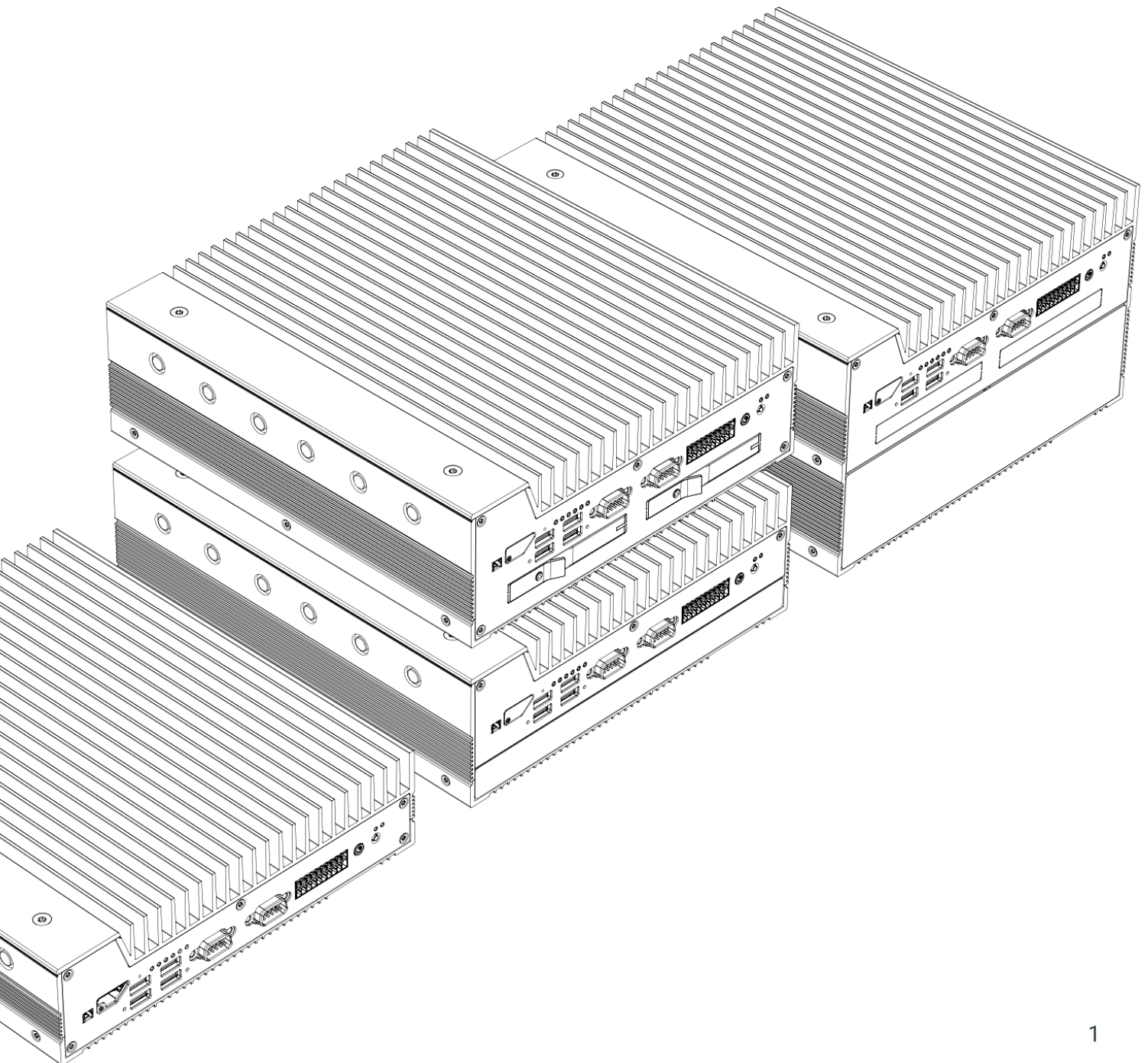


Karbon 800 Series BIOS Manual



Revision History

Revision History	Date
First release of K800 Series BIOS Manual	

Table of Contents

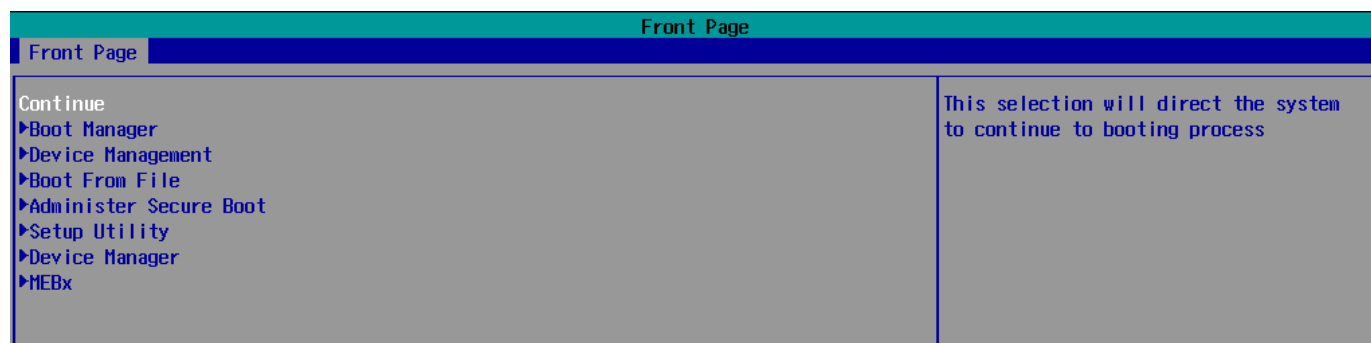
1 - Front Page	5
2 - Main Page	8
3 - Advanced Page	12
3.1 - Boot Configuration	12
3.2 - SATA Configuration	13
3.3 - Chipset Configuration (Intel PTT)	14
3.4 - ACPI Table/Features Control	14
3.4.1 - ACPI Settings	16
3.5 - Connectivity Configuration	20
3.6 - PCIE Configuration	21
3.7 - PCH-IO Configuration	22
3.7.1 - USB Configuration	25
3.7.2 - Security Configuration	27
3.7.3 - HD Audio Configuration	28
3.7.4.1 - HD Audio Advanced Configuration	33
3.7.4.2 - HD Audio DSP Features Configuration	39
3.7.4 - THC Configuration	50
3.7.5 - ISH Configuration	50
3.7.6 - Pch Thermal Throttling Control	51
3.8 - PCH-FW Configuration	52
3.8.1 - AMT Configuration	57

3.8.1.1 - ASF Configuration	59
3.8.1.2 - Secure Erase Configuration	60
3.8.1.3 - One Click Recovery(OCR) Configuration	61
3.8.2 - Firmware Update Configuration	62
3.8.3 - PTT Configuration	63
3.8.4 - FIPS Configuration	63
3.8.5 - Unique Platform Id Configuration	64
3.8.6 - ME Debug Configuration	65
3.8.6.1 - SMBIOS type 130 OEM capabilities	65
3.8.7 - Anti-Rollback SVN Configuration	67
3.9 - Thermal Configuration	68
3.9.1 - CPU Thermal Configuration	69
3.9.2 - Platform Thermal Configuration	72
3.9.3 - Intel(R) Dynamic Tuning Technology Configuration	79
3.9.4 - Hardware Health Monitor	83
3.10 - Platform Settings	84
3.10.1 - System Firmware Update Config	87
3.10.2 - VTIO	88
3.11 - CPU - BCLK Clock Settings	89
3.12 - OnLogic Feature Configuration	89
3.13 - SIO NCT5525D	90
3.13.1 - UART Port 1 Configuration	92
3.13.2 - UART Port 2 Configuration	96
3.13.3 - Fan Control	100
3.13.4 - Hardware Monitor	104

4 - Security Page	107
5 - Boot Page	110
5.1 - EFI	113
6 - Exit Page	114
7 - RAID Configuration	116
7.1 - RAID Overview	116
7.2 - Creating and Managing RAID Volumes with Intel RST	118
7.2.1 - Device Management Menu	118
7.2.2 - Intel(R) Rapid Storage Technology Menu	118
7.2.3 - Creating a New RAID Array	119
8 - BIOS Updates	120

NOTE: To enter the BIOS on Karbon 800 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

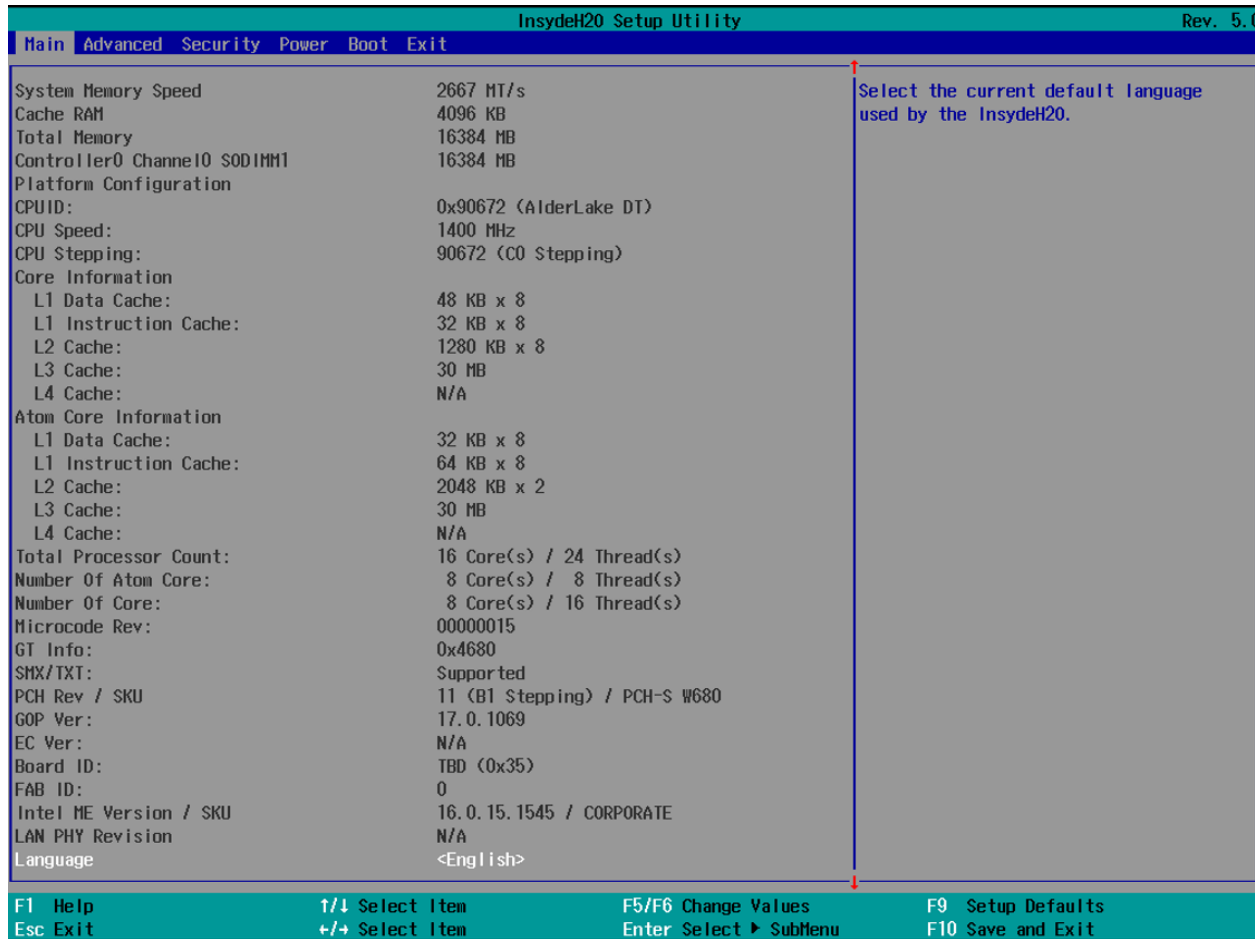
Setup Utility

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



System Memory Speed

Type	Information
BIOS Page	Main Page
Description	Displays current memory transfer rates

Cache RAM

Type	Information
BIOS Page	Main Page
Description	Displays total amount of Cache RAM available on the CPU

Total Memory

Type	Information
BIOS Page	Main Page
Description	Displays the total amount of System RAM

CPUID

Type	Information
BIOS Page	Main Page
Description	Displays CPUID of the processor installed

CPU Speed

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

CPU Stepping

Type	Information
BIOS Page	Main Page
Description	Displays the silicon and metal revision of the CPU

Atom Core/Core Information

Type	Information
BIOS Page	Main Page
Description	Displays L1 Cache sizes, L1 Instruction Sizes, L2 Cache, and L3 Cache for both Efficient (Atom) and Performance cores

Total Processor Count

Type	Information
BIOS Page	Main Page
Description	Displays the total Core(s) and Thread(s) available on the CPU and separates them from Atom and Performance Cores

Microcode Revision

Type	Information
BIOS Page	Main Page
Description	Displays the revision of Microcode being used in the BIOS

GT Info

Type	Information
BIOS Page	Main Page
Description	Displays the information about the iGPU on the CPU

SMX/TXT

Type	Information
BIOS Page	Main Page
Description	Displays whether the CPU supports SMX (Safer Mode Extensions) or TXT (Trusted Execution Technology)

PCH Rev / SKU

Type	Information
BIOS Page	Main Page
Description	Displays the onboard chipset as well as it's silicon and metal layer revision/step

GOP Ver

Type	Information
BIOS Page	Main Page
Description	Displays the GOP Version used by the BIOS

EC Ver

Type	Information
BIOS Page	Main Page

Description	Displays the version of the EC (Embedded Controller) used (N/A on K800 series)
--------------------	--

Fab ID

Type	Information
BIOS Page	Main Page
Description	Displays the FAB ID embedded in the BIOS (0 for K800 series)

Intel ME Version / SKU

Type	Information
BIOS Page	Main Page
Description	Displays the ME Version and SKU (Corporate on K800 series)

LAN PHY Revision

Type	Information
BIOS Page	Main Page
Description	Displays the LAN PHY Revision (K800 series does not use integrated PHY, will display N/A)

Language

Type	Configurable Setting
BIOS Page	Main Page
Description	Allows BIOS Language to be selected

