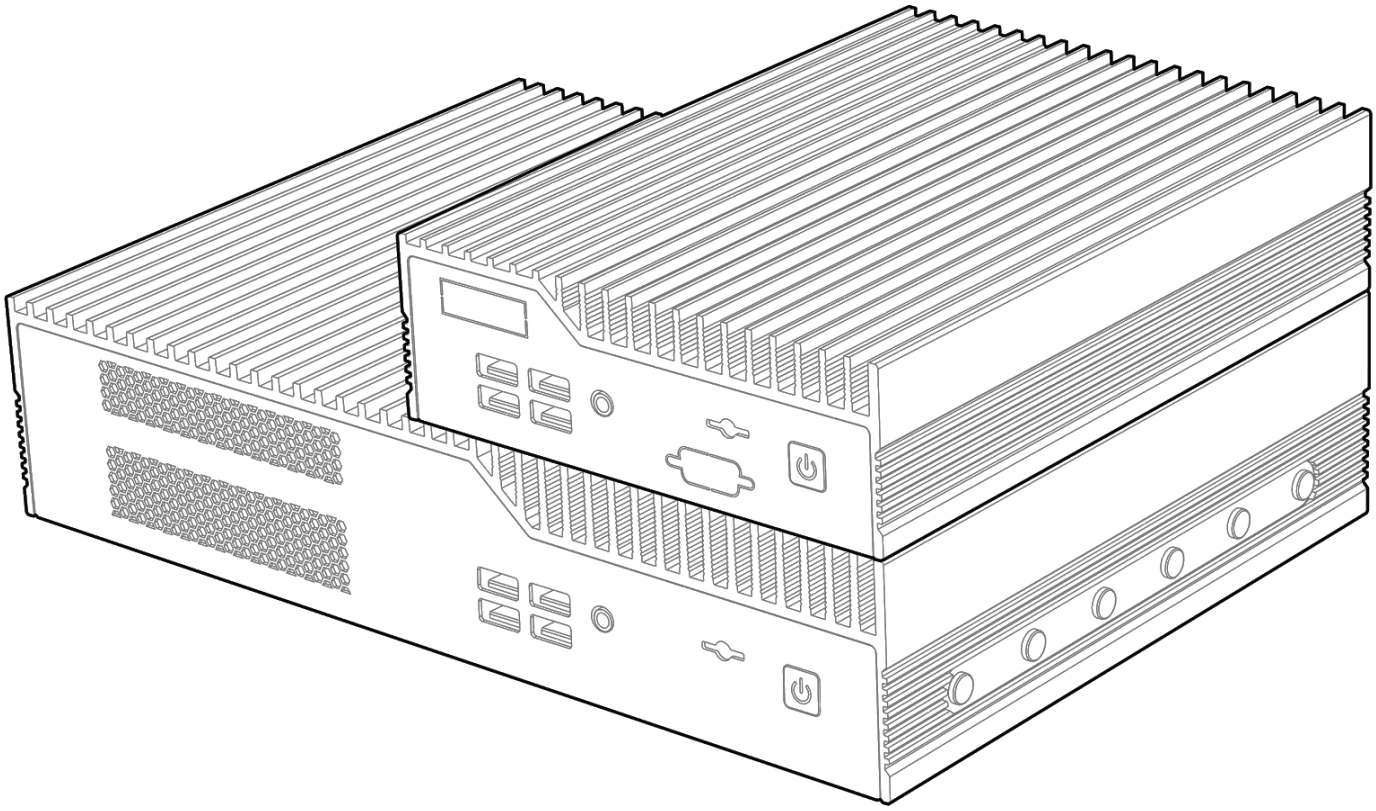
HX500 / HX600 BIOS Manual



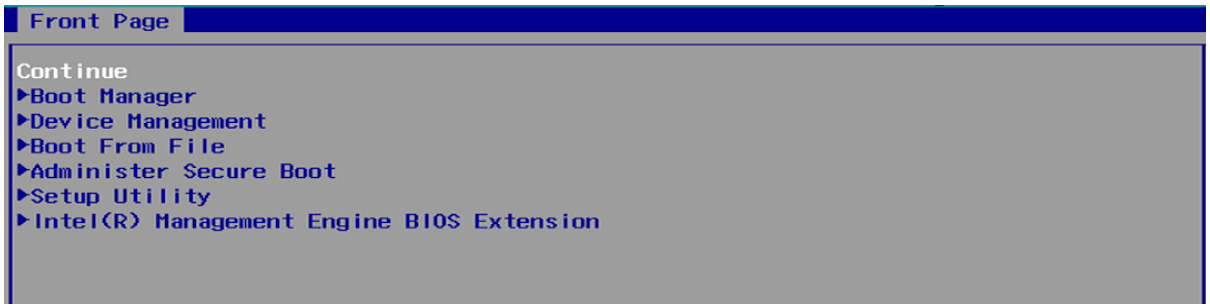
Revision History

Revision History	Date
First release of HX500/HX600 BIOS Manual	07/16/2020
Add link to BIOS Updates support page	12/15/2020

Table of Contents

NOTE: To enter the BIOS on Helix systems, hold the ‘Delete’ key on your keyboard during boot.

1 - Front Page



Boot Manager

Type	Menu
BIOS Page	Front Page
Description	Opens the list of detected bootable devices, allowing you to manually select a device to boot, such as an OS or PXE

Device Management

Type	Menu
BIOS Page	Front Page
Description	Opens the Device Manager menu which includes a configuration menu for Intel Rapid Storage Technology and a Network Device List (if RST and Network Stack are enabled)

Boot From File

Type	Menu
BIOS Page	Front Page
Description	Allows you to boot from a UEFI bootable file

Administer Secure Boot

Type	Menu
BIOS Page	Front Page
Description	Opens the Secure Boot configuration menu

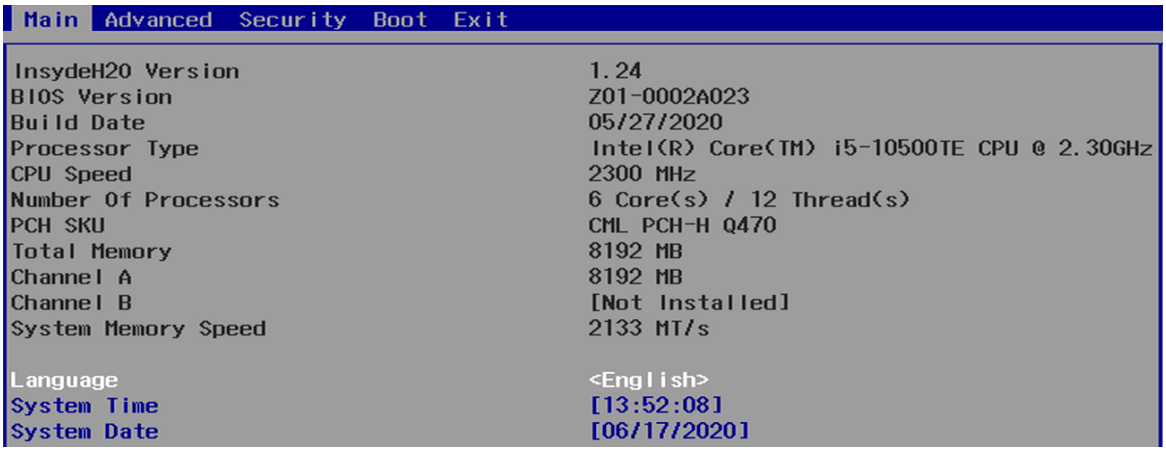
Setup Utility

Type	Menu
BIOS Page	Front Page
Description	Opens the primary BIOS configuration menu referenced in sections 2 through 6 of this manual

Intel(R) Management Engine BIOS Extension

Type	Menu
BIOS Page	Front Page
Description	Opens the Intel Management Engine BIOS Extension (MEBx) configuration interface

2 - Main Page



InsydeH20 Version

Type	Information
BIOS Page	Main Page
Description	Displays current InsydeH20 BIOS Framework version

BIOS Version

Type	Information
BIOS Page	Main Page
Description	Displays current BIOS version

Build Date

Type	Information
BIOS Page	Main Page
Description	Displays the BIOS build date in MM/DD/YYYY

Processor Type

Type	Information
BIOS Page	Main Page
Description	Displays model number of installed CPU

CPU Speed

Type	Information
BIOS Page	Main Page
Description	Displays base frequency of installed CPU

Number of Processors

Type	Information
BIOS Page	Main Page
Description	Displays core and thread count of installed CPU

PCH SKU

Type	Information
BIOS Page	Main Page
Description	Displays model number of PCH

Total Memory

Type	Information
BIOS Page	Main Page
Description	Displays total capacity of all memory installed in system

Channel A

Type	Information
BIOS Page	Main Page
Description	Displays capacity of memory installed in Channel A

Channel B

Type	Information
BIOS Page	Main Page
Description	Displays capacity of memory installed in Channel B

Memory Speed

Type	Information
BIOS Page	Main Page
Description	Displays base frequency of installed memory

Language

Type	Information
BIOS Page	Main Page
Description	Selects the current default language used by the BIOS

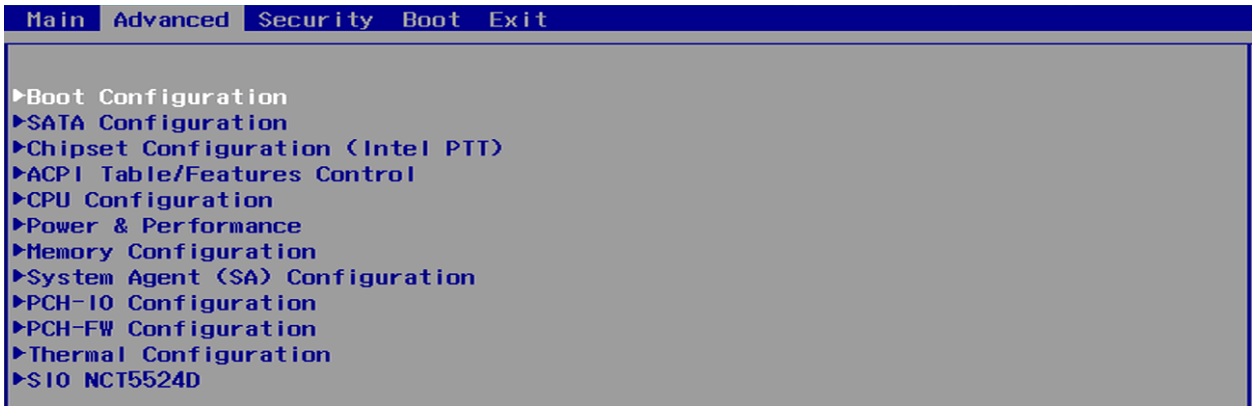
System Time

Type	Information
BIOS Page	Main Page
Description	Displays the time in HH:MM:SS. Valid range is from 0 to 23, 0 to 59, 0 to 59. Use +/- to increase/decrease

System Date

Type	Information
BIOS Page	Main Page
Description	Displays the date in MM:DD:YYYY. Valid range is from 1 to 12, 1 to 31, 2000 to 2099. Use +/- to increase/decrease

