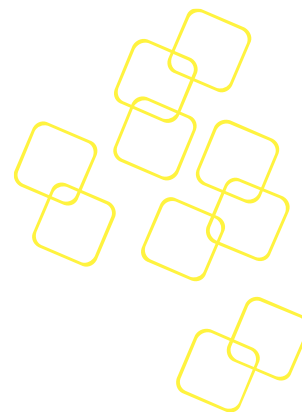


COMMON BIOS USER

REVISION 02

DATE 11/08/2023

MANUAL



INDEX

1. BIOS.....	4
1.1 BIOS DEFAULTS	4
1.2 BIOS SETUP MENU	4
1.2.1 Main Setup Menu	6
1.2.2 Platform Setup Menu	9
1.2.3 Hardware setup menu	20
1.2.4 Server Mgmt setup menu	20
1.2.5 Setup POST & Boot Menu	22
1.2.6 Security Setup	24
1.2.7 Save & Exit Menu	26
Figure 1.1 BIOS POST screen (example)	5
Figure 1.2 BIOS Setup Screen Organization	6
Figure 1.3 BIOS Setup Main screen	7
Figure 1.4 Platform Setup Main screen	9
Figure 1.5 Platform Setup: Console Redirection Menu	10
Figure 1.6 Platform Setup: USB Configuration Menu	12
Figure 1.7 Platform Setup: Trusted Computing with TPM2.0	14
Figure 1.8 Platform Setup: Trusted Computing with TPM1.2	16
Figure 1.9 Platform Setup: Virtualization	17
Figure 1.10 Platform Setup: Platform Management	18
Figure 1.11 Server Mgmt configuration	20
Figure 1.12 Boot Configuration	22
Figure 1.13 Post & Boot Setup: CSM Configuration Menu	24
Figure 1.14 Administrator Setup	25
Figure 1.15 Save & Exit Menu	26
Table 1.1 BIOS Setup: Main Menu	8
Table 1.2 Platform Setup: COM0 Console Redirection Menu Items	11
Table 1.3 USB Configuration Menu	13
Table 1.4 Platform Setup: Trusted Computing	13
Table 1.5 Trusted Computing Menu	14

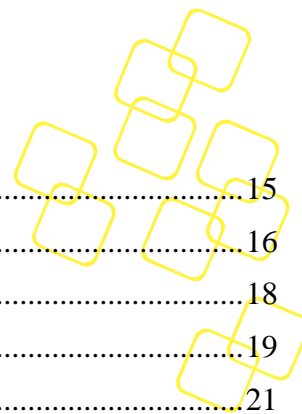


Table 1.6 Trusted Computing Menu with TPM2.0	15
Table 1.7 Trusted Computing Menu with TPM2.0	16
Table 1.8 Virtualization Menu	18
Table 1.9 Platform Management Menu	19
Table 1.10 Server Mgmt configuration Menu Items	21
Table 1.11 Boot Configuration	23
Table 1.12 CSM Configuration Menu	24
Table 1.13 Save & Exit Menu Options	27
Table 1.14 BOIS POST Codes	33



1. BIOS

BIOS is based on AMI's APTIO BIOS and compliant to the UEFI, SMBIOS and ACPI specifications.

The BIOS performs probing, initialization and configuration of the BOARD and initializes the OS boot process at the end of POST (Power-On-Self-Test).

Regular BIOS output as well as the setup menu are displayed via console port and please note that the BOARD does not have any on-board POST Code LEDs. A special POST code adapter is required to retrieve BIOS error codes.

All BIOS configuration parameters are stored in NVRAM, a dedicated section of the BIOS flash chip. Parameters are no longer stored in legacy CMOS RAM by the platform BIOS. I.e. BIOS configuration parameters will not be lost due to an empty battery.

1.1 BIOS Defaults

The BIOS comes with a set of configuration parameters when shipped by Advantech referred to as "Optimized Defaults" or "factory defaults". The user can change BIOS settings via the setup menu either temporarily or permanently by saving the changes as "User defaults".

The BIOS loads Optimized Defaults by the option "Restore Defaults; and loads User defaults by the option "Restore User Defaults". If no User defaults have been defined, the BIOS will do nothing.

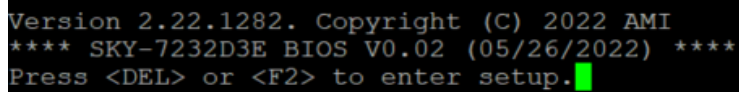
1.2 BIOS Setup Menu

This section describes the BOARD's UEFI BIOS based on AMI's APTIO BIOS.

Users can modify BIOS settings and control the special features of the BOARD using the BIOS setup menu.

Please note that Advantech supports shipping the BOARD with custom BIOS defaults to simplify the deployment and integration for our customers. Please contact your Advantech representative if you want to receive more information regarding this service.

The BIOS Setup Menu can be entered via the BIOS POST screen displayed on the console interface:

A screenshot of a BIOS POST screen. The background is black, and the text is white. The text reads: "Version 2.22.1282. Copyright (C) 2022 AMI", "**** SKY-7232D3E BIOS V0.02 (05/26/2022) ****", and "Press or <F2> to enter setup." followed by a green cursor. In the bottom right corner, the number "92" is displayed.

```
Version 2.22.1282. Copyright (C) 2022 AMI
**** SKY-7232D3E BIOS V0.02 (05/26/2022) ****
Press <DEL> or <F2> to enter setup.
```

Figure 1.1 BIOS POST screen (example)

BIOS Setup can be entered by hitting or <F2> keys during POST.

The BIOS setup menu screens have a few main elements as shown below. The menu bar displays the selectable menu pages as tabs. The parameter window displays and allows configuration of the settings available in a given menu page or a submenu thereof. Auxiliary text providing information about the selected setup item is displayed in the top right corner.



Figure 1.2 BIOS Setup Screen Organization

1.2.1 MAIN SETUP MENU

If security protection has been enabled previously (see chapter 0), you will be prompted for the BIOS password upon entering the BIOS Setup. After a successful check or if password protection has not been enabled, users will see the Main Setup screen shown below. Users can always return to the Main setup screen by selecting the Main tab.

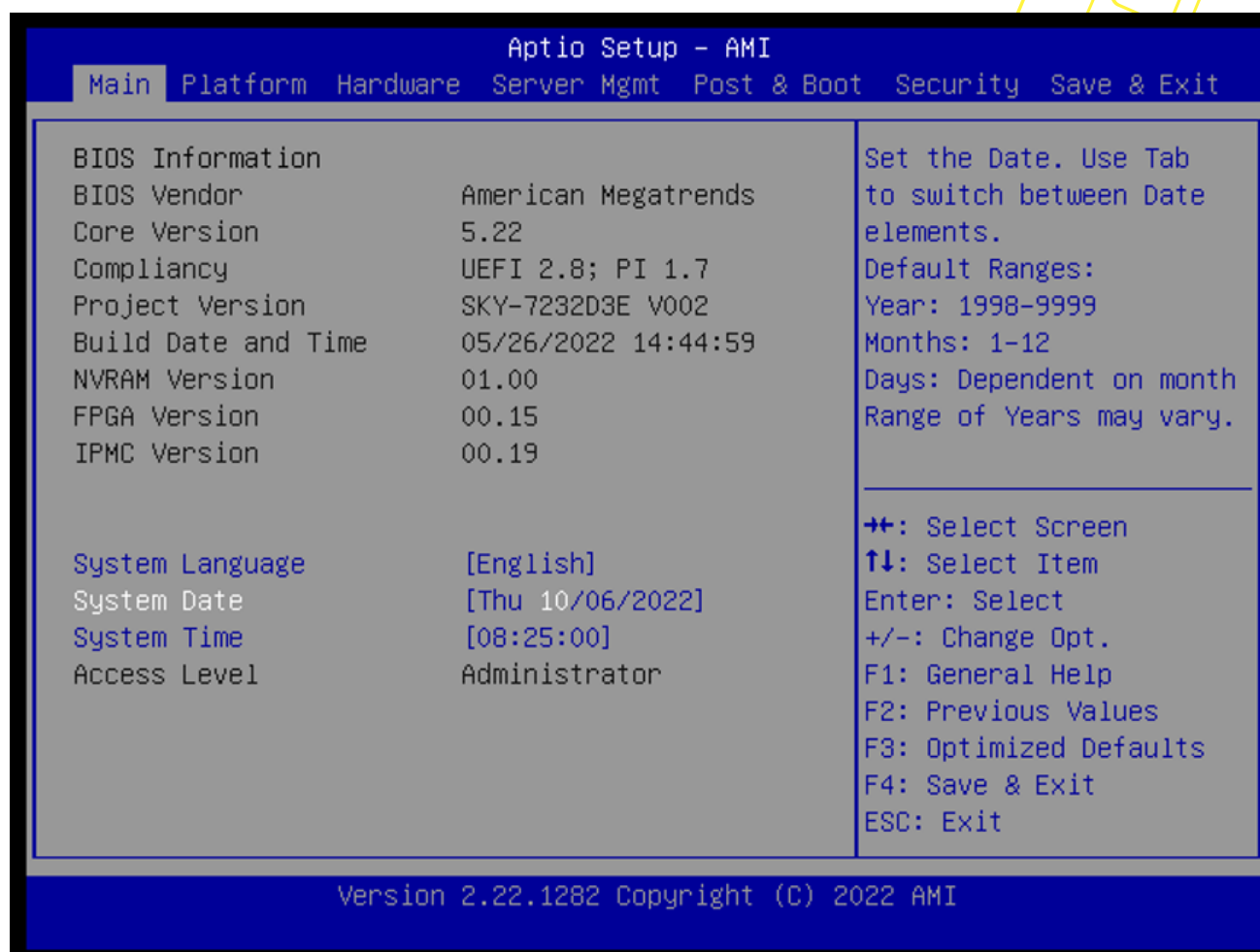


Figure 1.3 BIOS Setup Main screen

The main setup page displays system a summary of system and BIOS configuration and status information. The fields on this page are read-only except for the System Date and Time setting.

