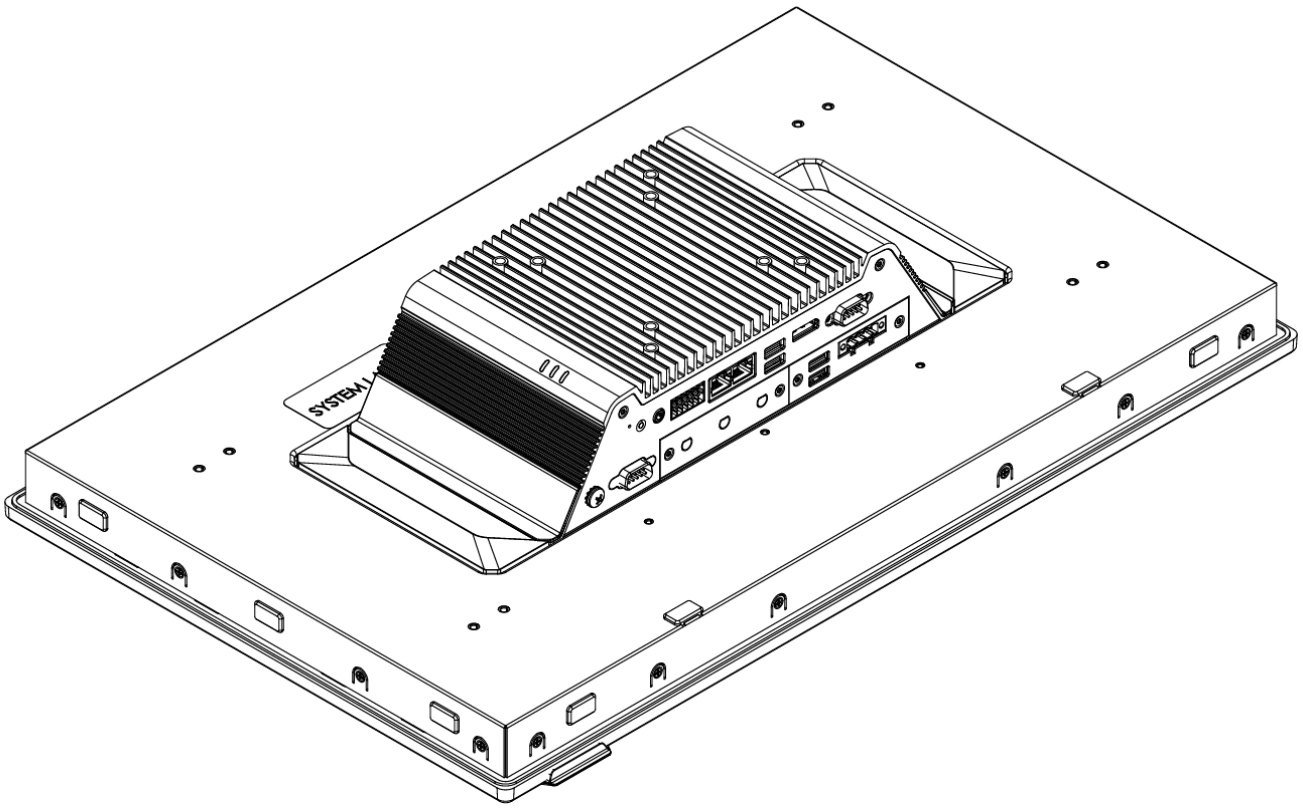
TC401 BIOS Manual

BIOS Version 1.36



Revision History

Revision History	Date
Initial Release	3/25/2024

Table of Contents

Introduction

The UEFI BIOS is a small program that 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 the particular hardware that 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

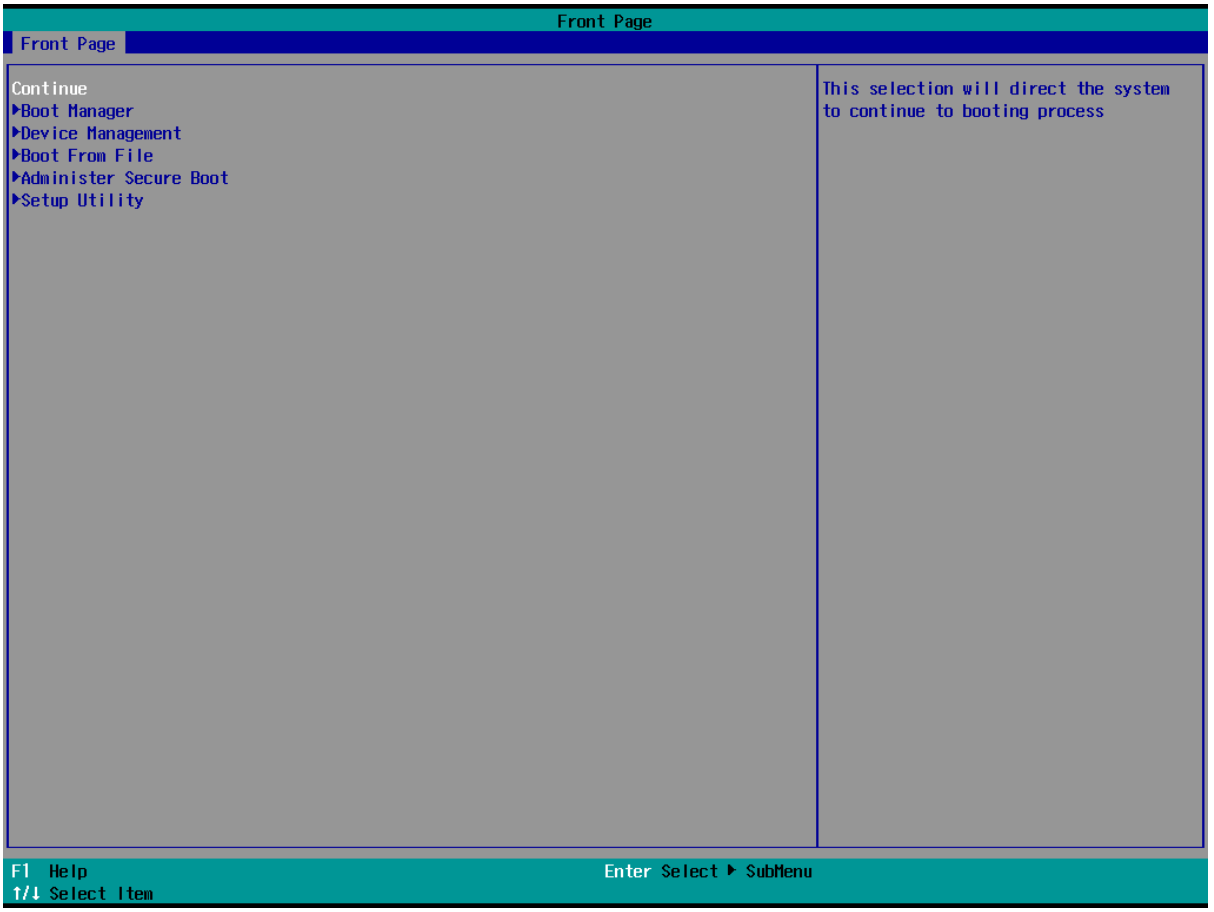
To access the BIOS setup menu, hold the Delete key on the keyboard while turning on the system. After a few seconds, the BIOS front page menu is shown (see below).