3 - Advanced Page

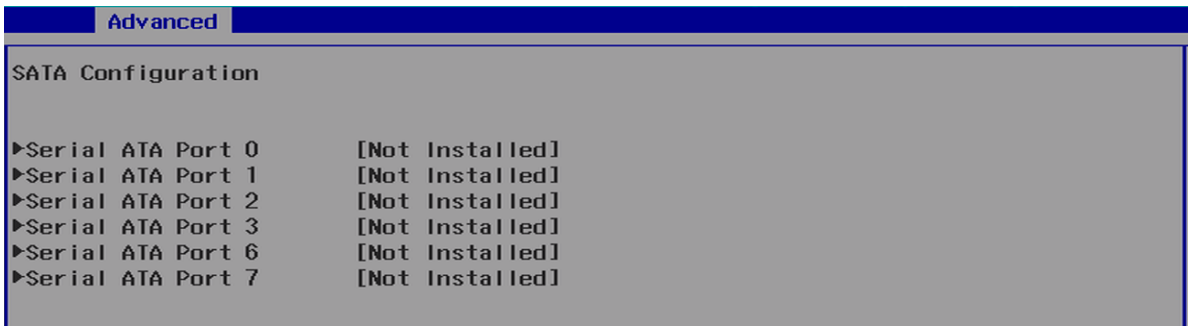


3.1 - Boot Configuration

Numlock

Type	Configurable Setting
BIOS Page	Advanced Page > Boot Configuration
Description	Sets state of Num Lock key when system is booted
Default Value	Off

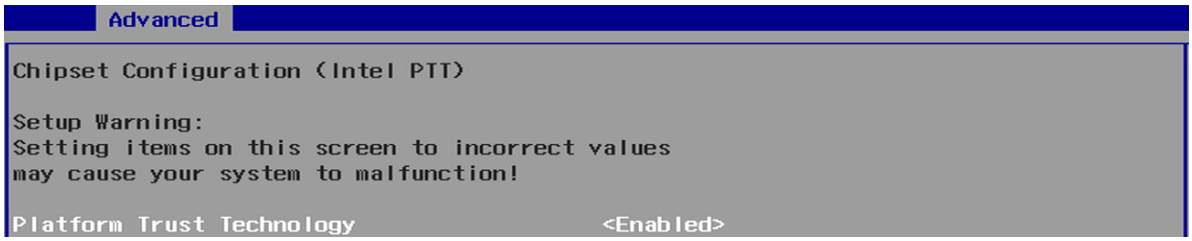
3.2 - SATA Configuration



Serial ATA Port X

Type	Information
BIOS Page	Advanced Page > SATA Configuration
Description	Displays model number of device installed in each SATA Port

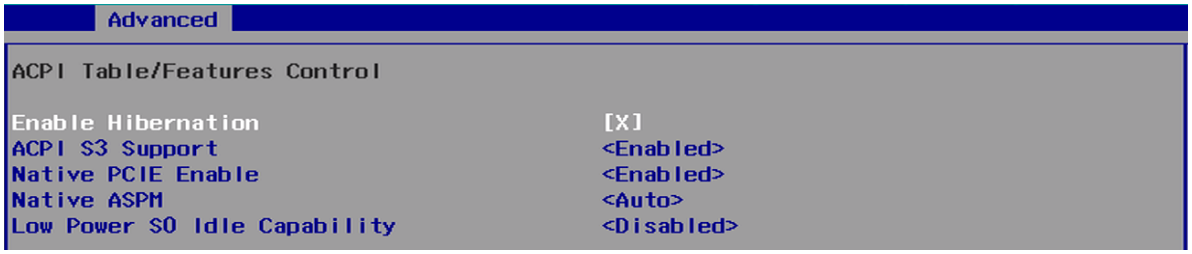
3.3 - Chipset Configuration (Intel PTT)



Platform Trust Technology

Type	Information
BIOS Page	Advanced Page > Chipset Configuration (Intel PTT)
Description	Enables or Disables Intel Platform Trust Technology (PTT).
Default Value	Enabled

3.4 - ACPI Table/Features Control



Enable Hibernation

Type	Configurable Setting
BIOS Page	Advanced Page > ACPI Table/Features Control
Description	Enables or Disables hibernation state (ACPI Sleep State S4) support. This option may not be effective with some OSes
Default Value	[X] (enabled)

ACPI S3 Support

Type	Configurable Setting
BIOS Page	Advanced Page > ACPI Table/Features Control
Description	Enables or Disables ACPI Sleep State S3 support
Default Value	Enabled

Native PCIE Enable

Type	Configurable Setting
BIOS Page	Advanced Page > ACPI Table/Features Control
Description	Enables or Disables Native PCIe, allowing the OS to control PCIe configuration
Default Value	Enabled

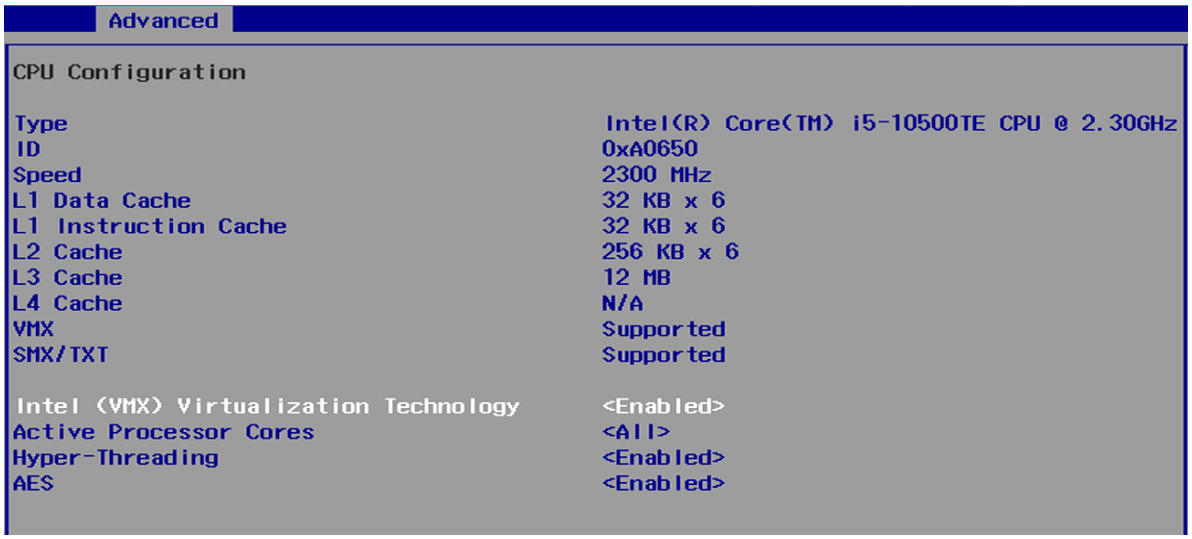
Native ASPM

Type	Configurable Setting
BIOS Page	Advanced Page > ACPI Table/Features Control
Description	Enables or Disables Native Active State Power Management (ASPM)
Possible Values	Auto Enabled - OS Controlled ASPM Disabled - BIOS Controlled ASPM
Default Value	Auto

Low Power S0 Idle Capability

Type	Configurable Setting
BIOS Page	Advanced Page > ACPI Table/Features Control
Description	Enable or Disable ACPI Lower Power S0 Idle Capability (mutually exclusive with Smart Connect). While this is enabled, it also disables 8254 timer for SLP_S0 support.
Default Value	Disabled

3.5 - CPU Configuration



Type

Type	Information
BIOS Page	Advanced Page > CPU Configuration
Description	Displays model number of installed CPU

ID

Type	Information
BIOS Page	Advanced Page > CPU Configuration
Description	Displays ID of installed CPU

Speed

Type	Information
BIOS Page	Advanced Page > CPU Configuration
Description	Displays base frequency of installed CPU

L1 Data Cache

Type	Information
BIOS Page	Advanced Page > CPU Configuration
Description	Displays capacity of L1 data cache

L1 Instruction Cache

Type	Information
BIOS Page	Advanced Page > CPU Configuration
Description	Displays capacity of L1 instruction cache

L2 Data Cache

Type	Information
BIOS Page	Advanced Page > CPU Configuration
Description	Displays capacity of L2 data cache

L3 Data Cache

Type	Information
BIOS Page	Advanced Page > CPU Configuration
Description	Displays capacity of L3 Data Cache

L4 Data Cache

Type	Information
BIOS Page	Advanced Page > CPU Configuration
Description	Displays capacity of L4 Data Cache

VMX

Type	Information
BIOS Page	Advanced Page > CPU Configuration
Description	Displays whether or not Virtual Machine Extensions (VMX) instruction set is supported

SMX/TXT

Type	Information
BIOS Page	Advanced Page > CPU Configuration
Description	Displays whether or not Safer Mode Extensions (SMX) and Trusted Execution Technology (TXT) are supported

Intel (VMX) Virtualization Technology

Type	Configurable Setting
BIOS Page	Advanced Page > CPU Configuration
Description	Enables or Disables Intel Virtual Machine Extensions (VMX). When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology
Default Value	Enabled

Active Processor Cores

Type	Configurable Setting
BIOS Page	Advanced Page > CPU Configuration
Description	Sets number of cores to enable in each processor package

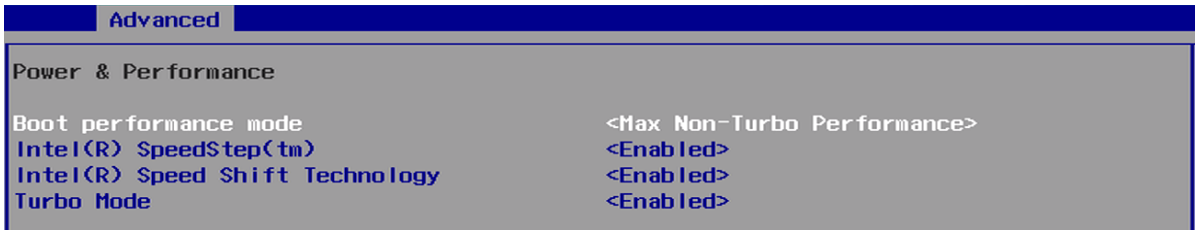
Hyper-Threading

Type	Configurable Setting
BIOS Page	Advanced Page > CPU Configuration
Description	Enables or Disables Hyper-Threading
Default Value	Enabled

AES

Type	Configurable Setting
BIOS Page	Advanced Page > CPU Configuration
Description	Enables or Disables Advanced Encryption Standard (AES) instruction set
Default Value	Enabled

3.6 - Power & Performance



Boot Performance Mode

Type	Configurable Setting
BIOS Page	Advanced Page > Power & Performance
Description	Sets the performance state that the BIOS will set starting from the reset vector
Possible Values	Max Non-Turbo Performance, Max Battery, Turbo Performance
Default Value	Max Non-Turbo Performance

Intel(R) SpeedStep(tm)

Type	Configurable Setting
BIOS Page	Advanced Page > Power & Performance
Description	Enables or Disables support for more than two CPU frequency ranges
Default Value	Enabled

Intel(R) Speed Shift Technology

Type	Configurable Setting
BIOS Page	Advanced Page > Power & Performance
Description	Enables or Disables Intel(R) Speed Shift Technology support. Enabling will expose the CPPC v2 interface to allow for hardware controlled P-states
Default Value	Enabled

Turbo Mode

Type	Configurable Setting
BIOS Page	Advanced Page > Power & Performance
Description	Enables or Disables processor Turbo Mode (requires Intel SpeedStep or Intel Speed Shift to be supported and enabled)
Default Value	Enabled

3.7 - Memory Configuration

HOB Buffer Size

Type	Configurable Setting
BIOS Page	Advanced Page > Memory Configuration
Description	Sets HOB buffer size
Possible Values	Auto, 1B, 1KB, Max (assuming 63KB total HOB size)
Default Value	Auto