Group	Setup item	Access / Options	Description
BIOS Information	BIOS Vendor	Display only	American Megatrends
	Core Version	Display only	Current AMI BIOS core version in use
	Compliance	Display only	UEFI Spec revision that the BIOS complies to
	Project Version	Display only	Advantech BIOS Version info EX: mmmm Vx.yz mmmm : model name X : major version Yz: minor version

Group	Setup item	Access / Options	Description
	Build Date & Time	Display only	Shows BIOS build date and time
	NVRAM Version	Display only	Shows current NVRAM ver.
System Language		Display only	Selects the Setup Menu Language. Only English is supported on the BOARD
System Date		MM/DD/YY	Displays and sets the system date as used by the BIOS
System Time		HH:MM:SS	Displays and sets the system time as used by the BIOS
Access Level		Display only	Shows the user privilege level according to the security settings. If password protection has not been enabled, this will default to "Administrator"

Table 1.1 BIOS Setup: Main Menu

1.2.1.1 Setting System Time and Date

Use this option to change the system time and date. Highlight System Time or System Date using the <Arrow> keys. Enter new values through the keyboard. Press the <Tab> key or the <Arrow> keys to move between fields. The date must be entered in MM/DD/YY format. The time is entered in HH:MM:SS format.

Please note that system time and date are set during manufacturing process according to factory's local time zone. You may need to update system time to reflect the desired time zone when you receive the unit.

1.2.2 PLATFORM SETUP MENU

Select the Platform tab from the BOARD setup screen to enter the Platform Setup screen. Users can select any of the items in the left frame of the screen, such as the Trusted Computing Configuration, to go to the sub menu for that item. Users can display a Platform BIOS Setup option by highlighting it using the <Arrow> keys. The Platform BIOS Setup screen is shown below. The sub menus are described on the following pages. Note: If BMC is Present in the system and Hardware Monitor page will be hidden.

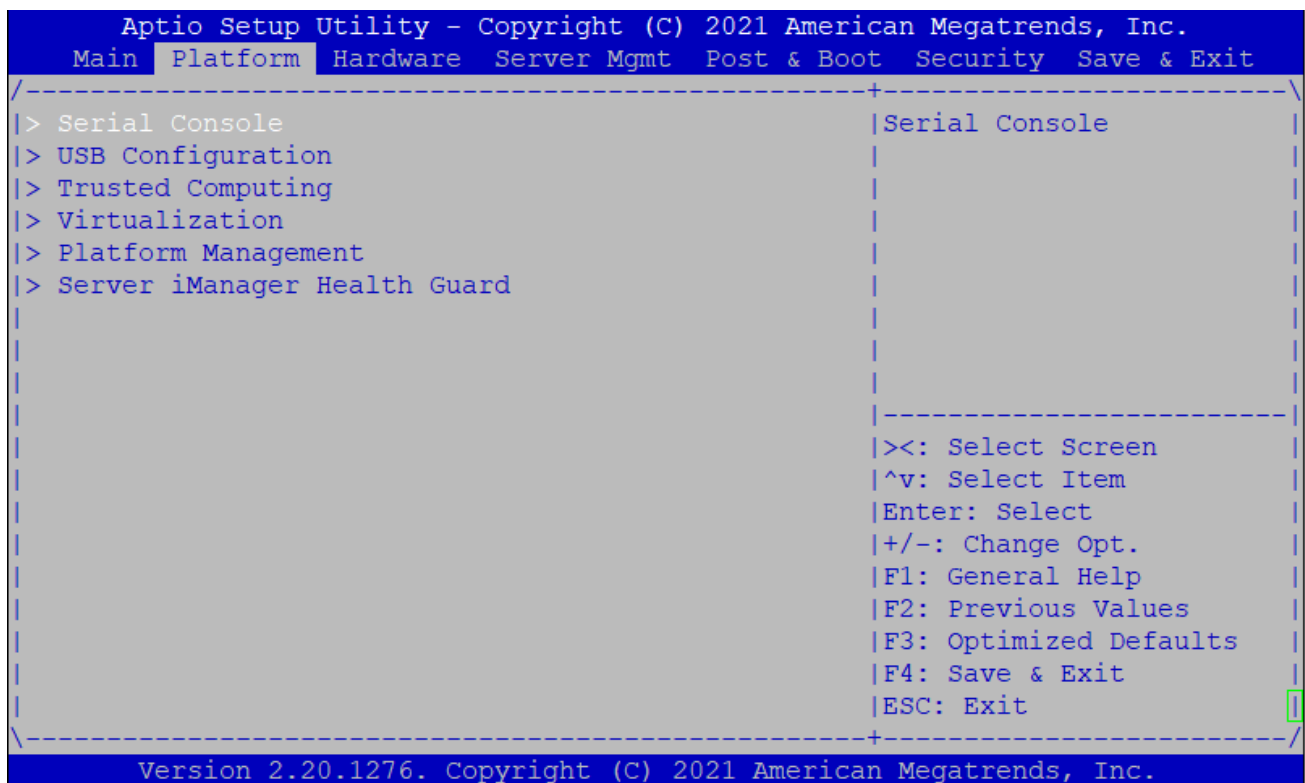


Figure 1.4 Platform Setup Main screen

1.2.2.1 Serial Console

This sub menu allows you to change the settings used for the serial console.

Note that the serial console is always using COM1 which is connected to the front panel.

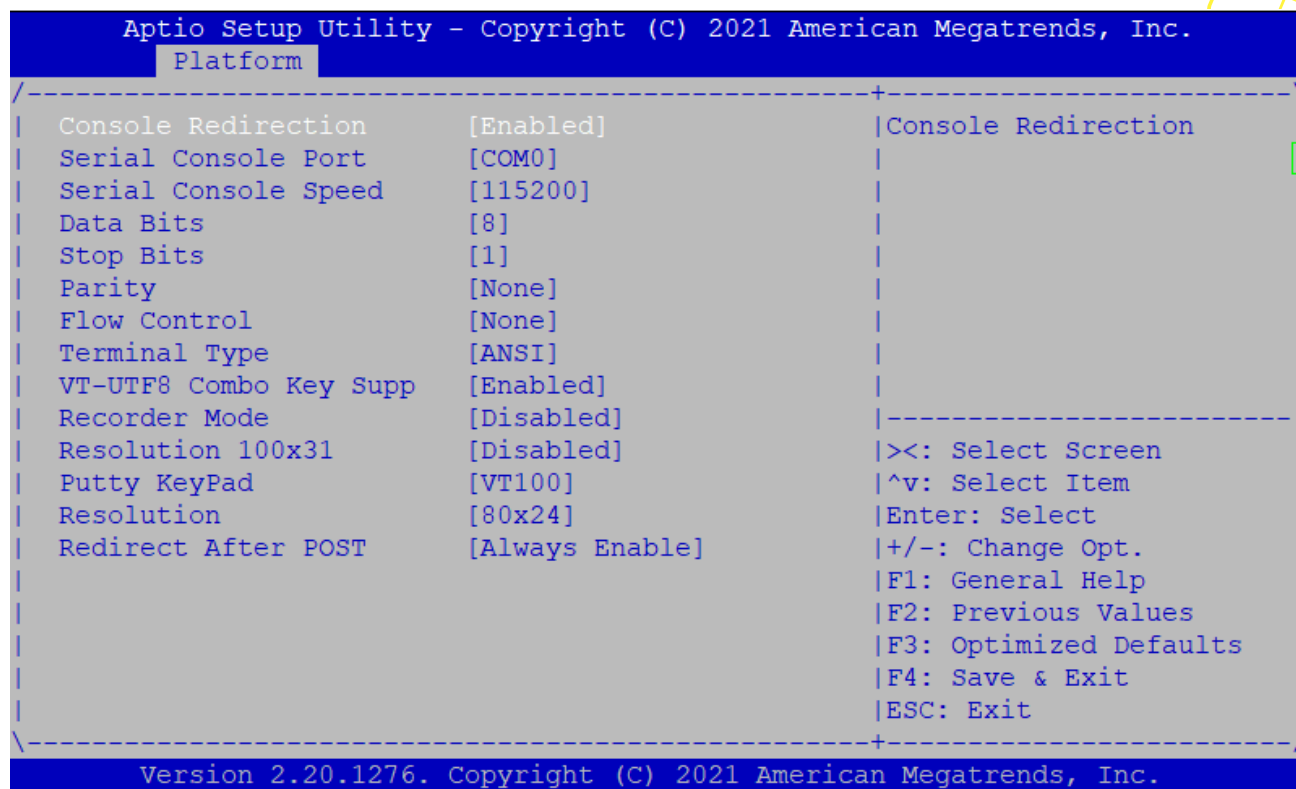


Figure 1.5 Platform Setup: Console Redirection Menu

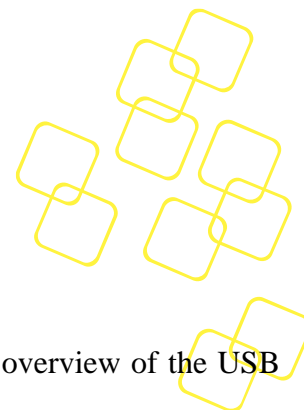
The settings for COM0 console can be accessed in this menu.

This sub menu allows you to change the settings used for the serial console. For example, users can define the terminal type, bits per second, data bits, parity, stop bits and others.