System Time

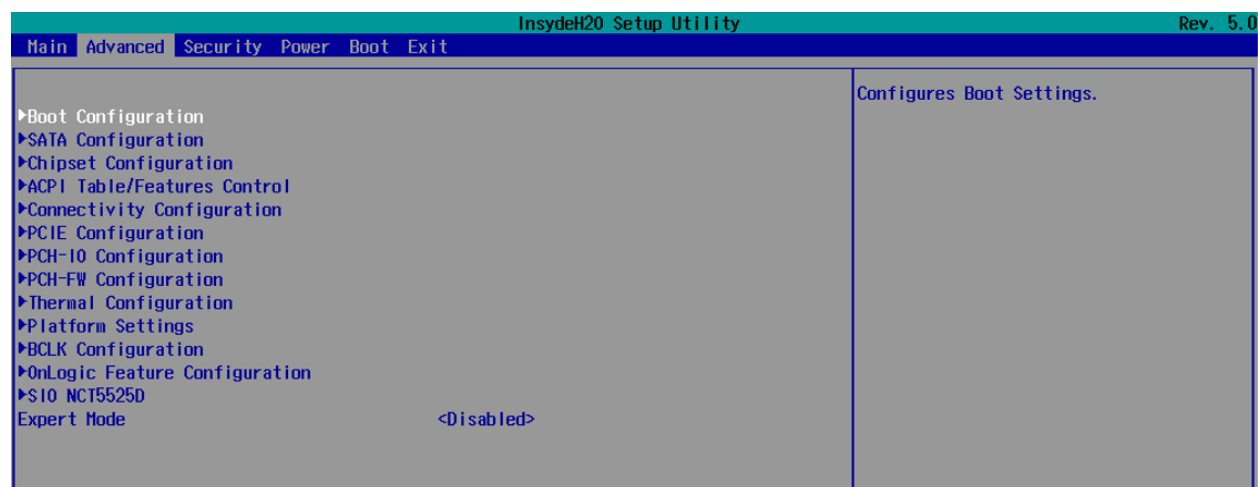
Type	Information
BIOS Page	Main Page

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
--------------------	--

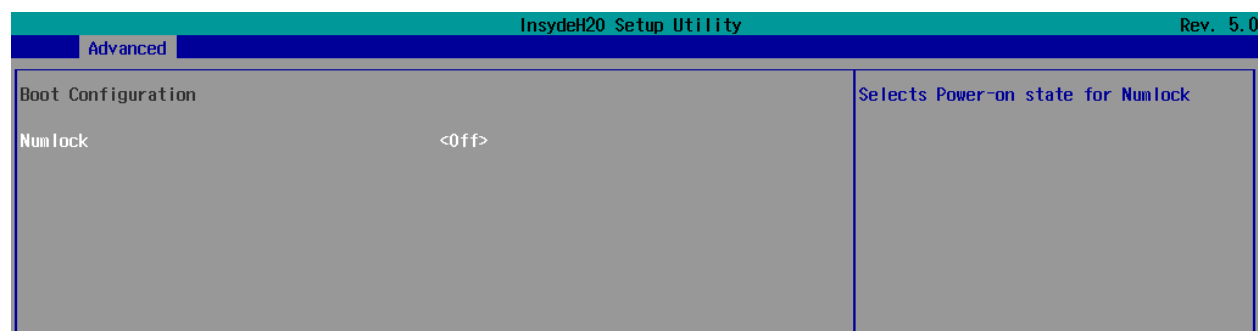
System Date

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



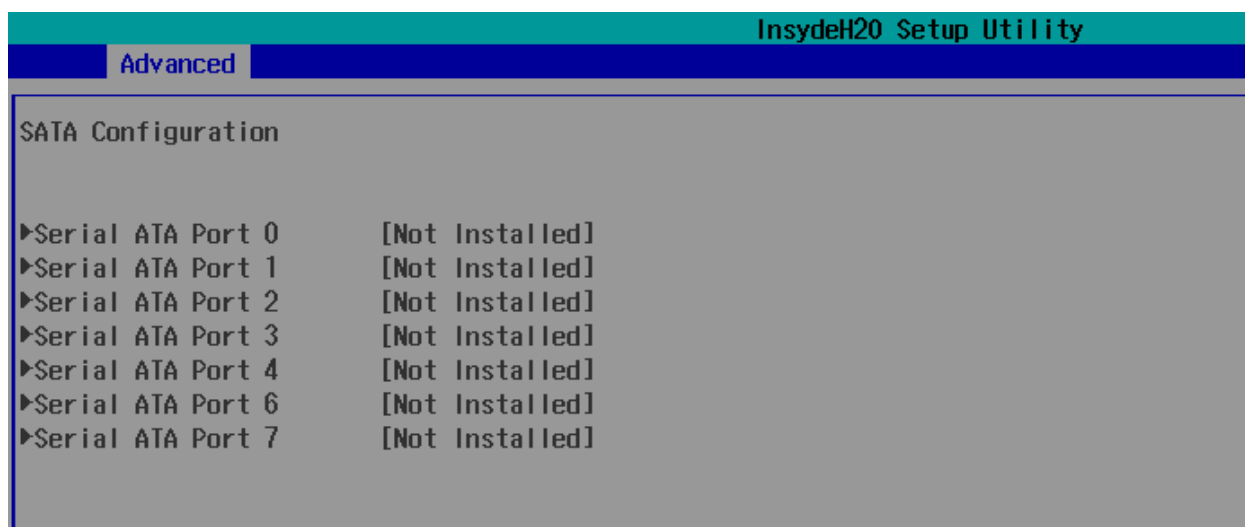
3.1 - Boot Configuration



Numlock

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

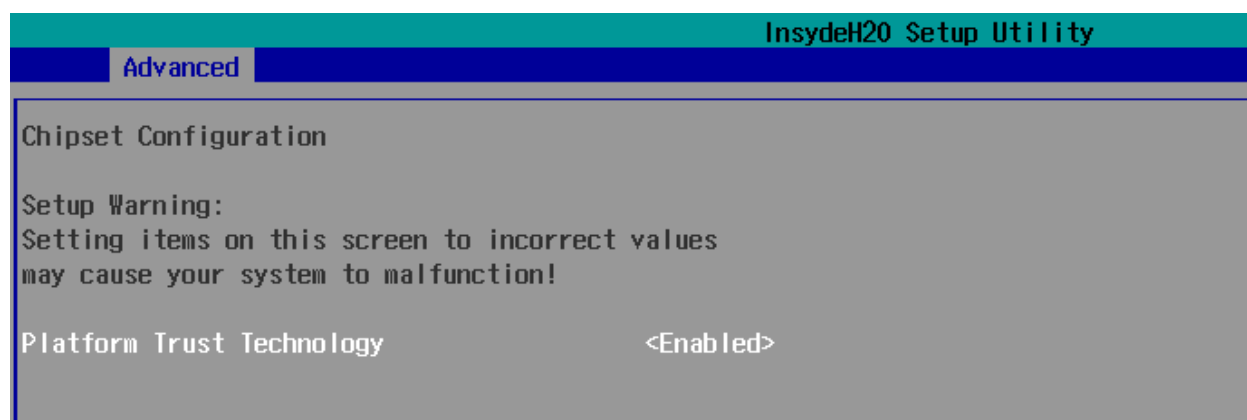
3.2 - SATA Configuration



Serial ATA Port X

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

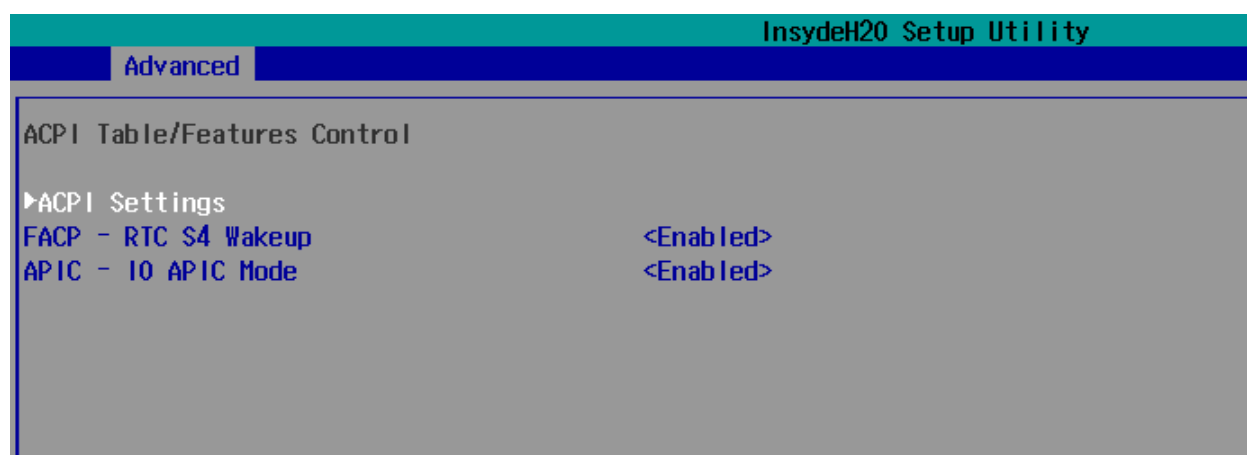
3.3 - Chipset Configuration (Intel PTT)



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



ACPI Settings

Type	Sub-Menu
BIOS Page	Advanced Page > ACPI Table/Features Control

Description	Opens ACPI Settings Menu
--------------------	--------------------------

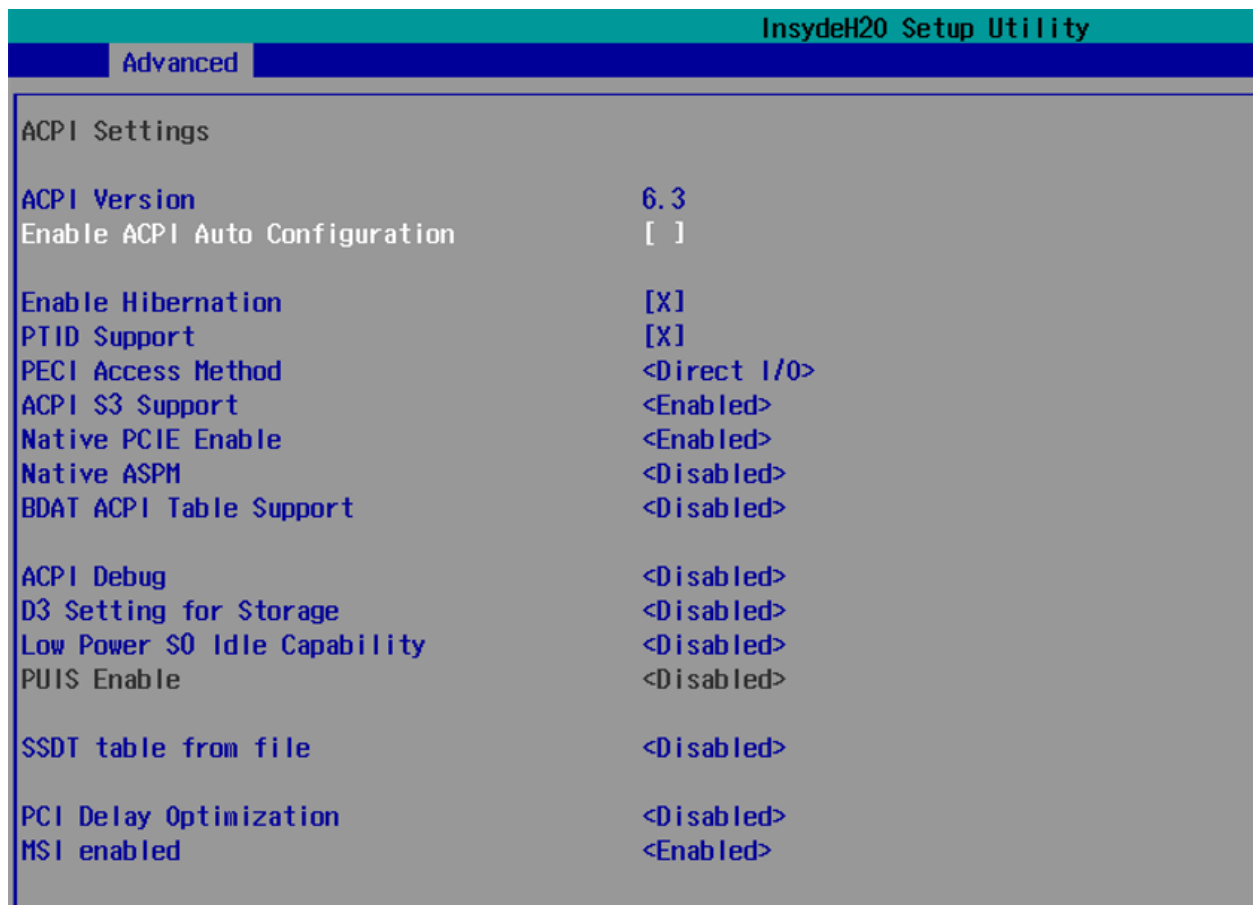
FACP - RTC S4 Wakeup

Type	Configurable Setting
BIOS Page	Advanced Page > ACPI Table/Features Control
Description	Enables or Disables FACP S4 Wakeup via the RTC
Default Value	Enabled

APIC - IO APIC Mode

Type	Configurable Setting
BIOS Page	Advanced Page > ACPI Table/Features Control
Description	Enables or disables IO APIC Mode
Default Value	Enabled

3.4.1 - ACPI Settings



ACPI Version

Type	Information
BIOS Page	Advanced Page > ACPI Table/Features Control > ACPI Settings
Description	Displays the current ACPI Version

Enable ACPI Auto Configuration

Type	Configurable Setting
BIOS Page	Advanced Page > ACPI Table/Features Control > ACPI Settings
Description	Enables or Disables ACPI Auto Configuration
Default Value	<Enabled>

Enable Hibernation

Type	Configurable Setting
BIOS Page	Advanced Page > ACPI Table/Features Control > ACPI Settings
Description	Enables or Disables Hibernation support
Default Value	[X] (Enabled)

PTID Support

Type	Configurable Setting
BIOS Page	Advanced Page > ACPI Table/Features Control > ACPI Settings
Description	Enables or Disables PTID support
Default Value	[X] (Enabled)

PECI Access Method

Type	Configurable Setting
BIOS Page	Advanced Page > ACPI Table/Features Control > ACPI Settings
Description	PECI Access Method select between Direct I/O or ACPI
Default Value	<Direct I/O>

ACPI S3 Support

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

Native PCIE Enable

Type	Configurable Setting
BIOS Page	Advanced Page > ACPI Table/Features Control > ACPI Settings
Description	Enable or disable Native PCIe Control

Default Value	<Enabled>
----------------------	-----------

Native ASPM

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

BDAT ACPI Table

Type	Configurable Setting
BIOS Page	Advanced Page > ACPI Table/Features Control > ACPI Settings
Description	Enables or Disables Native Active State Power Management (ASPM)
Default Value	<Disabled>

ACPI Debug

Type	Configurable Setting
BIOS Page	Advanced Page > ACPI Table/Features Control > ACPI Settings
Description	Enables or Disables ACPI Debug
Default Value	<Disabled>

D3 Setting for Storage

Type	Configurable Setting
BIOS Page	Advanced Page > ACPI Table/Features Control > ACPI Settings

Description	Enables or Disables RTD3 support for Storage. PCIe Storage PEP constraint needs to be set as D0/F1 under ACPI Settings > PEP PCIe Storage when this setup is Disabled/D3Hot
Default Value	<Disabled>

Low Power S0 Idle Capability

Type	Configurable Setting
BIOS Page	Advanced Page > ACPI Table/Features Control > ACPI Settings
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>

PUIS Enable

Type	Configurable Setting
BIOS Page	Advanced Page > ACPI Table/Features Control > ACPI Settings
Description	Enables or Disables Native Active State Power Management (ASPM)
Default Value	<Disabled>

SSDT table from file

Type	Configurable Setting
BIOS Page	Advanced Page > ACPI Table/Features Control > ACPI Settings
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>

PCI Delay Optimization

Type	Configurable Setting
BIOS Page	Advanced Page > ACPI Table/Features Control > ACPI Settings

Description	Enable or Disable ACPI additions for Firmware latency optimizations
Default Value	<Disabled>

MSI enabled

Type	Configurable Setting
BIOS Page	Advanced Page > ACPI Table/Features Control > ACPI Settings
Description	When disabled, MSI support is disabled in FADT
Default Value	<Disabled>

3.5 - Connectivity Configuration

InsydeH20 Setup Utility	
Advanced	
CNVi CRF Present	No
CNVi Configuration	
CNVi Mode	<Auto Detection>
Wi-Fi Core	<Enabled>
BT Core	<Enabled>
BT Audio Offload	<Disabled>
RFI Mitigation	<Enabled>
CoExistence Manager	<Disabled>

CNVi CRF Present

Type	Information
BIOS Page	Advanced Page > Connectivity Configuration
Description	Displays whether a CNVi module is present (Not supported on K800 series)

CNVi Mode

Type	Configurable Setting
-------------	----------------------

BIOS Page	Advanced Page > Connectivity Configuration
Description	Configures CNVi Connectivity
Possible Values	<Auto Detection> if a discrete solution is discovered, it will be enabled by default <Disable Integrated> Disables Integrated solution (Not supported on K800 series)
Default Value	<Auto Detection>

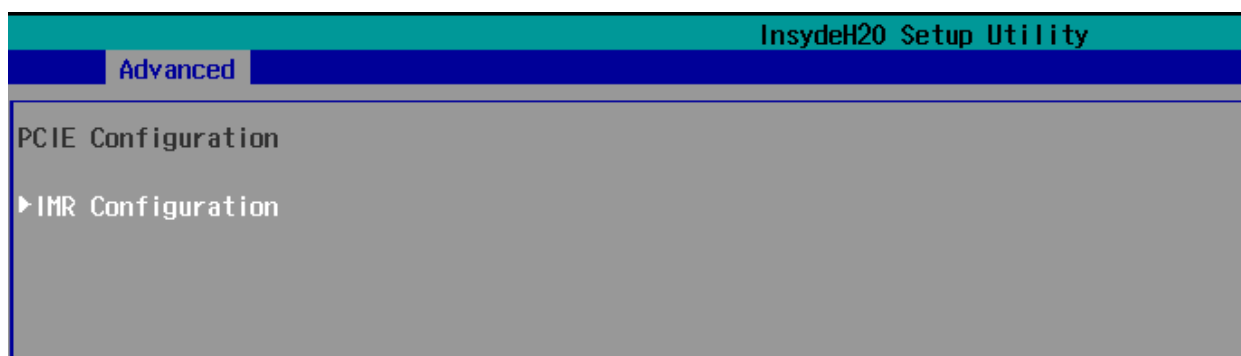
RFI Mitigation

Type	Configurable Setting
BIOS Page	Advanced Page > Connectivity Configuration
Description	Enables or Disables RFI Mitigation for DDR-RFIM
Default Value	<Enabled>

CoExistence Manager

Type	Configurable Setting
BIOS Page	Advanced Page > Connectivity Configuration
Description	Enables or disables CoExistence Manager (Not supported on K800 series)
Default Value	<Disabled>

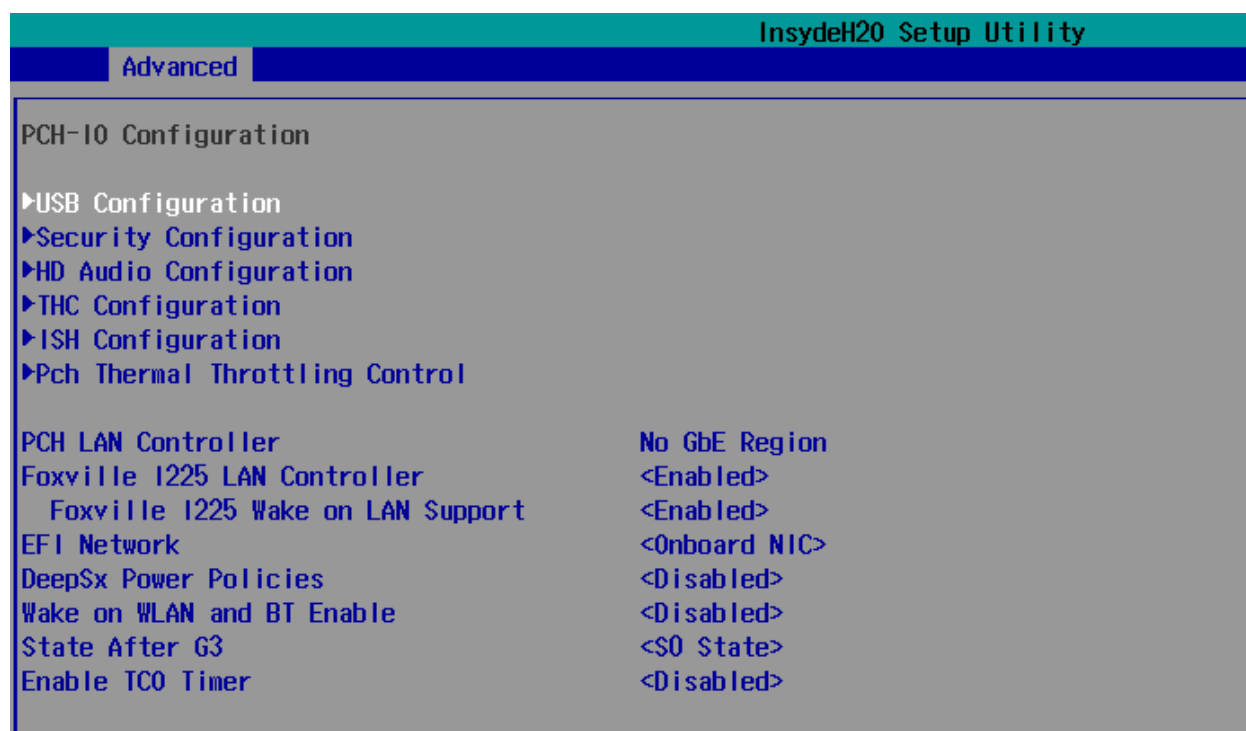
3.6 - PCIE Configuration



IMR Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCIE Configuration
Description	Opens up IMR Configuration - K800 does not support this and leads to a blank menu

3.7 - PCH-IO Configuration



USB Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO
Description	Opens USB Configuration Menu

Security Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO

Description	Opens Security Configuration Menu
--------------------	-----------------------------------

HD Audio Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO
Description	Opens HD Audio Configuration Menu

THC Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO
Description	Opens THC Configuration Menu

ISH Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO
Description	Opens ISH (Intel Sensor Hub) Settings Menu