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

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

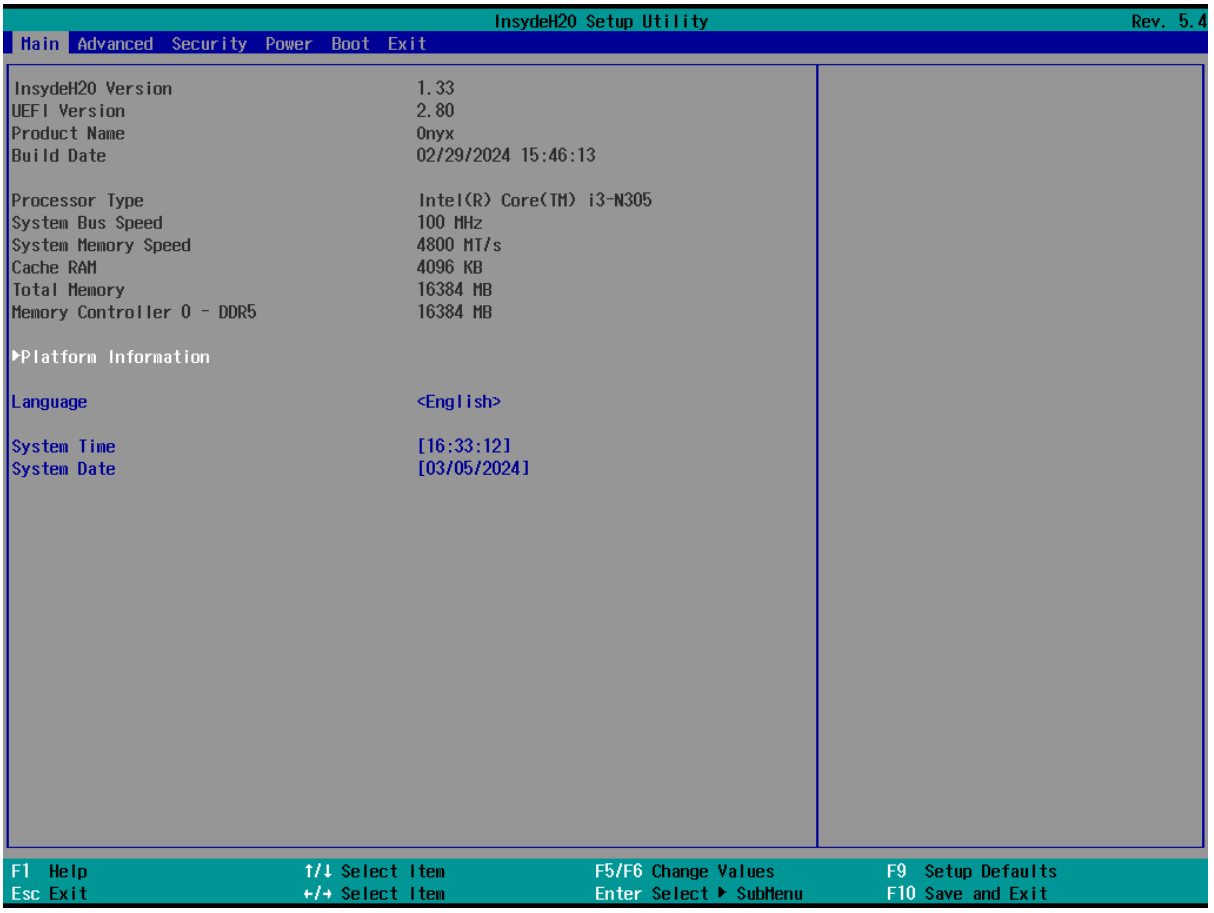
Several configuration options are frequently used.

Advanced > PCH-IO Configuration > State After G3

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

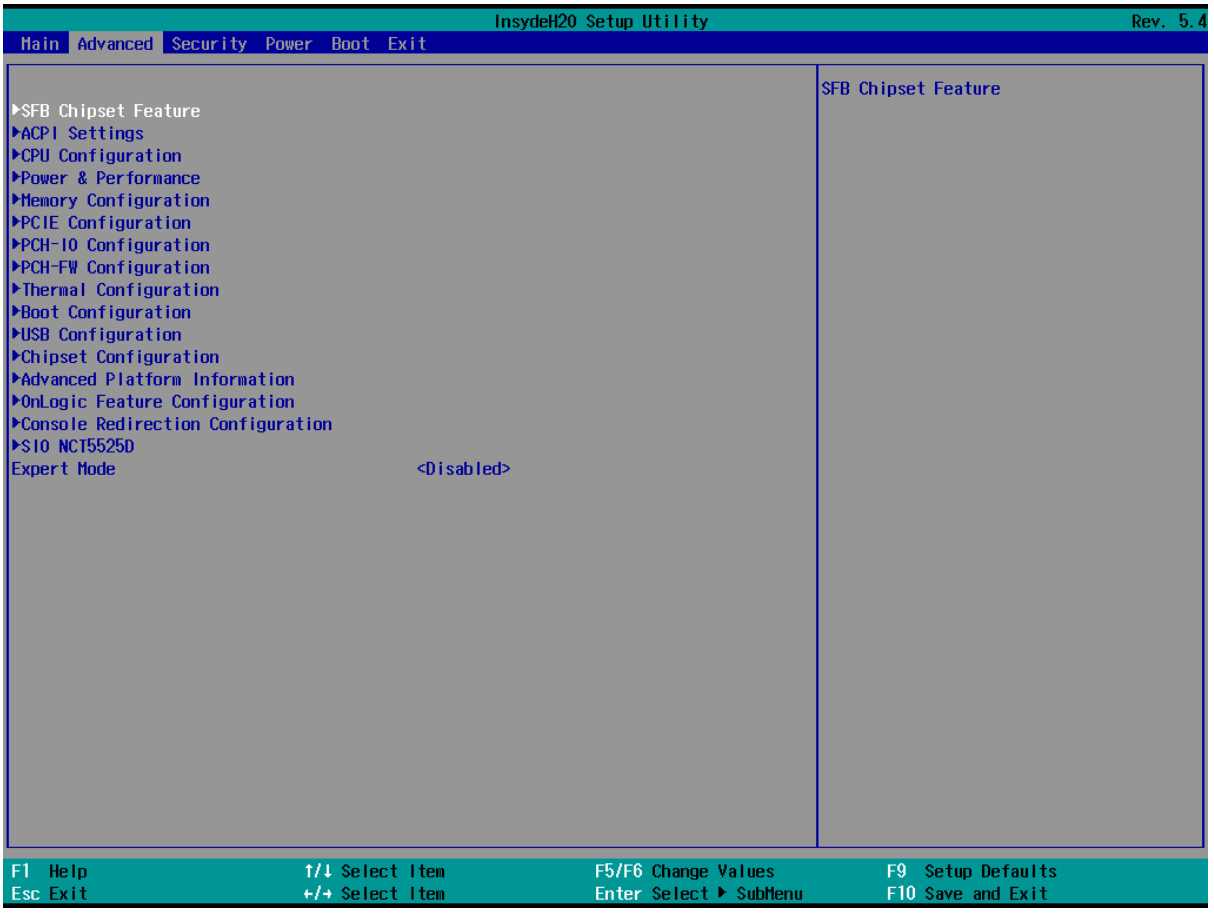
Controls the state the system enters after G3 (power loss). If set to S5, the system remains off when initially connected to power. If set to S0, the system boots when connected to power.