Setup item	Access / Options	Description
Console Redirection	Disabled / Enabled	Disabled / Enabled Console Redirection
Serial Console Port	COM0	Serial Console Port
Serial Console Speed	9600 / 19200 / 38400 / 57600 / 115200	Defines the baud rate.

Setup item	Access / Options	Description
Data Bits	7 / 8	Defines number of data bits in a character.
Stop Bits	1 / 2	Defines number of stop bits in a character.
Parity	None / Even / Odd / Mark / Space	Defines the parity scheme used.
Flow Control	None / Hardware RTS/CTS	Defines the flow control scheme.
Terminal Type	ANSI / VT100 / VT100+ / VT-UTF8	Select the target terminal emulation type: - ANSI to use the Extended ASCII Character Set. - VT100 to use the ASCII Character set. - VT100+ to add color and function key support. - VT-UTF8 to use UTF8 encoding to map Unicode characters into one or more bytes.
VT-UTF8 Combo Key	Disabled / Enabled	Enables VT-UTF8 Combination Key Support for ANSI / VT100 terminals
Recorder Mode	Disabled / Enabled	When Enabled the data displayed on a terminal will be captured and sent as text messages to a remote server.
Resolution 100x31	Disabled / Enabled	Enables or disables extended terminal resolution
PuTTY Keypad	VT100 / . LINUX / XTERMR6 / SCO / ESCN / VT400	Select Function Key and Key Pad Emulation on PuTTY.
Resolution	80x24 / 80x 25	When using Legacy OS, this item specifies the Number of Rows and Columns supported
Redirection after POST	Always Enable / BootLoader	This defines how long console redirection will be active: “BootLoader” means that legacy console redirection is disabled before booting into a Legacy OS. “Always Enable” means Legacy console Redirection is enabled permanently.

Table 1.2 Platform Setup: COM0 Console Redirection Menu Items



1.2.2.2 USB Configuration

This sub menu allows you to change the settings used for USB and to get an overview of the USB devices detected by the BIOS.

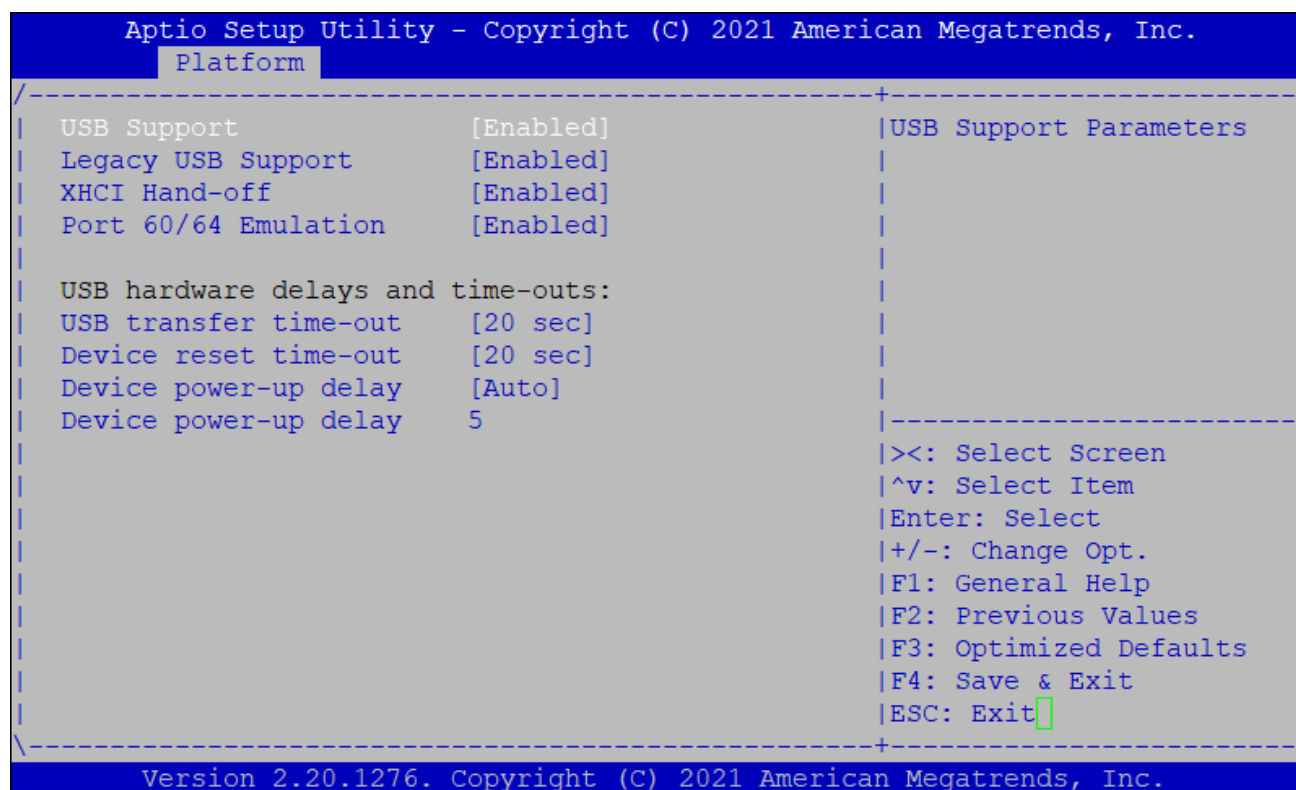


Figure 1.6 Platform Setup: USB Configuration Menu

Group	Setup item	Access / Options	Description
None	USB Support	Enabled Disabled	Enables or disables the support for USB. If disabled, the USB EHCI controller will not be initialized by the BIOS.
	Legacy USB Support	Auto Enabled Disabled	Enables legacy support over USB to support Keyboard and Mouse
	XHCI Hand-Off	Enabled Disabled	Controls the hand off of XHCI ownership from BIOS to OS at boot time.
	Port 60/64 Emulation	Enabled	Enables I/O port 60h/64h emulation support

Group	Setup item	Access / Options	Description
		Disabled	
USB hardware delay	USB transfer time-out	1sec / 5sec / 10sec / 20sec	The time-out value for Control, Bulk, and Interrupt transfers.
	Device Reset time-out	10sec / 20sec / 30sec / 40sec	Time Out for a device to Reset
	Device power-up delay	Auto Manual	Maximum time the device will take before it properly reports itself to the Host Controller.
	Device power-up delay	5	

Table 1.3 USB Configuration Menu

1.2.2.3 Trusted Computing

Please note that Trusted Computing support is disabled by default in the factory defaults to save system boot time. If disabled, the Trusted Computing Menu will not display any status information.

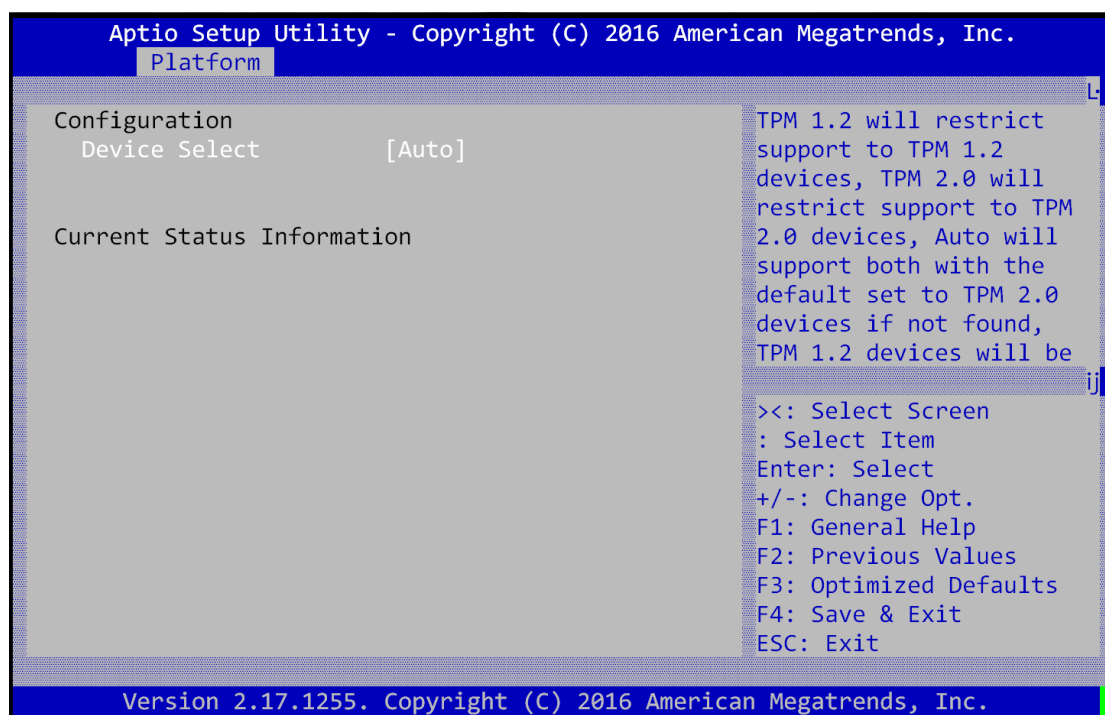


Table 1.4 Platform Setup: Trusted Computing

Group	Setup item	Access / Options	Description
Configuration	Security Device Sup	Auto TPM1.2 TPM2.0	Auto will support both or set the support for the TPM 1.2 or TPM2.0.
Current Status information	Support Turned Off	Display Only	Is displayed when TPM support is disabled
	TPM State	Display Only	Shows TPM Enablement Status
	TPM Active State	Display Only	Shows TPM Activation Status
	TPM Owner	Display Only	Shows Current TPM Owner

Table 1.5 Trusted Computing Menu

Trusted Computing with TPM module installed

When system with TPM2.0 module installed, and the BIOS will auto detect it and the related setting will be shown in the BIOS setup menu as below.

