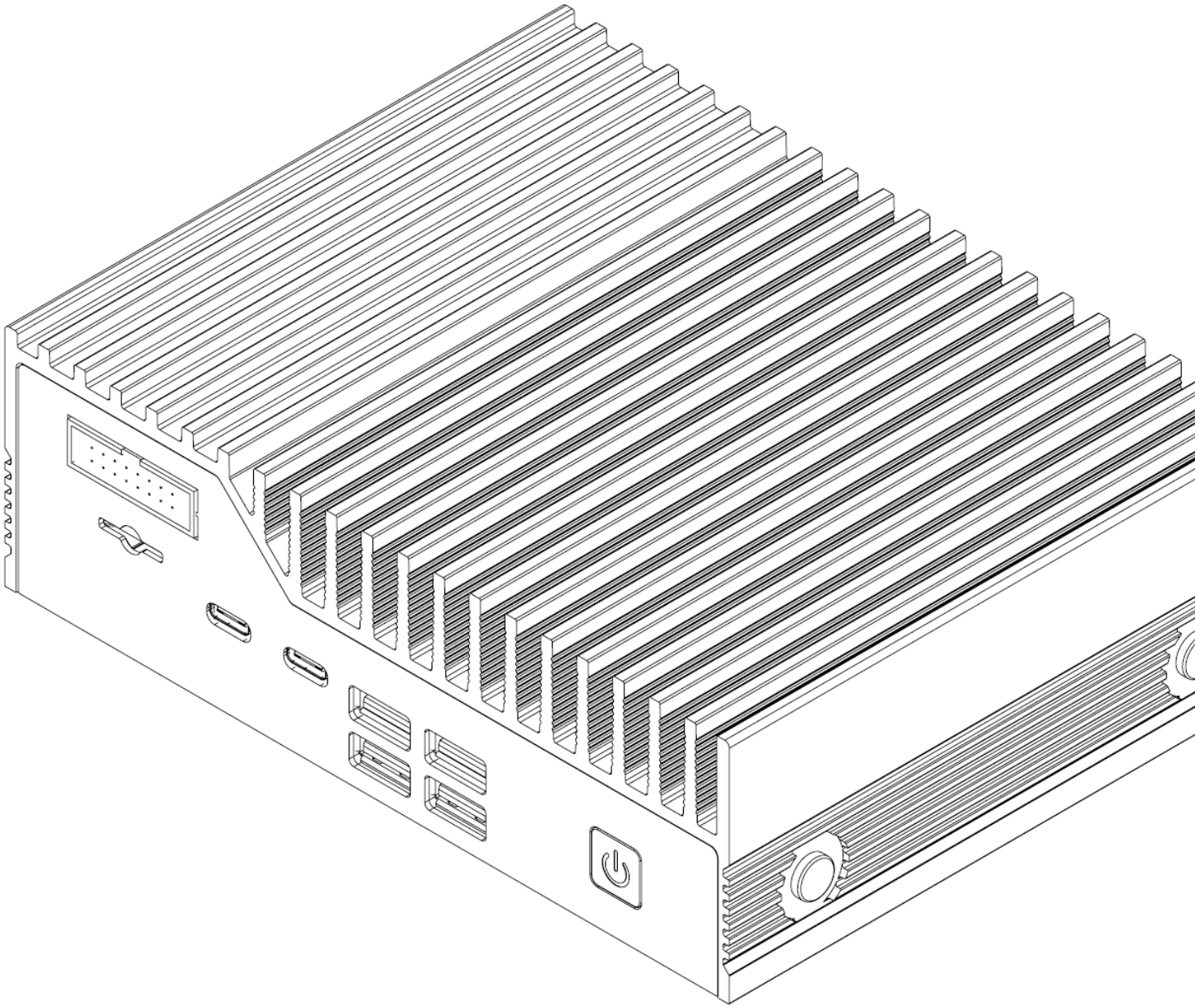
HX401 BIOS Manual

BIOS Version 1.49



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:

