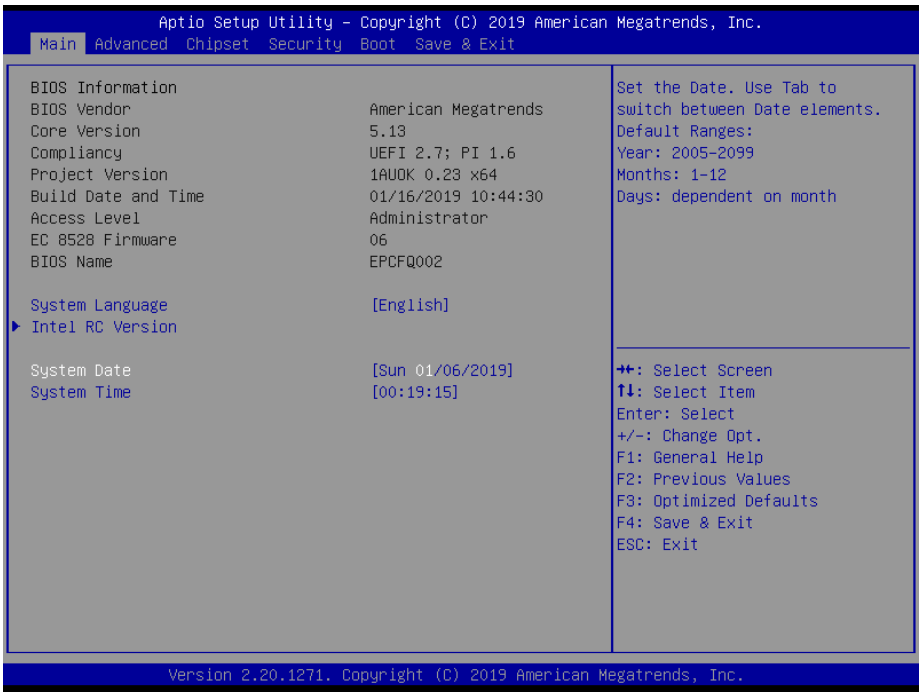
The best advice is to only alter settings which you thoroughly understand. To this end, we strongly recommend that you avoid making any changes to the chipset defaults. These defaults have been carefully chosen by both your systems manufacturer to provide the absolute maximum performance and reliability. Even a seemingly small change to the chipset setup has the potential for causing you to use the override.

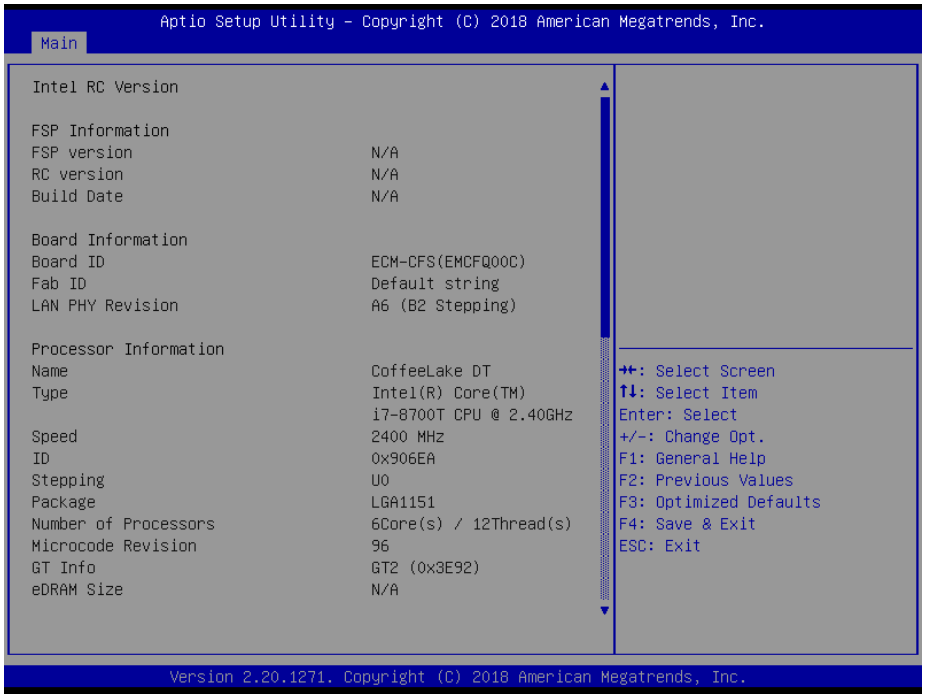
3.6 BIOS setup

Once you enter the Aptio Setup Utility, the Main Menu will appear on the screen. The Main Menu allows you to select from several setup functions and exit choices. Use the arrow keys to select among the items and press <Enter> to accept and enter the sub-menu.

3.6.1 Main Menu

This section allows you to record some basic hardware configurations in your computer and set the system clock.





3.6.1.1 System Language

This option allows choosing the system default language.

3.6.1.2 System Date

Use the system date option to set the system date. Manually enter the day, month and year.

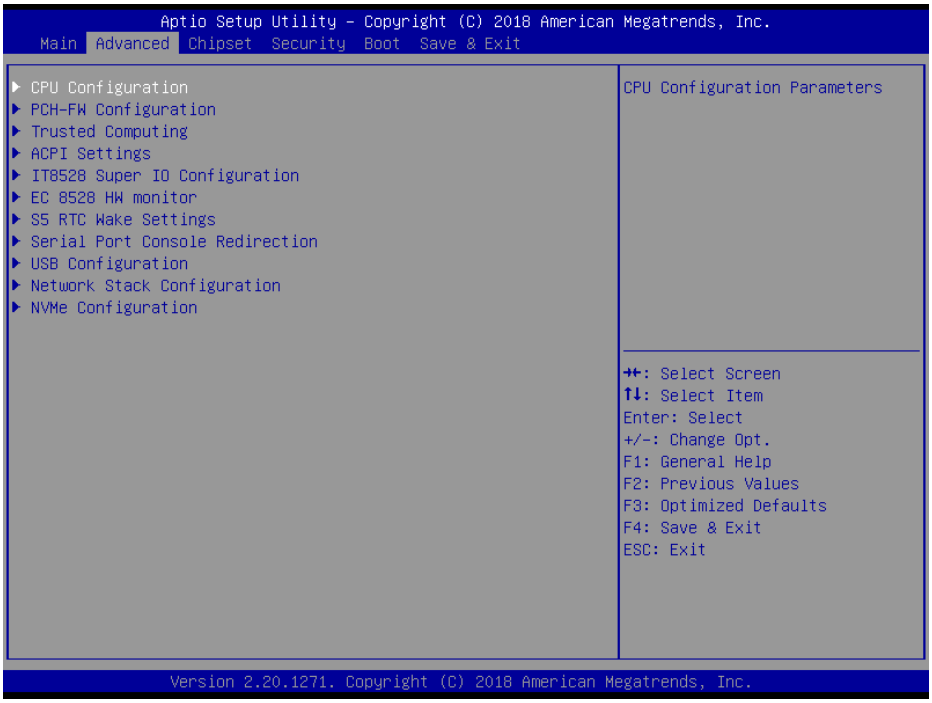
3.6.1.3 System Time

Use the system time option to set the system time. Manually enter the hours, minutes and seconds.

Note: The BIOS setup screens shown in this chapter are for reference purposes only, and may not exactly match what you see on your screen.
Visit the Avalue website (www.avalue.com.tw) to download the latest product and BIOS information.

3.6.2 Advanced Menu

This section allows you to configure your CPU and other system devices for basic operation through the following sub-menus.

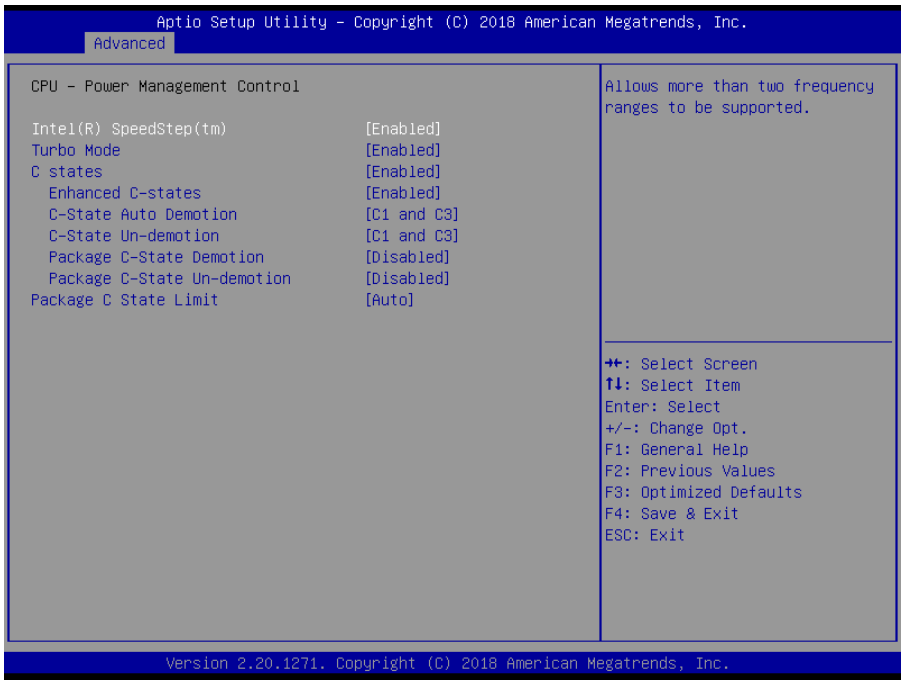


3.6.2.1 CPU Configuration

Use the CPU configuration menu to view detailed CPU specification and configure the CPU.

Item	Options	Description
Intel (VMX) Virtualization Technology	Disabled Enabled**[Default]**	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.
Active Processor Cores	All**[Default]** 1 2 3 4 5 6 7 8	Number of cores to enable in each processor package.

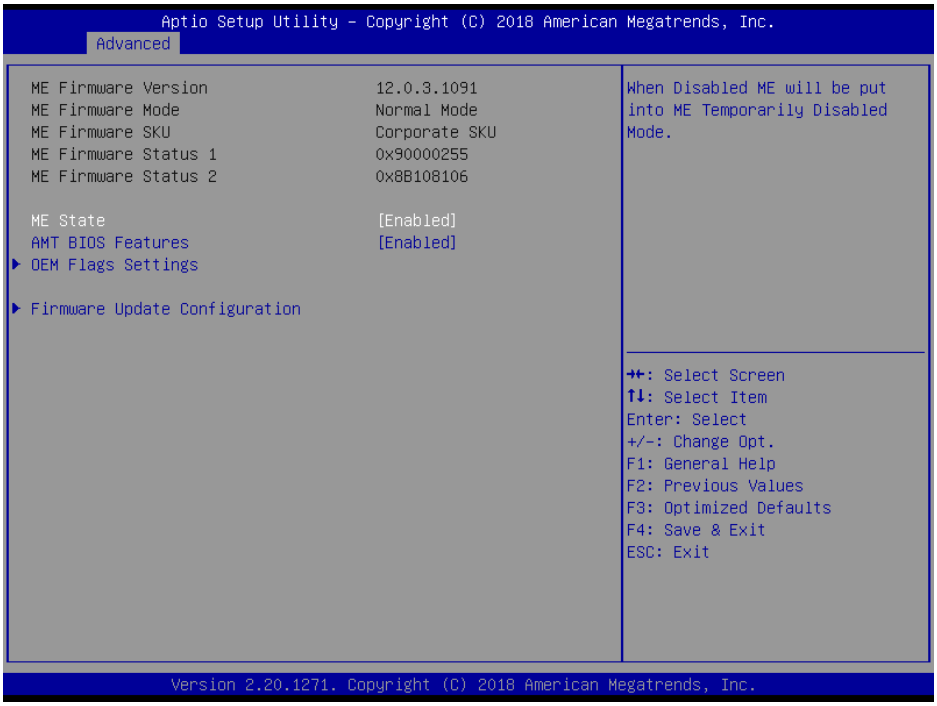
3.6.2.1.1 CPU – Power Management Control



Item	Option	Description
Intel® SpeedStep™	Enabled**[Default]**, Disabled	Allows more than two frequency ranges to be supported.
Turbo Mode	Enabled**[Default]**, Disabled	Enable/Disable processor Turbo Mode (requires Intel Speed Step or Intel Speed Shift to be available and enabled).
C States	Enabled**[Default]**, Disabled	Enable/Disable CPU Power Management. Allows CPU to go to C states when it's not 100% utilized.
Enhanced C-states	Enabled**[Default]**, Disabled	Enable/Disable C1E. When enabled, CPU will switch to minimum speed when all cores enter C-State.
C-State Auto Demotion	Disabled, C1 C3 C1 and C3**[Default]**	Configure C-State Auto Demotion.
C-State Un-demotion	Disabled, C1 C3 C1 and C3**[Default]**	Configure C-State Un-demotion.
Package C-State Demotion	Enabled Disabled**[Default]**,	Package C-State Demotion.
Package C-State Un-demotion	Enabled Disabled**[Default]**,	Package C-State Un-demotion.
Package C State Limit	C0/C1 C2 C3 C6 C7 C7S	Maximum Package C State Limit Setting. CPU Default: Leaves to Factory default value. Auto: Initializes to deepest available Package C State Limit.