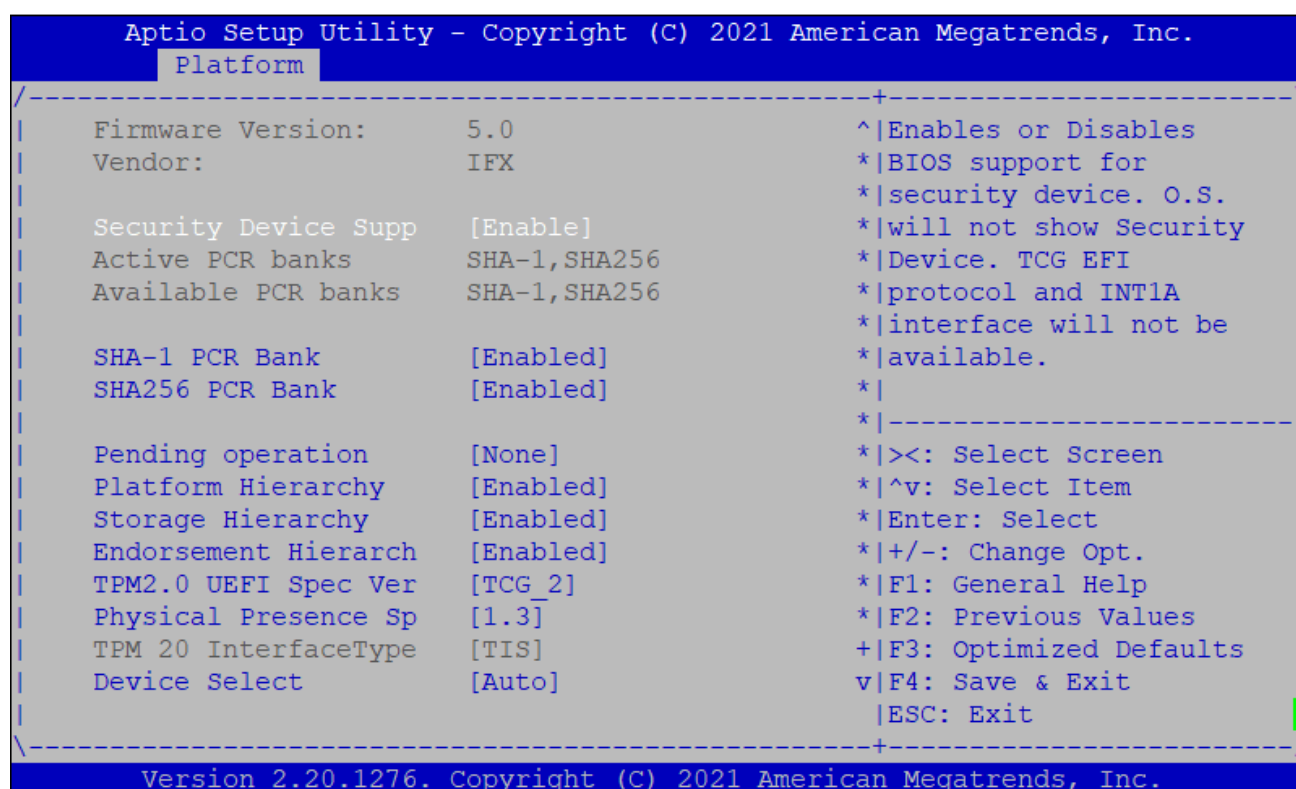


Figure 1.7 Platform Setup: Trusted Computing with TPM2.0

Group	Setup item	Access / Options	Description
TPM20 Device Found	Security Device Sup	Enable Disable	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 Disable	Enable/Disable SHA-1 PCR Bank
	SHA256 PCR Bank	Enable Disable	Enable/Disable SHA256 PCR Bank
	Pending operation	None TPM Clear	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 Disable	Enable or Disable Platform Hierarchy
	Storage Hierarchy	Enable Disable	Enable or Disable Storage Hierarchy
	Endorsement Hierarchy	Enable Disable	Enable or Disable Endorsement Hierarchy
	TPM2.0 UEFI Spec Version	TCG_2 TCG_1_2	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
	Physical Presence Spec Version	1.2 1.3	Select to Tell O.S. to support PPI Spec Version 1.2 or 1.3. Note some HCK tests might not support 1.3
	TPM 20 InterfaceTyp	Display only (TIS)	
	Device Select	Auto	Auto will support both or set the support for the TPM 1.2 or TPM2.0.
	TPM 2.0 HID	MSFT0101 PNP0C31	Choose TPM 2.0 HID return value. We suggest to use MSFT0101 for Windows and Linux kernel version 4.4 and to use PNP0C31 for Linux kernel with previous version from 4.4

Table 1.6 Trusted Computing Menu with TPM2.0

When system with TPM1.2 module installed, and the BIOS will auto detect it and the related setting will be shown in the BIOS setup menu as below.

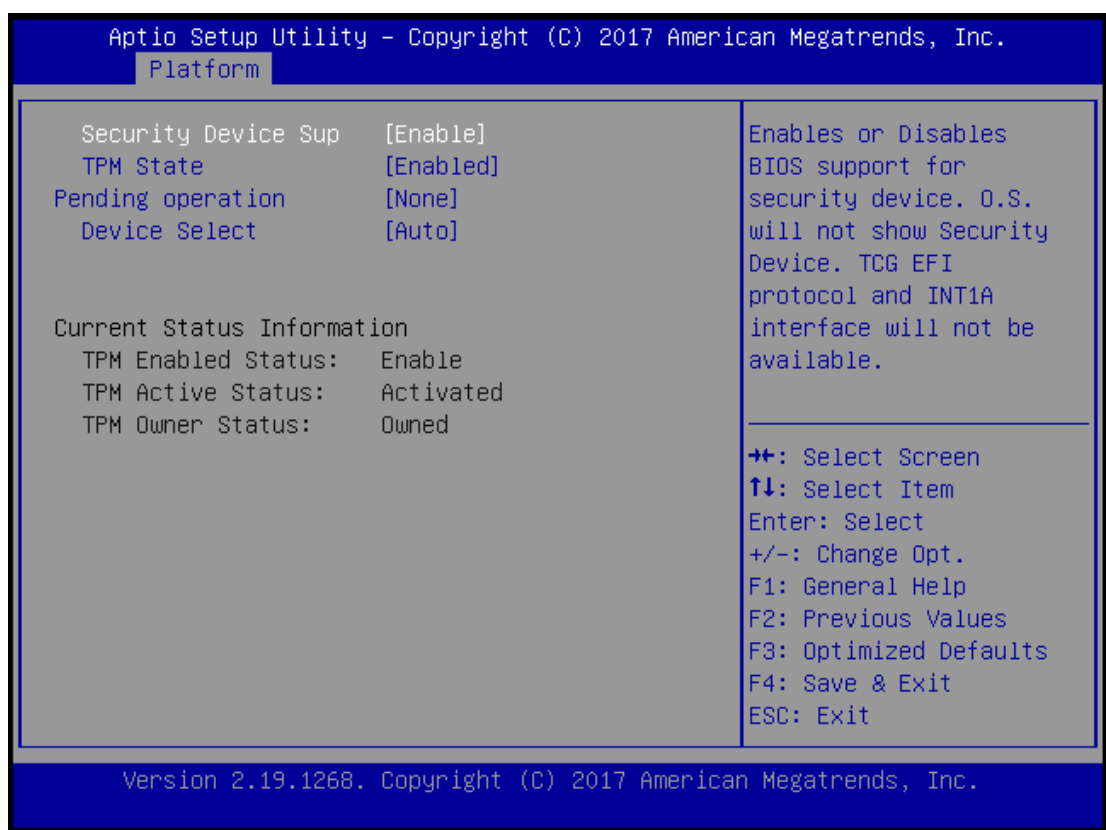


Figure 1.8 Platform Setup: Trusted Computing with TPM1.2

Group	Setup item	Access / Options	Description
TPM2.0 Device Found	Security Device Sup	Enable Disable	BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.
	TPM State	Enable Disable	Enable/Disable Security Device. NOTE: Your Computer will reboot during restart in order to change State of the Device.
	Pending operation	None	Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change State of Security Device.
	Device Select	Auto	Auto will support both or set the support for the TPM 1.2 or TPM2.0.

Table 1.7 Trusted Computing Menu with TPM2.0



1.2.2.4 Virtualization

This sub menu allows you to change the settings used for Virtualization function.

Intel® Virtualization Technology for Directed I/O (VT-d). Thus, BIOS handle virtual functions exposed by PCIe devices in case SR-IOV is supported, otherwise PCIe devices will be assigned to virtual machines in pass-through mode. This applies for all PCIe devices.