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:

- **SFB Chipset Feature** (menu)

  SFB Chipset Feature

- **ACPI Settings** (menu)

  System ACPI Parameters

- **CPU Configuration** (menu)

  CPU Configuration Parameters

- **Power & Performance** (menu)

  Power & Performance Options

- **Memory Configuration** (menu)

  Memory Configuration Parameters

- **PCIE Configuration** (menu)

PCIE Parameters

- **PCH-IO Configuration** (menu)

  PCH Parameters

- **PCH-FW Configuration** (menu)

  Configure Management Engine Technology Parameters

- **Thermal Configuration** (menu)

  Thermal Configuration Parameters

- **Boot Configuration** (menu)

  Configures Boot Settings.

- **USB Configuration** (menu)

  Configure the USB supp

- **Chipset Configuration** (menu)

  Advanced Chipset Configuration Options.

- **ACPI Table/Features Control** (menu; only in expert mode)

  Configures ACPI Tables/Features setting.

- **Advanced Platform Information** (menu)

  Advanced Platform Information

- **OnLogic Feature Configuration** (menu)

  OnLogic Feature Configuration Menu

- **SIO NCT5525D** (menu)

  SIO NCT5525D configuration menu

- **Console Redirection Configuration** (menu)

  Console Redirection settings.

- **H2O Event Log Config Manager** (menu)

  Show H2O Event Log Config Manager Utility

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

  SCU Expert Mode

Advanced > SFB Chipset Feature

The SFB Chipset Feature menu contains the following options:

- **Rotate Screen** (default value: Disable; possible values: Disable, 90 degrees clockwise, 180 degrees clockwise, 270 degrees clockwise)

  Enable/Disable Rotate Screen feature, support 90 and 270 degrees clockwise

Advanced > ACPI Settings

The ACPI Settings menu contains the following options:

- **ACPI Version**

  ACPI Version details

- **Enable ACPI Auto Configuration** (default value: unchecked; possible values: unchecked, checked)

  Enable or Disable BIOS ACPI Auto Configuration

- **Enable Hibernation** (default value: checked; possible values: unchecked, checked)

  Enables or Disables System ability to Hibernate (OS/S4 Sleep State). This option may not be effective with some OSs

- **PTID Support** (default value: checked; possible values: unchecked, checked)

  PTID Support will be loaded if enabled

- **PECI Access Method** (default value: Direct I/O; possible values: Direct I/O, ACPI)

  PECI Access Method is Direct I/O or ACPI

- **ACPI S3 Support** (default value: Enabled; possible values: Disabled, Enabled)

  Enable ACPI S3 support

- **Native PCIE Enable** (default value: Enabled; possible values: Disabled, Enabled)

  Bit - PCIe Native * control

  0 - ~ Hot Plug

  1 - SHPC Native Hot Plug control

  2 - ~ Power Management Events

  3 - PCIe Advanced Error Reporting control

  4 - PCIe Capability Structure control

5 - Latency Tolerance Reporting control

- **Native ASPM** (default value: Auto; possible values: Auto, Enabled, Disabled)

  Enabled - OS Controlled ASPM, Disabled - BIOS Controlled ASPM

- **D3 Setting for Storage** (default value: D3Hot; possible values: Disabled, D3Hot)

  RTD3 support for Storage. PCIE storage PEP constraint needs to be set as D0/F1 (Intel Advanced -> ACPI Settings -> PEP PCIe Storage) when this setup is disabled/D3Hot

- **Low Power S0 Idle Capability** (default value: Disabled; possible values: Disabled, Enabled)

  This variable determines if we enable ACPI Lower Power S0 Idle Capability (Mutually exclusive with Smart connect). While this is enabled, it also disable 8254 timer for SLP_S0 support

Advanced > CPU Configuration

The CPU Configuration menu contains the following options:

- **Efficient-core Information** (menu)

  Displays the E-core Information

- **Performance-core Information** (menu; disabled)

  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 (only in expert mode; default value: Disabled; possible values: Disabled, Enabled)**

  Enable/Disable CPU Flex Ratio Programming

- **CPU Flex Ratio Settings** (read-only; only in expert mode; 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).

- **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.

- **AP threads Idle Manner** (only in expert mode; default value: MWAIT Loop; possible values: HALT Loop, MWAIT Loop, RUN Loop)

  AP threads Idle Manner for waiting signal to run

- **AES** (only in expert mode; default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable AES (Advanced Encryption Standard)

- **MachineCheck** (only in expert mode; default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable Machine Check

- **MonitorMWait** (only in expert mode; default value: Enabled; possible values: Disabled, Enabled)

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

- **CPU SMM Enhancement** (menu)

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 > Memory Configuration

The Memory Configuration menu contains the following options:

- **Memory Thermal Configuration** (menu; only in expert mode)

  Memory Thermal Configuration Options

- **Memory Training Algorithms** (menu; only in expert mode)

  Enable/Disable Memory Training Algorithms.

- **Memory** (menu; only in expert mode)

  Memory Overclocking Menu

- **Memory RC Version** (only in expert mode)

  Memory RC Version

- **Memory Frequency** (only in expert mode)

  Displays the Frequency of Memory

- **tCL-tRCD-tRP-tRAS** (only in expert mode)

  Memory Timings

- **MC 0 Ch 0 DIMM 0** (only in expert mode)

  Controller Channel Slot Subtitle

- **Size** (only in expert mode)

Memory Size in the Slot.

- **Number of Ranks** (only in expert mode)

  Number of Ranks in the slot

- **Manufacturer** (only in expert mode)

  DIMM / DRAM Manufacturer Value

- **MC 0 Ch 0 DIMM 1** (only in expert mode)

  Controller Channel Slot Subtitle

- **Size** (only in expert mode)

  Memory Size in the Slot.

- **Number of Ranks** (only in expert mode)

  Number of Ranks in the slot

- **Manufacturer** (only in expert mode)

  DIMM / DRAM Manufacturer Value

- **MC 0 Ch 1 DIMM 0** (only in expert mode)

  Controller Channel Slot Subtitle

- **Size** (only in expert mode)

  Memory Size in the Slot.

