AV600-CHX1-MB

Military IP65 GPU Rugged Computer Intel XEON E2276ML Processor, Nvidia A1000 GPU CE Certification MIL-STD-461 EMI 18-36V DC-In

User's Manual

Revision Date: July. 19 2023

Safety Information

Electrical safety

- To prevent electrical shock hazard, disconnect the power cable from the electrical outlet before relocating the system.
- When adding or removing devices to or from the system, ensure that the power cables for the devices are unplugged before the signal cables are connected. If possible, disconnect all power cables from the existing system before you add a device.
- Before connecting or removing signal cables from the motherboard, ensure that all power cables are unplugged.
- Seek professional assistance before using an adapter or extension cord. These devices could interrupt the grounding circuit.
- Make sure that your power supply is set to the correct voltage in your area.
- If you are not sure about the voltage of the electrical outlet you are using, contact your local power company.
- If the power supply is broken, do not try to fix it by yourself. Contact a qualified service technician or your local distributor.

Operation safety

- Before installing the motherboard and adding devices on it, carefully read all the manuals that came with the package.
- Before using the product, make sure all cables are correctly connected and the power cables are not damaged. If you detect any damage, contact your dealer immediately.
- To avoid short circuits, keep paper clips, screws, and staples away from connectors, slots, sockets and circuitry.
- Avoid dust, humidity, and temperature extremes. Do not place the product in any area where it may become wet.
- Place the product on a stable surface.
- If you encounter any technical problems with the product, contact your local distributor

Statement

- All rights reserved. No part of this publication may be reproduced in any form or by any means, without prior written permission from the publisher.
- All trademarks are the properties of the respective owners.
- All product specifications are subject to change without prior notice

Revision History

Revision	Date (yyyy/mm/dd)	Changes
Version 1.0	2023/07/19	Initial release

Packing list

- ▶ **AV600-CHX1-MB Military IP65 GPU Rugged System**
- ▶ **CD (Driver + Quick Installation Guide)**

Ordering information

Model Number	[Description]
AV600X-CH	AV600X-CH Military IP65 GPU Rugged Computer with Intel® XEON E-2278ML, Nvidia RTX A1000, DDR4 128GB, 1 x SATA SSD, HD-SDI, CAN bus, IP65, with MIL-DTL-D38999 Connectors, Operating Temp. -40 to 60°C
AV600-TH	AV600X-CH Military IP65 GPU Rugged Computer with Intel® XEON E-2278ML, Nvidia RTX A1000, DDR4 64GB, 1 x SATA SSD, 4xCH HD-SDI, IP65, with MIL-DTL-D38999 Connectors, Operating Temp. -40 to 60°C
AV600-THT	AV600X-CH Military IP65 GPU Rugged Computer with Intel® XEON E-2278ML, Nvidia RTX A1000, DDR4 64GB, 1 x SATA SSD, Discrete IO: 4xDI 4xDO, IP65, with MIL-DTL-D38999 Connectors, Operating Temp. -40 to 60°C
AV600-THX	AV600X-CH Military IP65 GPU Rugged Computer with Intel® XEON E-2278ML, Nvidia RTX A1000, DDR4 64GB, 1 x SATA SSD, 4xCH HD-SDI, Discrete IO: 4xDI 4xDO, IP65, with MIL-DTL-D38999 Connectors, Operating Temp. -40 to 60°C

If any of the above items is damaged or missing, please contact your local distributor.

Index

1. CHAPTER 1: PRODUCT INTRODUCTION 5
1-1. KEY FEATURES 5
1-2. DIMENSIONS(2D) 6
1-3. PANEL COMPONENT 7
2. CHAPTER 2: JUMPERS AND CONNECTORS LOCATIONS 8
2.1. D38999 CONNECT PIN DEFINITIONS 8
3. CHAPTER 3: AMI BIOS UTILITY 11
3.1 STARTING 11
3.2 NAVIGATION KEYS 11
3.3 MAIN MENU 12
3.4 ADVANCED MENU 13
3.4.1 CPU CONFIGURATION 14
3.4.2 POWER & PERFORMANCE 15
3.4.3 PCH-FW CONFIGURATION 16
3.4.4 AMT CONFIGURATION 17
3.4.5 TRUSTED COMPUTING 24
3.4.6 ACPI SETTINGS 26
3.4.7 IT8786 SUPER IO CONFIGURATION 27
3.4.8 HARDWARE MONITOR 29
3.4.9 PCI SUBSYSTEM SETTINGS 31
3.4.10 USB CONFIGUATION 32
3.4.11 CSM CONFIGURATION 33
3.4.12 NVME CONFIGURATION 34
3.4.13 NETWORK STACK CONFIGURATION 35
3.5 CHIPSET 36
3.5.1 SYSTEM AGENT (SA) CONFIGURATION 36
3.5.2 PCH-IO CONFIGURATION 39
3.6 SECURITY 45
3.6.1 ADMINISTRATOR PASSWORD 45
3.6.2 USER PASSWORD 46
3.6.3 SECURE BOOT 46
3.7 BOOT 54

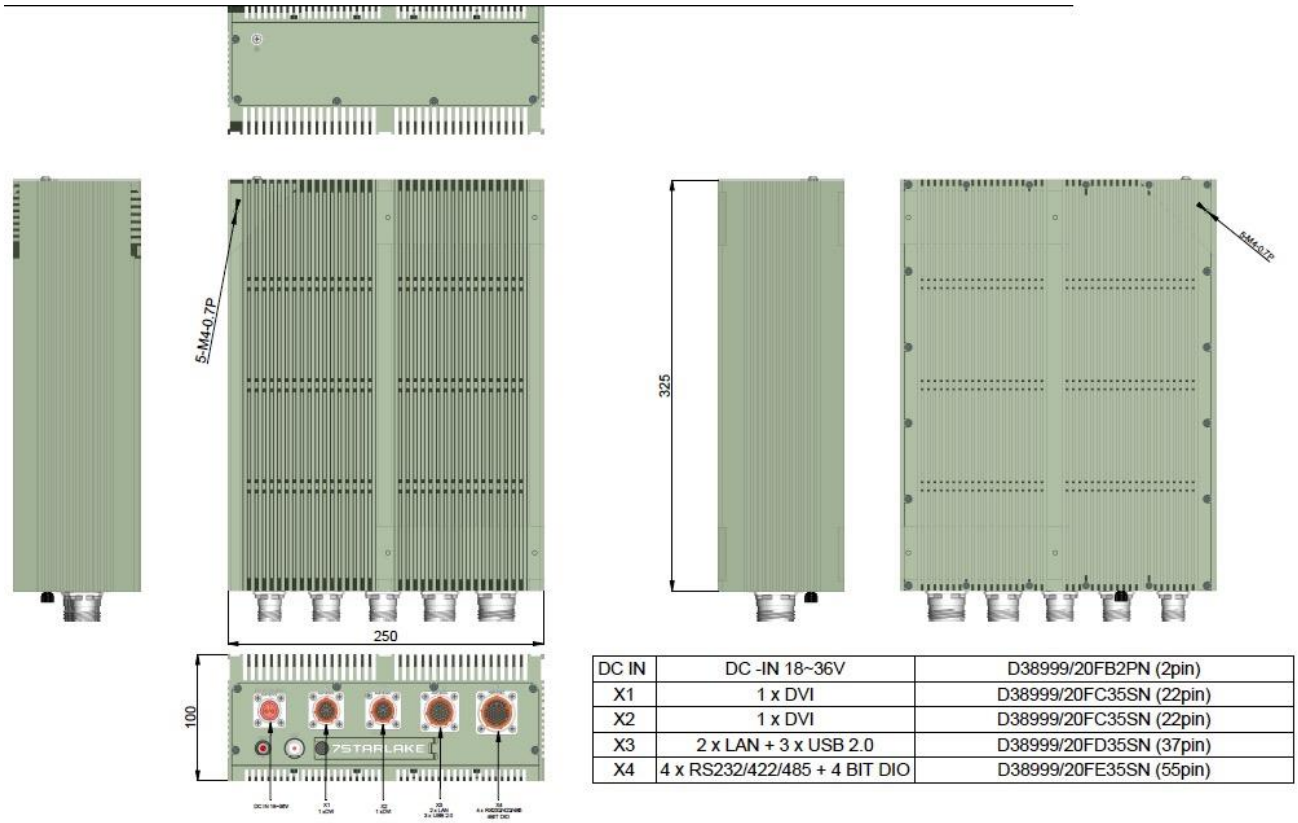
3.8 SAVE & EXIT 55
3.8.1 SAVE CHANGES AND EXIT 55
3.8.2 EXIT WITHOUT SAVING 56
3.8.3 SAVE & RESET 56
3.8.4 RESET WITHOUT SAVING 57
3.8.5 SAVE SETUP VALUES 57
3.8.6 LOAD PREVIOUS VALUES 58
3.8.7 LOAD OPTIMIZED DEFAULTS 58
3.8.8 SAVE VALUES AS USER DEFAULTS 59
3.8.9 RESTORE USER DEFAULTS 59

1. Chapter 1: Product Introduction

1-1. Key Features

System	
CPU	Intel® Xeon E2276ML (2.0Ghz, 25W, 12MB)
Memory Type	DDR4 2666MHz 32GB
Graphics	NVidia® RTX A1000 2048 CUDA® cores, 4GB GDDR6 128-bit
BIOS	AMI® BIOS
Storage Device	2.5" 128GB SATAIII SSD (Swappable SSD Tray)
Front I/O	
DC In	1 x Amphenol D38999/20FB2SN
X1	1 x Amphenol D38999 20FC35SN
X2	1 x Amphenol D38999 20FC35SN
X3	1 x Amphenol D38999 20FD35SN
X4	1 x Amphenol D38999 20FE35SN
SSD	Swappable SSD Tray
Power Button with LED backlight	
Applications	
Applications	Military IP65 GPU Rugged Mission MIL-STD 810 Computer is built to meet strict size, weight, and power (SWaP) requirements and to withstand harsh environments, including temperature extremes, shock/vibe, sand/dust, and salt/fog.
Operation System	
OS Support	Windows 10 64bit, Windows server 2019 64bit, Windows 2016 64bit, Hyper-V Server 2016 R2, Ubuntu 16.04.3 LTS/17.10/18.04.1 LTS, Fedora 25/26, RedHat Linux EL 6.8/6.9/7.3/7.4/7.6, VMware ESXi6.5u1, VMware ESXi6.7u2
Mechanical & Environment	
Chassis	Aluminum Alloy, Corrosion design
Finish	Anodic aluminum oxide
Cooling	Natural Passive Convection/Conduction. No Moving Parts
Ingress Protection	IP65
Power Requirements	MIL-STD-461 EMI Power Supply, 18-36V DC In
Dimension (W x D x H)	246 x 313 x 100mm (9.6" x 12.3" x 3.9")
Operating Temp.	-40 to 60°C
Storage Temp.	-40 to 85°C
Relative Humidity	5% to 95%, non-condensing

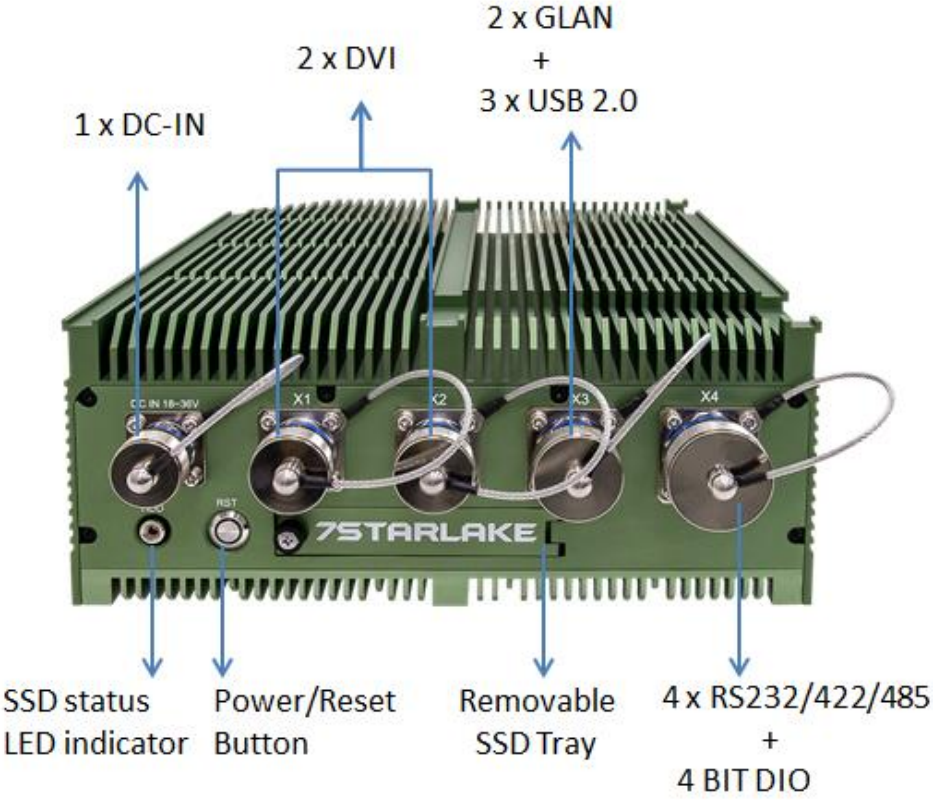
1-2. Dimensions(2D)



DC IN	DC -IN 18~36V	D38999/20FB2PN (2pin)
X1	1 x DVI	D38999/20FC35SN (22pin)
X2	1 x DVI	D38999/20FC35SN (22pin)
X3	2 x LAN + 3 x USB 2.0	D38999/20FD35SN (37pin)
X4	4 x RS232/422/485 + 4 BIT DIO	D38999/20FE35SN (55pin)

Dimensions(3D)

1-3. Panel Component



1	DVI label (X1)
2	DVI label (X2)
3	2 x LAN+3 x USB2.0 label (X3)
4	4 x RS232/422/485 + 4 BIT DIO label (X4)
5	DC-In, label
6	Swappable SSD Tray
7	Power button, label
8	HDD LED, label

2. Chapter 2: Jumpers and Connectors Locations

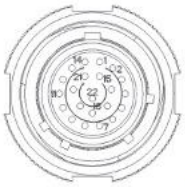
2.1. D38999 Connect Pin Definitions

DC-In

		D38999	Pin define	
	Power EXT	A	(+)	TN1
		B	(-)	TN2
		SHELL	G	O Plug

CON1
D38999/26MB2SN

X1, X2: DVI

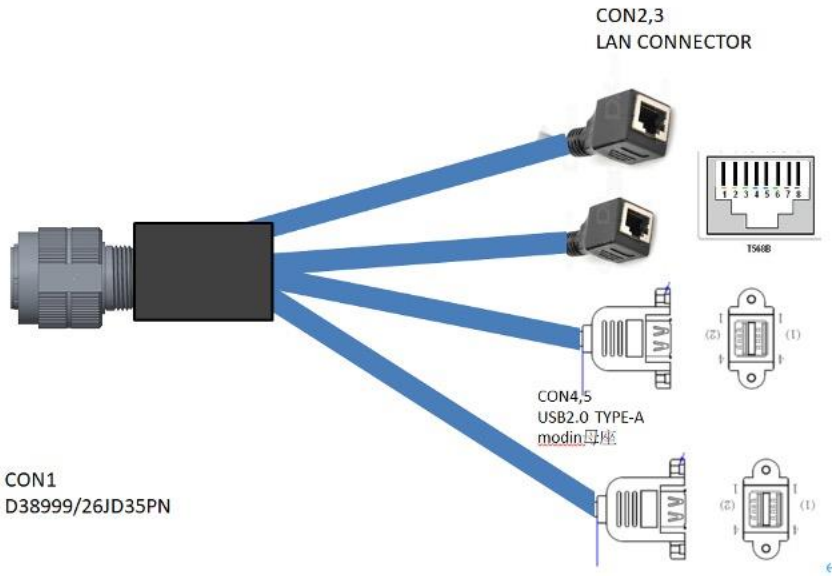
X1		Pin define	DVI
	1	DPA_TN0	1
	2	DPA_TP0	2
	3	GND	3
	4	DPA_AUXP_CLK(p)	6
	5	DPA_AUXP_CLK(n)	7
	6	GND	3
	7	DPA_TN1	9
	8	DPA_TP1	10
	9	GND	11
	10	DPA_PWR	14
	11	Return GND	15
	12	AUX_SEL/DPA_DET	16
	13	DPA_TN2	17
	14	DPA_TP2	18
	15	GND	19
	16	CLOCK Shield	22
	17	DPA_TP3	23
	18	DPA_TN3	24
	19	GND	shell

CON1
D38999/26FC35PN

CON2
DVI CONNECTOR (MALE)

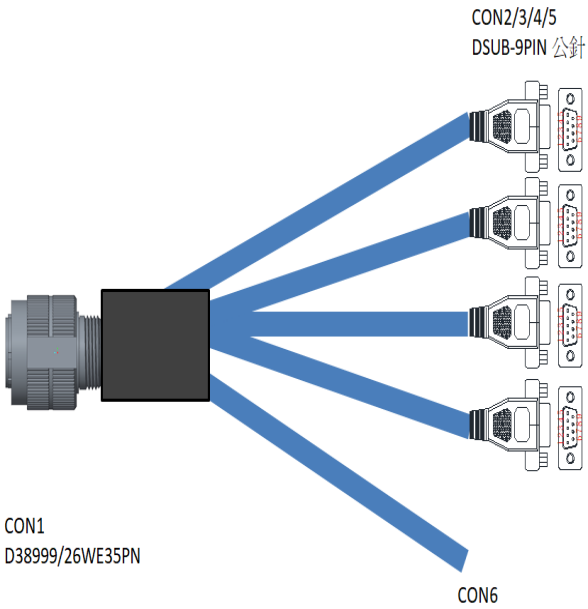
X3: LAN, USB 2.0

X3	D38999	Pin define	CON2	CON3	CON4	CON5
	1	WHITE / ORANGE	1			
	2	ORANG	2			
	3	WHITE / GREEN	3			
	4	BLUE	4			
	5	WHITE / BLUE	5			
	6	GREEN	6			
	7	WHITE / BROWN	7			
	8	BROWN	8			
	9	WHITE / ORANGE		1		
	10	ORANG		2		
	11	WHITE / GREEN		3		
	12	BLUE		4		
	13	WHITE / BLUE		5		
	14	GREEN		6		
	15	WHITE / BROWN		7		
	16	BROWN		8		
	17					
	18					
	19					
	20	Vcc			1	
	21	Date-			2	
	22	Date+			3	
	23	GND			4	
	24	Vcc			1	
	25	Date-			2	
	26	Date+			3	
	27	GND			4	
	28	Shell				
	29	Vcc				1
	30	Date-				2
	31	Date+				3
	32	GND				4
	33	Vcc				1
	34	Date-				2
	35	Date+				3
	36	GND				4
	37	Shell				



X4: 4 x COM and 4 BIT DIO

CON1	CON2	CON3	CON4			CON1	CON5	CON6	
1	1			DCD		28	1		DCD
2	2			RX		29	2		RX
3	3			TX		30	3		TX
4	4			DTR		31	4		DTR
5	5			GND		32	5		GND
6	6			DSR		33	6		DSR
7	7			RTS		34	7		RTS
8	8			CTS		35	8		CTS
9	9			RI		36	9		RI
10		1		DCD		37			
11		2		RX		38			
12		3		TX		39			
13		4		DTR		40			
14		5		GND		41		1	DIO0(IN)
15		6		DSR		42		2	DIO1(IN)
16		7		RTS		43		3	DIO2(IN)
17		8		CTS		44		4	DIO3(IN)
18		9		RI		45		5	DIO0(OUT)
19			1	DCD		46		6	DIO1(OUT)
20			2	RX		47		7	DIO2(OUT)
21			3	TX		48		8	DIO3(OUT)
22			4	DTR		49		9	3.3V
23			5	GND		50		10	GND
24			6	DSR		51			
25			7	RTS		52			
26			8	CTS		53			
27			9	RI		54			
						55			



3.Chapter 3: AMI BIOS Utility

This chapter provides users with detailed descriptions on how to set up a basic system configuration through the AMI BIOS setup utility.

3.1 Starting

To enter the setup screens, perform the following steps:

• Turn on the computer and press the <Del> key immediately.

• After the <Del> key is pressed, the main BIOS setup menu displays. Other setup screens can be accessed from the main BIOS setup menu, such as the Chipset and Power menus.

3.2 Navigation Keys

The BIOS setup/utility uses a key-based navigation system called hot keys. Most of the BIOS setup utility hot keys can be used at any time during the setup navigation process.
Some of the hot keys are <F1>, <F10>, <Enter>, <ESC>, and <Arrow> keys.

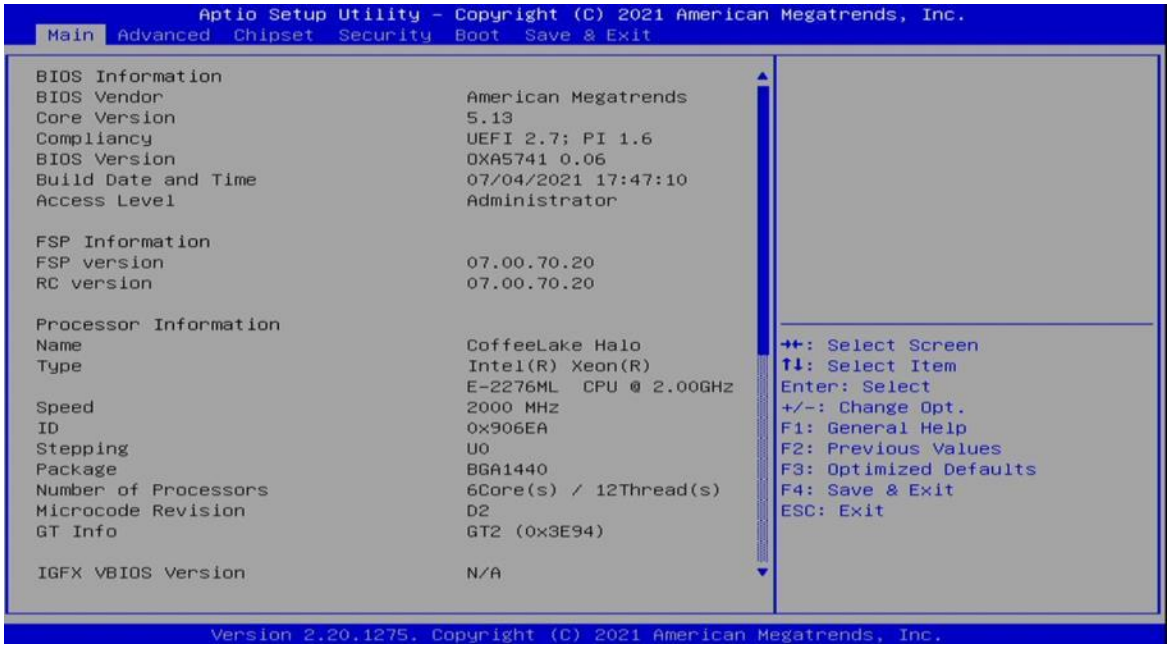
Some of the navigation keys may differ from one screen to another.

Left/Right	The Left and Right <Arrow> keys moves the cursor to select a menu.
Up/Down	The Up and Down <Arrow> keys moves the cursor to select a setup screen or sub-screen.
+– Plus/Minus	The Plus and Minus <Arrow> keys changes the field value of a particular setup setting.
Tab	The <Tab> key selects the setup fields.
F1	The <F1> key displays the General Help screen.
F10	The <F10> key saves any changes made and exits the BIOS setup utility.
Esc	The <Esc> key discards any changes made and exits the BIOS setup utility.
Enter	The <Enter> key displays a sub-screen or changes a selected or highlighted option in each menu.

3.3 MAIN MENU

The Main menu is the screen that first displays when BIOS Setup is entered, unless an error has occurred.

