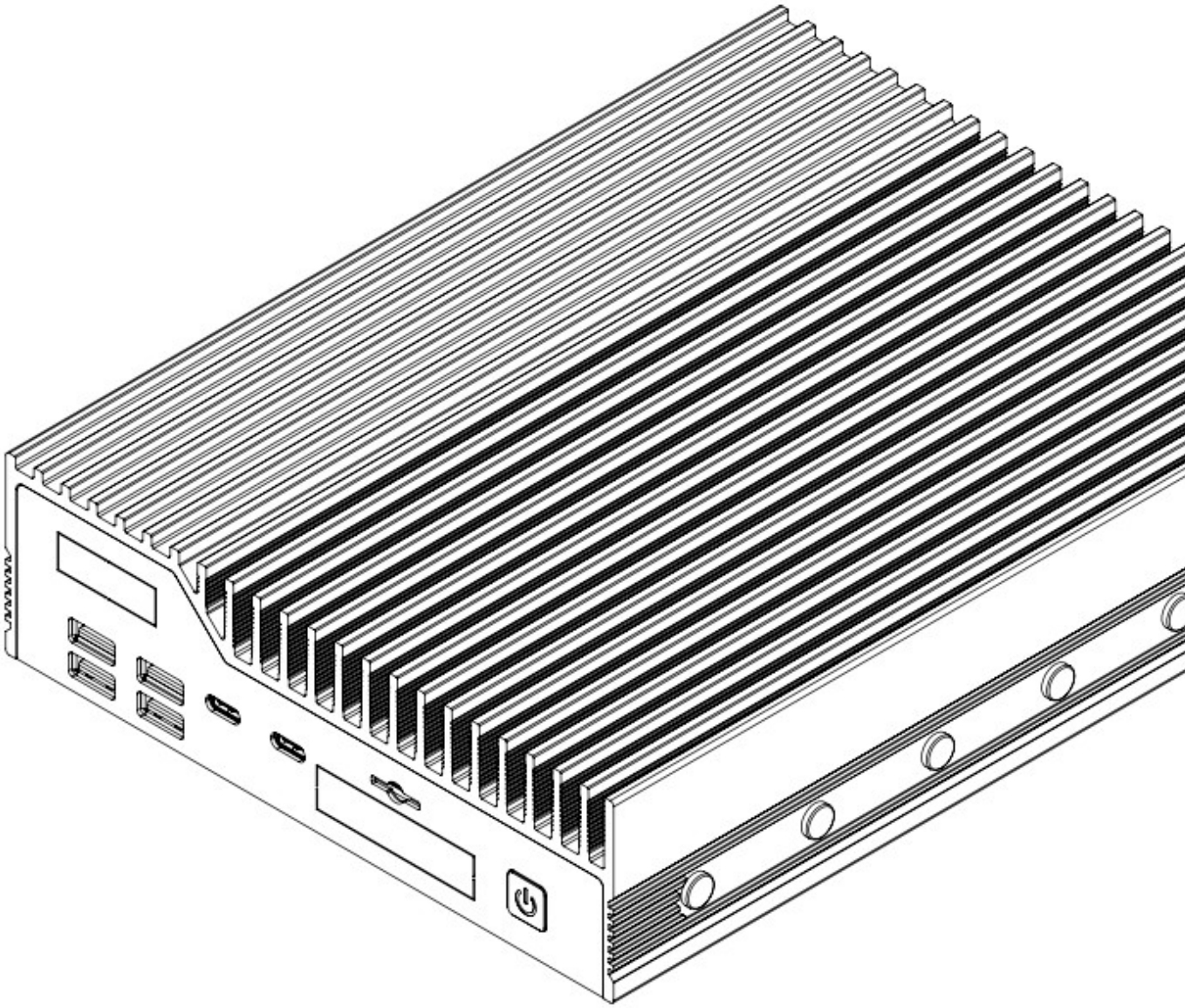
HX511 BIOS Manual

BIOS Version 1.20



Revision History

Revision History	Date
Initial Release	1/17/2023

Table of Contents

Introduction

The UEFI BIOS is a small program which runs when your computer starts and configures its basic functions. That configuration is automatic, and most users will be satisfied with the default configuration. If the default configuration is not sufficient, the BIOS has setup menus which can be used to reconfigure the computer.

The purpose of this manual is to document the function of the BIOS and its available configuration options. The text of this document lists the BIOS menus and options exactly as they appear in the BIOS menus: in the correct order, with the correct default values for this BIOS version. Some options are hidden based on how other options are set and which hardware is detected in the system, so some options may not appear on all systems. Informative screenshots are also provided throughout, but their contents may not exactly match this BIOS version.

Navigating the Setup Menu

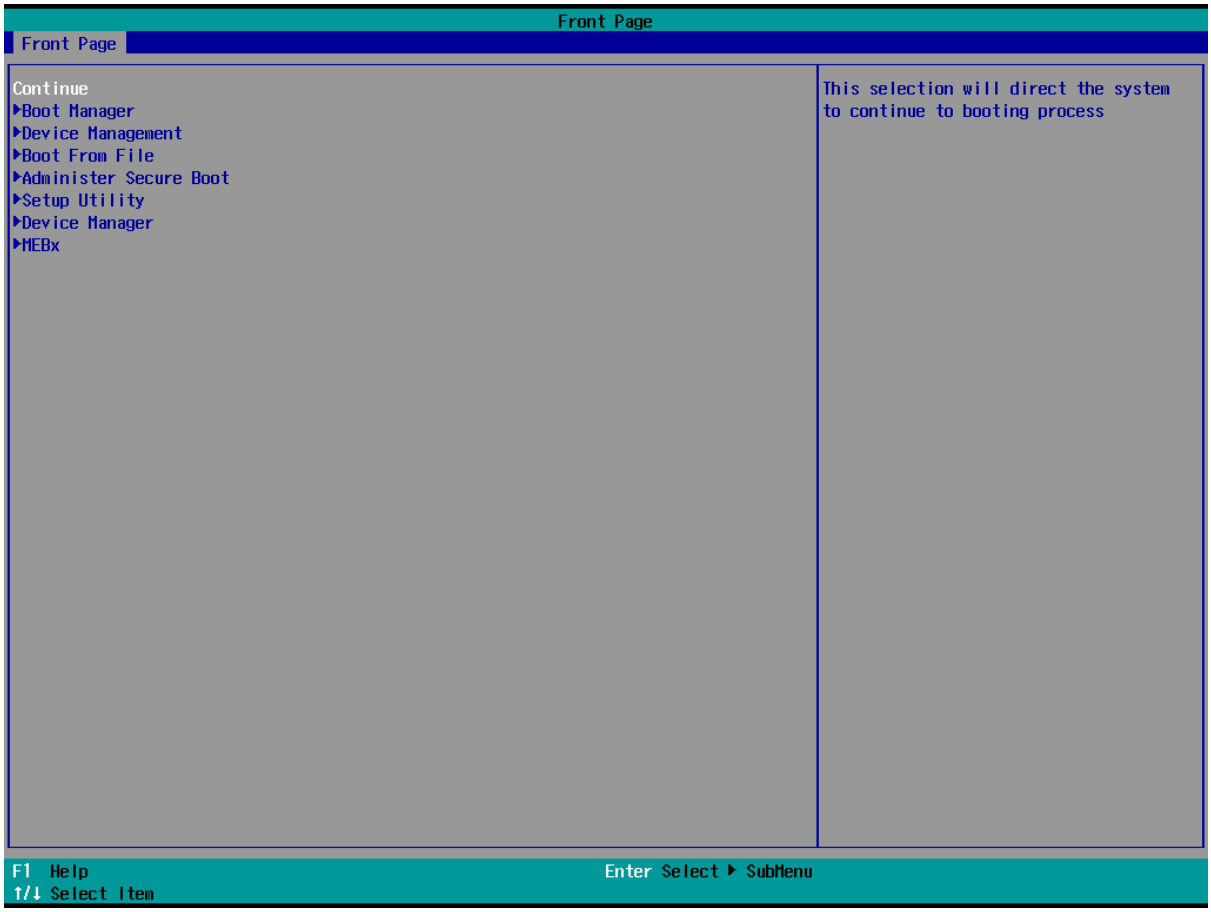
To access the BIOS setup menu, hold the Delete key on the keyboard while turning on the system. After a few seconds, the BIOS front page menu is shown:

On each menu, the selected option is shown in white, other options are shown in blue, and read-only options are shown in gray. Some menus have multiple screens, which are shown at the top of the screen. The active screen is shown with a gray background and inactive screens are shown with blue backgrounds.

BIOS menus are navigated by pressing keys on the keyboard:

- F1 shows help on available keyboard shortcuts
- ↑/↓ arrow keys select the option above or below the currently-selected option
- →/← arrow keys activate the screen to the right or left of the currently-activated screen
- Enter activates the selected option. If that option is a menu, it is opened. If it is a configuration option, a dialog is opened to select a new value.
- F5/F6 change the selected option to its previous or next value
- Esc returns to the previous menu
- F9 restores all options to their factory default values
- F10 saves all options and restarts the system

The Front Page



Several options are available on the front page:

- Continue: continues the boot process normally, booting the installed operating system
- Boot Manager: opens a menu to select which device should be booted
- Device Management: opens a menu which shows the status of the system hardware
- Boot From File: opens a menu to select a UEFI executable to boot
- Administer Secure Boot: opens a menu which manages the Secure Boot configuration of the system
- Setup Utility: opens the BIOS setup utility
- MEBx: opens the Intel AMT configuration utility

Boot Manager

The boot manager menu shows the devices available to be booted. The installed operating system and any attached USB drives will be listed. If enabled in the setup utility, the UEFI shell is also listed. Selecting an option boots it.

Setup Utility

The setup utility shows the status of the system and allows many configuration options to be changed. These options affect the functionality, stability and security of the system, and should not be changed without an understanding of their meaning.

The setup utility has many screens. Press the →/← arrow keys to select between them. Each screen is described below.