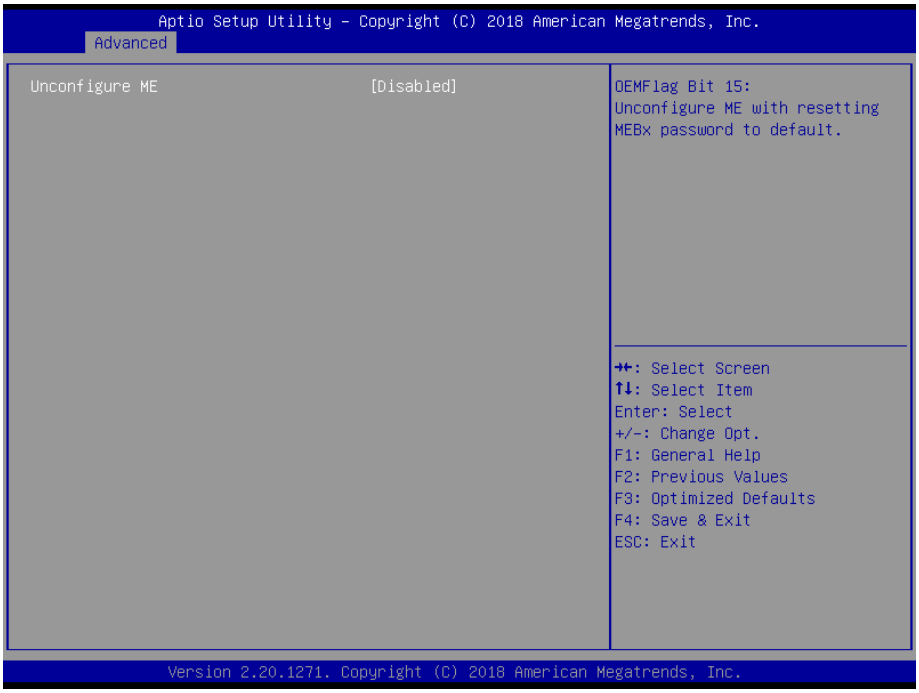
	C8 C9 C10 CPU Default Auto**[Default]**	

3.6.2.2 PCH-FW Configuration



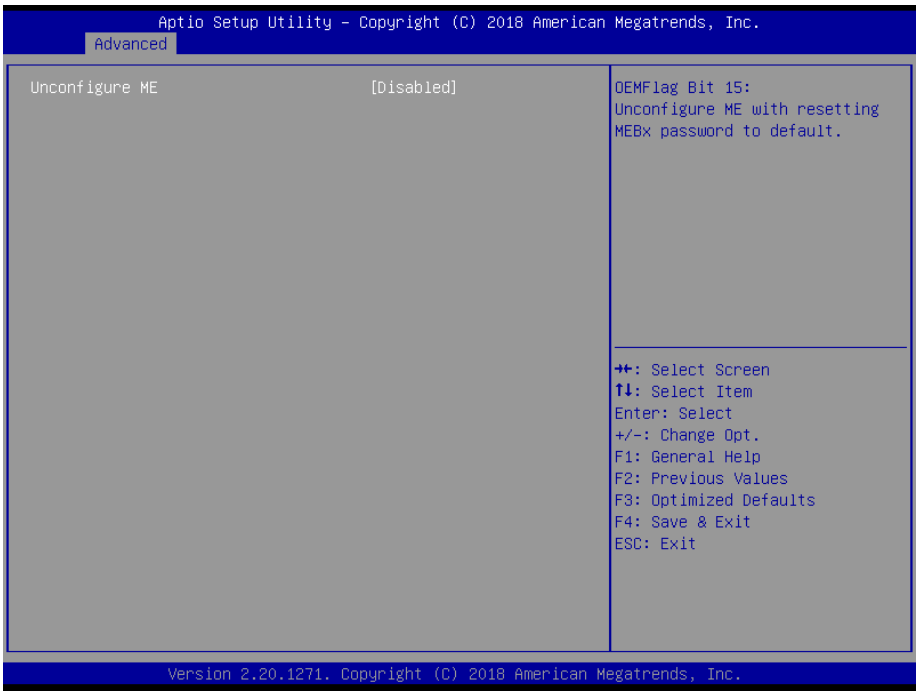
Item	Options	Description
ME State	Disabled, Enabled**[Default]**	When Disabled ME will be put into ME Temporarily Disabled Mode.
AMT BIOS Features	Disabled, Enabled**[Default]**	When disable AMT BIOS Features are no longer supported and user is no longer able to access MEBx Setup. Note: This option does not disable Manageability Features in FW.

3.6.2.2.1 OEM Flags Settings



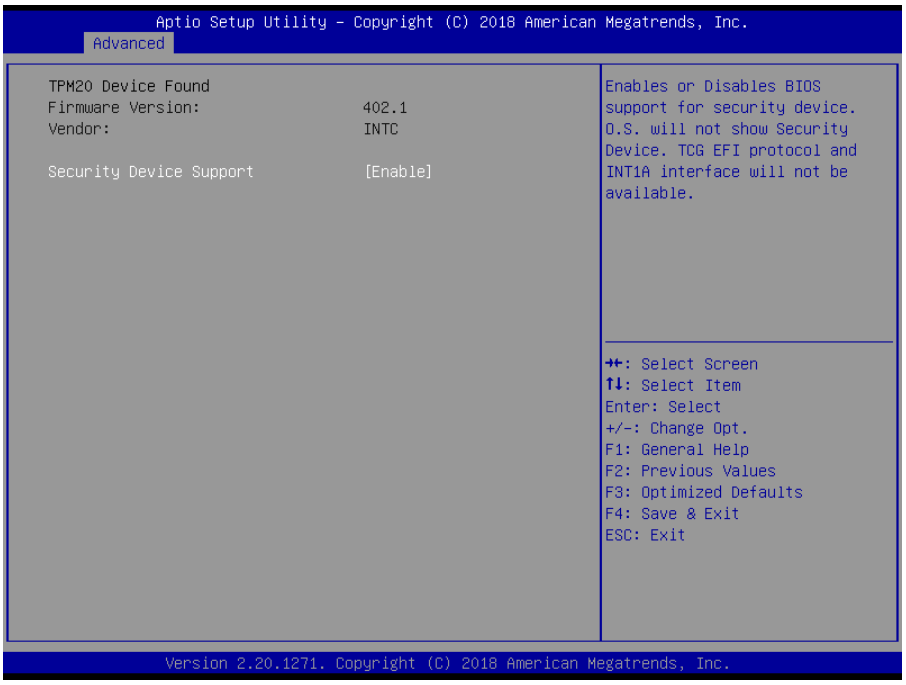
Item	Option	Description
Unconfigure ME	Disabled**[Default]**, Enabled	OEMFlag Bit 15: Unconfigure ME with resetting MEBx password to default.

3.6.2.2.2 Firmware Update Configuration



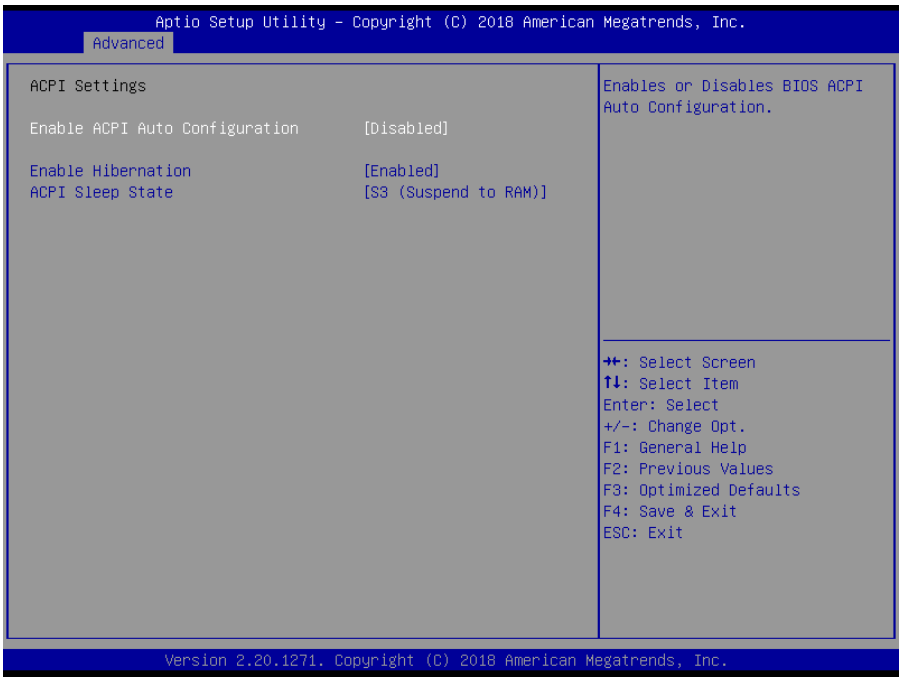
Item	Option	Description
Unconfigure ME	Disabled**[Default]**, Enabled	OEMFlag Bit 15: Unconfigure ME with resetting MEBx password to default.

3.6.2.3 Trusted Computing



Item	Options	Description
Security Device Support	Disable, Enable**[Default]**	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.

3.6.2.4 APCI Settings



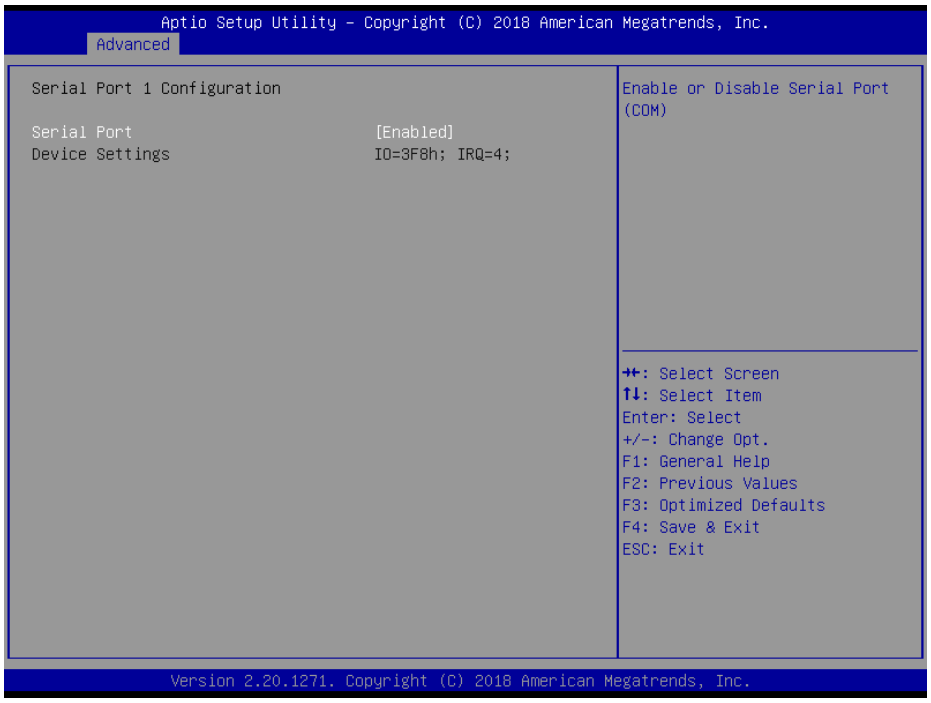
Item	Options	Description
Enable ACPI Auto Configuration	Disabled**[Default]**, Enabled	Enables or Disables BIOS ACPI Auto Configuration.
Enable Hibernation	Disabled Enabled**[Default]**,	Enables or Disables System ability to Hibernate (OS/S4 Sleep State). This option may not be effective with some OS.
ACPI Sleep State	Suspend Disabled, S3 (Suspend to RAM)**[Default]**	Select the highest ACPI sleep state the system will enter when the SUSPEND button is pressed.

3.6.2.5 IT8528 Super IO Configuration

You can use this item to set up or change the IT8528 Super IO configuration for serial ports. Please refer to 3.6.2.5.1~ 3.6.2.5.2 for more information.

