MITAC COMPUTING TECHNOLOGY CORP.

MB1-10AP

User Manual V1.4

Master Series Embedded System

Intel® Apollo Lake Processors

Efficient, Versatile, and Rugged & Reliable

PREFACE

Copyright Notice

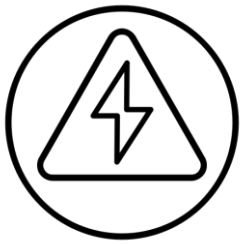
Disclaimer

We reserve the right to make changes, without notice, to any product, including circuits and/or software described or contained in this manual in order to improve design and/or performance. We assume no responsibility or liability for the use of the described product(s) conveys no license or title under any patent, copyright, or masks work rights to these products, and make no representations or warranties that these products are free from patent, copyright, or mask work right infringement, unless otherwise specified. Applications that are described in this manual are for illustration purposes only. We make no representation or guarantee that such application will be suitable for the specified use without further testing or modification.

Declaration of Conformity

FC	**FCC** 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 installed 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 him own expense.
CE	**CE** This equipment is in conformity with the requirement of the following EU legislations and harmonized standards. Product also complies with the Council directions.

Safety Information

	**WARNING! / AVERTISSEMENT!** 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/ATTENTION** 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.

Safety Precautions

For your safety, please carefully read all the safety instructions before using the device. All cautions and warnings on the equipment should be noted. Keep this user manual for future reference.

***Let service personnel to check the equipment in case any of the following problems appear:**

- The power cord or plug is damaged.
- Liquid has penetrated into the equipment.
- The equipment has been exposed to moisture.
- The equipment does not work well or you cannot get it to work according to the user manual.
- The equipment has been dropped and damaged.
- The equipment has obvious signs of breakage on the surface.

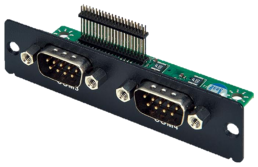
Ordering Information

Model Number	Description
MB1-10AP-N3350	Fanless embedded system with Intel® Apollo Lake N3350 processor. 1x204Pin DDR3L SO-DIMM 1857Mhz up to 8GB, 1xHDMI, 3xGbE LAN, 4xUSB3.0, 2xCOM, 8~24V DC-in, with wall mount, L6 system.
MB1-10AP-N3350-POE	Fanless embedded system with Intel® Apollo Lake N3350 processor. 1x204Pin DDR3L SO-DIMM 1857Mhz up to 8GB, 1xHDMI, 1xGbE LAN, 2xPoE LAN, 4xUSB3.0, 2xCOM, 8~24V DC-in, with wall mount, L6 system.
MB1-10AP-N4200	Fanless embedded system with Intel® Apollo Lake N4200 processor. 1x204Pin DDR3L SO-DIMM 1857Mhz up to 8GB, 1xHDMI, 3xGbE LAN, 4xUSB3.0, 2xCOM, 8~24V DC-in, with wall mount, L6 system.
MB1-10AP-N4200-POE	Fanless embedded system with Intel® Apollo Lake N4200 processor. 1x204Pin DDR3L SO-DIMM 1857Mhz up to 8GB, 1xHDMI, 1xGbE LAN, 2xPoE LAN, 4xUSB3.0, 2xCOM, 8~24V DC-in, with wall mount, L6 system.

Packing List

Item	Description	Q'ty
1	MB1-10AP Embedded System	1
2	Wall Mount Brackets (2 pcs in 1 set)	1
3	Driver CD	1
4	Full to Half Size mPCIe Card Adapter Plate	1
5	3-pin Terminal Block Power Connector	1
6	Quick Installation Guide	1

Optional Xpansion Modules

Model Number	Description
MS-01VGA-D10 	Xpansion Module with VGA Port
MS-01DVI-D10 	Xpansion Module with DVI-D Port
MS-01DPN-D10 	Xpansion Module with DisplayPort
MS-02COM-D10 	Xpansion Module with 2 x RS232/422/485 (Non-isolation) Support 5V/12V Power
MS-08DIO-T10 	Xpansion Module with 8-bit Isolated DIDO (4 x DI, 4 x DO)

CONTENTS

INTRODUCTION

1

This chapter provides the MB1-10AP Embedded System product overview, including features, hardware and mechanical specifications.

CHAPTER 1: INTRODUCTION

This chapter provides the MB1-10AP Embedded System product overview, including features, hardware, mechanical specifications, and I/O placement.

1.1 Overview

MiTAC's MB1-10AP embedded system is the next generation embedded system with Intel® Apollo Lake embedded processor. The efficient performance, OCP/OVP power protection, and expandable design provide the solution for routine tasks and most types of application.

1.2 Product Features

MB1-10AP Embedded System offers the following features:

- Intel® Apollo Lake-M N3350/N4200 Processors
- Support 2 x PoE LAN (Optional)
- Support HDMI as primary display, and VGA/DisplayPort/DVI-D as second option
- Fan-less chassis and Expandable module design
- Support COM/DIO via Xpansion Modules
- 8-24V Wide Power Voltage
- -25°C to 70°C (For non-PoE SKU, with 0.7m/s Air Flow and Wide Temperature Memory/Storage)
  -25°C to 60°C (For PoE SKU, with 0.7m/s Air Flow and Wide Temperature Memory/Storage)

1.3 Hardware Specification

SYSTEM	
CPU	Intel® Apollo Lake-M N3350 / N4200 Processors
Chipset	Intel® SoC Integrated
System Memory	DDR3L 1866 MHz / 1 x 204-pin SO-DIMM / Max. 8GB (Non-ECC)
Graphics	Intel® HD Graphics
Display Interface	HDMI 1.4 / Optional DisplayPort / VGA / DVI-D by Xpansion Module
Storage Slot	1 x 2.5 HDD / SSD (Default w/ HDD Bracket) 1 x mSATA
Ethernet	2 x Intel® I210-IT Giga LAN (2 x PoE LAN: Optional) 1 x Realtek RTL8154 LAN (Up to 480Mbps)
Audio	Realtek® ALC662
I/O Chipset	Nuvoton NCT6116D
TPM	Nuvoton NPCT750AAAYX TPM2.0 (Optional)
Expansion Slot	LTE/Wireless: Mini PCIe Full size (USB / PCIe), w/ SIM Card Holder (w/ Full to Half size adapter plate) Storage: mPCIe Full size (USB / PCIe / SATA)
Indicator	Power LED, HDD LED
FRONT I/O	1 x HDMI 1.4 4 x USB 3.0 1 x Xpansion Module Door 2 x RS232 / 422 / 485 (Support Power 5V / 12V) 2 x SMA Antenna (Optional for WiFi/LTE function)
REAR I/O	3 x RJ-45 1 x Mic-in & 1 x Line-out 1 x 2-pin Remote Power On/Off Header 1 x 3-pin Terminal Block Power Input 2 x SMA Antenna (Optional for WiFi/LTE function)
Watchdog Timer	1~255 Steps by Software Program
POWER REQUIREMENT	
Power Input	8~24V Wide Rage DC Input w/ Terminal Block Connectivity
MECHANICAL	
Thermal Design	Fanless
Mounting	Wall mount
Dimension	6.9” x 4.1” x 2.2” (170 x 105 x 57 mm)
Material	Top cover: Aluminum Alloy , Bezel and chassis: Steel
ENVIRONMENTAL	

Operating Temperature	-25°C to 70°C (For non-PoE SKU) -25°C to 60°C (For PoE SKU) with 0.7m/s Air Flow and Wide Temperature Memory/Storage
Operating Humidity	10%~90% R/H (Non-condensing)
Vibration Resistance	Operating, 5 Grms, 5-500 Hz, 3 Axes (w/ SSD, according to IEC60068-2-64)
Shock Resistance	Operating, 50 Grms, Half-sine 11 ms Duration (w/ SSD, according to IEC60068-2-27)
Certification	CE & FCC
OS	
OS Support	Windows® 10 64-bit, Linux (support by request)

**Notes[1]: Installation in Restricted Access Location (RAL)*
A restricted access location is a designated area within an incident area (High or Low temperature environment)
With authorized people can enter for a period of time and for a specific purpose.

1. *Access can only be gained by service people or by users who have been instructed about the reasons for the Restrictions applied to the location and about any precautions that shall be taken.*
2. *Access is through the use of a tool or lock and key, or other means of security, and is controlled by the authority Responsible for the location.*

**Notes[2]: Please make sure that the power consumption is in the spec of the power supply output capability from AC adaptor (72W or 120W). Please choose the suitable AC adaptor for your application.*

AC/DC 24V/5A, 120W 3PIN Terminal Block Power Adaptor (For PoE SKU)

AC/DC 24V/3A, 72W 3PIN Terminal Block Power Adaptor (For non-PoE SKU)

**Note[3]: Please choose 120W AC adaptor for the Optional Xpansion Module (MS-02COM-D10) COM ports in maximum power loading scenario (12V max. 1A loading).*

**Note[4]: Please don't load the COM power in the hardware configuration and high temperature condition. Don't operate the machine at maximum operating temperature 70℃ (Non-PoE SKU) & 60℃(PoE SKU) with 4*COM 12V*1A loading.*

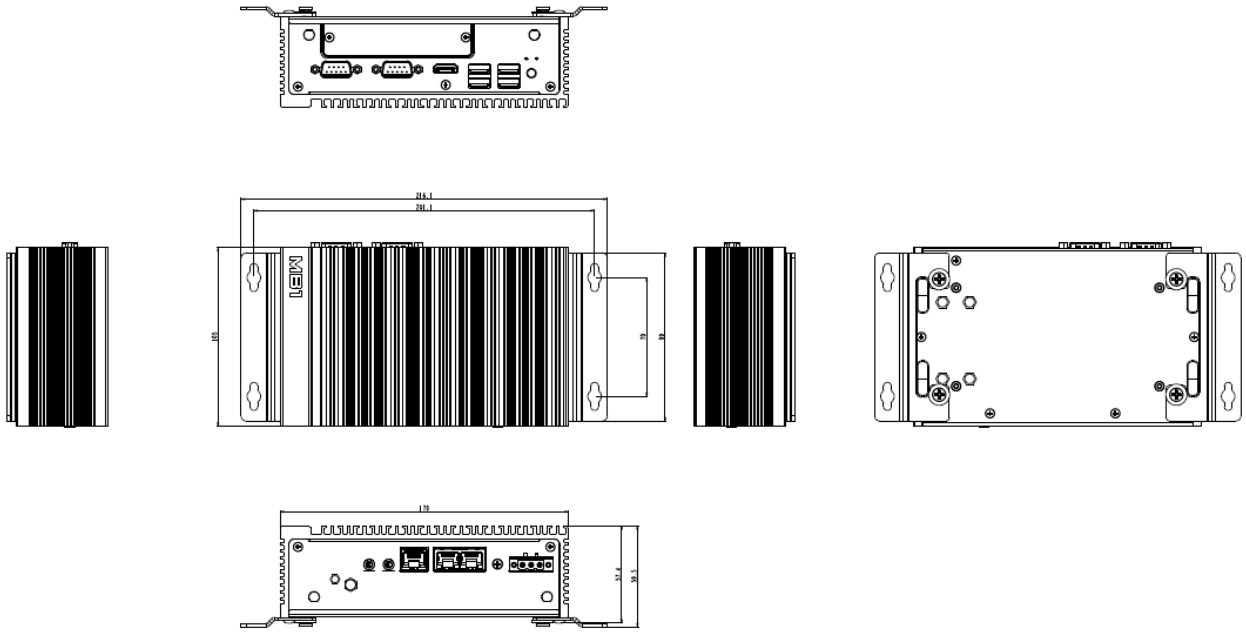
**Note[5]: The maximum ambient operating temperature is 40°C if the external AC adapter model: EA11011M or EA10681V will be placed in the same high temperature area with the embedded system.*

**Note[6]: CAUTION - Lithium battery is included in this embedded system. Please do not puncture, mutilate, or dispose of battery in fire. There will be danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by manufacturer. Dispose of used battery according to manufacturer instructions and in accordance with your local regulations.*