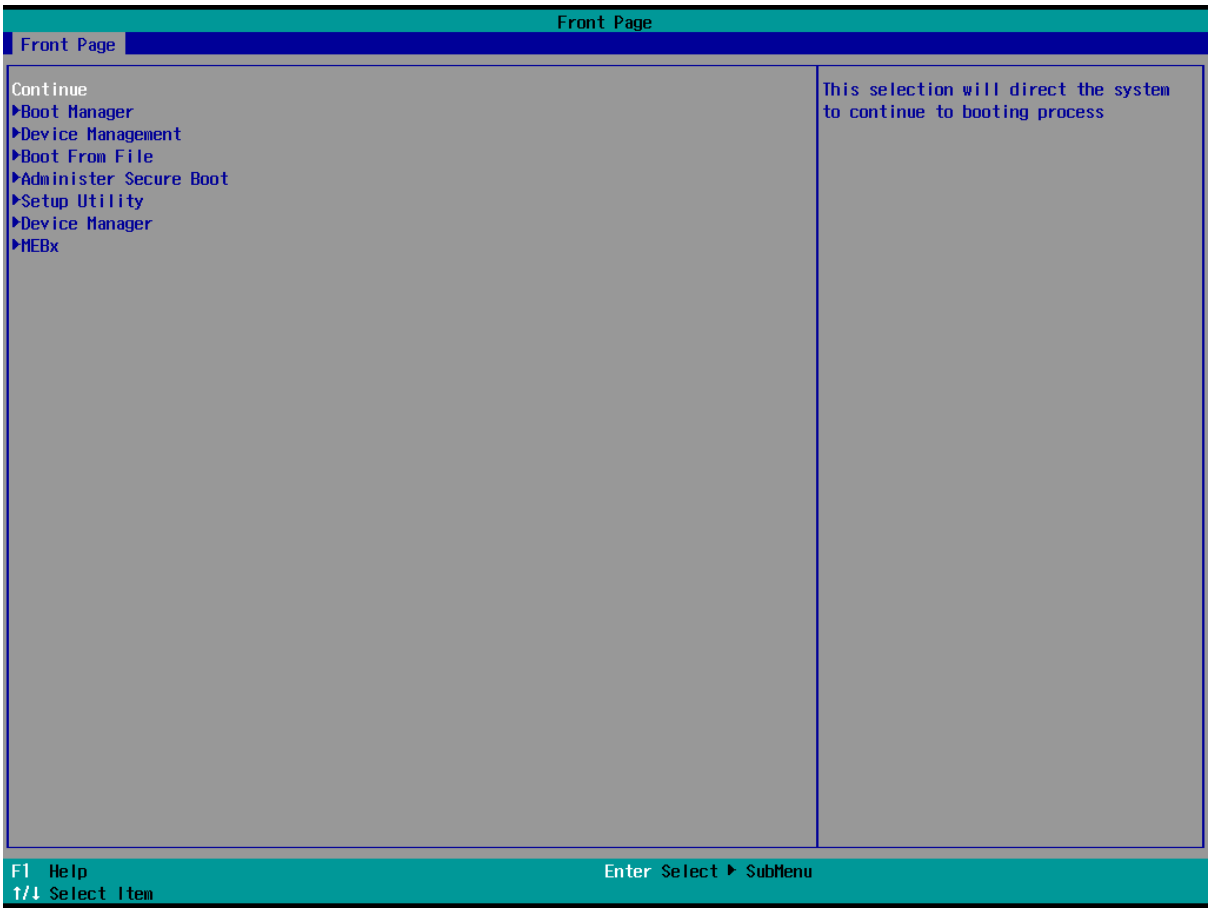
On each menu, the selected option is shown in white, other options are shown in blue, and read-only options are shown in gray. Some menus have multiple screens, which are shown at the top of the screen. The active screen is shown with a gray background and inactive screens are shown with blue backgrounds.

