ROC254A

MIL-STD Rugged Computer

User's Manual

User's Manual

Revision Date:May. 27. 2019

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 product specifications are subject to change without prior notice

Revision History

Revision	Date (yyyy/mm/dd)	Changes
V0.1	2019/03/27	Initial Release
V1.0	2020/06/15	First Release
V2.0	2023/09/19	Update Expansion slot with M.2 PCIe 3.0 x4 slot

Packing list

Item	Description	Q'ty
1	ROC254A Fanless Rugged System	1
2	CD (Driver + Quick Installation Guide)	1
3	Rack mount Bracket	1
4	Screws for Rack mount Bracket	1

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

Ordering Information

Model Number	Description
ROC254A	19" Rackmount Fanless Computer with Intel® Xeon D-1541, 1 x VGA, 2 x LAN, 1 x IPMI, 6 x USB, 220V AC-in, operating Temperature -5~+50°C

Safety Information 1

Electrical safety 1

Operation safety 1

Statement 1

Revision History 2

Packing list 2

Ordering Information 2

Chapter 1: Product Introduction 6

1.1 System 6

1.2 Dimension drawing 8

1.3 I/O Placement 9

Chapter 2: Connectors/IO Ports 10

2.1 Com port 10

2.2 Ethernet Ports 10

2.3 Universal Serial BUS(USB) 10

2.4 VGA 11

2.5 REAR I/O Control Panel 11

Chapter 3: BIOS 13

3.1 Main Setup 13

3.2 Advanced Setup Configurations 14

3.2.1. Boot Feature 14

3.2.2. Power Configuration 15

3.2.3. CPU Configuration 16

3.2.4. Advanced Power Management Configuration 18

3.2.5. CPU P State Control 18

3.2.6. CPU HWPM State Control 19

3.2.7. CPU C State Control 19
3.2.7.1.CPU T State Control 20
3.2.8. CPU Advanced PM Tuning 20
3.2.8.1.Energy Perf BIAS 20
3.2.8.2.Program PowerCTL_MSR 21
3.2.8.3.DRAM RAPL Configuration 21
3.2.8.4.DRAM RAPL Extended Range 21
3.2.9. Chipset Configuration 22
3.2.10. North Bridge 22
3.2.10.1.IIO Configuration 22
3.2.10.2.IIO1 Configuration 22
3.2.10.3.IOAT (Intel® IO Acceleration) Configuration 22
3.2.11. Intel® VT for Directed I/O (VT-d) 23
3.2.11.1.Memory Configuration 23
3.2.11.2.DIMM Information 24
3.2.11.3.Memory RAS (Reliability_Availability_Serviceability) Configuration 24
3.2.12. South Bridge 25
3.2.12.1.SATA Configuration 26
3.2.12.2.Server ME (Management Engine) Configuration 28
3.2.12.3.PCIe/PCI/PnP Configuration 28
3.2.12.4.Super IO Configuration 31
3.2.12.5.Serial Port 1 Configuration 31
3.2.12.6.Serial Port Console Redirection 32
3.2.12.7.COM1 Console Redirection Settings 32
3.2.12.8.SOL Console Redirection Settings 34
3.2.12.9.EMS Console Redirection Settings 36

3.2.13. ACPI Settings 37
3.2.14. Trusted Computing (Available when a TPM Device is Detected and TPM Jumper is Enabled) 38
3.3 Event Logs 39
3.3.1. Change SMBIOS Event Log Settings 40
3.3.2. View SMBIOS Event Log 42
3.4 IPMI 42
3.4.1. System Event Log 43
3.4.2. BMC Network Configuration 43
3.5 Security 45
3.5.1. Secure Boot Menu 46
3.5.2. Key Management 46
3.5.3. Enroll All Factory Default Keys 46
3.5.4. Platform Key (PK) 47
3.5.5. Key Exchange Key (KEK) 47
3.5.6. Authorized Signatures 47
3.5.7. Forbiden Signatures 47
3.5.8. Authorized TimeStamps 48
3.6 Boot Settings 48
3.6.1. Delete Boot Option 50
3.6.2. Network Drive BBS Priorities 50
3.6.3. UEFI Applicatoin Boot Priorities 50
3.7 Save and Exit 50

Chapter 1: Product Introduction

1.1 System

High Performance Processor	Intel® Xeon® Processor D-1541 / D-1587 (8 / 16 Core,16 / 32Thread Support, 12 /24 MB Smart Cache Build-in Turbo Boost Technology 2.0, VPro and Hyper-Threading support
Memory type	Up to 128GB ECC RDIMM DDR4-2400MHz
Chipset	System on Chip
Expansion Slot	1x PCI-E 3.0 x16 1x M.2 PCIe 3.0 x4 slot, M-key, 2242/2280 SSD, SATA III support
Display	
VGA	Resolution up to 1920×1200@60Hz
Storage	
Storage Device	2x 2.5" Solid State Disk (SSD) 64 / 128 / 256 / 512GB /1TB / 2TB Innodisk 3MG2-P Series MLC SATA III 6Gb/s Flash SSD, Rated for 520 MB/sec Sequential Read ; 350 MB/sec Write Max
Ethernet	
Ethernet	1x Intel I350-AM2 Gigabit Ethernet LAN Interfaces (10/100/1000Mbps)
Front I/O	
Button	1x Power Button w/Indicator LED
Indicator LED	1x HDD LED
USB Port	2x USB2.0 standard-A connectors
SSD Tray	2x 2.5 SSD Easy Swap Tray
REAR I/O	
Ethernet	2x RJ45 Gigabit Ethernet LAN Interfaces, 1x IPMI LAN Interface
VGA Port	1x DB15 connector
USB Port	2x USB3.0 standard-A connectors, 2x USB2.0 standard-A connectors
AC-IN	1x IEC C14 Plug
Power Requirement	
Power Input	90V to 264V AC-in, 200W max

Applications, Operating

Applications	Commercial and Military Platforms Requiring Compliance to MIL-STD-810G Embedded Computing, Process Control, Intelligent Automation and manufactur-ing applications where Harsh Temperature, Shock, Vibration, Altitude, Dust and EMI Conditions. Used in all aspects of the military
Operating System	Windows 10 64Bit, Windows Server 2008 R2, Windows Server 2012 R2 Ubuntu14.04, Fedora 20/23, RedHat Linux EL 7.1/7.2, Vmware ESXi 6.0, ESXi 6.5

Physical

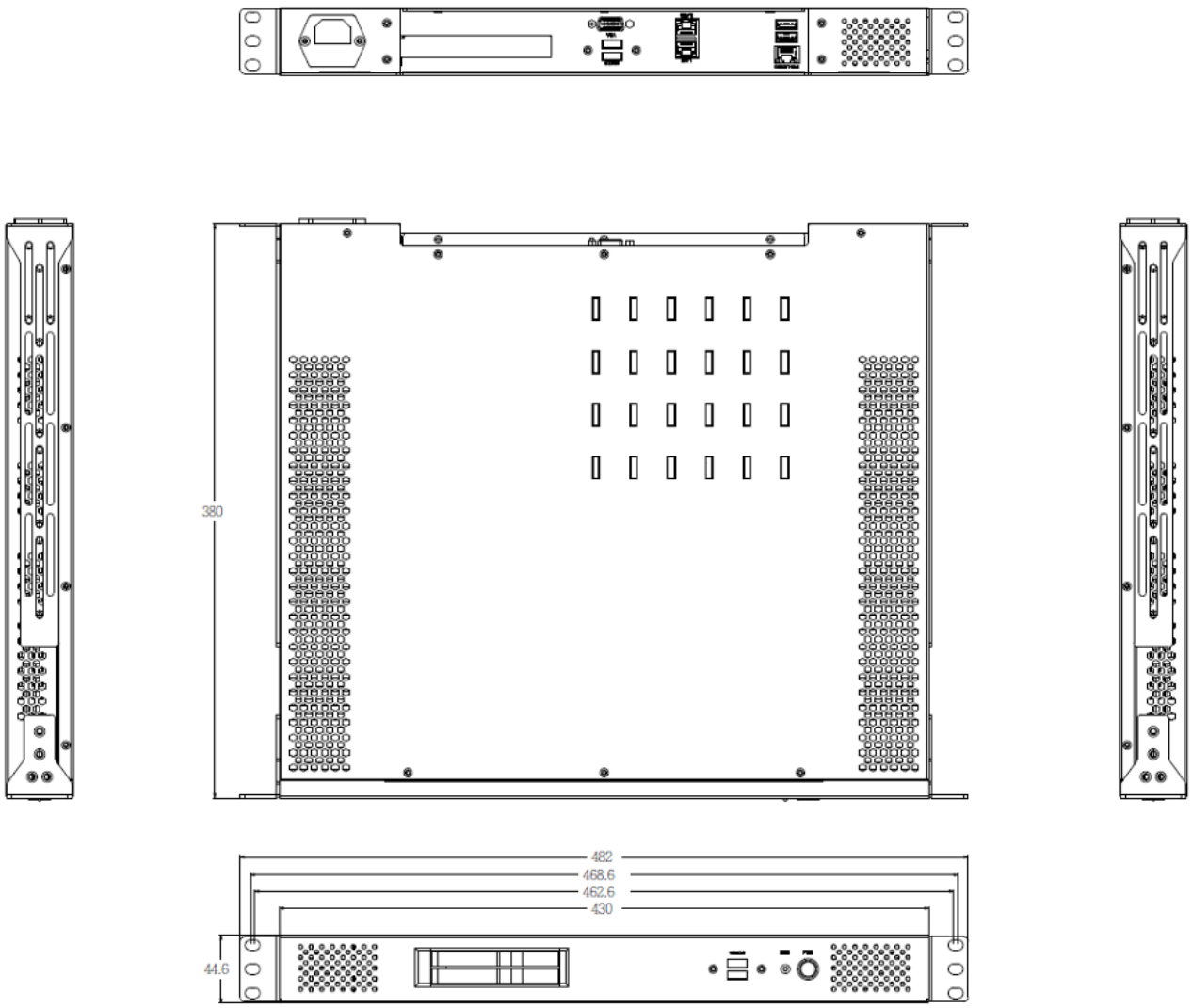
Dimension (W x D x H)	430 x 380 x 44.6mm
Weight	5.75kg(12.68lbs)
Chassis	SECC
Finish	Anodic aluminum oxide (Black)
Cooling	Natural Passive Convection/Conduction. No Moving Parts
Ingress Protection	Dust Proof (Similar to IP50)