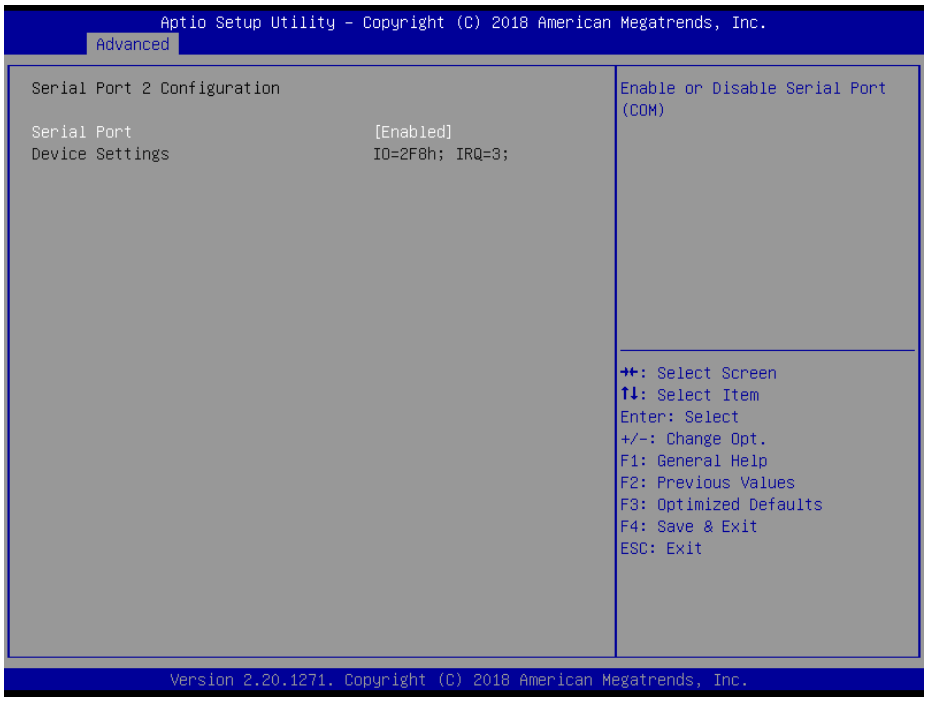
Item	Description
Serial Port 1 Configuration	Set Parameters of Serial Port 1 (COMA).
Serial Port 2 Configuration	Set Parameters of Serial Port 2 (COMB).

3.6.2.5.1 Serial Port 1 Configuration



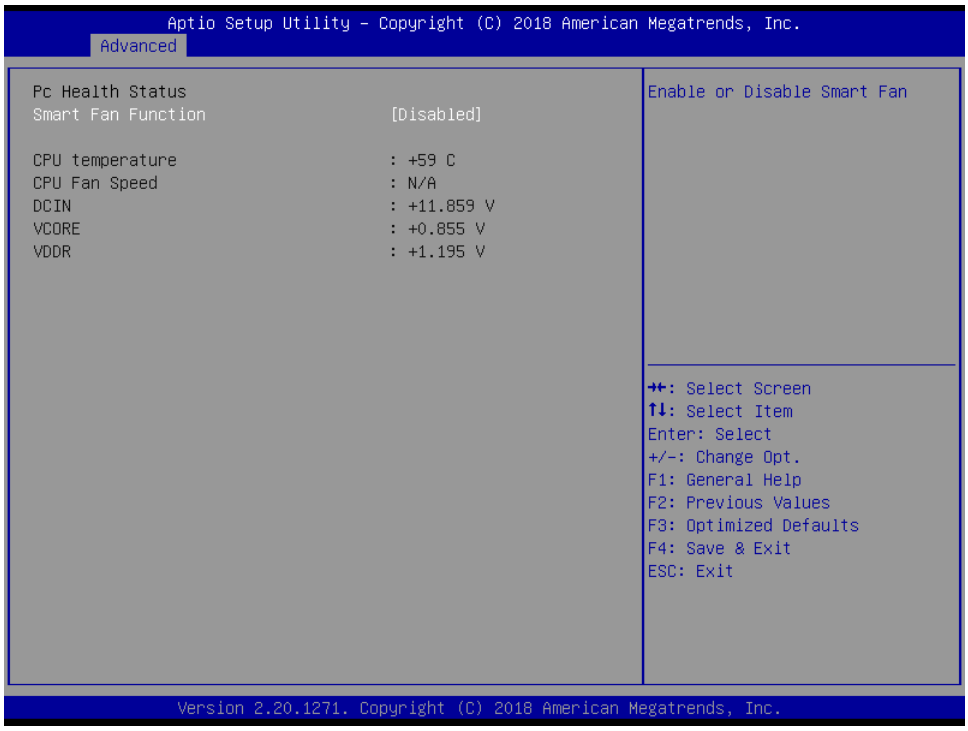
Item	Option	Description
Serial Port	Enabled**[Default]**, Disabled	Enable or Disable Serial Port (COM).

3.6.2.5.2 Serial Port 2 Configuration



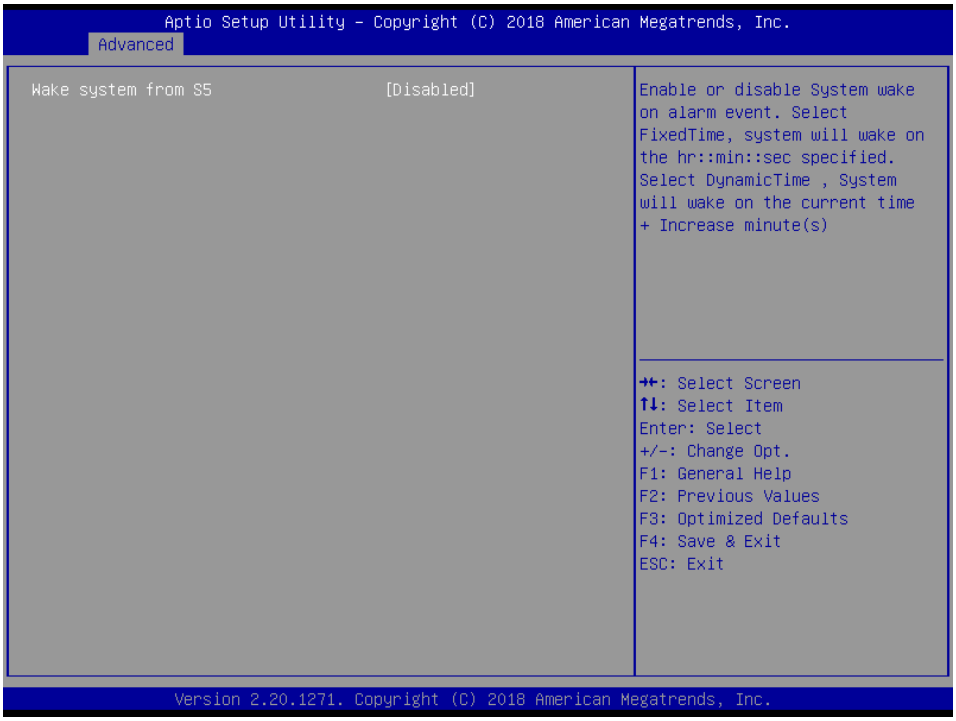
Item	Option	Description
Serial Port	Enabled**[Default]**, Disabled	Enable or Disable Serial Port (COM).

3.6.2.6 EC 8528 HW Monitor



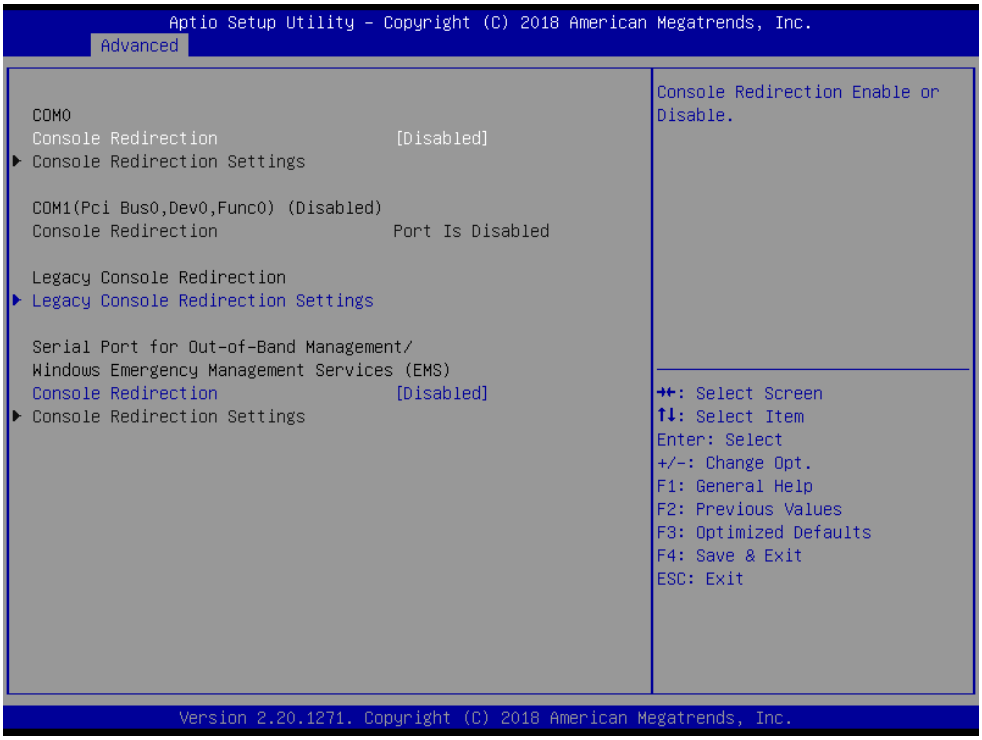
Item	Options	Description
Smart Fan Function	Enabled, Disabled**[Default]**	Enables or Disables Smart Fan.

3.6.2.7 S5 RTC Wake Settings



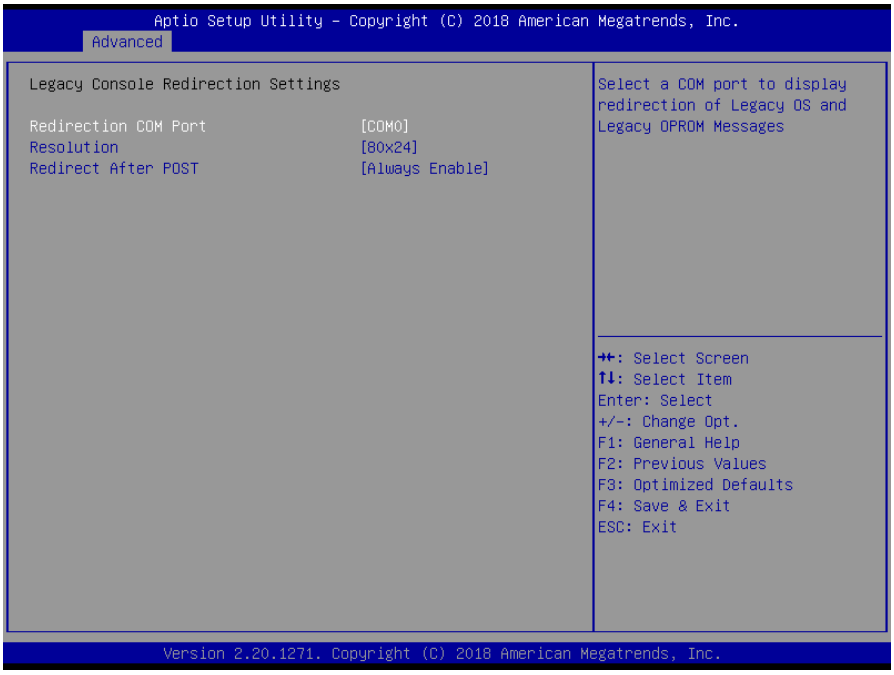
Item	Options	Description
Wake system from S5	Disabled**[Default]**, Fixed Time Dynamic Time	Enable or disable System wake on alarm event. Select Fixed Time, system will wake on the hr::min::sec specified. Select Dynamic Time, System will wake on the current time + Increase minute(s).

3.6.2.8 Serial Port Console Redirection



Item	Options	Description
Console Redirection	Disabled**[Default]**, Enabled	Console Redirection Enable or Disable.

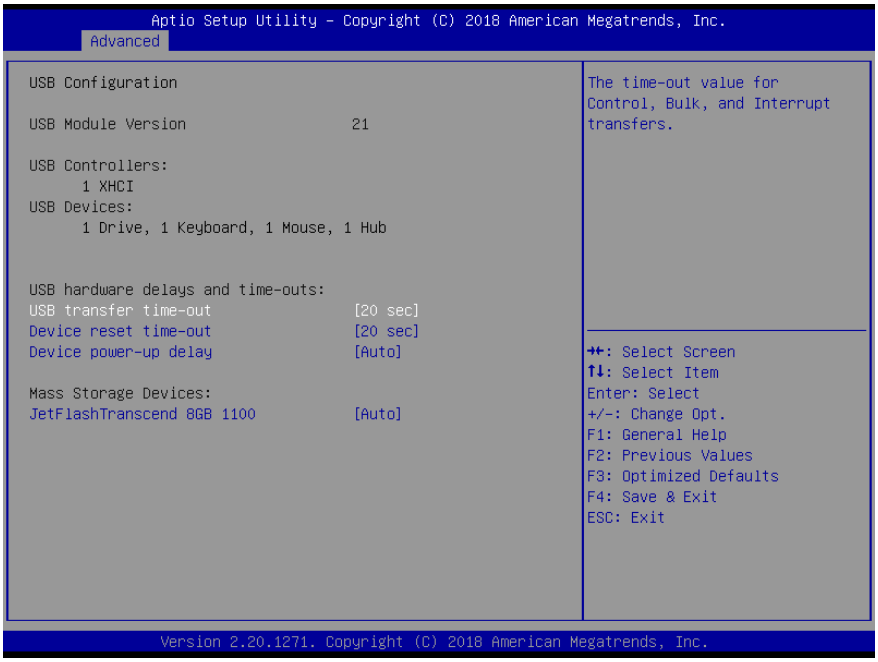
3.6.2.8.1 Legacy Console Redirection Settings



Item	Option	Description
Redirection COM Port	COM0**[Default]**	Select a COM port to display redirection of Legacy OS and Legacy OPROM Messages.
Resolution	80x24**[Default]** 80x25	On Legacy OS, the Number of Rows and Columns supported redirection.
Redirect After POST	Always Enable**[Default]** BootLoader	When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS. Default setting for this option is set to Always Enable.

