# SCH200

IEC-61850-3, IEEE-1613 1U Fanless
Power Automation Computer

## User's Manual

Revision Date: July. 10. 2020

# Safety Information

## Electrical safety

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

## Operation safety

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

## Statement

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

## Revision History

| Revision | Date (yyyy/mm/dd) | Changes |
|---|---|---|
| V1.0 | 2020/06/10 | First release |
| V1.1 | 2020/07/10 | Update the LAN module for optional. |

## Packing list

| Item | Description | Q'ty |
|---|---|---|
| 1 | SCH200 Embedded System | 1 |
| 2 | Driver CD | 1 |
| 3 | 3-pin Terminal Block Power Connector (For DC Power Input) | 1 |

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

**Perfectron RoHS Environmental Policy and Status Update**

Perfectron is a global citizen for building the digital infrastructure. We are committed to providing green products and services, which are compliant with

European Union RoHS (Restriction on Use of Hazardous Substance in Electronic Equipment) directive 2011/65/EU, to be your trusted green partner and to protect our environment.

In order to meet the RoHS compliant directives, Perfectron has established an engineering and manufacturing task force to implement the introduction of green products. The task force will ensure that we follow the standard Perfectron development procedure and that all the new RoHS components and new manufacturing processes maintain the highest industry quality levels for which Perfectron are renowned.

The model selection criteria will be based on market demand. Vendors and suppliers will ensure that all designed components will be RoHS compliant

**Safety Information** ..... 1
**Electrical safety** ..... 1
**Operation safety** ..... 1
**Statement** ..... 1
**Revision History** ..... 2
**Packing list** ..... 2
Perfectron RoHS Environmental Policy and Status Update ..... 3
**Chapter 1: Product Introduction** ..... 5
1.1 Specifications ..... 5
1.2 Front Panel i/o Placement ..... 7
1.3 Mechanical Dimension ..... 8
**Chapter 2: Front Panel Connector Pin Definitions** ..... 9
2.1 Front Panel Connector ..... 9
2.2 Front Panel Connector: Optional LAN module ..... 9
**Chapter 3: BIOS Specification** ..... 10
3.1 MAIN PAGE ..... 10
3.2 ADVANCED PAGE ..... 13
3.1.1 CPU CONFIGURATION ..... 15
3.1.2 TRUSTED COMPUTING (OPTIONAL) ..... 18
3.2.3 ACPI SETTINGS ..... 20
3.2.4 SMART SETTINGS ..... 21
3.2.5 SUPER IO CONFIGURATION ..... 22
3.2.5 NCT6116D HW MONITOR ..... 29
3.3 CHIPSET PAGE ..... 35
3.3.1 SYSTEM AGENT (SA) CONFIGURATION ..... 36
3.4 SECURITY PAGE ..... 42
3.4.1 HDD SECURITY ..... 44
3.4.2 SECURE BOOT ..... 46
3.4.3 bios update ..... 53
3.5 BOOT PAGE ..... 54
3.5.1 (LIST BOOT DEVICE TYPE) DRIVE BBS PRIORITIES ..... 58
3.6 SAVE & EXIT PAGE ..... 59
3.7 RECOVERY PAGE (ACTIVE FOR 3.4.3 SECURE FLASH UPDATE ONLY) ..... 60

# Chapter 1: Product Introduction

## 1.1 Specifications

| | |
|---|---|
| **System** | |
| CPU | Socket LGA 1151 for Intel® Core i7/i5/i3/Celeron® (Supports up to 65W) Intel® |
| Memory type | 2 x SO-DIMM DDR4 2400/2666 MHz up to 64GB |
| Chipset | Intel® Q370 Chipset |
| **Display** | |
| Display Port<br>HDMI | Resolution up to 4096 x 2304 60@Hz<br>Resolution up to 4096 x 2160 30@Hz |
| **Storage** | |
| M.2 | Up to 1TB<br>SSD RAID 0/1 (Optional) |
| **Ethernet** | |
| Ethernet | 2 x 100Base-FX port supported<br>2 x 100Base-TX port supported |
| **Rear I/O** | |
| Display | 1 x Display port<br>1 x HDMI port |
| Ethernet | 4 x RJ45 ( 2 x 10Gb/s SFP+ or 4 x 1Gb/s Base-T RJ45 , optional) |
| Audio | 2 x 3.5mm Audio Jacks (1 x MIC, 1 x Line-Out) |
| USB | 4 x USB 3.0 |
| DC-IN | 2 x DC-in (Redundant Optional) |
| Button | 1 x Power Button w/Indicator LED |
| COM | 8 x ports (6 x RS-232/422/485 support, 2 x RS-232) |
| **Power Requirement** | |
| Power Input | 125V DC-IN (this version) |
| **Applications, Operating System** | |
| Applications | Energy/Smart Grid/Power Plant Management, Intelligent Automation and manufacturing applications |

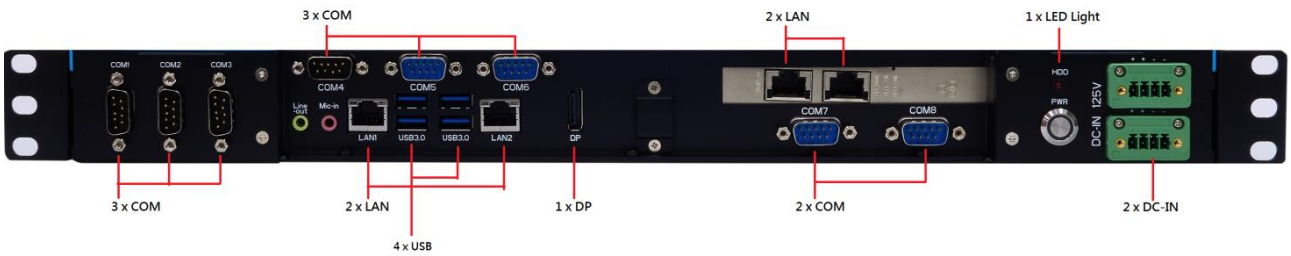
| | |
|---|---|
| Operating System | Windows 10 64Bit ,Windows server 2012 r2, Windows server 2016<br>Ubuntu13.04, Ubuntu13.10, Ubuntu14.04, Fedora20 |

| **Physical** | |
|---|---|
| Dimension | 450 x 482 x 44 mm (W x D x H) |
| Operation Temp. | -20°C to 60°C |
| Storage Temp. | -40°C to 85°C |
| Relative Humidity | 5% to 95%, non-condensing |
| System Design | Conduction Cooing |
| Heatsink | Aluminum Alloy, Corrosion Resistant |
| Finish | Anodic aluminum oxide |

| **Environment** | | |
|---|---|---|
| MIL-STD-810G Test | | |
| Operating Tests | | |
| Low Temperature | Method 502.5<br>Procedure 2 | exposure(24h x 3 cycle) at -40℃ min. |
| High Temperature | Method 501.5<br>Procedure 2 | 60ºC for 2 hours after temperature stabilization. |
| Humidity | Method 507.5<br>Procedure 2 | RH -95%. Test cycles: ten 24-hours , functional test after 5th and 10th cycles |
| Vibration | Method 514.6<br>Category 20 | 10—500Hz 1.04Grms<br>Test duration: 1 hours x 3 axis (total 3 hours) |
| Shock | Method 516.6<br>Procedure 1 | 20G, 11mSec, 3 per axis |
| Non-Operating Tests | | |
| Low Temperature Storage | Method 502.5 | exposure(24h x 7 cycle) at -40℃ min. |
| High Temperature Storage | Method 501.5<br>Procedure 1 | 71ºC for 2 hours after temperature stabilization. |

| | | |
|---|---|---|
| Vibration | Method 514.6<br>Category 24 | 200 to 2000Hz<br>Test duration: One hour per axis; rms = 7.7 gs |
| Shock | Method 516.6<br>Procedure V | 40G, 11ms, 3 pluse. |