- **Number of Ranks** (only in expert mode)

  Number of Ranks in the slot

- **Manufacturer** (only in expert mode)

  DIMM / DRAM Manufacturer Value

- **MC 0 Ch 1 DIMM 1** (only in expert mode)

  Controller Channel Slot Subtitle

- **Size** (only in expert mode)

  Memory Size in the Slot.

- **Number of Ranks** (only in expert mode)

  Number of Ranks in the slot

- **Manufacturer** (only in expert mode)

DIMM / DRAM Manufacturer Value

- **MC 0 Ch 2 DIMM 0** (only in expert mode)

  Controller Channel Slot Subtitle

- **Size** (only in expert mode)

  Memory Size in the Slot.

- **Number of Ranks** (only in expert mode)

  Number of Ranks in the slot

- **Manufacturer** (only in expert mode)

  DIMM / DRAM Manufacturer Value

- **MC 0 Ch 2 DIMM 1** (only in expert mode)

  Controller Channel Slot Subtitle

- **Size** (only in expert mode)

  Memory Size in the Slot.

- **Number of Ranks** (only in expert mode)

  Number of Ranks in the slot

- **Manufacturer** (only in expert mode)

  DIMM / DRAM Manufacturer Value

- **MC 0 Ch 3 DIMM 0** (only in expert mode)

  Controller Channel Slot Subtitle

- **Size** (only in expert mode)

  Memory Size in the Slot.

- **Number of Ranks** (only in expert mode)

  Number of Ranks in the slot

- **Manufacturer** (only in expert mode)

  DIMM / DRAM Manufacturer Value

- **MC 0 Ch 3 DIMM 1** (only in expert mode)

  Controller Channel Slot Subtitle

- **Size** (only in expert mode)

Memory Size in the Slot.

- **Number of Ranks** (only in expert mode)

  Number of Ranks in the slot

- **Manufacturer** (only in expert mode)

  DIMM / DRAM Manufacturer Value

- **MC 1 Ch 0 DIMM 0** (only in expert mode)

  Controller Channel Slot Subtitle

- **Size** (only in expert mode)

  Memory Size in the Slot.

- **Number of Ranks** (only in expert mode)

  Number of Ranks in the slot

- **Manufacturer** (only in expert mode)

  DIMM / DRAM Manufacturer Value

- **MC 1 Ch 0 DIMM 1** (only in expert mode)

  Controller Channel Slot Subtitle

- **Size** (only in expert mode)

  Memory Size in the Slot.

- **Number of Ranks** (only in expert mode)

  Number of Ranks in the slot

- **Manufacturer** (only in expert mode)

  DIMM / DRAM Manufacturer Value

- **MC 1 Ch 1 DIMM 0** (only in expert mode)

  Controller Channel Slot Subtitle

- **Size** (only in expert mode)

  Memory Size in the Slot.

- **Number of Ranks** (only in expert mode)

  Number of Ranks in the slot

- **Manufacturer** (only in expert mode)

DIMM / DRAM Manufacturer Value

- **MC 1 Ch 1 DIMM 1** (only in expert mode)

  Controller Channel Slot Subtitle

- **Size** (only in expert mode)

  Memory Size in the Slot.

- **Number of Ranks** (only in expert mode)

  Number of Ranks in the slot

- **Manufacturer** (only in expert mode)

  DIMM / DRAM Manufacturer Value

- **MC 1 Ch 2 DIMM 0** (only in expert mode)

  Controller Channel Slot Subtitle

- **Size** (only in expert mode)

  Memory Size in the Slot.

- **Number of Ranks** (only in expert mode)

  Number of Ranks in the slot

- **Manufacturer** (only in expert mode)

  DIMM / DRAM Manufacturer Value

- **MC 1 Ch 2 DIMM 1** (only in expert mode)

  Controller Channel Slot Subtitle

- **Size** (only in expert mode)

  Memory Size in the Slot.

- **Number of Ranks** (only in expert mode)

  Number of Ranks in the slot

- **Manufacturer** (only in expert mode)

  DIMM / DRAM Manufacturer Value

- **MC 1 Ch 3 DIMM 0** (only in expert mode)

  Controller Channel Slot Subtitle

- **Size** (only in expert mode)

Memory Size in the Slot.

- **Number of Ranks** (only in expert mode)

  Number of Ranks in the slot

- **Manufacturer** (only in expert mode)

  DIMM / DRAM Manufacturer Value

- **MC 1 Ch 3 DIMM 1** (only in expert mode)

  Controller Channel Slot Subtitle

- **Size** (only in expert mode)

  Memory Size in the Slot.

- **Number of Ranks** (only in expert mode)

  Number of Ranks in the slot

- **Manufacturer** (only in expert mode)

  DIMM / DRAM Manufacturer Value

- **Debug Valu**e (only in expert mode; default value: 0; possible values: numbers between 0 and 4294967295)

  Debug Value

- **MRC ULT Safe Config** (only in expert mode; default value: Disabled; possible values: Disabled, Enabled)

  MRC ULT Safe Config for PO

- **LPDDR DqDqs Re-Training** (only in expert mode; default value: Enabled; possible values: Disabled, Enabled)

  Disable/Enable LPDDR DqDqs Re Training

- **Safe Mode Support** (only in expert mode; 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** (only in expert mode; default value: Enabled; possible values: Disabled, Enabled)

  Enable Or Disable Base Memory Test Run on Warm Boot

- **Maximum Memory Frequency** (only in expert mode; 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** (only in expert 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** (only in expert mode; 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** (only in expert mode; 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** (only in expert mode; 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** (only in expert mode; 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** (only in expert mode; 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** (only in expert mode; default value: 96; possible values: numbers between 0 and 65535)

  LCT Cmd Eye Width 0= Auto

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

  Size to set HOB Buffer

- **ECC Support** (only in expert mode; default value: Enabled; possible values: Disabled, Enabled)

  Enable/disable DDR Ecc Support

- **Error Injection Address Match** (only in expert mode; default value: 0; possible values: numbers between 0 and 8589934591 in steps of 64)

  Address to match against for ECC error injection

- **Error Injection Mask** (only in expert mode; default value: 0; possible values: numbers between 0 and 8589934591)

  Mask to match against for ECC error injection

- **Error Injection Insertion Count** (only in expert mode; default value: 15; possible values: numbers between 0 and 4294967295)

  Number of transactions between ECC error injection

- **Max TOLUD** (only in expert mode; 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** (only in expert mode; 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.