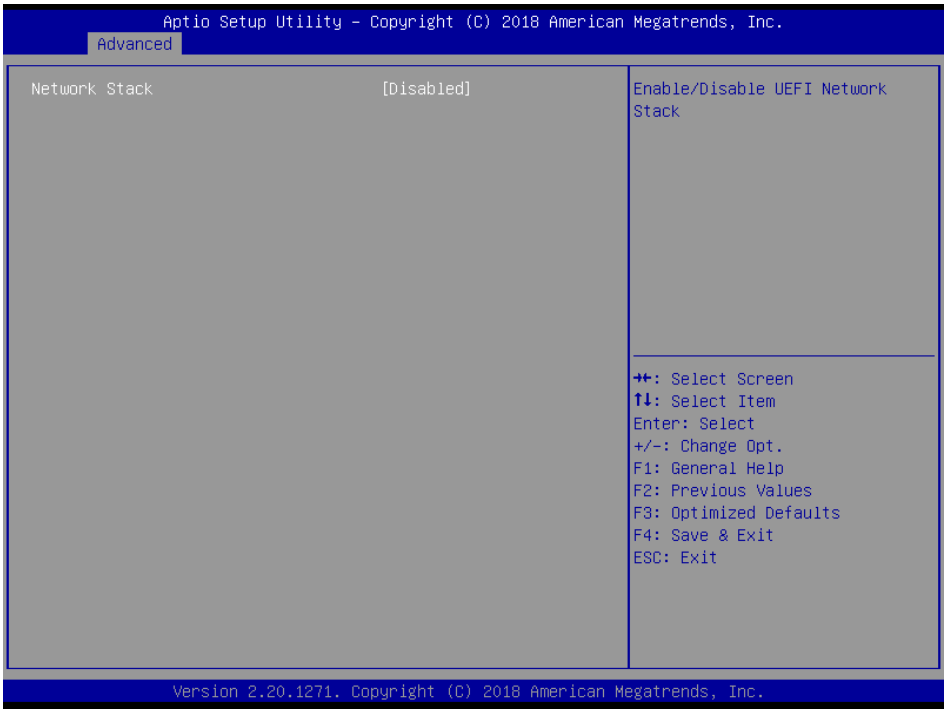
3.6.2.9 USB Configuration

The USB Configuration menu helps read USB information and configures USB settings.



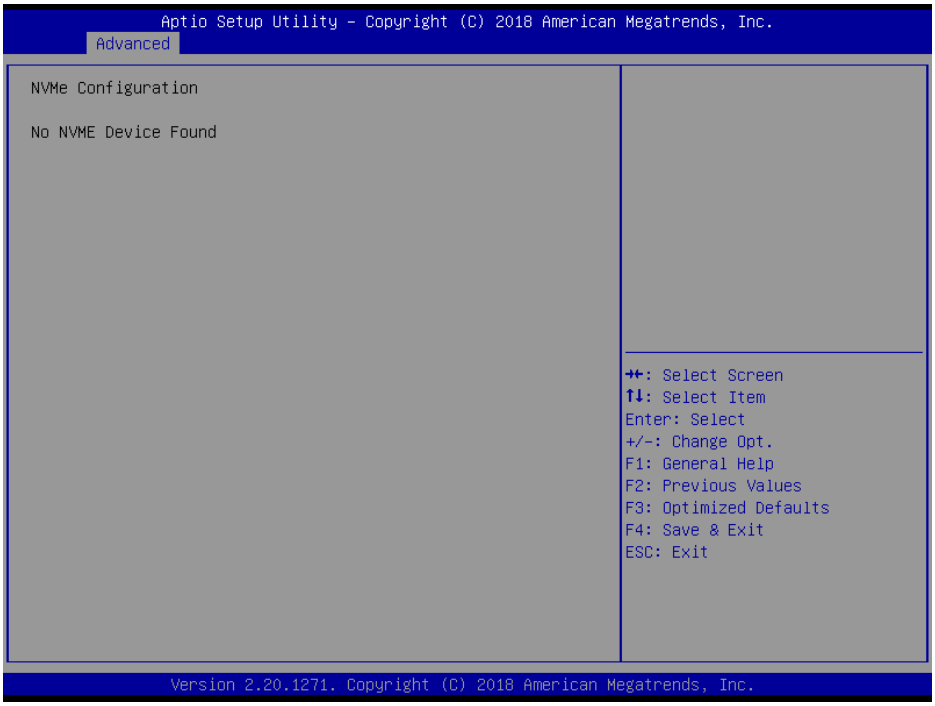
Item	Options	Description
USB transfer time-out	1 sec 5 sec 10 sec 20 sec**[Default]**	The time-out value for Control, Bulk, and Interrupt transfers.
Device reset time-out	10 sec 20 sec**[Default]** 30 sec 40 sec	USB mass storage device Start Unit command time-out.
Device power-up delay	Auto**[Default]** Manual	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 100ms, for a Hub port the delay is taken form Hub descriptor.
Mass Storage Devices	Auto**[Default]** Floppy Forced FDD Hard Disk CD-ROM	Mass storage device emulation type. 'AUTO' enumerates devices according to their media format. Optical drives are emulated as 'CDROM', drives with no media will be emulated according to a drive type.

3.6.2.10 Network Stack Configuration

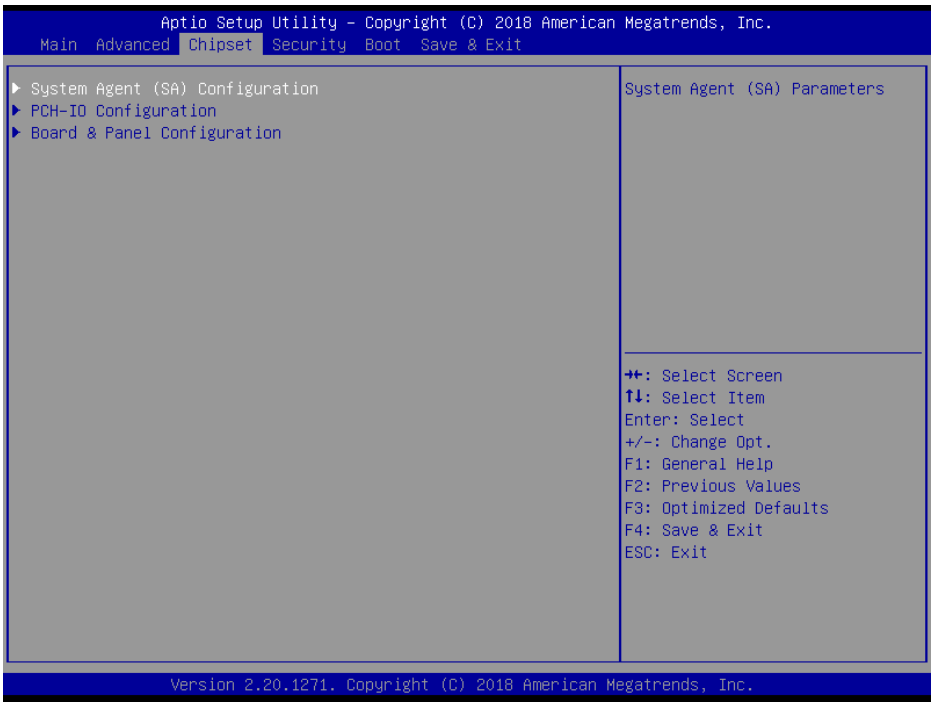


Item	Options	Description
Network Stack	Enabled Disabled**[Default]**	Enable/Disable UEFI Network Stack.

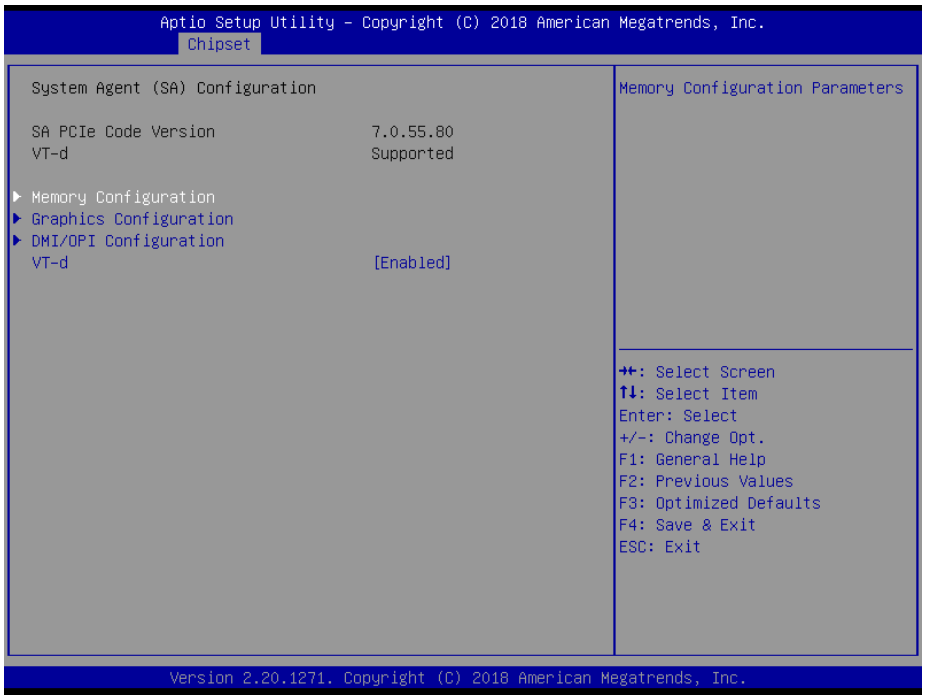
3.6.2.11 NVMe Configuration



3.6.3 Chipset

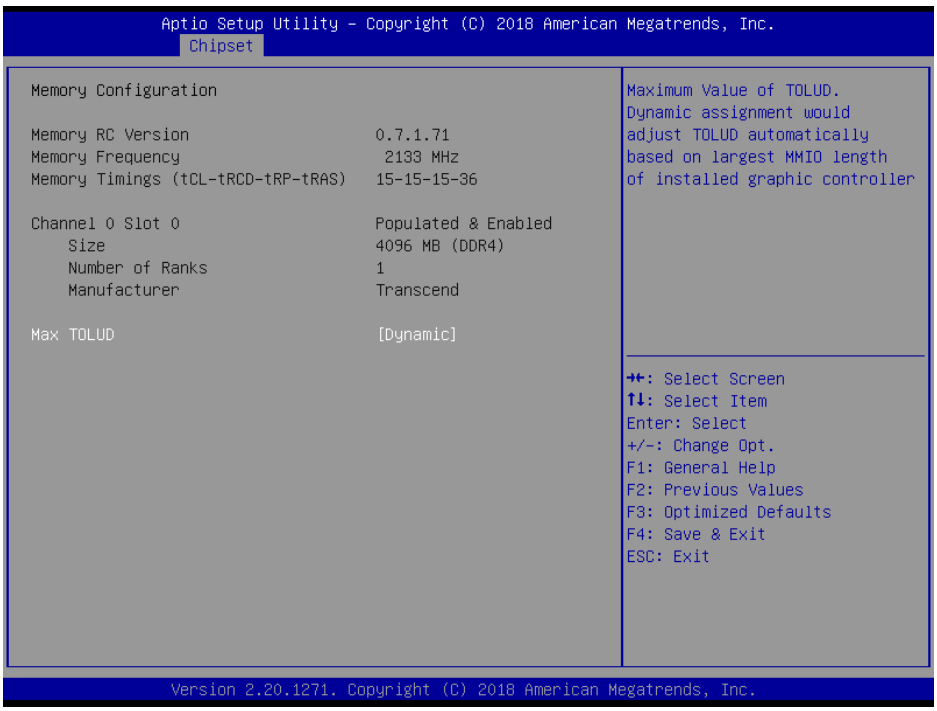


3.6.3.1 System Agent (SA) Configuration



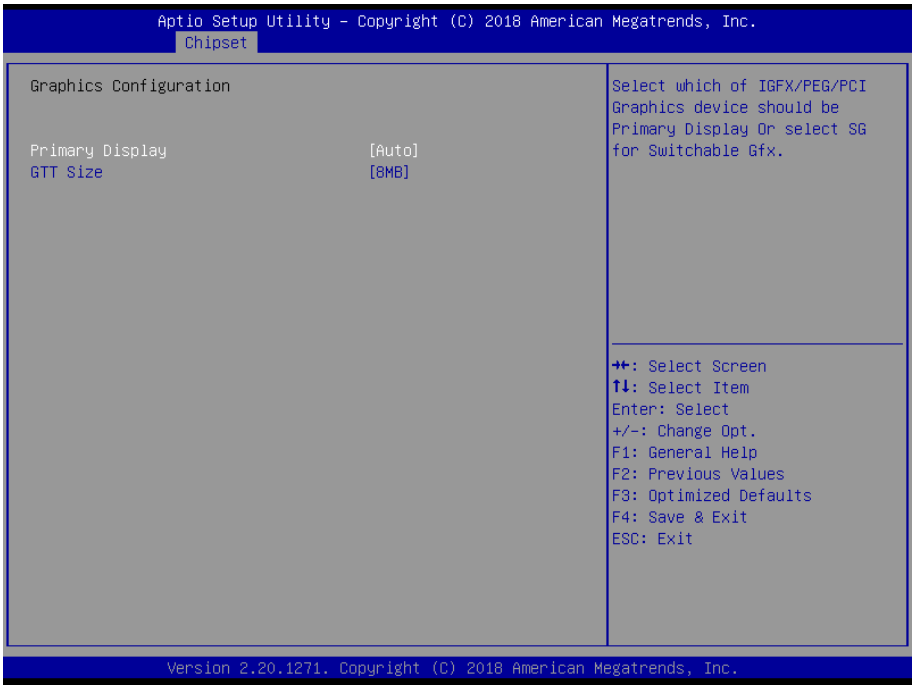
Item	Option	Description
VT-d	Enabled**[Default]** Disabled	VT-d capability.