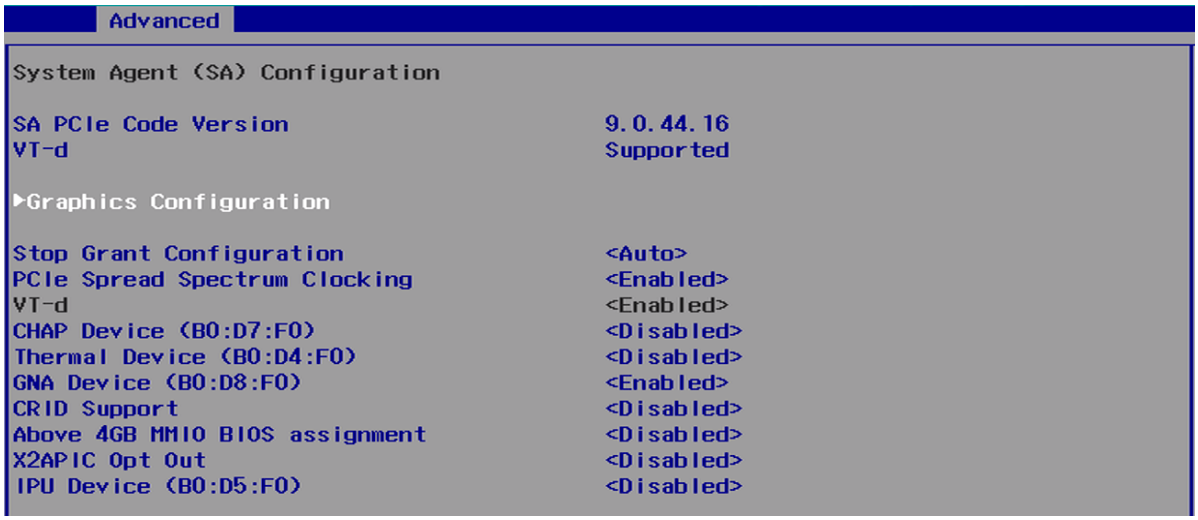
ECC Support

Type	Configurable Setting
BIOS Page	Advanced Page > Memory Configuration
Description	Enables or Disables Error-Correcting Code memory (ECC) support
Default Value	Enabled

Max TOLUD

Type	Configurable Setting
BIOS Page	Advanced Page > Memory Configuration
Description	Sets maximum value of TOLUD. Dynamic assignment would adjust TOLUD automatically based on the largest MMIO length of the installed graphic controller
Possible Values	Dynamic, 1, 1.25, 1.5, 1.75, 2, 2.25, 2.5, 2.75, 3, 3.25, 3.5 (GB)
Default Value	Dynamic

3.8 - System Agent (SA) Configuration



SA PCIe Code Version

Type	Information
BIOS Page	Advanced Page > System Agent (SA) Configuration
Description	Displays SA PCIe Code Version

VT-d

Type	Information
BIOS Page	Advanced Page > System Agent (SA) Configuration
Description	Displays whether or not Virtualization Technology for Directed I/O (VT-d) is supported

Graphics Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > System Agent (SA) Configuration
Description	Opens Graphics Configuration sub-menu (see section 3.8.1 below)

Stop Grant Configuration

Type	Configurable Setting
BIOS Page	Advanced Page > System Agent (SA) Configuration
Description	Sets stop grant configuration to automatic or manual
Possible Values	Auto, Manual
Default Value	Auto

PCIe Spread Spectrum Clocking

Type	Configurable Setting
BIOS Page	Advanced Page > System Agent (SA) Configuration
Description	Enables or Disables PCI Express Spread Spectrum Clocking (SSC) for compliance testing
Default Value	Enabled

VT-d

Type	Configurable Setting
BIOS Page	Advanced Page > System Agent (SA) Configuration
Description	Enables or Disables Virtualization Technology for Directed I/O (VT-d) capability
Default Value	Enabled

CHAP Device (B0:D7:F0)

Type	Configurable Setting
BIOS Page	Advanced Page > System Agent (SA) Configuration
Description	Enables or Disables SA CHAP Device
Default Value	Disabled

Thermal Device (B0:D4:F0)

Type	Configurable Setting
BIOS Page	Advanced Page > System Agent (SA) Configuration
Description	Enables or Disables SA Thermal Device
Default Value	Disabled

GNA Device (B0:D8:F0)

Type	Configurable Setting
BIOS Page	Advanced Page > System Agent (SA) Configuration
Description	Enables or Disables SA GNA Device
Default Value	Disabled

CRID Support

Type	Configurable Setting
BIOS Page	Advanced Page > System Agent (SA) Configuration
Description	Enables or Disables CRID control for Intel Stabled IT Platform Program (SIPP)
Default Value	Disabled

Above 4GB MMIO BIOS assignment

Type	Configurable Setting
BIOS Page	Advanced Page > System Agent (SA) Configuration
Description	Enables or Disables above 4GB MemoryMappedIO (MMIO) BIOS assignment. This is enabled automatically when Aperture Size is set to 2048MB
Default Value	Disabled

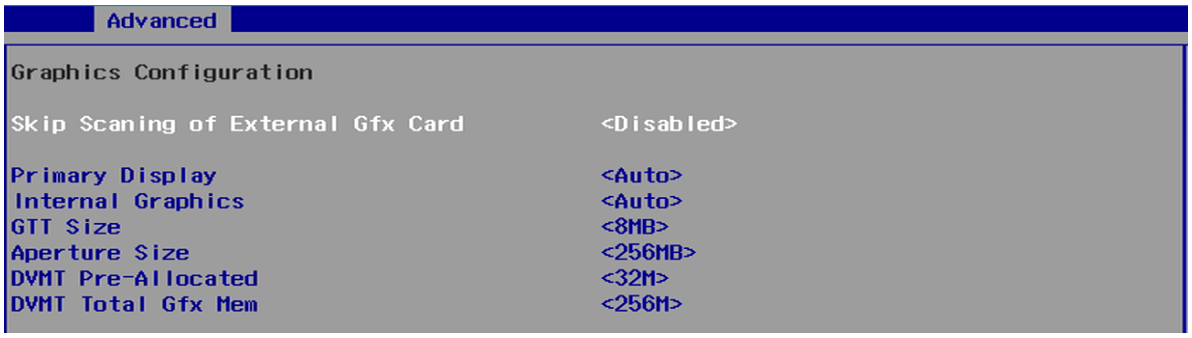
X2APIC Opt Out

Type	Configurable Setting
BIOS Page	Advanced Page > System Agent (SA) Configuration
Description	Enables or Disables X2APIC_OPT_OUT bit
Default Value	Disabled

IPU Device (B0:D5:F0)

Type	Configurable Setting
BIOS Page	Advanced Page > System Agent (SA) Configuration
Description	Enables or Disables SA IPU Device. Default value: Disabled

3.8.1 - Graphics Configuration



Skip Scanning of External Gfx Card

Type	Configurable Setting
BIOS Page	Advanced Page > System Agent (SA) Configuration > Graphics Configuration
Description	Sets whether or not the system will skip scanning for external GPUs on all PEG and PCH PCIe ports on boot
Default Value	Disabled (system will scan for external GPUs on boot)

Primary Display

Type	Configurable Setting
BIOS Page	Advanced Page > System Agent (SA) Configuration > Graphics Configuration
Description	Sets which iGFX/PEG/PCI graphics device should be used for the primary display output. Select SG for Switchable Graphics
Possible Values	Auto, IGFX, PEG, PCI, SG
Default Value	Auto

Internal Graphics

Type	Configurable Setting
BIOS Page	Advanced Page > System Agent (SA) Configuration > Graphics Configuration
Description	Enables or Disables Integrated Graphics (iGFX). Auto mode will enable or disable based on graphics settings above
Possible Values	Auto, Enabled, Disabled
Default Value	Auto

GTT Size

Type	Configurable Setting
BIOS Page	Advanced Page > System Agent (SA) Configuration > Graphics Configuration
Description	Sets size of the Graphics Translation Table (GTT)
Possible Values	2MB, 4MB, 8MB
Default Value	8MB

Aperture Size

Type	Configurable Setting
BIOS Page	Advanced Page > System Agent (SA) Configuration > Graphics Configuration
Description	Sets the Graphics Aperture Size. The Above 4GB MMIO BIOS assignment is automatically enabled when selecting 2048MB aperture. To use this feature, please disable CSM support
Possible Values	128MB, 256MB, 512MB, 1024MB, 2048MB
Default Value	256MB

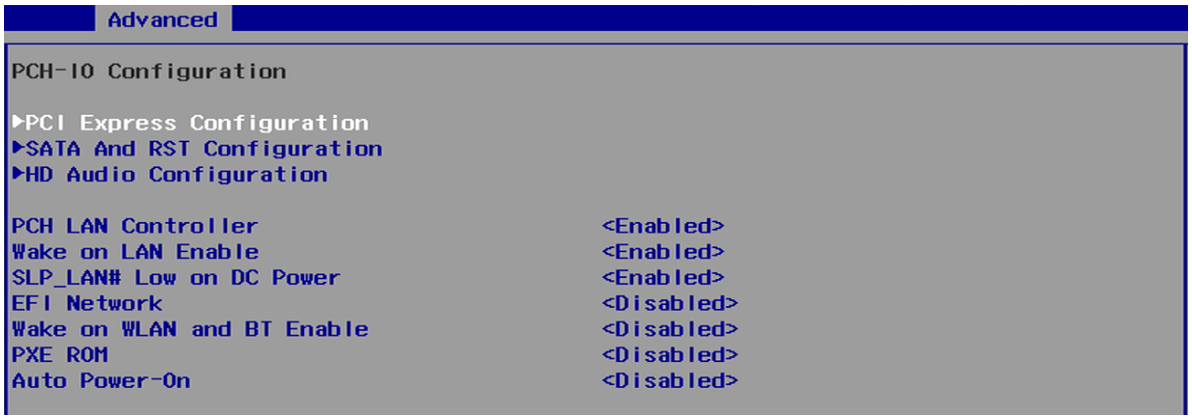
DVMT Pre-Allocated

Type	Configurable Setting
BIOS Page	Advanced Page > System Agent (SA) Configuration > Graphics Configuration
Description	Sets DVMT 5.0 Pre-Allocated (Fixed) graphics memory size used by the Integrated Graphics (iGFX)
Possible Values	0, 64, 4, 8, 12, 16, 20, 24, 28, 32/F7, 36, 40, 44, 48, 52, 56, 60 (M)
Default Value	32M

DVMT Total Gfx Mem

Type	Configurable Setting
BIOS Page	Advanced Page > System Agent (SA) Configuration > Graphics Configuration
Description	Select DVMT 5.0 Total Graphic Memory size used by the Integrated Graphics (iGFX)
Possible Values	256M, 128M
Default Value	256M

3.9 - PCH-IO Configuration



PCI Express Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO Configuration
Description	Opens the PCI Express Configuration sub-menu (see section 3.9.1 below)

SATA and RST Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO Configuration
Description	Opens the SATA Device Options Configuration sub-menu (see section 3.9.2 below)

HD Audio

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO Configuration
Description	Opens the HD Audio Subsystem Configuration sub-menu (see section 3.9.3 below)

PCH LAN Controller

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO Configuration
Description	Enables or Disables UEFI initialization of onboard NICs
Default Value	Enabled

Wake on LAN Enable

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO Configuration
Description	Enables or Disables the ability of onboard NICs to wake the system from non-DeepSx states.
Default Value	Enabled

SLP_LAN# Low on DC Power

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO Configuration
Description	Enables or Disables SLP_LAN# Low on DC Power
Default Value	Enabled

EFI Network

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO Configuration
Description	Enables or Disables EFI Network support for onboard NICs and/or WiFi module
Possible Values	Disabled, Onboard NIC, WiFi, Onboard NIC & WiFi
Default Value	Disabled

Wake on WLAN and BT Enable

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO Configuration
Description	Enables or Disables ability of PCI Express Wireless LAN and Bluetooth to wake the system
Default Value	Disabled