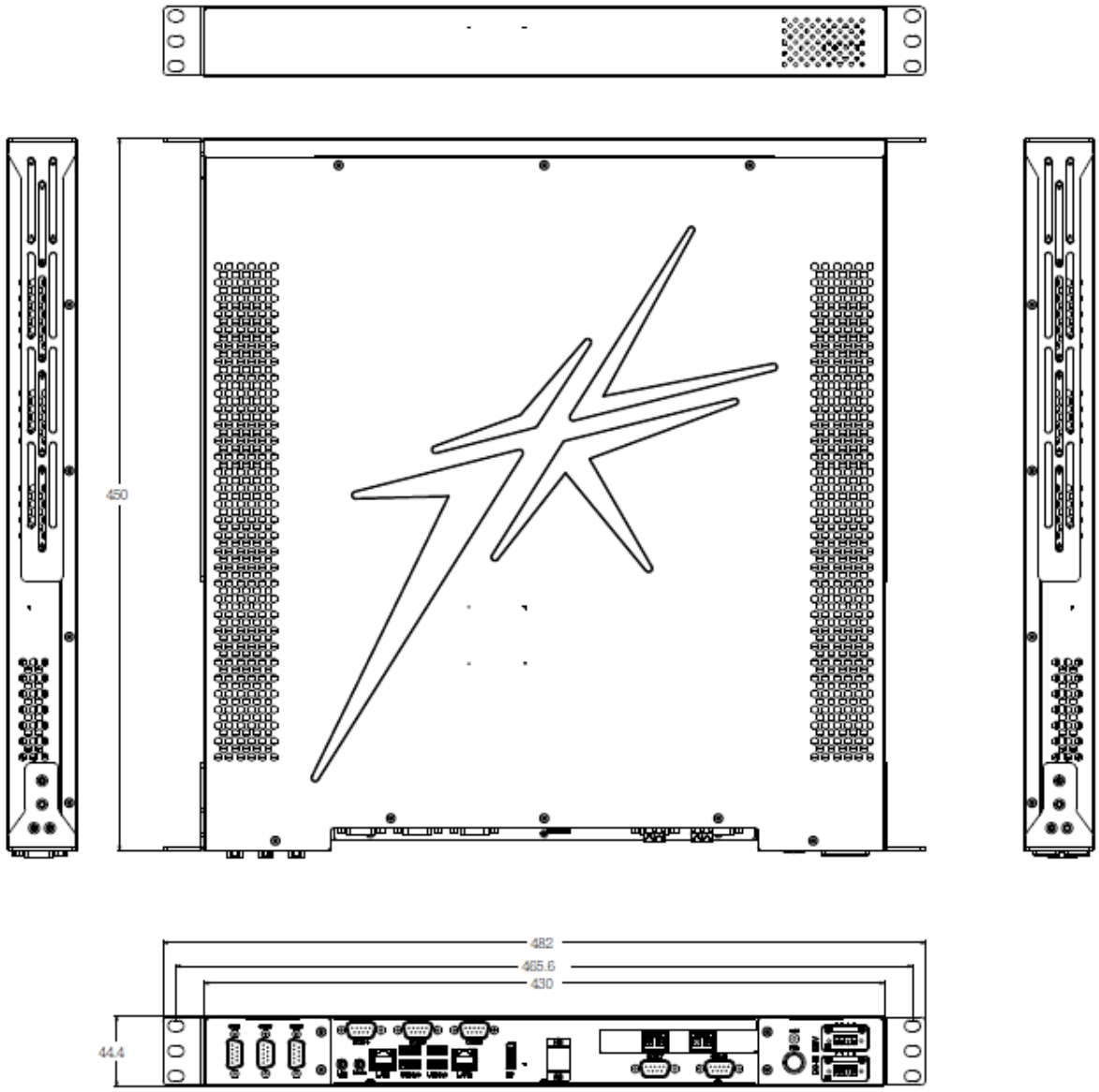
### 1.2 Front Panel i/o Placement




| | |
|---|---|
| 1 | COM x 8 |
| 2 | USB 3.0 x 4 |
| 3 | LAN x 4 |
| 4 | Display Port x 1 |
| 5 | Audio Jack (Mic-in, Line-out) |
| 6 | Power Button with LED light x1 |
| 7 | DC-IN x 2 |

*Optional:
Intel 82599ES Lan card, 2*10Gb/s SFP+, Gen2 PCI-e x8
Intel I350-AM4 Lan card, 4*1Gb/s Base-T RJ45, Gen2 PCI-ex8

### 1.3 Mechanical Dimension



# Chapter 2: Front Panel Connector Pin Definitions

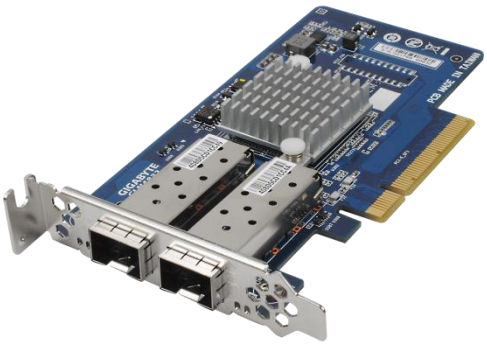
## 2.1 Front Panel Connector

| COM | DEFINITION |
|---|---|
| COM1 | RS-232/422/485 via mother Board |
| COM2 | RS-232/422/485 via mother board |
| COM3 | RS-232 via mother board |
| COM4 | RS-232 via mother board |
| COM5 | RS-232/422/485 |
| COM6 | RS-232/422/485 |
| COM7 | RS-232/422/485 |
| COM8 | RS-232/422/485 |

## 2.2 Front Panel Connector: Optional LAN Card Module

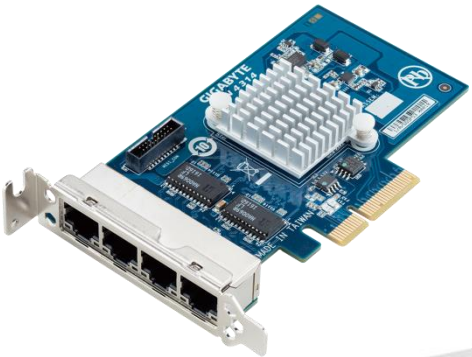
OPTIONAL 1: Intel® 82599ES 10Gb/s 2-port LAN Card

- Intel® 82599ES
- 2 x SFP+ LAN ports
- Supports 10Gb/s per port
- PCIe x8 (Gen2 x8 bus)



OPTIONAL 2: Intel® I350-AM4 1Gb/s 4-port LAN Card

- Intel® I350-AM4
- 4 x 1000BASE-T RJ45 LAN ports
- Supports 1Gb/s, 100Mb/s per port
- PCIe x4 (Gen2 x4 bus)



# Chapter 3: BIOS Specification

## 3.1 MAIN PAGE

| Main | Advanced | Chipset | Security | Boot | Save & Exit |
|---|---|---|---|---|---|

| BIOS Information | | Item help |
|---|---|---|
| BIOS Vender | American Megatrends | |
| Core Version | 5.13 | |
| Compliancy | UEFI 2.6 ; PI 1.4 | |
| BIOS Version | D7980A01 | |
| Build Date and Time | 04/21/2017 | |
| ME FW Version | 11.8.50.3399 | |
| **Processor Information** | | |
| Intel(R) CORE(TM) i3-9100 CPU @ 3.60GHz | | |
| **Memory Information** | | |
| Total Memory | 32768 MB | |
| DIMM#1 | 16384 MB (DDR4) | |
| DIMM#2 | 16384 MB (DDR4) | →←: Select Screen |
| Memory Frequency | 2133 MHz | ↑↓: Select Item |
| | | Enter: Select |
| SATA1 | Empty | +/- : Change Opt. |
| SATA2 | Empty | F1: General Help |
| SATA3 | Empty | |
| SATA4(M.2) | Empty | |
| | | F2: Previous Values |
| | | F3: Optimized Defaults |
| System Date | [Www mm/dd/yyyy] | F4: Save & Reset |
| System Time | [hh:mm:ss] | ESC: Exit |

Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.