When you first enter the BIOS Setup Utility, you will encounter the Main setup screen. You can always return to the Main setup screen by selecting the Main tab. There are two Main Setup options. They are described in this section. The Main BIOS Setup screen is shown below.



The Main BIOS setup screen has two main frames. The left frame displays all the options that can be configured. Grayed-out options cannot be configured; options in blue can. The right frame displays the key legend. Above the key legend is an area reserved for a text message. When an option is selected in the left frame, it is highlighted in white. Often a text message will accompany it.

System Date

Use this function to change the system date.

Select System Date using the Up and Down <Arrow> keys. Enter the new values through the keyboard. Press the Left and Right <Arrow> keys to move between fields.

The date setting must be entered in MM/DD/YY format.

System Time

Use this function to change the system time.

Select System Time using the Up and Down <Arrow> keys. Enter the new values through the keyboard. Press the Left and Right <Arrow> keys to move between ields.

The time setting is entered in HH:MM:SS format.

Note: The time is in 24-hour format. For example, 5:30 A.M. appears as 05:30:00, and 5:30 P.M. as

17:30:00.

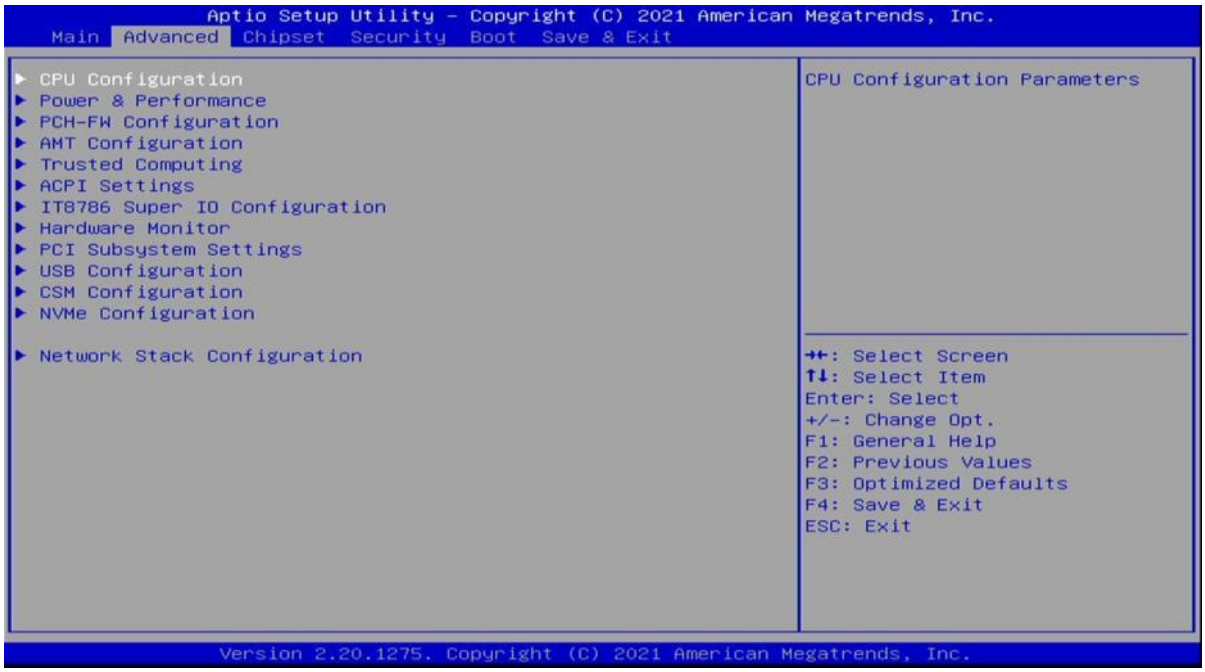
Access Level

Display the access level of the current user in the BIOS.

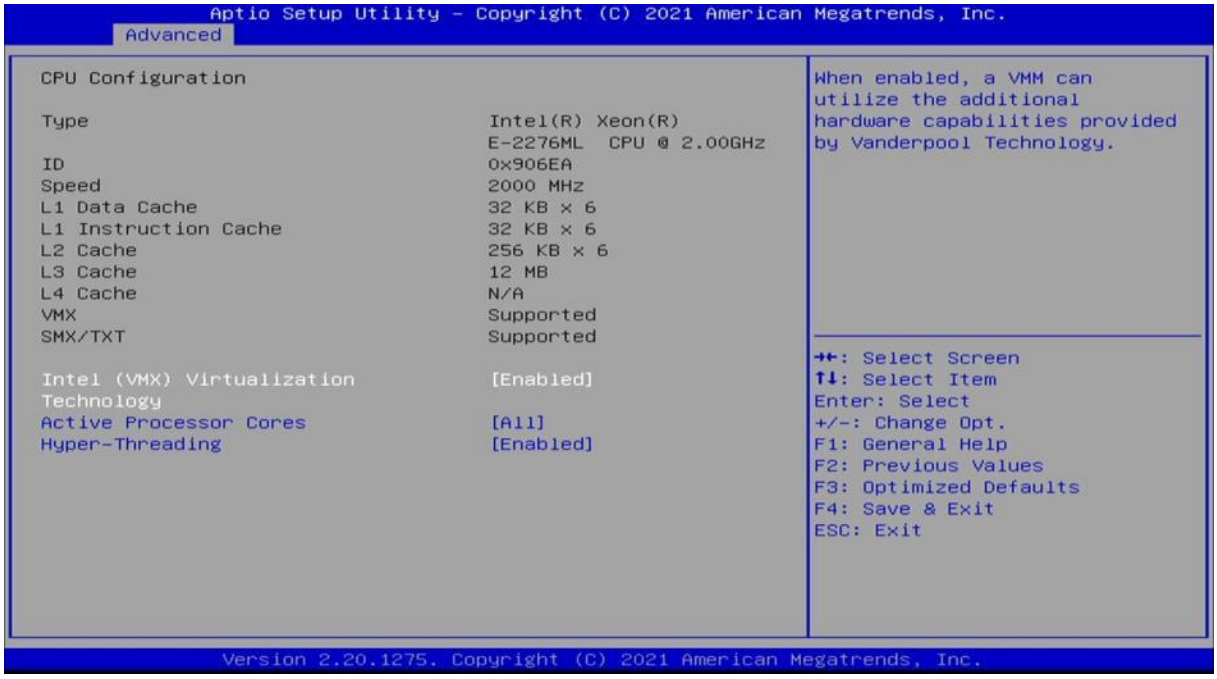
3.4 ADVANCED MENU

The Advanced Menu allows you to configure your system for basic operation. Some entries are defaults required by the system board, while others, if enabled, will improve the performance of your system or let you set some features according to your preference.

Setting incorrect field values may cause the system to malfunction.



3.4.1 CPU CONFIGURATION

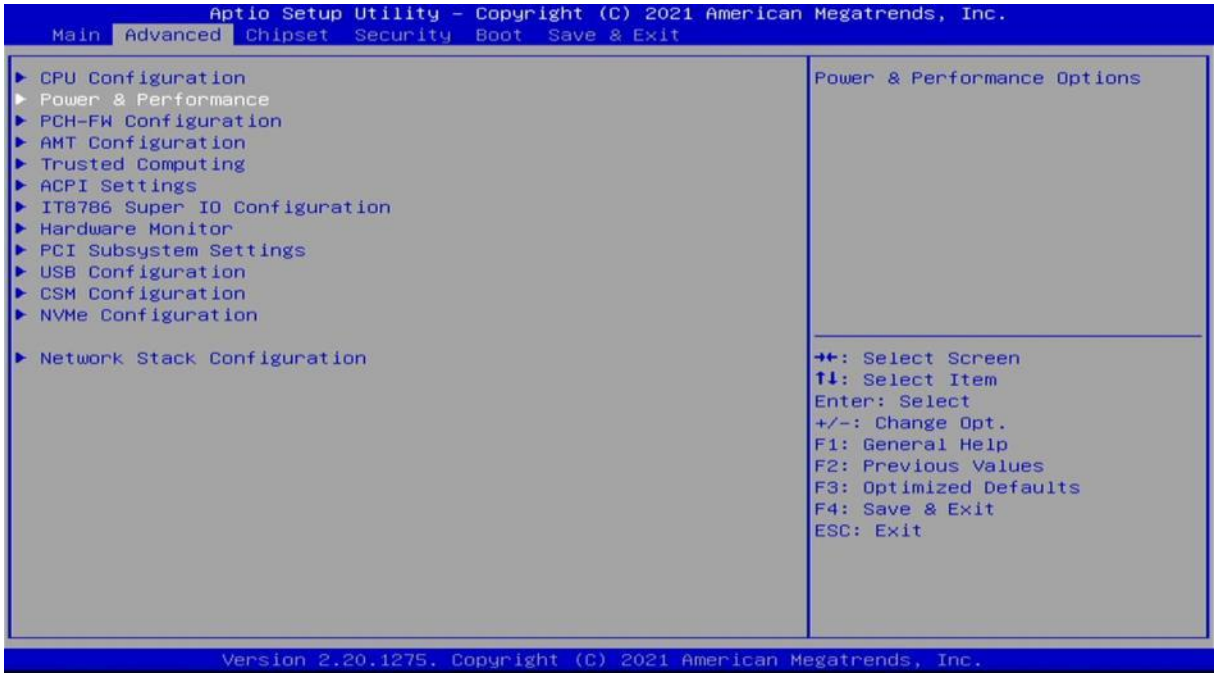


Field Name	**Intel (VMX) Virtualization Technology**
Default Value	[Enabled]
Possible Value	Disabled Enabled

Field Name	**Active Processor Cores**
Default Value	[A11]
Possible Value	A11 1 2 3 4 5

Field Name	**Hyper-Threading**
Default Value	[Enabled]
Possible Value	Disabled Enabled

3.4.2 POWER & PERFORMANCE

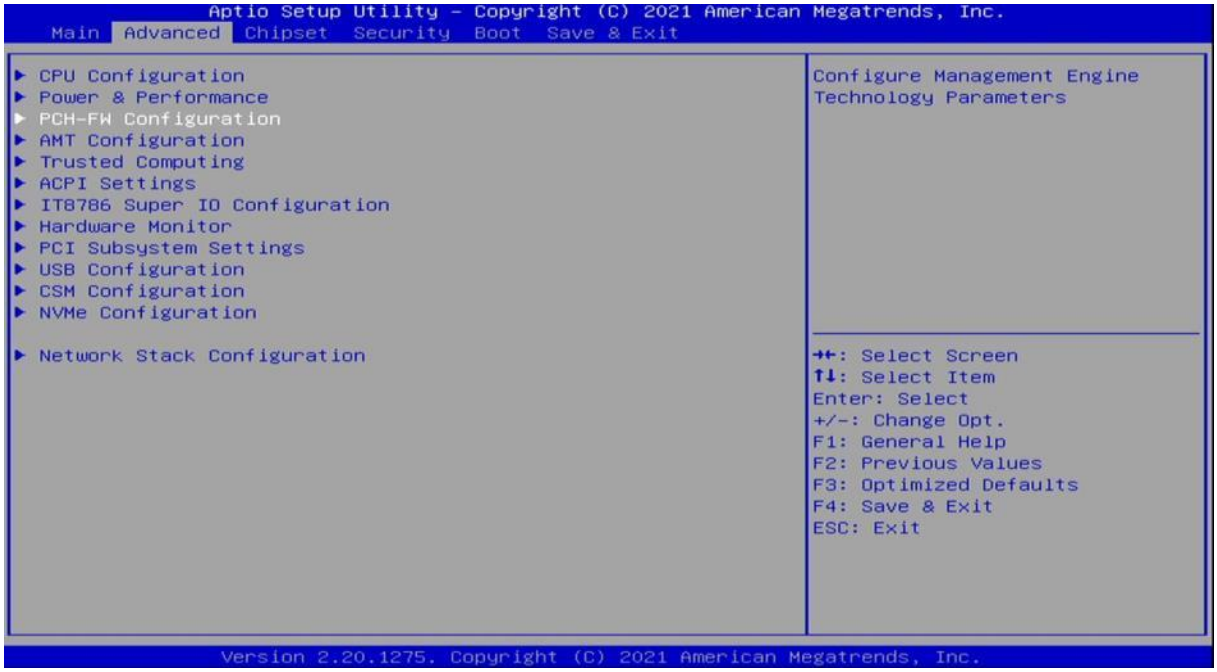


Field Name	**Intel (R) SpeedStep(tm)**
Default Value	[Enabled]
Possible Value	Disabled Enabled

Field Name	**Turbo Mode**
Default Value	[Enabled]
Possible Value	Disabled Enabled

Field Name	**C states**
Default Value	[Disabled]
Possible Value	Disabled Enabled

3.4.3 PCH-FW CONFIGURATION

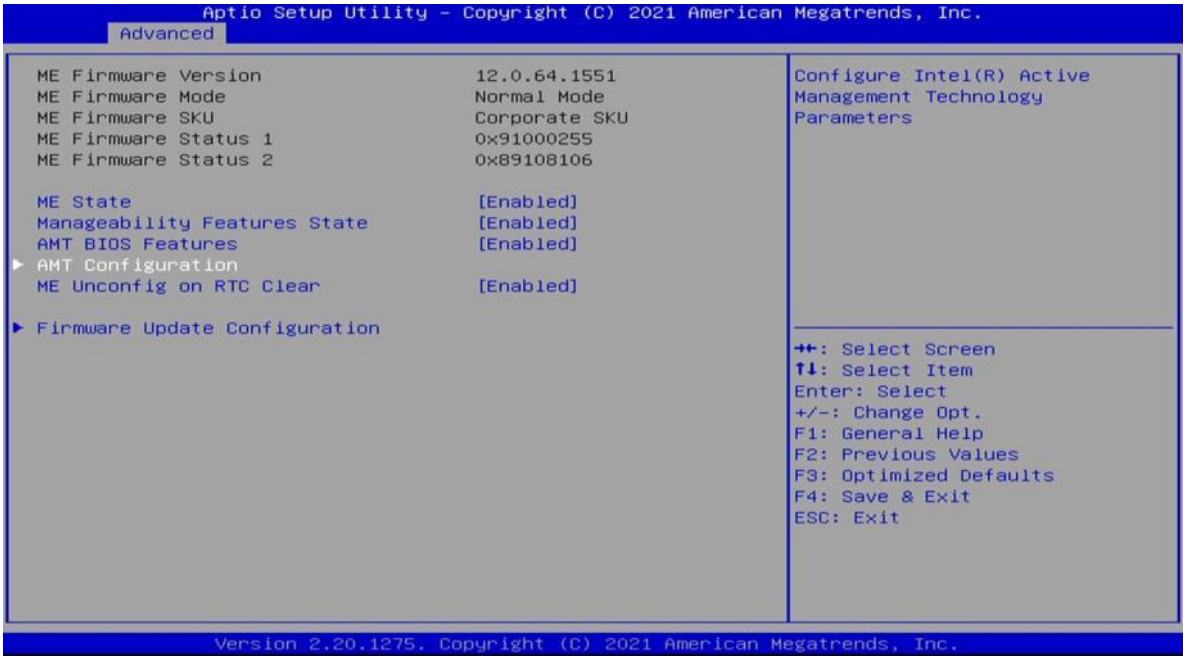


Field Name	**ME State**
Default Value	[Enabled]
Possible Value	Disabled Enabled

Field Name	**Manageability Features State**
Default Value	[Enabled]
Possible Value	Disabled Enabled

Field Name	**AMT BIOS Features**
Default Value	[Enabled]
Possible Value	Disabled Enabled

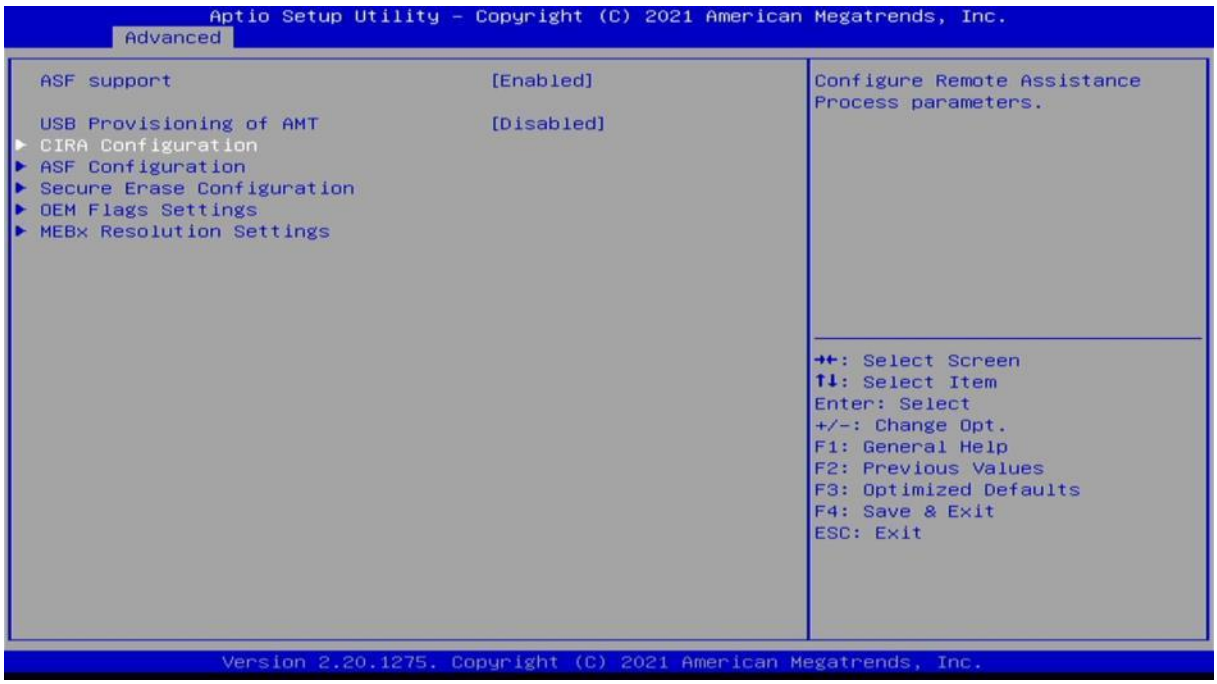
3.4.4 AMT CONFIGURATION



Field Name	ASF support
Default Value	[Enabled]
Possible Value	Disabled Enabled

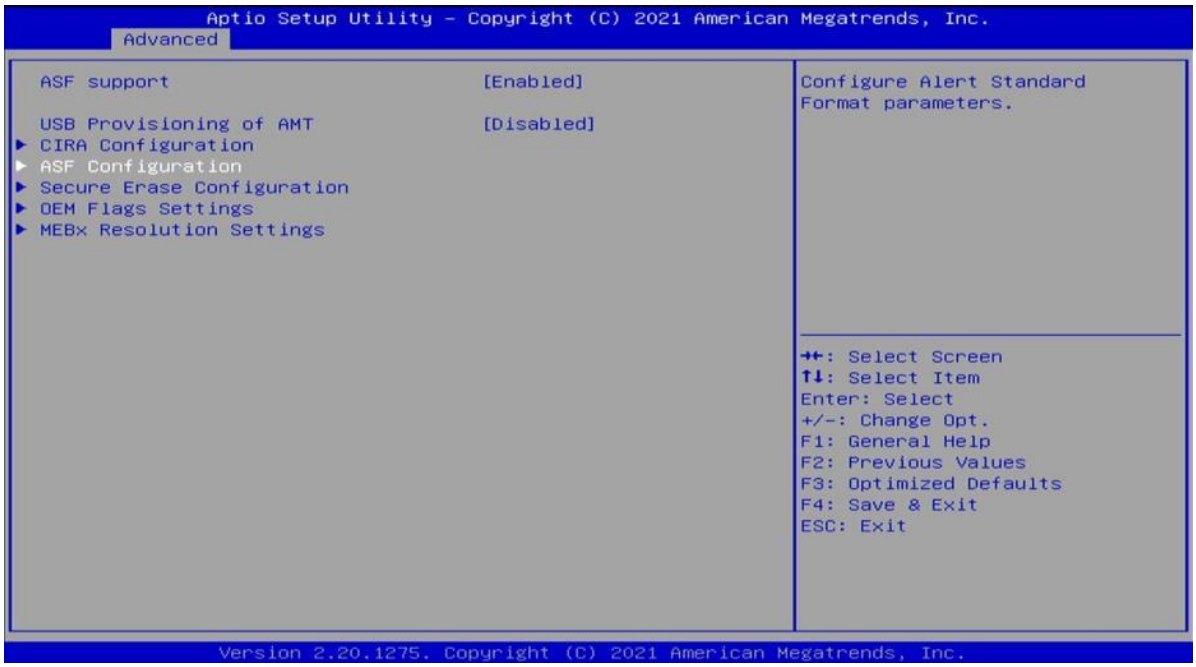
Field Name	USB Provisioning of AMT
Default Value	[Disabled]
Possible Value	Disabled Enabled

3.4.4.1 CIRA CONFIGURATION



Field Name	Activate Remote Assistance Process
Default Value	[Disabled]
Possible Value	Disabled Enabled

3.4.4.2 ASF CONFIGURATION



Field Name	**PET Progress**
Default Value	[Enabled]
Possible Value	Disabled Enabled

Field Name	**WatchDog**
Default Value	[Disabled]
Possible Value	Disabled Enabled

Field Name	**ASF Sensors Table**
Default Value	[Disabled]
Possible Value	Disabled Enabled

3.4.4.3 SECURE ERASE CONFIGURATION

Field Name	Secure Erase mode
Default Value	[Simulated]
Possible Value	Simulated Real

Field Name	Force Secure Erase
Default Value	[Disabled]
Possible Value	Disabled Enabled

3.4.4.4 OEM FLAGS SETTINGS

Field Name	MEBx hotkey Pressed
Default Value	[Disabled]
Possible Value	Disabled Enabled

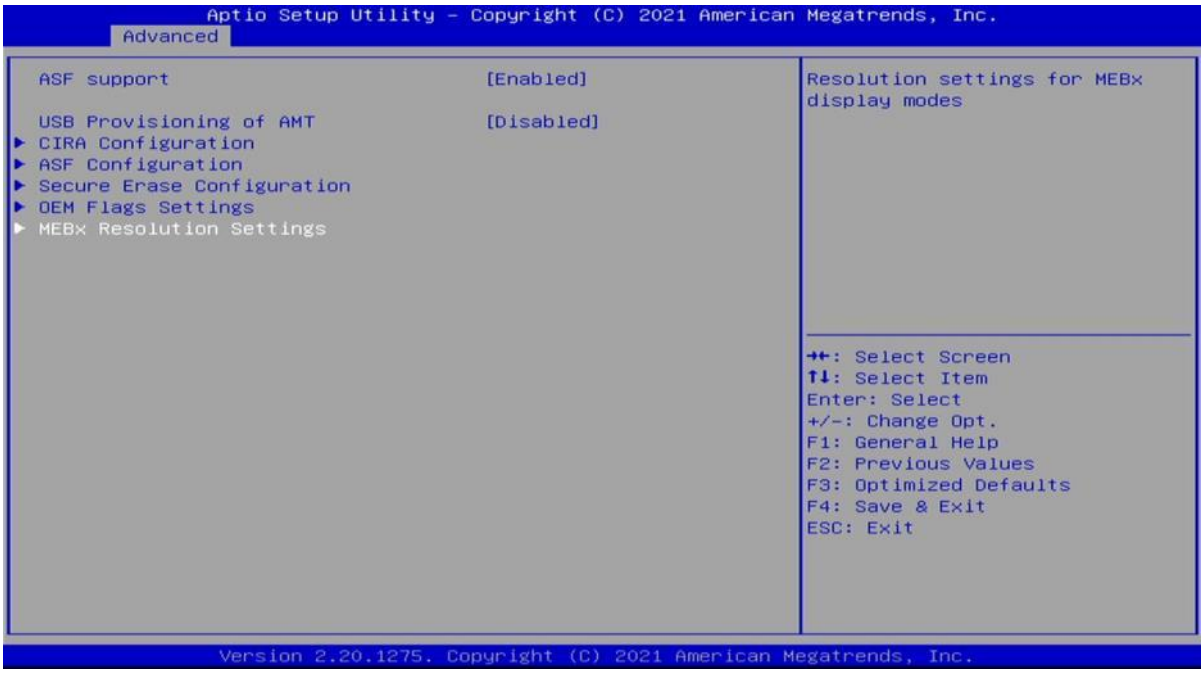
Field Name	MEBx Selection Screen
Default Value	[Disabled]
Possible Value	Disabled Enabled