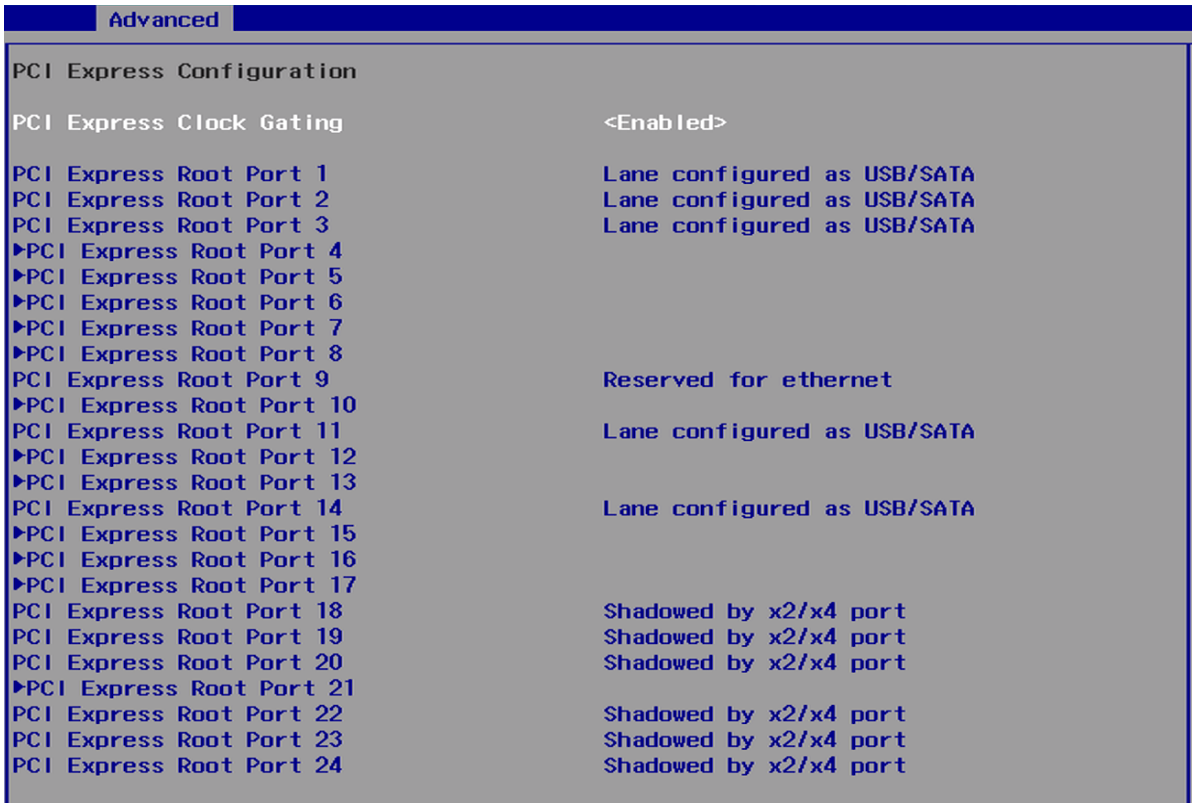
PXE ROM

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO Configuration
Description	Enables or Disables PXE Option ROM execution
Default Value	Disabled

Auto Power-On

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO Configuration
Description	Sets resume state when the system is restored after a mechanical power-off (ACPI G3 state)
Possible Values	Enabled (System will boot directly as soon as power is applied) Disabled (System will remain in power-off state until the power button is pressed)
Default Value	Disabled

3.9.1 - PCI Express Configuration



PCI Express Clock Gating

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO Configuration
Description	Enables or Disables PCI Express Clock Gating
Default Value	Enabled

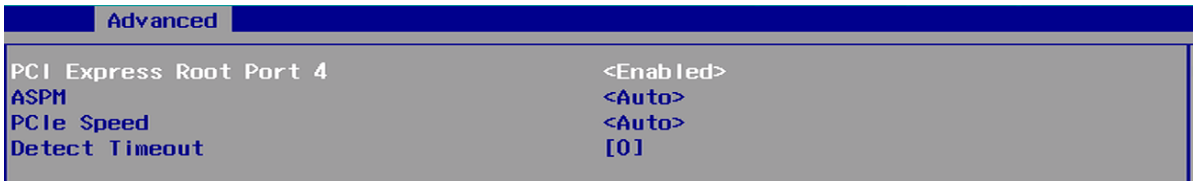
PCI Express Root Port <n>

Type	Information
BIOS Page	Advanced Page > PCH-IO Configuration > PCI Express Configuration
Description	Displays configuration of specified PCI Express Root Port

► PCI Express Root Port <n>

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO Configuration > PCI Express Configuration
Description	Opens the PCI Express Root Port configuration sub-menu for the selected port (see section 3.9.1.1 below)

3.9.1.1 - PCI Express Root Port Settings



PCI Express Root Port

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO Configuration > PCI Express Configuration > PCI Express Root Port Settings
Description	Enables or disables the selected PCI Express Root Port
Default Value	Enabled

ASPM

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO Configuration > PCI Express Configuration > PCI Express Root Port Settings
Description	Sets the PCI Express Active State Power Management mode
Possible Values	Auto, Disabled, L0s, L1, L0sL1
Default Value	Auto

PCIE Speed

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO Configuration > PCI Express Configuration > PCI Express Root Port Settings
Description	Sets the PCIe Speed of the selected port
Possible Values	Auto, Gen1, Gen2, Gen3
Default Value	Auto

Detect Timeout

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO Configuration > PCI Express Configuration > PCI Express Root Port Settings
Description	Sets the number of milliseconds reference code will wait for the link to exit detect state for enabled ports before assuming there is no device and potentially disabling the port
Default Value	0

3.9.2 - SATA and RST Configuration

SATA Controllers

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO Configuration > SATA and RST Configuration
Description	Enables or Disables the SATA controller and all SATA devices
Default Value	Enabled

SATA Mode Selection

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO Configuration > SATA and RST Configuration
Description	Sets the mode of operation of the SATA controller. Setting this to Intel RST Premium With Intel Optane System Acceleration will enabled integrated firmware RAID (see chapter 7 for details) **Note:** Setting this to Intel RST Premium will prevent the Linux kernel from properly interacting with SATA disks
Possible Values	AHCI, Intel RST Premium With Intel Optane System Acceleration
Default Value	AHCI

Serial ATA Port <n>

Type	Information
BIOS Page	Advanced Page > PCH-IO Configuration > SATA and RST Configuration
Description	Displays the model number of the installed device using the specified port, or “Empty” if no device is detected

Software Preserve

Type	Information
BIOS Page	Advanced Page > PCH-IO Configuration > SATA and RST Configuration
Description	Displays whether or not Software Preserve is supported on the specified port

Port <n>

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO Configuration > SATA and RST Configuration
Description	Enables or Disables the specified SATA Port
Default Value	Enabled

Hot Plug

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO Configuration > SATA and RST Configuration
Description	Enables or Disables SATA Hot Plug support for the specified port
Default Value	Disabled

Configured as eSATA

Type	Information
BIOS Page	Advanced Page > PCH-IO Configuration > SATA and RST Configuration
Description	Displays whether or not the specified port is configured as eSATA

External

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO Configuration > SATA and RST Configuration
Description	Sets whether or not the specified port is external
Default Value	Disabled

Spin Up Device

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO Configuration > SATA and RST Configuration
Description	Enables or Disables Staggered Spin Up. If enabled for any port, Staggered Spin Up will be performed and only the drives which have this option enabled will spin up at boot
Default Value	Disabled

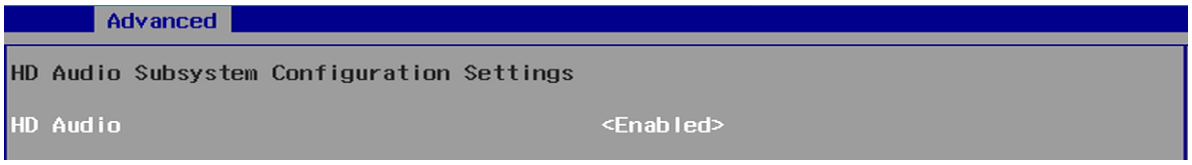
SATA Device Type

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO Configuration > SATA and RST Configuration
Description	Sets the type of disk is connected to the specified SATA port. Certain configuration settings are only applied when this is set to Hard Disk Drive
Possible Values	Hard Disk Drive, Solid State Drive
Default Value	Hard Disk Drive

Topology

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO Configuration > SATA and RST Configuration
Description	Sets the SATA topology type of the installed device
Possible Values	Unknown, ISATA, Direct Connect, Flex, M2
Default Value	Unknown

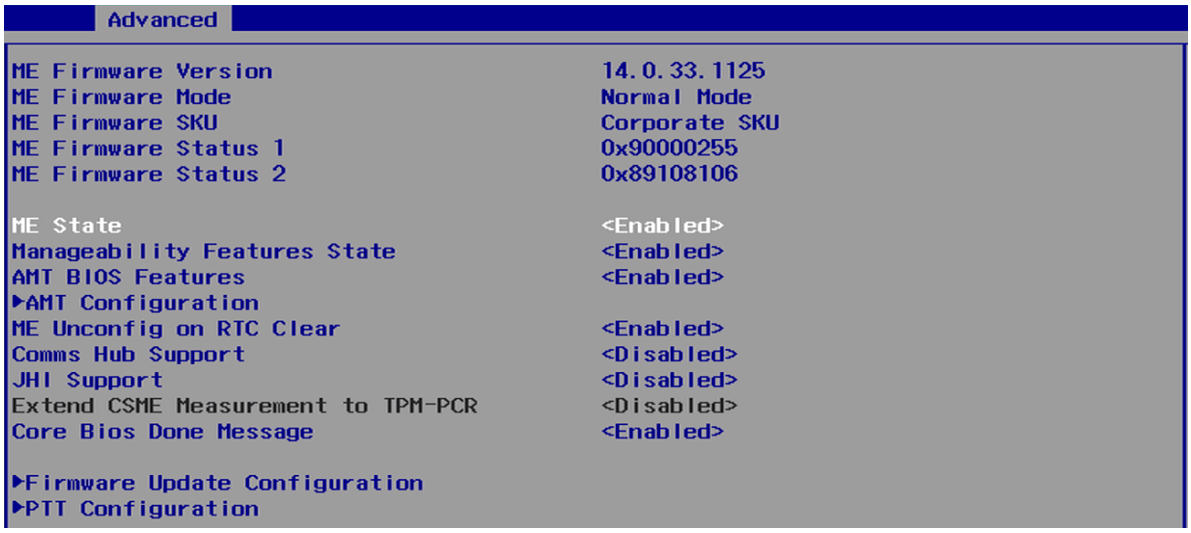
3.9.3 - HD Audio



HD Audio

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO Configuration > HD Audio
Description	Enables or Disables the integrated HD Audio device Default value: Enabled
Possible Values	Disabled (HDA will be unconditionally disabled) Enabled (HDA will be unconditionally enabled)
Default Value	Enabled

3.10 - PCH-FW Configuration



ME Firmware Version

Type	Information
BIOS Page	Advanced Page > PCH-FW Configuration
Description	Displays Management Engine firmware version

ME Firmware Mode

Type	Information
BIOS Page	Advanced Page > PCH-FW Configuration
Description	Displays Management Engine firmware mode

ME Firmware SKU

Type	Information
BIOS Page	Advanced Page > PCH-FW Configuration
Description	Displays Management Engine firmware SKU

ME Firmware Status 1

Type	Information
BIOS Page	Advanced Page > PCH-FW Configuration
Description	Displays Management Engine firmware status 1

ME Firmware Status 2

Type	Information
BIOS Page	Advanced Page > PCH-FW Configuration
Description	Displays Management Engine firmware status 2

ME State

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-FW Configuration
Description	When Disabled ME will be put into ME Temporarily Disabled Mode. Default value: Enabled
Possible Values	Enabled (Management Engine will act normally) Disabled (Management Engine will be put into ME Temporarily Disabled Mode)
Default Value	Enabled