Environmental

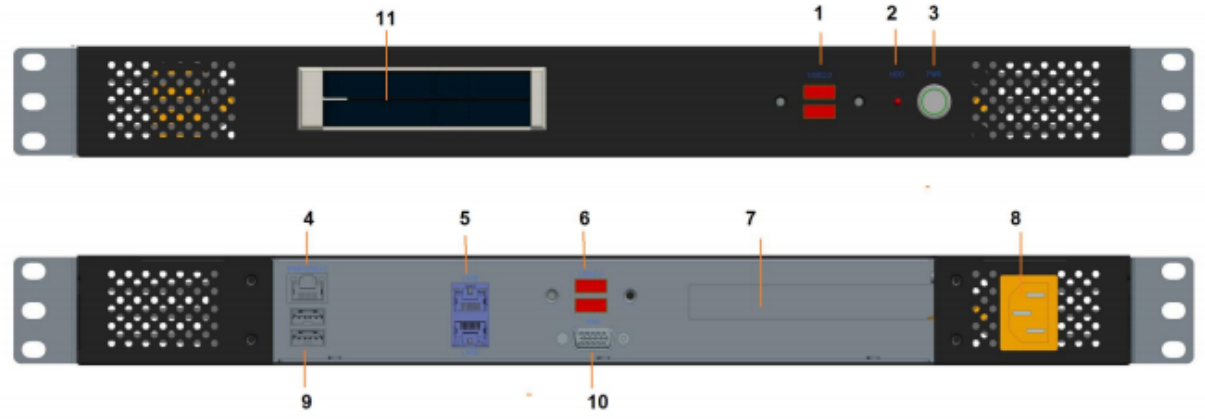
MIL-STD-810G	Method 507.5, Procedure II (Temperature & Humidity)
Test	Method 516.6 Shock-Procedure V Non-Operating (Mechanical Shock)
	Method 516.6 Shock-Procedure I Operating (Mechanical Shock)
	Method 514.6 Vibration Category 24/Non-Operating (Category 20 & 24, Vibration)
	Method 514.6 Vibration Category 20/Operating (Category 20 & 24, Vibration)
	Method 501.5, Procedure I (Storage/High Temperature)
	Method 501.5, Procedure II (Operation/High Temperature)
	Method 502.5, Procedure I (Storage/Low Temperature)
	Method 502.5, Procedure II (Operation/Low Temperature)
	Method 503.5, Procedure I (Temperature shock)
Operating Temperature	-10 to 60°C (ambient with 0.7m/s airflow)
Storage Temperature	-40 to 85°C
EMC	CE and FCC compliance

Specifications are subject to change without notice

1.2 Dimension drawing



1.3 I/O Placement

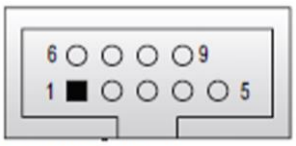


1	2 x USB 2.0
2	HDD LED
3	Power Button w/ Indicator LED
4	IPMI
5	2 x RJ45 (Gigabit Ethernet)
6	2 x USB 2.0
7	1 x PCIex16 Expansion Slot
8	AC Inlet
9	2 x USB 3.0
10	1 x COM (RS232)
11	2 x SSD swappable Tray

Chapter 2: Connectors/IO Ports

2.1 COM port

COM1 port is located near DIMM slot A1 to provide a front accessible serial connection. See the table on the right for pin definitions.



COM1 Pin Lavout

COM Port 1 Pin Definitions			
Pin #	Definition	Pin #	Definition
1	DCD	6	DSR
2	RXD	7	RTS
3	TXD	8	CTS
4	DTR	9	RI
5	Ground	10	N/A

2.2 Ethernet Ports

Two Gigabit Ethernet ports (LAN1~LAN2), two 10G Ethernet ports (LAN3~LAN4) (availability varies by model), and an IPMI LAN port are located on the I/O back panel to provide network connections. These ports accept RJ45 type cables.

LAN Ports Pin Definitions			
Pin #	Definition	Pin #	Definition
1	VCC	10	SGND
2	TD0+	11	Act LED
3	TD0-	12	P3V3SB
4	TD1+	13	Link 100 LED (Green, +3V3SB)
5	TD1-	14	Link 1000 LED (Yellow, +3V3SB)
6	TD2+	15	Ground
7	TD2-	16	Ground
8	TD3+	17	Ground
9	TD3-	18	Ground

2.3 Universal Serial BUS(USB)

Two USB 3.0 ports (USB0/1) are located on the I/O back panel. Two USB 2.0 headers (USB2/3, 4/5) are on the motherboard to provide front panel access. USB cables are not included. See the tables below for pin definitions

Back Panel USB Pin Definitions			
Pin #	Definition	Pin #	Definition
1	+5V		+5V
2	USB_PN1		USB_PN0
3	USB_PP1		USB_PP0
4	Ground		Ground

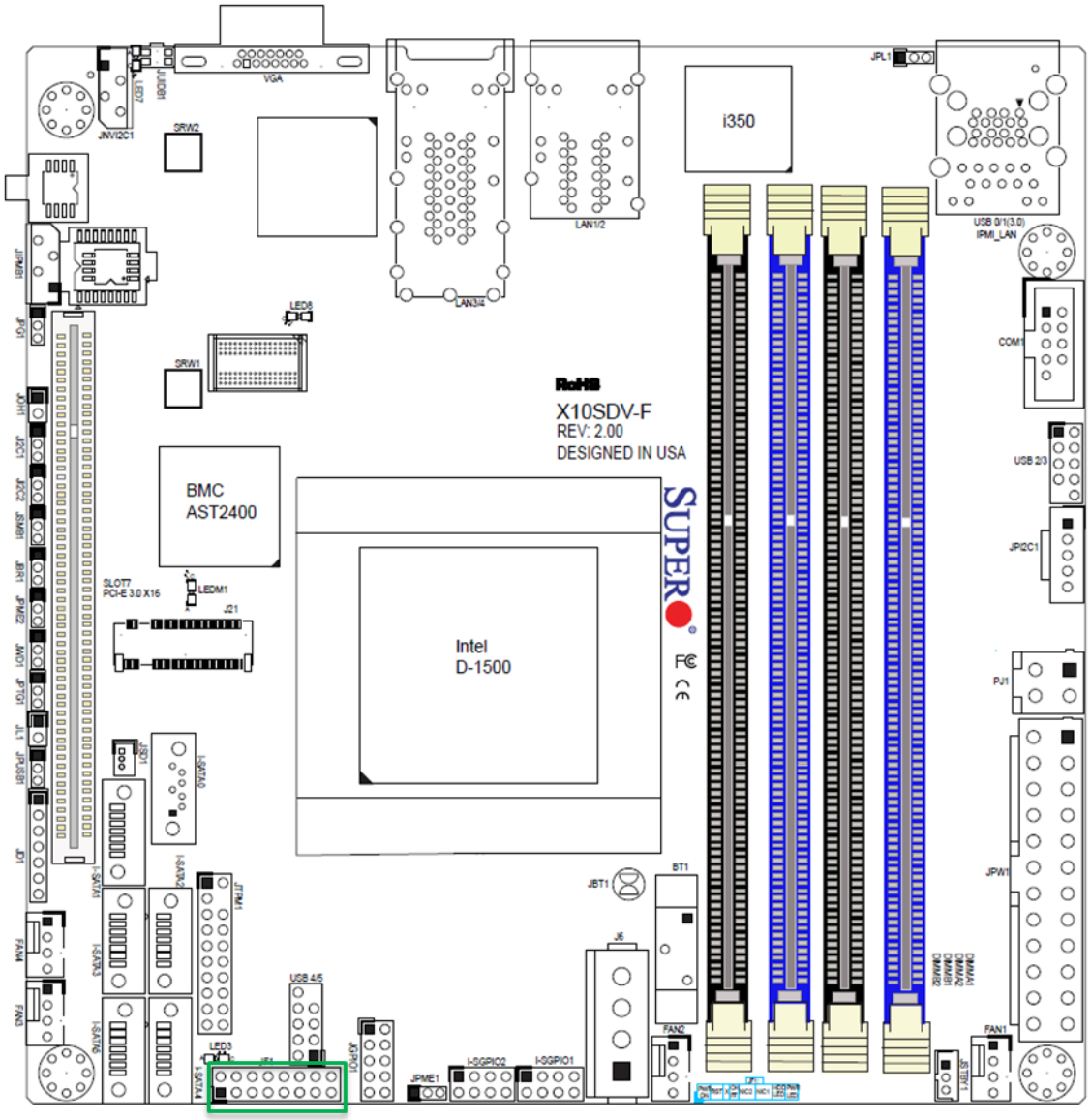
Internal USB Port 2.0 Pin Definitions			
Pin #	Definition	Pin #	Definition
1	+5V	2	+5V
3	USB_PN2	4	USB_PN3
5	USB_PP2	6	USB_PP3
7	Ground	8	Ground
9	Key	10	NC

2.4 VGA

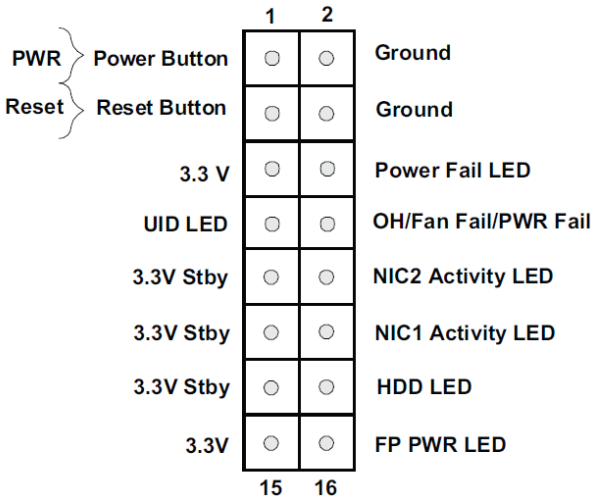
A VGA port is located next to the LAN ports on the I/O back panel. Use this port to connect to a compatible VGA display.

2.5 REAR I/O CONTROL PANEL

JF1 contains header pins for various buttons and indicators that are normally located on a control panel at the rear of the chassis. See the figure below for the descriptions of the rear control panel buttons and LED indicators. Refer to the following section for descriptions and pin definitions.



JF1 Header Pins



POWER LED

The Power LED connection is located on pins 15 and 16 of JF1. Refer to the table on the right for pin definitions.

Power LED Pin Definitions (JF1)	
Pin#	Definition
15	3.3V
16	PWR LED

HDD LED

The HDD LED connection is located on pins 13 and 14 of JF1. Attach a cable here to indicate the status of HDD-related activities, including SATA activities. See the table on the right for pin definitions.