Field Name	Hide Unconfigure ME Confirmation Prompt
Default Value	[Disabled]
Possible Value	Disabled Enabled

Field Name	MEBx OEM Debug Menu Enable
Default Value	[Disabled]
Possible Value	Disabled Enabled

Field Name	Unconfigure ME
Default Value	[Disabled]
Possible Value	Disabled Enabled

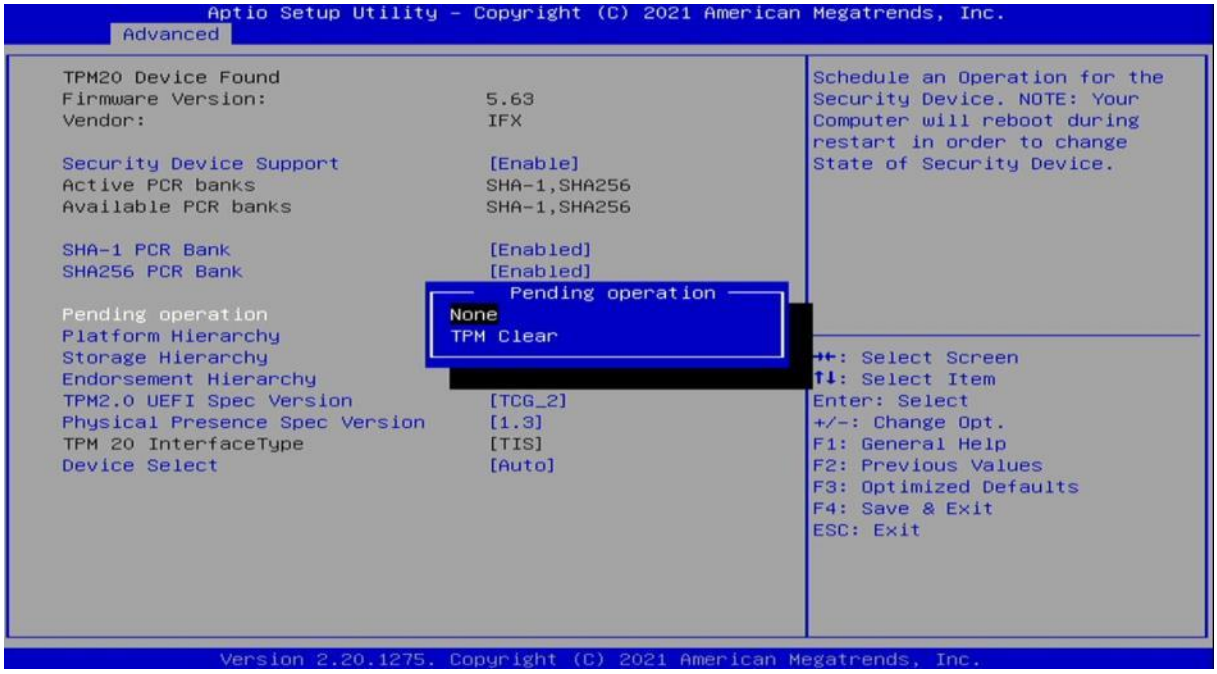
3.4.4.5 MEBx Resolution Settings



Field Name	Non-UI Mode Resoultion
Default Value	[Auto]
Possible Value	Auto 80x25 100x31

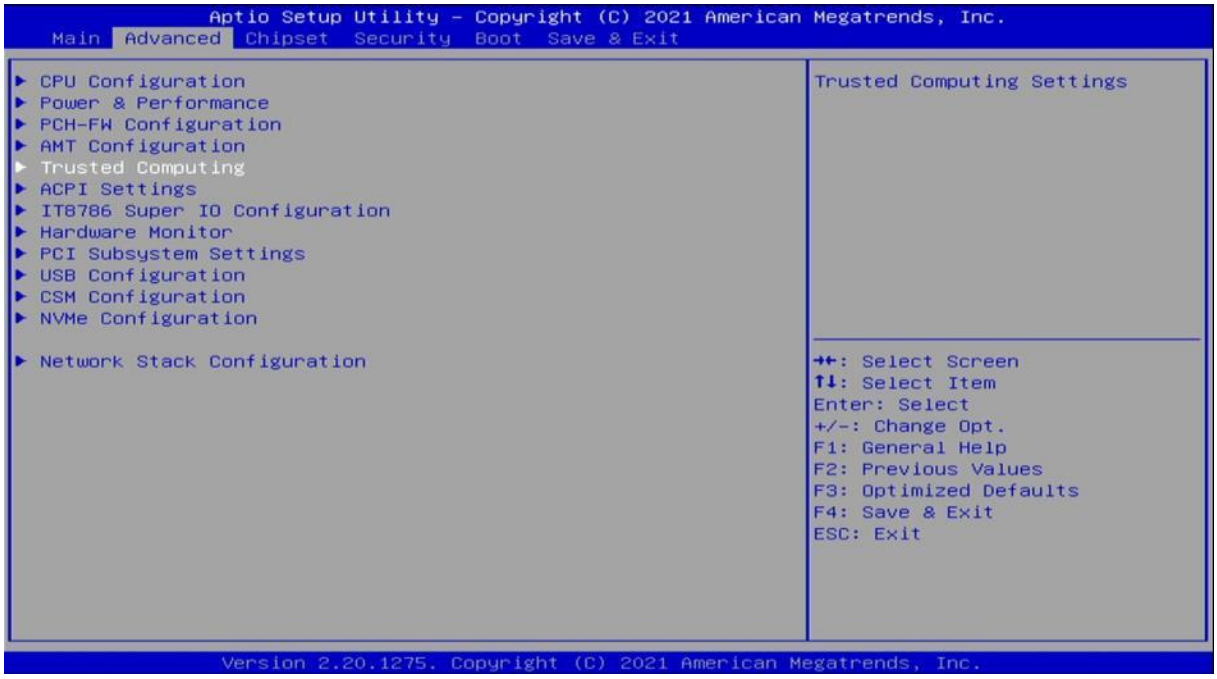
Field Name	UI Mode Resolution
Default Value	[Auto]
Possible Value	Auto 80x25 100x31

Field Name	Graphics Mode Resoultion
Default Value	[Auto]
Possible Value	Auto 640x480 800x600 1024x768



Field Name	Pending operation
Default Value	[None]
Possible Value	None TPM Clear

3.4.5 TRUSTED COMPUTING



Field Name	**Security Device Support**
Default Value	[Enabled]
Possible Value	Disabled Enabled

Field Name	**SHA-1 PCR Bank**
Default Value	[Enabled]
Possible Value	Disabled Enabled

Field Name	**SHA256 PCR Bank**
Default Value	[Enabled]
Possible Value	Disabled Enabled

Field Name	**Pending operation**
Default Value	[None]
Possible Value	None TPM Clear

Field Name	**Platform Hierarchy**
Default Value	[Enabled]
Possible Value	Disabled Enabled

Field Name	Storage Hierarchy
Default Value	[Enabled]
Possible Value	Disabled Enabled

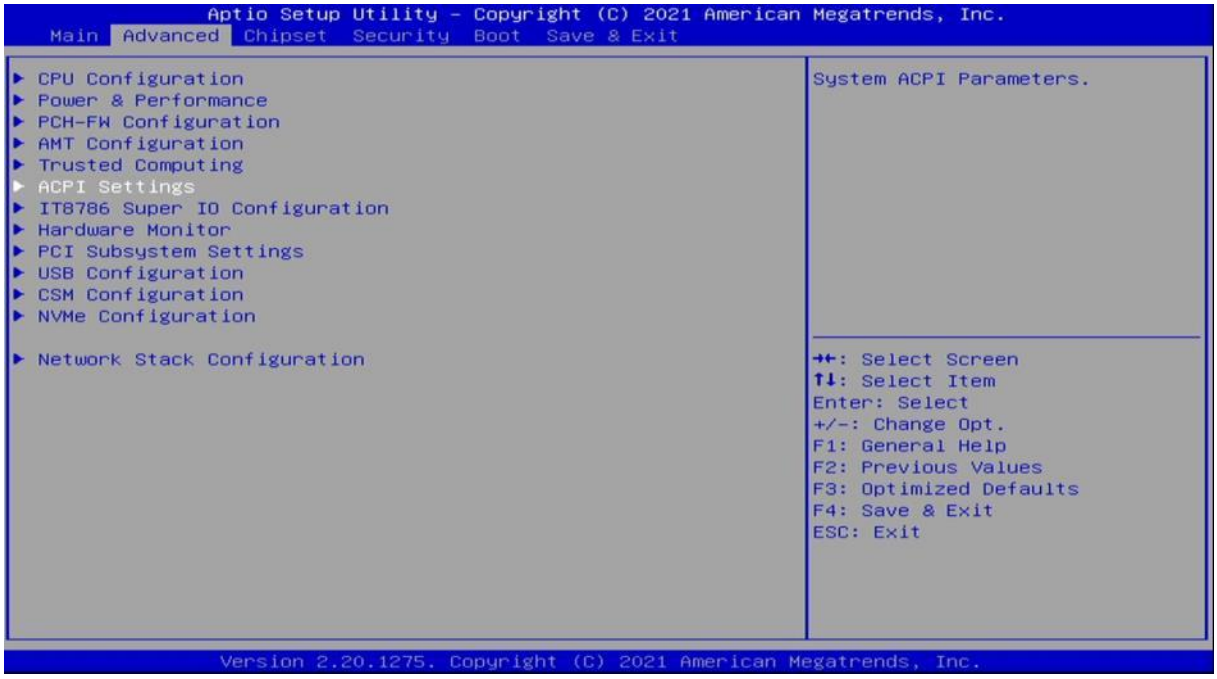
Field Name	Endorsement Hierarchy
Default Value	[Enabled]
Possible Value	Disabled Enabled

Field Name	TPM2.0 UEFI Spec Version
Default Value	[TCG_2]
Possible Value	TCG_1_2 TCG_2

Field Name	Physical Presence Spec Version
Default Value	[1.3]
Possible Value	1.2 1.3

Field Name	Device Select
Default Value	[Auto]
Possible Value	TPM 1.2 TPM 2.0 Auto

3.4.6 ACPI SETTINGS



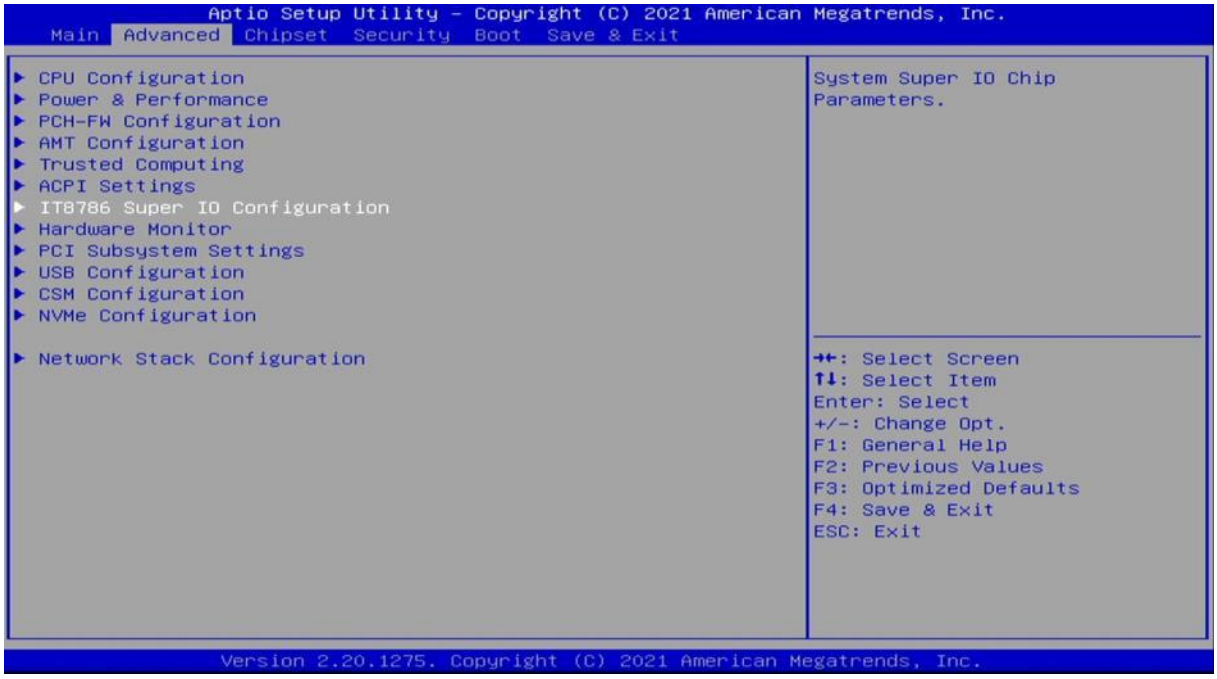
Field Name	**Enable ACPI Auto Configuration**
Default Value	[Disabled]
Possible Value	Disabled Enabled

Field Name	**Enable Hibernation**
Default Value	[Enabled]
Possible Value	Disabled Enabled

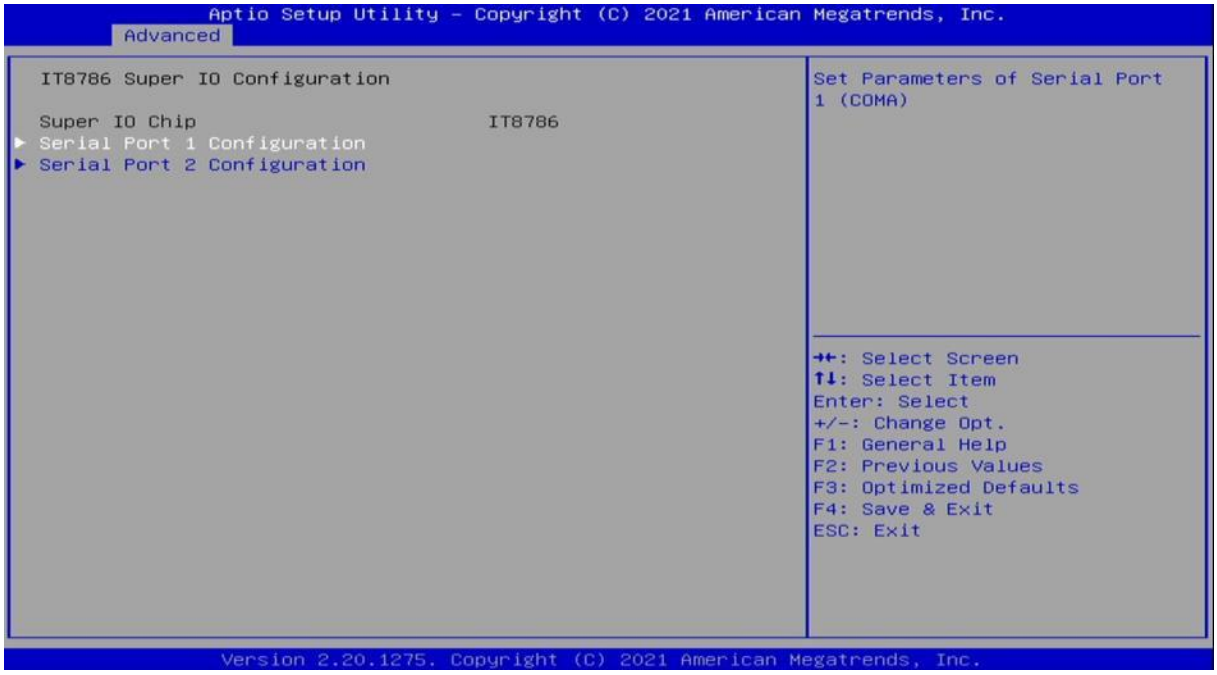
Field Name	**ACPI Sleep State**
Default Value	[S3 (Suspend to RAM)]
Possible Value	Suspend Disabled S3 (Suspend to RAM)

Field Name	**Lock Legacy Resources**
Default Value	[Disabled]
Possible Value	Disabled Enabled

3.4.7 IT8786 SUPER IO CONFIGURATION



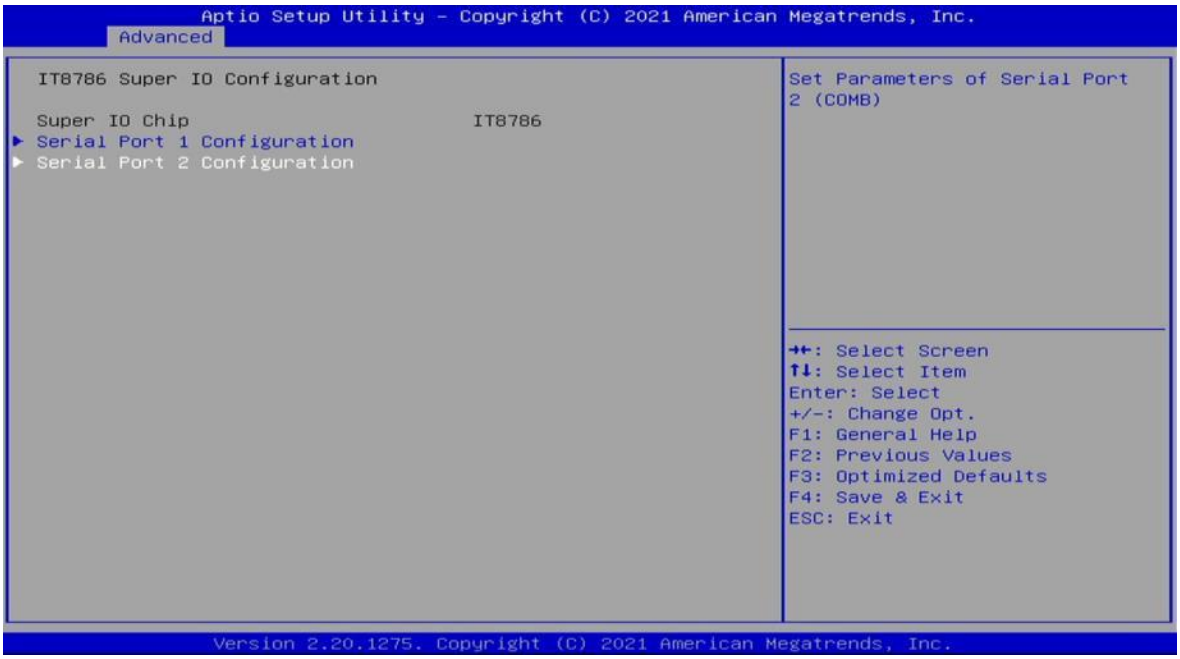
3.4.7.1 SECIAL PORT 1 CONFIGURATION



Field Name	Serial Port
Default Value	[Enabled]
Possible Value	Disabled Enabled

Field Name	COM1 Control
Default Value	[RS-232]
Possible Value	Loopback RS-232 RS-485 Half Duplex RS-485/422 Full Duplex

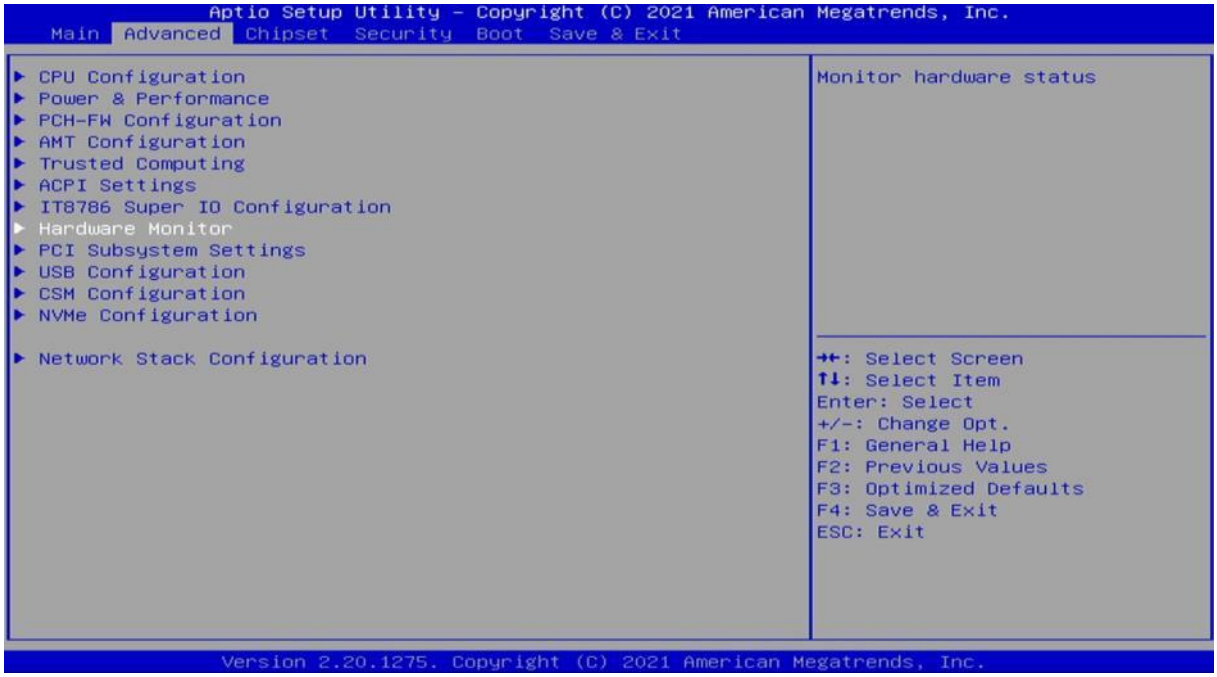
3.4.7.2 SERIAL PORT 2 CONFIGURATION



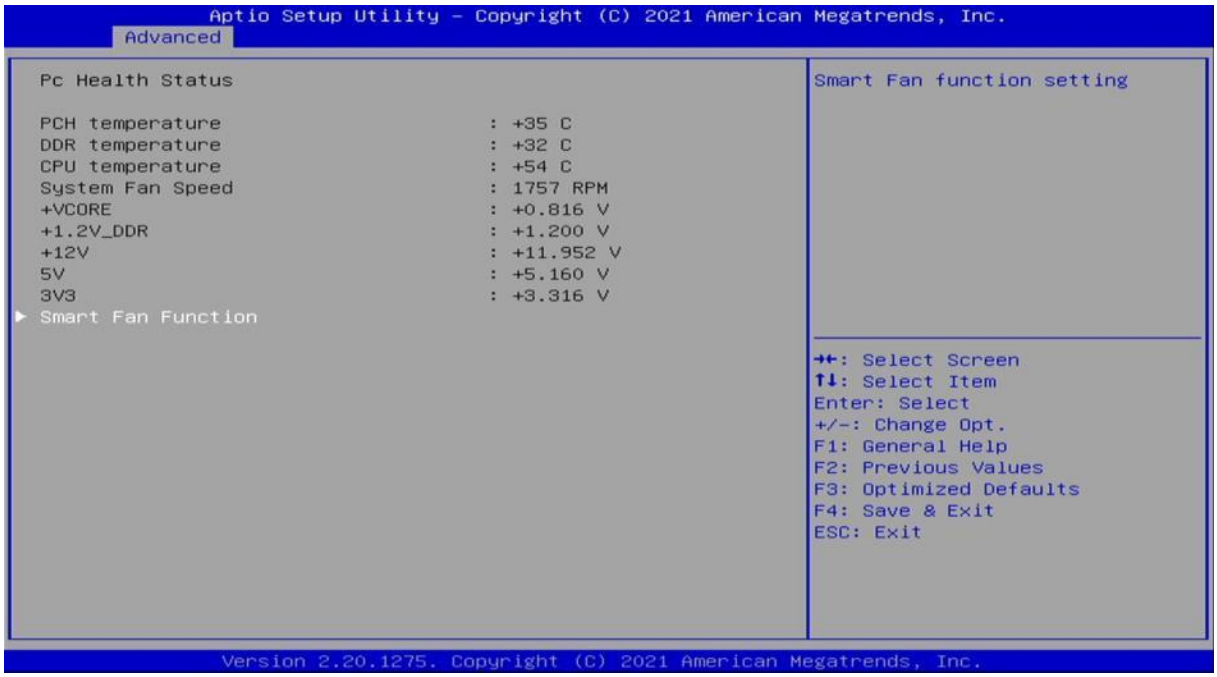
Field Name	Serial Port
Default Value	[Enabled]
Possible Value	Disabled Enabled