Manageability Features State

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-FW Configuration
Description	Enables or Disables Intel Manageability features **Note:** This option disables/enables Manageability Features support in FW. Platform must be in an unprovisioned state before disabling ME support
Default Value	Enabled

AMT BIOS Features

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-FW Configuration
Description	Enables or Disables Active Management Technology (AMT) BIOS Features. Disabling this prevents the user from accessing the MEBx configuration **Note:** This option does not disable Manageability Features in the firmware
Default Value	Enabled

AMT Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-FW Configuration
Description	Opens the Intel Active Management Technology (AMT) configuration sub-menu (see section 3.10.1 below)

ME Unconfig on RTC Clear

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-FW Configuration
Description	Enables or Disables clearing of Management Engine configuration on CMOS clear
Possible Values	Enabled (ME settings will be cleared on CMOS clear) Disabled (ME settings will be retained on CMOS clear)
Default Values	Enabled

Comms Hub Support

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-FW Configuration
Description	Enables or Disables support for Comms Hub
Default Value	Disabled

JHI Support

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-FW Configuration
Description	Enables or Disables Intel DAL Host Interface Service (JHI)
Default Value	Disabled

Core BIOS Done Message

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-FW Configuration
Description	Enable or Disable sending Core BIOS Done Message to ME
Default Value	Enabled

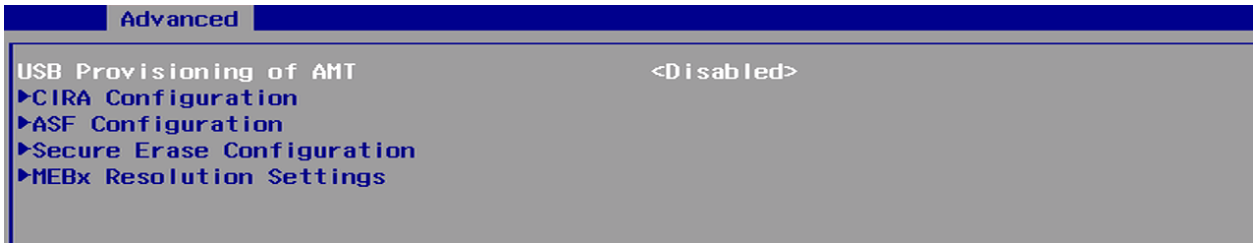
Firmware Update Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-FW Configuration
Description	Opens the Management Engine Firmware Update configuration sub-menu (see section 3.10.2 below)

PTT Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-FW Configuration
Description	Opens the Platform Trust Technology (PTT) configuration sub-menu (see section 3.10.3 below)

3.10.1 - AMT Configuration



ASF Support

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-FW Configuration > AMT Configuration
Description	Enables or Disables Alert Standard Format support
Default Value	Enabled

USB Provisioning of AMT

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-FW Configuration > AMT Configuration
Description	Enables or Disables Active Management Technology (AMT) USB Provisioning
Default Value	Disabled

CIRA Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-FW Configuration > AMT Configuration
Description	Opens the Client Initiated Remote Assistance (CIRA_ configuration sub-menu (see section 3.10.1.1 below)

ASF Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-FW Configuration > AMT Configuration
Description	Opens the Alert Standard Format (ASF) configuration sub-menu (see section 3.10.1.2 below)

Secure Erase Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-FW Configuration > AMT Configuration
Description	Opens the Secure Erase configuration sub-menu (see section 3.10.1.3 below)

MEBx Resolution Settings

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-FW Configuration > AMT Configuration
Description	Opens the Management Engine BIOS Extension (MEBx) configuration sub-menu (see section 3.10.1.4 below)

3.10.1.1 - CIRA Configuration

Activate Remote Assistance Process

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-FW Configuration > AMT Configuration > CIRA Configuration
Description	Enables or Disables the Client Initiated Remote Assistance boot process
Default Value	[ ] (disabled)

CIRA Timeout

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-FW Configuration > AMT Configuration > CIRA Configuration
Description	Sets the timeout for the CIRA remote assistance connection to be established **Note:** This setting is only available if the Activate Remote Assistance Process setting is enabled
Possible Values	0 to 255 (0 for default timeout of 60 seconds, 255 for no timeout)
Default Value	0

3.10.1.2 - ASF Configuration

PET Progress

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-FW Configuration > AMT Configuration > ASF Configuration
Description	Enables or Disables the ability to receive Platform Event Trap (PET) events
Default Value	Enabled

WatchDog

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-FW Configuration > AMT Configuration > ASF Configuration
Description	Enables or Disables the Watchdog Timer
Default Value	Disabled

OS Timer

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-FW Configuration > AMT Configuration > ASF Configuration
Description	Sets the WatchDog Timer duration in seconds so that an OS can interact with it **Note:** This setting is only available if the WatchDog setting is enabled
Default Value	0

BIOS Timer

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-FW Configuration > AMT Configuration > ASF Configuration
Description	Sets the WatchDog Timer duration in seconds at the BIOS level. This timer will reset the system if it fails to POST within the duration **Note:** This setting is only available if the WatchDog setting is enabled
Default Value	0

ASF Sensors Table

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-FW Configuration > AMT Configuration > ASF Configuration
Description	Enables or Disables adding the ASF Sensor Table to the ASF ACPI Table
Default Value	Disabled

3.10.1.3 - Secure Erase Configuration

Secure Erase Mode

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-FW Configuration > AMT Configuration > Secure Erase Configuration
Description	Sets the behavior of the Secure Erase module
Possible Values	- Simulated (performs the Secure Erase process without erasing disks) - Real (performs the Secure Erase process, erasing disks)
Default Value	Simulated

Force Secure Erase

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-FW Configuration > AMT Configuration > Secure Erase Configuration
Description	Enables or Disables forcing the Secure Erase process to occur on next boot
Default Value	Disabled

3.10.1.4 - MEBx Resolution Settings

Non-UI Mode Resolution

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-FW Configuration > AMT Configuration > MEBx Resolution Settings
Description	Sets the resolution for the non-UI text-based MEBx mode
Possible Values	Auto, 80x25, 100x31
Default Value	Auto

UI Mode Resolution

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-FW Configuration > AMT Configuration > MEBx Resolution Settings
Description	Sets the resolution for the UI text-based MEBx mode
Possible Values	Auto, 80x25, 100x31
Default Value	Auto

Graphics Mode Resolution

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-FW Configuration > AMT Configuration > MEBx Resolution Settings
Description	Sets the resolution for the Graphical MEBx mode
Possible Values	Auto, 640x480, 800x600, 1024x768
Default Value	Auto

3.10.2 - Firmware Update Configuration

ME Firmware Re-Flash

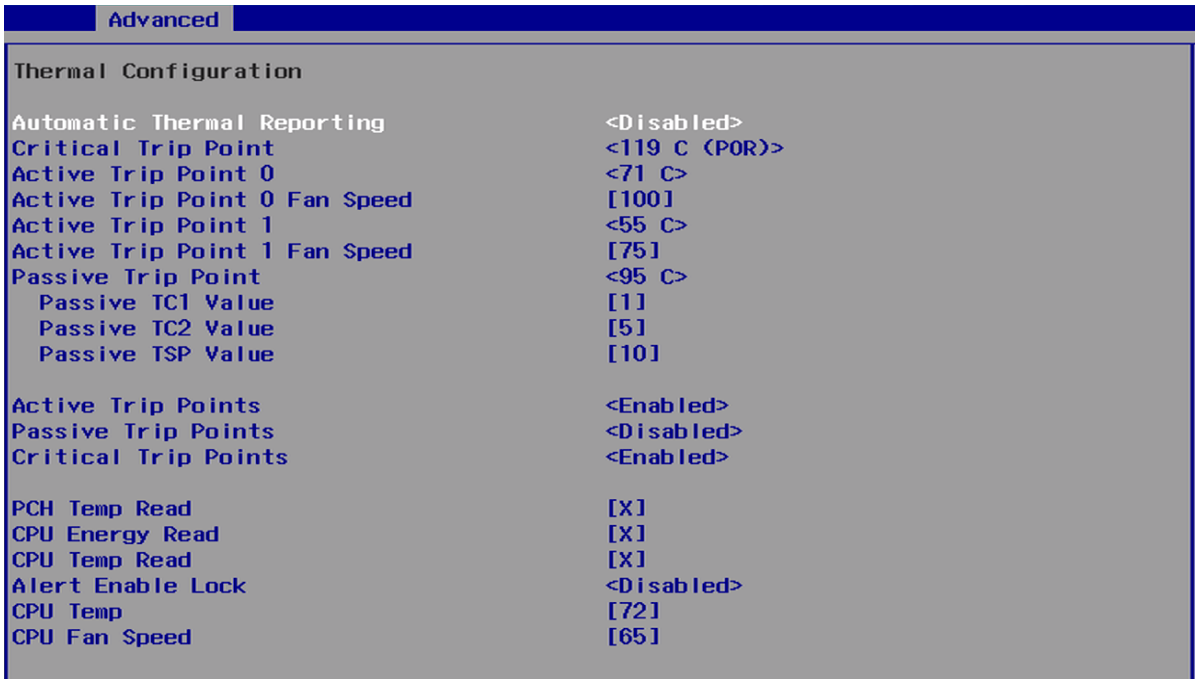
Type	Configurable Setting
BIOS Page	Advanced Page > PCH-FW Configuration > Firmware Update Configuration
Description	Enables or Disables Management Engine Firmware Image Re-Flash function
Default Value	Disabled

3.10.3 - PTT Configuration

PTT Capability / State

Type	Information
BIOS Page	Advanced Page > PCH-FW Configuration > PTT Configuration
Description	Displays Platform Trust Technology (PTT) Capability / Enablement State

3.11 - Thermal Configuration



Automatic Thermal Reporting

Type	Configurable Setting
BIOS Page	Advanced Page > Thermal Configuration
Description	Enables or Disables automatic configuration of _CRT, _PSV and _AC0 based on values recommended in BWG's Thermal Reporting for Thermal Management settings
Possible Values	Enabled (automatic configuration) Disabled (manual configuration)
Default Value	Disabled

Critical Trip Point

Type	Configurable Setting
BIOS Page	Advanced Page > Thermal Configuration
Description	Sets the temperature value of the ACPI Critical Trip Point (the point at which the system will shut off.) **Note:** 119C is the Plan Of Record (POR) for all Intel processors.
Possible Values	15, 23, 31, 39, 47, 55, 63, 71, 79, 87, 95, 100, 103, 111, 119, 127 (C)
Default Value	119 C (POR)

Active Trip Point 0

Type	Configurable Setting
BIOS Page	Advanced Page > Thermal Configuration
Description	Sets the temperature value of the ACPI Active Trip Point 0 (the point at which the OS will set the processor fan to Active Trip Point 0 Fan Speed)
Possible Values	15, 23, 31, 39, 47, 55, 63, 71, 79, 87, 95, 100, 111, 127 (C)
Default Value	71 C

Active Trip Point 0 Fan Speed

Type	Configurable Setting
BIOS Page	Advanced Page > Thermal Configuration
Description	Sets Active Trip Point 0 Fan Speed percentage (the percentage of maximum speed at which the fan will run when Active Trip Point 0 is crossed)
Possible Values	0 to 100
Default Value	100

Active Trip Point 1

Type	Configurable Setting
BIOS Page	Advanced Page > Thermal Configuration
Description	Sets the temperature value of the ACPI Active Trip Point 1 (the point at which the OS will set the processor fan to Active Trip Point 1 Fan Speed)
Possible Values	15, 23, 31, 39, 47, 55, 63, 71, 79, 87, 95, 100, 111, 127 (C)
Default Value	55 C