HDD LED Pin Definitions (JF1)	
Pin#	Definition
13	3.3V Standby
14	HD LED

Reset Button

The Reset Button connection is located on pins 3 and 4 of JF1. Attach it to a hardware reset switch on the computer case to reset the system. Refer to the table on the right for pin definitions.

Reset Button Pin Definitions (JF1)	
Pin#	Definition
3	Reset
4	Ground

Power Button

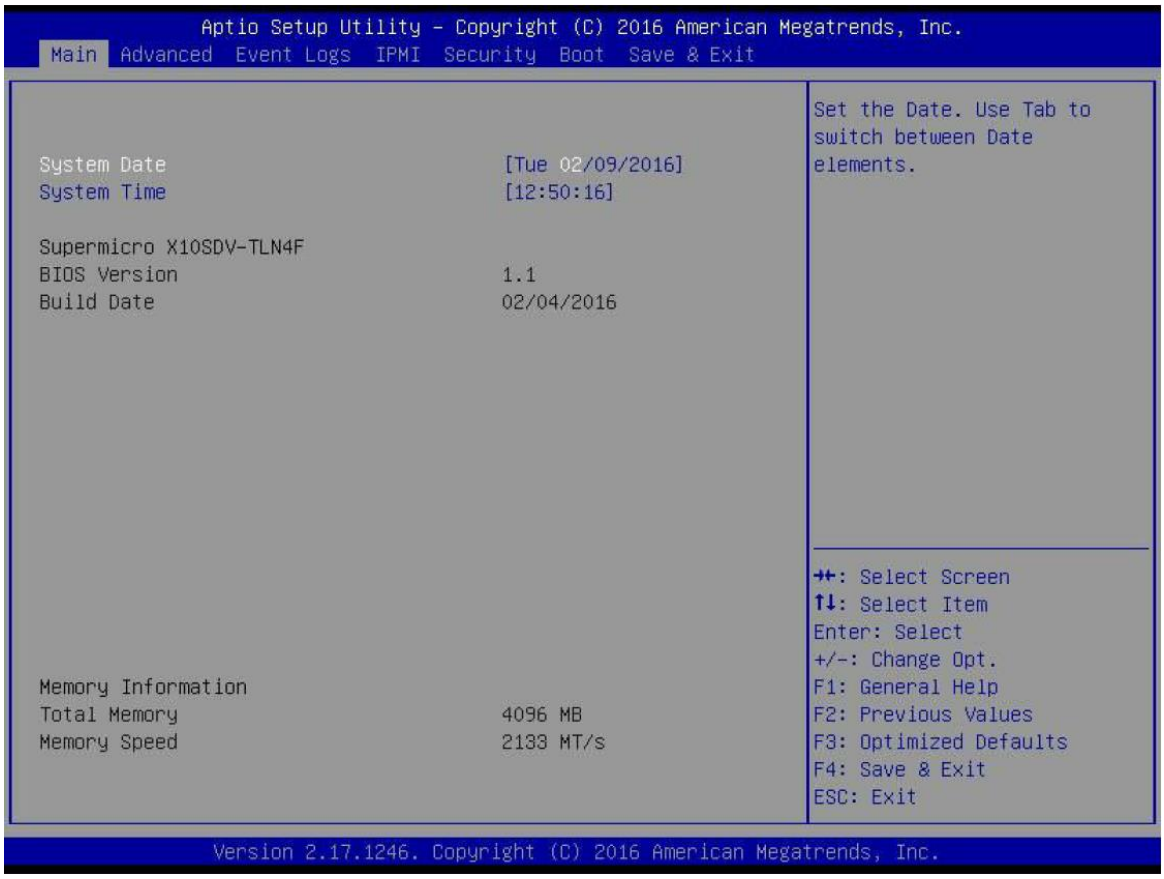
The Power Button connection is located on pins 1 and 2 of JF1. Momentarily contacting both pins will power on/off the system. This button can be configured as 4 Seconds Override or Instant Off (with a setting in the BIOS setting, see Chapter 4). Refer to the table on the right for pin definitions.

Power Button Pin Definitions (JF1)	
Pin#	Definition
1	Signal
2	Ground

Chapter 3: BIOS

3.1 Main Setup

When you first enter the AMI BIOS setup utility, you will enter the Main setup screen. You can always return to the Main setup screen by selecting the Main tab on the top of the screen. The Main BIOS Setup screen is shown below.



The following Main menu items will display:

System Date/System Time

Use this feature to change the system date and time. Highlight System Date or System Time using

the arrow keys. Enter new values using the keyboard. Press the <Tab> key or the arrow keys to move between fields. The date must be entered in Day MM/DD/YY format. The time is entered in HH:MM:SS format.

Note: The time is in the 24-hour format. For example, 5:30 P.M. appears as 17:30:00.

Version

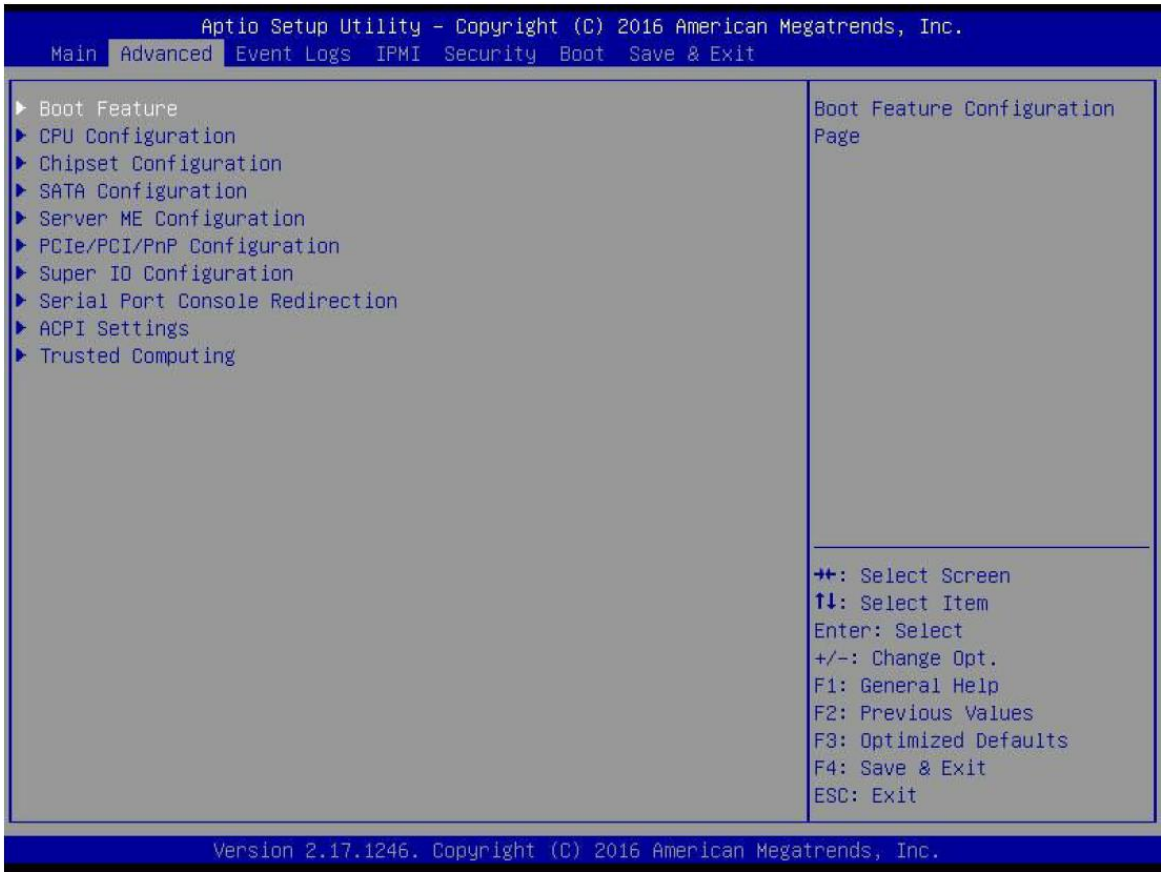
Build Date

Memory Information Total Memory

This displays the total size of memory available in the system.

3.2 Advanced Setup Configurations

Use the arrow keys to select Boot Setup and press <Enter> to access the submenu items.



Warning: Take caution when changing the Advanced settings. An incorrect value, a very high DRAM frequency, or an incorrect DRAM timing setting may make the system unstable. When this occurs, revert to the default to the manufacture default settings.

3.2.1. Boot Feature

Quiet Boot

Use this feature to select the screen display between the POST messages and the OEM logo upon

bootup. Select Disabled to display the POST messages. Select Enabled to display the OEM logo instead of the normal POST messages. The options are Enabled and Disabled.

AddOn ROM Display Mode

Use this feature to set the display mode for the Option ROM. Select Keep Current to display the current AddOn ROM setting. Select Force BIOS to use the Option ROM display set by the system BIOS. The options are Force BIOS and Keep Current.

Bootup NumLock State

Use this feature to set the Power-on state for the <Numlock> key. The options are Off and On.

Wait For 'F1' If Error

Use this feature to force the system to wait until the 'F1' key is pressed if an error occurs. The options are Disabled and Enabled.

INT19 (Interrupt 19) Trap Response

Interrupt 19 is the software interrupt that handles the boot disk function. When this item is set to Immediate, the ROM BIOS of the host adapters will "capture" Interrupt 19 at bootup immediately and allow the drives that are attached to these host adapters to function as bootable disks. If this item is set to Postponed, the ROM BIOS of the host adapters will not capture Interrupt 19 immediately and allow the drives attached to these adapters to function as bootable devices at bootup. The options are Immediate and Postponed.

Re-try Boot

If this item is enabled, the BIOS will automatically reboot the system from a specified boot device after its initial boot failure. The options are Disabled, Legacy Boot, and EFI Boot.

3.2.2. Power Configuration

Watch Dog Function

If enabled, the Watch Dog Timer will allow the system to reset or generate NMI based on jumper settings when it is expired for more than 5 minutes. The options are Disabled and Enabled.

Power Button Function

This feature controls how the system shuts down when the power button is pressed. Select 4_Seconds_Override for the user to power off the system after pressing and holding the power button for 4 seconds or longer. Select Instant Off to instantly power off the system as soon as the user presses the power button. The options are 4 Seconds Override and Instant Off.

Restore on AC Power Loss

Use this feature to set the power state after a power outage. Select Stay-Off for the system power to remain off after a power loss. Select Power-On for the system power to be turned on after a power loss. Select Last State to allow the system to resume its last power state before a power loss. The options are Power-On, Stay-Off, and Last State.