Field Name	COM2 Control
Default Value	[RS-232]
Possible Value	Loopback RS-232 RS-485 Half Duplex RS-485/422 Full Duplex

3.4.8 HARDWARE MONITOR



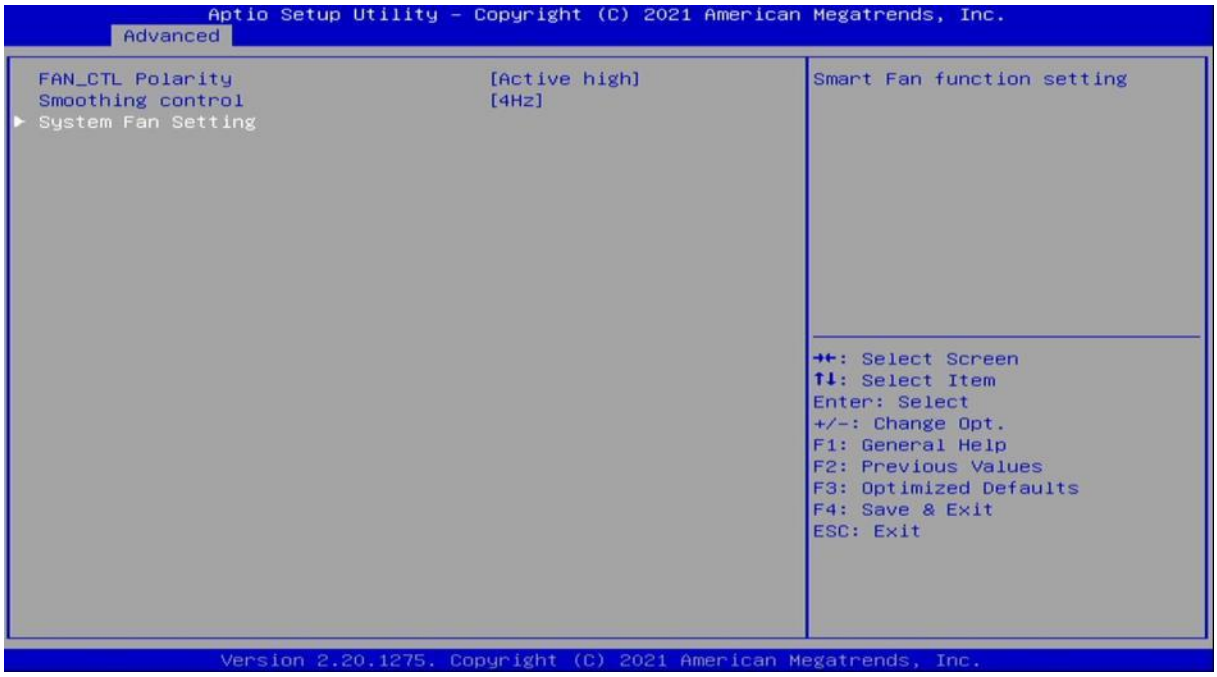
3.4.8.1 SMART FAN FUNCTION



Field Name	FAN_CTL Polarity
Default Value	[Active high]
Possible Value	Active low Active high

Field Name	Smoothing control
Default Value	[4Hz]
Possible Value	1Hz 16Hz 8Hz 4Hz

3.4.8.2 System Fan Setting



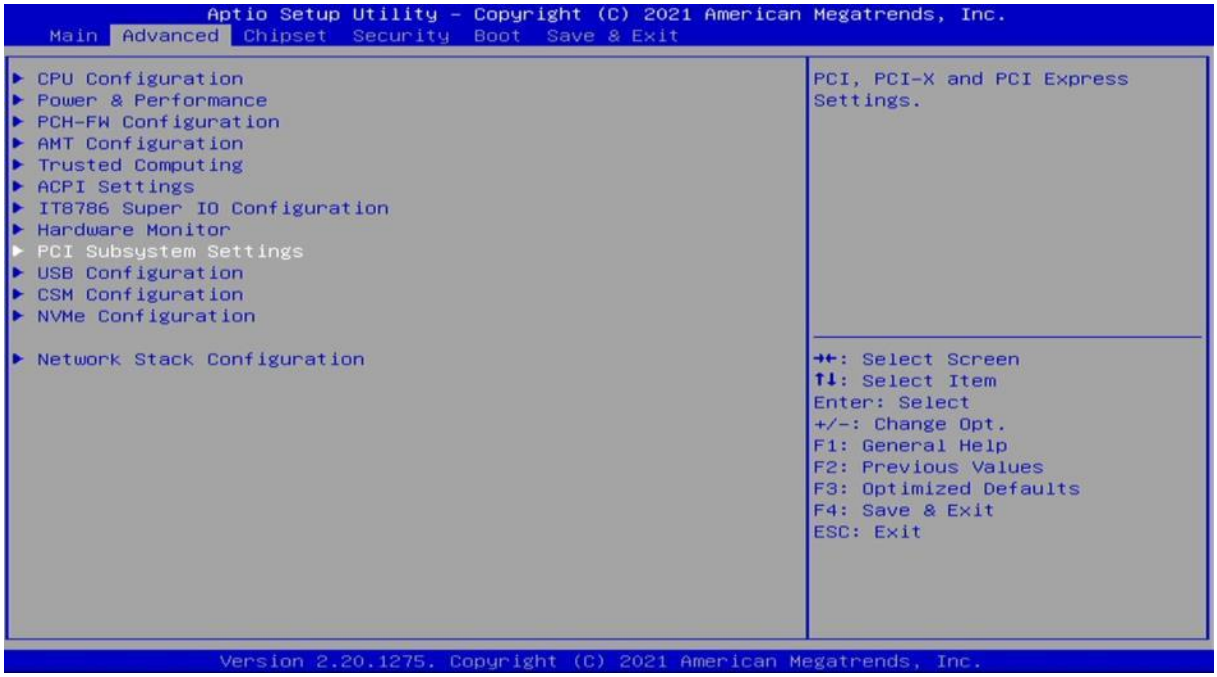
Field Name	Smart Fan Mode
Default Value	[Automatic Mode]
Possible Value	Software Mode Automatic Mode

Field Name	Smart Fan Mode
Default Value	[Automatic Mode]
Possible Value	Software Mode Automatic Mode

Field Name	System Fan Type
Default Value	[PWM]
Possible Value	PWM RPM

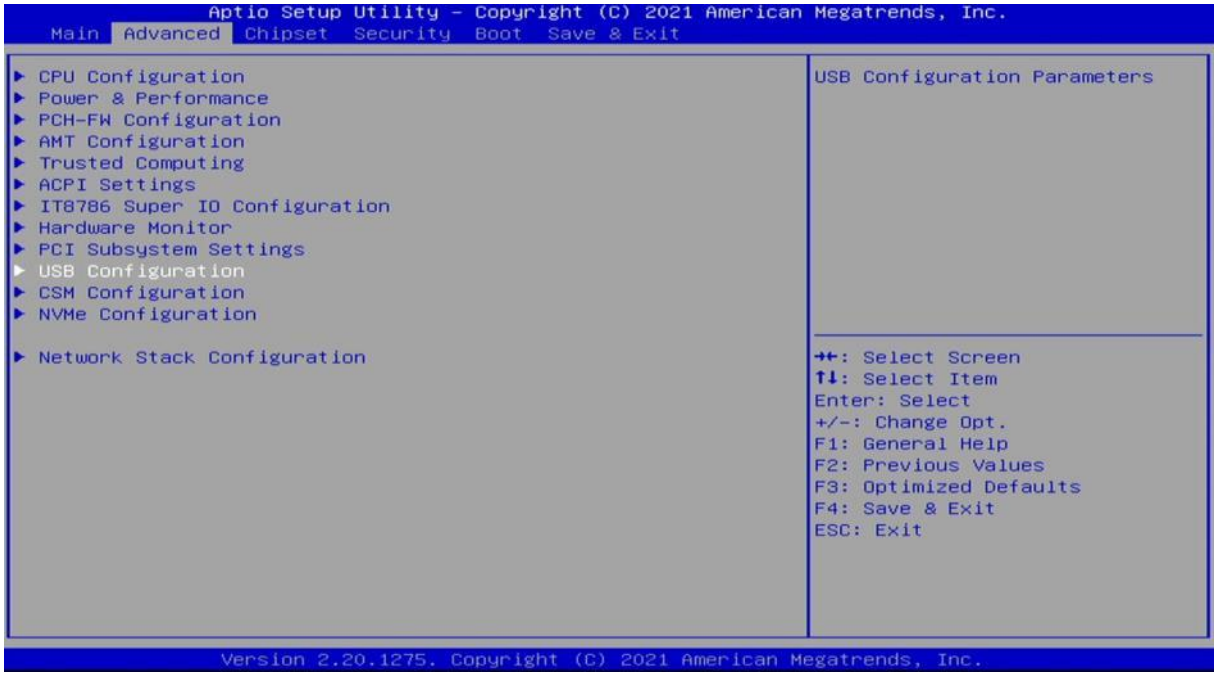
Field Name	Temperature select
Default Value	[TMP IN3]
Possible Value	TMP IN1 TMP IN2 TMP IN3

3.4.9 PCI Subsystem Settings



Field Name	Above 4G Decoding
Default Value	[Disabled]
Possible Value	Disabled Enabled

3.4.10 USB CONFIGUATION



Field Name	**Legacy USB Support**
Default Value	[Enabled]
Possible Value	Enabled Disabled Auto

Field Name	**XHCI Hand-off**
Default Value	[Enabled]
Possible Value	Enabled Disabled

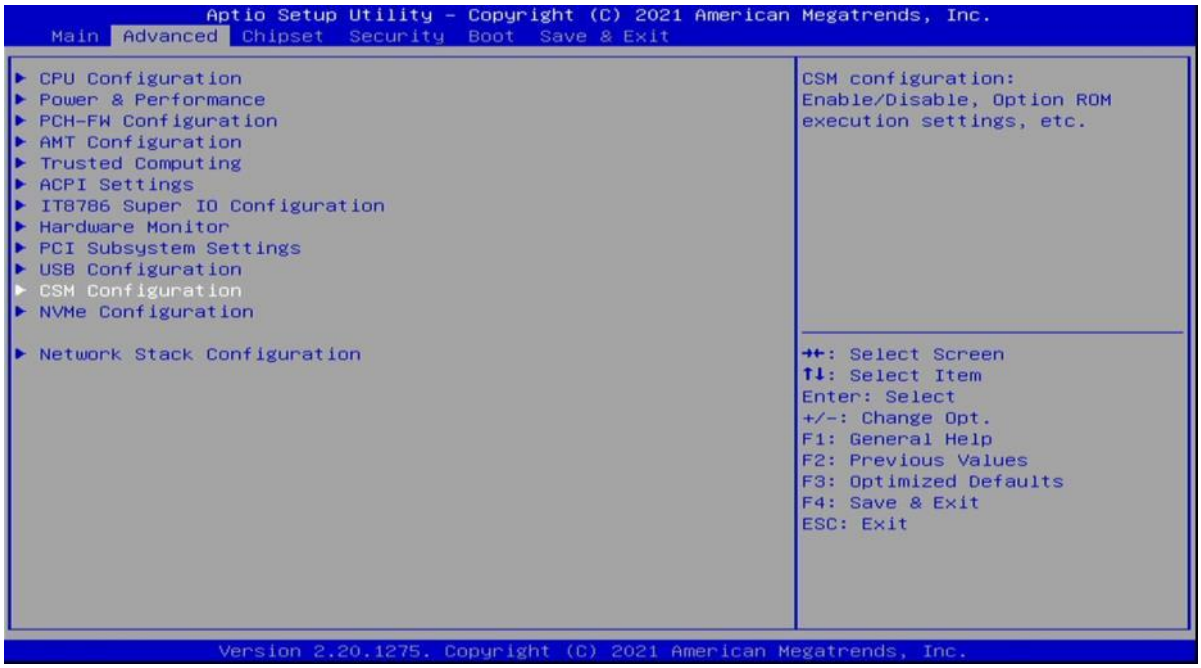
Field Name	**USB Mass Storage Driver Support**
Default Value	[Enabled]
Possible Value	Disabled Enabled

Field Name	**USB transfer time-out**
Default Value	[20 sec]
Possible Value	1 sec 5 sec 10 sec 20 sec

Field Name	Device reset time-out
Default Value	[20 sec]
Possible Value	10 sec 20 sec 30 sec 40 sec

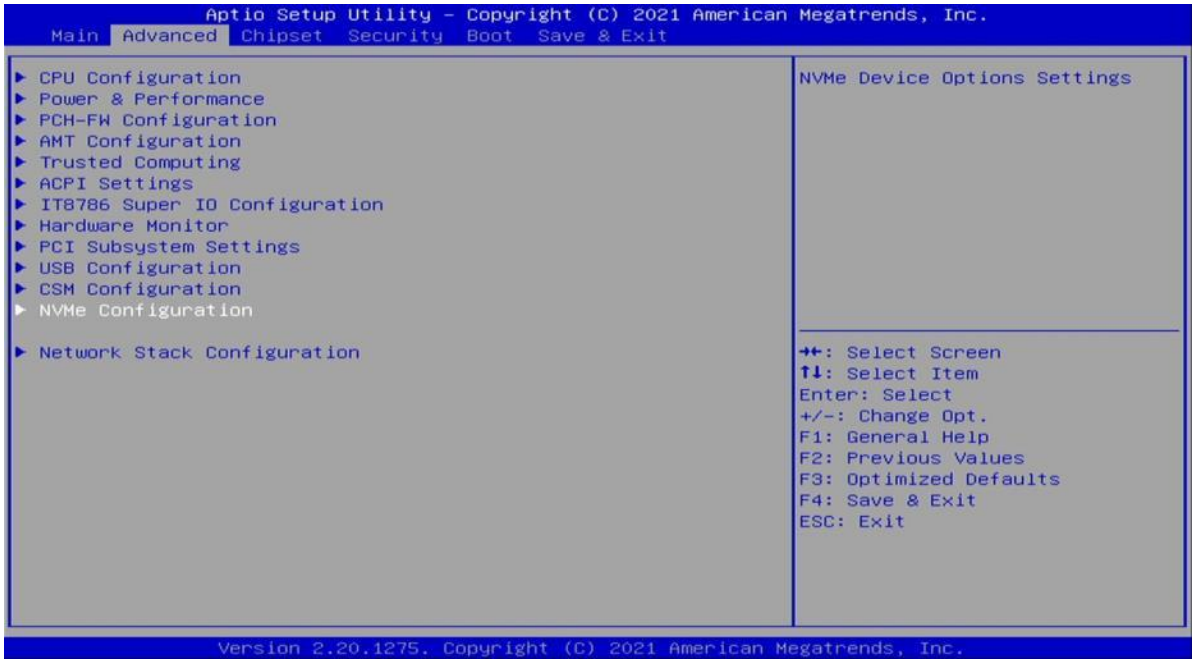
Field Name	Device power-up delay
Default Value	[Auto]
Possible Value	Auto Manual

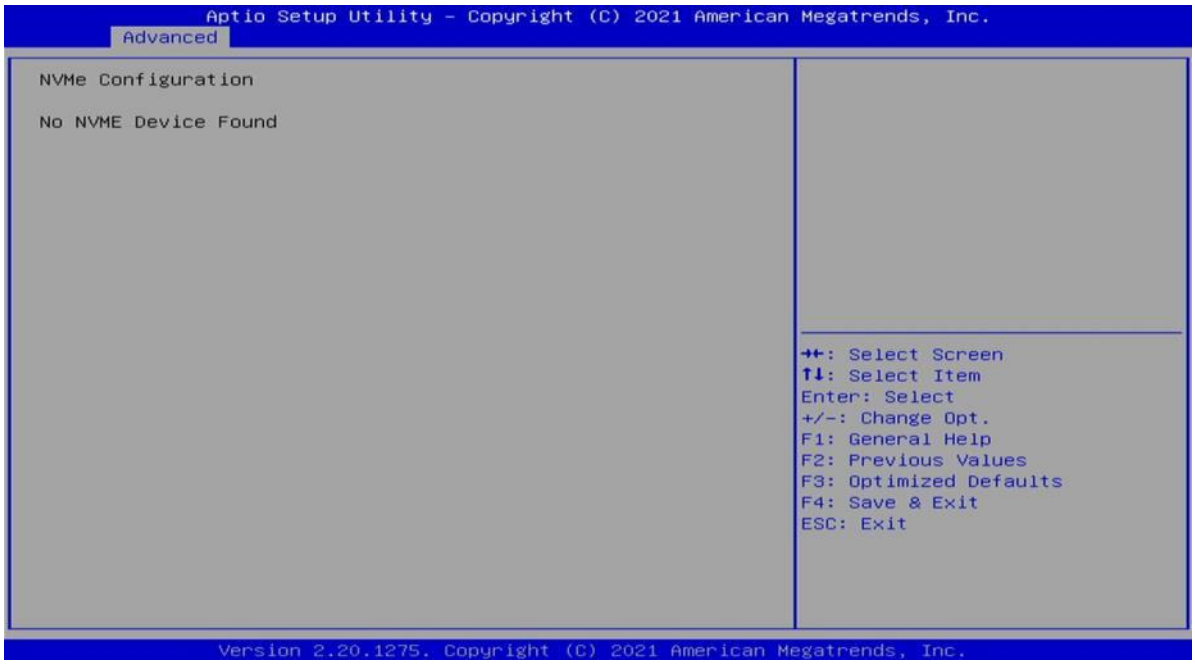
3.4.11 CSM CONFIGURATION



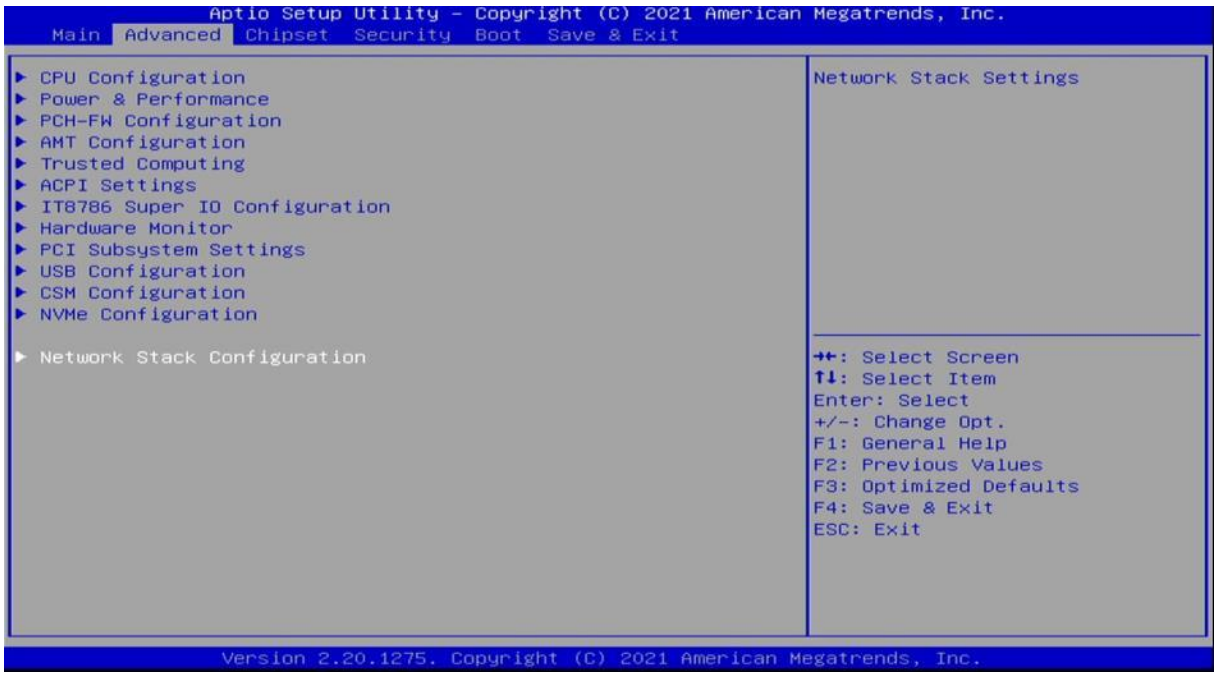
Field Name	CSM Support
Default Value	[Disabled]
Possible Value	Disabled Enabled

3.4.12 NVME CONFIGURATION





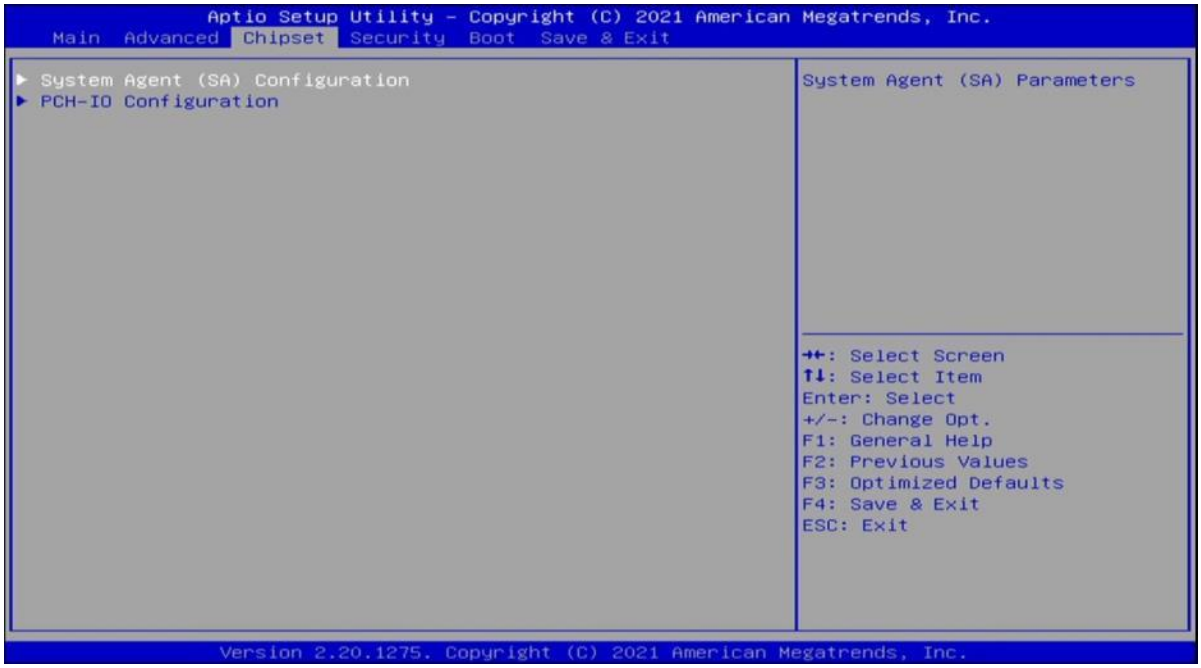
3.4.13 Network Stack Configuration

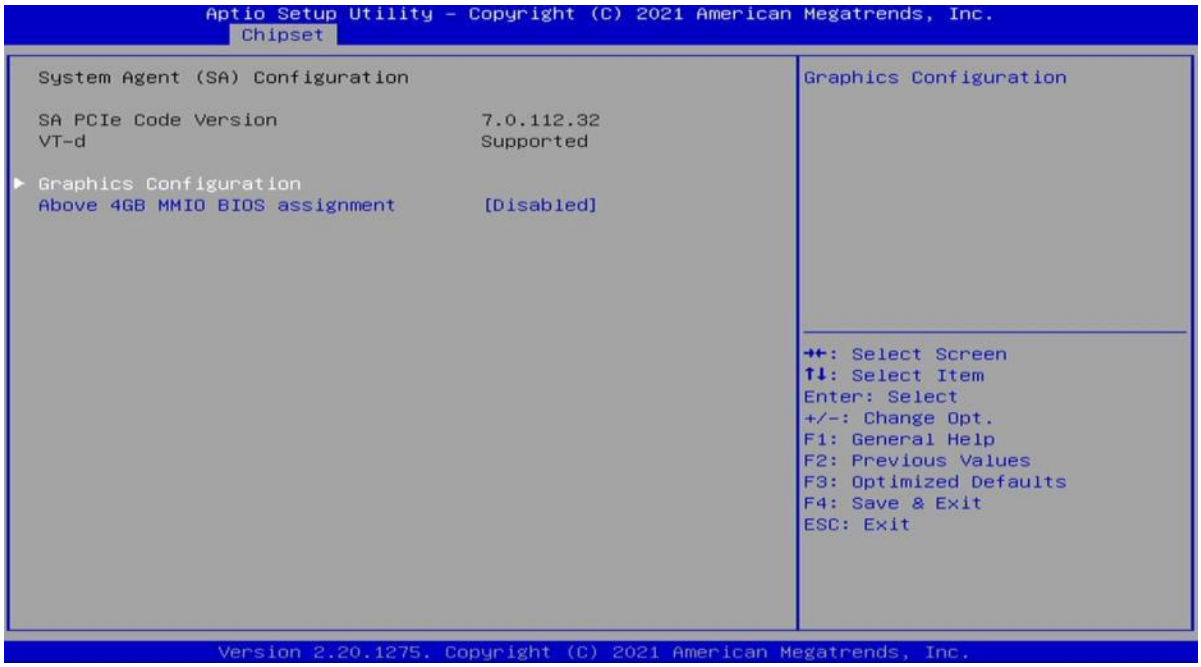


Field Name	Network Stack
Default Value	[Disabled]
Possible Value	Disabled Enabled