3.6.3.1.1 Memory Configuration



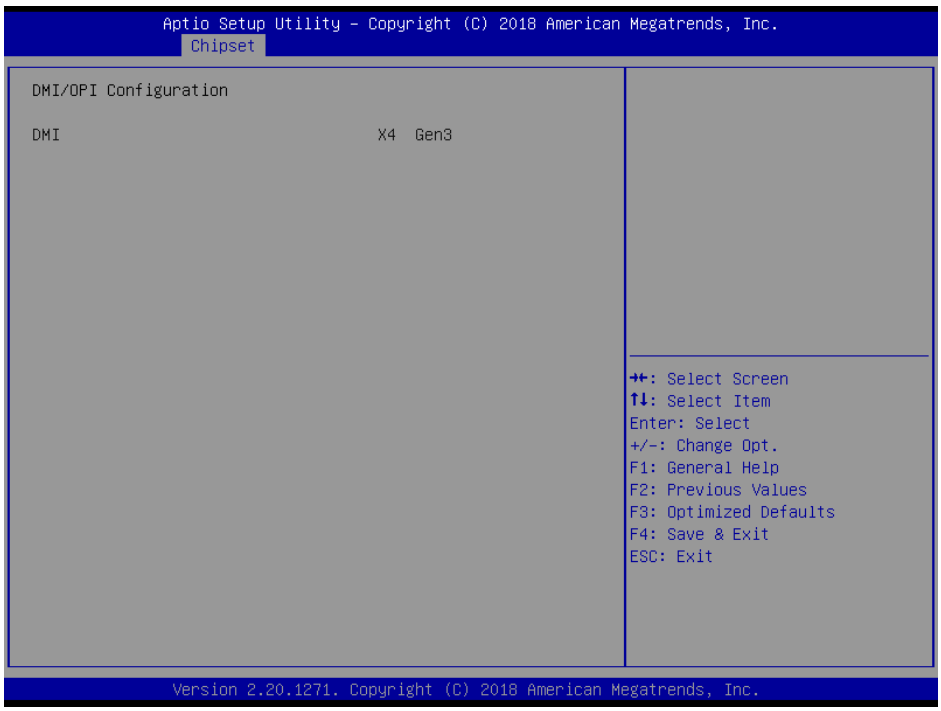
Item	Option	Description
Max TOLUD	Dynamic**[Default]** 1 GB 1.25 GB 1.5 GB 1.75 GB 2 GB 2.25 GB 2.5 GB 2.75 GB 3 GB	Maximum Value of TOLUD. Dynamic assignment would adjust TOLUD automatically based on largest MMIO length of installed graphic controller.

3.6.3.1.2 Graphics Configuration

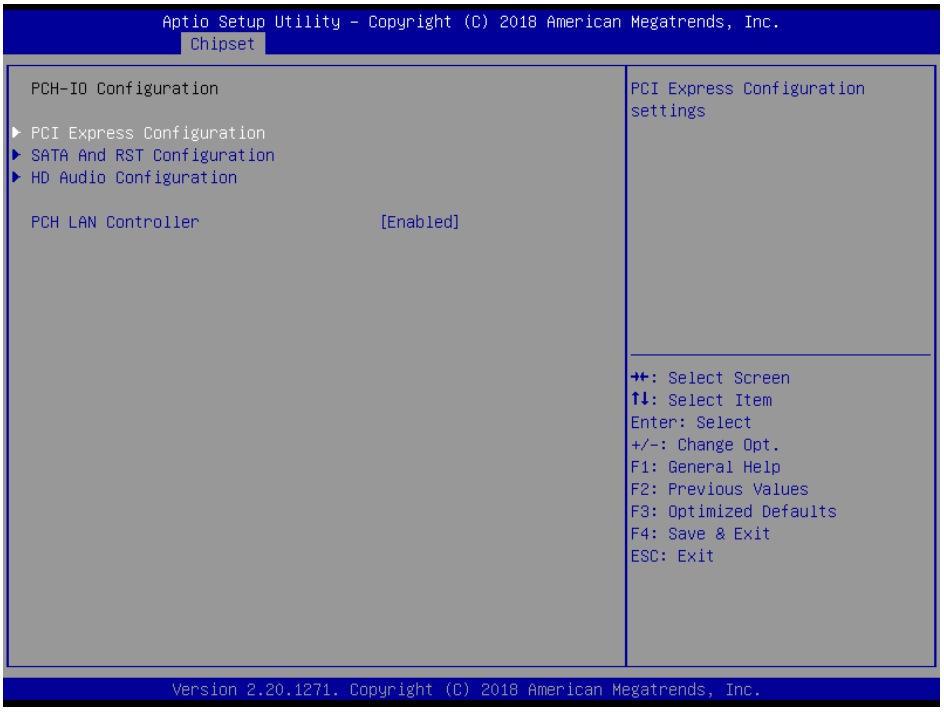


Item	Option	Description
Primary Display	Auto**[Default]** IGFX	Select which of IGFX/PEG/PCI Graphics device should be Primary Display Or select SG for Switchable Gfx.
GTT Size	2MB 4MB 8MB**[Default]**	Select the GTT Size.

3.6.3.1.3 DMI/OPI Configuration



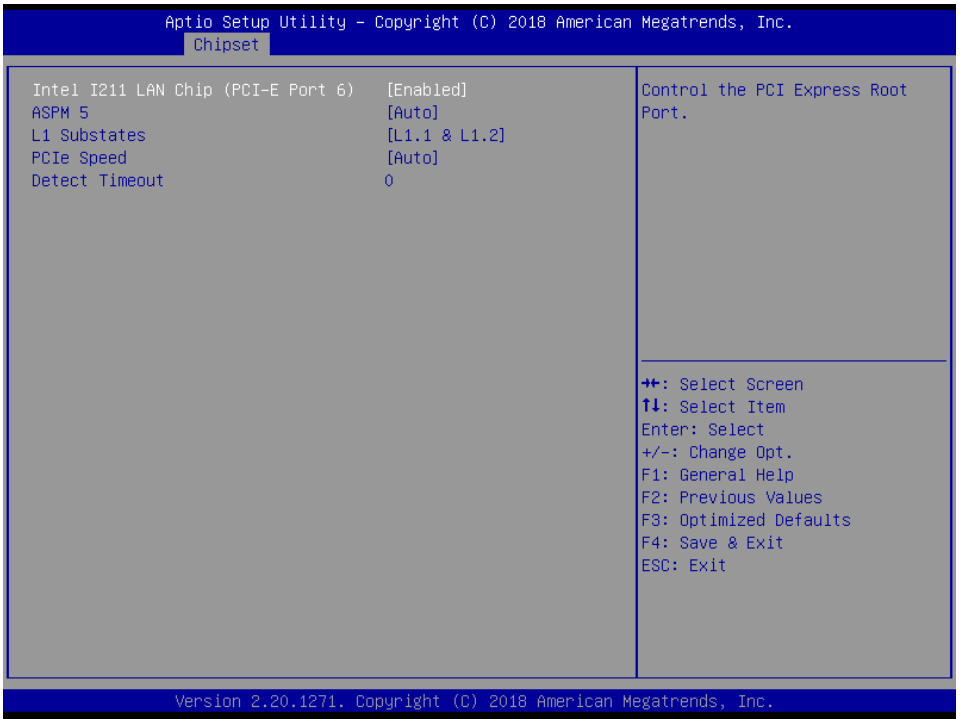
3.6.3.2 PCH-IO Configuration



Item	Option	Description
PCH LAN Controller	Disabled Enabled**[Default]**	Enable/Disable onboard NIC.

3.6.3.2.1 PCI Express Configuration

3.6.3.2.1.1 Intel I211 LAN Chip (PCI-E Port 6)



Item	Option	Description
Intel I211 LAN Chip (PCI-E Port 6)	Enabled**[Default]**, Disabled	Control the PCI Express Root Port.
ASPM 5	Disabled, L0s	Set the ASPM Level: Force L0s – Force all links to L0s State AUTO – BIOS auto

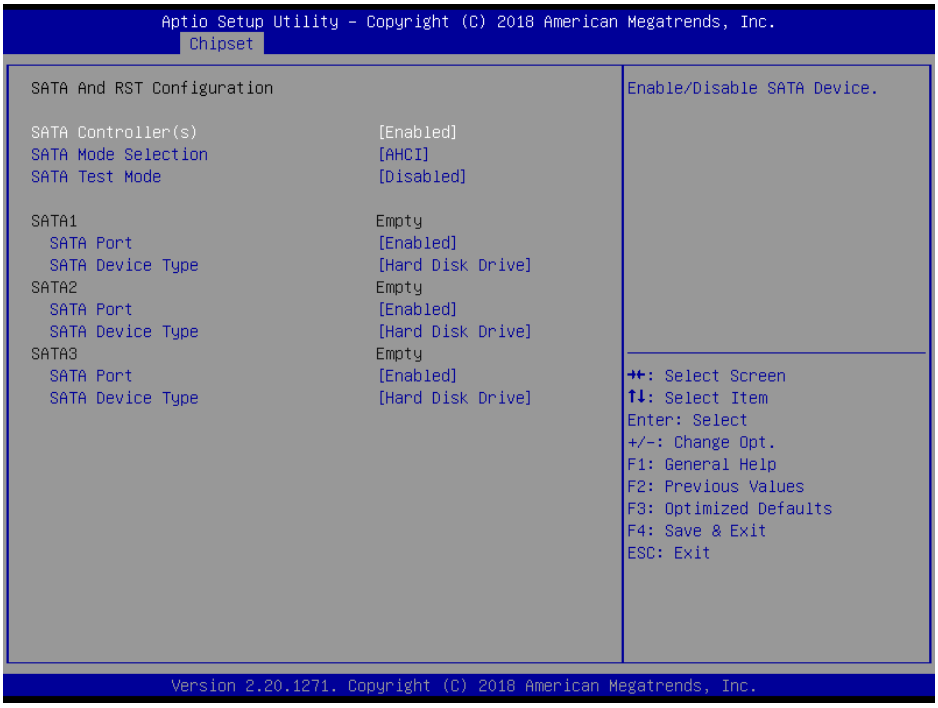
	L1 L0sL1 Auto**[Default]**	configure DISABLE – Disables ASPM.
L1 Substates	Disabled, L1.1 L1.1 & L1.2**[Default]**	PCI Express L1 Substates settings.
PCIe Speed	Auto**[Default]** Gen1 Gen2 Gen3	Configure PCIe Speed.
Detect Timeout	0	The number of milliseconds reference code will wait for link to exit Detect state for enabled ports before assuming there is no device and potentially disabling the port.

3.6.3.2.1.2 mPCIe/mSATA Slot (PEI-E Port 15)

Item	Option	Description
mPCIe/mSATA Slot (PEI-E Port 15)	Enabled**[Default]**, Disabled	Control the PCI Express Root Port.
ASPM 14	Disabled, L0s L1 L0sL1 Auto**[Default]**	Set the ASPM Level: Force L0s – Force all links to L0s State AUTO – BIOS auto configure DISABLE – Disables ASPM.
L1 Substates	Disabled, L1.1 L1.1 & L1.2**[Default]**	PCI Express L1 Substates settings.
PCIe Speed	Auto**[Default]** Gen1 Gen2	Configure PCIe Speed.