**Note[7]: CAUTION - Only allow technically qualified personnel to touch the I/O surface, and only when the unit is well fastened by wall mount, VESA mount, or DIN Rail mount. Please also avoid to contact the I/O surface more than 1 second in high temperature and harsh environment. Not allow to touch aluminum alloy surface at high temperature. The technically qualified personnel also needs to have technical knowledge, operating experiences, and basic knowledge about MB1-10AP product spec.*

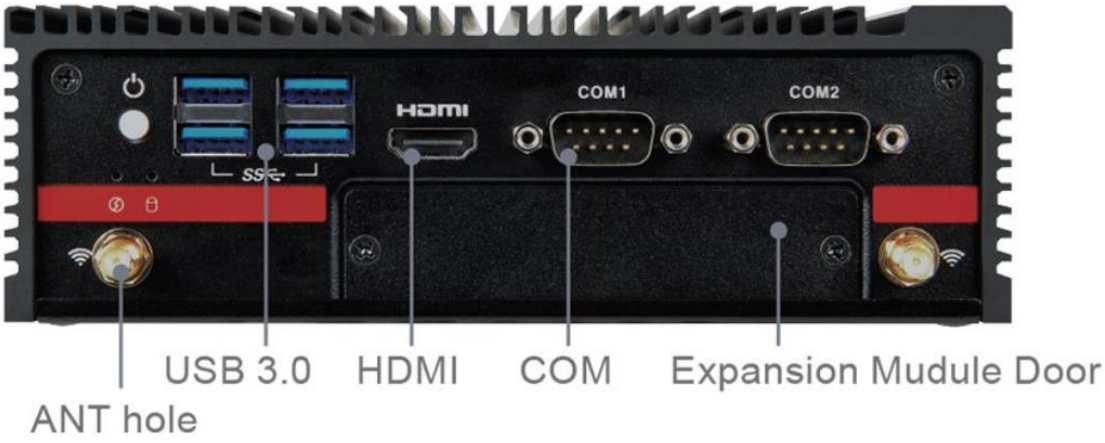
1.4 Mechanical Specification

- Mechanical Dimension: 170 mm x 105 mm x 57 mm

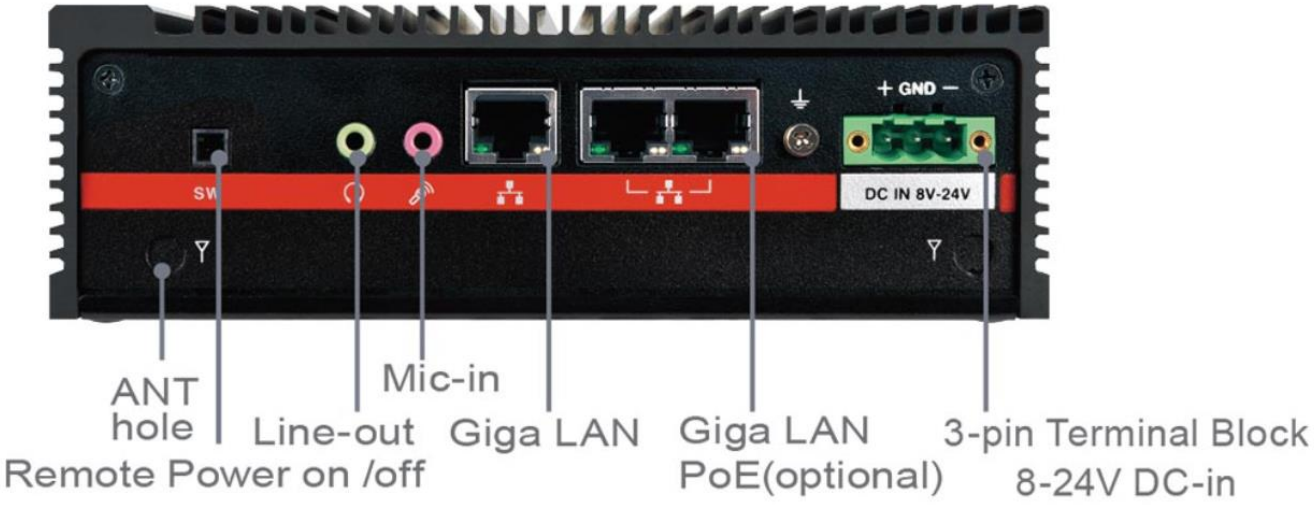


1.5 System I/O Placement

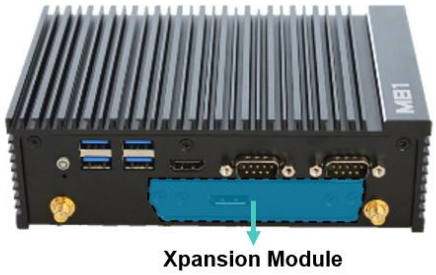
- **Front I/O:**

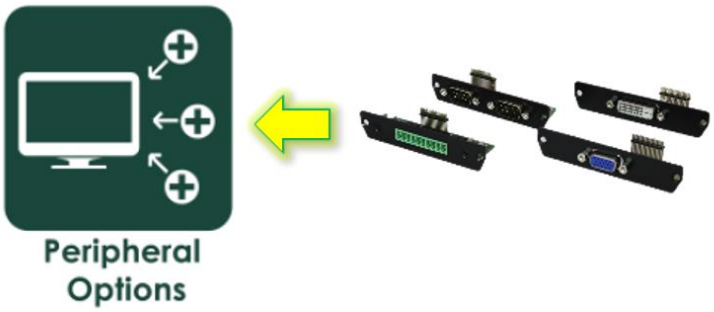


- **Rear I/O:**



■ Xpansion Module (Optional) Configuration





Model Number	Function	Supports
MS-01VGA-D10	VGA Port Expansion	V
MS-01DVI-D10	DVI-D Port Expansion	V
MS-01DPN-D10	DisplayPort Expansion	V
MS-02COM-D10	2 x RS232/422/485; Supports 5V/12V	V
MS-08DIO-T10	Digital I/O Expansion 8-bit DIDO (4 x DI, 4 x DO)	V

DIP SWITCH SETTING AND PIN DEFINITION

2

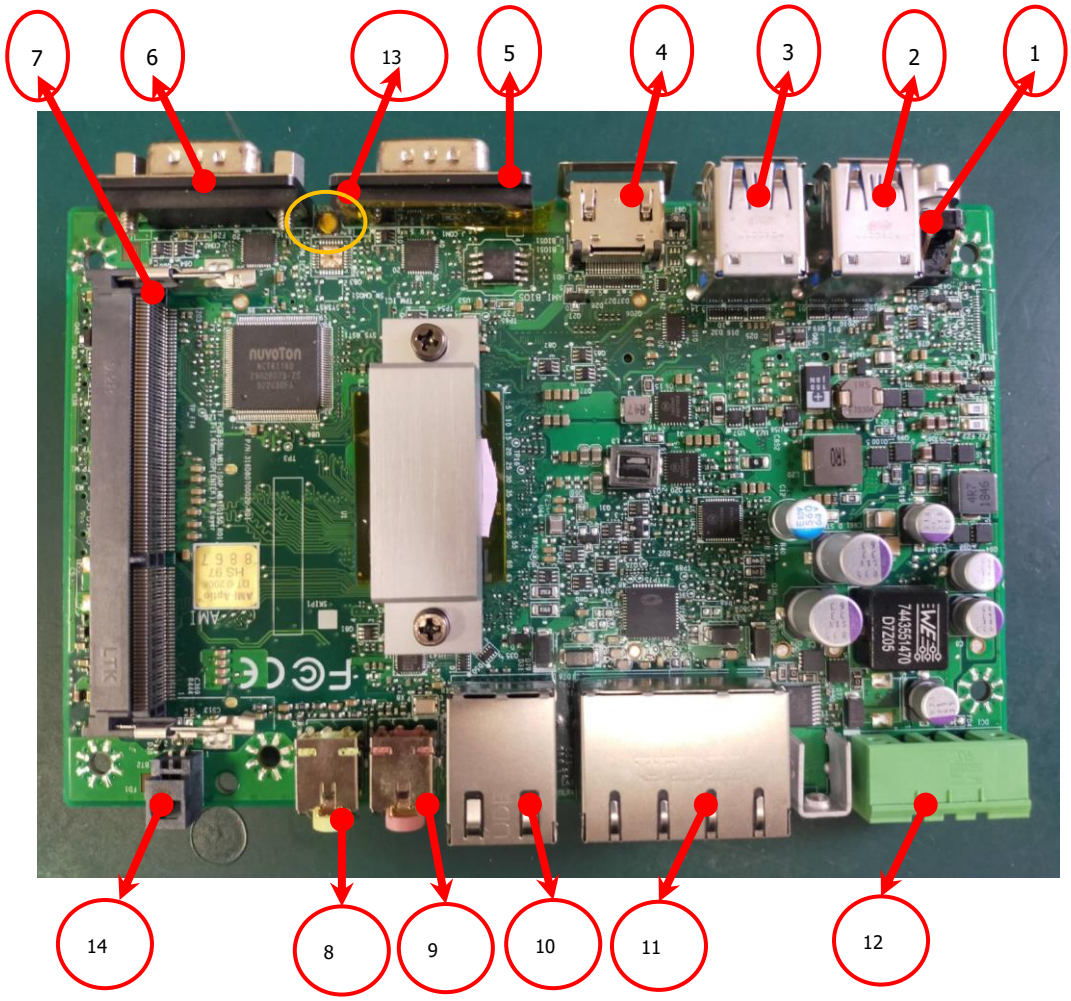
This chapter provides information about how to set up the dip switch and use I/Os of MB1-10AP Embedded System hardware.

CHAPTER 2: DIP SWITCH SETTING AND PIN DEFINITION

This chapter provides information about how to set up the dip switch, and use internal I/Os of MB1-10AP Embedded System hardware.

2.1 DIP Switch and Connector Overall Placement

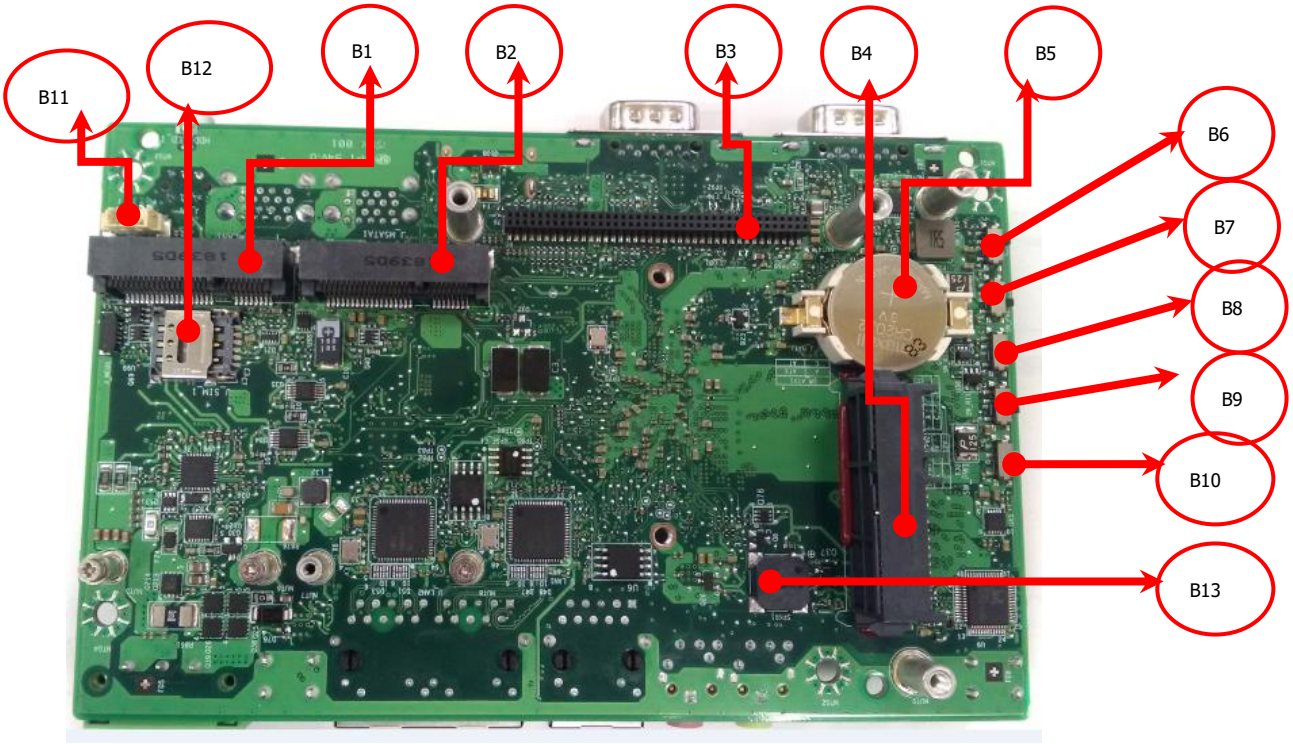
Front View:



1	Power button
2	Dual USB3.0
3	Dual USB3.0
4	HDMI
5	COM port
6	COM port
7	DDR3L SO-DIMM
8	Line-out Audio Jack

9	Mic-in Audio Jack
10	RJ45 10/100/1G
11	Dual RJ45 10/100/1G (Non PoE or PoE)
12	3-pin Terminal Block DC IN
13	SW_CMOS1
14	Remote Power on/off Header

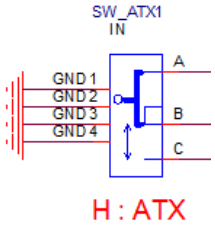
Bottom View:



B1	J_WLAN1
B2	J_MSATA1
B3	J_DB1
B4	J_SATA1
B5	J_BAT1
B6	AT/ATX Switch
B7	SW_PW2
B8	SW_RI2
B9	SW_RI1
B10	SW_PW1
B11	J_PW1
B12	J_SIM_1
B13	Buzzer

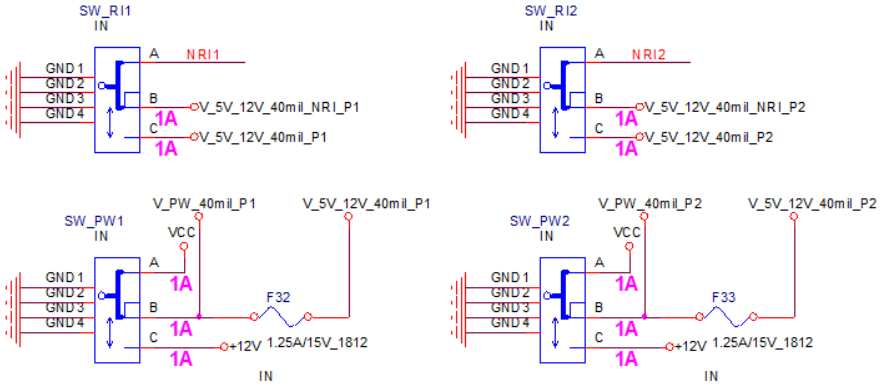
2.2 DIP Switch Setting

■ Location #B6



SW_ATX1	
A	ATX
C	AT

■ Location #B7/B8/B9/B10

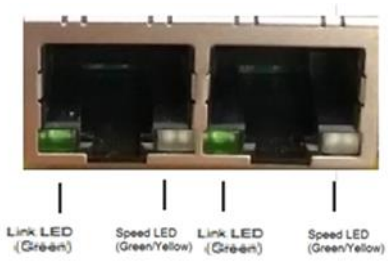


SW_RI1	SW_RI2
A	RI
C	PWR

SW_PW1	SW_PW2
A	5V
C	12V

2.3 Connector Pin Definition

■ Indicator for Dual Intel i210-IT LAN

Diagram	LED	Color	State	Condition
	Link	NA	off	LAN link is not established or LAN disable
	Link	Green	on	LAN link is established or LAN port disable
	Link	Green	blinking	LAN activity occurring
	Speed	NA	off	10 M b/s data rate or LAN disable
	Speed	Green	on	100 M b/s data rate
	Speed	Orange	on	1000 M b/s data rate or LAN port disable

■ Indicator for Realtek RTL8154B LAN

S0		
	(Activity LED)	(Speed LED)
LAN LED	Left-Green	Right-Green
10Mb	ON(Green Blink)	OFF
100Mb	ON(Green Blink)	Green
1000Mb	ON(Green Blink)	Green Blink
Disconnected	OFF	OFF

■ Location #B4 – SATA and SATA PWR Connector

Pin	Signal Name
P1	VCC3
P2	VCC3
P3	VCC3
P4	GND

P5	GND
P6	GND
P7	VCC
P8	VCC
P9	VCC
P10	GND
P11	RES
P12	GND
P13	+12V
P14	+12V
P15	+12V
S1	GND
S2	SATAHDR_TXP0_C
S3	SATAHDR_TXN0_C
S4	GND
S5	SATAHDR_RXN0_C
S6	SATAHDR_RXP0_C
S7	GND

■ 3-pin terminal block for DC Input

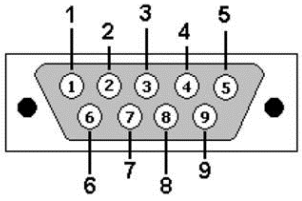
Pin	Signal
1	DC IN +8~24VIN
2	GND
3	-

■ 2-pin Remote Power On/Off Header

Pin	Signal
1	Signal
2	GND

MB Side Connector: Molex 151064-0152
Suggestive Cable Side Plug: Molex 151100-0002

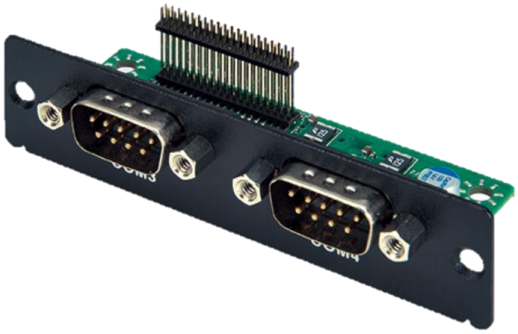
■ COM1 and COM2 on M/B



Pin No	RS-232	RS-422	RS-485
1	DCD	TX-	DATA-
2	RX	TX+	DATA+
3	RTX	RX+	NC
4	DTR	RX-	NC
5	GND	GND	GND
6	DSR	NC	NC
7	RTS	NC	NC
8	CTS	NC	NC
9	RI	NC	NC

MB COM1 and COM2 RS232, RS422, RS485 setting is at BIOS setup menu

■ MS-02COM-D10 (Optional)

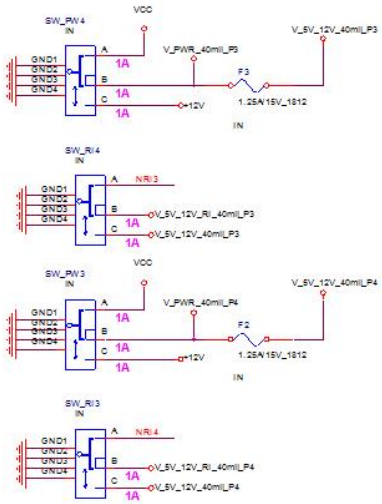


Xpansion Module with 2 x RS232/422/485 (Non-isolation)
Support 5V/12V DC Power Output

Notes: Don't support Power HOT switch at SW_PW3 and SW_PW4 in Xpansion Module
Below is Xpansion Module with COM3 and COM4: See the power RS232 setting as below table:

SW_RI3 SW_RI4	
A	RI
C	PWR

SW_PW3 SW_PW4	
A	5V
C	12V

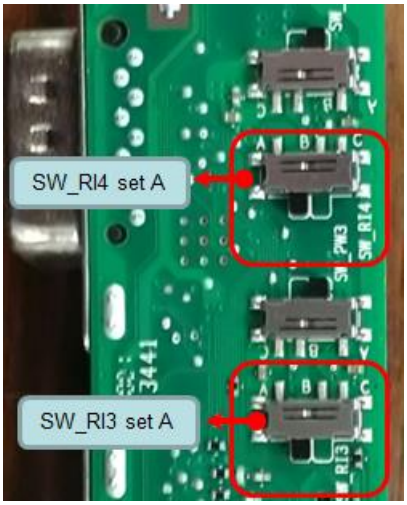


Default setting is RI signal at A location from SW_RI3 and SW_RI4

Power COM setting with RI signal: Default setting

SET at A location from SW_RI3 and SW_RI4

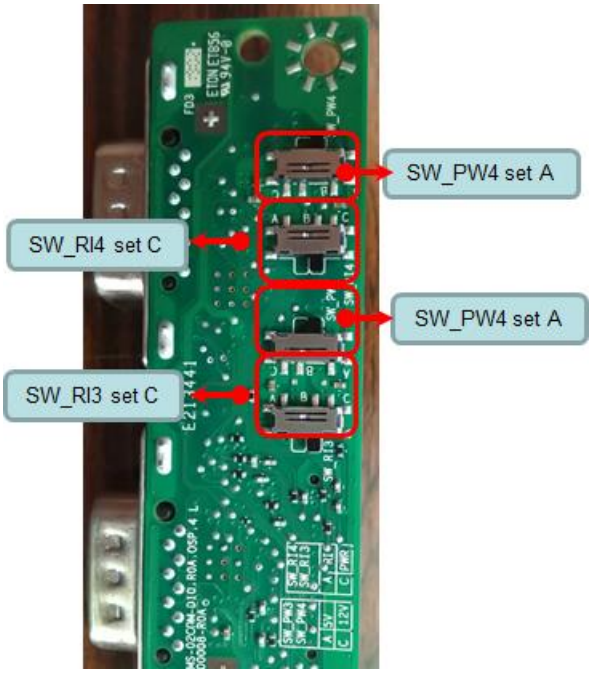
SET at A location from SW_PW3 and SW_PW4



Power 5V setting:

SET at C location from SW_RI3 and SW_RI4

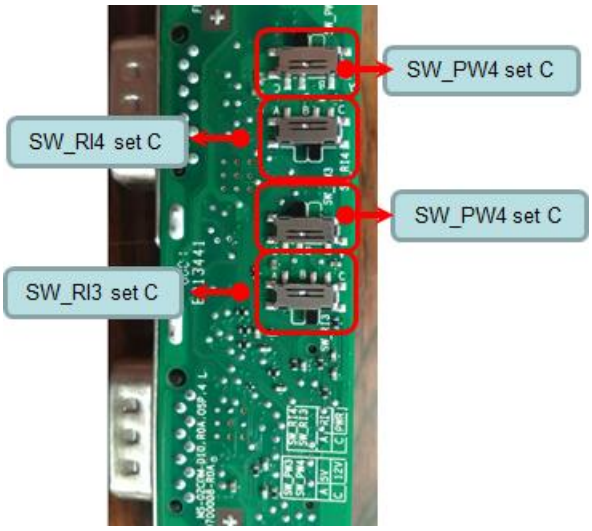
SET at A location from SW_PW3 and SW_PW4



Power 12V setting:

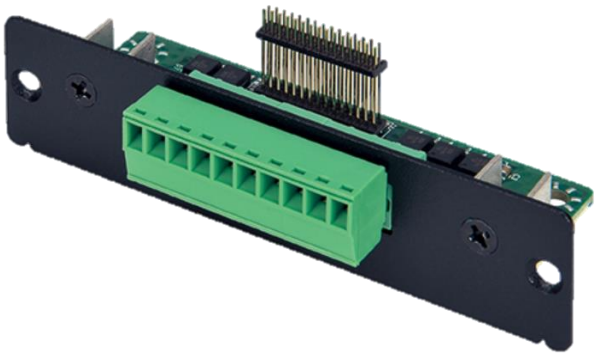
SET at C location from SW_RI3 and SW_RI4

SET at C location from SW_PW3 and SW_PW4



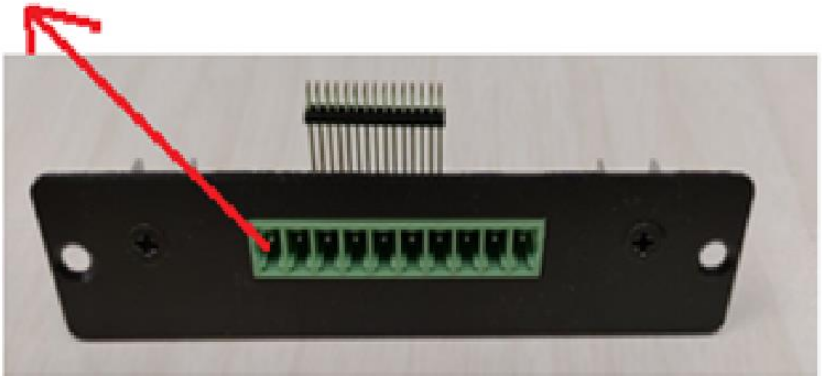
Power 12V setting: Change at C location from SW_RI3 and SW_RI4 and at C location from SW_PW3 and SW_PW4

■ MS-08DIO-T10 (Optional)



Xpansion Module with 8-bit Optical Isolation DIDO (4 x DI, 4 x DO)

1	2	3	4	5	6	7	8	9	10
V_ISO	ISO_DO_0	ISO_DO_1	ISO_DO_2	ISO_DO_3	ISO_DI_0	ISO_DI_1	ISO_DI_2	ISO_DI_3	GND_ISO



SYSTEM SETUP

This chapter provides information about how to set up the MB1-10AP Embedded System hardware installation.