- **Gear Ratio** (only in expert mode; default value: 0; possible values: numbers between 0 and 4)

  Gear ratio when SAGV is disabled. 0-Auto, 1-G1, 2-G2, 4-G4

- **First Point Frequency** (only in expert mode; 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** (only in expert mode; 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** (only in expert mode; 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** (only in expert mode; 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** (only in expert mode; 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** (only in expert mode; 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** (only in expert mode; 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** (only in expert mode; 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** (only in expert mode; 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** (only in expert mode; 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** (only in expert mode; 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** (only in expert mode; 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** (only in expert mode; 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** (only in expert mode; 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** (only in expert mode; default value: Enabled; possible values: Disabled, Enabled)

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

- **DDR4_1DPC** (only in expert mode; 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** (only in expert 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** (only in expert mode; 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** (only in expert mode; 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** (only in expert mode; default value: NORMAL Refresh; possible values: NORMAL Refresh, 2x Refresh, 4x Refresh)

  Select refresh rate on the MC

- **Refresh Watermarks** (only in expert mode; default value: High; possible values: Low, High)

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

- **LPDDR ODT RttWr** (only in expert mode; 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** (only in expert mode; 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) (only in expert mode; default value: Enabled; possible values: Disabled,

Enabled)

Exit On Failure for MRC training steps

- **New Features 1 - MRC** (only in expert mode; default value: Disabled; possible values: Disabled, Enabled)

  Enabling/Disabling Generic New Features 1

- **New Features 2 - MRC** (only in expert mode; default value: Disabled; possible values: Disabled, Enabled)

  Enabling/Disabling Generic New Features 2

- **Ch Hash Override** (only in expert mode; default value: Disabled; possible values: Disabled, Enabled)

  Override Channel Hash settings

- **Ch Hash Support** (read-only; only in expert mode; possible values: Disabled, Enabled)

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

- **Ch Hash Mask** (read-only; only in expert mode; 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; only in expert mode; 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** (only in expert mode; default value: Enabled; possible values: Disabled, Enabled)

  Enable/disable Extended Bank Hashing.

- **Per Bank Refresh** (only in expert mode; 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** (only in expert mode; default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable VC1 Read Metering Feature (RdMeter)

- **Strong Weak Leaker** (only in expert mode; default value: 7; possible values: numbers between 1 and 7)

Value for StrongWkLeaker

- **Power Down Mode** (only in expert mode; default value: Auto; possible values: Auto, No Power Down, APD, PPD-DLLoff)

  CKE Power Down Mode Control

- **Pwr Down Idle Timer** (only in expert mode; 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** (only in expert mode; default value: Enabled; possible values: Enabled, Disabled)

  Page Close Idle Timeout Control

- **Memory Scrambler** (only in expert mode; default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable Memory Scrambler support.

- **Force ColdReset** (only in expert mode; 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** (only in expert mode; default value: Enabled; possible values: Enabled, Disabled)

  Controller 0, Channel 0 Control - Enable or Disable Controller 0, Channel 0.

- **Controller 0, Channel 1 Control** (only in expert mode; default value: Enabled; possible values: Enabled, Disabled)

  Controller 0, Channel 1 Control - Enable or Disable Controller 0, Channel 1.

- **Controller 0, Channel 2 Control** (only in expert mode; default value: Enabled; possible values: Enabled, Disabled)

  Controller 0, Channel 2 Control - Enable or Disable Controller 0, Channel 2.

- **Controller 0, Channel 3 Control** (only in expert mode; default value: Enabled; possible values: Enabled, Disabled)

  Controller 0, Channel 3 Control - Enable or Disable Controller 0, Channel 3.

- **Controller 1, Channel 0 Control** (only in expert mode; default value: Enabled; possible values: Enabled, Disabled)

Controller 1, Channel 0 Control - Enable or Disable Controller 1, Channel 0.

- **Controller 1, Channel 1 Control** (only in expert mode; default value: Enabled; possible values: Enabled, Disabled)

  Controller 1, Channel 1 Control - Enable or Disable Controller 1, Channel 1.

- **Controller 1, Channel 2 Control** (only in expert mode; default value: Enabled; possible values: Enabled, Disabled)

  Controller 1, Channel 2 Control - Enable or Disable Controller 1, Channel 2.

- **Controller 1, Channel 3 Control** (only in expert mode; default value: Enabled; possible values: Enabled, Disabled)

  Controller 1, Channel 3 Control - Enable or Disable Controller 1, Channel 3.

- **Force Single Rank** (only in expert mode; default value: Disabled; possible values: Disabled, Enabled)

  When enabled, only Rank 0 will be used in each DIMM

- **In-Band ECC Suppor**t (default value: Disabled; possible values: Disabled, Enabled)

  Enable/Disable In-Band ECC. Will be enabled if memory has symmetric configuration

- **Memory Remap** (only in expert mode; default value: Enabled; possible values: Enabled, Disabled)

  Enable/Disable Memory Remap above 4GB

- **Time Measure** (only in expert mode; default value: Disabled; possible values: Disabled, Enabled)

  Enable/Disable printing of the time it takes to execute MRC.

- **Fast Boot** (only in expert mode; default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable fast path thru the MRC

- **Rank Margin Tool Per Task** (only in expert mode; default value: Disabled; possible values: Disabled, Enabled)

  Enables/Disables RMT running at every major training step

- **Training Tracing** (only in expert mode; default value: Disabled; possible values: Disabled, Enabled)

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

- **Lpddr Mem WL Set** (only in expert mode; 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; only in expert mode; 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** (only in expert mode; 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** (only in expert mode; default value: Disabled; possible values: Disabled, Enabled)

  Enable/Disable ECC DFT feature

- **Write0** (only in expert mode; default value: Disabled; possible values: Disabled, Enabled)

  Write0 feature for LP5/DDR5

- **Periodic DCC** (only in expert mode; default value: Disabled; possible values: Disabled, Enabled)

  Enable / Disable Periodic DCC

- **LPMode** (only in expert mode; default value: Auto; possible values: Auto, Enabled, Disabled)

  Control LPMode feature

- **PPR Enable** (only in expert mode; default value: Disabled; possible values: Disabled, Hard PPR)

  PPR permanently repairs failed rows (if possible).

- **SAM Overloading** (only in expert mode; default value: Disabled; possible values: Disabled, Enabled)

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

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
- **Pch Thermal Throttling Control** (menu; only in expert mode)

  Pch Thermal Throttling Control
- **TSN GBE Configuration** (menu; disabled)

  Time Sensitive Network GBE Configuration.
- **DeepSx Power Policies** (default value: Disabled; possible values: Disabled, Enabled in S4-S5, Enabled in S5)

  configure the DeepSx Mode configuration.
- **State After G3** (default value: S5 State; possible values: S0 State, S5 State)

  Specify what state to go to when power is re-applied after a power failure (G3 state).

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

- **PTT Configuration** (menu)

  Configure PTT

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

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 > 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

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:

- **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

- **FACP - Fixed Power Button** (default value: Enabled; possible values: Disabled, Enabled)

  Enable/Disable the FACP Fixed Power Button feature. If S0Ix is enabled, the fixed power button will be disabled.

- **DSDT - APIC Power Button** (default value: Enabled; possible values: Disabled, Enabled, Auto)

  Controls the APIC power button, please disable this option if fixed power button is enabled for FWTS.