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

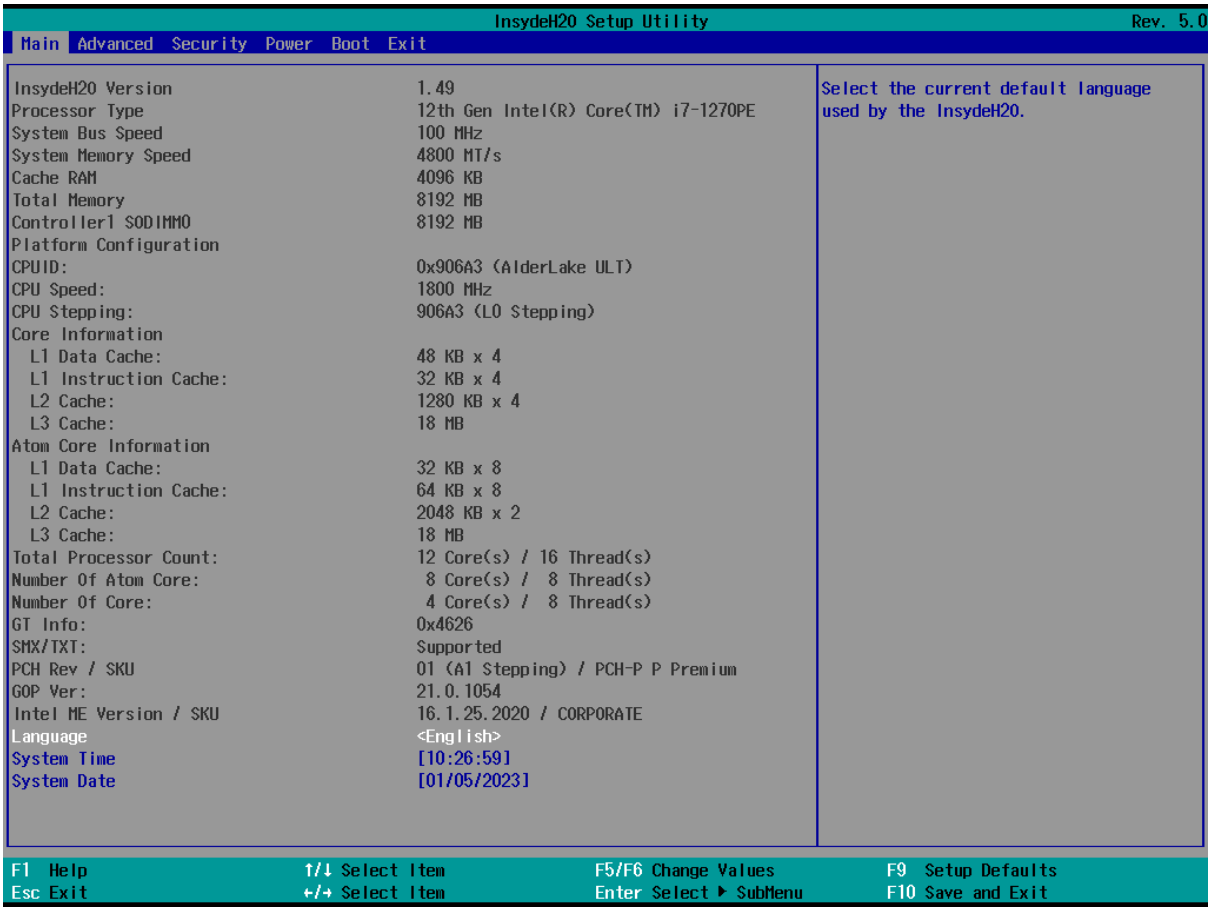
Controls the state the system enters after G3 (power loss). If set to S5, the system remains off when initially connected to power. If set to S0, the system boots when connected to power.