3.5 CHIPSET

3.5.1 SYSTEM AGENT (SA) CONFIGURATION





Field Name	Primary Display
Default Value	[Auto]
Possible Value	Auto IGFX PEG PCI SG

Field Name	Internal Graphics
Default Value	[Auto]
Possible Value	Auto Disabled Enabled

Field Name	GTT Size
Default Value	[8MB]
Possible Value	2MB 4MB 8MB

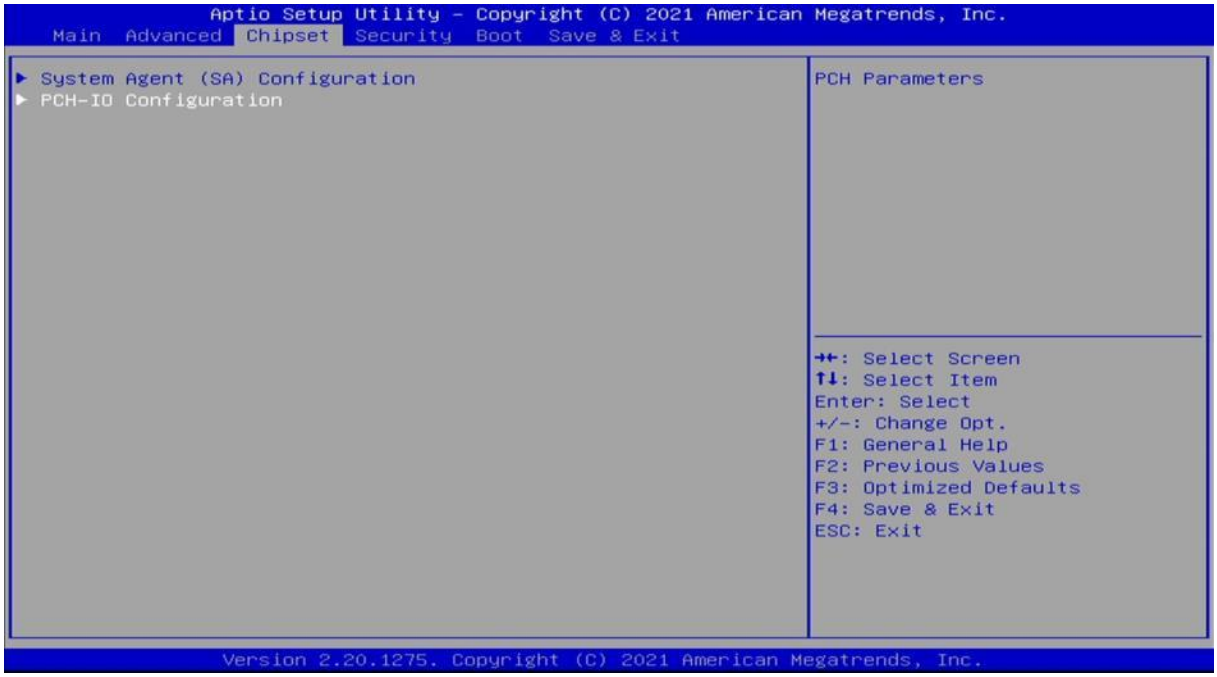
Field Name	Aperture Size
Default Value	[256MB]
Possible Value	128MB 256MB 512MB 1024MB 2048MB

Field Name	DVMT Pre-Allocated
Default Value	[32M]
Possible Value	0M 32M 64M 4M 8M 12M 16M 20M 24M 28M 32M/F7 36M 40M 44M 48M 52M 56M 60M

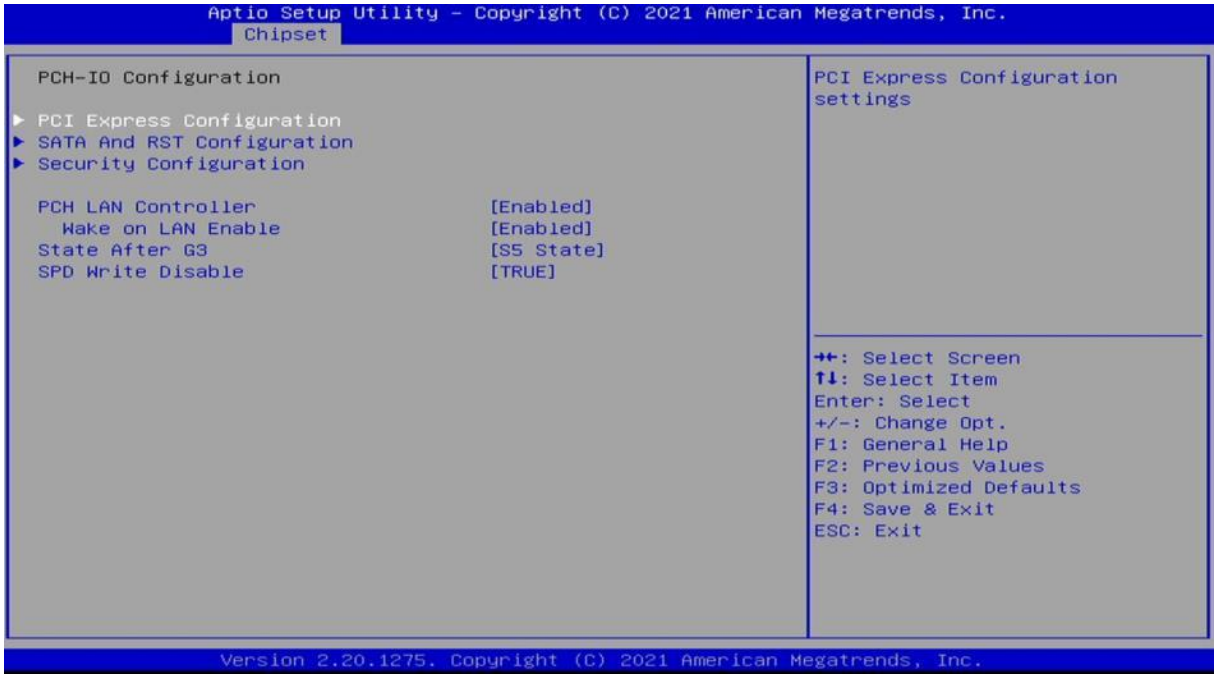
Field Name	DVMT Total Gfx Mem
Default Value	[128M]
Possible Value	128M 256M MAX

Field Name	Above 4GB MMIO BIOS assignment
Default Value	[Enabled]
Possible Value	Enabled Disabled

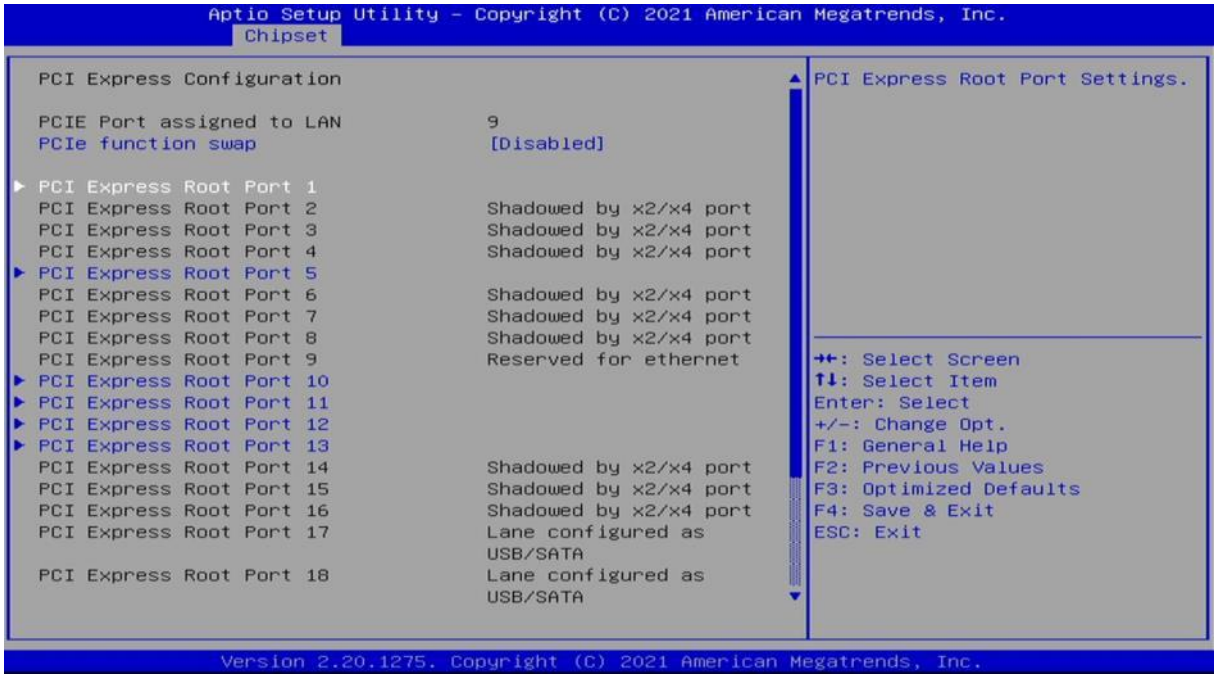
3.5.2 PCH-IO CONFIGURATION

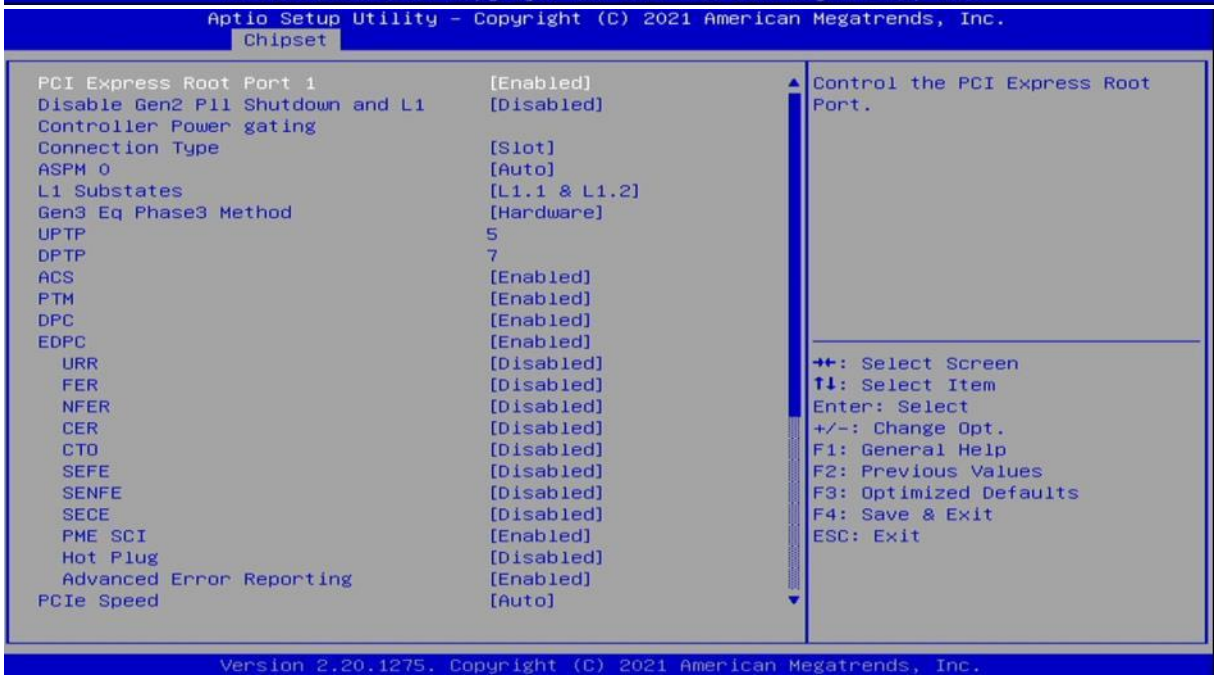


3.5.2.1 PCI EXPRESS CONFIGURATION



Field Name	PCIe function swap
Default Value	[Disabled]
Possible Value	Disabled Enabled





Field Name	**PCI Express Root Port 1**
Default Value	[Enabled]

Field Name	**PCI Express Root Port 5**
Default Value	[Enabled]

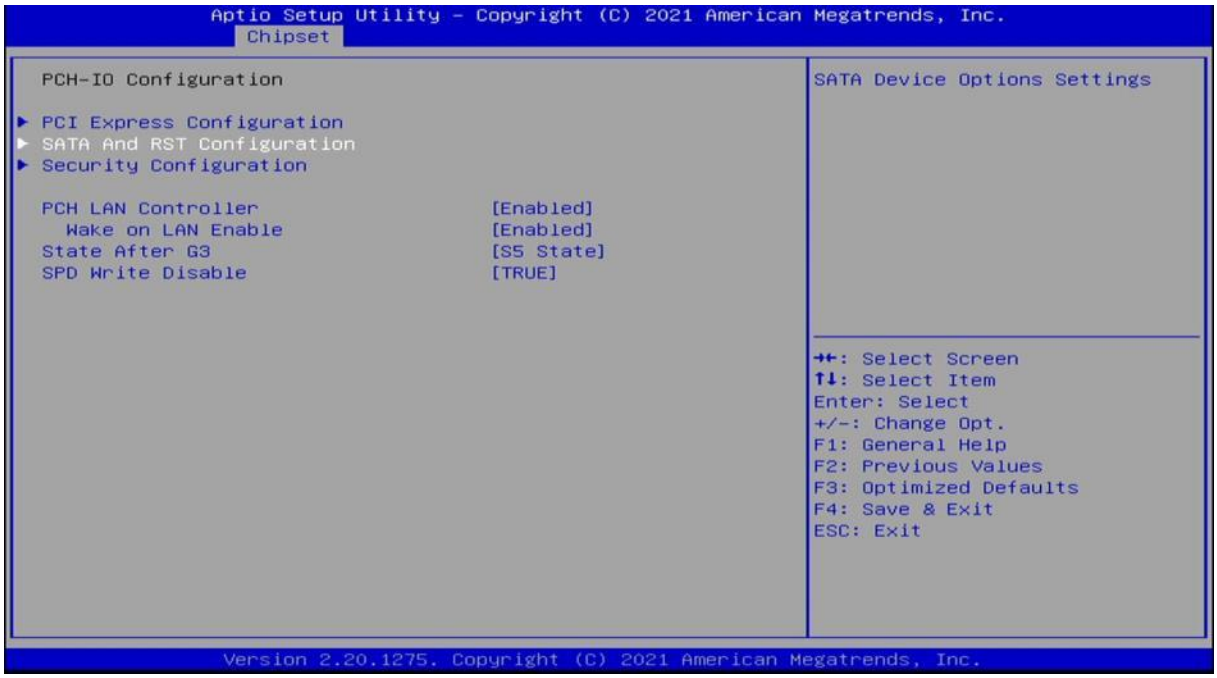
Field Name	**PCI Express Root Port 10**
Default Value	[Enabled]

Field Name	PCI Express Root Port 11
Default Value	[Enabled]

Field Name	PCI Express Root Port 12
Default Value	[Enabled]

Field Name	PCI Express Root Port 13
Default Value	[Enabled]

3.5.2.2 SATA AND RST CONFIGURATION



Field Name	SATA Controller(s)
Default Value	[Enabled]
Possible Value	Enabled Disabled

Field Name	SATA Mode Selection
Default Value	[AHCI]
Possible Value	AHCI

Field Name	M.2 Port
Default Value	[Disabled]
Possible Value	Disabled Enabled

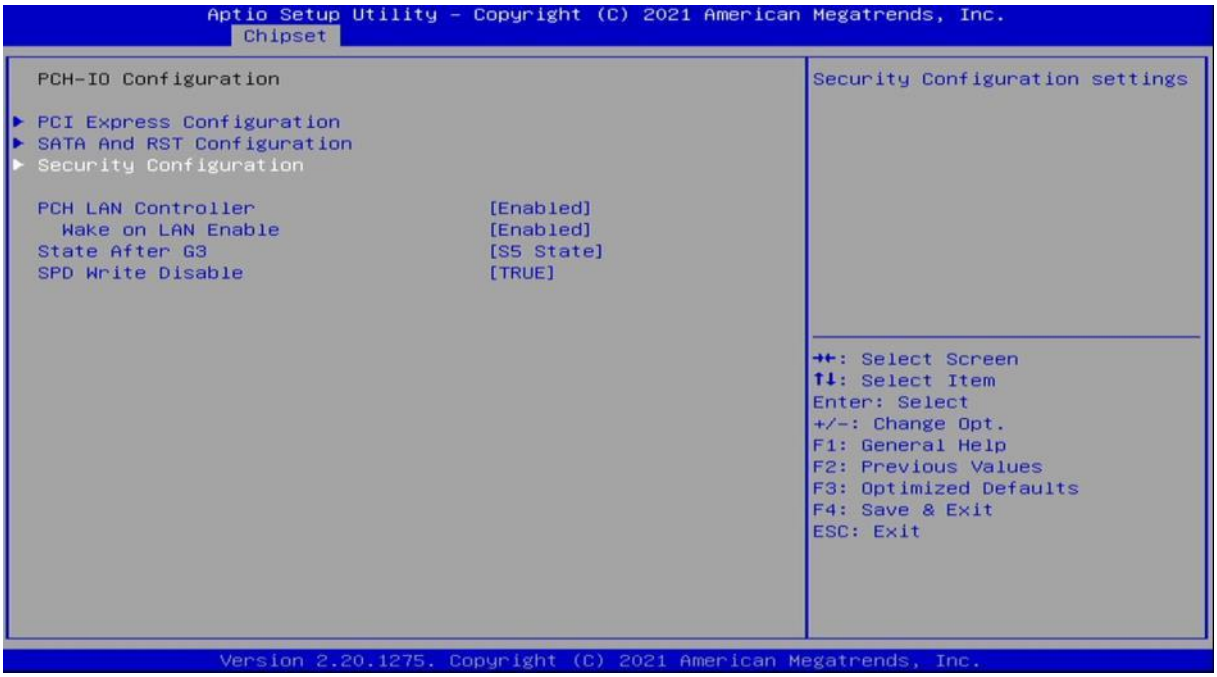
Field Name	Port 1
Default Value	[Enabled]
Possible Value	Disabled Enabled

Field Name	Port 2
Default Value	[Enabled]
Possible Value	Disabled Enabled

Field Name	Port 3
Default Value	[Enabled]
Possible Value	Disabled Enabled

Field Name	Port 4
Default Value	[Enabled]
Possible Value	Disabled Enabled

3.5.2.3 SECURITY CONFIGURATION



Field Name	**RTC Memory Lock**
Default Value	[Enabled]
Possible Value	Disabled Enabled

Field Name	**BIOS Lock**
Default Value	[Enabled]
Possible Value	Disabled Enabled

Field Name	**Force unlock on all GPIO pads**
Default Value	[Enabled]
Possible Value	Disabled Enabled

Field Name	**PCH LAN Controller**
Default Value	[Enabled]
Possible Value	Disabled Enabled

Field Name	**Wake on LAN Enable**
Default Value	[Enabled]