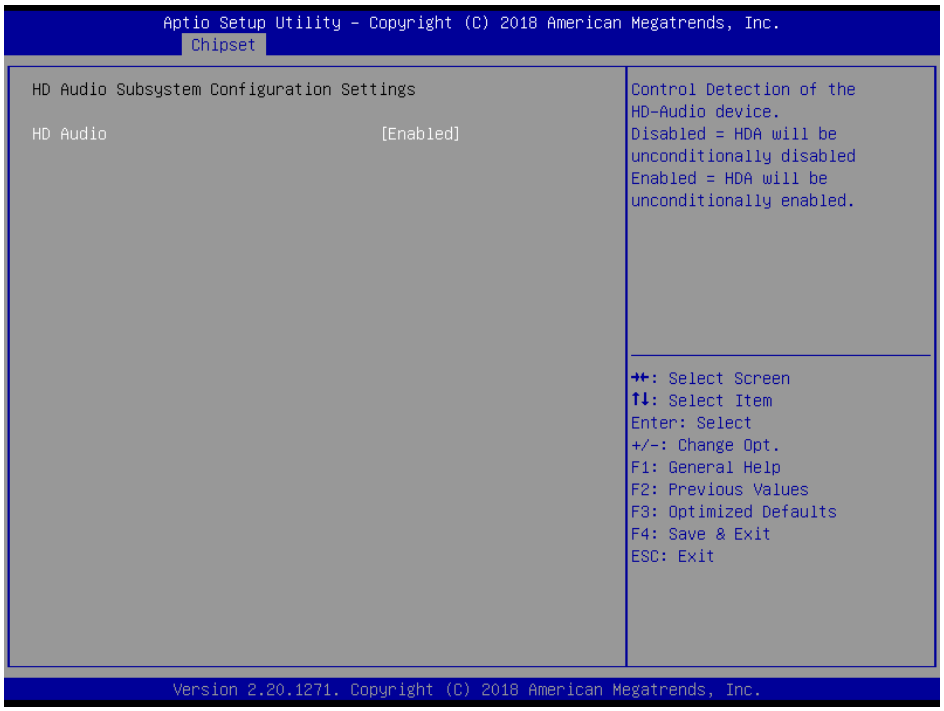
	Gen3	
Detect Timeout	0	The number of milliseconds reference code will wait for link to exit Detect state for enabled ports before assuming there is no device and potentially disabling the port.

3.6.3.2.2 SATA And RST Configuration



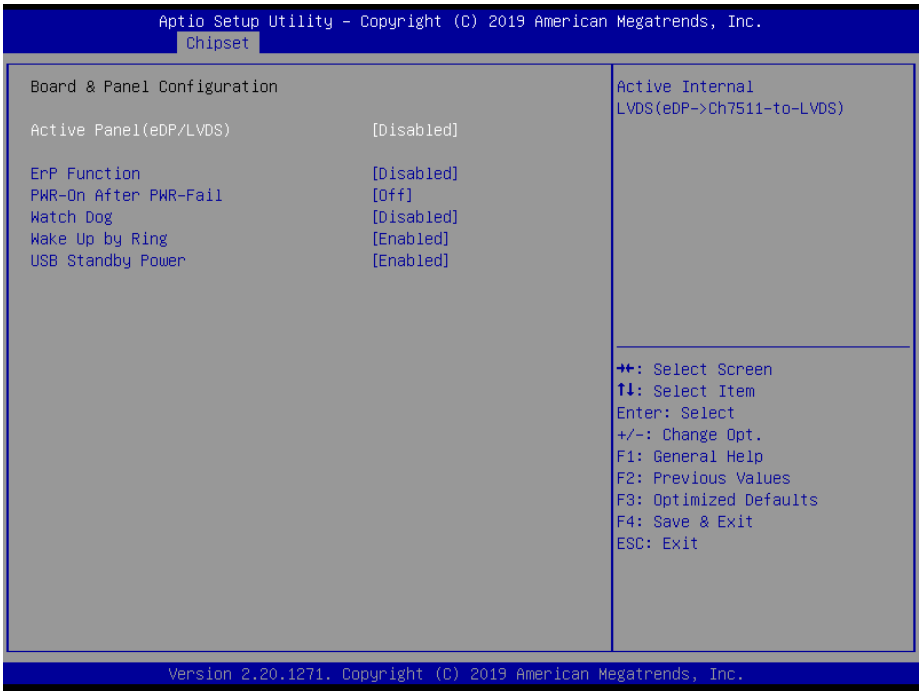
Item	Options	Description
SATA Controller(s)	Enabled**[Default]** Disabled,	Enable/Disable SATA Device.
SATA Mode Selection	AHCI**[Default]**, RAID	Determines how SATA controller(s) operate.
SATA Test Mode	Enabled Disabled**[Default]**	The Mode Enable/Disable (Loop Back).
SATA Port	Enabled**[Default]** Disabled	Enable or Disable SATA Port.
SATA Device Type	Hard Disk Drive**[Default]** Solid State Drive	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.

3.6.3.2.3 HD Audio Configuration



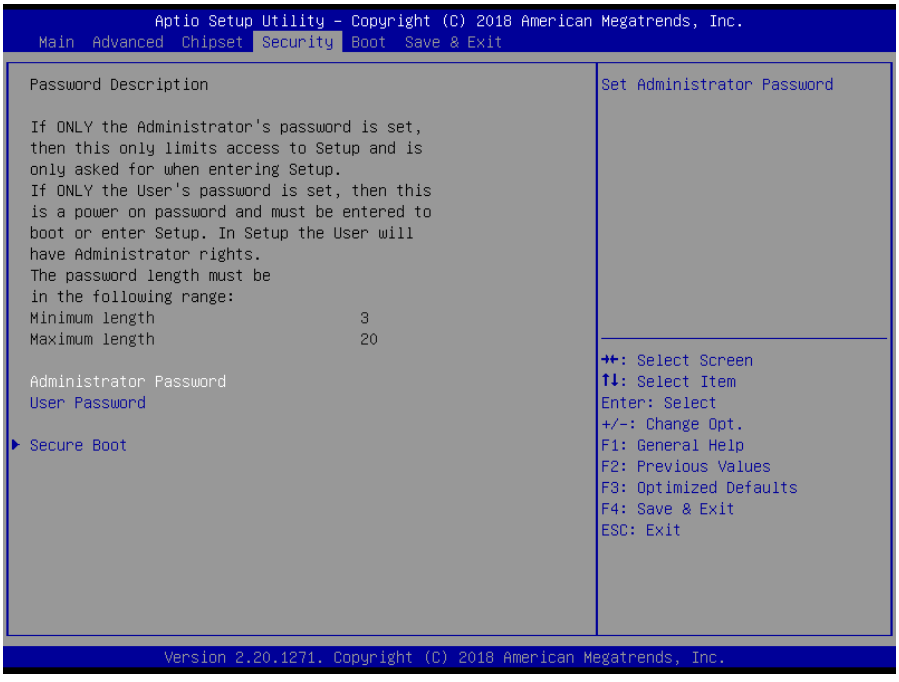
Item	Option	Description
HD Audio	Disabled Enabled**[Default]**	Control Detection of the HD-Audio device. Disable = HDA will be unconditionally disabled Enabled = HDA will be unconditionally enabled

3.6.3.3 Board & Panel Configuration



Item	Option	Description
Active Panel (eDP/LVDS)	Disabled**[Default]** Enabled	Active Internal LVDS(eDP->Cg7511-to-LVDS).
ErP Function	Disabled**[Default]** Enabled	ErP Function (Deep S5).
PWR-On After PWR-Fail	Off**[Default]** On Last state	AC loss resume.
Watch Dog	Disabled**[Default]** 30 sec 40 sec 50 sec 1 min 2 min 10 min 30 min	Select WatchDog.
Wake Up by Ring	Disabled Enabled**[Default]**	Wake Up by Ring from S3/S4/S5.
USB Standby Power	Disabled Enabled**[Default]**	Enable/Disabled USB Standby Power during S3/S4/S5.