Advanced > Advanced Platform Information

The Advanced Platform Information menu contains the following options:

- **Memory Information** (menu)

  Memory Information

- **NVM Express Information** (menu)

  NVM Express Information
- **PCI Device Information** (menu)

  PCI Device Information
- **CPU Information** (menu)

  CPU Information
- **SATA Drive Information** (menu)

  SATA Drive Information
- **USB Device Viewer** (menu)

  Shows information of all attached USB devices

Advanced > OnLogic Feature Configuration

The OnLogic Feature Configuration menu contains the following options:

- **I226 LAN Controller** (default value: Enabled; possible values: Enabled, Disabled)

  Enable/Disable I226 LAN controller.
- **Pseudo G3** (default value: Disabled; possible values: Enabled, Disabled)

  Enable/Disable Pseudo G3.
- **Prevent boot when no display detected** (default value: Disabled; possible values: Enabled, Disabled)

  Enable: Prevent boot

  Disable: Allow boot
- **Intrusion Detect** (default value: Disabled; possible values: Enabled, Disabled)

  Enable/Disable Intrusion Detect.
- **Wake on LAN** (default value: Enabled; possible values: Enabled, Disabled)

  Enable/Disable Wake on LAN.

Advanced > Console Redirection Configuration

The Console Redirection Configuration menu contains the following options:

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

  Enable or disable the serial console redirection function.

- **Terminal Type** (default value: VT_100; possible values: VT_100, VT_100+, VT_UTF8, PC_ANSI, LOG_TERM, TTY_TERM, LINUX_TERM, XTERM_R6, VT_400, SCO_TERM)

  Select the target terminal emulation type for console redirection.

- **Baud Rate** (default value: 115200; possible values: 115200, 57600, 38400, 19200, 9600, 4800, 2400, 1200)

  Select the baud rate for console redirection.

- **Data Bits** (default value: 8 Bits; possible values: 7 Bits, 8 Bits)

  Select the data transmission size for console redirection.

- **Parity** (default value: None; possible values: None, Even, Odd, Mark, Space)

  Select an option for sending parity bits with regular data bits to detect data transmission errors.

- **Stop Bits** (default value: 1 Bit; possible values: 1 Bit, 2 Bits)

  Select a stop bit to indicate the end of a serial data packet.

- **Flow Control** (default value: None; possible values: None, RTS/CTS, XON/XOFF)

  Select the flow control for console redirection.

- **Information Wait Time** (default value: 5 Seconds; possible values: 0 Second, 2 Seconds, 5 Seconds, 10 Seconds, 30 Seconds)

  Set Console Redirection port information display time.

- **C.R. After Legacy Boot** (default value: Yes; possible values: Yes, No)

  Console Redirection continue works after Legacy Boot.

  Text Mode Resolution (default value: AUTO; possible values: AUTO, Force 80x25, Force 80x24 (DEL FIRST ROW), Force 80x24 (DEL LAST ROW), Limit 128x40)

  Console Redirection Text Mode Resolution. Changing this setting will affect the VGA resolution.

  Auto:

  Follow VGA text mode.

  Force 80x25:

  Don't care VGA, force text mode be 80x25 (VGA 640x480).

Force 80x24 (DEL FIRST ROW):

Don't care VGA, force text mode be 80x24, Del First Row.

Force 80x24 (DEL LAST ROW):

Don't care VGA, force text mode be 80x24, Del Last Row.

Limit 128x40:

Limit the VGA max text mode on 128x40 (VGA 1024x768).

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

  When feature enable, screen will be auto refresh once after detect remote terminal was connected.

  Auto adjust Terminal resolution (default value: Enabled; possible values: Disabled, Enabled)

  Through send extra ESC sequencs code to adjust terminal resolution to fit host screen.

  Supporting terminals:

  1.PuTTY:

  Please uncheck the "Disable remote-controlled terminal resizing" in Terminal->Features setting.

  2.Tera Term:

  Please check the "Term Size = win size" in Setup->Terminal.

- **CR Policy Override** (menu)

  Override the CR policy

Advanced > SIO NCT5525D

The SIO NCT5525D menu contains the following options:

- **UART Port 1 Configuration** (menu)

  UART Configuration

- **UART Port 2 Configuration** (menu)

  UART Configuration

- **Hardware Monitor** (menu)

  Monitor all hardware sensors like voltage/temperature/fan speed

Advanced > H2O Event Log Config Manager

The H2O Event Log Config Manager menu contains the following options:

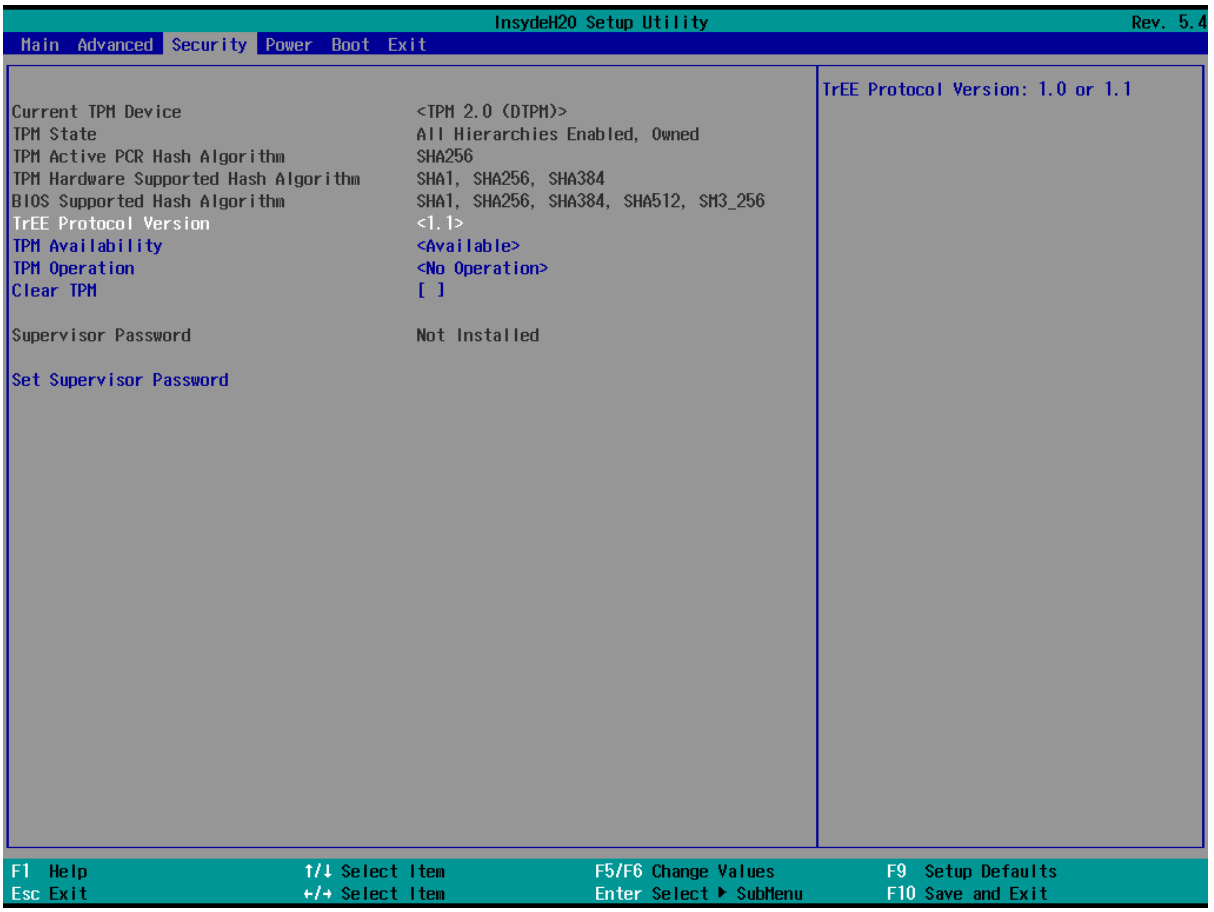
- **Configuration Pages** (menu)

  Show all of the configuration pages.