Active Trip Point 1 Fan Speed

Type	Configurable Setting
BIOS Page	Advanced Page > Thermal Configuration
Description	Sets Active Trip Point 1 Fan Speed percentage (the percentage of maximum speed at which the fan will run when Active Trip Point 1 is crossed)
Possible Values	0 to 100
Default Value	75

Passive Trip Point

Type	Configurable Setting
BIOS Page	Advanced Page > Thermal Configuration
Description	Sets the temperature value of the ACPI Passive Trip Point (the point in which the OS will begin throttling the processor frequency)
Possible Values	15, 23, 31, 39, 47, 55, 63, 71, 79, 87, 100, 103, 111, 119 (POR), 127 (C)
Default Value	95 C

Passive TC1 Value

Type	Configurable Setting
BIOS Page	Advanced Page > Thermal Configuration
Description	Sets the TC1 value for the ACPI Passive Cooling Formula
Possible Values	1 to 16
Default Value	1

Passive TC2 Value

Type	Configurable Setting
BIOS Page	Advanced Page > Thermal Configuration
Description	Sets the TC2 value for the ACPI Passive Cooling Formula
Possible Values	1 to 16
Default Value	5

Passive TSP Value

Type	Configurable Setting
BIOS Page	Advanced Page > Thermal Configuration
Description	Sets the TSP value for the ACPI Passive Cooling Formula. This value represents how often (in tenths of a second) the OS will read the temperature when passive cooling is enabled
Possible Values	2 to 32
Default Value	10

Active Trip Points

Type	Configurable Setting
BIOS Page	Advanced Page > Thermal Configuration
Description	Enables or Disables Active Trip Points
Default Value	Enabled

Passive Trip Points

Type	Configurable Setting
BIOS Page	Advanced Page > Thermal Configuration
Description	Enables or Disables Passive Trip Points
Default Value	Disabled

Critical Trip Points

Type	Configurable Setting
BIOS Page	Advanced Page > Thermal Configuration
Description	Enables or Disables Critical Trip Points
Default Value	Enabled

Active Trip Points

Type	Configurable Setting
BIOS Page	Advanced Page > Thermal Configuration
Description	Enables or Disables Active Trip Points
Default Value	Enabled

PCH Temp Read

Type	Configurable Setting
BIOS Page	Advanced Page > Thermal Configuration
Description	Enables or Disables reading of PCH temperature
Default Value	[X] (enabled)

CPU Energy Read

Type	Configurable Setting
BIOS Page	Advanced Page > Thermal Configuration
Description	Enables or Disables reading of CPU power draw
Default Value	[X] (enabled)

CPU Temp Read

Type	Configurable Setting
BIOS Page	Advanced Page > Thermal Configuration
Description	Enables or Disables reading of CPU temperatures
Default Value	[X] (enabled)

Alert Enable Lock

Type	Configurable Setting
BIOS Page	Advanced Page > Thermal Configuration
Description	Enables or Disables locking of all Alert Enable settings
Default Value	Disabled

CPU Temp

Type	Configurable Setting
BIOS Page	Advanced Page > Thermal Configuration
Description	Sets the Fail Safe temperature that the embedded controller will use if the OS is hung
Default Value	75

CPU Fan Speed

Type	Configurable Setting
BIOS Page	Advanced Page > Thermal Configuration
Description	Sets the fan speed that the embedded controller will use if the OS is hung
Possible Values	0-100%
Default Value	65%

3.12 - SIO NCT5524D

UART Port 1 Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > SIO NCT5524D Chip
Description	Opens the UART Port 1 (COM1) configuration sub-menu (see section 3.12.1 below)

UART Port 2 Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > SIO NCT5524D Chip
Description	Opens the UART Port 2 (COM2) configuration sub-menu (see section 3.12.1 below)

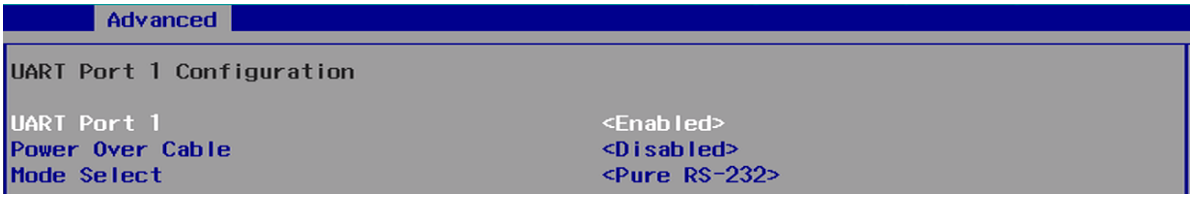
Fan Control

Type	Sub-Menu
BIOS Page	Advanced Page > SIO NCT5524D Chip
Description	Opens the Fan Control configuration sub-menu (see section 3.12.2 below)

Hardware Monitor

Type	Sub-Menu
BIOS Page	Advanced Page > SIO NCT5524D Chip
Description	Opens the Hardware Monitor sub-menu to display hardware monitoring values (see section 3.12.6 below)

3.12.1 - UART Port 1/2 Configuration



UART Port <n>

Type	Configurable Setting
BIOS Page	Advanced Page > SIO NCT5524D Chip > UART Port X Configuration
Description	Enables or Disables selected COM port
Default Value	Enabled

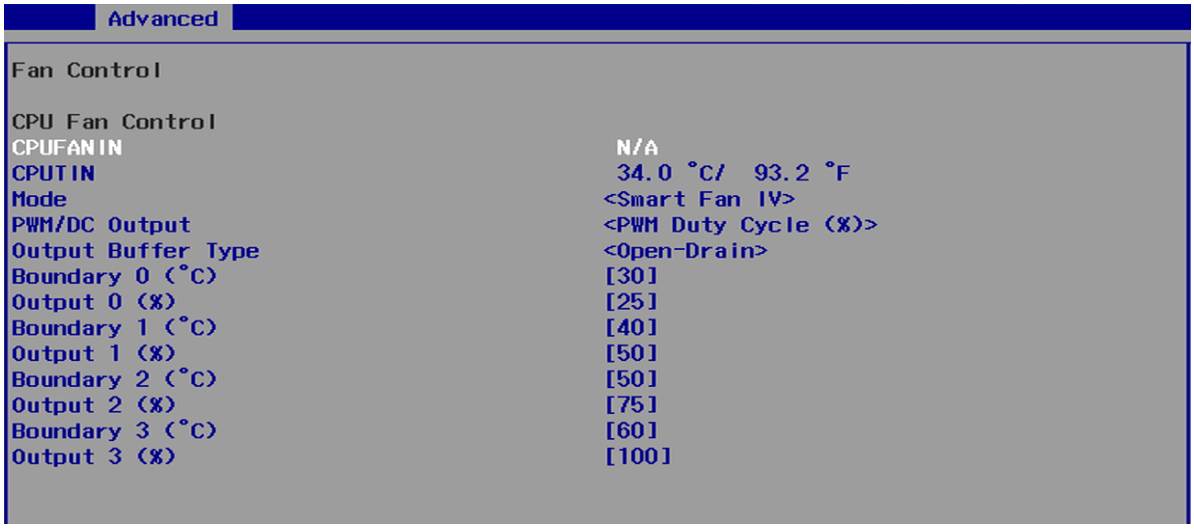
Power Over Cable

Type	Configurable Setting
BIOS Page	Advanced Page > SIO NCT5524D Chip > UART Port X Configuration
Description	Enables or Disables DC power on pin 9 of selected COM port

Mode Select

Type	Configurable Setting
BIOS Page	Advanced Page > SIO NCT5524D Chip > UART Port X Configuration
Description	Sets the communication protocol of the selected COM port
Possible Values	- Pure RS-232 - RS-422 Full Duplex - RS-485 Half Duplex (TX ENABLE Low Active) - RS-422 Full Duplex (with termination resistor and bias resistor) - Pure RS-232 (co-exists with RS485) - RS-485 Half Duplex (with termination resistor and bias resistor) - Low Power Shutdown* *This option puts the transceiver into a low-power mode, deactivating the serial communications to minimize power draw. When selected, the serial ports will not be usable
Default Value	Pure RS-232

3.12.2 - Fan Control



CPUFANIN

Type	Information
BIOS Page	Advanced Page > SIO NCT5524D > Fan Control
Description	Displays current CPU Fan RPM

CPUTIN

Type	Information
BIOS Page	Advanced Page > SIO NCT5524D > Fan Control
Description	Displays current CPU package temperature

Mode

Type	Configurable Setting
BIOS Page	Advanced Page > SIO NCT5524D > Fan Control
Description	Sets fan control mode. Certain modes will add or remove settings that only pertain to that mode; see sections 3.12.2.1 through 3.12.2.3 for mode-specific configuration options
Possible Values	Manual, Thermal Cruise, Speed Cruise, Smart Fan IV
Default Value	Smart Fan IV

PWM/DC Output

Type	Configurable Setting
BIOS Page	Advanced Page > SIO NCT5524D > Fan Control
Description	Sets the type of fan control signal
Possible Values	PWM Duty Cycle (%), DC Voltage (%)
Default Value	PWM Duty Cycle (%)

Output Buffer Type

Type	Configurable Setting
BIOS Page	Advanced Page > SIO NCT5524D > Fan Control
Description	Sets the characteristics of the output buffer **Note:** This setting is only available if the PWM/DC Output option is set to PWM Duty Cycle (%)
Possible Values	Open-Drain, Push-Pull
Default Value	Open-Drain

PWM Duty Cycle (%)

Type	Configurable Setting
BIOS Page	Advanced Page > SIO NCT5524D > Fan Control
Description	Sets the duty cycle percentage for the fan control PWM signal **Note:** This setting is only available if the PWM/DC Output option is set to PWM Duty Cycle (%)
Possible Values	0 to 100
Default Value	50

PWM Duty Cycle (%)

Type	Configurable Setting
BIOS Page	Advanced Page > SIO NCT5524D > Fan Control (with Mode option set to Manual)
Description	Sets the DC voltage percentage for the fan control signal **Note:** This setting is only available if the Mode option is set to Manual and the PWM/DC Output option is set to DC Voltage (%)
Possible Values	0 to 100
Default Value	50

3.12.2.1 - Fan Control (Thermal Cruise Mode)

The following settings are only available if the Mode option above is set to Thermal Cruise.