Commonly-used Configuration Options

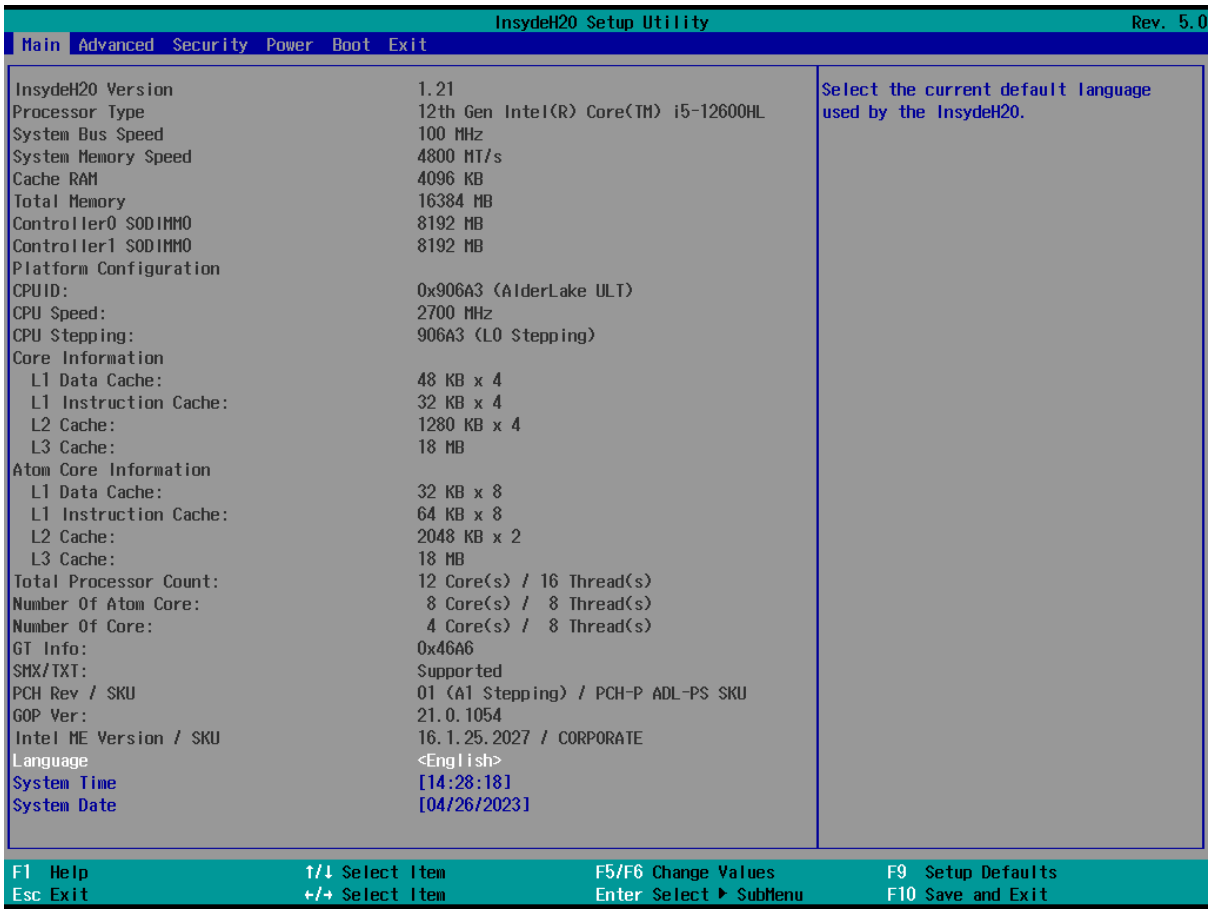
Several configuration options are frequently used.

Advanced > PCH-IO Configuration > State After G3

Default value: S0 State; possible values: S0 State, S5 State, Last

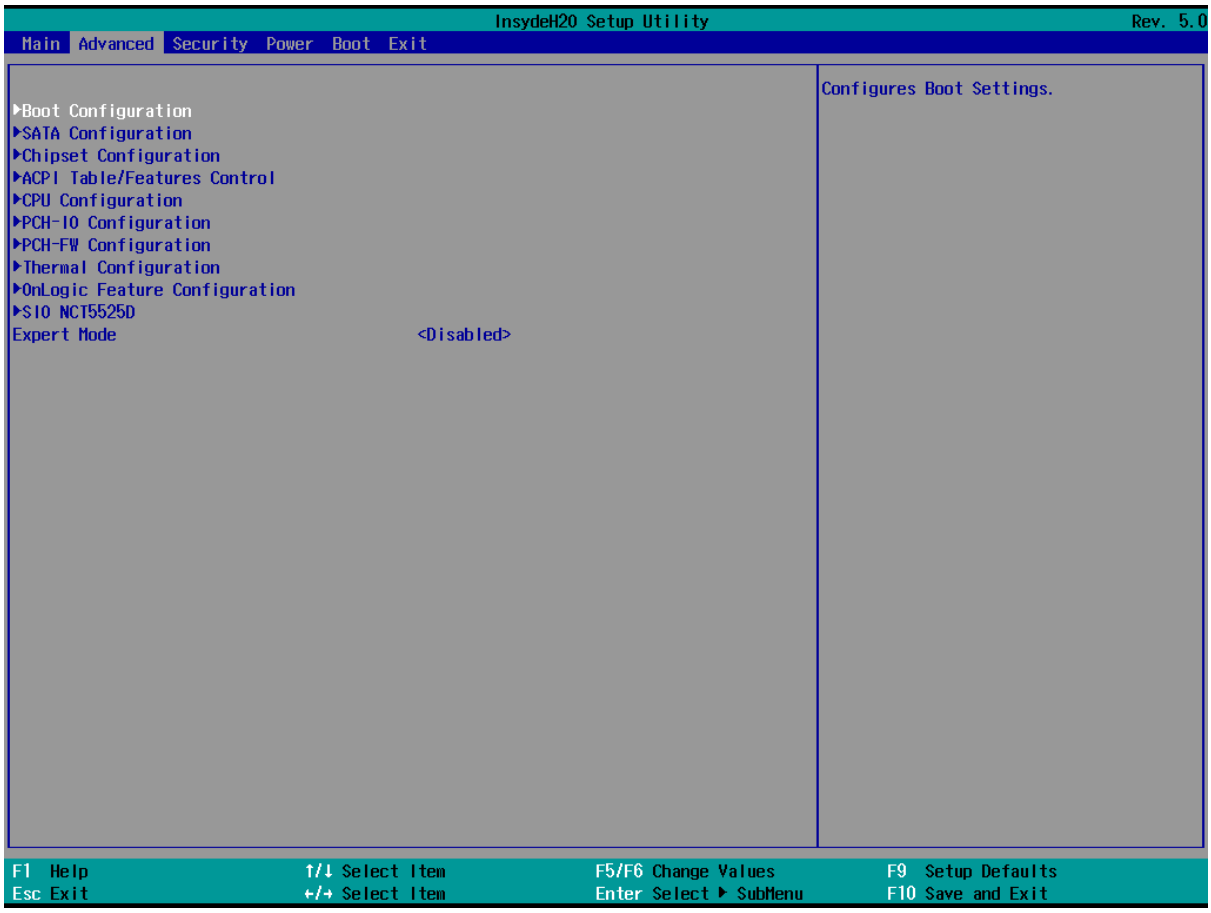
Controls the state the system enters after G3 (power loss). If set to S5, the system remains off when initially connected to power. If set to S0, the system boots when connected to power.

Main



The main screen shows the BIOS version, information about the installed CPU, and the system date and language.

Advanced



The Advanced menu contains the following options:

- Boot Configuration (menu)

  Configures Boot Settings.

- Peripheral Configuration (menu; only in expert mode)

  Configures the peripheral devices.

- SATA Configuration (menu)

  Select the SATA controller and hard disk drive type installed in your system

- USB Configuration (menu; only in expert mode)

  Configure the USB supp

- Chipset Configuration (menu)

  Advanced Chipset Configuration Options.

- Debug Settings (menu; only in expert mode)

  Debug interface Settings
- PCI Subsystem Settings (menu; only in expert mode)

  PCI, PCI-X and PCI Express Settings.
- ACPI Table/Features Control (menu)

  Configures ACPI Tables/Features setting.
- CPU Configuration (menu)

  CPU Configuration
- Connectivity Configuration (menu; only in expert mode)

  Configure Connectivity related options
- Power & Performance (menu; only in expert mode)

  Power & Performance Options
- Functional Safety Configuration (menu)

  Functional Safety Configuration options
- OverClocking Performance Menu (menu; only in expert mode)

  Performance Menu for Processor and Memory.
- Memory Configuration (menu; only in expert mode)

  Memory Configuration Parameters
- System Agent (SA) Configuration (menu; only in expert mode)

  System Agent (SA) Parameters
- PCIE Configuration (menu; only in expert mode)

  PCIE Parameters
- PCH-IO Configuration (menu)

  PCH Parameters
- PCH-FW Configuration (menu)

  Configure Management Engine Technology Parameters
- Thermal Configuration (menu)

  Thermal Configuration Parameters
- Platform Settings (menu; only in expert mode)

Platform related settings

- ACPI D3Cold settings (menu; only in expert mode)

  ACPI D3Cold related settings

- BCLK Configuration (menu; only in expert mode)

  BCLK Configuration options

- Console Redirection (menu)

  Console Redirection Settings

- OnLogic Feature Configuration (menu)

  OnLogic Feature Configuration Menu

- SIO NCT5124D (menu)

  SIO NCT5124D configuration menu

- Expert Mode (default value: Disabled; possible values: Disabled, Enabled)

  SCU Expert Mode

Advanced > Boot Configuration

The Boot Configuration menu contains the following options:

- Numlock (default value: Off; possible values: Off, On)

  Selects Power-on state for Numlock

Advanced > Peripheral Configuration

The Peripheral Configuration menu contains the following options:

- Serial Port A (default value: Disabled; possible values: Disabled, Auto, Enabled)

  Configure Serial port A using options : [Disable] No Configuration [Enable] User Configuration [Auto] EFI/OS chooses configuration

- Infrared Port (default value: Disabled; possible values: Disabled, Auto, Enabled)

  Configure Infrared port using options : [Disable] No Configuration [Enable] User Configuration [Auto] EFI/OS chooses configuration

Advanced > SATA Configuration

The SATA Configuration menu contains the following options:

- Serial ATA Port 0 (menu; disabled)

  Serial ATA Port 0 Device configuration

- Serial ATA Port 1 (menu; disabled)

  Serial ATA Port 1 Device configuration

Advanced > USB Configuration

The USB Configuration menu contains the following options:

- USB BIOS Support (default value: Enabled; possible values: Disabled, Enabled, UEFI Only)

  USB keyboard/mouse/storage support under UEFI and DOS environment. It will supporting UEFI environment only if set to UEFI Only

- Usb Legacy SMI bit Clean (default value: Disabled; possible values: Disabled, Enabled)

  Clean Usb Legacy SMI bit for xHCI and EHCI

Advanced > Chipset Configuration

The Chipset Configuration menu contains the following options:

- Platform Trust Technology (default value: Enabled; possible values: Enabled, Disabled)

  Enable/Disable Platform Trust Technology.