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

| Field Name | **Core Version** |
|---|---|
| Default Value | 5.12 |
| Comment | This field is not selectable. There is no help text associated with it. |

| Field Name | **Compliancy** |
|---|---|
| Default Value | UEFI 2.6 ; PI 1.4 |
| 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 and Time** |
|---|---|
| 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 FW Version** |
|---|---|
| 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 | **DIMM#[1:2]** |
| Help | Memory in the DIMM. |
| 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 | **SATA1** |
| 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 :<br>Mon/Tue/Wed/Thu/Fri/Sat/Sun<br>mm : 1-12<br>dd : 1-31<br>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<br>mm : 0-59<br>ss : 0-59 |
| Help | Set the Time. Use Tab to switch between Time elements. |

### 3.2 ADVANCED PAGE

| Main | Advanced | Chipset | Security | Boot | Save & Exit |
|---|---|---|---|---|---|

| | |
|---|---|
| ► CPU Configuration | **Item help** |
| ► Trusted Computing | |
| ► ACPI Settings | |
| ► SMART Settings | |
| ► Super IO Configuration | |
| ► NCT6116D HW Monitor | **→←: Select Screen** |
| ► S5 RTC Wake Settings | **↑↓: Select Item** |
| ► NVMe Configuration | **Enter: Select** |
| | **+/- : Change Opt** |
| ► Network Stack Configuration | **F1: General Help** |
| | **F2: Previous Values** |
| | **F3: Optimized Defaults** |
| | **F4: Save & Reset** |
| | **ESC: Exit** |

**Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.**

| Field Name | **CPU Configuration** |
|---|---|
| Help | CPU Configuration Parameters. |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

| Field Name | **Trusted Computing** |
|---|---|
| Help | Trusted Computing Settings |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

| Field Name | **ACPI Settings** |
|---|---|
| Help | System ACPI Parameters. |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

| Field Name | **SMART Settings** |
|---|---|
| Help | System SMART Settings. |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

| Field Name | **Super IO Configuration** |
|---|---|
| Help | System Super IO Chip Parameters. |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

| Field Name | **NCT6116D HW Monitor** |
|---|---|
| Help | Monitor hardware status |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

| Field Name | **S5 RTC Wake Settings** |
|---|---|
| Help | Enable system to wake from S5 using RTC alarm. |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

| Field Name | **Network Stack Configuration** |
|---|---|
| Help | Network Stack Settings. |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

| Field Name | **NVMe Configuration** |
|---|---|
| Help | NVMe Device Options Setting. |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

### 3.1.1 CPU CONFIGURATION

| Main | Advanced | Chipset | Security | Boot | Save & Exit |
|---|---|---|---|---|---|

| CPU Configuration | | Item help |
|---|---|---|
| Type | Intel(R) Core(TM) CPU i3-9100 @ 3.60 GHz | |
| ID | 0x806E9 | |
| Speed | 3600 MHz | |
| L1 Data Cache | 32 KB x 2 | |
| L1 Instruction Cache | 32 KB x 2 | |
| L2 Cache | 256 KB x 2 | |
| L3 Cache | 3MB | |
| L4 Cache | N/A | |
| VMX | Supported | |
| SMX/TXT | Supported | |
| Intel Trusted Execution Technology | [Disabled] | →←: Select Screen<br>↑↓: Select Item<br>Enter: Select<br>+/- : Change Opt<br>F1: General Help<br>F2: Previous Values<br>F3: Optimized Defaults<br>F4: Save & Reset<br>ESC: Exit |

Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.

| Field Name | **Type** |
|---|---|
| Default Value | [Intel CPU Brand String] |
| Comment | This field is not selectable. There is no help text associated with it. |

| Field Name | **ID** |
|---|---|
| Default Value | Displays CPU Signature |
| Comment | This field is not selectable. There is no help text associated with it. |

| Field Name | **Speed** |
|---|---|
| Default Value | Displays the CPU Speed |
| Comment | This field is not selectable. There is no help text associated with it. |

| Field Name | **L1 Data Cache** |
|---|---|
| Default Value | L1 Data Cache Size |
| Comment | This field is not selectable. There is no help text associated with it. |

| Field Name | **L1 Instruction Cache** |
|---|---|
| Default Value | L1 Code Cache Size |
| Comment | This field is not selectable. There is no help text associated with it. |

| Field Name | **L2 Cache** |
|---|---|
| Default Value | L2 Cache Size |
| Comment | This field is not selectable. There is no help text associated with it. |

| Field Name | **L3 Cache** |
|---|---|
| Default Value | L3 Cache Size |
| Comment | This field is not selectable. There is no help text associated with it. |

| Field Name | **L4 Cache** |
|---|---|
| Default Value | L4 Cache Size |
| Comment | This field is not selectable. There is no help text associated with it. |

| | |
|---|---|
| Field Name | **VMX** |
| Default Value | VMX Supported or Not |
| Comment | This field is not selectable. There is no help text associated with it. |

| | |
|---|---|
| Field Name | **SMX/TXT** |
| Default Value | SMX/TXT Supported or Not |
| Comment | This field is not selectable. There is no help text associated with it. |

| | |
|---|---|
| Field Name | **Intel Trusted Execution Technology(Dependent on dTPM enable)** |
| Default Value | [Disabled] |
| Possible Value | Enabled<br>Disabled |
| Help | Enables utilization of additional hardware capabilities provided by Intel<br>(R) Trusted Execution Technology.<br>Changes require a full power cycle to take effect. |

### 3.1.2 TRUSTED COMPUTING (OPTIONAL)

| Main | Advanced | Chipset | Security | Boot | Save & Exit |
|---|---|---|---|---|---|

| | | |
|---|---|---|
| **TPM20 Device Found** | | **Item help** |
| **Vender : NTC** | | |
| **Firmware Version: 1.3** | | |
| Security Device Support | [Enable] | |
| Pending operation | [None] | →←: Select Screen |
| TPM2.0 UEFI Spec Version | [TCG_2] | ↑↓: Select Item |
| | | Enter: Select |
| | | +/- : Change Opt |
| | | F1: General Help |
| | | F2: Previous Values |
| | | F3: Optimized Defaults |
| | | F4: Save & Reset |
| | | ESC: Exit |

Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.

| Field Name | **Security Device SUPPORT** |
|---|---|
| Default Value | [Enable] |
| Possible Value | Enable<br>Disable |
| Help | 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. |

| Field Name | **Pending operation** |
|---|---|
| Default Value | [None] |
| Possible Value | None<br>TPM Clear |
| Help | Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change State of Security Device. |

| Field Name | **TPM2.0 UEFI Spec Version** |
|---|---|
| Default Value | [TCG_2] |
| Possible Value | TCG_1_2<br>TCG_2 |
| Help | Select the TCG2 Spec Version Support,TCG_1_2: the Compatible mode for Win8/Win10,TCG_2: Support new TCG2 protocol and event format for Win10 or later. |

### 3.2.3 ACPI SETTINGS

| Main | Advanced | Chipset | Security | Boot | Save & Exit |
|---|---|---|---|---|---|

**ACPI Settings**

| | | Item help |
|---|---|---|
| Enable ACPI Auto Configuration | [Disabled] | →←: Select Screen |
| | | ↑↓: Select Item |
| Enable Hibernation | [Enabled] | Enter: Select |
| ACPI Sleep State | [S3 (Suspend to RAM)] | +/- : Change Opt |
| | | F1: General Help |
| | | F2: Previous Values |
| | | F3: Optimized Defaults |
| | | F4: Save & Reset |
| | | ESC: Exit |

Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.

| Field Name | **Enable ACPI Auto Configuration** |
|---|---|
| Default Value | [Disabled] |
| Possible Value | Enabled<br>Disabled |
| Help | Enables or Disables BIOS ACPI Auto Configuration. |

| Field Name | **Enable Hibernation** |
|---|---|
| Default Value | [Enabled] |
| Possible Value | Enabled<br>Disabled |
| Help | Enables or Disables System ability to Hibernate (OS/S4 Sleep State).<br>This option may be not effective with some operating systems. |

| Field Name | **ACPI Sleep State** |
|---|---|
| Default Value | [S3 (Suspend to RAM)] |
| Possible Value | Suspend Disabled<br>S3 (Suspend to RAM) |
| Help | Select the highest ACPI sleep state the system will enter when the SUSPEND button is pressed. |

### 3.2.4 SMART SETTINGS

| Main | Advanced | Chipset | Security | Boot | Save & Exit |
|---|---|---|---|---|---|

| SMART Settings | | Item help |
|---|---|---|
| SMART Self Test | [Disabled] | →←: Select Screen<br>↑↓: Select Item<br>Enter: Select<br>+/- : Change Opt<br>F1: General Help<br>F2: Previous Values<br>F3: Optimized Defaults<br>F4: Save & Reset<br>ESC: Exit |

Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.

| Field Name | **SMART Self Test** |
|---|---|
| Default Value | [Disabled] |
| Possible Value | Disabled<br>Enabled |
| Help | Run SMART Self Test on all HDDs during POST. |

### 3.2.5 SUPER IO CONFIGURATION

| Main | Advanced | Chipset | Security | Boot | Save & Exit |
|---|---|---|---|---|---|

| SIO Configuration | | Item help |
|---|---|---|
| Super IO Chip | NCT6116D | |
| ► Serial Port 1 Configuration | | →←: Select Screen |
| ► Serial Port 2 Configuration | | ↑↓: Select Item |
| ► Serial Port 3 Configuration | | Enter: Select |
| ► Serial Port 4 Configuration | | +/- : Change Opt |
| | | F1: General Help |
| | | F2: Previous Values |
| | | F3: Optimized Defaults |
| | | F4: Save & Reset |
| | | ESC: Exit |

Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.

| Field Name | **Serial Port 1 Configuration** |
|---|---|
| Help | Set Parameters of Serial Port 1 (COMA) |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

| Field Name | **Serial Port 2 Configuration** |
|---|---|
| Help | Set Parameters of Serial Port 2 (COMB) |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

| Field Name | **Serial Port 3 Configuration** |
|---|---|
| Help | Set Parameters of Serial Port 3 (COMC) |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

| Field Name | **Serial Port 4 Configuration** |
|---|---|
| Help | Set Parameters of Serial Port 4 (COMD) |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

### ▪ 3.2.5.1 Serial Port 1 Configuration

| Main | Advanced | Chipset | Security | Boot | Save & Exit |
|---|---|---|---|---|---|

| Serial Port 1 Configuration | | Item help |
|---|---|---|
| Serial Port | [Enabled] | →←: Select Screen |
| Device Settings | IO=3E8h; IRQ=7; | ↑↓: Select Item |
| | | Enter: Select |
| Change Settings | [Auto] | +/- : Change Opt |
| Mode Configuration | [3T/5R RS232] | F1: General Help |
| | | F2: Previous Values |
| | | F3: Optimized Defaults |
| | | F4: Save & Reset |
| | | ESC: Exit |

Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.

| Field Name | **Serial Port** |
|---|---|
| Default Value | [Enabled] |
| Possible Value | Disabled<br>Enabled |
| Help | Enable or Disable Serial Port(COM) |

| Field Name | **Device Settings** |
|---|---|
| Default Value | Device Super IO COM1 Address and IRQ. |
| Comment | This field is not selectable. There is no help text associated with it. |

| Field Name | **Change Settings** |
|---|---|
| Default Value | [Auto] |
| Possible Value | Auto<br>IO=3E8h; IRQ=7;<br>IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12;<br>IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;<br>IO=2F0h; IRQ=3,4,5,6,7,9,10,11,12;<br>IO=2E0h; IRQ=3,4,5,6,7,9,10,11,12; |
| Help | Select an optimal settings for Super IO Device |

| Field Name | **Mode Configuration** |
|---|---|
| Default Value | [3T/5R RS232] |
| Possible Value | 1T/1R RS422<br>3T/5R RS232<br>1T/1R RS485 TX ENABLE Low Active |
| | 1T/1R RS485 with termination resistor TX ENABLE Low Active<br>Disabled |
| Help | Configure serial port as RS232/RS422/RS485. |

- **3.2.5.2 Serial Port 2 Configuration**

| Main | Advanced | Chipset | Security | Boot | Save & Exit |
|---|---|---|---|---|---|

| Serial Port 2 Configuration | | Item help |
|---|---|---|
| Serial Port | [Enabled] | →←: Select Screen |
| Device Settings | IO=2E8h; IRQ=7; | ↑↓: Select Item |
| | | Enter: Select |
| Change Settings | [Auto] | +/- : Change Opt |
| Mode Configuration | [3T/5R RS232] | F1: General Help |
| | | F2: Previous Values |
| | | F3: Optimized Defaults |
| | | F4: Save & Reset |
| | | ESC: Exit |

Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.

| Field Name | **Serial Port** |
|---|---|
| Default Value | [Enabled] |
| Possible Value | Disabled<br>Enabled |
| Help | Enable or Disable Serial Port(COM) |

| Field Name | **Device Settings** |
|---|---|
| Default Value | Device Super IO COM2 Address and IRQ. |
| Comment | This field is not selectable. There is no help text associated with it. |

| Field Name | **Change Settings** |
|---|---|
| Default Value | [Auto] |
| Possible Value | Auto<br>IO=2E8h; IRQ=7;<br>IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12;<br>IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;<br>IO=2F0h; IRQ=3,4,5,6,7,9,10,11,12;<br>IO=2E0h; IRQ=3,4,5,6,7,9,10,11,12; |
| Help | Select an optimal settings for Super IO Device |

| Field Name | **Mode Configuration** |
|---|---|
| Default Value | [3T/5R RS232] |
| Possible Value | 1T/1R RS422<br>3T/5R RS232<br>1T/1R RS485 TX ENABLE Low Active<br>1T/1R RS485 with termination resistor TX ENABLE Low Active Disabled |
| Help | Configure serial port as RS232/RS422/RS485. |

### ▪ 3.2.5.3 Serial Port 3 Configuration

| Main | Advanced | Chipset | Security | Boot | Save & Exit |
|---|---|---|---|---|---|

| Serial Port 3 Configuration | | Item help |
|---|---|---|
| Serial Port | [Enabled] | →←: Select Screen |
| Device Settings | IO=2F0h; IRQ=7; | ↑↓: Select Item |
| | | Enter: Select |
| Change Settings | [Auto] | +/- : Change Opt |
| | | F1: General Help |
| | | F2: Previous Values |
| | | F3: Optimized Defaults |
| | | F4: Save & Reset |
| | | ESC: Exit |

Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.