3.2.3. CPU Configuration

The following CPU information will be displayed:

- Processor ID
- Processor Frequency
- Processor Max Ratio
- Processor Min Ratio
- Microcode Revision
- L1 Cache RAM
- L2 Cache RAM
- L3 Cache Ram
- CPU Version

Clock Spread Spectrum

If this feature is set to Enabled, the BIOS utility will monitor the level of Electromagnetic Interference caused by the components and will attempt to reduce the interference whenever needed. The options are Disabled and Enabled.

Hyper-Threading (ALL)

Select Enable to use Intel Hyper-Threading Technology to enhance CPU performance. The options are Disable and Enable.

Cores Enabled

Set a numeric value to enable the number of cores. (Please refer to Intel's website for more information.) Enter 0 to enable all cores.

Monitor/Mwait

Select Enabled to enable the Monitor/MWait instructions. The Monitor instruction monitors a region of memory for writes, and MWait instructions instruct the CPU to stop until the monitored region begins to write. The options are Disable and Enable.

Execute Disable Bit (Available if supported by the OS & the CPU)

Select Enabled to enable the Execute-Disable Bit which will allow the processor to designate areas in the system memory where an application code can execute and where it cannot, thus preventing a worm or a virus from flooding illegal codes to overwhelm the processor or damage the system during an attack. The default is Enable. (Refer to the Intel® and Microsoft® websites for more information.)

PPIN Control

Select Unlock/Enable to use the Protected-Processor Inventory Number (PPIN) in the system. The options are Unlock/Enable and Unlock/Disable.

Hardware Prefetcher (Available when supported by the CPU)

If set to Enabled, the hardware prefetcher will prefetch streams of data and instructions from the main memory to the L2 cache to improve CPU performance. The options are Enable and Disable.

Adjacent Cache Prefetch (Available when supported by the CPU)

The CPU prefetches the cache line for 64 bytes if this feature is set to Disabled. The CPU prefetches both cache lines for 128 bytes as comprised if this feature is set to Enable.

DCU Streamer Prefetcher (Available when supported by the CPU)

Select Enabled to enable the DCU (Data Cache Unit) Streamer Prefetcher which will stream and prefetch data and send it to the Level 1 data cache to improve data processing and system

performance. The options are Enable and Disable.

DCU IP Prefetcher (Available when supported by the CPU)

Select Enabled for DCU (Data Cache Unit) IP Prefetcher support, which will Prefetch IP addresses to improve network connectivity and system performance. The options are Enable and Disable.

Direct Cache Access (DCA)

Select Enabled to use Intel's DCA (Direct Cache Access) Technology to improve data transfer efficiency. The options are Disable, Enable, and Auto.

Intel® Virtualization Technology (Available when supported by the CPU)

Select Enabled to support Intel® Virtualization Technology, which will allow one platform to run multiple operating systems and applications in independent partitions, creating multiple "virtual" systems in one physical computer. The options are Enable and Disable.
Note: *If a change is made to this setting, you will need to reboot the system for the change to take effect. Refer to Intel's website for detailed information.*

3.2.4. Advanced Power Management Configuration

This section is used to configure the following CPU Power Management settings.

EIST (P-States)
EIST (Enhanced Intel SpeedStep Technology) allows the system to automatically adjust processor voltage and core frequency to reduce power consumption and heat dissipation. The options are Disable and Enable.

If the above is set to Enable, CPU P State will display:

3.2.5. CPU P State Control

P State Domain

This feature allows the user to indicate the P-State domain for each logical process in the system. All processes indicate the same domain in the same package. The options are ALL and ONE.

P-State Coordination
This feature allows the user to change the P-State (Power-Performance State) coordination type.

P-State is also known as "SpeedStep" for Intel processors. Select HW_ALL to change the P-State coordination type for hardware components only. Select SW_ALL to change the P-State coordination type for all software installed in the system. Select SW_ANY to change the P-State coordination type for a software program in the system. The options are HW_All, SW_ALL, and SW_ANY.

Energy Efficient P-State

Select Enable to support power-saving mode for P-State. The options are Disable and Enable.

Boot Performance Mode

This feature allows the user to select the performance state that the BIOS will set before the operating system handoff. The options are Max Performance and Max Efficient.

Turbo Mode

Select Enable for processor cores to run faster than the frequency specified by the manufacturer. The options are Disable and Enable.

3.2.6. CPU HWPM State Control

Enable CPU HWPM

Select Enable for better CPU energy performance. The options are Disable, HWPM NATIVE MODE, and HWPM OOB MODE.

Enable CPU Autonomous Cstate

Use this feature to enable CPU Autonomous C State, which converts HALT instructions to Mwait. The options are Disable and Enable.

3.2.7. CPU C State Control

CPU C State

Use this feature to enable the enhanced C State of the CPU. The options are Disable and Enable.

Package C State Limit

This feature allows the user to set the limit on the C State package register. The options are C0/C1 State, C2 State, C6 (Non Retention) State, C6 (Rentention) state, and No Limit.

CPU C3 Report

Select Enabled to allow the BIOS to report the CPU C3 State (ACPI C2) to the operating system. During the CPU C3 State, the CPU clock generator is turned off. The options are Enable and Disable.

CPU C6 Report

Select Enabled to allow the BIOS to report the CPU C6 State (ACPI C3) to the operating system. During the CPU C6 State, the power to all cache is turned off. The options are Enable and Disable.

Enhanced Halt State (C1E)

Select Enabled to use Enhanced Halt-State technology, which will significantly reduce the CPU's power consumption by reducing the CPU's clock cycle and voltage during a Halt-state. The options are Disable and Enable.

3.2.7.1. CPU T State Control

ACPI (Advanced Configuration Power Interface) T-States

Select Enable to support CPU throttling by the operating system to reduce power consumption. The options are Enable and Disable.

3.2.8. CPU Advanced PM Tuning

3.2.8.1. Energy Perf BIAS

Energy Performance Tuning

When enabled, this item selects whether the BIOS or Operating System can turn on the energy performance bias tuning. The options are Enable and Disable.

If the above is set to Disable, Energy Performance BIAS Setting will display:
Energy Performance BIAS Setting

This feature allows balancing Power Efficiency vs Performance. This will override whatever setting is in the Operating System. The options are Performance, Balanced Performance, Balanced Power, and

Power.

Power/Performance Switch

This feature allows dynamic switching between Power and Performance power efficiency. The options are Enable and Disable.

Workload Configuration

This feature allows for optimization of workload. Balanced is recommended. The options are Balanced and I/O Sensitive.

3.2.8.2. Program PowerCTL_MSR

PKG C-state Lat. Neg.

Use this feature to indicate whether latency should be negotiated with PCH for packaging C-States. The options are Enable and Disable.

SAPM Control

This feature indicates whether the PCU should control the System Agent PM using its power-performance tuning algorithm. The options are Enable and Disable.

Energy Efficient Turbo

Use this feature to enable energy efficient turbo mode. The options are Enable and Disable.

3.2.8.3. DRAM RAPL Configuration

Override BW_LIMIT_TF

Use this feature to set the value for the custom tuning of BW_LIMIT_TF. The default value is 1.

3.2.8.4. DRAM RAPL Extended Range

Use this feature to set the DRAM Running Average Power Limit (RAPL) Extended Range. The options are Disable and Enable.

3.2.9. Chipset Configuration

Warning: Setting the wrong values in the following features may cause the system to malfunction.

3.2.10. North Bridge

This feature allows the user to configure the following North Bridge settings.

3.2.10.1. IIO Configuration

EV DFX (Device Function On-Hide) Features
When this feature is set to Enable, the EV_DFX Lock Bits that are located on a processor will always remain clear during electric tuning. The options are Disable and Enable.

3.2.10.2. IIO1 Configuration

M.2 PCI-E 3.0 X4

This item configures the link speed of the PCI-E port specified by the user. The options are Gen 1 (Generation 1) (2.5 GT/s), Gen 2 (Generation 2) (5 GT/s) and Gen 3 (Generation 3) (8 GT/s).

SLOT 7 PCI-E 3.0 X16
This item configures the link speed of the PCI-E port specified by the user. The options are Gen 1 (Generation 1) (2.5 GT/s), Gen 2 (Generation 2) (5 GT/s) and Gen 3 (Generation 3) (8 GT/s).

3.2.10.3. IOAT (Intel® IO Acceleration) Configuration

Enable IOAT

Select Enable to enable Intel I/OAT (I/O Acceleration Technology) support, which significantly reduces CPU overhead by leveraging CPU architectural improvements and freeing the system resource for other tasks. The options are Disable and Enable.

No Snoop

Select Enable to support no-snoop mode for each CB device. The options are Disable and Enable.

3.2.11. Intel® VT for Directed I/O (VT-d)

Intel® VT for Directed I/O (VT-d)

Select Enable to use Intel® Virtualization Technology support for Direct I/O VT-d support by reporting the I/O device assignments to the VMM (Virtual Machine Monitor) through the DMAR ACPI Tables. This feature offers fully-protected I/O resource sharing across Intel platforms, providing greater reliability, security and availability in networking and data-sharing. The options are Enable and Disable.

ACS Control

Use this feature to program Access Control Services (ACS) to the PCI-E Root Port Bridges. The options are Enable and Disable.

Interrupt Remapping

Select Enable for Interrupt Remapping support to enhance system performance. The options are Enable and Disable.

3.2.11.1. Memory Configuration

Enforce POR

Select Enable to enforce POR restrictions on DDR4 frequency and voltage programming. The options are Enabled and Disabled.

Memory Frequency

Use this feature to set the maximum memory frequency for onboard memory modules. The options are Auto, 1333, 1400, 1600, 1800, 1867, 2000, 2133, 2200, 2400, 2600, 2667, and Reserved (Do not select Reserved).

Data Scrambling

Select Enabled to enable data scrambling to enhance system performance and data integrity. The options are Auto, Disabled and Enabled.

DRAM RAPL Baseline

Use this feature to set the run-time power-limit baseline for DRAM modules. The options are Disable, DRAM RAPL Mode 0, and DRAM RAPL Mode 1.

Set Throttling Mode

Throttling improves reliability and reduces power consumption in the processor via automatic voltage control during processor idle states. The options are Disabled and CLTT (Closed Loop Thermal Throttling).

A7 Mode

Select Enabled to support the A7 (Addressing) mode to improve memory performance. The options are Enable and Disable.

3.2.11.2. DIMM Information

This item displays the status of a DIMM module specified by the user.

- DIMMA1
- DIMMB1
- DIMMA2
- DIMMB2

3.2.11.3. Memory RAS (Reliability_Availability_Serviceability) Configuration

Use this submenu to configure the following Memory RAS settings.