Advanced > Debug Settings

The Debug Settings menu contains the following options:

- Kernel Debug Serial Port (default value: Legacy UART; possible values: Legacy UART, SERIALIO UART0)

  Select Kernel Debug Port and report in ACPI DBG2 table

- Kernel Debug Patch (default value: Disabled; possible values: Disabled, Enabled)

  Enable/Disable Kernel Debug Patch

- Debug Token is present

  Debug Token is present

- Platform Debug Consent (default value: Disabled; possible values: Disabled, Enabled (All Probes+TraceHub), Enabled (Low Power), Manual)

  Enabled(All Probes+TraceHub) supports all probes with TraceHub enabled and blocks s0ix

Enabled(Low Power) Tracehub is powergated by default, s0ix is viable

Manual:user needs to configure Advanced Debug Settings manually, aimed at advanced users

- VT-d Debug Settings (menu)

  Vt-d Debug Settings

- Advanced Debug Settings (menu)

  Advanced Debug Settings

Advanced > PCI Subsystem Settings

The PCI Subsystem Settings menu contains the following options:

- PCI Bus Driver Version

  PCI, PCI-X and PCI Express Settings.

- PCI ROM Priority (default value: EFI Compatible ROM; possible values: Legacy ROM, EFI Compatible ROM)

  In case of multiple Option ROMs (Legacy and EFI Compatible), specifies what PCI Option rom to launch.

- External DMA Allowed On Boot (default value: No; possible values: No, Yes)

  External DMA Allowed On Boot for devices such as 1394, PCMCIA, & CardBus

- Install Ext OpRom Before BIOS Setup (default value: Disabled; possible values: Disabled, Ext PCIE Storage OpRom, Ext PCIE Other OpRom, Ext PCIE Both Storage and Other OpRom)

  Install Ext OpRom for Storage or Other device before BIOS Setup, That we can get the Ext PCIE Card OpRom Setup Menu and have chance to enter into it

- PCI Latency Timer (default value: 32 PCI Bus Clocks; possible values: 32 PCI Bus Clocks, 64 PCI Bus Clocks, 96 PCI Bus Clocks, 128 PCI Bus Clocks, 160 PCI Bus Clocks, 192 PCI Bus Clocks, 224 PCI Bus Clocks, 248 PCI Bus Clocks)

  Value to be programmed into PCI Latency Timer Register.

Advanced > ACPI Table/Features Control

The ACPI Table/Features Control menu contains the following options:

- ACPI Settings (menu)

  System ACPI Parameters

- FACP - RTC S4 Wakeup (default value: Enabled; possible values: Disabled, Enabled)

  Value only for ACPI. Enable/Disable for S4 Wakeup from RTC

- APIC - IO APIC Mode (default value: Enabled; possible values: Disabled, Enabled)

  This item is valid only for WIN2k and WINXP.Also,a fresh install of the OS must occur when APIC Mode is desired.Test the IO ACPI by setting item to Enable.The APIC Table will then be pointed to by the RSDT,the Local APIC will be initialized,and the proper enable bits will be set in ICH4M

Advanced > CPU Configuration

The CPU Configuration menu contains the following options:

- Efficient-core Information (menu)

  Displays the E-core Information

- Performance-core Information (menu)

  Displays the P-core Information

- ID

  Displays the Processor ID.

- Brand String

  Brand String of the Performance Processor

- VMX

  VMX Supported or Not

- SMX/TXT

  SMX/TXT Supported or Not

- TXT Crash Code

  TXT Crash Code Register value

- TXT SPAD

  TXT SPAD Register value

- Boot Guard Status

  Boot Guard Status Register value

- Boot Guard ACM Policy Status

  Boot Guard ACM Policy Status value

- Boot Guard SACM Information

  Boot Guard SACM Info MSR value

- C6DRAM (default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable moving of DRAM contents to PRM memory when CPU is in C6 state

- CPU Flex Ratio Override (default value: Disabled; possible values: Disabled, Enabled)

  Enable/Disable CPU Flex Ratio Programming

- CPU Flex Ratio Settings (read-only; possible values: numbers between 0 and 63)

  This value must be between Max Efficiency Ratio (LFM) and Maximum non-turbo ratio set by Hardware (HFM).

- Hardware Prefetcher (default value: Enabled; possible values: Disabled, Enabled)

  To turn on/off the MLC streamer prefetcher.

- Adjacent Cache Line Prefetch (default value: Enabled; possible values: Disabled, Enabled)

  To turn on/off prefetching of adjacent cache lines.

- Intel (VMX) Virtualization Technology (default value: Enabled; possible values: Disabled, Enabled)

  When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.

- PECI (default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable PECI

- AVX (default value: Enabled; possible values: Enabled, Disabled)

  Enable/Disable the Avx 2 Instructions. This is applicable for Performance-core only

- Active Performance-cores (default value: All; possible values: All)

  Number of P-cores to enable in each processor package. Note: Number of Cores and E-cores are looked at together. When both are {0,0}, Pcode will enable all cores.

- Active Efficient-cores (default value: All; possible values: All, 0)

  Number of E-cores to enable in each processor package. Note: Number of Cores and E-cores are looked at together. When both are {0,0}, Pcode will enable all cores.

- Hyper-Threading (default value: Enabled; possible values: Disabled, Enabled)

  Enable or Disable Hyper-Threading Technology.

- BIST (default value: Disabled; possible values: Disabled, Enabled)

  Enable/Disable BIST (Built-In Self Test) on reset

- AP threads Idle Manner (default value: MWAIT Loop; possible values: HALT Loop, MWAIT Loop, RUN Loop)

  AP threads Idle Manner for waiting signal to run

- AES (default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable AES (Advanced Encryption Standard)

- MachineCheck (default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable Machine Check

- MonitorMWait (default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable MonitorMWait, if Disable MonitorMwait, the AP threads Idle Manner should not set in MWAIT Loop

- Intel Trusted Execution Technology (default value: Disabled; possible values: Disabled, Enabled)

  Enables utilization of additional hardware capabilities provided by Intel (R) Trusted Execution Technology.

  Changes require a full power cycle to take effect.

- Alias Check Request (read-only; possible values: Disabled, Enabled)

  Enables Txt Alias Checking capability

  Changes require full Txt capability before it will take effect.

  It is a one time only change, next reboot will be reset.

- DPR Memory Size (MB) (read-only; possible values: numbers between 0 and 255)

  Reserve DPR memory size (0-255) MB

- Reset AUX Content (read-only; possible values: Yes, No)

  Reset TPM Aux content. Txt may not functional after AUX content gets reset.

- CPU SMM Enhancement (menu)

  CPU SMM Enhancement

- Total Memory Encryption (default value: Disabled; possible values: Disabled, Enabled)

  Configure Total Memory Encryption (TME) to protect DRAM data from physical attacks.

Advanced > Connectivity Configuration

The Connectivity Configuration menu contains the following options:

- RFI Mitigation (default value: Enabled; possible values: Enabled, Disabled)

  This is an option intended to Enable/Disable DDR-RFIM feature for Connectivity

  This RFI mitigation feature may result in temporary slowdown of the DDR speed.
- CoExistence Manager (read-only; possible values: Disabled, Enabled)

  CoEx Manager mitigates radio coexistence issues between Intel WWAN (modem) and Intel WLAN (WiFi/BT).

  This should be enabled only if both WWAN and WLAN solutions are based on Intel components
- Preboot BLE (default value: Disabled; possible values: Disabled, Enabled)

  This will be used to enable Preboot Bluetooth function
- Discrete Bluetooth Interface (default value: USB; possible values: Disabled, USB)

  SerialIo UART0 needs to be enabled to select BT interface
- BT Tile Mode (default value: Disabled; possible values: Disabled, Enabled)

  Enable/Disable Tile
- Advanced settings (default value: Disabled; possible values: Disabled, Enabled)

  Configure ACPI objects for wireless devices
- WWAN Configuration (menu)

  Configure WWAN related options

Advanced > Power & Performance

The Power & Performance menu contains the following options:

- CPU - Power Management Control (menu)

  CPU - Power Management Control Options
- GT - Power Management Control (menu)

  GT - Power Management Control Options
- Intel(R) Speed Shift Technology Interrupt Control (default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable Intel(R) Speed Shift Technology Interrupts

Advanced > Functional Safety Configuration

The Functional Safety Configuration menu contains the following options:

- Fusa Enable (default value: Disabled; possible values: Disabled, Enabled)

  Enable/Disable all Functional Safety (FUSA) feature

- Enable Startup Array BIST (default value: Disabled; possible values: Disabled, Enabled)

  Enabling this will execute startup array test during boot

- Enable Startup Scan BIST (default value: Disabled; possible values: Disabled, Enabled)

  Enabling this will execute startup scan test during boot

- Enable Periodic Scan BIST (default value: Disabled; possible values: Disabled, Enabled)

  Enabling this will execute periodic scan test during boot

- Core Lockstep Configuration (default value: Disable lockstep; possible values: Disable lockstep, Enable lockstep for Core 0 with Core 1, Core 2 with Core 3, Enable lockstep for Core 0 with Core 1, Enable lockstep for Core 2 with Core 3)

  Enable/Disable Lockstep for Efficient-core module, which has 4 cores each

- Core Lockstep Configuration (default value: Disable lockstep; possible values: Disable lockstep, Enable lockstep for Core 0 with Core 1, Core 2 with Core 3, Enable lockstep for Core 0 with Core 1, Enable lockstep for Core 2 with Core 3)

  Enable/Disable Lockstep for Efficient-core module, which has 4 cores each

- Display Fusa Configuration (default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable Functional Safety (FUSA) on Display

- Graphics Fusa Configuration (default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable Functional Safety (FUSA) on Graphics

- Opio Fusa Configuration (default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable Functional Safety (FUSA) on Opio

- Psf Fusa Configuration (default value: Disabled; possible values: Disabled, Enabled)

  Enable/Disable Functional Safety (FUSA) on Psf

- Iop Fusa Configuration (default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable Functional Safety (FUSA) on Iop

Advanced > OverClocking Performance Menu

The OverClocking Performance Menu menu contains the following options:

- OverClocking Feature (read-only; possible values: Disabled, Enabled)

  Performance Menu for Processor and Memory.
- WDT Enable (default value: Disabled; possible values: Disabled, Enabled)

  Enable/Disable WatchDog Timer. Note: This option is ignored on debug BIOS.
- BCLK Frequency

Advanced > Memory Configuration

The Memory Configuration menu contains the following options:

- Memory Thermal Configuration (menu)

  Memory Thermal Configuration Options
- Memory Training Algorithms (menu)

  Enable/Disable Memory Training Algorithms.
- Memory (menu)

  Memory Overclocking Menu
- Memory RC Version

  Memory RC Version
- Memory Frequency

  Displays the Frequency of Memory
- tCL-tRCD-tRP-tRAS

  Memory Timings
- MC 0 Ch 0 DIMM 0

  Controller Channel Slot Subtitle
- MC 0 Ch 0 DIMM 1

  Controller Channel Slot Subtitle
- Size

  Memory Size in the Slot.
- Number of Ranks

Number of Ranks in the slot

- Manufacturer

  DIMM / DRAM Manufacturer Value

- MC 1 Ch 0 DIMM 0

  Controller Channel Slot Subtitle

- MC 1 Ch 0 DIMM 1

  Controller Channel Slot Subtitle

- Size

  Memory Size in the Slot.