| Field Name | **Serial Port** |
|---|---|
| Default Value | [Enabled] |
| Possible Value | Disabled<br>Enabled |
| Help | Enable or Disable Serial Port(COM) |

| Field Name | **Device Settings** |
|---|---|
| Default Value | Device Super IO COM3 Address and IRQ. |
| Comment | This field is not selectable. There is no help text associated with it. |

| Field Name | **Change Settings** |
|---|---|
| Default Value | [Auto] |
| Possible Value | Auto<br>IO=2E0h; IRQ=7;<br>IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12;<br>IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;<br>IO=2F0h; IRQ=3,4,5,6,7,9,10,11,12;<br>IO=2E0h; IRQ=3,4,5,6,7,9,10,11,12; |

| | |
|---|---|
| Help | Select an optimal settings for Super IO Device |

- **2.2.5.4 Serial Port 4 Configuration**

| Main | Advanced | Chipset | Security | Boot | Save & Exit |
|---|---|---|---|---|---|

| Serial Port 4 Configuration | | Item help |
|---|---|---|
| Serial Port | [Enabled] | →←: Select Screen |
| Device Settings | IO=3F8h; IRQ=4; | ↑↓: Select Item |
| | | Enter: Select |
| Change Settings | [Auto] | +/- : Change Opt |
| | | F1: General Help |
| | | F2: Previous Values |
| | | F3: Optimized Defaults |
| | | F4: Save & Reset |
| | | ESC: Exit |

Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.

| Field Name | **Serial Port** |
|---|---|
| Default Value | [Enabled] |
| Possible Value | Disabled<br>Enabled |
| Help | Enable or Disable Serial Port(COM) |

| Field Name | **Device Settings** |
|---|---|
| Default Value | Device Super IO COM4 Address and IRQ. |
| Comment | This field is not selectable. There is no help text associated with it. |

| Field Name | **Change Settings** |
|---|---|
| Default Value | [Auto] |
| Possible Value | Auto<br>IO=3F8h; IRQ=4;<br>IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12;<br>IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12; |

| | |
|---|---|
| | IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12;<br>IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12; |
| Help | Select an optimal settings for Super IO Device |

### 3.2.5 NCT6116D HW MONITOR

| Main | Advanced | Chipset | Security | Boot | Save & Exit |
|---|---|---|---|---|---|

| PC Health Status | | Item help |
|---|---|---|
| CPU temperature | : xx °C | →←: Select Screen |
| CPU VR temperature | : xx °C | ↑↓: Select Item |
| DIMM temperature | : xx °C | Enter: Select |
| CPU Fan Speed | : xxxx RPM | +/- : Change Opt |
| System Fan Speed | : xxxx RPM | |
| VCORE | : x.xxx V | F1: General Help |
| PCH IO volt | : x.xxx V | |
| System Memory | : x.xxx V | F2: Previous Values |
| AVSB | : x.xxx V | F3: Optimized Defaults |
| VSB3V | : x.xxx V | F4: Save & Reset |
| | | ESC: Exit |

Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.

- **3.2.6 S5 RTC WAKE SETTINGS**

| Main | Advanced | Chipset | Security | Boot | Save & Exit |
|---|---|---|---|---|---|

| | | |
|---|---|---|
| Wake system from S5 | [Disabled] | **Item help** |
| | | **→←: Select Screen**<br>**↑↓: Select Item**<br>**Enter: Select**<br>**+/- : Change Opt**<br>**F1: General Help**<br>**F2: Previous Values**<br>**F3: Optimized Defaults**<br>**F4: Save & Reset**<br>**ESC: Exit** |

**Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.**

| | |
|---|---|
| Field Name | Wake system from S5 |
| Default Value | [Disabled] |
| Possible Value | Disabled<br>Fixed Time |
| Help | Enabler or disable System wake on alarm event, Select FixedTime,<br>system will wake on the hr::min::sec specified. |

| | |
|---|---|
| Field Name | Wake up hour(Show when Wake system from S5 set to Fixed Time) |
| Default Value | 0 |
| Possible Value | 0-23 |
| Help | Select 0-23 For example enter 3 for 3am and 15 for 3pm |

| | |
|---|---|
| Field Name | Wake up minute(Show when Wake system from S5 set to Fixed Time) |
| Default Value | 0 |
| Possible Value | 0-59 |
| Help | select 0-59 for Minute |

| | |
|---|---|
| Field Name | Wake up second(Show when Wake system from S5 set to Fixed Time) |
| Default Value | 0 |
| Possible Value | 0 - 59 |
| Help | select 0-59 for Second |

### ▪ 3.2.7 NETWORK STACK CONFIGURATION

| Main | Advanced | Chipset | Security | Boot | Save & Exit | |
|---|---|---|---|---|---|---|
| Network stack | | | [Disabled] | | | Item help |
| | | | | | | →←: Select Screen<br>↑↓: Select Item<br>Enter: Select<br>+/- : Change Opt<br>F1: General Help<br>F2: Previous Values<br>F3: Optimized Defaults<br>F4: Save & Reset<br>ESC: Exit |
| Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc. | | | | | | |

| Field Name | **Network stack** |
|---|---|
| Default Value | [Disabled] |
| Possible Value | Disabled<br>Enabled |
| Help | Enable/Disable UEFI Network stack. |

| Field Name | **Ipv4 PXE Support** |
|---|---|
| Default Value | [Disabled] |
| Possible Value | Disabled<br>Enabled |
| Help | Enable/Disable IPv4 PXE boot support. If disabled, IPv4 PXE boot<br>support will not be available. |

| Field Name | **Ipv6 PXE Support** |
|---|---|
| Default Value | [Disabled] |
| Possible Value | Disabled<br>Enabled |
| Help | Enable/Disable IPv6 PXE boot support. If disabled, IPv6 PXE boot<br>support will not be available. |

### ▪ 3.2.8 NVME CONFIGURATION

| Main | Advanced | Chipset | Security | Boot | Save & Exit |
|---|---|---|---|---|---|

| NVMe Configuration | Item help |
|---|---|
| No NVME Device Found | →←: Select Screen<br>↑↓: Select Item<br>Enter: Select<br>+/- : Change Opt<br>F1: General Help<br>F2: Previous Values<br>F3: Optimized Defaults<br>F4: Save & Reset<br>ESC: Exit |

Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.

## 3.3 CHIPSET PAGE

| Main | Advanced | Chipset | Security | Boot | Save & Exit |
|---|---|---|---|---|---|

| | |
|---|---|
| ► System Agent (SA) Configuration<br>► PCH-IO Configuration | **Item help**<br><br>**→←: Select Screen**<br>**↑↓: Select Item**<br>**Enter: Select**<br>**+/- : Change Opt**<br>**F1: General Help**<br>**F2: Previous Values**<br>**F3: Optimized Defaults**<br>**F4: Save & Reset**<br>**ESC: Exit** |

**Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.**

| Field Name | **System Agent (SA) Configuration** |
|---|---|
| Help | System Agent (SA) Parameters |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

| Field Name | **PCH-IO Configuration** |
|---|---|
| Help | PCH Parameters |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

### 3.3.1 SYSTEM AGENT (SA) CONFIGURATION

| Main | Advanced | Chipset | Security | Boot | Save & Exit |
|---|---|---|---|---|---|

| System Agent (SA) Configuration | Item help |
|---|---|
| ► Graphics Configuration | |
| | →←: Select Screen<br>↑↓: Select Item<br>Enter: Select<br>+/- : Change Opt<br>F1: General Help<br>F2: Previous Values<br>F3: Optimized Defaults<br>F4: Save & Reset<br>ESC: Exit |

Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.

| Field Name | **Graphics Configuration** |
|---|---|
| Help | Graphics Configuration |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

### 3.3.1.1 Graphics Configuration

| Main | Advanced | Chipset | Security | Boot | Save & Exit |
|---|---|---|---|---|---|

| Graphics Configuration | | Item help |
|---|---|---|
| DVMT Pre-Allocated | [64M] | →←: Select Screen |
| DVMT Total Gfx Mem | [256M] | ↑↓: Select Item |
| | | Enter: Select |
| | | +/- : Change Opt |
| | | F1: General Help |
| | | F2: Previous Values |
| | | F3: Optimized Defaults |
| | | F4: Save & Reset |
| | | ESC: Exit |

Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.