Pch Thermal Throttling Control

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO
Description	Opens PCH Thermal Throttling Control Settings Menu

PCH LAN Controller

Type	Information
BIOS Page	Advanced Page > PCH-IO
Description	Displays status of PCH LAN Controller. K800 does not use internal PCH controller, and therefore has the GbE Region Disabled
Default Value	<No GbE Region>

Foxville I225 LAN Controller

Type	Configurable
BIOS Page	Advanced Page > PCH-IO
Description	Displays status of the i225-LM LAN Controller (LAN1)
Default Value	<Enabled>

Foxville I225 Wake on LAN Support

Type	Configurable
BIOS Page	Advanced Page > PCH-IO
Description	Enables or disables Wake on LAN Support
Default Value	<Enabled>

EFI Network

Type	Configurable
BIOS Page	Advanced Page > PCH-IO
Description	Enables/Disables EFI Network support for onboard LAN
Default Value	<Onboard NIC>

DeepSx Power Policies

Type	Configurable
BIOS Page	Advanced Page > PCH-IO
Description	Enables or disables DeepSx or Deep Sleep/Ultra Low power states
Default Value	<Disabled>

Wake on WLAN and BT Enable

Type	Configurable
BIOS Page	Advanced Page > PCH-IO
Description	Enables or disables Wake on WLAN and BT Enable for CNVi cards (Not supported on K800 series)
Default Value	<Disabled>

State After G3

Type	Configurable
BIOS Page	Advanced Page > PCH-IO
Description	Defines the state after entering a G3 state (Power unplugged from system entirely)
Possible Values	<S0 State> <S5 State>
Default Value	<S0 State>

Enable TCO Timer

Type	Configurable
BIOS Page	Advanced Page > PCH-IO
Description	Enables or Disables the TCO Watchdog Timer
Default Value	<Disabled>

3.7.1 - USB Configuration

InsydeH20 Setup Utility	
Advanced	
USB Configuration	
xDCI Support	<Disabled>
USB PDO Programming	<Enabled>
USB Overcurrent	<Enabled>
USB Overcurrent Lock	<Enabled>
USB Audio Offload	<Enabled>
Enable HSII on xHCI	<Enabled>
USB Port Disable Override	<Disable>

xDCI Support

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > USB Configuration

Description	Enables or Disables xDCI Support for USB OTG (Not supported on K800 Series)
Default Value	<Disabled>

USB PDO Programming

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > USB Configuration
Description	Select 'Enabled' if Port Disable Override functionality is used
Default Value	<Enabled>

USB Overcurrent

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > USB Configuration
Description	Enables or Disables overcurrent notifications in the Operating systems
Default Value	<Enabled>

USB Overcurrent Lock

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > USB Configuration
Description	Select 'Enabled' if Overcurrent functionality is used. Enabling this will make xHCI controller consume the Overcurrent mapping data
Default Value	<Enabled>

USB Audio Offload

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > USB Configuration
Description	Enables or Disables USB Audio Offloading
Default Value	<Enabled>

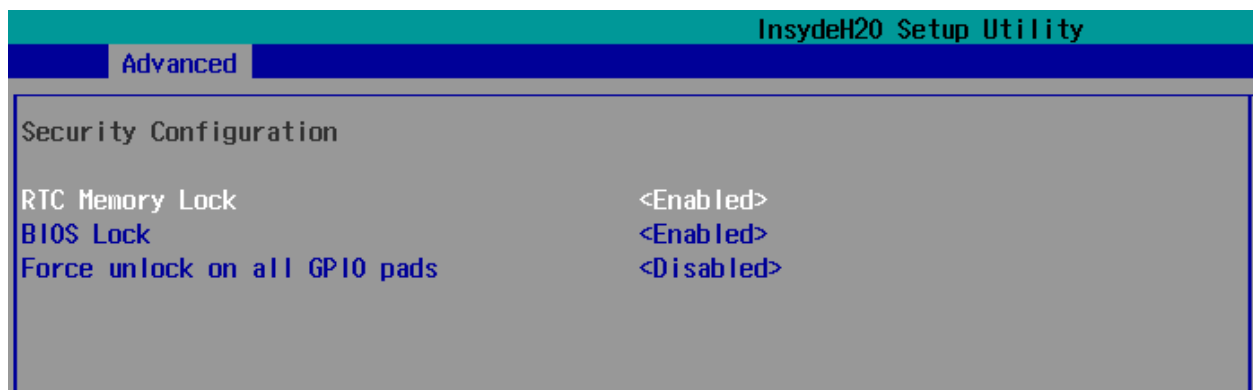
Enable HSII on xHCI

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > USB Configuration
Description	Enable or Disable HSII feature. It may lead to increased power consumption
Default Value	<Enabled>

USB Port Disable Override

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > USB Configuration
Description	Enables or Disables override capabilities on USB Ports
Default Value	<Disabled>

3.7.2 - Security Configuration



RTC Memory Lock

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Security Configuration
Description	Enables or Disables RTC Memory Lock
Default Value	<Enabled>

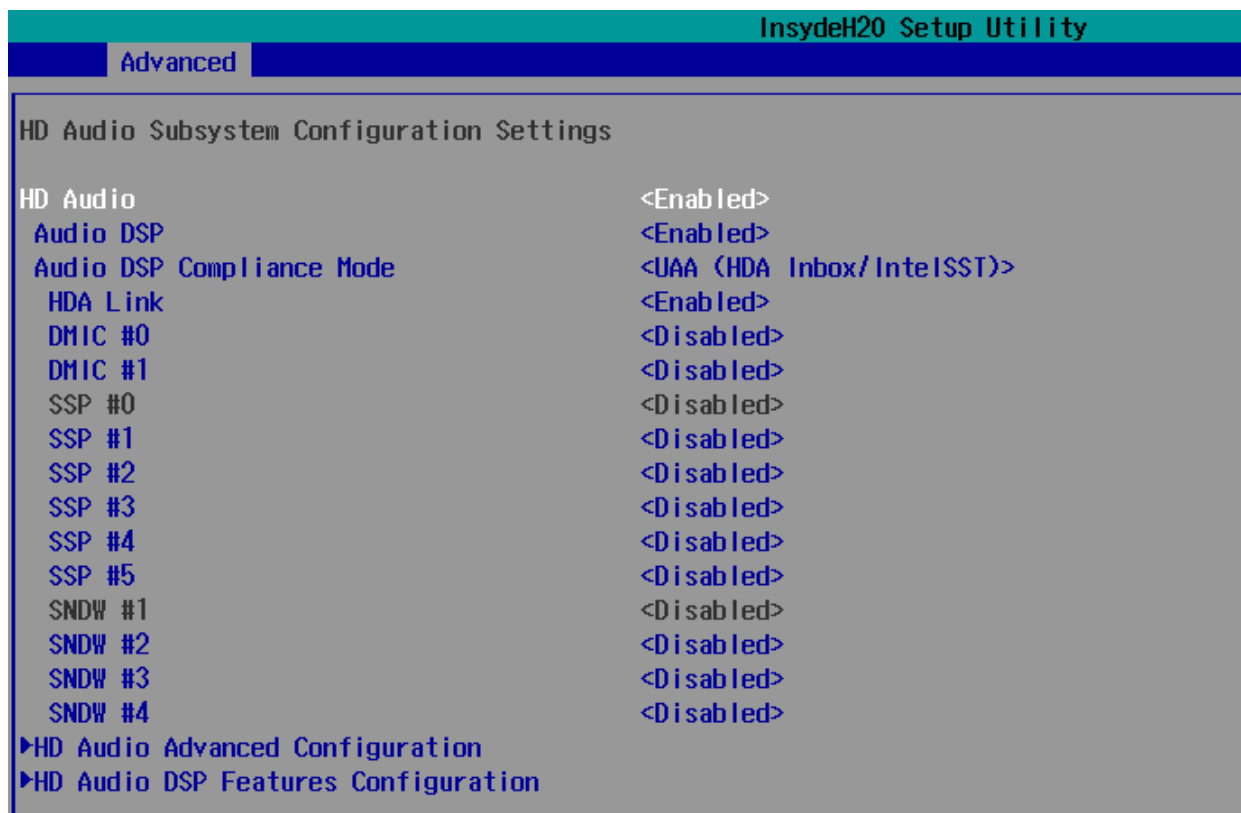
BIOS Lock

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Security Configuration
Description	Enables or Disables BIOS Lock
Default Value	<Enabled>

Force unlock on all GPIO pads

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Security Configuration
Description	Enables or Disables forcing all GPIO pads to be in an unlocked state
Default Value	<Disabled>

3.7.3 - HD Audio Configuration



HD Audio

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration
Description	Enables or disables the onboard audio (ALC888)
Default Value	<Enabled>

Audio DSP

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration
Description	Enables or disables the Audio DSP
Default Value	<Enabled>

Audio DSP Compliance Mode

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration
Description	Selects the audio DSP, default is HD Audio Inbox for Windows/Intel Smart Sound Technology
Default Value	<UAA (HDA Inbox/IntelSST)>

HDA Link

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration
Description	Enables or Disables the HD Audio Link
Default Value	<Enabled>

DMIC #0

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration
Description	Enables or disables DMIC #0 (Not supported on K800 series)
Default Value	<Disabled>

DMIC #1

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration
Description	Enables or disables DMIC #1 (Not supported on K800 series)
Default Value	<Disabled>

SSP #0

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration
Description	Enables or disables SSP #0 (Not supported on K800 series)
Default Value	<Disabled>

SSP #1

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration
Description	Enables or disables SSP #1 (Not supported on K800 series)
Default Value	<Disabled>

SSP #2

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration
Description	Enables or disables SSP #2 (Not supported on K800 series)
Default Value	<Disabled>

SSP #3

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration
Description	Enables or disables SSP #3 (Not supported on K800 series)
Default Value	<Disabled>

SSP #4

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration
Description	Enables or disables SSP #4 (Not supported on K800 series)
Default Value	<Disabled>

SSP #5

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration
Description	Enables or disables SSP #5 (Not supported on K800 series)
Default Value	<Disabled>

SNDW #1

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration
Description	Enables or disables SNDW #1 (Not supported on K800 series)
Default Value	<Disabled>

SNDW #2

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration
Description	Enables or disables SNDW #2 (Not supported on K800 series)
Default Value	<Disabled>

SNDW #3

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration
Description	Enables or disables SNDW #3 (Not supported on K800 series)

Default Value	<Disabled>
----------------------	------------

SNDW #4

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration
Description	Enables or disables SNDW #4 (Not supported on K800 series)
Default Value	<Disabled>

HD Audio Advanced Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration
Description	Opens HD Audio Advanced Configuration Menu

HD Audio DSP Features Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration
Description	Opens HD Audio DSP Features Configuration

3.7.4.1 - HD Audio Advanced Configuration

```

InsydeH20 Setup Utility

Advanced

HD Audio Subsystem Advanced Configuration Settings

iDisplay Audio Disconnect          <Disabled>
Codec Sx Wake Capability          <Disabled>
PME Enable                        <Disabled>
Statically Switchable BCLK Clock Frequency Configuration:
  HD Audio Link Frequency          <24 MHz>
  iDisplay Audio Link Frequency    <96 MHz>
  iDisplay Audio Link T-Mode       <8T Mode>
Autonomous Clock Stop SNDW #1     <Disabled>
Autonomous Clock Stop SNDW #2     <Disabled>
Autonomous Clock Stop SNDW #3     <Disabled>
Autonomous Clock Stop SNDW #4     <Disabled>
Data On Active Interval Select SNDW #1 <11 clock periods>
Data On Active Interval Select SNDW #2 <11 clock periods>
Data On Active Interval Select SNDW #3 <11 clock periods>
Data On Active Interval Select SNDW #4 <11 clock periods>
Data On Delay Select SNDW #1       <3 clock periods>
Data On Delay Select SNDW #2       <3 clock periods>
Data On Delay Select SNDW #3       <3 clock periods>
Data On Delay Select SNDW #4       <3 clock periods>

```

iDisplay Audio Disconnect

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables iDisplay Audio Connect
Default Value	<Disabled>

Codec Sx Wake Capability

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Codec Sx Wake Capabilities
Default Value	<Disabled>

PME Enable

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables PME (Power Management Event) wake of HD Audio Controller during POST
Default Value	<Disabled>

HD Audio Link Frequency

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Selects clock frequency for HD Audio Link - OnLogic has only validated 24MHz functionality. Changing this setting may impact performance/functionality
Possible Values	<6 MHz> <12 MHz> <24 MHz>
Default Value	<24 MHz>

iDisplay Audio Link Frequency

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Selects clock frequency for iDisplay Audio Link
Possible Values	<48 MHz> <96 MHz>
Default Value	<96 MHz>

iDisplay Audio Link T-Mode

Type	Configurable
-------------	--------------

BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Selects iDisplay Audio Link T-Mode
Possible Values	<1T Mode> <2T Mode> <4T Mode> <8T Mode> <16T Mode>
Default Value	<8T Mode>

Autonomous Clock Stop SNDW #1

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Autonomous Clock Stop on SNDW #1 (Not supported by K800)
Default Value	<Disabled>

Autonomous Clock Stop SNDW #2

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Autonomous Clock Stop on SNDW #2 (Not supported by K800)
Default Value	<Disabled>

Autonomous Clock Stop SNDW #3

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Autonomous Clock Stop on SNDW #3 (Not supported by K800)
Default Value	<Disabled>

Autonomous Clock Stop SNDW #4

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Autonomous Clock Stop on SNDW #1 (Not supported by K800)
Default Value	<Disabled>

Data On Active on Interval Select SNDW #1

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Data On Active on Interval Select SNDW #1 (Not supported by K800)
Default Value	<Disabled>

Data On Active on Interval Select SNDW #2

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Data On Active on Interval Select SNDW #2 (Not supported by K800)
Default Value	<Disabled>

Data On Active on Interval Select SNDW #3

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Data On Active on Interval Select SNDW #3 (Not supported by K800)
Default Value	<Disabled>

Data On Active on Interval Select SNDW #4

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Data On Active on Interval Select SNDW #4 (Not supported by K800)
Default Value	<Disabled>

Data On Delay Select SNDW #1

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Data On Delay Select for SNDW #1 (Not supported by K800)
Default Value	<Disabled>

Data On Delay Select SNDW #2

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Data On Delay Select for SNDW #2 (Not supported by K800)
Default Value	<Disabled>

Data On Delay Select SNDW #3

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Data On Delay Select for SNDW #3 (Not supported by K800)
Default Value	<Disabled>

Data On Delay Select SNDW #4

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Data On Delay Select for SNDW #4 (Not supported by K800)
Default Value	<Disabled>

3.7.4.2 - HD Audio DSP Features Configuration

HD Audio Subsystem Features Configuration (ACPI)

Audio DSP NHLT Endpoints Configuration:

Dmic Mono 38.4MHz	<Disabled>
Dmic Stereo 38.4MHz	<Disabled>
Dmic Quad 38.4MHz	<Disabled>
Dmic Mono 24MHz	<Disabled>
Dmic Stereo 24MHz	<Disabled>
Dmic Quad 24MHz	<Disabled>
Bluetooth 38.4MHz	<Disabled>
Bluetooth 24MHz	<Disabled>
I2S ALC274 38.4MHz	<Disabled>
I2S ALC274 24MHz	<Disabled>
I2S Codec Select	<Disabled>
I2S Codec Bus Number	<I2C0 Controller>

Audio DSP Feature Support:

WoV (Wake on Voice)	[X]
Bluetooth Sideband	[]
BT Intel HFP	[]
BT Intel A2DP	[]
Codec based VAD	[]
DSP based Speech	[]
Pre-Processing Disabled	
Voice Activity Detection	<Windows 10 Voice Activation>

Audio DSP Pre/Post-Processing Module Support:

Waves Post-process	[]
DTS	[]
Intel SST Speech	[]
Dolby	[]
Waves Pre-process	[]
Audyssey	[]
Maxim Smart AMP	[]

Maxim Smart AMP	[]
FortMedia SAMSoft	[]
Sound Research IP	[]
Conexant Pre-Process	[]
Conexant Smart Amp	[]
Realtek Post-Process	[]
Realtek Smart Amp	[]
Icepower IP MFX sub module	[]
Icepower IP EFX sub module	[]
Icepower IP SFX sub module	[]
Voice Preprocessing	[]
Acoustic Context Awareness (ACA)	[]
Custom Module 'Alpha'	[]
Custom Module 'Beta'	[]
Custom Module 'Gamma'	[]

Dmic Mono 38.4MHz

Type	Information
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio DSP Features Configuration
Description	Displays the status of the Dmic Mono 38.4MHz audio

Dmic Stereo 38.4MHz

Type	Information
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio DSP Features Configuration
Description	Displays the status of the Dmic Stereo 38.4MHz audio

Dmic Quad 38.4MHz

Type	Information
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio DSP Features Configuration
Description	Displays the status of the Dmic Stereo 38.4MHz audio

Dmic Mono 24MHz

Type	Information
------	-------------

BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio DSP Features Configuration
Description	Displays the status of the Dmic Mono 24MHz audio

Dmic Stereo 24MHz

Type	Information
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio DSP Features Configuration
Description	Displays the status of the Dmic Stereo 24MHz audio

Dmic Quad 24MHz

Type	Information
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio DSP Features Configuration
Description	Displays the status of the Dmic Quad 24MHz audio

Bluetooth 38.4MHz

Type	Information
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio DSP Features Configuration
Description	Displays the status of the Bluetooth 38.4MHz audio

Bluetooth 24MHz

Type	Information
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio DSP Features Configuration
Description	Displays the status of the Bluetooth 24MHz audio

I2S ALC274 38.4MHz

Type	Information
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio DSP Features Configuration

Description	Displays the status of the I2S ALC274 38.4MHz audio (K800 Series uses ALC888)
--------------------	---

I2S ALC274 24MHz

Type	Information
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio DSP Features Configuration
Description	Displays the status of the I2S ALC274 24MHz audio (K800 Series uses ALC888)

I2S Codec Select

Type	Information
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio DSP Features Configuration
Description	Displays the status of the I2S Codec selection

I2S Codec Bus Number

Type	Information
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio DSP Features Configuration
Description	Displays the status of the I2S Codec Bus Number (K800 uses HDA not I2S bus)

WoV (Wake on Voice)

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Wake on Voice functionality
Default Value	[X] (Enabled)