3

CHAPTER 3: SYSTEM SETUP

This chapter provides information about how to set up the MB1-10AP Embedded System hardware installation.

⚠	Warning: The edge of MB1-10AP aluminum alloy fins is a little bit sharp. Please be careful when you move the unit, do the installation, and operate the embedded system!

3.1 2.5” SATA HDD/SSD Installation

Please follow the instructions to install SATA HDD as below.

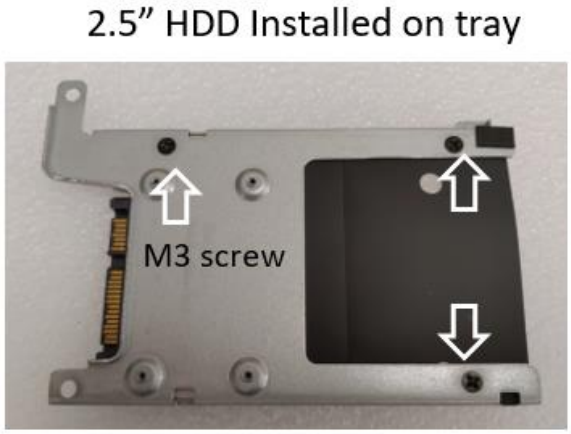
- Loosen 6 screws from Bottom cover as the arrow locations

- Loosen 4 screws as the arrow directions

- Move HDD tray as arrow direction

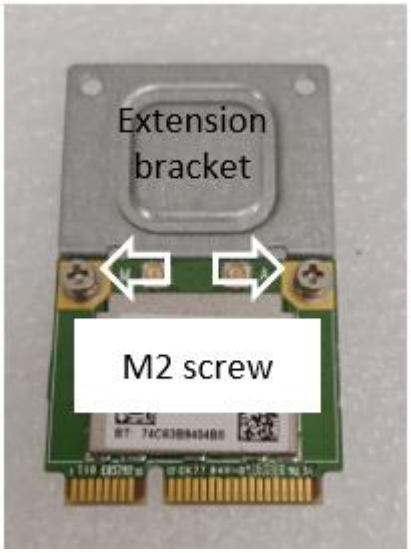
- Lift HDD tray about 45 degrees and draw it out

- Install 2.5”HDD to the HDD tray



3.2 WiFi module Installation

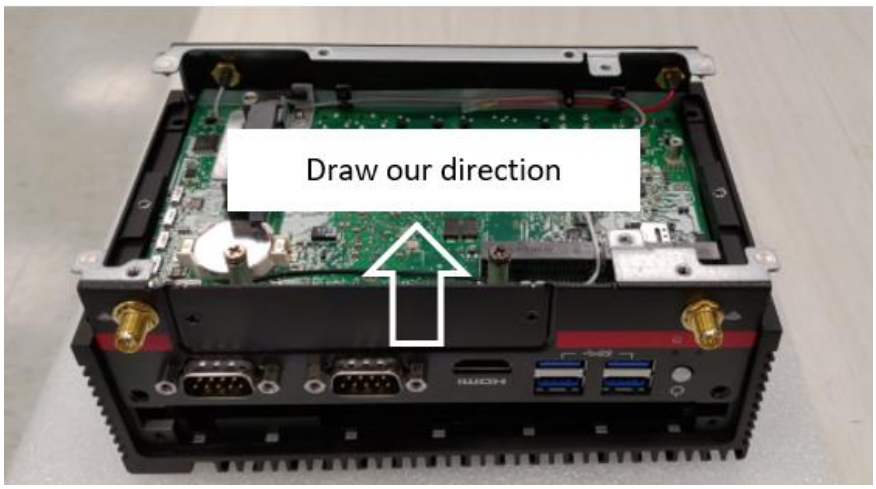
- Use mPCIe extension bracket which is in accessories kit to fix half size mPCIe wifi module, and install to the full size mPCIe slot



3.3 DRAM Installation

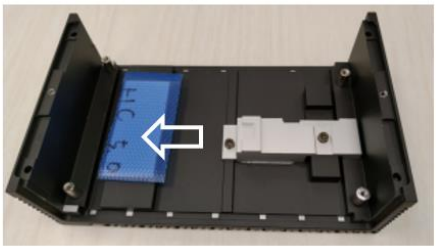
- Loosen 4 screws from MB (2 screws from front & rear cover)

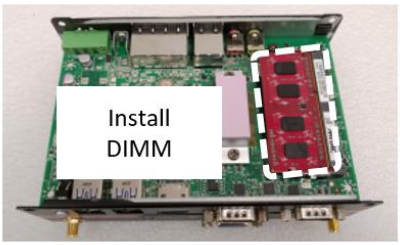
- Draw the MB sub-assembly out from top cover as arrow direction



- Remove the film from top cover & install DIMM to MB

Peel off the protective film





BIOS SETUP

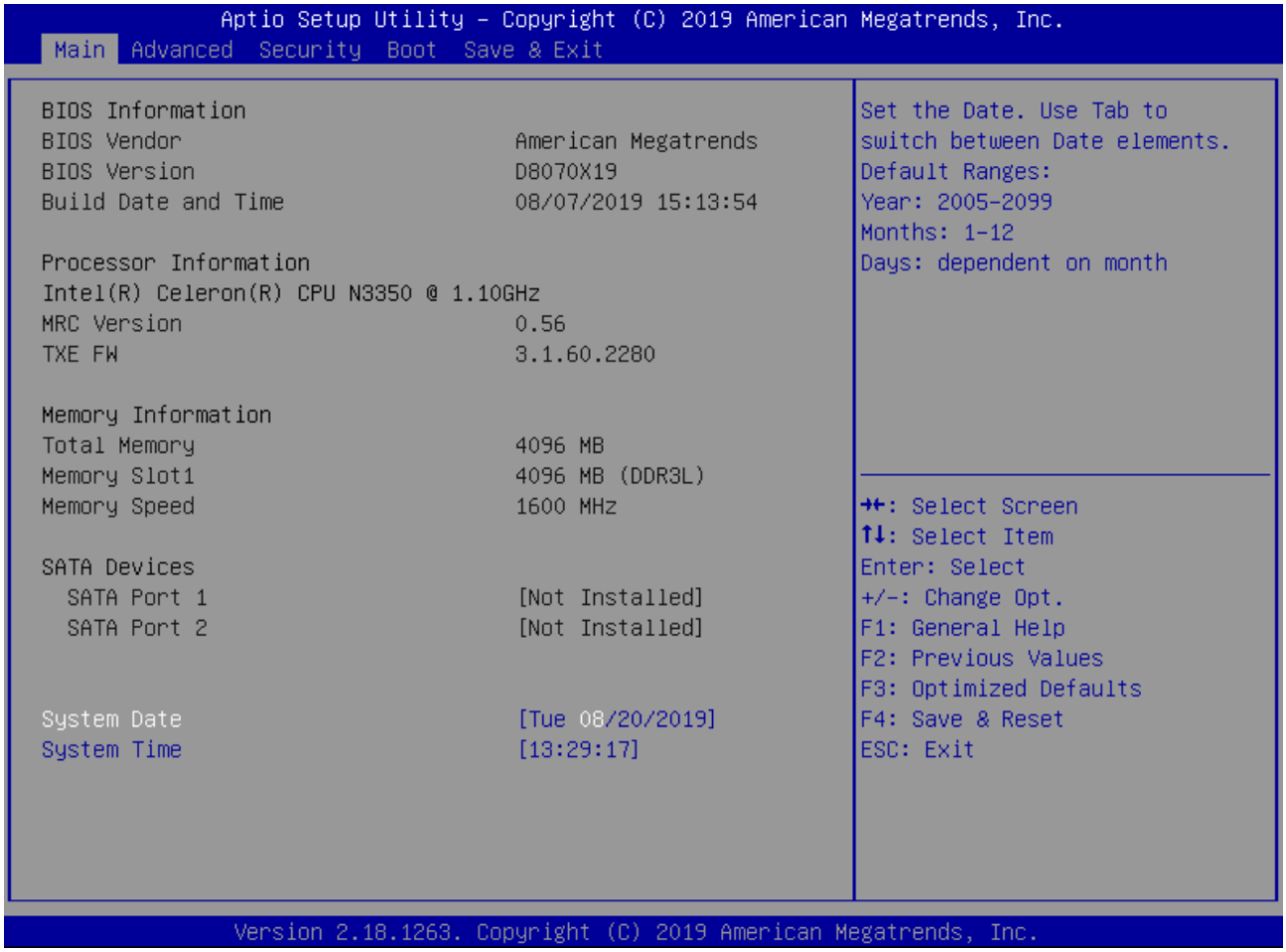
This chapter provides information about how to set up BIOS and use BIOS menu items to adjust basic function settings.

4

CHAPTER 4: BIOS SETUP

This chapter provides information about how to set up BIOS and use BIOS menu items to adjust basic function settings.

4.1 Main Page



Field Name	**BIOS Vender**
Default Value	AMI Megatrends
Comment	This field is not selectable. There is no help text associated with it.

Field Name	**BIOS Version**
Default Value	Display the version of the BIOS
Comment	This field is not selectable. There is no help text associated with it.

Field Name	**Build Date**
Default Value	Display build date of the BIOS
Comment	This field is not selectable. There is no help text associated with it.

Field Name	**ME (TXE) FW Version**
Default Value	ME Firmware Version.
Comment	This field is not selectable. There is no help text associated with it.

Field Name	**Processor Information**
Value	Display the installed CPU brand.
Comment	This field is not selectable. There is no help text associated with it.

Field Name	**Total Memory**
Value	Display the installed memory size.
Comment	This field is not selectable. There is no help text associated with it.