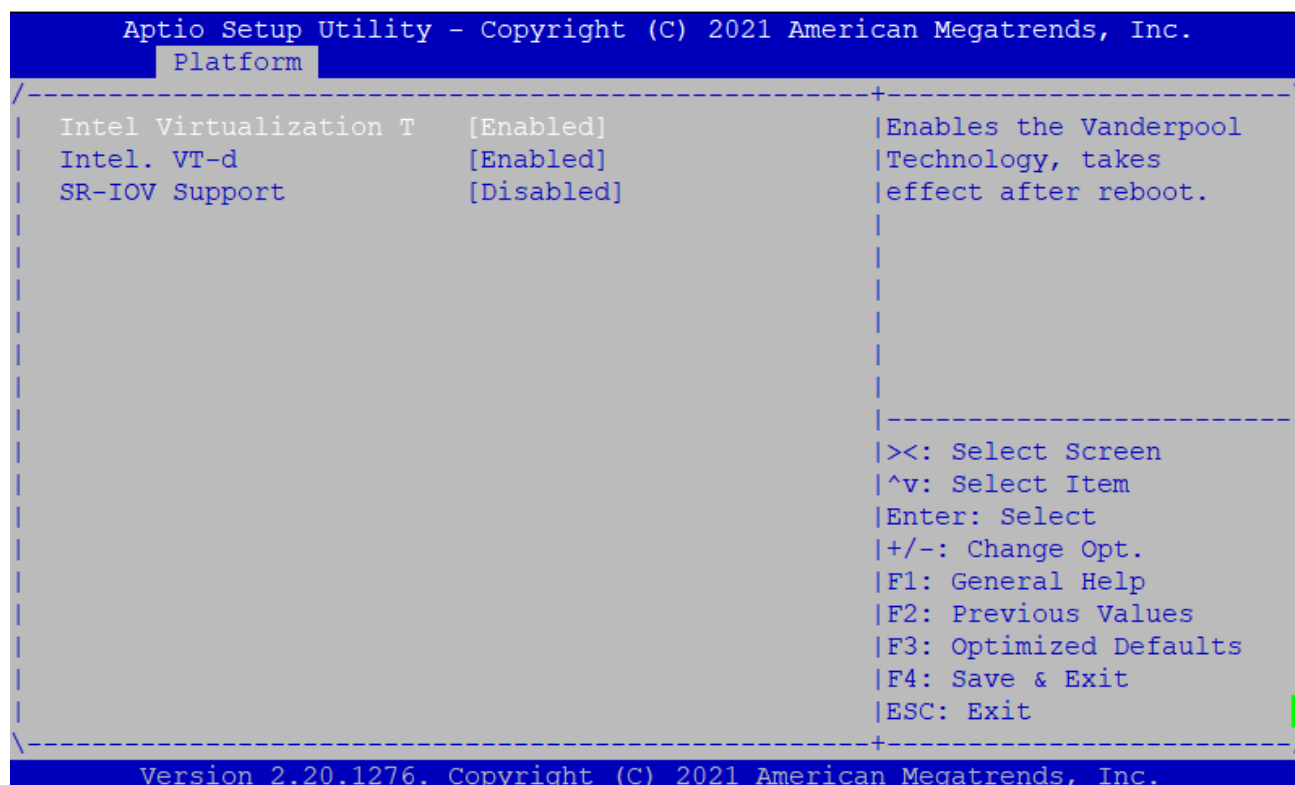
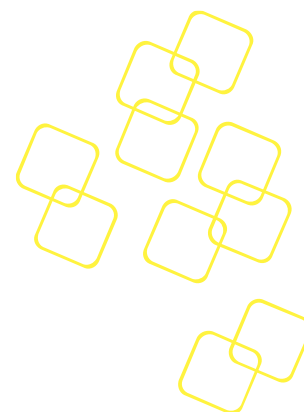


Figure 1.9 Platform Setup: Virtualization

Group	Setup item	Access / Options	Description
None	Intel Virtualization	Enable Disable	Enable/Disable Intel Virtualization Technology , take effect after reboot
	Intel VT-d	Enable Disable	Enable/disable Intel Virtualization Technology for Directed I/O (VT-d) by reporting the I/O device
	SR-IOV Support	Enable Disable	If system has SR-IOV capable PCIe Devices, this option Enables or Disables Single Root IO <u>Virtualization</u> Support

Table 1.8 Virtualization Menu



1.2.2.5 Platform Management

This sub menu allows you to change the settings used for related CPU utilization setting.

The default configuration for CPU was optimized setting for getting better performance for networking, so it is not recommended to change it.

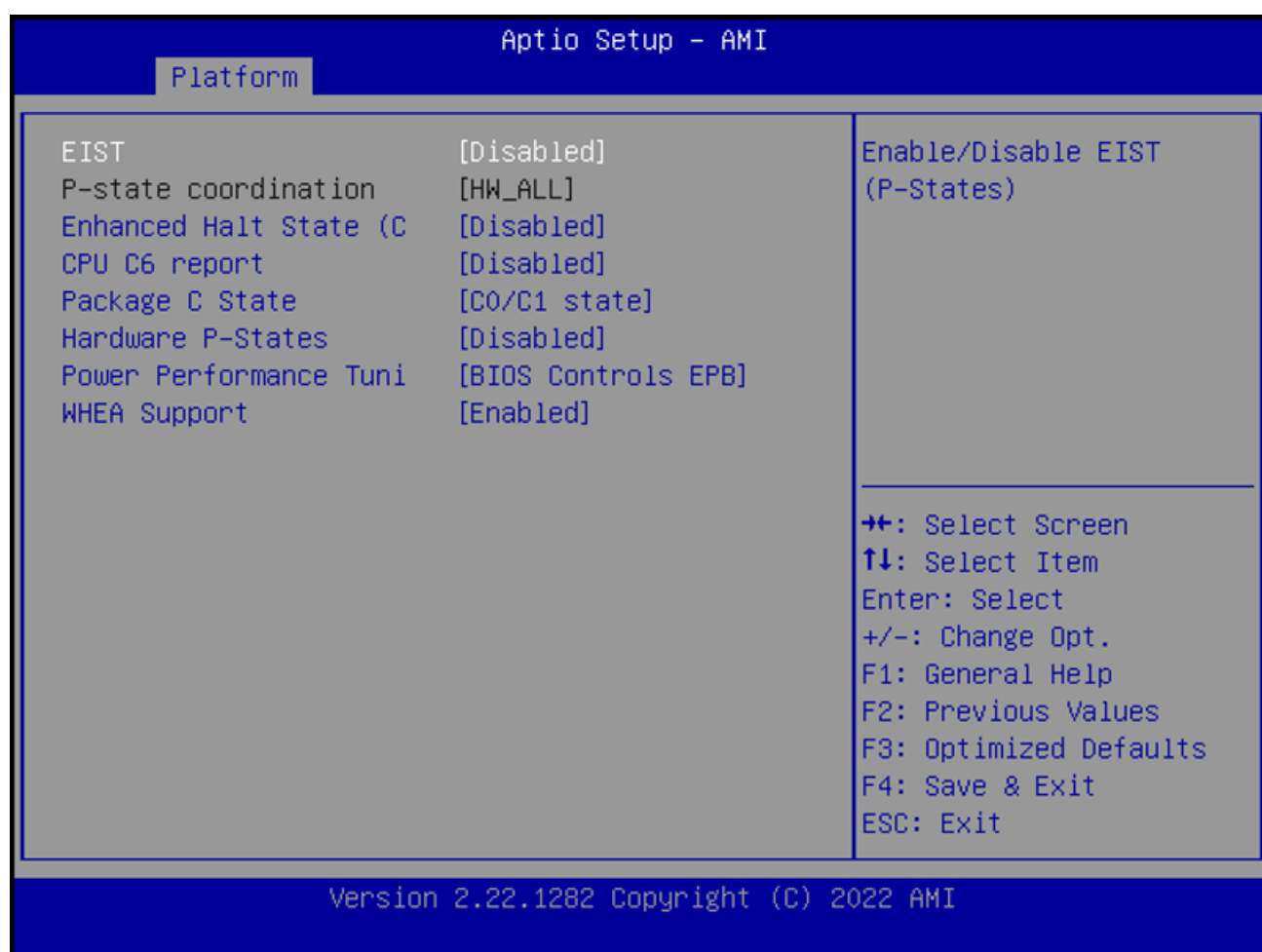


Figure 1.10 Platform Setup: Platform Management

Group	Setup item	Access / Options	Description
None	EIST	Enable Disable	Enable or disable BIOS support for Enhanced Intel SpeedStep Technology, When enabled, OS sets CPU frequency

Group	Setup item	Access / Options	Description
			according load. When disabled, CPU frequency is set at max non-turbo.
	P-state coordination	HW_ALL	HW_ALL (hardware) coordination is recommended over SW_ALL and SW_ANY (software coordination).
	Enhanced Halt State (C1E)	Enable Disable	Core C1E auto promotion Control. Takes effect after reboot.
	CPU C6 report	Enable Disable	Enable/Disable CPU C6(ACPI C2) report to OS Recommended to be enabled.
	Package C State limit	C0/C1 state C2 state C6(non Retention) state C6(Retention) state	Package C State limit. The "waking-up time" will be longer if Package C state limit setting is deep C state support.
	Hardware P-States	Disabled, Native Mode, Out of Band Mode, Native Mode with No Legacy Support	Disable: Hardware chooses a P-state based on OS Request (Legacy P-States) Native Mode: Hardware chooses a P-state based on OS guidance Out of Band Mode: Hardware autonomously chooses a P-state (no OS guidance)
	Power Performance Tuning	OS Controls EPB BIOS Controls EPB PECI Controls EPB	Selects whether BIOS or Operating System chooses energy performance bias tuning.
	WHEA Support	Enable Disable	Enable or disable the WHEA support

Table 1.9 Platform Management Menu

1.2.3 HARDWARE SETUP MENU

This sub menu allows you to change the settings of the chipset. It is hardware-related, please refer to the BIOS section in the user manual of each product.