| Field Name | **DVMT Pre-Allocated** |
|---|---|
| Default Value | [64M] |
| Possible Value | 64M /32M/F7/ 36M/ 40M/ 44M/ 48M/ 52M/ 56M/ 60M |
| Help | Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by<br>the Internal Graphics Device. |

| Field Name | **DVMT Total Gfx Mem** |
|---|---|
| Default Value | [256M] |
| Possible Value | 128MB / 256MB / MAX |
| Help | Select DVMT5.0 Total Graphic Memory size used by the Internal<br>Graphics Device. |

### 3.3.2 PCH-IO CONFIGURATION

| Main | Advanced | Chipset | Security | Boot | Save & Exit |
|---|---|---|---|---|---|

| PCH-IO Configuration | | Item help |
|---|---|---|
| ► SATA And RST Configuration | | |
| ► HD Audio Configuration | | →←: Select Screen |
| | | ↑↓: Select Item |
| Wake On LAN | [Disabled] | Enter: Select |
| DeepSx Power Policies | [Enable in S4-S5] | +/- : Change Opt |
| State After G3 | [S5 State] | F1: General Help |
| Chassis Intrusion | [Enable] | |
| | | F2: Previous Values |
| | | F3: Optimized Defaults |
| | | F4: Save & Reset |
| | | ESC: Exit |

Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.

| Field Name | **SATA And RST Configuration** |
|---|---|
| Help | SATA Device Options Settings |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

| Field Name | **HD Audio Configuration** |
|---|---|
| Help | HD Audio Subsystem Configuration Settings |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

| Field Name | **DeepSx Power Policies** |
|---|---|
| Default Value | [Enabled in S4-S5] |
| Possible Value | Enabled in S4-S5<br>Disabled |
| Help | configure the DeepSx Mode configuration. |

| Field Name | **Wake On LAN** |
|---|---|
| Default Value | [Disabled] |
| Possible Value | Enabled<br>Disabled |
| Help | Enabled/Disabled integrated LAN to wake the system. |

| Field Name | **State After G3** |
|---|---|
| Default Value | [S5 State] |
| Possible Value | S0 State<br>S5 State |
| Help | Specify what state to go to when power is re-applied after a power |
| | failure (G3 state). |

| Field Name | **Chassis Intrusion** |
|---|---|
| Default Value | [Enable] |
| Possible Value | Disable<br>Enable<br>Reset |
| Help | Configure Chassis Intrusion. |

### 3.3.2.1 SATA And RST Configuration

| Main | Advanced | Chipset | Boot | Security | Save & Exit |
|---|---|---|---|---|---|

| SATA And RST Configuration | | Item help |
|---|---|---|
| SATA Mode Selection | [AHCI] | |
| | | →←: Select Screen<br>↑↓: Select Item<br>Enter: Select<br>+/- : Change Opt<br>F1: General Help<br>F2: Previous Values<br>F3: Optimized Defaults<br>F4: Save & Reset<br>ESC: Exit |

Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.

| Field Name | **SATA Mode Selection** |
|---|---|
| Value | [AHCI] |
| Possible Value | AHCI / Intel RST Premium With Intel Optane System Acceleration |
| Help | Determines how SATA controller(s) operate. |

### 3.2.2.2 HD Audio Configuration

| Main | Advanced | Chipset | Boot | Security | Save & Exit |
|---|---|---|---|---|---|

| HD Audio Subsystem Configuration Settings | | Item help |
|---|---|---|
| HD Audio | [Enable] | |
| | | →←: Select Screen<br>↑↓: Select Item<br>Enter: Select<br>+/- : Change Opt<br>F1: General Help<br>F2: Previous Values<br>F3: Optimized Defaults<br>F4: Save & Reset<br>ESC: Exit |

Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.

| Field Name | **HD Audio** |
|---|---|
| Value | [Enable] |
| Possible Value | Enable / Disable |
| Help | Control Detection of the HD-Audio device.<br>Disabled = HDA will be unconditionally<br>disabled Enable = HDA will be<br>unconditionally enabled |

### 3.4 SECURITY PAGE

| Main | Advanced | Chipset | Security | Boot | Save & Exit |
|---|---|---|---|---|---|

| Password Description | | Item help |
|---|---|---|
| If Only the Administrator's password is set, then this only limits access to Setup and is only asked for when entering Setup. | | |
| If ONLY the User's password is set, then this is a power on password and must be entered to boot or enter Setup. In Setup the User will have Administrator rights.. | | |
| The password length must be in the following range: | | |
| Minimum length | 3 | |
| Maximum length | 20 | →←: Select Screen |
| | | ↑↓: Select Item |
| Administrator Password | | Enter: Select |
| User Password | | +/- : Change Opt |
| | | F1: General Help |
| HDD Security Configuration: | | F2: Previous Values |
| HDD Security drive | | F3: Optimized Defaults |
| | | F4: Save & Reset |
| ► Secure Boot | | ESC: Exit |
| ► BIOS Update | | |

Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.

| | |
|---|---|
| Field Name | **Administrator Password** |
| Help | Set Administrator Password |

| | |
|---|---|
| Field Name | **User Password** |
| Help | Set User Password. |

| | |
|---|---|
| Field Name | **HDD Security drive** |
| Help | HDD Security Configuration for selected drive |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

| | |
|---|---|
| Field Name | **Secure Boot** |
| Help | Secure Boot configuration |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

| | |
|---|---|
| Field Name | **BIOS Update** |
| Help | BIOS Update support |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

### 3.4.1 HDD SECURITY

| Main | Advanced | Chipset | Security | Boot | Save & Exit |
|---|---|---|---|---|---|

| | |
|---|---|
| HDD Password Description :<br><br>Allows Access to Set, Modify and Clear<br>Hard Disk User Password<br>And Master Password.<br>User Password is mandatory to Enable HDD security. If<br>Master password is installed (optional),<br>It can also be used to unlock the HDD.<br>If the 'Set User Password' option is hidden, do<br>power cycle to enable the option again.<br><br>HDD PASSWORD CONFIGURATION:<br><br>Security Supported : Yes<br>Security Enabled : No<br>Security Locked : No<br>Security Frozen : No<br><br>HDD User Pwd Status : NOT INSTALLED<br><br>Set User Password | **Item help**<br><br>**→←: Select Screen**<br>**↑↓: Select Item**<br>**Enter: Select**<br>**+/- : Change Opt**<br>**F1: General Help**<br>**F2: Previous Values**<br>**F3: Optimized Defaults**<br>**F4: Save & Reset**<br>**ESC: Exit** |

**Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.**

| Field Name | **Set User Password** |
|---|---|
| Help | Set HDD User Password. *** Advisable to Power Cycle System after Setting Hard Disk Passwords ***.Discard or Save changes option in setup does not have any impac on HDD when password is set or removed. If the 'Set HDD User Password' option is hidden out, do power cycle to enable the option again |

### 3.4.2 SECURE BOOT

| Main | Advanced | Chipset | Security | Boot | Save & Exit | |
|---|---|---|---|---|---|---|
| System Mode | | | Setup | | | **Item help** |
| Secure Boot | | | [Disabled]<br>Not Active | | | →←: Select Screen<br>↑↓: Select Item<br>Enter: Select<br>+/- : Change Opt<br>F1: General Help<br>F2: Previous Values<br>F3: Optimized Defaults<br>F4: Save & Reset<br>ESC: Exit |
| Secure Boot Mode | | | [Custom] | | | |
| ► Restore Factory Keys | | | | | | |
| ► Reset To Setup Mode | | | | | | |
| ► Key Management | | | | | | |
| Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc. | | | | | | |

| Field Name | **Secure Boot Enable** |
|---|---|
| Default Value | [Disabled] |
| Possible Value | Enabled<br>Disabled |
| Help | Secure Boot feature is active if Secure Boot is Enabled. Platform Key(PK) is enrolled and the System is in User mode. The mode change requires platform reset |

| Field Name | **Secure Boot Mode** |
|---|---|
| Default Value | [Custom] |
| Possible Value | Standard<br>Custom |
| Help | Secure Boot mode options: Standard or Custom. In Custom mode Secure Boot Policy<br>variables can be configured by a physically present user without full authentication |

| Field Name | **Key Management** |
|---|---|
| Help | Enables expert users to modify Secure Boot Policy variables without full authentication |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

| Field Name | **Restore Factory Keys** |
|---|---|
| Help | Force System to User Mode. Install factory default Secure Boot key databases |