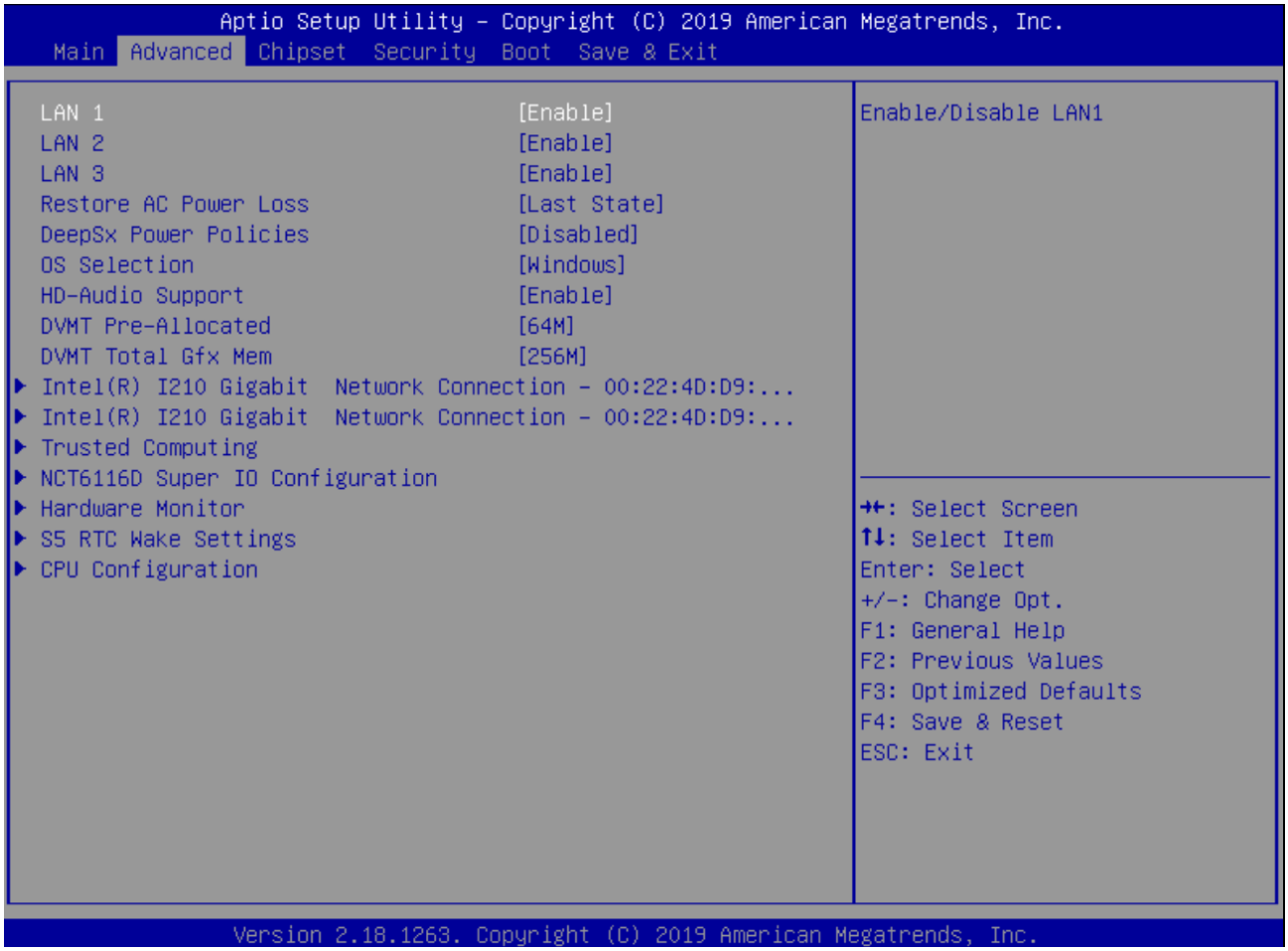
Field Name	**Memory Frequency**
Value	Display the installed memory frequency.
Comment	This field is not selectable. There is no help text associated with it.

Field Name	**SATA#1 / SATA#2**
Value	Display the installed SATA port device.
Comment	This field is not selectable. There is no help text associated with it.

Field Name	**System Date**
Default Value	[Www mm/dd/yyyy]
Possible Value	Www : Mon/Tue/Wed/Thu/Fri/Sat/Sun mm : 1-12 dd : 1-31 yyyy : 1998-9999
Help	Set the Date. Use Tab to switch between Date elements.

Field Name	**System Time**
Default Value	[hh :mm :ss]
Possible Value	hh : 0-23 mm : 0-59 ss : 0-59
Help	Set the Time. Use Tab to switch between Time elements.

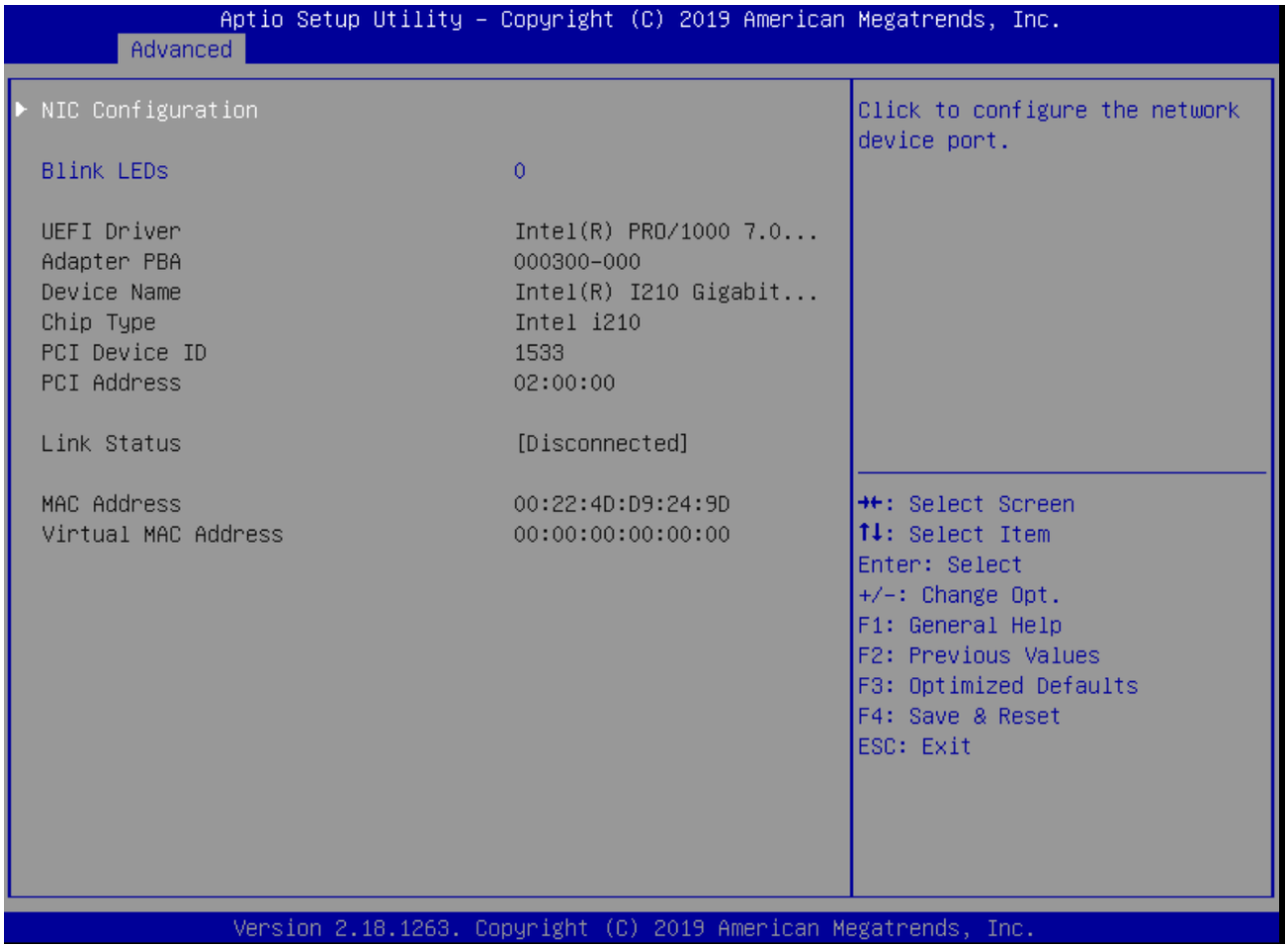
4.2 Advance Page



BIOS Setup Name	[Default] / Select Value	Description
LAN 1	Disabled / [Enabled]	Enable/Disable LAN1
LAN 2	Disabled / [Enabled]	Enable/Disable LAN2
LAN 3	Disabled / [Enabled]	Enable/Disable LAN3
Restore AC Power Loss	Turn on / Turn off / [Last state]	Select AC power state when power is re-applied after a power failure.
DeepSx Power Policies	[Disabled] / Enabled	Configure the DeepSx Mode configuration.
OS Selection	[Windows]/Intel Linux	Select the target OS
HD-Audio Support	Disabled / [Enabled]	Enable/Disable HD-Audio Support
DVMT Pre-Allocated	[64M]/ 128M / 256M / 512M	Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.
DVMT Total Gfx	128M /[256M] / Max	Select DVMT 5.0 Total Graphic Memory size used by

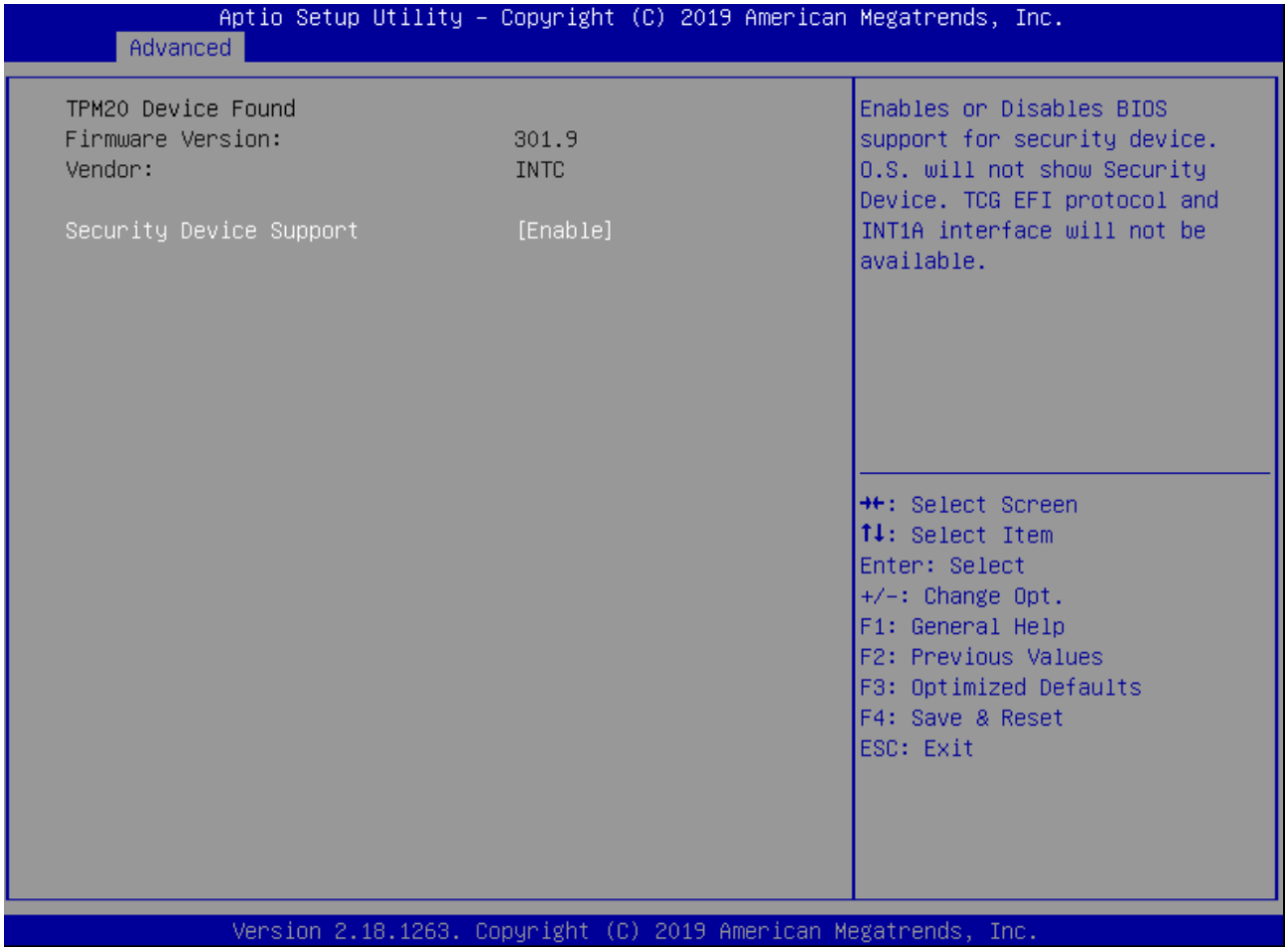
Mem		the Internal Graphics Device.
▸ **Intel(R) I210 Gigabit Network Connection**		Configure Gigabit Ethernet device parameters
▸ **Trusted Computing**		Select fTPM/dTPM
▸ **NCT6116D Super IO Configuration**		System Super IO Chip Parameters.
▸ **Hardware Monitor**		Monitor hardware status
▸ **S5 RTC Wake Setting**		Enable system to wake from S5 using RTC alarm
▸ **CPU Configuration**		CPU Configuration Parameters