1.2.4 SERVER MGMT SETUP MENU

The Server Mgmt menu supports configuring BMC related features such as OS Watchdog Timer, etc.

```

Aptio Setup Utility - Copyright (C) 2021 American Megatrends, Inc.
Main Platform Hardware Server Mgmt Post & Boot Security Save & Exit
/-----+-----/
| BMC Self Test Status      PASSED          | If enabled, starts a ^|
| OS Watchdog Timer        [Disabled]        | BIOS timer which can *|
| OS Wtd Timer Timeout     [10 minutes]      | only be shut off by  *|
| OS Wtd Timer Policy      [Reset]           | Management Software  *|
|> BMC network configuration | after the OS loads.  *|
|> BMC self test log       | Helps determine that *|
|> System Event Log        | the OS successfully +|
|                           | loaded or follows the v|
|                           | -----|
|                           | ><: Select Screen   |
|                           | ^v: Select Item    |
|                           | Enter: Select     |
|                           | +/-: Change Opt.  |
|                           | F1: General Help  |
|                           | F2: Previous Values|
|                           | F3: Optimized Defaults|
|                           | F4: Save & Exit    |
|                           | ESC: Exit         |
|                           | -----|
|                           |
|-----+-----|
Version 2.20.1276. Copyright (C) 2021 American Megatrends, Inc.

```

Figure 1.11 Server Mgmt configuration

Group	Setup item	Access / Options	Description
None	BMC Self Test Status	Display only (Passed)	BMC self test status indication during power on process
	OS Watchdog Timer	Enable Disable	If enabled, starts a BIOS timer which can only be shut off by Management Software after the OS loads. Helps determine that the OS successfully loaded or follows the OS Boot Watchdog Timer

Group	Setup item	Access / Options	Description
	OS Wtd Timer Timeout	5 minutes 10 minutes 15 minutes 20 minutes	Configure the length of the OS Boot Watchdog Timer. Not available if OS Boot Watchdog Timer is disabled.
	OS Wtd Timer Policy	Do Nothing Reset Power Down	Configure how the system should respond if the OS Boot Watchdog Timer expires. Not available if OS Boot Watchdog Timer is disabled.
BMC network configuration	Configuration Address	Unspecified Static Dynamic BMC DHCP	Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase
BMC self-test log	Erase Log	NO Yes, On every reset	Erase Log Options
	When log is full	Clear Log Do not log any more	Select the action to be taken when log is full
System event log	SEL Components	Enable Disable	Change this to enable or disable all features of System Event Logging during boot.
	Erase SEL	No Yes, On next reset Yes, ON every reset	Choose options for erasing SEL.
	When SEL is Full	Do Nothing Erase Immediately	Choose options for reactions to a full SEL.
	Log EFI Status Codes	Disable Both Error code Progress code	Disable the logging of EFI Status Codes or log only error code or only progress code or both

Table 1.10 Server Mgmt. configuration Menu Items

1.2.5 SETUP POST & BOOT MENU

Users can configure the system boot priority settings via the boot page. The default setting of boot priority of boot option #1 is “UEFI: Built-in EFI Shell”; Users can define the boot priorities based on the application.

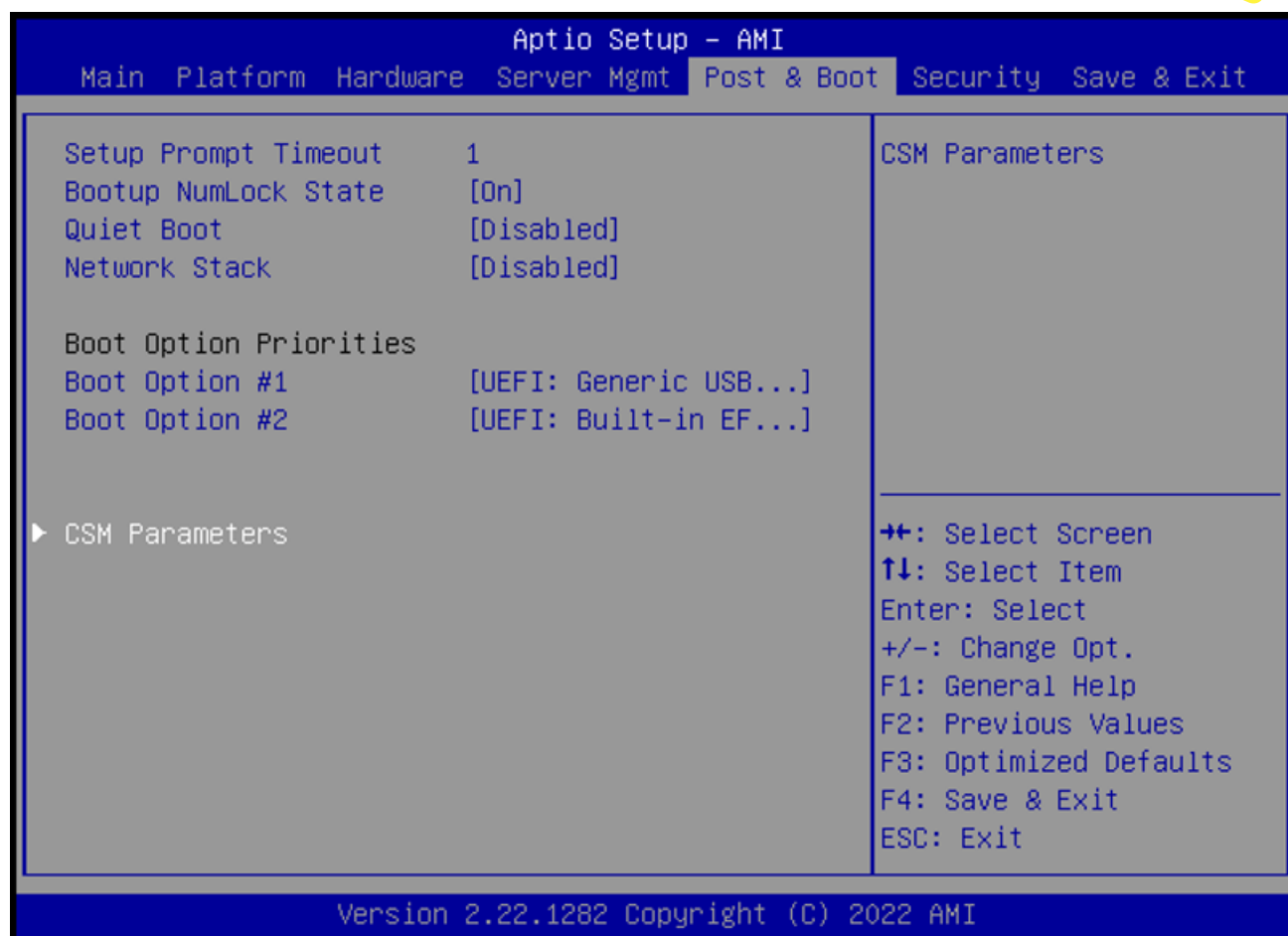


Figure 1.12 Boot Configuration

Feature	Default	Description
Setup Prompt Timeout	1	Number of seconds to wait for setup activation key.
Bootup NumLock State	On	Select the keyboard NumLock state.
Quiet Boot	Disabled	Enables or disables Quiet Boot option.
Network Stack	Disabled	Enables or disables boot via Network (PXE)
UEFI PXE Support	Enabled	Enable/Disable IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available
Boot Option Priority	User Defined	Sets the system boot order.
CSM Parameters	CSM Support	Enable the CSM support

Table 1.11 Boot Configuration

1.2.5.1 Compatibility Support Module (CSM) Configuration

This submenu allows users to configure the support for legacy BIOS mechanisms and option ROMs.