Patrol Scrub

Patrol Scrubbing is a process that allows the CPU to correct correctable memory errors detected on a memory module and send the correction to the requestor (the original source). When this item is set to Enabled, the IO hub will read and write back one cache line every 16K cycles, if there is no delay caused by internal processing. By using this method, roughly 64 GB of memory behind the IO hub will be scrubbed every day. The options are Enable and Disable.

Patrol Scrub Interval

This feature allows you to decide how many hours the system should wait before the next complete

patrol scrub is performed. Use the keyboard to enter a value from 0-24. The Default setting is 24.

Demand Scrub

Demand Scrubbing is a process that allows the CPU to correct correctable memory errors found on a memory module. When the CPU or I/O issues a demand-read command, and the read data from memory turns out to be a correctable error, the error is corrected and sent to the requestor (the original source). Memory is updated as well. Select Enable to use Demand Scrubbing for ECC memory correction. The options are Enable and Disable.

Device Tagging

Select Enable to support device tagging. The options are Disable and Enable.

3.2.12. South Bridge

The following South Bridge information will display:

- USB Configuration
- USB Module Version
- USB Devices

Legacy USB Support

This feature enables support for legacy USB devices. Select Auto to disable legacy support if USB devices are not present. Select Disable to have USB devices available only for EFI applications. The options are Enabled, Disabled and Auto.

XHCI Hand-Off

This is a work-around solution for operating systems that do not support XHCI (Extensible Host Controller Interface) hand-off. The XHCI ownership change should be claimed by the XHCI driver. The settings are Enabled and Disabled.

EHCI Hand-Off

This item is for the Operating Systems that do not support Enhanced Host Controller Interface (EHCI) hand-off. When this item is enabled, EHCI ownership change will be claimed by the EHCI driver. The settings are Enabled and Disabled.

Port 60/64 Emulation

This feature enables or disables I/O port 60h/64h emulation support. This should be enabled for complete USB keyboard legacy support for non-USB-aware Operating Systems. The options are Disabled and Enabled.

USB 3.0 Support

Select Enabled for USB 3.0 support. The options are Smart Auto, Auto, Disabled, and Enabled.

EHCI1

Select Enabled to enable EHCI (Enhanced Host Controller Interface) support on USB 2.0 connector #1 (at least one USB 2.0 connector should be enabled for EHCI support). The options are Disabled and Enabled.

EHCI2

Select Enabled to enable EHCI (Enhanced Host Controller Interface) support on USB 2.0 connector #2 (at least one USB 2.0 connector should be enabled for EHCI support). The options are Disabled and Enabled.

XHCI Pre-Boot Driver

Select Enabled to enable XHCI (Extensible Host Controller Interface) support on a pre-boot drive specified by the user. The options are Enabled and Disabled.

3.2.12.1. SATA Configuration

When this submenu is selected, the AMI BIOS automatically detects the presence of the SATA devices that are supported by the Intel PCH chip and displays the following items:

SATA Controller

This item enables or disables the onboard SATA controller supported by the Intel PCH chip. The options are Enabled and Disabled.

Configure SATA as

Select IDE to configure a SATA drive specified by the user as an IDE drive. Select AHCI to configure a SATA drive specified by the user as an AHCI drive. Select RAID to configure a SATA drive specified by the user as a RAID drive. The options are IDE, AHCI, and RAID.
**If the item above "Configure SATA as" is set to AHCI, the following items will display:*

SATA Frozen

Use this item to enable the HDD Security Frozen Mode. The options are Enabled and Disabled.

SATA AHCI LPM

Use this feature to enable the Link Power Management for SATA AHCI. The options are Disabled and Enabled.

Support Aggressive Link Power Management
When this item is set to Enabled, the SATA AHCI controller manages the power usage of the SATA link. The controller will put the link in a low power mode during extended periods of I/O inactivity, and will return the link to an active state when I/O activity resumes. The options are Enabled and Disabled.

SATA Port 0~ Port 5

This item displays the information detected on the installed SATA drive on the particular SATA port.
- Model number of drive and capacity
- Software Preserve Support

Port 0 ~ Port 5 Hot Plug

This feature designates this port for hot plugging. Set this item to Enabled for hot-plugging support, which will allow the user to replace a SATA drive without shutting down the system. The options are Enabled and Disabled.

Port 0 ~ Port 5 Spin Up Device

On an edge detect from 0 to 1, set this item to allow the PCH to initialize the device. The options are Enabled and Disabled.

Port 0 ~ Port 5 SATA Device Type

Use this item to specify if the connected SATA device is a Solid State drive or a Hard Disk Drive. The options are Hard Disk Drive and Solid State Drive.
**If the item above "Configure SATA as" is set to IDE, the following items will display:*

Port 0 ~ Port 5 SATA Device Type (Available when a SATA port is detected)

Use this item to specify if the connected SATA device is a Solid State drive or a Hard Disk Drive. The options are Hard Disk Drive and Solid State Drive.

3.2.12.2. Server ME (Management Engine) Configuration

This feature displays the following system ME configuration settings.

- General ME Configuration
- Operational Firmware Version
- ME Firmware Type
- Recovery Firmware Version
- ME Firmware Features
- ME Firmware Status #1
- ME Firmware Status #2
  - Current State
  - Error Code

3.2.12.3. PCIe/PCI/PnP Configuration

The following information will display:

- PCI Bus Driver Version
- PCI Devices Common Settings:

PCI PERR/SERR Support

Select Enabled to allow a PCI device to generate a PERR/SERR number for a PCI Bus Signal Error Event. The options are Enabled and Disabled.

Above 4G Decoding (Available if the system supports 64-bit PCI decoding)

Select Enabled to decode a PCI device that supports 64-bit in the space above 4G Address. The

options are Enabled and Disabled.

SR-IOV (Available if the system supports Single-Root Virtualization)

Select Enabled for Single-Root IO Virtualization support. The options are Enabled and Disabled.
*Onboard 10GbE LAN SR-IOV not supported on D-1540/D-1520.

Maximum Payload
Use this feature to select the setting for the PCI Express maximum payload size. The options are Auto, 128 Bytes, 256 Bytes, 512 Bytes, 1024 Bytes, 2048 Bytes, and 4096 Bytes.

Relaxed Ordering
Select Enable to enable Relaxed Ordering support which will allow certain transactions to violate the strict-ordering rules of PCI bus for a transaction to be completed prior to other transactions that have already been enqueued. The options are Enabled and Disabled.

Extended Tag

Use this item to allow a device to use the 8-bit tag field as a requester. The options are Disabled and Enabled.

ARI Forwarding

When this feature is enabled, the Downstream Port disables its traditional device number to 0 when turning Type1 Configuration Request into a Type0 Configuration Request. The default value is Disabled.

M.2 PCI-E 3.0 X4 OPROM

Use this feature to select which firmware type to be loaded for the add-on card in this slot. The options are Disabled, Legacy, and EFI.

SLOT 7 PCI-E 3.0 X16 Bifurcation

Use this feature to set the PCI-E slot to operate as a sinlge x16 slot or to bifurcate into two x8 slots. A proper riser card must be used to take advantage of bifurication. The options are x8x8 and x16.

SLOT 7 PCI-E 3.0 X16 OPROM

Use this feature to select which firmware type to be loaded for the add-on card in this slot. The options are Disabled, Legacy, and EFI.

Onboard LAN Option ROM Type

Use this option to enable Option ROM support to boot the computer using a network device specified by the user. The options are Legacy and EFI.

Onboard LAN1 Option ROM

Use this option to select the type of device installed in LAN Port 1 used for system boot. The options are Disabled, PXE, and iSCSI.

Onboard LAN2 Option ROM

Use this option to select the type of device installed in LAN Port 2 used for system boot. The options are Disabled and PXE.

Onboard LAN3 Option ROM

Use this option to select the type of device installed in LAN Port 3 used for system boot. The options are Disabled and PXE.

Onboard LAN4 Option ROM

Use this option to select the type of device installed in LAN Port 4 used for system boot. The options are Disabled and PXE.

Onboard Video Option ROM

Use this item to select the Onboard Video Option ROM type. The options are Disabled, Legacy, and EFI.

VGA Priority

This feature allows the user to select the graphics adapter to be used as the primary boot device. The options are Onboard and Offboard.

Network Stack

Use this feature to enable PXE (Preboot Execution Environment) or UEFI (Unified Extensible Firmware Interface) for network stack support. The options are Disabled and Enabled.
**If the item above set to Enabled, the four items below will appear:*

IPv4 PXE Support

Use this feature to enable IPv4 PXE boot support. The options are Enabled and Disabled.

IPv6 PXE Support

Use this feature to enable IPv6 PXE boot support. The options are Enabled and Disabled.

PXE boot wait time

Use this option to specify the number of times media will be checked. Press "+" or "-" on your keyboard to change the value. The default setting is 0.

Media detect count
Use this option to specify the number of times media will be checked. Press "+" or "-" on your keyboard to change the value. The default setting is 1.

3.2.12.4. Super IO Configuration

Super IO Chip AST2400

3.2.12.5. Serial Port 1 Configuration

This submenu allows the user the configure settings of Serial Port 1.

Serial Port

Select Enabled to enable the selected onboard serial port. The options are Enabled and Disabled.

Device Settings

This item displays the status of a serial part specified by the user.

Change Port 1 Settings

This feature specifies the base I/O port address and the Interrupt Request address of a serial port specified by the user. Select Auto to allow the BIOS to automatically assign the base I/O and IRQ address. The options for Serial Port 1 are Auto, (IO=3F8h; IRQ=4), (IO=3F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12), (IO=2F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12), (IO=3E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12) and (IO=2E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12).

3.2.12.6. Serial Port Console Redirection

COM1 Console Redirection

Console Redirection

Select Enabled to enable console redirection support for a serial port specified by the user. The options are Enabled and Disabled.

3.2.12.7. COM1 Console Redirection Settings

This feature allows the user to specify how the host computer will exchange data with the client computer, which is the remote computer used by the user.

Terminal Type

This feature allows the user to select the target terminal emulation type for Console Redirection. Select VT100 to use the ASCII Character set. Select VT100+ to add color and function key support. Select ANSI to use the Extended ASCII Character Set. Select VT-UTF8 to use UTF8 encoding to map Unicode characters into one or more bytes. The options are ANSI, VT100, VT100+, and VT-UTF8.

Bits Per second

Use this feature to set the transmission speed for a serial port used in Console Redirection. Make sure that the same speed is used in the host computer and the client computer. A lower transmission speed may be required for long and busy lines. The options are 9600, 19200, 38400, 57600 and 115200 (bits per second).

Data Bits

Use this feature to set the data transmission size for Console Redirection. The options are 7 Bits and 8 Bits.