Bluetooth Sideband

Type	Configurable
-------------	--------------

BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Bluetooth Sideband
Default Value	[] (Disabled)

BT Intel HFP

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Bluetooth Intel HFP
Default Value	[] (Disabled)

BT Intel A2DP

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Bluetooth Intel A2DP
Default Value	[] (Disabled)

Codec based VAD

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables codec based VAD
Default Value	[] (Disabled)

DSP based speech

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables DSP based speech

Default Value	[] (Disabled)
----------------------	----------------

Voice Activity Detection

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables DSP based speech
	<Intel Wake on Voice> <Windows 10 Voice Activation>
Default Value	<Windows 10 Voice Activation>

Waves Post-process

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Waves Post-process
Default Value	[] (Disabled)

DTS

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables DTS
Default Value	[] (Disabled)

Intel SST Speech

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Intel SST Speech
Default Value	[] (Disabled)

Dolby

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Dolby
Default Value	[] (Disabled)

Waves Pre-process

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Waves Pre-process
Default Value	[] (Disabled)

Audyssey

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Audyssey
Default Value	[] (Disabled)

Maxim Smart AMP

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Maxim Smart AMP
Default Value	[] (Disabled)

ForteMedia SAMSoft

Type	Configurable
-------------	--------------

BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables ForteMedia SAMSoft
Default Value	[] (Disabled)

Sound Research IP

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Sound Research IP
Default Value	[] (Disabled)

Conexant Pre-Process

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Conexant Pre-Process
Default Value	[] (Disabled)

Conexant Smart Amp

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Conexant Smart Amp
Default Value	[] (Disabled)

Realtek Post-Process

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Realtek Post-Process

Default Value	[] (Disabled)
----------------------	----------------

Realtek Smart Amp

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Realtek Smart Amp
Default Value	[] (Disabled)

Icepower IP MFX sub module

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Icepower IP MFX sub module
Default Value	[] (Disabled)

Icepower IP EFX sub module

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Icepower IP EFX sub module
Default Value	[] (Disabled)

Icepower IP SFX sub module

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Icepower IP SFX sub module
Default Value	[] (Disabled)

Voice Preprocessing

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Voice Preprocessing
Default Value	[] (Disabled)

Acoustic Context Awareness (ACA)

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Acoustic Context Awareness (ACA)
Default Value	[] (Disabled)

Custom Module 'Alpha'

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Custom Module 'Alpha'
Default Value	[] (Disabled)

Custom Module 'Beta'

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Custom Module 'Beta'
Default Value	[] (Disabled)

Custom Module 'Gamma'

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings

Description	Enables or Disables Custom Module 'Gamma'
Default Value	[] (Disabled)

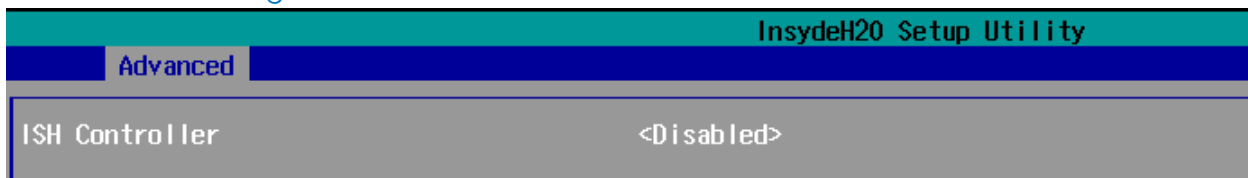
3.7.4 - THC Configuration



THC Configuration

Type	Information
BIOS Page	Advanced Page > PCH-IO > THC Configuration
Description	THC (Touch Host Controller) Configuration is not Available on K800 Series

3.7.5 - ISH Configuration



ISH Controller

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > HD Audio Configuration > HD Audio Subsystem Advanced Configuration Settings
Description	Enables or Disables Intel Sensor Hub (Not used on K800 Series)
Default Value	<Disabled>

3.7.6 - Pch Thermal Throttling Control

InsydeH20 Setup Utility	
Advanced	
Thermal Throttling Level	<Suggested Setting>
DMI Thermal Setting	<Suggested Setting>
SATA Thermal Setting	<Suggested Setting>

Thermal Throttling Level

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Pch Thermal Throttling Control
Description	Decide whether to use suggested settings, or set to manual settings
Default Value	<Suggested Setting>

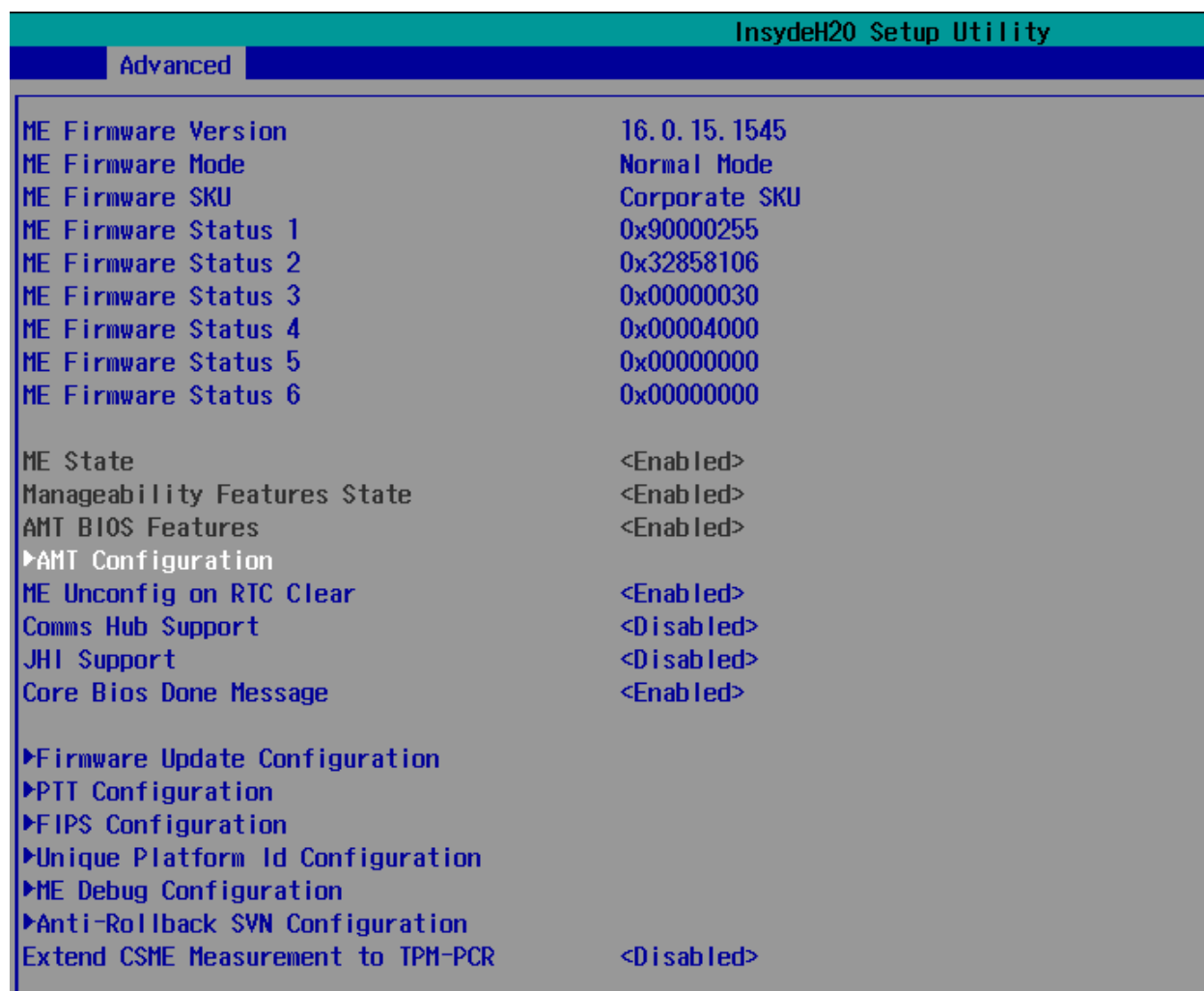
DMI Thermal Setting

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Pch Thermal Throttling Control
Description	Decide whether to use suggested settings, or set to manual settings
Default Value	<Suggested Setting>

SATA Thermal Setting

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Pch Thermal Throttling Control
Description	Decide whether to use suggested settings, or set to manual settings
Default Value	<Suggested Setting>

3.8 - PCH-FW Configuration



ME Firmware Version

Type	Information
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration
Description	Displays the Intel Management Engine Firmware Version

ME Firmware Mode

Type	Information
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration
Description	Displays the Intel Management Engine Firmware Mode

ME Firmware SKU

Type	Information
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration
Description	Displays the Intel Management Engine Firmware SKU

ME Firmware Status 1

Type	Information
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration
Description	Displays the Intel Management Engine Firmware Status 1

ME Firmware Status 2

Type	Information
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration
Description	Displays the Intel Management Engine Firmware Status 2

ME Firmware Status 3

Type	Information
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration
Description	Displays the Intel Management Engine Firmware Status 3

ME Firmware Status 4

Type	Information
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration
Description	Displays the Intel Management Engine Firmware Status 4

ME Firmware Status 5

Type	Information
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration
Description	Displays the Intel Management Engine Firmware Status 5

ME Firmware Status 6

Type	Information
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration
Description	Displays the Intel Management Engine Firmware Status 6

ME State

Type	Information
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration
Description	Displays the status of the Management Engine

Manageability Features State

Type	Information
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration
Description	Displays the status of the Management Engine Manageability Features state

AMT BIOS Features

Type	Information
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration
Description	Displays the status of the AMT BIOS Features

AMT Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration
Description	Opens AMT Configuration Sub-Menu

ME Unconfic on RTC Clear

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration
Description	Enables or disables unconfiguration upon RTC Clear

Default Value	<Enabled>
----------------------	-----------

Comms Hub Support

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration
Description	Enables or disables Comms Hub Support
Default Value	<Disabled>

JHI Support

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration
Description	Enables or disables JHI Support
Default Value	<Disabled>

Core Bios Done Message

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration
Description	Enables or disables Core Bios Done Message
Default Value	<Enabled>

Firmware Update Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration
Description	Opens Firmware Update Configuration Sub-Menu

PTT Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration
Description	Opens PTT Configuration Sub-Menu

FIPS Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration
Description	Opens PTT FIPS Configuration Sub-Menu

Unique Platform Id Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration
Description	Opens Unique Platform Id Configuration Sub-Menu

ME Debug Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration
Description	Opens ME Debug Configuration Sub-Menu

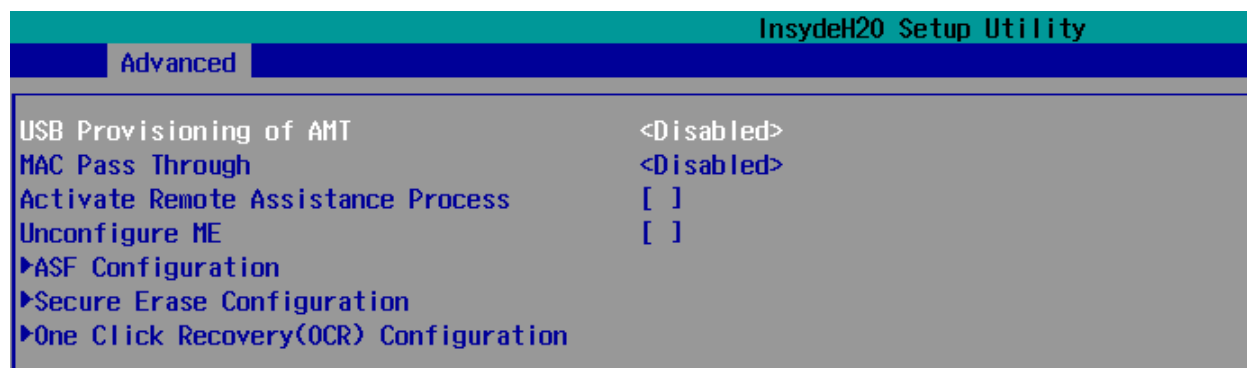
Anti-Rollback SVN Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration
Description	Opens Anti-Rollback SVN Configuration Sub-Menu

Extend CSME Measurement to TPM-PCR

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration
Description	Enables or disables Extending CSME Measurement to TPM-PCR
Default Value	<Disabled>

3.8.1 - AMT Configuration



USB Provisioning of AMT

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > PTT Configuration
Description	Enables or disables USB Provisioning of AMT
Default Value	<Disabled>

MAC Pass Through

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > PTT Configuration
Description	Enables or disables MAC Pass Through on the AMT enabled port (i225-LM/LAN1)
Default Value	<Disabled>

Activate Remote Assistance Process

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > PTT Configuration
Description	Enables or disables Remote Assistance Process
Default Value	[] (Disabled)

Unconfigure ME

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > PTT Configuration
Description	Unconfigures the current Management Engine settings
Default Value	[] (Disabled)

ASF Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > PTT Configuration
Description	Opens ASF (Alert Standard Format) Configuration Sub-Menu

Secure Erase Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > PTT Configuration
Description	Opens Secure Erase Configuration Sub-Menu

One Click Recovery (OCR) Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > PTT Configuration
Description	Opens Secure Erase Configuration Sub-Menu

3.8.1.1 - ASF Configuration

InsydeH20 Setup Utility	
Advanced	
PET Progress	<Enabled>
WatchDog	<Disabled>
OS Timer	[0]
BIOS Timer	[0]
ASF Sensors Table	<Disabled>

PET Progress

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > PTT Configuration > ASF Configuration
Description	Enable/Disable PET Events Progress to receive PET Events
Default Value	<Enabled>

Watchdog

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > PTT Configuration > ASF Configuration
Description	Enable/Disable Watchdog
Default Value	<Disabled>

OS Timer

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > PTT Configuration > ASF Configuration
Description	Set the OS Timer for the Watchdog
Default Value	[0]

BIOS Timer

Type	Configurable
-------------	--------------

BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > PTT Configuration > ASF Configuration
Description	Set the BIOS Timer for the Watchdog
Default Value	[0]

ASF Sensors Table

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > PTT Configuration > ASF Configuration
Description	Display the ASF (Alert Sensor Format) Sensors Table
Default Value	<Disabled>

3.8.1.2 - Secure Erase Configuration

InsydeH20 Setup Utility	
Advanced	
Secure Erase mode	<Simulated>
Force Secure Erase	<Disabled>

Secure Erase mode

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > PTT Configuration > Secure Erase Configuration
Description	Define the secure erase mode - Either Simulated or Real
Default Value	<Simulated>

Force Secure Erase

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > PTT Configuration > Secure Erase Configuration
Description	Enable/Disable Force Secure Erase

Default Value	<Disabled>
----------------------	------------

3.8.1.3 - One Click Recovery(OCR) Configuration

InsydeH20 Setup Utility	
Advanced	
OCR Https Boot	<Enabled>
OCR PBA Boot	<Enabled>
OCR Windows Recovery Boot	<Enabled>
OCR Disable Secure Boot	<Enabled>

OCR Https Boot

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > PTT Configuration > One Click Recovery(OCR) Configuration
Description	Enable/Disable One Click Recovery Https Boot
Default Value	<Enabled>

OCR PBA Boot

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > PTT Configuration > One Click Recovery(OCR) Configuration
Description	Enable/Disable One Click Recovery PBA Boot
Default Value	<Enabled>

OCR Windows Recovery Boot

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > PTT Configuration > One Click Recovery(OCR) Configuration
Description	Enable/Disable One Click Recovery Windows Recovery Boot
Default Value	<Enabled>

OCR Disable Secure Boot

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > PTT Configuration > One Click Recovery(OCR) Configuration
Description	Enable/Disable One Click Recovery Windows Boot
Default Value	<Enabled>

3.8.2 - Firmware Update Configuration

InsydeH20 Setup Utility	
Advanced	
Me FW Image Re-Flash	<Disabled>
FW Update	<Enabled>

Me FW Image Re-Flash

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > PTT Configuration > Firmware Update Configuration
Description	Enable/Disable Me FW Image Re-Flash Function
Default Value	<Disabled>

FW Update

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > PTT Configuration > Firmware Update Configuration
Description	Enable/Disable Me FW Update
Default Value	<Enabled>

3.8.3 - PTT Configuration

InsydeH20 Setup Utility	
Advanced	
PTT Capability / State	N/A

PTT Configuration

Type	Information
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > PTT Configuration
Description	Displays the status of PTT

3.8.4 - FIPS Configuration

InsydeH20 Setup Utility	
Advanced	
FIPS Mode Select	<Disabled>
Current FIPS mode	Disabled
Crypto driver FIPS version	16.0.1545.15

FIPS Mode Select

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > FIPS Configuration
Description	FIPS Mode Configuration
Default Value	<Enabled>

Current FIPS mode

Type	Information
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > FIPS Configuration
Description	Displays the status of the current FIPS mode

Crypto driver FIPS version

Type	Information
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > FIPS Configuration
Description	Displays the Crypto driver FIPS version

3.8.5 - Unique Platform Id Configuration

InsydeH20 Setup Utility	
Advanced	
OEM Platform Id	N/A
CSME Platform Id	N/A
Upid State	<Disabled>
Upid OS Control State	<Enabled>

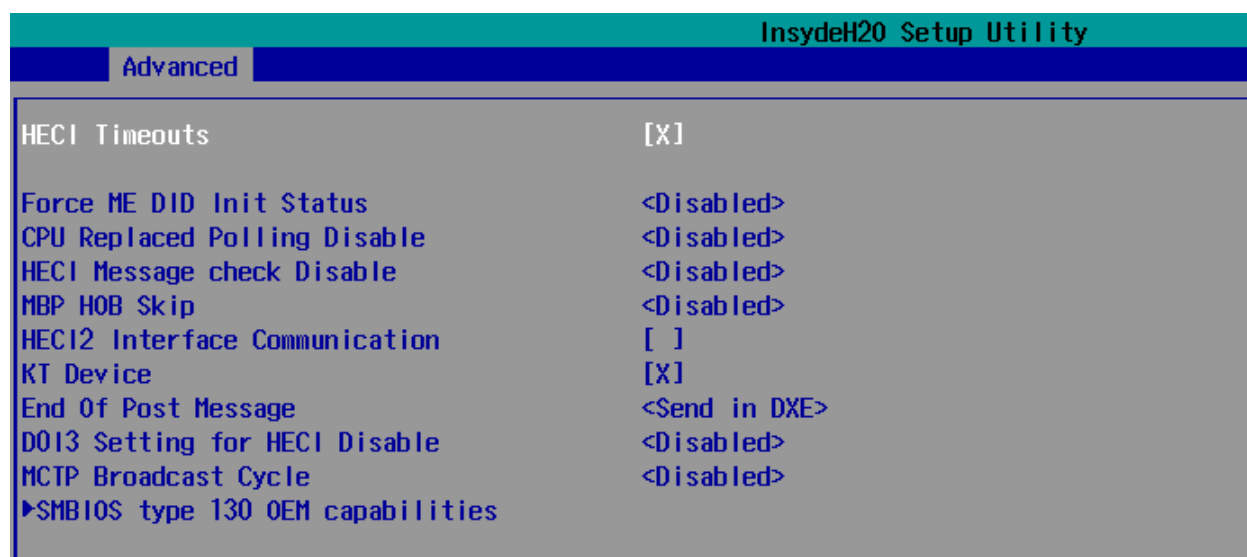
OEM Platform Id

Type	Information
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > Unique Platform Id Configuration
Description	Displays the OEM Platform ID