Advanced > PCH-IO Configuration > Wake on LAN Enable

Default value: Enabled; possible values: Enabled, Disabled

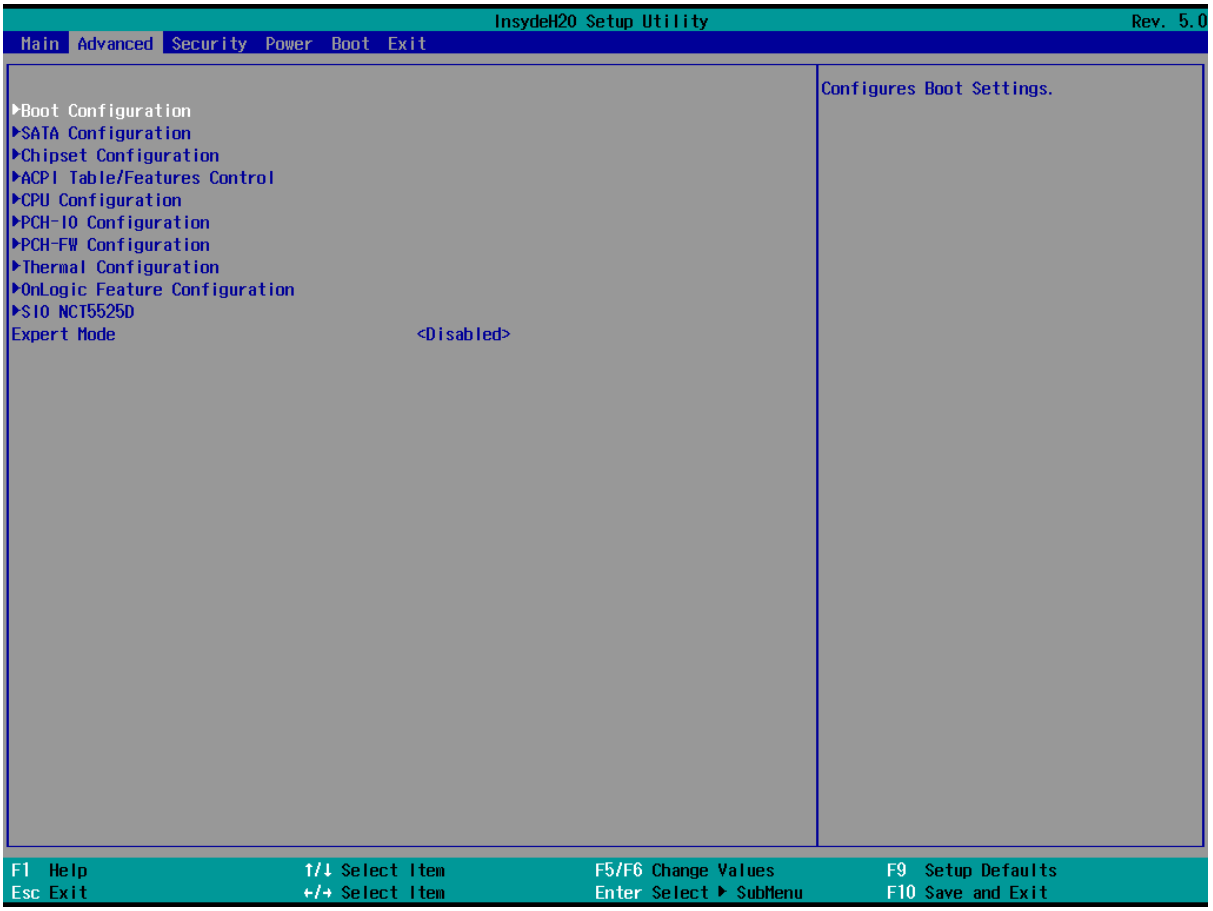
Enables or disables Wake-on-LAN functionality on the onboard network interfaces.

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)
- SATA Configuration (menu)
- Chipset Configuration (menu)
- ACPI Table/Features Control (menu)
- CPU Configuration (menu)
- Functional Safety Configuration (menu)
- PCH-IO Configuration (menu)
- PCH-FW Configuration (menu)
- Thermal Configuration (menu)

- OnLogic Feature Configuration (menu)
- SIO NCT5525D (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 > SATA Configuration

The SATA Configuration menu contains the following options:

- Serial ATA Port 0 (menu)

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 > ACPI Table/Features Control

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

- ACPI Settings (menu)
- 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:

- Performance-core Information (menu)
- 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
- 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.

- 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

- 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

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

- 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 > PCH-IO Configuration

The PCH-IO Configuration menu contains the following options:

- PCI Express Configuration (menu)
- SATA Configuration (menu)
- USB Configuration (menu)
- Security Configuration (menu)
- HD Audio Configuration (menu)
- THC Configuration (menu)
- SerialIo Configuration (menu)

- SCS Configuration (menu)
- ISH Configuration (menu)
- Pch Thermal Throttling Control (menu)
- Skip VCCIN_AUX Configuration (default value: Disabled; possible values: Disabled, Enabled)
  Skips VCCIN_AUX Configuration if enabled
- FIVR Configuration (menu)
- PMC Configuration (menu)
- PCH LAN Controller
- LAN Wake From DeepSx (default value: Enabled; possible values: Enabled, Disabled)
  Wake from DeepSx by the assertion of LAN_WAKE# pin
- Wake on LAN Enable (default value: Enabled; possible values: Enabled, Disabled)
  Enable/Disable integrated LAN to wake the system.
- SLP_LAN# Low on DC Power (default value: Enabled; possible values: Enabled, Disabled)
  Enable/Disable SLP_LAN# Low on DC Power. Please notice this knob only applies to CNVd.
- 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.
- Disable DSX ACPRESENT PullDown (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)
  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)