- Number of Ranks

  Number of Ranks in the slot

- Manufacturer

  DIMM / DRAM Manufacturer Value

- Debug Value (default value: 0; possible values: numbers between 0 and 4294967295)

  Debug Value

- MRC ULT Safe Config (default value: Disabled; possible values: Disabled, Enabled)

  MRC ULT Safe Config for PO

- LPDDR DqDqs Re-Training (default value: Enabled; possible values: Disabled, Enabled)

  Disable/Enable LPDDR DqDqs Re Training

- Safe Mode Support (default value: Disabled; possible values: Disabled, Enabled)

  Safe Mode enable support. Option will be used for changes/WAs that may affect an stable MRC

- Memory Test on Warm Boot (default value: Enabled; possible values: Disabled, Enabled)

  Enable Or Disable Base Memory Test Run on Warm Boot

- Maximum Memory Frequency (default value: Auto; possible values: Auto, 1067, 1333, 1400, 1600, 1800, 1867, 2000, 2133, 2200, 2400, 2600, 2667, 2800, 2933, 3000, 3200, 3467, 3600, 3733, 4000, 4200, 4267, 4400, 4600, 4800, 5000, 5200, 5400, 5600, 5800, 6000, 6200, 6400, 10000, 12800)

  Maximum Memory Frequency Selections in Mhz.

- LP5 Bank Mode (default value: Auto; possible values: Auto, LP5 8 Bank Mode, LP5 16 Bank Mode, LP5 BG Mode)

LP5 Bank Mode

- Frequency Limit for Mixed 2DPC DDR4 (default value: 0; possible values: numbers between 0 and 65535)

  Override the reduced speed in mixed 2DPC config or non-POR 2DPC config. 0=Auto, otherwise speed in MT/s

- Frequency Limit for Mixed 2DPC DDR5 1 Rank 8GB and 8GB (default value: 2000; possible values: numbers between 0 and 65535)

  Override the reduced speed in mixed 2DPC config or non-POR 2DPC config. 0=Auto, otherwise speed in MT/s

- Frequency Limit for Mixed 2DPC DDR5 1 Rank 16GB and 16GB (default value: 2000; possible values: numbers between 0 and 65535)

  Override the reduced speed in mixed 2DPC config or non-POR 2DPC config. 0=Auto, otherwise speed in MT/s

- Frequency Limit for Mixed 2DPC DDR5 1 Rank 8GB and 16GB (default value: 2000; possible values: numbers between 0 and 65535)

  Override the reduced speed in mixed 2DPC config or non-POR 2DPC config. 0=Auto, otherwise speed in MT/s

- Frequency Limit for Mixed 2DPC DDR5 2 Rank (default value: 2000; possible values: numbers between 0 and 65535)

  Override the reduced speed in mixed 2DPC config or non-POR 2DPC config. 0=Auto, otherwise speed in MT/s

- LCT Cmd Eye Width (default value: 96; possible values: numbers between 0 and 65535)

  LCT Cmd Eye Width 0= Auto

- HOB Buffer Size (default value: Auto; possible values: Auto, 1B, 1KB, Max (assuming 63KB total HOB size))

  Size to set HOB Buffer

- Max TOLUD (default value: Dynamic; possible values: Dynamic, 1 GB, 1.25 GB, 1.5 GB, 1.75 GB, 2 GB, 2.25 GB, 2.5 GB, 2.75 GB, 3 GB, 3.25 GB, 3.5 GB)

  Maximum Value of TOLUD. Dynamic assignment would adjust TOLUD automatically based on largest MMIO length of installed graphic controller

- SA GV (default value: Enabled; possible values: Disabled, Enabled, Fixed to 1st Point, Fixed to 2nd Point, Fixed to 3rd Point, Fixed to 4th Point)

  System Agent Geyserville. Can disable, fix to a specific point, or enable frequency switching.

- First Point Frequency (default value: 0; possible values: numbers between 0 and 65535)

  Specify the frequency for the given point. 0 - MRC auto, Else a specific frequency as an integer: 1333

- First Point Gear (default value: 0; possible values: numbers between 0 and 4)

  Gear ratio for this SAGV point. 0-Auto, 1-G1, 2-G2, 4-G4

- Second Point Frequency (default value: 0; possible values: numbers between 0 and 65535)

  Specify the frequency for the given point. 0 - MRC auto, Else a specific frequency as an integer: 1333

- Second Point Gear (default value: 0; possible values: numbers between 0 and 4)

  Gear ratio for this SAGV point. 0-Auto, 1-G1, 2-G2, 4-G4

- Third Point Frequency (default value: 0; possible values: numbers between 0 and 65535)

  Specify the frequency for the given point. 0 - MRC auto, Else a specific frequency as an integer: 1333

- Third Point Gear (default value: 0; possible values: numbers between 0 and 4)

  Gear ratio for this SAGV point. 0-Auto, 1-G1, 2-G2, 4-G4

- Fourth Point Frequency (default value: 0; possible values: numbers between 0 and 65535)

  Specify the frequency for the given point. 0 - MRC auto, Else a specific frequency as an integer: 1333

- Fourth Point Gear (default value: 0; possible values: numbers between 0 and 4)

  Gear ratio for this SAGV point. 0-Auto, 1-G1, 2-G2, 4-G4

- SAGV Switch Factor IA (default value: 30; possible values: numbers between 1 and 50)

  SAGV Switch Factor of IA Load Percentage To Trigger Switching Up And Down

- SAGV Switch Factor GT (default value: 30; possible values: numbers between 1 and 50)

  SAGV Switch Factor of GT Load Percentage To Trigger Switching Up And Down

- SAGV Switch Factor IO (default value: 30; possible values: numbers between 1 and 50)

  SAGV Switch Factor of IO Load Percentage To Trigger Switching Up And Down

- SAGV Switch Factor Stall (default value: 30; possible values: numbers between 1 and 50)

  SAGV Switch Factor of IA/GT Stall Percentage To Trigger Switching Up And Down

- Threshold For Switch Up (default value: 1; possible values: numbers between 1 and 50)

  Duration In MS Of High Activity After Which SAGV Will Switch Up

- Threshold For Switch Down (default value: 1; possible values: numbers between 1 and 50)

  Duration In MS Of Low Activity After Which SAGV Will Switch Down

- Retrain on Fast Fail (default value: Enabled; possible values: Disabled, Enabled)

  Restart MRC in Cold mode if SW MemTest fails during Fast flow. Default = Enabled

- DDR4_1DPC (default value: Enabled; possible values: Disabled, Enabled on DIMM0 only, Enabled on DIMM1 only, Enabled)

  DDR4 1DPC performance feature for 2R DIMMs. Can be enabled on DIMM0 or DIMM1 only, or on both

- Row Hammer Mode (default value: RFM; possible values: Disabled, RFM, pTRR)

  Row Hammer Prevention Mode. RFM will fall back to pTRR if not available

- RH LFSR0 Mask (default value: 1/2^11; possible values: 1/2^1, 1/2^2, 1/2^3, 1/2^4, 1/2^5, 1/2^6, 1/2^7, 1/2^8, 1/2^9, 1/2^10, 1/2^11, 1/2^12, 1/2^13, 1/2^14, 1/2^15)

  LFSR0 mask for RH pTRR

- RH LFSR1 Mask (default value: 1/2^11; possible values: 1/2^1, 1/2^2, 1/2^3, 1/2^4, 1/2^5, 1/2^6, 1/2^7, 1/2^8, 1/2^9, 1/2^10, 1/2^11, 1/2^12, 1/2^13, 1/2^14, 1/2^15)

  LFSR1 mask for RH pTRR

- MC Refresh Rate (default value: NORMAL Refresh; possible values: NORMAL Refresh, 2x Refresh, 4x Refresh)

  Select refresh rate on the MC

- Refresh Watermarks (default value: High; possible values: Low, High)

  Sets Refresh Panic Watermark and Refresh High-Priority Watermark to HIGH or LOW values

- LPDDR ODT RttWr (default value: 0; possible values: numbers between 0 and 255)

  Initial RttWr ODT override for LP4/5 in Ohms. Range 0x01 - 0xFF, default 0 = AUTO

- LPDDR ODT RttCa (default value: 0; possible values: numbers between 0 and 255)

  Initial RttCa ODT override for LP4/5 in Ohms. Range 0x01 - 0xFF, default 0 = AUTO

- Exit On Failure (MRC) (default value: Enabled; possible values: Disabled, Enabled)

  Exit On Failure for MRC training steps

- New Features 1 - MRC (default value: Disabled; possible values: Disabled, Enabled)

  Enabling/Disabling Generic New Features 1

- New Features 2 - MRC (default value: Disabled; possible values: Disabled, Enabled)

  Enabling/Disabling Generic New Features 2

- Ch Hash Override (default value: Disabled; possible values: Disabled, Enabled)

  Override Channel Hash settings

- Ch Hash Support (read-only; possible values: Disabled, Enabled)

  Enable/Disable Channel Hash Support. NOTE: ONLY if Memory interleaved Mode

- Ch Hash Mask (read-only; possible values: numbers between 1 and 16383)

  Set the BIT(s) to be included in the XOR function. NOTE BIT mask corresponds to BITS [19:6}

- Ch Hash Interleaved Bit (read-only; possible values: BIT6, BIT7, BIT8, BIT9, BIT10, BIT11, BIT12, BIT13)

  Select the BIT to be used for Channel Interleaved mode. NOTE: BIT7 will interlave the channels at a 2 cacheline granularity, BIT8 at 4 and BIT9 at 8

- Extended Bank Hashing (default value: Enabled; possible values: Disabled, Enabled)

  Enable/disable Extended Bank Hashing.