CSME Platform Id

Type	Information
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > Unique Platform Id Configuration
Description	Displays the OEM CSME Platform ID

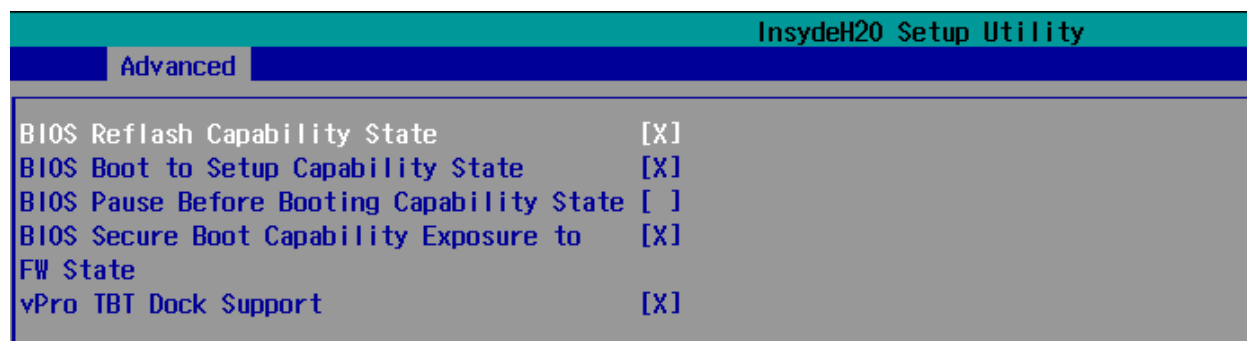
3.8.6 - ME Debug Configuration



HECI Timeouts

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > ME Debug Configuration
Description	Enable/Disable HECI Send/Receive Timeouts
Default Value	[X] (Enabled)

3.8.6.1 - SMBIOS type 130 OEM capabilities



BIOS Reflash Capability State

Type	Configurable
-------------	--------------

BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > ME Debug Configuration > SMBIOS type 130 OEM Capabilities
Description	Enable BIOS Reflash Capabilities
Default Value	[X] (Enabled)

BIOS Boot to Setup Capability State

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > ME Debug Configuration > SMBIOS type 130 OEM Capabilities
Description	Enable BIOS capabilities to boot to setup
Default Value	[X] (Enabled)

BIOS Pause Before Booting Capability State

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > ME Debug Configuration > SMBIOS type 130 OEM Capabilities
Description	Enable the BIOS to pause before booting to capability states
Default Value	[] (Disabled)

BIOS Secure Boot Capability Exposure to FW State

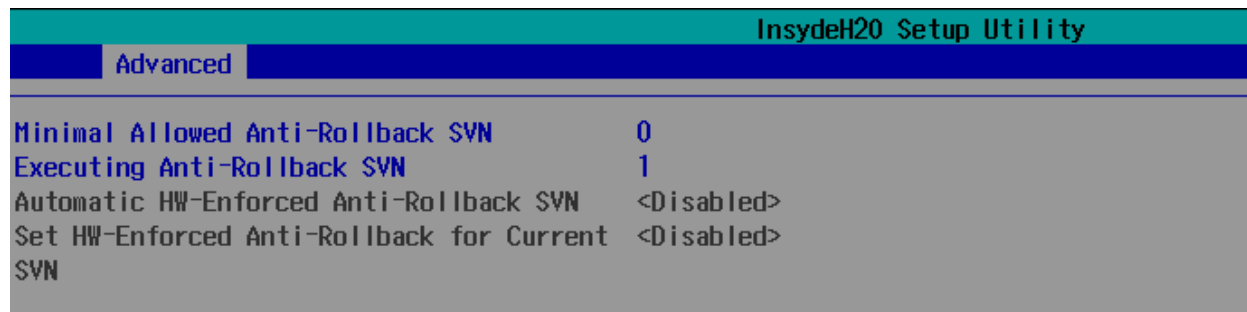
Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > ME Debug Configuration > SMBIOS type 130 OEM Capabilities
Description	Enable or Disabled BIOS Secure Boot Capability Exposure to FW State
Default Value	[X] (Enabled)

vPro TBT Dock Support

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > ME Debug Configuration > SMBIOS type 130 OEM Capabilities

Description	Enable or Disable vPro Support over a Thunderbolt Dock (K800 does not support Thunderbolt)
Default Value	[X] (Enabled)

3.8.7 - Anti-Rollback SVN Configuration



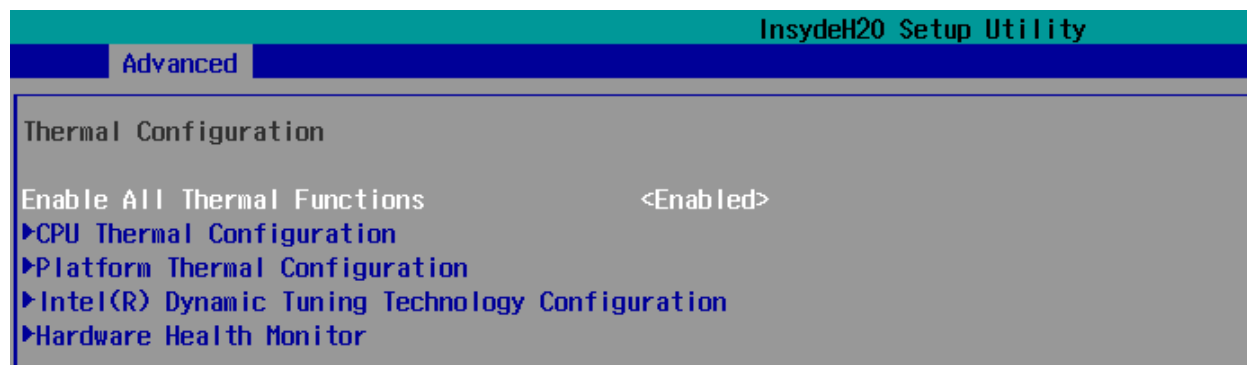
Minimal Allowed Anti-Rollback SVN

Type	Information
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > Anti-Rollback SVN Configuration
Description	Displays the minimum amount of allowed (SVN) Serial Version Number Anti-Rollbacks

Executing Anti-Rollback SVN

Type	Information
BIOS Page	Advanced Page > PCH-IO > PCH-FW Configuration > Anti-Rollback SVN Configuration
Description	Displays the amount of allowed (SVN) Serial Version Number Anti-Rollbacks

3.9 - Thermal Configuration



Enable All Thermal Functions

Type	Configurable
BIOS Page	Advanced Page > Thermal Configuration
Description	Enables or Disables thermal functions of the K800
Default Value	<Enabled>

CPU Thermal Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > Thermal Configuration
Description	Opens CPU Thermal Configuration Menu

Platform Thermal Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > Thermal Configuration
Description	Opens Platform Thermal Configuration Menu

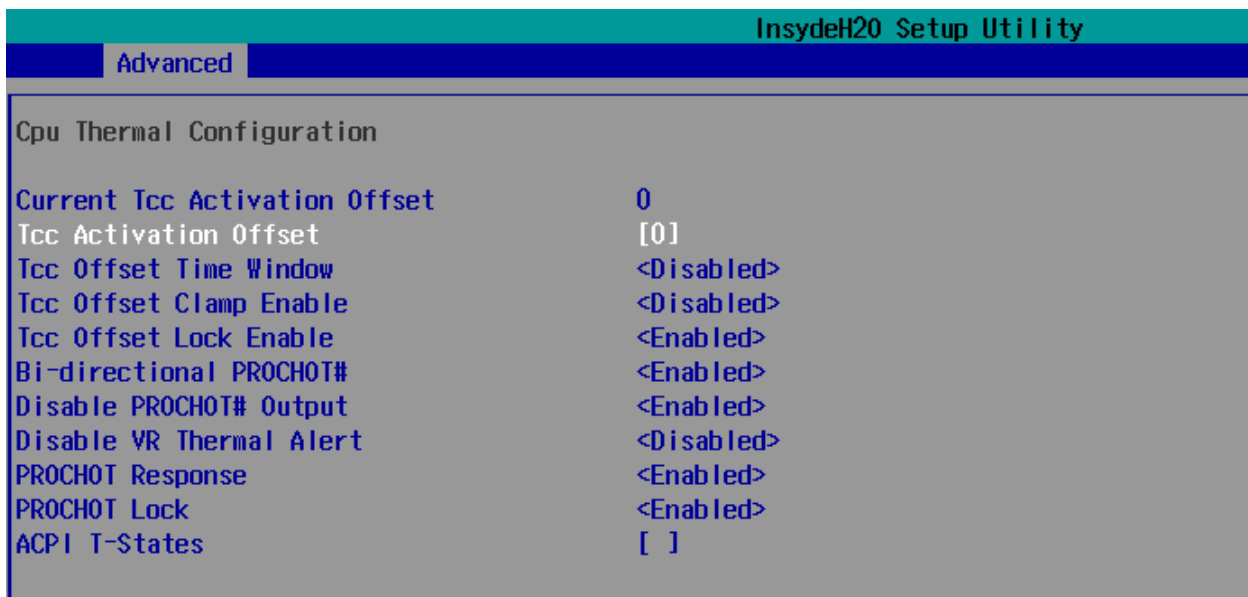
Intel(R) Dynamic Tuning Technology Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > Thermal Configuration
Description	Opens Intel(R) Dynamic Tuning Technology Configuration Menu

Hardware Health Monitor

Type	Sub-Menu
BIOS Page	Advanced Page > Thermal Configuration
Description	Opens Hardware Health Monitor Menu

3.9.1 - CPU Thermal Configuration



Current Tcc Activation Offset

Type	Information
BIOS Page	Advanced Page > Thermal Configuration > CPU Thermal Configuration
Description	Displays the current TCC Activation Offset

Tcc Activation Offset

Type	Configurable
BIOS Page	Advanced Page > Thermal Configuration > CPU Thermal Configuration
Description	Allows setting of Tcc Activation Offset

Default Value	[0]
----------------------	-----

Tcc Offset Time Window

Type	Configurable
BIOS Page	Advanced Page > Thermal Configuration > CPU Thermal Configuration
Description	Allows setting the time window for Tcc Offset
Default Value	<Disabled>

Tcc Offset Clamp Enable

Type	Configurable
BIOS Page	Advanced Page > Thermal Configuration > CPU Thermal Configuration
Description	Enables or Disables the Tcc Offset Clamp
Default Value	<Disabled>

Tcc Offset Lock Enable

Type	Configurable
BIOS Page	Advanced Page > Thermal Configuration > CPU Thermal Configuration
Description	Enables or Disables the Tcc Lock Clamp
Default Value	<Disabled>

Bi-directional PROCHOT#

Type	Configurable
BIOS Page	Advanced Page > Thermal Configuration > CPU Thermal Configuration
Description	Enables or Disables Bi-Directional PROCHOT#
Default Value	<Enabled>

Disable PROCHOT# Output

Type	Configurable
BIOS Page	Advanced Page > Thermal Configuration > CPU Thermal Configuration
Description	Enables or Disables the PROCHOT# output
Default Value	<Enabled>

Disable VR Thermal Alert

Type	Configurable
BIOS Page	Advanced Page > Thermal Configuration > CPU Thermal Configuration
Description	Enables or Disables the VR Thermal Alert
Default Value	<Enabled>

PROCHOT Response

Type	Configurable
BIOS Page	Advanced Page > Thermal Configuration > CPU Thermal Configuration
Description	Enables or Disables the PROCHOT Response
Default Value	<Enabled>

PROCHOT Lock

Type	Configurable
BIOS Page	Advanced Page > Thermal Configuration > CPU Thermal Configuration
Description	Enables or Disables the PROCHOT Lock
Default Value	<Enabled>

ACPI T States

Type	Configurable
BIOS Page	Advanced Page > Thermal Configuration > CPU Thermal Configuration

Description	Enables or Disables the ACPI T-States
Default Value	[] (Disabled)

3.9.2 - Platform Thermal Configuration

InsydeH20 Setup Utility	
Advanced	
Platform Thermal Configuration	
Critical Trip Point	<119 C (POR)>
Active Trip Point 0	<71 C>
Active Trip Point 0 Fan Speed	[100]
Active Trip Point 1	<55 C>
Active Trip Point 1 Fan Speed	[75]
Passive Trip Point	<95 C>
Passive TC1 Value	[1]
Passive TC2 Value	[5]
Passive TSP Value	[10]
Active Trip Points	<Enabled>
Passive Trip Points	<Disabled>
Critical Trip Points	<Enabled>
PCH Temp Read	[X]
CPU Energy Read	[X]
CPU Temp Read	[X]
Alert Enable Lock	<Disabled>
CPU Temp	[72]
CPU Fan Speed	[65]

Critical Trip Point

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Platform Thermal Configuration
Description	This value controls the temperature of the ACPI Critical Trip Point - the point in which the OS will shut the system off.
Possible Values	<15 C> <23 C> <31 C>

	<39 C> <47 C> <55 C> <63 C> <71 C> <79 C> <87 C> <95 C> <100 C> <111 C> <119 C (POR)> <127 C> <130 C>
Default Value	<119 C (POR)>

Active Trip Point 0

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Platform Thermal Configuration
Description	This value controls the temperature of the ACPI Active Trip Point 0 - the point in which the OS will turn the processor fan on Active Trip Point 0 Fan Speed
Possible Values	<Disabled> <15 C> <23 C> <31 C> <39 C> <47 C> <55 C> <63 C> <71 C> <79 C> <87 C> <95 C> <100 C> <111 C> <119 C (POR)>
Default Value	<71 C>

Active Trip Point 0 Fan Speed

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Platform Thermal Configuration
Description	Active Trip Point 0 Fan Speed in percentage. Value must be between 0 (Fan off) - 100 (Max fan speed). This is the speed at which the fan will run when the Active Trip Point 0 threshold is met
Possible Values	Any value between 0 and 100
Default Value	<100>

Active Trip Point 1

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Platform Thermal Configuration
Description	This value controls the temperature of the ACPI Active Trip Point 0 - the point in which the OS will turn the processor fan on Active Trip Point 1 Fan Speed
Possible Values	<Disabled> <15 C> <23 C> <31 C> <39 C> <47 C> <55 C> <63 C> <71 C> <79 C> <87 C> <95 C> <100 C> <111 C> <119 C (POR)>
Default Value	<55 C>

Active Trip Point 1 Fan Speed

Type	Configurable
-------------	--------------

BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Platform Thermal Configuration
Description	Active Trip Point 0 Fan Speed in percentage. Value must be between 0 (Fan off) - 100 (Max fan speed). This is the speed at which the fan will run when the Active Trip Point 1 threshold is met
Possible Values	Any value between 0 and 100
Default Value	<75>

Passive Trip Point

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Platform Thermal Configuration
Description	This value controls the temperature of the ACPI Passive Trip Point -the point in which the OS will begin throttling the processor
	<Disabled> <15 C> <23 C> <31 C> <39 C> <47 C> <55 C> <63 C> <71 C> <79 C> <87 C> <95 C> <100 C> <111 C> <119 C (POR)>
Default Value	<95 C>

Passive TC1 Value

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Platform Thermal Configuration

Description	This value sets the TC1 value for the ACPI Passive Cooling Formula. Range 1-16
Default Value	[1]

Passive TC2 Value

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Platform Thermal Configuration
Description	This value sets the TC2 value for the ACPI Passive Cooling Formula. Range 1-16
Default Value	[5]

Passive TSP Value

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Platform Thermal Configuration
Description	This item sets the TSP value for the ACPI Passive Cooling Formula. It represents in tenths of a second how often the OS will read the temperature when passive cooling is enabled. Range 2-32
Default Value	[10]

Active Trip Points

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Platform Thermal Configuration
Description	Enables or Disables the Active Trip Points
Default Value	<Enabled>

Passive Trip Points

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Platform Thermal Configuration

Description	Enables or Disables the Passive Trip Points
Default Value	<Disabled>

Critical Trip Points

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Platform Thermal Configuration
Description	Enables or Disables the Passive Trip Points
Default Value	<Enabled>

PCH Temp Read

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Platform Thermal Configuration
Description	Enables or Disables temperature reading of the PCH
Default Value	[X] (Enabled)

CPU Energy Read

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Platform Thermal Configuration
Description	Enables or Disables CPU Energy Read
Default Value	[X] (Enabled)

CPU Temp Read

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Platform Thermal Configuration
Description	Enables or Disables temperature reading of the CPU
Default Value	[X] (Enabled)

Alert Enable Lock

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Platform Thermal Configuration
Description	Enables or Disables the Alert Enable Lock
Default Value	<Disabled>