4.2.1 Intel(R) I210 Gigabit Network Connection



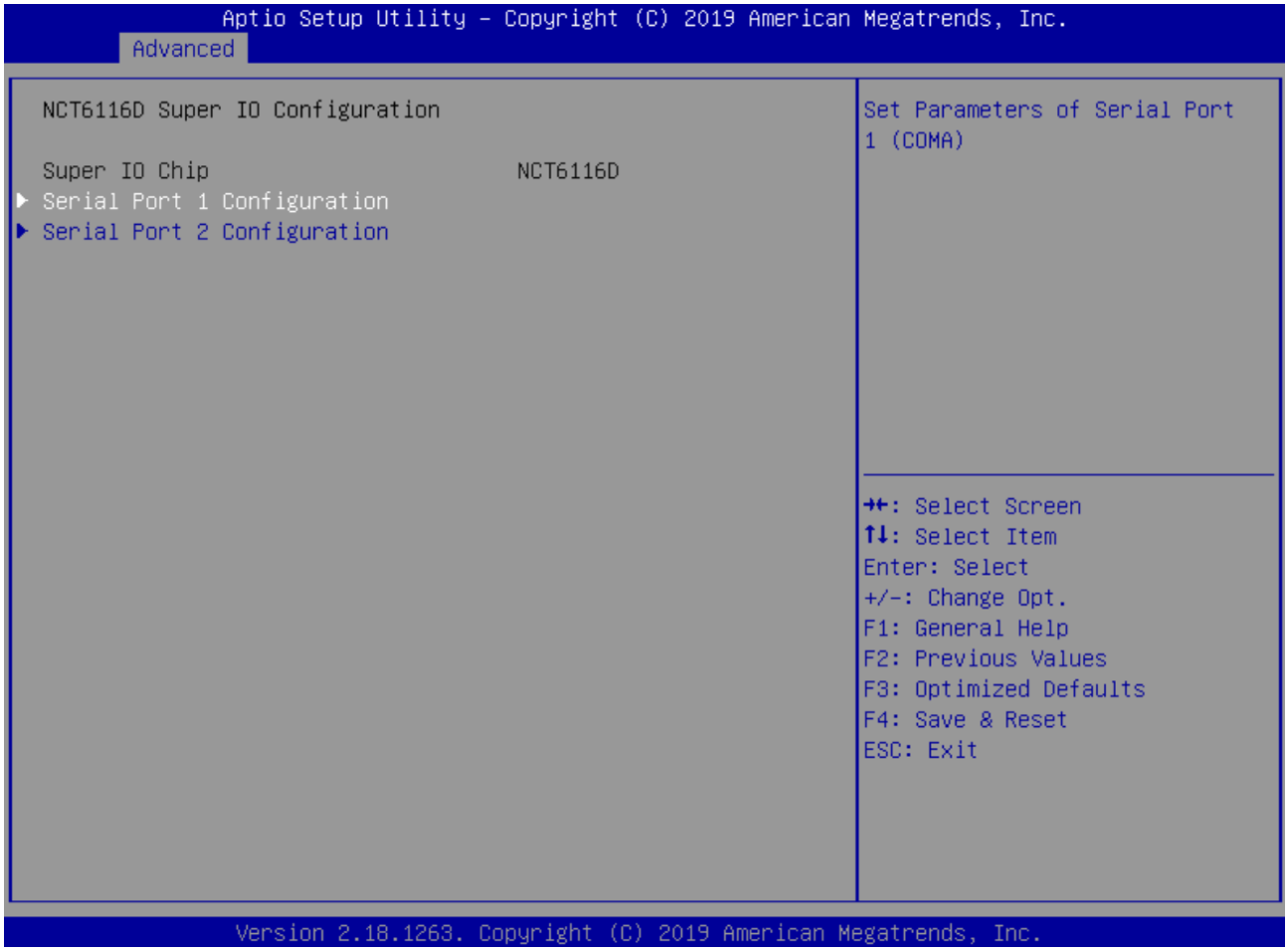
BIOS Setup Name	[Default] / Select Value
▸ Intel(R) I210 Gigabit Network Conection	
▸ NIC Configuration	
Link Speed	[Auto] / 10 Mbps Half / 10 Mbps Full / 100 Mbps Half /100 Mbps Full
Wake On LAN	Enabled / [Disabled]
▸ NIC Configuration	
Link Speed	[Auto] / 10 Mbps Half / 10 Mbps Full / 100 Mbps Half /100 Mbps Full
Wake On LAN	Enabled / [Disabled]

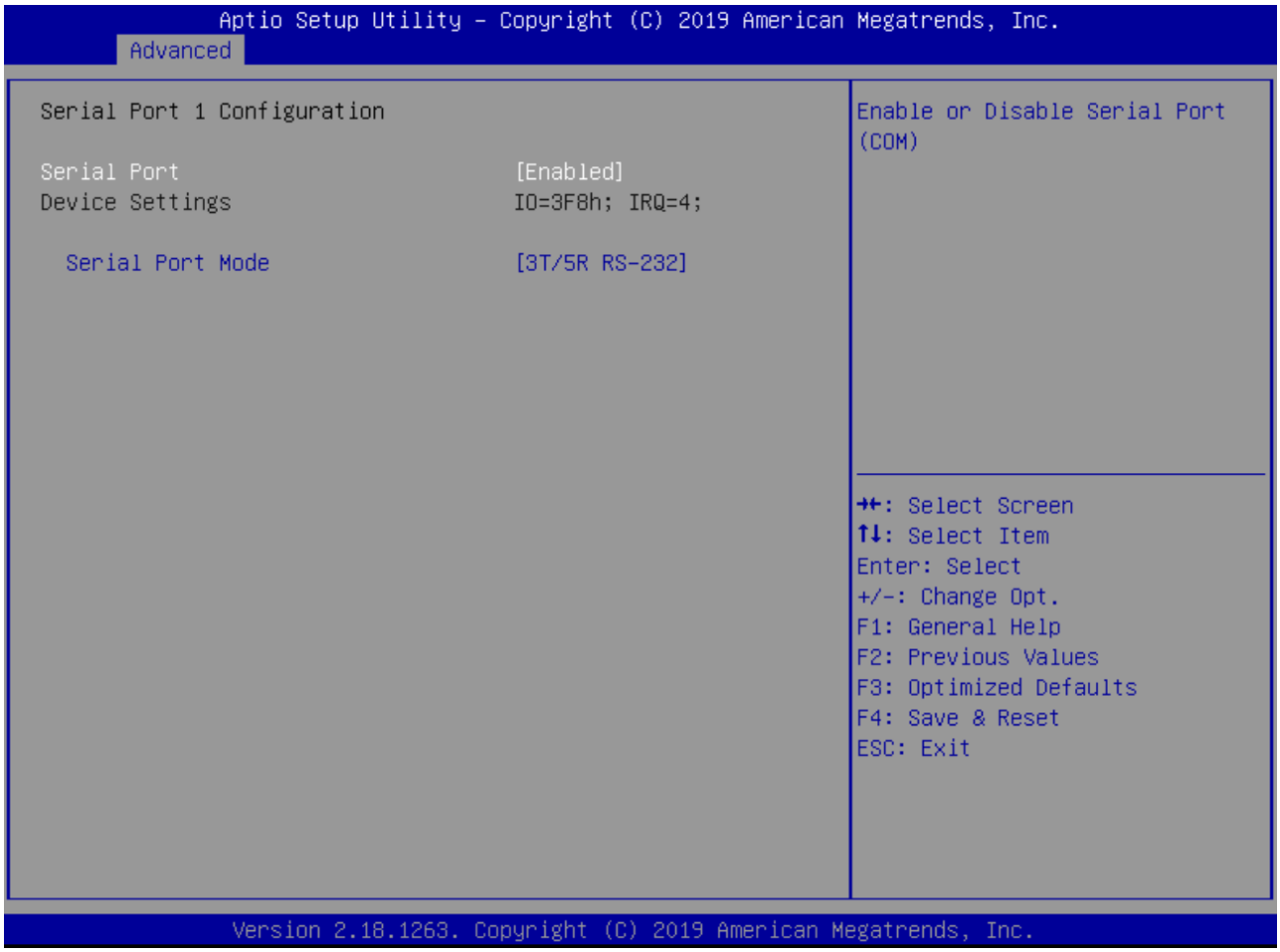
4.2.2 Trusted Computing



BIOS Setup Name	[Default] / Select Value	Description
Security Device Support	Disabled / [Enabled]	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.

4.2.3 NCT6116D Super IO Configuration

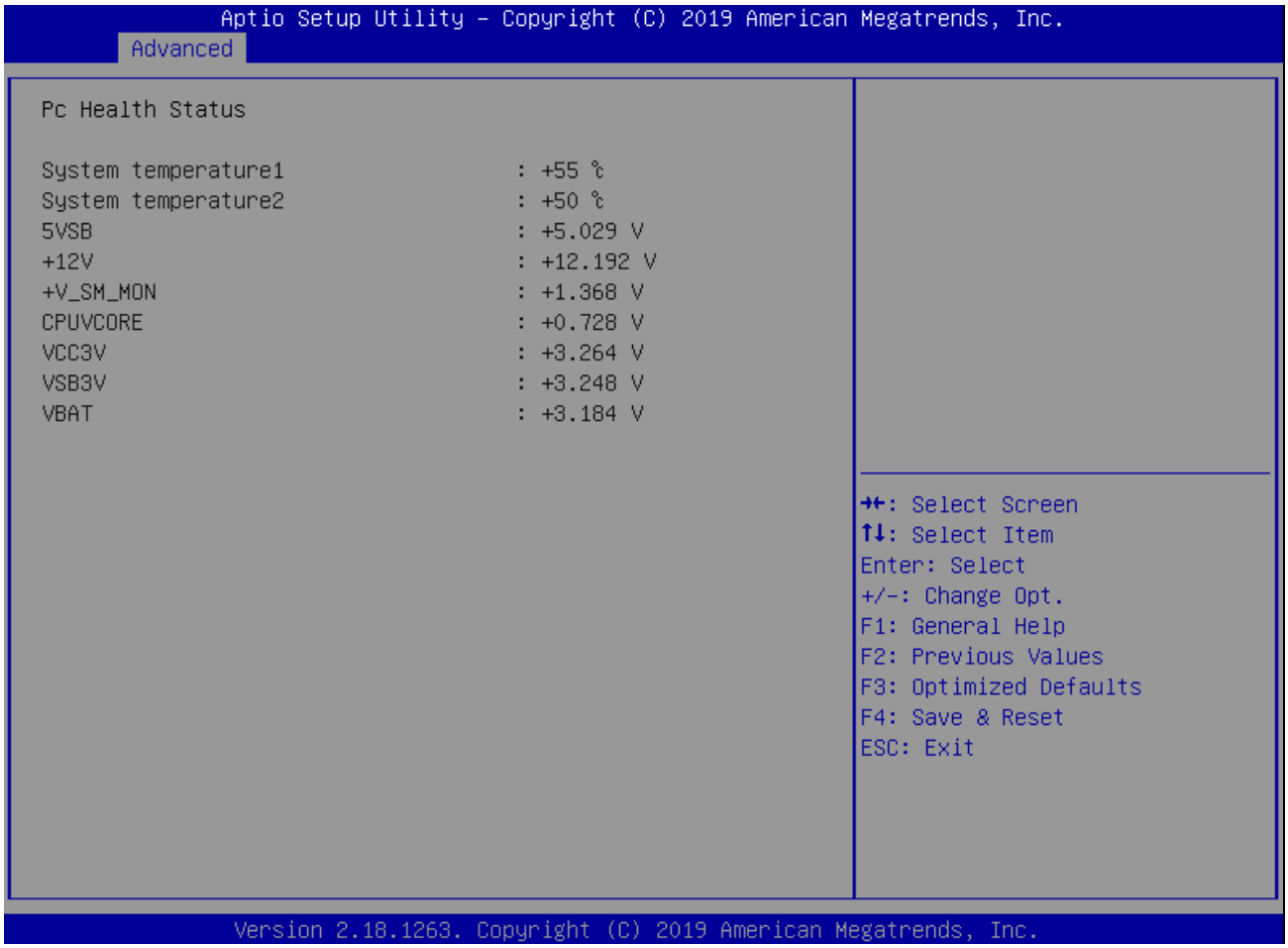

Aptio Setup Utility – Copyright (C) 2019 American Megatrends, Inc.
Advanced
NCT6116D Super IO Configuration
Super IO Chip NCT6116D
Serial Port 1 Configuration
Serial Port 2 Configuration
Set Parameters of Serial Port 1 (COMA)
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Reset
ESC: Exit
Version 2.18.1263. Copyright (C) 2019 American Megatrends, Inc.