### 3.4.2.1 Key Management

| Main | Advanced | Chipset | Security | Boot | Save & Exit |
|---|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| Vendor Key | | | Valid | **Item help** |
| Factory Key Provision | | | [Disabled] | |
| ► Restore Factory Keys | | | | |
| ► Reset To Setup Mode | | | | |
| ► Export Secure Boot variables | | | | |
| ► Enroll Efi Image | | | | |
| Device Guard ready | | | | |
| ► Remove 'UEFI CA' from DB | | | | →←: Select Screen |
| ► Restore DB defaults | | | | ↑↓: Select Item |
| | | | | Enter: Select |
| Secure Boot variable | Size | Key | Key Source | +/- : Change Opt. |
| ► Platform Key(PK) | 0 | 0 | No Key | F1: General Help |
| ► Key Exchange Key | 0 | 0 | No Key | F2: Previous Values |
| ► Authorized Signatures | 0 | 0 | No Key | F3: Optimized Defaults |
| ► Forbidden Signatures | 0 | 0 | No Key | F4: Save & Reset |
| ► Authorized TimeStamps | 0 | 0 | No Key | ESC: Exit |
| ► OsRecovery Signatures | 0 | 0 | No Key | |

Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.

| Field Name | **Factory Key Provision** |
|---|---|
| Default Value | [Disabled] |
| Possible Value | Enabled<br>Disabled |
| Help | Install factory default Secure Boot keys after the platform reset and while the System i in Setup mode |

| Field Name | **Restore Factory Keys** |
|---|---|
| Help | Force System to User Mode. Install factory default Secure Boot keys |

| | |
|---|---|
| | databases |

| | |
|---|---|
| Field Name | **Reset to Setup Mode** |
| Help | Delete all Secure Boot key databases from NVRAM |

| | |
|---|---|
| Field Name | **Export Secure Boot variables** |
| Help | Copy NVRAM content of Secure Boot variables to files in a root folder on a file |
| | system device |

| | |
|---|---|
| Field Name | **Enroll Efi Image** |
| Help | Allow the image to run in Secure Boot mode. Enroll SHA256 Hash certificate of a PE<br>image into Authorized Signature Database (db) |

| | |
|---|---|
| Field Name | **Remove 'UEFI CA' from DB** |
| Help | Device Guard ready system must not list 'Microsoft UEFI CA' Certificate in<br>Authorized Signature database (db) |

| | |
|---|---|
| Field Name | **Remove DB defaults** |
| Help | Restore DB variable to factory defaults |

| | |
|---|---|
| Field Name | **Platform Key (PK)** |
| Default Value | Size:0, Keys, Key source: No Key |
| Help | Enroll Factory Defaults or load certificates from a file:<br>1. Public Key Certificate:<br>a)EFI_SIGNATURE_LIST<br>b)EFI_CERT_X509 (DER encoded)<br>c)EFI_CERT_RSA2048 (bin)<br>d)EFI_CERT_SHA256,384,512<br>2.Authenticated UEFI Variable<br>3.EFI PE/COFF Image(SHA256)<br>Key Source:<br>Factory,External,Mixed |
| comment | Press Enter when selected to go into the associated Sub-Menu "Key Management". |

| Field Name | **Key Exchange Key** |
|---|---|
| Default Value | Size:0, Keys, Key source: No Key |
| Help | Enroll Factory Defaults or load certificates from a file:<br>1. Public Key Certificate:<br>a)EFI_SIGNATURE_LIST<br>b)EFI_CERT_X509 (DER encoded)<br>c)EFI_CERT_RSA2048 (bin)<br>d)EFI_CERT_SHA256,384,512<br>2.Authenticated UEFI Variable<br>3.EFI PE/COFF Image(SHA256)<br>Key Source:<br>Factory,External,Mixed |
| comment | Press Enter when selected to go into the associated Sub-Menu. |

| Field Name | **Authorized Signature** |
|---|---|
| Default Value | Size:0, Keys, Key source: No Key |
| Help | Enroll Factory Defaults or load certificates from a file:<br>1. Public Key Certificate:<br>a)EFI_SIGNATURE_LIST<br>b)EFI_CERT_X509 (DER encoded) |
| | c)EFI_CERT_RSA2048 (bin)<br>d)EFI_CERT_SHA256,384,5<br>12<br>2.Authenticated UEFI<br>Variable 3.EFI PE/COFF<br>Image(SHA256)<br>Key Source:<br>Factory,External,Mixed |
| comment | Press Enter when selected to go into the associated Sub-Menu. |

| Field Name | **Forbidden Signature** |
|---|---|
| Default Value | Size:0, Keys, Key source: No Key |
| Help | Enroll Factory Defaults or load certificates from a file:<br>1. Public Key Certificate:<br>a)EFI_SIGNATURE_LIST<br>b)EFI_CERT_X509 (DER encoded)<br>c)EFI_CERT_RSA2048 (bin)<br>d)EFI_CERT_SHA256,384,512<br>2.Authenticated UEFI Variable<br>3.EFI PE/COFF Image(SHA256)<br>Key Source:<br>Factory,External,Mixed |
| comment | Press Enter when selected to go into the associated Sub-Menu. |

| Field Name | **Authorized TimeStamps** |
|---|---|
| Default Value | Size:0, Keys, Key source: No Key |
| Help | Enroll Factory Defaults or load certificates from a file:<br>1. Public Key Certificate:<br>a)EFI_SIGNATURE_LIST<br>b)EFI_CERT_X509 (DER encoded)<br>c)EFI_CERT_RSA2048 (bin)<br>d)EFI_CERT_SHA256,384,512<br>2.Authenticated UEFI Variable<br>3.EFI PE/COFF Image(SHA256)<br>Key Source:<br>Factory,External,Mixed |
| comment | Press Enter when selected to go into the associated Sub-Menu. |

| | |
|---|---|
| Field Name | **OsRecovery Signatures** |
| Default Value | Size:0, Keys, Key source: No Key |
| Help | Enroll Factory Defaults or load certificates from a file:<br>1. Public Key Certificate:<br>a)EFI_SIGNATURE_LIST<br>b)EFI_CERT_X509 (DER encoded)<br>c)EFI_CERT_RSA2048 (bin)<br>d)EFI_CERT_SHA256,384,512<br>2.Authenticated UEFI Variable<br>3.EFI PE/COFF Image(SHA256)<br>Key Source:<br>Factory,External,Mixed |
| comment | Press Enter when selected to go into the associated Sub-Menu. |

### 3.4.3 bios update

| Main | Advanced | Chipset | Security | Boot | Save & Exit |
|---|---|---|---|---|---|

| | |
|---|---|
| ► Path for ROM Image<br><br>Notice :<br>ROM Image must in the root folder of storage device.<br>File name must match with current BIOS project. | **Item help**<br><br>**→←: Select Screen**<br>**↑↓: Select Item**<br>**Enter: Select**<br>**+/- : Change Opt**<br>**F1: General Help**<br>**F2: Previous Values**<br>**F3: Optimized Defaults**<br>**F4: Save & Reset**<br>**ESC: Exit** |

**Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.**

| Field Name | **Path for ROM Image** |
|---|---|
| Help | Enter the path to the Secure flash option |