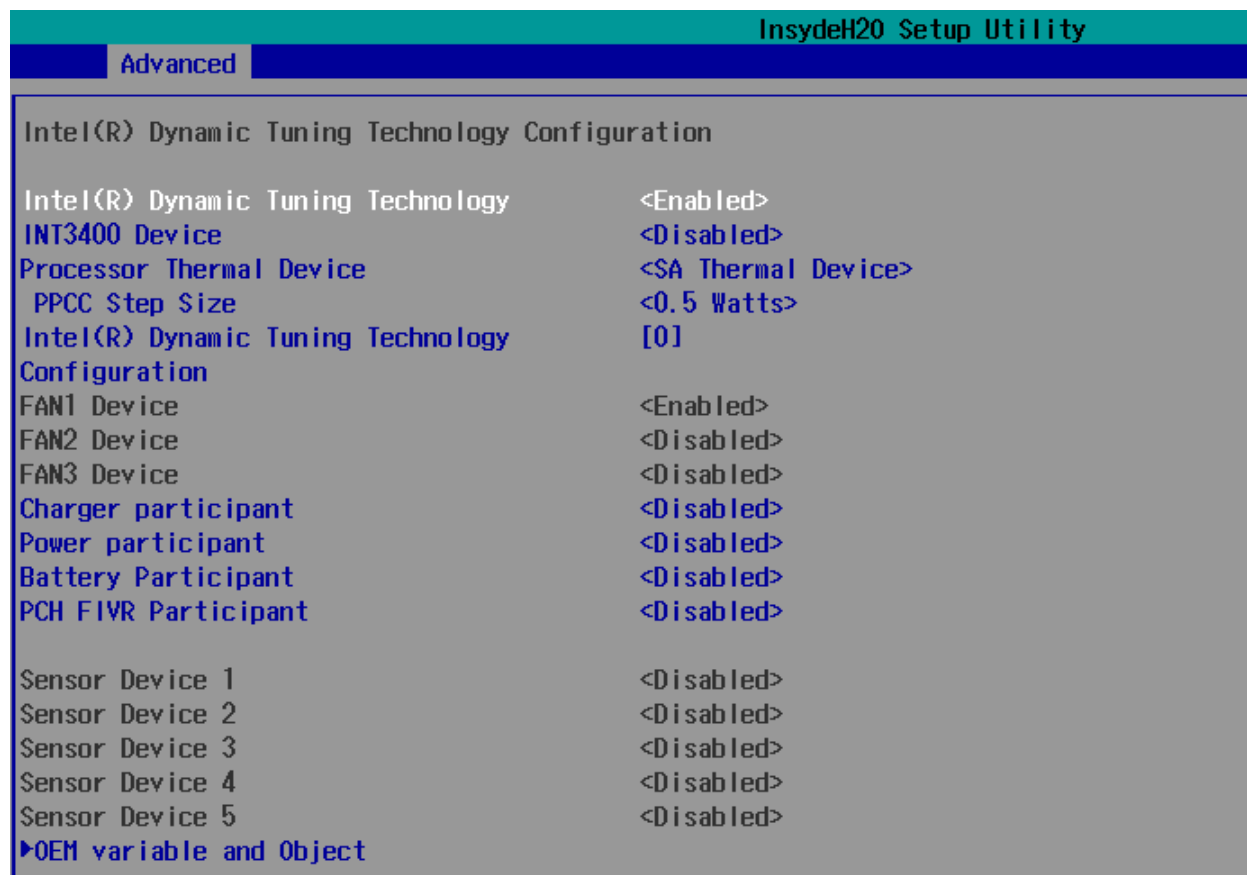
CPU Temp

Type	Information
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Platform Thermal Configuration
Description	Displays the current CPU Temperature

CPU Fan Speed

Type	Information
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Platform Thermal Configuration
Description	Displays the current CPU Fan Duty Cycle

3.9.3 - Intel(R) Dynamic Tuning Technology Configuration



Intel(R) Dynamic Tuning Technology

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Intel(R) Dynamic Tuning Technology Configuration
Description	Enables or Disables Intel(R) DTT
Default Value	<Enabled>

INT3400 Device

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Intel(R) Dynamic Tuning Technology Configuration
Description	Enables or Disables Intel3400 device

Default Value	<Disabled>
----------------------	------------

Processor Thermal Device

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Intel(R) Dynamic Tuning Technology Configuration
Description	Enable or Disable Processor Thermal Device
Possible Values	<Disabled> <SA Thermal Device>
Default Value	<SA Thermal Device>

PPCC Step Size

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Intel(R) Dynamic Tuning Technology Configuration
Description	Sets the PPCC Step Size (Step size for Turbo power limit (RAPL) control)
	<0.5 Watts> <1.0 Watts> <1.5 Watts> <2.0 Watts>
Default Value	<0.5 Watts>

Intel(R) Dynamic Tuning Technology Configuration

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Intel(R) Dynamic Tuning Technology Configuration
Description	Allows you to select the configuration of Intel(R) DTT
Default Value	[0]

FAN1 Device

Type	Information
-------------	-------------

BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Intel(R) Dynamic Tuning Technology Configuration
Description	Status of FAN1 device

FAN2 Device

Type	Information
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Intel(R) Dynamic Tuning Technology Configuration
Description	Status of FAN2 device

FAN3 Device

Type	Information
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Intel(R) Dynamic Tuning Technology Configuration
Description	Status of FAN3 device

Charger Participant

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Intel(R) Dynamic Tuning Technology Configuration
Description	Enable or disable charger participant (Not available on K800 series)
Default Value	<Disabled>

Power Participant

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Intel(R) Dynamic Tuning Technology Configuration
Description	Enable or disable Power participant (Not available on K800 series)
Default Value	<Disabled>

Battery Participant

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Intel(R) Dynamic Tuning Technology Configuration
Description	Enable or disable Battery participant (Not available on K800 series)
Default Value	<Disabled>

PCH FIVR Participant

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Intel(R) Dynamic Tuning Technology Configuration
Description	Enable or disable PCH FIVR participant (Not available on K800 series)
Default Value	<Disabled>

Sensor Device 1

Type	Information
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Intel(R) Dynamic Tuning Technology Configuration
Description	Enable or disable Sensor Device 1 (Not available on K800 series)
Default Value	<Disabled>

Sensor Device 2

Type	Information
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Intel(R) Dynamic Tuning Technology Configuration
Description	Enable or disable Sensor Device 2 (Not available on K800 series)
Default Value	<Disabled>

Sensor Device 3

Type	Information
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Intel(R) Dynamic Tuning Technology Configuration
Description	Enable or disable Sensor Device 3 (Not available on K800 series)
Default Value	<Disabled>

Sensor Device 4

Type	Information
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Intel(R) Dynamic Tuning Technology Configuration
Description	Enable or disable Sensor Device 4 (Not available on K800 series)
Default Value	<Disabled>

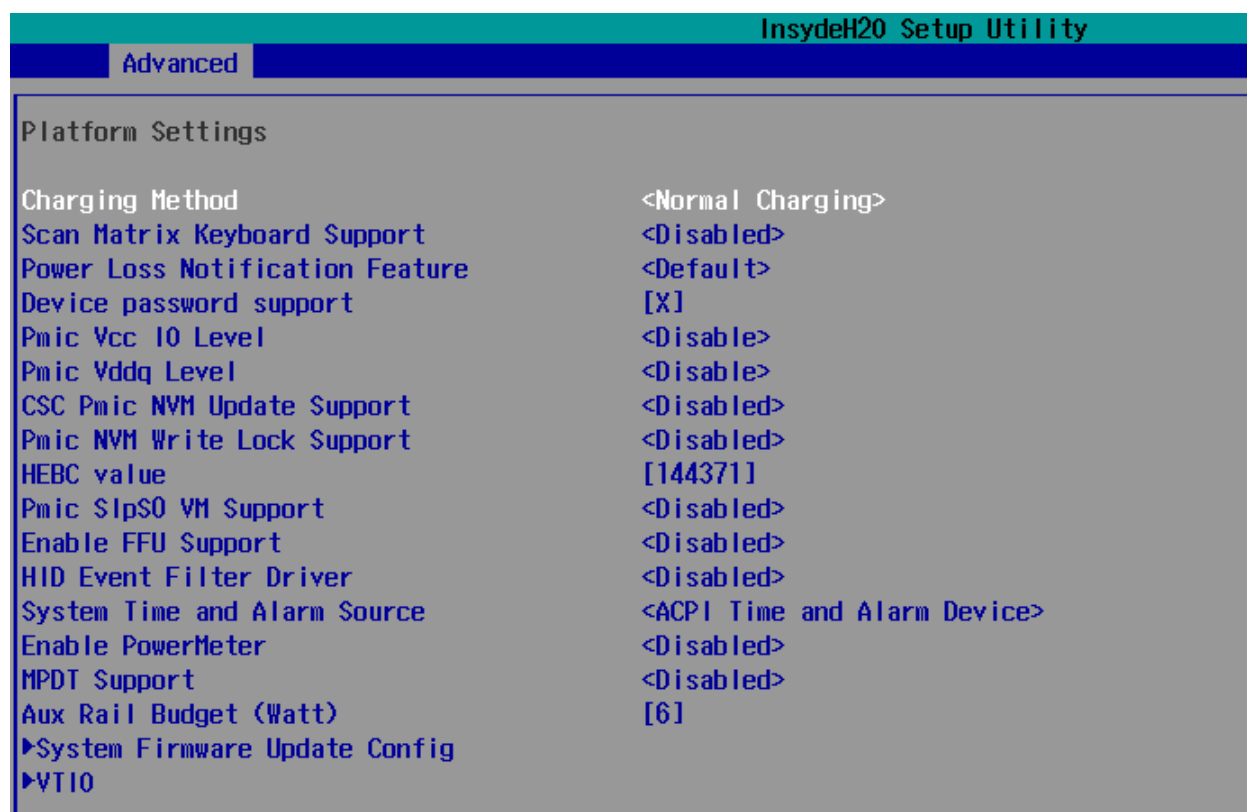
Sensor Device 5

Type	Information
BIOS Page	Advanced Page > PCH-IO > Thermal Configuration > Intel(R) Dynamic Tuning Technology Configuration
Description	Enable or disable Sensor Device 5 (Not available on K800 series)
Default Value	<Disabled>

3.9.4 - Hardware Health Monitor

Needs to be removed in future revision or link to the one that works

3.10 - Platform Settings



Charging Method

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Platform Settings
Description	Define the charging method (Not available on K800 Series)
Default Value	<Normal Charging>

Scan Matrix Keyboard Support

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Platform Settings
Description	Enable or Disable Scan Matrix Keyboard Support

Default Value	<Disabled>
----------------------	------------

Power Loss Notification Feature

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Platform Settings
Description	Define the Power Loss Notification Feature
Default Value	<Default>

Device password support

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Platform Settings
Description	Enable or disable device password support
Default Value	[X] (Enabled)

Pmic Vcc IO Level

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Platform Settings
Description	Define the PMIC VCC IO Level (K800 does not use a PMIC)
Default Value	<Disabled>

Pmic Vddq Level

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Platform Settings
Description	Define the PMIC VDDQ Level (K800 does not use a PMIC)
Default Value	<Disabled>

CSC Pmic NVM Update Support

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Platform Settings

Description	Ability to update PMIC NVM (K800 does not use a PMIC)
Default Value	<Disabled>

Pmic NVM Write Lock Support

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Platform Settings
Description	Ability to update PMIC NVM (K800 does not use a PMIC)
Default Value	<Disabled>

Enable FFU Support

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Platform Settings
Description	Enable FFU Support
Default Value	<Disabled>

HID Event Filter Driver

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Platform Settings
Description	Enables the HID Event Filter Driver
Default Value	<Disabled>

System Time and Alarm Source

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Platform Settings
Description	Defines the System Time and Alarm Source
Default Value	<ACPI Time and Alarm Device>

Enable PowerMeter

Type	Configurable
-------------	--------------

BIOS Page	Advanced Page > PCH-IO > Platform Settings
Description	Enables or disables PowerMeter
Default Value	<Disabled>

Aux Rail Budget (Watt)

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Platform Settings
Description	Defines the power budget for the VCCAUX power rail. Setting this to any lower than 6 may lead to abnormal system behavior
Default Value	[6]

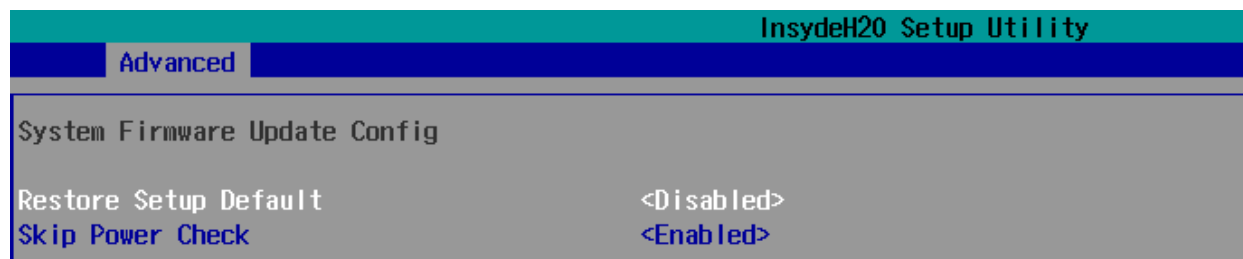
System Firmware Update Config

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO > Platform Settings
Description	Opens System Firmware Update Config Menu

VTIO

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO > Platform Settings
Description	Opens the VTIO Menu

3.10.1 - System Firmware Update Config



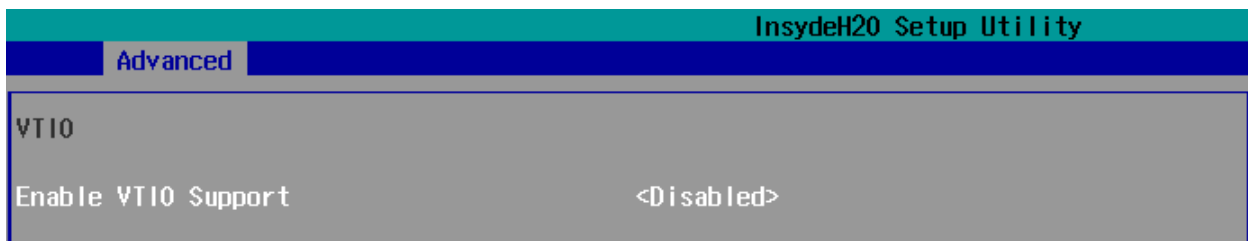
Restore Setup Default

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Platform Settings > System Firmware Update Config
Description	When enabled resets the systems BIOS settings
Default Value	<Disabled>

Skip Power Check

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Platform Settings > System Firmware Update Config
Description	Skips the power check during POST
Default Value	<Enabled>

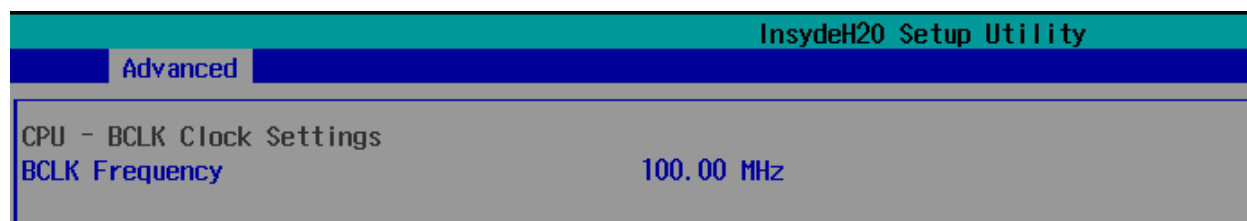
3.10.2 - VTIO



Enable VTIO Support

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > Platform Settings > VTIO
Description	Enables VTIO Support
Default Value	<Disabled>

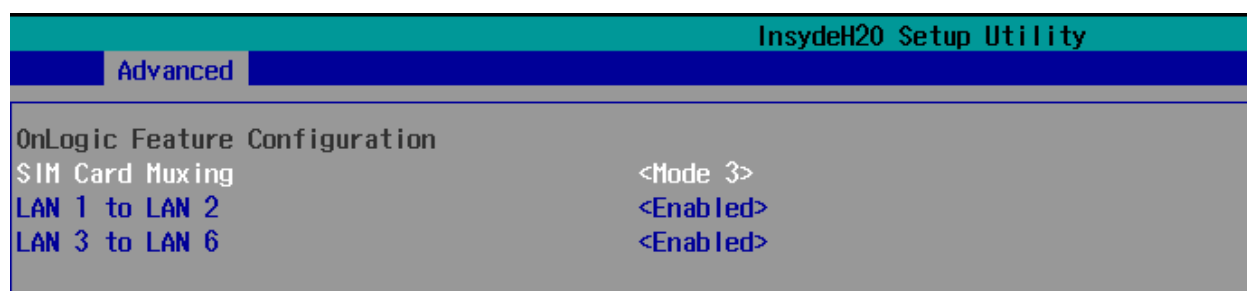
3.11 - CPU - BCLK Clock Settings



BCLK Frequency

Type	Information
BIOS Page	Advanced Page > CPU - BCLK Clock Settings
Description	Displays the BCLK frequency of the system

3.12 - OnLogic Feature Configuration



SIM Card Muxing

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > OnLogic Feature Configuration
Description	Enables VTIO Support
Possible Values	<Mode 1> - UIM1 to mPCIe, UIM2 to B-Key <Mode 2> - UIM1 to B-Key, UIM2 to mPCIe <Mode 3> - UIM1 & UIM2 to B-Key
Default Value	<Mode 3>

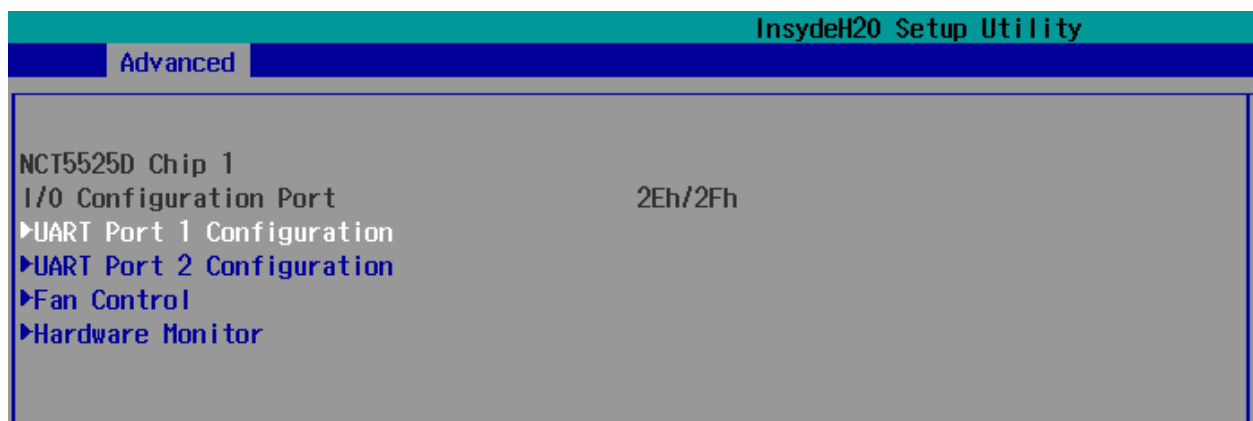
LAN 1 to LAN 2

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > OnLogic Feature Configuration
Description	Enables LAN 1 and LAN 2
Default Value	<Enabled>