- 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)

- PTT Configuration (menu)

- FIPS Mode (menu)

- Unique Platform Id Configuration (menu)

- ME Debug Configuration (menu)

- Anti-Rollback SVN Configuration (menu)

- OEM Key Revocation Configuration (menu)

- 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)
- Platform Thermal Configuration (menu)
- Intel(R) Dynamic Tuning Technology Configuration (menu)
- Hardware Health Monitor (menu)

Advanced > OnLogic Feature Configuration

The OnLogic Feature Configuration menu contains the following options:

- I210 LAN Controller (default value: Enabled; possible values: Enabled, Disabled)
  Enable/Disable I210 LAN controller.
- Pseudo G3 (default value: Disabled; possible values: Enabled, Disabled)
  Enabled: BIOS will send a sequence data to MCU. Disabled: Do nothing.
- Retimer Compliance Mode (default value: Disabled; possible values: Enabled, Disabled)
  Enable/Disable Retimer compliance mode.

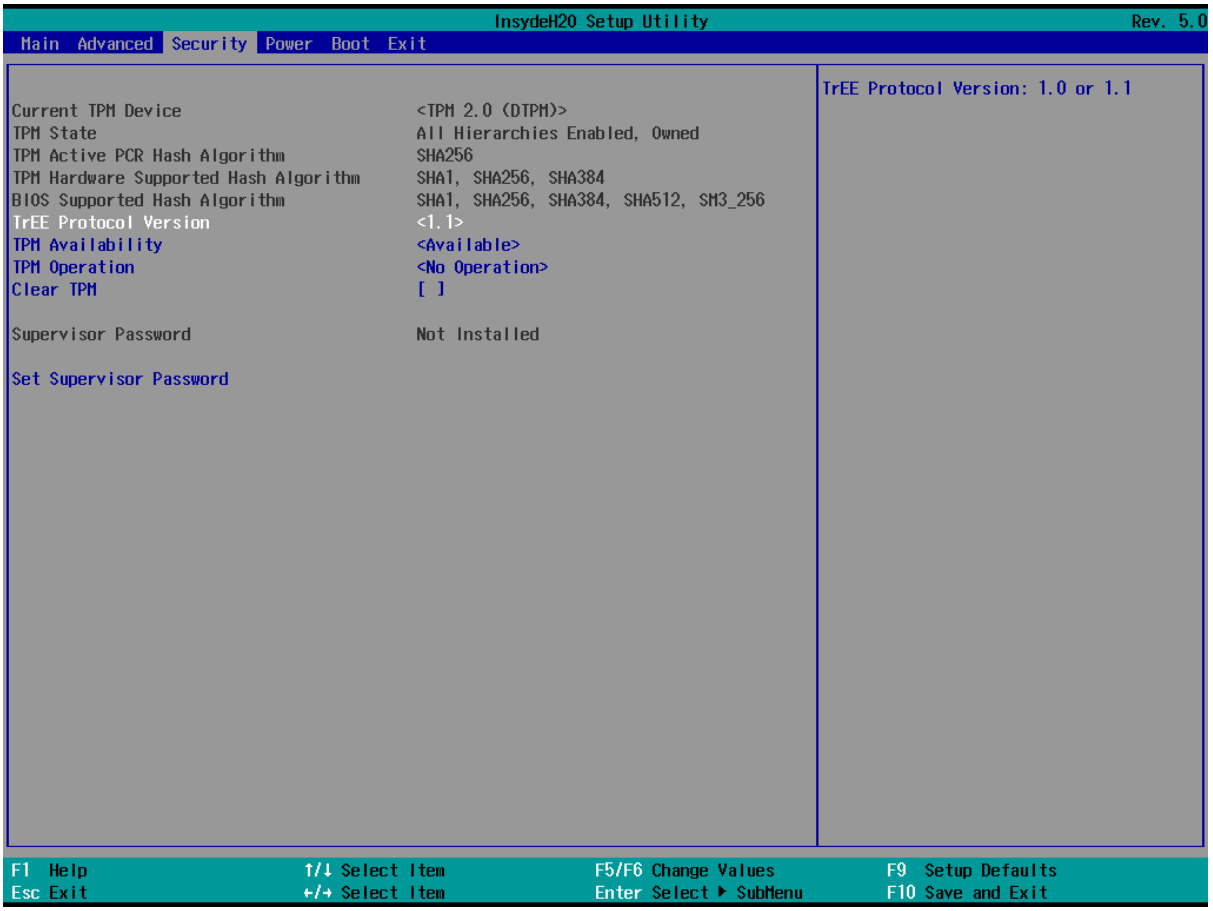
Advanced > SIO NCT5525D

The SIO NCT5525D menu contains the following options:

- UART Port 1 Configuration (menu)

- Hardware Monitor (menu)

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

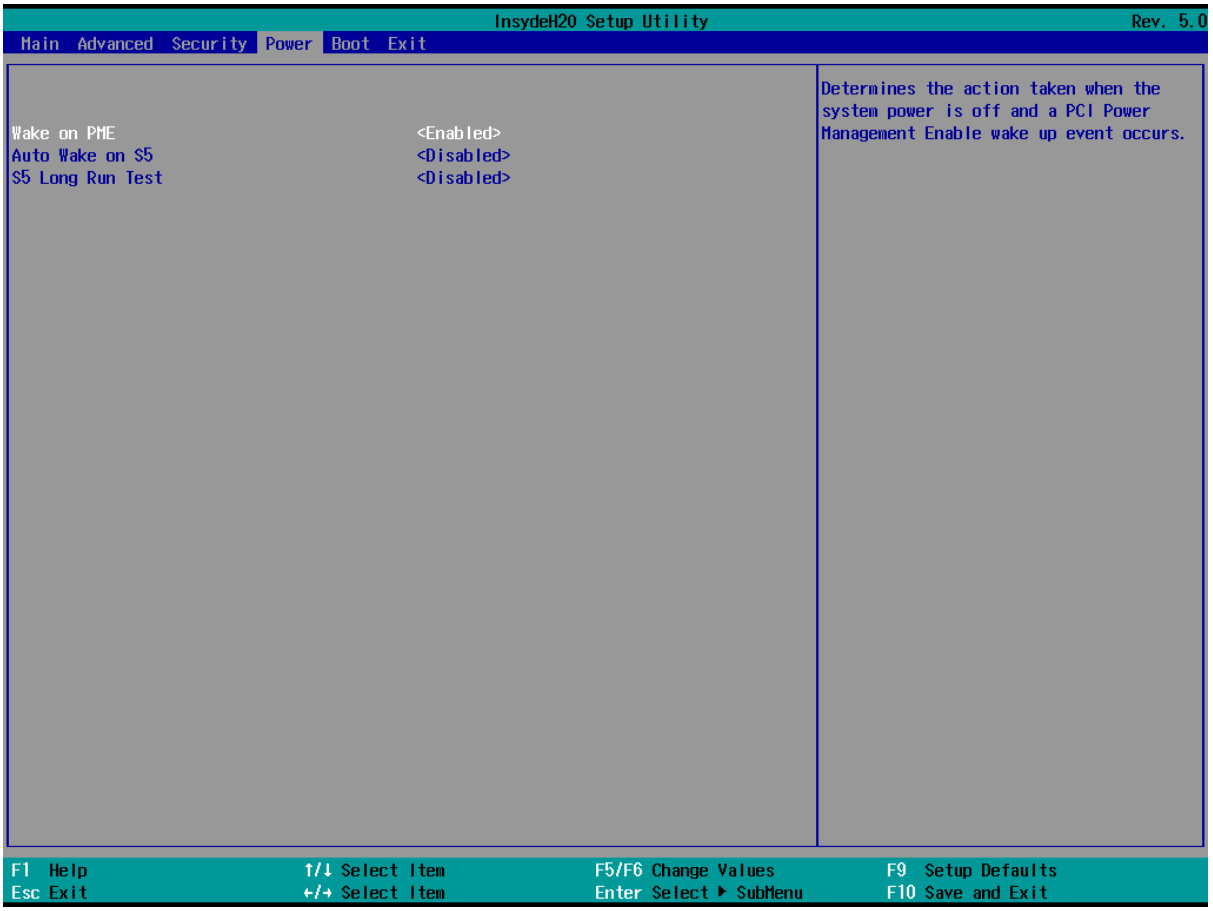
- TrEE Protocol Version (default value: 1.1; possible values: 1.0, 1.1)
  TrEE Protocol Version: 1.0 or 1.1
- TPM Availability (default value: Available; possible values: Available, Hidden)
  When Hidden, don't exposes TPM to OS
- Supervisor Password (read-only)
- Storage Password Setup Page (menu)