### 3.5 BOOT PAGE

| Main | Advanced | Chipset | Security | Boot | Save & Exit |
|---|---|---|---|---|---|

| | | Item help |
|---|---|---|
| **Boot Configuration** | | |
| Setup Prompt Timeout | 1 | |
| Bootup NumLock State | [On] | |
| **FIXED BOOT ORDER Priorities** | | →←: Select Screen |
| Boot Option #1 | [USB Floppy] | ↑↓: Select Item |
| Boot Option #2 | [CD/DVD] | Enter: Select |
| Boot Option #3 | [USB CD/DVD] | +/- : Change Opt. |
| Boot Option #4 | [Hard Disk] | F1: General Help |
| Boot Option #5 | [USB Key] | F2: Previous Values |
| Boot Option #6 | [USB Hard Disk] | F3: Optimized Defaults |
| Boot Option #7 | [Network] | F4: Save & Reset |
| | | ESC: Exit |
| ▶ USB Floppy Drive BBS Priorities | | |
| ▶ CDROM/DVD Drive BBS Priorities | | |
| ▶ USB CDROM/DVD Drive BBS Priorities | | |
| ▶ Hard Disk Drive BBS Priorities | | |
| ▶ USB Key Drive BBS Priorities | | |
| ▶ USB Hard Disk Drive BBS Priorities | | |
| ▶ USB Lan Drive BBS Priorities | | |
| ▶ Network Drive BBS Priorities | | |

Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.

| Field Name | **Setup Prompt Timeout** |
|---|---|
| Default Value | 1 |
| Possible Value | 1~65535 |
| Help | Number of seconds to wait for setup activation key.<br>65535(0xFFFF) means indefinite waiting. |

| Field Name | **Bootup NumLock State** |
|---|---|
| Default Value | [On] |
| Possible Value | On<br>Off |
| Help | Select the keyboard NumLock state |

| Field Name | **Boot Option #1** |
|---|---|
| Default Value | [USB Floppy] |
| Possible Value | USB Floppy, CD/DVD, USB CD/DVD, Hard Disk, USB Key, USB<br>Hard Disk, Network, Disable |
| Help | Sets the system boot order |

| Field Name | **Boot Option #2** |
|---|---|
| Default Value | [CD/DVD] |
| Possible Value | USB Floppy, CD/DVD, USB CD/DVD, Hard Disk, USB Key, USB<br>Hard Disk, Network, Disable |
| Help | Sets the system boot order |

| Field Name | **Boot Option #3** |
|---|---|
| Default Value | [USB CD/DVD] |
| Possible Value | USB Floppy, CD/DVD, USB CD/DVD, Hard Disk, USB Key, USB<br>Hard Disk, Network, Disable |
| Help | Sets the system boot order |

| Field Name | **Boot Option #4** |
|---|---|
| Default Value | [Hard Disk] |
| Possible Value | USB Floppy, CD/DVD, USB CD/DVD, Hard Disk, USB Key, USB Hard Disk, Network, Disable |
| Help | Sets the system boot order |

| Field Name | **Boot Option #5** |
|---|---|
| Default Value | [USB Key] |
| Possible Value | USB Floppy, CD/DVD, USB CD/DVD, Hard Disk, USB Key, USB<br>Hard Disk, Network, Disable |
| Help | Sets the system boot order |

| Field Name | **Boot Option #6** |
|---|---|
| Default Value | [USB Hard Disk] |
| Possible Value | USB Floppy, CD/DVD, USB CD/DVD, Hard Disk, USB Key, USB<br>Hard Disk, Network, Disable |
| Help | Sets the system boot order |

| Field Name | **Boot Option #7** |
|---|---|
| Default Value | [Network] |
| Possible Value | USB Floppy, CD/DVD, USB CD/DVD, Hard Disk, USB Key, USB<br>Hard Disk, Network, Disable |
| Help | Sets the system boot order |

| Field Name | **USB Floppy Drive BBS Priorities** |
|---|---|
| Help | Specifies the Boot Device Priority sequence from available UEFI USB<br>Floppy |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

| Field Name | **CDROM/DVD Drive BBS Priorities** |
|---|---|
| Help | Specifies the Boot Device Priority sequence from available CDROM/DVD |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

| Field Name | **USB CD/DVD ROM Drive BBS Priorities** |
|---|---|
| Help | Specifies the Boot Device Priority sequence from available UEFI USB |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

| Field Name | **USB Hard Disk Drive BBS Priorities** |
|---|---|
| Help | Specifies the Boot Device Priority sequence from available UEFI USB Hard Disk |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

| Field Name | **USB KEY Drive BBS Priorities** |
|---|---|
| Help | Specifies the Boot Device Priority sequence from available UEFI USB Key Drives. |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

| Field Name | **Hard Disk Drive BBS Priorities** |
|---|---|
| Help | Specifies the Boot Device Priority sequence from available UEFI Hard Disk Drives. |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

| Field Name | **NETWORK Drive BBS Priorities** |
|---|---|
| Help | Specifies the Boot Device Priority sequence from available UEFI NETWORK. |
| Comment | Press Enter when selected to go into the associated Sub-Menu. |

### 3.5.1 (LIST BOOT DEVICE TYPE) DRIVE BBS PRIORITIES

| Main | Advanced | Chipset | Security | Boot | Save & Exit |
|---|---|---|---|---|---|

| | | |
|---|---|---|
| Boot Option #1 | [Boot Device Name 1] | **Item help** |
| Boot Option #2 | [Boot Device Name 2] | |
| | | →←: Select Screen |
| | | ↑↓: Select Item |
| | | Enter: Select |
| | | +/- : Change Opt |
| | | F1: General Help |
| | | F2: Previous Values |
| | | F3: Optimized Defaults |
| | | F4: Save & Reset |
| | | ESC: Exit |

Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.

| Field Name | **Boot Option #1** |
|---|---|
| Default Value | |
| Possible Value | Boot Device Name 1 of this type |
| Help | Sets the system boot order |

| Field Name | **Boot Option #2** |
|---|---|
| Default Value | |
| Possible Value | Boot Device Name 2 of this type |
| Help | Sets the system boot order |

### 3.6 SAVE & EXIT PAGE

| Main | Advanced | Chipset | Security | Boot | Save & Exit | |
|---|---|---|---|---|---|---|
| Save Options | | | | | | **Item help** |
| Discard Changes and Exit | | | | | | |
| Save Changes and Reset | | | | | | |
| Discard Changes and Reset | | | | | | |
| Restore Defaults | | | | | | |
| | | | | | | →←: Select Screen |
| | | | | | | ↑↓: Select Item |
| | | | | | | Enter: Select |
| | | | | | | +/- : Change Opt |
| | | | | | | F1: General Help |
| | | | | | | F2: Previous Values |
| | | | | | | F3: Optimized Defaults |
| | | | | | | F4: Save & Reset |
| | | | | | | ESC: Exit |
| Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc. | | | | | | |

| Field Name | **Discard Changes and Exit** |
|---|---|
| Help | Exit system setup without saving any changes. |

| Field Name | **Save Changes and Reset** |
|---|---|
| Help | Reset the system after saving the changes. |

| Field Name | **Discard Changes and Rest** |
|---|---|
| Help | Reset system setup without saving any changes. |

| Field Name | **Restore Defaults** |
|---|---|
| Help | Restore/Load Default values for all the setup options. |

### 3.7 RECOVERY PAGE (ACTIVE FOR 3.4.3 SECURE FLASH UPDATE ONLY)

| Main | Advanced | Chipset | Security | Boot | Save & Exit | Recovery |
|---|---|---|---|---|---|---|

Please select block you want to update

Reset NVRAM [Disabled]

► Process with flash update

**Item help**

→←: Select Screen
↑↓: Select Item
Enter: Select
+/- : Change Opt
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Reset
ESC: Exit

Version 2.18.1264. Copyright (C) 2017 American Megatrends, Inc.

| Field Name | **Reset NVRAM** |
|---|---|
| Default Value | [Disabled] |
| Possible Value | Enabled<br>Disabled |
| Help | Set this option to reset NVRAM to default values |

| Field Name | **Process with flash update** |
|---|---|
| Help | Select this to start flash update |