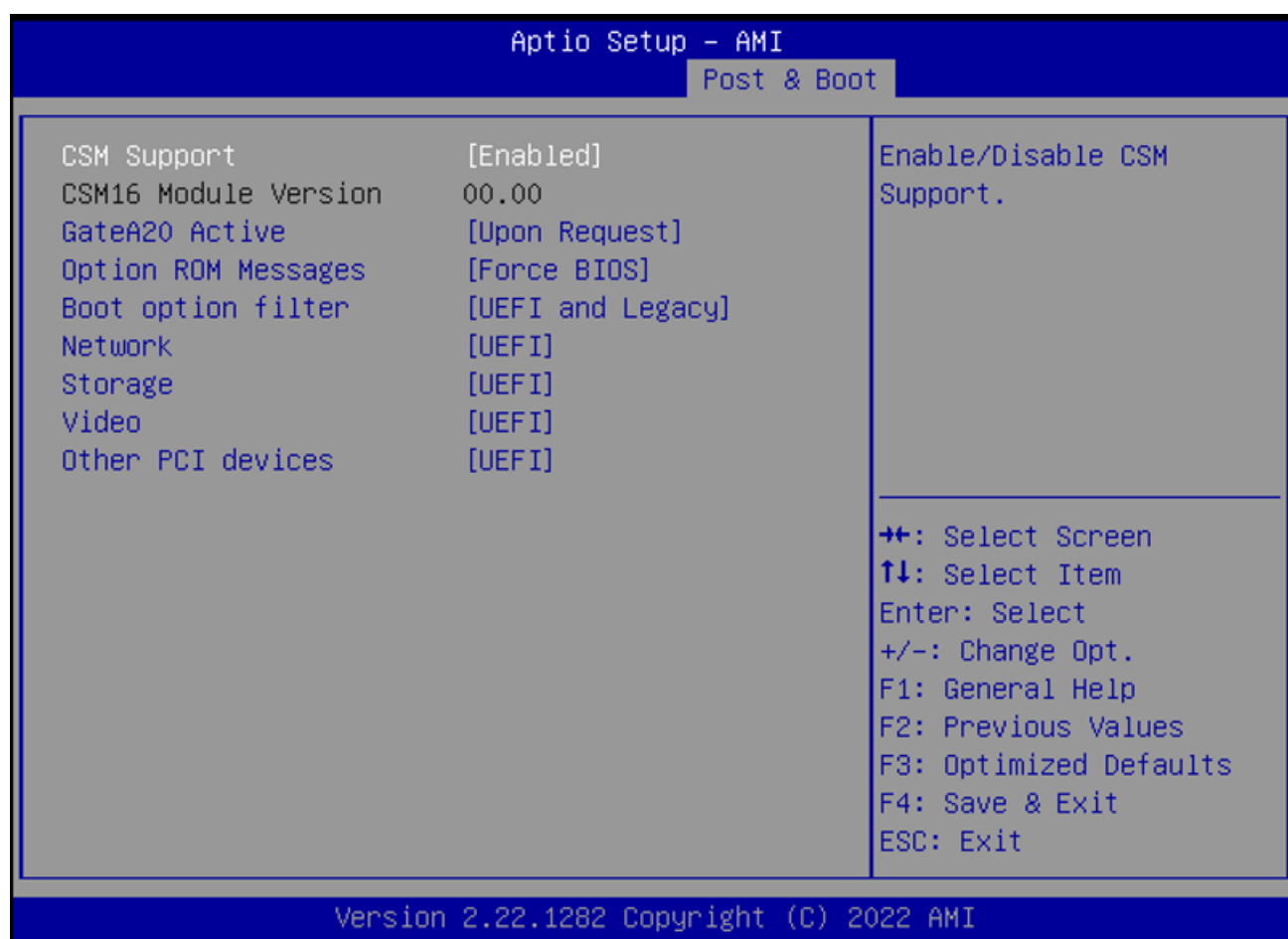


Figure 1.13 Post & Boot Setup: CSM Configuration Menu

Group	Setup item	Access / Options	Description
None	CSM Support	Enabled Disabled	Enables or disables the Compatibility Support Module.
	GateA20 Active	Upon Request Always	UPON REQUEST - GA20 can be disabled using BIOS services. ALWAYS - do not allow disabling GA20; this option is useful when any RT code is executed above 1MB
	Option ROM Messages	Force BIOS Keep Current	Set display mode for Option ROM
	Boot option filter	UEFI and Legacy Legacy Only UEFI Only	This item allows to control the execution of legacy and UEFI compliant Option ROMs
	Network	Do not launch UEFI Legacy	This item allows a more granular control of OptionROM execution depending of the type of extension device.
	Storage		
	Video		
	Other PCI device ROM		

Table 1.12 CSM Configuration Menu

1.2.6 SECURITY SETUP

“**Administrator Password**” allows users to configure the system so that a password after being installed is required each time the system boots, and/or an attempt is made to enter the Setup program.

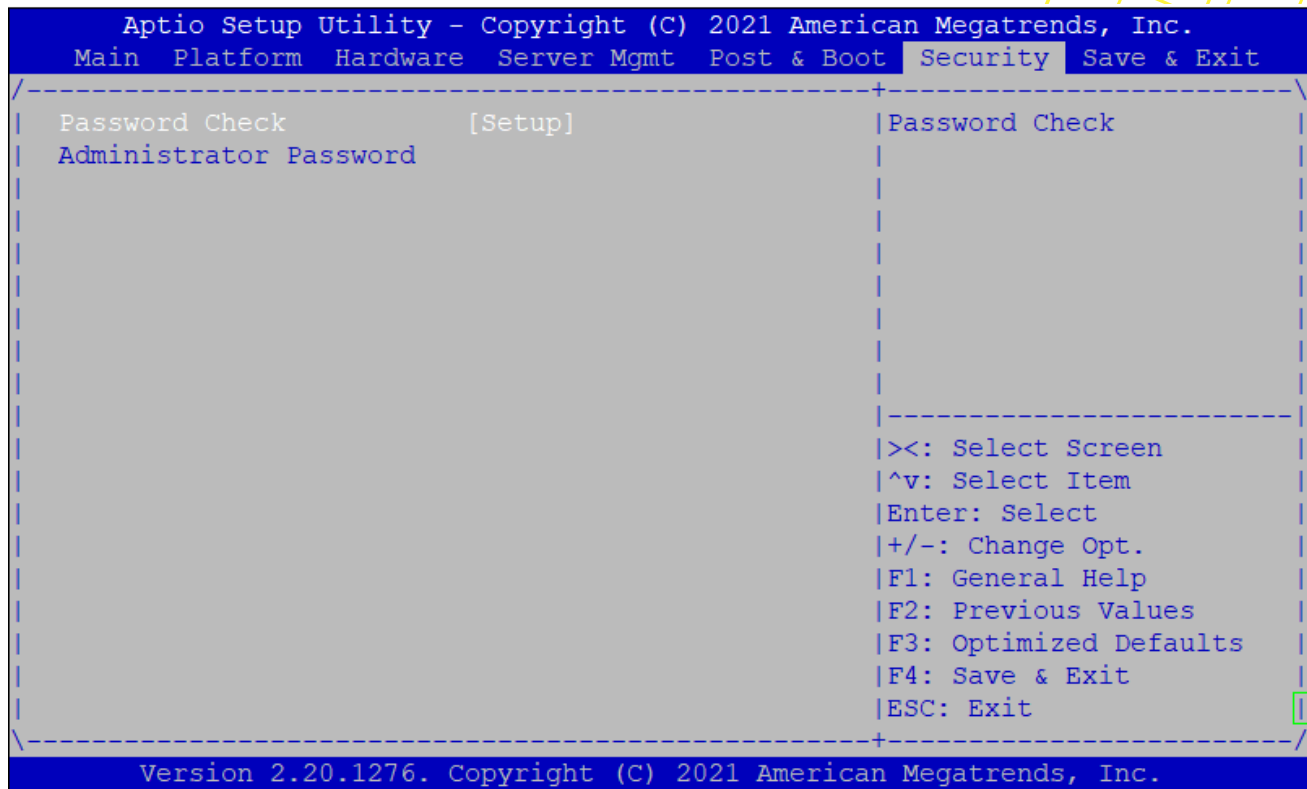
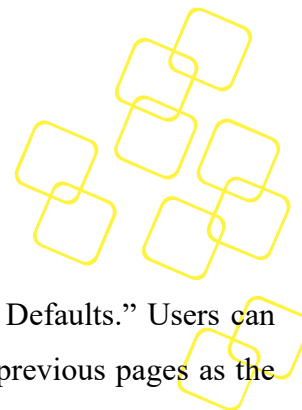


Figure 1.14 Administrator Setup

Note:

- ◆ If set the “Password Check” is [Setup], then this limits the access to Setup and is only asked for when entering Setup.
- ◆ If set the “Password Check” is [Always], then this is a power on password and must be entered to boot or enter Setup. In Setup the User will have Administrator rights.
- ◆ The password length must be in the following range:
 - Minimum length: 3
 - Maximum length: 2



1.2.7 SAVE & EXIT MENU

The BOARD BIOS allows users to store BIOS configuration results as “User Defaults.” Users can select “Save as User Defaults” to record all changes which had been made in previous pages as the default setting for further use.

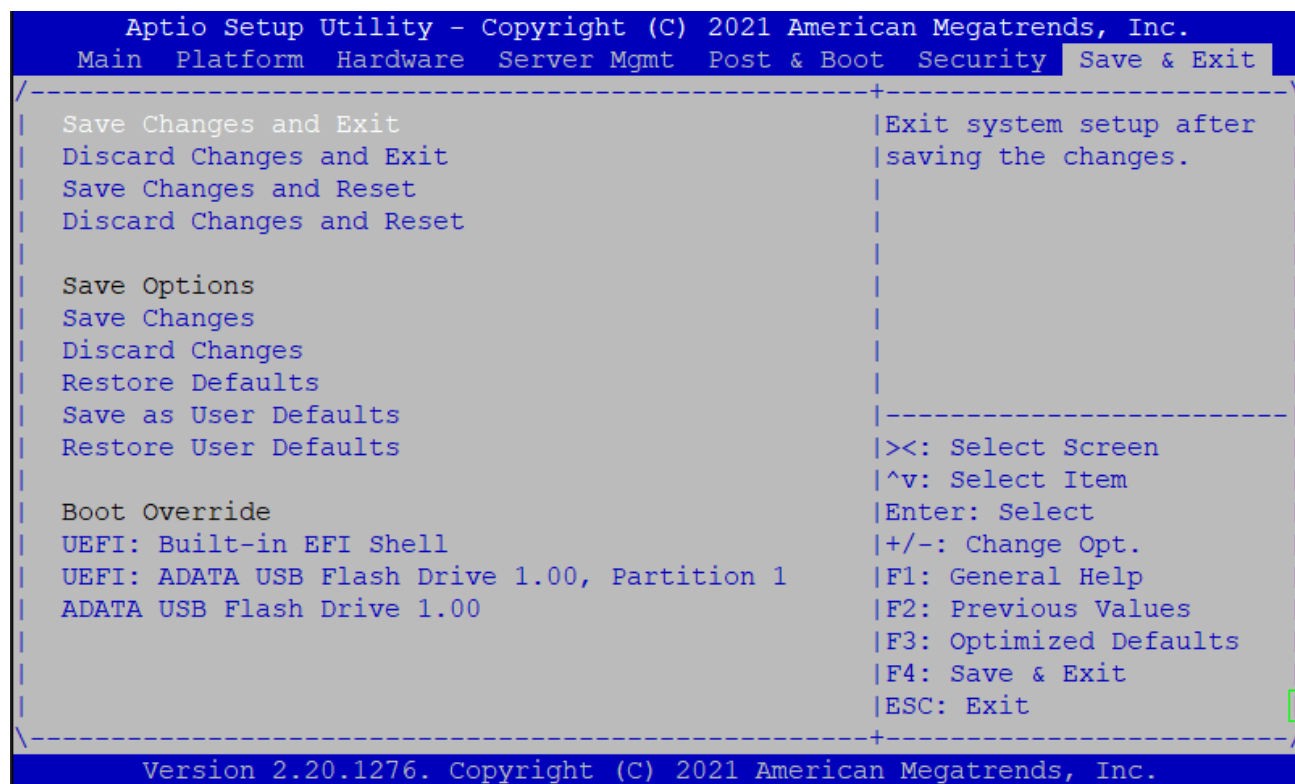


Figure 1.15 Save & Exit Menu

Group	Setup item	Description
None	Save Changes and Exit	Exit setup after saving the changes. Does not update User defaults.
	Discard Changes and Exit	Exit setup without saving any changes.
	Save Changes and Reset	Reset system after saving the changes. Does not update User Defaults.
	Discard Changes and Reset	Reset system without saving the changes.
Save Options	Save Changes	Save Changes made so far to any of the setup options.
	Discard Changes	Discard Changes made so far to any of the setup options.
	Restore Defaults	Restores the BIOS factory defaults to all the setup options.