Target Temperature (°C)

Type	Configurable Setting
BIOS Page	Advanced Page > SIO NCT5524D > Fan Control (with Mode option set to Thermal Cruise)
Description	Sets the target CPU temperature in degrees Celsius that the fan control will adjust to maintain
Default Value	0

Tolerance (°C)

Type	Configurable Setting
BIOS Page	Advanced Page > SIO NCT5524D > Fan Control (with Mode option set to Thermal Cruise)
Description	Sets the temperature tolerance in degrees Celsius for the Target Temperature set above
Default Value	0

3.12.2.2 - Fan Control (Speed Cruise Mode)

Target Fan Speed

Type	Configurable Setting
BIOS Page	Advanced Page > SIO NCT5524D > Fan Control (with Mode option set to Speed Cruise)
Description	Sets the target fan speed that the fan control will adjust to maintain
Default Value	0

Tolerance

Type	Configurable Setting
BIOS Page	Advanced Page > SIO NCT5524D > Fan Control (with Mode option set to Thermal Cruise)
Description	Sets the tolerance for the target fan speed set above
Default Value	0

3.12.2.3 - Fan Control (Smart Fan IV Mode)

Boundary 0 (°C)

Type	Configurable Setting
BIOS Page	Advanced Page > SIO NCT5524D Chip > Fan Control (with Mode option set to Smart Fan IV)
Description	Sets the temperature at which the fan speed will be set to the value specified in the Output 0 option
Default Value	30

Output 0 (%)

Type	Configurable Setting
BIOS Page	Advanced Page > SIO NCT5524D Chip > Fan Control (with Mode option set to Smart Fan IV)
Description	Sets the fan speed percentage that will be used when the temperature hits the threshold specified in the Boundary 0 option
Possible Values	0 to 100
Default Value	25

Boundary 1 (°C)

Type	Configurable Setting
BIOS Page	Advanced Page > SIO NCT5524D Chip > Fan Control (with Mode option set to Smart Fan IV)
Description	Sets the temperature in degrees Celsius at which the fan speed will be set to the value specified in the Output 1 option
Default Value	40

Output 1 (%)

Type	Configurable Setting
BIOS Page	Advanced Page > SIO NCT5524D Chip > Fan Control (with Mode option set to Smart Fan IV)
Description	Sets the fan speed percentage that will be used when the temperature hits the threshold specified in the Boundary 1 option
Possible Values	0 to 100
Default Value	50

Boundary 2 (°C)

Type	Configurable Setting
BIOS Page	Advanced Page > SIO NCT5524D Chip > Fan Control (with Mode option set to Smart Fan IV)
Description	Sets the temperature in degrees Celsius at which the fan speed will be set to the value specified in the Output 2 option
Default Value	50

Output 2 (%)

Type	Configurable Setting
BIOS Page	Advanced Page > SIO NCT5524D Chip > Fan Control (with Mode option set to Smart Fan IV)
Description	Sets the fan speed percentage that will be used when the temperature hits the threshold specified in the Boundary 2 option
Possible Values	0 to 100
Default Value	75

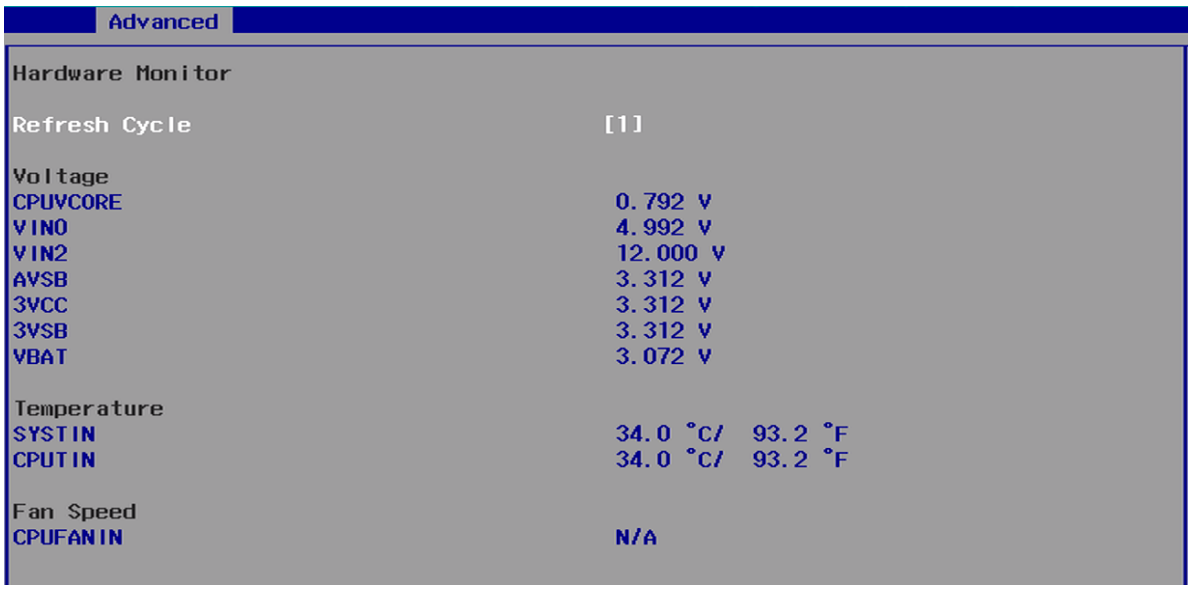
Boundary 3 (°C)

Type	Configurable Setting
BIOS Page	Advanced Page > SIO NCT5524D Chip > Fan Control (with Mode option set to Smart Fan IV)
Description	Sets the temperature in degrees Celsius at which the fan speed will be set to the value specified in the Output 3 option
Default Value	60

Output 3 (%)

Type	Configurable Setting
BIOS Page	Advanced Page > SIO NCT5524D Chip > Fan Control (with Mode option set to Smart Fan IV)
Description	Sets the fan speed percentage that will be used when the temperature hits the threshold specified in the Boundary 3 option
Possible Values	0 to 100
Default Value	100

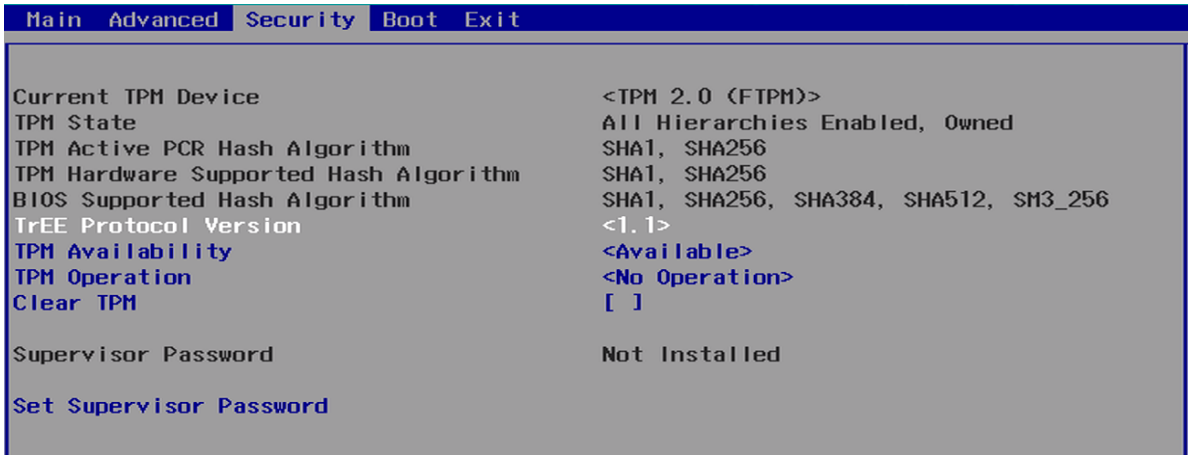
3.12.3 - Hardware Monitor



Refresh Cycle

Type	Configurable Setting
BIOS Page	Advanced Page > SIO NCT5524D Chip > Hardware Monitor
Description	Sets the interval in seconds at which the monitor updates values
Possible Values	0 to 15 (setting to 0 stops the monitor from updating values)
Default Value	1

4 - Security Page



Current TPM Device

Type	Information
BIOS Page	Security Page
Description	Displays current TPM device

TPM State

Type	Information
BIOS Page	Security Page
Description	Displays current TPM state

TPM Active PCR Hash Algorithm

Type	Information
BIOS Page	Security Page
Description	Displays active PCR hash algorithm

TPM Hardware Supported Hash Algorithm

Type	Information
BIOS Page	Security Page
Description	Displays hardware supported hash algorithm

BIOS Supported Hash Algorithm

Type	Information
BIOS Page	Security Page
Description	Displays BIOS supported hash algorithm

TrEE Protocol Version

Type	Configurable Setting
BIOS Page	Security Page
Description	Sets the TrEE Protocol Version: 1.0 or 1.1. Possible values: 1.1, 1.0. Default value: 1.1
Possible Values	1.1, 1.0
Default Value	1.1

TPM Availability

Type	Configurable Setting
BIOS Page	Security Page
Description	Enables or Disables the TPM hardware
Possible Values	Available (enabled), Hidden (disabled)
Default Value	Available

TPM Operation

Type	Configurable Setting
BIOS Page	Security Page
Description	Sets the TPM2 operation state
Possible Values	- No Operation - Enable - SetPCRBanks(Algorithm) - LogAllDigests - SetPPRequiredForClear_True - SetPPRequiredForClear_False - SetPPRequiredForTurnOn_False - SetPPRequiredForTurnOn_True - SetPPRequiredForTurnOff_False - SetPPRequiredForTurnOff_True - SetPPRequiredForChangePCRs_False - SetPPRequriedForChangePCRs_True - SetPPRequiredForChangeEPS_False - SetPPRequiredForChangeEPS_True - ChangeEPS
Default Value	No Operation

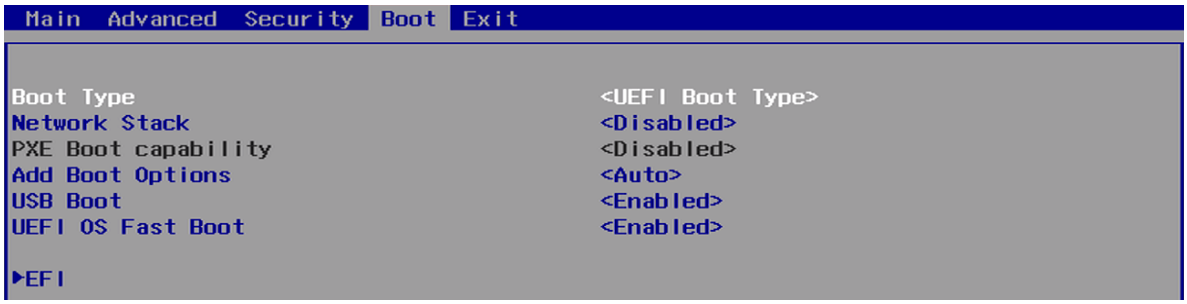
Clear TPM

Type	Configurable Setting
BIOS Page	Security Page
Description	Enables or Disables clearing TPM user data such as passwords, certificates, and keys
Default Value	[ ] (disabled)

Set Supervisor Password

Type	Configurable Setting
BIOS Page	Security Page
Description	Sets or Changes the supervisor password **Note:** The password must be more than one character in length

5 - Boot Page



Boot Type

Type	Configurable Setting
BIOS Page	Boot Page
Description	Sets the boot mode
Possible Values	UEFI Boot Type, Legacy Boot Type, Dual Boot Type
Default Value	UEFI Boot Type

Network Stack

Type	Configurable Setting
BIOS Page	Boot Page
Description	Enables or Disables the onboard NICs before UEFI handoff Default value: Disabled
Default Value	Disabled

PXE Boot Capability

Type	Configurable Setting
BIOS Page	Boot Page
Description	Sets the PXE Boot mode **Note:** This setting is unavailable unless Network Stack is Enabled
Possible Values	- Disabled - UEFI: IPv4 - UEFI: IPv6 - UEFI: IPv4/IPv6
Default Value	Disabled

Add Boot Options

Type	Configurable Setting
BIOS Page	Boot Page
Description	Sets which device in the boot order list the system will attempt to boot first and the direction it will move through the list (see section 5.1 below)
Possible Values	- Auto (boot order is not configurable, uses the system default) - First (system moves through the boot order list top to bottom) - Last (system moves through the boot order list bottom to top)
Default Value	Auto

USB Boot

Type	Configurable Setting
BIOS Page	Boot Page
Description	Enables or Disables booting from USB devices
Default Value	Enabled

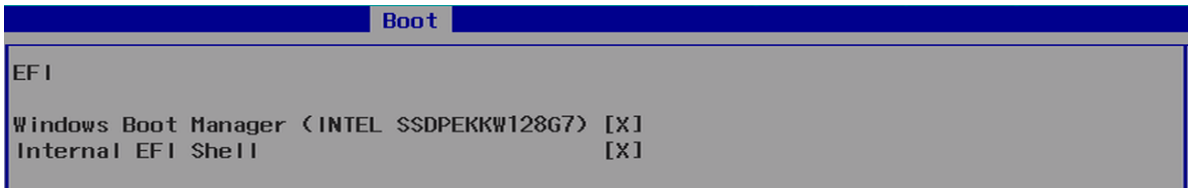
UEFI OS Fast Boot

Type	Configurable Setting
BIOS Page	Boot Page
Description	Enables or Disables Fast Boot mode. When enabled, the BIOS will not initialize the keyboard during boot or watch for the BIOS menu keypress
Default Value	Disabled

EFI

Type	Sub-Menu
BIOS Page	Boot Page
Description	Opens the EFI Boot Order sub-menu (see section 5.1 below)

5.1 - EFI



Note: The EFI boot order configuration in this menu can only be changed if the Add Boot Options option above is set to First or Last.