LAN 3 to LAN 6

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > OnLogic Feature Configuration
Description	Enables LAN 3, LAN 4, LAN 5, and LAN 6
Default Value	<Enabled>

3.13 - SIO NCT5525D



I/O Configuration Port

Type	Information
BIOS Page	Advanced Page > SIO NCT5525D
Description	Displays memory location of the SIO

UART Port 1 Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > SIO NCT5525D
Description	Opens the configuration menu for UART Port 1

UART Port 2 Configuration

Type	Sub-Menu
BIOS Page	Advanced Page > SIO NCT5525D
Description	Opens the configuration menu for UART Port 2

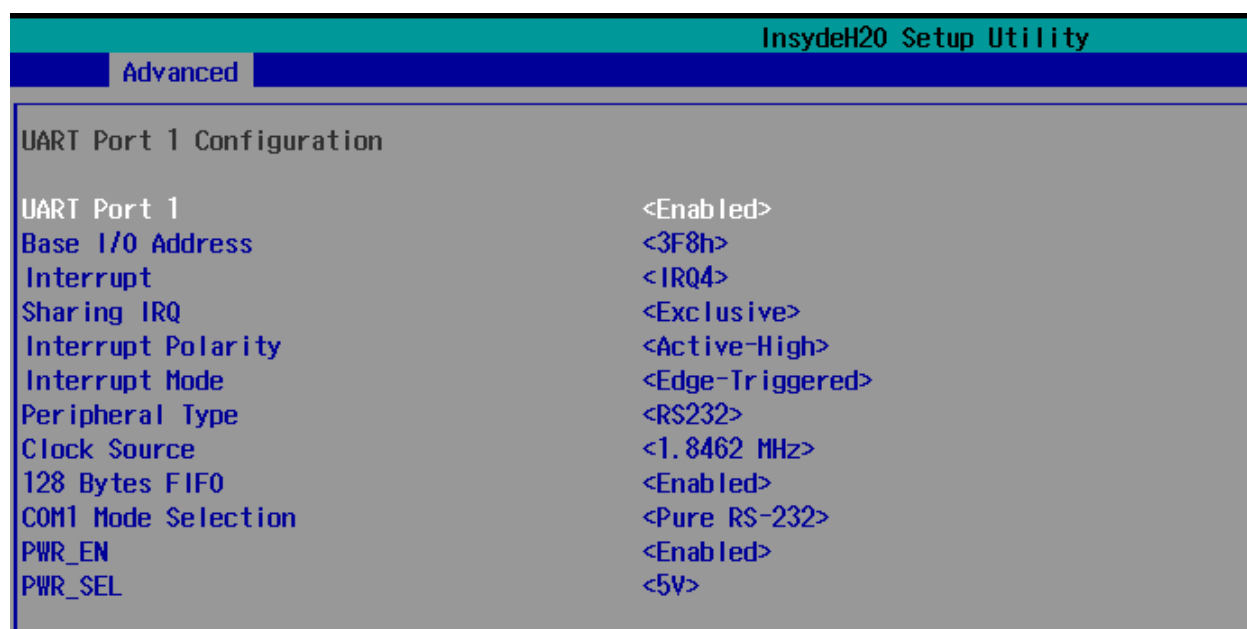
Fan Control

Type	Sub-Menu
BIOS Page	Advanced Page > SIO NCT5525D
Description	Opens the Fan Control Menu

Hardware Monitor

Type	Sub-Menu
BIOS Page	Advanced Page > SIO NCT5525D
Description	Opens the Hardware Monitor Menu

3.13.1 - UART Port 1 Configuration



UART Port 1

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > UART Port 1 Configuration
Description	Enables or disables UART Port 1
Default Value	<Enabled>

Base I/O Address

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > UART Port 1 Configuration
Description	Defines the Base I/O Address for UART Port 1

Possible Values	<3F8h> <2F8h> <3E8h> <2E8h> <338h> <228h> <220h> <238h>
Default Value	<38Fh>

Interrupt

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > UART Port 1 Configuration
Description	Defines the Interrupt for UART Port 1
Possible Values	<IRQ3> <IRQ4> <IRQ5> <IRQ6> <IRQ7> <IRQ10> <IRQ11>
Default Value	<IRQ4>

Sharing IRQ

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > UART Port 1 Configuration
Description	Defines IRQ Exclusivity for UART Port 1
Possible Values	<Shared> <Exclusive>
Default Value	<Exclusive>

Interrupt Polarity

Type	Configurable
-------------	--------------

BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > UART Port 1 Configuration
Description	Defines the Interrupt Polarity for UART Port 1
Possible Values	<Active-High> <Active-Low>
Default Value	<Active-High>

Interrupt Mode

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > UART Port 1 Configuration
Description	Defines the Interrupt Mode for UART Port 1
Possible Values	<Level-Triggered> <Edge-Triggered>
Default Value	<Edge-Triggered>

Peripheral Type

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > UART Port 1 Configuration
Description	Defines the Peripheral Type for UART Port 1
Possible Values	<RS232> <RS485>
Default Value	<RS232>

Clock Source

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > UART Port 1 Configuration
Description	Defines the frequency of the clock source
Possible Values	<1.8462 MHz> <2 MHz>

	<24 MHz> <14.769 MHz>
Default Value	<1.8462 MHz>

128 Bytes FIFO

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > UART Port 1 Configuration
Description	Enables or Disable 128 Byte FIFO
Default Value	<Enabled>

COM1 Mode Selection

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > UART Port 1 Configuration
Description	Defines the mode the transceiver for COM1 will transmit in
Possible Values	<Low Power Shutdown> <Pure RS-232> <RS-485 Half Duplex (TX ENABLE Low Active)> <RS-485 Half Duplex (TX ENABLE High Active)> <RS-485 Half Duplex (Terminated)> <RS-422 Full Duplex> <Pure RS-232 (co-exists with RS485)> <RS-422 Full Duplex (Terminated)>
Default Value	<Pure RS-232>

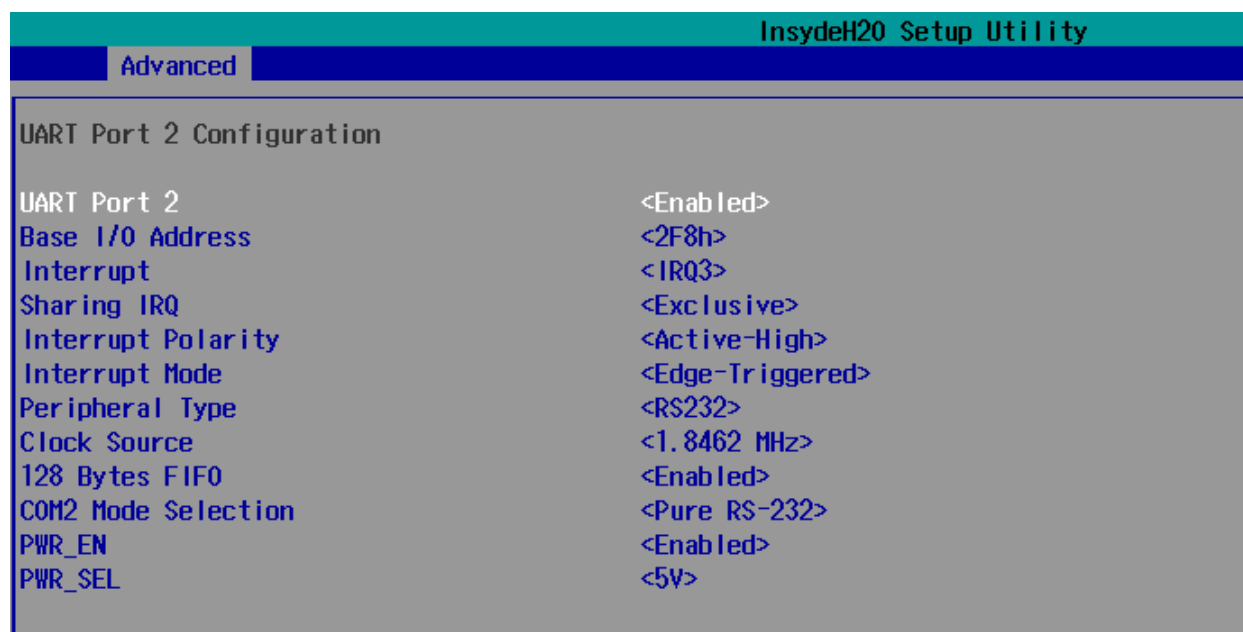
PWR_EN

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > UART Port 1 Configuration
Description	Enable the power output on Pin 9 Ring Indicator
Default Value	<Enabled>

PWR_SEL

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > UART Port 1 Configuration
Description	Defines the Voltage on Pin 9 Ring Indicator
Possible Values	<5V> <12V>
Default Value	<5V>

3.13.2 - UART Port 2 Configuration



UART Port 2

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > UART Port 2 Configuration
Description	Enables or disables UART Port 2
Default Value	<Enabled>

Base I/O Address

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > UART Port 2 Configuration
Description	Defines the Base I/O Address for UART Port 2
Possible Values	<3F8h> <2F8h> <3E8h> <2E8h> <338h> <228h> <220h> <238h>
Default Value	<28FH>

Interrupt

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > UART Port 2 Configuration
Description	Defines the Interrupt for UART Port 2
Possible Values	<IRQ3> <IRQ4> <IRQ5> <IRQ6> <IRQ7> <IRQ10> <IRQ11>
Default Value	<IRQ3>

Sharing IRQ

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > UART Port 2 Configuration
Description	Defines IRQ Exclusivity for UART Port 2

Possible Values	<Shared> <Exclusive>
Default Value	<Exclusive>

Interrupt Polarity

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > UART Port 2 Configuration
Description	Defines the Interrupt Polarity for UART Port 2
Possible Values	<Active-High> <Active-Low>
Default Value	<Active-High>

Interrupt Mode

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > UART Port 2 Configuration
Description	Defines the Interrupt Mode for UART Port 2
Possible Values	<Level-Triggered> <Edge-Triggered>
Default Value	<Edge-Triggered>

Peripheral Type

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > UART Port 2 Configuration
Description	Defines the Peripheral Type for UART Port 2
Possible Values	<RS232> <RS485>
Default Value	<RS232>

Clock Source

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > UART Port 2 Configuration
Description	Defines the frequency of the clock source
Possible Values	<1.8462 MHz> <2 MHz> <24 MHz> <14.769 MHz>
Default Value	<1.8462 MHz>

128 Bytes FIFO

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > UART Port 2 Configuration
Description	Enables or Disable 128 Byte FIFO
Default Value	<Enabled>

COM1 Mode Selection

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > UART Port 2 Configuration
Description	Defines the mode the transceiver for COM1 will transmit in
Possible Values	<Low Power Shutdown> <Pure RS-232> <RS-485 Half Duplex (TX ENABLE Low Active)> <RS-485 Half Duplex (TX ENABLE High Active)> <RS-485 Half Duplex (Terminated)> <RS-422 Full Duplex> <Pure RS-232 (co-exists with RS485)> <RS-422 Full Duplex (Terminated)>
Default Value	<Pure RS-232>

PWR_EN

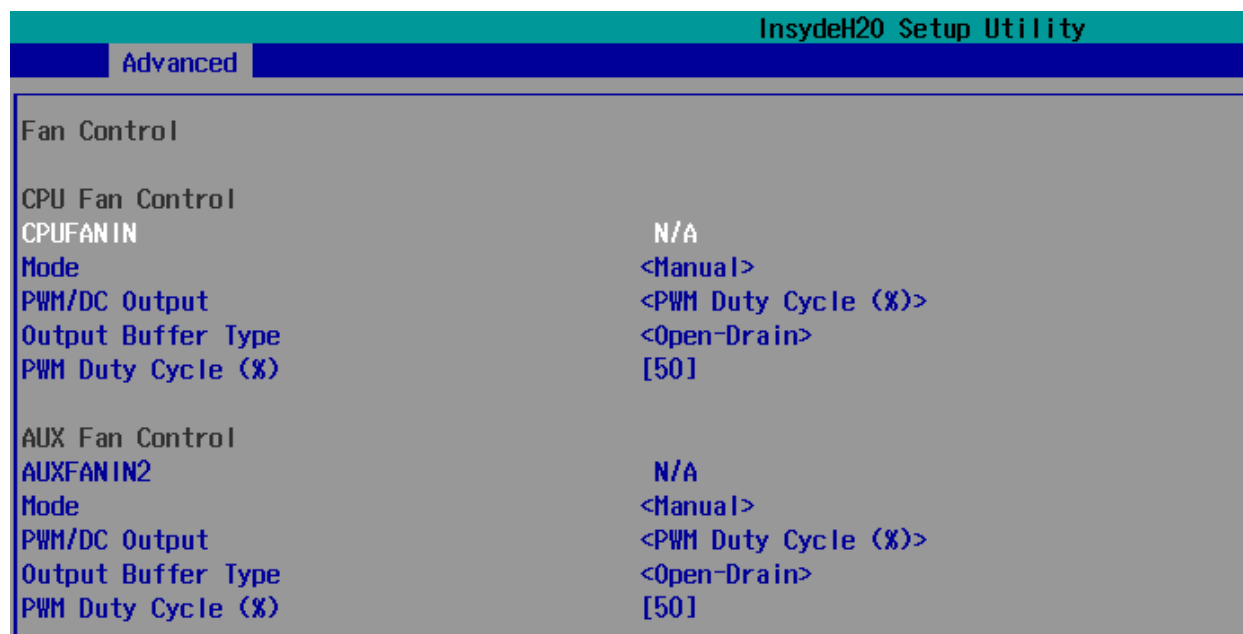
Type	Configurable
-------------	--------------

BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > UART Port 2 Configuration
Description	Enable the power output on Pin 9 Ring Indicator
Default Value	<Enabled>

PWR_SEL

Type	Configurable
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > UART Port 2 Configuration
Description	Defines the Voltage on Pin 9 Ring Indicator
Possible Values	<5V> <12V>
Default Value	<5V>

3.13.3 - Fan Control



CPUFANIN

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > Fan Control
Description	Displays the status of CPUFANIN (The external fan on the K800)

Mode

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > Fan Control
Description	Defines the Mode the Fan can operate
Possible Values	<Manual> <Thermal Cruise> <Speed Cruise> <Smart Fan IV>
Default Value	<Manual>

PWM/DC Output

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > Fan Control
Description	Sets the fan in PWM or DC mode
Possible Values	<PWM Duty Cycle (%)> <DC Voltage (%)>
Default Value	<PWM Duty Cycle (%)>

Output Buffer Type

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > Fan Control
Description	Sets the output buffer type
Possible Values	<Open-Drain> <Push-Pull>
Default Value	<Open-Drain>

PWM Duty Cycle (%)

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > Fan Control
Description	Sets the Duty Cycle for the external fan header on the K800
Possible Values	Any value between 0 and 100
Default Value	50

AUXFANIN2

Type	Sub-Menu
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > Fan Control
Description	Displays the status of AUXFANIN2 (Fan control on Riser cards featured on K803 and K804)

Mode

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > Fan Control
Description	Defines the Mode the Fan can operate (Fan control on Riser cards featured on K803 and K804)
Possible Values	<Manual> <Thermal Cruise> <Speed Cruise> <Smart Fan IV>
Default Value	<Manual>

PWM/DC Output

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > Fan Control
Description	Sets the fan in PWM or DC mode (Fan control on Riser cards featured on K803 and K804)
Possible Values	<PWM Duty Cycle (%)> <DC Voltage (%)>

Default Value	<PWM Duty Cycle (%)>
----------------------	----------------------

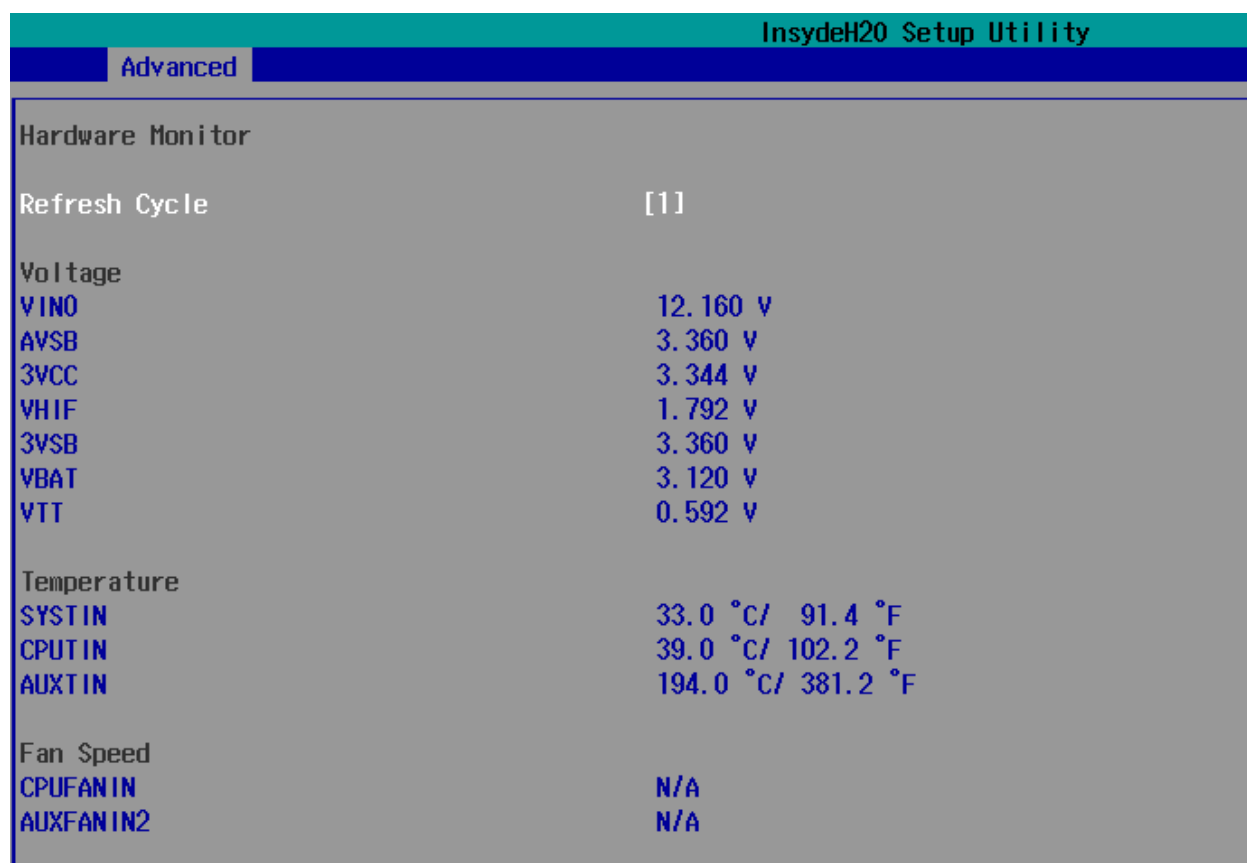
Output Buffer Type

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > Fan Control
Description	Sets the output buffer type (Fan control on Riser cards featured on K803 and K804)
Possible Values	<Open-Drain> <Push-Pull>
Default Value	<Open-Drain>