- **Event And Message Pages** (menu)

  Show all of the Event And Message pages.

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)

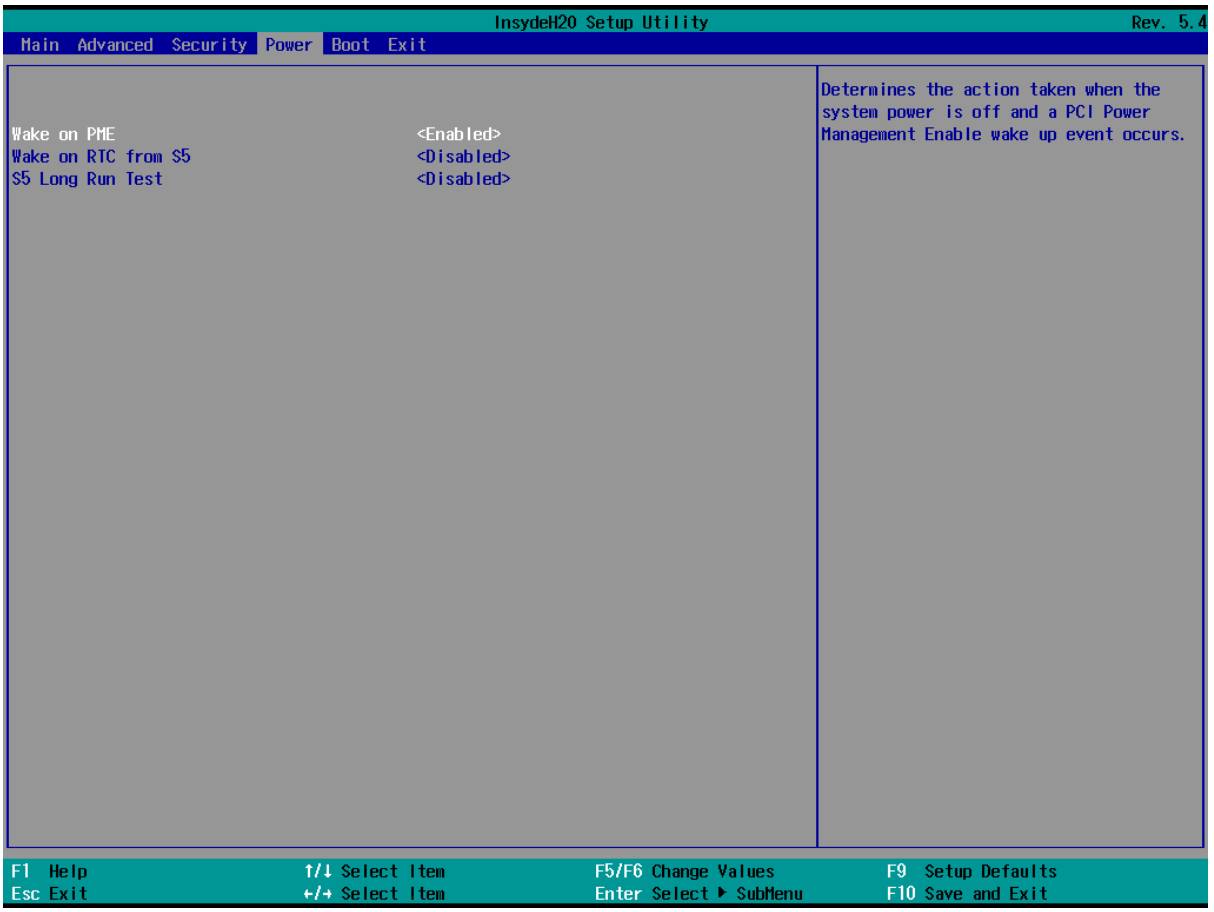
  TrEE Protocol Version: 1.0 or 1.1

- **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.

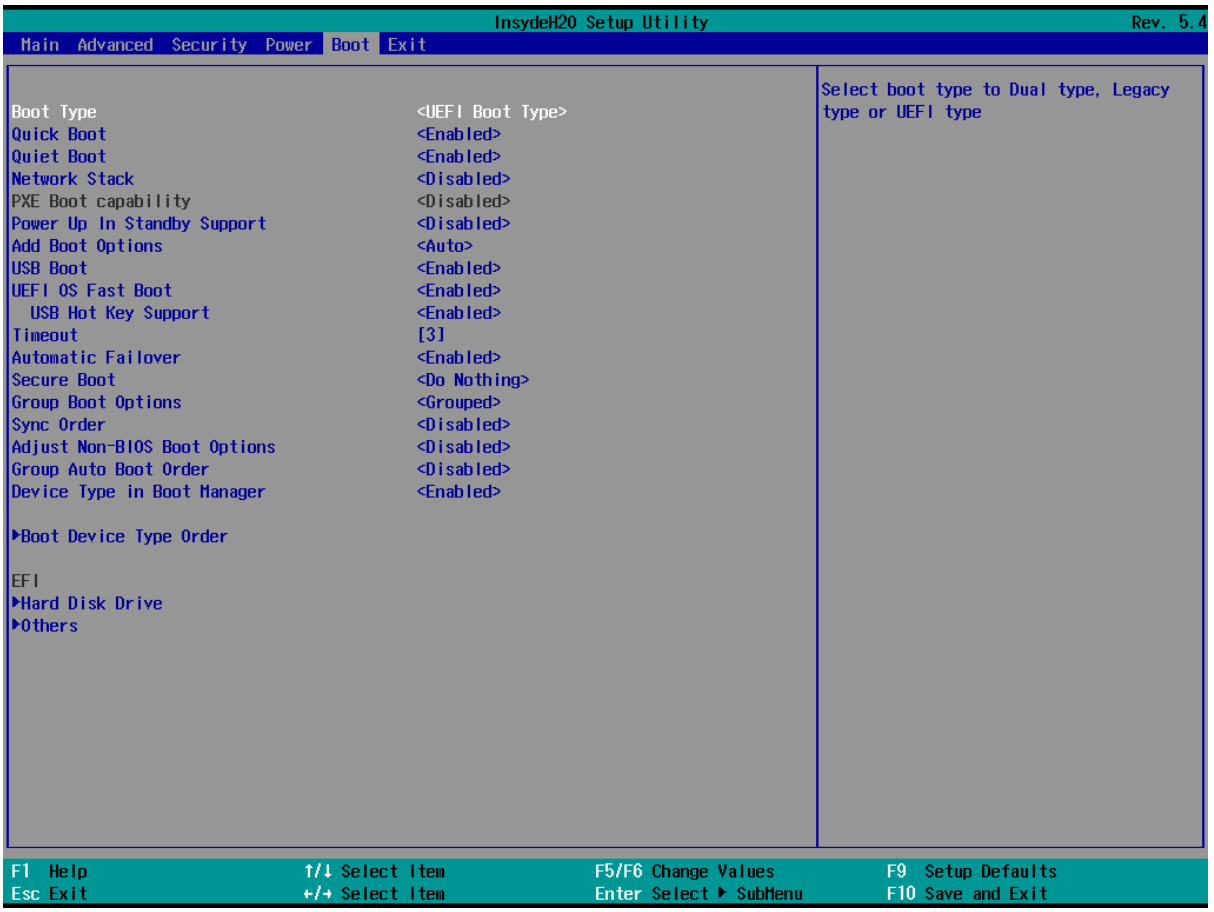
- **Wake on RTC from S5** (default value: Disabled; possible values: Disabled, By Every Day, By Day of Month)