Security > Storage Password Setup Page

The Storage Password Setup Page menu contains the following options:

- BlockSID is enabled (read-only)
- BlockSID is disabled (read-only)
- Require physical presence when enable BlockSID (read-only)
- Not require physical presence when disable BlockSID (read-only)
- TCG Storage Action (default value: No Operation; possible values: No Operation, Enable_BlockSIDFunc, Disable_BlockSIDFunc, PPRequiredForEnableBlockSID_True, PPRequiredForEnableBlockSID_False, PPRequiredForDisableBlockSID_True, PPRequiredForDisableBlockSID_False)
  Change BlockSID actions, includes enable or disable BlockSID, Require or not require physical presence when remote enable or disable BlockSID

Power



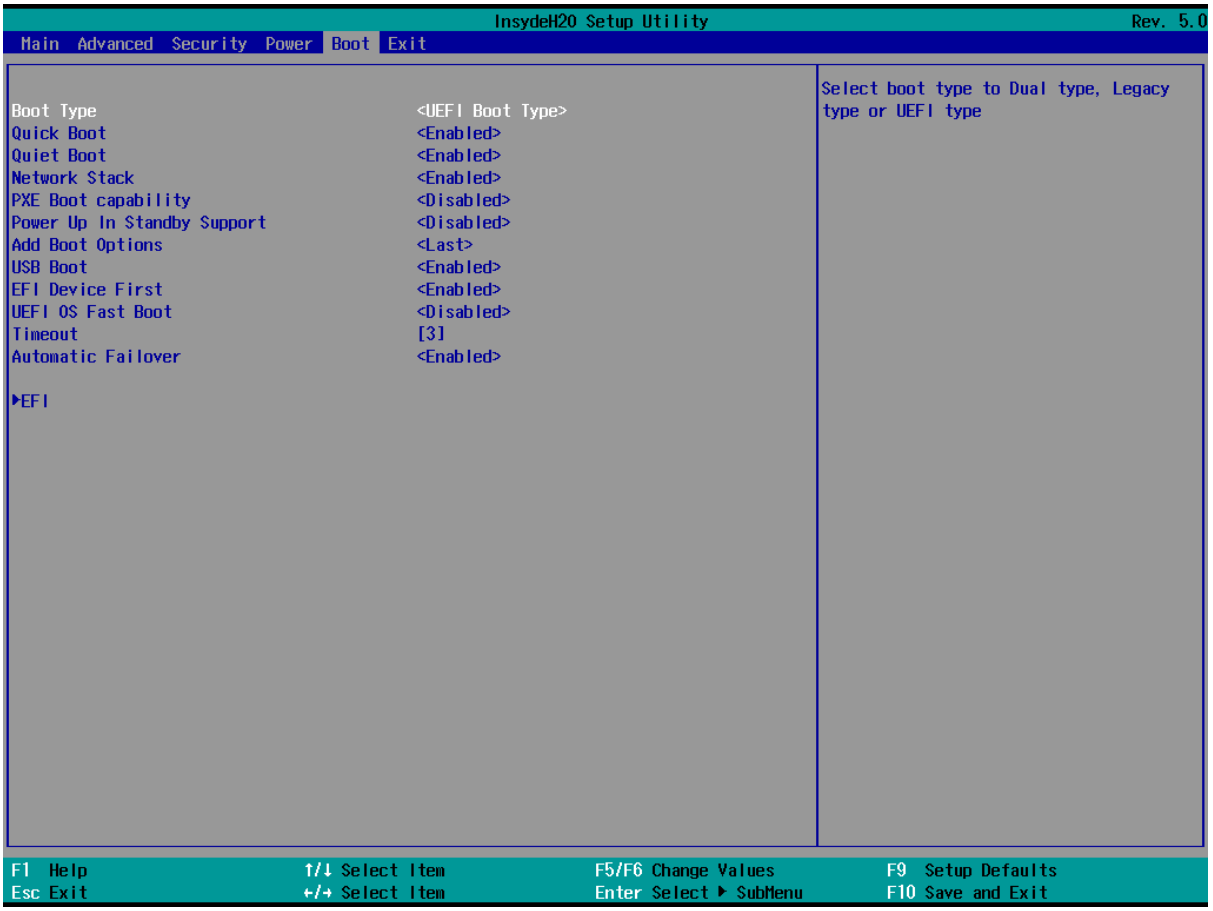
The Power menu contains the following options:

- 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

- S5 Long Run Test (default value: Disabled; possible values: Disabled, Enabled)
  Enable : force to enable RTC S5 wake up, even if OS disables it. Support ipwrtest to do RTC S5 wakeup.