Parity

A parity bit can be sent along with regular data bits to detect data transmission errors. Select Even if the parity bit is set to 0, and the number of 1's in data bits is even. Select Odd if the parity bit is set to 0, and the number of 1's in data bits is odd. Select None if you do not want to send a parity bit with your data bits in transmission. Select Mark to add a mark as a parity bit to be sent along with the data bits. Select Space to add a Space as a parity bit to be sent with your data bits. The options are None, Even, Odd, Mark and Space.

Stop Bits

A stop bit indicates the end of a serial data packet. Select 1 Stop Bit for standard serial data communication. Select 2 Stop Bits if slower devices are used. The options are 1 and 2.

Flow Control

Use this feature to set the flow control for Console Redirection to prevent data loss caused by buffer overflow. Send a "Stop" signal to stop sending data when the receiving buffer is full. Send a "Start" signal to start sending data when the receiving buffer is empty. The options are None and Hardware RTS/CTS.

VT-UTF8 Combo Key Support

Select Enabled to enable VT-UTF8 Combination Key support for ANSI/VT100 terminals. The options are Enabled and Disabled.

Recorder Mode

Select Enabled to capture the data displayed on a terminal and send it as text messages to a remote server. The options are Disabled and Enabled.

Resolution 100x31

Select Enabled for extended-terminal resolution support. The options are Disabled and Enabled.

Legacy OS Redirection Resolution

Use this feature to select the number of rows and columns used in Console Redirection for legacy OS support. The options are 80x24 and 80x25.

Putty KeyPad

This feature selects the settings for Function Keys and KeyPad used for Putty, which is a terminal emulator designed for the Windows OS. The options are VT100, LINUX, XTERMR6, SC0, ESCN, and VT400.

Redirection After BIOS POST

Use this feature to enable or disable legacy console redirection after BIOS POST. When set to Bootloader, legacy console redirection is disabled before booting the OS. When set to Always Enable, legacy console redirection remains enabled when booting the OS. The options are Always Enable and Bootloader.

SOL Console Redirection

Select Enabled to use the SOL port for Console Redirection. The options are Enabled and Disabled.
**If the item above set to Enabled, the following items will become available for user's configuration:*

3.2.12.8. SOL Console Redirection Settings

Use this feature to specify how the host computer will exchange data with the client computer, which is the remote computer used by the user.

Terminal Type

Use this feature to select the target terminal emulation type for Console Redirection. Select VT100 to use the ASCII Character set. Select VT100+ to add color and function key support. Select ANSI to use the Extended ASCII Character Set. Select VT-UTF8 to use UTF8 encoding to map Unicode characters into one or more bytes. The options are ANSI, VT100, VT100+, and VT-UTF8.

Bits Per second

Use this feature to set the transmission speed for a serial port used in Console Redirection. Make

sure that the same speed is used in the host computer and the client computer. A lower transmission speed may be required for long and busy lines. The options are 9600, 19200, 38400, 57600 and 115200 (bits per second).

Data Bits

Use this feature to set the data transmission size for Console Redirection. The options are 7 (Bits) and 8 (Bits).

Parity

A parity bit can be sent along with regular data bits to detect data transmission errors. Select Even if the parity bit is set to 0, and the number of 1's in data bits is even. Select Odd if the parity bit is set to 0, and the number of 1's in data bits is odd. Select None if you do not want to send a parity bit with your data bits in transmission. Select Mark to add a mark as a parity bit to be sent along with the data bits. Select Space to add a Space as a parity bit to be sent with your data bits. The options are None, Even, Odd, Mark and Space.

Stop Bits

A stop bit indicates the end of a serial data packet. Select 1 Stop Bit for standard serial data communication. Select 2 Stop Bits if slower devices are used. The options are 1 and 2.

Flow Control

Use this feature to set the flow control for Console Redirection to prevent data loss caused by buffer overflow. Send a "Stop" signal to stop sending data when the receiving buffer is full. Send a "Start" signal to start sending data when the receiving buffer is empty. The options are None and Hardware RTS/CTS.

VT-UTF8 Combo Key Support

Select Enabled to enable VT-UTF8 Combination Key support for ANSI/VT100 terminals. The options are Enabled and Disabled.

Recorder Mode

Select Enabled to capture the data displayed on a terminal and send it as text messages to a remote

server. The options are Disabled and Enabled.

Resolution 100x31

Select Enabled for extended-terminal resolution support. The options are Disabled and Enabled.

Legacy OS Redirection Resolution

Use this feature to select the number of rows and columns used in Console Redirection for legacy OS support. The options are 80x24 and 80x25.

Putty KeyPad

This feature selects Function Keys and KeyPad settings for Putty, which is a terminal emulator designed for the Windows OS. The options are VT100, LINUX, XTERMR6, SCO, ESCN, and VT400.

Redirection After BIOS POST

Use this feature to enable or disable legacy Console Redirection after BIOS POST. When set to Bootloader, legacy Console Redirection is disabled before booting the OS. When set to Always Enable, legacy Console Redirection remains enabled when booting the OS. The options are Always Enable and Bootloader.

Serial Port for Out-of-Band Management/Windows Emergency Management Services (EMS)

The submenu allows the user to configure Console Redirection settings to support Out-of-Band Serial Port management.

EMS (Emergency Management Services) Console Redirection

Select Enabled to use a COM port selected by the user for EMS Console Redirection. The options are Enabled and Disabled.

**If the item above set to Enabled, the following items will become available for user's configuration:*

3.2.12.9. EMS Console Redirection Settings

This feature allows the user to specify how the host computer will exchange data with the client computer, which is the remote computer used by the user.

Out-of-Band Mgmt Port

The feature selects a serial port in a client server to be used by the Microsoft Windows Emergency Management Services (EMS) to communicate with a remote host server. The options are COM1 and SOL.

Terminal Type

Use this feature to select the target terminal emulation type for Console Redirection. Select VT100 to use the ASCII character set. Select VT100+ to add color and function key support. Select ANSI to use the extended ASCII character set. Select VT-UTF8 to use UTF8 encoding to map Unicode characters into one or more bytes. The options are ANSI, VT100, VT100+, and VT-UTF8.

Bits Per Second

This item sets the transmission speed for a serial port used in Console Redirection. Make sure that the same speed is used in the host computer and the client computer. A lower transmission speed may be required for long and busy lines. The options are 9600, 19200, 57600, and 115200 (bits per second).

Flow Control

Use this item to set the flow control for Console Redirection to prevent data loss caused by buffer overflow. Send a "Stop" signal to stop sending data when the receiving buffer is full. Send a "Start" signal to start sending data when the receiving buffer is empty. The options are None, Hardware RTS/CTS, and Software Xon/Xoff.

Data Bits

Parity

Stop Bits

3.2.13. ACPI Settings

WHEA Support

This feature Enables the Windows Hardware Error Architecture (WHEA) support for the Windows

2008 (or a later version) operating system. The options are Enabled and Disabled.

High Precision Event Timer

Use this feature to activate the High Performance Event Timer (HPET) that produces periodic interrupts at a much higher frequency than a Real-time Clock (RTC) does in synchronizing multimedia streams, providing smooth playback and reducing the dependency on other timestamp calculation devices, such as an x86 RDTSC Instruction embedded in the CPU. The High Performance Event Timer is used to replace the 8254 Programmable Interval Timer. The options are Enabled and Disabled.

PCI AER Support

Use this feature to enable the ACPI OS to manage PCI Advanced Error Reporting. The options are Enabled and Disabled.

3.2.14. Trusted Computing (Available when a TPM Device is Detected and TPM Jumper is Enabled)

Configuration

Security Device Support

Select Enable for the AMI BIOS to automatically download the drivers needed to provide Trusted Computing platform support for this machine to ensure date integrity and network security. The options are Disable and Enable.

TPM State

Select Enabled to use TPM (Trusted Platform Module) settings for system data security. The options are Disabled and Enabled.
Note: The system will reboot for the change on TPM State to take effect.

Pending Operation

Use this item to schedule a TPM-related operation to be performed by a security device for TPM support. The options are None, Enable Take Ownership, Disable Take Ownership, and TPM Clear.
Note: The computer will reboot to carry out a pending TPM operation and change TPM state for a

TPM device.

Current Status Information

This feature indicates the status of the following TPM items:

TPM Enabled Status

TPM Active Status

TPM Owner Status

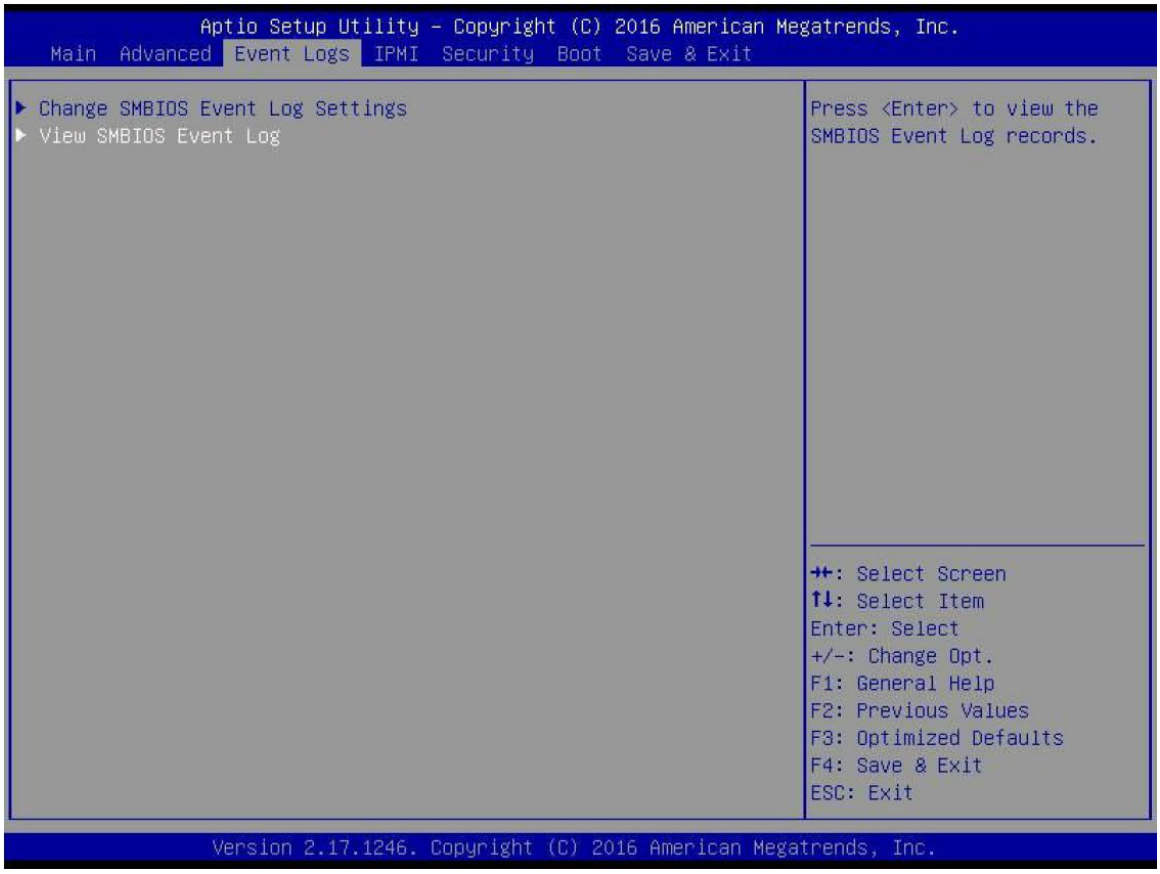
Intel TXT (LT-SX) Configuration

TXT Support

Intel TXT (Trusted Execution Technology) helps protect against software-based attacks to ensure the security, confidentiality, and integrity of all data stored in the system. The options are Enabled and Disabled.