- Per Bank Refresh (default value: Enabled; possible values: Disabled, Enabled)

  Enables and Disables the per bank refresh. This only impacts memory technologies that support PBR: LPDDR4, LPDDR5 and DDR5

- VC1 Read Metering (default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable VC1 Read Metering Feature (RdMeter)

- Strong Weak Leaker (default value: 7; possible values: numbers between 1 and 7)

  Value for StrongWkLeaker

- Power Down Mode (default value: Auto; possible values: Auto, No Power Down, APD, PPD-DLLoff)

  CKE Power Down Mode Control

- Pwr Down Idle Timer (default value: 0; possible values: numbers between 0 and 255)

  The minimum value should = to the worst case Roundtrip delay + Burst_Length. 0 means AUTO: 64 for ULX/ULT, 128 for DT/Halo

- Page Close Idle Timeout (default value: Enabled; possible values: Enabled, Disabled)

  Page Close Idle Timeout Control

- Memory Scrambler (default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable Memory Scrambler support.

- Force ColdReset (default value: Disabled; possible values: Enabled, Disabled)

  Force ColdReset OR Choose MrcColdBoot mode, when Coldboot is required during MRC

execution. Note: If ME 5.0MB is present, ForceColdReset is required!

- Controller 0, Channel 0 Control (default value: Enabled; possible values: Enabled, Disabled)

  Controller 0, Channel 0 Control - Enable or Disable Controller 0, Channel 0.
- Controller 0, Channel 1 Control (default value: Enabled; possible values: Enabled, Disabled)

  Controller 0, Channel 1 Control - Enable or Disable Controller 0, Channel 1.
- Controller 0, Channel 2 Control (default value: Enabled; possible values: Enabled, Disabled)

  Controller 0, Channel 2 Control - Enable or Disable Controller 0, Channel 2.
- Controller 0, Channel 3 Control (default value: Enabled; possible values: Enabled, Disabled)

  Controller 0, Channel 3 Control - Enable or Disable Controller 0, Channel 3.
- Controller 1, Channel 0 Control (default value: Enabled; possible values: Enabled, Disabled)

  Controller 1, Channel 0 Control - Enable or Disable Controller 1, Channel 0.
- Controller 1, Channel 1 Control (default value: Enabled; possible values: Enabled, Disabled)

  Controller 1, Channel 1 Control - Enable or Disable Controller 1, Channel 1.
- Controller 1, Channel 2 Control (default value: Enabled; possible values: Enabled, Disabled)

  Controller 1, Channel 2 Control - Enable or Disable Controller 1, Channel 2.
- Controller 1, Channel 3 Control (default value: Enabled; possible values: Enabled, Disabled)

  Controller 1, Channel 3 Control - Enable or Disable Controller 1, Channel 3.
- Force Single Rank (default value: Disabled; possible values: Disabled, Enabled)

  When enabled, only Rank 0 will be used in each DIMM
- Memory Remap (default value: Enabled; possible values: Enabled, Disabled)

  Enable/Disable Memory Remap above 4GB
- Time Measure (default value: Disabled; possible values: Disabled, Enabled)

  Enable/Disable printing of the time it takes to execute MRC.
- Fast Boot (default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable fast path thru the MRC
- Rank Margin Tool Per Task (default value: Disabled; possible values: Disabled, Enabled)

  Enables/Disables RMT running at every major training step
- Training Tracing (default value: Disabled; possible values: Disabled, Enabled)

  Enables/Disables printing of the current trained state at every major training step.

- Lpddr Mem WL Set (default value: Set B; possible values: Set A, Set B)

  Only applicable to LPDDR, Memory Write Latency Set selection (A is default, B will be used if memory devices support it)

- BDAT Memory Test Type (read-only; possible values: Rank Margin Tool Rank, Rank Margin Tool Bit, Margin 2D)

  Indicates the type of Memory Training data to populate into the BDAT ACPI table.

- Rank Margin Tool Loop Count (default value: 0; possible values: numbers between 0 and 32)

  Specifies the Loop Count to be used during Rank Margin Tool Testing. 0 - AUTO

- ECC DFT (default value: Disabled; possible values: Disabled, Enabled)

  Enable/Disable ECC DFT feature

- Write0 (default value: Disabled; possible values: Disabled, Enabled)

  Write0 feature for LP5/DDR5

- Periodic DCC (default value: Disabled; possible values: Disabled, Enabled)

  Enable / Disable Periodic DCC

- LPMode (default value: Auto; possible values: Auto, Enabled, Disabled)

  Control LPMode feature

- PPR Enable (default value: Disabled; possible values: Disabled, Hard PPR)

  PPR permanently repairs failed rows (if possible).

- SAM Overlaoding (default value: Disabled; possible values: Disabled, Enabled)

  Enable: copy the sagv frequency point. Disable: not copy.

Advanced > System Agent (SA) Configuration

The System Agent (SA) Configuration menu contains the following options:

- VT-d

  VT-d capability

- Graphics Configuration (menu)

  Graphics Configuration

- DMI/OPI Configuration (menu)

  Control various DMI functions.

- TCSS setup menu (menu)

TCSS Configuration settings

- VMD setup menu (menu)

  VMD Configuration settings

- Display setup menu (menu)

  Display Configuration settings

- PCI Express Configuration (menu)

  PCI Express Configuration settings

- Stop Grant Configuration (default value: Auto; possible values: Auto, Manual)

  Automatic/Manual stop grant configuration

- VT-d (default value: Enabled; possible values: Disabled, Enabled)

  VT-d capability

- Control Iommu Pre-boot Behavior (default value: Enable IOMMU during boot; possible values: Disable IOMMU, Enable IOMMU during boot)

  Enable IOMMU in Pre-boot environment (If DMAR table is installed in DXE and If VTD_INFO_PPI is installed in PEI.)

- X2APIC Opt Out (default value: Disabled; possible values: Enabled, Disabled)

  Enable/Disable X2APIC_OPT_OUT bit

- DMA Control Guarantee (default value: Enabled; possible values: Enabled, Disabled)

  Enable/Disable DMA_CONTROL_GUARANTEE bit

- Thermal Device (B0:D4:F0) (default value: Disabled; possible values: Enabled, Disabled)

  Enable/Disable SA Thermal Device. Always enabled for ICL A0 stepping.

- Cpu CrashLog (Device 10) (default value: Enabled; possible values: Enabled, Disabled)

  Enable/Disable Cpu CrashLog Device.

- GNA Device (B0:D8:F0) (default value: Enabled; possible values: Enabled, Disabled)

  Enable/Disable SA GNA Device.

- CRID Support (default value: Disabled; possible values: Enabled, Disabled)

  Enable/Disable SA CRID and TCSS CRID control for Intel SIPP

- Above 4GB MMIO BIOS assignment (default value: Enabled; possible values: Enabled, Disabled)

  Enable/Disable above 4GB MemoryMappedIO BIOS assignment

This is enabled automatically when Aperture Size is set to 2048MB.

- IPU Device (B0:D5:F0) (default value: Enabled; possible values: Enabled, Disabled)

  Enable/Disable SA IPU Device.

- IPU 1181 Dash Camera (default value: Disabled; possible values: Enabled, Disabled)

  Enable/Disable SA IPU 1181 Dash Camera support.

- MIPI Camera Configuration (menu)

  MIPI Camera Configuration

Advanced > PCIE Configuration

The PCIE Configuration menu contains the following options:

- IMR Configuration (menu)

  IMR Configuration

Advanced > PCH-IO Configuration

The PCH-IO Configuration menu contains the following options:

- PCI Express Configuration (menu)

  PCI Express Configuration settings

- SATA Configuration (menu)

  SATA Device Options Settings

- USB Configuration (menu)

  USB Configuration settings

- Security Configuration (menu)

  Security Configuration settings

- HD Audio Configuration (menu)

  HD Audio Subsystem Configuration Settings

- THC Configuration (menu; disabled)

  Touch Host Controller Configuration Settings

- Seriallo Configuration (menu)

  Seriallo Configuration Settings

- ISH Configuration (menu)

  Integrated Sensor Hub (ISH) Configuration
- Pch Thermal Throttling Control (menu)

  Pch Thermal Throttling Control
- Skip VCCIN_AUX Configuration (default value: Disabled; possible values: Disabled, Enabled)

  Skips VCCIN_AUX Configuration if enabled
- FIVR Configuration (menu)

  Menu for changing FIVR configuration parameters
- PMC Configuration (menu)

  Power management controller configuration
- EFI Network (default value: Disabled; possible values: Onboard NIC, WiFi, Onboard NIC & WiFi, Disabled)

  Enable/Disable EFI Network support for onboard LAN or WiFi module.
- DeepSx Power Policies (default value: Disabled; possible values: Disabled, Enabled in S4-S5-Battery, Enabled in S5-Battery, Enabled in S4-S5, Enabled in S5)

  configure the DeepSx Mode configuration.
- Wake on WLAN and BT Enable (only in expert mode; default value: Disabled; possible values: Enabled, Disabled)

  Enable/Disable PCI Express Wireless LAN and Bluetooth to wake the system.
- Disable DSX ACPRESENT PullDown (only in expert mode; default value: Disabled; possible values: Enabled, Disabled)

  Disable PCH internal ACPRESENT PullDown when DeepSx or G3 exit.
- State After G3 (default value: S0 State; possible values: S0 State, S5 State, Last)

  Specify what state to go to when power is re-applied after a power failure (G3 state).
- Port 80h Redirection (default value: LPC Bus; possible values: LPC Bus, PCIE Bus)

  Control where the Port 80h cycles are sent.
- Enhance Port 80h LPC Decoding (default value: Enabled; possible values: Disabled, Enabled)

  Support the word/dword decoding of port 80h behind LPC
- Compatible Revision ID (read-only; possible values: Disabled, Enabled)

  Enable/Disable the PCH Compatible Revision ID feature

- Legacy IO Low Latency (default value: Disabled; possible values: Disabled, Enabled)

  Set to enable low latency of legacy IO. Some systems require lower IO latency irrespective of power. This is a tradeoff between power and IO latency.