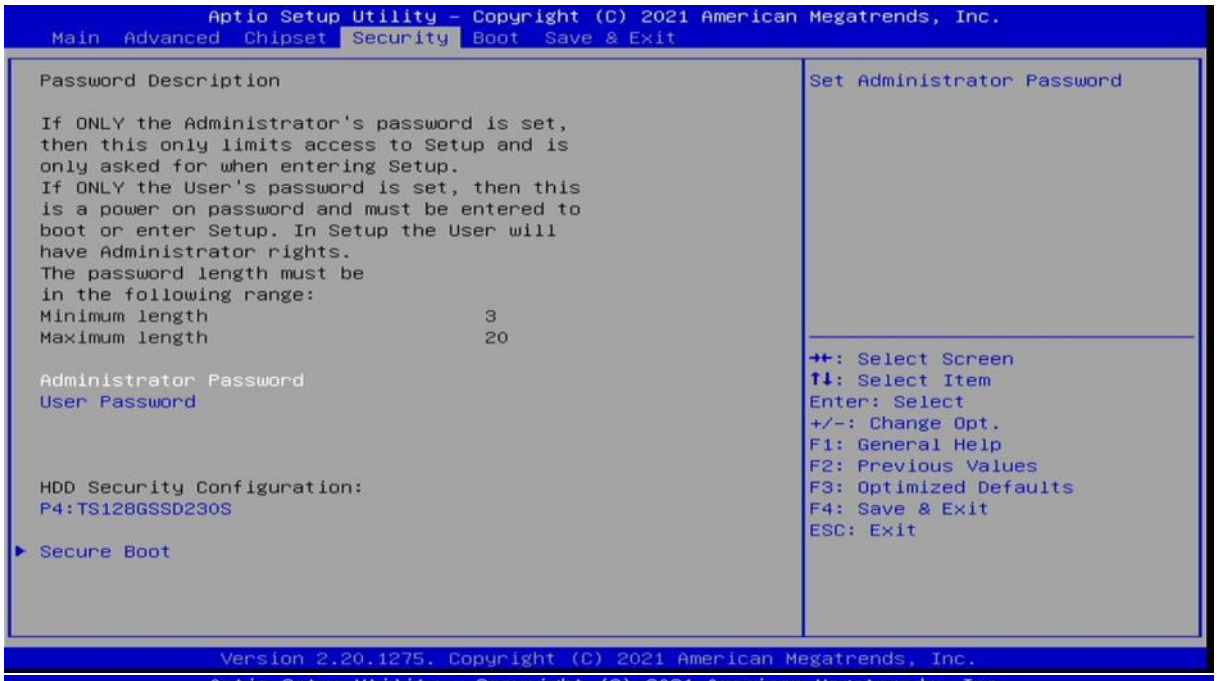
Possible Value	Disabled Enabled

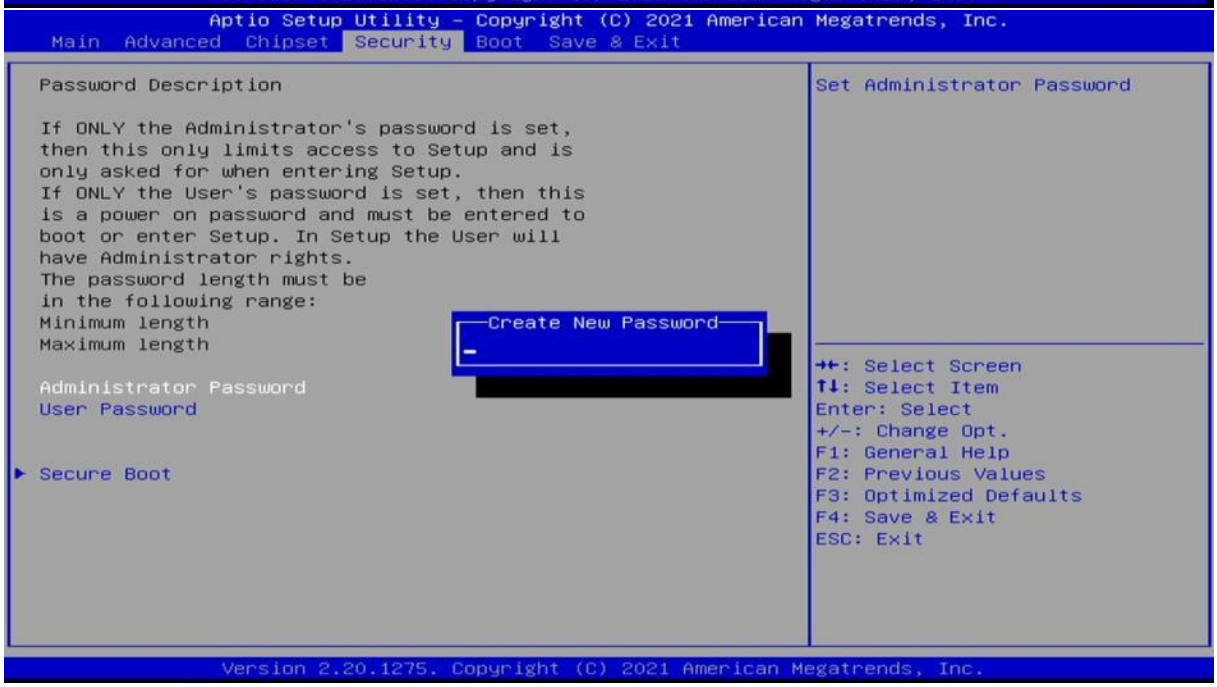
Field Name	**State After G3**
Default Value	[S5 State]
Possible Value	S0 State S5 State

Field Name	**SPD Write Disable**
Default Value	[TRUE]
Possible Value	TRUE FALSE

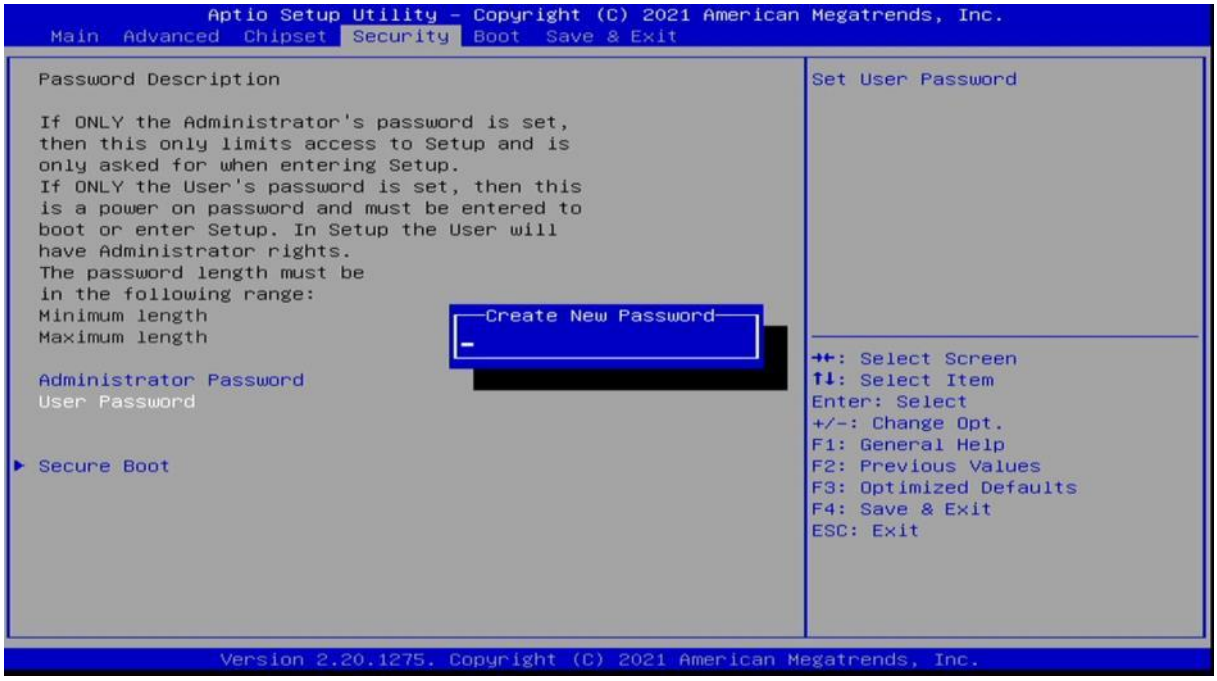
3.6 SECURITY

3.6.1 ADMINISTRATOR PASSWORD

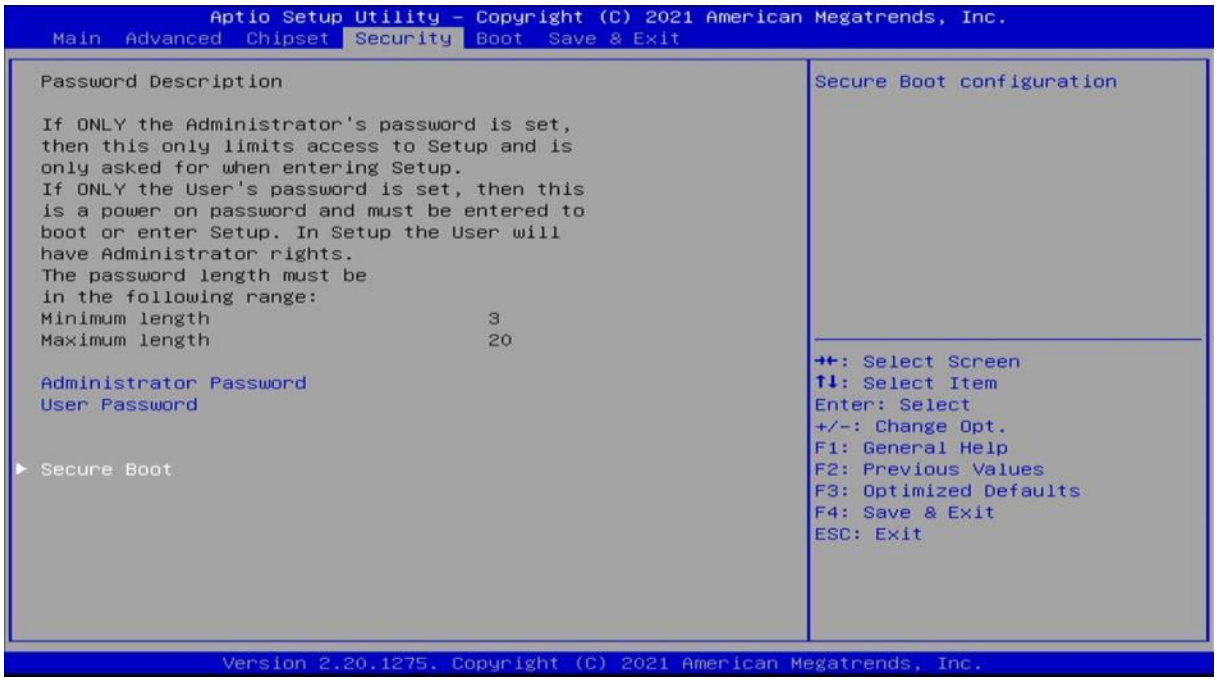




3.6.2 User Password



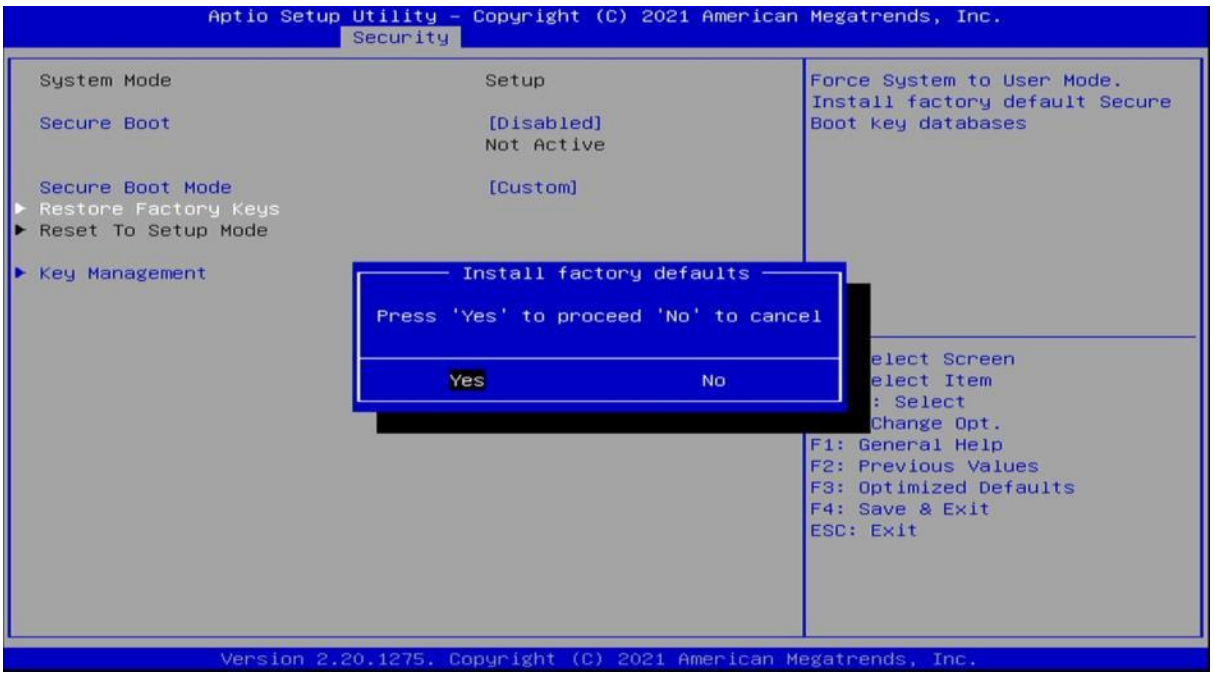
3.6.3 Secure Boot



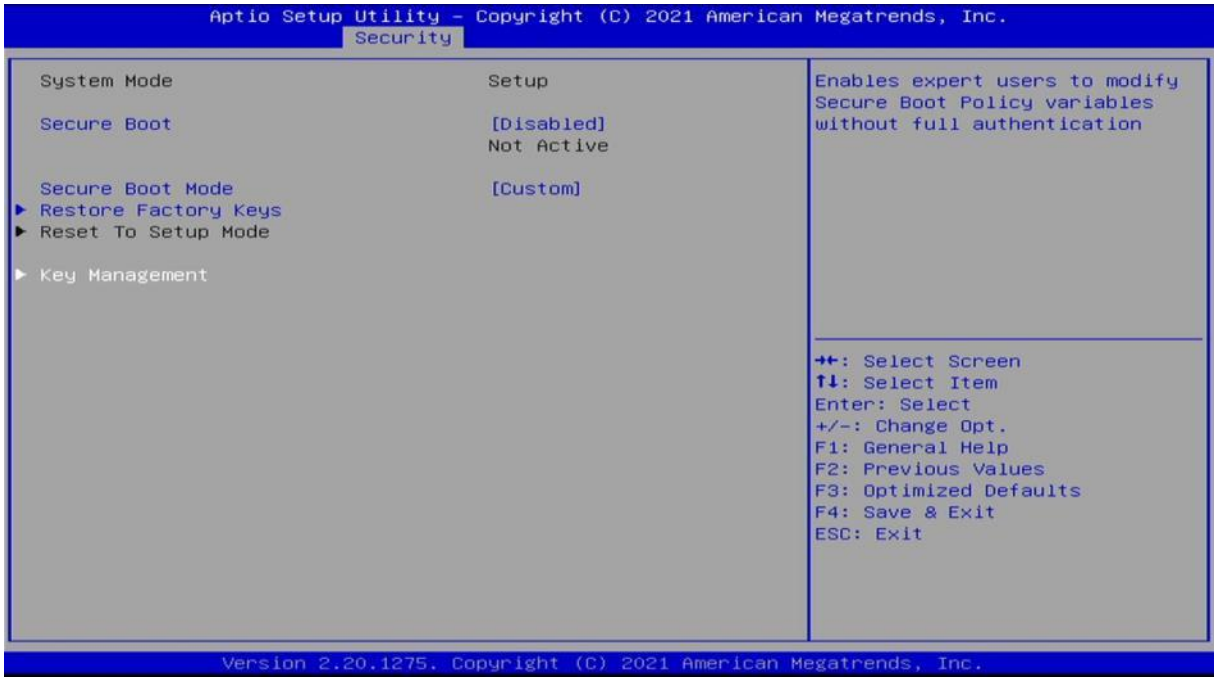
Field Name	**Secure Boot**
Default Value	[Disabled]
Possible Value	Disabled Enabled

Field Name	Secure Boot Mode
Default Value	[Custom]
Possible Value	Standard Custom

3.6.3.1 RESTORE FACTORY KEYS

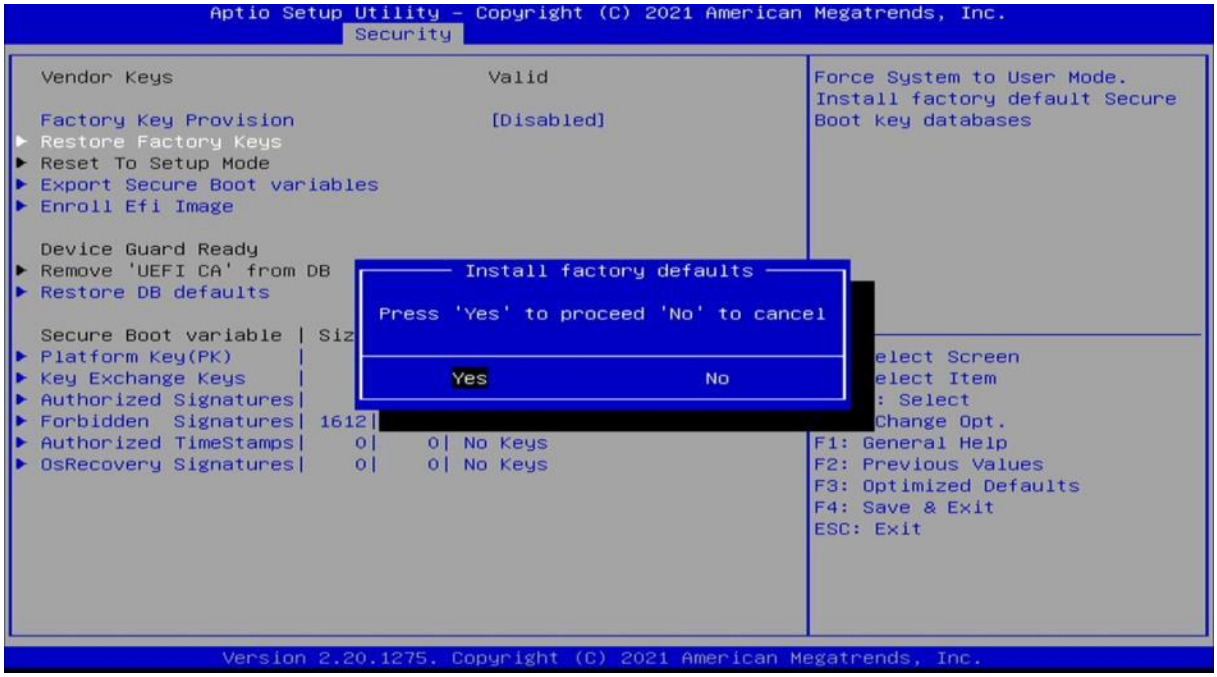


3.6.3.2 KEY MANAGEMENT

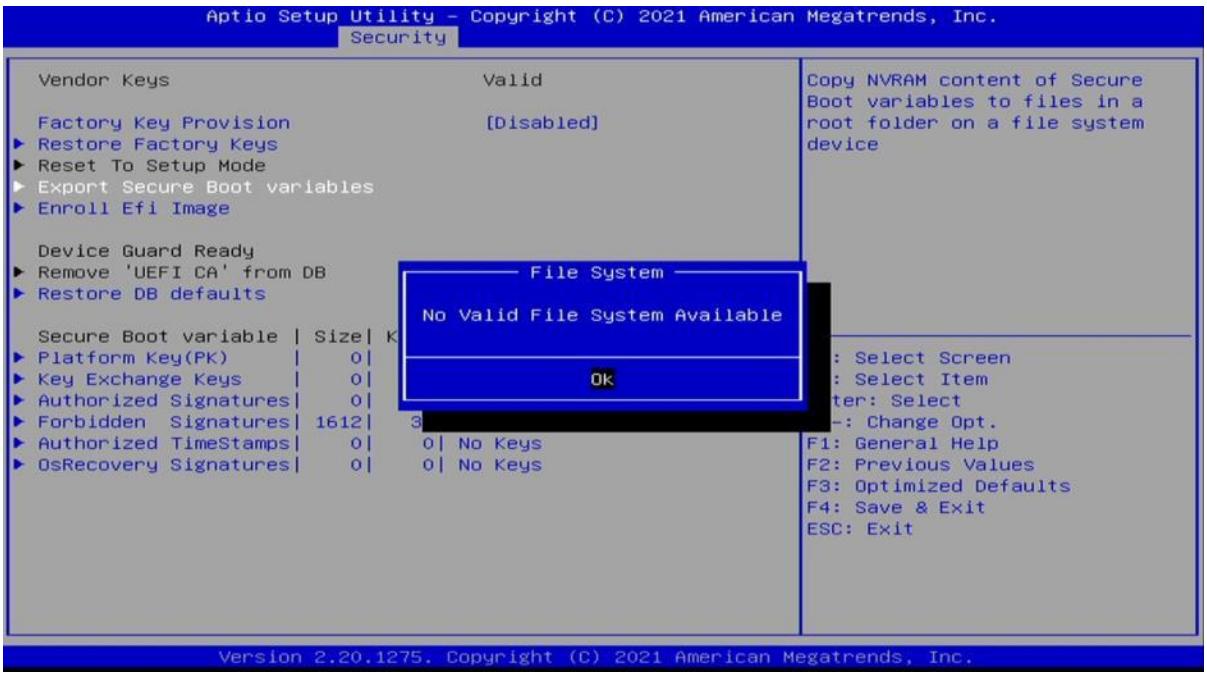


Field Name	Factory Key Provision
Default Value	[Disabled]
Possible Value	Disabled Enabled