BIOS Setup Name	[Default] / Select Value	Description
▸ NCT6116D Super IO Configuration		System Super IO Chip Parameters.
Super IO Chip	NCT6116D	
▸ Serial Port 1 Configuration		Set Parameters of Serial Port 1 (COMA)
Serial Port	[Enabled] / Disabled	Enable or Disable Serial Port (COM)
Device Settings	IO=3F8h; IRQ=4	
Serial Port Mode	1T/1R RS-422 / [3T/5R RS-232] / 1T/1R RS-485 TX ENABLE Low Active / 1T/1R RS-422 with termination resister / 1T/1R RS-485 with termination resister TX ENABLE Low Active / Disable	Select Serial Port Mode
▸ Serial Port 2 Configuration		Set Parameters of Serial Port 2 (COMC)

Serial Port	[Enabled] / Disabled	Enable or Disable Serial Port (COM)
Device Settings	IO=2F8h; IRQ=3	
Serial Port Mode	1T/1R RS-422 / [3T/5R RS-232] / 1T/1R RS-485 TX ENABLE Low Active / 1T/1R RS-422 with termination resister / 1T/1R RS-485 with termination resister TX ENABLE Low Active / Disable	Select Serial Port Mode

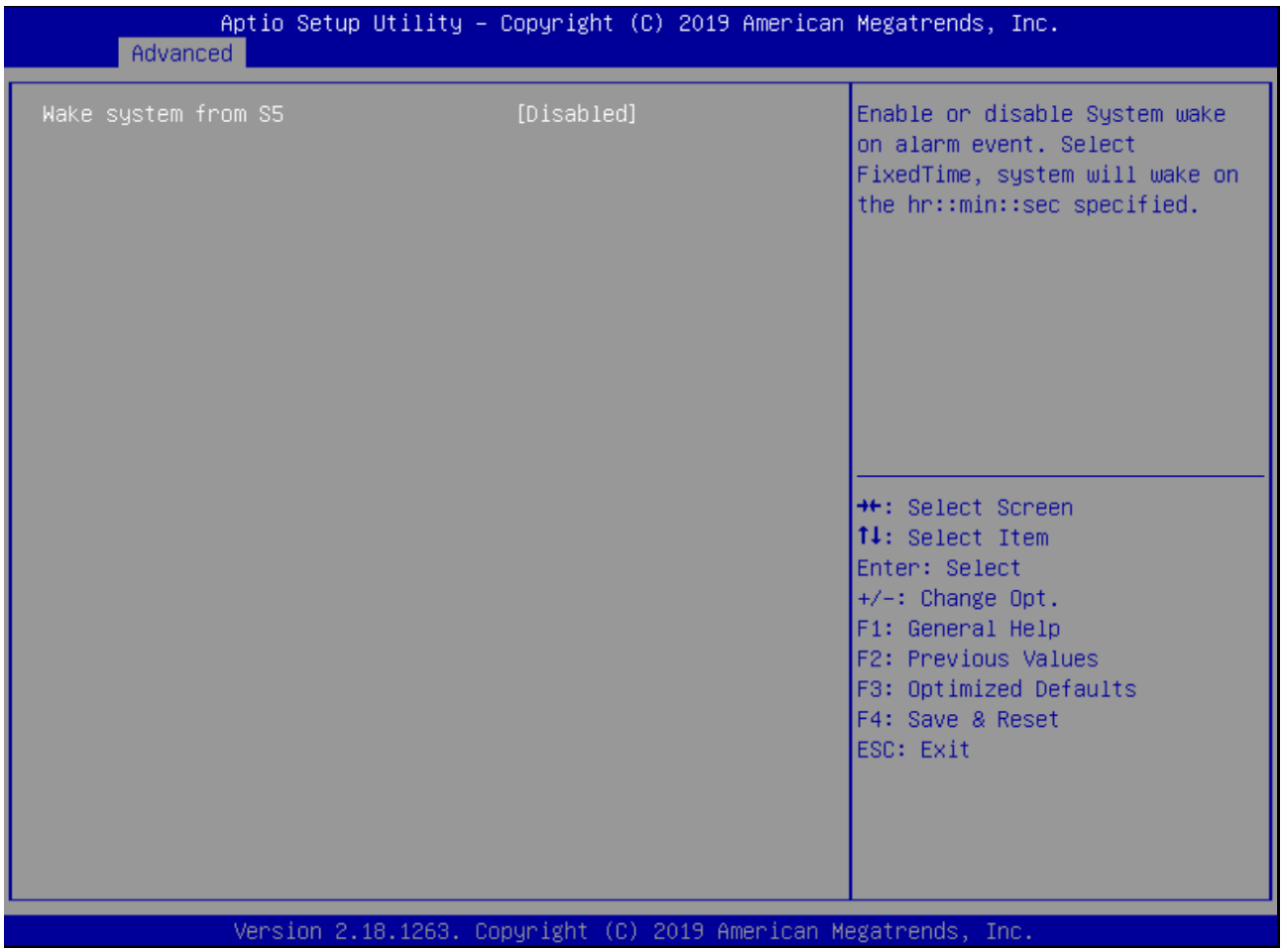
4.2.4 Hardware Monitor



PC Health Status	Value
System temperature1	+ xx C
System temperature2	+ xx C
3VSB	+ x.xxx V
V_SM_MON	+ x.xxx V

+12V	+ x.xxx V
AVSB	+ x.xxx V
CPUVCORE	+ x.xxx V
VCC3V	+ x.xxx V
VSB3V	+ x.xxx V
VBAT	+ x.xxx V

4.2.5 S5 RTC Wake Setting

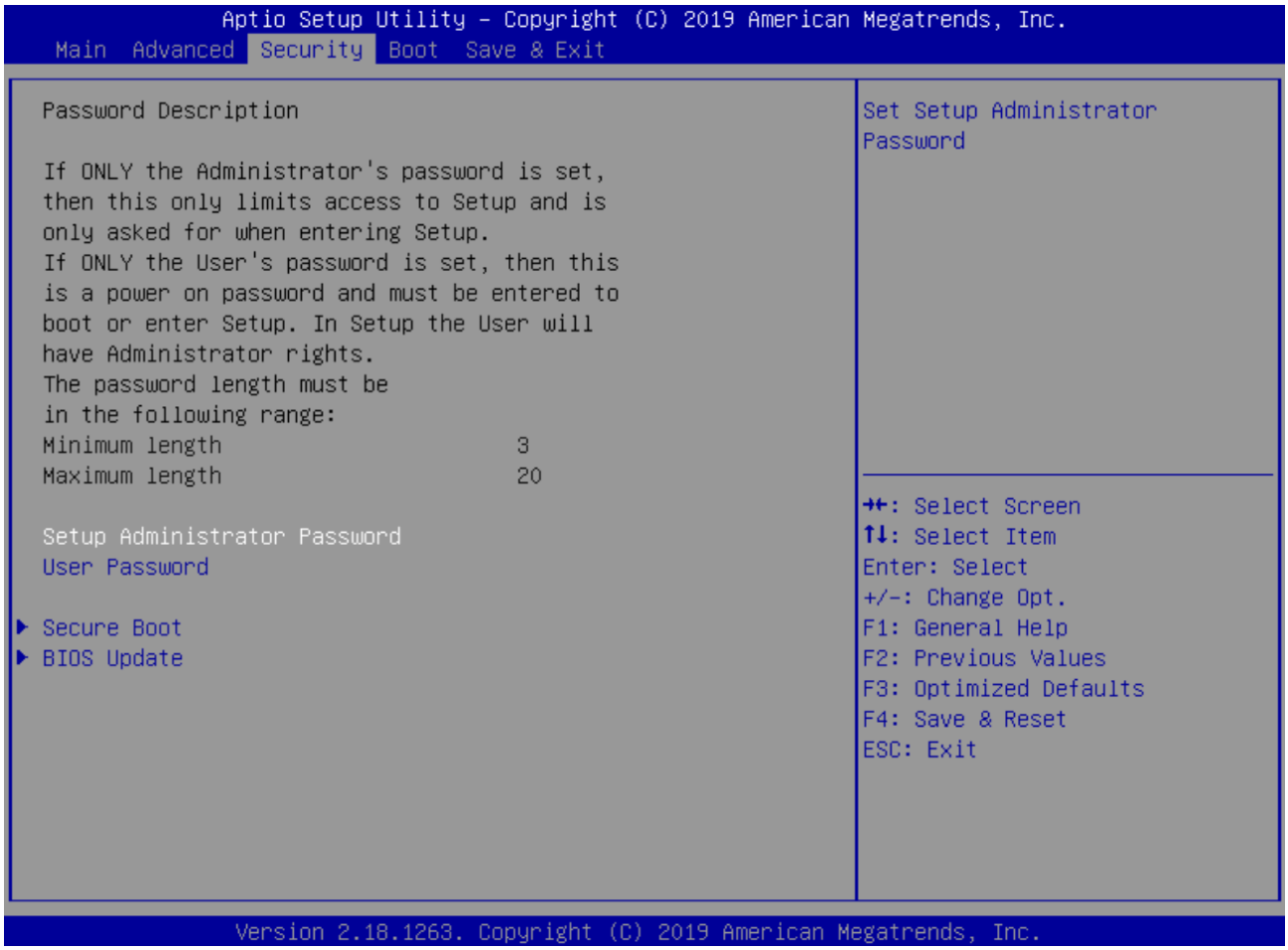


BIOS Setup Name	[Default] / Select Value	Description
Wake System from S5	[Disabled] / Fixed Time	Enabler or disable System wake on alarm event, Select FixedTime, system will wake on the hr::min::sec specified.
Wake up hour	[0] ~ 23	Select 0-23 For example enter 3 for 3am and 15 for 3pm
Wake up minute	[0] ~ 59	select 0 - 59 for Minute
Wake up second	[0] ~ 59	select 0 - 59 for Second

4.2.6 CPU Configuration

BIOS Setup Name	[Default] / Select Value	Description
Intel Virtualization Technology	Disabled / [Enabled]	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology
Burst Frequency	Disabled /[Enabled]	Burst Frequencey

4.3 Security Page



Security	Value	Description
Setup Administrator Password	xxxx	Set Administrator Password
User Password	xxxx	Set User Password
▸ **Secure Boot**		Secure Boot configuration
▸ **BIOS Update**		BIOS Update support