- PCH Cross Throttling (default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable the PCH Cross Throttling feature. Only ULT support this feature.

- PCH Energy Reporting (default value: Enabled; possible values: Disabled, Enabled)

  Enable Energy Report. MUST set it as ENABLED. This is only for test purpose.

- LPM S0i2.0 (default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable S0ix sub-state. This setting is for test purpose. S0ix sub-states should be enabled for production.

- LPM S0i3.0 (default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable S0ix sub-state. This setting is for test purpose. S0ix sub-states should be enabled for production.

- C10 Dynamic threshold adjustment (default value: Disabled; possible values: Disabled, Enabled)

  Enable/Disable C10 dynamic threshold adjustment

- IEH Mode (default value: Bypass Mode; possible values: Bypass Mode, Enabled)

  Enable/Bypass IEH Mode

- Enable TCO Timer (default value: Disabled; possible values: Disabled, Enabled)

  Enable/Disable TCO timer. When disabled, it disables PCH ACPI timer, stops TCO timer, and ACPI WDAT table will not be published.

- Enable Timed GPIO0 (default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable Timed GPIO0. When disabled, it disables cross time stamp time-synchronization as extension of Hammock Harbor time synchronization.

- Enable Timed GPIO1 (default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable Timed GPIO1. When disabled, it disables cross time stamp time-synchronization as extension of Hammock Harbor time synchronization.

- Pcie Pll SSC (default value: Auto; possible values: Auto, 0.0%, 0.1%, 0.2%, 0.3%, 0.4%, 0.5%, 0.6%, 0.7%, 0.8%, 0.9%, 1.0%, 1.1%, 1.2%, 1.3%, 1.4%, 1.5%, 1.6%, 1.7%, 1.8%, 1.9%, 2.0%, Disable)

  Pcie Pll SSC percentage.AUTO - Keep hw default, no BIOS override. Range is 0.0%-2.0%.

- IOTG PLL SSCEN (CPU Side SSC) (default value: Enabled; possible values: Disabled, Enabled)

Enable/Disable IOTG PLL SSCEN

- Enable 8254 Clock Gate (default value: Enabled; possible values: Disabled, Enabled, Enabled In Runtime and S3 Resume)

  Enables/Disables 8254 clock gate in early phase. Set 8254CGE is necessary for SLP_S0 support. Platform is albe to disable this policy and set 8254CGE in late phase.

- Lock PCH Sideband Access (default value: Enabled; possible values: Disabled, Enabled)

  Lock PCH Sideband access, include SideBand interface lock and SideBand PortID mask for certain end point (e.g. PSFx). The option is invalid if POSTBOOT SAI is set.

- Flash Protection Range Registers (FPRR) (default value: Enabled; possible values: Disabled, Enabled)

  Enable Flash Protection Range Registers

- SPD Write Disable (default value: TRUE; possible values: TRUE, FALSE)

  Enable/Disable setting SPD Write Disable. For security recommendations, SPD write disable bit must be set.

- LGMR (default value: Disabled; possible values: Enabled, Disabled)

  64KB memory block for LGMR (LPC Memory Range Decode)

- HOST_C10 reporting to Target (default value: Disabled; possible values: Disabled, Enabled)

  This option enables HOST_C10 reporting to Target via eSPI Virtual Wire

- OS IDLE Mode (default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable OS Idle Mode Feature

- S0ix Auto Demotion (default value: Enabled; possible values: Enabled, Disabled)

  Enable/Disable Host Low Power Mode S0ix Auto-Demotion

- Latch Events C10 Exit (default value: Disabled; possible values: Enabled, Disabled)

  Enable/Disable Latch Events on C10 Exit

- Extended BIOS Range Decode (default value: Disabled; possible values: Disabled, Enabled)

  Enabling this will make memory cycles falling in a specific area to be redirected to SPI flash controller

- ACPI L6D PME Handling (default value: Disabled; possible values: Enabled, Disabled)

  BIOS through ACPI code can associate specific method to a particular GPE. In this case _L6D for Level-triggered Event, BIOS-ACPI can verify PMEENABLE and PMESTATUS of each device that requires GPE related wake.

Advanced > PCH-FW Configuration

The PCH-FW Configuration menu contains the following options:

- ME Firmware Version

  ME Firmware Version

- ME Firmware Mode

  ME Firmware Mode

- ME Firmware SKU

  ME Firmware SKU

- ME Firmware Status 1

  ME Firmware Status 1

- ME Firmware Status 2

  ME Firmware Status 2

- ME Firmware Status 3

  ME Firmware Status 3

- ME Firmware Status 4

  ME Firmware Status 4

- ME Firmware Status 5

  ME Firmware Status 5

- ME Firmware Status 6

  ME Firmware Status 6

- ME State (default value: Enabled; possible values: Disabled, Enabled)

  When Disabled ME will be put into ME Temporarily Disabled Mode.

- Manageability Features State (default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable Intel(R) Manageability features.

  NOTE:

  This option disables/enables Manageability Features support in FW.

  To disable support platform must be in an unprovisioned state first.

- AMT BIOS Features (default value: Enabled; possible values: Disabled, Enabled)

  When disabled AMT BIOS Features are no longer supported and user is no longer able to

access MEBx Setup.

Note:

This option does not disable Manageability Features in FW.

- AMT Configuration (menu)

  Configure Intel(R) Active Management Technology Parameters

- ME Unconfig on RTC Clear (default value: Enabled; possible values: Disabled, Enabled)

  When Disabled ME will not be unconfigured on RTC Clear

- Comms Hub Support (default value: Disabled; possible values: Disabled, Enabled)

  Enables/Disables support for Comms Hub.

- JHI Support (default value: Disabled; possible values: Disabled, Enabled)

  Enable/Disable Intel(R) DAL Host Interface Service (JHI)

- Core Bios Done Message (default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable Core Bios Done message sent to ME

- Firmware Update Configuration (menu)

  Configure Management Engine Technology Parameters

- PTT Configuration (menu)

  Configure PTT

- FIPS Configuration (menu)

  FIPS Mode help

- Unique Platform Id Configuration (menu; disabled)

  Configure Unique Platform Id Feature

- ME Debug Configuration (menu)

  Configure ME debug options

  NOTE:

  This menu is provided for testing purposes. It is recommended to leave the options in their default states

- Anti-Rollback SVN Configuration (menu)

  Configure Anti-Rollback SVN

- OEM Key Revocation Configuration (menu)

Configure OEM Key Revocation

- Extend CSME Measurement to TPM-PCR (default value: Disabled; possible values: Disabled, Enabled)

  Enable/Disable Extend CSME Measurement to TPM-PCR[0] and AMT Config to TPM-PCR[1]

Advanced > Thermal Configuration

The Thermal Configuration menu contains the following options:

- Enable All Thermal Functions (default value: Enabled; possible values: Disabled, Enabled)

  Enable All Thermal Functions" is Enabled it Enables 'Memory Thermal Management','Active Trip Points', 'Critical Trip Points'.Set to disabled for Manual Configuration

- CPU Thermal Configuration (menu)

  CPU Thermal Configuration options

- Platform Thermal Configuration (menu)

  Platform Thermal Configuration options

- Intel(R) Dynamic Tuning Technology Configuration (menu)

  Intel(R) Dynamic Tuning Technology Configuration options

- Hardware Health Monitor (menu)

  Monitor the Hardware Health.

Advanced > Platform Settings

The Platform Settings menu contains the following options:

- Charging Method (default value: Normal Charging; possible values: Normal Charging, Fast Charging)

  Select charging method as Normal Charging or Fast Charging.

- Scan Matrix Keyboard Support (default value: Enabled; possible values: Enabled, Disabled)

  Enable Scan Matrix Keyboard Support

- EC PECI Mode (default value: Legacy PECI mode; possible values: Legacy PECI mode, PECI over eSPI mode)

  Switch eSPI PECI Mode or Legacy PECI mode

- Power Loss Notification Feature (default value: Default; possible values: Disabled, Enabled, Default)

Enable/Disable Power Loss Notification Feature

- Pmic Vcc IO Level (default value: Disable; possible values: Disable, 1.05V, 1.071V, 1.023V, 0.997V, 0.850V, 0.900V, 0.950V)

  Select the Pmic Vcc IO Voltage Level

- Pmic Vddq Level (default value: Disable; possible values: Disable, 0, 1, 2, 3, 4, 5, 6, 7)

  Select the Pmic Vddq Voltage Level

- CSC Pmic NVM Update Support (default value: Disabled; possible values: Enabled, Disabled)

  Enable/Disable CastroCove Pmic Nvm Update

- Pmic NVM Write Lock Support (default value: Disabled; possible values: Disabled, Enabled)

  Enable/Disable WarrenCove/CastroCove Pmic Nvm Write Lock

- Pmic SlpS0 VM Support (default value: Disabled; possible values: Disabled, Enabled)

  Support to auto check Primium PMIC and disable SlpS0 voltage.

- Power Sharing Manager (default value: Disabled; possible values: Disabled, Enabled)

  Configure the PSM ACPI objects.

- Enable FFU Support (default value: Disabled; possible values: Disabled, Enabled)

  Enable/Disable FFU Support.

- HID Event Filter Driver (default value: Enabled; possible values: Disabled, Enabled)

  Enables/Disables HID Event Filter Driver interface to OS.

- System Time and Alarm Source (default value: ACPI Time and Alarm Device; possible values: ACPI Time and Alarm Device, Legacy RTC)

  Select source of system time and alarm functions. ACPI Time and Alarm (default, legacy RTC disabled) or Legacy RTC support only

- DG Platform Support (default value: Add In Card; possible values: Add In Card, MB Down)

  DG is supported as MotherBoard Down OR Add In Card

- Enable PowerMeter

- Intel Trusted Device Setup Boot (default value: Disabled; possible values: Enabled, Disabled)

  Enables/Disables a Intel Trusted Device Setup Boot on the next boot

- MPDT Support (default value: Disabled; possible values: Disabled, Sensor_BOM1, Sensor_BOM2, Sensor_BOM1 with Companion Chip)

  Enable(Sensor_BOM1,Sensor_BOM2 and Sensor_BOM1 with Companion Chip)/Disable MPDT Support in BIOS

- Closed Lid WoV LED Lighting Support (default value: Disabled; possible values: Disabled, Enabled)

  Disables/Enables Closed Lid WoV LED Lighting Support.