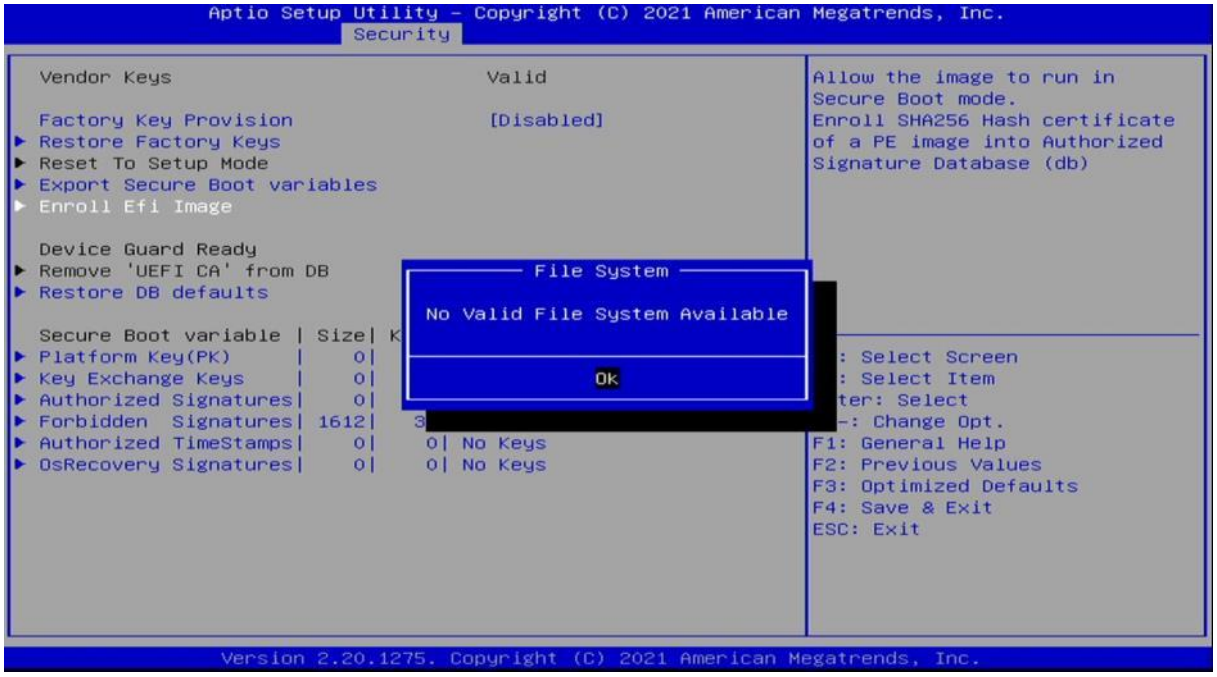
3.6.3.3 INSTALL FACTORY DEFAULTS



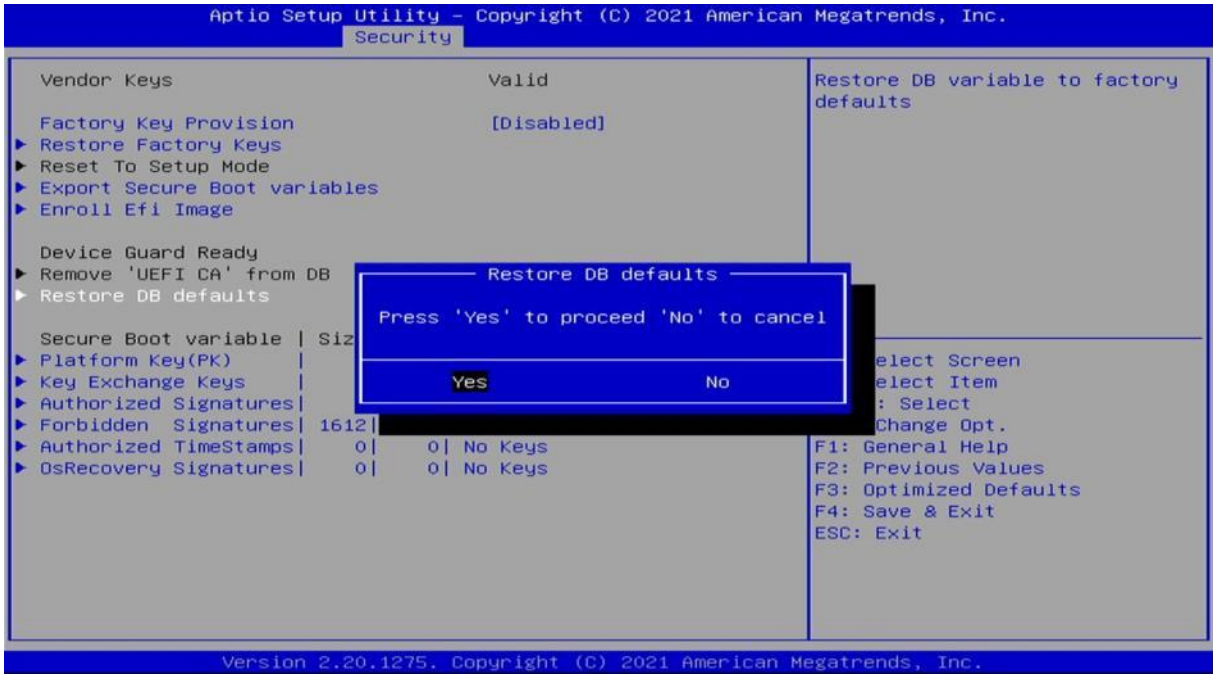
3.6.3.4 FILE SYSTEM



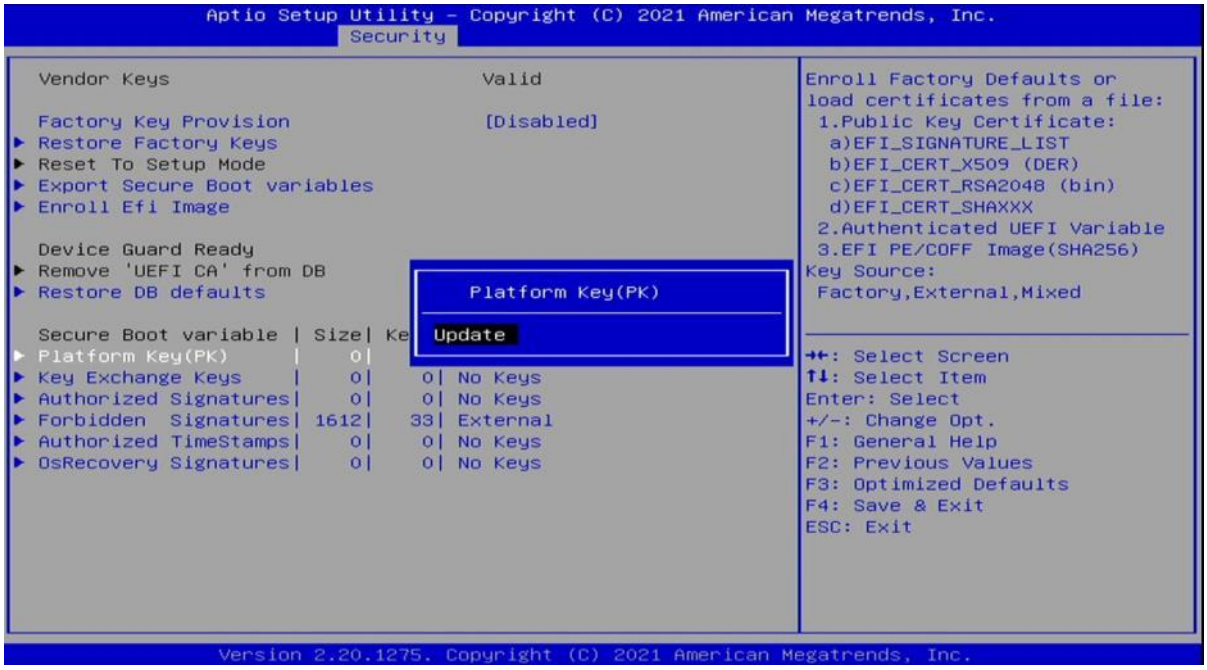
3.6.3.5 FILE SYSTEM



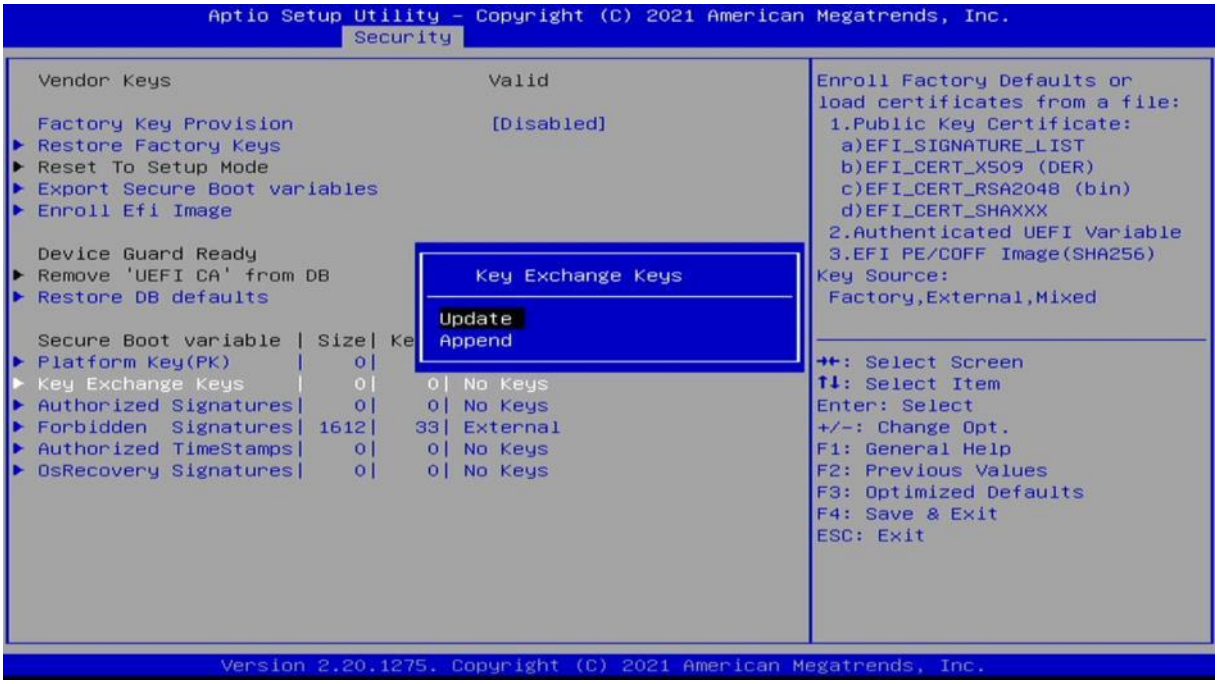
3.6.3.6 RESTORE DB DEFAULTS



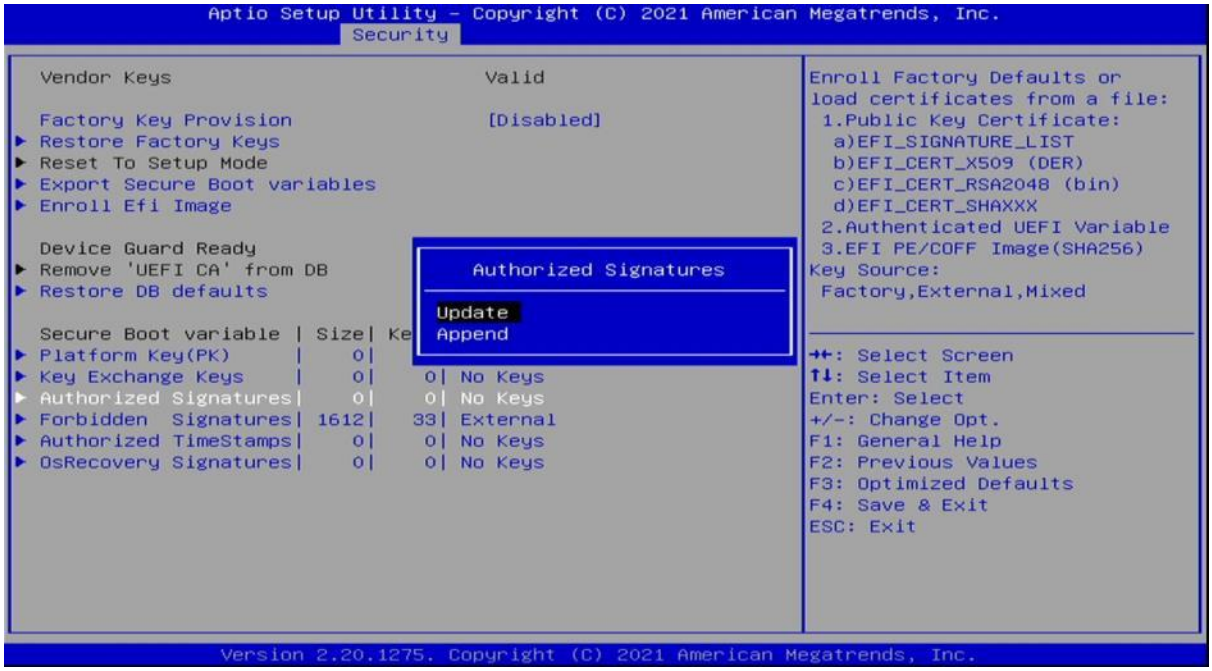
3.6.3.7 PLATFORM KEY(PK)



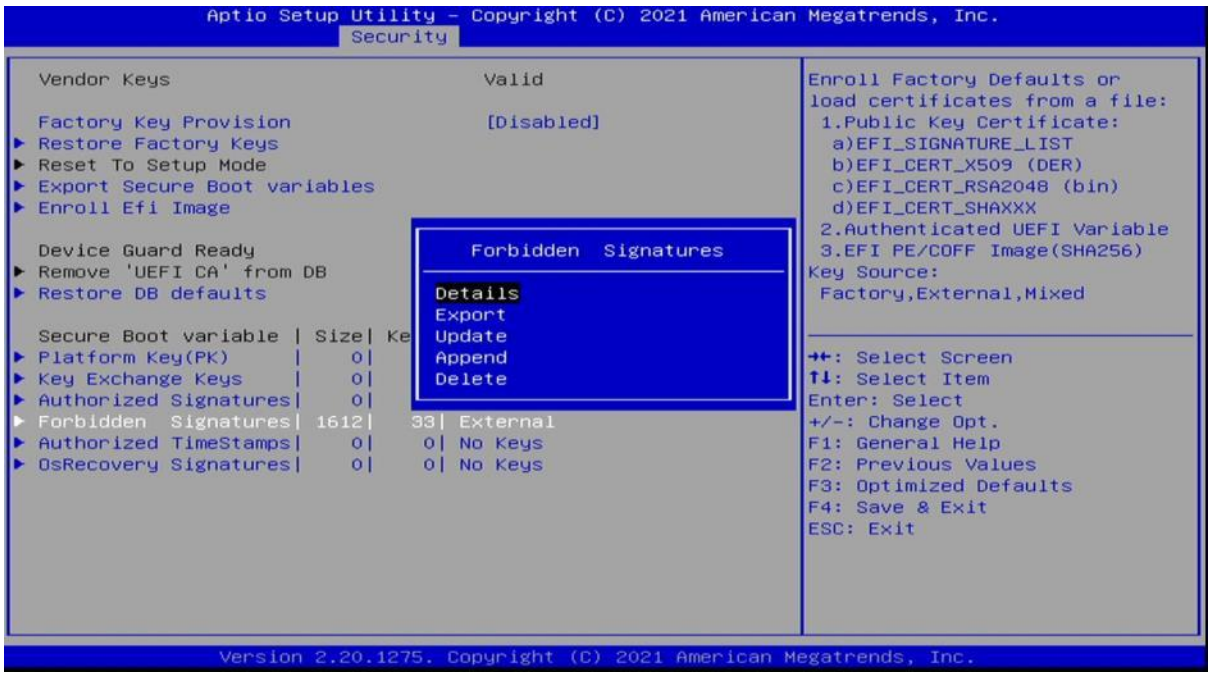
3.6.3.8 KEY EXCHANGE KEYS



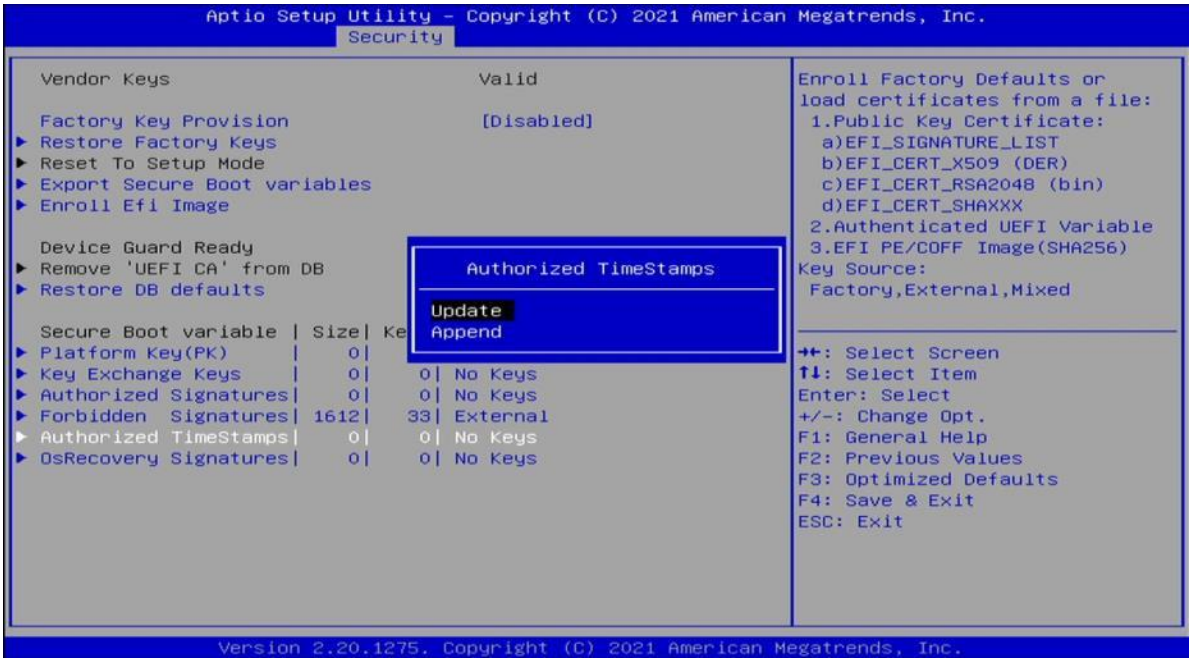
3.6.3.9 AUTHORIZED SIGNATURES



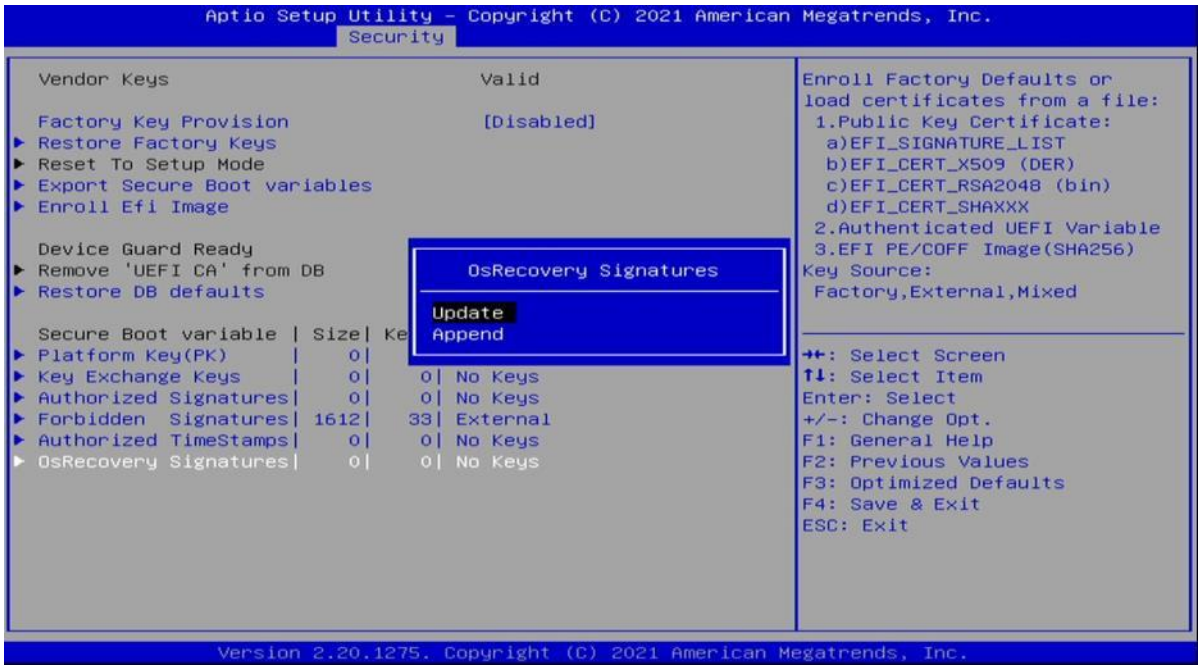
3.6.3.10 FORBIDDEN SIGNATURES



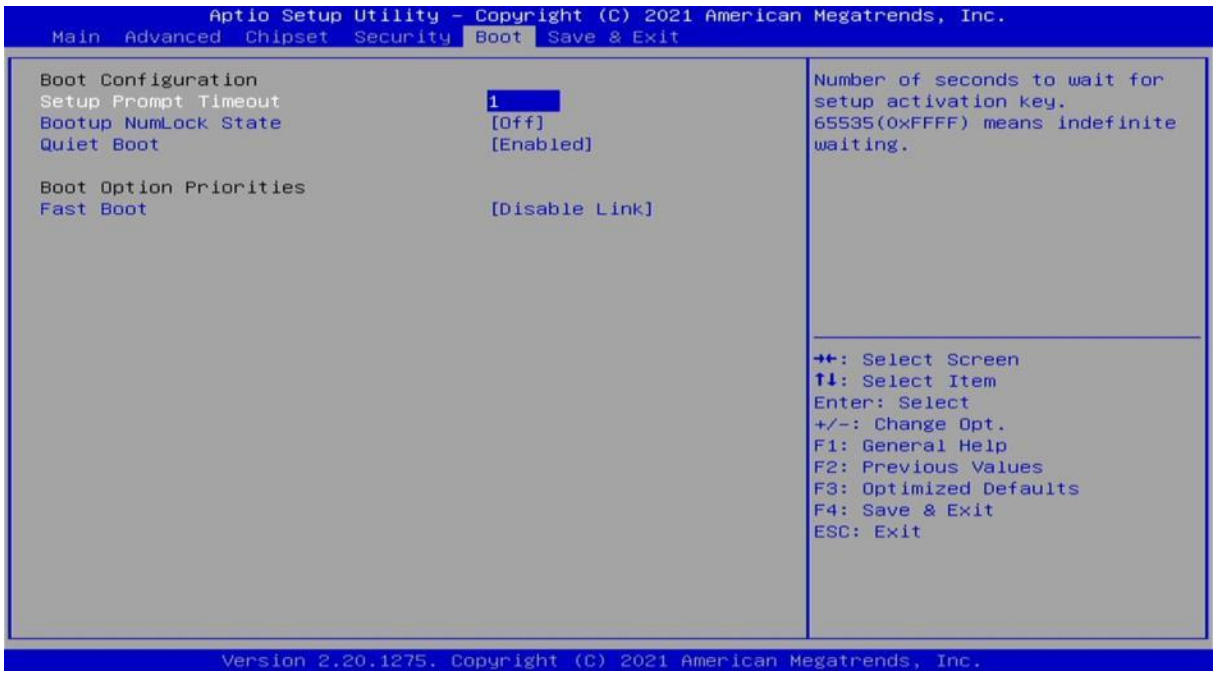
3.6.3.11 AUTHORIZED TIMESTAMPS



3.6.3.12 OsRecovery Signatures



3.7 Boot



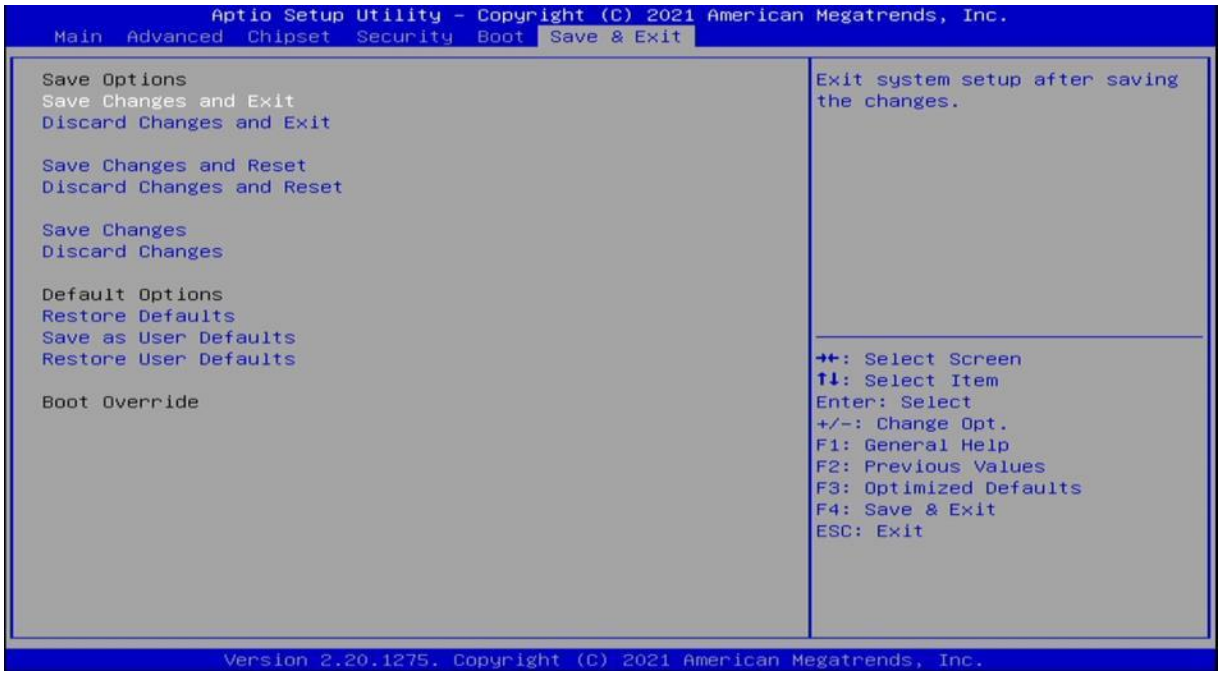
Field Name	**Bootup NumLock State**
Default Value	[Off]
Possible Value	On Off

Field Name	**Quiet Boot**
Default Value	[Enabled]
Possible Value	Disabled Enabled