In this menu, you set which devices the system can boot to, as well as change the order in which it attempts to boot. Highlight a boot device and press Enter to enable or disable booting to it. Use the F5 and F6 keys to move the boot device up and down the list.

6 - Exit Page

Exit Saving Changes

Type	Exit Mode
BIOS Page	Exit Page
Description	Saves your changes and exits the BIOS setup menu

Save Change Without Exit

Type	Exit Mode
BIOS Page	Exit Page
Description	Saves your changes, but does not exit the BIOS setup menu

Exit Discarding Changes

Type	Selectable
BIOS Page	Exit Page
Description	Exits the BIOS setup menu without saving your changes

Load Optimal Defaults

Type	Selectable
BIOS Page	Exit Page
Description	Loads the firmware's optimal default settings

Load Custom Defaults

Type	Selectable
BIOS Page	Exit Page
Description	Loads user-specified set of default settings

Save Custom Defaults

Type	Selectable
BIOS Page	Exit Page
Description	Saves current settings as user-specified set

Discard Changes

Type	Selectable
BIOS Page	Exit Page
Description	Discards all changes, but does not exit the BIOS setup menu

7 - RAID Configuration

7.1 - RAID Overview

RAID (Redundant Array of Independent Disks) is a technology used to stitch multiple storage drives together into a single volume for a variety of purposes. The Intel Q470 chipset on the Helix platform features Intel Rapid Storage Technology (RST), an integrated firmware-level RAID utility for SATA disks. Intel RST on Comet Lake chipsets is only supported in Windows; Linux users will need to use a dedicated hardware RAID solution or a software-level RAID utility such as mdadm.

Because the RAID volumes are maintained at the firmware level, the disks in an array do not need to match perfectly. However, the timing parameters of all disks in a certain array, such as write speed, will be limited by the chipset to the lowest value among those disks.

On the Helix platform, the M.2 B-Key, M.2 M-Key, and both cabled SATA connectors can be configured in RAID arrays.

Different types of RAID arrays are referred to as “levels”. Intel RST on the Helix platform supports four RAID levels:

RAID 0 (Striped): In a RAID 0 array, data written to the volume is split between two or more disks. Each disk’s storage space is divided into blocks, the size of which can be set by the user. When writing data to the volume, the SATA controller will rotate block-by-block between the disks. This methodology can provide noticeable improvements to read and write speeds; however, if one disk in a RAID 0 array fails, the data on the entire volume will be lost.

RAID 1 (Mirrored): In a RAID 1 array, the SATA controller mirrors all data between two or more disks. The primary benefit of this methodology is that if a drive in the array is disconnected or fails altogether, the volume will continue to function as normal. If an OS is installed on the volume, it will not be interrupted by a failing drive. A drive can then be reconnected or replaced, at which time the SATA controller will rebuild the volume (note that the rebuild process can take several hours or even days for larger volumes). This RAID configuration has no noticeable effect on write speeds but typically improves read speeds, as the system can read from multiple disks simultaneously.

RAID 5 (Striped with Parity): A RAID 5 array functions similarly to a RAID 0 array in that it stripes data across multiple disks; however, for each set of blocks, it also writes a block of parity data that can be used to recover a block on another disk if it loses that data. Thus, you can achieve some of the performance gains of a RAID 0 array while being able to withstand a single disk failure. This methodology requires at least three disks.

RAID 10 (Striped and Mirrored): A RAID 10 array combines two RAID 1 arrays in a RAID 0 array. This allows you to achieve the performance gains of a RAID 0 array while still maintaining the fault tolerance of a RAID 1 array. Data is striped between the two RAID 1 volumes, which are able to withstand and rebuild after a failed disk. This methodology requires at least four disks. This RAID level is also sometimes referred to as RAID 1+0.

Recovery: Intel Rapid Recovery Technology creates a special RAID 1 array where instead of two equivalent disks, one disk is designated the “primary” and the other the “secondary”. Data is written to the primary drive, then copied to the secondary drive as a backup. This allows you to decide if you would like the mirroring to occur continuously or only on request; in addition, the time it takes to rebuild the array after a disk failure is decreased. However, the read speed improvements of a typical RAID 1 array are not seen here, as the SATA controller will typically only read from the primary drive.

Note: Creating a new RAID array will erase all filesystems and data on all the disks used.

7.2 - Creating and Managing RAID Volumes with Intel RST

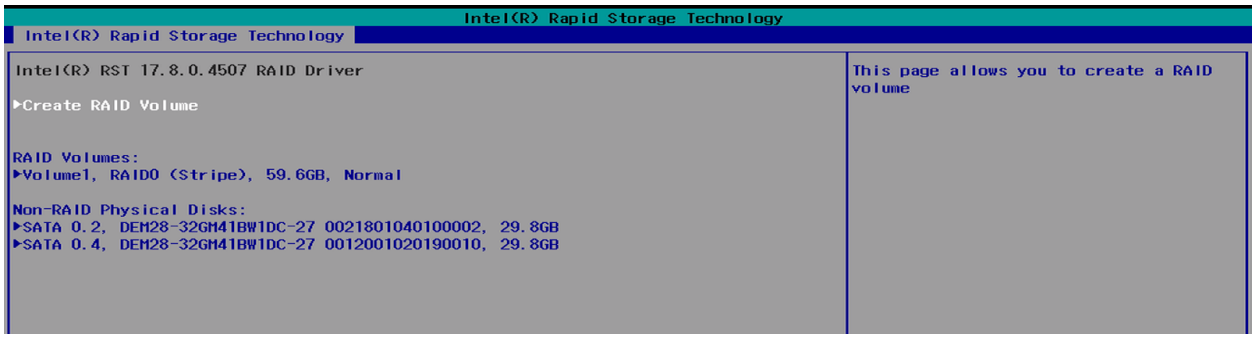
7.2.1 - Device Management Menu

From the main menu, select “Device Management”. You will be greeted with the Device Manager options pictured below. Select “Intel(R) Rapid Storage Technology” to continue.

Note: The Intel(R) Rapid Storage Technology menu will only appear if you have set the SATA Mode Selection option to Intel RST Premium With Intel Optane System Acceleration. This option is located in the main BIOS setup under Advanced > PCH-IO Configuration > SATA And RST Configuration.

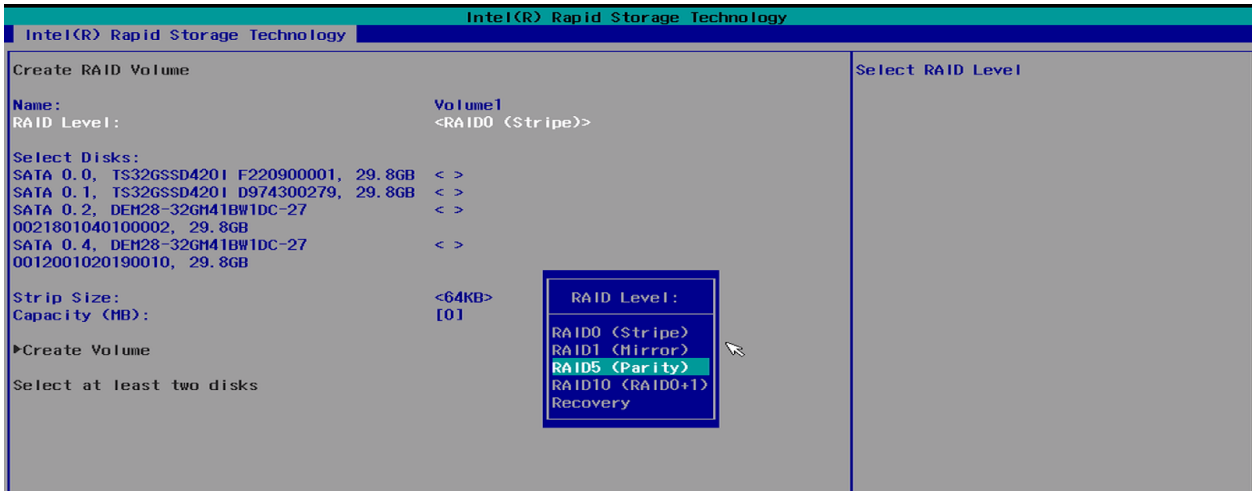
7.2.2 - Intel(R) Rapid Storage Technology Menu

This menu will list all existing RAID arrays, as well as all SATA disks that are not currently in an array. Select “Create RAID Volume” to continue.

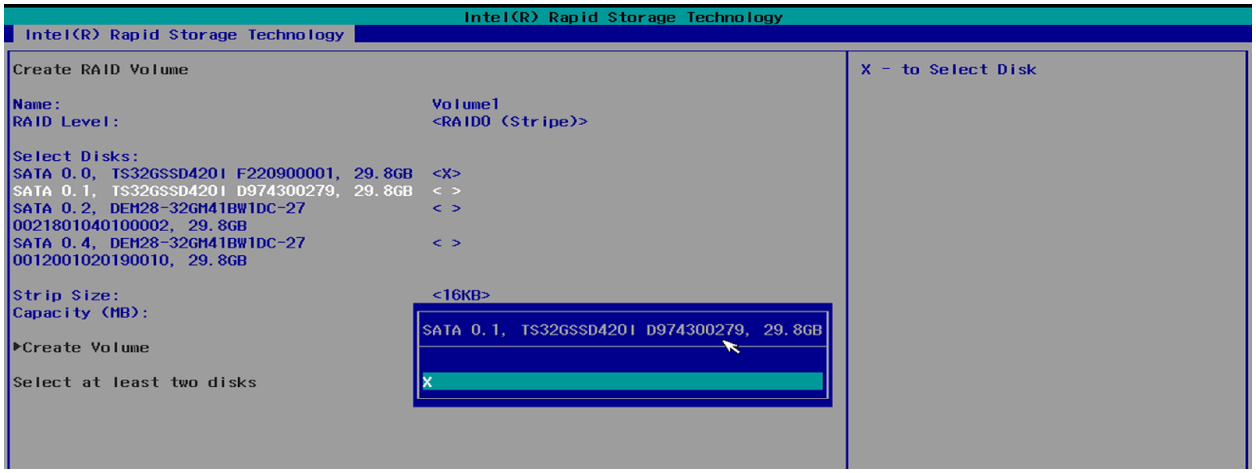


7.2.3 - Creating a New RAID Array

The following menu will give you the option to specify the name of your RAID volume, the RAID level of the configuration, and which disks will become part of the array. Begin by specifying the name of the volume if desired and selecting a RAID Level.



Then, select which SATA disks will be used to create the array. Note that any disks being used in a different RAID array will not be selectable. If you are creating an array with the RAID level “Recovery”, you will need to select which drive is the primary (M) and which is the secondary (R).



For RAID 0, 5, and 10 configurations, you can specify the strip size if desired. The strip size options vary depending on the RAID level of the configuration. In addition, you can set the capacity of the volume if you would like it smaller than the maximum available. If you are

creating a “Recovery” array, you can also select if the slave drive is synchronized with the master continuously or only on request.

Select “Create Volume” to return to the Device Manager menu. You should now see your new volume listed in the menu; hit F10 to save your new settings and Escape to return to the main BIOS menu.

Your RAID array is now created and ready for use.

8 - BIOS Updates

The latest BIOS updates are available from the OnLogic support site.