PWM Duty Cycle (%)

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > Fan Control
Description	Sets the Duty Cycle for the fan control on Riser cards featured on K803 and K804
Possible Values	Any value between 0 and 100
Default Value	<Open-Drain>

3.13.4 - Hardware Monitor



Refresh Cycle

Type	Configurable Setting
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > Hardware Monitor
Description	Sets the refresh rate for sensors to be updated
Default Value	[1]

VINO

Type	Information
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > Hardware Monitor

Description	Displays the measured Voltage on the 12V rail
--------------------	---

AVSB

Type	Information
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > Hardware Monitor
Description	Displays the measured Voltage on the 3.3V auxiliary Standby rail

3VCC

Type	Information
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > Hardware Monitor
Description	Displays the measured Voltage on the 3.3V rail

VHIF

Type	Information
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > Hardware Monitor
Description	Displays the measured Voltage on the 1.8V rail

3VSB

Type	Information
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > Hardware Monitor
Description	Displays the measured Voltage on the 3.3V standby rail

VBAT

Type	Information
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > Hardware Monitor
Description	Displays the measured Voltage on the CMOS battery

VTT

Type	Information
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > Hardware Monitor
Description	Displays the measured Voltage on the VTT Power Rail

SYSTIN

Type	Information
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > Hardware Monitor
Description	Displays the measured temperature on the chipset

CPUTIN

Type	Information
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > Hardware Monitor
Description	Displays the measured temperature on the CPU

AUXTIN

Type	Information
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > Hardware Monitor
Description	Reserved for future thermal sensing

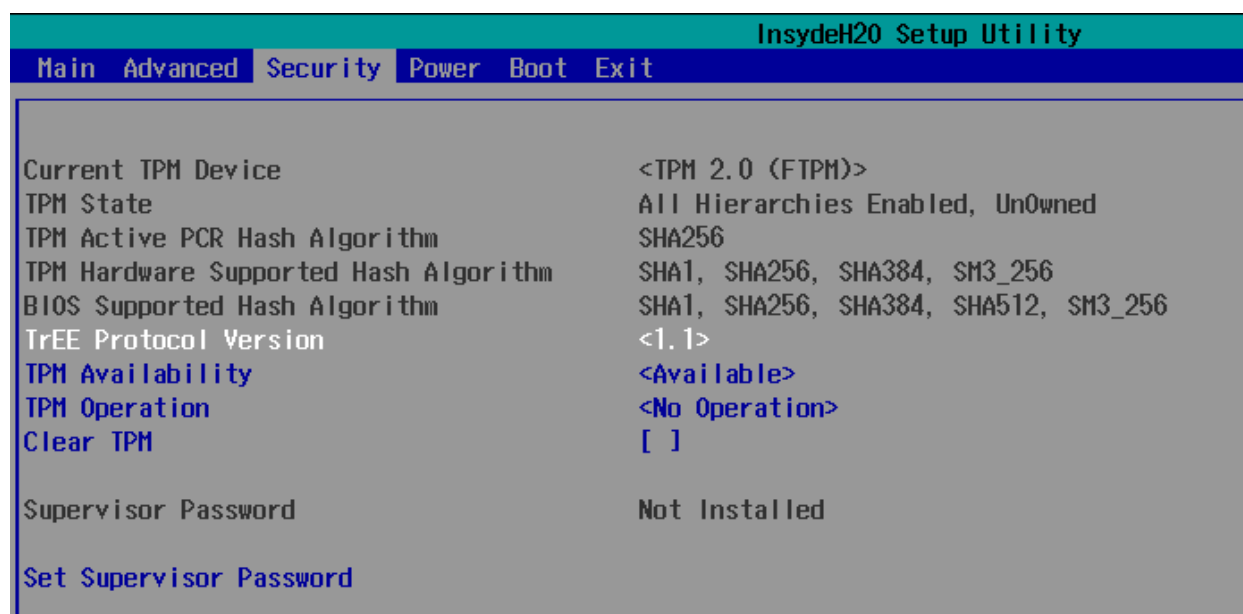
CPUFANIN

Type	Information
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > Hardware Monitor
Description	Displays the CPU Fan Speed (Located on the I/O of the K800)

AUXFANIN2

Type	Information
BIOS Page	Advanced Page > PCH-IO > SIO NCT5525D > Hardware Monitor
Description	Displays the Fan Speed on the risers for K803 and K804

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 - SetPPRequiredForChangePCRs_True - SetPPRequiredForChangeEPS_False - SetPPRequiredForChangeEPS_True - ChangeEPS
Default Value	No Operation

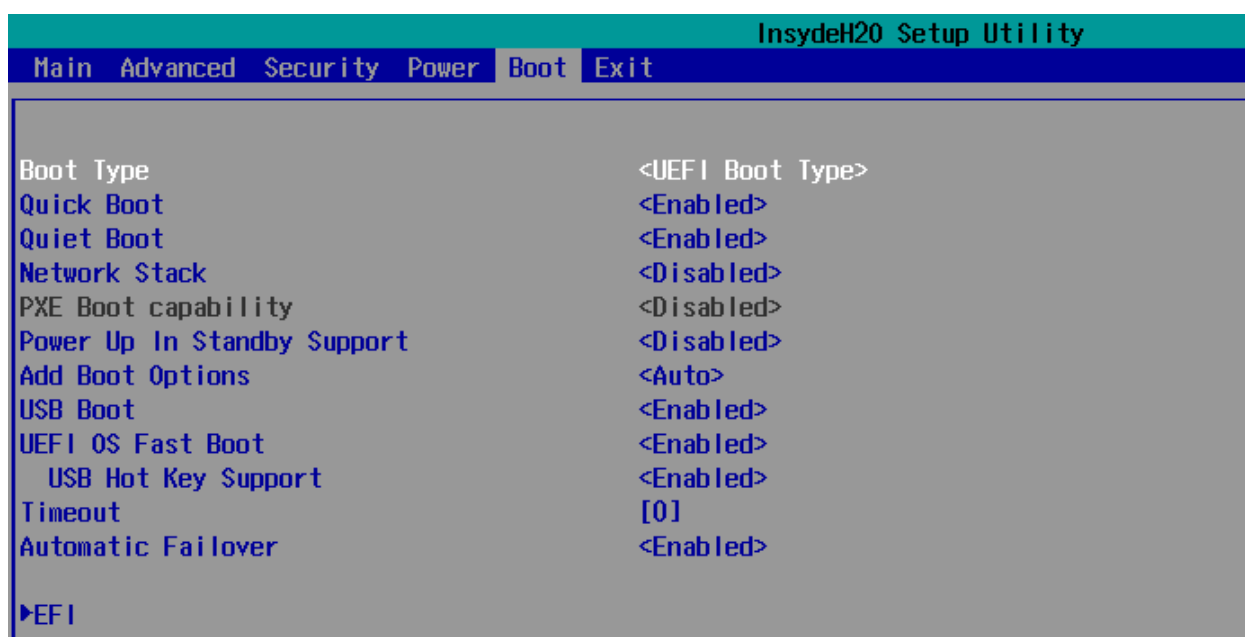
Clear TPM

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>

Quick Boot

Type	Configurable Setting
-------------	----------------------

BIOS Page	Boot Page
Description	Enables or Disables Quick Boot
Default Value	<Enabled>

Quiet Boot

Type	Configurable Setting
BIOS Page	Boot Page
Description	Enables or Disables Quiet Boot
Default Value	<Enabled>

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>

USB Hot Key Support

Type	Configurable Setting
BIOS Page	Boot Page
Description	Enables or Disables USB Hot Key Support

Default Value	<Enabled>
----------------------	-----------

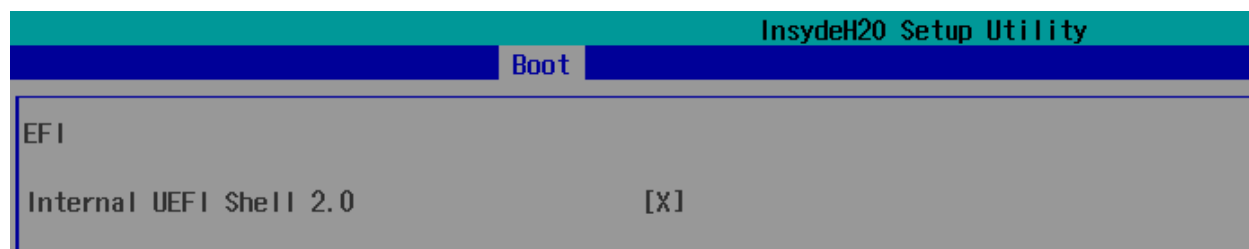
Timeout

Type	Configurable Setting
BIOS Page	Boot Page
Description	The number of seconds that the firmware will wait before booting the original default boot selection
Default Value	[0]

EFI

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

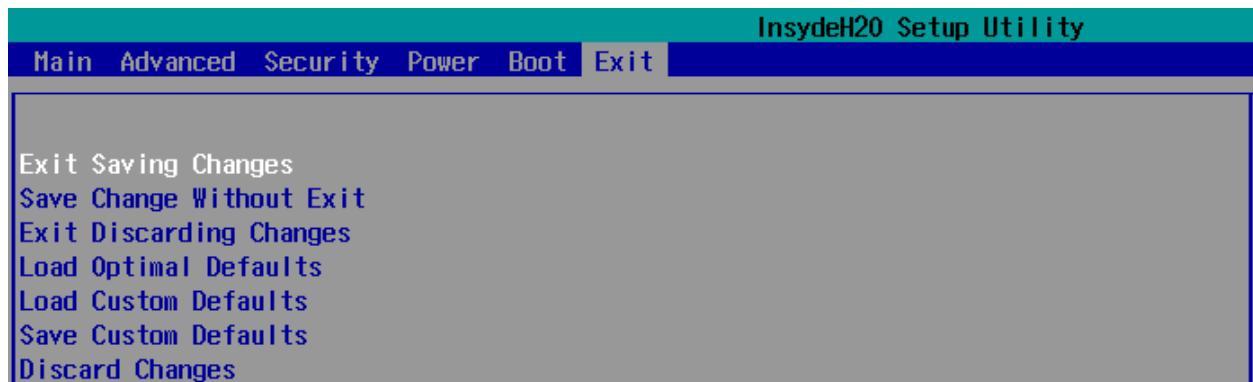
5.1 - EFI



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 W680 chipset on the Karbon 800 platform features Intel Rapid Storage Technology (RST), an integrated firmware-level RAID utility for SATA and NVMe disks. Intel RST on Alder 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 Karbon platform, the M.2 B-Key, both 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.

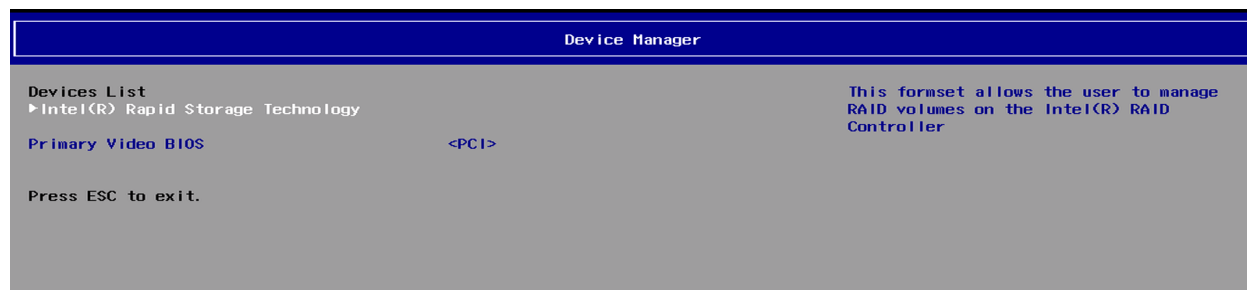
Recovery: Intel Rapid Recovery Technology creates a special RAID 1 array where instead of two equivalent disks, one disk is designated the “primary” and the other the “secondary”. Data is written to the primary drive, then copied to the secondary drive as a backup. This allows you to decide if you would 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

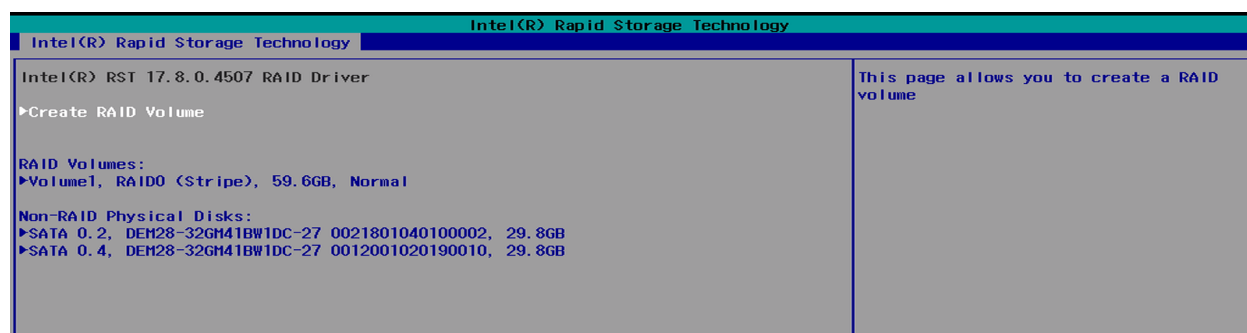
From the main menu, select “Device Management”. You will be greeted with the Device Manager options pictured below. Select “Intel(R) Rapid Storage Technology” to continue.



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.

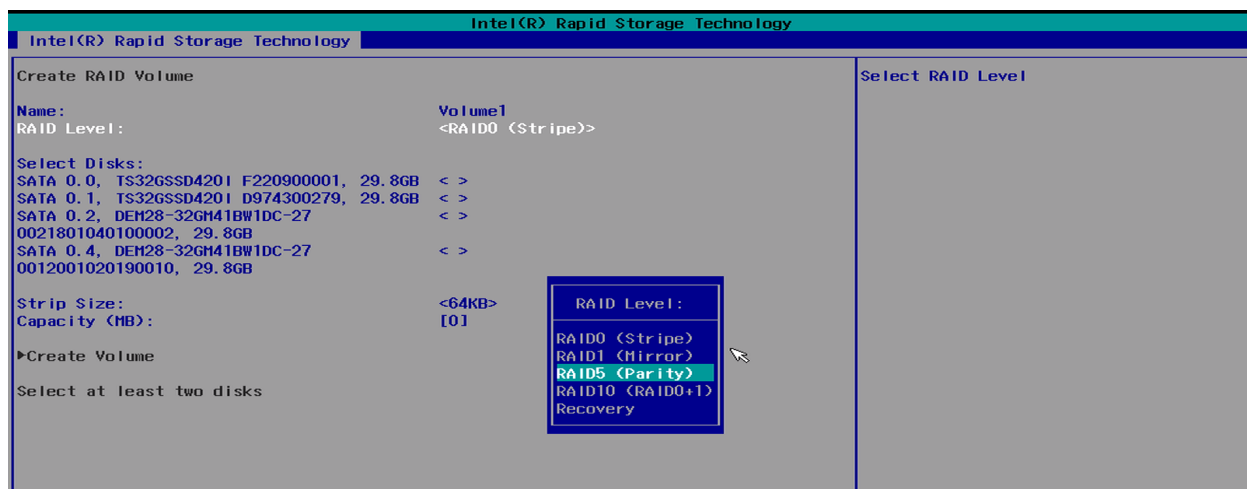
7.2.2 - Intel(R) Rapid Storage Technology Menu

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.

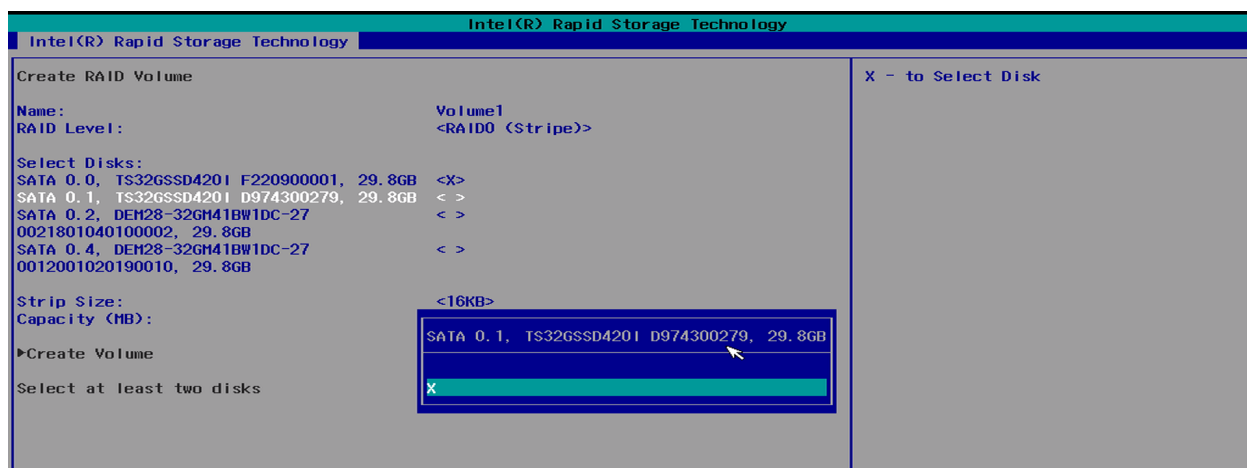


7.2.3 - Creating a New RAID Array

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](#).