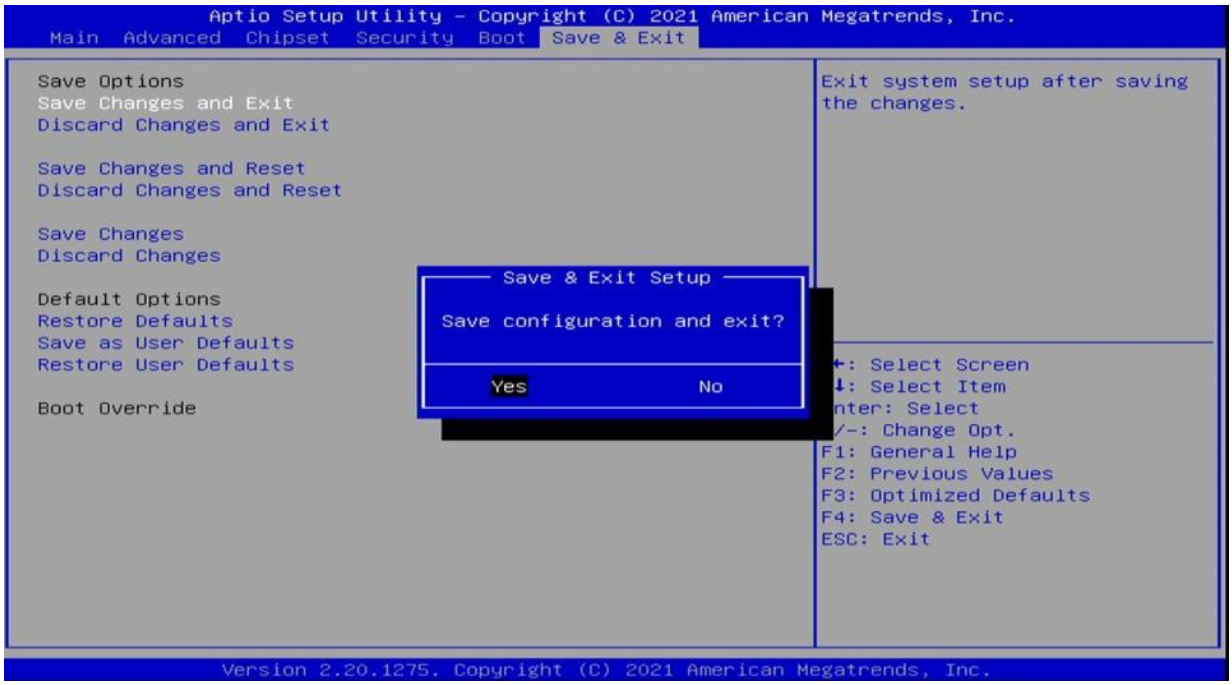
Field Name	**Fast Boot**
Default Value	[Disable Link]
Possible Value	Disable Link Enabled

3.8 SAVE & EXIT

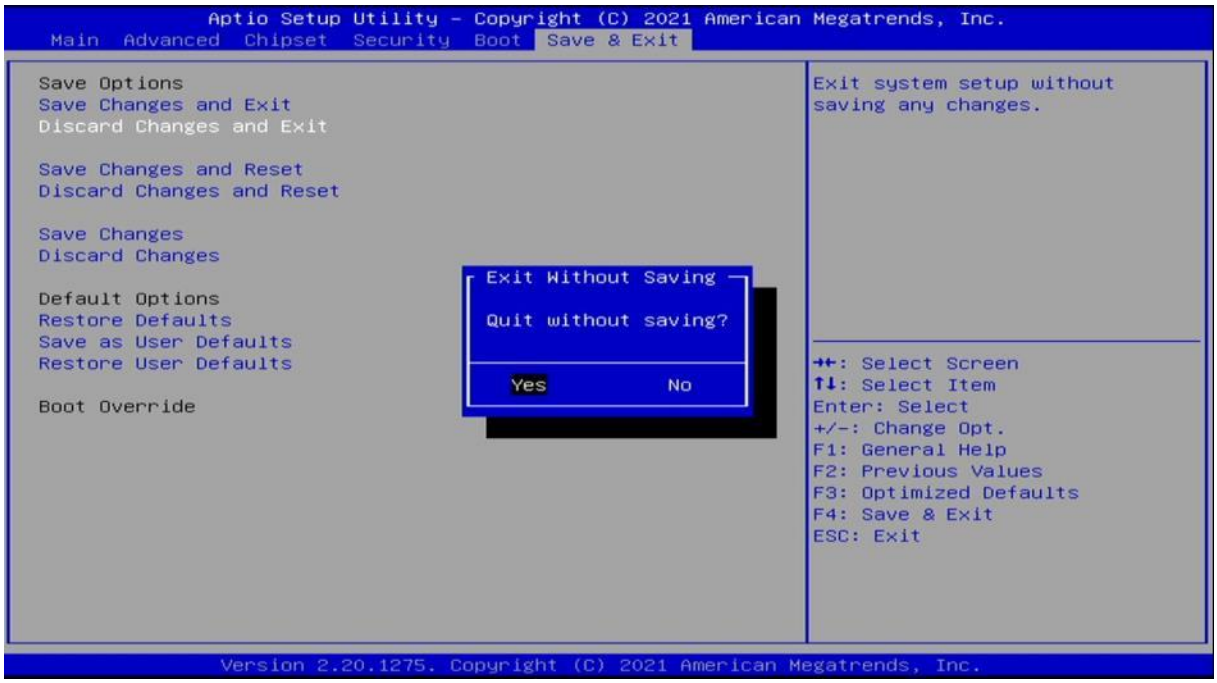
3.8.1 SAVE CHANGES AND EXIT



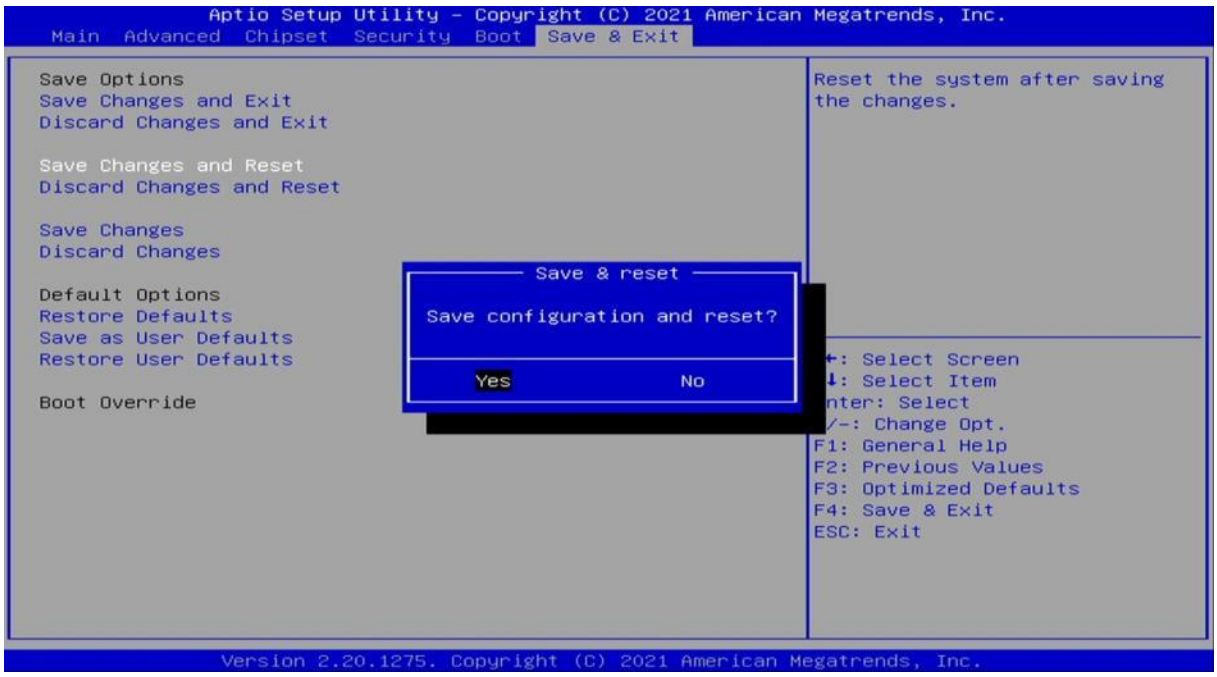
3.8.1.1 SAVE & EXIT SETUP



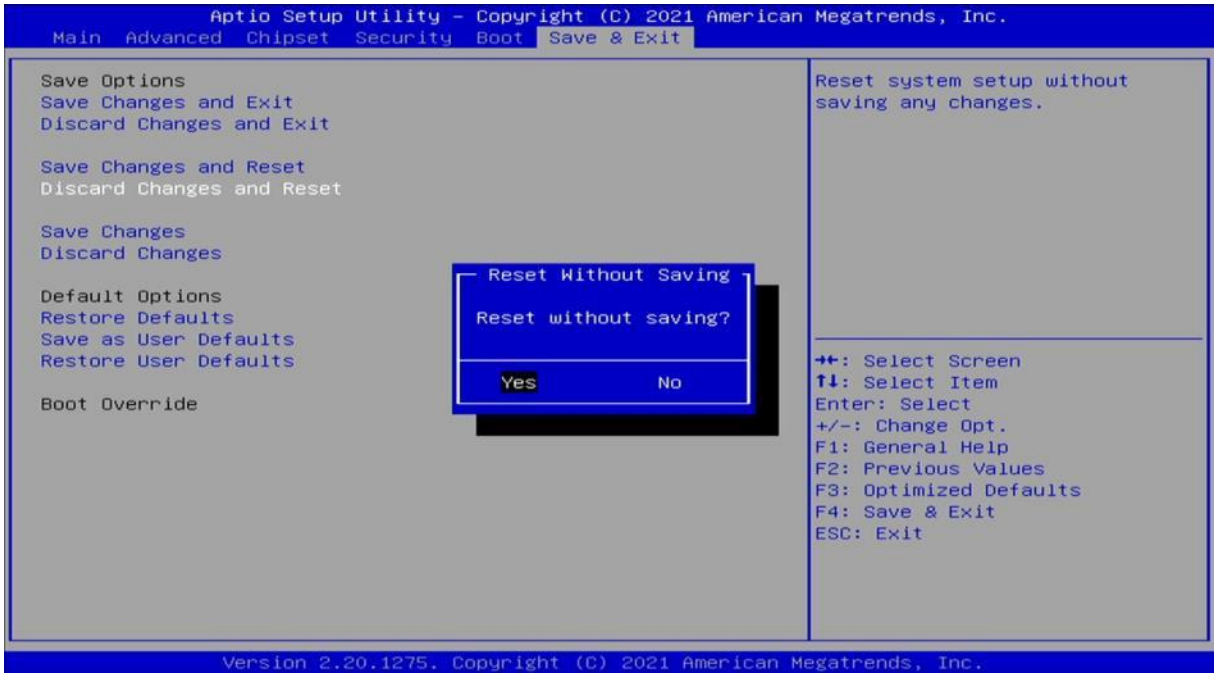
3.8.2 EXIT WITHOUT SAVING



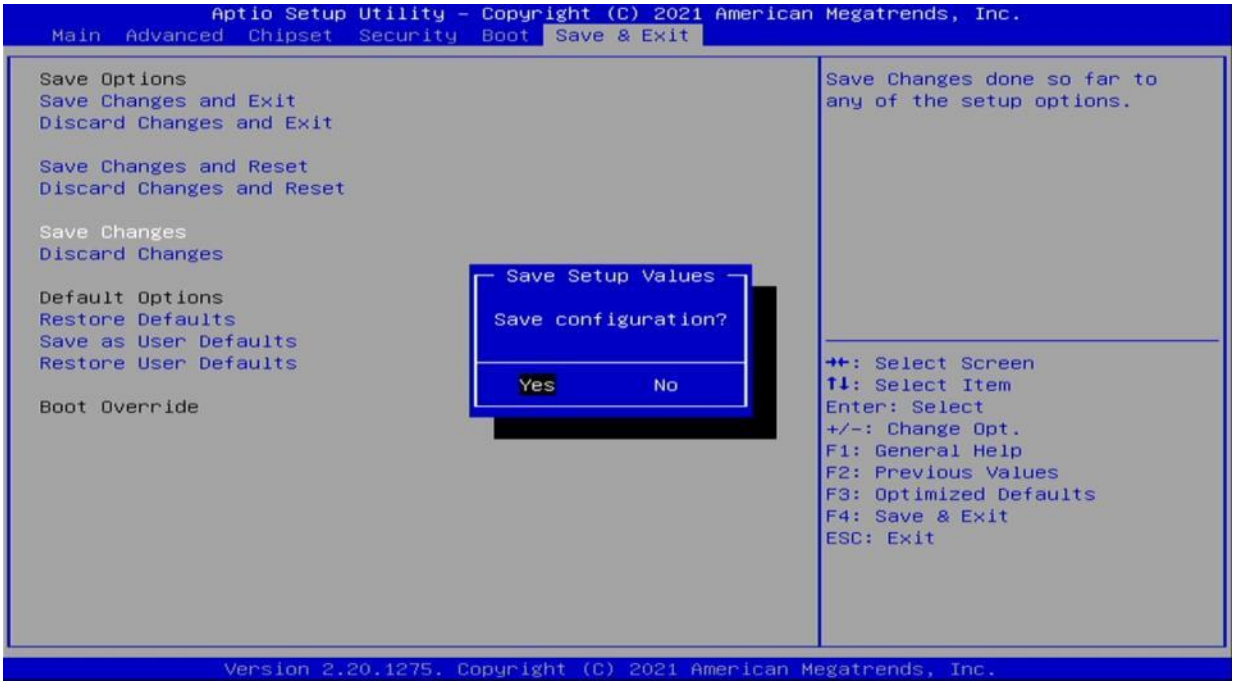
3.8.3 SAVE & RESET



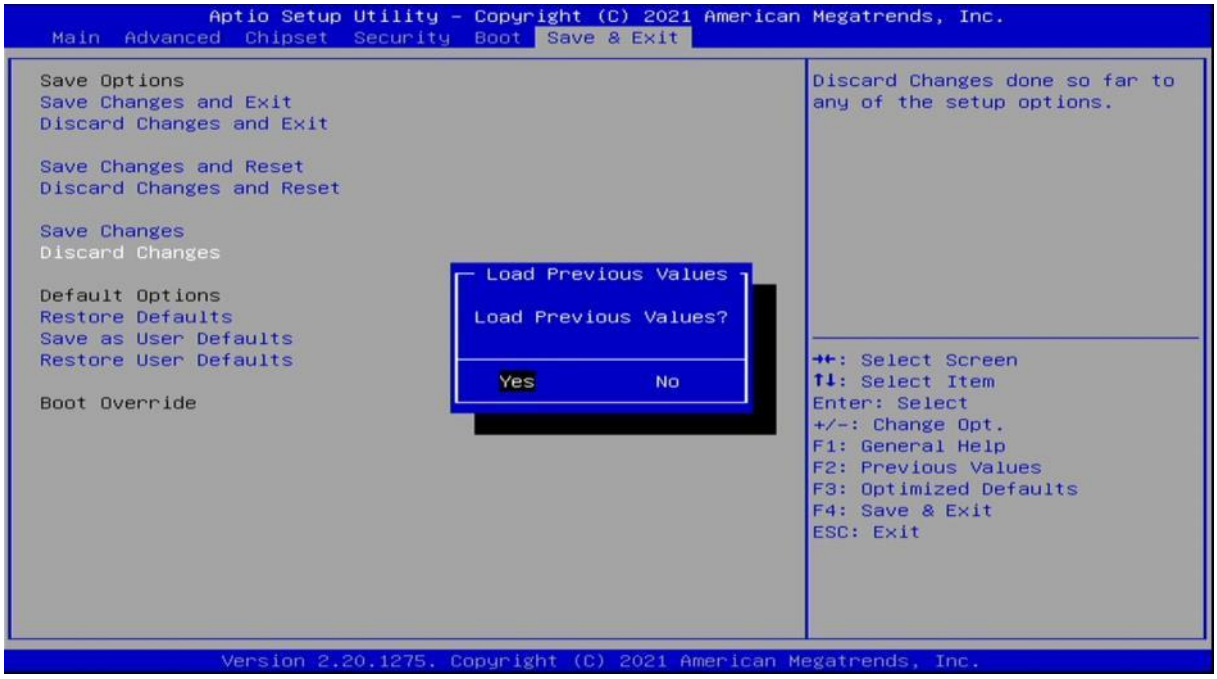
3.8.4 Reset Without Saving



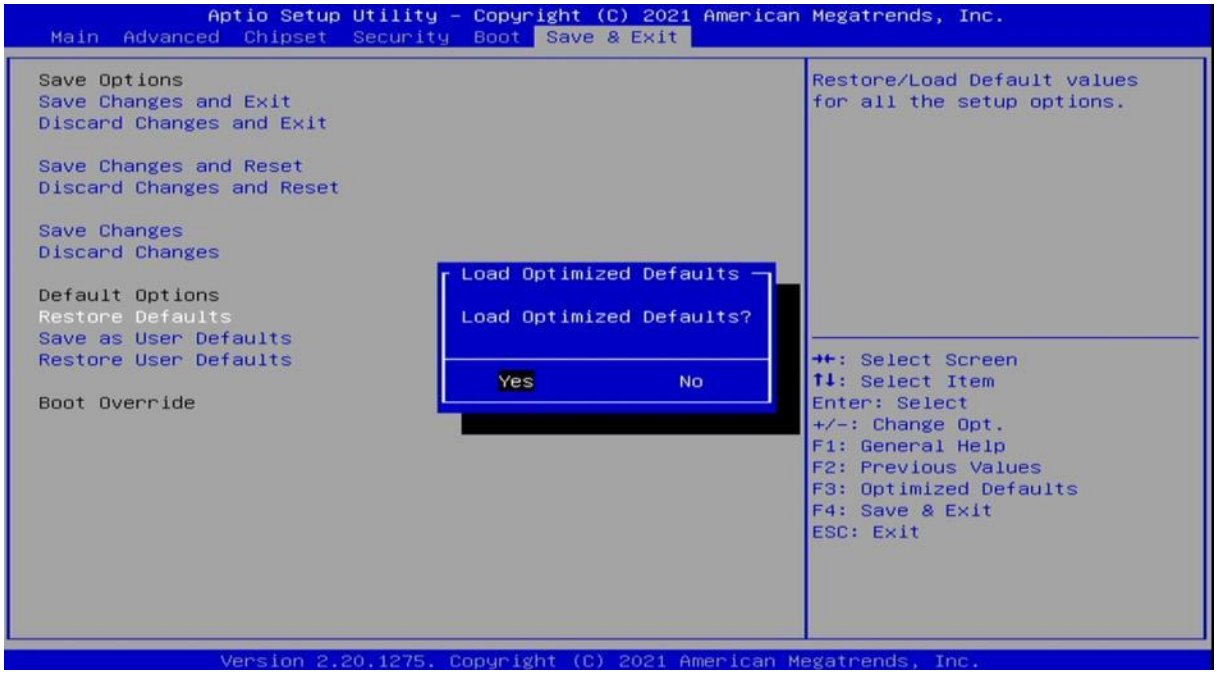
3.8.5 Save Setup Values



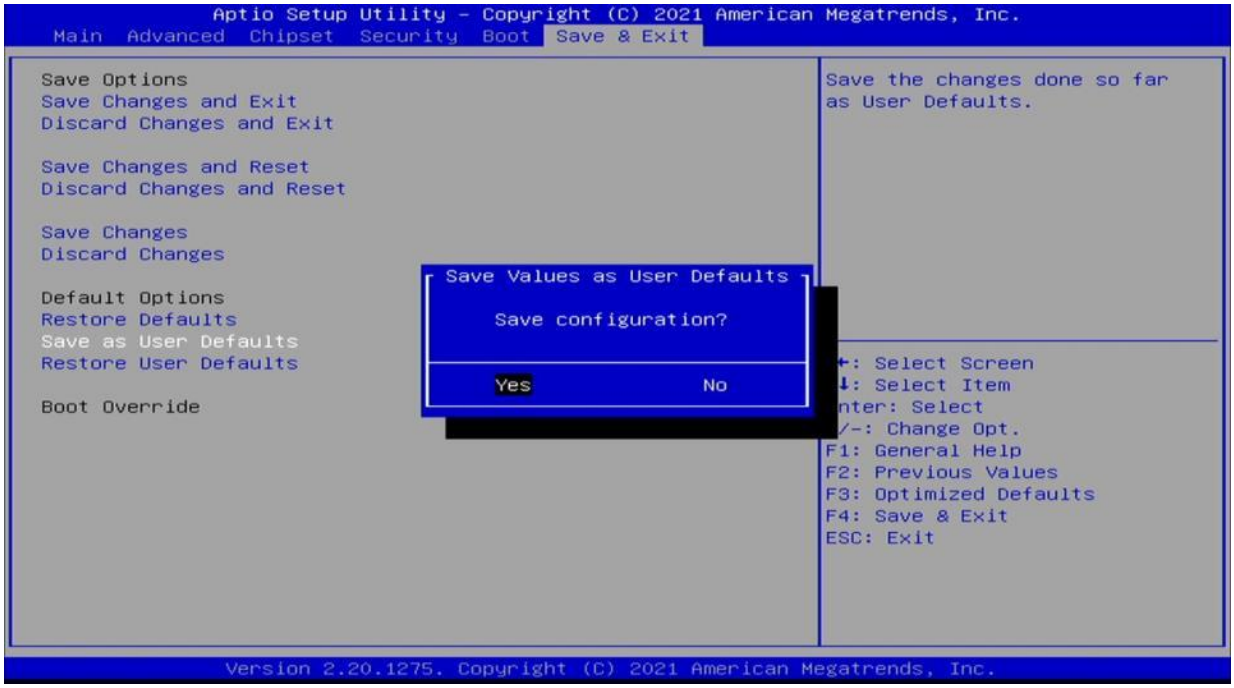
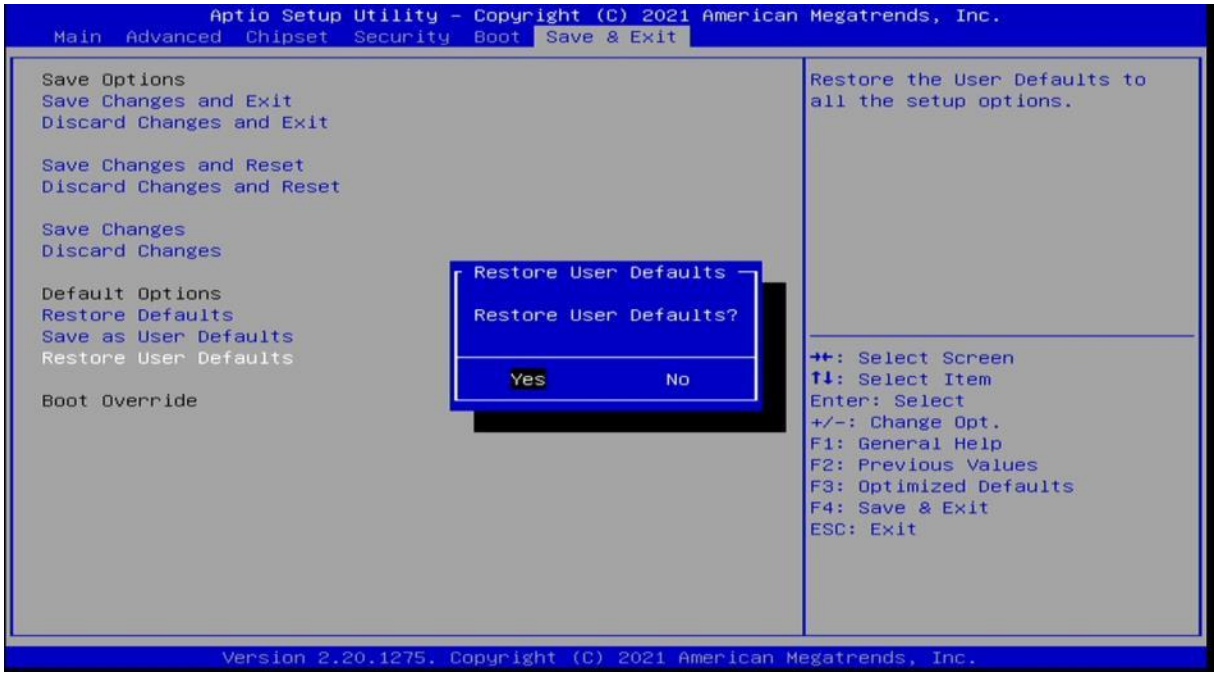
3.8.6 Load Previous Values



3.8.7 Load Optimized Defaults



3.8.8 SAVE VALUES AS USER DEFAULTS



3.8.9 RESTORE USER DEFAULTS