3.6.4 Security



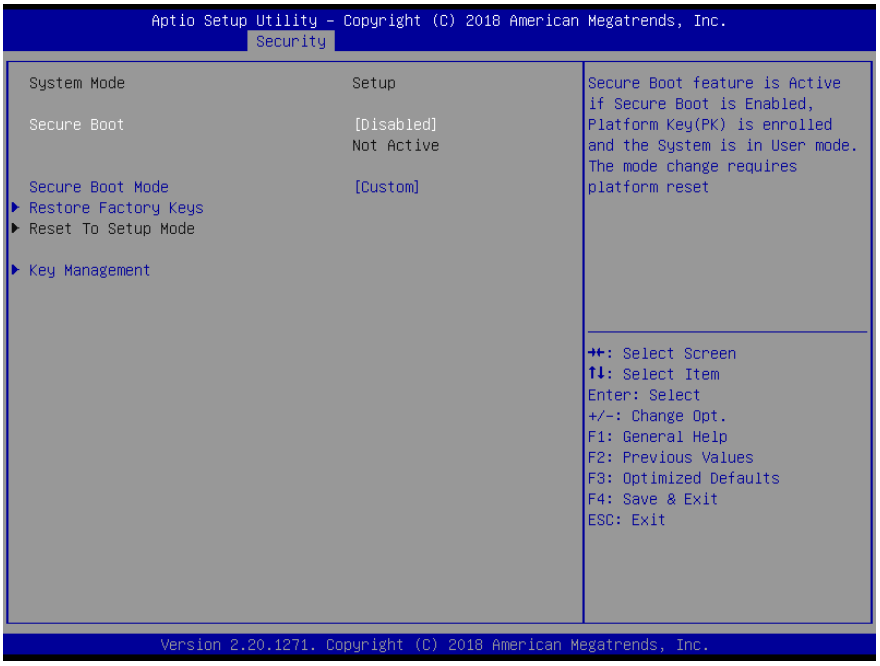
- **Administrator Password**

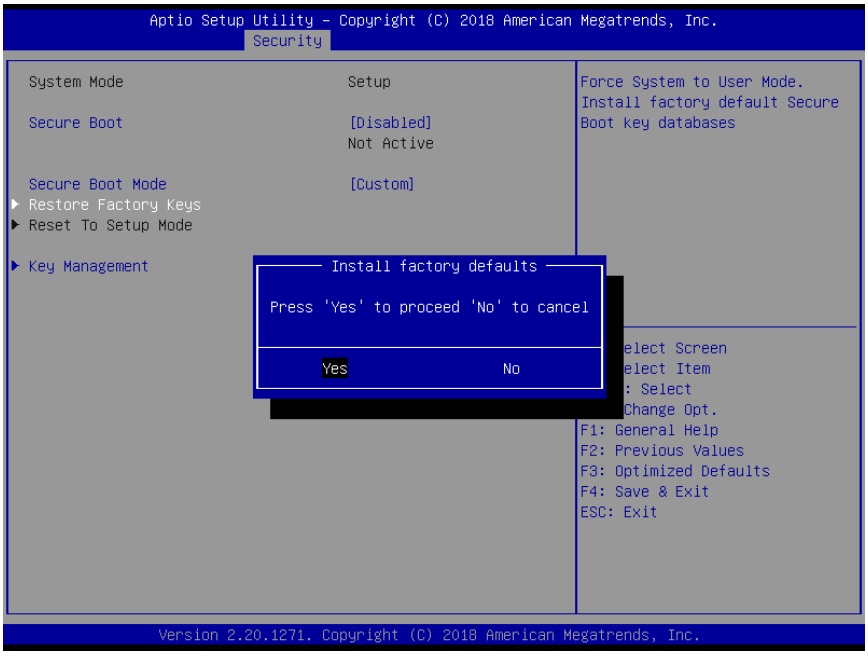
Set setup Administrator Password

- **User Password**

Set User Password

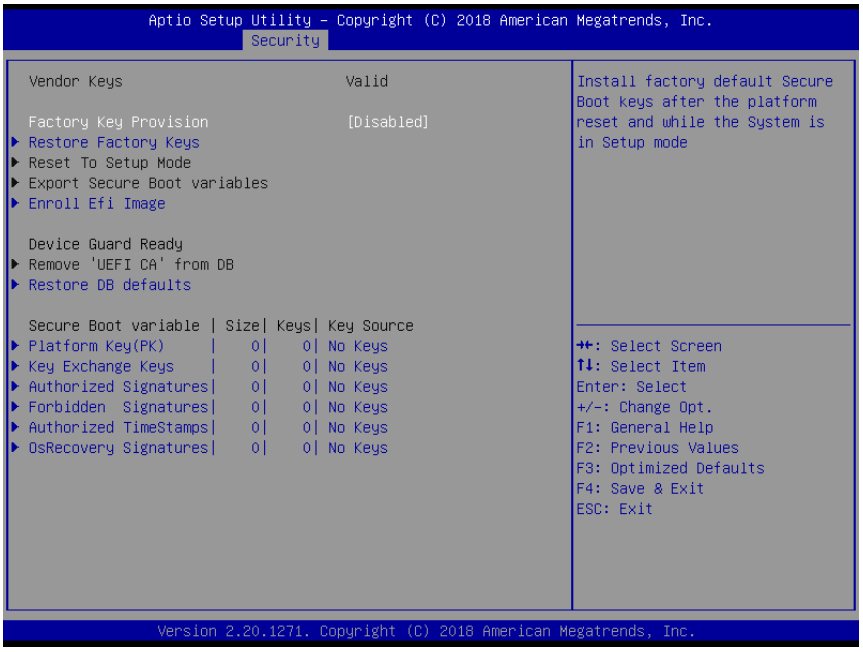
3.6.4.1 Secure Boot

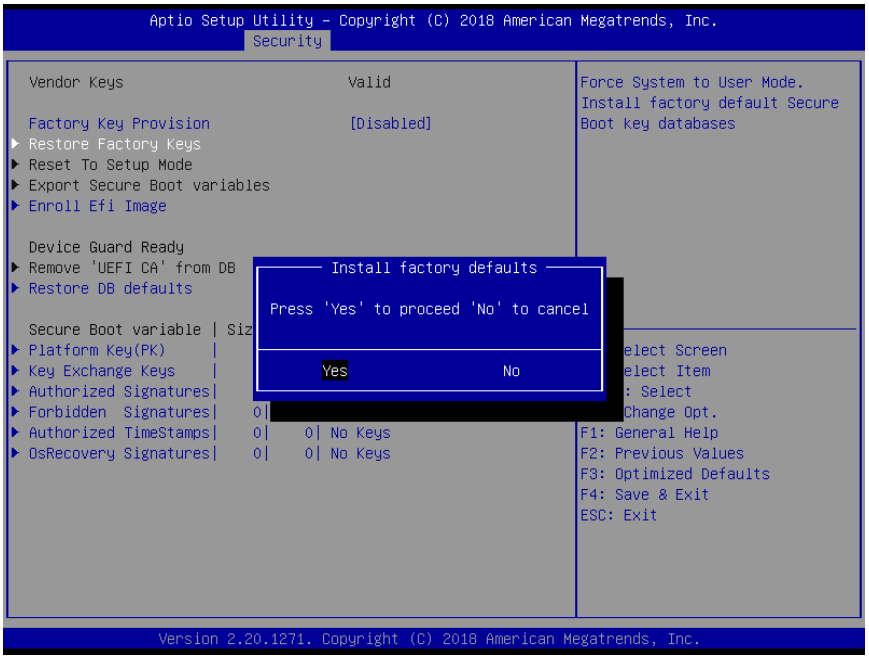


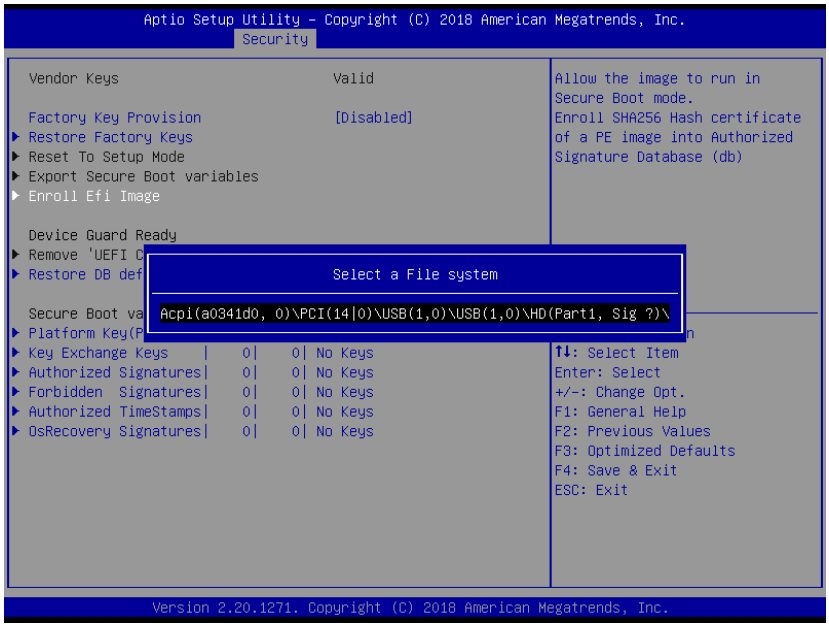


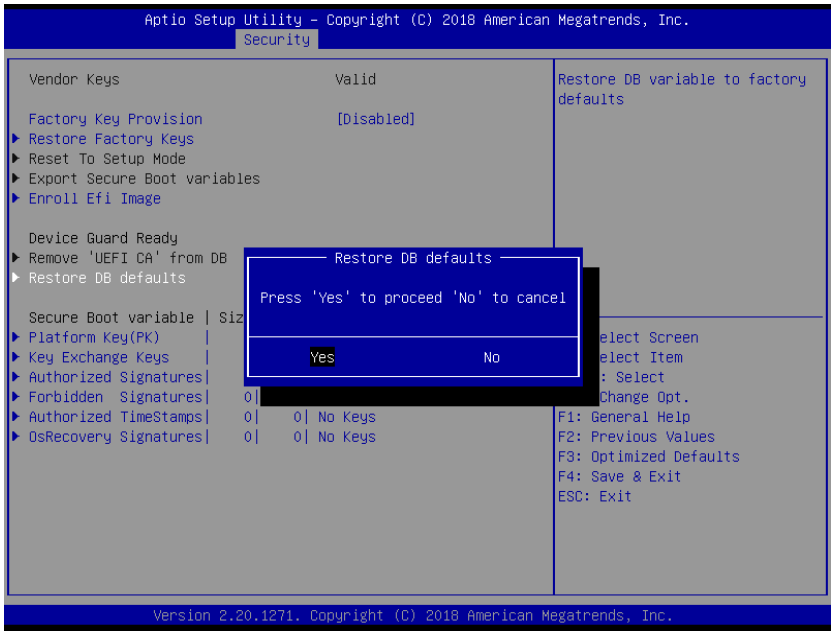
Item	Option	Description
Secure Boot	Disabled**[Default]** Enabled	Secure Boot feature is Active if Secure Boot is Enabled, Platform Key(PK) is enrolled and the System is in User mode. The mode chagne requires platform reset.
Secure Boot Mode	Standard Custom**[Default]**	Secure Boot mode selector: Standard/Custom. In Custom mode Secure Boot Variables can be configured without authentication.

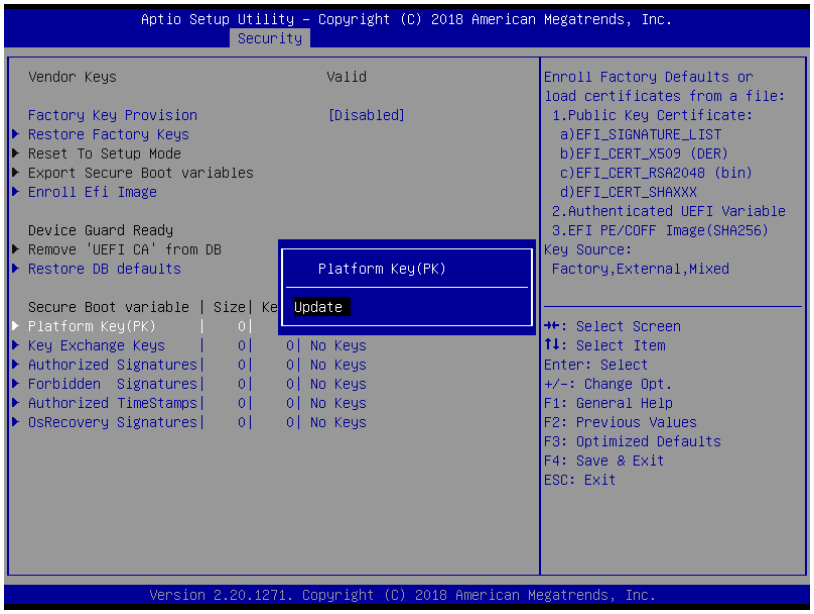
3.6.4.1.1 Key Management

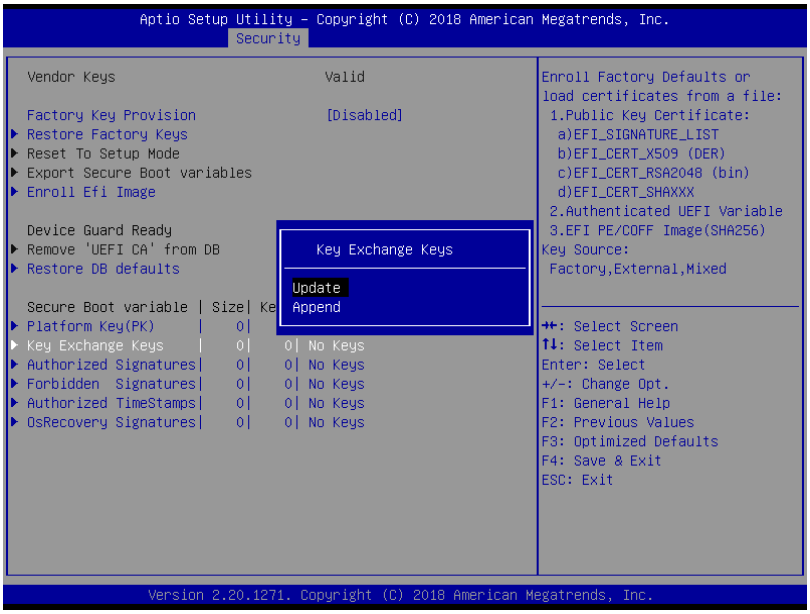


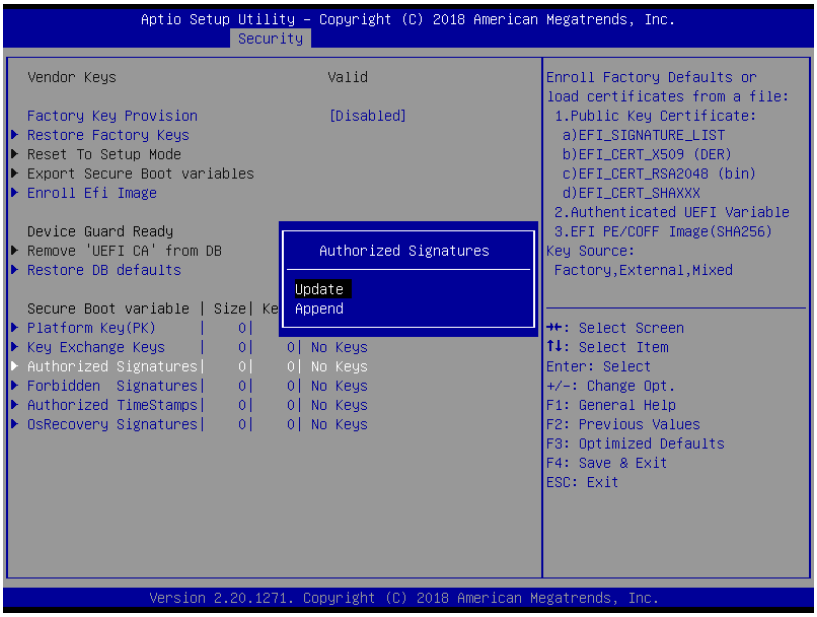


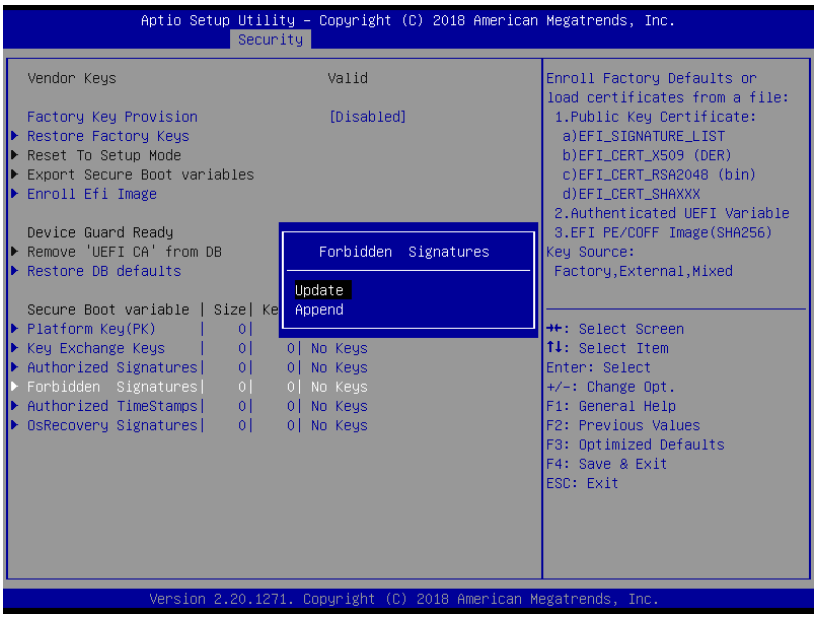

Aptio Setup Utility – Copyright (C) 2018 American Megatrends, Inc.
Security
Vendor Keys
Valid
Factory Key Provision
[Disabled]
Restore Factory Keys
Reset To Setup Mode
Export Secure Boot variables
Enroll Efi Image
Device Guard Ready
Remove 'UEFI C
Restore DB def
Secure Boot va
Platform Key(P
Key Exchange Keys | 0| 0| No Keys
Authorized Signatures| 0| 0| No Keys
Forbidden Signatures| 0| 0| No Keys
Authorized TimeStamps| 0| 0| No Keys
OsRecovery Signatures| 0| 0| No Keys
Select a File system
Acpi(a0341d0, 0)\PCI(14|0)\USB(1,0)\USB(1,0)\HD(Part1, Sig ?)\
Allow the image to run in Secure Boot mode.
Enroll SHA256 Hash certificate of a PE image into Authorized Signature Database (db)
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.20.1271. Copyright (C) 2018 American Megatrends, Inc.