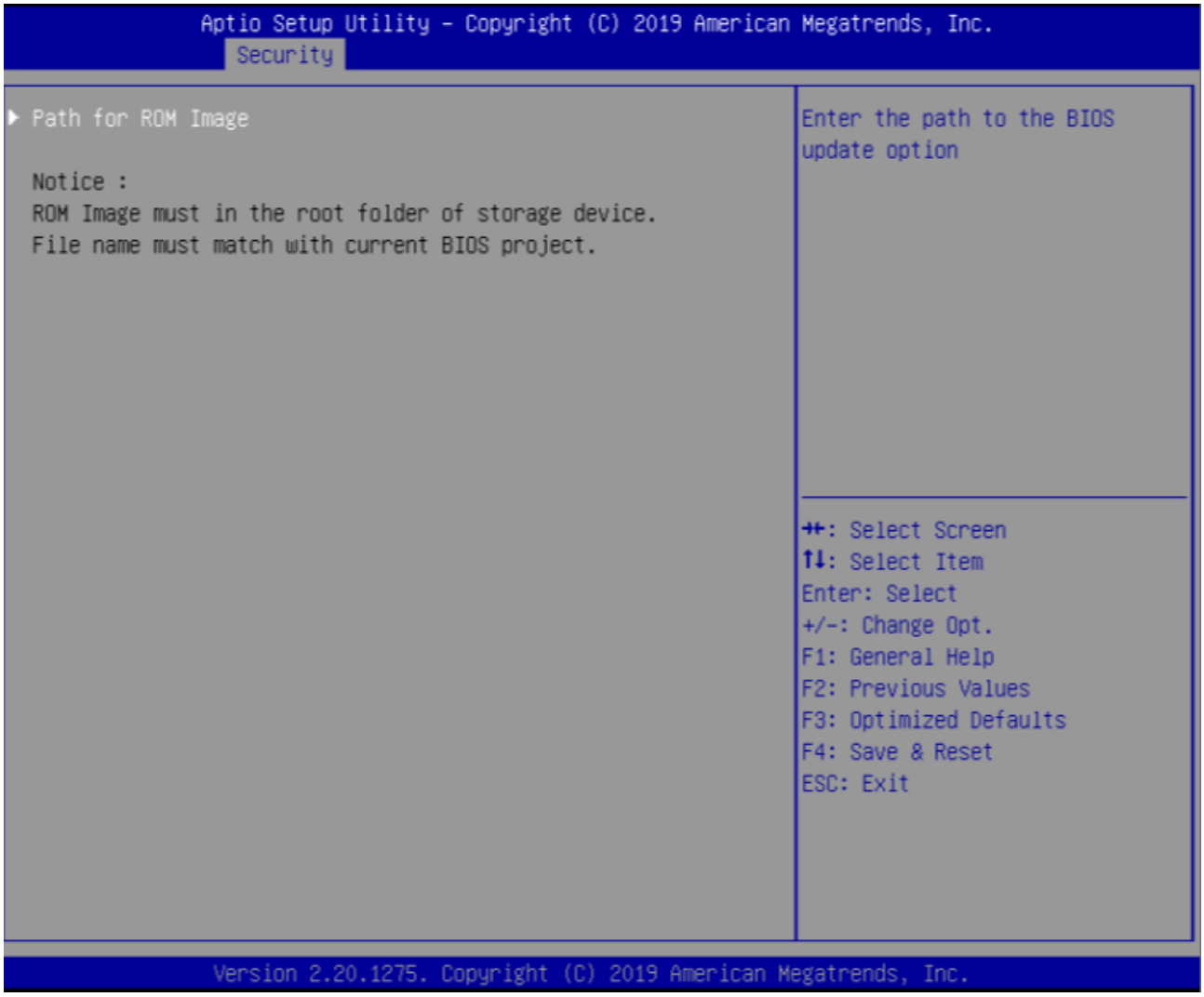
4.3.1 Secure Boot

Security	Value	Description
Secure Boot	Disabled / [Enabled]	Secure Boot activated when: Secure Boot is enabled Platform Key(PK) is enrolled, System mode is User/Deployed, and CSM is disabled
Secure Boot Customization	[Standard] / Customer	Secure Boot Mode - Custom & Standard, Set UEFI Secure Boot Mode to STANDARD mode or CUSTOM mode, this change is effect after save. And after reset, the mode will return to STANDARD mode

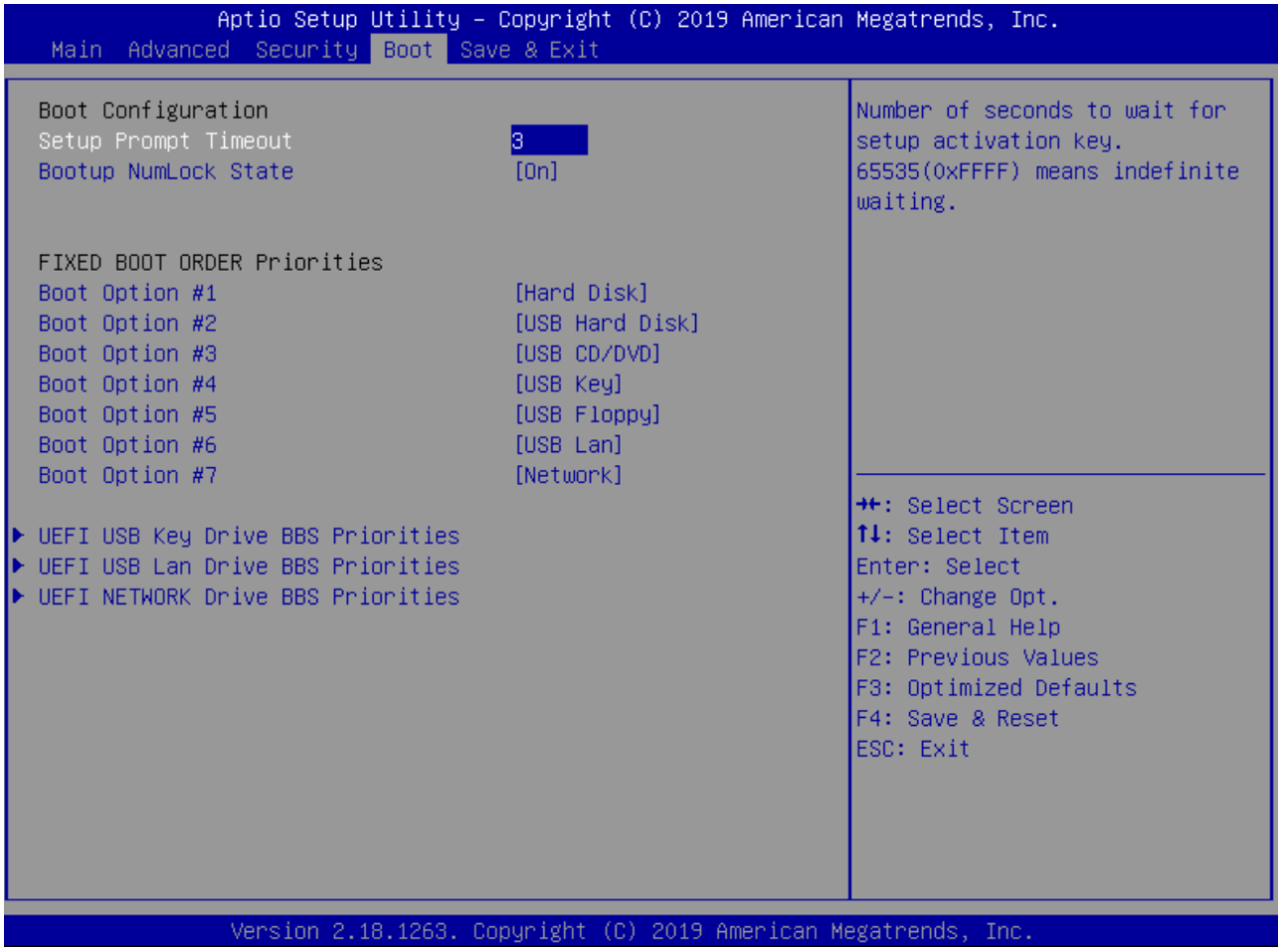
Key Management		
Factory Key Provision	[Disabled] / Enabled	Provision factory default keys on next re-boot only when System in Setup Mode
► Restore Factory Keys	[Yes] / No	Force System to User Mode.Configure NVRAM to contain OEM-defined factory default Secure Boot keys
► Reset To Setup Mode	[Yes] / No	Force System to Setup Mode - clear all Secure Boot Variables
► Export Secure	Drive: \Path	Copy NVRAM content of Secure Boot variables to files in a

Boot variables		root folder on a file system device
Secure Boot variables | Size | Keys | Key Source		
► Platform Key(PK)	[Details] / Export / Update / Delete	Enroll Factory Defaults or load keys from a file formatted as: 1.Public Key Certificate in: a)EFI_SIGNATURE_LIST, b)EFI_CERT_X509 (DER encoded), c)EFI_CERT_RSA2048 (bin), d)EFI_CERT_SHA256 (bin) 2.Authenticated UEFI Variable Key origin legend: Factory Default, Custom, Mixed * user modified via the Setup
► Key Exchange Keys	[Details] / Export / Update / Append / Delete	Enroll Factory Defaults or load keys from a file formatted as: 1.Public Key Certificate in: a)EFI_SIGNATURE_LIST, b)EFI_CERT_X509 (DER encoded), c)EFI_CERT_RSA2048 (bin), d)EFI_CERT_SHA256 (bin) 2.Authenticated UEFI Variable Key origin legend: Factory Default, Custom, Mixed * user modified via the Setup
► Authorized Signatures	[Details] / Export / Update / Append / Delete	Enroll Factory Defaults or load keys from a file formatted as: 1.Public Key Certificate in: a)EFI_SIGNATURE_LIST, b)EFI_CERT_X509 (DER encoded), c)EFI_CERT_RSA2048 (bin), d)EFI_CERT_SHA256 (bin) 2.Authenticated UEFI Variable Key origin legend: Factory Default, Custom, Mixed * user modified via the Setup
► Forbidden Signatures	[Details] / Export / Update / Append / Delete	Enroll Factory Defaults or load keys from a file formatted as: 1.Public Key Certificate in: a)EFI_SIGNATURE_LIST, b)EFI_CERT_X509 (DER encoded), c)EFI_CERT_RSA2048 (bin), d)EFI_CERT_SHA256 (bin) 2.Authenticated UEFI Variable Key origin legend: Factory Default, Custom, Mixed * user modified via the Setup
► Authorized TimeStamps	[Details] / Export / Update / Append / Delete	Enroll Factory Defaults or load keys from a file formatted as: 1.Public Key Certificate in: a)EFI_SIGNATURE_LIST, b)EFI_CERT_X509 (DER encoded), c)EFI_CERT_RSA2048 (bin), d)EFI_CERT_SHA256 (bin) 2.Authenticated UEFI Variable Key origin legend: Factory Default, Custom, Mixed * user modified via the Setup
► OsRecovery Signatures	[Details] / Export / Update / Append / Delete	Enroll Factory Defaults or load keys from a file formatted as: 1.Public Key Certificate in: a)EFI_SIGNATURE_LIST, b)EFI_CERT_X509 (DER encoded), c)EFI_CERT_RSA2048 (bin), d)EFI_CERT_SHA256 (bin) 2.Authenticated UEFI Variable Key origin legend: Factory Default, Custom, Mixed * user modified via the Setup

4.3.2 BIOS Update



4.4 Boot Page



Security	Value	Description
Boot Configuration		
Setup Prompt Timeout	3	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.
Bootup NumLock State	[On] / Off	Select the keyboard NumLock state
FIXED BOOT ORDER Priorities		
Boot Optoin #1	Hard Disk	Set the system boot order
Boot Optoin #2	USB Hard Disk	Set the system boot order
Boot Optoin #3	USB CD/DVD	Set the system boot order
Boot Optoin #4	USB Key:UEFI: xxxx	Set the system boot order
Boot Optoin #5	USB Floppy	
Boot Optoin #6	USB LAN	
Boot Optoin #7	Network:UEFI: PXE xxxx	Set the system boot order

4.5 Save & Exit Page

Save & Exit	Description
Save Changes and Reset	Reset the system after saving the changes.
Discard Changes and Reset	Exit system setup without saving any change.
Restore Defaults	Restore/Load Default values for all the setup options.