Group	Setup item	Description
	Save as User Defaults	Saves the Current BIOS Settings as User Defaults.
	Restore User Defaults	Restores the User defaults to all the setup options.
Boot Override	UEFI: < boot device>	This option allows you to override the specified boot order and use a different boot device for the next boot.

Table 1.13 Save & Exit Menu Options

1.2.8 BIOS POST CODE

POST Codes are diagnostic codes sent by the BIOS to IO address 0x80. A POST adapter needs to be installed in the system to view these POST Codes. Codes not listed are reserved by AMI.

POST Code	Description
0x01	Power on. Reset <u>type</u> detection (soft/hard).
0x02	AP initialization before microcode loading
0x03	North Bridge initialization before microcode loading
0x04	South Bridge initialization before microcode loading
0x05	OEM initialization before microcode loading
0x06	Microcode loading
0x07	AP initialization after microcode loading
0x08	North Bridge initialization after microcode loading
0x09	South Bridge initialization after microcode loading
0x0A	OEM initialization after microcode loading
0x0B	Cache initialization
0x0C – 0x0D	Reserved for future AMI SEC error codes
0x0E	Microcode not found
0x0F	Microcode not loaded
0x10	PEI Core is started
0x11	Pre-memory CPU initialization is started

POST Code	Description
0x12	Pre-memory CPU initialization (CPU module specific)
0x13	Pre-memory CPU initialization (CPU module specific)
0x14	Pre-memory CPU initialization (CPU module specific)
0x15	Pre-memory North Bridge initialization is started
0x16	Pre-Memory North Bridge initialization (North Bridge module specific)
0x17	Pre-Memory North Bridge initialization (North Bridge module specific)
0x18	Pre-Memory North Bridge initialization (North Bridge module specific)
0x19	Pre-memory South Bridge initialization is started
0x1A	Pre-memory South Bridge initialization (South Bridge module specific)
0x1B	Pre-memory South Bridge initialization (South Bridge module specific)
0x1C	Pre-memory South Bridge initialization (South Bridge module specific)
0x1D – 0x2A	OEM pre-memory initialization codes
0x2B	Memory initialization. Serial Presence Detect (SPD) data reading
0x2C	Memory initialization. Memory presence detection
0x2D	Memory initialization. Programming memory timing information
0x2E	Memory initialization. Configuring memory
0x2F	Memory initialization (other).
0x30	Reserved for ASL (see ASL Status Codes section below)
0x31	Memory Installed
0x32	CPU post-memory initialization is started
0x33	CPU post-memory initialization. Cache initialization
0x34	CPU post-memory initialization. Application Processor(s) (AP) initialization
0x35	CPU post-memory initialization. Boot Strap Processor (BSP) selection
0x36	CPU post-memory initialization. System Management Mode (SMM) initialization
0x37	Post-Memory North Bridge initialization is started
0x38	Post-Memory North Bridge initialization (North Bridge module specific)
0x39	Post-Memory North Bridge initialization (North Bridge module specific)

POST Code	Description
0x3A	Post-Memory North Bridge initialization (North Bridge module specific)
0x3B	Post-Memory South Bridge initialization is started
0x3C	Post-Memory South Bridge initialization (South Bridge module specific)
0x3D	Post-Memory South Bridge initialization (South Bridge module specific)
0x3E	Post-Memory South Bridge initialization (South Bridge module specific)
0x3F-0x4E	OEM post memory initialization codes
0x4F	DXE IPL is started
0x50	Memory initialization error. Invalid memory type or incompatible memory speed
0x51	Memory initialization error. SPD reading has failed
0x52	Memory initialization error. Invalid memory size or memory modules do not match.
0x53	Memory initialization error. No usable memory detected
0x54	Unspecified memory initialization error.
0x55	Memory not installed
0x56	Invalid CPU type or Speed
0x57	CPU mismatch
0x58	CPU self-test failed or possible CPU cache error
0x59	CPU micro-code is not found, or micro-code update is failed
0x5A	Internal CPU error
0x5B	reset PPI is not available
0x5C	PEI phase BMC self-test failure
0x5C-0x5F	Reserved for future AML error codes
0x60 DXE	Core is started
0x61	NVRAM initialization
0x62	Installation of the South Bridge Runtime Services
0x63	CPU DXE initialization is started
0x64	CPU DXE initialization (CPU module specific)
0x65	CPU DXE initialization (CPU module specific)

POST Code	Description
0x66	CPU DXE initialization (CPU module specific)
0x67	CPU DXE initialization (CPU module specific)
0x68	PCI host bridge initialization
0x69	North Bridge DXE initialization is started
0x6A	North Bridge DXE SMM initialization is started
0x6B	North Bridge DXE initialization (North Bridge module specific)
0x6C	North Bridge DXE initialization (North Bridge module specific)
0x6D	North Bridge DXE initialization (North Bridge module specific)
0x6E	North Bridge DXE initialization (North Bridge module specific)
0x6F	North Bridge DXE initialization (North Bridge module specific)
0x70	South Bridge DXE initialization is started
0x71	South Bridge DXE SMM initialization is started
0x72	South Bridge devices initialization
0x73	South Bridge DXE Initialization (South Bridge module specific)
0x74	South Bridge DXE Initialization (South Bridge module specific)
0x75	South Bridge DXE Initialization (South Bridge module specific)
0x76	South Bridge DXE Initialization (South Bridge module specific)
0x77	South Bridge DXE Initialization (South Bridge module specific)
0x78	ACPI module initialization
0x79	CSM initialization
0x7A – 0x7F	Reserved for future AMI DXE codes
0x80 – 0x8F	OEM DXE initialization codes
0x90	Boot Device Selection (BDS) phase is started
0x91	Driver connecting is started
0x92	PCI Bus initialization is started
0x93	PCI Bus Hot Plug Controller Initialization
0x94	PCI Bus Enumeration

POST Code	Description
0x95	PCI Bus Request Resources
0x96	PCI Bus Assign Resources
0x97	Console Output devices connect
0x98	Console input devices connect
0x99	Super IO Initialization
0x9A	USB initialization is started
0x9B	USB Reset
0x9C	USB Detect
0x9D	USB Enable
0x9E – 0x9F	Reserved for future AML codes
0xA0	IDE initialization is started
0xA1	IDE Reset
0xA2	IDE Detect
0xA3	IDE Enable
0xA4	SCSI initialization is started
0xA5	SCSI Reset
0xA6	SCSI Detect
0xA7	SCSI Enable
0xA8	Setup Verifying Password
0xA9	Start of Setup
0xAA	Reserved for ASL (see ASL Status Codes section below)
0xAB	Setup Input Wait
0xAC	Reserved for ASL (see ASL Status Codes section below)
0xAD	Ready To Boot event
0xAE	Legacy Boot event
0xAF	Exit Boot Services event
0xB0	Runtime Set Virtual Address MAP Begin

POST Code	Description
0xB1	Runtime Set Virtual Address MAP End
0xB2	Legacy Option ROM Initialization
0xB3	System Reset
0xB4	USB hot plug
0xB5	PCI bus hot plug
0xB6	Clean-up of NVRAM
0xB7	Configuration Reset (reset of NVRAM settings)
0xB8 – 0xBF	Reserved for future AML codes
0xC0 – 0xCF	OEM BDS initialization codes
0xD0	CPU initialization error
0xD1	North Bridge initialization error
0xD2	South Bridge initialization error
0xD3	Some of the Architectural Protocols are not available
0xD4	PCI resource allocation error. Out of Resources
0xD5	No Space for Legacy Option ROM
0xD6	No Console Output Devices are found
0xD7	No Console Input Devices are found
0xD8	Invalid password
0xD9	Error loading Boot Option (Load Image returned error)
0xDA	Boot Option is failed (Start Image returned error)
0xDB	Flash update is failed
0xDC	Reset protocol is not available
0xDD DXE	phase BMC self-test failure
0xE0	S3 Resume is started (S3 Resume PPI is called by the DXE IPL)
0xE1	S3 Boot Script execution
0xE2	Videos repost
0xE3	OS S3 wake vector call

POST Code	Description
0xE4-0xE7	Reserved for future AML progress codes 0xE8 S3 Resume Failed
0xE9	S3 Resume PPI not Found
0xEA	S3 Resume Boot Script Error
0xEB	S3 OS Wake Error
0xEC-0xEF	Reserved for future AML error codes
0xF0	Recovery condition triggered by firmware (Auto recovery)
0xF1	Recovery condition triggered by user (Forced recovery)
0xF2	Recovery process started
0xF3	Recovery firmware image is found
0xF4	Recovery firmware image is loaded
0xF5-0xF7	Reserved for future AML progress codes
0xF8	Recovery PPI is not available
0xF9	Recovery capsule is not found
0xFA	Invalid recovery capsule
0xFB – 0xFF	Reserved for future AML error codes

Table 1.14: BIOS POST Codes