  Wake on RTC from S5 state, By Day of Month, Fixed time of every day, By sleep time or By OS utility.

- **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 (non-POR), Legacy Boot Type (non-POR), 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: Enabled; 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

- **PXE/ HTTP Boot Retry Policy** (default value: 0; possible values: numbers between 0 and 255)

  PXE/ HTTP boot retry setting.

  The max value is 255, if you Enter 255, the retry will go INFINITELY.

- **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)

  The policy of how to insert new boot option into Boot Order. If boot options are not grouped, Auto is the same as First.

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

  Disables or enables booting to USB boot devices.

- **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: Enabled; 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.

- **Secure Boot** (default value: Do Nothing; possible values: Do Nothing, Enabled)

  Enable secure boot by H2OEZE.

- **Group Boot Options** (default value: Non-Grouped; possible values: Grouped, Non-Grouped)

  Boot options are grouped or not.

- **Sync Order** (read-only; possible values: Disabled, Sync Boot Order, Sync Boot Device Type Order)

  Disabled: No effect.

  Sync Boot Order: Group boot options in Boot Order is adjusted to follow boot device type priority.

  Sync Boot Device Type Order: Boot device type order is adjusted to follow the order of group boot options in Boot Order.

- **Adjust Non-BIOS Boot Options** (default value: Disabled; possible values: Disabled, Enabled)

  When enabled, position of Non-BIOS created boot options will be adjusted to follow boot options position policy each time before enumerate boot devices.

- **Group Auto Boot Order** (default value: Disabled; possible values: Disabled, Enabled)

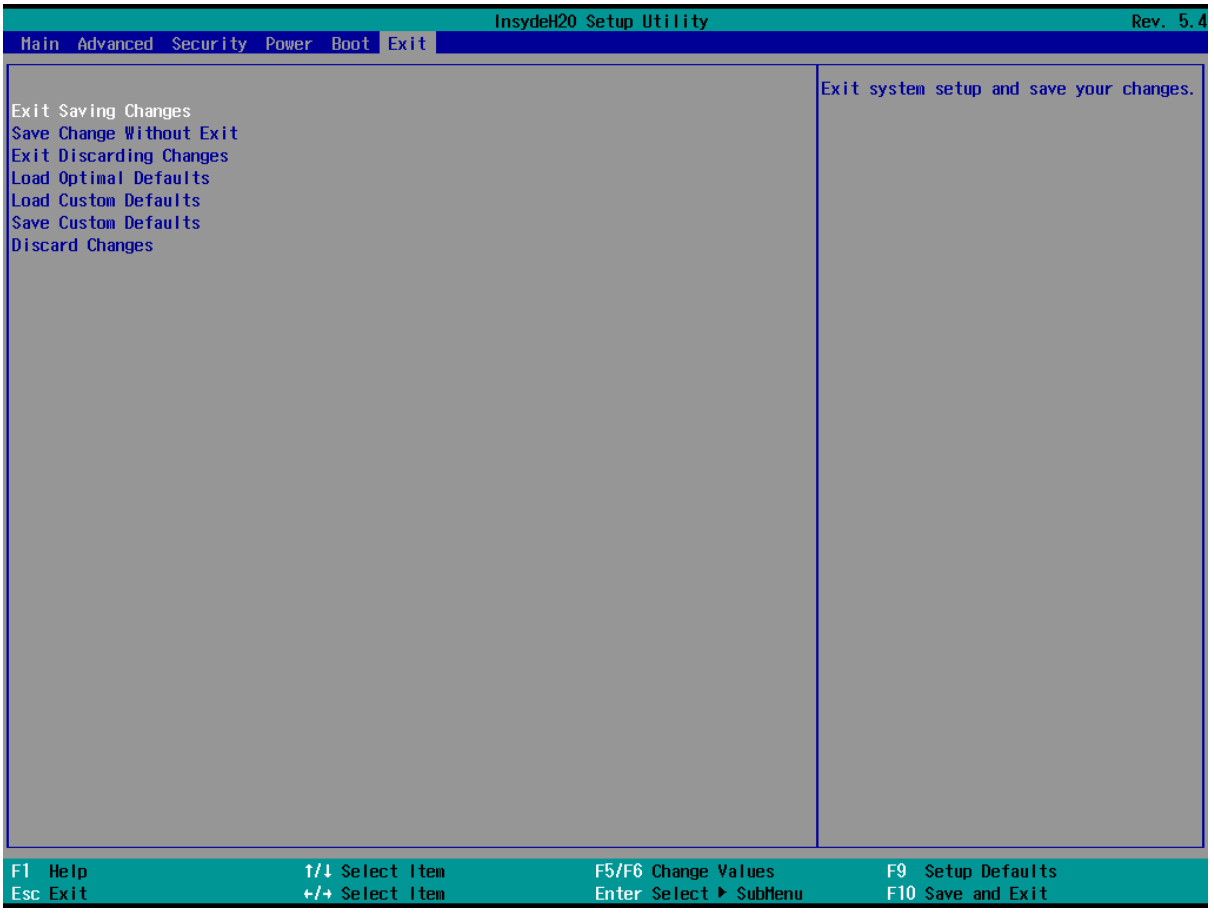
  When enabled, keep boot option order of each group in "Auto" position policy.

- **Device Type in Boot Manager** (default value: Enabled; possible values: Disabled, Enabled)

  Enabled: Show Boot Device Type Label in Boot Manager.

  Disabled: Hide Boot Device Type Label in Boot Manager.

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