- System Firmware Update Config (menu)

  Config settings for System Firmware Update (Capsule Update)

- VTIO (menu)

  Configure settings for VTIO

- TCSS Platform Setting (menu)

  Configure TCSS Platform Setting

Advanced > ACPI D3Cold settings

The ACPI D3Cold settings menu contains the following options:

- ACPI D3Cold Support (default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable ACPI D3Cold support to be executed on D3 entry and exit

  Note: Disable it would affect the Storage D3 setting

Advanced > BCLK Configuration

The BCLK Configuration menu contains the following options:

- BCLK Source Config (default value: CPU BCLK; possible values: CPU BCLK)

  CPU BCLK is only BCLK Source for ADL.

- BCLK Frequency

Advanced > Console Redirection

The Console Redirection menu contains the following options:

- Console Serial Redirect (default value: Enabled; possible values: Enabled, Disabled)

  Enable Console Redirection Function

Advanced > OnLogic Feature Configuration

The OnLogic Feature Configuration menu contains the following options:

- I225 LAN Controller (default value: Enabled; possible values: Enabled, Disabled)

Enable/Disable I225 LAN controller.

- Wake on Lan (default value: Enabled; possible values: Enabled, Disabled)

  Enable/Disable Wake on Lan

- Pseudo G3 (default value: Disabled; possible values: Enabled, Disabled)

  Enable/Disable Pseudo G3.

  If Pseudo G3 is enabled, "Advanced > PCH-IO Configuration > DeepSx Power Policies" will be set to "Enabled in S4/S5" in the next boot automatically.

Advanced > SIO NCT5124D

The SIO NCT5124D menu contains the following options:

- UART Port 1 Configuration (menu)

  UART Configuration

- UART Port 2 Configuration (menu)

  UART Configuration

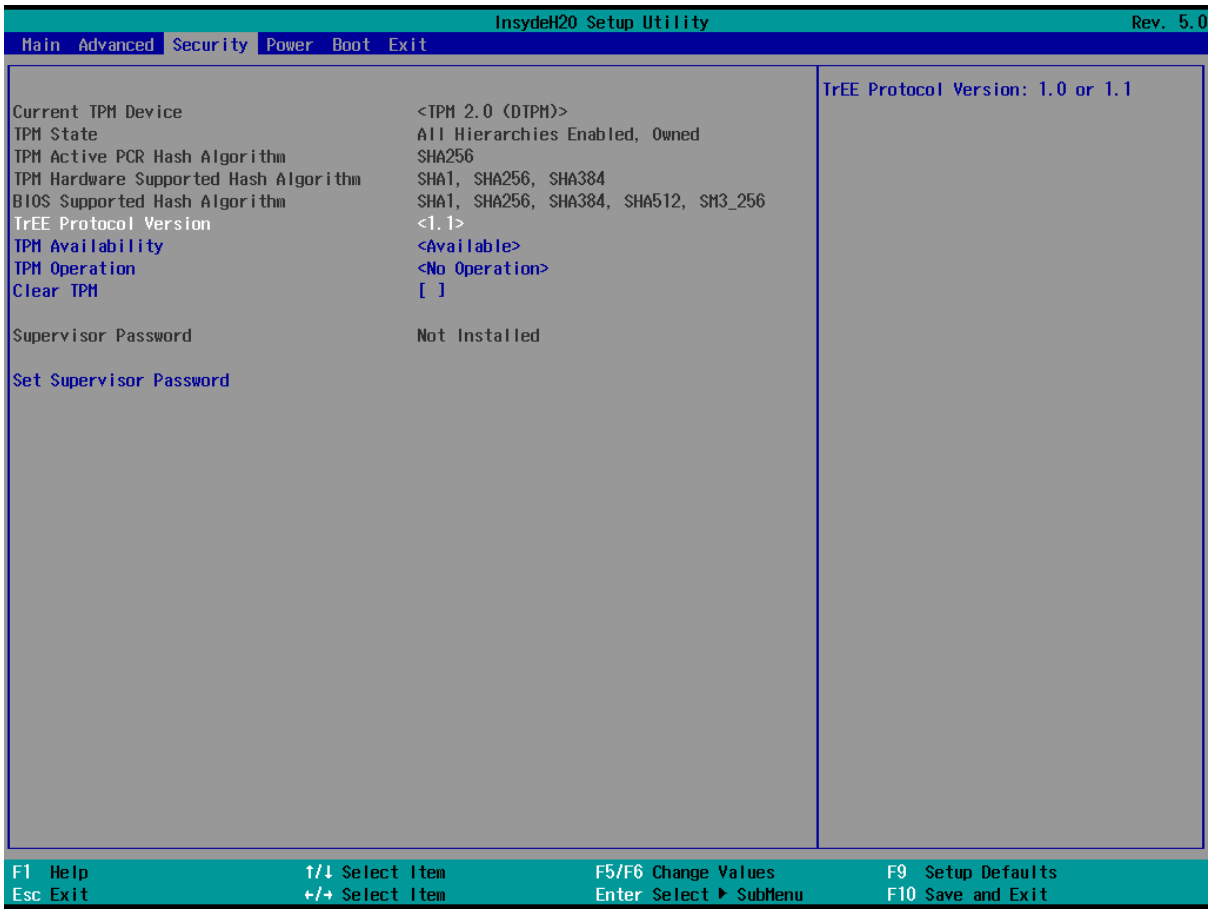
- UART Port 3 Configuration (menu)

  UART Configuration

- UART Port 4 Configuration (menu)

  UART Configuration

Security



The Security menu contains the following options:

- Current TPM Device (read-only; possible values: Not Detected, TPM 1.2, TPM 2.0)

  Current TPM Device: TPM1.2, or TPM2.0.

- TPM Active PCR Hash Algorithm (read-only)

  TPM Active PCR Hash Algorithm: SHA1, SHA256, SHA384, SHA512, SM3_256

- TPM Hardware Supported Hash Algorithm (read-only)

  TPM Hardware Supported Hash Algorithm: SHA1, SHA256, SHA384, SHA512, SM3_256

- BIOS Supported Hash Algorithm (read-only)

  BIOS Supported Hash Algorithm: SHA1, SHA256, SHA384, SHA512, SM3_256

- TrEE Protocol Version (default value: 1.1; possible values: 1.0, 1.1)

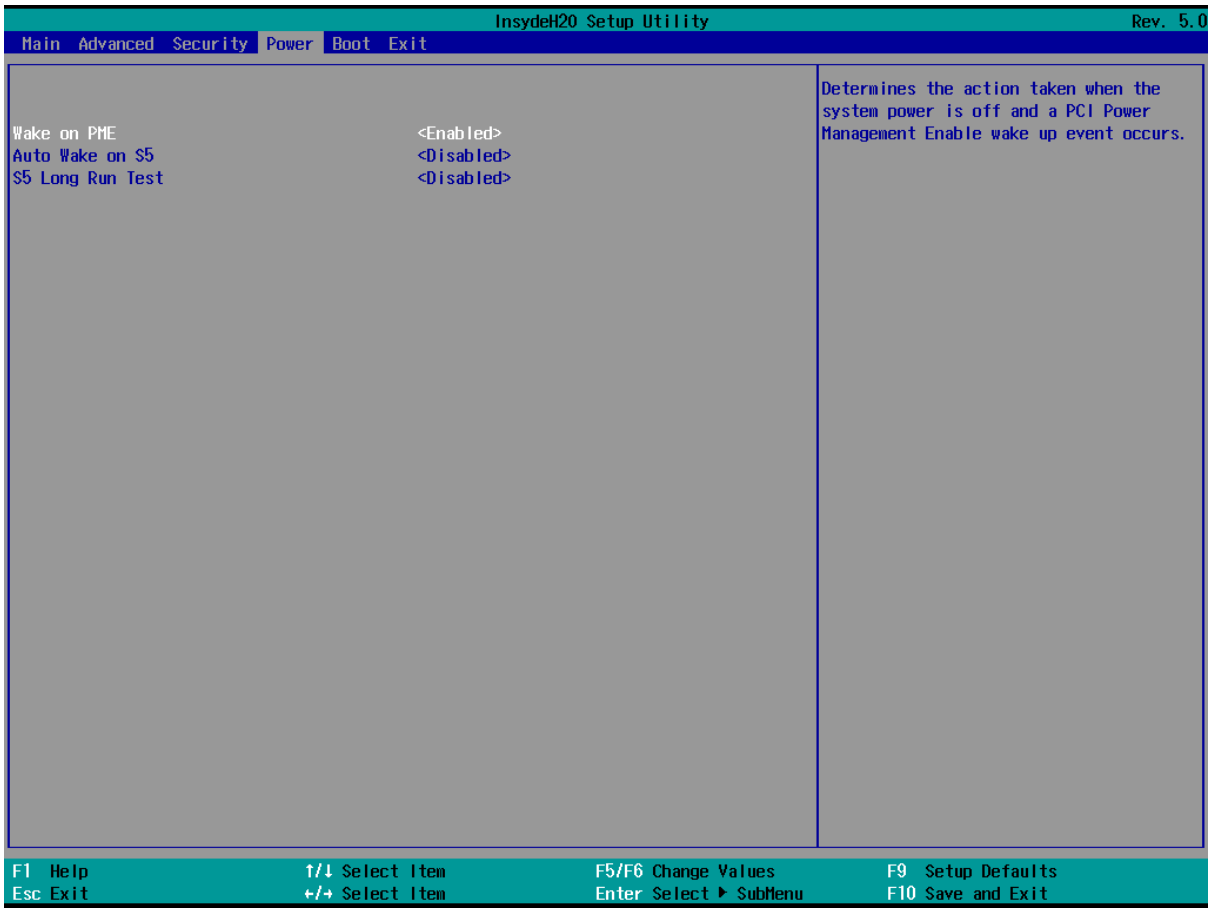
  TrEE Protocol Version: 1.0 or 1.1

- TPM Availability (default value: Available; possible values: Available, Hidden)

  When Hidden, don’t exposes TPM to OS

- Supervisor Password (read-only)

Power



The Power menu contains the following options:

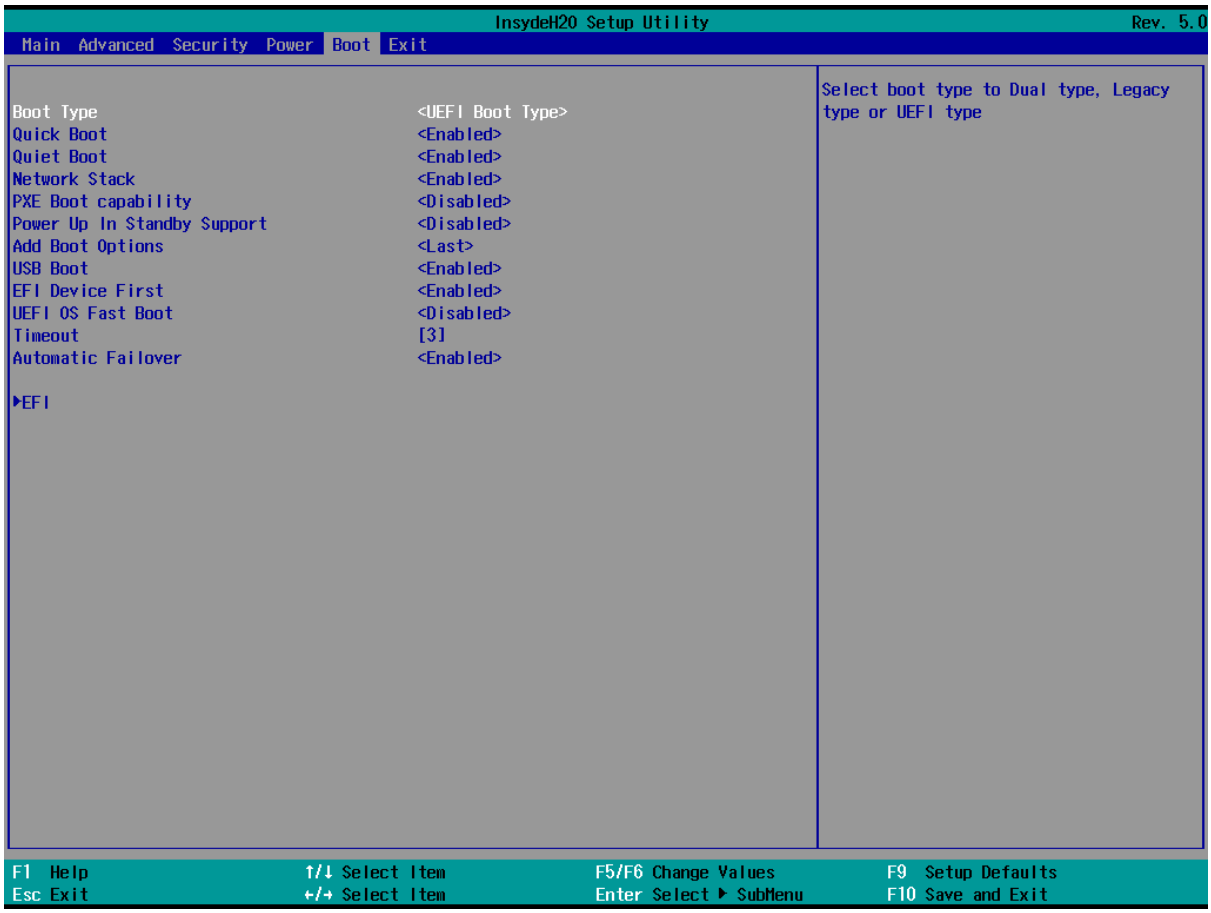
- Wake on PME (default value: Enabled; possible values: Disabled, Enabled)

  Determines the action taken when the system power is off and a PCI Power Management Enable wake up event occurs.

- Auto Wake on S5 (default value: Disabled; possible values: Disabled, By Every Day, By Day of Month)

  Auto wake on S5, By Day of Month or Fixed time of every day

Boot



The Boot menu contains the following options:

- Boot Type (default value: UEFI Boot Type; possible values: Dual Boot Type, Legacy Boot Type, UEFI Boot Type)

  Select boot type to Dual type, Legacy type or UEFI type

- Quick Boot (default value: Enabled; possible values: Enabled, Disabled)

  Allows InsydeH2O to skip certain tests while booting. This will decrease the time needed to boot the system.

- Quiet Boot (default value: Enabled; possible values: Enabled, Disabled)

  Disables or enables booting in Text Mode.

- Network Stack (default value: Disabled; possible values: Disabled, Enabled)

  Network Stack Support:

  Windows 8 BitLocker Unlock

  UEFI IPv4/IPv6 PXE

  Legacy PXE OPROM

- PXE Boot capability (default value: Disabled; possible values: Disabled)

  Disabled : Support Network Stack

  UEFI PXE : IPv4/IPv6

  Legacy : Legacy PXE OPROM only

- Power Up In Standby Support (default value: Disabled; possible values: Enabled, Disabled)

  Disable or enable Power Up In Standby Support.

  The PUIS feature set allows devices to be powered-up into the Standby power management state to minimize inrush current at power-up and to allow the host to sequence the spin-up of devices.

- USB Boot (default value: Enabled; possible values: Enabled, Disabled)

  Disables or enables booting to USB boot devices.

- EFI Device First (default value: Enabled; possible values: Disabled, Enabled)

  Determine EFI device first or legacy device first. If enable, it is EFI device first. If disable, it is Legacy device first.

- UEFI OS Fast Boot (default value: Enabled; possible values: Enabled, Disabled)

  If enabled the system firmware does not initialize keyboard and check for firmware menu key.

- USB Hot Key Support (default value: Disabled; possible values: Disabled, Enabled)

  Enable/Disable to support USB hot key while booting. This will decrease the time needed to boot the system.

- Timeout (default value: 3; possible values: numbers between 0 and 10)

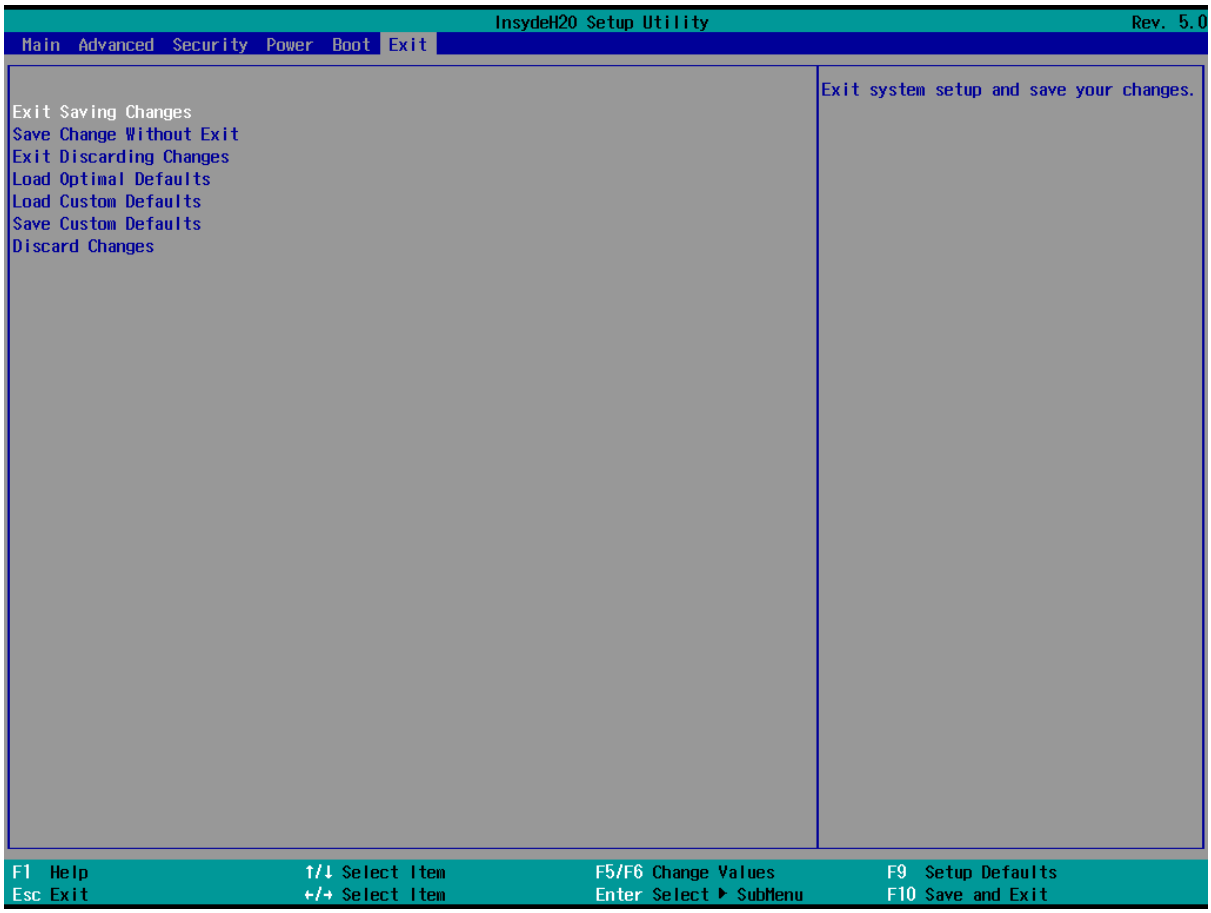
  The number of seconds that the firmware will wait before booting the original default boot selection.

- Automatic Failover (default value: Enabled; possible values: Disabled, Enabled)

  Enable: if boot to default device fail, it will directly try to boot next device.

  Disable: if boot to default device fail, it will pop warning message then go into firmware UI.

Exit



The exit screen provides options to leave the setup utility and to load and save settings.

- Exit Saving Changes: saves the current configuration and restarts the system to apply it
- Save Change Without Exit: saves the current configuration but does not restart the system
- Exit Discarding Changes: returns to the front page without saving or applying the current configuration
- Load Optimal Defaults: loads the factory default configuration
- Load Custom Defaults: loads a previously saved custom configuration
- Save Custom Defaults: saves the current configuration so it can be loaded later
- Discard Changes: restores the current configuration to its original state

MEBx

The Intel AMT configuration utility is password-protected. By default, the password is “admin”, but it must be changed immediately. A strong password using upper- and lower-case letters, symbols, and numbers is required.