3.3 Event Logs

Use this feature to configure Event Log settings.



3.3.1. Change SMBIOS Event Log Settings

Enabling/Disabling Options

SMBIOS Event Log

Change this item to enable or disable all features of the SMBIOS Event Logging during system boot. The options are Enabled and Disabled.

Runtime Error Logging Support

Use this feature to enable Runtime Error Logging support. The options are Enable and Disable. If this item is set to Enable, the following item will be available for configuration:

Memory Corrected Error Enabling (Available when the item above - Runtime Error Logging Support is set to Enable)

Select Enable for the BIOS to correct a memory error if it is correctable. The options are Disable and Enable.

Memory Corr. Error Threshold

Use this item to enter the threshold value for correctable memory errors. The default setting is 10.

PCI-Ex Error Enable

Select Yes for the BIOS to correct errors occurred in the PCI-E slots. The options are Yes and No.

Erasing Settings

Erase Event Log

If No is selected, data stored in the event log will not be erased. If Yes, Next Reset is selected, data in the event log will be erased upon next system reboot. If Yes, Every Reset is selected, data in the event log will be erased upon every system reboot. The options are No, Yes, Next reset, and Yes, Every reset.

When Log is Full

Select Erase Immediately for all messages to be automatically erased from the event log when the event log memory is full. The options are Do Nothing and Erase Immediately.

SMBIOS Event Long Standard Settings

Log System Boot Event

This option toggles the System Boot Event logging to enabled or disabled. The options are Disabled and Enabled.

MECI

The Multiple Event Count Increment (MECI) counter counts the number of occurences that a duplicate event must happen before the MECI counter is incremented. This is a numeric value. The default value is 1.

METW

The Multiple Event Time Window (METW) defines number of minutes must pass between duplicate log events before MECI is incremented. This is in minutes, from 0 to 99. The default value is 60.
Note: After making changes on a setting, be sure to reboot the system for the changes to take effect.

3.3.2. View SMBIOS Event Log

This section displays the contents of the SMBIOS Event Log.

3.4 IPMI

Use this feature to configure Intelligent Platform Management Interface (IPMI) settings.

BMC Firmware Revision

This item indicates the IPMI firmware revision used in your system.

IPMI Status (Baseboard Management Controller)

This item indicates the status of the IPMI firmware installed in your system.

3.4.1. System Event Log

Enabling/Disabling Options

SEL Components

Select Enabled for all system event logging at bootup. The options are Enabled and Disabled.

Erasing Settings

Erase SEL

Select Yes, On next reset to erase all system event logs upon next system reboot.
Select Yes, On every reset to erase all system event logs upon each system reboot.
Select No to keep all system event logs after each system reboot. The options are
No, Yes, On next reset, and Yes, On every reset.

When SEL is Full

This feature allows the user to decide what the BIOS should do when the system event log is full.
Select Erase Immediately to erase all events in the log when the system event log is full. The options are Do Nothing and Erase Immediately.
Note: After making changes on a setting, be sure to reboot the system for the changes to take effect.

3.4.2. BMC Network Configuration

BMC Network Configuration

IPMI LAN Selection

This item displays the IPMI LAN setting. The default setting is Failover.

IPMI Network Link Status

This item displays the IPMI Network Link status. The default setting is Dedicated LAN.

Update IPMI LAN Configuration

Select Yes for the BIOS to implement all IP/MAC address changes at the next system boot. The options are No and Yes

Configuration Address Source

This feature allows the user to select the source of the IP address for this computer. If Static is selected, you will need to know the IP address of this computer and enter it to the system manually in the field. If DHCP is selected, the BIOS will search for a DHCP (Dynamic Host Configuration Protocol) server in the network that is attached to and request the next available IP address for this computer. The options are DHCP and Static. The following items are assigned IP addresses automatically if DHCP is selected.

Current Configuration Address Source

This item displays the current configuration address for this computer.

Station IP Address

This item displays the Station IP address for this computer. This should be in decimal and in dotted quad form (i.e., 192.168.10.253).

Subnet Mask

This item displays the sub-network that this computer belongs to. The value of each three-digit number separated by dots should not exceed 255.

Station MAC Address

This item displays the Station MAC address for this computer. Mac addresses are 6 two-digit hexadecimal numbers.

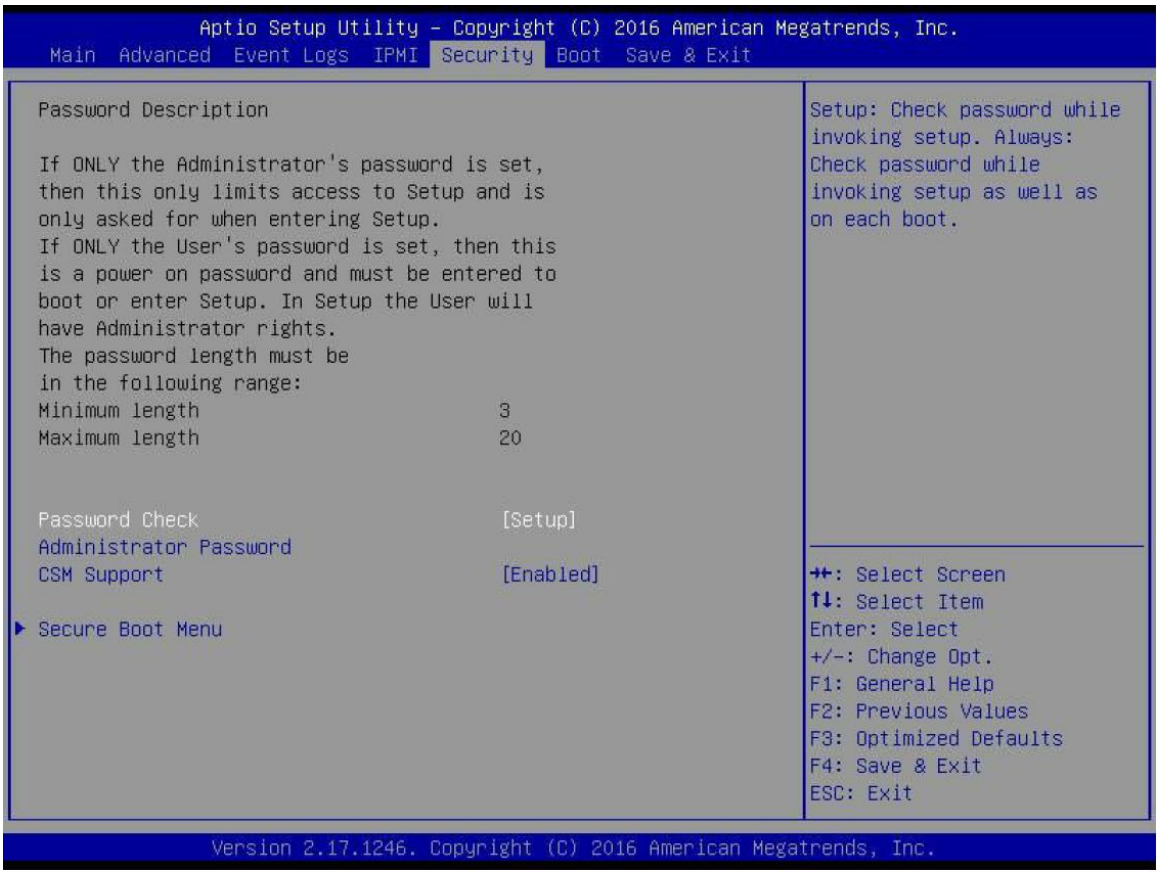
Gateway IP Address

This item displays the Gateway IP address for this computer. This should be in decimal and in dotted quad form (i.e., 172.31.0.1).

IPMI Function Support

Use this feature to enable or disable IPMI support within the BIOS. The options are Enabled and Disabled. When Disabled, the motherboard powers on quickly by removing BIOS control for extended IPMI features. The Disable option is for applications that require faster power on time wthout using Supermicro Update Manager (SUM) or extended IPMI features. The BMC network configuration in the BIOS setup is also invalid when IPMI Function Support is disabled. General BMC function and motherboard health monitor such as temperature and fan control are still active even when this option is disabled.

3.5 Security



This menu allows the user to configure the following security settings for the system.

Password Check

Select Setup for the system to check for a password at Setup. Select Always for the system to check for a password at bootup or upon entering the BIOS Setup utility. The options are Setup and Always.

Administrator Password

Press Enter to create a new, or change an existing Administrator password.

CSM Support

Select Enabled to support the EFI Compatibility Support Module (CSM), which provides compatibility support for traditional legacy BIOS for system boot. The options are Enabled and Disabled. The options are Enabled and Disabled.

3.5.1. Secure Boot Menu

This section displays the contents of the following secure boot features:

- System Mode
- Secure Boot
- Vendor Keys

Secure Boot

Use this item to enable secure boot. The options are Disabled and Enabled.

Secure Boot Mode

Use this item to select the secure boot mode. The options are Standard and Custom.

3.5.2. Key Management

This submenu allows the user to configure the following Key Management settings.

Factory Default Key Provision

Select Enabled to install the default Secure Boot keys set by the manufacturer. The options are Disabled and Enabled.

3.5.3. Enroll All Factory Default Keys

Select Yes to install all default secure keys set by the manufacturer. The options are Yes and No.

Save All Secure Boot Variables

This feature allows the user to decide if all secure boot variables should be saved.

3.5.4. Platform Key (PK)

This feature allows the user to configure the settings of the platform keys.

Set New Key

Select Yes to load the new platform keys (PK) from the manufacturer's defaults.
Select No to load the platform keys from a file. The options are Yes and No.