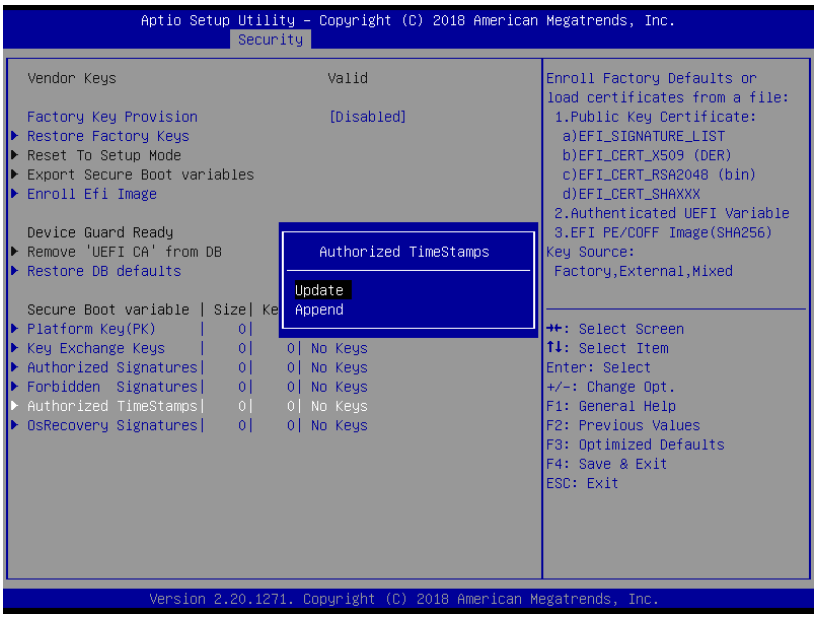

Aptio Setup Utility – Copyright (C) 2018 American Megatrends, Inc.
Security
Vendor Keys
Valid
Factory Key Provision
[Disabled]
Restore Factory Keys
Reset To Setup Mode
Export Secure Boot variables
Enroll Efi Image
Device Guard Ready
Remove 'UEFI CA' from DB
Restore DB defaults
Secure Boot variable | Siz
Platform Key(PK)
Key Exchange Keys
Authorized Signatures|
Forbidden Signatures| 0|
Authorized TimeStamps| 0| 0| No Keys
OsRecovery Signatures| 0| 0| No Keys
Restore DB defaults
Press 'Yes' to proceed 'No' to cancel
Yes
No
Restore DB variable to factory defaults
elect Screen
elect Item
: Select
Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.20.1271. Copyright (C) 2018 American Megatrends, Inc.

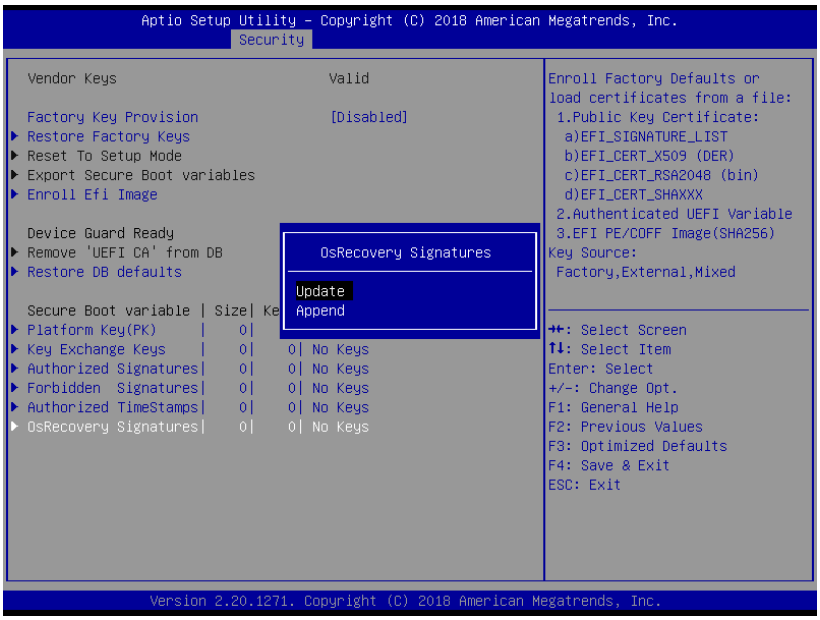

Aptio Setup Utility – Copyright (C) 2018 American Megatrends, Inc.
Security
Vendor Keys
Valid
Factory Key Provision
[Disabled]
Restore Factory Keys
Reset To Setup Mode
Export Secure Boot variables
Enroll Efi Image
Device Guard Ready
Remove 'UEFI CA' from DB
Restore DB defaults
Secure Boot variable | Size| Ke
Platform Key(PK) | 0|
Key Exchange Keys | 0| 0| No Keys
Authorized Signatures| 0| 0| No Keys
Forbidden Signatures| 0| 0| No Keys
Authorized TimeStamps| 0| 0| No Keys
OsRecovery Signatures| 0| 0| No Keys
Platform Key(PK)
Update
Enroll Factory Defaults or load certificates from a file:
1.Public Key Certificate:
a)EFI_SIGNATURE_LIST
b)EFI_CERT_X509 (DER)
c)EFI_CERT_RSA2048 (bin)
d)EFI_CERT_SHAXXX
2.Authenticated UEFI Variable
3.EFI PE/COFF Image(SHA256)
Key Source:
Factory,External,Mixed
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.20.1271. Copyright (C) 2018 American Megatrends, Inc.


Aptio Setup Utility – Copyright (C) 2018 American Megatrends, Inc.
Security
Vendor Keys Valid
Factory Key Provision [Disabled]
Restore Factory Keys
Reset To Setup Mode
Export Secure Boot variables
Enroll Efi Image
Device Guard Ready
Remove 'UEFI CA' from DB
Restore DB defaults
Secure Boot variable | Size| Ke
Platform Key(PK) | 0|
Key Exchange Keys | 0| 0| No Keys
Authorized Signatures| 0| 0| No Keys
Forbidden Signatures| 0| 0| No Keys
Authorized TimeStamps| 0| 0| No Keys
OsRecovery Signatures| 0| 0| No Keys
Key Exchange Keys
Update
Append
Enroll Factory Defaults or load certificates from a file:
1.Public Key Certificate:
a)EFI_SIGNATURE_LIST
b)EFI_CERT_X509 (DER)
c)EFI_CERT_RSA2048 (bin)
d)EFI_CERT_SHAXXX
2.Authenticated UEFI Variable
3.EFI PE/COFF Image(SHA256)
Key Source:
Factory,External,Mixed
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.20.1271. Copyright (C) 2018 American Megatrends, Inc.


Aptio Setup Utility – Copyright (C) 2018 American Megatrends, Inc.
Security
Vendor Keys Valid
Factory Key Provision [Disabled]
Restore Factory Keys
Reset To Setup Mode
Export Secure Boot variables
Enroll Efi Image
Device Guard Ready
Remove 'UEFI CA' from DB
Restore DB defaults
Secure Boot variable | Size| Ke
Platform Key(PK) | 0|
Key Exchange Keys | 0| 0| No Keys
Authorized Signatures| 0| 0| No Keys
Forbidden Signatures| 0| 0| No Keys
Authorized TimeStamps| 0| 0| No Keys
OsRecovery Signatures| 0| 0| No Keys
Authorized Signatures
Update
Append
Enroll Factory Defaults or load certificates from a file:
1.Public Key Certificate:
a)EFI_SIGNATURE_LIST
b)EFI_CERT_X509 (DER)
c)EFI_CERT_RSA2048 (bin)
d)EFI_CERT_SHAXXX
2.Authenticated UEFI Variable
3.EFI PE/COFF Image(SHA256)
Key Source:
Factory,External,Mixed
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.20.1271. Copyright (C) 2018 American Megatrends, Inc.


Aptio Setup Utility – Copyright (C) 2018 American Megatrends, Inc.
Security
Vendor Keys Valid
Factory Key Provision [Disabled]
Restore Factory Keys
Reset To Setup Mode
Export Secure Boot variables
Enroll Efi Image
Device Guard Ready
Remove 'UEFI CA' from DB
Restore DB defaults
Secure Boot variable | Size| Ke
Platform Key(PK) | 0|
Key Exchange Keys | 0| 0| No Keys
Authorized Signatures| 0| 0| No Keys
Forbidden Signatures| 0| 0| No Keys
Authorized TimeStamps| 0| 0| No Keys
OsRecovery Signatures| 0| 0| No Keys
Forbidden Signatures
Update
Append
Enroll Factory Defaults or load certificates from a file:
1.Public Key Certificate:
a)EFI_SIGNATURE_LIST
b)EFI_CERT_X509 (DER)
c)EFI_CERT_RSA2048 (bin)
d)EFI_CERT_SHAXXX
2.Authenticated UEFI Variable
3.EFI PE/COFF Image(SHA256)
Key Source:
Factory,External,Mixed
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.20.1271. Copyright (C) 2018 American Megatrends, Inc.



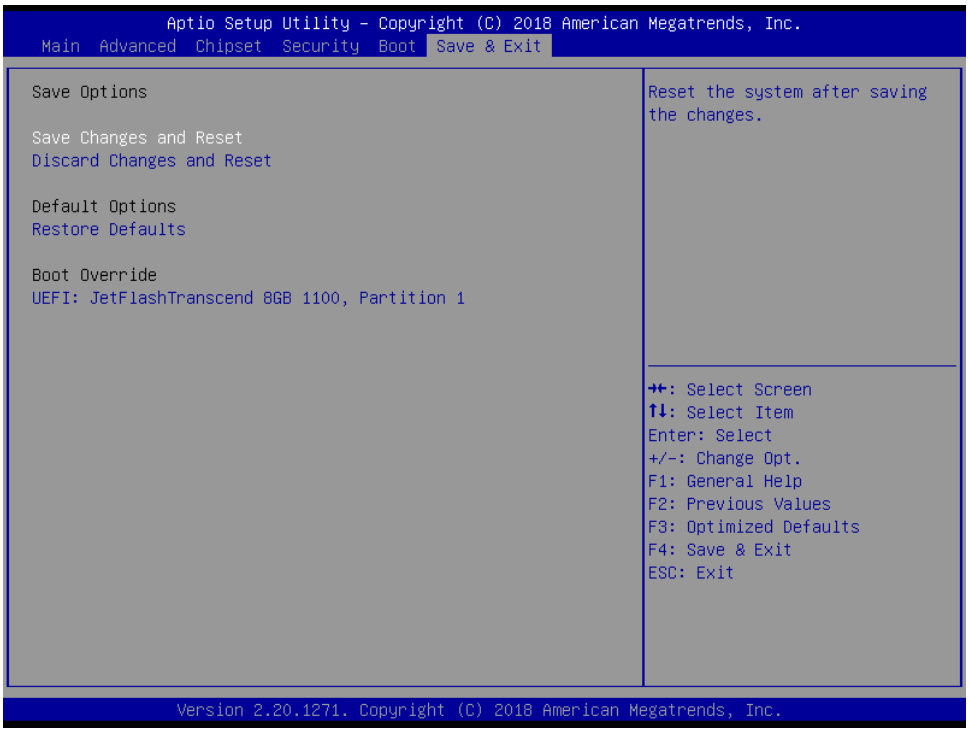


Item	Option	Description
Factory Key Provision	Disabled**[Default]** Enabled	Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode.

3.6.5 Boot

Item	Option	Description
Setup Prompt Timeout	1~ 65535	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.
Bootup NumLock State	On Off**[Default]**	Select the Keyboard NumLock state
Quiet Boot	Disabled**[Default]** Enabled	Enables or disables Quiet Boot option
Boot Option #1	Set the system boot order.	

3.6.6 Save and exit



3.6.6.1 Save Changes and Reset

Reset the system after saving the changes.

3.6.6.2 Discard Changes and Reset

Any changes made to BIOS settings during this session of the BIOS setup program are discarded. The setup program then exits and reboots the controller.

3.6.6.3 Restore Defaults

This option restores all BIOS settings to the factory default. This option is useful if the controller exhibits unpredictable behavior due to an incorrect or inappropriate BIOS setting.

3.6.6.4 Launch EFI Shell from filesystem device

Attempts to Launch EFI Shell application (Shellx64.efi) from one of the available filesystem devices.