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.

- Add Boot Options (default value: Auto; possible values: First, Last, Auto)
  Position in Boot Order for Shell,Network and Removables

- 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.

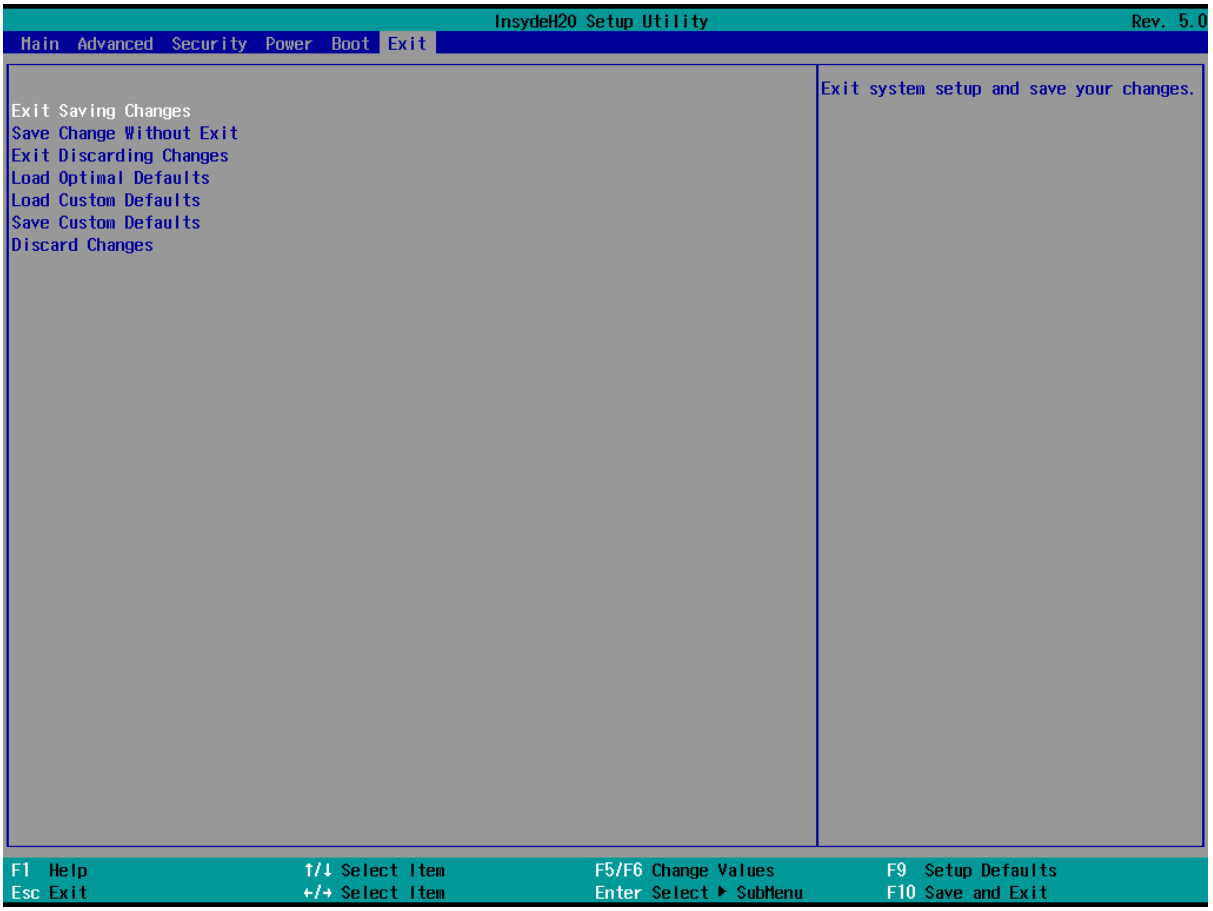
- UEFI OS Fast Boot (default value: Enabled; possible values: Enabled, Disabled)
  If enabled the system firmware does not initialize keyboard and check for firmware menu key.

- 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.

BIOS Updates

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