3.5.5. Key Exchange Key (KEK)

Set New Key

Select Yes to load the KEK from the manufacturer's defaults. Select No to load the KEK from a file. The options are Yes and No.

Append Key

Select Yes to add the KEK from the manufacturer's defaults list to the existing KEK. Select No to load the KEK from a file. The options are Yes and No.

3.5.6. Authorized Signatures

Set New Key

Select Yes to load the database from the manufacturer's defaults. Select No to load the DB from a file. The options are Yes and No.

Append Key

Select Yes to add the database from the manufacturer's defaults to the existing DB. Select No to load the DB from a file. The options are Yes and No.

3.5.7. Forbiden Signatures

Set New Key

Select Yes to load the DBX from the manufacturer's defaults. Select No to load the DBX from a file. The options are Yes and No.

Append New Key

Select Yes to add the DBX from the manufacturer's defaults to the existing DBX. Select No to load the DBX from a file. The options are Yes and No.

3.5.8. Authorized TimeStamps

Set New Key

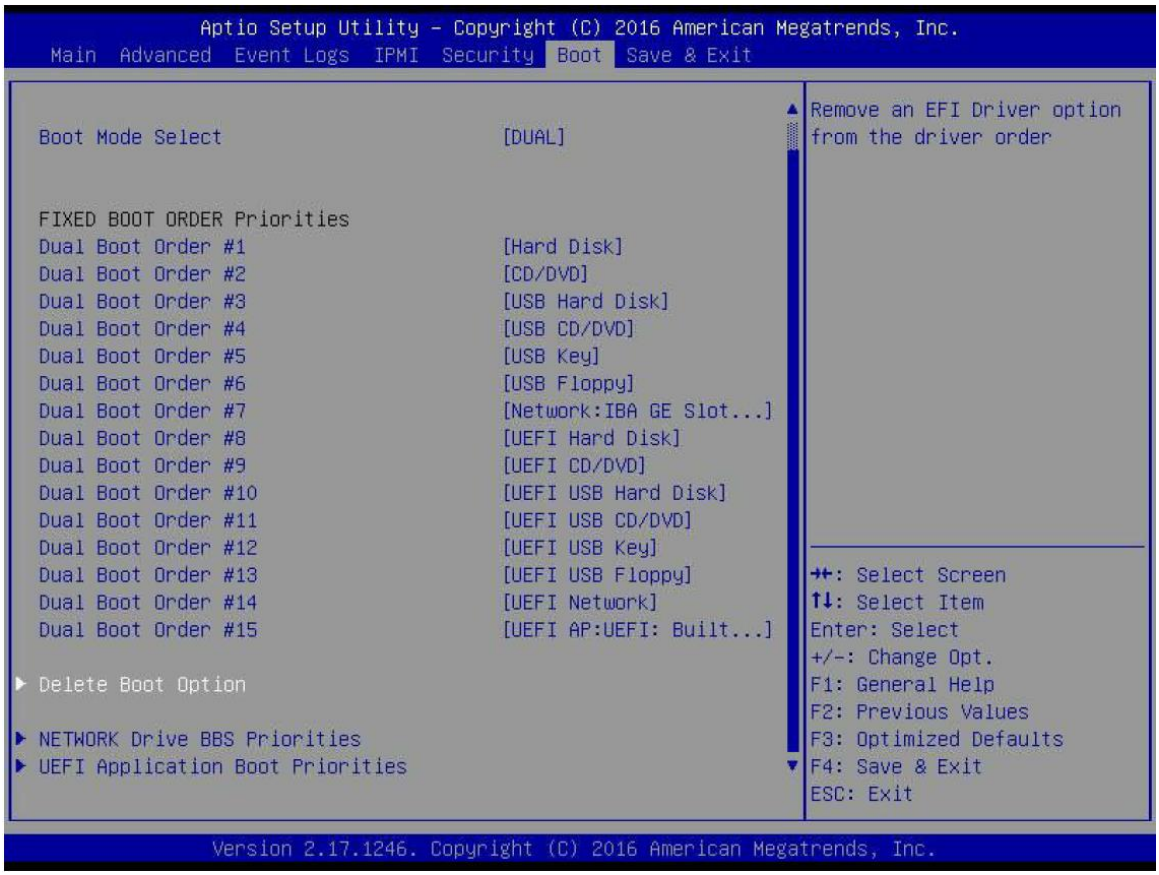
Select Yes to load the DBT from the manufacturer's defaults. Select No to load the DBT from a file. The options are Yes and No.

Append Key

Select Yes to add the DBT from the manufacturer's defaults list to the existing DBT. Select No to load the DBT from a file. The options are Yes and No.

3.6 Boot Settings

Use this feature to configure Boot Settings:



Setup Prompt Timeout

Use this item to indicate the length of time (the number of seconds) for the BIOS to wait before rebooting the system when the setup activation key is pressed. Enter the value of 65535 (0xFFFF) for the BIOS to wait indefinitely. The default setting is 1.

Boot Mode Select

Use this item to select the type of device that the system is going to boot from. The options are Legacy, UEFI, and Dual. The default setting is Dual.

Fixed Boot Order Priorities

This option prioritizes the order of bootable devices that the system to boot from.
Press <Enter> on each entry from top to bottom to select devices.

- Dual Boot Order #1
- Dual Boot Order #2
- Dual Boot Order #3
- Dual Boot Order #4

- Dual Boot Order #5
- Dual Boot Order #6
- Dual Boot Order #7
- Dual Boot Order #8
- Dual Boot Order #9
- Dual Boot Order #10
- Dual Boot Order #11
- Dual Boot Order #12
- Dual Boot Order #13
- Dual Boot Order #14
- Dual Boot Order #15

3.6.1. Delete Boot Option

Use this feature to remove a pre-defined boot device from which the system will boot during startup.
The settings are [any pre-defined boot device].

3.6.2. Network Drive BBS Priorities

This feature allows the user to specify which Network devices are boot devices.

- Legacy Boot Order #1

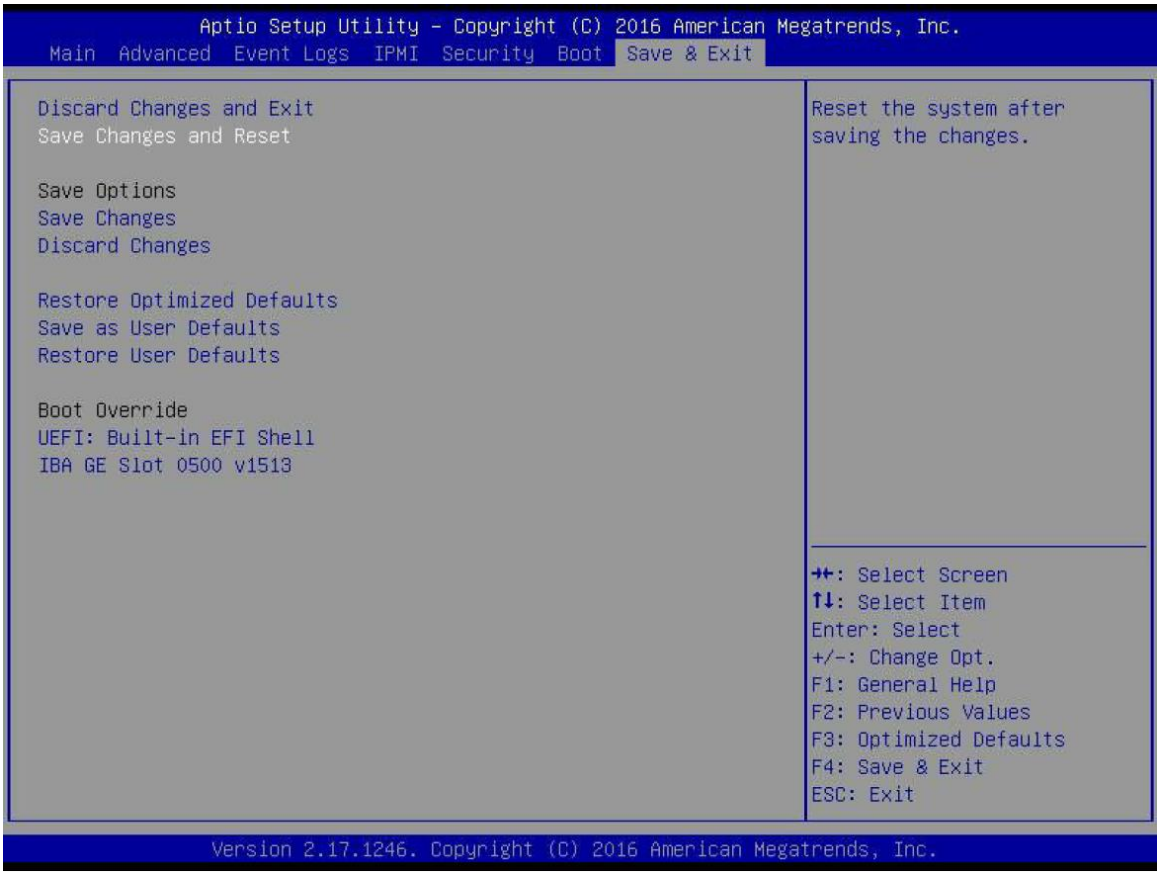
3.6.3. UEFI Applicatoin Boot Priorities

This feature allows the user to specify which UEFI devices are boot devices.

- UEFI Boot Order #1

3.7 Save and Exit

Select the Exit tab from the BIOS setup utility screen to enter the Exit BIOS Setup screen.



Discard Changes and Exit

Select this option to quit the BIOS Setup without making any permanent changes to the system configuration, and reboot the computer. Select Discard Changes and Exit from the Exit menu and press <Enter>.

Save Changes and Reset

When you have completed the system configuration changes, select this option to leave the BIOS setup utility and reboot the computer, so the new system configuration parameters can take effect. Select Save Changes and Exit from the Exit menu and press <Enter>.

Save Options

Save Changes

After completing the system configuration changes, select this option to save the changes you have made. This will not reset (reboot) the system.

Discard Changes

Select this option and press <Enter> to discard all the changes and return to the AMI BIOS utility Program.

Restore Defaults

To set this feature, select Restore Defaults from the Save & Exit menu and press <Enter>. These are factory settings designed for maximum system stability, but not for maximum performance.

Save As User Defaults

To set this feature, select Save as User Defaults from the Exit menu and press <Enter>. This enables the user to save any changes to the BIOS setup for future use.

Restore User Defaults

To set this feature, select Restore User Defaults from the Exit menu and press <Enter>. Use this feature to retrieve user-defined settings that were saved previously.